

Мессенджер и ВКС

**Инструкция по настройке SSO-аутентификации
(SAML, OIDC, Kerberos)**

Оглавление

Назначение документа	4
Дополнительная документация	4
Предварительные условия для настройки SSO аутентификации	5
Функциональное описание	5
Механизм аутентификации по протоколу OIDC	7
Механизм аутентификации по протоколу SAML	9
Настройка SSO аутентификации по протоколам OIDC и SAML	11
Шаг 1. Настройка подсистемы авторизации сервера Мессенджер и ВКС	11
Шаг 2. Добавление провайдера аутентификации	15
Протокол OIDC	15
Протокол SAML	17
Шаг 3. Регистрация провайдеров аутентификации в сервисах Мессенджер и ВКС	20
Шаг 4. Настройка внешней аутентификации	22
Шаг 5. Настройка protocol mappers	23
Настройка SSO аутентификации по протоколу Kerberos в Microsoft Active Directory	24
Предварительная настройка на сервере Active Directory	24
Шаг 1. Создание файла .keytab	25
Шаг 2. Настройка realm	28
Шаг 3. Подключение пользователей из Keycloak через User Federation	28
Шаг 4. Регистрация Keycloak в сервисе Stdb	32
Шаг 5. Настройка внешней аутентификации	32
Шаг 6. Настройка браузеров для работы с Kerberos	33
Edge, Internet Explorer	33
Google chrome	36
Распространенные проблемы	38
Надпись «Server error» в веб-интерфейсе Мессенджер и ВКС, окно логина не открылось	38
Вместо окна логина отображается «Required parameter not found»	38
После логина появляется ошибка «Unexpected error when authenticating with identity provider»	38
Ошибка {"status": {"code": 40000, "reason": "Required parameter not found"}}	38

В логах Keycloak ошибка: Invalid argument (400) - Cannot find key of appropriate type to decrypt AP-REQ	39
Внутри пода Keycloak невозможно достучаться до контроллера домена	39
Внутри пода Keycloak необходимо настроить krb5.conf	40
	40

Назначение документа

В данной инструкции представлено описание процесса настройки Single Sign-On аутентификации по протоколам [SAML](#) и [OIDC](#), а также SSO-аутентификации по протоколу [Kerberos в Microsoft Active Directory](#).

Документ предназначен для использования администраторами организации.

Дополнительная документация

Архитектура и описание системы — в документе представлена информация о сервисах Мессенджер и ВКС, обеспечивающих функциональность SSO-аутентификации, а также расположение log-файлов данных сервисов. Не является частью публичной документации, обратитесь к представителю VK Tech, чтобы ознакомиться с документом.

Предварительные условия для настройки SSO аутентификации

Клиентские платформы в рамках запроса аутентификации должны поддерживать аутентификацию через внешнего провайдера аутентификации, в результате которой сервер отдаст ответ, содержащий email и atoken (ключ, необходимый для инициализации сессии и получения идентификатора сессии – aimsid), используемые далее при старте сессии мессенджера.

Необходимо отключить блокировку всплывающих окон в браузере, так как поддержка OIDC реализована через всплывающие окна.

Функциональное описание



Внешний провайдер аутентификации (Identity Provider) – провайдер осуществляющий аутентификацию и поддерживающий протоколы аутентификации SAML и OpenID Connect. Провайдером является SAML IDP или OIDC Authentication server.

В процессе аутентификации пользователя сервер Мессенджер и ВКС перенаправляет пользователя на провайдера аутентификации. Клиент переходит по указанным redirect'ам, пользователь вводит аутентификационные данные. Далее клиент начинает новую сессию мессенджера и пользуется идентификатором сессии (aimsid) во всех запросах. При отзыве access_token'a aimsid инвалидируется.

На клиентских приложениях aimsid хранится во внутреннем хранилище ОС в зашифрованном виде (за исключением web-версии), в соответствии с таблицей:

Платформа	Технология для хранения aimsid
Web	Cookie
MacOS	Симметрично зашифрован в локальном файле конфигурации
Windows	Симметрично зашифрован в локальном файле конфигурации
Linux	Симметрично зашифрован в локальном файле конфигурации

Платформа	Технология для хранения aimsid
iOS	Keychain
Android	Encrypted Shared Preferences

По окончании процесса аутентификации все управление токенами и взаимодействие с провайдером аутентификации осуществляется на стороне сервера Мессенджер и ВКС.

Хранением, обновлением, проверкой токенов занимается сервис Tokeeper. Сервис хранит данные, используя БД Tarantool. БД Tarantool отслеживает токены, период жизни которых истек, и автоматически удаляет их из базы.

Настройка взаимодействия «клиент – сервер Мессенджер и ВКС» представлена в разделе [Шаг 1.](#)

[Настройка подсистемы авторизации сервера VK Teams.](#)

Настройка взаимодействия «сервер Мессенджер и ВКС – Identity Provider» представлена в [Шагах 2-5.](#)

Ограничения Keycloak

Сервис Keycloak не взаимодействует с внешним провайдером аутентификации после авторизации. Соответственно, не сможет инвалидировать свою сессию при инвалидации сессии пользователя на внешнем провайдере аутентификации.

Однако, если инвалидировать сессию пользователя в сервисе Keycloak, клиент Мессенджер и ВКС разлогинит пользователя.

Одновременная работа с несколькими провайдерами аутентификации

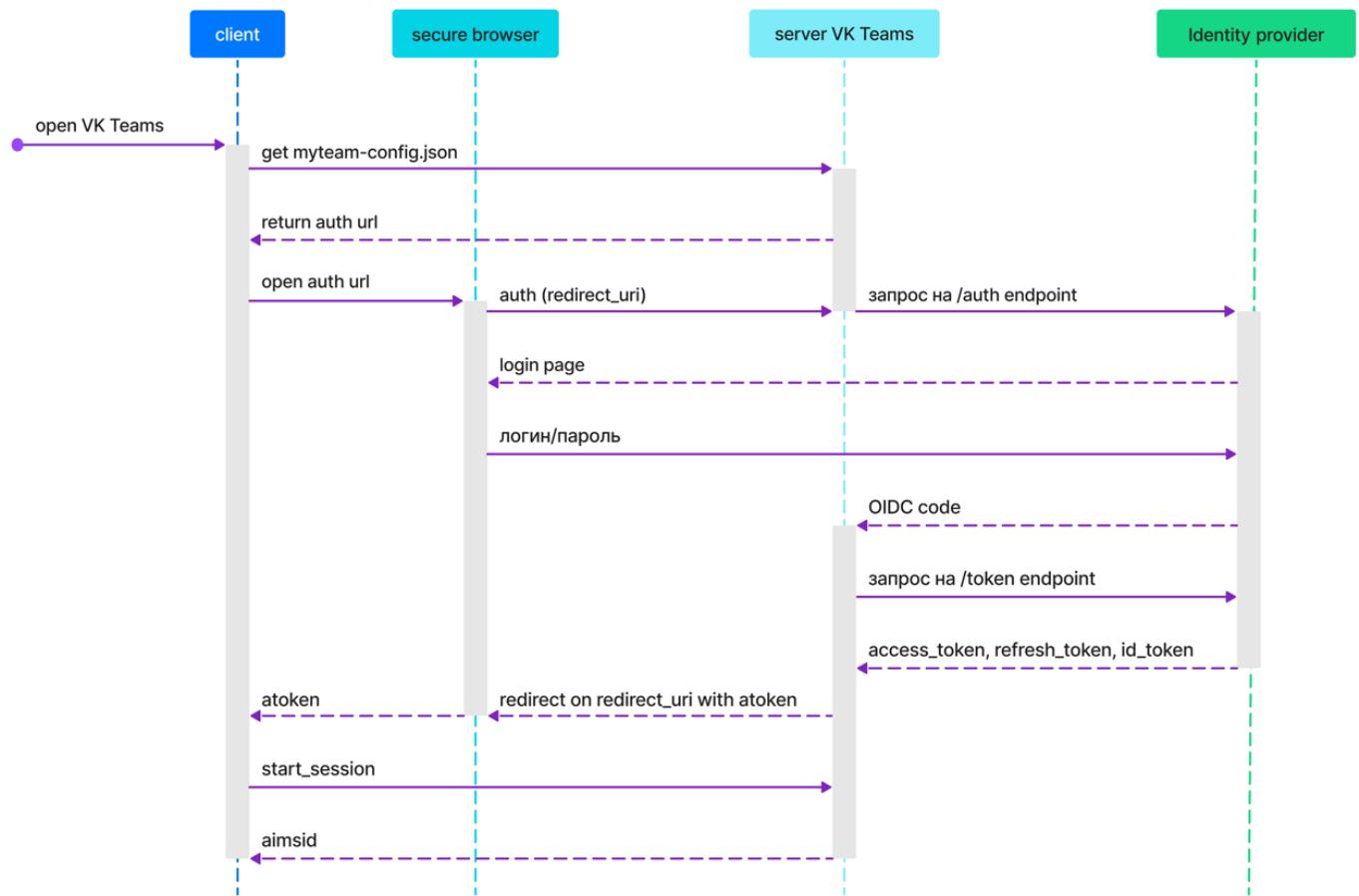
SSO аутентификация поддерживает аутентификацию через несколько провайдеров.

Выбор нужного провайдера осуществляется на основе useragent'a, переданного параметром в начале процесса аутентификации. Процесс настройки провайдеров представлен [ниже.](#)

Secure Browser

- Для iOS – ASWebAuthenticationSession.
- Для Android – Android Custom Tab.
- Для Web – Window.open.
- Для Desktop – открытие в стандартном браузере.

Механизм аутентификации по протоколу OIDC



1. Клиент из файла myteam-config.json получает auth-url для аутентификации (см. описание в [разделе](#)).
2. Сервер Мессенджер и ВКС составляет запрос в Identity Provider на /auth endpoint и перенаправляет на него клиента.
3. Пользователь (в secure browser) вводит аутентификационные данные:
 - если пользователем уже вошел в Систему, сработает SSO, и пользователю ничего вводить не потребуется;
 - в случае ошибки логина/пароля — об этом пользователю сообщит Identity Provider внутри secure_browser в окне логина («Invalid username or password») и предложит ввести логин/пароль повторно.
4. Identity Provider перенаправляет на указанный сервером redirect_uri, находящийся на сервере.
5. Сервер Мессенджер и ВКС обрабатывает redirect от Identity Provider:
 - в параметрах запроса получает:
 - state;
 - code.

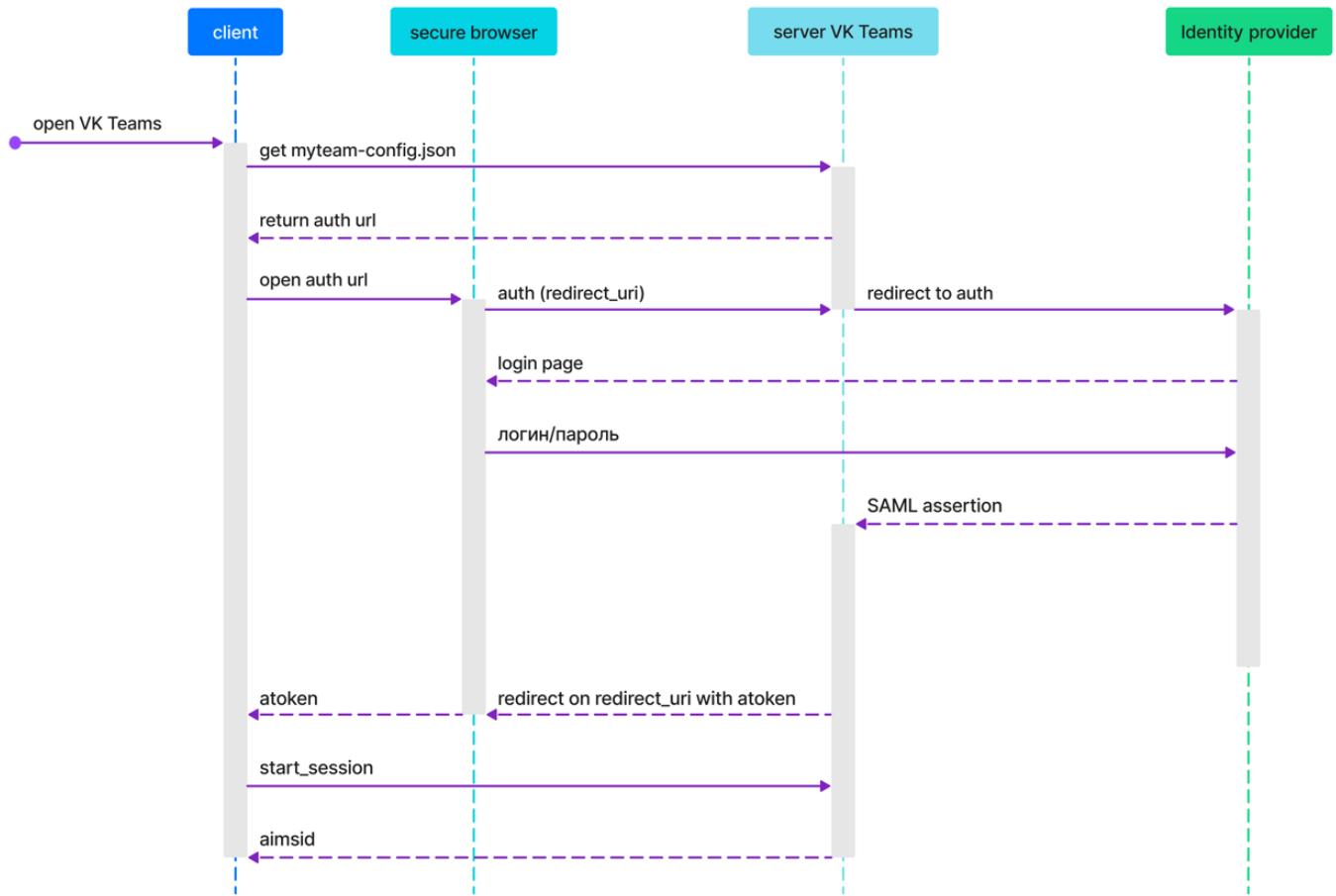
6. Сервер Мессенджер и ВКС составляет и отправляет запрос в Identity Provider на /token endpoint:

- в ответ получает необходимые токены и периоды их жизни (access_token, refresh_token, id_token и т.д.)
- сохраняет их, если ещё нет токенов для этого пользователя в хранилище сервера.

7. Сервер Мессенджер и ВКС завершает действия, необходимые для аутентификации, и осуществляет редирект на переданный redirect_uri, в параметрах передавая результат:

- code:
 - 20000 – успех;
 - 50000 - server error.
- reason — передается в случае ошибки;
- atoken;
- email;
- host_time.

Механизм аутентификации по протоколу SAML



1. Клиент из файла myteam-config.json получает auth-url для аутентификации (см. описание в [разделе](#)).
2. Сервер Мессенджер и ВКС составляет запрос в Identity Provider на /auth endpoint и перенаправляет на него клиента.
3. Пользователь (в secure browser) вводит аутентификационные данные:
 - если пользователем уже вошел в Систему, сработает SSO, и пользователю ничего вводить не потребуется;
 - в случае ошибки логина/пароля — об этом пользователю сообщит Identity Provider внутри secure_browser в окне логина («Invalid username or password») и предложит ввести логин/пароль повторно.
4. Identity Provider перенаправляет на указанный сервером redirect_uri, находящийся на сервере.
5. Сервер Мессенджер и ВКС обрабатывает redirect от Identity Provider:
 - в параметрах запроса получает:
 - state;
 - code.

6. Сервер Мессенджер и ВКС завершает действия, необходимые для аутентификации, и осуществляет редирект на переданный redirect_uri, в параметрах передавая результат:

- code:
 - 20000 – успех;
 - 50000 - server error.
- reason — передается в случае ошибки;
- atoken;
- email;
- host_time.

Настройка SSO аутентификации по протоколам OIDC и SAML

Необходимые шаги для включения SSO аутентификации представлены ниже:

Шаг 1. Настройка подсистемы авторизации сервера Мессенджер и ВКС

1. Перейти в веб-интерфейс сервиса Keycloak:

- открыть доступ для домена mridme. <DOMAIN> и перейти в браузере на <https://mridme.<DOMAIN>>



Примечание

По умолчанию имя mridme не заведено в DNS, и в настройках nginx выставлено deny all. Не рекомендуется использовать этот способ доступа без крайней необходимости.

или

- пробросить локальный порт на сервер:

```
ssh -L 8080:keycloak-http.keycloak.svc.cluster.local:80 centos@<server>
```

и перейти в браузере <http://127.0.0.1:8080/auth>

2. Логин: admin

Пароль: пароль необходимо получить в службе технической поддержки

3. Перейти **Manage** → **Clients** → выбрать **nomailcli** → вкладка **Settings** → установить значения для полей:

- **Valid redirect URIs** – https://u.<DOMAIN_EXAMPLE.COM>/api/v87/rapi/auth/oidc/submitCode, где <DOMAIN_EXAMPLE.COM> – ваш домен;
- **Client authentication** – **On**:

The screenshot shows the Keycloak Admin UI for a client configuration. The left sidebar is titled 'Manage' and includes 'Clients' (which is selected and highlighted with a red box), 'Client scopes', 'Realm roles', 'Users', 'Groups', 'Sessions', 'Events', 'Configure', 'Realm settings', 'Authentication', 'Identity providers', and 'User federation'. The main content area is titled 'Home URL' and contains fields for 'Valid redirect URIs' (with a red box around it), 'Valid post logout redirect URIs', 'Web origins', and 'Admin URL'. Below this is a 'Capability config' section with a 'Client authentication' toggle switch (set to 'On', highlighted with a red box) and an 'Authorization' toggle switch (set to 'Off'). Under 'Authentication flow', several options are listed: 'Standard flow' (checked), 'Direct access grants' (checked), 'Implicit flow' (unchecked), 'Service accounts roles' (unchecked), 'OAuth 2.0 Device Authorization Grant' (unchecked), and 'OIDC CIBA Grant' (unchecked). A vertical sidebar on the right is titled 'Jump to section' and lists 'General Settings', 'Access settings' (which is selected and highlighted with a blue box), 'Capability config', 'Login settings', and 'Logout settings'.

- Вкладка **Advanced** → **Advanced Settings** → поле **Proof Key for Code Exchange Code Challenge Method** → указать **S256**:

The screenshot shows the 'Advanced Settings' section for a client. The left sidebar is the same as the previous screenshot. The main content area is titled 'Advanced Settings' and includes fields for 'Access Token Lifespan' (set to 'Never expires'), 'Client Session Idle' (set to 'Never expires'), 'Client Session Max' (set to 'Never expires'), 'Client Offline Session Idle' (set to 'Never expires'), 'Client Offline Session Max' (set to 'Never expires'), 'OAuth 2.0 Mutual TLS Certificate Bound Access Tokens Enabled' (toggle switch set to 'Off'), and a 'Proof Key for Code Exchange Code Challenge Method' dropdown (set to 'S256', highlighted with a red box). A vertical sidebar on the right is titled 'Jump to section' and lists 'Revocation', 'Fine grain OpenID Connect configuration', 'Open ID Connect Compatibility Modes', 'Advanced Settings' (which is selected and highlighted with a blue box), and 'Authentication flow overrides'.

- Вкладка **Credentials** → поле **Client Authenticator** → указать **Client Id and Secret**:

KEYCLOAK

Clients > Client details

nomailcli (OpenID Connect)

Enabled Action

Manage Clients Client scopes Realm roles Users Groups Sessions Events Configure Realm settings Authentication Identity providers User federation

Client Authenticator Client Id and Secret

Client secret Save

Registration access token Regenerate

4. Необязательные параметры:

- Перейти **Realm settings** → вкладка **Tokens**:

можно указать время жизни различных токенов (на весь realm):

KEYCLOAK

myteam

Enabled Action

Manage Clients Client scopes Realm roles Users Groups Sessions Events Configure Realm settings Authentication Identity providers User federation

Tokens

General

Default Signature Algorithm RS256

Refresh tokens

Revoke Refresh Token Disabled

Access tokens

Access Token Lifespan 5 Minutes It is recommended for this value to be shorter than the SSO session idle timeout: 30 minutes

Access Token Lifespan 15 Minutes For Implicit Flow

Client Login Timeout 1 Minutes

- Перейти **Clients** → выбрать **nomailcli** → вкладка **Advanced** → **Advanced Settings**:

можно указать время жизни access_token:

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Advanced Settings

This section is used to configure advanced settings of this client related to OpenID Connect protocol

Access Token Lifespan Expires in 1 Minutes

Client Session Idle Expires in

Client Session Max Never expires

Client Offline Session Idle Never expires

Jump to section

Revocation

Fine grain OpenID Connect configuration

Open ID Connect Compatibility Modes

Advanced Settings

Authentication flow overrides

5. Проставить поведение при первом логине:

- Перейти **Configure** → вкладка **Identity providers** → выбрать провайдера → в поле **First login flow** указать «**first broker login**»:

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Client authentication Client secret sent as post

Client ID 1212121

Client Secret

Advanced

Advanced settings

Store tokens Off

Stored tokens readable Off

Trust Email Off

Account linking only Off

Hide on login page Off

First login flow first broker login

Post login flow None

Sync mode Import

Jump to section

General settings

OpenID Connect settings

Advanced settings

Шаг 2. Добавление провайдера аутентификации

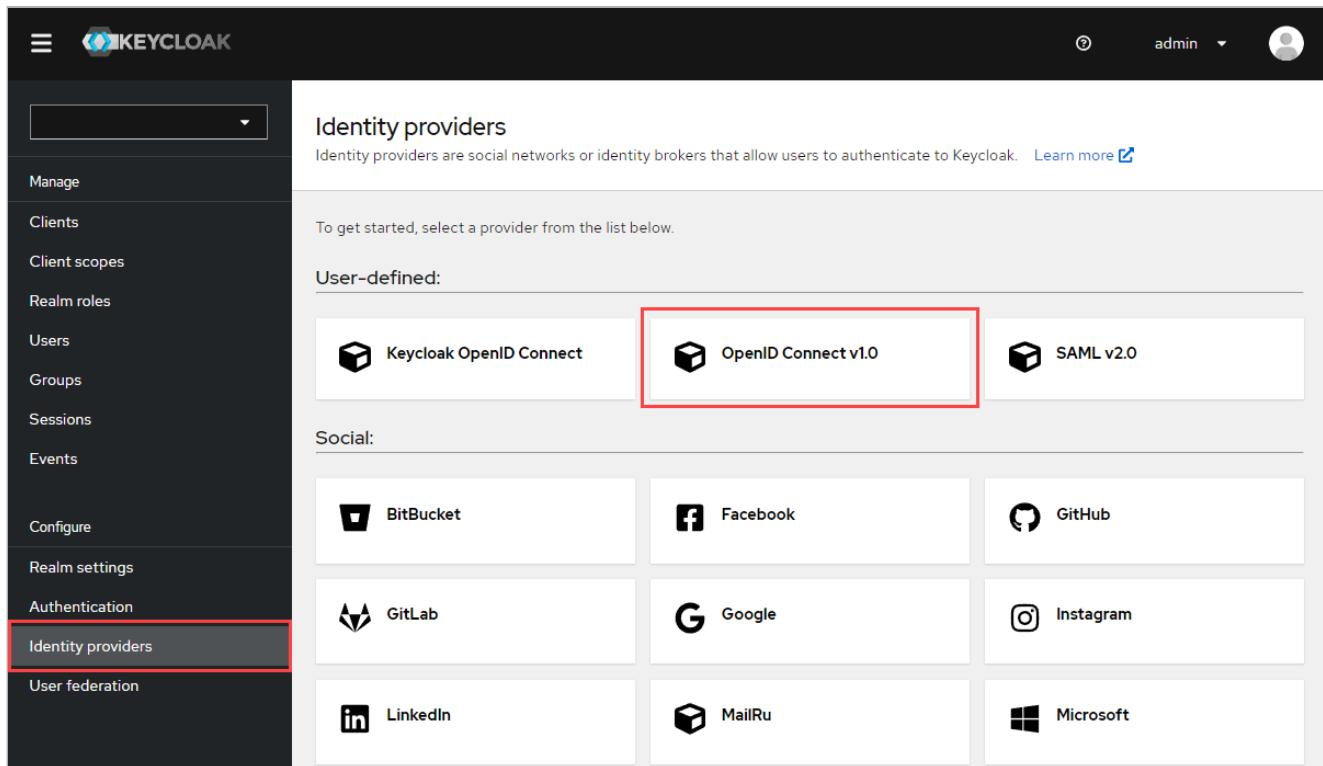
Протокол OIDC

Ниже представлено добавление провайдера аутентификации при использовании протокола OIDC. Если Вы используете протокол SAML, перейдите к разделу [Протокол SAML](#).

1. Проверить доступность адреса `mridme.<DOMAIN_TEAMS>`.

2. Создать и настроить провайдера аутентификации:

Перейти **Identity Providers** → выбрать необходимый протокол:



3. Указать следующие значения полей:

- **Alias** — задать Alias провайдера;
- **Display name** — задать имя провайдера;
- **Use discovery endpoint** — **Off**;
- **Authorization URL** — запросить у администратора Authentication server;
- **Token URL** — запросить у администратора Authentication server;
- **Logout URL** — запросить у администратора Authentication server;
- **User Info URL** — запросить у администратора Authentication server;
- **Issuer** — запросить у администратора Authentication server:

Identity providers > Add OpenID Connect provider

Add OpenID Connect provider

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Redirect URI: https://mridme.x5.onprem.ru/auth/realms/myteam/broker/oidc/endpoint

Alias *:

Display name *:

Display order:

OpenID Connect settings

Use discovery endpoint: Off

Import config from file: Drag a file here or browse to upload

Authorization URL *:

Token URL *:

Logout URL:

User Info URL:

Issuer:

- **Validate Signatures — On;**
- **Use JWKS URL — On;**
- **JWKS URL** — запросить у администратора Authentication server;
- **Client authentication — Client secret sent as post;**
- **Client ID** — запросить у администратора Authentication server;
- **Client Secret** — запросить у администратора Authentication server:

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Issuer:

Validate Signatures: On

Use JWKS URL: On

JWKS URL:

Use PKCE: Off

Client authentication: Client secret sent as post

Client ID *:

Client Secret *:

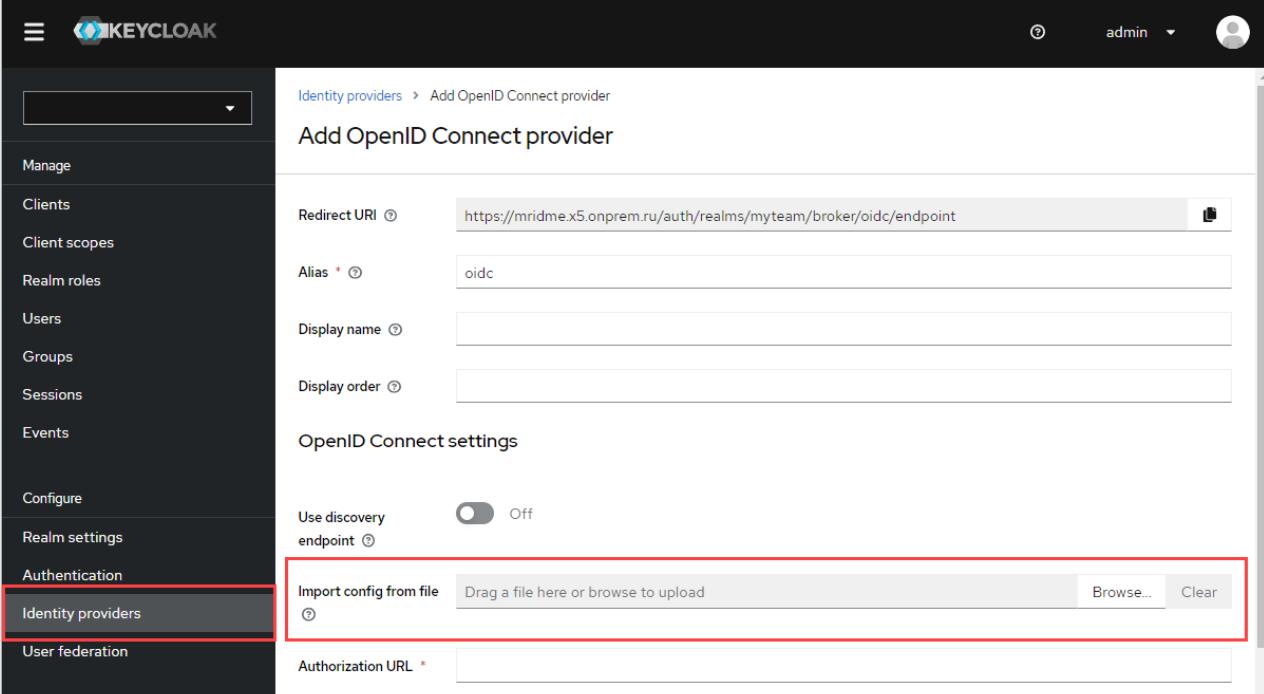
Примечание

Данные поля также можно заполнить, импортировав файл конфигурации. Запросить Import External Config можно у администратора Authentication server.

- Перетащить файл в поле **Import config from file**

ИЛИ

- В поле **Import config from file** нажать **Browse** → выбрать файл <Import External Config>:



The screenshot shows the Keycloak administration interface. The left sidebar has a dark theme with white text. The 'Identity providers' menu item is highlighted with a red box. The main content area is titled 'Add OpenID Connect provider'. It contains fields for 'Redirect URI' (set to <https://mridme.x5.onprem.ru/auth/realms/myteam/broker/oidc/endpoint>), 'Alias' (set to 'oidc'), 'Display name' (empty), 'Display order' (empty), and 'OpenID Connect settings'. Under 'OpenID Connect settings', there is a toggle switch for 'Use discovery endpoint' which is set to 'Off'. At the bottom, there is an 'Import config from file' input field with the placeholder 'Drag a file here or browse to upload' and a 'Browse...' button. This 'Import config from file' field is also highlighted with a red box.

4. Нажать **Save**.

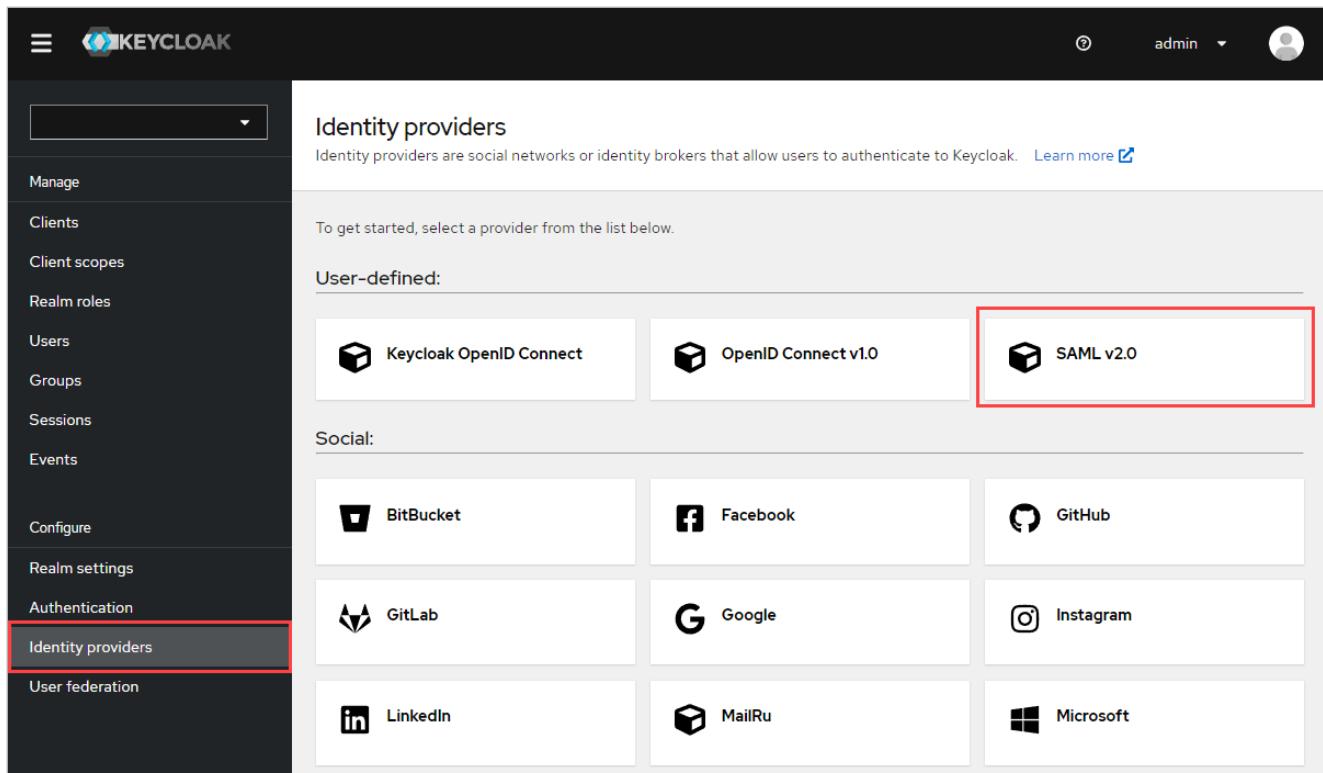
Протокол SAML

Ниже представлено добавление провайдера аутентификации при использовании протокола SAML. Если Вы используете протокол OIDC, перейдите к разделу [Шаг 3. Регистрация провайдеров аутентификации в сервисах Мессенджер и ВКС](#).

1. Проверить доступность адреса mridme.<DOMAIN_TEAMS>.

2. Создать и настроить провайдера аутентификации:

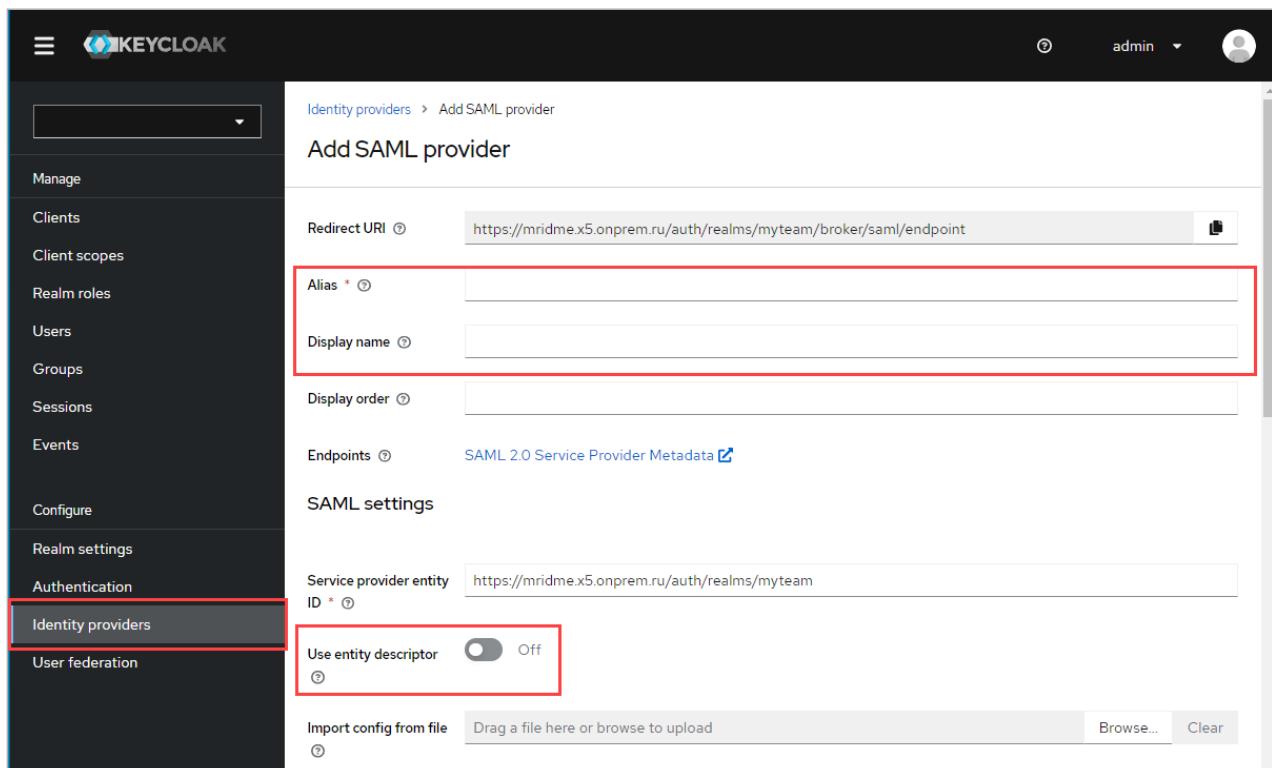
Перейти **Identity Providers** → выбрать необходимый протокол:



The screenshot shows the Keycloak administration interface. The left sidebar is dark with white text, showing a list of management options: Manage, Clients, Client scopes, Realm roles, Users, Groups, Sessions, Events, Configure, Realm settings, Authentication, Identity providers (which is selected and highlighted with a red box), and User federation. The main content area is titled 'Identity providers' with the sub-instruction 'Identity providers are social networks or identity brokers that allow users to authenticate to Keycloak.' Below this, a message says 'To get started, select a provider from the list below.' The providers are categorized into 'User-defined:' and 'Social:'. Under 'User-defined:', there are three boxes: 'Keycloak OpenID Connect', 'OpenID Connect v1.0', and 'SAML v2.0', with the latter being the selected provider and highlighted with a red box. Under 'Social:', there are three rows of three providers each: BitBucket, Facebook, GitHub; GitLab, Google, Instagram; LinkedIn, MailRu, Microsoft.

3. Указать следующие значения полей:

- **Alias** — задать Alias провайдера;
- **Display name** — задать имя провайдера;
- **Use entity descriptor — Off**:



The screenshot shows the 'Add SAML provider' page within the Keycloak administration interface. The left sidebar is identical to the previous screenshot, with the 'Identity providers' section selected and highlighted with a red box. The main form is titled 'Add SAML provider'. It contains several input fields: 'Redirect URI' with the value 'https://mridme.x5.onprem.ru/auth/realms/myteam/broker/saml/endpoint'; 'Alias' (marked with a red box) and 'Display name' (also marked with a red box); 'Display order'; 'Endpoints' with a link to 'SAML 2.0 Service Provider Metadata'; 'SAML settings'; 'Service provider entity ID' with the value 'https://mridme.x5.onprem.ru/auth/realms/myteam'; and a toggle switch for 'Use entity descriptor' which is set to 'Off' (also highlighted with a red box). At the bottom, there are buttons for 'Import config from file' (with a placeholder 'Drag a file here or browse to upload'), 'Browse...', and 'Clear'.

- **Single Sign-On service URL** — запросить у администратора IDP-сервера;
- **Single logout service URL** — запросить у администратора IDP-сервера;
- **NameID policy format** — **Unspecified**;
- **HTTP-POST binding response** — **On**;

- HTTP-POST binding for AuthnRequest – On;

- HTTP-POST binding logout – On:

Single Sign-On service URL * (empty)

Single logout service URL (empty)

Backchannel logout Off

NameID policy format Unspecified

Principal type Subject NameID

Allow create On

HTTP-POST binding response On

HTTP-POST binding for AuthnRequest On

HTTP-POST binding logout On

- Allowed clock skew – 30:

Pass subject Off

Allowed clock skew 30

Attribute Consuming Service Index (empty)

Attribute Consuming Service Name (empty)

Add Cancel

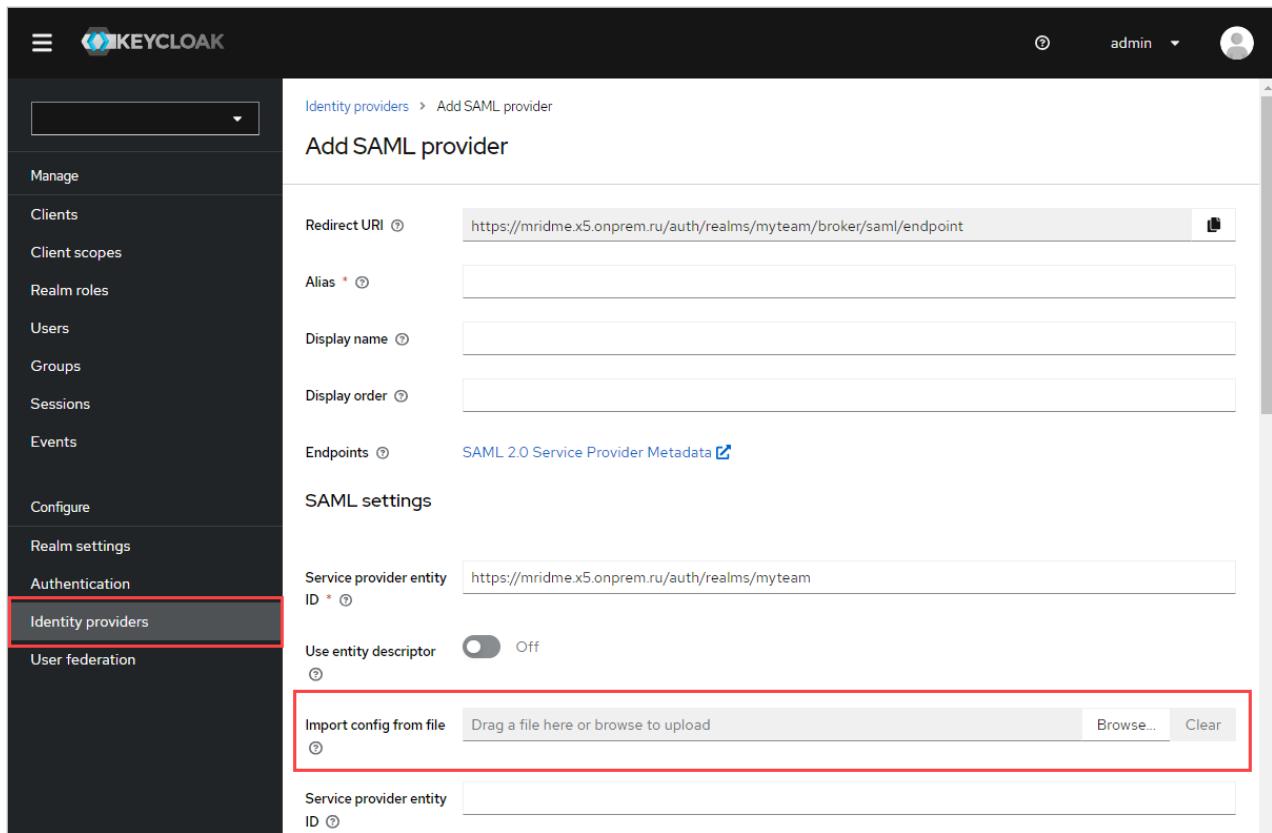
Примечание

Данные поля также можно заполнить, импортировав файл конфигурации. Запросить Import External Config можно у администратора IDP-сервера.

- Перетащить файл в поле **Import config from file**

ИЛИ

- В поле **Import config from file** нажать **Browse** → выбрать файл <Import External Config>:



The screenshot shows the Keycloak administration interface. The left sidebar has a 'Manage' section with links: Clients, Client scopes, Realm roles, Users, Groups, Sessions, Events, Configure, Realm settings, Authentication, **Identity providers** (which is selected and highlighted with a red box), and User federation. The main content area is titled 'Add SAML provider'. It contains fields for 'Redirect URI' (https://mridme.x5.onprem.ru/auth/realm/myteam/broker/saml/endpoint), 'Alias' (empty), 'Display name' (empty), 'Display order' (empty), 'Endpoints' (SAML 2.0 Service Provider Metadata), 'SAML settings', 'Service provider entity ID' (https://mridme.x5.onprem.ru/auth/realm/myteam), and a toggle for 'Use entity descriptor' which is off. Below these is a section for 'Import config from file' with a 'Browse...' and 'Clear' button, and another 'Service provider entity ID' field. The 'Import config from file' section is also highlighted with a red box.

4. Нажать **Save**.

Шаг 3. Регистрация провайдеров аутентификации в сервисах Мессенджер и ВКС

Провайдеры регистрируются в сервисе Stdb. Оттуда информацию о них получают сервисы Front и Tokeeper.

SSO аутентификация поддерживает аутентификацию через несколько провайдеров.

Возможна поддержка нескольких провайдеров в двух форматах:

Вариант 1. Сервис Keycloak подключается к провайдеру аутентификации в режиме посредника, все взаимодействие с провайдером лежит на сервисе Keycloak.

Настроить выбор провайдера для различных вариантов подключения:

- Подключиться к сервису Stdb:

```
rlwrap nc stdb.vkteams.svc.cluster.local. 4020
```

- Далее добавить таблицу с данными провайдеров:

```
stdb_table_add idp_configurations issuer@string addr@string client_id@string scope@string
client_secret@string platforms_and_auth_extra_params@string need_register_user@string

# для версий до 25.2
stdb_row_add idp_configurations KK https://di.<DOMAIN_EXAMPLE.COM>/auth/realm/
myteam/.well-known/openid-configuration nomailcli openid use_secrets_luke '{ "web":
"di_idp_hint=<Alias_1>", "desktop": "di_idp_hint=<Alias_2>", "default":
"di_idp_hint=<Alias_3>" }' false

# Если поле default пусто и нет алиасов

stdb_row_add idp_configurations KK https://di.<DOMAIN_EXAMPLE.COM>/auth/realm/
myteam/.well-known/openid-configuration nomailcli openid use_secrets_luke { "default": "" }
false

# для версии 25.2 и выше
stdb_row_add idp_configurations KK https://kc.<DOMAIN_EXAMPLE.COM>/auth/realm/
myteam/.well-known/openid-configuration nomailcli openid use_secrets_luke '{ "web":
"kc_idp_hint=<Alias_1>", "desktop": "kc_idp_hint=<Alias_2>", "default":
"kc_idp_hint=<Alias_3>" }' false
```

где `<Alias_1>`, `<Alias_2>`, `<Alias_3>` – значение поля **Alias** для провайдеров в Keycloak (см. [Шаг 2. Добавление провайдера аутентификации](#)).

Для разграничения платформ используется поле **platforms_and_auth_extra_params** таблицы сервиса Stdb. Уточнения значения этого поля:

- `default` – переходим на базовую страницу авторизации сервиса Keycloak.
- `di_idp_hint` или `kc_idp_hint=<Alias` провайдера в настройках Keycloak`>`.

Доступные платформы:

- Web;
- Android;
- Desktop;
- IOS.

Внимание

Если одну и ту же платформу указать для нескольких провайдеров, сервис Stdb сообщит об этом в лог, SSO аутентификация работать не будет.

Примечание

Полезные команды в rlwrap:

- get //получить список:

```
stldb_table_get idp_configurations
```

- del // удалить:

```
stldb_row_del idp_configurations 1
```

- set // изменить:

```
# для версий до 25.2
stldb_row_set idp_configurations 1 KK http://di.<DOMAIN_EXAMPLE.COM>/auth/realm/myteam/.well-known/openid-configuration nomailcli openid use_secrets_luke '{ "web": "di_idp_hint=saml", "desktop": "di_idp_hint=saml", "default": "di_idp_hint=ws1" }' false
```

```
# для версии 25.2 и выше
stldb_row_set idp_configurations 1 KK http://kc.<DOMAIN_EXAMPLE.COM>/auth/realm/myteam/.well-known/openid-configuration nomailcli openid use_secrets_luke '{ "web": "kc_idp_hint=saml", "desktop": "kc_idp_hint=saml", "default": "kc_idp_hint=ws1" }' false
```

Вариант 2. Отдельная регистрация каждого провайдера: в таблицу каждый провайдер добавляется новой строкой.

Шаг 4. Настройка внешней аутентификации

1. Добавьте в конфигурационный файл **/usr/local/nginx-im/html/myteam/myteam-config.json** указанное содержимое:

```
"oauth-authorization": {
  "enabled": true,
  "config": {
    "auth-url": "https://u.<DOMAIN_EXAMPLE.COM>/api/v87/rapi/auth/oidc/authorize"
  }
},
```

2. Для инсталляции на одну виртуальную машину выполните команду:

```
HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t godmod
```

Для кластерной инсталляции:

```
HELMWAVE_USE_LOCAL_REPO_CACHE=true HELMWAVE_ENV_NAME=cluster hwup -t godmod
```

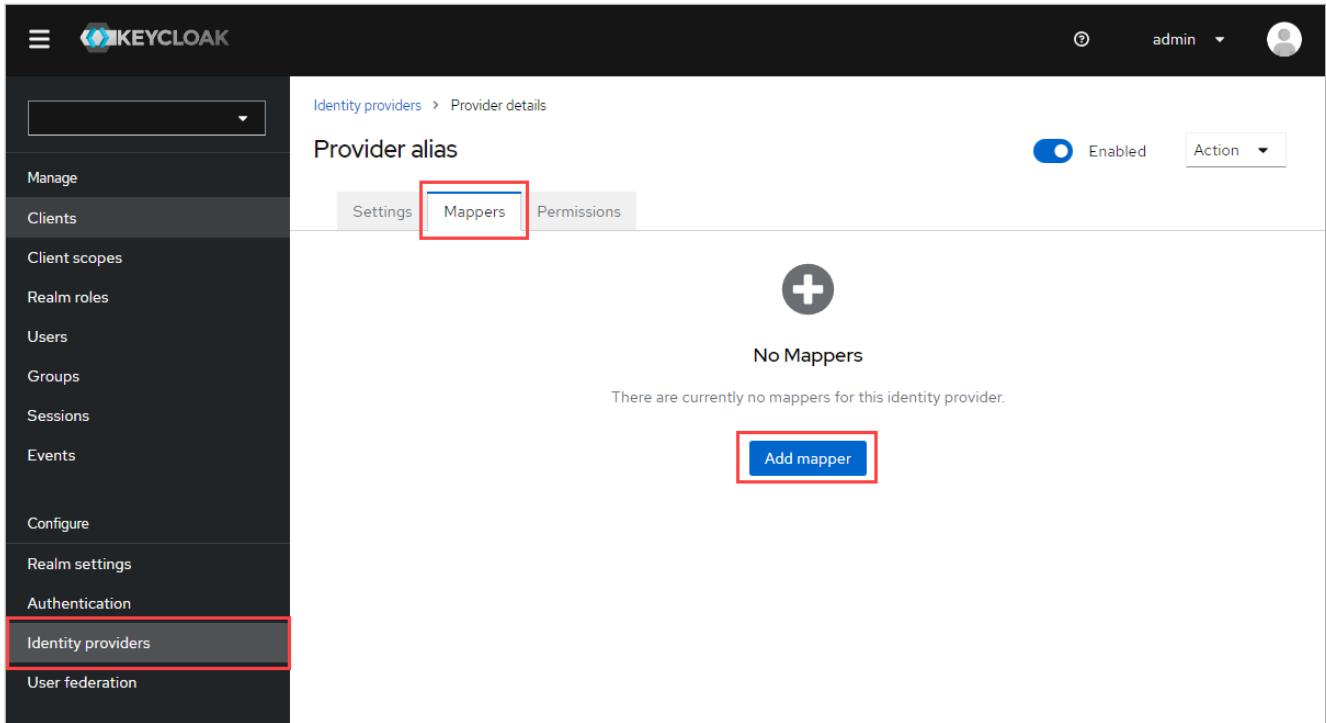
3. Перезапустите под в технологическое окно (может приводить к сбою в новых подключениях):

```
kubectl delete pods -n vkteams -l app=myteam-admin
```

Шаг 5. Настройка protocol mappers

Необходимо настроить по три mapper'a для каждого провайдера — **email**, **lastName** и **firstName**.

1. Перейти **Identity Providers** → выбрать провайдера → вкладка **Mappers** → нажать **Add mapper**:



The screenshot shows the Keycloak administration interface. On the left, a sidebar menu is open with the following items: Manage, Clients, Client scopes, Realm roles, Users, Groups, Sessions, Events, Configure, Realm settings, Authentication, Identity providers (which is highlighted with a red box), and User federation. The main content area is titled 'Identity providers > Provider details' for a provider named 'Provider alias'. The 'Mappers' tab is selected and highlighted with a red box. A large 'No Mappers' message is displayed, along with a 'Add mapper' button, which is also highlighted with a red box. The top right corner shows the user is 'admin'.

2. Указать следующие значения полей:

- **Name** — задать имя mapper'a;
- **Sync mode override** — **Inherit**;
- **Mapper type** — **Attribute Importer**;
- **Claim** — маска для поиска атрибута в токене (запросить у администратора IDP-сервера);
- **User Attribute Name** — прописать один из вариантов — **email**; **lastName** или **firstName**:

The screenshot shows the Keycloak administration interface. The left sidebar has a 'myteam' dropdown and a list of management options: Manage, Clients, Client scopes, Realm roles, Users, Groups, Sessions, Events, Configure, Realm settings, Authentication, Identity providers (which is selected and highlighted with a red box), and User federation. The main content area is titled 'Edit Identity Provider Mapper' and shows a configuration form for an 'email' mapper. The form includes fields for Name (email), Sync mode override (Inherit), Mapper type (Attribute Importer), Claim (email), and User Attribute Name (email). At the bottom are 'Save' and 'Cancel' buttons. A red box highlights the 'Identity providers' menu item in the sidebar.

3. Нажать **Save**.

4. Повторить шаги 1-4 для создания остальных двух mappers.

Настройка SSO аутентификации по протоколу Kerberos в Microsoft Active Directory

Предварительная настройка на сервере Active Directory

На контроллере домена необходимо зарегистрировать учетную запись.

В разделе **Account** ввести в поле **User logon name** `HTTP/<почтовый домен>`.

В окне **Account options** внутри того же раздела отметьте чекбоксы:

- User cannot change password.
- Password never expires.
- This account supports Kerberos AES 128 bit encryption.
- This account supports Kerberos AES 256 bit encryption.
- Do not require Kerberos preauthentication.

Затем в разделе управления групповыми политиками перейдите к настройке политики `Configure encryption types allowed for Kerberos`.

Во вкладке **Security Policy Setting** отметьте следующие политики:

- RC4_HMAC_MD5.
- AES128_HMAC_SHA1.
- AES256_HMAC_SHA1.

Шаг 1. Создание файла .keytab

В зависимости от выбранного типа шифрования — [RC4-HMAC-NT](#) или [AES128-SHA1, AES256-SHA1](#) — выполните шаги, представленные ниже:

При использовании шифрования RC4-HMAC-NT

1. Получить параметр `msDS-KeyVersionNumber`:

```
Get-ADUser -Identity i.ivanov -Properties msDS-KeyVersionNumber
```

`msDS-KeyVersionNumber` — атрибут объекта учетной записи в Active Directory, который указывает версию ключа, используемого для шифрования данных, связанных с этой учетной записью.

Аналогично `kvno_number` в Kerberos, но специфично для Active Directory.

2. На Windows Server сгенерировать файл .keytab для Kerberos аутентификации в Active Directory:

```
ktpass -princ HTTP/computer.contoso.com@CONTOSO.COM -mapuser CONTOSO\keycloak -out mcs.keytab -crypto ALL -ptype KRB5_NT_PRINCIPAL /pass "SomePassword" -kvno kvno_number
```

, где:

- `-princ` — FQDN сервера Keycloak в формате «HTTP/computer.contoso.com@CONTOSO.COM» для организации связи между сервисом Keycloak и Active Directory



Примечание

Данный параметр учитывает регистр.

- `-mapuser` — пользователь, для которого регистрируется SPN и генерируется файл .keytab;
- `-pass` — пароль пользователя;
- `-crypto` — тип шифрования. Чтобы сгенерировать файл .keytab, поддерживающий все способы шифрования, укажите для ключа `-crypto` значение `ALL`;
- `-ptype` — тип принципала;
- `-out` — имя создаваемого файла .keytab.
- `kvno` — номер версии ключа для идентификации версии ключа шифрования, используемого для защиты данных. `kvno_number` должен быть равен следующему значению:

```
msDS-KeyVersionNumber + 1
```

3. Проверить значение параметра `msDS-KeyVersionNumber`, он должен быть равен значению `kvno_number` из предыдущей команды.
4. Дополнительно включить шифрование RC4-HMAC-NT в контейнере с Keycloak (оно автоматически отключается, так как считается слабым):

- создать файл через любой текстовый редактор (название указать любое, в примере использовано название файла **allow-weak**) со следующим содержимым:

```
[libdefaults]
allow_weak_crypto = true
permitted_enctypes = aes256-cts-hmac-sha1-96 aes256-cts-hmac-sha384-192 camellia256-
cts-cmac aes128-cts-hmac-sha1-96 aes128-cts-hmac-sha256-128 camellia128-cts-cmac
arcfour-hmac
```

- создать ConfigMap на основе файла, созданного на предыдущем шаге:

```
kubectl create configmap krb5-week-conf --from-file=allow-weak --namespace=keycloak
```

- чтобы отредактировать deployments выполните команду:

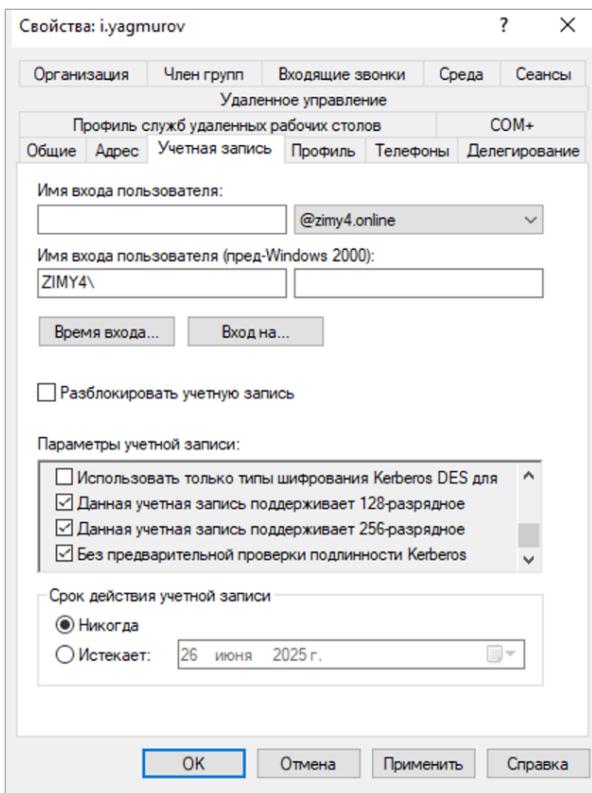
```
kubectl -n keycloak edit deployments
```

- добавить строки в секции `volumeMounts:` и `volumes:`:

```
spec:
  template:
    spec:
      containers:
        volumeMounts:
          - mountPath: /etc/krb5.conf.d/
            name: krb5-week-conf
        volumes:
          - configMap:
              defaultMode: 420
              name: krb5-week-conf
            name: krb5-week-conf
```

При использовании шифрования AES128-SHA1, AES256-SHA1

1. При использовании шифрования AES128-SHA1, AES256-SHA1 необходимы настройки для пользователей в Active Directory. В свойствах учетных записей пользователей необходимо установить поддержку типов шифрования AES128-SHA1, AES256-SHA1 — либо через групповые политики, либо вручную.



2. Получить параметр `msDS-KeyVersionNumber` :

```
Get-ADUser -Identity i.ivanov -Properties msDS-KeyVersionNumber
```

`msDS-KeyVersionNumber` — атрибут объекта учетной записи в Active Directory, который указывает версию ключа, используемого для шифрования данных, связанных с этой учетной записью. Аналогично `kvno_number` в Kerberos, но специфично для Active Directory.

3. На Windows Server сгенерировать файл .keytab для Kerberos аутентификации в Active Directory :

```
ktpass -princ HTTP/computer.contoso.com@CONTOSO.COM -mapuser CONTOSO\keycloak -out mcs.keytab -crypto ALL -ptype KRB5_NT_PRINCIPAL /pass "SomePassword" -kvno kvno_number
```

, где:

- `-princ` — FQDN сервера Keycloak в формате «HTTP/computer.contoso.com@CONTOSO.COM» для организации связи между сервисом Keycloak и Active Directory

Примечание

Данный параметр учитывает регистр.

- `-mapuser` — пользователь, для которого регистрируется SPN и генерируется файл .keytab;
- `-pass` — пароль пользователя;
- `-crypto` — тип шифрования. Чтобы сгенерировать файл .keytab, поддерживающий все способы шифрования, укажите для ключа `-crypto` значение `ALL`;
- `-ptype` — тип принципала;
- `-out` — имя создаваемого файла .keytab.

4. Создать секрет из файла .keytab и прокинуть его внутрь контейнера с Keycloak:

```
kubectl -n keycloak create secret generic keycloak-keytab --from-file=mcs_new.keytab --dry-run=client -o yaml | kubectl apply -f -
```

5. Проверить наличие нового .keytab файла и сравнить kvno с актуальным:

```
klist -k /path/to/keytab
```

Если внутри пода неактуальный kvno (устаревший .keytab), то перезапустите под и повторите проверку. Внутри пода команда `klist` по умолчанию недоступна, чтобы получить файл из пода выполните команду:

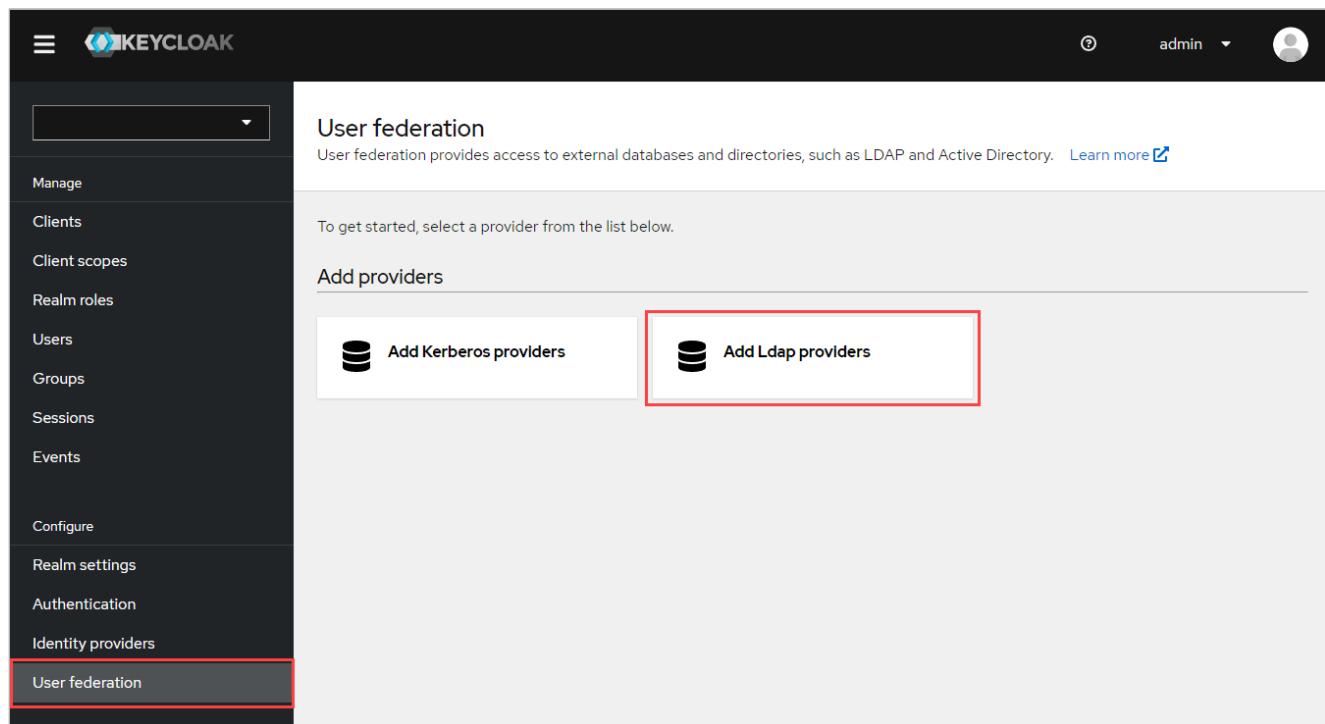
```
kubectl cp -n keycloak keycloak-7d7d67fd79-1vckt:/path/to/keytab/in/pod /path/to/keytab/on/machine
```

Шаг 2. Настройка realm

Перейдите в веб-интерфейс сервиса Keycloak и выполните все действия из раздела [Шаг 1. Настройка подсистемы авторизации сервера Мессенджер и ВКС](#).

Шаг 3. Подключение пользователей из Keycloak через User Federation

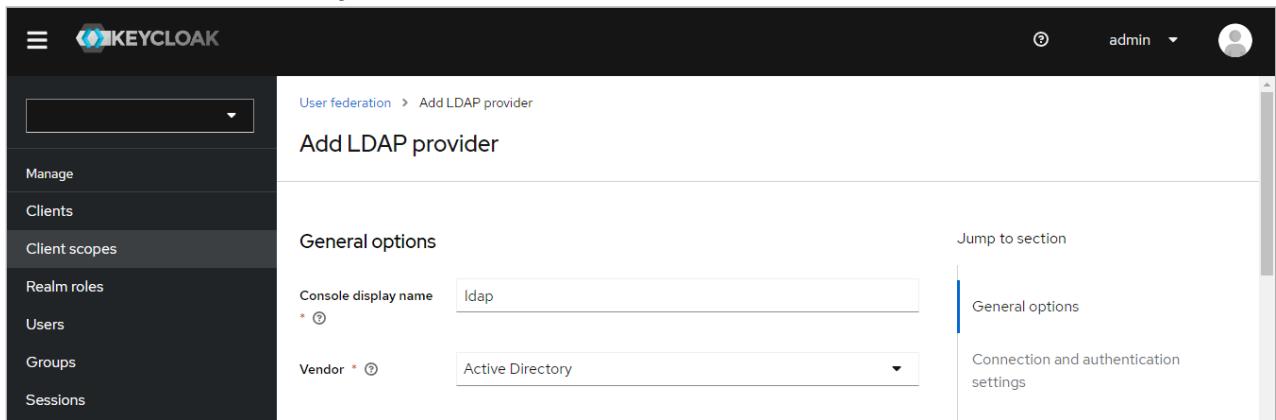
1. Перейти в раздел **Configure** → **User federation** → нажать на кнопку **Add Ldap providers**:



The screenshot shows the Keycloak configuration interface. The left sidebar has a red box around the 'User federation' item. The main content area is titled 'User federation' and contains the text: 'User federation provides access to external databases and directories, such as LDAP and Active Directory.' Below this is a note: 'To get started, select a provider from the list below.' Under the heading 'Add providers', there are two buttons: 'Add Kerberos providers' and 'Add Ldap providers', with the 'Add Ldap providers' button also having a red box around it.

2. Установить следующие значения полей:

- **Vendor – Active Directory:**



Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

User federation > Add LDAP provider

Add LDAP provider

General options

Console display name: ldap

Vendor: Active Directory

Jump to section

General options

Connection and authentication settings

- **Connection URL** – IP-адрес контроллера домена Active Directory.

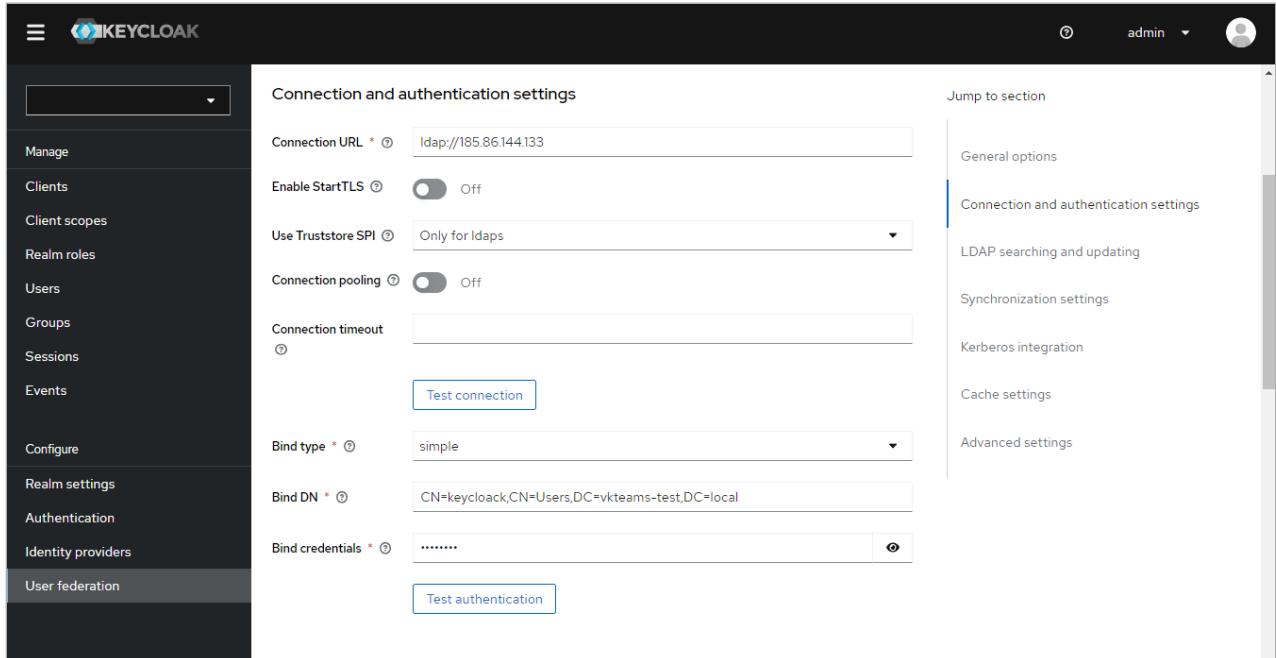
При использовании защищенного соединения, указать протокол **ldaps** и сделать активными переключатели:

- **Enable StartTLS – On;**
- **Connection pooling – On.**

Для проверки настроенного соединения нажать на кнопку **Test connection**. При успешном соединении получаем сообщение «Successfully connected to LDAP».

- Указать Bind DN и пароль пользователя, от имени которого планируется подключаться к Active Directory.

Для проверки подключения к Active Directory нажать на кнопку **Test authentication**. При успешном соединении получаем сообщение «Successfully connected to LDAP».



Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Connection and authentication settings

Connection URL: ldap://185.86.144.133

Enable StartTLS: On

Use Truststore SPI: Only for ldaps

Connection pooling: Off

Connection timeout: 0

Test connection

Bind type: simple

Bind DN: CN=keycloak,CN=Users,DC=vkteams-test,DC=local

Bind credentials:

Test authentication

Jump to section

General options

Connection and authentication settings

LDAP searching and updating

Synchronization settings

Kerberos integration

Cache settings

Advanced settings

3. Определите в каком параметре передается `username`. Пример команды:

```
ldapsearch -x -D "CN=Administrator,CN=Users,DC=contoso,DC=com" -H ldap://<AD IP> -b "CN=Users,DC=contoso,DC=com" -W
```

4. Если username передается не в параметре `cn`, то необходимо обновить информацию в разделе User Federation → LDAP → Mappers → username, поле LDAP Attribute:

User federation > Settings > Mapper details

username

ID	13409cdd-3bf9-4404-b03a-b11a1ee70fc8
Name *	username
Mapper type *	user-attribute-ldap-mapper
User Model Attribute	username
LDAP Attribute	sAMAccountName
Read Only	<input checked="" type="checkbox"/> On
Always Read Value From LDAP	<input type="checkbox"/> Off
Is Mandatory In LDAP	<input checked="" type="checkbox"/> On
Attribute default value	
Force a Default Value	<input checked="" type="checkbox"/> On

5. В блоке с настройками поиска и обновления LDAP указать следующие значения полей:

- **Edit mode** – **READ_ONLY**;
- **UsersDN** – атрибут **distinguishedName** из Active Directory;
- **Username LDAP attribute** – `cn` или параметр определенный выше. Достаточно часто это параметр `sAMAccountName` .
- **RDN LDAP attribute** – `cn`;
- **UUID LDAP attribute** – `objectGUID`;
- **User object classes** – `person, organizationalPerson, user`;
- **User LDAP filter** – опциональный фильтр, который указывает, из какой группы в Active Directory брать пользователей;
- **Search scope** – **Subtree** для сквозного поиска пользователей согласно фильтру в поле **User LDAP filter**.

6. В блоке с настройками синхронизации указать следующие значения полей:

- **Import users** – On;
- **Sync Registrations** – On;
- **Periodic full sync** – On;
- **Full sync period** – указать период синхронизации в секундах;
- **Periodic changed users sync** – On;
- **Changed users sync period** – указать период синхронизации в секундах.

7. В блоке с настройками Kerberos указать следующие значения полей:

- **Allow Kerberos authentication** – On;
- **Kerberos realm** – заглавными буквами указать наименование домена, настроенного [на шаге 2](#);
- **Server principal** – указать SPN, указанный при создании файла .keytab ([см. шаг 1](#));
- **Key tab** – указать путь до файла .keytab;
- **Debug** – On (опционально).

Kerberos integration

Allow Kerberos authentication On

Kerberos realm *

Server principal *

Key tab *

Debug On

Use Kerberos for password authentication Off

Cache settings

Cache policy

Advanced settings

Enable the LDAPv3 password modify extended operation Off

Save Cancel

8. Нажать на кнопку **Save**.

9. Если в атрибуте **cn** приходит значение, отличное от username почтового адреса (без домена), нужно настроить маппинг поля username на тот атрибут, в котором приходит значение username.

Для этого в только что созданном провайдере - можно найти в User federation → ldap:

- на вкладке Mappers открыть "username"
- в поле "LDAP Attribute" указать название атрибута, в котором приходит username
- нажать на кнопку **Save**.

Далее в настройке из п. 3, в блоке с настройками поиска и обновления LDAP, в поле **Username LDAP attribute** также указать название атрибута, в котором приходит username.

Шаг 4. Регистрация Keycloak в сервисе Stdb

Описание представлено в [разделе](#).

Шаг 5. Настройка внешней аутентификации

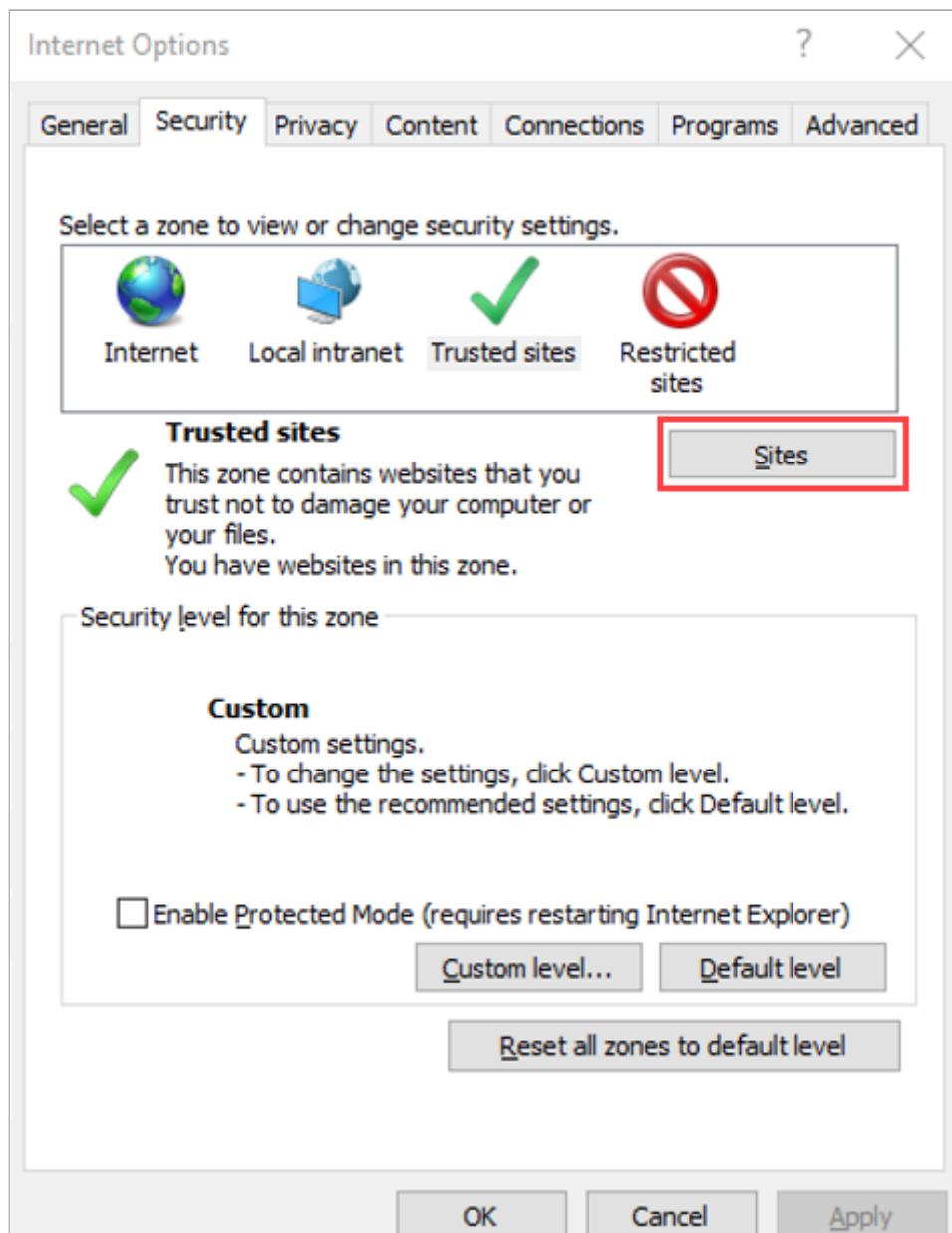
Описание в [разделе](#).

Шаг 6. Настройка браузеров для работы с Kerberos

Edge, Internet Explorer

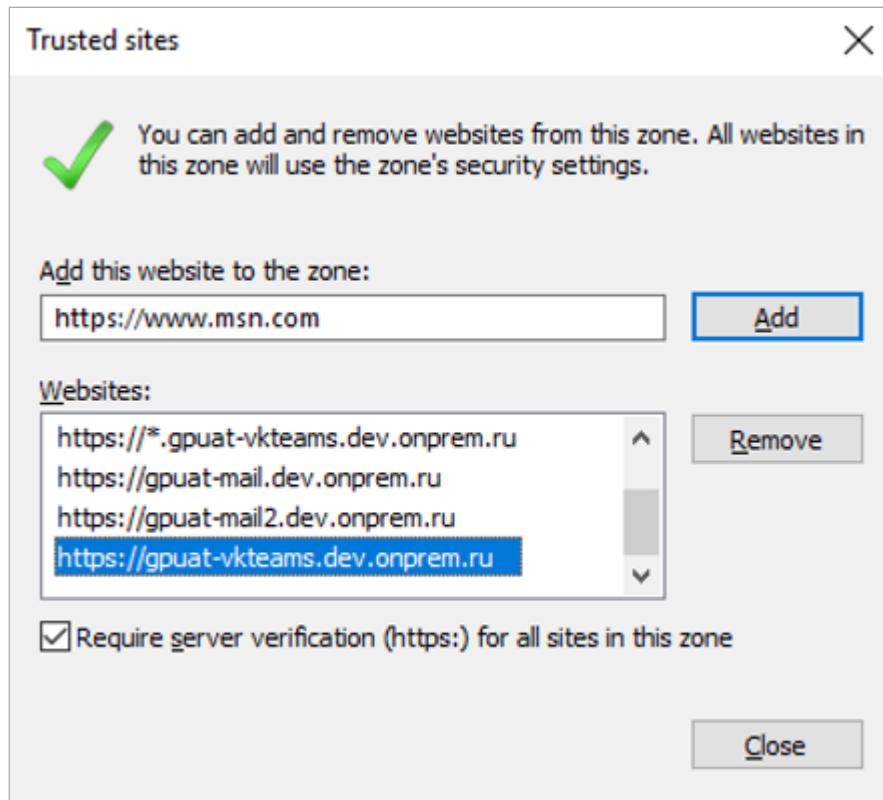
1. Нажать **Win + R**, ввести **inetcpl.cpl** и нажать **OK**.

2. Перейти на вкладку **Security** → нажать **Trusted sites** → нажать на кнопку **Sites**:

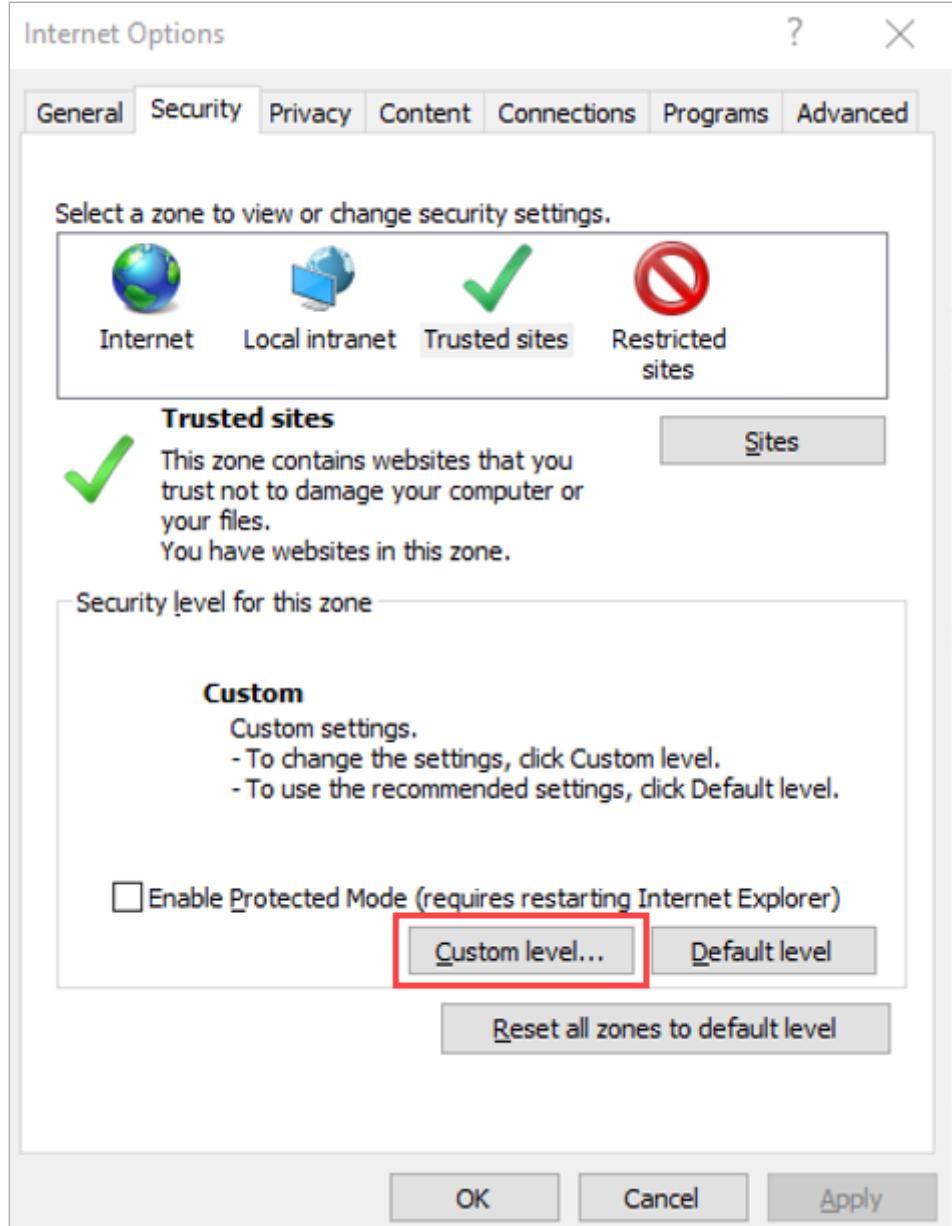


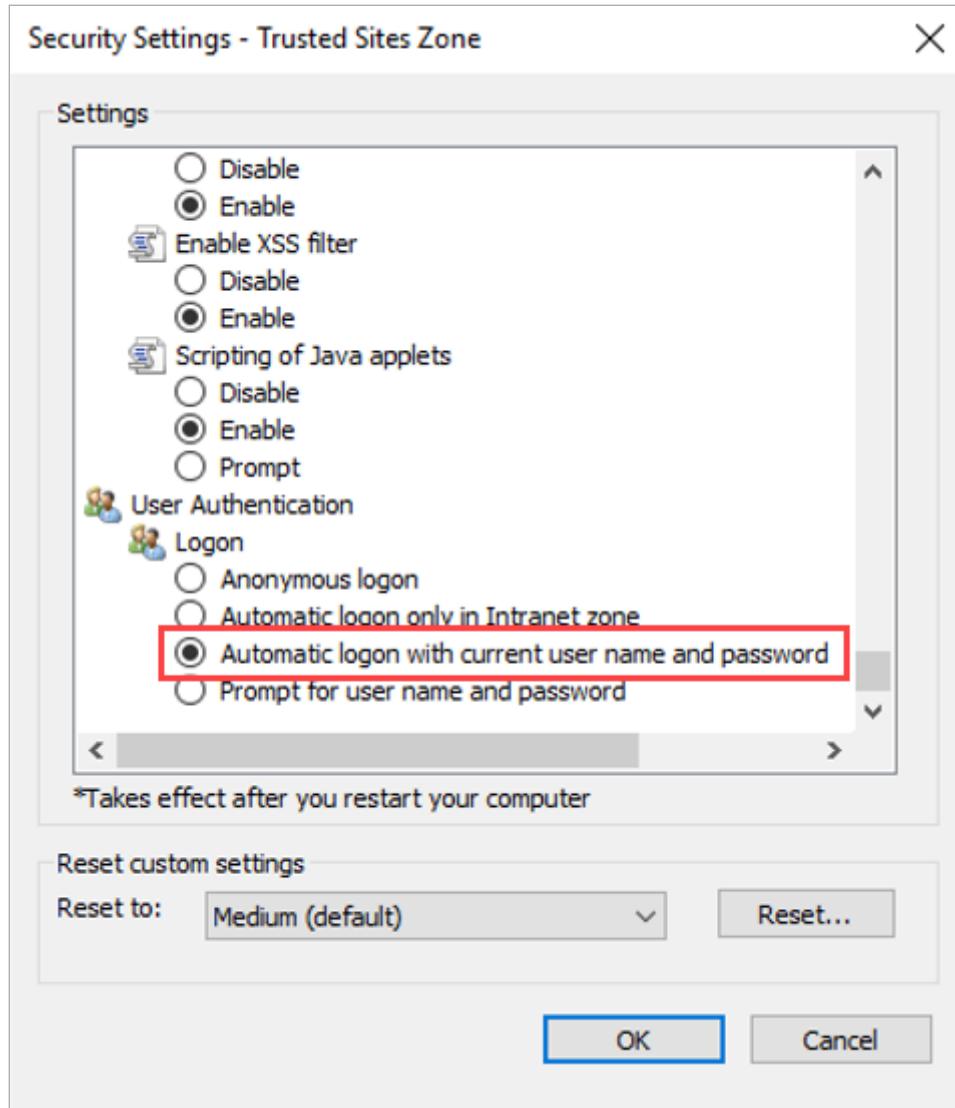
3. Добавить:

- https://<vkteams_domain>
- https://*.<vkteams_domain>



4. Нажать на кнопку **Custom level...** и установить переключатель **Automatic login with current user name and password:**





5. Нажать на кнопку **OK**, чтобы сохранить изменения.

Google chrome

Изменить реестр HKEY_LOCAL_MACHINE/SOFTWARE/Policies/Google/Chrome.

Установить:

- **AuthNegotiateDelegateWhitelist:** *.<VKTeams_DOMAIN>,< VKTeams_DOMAIN >
- **AuthServerWhitelist:** *.<VKTeams_DOMAIN>,< VKTeams_DOMAIN >
- **AuthNegotiateDelegateAllowlist:** *.<VKTeams_DOMAIN>,< VKTeams_DOMAIN >
- **AuthServerAllowlist:** *.<VKTeams_DOMAIN>,< VKTeams_DOMAIN >

Registry Editor

File Edit View Favorites Help

The screenshot shows the Windows Registry Editor with the following tree structure on the left:

- Computer
 - HKEY_CLASSES_ROOT
 - HKEY_CURRENT_USER
 - HKEY_LOCAL_MACHINE
 - BCD00000000
 - HARDWARE
 - SAM
 - SECURITY
 - SOFTWARE
 - Classes
 - Clients
 - Cloudbase Solutions
 - Intel
 - Microsoft
 - ODBC
 - Partner
 - Policies
 - Google
 - Chrome
 - Microsoft
 - RedHat
 - RegisteredApplication
 - WOW6432Node
 - SYSTEM
 - HKEY_USERS
 - HKEY_CURRENT_CONFIG

On the right, a table displays the contents of the Google\Chrome key:

Name	Type	Data
ab (Default)	REG_SZ	(value not set)
ab AuthNegotiateDelegateWhitelist	REG_SZ	*.gpuat-mail2.dev.onprem.ru, gpuat-mail2.dev.on...
ab AuthServerWhitelist	REG_SZ	*.gpuat-mail2.dev.onprem.ru, gpuat-mail2.dev.on...
ab AuthNegotiateDelegateAllowlist	REG_SZ	*
ab AuthServerAllowlist	REG_SZ	*

Распространенные проблемы

Надпись «Server error» в веб-интерфейсе Мессенджер и ВКС, окно логина не открылось

Отключите блокировку всплывающих окон в браузере.

Вместо окна логина отображается «Required parameter not found»

Проверьте, что в сервисе Stdb верно прописано поле **addr** в **idp_configurations**.

После логина появляется ошибка «Unexpected error when authenticating with identity provider»

В логах сервиса Keycloak: «Failed to make identity provider oauth callback: javax.net.ssl.SSLHandshakeException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target».

Проверьте, что у сервиса Keycloak есть все сертификаты.

Ошибка {"status": {"code": 40000, "reason": "Required parameter not found"}}

Появляется при попытке входа по SSO при включении SSO-аутентификации через сервис Keycloak версии 24.9.5.

Проблема связана с эндпоинтом `di.<vkt_domain>/auth/realms/myteam/`. Сервис Front идет по url-адресу и попадает на Nginx (API Gateway), на котором нет этого домена.

Окружение

Версия: 24.9, 24.11.

Операционные системы: Centos, Redos, Redos CE.

Тип инсталляции: 1 виртуальная машина, кластерная инсталляция, DMZ.

Решение

Из файла `/etc/coredns/conf.d/main_domains.hosts` удалите строку `di.{$COREDNS_EXTERNAL_DOMAIN}` и перезапустите CoreDNS командой:

```
systemctl restart coredns
```

В логах Keycloak ошибка: Invalid argument (400) - Cannot find key of appropriate type to decrypt AP-REQ

Проблема может возникнуть из-за того, что Java Keycloak не может прочитать keytab файл:

1. Необходимо исправить **deployments** Keycloak, добавив следующие данные:

```
volumeMounts:
- mountPath: /mnt/keytab-writable
  name: keytab-tmp

volumes:
- emptyDir: {}
  name: keytab-tmp
```

2. Перезапустите под.

3. Переместите keytab в папку `/mnt/keytab-writable`:

```
kubectl cp mcs_new.keytab keycloak-pod:/mnt/keytab-writable/mcs_test.keytab -n keycloak
```

4. Измените путь до keytab в веб-интерфейсе Keycloak.

Внутри пода Keycloak невозможно достучаться до контроллера домена

Проверьте, что из пода доступен контроллер домена. Например:

```
nc -zv dc01.contoso.com 88
```

Если команда завершается ошибкой, то необходимо добавить в deployments Keycloak, в секцию `spec.template.spec` следующие строчки:

```
hostAliases:
- ip: "айпи"
  hostnames:
  - "dc01.contoso.com"
```

Внутри пода Keycloak необходимо настроить krb5.conf

1. Создайте на машине с Keycloak файл krb5.conf. Пример содержимого:

```
[libdefaults]
    default_realm = CONTOSO.COM
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true
    isInitiator=false
    fcc-mit-ticketflags = true
    allow_weak_crypto = true
    default_tkt_enctypes = aes256-cts-hmac-sha1-96
    default_tgs_enctypes = aes256-cts-hmac-sha1-96
    permitted_enctypes = aes256-cts-hmac-sha1-96 aes256-cts-hmac-sha384-192
    camellia256-cts-cmac aes128-cts-hmac-sha1-96 aes128-cts-hmac-sha256-128 camellia128-cts-
    cmac arcfour-hmac
[realms]
    CONTOSO.COM = {
        kdc = dc01.CONTOSO.COM
        admin_server = dc01.CONTOSO.COM
    }
[domain_realm]
    .contoso.com = CONTOSO.COM
    contoso.com = CONTOSO.COM
```

2. Выполните команду, указав путь до файла krb5.conf :

```
kubectl create configmap krb5-conf --from-file=krb5.conf=<путь до файла>/krb5.conf -n
keycloak
```

3. Обновите **deployments**:

```
kubectl -n keycloak describe deployments
```

И вставьте:

```
volumeMounts:
- mountPath: /etc/krb5.conf
name: krb5
subPath: krb5.conf

volumes:
- configMap:
defaultMode: 420
name: krb5-conf
name: krb5
```

👤 Технический писатель: Белова Ирина

⌚ 3 декабря 2025 г.