Интеграция BearPass со службой каталога ALD Pro

01/28/2026

Содержание

BearPass — корпоративный менеджер паролей, обеспечивающий централизованное и защищенное хранение учетных данных к корпоративным системам и сервисам. Он снимает рутину управления доступами: ускоряет выдачу прав новым сотрудникам, мгновенно отзывает доступы при увольнении, позволяет управлять правами через роли и группы, а также ведет детальное журналирование всех действий. Встроенный аудит безопасности и мониторинг компрометаций помогают быстро находить слабые, устаревшие или утекшие пароли и эффективно расследовать инциденты.

Интеграция позволяет:
- настроить синхронизацию пользователей и групп из ALD Pro через LDAP Bind и использовать их для последующей аутентификации в BearPass;
- централизовать управление учетными записями и доступами: профили пользователей создаются, блокируются и обновляются автоматически;
- права (роли/доступ к папкам и секретам) назначаются согласно настроенным правилам привязки LDAP-групп к группам BearPass.

1 Описание стенда

Параметр	Значение
IP сервера BearPass	`192.168.121.180`
Имя хоста сервера BearPass	`bearpass.ald.company.lan`
Имя контроллера домена ALD Pro	`dc-1.ald.company.lan`
IP контроллера домена ALD Pro	`192.168.121.10`

2 Лицензия

Для использования интеграции вам необходимо приобрести коммерческую лицензию BearPass, после чего активировать ее в разделе **Администрирование** → **Настройки** → **Лицензия** (рис 1).

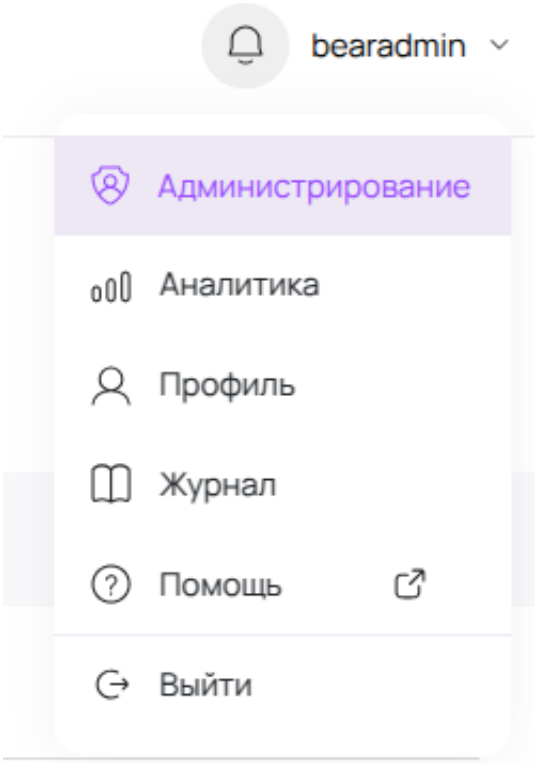

Рисунок 1 - Меню перехода в раздел **Администрирование**

В разделе **Лицензия** введите ключ лицензии и нажмите "Сохранить", после чего можно будет продолжить настройку (рис. 2).

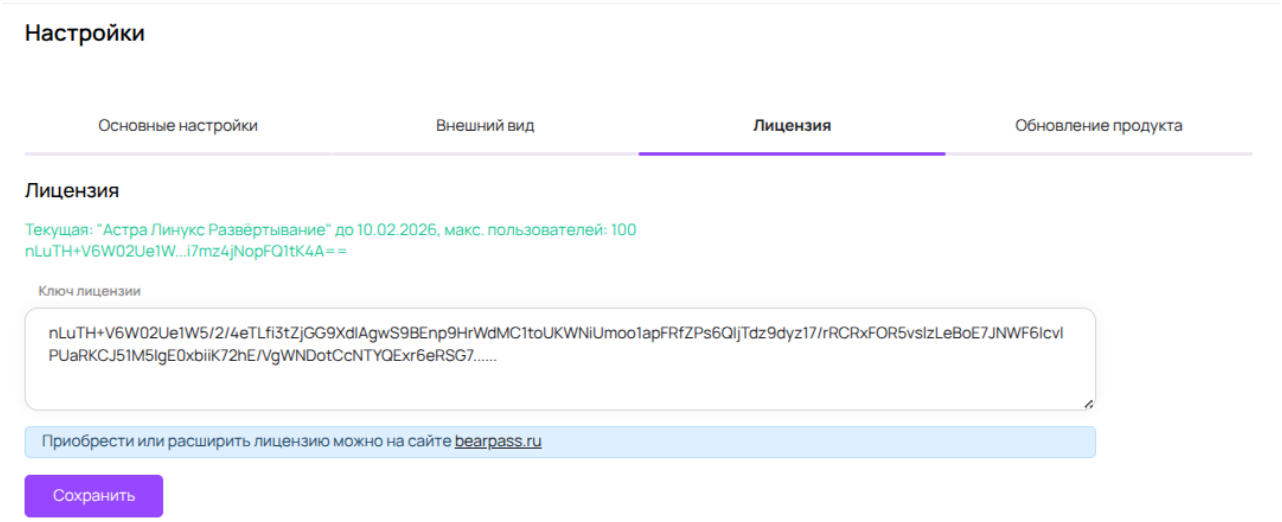

Рисунок 2 - Активация лицензии

3 Настройка интеграции через LDAP

3.1 Предварительные настройки

Подключение к ALD Pro рекомендуется выполнять по защищенному соединению LDAPS: необходимо настроить разрешение имени контроллера домена ALD Pro и подключить используемый SSL-сертификат.

Для получения сертификата на контроллере домена выполните следующую команду и сохраните вывод сертификата:

```
sudo cat /etc/ssl/freeipa/ca.crt

# пример вывода
-----BEGIN CERTIFICATE-----
MIIDIzCCAgugAwIBAgIUNAiEhdsuCHNr1THs+L+WlT3+L9EwDQYJKoZIhvcNAQEL
BQAwITEfMB0GA1UEAwwWQ0EgU2lnbmluZyBDZXJ0aWZpY2F0ZTAeFw0yNjAxMjMw
OTM3MTVaFw00NjAxMTgwOTM3MTVaMCExHzAdBgNVBAMMFkNBIFNpZ25pbmcgQ2Vy
dGlmaWNhdGUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC1NUu29CLE
G5ASeFReh6bbINNR7Tmt4+9nEnUVnfZNjS5Tj0a/nY6+0CVsW3VXv99VJ3PSpIWT
J3xsSgpVOph28Lg6rGSf26csTiyljQFSEloaLhM4skCPIweq3lXo....
...
-----END CERTIFICATE-----
```

3.1.1 Настройка разрешения имени контроллера домена

Нативная установка

Добавьте строки для привязки имени контроллера домена к адресу.

Для нативной установки достаточно добавить следующую запись в файл `/etc/hosts`:

```
# fqdn ip
192.168.121.10 dc-1.ald.company.lan
```

> **Примечание**
>
> Если компьютер является членом домена ALD Pro, то имя контроллера домена должно разрешаться автоматически, и этот шаг можно пропустить.

Установка в контейнерах

При установке в контейнерах для настройки разрешения имени из-под пользователя bearpass отредактируйте файл `/opt/bearpass/docker/docker-compose.override.yml`, где `/opt/bearpass/docker` путь до рабочей директории BearPass.

Добавьте `extra_hosts:` с FQDN и адресом контроллера домена ALD Pro.

При пересоздании контейнера запись будет добавлена в `/etc/hosts` внутри контейнера автоматически.

Пример:

```
  app:
    restart: unless-stopped
    volumes:
      - ../app:/var/www/bearpass
    extra_hosts:
      - "dc-1.ald.company.lan:192.168.121.10"
```

После изменений пересоздайте контейнер.

```
cd /opt/bearpass/docker
docker compose down
docker compose up -d
```

3.1.2 Настройка сервисной учетной записи

Для интеграции с ALD Pro по протоколу LDAP рекомендуется использовать сервисную учетную запись.

Аутентификация и авторизация выполняются методом LDAP Bind, для чего необходимо создать в ALD Pro сервисную учетную запись, которая не является POSIX-пользователем, не имеет прав на вход в домен и не отображается в портале управления, а используется только для чтения LDAP.

Для этого нужно подключиться по SSH к контроллеру домена и выполнить следующие шаги:

1. Создать файл с именем `ldap-bind.update`.

2. Внести в файл следующее содержимое:

```
dn: uid=system,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan
add:objectclass: account
add:objectclass: simplesecurityobject
add:uid: system
add:userPassword: Pa$$w0rd
add:passwordExpirationTime: 20380119031407Z
add:nsIdleTimeout: 0
```

Разъяснения:

- **dn** — уникальный идентификатор записи пользователя в LDAP;
- **add:objectclass: account** — добавляет базовый класс для учетной записи;
- **add:objectclass: simplesecurityobject** — добавляет класс для хранения пароля и других атрибутов безопасности;
- **add:uid: ldap-bind** — уникальный идентификатор пользователя;
- **add:userPassword: securePassword** — пароль для учетной записи, заменить на желаемый;
- **add:passwordExpirationTime: 20380119031407Z** — время истечения пароля (можно адаптировать под политики безопасности);
- **add:nsIdleTimeout: 0** — отключает тайм-аут простоя для этой учетной записи.

Выполните создание сервисной учетной записи от имени суперпользователя:

```
kinit admin && ipa-ldap-updater  ldap-bind.update
```

Проверьте, что вы можете выполнять запросы из-под системной учетной записи:

```
ldapsearch -LLL -xD 'uid=system,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan' -w
'Pa$$w0rd' -s base
# вывод
dn: dc=ald,dc=company,dc=lan
objectClass: top
objectClass: domain
objectClass: pilotObject
objectClass: domainRelatedObject
objectClass: nisDomainObject
dc: ald
info: IPA V2.0
nisDomain: ald.company.lan
associatedDomain: ald.company.lan
```

3.2 Настройка LDAP-провайдера

В интерфейсе BearPass перейдите в раздел **Администрирование** → **LDAP** → **Добавить**.

Введите актуальные для вашего домена параметры. В качестве примера рассмотрим параметры, приведенные ниже.

Основные параметры

Название: `ald.company.lan`

Данные для подключения

Схема: `FreeIPA`

Хост: `ldaps://dc-1.ald.company.lan`

Сертификаты: введите сертификат, полученный ранее.

```
-----BEGIN CERTIFICATE-----
MIIDIzCCAgugAwIBAgIUNAiEhdsuCHNr1THs+L+WlT3+L9EwDQYJKoZIhvcNAQEL
BQAwITEfMB0GA1UEAwwWQ0EgU2lnbmluZyBDZXJ0aWZpY2F0ZTAeFw0yNjAxMjMw
OTM3MTVaFw00NjAxMTgwOTM3MTVaMCExHzAdBgNVBAMMFkNBIFNpZ25pbmcgQ2Vy
dGlmaWNhdGUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC1NUu29CLE
....
-----END CERTIFICATE-----
```

Использовать TLS — `Да`

Игнорировать ошибки сертификата — `Нет`

Базовый DN: `dc=ald,dc=company,dc=lan`

Сервисная учетная запись

Логин: `uid=system,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan`

Пароль: укажите пароль сервисной учетной записи (здесь: `Pa$$w0rd`).

Синхронизация

При синхронизации настроенного LDAP-провайдера создаются пользователи, которые попадают под фильтры. Если пользователь был синхронизирован и создан, а при повторном синке он не будет присутствовать в списке, учетная запись будет заблокирована на стороне BearPass.

Для корректной работы блокировки в ALD Pro нужно использовать фильтр, содержащий `nsaccountlock=false`.

Ниже приводятся примеры фильтров.

- Фильтр DN для получения списка пользователей

```
(& (|
     (objectclass=bearpassTest)
     (objectclass=posixAccount)
     (uid=*)
     (sAMAccountType=805306368)
     (&(objectCategory=person)(objectClass=user))
   )
   (nsaccountlock=false)
)
```

- Фильтр DN для получения списка групп

```
(|
       (objectclass=group)
       (objectclass=groupofnames)
       (objectclass=groupofuniquenames)
       (objectclass=organizationalRole)
       (objectclass=posixGroup)
)
```

Авторизация

Имя атрибута логина: `uid`

Маска логина: `uid={{login}},cn=users,cn=accounts,dc=ald,dc=company,dc=lan`

Запретить вход по паролю — `Нет`

Фоновая синхронизация — `Включена`

После заполнения всех необходимых полей нажмите кнопку "Сохранить" внизу страницы.

Для проверки перейдите на вкладку **Настройки синхронизации**. Будет выполнена проверка подключения к LDAP-серверу и корректности указанных параметров.

На рисунках 3 и 4 показан описанный выше пример настройки.

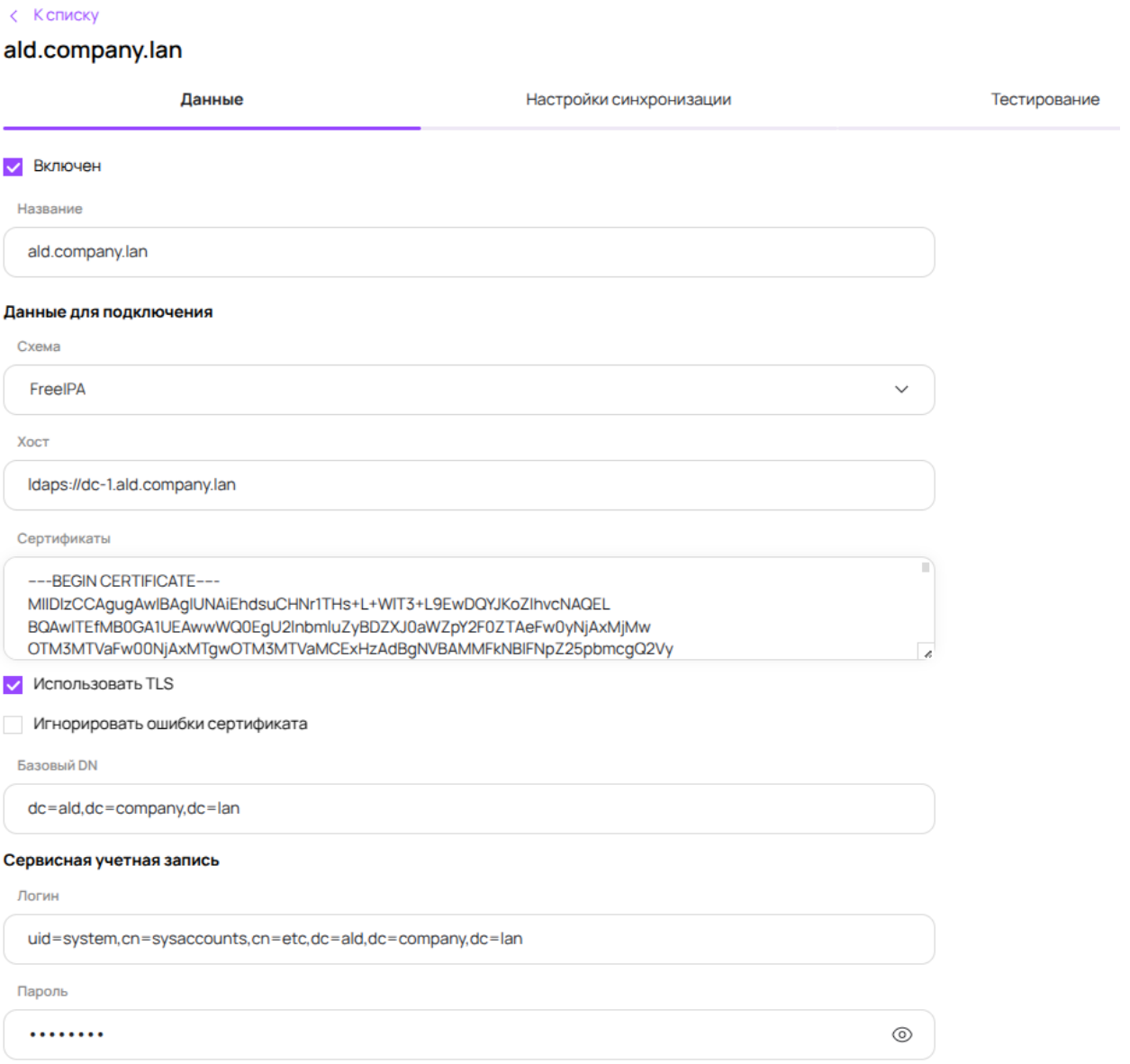

Рисунок 3 - Пример настройки

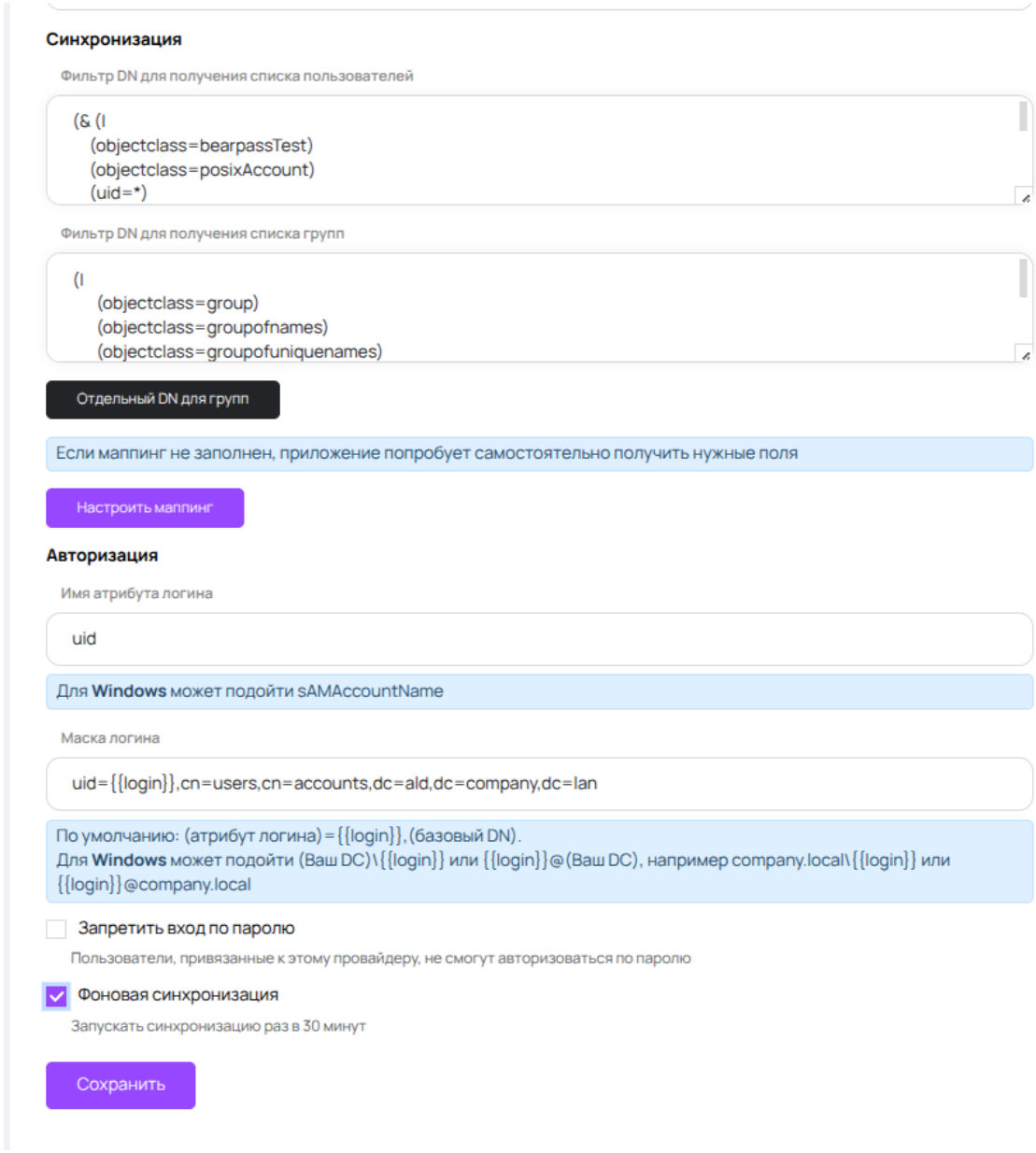

Рисунок 4 - Пример настройки (продолжение)

Дополнительно при необходимости можно настроить привязку групп из ALD Pro к локальным группам, для этого их нужно предварительно создать (рис. 5).

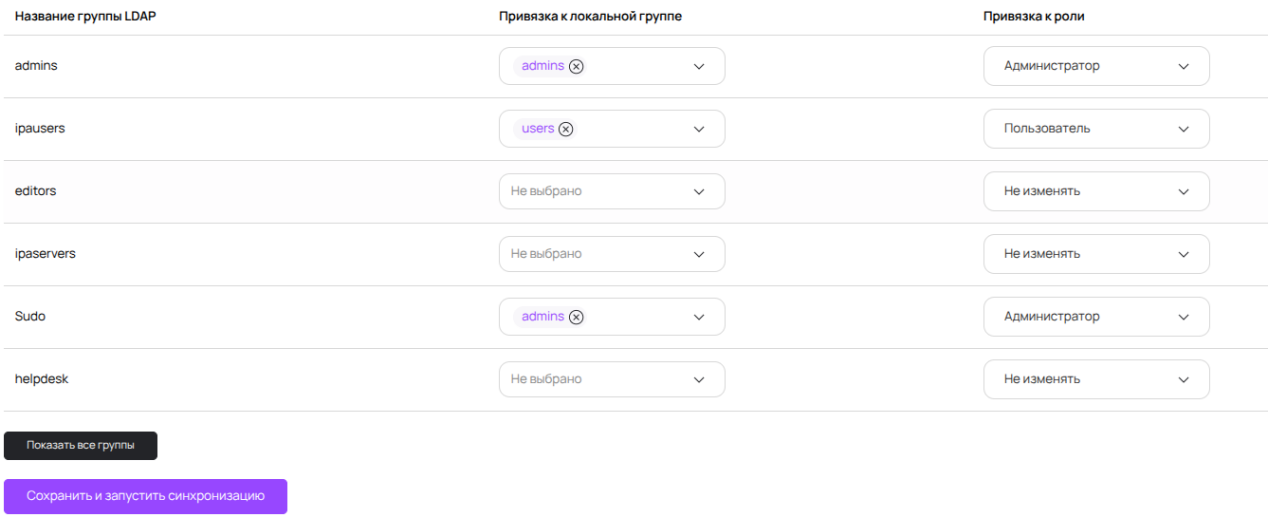

Рисунок 5 - Пример привязки к локальным группам admins, users

При успешной синхронизации вы увидите изменения при создании, обновлении и блокировке пользователей.

```
Добавлено пользователей: 1
Обновлено пользователей: 0
Заблокировано пользователей: 0
Разблокировано пользователей: 0
```

После успешной синхронизации можно авторизоваться под доменным пользователем и паролем.

Дополнительную информацию по использованию и настройке см. по ссылке https://docs.bearpass.ru/.