Диск VK WorkSpace

Настройка SSO-аутентификации

Портал с документацией: https://biz.mail.ru/docs/on-premises/

Оглавление

Назначение документа

В документе описан порядок действий для настройки SSO как с использованием сервиса Keycloak, так и без него. По завершении интеграции пользователи получат возможность проходить SSO-аутентификацию внутри Диска 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 Диска и в панель администратора 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/<домен Диска>`.
- Для интеграции без Keycloak — `HTTP/auth.<домен Диска>`.

В окне **Account options** внутри того же раздела 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
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.

Как получить Kerberos SPN и REALM

Выполните следующие команды на сервере Active Directory для получения SPN и REALM:

```
Get-ADComputer -Identity <dc-name> -Properties servicePrincipalName | Select-Object
servicePrincipalName

Get-ADDomain | Select-Object Name, DNSRoot, Forest
```

Сохраните полученные значения: - **DNSRoot** — будет использоваться как Kerberos Realm. - **servicePrincipalName** — пример формата SPN.

Как сгенерировать keytab-файлы

Команды ниже выполняйте на сервере Active Directory.

При интеграции с Keycloak

Пример команды, чтобы создать keytab для WEB:

```
ktpass -princ HTTP/infra-01.dev.onprem.ru@AD2013.ON-PREMISE.RU -mapuser AD2013\kcuser3 -out C:
\tmp\keycloak.keytab -mapOp set -crypto AES256-SHA1 -setupn -setpass -ptype
KRB5_NT_PRINCIPAL /pass strongSecret
```

Сохраните созданный keytab-файл для HTTP на сервере Диска.

Чтобы сгенерировать keytab-файлы для SMTP и IMAP, используйте следующие команды:

```
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 AES256-SHA1 -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 AES256-SHA1 -setupn -setpass -ptype
KRB5_NT_PRINCIPAL /kvno <N> /pass strongSecret
```

Фйалы .keytab для IMAP и SMTP нужно сохранить на сервере Диска. В дальнейшем их нужно будет добавить в установщик.

Без интеграции с Keycloak

Пример команд, чтобы создать keytab для WEB:

```
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>"
```

Чтобы сгенерировать keytab-файлы для SMTP, IMAP и WebDAV, используйте следующие команды:

```
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 AES256-SHA1 -setupn -setpass -ptype
KRB5_NT_PRINCIPAL /kvno <N> /pass strongSecret
ktpass -princ webdav/infra-01.dev.onprem.ru@AD2013.ON-PREMISE.RU -mapuser AD2013\webdav_user -
out C:\tmp\infra_webdav.keytab -mapOp add -crypto AES256-SHA1 -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 AES256-SHA1 -setupn -setpass -ptype
KRB5_NT_PRINCIPAL /kvno <N> /pass strongSecret
```

Файлы .keytab для IMAP, SMTP и WebDAV нужно сохранить на сервере Диска. В дальнейшем их нужно будет добавить в установщик.

Параметры команды ktpass

- `princ` — имя SPN в Keycloak для идентификации в среде Kerberos.

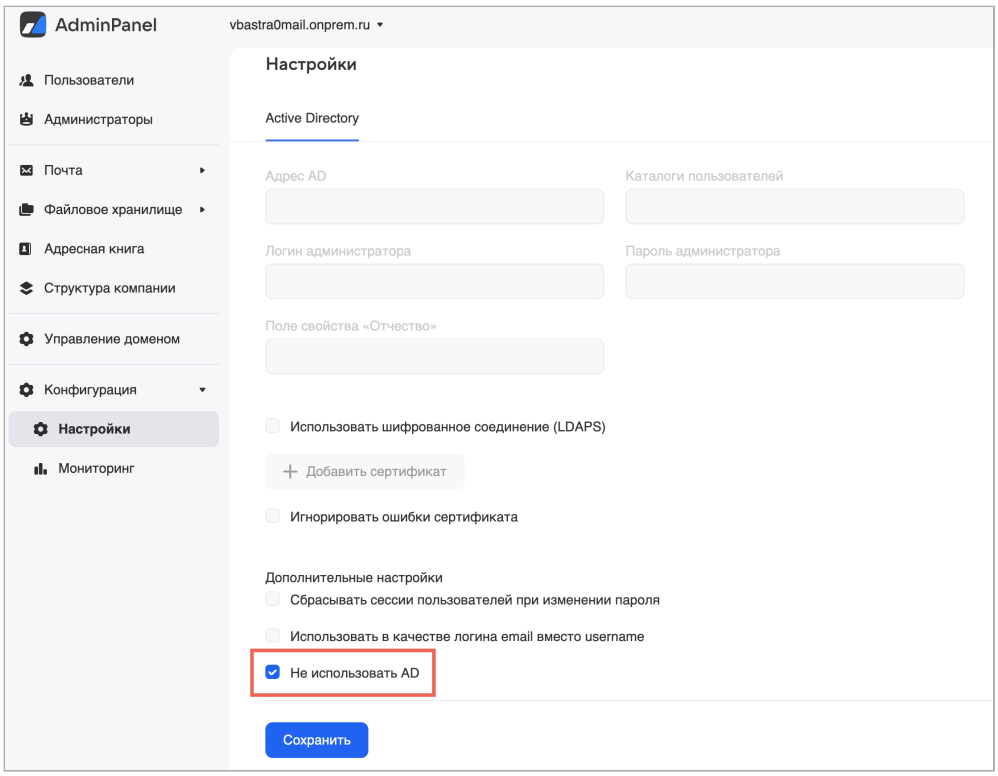
  Имя состоит из: - Транспортного протокола. Для HTTP в верхнем регистре.\ - Имени хоста сервера Keycloak или адреса сервера Диска для интеграций внутри инсталляции. - Kerberos Realm. Для HTTP в верхнем регистре.
- `mapuser` – имя созданной в домене учетной записи для сервера Keycloak (DOMAIN\username).
- `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 AES256-SHA1 -ptype KRB5_NT_PRINCIPAL`.
- Параметр -setupn необходим для того, чтобы UPN не менялся.

Настройка интеграции с Active Directory

> **Внимание**
>
> Учетные записи в Active Directory должны быть отдельными для каждого сервиса:
>
> - `smtp_user` — для SMTP
> - `imap_user` — для IMAP
> - `http_user` — для HTTP
> - `webdav_user` — для WebDAV
>
> Не используйте одну учетную запись для всех сервисов.

1. Авторизуйтесь в панели администратора 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 Диска.

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

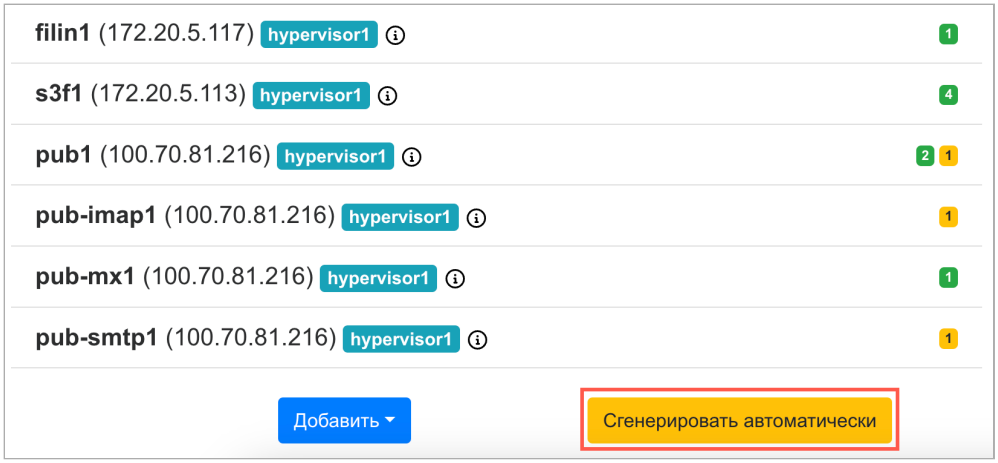
12. Нажмите на кнопку **Сохранить**, чтобы применить настройки.

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

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

SSO через Kerberos

1. Перейдите в веб-интерфейс установщика, в адресной строке браузера укажите адрес: `http://server-ip-address:8888`.
2. Нажмите на значок ⓘ и перейдите в раздел **Продукты**.
3. Перейдите на вкладку **Администрирование**.
4. Включите опции **Вход через Kerberos** и **Keycloak (внешний)**.
5. Сохраните изменения и вернитесь к списку ролей, чтобы сгенерировать дополнительные контейнеры.



6. Затем в Настройках перейдите в раздел **Интеграции → Вход через Kerberos**.
7. 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)**.
8. Добавьте keytab-файлы в соответствующие поля и сохраните изменения.
9. Чтобы применить новую конфигурацию перейдите к списку ролей и повторите соответствующие шаги или запустите автоматическую установку.

Пример конфигурации krb5.conf

На сервере Диска проверьте файл `/etc/krb5.conf`:

```
[libdefaults]
    default_realm = <YOUR_REALM>
    dns_lookup_realm = false
    dns_lookup_kdc = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    allow_weak_crypto = true
    default_tkt_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 rc4-hmac
    default_tgs_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 rc4-hmac
    permitted_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 rc4-hmac
    rdns = false

[realms]
    <YOUR_REALM> = {
        kdc = <ad-server>:88
        admin_server = <ad-server>:749
    }

[domain_realm]
    .<your-domain> = <YOUR_REALM>
    <your-domain> = <YOUR_REALM>
```

Замените `<YOUR_REALM>`, `<ad-server>` и `<your-domain>` на ваши значения.

Как настроить политики браузера Google Chrome?

Для корректной работы SSO на клиентских машинах необходимо настроить политики Google Chrome. Выполните следующие команды в терминале с правами администратора:

```
reg add "HKLM\SOFTWARE\Policies\Google\Chrome" /v AuthSchemes /t REG_SZ /d
"negotiate,ntlm,basic,digest" /f

reg add "HKLM\SOFTWARE\Policies\Google\Chrome" /v AuthServerAllowlist /t REG_SZ /d "*.<your-
domain>,<ad-server>,<kerberos-realm>,*.<mail-domain>" /f

reg add "HKLM\SOFTWARE\Policies\Google\Chrome" /v AuthNegotiateDelegateAllowlist /t REG_SZ /d
"*.<your-domain>,*.<mail-domain>" /f
```

После настройки политик проверьте их в браузере Chrome: 1. Откройте `chrome://policy` 2. Убедитесь, что политики `AuthSchemes`, `AuthServerAllowlist`, `AuthNegotiateDelegateAllowlist` отображаются без ошибок

SSO в деплоере

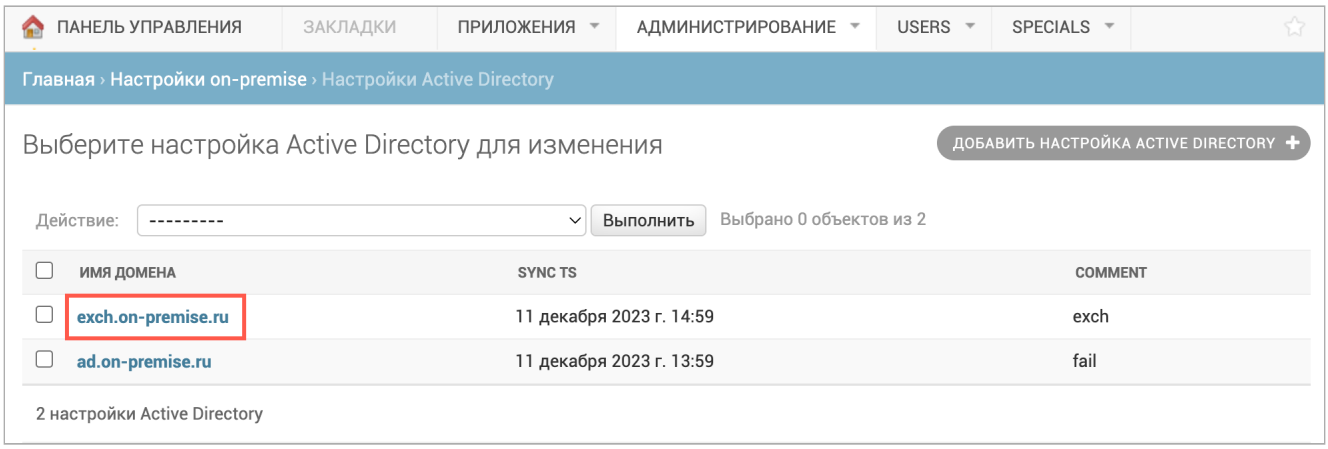
Политики должны быть подсвечены как гиперссылки, без ошибок (error).

SSO через Keycloak

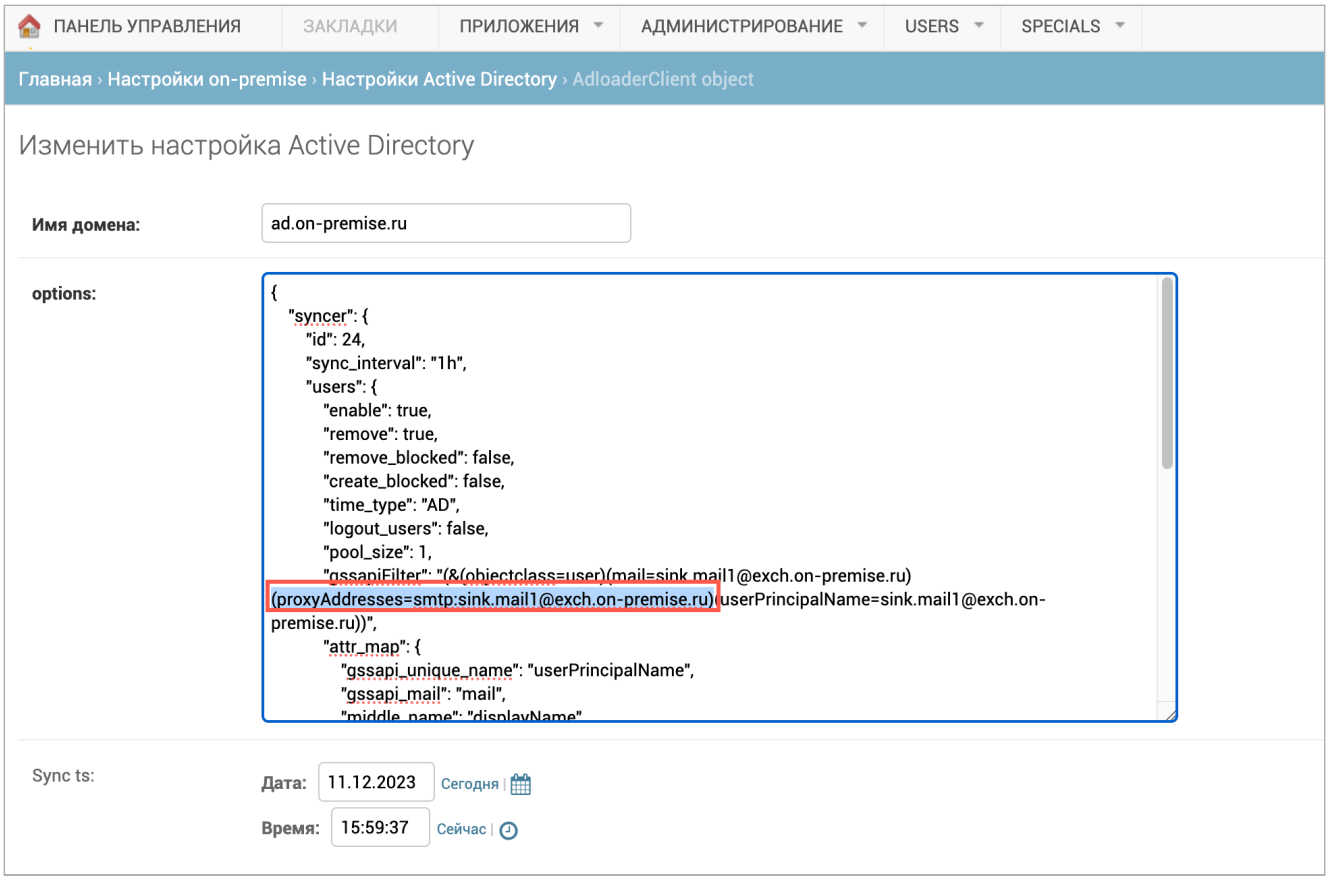
Шаг 1. Проверьте настройки домена

Проверьте 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.



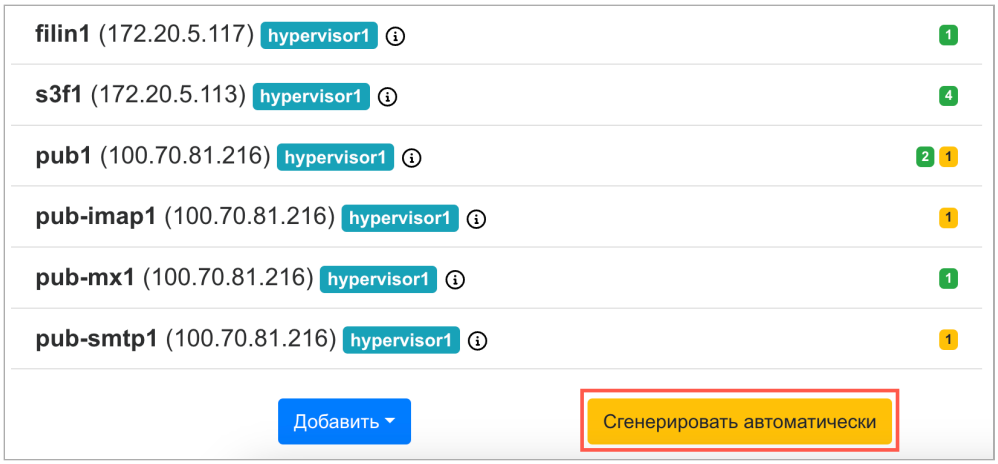
2. Убедитесь, что в разделе **options** отсутствует значение `proxyAddresses`.



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

Шаг 2. Настройте интеграцию в установщике

1. Перейдите в веб-интерфейс установщика, в адресной строке браузера укажите адрес: `http://server-ip-address:8888`.
2. Нажмите на значок ⓘ и перейдите в раздел **Продукты**.
3. Перейдите на вкладку **Администрирование**.
4. Включите опции **Вход через Kerberos** и **Keycloak внутри инсталляции**. Если вы планируете использовать внешний сервис Keycloak, нужно включить опцию **Интеграция с внешним Keycloak сервером**.
5. Сохраните изменения и вернитесь к списку ролей, чтобы сгенерировать дополнительные контейнеры.



6. В настройках перейдите в раздел **Интеграции** → **Вход через Kerberos**.
7. Введите заглавными буквами адрес сервера Active Directory, который будет использоваться в интеграции, в поле **Имя REALM в Keycloak**.

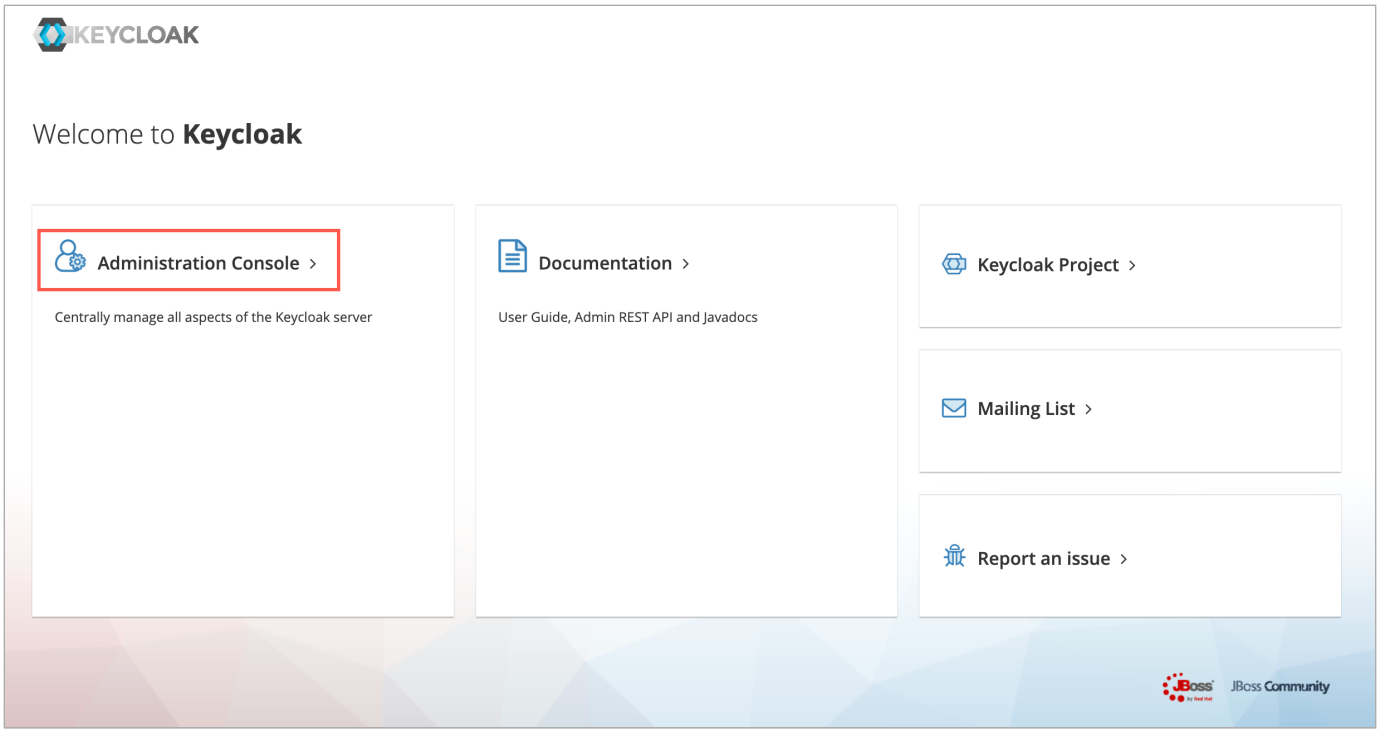
   В поле можно также ввести любое ключевое название, например KEYCLOAKREALM. Позже это значение будет использоваться при настройках в интерфейсе Keycloak. REALM в установщике не должен совпадать с Kerberos REALM, у них разное назначение.
8. Сохраните изменения.
9. Если установщик выдаст ошибку, попробуйте сохранить еще раз.
10. Прежде чем перейти в интерфейс Keycloak, на сервере с дистрибутивом Диска выполните команду:

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

Шаг 3. Перейдите в Keycloak

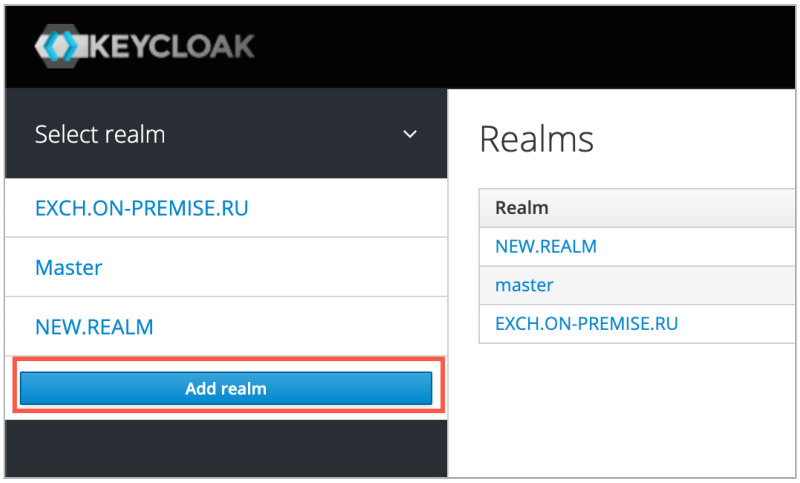
Для перехода в Keycloak в строке браузера введите адрес: `https://biz.<mail_domain>/auth`.

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

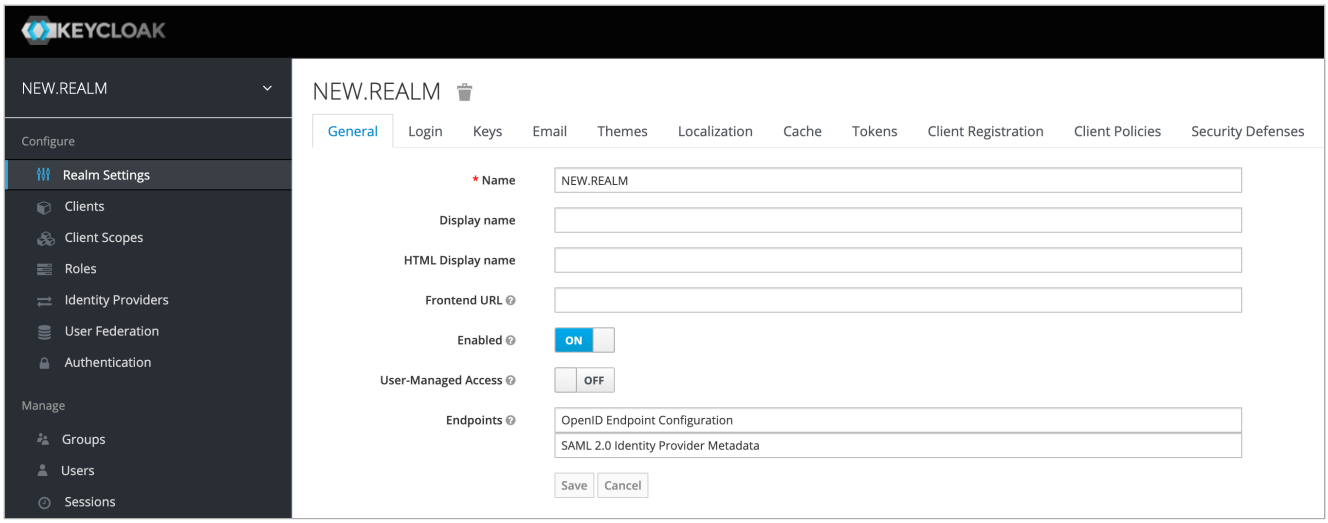


Шаг 4. Создайте и настройте REALM

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



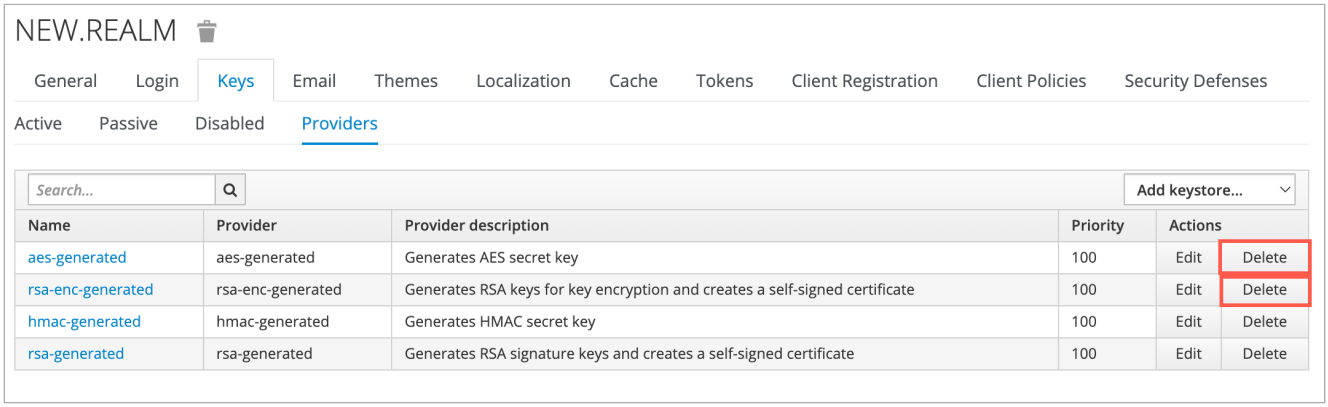
2. В поле **Name** введите имя REALM, аналогичное указанному в интерфейсе установщика.
3. Нажмите на кнопку **Create** — откроется окно настроек, раздел **General.**



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

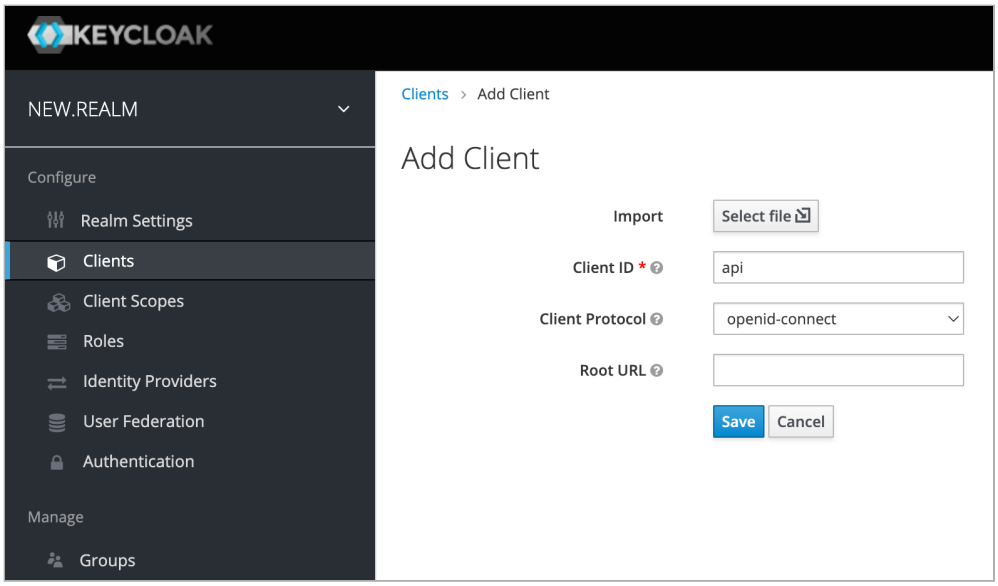
> **Примечание**
>
> При использовании внешнего сервера Keycloak нужна дополнительная настройка на `/auth` с помощью параметра `http-relative-path=/auth`.

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`).



Шаг 5. Добавьте Client API

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

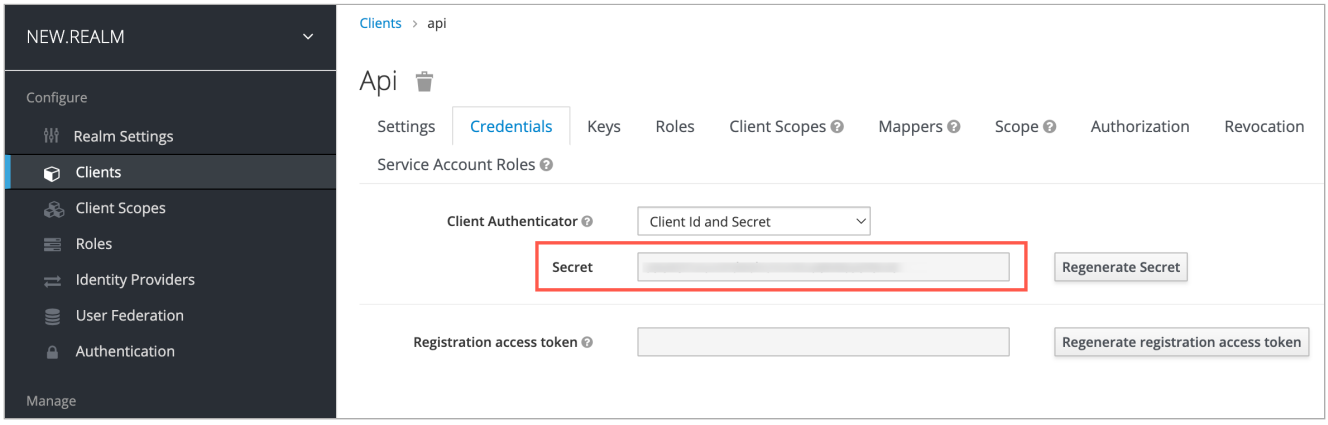


2. Вкладку Settings нужно настроить следующим образом:

> **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**.



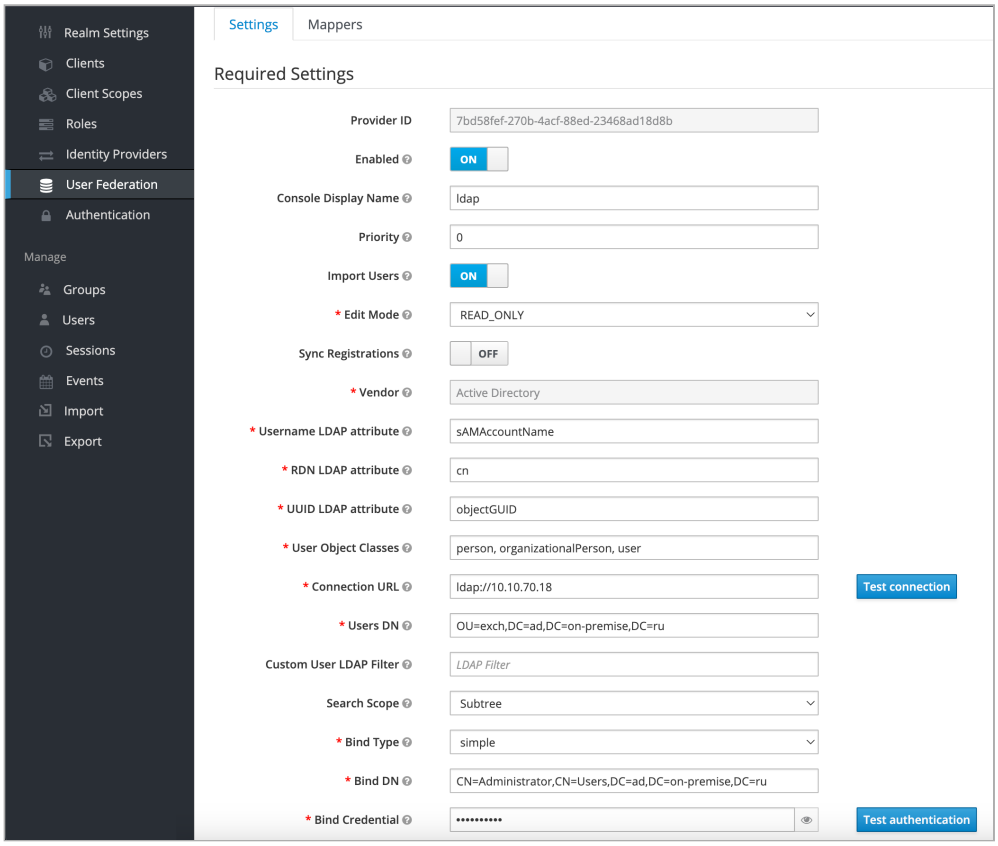
Шаг 6. Настройте интеграцию с LDAP

1. Перейдите в раздел **User Federation** и в выпадающем меню Add provider выберите **ldap**.

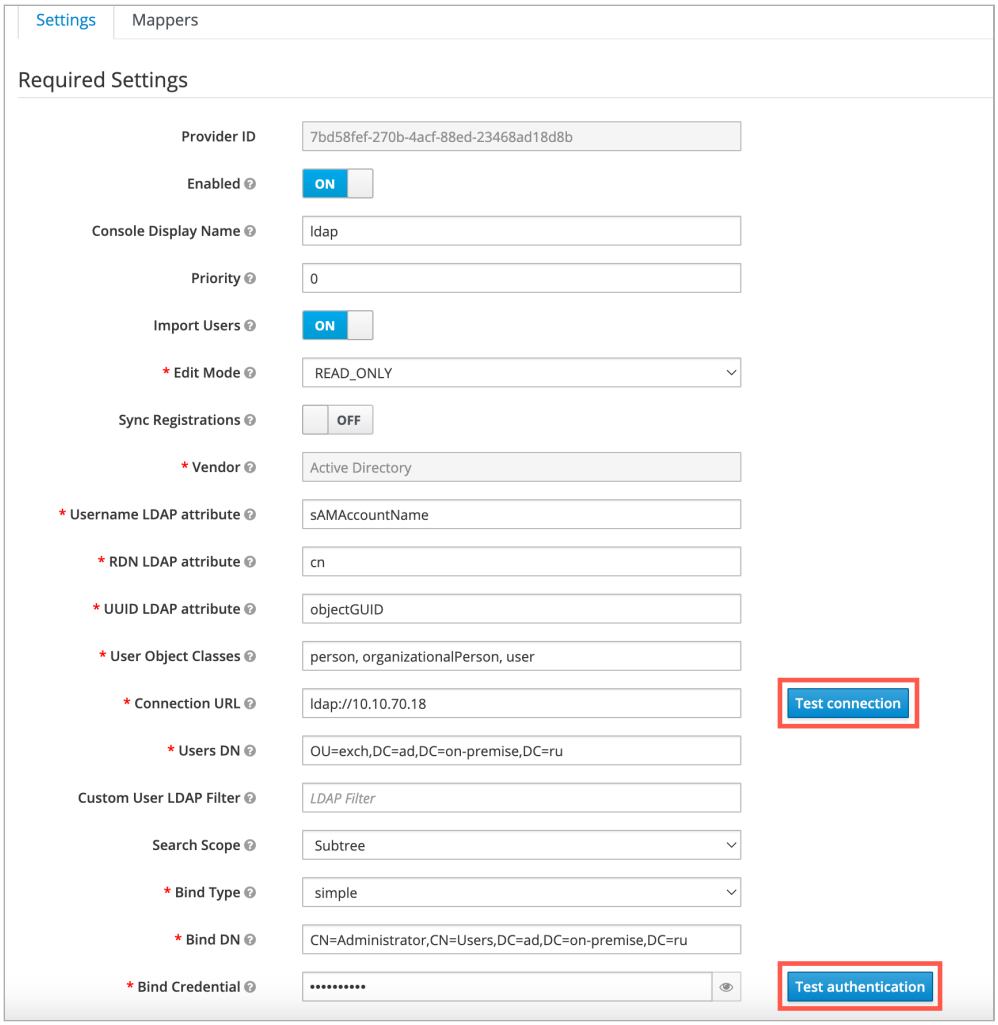
2. Внесите данные в соотвествие с настройками LDAP в вашем каталоге Active Directory.

   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.

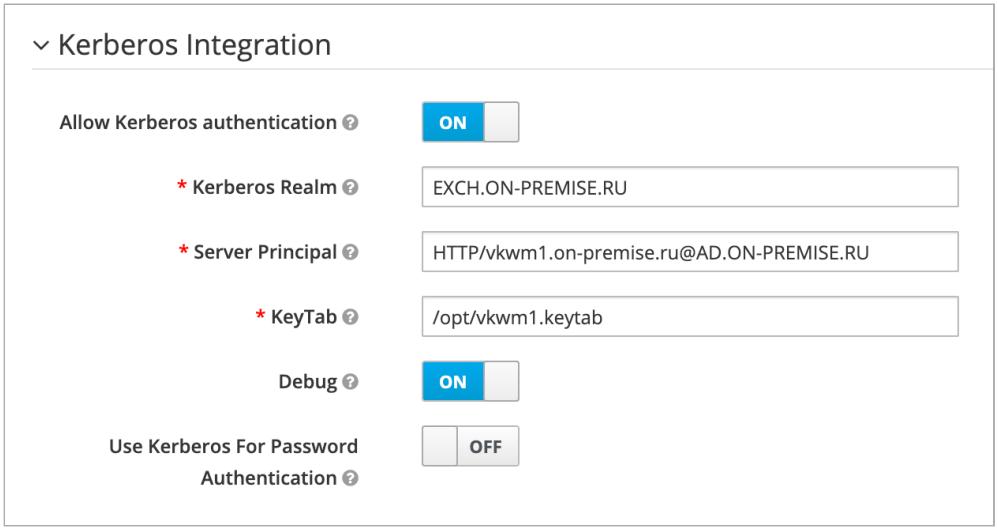


3. Проверьте соединение с помощью кнопок **Test connection** и **Bind Credential**.



Шаг 7. Настройте интеграцию с Kerberos при работе с Keycloak

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



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 8. Добавьте в контейнер Keycloak файла .keytab

Выполните следующую команду на сервере Диска:

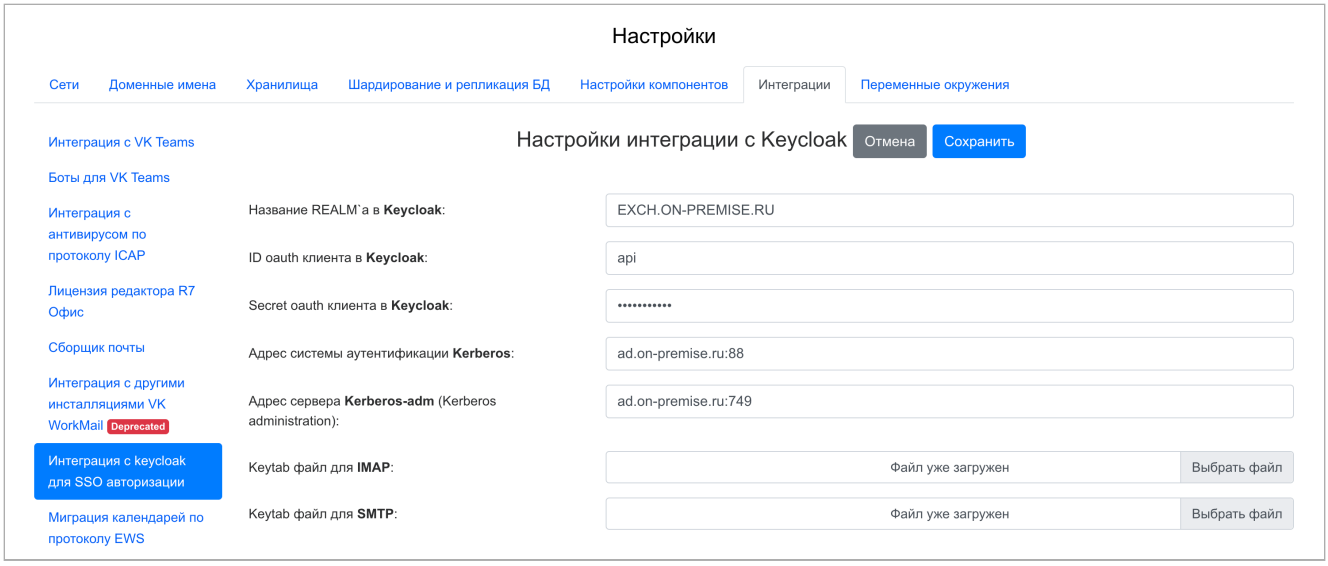
```
cp http.keytab /opt/mailOnPremise/dockerVolumes/keycloak1/keytabs/
cp smtp.keytab /opt/mailOnPremise/dockerVolumes/keycloak1/keytabs/
cp imap.keytab /opt/mailOnPremise/dockerVolumes/keycloak1/keytabs/
cp webdav.keytab /opt/mailOnPremise/dockerVolumes/keycloak1/keytabs/
```

Или скопируйте все keytab-файлы одной командой:

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

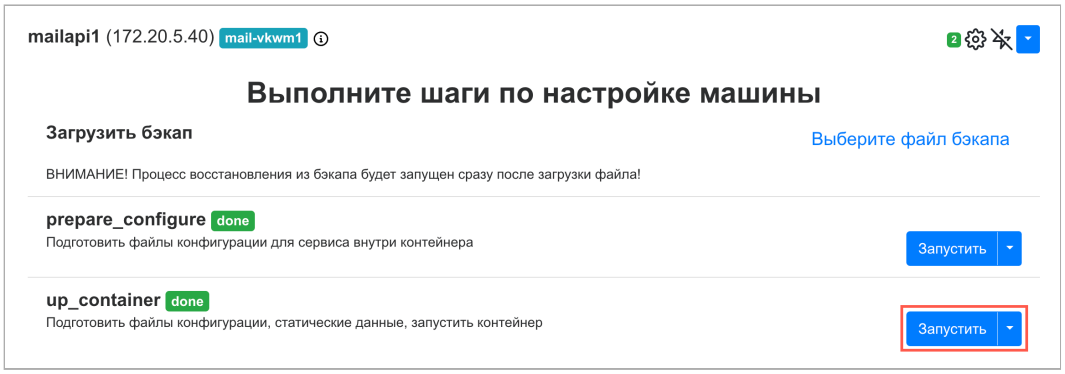
Шаг 9. Настройте параметры интеграции с Keycloak в установщике

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



2. В поле **Client Secret в Keycloak** введите код из раздела **Clients → Credentials** в Keycloak, который вы сохранили ранее.
3. Добавьте адреса сервисов Kerberos (с портами) и keytab-файлов для IMAP и SMTP.
4. Сохраните изменения.

5. Чтобы применить изменения перейдите к списку ролей и запустите автоматическую установку.
6. Чтобы в интерфейсе пользователей начала отображаться кнопка **Войти через SSO**, выполните в контейнере **mailapi1** шаг **up_container**.



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

24 июня 2026 г.