eSecu FIDO U2F Security Key
User Manual
(v1.0)

FCC ID: 2ARDD-FD200

Shenzhen Excelsecu Data Technology Co., Ltd.

NO WARRANTIES OF ANY NATURE ARE EXTENDED BY THIS DOCUMENT. Any product and related material disclosed herein are only furnished pursuant and subject to the terms and conditions of a duly executed Program Product Licence or Agreement to purchase or lease equipment. The only warranties made by Excelsecu Technology, if any, with respect to the products described in this document are set forth in such Licence or Agreement. Excelsecu Technology cannot accept any financial or other responsibility that may be the result of your use of the information or software material, including direct, indirect, special or consequential damages.

You should be careful to ensure that the use of this information and/or software material complies with the laws, rules, and regulations of the jurisdictions with respect to which it is used. All rights reserved.

Copyright © 2018 Shenzhen Excelsecu Data Technology Co., Ltd.

Table of Contents

1. Product Overview....4
2. Product Picture....4
3. The Basic Operation....5
3.1 Register (First Time Only)....5
3.2 Signing-In (After Completing Registration)....6
3.2.1 BLE Mode (First Time Only)....6
3.2.2 BLE Mode (Paired Before)....6
3.2.3 USB Mode....7
4. How to use eSecu FIDO Key with Google....7
4.1 Register....7
4.2 Sign in with eSecu FIDO Key (USB Mode)....12
4.3 Sign in with eSecu FIDO Key (BLE Mode + Android Mobile Device)....14
4.4 Sign in with eSecu FIDO Key (BLE Mode + iOS Mobile Device)....15
5 FAQ....17
Question 1: I have two gmail accounts, how many FIDO keys do I need to protect two gmail account. Do I need 2 FIDO keys?....17
Question 2: What should I do if I lost my FIDO key?....17
Question 3: Dose this FIDO key have NFC capabilities?....17
Question 4: How can I pair the FIDO Key with iPhone?....17
Question 5: Can I use FIDO Key on PC over Bluetooth?....17
Question 6: What applications support FIDO Key?....17
Question 7: Can I register a FIDO Key over my smart phone?....17
Question 8: How can I know when to charge my FIDO key?....18
6. Product Spec....18

Thank You for Using eSecu FIDO U2F Security Key

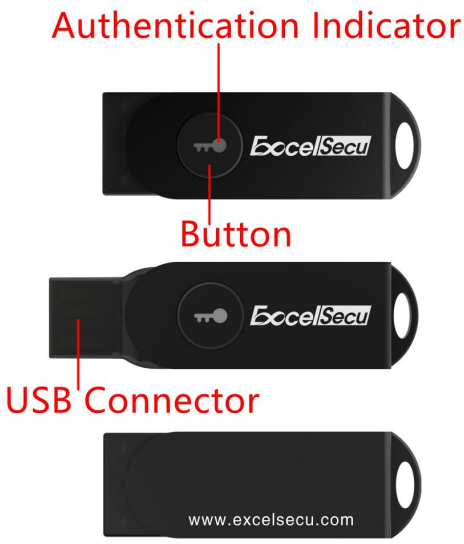
IMPORTANT INSTRUCTIONS

Please read this manual before operating your eSecu FIDO U2F Security Key (eSecu FIDO Key for short) and keep it for future reference.

1. Product Overview

eSecu FIDO® series are hardware authenticators complying with Universal Second Factor (U2F) standard. By adding an eSecu FIDO Key to user login, the online services significantly increase the security of their existing password infrastructure. The users are less to worry about their account information stolen by phishing, hacking or viruses. Simply tapping on a button, the users can easily authenticate to all their U2F-enabled services and applications (e.g. Google Apps) with a single device.

2. Product Picture



eSecu FIDO® HID

The button has the following lighting states:

Steady white light: Insert the eSecu FIDO Key in the computer's USB port.

Flashing white light: The eSecu FIDO Key blinks white light when received an authentication request. Taping on the button to complete the sigh-in.

eSecu FIDO® BLE

The button has the following lighting states:

Steady blue light: long press the button for 5 seconds to power on, and enter the bluetooth pairing mode for the first time. After paired successfully, the steady blue light turns to flashing blue light.

Flashing blue light: short press the button to enter the bluetooth mode. The eSecu FIDO Key responses the authentication request automatically.

Steady white light: Insert the eSecu FIDO Key in the computer's USB port when it is powered off (not in bluetooth mode).

Flashing white light: In the USB mode, the eSecu FIDO Key blinks white light when received an authentication request. Taping on the button to complete the sigh-in.

Flashing red light: low power state. Blinking red light every 5 seconds. Please charge it in time.

3. The Basic Operation

3.1 Register (First Time Only)

The following registration process can only be done on PC over USB connection.

1. Enter the user name and password to log in to any application that supports FIDO U2F.
2. Insert the eSecu FIDO Key in a USB port.

3. Add the eSecu FIDO Key to your account(s).

3.2 Signing-In (After Completing Registration)

1. Enter the user name and password to log in to any web service that supports FIDO U2F.
2. Connect the registered eSecu FIDO Key to the mobile device (BLE mode) or PC (USB mode).
3. When prompted, press the button on eSecu FIDO Key to sign in.

- Using FIDO key with BLE mode on android mobile devices requires application (e.g. **Chrome browser** + **Google authenticator**).
- Using FIDO key with BLE mode on iOS mobile devices requires application (e.g. **Chrome browser** + **Smart Lock**).
- Using FIDO key with USB mode on web services requires application (e.g. **Chrome browser**).

3.2.1 BLE Mode (First Time Only)

1. Long press the button for 5 seconds to power on and enter the BLE pairing mode for the first time. The indicator light is blue on all the time. If there is no pairing request received in 60 seconds, the indicator light goes out and eSecu FIDO Key shuts down automatically.
2. Scan BLE devices on your client side (e.g. a smart phone). Connect the BLE device which has the same SN as printed on the back of the eSecu FIDO Key.
3. Input 6-digits PIN as printed on the back of the eSecu FIDO Key. When paired successfully, the blue light should start blinking.
4. When an authentication request is received, the blue light blinks and the eSecu FIDO Key will respond the request automatically.

For security purpose, the FIDO key will be forced to shut down after 15 seconds after powered on. Short press the button to re-enter BLE mode and to complete the authentication.

3.2.2 BLE Mode (Paired Before)

1. Short press the button to power on and enter the BLE mode. The indicator light blinks blue.
2. When an authentication request is received, the blue light blinks and the eSecu FIDO Key will

respond the request automatically.

For security purpose, the FIDO key will be forced to shut down after 15 seconds after powered on. Short press the button to re-enter BLE mode and to complete the authentication.

3.2.3 USB Mode

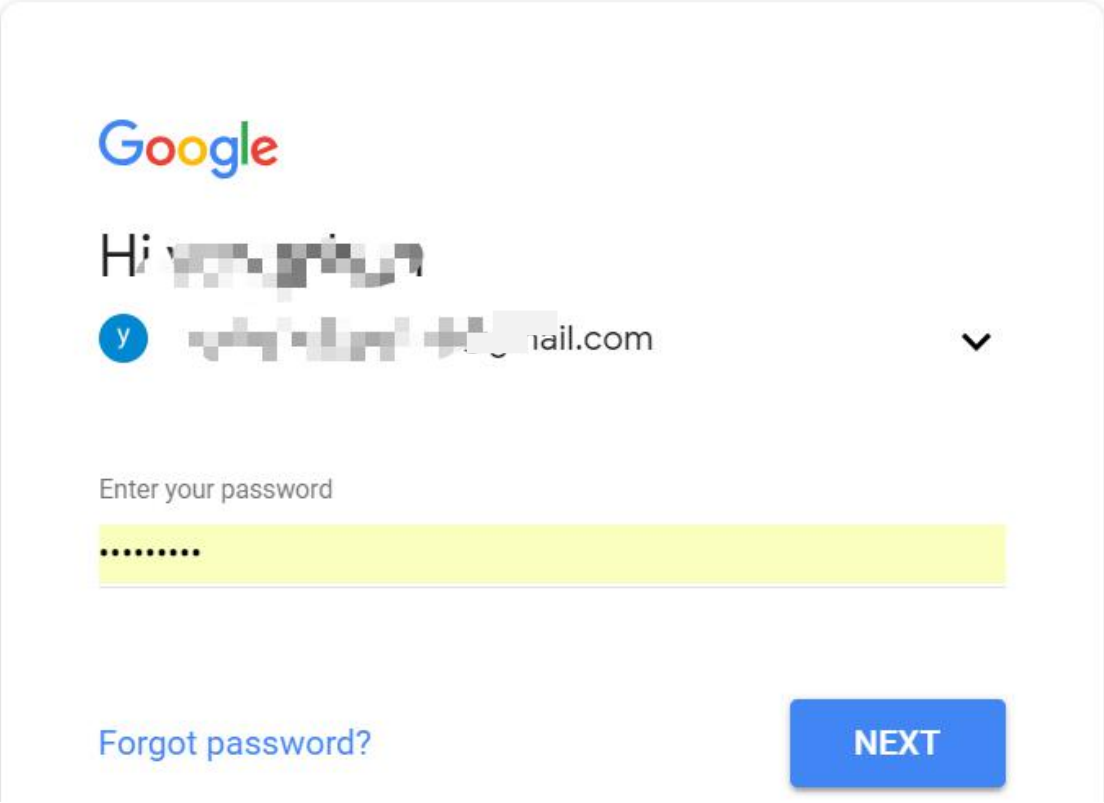
1. Make sure eSecu FIDO Key is powered off (Not in BLE mode).
2. Insert eSecu FIDO Key to the computer's USB port. The indicator light is white on all the time.
3. When an authentication request is received, the white light blinks. Press the button to confirm this authentication.

4. How to use eSecu FIDO Key with Google

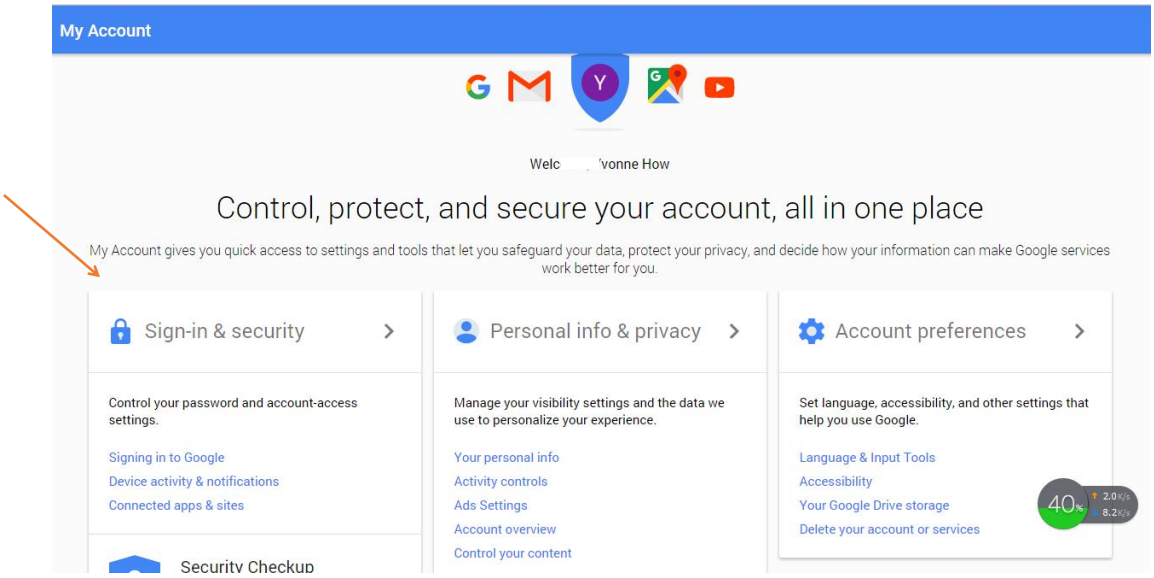
4.1 Register

Register eSecu FIDO Key with your Google account to make it become the second authentication factor.

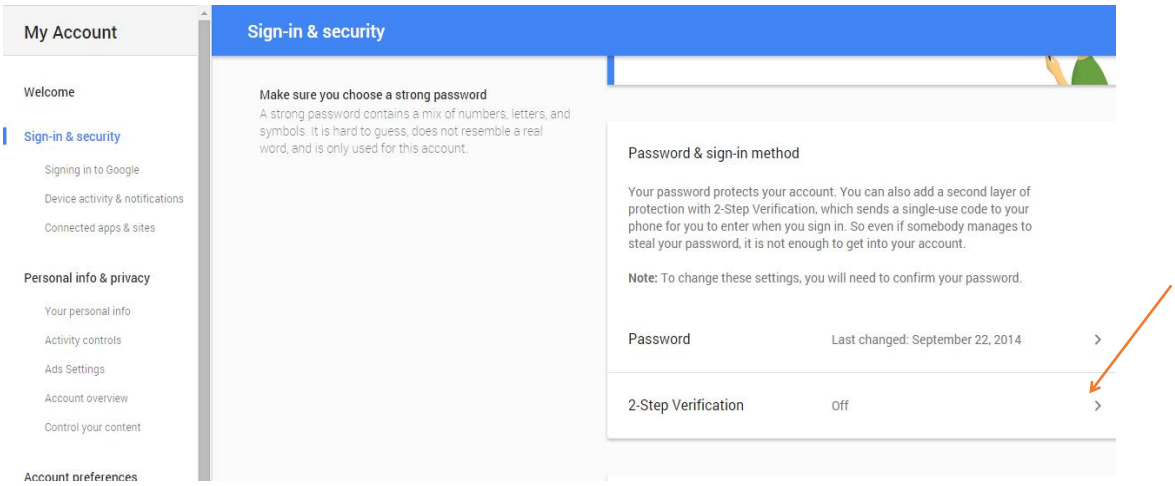
1. Sign in to your Google account as before.



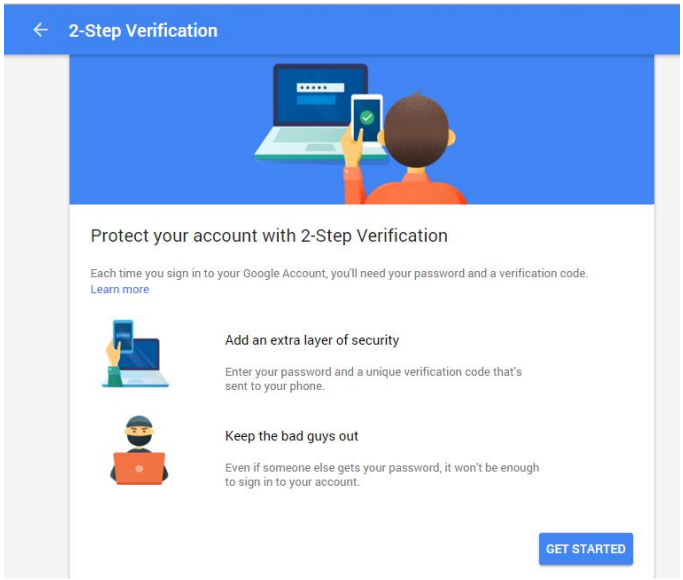
2. Click **Sign-in & security**.



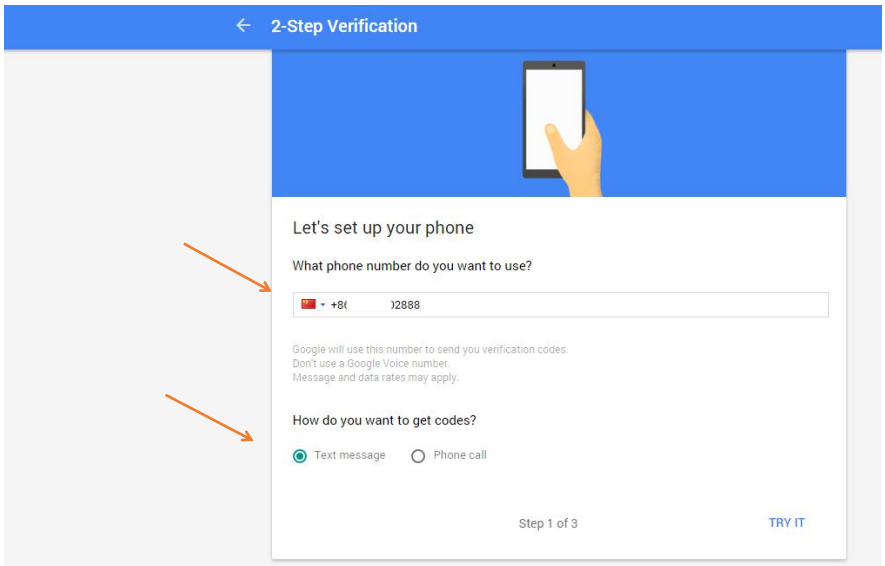
3. Click **2-Step Verification**.



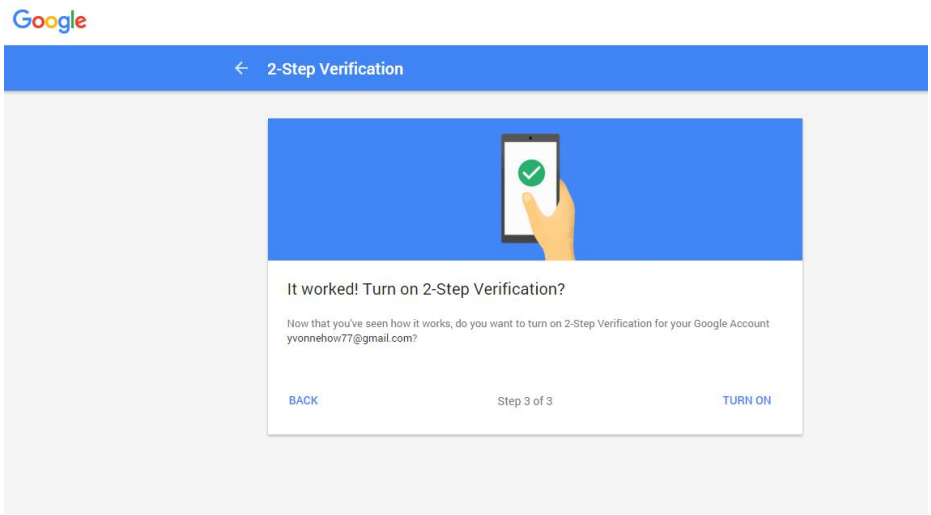
4. Click **GET STARTED**. For security reasons, you'll be asked to re-enter your password to enable 2-Step Verification.



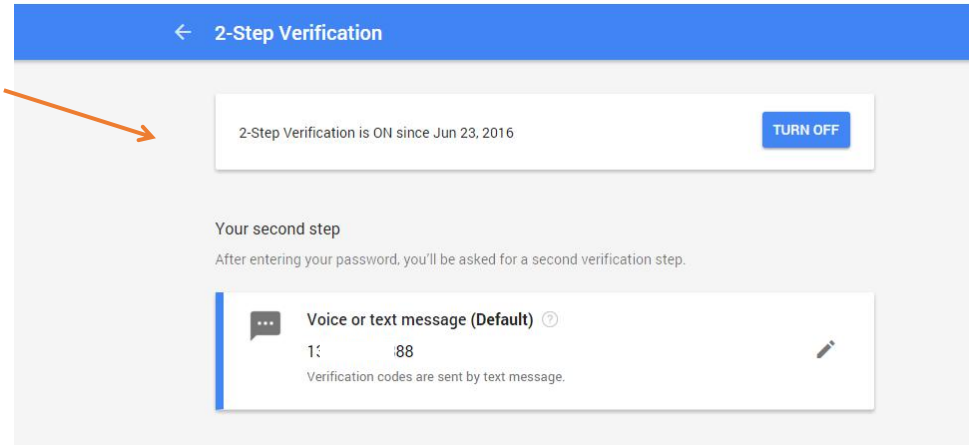
5. Once you do, you'll be given the choice to receive your security code by **Text message** or **Phone call**. Here select **Text message** as an example and enter the phone number.



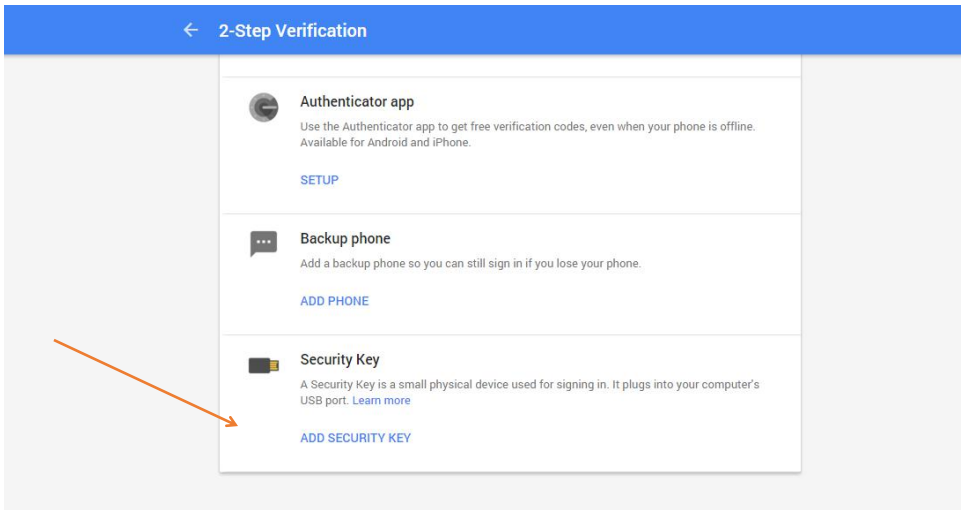
6. Enter the security code you received then click **TURE ON** to complete the setup of 2-Step Verification.



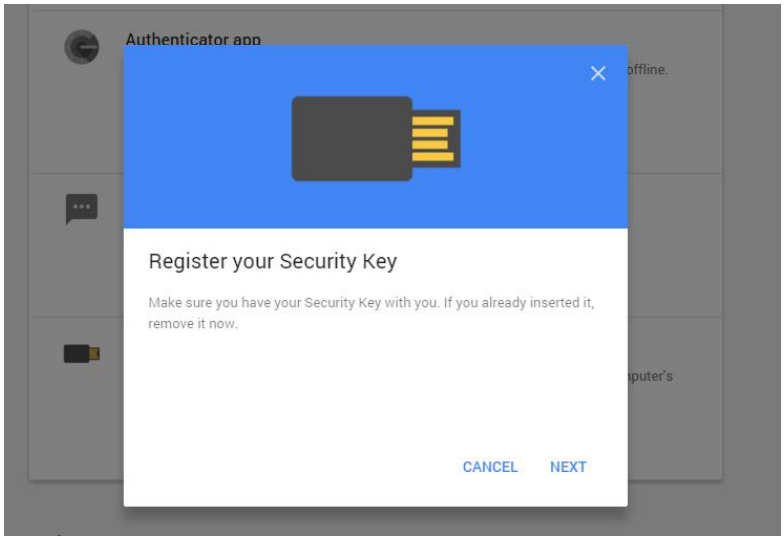
7. 2-Step Verification is **ON** now.



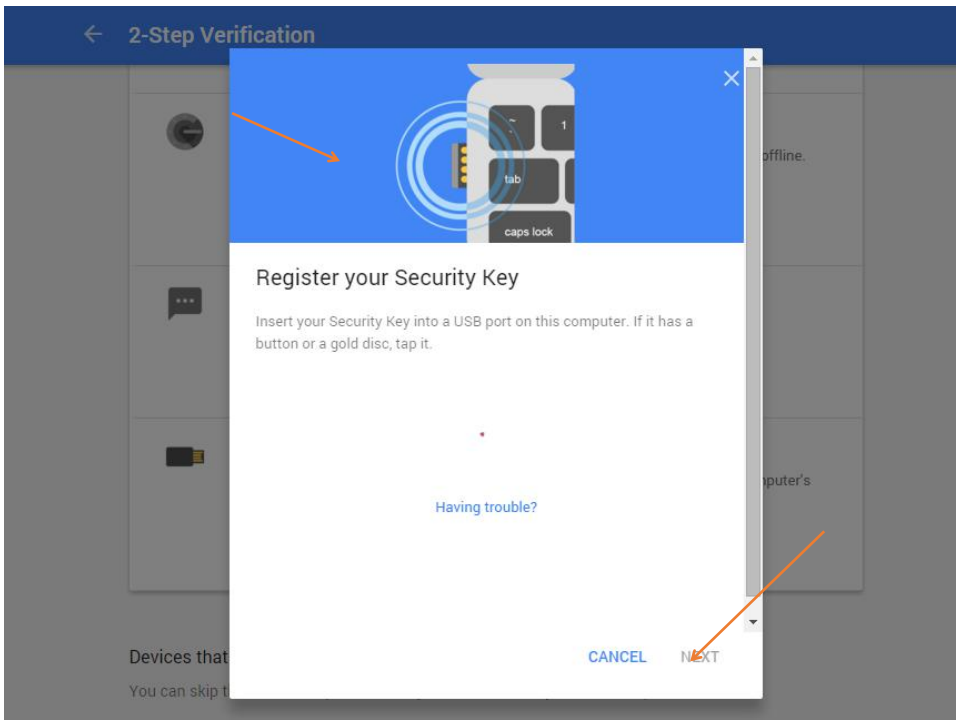
8. Click **ADD SECURITY KEY** to register eSecu FIDO Key to your account as the second factor of authentication.



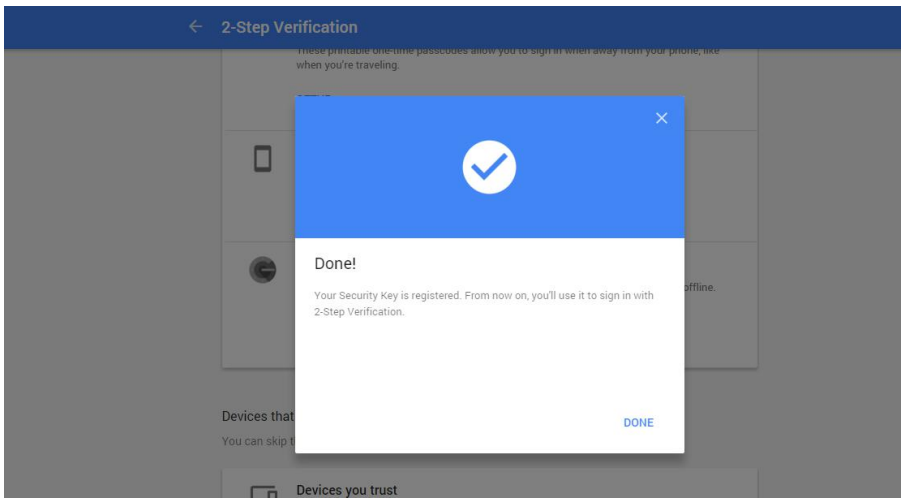
9. Click **NEXT** to register.



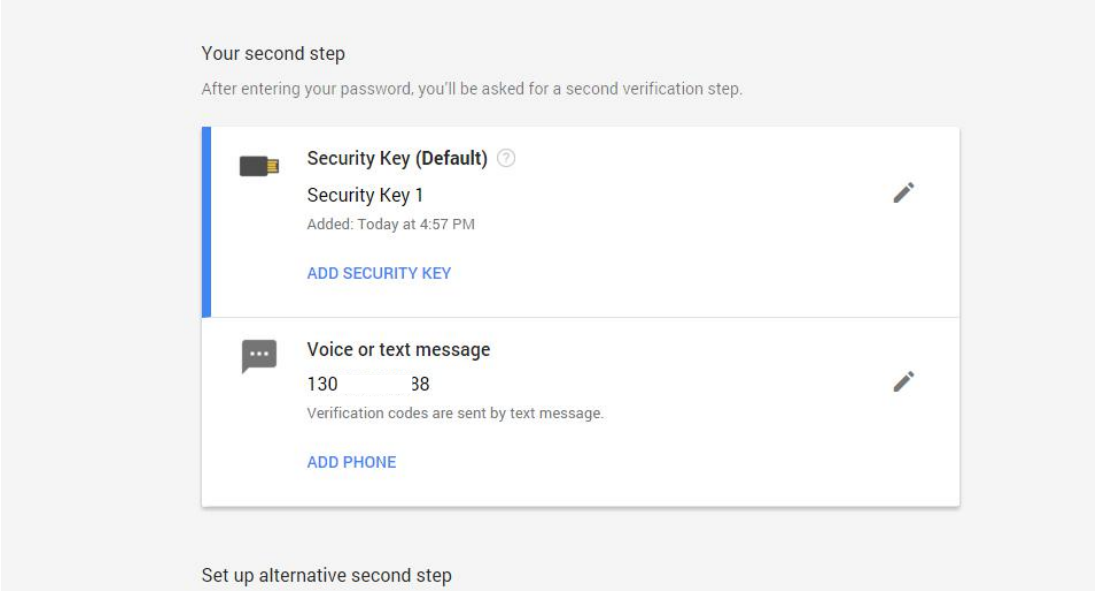
10. You will be prompted to insert your security key into a USB port and tap the button on eSecu FIDO Key. Click **NEXT** to continue.



11. The eSecu FIDO Key is registered successfully.

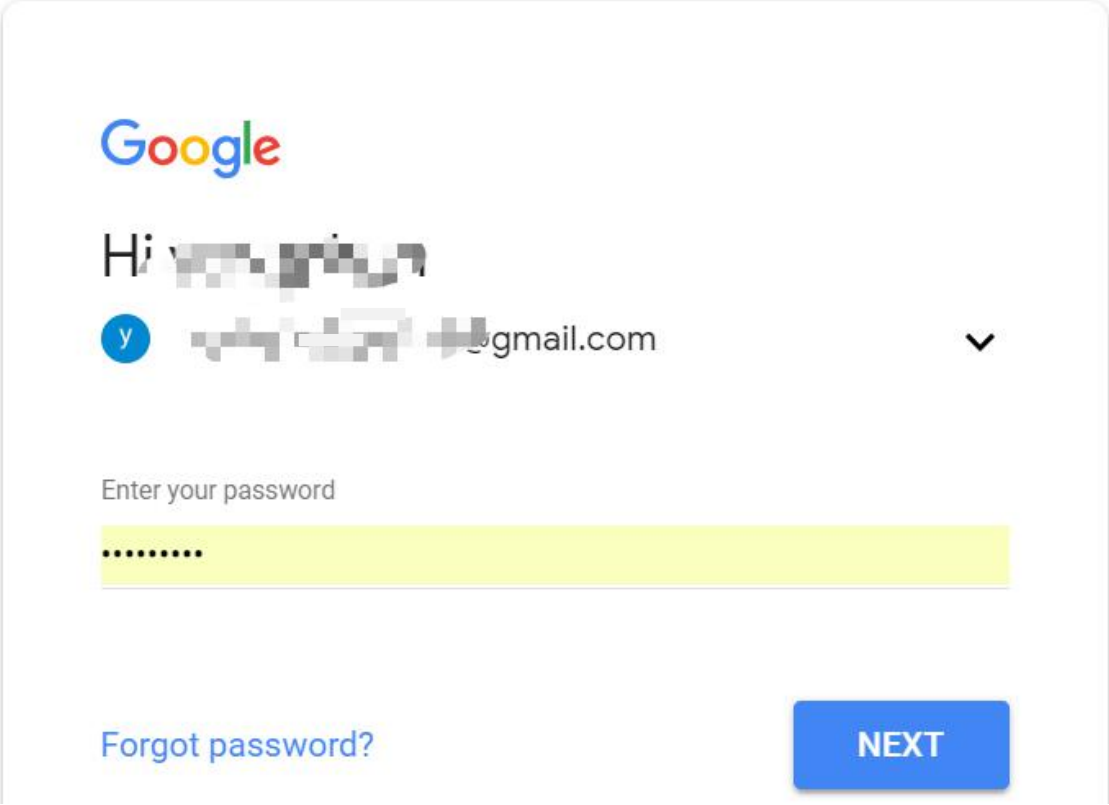


12. The eSecu FIDO Key becomes the default second authentication factor of your account. You will be asked to use it to complete 2-Step Verification when sign in to Google in the future.

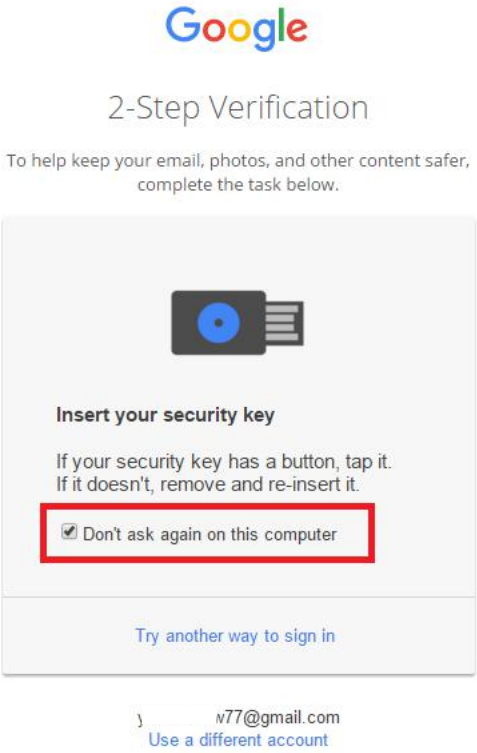


4.2 Sign in with eSecu FIDO Key (USB Mode)

1. Sign in to Google with username and password. Since you have an eSecu FIDO key as the strong second authentication factor, you can simplify your password (e.g. 4-digit PIN) without compromising security.



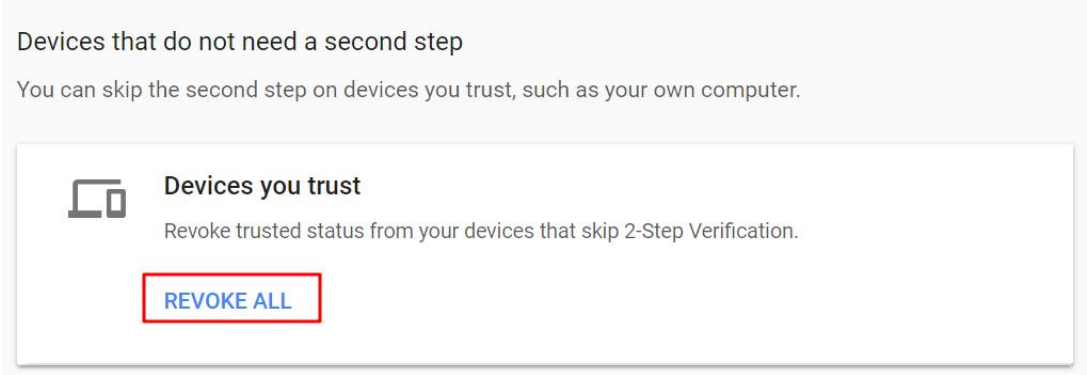
2. Insert eSecu FIDO Key to a USB port and tap the button on the key. You will be authorized to access your Google account now.



By default, "Don't ask again on this computer" is checked. After checking the box, the next login will skip the two-step verification and log in directly with the user name and password.

You can undo trusted devices in settings to restore the use of two-step verification.

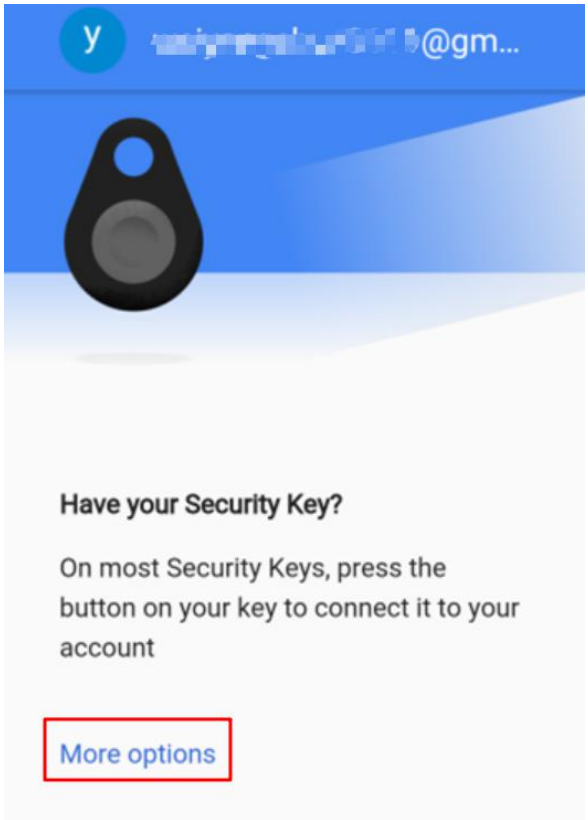
Click **Revoke All** to clear the trusted device and restore the use of two-step verification.



4.3 Sign in with eSecu FIDO Key (BLE Mode + Android Mobile Device)

Using FIDO key with BLE mode on android mobile devices requires application (e.g. Chrome browser + Google authenticator).

1. Open the Chrome browser, then go to "**Settings > Account > Add Account > Google Account**", and enter the username and password.
2. When prompted, present your registered FIDO key. Make sure the Bluetooth of your mobile device is turned on.
3. You need to pair your registered FIOD key when using it on your mobile device for the first time.

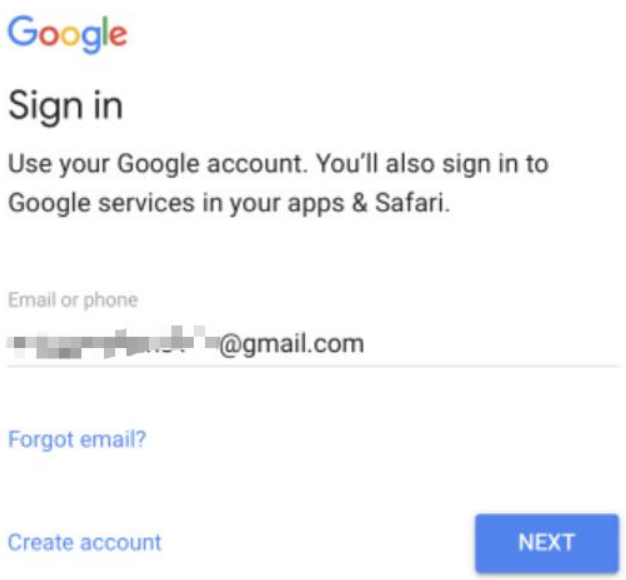


4. Click “More option > Pair a new security key > Next” to start pairing procedure.
5. Long press the button for 5 seconds to power on and enter the BLE pairing mode for the first time. The indicator light is blue on all the time.
6. Connect the BLE device which has the same SN as printed on the back of the eSecu FIDO Key. Input 6-digits PIN as printed on the back of the eSecu FIDO Key. When paired successfully, the blue light should start blinking. When an authentication request is received, the blue light blinks and the eSecu FIDO Key will respond the request automatically.
7. When you are signing with eSecu FIDO key on the mobile device again, enter your google account and password.
8. When prompted, present your registered FIDO key. Make sure the Bluetooth of your mobile device is turned on.
9. Short press the button to power on and enter the BLE mode. The indicator light blinks blue. When an authentication request is received, the blue light blinks and the eSecu FIDO Key will respond the request automatically.

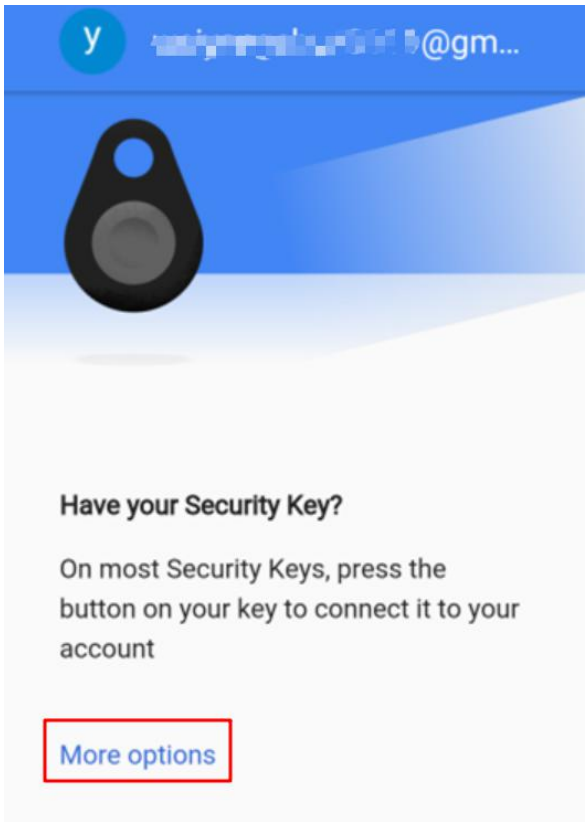
4.4 Sign in with eSecu FIDO Key (BLE Mode + iOS Mobile Device)

Using FIDO key with BLE mode on iOS mobile devices requires application (e.g. Chrome browser + Smart Lock).

1. Open the Smart Lock, enter your google account and password.



2. When prompted, present your registered FIDO key. Make sure the Bluetooth of your mobile device is turned on.
3. You need to pair your registered FIOD key when using it on your mobile device for the first time.



4. Click "More option > Pair a new security key > Next" to start pairing procedure.
5. Long press the button for 5 seconds to power on and enter the BLE pairing mode for the first time. The indicator light is blue on all the time.
6. Connect the BLE device which has the same SN as printed on the back of the eSecu FIDO Key. Input 6-digits PIN as printed on the back of the eSecu FIDO Key. When paired successfully, the blue light should start blinking. When an authentication request is received, the blue light blinks and the eSecu FIDO Key will respond the request automatically.

7. When you are signing with eSecu FIDO key on the mobile device again, enter your google account and password.
8. When prompted, present your registered FIDO key. Make sure the Bluetooth of your mobile device is turned on.
9. Short press the button to power on and enter the BLE mode. The indicator light blinks blue. When an authentication request is received, the blue light blinks and the eSecu FIDO Key will respond the request automatically.

5 FAQ

Question 1: I have two gmail accounts, how many FIDO keys do I need to protect two gmail account. Do I need 2 FIDO keys?

Answer: You can use one FIDO key with multiple accounts, but that is not recommended. Regardless of if you're protecting one gmail account, or two - you should register multiple keys (if the service allows it). That way, if you lose your key, or it's damaged, or it's stolen, you will still have a backup key ready to use.

Question 2: What should I do if I lost my FIDO key?

Answer: Just go to the website your key already registered. On the 2-step verification tab or similar tab, delete the device. Two FIDO keys are recommended, one for normal use, the other for backup.

Question 3: Dose this FIDO key have NFC capabilities?

Answer: No

Question 4: How can I pair the FIDO Key with iPhone?

Answer: iPhone does not allow the FIDO Key to be paired over the Bluetooth setting page directly. You need to download the application “Smart Lock” from app store and use the “Smart Lock” to pair the FIDO Key.

Question 5: Can I use FIDO Key on PC over Bluetooth?

Answer: Most of the FIDO® U2F PC applications rely on HID interface which Bluetooth is not compatible with that. Please use the FIDO key on PC over USB interface.

Question 6: What applications support FIDO Key?

Answer: The applications support FIDO® U2F include but not limited to: Google, Facebook, Dropbox, GitHub, Dashlane, DUO, StrongAuth etc.

Question 7: Can I register a FIDO Key over my smart phone?

Answer: No. You can always authenticate the FIDO key with your mobile devices, but registration can

only be done from a non-mobile device with Chrome and other U2F supported browsers.

Question 8: How can I know when to charge my FIDO key?

Answer: When a red indicator blinks every 5 seconds a time, the FIDO key is in low power state. Charging process starts automatically when FIDO key is plugged in the USB port of the PC.

6. Product Spec

Product	eSecu FIDO® HID	eSecu FIDO® BLE
System	Windows, MacOS, Linux, Chrome OS	Windows, MacOS, Linux, Chrome OS, Android, iOS
Authorization	FIDO® U2F	FIDO® U2F L1
Algorithm	ECDSA, SHA256	ECDSA, SHA256
Size	44.7*16.0*9.0 (mm)	54.2*18.0*10.9 (mm)
Interface	USB	USB
Protocol	HID	HID, BLE
Data Retention	≥20 years	≥20 years
Rewrite Cycle	≥100,000 times	≥100,000 times
Operating Voltage	5V±10%	5V±10%
Operating Current	Max <40mA	max for USB <80mA max for BLE <20mA
Operating Temperature	-10~60℃	-10~60℃
Storage Temperature	-20~60℃	-20~60℃
Operating Humidity	10~90%	10~90%
Buttons	Single button	Single button
Button Durability	≥100,000 times	≥100,000 times
LED	White	Blue, white and red LED lights
Material	Aluminum alloy, PC	Aluminum alloy, PC
Battery	-	40mA
Battery Life	-	Rechargeable 500 times

FCC STATEMENT :

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

Warning: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

RF warning statement:

The device has been evaluated to meet general RF exposure requirement. The device can be used in portable exposure condition without restriction.