



# 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**.

Настоящий документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации. Обладателем исключительных авторских и имущественных прав является ЗАО «Аладдин Р. Д.». Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ.

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены компанией «Аладдин Р. Д.» без предварительного уведомления. Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе компания «Аладдин Р. Д.» не предоставляет никаких ни явных, ни подразумеваемых гарантий.

Владельцем товарных знаков Аладдин, Aladdin, JaCarta, логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является ЗАО «Аладдин Р. Д.».

Владельцем товарных знаков Apple, iPad, iPhone, Mac OS, OS X является корпорация Apple Inc. Владельцем товарного знака IOS является компания Cisco (Cisco Systems, Inc). Владельцем товарного знака Windows Vista и др. — корпорация Microsoft (Microsoft Corporation). Названия прочих технологий, продуктов, компаний, упоминающихся в данном документе, могут являться товарными знаками своих законных владельцев.

Сведения, приведённые в данном документе, актуальны на дату его публикации.

При перепечатке и использовании данных материалов либо любой их части ссылки на ЗАО «Аладдин Р. Д.» обязательны.

© ЗАО «Аладдин Р. Д.», 1995–2017. Все права защищены.

# Оглавление

О платформе Duo Security	4
Об Электронных ключах JaCarta WebPass/U2F	5
JaCarta WebPass	5
JaCarta U2F	6
Подключение web-плагина DUO Security к web-сайту на CMS WordPress	7
Добавление электронного ключа JaCarta U2F в платформу DUO	11
Добавление электронного ключа JaCarta WebPass в платформу DUO	16
Защита других приложений и протоколов	26
Контакты, техническая поддержка	27
Регистрация изменений	28

# 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 "ОТР 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 межсетевое 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 объемом 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.

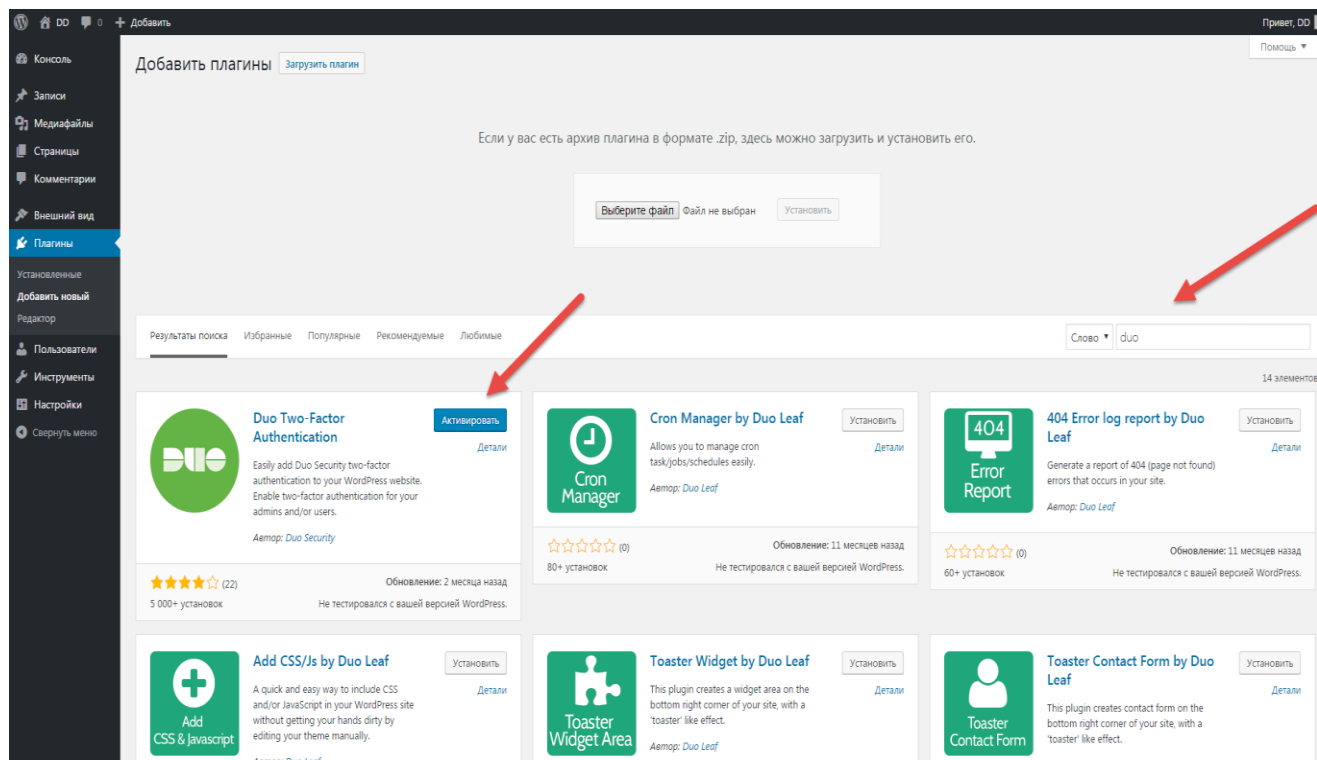
# Подключение web-плагина DUO Security к web-сайту на CMS WordPress

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>

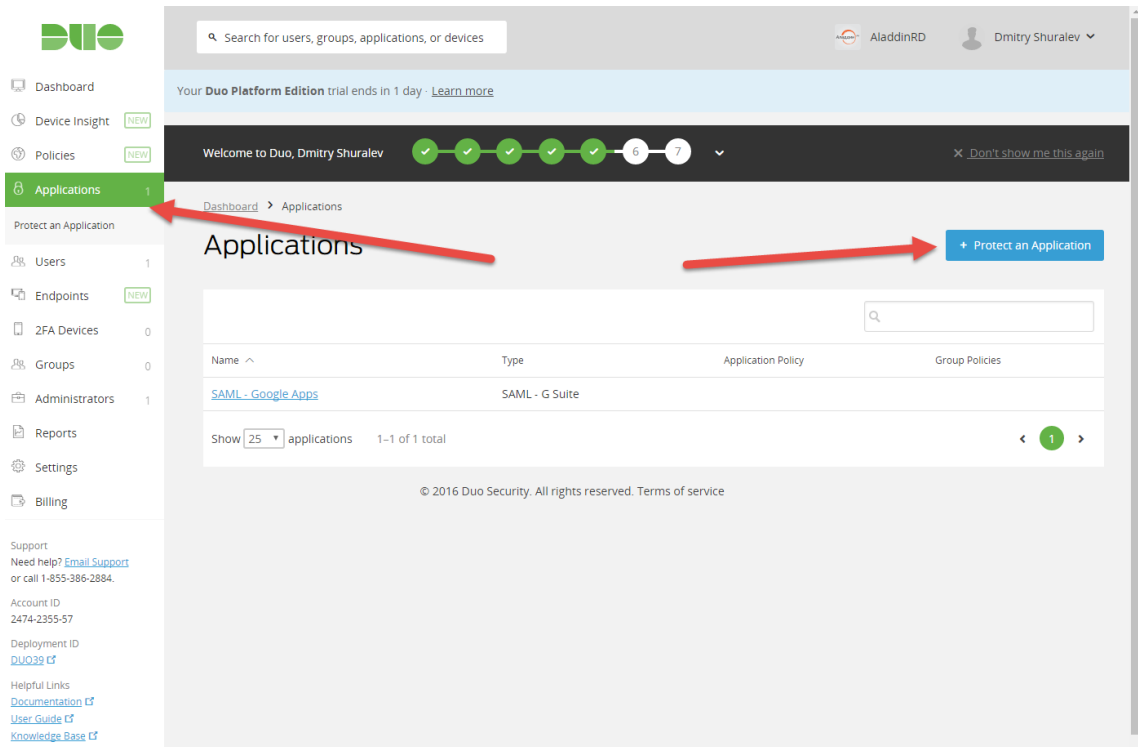
Чтобы защитить какое либо приложение или протокол, по средствам платформы DUO, необходимо выбрать что защищать в самой платформе и связать платформу с защищаемым приложением. В настоящем примере необходимо выполнить следующие действия.

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**.

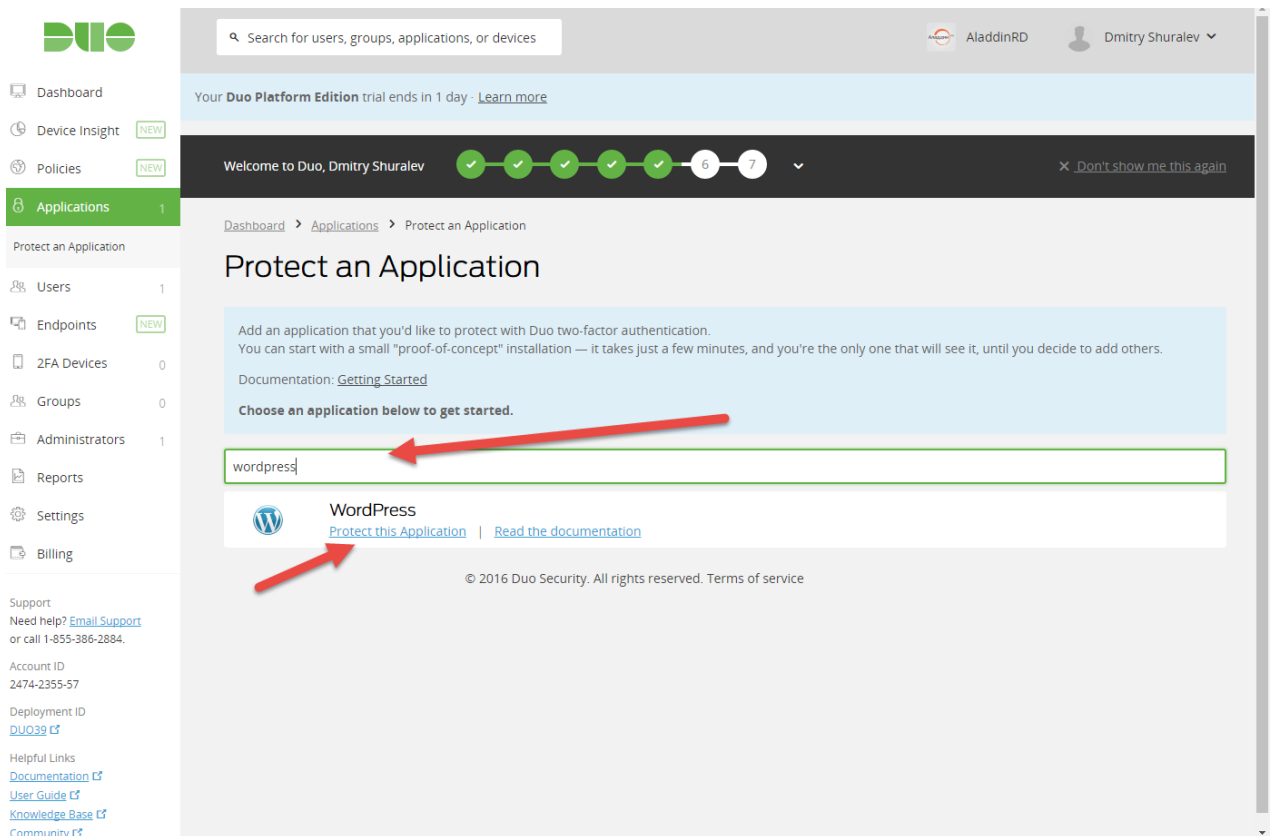


The screenshot shows the WordPress dashboard's 'Add Plugins' page. The search bar at the top right contains the text 'duo'. Below the search bar, a grid of plugin cards is displayed. The first card, 'Duo Two-Factor Authentication' by Duo Security, is highlighted with a red arrow pointing to its 'Активировать' (Activate) button. Another red arrow points to the search bar, and a third red arrow points to the 'Установить' (Install) button of the 'Duo Two-Factor Authentication' plugin. The interface includes a sidebar on the left with navigation options like 'Консоль', 'Зачислы', 'Медиафайлы', 'Страницы', 'Комментарии', 'Внешний вид', 'Плагины', 'Установленные', 'Добавить новый', 'Редактор', 'Пользователи', 'Инструменты', 'Настройки', and 'Свернуть меню'. The main content area has a header 'Добавить плагины' and a sub-header 'Если у вас есть архив плагина в формате .zip, здесь можно загрузить и установить его.' with a 'Выберите файл' button and a 'Установить' button. Below the search bar, there are tabs for 'Результаты поиска', 'Избранные', 'Популярные', 'Рекомендуемые', and 'Любимые'. The search results show 14 elements.

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)**.

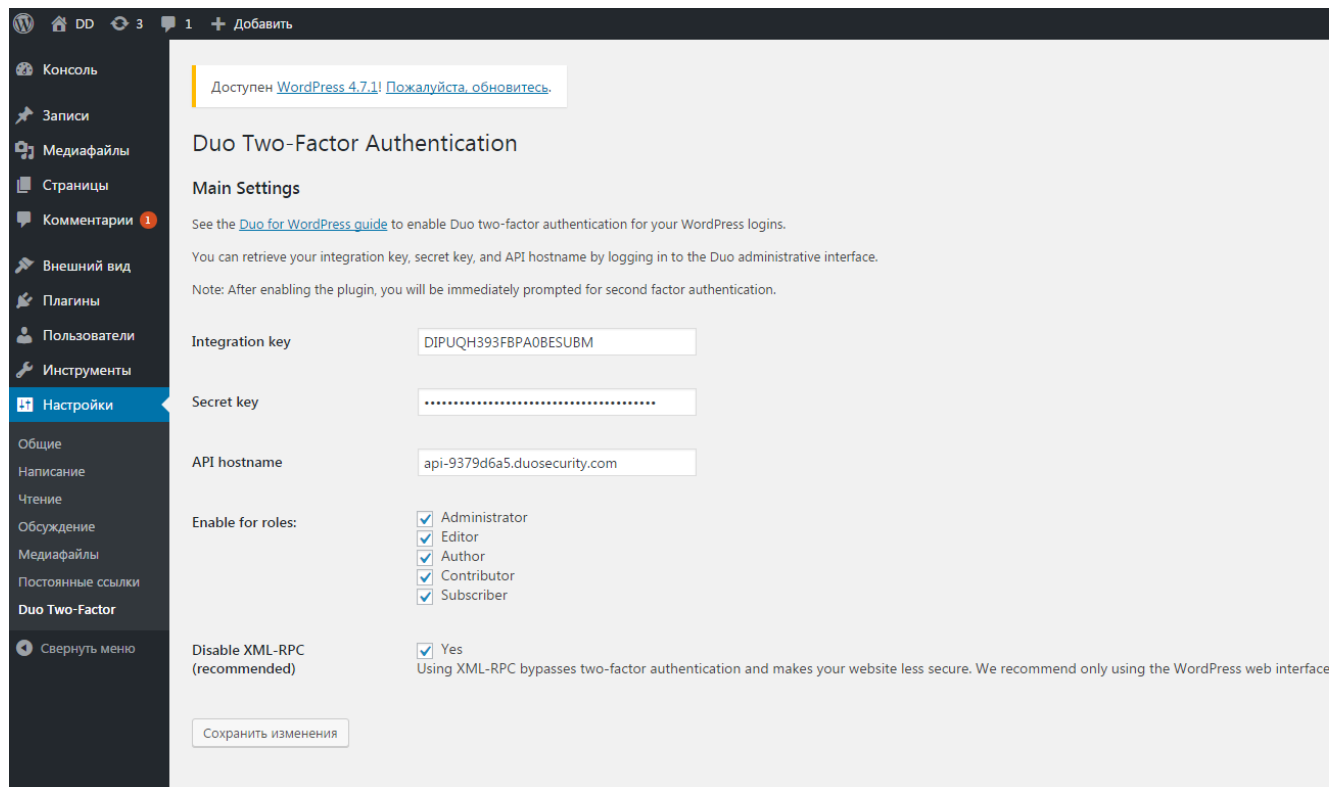




4. Отобразятся 3 ключевых поля, **Integration Key**, **Secret Key** и **API Hostname**.

The screenshot displays the Duo Security management console. On the left is a navigation sidebar with options like Dashboard, Device Insight, Policies, Applications, Users, Endpoints, 2FA Devices, Groups, Administrators, Reports, Settings, and Billing. The main content area shows the 'WordPress' application configuration. A green notification banner at the top states 'Successfully added WordPress to protected applications.' Below this, the 'Details' section contains three input fields: 'Integration key' (value: D1P0Q8393FBPA0BESUBM), 'Secret key' (value: Click to view), and 'API hostname' (value: api-9379d6a5.duosecurity.com). Red arrows point to each of these fields. The 'Settings' section below includes a 'General' tab with fields for 'Type' (WordPress), 'Name' (WordPress), 'Self-service portal' (checkbox), 'Username normalization' (radio buttons for None and Simple), 'Voice greeting' (text area with 'Welcome to Duo.'), 'Notes' (text area), and 'Permitted groups' (checkbox and 'Select groups' dropdown). A red arrow points to the 'Save Changes' button at the bottom of the settings panel. The footer of the page reads '© 2016 Duo Security. All rights reserved. Terms of service'.

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

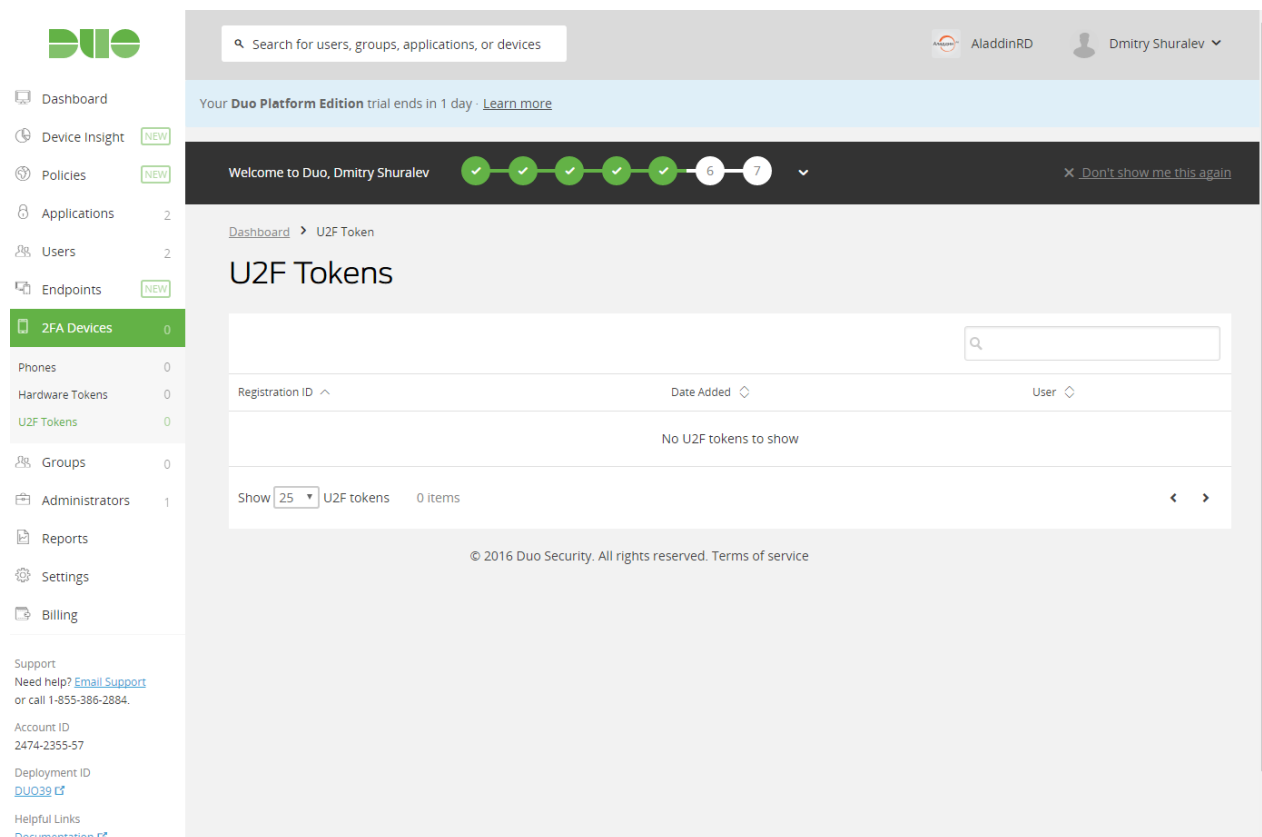


6. На этом настройка связи web-сайта с платформой Duo завершена, далее необходимо добавить в систему пользователя и токен.

# Добавление электронного ключа JaCarta U2F в платформу DUO

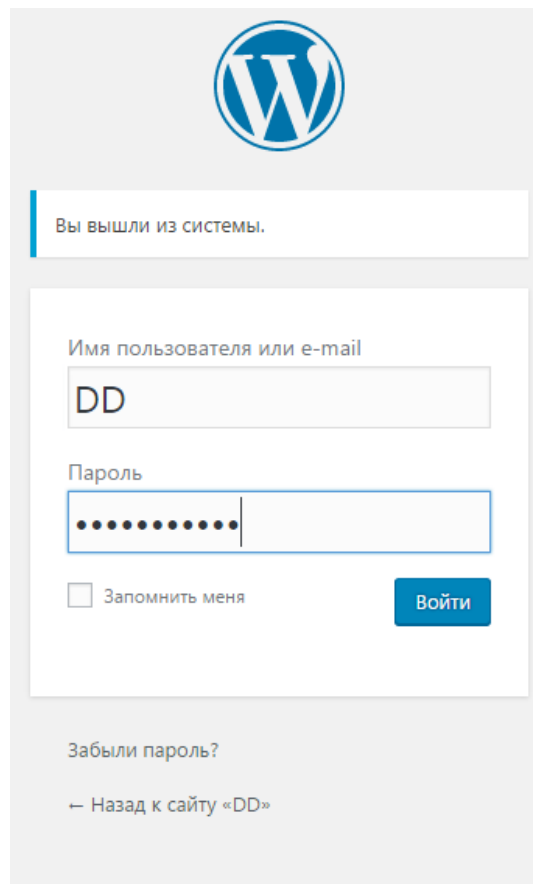
Добавление электронных ключей **JaCarta U2F** происходит пользователем со стороны web-сайта.

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



The screenshot shows the Duo Security web interface. The top navigation bar includes the Duo logo, a search bar, and user information for AladdinRD and Dmitry Shuralev. A notification banner indicates that the Duo Platform Edition trial ends in 1 day. The main content area is titled 'U2F Tokens' and features a search bar and a table with columns for 'Registration ID', 'Date Added', and 'User'. The table is currently empty, displaying the message 'No U2F tokens to show'. The left sidebar shows the navigation menu with '2FA Devices' highlighted, and a count of 0 items. The footer of the page includes the copyright notice '© 2016 Duo Security. All rights reserved. Terms of service'.

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

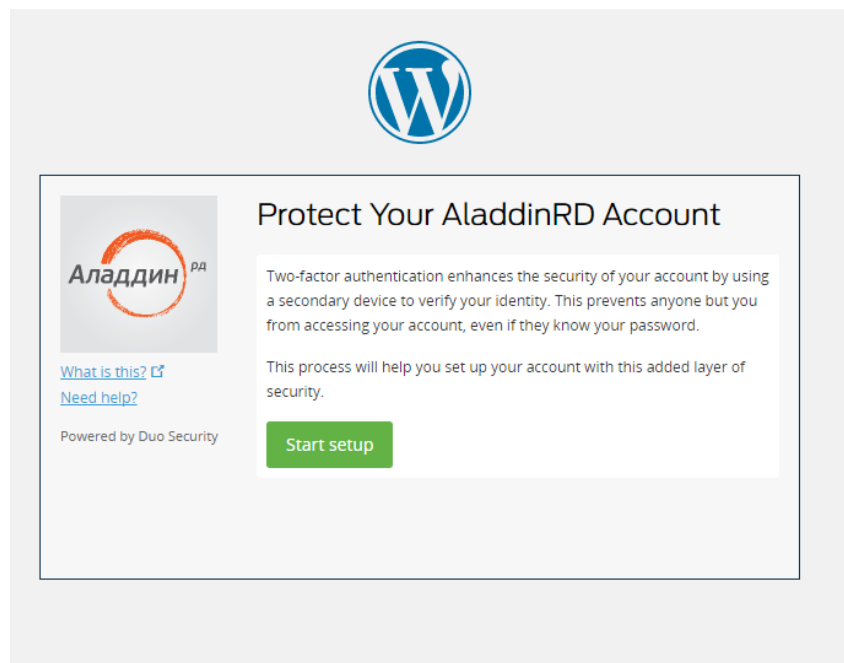


The image shows a WordPress login page. At the top center is the WordPress logo. Below it, a message reads "Вы вышли из системы." (You have logged out of the system). The main login form contains the following elements:

- A label "Имя пользователя или e-mail" (Username or email) above a text input field containing "DD".
- A label "Пароль" (Password) above a password input field with masked characters (dots).
- A checkbox labeled "Запомнить меня" (Remember me) which is currently unchecked.
- A blue button labeled "Войти" (Log in).

Below the login form, there is a link "Забыли пароль?" (Forgot password?) and a link "← Назад к сайту «DD»" (← Back to the «DD» site).

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



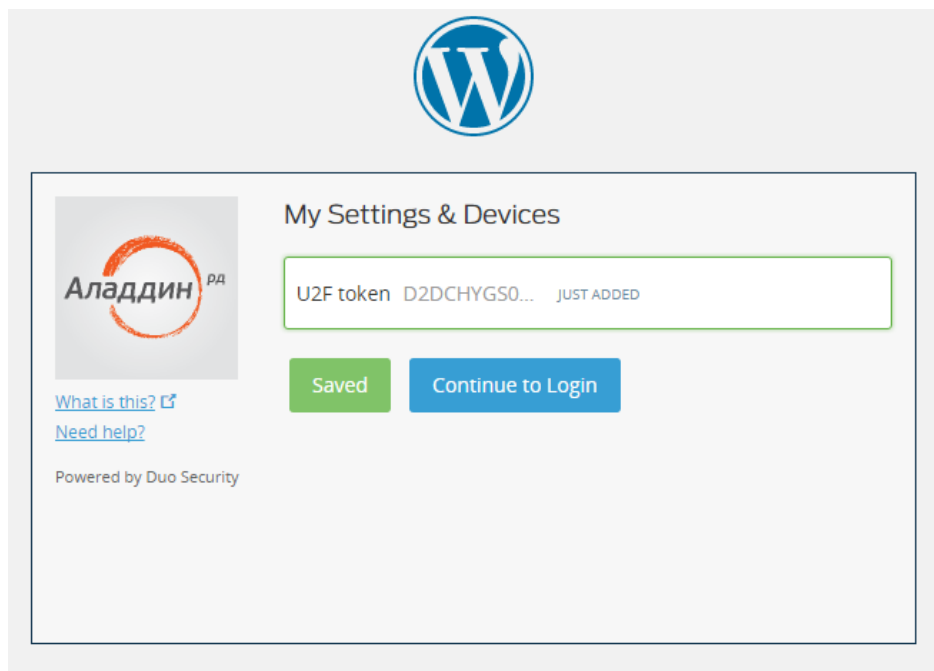
The image shows a Duo Security setup screen for an Aladdin RD account. At the top center is the WordPress logo. The main content area is titled "Protect Your AladdinRD Account" and includes the following information:

- A logo for "Аладдин РД" (Aladdin RD) on the left.
- Text explaining that two-factor authentication enhances security by using a secondary device to verify identity.
- A statement: "This process will help you set up your account with this added layer of security."
- A green button labeled "Start setup".
- Links for "What is this?" and "Need help?".
- Text at the bottom left: "Powered by Duo Security".

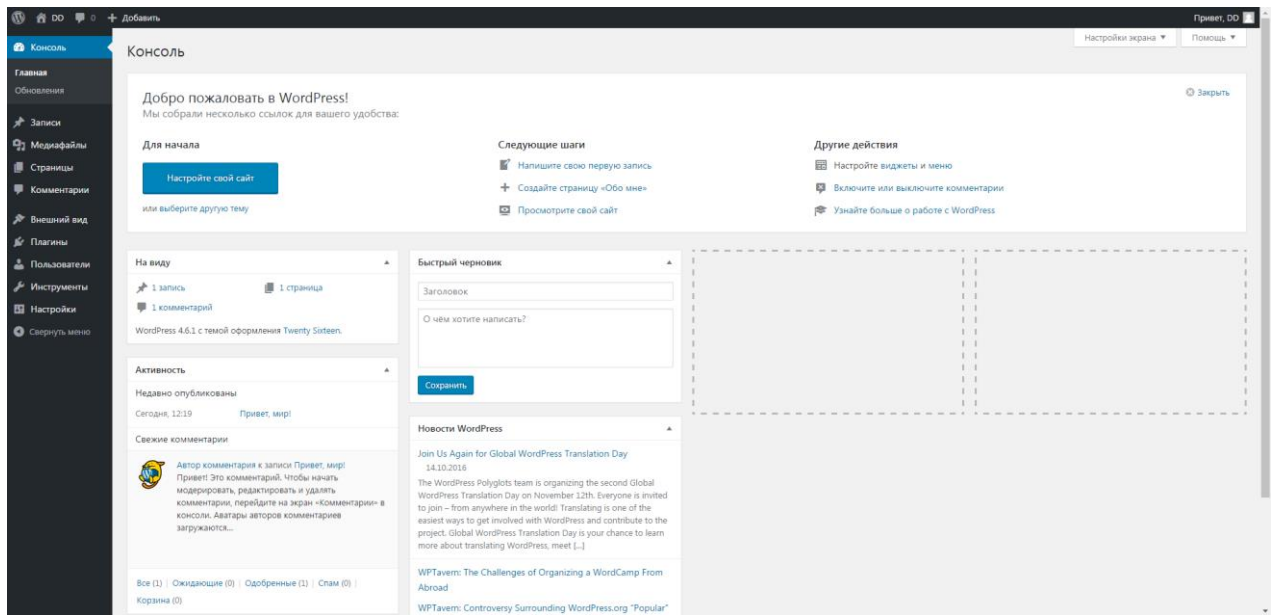
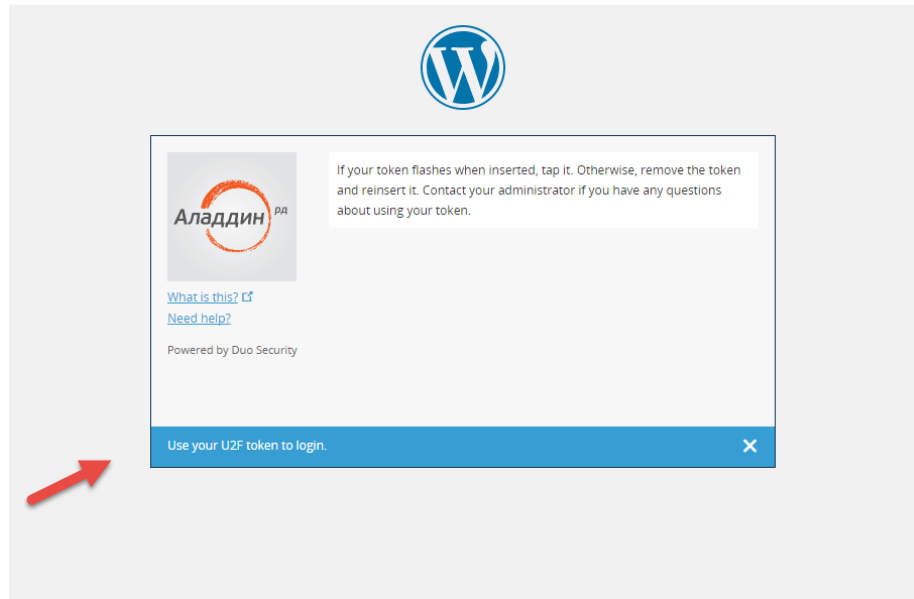
Выберите **U2F token**.



Подсоедините **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 добавленное устройство и его ID.

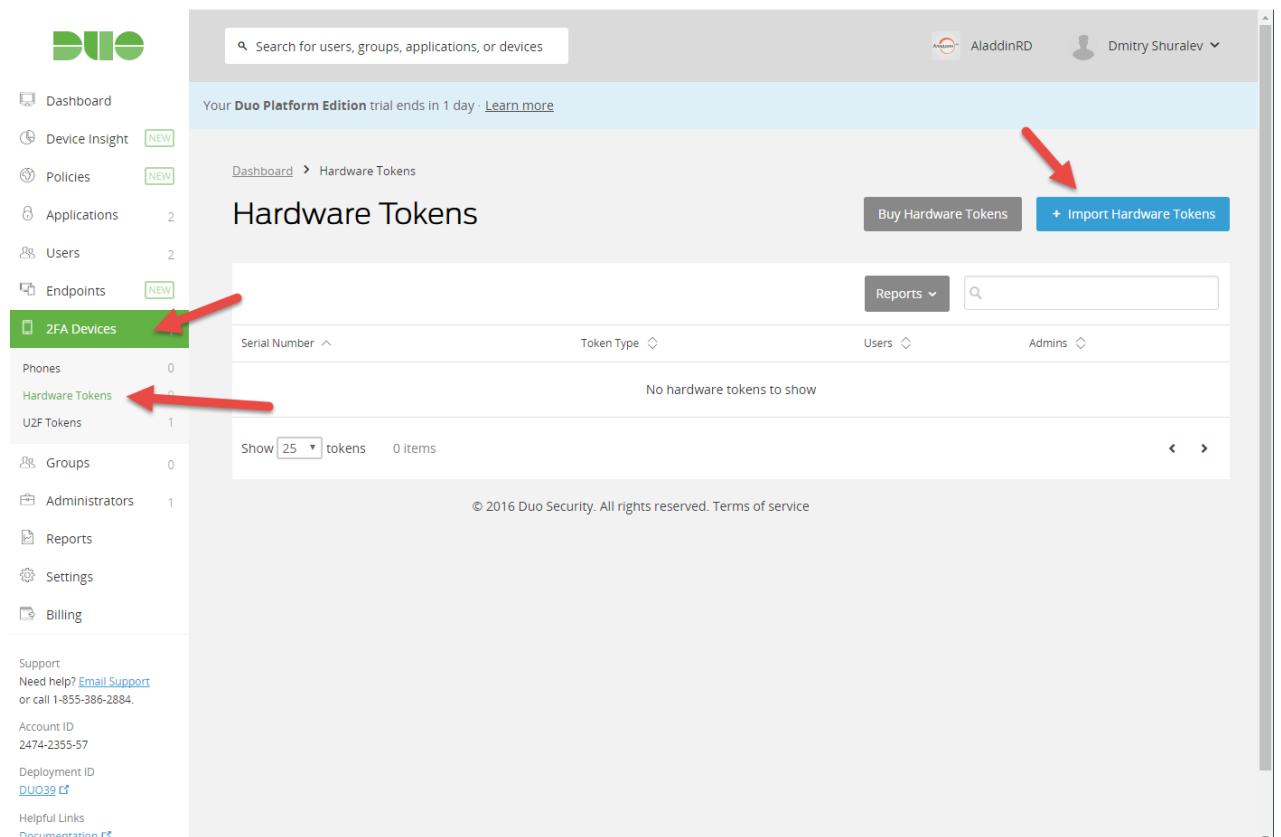
The screenshot shows the Duo Security dashboard interface. On the left sidebar, the '2FA Devices' menu item is highlighted in green. The main content area displays the 'U2F Tokens' page. A table lists the registered U2F tokens. The first row shows a registration ID of 'D25306IXZVW8O45VBHQF', added on 'October 27, 2016', for the user 'dd'. A 'Remove' button is visible next to the user name. Below the table, it indicates '1-1 of 1 total' U2F tokens. Two red arrows are overlaid on the image: one points to the '2FA Devices' menu item in the sidebar, and the other points to the registration ID in the table.

Registration ID	Date Added	User
D25306IXZVW8O45VBHQF	October 27, 2016	dd

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, то есть через саму платформу **Duo**. Для этого, в левом меню откройте **2FA Devices (2Ф устройства)** -> **Hardware Tokens (Физический токен)**. Отобразятся настройки **Hardware Tokens**. Выберите **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**

Search for users, groups, applications, or devices

Your Duo Platform Edition trial ends in 1 day · [Learn more](#)

Dashboard > Hardware Tokens > Import Hardware Tokens

## Import Hardware Tokens

Duo supports HOTP, TOTP, and YubiKey tokens. Use this form to import your tokens; then you'll be able to add them to your users.

The CSV format depends on the type of tokens you're importing:

**HOTP** <serial number>,<HOTP secret key>[,<HOTP counter>]  
**TOTP** <serial number>,<TOTP secret key>[,<TOTP time step>]  
**YubiKey** <serial number>,<private identity>,<secret key>

**Note:** The HOTP counter field is optional and assumed to be 0 if not specified. The TOTP time step field is also optional and is assumed to be 30 seconds if not specified

Token type: HOTP 6-digit

**Note:** Duo Security does not support TOTP token drift or TOTP resync. As a result, TOTP tokens may eventually fall out of sync and generate invalid passcodes.

CSV token data: 87a1c7ac, 2a099b8b00d35c5c11b0ea529d365c8ec0ec3f68

+ Import Hardware Tokens

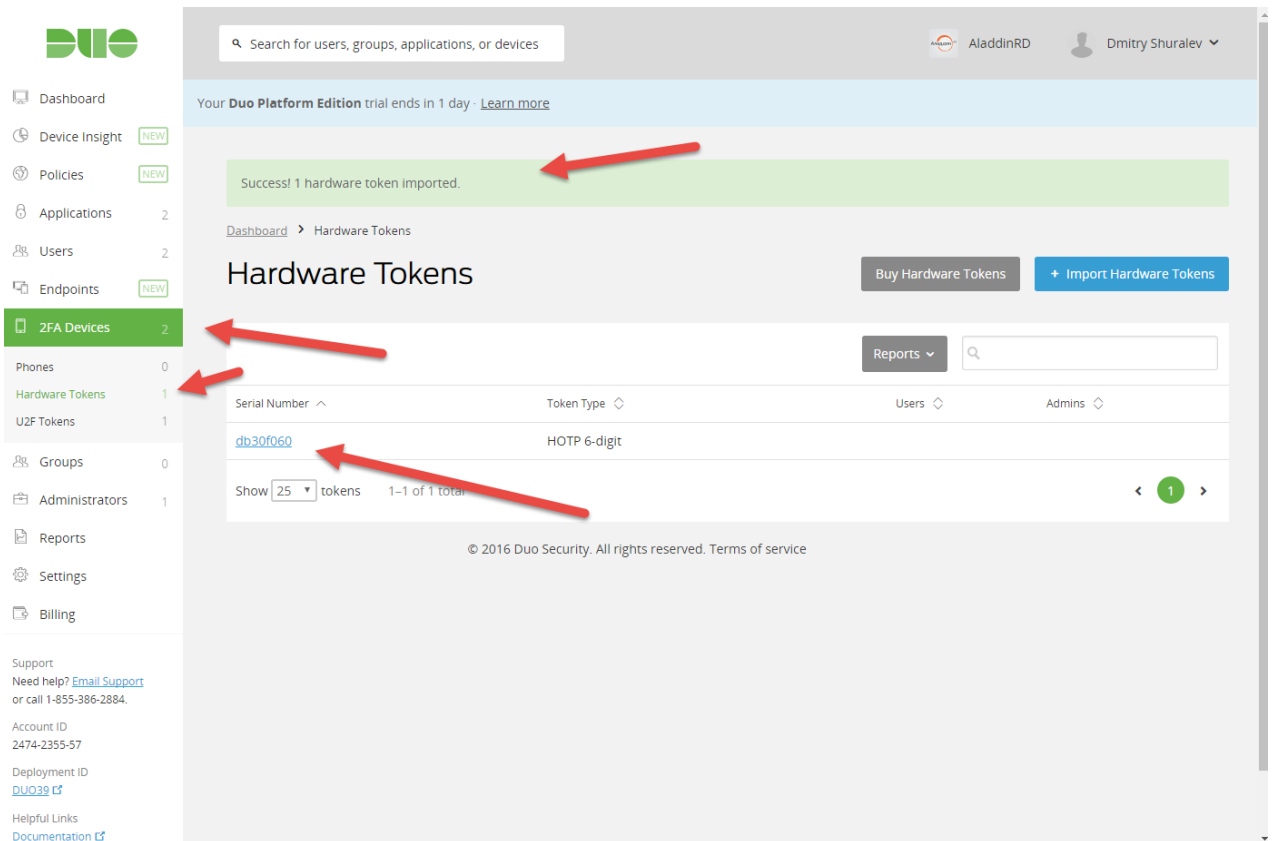
Эти данные необходимо взять из **.dat** файла из комплекта поставки ключей.

**Serial number** соответствует полю **sccAuthenticatorId**, а **secret key** соответствует полю **sccKey**.

```
dn: sccAuthenticatorId=87a1c7ac
objectclass: sccCompatibleToken
sccAuthenticatorId: 87a1c7ac
sccTokenType: JC-webPass
sccTokenData: s|sccKey=2a099b8b00d35c5c11b0ea529d365c8ec0ec3f68; sccMode=E; sccPwLen=6; sccVer=6.20;
```

Если необходимо импортировать множество ключей, по очереди 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.

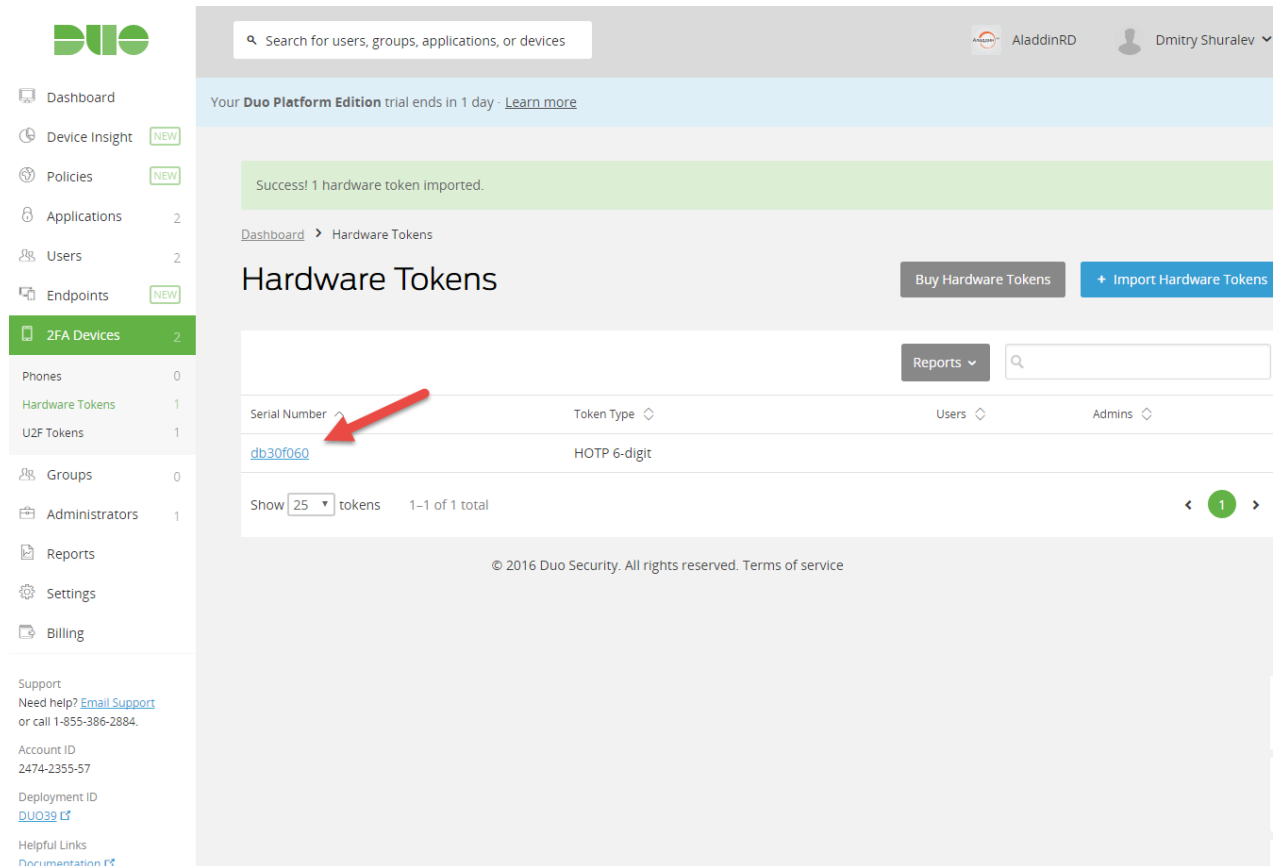
Если все введено верно отобразится сообщение **Success! 1 hardware token imported (Успех! Токен импортирован)**. Так же в списке появится его серийный номер и тип.



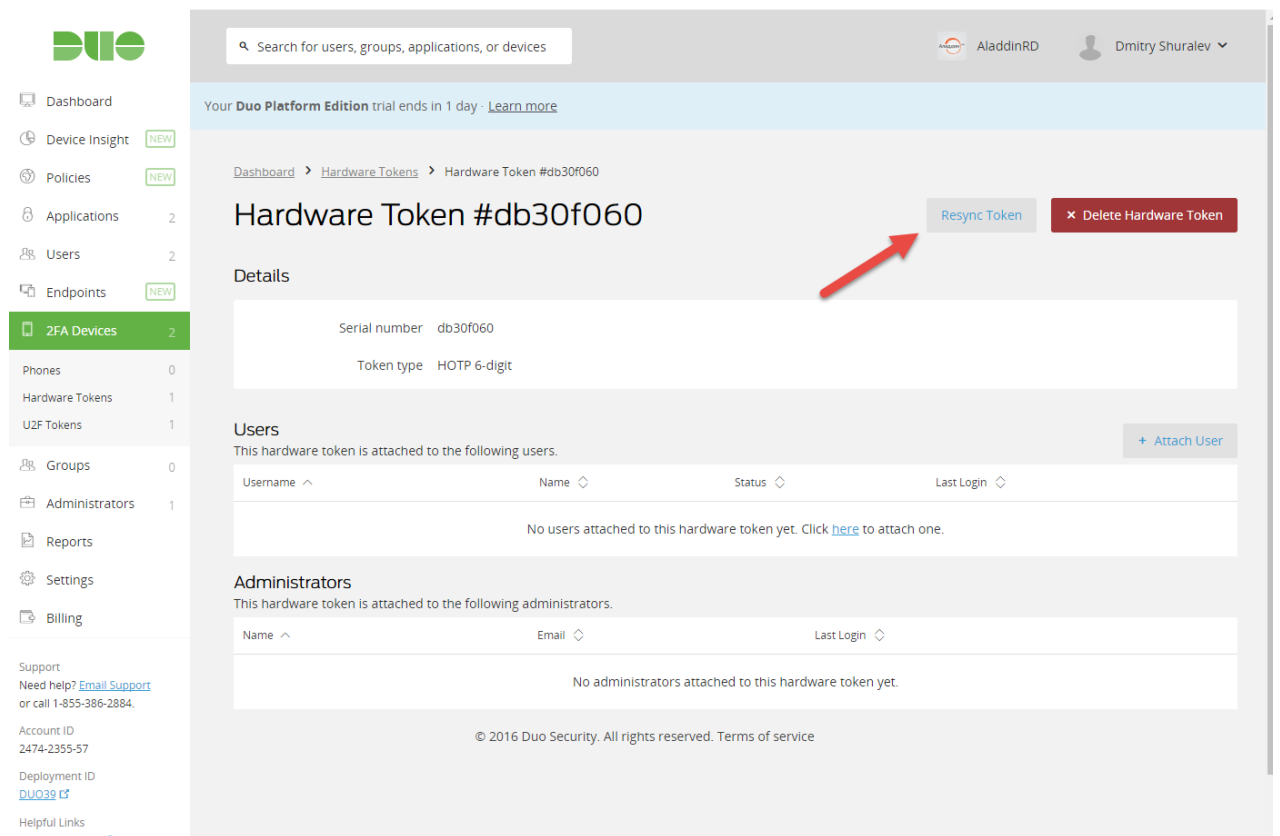
The screenshot displays the Duo Security management interface. At the top, a search bar and user profile (AladdinRD, Dmitry Shuralev) are visible. A notification banner at the top center reads "Success! 1 hardware token imported." with a red arrow pointing to it. Below this, the "Hardware Tokens" section is active, showing a table with one token. The table has columns for "Serial Number", "Token Type", "Users", and "Admins". The single token listed has a serial number of "db30f060" and is a "HOTP 6-digit" type. A red arrow points to the serial number. The left sidebar shows the navigation menu with "2FA Devices" selected, and a red arrow points to it. The "Hardware Tokens" sub-item in the sidebar also has a red arrow pointing to it. At the bottom of the table, it says "Show 25 tokens 1-1 of 1 total".

Serial Number	Token Type	Users	Admins
<a href="#">db30f060</a>	HOTP 6-digit		

Зайдите в свойства токена щелкнув по его серийному номеру.



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



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

Search for users, groups, applications, or devices

AladdinRD Dmitry Shuralev

Your Duo Platform Edition trial ends in 1 day - [Learn more](#)

Dashboard > Hardware Token #db30f060 > Resync

## Resync Token #db30f060

### Resync Hardware Token

Generate three passcodes in a row and enter them here to resync this hardware token.

1st code: 709945

2nd code: 047831

3rd code: 946859

[Resync Hardware Token](#)

© 2016 Duo Security. All rights reserved. Terms of service

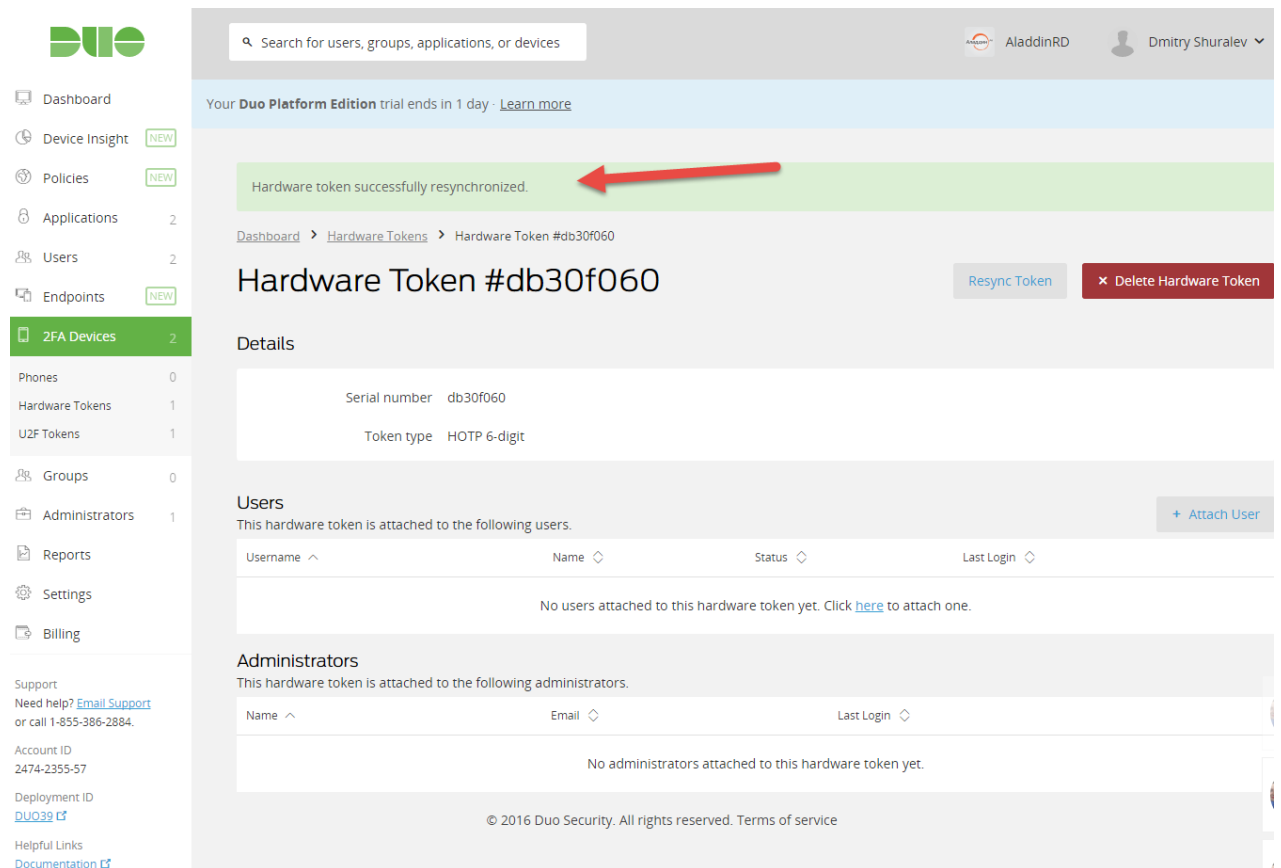
Support  
Need help? [Email Support](#)  
or call 1-855-386-2884.

Account ID  
2474-2355-57

Deployment ID  
[DUO39](#)

Helpful Links  
[Documentation](#)

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



The screenshot displays the Duo Security management interface. At the top, there is a search bar and user information for AladdinRD and Dmitry Shuralev. A notification banner at the top indicates that the Duo Platform Edition trial ends in 1 day. A prominent green message box states "Hardware token successfully resynchronized.", with a red arrow pointing to it. Below this, the page shows the details for a specific hardware token, #db30f060, including its serial number and token type (HOTP 6-digit). There are buttons for "Resync Token" and "Delete Hardware Token". The interface also shows sections for "Users" and "Administrators" attached to the token, both currently empty. The footer includes support information, account ID (2474-2355-57), deployment ID (DUO39), and copyright information for Duo Security.

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

The screenshot displays the Duo Security management interface. On the left is a sidebar with a navigation menu including Dashboard, Device Insight, Policies, Applications, Users, Endpoints, 2FA Devices (highlighted), Phones, Hardware Tokens, U2F Tokens, Groups, Administrators, Reports, Settings, and Billing. The main content area shows the configuration for a specific hardware token, #db30f060. It includes a search bar at the top, a trial notice, and breadcrumb navigation. The token details section shows the serial number (db30f060) and token type (HOTP 6-digit). Below the details are sections for 'Users' and 'Administrators', both indicating that no users or administrators are currently attached to this token. A red arrow points to the '+ Attach User' button in the Users section. The footer contains support information and a copyright notice for Duo Security.

Выберите необходимого пользователя в отобразившемся списке.

The screenshot shows the Duo Security management interface. On the left is a navigation sidebar with categories like Dashboard, Device Insight, Policies, Applications, Users, Endpoints, 2FA Devices, Groups, Administrators, Reports, Settings, and Billing. The main content area displays the configuration for a specific hardware token, #db30f060. It includes a success message, breadcrumb navigation, and buttons for 'Resync Token' and 'Delete Hardware Token'. The 'Details' section shows the serial number and token type. The 'Users' section lists users attached to the token, with a table containing columns for Username, Name, Status, and Last Login. A red arrow points to the user 'dd' in this list. Below the users list is an 'Administrators' section which is currently empty.

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

The screenshot shows a web login page with a blue 'W' logo at the top. Below the logo is a message box that says 'Вы вышли из системы.'. The main form contains two input fields: 'Имя пользователя или e-mail' with the value 'DD' and 'Пароль' with masked characters. There is a checkbox for 'Запомнить меня' and a blue 'Войти' button. At the bottom, there is a link for 'Забыли пароль?' and a link to 'Назад к сайту «DD»'.

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

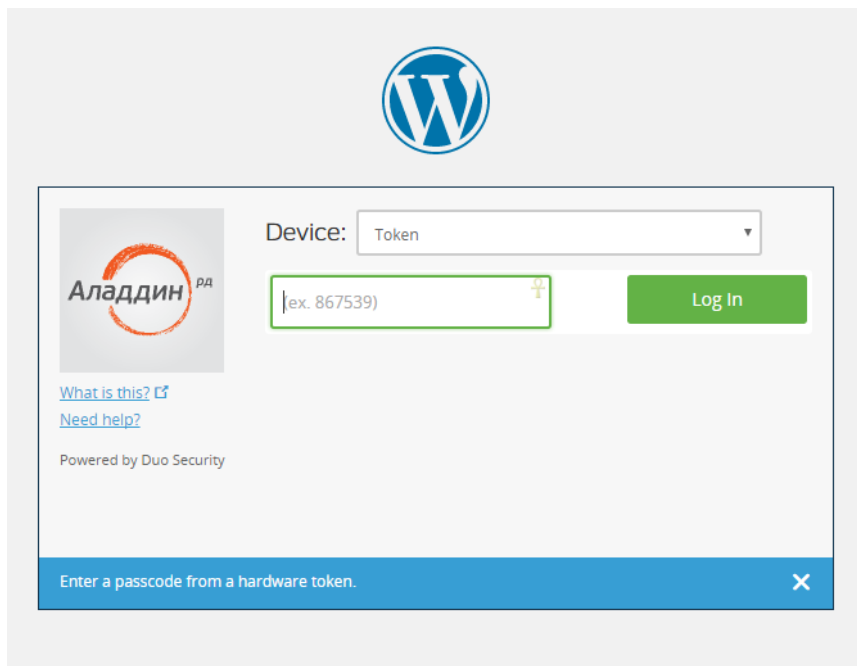
Нажмите **Enter a Passcode**.





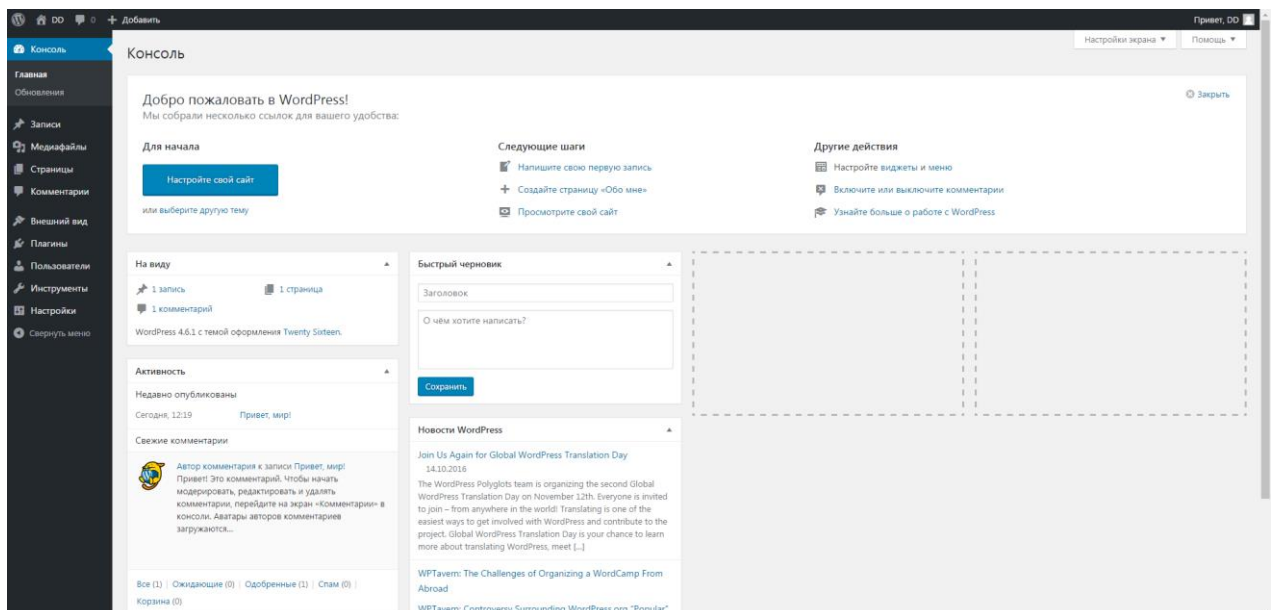
Нажмите кнопку на токене, OTP-значении подставится в поле автоматически.

Нажмите **Log In**.



The image shows the WordPress login interface. At the top center is the WordPress logo. Below it, a white box contains the login form. On the left of this box is the JaCarta logo, which includes the text "Аладдин" and "P.A.". To the right of the logo, there is a "Device:" dropdown menu set to "Token". Below this is a text input field containing "[ex. 867539]" and a green "Log In" button. Underneath the input field are two links: "What is this?" and "Need help?". At the bottom left of the white box, it says "Powered by Duo Security". A blue banner at the bottom of the white box contains the text "Enter a passcode from a hardware token." with a close button (X) on the right.

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



The image shows the WordPress admin dashboard. At the top, there is a navigation bar with "Консоль" (Dashboard) selected. Below the navigation bar, the main content area is titled "Консоль" and contains a welcome message: "Добро пожаловать в WordPress! Мы собрали несколько ссылок для вашего удобства:". There are three main sections: "Для начала" (Getting started) with a "Настройте свой сайт" button; "Следующие шаги" (Next steps) with links to "Напишите свою первую запись", "Создайте страницу «Обо мне»", and "Просмотрите свой сайт"; and "Другие действия" (Other actions) with links to "Настройте виджеты и меню", "Включите или выключите комментарии", and "Узнайте больше о работе с WordPress". Below these are several widgets: "На виду" (At a glance) showing 1 post and 1 page; "Быстрый черновик" (Quick draft) with a "Сохранить" button; "Активность" (Activity) showing a recent post "Привет, мир!" and a comment; "Новости WordPress" (WordPress news) with several articles; and a bottom navigation bar with "Все (1)", "Ожидющие (0)", "Одобренные (1)", "Спам (0)", and "Корзина (0)".

## Защита других приложений и протоколов

---

По аналогии можно подключить токены JaCarta WebPass и JaCartaU2F и к другим приложениям или протоколами которые 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](mailto:aladdin@aladdin-rd.ru) (общий).

Web: [www.aladdin-rd.ru](http://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](http://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

© ЗАО «Аладдин Р. Д.», 1995–2017. Все права защищены.

Тел. +7 (495) 223-00-01 Email: [aladdin@aladdin-rd.ru](mailto:aladdin@aladdin-rd.ru) Web: [www.aladdin-rd.ru](http://www.aladdin-rd.ru)