

# Интеграция с Keycloak для SSO авторизации

Пошаговая инструкция



Описание документа	3
Предварительные условия	3
Настройки на сервере Active Directory	3
Генерация keytab-файлов	4
Настройка интеграции с Active Directory	5
Проверка настроек домена	6
Предварительная настройка Deployer	7
Настройки в интерфейсе Keycloak	9
Создание и настройка REALM	10
Добавление Client API	11
Настройка интеграции с LDAP	12
Настройка интеграции с Kerberos	13
Добавление в контейнер Keycloak файла .keytab	14
Настройка параметров интеграции для SSO в Deployer	14

## Информация

**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.



# Описание документа

---

В документе описан порядок действий для настройки интеграции VK WorkMail с сервисом Keycloak, размещенном как на внешнем сервере, так и внутри инсталляции VK WorkMail. По завершении интеграции пользователи получают возможность проходить SSO-аутентификацию внутри VK Workspace.

## Предварительные условия

---

Чтобы начать настройку, вам потребуется:

- Доступ на сервер VK WorkMail 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 для сервера Keycloak.

В разделе настроек пользователя (**Account** → **Account options**) отметьте чекбосы:

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.

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.



### Важно

Для использования алгоритма **AES-256** также нужно включить для пользователей параметры:  
This account supports Kerberos AES 256 bit и Do not require Kerberos preauthentication.

## Генерация keytab-файлов

### Примечание

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

Необходимо создать Service Principal Name (SPN) для идентификации сервера Keycloak сервером Kerberos. Пример команды для создания SPN:

```
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
```

Параметры команды ktpass :

- `princ` — имя SPN в Keycloak для идентификации в среде Kerberos.  
Имя состоит из: транспортного протокола **в верхнем регистре** (HTTP/); имени хоста сервера Keycloak (или адреса почтового сервера для интеграций внутри инсталляции); Kerberos Realm **в верхнем регистре** (@DOMAIN.LOC).
- `mapuser` — имя созданной в домене учетной записи для сервера Keycloak (DOMAIN\username).
- `mapOp` — если задан в 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.

Сохраните созданный keytab-файл для HTTP на сервере **Keycloak**. Путь к этому файлу нужно будет указать при настройках в разделе **Настройка интеграции с Kerberos**.

Для генерации keytab-файлов для работы с SMTP и IMAP используются следующие команды:

```
dsquery * -filter sAMAccountName=kuser3 -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\kuser3 -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 **сохранить на сервере VK WorkMail**. В дальнейшем их нужно будет добавить в Deployer.

## Настройка интеграции с Active Directory

Авторизуйтесь в Admin Panel VK WorkMail под учетной записью администратора. Выберите адрес сервера, для которого нужно настроить интеграцию с Keycloak. У выбранного домена должна быть настроена **MX-запись**.

Для настройки интеграции с **Active Directory** перейдите в раздел административной панели **Конфигурация → Настройки**.

Чтобы начать настройку, уберите чекбокс **Не использовать AD**.

The screenshot shows the 'Настройки' (Settings) page for 'Active Directory' integration in the VK AdminPanel. The left sidebar contains navigation links: Пользователи, Администраторы, Почта, Файловое хранилище, Адресная книга, Структура компании, Управление доменом, Конфигурация, Настройки (selected), and Мониторинг. The main content area is titled 'Настройки' and 'Active Directory'. It contains several input fields: 'Адрес AD', 'Каталоги пользователей', 'Логин администратора', and 'Пароль администратора'. There are also checkboxes for 'Использовать шифрованное соединение (LDAPS)', 'Игнорировать ошибки сертификата', and 'Не использовать AD' (which is checked and highlighted with a red box). A 'Сохранить' (Save) button is at the bottom.

**Адрес AD** — введите в поле адрес вашего каталога Active Directory.

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

### Примечание

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



**Логин администратора** — введите в поле логин администратора Active Directory.

**Пароль администратора** — вставьте в поле пароль администратора Active Directory.

**Поле свойства «Отчество»** — если вы используете свойство **Отчество**, введите его значение в это поле.

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

**Игнорировать ошибки сертификата** — если у вас самоподписанный SSL-сертификат, отметьте этот чекбокс.

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

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

Для применения настроек нажмите на кнопку **Сохранить**.

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

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

## Проверка настроек домена

Далее необходимо проверить файл настроек домена, для которого будет настраиваться интеграция с Keycloak. Перейдите по URL административной панели

[https://biz.<domain\\_name>/admin/misc/configurations/adloaderclient/](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"/>	<div>exch.on-premise.ru</div>	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

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







VK WorkDisk

1 виртуальная машина на любом гипервизоре, 16 GB RAM, 8 vCPU, 100 GB SSD

Интеграция с антивирусом по протоколу ICAP

Инструменты разработки

Интеграция с VK Teams

Интеграция с ЕСИА

Интеграция с другими инсталляциями VK WorkMail 

Deprecated

Интеграция с keycloak для SSO авторизации

Keycloak внутри инсталляции v17.0.1

1 GB RAM, 1 vCPU

Средства резервного копирования почтовых ящиков

Двухфакторная аутентификация

Примечание

Если вы планируете использовать внешний сервис Keycloak, вторую опцию включать **не нужно**.

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

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

Затем в Настройках перейдите в раздел **Интеграции** → **Интеграция с keycloak для SSO авторизации**.



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

#### Информация

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

Сохраните изменения. Если деплоер выдаст ошибку, попробуйте сохранить еще раз.

## Настройки в интерфейсе Keycloak

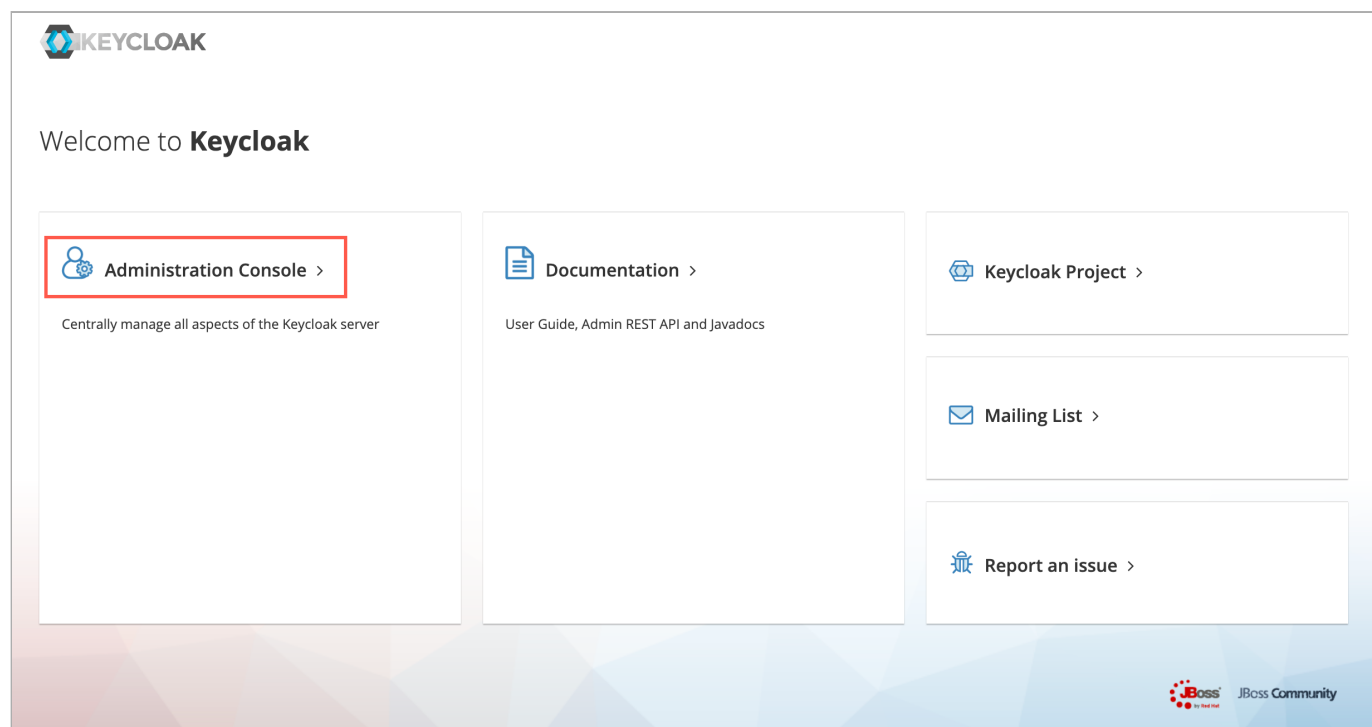
Прежде чем перейти в интерфейс Keycloak, на сервере с дистрибутивом VK WorkMail выполните команду:

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

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

#### Примечание

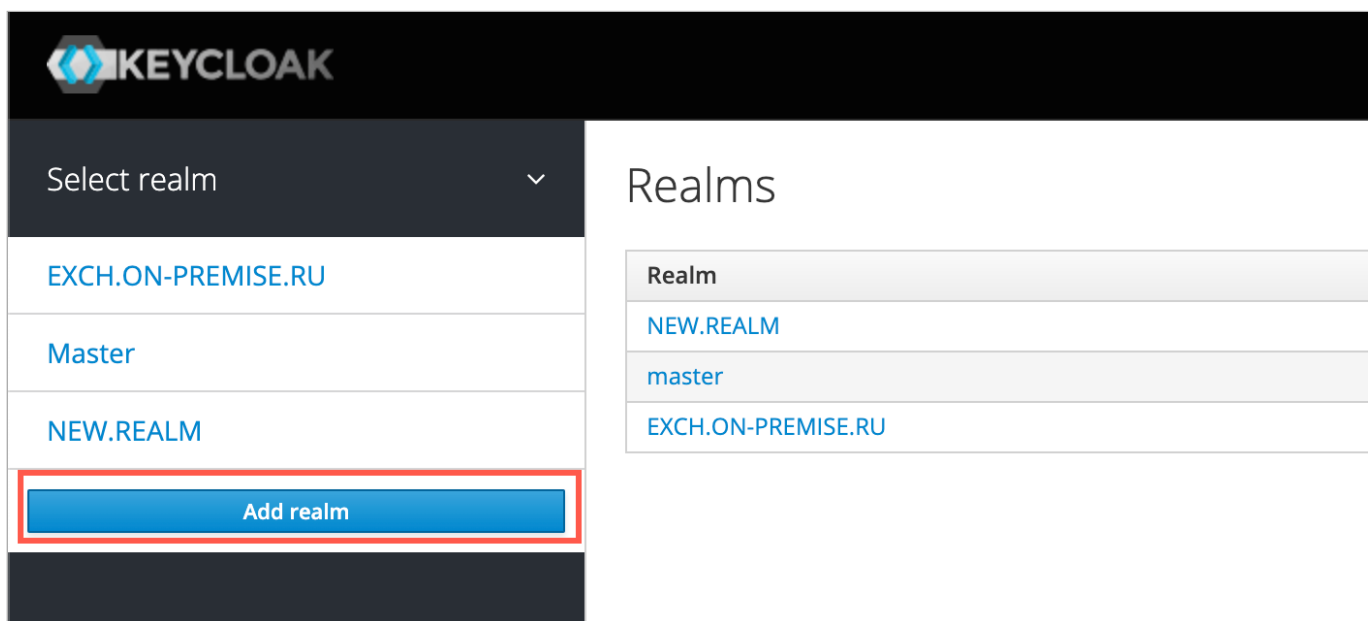
Если вы используете внешний сервер Keycloak, перейдите в его панель администрирования.



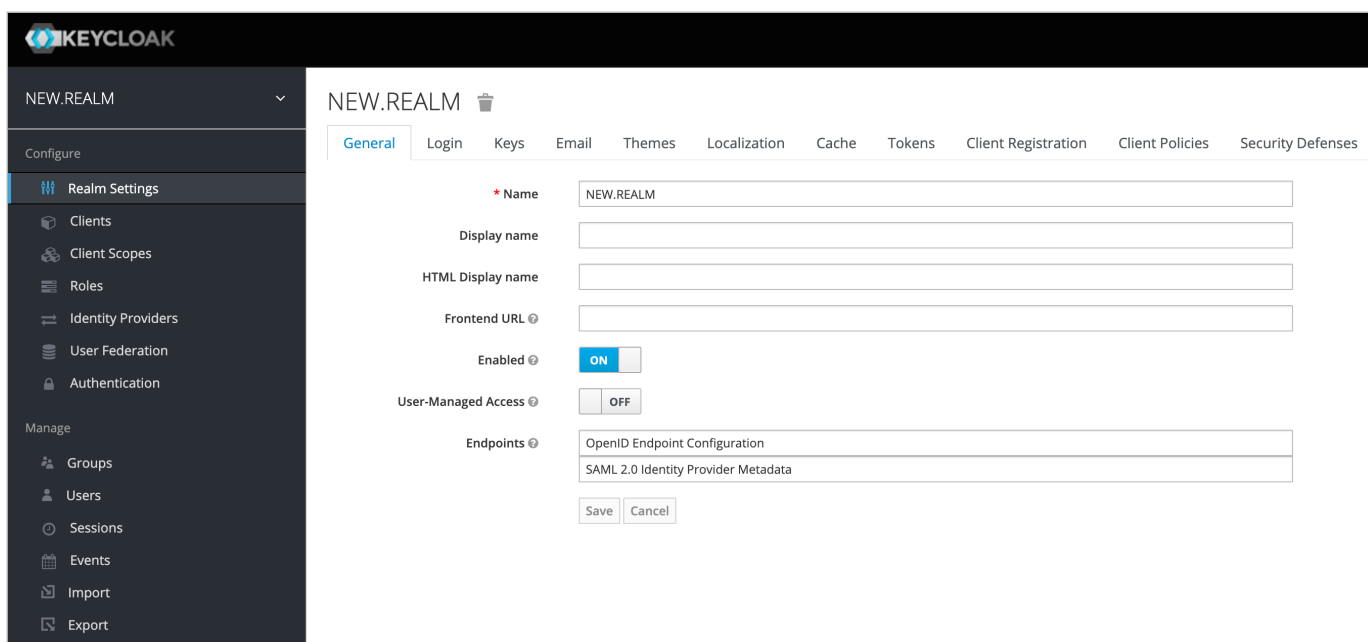


# Создание и настройка REALM

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



В поле **Name** введите имя REALM, аналогичное указанному в интерфейсе деплоера, и нажмите на кнопку **Create** — откроется окно настроек, раздел **General**.



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

## Примечание

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

Во вкладке **Login** у параметра **Require SSL** необходимо выбрать значение **none**. Настройки нужно также **сохранить**.



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...

Q

Add keystore...

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

## Добавление Client API

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

KEYCLOAK

NEW.REALM

Configure

Realm Settings

Clients

Client Scopes

Roles

Identity Providers

User Federation

Authentication

Manage

Groups

Clients > Add Client

Add Client

Import

Select file

Client ID

api

Client Protocol

openid-connect

Root URL

Save

Cancel

Вкладку Settings нужно настроить следующим образом:

### Важно

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 \*);

По завершении настроек сохраните изменения и перейдите во вкладку **Credentials**.

Скопируйте или сохраните значение поля **Secret**.



NEW.REALM

Configure

- Realm Settings
- Clients**
- Client Scopes
- Roles
- Identity Providers
- User Federation
- Authentication

Manage

- Groups
- Users
- Sessions
- Events

Clients > api

Api

Settings Credentials Keys Roles Client Scopes Mappers Scope Authorization Revocation

Service Account Roles

Client Authenticator Client Id and Secret

Secret Regenerate Secret

Registration access token Regenerate registration access token

## Настройка интеграции с LDAP

Далее нужно перейти в раздел **User Federation** и в выпадающем меню Add provider выбрать **Idap**.

Внесите данные в соответствие 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 ON

Console Display Name Idap

Priority 0

Import Users ON

Edit Mode READ\_ONLY

Sync Registrations OFF

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



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

Settings Mappers

Required Settings

Provider ID7bd58fef-270b-4acf-88ed-23468ad18d8b

Enabled?ON

Console Display Name?ldap

Priority?0

Import Users?ON

\* Edit Mode?READ\_ONLY

Sync Registrations?OFF

\* 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

## Настройка интеграции с Kerberos

Затем раскройте вкладку **Kerberos Integration** 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

**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.

Сохраните изменения.

# Добавление в контейнер Keycloak файла .keytab

Для добавления файла в контейнер выполните следующую команду на сервере VK WorkMail:

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

# Настройка параметров интеграции для SSO в Deployer

Теперь в настройках установщика VK VorkMail необходимо перейти в раздел **Интеграции** → **Интеграция с keycloak для SSO авторизации**.

Настройки

СетиДоменные именаХранилищаШардирование и репликация БДНастройки компонентовИнтеграцииПеременные окружения

Интеграция с VK TeamsБоты для VK TeamsИнтеграция с антивирусом по протоколу ICAPЛицензия редактора R7 ОфисСборщик почтыИнтеграция с другими инсталляциями VK WorkMail DeprecatedИнтеграция с keycloak для SSO авторизацииМиграция календарей по протоколу EWS

Настройки интеграции с Keycloak

ОтменаСохранить

Название REALM'а в Keycloak:	EXCH.ON-PREMISE.RU
ID oauth клиента в Keycloak:	api
Secret oauth клиента в Keycloak:	*****
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 <div>Выбрать файл</div>
Keytab файл для SMTP:	Файл уже загружен <div>Выбрать файл</div>

**Secret oauth клиента в Keycloak** — введите в поле код из раздела **Clients** → **Credentials** в Keycloak, который вы сохранили ранее.

Далее необходимо добавить адреса сервисов Kerberos (с портами) и [keytab-файлов](#) для IMAP и SMTP и **сохранить** изменения.

Для применения настроек 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**.



## 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.