

FEITIAN U2F scenarios instructions

Contents

1. Introduction	2
2. Windows platform service	2
2.1. Google	2
2.2. Facebook	7
2.3. Twitter	11
2.4. Dropbox	16
2.5. GitHub	20
2.6. GitLab	23
2.7. Salesforce	26
2.8. Bitbucket	30
2.9. Dashlane	33
2.10. DUO	36
2.11. Digidentity	39
2.12. BITFINEX	41
2.13. FastMail	43
2.14. Gandi.net	45
2.15. Keeper	47
2.16. Sentry	50
2.17. Okta	53
3. Mobile based scenarios	57
3.1. IOS platform	57
3.1.1. Google account	57

1. Introduction

This document provides a guide for end-users to enable Two-Factor Authentication, for specific online services, platforms and applications, using FEITIAN ePass FIDO.

2. Windows platform service

This chapter introduces a guide for end users about using FEITIAN ePass FIDO as a second authentication factor on Windows platform, including online services and Windows apps.

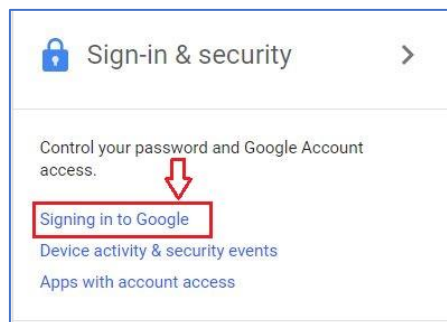
2.1. Google

Login Google account and enable 2-step verification.

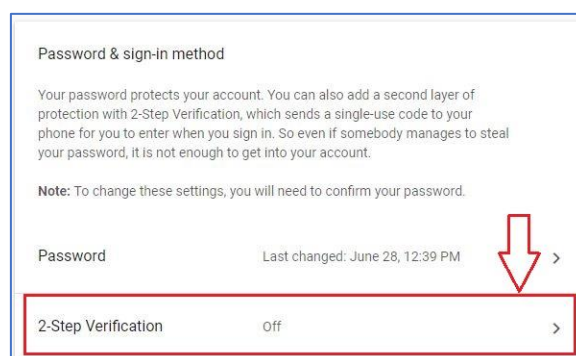
Click **Google Account** and go to **Settings**.




In 'Sign-in & security' tab, click **Signing in to Google**.



Now you can click **2-Step Verification** to enable it.





Follow the given instructions.





Protect your account with 2-Step Verification

Each time you sign in to your Google Account, you'll need your password and a verification code.
[Learn more](#)

**Add an extra layer of security**
Enter your password and a unique verification code that's sent to your phone.

**Keep the bad guys out**
Even if someone else gets your password, it won't be enough to sign in to your account.

**GET STARTED**





Hi Nick


To continue, first verify it's you

Enter your password

[Forgot password?](#)


**Input your password and click NEXT**


**NEXT**



Let's set up your phone

What phone number do you want to use?

 +86


**Select your country and input phone number, then click NEXT**


Google will only use this number for account security.
Don't use a Google Voice number.
Message and data rates may apply.

How do you want to get codes?

☒ Text message ☐ Phone call

Step 1 of 3

**NEXT**



Confirm that it works

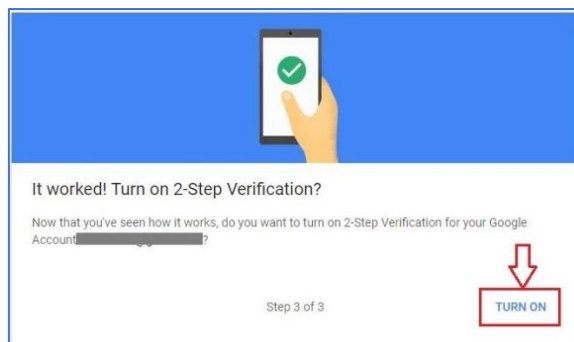
Google just sent a text message with a verification code to [REDACTED]

Enter the code

Enter the code you received and click NEXT

Didn't get it? Resend

BACK Step 2 of 3 NEXT



It worked! Turn on 2-Step Verification?

Now that you've seen how it works, do you want to turn on 2-Step Verification for your Google Account [REDACTED]?

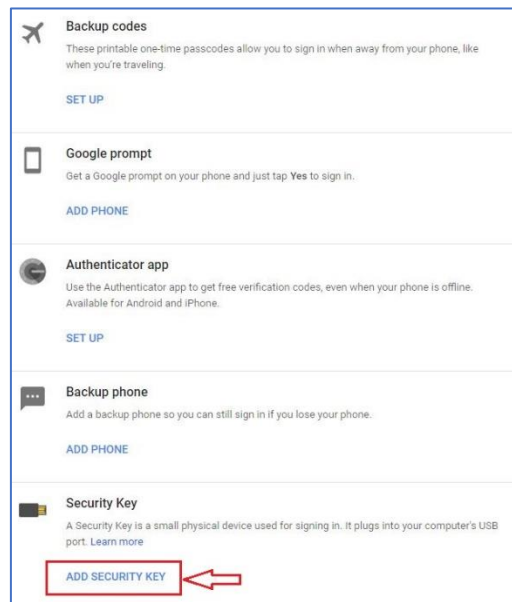
Step 3 of 3

TURN ON

You have successfully enabled 2-step verification after all above completed.

Register FEITIAN ePass FIDO.

Add ePass FIDO as security key for your account.



Backup codes

These printable one-time passcodes allow you to sign in when away from your phone, like when you're traveling.

SET UP

Google prompt

Get a Google prompt on your phone and just tap **Yes** to sign in.

ADD PHONE

Authenticator app

Use the Authenticator app to get free verification codes, even when your phone is offline. Available for Android and iPhone.

SET UP

Backup phone

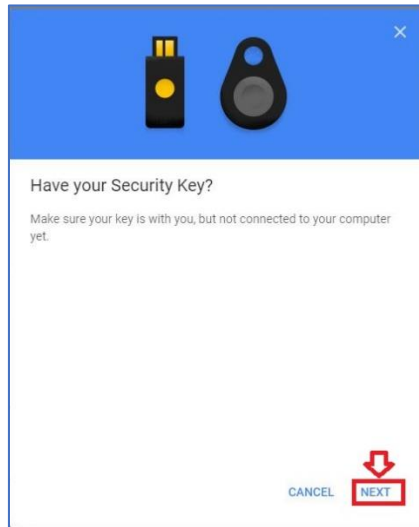
Add a backup phone so you can still sign in if you lose your phone.

ADD PHONE

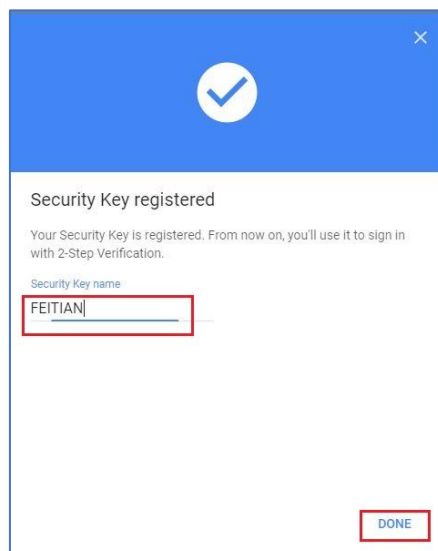
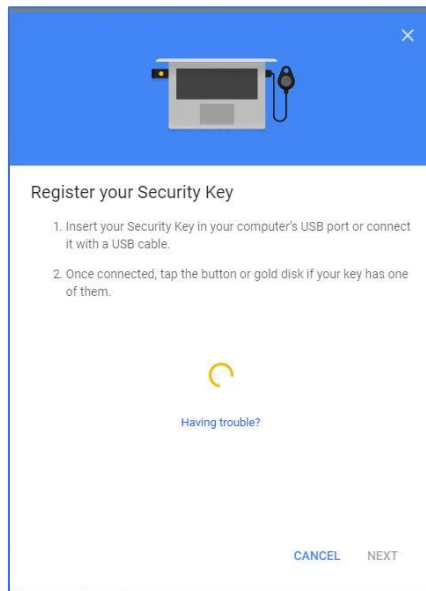
Security Key

A Security Key is a small physical device used for signing in. It plugs into your computer's USB port. [Learn more](#)

ADD SECURITY KEY



Insert ePass FIDO device and name it.

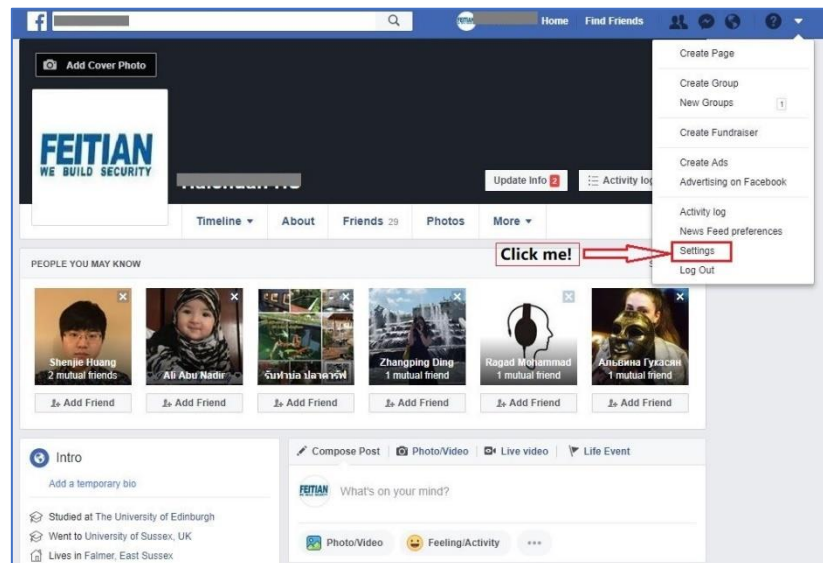


Now your ePass FIDO security key has been added successfully, and you can sign out and re-sign in to try out.

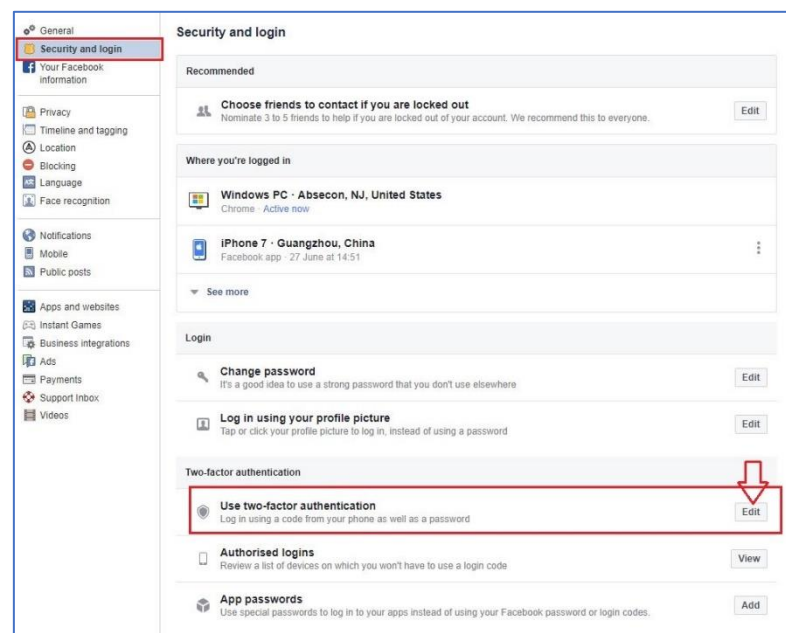
You may have more information about Google 2-step verification by click [here](#).

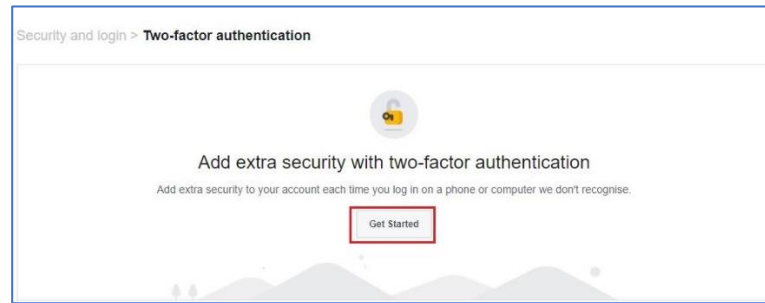
2.2. Facebook

By registering your ePass FIDO device, you need to login your Facebook account and go to **Settings**.

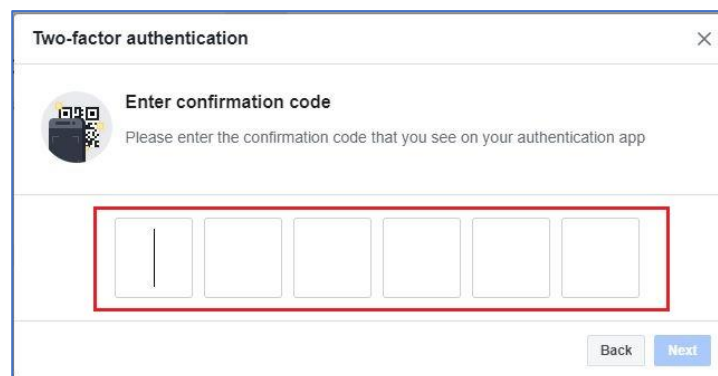
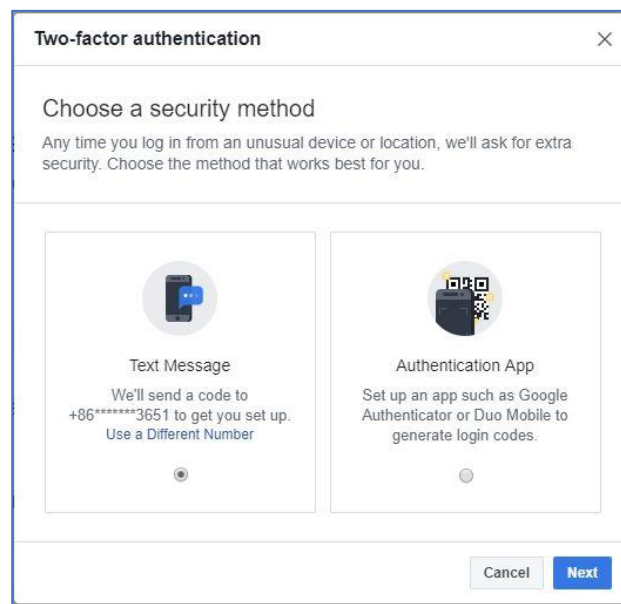


Under **Security and Login** tab, Click the highlighted **Edit** button and follow the instructions to turn on Two-factor authentication.

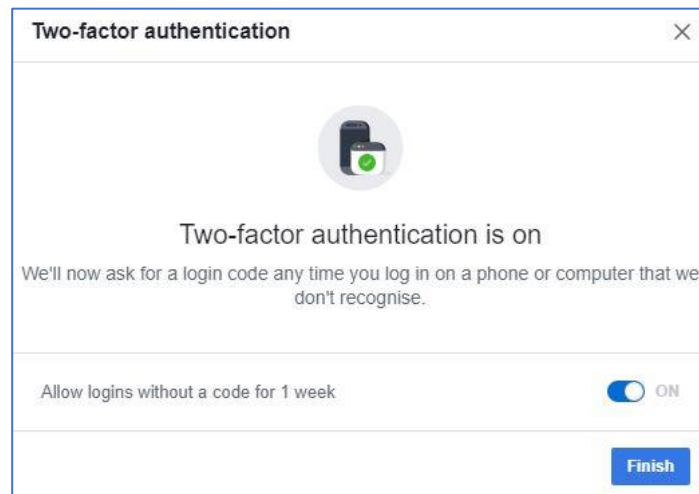




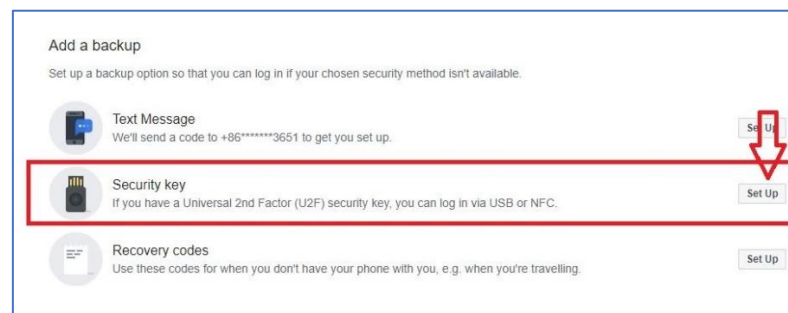
Choose a security method to verify your account and input confirmation code.



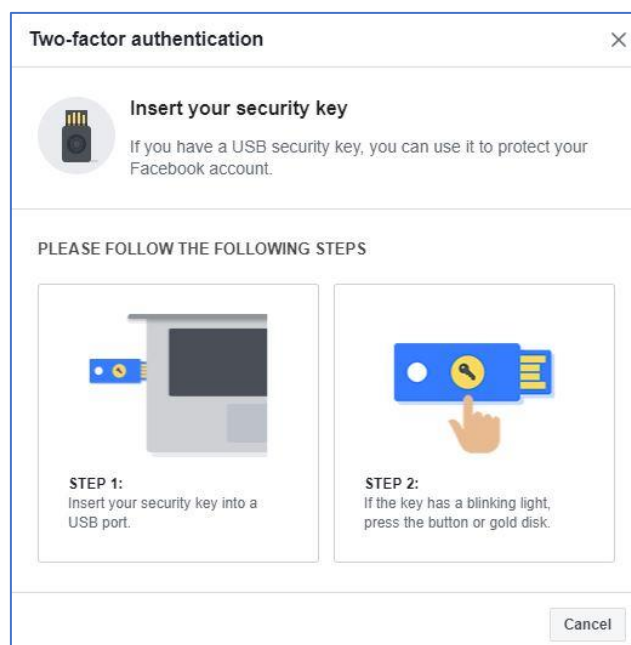
Once you have a pop-up windows like below, you have successfully enabled Two-factor authentication.




Set up a security key.




Follow instructions to insert your FEITIAN ePass FIDO security key and touch the gold disk. And then you will have an added key listed. You may name it.



Two-factor authentication



Via security key
You can choose a key you've already registered or add a new key.



Security key successfully added.

REGISTERED KEYS

FEITIAN security key
Last used 4 July 2018

Edit

Delete

Add new security key

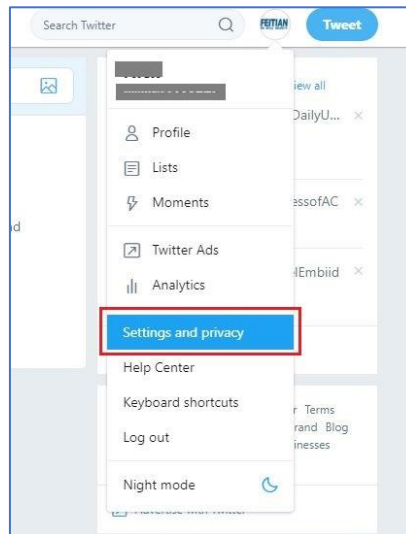
>

Back

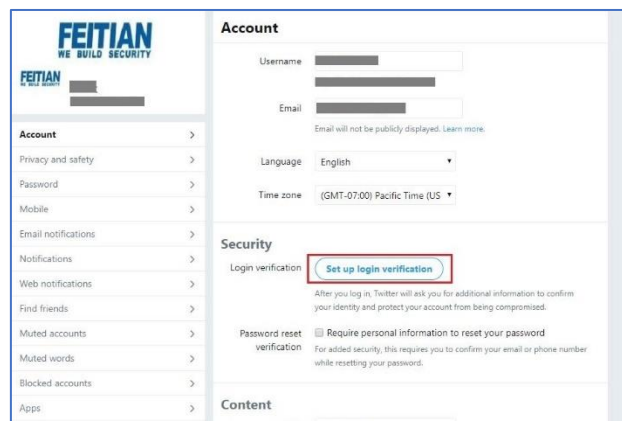
When you finish registration, you can now re-login your account to try out the two-factor authentication

2.3. Twitter

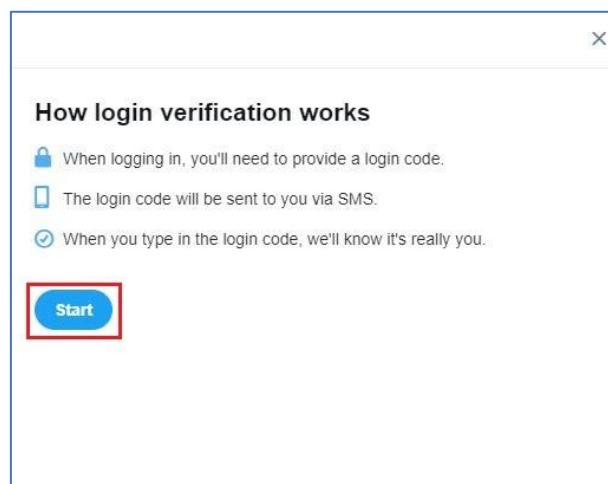
Log in your Twitter account and go to **Settings and privacy** tab.



Follow the instructions to click **Set up login verification**.

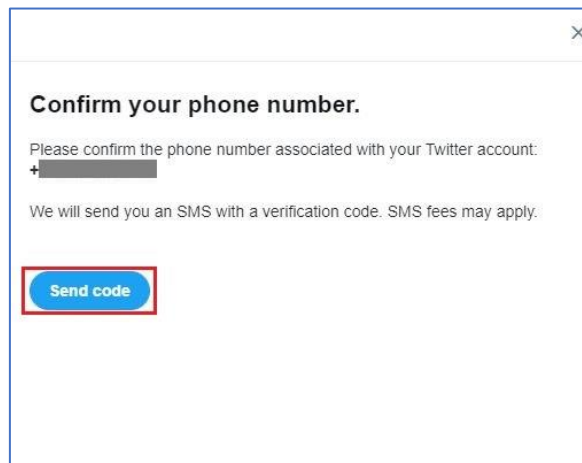


Read the overview instructions, then click **Start**.



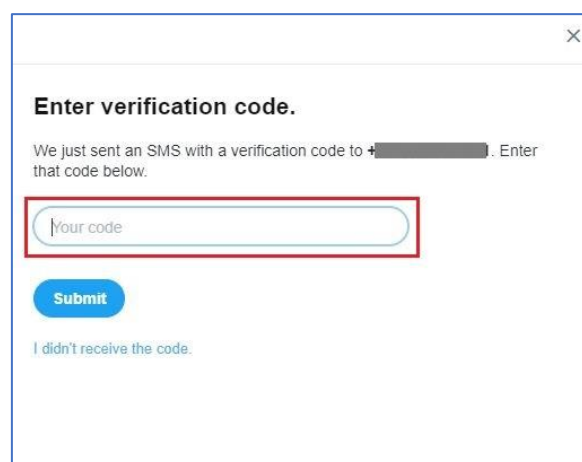
Click **Send code** to add your phone number.

Note: If you already have a phone number associated with your Twitter account, we will send you an SMS to confirm your number.



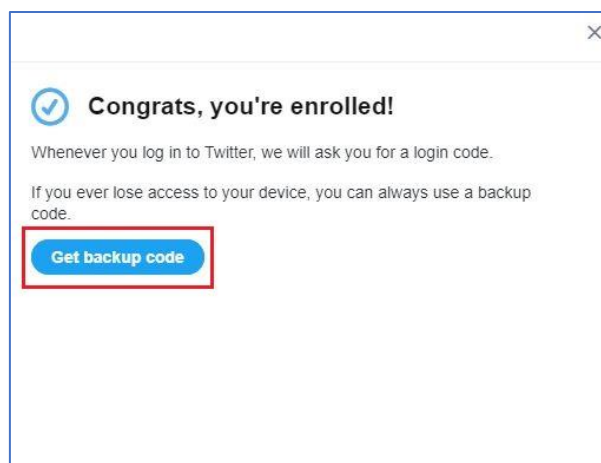
A dialog box titled "Confirm your phone number." with a close button (X) in the top right corner. The text inside reads: "Please confirm the phone number associated with your Twitter account: +[redacted]". Below this, it says: "We will send you an SMS with a verification code. SMS fees may apply." At the bottom, there is a blue button labeled "Send code" which is highlighted with a red rectangular border.

Enter the verification code sent to your device, then click **Submit**.



A dialog box titled "Enter verification code." with a close button (X) in the top right corner. The text inside reads: "We just sent an SMS with a verification code to +[redacted]. Enter that code below." Below the text is a text input field with the placeholder text "Your code" and a cursor, which is highlighted with a red rectangular border. Below the input field is a blue button labeled "Submit". At the bottom, there is a link that says "I didn't receive the code."

Click **Get Backup Code** to view a code, generated by Twitter. We recommend you store a screenshot of the code in case you need it for future use. This will help you access your account if you lose your mobile phone or change your phone number.



A dialog box titled "Congrats, you're enrolled!" with a checkmark icon in a blue circle to the left of the title. Below the title, the text reads: "Whenever you log in to Twitter, we will ask you for a login code." and "If you ever lose access to your device, you can always use a backup code." At the bottom, there is a blue button labeled "Get backup code" which is highlighted with a red rectangular border.

Backup code for [redacted]

Store this backup code somewhere safe - print it, write it down, or save a screenshot.

If you ever lose access to your device, you can use this code to verify your identity. This code can only be used once. [Learn more](#)

[Redacted Backup Code]

[Generate a new code](#)

[Print this code](#) [Done](#)

By adding a FEITIAN ePass FIDO, click **Review your login verification methods**.

Security

Login verification [Review your login verification methods](#)

After you log in, Twitter will ask you for additional information to confirm your identity and protect your account from being compromised.

Password reset verification ☐ Require personal information to reset your password

For added security, this requires you to confirm your email or phone number while resetting your password.

Enter your password and click **Confirm** to continue.

Edit your login verification methods

Confirm password

This page contains personal information. Confirm your password to continue.

[Forgot your password?](#)

[Confirm](#)

From the selections, click Set up next to **Security key**.

← Account

Login verification

After you login, Twitter will ask you for additional verification to protect your account against possible compromise.

This will enable or disable all of the settings on this page. [Turn off](#)

Text message [Edit](#)
Twitter will send a text to your mobile phone with a six-digit login code to enter.

Security key [Set up](#)
You can use a physical electronic key to approve login attempts.

Mobile security app [Set up](#)
You can use a separate app to generate your verification codes.



Backup code [Get backup code](#)
Save a backup code in case you lose your device.

Temporary password [Generate app password](#)
Generate a one-time password to use when logging in to third party apps and services.

Read the instructions and then click **Start**.

✕

Security key

You can use a USB security key to securely log in to Twitter.

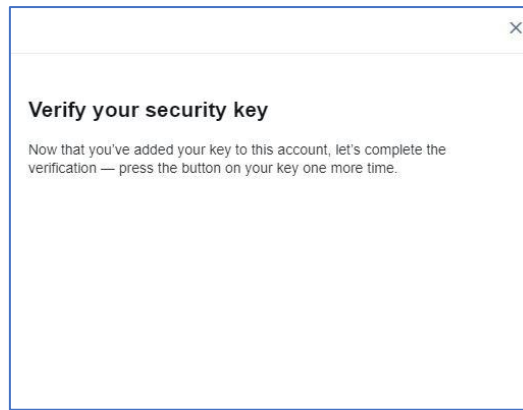
Start

If you're asked to verify your password, enter it and click Verify. Then you will see a pop-up window asking you to register your key by inserting it into your computer's USB port. Once inserted, press the button located on your key. Then verify the key by pressing the button one more time.

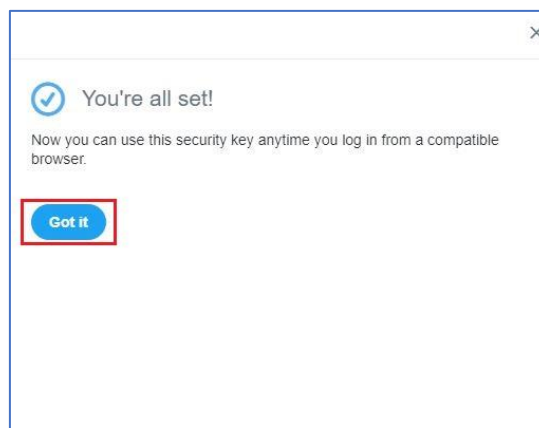
✕

Add your security key

Insert your key into your USB port, and then press the button on your key.

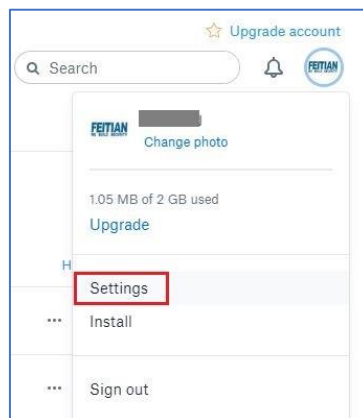


Congratulations! You are ready to use FEITIAN ePass FIDO to authenticate your twitter account.

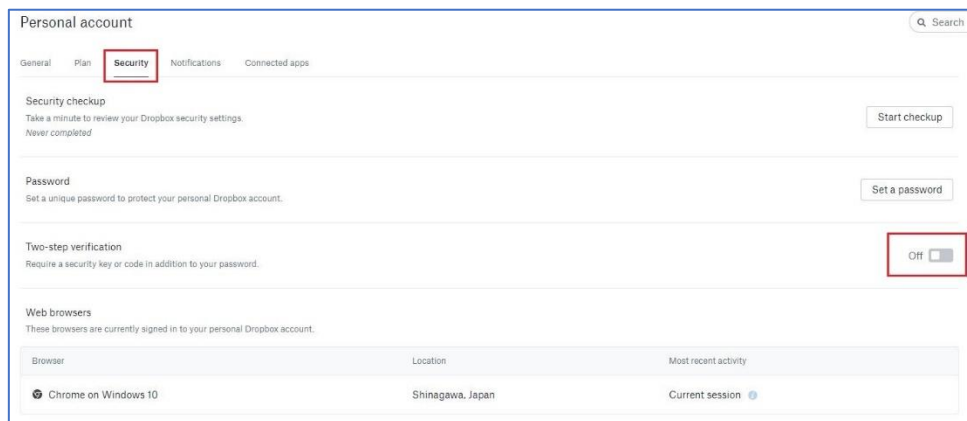


2.4. Dropbox

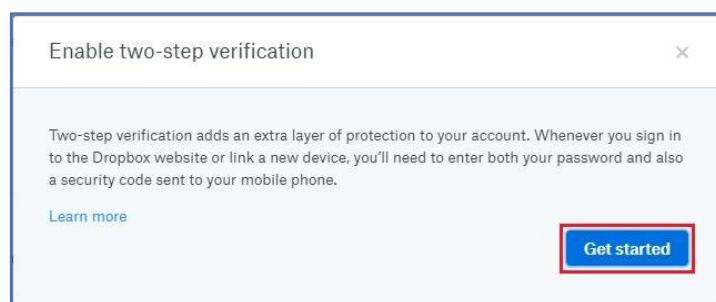
Sign in your Dropbox and go to **Settings** tab.



Under **security** tab, click highlighted **Off** to enable Two-step verification.



Follow the instructions.



Enable two-step verification

For security, please enter your password for [redacted]

Enter your password and click Next

Next

Enable two-step verification

How would you like to receive your security codes?

☒ Use text messages
Security codes will be sent to your mobile phone

☐ Use a mobile app
Security codes will be generated by an authenticator app

Next

Enable two-step verification

Enter the security code generated by your mobile authenticator app to make sure it's configured correctly.

597073

Next Back

Input a backup phone number. **Note**, this is optional.

Enable two-step verification

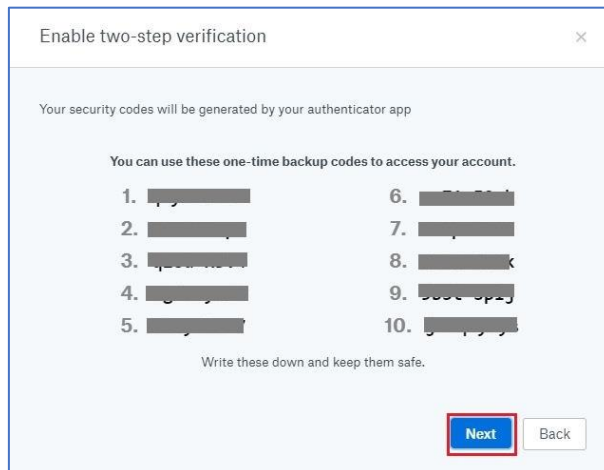
Backup phone number (optional)
If you lose access to your primary security code source, we can send them to your backup mobile number instead.

China +86 31 2345 6789

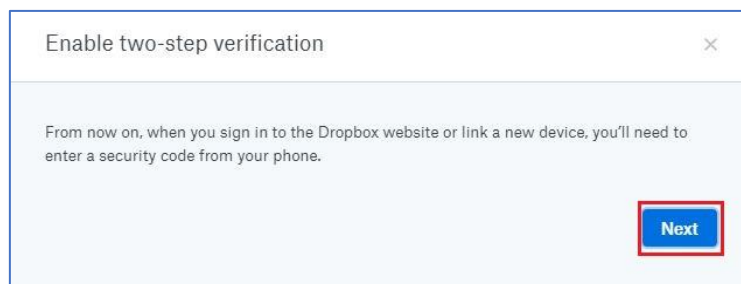
While this step is optional, we encourage you to set up a backup phone number in case you lose your mobile phone or are otherwise unable to receive your security code.

Next Back

Carefully save the one-time backup codes and click **Next**.

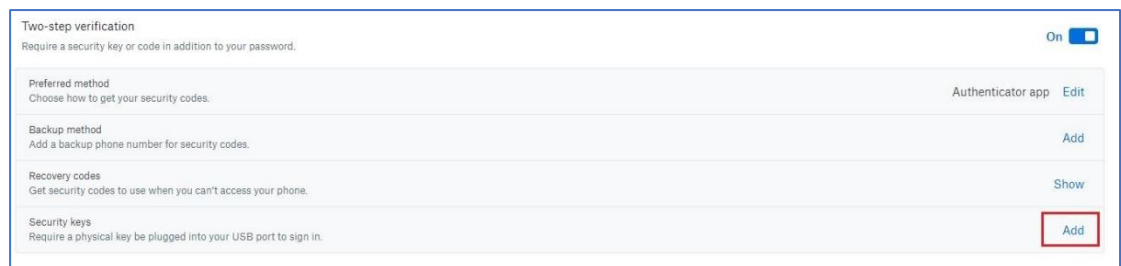


Read the lines and click **Next** and you have successfully enabled the two-step verification.

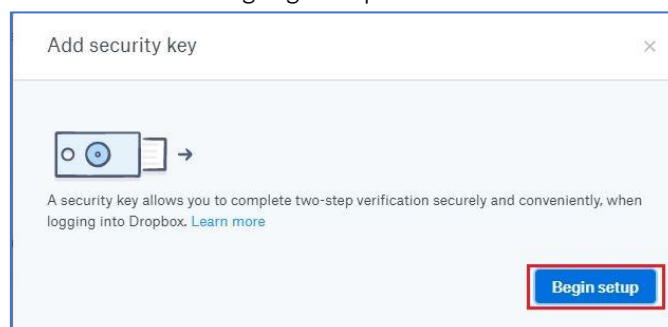


Register your FEITIAN ePassFIDO.

Click **Add** next to **Security keys** under **Two-step verification** tab.



Follow instructions indicated as highlighted part.



Enter your password and click **Next**.

Add security key

For security, please enter your password for [redacted]

Enter your password and click Next

Next

Insert your FEITIAN ePass FIDO and press it.

Add security key

Start by inserting your security key into a USB port. [Learn more](#)

Key inserted

Add security key

Scanning for security key

If your key has a button or a gold disk, tap it now. [Learn more](#)

Click **Allow** on the pop-up window.

www.dropbox.com wants to

See the make and model of your Security Key

Allow Block

Finally, you have added a security key to your account.

Add security key

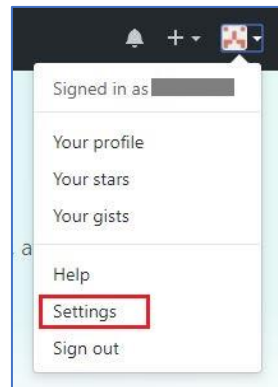
Key added!

You can now use your security key to complete two-step verification when you sign into Dropbox.

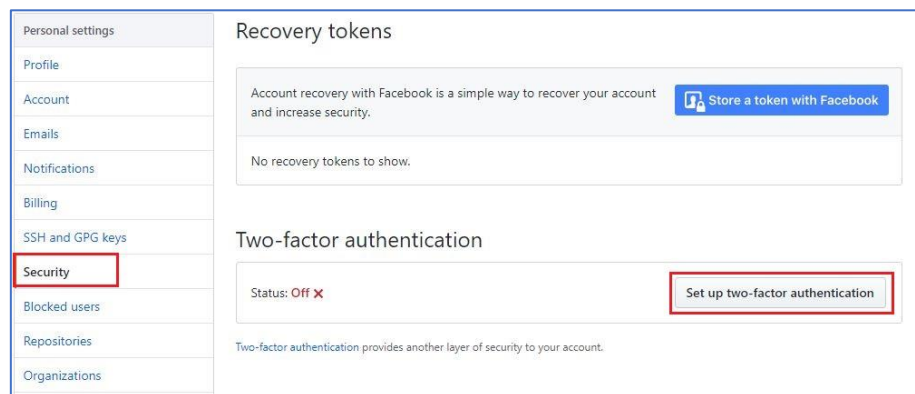
Finish

2.5. GitHub

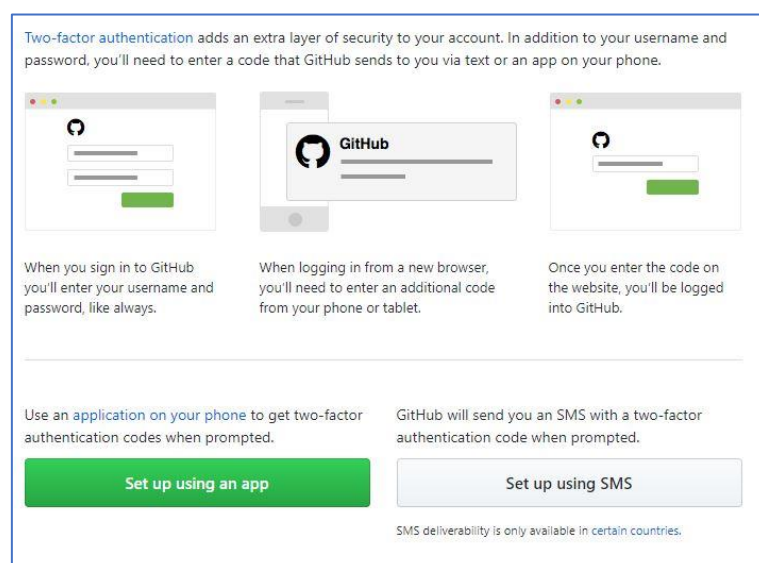
Log in your GitHub account and go to **Settings**.



Under **Security** tab, click **Set up two-factor authentication** to enable the feature.



Two ways to get the verification code provided by GitHub. Here we use an app as example.



Carefully save the recovery codes and click **Next**.

1. Recovery codes

Recovery codes are used to access your account in the event you cannot receive two-factor authentication codes.

Download, print, or copy your recovery codes before continuing two-factor authentication setup below.

Download

Print

Copy

Treat your recovery codes with the same level of attention as you would your password! We recommend saving them with a password manager such as Lastpass, 1Password, or Keeper.


Next

Cancel

Use your app to scan the QR code and fetch a six-digit code. Input it and click **Enable**.

2. Scan this barcode with your app.

Scan the image above with the two-factor authentication app on your phone. If you can't use a barcode, enter this text code instead.



Enter the six-digit code from the application

After scanning the barcode image, the app will display a six-digit code that you can enter below.

123456

Enable

Cancel

Register a FEITIAN ePass FIDO by clicking the highlighted button in **Security keys** tab.

Enabled ✓

Two-factor authentication is currently on

Disable two-factor authentication

Recover accounts elsewhere

GitHub can store a recovery token with another provider. This can be used to help verify your identity if you get locked out of your account.

Recover your GitHub account with:

<https://www.facebook.com>

Recovery codes

Recovery codes can be used to access your account in the event you lose access to your device and cannot receive two-factor authentication codes.

GitHub Support cannot restore access to accounts with two-factor authentication enabled for security reasons, **saving your recovery codes in a safe place can help keep you from being locked out of your account.**

[View recovery codes](#)

Fallback SMS number

Providing a fallback SMS number will allow GitHub to send your two-factor authentication codes to an alternate device if you lose your primary device.

For security reasons, GitHub Support cannot restore access to accounts with two-factor authentication enabled. If you lose access to both your primary device and your recovery keys, a backup SMS number can get you back in to your account.

[Add fallback SMS number](#)

Delivery options

Your primary delivery method is: **authenticator application.**

[Reconfigure two-factor authentication](#)

Security keys

Security keys are hardware devices that can be used as your second factor of authentication. When signing in, you press a button on the device rather than typing a verification code. Security keys use the FIDO U2F standard.

Register new device


Insert the FEITIAN security key and press it and then you have successfully added a device.

Security keys

Security keys are hardware devices that can be used as your second factor of authentication. When signing in, you press a button on the device rather than typing a verification code. Security keys use the FIDO U2F standard.

FEITIAN

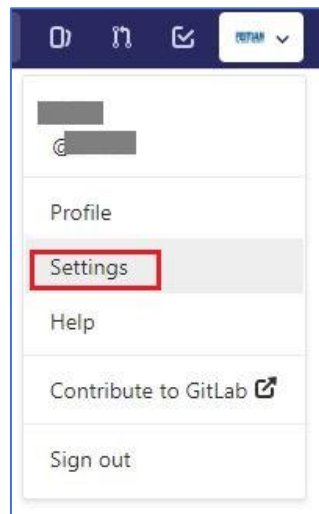
Add



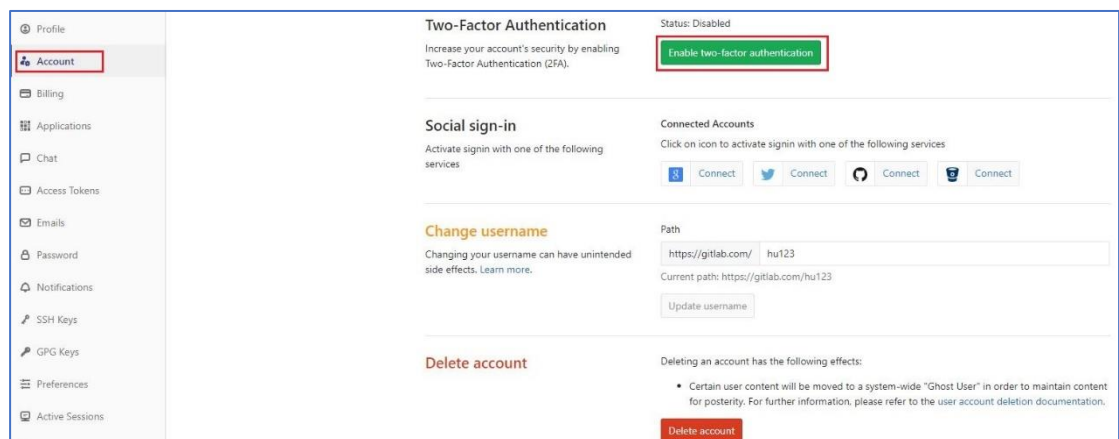
Waiting for device
Press the button on your security key device to register it with GitHub.

2.6. GitLab

Sign in GitLab account and go to **Settings**.



Under **Account** tab, click **Enable two-factor authentication**.




Use Google Authenticator to fetch a pin code and click **Register with two-factor app**.

User Settings > Two-Factor Authentication > Account

Register Two-Factor Authentication App

Use an app on your mobile device to enable two-factor authentication (2FA).

Download the Google Authenticator application from App Store or Google Play Store and scan this code. More information is available in the documentation.



Can't scan the code?
To add the entry manually, provide the following details to the application on your phone.
Account: gitlab.com:nick@itsafe.com
Key: s2vu wlfm thds ozaj 3xnl jykd vej7 msry
Time based: Yes

Pin code

[Register with two-factor app](#)

Register Universal Two-Factor (U2F) Device

Use a hardware device to add the second factor of authentication.

As U2F devices are only supported by a few browsers, we require that you set up a two-factor authentication app before a U2F device. That way you'll always be able to log in - even when you're using an unsupported browser.

[Setup new U2F device](#)

You need to register a two-factor authentication app before you can set up a U2F device.

U2F Devices (0)

You don't have any U2F devices registered yet.

Carefully save recovery codes and click **Proceed** to enable the two-factor authentication.

Congratulations! You have enabled Two-factor Authentication!

Should you ever lose your phone, each of these recovery codes can be used one time each to regain access to your account. Please save them in a safe place, or you **will** lose access to your account.

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[Proceed](#)

Click **Manage two-factor authentication** to register a FEITIAN ePass FIDO.

Two-Factor Authentication Status: Enabled

Increase your account's security by enabling Two-Factor Authentication (2FA).

[Manage two-factor authentication](#)

Click **Setup new U2F device** to add the security key.

Register Two-Factor Authentication App

Use an app on your mobile device to enable two-factor authentication (2FA).

You've already enabled two-factor authentication using mobile authenticator applications. In order to register a different device, you must first disable two-factor authentication.

[Disable two-factor authentication](#)

Register Universal Two-Factor (U2F) Device

Use a hardware device to add the second factor of authentication.

As U2F devices are only supported by a few browsers, we require that you set up a two-factor authentication app before a U2F device. That way you'll always be able to log in - even

[Setup new U2F device](#)

Your U2F device needs to be set up. Plug it in (if not already) and click the button on the left.

U2F Devices (0)

You don't have any U2F devices registered yet.

After naming your security key, click **Register U2F device** to finish the registration.

Register Universal Two-Factor (U2F) Device

Use a hardware device to add the second factor of authentication.

Your device was successfully set up! Give it a name and register it with the GitLab server.

Register U2F device

2.7. Salesforce

Log in your account and go to **My Domain** tab, click **Deploy to Users**.

Step 3 Domain Ready for Testing

Choose Domain Name → Domain Registration Pending → Domain Ready for Testing → Domain Deployed to Users

Test domain URL Then deploy to users

Your domain name is nickhnc.my.salesforce.com

Your domain name is ready. Log in to test it out. [Log in](#)

To test your new domain, click tabs and links. If you've customized the UI, check for hard links to your original URL.

[Deploy to Users](#) Roll out the new domain to your org. [?](#)

Tick **Let users use a security key** in **Identity Verification** tab.

Quick Find / Search... [Expand All](#) [Collapse All](#)

Salesforce Mobile Quick Start

Home

Administer

- Manage Users
- Manage Apps
- Company Profile
- Security Controls
- Identity Verification**
- Health Check
- Sharing Settings
- Field Accessibility
- Password Policies
- Session Settings
- Login Flows
- Network Access
- Activations
- Session Management
- Login Access Policies
- Certificate and Key Management
- Single Sign-On Settings
- Auth. Providers
- Identity Provider
- View Setup Audit Trail
- Expire All Passwords
- Remote Site Settings

SETUP Identity Verification

Control how and when your users are prompted to verify their identity.

- ☐ Enable the SMS method of identity verification
- ☒ Require security tokens for API logins from callouts (API version 31.0 and earlier)
- ☒ **Let users use a security key (U2F)**
- ☒ Require identity verification during two-factor authentication registration
- ☐ Require identity verification for change of email address
- ☒ Allow location-based automated verifications with Salesforce Authenticator
- ☐ Allow only from trusted IP addresses

Session Security Level Policies

Require a high assurance level of security for sensitive operations, or block users altogether. If users already have a high assurance session after logging in, they aren't prompted to verify their identity again in the same session, even if you require high assurance for these operations. If you want to see the session levels that users are granted at login, see Session Security Levels in Session Settings.

These settings only apply to users who have user permissions assigned to access these operations.

Reports and Dashboards: [?](#) None

Manage Auth. Providers: [?](#) None

Manage Login Access Policies: [?](#) None

Manage IP Addresses: [?](#) None

Manage Password Policies: [?](#) None

[Save](#)

Enable two-factor authentication for users.

Find **Permission Sets** tab and click **New** button to create a new group.

Setup Home

ADMINISTRATION

- Users
- Permission Sets**
- Profiles
- Public Groups
- Queues
- Roles
- User Management Settings
- Users
- Data

SETUP Permission Sets

Permission Sets

On this page you can create, view, and manage permission sets.

In addition, you can use the SalesforceA mobile app to assign permission sets to a user. Download SalesforceA from the App Store or Google Play: [iOS](#) | [Android](#)

[Run](#) [Edit](#) [Delete](#) [Create New View](#)

[New](#) [?](#)

Action	Permission Set Label	Description
Clone	Sales Cloud User	Denotes that the user is a Sales Cloud user.
Del Clone	Sales User	
Clone	Salesforce Console User	Enable Salesforce Console User
Clone	Standard Einstein Activity Capture	Access to Standard Einstein Activity Capture

Name it and choose license for it.

Save Cancel

Enter permission set information

Label **2FA-FEITIAN**

API Name **X2FA_FEITIAN** ⓘ

Description

Session Activation Required ⓘ

Select the type of users who will use this permission set

Who will use this permission set?

- Choose "--None--" if you plan to assign this permission set to multiple users with different user and permission set licenses.
- Choose a specific user license if you want users with only one license type to use this permission set.
- Choose a specific permission set license if you want this permission set license auto-assigned with the permission set.

Not sure what a permission set license is? [Learn more here.](#)

License **Salesforce** ▼

Save Cancel

In the next stage, search 'two factor authentication' and locate it. Click **Edit** and scroll down to find and tick it. Scroll up to save the configuration.

Permission Set: **2FA-FEITIAN** Video Tutorial | Help

Search **two factor authentication**

Q | Clone Delete Edit Properties Manage Assignments

Permission Set Overview > System Permissions ▼

System Permissions **Edit**

Permission Name	Enabled	Description
Access Libraries	<input type="checkbox"/>	Access libraries.
Add People to Direct Messages	<input type="checkbox"/>	Lets a user add others to direct messages the user is in.
Allow Access to Customized Actions	<input type="checkbox"/>	Show users customized actions from the page layout editor. Enabled by default for all profiles except Chatter Free User, Chatter External User, Cloud Integration User, and any custom profiles cloned from them.
Allow Inclusion of Code Snippets from UI	<input type="checkbox"/>	Allow users to post code snippets from the UI where available.
Allow sending of List Emails	<input type="checkbox"/> ⓘ	Allow users to create, edit and send List Emails.
Apex REST Services	<input type="checkbox"/>	Allow access to Apex REST services.
Assign Topics	<input type="checkbox"/>	Assign existing topics to feed items. Remove topics from feed items.
Can Approve Feed Post and Comment	<input type="checkbox"/>	Lets users control the visibility of content to other users by updating the status of a feed item or comment from pending review to published or from published to pending review.
Change Dashboard Colors	<input type="checkbox"/>	Choose dashboard color theme and palette.
Chatter Internal User	<input type="checkbox"/>	Use all Chatter features.
Close Conversation Threads	<input type="checkbox"/>	Close conversation threads in profile, group, and topic feeds in communities.
Configure Custom Recommendations	<input type="checkbox"/>	Add custom recommendations in the feed, motivating users to get engaged and take action.
Connect Organization to Environment Hub	<input type="checkbox"/>	Allows a user to connect this organization to an Environment Hub.
Create and Customize Dashboards	<input type="checkbox"/>	Create, edit, and delete dashboards in personal folders.
Create and Customize List Views	<input type="checkbox"/>	Create list views, modify, and delete own list views.

Two-Factor Authentication for User Interface Logins	<input checked="" type="checkbox"/>	Require users to use a second factor of authentication during login with username and password to Salesforce orgs.
---	-------------------------------------	--

Permission Set: **2FA-FEITIAN**

Find Settings... ⓘ Clone Delete Edit Properties Manage Assignments

Permission Set Overview > System Permissions ▼

System Permissions **Save** Cancel

Click Add Assignments to add users who need two-factor authentication.

Assigned Users: **2FA-FEITIAN** [Back to: Permission Set](#)

Add Assignments Remove Assignments

Full Name ↑	Alias	Username	Last Login
No records to display.			

Add Assignments Remove Assignments

Assign Users
All Users

View: All Users Edit Create New View


Assign Cancel

Action	Full Name ↑	Alias	Username
<input type="checkbox"/> Edit	Chatter Expert	Chatter	chatty.00d6f0000029vbguae.jkoyqvkjow5@chatter.salesforce.com
<input checked="" type="checkbox"/> Edit			@force.com
<input type="checkbox"/> Edit	Integration CPQ	cpquqr	cpqintegration@00d6f0000029vbguae.ext

Assign Cancel

Register a FEITIAN ePass FIDO for your account.

Log out and re-log in your account, a window will pop up. Click **Choose Another Verification Methods**.



Connect Salesforce Authenticator

For security reasons, you have to connect Salesforce Authenticator to your account. The app sends a notification when we need to verify your identity, and you verify with just a tap. You can also enable location services to have the app verify you automatically from trusted locations. The app provides codes to use as an alternate verification method.


1. Download Salesforce Authenticator from the App Store or Google Play and install it on your mobile device.
2. Open the app and tap + to add your account.
3. The app shows you a unique two-word phrase. Enter the phrase below.

Two-Word Phrase

Back Connect

Choose Another Verification Method

Choose the option of 'use a universal U2F key



Choose a Verification Method

How would you like to verify your identity?

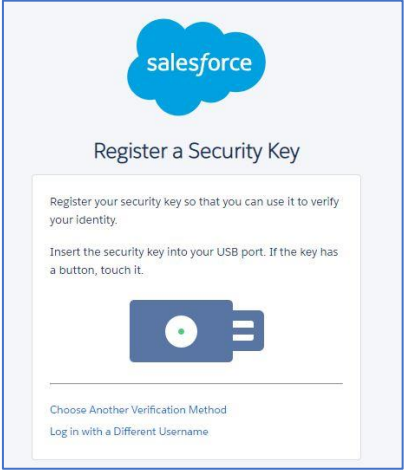
☐ Use the Salesforce Authenticator mobile app

☒ Use a Universal Second Factor (U2F) key

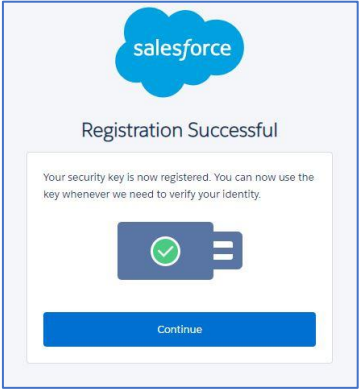
☐ Use verification codes from an authenticator app

Continue

Insert your FEITIAN ePass FIDO security key and touch it.

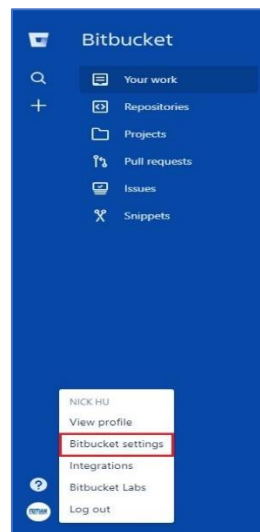


Now, you have successfully registered a security for your account.



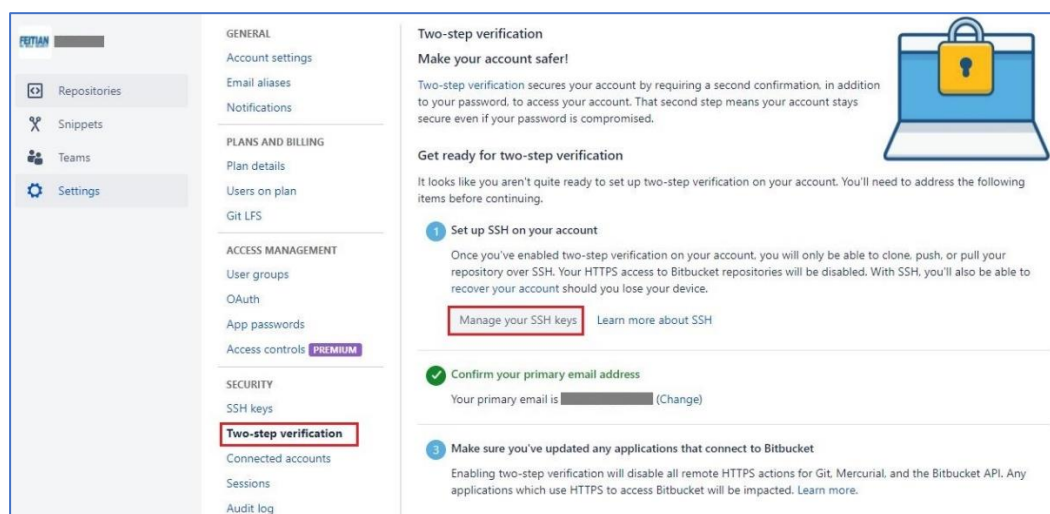
2.8. Bitbucket

Sign in Bitbucket account and go to **Bitbucket settings**.

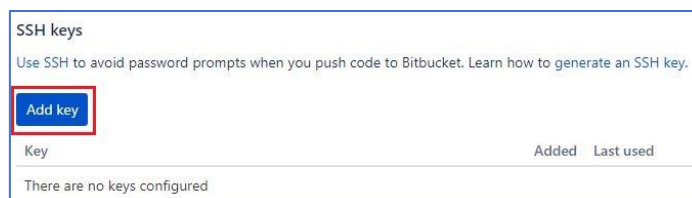


Under **Two-step verification** tab, click **Manage your SSH keys**.

Before you can enable two-factor authentication, Bitbucket requires you to add SSH keys firstly.



Click **Add key** to get a pup-up window where you can input your key.

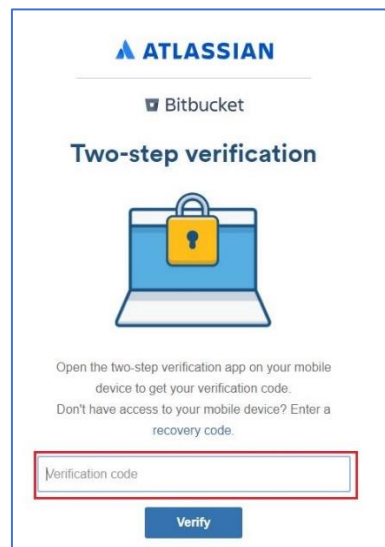


Generate SSH key under windows command prompt.

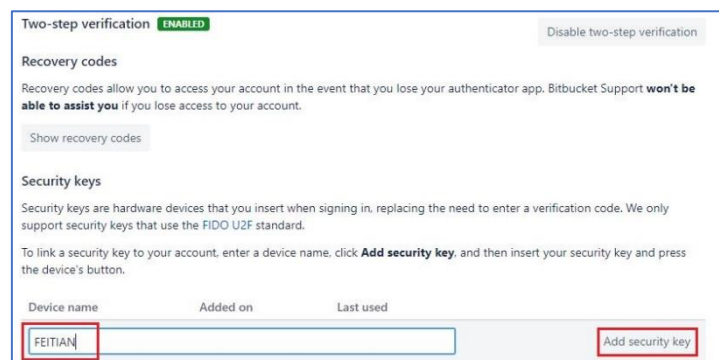
Follow the instructions as indicated in the picture and you can find your key files in the specific directory.



Re-enter verification code again.



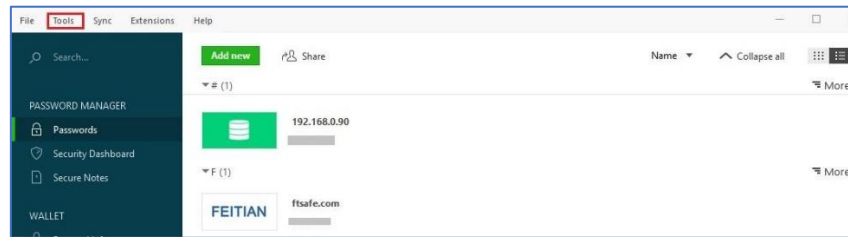
Add FEITIAN ePass FIDO security key. Name it and click **Add security key**.



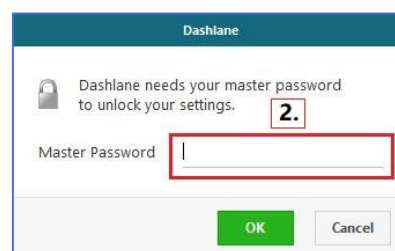
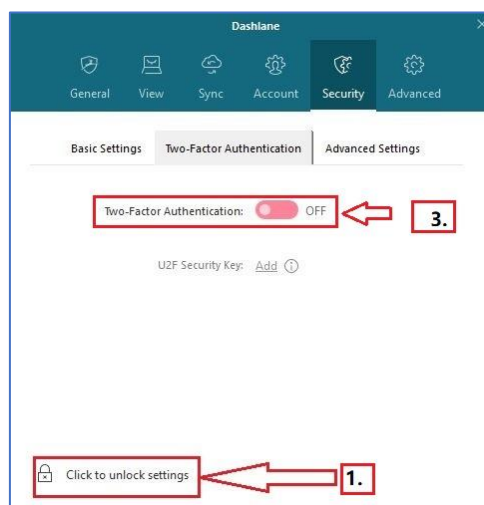
So far, you are ready to try two-step verification in Bitbucket account.

2.9. Dashlane

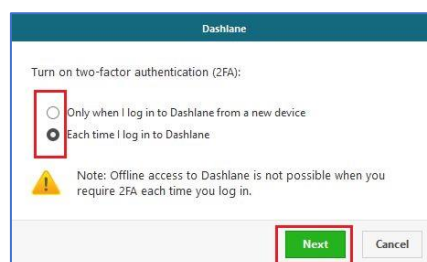
Log in Dashlane account and go to **Tools/Preferences**.



Under **Security** tab, follow the instruction highlighted. Firstly, click **Click to unlock settings**, by doing this, it requires your password showed in step 2. Then click the toolbar next to **OFF**.

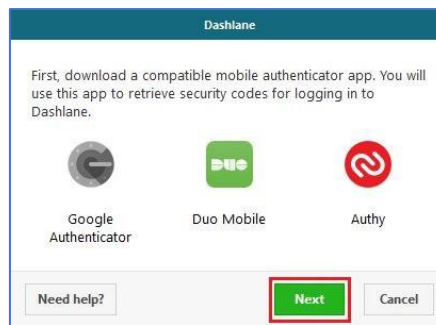


In the pop-up window, choose one of the options and click **Next**.

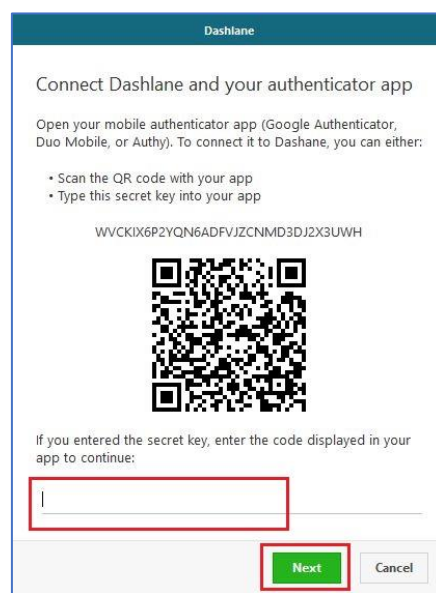


Chose a compatible mobile authenticator app to retrieve security codes and click

Next.



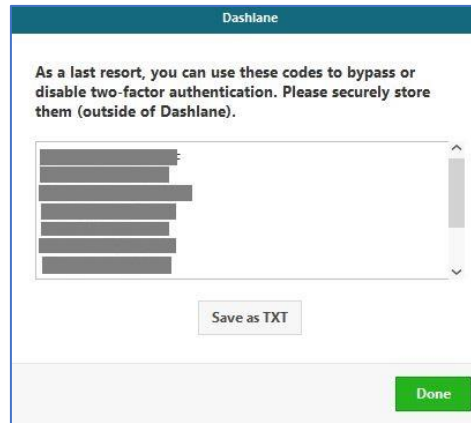
Use the chosen mobile authenticator app to scan the QR bar, input it and click **Next**.



Input a backup phone number if you do not have one and click **Next**.

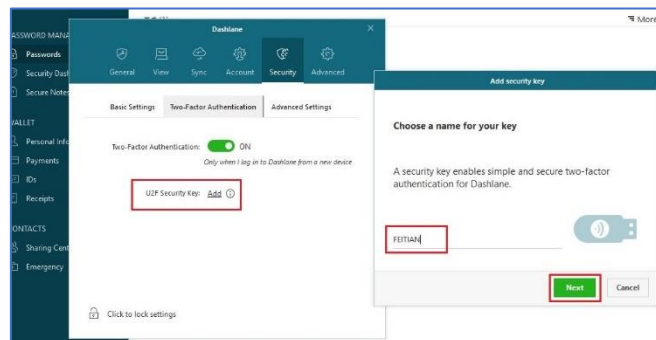


Carefully save the recovery codes and click **Done**.



Register your FEITIAN ePass FIDO.

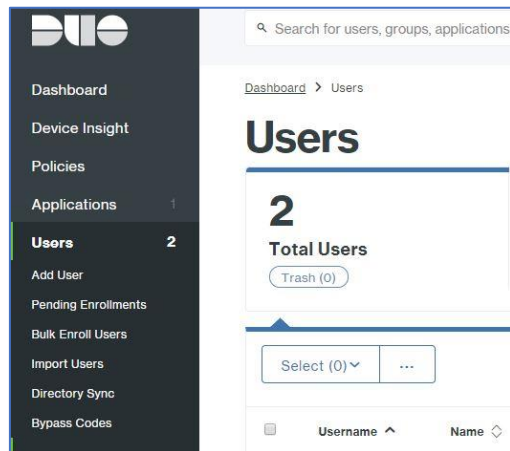
Next to **U2F Security key**, click **Add**. You should name your security key in the pop-up window and click **Next**.



Congratulations! You have successfully registered a security for your account.

2.10. DUO

Log in DUO account and click **Users** to manage user list.



Click **Add User** to enroll a none existing user.



Name the user and click **Add User**.

A screenshot of the 'Add User' form. The title 'Add User' is at the top. Below it is a section 'Adding Users' with explanatory text and a link to 'Learn more about adding users'. The 'Username' field contains the text 'NICKHLJ' and is highlighted with a red box. A note below the field says 'Should match the primary authentication username.' At the bottom of the form, the 'Add User' button is highlighted with a red box.

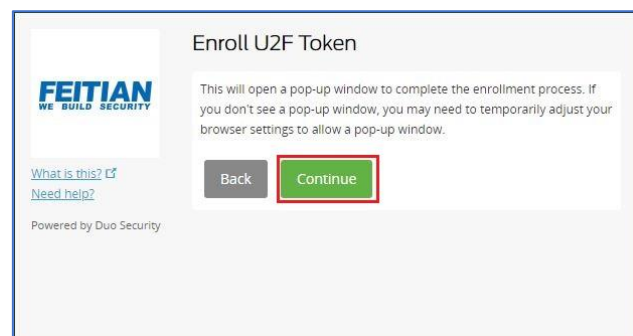
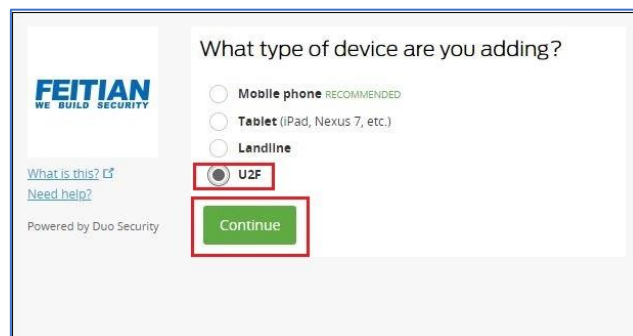
Enter user's email and click **Send Enrollment email**.

A screenshot of the 'Send Enrollment email' form. At the top right, there are links for 'Logs', 'Send Enrollment Email' (highlighted with a red box), and 'Send to Trash'. A message states: 'This user has not enrolled yet. See our [enrollment documentation](#) to learn more about enrolling users.' The form contains several input fields: 'Username' (with a dropdown), 'Username Alias 1', 'Add alias' (with a note 'Users can have up to 4 aliases'), 'Real Name', and 'Email' (containing 'nicky@ftsafe.com' and highlighted with a red box).

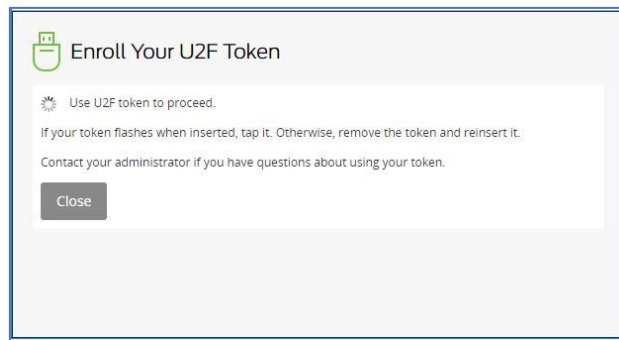
Register FEITIAN ePassFIDO security key.
You may find a link within your email and click it.



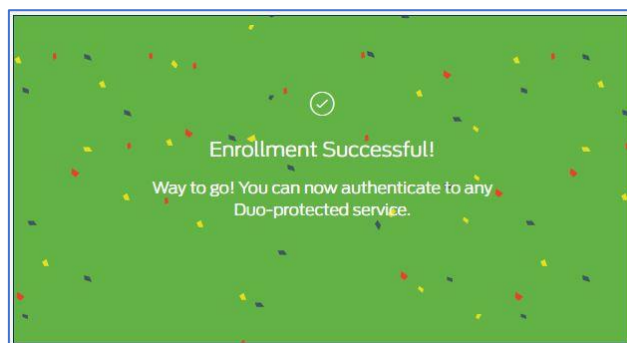
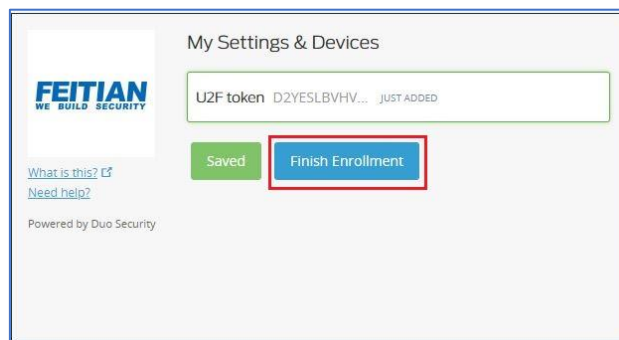
Follow the instructions, click **Start setup**, choose U2F token to continue.



Insert your FEITIAN ePass FIDO token and tap it.

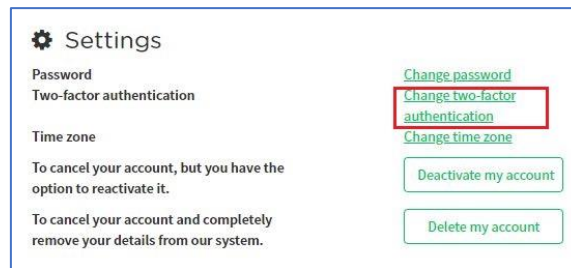


Click **Finish Enrollment** to complete the registration.

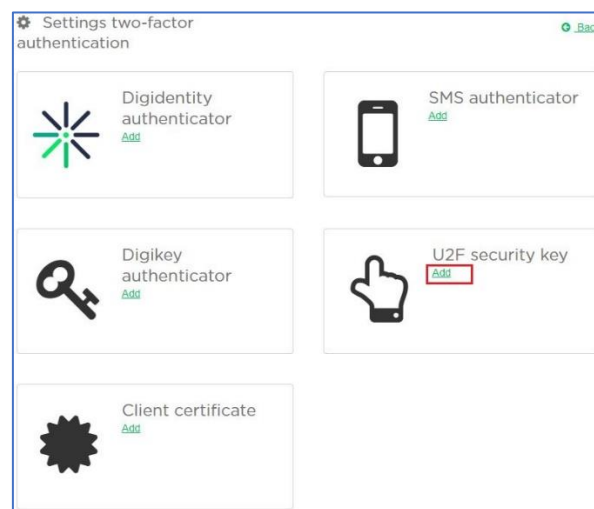


2.11. Digidentity

Log in Digidentity account and go to **Settings**. And click Change **two-factor authentication**.



Click Add under U2F security key.



Name your FEITIAN ePass FIDO and tick **External security key**, then click **Create authenticator**.

Add U2F security key

A FIDO U2F compatible security key is a hardware device that can be used to secure your profile with two-factor authentication. When logging in, you tap a button on the device instead of typing a security code from your mobile phone. Currently only Chrome version 41 or later is supported.

In the field below you can enter a name to identify the security key you are about to set up. Please make sure the key is inserted before continuing.

Name

Type of U2F security key

☒ External security key

☐ Internal security key

[Create authenticator](#) [Cancel](#)

Follow instructions to insert FEITIAN ePass FIDO and tap it.

Add U2F security key

Insert your U2F key into a USB port. If your security key has a button or a gold disc, tap it now.

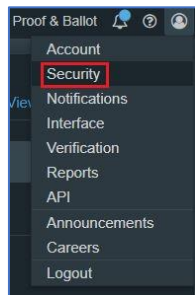


[Cancel](#)

You have finish registration and ready to go!

2.12. BITFINEX

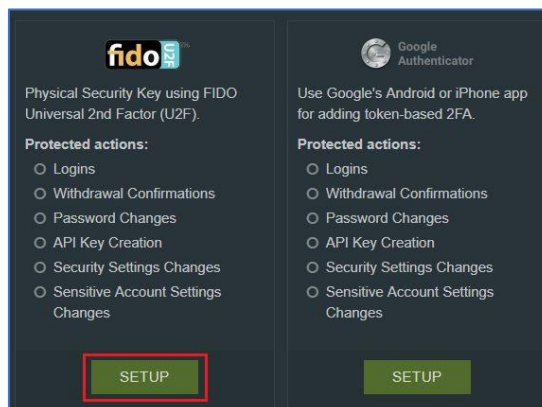
Log in your account and go to **Security**.



Click **two-factor authentication**.



Choose to setup **Physical Security Key using FIDO Universal 2nd Factor (U2F)**.



Name your FEITIAN ePass FIDO and click **Click here** to start registration.

Enable U2F [What is U2F?](#)

REQUIREMENTS

- An up-to-date version of the Chrome browser (or modern browser with U2F support).
- A Security Key device that plugs into a USB port and works with FIDO Universal 2nd Factor (U2F)

OPTIONS

- Enter a label for this Security Key (useful if you are using multiple keys).
- Choose if a user who logs in using this Security Key should have permission to trade and/or withdraw.

Label:

☒ Withdraw ☒ Trade

[Click here](#) to start device registration

Insert your security key as indicated and press it.

Enable U2F [What is U2F?](#)

REQUIREMENTS

- An up-to-date version of the Chrome browser (or modern browser with U2F support).
- A Security Key device that plugs into a USB port and works with FIDO Universal 2nd Factor (U2F)

OPTIONS

- Enter a label for this Security Key (useful if you are using multiple keys).
- Choose if a user who logs in using this Security Key should have permission to trade and/or withdraw.

Label:

☒ Withdraw ☒ Trade

[Click here](#) to start device registration

A notification email will be sent to you, and you need to go to your email and click **ACTIVATE U2F 2FA NOW** to finish registration.

Almost Done! Please check your email to complete the setup of this U2F security key.

Okay

Activate U2F two-factor authentication

Someone requested to activate U2F two-factor authentication (2FA) on your account. **If you did not make this request please ignore this email and do NOT follow the link below.**

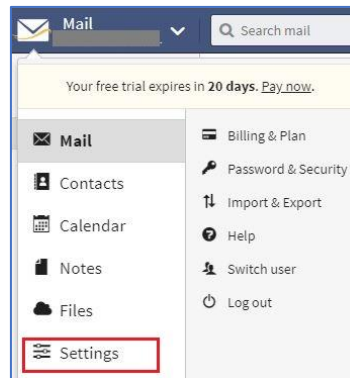
The following secure link is valid for only one use and will expire after 24 hours. If you have a problem using the link below, please restart this process to receive a new email with a new secure link.

[ACTIVATE U2F 2FA NOW](#)

Regards,
The Bitfinex Team

2.13. FastMail

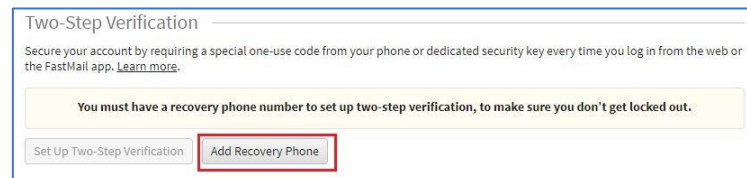
Sign in your Fastmail account and go to **Settings**.



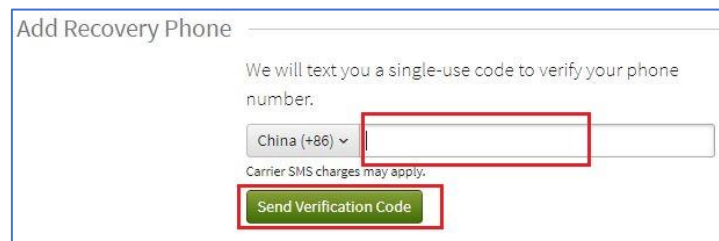
Under **Password & Security** tab, you need to input your password to unlock the functions.



Before you enable the two-step verification, it requires you to add a recovery phone if you do not have one.



Input your phone number and click **Send Verification Code**.



Input the codes you received.

Add Recovery Phone

Please enter the code sent to +86

Texts may take up to 30 seconds to arrive.

Now you are able to do the enable operation. Click **Set Up Two-Step Verification**.

Two-Step Verification

Secure your account by requiring a special one-use code from your phone or dedicated security key every time you log in from the web or the FastMail app. [Learn more.](#)

In the following webpage, choose **Set Up Security Key** under **Security Key (U2F)**.


Add Verification Device

<p>Authenticator App (TOTP)</p> <p>Use a free app on your phone to get a time-limited verification code. Learn more.</p> <p><input type="button" value="Set Up Authenticator App"/></p>	<p>Security Key (U2F)</p> <p>Use a USB security key to verify your identity. Very secure. U2F is currently only supported by Google Chrome. Learn more.</p> <p><input type="button" value="Set Up Security Key"/></p>	<p>YubiKey OTP</p> <p>Use an older YubiKey USB security key to verify your identity. Learn more.</p> <p><input type="button" value="Set Up YubiKey OTP"/></p>
---	---	---

Insert your FEITIAN ePass FIDO as indicated and touch it.

Set Up Security Key

① Insert your security key into the computer. Then if it has a button, press it.




Waiting for device

Name your security and save it. You are ready to go!

Set Up Security Key

① Insert your security key into the computer. Then if it has a button, press it.

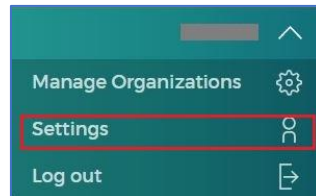


Got it

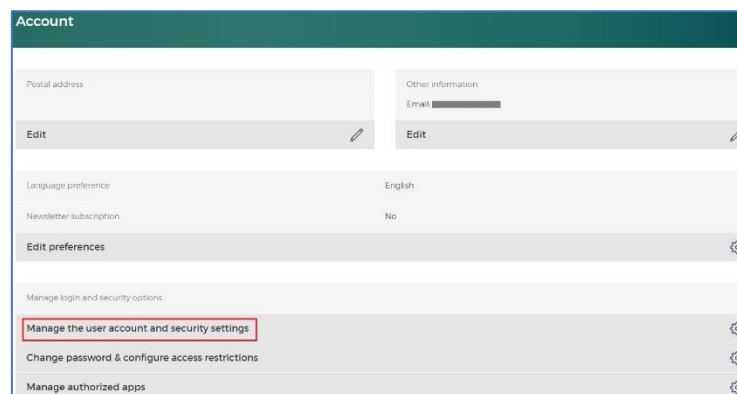
② Give this security key a name so you can easily identify it should you need to remove access later:

2.14. Gandi.net

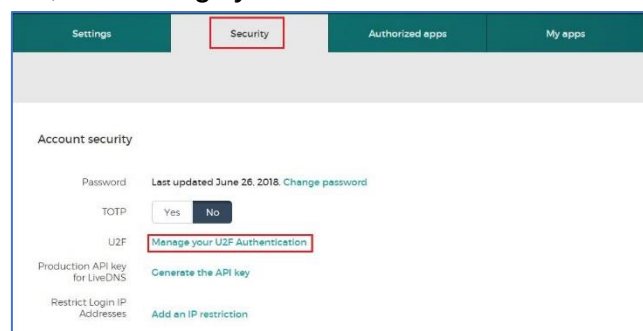
Log in your account and go to Settings.



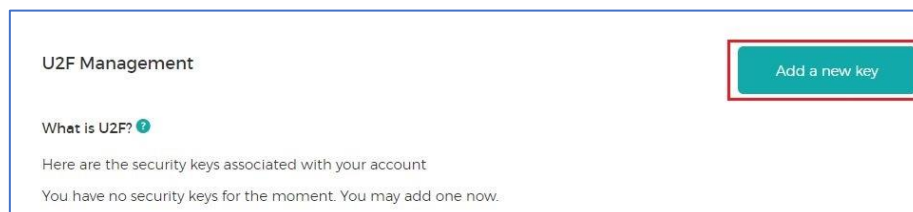
Click **Manage the user account and security settings**.



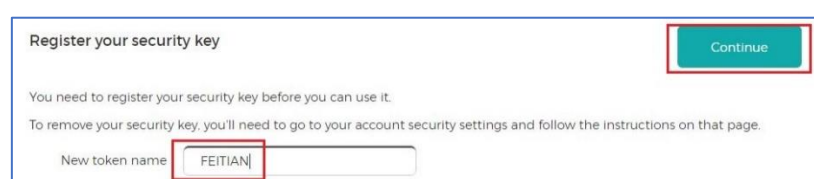
Under Security tab, click **Manage your U2F Authentication**.



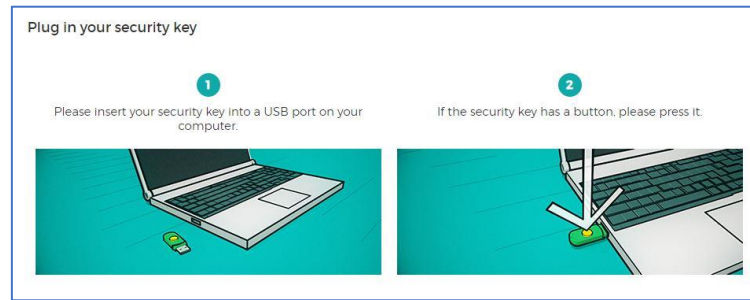
Register your FEITIAN ePass FIDO security key by click **Add a new key**.



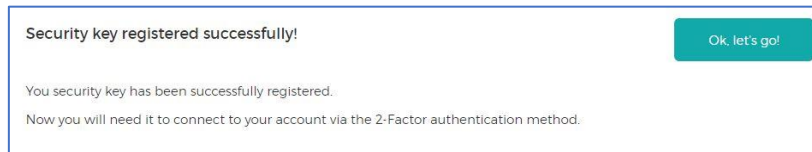
Name your security key and continue.



Insert and press the external hardware key as indicated.

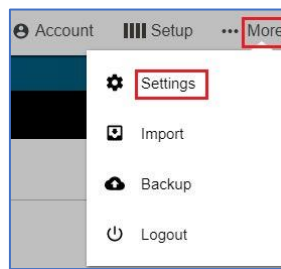


You have successfully registered a FEITIAN ePass FIDO and ready to try out.



2.15. Keeper

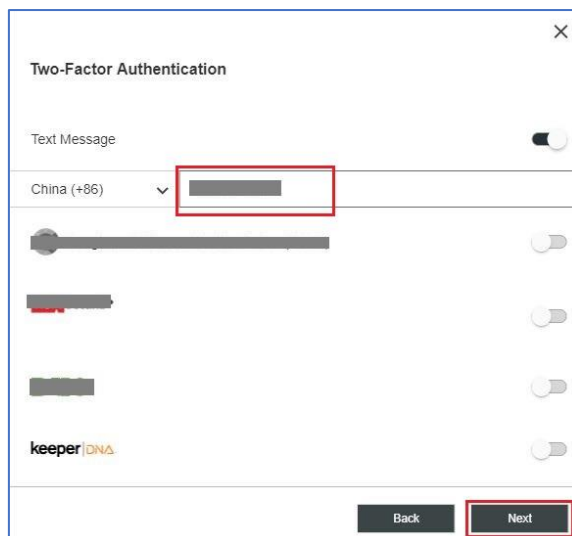
Log in your account and go to **More/Settings**.



Under **Security** tab, click **Setup** next to **Two-Factor Authentication**.




Input your phone number and click **Next**.



Enter code you received and click **Next**.

×

Two-Factor Authentication Sign Up



A 6-digit confirmation code has been sent by SMS to [REDACTED]. Please enter the code in the confirmation box to verify your number.

123456

Send a new code

Back

Next

Carefully save the backup codes.

×

Backup Codes

If you are unable to receive Two-Factor codes, you will need the below backup codes to access your account.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

When you have written these codes down, please click below:

I have written these codes down.

Register your security key by clicking **Setup** next to **Security Keys**.

×

Settings

General

Security

Advanced Settings

KeeperFill

Auto-Logout

Two-Factor Authentication ?

Notification Method

Edit Two-Factor

Text Message


Security Keys ?

Setup

Name your security key and click **Register**, and the **Done**.

×

Add Security Key



Register Your Security Key

Insert your Security Key into a USB port.

Security Key Name

FEITIAN ePassFIDO


Register

BackDone

Now you have already successfully registered the security.

×

Associated Security Keys

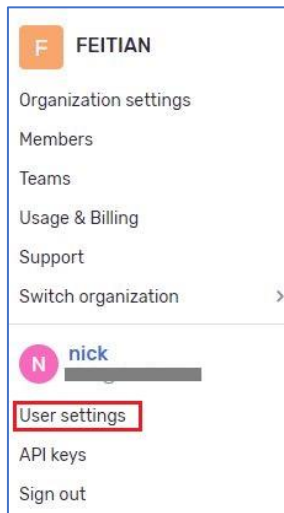
Name	Added	
● FEITIAN ePassFIDO	7/6/2018, 10:47:25 AM	

Add Security Key

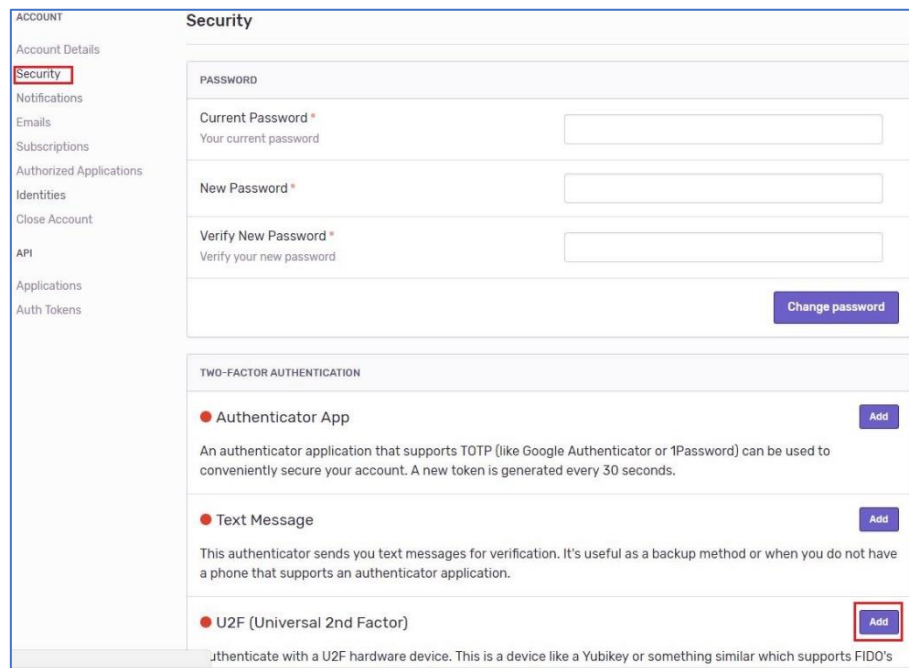
Done

2.16. Sentry

Log in your account and go to **User settings**.



Under **Security** tab, click Add next to **U2F (Universal 2nd Factor)**.



Name your security key and press it.


U2F (Universal 2nd Factor)

Authenticate with a U2F hardware device. This is a device like a Yubikey or something similar which supports FIDO's U2F specification. This also requires a browser which supports this system (like Google Chrome).


CONFIGURATION

Device name

FEITIAN ePassFDIO



To enroll your U2F device insert it now or tap the button on it to activate it.



These settings are currently in beta. Please report any issues. You can temporarily visit the [old settings page](#) if necessary.

A phone number is required, but you could also skip it.

Two-Factor Authentication Enabled

Two-factor authentication via U2F (Universal 2nd Factor) has been enabled.

You should now set up recovery options to secure your account.

We recommend adding a phone number as a backup 2FA method.

Skip this step

Add a Phone Number

Get recovery codes for next step, and carefully save them.

Two-Factor Authentication Enabled

Two-factor authentication via U2F (Universal 2nd Factor) has been enabled.

You should now set up recovery options to secure your account.

Recovery codes are the only way to access your account if you lose your device and cannot receive two-factor authentication codes.

Get Recovery Codes

UNUSED CODES

Regenerate Codes

Make sure to save a copy of your recovery codes and store them in a safe place.

These settings are currently in beta. Please report any issues. You can temporarily visit the [old settings page](#) if necessary.

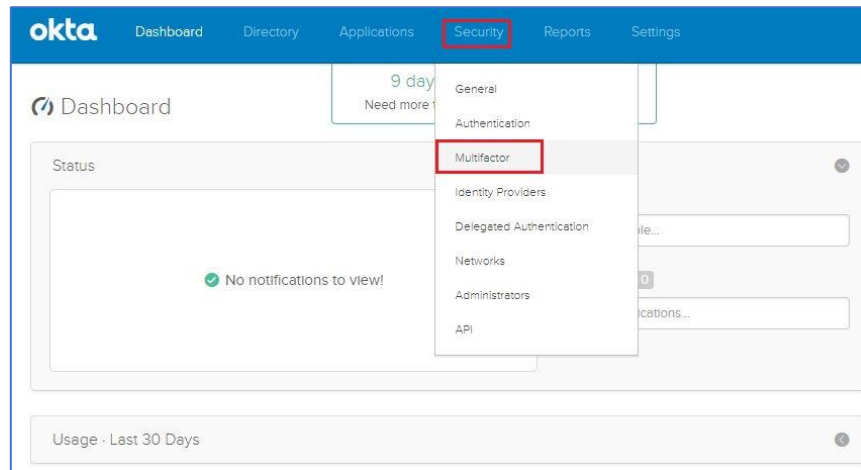
Finally, you have added a security to your account as a second authentication factor.

2.17. Okta

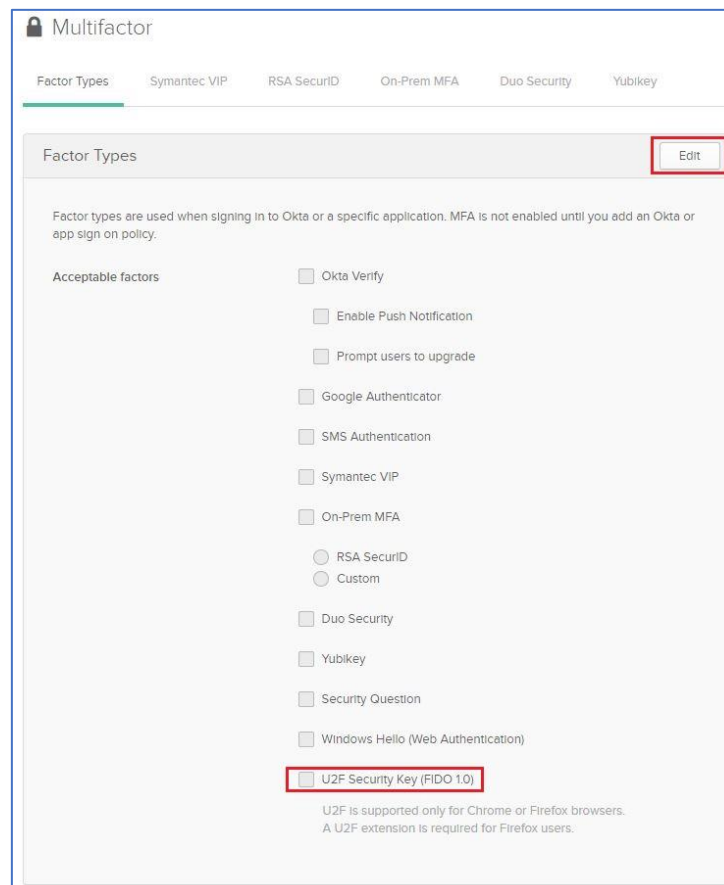
Contact Okta support to enable U2F feature as it is not default enabled.
Login your Okta account and click **Admin**.



Under **Security** tab, click **Multifactor**.



Click **Edit** button, tick **U2F security key** and save it.



Multifactor

Factor Types Symantec VIP RSA SecurID On-Prem MFA Duo Security Yubikey

Factor Types Cancel

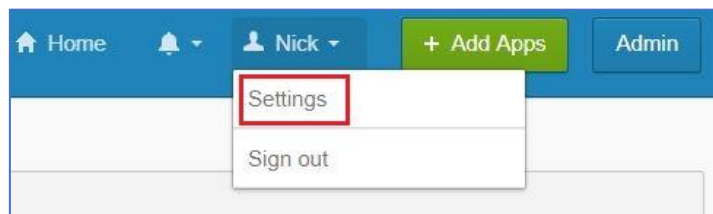
Factor types are used when signing in to Okta or a specific application. MFA is not enabled until you add an Okta or app sign on policy.

Acceptable factors

- ☐ Okta Verify
 - ☐ Enable Push Notification
 - ☐ Prompt users to upgrade
- ☐ Google Authenticator
- ☐ SMS Authentication
- ☐ Symantec VIP Configure
- ☐ On-Prem MFA
- ☐ RSA SecurID Configure
- ☐ Custom Configure
- ☐ Duo Security Configure
- ☐ Yubikey Configure
- ☐ Security Question
- ☐ Windows Hello (Web Authentication)
- ☒ **U2F Security Key (FIDO 1.0)**
U2F is supported only for Chrome or Firefox browsers.
A U2F extension is required for Firefox users.

Save Cancel

Re-login and go to **Settings**.



Click **Setup** next to **second key(U2F)** under **Extra Verification** tab.

Account

Personal Information Edit

First name Nick

Last name HU

Okta username nick@ftsefe.com

Primary email nick@ftsefe.com

Secondary email

Mobile phone

Change Password

Password requirements: at least 8 characters, a lowercase letter, an uppercase letter, a number, no parts of your username.

Enter current password


Enter new password

Repeat new password

Change Password

Security Image Edit

Your security image gives you additional assurance that you are logging into Okta, and not a fraudulent website.



Forgotten Password Question Edit


Select a forgotten password question so you can reset your password in case you have trouble signing in to your Okta account.

Question

Where did you go for your favorite vacation?


Extra Verification

Extra verification increases your account security when signing in to Okta and other applications you use.

Security Key (U2F)  Setup

You may have a pop-up window like below, ignore it and re-try.

Set Up Security Key (U2F) ×

 Security Key (U2F) is not supported on this browser. Contact your admin for assistance.

Follow the instructions to insert the security key and press it, you will finally register your FEITIAN ePass FIDO successfully.

Set Up Security Key (U2F) ×

1. Make sure you have a Security Key.
2. If you have a Bluetooth Security Key, turn on your computer's Bluetooth.

Register

Set Up Security Key (U2F)



Insert your Security Key into a USB port on this computer.
Tap the button or gold disk.

If you are using a Bluetooth Security Key, press the button.



3. Mobile based scenarios

In this sector, FEITIAN MultiPass FIDO scenarios on mobile, including IOS and Android, will be introduced.

Our MultiPass FIDO integrates three communication protocols, which are HID, Bluetooth and NFC. The feature enables us to communicate between mobile phone and FEITIAN FIDO token.

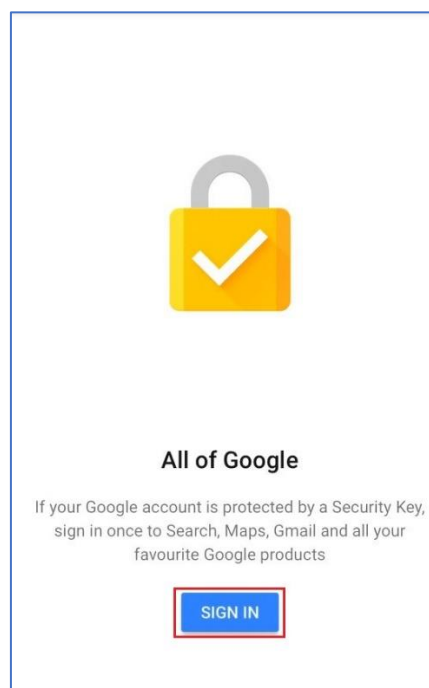
3.1. IOS platform

3.1.1. Google account

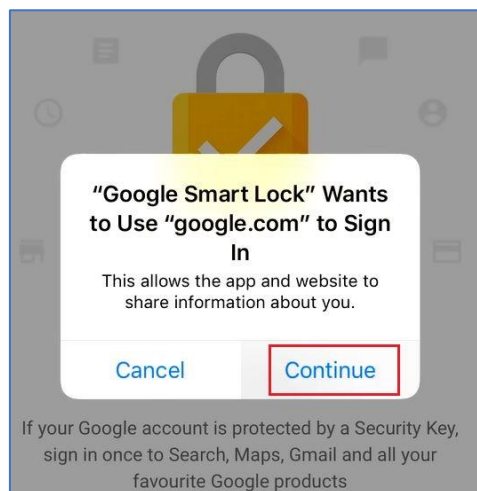
Register your FEITIAN MultiPass FIDO through online service as described in chapter 2.1.

Download **Smart Lock** APP from apple store and sign in. (make sure your phone's Bluetooth is set on and clear the existing connection with FEITIAN MultiPass FIDO)

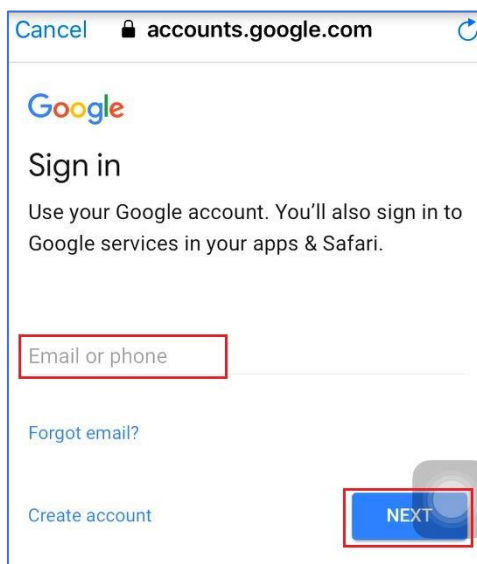
Click **SIGN IN** on **Smart Lock** UI.



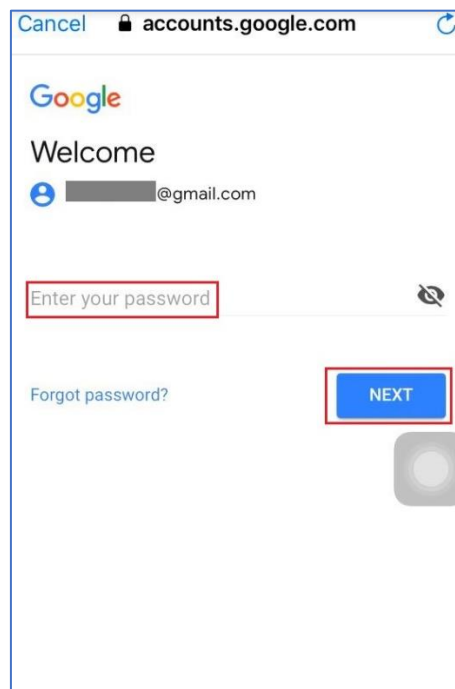
Click **Continue** on pop-up window.



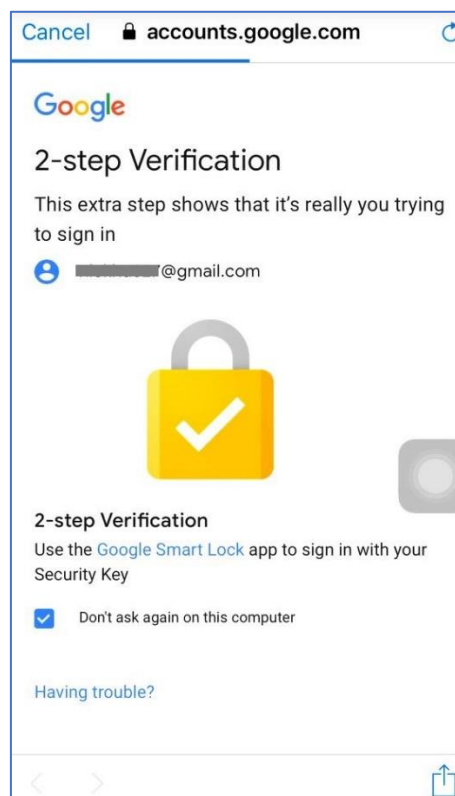
Enter your google account and click **NEXT**.



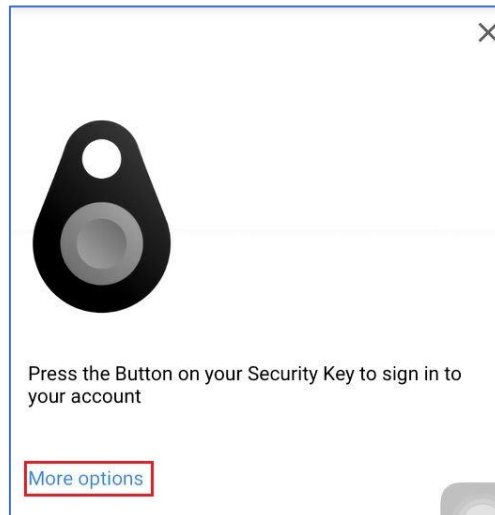
On next pop-up window, you are required to enter your password, then click **NEXT**.



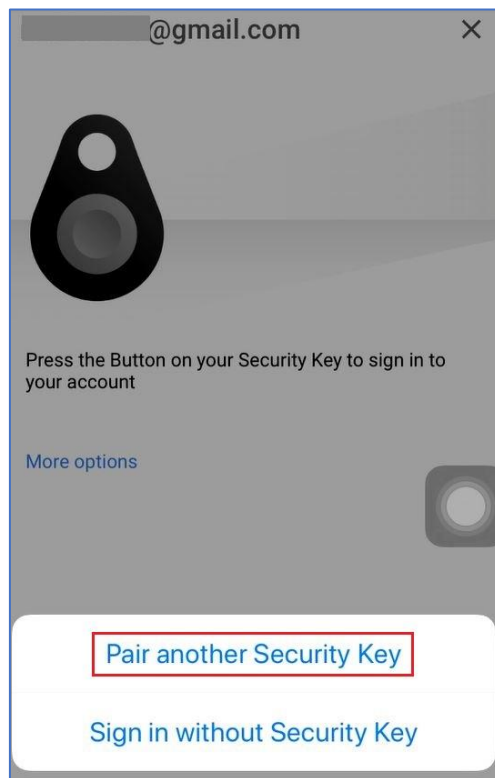
A notification window pops up and no operation is needed.



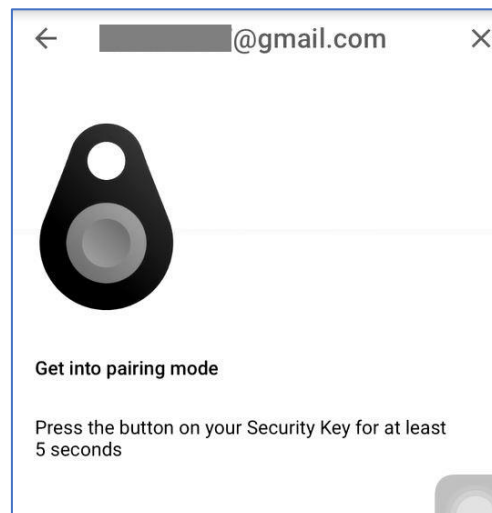
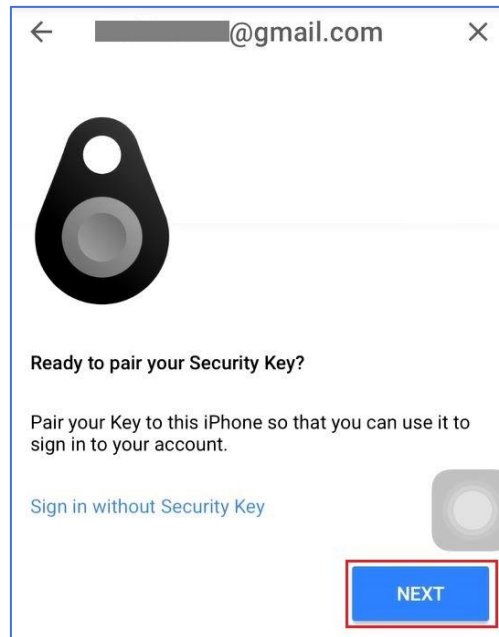
If it is the first time you connect FEITIAN MultiPass FIDO, press **More option** to connect hardware token.



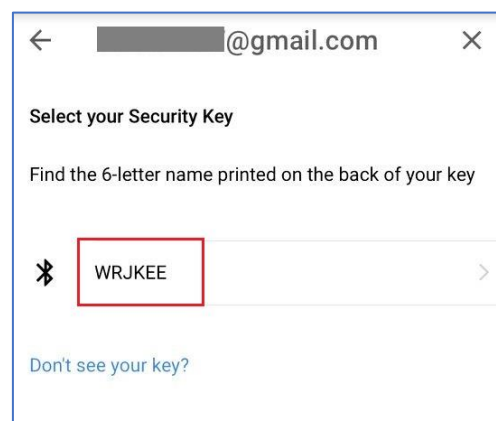
Press **Pair another Security Key**.

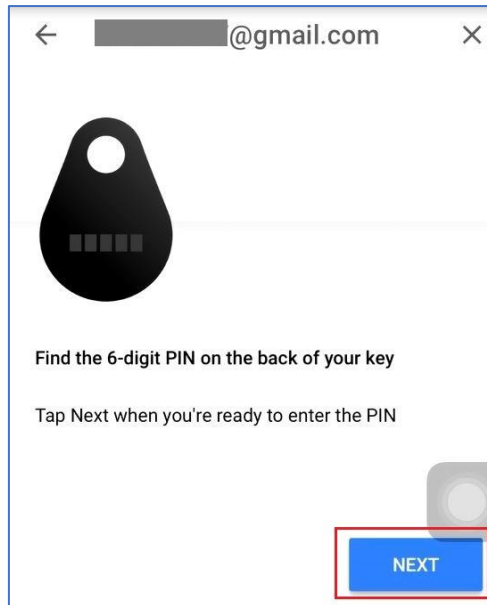


Press **NEXT** and then press the button on your security key for at least five minutes as indicated.

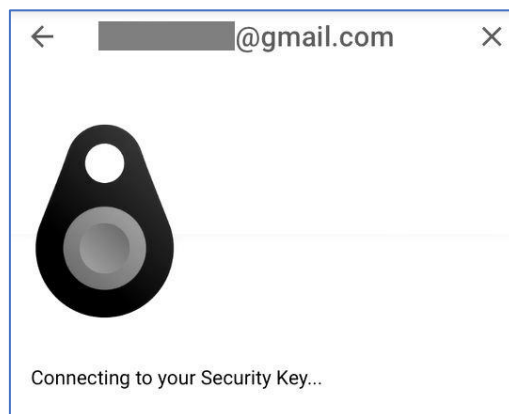


This pop-up window shows the name of your security key, press the name.
Next window indicates you to find 6-digit PIN on the back of your key, press **NEXT**.

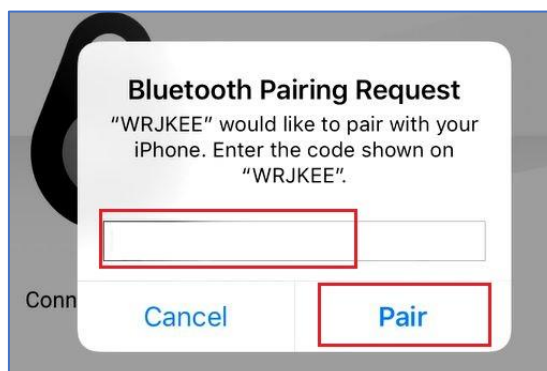




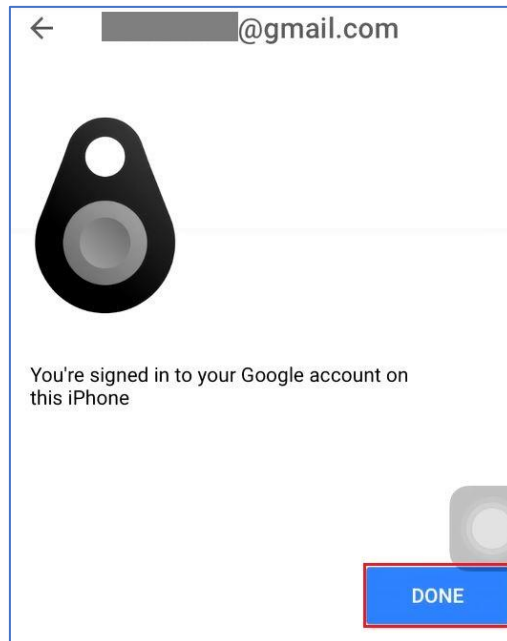
Waits for connecting to your security key.



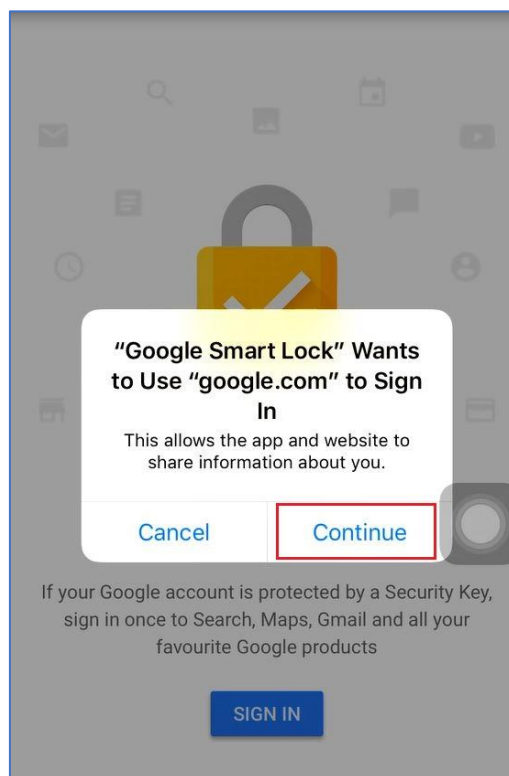
Type in the PIN on the back of your security key and press **Pair**.

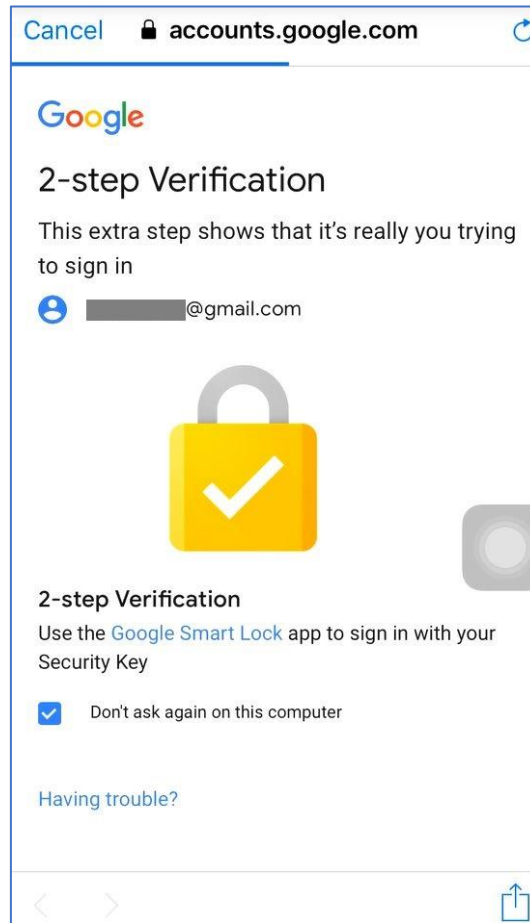


Press **DONE**.



Click **Continue** for next windows and no further operation is needed.





You have successfully added a Google account to Smart Lock now!

