V1.0

# User's Manual for

# G310H/G320H/B210H

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.

# Contents

# 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/G320H/B210H 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)

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 |

# 2. TrustKey's Security Keys

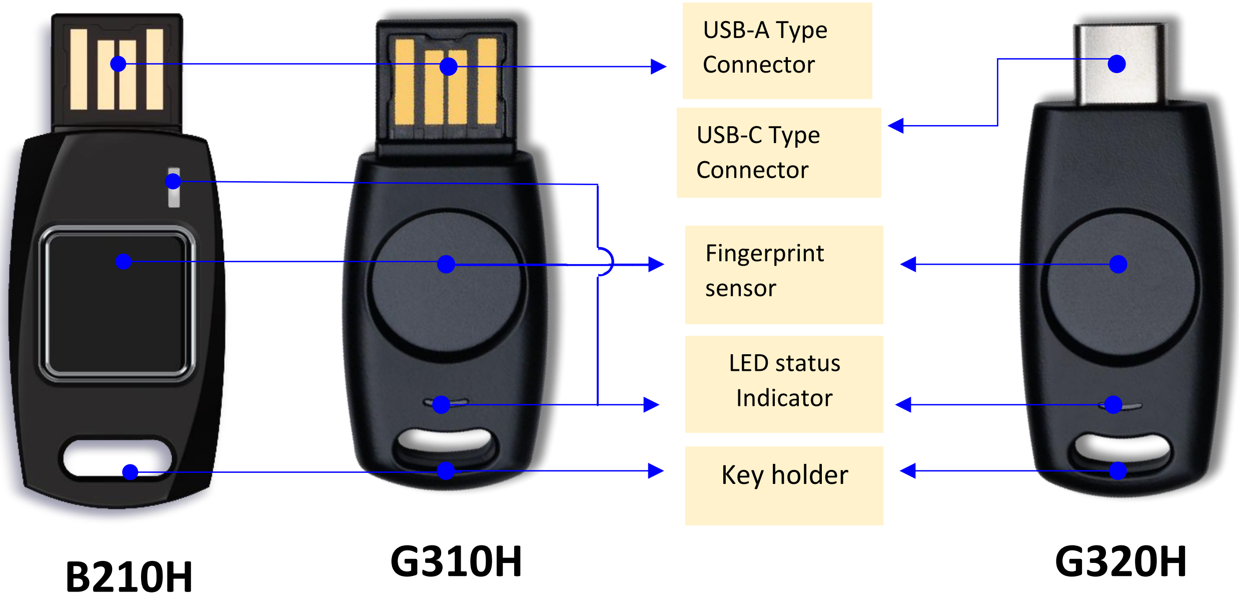
## 1. Product Specification

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

*Note:*

1. *-4°F ~ 140°F*
2. *-40°F ~ 185°F*

## 2. Security Key Description



## 3. LED Status Indicator

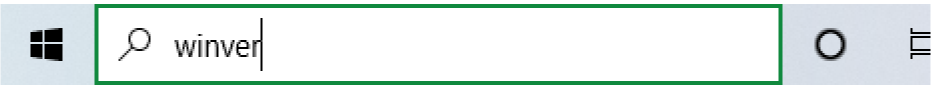
| Color | Status | Description | Action |
|---|---|---|---|
| 🟩 | On | - Key connection OK<br>- Authentication Sucess | |
| 🟦 | On | N/A | |
| | Blinking | Wating for fingerprint scan (FIDO2) | |
| 🟧 | Blinking | Waing for fingerprint scan (U2F) | |
| 🟥 | On | Security key is locked due to authentication failure | Unlock the security key |
| | Blinking | Authentication failure | Rescan fingerprint |
| 🟦 | Blinking | - Waiting for action (factory reset mode)<br>- Security Key selection mode (when no fingerprint is enrolled) | |
| LED Off | | Not connected | Reinsert the security key |

# 3. Security Key Fingerprint Enrollment

## 1. Fingerprint Enrolment steps (Windows 10)

**Step 0: Check Windows version First**

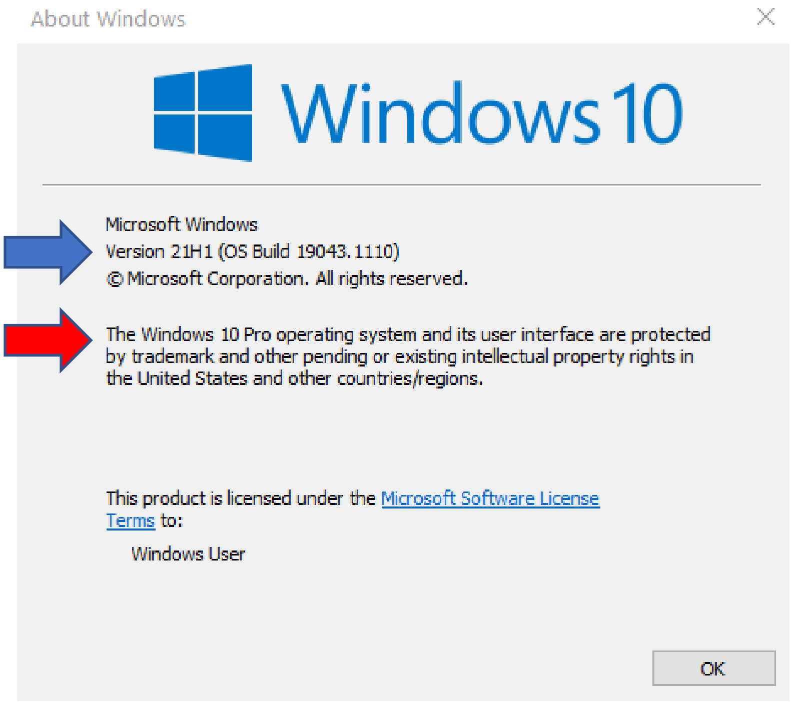
Please check your Windows version before enrolment by typing "winver" at the Windows search bar.



winver

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.



About Windows

Windows 10

Microsoft Windows
Version 21H1 (OS Build 19043.1110)
© Microsoft Corporation. All rights reserved.

The Windows 10 Pro operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

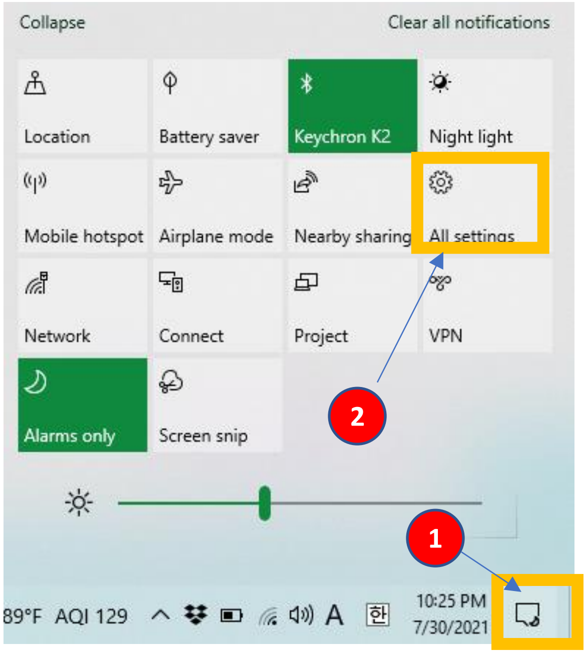
This product is licensed under the Microsoft Software License Terms to:

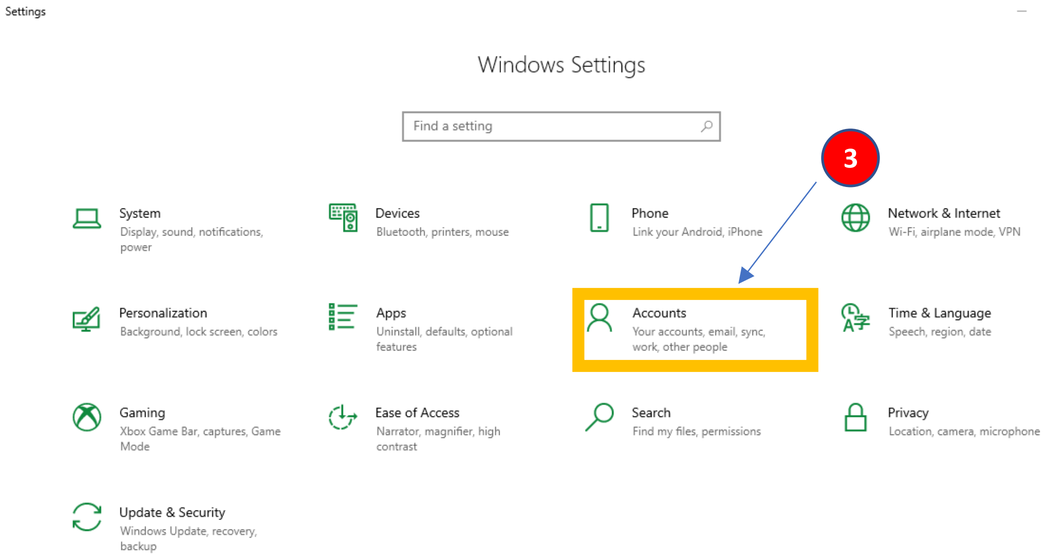
Windows User

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

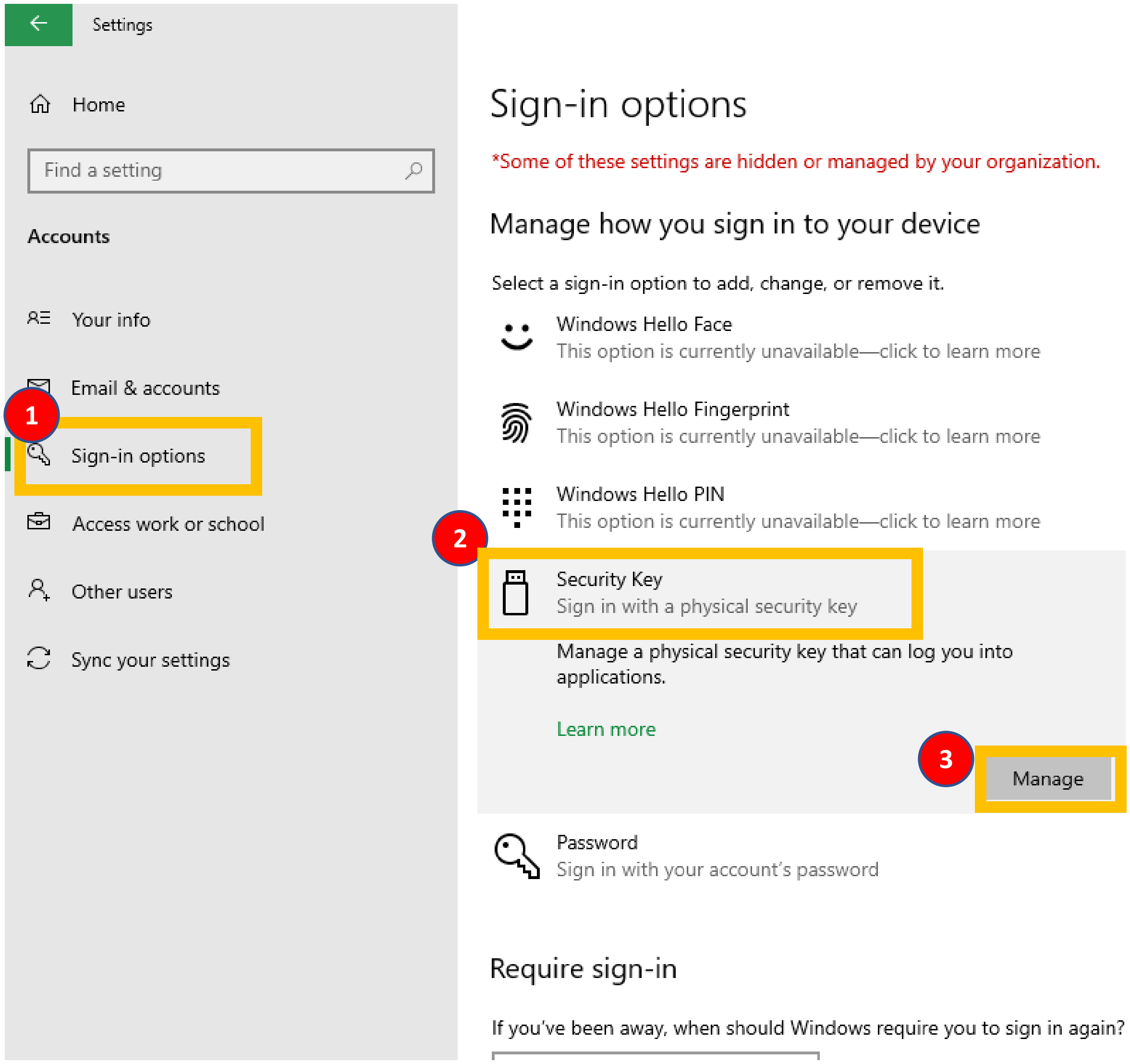
## 2. Fingerprint Enrolment steps

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




Settings
Windows Settings
Find a setting
3
System
Display, sound, notifications, power
Devices
Bluetooth, printers, mouse
Phone
Link your Android, iPhone
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Apps
Uninstall, defaults, optional features
Accounts
Your accounts, email, sync, work, other people
Time & Language
Speech, region, date
Gaming
Xbox Game Bar, captures, Game Mode
Ease of Access
Narrator, magnifier, high contrast
Search
Find my files, permissions
Privacy
Location, camera, microphone
Update & Security
Windows Update, recovery, backup

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



Settings

Home

Find a setting

Accounts

Your info

Email & accounts

Sign-in options

Access work or school

Other users

Sync your settings

Sign-in options

*Some of these settings are hidden or managed by your organization.

Manage how you sign in to your device

Select a sign-in option to add, change, or remove it.

Windows Hello Face
This option is currently unavailable—click to learn more

Windows Hello Fingerprint
This option is currently unavailable—click to learn more

Windows Hello PIN
This option is currently unavailable—click to learn more

Security Key
Sign in with a physical security key

Manage a physical security key that can log you into applications.

Learn more

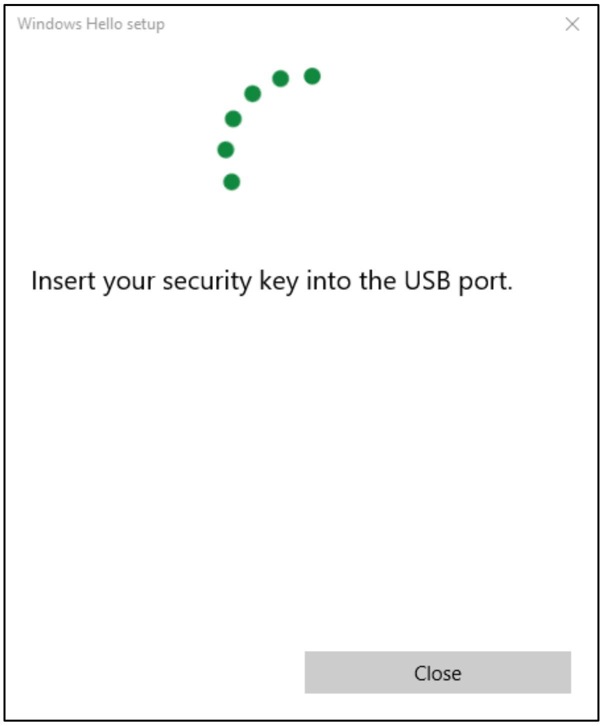
Manage

Password
Sign in with your account's password

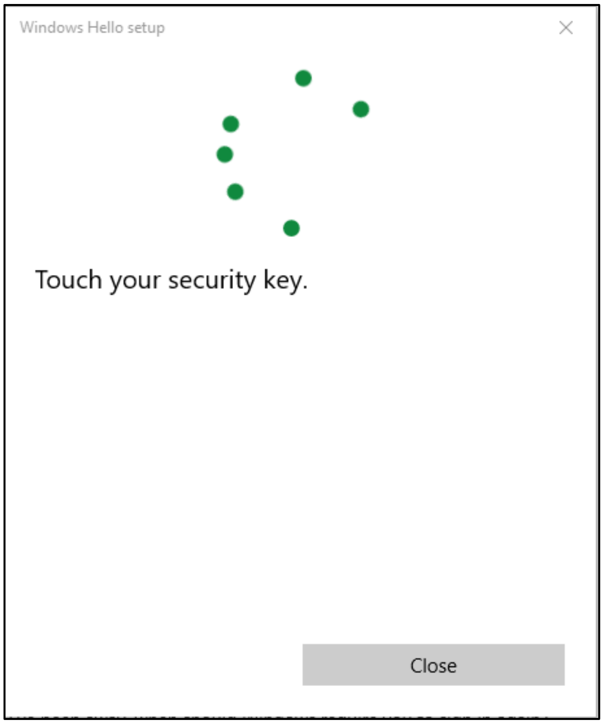
Require sign-in

If you've been away, when should Windows require you to sign in again?

Step 3: Insert the security key and touch the key

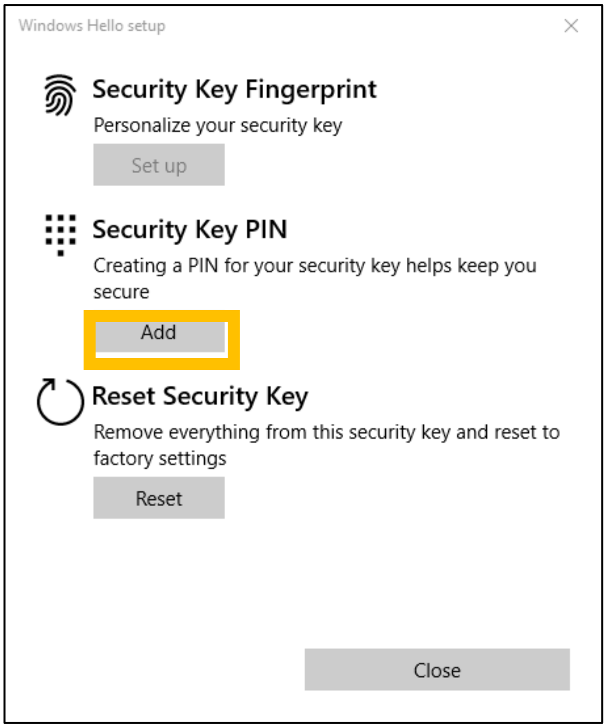


Insert your security key into the USB port.



Touch your security key.

Step 4: set up PIN first



Security Key Fingerprint

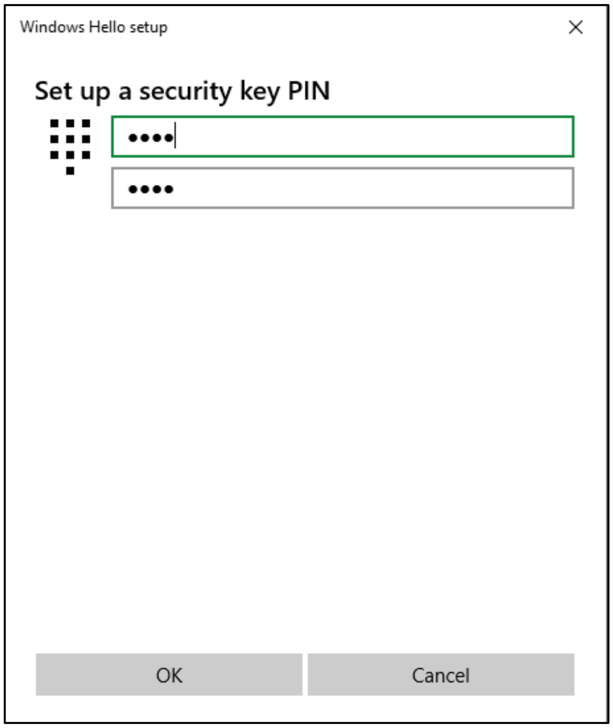
Personalize your security key

Security Key PIN

Creating a PIN for your security key helps keep you secure

Reset Security Key

Remove everything from this security key and reset to factory settings

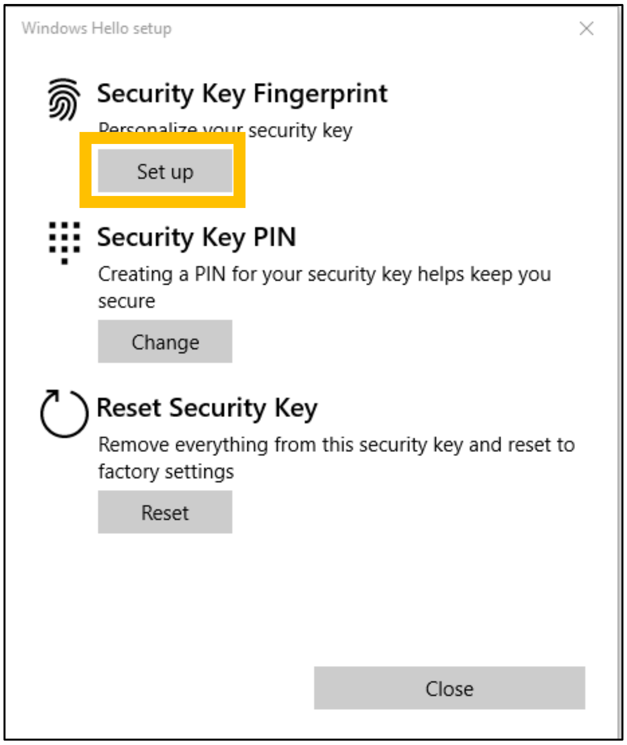


Set up a security key PIN

••••

••••

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



Security Key Fingerprint

Personalize your security key

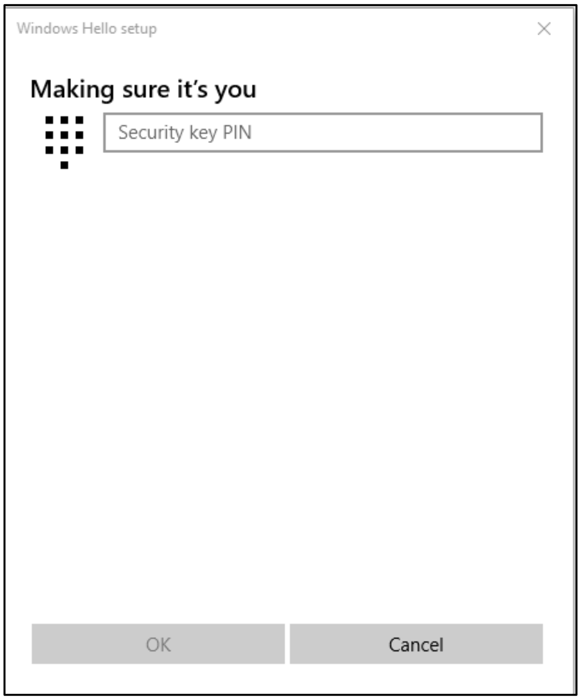
Security Key PIN

Creating a PIN for your security key helps keep you secure

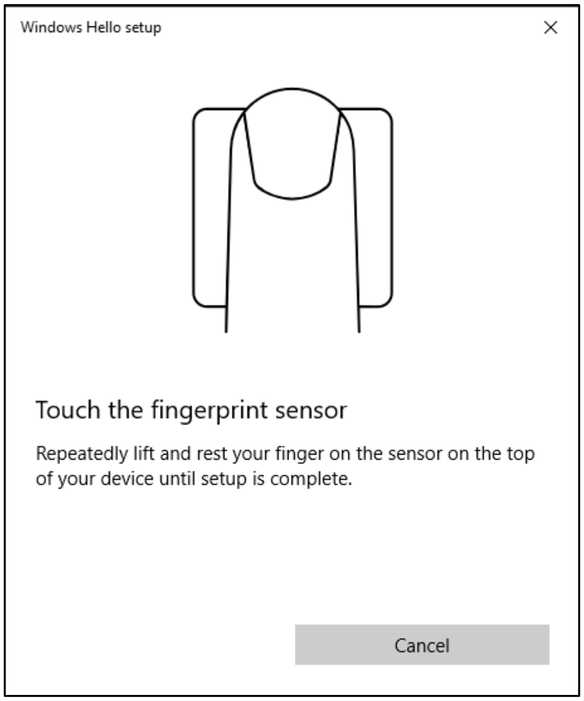
Reset Security Key

Remove everything from this security key and reset to factory settings

Need PIN authentication for fingerprint enrolment.



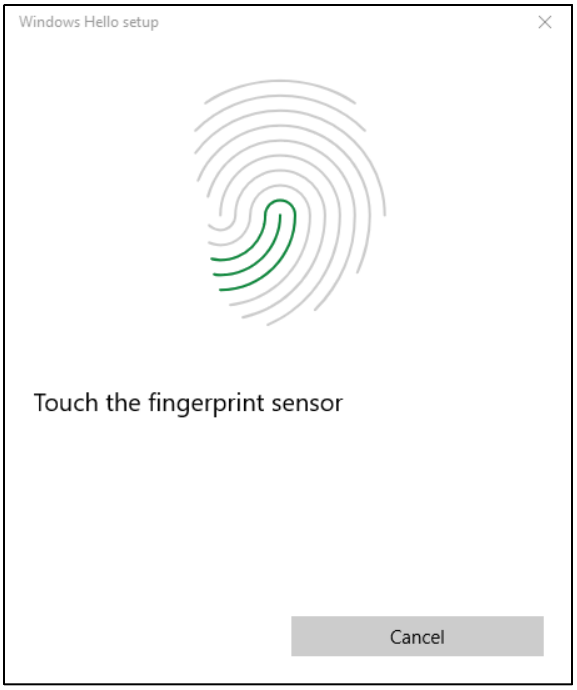
Making sure it's you



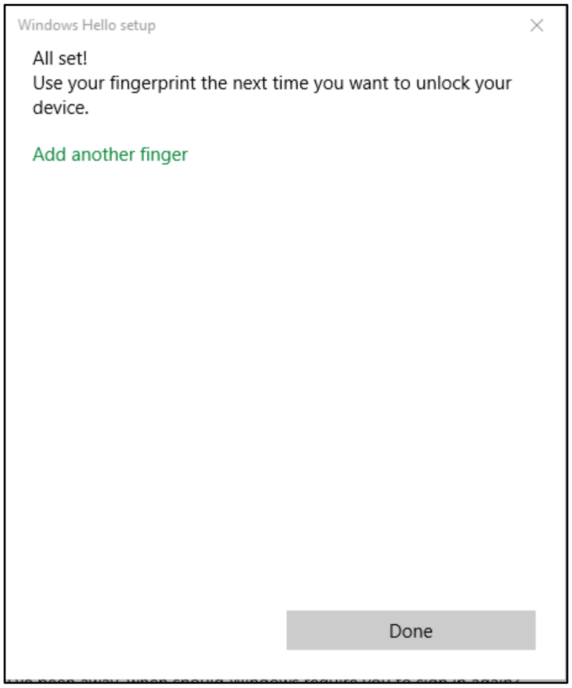
Touch the fingerprint sensor

Repeatedly lift and rest your finger on the sensor on the top of your device until setup is complete.

Scan your fingerprint multiple times until done.



Touch the fingerprint sensor



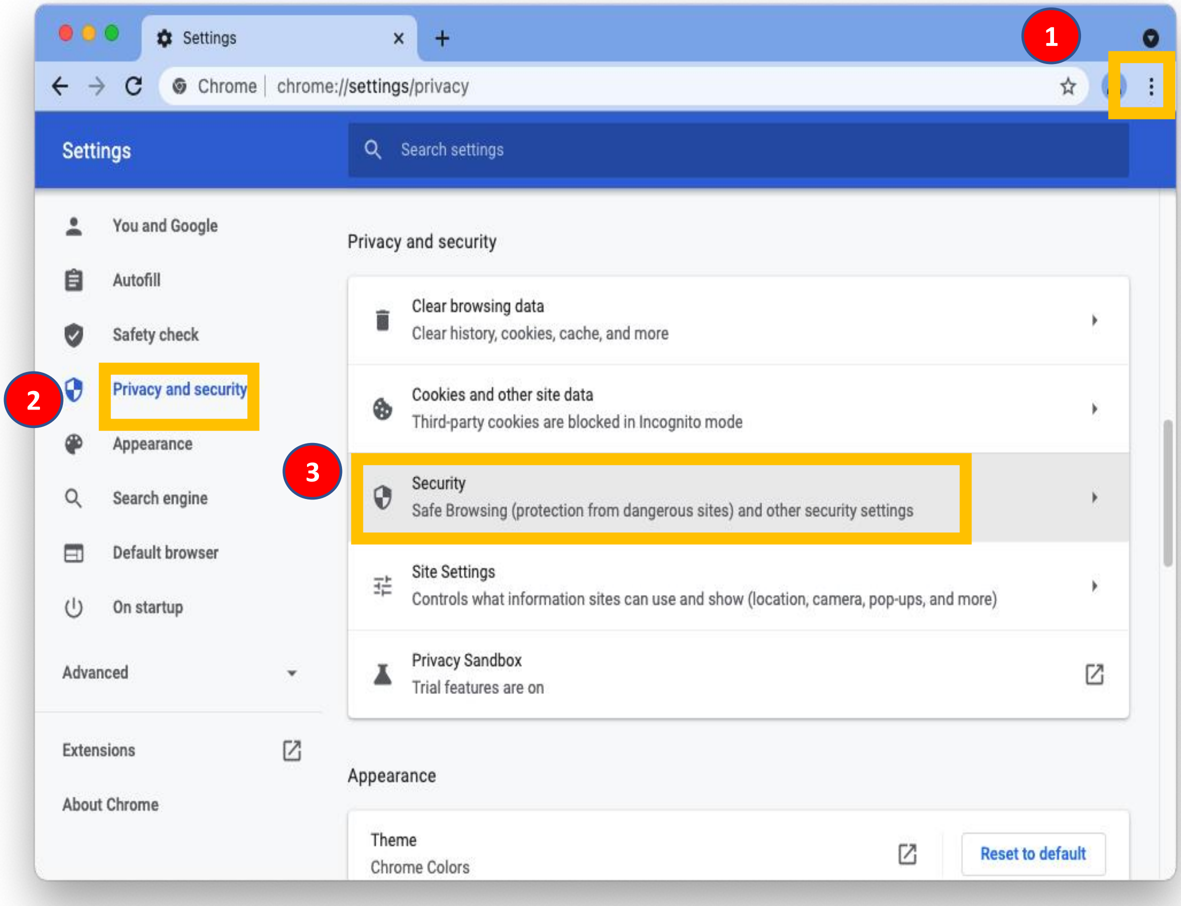
All set!
Use your fingerprint the next time you want to unlock your device.

## 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."



Privacy and security

Clear browsing data
Clear history, cookies, cache, and more

Cookies and other site data
Third-party cookies are blocked in Incognito mode

Security
Safe Browsing (protection from dangerous sites) and other security settings

Site Settings
Controls what information sites can use and show (location, camera, pop-ups, and more)

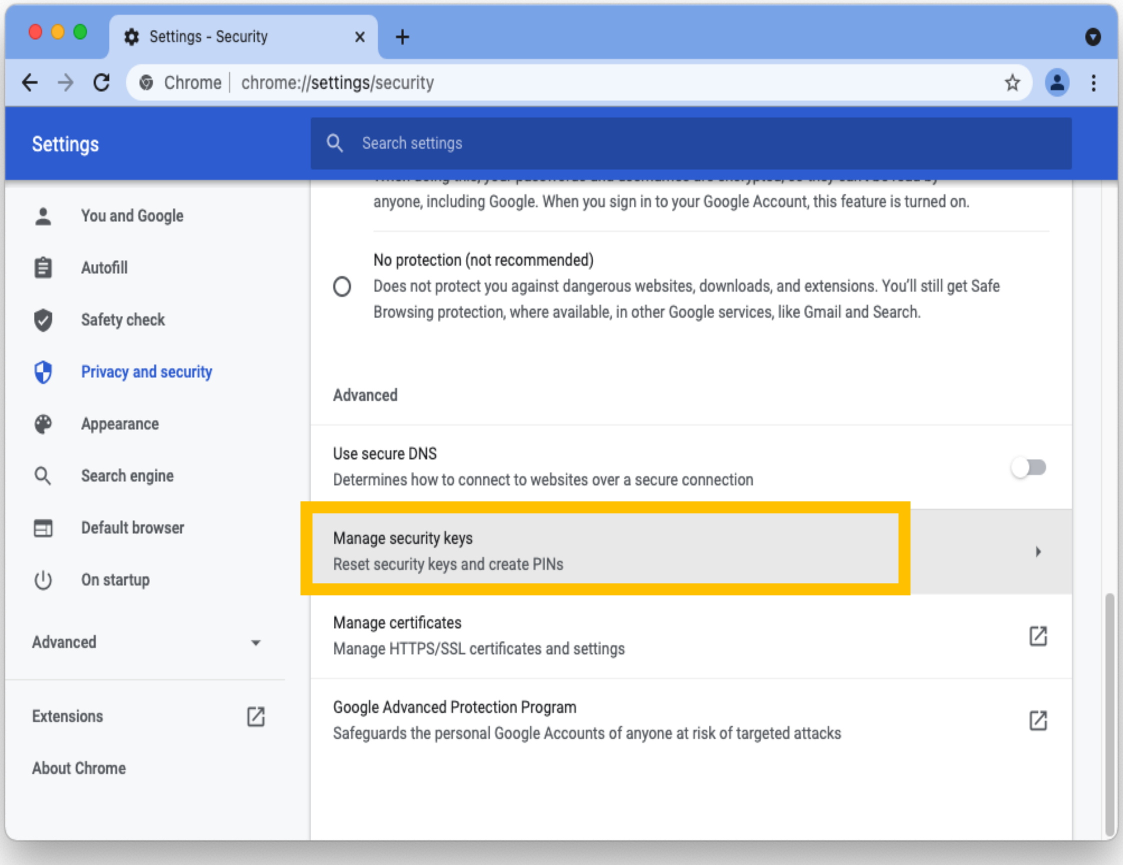
Privacy Sandbox
Trial features are on

Appearance

Theme
Chrome Colors

Reset to default

Step 2: click "Manage security keys"



anyone, including Google. When you sign in to your Google Account, this feature is turned on.

○ No protection (not recommended)
Does not protect you against dangerous websites, downloads, and extensions. You'll still get Safe Browsing protection, where available, in other Google services, like Gmail and Search.

Advanced

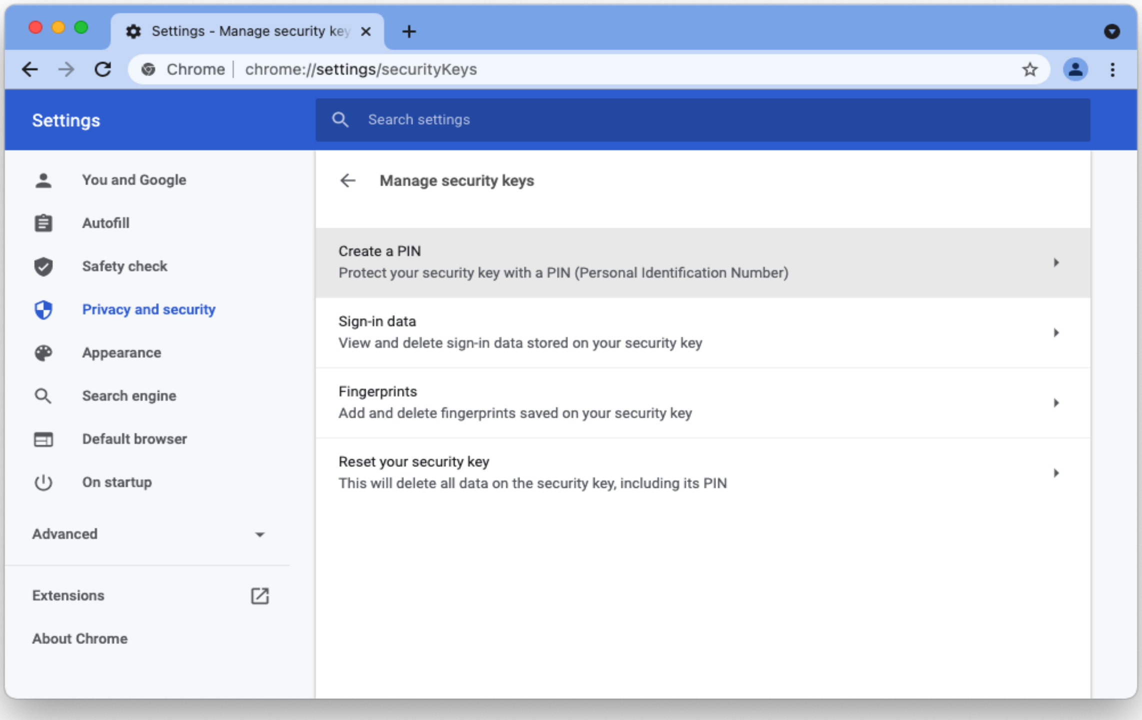
Use secure DNS
Determines how to connect to websites over a secure connection

Manage security keys
Reset security keys and create PINs

Manage certificates
Manage HTTPS/SSL certificates and settings

Google Advanced Protection Program
Safeguards the personal Google Accounts of anyone at risk of targeted attacks

Step 3: Create a PIN



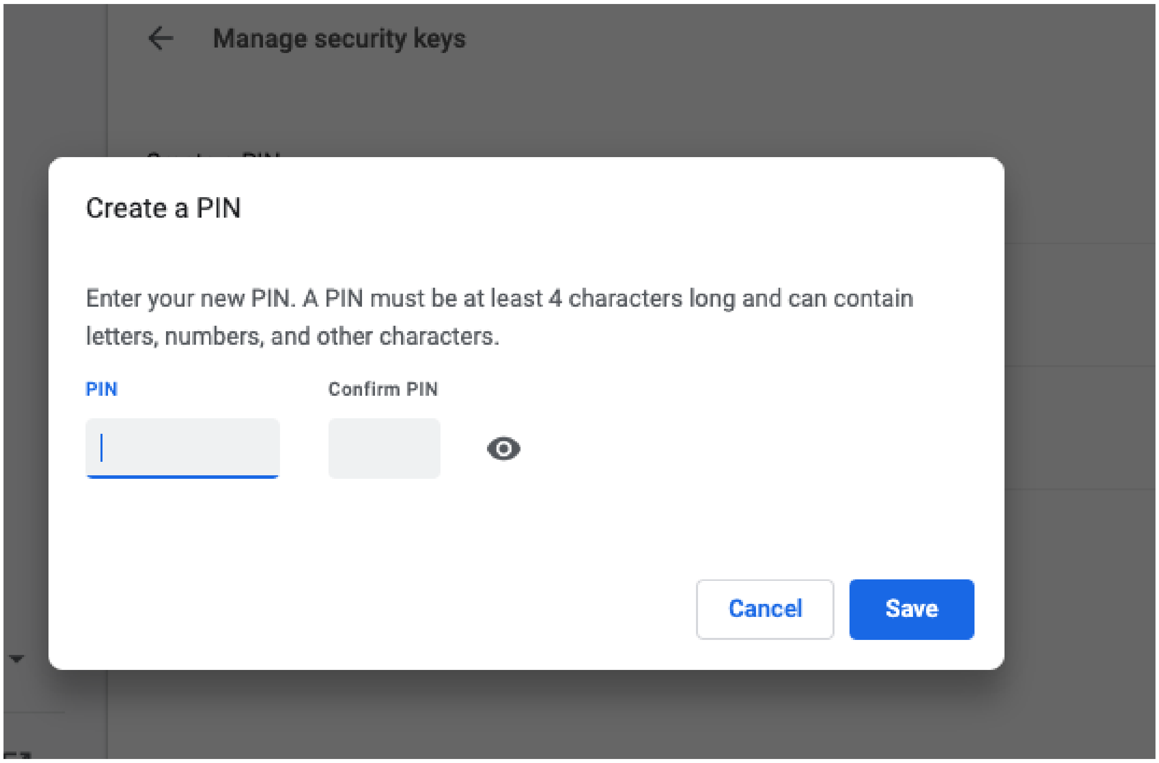
Manage security keys

Create a PIN
Protect your security key with a PIN (Personal Identification Number)

Sign-in data
View and delete sign-in data stored on your security key

Fingerprints
Add and delete fingerprints saved on your security key

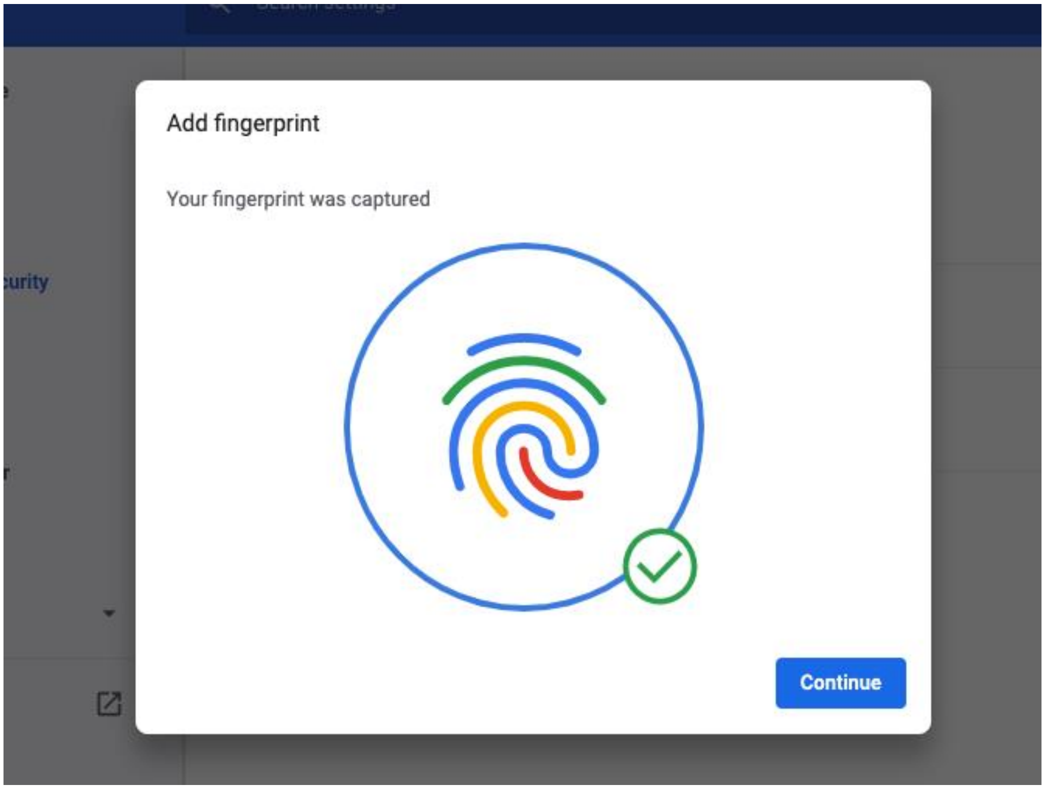
Reset your security key
This will delete all data on the security key, including its PIN


Manage security keys

Create a PIN

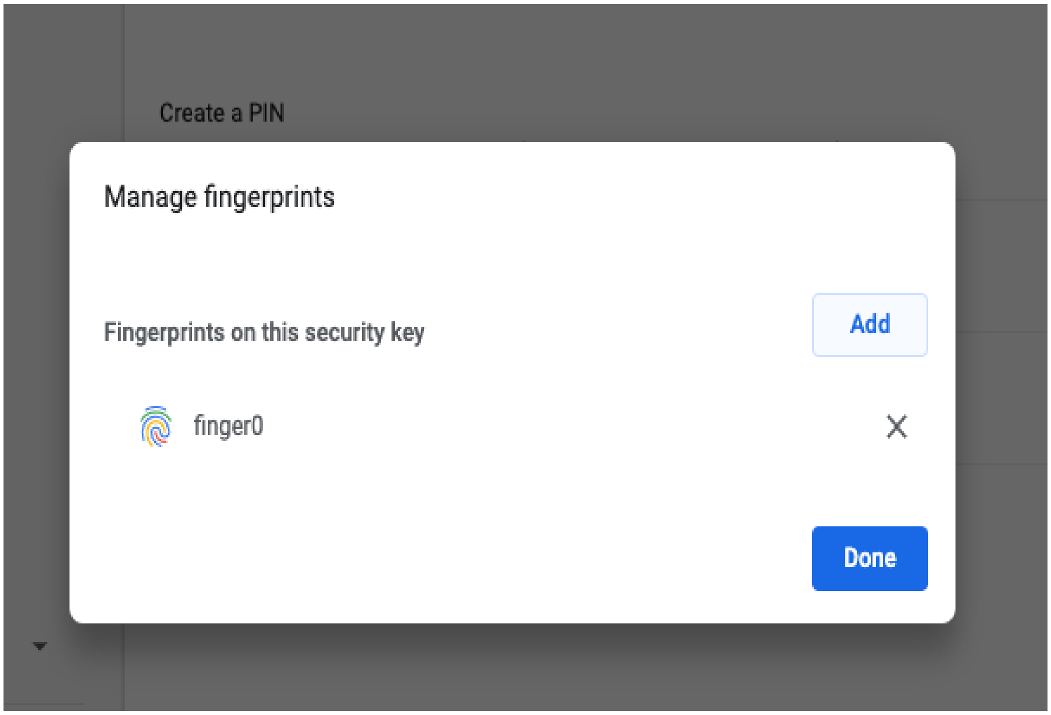
Enter your new PIN. A PIN must be at least 4 characters long and can contain letters, numbers, and other characters.

Step 4: Enroll fingerprints



Add fingerprint

Your fingerprint was captured



Create a PIN

Manage fingerprints

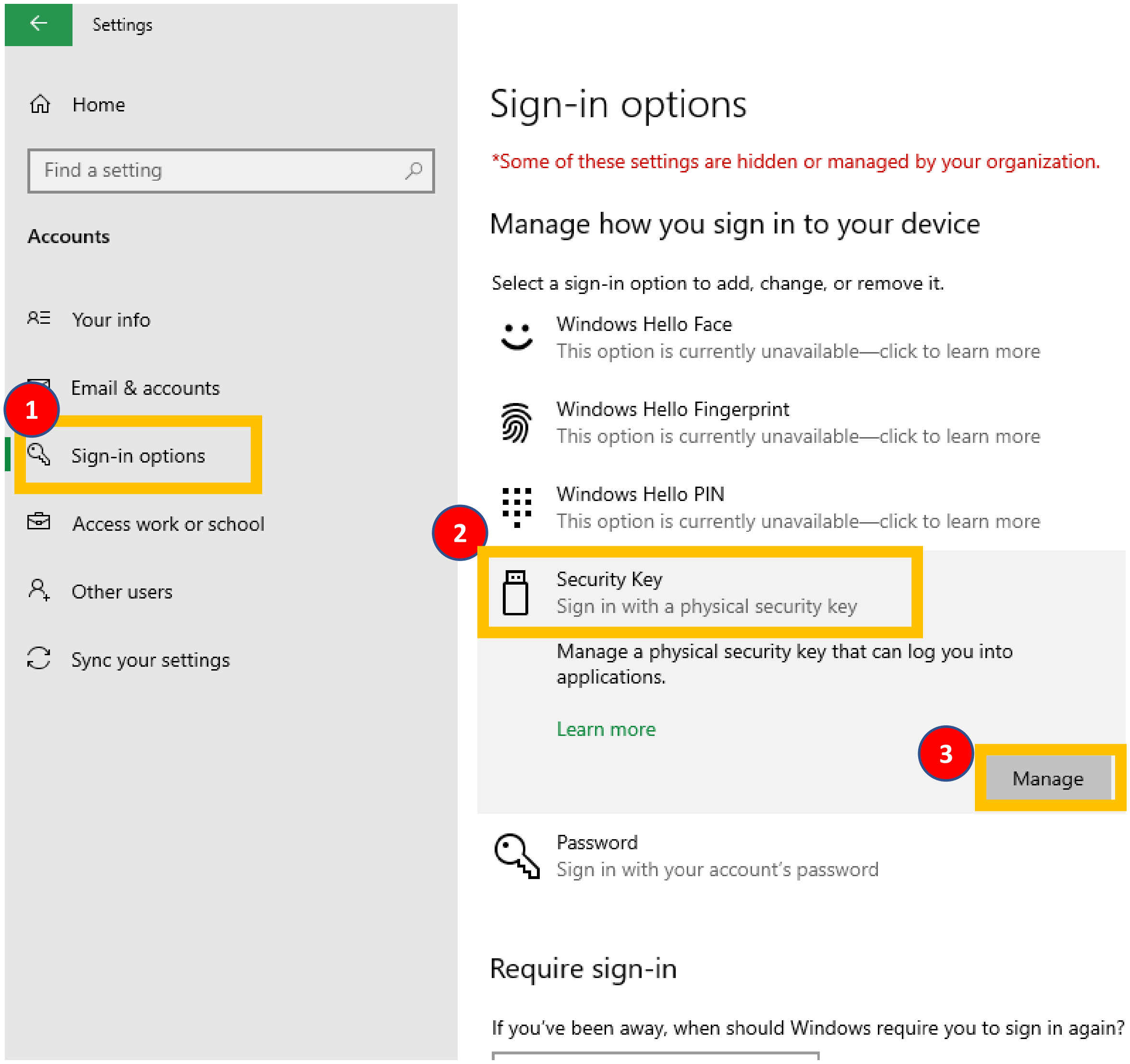
Fingerprints on this security key

finger0

## 4. Security Key Fingerprint Removal Procedure

### 1. Fingerprint removal (Windows10)

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



Sign-in options

*Some of these settings are hidden or managed by your organization.

Manage how you sign in to your device

Select a sign-in option to add, change, or remove it.

Windows Hello Face
This option is currently unavailable—click to learn more

Windows Hello Fingerprint
This option is currently unavailable—click to learn more

Windows Hello PIN
This option is currently unavailable—click to learn more

Security Key
Sign in with a physical security key

Manage a physical security key that can log you into applications.

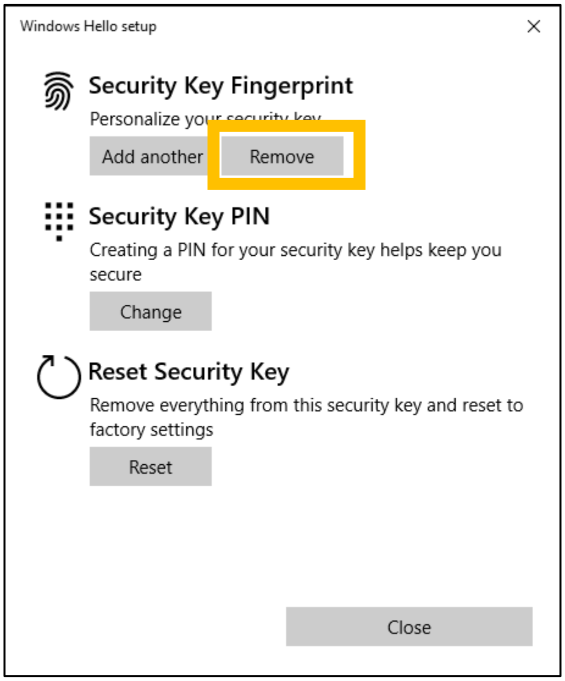
Learn more

Password
Sign in with your account's password

Require sign-in

If you've been away, when should Windows require you to sign in again?

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



Windows Hello setup ×

Security Key Fingerprint

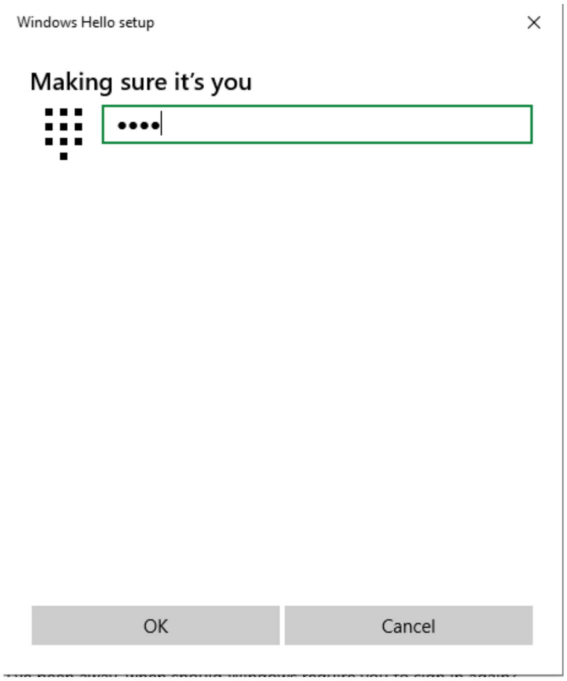
Personalize your security key

Security Key PIN

Creating a PIN for your security key helps keep you secure

Reset Security Key

Remove everything from this security key and reset to factory settings



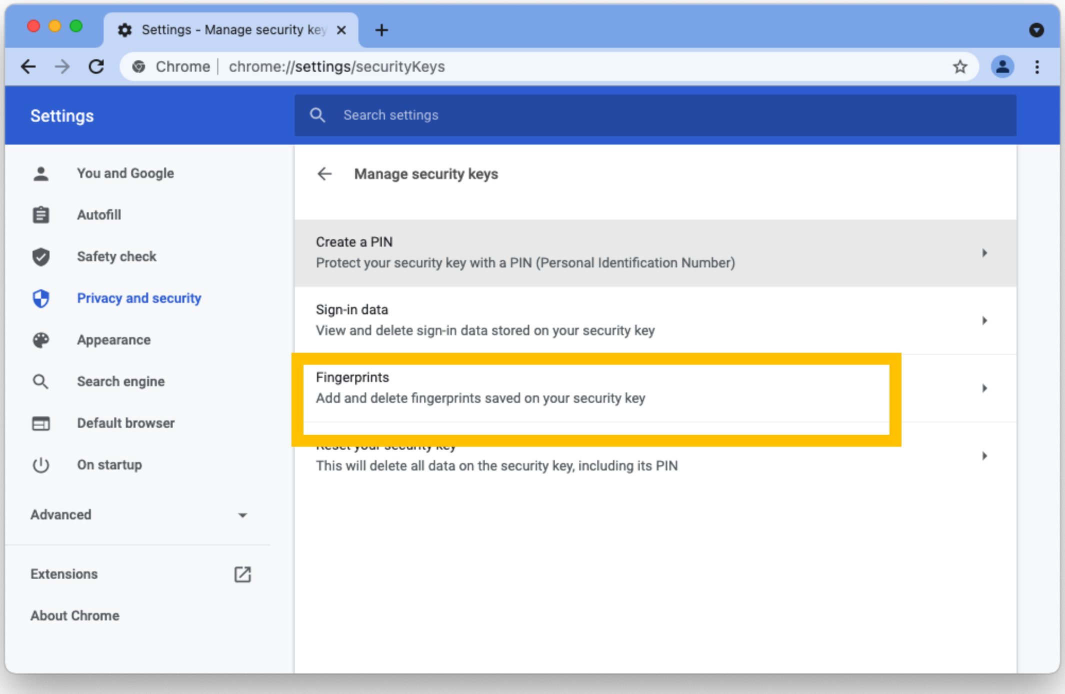
Windows Hello setup ×

Making sure it's you

••••

## 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.



Manage security keys

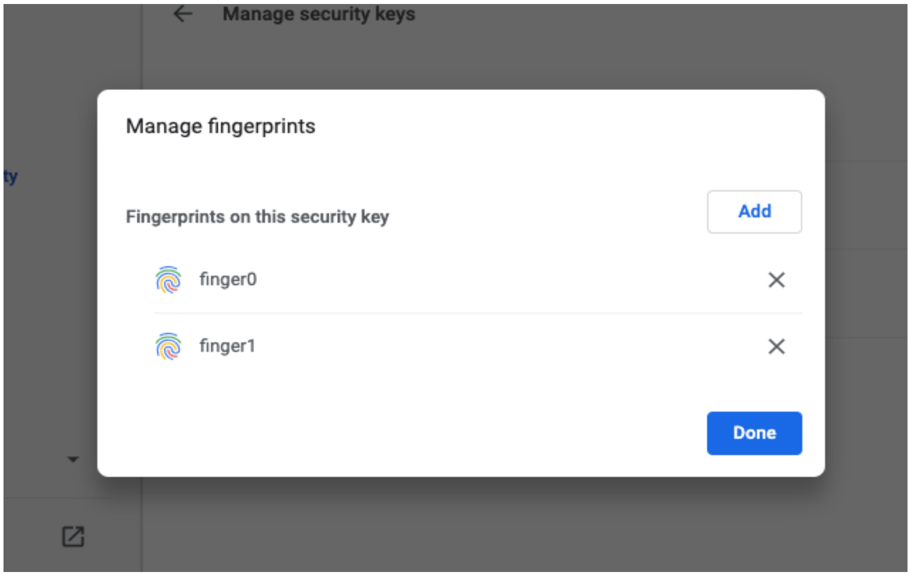
Create a PIN
Protect your security key with a PIN (Personal Identification Number)

Sign-in data
View and delete sign-in data stored on your security key

Fingerprints
Add and delete fingerprints saved on your security key

Reset your security key
This will delete all data on the security key, including its PIN

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



Manage fingerprints

Fingerprints on this security key

finger0 ✕

finger1 ✕

# 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.

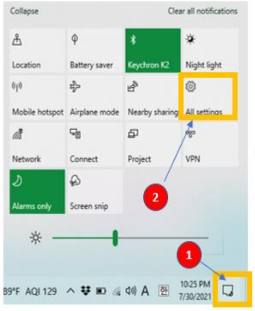
The PIN is needed for fingerprint enrolment and modification. It is also used for backup authentication when fingerprint authentication failed.

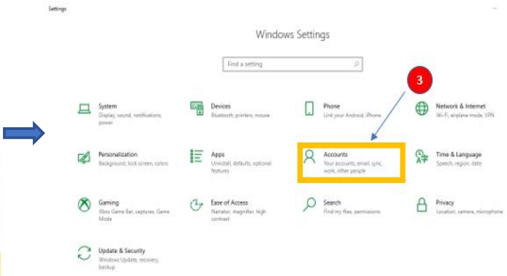
We recommend that the user use a complex combination of digits and letters to protect the user from being leaked.

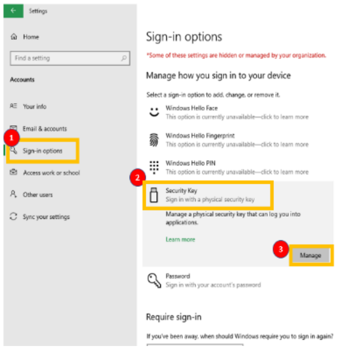
## 2. PIN setup

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

Open Setting →Sign-in Option → Security Key







Sign-in options

*Some of these settings are hidden or managed by your organization.

Manage how you sign in to your device

Select a sign-in option to add, change, or remove it.

Windows Hello Face — This option is currently unavailable—click to learn more

Windows Hello Fingerprint — This option is currently unavailable—click to learn more

Windows Hello PIN — This option is currently unavailable—click to learn more

Security Key — Sign in with a physical security key

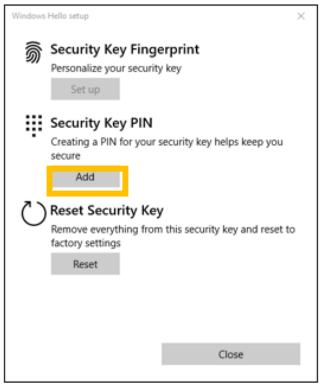
Manage a physical security key that can log you into applications.

Learn more

Password — Sign in with your account's password

Require sign-in

If you've been away, when should Windows require you to sign in again?



Security Key Fingerprint

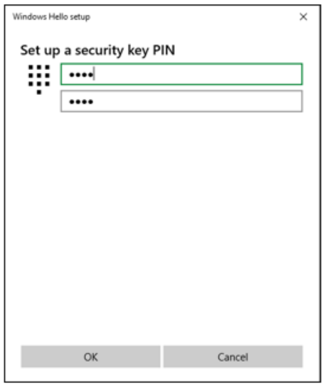
Personalize your security key

Security Key PIN

Creating a PIN for your security key helps keep you secure

Reset Security Key

Remove everything from this security key and reset to factory settings



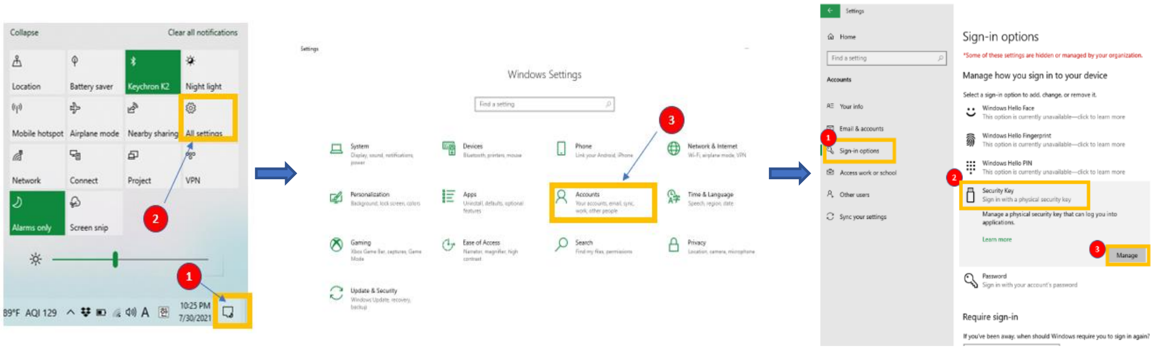
Set up a security key PIN

••••

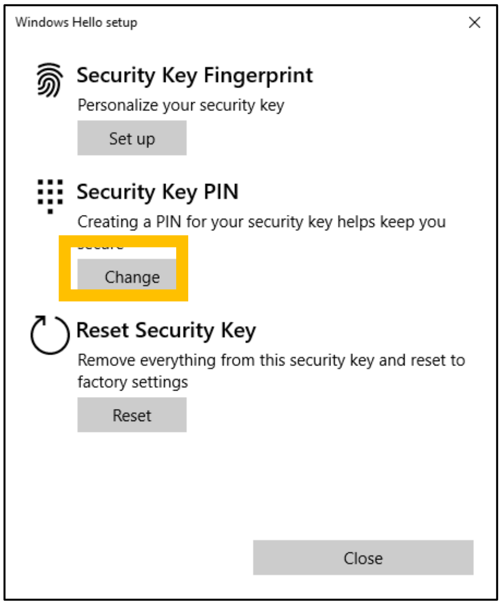
••••

## 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.



Windows Hello setup ✕

**Security Key Fingerprint**

Personalize your security key

Set up

**Security Key PIN**

Creating a PIN for your security key helps keep you secure

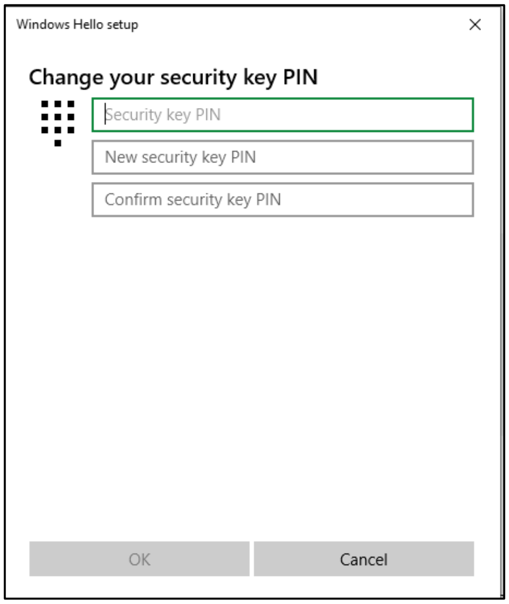
Change

**Reset Security Key**

Remove everything from this security key and reset to factory settings

Reset

Close



Windows Hello setup ✕

**Change your security key PIN**

Security key PIN

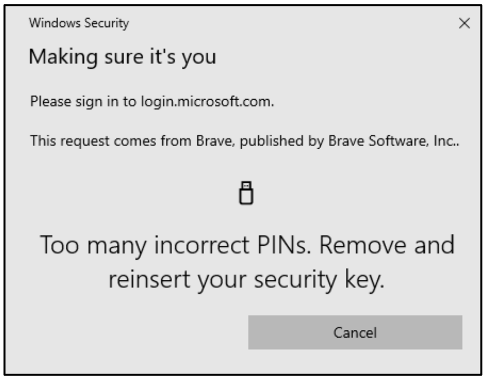
New security key PIN

Confirm security key PIN

OK Cancel

## 4. PIN Authentication Failure

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



Windows Security

Making sure it's you

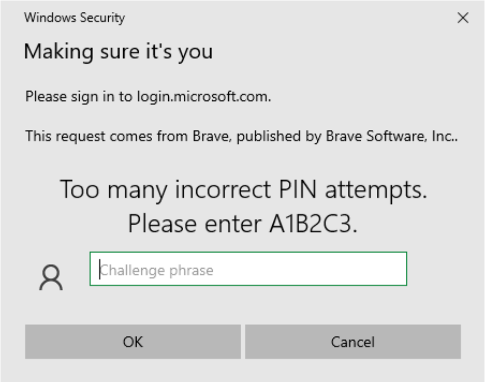
Please sign in to login.microsoft.com.

This request comes from Brave, published by Brave Software, Inc..

Too many incorrect PINs. Remove and reinsert your security key.

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.



Windows Security

Making sure it's you

Please sign in to login.microsoft.com.

This request comes from Brave, published by Brave Software, Inc..

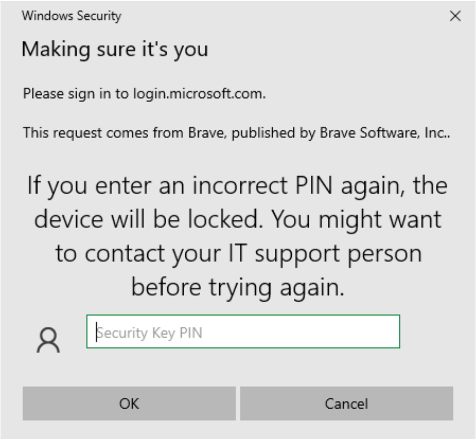
Too many incorrect PIN attempts. Please enter A1B2C3.

Challenge phrase

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.



Windows Security

Making sure it's you

Please sign in to login.microsoft.com.

This request comes from Brave, published by Brave Software, Inc..

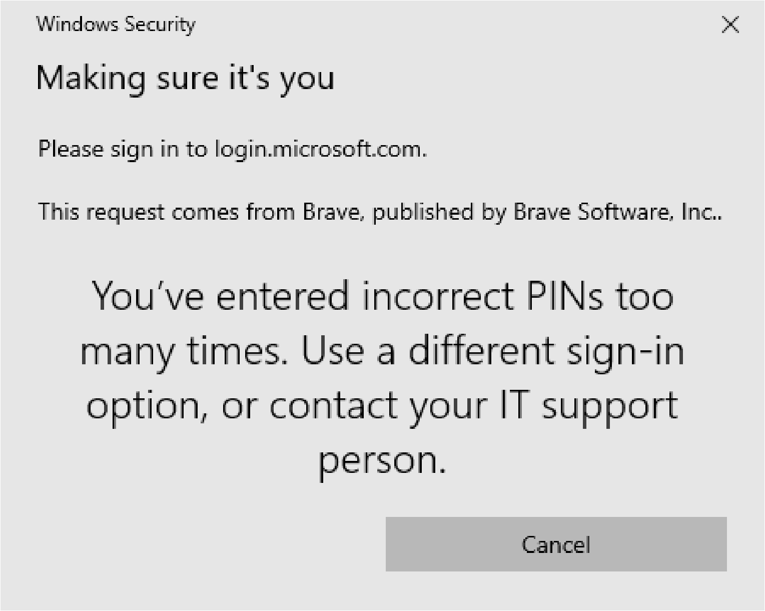
If you enter an incorrect PIN again, the device will be locked. You might want to contact your IT support person before trying again.

Security Key PIN

**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.



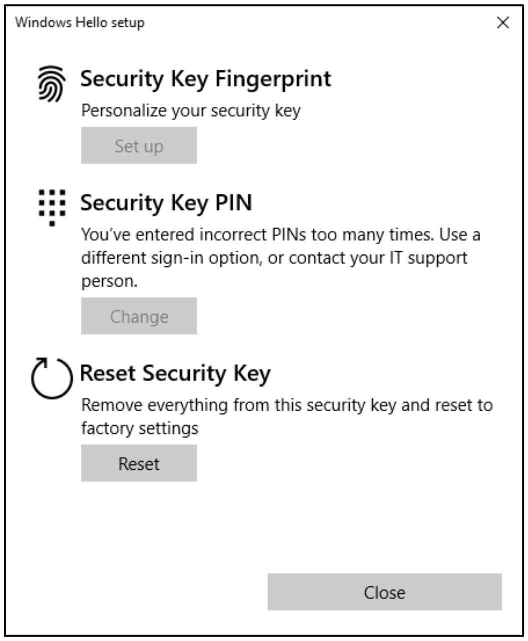
Windows Security

Making sure it's you

Please sign in to login.microsoft.com.

This request comes from Brave, published by Brave Software, Inc..

You've entered incorrect PINs too many times. Use a different sign-in option, or contact your IT support person.



Windows Hello setup

Security Key Fingerprint

Personalize your security key

Security Key PIN

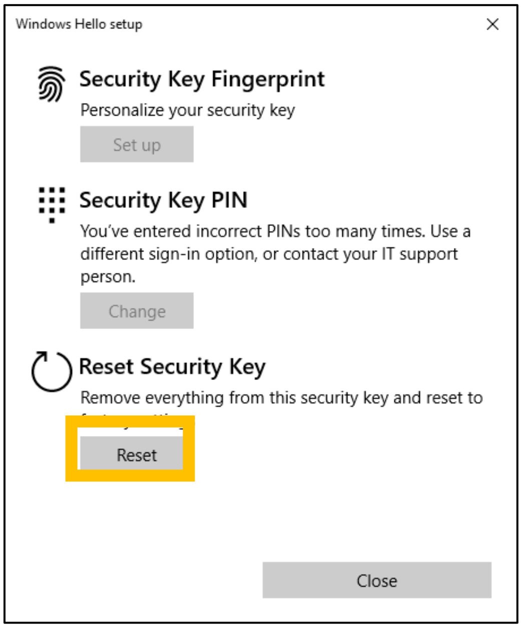
You've entered incorrect PINs too many times. Use a different sign-in option, or contact your IT support person.

Reset Security Key

Remove everything from this security key and reset to factory settings

## 5. Security Key Factory Reset

From Settings → Sign-in Options → Security key



Windows Hello setup

**Security Key Fingerprint**

Personalize your security key

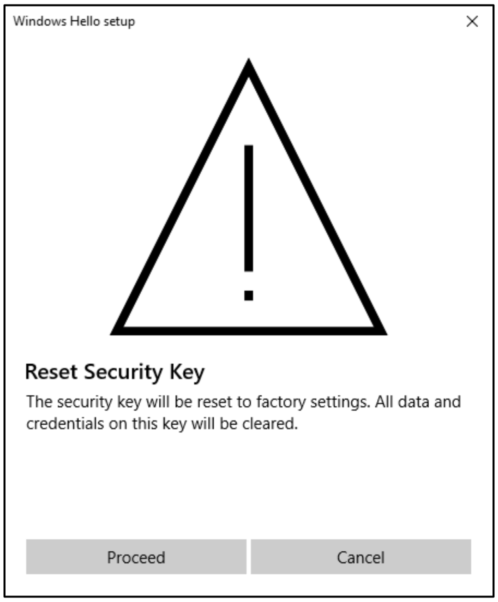
**Security Key PIN**

You've entered incorrect PINs too many times. Use a different sign-in option, or contact your IT support person.

**Reset Security Key**

Remove everything from this security key and reset to

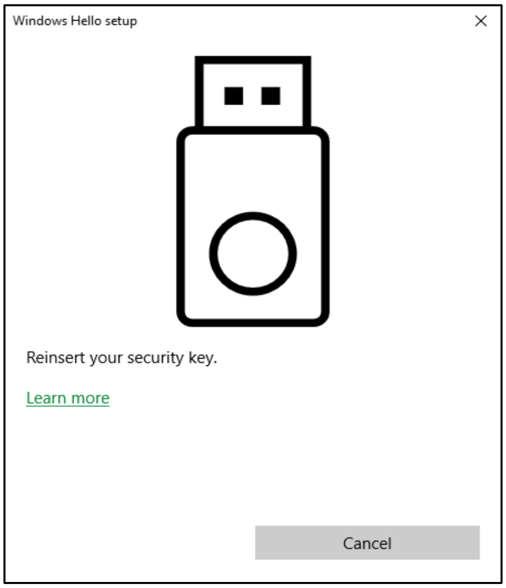
The following are the steps that you need to take for a factory reset.



Windows Hello setup

**Reset Security Key**

The security key will be reset to factory settings. All data and credentials on this key will be cleared.

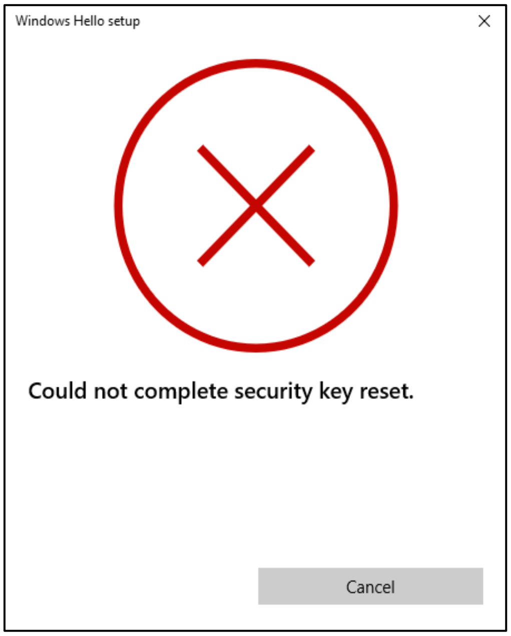


Windows Hello setup

Reinsert your security key.

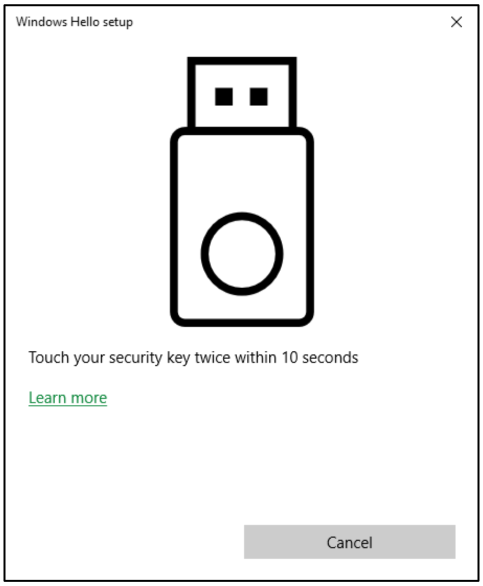
Learn more

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

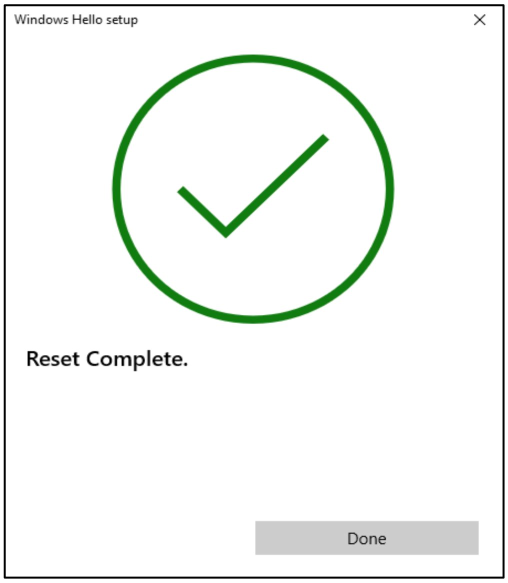

Windows Hello setup

Could not complete security key reset.

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


Windows Hello setup

Touch your security key twice within 10 seconds


Windows Hello setup

Reset Complete.

**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.**

# 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.

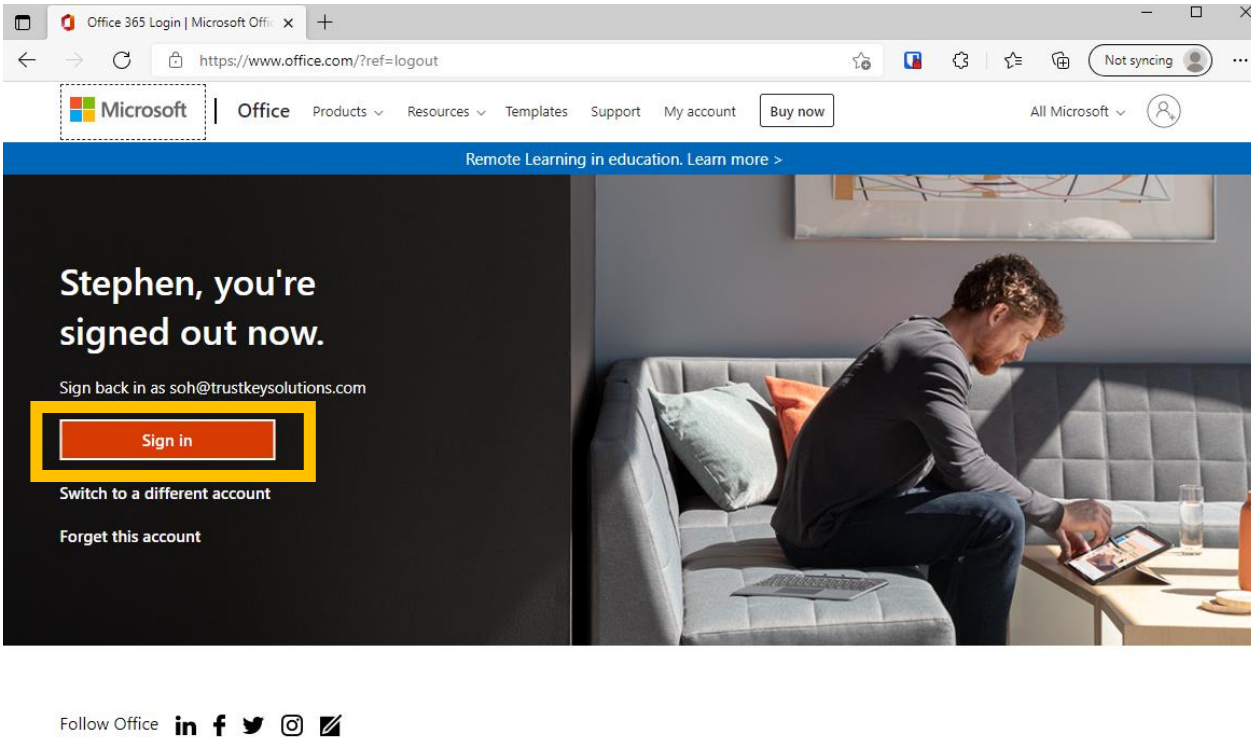
The steps shown below are the case that a user uses www.office.com for the security key registration. The user can use one of the following sites for registration.

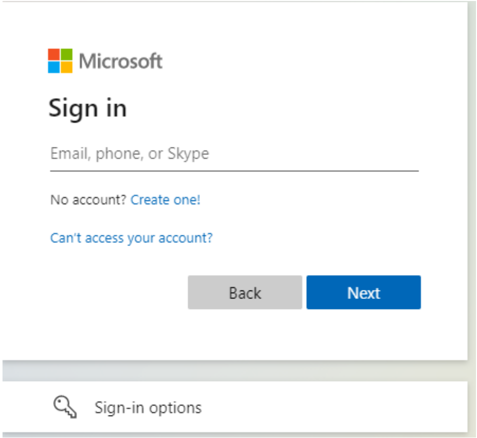
Registration sites:

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.


Office 365 Login | Microsoft Offi
https://www.office.com/?ref=logout
Not syncing
Microsoft
Office
Products
Resources
Templates
Support
My account
Buy now
All Microsoft
Remote Learning in education. Learn more >
Stephen, you're signed out now.
Sign back in as soh@trustkeysolutions.com
Sign in
Switch to a different account
Forget this account
Follow Office


Microsoft

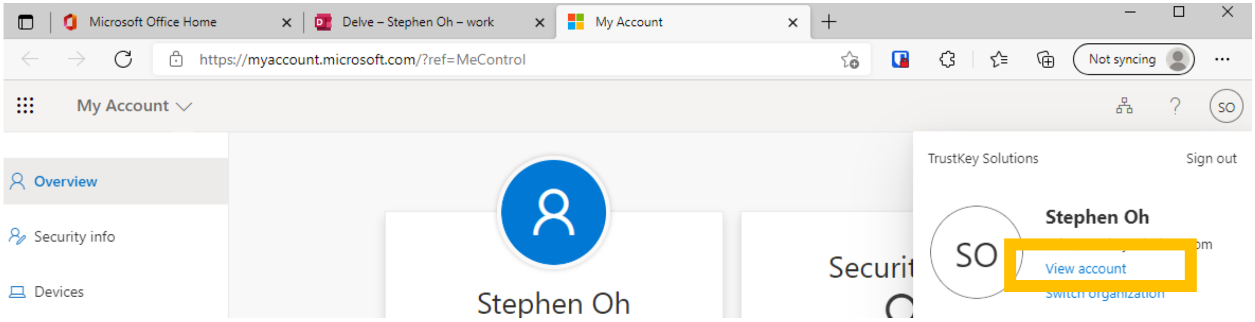
Sign in

Email, phone, or Skype

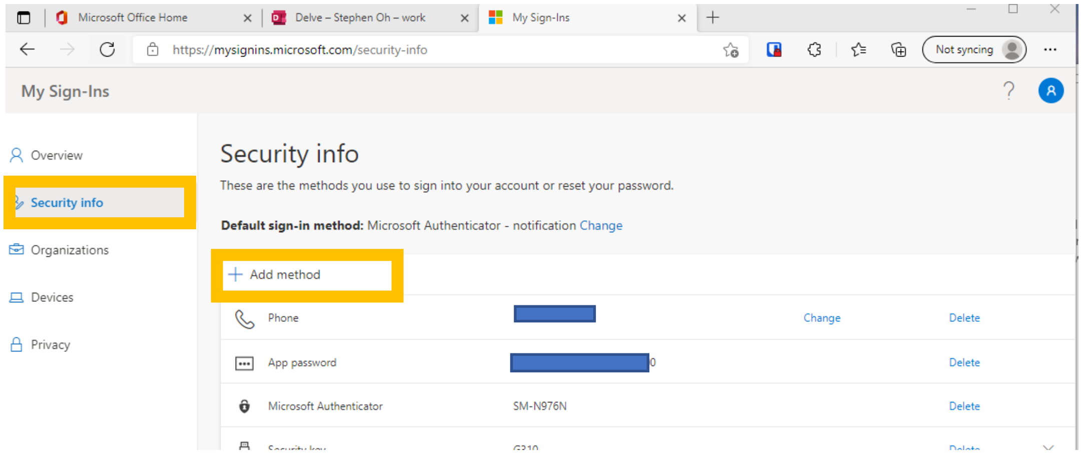
No account? Create one!

Can't access your account?

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



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



Security info

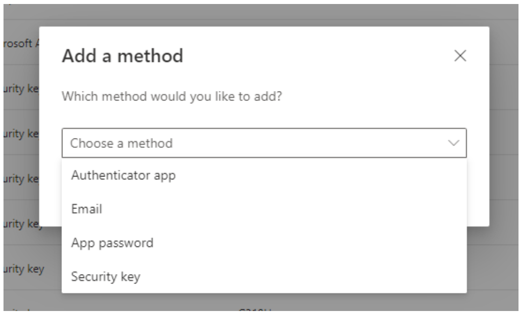
These are the methods you use to sign into your account or reset your password.

**Default sign-in method:** Microsoft Authenticator - notification Change

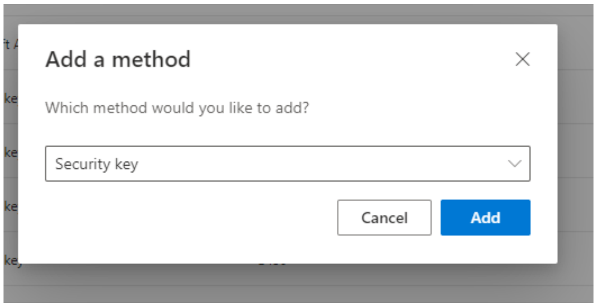
+ Add method

| | | | |
|---|---|---|---|
| Phone | [redacted] | Change | Delete |
| App password | [redacted] | | Delete |
| Microsoft Authenticator | SM-N976N | | Delete |
| Security key | G310 | | Delete |

Step 4: follow the registration flow

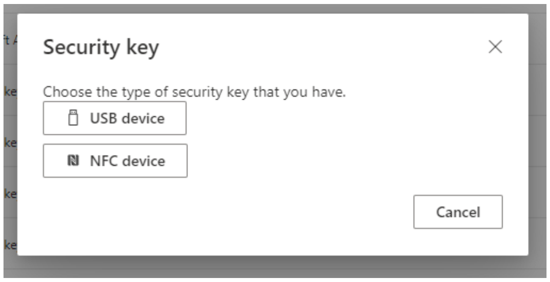

Add a method

Which method would you like to add?

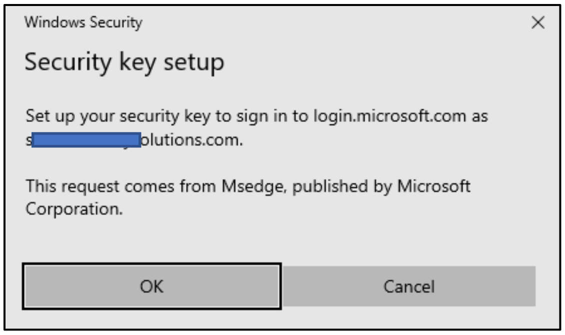

Add a method

Which method would you like to add?

Security key


Security key

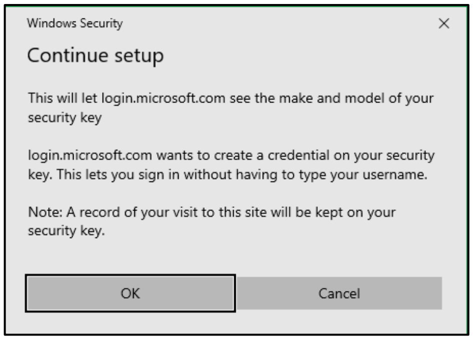
Choose the type of security key that you have.


Windows Security

Security key setup

Set up your security key to sign in to login.microsoft.com as s[redacted]olutions.com.

This request comes from Msedge, published by Microsoft Corporation.

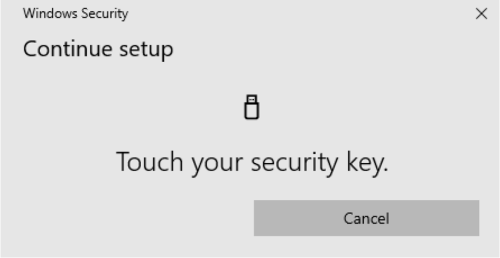

Windows Security

Continue setup

This will let login.microsoft.com see the make and model of your security key

login.microsoft.com wants to create a credential on your security key. This lets you sign in without having to type your username.

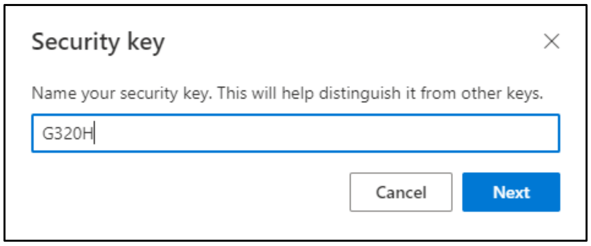
Note: A record of your visit to this site will be kept on your security key.


Windows Security

Continue setup

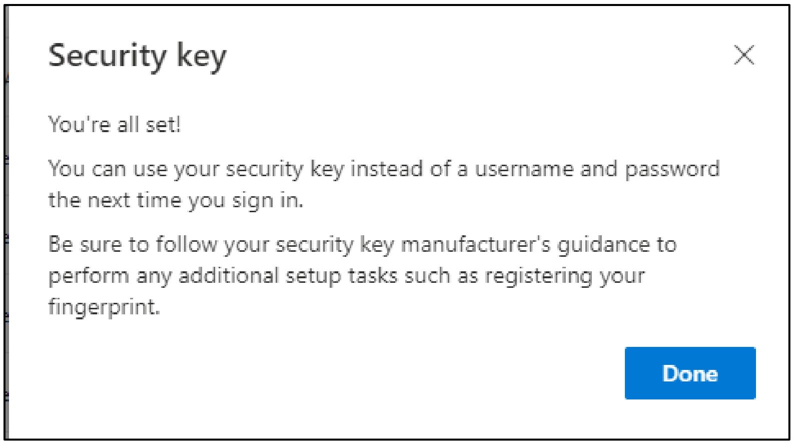
Touch your security key.

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.


Security key

Name your security key. This will help distinguish it from other keys.

G320H



Security key

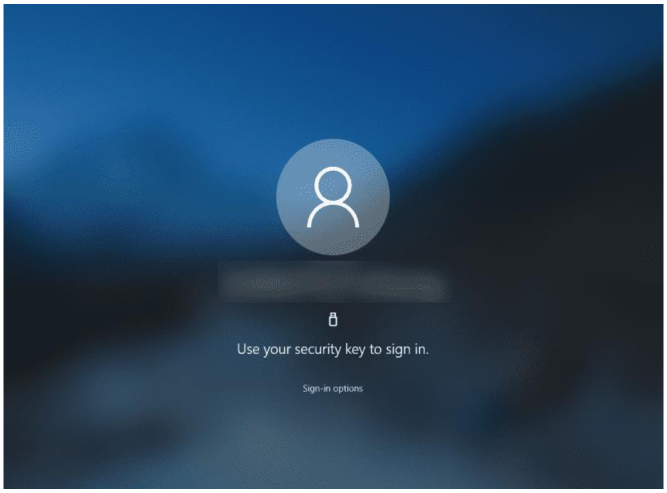
You're all set!

You can use your security key instead of a username and password the next time you sign in.

Be sure to follow your security key manufacturer's guidance to perform any additional setup tasks such as registering your fingerprint.

### 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)



Use your security key to sign in.

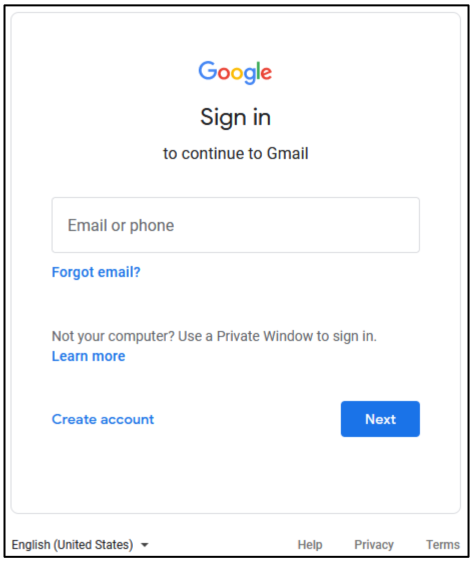
Note: Please refer to our blog here for more information.

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

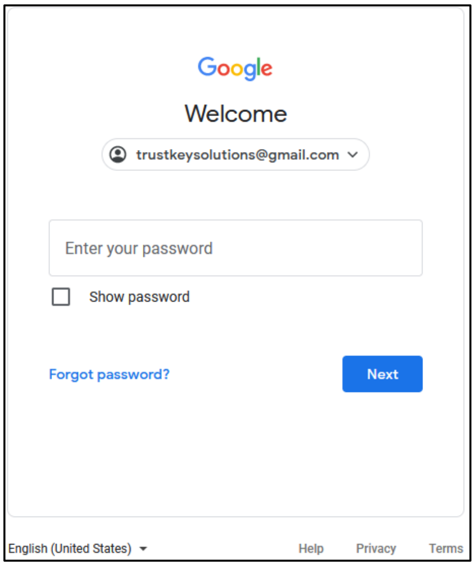
## 2. Google G-suite

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.

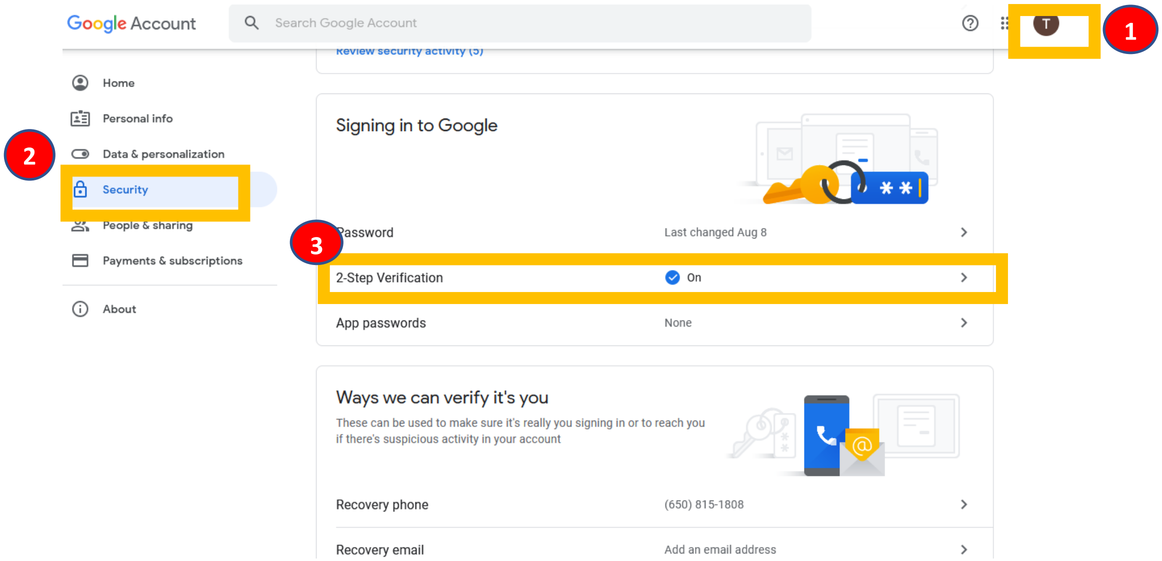


Not your computer? Use a Private Window to sign in.



trustkeysolutions@gmail.com

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

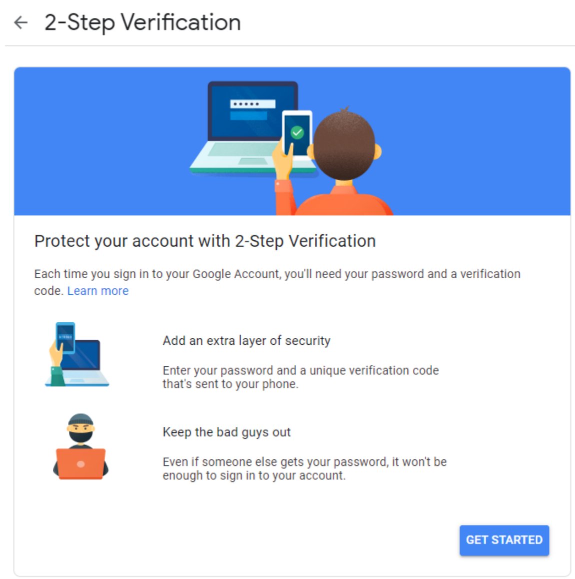


| | |
|---|---|
| Password | Last changed Aug 8 |
| 2-Step Verification | On |
| App passwords | None |

These can be used to make sure it's really you signing in or to reach you if there's suspicious activity in your account

| | |
|---|---|
| Recovery phone | (650) 815-1808 |
| Recovery email | Add an email address |

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



← 2-Step Verification

Protect your account with 2-Step Verification

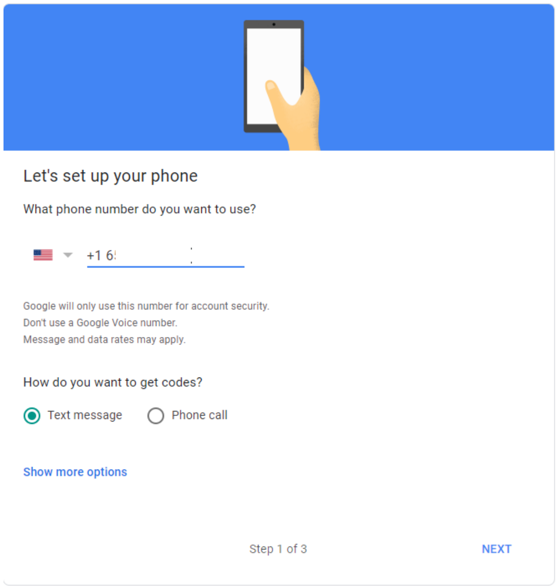
Each time you sign in to your Google Account, you'll need your password and a verification code. Learn more

Add an extra layer of security

Enter your password and a unique verification code that's sent to your phone.

Keep the bad guys out

Even if someone else gets your password, it won't be enough to sign in to your account.



Let's set up your phone

What phone number do you want to use?

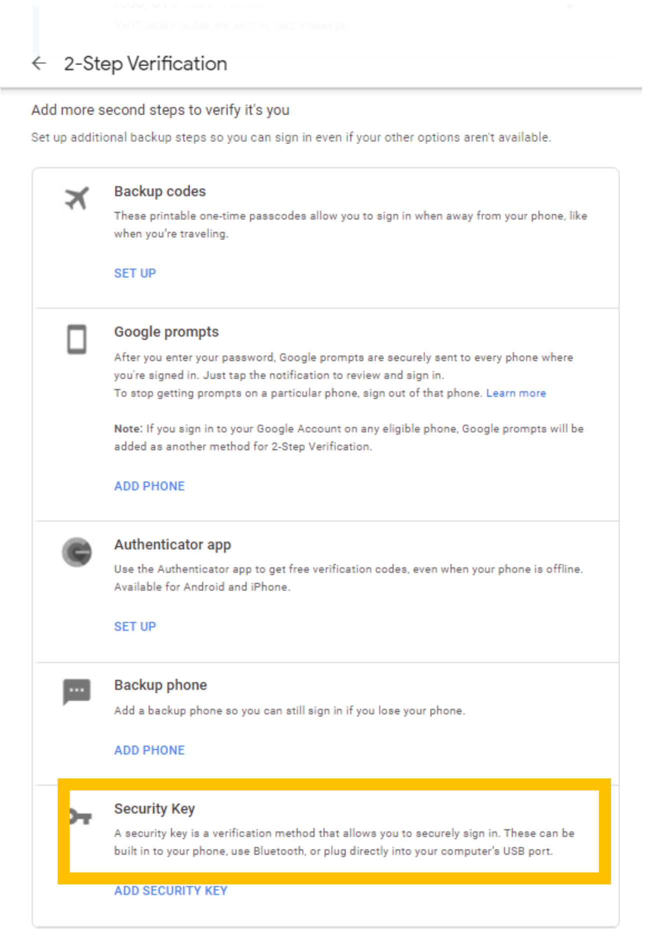
+1 6

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

How do you want to get codes?

● Text message ○ Phone call

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



← 2-Step Verification

Add more second steps to verify it's you

Set up additional backup steps so you can sign in even if your other options aren't available.

**Backup codes**

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

**Google prompts**

After you enter your password, Google prompts are securely sent to every phone where you're signed in. Just tap the notification to review and sign in.
To stop getting prompts on a particular phone, sign out of that phone. Learn more

**Note:** If you sign in to your Google Account on any eligible phone, Google prompts will be added as another method for 2-Step Verification.

**Authenticator app**

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

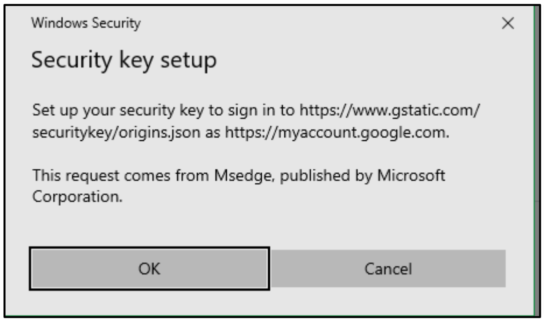
**Backup phone**

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

**Security Key**

A security key is a verification method that allows you to securely sign in. These can be built in to your phone, use Bluetooth, or plug directly into your computer's USB port.

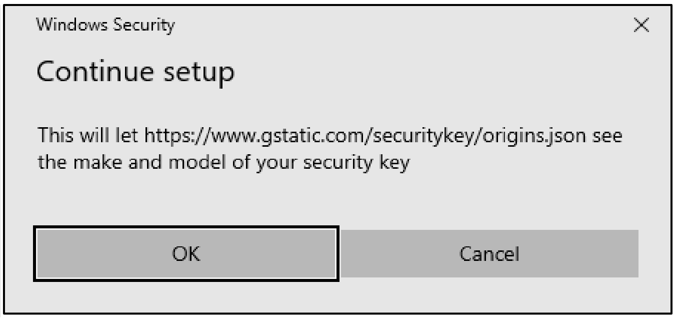
Step 5: follow the browser's instructions



Security key setup

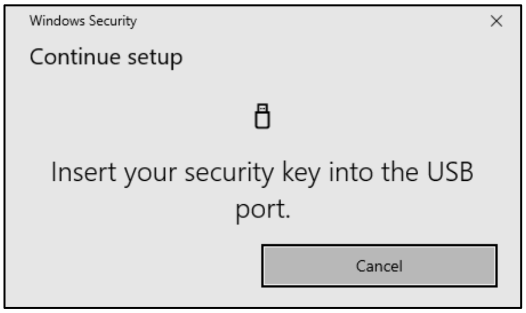
Set up your security key to sign in to https://www.gstatic.com/securitykey/origins.json as https://myaccount.google.com.

This request comes from Msedge, published by Microsoft Corporation.



Continue setup

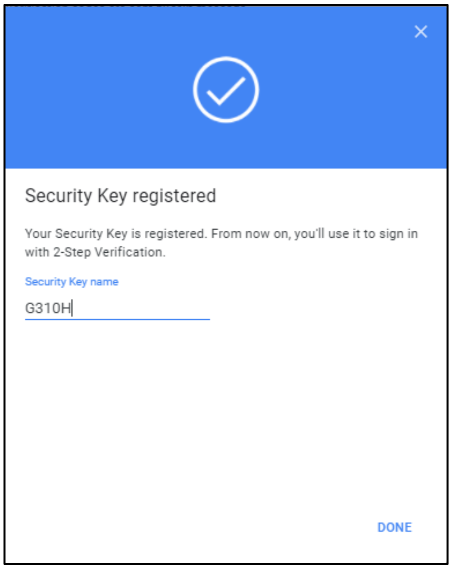
This will let https://www.gstatic.com/securitykey/origins.json see the make and model of your security key



Continue setup

Insert your security key into the USB port.

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

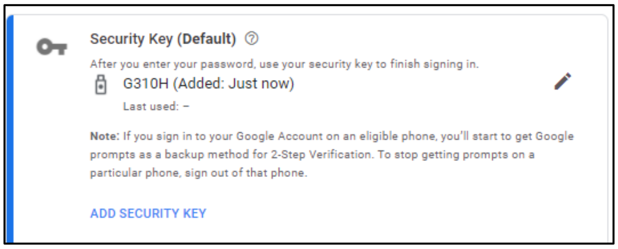


Security Key registered

Your Security Key is registered. From now on, you'll use it to sign in with 2-Step Verification.

Security Key name

G310H



Security Key (Default)

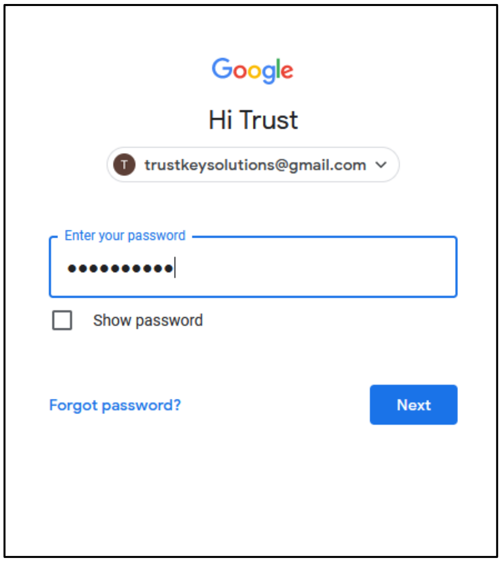
After you enter your password, use your security key to finish signing in.

G310H (Added: Just now)

Last used: –

**Note:** If you sign in to your Google Account on an eligible phone, you'll start to get Google prompts as a backup method for 2-Step Verification. To stop getting prompts on a particular phone, sign out of that phone.

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



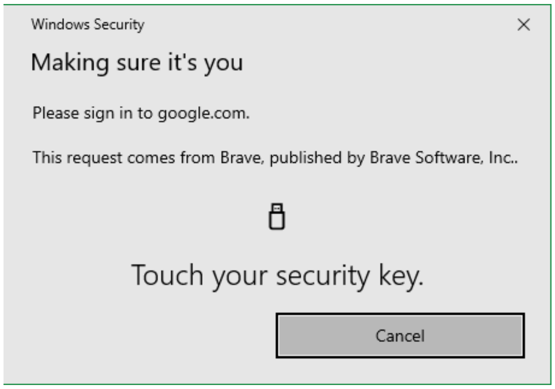
Hi Trust

trustkeysolutions@gmail.com

Enter your password

••••••••••

□ Show password



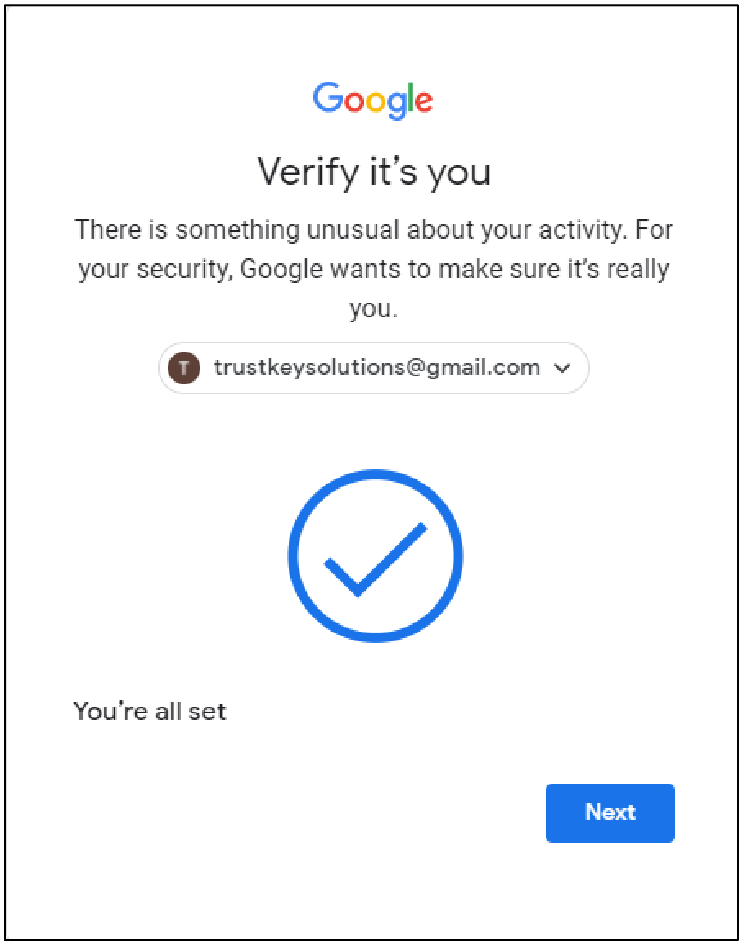
Windows Security

Making sure it's you

Please sign in to google.com.

This request comes from Brave, published by Brave Software, Inc..

Touch your security key.



Verify it’s you

There is something unusual about your activity. For your security, Google wants to make sure it’s really you.

trustkeysolutions@gmail.com

You’re all set

## 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.

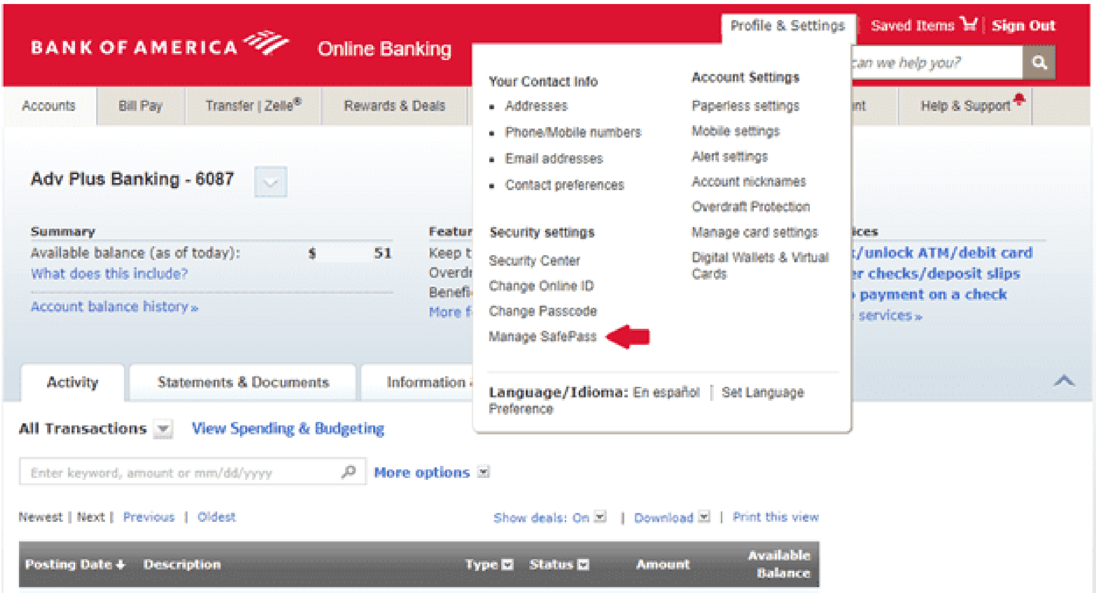
Bank of America allows customers to increase the protection of online accounts with new Security Key feature.

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.

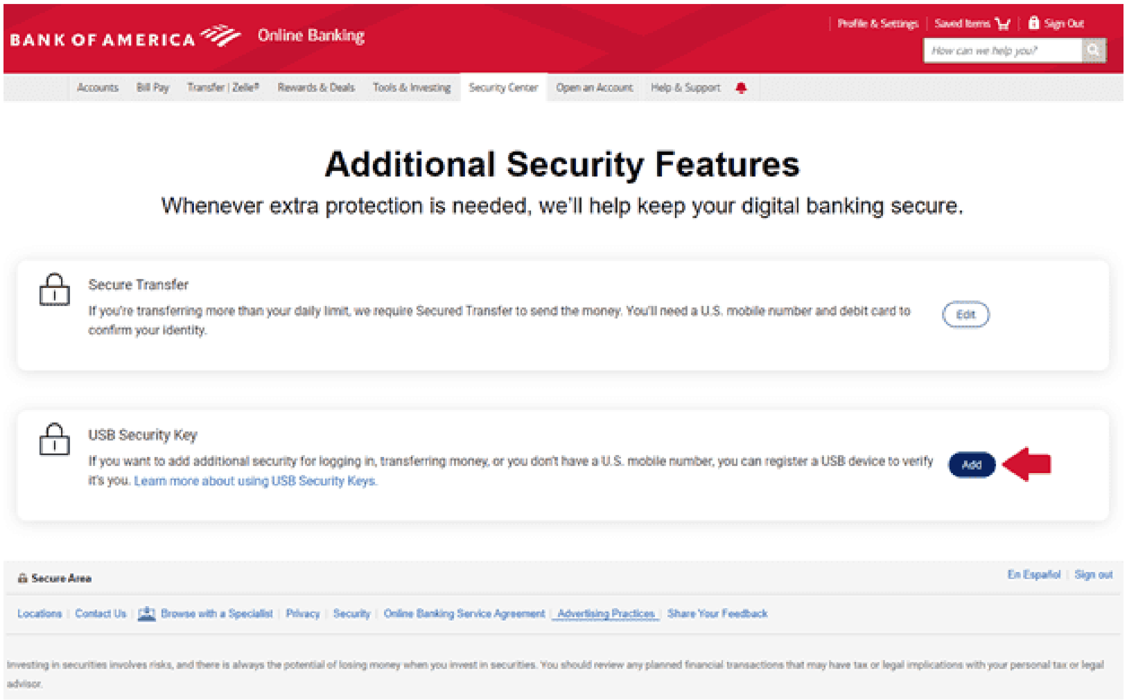
SafePass has long been Bank of America's solution to provide an additional layer of security against unauthorized transactions. However, SafePass only allows customers to use mobile authentication with a one-time code. With the introduction of the Secured Transfer feature, Bank of America has managed 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.



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



## Additional Security Features

Whenever extra protection is needed, we'll help keep your digital banking secure.

Secure Transfer

If you're transferring more than your daily limit, we require Secured Transfer to send the money. You'll need a U.S. mobile number and debit card to confirm your identity.

Edit

USB Security Key

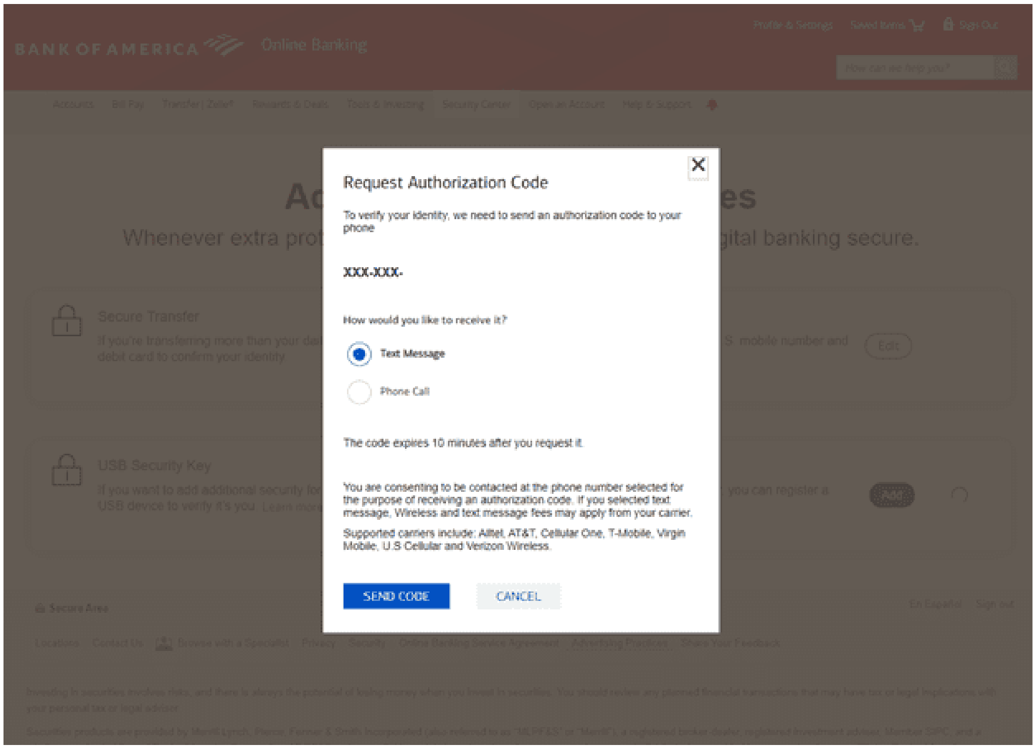
If you want to add additional security for logging in, transferring money, or you don't have a U.S. mobile number, you can register a USB device to verify it's you. Learn more about using USB Security Keys.

Add

Secure Area
En Español | Sign out
Locations | Contact Us | Browse with a Specialist | Privacy | Security | Online Banking Service Agreement | Advertising Practices | Share Your Feedback

Investing in securities involves risks, and there is always the potential of losing money when you invest in securities. You should review any planned financial transactions that may have tax or legal implications with your personal tax or legal advisor.

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



Request Authorization Code

To verify your identity, we need to send an authorization code to your phone

XXX-XXX-

How would you like to receive it?

● Text Message

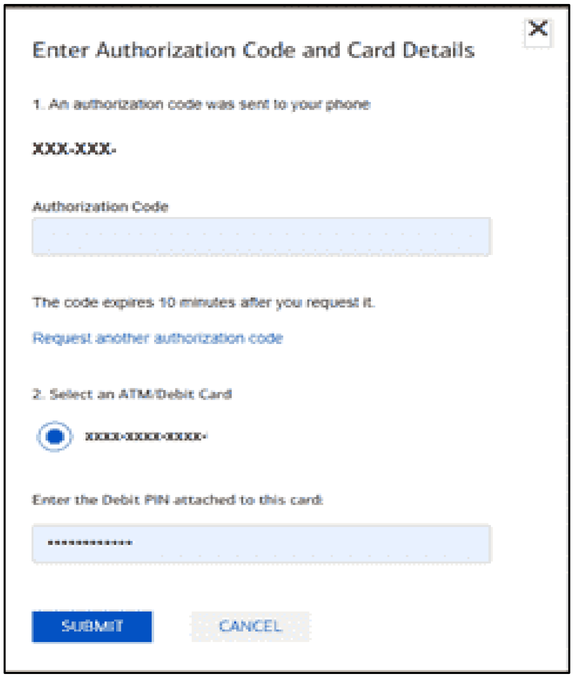
○ Phone Call

The code expires 10 minutes after you request it.

You are consenting to be contacted at the phone number selected for the purpose of receiving an authorization code. If you selected text message, Wireless and text message fees may apply from your carrier.

Supported carriers include: Alltel, AT&T, Cellular One, T-Mobile, Virgin Mobile, U.S Cellular and Verizon Wireless.

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



Enter Authorization Code and Card Details

1. An authorization code was sent to your phone

XXX-XXX-

Authorization Code

The code expires 10 minutes after you request it.

Request another authorization code

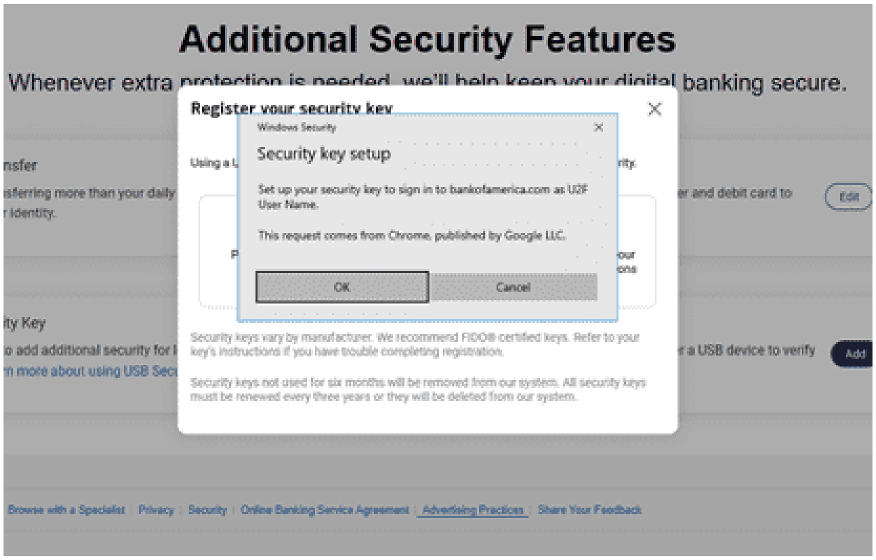
2. Select an ATM/Debit Card

● XXXX-XXXX-XXXX-

Enter the Debit PIN attached to this card:

************

Step 5: Click OK to Security key setup popup.



Additional Security Features

Whenever extra protection is needed, we'll help keep your digital banking secure.

Register your security key

Windows Security

Security key setup

Set up your security key to sign in to bankofamerica.com as U2F User Name.

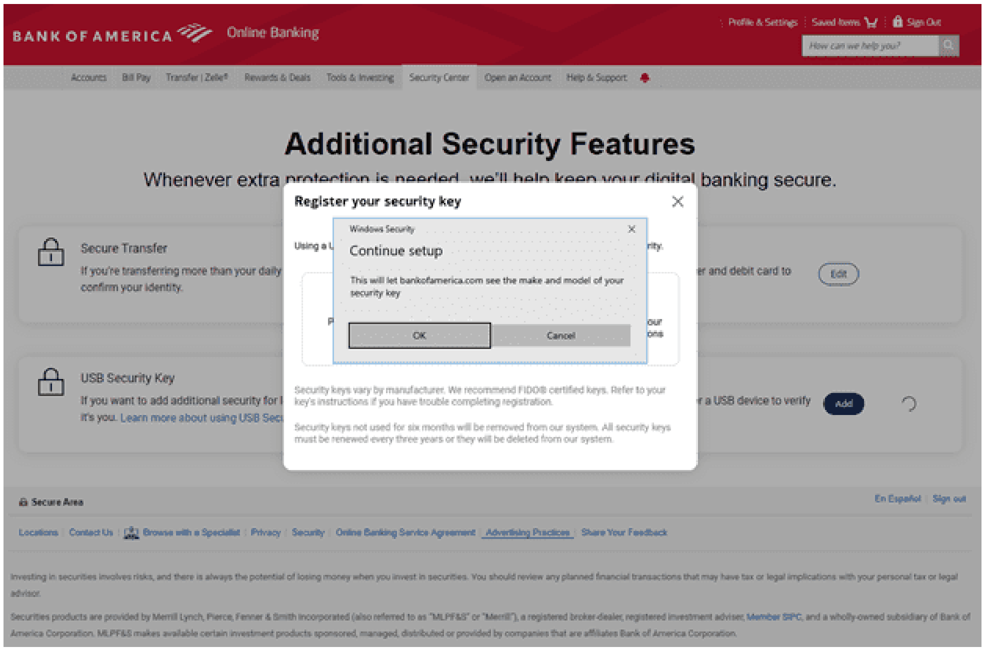
This request comes from Chrome, published by Google LLC.

Security keys vary by manufacturer. We recommend FIDO® certified keys. Refer to your key's instructions if you have trouble completing registration.

Security keys not used for six months will be removed from our system. All security keys must be renewed every three years or they will be deleted from our system.

OK
Cancel
nsfer
sferring more than your daily
r identity.
Using a U
rity.
er and debit card to
Edit
ity Key
o add additional security for
n more about using USB Sec
r a USB device to verify
Add
Browse with a Specialist | Privacy | Security | Online Banking Service Agreement | Advertising Practices | Share Your Feedback

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



BANK OF AMERICA Online Banking

Profile & Settings | Saved Items | Sign Out

How can we help you?

Accounts | Bill Pay | Transfer | Zelle® | Rewards & Deals | Tools & Investing | Security Center | Open an Account | Help & Support

## Additional Security Features

Whenever extra protection is needed, we'll help keep your digital banking secure.

Secure Transfer

If you're transferring more than your daily … er and debit card to confirm your identity.

Edit

USB Security Key

If you want to add additional security for … r a USB device to verify it's you. Learn more about using USB Sec…

Add

**Register your security key**

Using a U… rity.

Windows Security

Continue setup

This will let bankofamerica.com see the make and model of your security key

OK | Cancel

Security keys vary by manufacturer. We recommend FIDO® certified keys. Refer to your key's instructions if you have trouble completing registration.

Security keys not used for six months will be removed from our system. All security keys must be renewed every three years or they will be deleted from our system.

Secure Area

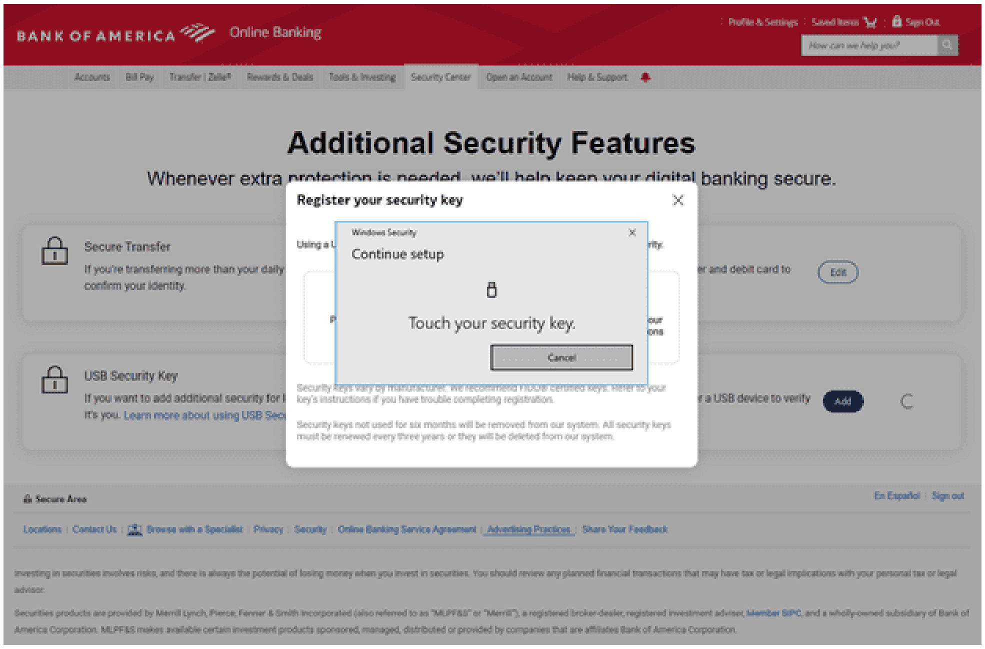
En Español | Sign out

Locations | Contact Us | Browse with a Specialist | Privacy | Security | Online Banking Service Agreement | Advertising Practices | Share Your Feedback

Investing in securities involves risks, and there is always the potential of losing money when you invest in securities. You should review any planned financial transactions that may have tax or legal implications with your personal tax or legal advisor.

Securities products are provided by Merrill Lynch, Pierce, Fenner & Smith Incorporated (also referred to as "MLPF&S" or "Merrill"), a registered broker-dealer, registered investment adviser, Member SIPC, and a wholly-owned subsidiary of Bank of America Corporation. MLPF&S makes available certain investment products sponsored, managed, distributed or provided by companies that are affiliates Bank of America Corporation.

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



BANK OF AMERICA Online Banking

Profile & Settings | Saved Items | Sign Out

How can we help you?

Accounts | Bill Pay | Transfer | Zelle® | Rewards & Deals | Tools & Investing | Security Center | Open an Account | Help & Support

## Additional Security Features

Whenever extra protection is needed, we'll help keep your digital banking secure.

Secure Transfer

If you're transferring more than your daily … er and debit card to confirm your identity.

Edit

USB Security Key

If you want to add additional security for … r a USB device to verify it's you. Learn more about using USB Sec…

Add

**Register your security key**

Using a U… rity.

Windows Security

Continue setup

Touch your security key.

Cancel

Security keys vary by manufacturer. We recommend FIDO® certified keys. Refer to your key's instructions if you have trouble completing registration.

Security keys not used for six months will be removed from our system. All security keys must be renewed every three years or they will be deleted from our system.

Secure Area

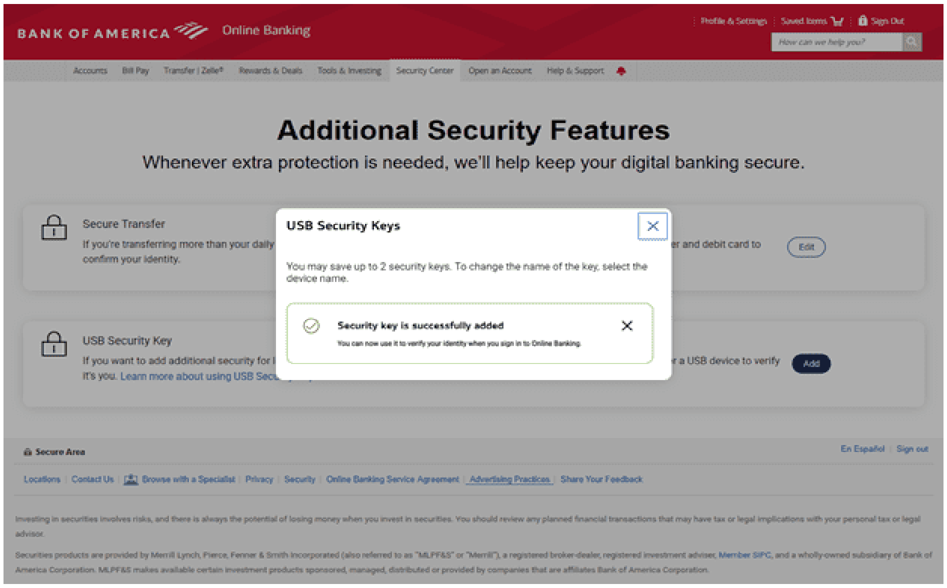
En Español | Sign out

Locations | Contact Us | Browse with a Specialist | Privacy | Security | Online Banking Service Agreement | Advertising Practices | Share Your Feedback

Investing in securities involves risks, and there is always the potential of losing money when you invest in securities. You should review any planned financial transactions that may have tax or legal implications with your personal tax or legal advisor.

Securities products are provided by Merrill Lynch, Pierce, Fenner & Smith Incorporated (also referred to as "MLPF&S" or "Merrill"), a registered broker-dealer, registered investment adviser, Member SIPC, and a wholly-owned subsidiary of Bank of America Corporation. MLPF&S makes available certain investment products sponsored, managed, distributed or provided by companies that are affiliates Bank of America Corporation.

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



Additional Security Features

Whenever extra protection is needed, we'll help keep your digital banking secure.

Secure Transfer

If you're transferring more than your daily … er and debit card to confirm your identity.

USB Security Key

If you want to add additional security for l… r a USB device to verify it's you. Learn more about using USB Secu…

USB Security Keys

You may save up to 2 security keys. To change the name of the key, select the device name.

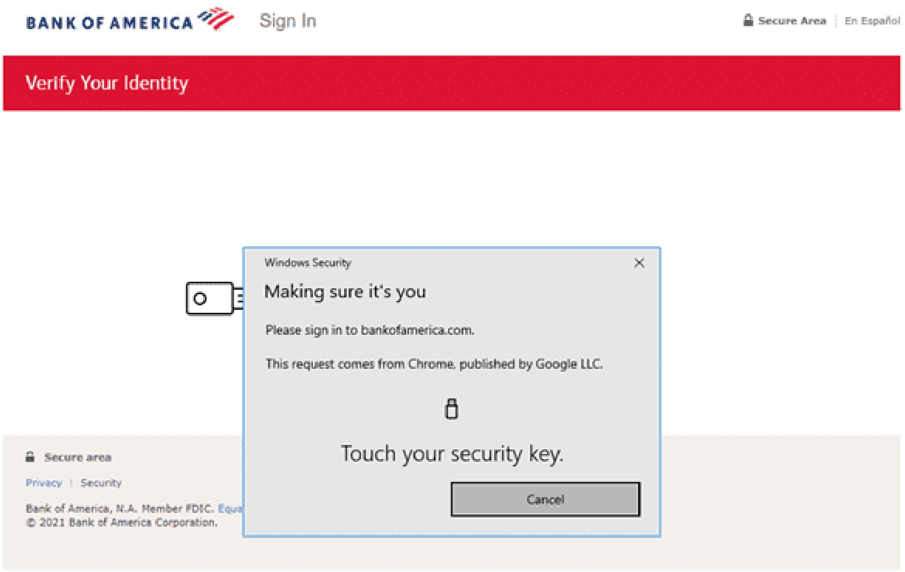
Security key is successfully added

You can now use it to verify your identity when you sign in to Online Banking.

Investing in securities involves risks, and there is always the potential of losing money when you invest in securities. You should review any planned financial transactions that may have tax or legal implications with your personal tax or legal advisor.

Securities products are provided by Merrill Lynch, Pierce, Fenner & Smith Incorporated (also referred to as "MLPF&S" or "Merrill"), a registered broker-dealer, registered investment adviser, Member SIPC, and a wholly-owned subsidiary of Bank of America Corporation. MLPF&S makes available certain investment products sponsored, managed, distributed or provided by companies that are affiliates Bank of America Corporation.

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.



Verify Your Identity

Windows Security

Making sure it's you

Please sign in to bankofamerica.com.

This request comes from Chrome, published by Google LLC.

Touch your security key.

Bank of America, N.A. Member FDIC. Equa…
© 2021 Bank of America Corporation.

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.

## 4. Other Online services

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

Dropbox yahoo!

YouTube facebook. twitter

GitHub

LOGIN.GOV

1Password bitwarden

ebay

# 7. Windows Hello Set-up Guide

## What is Windows Hello?

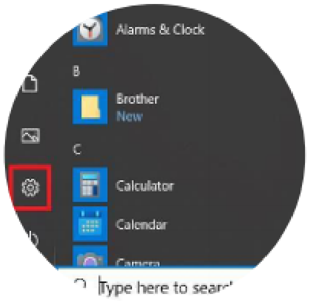
Microsoft Windows Hello, part of Windows 10, gives users a personal, secured experience where the device is authenticated based on their presence. Users can log in with a look or a touch, with no need for a password. In conjunction with Microsoft Passport, biometric authentication uses fingerprints or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

Note:

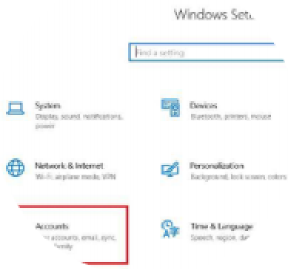
Please note that Fingerprint enrolment for **Windows Hello** and **USB Security Key** is different
The user needs to enroll the user's fingerprint separately with Windows Hello (for PC login) and a security Key (for Web login).

- 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

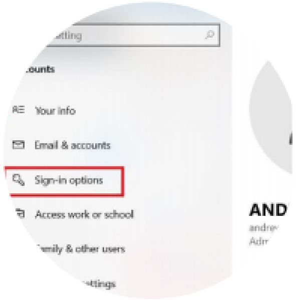


1. From the Start Menu, select **Settings**.

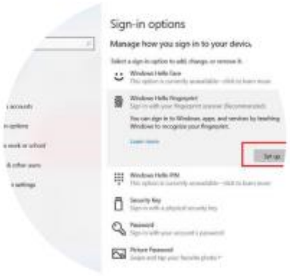

Windows Sett
Find a setting
System
Display, sound, notifications, power
Devices
Bluetooth, printers, mouse
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Accounts
accounts, email, sync, family
Time & Language
Speech, region, da

2. Select **Accounts.**

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



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!

# 8. Additional Services

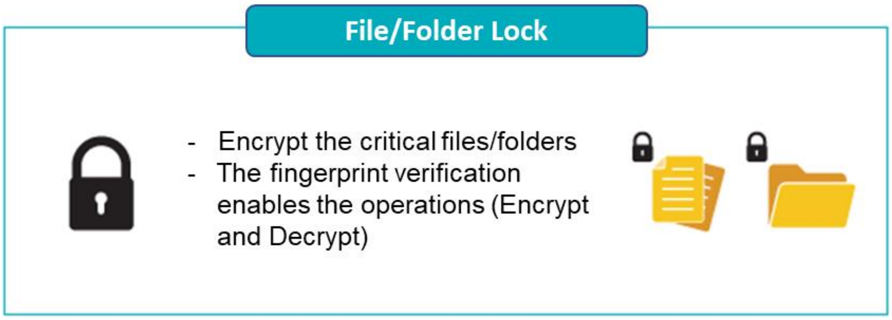
## 1. TrustKey ThumbLock Solution

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.

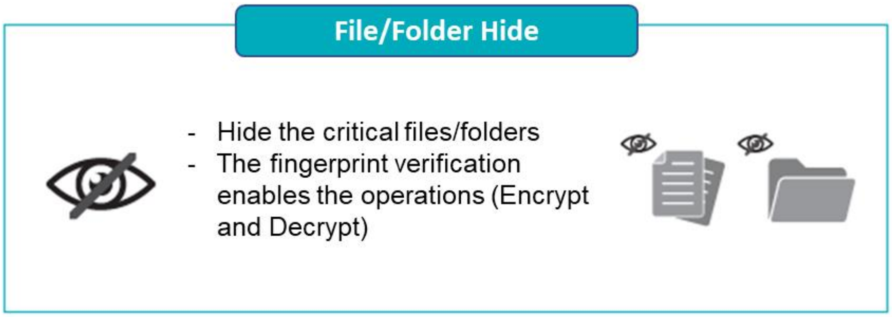
**Fingerprint Verification**

Registered Users Only



**File/Folder Lock**

- Encrypt the critical files/folders
- The fingerprint verification enables the operations (Encrypt and Decrypt)



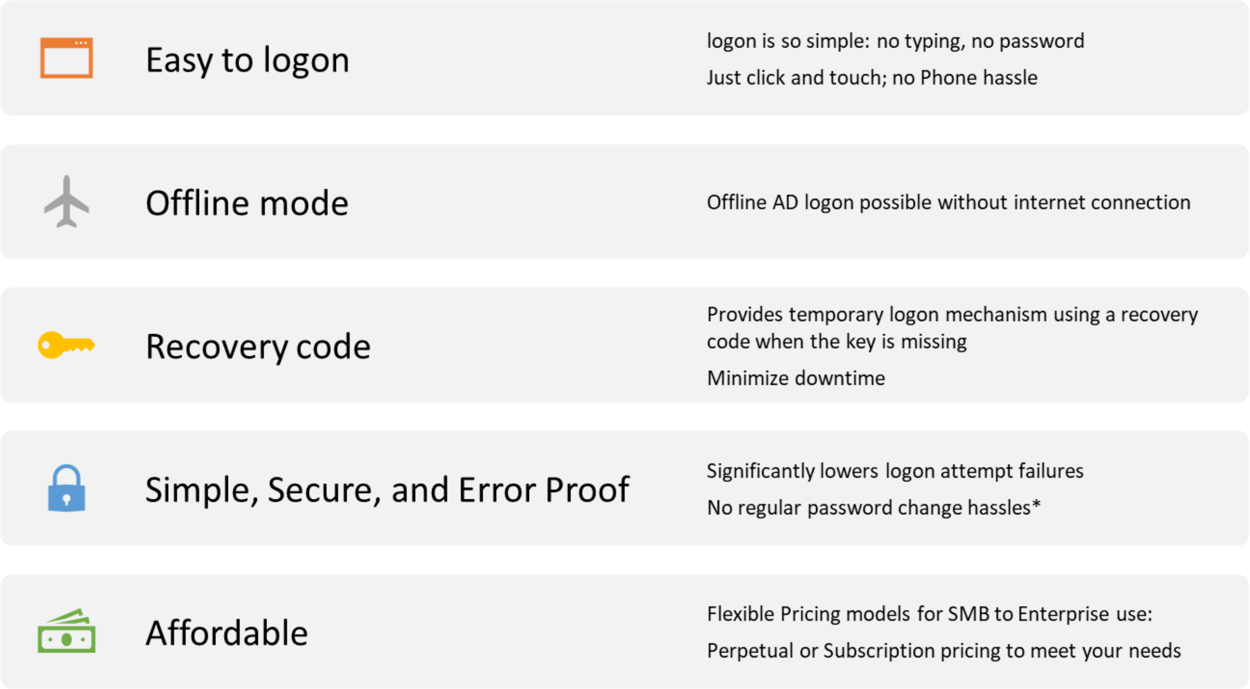
**File/Folder Hide**

- Hide the critical files/folders
- The fingerprint verification enables the operations (Encrypt and Decrypt)

## 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<br>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<br>Minimize downtime |
| Simple, Secure, and Error Proof | Significantly lowers logon attempt failures<br>No regular password change hassles* |
| Affordable | Flexible Pricing models for SMB to Enterprise use:<br>Perpetual or Subscription pricing to meet your needs |

# Appendix

## 1. Frequently Asked Questions

### Using G-Series Security Keys

**How do you enroll your fingerprint to the G-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 G-Series keys hold?**

G-Series keys can hold up to 150 resident keys.

**What should I do if the key is locked?**

For security reasons, the G-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.

## Supported Platform · Environment

**Which OS does Key Manager support?**

Key Manager supports Windows, macOS, and Linux

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

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

**Which web browsers do you support?**

G-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.

## G-Series Security Key Features

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

G-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?**

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

**Can I use the security key on different computers?**

Sure! G-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?**

G-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.

**How to enroll the fingerprint to the G-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?**

G-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?**

G-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@trustkeysolutions.com

## 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.

## 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

| Consumer Complaint | | | Resolution | |
|---|---|---|---|---|
| | | | Under warranty | After warranty |
| Malfunction under normal conditions of use | When the product requires major repair within ten (10) days of purchase | | Product exchange or full refund | None |
| | When the product requires major repair within one (1) month of purchase | | Product exchange or refund | |
| | Product exchange not possible | | Full Refund | |
| | When the exchanged product requires major repair within one (1) month | | | |
| | In case of damage caused during transportation when purchasing the product | | Product exchange | |
| | Repair Possible | The same defects occur twice | Free Repair | |
| | | The same defects occur three times | Product exchange or full refund | |
| | | The same defects occur up to five times | | |
| | Repair not possible | Repair is not possible | | |
| | Exchange not possible | When repair is impossible because there are no repair parts within the parts retention period | | Refund by adding 10% to the amount of straight-line depreciation |
| | | If the product requested by the customer for repair is lost | | Refund by adding 10% to the amount of straight-line depreciation (maximum limit: purchase price) |
| malfunction due to the intention or negligence of the consumer | When the repair is possible | | Repair with charge | Repair with charge |
| | 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.)

# Manufacturer Information

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

## 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

**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