V1.0

User's Manual for

G310H/B320H/B210H/B220H

Please read the manual carefully before use. The graphics here can be different from the user's computer and can also be changed without notice. The content can be modified later.

Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

Contents

1. USB Security Key from TrustKey Solutions 4
   1. What is the USB Security Key? 4
   2. Please read the following before you use the security key 4
2. TrustKey's Security Keys 6
   1. Product Specification 6
   2. Security Key Description 7
   3. LED Status Indicator 7
3. Security Key Fingerprint Enrollment 8
   1. Fingerprint Enrolment steps (Windows 10) 8
   2. Fingerprint Enrolment steps 9
   3. Security Key Fingerprint Enrollment (MacOS, Linux) 14
4. Security Key Fingerprint Removal Procedure 18
   1. Fingerprint removal (Windows10) 18
   2. Fingerprint Removal (MacOS, Linux) 20
5. Security Key PIN 21
   1. PIN (Personal Identification Number) 21
   2. PIN setup 21
   3. PIN information change 22
   4. PIN Authentication Failure 23
   5. Security Key Factory Reset 25
6. Online usage of the security keys 28
   1. Microsoft Azure AD 28
      a. Azure AD user registration 28
      b. Sign in Windows (Azure AD joined) 31
   2. Google G-suite 32
   3. Bank of America USB Security Key Experience 36
   4. Other Online services 41
7. Windows Hello Set-up Guide 42
   What is Windows Hello? 42
   Setup Devices in Windows Hello 42
8. Additional Services 44

Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

1. TrustKey ThumbLock Solution 44
2. TrustKey Login Solution 45
Appendix 46
1. Frequently Asked Questions 46
Using H-series Security Keys 46
Supported Platform · Environment 47
H-series Security Key Features 47
Misc. 48
2. Safety precautions 49
3. Warranty and Consumer Dispute Resolution Policies 50
Standard Warranty: 50
Consumer Dispute Resolution 50
Service with charge 51
Manufacturer Information 52
FCC Warning Statements 53
Supplier’s Declaration of Conformity: 53

Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

1. USB Security Key from TrustKey Solutions

1. What is the USB Security Key?

A security key is a peripheral device used to gain access to an electronically restricted resource. The hardware key is used in addition to or in place of a password. It acts like an electronic key to access something. A Security key is also called a security token.
A USB Security Key is a security key with a USB interface to connect to a PC.

TrustKey's G310H/B320H/B210H/B220H is a biometric (fingerprint) security key with a USB interface from TrustKey Solutions.

2. Please read the following before you use the security key

1. Please note that Fingerprint enrolment for **Windows Hello** and **USB Security Key** is different

2. The user needs to enroll the user's fingerprint separately with Windows Hello (for PC login) and a security Key (for Web login).

    - Security Key Fingerprint enrolment
        - Use for login websites that are offering FIDO (U2F/FIDO2) authentication login mechanisms
        - Fingerprint templates are stored inside the security key and never leaves the security key
    - Windows Hello Fingerprint enrolment
        - Use for login PC using fingerprint rather than a password or PIN
        - Fingerprint templates are stored inside the secure storage of the PC

3. Our recommendation
    a. Please use the security keys after fingerprint enrollment. The user can use the TrusrtKey security key without fingerprint enrollment. However, the user can enjoy the benefit of biometric authentication, including no typing PIN. Note that PIN can also be leaked. Authentication with fingerprint recognition is the safest method of all!
    b. Microsoft mandates the user to set up a PIN for the security key before fingerprint enrollment. The PIN is also used for fingerprint modification (add/delete fingerprints)
    c. Please make sure that the PC supports the security key's USB type (USB-A or USB-C)

Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

4. Check the version of the device

Device Platform	Version	Description
Windows 10	v.1809 or later	Cannot be used with Windows 7, 8
MacOS	Mojave or later	
Linux	Latest version	64 bit Ubuntu 14.04 or later, Debian 8 or later, openSUSE 13.3 or later, Fedora Linux 24 or later
Android OS	v.7 or later	
iPadOS	v.13 or later	
Chrome	Latest version	Recommend to use the latest version
Edge	Latest version	Recommend to use the latest version
Firefox	Latest version	Recommend to use the latest version
Safari	Latest version	Recommend to use the latest version
Other Web Browers	Latest version	Support all Chromium-based web browsers

Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

2. TrustKey's Security Keys

1. Product Specification

Product Name	**B210H**	**B220H**	**G310H**	**G320H**
Model Name	B210h	B220h	eFA310h	eFA320h
FIDO Protocol	FIDO2, U2F	FIDO2, U2F	FIDO2 , U2F	FIDO2 , U2F
FIDO Security Level	Level 2	Level 2	Level 2	Level 2
USB Type	Type A	Type C	Type A	Type C
Resolution	160 x 160 pixel	160 x 160 pixel	160 x 160 pixel	160 x 160 pixel
Status Indicator	3 Color LED	3 Color LED	3 Color LED	3 Color LED
Device Type	FIDO2 HID device	FIDO2 HID device	FIDO2 HID device	FIDO2 HID device
Algorithm	Precise™ Biometrics	Precise™ Biometrics	Precise™ Biometrics	Precise™ Biometrics
Material	Polycarbonate	Polycarbonate	Polycarbonate	Polycarbonate
Certification	KC, FCC, CE, UKCA, RoHS	KC, FCC, CE, UKCA, RoHS	KC, FCC, CE, RoHS	KC, FCC, CE, RoHS
Operation Temp[1]	-20℃ ~ +60℃	-20℃ ~ +60℃	-20℃ ~ +60℃	-20℃ ~ +60℃
Storage Temp[2]	-40℃ ~ +85℃	-40℃ ~ +85℃	-40℃ ~ +85℃	-40℃ ~ +85℃
Color	Black	Black	Black	Black
Size	45.8 x 20.1 x 5.4 mm	45.8 x 20.1 x 5.4 mm	41.6 x 17.8 x 4.7 mm	41.9 x 17.8 x 4.7 mm
Weight	4.0 g	4.0 g	3.1 g	3.1 g

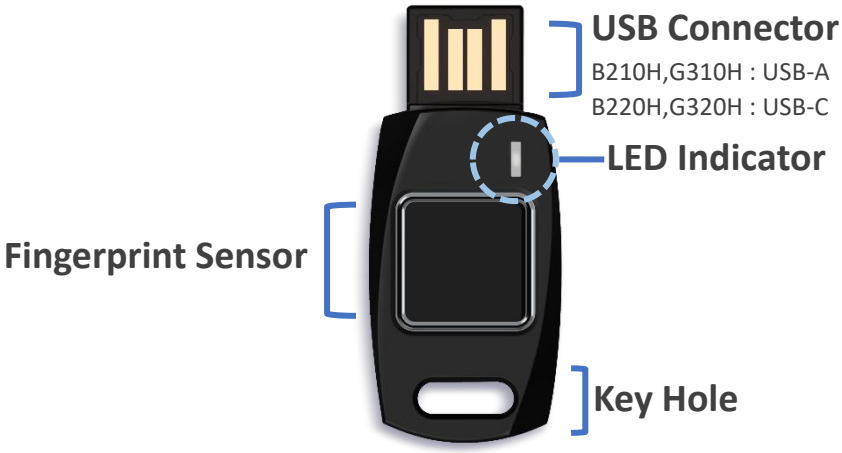
Note:

1. *-4°F ~ 140°F*

Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

2. -40°F ~ 185°F

2. Security Key Description



Example Model: B210H

3. LED Status Indicator

Color	Status	Description	Action
Green	On	- Key connection OK - Authentication Sucess	
Blue	On	N/A	
	Blinking	Waiting for fingerprint scan (FIDO2)	
Yellow	Blinking	Waing for fingerprint scan (U2F)	
Red	On	Security key is locked due to authentication failure	Unlock the security key
	Blinking	Authentication failure	Rescan fingerprint
Skyblue	Blinking	- Waiting for action (factory reset mode) - Security Key selection mode (when no fingerprint is enrolled)	
LED Off		Not connected	Reinsert the security key

Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

3. Security Key Fingerprint Enrollment

1. Fingerprint Enrolment steps (Windows 10)

Step 0: Check Windows version First

Please check your Windows version before enrolment by typing "winver" at the Windows search bar.

Please check the Windows Product Name (Windows Home, Pro, or Enterprise) as a red arrow indicates below. Also, look for the Windows version as the blue arrow indicates.

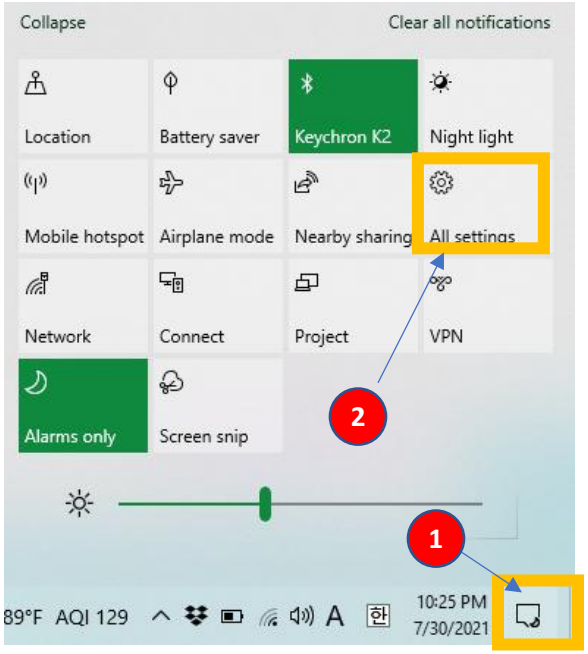
The user's Windows version should be Version 19H1 (or 1903) or later with Windows 10 Home, Professional, or Enterprise. The figure below indicates the PC's version is 21H1 with Windows 10 Pro.

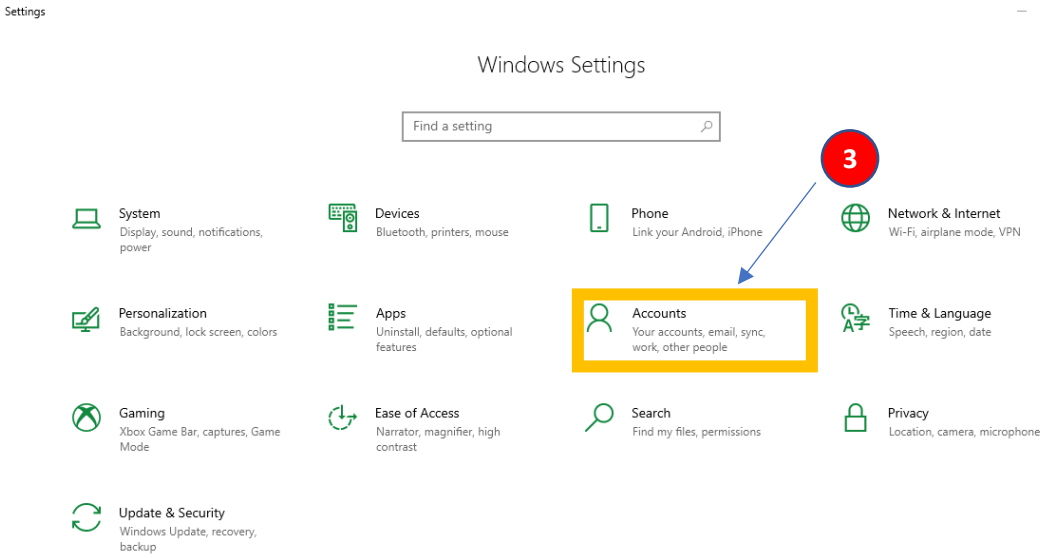
If your Windows version is earlier than 18298, then you need to upgrade.

Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

2. Fingerprint Enrolment steps

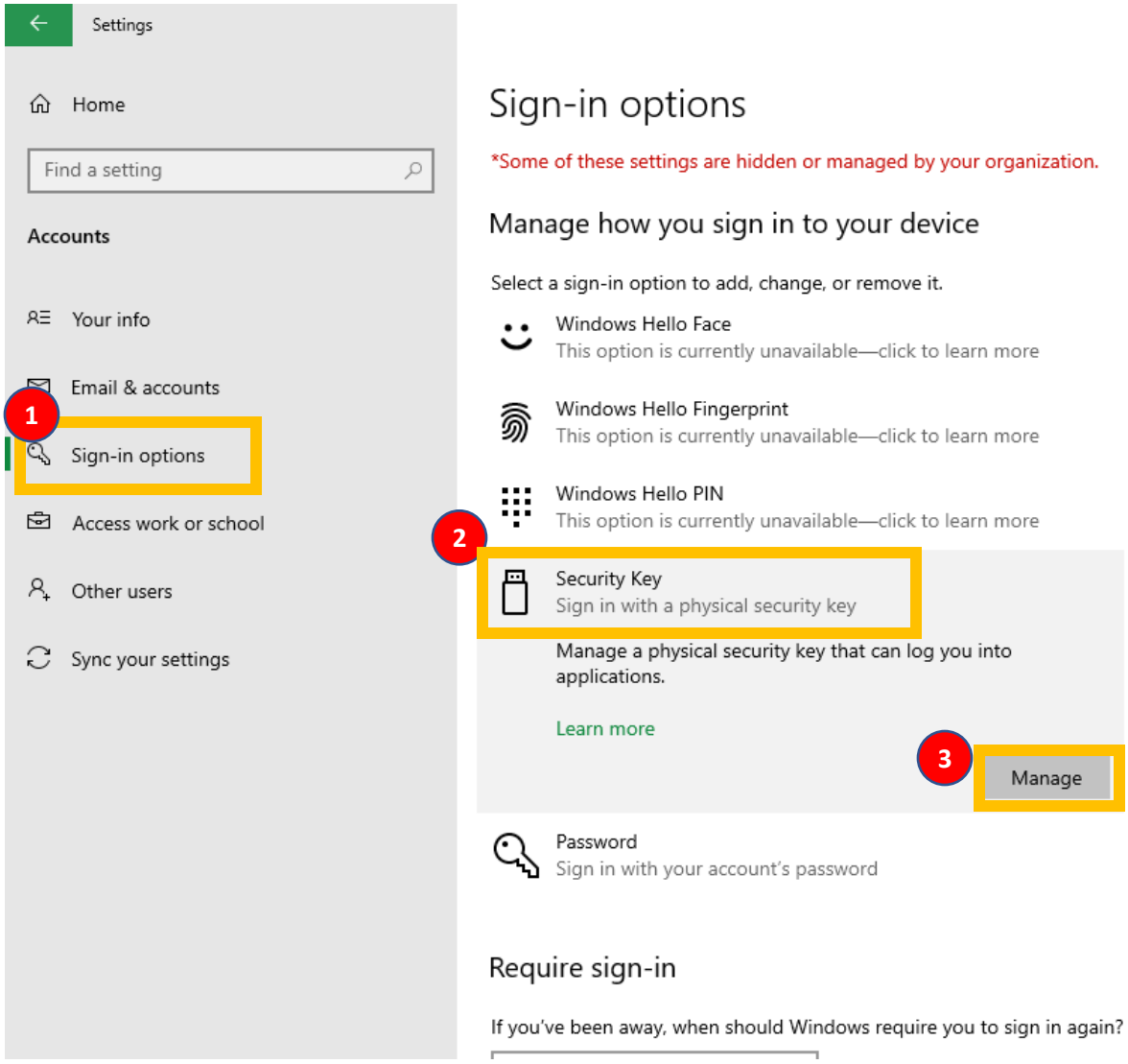
Step1: click the right down corner of the Windows screen ①, select "All settings" ②, and Accounts ③.





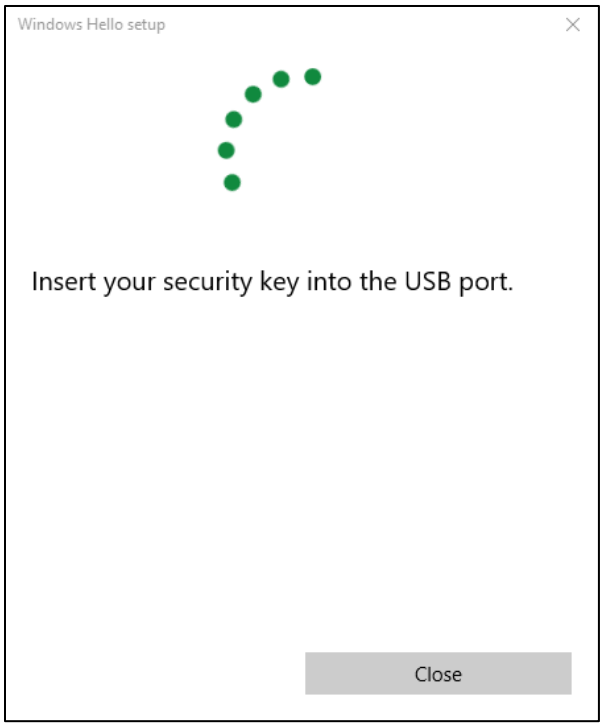
Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

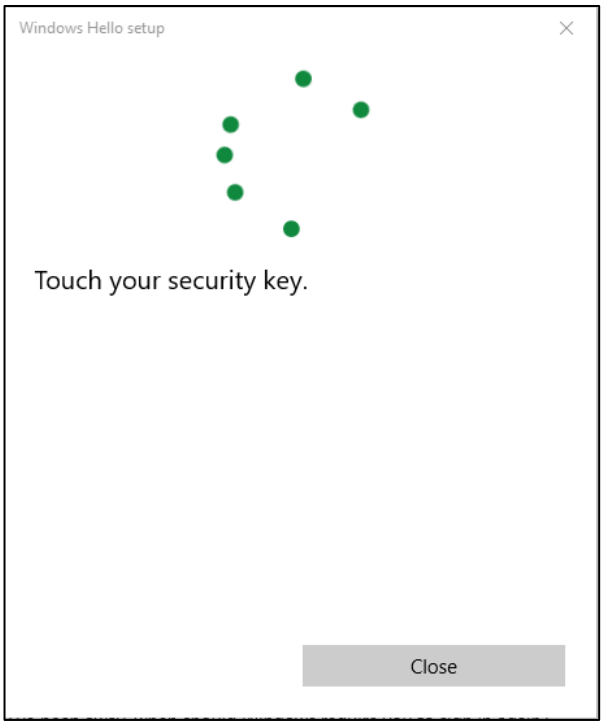
Step 2: From Settings, click "Sign-in Option" ① and Security Key ②, and Manage ③.



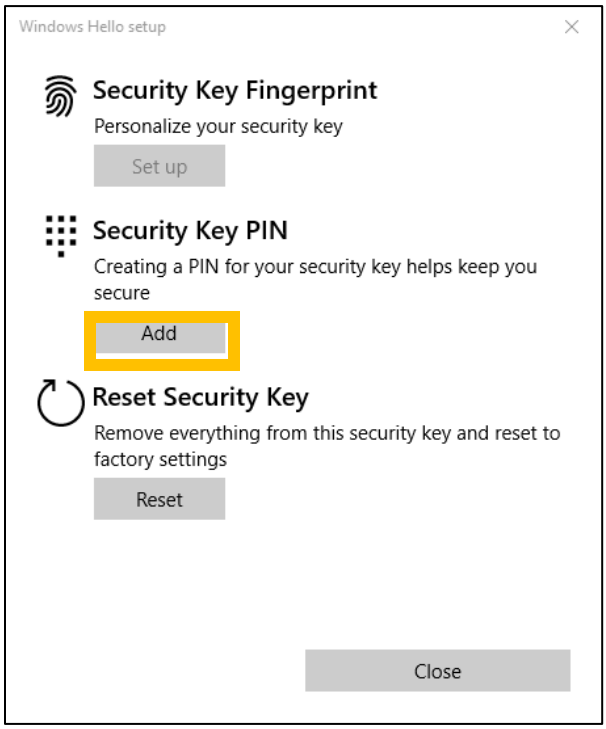
Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

Step 3: Insert the security key and touch the key



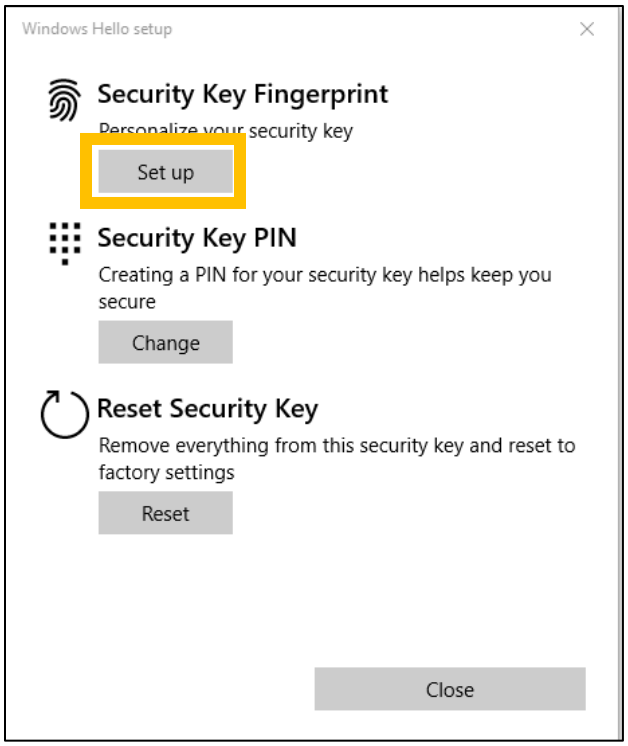


Step 4: set up PIN first

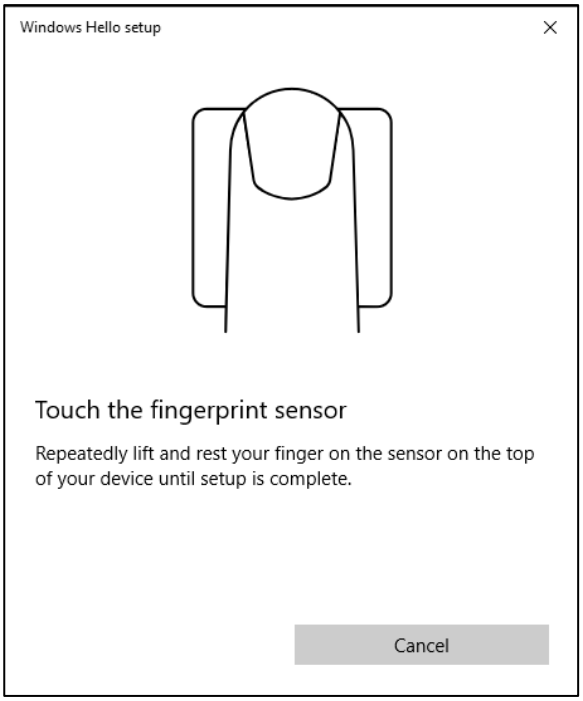


Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

Step 5: Now, you are ready to enroll the fingerprint.

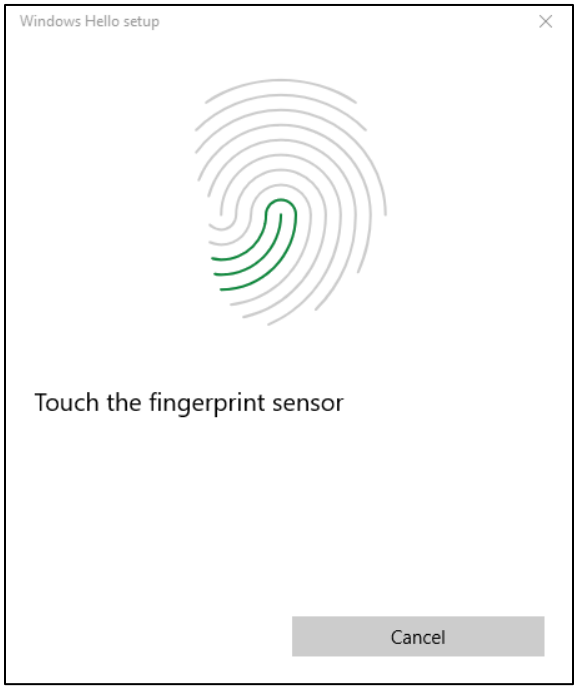


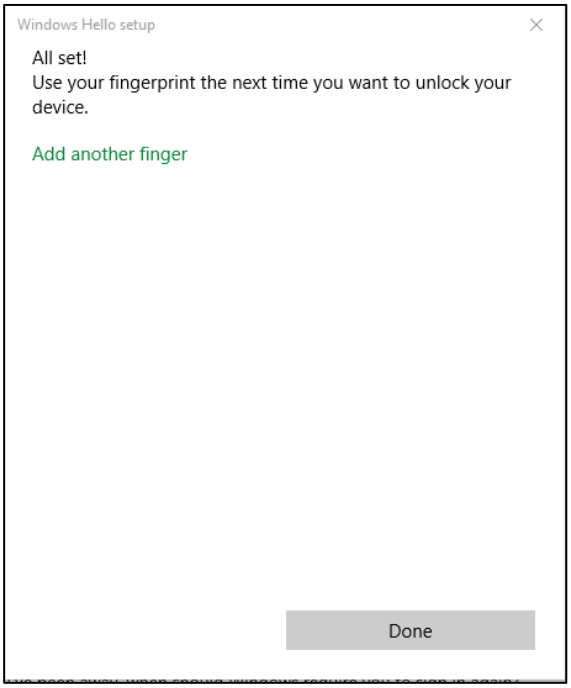
Need PIN authentication for fingerprint enrolment.



Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

Scan your fingerprint multiple times until done.





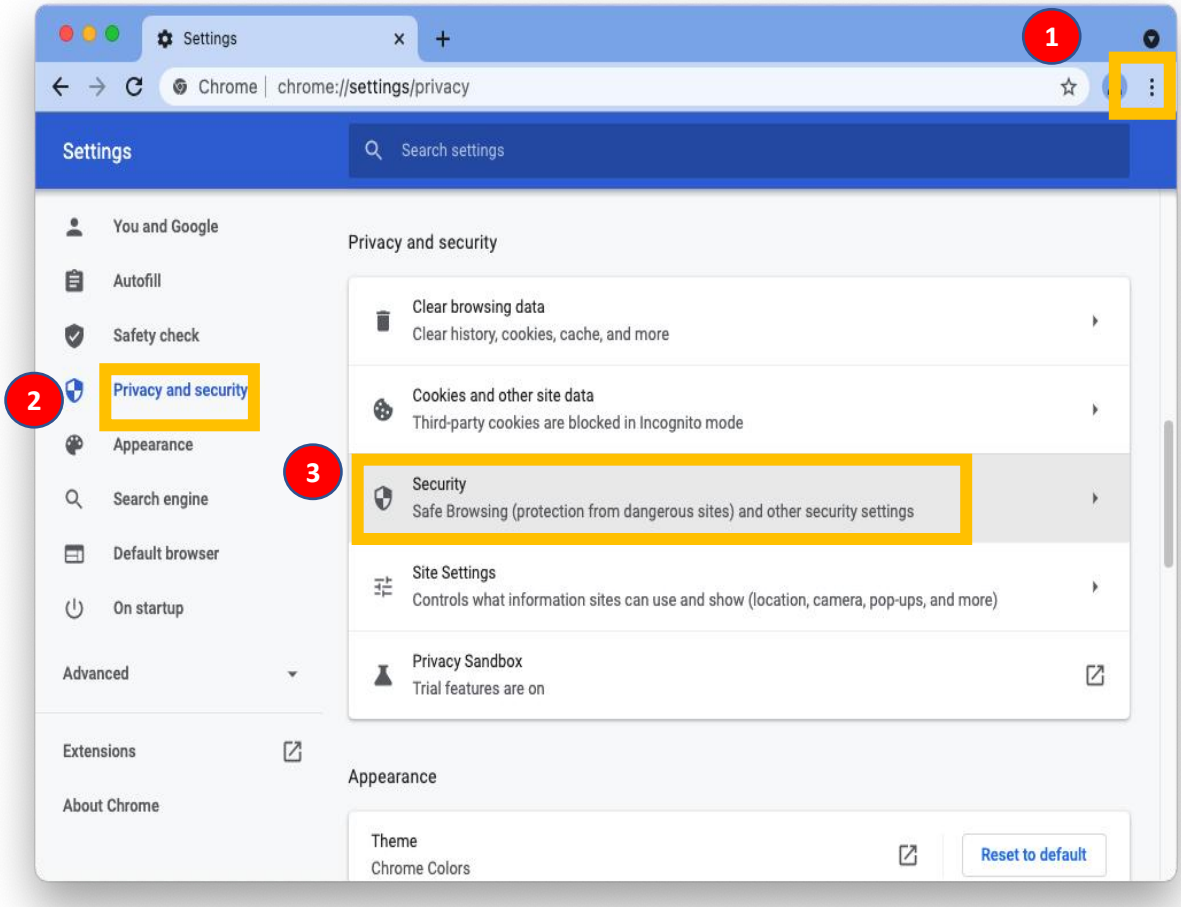
Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

3. Security Key Fingerprint Enrollment (MacOS, Linux)

Note:

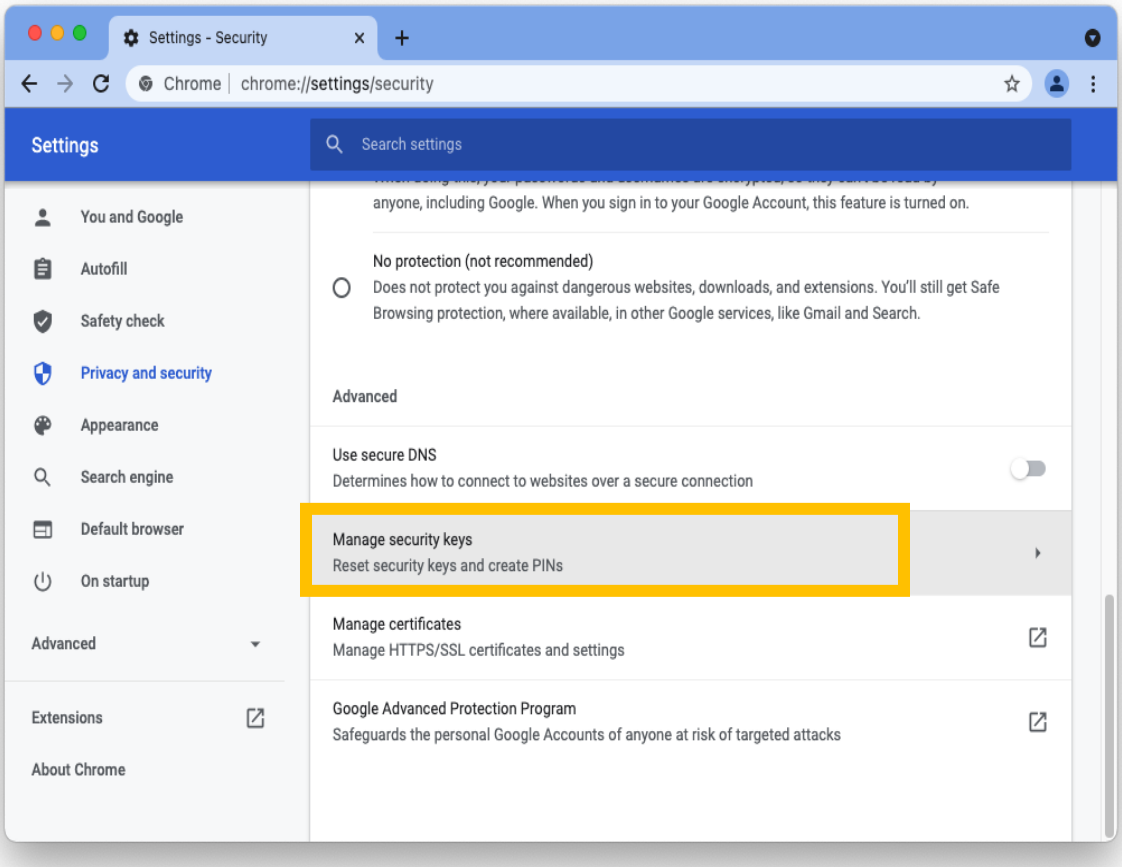
We recommend using the Chome web browser for fingerprint enrolment with a Google account.

Step 1: After login into the Chrome browser with ID and password, click ① "Customize and control Google Chrome," then ② "Privacy and security," and ③ "Security."



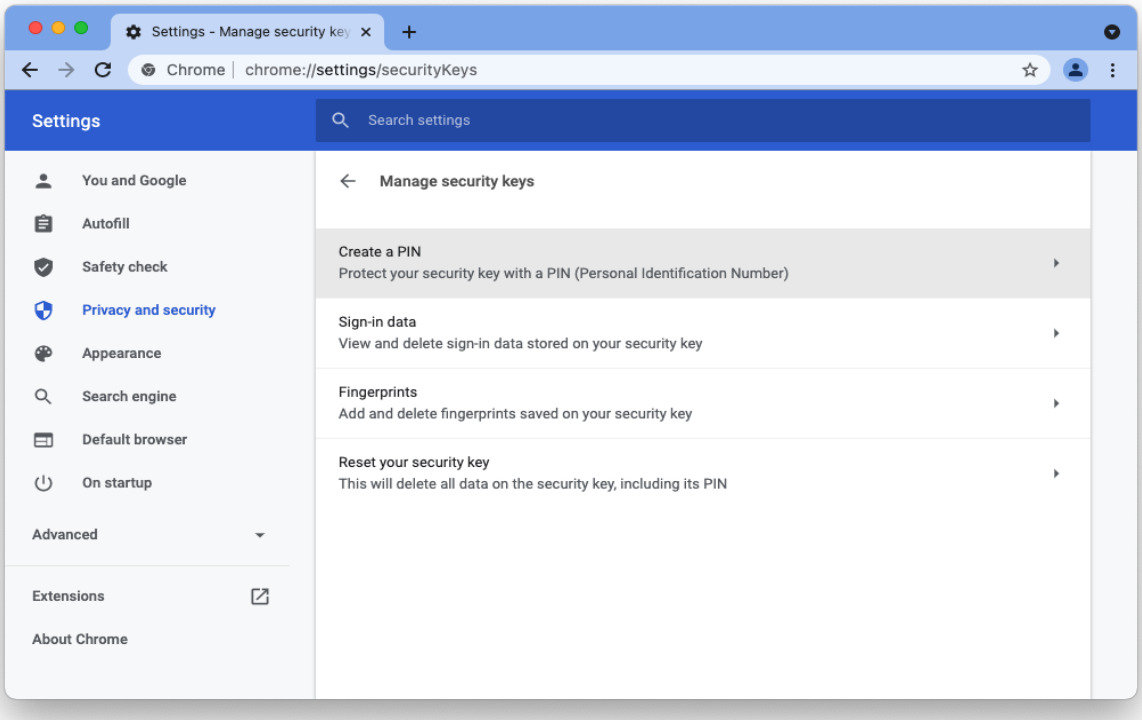
Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

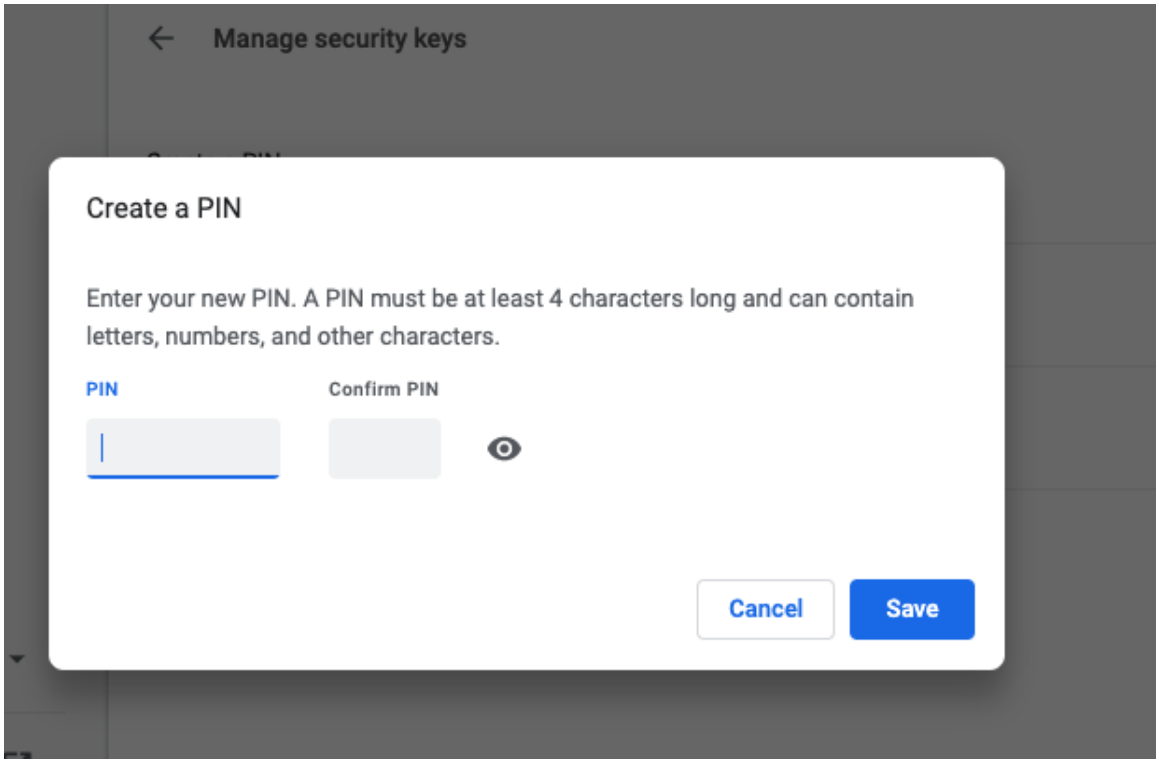
Step 2: click "Manage security keys"



Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

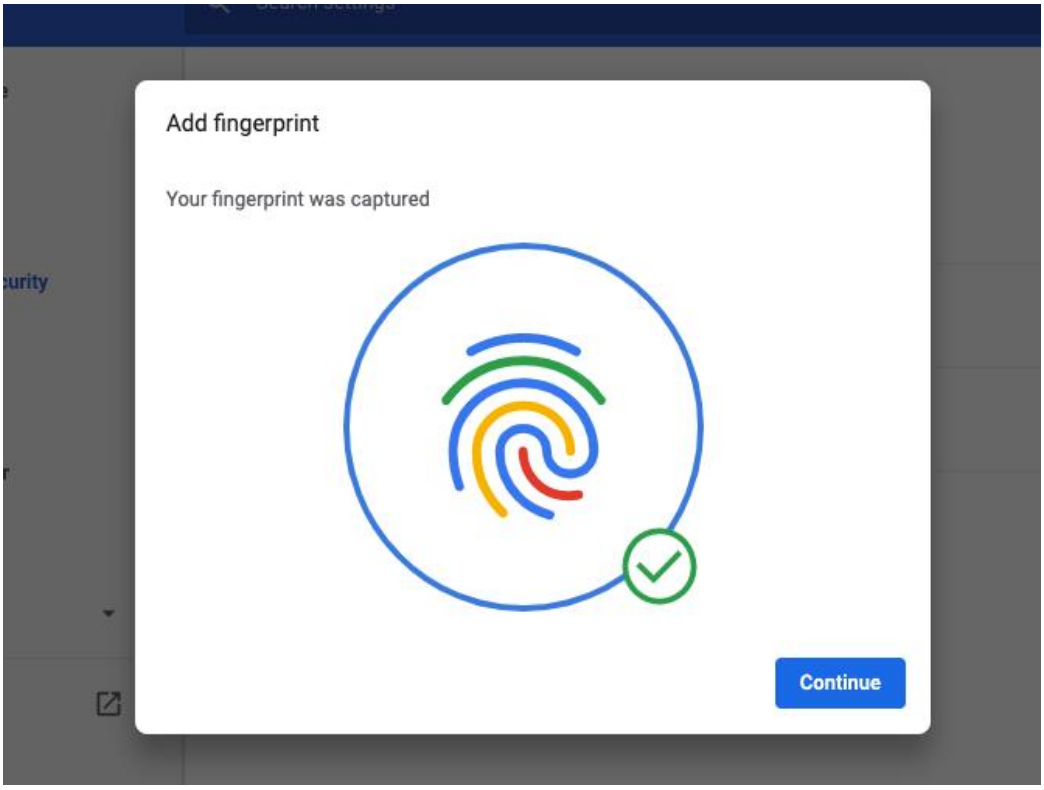
Step 3: Create a PIN

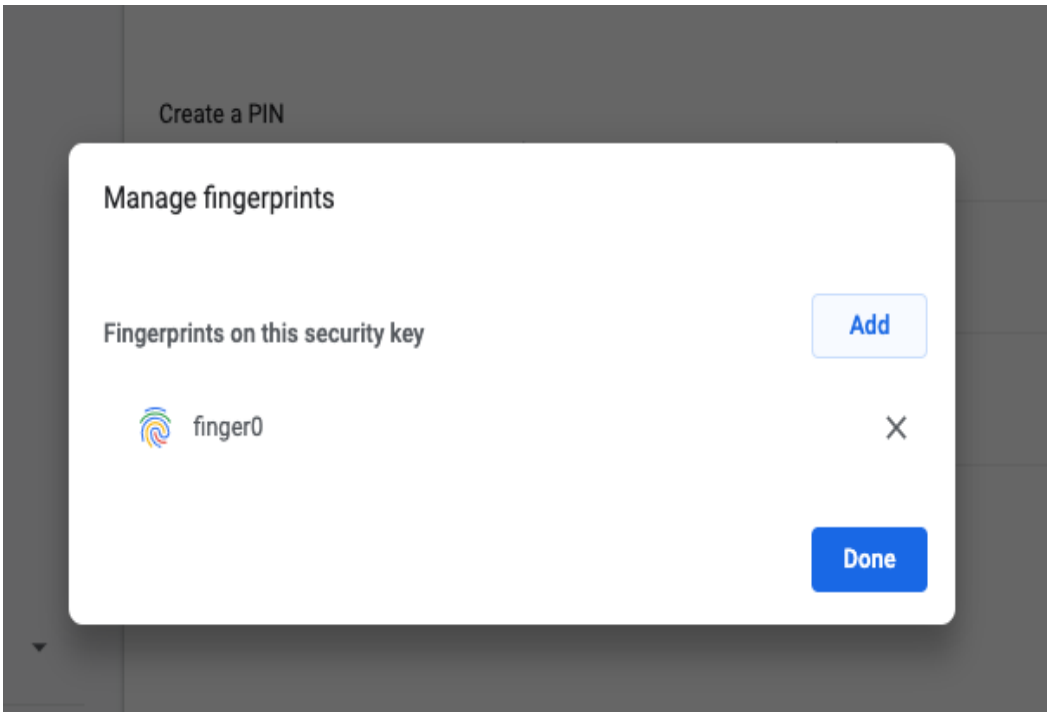




Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

Step 4: Enroll fingerprints



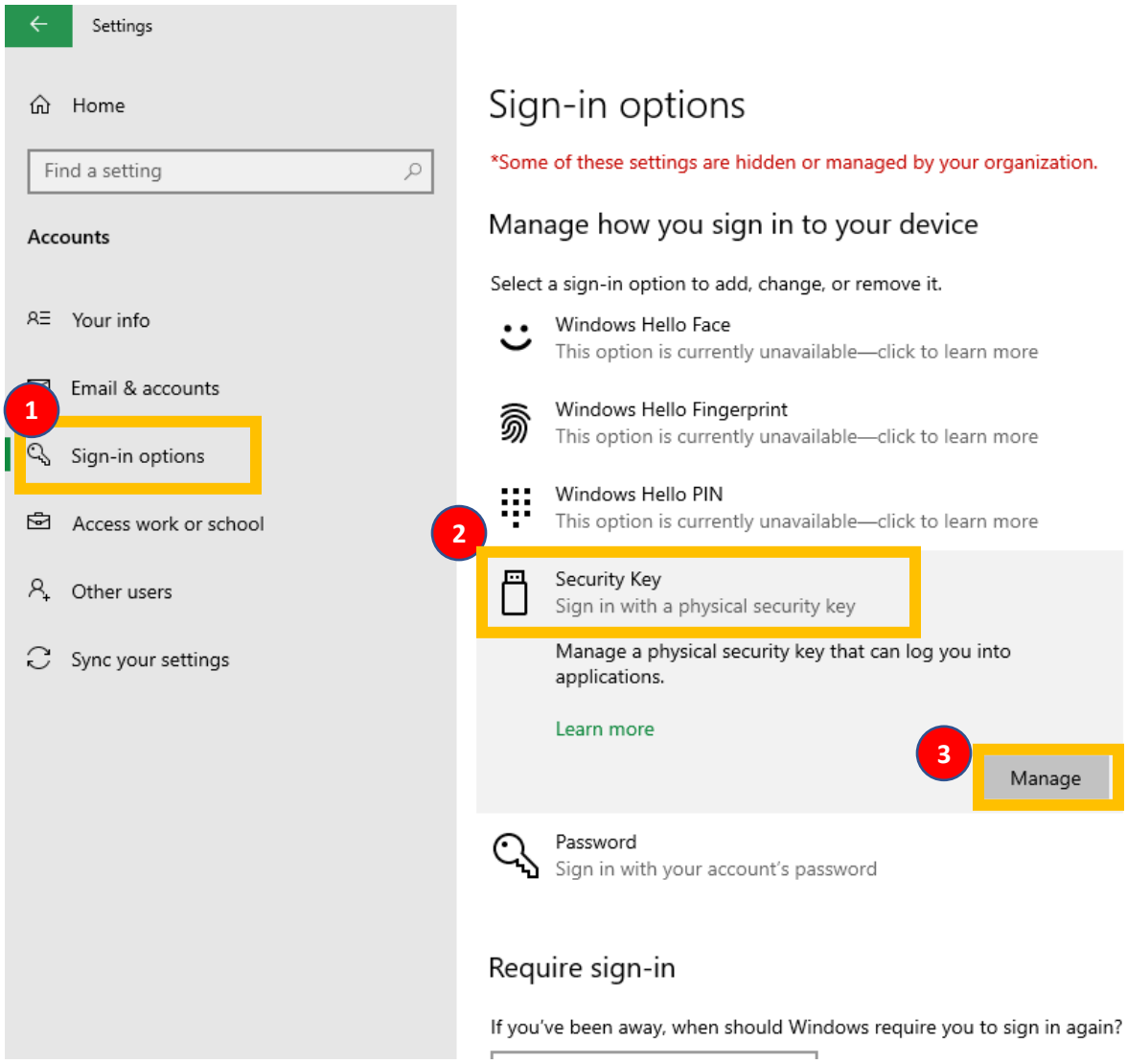


Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

4. Security Key Fingerprint Removal Procedure

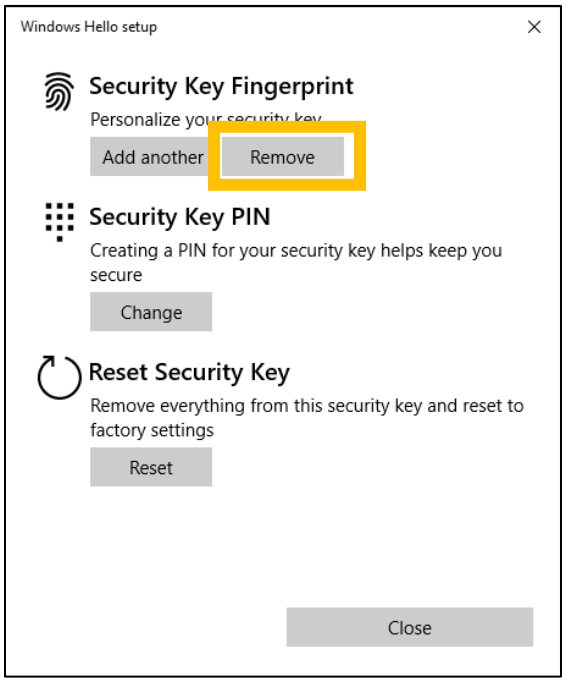
1. Fingerprint removal (Windows10)

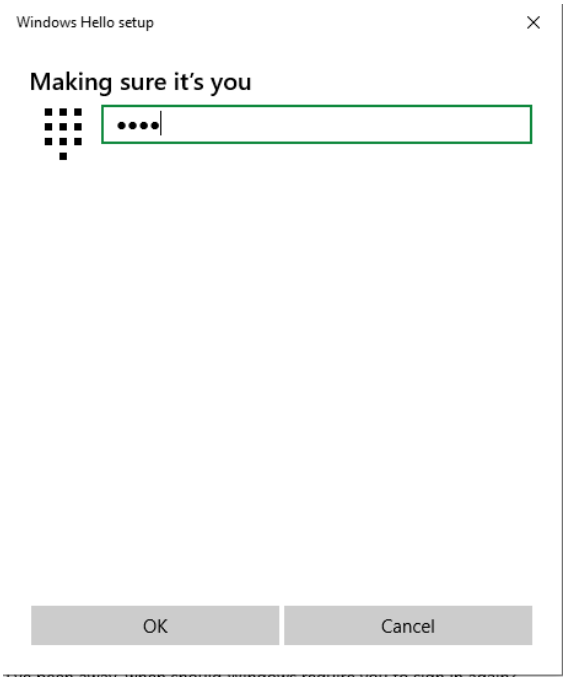
Step 1: Take the same steps (first 2 steps) as the Fingerprint enrolment



Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

Step 2: select "remove" and type PIN for confirmation

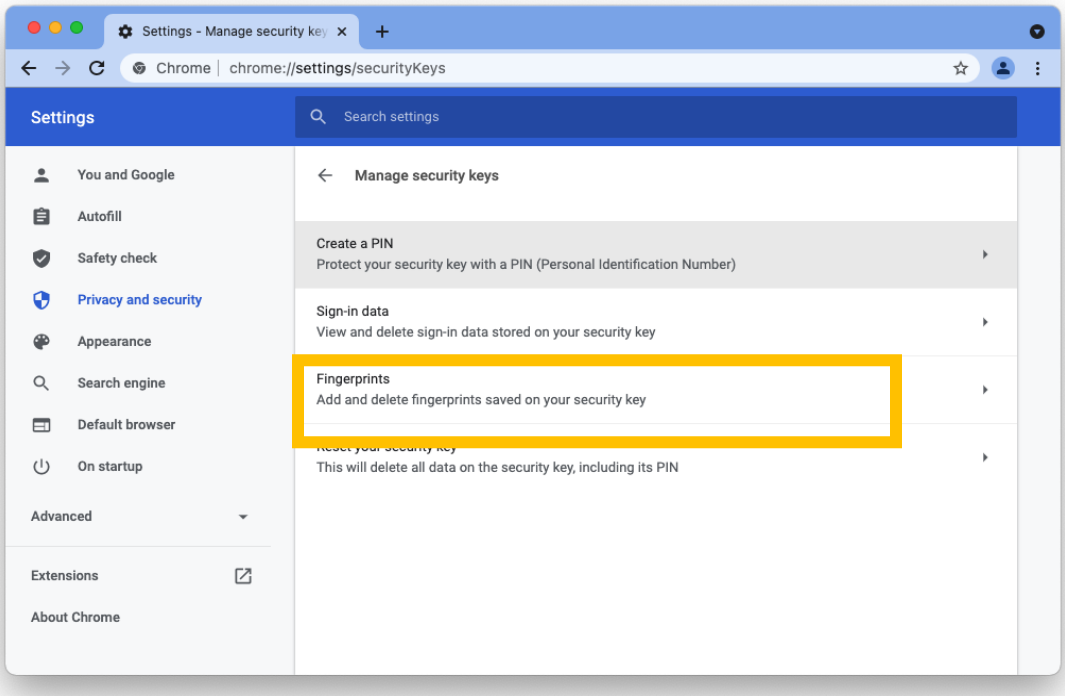




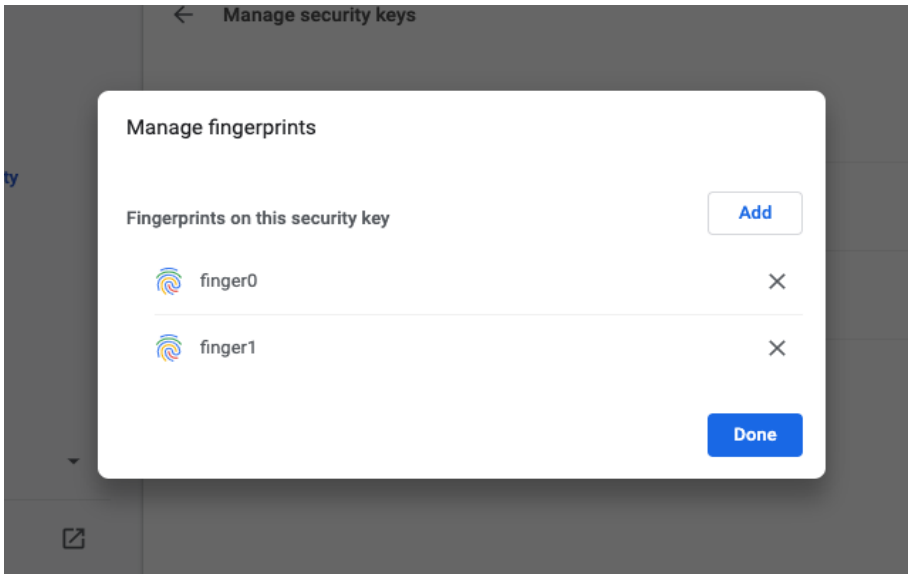
Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

2. Fingerprint Removal (MacOS, Linux)

Step1: Take the same steps (steps 1 and 2) using the Google Chrome browser. Please note that you need to login into your Google account with your ID and password.



Step2: remove the fingerprint from the list by clicking one of the x's



Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

5. Security Key PIN

1. PIN (Personal Identification Number)

The PIN is similar to the password but used differently. The password is a shared secret between the user and the server. The client system asks the user to type in the password and sends the information of the password to the server for verification. Unlike the password, the PIN is not sent to the server; a PIN is a shared secret between the user and the security key. Therefore, the verification happens at the device, not the server.

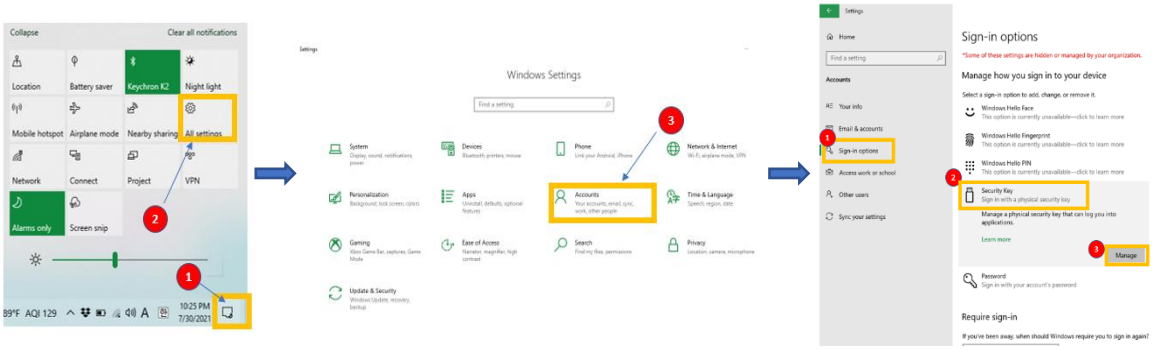
The PIN is needed for fingerprint enrolment and modification. It is also used for backup authentication when fingerprint authentication failed.

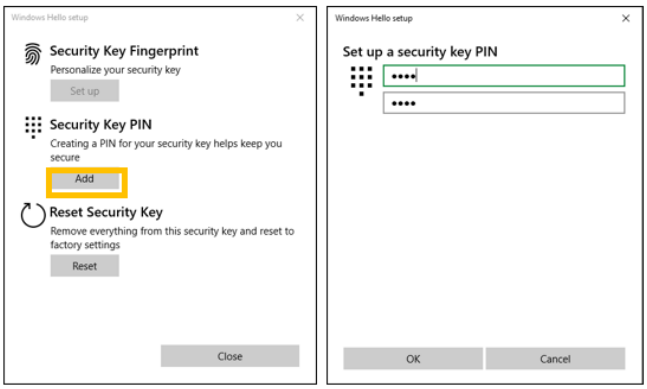
We recommend that the user use a complex combination of digits and letters to protect the user from being leaked.

2. PIN setup

The initial PIN setup is exactly the same as described on pages xx to yy.

Open Setting →Sign-in Option → Security Key

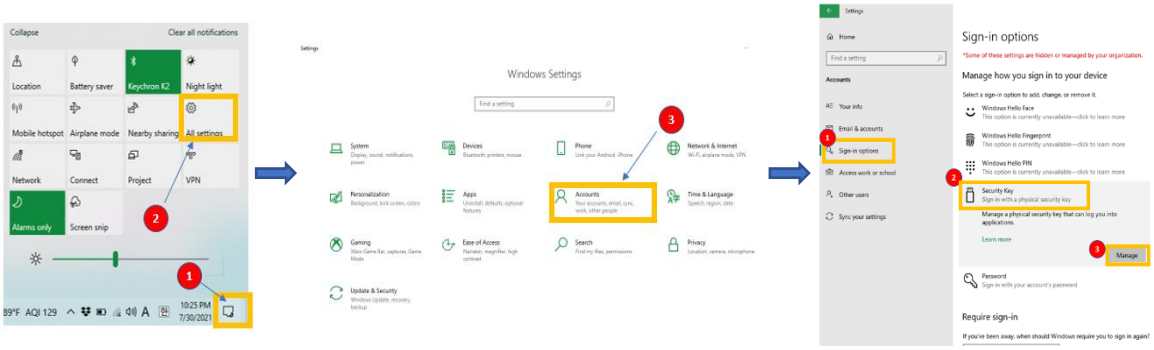




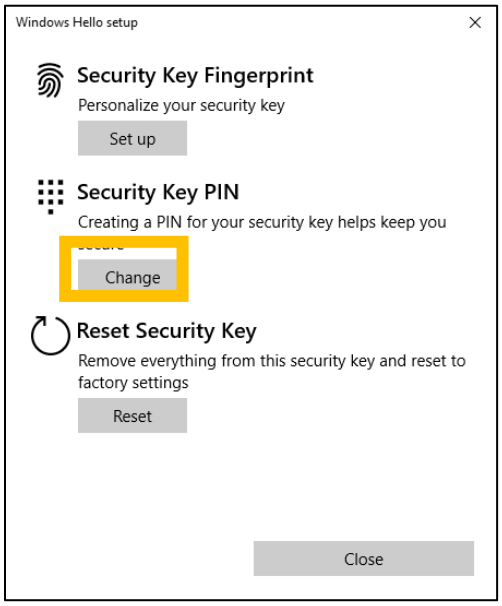
Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

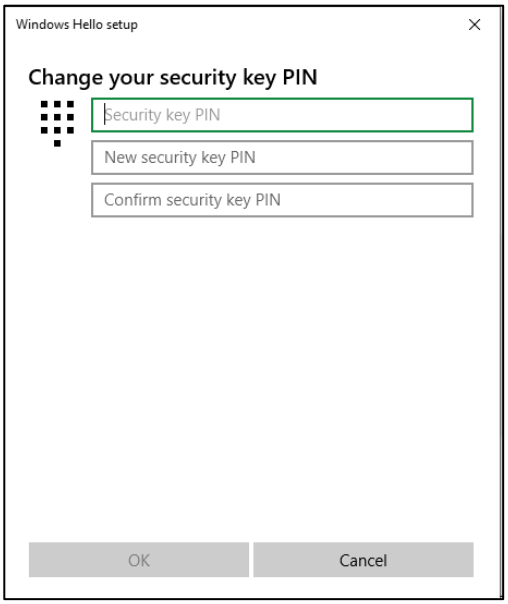
3. PIN information change

Open Setting →Sign-in Option → Security Key



One can change the Security Key PIN by clicking "Change." The user needs to input the existing PIN and new PIN twice.

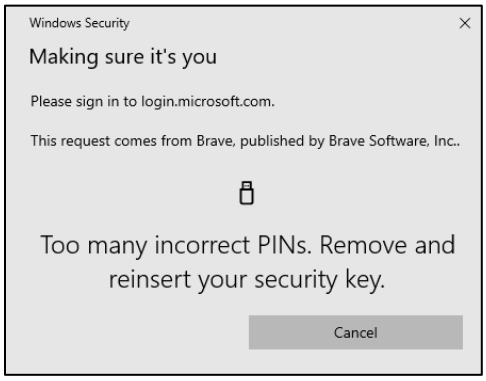




Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

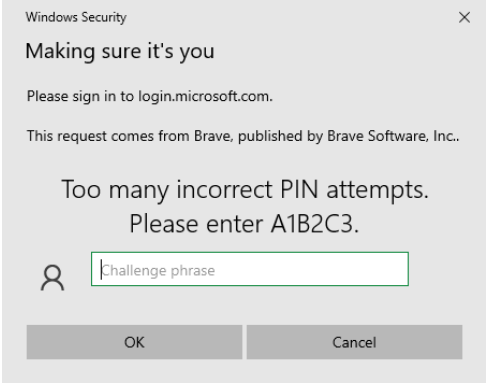
4. PIN Authentication Failure

When the user fails to type the correct PIN four times consecutively, then the below message appears.



The user needs to pull out and reinsert the security key and type the correct PIN.

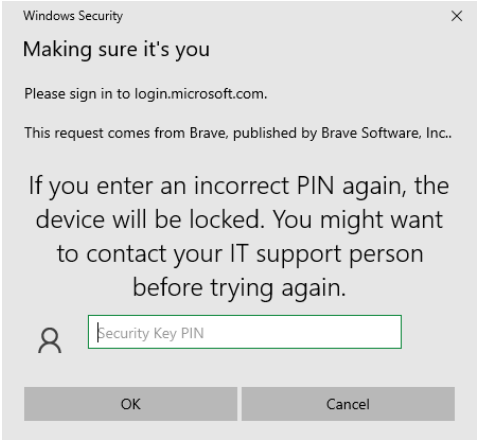
However, if the user continues to type in incorrect PIN more, the user will get this message.



The above message is a mechanism to make sure that the keyboard input is correct.

If the user types A1B2C3 correctly, the system assumes that the keyboard is working correctly.

Then, the final warning message pops out.

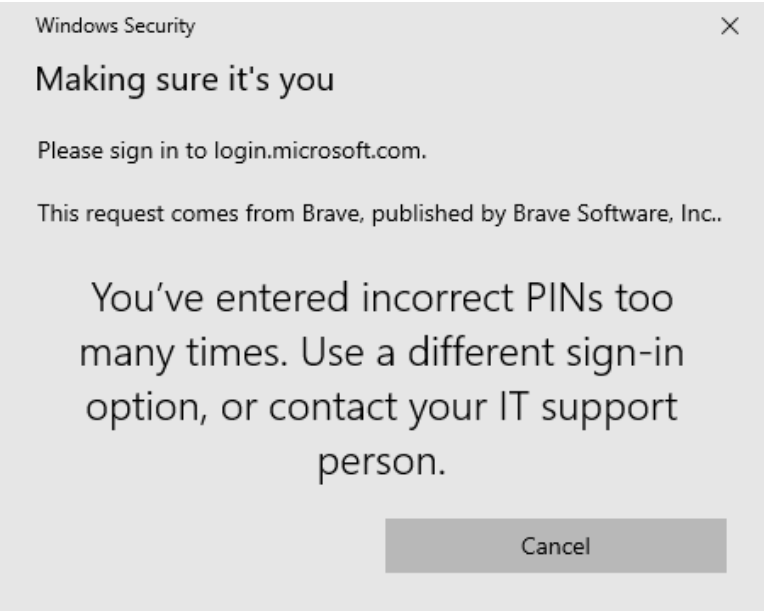


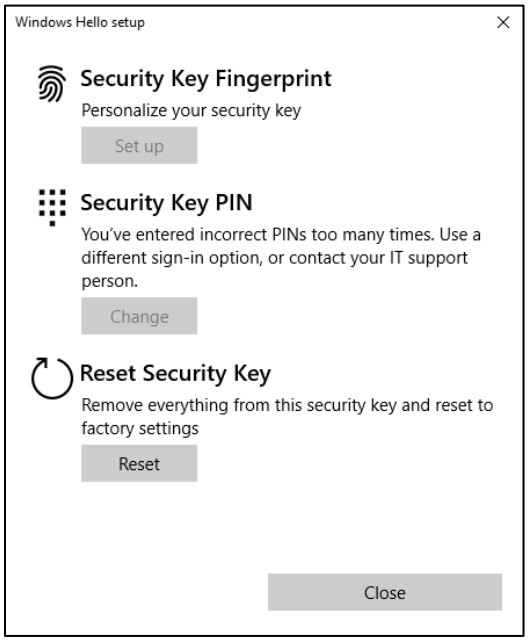
Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

Warning!

There is no recovery mechanism when the device (security key) is locked due to multiple incorrect PIN attempts. Once the security key is locked, then the key cannot be used at all. The only way to make the security key operational is to do a "factory reset" of the security key. A factory reset removes the existing data and all previously created credentials.

If the user types the incorrect PIN for the last time, the security key is locked.

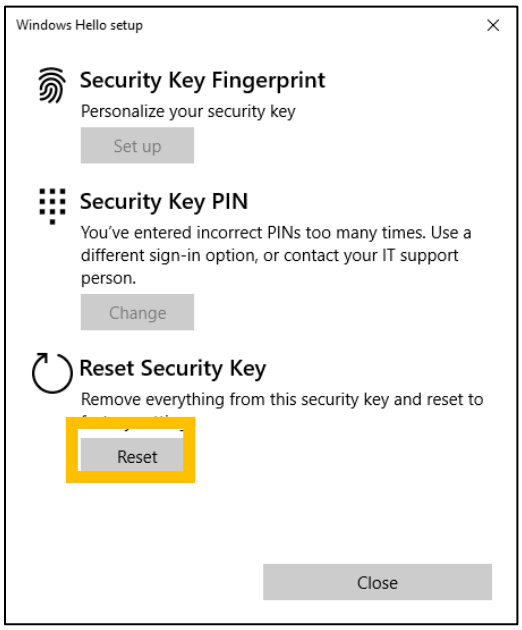




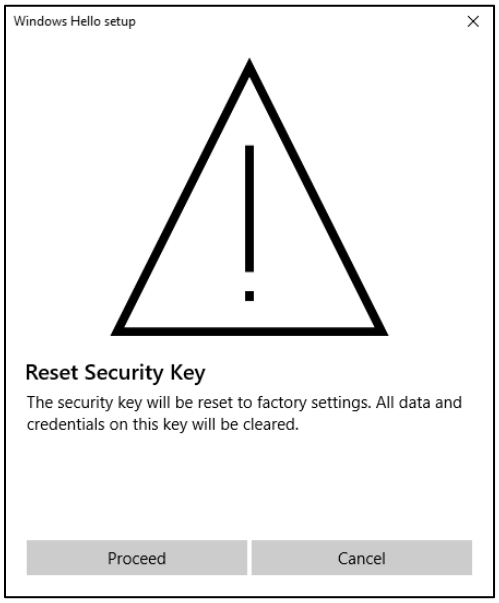
Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

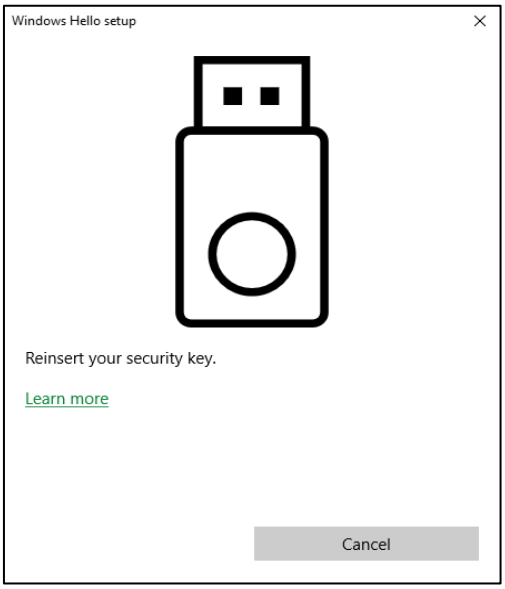
5. Security Key Factory Reset

From Settings → Sign-in Options → Security key



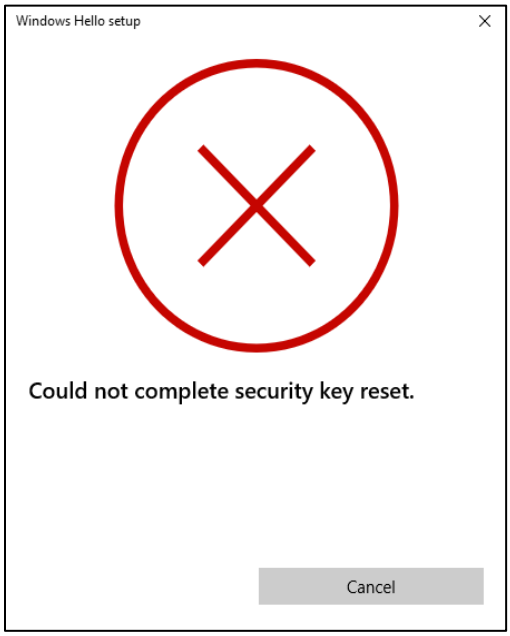
The following are the steps that you need to take for a factory reset.



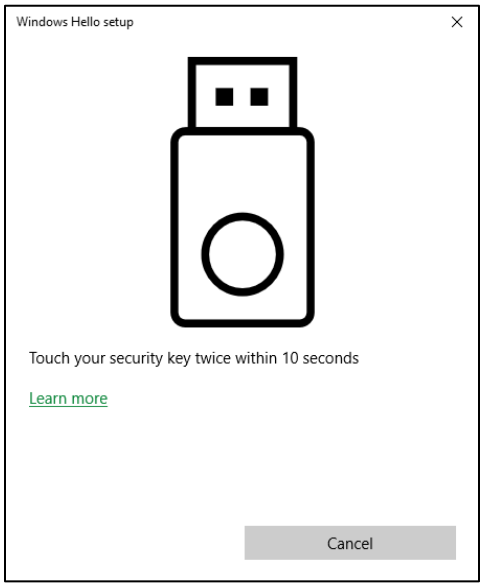


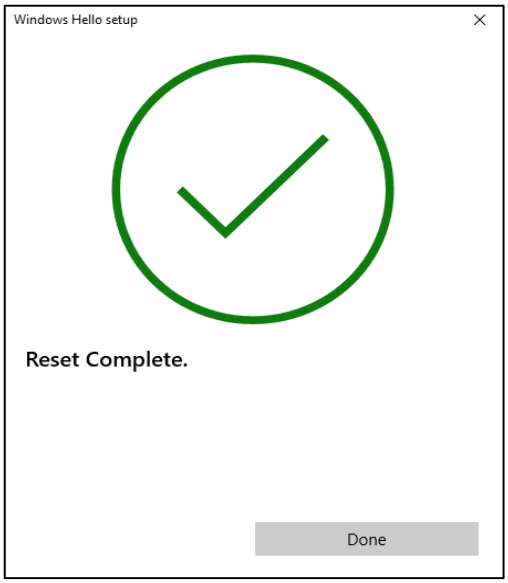
Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

The user needs to reinsert the security in 10 seconds to perform a factory reset. Otherwise, the factory reset procedure will not complete.



Once the above message appears, the user needs to restart a factory reset again.





Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

Note:

- **The security key will be locked after 15 consecutive failed attempts of fingerprint authentication and followed by seven failed PIN authentication.**
- **The security key LED is solid RED all the time; the key is locked and cannot be used.**
- **The security key will be of service after a factory reset.**

Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

6. Online usage of the security keys

1. Microsoft Azure AD

a. Azure AD user registration

This is for individual registration of the organization with Azure AD accounts.

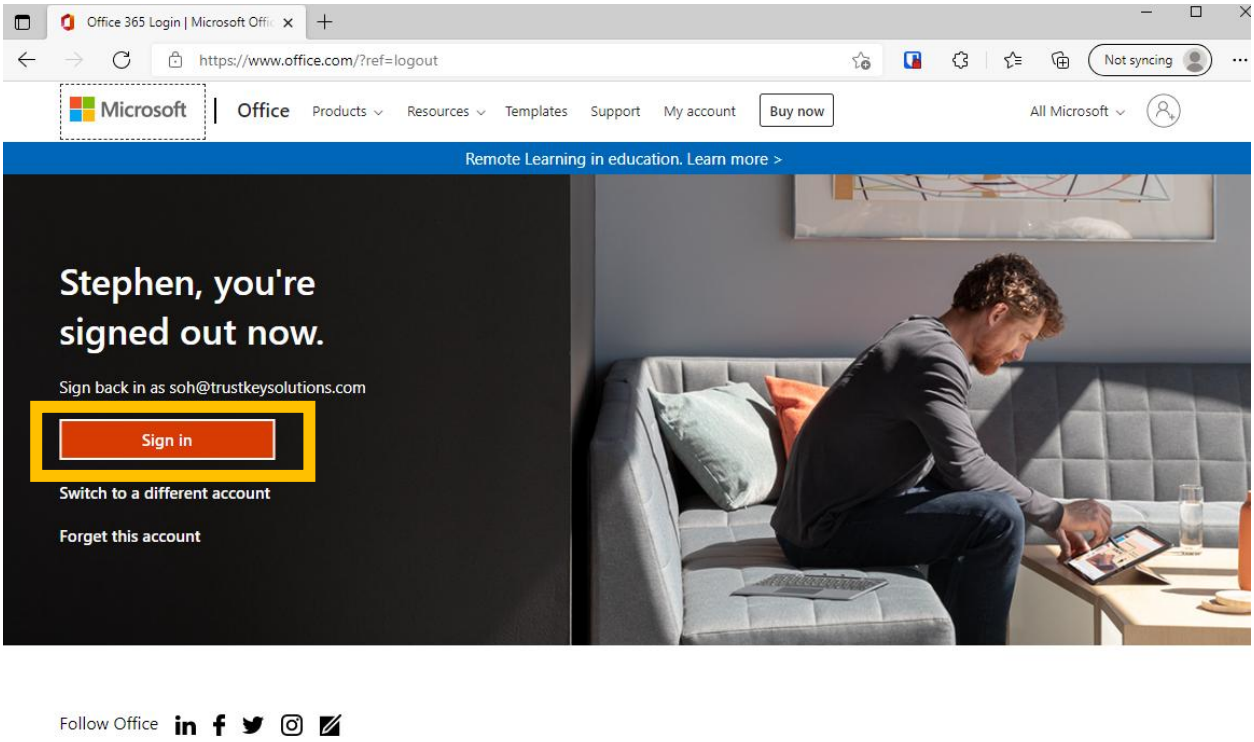
The steps shown below are the case that a user uses www.office.com for the security key registration. The user can use one of the following sites for registration.

Registration sites:

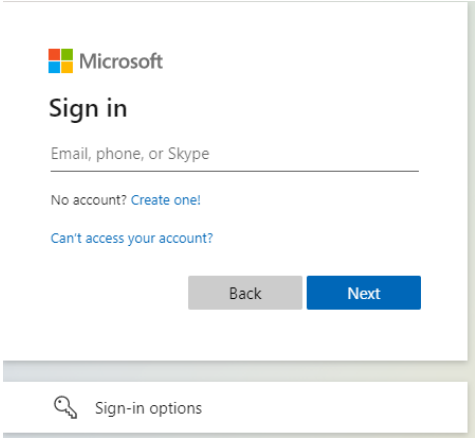
https://www.office.com

https://login.microsoftonline.com

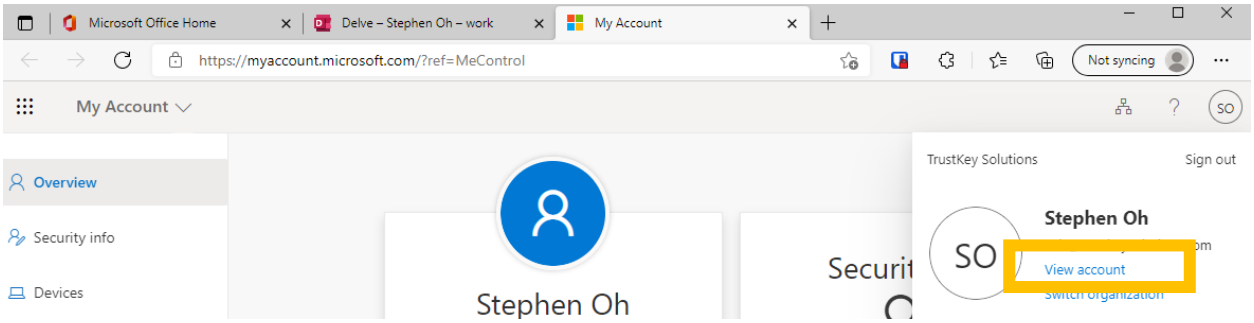
Step 1: The user needs to sign in at www.office.com using the user's ID and the password.



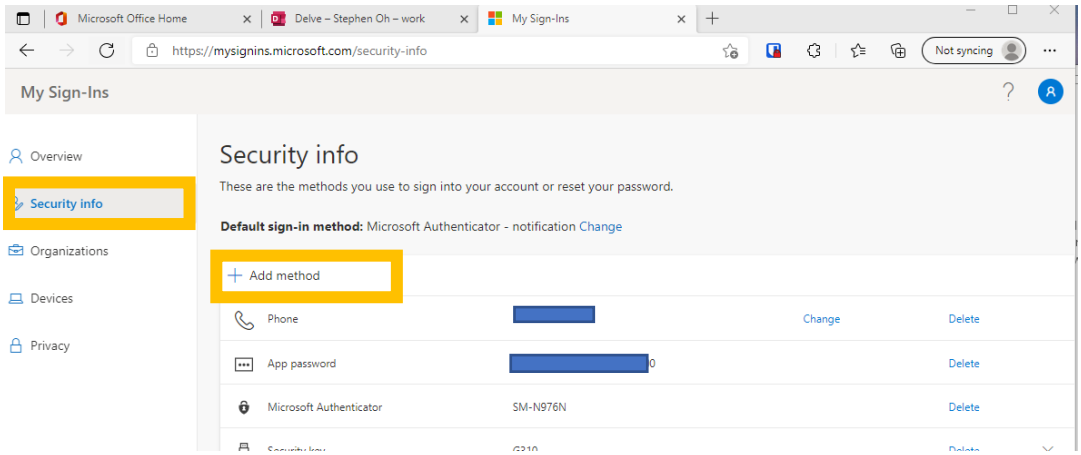
Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved



Step 2: for the security key registration, click "View Account"

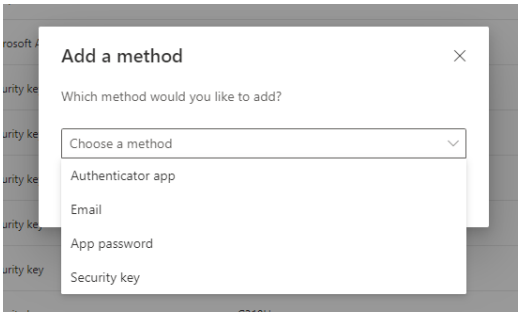


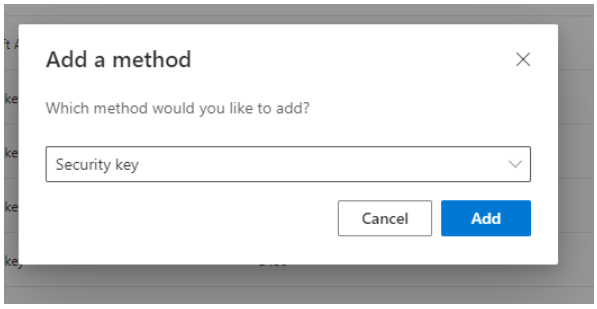
Step 3: select "Security info" and select "+Add method"

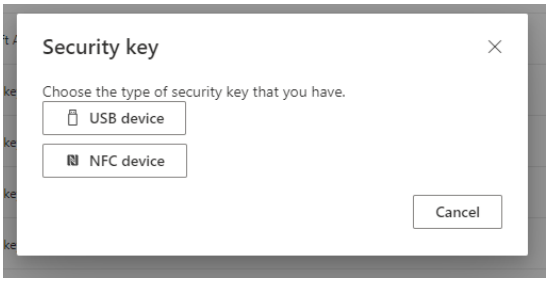


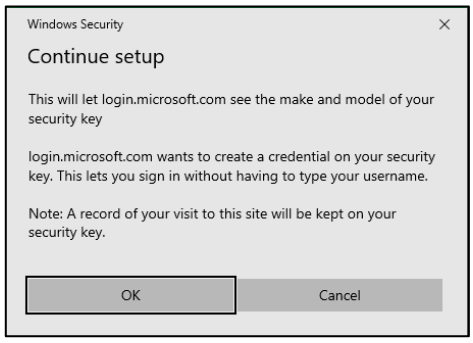
Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

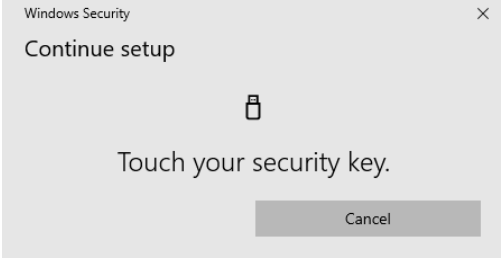
Step 4: follow the registration flow



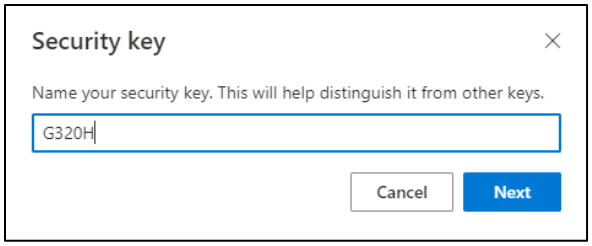




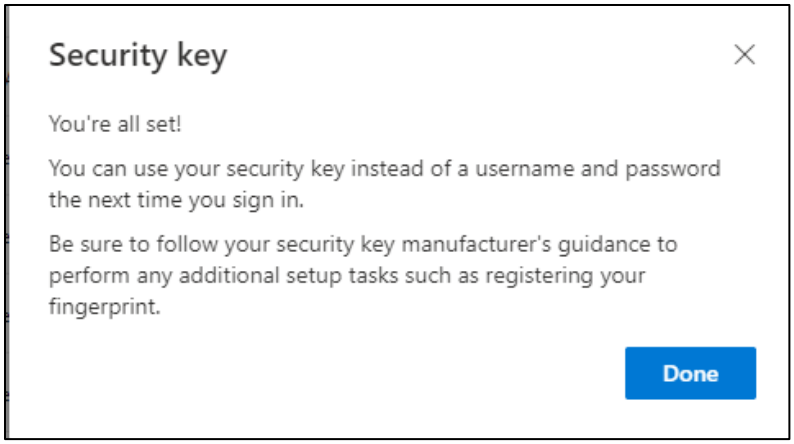




Step 5: the user needs to name the security key to differentiates the key from other keys since the user can register up to 10 security keys.

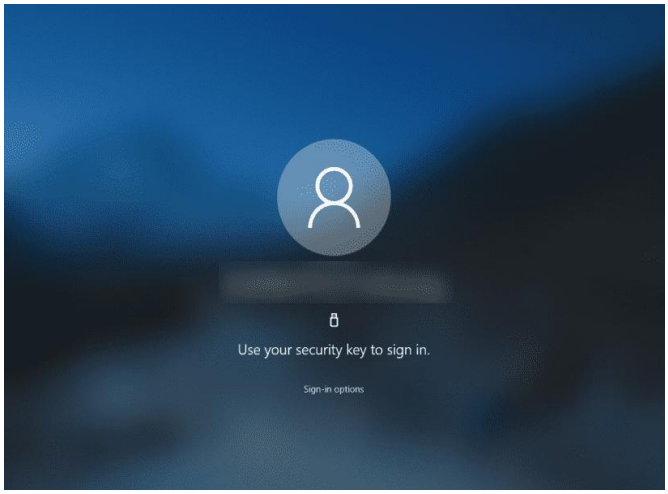


Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved



b. Sign in Windows (Azure AD joined)

As the users registered the security key with their Azure accounts, the IT admin needs to configure the system so that users can sign in to their Windows PC with the security keys (example: setup at Microsoft Intune)



Note: Please refer to our blog here for more information.

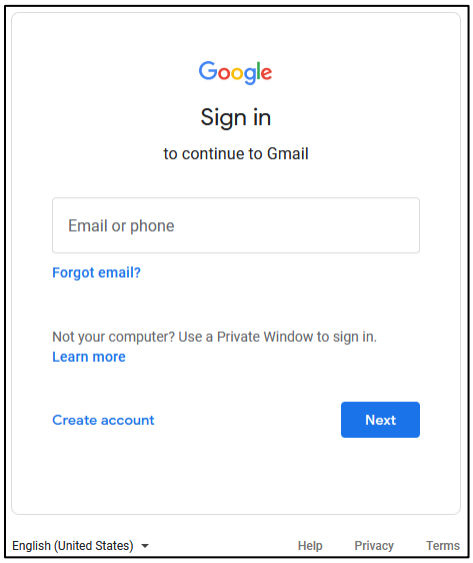
(https://www.trustkeysolutions.com/blog/preview-of-fido2-security-keys-for-hybrid-azure-ad-joined-environments/)

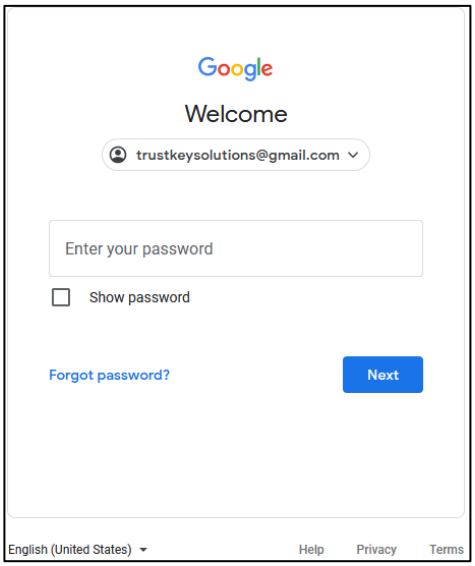
Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

2. Google G-suite

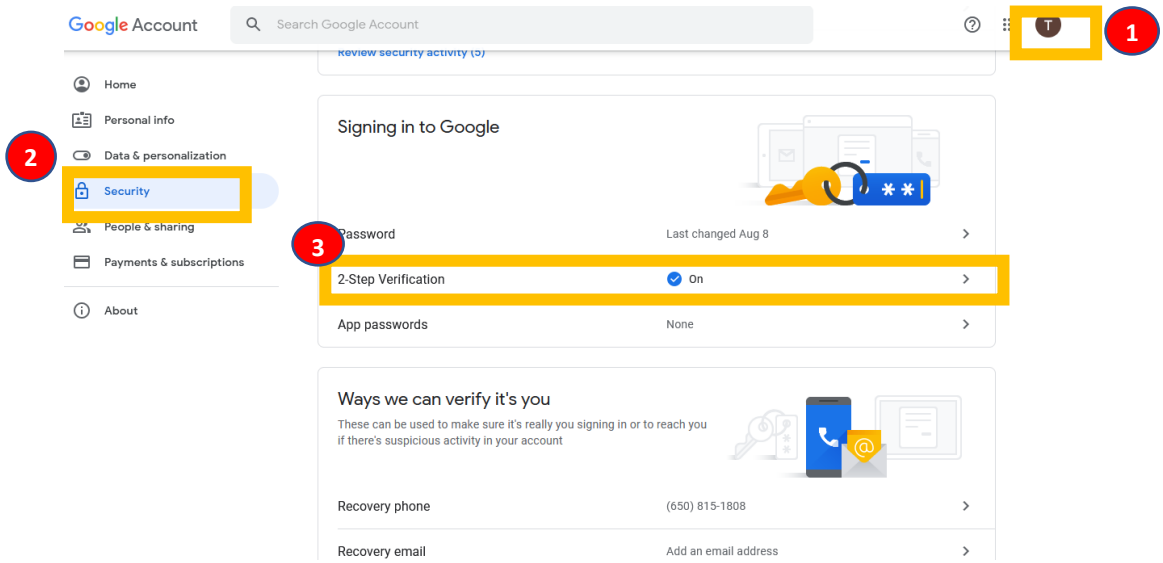
Security Key registrations for Google's G-Suite are described in this section. Note that Google is using the security key as the second-factor authentication. The user needs to type ID and password and use the security key to sign in.

Step1: The user needs to sign in with the existing account ID and the password.



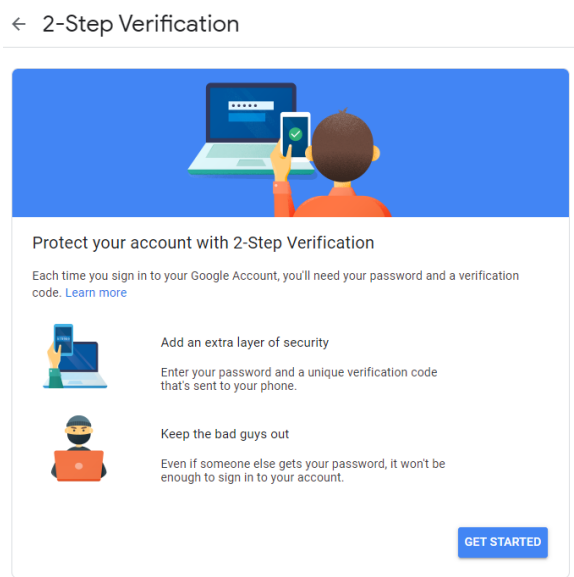


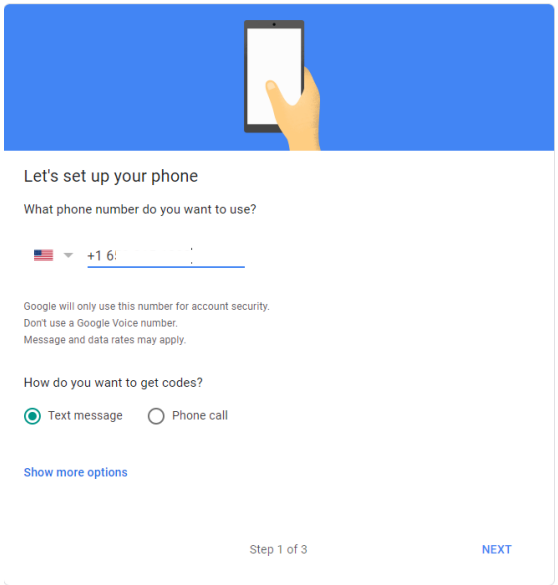
Step 2: click ① the upper right corner and select ② "Security," and ③ turn on "2-Step Verification."



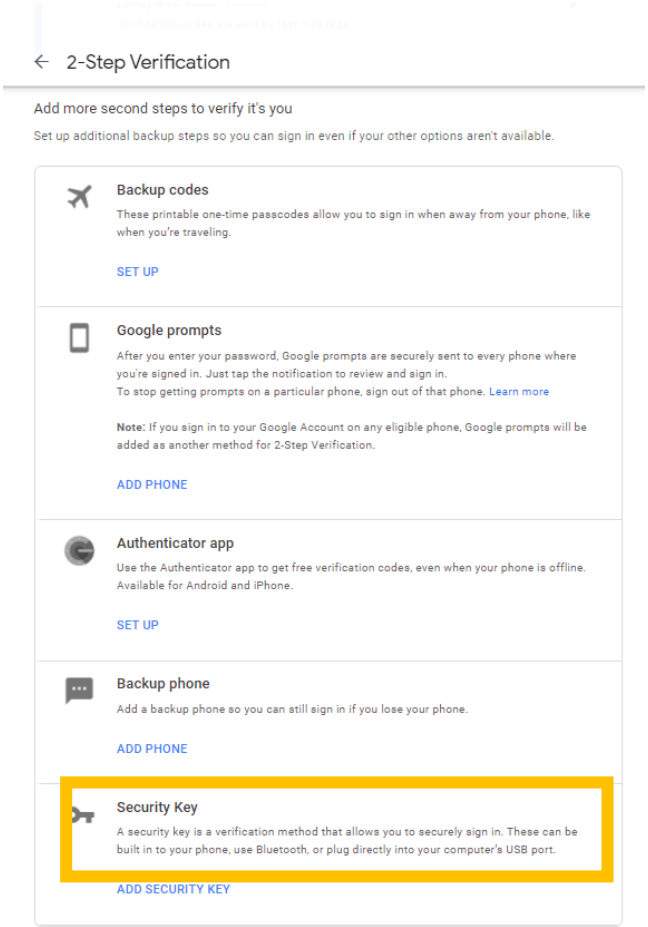
Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

Step 3: Need to initial 2-Step verification with your phone



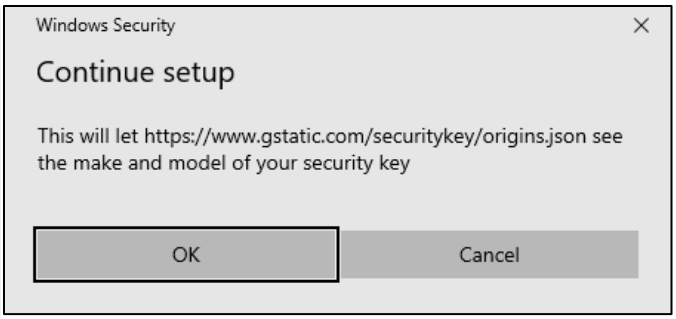


Step 4: The user needs to add the security key for 2-step verification

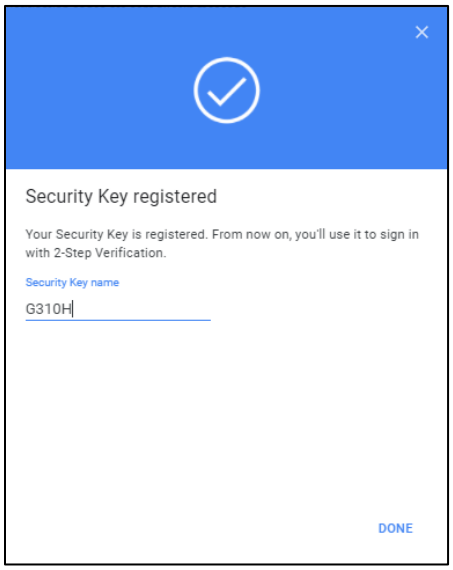


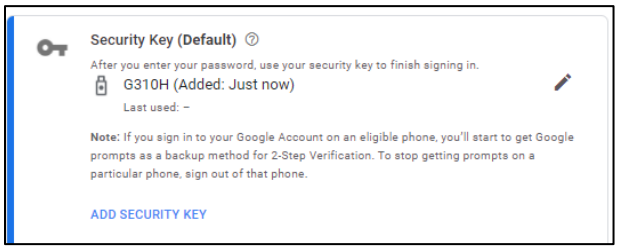
Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

Step 5: follow the browser's instructions



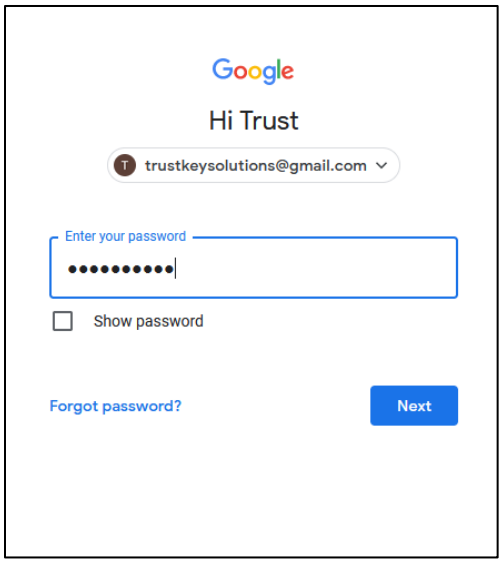
Step 6: After successful registration, the user needs to name the key

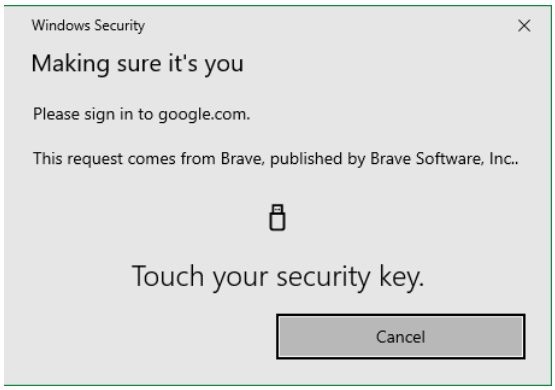


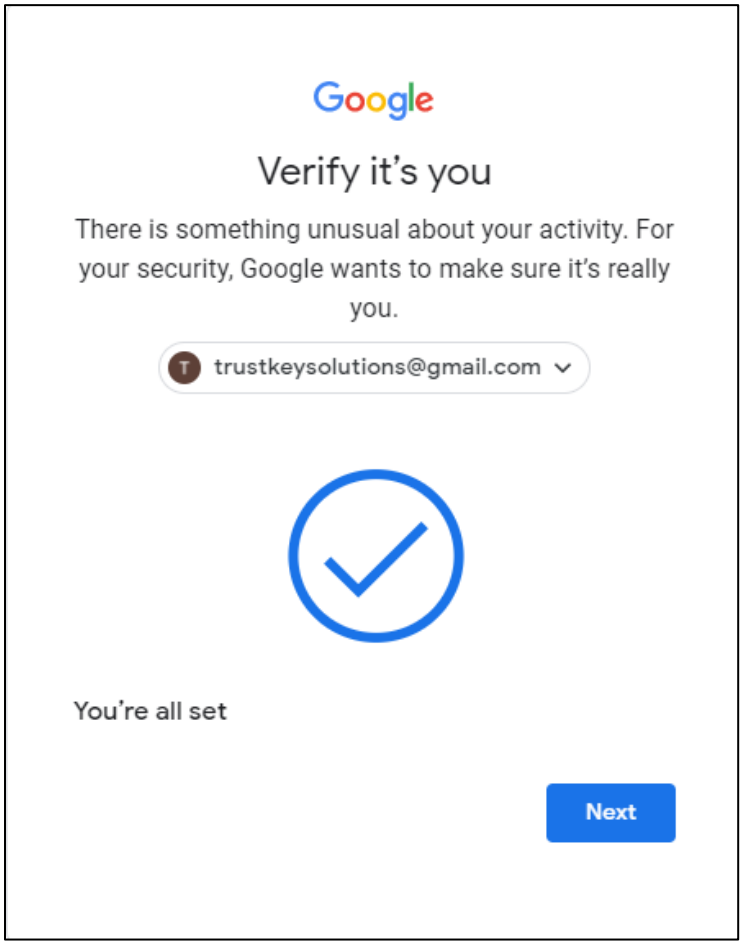


Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

Step 7: The user now can sign in Gmail with the security key.







Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

3. Bank of America USB Security Key Experience

Bank of America allows customers to increase the protection of online accounts with new Security Key feature. Once your USB security key is set up, it serves as an extra layer of security for adding transfer recipients to your account and for extra security at sign-in.

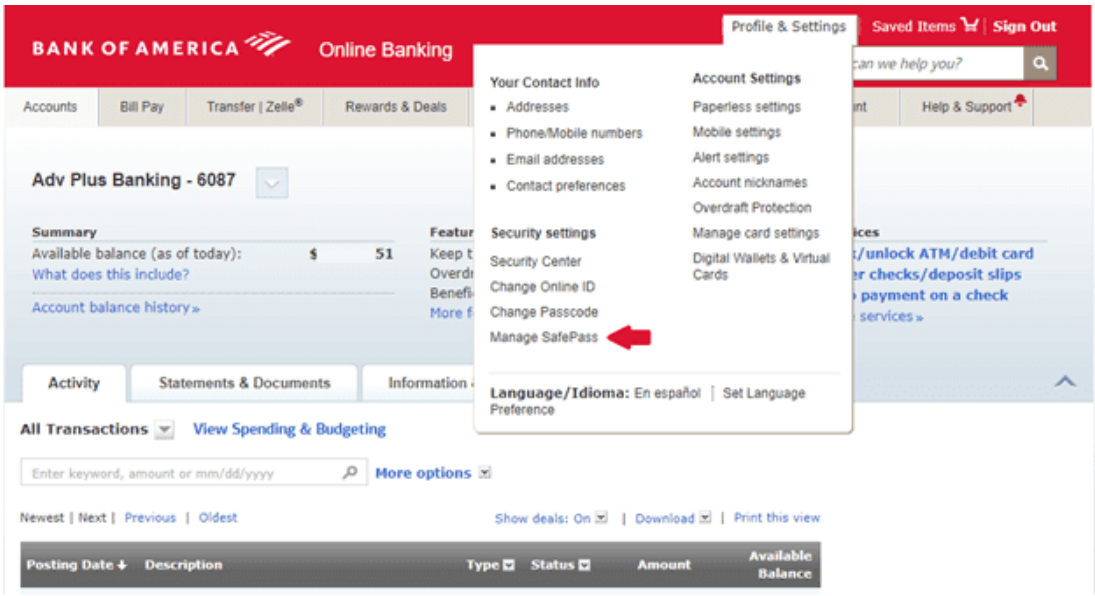
Bank of America allows customers to increase the protection of online accounts with new Security Key feature.

Bank of America has announced that they are replacing SafePass with the new Secured Transfer feature, which allows for USB security key registration and transfer authentication with FIDO security keys. They have also provided the option for many Bank of America customers to sign-in to their online banking account with a FIDO security key.

SafePass has long been Bank of America's solution to provide an additional layer of security against unauthorized transactions. However, SafePass only allows customers to use mobile authentication with a one-time code. With the introduction of the Secured Transfer feature, Bank of America has managed to introduce an even more secure and, most importantly, FIDO-based hardware authentication. As a result, customers are 99.99% protected from phishing attacks and no longer need to worry about their data security.

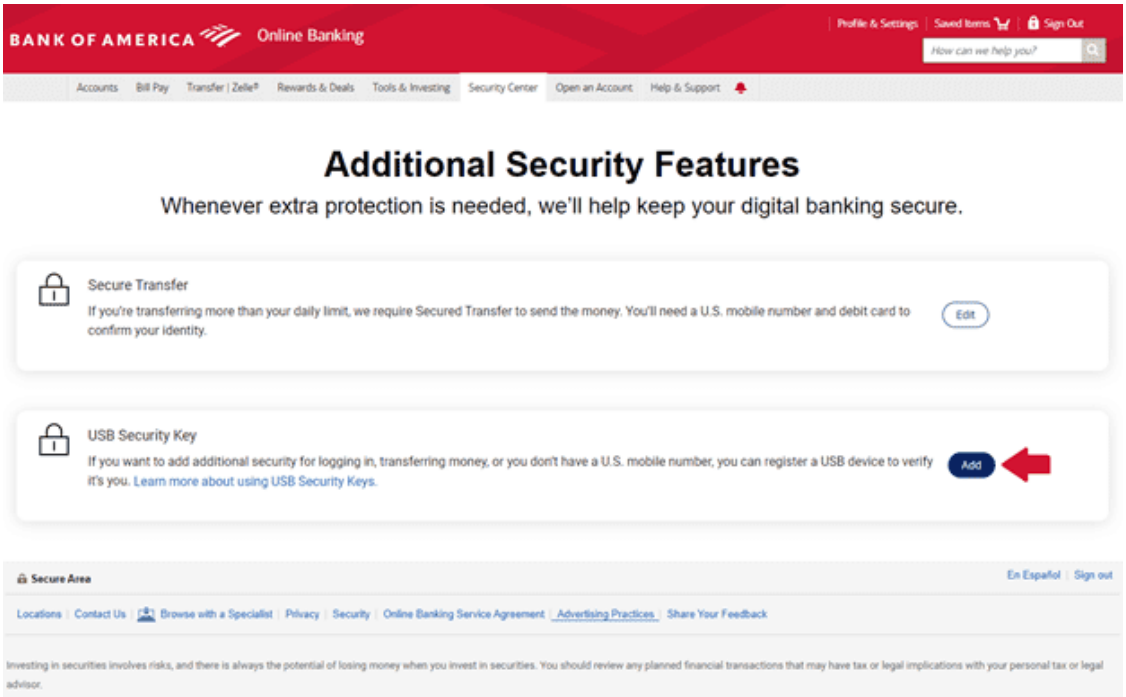
Adding and using a security key is as easy as 1 2 3. Here are the easy steps to adding a security key and using it on successive logins.

Step 1: After logging into your account, select Profile & Settings -> Manage SafePass.

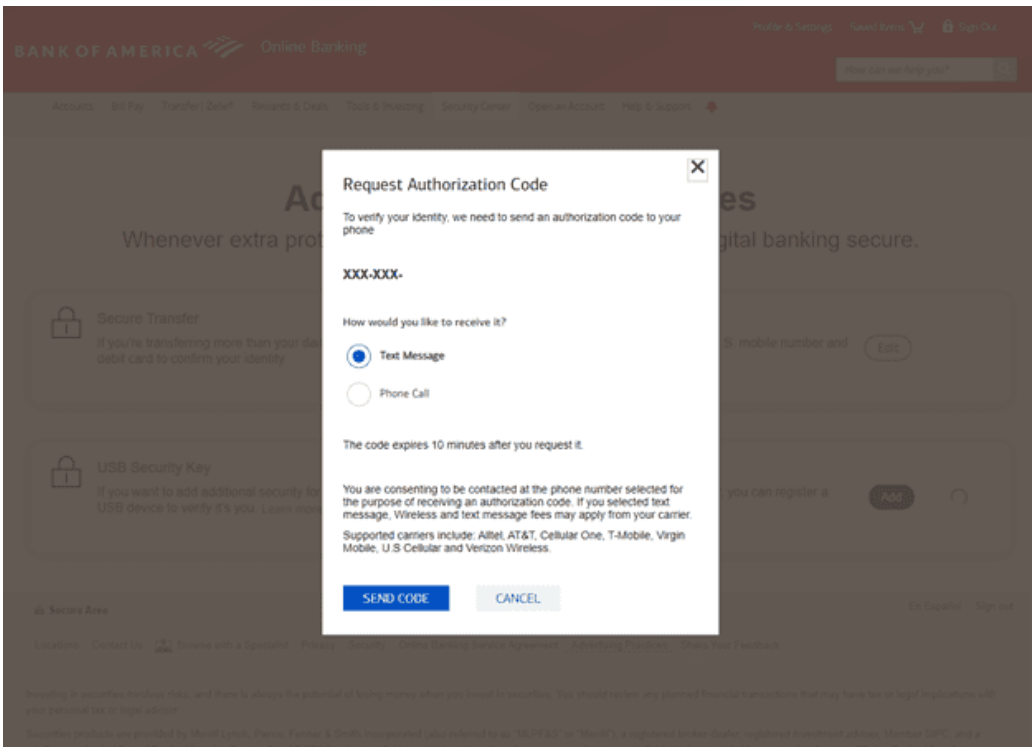


Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

Step 2: Click Add button from the Security Center page.

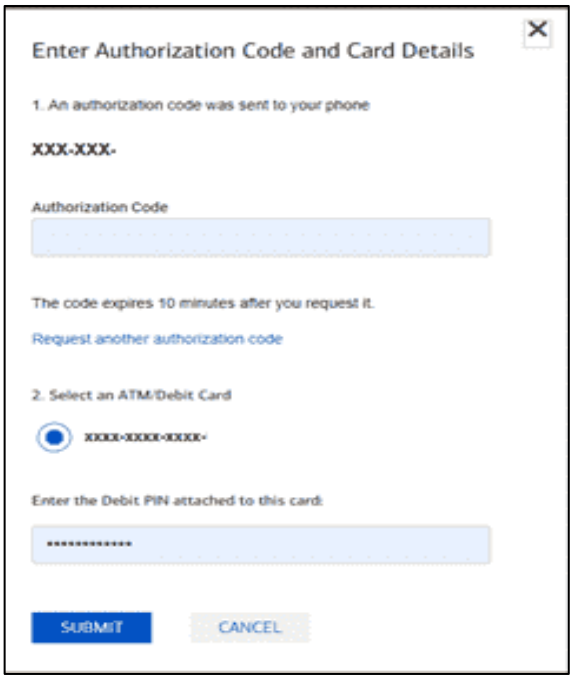


Step 3: You will be sent Authorization Code via Text Message or Call to your phone when you click SEND CODE button.

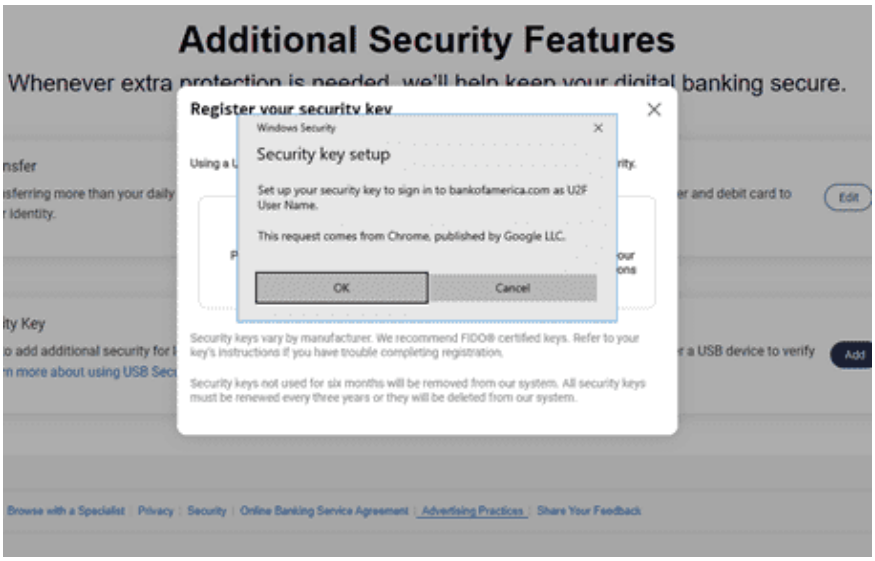


Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

Step 4: Enter Authorization Code and Debit PIN then click SUBMIT.

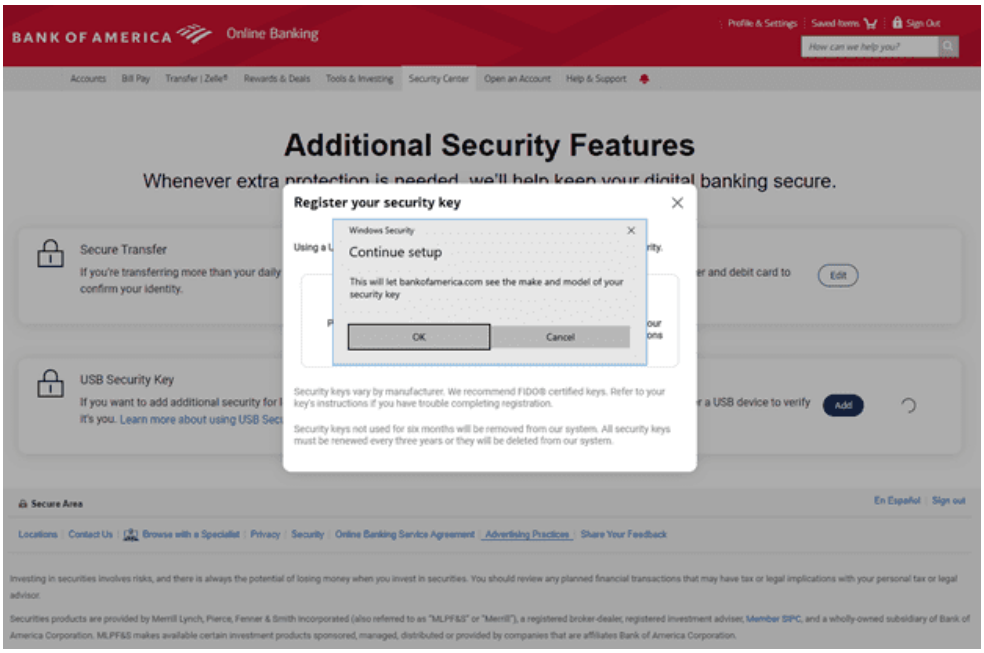


Step 5: Click OK to Security key setup popup.

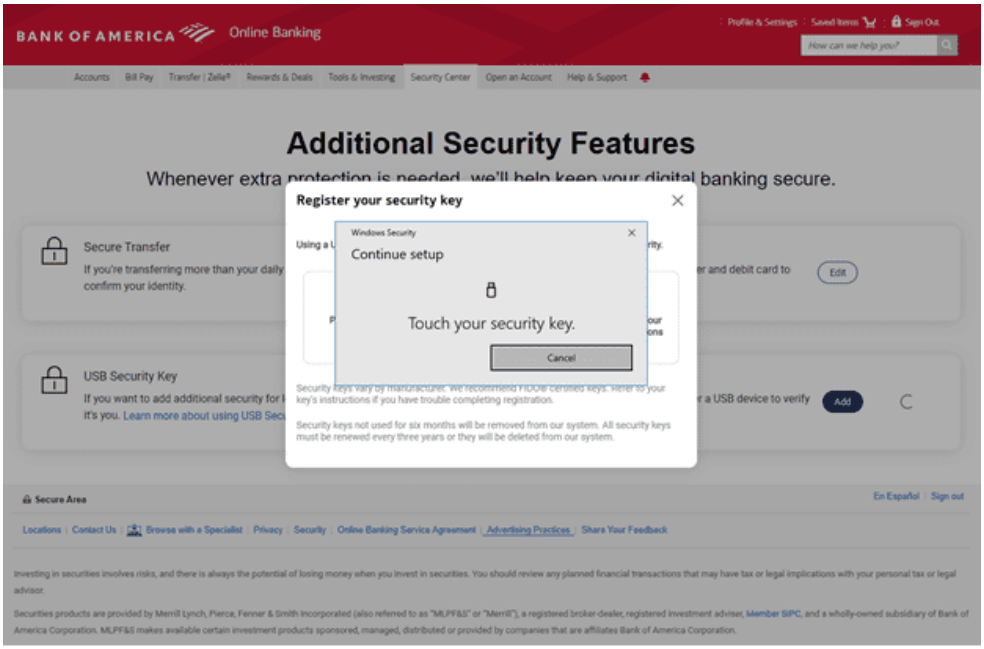


Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

Step 6: Click OK to allow Bank of America to see make and model of your security key.

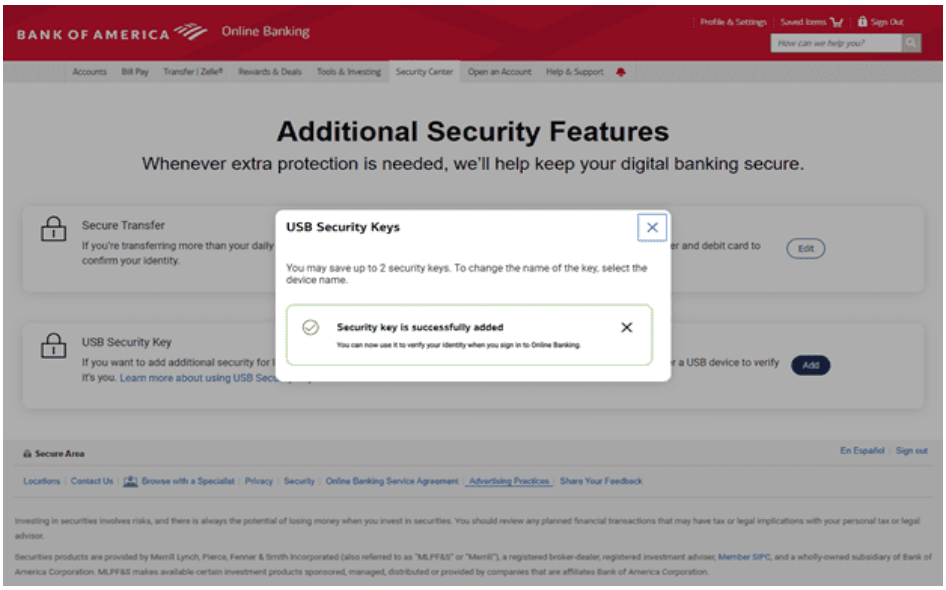


Step 7: Insert your security key and then touch the security key.

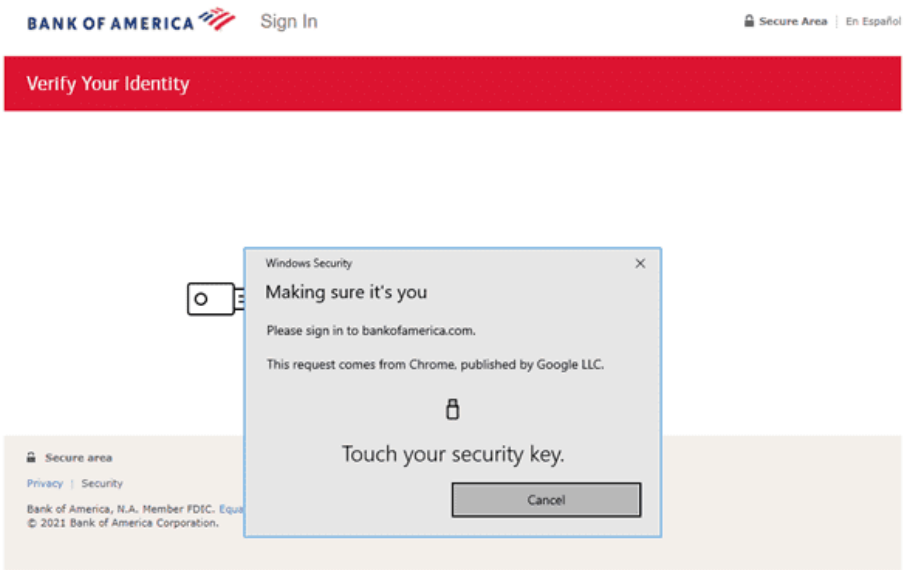


Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

Step 8: If successful, you will see the message that shows security key is successfully added.



Step 9: Step 9: Logout of your account and then log back in. When you try to log back in, it will ask you to touch your security key to verify you are the owner of the account.



Once your USB security key is set up, it serves as an extra layer of security for adding transfer recipients to your account and for extra security at sign-in.

Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

4. Other Online services

The following is a list of online services that are supporting FIDO Authentication (U2F and FIDO2).

Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

7. Windows Hello Set-up Guide

What is Windows Hello?

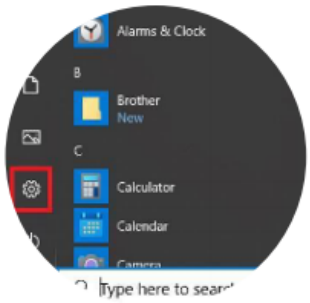
Microsoft Windows Hello, part of Windows 10, gives users a personal, secured experience where the device is authenticated based on their presence. Users can log in with a look or a touch, with no need for a password. In conjunction with Microsoft Passport, biometric authentication uses fingerprints or facial recognition and is more secure, more personal, and more convenient.[1]

Note:

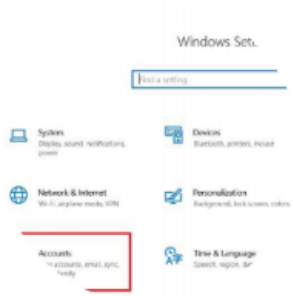
Please note that Fingerprint enrolment for **Windows Hello** and **USB Security Key** is different
The user needs to enroll the user's fingerprint separately with Windows Hello (for PC login) and a security Key (for Web login).

- Windows Hello Fingerprint enrolment
    - Use for login PC using fingerprint rather than a password or PIN
    - Fingerprint templates are stored inside the secure storage of the PC
-

Setup Devices in Windows Hello



1. From the Start Menu, select **Settings**.

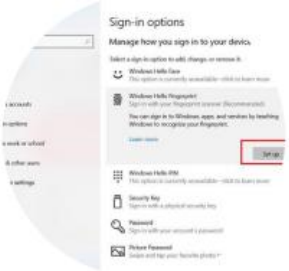


2. Select **Accounts**.

[1] https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/windows-hello

Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

3. Select **Sign In Options**.



4. Under Windows Hello, Select **Set Up**. Follow the steps on the screen to finish setting up the key.

5. Once you have completed the steps, the inserted G310H LED will display a solid blue light when the Windows Login screen is displayed.

6. Now you may use your fingerprint to log in to Windows!

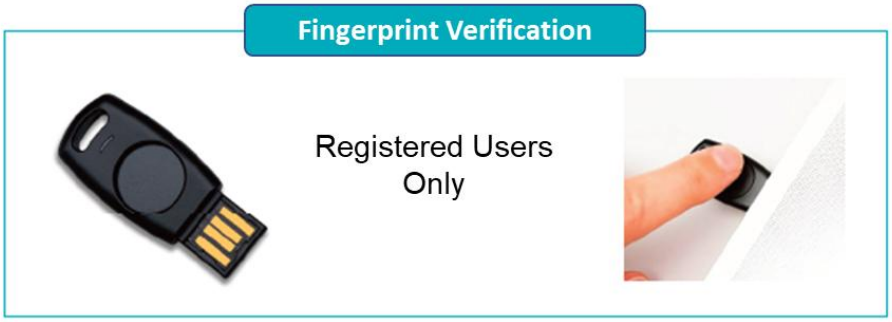
Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

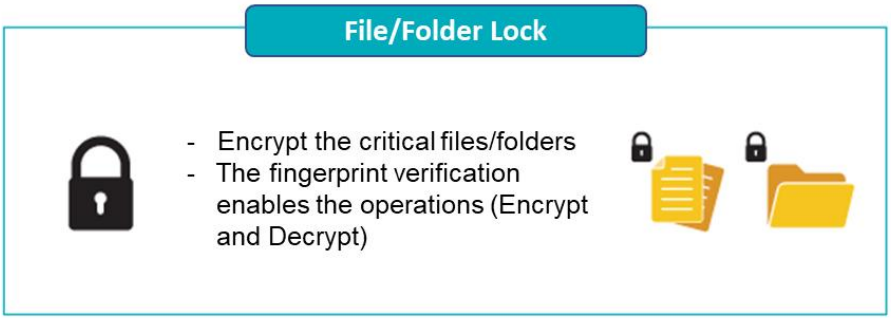
8. Additional Services

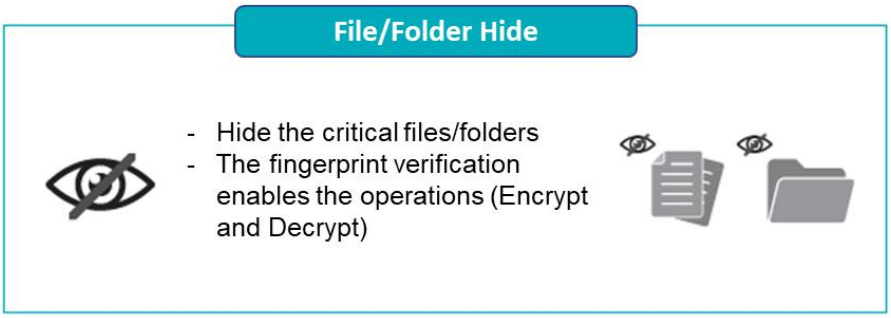
1. TrustKey ThumbLock Solution

TrustKey Thumblock is a Windows program to protect files and folders using TrustKey's Security Key. ThumbLock program is one of TrustKey's solutions based on our Authorization by Strong Authentication (ASA) principle.

Major features include (1) encrypt (and decrypt) files/folders with FIDO authentication and (2) hide (and unhide) files/folders. Our TrustKey security key needs to be inserted for proper operation.







Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

2. TrustKey Login Solution

TrustKey Login is a Windows PC logon and AD join mechanism using TrustKey's security key based on our Authorization by Strong Authentication principle. TrustKey Login is a passwordless solution to allow the PC user to log on to a PC with only fingerprint verification.

Features:

Easy to logon	logon is so simple: no typing, no password Just click and touch; no Phone hassle
Offline mode	Offline AD logon possible without internet connection
Recovery code	Provides temporary logon mechanism using a recovery code when the key is missing Minimize downtime
Simple, Secure, and Error Proof	Significantly lowers logon attempt failures No regular password change hassles*
Affordable	Flexible Pricing models for SMB to Enterprise use: Perpetual or Subscription pricing to meet your needs

Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

Appendix

1. Frequently Asked Questions

Using H-Series Security Keys

How do you enroll your fingerprint to the H-series security key?

There are two different ways to enroll fingerprints: Microsoft Windows 1903 and later. and Key Manager, Google Chrome application

How many fingerprints can I enroll?

A total of 3 fingerprints can be enrolled on each key.

How many resident keys do H-Series keys hold?

H-series keys can hold up to 150 resident keys.

What should I do if the key is locked?

For security reasons, the H-series security key will automatically lock if the registered fingerprint fails 15 times in a row. If the "RED" light is turned on the device, open Key Manager and enter your PIN to unlock the device.

Can I reset the security key to the factory setting?

Factory Reset can be done through Key Manager. After installing Key Manager, click the Factory Reset button and reinsert the device. Next, touch the sensor within 10 seconds. You can refer to the Key Manager User Manual for details.

What happens if my key is lost or stolen?

The best practice is always to ensure that you register more than one security key. Most websites that accept FIDO2 or U2F allow you to register more than one key. This gives you a backup should you lose a key.

Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

Supported Platform · Environment

Which OS does Key Manager support?

Key Manager supports Windows, macOS, and Linux

Can I use the H-Series security key with Windows PC, Mac?

Yes, the H-Series security key works with Windows PC, Mac. Moreover, it also works with Linux, Chromebook, and Android.

Which web browsers do you support?

H-Series security key works with all major web browsers, including Google Chrome, Microsoft Edge, Mozilla Firefox, Apple Safari, etc.

Which major online services are available that support FIDO2?

Most major online service providers support/implement FIDO2 certification. Currently, Microsoft Azure Active Directory, Microsoft, GitHub, Dropbox, Twitter, Login.gov, etc., provide FIDO authentication service.

I get an error when signing in to Windows with my security key
If it is an error of 'Unknown Device State (Code:1,9.0x800700d)', this is an intermittent issue that occurs when trying to log in to Windows while both fingerprint registration for Windows Hello login and security key fingerprint registration are enabled. In this case, remove the security key from the USB port and reinsert it to retry the login, and in most cases, you can log-in normally.

H-Series Security Key Features

Can I log in to Microsoft Azure Active Directory(AD) using my security key?

H-series security keys fully support Microsoft Azure AD. It can be used to sign in to Azure joined Windows PC whether you are online or offline/airplane mode.

Can I use my security key in place of another vendor's U2F key?

H-series security keys are now available on a variety of operating systems and platforms that offer U2F and FIDO2 certification services. Therefore, H-series security keys can be used wherever U2F or FIDO2 is supported.

Can I use the security key on different computers?

Sure! H-series Security key is a roaming authenticator. It can be used in conjunction with more than one user device-supported USB port.

Is my fingerprint data stored in the computer during the enrollment process?

H-series security key stores scanned and encrypted fingerprint data in the special secure storage called TrustZone®. The stored data can never leave the key, even during registration or authentication.

Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

How to enroll the fingerprint to the H-series security key?

There are two different ways to enroll fingerprints: Microsoft OS and the Key Manager application.

Misc.

Which certification level do you have?

H-series security key is the world's first authentication device to achieve FIDO2 Level 2 security certification by satisfying secure operating environment requirements by the FIDO Alliance.

What is the difference between FIDO Certified Authenticator Level 1 and Level 2?

FIDO2 Level 2 is certified with the evaluations for physical security and operating environment besides Level 1 security requirements. It also requires the strength of the cipher 112 bit and more, key protection, and Random Number Generator. Visit FIDO Alliance for more information.

Can I use my security key without enrolling the fingerprint in the U2F environment?

In the U2F environment, using the security key without enrolling the fingerprint allows anyone with my security key access to my account. Therefore, this is NOT recommended. If you want to securely protect your account, simply register your fingerprint according to the enroll fingerprint procedure, then touch the fingerprint sensor on the key to complete the login and access the account.

Do you support Windows Hello login option?

Yes. G310H, G320H and B210H support Windows Hello.

Is my fingerprint image stored in the computer during the enrollment process?

H-series security key stores the scanned and encrypted fingerprint data in the secure storage area. The stored data never leaves the key, even during registration or authentication.

Who should I contact if I have some technical questions or want to resell your product?

Please send an email to support@trustkey.kr

Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

2. Safety precautions

1. Please do not disassemble, repair, or modify the security key arbitrarily.
2. Please do not expose the security key to direct sunlight for a long time.
3. Please do not store the security key at too low or too high a temperature
4. Please do not place the security key near or put it in a hot-air appliance (stove, microwave, etc.), heating cookware, or high-pressure container.
5. Please do not put the security key in a container filled with liquid.
6. Be careful not to drop the security key or subject it to impact.
7. Please do not store the security key in a humid place for a long time.
8. To clean the security key, lightly wipe it with a dry towel.
9. Please do not use the security key within reach of children.
10. When using the security key in a dry environment, be careful as static electricity may be generated.

Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

3. Warranty and Consumer Dispute Resolution Policies

Standard Warranty:

The standard warranty of the products is one year from the purchase except for the EU.

The EU mandates a two-year warranty.

Consumer Dispute Resolution

<table>
<tr><th colspan="3" rowspan="2">Consumer Complaint</th><th colspan="2">Resolution</th></tr>
<tr><th>Under warranty</th><th>After warranty</th></tr>
<tr><td rowspan="11">Malfunction under normal conditions of use</td><td colspan="2">When the product requires major repair within ten (10) days of purchase</td><td>Product exchange or full refund</td><td rowspan="7">None</td></tr>
<tr><td colspan="2">When the product requires major repair within one (1) month of purchase</td><td>Product exchange or refund</td></tr>
<tr><td colspan="2">Product exchange not possible</td><td rowspan="2">Full Refund</td></tr>
<tr><td colspan="2">When the exchanged product requires major repair within one (1) month</td></tr>
<tr><td colspan="2">In case of damage caused during transportation when purchasing the product</td><td>Product exchange</td></tr>
<tr><td rowspan="3">Repair Possible</td><td>The same defects occur twice</td><td>Free Repair</td></tr>
<tr><td>The same defects occur three times</td><td rowspan="4">Product exchange or full refund</td></tr>
<tr><td>The same defects occur up to five times</td></tr>
<tr><td>Repair not possible</td><td>Repair is not possible</td></tr>
<tr><td rowspan="2">Exchange not possible</td><td>When repair is impossible because there are no repair parts within the parts retention period</td><td>Refund by adding 10% to the amount of straight-line depreciation</td></tr>
<tr><td>If the product requested by the customer for repair is lost</td><td>Refund by adding 10% to the amount of straight-line depreciation (maximum limit: purchase price)</td></tr>
<tr><td></td><td colspan="2">When the repair is possible</td><td>Repair with charge</td><td>Repair with charge</td></tr>
</table>

Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

malfunction due to the intention or negligence of the consumer	When the repair is not possible	Exchange with charge	None

Service with charge

- In case of malfunction due to the user's negligence in handling, disassembly, or assembly

- In case of external environmental problems caused by software (OS and application programs, viruses, etc.) and Internet, antenna, wired signals, etc., not defective products

- In case of breakdown due to natural disaster (fire, salt damage, flood damage, etc.)

Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

Manufacturer Information

Manufacturer	TrustKey Co. Ltd (Korea)
Technical support	Korea: Tel : +82-02-556-7878 / email : support@trustkey.kr USA: Tel : +1-(509)-418-6130 / email : contactus@trustkey.kr
Webpages	www.trustkey.kr
Addresses	Korea: (06236) 2F, 14, Teheran-ro 22-gil, Gangnam-gu, Seoul

Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

FCC Warning Statements

1. FCC Part 15.19 statements:

   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.

2. FCC Part 15.105 statement:

   This equipment has been tested an 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 and outlet on a circuit different from that to which the receiver is connected.
   - Consult the dealer or an experienced radio/TV technician for help.

3. FCC part 15.21 statement:

   Any changes or modifications not expressly approved by the party responsible for compliance could void the user′s authority to operate this equipment.

Supplier’s Declaration of Conformity:

47 CFR §2.1077 Compliance Information

Copyright ⓒ 2023 TrustKey Co., Ltd. All Rights Reserved

Unique Identifier : H-series Security Keys (eFA310h, eFA320h, b210h)

Responsible Party – U.S. Contact Information

TRUSTKEY Solution Global.
702 Hayes, Irvine, Ca 92620, USA
+1 (509) 418-6130

Copyright

Copyright ⓒ 2023 TrustKey

This instruction manual is a copyrighted work. No part or whole of this user manual may be reproduced, publicly transmitted, distributed, translated, or converted into an electronic medium or machine-readable form ***without TrustKey's prior written consent****.*