

Настройка SSO- аутентификации для Почты

Пошаговая инструкция

Назначение документа	3
Предварительные условия	3
Настройки на сервере Active Directory	3
Сгенерируйте keytab-файлы	4
Настройка интеграции с Active Directory	5
Проверка настроек домена	7
Настройка установщика	8
Для работы с Keycloak	8
Для работы без Keycloak	9
Настройки интеграции с Keycloak	11
Шаг 1. Создайте и настройте REALM	11
Шаг 2. Добавьте Client API	13
Шаг 3. Настройте интеграцию с LDAP	14
Шаг 4. Настройте интеграцию с Kerberos при работе с Keycloak	16
Шаг 5. Добавьте в контейнер Keycloak файла .keytab	17
Шаг 6. Настройте параметры интеграции с Keycloak в установщике	17

Назначение документа

В документе описан порядок действий для настройки SSO как с использованием сервиса Keycloak, так и без него. По завершении интеграции пользователи получают возможность проходить SSO-аутентификацию внутри Почты VK WorkSpace.

SSO (Single Sign-On) — технология, позволяющая проходить при авторизации процесс аутентификации один раз и автоматически получать доступ к нескольким системам без повторного ввода учетных данных.

Предварительные условия

Чтобы начать настройку, вам потребуется:

- Доступ на сервер Почты и в административную панель VK WorkSpace;
- Доступ к Active Directory;
- Пользователь Active Directory с правами администратора;
- Доступ в Keycloak (для интеграций с внешним сервером);
- Навыки системного администрирования (Linux, Windows).

Настройки на сервере Active Directory

На контролере домена необходимо зарегистрировать учетную запись.

В разделе **Account** ввести в поле **User logon name** следующее:

- Для интеграции с Keycloak — `HTTP/<почтовый домен>` ;
- Для интеграции без Keycloak — `HTTP/auth.<почтовый домен>` .

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

1. User cannot change password;
2. Password never expires;
3. This account supports Kerberos AES 128 bit encryption;
4. This account supports Kerberos AES 256 bit encryption;
5. Do not require Kerberos preauthentication.

Затем в разделе управления групповыми политиками перейдите к настройке политики **Configure encryption types allowed for Kerberos** (настройка актуальна как для работы с Keycloak, так и без него).

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

- RC4_HMAC_MD5,
- AES128_HMAC_SHA1,
- AES256_HMAC_SHA1.

Сгенерируйте keytab-файлы

Команды, которые представлены ниже, необходимо выполнять на сервере **Active Directory**.

Пример команды, чтобы создать keytab для WEB (интеграция **с Keycloak**):

```
ktpass -princ HTTP/infra-01.dev.onprem.ru@AD2013.ON-PREMISE.RU -mapuser AD2013\kuser3 -out C:\tmp\keycloak.keytab -mapOp set -crypto ALL -setupn -setpass -ptype KRB5_NT_PRINCIPAL /pass strongSecret
```

Сохраните созданный keytab-файл для HTTP на **почтовом сервере**.

Пример команд, чтобы создать keytab для WEB (интеграция **без Keycloak**):

```
ktpass -princ HTTP/auth.infra-01.dev.onprem.ru@AD2013.ON-PREMISE.RU -mapuser "<username>@ad2013.on-premise.ru" -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass "<userpass>" +dumpsalt -out C:\Users\Admin\Documents\keytabs_sso\http.keytab

ktpass -princ "HTTP/infra-01.dev.onprem.ru@AD2013.ON-PREMISE.RU" -mapuser "<username>@ad2013.on-premise.ru" -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass "<userpass>" -in C:\Users\Admin\Documents\keytabs_sso\http.keytab -out C:\Users\Admin\Documents\keytabs_sso\httpq.keytab -setupn -setpass -rawsalt "<Hashing password with salt из вывода прошлой команды>"
```

Параметры команды `ktpass`:

- `princ` — имя SPN в Keycloak для идентификации в среде Kerberos.
Имя состоит из: транспортного протокола (для HTTP в верхнем регистре); имени хоста сервера Keycloak (или адреса почтового сервера для интеграций внутри инсталляции); Kerberos Realm (для HTTP в верхнем регистре).
- `mapuser` — имя созданной в домене учетной записи для сервера Keycloak (DOMAIN\username).
- `mapOp` — если задано значение `add`, то новый SPN будет добавлен к существующим. Если задано значение `set`, то SPN будет перезаписан.
- `out` — задает путь к генерируемому keytab-файлу. Например, C:\temp\spnego_spn.keytab.
- `/pass` — значение пароля от учетной записи для сервера Keycloak в домене.
- параметры `crypto` и `ptype` задают ограничения на используемые алгоритмы и тип генерируемой Kerberos-службы. Рекомендуется задать параметры, как в указанном примере: `-crypto ALL -ptype KRB5_NT_PRINCIPAL`.
- параметр `-setupn` необходим для того, чтобы UPN не менялся.

Внимание

Отдельно сохраните значение SPN (Service Principal Name) из команды выше, оно потребуется вам позднее.

Чтобы сгенерировать keytab-файлы для SMTP и IMAP, используйте следующие команды (актуальны как для работы с Keycloak, так и без него):

```
dsquery * -filter sAMAccountName=kcuser3 -attr msDS-KeyVersionNumber

# В следующих командах /kvno <N> – результат выполнения первой команды
ktpass -princ smtp/infra-01.dev.onprem.ru@AD2013.ON-PREMISE.RU -mapuser AD2013\kcuser3 -out C:\tmp\infra_smtp.keytab -mapOp add -crypto ALL -setupn -setpass -ptype KRB5_NT_PRINCIPAL /kvno <N> /pass strongSecret
ktpass -princ imap/infra-01.dev.onprem.ru@AD2013.ON-PREMISE.RU -mapuser AD2013\kcuser3 -out C:\tmp\infra_imap.keytab -mapOp add -crypto ALL -setupn -setpass -ptype KRB5_NT_PRINCIPAL /kvno <N> /pass strongSecret
```

Два файла .keytab для IMAP и SMTP нужно также **сохранить на сервере Почты**. В дальнейшем их нужно будет добавить в установщик.

Настройка интеграции с Active Directory

1. Авторизуйтесь в Admin Panel сервиса Почта под учетной записью администратора.
2. Выберите адрес сервера, для которого нужно настроить интеграцию с Keycloak. У выбранного домена должна быть настроена **MX-запись**.
3. Перейдите в раздел **Конфигурация** → **Настройки** панели администратора.
4. Чтобы начать настройку, уберите чекбокс **Не использовать AD**.

5. Введите в поле **Адрес AD** адрес вашего каталога Active Directory.

6. **Каталоги пользователей** — введите значение поля **distinguishedName** из списка атрибутов каталога. Например, `OU=demoapp.DC=presale.DC=local`.

Если вам нужно указать больше одного каталога пользователей, обратитесь к представителю VK.

7. Введите в поле **Логин администратора** логин администратора Active Directory.

8. Вставьте в поле **Пароль администратора** пароль администратора Active Directory.

9. Если вы используете свойство **Отчество**, введите его значение в **Поле свойства «Отчество»**.

10. **Использовать шифрованное соединение (LDAPS)** — есть возможность добавления сертификата LDAPS с помощью кнопки **Добавить сертификат**.

11. Отметьте чекбокс **Игнорировать ошибки сертификата**, если у вас самоподписанный SSL-сертификат.

Сбрасывать сессии пользователей при изменении пароля — если чекбокс отмечен, при изменении пароля пользователя в Active Directory будет сбрасываться сессия в Почте.

Использовать в качестве логина email вместо username — в текущей версии поле не используется.

12. Нажмите на кнопку **Сохранить**, чтобы применить настройки.

Если пользователи не появились в Почте, нужно проверить корректность настроек синхронизации с Active Directory с помощью консольной команды:

```
sudo journalctl -fu onpremise-container-adloader1.service
```

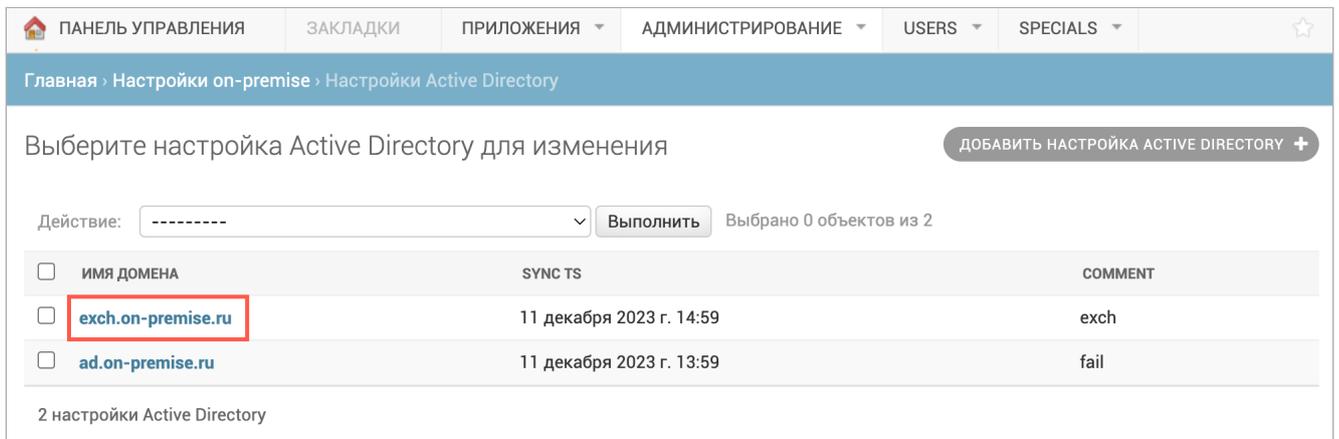
Проверка настроек домена

Если вы не планируете использовать Keycloak, перейдите к [настройке Deployer](#).

Далее необходимо проверить файл настроек домена, для которого будет настраиваться интеграция с Keycloak.

1. Перейдите по URL административной панели

https://biz.<domain_name>/admin/misc/configurations/adloaderclient/ и кликните по адресу домена.



ПАНЕЛЬ УПРАВЛЕНИЯ ЗАКЛАДКИ ПРИЛОЖЕНИЯ АДМИНИСТРИРОВАНИЕ USERS SPECIALS

Главная > Настройки on-premise > Настройки Active Directory

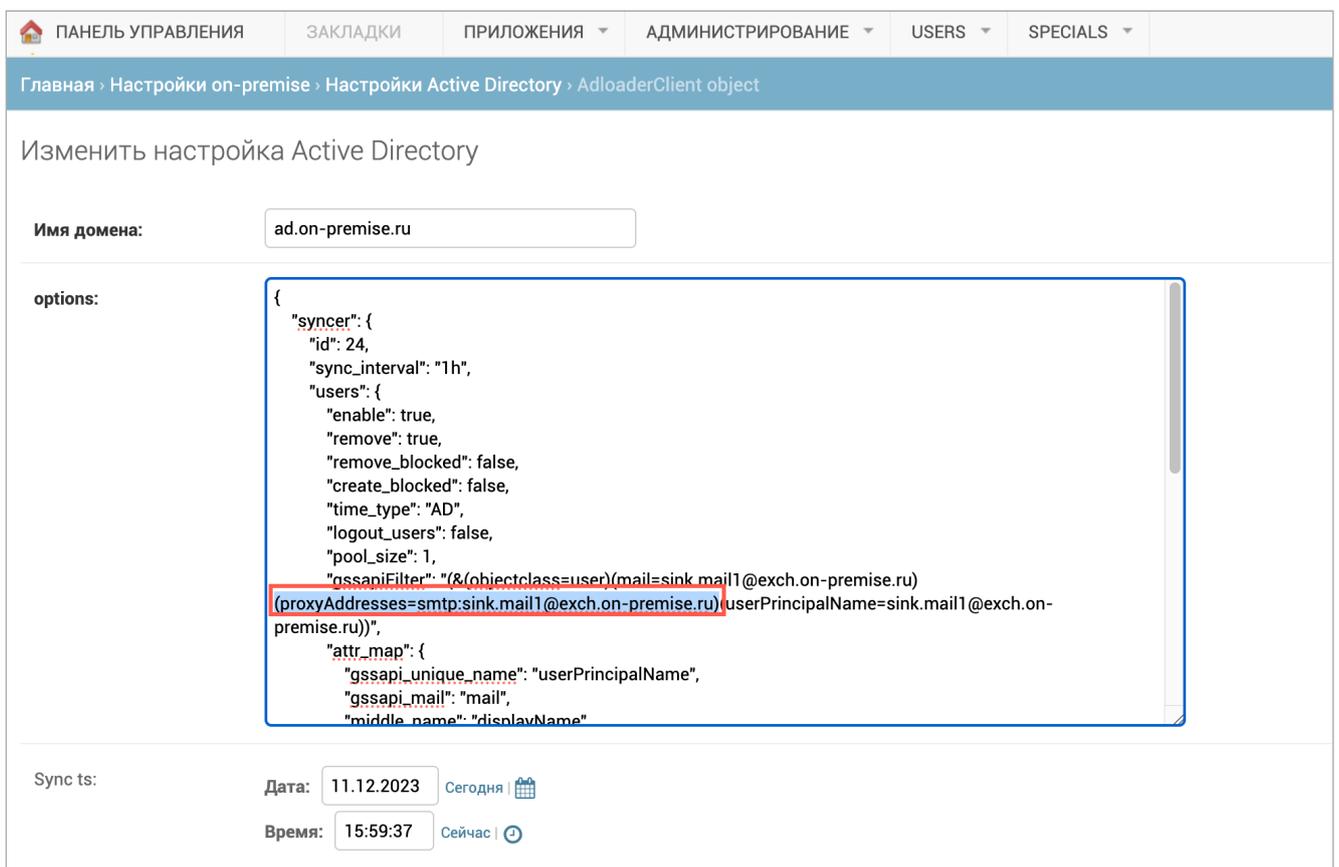
Выберите настройка Active Directory для изменения ДОБАВИТЬ НАСТРОЙКА ACTIVE DIRECTORY +

Действие: ----- ▾ Выполнить Выбрано 0 объектов из 2

<input type="checkbox"/>	ИМЯ ДОМЕНА	SYNC TS	COMMENT
<input type="checkbox"/>	exch.on-premise.ru	11 декабря 2023 г. 14:59	exch
<input type="checkbox"/>	ad.on-premise.ru	11 декабря 2023 г. 13:59	fail

2 настройки Active Directory

2. Убедитесь, что в разделе **options** отсутствует значение `proxyAddresses`.



ПАНЕЛЬ УПРАВЛЕНИЯ ЗАКЛАДКИ ПРИЛОЖЕНИЯ АДМИНИСТРИРОВАНИЕ USERS SPECIALS

Главная > Настройки on-premise > Настройки Active Directory > AdloaderClient object

Изменить настройка Active Directory

Имя домена:

options:

```
{
  "syncer": {
    "id": 24,
    "sync_interval": "1h",
    "users": {
      "enable": true,
      "remove": true,
      "remove_blocked": false,
      "create_blocked": false,
      "time_type": "AD",
      "logout_users": false,
      "pool_size": 1,
      "gssapiFilter": "(&(objectclass=user)(mail=sink.mail1@exch.on-premise.ru)
(proxyAddresses=smtp:sink.mail1@exch.on-premise.ru)userPrincipalName=sink.mail1@exch.on-premise.ru)",
      "attr_map": {
        "gssapi_unique_name": "userPrincipalName",
        "gssapi_mail": "mail",
        "middle_name": "displayName"
      }
    }
  }
}
```

Sync ts: Дата: Сегодня | 📅
 Время: Сейчас | 🕒

3. Если значение `proxyAddresses` присутствует, необходимо удалить его, включая скобки:
(`proxyAddresses=smtp:sink.mail1@exch.on-premise.ru`).
4. Сохраните изменения.

Настройка установщика

Для перехода в веб-интерфейс в адресной строке браузера необходимо указать адрес: `http://server-ip-address:8888`. Нажмите на значок  и перейдите в раздел **Продукты**.

Для работы с Keycloak

1. Включите опции **Интеграция с Kerberos (SSO-авторизация)** и **Keycloak внутри инсталляции**.

Интеграция с другими инсталляциями VK WorkMail Deprecated	<input checked="" type="checkbox"/>
Интеграция с Kerberos (SSO-авторизация)	<input checked="" type="checkbox"/>
Keycloak внутри инсталляции v17.0.1 1 GB RAM, 1 vCPU	<input checked="" type="checkbox"/>
Интеграция с внешним Keycloak сервером	<input type="checkbox"/>
Средства резервного копирования почтовых ящиков	<input checked="" type="checkbox"/>

Если вы планируете использовать внешний сервис Keycloak, нужно включить опцию **Интеграция с внешним Keycloak сервером**.

2. Сохраните изменения и вернитесь к списку ролей, чтобы сгенерировать дополнительные контейнеры.

filin1 (172.20.5.117) hypervisor1 ⓘ	1
s3f1 (172.20.5.113) hypervisor1 ⓘ	4
pub1 (100.70.81.216) hypervisor1 ⓘ	2 1
pub-imap1 (100.70.81.216) hypervisor1 ⓘ	1
pub-mx1 (100.70.81.216) hypervisor1 ⓘ	1
pub-smtp1 (100.70.81.216) hypervisor1 ⓘ	1

Добавить ▾
Сгенерировать автоматически

3. В настройках перейдите в раздел **Интеграции** → **Интеграция с Kerberos (SSO-авторизация)**.

4. Введите **заглавными буквами** адрес сервера Active Directory, который будет использоваться в интеграции, в поле **Название REALM`а в Keycloak**.

В поле можно также ввести любое ключевое название, например KEYCLOAKREALM. Позже это значение будет использоваться при настройках в интерфейсе Keycloak. REALM в установщике не должен совпадать с Kerberos REALM, у них разное назначение.

5. Сохраните изменения.

6. Если установщик выдаст ошибку, попробуйте сохранить еще раз.

7. Прежде чем перейти в интерфейс Keycloak, на сервере с дистрибутивом Почты выполните команду:

```
grep KEYC /opt/mail0nPremise/dockerVolumes/keycloak1/keycloak.env
```

Для работы без Keycloak

1. Включите опции **Интеграция с Kerberos (SSO-авторизация)**.

Интеграция с другими инсталляциями VK WorkMail Deprecated	<input checked="" type="checkbox"/>
Интеграция с Kerberos (SSO-авторизация)	<input checked="" type="checkbox"/>
Keusloak внутри инсталляции v17.0.1 1 GB RAM, 1 vCPU	<input type="checkbox"/>
Интеграция с внешним Keusloak сервером	<input type="checkbox"/>
Средства резервного копирования почтовых ящиков	<input checked="" type="checkbox"/>

2. Сохраните изменения и вернитесь к списку ролей, чтобы сгенерировать дополнительные контейнеры.

filin1 (172.20.5.117) hypervisor1 ⓘ	1
s3f1 (172.20.5.113) hypervisor1 ⓘ	4
pub1 (100.70.81.216) hypervisor1 ⓘ	2 1
pub-imap1 (100.70.81.216) hypervisor1 ⓘ	1
pub-mx1 (100.70.81.216) hypervisor1 ⓘ	1
pub-smtp1 (100.70.81.216) hypervisor1 ⓘ	1
Добавить ▾ Сгенерировать автоматически	

3. Затем в Настройках перейдите в раздел **Интеграции** → **Интеграция с Kerberos (SSO-авторизация)**.

4. Заполните поля:

- **Адрес системы аутентификации Kerberos** — адрес сервера, на котором установлен AD/Kerberos и порт 88.
- **Адрес сервера Kerberos-adm (Kerberos administration)** — адрес сервера, на котором установлена административная панель Kerberos и порт 749.
- **Имя REALM в Kerberos** — заглавными буквами введите имя REALM (чаще всего оно совпадает с адресом сервера AD/Kerberos).
- **Адрес сервера SPN (Service Principal Name)**.

5. Добавьте keytab-файлы в соответствующие поля и сохраните изменения.

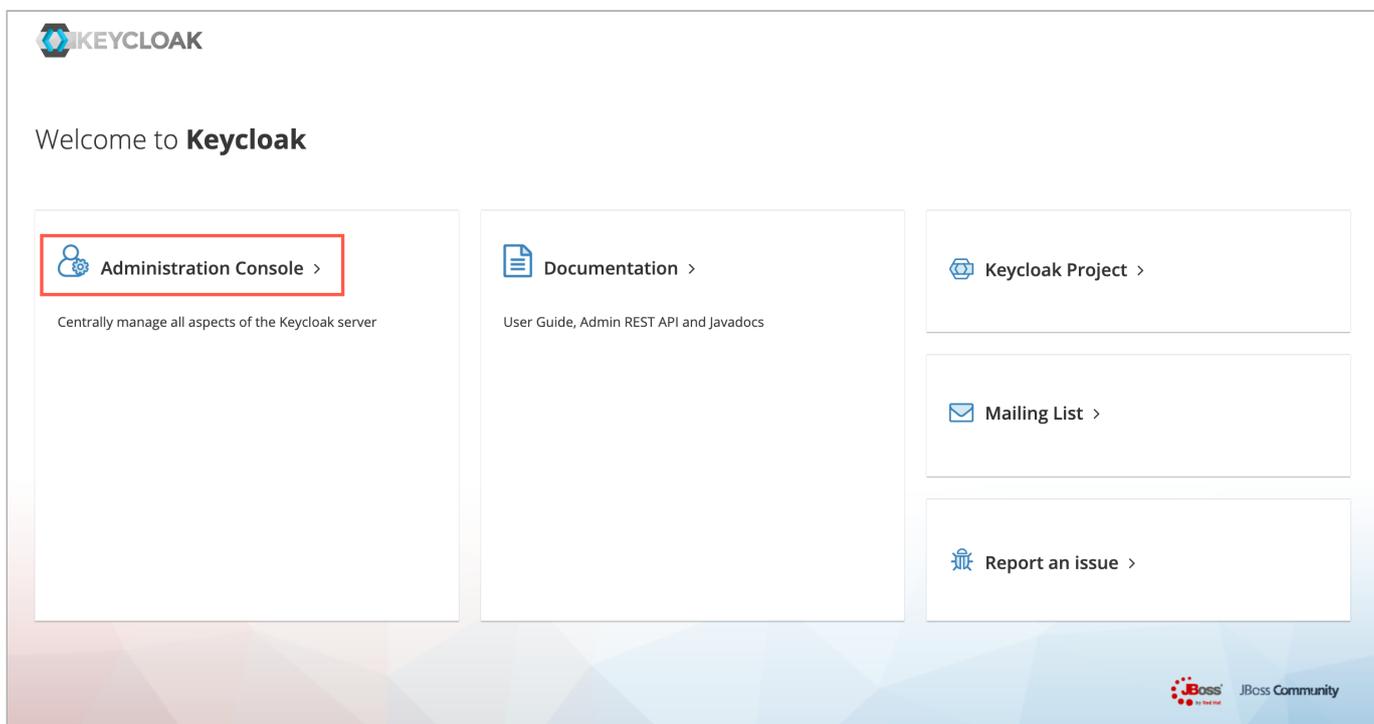
6. Чтобы применить новую конфигурацию перейдите к списку ролей и повторите соответствующие шаги или запустите автоматическую установку.

На этом интеграцию с Kerberos **без Keycloak** можно считать завершённой.

Настройки интеграции с Keycloak

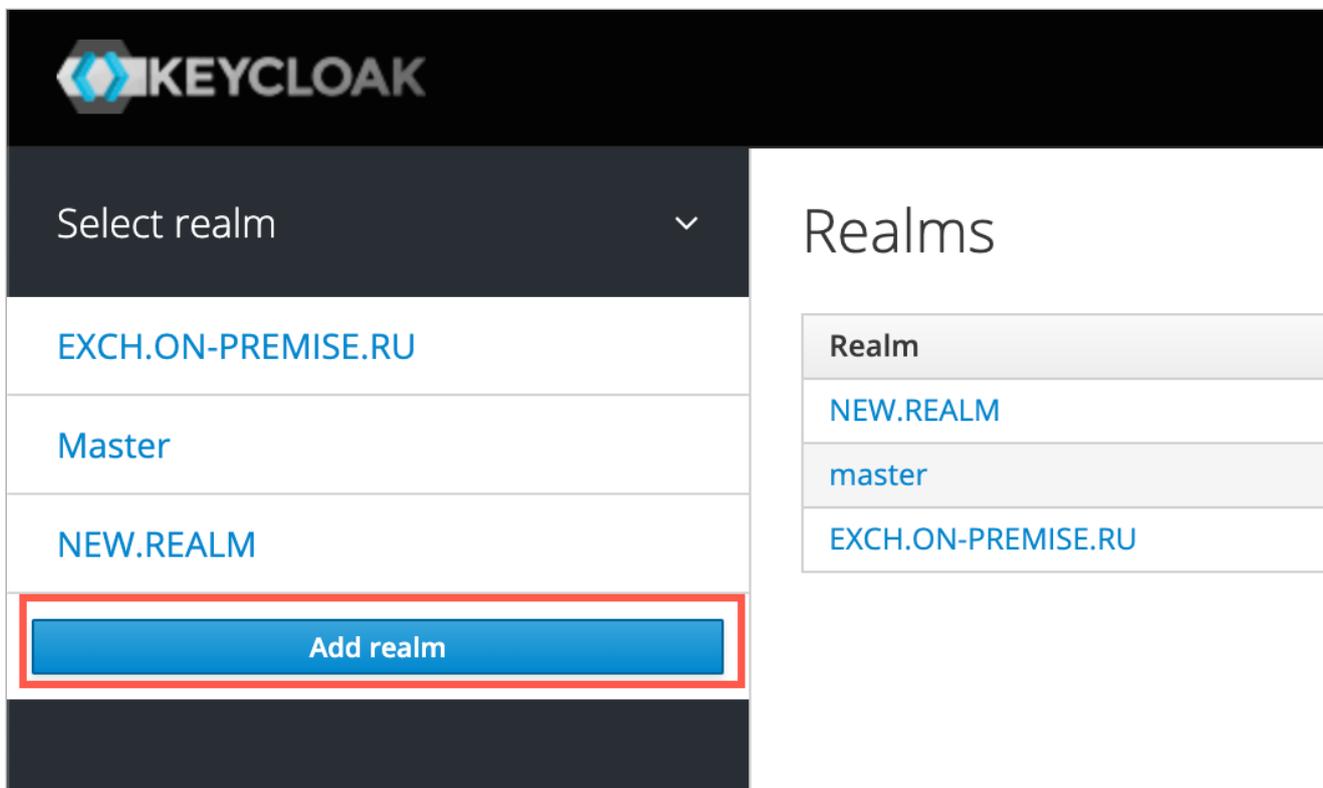
Для перехода в Keycloak в строке браузера введите адрес: `https://biz.<mail_domain>/auth`.

Если вы используете внешний сервер Keycloak, перейдите в его панель администрирования.

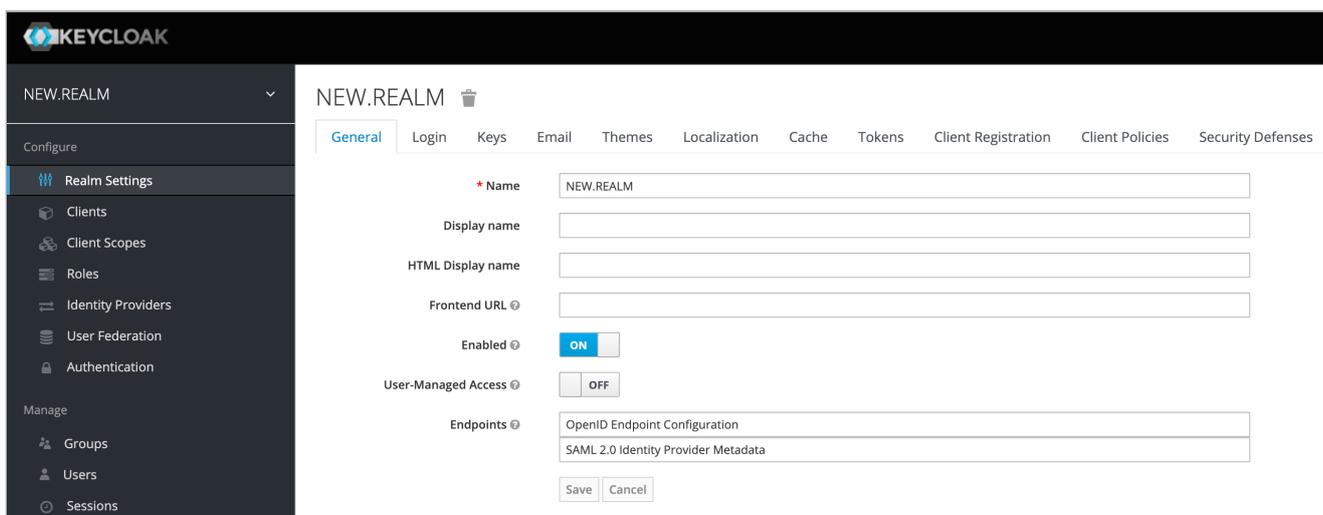


Шаг 1. Создайте и настройте REALM

1. В выпадающем меню нажмите на кнопку **Add realm**.



2. В поле **Name** введите имя REALM, аналогичное указанному в интерфейсе установщика.
3. Нажмите на кнопку **Create** — откроется окно настроек, раздел **General**.



4. В поле **Frontend URL** добавьте URL вида: `http://biz.<mail_domain>:80/auth`.

Примечание

При использовании внешнего сервера Keycloak нужна дополнительная настройка на `/auth` с помощью параметра `http-relative-path=/auth`.

5. Сохраните изменения.
6. Во вкладке **Login** у параметра **Require SSL** необходимо выбрать значение **none**.
7. Сохраните настройки.
8. Перейдите во вкладку **Keys** → **Providers** и удалите неподдерживаемые провайдеры (`aes-generated` и `rsa-enc-generated`).

NEW.REALM 

General Login **Keys** Email Themes Localization Cache Tokens Client Registration Client Policies Security Defenses

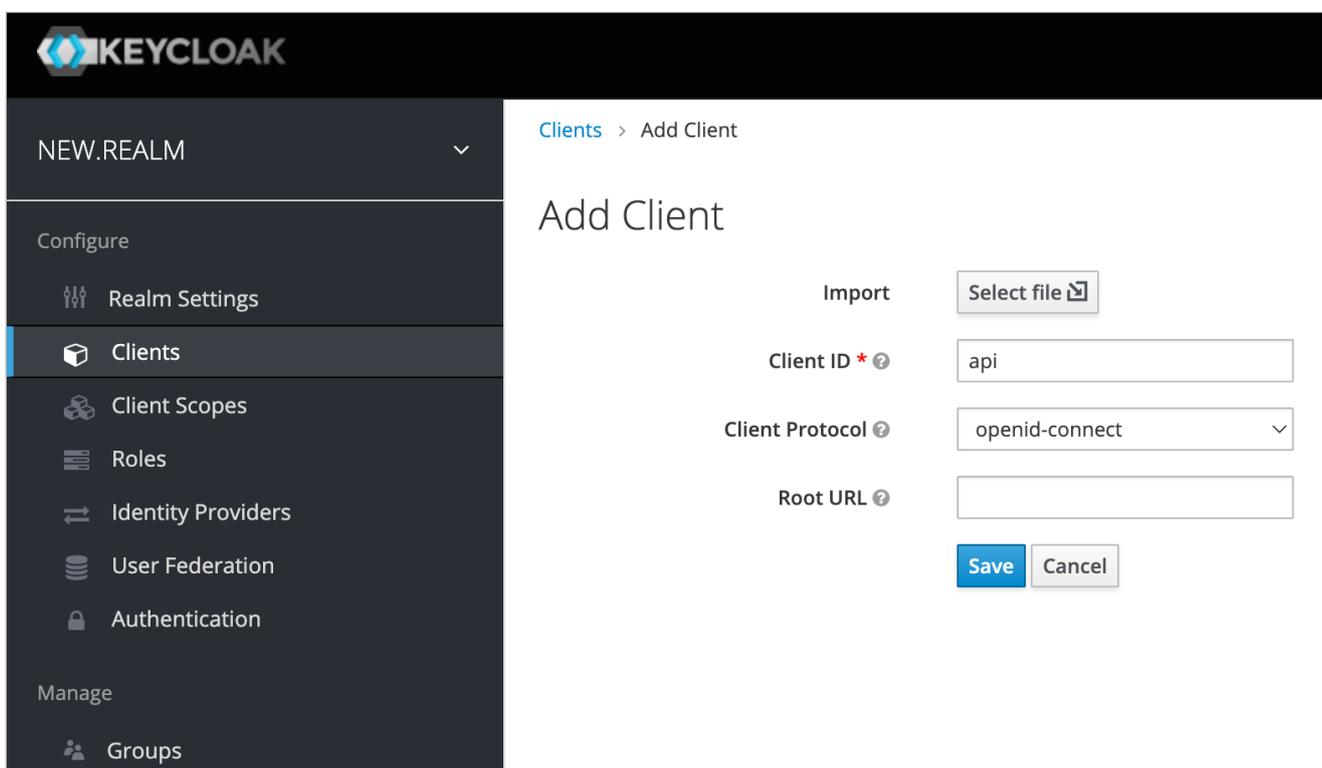
Active Passive Disabled **Providers**

Search...

Name	Provider	Provider description	Priority	Actions
aes-generated	aes-generated	Generates AES secret key	100	Edit Delete
rsa-enc-generated	rsa-enc-generated	Generates RSA keys for key encryption and creates a self-signed certificate	100	Edit Delete
hmac-generated	hmac-generated	Generates HMAC secret key	100	Edit Delete
rsa-generated	rsa-generated	Generates RSA signature keys and creates a self-signed certificate	100	Edit Delete

Шаг 2. Добавьте Client API

1. В разделе **Clients** создайте нового клиента. Для этого в поле **Client ID** введите значение **api** и нажмите на кнопку **Save**.



The screenshot shows the Keycloak administration interface for adding a new client. The left sidebar shows the navigation menu with 'Clients' selected. The main content area is titled 'Add Client' and contains the following fields:

- Import:** A 'Select file' button.
- Client ID ***: A text input field containing the value 'api'.
- Client Protocol**: A dropdown menu set to 'openid-connect'.
- Root URL**: An empty text input field.
- Buttons:** 'Save' and 'Cancel' buttons.

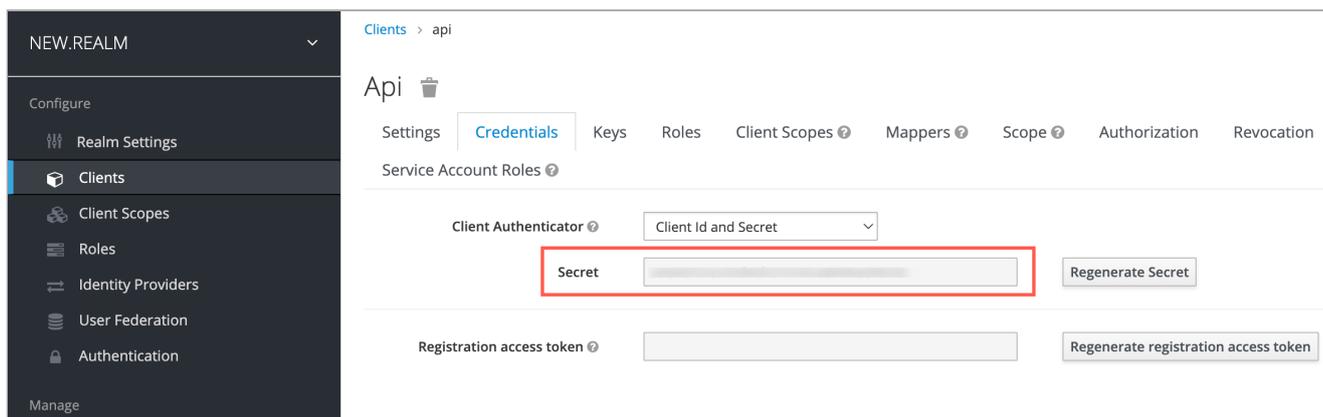
2. Вкладку Settings нужно настроить следующим образом:

Внимание

Поля, настройки которых не будут изменяться, следует оставить заполненными по умолчанию.

- **Access Type** — confidential (после изменения типа доступа появятся дополнительные настройки);
- **Service Accounts Enabled** — ON;
- **Authorization Enabled** — ON;
- **Valid Redirect URIs** — * (необходимо ввести в поле символ *);

3. Сохраните изменения.
4. Перейдите во вкладку **Credentials**.
5. Скопируйте или сохраните значение поля **Secret**.



Шаг 3. Настройте интеграцию с LDAP

1. Перейдите в раздел **User Federation** и в выпадающем меню Add provider выберите **ldap**.
2. Внесите данные в соответствии с настройками LDAP в вашем каталоге Active Directory.

Обратите внимание:

- В строке **Username LDAP attribute** необходимо указать название поля в Active Directory, в котором содержатся юзернеймы пользователей.
- В поле **Bind DN** нужно добавить точное местоположение пользователя для синхронизации в каталоге AD.

Settings Mappers

Required Settings

Provider ID	7bd58fef-270b-4acf-88ed-23468ad18d8b
Enabled	<input checked="" type="checkbox"/>
Console Display Name	ldap
Priority	0
Import Users	<input checked="" type="checkbox"/>
* Edit Mode	READ_ONLY
Sync Registrations	<input type="checkbox"/>
* Vendor	Active Directory
* Username LDAP attribute	sAMAccountName
* RDN LDAP attribute	cn
* UUID LDAP attribute	objectGUID
* User Object Classes	person, organizationalPerson, user
* Connection URL	ldap://10.10.70.18
* Users DN	OU=exch,DC=ad,DC=on-premise,DC=ru
Custom User LDAP Filter	LDAP Filter
Search Scope	Subtree
* Bind Type	simple
* Bind DN	CN=Administrator,CN=Users,DC=ad,DC=on-premise,DC=ru
* Bind Credential

[Test connection](#)

[Test authentication](#)

3. Проверьте соединение с помощью кнопок **Test connection** и **Bind Credential**.

Settings Mappers

Required Settings

Provider ID	<input type="text" value="7bd58fef-270b-4acf-88ed-23468ad18d8b"/>
Enabled ?	<input checked="" type="checkbox"/> ON
Console Display Name ?	<input type="text" value="ldap"/>
Priority ?	<input type="text" value="0"/>
Import Users ?	<input checked="" type="checkbox"/> ON
* Edit Mode ?	<input type="text" value="READ_ONLY"/>
Sync Registrations ?	<input type="checkbox"/> OFF
* Vendor ?	<input type="text" value="Active Directory"/>
* Username LDAP attribute ?	<input type="text" value="sAMAccountName"/>
* RDN LDAP attribute ?	<input type="text" value="cn"/>
* UUID LDAP attribute ?	<input type="text" value="objectGUID"/>
* User Object Classes ?	<input type="text" value="person, organizationalPerson, user"/>
* Connection URL ?	<input type="text" value="ldap://10.10.70.18"/>
* Users DN ?	<input type="text" value="OU=exch,DC=ad,DC=on-premise,DC=ru"/>
Custom User LDAP Filter ?	<input type="text" value="LDAP Filter"/>
Search Scope ?	<input type="text" value="Subtree"/>
* Bind Type ?	<input type="text" value="simple"/>
* Bind DN ?	<input type="text" value="CN=Administrator,CN=Users,DC=ad,DC=on-premise,DC=ru"/>
* Bind Credential ?	<input type="password" value="....."/>

Шаг 4. Настройте интеграцию с Kerberos при работе с Keycloak

1. Раскройте вкладку **Kerberos Integration** и внесите данные для интеграции.

▼ Kerberos Integration

Allow Kerberos authentication  ON

* Kerberos Realm  EXCH.ON-PREMISE.RU

* Server Principal  HTTP/vkwm1.on-premise.ru@AD.ON-PREMISE.RU

* KeyTab  /opt/vkwm1.keytab

Debug  ON

Use Kerberos For Password Authentication  OFF

2. Заполните поля:

- **Kerberos Realm** — введите имя REALM из Kerberos.
- **Server Principal** — укажите ранее созданный SPN Например, HTTP/biz.infra-01.dev.onprem.ru@AD2013.ON-PREMISE.ru .
- **KeyTab** — добавьте в путь до [keytab-файла](#) для HTTP.

Менять положение флагов не нужно.

3. Сохраните изменения.

Шаг 5. Добавьте в контейнер Keycloak файла .keytab

Выполните следующую команду на сервере Почты:

```
cp keycloak.keytab /opt/mail0nPremise/dockerVolumes/keycloak1/keytabs/
```

Шаг 6. Настройте параметры интеграции с Keycloak в установщике

1. В настройках установщика Почты необходимо перейдите в раздел **Интеграции** → **Интеграция с keycloak для SSO авторизации**.

Настройки

Сети Доменные имена Хранилища Шардирование и репликация БД **Настройки компонентов** Интеграции Переменные окружения

Настройки интеграции с Keycloak Отмена Сохранить

Интеграция с VK Teams	Боты для VK Teams	Название REALM в Keycloak:	EXCH.ON-PREMISE.RU
Интеграция с антивирусом по протоколу ICAP	Лицензия редактора R7 Офис	ID oauth клиента в Keycloak:	api
Сборщик почты	Интеграция с другими инсталляциями VK WorkMail <small>Deprecated</small>	Secret oauth клиента в Keycloak:	*****
Интеграция с keycloak для SSO авторизации	Миграция календарей по протоколу EWS	Адрес системы аутентификации Kerberos:	ad.on-premise.ru:88
		Адрес сервера Kerberos-adm (Kerberos administration):	ad.on-premise.ru:749
		Keytab файл для IMAP:	Файл уже загружен Выбрать файл
		Keytab файл для SMTP:	Файл уже загружен Выбрать файл

- В поле **Secret oauth клиента в Keycloak** введите код из раздела **Clients** → **Credentials** в Keycloak, который вы сохранили ранее.
- Добавьте адреса сервисов Kerberos (с портами) и [keytab-файлов](#) для IMAP и SMTP.
- Сохраните изменения.
- Чтобы применить изменения перейдите к списку ролей и запустите автоматическую установку.
- Чтобы в интерфейсе пользователей начала отображаться кнопка **Войти через SSO**, выполните в контейнере **mailapi1** шаг **up_container**.

mailapi1 (172.20.5.40) [mail-vkwm1](#) ⓘ

2 ⚙️ ✖️ ▼

Выполните шаги по настройке машины

Загрузить бэкап [Выберите файл бэкапа](#)

ВНИМАНИЕ! Процесс восстановления из бэкапа будет запущен сразу после загрузки файла!

prepare_configure done

Подготовить файлы конфигурации для сервиса внутри контейнера [Запустить](#) ▼

up_container done

Подготовить файлы конфигурации, статические данные, запустить контейнер [Запустить](#) ▼

- Проверьте успешность интеграции, войдя в систему через SSO под учетной записью пользователя.