JAS и JaCarta WebPass для OTP-аутентификации в Linux SSH

Интеграционная инструкция

Версия продукта:	1.0
Версия документа:	1.0
Редакция от:	15 мая 2017 г.
Статус:	Внешний документ
Листов:	255
Автор:	Timofey Alekseev

Аннотация

В настоящем документе описаны основные этапы настройки аутентификации в Linux SSH для замены парольной аутентификации одноразовыми паролями.

Оглавление

Сценарий 4
Используемое для демонстрации окружение 4
Требования к окружению 4
Настройка на стороне RADIUS сервера 7
Подготовка JaCarta WebPass 10
Настройка на стороне JAS 15
Настройка на стороне Linux Server 19
Проверка решения 20
Контакты, техническая поддержка 23
Регистрация изменений 24

Сценарий

В настоящем документе описан сценарий аутентификации в сессию SSH-подключения к Linux OS посредством одноразовых паролей с использованием устройства JaCarta WebPass. Сценарий подразумевает использование RADIUS сервера для проверки подлинности введённого одноразового кода, а также системы проверки OTP-значения. В качестве системы управления OTP-ключами мы будем использовать JaCarta Authentication Server (JAS).

Пользователь, при установленном SSH-соединении, на этапе аутентификации будет вводить OTP-значение вместо пароля. PAM модуль отправит переданное значение на RADIUS Server, который проверит его и разрешит, либо запретит аутентификацию.

Используемое для демонстрации окружение

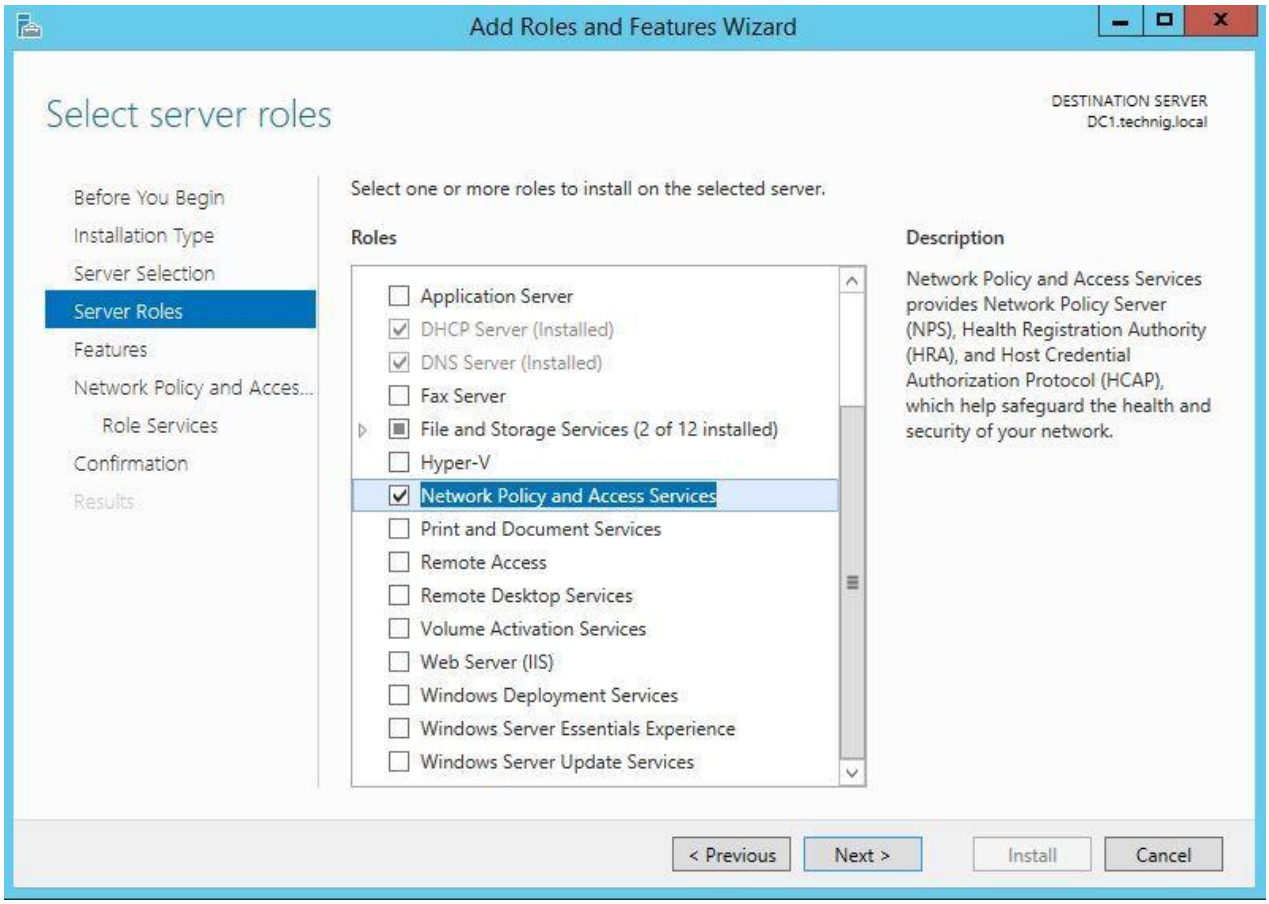
В данной инструкции производится настройка для следующих версий операционных систем:

- Microsoft Windows Server 2012;
- Ubuntu Server 16;
- Microsoft Windows 7.

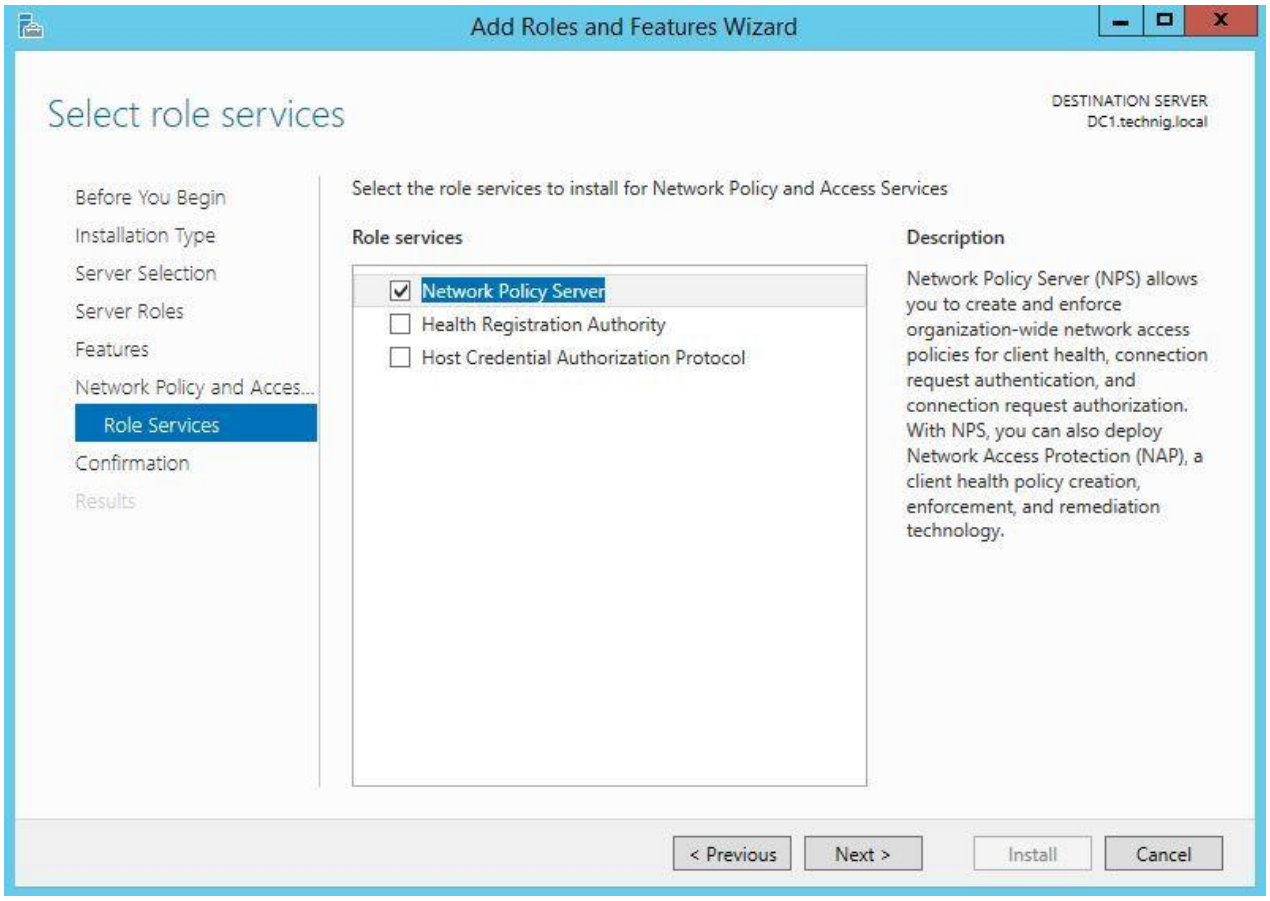
Требования к окружению

Для Windows Server необходимо создать домен, добавить роль NPS. Для этого следуйте советам ниже.

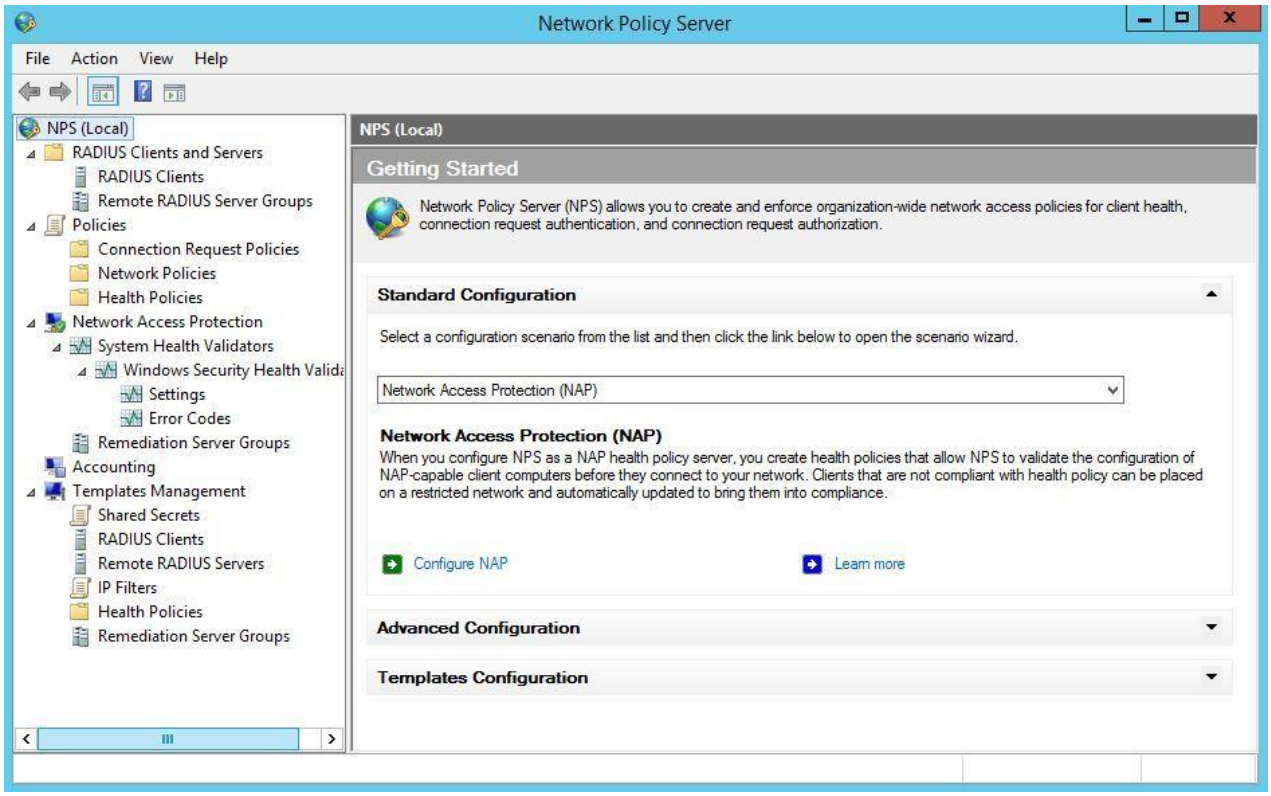
Откройте оснастку для добавления роли NPS.



При выборе служб и компонентов выберите Network Policy Server.



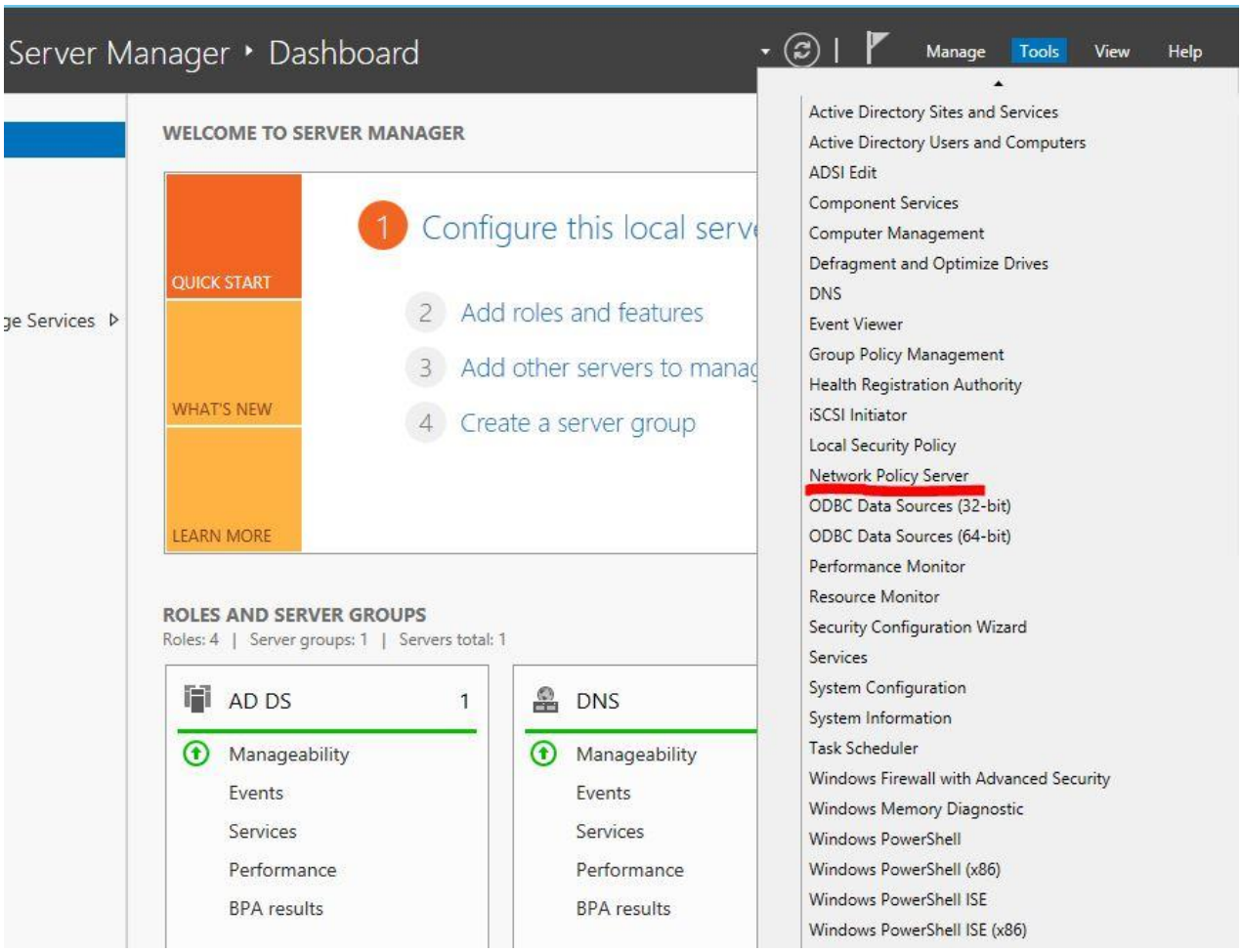
После этого вам станет доступна оснастка NPS.



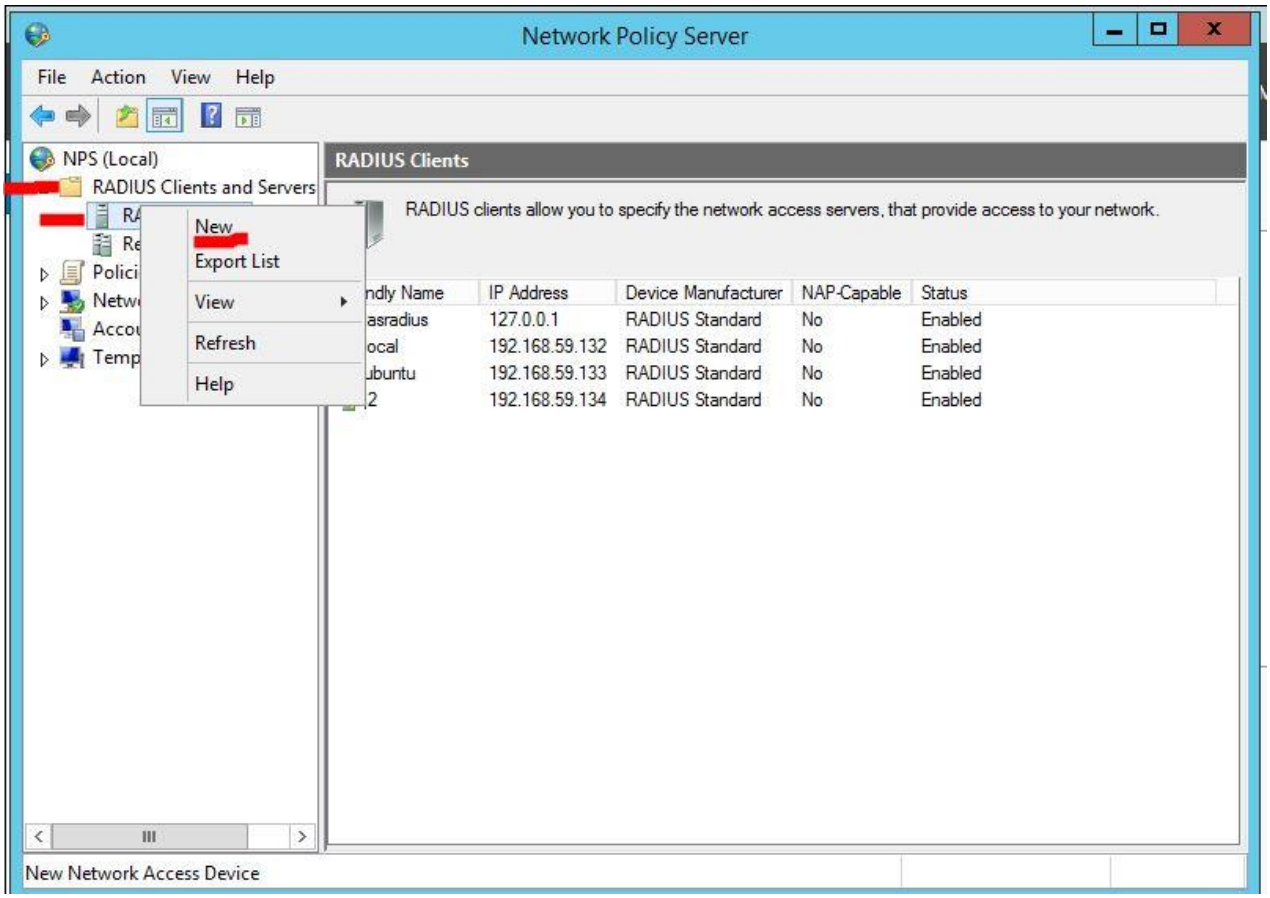
Настройка на стороне RADIUS сервера

На стороне сервера необходимо выполнить следующие шаги:

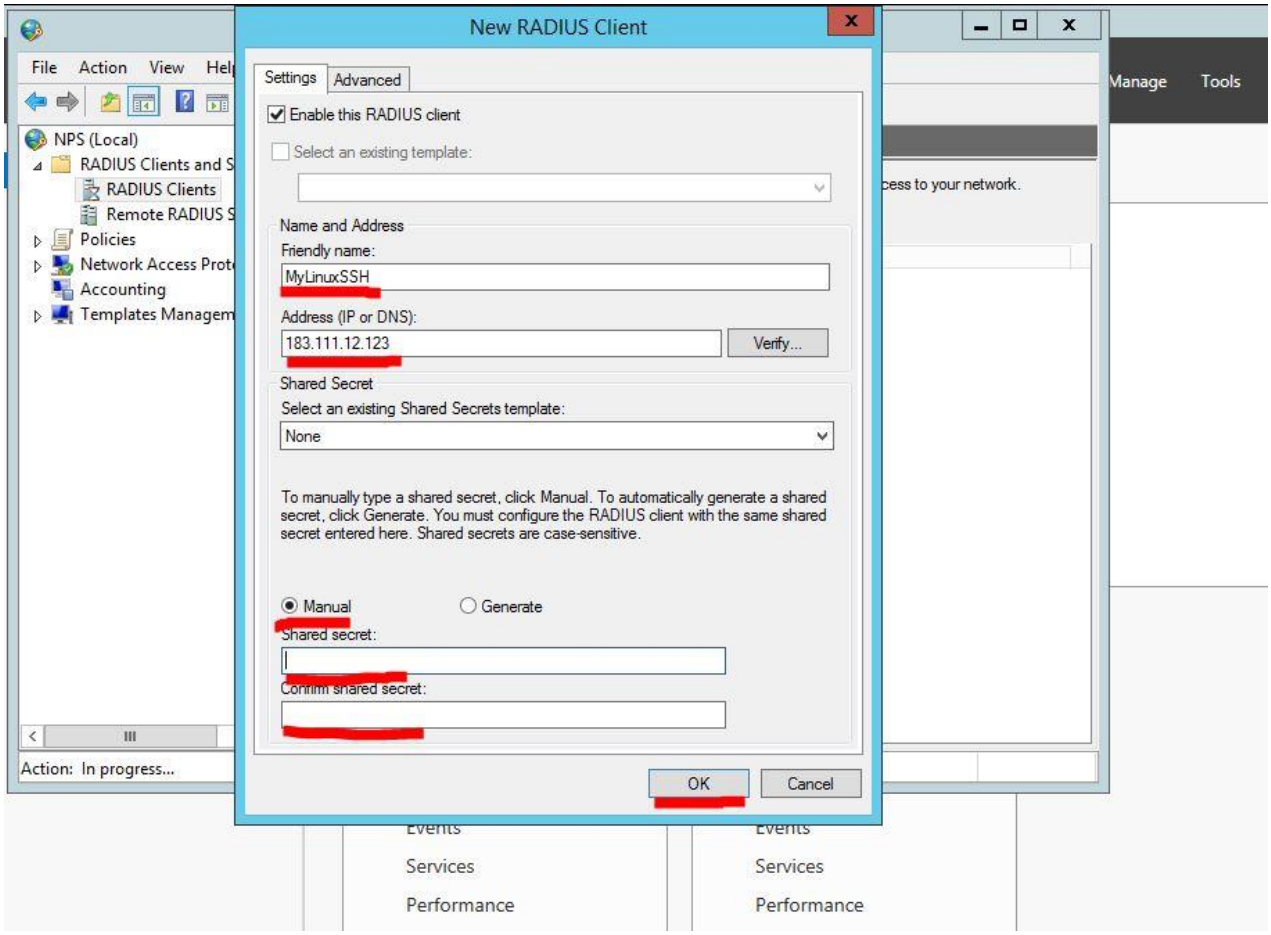
- добавьте радиус клиента с IP-адресом, либо именем Linux сервера;
- выберите оснастку NPS на сервере.



В меню оснастки выберите пункт NPS – RADIUS Clients and Servers – RADIUS Clients, затем правым кликом вызовите контекстное меню и нажмите New.



Введите настройки клиента для подключения к RADIUS серверу: имя, отображаемое в оснастке, адрес либо имя клиента, общий секрет для клиента и сервера (необходимо придумать).

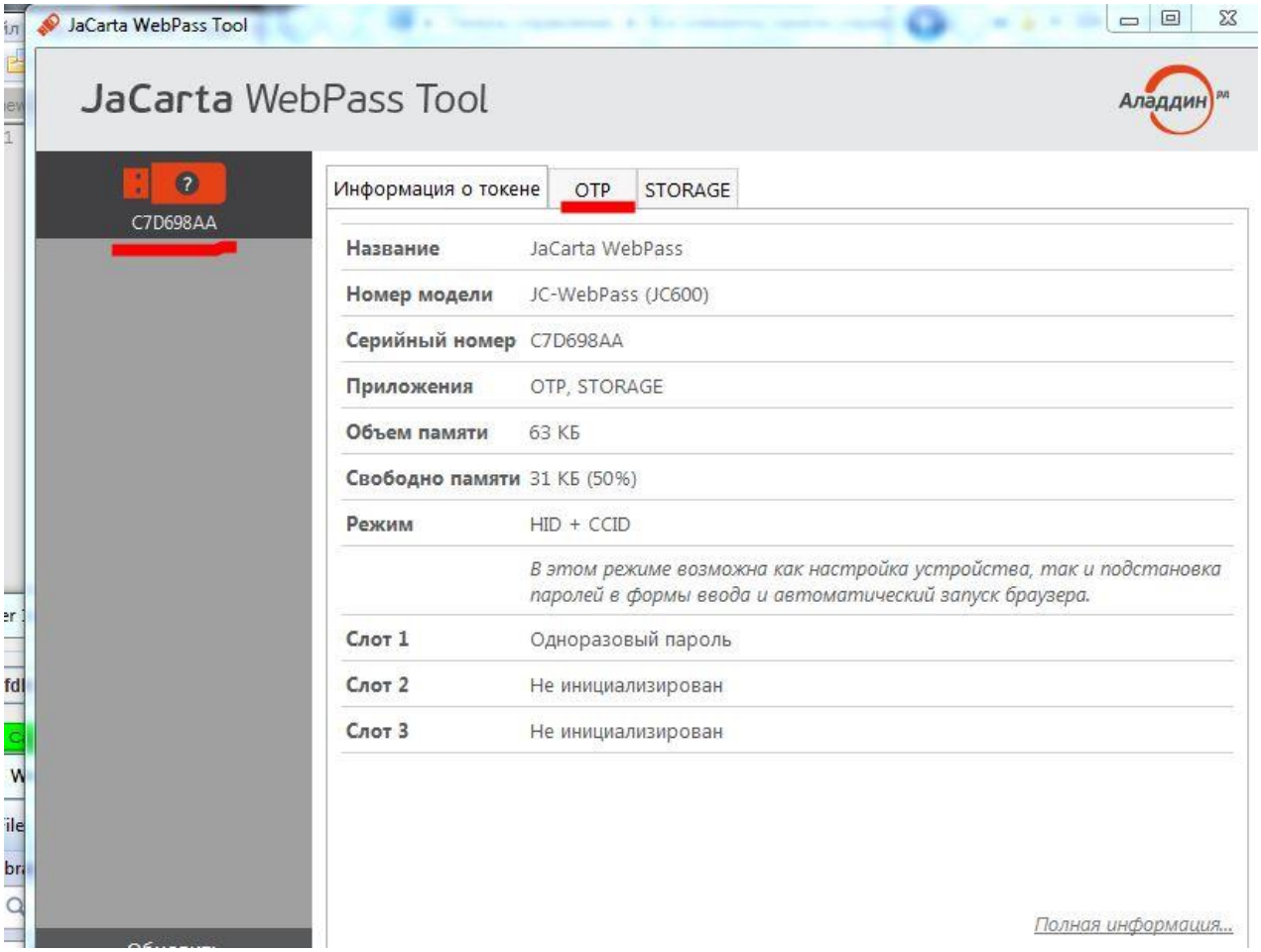


Создайте доменного пользователя, имя которого будет использоваться для аутентификации на Linux сервере.

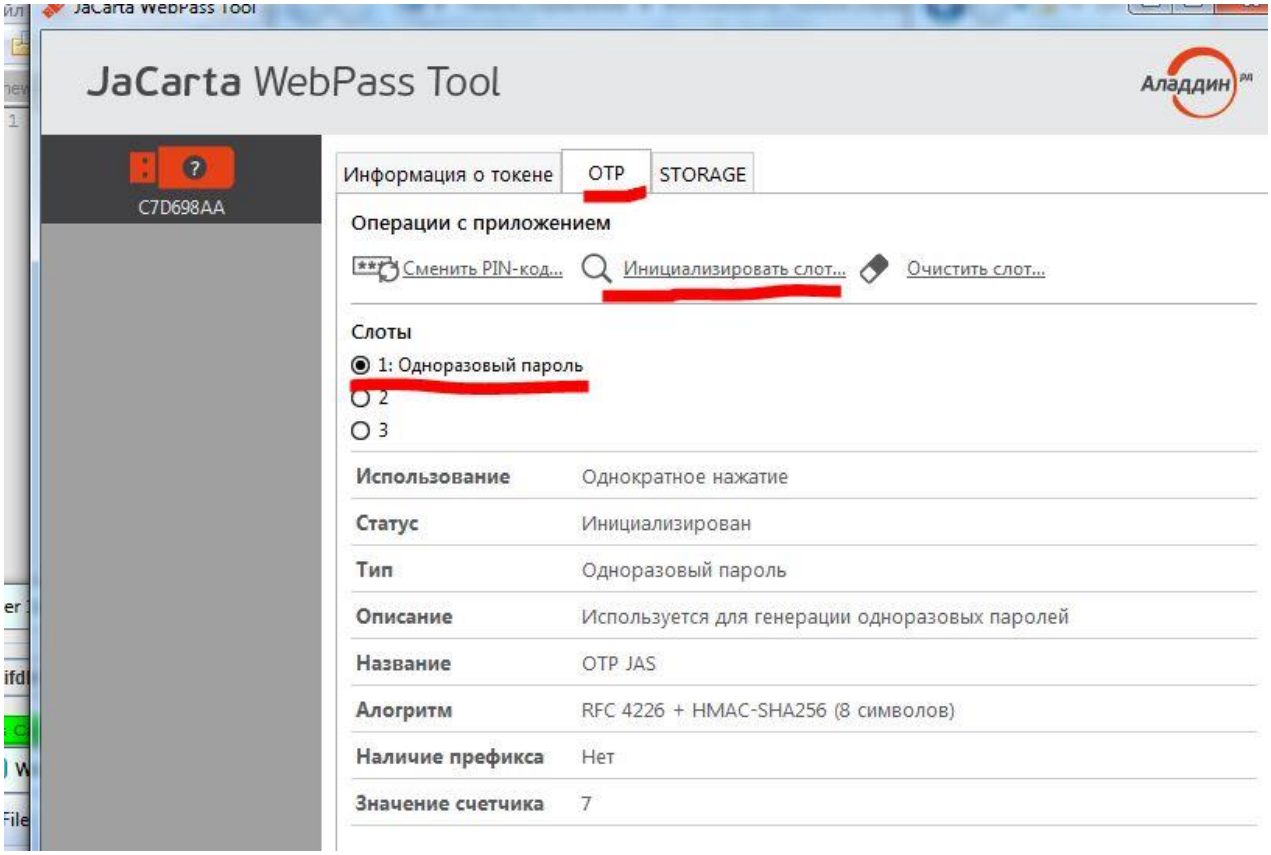
Подготовка JaCarta WebPass

Для инициализации JaCarta WebPass необходимо открыть приложение Web Pass Tool, которое входит в состав программного обеспечения "Единый Клиент JaCarta". Загрузить ПО можно по ссылке https://www.aladdin-rd.ru/support/downloads/jacarta/.

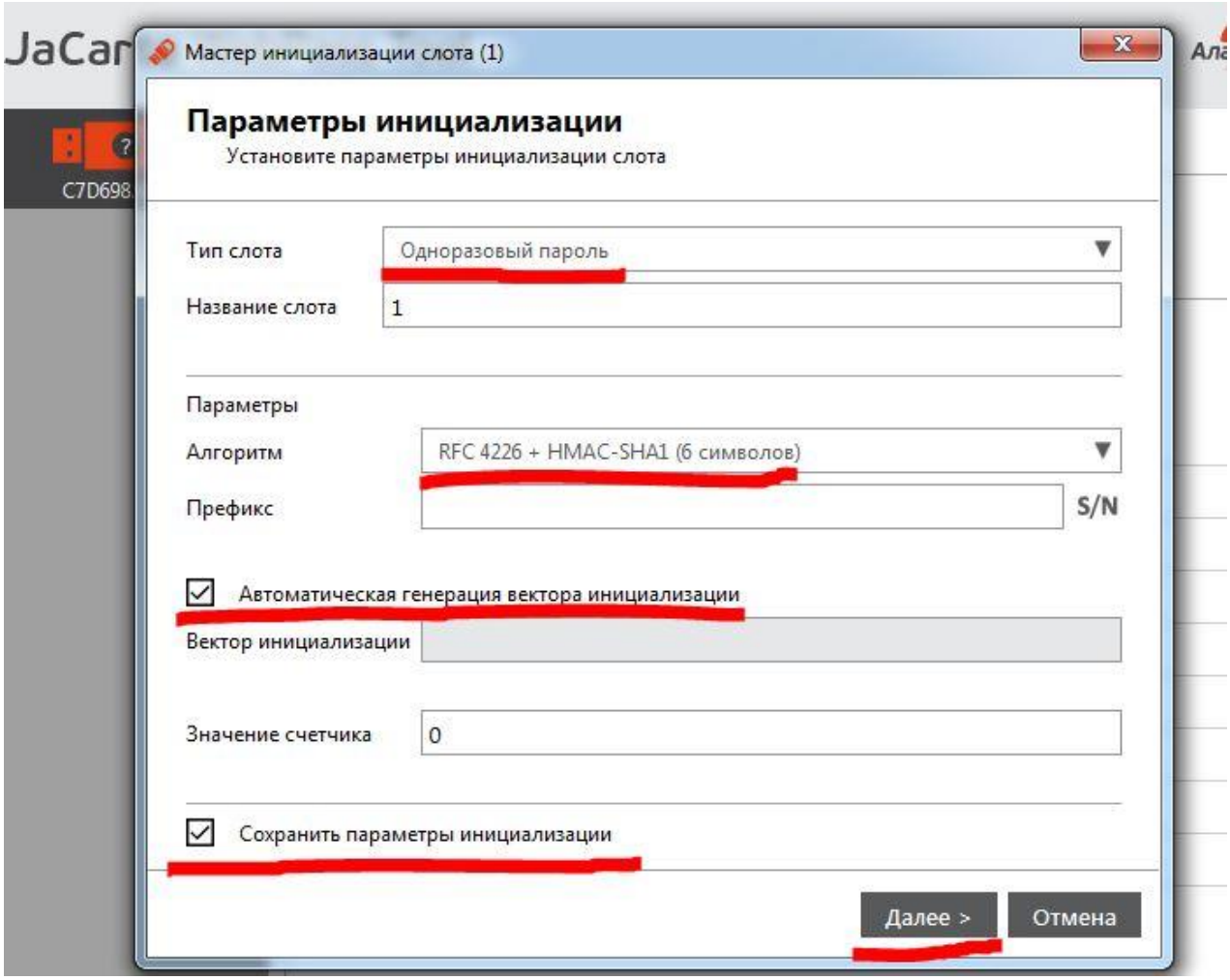
Откройте приложение JaCarta WebPass Tool, выберите вкладку OTP.



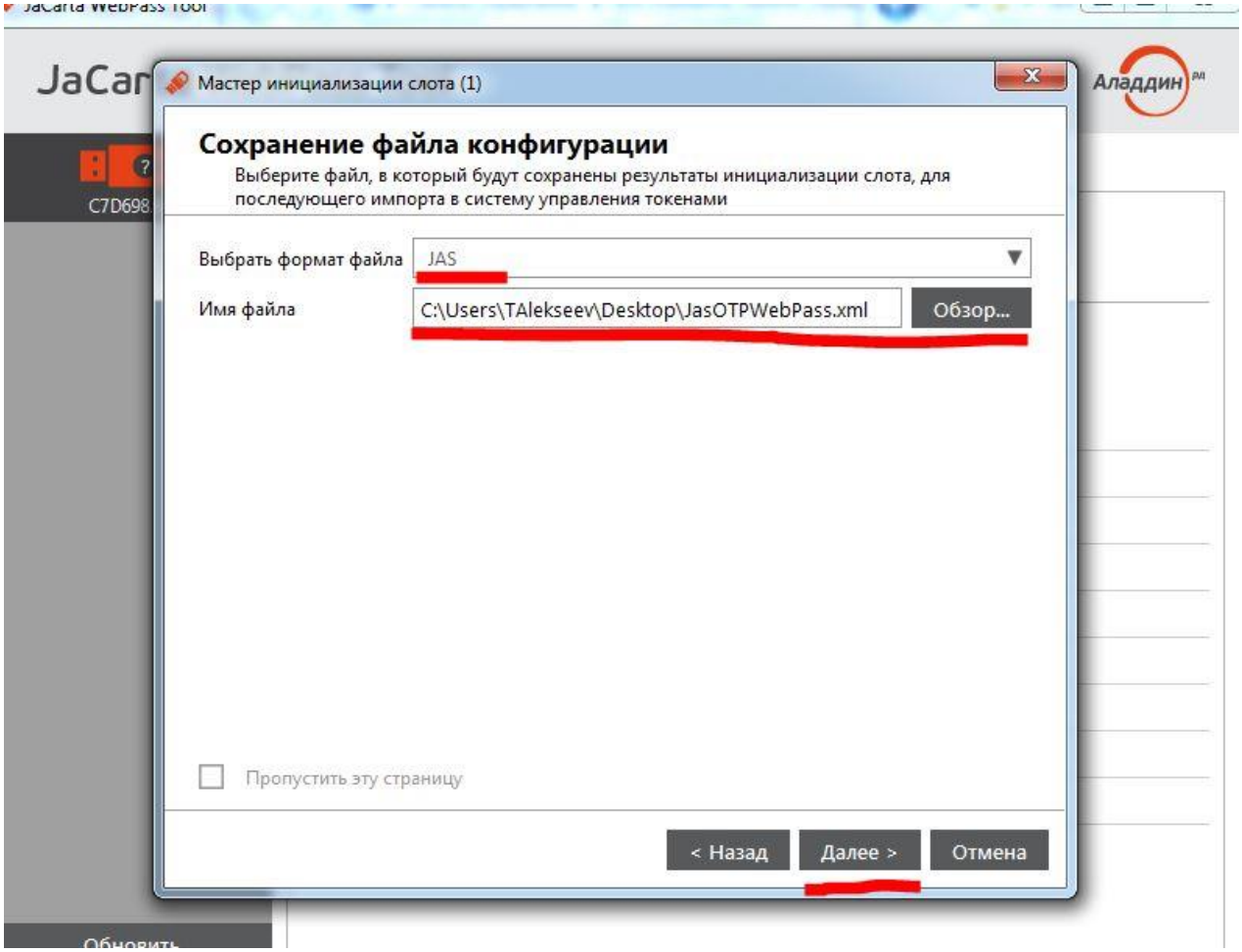
Выберите слот для инициализации, затем нажмите в меню пункт Инициализация.



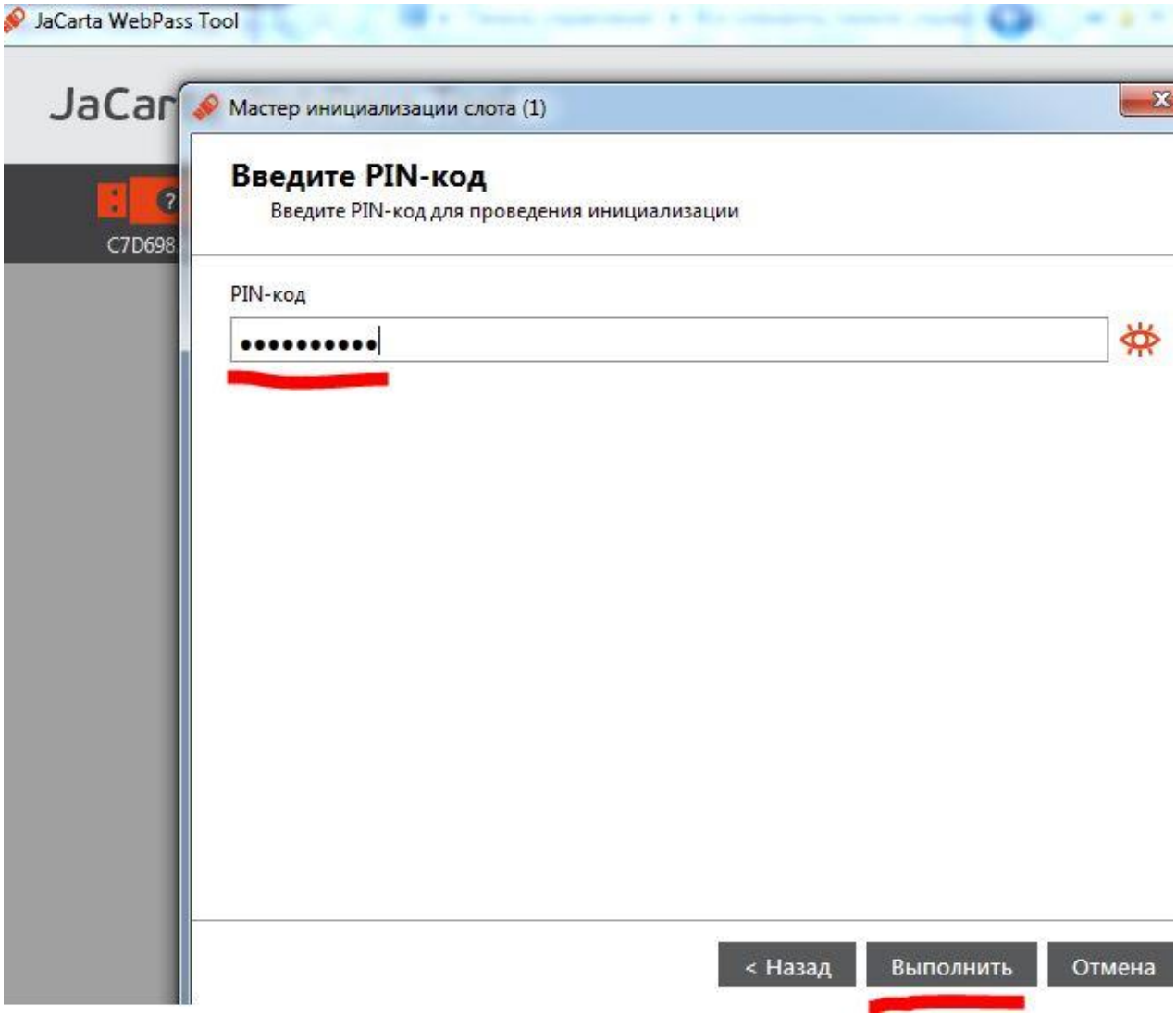
В настройках укажите Одноразовый пароль, первый механизм из выпадающего списка, отметьте Сохранение параметров инициализации и нажмите Далее.



Выберите формат файла JAS, а также путь до папки, куда будет сохранён файл инициализации. Этот файл потребуется для подключения ключа к JAS.



Введите PIN-код для ключа и нажмите Далее.

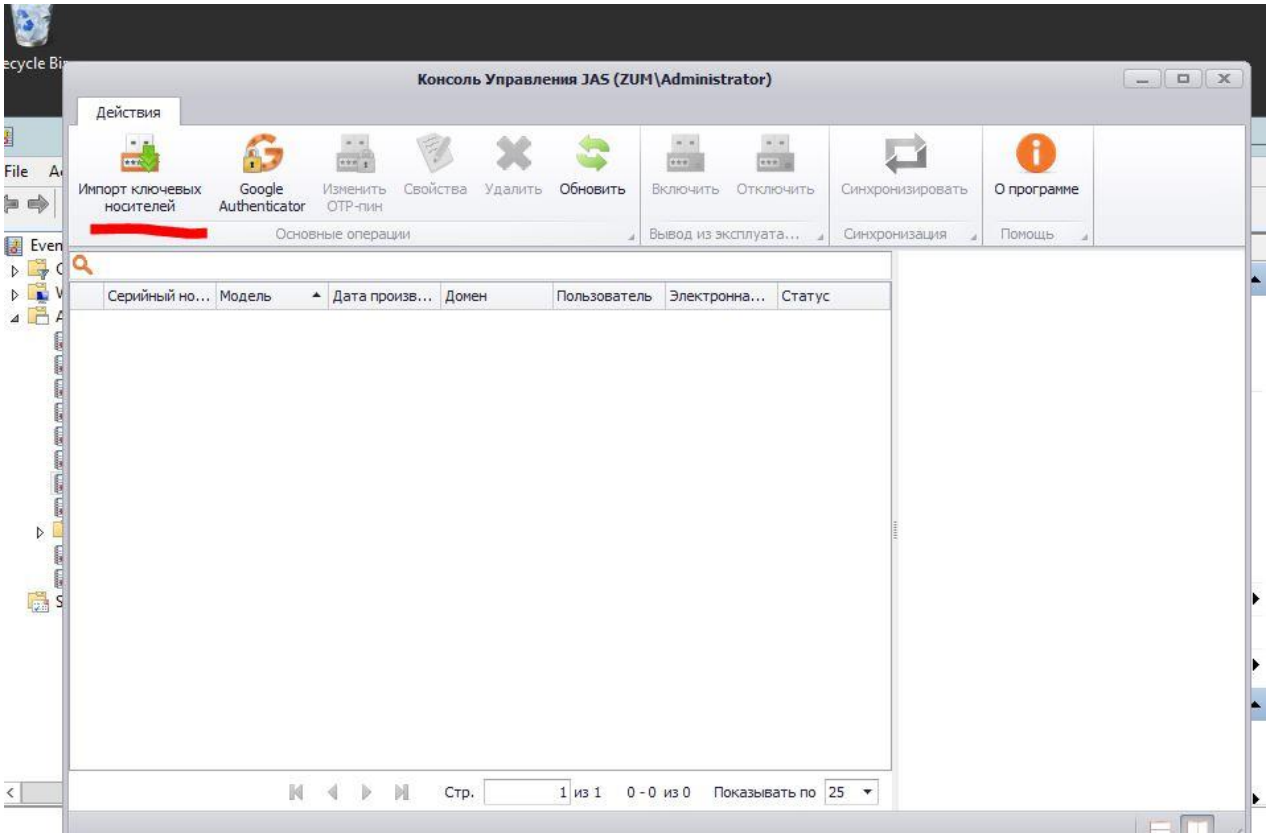


Настройка на стороне JAS

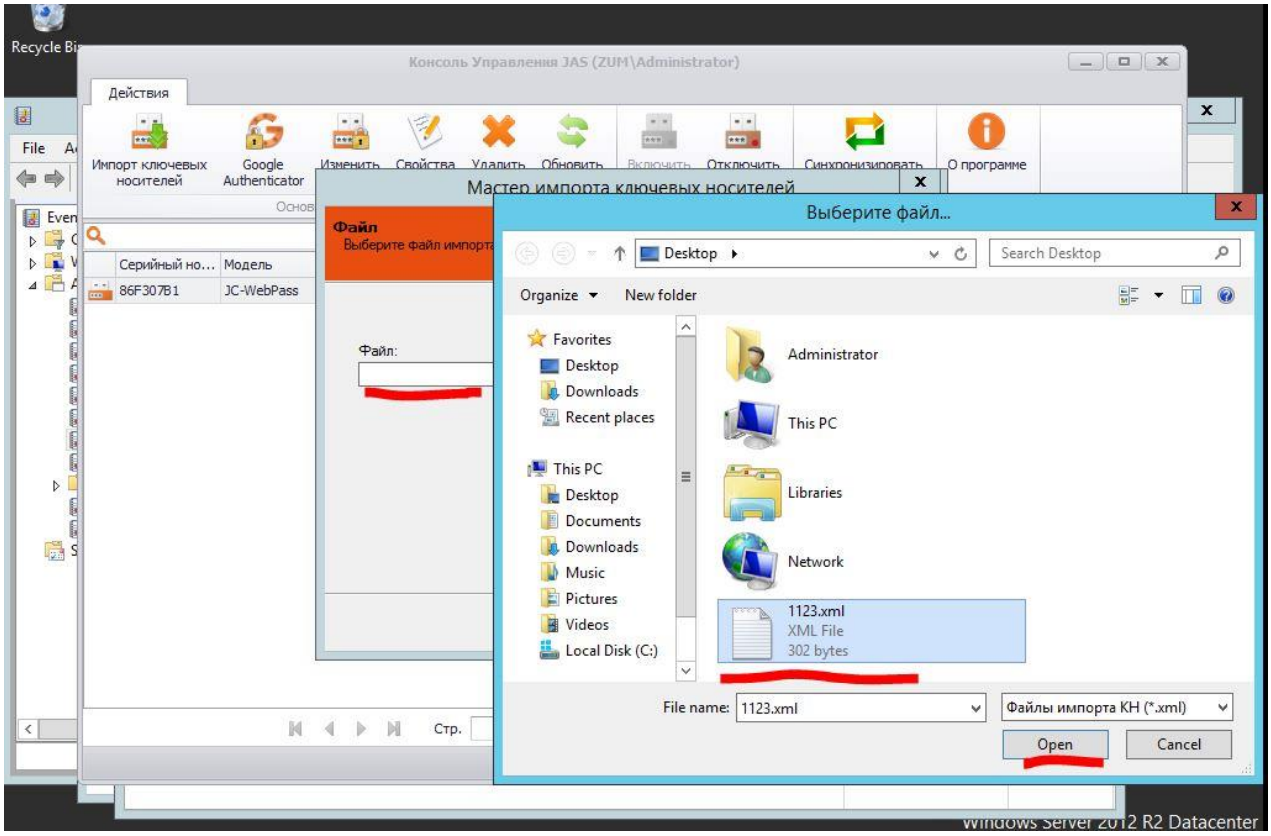
На стороне JAS необходимо выполнить перечисленные ниже шаги.

Добавьте устройство OTP в систему, привяжите пользователя к устройству. Для этого откройте оснастку JAS.

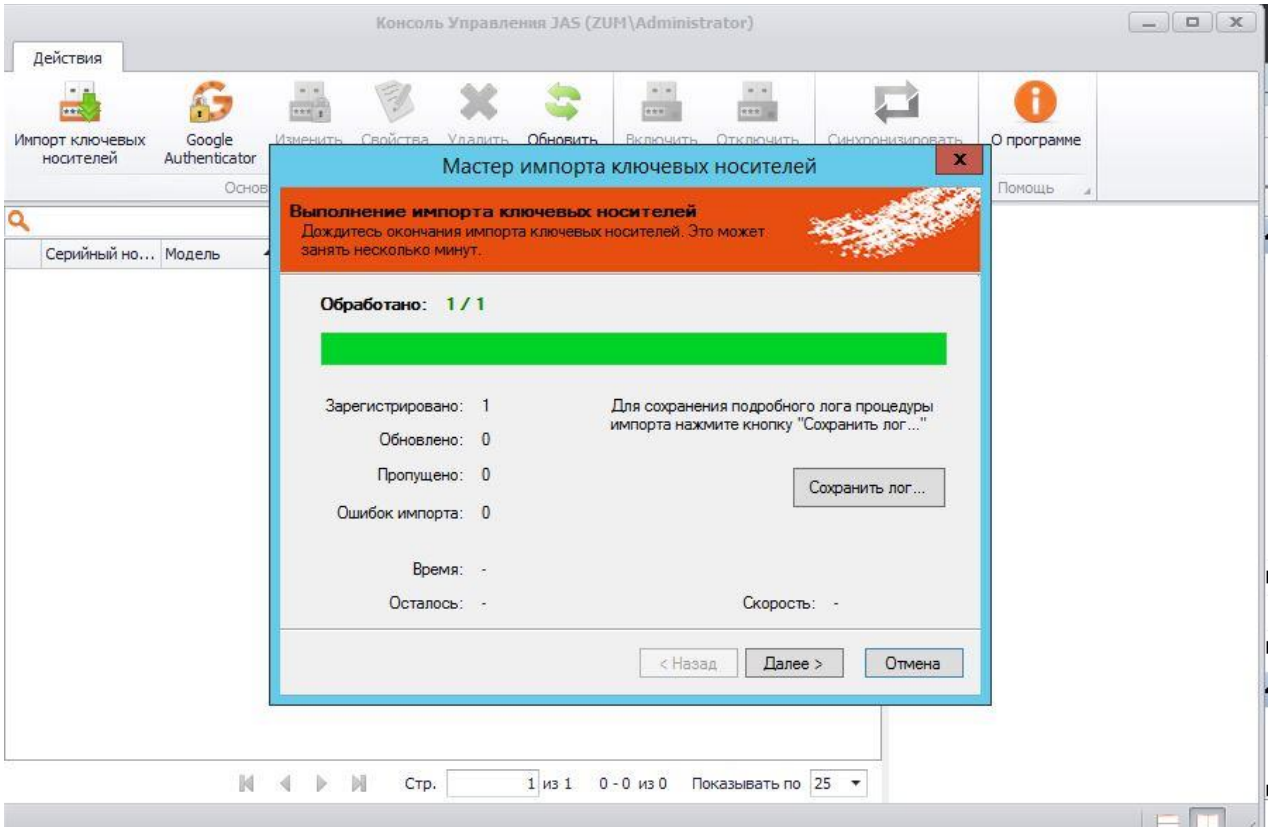
В оснастке выберите Импорт ключевых носителей.



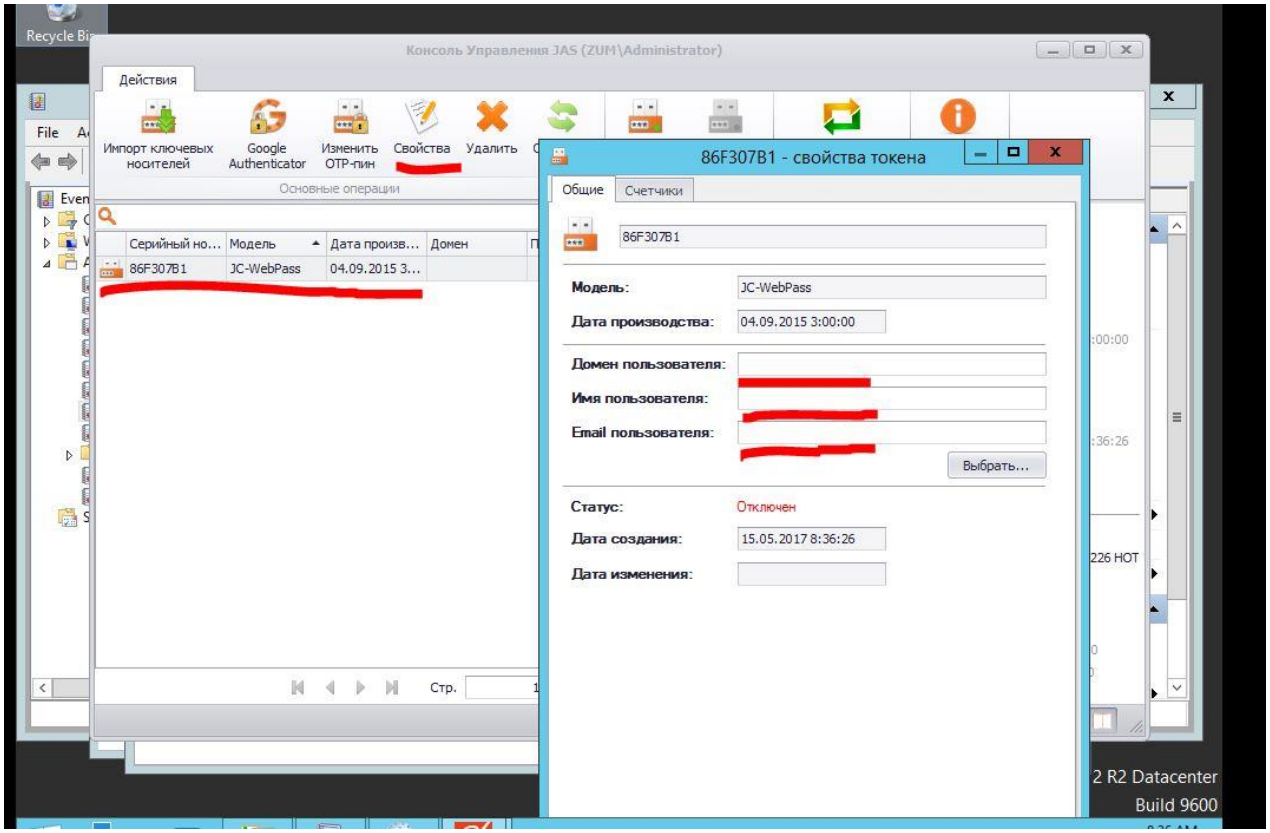
Укажите путь до файла с данными инициализации JaCarta WebPass (файл можно получить при инициализации слота в приложении Web Pass Tool, который входит в состав программного обеспечения "Единый Клиент JaCarta". Загрузить ПО можно по ссылке https://www.aladdin-rd.ru/support/downloads/jacarta/).



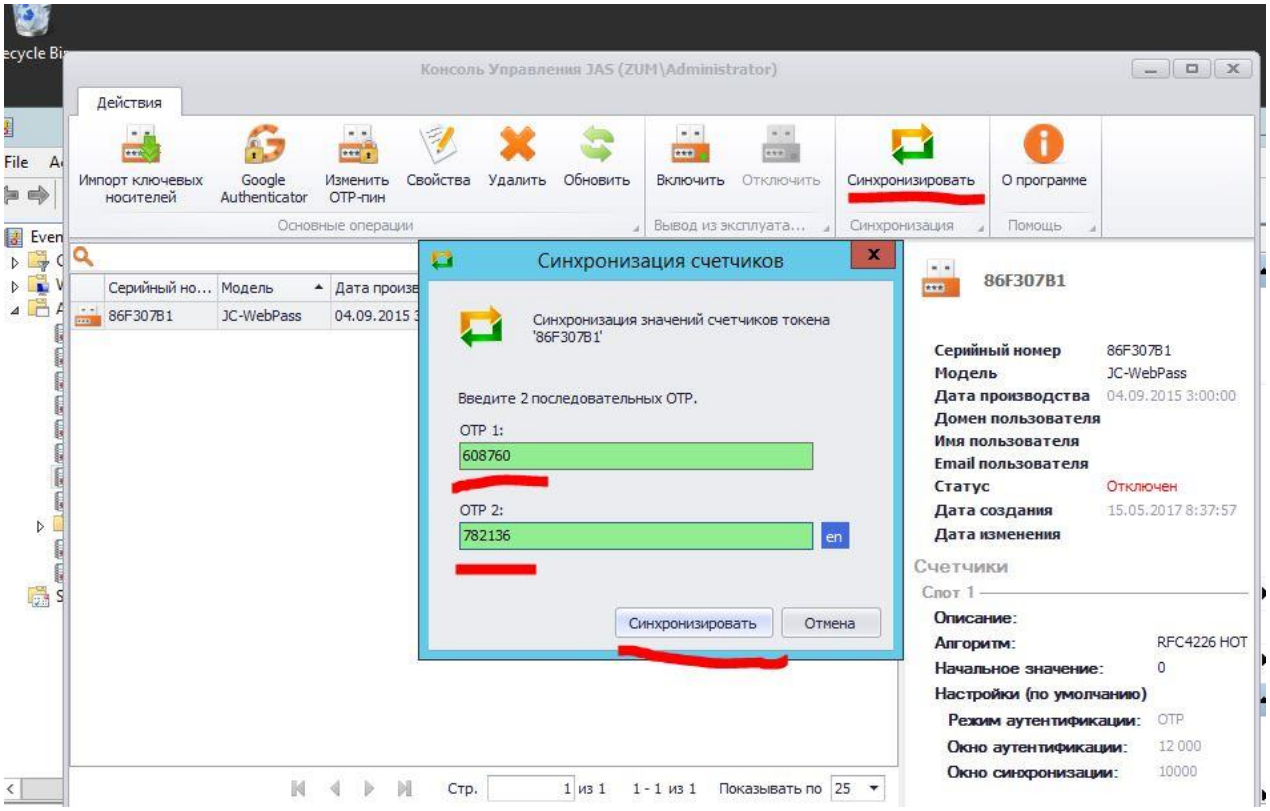
В случае успеха нажмите Далее.



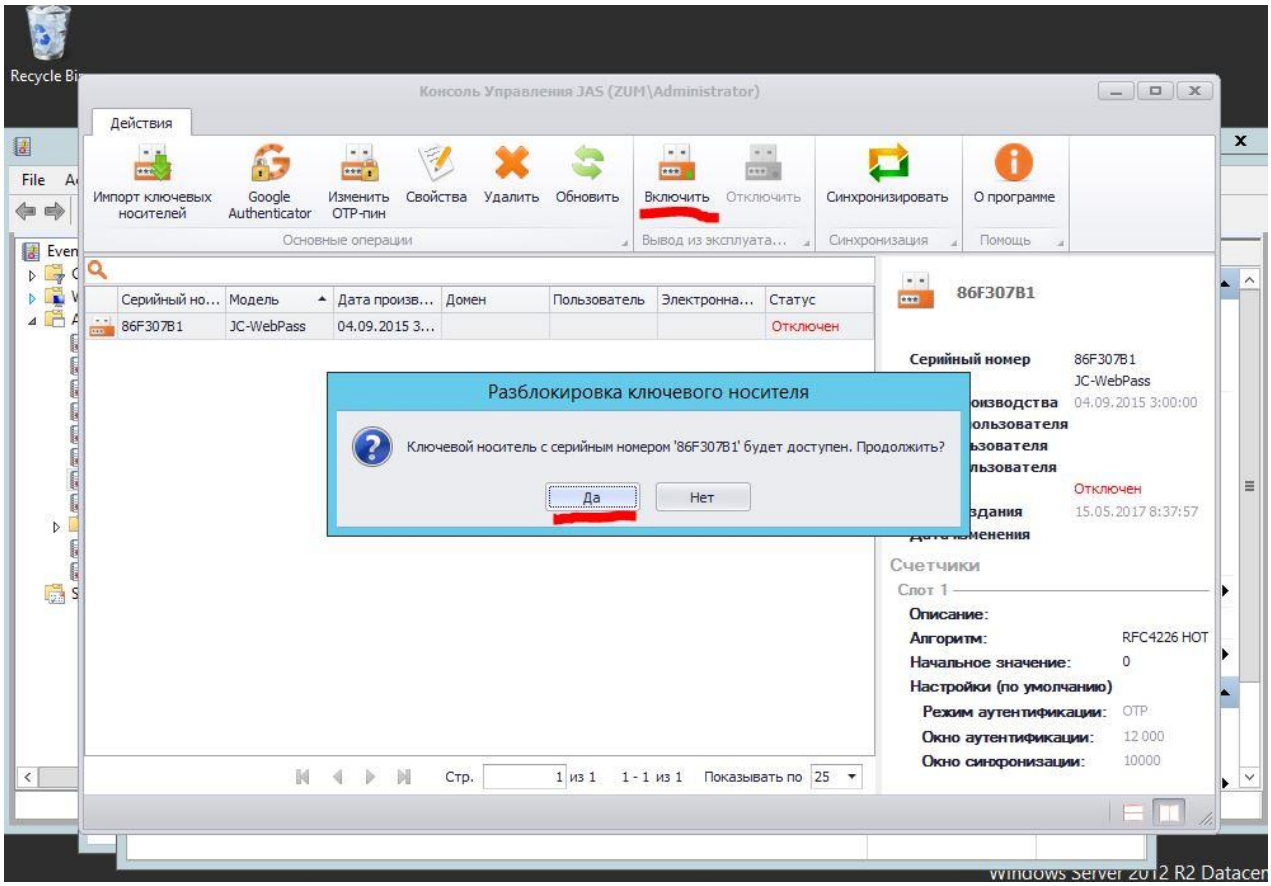
Выберите добавленный ключ, нажмите Свойства в меню. Для привязки к пользователю следует указать имя и адрес электронной почты для доменного пользователя.



Перед активацией следует произвести синхронизацию устройства, для этого нажмите Синхронизация в меню, укажите в окно OTP 1 и нажмите на кнопку устройства JaCarta WebPass, затем повторите с окном OTP 2.



Для активации выберите пункт Включить.



Настройка на стороне Linux Server

На стороне Linux сервера все операции необходимо производить от имени root.

```
# sudo -i
```

```
# apt-get install libpam-radius-auth
```

Добавьте значения для вашего RADIUS сервера, IP-адрес, либо имя сервера, общий секрет в файл /etc/pam_radius_auth.conf.

```
# nano /etc/pam_radius_auth.conf
```

```
#  The timeout field controls how many seconds the module waits before
#  deciding that the server has failed to respond.
#
# server[:port] shared_secret      timeout (s)
[SERVER IP] [Общий секрет]            3
```

В файле /etc/pam.d/sshd добавьте строку auth sufficient pam_radius_auth.so над @include common-auth, как показано ниже.

```
# nano /etc/pam.d/sshd
```

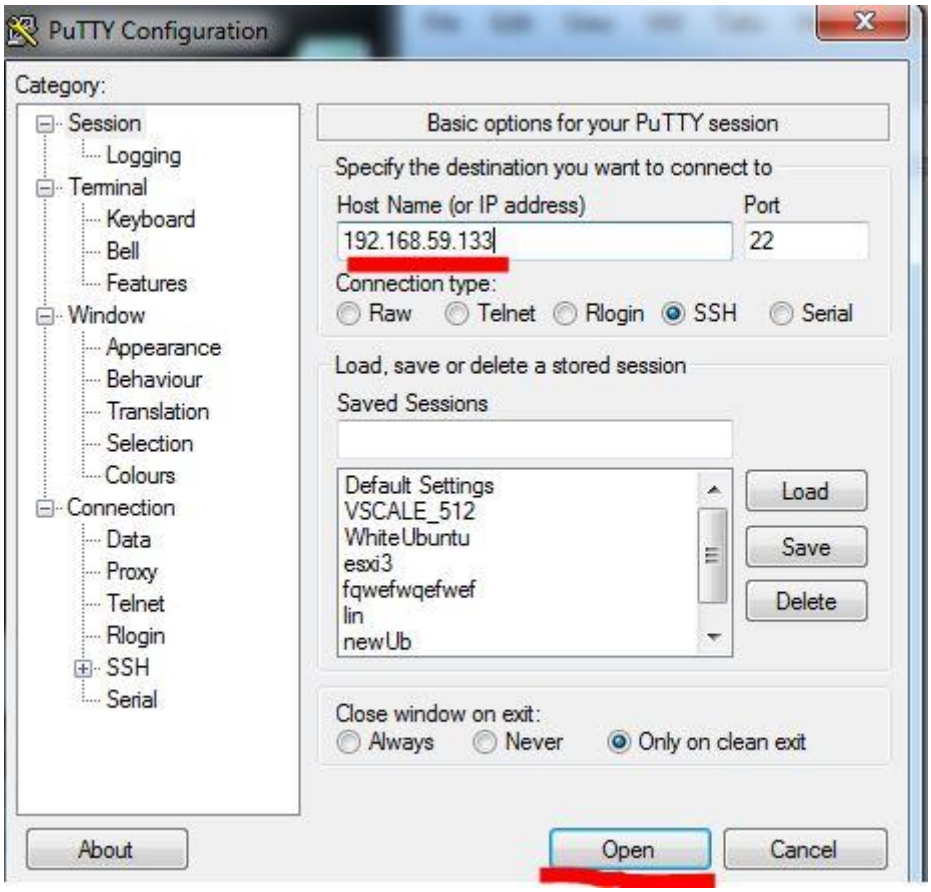
```
# PAM configuration for the Secure Shell service

# Standard Un*x authentication.
auth sufficient pam_radius_auth.so
@include common-auth


# Disallow non-root logins when /etc/nologin exists.
```

Создайте локального пользователя с именем, соответствующим пользователю в AD.

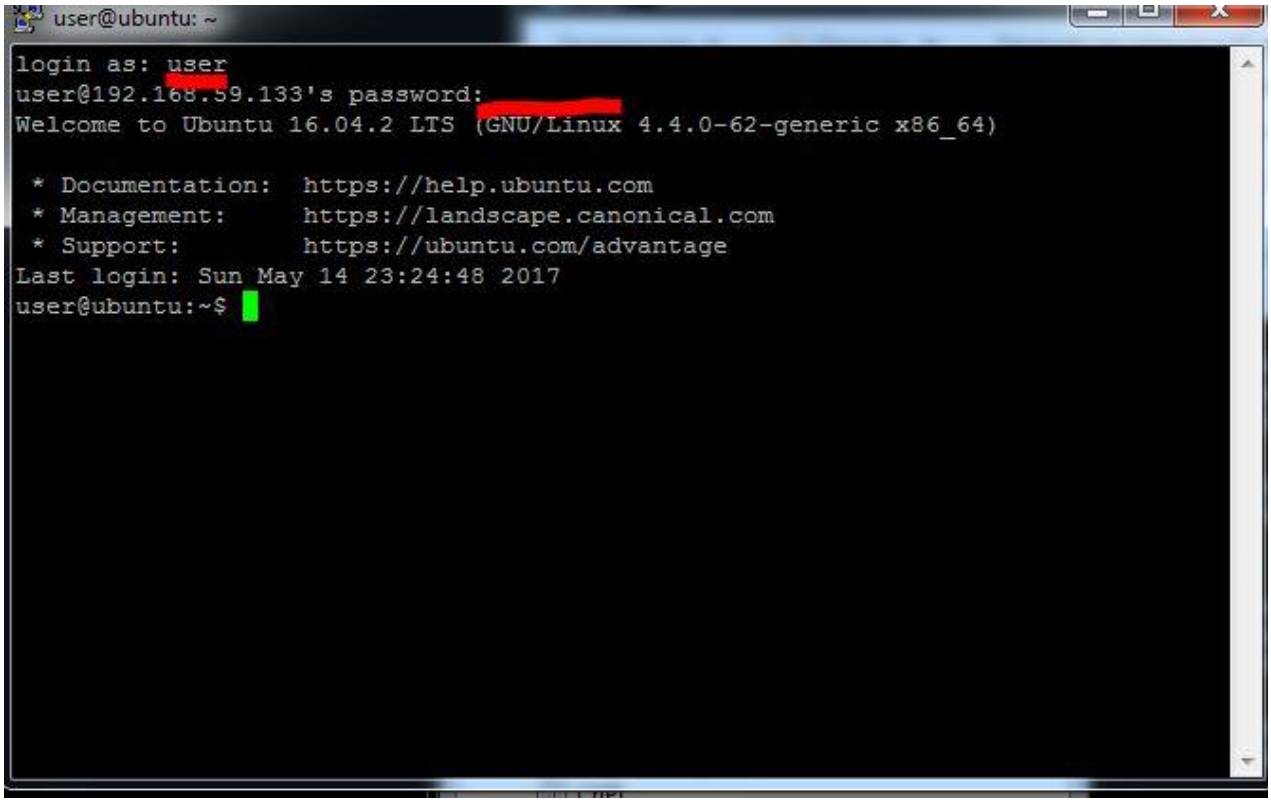
Проверка решения

Для проверки воспользуемся операционной системой Microsoft Windows 7 с установленным SSH клиентом PUTTY.

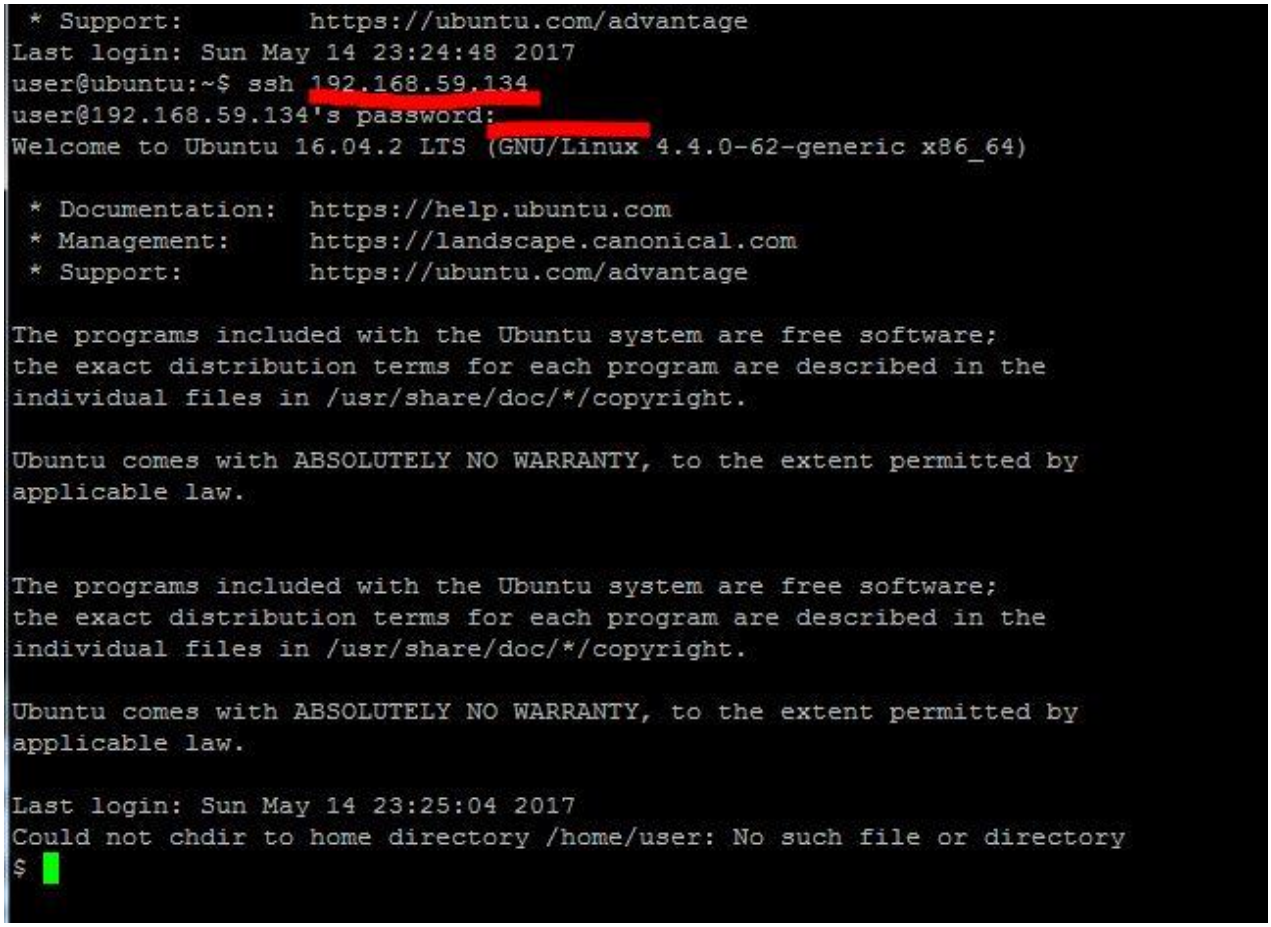
Откроем Putty и укажем адрес интересующей нас машины на Linux.



Введите имя пользователя, Ввод, затем нажмите на кнопку устройства JaCarta WebPass, Ввод.



Далее введите команду SSH [Servername2], Ввод, нажмите кнопку на устройстве, Ввод.



Контакты, техническая поддержка

Офис (общие вопросы)

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

Телефоны: +7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40

Факс: +7 (495) 646-08-82

E-mail: aladdin@aladdin-rd.ru (общий)

Web: www.aladdin-rd.ru

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

Техподдержка

Служба техподдержки принимает запросы только в письменном виде через Web-сайт:

www.aladdin-rd.ru/support/index.php

Для оперативного решения Вашей проблемы укажите используемый Вами продукт, его версию, подробно опишите условия и сценарии применения, по возможности, снабдите сообщение снимками экрана, примерами исходного кода.

Регистрация изменений[1]

Версия	Изменения
1.0	Переделаны разделы 2, 4, добавлен раздел 10
0.9	Добавлены разделы 4, 7, 9, изменено форматирование
0.3 draft	Создание документа

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 2874 от 18.05.12
Лицензии ФСБ России № 12632 Н от 20.12.12, № 24530 от 25.02.14
Система менеджмента качества компании соответствует требованиям стандарта ISO/ИСО 9001-2011
Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15
Apple Developer

Тел. +7 (495) 223-00-01 Email: aladdin@aladdin-rd.ru Web: www.aladdin-rd.ru