6. Создание сертификатов из веб-интерфейса администратора

Подключение клиентов возможно двумя способами:

1) с помощью физического ключа Рутокен;

2) с помощью мобильного устройства.

Подключение с помощью физического ключа Рутокен

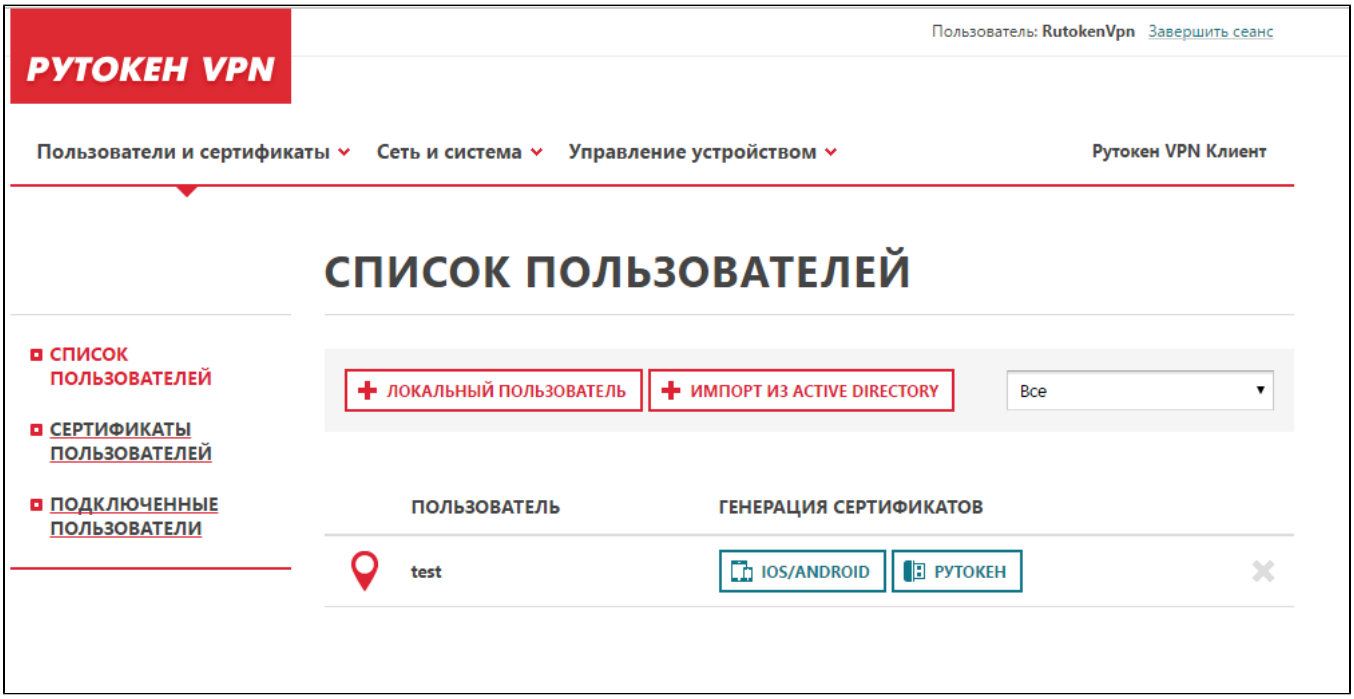
Обычно используется для компьютера или ноутбуков на базе ОС Windows или macOS.

Для этого подключения необходимы:

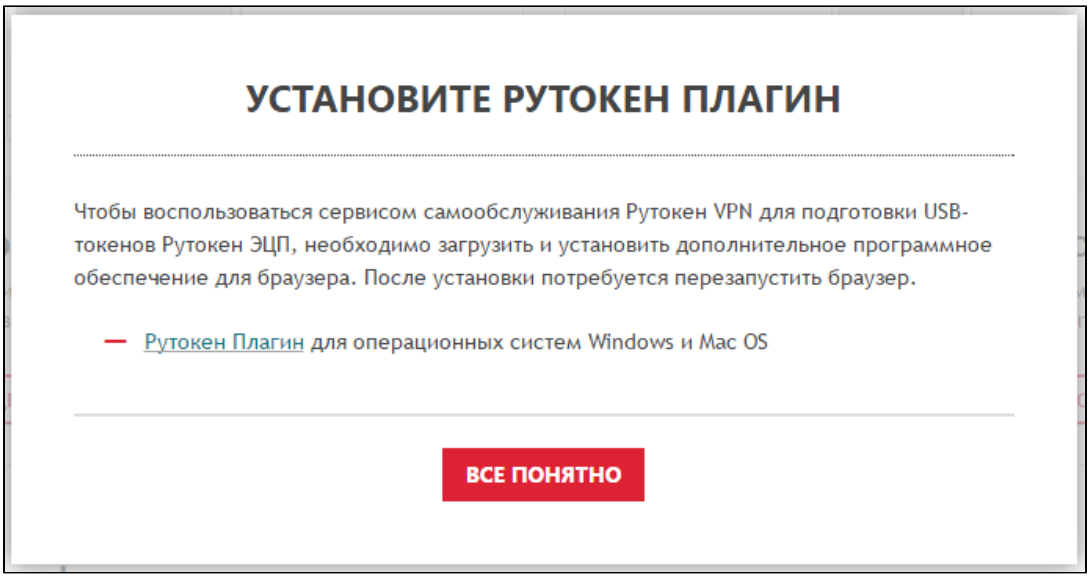
- Рутокен с действующим сертификатом.
- Программа Рутокен VPN Клиент, установленная на компьютере.
- Конфигурационный файл для настройки Рутокен VPN Клиента

1) Для генерации сертификата и конфигурационного файла, перейдите на вкладку "Пользователи и сертификаты" и выберите "Список пользователей".

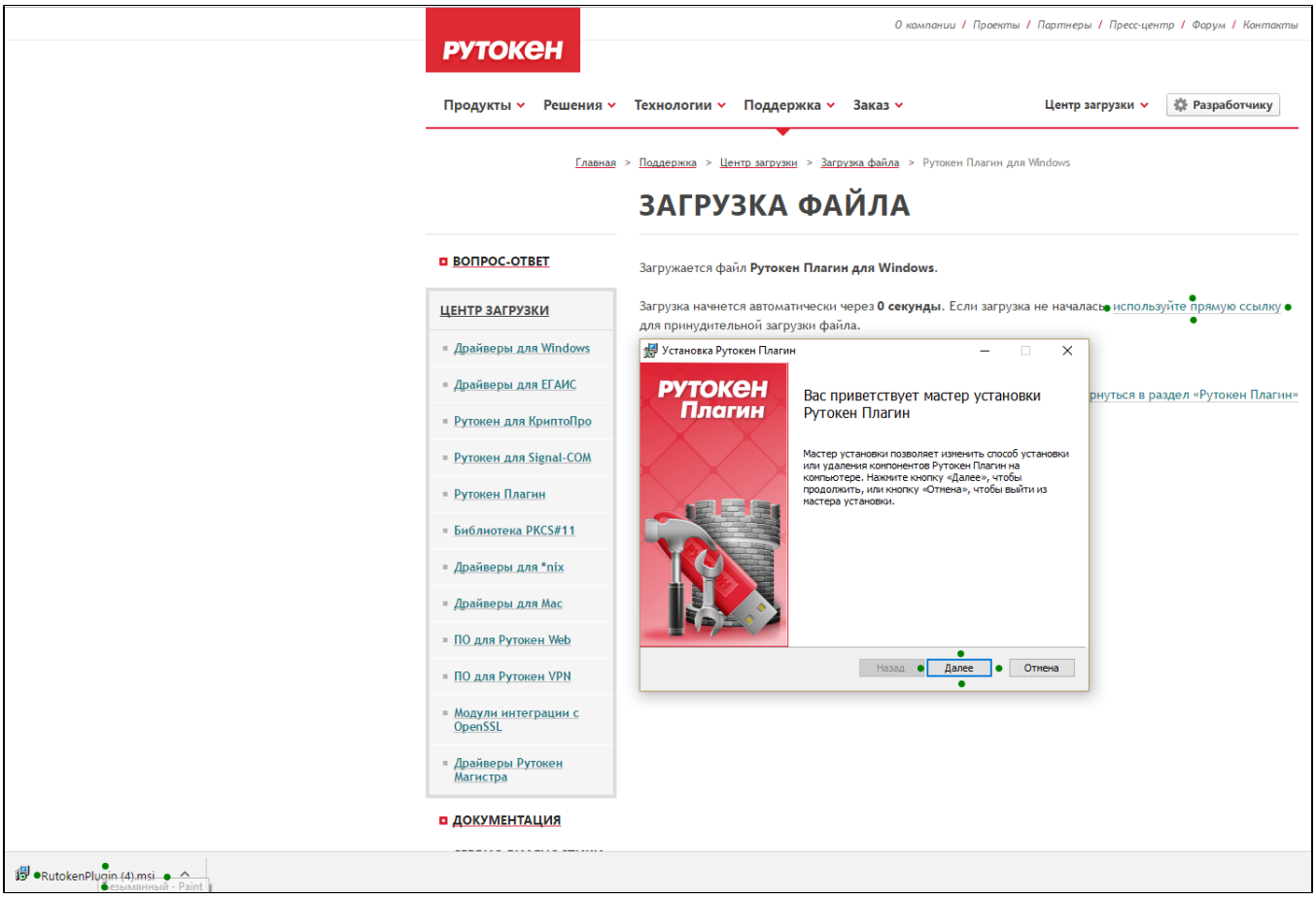
Напротив нужного пользователя нажмите "Рутокен".



2) Для генерации сертификата на Рутокен, необходимо установить на компьютер Рутокен Плагин и включить в браузере расширение Адаптер Рутокен Плагин.

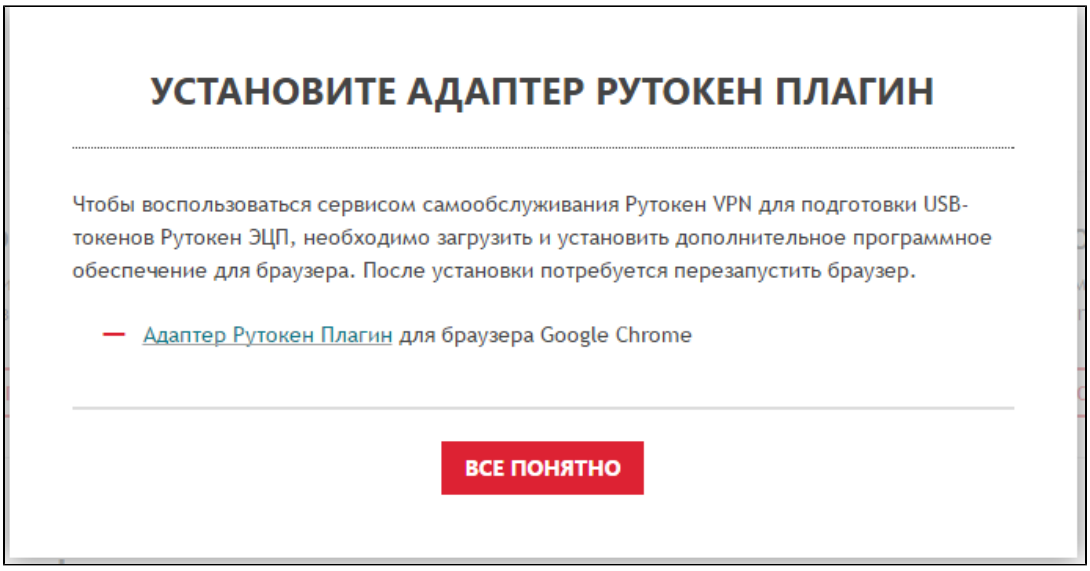


Перейдите по специальной ссылке на странице и выполните установку.



Если Рутокен Плагин уже был установлен, переходите к следующему шагу.

3) Установите и включите в браузере Адаптер Рутокен Плагин.

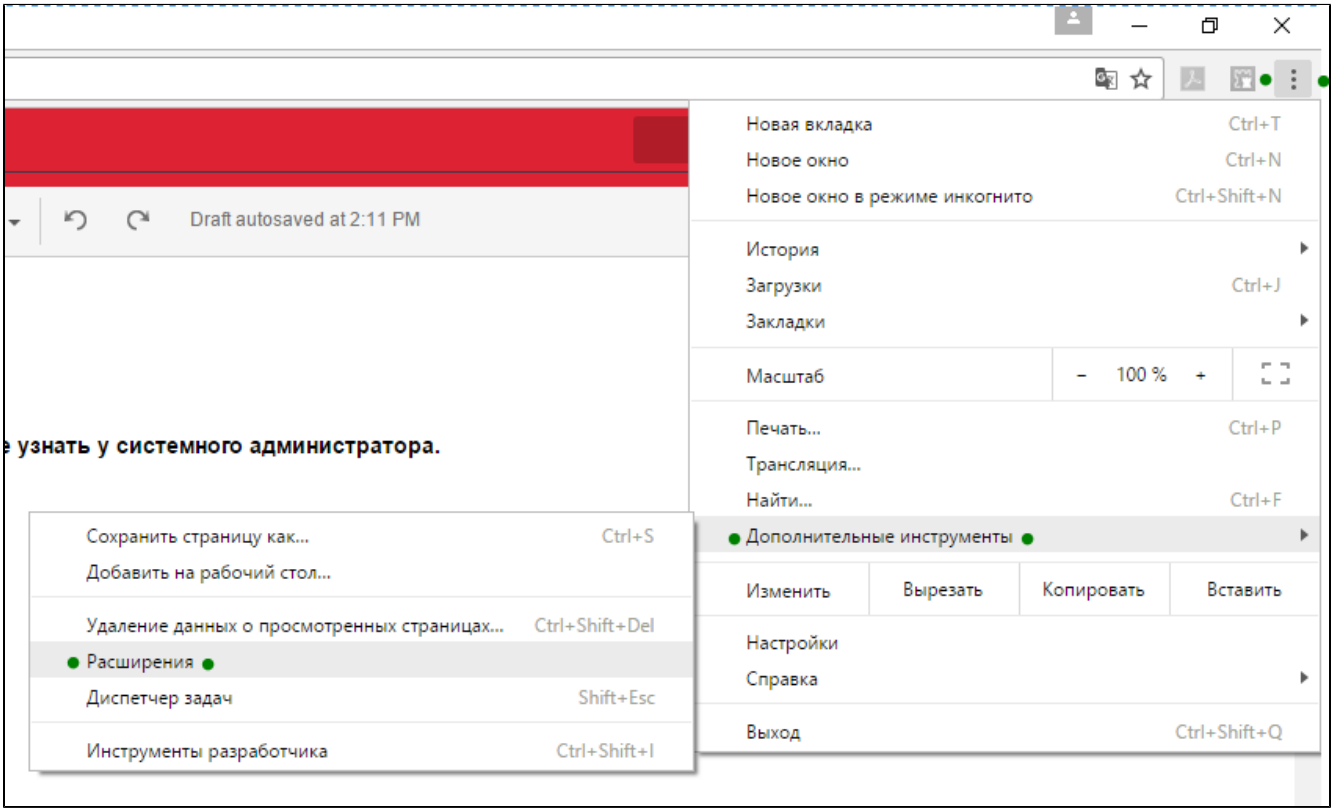


Для браузера Google Chrome

1) Установите расширение Адаптер Рутокен Плагин

2) Если расширение Адаптер Рутокен Плагин уже установлено, но окно все равно отображается, то выполните одно из действий:

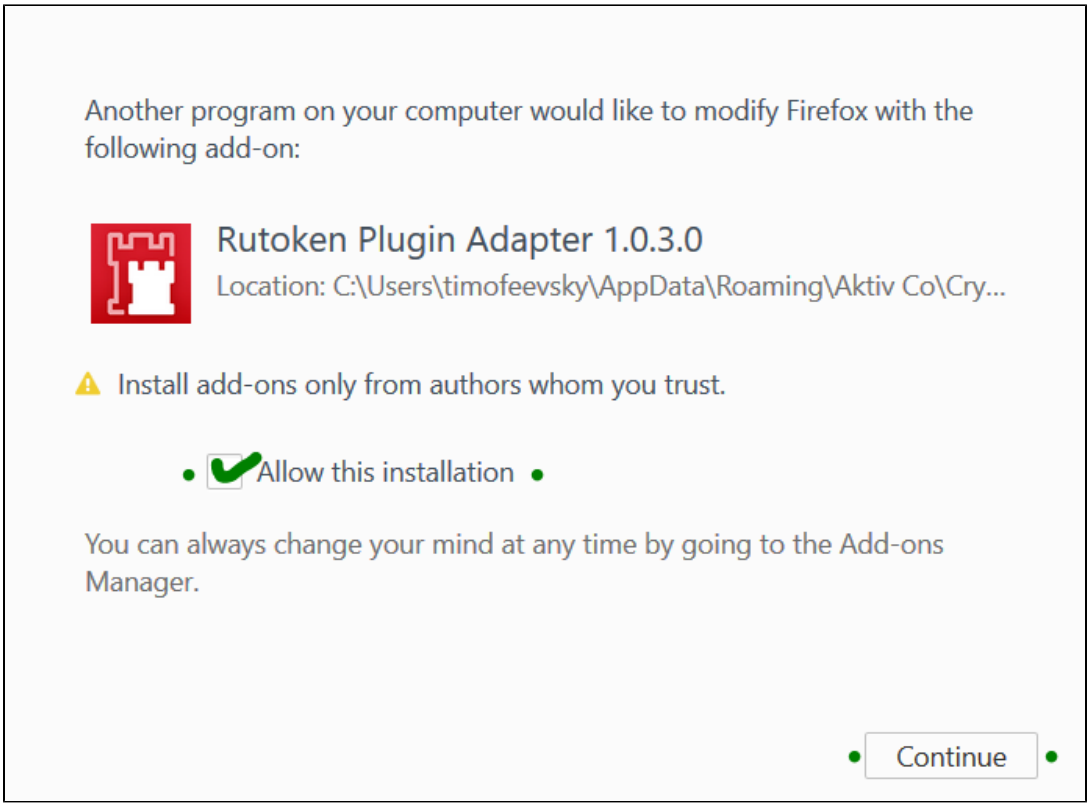
- Пройдите по ссылке и в верхней части окна нажмите "Включить".
- Включите адаптер в настройках браузера : Дополнительные инструменты - Расширения - Адаптер Рутокен Плагин.



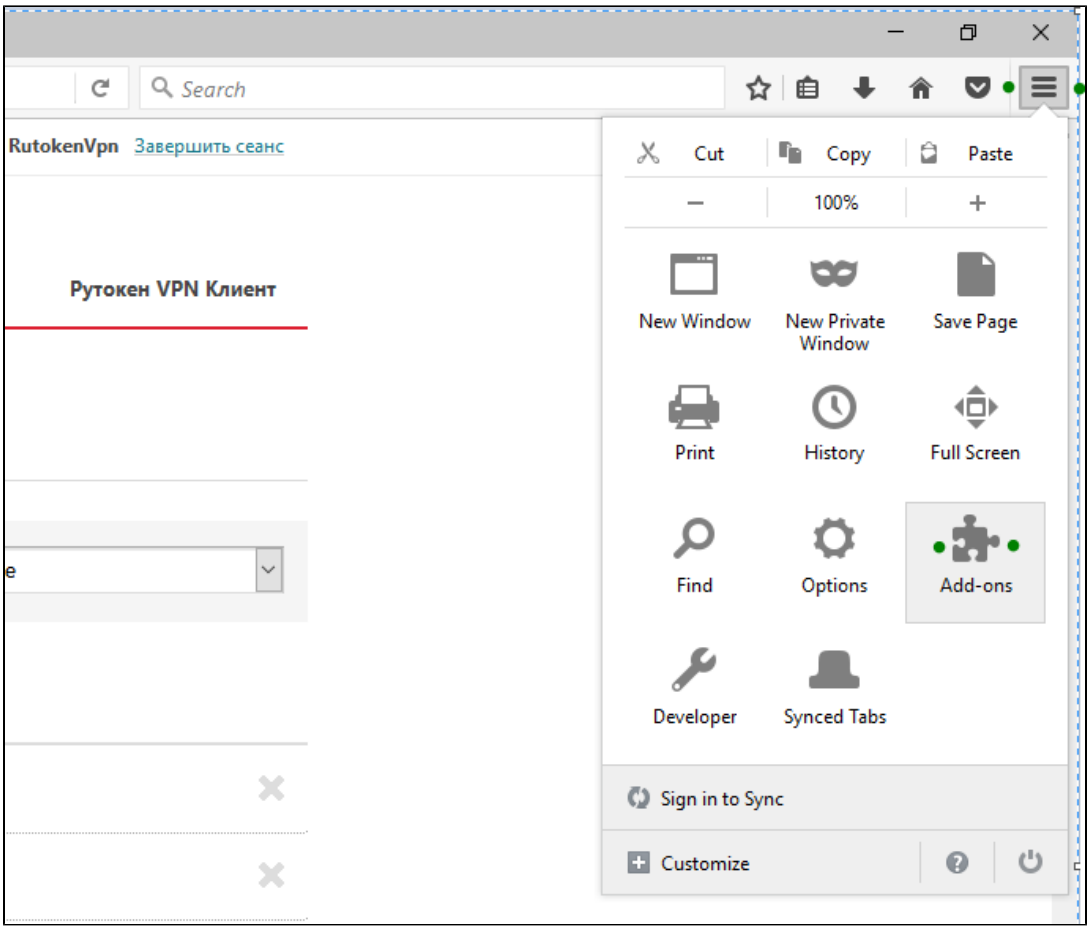
Для браузера Mozilla Firefox

Зайдите в расширения и включите расширение Адаптер Рутокен Плагин.

После установки Рутокен Плагина при первом запуске, в браузере отобразится окно с сообщением о разрешении установить Адаптер Рутокен Плагин. Разрешите установку.



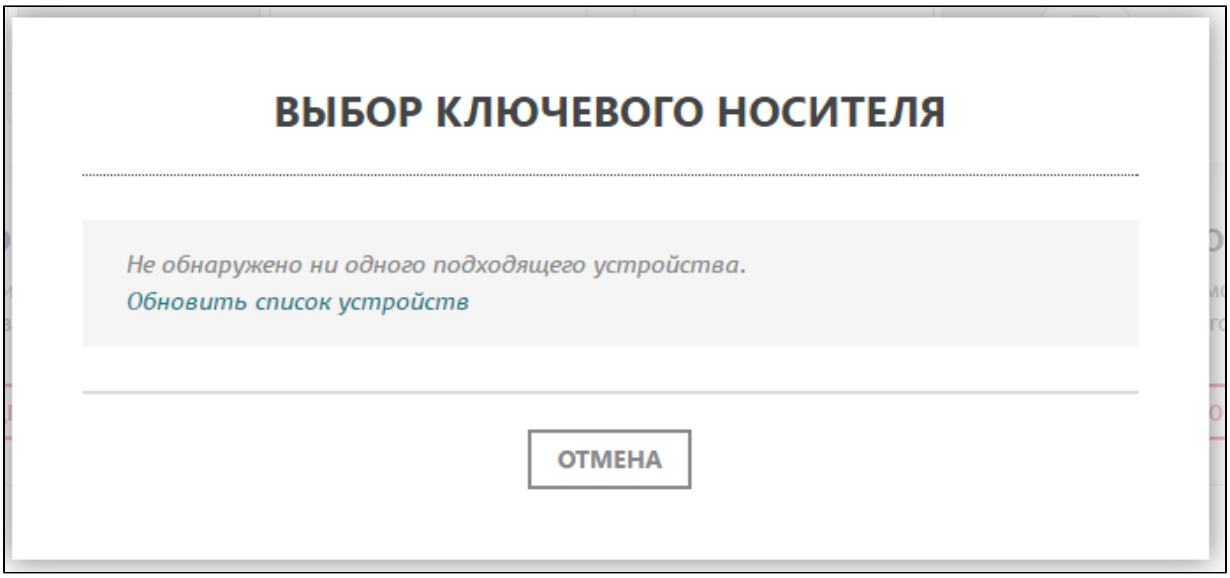
Если по какой то причине пропустили это окна, то зайдите в расширения и включите Адаптер Рутокен Плагин.

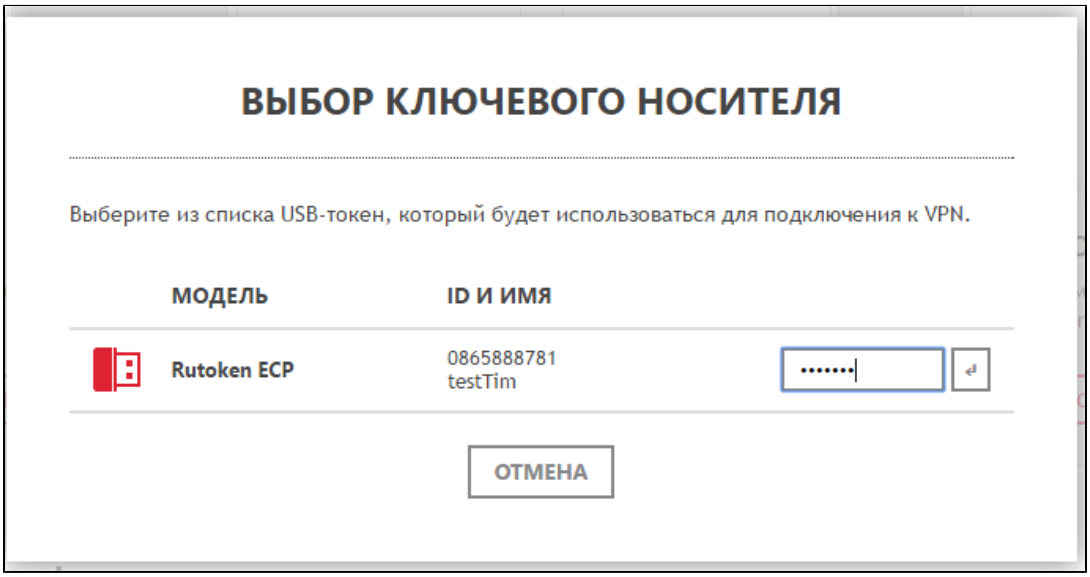


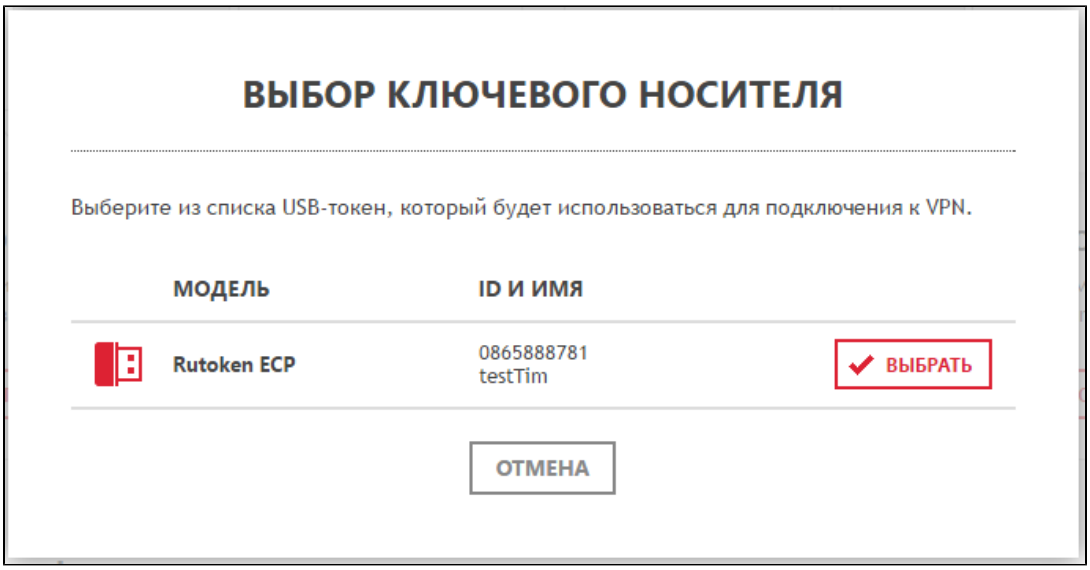
4) Подключите Рутокен к компьютеру и обновите список устройств.

5) Введите PIN-код устройства.

6) Рядом с ID необходимого устройства нажмите "Выбрать".





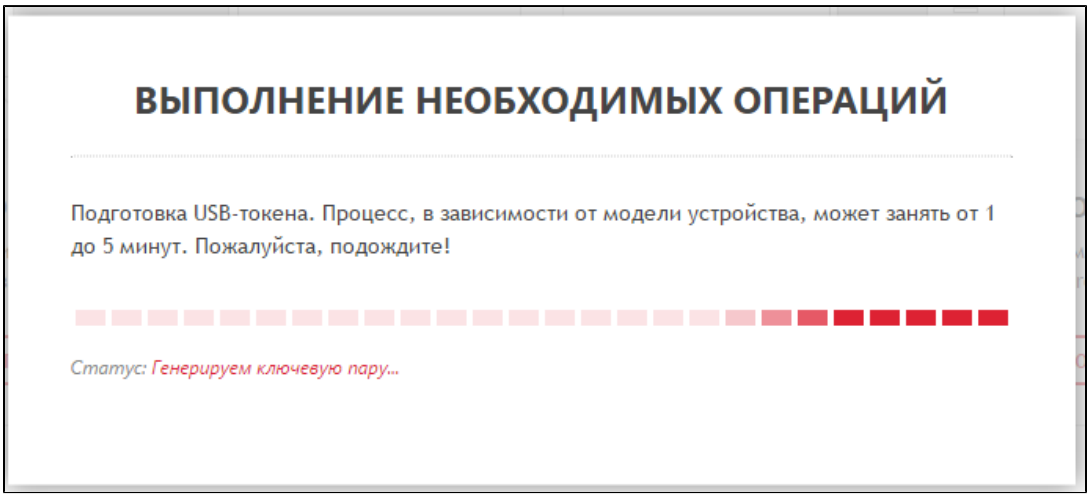


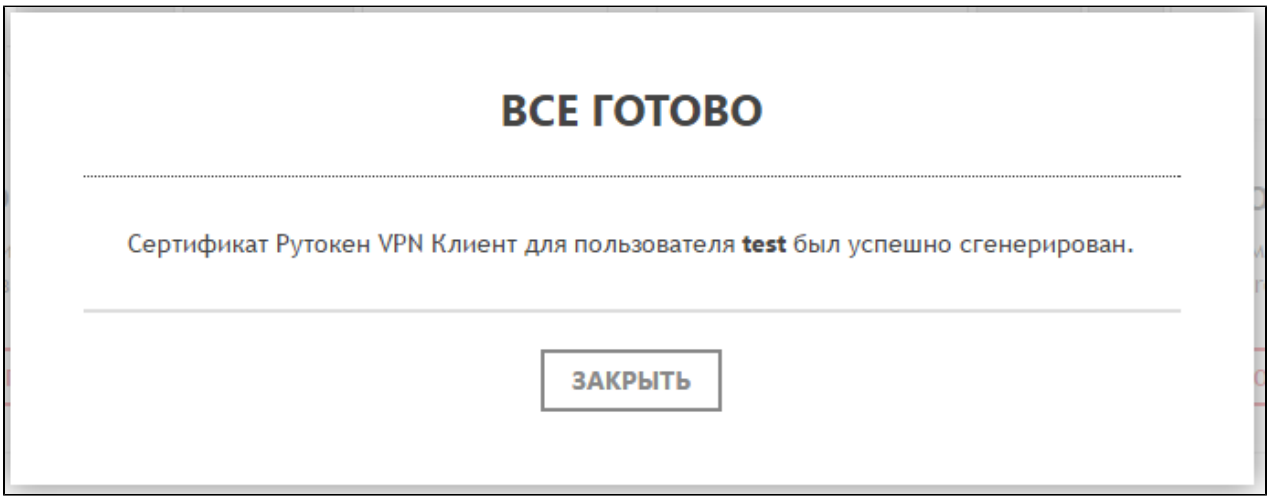
7) Дождитесь окончания процесса генерации сертификата.

Обычно этот процесс занимает от 30 секунд до 5 минут, это зависит от модели Рутокена.

Пользовательский сертификат имеет стандартный срок действия 2 года.

При необходимости можно удалить пользовательский сертификат с сервера, после этого подключение по данному сертификату установить будет невозможно.

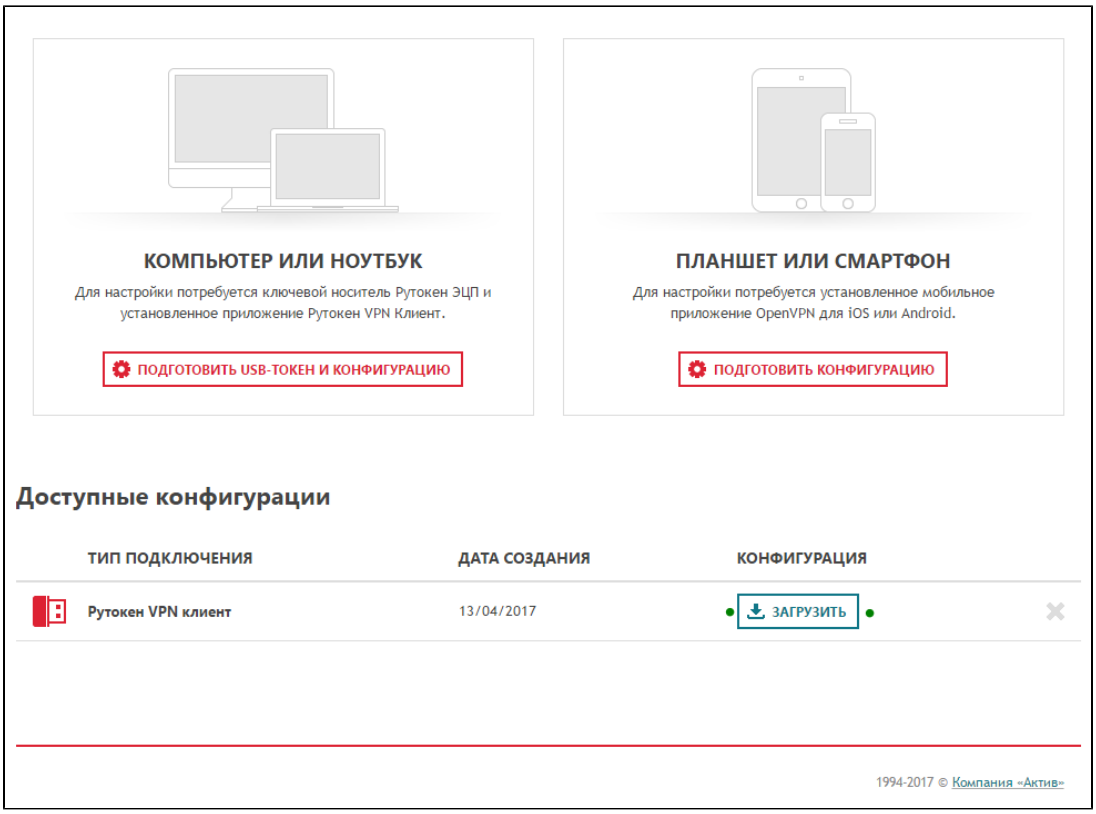




8) Загрузите конфигурационный файл.

Для этого в строке с необходимой конфигурацией нажмите "Загрузить".

9) Сохраните его на внешний носитель для передачи сотруднику или отправьте по электронной почте.

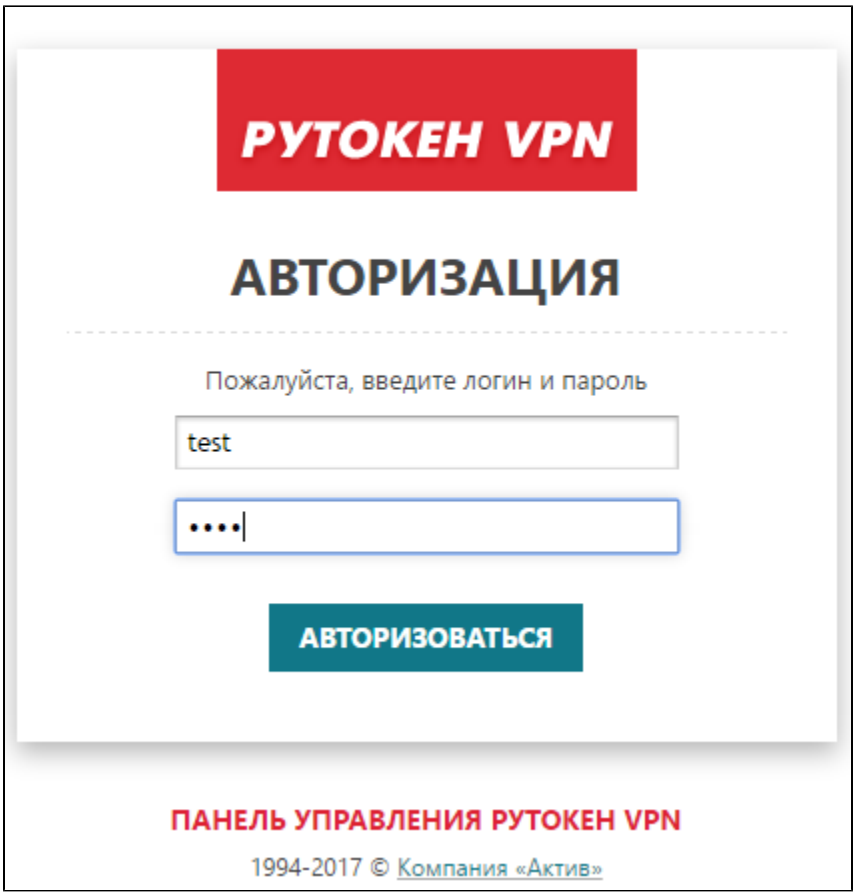


Подключение с помощью мобильного устройства

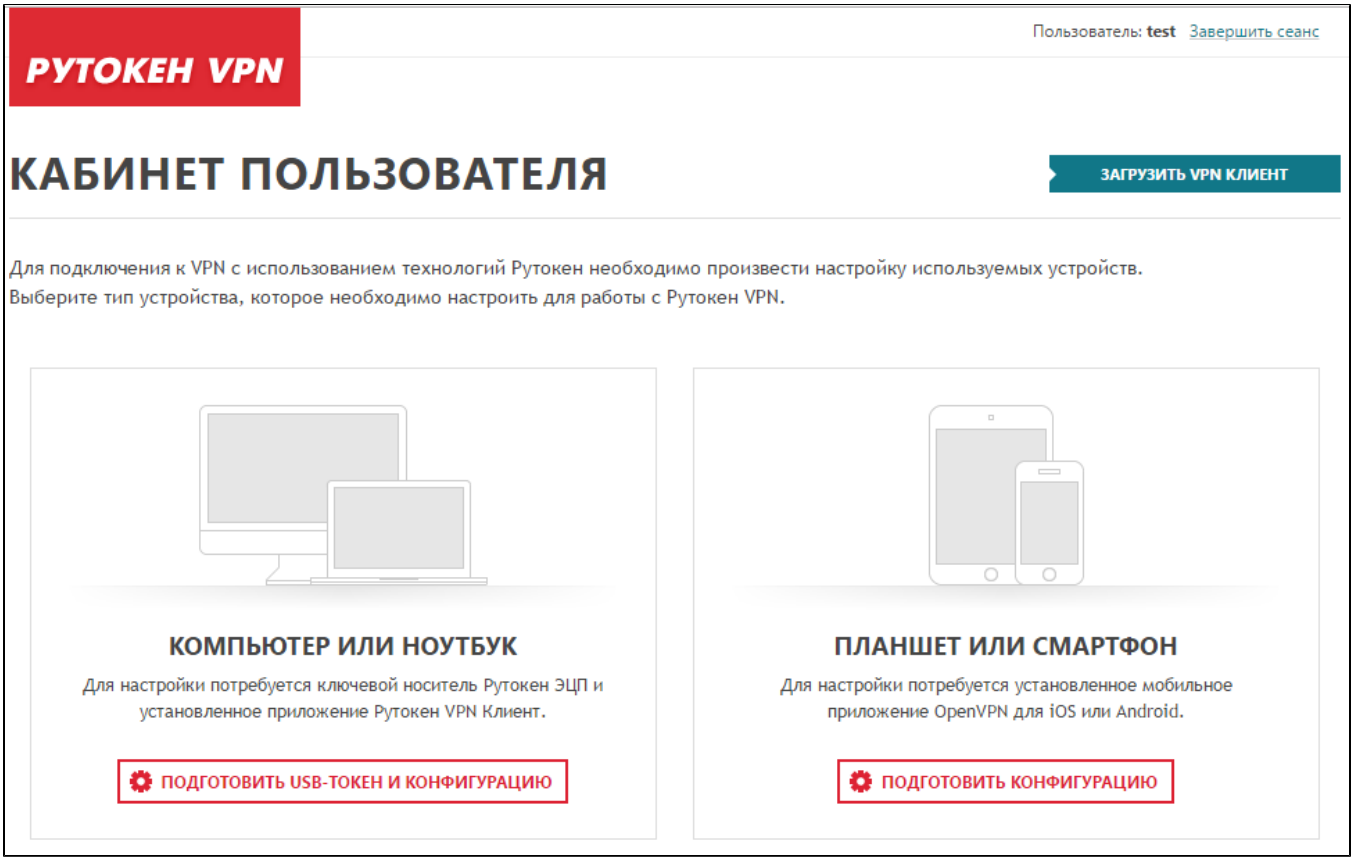
Данный тип подключения доступен в интерфейсе только в RSA-режиме конфигурации Центра Сертификации.

1) Войдите в свой личный кабинет с устройства, которое находится в корпоративной сети.

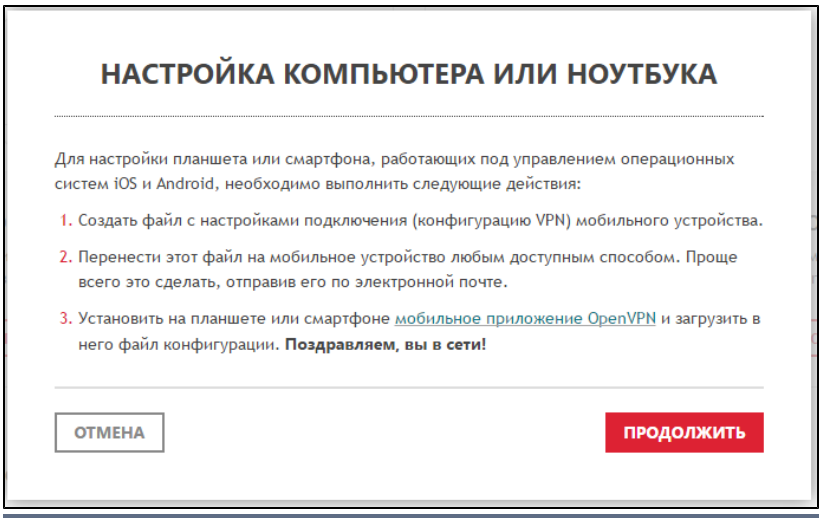
Логин и пароль вам необходимо узнать у своего системного администратора.



2) Выберите тип устройства - Планшет или смартфон.



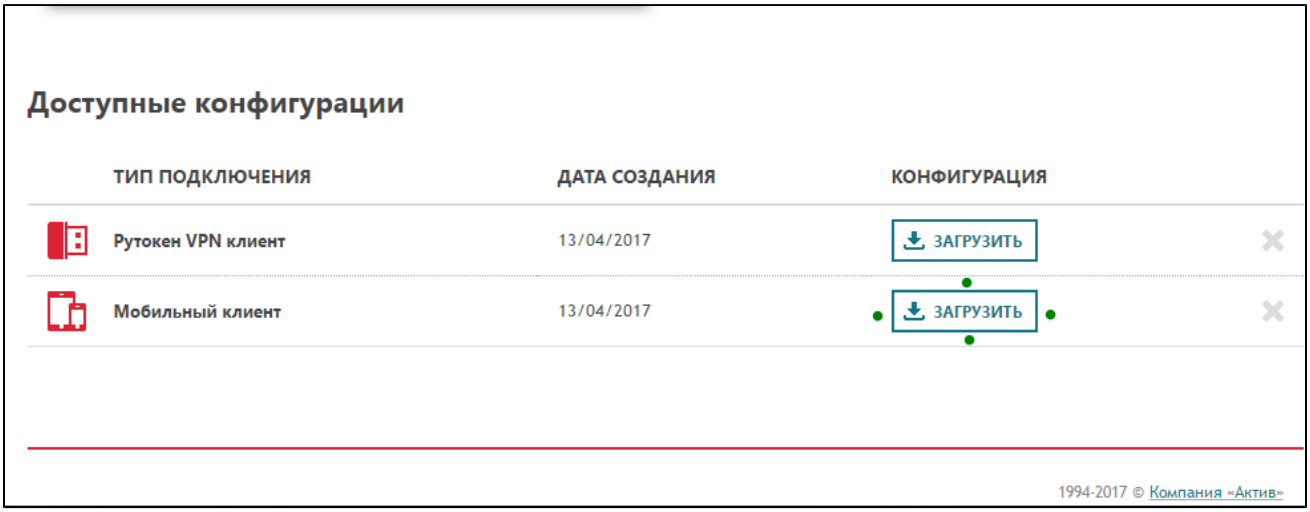
Ознакомьтесь с тремя шагами настройки и нажмите "Продолжить".



3) Загрузите конфигурационный файл для мобильного клиента.

Для этого нажмите "Загрузить".

4) Сохраните его на внешний носитель для передачи сотруднику или отправьте по электронной почте.


Доступные конфигурации
ТИП ПОДКЛЮЧЕНИЯ
ДАТА СОЗДАНИЯ
КОНФИГУРАЦИЯ
Рутокен VPN клиент
13/04/2017
ЗАГРУЗИТЬ
Мобильный клиент
13/04/2017
ЗАГРУЗИТЬ
1994-2017 © Компания «Актив»

Назад Далее