FEITIAN U2F scenarios instructions

Contents

1. Introduction

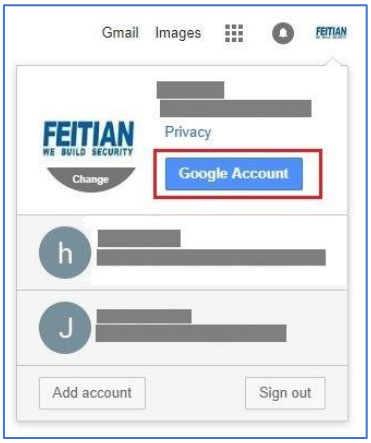
This document provides a guide for end-users to enable Two-Factor Authentication, for specific online services, platforms and applications, using FEITIAN ePass FIDO.

2. Windows platform service

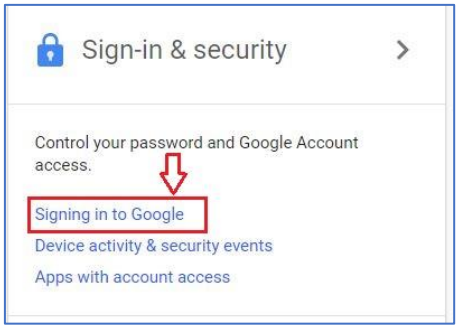
This chapter introduces a guide for end users about using FEITIAN ePass FIDO as a second authentication factor on Windows platform, including online services and Windows apps.

2.1. Google

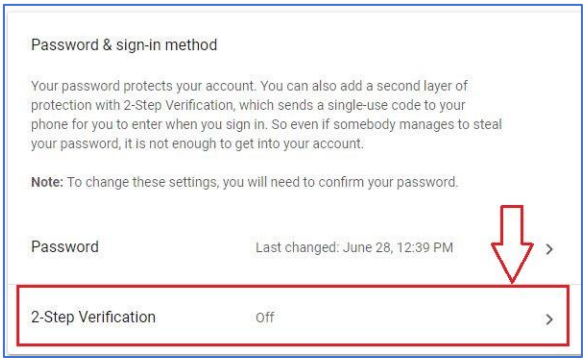
Login Google account and enable 2-step verification.
Click **Google Account** and go to **Settings**.



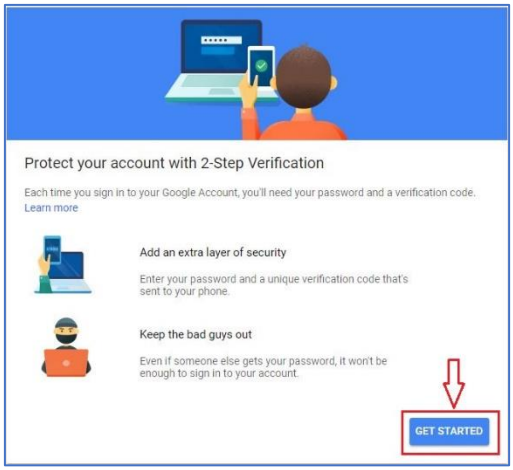
In '**Sign-in & security**' tab, click **Signing in to Google**.

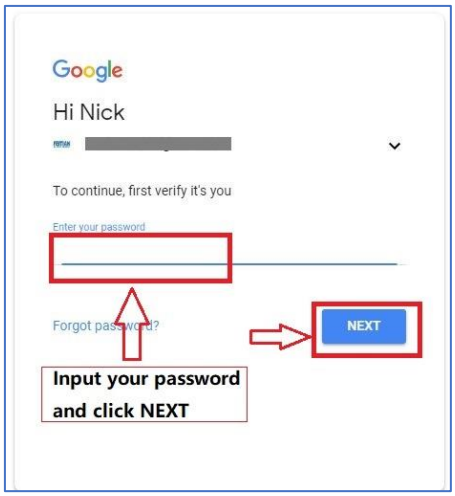


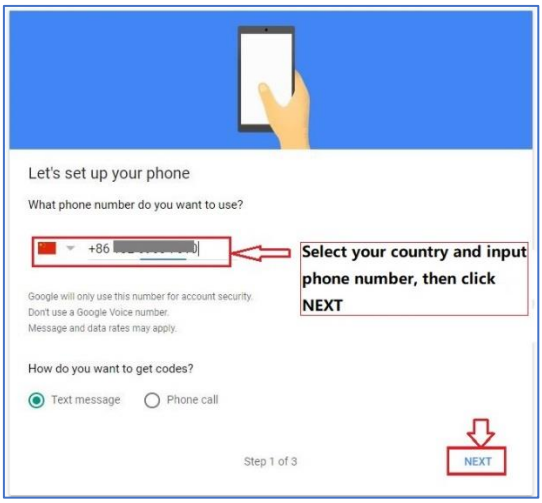
Now you can click **2-Step Verification** to enable it.

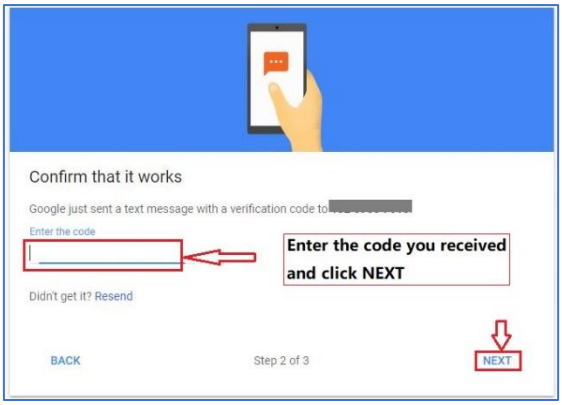


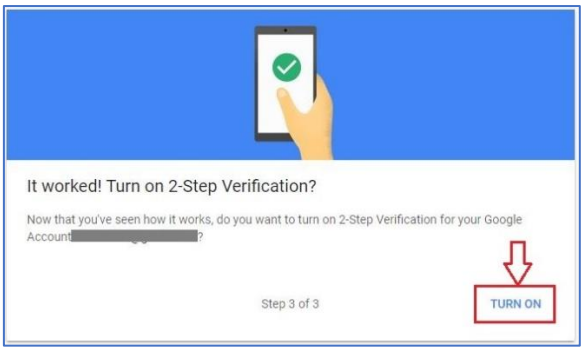
Follow the given instructions.





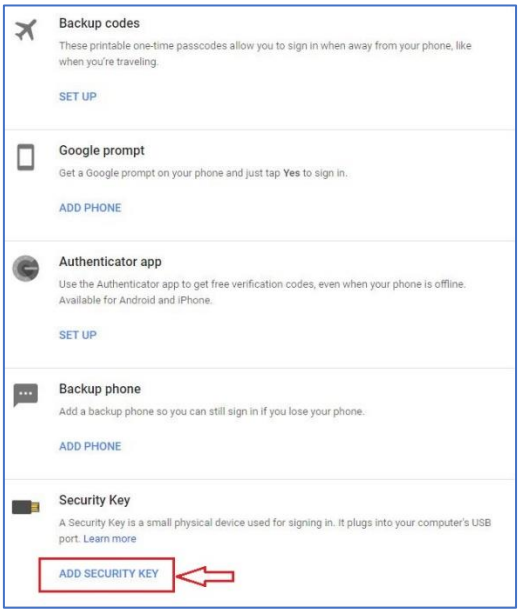


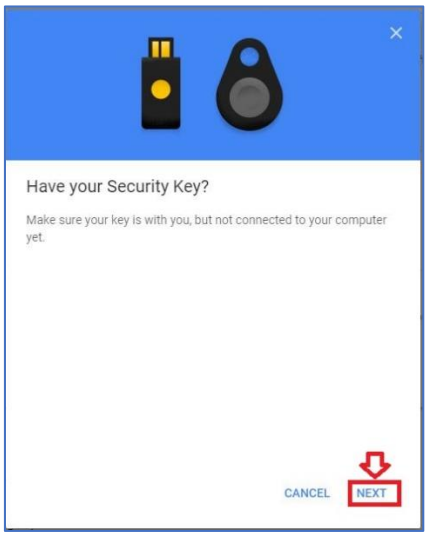




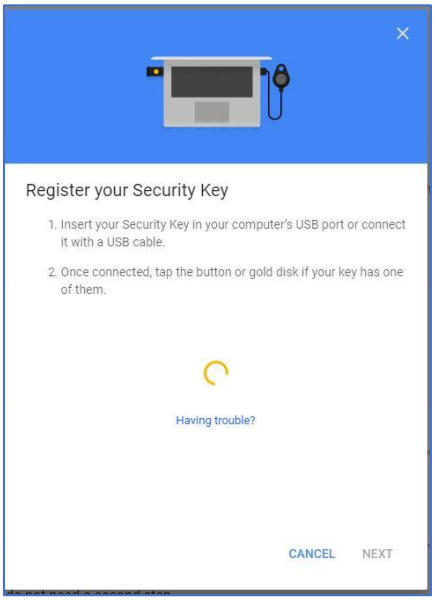
You have successfully enabled 2-step verification after all above completed.

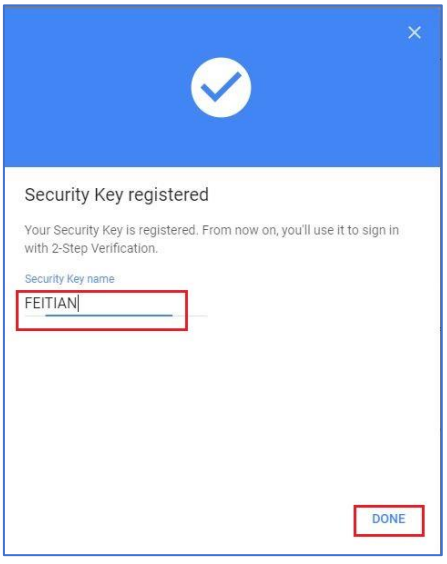
Register FEITIAN ePass FIDO.
Add ePass FIDO as security key for your account.





Insert ePass FIDO device and name it.



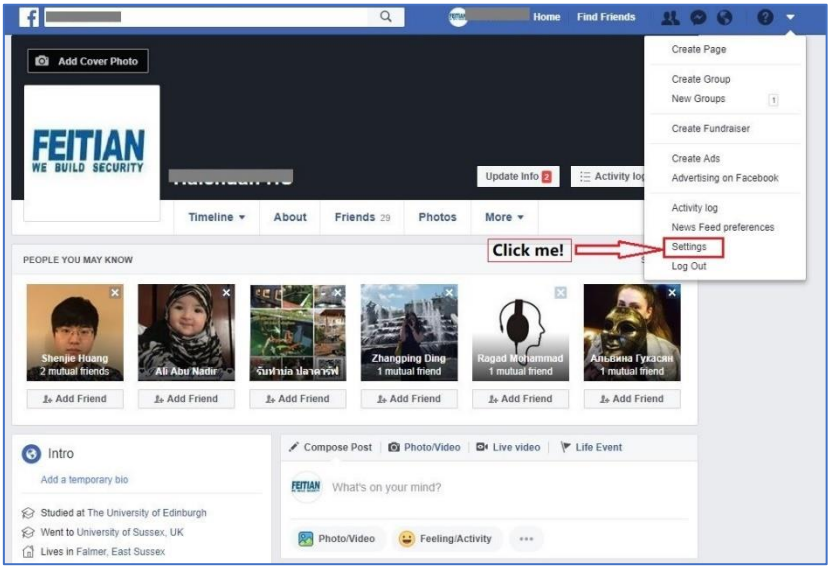


Now your ePass FIDO security key has been added successfully, and you can sign out and re-sign in to try out.

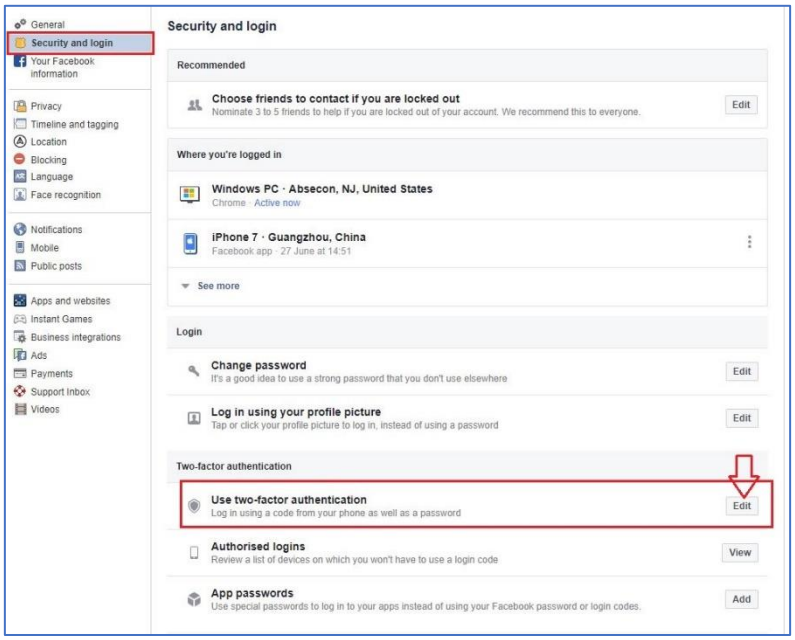
You may have more information about Google 2-step verification by click here.

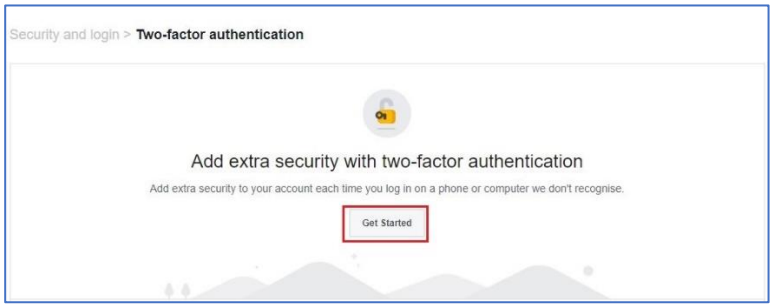
2.2. Facebook

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

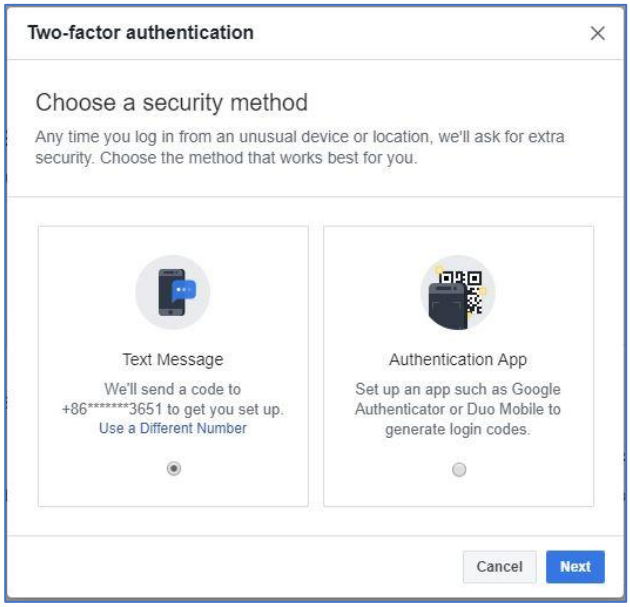


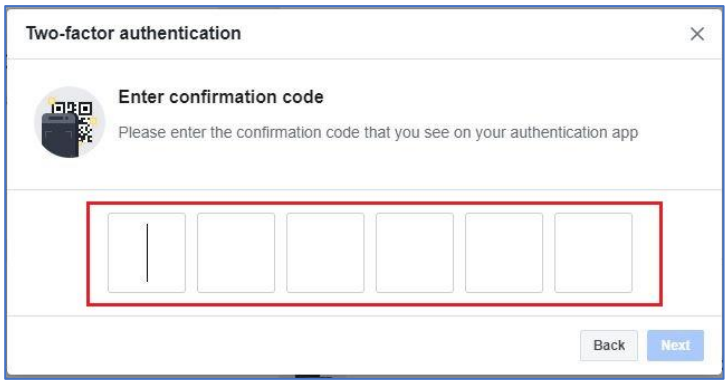
Under **Security and Login** tab, Click the highlighted **Edit** button and follow the instructions to turn on Two-factor authentication.



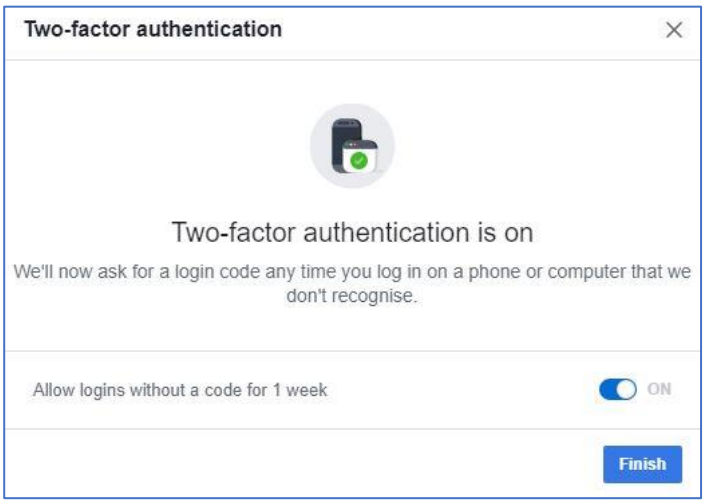


Choose a security method to verify your account and input confirmation code.

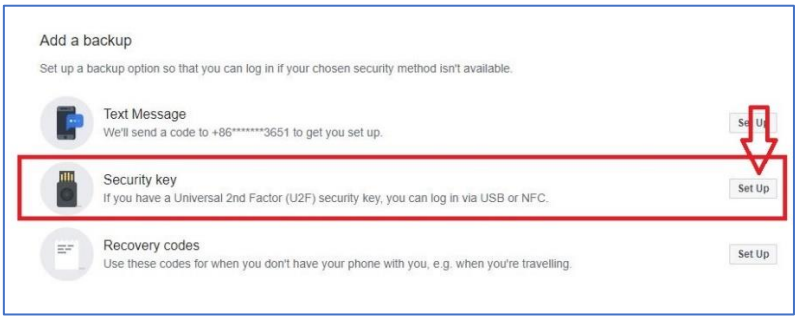




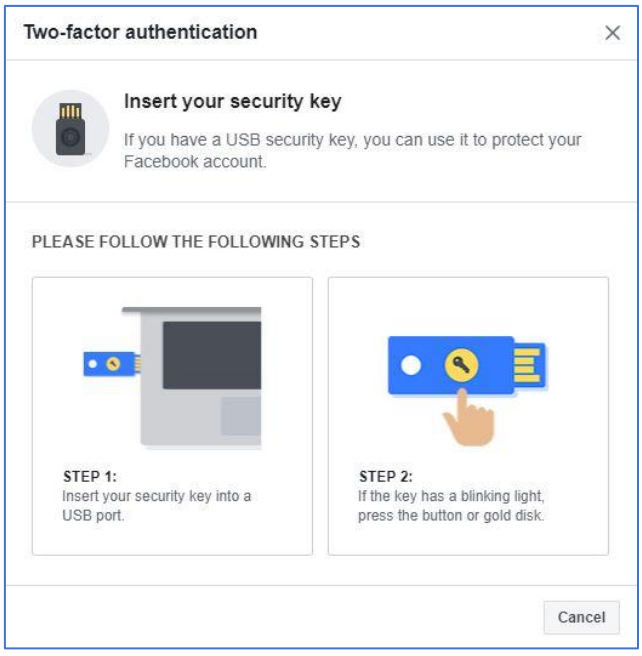
Once you have a pop-up windows like below, you have successfully enabled Two-factor authentication.

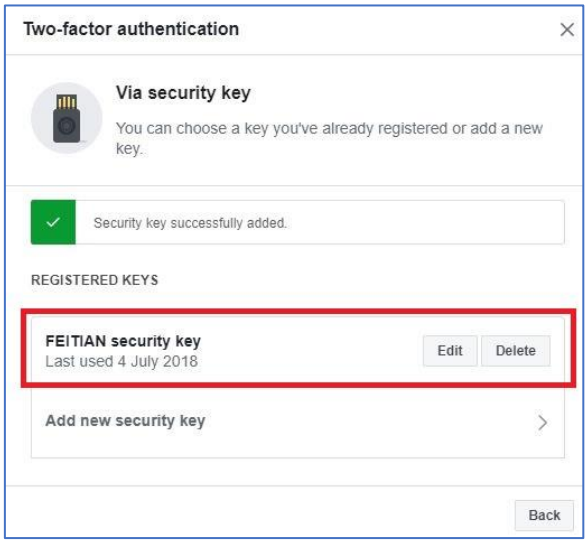


Set up a security key.



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.

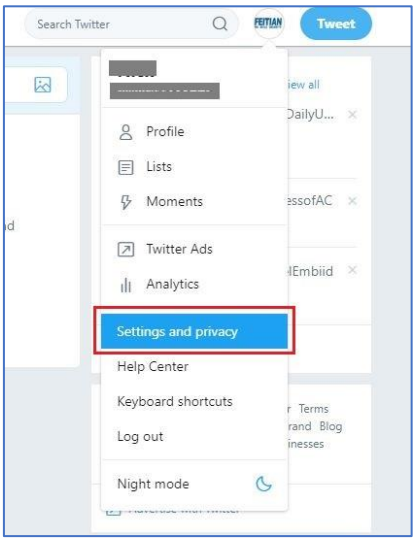




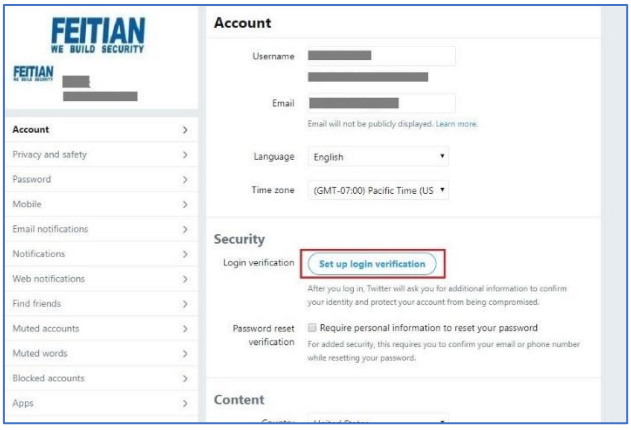
When you finish registration, you can now re-login your account to try out the two-factor authentication

2.3. Twitter

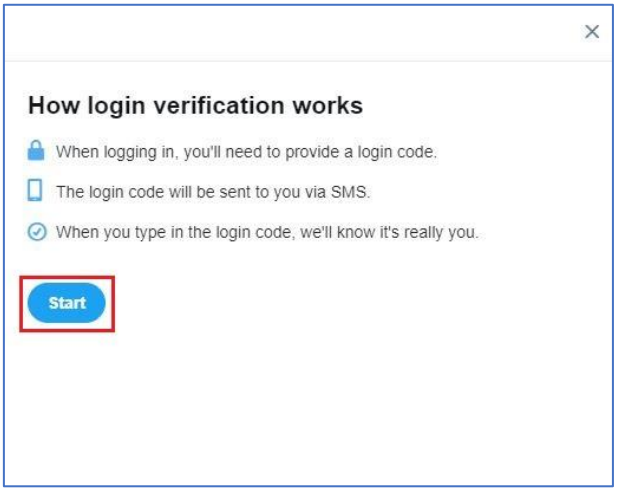
Log in your Twitter account and go to **Settings and privacy** tab.



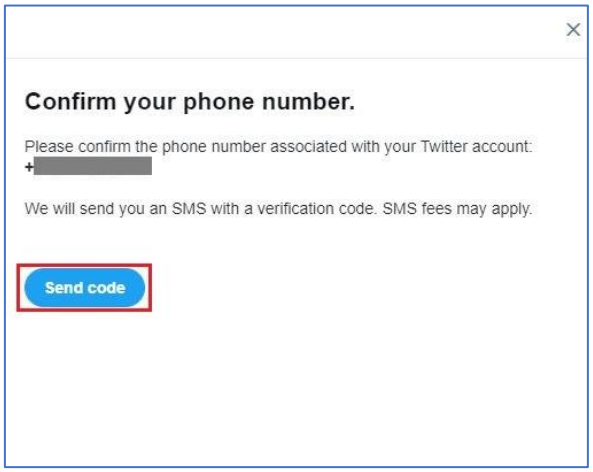
Follow the instructions to click **Set up login verification**.



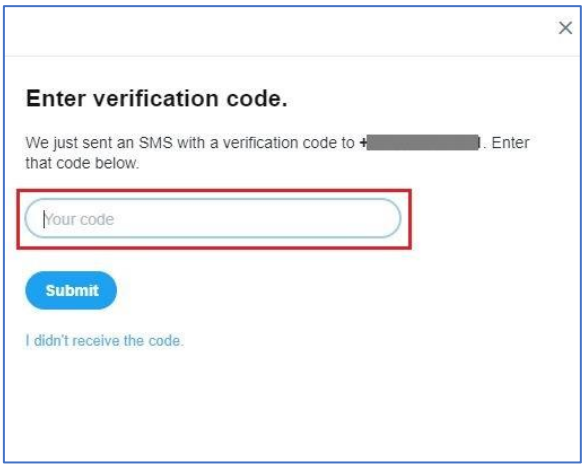
Read the overview instructions, then click **Start**.



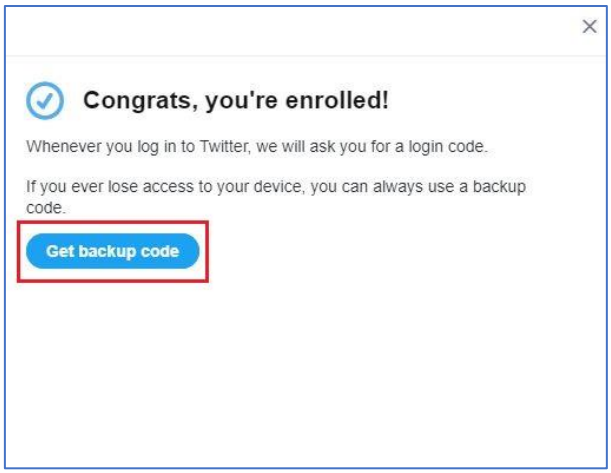
Click **Send code** to add your phone number.
Note: If you already have a phone number associated with your Twitter account, we will send you an SMS to confirm your number.

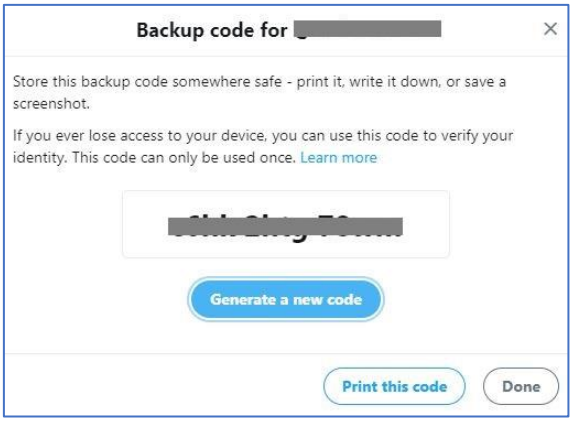


Enter the verification code sent to your device, then click **Submit**.

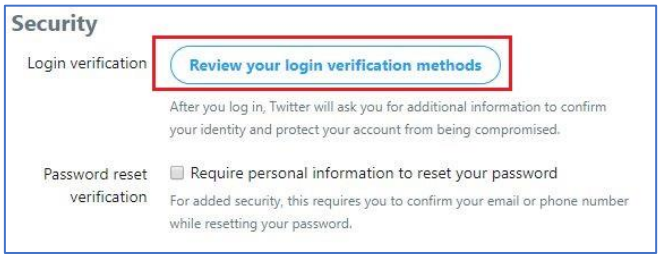


Click **Get Backup Code** to view a code, generated by Twitter. We recommend you store a screenshot of the code in case you need it for future use. This will help you access your account if you lose your mobile phone or change your phone number.

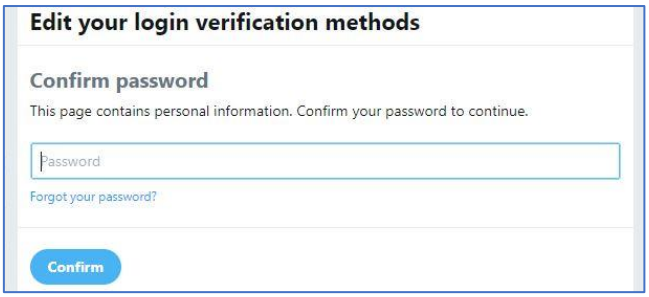




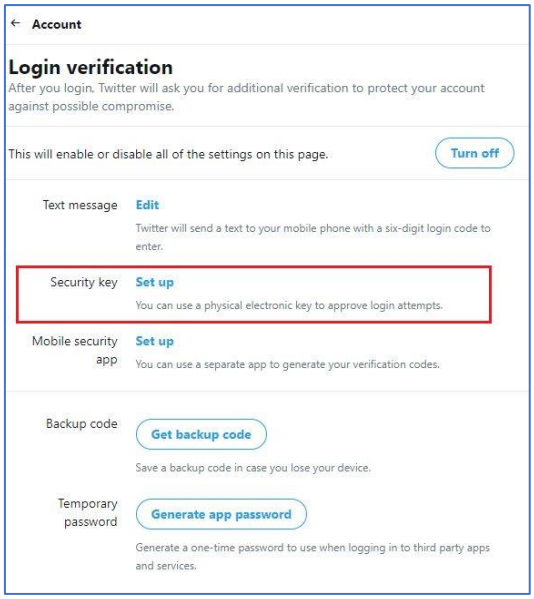
By adding a FEITIAN ePass FIDO, click **Review your login verification methods**.



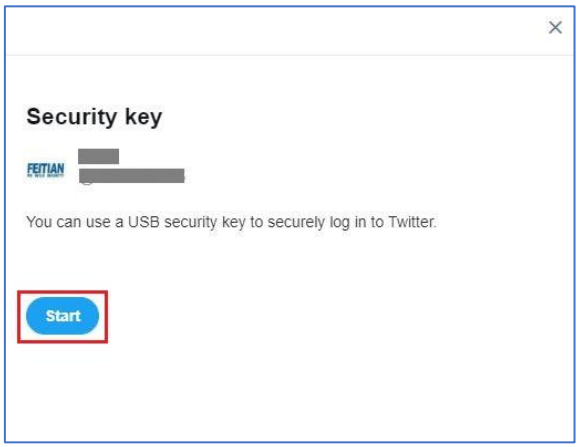
Enter your password and click **Confirm** to continue.



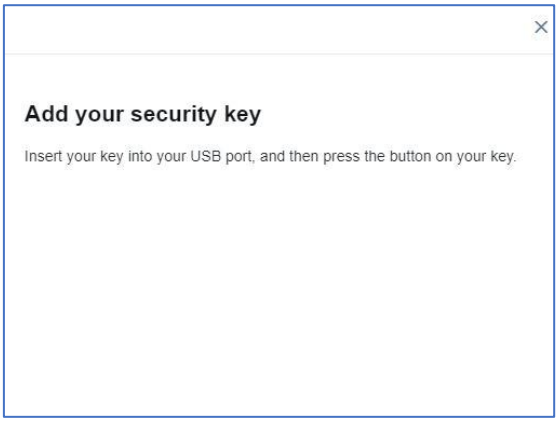
From the selections, click Set up next to **Security key**.

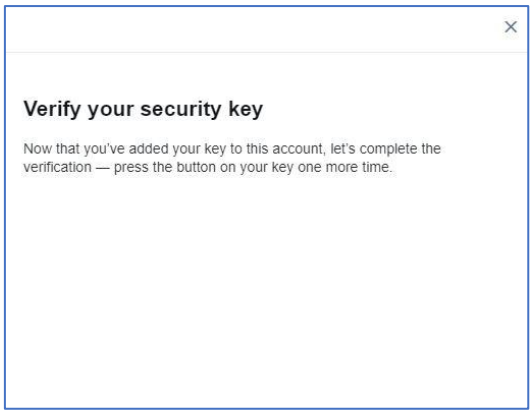


Read the instructions and then click **Start**.

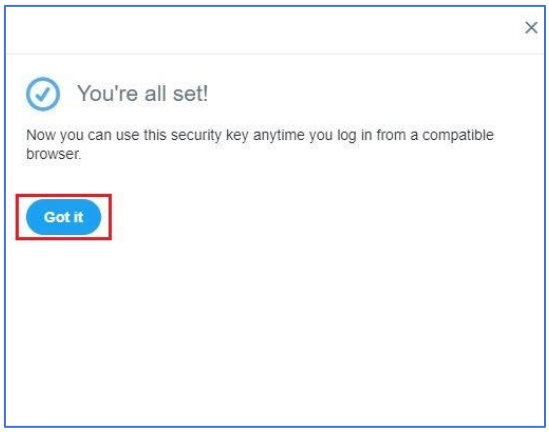


If you're asked to verify your password, enter it and click Verify. Then you will see a pop-up window asking you to register your key by inserting it into your computer's USB port. Once inserted, press the button located on your key. Then verify the key by pressing the button one more time.



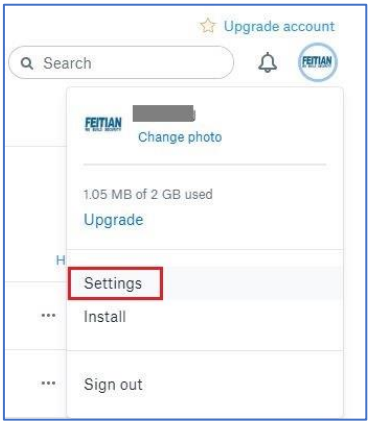


Congratulations! You are ready to use FEITIAN ePass FIDO to authenticate your twitter account.

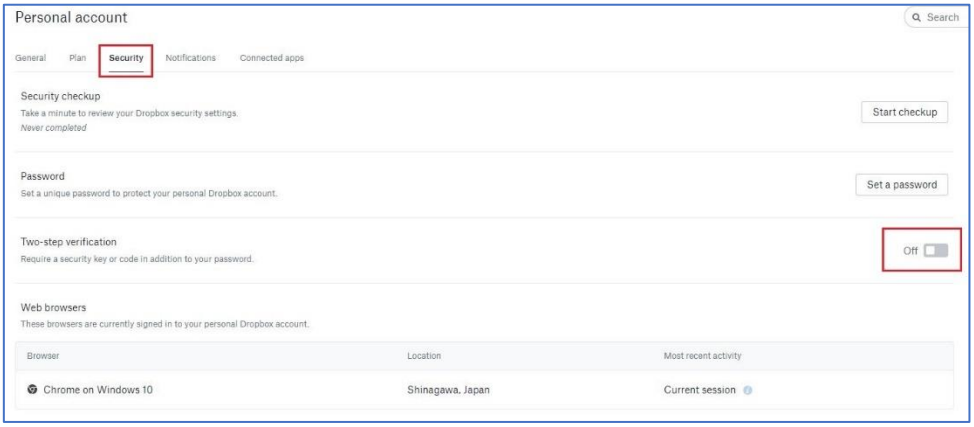


2.4. Dropbox

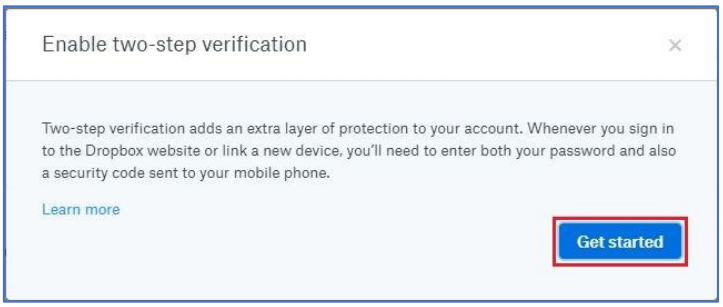
Sign in your Dropbox and go to **Settings** tab.

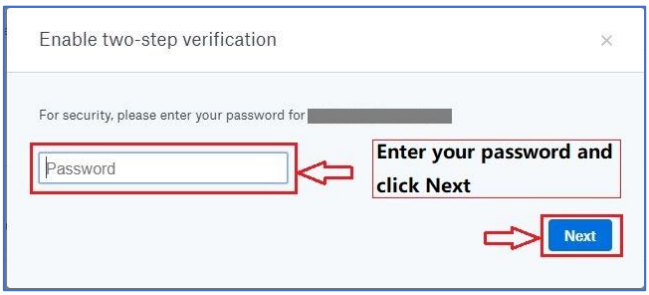


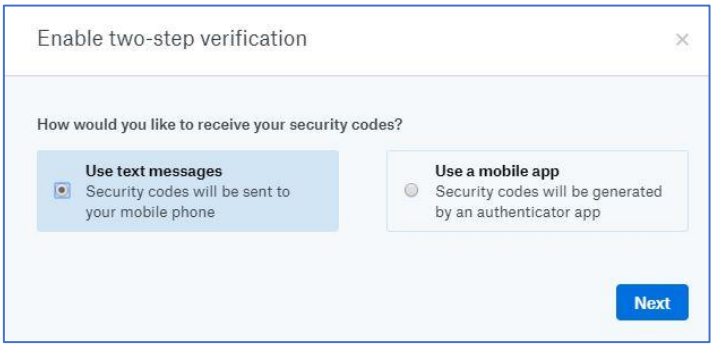
Under **security** tab, click highlighted **Off** to enable Two-step verification.

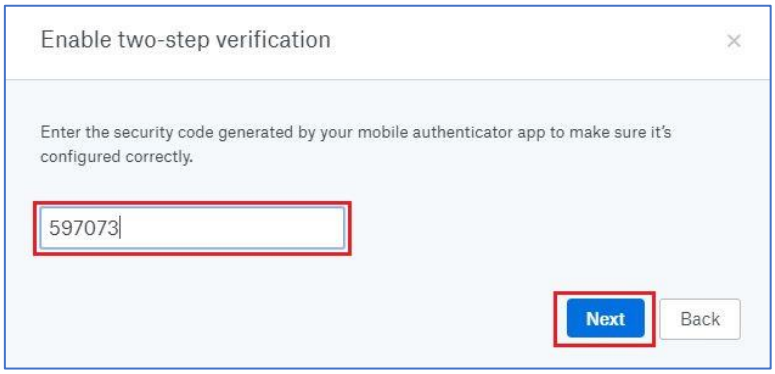


Follow the instructions.

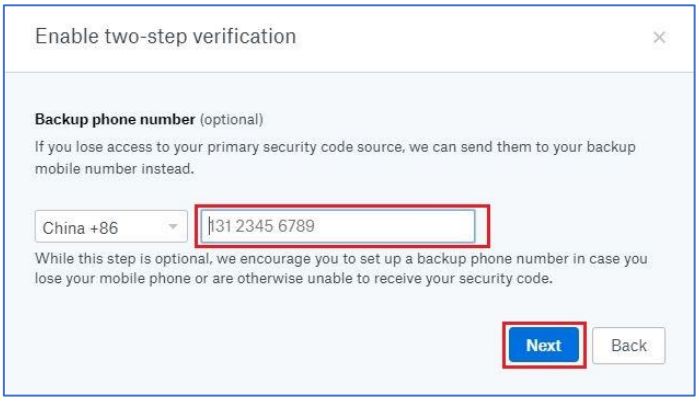




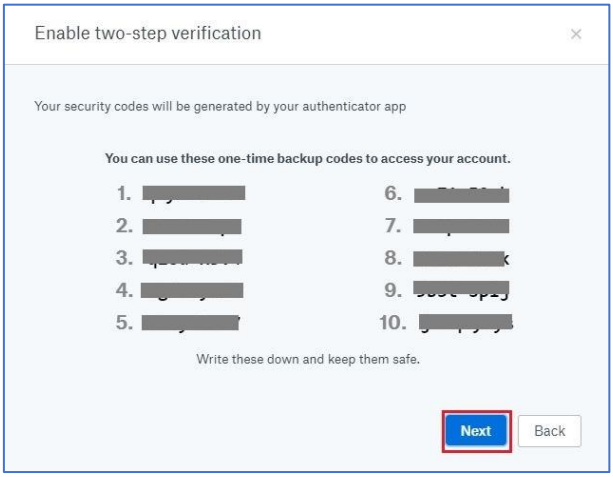




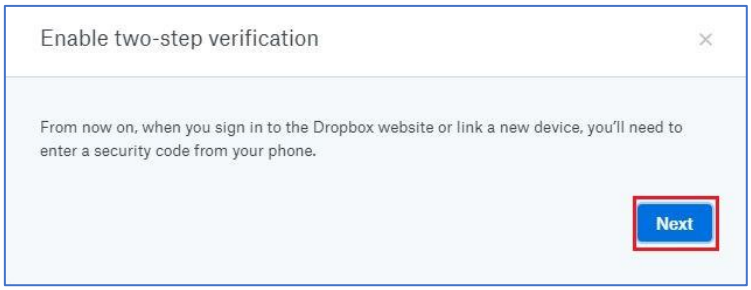
Input a backup phone number. **Note**, this is optional.



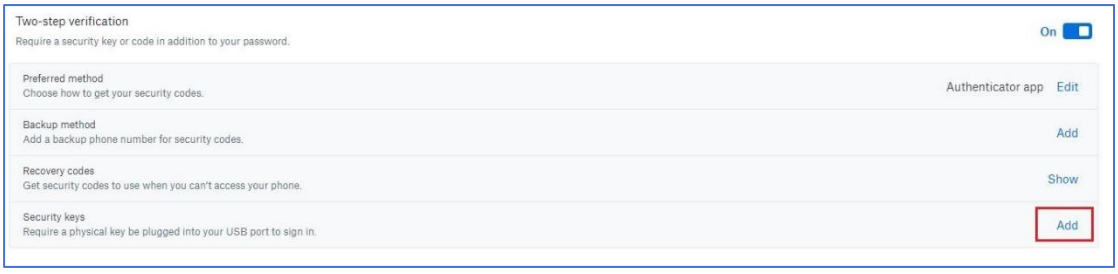
Carefully save the one-time backup codes and click **Next**.



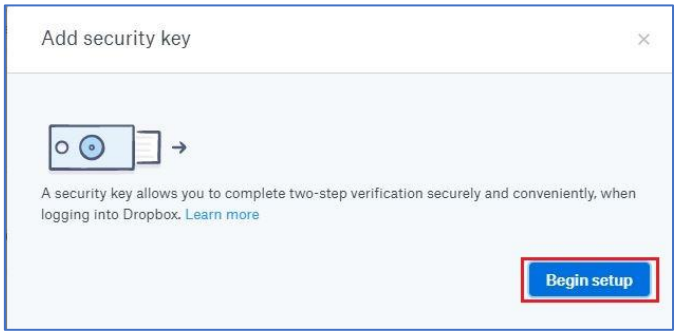
Read the lines and click **Next** and you have successfully enabled the two-step verification.



Register your FEITIAN ePassFIDO.
Click **Add** next to **Security keys** under **Two-step verification** tab.

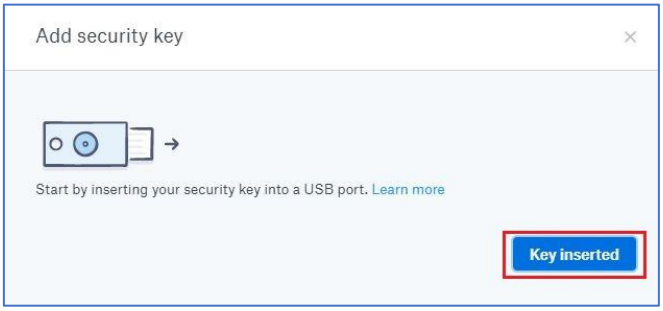


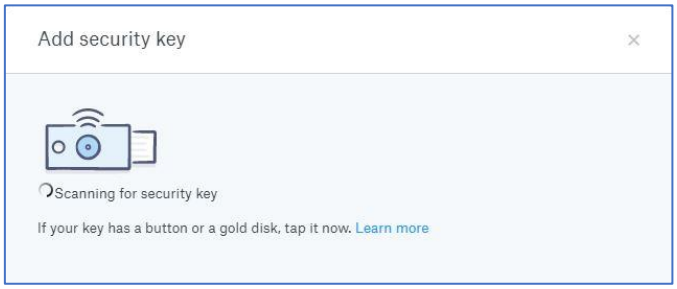
Follow instructions indicated as highlighted part.



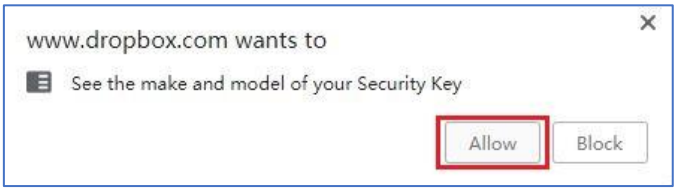
Enter your password and click **Next**.

Insert your FEITIAN ePass FIDO and press it.

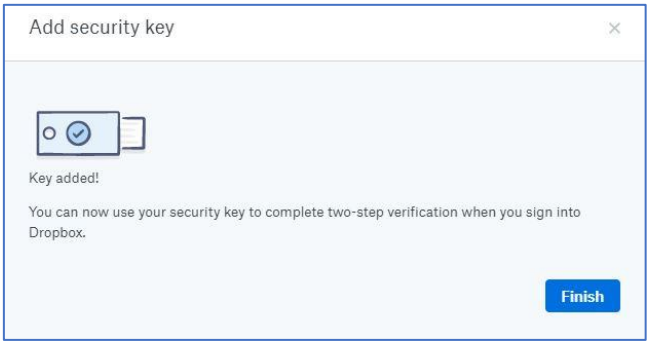




Click **Allow** on the pop-up window.

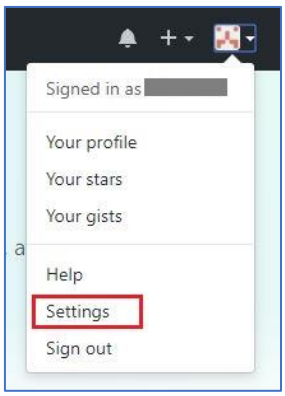


Finally, you have added a security key to your account.

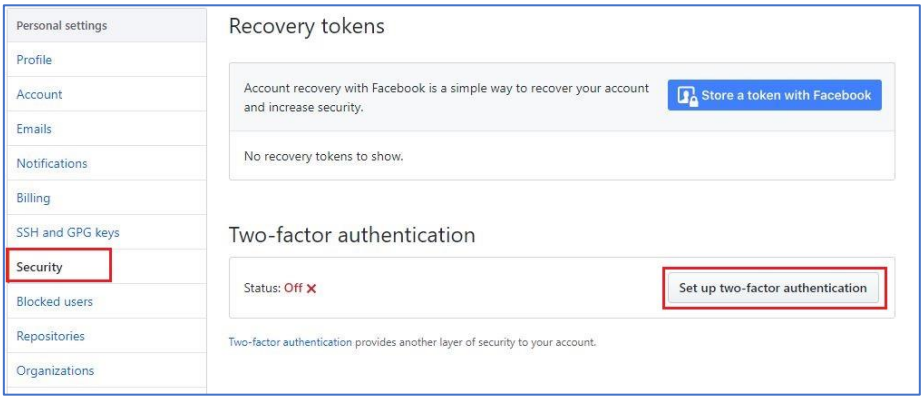


2.5. GitHub

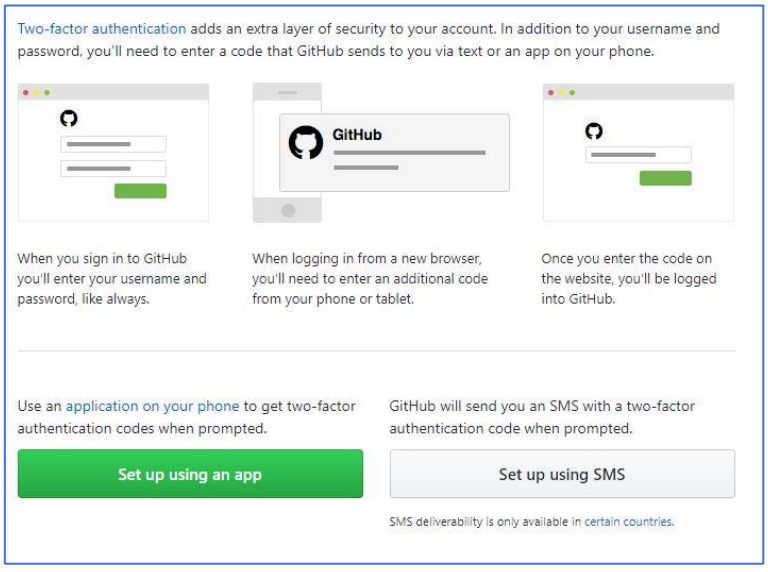
Log in your GitHub account and go to **Settings**.



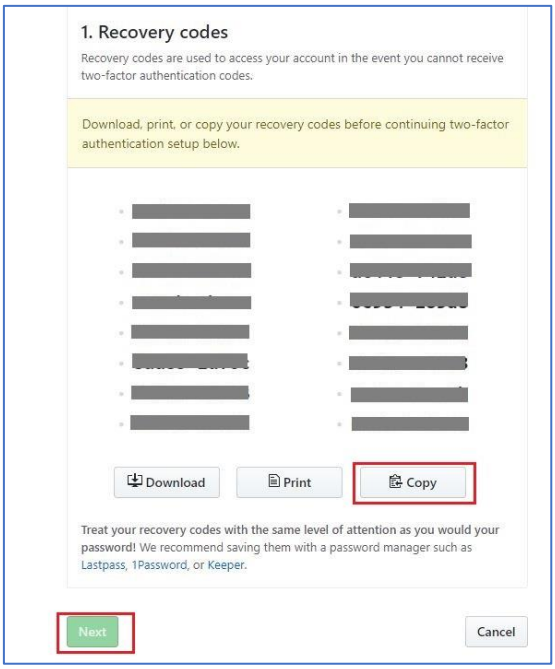
Under **Security** tab, click **Set up two-factor authentication** to enable the feature.



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

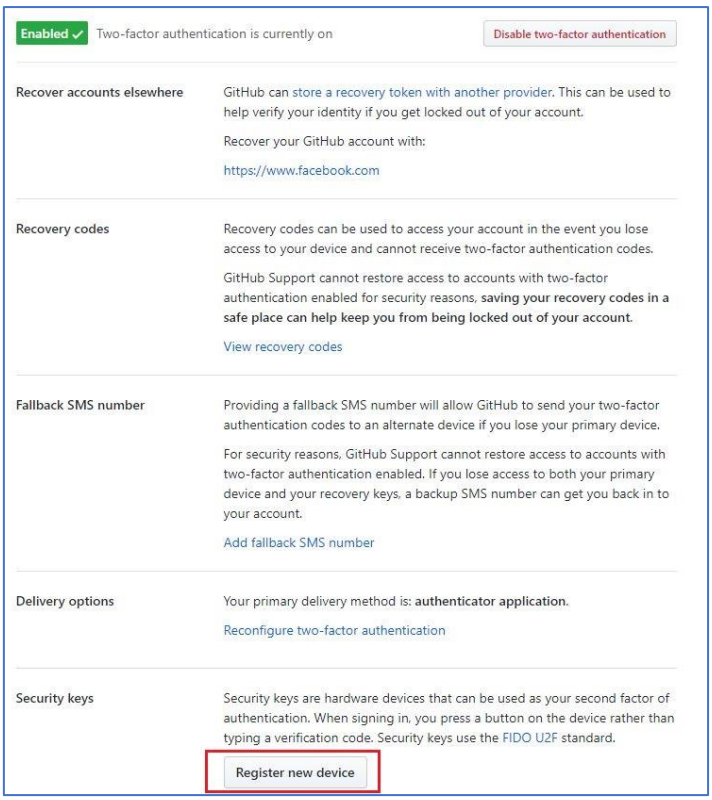


Carefully save the recovery codes and click **Next**.

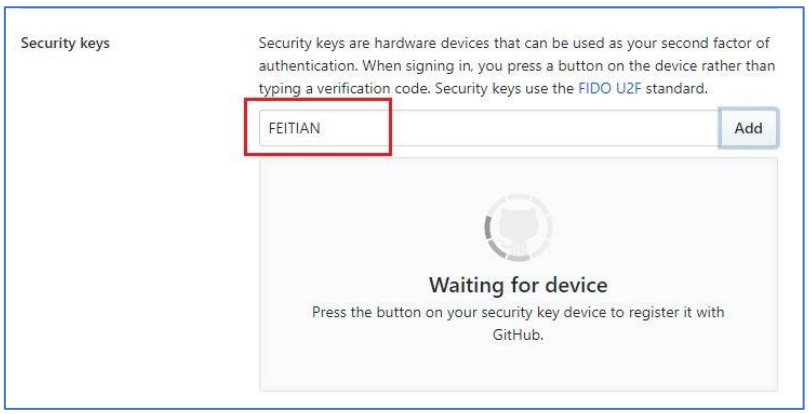


Use your app to scan the QR code and fetch a six-digit code. Input it and click **Enable**.

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

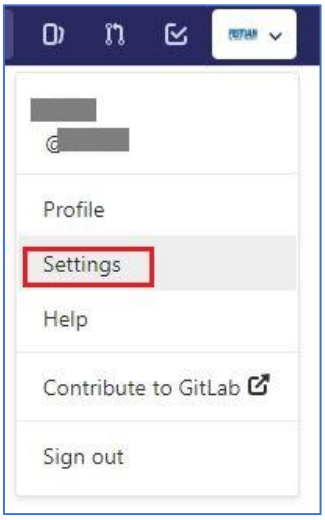


Insert the FEITIAN security key and press it and then you have successfully added a device.

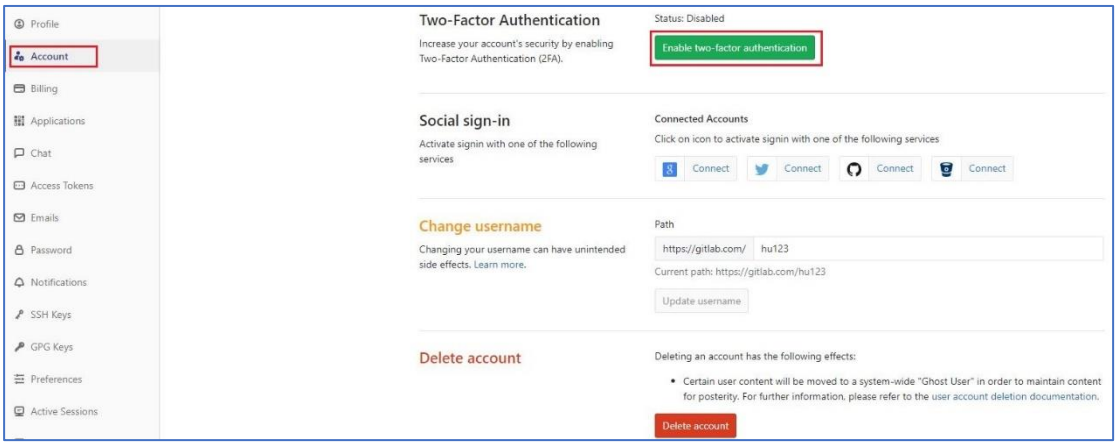


2.6. GitLab

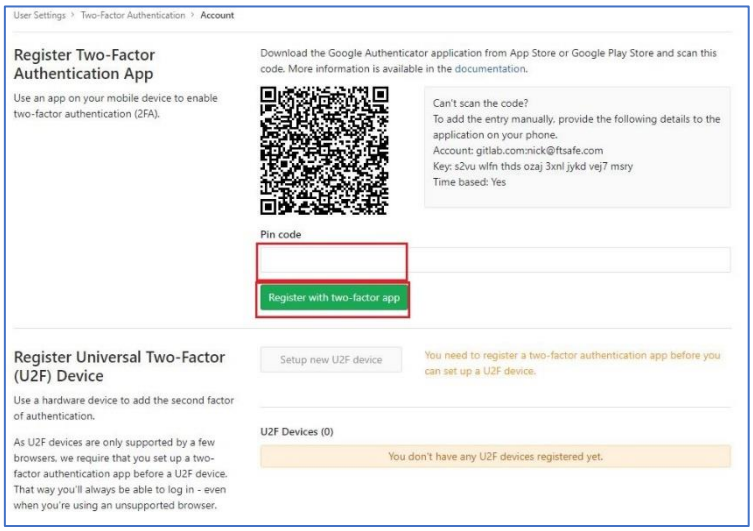
Sign in GitLab account and go to **Settings**.



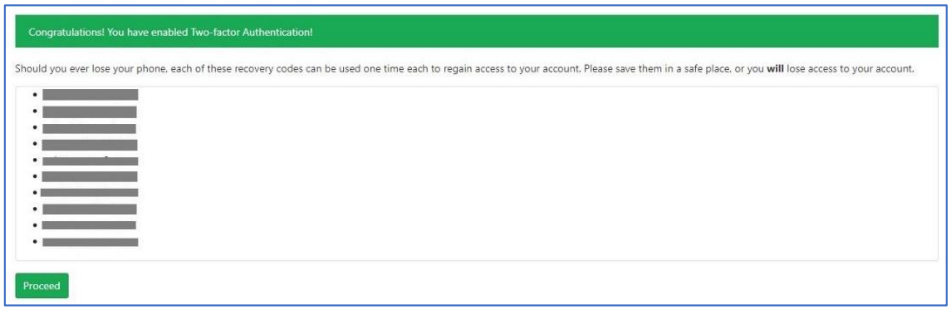
Under **Account** tab, click **Enable two-factor authentication**.



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



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



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

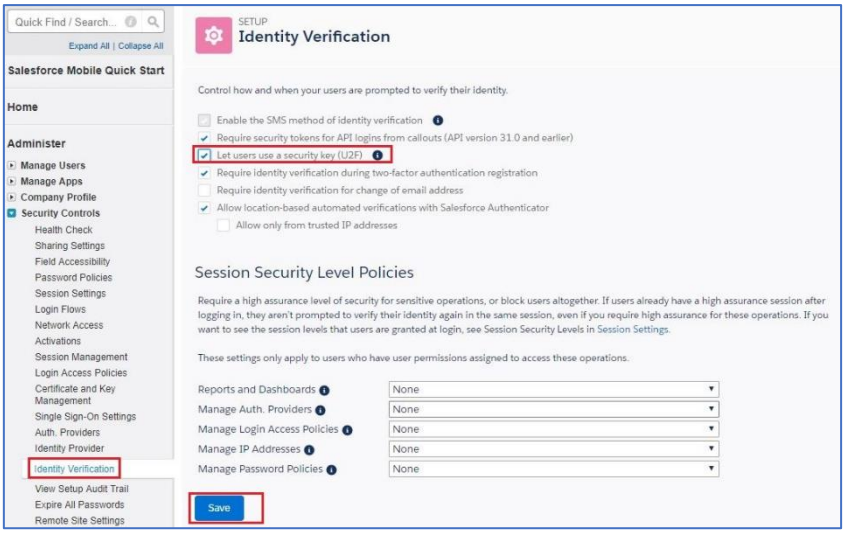
Click **Setup new U2F device** to add the security key.

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

2.7. Salesforce

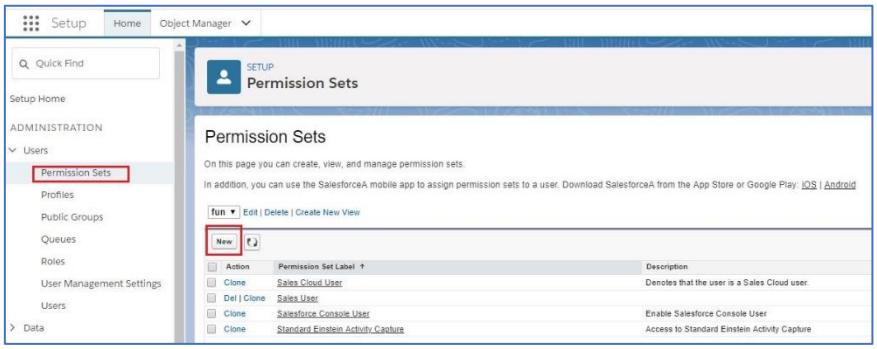
Log in your account and go to **My Domain** tab, click **Deploy to Users**.

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

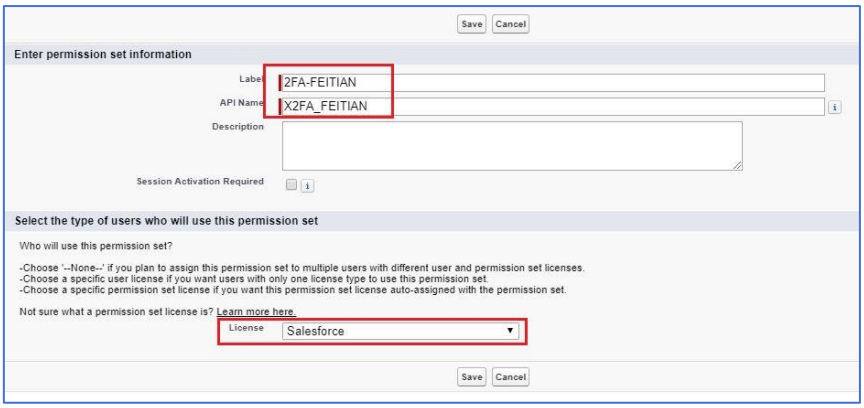


Enable two-factor authentication for users.

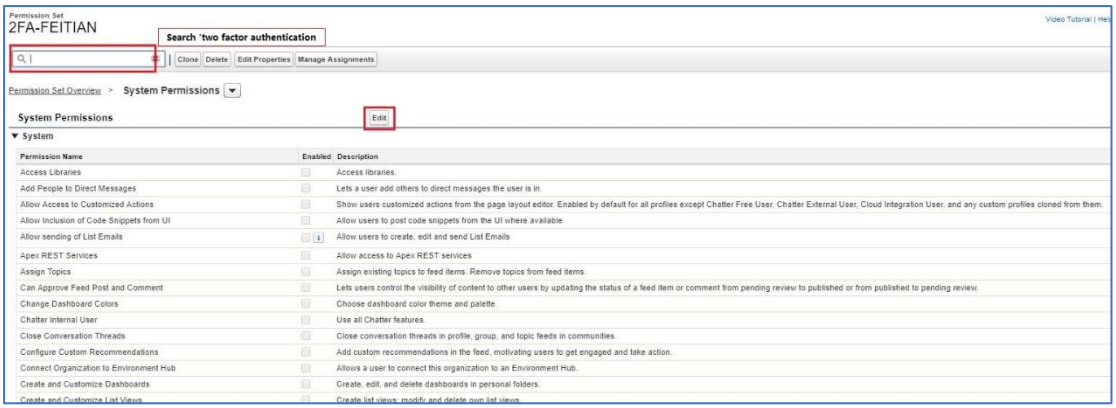
Find **Permission Sets** tab and click **New** button to create a new group.



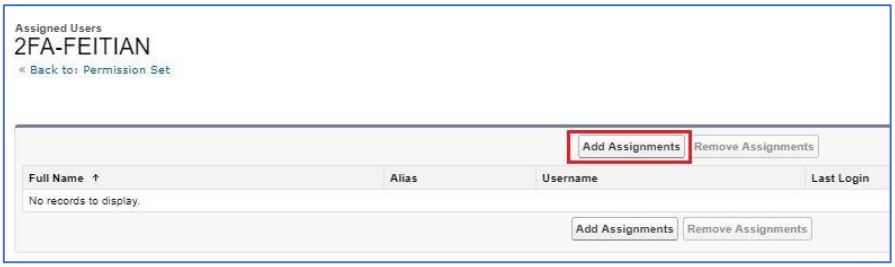
Name it and choose license for it.

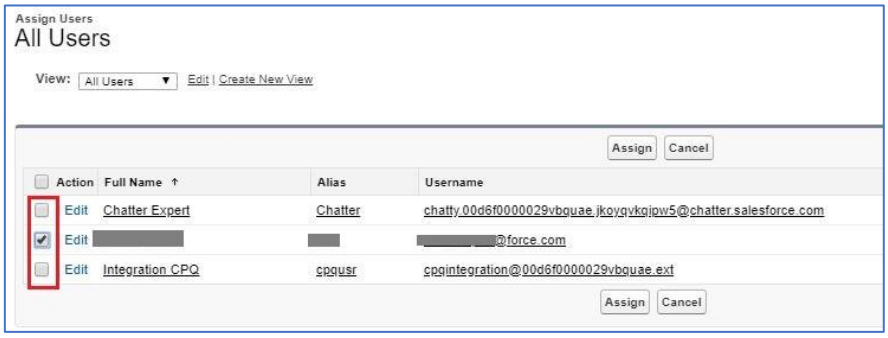


In the next stage, search 'two factor authentication' and locate it. Click **Edit** and scroll down to find and tick it. Scroll up to save the configuration.



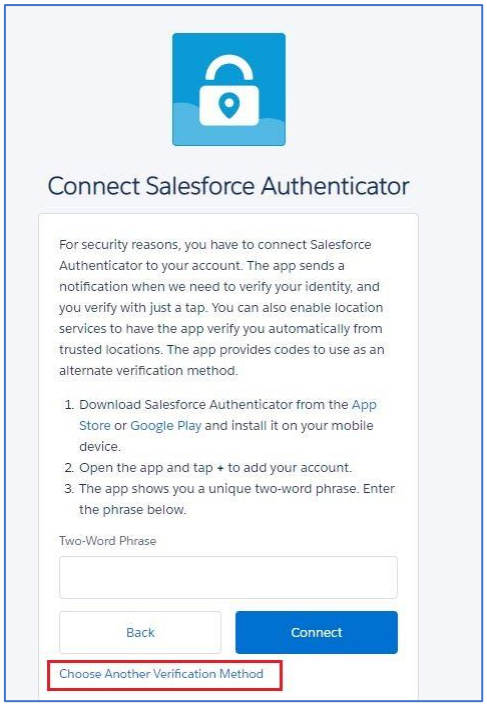
Click Add Assignments to add users who need two-factor authentication.



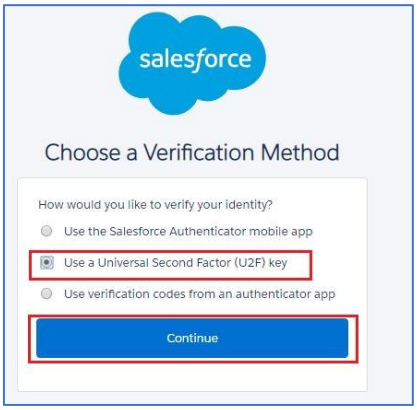


Register a FEITIAN ePass FIDO for your account.

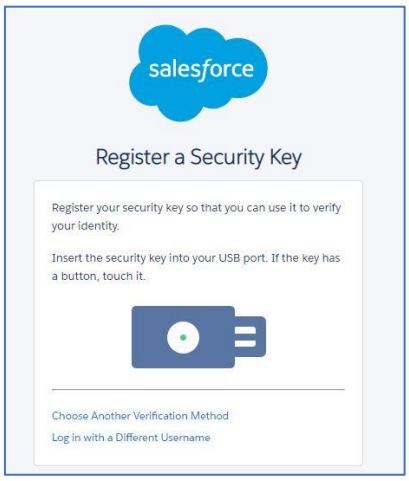
Log out and re-log in your account, a window will pop up. Click **Choose Another Verification Methods**.



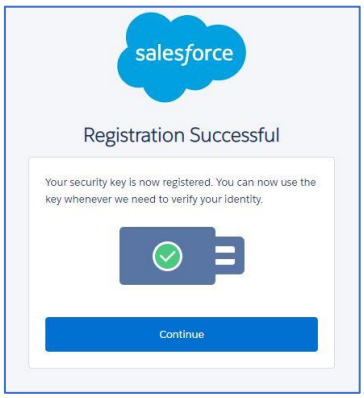
Choose the option of 'use a universal U2F key



Insert your FEITIAN ePass FIDO security key and touch it.

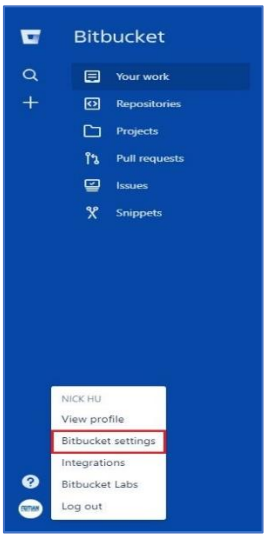


Now, you have successfully registered a security for your account.

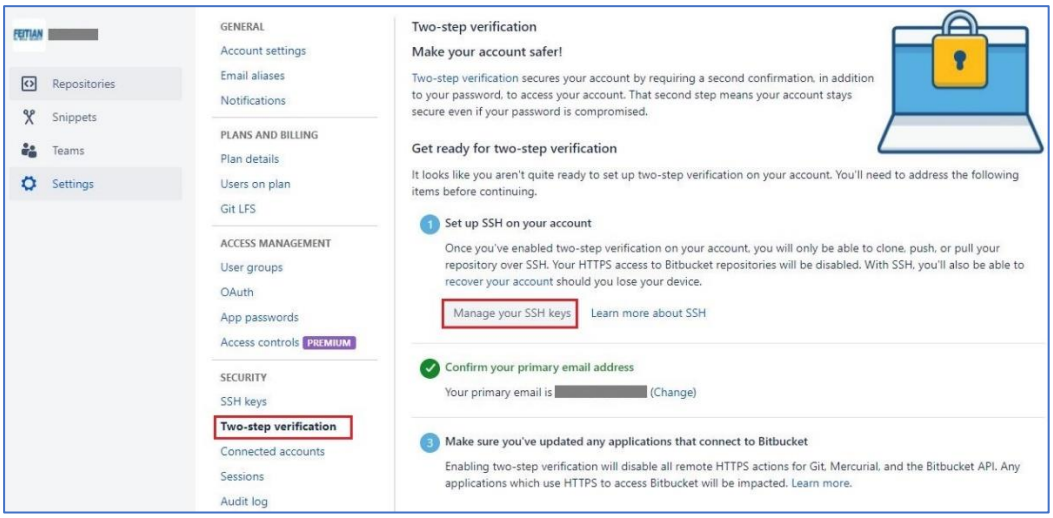


2.8. Bitbucket

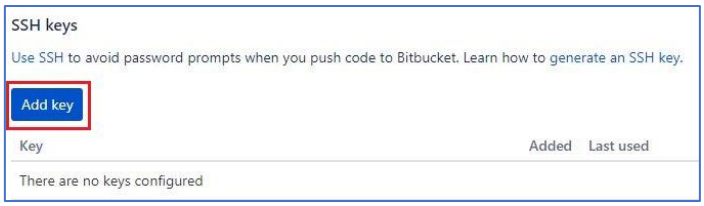
Sign in Bitbucket account and go to **Bitbucket settings**.



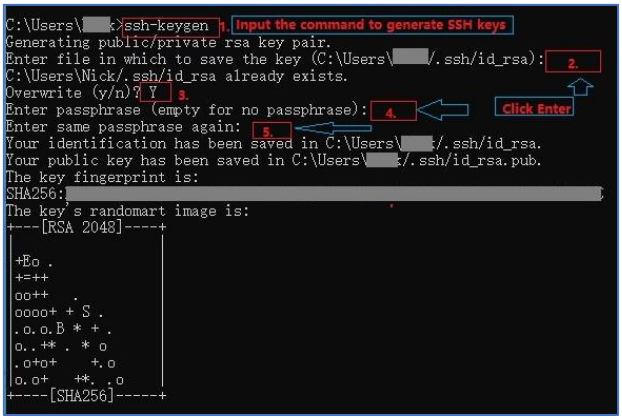
Under **Two-step verification** tab, click **Manage your SSH keys**.
Before you can enable two-factor authentication, Bitbucket requires you to add SSH keys firstly.



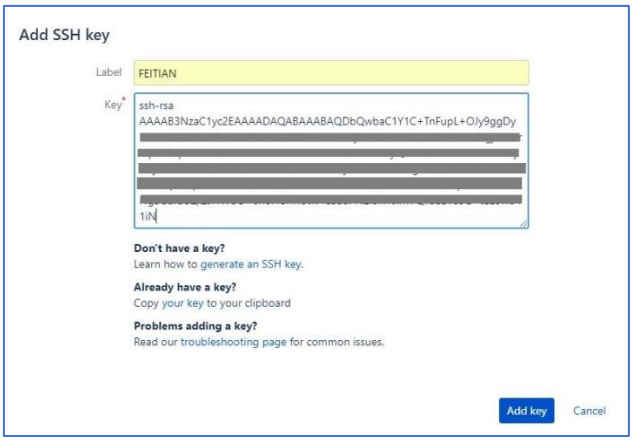
Click **Add key** to get a pup-up window where you can input your key.



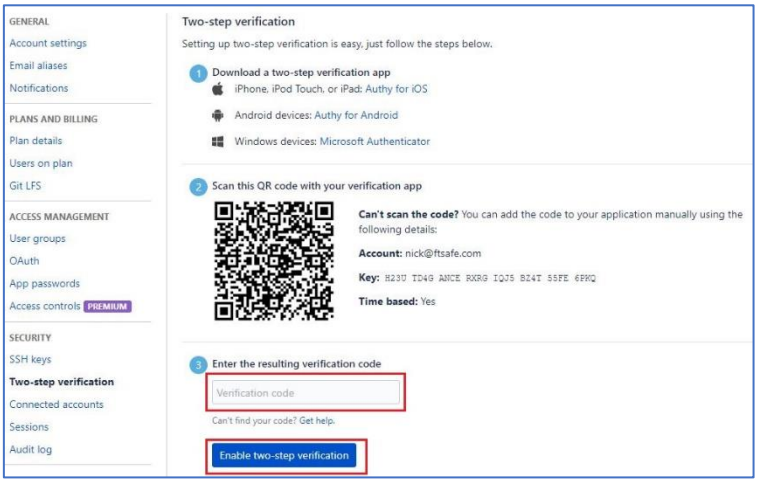
Generate SSH key under windows command prompt.
Follow the instructions as indicated in the picture and you can find your key files in the specific directory.



Name your SSH key and copy public key into pop-up window.

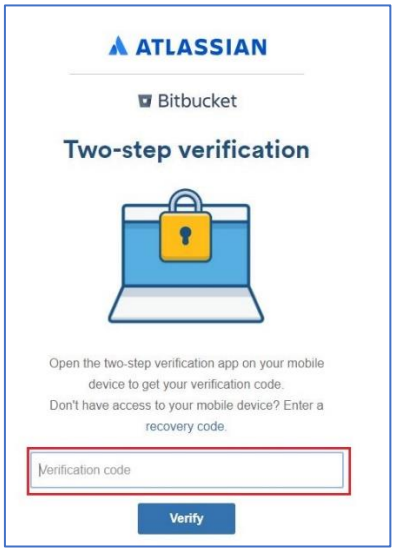


Use your mobile authenticator app to scan the QR code, input it and click **Enable two-step verification**.

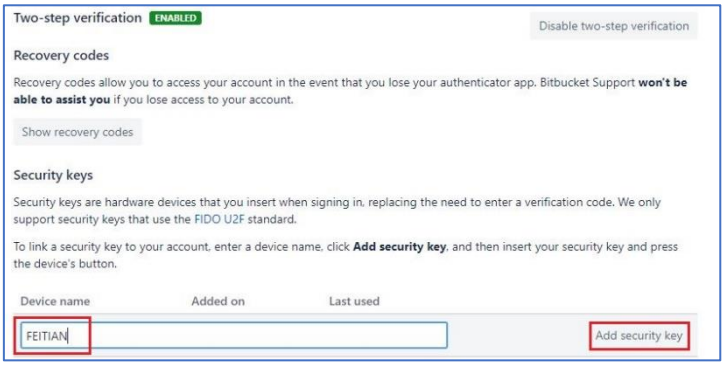


You will get a confirmation letter in our email and click the button.

Re-enter verification code again.



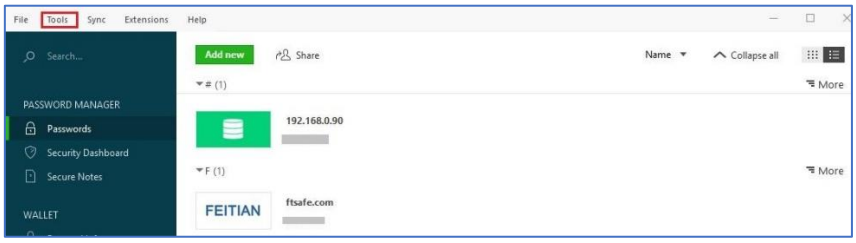
Add FEITIAN ePass FIDO security key. Name it and click **Add security key**.



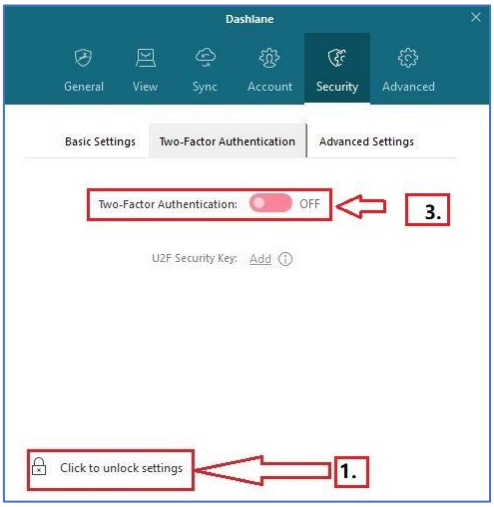
So far, you are ready to try two-step verification in Bitbucket account.

2.9. Dashlane

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



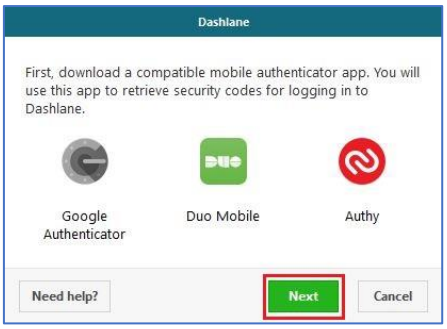
Under **Security** tab, follow the instruction highlighted. Firstly, click **Click to unlock settings**, by doing this, it requires your password showed in step 2. Then click the toolbar next to **OFF**.



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

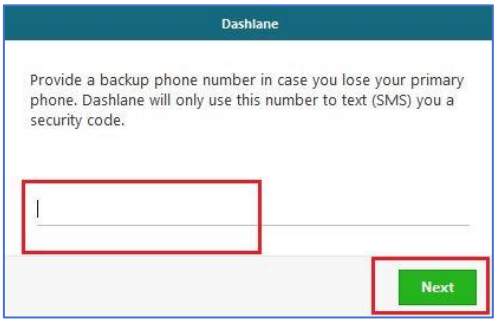
Chose a compatible mobile authenticator app to retrieve security codes and click

Next.

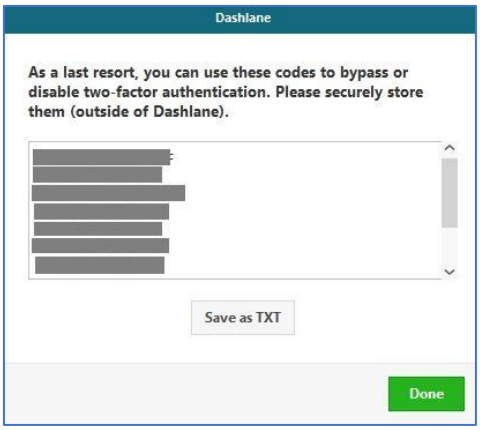


Use the chosen mobile authenticator app to scan the QR bar, input it and click **Next**.

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

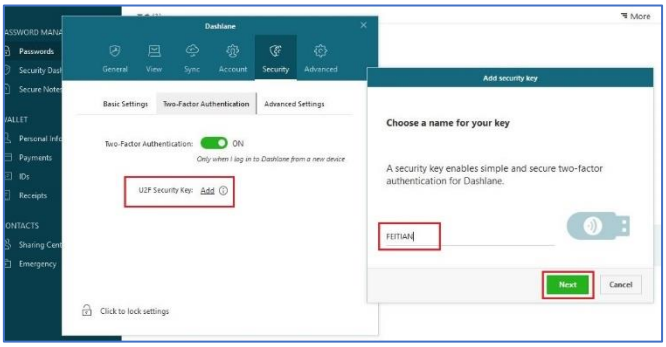


Carefully save the recovery codes and click **Done**.



Register your FEITIAN ePass FIDO.

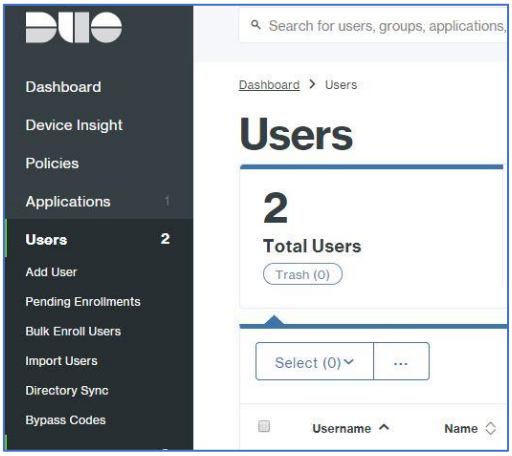
Next to **U2F Security key**, click **Add**. You should name your security key in the pop-up window and click **Next**.



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

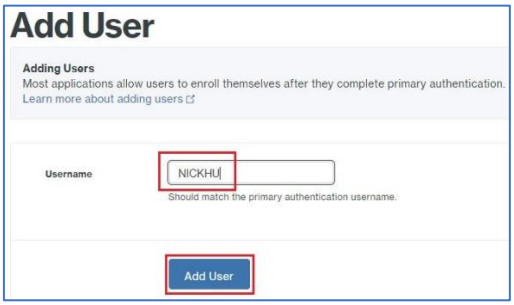
2.10. DUO

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

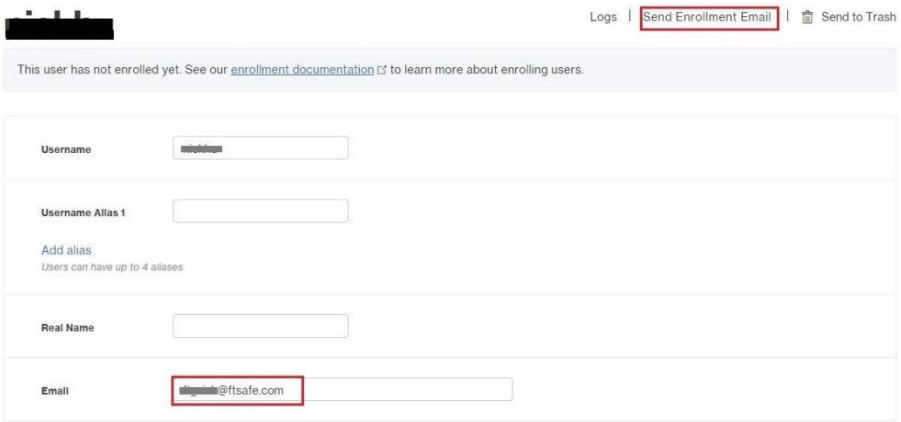


Click **Add User** to enroll a none existing user.

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



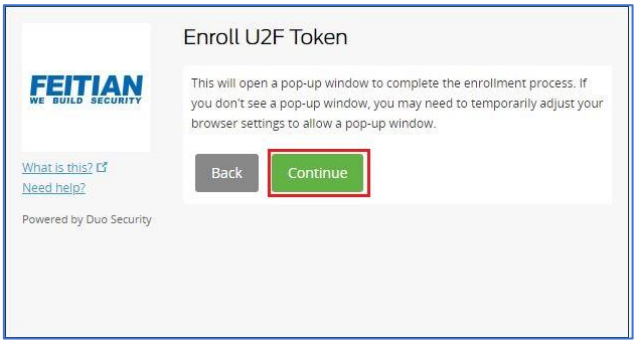
Enter user's email and click **Send Enrollment email**.



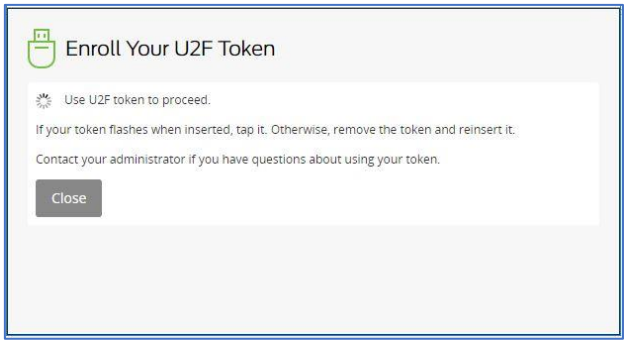
Register FEITIAN ePassFIDO security key.

You may find a link within your email and click it.

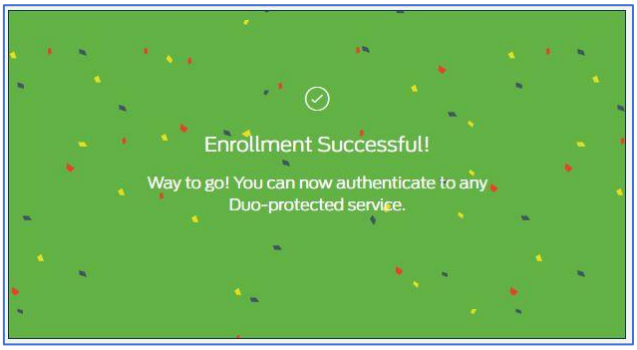
Follow the instructions, click **Start setup**, choose U2F token to continue.



Insert your FEITIAN ePass FIDO token and tap it.

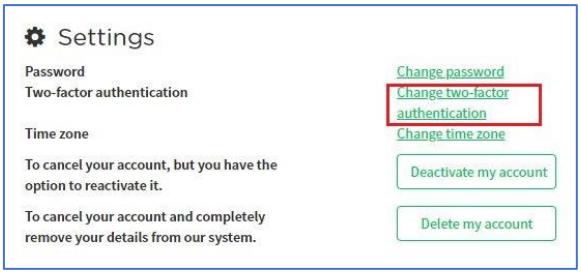


Click **Finish Enrollment** to complete the registration.

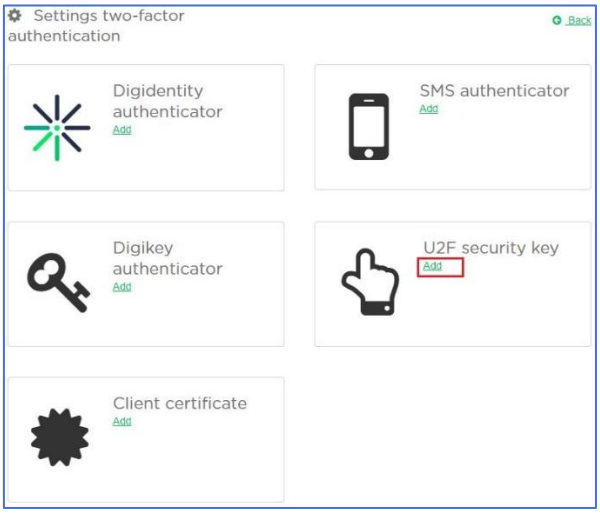


2.11. Digidentity

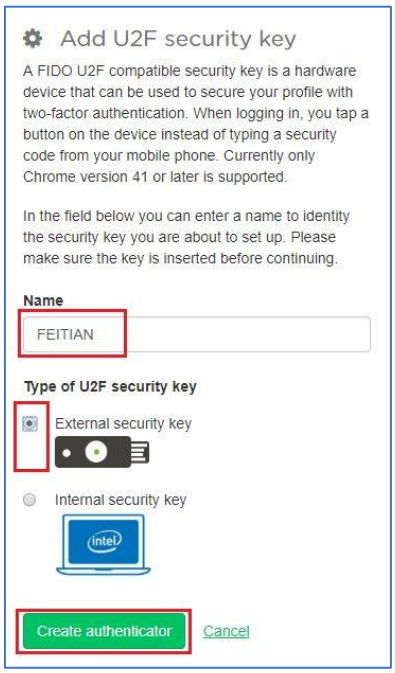
Log in Digidentity account and go to **Settings**. And click Change **two-factor authentication**.



Click Add under U2F security key.



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

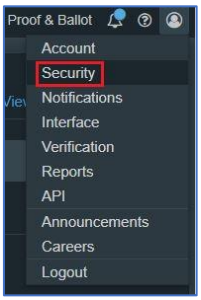


Follow instructions to insert FEITIAN ePass FIDO and tap it.

You have finish registration and ready to go!

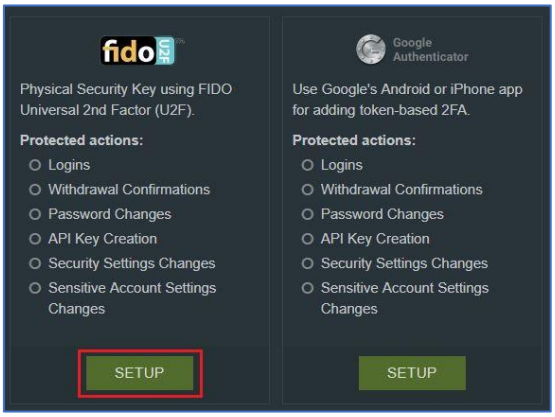
2.12. BITFINEX

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



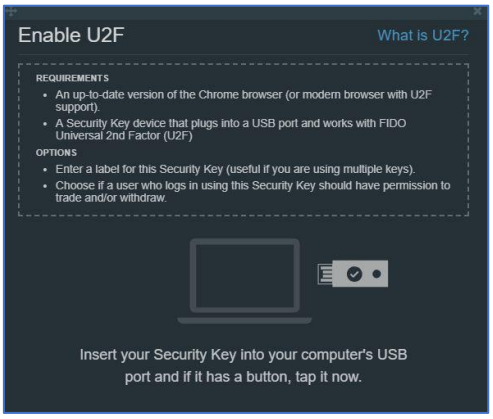
Click **two-factor authentication**.

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

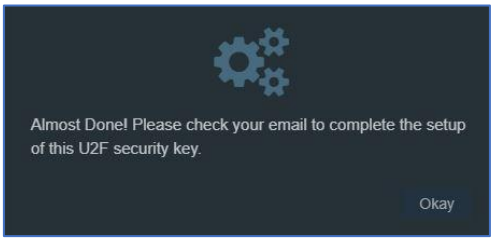


Name your FEITIAN ePass FIDO and click **Click here** to start registration.

Insert your security key as indicated and press it.

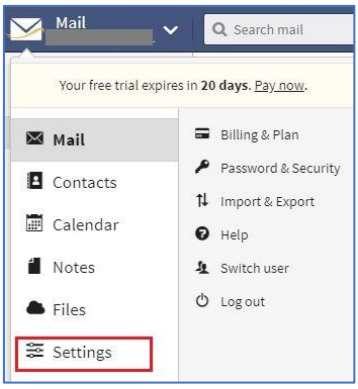


A notification email will be sent to you, and you need to go to your email and click **ACTIVATE U2F 2FA NOW** to finish registration.

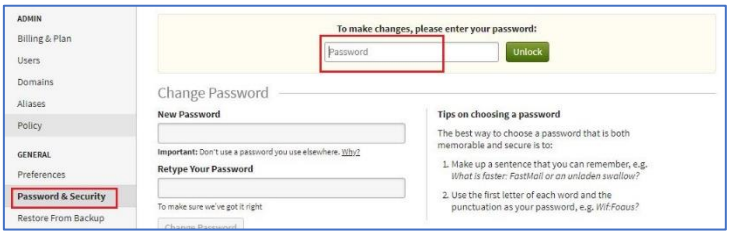


2.13. FastMail

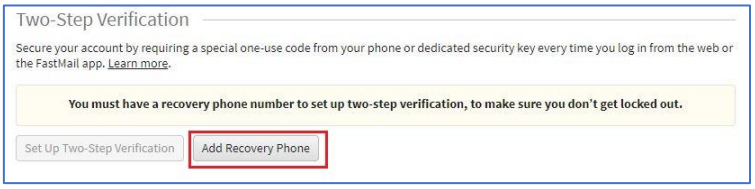
Sign in your Fastmail account and go to **Settings**.



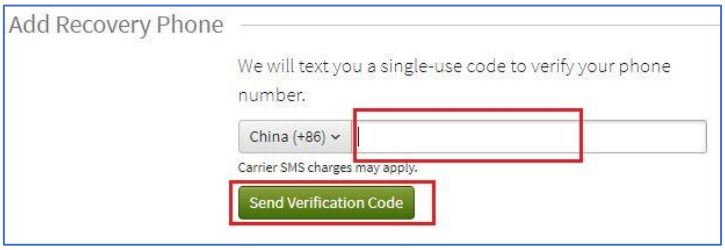
Under **Password & Security** tab, you need to input your password to unlock the functions.



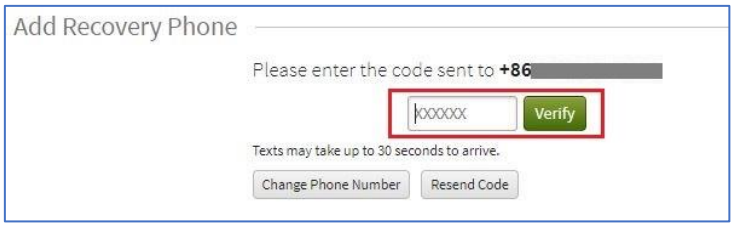
Before you enable the two-step verification, it requires you to add a recovery phone if you do not have one.



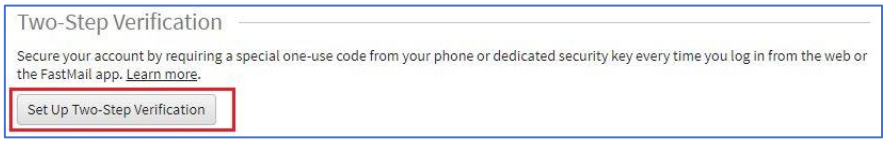
Input your phone number and click **Send Verification Code**.



Input the codes you received.

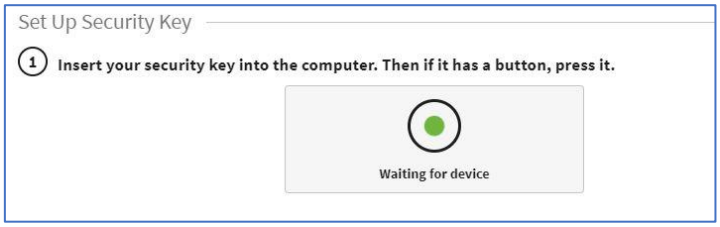


Now you are able to do the enable operation. Click **Set Up Two-Step Verification**.



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

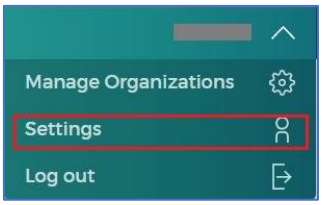
Insert your FEITIAN ePass FIDO as indicated and touch it.



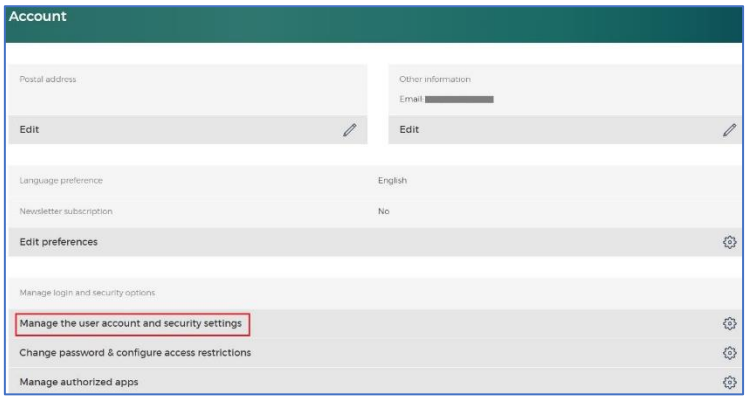
Name your security and save it. You are ready to go!

2.14. Gandi.net

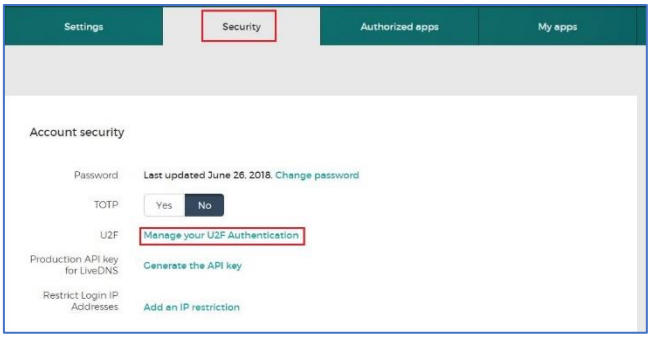
Log in your account and go to Settings.



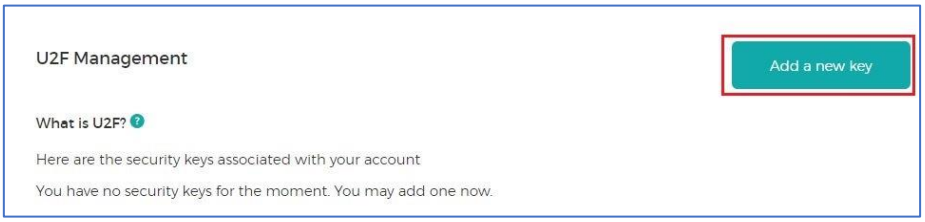
Click **Manage the user account and security settings**.



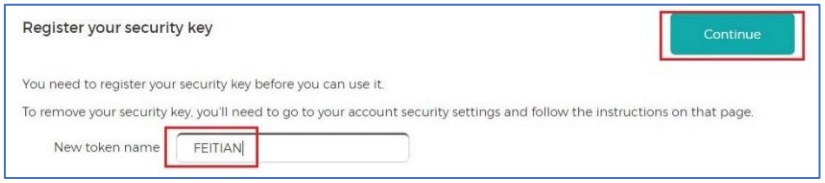
Under Security tab, click **Manage your U2F Authentication**.



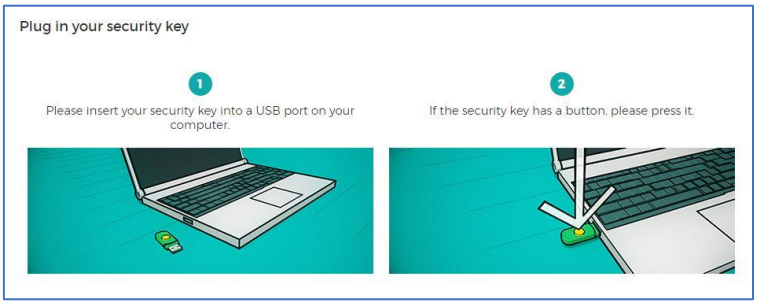
Register your FEITIAN ePass FIDO security key by click **Add a new key**.



Name your security key and continue.



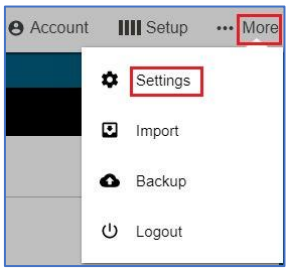
Insert and press the external hardware key as indicated.



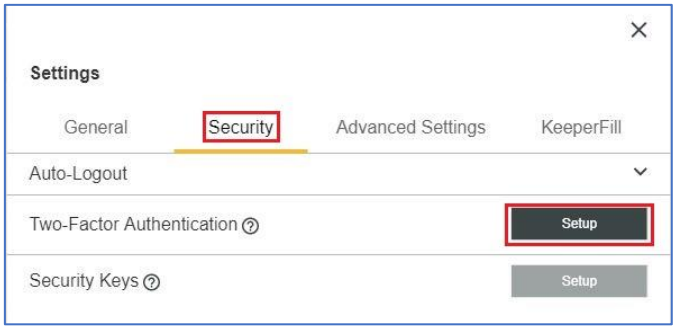
You have successfully registered a FEITIAN ePass FIDO and ready to try out.

2.15. Keeper

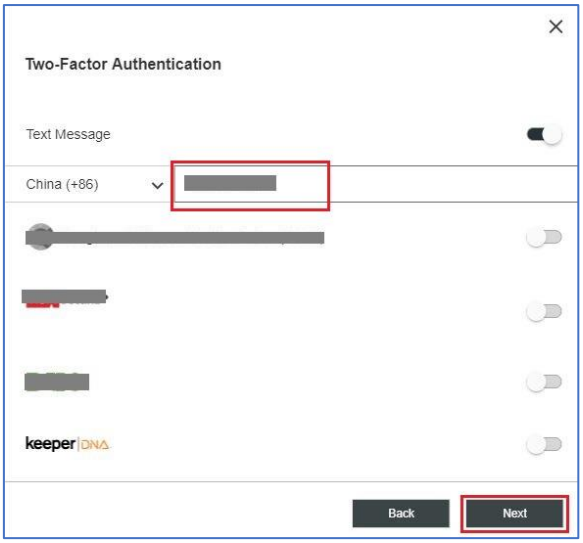
Log in your account and go to **More/Settings**.



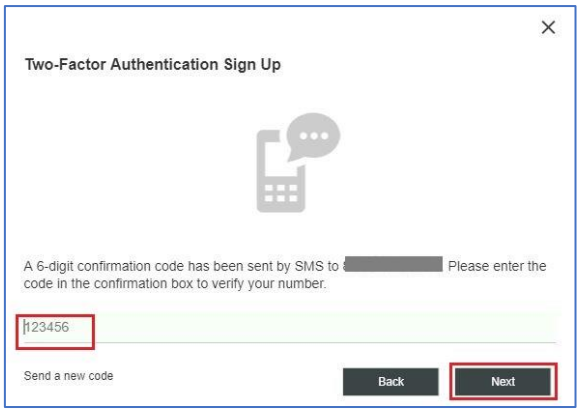
Under **Security** tab, click **Setup** next to **Two-Factor Authentication**.



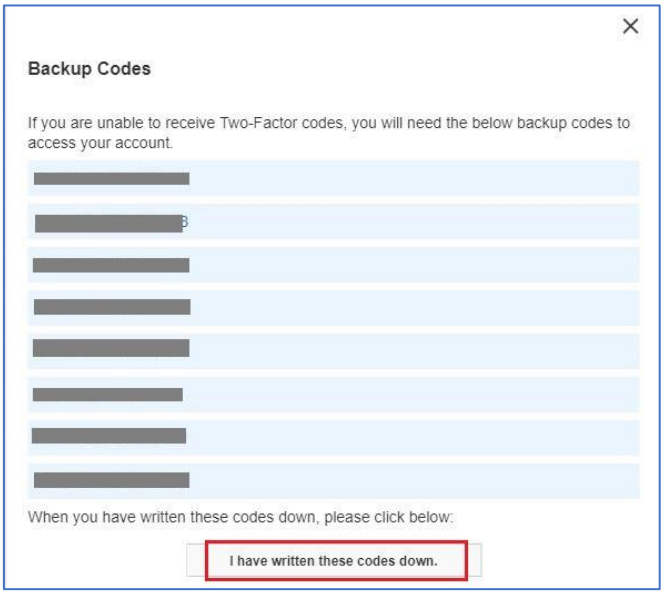
Input your phone number and click **Next**.



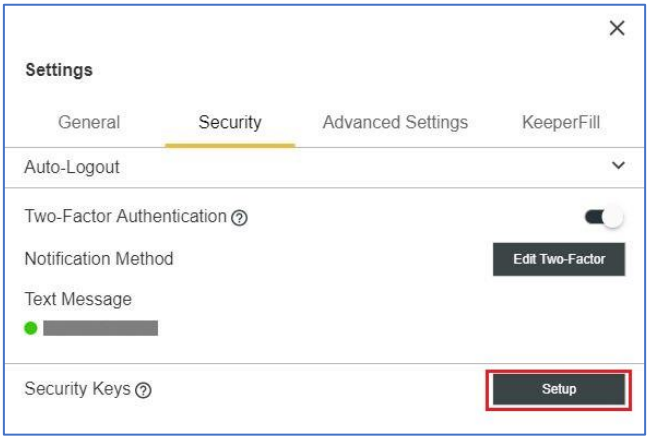
Enter code you received and click **Next**.



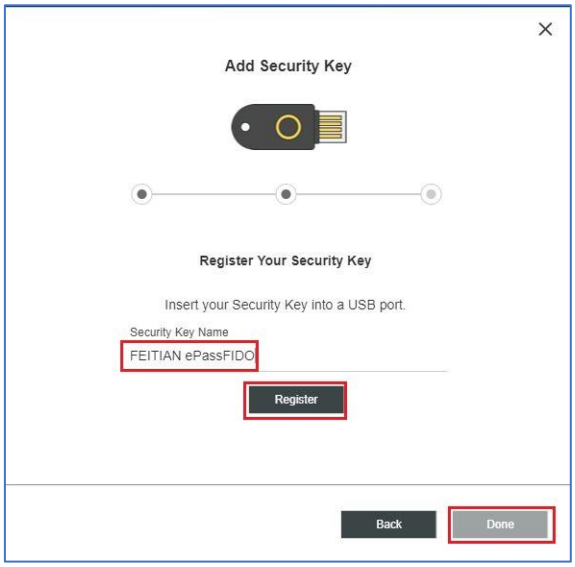
Carefully save the backup codes.



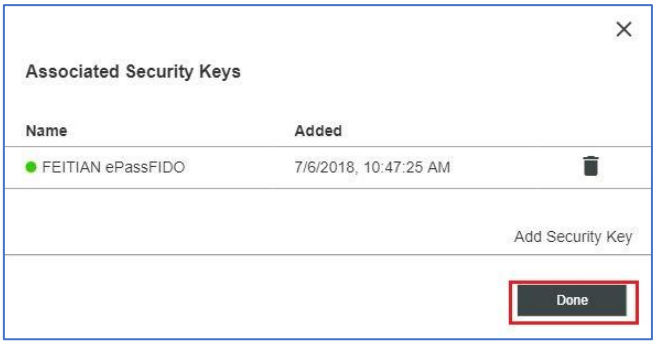
Register your security key by clicking **Setup** next to **Security Keys**.



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

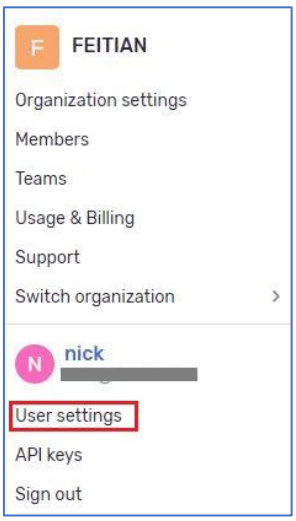


Now you have already successfully registered the security.

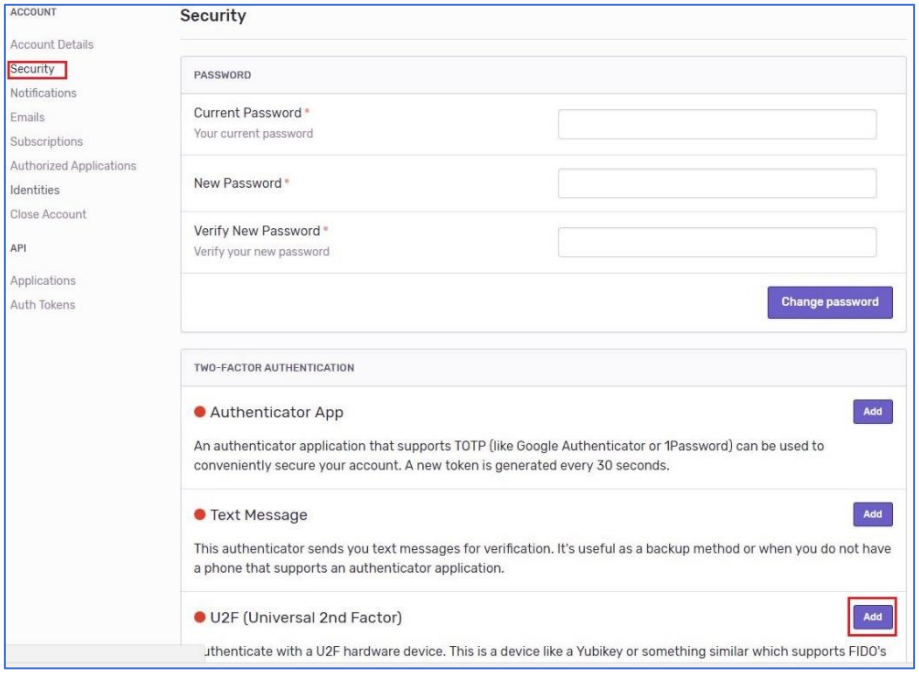


2.16. Sentry

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

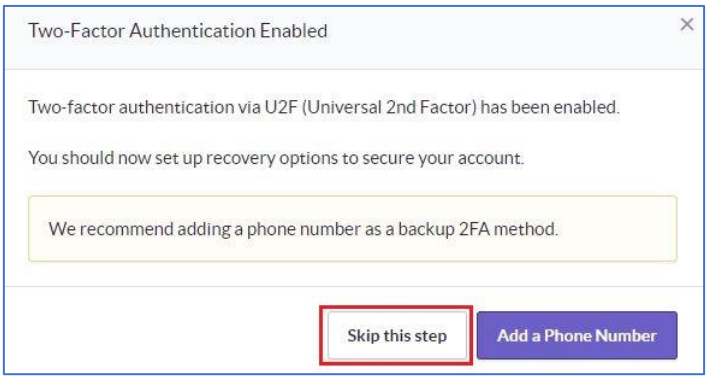


Under **Security** tab, click Add next to **U2F (Universal 2nd Factor)**.

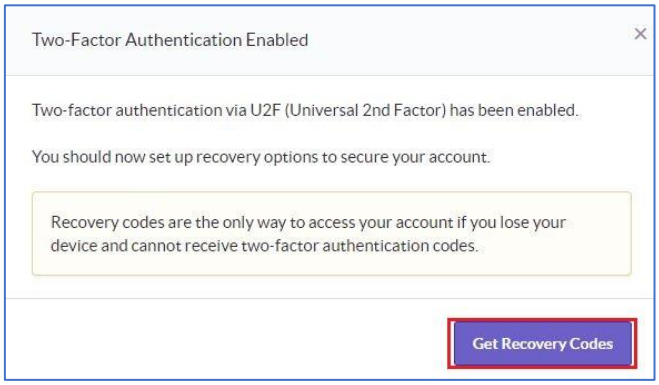


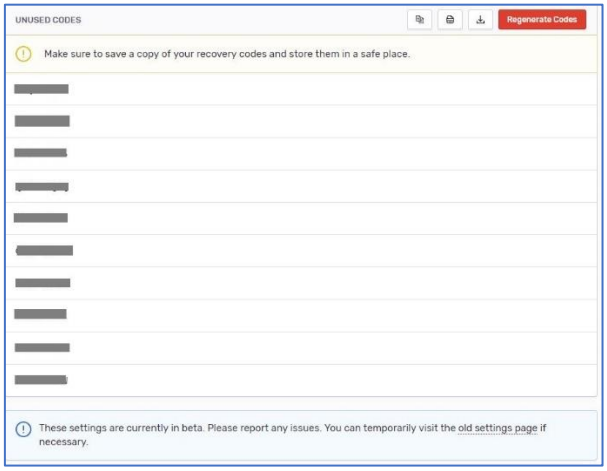
Name your security key and press it.

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



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



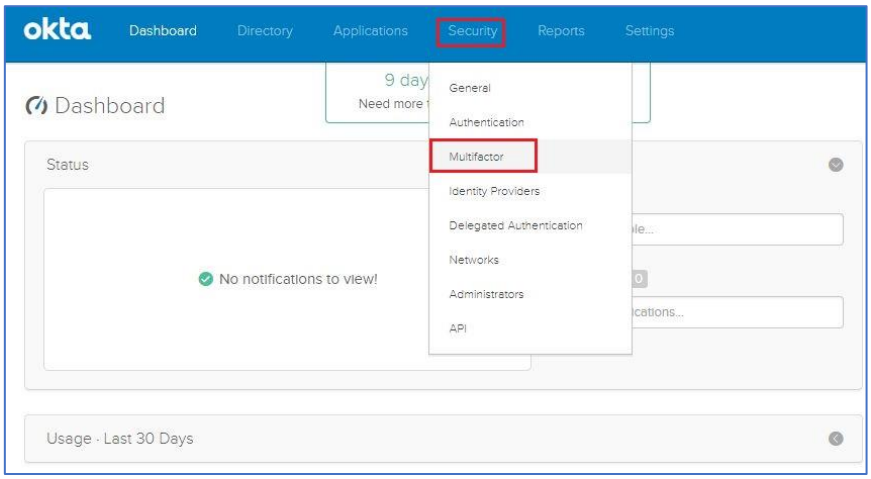


Finally, you have added a security to your account as a second authentication factor.

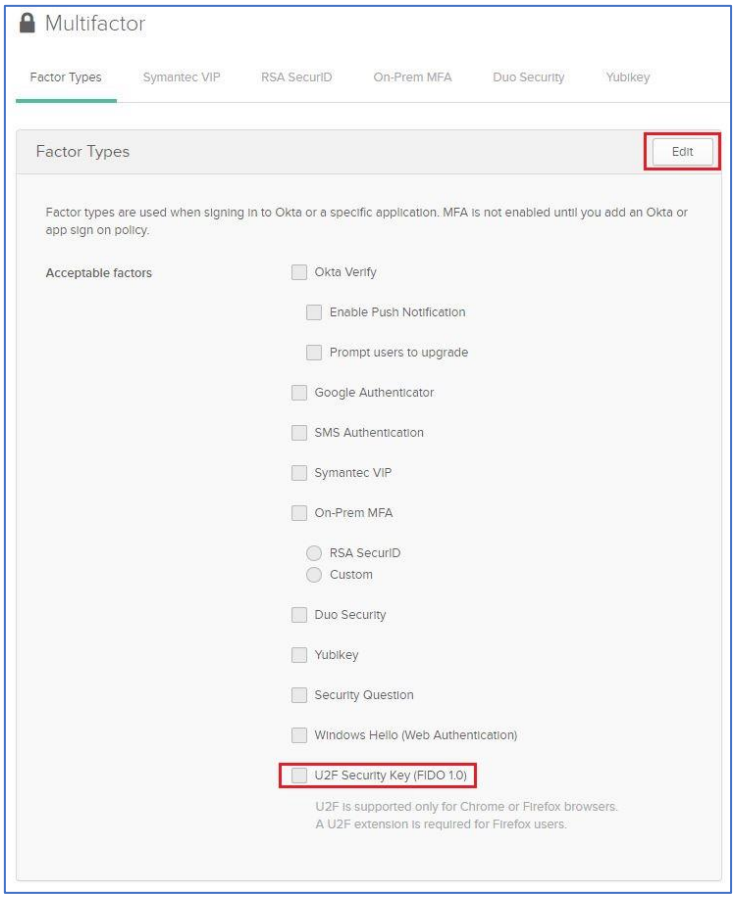
2.17. Okta

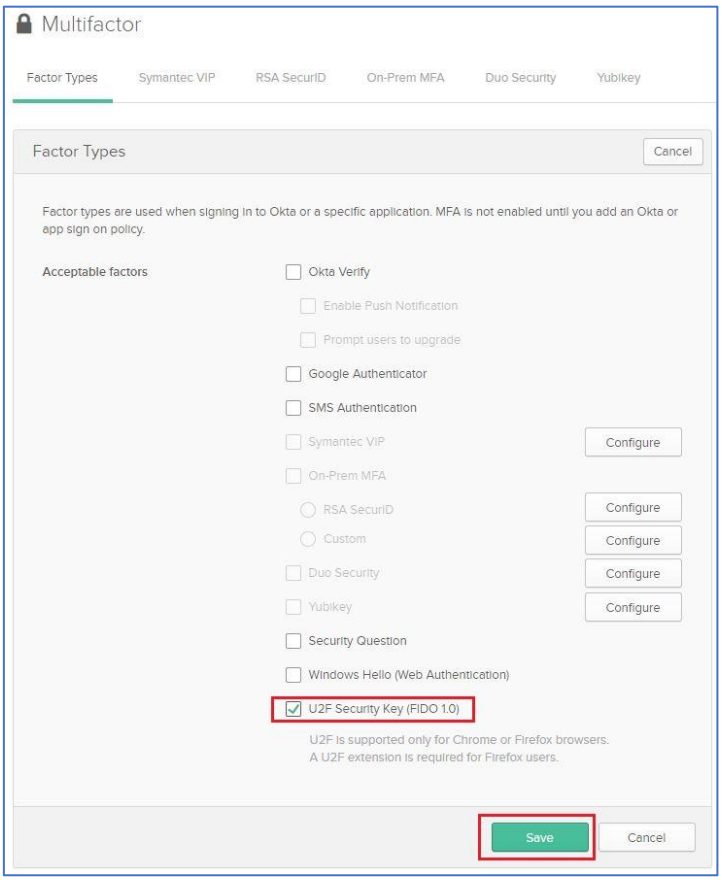
Contact Okta support to enable U2F feature as it is not default enabled.
Login your Okta account and click **Admin**.

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

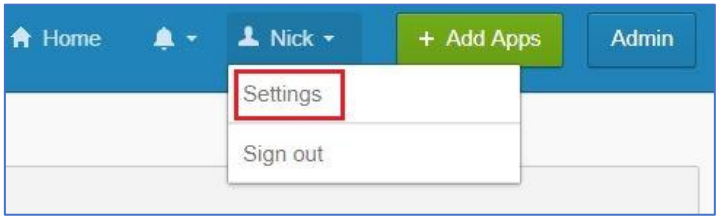


Click **Edit** button, tick **U2F security key** and save it.

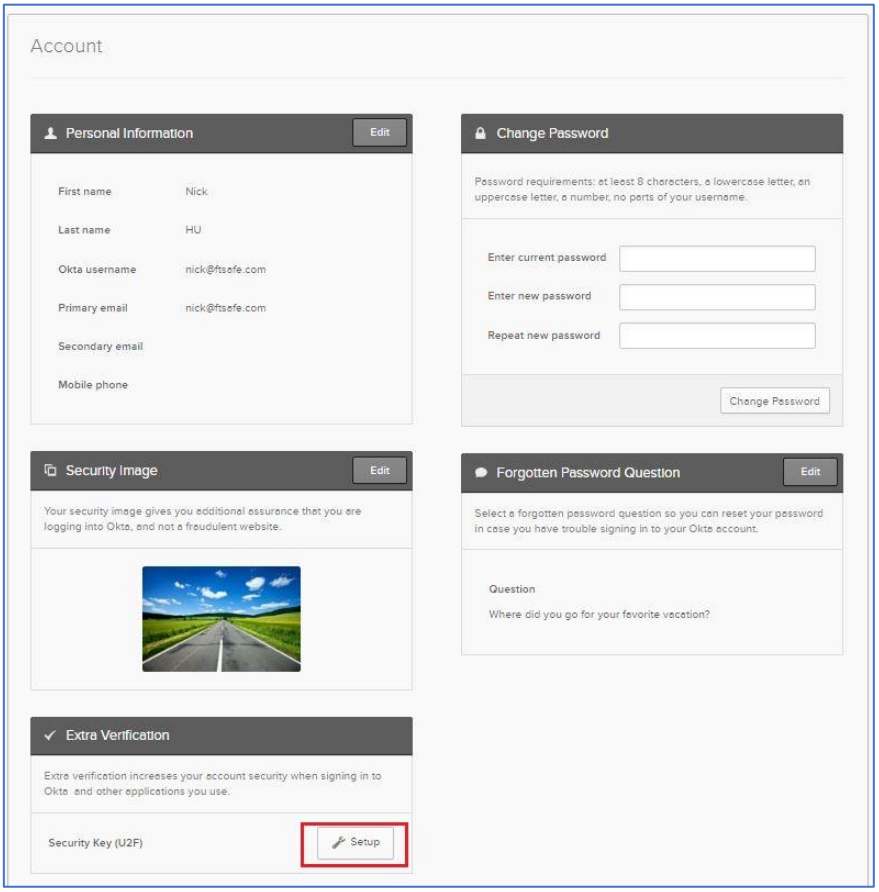




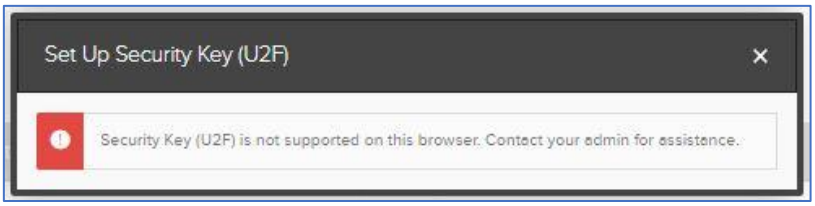
Re-login and go to **Settings**.



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



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



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)
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.

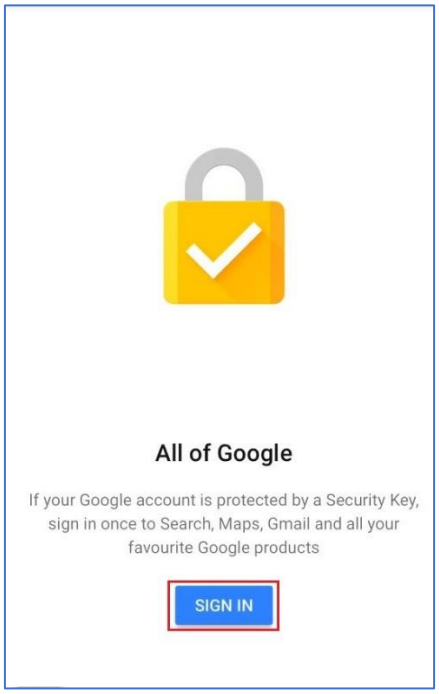
3.1. IOS platform

3.1.1. Google account

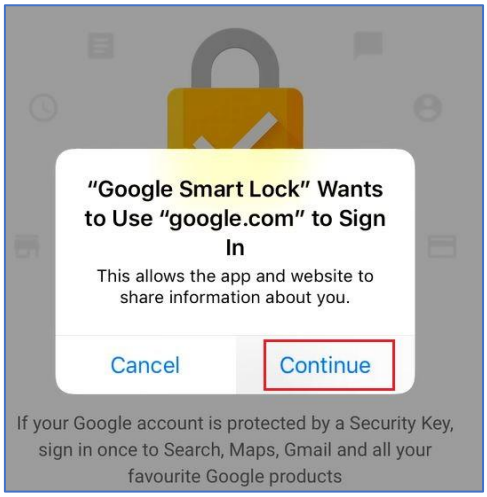
Register your FEITIAN MultiPass FIDO through online service as described in chapter 2.1.

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

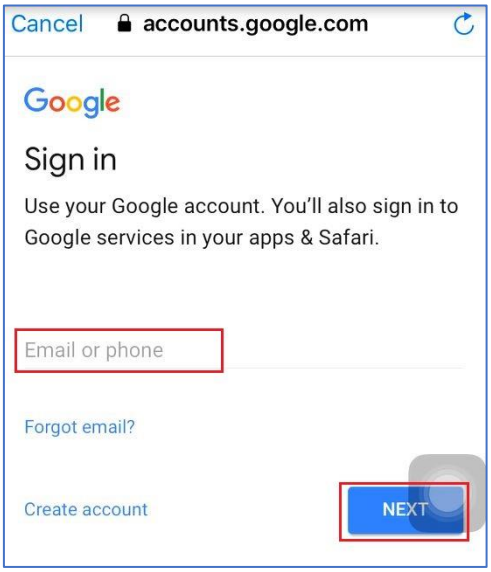
Click **SIGN IN** on **Smart Lock** UI.



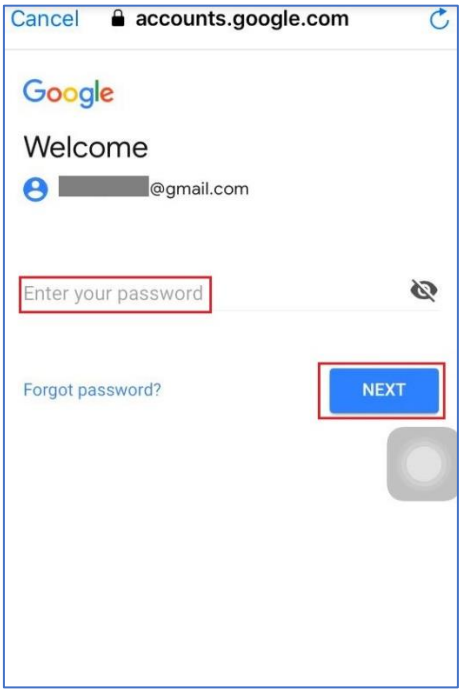
Click **Continue** on pup-up window.



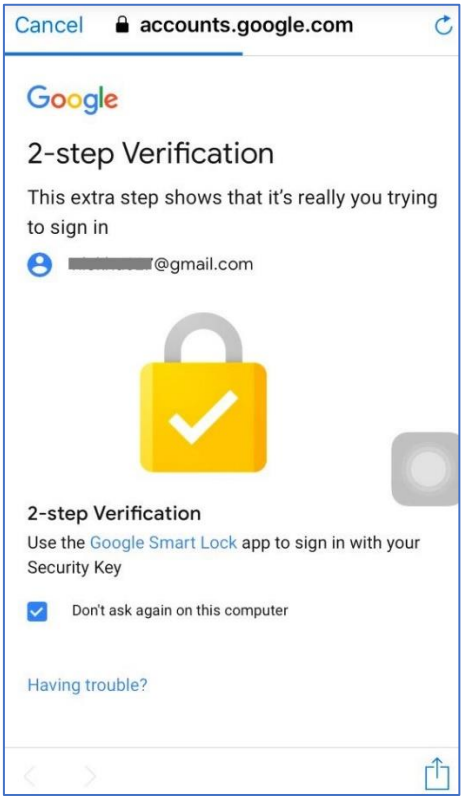
Enter your google account and click **NEXT**.



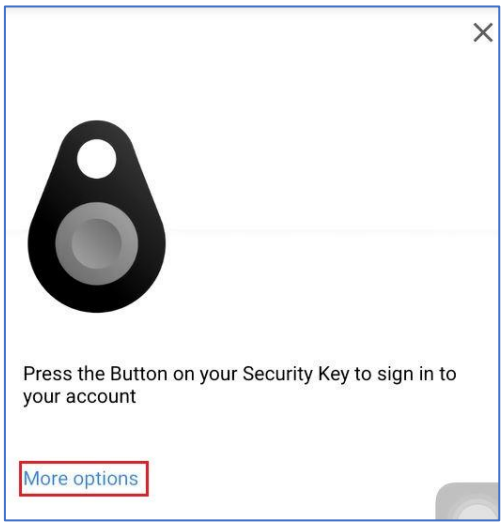
On next pop-up window, you are required to enter your password, then click **NEXT**.



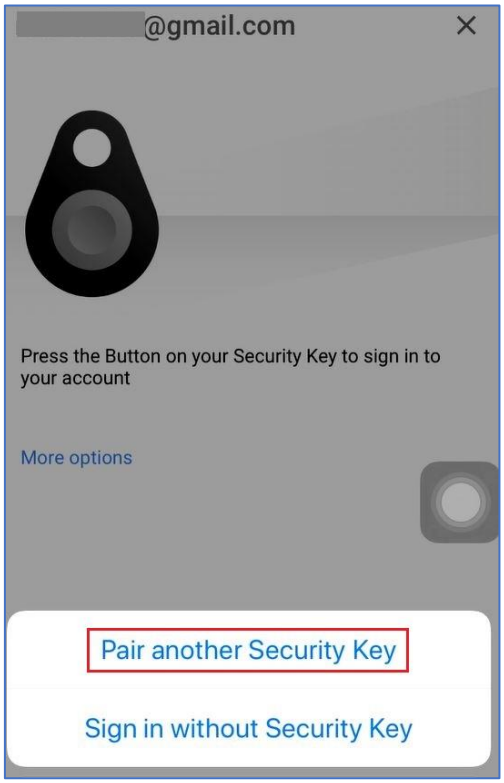
A notification window pops up and no operation is needed.



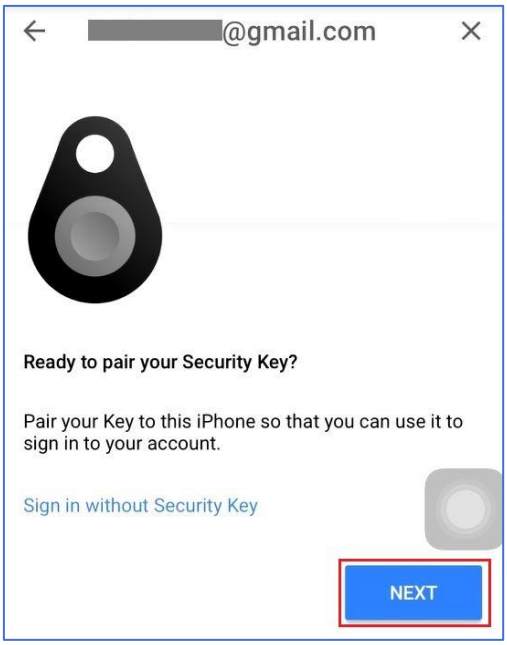
If it is the first time you connect FEITIAN MultiPass FIDO, press **More option** to connect hardware token.

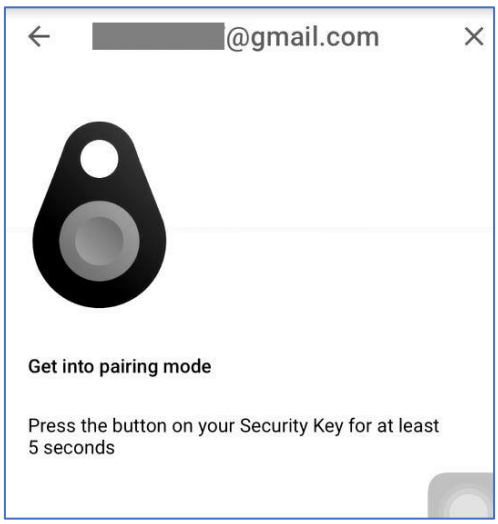


Press **Pair another Security Key**.

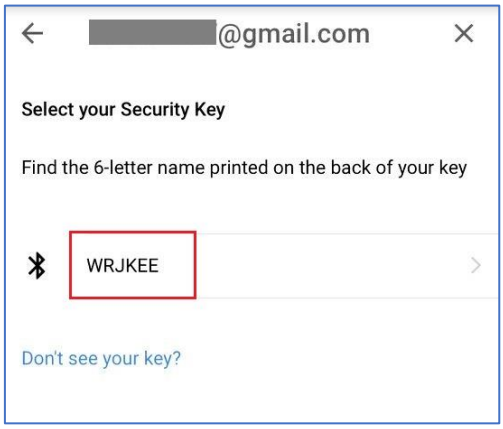


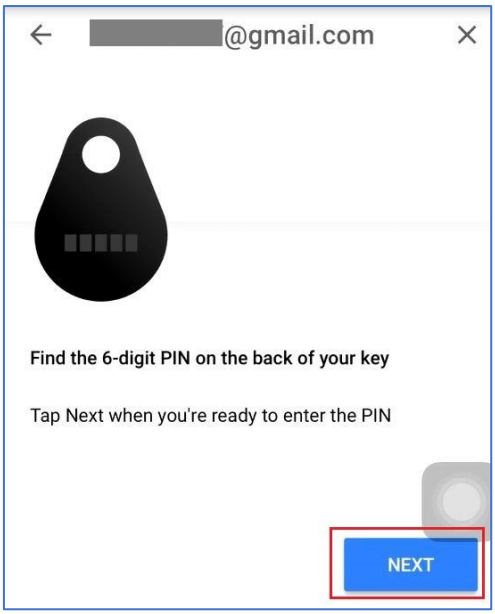
Press **NEXT** and then press the button on your security key for at least five minutes as indicated.



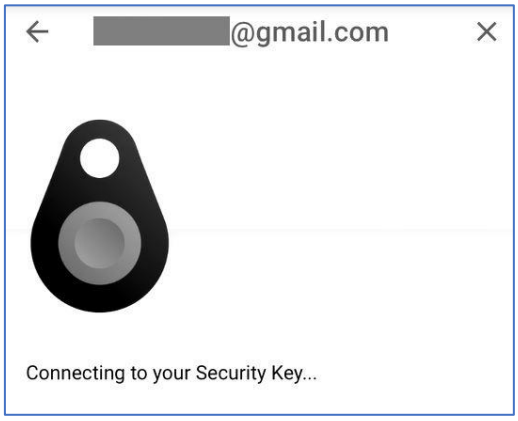


This pop-up window shows the name of your security key, press the name.
Next window indicates you to find 6-digit PIN on the back of your key, press **NEXT**.

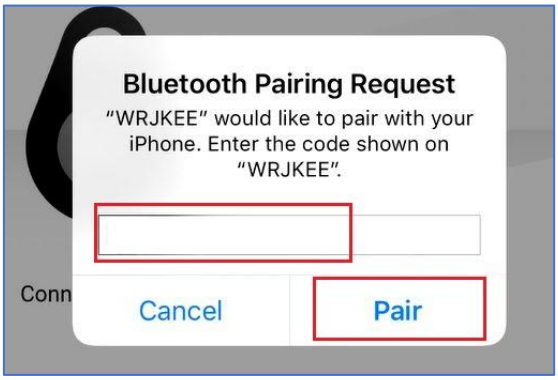




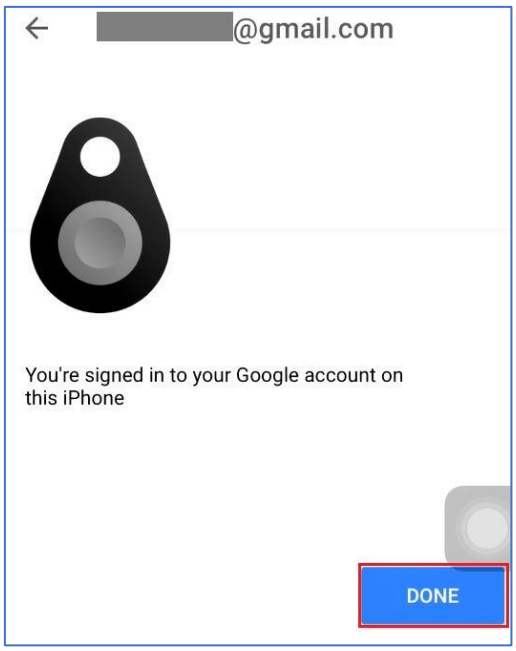
Waits for connecting to your security key.



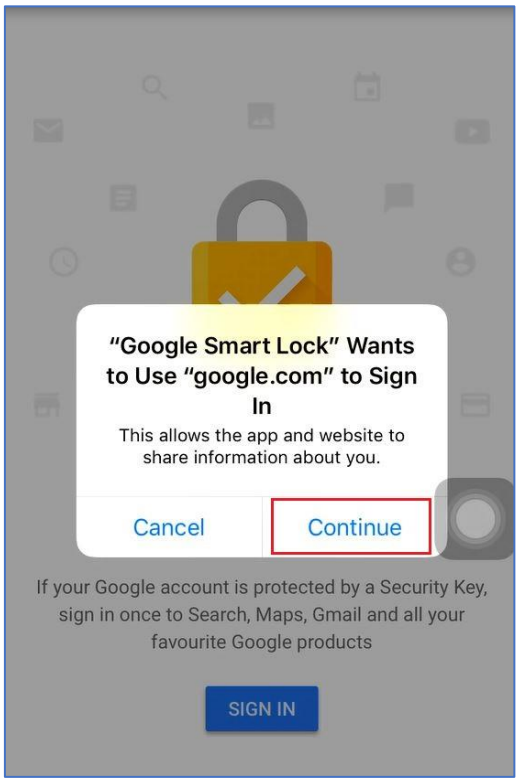
Type in the PIN on the back of your security key and press **Pair**.

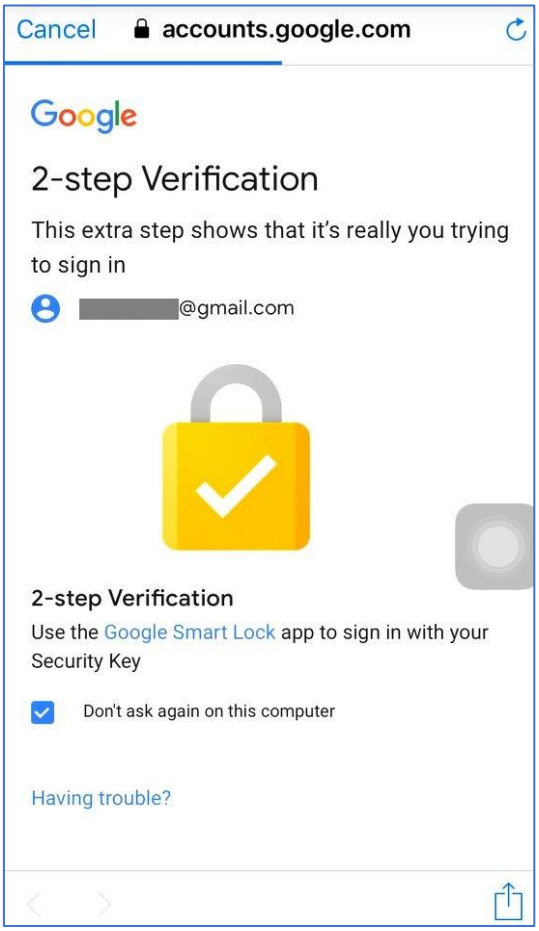


Press **DONE**.



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





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