SOLAR

SafeConnect

Версия 1.17.0

Инструкция по настройке двухфакторной аутентификации по протоколу RADIUS от Aladdin 2FA

Москва, 2026

Содержание

1. Настройка 2FA OTP на Solar SafeConnect 3
2. Выпуск программных OTP-токенов (мобильное приложение) 4
3. Настройка JAS RADIUS SERVER JRS 8
4. Настройка 2FA доступа к системе SafeConnect 10

1. Настройка 2FA OTP на Solar SafeConnect

В данной инструкции представлены примеры настроек с использованием следующего программного обеспечения:

- SafeConnect версии 1.12.0 и выше;
- Aladdin JMS версии 4.1.0.6201;
- Aladdin JAS Radius Server версии 1.0.0.259;
- Aladdin 2FA Service версии 1.3.1.138.

Для реализации двухфакторной аутентификации можно использовать внешний сервер RADIUS. В данной инструкции представлена реализация второго фактора с помощью программного OTP-токена.

Примечание:

Предполагается, что уже установлены и настроены: JMS, сервер JAS в системе JMS. Выполнена настройка интеграции со службой управления учетными записями FreeIPA/MS AD. Сервис A2FA подключен к серверу JAS. Развернут компонент JAS RADIUS Server (JRS) для коммуникации с PAM-системой через протокол RADIUS.

2. Выпуск программных OTP-токенов (мобильное приложение)

Для выпуска программных OTP-токенов необходимо выполнить следующее:

1. Создать профиль выпуска программных OTP-токенов, руководствуясь разделом **Настройка профиля выпуска программных OTP-токенов** (стр. 166 JMS-4LX Руководства администратора, ч. 2).

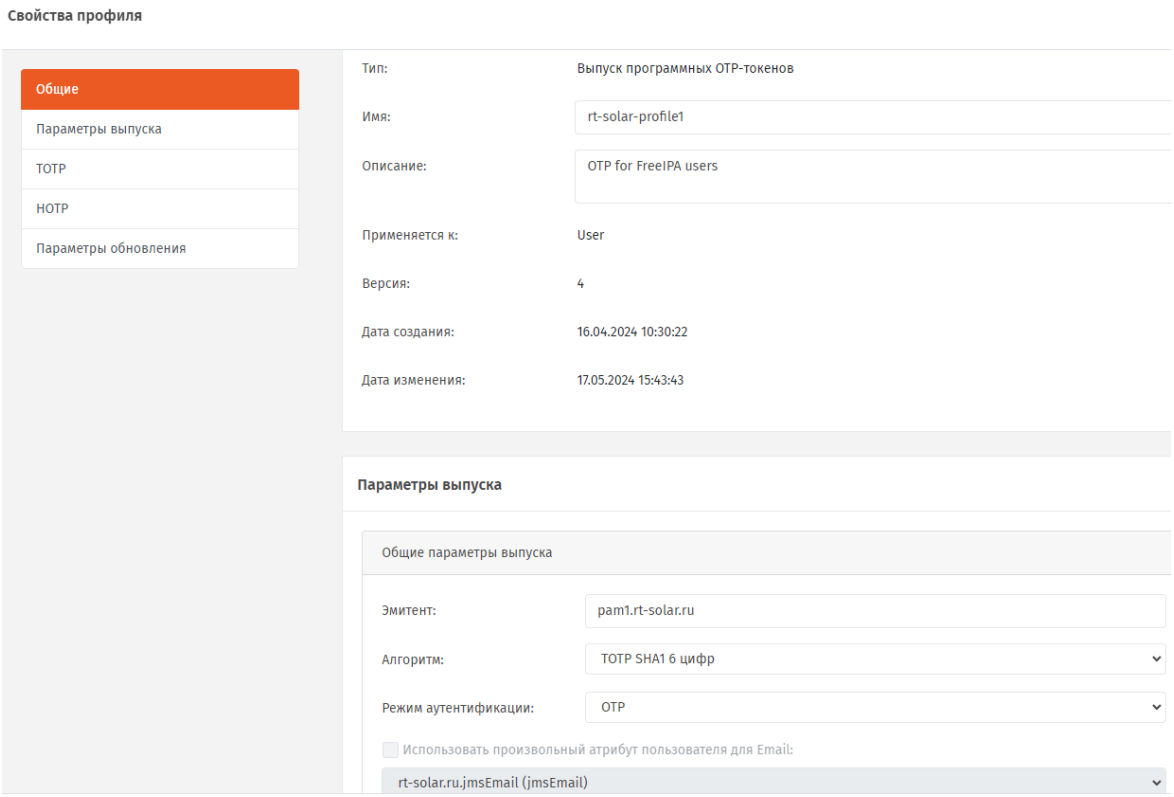


Рис. 2.1. Создание профиля выпуска программных OTP-токенов

2. Зарегистрировать пользователя (пользователей) (стр. 15 JMS-4LX Руководства администратора ч. 2).

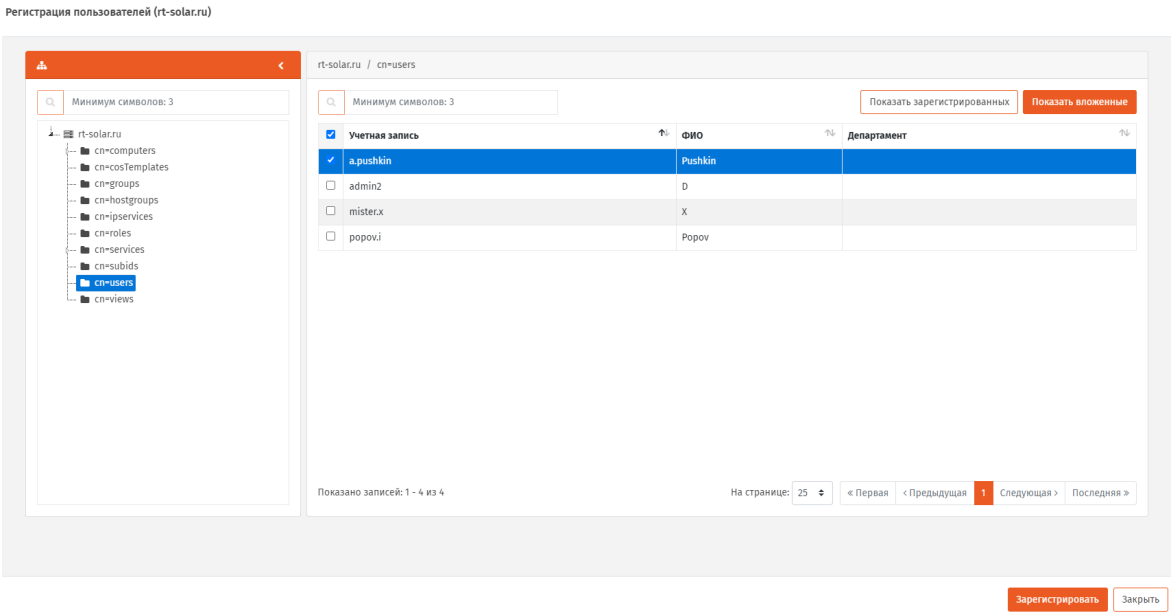


Рис. 2.2. Регистрация пользователей

Внимание!

У пользователя должен быть указан действующий адрес электронной почты

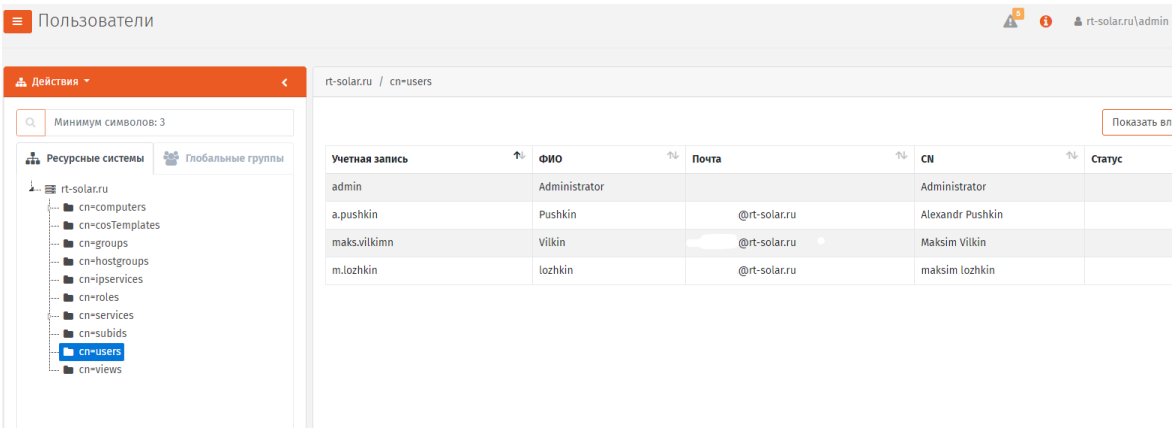


Рис. 2.3. Регистрация пользователей (проверка e-mail)

3. Настроить для выпуска программные OTP-токены.

   Запустить на выполнение соответствующий план обслуживания (разделы **План обслуживания жизненного цикла OTP-токенов** на стр. 283 и **Запуск и просмотр результатов планов обслуживания** на стр. 276 JMS-4LX Руководства администратора ч. 2).

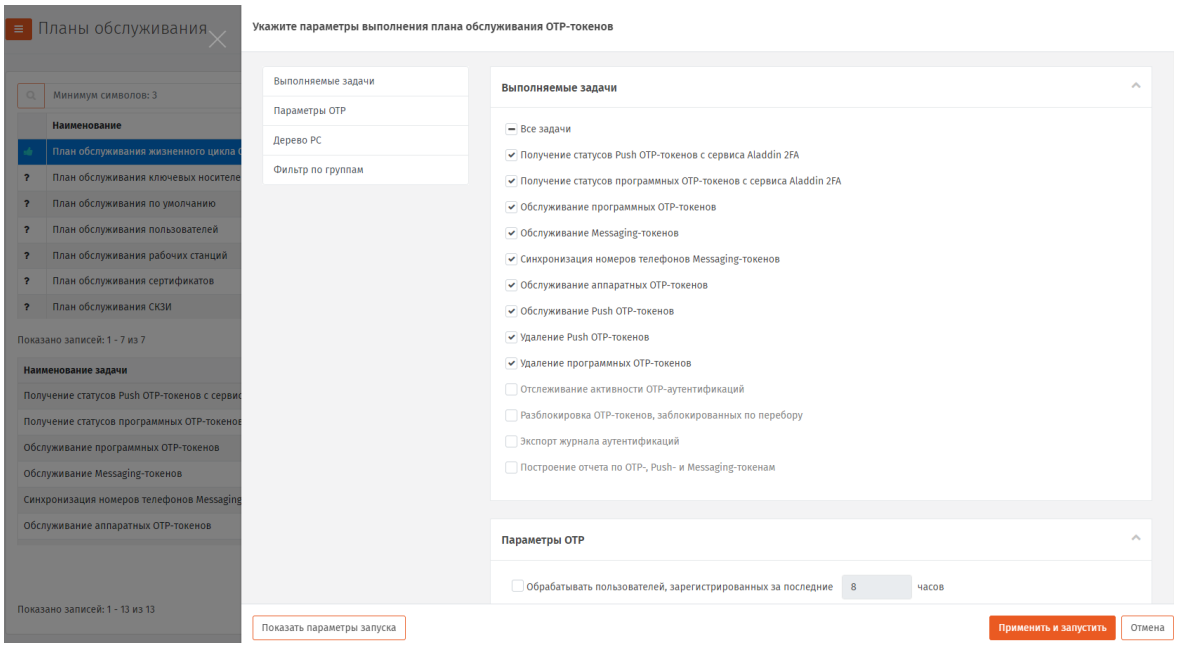


Рис. 2.4. Настройка OTP-токенов

4. Выпущенные и готовые к использованию (статус **Используется**) экземпляры программных OTP-токенов отобразятся в консоли управления JMS со значением SoftwareOTP в поле Модель.

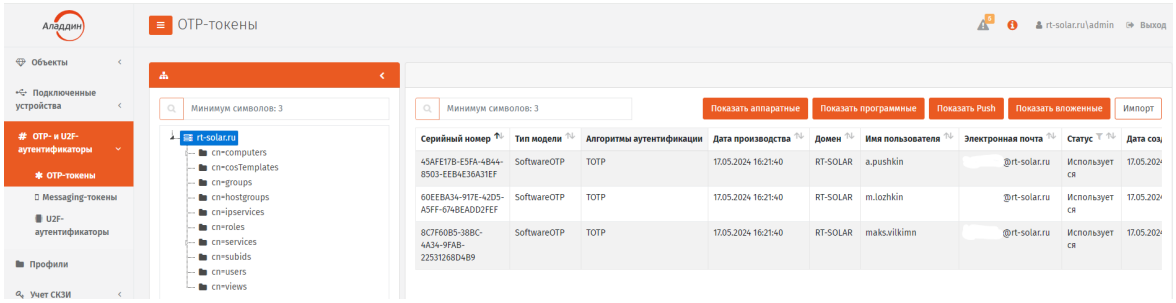


Рис. 2.5. Выпущенные OTP-токены

Пользователи, для которых были выпущены токены, получат на свой электронный адрес сообщение, содержащее PIN для OTP и QR-код.

Subject: [JMS] Регистрация программного OTP-токена

Уважаемый пользователь a.pushkin,

Программный OTP-токен с серийным номером 'XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX' был успешно зарегистрирован.

OTP PIN-код не был назначен.

Код для регистрации:



Если не удается отсканировать штрихкод добавьте его вручную.
Укажите адрес электронной почты и этот секретный код:

Рис. 2.6. Сообщение, содержащее PIN для OTP и QR-код

Пользователь с помощью своего мобильного устройства, на котором установлено необходимое приложение (например, мобильное приложение Aladdin 2FA компании Аладдин), должен отсканировать QR-код, после чего он сможет генерировать значения OTP.

3. Настройка JAS RADIUS SERVER JRS

Примечание

С полным описанием настройки можно ознакомиться в документе JRS Руководство Администратора.pdf.

Ниже приведен пример конфигурации **/etc/aladdin/jas-radius-server/config.json**:

```
{
 "InboundInterface": "*:1812",
 "OutboundInterface": "*",
 "JasServiceUri": "http://localhost:8221/api/v4.1",
 "JasAuthType": "None",
 "JasUsername": "",
 "JasPassword": "O3nMDlBrc5LwBn+Fn444=",
 "JasTimeout": 50000,
 "DefaultUserDomain": "rt–solar.ru",
 "LdapConnections": [
  {
   "DomainName": "rt–solar.ru",
   "LdapServerUri": "ldap://ipa1.rt–solar.ru",
   "LdapServerUsername": "uid=admin,cn=users,cn=accounts,dc=rt–solar,dc=ru",
   "LdapServerPassword": "PgKBeHVABc=",
   "LdapType": "FreeIPA"
  }
 ],
 "ChallengeResponseRadiusAuth": true,
 "SecondFactorAuthFirst": false,
 "AllowChangeExpiredPassword": true,
 "CheckPasswordAgainstExternalRadiusServer": false,
 "ExternalRadiusServer": "10.68.14.201:1812",
 "ExternalRadiusServerSharedSecret": " 982lU3TNqbxHzM8D8=",
 "ExternalRadiusServerRetryCount": 3,
 "ExternalRadiusServerRetryDelay": 1000,
 "ExternalRadiusServerTimeout": 50000,
 "UserNotFoundAction": "Pass",
 "TokensNotFoundAction": "Reject",
 "CheckA2faTokenState": true,
 "A2faNotActivatedAction": "Reject",
 "AuthTypes": "OTP",
 "AuthTypeSelection": "Auto",
 "MessagingAdditionalInfo": "",
 "MessagingSystemId": "",
 "MessagingRetryDelay": 5000,
 "MessagingTtl": 180,
 "ReplyMessageCodePage": 65001,
 "Culture": "ru",
 "Clients": [
  {
   "RadiusClientAddress": "172.20.14.183",
   "RadiusClientName": "safeconnect",
   "RadiusClientSharedSecret": "ieQLECZ5XjyRlU7k0="
  }
 ],
```

```
  "Localization": {
    "Select2FAMessage": "Выберите второй фактор: ",
    "OtpCodeMessage": "Введите OTP–код",
    "SMSCodeMessage": "Введите код из SMS",
    "SMSCodeMessageWithAttempts": "Введите код из SMS. Осталось попыток: ",
    "ExpiredPasswordMessage": "Срок действия пароля учетной записи истек. Смените пароль или
 обратитесь к администратору",
    "NewPasswordNotMatchMessage": "Введенные пароли не совпадают",
    "NewPasswordComplexityMessage": "Пароль не соответствует требованиям сложности. Если
Вы не знаете требования к сложности пароля, обратитесь к администратору",
    "NewPasswordExpiredMessage": "Пароль пользователя истек. Введите новый пароль",
    "ConfirmPasswordMessage": "Подтвердите новый пароль",
   "MaxAttemptsExceededMessage": "Превышено максимальное количество попыток смены пароля",

    "OtpName": "OTP",
    "MessagingName": "Messaging",
    "PushName": "Push"
  },
  "HealthCheckConfig": {
    "Interfaces": "http://*:9999"
  }
}
```

После применения конфигурации сервер готов к работе.

Далее необходимо перейти к настройке SafeConnect.

4. Настройка 2FA доступа к системе SafeConnect

Для настройки 2FA доступа к системе SafeConnect необходимо:

1. С правами администратора SafeConnect перейти в раздел **Настройки**.
2. Перейти на вкладку **Серверы RADIUS**.
3. Нажать кнопку **Добавить**.
4. Задать IP-адрес сервера RADIUS.
5. Выбрать назначение **2FA доступ к SafeConnect**.
6. Ввести и подтвердить пароль.
7. Подтвердить пароль.
8. Сохранить настройки.

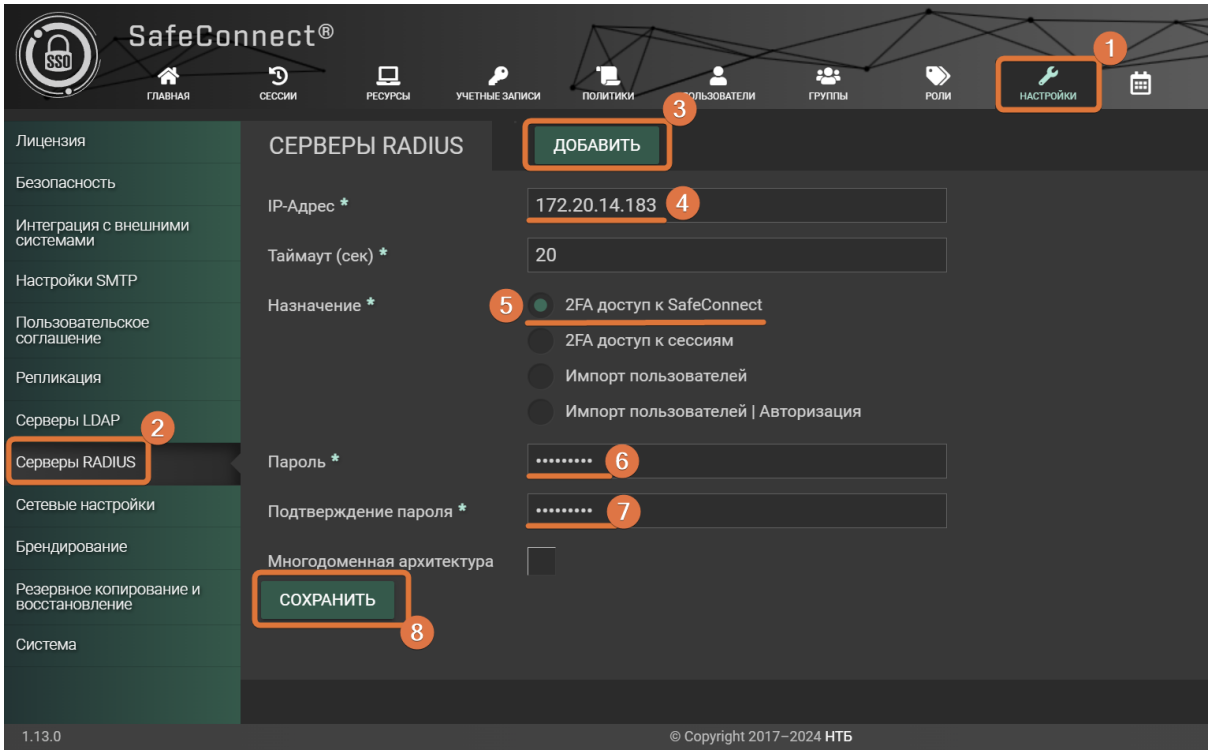


Рис. 4.1. Настройка доступа 2FA к системе

Теперь можно проверить 2FA-доступ к порталу.

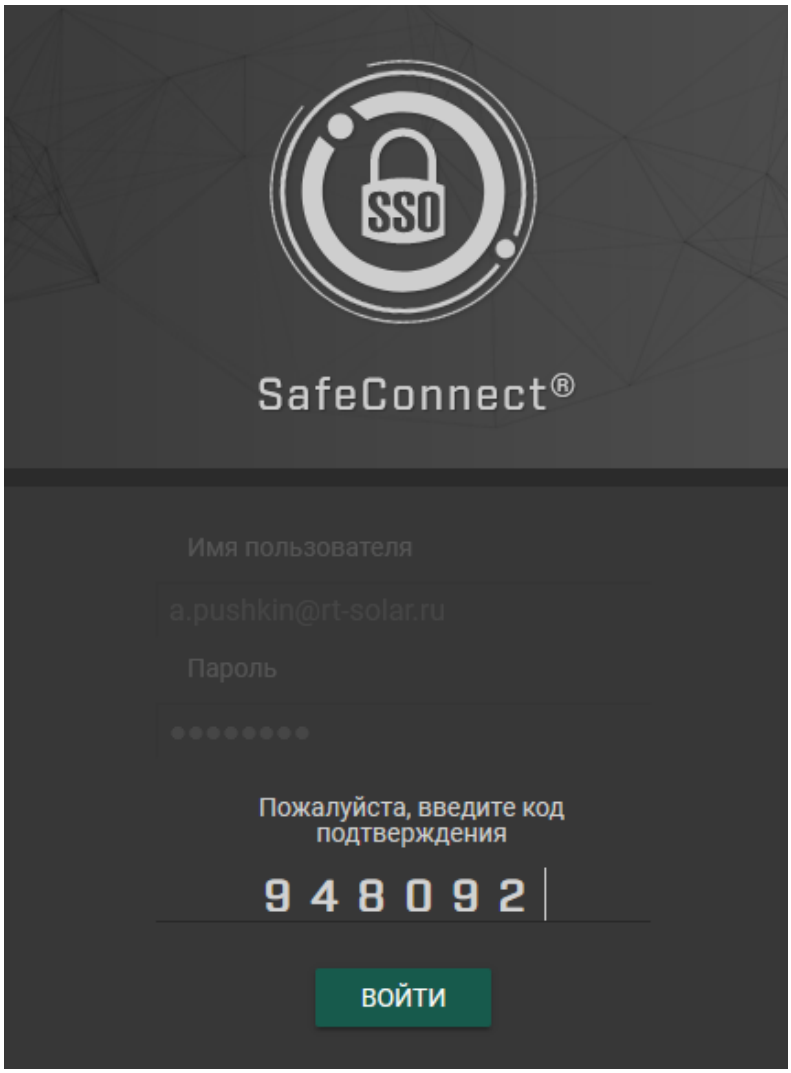


Рис. 4.2. Настроенный доступ 2FA к системе