Duo Security и JaCarta WebPass/U2F

Интеграция электронных ключей JaCarta в платформу DuoSecurity

Версия документа:	1.0
Листов:	29
Автор:	Dmitry Shuralev

Аннотация

Настоящий документ описывает интеграцию токенов **JaCarta U2F** и **JaCarta WebPass** в облачную платформу двухфакторной аутентификации **Duo Security**. А так же описывает работоспособность платформы **Duo** и токенов **JaCarta**, на примере аутентификации в **CMS WordPress** с использованием токенов **JaCarta** и плагина от **DuoSecurity**.

Оглавление

О платформе Duo Security

Duo.com — облачный провайдер двухфакторной аутентификации.

Платформа **Duo Security** позволяет подключить двухфакторную аутентификацию для защиты пользовательских аккаунтов и сервисов. Решение защищает организации от утечки данных, обеспечивая только легальным пользователям и соответствующим устройствам доступ к конфиденциальным данным и приложениям в любое время и в любом месте. Платформа **Duo Security** доступна для различных операционных систем и платформ. Интегрирована с огромным множеством ПО (различные VDI решения, VPN решения, Web-сервисы, облачные-сервисы, Windows, Unix SSH, Radius, Shibboleth и многое другое).

Подробная информация доступна на сайте **Duo Security:**

- https://duo.com/

В качестве аутентификаторов платформа по умолчанию использует выбор из OTP по СМС, Push-уведомление или обратный звонок. Дополнительно поддерживает OTP токены **JaCarta**, модель **JaCarta WebPass**, а также U2F токены, модель **JaCarta U2F**.

Кроме двухфакторной аутентификации платформа имеет широчайший комплекс по управлению пользователями и пользовательскими устройствами, назначение и управление различными политиками, сбор статистики о пользовательских устройствах, версиях ПО и другое.

Об Электронных ключах JaCarta WebPass/U2F

JaCarta WebPass

USB-токен с "OTP на борту" для двухфакторной аутентификации пользователей при доступе к защищённым информационным ресурсам с использованием одноразового пароля, либо хранимого в памяти токена многоразового пароля

- Автоматическая подстановка паролей в поля экранных форм
- Защищённое хранение адресов Web-ресурсов и запуск Web-браузера с переходом по сохранённому адресу
- Хранение криптоконтейнеров программных СКЗИ
- Полная совместимость с классическими OTP-токенами (eToken PASS, eToken NG-OTP и др.), согласно RFC 4226

Решаемые задачи

- Усиление парольной аутентификации пользователей при доступе к информационным ресурсам за счёт перехода к двухфакторной аутентификации с использованием токена. Генерируемый токеном одноразовый пароль может использоваться совместно с запоминаемым паролем.
- Избавление пользователей от необходимости запоминать сложные пароли. Пароли генерируются и хранятся в токене.
- Избавление пользователей от возможных ошибок, возникающих при ручном вводе паролей и адресов Web-ресурсов. Пароли автоматически подставляются в формы ввода при нажатии на кнопку. Запуск Web-браузера и переход по сохранённому адресу также осуществляются при нажатии на кнопку.

Ключевые особенности

- Механическая кнопка для генерации паролей, запуска Web-браузера и подтверждения присутствия человека за ПК.
- Автоматическая подстановка паролей в поля экранных форм по нажатию кнопки.
- Двухчиповая конструкция:
  - микроконтроллер, отвечающий за коммуникации с ПК, взаимодействие с пользователем и выполняющий роль межсетевого экрана для команд APDU;
  - смарт-карта, реализующая функции безопасности (генерация одноразовых паролей, генерация и хранение многоразового пароля).
- Поддержка интерфейсов HID, CCID с возможностью одновременного использования обоих интерфейсов и переключения между ними в процессе работы.
- Токен можно использовать на любых устройствах, оснащённых USB-портом Type A Female и допускающих использование USB-клавиатур.
- Отсутствие внутренних элементов питания – питание осуществляется от порта USB.

- Поддержка любых ОС Microsoft Windows, Linux, Mac OS X, Google Android, Apple iOS (через Camera Connection Kit).
- Для использования токена не требуется установки дополнительных драйверов и программного обеспечения (ввод одноразовых паролей происходит по HID-интерфейсу).
- Один токен может быть использован для доступа к нескольким различным ресурсам ("один ко многим").

JaCarta U2F

Универсальный USB-токен, предназначенный для использования в качестве второго фактора при аутентификации конечных пользователей онлайн-сервисов, поддерживающих стандарт U2F разработанный альянсом FIDO.

https://fidoalliance.org/

Функциональные возможности

Аутентификация по стандарту FIDO U2F

Ключевые особенности

- Самостоятельная регистрация пользователей – в отличие от систем аутентификации на основе традиционных PKI-токенов, в процессе регистрации токена JaCarta U2F на конкретном Web-ресурсе не требуется участия администратора. Для регистрации необходимо просто ввести логин и пароль, подключить токен к компьютеру и нажать на кнопку (тем самым подтвердив физическое присутствие пользователя за компьютером). В процессе регистрации пользователем своего U2F-токена на Web-ресурсе происходит генерация ключевой пары (открытый и закрытый ключ) без сертификата открытого ключа. Сгенерированная ключевая пара используется для дальнейшей аутентификации.
- Концепция "один ко многим" – один токен может использоваться для доступа к множеству различных Web-ресурсов (количество ресурсов ограничено лишь объёмом памяти токена, используемой для хранения аутентификационных данных).
- Защита от фишинга – каждый закрытый ключ, хранящийся в памяти токена и используемый для доступа к конкретному ресурсу, "связан" с адресом данного ресурса (URL). Таким образом, если злоумышленник попытается перенаправить пользователя на "поддельный" ресурс, пользователь не сможет пройти аутентификацию, так как закрытый ключ, соответствующий "поддельному" ресурсу, не будет найден.

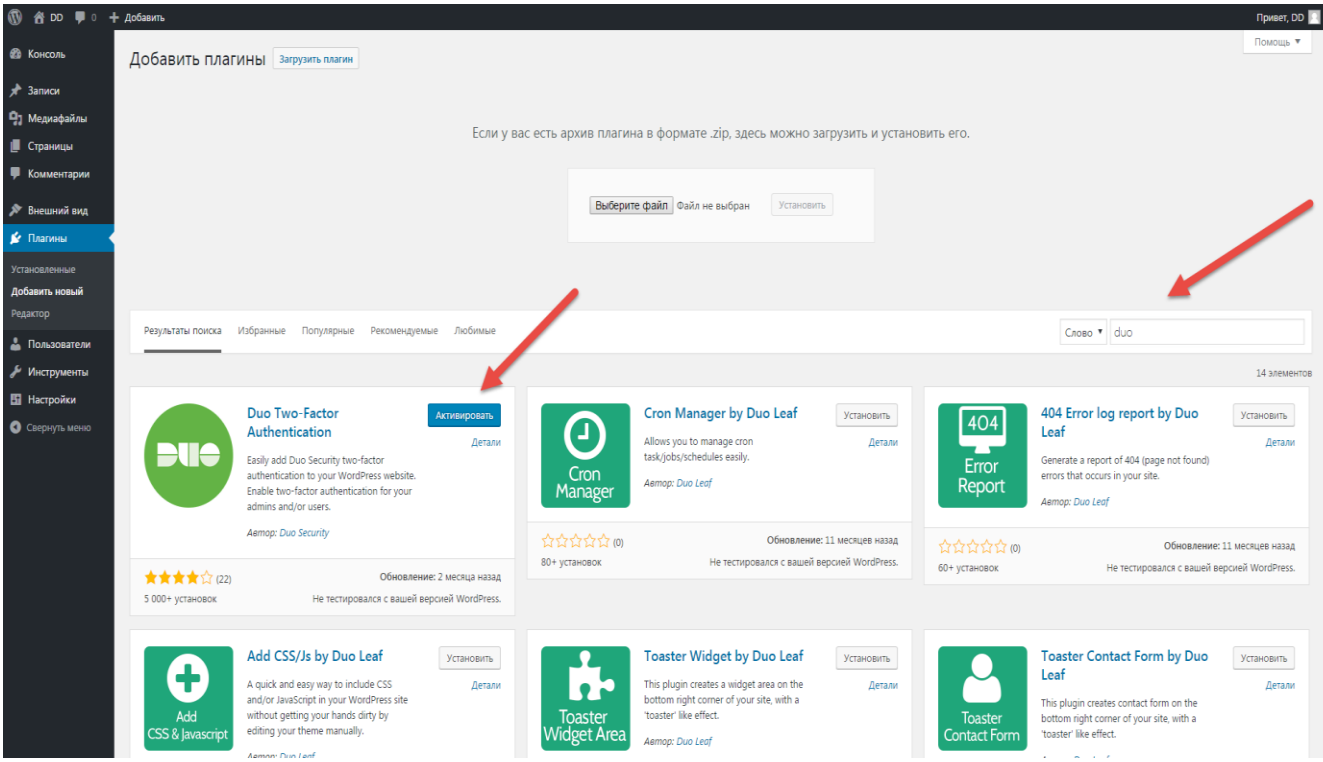
Подключение web-плагина DUO Security к web-сайту на CMS WordPress

В настоящем документе рассматриваются варианты интеграции электронных ключей **JaCarta U2F** и **JaCarta WebPass** и использование этих ключей в качестве второго фактора аутентификации на web-сайте на основе CMS WordPress с web-плагином DUO.

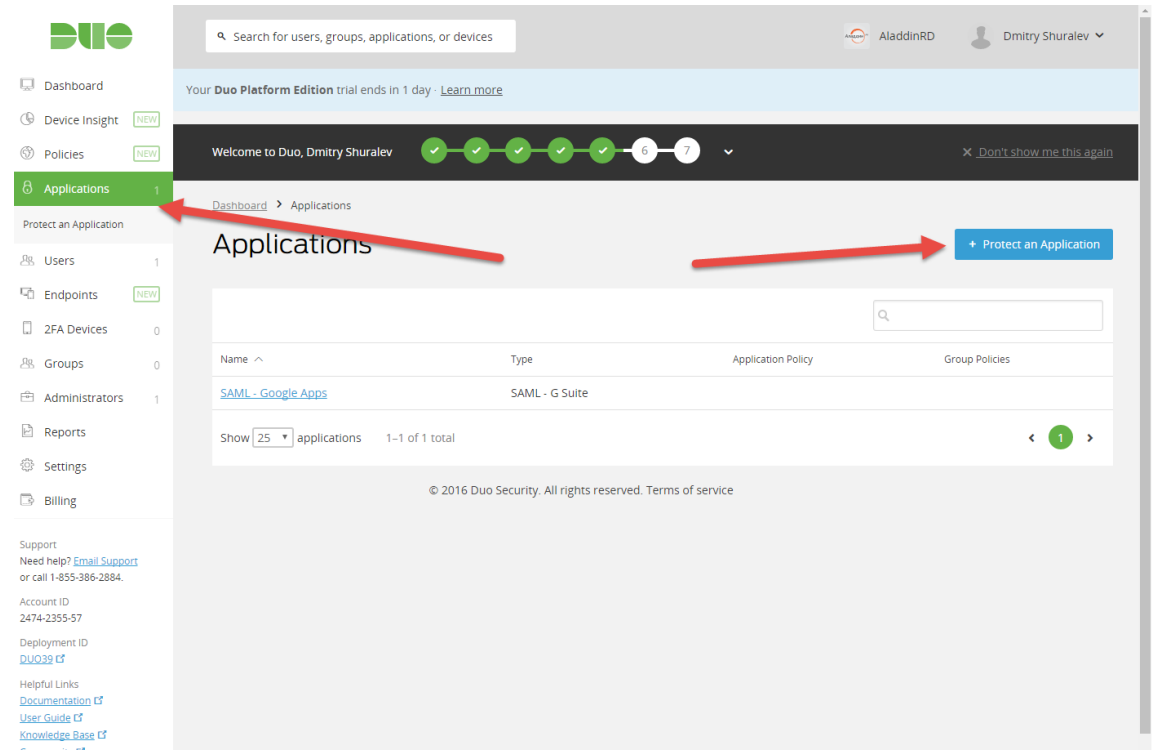
Добавленные в платформу DUO Security ключи, можно использовать, не только с плагином для WordPress, а с любым ПО или протоколом из списка поддерживаемых платформой DUO. Подробная информация доступна на сайте DUO Security — https://duo.com/docs

Чтобы защитить какое либо приложение или протокол, по средствам платформы DUO, необходимо выбрать что защищать в самой платформе и связать платформу с защищаемым приложением. В настоящем примере необходимо выполнить следующией действия.

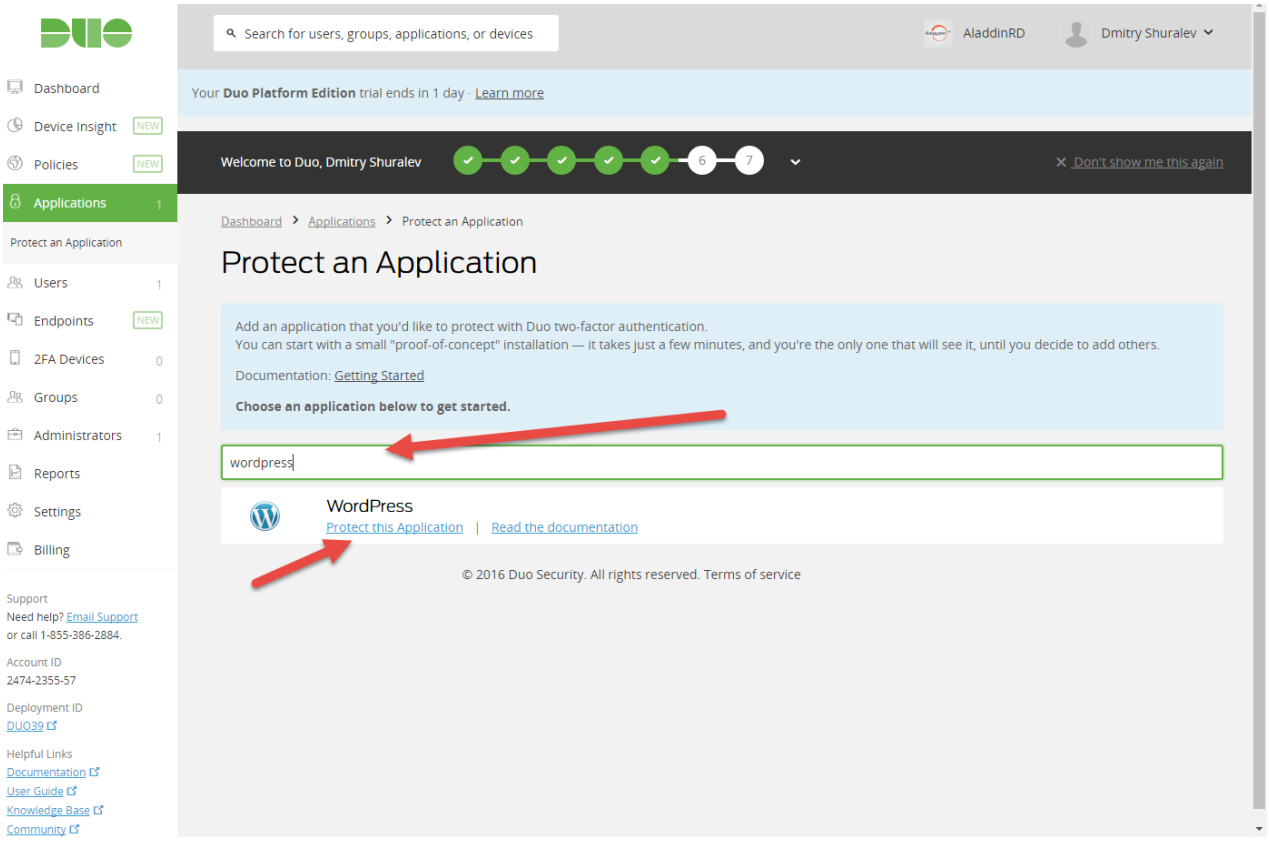
1. Со стороны Web-Сайта добавьте **Duo плагин,** для этого в меню **Плагины** в поиске найдите **Duo-Two-Factor Authentication** и нажмите **Установить.** После установки нажмите **Активировать.**



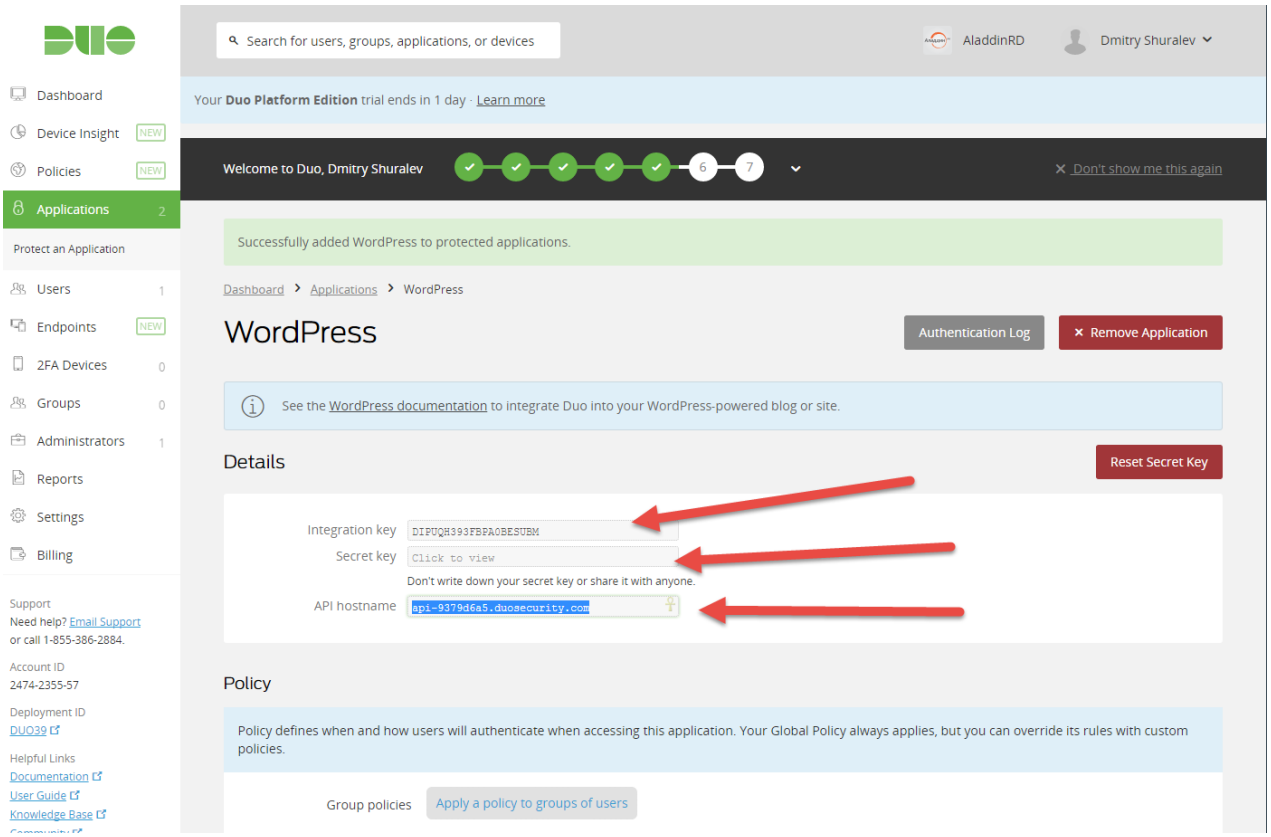
2. Со стороны платформы войдите в меню **Приложения (Applications)** и выберите **Защитить приложение (Protect an Application).**

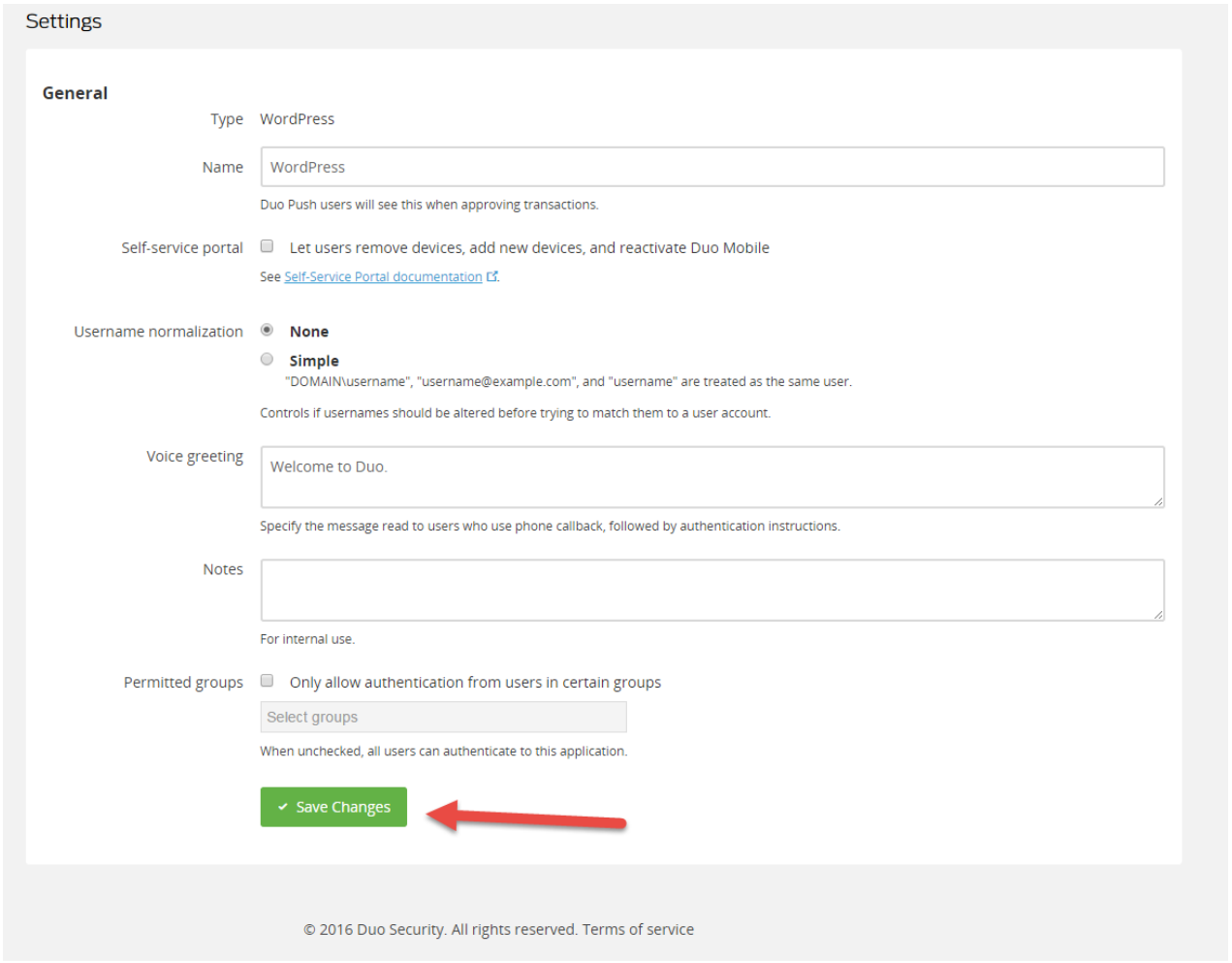


3. В отобразившемся меню поиска наберите WordPress и нажмите **Защитить это приложение (Protect this Application).**

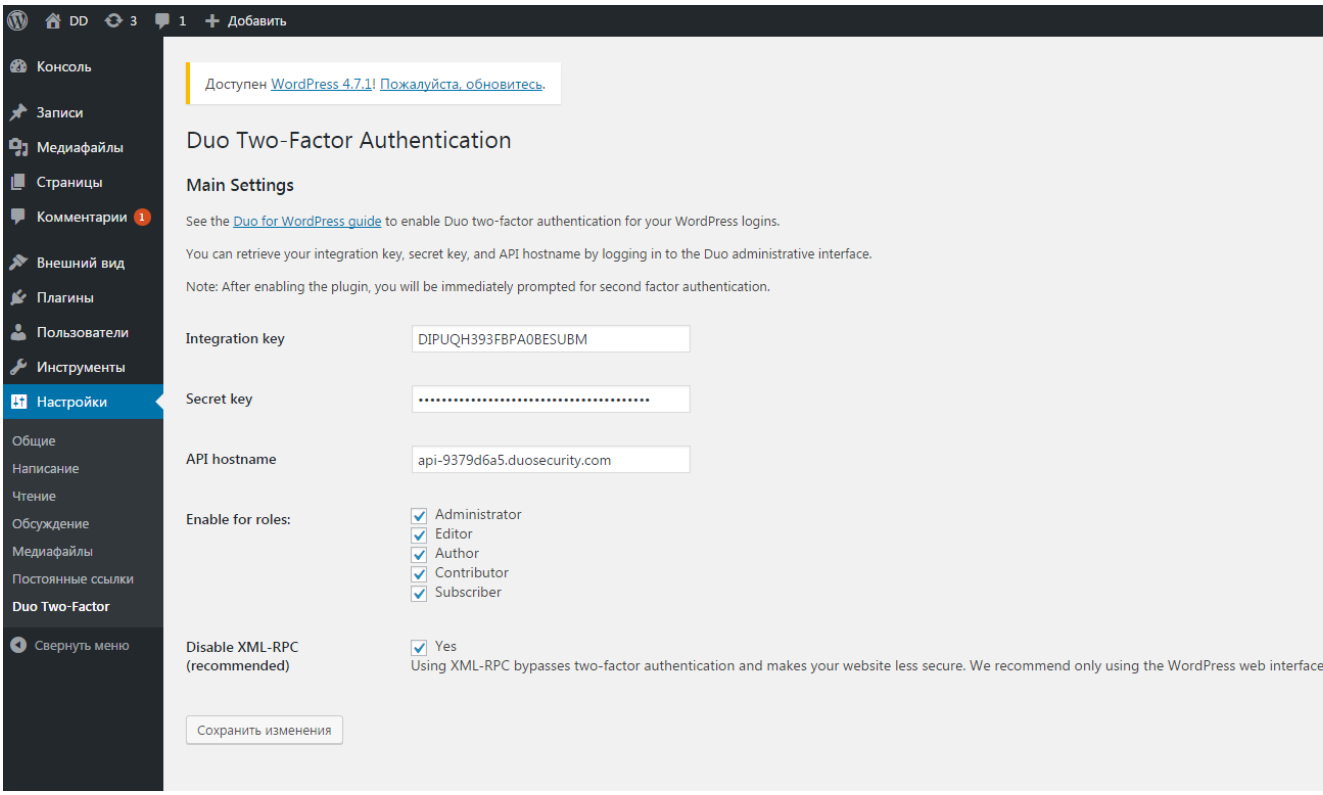


4. Отобразятся 3 ключевых поля, **Integration Key, Secret Key и API Hostname.**





5. Значения этих полей нужно перенести в соответсвующие поля плагина на web-сайте.

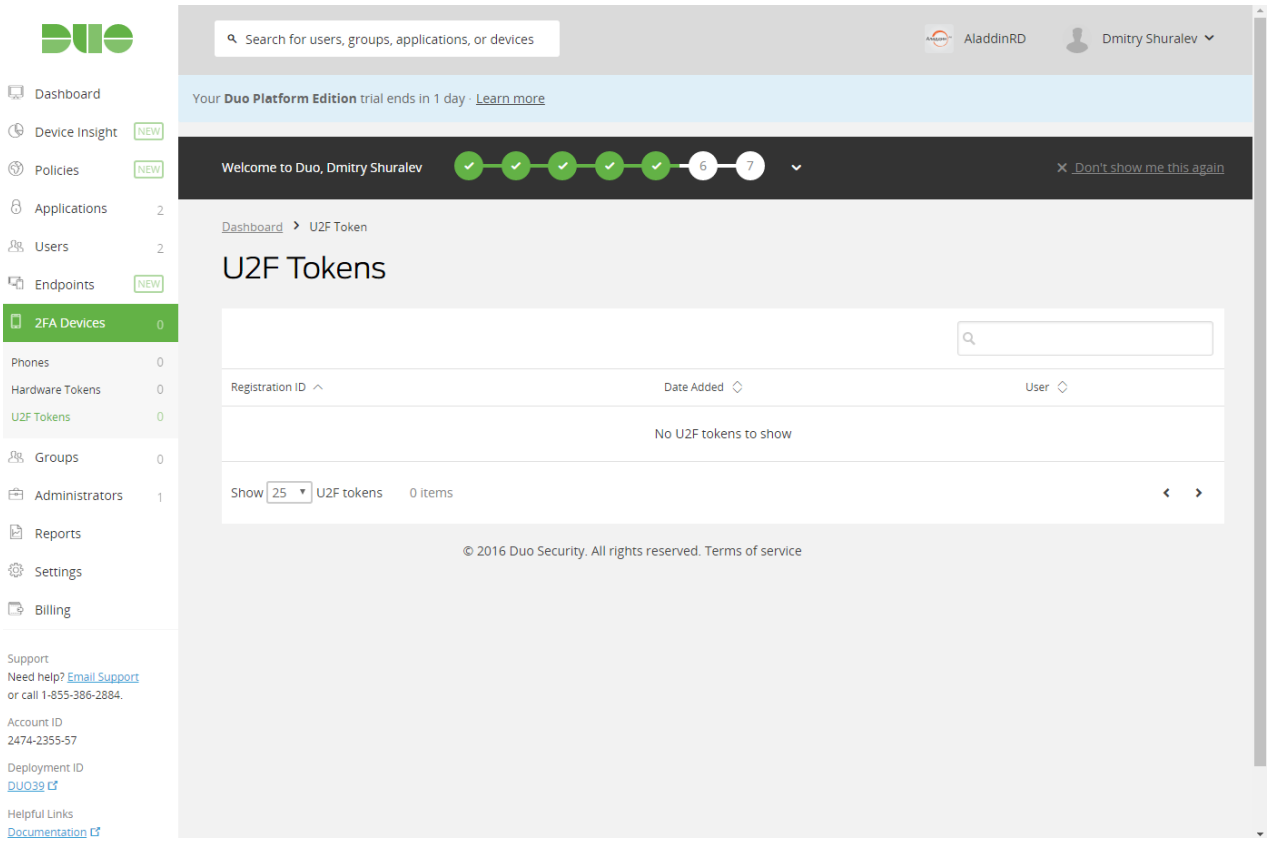


6. На этом настройка связи web-сайта с платформой Duo завершена, далее необходимо добавить в систему пользователя и токен.

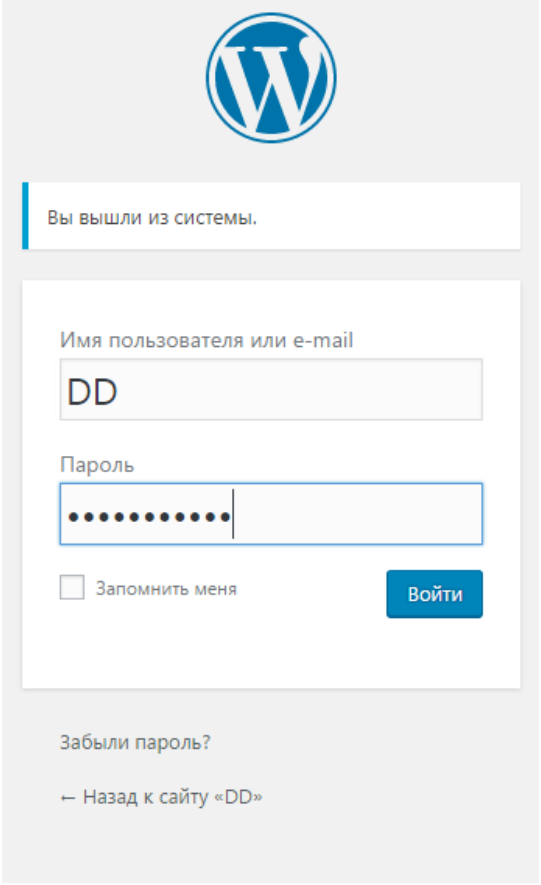
Добавление электронного ключа JaCarta U2F в платформу DUO

Добавление электронных ключей **JaCarta U2F** происходит пользователем со стороны web-сайта.

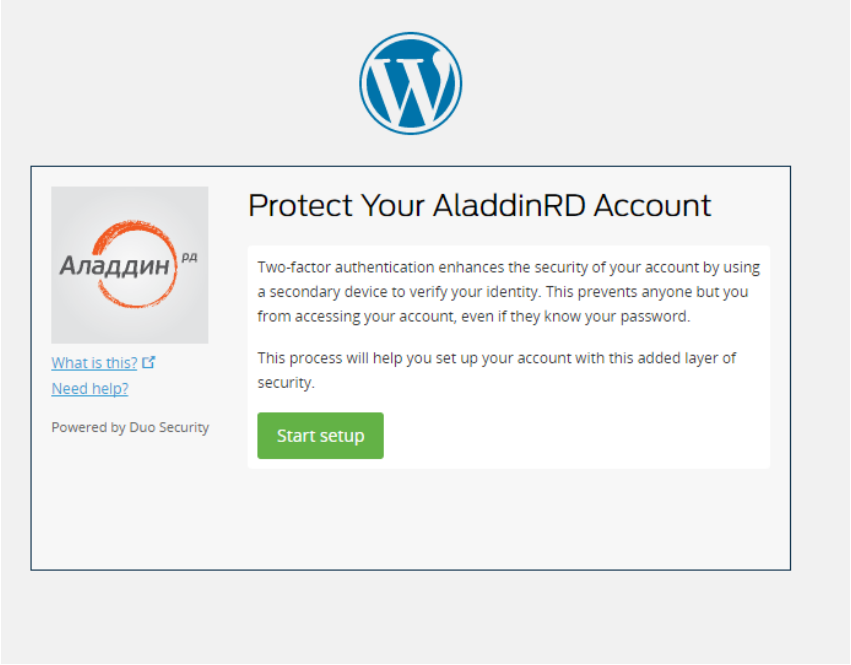
Для начала, со стороны платформы войдите в меню **2FA Devices (2Ф устройства)**. Убедитесь что список устройств пуст.



Аутентифицируйтесь по паролю, на том web-сайте куда ранее была привязана платформа Duo.

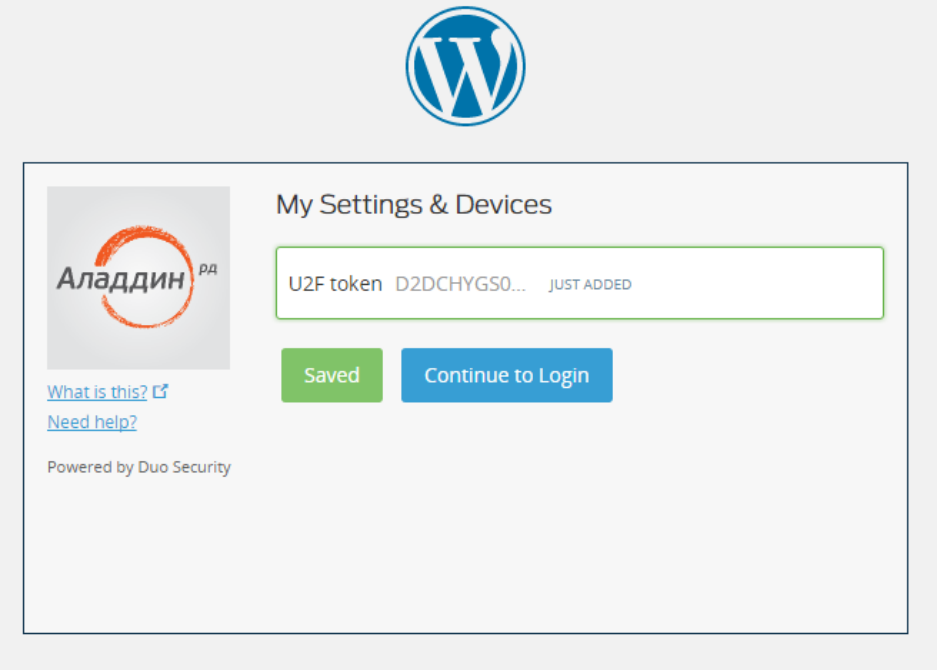


Установленный и настроенный плагин Duo предложит настроить защиту аккаунта. Нажмите **Start Setup.**

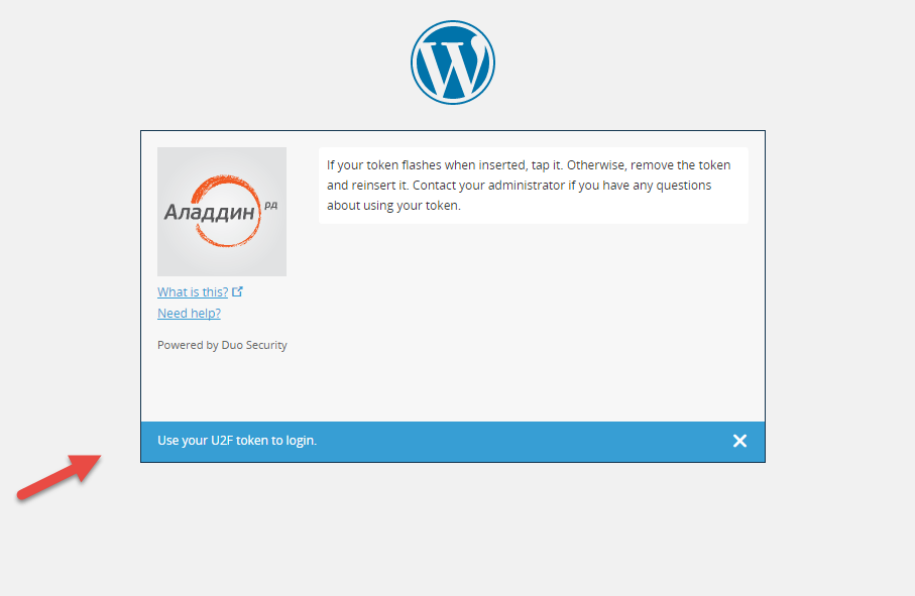


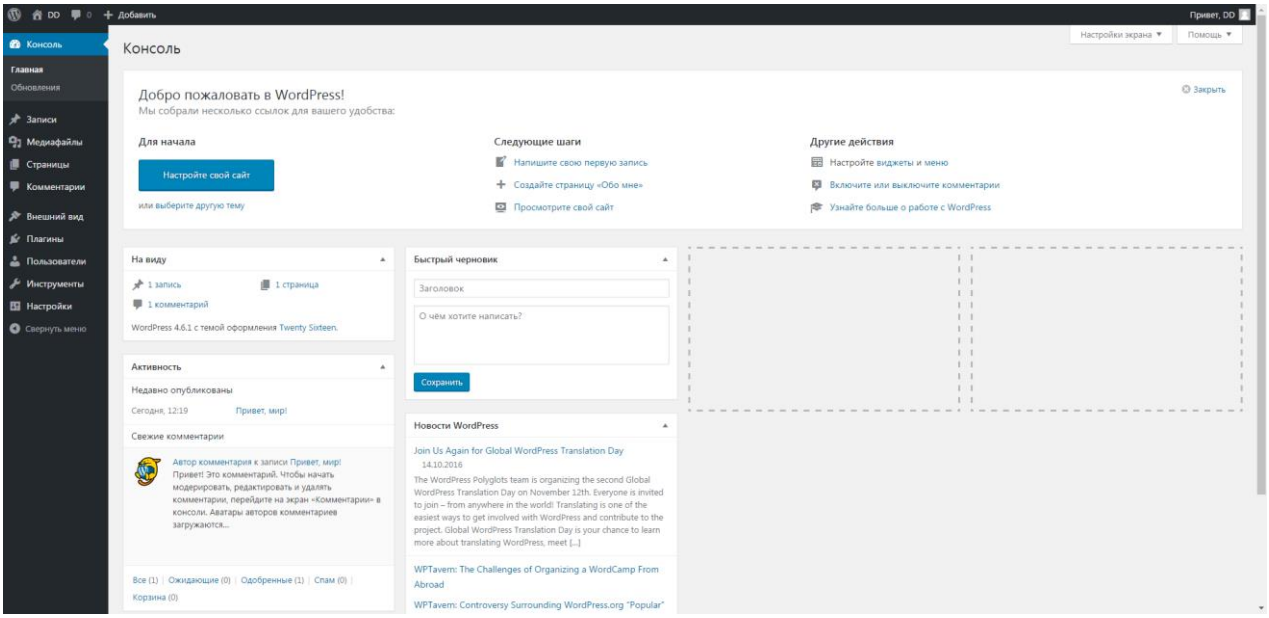
Веберете **U2F token.**

Подсоедените **JaCarta U2F** к USB порту и следуйте указаниям.

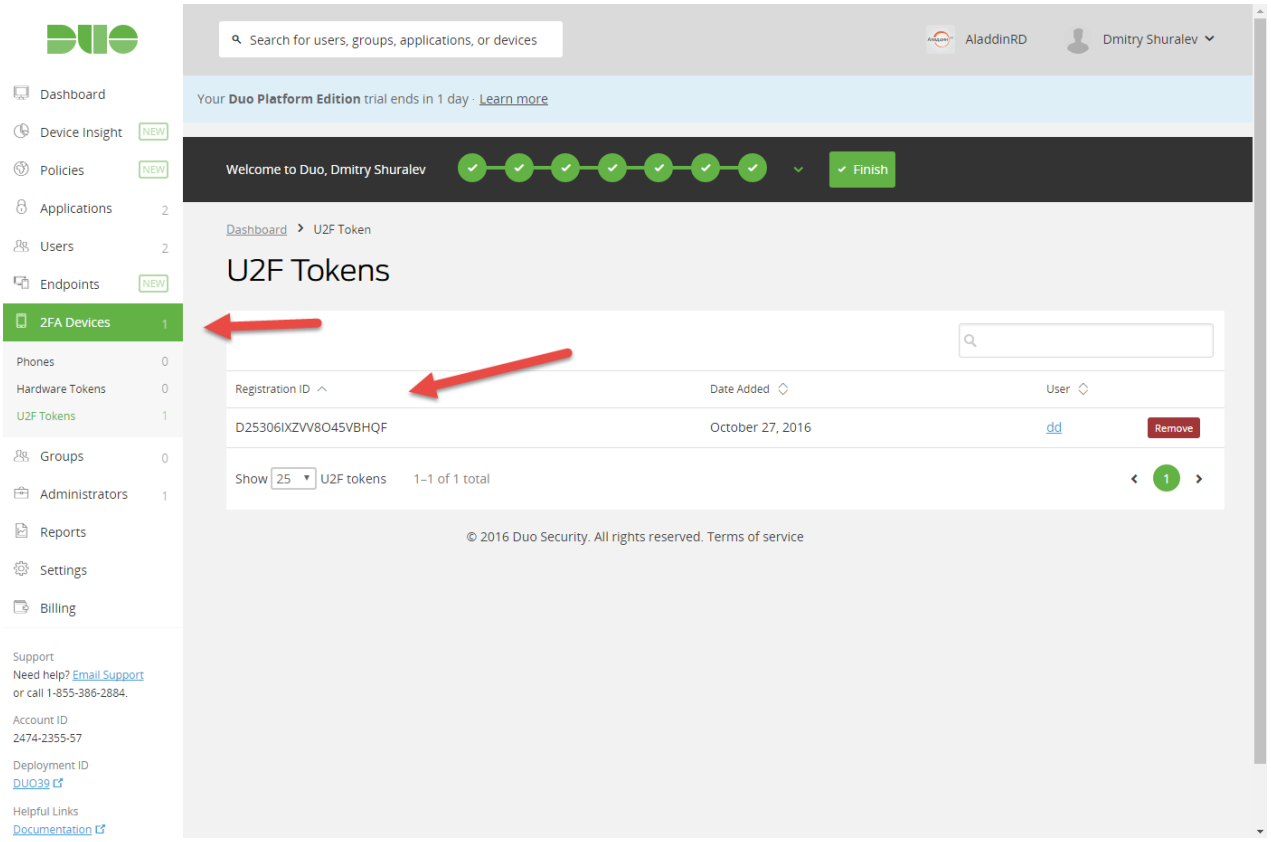


По завершению вы попадете в админ часть сайта, пройдя аутентификацию с использованием **JaCarta U2F.**





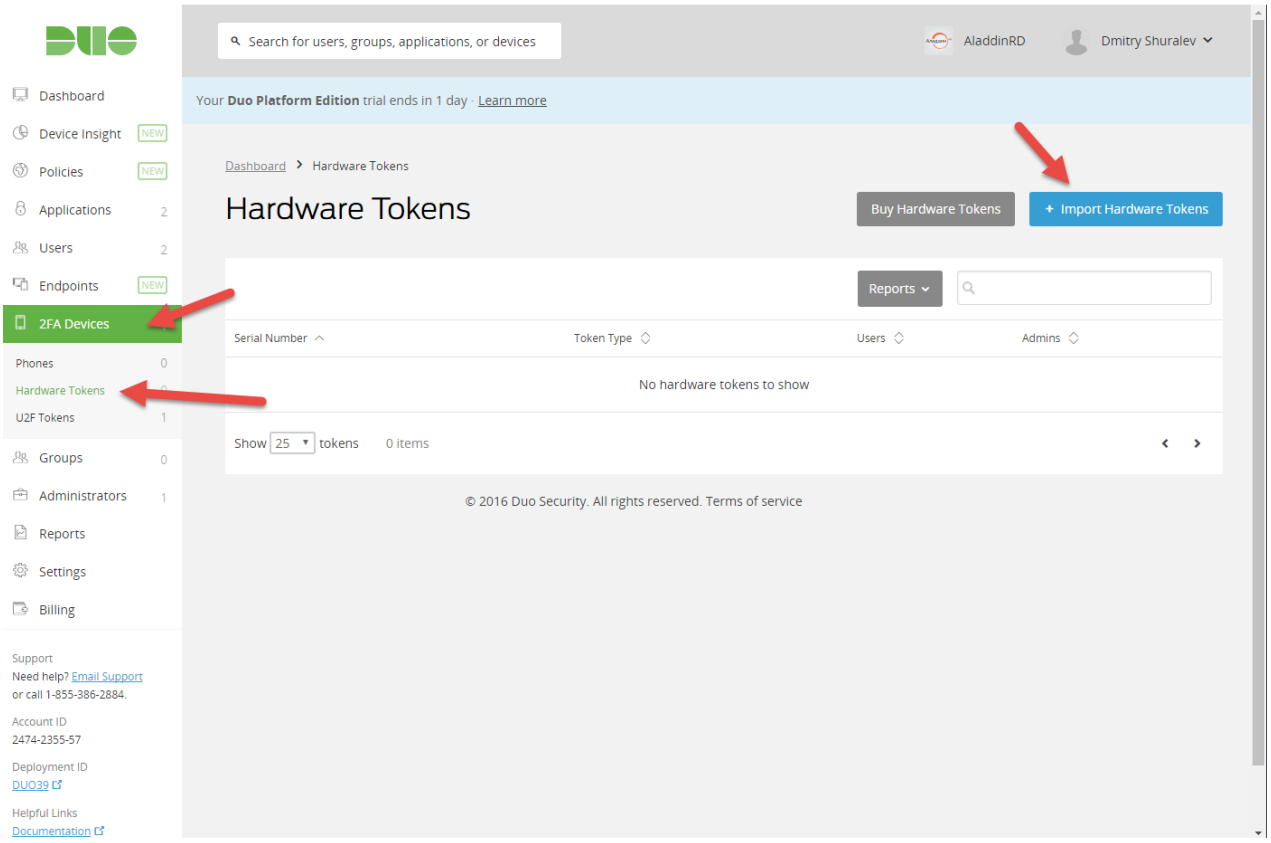
Снова зайдите в меню **2FA Devices (2Ф устройства)** в платформе Duo, в списке отобразится ранее добавленое устройство и его **ID.**



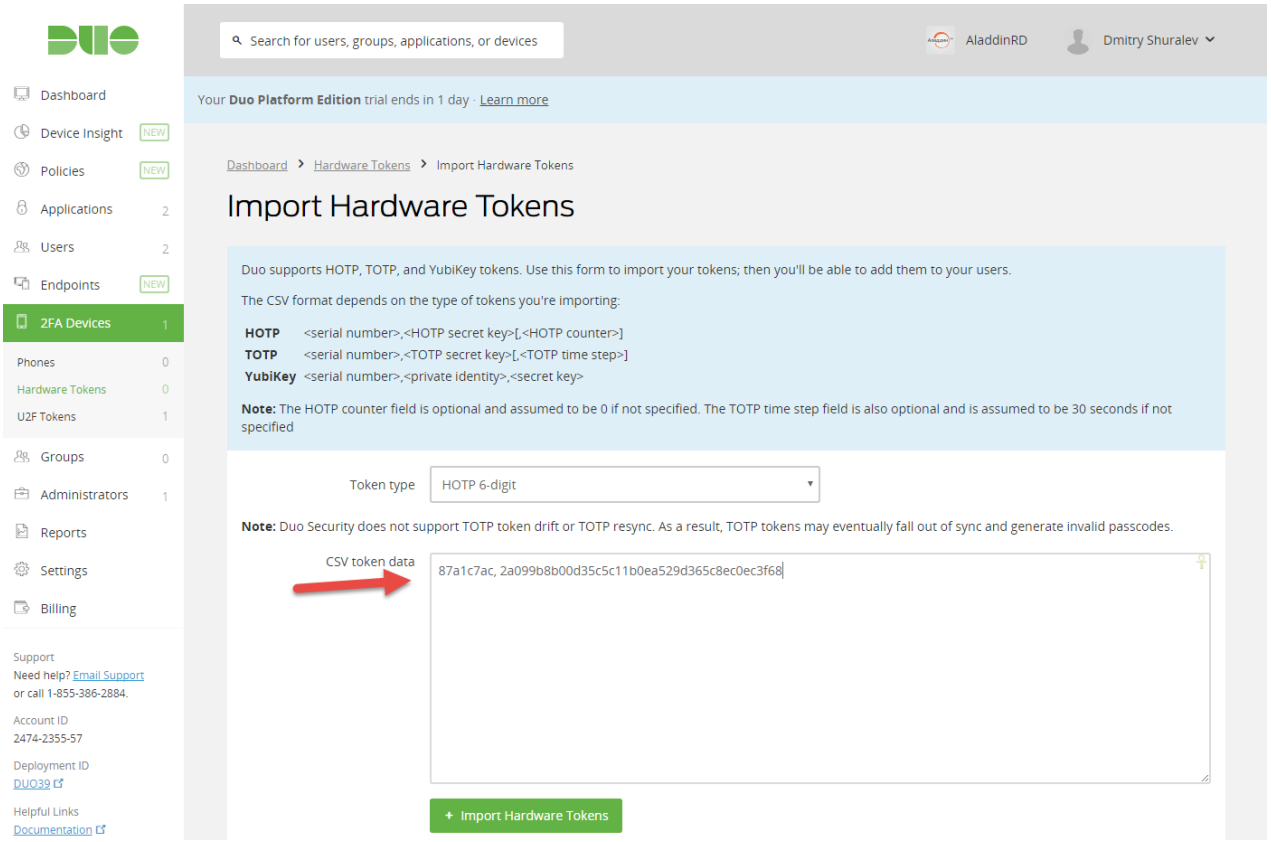
В дальнейшем этот пользователь сможет заходить на этот web-сайт с использованием **JaCarta U2F** из любого места в любое время.

Добавление электронного ключа JaCarta WebPass в платформу DUO

В отличие от **JaCarta U2F, JaCarta WebPass** добавляется со стороны сервера, тоесть через саму платформу **Duo.** Для этого, в левом меню откройте **2FA Devices (2Ф устройства) -> Hardware Tokens (Физический токен)**. Отобразятся настройки **Hardware Tokens.** Выберете **Import Hardware Tokens.**

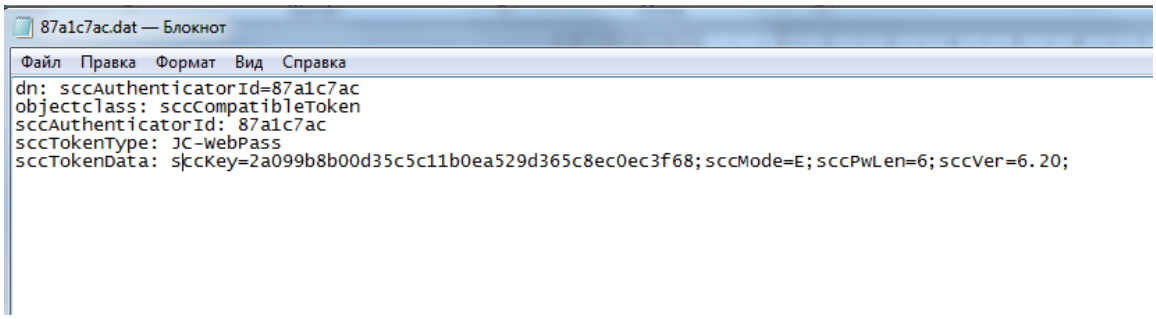


В отобразившемся меню необходимо выбрать тип токена, в нашем случае **HOTP** и ввести через запятую, как показано в примере его **серийный номер (serial number)** и **секрет (secret key)/SSID**



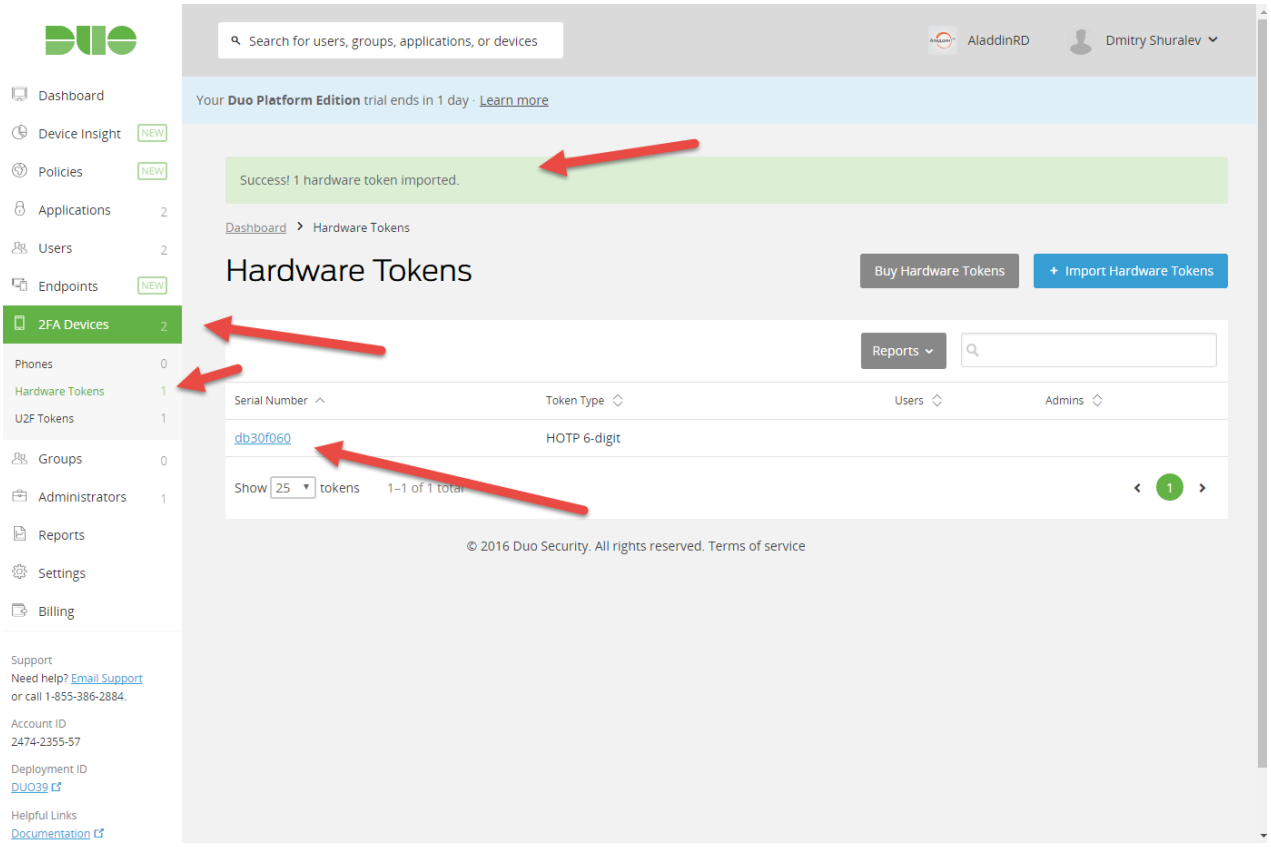
Эти данные необходимо взять из **.dat** файла из комплекта поставки ключей.

Serial number соотвествует полю **sccAuthenticatorId**, а **secret key** соответсвует полю **sccKey.**

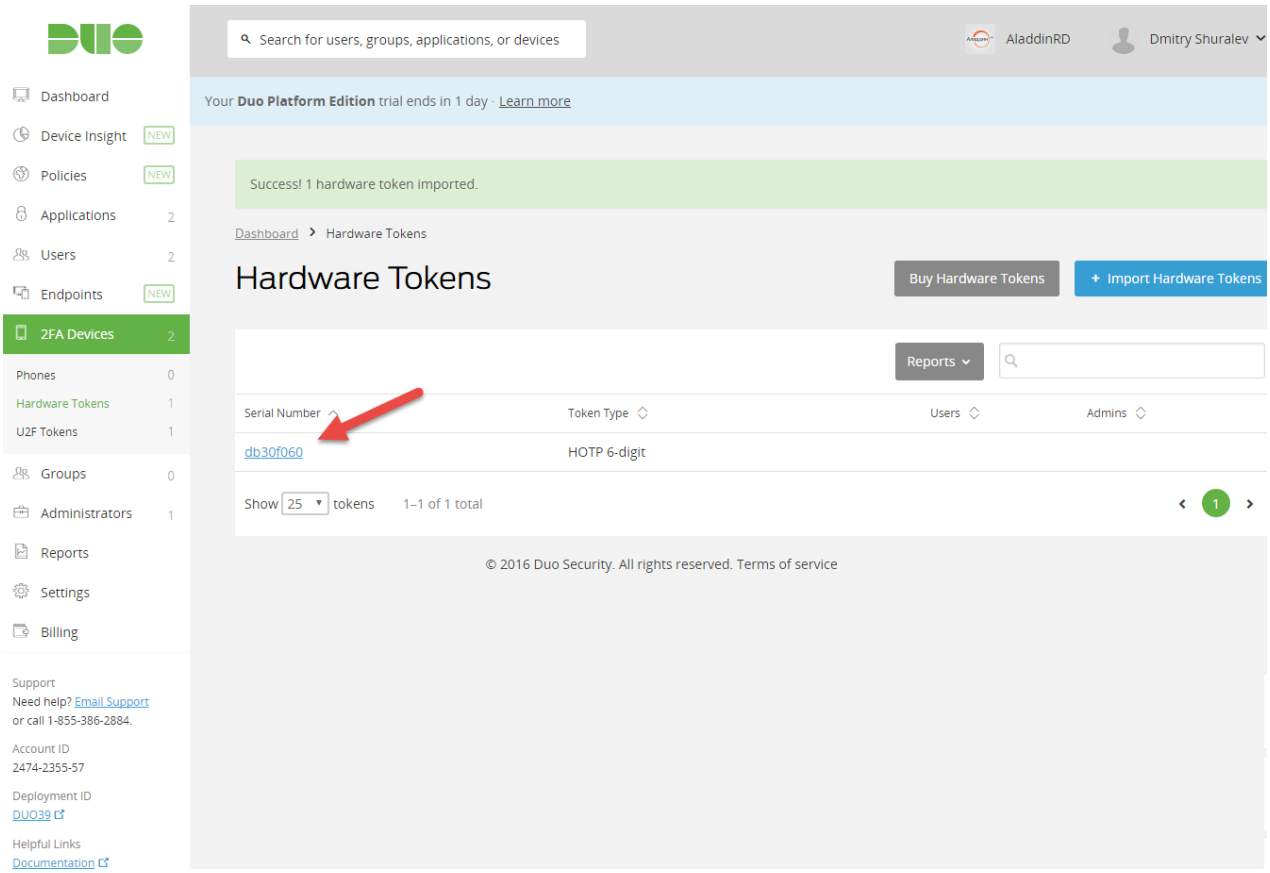


Если необходимо импортировать множество ключей, по очередно это делать не обязательно. В этом случае можно попросить содействия в службе поддержки DuoSecurity, передать им файл с перечнем информации о токенах, по их шаблону, и они произведут импорт со своей стороны.

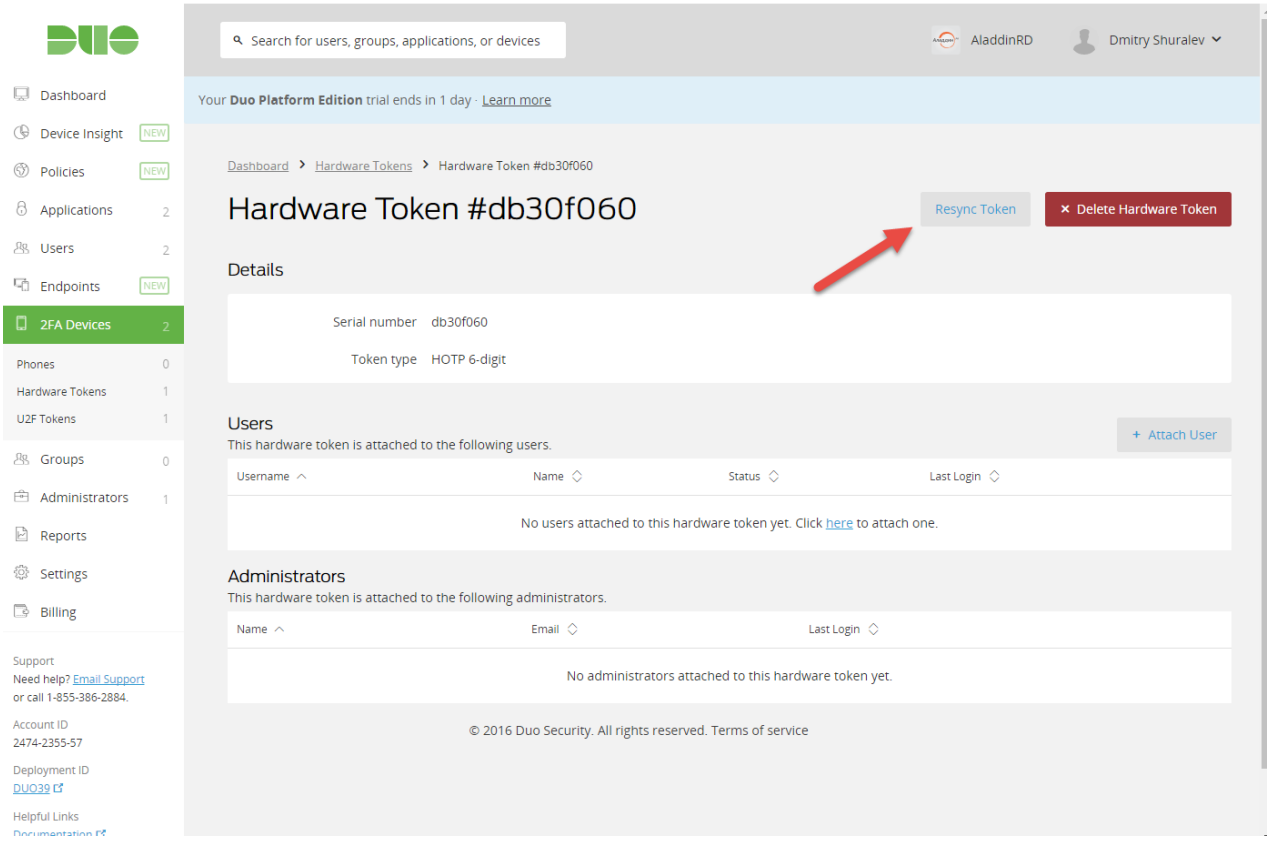
Если все введено верно отобразится сообщение **Success! 1 hardware token imported (Успех! Токен импортирован).** Так же в списке появится его серийный номер и тип.



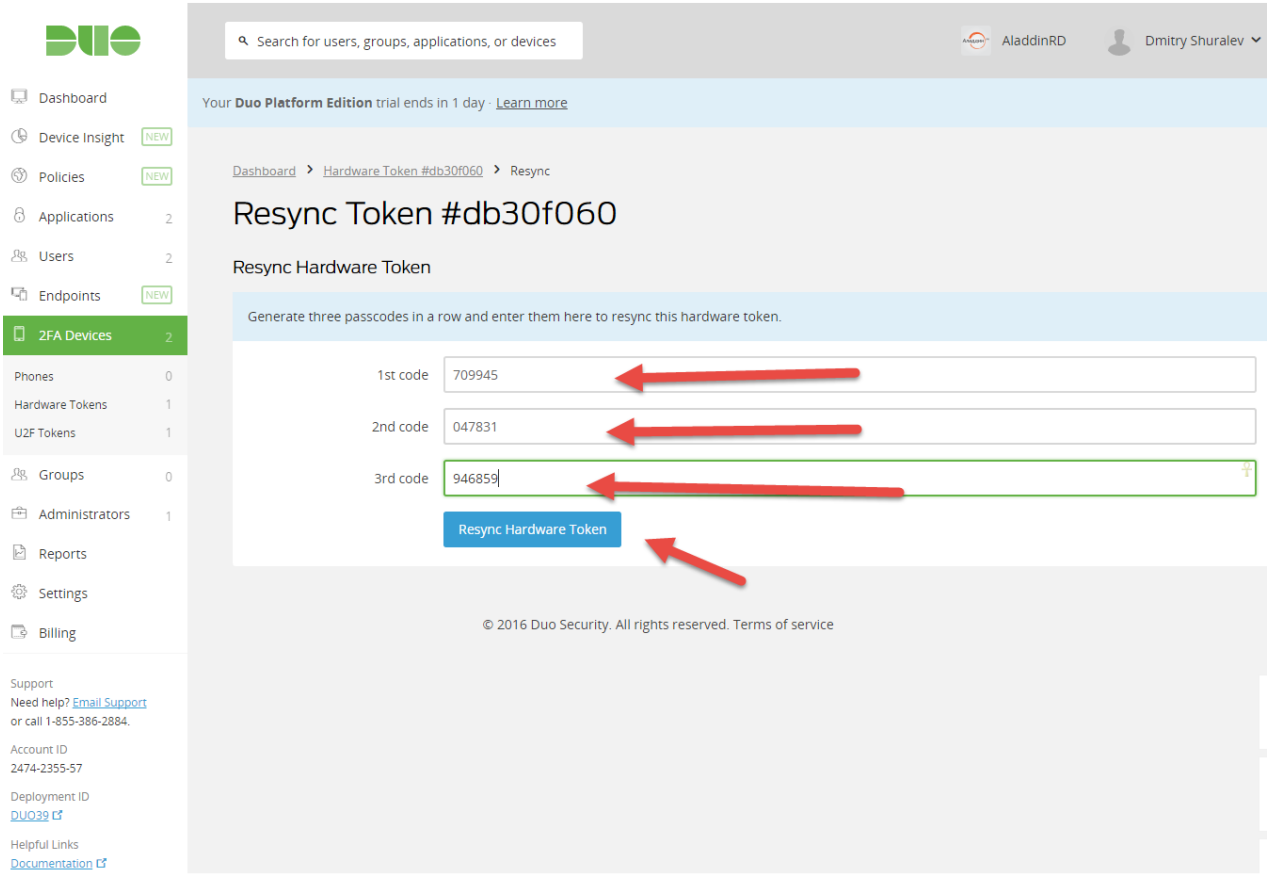
Зайдите в свойства токена щелкнув по его серийному номеру.



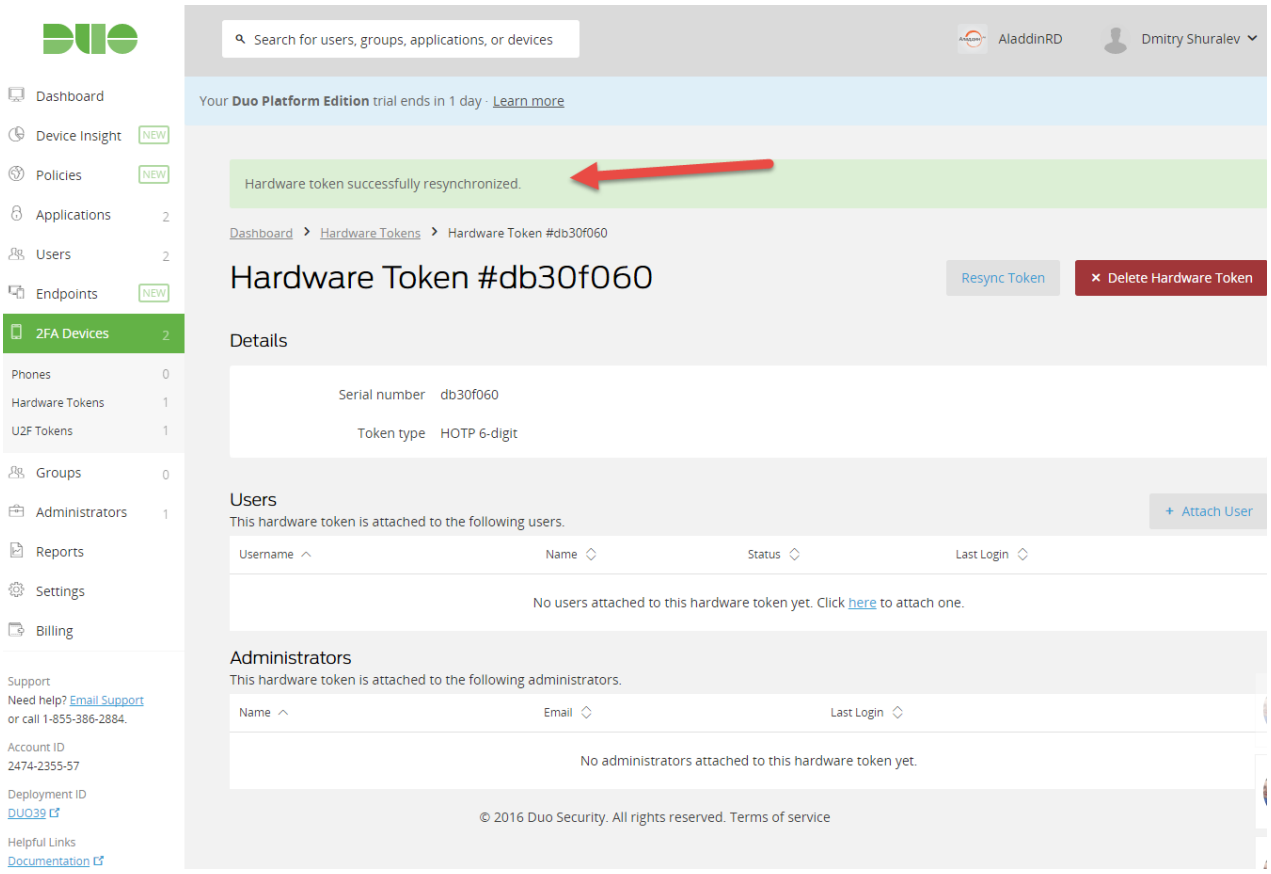
В верхнем меню выберете **Resync Token (Синхронизировать токен).**



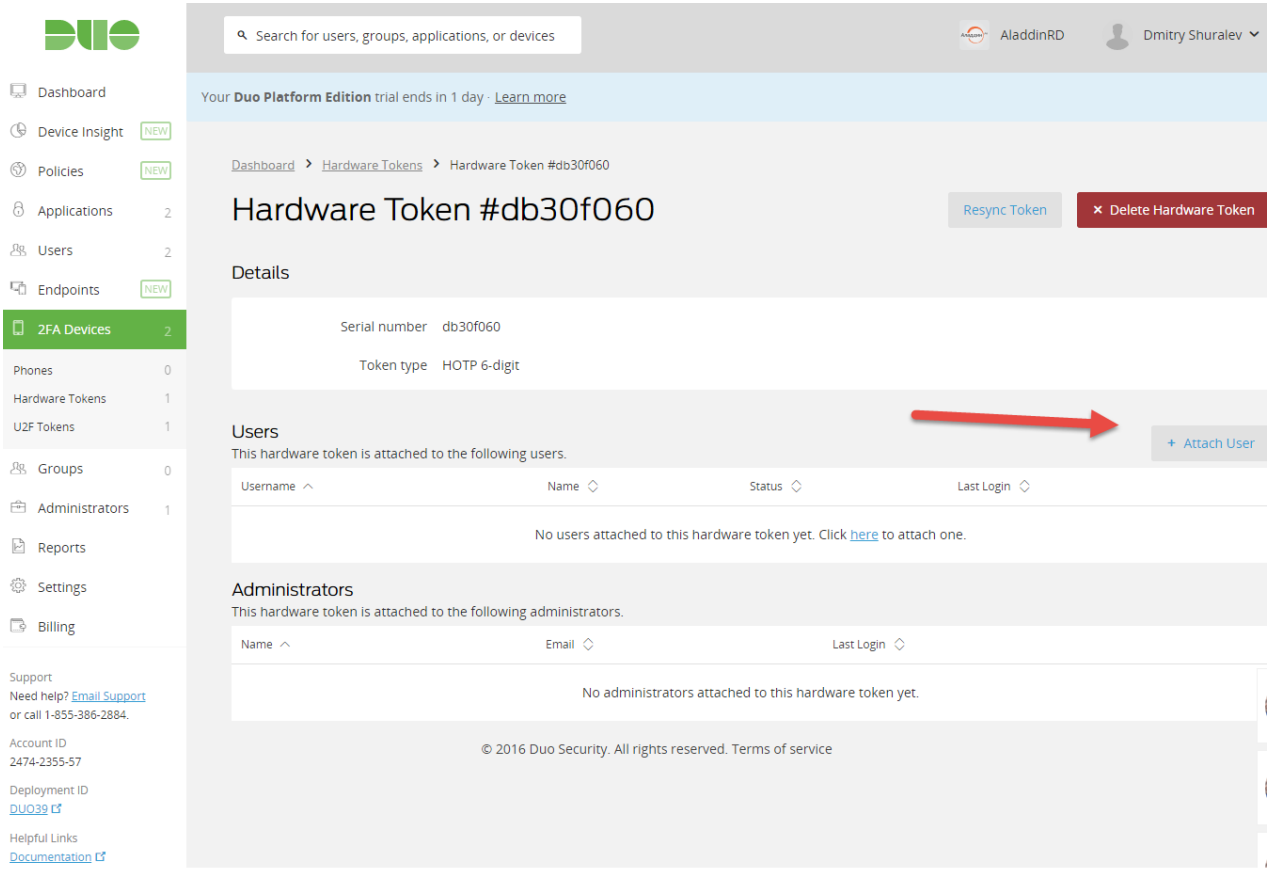
Поставьте курсор по очередно в каждое из трех отобразившихся полей и каждый раз нажимайте кнопку на токене формируя OTP-значение, после чего нажмите **Resync Hardware Token.**



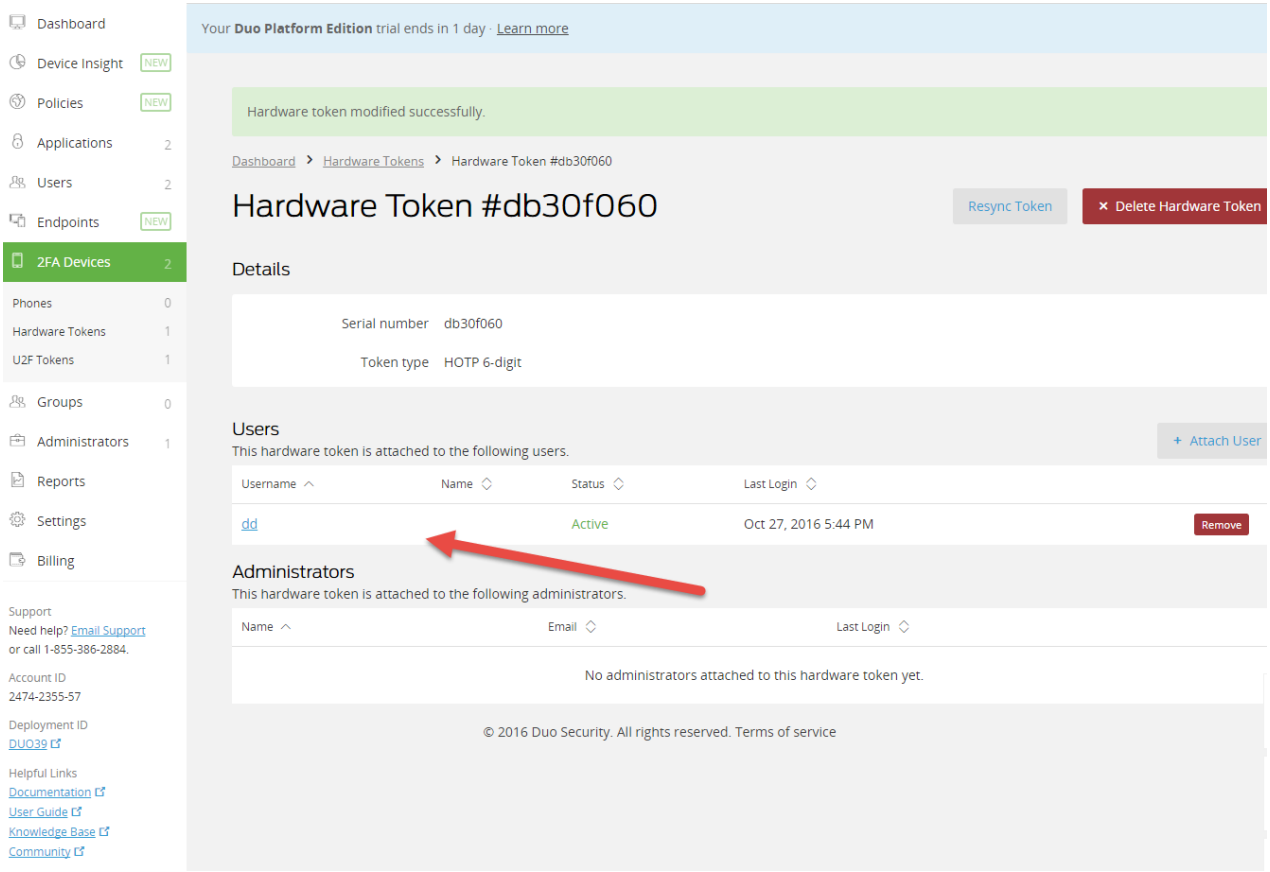
Если все введено верно отобразится сообщение **Hardware token successfully resyncronized (Токен успешно синхронизирован).**



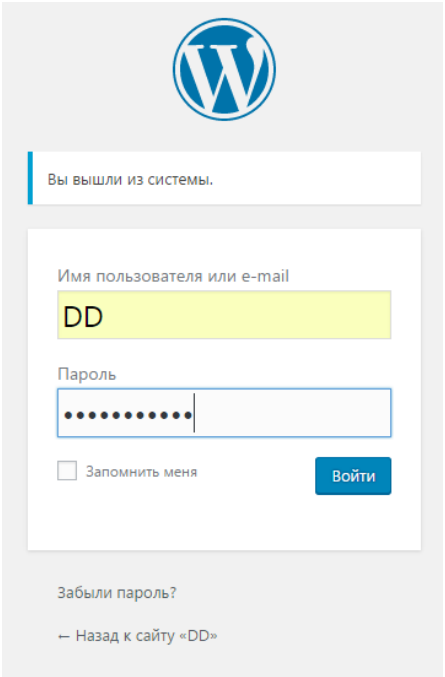
Нажмите **Attach User (Привязать пользователя)** для назначения пользователя для этого токена.



Выберете необходимого пользователя в отобразившемся списке.



Переключитесь на web-сайт и выполните аутентификацию пользователем которому вы ранее назначили токен.

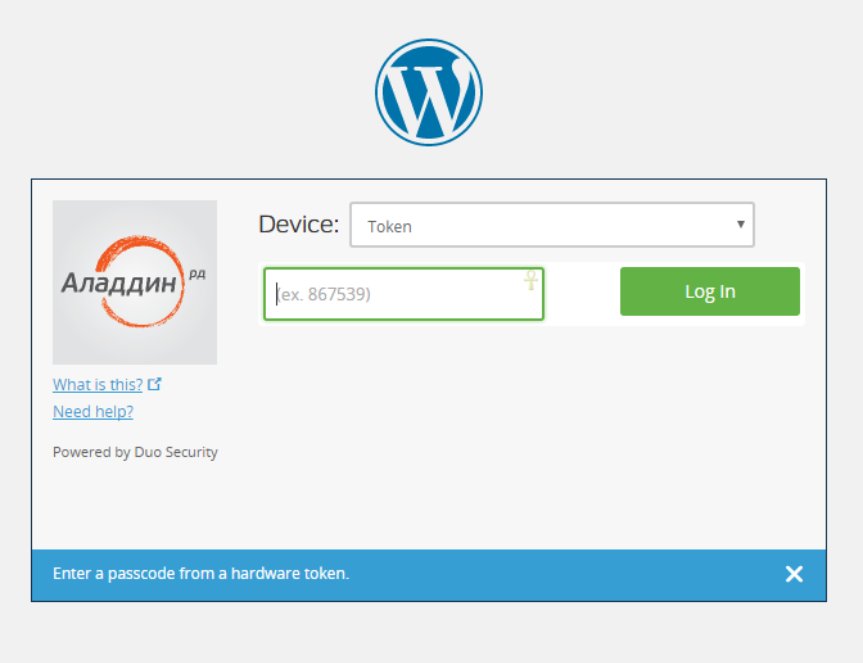


Плагин автоматически увидит, что пользователю назначен токен и предложит ввести OTP-значение.

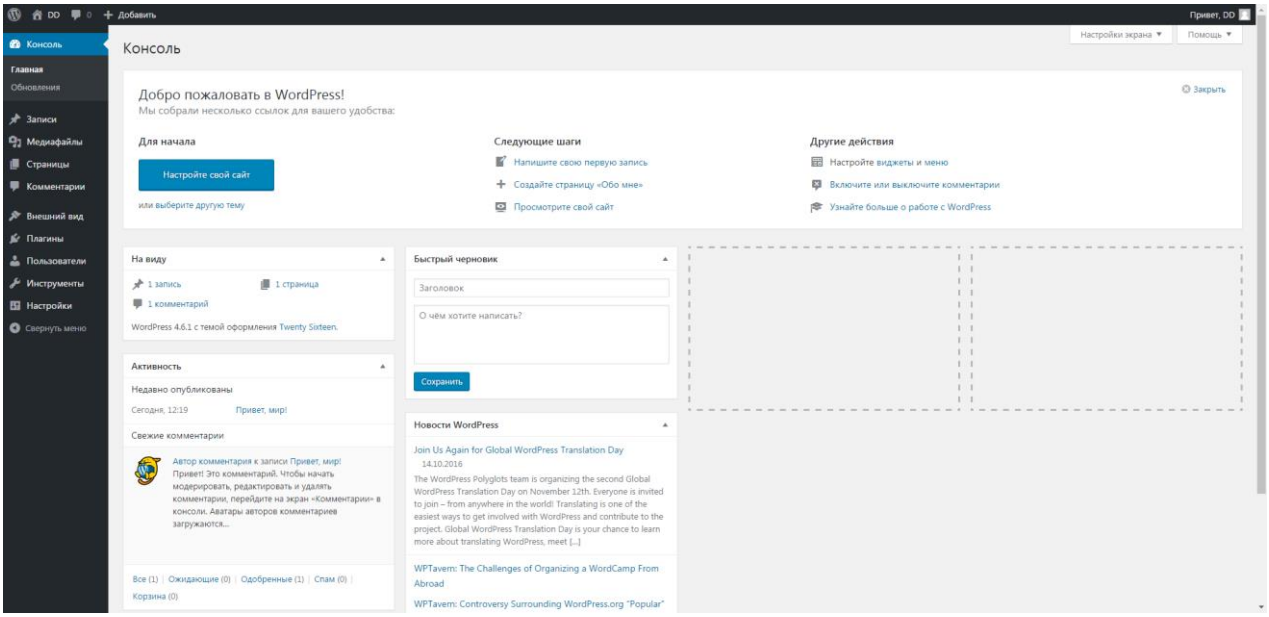
Нажмите **Enter a Passcode.**

Нажмите кнопку на токене, OTP-значенеи подставится в поле автоматически.

Нажмите **Log In.**



Отобразится админ панель web-сайта, аутентификация при помощи **JaCarta WebPass** пройдена.



Защита других приложений и протоколов

По аналогии можно подключить токены JaCarta WebPass и JaCartaU2F и к другим приложениям или протоколами котоорые поддерживаются платформой DUO Security. Полный список поддерживаемых приложений и протоколов смотрите на официальном сайте платформы Duo — https://duo.com/docs

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 веб-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

Версия	Изменения
1.0	Исходная версия 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.К00073 от 20.08.13
Microsoft Silver OEM Hardware Partner, Apple Developer, Oracle Gold Partner

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