



JaCarta Virtual Token

Руководство администратора

Версия продукта	1.1
Статус	Публичный
Дата	17.07.2024
Листов	69

Оглавление

1. О документе.....	4
1.1 Назначение документа.....	4
1.2 На кого ориентирован документ.....	4
1.3 Обозначения и сокращения.....	4
2. Общие сведения	5
2.1 Назначение продукта.....	6
2.2 Системные требования	6
2.3 Описание пакетов установки.....	7
3. Сервер JaCarta Virtual Token. Установка и настройка	9
3.1 Установка Сервера JaCarta Virtual Token на ОС Linux	9
3.2 Конфигурация Сервера JaCarta Virtual Token.....	9
3.3 Структура портов	10
3.3.1 Основные порты	11
3.3.2 Специальные порты.....	11
3.4 Установка лицензии	12
3.5 Запуск Сервера JaCarta Virtual Token с помощью утилиты systemctl.....	12
4. Административная консоль. Настройка и работа	13
4.1 Настройка административной веб-страницы	13
4.1.1 Настройка доступа к административной веб-странице	13
4.1.2 Настройка отображения истекающих/истекших серийных номеров	14
4.1.3 Настройка шаблона электронного письма.....	14
4.1.4 Настройка SMTP-сервера	15
4.1.5 Возможность изменения e-mail владельца серийного номера	15
4.1.6 Отображение QR-кода регистрации серийного номера в интерфейсе административной консоли	16
4.2 Работа в административной консоли.....	16
4.2.1 Регистрация суперпользователя.....	16
4.2.2 Создание пользователя	17
4.2.3 Роли учётных записей. Создание и редактирование	19
4.2.4 Первый вход в административную консоль.....	21
4.2.5 Вход в административную консоль.....	22
4.2.6 Сброс второго фактора.....	23
4.2.7 Сброс пароля и второго фактора Администратором.....	26
4.2.8 Смена пароля пользователем	27
4.2.9 Удаление пользователя	28
4.2.10 Автоматические уведомления	28
4.2.11 Подтверждение действий с помощью OTP-кода.....	29
4.2.12 Работа с серийными номерами.....	29
4.2.13 Генерация серийного номера	35
5. Клиент JaCarta Virtual Token. Установка и настройка	43
5.1 Настройка конфигурации.....	43
5.1.1 Создание конфигурационного файла.....	43
5.1.2 Обновление конфигурационного файла	44
5.1.3 Перезапись конфигурационного файла	45
5.2 Клиент JaCarta Virtual Token на ОС Windows.....	47
5.2.1 Установка JaCarta Virtual Token	47
5.2.2 Удаление Клиента JaCarta Virtual Token	50
5.2.3 Обновление Клиент JaCarta Virtual Token	50
5.2.4 Сбор логов.....	51

5.2.5	Прокси-соединение.....	51
5.3	Клиент JaCarta Virtual Token на ОС Linux.....	57
5.3.1	Установка JaCarta Virtual Token ОС Linux.....	57
5.3.2	Удаление Клиента JaCarta Virtual Token	59
5.3.3	Обновление Клиента JaCarta Virtual Token.....	59
5.3.4	Сбор логов.....	59
Приложение А. Пример конфигурационного файла config.yaml!		61
Контакты		67
	Офис (общие вопросы)	67
	Техническая поддержка.....	67
Список литературы		68
Регистрация изменений		69

1. О документе

1.1 Назначение документа

Настоящий документ представляет собой описание операций по установке и настройке серверного приложения JaCarta Virtual Token.

1.2 На кого ориентирован документ

Документ предназначен для администраторов, осуществляющих установку и настройку ПО JaCarta Virtual Token.

1.3 Обозначения и сокращения

- APDU (Application Protocol Data Unit)-команда – команда, используемая для обмена данными между картами и устройствами чтения карт. Служит для выполнения операций чтения и записи данных на карте, аутентификации, проверки пароля;
- SQLite, MSSQL, Postgresql – встраиваемая СУБД;
- Виртуальный токен – установленное на смартфон мобильное приложение, которое содержит апплеты, реализующие криптографические механизмы;
- Токен – аппаратное или/и программное устройство, предназначенное для обеспечения информационной безопасности и используемое для идентификации его владельца;
- Дистрибутив – форма распространения программного обеспечения, обычно содержащая программу-установщик (для выбора режимов и параметров установки) и набор файлов, содержащих отдельные части программного средства;
- HTTPS – протокол передачи данных, расширенный поддержкой шифрования в целях повышения безопасности;
- WebSocket – протокол связи поверх TCP-соединения, предназначенный для обмена сообщениями между браузером и веб-сервером в режиме реального времени;
- Аутентификация – процедура проверки подлинности;
- ЭП – электронная подпись.

2. Общие сведения

JaCarta Virtual Token – программное решение, добавляющее в любой смартфон функцию полноценного программного PKI–токена.

Мобильное приложение JaCarta Virtual Token подключается к рабочей станции и реализует функции строгой двухфакторной аутентификации (вход по смарт-карте), усиленной электронной подписи, безопасное хранение ключей шифрования и других пользовательских данных.

ПО JaCarta Virtual Token включает в себя:

- Мобильное приложение JaCarta Virtual Token – мобильное приложение, которое реализует функции виртуального токена, полностью повторяя функциональность аппаратного. Приложение полностью обратно-совместимо с аппаратным – система будет одинаково работать как с виртуальным токеном на смартфоне, так и с аппаратным USB-токеном или смарт-картой;
- Сервер JaCarta Virtual Token – серверное приложение, которое размещается в инфраструктуре заказчика. Сервер JaCarta Virtual Token позволяет взаимодействовать Мобильному приложению JaCarta Virtual Token и Клиенту JaCarta Virtual Token, на рабочей станции, производя сетевой обмен APDU–командами;
- Клиент JaCarta Virtual Token - приложения для рабочей станции, на которой необходимо использовать виртуальный токен. Приложение позволяет подключить виртуальный токен к рабочей станции, используя для этих целей серверное приложение Сервер JaCarta Virtual Token. Клиент JaCarta Virtual Token состоит из следующих компонент:
 - Драйвер JaCarta Virtual Token – программное обеспечение, позволяющее получать доступ к аппаратному обеспечению рабочей станции, на которой установлен Клиент JaCarta Virtual Token;
 - Панель управления JaCarta Virtual Token – панель управления Клиента JaCarta Virtual Token, позволяющая управлять конфигурацией подключения к Серверу JaCarta Virtual Token и регистрацией Мобильного приложения JaCarta Virtual Token на рабочей станции.

Взаимодействие компонентов JaCarta Virtual Token приведено на рисунке ниже (см. Рисунок 1).

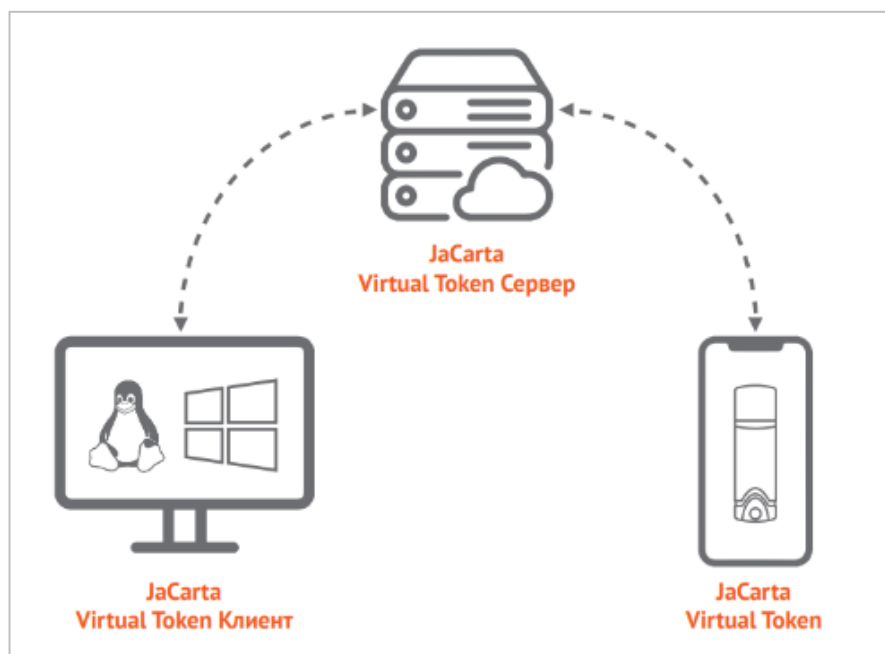


Рисунок 1 – JaCarta Virtual Token. Архитектура решения

Для взаимодействия Мобильного приложения JaCarta Virtual Token и Клиента JaCarta Virtual Token и для выстраивания защищённого канала между ними, на Сервере JaCarta Virtual Token предусмотрено два интерфейса:

- HTTPS;
- WebSocket;

HTTPS интерфейс предназначен для обработки запросов на регистрацию Мобильного приложения JaCarta Virtual Token и Клиента JaCarta Virtual Token на Сервере JaCarta Virtual Token.

WebSocket интерфейс предназначен для выстраивания защищённого канала соединения между Мобильным приложением JaCarta Virtual Token и Клиентом JaCarta Virtual Token. Данный интерфейс предназначен для передачи данных и APDU-команд.

Мобильное приложение JaCarta Virtual Token соединяется с Клиентом JaCarta Virtual Token через Сервер JaCarta Virtual Token по WebSocket интерфейсу. Все взаимодействия происходит в рамках операций и APDU-команд.

Установка и настройка JCVT осуществляется в два этапа. Для начала необходимо настроить Сервер JaCarta Virtual Token. Подробное описание процесса установки приведено в п.3. Сервер JaCarta Virtual Token. Установка и настройка.

На втором этапе работы нужно установить и настроить Клиент JaCarta Virtual Token. Описание процесса конфигурации приведено в п.4.

2.1 Назначение продукта

JaCarta Virtual Token позволяет заменить аппаратные PKI-токены, там, где это необходимо, без дополнительных затрат – решение не требует интеграции и уже имеет полную совместимость со всеми сценариями, доступными аппаратным PKI-токенам. Подключённый к рабочей станции виртуальный токен будет восприниматься системой как уже знакомый ей аппаратный.

Примеры использования JaCarta Virtual Token:

- Аутентификация в доменную учётную запись Windows и Linux с использованием сертификата;
- Аутентификация по сертификату на удалённых рабочих станциях и удалённых виртуальных машинах, даже на тех, на которые невозможно пробросить аппаратный токен;
- Аутентификация в VPN-клиентах с использованием сертификата;
- Корпоративная ЭП в электронной почте и шифрование писем;
- Аутентификация в личном кабинете клиента банка или на портале электронного документооборота, ЭП банковских поручений или документов в рамках документооборота.

2.2 Системные требования

Системные требования, необходимые для установки Сервера JaCarta Virtual Token и Клиента JaCarta Virtual Token, приведены ниже (см. Таблица 1).

Таблица 1 – Требования к среде функционирования

Параметр	Значение
Сервер JaCarta Virtual Token	
Операционная система	Microsoft Windows
	Ubuntu 22
	РЕД ОС 7.3.2

Astra Linux 1.7.3	
Сервер СУБД	MSSQL Postgresql
Процессор	4 ядра
Оперативная память (не менее)	8 Гб
Сетевой адаптер	100 Мб/с
Свободное место на жёстком диске (не менее)	25 Гб

Клиент JaCarta Virtual Token

Операционная система	Windows 10, 11 RedOs 7.3.2 Astra Linux 1.7.3
----------------------	----------------------------------------------------

2.3 Описание пакетов установки

Дистрибутив JaCarta Virtual Token включает следующие пакеты установки и обновления (см. Таблица 2 и Таблица 3):

Сервер JaCarta Virtual Token

Таблица 2 – Виды установочного файла Сервера JaCarta Virtual Token, в зависимости от ОС

ОС	Установочный файл	Зависимости
RedOS	jcvt-server_x.x.x.x_x64.rpm	pcsc-lite ccid
Ubuntu Astra Linux	jcvt-server_x.x.x.x_x64.deb	libccid pcscd

Клиент JaCarta Virtual Token

Таблица 3 – Виды установочного файла Клиента JaCarta Virtual Token, в зависимости от ОС

ОС	Установочный файл	Зависимости
Windows	JaCartaVirtualToken-x64-x.x.x.x.msi	—
RedOS	JaCartaVirtualToken-x64-x.x.x.x.rpm	pcsc-lite ccid
Ubuntu Astra Linux	JaCartaVirtualToken-x64-x.x.x.x.deb	libccid pcscd

Подробнее про настройку и работу мобильного приложения JaCarta Virtual Token приведено в документе [1] «JaCarta Virtual Token. Руководство пользователя».

3. Сервер JaCarta Virtual Token. Установка и настройка

Сервер JaCarta Virtual Token – серверное приложение, располагаемое в инфраструктуре заказчика. Сервер JaCarta Virtual Token позволяет взаимодействовать Мобильному приложению JaCarta Virtual Token и Клиенту JaCarta Virtual Token, на рабочей станции, производя сетевой обмен APDU–командами.

3.1 Установка Сервера JaCarta Virtual Token на ОС Linux

Для установки Сервер JaCarta Virtual Token через командную строку следует:

1. Открыть командную строку;
2. Перейти в каталог с установочным файлом и установить его, выполнив команду:
 - для дистрибутивов RedOS:

```
sudo yum install jcvt-server_ x.x.x.x_x64.rpm
```

- для дистрибутивов Ubuntu, Astra Linux:

```
sudo apt-get install -f jcvt-server_ x.x.x.x_x64.deb
```

Если данный способ установки не получился, то выполните следующую команду:

```
sudo apt --fix-broken install jcvt-server_ x.x.x.x_x64.deb
```

В случае необходимости установить последнюю версию репозитория вручную, с инструкцией можно ознакомиться, перейдя по этой [ссылке](#).

Для самостоятельной установки необходимых библиотек, их можно найти по этой [ссылке](#).

3.2 Конфигурация Сервера JaCarta Virtual Token

По умолчанию в каталоге `/etc/jcvt-server/` будут созданы файл конфигурации `config.yaml` и файл с вариантами настройки сервера `config_example.yaml`.

С помощью текстового редактора (например, nano) изменить конфигурационный файл `config.yaml`.

В поле `externalAddress` в разделе `apiServer` необходимо указать адрес сервера, к которому будут обращаться клиенты.

Пример файла `config.yaml` для работы с БД SQLite и настройками TLS с использованием контейнера PFX для `apiServer` и `transportServer` приведён ниже:

```
# Конфигурация базы данных
database:
  # Тип БД
  type: sqlite
  # Подключаемая БД
  path: /etc/jcvt-server/jcvt.db
# Конфигурация api-сервера
apiServer:
  # Адрес сервера, к которому будут обращаться клиенты.
  # Это может быть, как адрес сервера, так и адрес прокси-сервера.
```

```
# Этот адрес будет добавляться в QR-код.
externalAddress: https://jcvrt.a-rd.ru

# Адрес запуска сервера
# address: "localhost:6788" # полный адрес
address: ":9001" # только порт
tls:
  pfx:
    pfxContainer: /home/debian/trustedcert.pfx
    pwdContainer: "X5553535"

# Конфигурация websocket-сервера
transportServer:
  # Адрес запуска сервера
  # address: "localhost:6789" # полный адрес
  address: ":9000" # только порт
  tls:
    pfx:
      pfxContainer: /home/debian/horizon_key.pfx
      pwdContainer: "X5553535"
```

3.3 Структура портов

На рисунке ниже (см. Рисунок 2) приведена схема взаимодействия интерфейсов и соответствующих им портов.

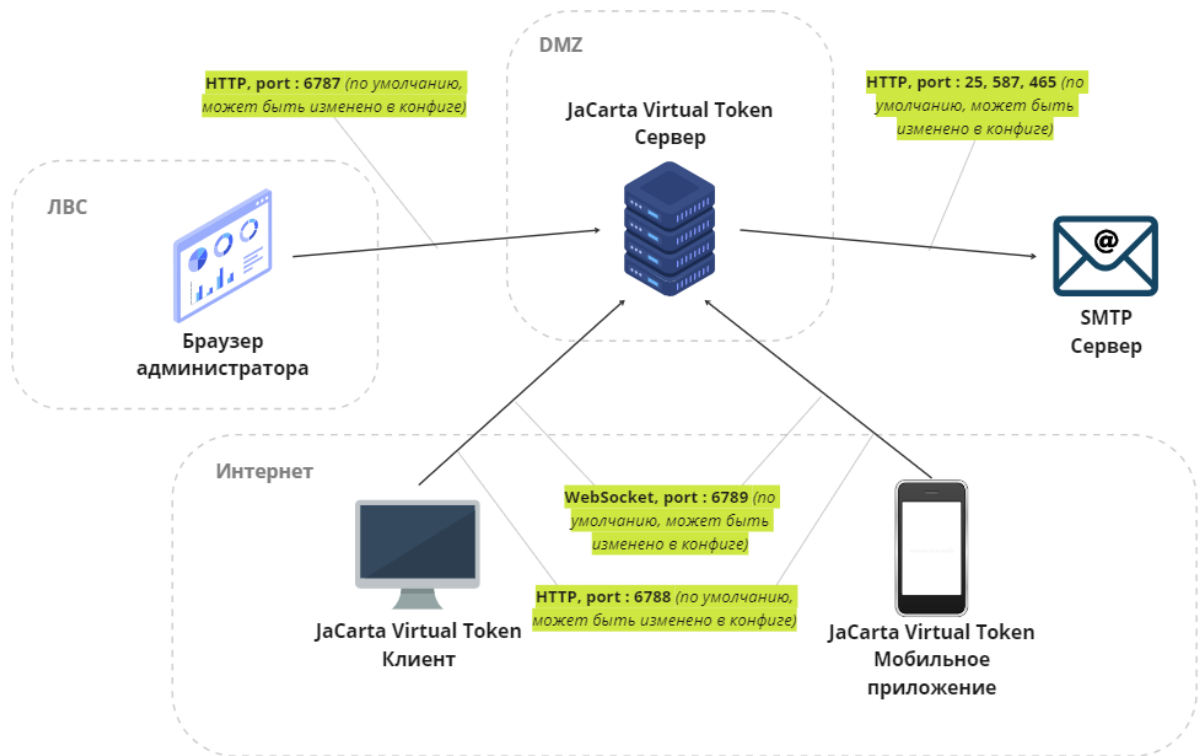


Рисунок 2 – Структура портов

3.3.1 Основные порты

Основные порты сервера JaCarta Virtual Token используются для ряда компонент, входящих в состав сервера.

Описание основных портов:

- Private Server – интерфейс консоли администратора. По умолчанию используется порт 6787. Настраивается в файле конфигурации сервера;
- API Server – интерфейс для HTTP-соединений. Адрес сервера, к которому будут обращаться клиенты. Это может быть, как адрес сервера, так и адрес прокси-сервера. По умолчанию, используется порт 6788. Настраивается в файле конфигурации сервера;
- Transport Server – интерфейс для WebSocket-соединений. Адрес сервера, к которому будут обращаться клиенты. Это может быть, как адрес сервера, так и адрес прокси-сервера. По умолчанию используется порт 6789. Настраивается в файле конфигурации сервера;
- SMTP Server – интерфейс для отправки e-mail, используя SMTP-сервер. По умолчанию используются порты 25, 587, 465. Настраивается в файле конфигурации сервера.

3.3.2 Специальные порты

У Сервера JaCarta Virtual Token имеется несколько технически занятых портов, которые выполняют различные функции – специальные порты. Рекомендуется не закрывать специальные порты, чтобы не происходило сбоев работы какой-либо функции. Порты не связаны с самим Сервером JaCarta Virtual Token, а занимают их различные компоненты Клиента JaCarta Virtual Token.

Описание специальных портов:

- JaCarta Virtual Token Discovery UDP 8517 – этот порт используется мобильными приложениями для поиска драйвера и работает в офлайн-режиме;

- JaCarta Virtual Token Local Server TCP 8520 – этот порт предназначен для локального сервера драйвера в офлайн-режиме;
- JaCarta Virtual Token Control Service 8515 – этот порт служит для взаимодействия между компонентами драйвера.

Рекомендуется не выключать специальные порты, так как это может привести к некорректной работе ПО JaCarta Virtual Token или полной неработоспособности системы

3.4 Установка лицензии

В директории `/etc/jcvt-server/` необходимо создать папку `licence` и скопировать туда файл лицензии.

3.5 Запуск Сервера JaCarta Virtual Token с помощью утилиты `systemctl`

После настройки конфигурационного файла и установки лицензии можно переходить к запуску сервера. С помощью утилиты `systemctl` запустить сервер:

```
sudo systemctl start jcvt-server
```

Проверить работу сервиса можно с помощью команды:

```
sudo systemctl status jcvt-server
```

Об успешном запуске Сервера JaCarta Virtual Token говорит состояние `active` (см. Рисунок 3).

```
root@debian:/etc/jcvt-server# sudo systemctl status jcvt-server
• jcvt-server.service - JaCarta Virtual Token Server
  Loaded: loaded (/lib/systemd/system/jcvt-server.service; disabled; vendor preset: enabled)
  Active: active (running) since Tue 2022-06-28 12:15:43 MSK; 2h 0min ago
```

Рисунок 3 – JaCarta Virtual Token. Просмотр статуса Сервера JaCarta Virtual Token

4. Административная консоль. Настройка и работа

4.1 Настройка административной веб-страницы

4.1.1 Настройка доступа к административной веб-странице

Настройка административной веб-страницы осуществляется с помощью добавления в конфигурационный файл следующего фрагмента кода:

```
privateServer:

# Адрес запуска сервера. Если не указан - сервер не будет запускаться
# address: "localhost:6787" # полный адрес
address: ":6787" # только порт

# Язык возвращаемых ошибок: ru/en. По умолчанию: en
errorLanguage: ru

# Логин/пароль для доступа к серверу. Если не указано - без авторизации
#login: login
#password: password

# Настройки TLS
# tls:

# # Вариант 1. TLS с использованием сертификата и закрытого ключа
# cert:

# # Путь до сертификата
# certificate: ../wks218.aladdin.ru.crt
# #certificate: ../wks218-root.crt
# #certificate: ../trustedcert.crt

# # Путь до закрытого ключа
# privateKey: ../wks218.aladdin.ru_pvk.pem
# #privateKey: ../wks218-root_pvk.pem
# #privateKey: ../trustedcert.key

# # Вариант 2. TLS с использованием PFX контейнера
# pfx:

# # Путь до PFX контейнера
# pfxContainer: ../trustedcert.pfx
```

```
# # Пароль от PFX контейнера  
# pwdContainer: "password"
```

где

- `address` - адрес/порт, который будет занимать web-сервер. Если не указан - веб-интерфейсу не будет запускаться;
- `login/password` - логин/пароль для доступа к web-серверу. Если не указаны - доступ к веб-интерфейсу будет предоставляться без авторизации;
- `errorLanguage` - язык возвращаемых ошибок;
- `tls` - настройки TLS.

Пример конфигурационного файла приведен в Приложение А. Пример конфигурационного файла `config.yaml`

4.1.2 Настройка отображения истекающих/истекших серийных номеров

Настройка цветовой дифференциации периода истекающих/истекших серийных номеров в таблице веб-интерфейса JCVT на странице [Статус серийного номера] (см. подробнее п.4.2.12):

```
licensing:  
  ...  
  
  # количество дней до истечения срока действия для индикации желтым цветом  
  snValidToWarningPeriodDays: 14  
  
  # количество дней до истечения срока действия для индикации красным цветом  
  snValidToDangerPeriodDays: 7
```

4.1.3 Настройка шаблона электронного письма

Шаблон электронного письма пользователю, содержащего QR-код, устанавливается автоматически в момент установки Сервера JaCarta Virtual Token. При желании можно поменять шаблон: для этого необходимо открыть файл `sn_qr_code_template.html` (находящийся в папке `/etc/jcvt-server/`) и изменить в нем необходимые поля.

В конфигурационном файле внешний вид электронного письма и параметры его отправки настраиваются в следующих секциях:

```
# Настройки отправки e-mail  
email:  
  
  # Тема письма для отправки QR-кода на активацию серийного номера  
  snQrCodeSubject: "Активация серийного номера JCVT"  
  
  # Путь к файлу с шаблоном письма для отправки QR-кода на активацию  
  серийного номера  
  snQrCodeTemplate: ./sn_qr_code_template.html  
  
  # Размер картинки QR-кода на активацию серийного номера. По умолчанию: 300
```

```
snQrCodeSize: 300
```

4.1.4 Настройка SMTP-сервера

Для того чтобы пользователям отправлялись письма с серийными номерами и уведомлениями, необходимо настроить сервер отправки e-mail.

В конфигурационном файле параметры сервера отправки e-mail настраиваются в следующих секциях:

```
# Настройки сервера отправки e-mail

server:

  # Включить отправки e-mail

  enable: false

  # Использовать TLS. По умолчанию: false

  tls: true

  # Адрес SMTP-сервера

  smtp: smtp.test.ru

  # Адрес отправителя

  #from: jcvт@test.ru

  from: JCVT <jcvт@test.ru>

  # Логин на SMTP-сервере

  login: login

  # Пароль на SMTP-сервере

  password: password
```

Пример конфигурационного файла приведен в Приложение А. Пример конфигурационного файла `config.yaml`

4.1.5 Возможность изменения e-mail владельца серийного номера

В конфигурационном файле есть опция, позволяющая изменять e-mail владельца серийного номера после генерации и регистрации его в системе.

По умолчанию данная опция выключена.

В конфигурационном файле параметр, позволяющий редактировать e-mail владельца серийного номера настраивается в следующей секции:

```
# возможность редактировать e-mail-ы серийных номеров из административного  
интерфейса  
  
snEmailEditAccess: false
```

4.1.6 Отображение QR-кода регистрации серийного номера в интерфейсе административной консоли

В конфигурационном файле есть опция, позволяющая отображать QR-код регистрации серийного номера в интерфейсе.

По умолчанию данная опция выключена.

В конфигурационном файле параметр, позволяющий отображать QR-код регистрации серийного номера в интерфейсе настраивается в следующей секции:

```
# возможность отображения QR-кодов серийных номеров в административном  
интерфейсе  
  
snQrCodeAdminAccess: false
```

4.2 Работа в административной консоли

4.2.1 Регистрация суперпользователя

При первом входе в административную консоль необходимо создать суперпользователя. Это учётная запись администратора, необходимая для корректной работы административной консоли (см. Рисунок 4).

В административной консоли всегда должен быть хотя бы один суперпользователь

Авторизация

Еще нет ни одного пользователя.
Создайте первого пользователя:

Логин (Email):

Пароль: Вставить

Подтвердите пароль:

Создать пользователя

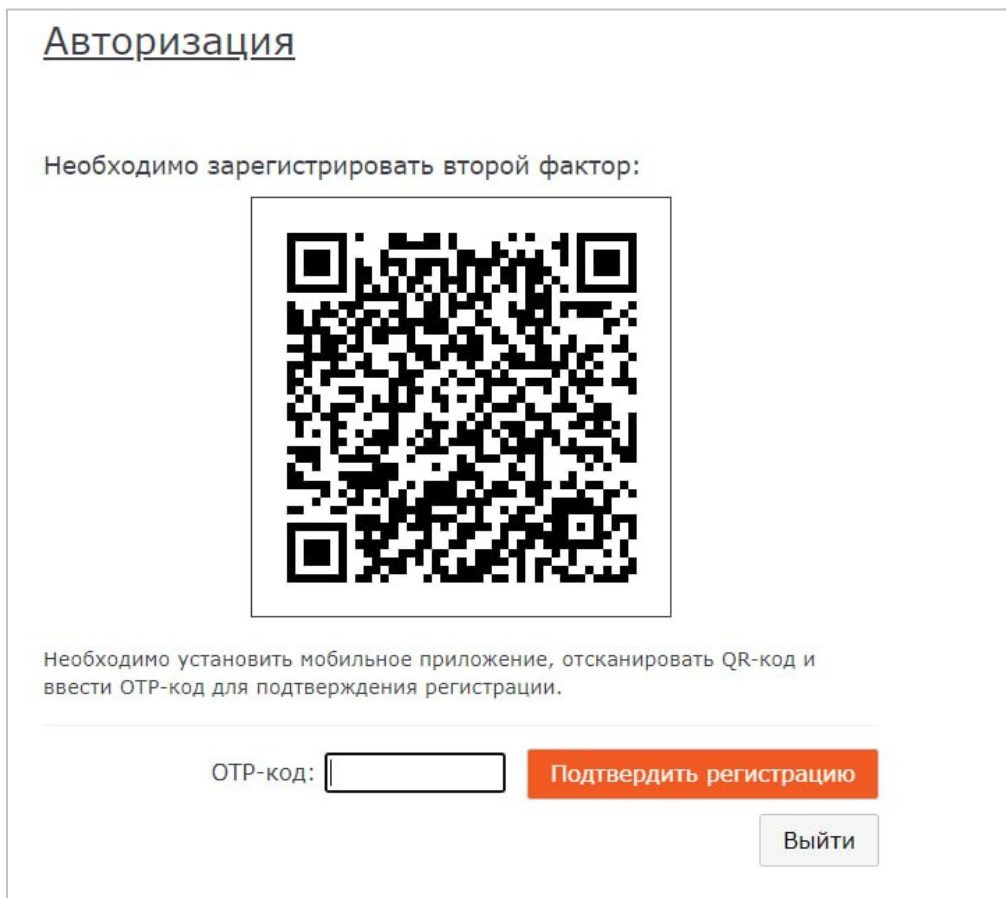
Рисунок 4 – Веб-интерфейс JCVT. Вкладка [Авторизация]. Регистрация суперпользователя.

Для первой авторизации администратору необходимо выполнить следующие действия:

1. Ввести [Логин (Email)] суперпользователя. Поле должно содержать валидный e-mail администратора;


Данный e-mail будет использоваться для дальнейшей авторизации и уведомлений супер-Администратора о ключевых событиях в Административной консоли.

2. Ввести пароль и его подтверждение для суперпользователя в соответствующих полях. Далее отображается QR-код для регистрации второго фактора авторизации (см. Рисунок 5).



Авторизация

Необходимо зарегистрировать второй фактор:



Необходимо установить мобильное приложение, отсканировать QR-код и ввести OTP-код для подтверждения регистрации.

OTP-код:

Подтвердить регистрацию

Выйти

Рисунок 5 – Веб-интерфейс JCVT. Страница [Авторизация]. Регистрация 2FA

Администратору необходимо отсканировать QR-код для регистрации второго фактора аутентификации¹, ввести OTP-код, нажать кнопку <Подтвердить регистрацию>. После этого процедура регистрации считается успешно завершённой. Будет открыта вкладка [Статус серийного номера].

4.2.2 Создание пользователя

Администратор может создать в системе учётные записи пользователей, которые будут иметь доступ к административной консоли, и совершать в ней действия согласно настроенным разрешениям.

Для создания пользователя администратор должен выполнить следующие шаги:

1. В боковом меню выбрать пункт меню [Пользователи] (см. Рисунок 18);
2. Нажать кнопку <Создать пользователя> (см. Рисунок 6);

¹ Рекомендуется использовать решение для PUSH- и OTP-аутентификации [Aladdin2FA](#)

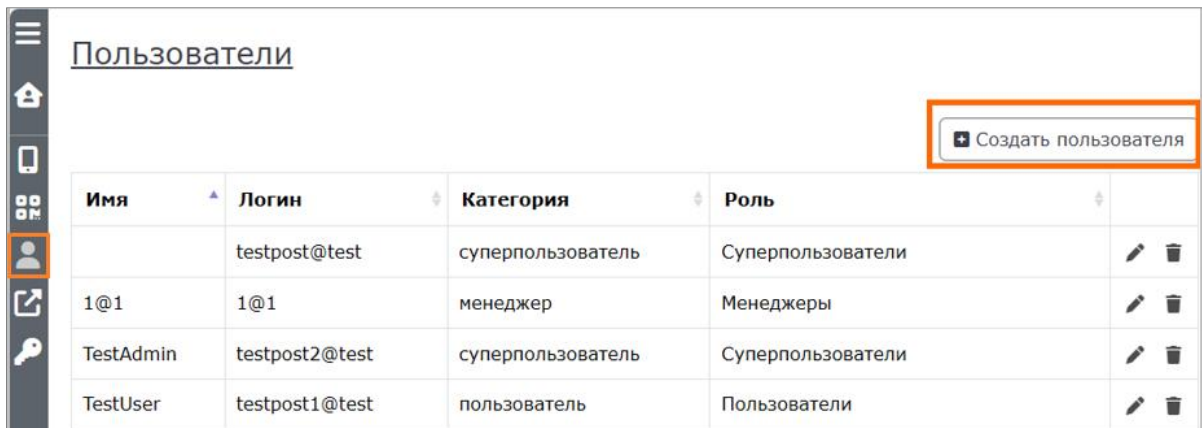


Рисунок 6 – Веб-интерфейс JCVT. Вкладка [Пользователи]. Создание пользователя

3. В окне [Создание пользователя] ввести значения в поля [Имя], [Логин(e-mail)] (см. Рисунок 7) и выбрать <Роль> пользователя в системе (см. Рисунок 8);

Создание пользователя

Имя:

Логин (E-Mail):

Роль:

Рисунок 7 – Веб-интерфейс JCVT. Вкладка [Пользователи]. Окно [Создание пользователя]

Выберите роль:

	Имя	Категория	Назначение	
<input type="radio"/>	Администраторы	администратор	локальная	
<input type="radio"/>	алапапавпапа	пользователь	локальная	
<input type="radio"/>	Менеджеры	менеджер	локальная	
<input checked="" type="radio"/>	Пользователи	пользователь	локальная	
<input type="radio"/>	Суперпользователи	суперпользователь	локальная	

Рисунок 8 – Веб-интерфейс JCVT. Вкладка [Пользователи]. Выбор роли

4. Нажать кнопку «Создать».

Пользователю на указанный электронный адрес будет выслано письмо с уведомлением о созданной учётной записи (см. Рисунок 9).

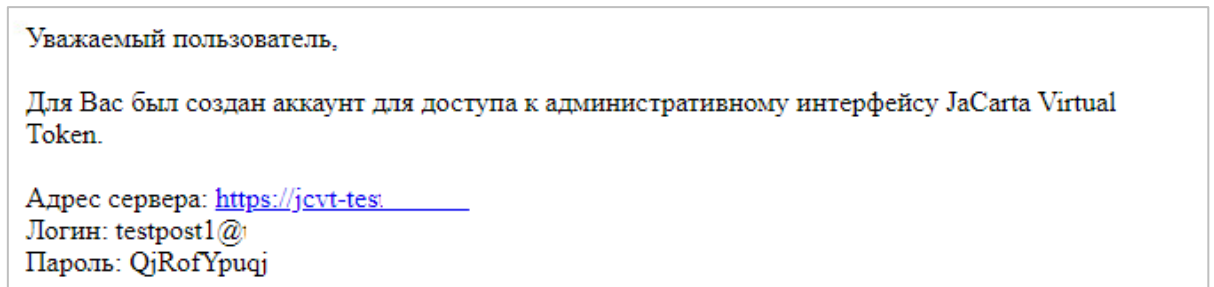


Рисунок 9 – Уведомление пользователю о создании учётной записи

4.2.3 Роли учётных записей. Создание и редактирование

Роли – это разрешения, которые назначаются для учетной записи и позволяют выполнять определенные действия в интерфейсе и получать доступ к определенным функциям административной консоли.

Для создания Роли администратор должен выполнить следующее:

1. В боковом меню выбрать пункт <Роли> (см. Рисунок 10);

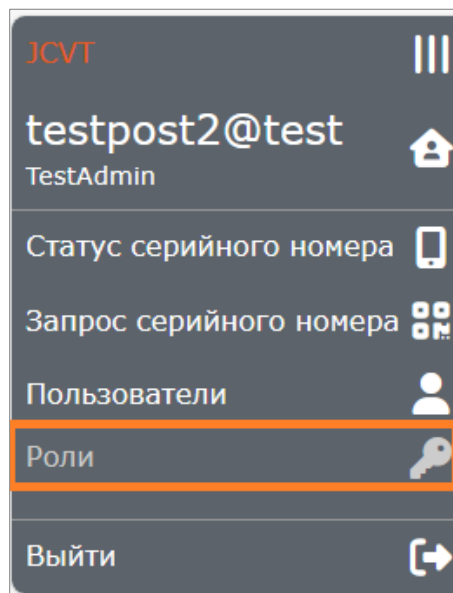


Рисунок 10 – Веб-интерфейс JCVT. Боковое меню - <Роли>

2. На странице ролей нажать кнопку <Создать роль> (см. Рисунок 11);

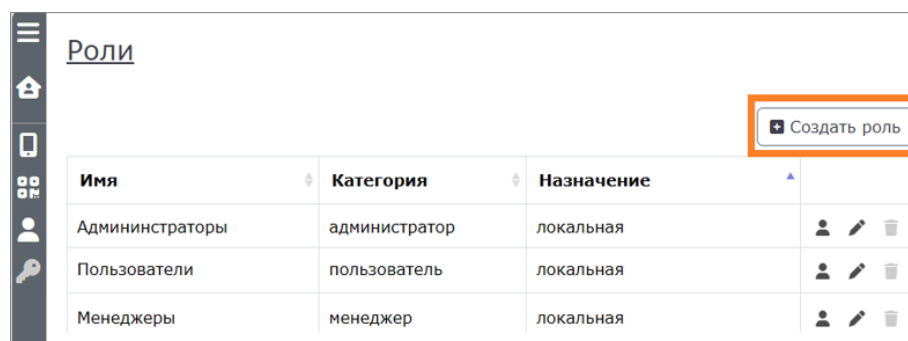


Рисунок 11 – Веб-интерфейс JCVT. Вкладка [Роли]

3. В окне [Создание роли] ввести значения (см. Таблица 4) в полях [Название роли], [Категория], настроить выпадающий список [Назначение], разрешения для групп [Серийные номера], [Лицензии], [Пользователи], нажать кнопку <Создать> (см. Рисунок 12);

Рисунок 12 – Веб-интерфейс JCVT. Окно [Создание роли]

Таблица 4 – Опции настроек роли

Настройка	Описание
Поля	
[Название роли]	Название роли
[Категория]	Преднастроенный набор опций
[Назначение]	Назначение использования роли
Опции	
[Просмотр серийных номеров]	Возможность открытия страницы со списком серийных номеров
[Редактирование серийных номеров]	Возможность редактирования серийных номеров ²
[Деактивация серийных номеров]	Возможность деактивировать серийный номер

² Зависит от настроек сервера. См. 4.1.5

[Выпуск серийных номеров]	Возможность открытия страницы генерации и выпуска серийных номеров
[Просмотр лицензий]	Возможность просмотра информации по лицензиям
[Просмотр пользователей]	Возможность открыть страницу со списком пользователей
[Просмотр ролей]	Возможность открыть страницу со списком ролей
[Управление ролями и пользователями]	Возможность редактирования пользователей и ролей

4.2.4 Первый вход в административную консоль

При первом входе в административную консоль пользователь должен выполнить следующие действия:

1. Ввести значения в полях [Логин] и [Пароль], которые были присланы ему на почту (см. Рисунок 13);

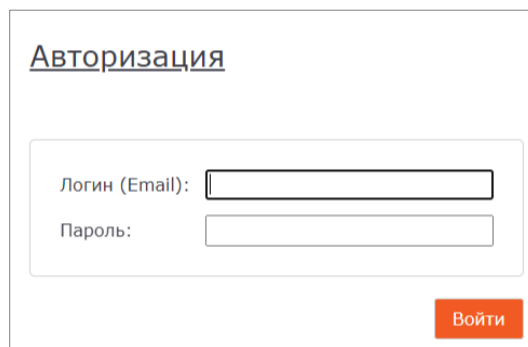


Рисунок 13 – Веб-интерфейс JCVT. Вкладка [Авторизация]. Ввод логина и пароля

2. Сменить автоматически созданный пароль (см. Рисунок 14);

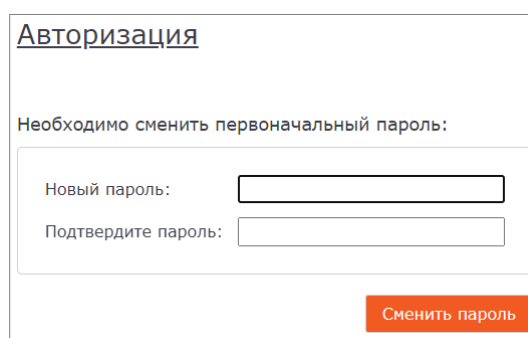


Рисунок 14 – Веб-интерфейс JCVT. Вкладка [Авторизация]. Смена пароля

3. Зарегистрировать второй фактор аутентификации и ввести значение OTP-кода (см. Рисунок 15);

Авторизация

Необходимо зарегистрировать второй фактор:

Необходимо установить мобильное приложение, отсканировать QR-код и ввести OTP-код для подтверждения регистрации.

OTP-код:

Подтвердить регистрацию

Выйти

Рисунок 15 – Веб-интерфейс JCVT. Вкладка [Авторизация]. Регистрация второго фактора

4. После ввода значения OTP-кода процедура регистрации завершена. Будет открыта вкладка [Статус серийного номера].

Если пользователь установил пароль, но не установил второй фактор, то при следующем входе по паролю ему опять отобразится страница с QR-кодом для регистрации второго фактора

4.2.5 Вход в административную консоль

При входе в административную консоль, пользователю необходимо:

1. Ввести значения Логина и Пароля. (См. Рисунок 16);

Авторизация

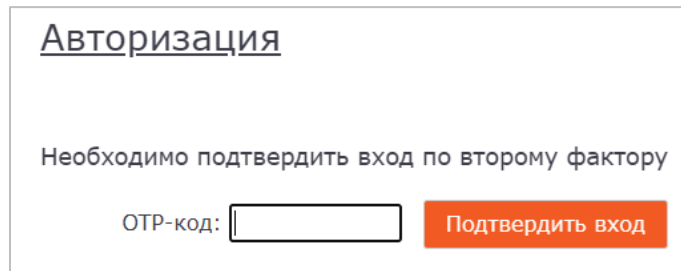
Логин (Email):

Пароль:

Войти

Рисунок 16 – Веб-интерфейс JCVT. Страница [Авторизация]. Ввод Логина и Пароля

2. Ввести значение OTP-кода (см. Рисунок 17);



Авторизация

Необходимо подтвердить вход по второму фактору

ОТР-код: Подтвердить вход

Рисунок 17 – Веб-интерфейс JCVT. Страница [Авторизация]. Ввод ОТР-кода

Процедура авторизации завершена. Открывается страница «Статус серийного номера».

4.2.6 Сброс второго фактора

Сброс второго фактора администратором

Для сброса привязки второго фактора аутентификации Администратор должен:

1. В боковом меню Административной консоли выбрать пункт меню [Пользователи] (см. Рисунок 18);

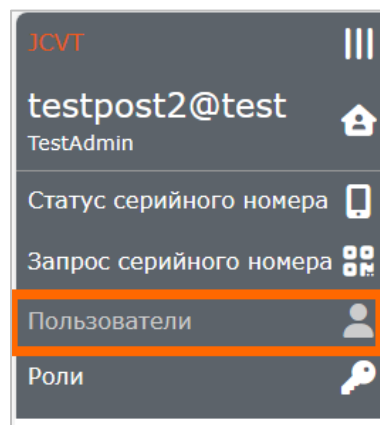
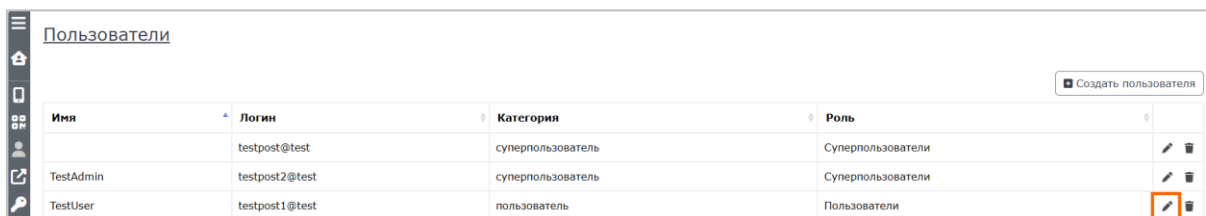


Рисунок 18 – Веб-интерфейс JCVT. Боковое меню - Пользователи

2. Вызвать меню редактирования Пользователя нажав соответствующую кнопку (см. Рисунок 19);



Имя	Логин	Категория	Роль
	testpost@test	суперпользователь	Суперпользователи
TestAdmin	testpost2@test	суперпользователь	Суперпользователи
TestUser	testpost1@test	пользователь	Пользователи

Рисунок 19 – Веб-интерфейс JCVT. Страница Пользователи - Редактирование

3. В меню редактирования Пользователя, выбрать опцию «Сбросить второй фактор» (См. Рисунок 20);

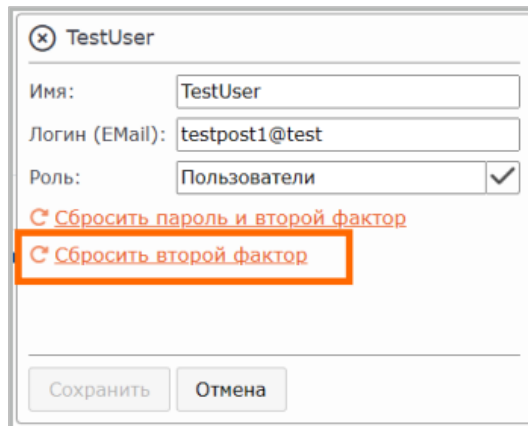


Рисунок 20 – Веб-интерфейс JCVT. Меню редактирования пользователя – сброс 2FA

4. Подтвердить сброс второго фактора во всплывшем окне (см. Рисунок 21);

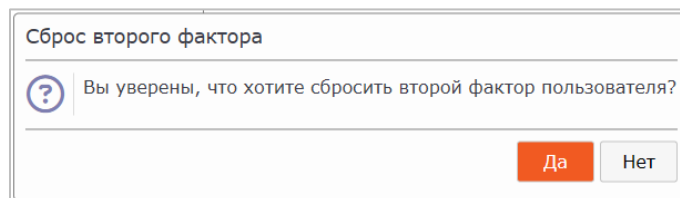


Рисунок 21 – Веб-интерфейс JCVT. Сброс второго фактора. Окно подтверждения

После этого пользователю сбрасывается привязка второго фактора аутентификации. Пользователю, на указанный e-mail, приходит уведомление:

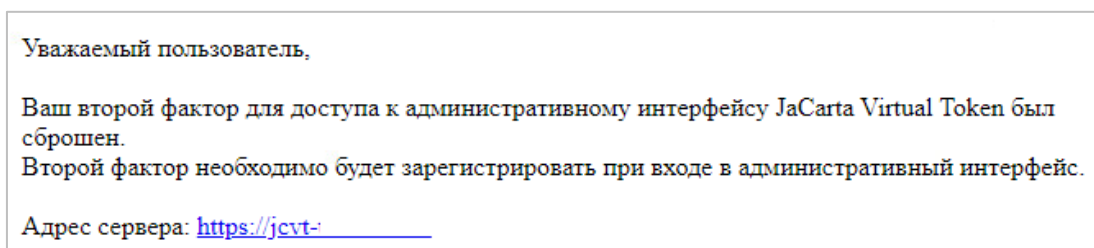


Рисунок 22 – Веб-интерфейс JCVT. Уведомление о сбросе второго фактора

Сброс второго фактора пользователем

Для сброса привязки второго фактора аутентификации Администратор должен:

1. В боковом меню Административной консоли выбрать пункт меню [Профиль] (см. Рисунок 23);

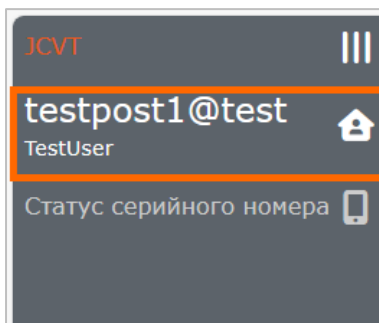


Рисунок 23 – Веб-интерфейс JCVT. Боковое меню – Профиль

2. На странице профиля, выбрать [Сменить второй фактор] (см. Рисунок 24);

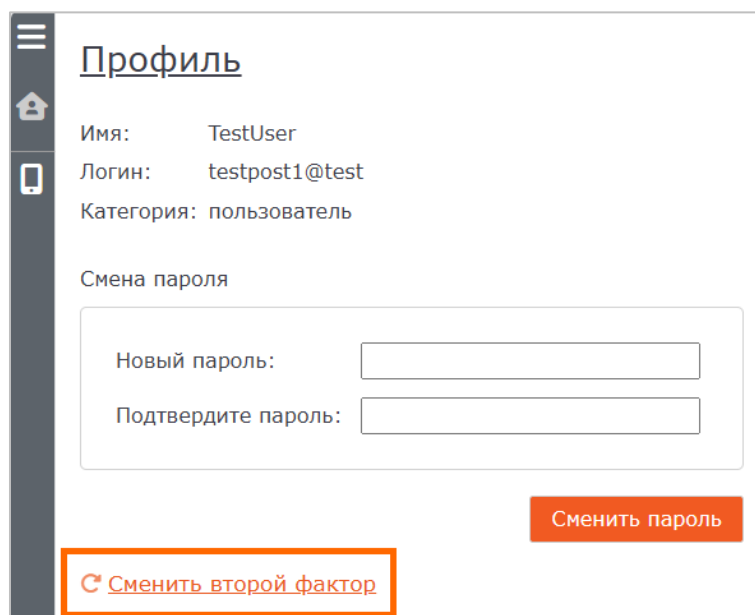


Рисунок 24 – Веб-интерфейс JCVT. Профиль – сброс 2FA

3. Подтвердить действие в окне уведомления (см. Рисунок 21);
4. Зарегистрировать второй фактор аутентификации и ввести значение OTP-кода в открывшемся меню (см. Рисунок 25);

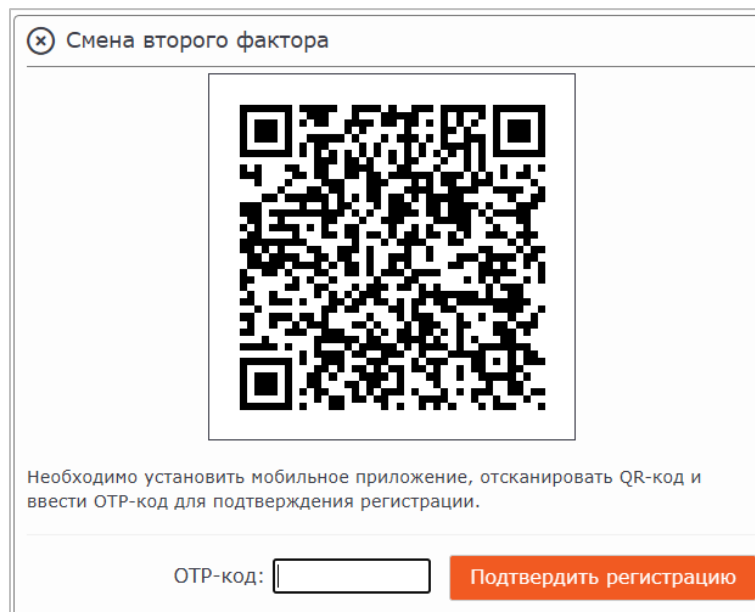


Рисунок 25 – Веб-интерфейс JCVT. Профиль – Смена второго фактора

Если пользователь не установил второй фактор, то при следующем входе по паролю ему опять отобразится страница с QR-кодом для регистрации второго фактора.

4.2.7 Сброс пароля и второго фактора Администратором

Для сброса пароля и привязки второго фактора аутентификации, Администратор должен:

1. В боковом меню Административной консоли выбрать пункт меню [Пользователи] (см. Рисунок 18);
2. Вызвать меню редактирования Пользователя нажав соответствующую кнопку (см. Рисунок 19);
3. В меню редактирования пользователя, выбрать пункт «Сбросить пароль и второй фактор» (см. Рисунок 26);

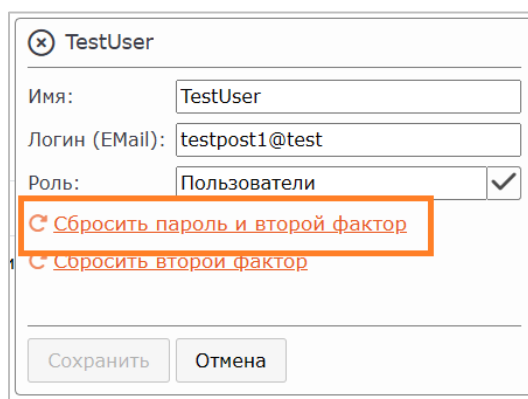


Рисунок 26 – Веб-интерфейс JCVT. Меню редактирования пользователя – сброс пароля и 2FA

4. Подтвердить сброс пароля и второго фактора во всплывшем окне (см. Рисунок 27);

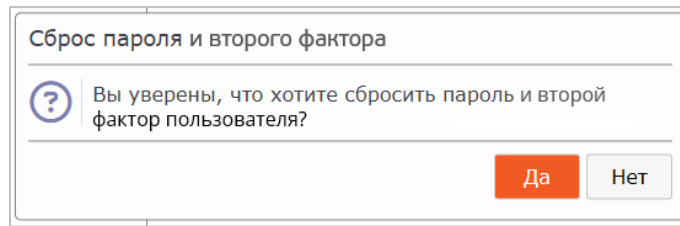


Рисунок 27 – Веб-интерфейс JCVT. Сброс пароля и второго фактора. Окно подтверждения пароль и 2FA

После этого пользователю сбрасывается привязка пароля и второго фактора аутентификации. Пользователю, на указанный e-mail, приходит уведомление:

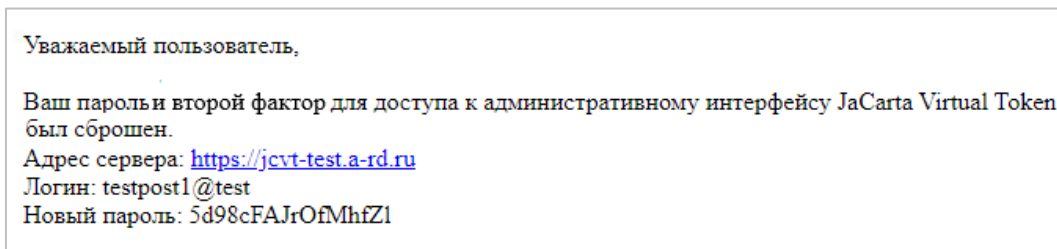


Рисунок 28 – Веб-интерфейс JCVT. Уведомление о сбросе пароля и второго фактора

4.2.8 Смена пароля пользователем

Для смены пароля пользователю необходимо:

1. В боковом меню Административной консоли выбрать пункт меню [Профиль] (см. Рисунок 23);
2. На странице профиля, ввести значение нового пароля и подтвердить его. Нажать кнопку [Сменить пароль] (см. Рисунок 29);

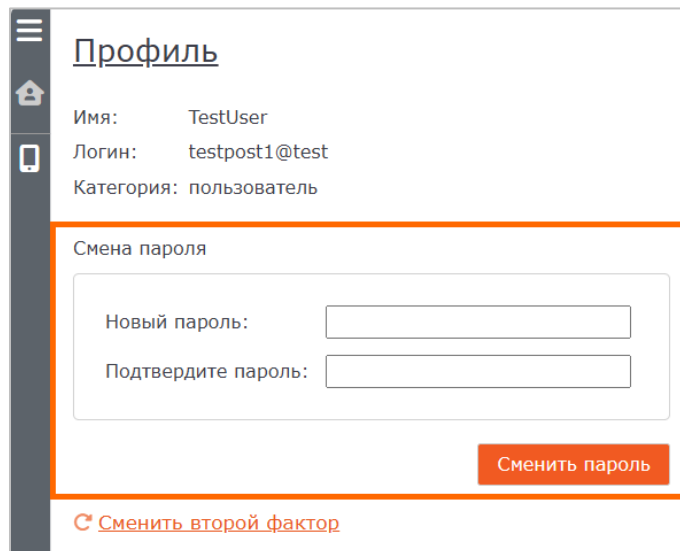
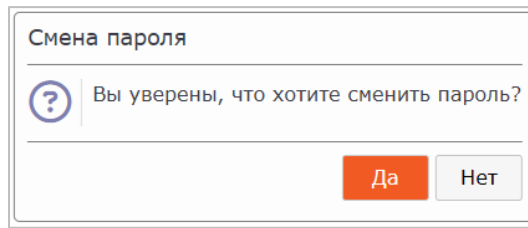


Рисунок 29 – Веб-интерфейс JCVT. Профиль – Смена пароля

3. Подтвердить действие в уведомлении (см. Рисунок 30);



Смена пароля

Вы уверены, что хотите сменить пароль?


Да Нет

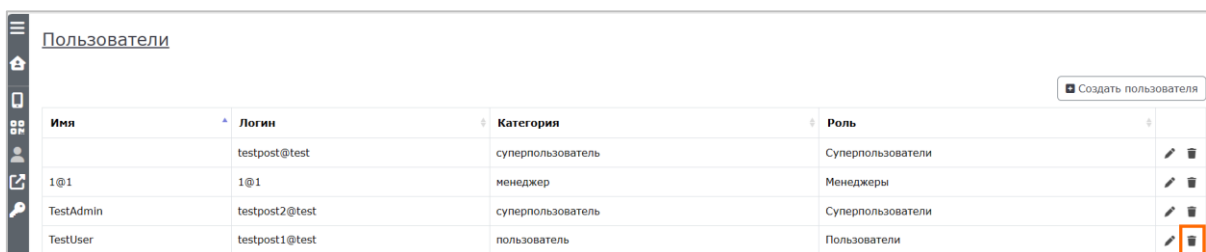
Рисунок 30 – Веб-интерфейс JCVT. Профиль – Подтверждение Смены пароля

4.2.9 Удаление пользователя

Для удаления пользователя Администратор должен:

1. В боковом меню Административной консоли выбрать пункт меню [Пользователи] (см. Рисунок 18);

2. В записи требуемого пользователя нажать кнопку  (см. Рисунок 31);



Пользователи

Создать пользователя









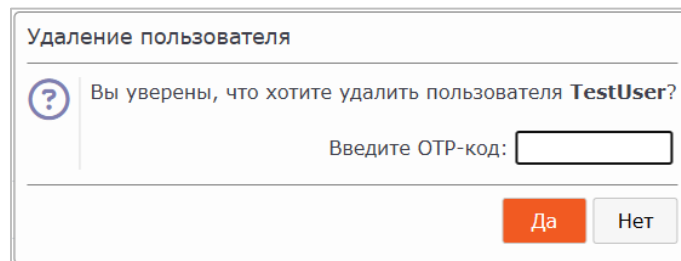
Имя	Логин	Категория	Роль	
	testpost@test	суперпользователь	Суперпользователи	 
1@1	1@1	менеджер	Менеджеры	 
TestAdmin	testpost2@test	суперпользователь	Суперпользователи	 
TestUser	testpost1@test	пользователь	Пользователи	 

Рисунок 31 – Веб-интерфейс JCVT. Страница Пользователи - Удалить

3. Подтвердить действие вводом OTP-кода (см. Рисунок 32);



Удаление пользователя

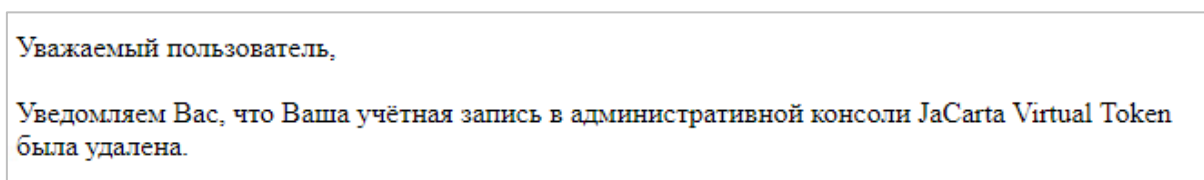
Вы уверены, что хотите удалить пользователя **TestUser**?

Введите OTP-код:

Да Нет

Рисунок 32 – Веб-интерфейс JCVT. Страница Пользователи – Подтверждение удаления пользователя

После удаления пользователю придёт уведомление на почту, о том, что его учётную запись удалили.



Уважаемый пользователь,

Уведомляем Вас, что Ваша учётная запись в административной консоли JaCarta Virtual Token была удалена.

Рисунок 33 – Уведомление пользователю об удалении учётной записи

4.2.10 Автоматические уведомления

1. Удаление пользователя:

При удалении пользователя, пользователю должно прийти письмо, на указанный e-mail:

"Уважаемый пользователь!

Уведомляем Вас, что Ваша учётная запись в административной консоли JaCarta Virtual Token была удалена."

2. Сброс пароля и второго фактора:

При сбросе пароля и второго фактора аутентификации администратором, пользователю должно прийти письмо, на указанный e-mail:

"Уважаемый пользователь,

Ваш пароль и второй фактор аутентификации для доступа к административному интерфейсу JaCarta Virtual Token были сброшены.

Адрес сервера:

Логин:

Новый пароль:"

3. Сброс второго фактора:

При сбросе второго фактора аутентификации администратором пользователю должно прийти письмо, на указанный e-mail:

"Уважаемый пользователь,

Ваш второй фактор аутентификации для доступа к административному интерфейсу JaCarta Virtual Token был сброшен.

Второй фактор необходимо будет зарегистрировать при входе в административный интерфейс.

Адрес сервера:"

4.2.11 Подтверждение действий с помощью OTP-кода

Для ряда ключевых действий в системе потребуется ввести OTP-код, который был зарегистрирован при первом входе в административную консоль.

Список действий, для подтверждения которых необходимо ввести OTP-код:

- Удаление пользователя;
- Деактивация серийного номера на странице серийных номеров;
- Деактивация серийного номера через кнопку редактирования.

4.2.12 Работа с серийными номерами

На странице [Статус серийного номера] (см. Рисунок 34) можно управлять сгенерированным ранее серийным номером: редактировать серийный номер³, проверить статус, срок действия выданного серийного номера, количество активированных и свободных серийных номеров, деактивировать выданные ранее серийные номера.

³ Зависит от настроек сервера. См. 4.1.5

Статус серийного номера

Активированные серийные номера: 4/6
Ожидают активации серийные номера: 2/6
Свободные серийные номера: 0/6

Поиск: Серийный номер, Email или имя

Последняя активность от: Статус: без фильтра Статус Email: без фильтра

Записи с 1 по 6 из 6

<input type="checkbox"/>	Серийный номер	Статус	Статус изменен	Активен до	Устройство	Активность	Email	Статус отправки Email	Имя	Лицензия до	<input type="button" value="✎"/>
<input type="checkbox"/>	FFFFFFFF0000CED3	Ожидание активации	01.07.2024 14:33	-	-	-	dxcdc@vcvvc	Отправлено 01.07.2024	-	Бессрочно	<input type="button" value="✎"/>
<input type="checkbox"/>	FFFFFFFF0000CED5	Активирован	25.06.2024 14:51	Бессрочно	iPhone 11 Apple	26.06.2024 15:52	sds@dsds	Не отправлено	-	Бессрочно	<input type="button" value="✎"/>
<input type="checkbox"/>	FFFFFFFF0000CED6	Активирован	26.06.2024 12:17	Бессрочно	SM-A225F samsung	26.06.2024 12:43	sddssd@sdds	Не отправлено	-	Бессрочно	<input type="button" value="✎"/>
<input type="checkbox"/>	FFFFFFFF0000CEF6	Активирован	27.06.2024 08:16	Бессрочно	iPhone 13 Pro Apple	27.06.2024 10:35	testmail@internet.ru	Отправлено 27.06.2024	-	Бессрочно	<input type="button" value="✎"/>
<input type="checkbox"/>	FFFFFFFF0000CEF7	Активирован	27.06.2024 10:44	Бессрочно	iPhone 8 Apple	27.06.2024 10:55	testmail@internet.ru	Отправлено 27.06.2024	-	Бессрочно	<input type="button" value="✎"/>
<input type="checkbox"/>	FFFFFFFF0000CEF9	Ожидание активации	02.07.2024 11:40	-	-	-	test	Не отправлено	-	Бессрочно	<input type="button" value="✎"/>

Записи с 1 по 6 из 6

Рисунок 34 - Веб-интерфейс JCVT. Страница [Статус серийного номера]

Ниже подробное описание следующих опций:

1. Редактирование серийного номера.

Для перехода в режим редактирования серийного номера необходимо в таблице нажать



в соответствующей строке. В открывшемся окне (см. Рисунок 35) можно изменить электронный адрес⁴, отправить повторно или сохранить QR-код, деактивировать серийный номер.

FFFFFFFF0000CED3: dxcdc@vcvvc

Серийный номер:

Email владельца:

Время истечения тикета: 31.07.2024 14:33


Рисунок 35 - Веб-интерфейс JCVT. Страница [Статус серийного номера]. Редактирование серийного номера

2. Проверка срока действия серийного номера.

Срок действия серийного номера - срок действия файла лицензии, в которой содержится этот серийный номер.

Для наглядности предусмотрена следующая цветовая дифференциация срока действия в таблице:

⁴ Зависит от настроек сервера. См. 4.1.5

- Желтый цвет - 0000000000000004 - серийный номер, выделенный желтым цветом, означает, что до конца его срока действия осталось две недели;
 - Красный цвет - 0000000000000007 - серийный номер, выделенный красным цветом, означает, что до конца его срока действия осталось меньше 7 дней.
- По окончании срока действия лицензии в колонке [Срок действия] указана дата, по которую серийный номер был активен, рядом отображается красный восклицательный знак -  (см. Рисунок 36).

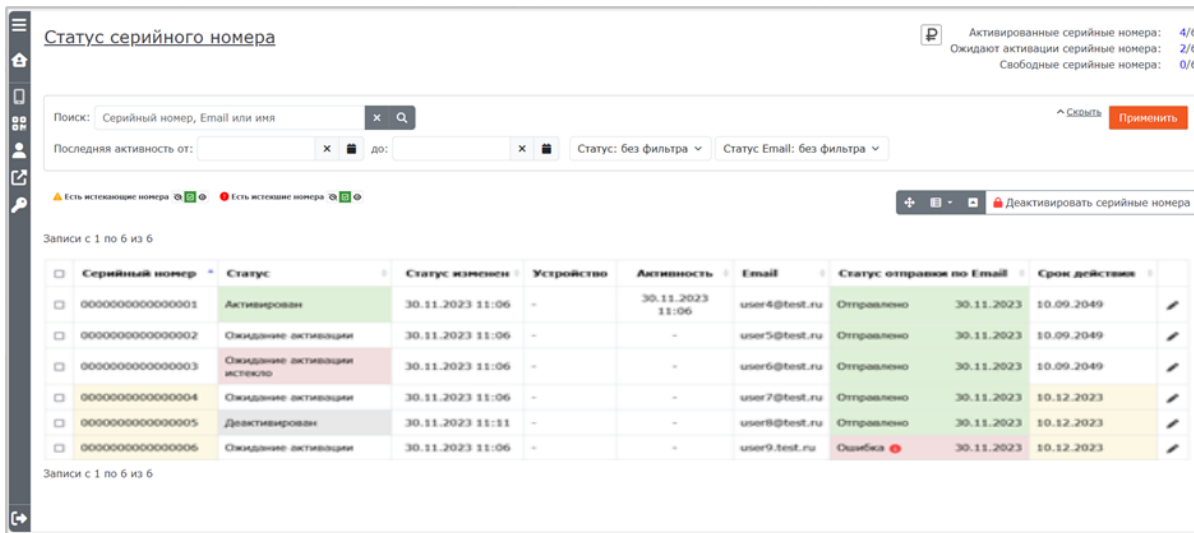





Рисунок 36 - Веб-интерфейс JCVT. Страница [Статус серийного номера]. Цветовая дифференциация серийных номеров

При наличии в таблице истекающих и (или) истекших серийных номеров отображаются соответствующие индикаторы с фильтром отображения:



где варианты настройки фильтра отображения:

-  - отображать все серийные номера, включая истекающие/истекшие серийные номера. (см. Рисунок 36);
-  - отображать только истекающие/истекшие серийные номера. Остальные серийные номера будут скрыты;
-  - скрыть истекающие/истекшие серийные номера. В таблице будут отображаться все серийные номера, кроме истекающих/истекших.

Период истекающих/истекших серийных номеров настраивается в файле конфигурации в разделе `licensing` (см. п.4.1.2).


По умолчанию заданы следующие значения:

- меньше 14 дней до истечения лицензии – желтый цвет;
- меньше 7 дней до истечения лицензии – красный цвет.

3. Проверка статуса серийного номера.

Проверить статус можно с помощью строки поиска или с помощью таблицы, представленной на странице.

- Проверка статуса с помощью строки поиска – данный способ удобен, если необходимо проверить конкретный серийный номер или пользователя, на электронную почту которого был сгенерирован серийный номер. После ввода

серийного номера или данных пользователя и нажатия на кнопку  в таблице будет отображена соответствующая информация (см. Рисунок 37);

Статус серийного номера Активированные серийные номера: 4/6
Ожидают активации серийные номера: 2/6
Свободные серийные номера: 0/6

Поиск: ^ Скрыть Применить

Последняя активность от: до: Все статусы (6) Все статусы Email (3)

Деактивировать серийные номера

Записи с 1 по 3 из 3

<input type="checkbox"/>	Серийный номер	Статус	Статус изменен	Активен до	Устройство	Активность	Email	Статус отправки Email	Имя
<input type="checkbox"/>	FFFFFFFF0000CEF6	Активирован	27.06.2024 08:16	Бессрочно	iPhone 13 Pro Apple	27.06.2024 10:35	testmai1@internet.ru	Отправлено 27.06.2024	-
<input type="checkbox"/>	FFFFFFFF0000CEF7	Активирован	27.06.2024 10:44	Бессрочно	iPhone 8 Apple	27.06.2024 10:55	testmai1@internet.ru	Отправлено 27.06.2024	-
<input type="checkbox"/>	FFFFFFFF0000CEF9	Ожидание активации	02.07.2024 12:44	-	-	-	test_cvet	Не отправлено	-

Записи с 1 по 3 из 3

Рисунок 37 - Веб-интерфейс JCVT. Страница [Статус серийного номера]. Проверка статуса серийного номера

- Проверка статуса с помощью таблицы – для большого количества серийных номеров, подходящих под определенную категорию, удобно пользоваться таблицей и фильтрами. Например, на рисунке ниже (см. Рисунок 38) в таблице отображены сгенерированные серийные номера, имеющие статус [Активирован: бессрочно] и статус отправки по e-mail [Отправлено], которые были выбраны в секции [Фильтр].

Статус серийного номера Активированные серийные номера: 4/6
Ожидают активации серийные номера: 2/6
Свободные серийные номера: 0/6

Поиск: ^ Скрыть Применить

Последняя активность от: до: бессрочный Отправлено

Деактивировать серийные номера

Записи с 1 по 2 из 2




<input type="checkbox"/>	Серийный номер	Статус	Статус изменен	Активен до	Устройство	Активность	Email	Статус отправки Email	Имя
<input type="checkbox"/>	FFFFFFFF0000CEF6	Активирован	27.06.2024 08:16	Бессрочно	iPhone 13 Pro Apple	27.06.2024 10:35	testmai1@internet.ru	Отправлено 27.06.2024	-
<input type="checkbox"/>	FFFFFFFF0000CEF7	Активирован	27.06.2024 10:44	Бессрочно	iPhone 8 Apple	27.06.2024 10:55	testmai1@internet.ru	Отправлено 27.06.2024	-



Записи с 1 по 2 из 2

Рисунок 38- Веб-интерфейс JCVT. Страница [Статус серийного номера]. Отображение серийных номеров, удовлетворяющих фильтру

Ниже (см. Таблица 5) приведено описание столбцов таблицы и фильтров, с помощью которых можно настроить поиск нужных категорий сгенерированных серийных номеров;

Таблица 5 - Веб-интерфейс JCVT. Страница [Статус серийного номера]. Настройки

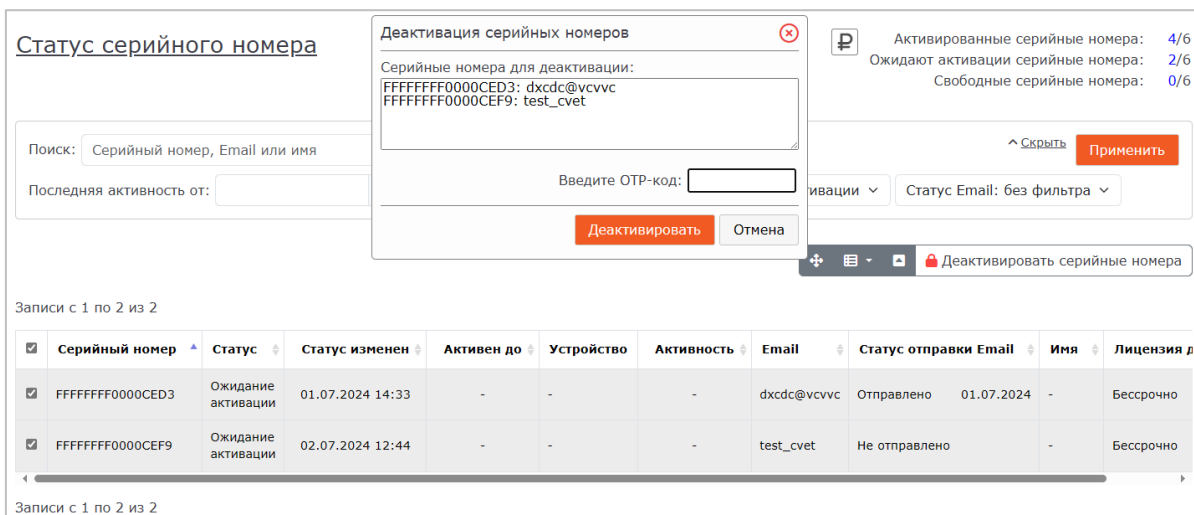
Настройка	Описание
Фильтр	
[Поиск]	Строка для ввода серийного номера или электронной почты пользователя
[Последняя активность]	Задание временных рамок для поиска серийных номеров, попадающих в данный интервал
[Статус]	Выпадающий список статусов, в соответствии с которыми настраивается поиск
[Статус E-mail]	Выпадающий список статусов, в соответствии с которыми настраивается поиск
	Опция позволяющая развернуть таблицу серийных номеров на весь экран
	Опция позволяющая настроить список выводимых в таблице колонок
	Опция позволяющая убрать верхнюю постраничную навигацию
Таблица	
[Серийный номер]	Столбец, в котором отображаются серийные номера
[Статус]	В данном столбце отображаются статусы сгенерированных серийных номеров
[Статус изменения]	Время и дата последнего изменения статуса серийного номера
[Активен до]	Дата окончания срока действия серийного номера. При истечении срока действия серийного номера поле очищается.
[Устройство]	Наименование устройства, с которого был активирован серийный номер. Если активации серийного номера не было, в столбце отображается «-»

	При истечении срока действия серийного номера поле очищается.
[Активность]	Дата последней активности
[Email]	Адрес электронной почты, на имя которой был сгенерирован серийный номер
[Статус отправки по Email]	Отображение статуса электронного письма пользователю
[Лицензия]	<p>Отображения срока действия лицензии сервера.</p> <p>Цветовая дифференциация даты соответствует серийному номеру.</p> <p>По окончании срока действия рядом с датой отображается восклицательный знак - .</p> <p>Если до конца срока действия серийного номера больше 45 лет, отображается не дата, а статус [Бессрочный]</p>
	Переход к режиму редактирования

4. Деактивация серийного номера

Для деактивации серийного номера необходимо отметить галочкой запись в таблице и нажать кнопку <Деактивировать серийные номера>.

Можно осуществлять и массовую деактивацию серийных номеров, удовлетворяющих настроенному фильтру. На рисунке ниже (см. Рисунок 39) приведена деактивация серийных номеров, находящихся в статусе [Ожидание активации].



The screenshot shows the 'Статус серийного номера' (Serial Number Status) page. A modal window titled 'Деактивация серийных номеров' (Deactivation of serial numbers) is open, displaying a list of serial numbers for deactivation: FFFFFFFF0000CED3: dxcdc@vcvvc and FFFFFFFF0000CEF9: test_cvet. Below the list is an input field for an OTP code and buttons for 'Деактивировать' (Deactivate) and 'Отмена' (Cancel). In the background, a table lists serial numbers with their status, change date, and other details. The table has columns: Серийный номер, Статус, Статус изменен, Активен до, Устройство, Активность, Email, Статус отправки Email, Имя, and Лицензия. Two rows are visible, both with a status of 'Ожидание активации' (Waiting for activation).


Серийный номер	Статус	Статус изменен	Активен до	Устройство	Активность	Email	Статус отправки Email	Имя	Лицензия
FFFFFFFF0000CED3	Ожидание активации	01.07.2024 14:33	-	-	-	dxcdc@vcvvc	Отправлено	01.07.2024	Бессрочно
FFFFFFFF0000CEF9	Ожидание активации	02.07.2024 12:44	-	-	-	test_cvet	Не отправлено	-	Бессрочно

Рисунок 39 - Веб-интерфейс JCVT. Страница [Статус серийного номера]. Деактивация серийных номеров, удовлетворяющих фильтру

При нажатии на кнопку <Деактивировать серийные номера> отобразится окно с серийными номерами. Необходимо подтвердить действие введя OTP-код второго фактора аутентификации. Для продолжения операции нажать кнопку <Деактивировать>. После этого отобразится уведомление о деактивации номеров, а счётчик свободных серийных номеров увеличится на число, равное количеству деактивированных серийных номеров;

5. Информация о лицензиях



По нажатию на кнопку  будет открыто окно с информацией об общем количестве лицензий и их сроке годности (см. Рисунок 40). Также отображается количество серийных номеров в разных статусах.

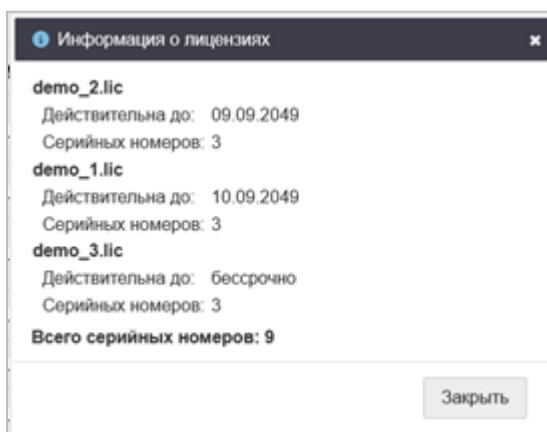


Рисунок 40 - Веб-интерфейс JCVT. Страница [Статус серийного номера]. Информация о лицензиях

Если JCVT Server одновременно использует бессрчную и временные лицензии, то серийные номера выдаются сначала из количества бессрчной лицензии.

Если есть только временные лицензии, то серийные номера выдаются сначала из тех лицензий, которые имеют наибольший срок действия.

При удалении файла лицензии администратором, серийные номера перестают отображаться

4.2.13 Генерация серийного номера

Для доступа пользователей, которые используют мобильное приложение JCVT, к корпоративным ресурсам необходимо, чтобы каждое устройство имело зарегистрированный серийный номер.


Выдача серийных номеров осуществляется с помощью административного веб-интерфейса сервера.


Это единственный способ получения серийного номера.


Один серийный номер соответствует одному виртуальному токenu

На странице [Запрос серийного номера] (см. Рисунок 41) представлены две секции: для создания серийного номера – [Генерация нового серийного номера] и его редактирования – [Редактирование серийного номера].

Редактирование серийного номера [Статус серийного номера](#)



Серийный номер: 

Email владельца: 

[Сохранить QR-код в файл](#)

[Отправить QR-код по Email](#)

Генерация нового серийного номера

Email владельца: [Сгенерировать и сохранить QR-код в файл](#)

Перед генерацией введите Email будущего владельца токена. При вводе email, письмо с QR-кодом можно будет отправлено на него.

Срок действия QR-кода:

[Сгенерировать и отправить QR-код по Email](#)

[Массовая генерация и рассылка QR-кодов по Email](#)

[Проверка отправки Email](#)

Рисунок 42 – Веб-интерфейс JCVT. Страница [Запрос серийного номера]. Генерация серийного номера

- **С помощью кнопки <Сгенерировать и отправить QR-код по Email>.**

В этом случае можно сразу отправить сгенерированный QR-код на электронную почту пользователю. Для этого необходимо ввести время жизни (в часах или днях) для сканирования QR-кода в поле [Срок действия QR-кода], в поле [Email владельца] ввести электронный адрес, на который будет отправлено письмо с QR-кодом. Опционально можно ограничить срок действия серийного номера, проставив флаг [Срок действия серийного номера] и указав срок действия в днях. По умолчанию, при снятом флаге, – бессрочно. После нажать кнопку <Сгенерировать и сохранить QR-код по Email>. QR-код отобразится в квадратной области выше⁶ и будет отправлен пользователю на указанный адрес электронной почты. Пример письма для пользователя приведен ниже (см. Рисунок 43). Шаблон письма настраивается и, может быть, изменён (см. подробнее п.4.1.3);

⁶ Зависит от настроек сервера. См. 4.1.6

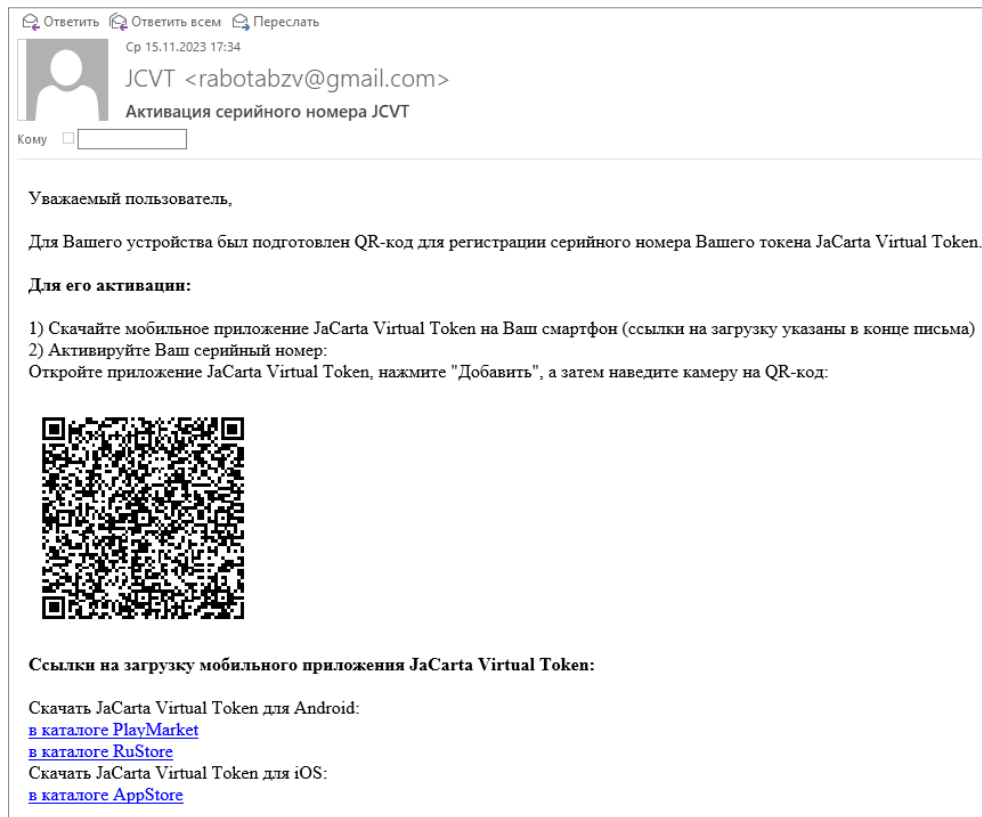


Рисунок 43 – Пример письма пользователю с сгенерированным QR-кодом для регистрации серийного номера

- **С помощью кнопки <Массовая генерация и рассылка QR-код по Email>.**

В этом случае можно сразу отправить сгенерированные QR-коды на электронную почту большому количеству пользователей. Для этого необходимо ввести время жизни (в часах или днях) для сканирования QR-кода в поле [Срок действия QR-кода]. Опционально можно ограничить срок действия серийного номера, проставив флаг [Срок действия серийного номера] и указав срок действия в днях. По умолчанию, при снятом флаге, – бессрочно. И нажать кнопку <Массовая генерация и рассылка QR-код по Email>. Будет открыто одноименное окно (см. Рисунок 44), где необходимо ввести перечень электронных адресов и нажать кнопку <Сгенерировать и отправить>.

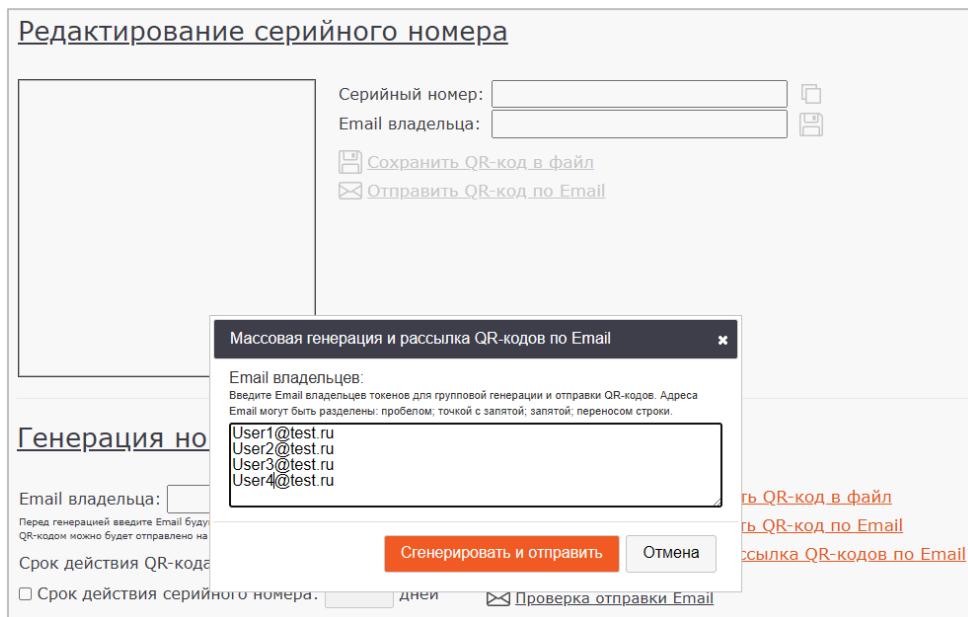


Рисунок 44 – Веб-интерфейс JCVT. Страница [Запрос серийного номера]. Массовая генерация и рассылка QR-код по Email

В случае успешной отправки отобразится соответствующее уведомление (см. Рисунок 45). Пользователи получают электронные письма с QR-кодом серийного номера (см. Рисунок 43).

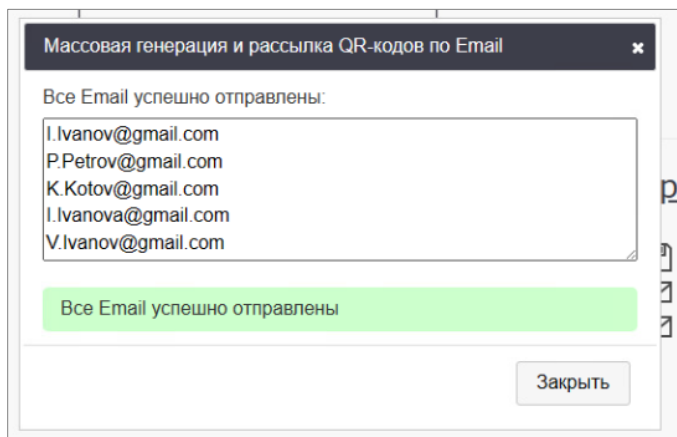


Рисунок 45 – Веб-интерфейс JCVT. Страница [Массовая генерация и рассылка QR-код по Email]. Уведомление об успешной отправке

В случае если был указан некорректный формат электронного ящика, будет отображено соответствующее сообщение (см. Рисунок 46), письмо на этот адрес отправлено не будет.

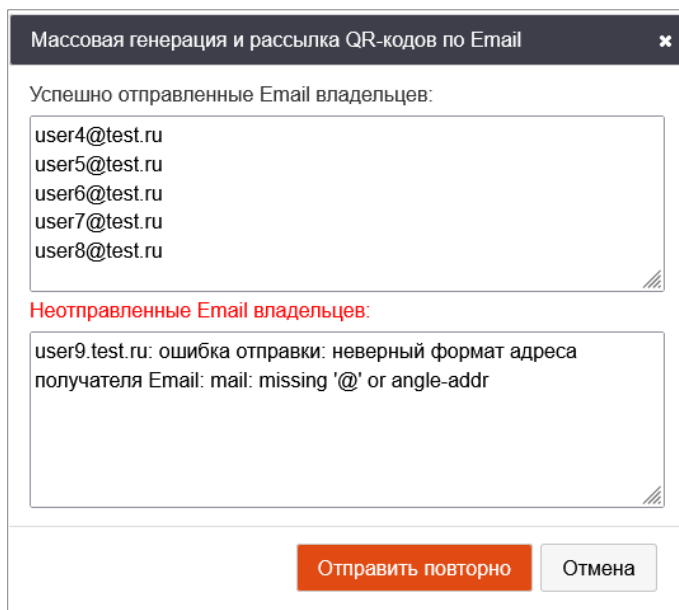




Рисунок 46 – Веб-интерфейс JCVT. Страница [Массовая генерация и рассылка QR-код по Email]. Письмо не было отправлено на некорректный адрес

Описание настроек страницы [Запрос серийного номера] приведено в Таблица 6.

Таблица 6 - Веб-интерфейс JCVT. Страница [Запрос серийного номера]. Настройки

Настройка	Описание
Секция [Редактирование серийного номера]	
[Серийный номер]	В поле отображается сгенерированный зарезервированный серийный номер для выдачи мобильному приложению
[Email владельца]	В поле отображается введенный в секции [Генерация нового серийного номера] электронный адрес пользователя. В этом поле возможно изменить адрес/указать новую электронную почту для повторной отправки письма, содержащего QR-код для регистрации серийного номера
	Кнопка для сохранения QR-кода в файл формата *.png и последующей отправки его пользователю ⁷
	Кнопка для копирования содержимого поля
<Сохранить QR-код в файл>	Кнопка для сохранения QR-кода в файл формата *.png ⁸

⁷ Зависит от настроек сервера. См. 4.1.6

⁸ Зависит от настроек сервера. См. 4.1.6

<Отправить QR-код по Email>	Кнопка для отправления QR-кода электронным письмом по заданному в поле [Email владельца] адресу
Секция [Генерация нового серийного номера]	
[Email владельца]	Поле для ввода электронной почты пользователя. Обязательное поле для заполнения
<Срок действия QR-кода>	Выпадающий список, в котором задаётся срок действия QR-кода в днях или часах (значения можно выбрать во втором выпадающем списке). Если в течение этого периода QR-код не будет отсканирован в мобильном приложении, то этот QR-код будет считаться просроченным, а зарезервированный серийный номер будет считаться свободным для повторной выдачи. Обязательное поле для заполнения
<Срок действия серийного номера>	Флаг и Выпадающий список, в котором задаётся срок действия серийного номера в днях.
<Сгенерировать и сохранить QR-код в файл>	Кнопка для генерации QR-кода с последующим сохранением его в файл формата *.png. Генерация QR-кода происходит только после заполненных значений полей [Email владельца] и <Срок действия тикета> Генерация QR-кода в файл возможна только если в настройках сервера разрешена опция отображения QR-кодов в интерфейсе.
<Сгенерировать и отправить QR-код по Email>	Кнопка для генерации QR-кода с его последующей отправкой на электронную почту, указанную в поле [Email владельца]. Генерация QR-кода происходит только после заполненных значений полей [Email владельца] и <Срок действия QR-кода>
<Массовая генерация и рассылка QR-кодов по Email>	Кнопка для генерации нескольких QR-кодов с их последующей рассылкой по указанным электронным адресам. Генерирует QR-код только после заполненного значения настройки <Срок действия QR-кода>

<Проверка отправки Email>

Отправляет письмо на электронный адрес, введённый в поле [Email владельца].
Отправляется письмо с тестовым QR-кодом.
Данная функция подходит для проверки правильности настроек SMTP-сервера и настройки шаблона письма

5. Клиент JaCarta Virtual Token. Установка и настройка

Клиент JaCarta Virtual Token - приложение для рабочей станции, осуществляющее подключение к ней виртуального токена с помощью серверного приложения Сервер JaCarta Virtual Token.

5.1 Настройка конфигурации

Для первичной настройки соединения Клиента JaCarta Virtual Token и Сервера JaCarta Virtual Token необходим конфигурационный файл. Его можно создать (см. п. 5.1.1) или перенастроить заново (см. п. 5.1.2), в зависимости от того, это первоначальная настройка или изменение уже существующих настроек.

5.1.1 Создание конфигурационного файла

С помощью текстового редактора создать файл со следующей структурой:

```
{
  "readers":
  [
    {
      "transport":
      {
        "address": "wss://domain.ru:6789",
        "apiAddress": "https://domain.ru:6788"
      }
    }
  ]
}
```

где

- адреса `wss://domain.ru:6789` и `https://domain.ru:6788` должны указывать на развёрнутый Сервер JaCarta Virtual Token, с соответствующими портами, заданными в конфигурационном файле Сервера JaCarta Virtual Token (в примере выше указаны порты, которые предлагаются в стандартном файле конфигурации Сервера JaCarta Virtual Token по умолчанию: 6789 и 6788);
- `address` - адрес websocket-интерфейса Сервера JaCarta Virtual Token. Используется для передачи сообщений между Клиентом JaCarta Virtual Token и Мобильным приложением JaCarta Virtual Token;
- `apiAddress` - адрес api-интерфейса Сервера JaCarta Virtual Token. Используется для обработки команд от Клиентов JaCarta Virtual Token и Мобильных приложений JaCarta Virtual Token самим Сервером JaCarta Virtual Token.


Сохранить файл, установив тип `*.cfg` и задав имя `JaCartaVirtualToken - JaCartaVirtualToken.cfg`.

5.1.2 Обновление конфигурационного файла

В случае если необходимо перенастроить подключение Клиента JaCarta Virtual Token и текущего Сервера JaCarta Virtual Token или подключить его к новому, следует загрузить новый конфигурационный файл.

Для того чтобы обновить конфигурацию подключения Клиента JaCarta Virtual Token необходимо:

1. Создать новый конфигурационный файл, с необходимыми настройками подключения (см. п. 5.1.1);

2. Открыть Панель управления JaCarta Virtual Token, используя ярлык приложения  на рабочем столе;

3. Перейти в настройки, нажав кнопку ;

4. Нажать кнопку <Зарегистрировать> (см. Рисунок 47);

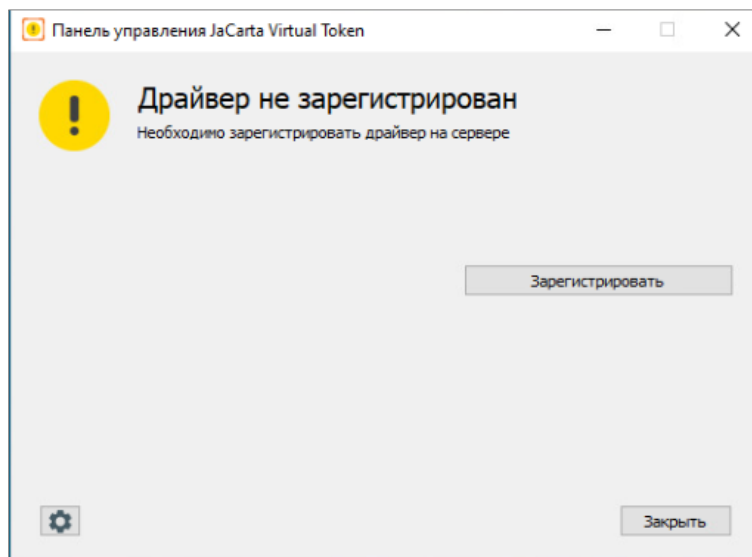


Рисунок 47 – Панель управления JaCarta Virtual Token. Загрузка конфигурации сервера

5. В открывшемся окне выбрать конфигурационный файл `JaCartaVirtualToken.cfg`, созданный ранее;
6. При успешной загрузке конфигурации будет отображено информационное сообщение (см. Рисунок 48).

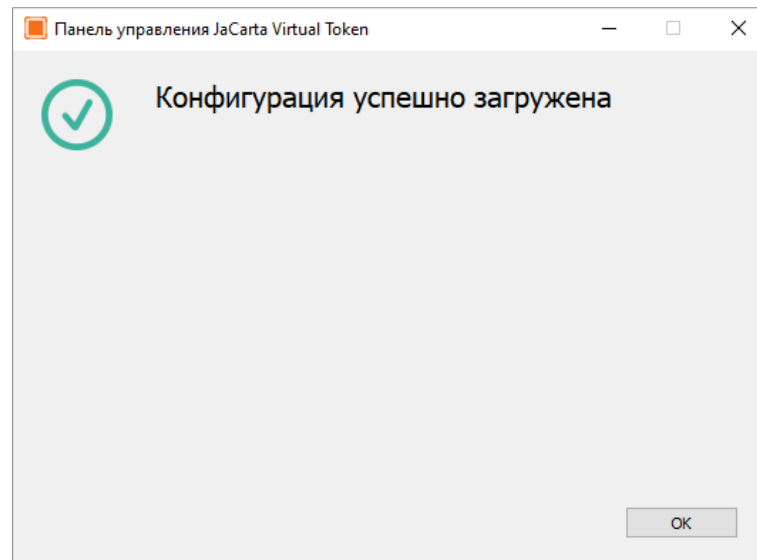


Рисунок 48 - Панель управления JaCarta Virtual Token. Успешная загрузка конфигурации

5.1.3 Перезапись конфигурационного файла

При попытке загрузить конфигурационный файл на Панель управления JaCarta Virtual Token, у которого адрес транспортного сервиса совпадает с адресом, указанным в загруженном ранее конфигурационном файле, будет отображено диалоговое окно, приведенное ниже (см. Рисунок 49).

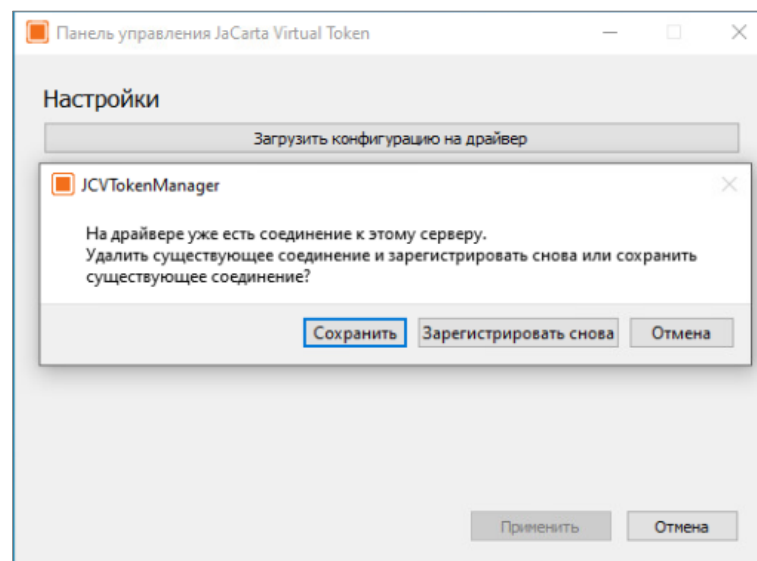


Рисунок 49 - Панель управления JaCarta Virtual Token. Сообщение при перезаписи конфигурационного файла

При нажатии на кнопку <Сохранить> логин и пароль для доступа к транспортному серверу будут сохранены без изменений. Будет осуществлен переход на экран с успешной загрузкой конфигурации (см. Рисунок 50).

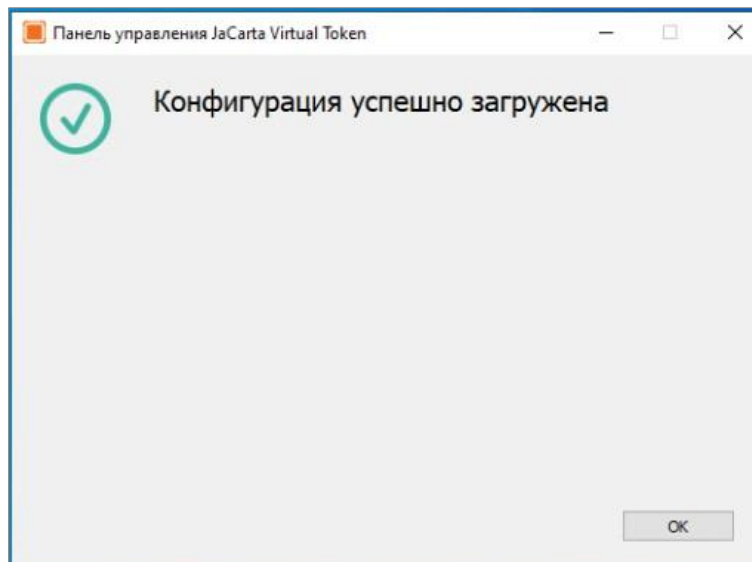



Рисунок 50 - Панель управления JaCarta Virtual Token. Успешная загрузка конфигурации

При нажатии на кнопку <Зарегистрировать снова> текущий конфигурационный файл будет перезаписан: будут удалены существующие логин и пароль для доступа к транспортному серверу. После отобразится сообщение, что конфигурация была успешно загружена (см.

Рисунок 51), но необходима регистрация драйвера (иконка  в заголовке экрана).

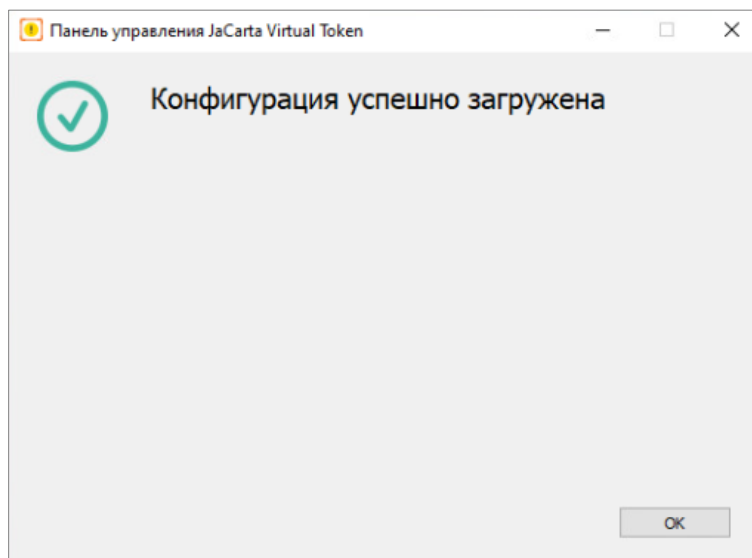


Рисунок 51 - Панель управления JaCarta Virtual Token. Успешная загрузка конфигурации с последующей регистрацией драйвера

Нажать кнопку <OK>, будет открыто окно [Драйвер не зарегистрирован] (см. Рисунок 52). Нажать кнопку <Зарегистрировать>.

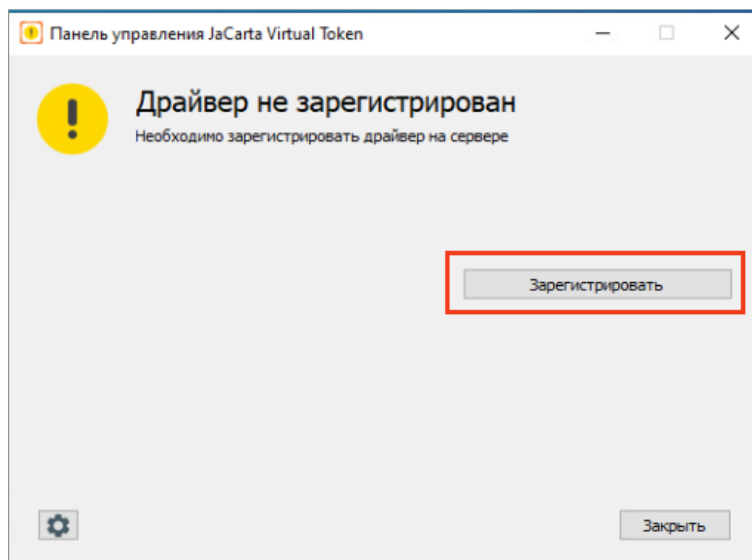


Рисунок 52 - Панель управления JaCarta Virtual Token. Драйвер не зарегистрирован

Будет осуществлен переход на экран с успешной регистрацией драйвера (см. Рисунок 53).

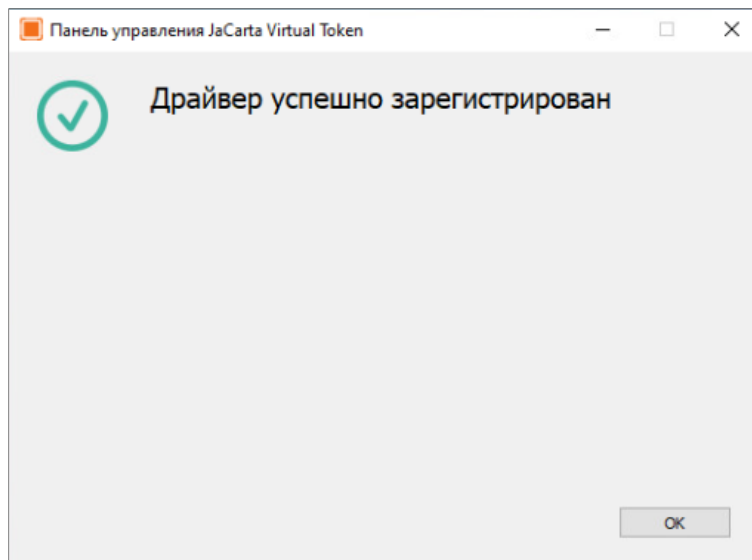


Рисунок 53 - Панель управления JaCarta Virtual Token. Успешная регистрация драйвера

В случае нажатии кнопки <Отмена> (см. Рисунок 49), диалоговое окно закроется, конфигурация не будет загружена.

5.2 Клиент JaCarta Virtual Token на ОС Windows

5.2.1 Установка JaCarta Virtual Token

Для того чтобы установить Клиент JaCarta Virtual Token необходимо выполнить следующие действия:

1. Расположить дистрибутив JaCartaVirtualToken-x64-x.x.x.msi и файл конфигурации в одной папке;
2. Запустить дистрибутив;
3. Нажать кнопку <Далее> (см. Рисунок 54);

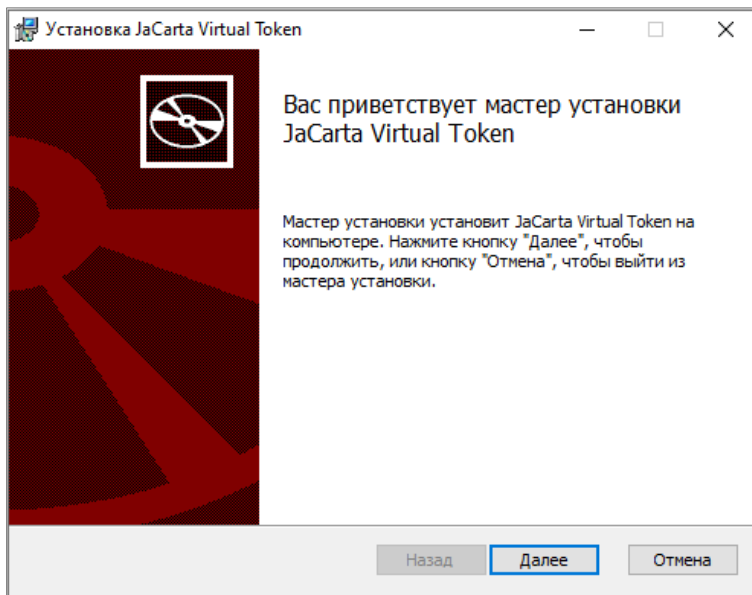


Рисунок 54 – JaCarta Virtual Token. Мастер установки Клиента JaCarta Virtual Token

4. Принять Лицензионное соглашение и нажать кнопку <Далее>(см. Рисунок 55);

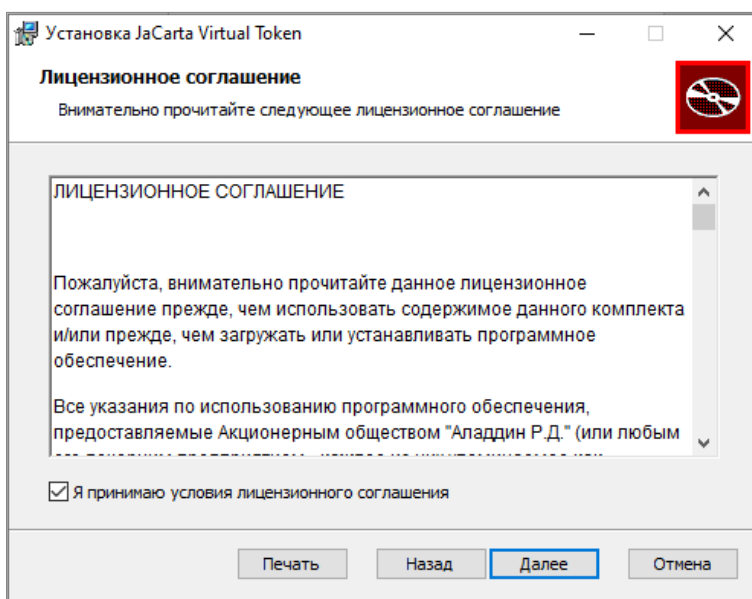


Рисунок 55 - JaCarta Virtual Token. Мастер установки Клиента JaCarta Virtual Token

5. Выбрать папку установки и нажать кнопку <Далее> (см. Рисунок 56);

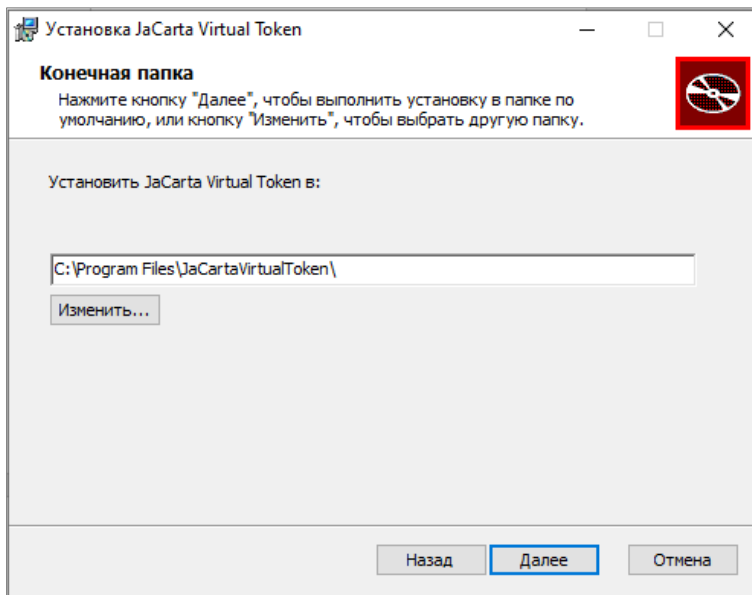


Рисунок 56 - JaCarta Virtual Token. Мастер установки Клиента JaCarta Virtual Token

6. Нажать кнопку <Установить> (см. Рисунок 57);

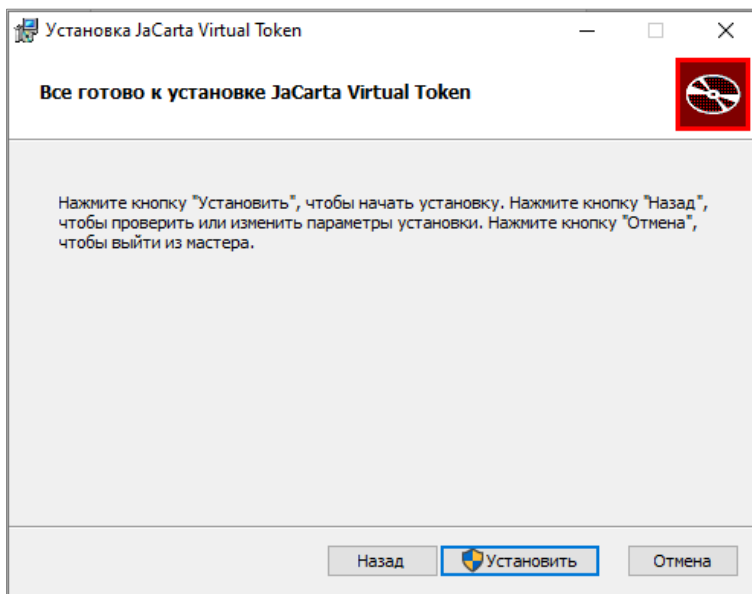


Рисунок 57 - JaCarta Virtual Token. Мастер установки Клиента JaCarta Virtual Token

7. Согласиться с системным уведомлением об установке Клиента JaCarta Virtual Token;
8. Нажать кнопку <Готово> (см. Рисунок 58);

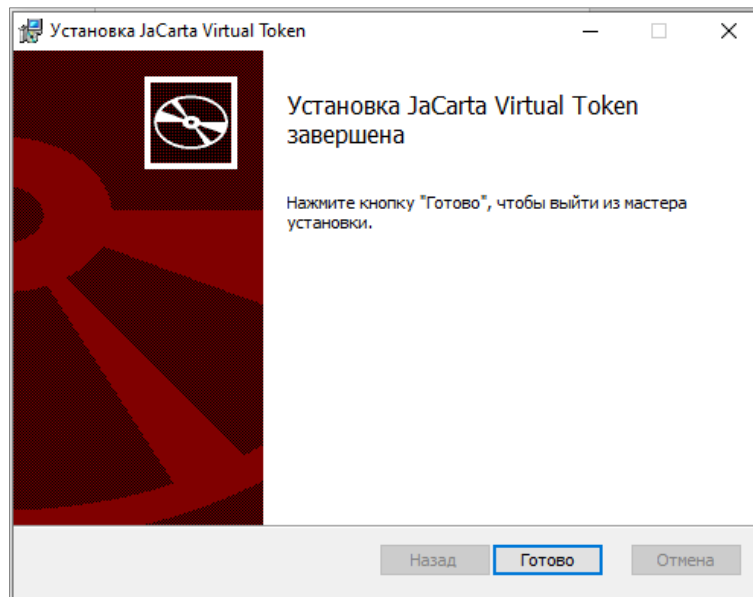


Рисунок 58 - JaCarta Virtual Token. Мастер установки Клиента JaCarta Virtual Token

5.2.2 Удаление Клиента JaCarta Virtual Token

Для удаления Клиента JaCarta Virtual Token необходимо совершить следующие действия:

1. Последовательно выбрать Пуск → Параметры → Приложения;
2. Найти в списке JaCarta Virtual Token и нажать кнопку <Удалить> (см. Рисунок 59).

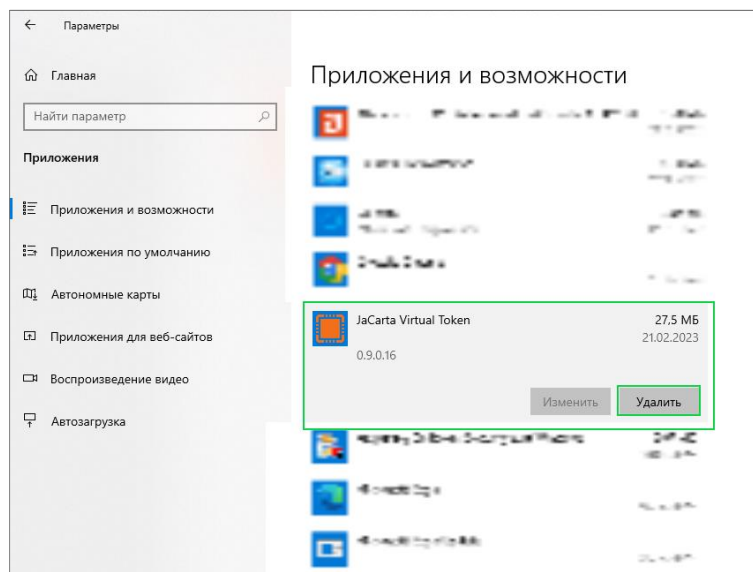


Рисунок 59 - JaCarta Virtual Token. Удаление Клиента JaCarta Virtual Token

5.2.3 Обновление Клиент JaCarta Virtual Token

Для обновления Клиент JaCarta Virtual Token до актуальной версии необходимо выполнить следующие действия:

1. Скачать новую версию Клиента JaCarta Virtual Token сайта Алалдин;
2. Удалить предыдущую версию Клиента JaCarta Virtual Token;
3. Установить новую версию.

5.2.4 Сбор логов

В случае возникновения ошибок в приложении или непредвиденных ситуаций, может возникнуть необходимость сформировать логи.

Сформировать логи можно несколькими способами: из системного трея (область уведомлений) или через проводник файлов.

1. Сбор логов из трея:

- Открыть трей (область уведомлений);
- Навести курсор на иконку Панель управления JaCarta Virtual Token;
- С помощью правой кнопки мыши вызвать контекстное меню и выбрать пункт <Сохранить логи> (см. Рисунок 60 - JaCarta Virtual Token. Сбор логов из области уведомлений);
- В открывшемся окне выбрать папку сохранения архива с файлами логов;

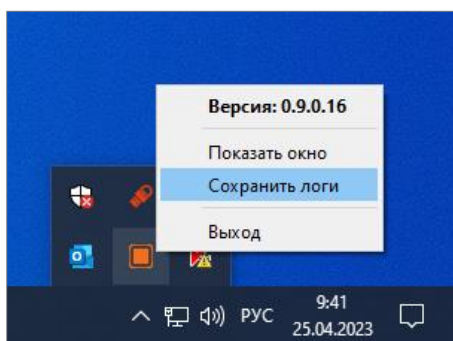


Рисунок 60 - JaCarta Virtual Token. Сбор логов из области уведомлений

2. Сбор логов через проводник файлов:

- Открыть проводник;
- Перейти в директорию `C:\ProgramData\JaCartaVirtualToken\logs`;
- При необходимости скопировать файлы логов в другое место.

5.2.5 Прокси-соединение

В Панели JaCarta Virtual Token предусмотрена возможность включать или отключать использование системных настроек прокси (см. Рисунок 61).

Ниже приведена инструкция по настройке прокси-соединения.

1. Настроить Клиент JaCarta Virtual Token: открыть Панель управления JaCarta Virtual Token, выбрать <Использовать системные настройки прокси> (см. Рисунок 61);

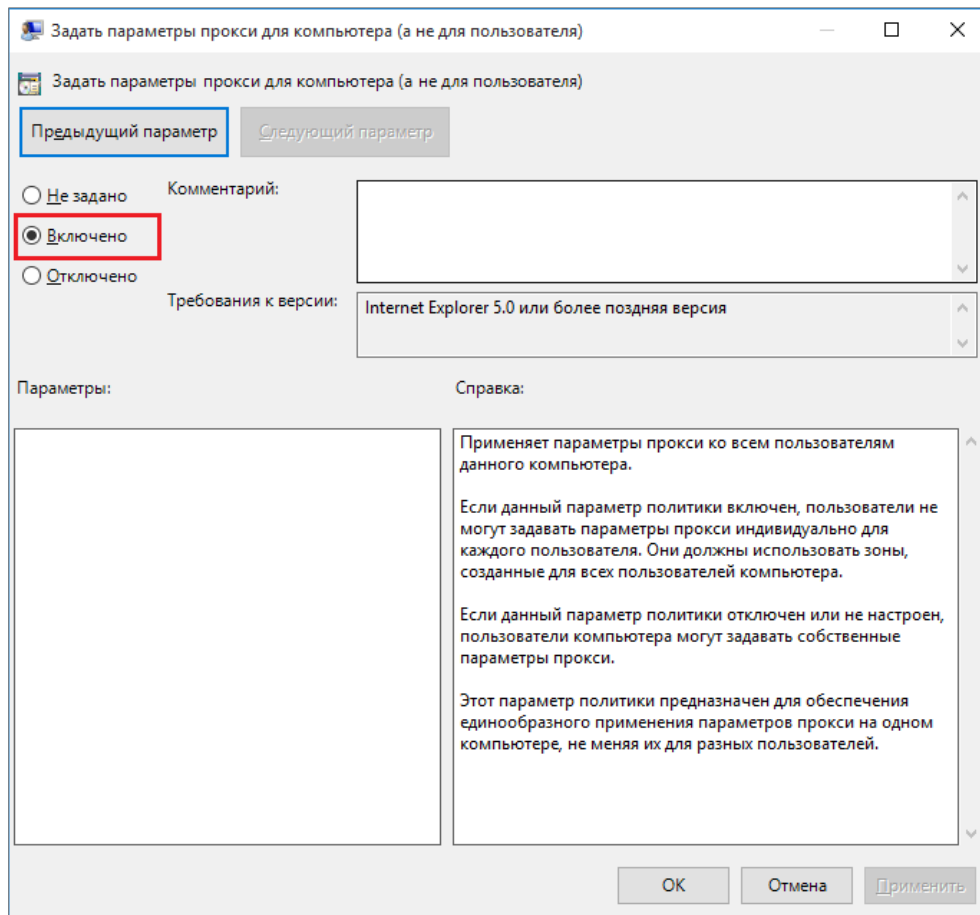


Рисунок 63 - Редактор локальной групповой политики. Включение состояния настройки

- Последовательно выбрать [Конфигурация компьютера] -> [Административные шаблоны] -> [Система] -> [Групповая политика] (см. Рисунок 64).

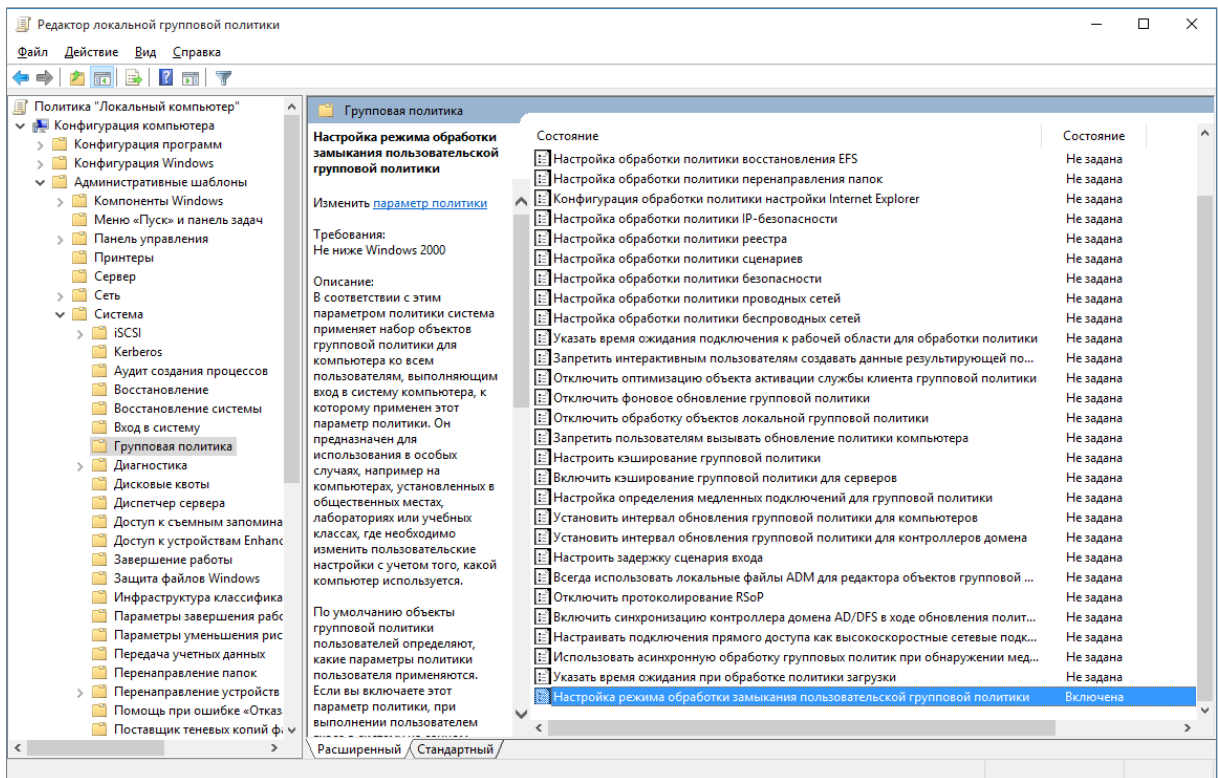


Рисунок 64 – Редактор локальной групповой политики. Настройка групповых политик

Выбрать [Настройка режима обработки замыкания пользовательской групповой политики], включить его и выставить режим <Слияние> (см. Рисунок 65);

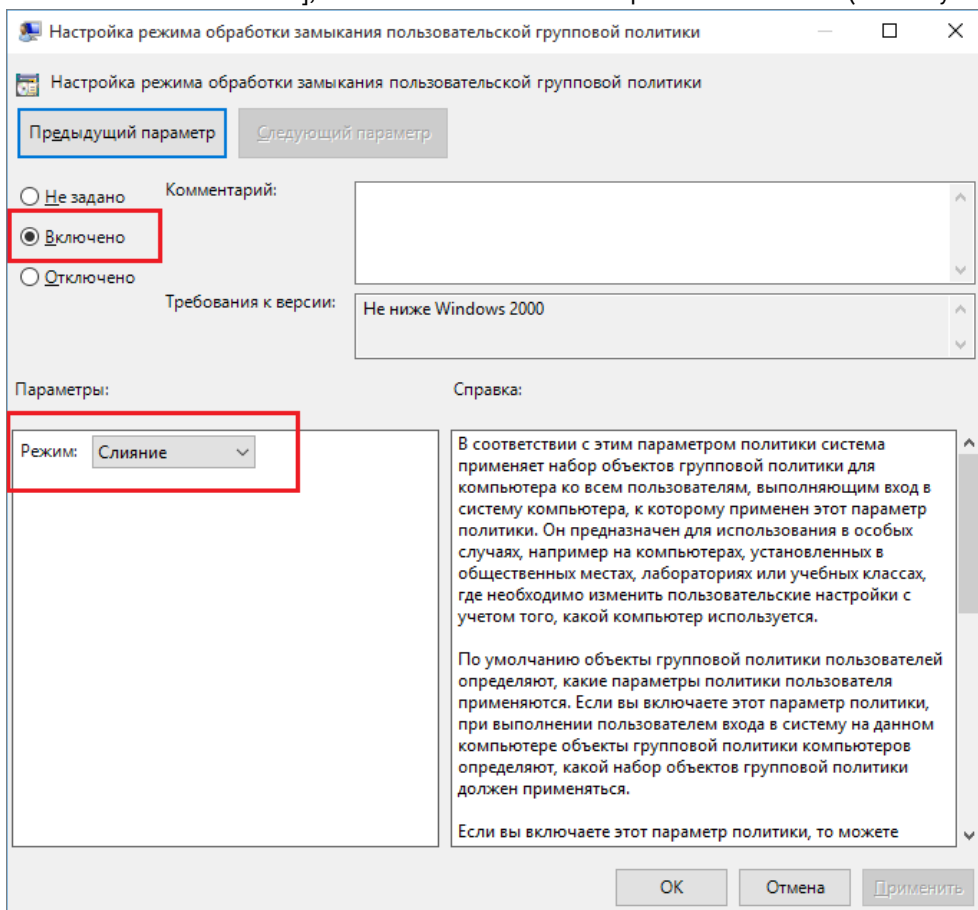


Рисунок 65 - Редактор локальной групповой политики. Включение состояния и режима настройки

3. Разместить файл автоконфигурации прокси на избранном web-сервере, например, IIS:

- На web-сервере разместить файл `test_proxy.pac`;
- Изменить в файле (см. Рисунок 66):
 - адрес транспортного сервера на актуальный (если необходимо). В примере ниже - `beyond.aladdin-rd.ru`;
 - адрес прокси-сервера (адрес **PC-Proxy**) на актуальный (порт не менять). В примере ниже - `wks218.aladdin.ru`.

```
function FindProxyForURL(url, host)
{
    if(host == "beyond.aladdin-rd.ru") {
        return "PROXY wks218.aladdin.ru:3128";
    }
    return "DIRECT";
}
```

Рисунок 66 – Пример файла автоконфигурации прокси с изменениями

4. Настроить параметры прокси на PC-Driver:

- Запустить Internet Explorer от имени администратора;
- Открыть <Свойства браузера> (см. Рисунок 67);

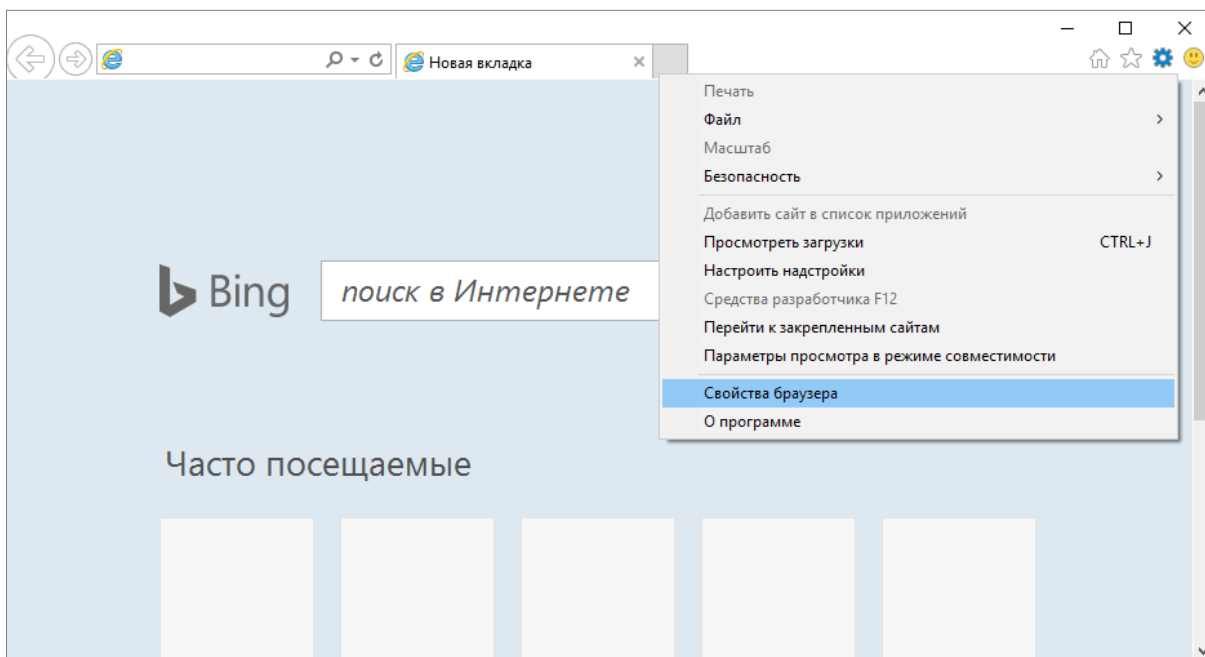


Рисунок 67 - Internet Explorer. Выбор элемента управления <Свойства браузера>

- Перейти на вкладку [Подключение], нажать кнопку <Настройки сети> (см. Рисунок 68);

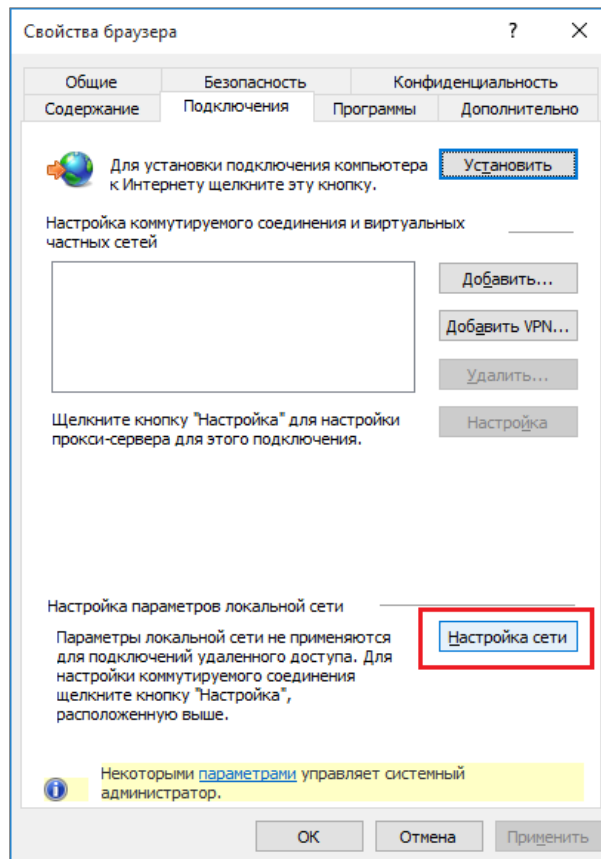


Рисунок 68 - Internet Explorer. Окно [Свойства браузера]. Выбор элемента управления <Настройки сети>

- Настроить адрес файла автоконфигурации прокси: указать http-адрес к файлу `test_proxy.pac`, размещенному на web-сервере.

В примере ниже (см. Рисунок 69) -

`http://wks218.aladdin.ru:8011/proxy test/test proxy.pac.`

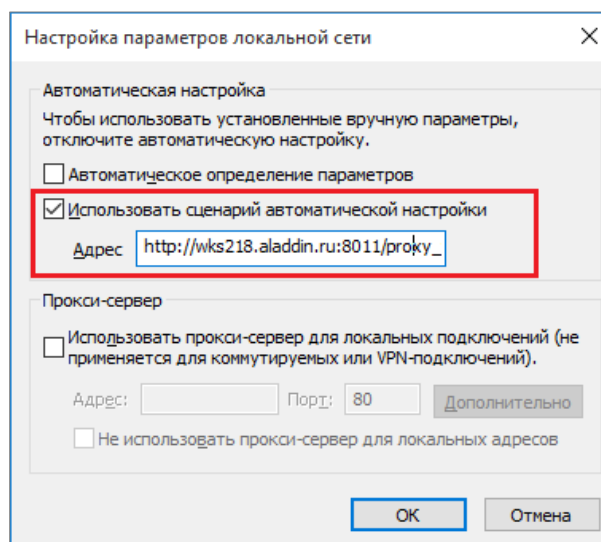


Рисунок 69 - Internet Explorer. Окно [Настройка параметров локальной сети]. Задание http-адреса

5.3 Клиент JaCarta Virtual Token на ОС Linux

Установочный файл Клиента JaCarta Virtual Token для ОС Linux зависит от версии операционной системы. (см. Таблица 3)..

5.3.1 Установка JaCarta Virtual Token ОС Linux

Клиент JaCarta Virtual Token на ОС Linux может быть установлен:

- При помощи графического интерфейса менеджера пакетов;
- С помощью консоли.

Ниже приведено подробное описание каждого способа:

1. Установка с использованием интерфейса менеджера пакетов (на примере Astra Linux).
Для установки необходимо выполнить следующие действия:
 - 1) Получить от разработчика дистрибутив, соответствующий ОС;
 - 2) Запустить дистрибутив;
 - 3) Нажать кнопку <Установить пакет> (см. Рисунок 70);

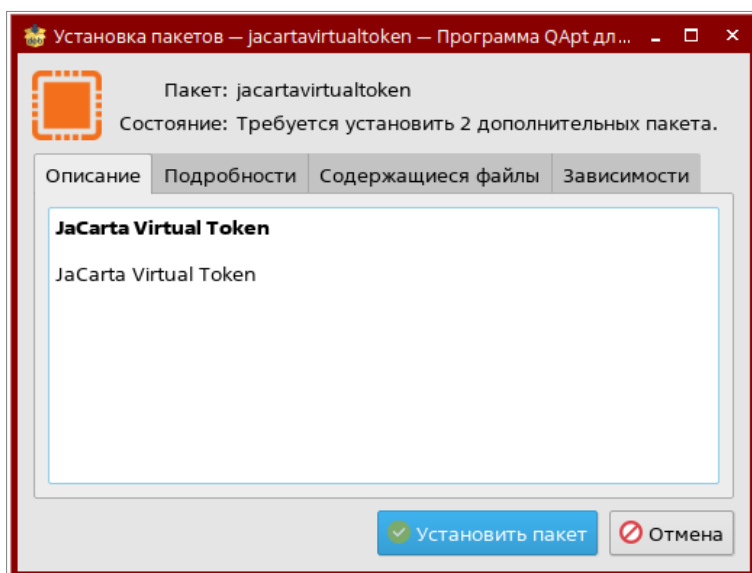


Рисунок 70 - JaCarta Virtual Token. Установка Клиента JaCarta Virtual Token на Linux

- 4) Ввести пароль учётной записи, если требуется (см. Рисунок 71);

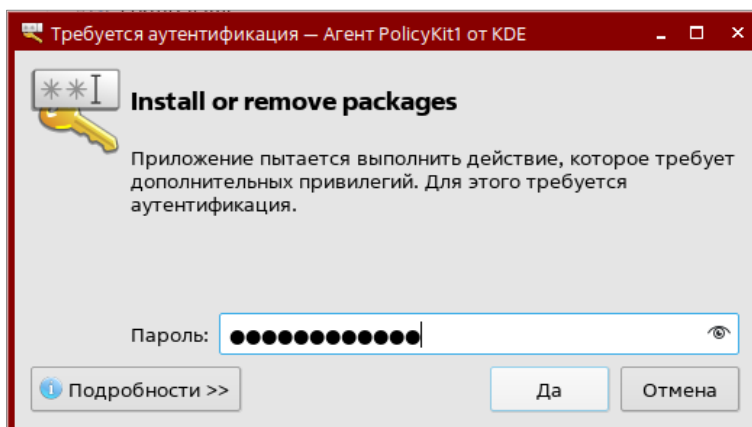


Рисунок 71 - JaCarta Virtual Token. Установка Клиента JaCarta Virtual Token на Linux

- 5) Дождаться конца установки, закрыть окно [Установка пакетов] с помощью кнопки <Заккрыть> (см. Рисунок 72);

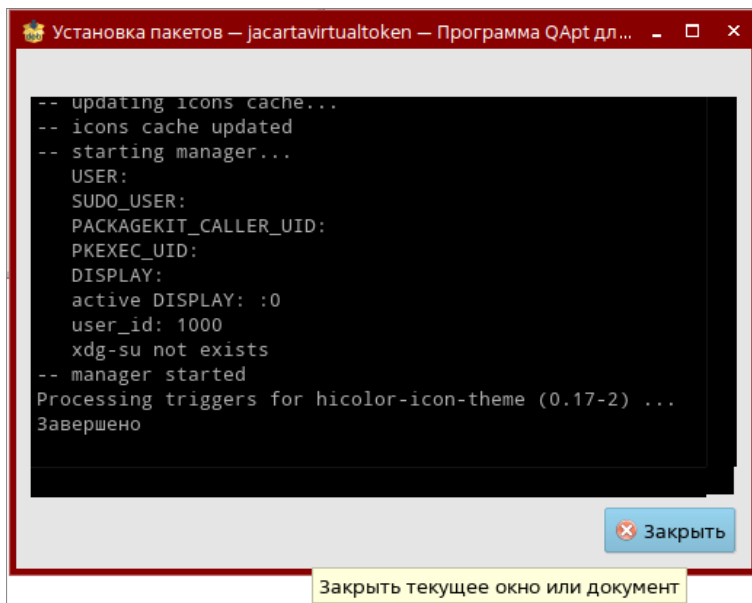


Рисунок 72 - JaCarta Virtual Token. Установка Клиента JaCarta Virtual Token на Linux

- 6) После установки, в открывшемся окне Клиента JaCarta Virtual Token нажать кнопку <Загрузить конфигурацию> (см. Рисунок 73);

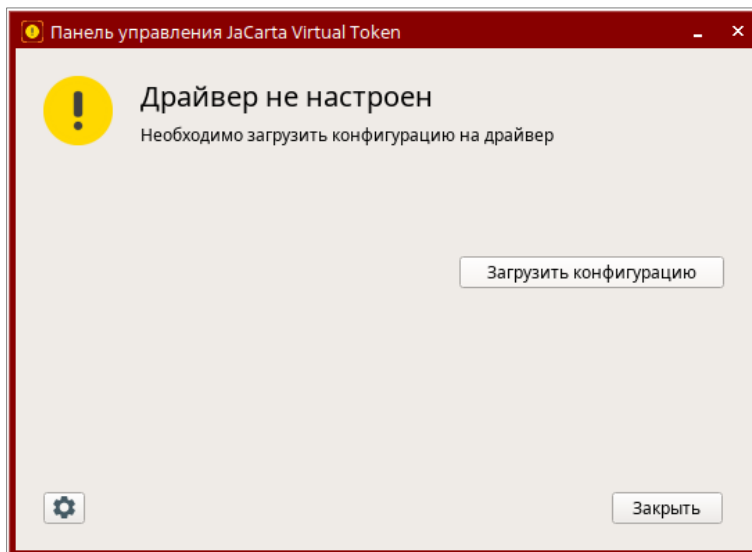


Рисунок 73 - JaCarta Virtual Token. Загрузка конфигурации Сервера JaCarta Virtual Token на Linux

- 7) Выбрать конфигурационный файл `JaCartaVirtualToken.cfg`, созданный ранее.
2. Установка с использованием командной строки. Для установки необходимо выполнить следующие действия:
- Открыть командную строку;
 - Перейти в каталог с установочным файлом и установить его, выполнив команду:

```
sudo yum install JaCartaVirtualToken-x64-x.x.x.x.rpm
```

- для дистрибутивов **Ubuntu, Astra Linux**:

```
sudo apt-get install -f JaCartaVirtualToken-x64-x.x.x.x.deb
```

- После установки будет открыто окно [Панель управления JaCarta Virtual Token], в котором необходимо загрузить конфигурацию с помощью соответствующей кнопки (см. Рисунок 73);
- В открывшемся окне <Выбор файла конфигурации> выбрать конфигурационный файл `JaCartaVirtualToken.cfg`, созданный ранее.

5.3.2 Удаление Клиента JaCarta Virtual Token

Для удаления Клиента JaCarta Virtual Token необходимо выполнить следующие действия:

1. Открыть консоль;
2. Выполнить команду:
 - для дистрибутивов **RedOS**:

```
sudo yum remove JaCartaVirtualToken
```

- для дистрибутивов **Ubuntu, Astra Linux**:

```
sudo apt-get remove JaCartaVirtualToken
```

5.3.3 Обновление Клиента JaCarta Virtual Token

Для обновления Клиента JaCarta Virtual Token до актуальной версии необходимо выполнить следующие действия:

1. Скачать новую версию Клиента JaCarta Virtual Token с сайта Аладдин;
2. Удалить предыдущую версию Клиента JaCarta Virtual Token;
3. Установить новую версию Клиента JaCarta Virtual Token.

5.3.4 Сбор логов

В случае возникновения ошибок в приложении или непредвиденных ситуаций, может возникнуть необходимость сформировать логи.

Сформировать логи можно несколькими способами: из системного трей (область уведомлений) или через проводник файлов.

1. Сбор логов из трей:
 - Открыть трей (область уведомлений);
 - Навести курсор на иконку Панель управления JaCarta Virtual Token;
 - С помощью правой кнопки мыши вызвать контекстное меню и выбрать пункт <Сохранить логи> (см. Рисунок 74);
 - В открывшемся окне выбрать папку сохранения архива с файлами логов.

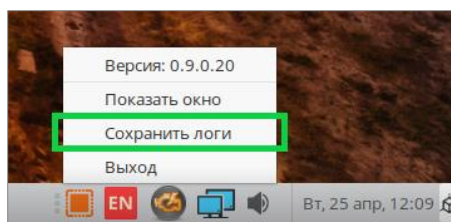


Рисунок 74 - JaCarta Virtual Token. Сбор логов из трей на Linux

2. Сбор логов через проводник файлов:

- Открыть проводник;
- Перейти в директорию `/var/log/JaCartaVirtualToken/`;
- При необходимости скопировать файлы логов в другое место.

Приложение А. Пример конфигурационного файла config.yaml

```
# Конфиграция базы данных
database:
  # Тип БД
  type: sqlite

  # Подключаемая БД
  path: /var/lib/jacarta-virtual-token-server/jacarta-virtual-token-
server.sqlite

  # type: mssql

  # path:
  sqlserver://username:password@host/instance?param1=value&param2=value

  # См. https://github.com/denisenkom/go-mssqldb

  # The connection string can be specified in one of three formats:

  # URL: with sqlserver scheme. username and password appears before
the host. Any instance appears as the first segment in the path. All other
options are query parameters. Examples:

  #
  sqlserver://username:password@host/instance?param1=value&param2=value

  # sqlserver://username:password@host:port?param1=value&param2=value

  #
  sqlserver://sa@localhost/SQLExpress?database=master&connection+timeout=30 //
`SQLExpress instance.

  #
  sqlserver://sa:mypass@localhost?database=master&connection+timeout=30 //
username=sa, password=mypass.

  #
  sqlserver://sa:mypass@localhost:1234?database=master&connection+timeout=30 //
port 1234 on localhost.

  # sqlserver://sa:my%7Bpass@somehost?connection+timeout=30 //
password is "my{pass}"

  # ADO: key=value pairs separated by ;. Values may not contain ;,
leading and trailing whitespace is ignored. Examples:

  # server=localhost\\SQLExpress;user id=sa;database=master;app
name=MyAppName

  # server=localhost;user id=sa;database=master;app name=MyAppName

  # ODBC: Prefix with odbc, key=value pairs separated by ;. Allow ;
by wrapping values in {}. Examples:
```

```
# odbc:server=localhost\\SQLExpress;user id=sa;database=master;app
name=MyAppName

# odbc:server=localhost;user id=sa;database=master;app
name=MyAppName

# odbc:server=localhost;user id=sa;password={foo;bar} // Value
marked with {}, password is "foo;bar"

# odbc:server=localhost;user id=sa;password={foo{bar} // Value
marked with {}, password is "foo{bar}"

# odbc:server=localhost;user id=sa;password={foobar } // Value
marked with {}, password is "foobar "

# odbc:server=localhost;user id=sa;password=foo{bar // Literal {,
password is "foo{bar"

# odbc:server=localhost;user id=sa;password=foo}bar // Literal },
password is "foo}bar"

# odbc:server=localhost;user id=sa;password={foo{bar} // Literal {,
password is "foo{bar"

# odbc:server=localhost;user id=sa;password={foo}}bar} // Escaped }
with }}`, password is "foo}bar"

# type: postgresql

# path: postgres://username:password@host:5432/database_name

licensing:

# количество дней до истечения срока действия для индикации желтым цветом
snValidToWarningPeriodDays: 14

# количество дней до истечения срока действия для индикации красным цветом
snValidToDangerPeriodDays: 7

# возможность отображения QR-кодов серийных номеров в административном
интерфейсе
snQrCodeAdminAccess: false

# возможность редактировать e-mail-ы серийных номеров из административного
интерфейса
snEmailEditAccess: false

# Конфигурация private-сервера
privateServer:

# Адрес запуска сервера. Если не указан - сервер не будет запускаться

# address: "localhost:6787" # полный адрес

address: ":6787" # только порт
```

```
# Адрес сервера, который будет отправляться пользователям в e-mail. Это
может быть как адрес сервера, так и адрес прокси-сервера.

externalAddress: http://jcvr-admin.ru:6787

# Язык возвращаемых ошибок: ru/en. По умолчанию: ru
errorLanguage: ru

# Настройки TLS
# tls:

# # Вариант 1. TLS с использованием сертификата и закрытого ключа
# cert:

# # Путь до сертификата
# certificate: ../wks218.aladdin.ru.crt
# #certificate: ../wks218-root.crt
# #certificate: ../trustedcert.crt
# # Путь до закрытого ключа
# privateKey: ../wks218.aladdin.ru_pvk.pem
# #privateKey: ../wks218-root_pvk.pem
# #privateKey: ../trustedcert.key

# # Вариант 2. TLS с использованием PFX контейнера
# pfx:

# # Путь до PFX контейнера
# pfxContainer: ../trustedcert.pfx
# # Пароль от PFX контейнера
# pwdContainer: "1234567890"

# Конфигурация api-сервера
apiServer:

# Адрес сервера, к которому будут обращаться клиенты. Это может быть как
адрес сервера, так и адрес прокси-сервера.
# Этот адрес будет добавляться в QR-код.
externalAddress: http://jcvr-transport.ru:6788

# Адрес запуска сервера
```

```
# address: "localhost:6788" # полный адрес
address: ":6788" # только порт

# Язык возвращаемых ошибок: ru/en. По умолчанию: ru
errorLanguage: ru

# # Настройки TLS
# tls:
# # Вариант 1. TLS с использованием сертификата и закрытого ключа
# cert:
# # Путь до сертификата
# certificate: tls/privateServer/localhost_9000_cert.pem
# # Путь до закрытого ключа
# privateKey: tls/privateServer/localhost_9000_key.pem
#
# # Вариант 2. TLS с использованием PFX контейнера
# pfx:
# # Путь до PFX контейнера
# pfxContainer: tls/privateServer/localhost_9000.pfx
# # Пароль от PFX контейнера
# pwdContainer: "1234567890"

# Конфигурация websocket-сервера
transportServer:
# Адрес сервера, к которому будут обращаться клиенты. Это может быть как
адрес сервера, так и адрес прокси-сервера.
# Этот адрес будет добавляться в QR-код.
externalAddress: ws://jcvt-transport.ru:6789

# Адрес запуска сервера
# address: "localhost:6789" # полный адрес
address: ":6789" # только порт

# Язык возвращаемых ошибок: ru/en. По умолчанию: ru
errorLanguage: ru
```



```
# # Настройки TLS

# tls:

# # Вариант 1. TLS с использованием сертификата и закрытого ключа

# cert:

# # Путь до сертификата

# certificate: tls/privateServer/localhost_9000_cert.pem

# # Путь до закрытого ключа

# privateKey: tls/privateServer/localhost_9000_key.pem

# # Вариант 2. TLS с использованием PFX контейнера

# pfx:

# # Путь до PFX контейнера

# pfxContainer: tls/privateServer/localhost_9000.pfx

# # Пароль от PFX контейнера

# pwdContainer: "1234567890"

# Настройки отправки e-mail

email:

# Тема письма для отправки QR-кода на активацию серийного номера

snQrCodeSubject: "Активация серийного номера JCVT"

# Путь к файлу с шаблоном письма для отправки QR-кода на активацию
серийного номера

snQrCodeTemplate: ./sn_qr_code_template.html

# Размер картинки QR-кода на активацию серийного номера. По умолчанию: 300

snQrCodeSize: 300

# Настройки сервера отправки e-mail

server:

# Включить отправку e-mail

enable: true

# Использовать TLS. По умолчанию: false

tls: true
```

```
# Адрес SMTP-сервера
smtp: smtp.example.ru

# Адрес отправителя
#from: jcvt@example.ru
# Если авторизация на требуется - не указывать
from: JCVT <jcvt@example.ru>

# Логин на SMTP-сервере
# Если авторизация на требуется - не указывать
login: login

# Пароль на SMTP-сервере
password: password
```

Контакты

Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, 7 этаж, компания "Аладдин Р.Д."

Телефон: +7 (495) 223-00-01 (секретарь)

E-mail: aladdin@aladdin.ru (общий)

Web: <https://www.aladdin.ru>

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

Техническая поддержка

Контакты службы техподдержки:

Телефон: +7 (499) 702-39-68

Web: www.aladdin.ru/support/

Список литературы

- 1 JaCarta Virtual Token. Руководство пользователя

Регистрация изменений

Версия документа	Изменения
1.4	<p>В связи с реализованной функциональностью изменен п. «Режимы выдачи серийных номеров».</p> <p>Добавлены п. «Запрос серийного номера», «Статус серийного номера»;</p>
1.3	<p>В рамках выхода релиза 1.1.0 внесены следующие изменения:</p> <ul style="list-style-type: none">• Добавлен п. «Режимы выдачи серийных номеров»;• Добавлен п. «Специальные порты»;• Добавлен п. «Прокси-соединение»;• Добавлен п. «Перезапись конфигурационного файла»;• Добавлен п. «Приложение А. Пример конфигурационного файла config.yaml»
1.2	<p>Приведение документа к корпоративному формату</p>
1.1.	<p>Добавлено разделение по ОС - Windows, Linux. Добавлены сценарии: Удаление, Обновление, Сбор логов, Обновление конфигурационного файла, Установка (для Linux). Добавлено описание администрирования функциональности Сервера JaCarta Virtual Token.</p>
1.0	<p>Исходная версия документа для JCVT</p>