V0.1

User Manual for T110/T120

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

Contents

1. USB Security Key from TrustKey Solutions

1. What is a 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 your protected online resources. A Security key can also be referred to as a security token.
A USB Security Key is a security key with a USB interface to connect to a PC.

TrustKey's T110/T120 is an affordable security key with a USB interface from TrustKey Solutions.

There are three factors that a user can present for authentications. The three factors are:

1) What you know – something that the user knows, including password, passphrase, PIN, etc.
2) What you have – physical device including Phone, OTP token, and USB security key
3) Who you are – biometric factors including face, fingerprint, IRIS, etc.

The modern authentication method requires more than one factor. Note that the traditional system with account ID and password represents only one factor: what you know.
Our G310H/G320H can provide two factors using what you have (the key itself) and who you are (fingerprint).
Our T110/T120 is using what you have (the key) and what you know (PIN to the security key) for multi-factor authentication

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

1. You need to register PIN before use. The detailed steps on how to register a PIN will be in Section 2.
2. Choose the correct USB port for your security key (USB-A vs. USB-C)

3. Check the version of your devices including Windows PC, Macs, Android Smartphone and Apple Products.

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

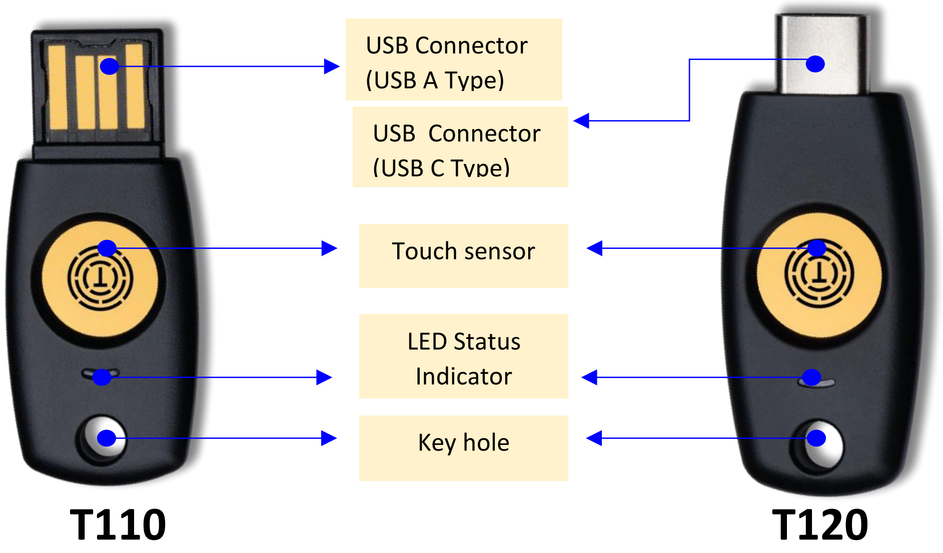
1. Product Specification

Product Name	T110	T120
Model Name	eTA310	eTA320
FIDO Protocol	FIDO2 , U2F	FIDO2 , U2F
FIDO Security Level	Level 1	Level 1
USB Type	Type A	Type C
Authentication Action	PIN + Touch	PIN + Touch
Status Indicator	White color LED	White color LED
Device Type	FIDO2 HID device	FIDO2 HID device
Material	Polycarbonate Gold Plate (touch area)	Polycarbonate Gold Plate (touch area)
Certification	KC, FCC, CE, RoHS	KC, FCC, CE, RoHS
Operation Temp[1]	-20℃ ~ +60℃	-20℃ ~ +60℃
Storage Temp[2]	-40℃ ~ +85℃	-40℃ ~ +85℃
Color	Black	Black
Size	41.89 x 17.8 x 3.8 mm	41.6 x 17.8 x 4.6 mm
Weight	2.9 g	2.9 g

Note:

1. *-4°F ~ 140°F*
2. *-40°F ~ 185°F*

2. Security Key Description



3. LED Status Indicator

Color	Status	Description	Action
□ White	On	- Key connection OK - Authentication Success	
	Blinking		
	Off	Not connected	Reinsert the security key

3. Security Key Fingerprint Enrollment for Windows

1. What is PIN?

A PIN is similar to a password but is used differently. A 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 password information to the server for verification. Unlike a password, a 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.

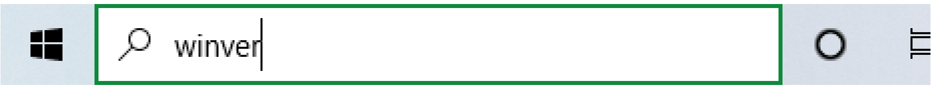
A PIN is needed for fingerprint enrolment and modification. It is also used for backup authentication when the fingerprint authentication has failed.

We recommend that users use a complex combination of digits and letters to ensure that the PIN is not compromised.

2. Windows 10 Version Check

Step 0: Check Windows Version First

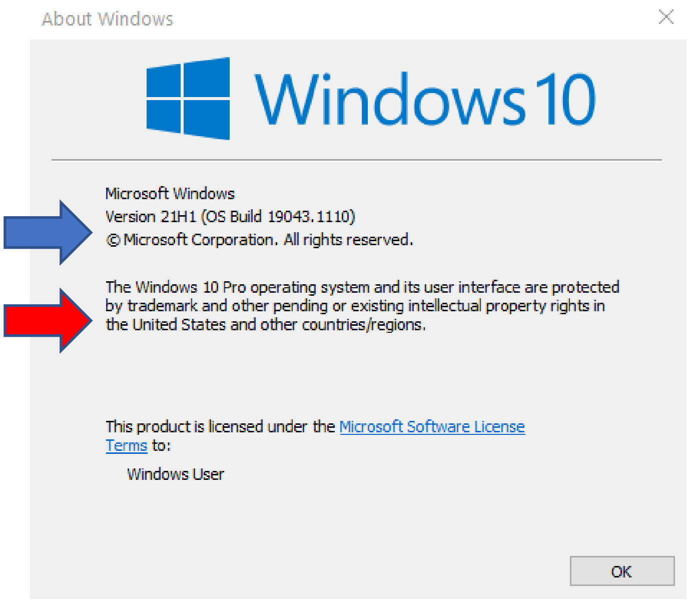
Please check your Windows version before enrolment by typing “winver” at the Windows search bar.



winver

Please check the Windows Product Name (Windows Home, Pro, or Enterprise) as the 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

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.

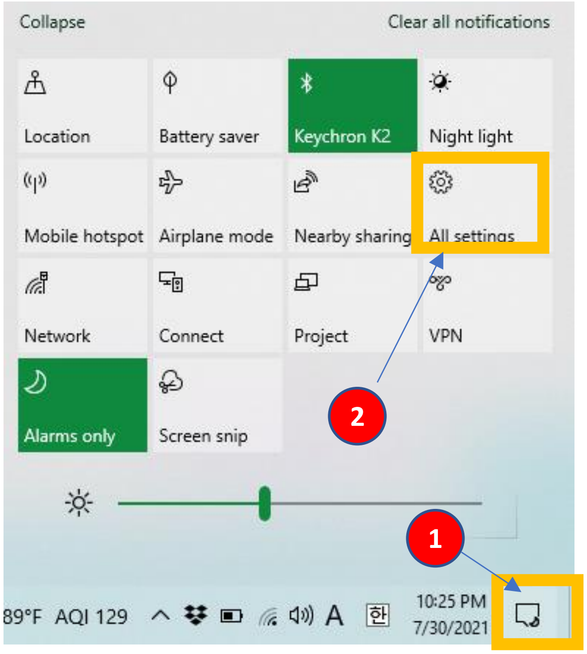
This product is licensed under the Microsoft Software License Terms to:

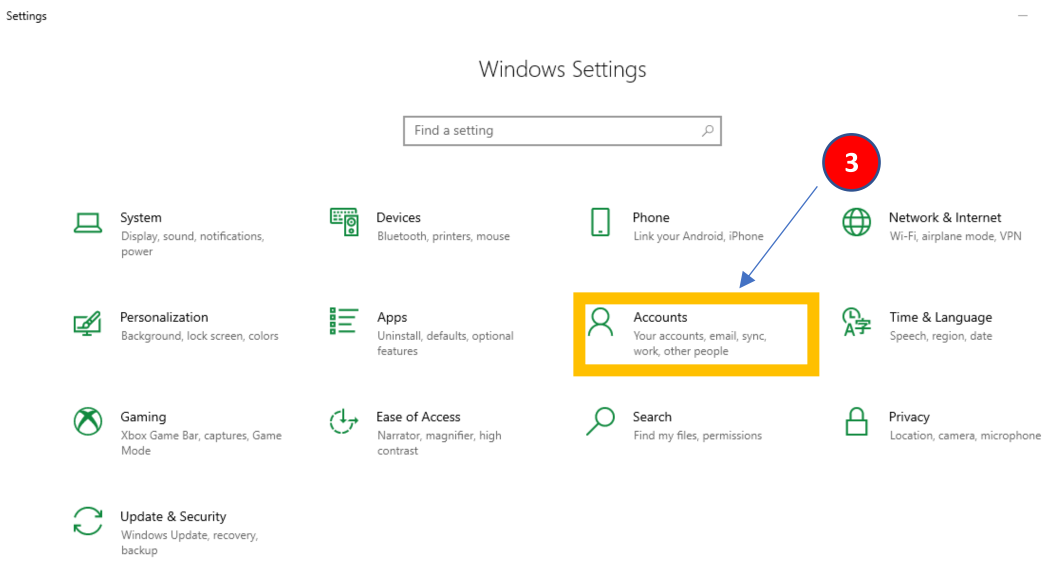
Windows User

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

Step1: Windows Setting

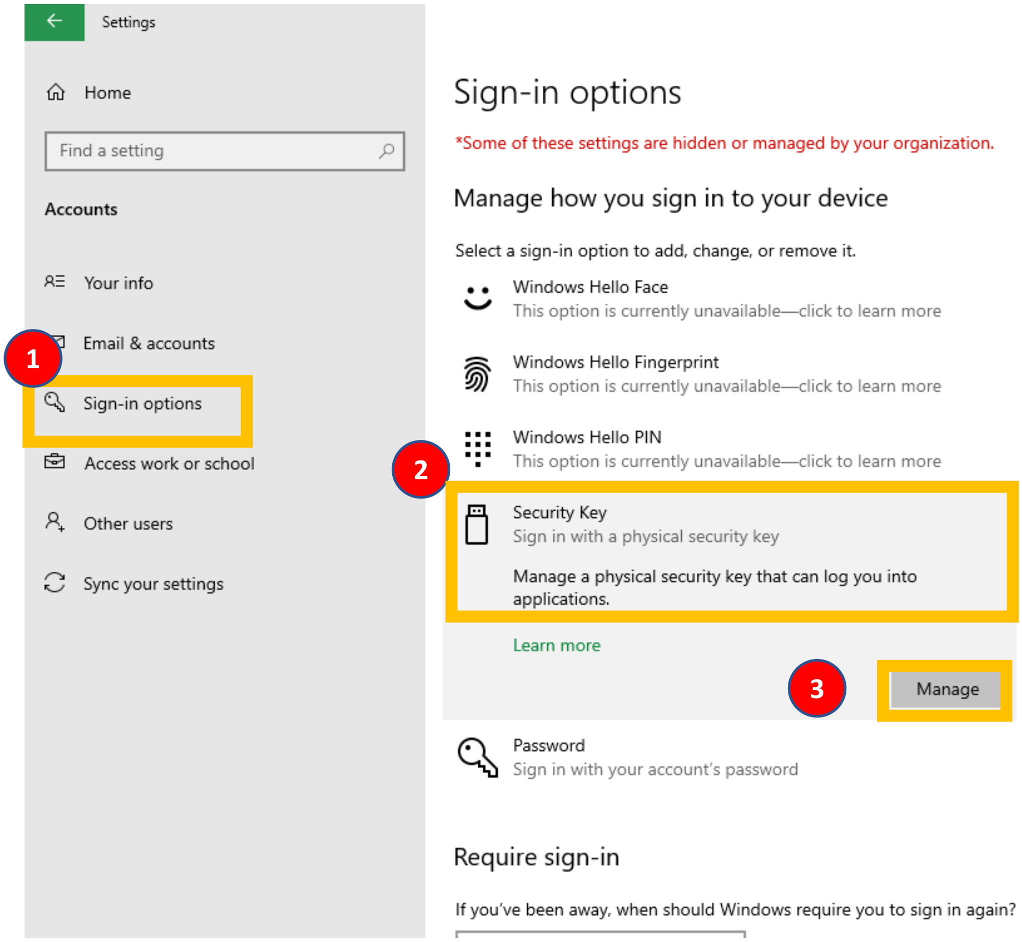
Click the right down corner of the Windows screen ①, select “All settings” ②, and Accounts ③.




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: Sign-in Option

From Settings, click “Sign-in Option” ① and Security Key ②, and Manage ③.



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.

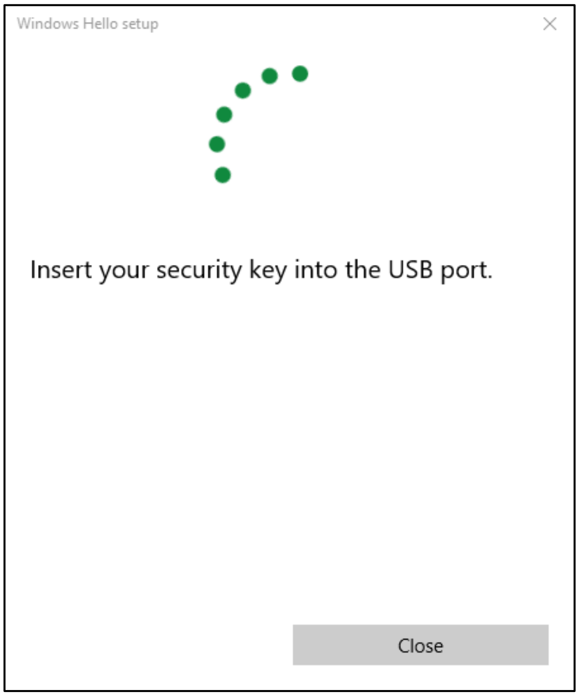
Password
Sign in with your account’s password

Require sign-in

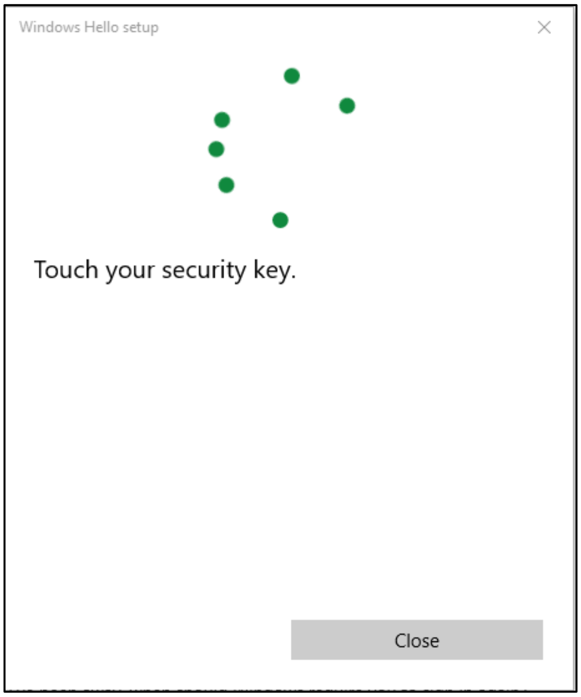
If you’ve been away, when should Windows require you to sign in again?

Step 3: Security Key Management

Insert the security key and touch the key

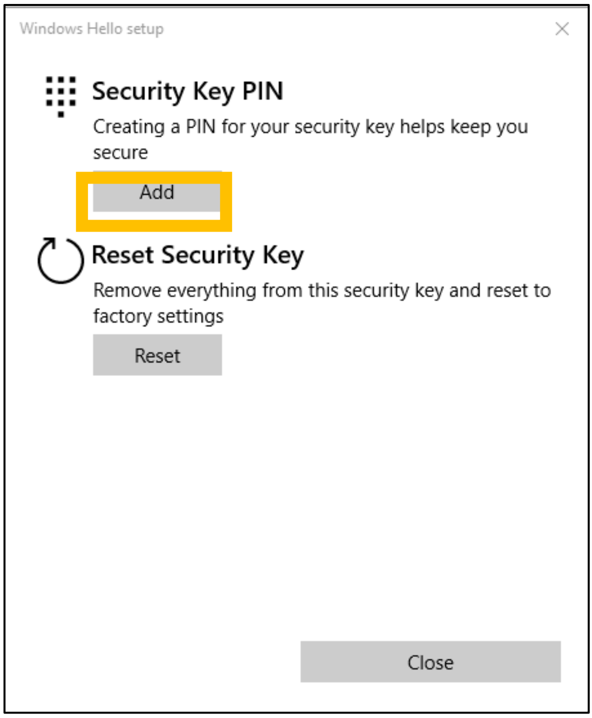


Insert your security key into the USB port.



Touch your security key.

Step 4: Set Up PIN

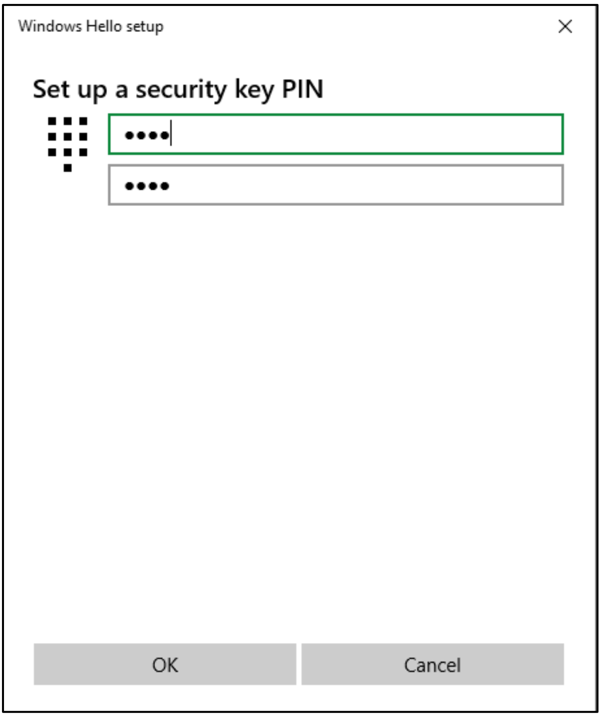


Security Key PIN

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

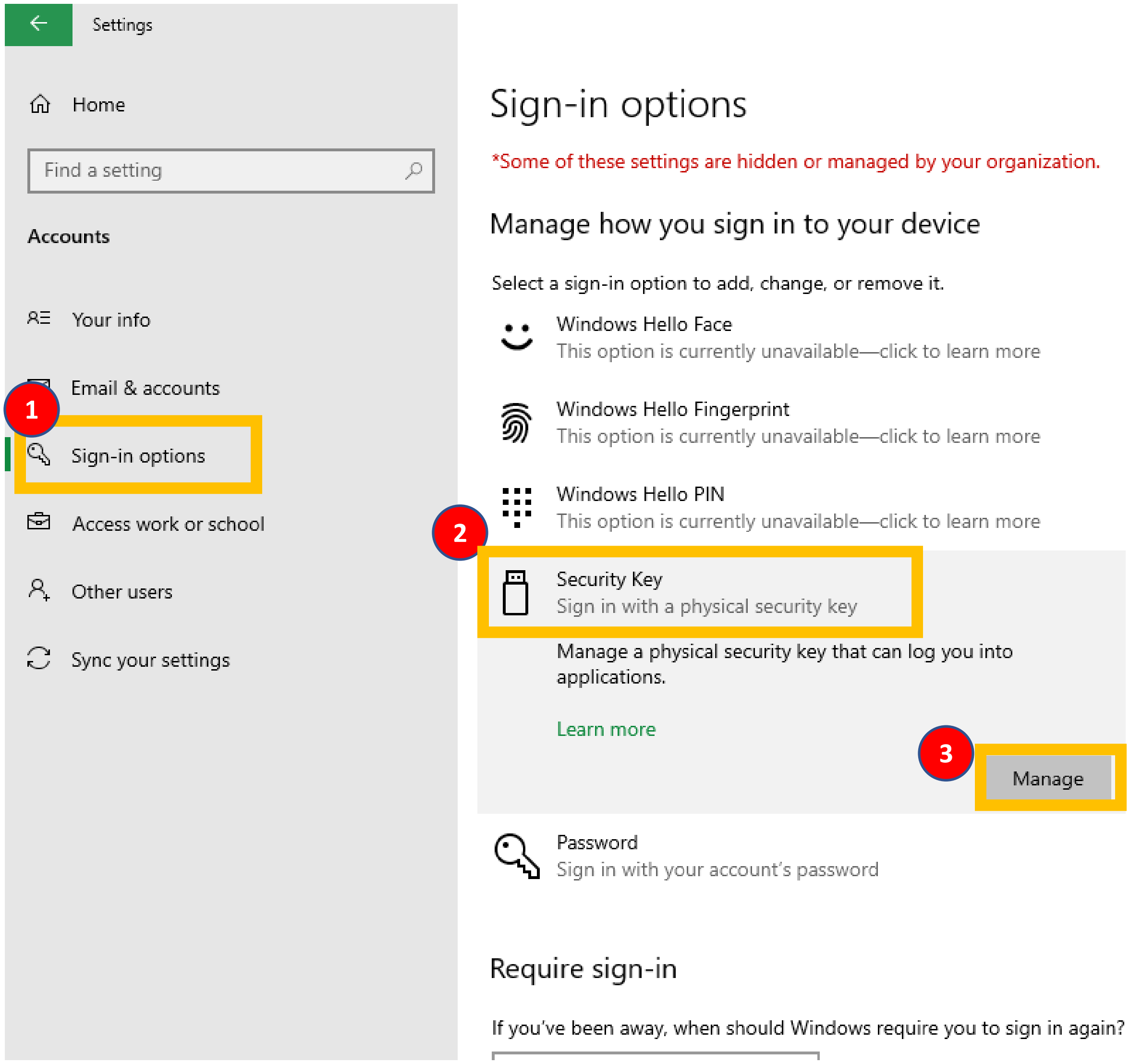
••••

••••

Done!

3. Security Key PIN change Procedure

Step 1: Take the same steps (first two steps) as the PIN 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

2 Security Key
Sign in with a physical security key

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

Learn more

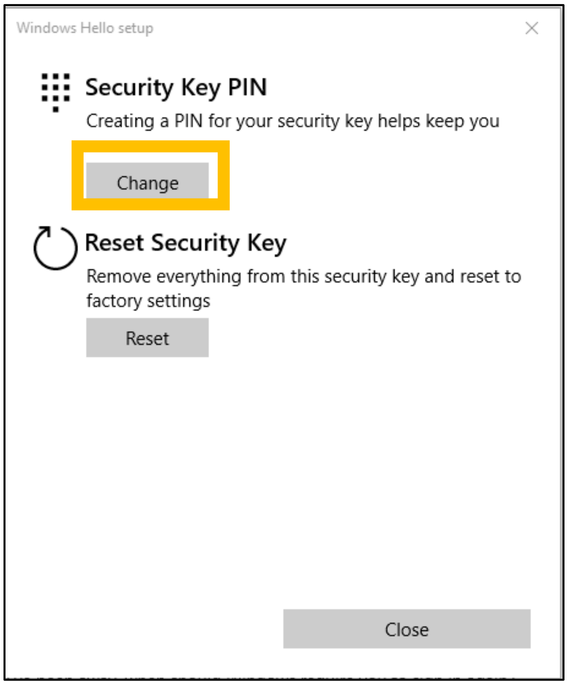
3 Manage

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 2: select “change” and type the PIN in for confirmation. The user needs to input the existing PIN and the new PIN twice.



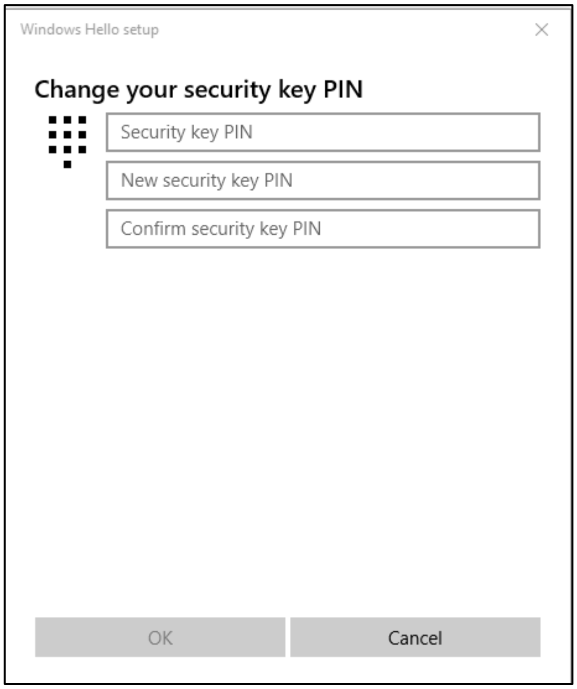
Windows Hello setup

Security Key PIN

Creating a PIN for your security key helps keep you

Reset Security Key

Remove everything from this security key and reset to factory settings



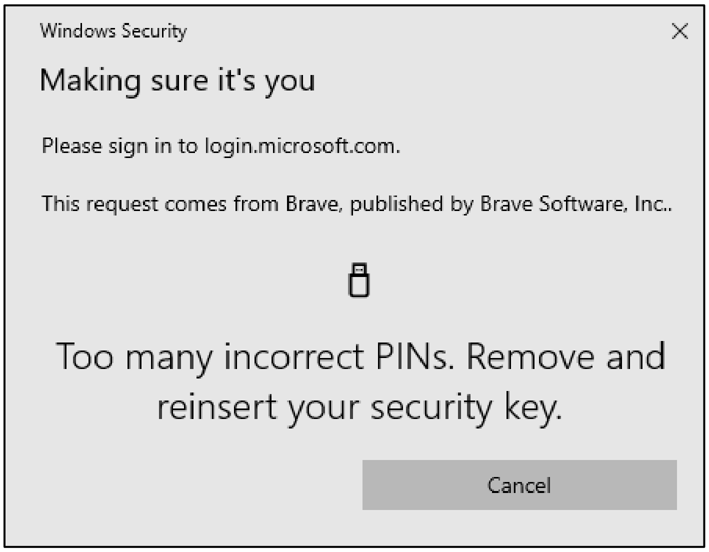
Windows Hello setup

Change your security key PIN

Done!

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

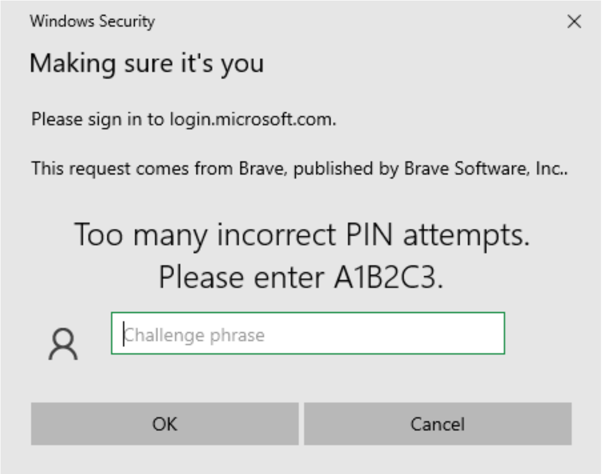
Please sign in to login.microsoft.com.

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 in the correct PIN.

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



Windows Security

Making sure it's you

Please sign in to login.microsoft.com.

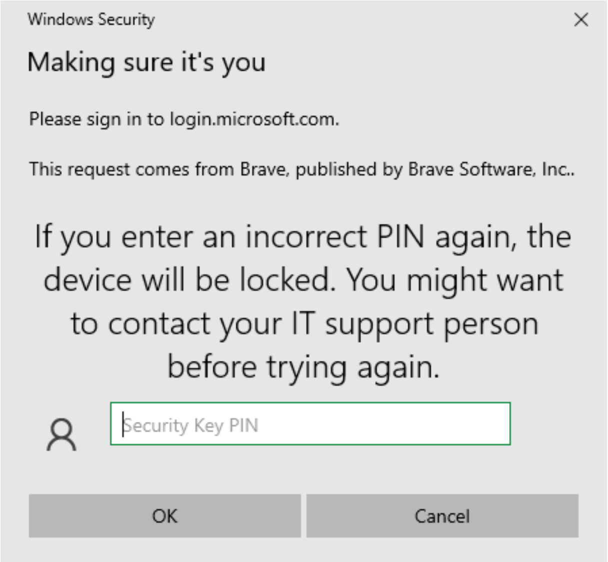
This request comes from Brave, published by Brave Software, Inc..

Too many incorrect PIN attempts.
Please enter A1B2C3.

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.

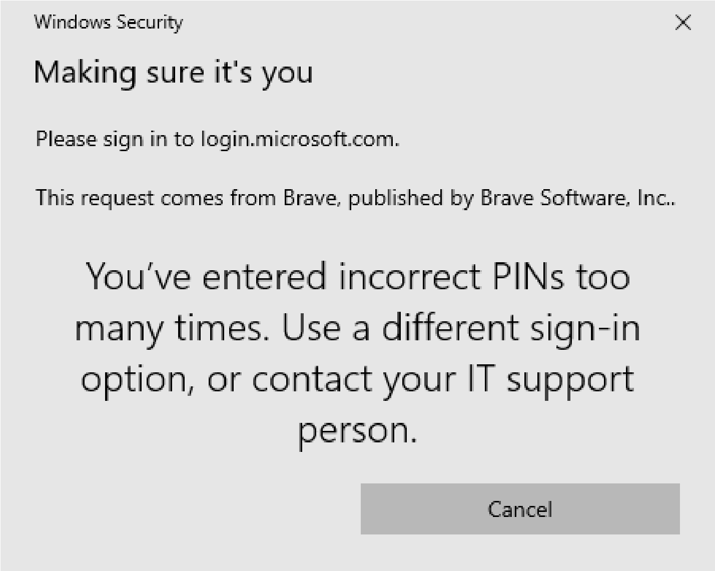
This request comes from Brave, published by Brave Software, Inc..

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

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

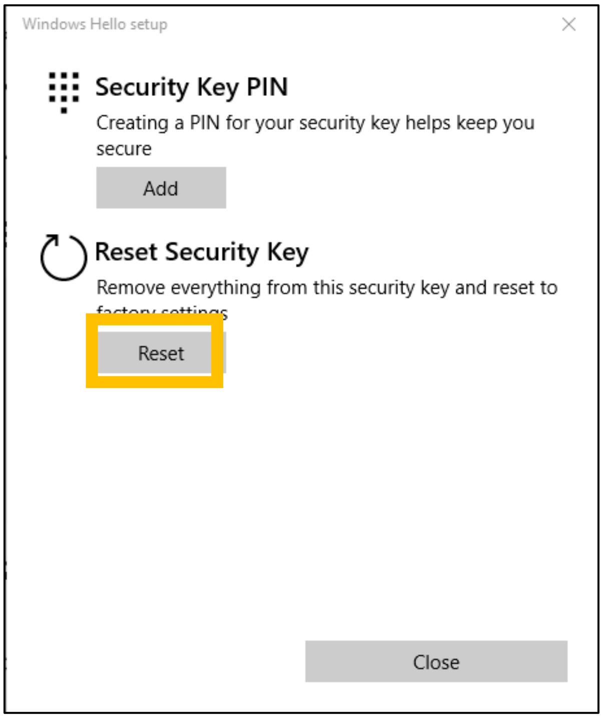
Please sign in to login.microsoft.com.

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.

5. Security Key Factory Reset

From Settings → Sign-in Options → Security key



Windows Hello setup

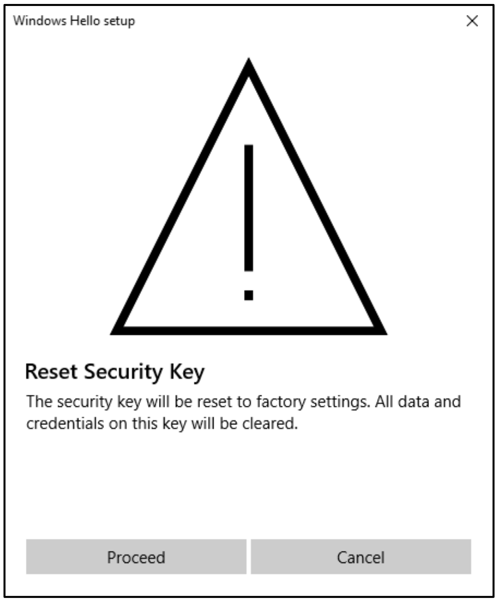
Security Key PIN

Creating a PIN for your security key helps keep you secure

Reset Security Key

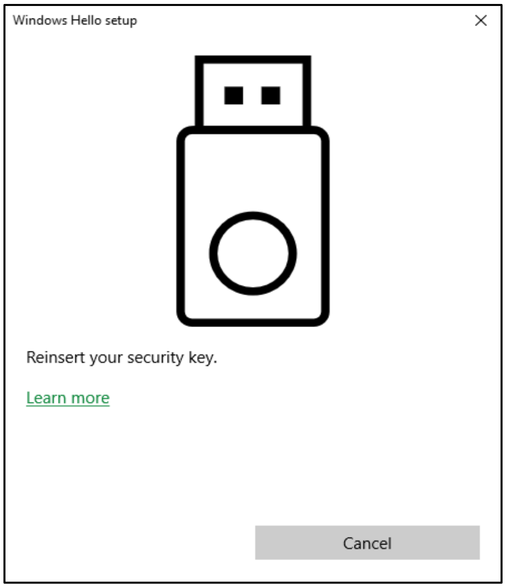
Remove everything from this security key and reset to factory settings

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



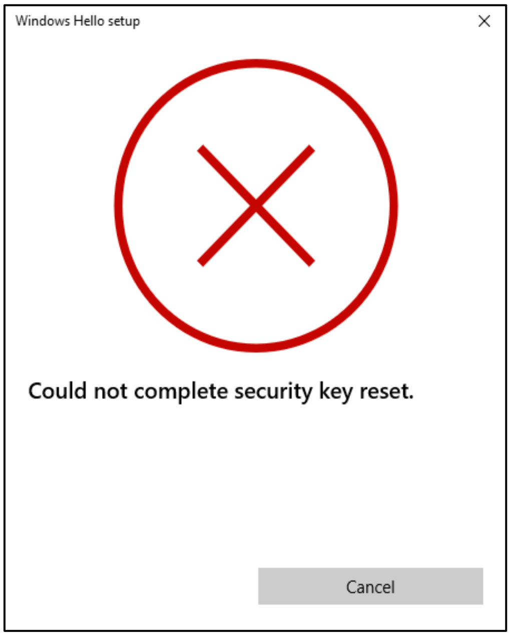
Reset Security Key

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



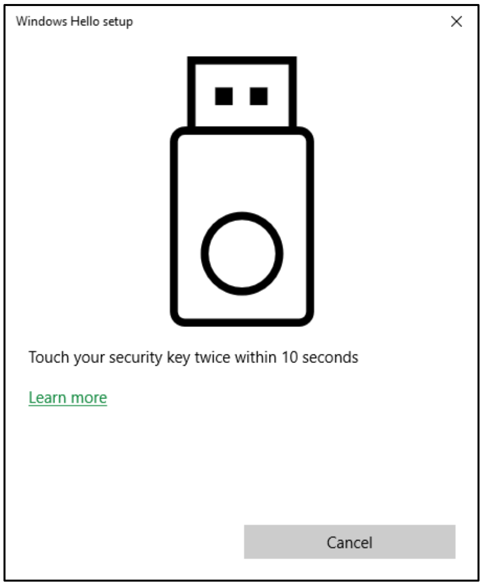
Reinsert your security key.

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

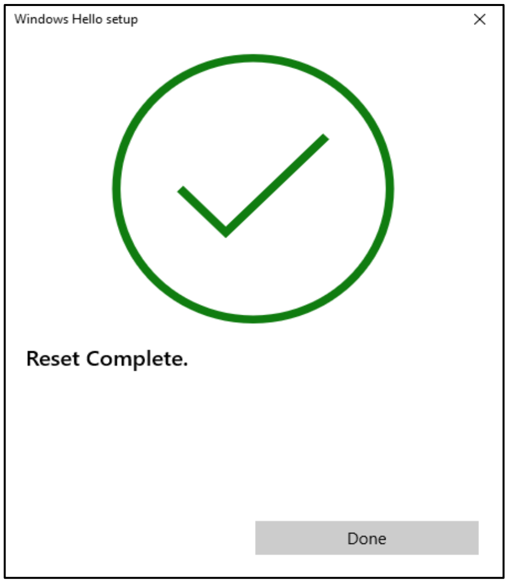


Could not complete security key reset.

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



Touch your security key twice within 10 seconds



Reset Complete.

Note:

- **The security key LED is OFF all the time; the key is locked and cannot be used.**
- **The security key will be of service after a factory reset.**

4. Set the Security Key using KeyManager at Windows

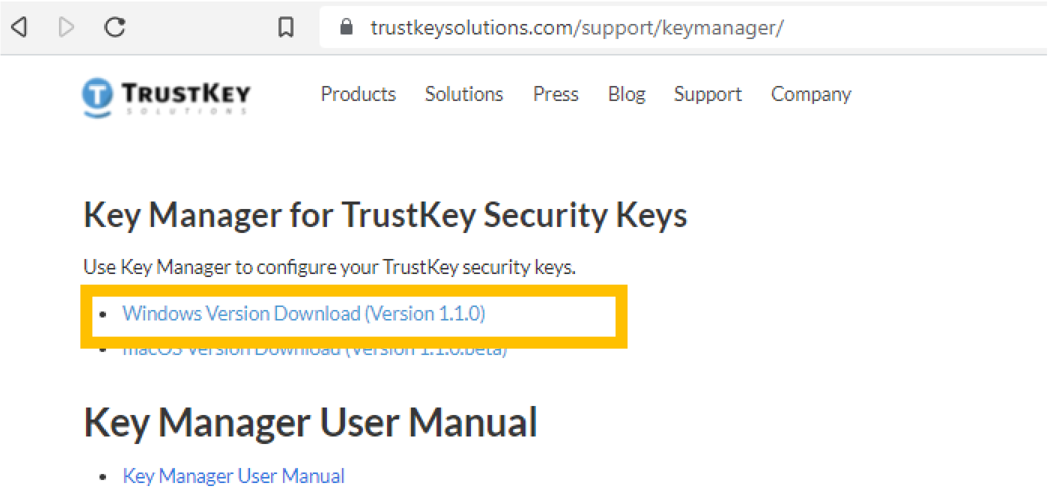
1. KeyManager

TrustKey's KeyManager is a program to manage PIN for security key as well as registering/managing OTP features of the security key.

Make sure that KeyManager™ application is downloaded on your PC/Mac.

https://www.trustkeysolutions.com/support/keymanager/

Please download the correct version for your OS. For Windows, you can download the file (version 1.1.0)



Key Manager for TrustKey Security Keys

Use Key Manager to configure your TrustKey security keys.

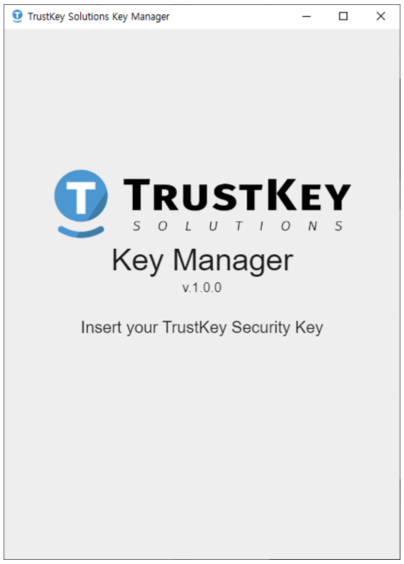
- Windows Version Download (Version 1.1.0)
- macOS Version Download (Version 1.1.0.beta)

Key Manager User Manual

- Key Manager User Manual

You can also download KeyManger User Manual for managing the security key with the program. The following description is the same as that of the User Manual.

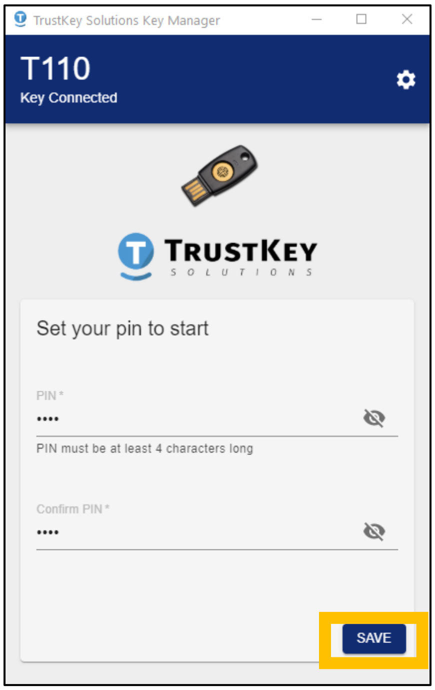
Launch the Key Manager™ application. If you see the following screen, plug your TRUSTKEY's security key into the USB port on your PC/Mac.



Insert your TrustKey Security Key

2. Setting up New PIN

1. Lauch KeyManager program
2. Insert T110/T120 into a USB port and enter the PIN and confirm the PIN
   - PIN must be at least four (4) characters long
   - PIN can be digits, characters, and mixture of them
3. Click SAVE



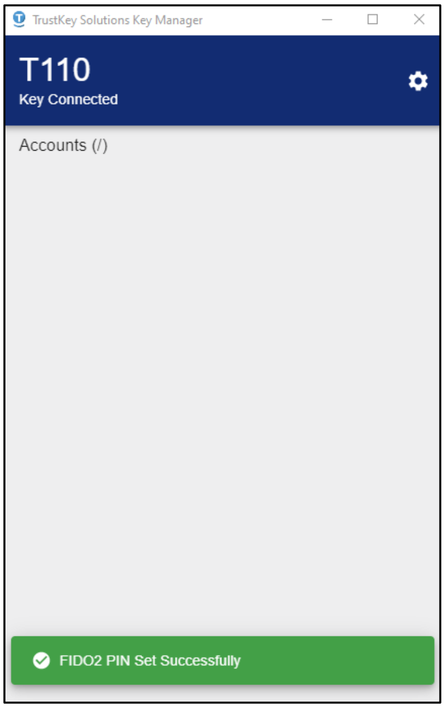
Set your pin to start

PIN * ••••

PIN must be at least 4 characters long

Confirm PIN * ••••

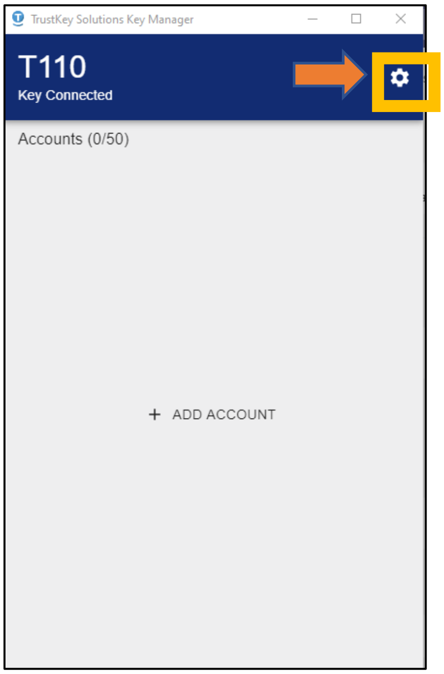
4. PIN setup done!



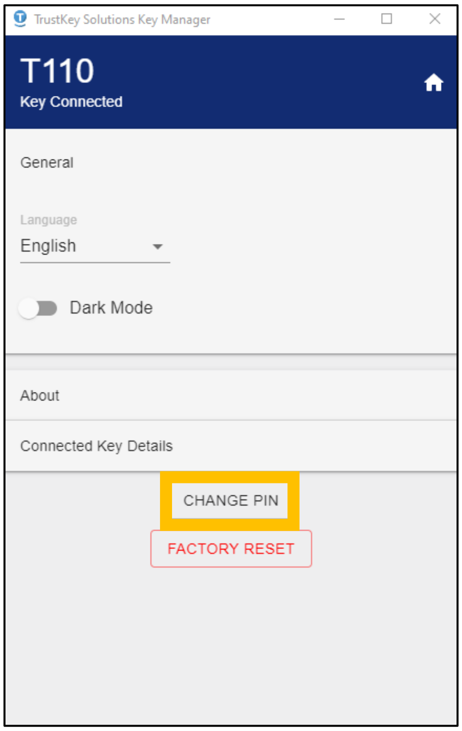
FIDO2 PIN Set Successfully

3. How to Change PIN

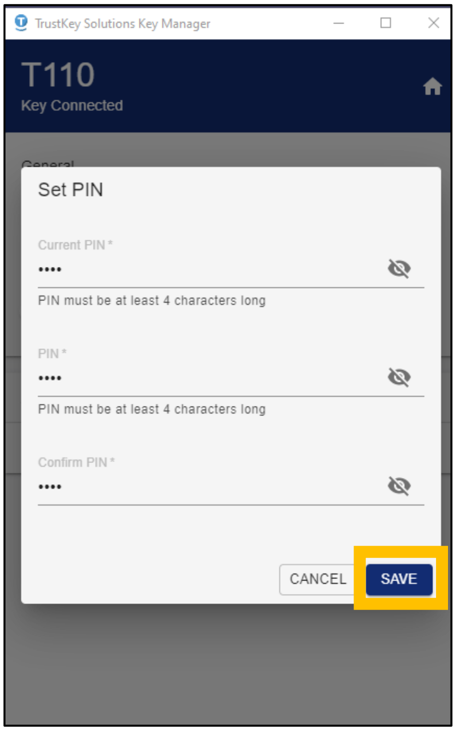
1. Click setup button



2. Click CHANGE PIN



3. Enter the Current PIN, PIN (new PIN) and Confirm PIN. Click SAVE



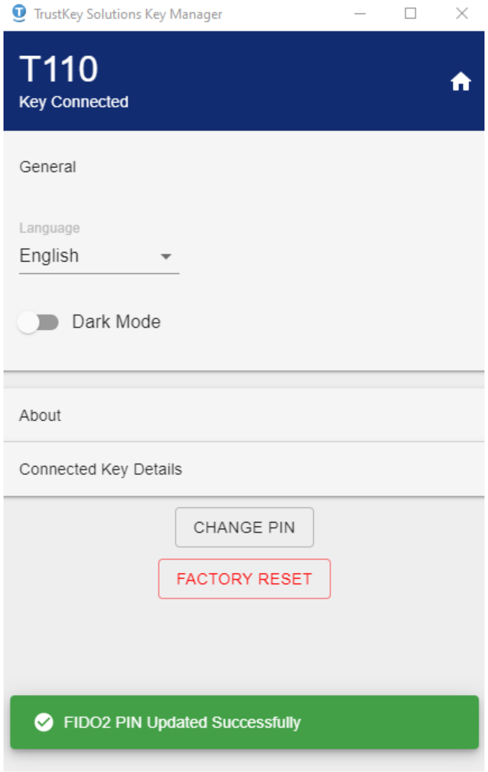
Set PIN

Current PIN *
••••
PIN must be at least 4 characters long

PIN *
••••
PIN must be at least 4 characters long

Confirm PIN *
••••

4. You have updated PIN for the security key



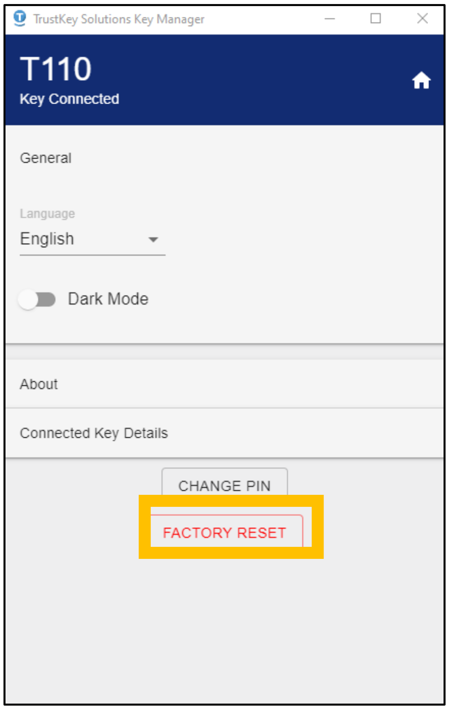
Language
English

Dark Mode

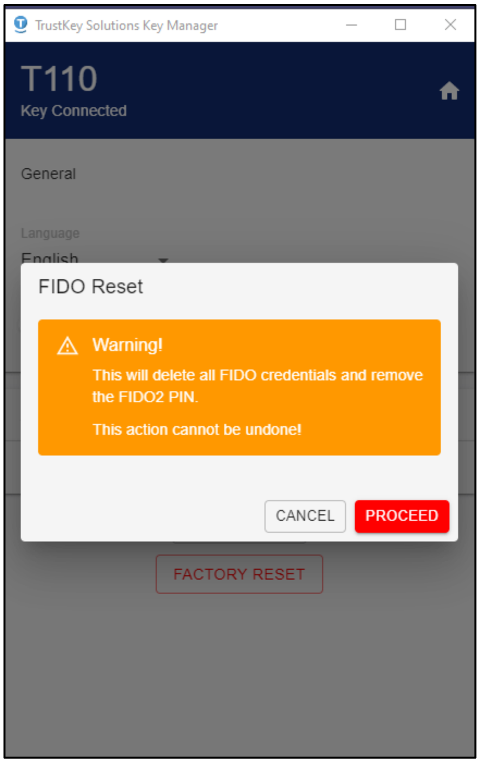
FIDO2 PIN Updated Successfully

4. How to Factory Reset a Key

1. Click FACTORY RESET. This will reset the PIN and other FIDO2 related credentials. Note that the factory reset will NOT erase TOTP/HOTP accounts. Please remove all OTP accounts before the factory reset.



2. Click PROCEED.

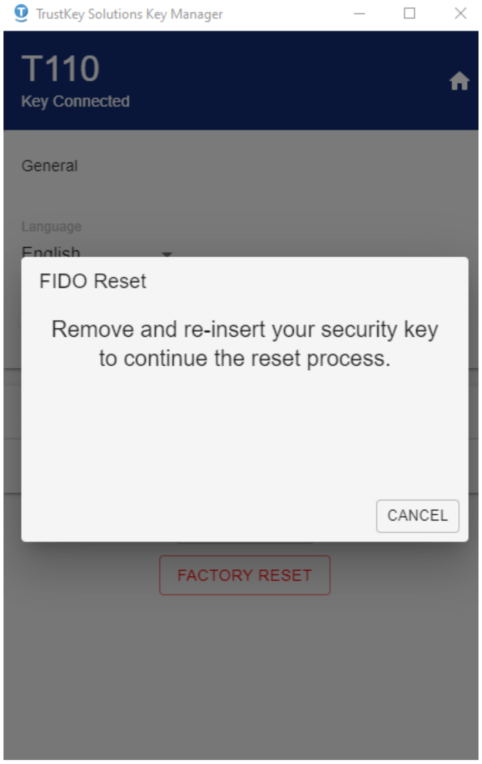


⚠ Warning!

This will delete all FIDO credentials and remove the FIDO2 PIN.

This action cannot be undone!

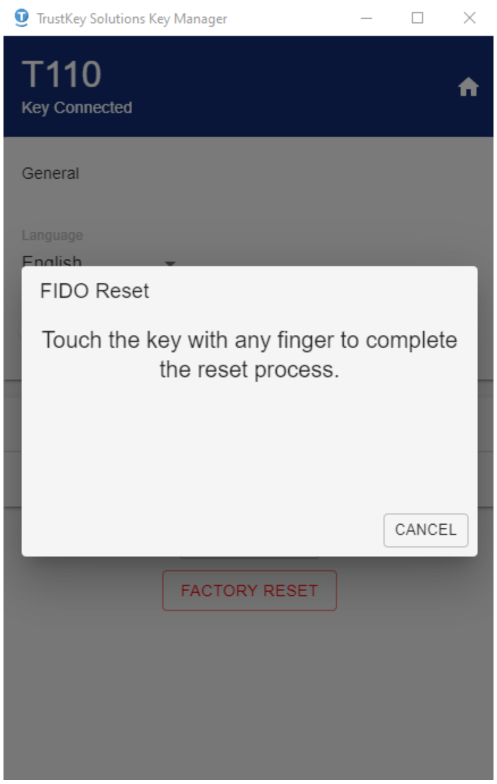
3. Remove your security key from the USB Port



FIDO Reset

Remove and re-insert your security key to continue the reset process.

4. Reinsert the security key and touch the sensor to complete the reset process. The user needs to touch the key within 10 seconds after the key reinsert. Otherwise, the whole factory reset process will be aborted and needs to start from the beginning.

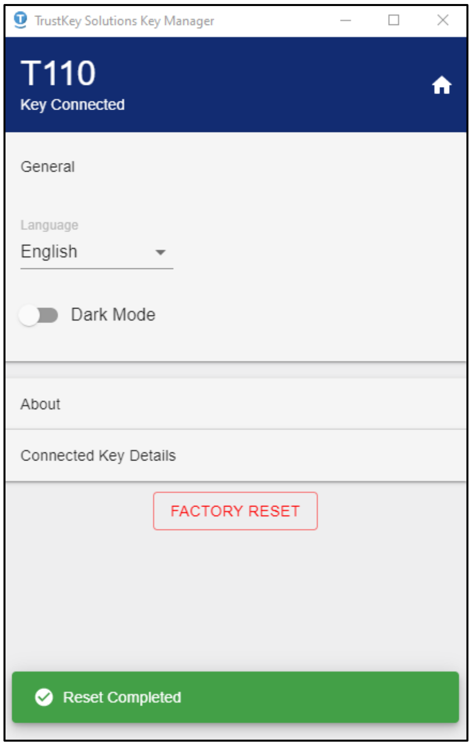


Language
English

FIDO Reset

Touch the key with any finger to complete the reset process.

5. You have reset the security key to factory settings



Language
English

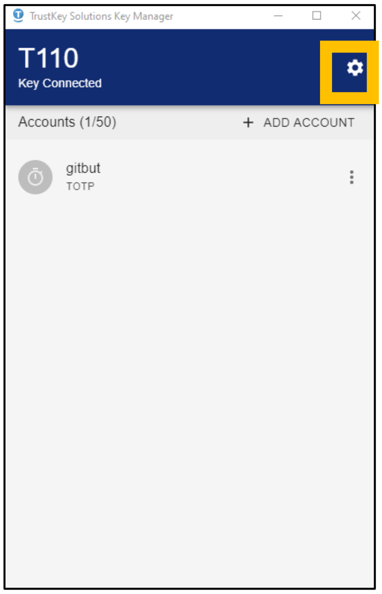
Dark Mode

Reset Completed

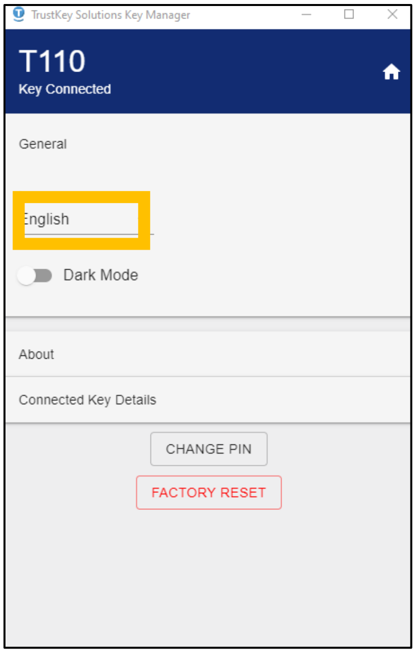
5. Other KeyManager Features

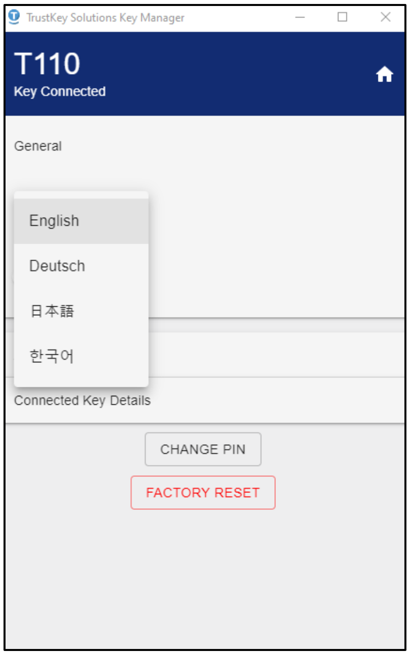
1. Language selection

   Select ⚙

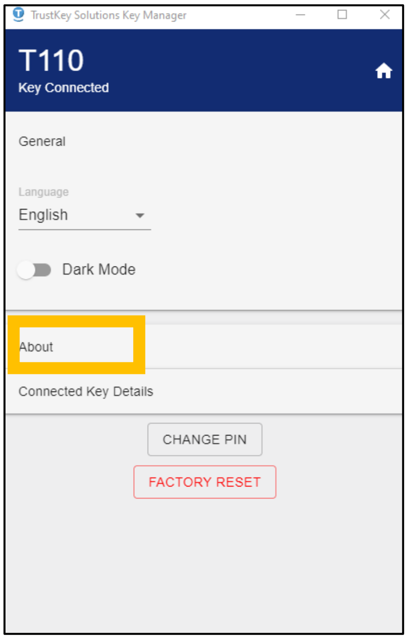


Click Language to choose a different language other than the default language. Currently, the KeyManager supports four languages (English/Korean/Japanese/German).



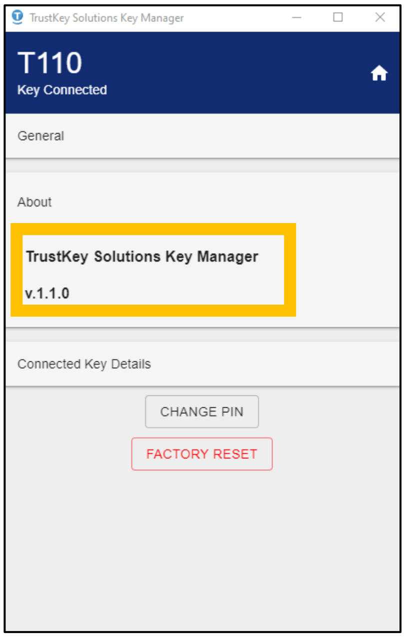


2. KeyManager version check
   Click “About”



Language
English

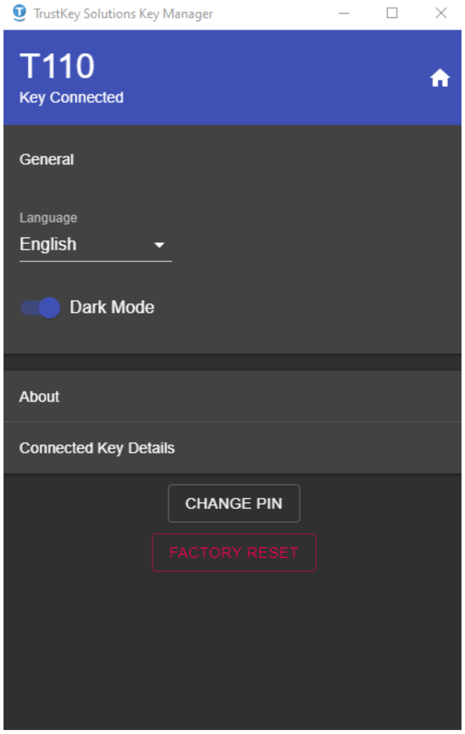
Dark Mode



TrustKey Solutions Key Manager

v.1.1.0

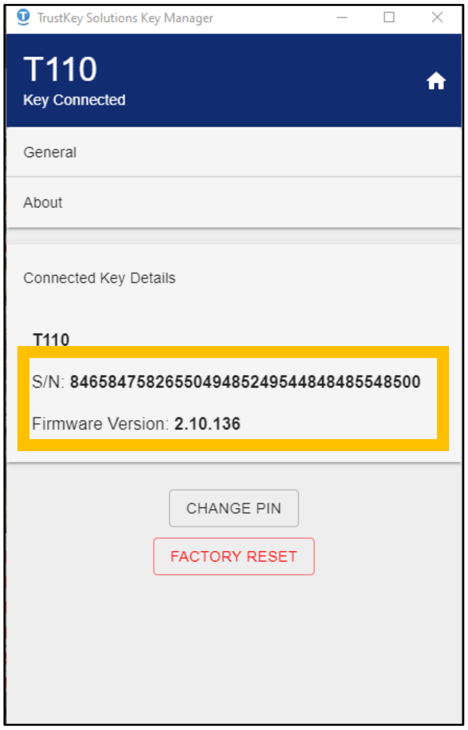
3. Dark mode



Language
English

Dark Mode

4. The connected (inserted) Key information
   This section describes the key serial number and firmware version.



T110

Key Connected

Connected Key Details

T110

S/N: **84658475826550494852495448484855548500**

Firmware Version: **2.10.136**

~~5. TrustKey Security Key OTP Account Management~~

(We are currently developing a patch for the Key Manager Program in 2023.)

TrustKey FIDO security key (both G-series and T-series keys) can store OTP accounts. You can keep 50 OTP accounts – a max of one (1) HOPT account or a maximum of 50 TOTP accounts or a combination of HOTP and TOTP accounts adding up to 50 accounts.

1. What is OTP?

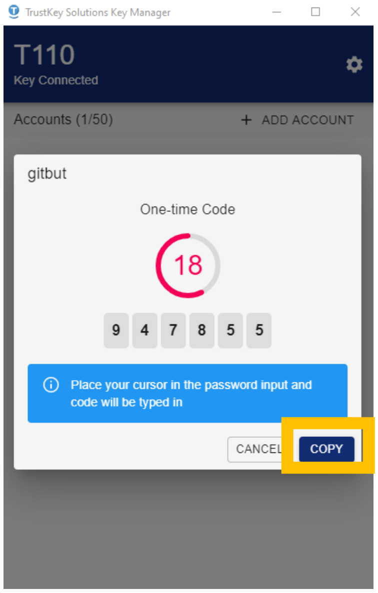
OTP is abbreviated form of One Time Password (or One Time Passcode). A one-time password (OTP), also known as a one-time PIN, one-time authorization code (OTAC) or dynamic password, is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid several shortcomings that are associated with traditional (static) password-based authentication; a number of implementations also incorporate two-factor authentication by ensuring that the one-time password requires access to something a person has (such as a small keyring fob device with the OTP calculator built into it, or a smartcard or specific cellphone) as well as something a person knows (such as a PIN).

TOTP (Time-Based One-Time Passcode)

The TOTP method enables you to authenticate using the time-based one-time passcode. TOTP is generated on many hardware devices, including our T110/T120 and G310/G320 security keys and the Github Authenticator app, Google Authenticator app, and Microsoft Authenticator app. TOTP implementation was done based on RFC7238.

The TOTP is valid for a short duration. The default value for the period is 30 seconds.

The KeyManager will generate TOTP output with the security key inserted. The output can be copy-and-paste using clicking the “COPY” button.

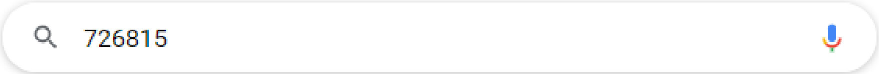


Place your cursor in the password input and code will be typed in

HOTP (HMAC based One Time Passcode)

HOTP is a counter-based one-time password. This method enables you to authenticate using the counter-based one-time passcode generated on the security keys. The counter on the token must be in sync with the server. HOTP implementation was done based on RFC 4226.

You do not need to run KeyManager to get HOTP output. Just place the cursor at any text field and push the button of the security key.

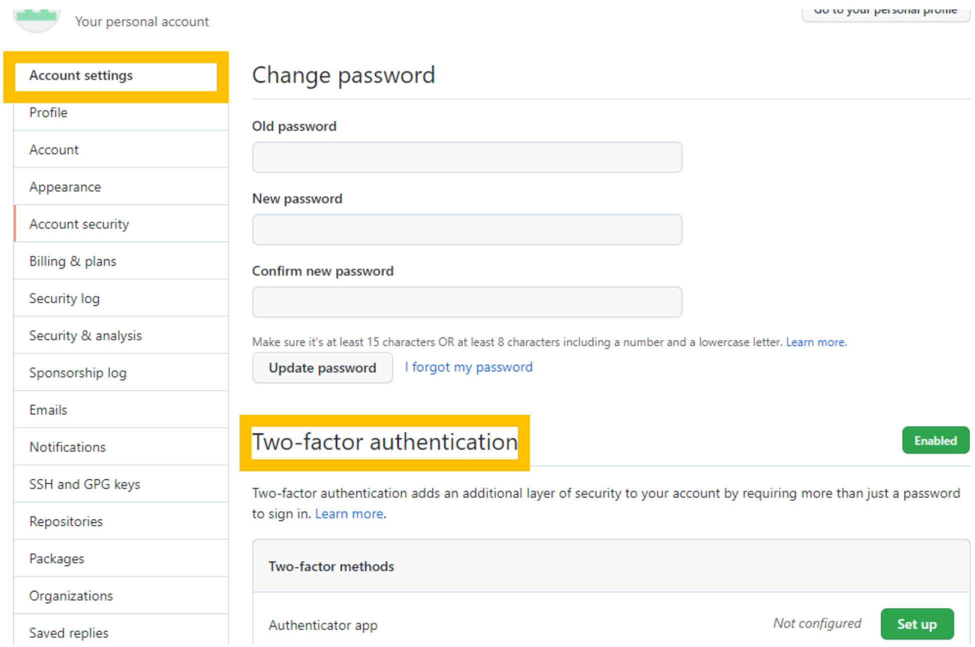


726815

You can enroll the TOTP and HOTP authenticator using the KeyManager program.

2. Setting up TOTP accounts using QR scan (Github example)

1. A Github account setup example is given here.
   From the Github account, look for “Account setting” and “Two-factor authentication.”



Change password

Old password

New password

Confirm new password

Make sure it's at least 15 characters OR at least 8 characters including a number and a lowercase letter. Learn more.

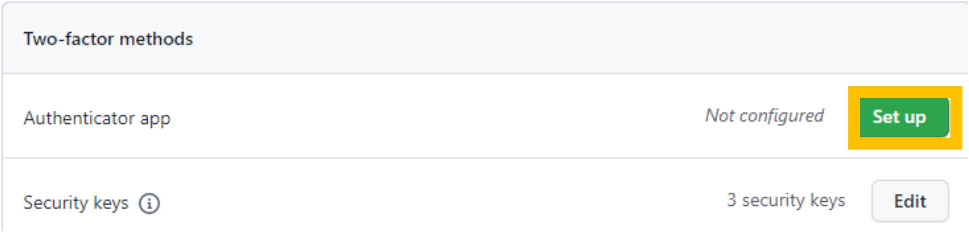
Two-factor authentication

Two-factor authentication adds an additional layer of security to your account by requiring more than just a password to sign in. Learn more.

Two-factor methods

Authenticator app *Not configured*

2. Click “Set up”

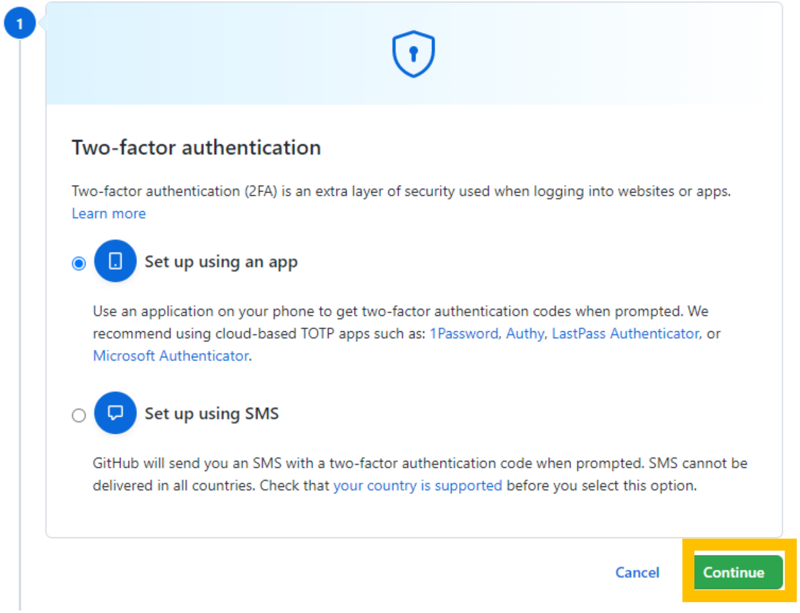


Two-factor methods

Authenticator app — *Not configured* — Set up

Security keys ⓘ — 3 security keys — Edit

3. Click Continue



1

Two-factor authentication

Two-factor authentication (2FA) is an extra layer of security used when logging into websites or apps. Learn more

● Set up using an app

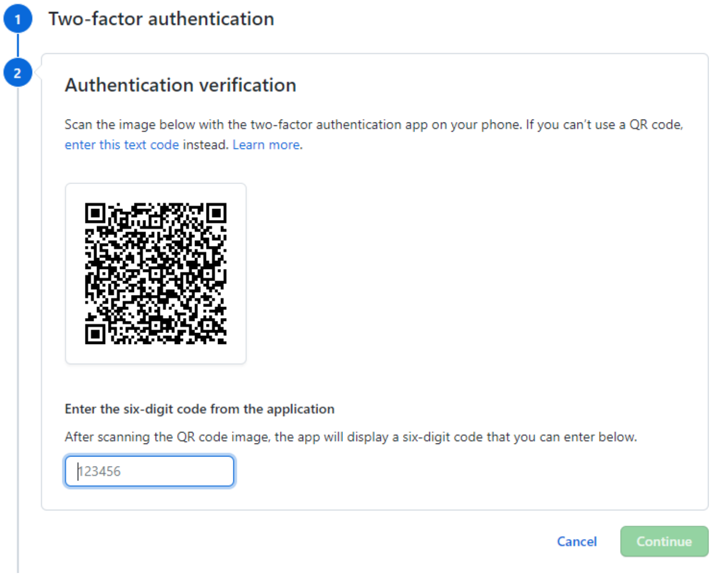
Use an application on your phone to get two-factor authentication codes when prompted. We recommend using cloud-based TOTP apps such as: 1Password, Authy, LastPass Authenticator, or Microsoft Authenticator.

○ Set up using SMS

GitHub will send you an SMS with a two-factor authentication code when prompted. SMS cannot be delivered in all countries. Check that your country is supported before you select this option.

Cancel Continue

4. Then, a QR code is shown as the figure be as below:



1 Two-factor authentication

2 Authentication verification

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

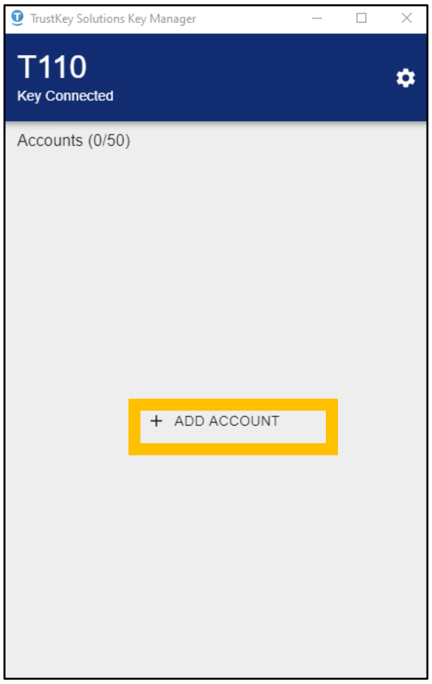
Enter the six-digit code from the application

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

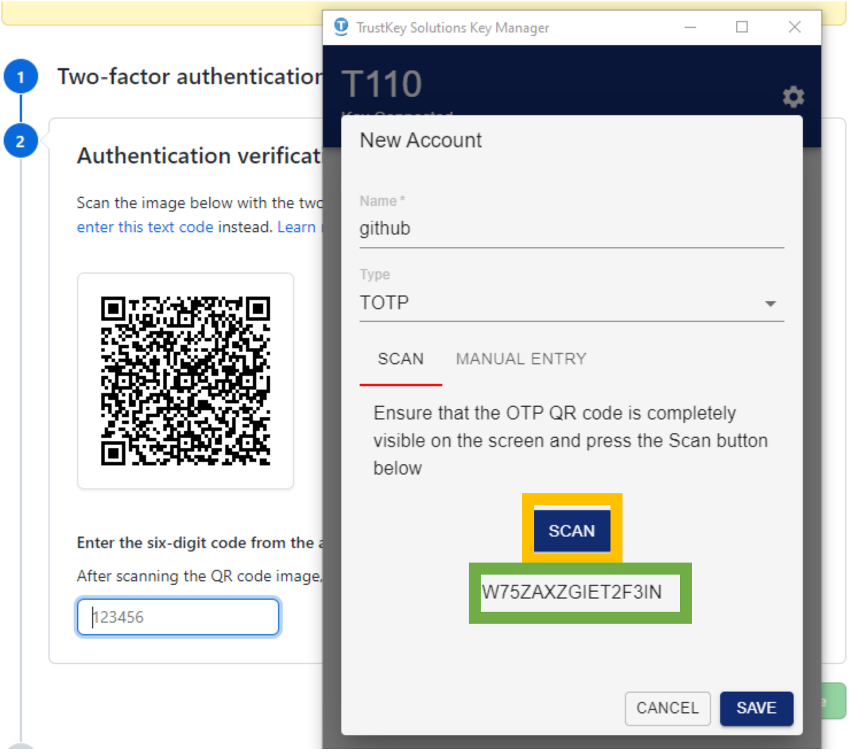
123456

Cancel Continue

5. Open KeyManager and click ADD ACCOUNT



6. If you have a QR code given by the server, open the code and press SCAN.



Scan the image below with the two
enter this text code instead. Learn

Enter the six-digit code from the a

After scanning the QR code image,

123456

New Account

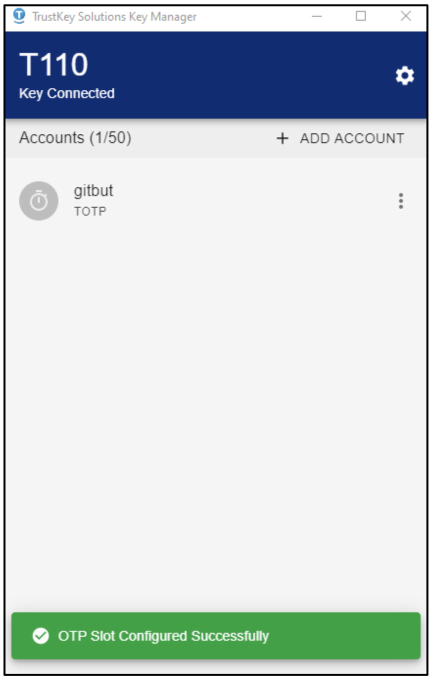
Name *
github

Type
TOTP

Ensure that the OTP QR code is completely visible on the screen and press the Scan button below

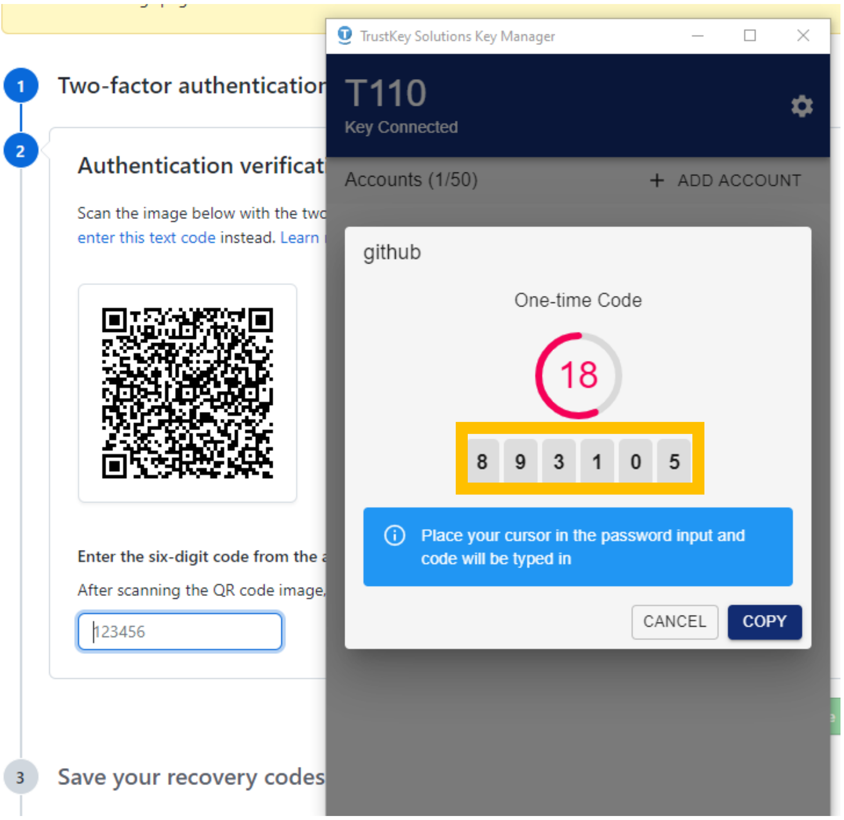
W75ZAXZGIET2F3IN

7. You have saved a TOTP account



OTP Slot Configured Successfully

8. ~~Github~~ Verify the TOTP sequence based on the code given by the QR code



Scan the image below with the two
enter this text code instead. Learn

Enter the six-digit code from the a

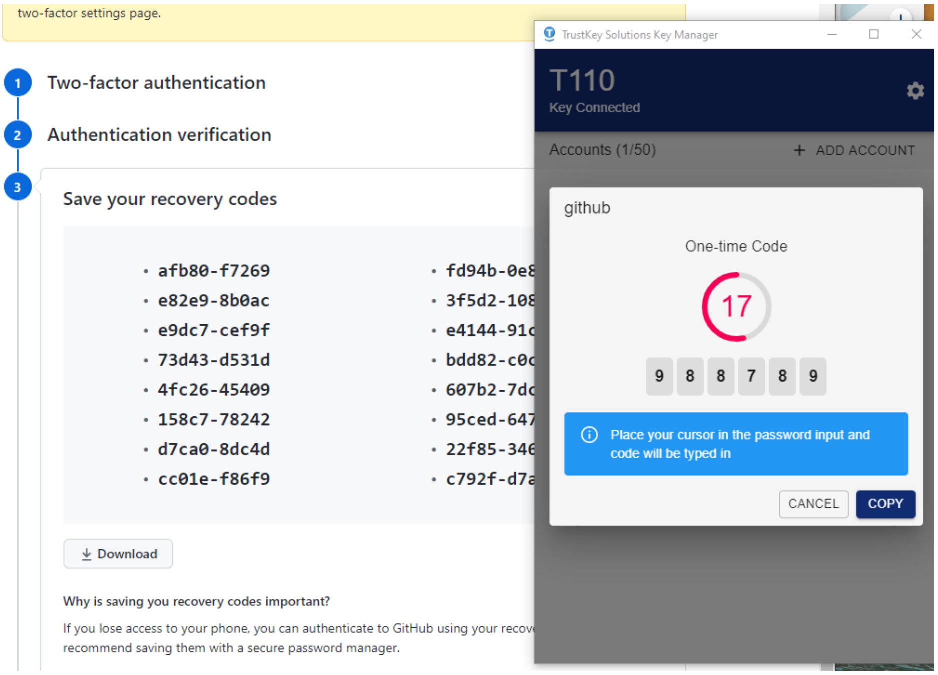
After scanning the QR code image,

123456

8 9 3 1 0 5

Place your cursor in the password input and code will be typed in

9. Github server verified the TOTP sequence and processed the next phase



two-factor settings page.

1 Two-factor authentication

2 Authentication verification

3 Save your recovery codes

- afb80-f7269
- e82e9-8b0ac
- e9dc7-cef9f
- 73d43-d531d
- 4fc26-45409
- 158c7-78242
- d7ca0-8dc4d
- cc01e-f86f9
- fd94b-0e8
- 3f5d2-108
- e4144-91c
- bdd82-c0c
- 607b2-7dc
- 95ced-647
- 22f85-346
- c792f-d7a

Download

Why is saving you recovery codes important?

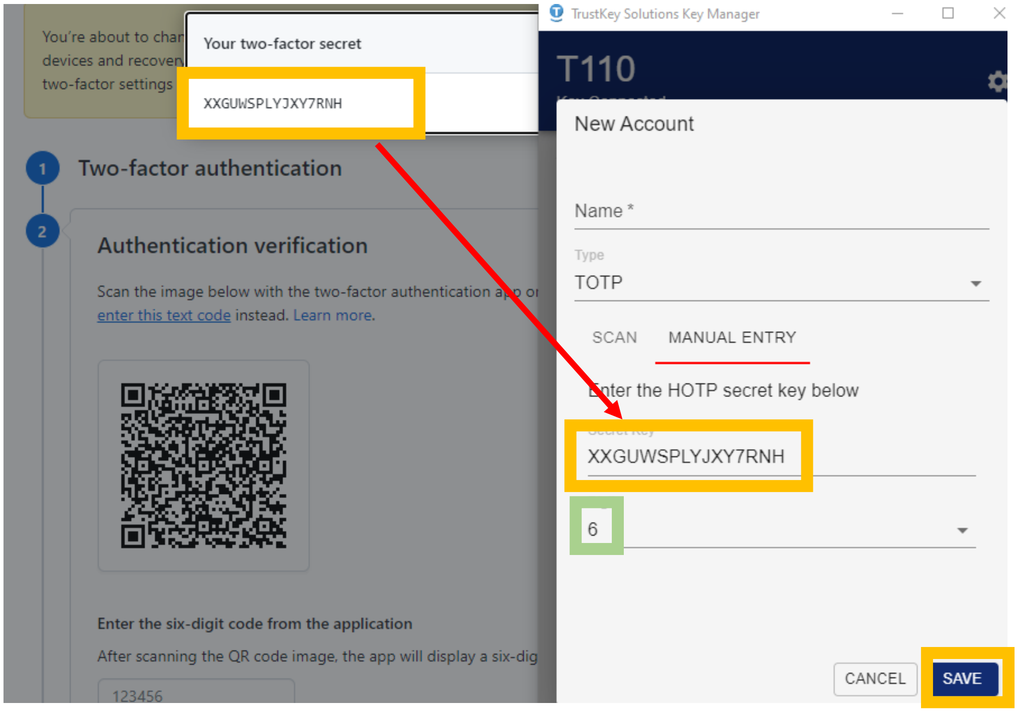
If you lose access to your phone, you can authenticate to GitHub using your recov
recommend saving them with a secure password manager.

9 8 8 7 8 9

Place your cursor in the password input and code will be typed in

3. Setting up TOTP accounts using Manual Entry (Github example)

Instead of using the SCAN button, you can enter Secret Key manually. The green box ("Digit") is the number of digits for TOTP output. Note that the Manual Entry digits should be in a Base32 format.



You're about to char
devices and recovery
two-factor settings

Your two-factor secret

XXGUWSPLYJXY7RNH

1 Two-factor authentication

2 Authentication verification

Scan the image below with the two-factor authentication app or enter this text code instead. Learn more.

Enter the six-digit code from the application

After scanning the QR code image, the app will display a six-dig

123456

Name *

Type: TOTP

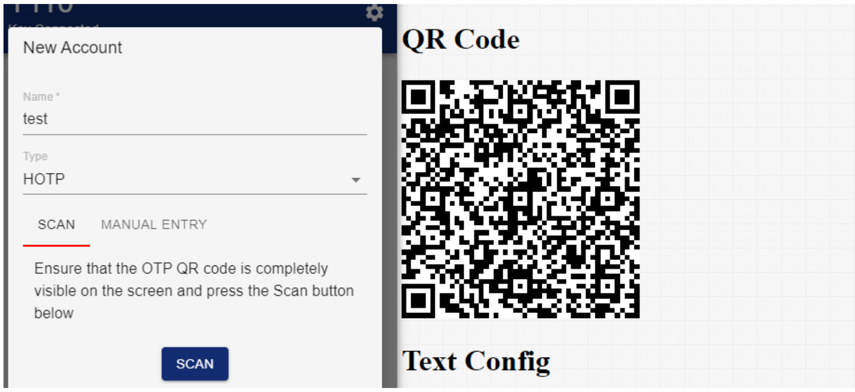
Enter the HOTP secret key below

Secret Key: XXGUWSPLYJXY7RNH

6

4. Setting up HOTP account using KeyManager

You can set up an HOTP account by QR scan as below:



New Account

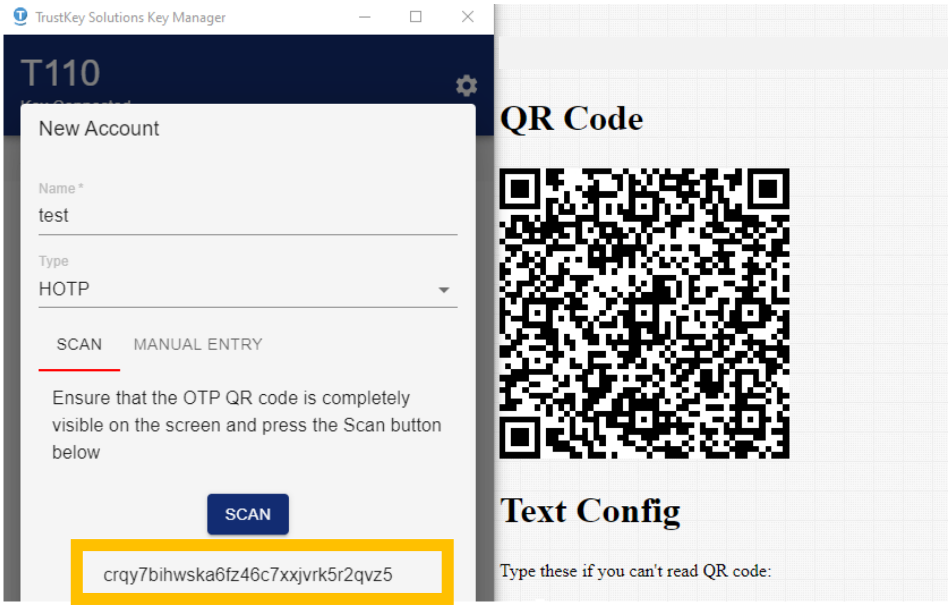
Name * test

Type HOTP

Ensure that the OTP QR code is completely visible on the screen and press the Scan button below

QR Code

Text Config



T110

New Account

Name * test

Type HOTP

Ensure that the OTP QR code is completely visible on the screen and press the Scan button below

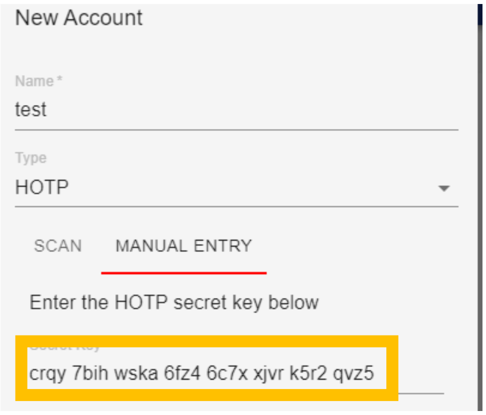
crqy7bihwska6fz46c7xxjvrk5r2qvz5

QR Code

Text Config

Type these if you can't read QR code:

Or, as a TOTP case, you can set up the HOTP account by manual entry. Note that the manual entry data should be in a Base32 format.



New Account

Name * test

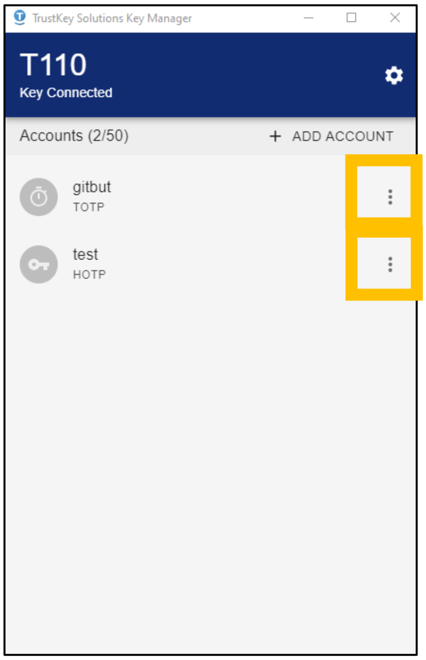
Type HOTP

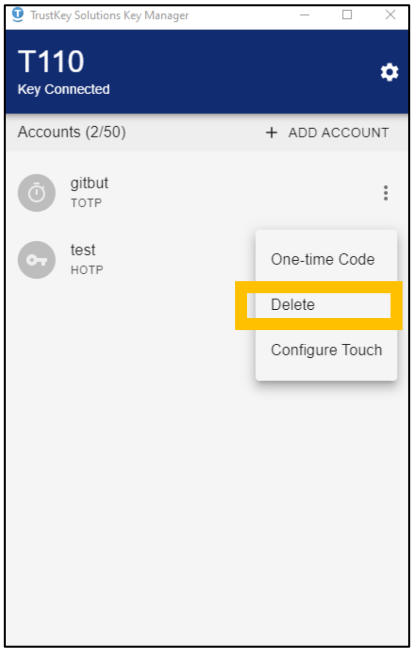
Enter the HOTP secret key below

crqy 7bih wska 6fz4 6c7x xjvr k5r2 qvz5

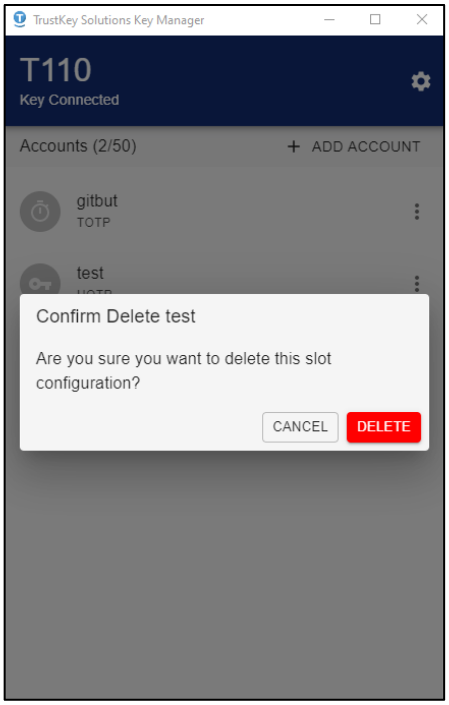
5. How to delete TOTP/HOTP slot

1. Click on the vertical 3-dots and select Delete



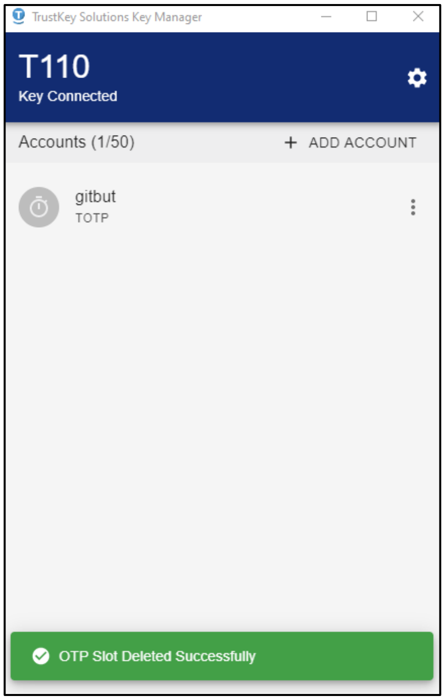


2. Click Delete and done!



Confirm Delete test

Are you sure you want to delete this slot configuration?



OTP Slot Deleted Successfully

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.

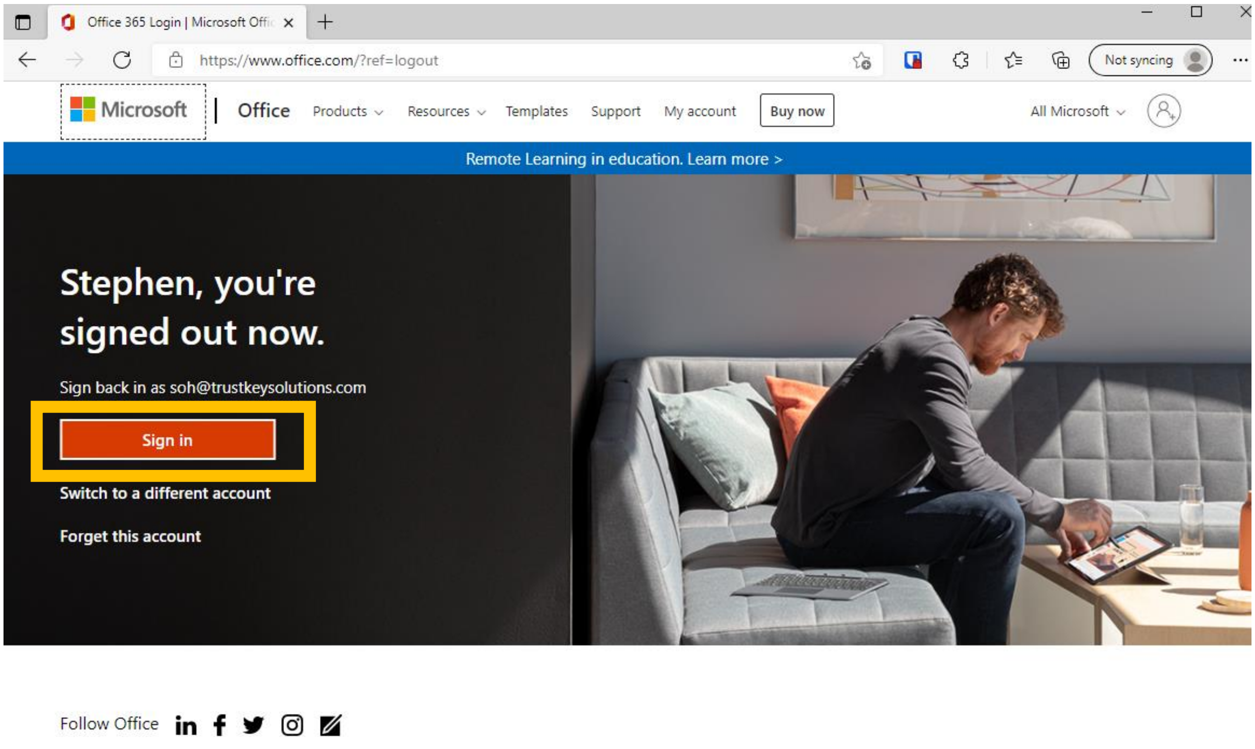
The steps shown below are the case that a user uses www.office.com for the security key registration. The user can use one of the following sites for registration.

Registration sites:

https://www.office.com

https://login.microsoftonline.com

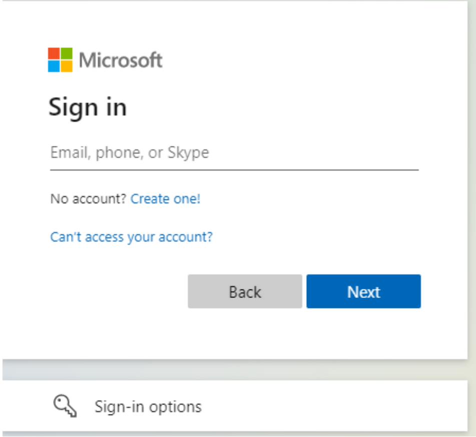
Step 1: The user needs to sign in at www.office.com using the user's ID and the password.



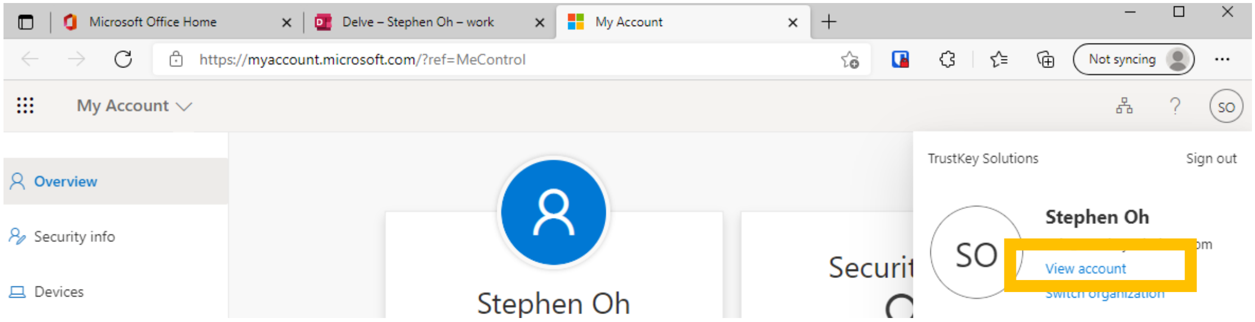
Stephen, you're signed out now.

Sign back in as soh@trustkeysolutions.com

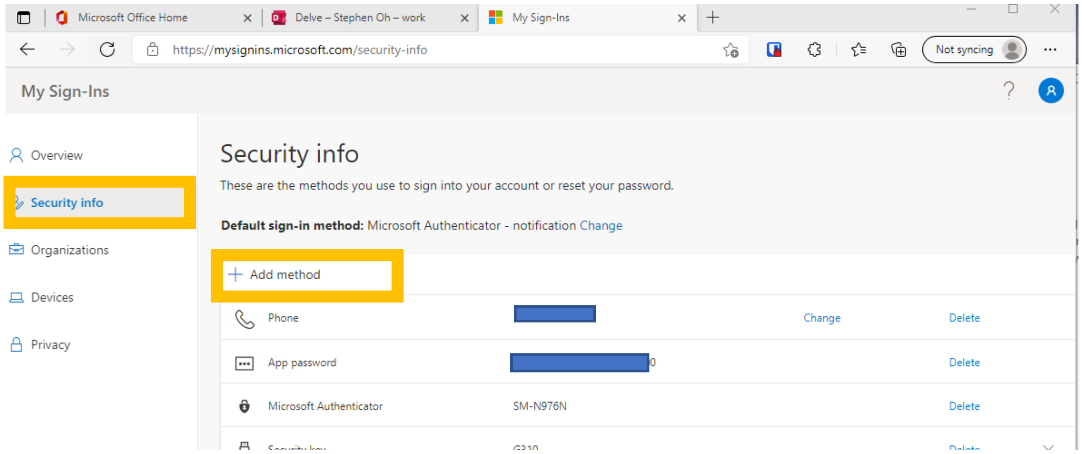
Office 365 Login | Microsoft Offic
https://www.office.com/?ref=logout
Not syncing
Microsoft
Office
Products
Resources
Templates
Support
My account
Buy now
All Microsoft
Remote Learning in education. Learn more >
Sign in
Switch to a different account
Forget this account
Follow Office



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.

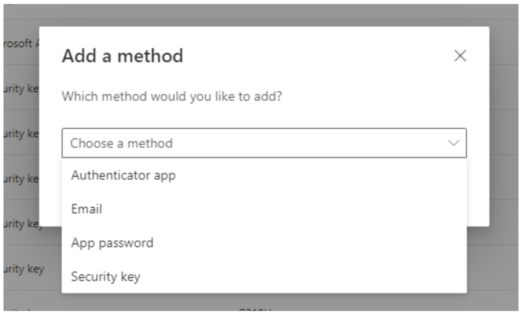
Default sign-in method: Microsoft Authenticator - notification Change

+ Add method

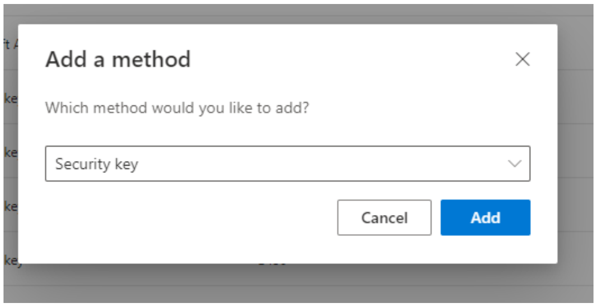
Phone	[redacted]	Change	Delete
App password	[redacted]		Delete
Microsoft Authenticator	SM-N976N		Delete
Security key	G310		Delete

Copyright ⓒ 2021 TrustKey Co., Ltd. All Rights Reserved

Step 4: follow the registration flow

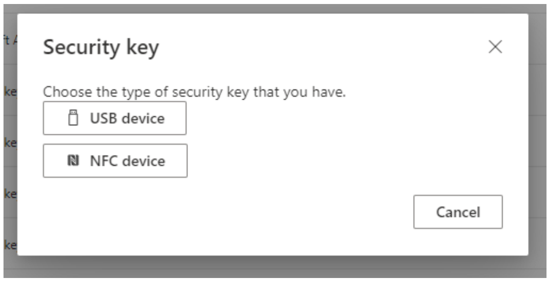

Add a method

Which method would you like to add?

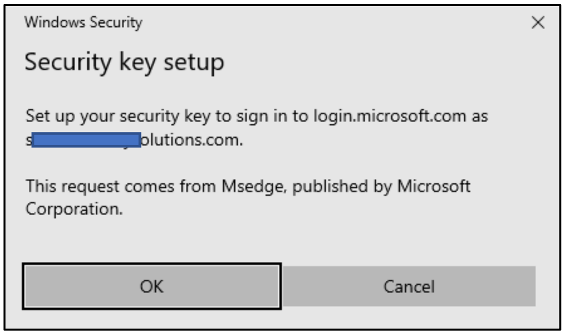

Add a method

Which method would you like to add?

Security key


Security key

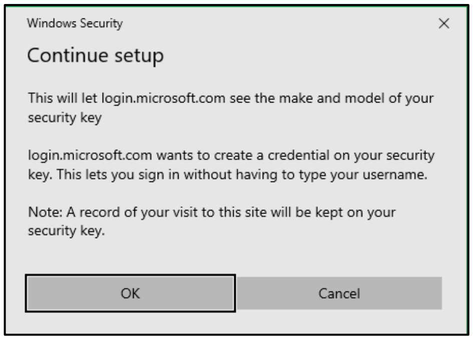
Choose the type of security key that you have.


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.

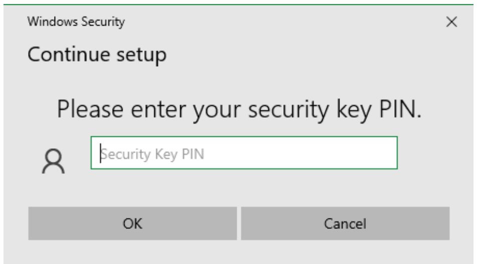

Windows Security

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.

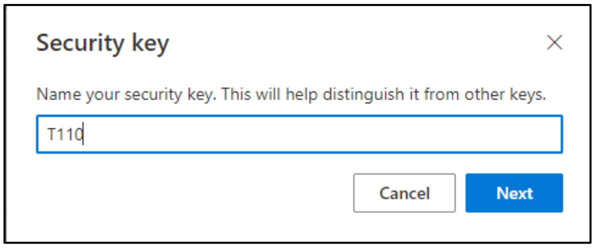
Note: A record of your visit to this site will be kept on your security key.


Windows Security

Continue setup

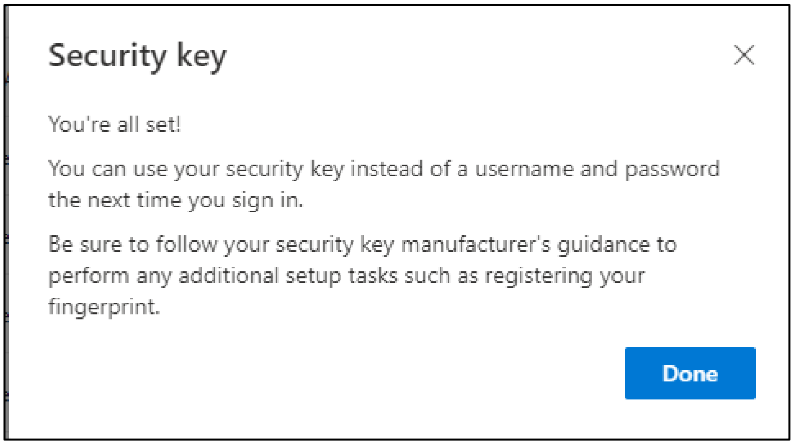
Please enter your security key PIN.

Step 5: the user needs to name the security key to differentiate 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.

T110



Security key

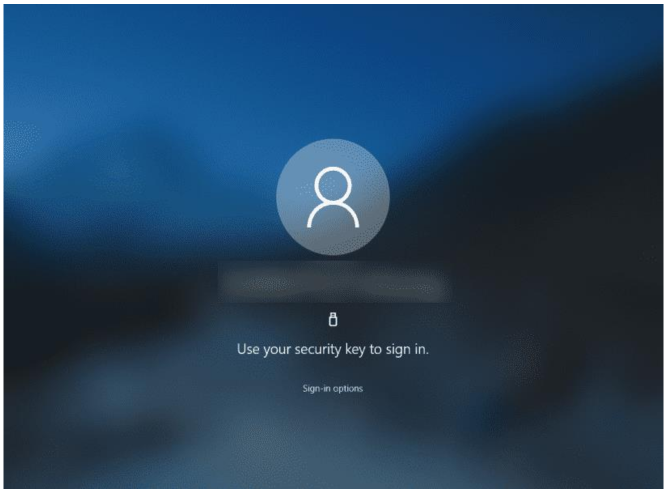
You're all set!

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.

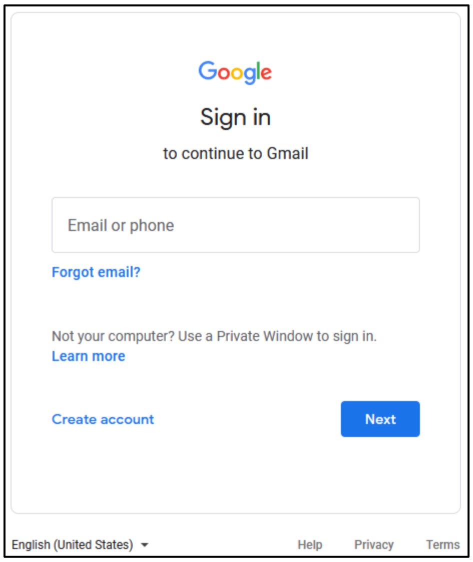
Note: Please refer to our blog here for more information.

(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.

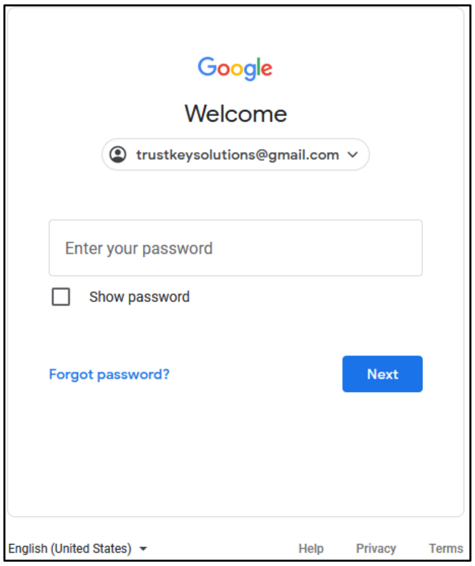
Step1: The user needs to sign in with the existing account ID and the password.



Sign in

to continue to Gmail

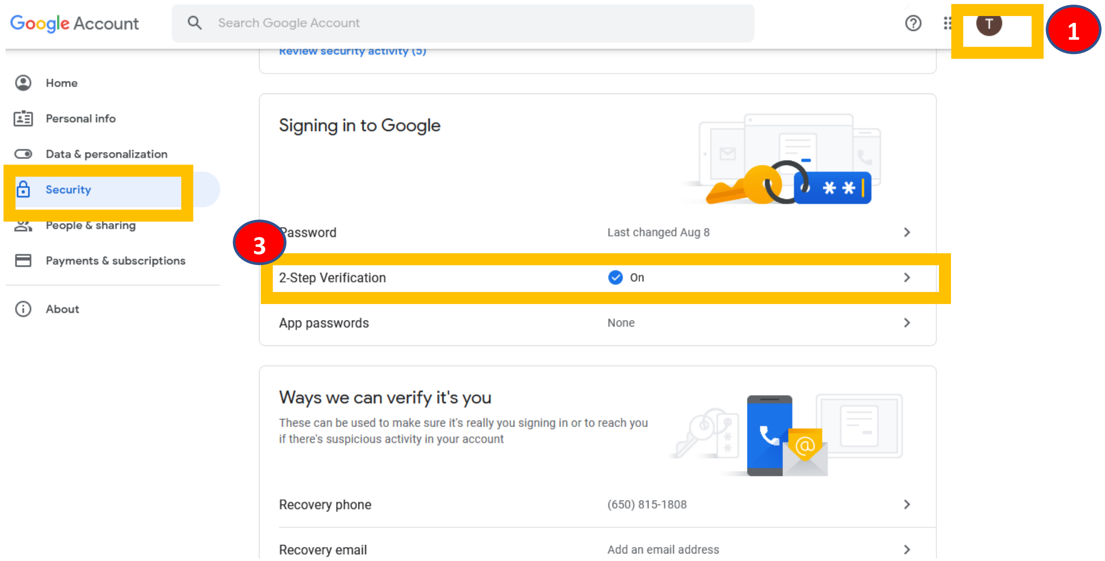
Not your computer? Use a Private Window to sign in. Learn more



Welcome

trustkeysolutions@gmail.com

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



Signing in to Google

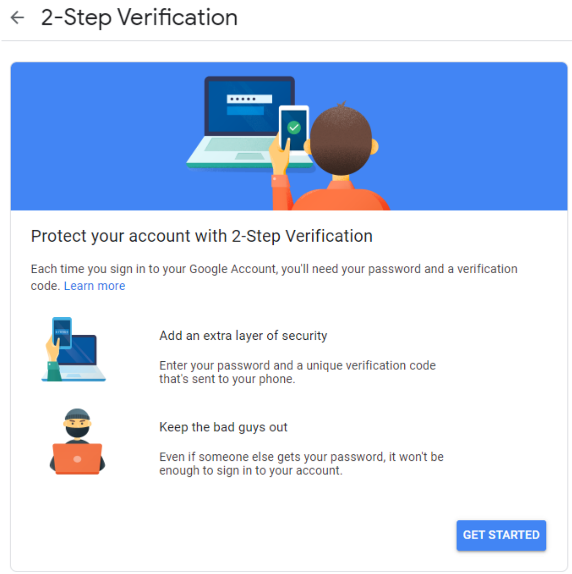
Password	Last changed Aug 8
2-Step Verification	On
App passwords	None

Ways we can verify it's you

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 perform the initial 2-Step verification with your phone



← 2-Step Verification

Protect your account with 2-Step Verification

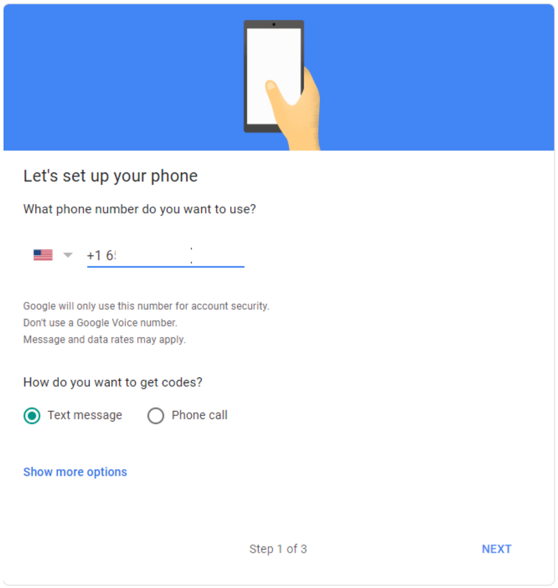
Each time you sign in to your Google Account, you'll need your password and a verification code. Learn more

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?

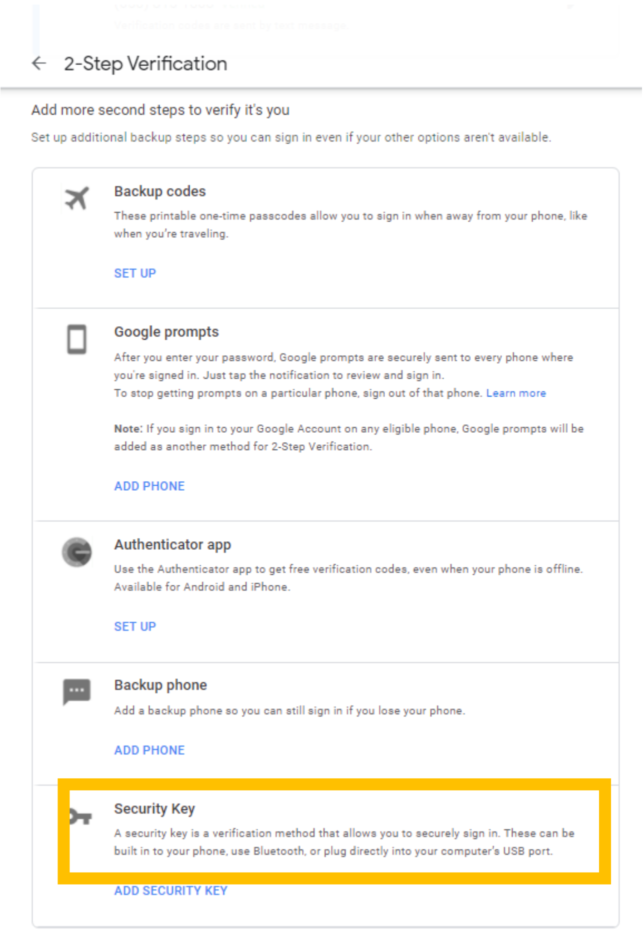
+1 6

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



Verification codes are sent by text message.

← 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.

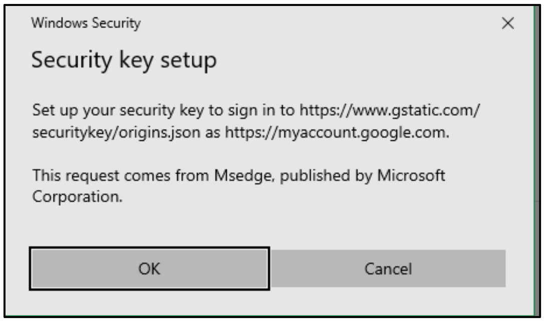
Backup phone

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.

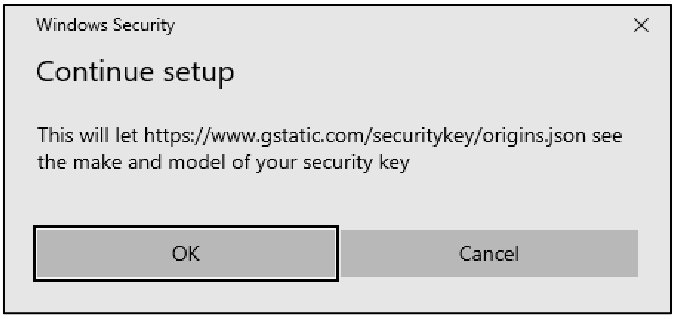
Step 5: follow the browser's instructions


Windows Security

Security key setup

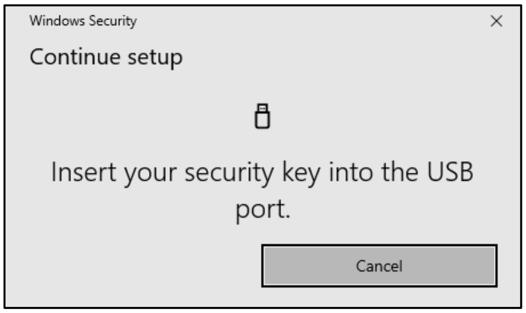
Set up your security key to sign in to https://www.gstatic.com/securitykey/origins.json as https://myaccount.google.com.

This request comes from Msedge, published by Microsoft Corporation.


Windows Security

Continue setup

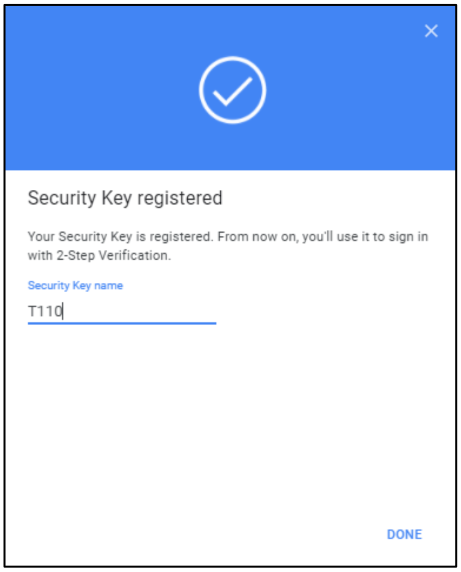
This will let https://www.gstatic.com/securitykey/origins.json see the make and model of your security key


Windows Security

Continue setup

Insert your security key into the USB port.

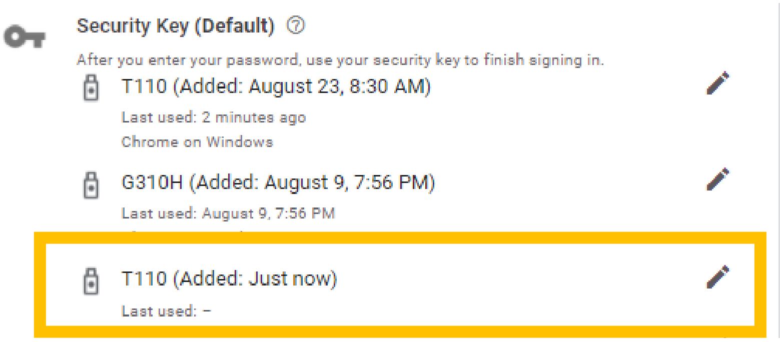
Step 6: After successful registration, the user needs to name the key


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

T110


Security Key (Default)

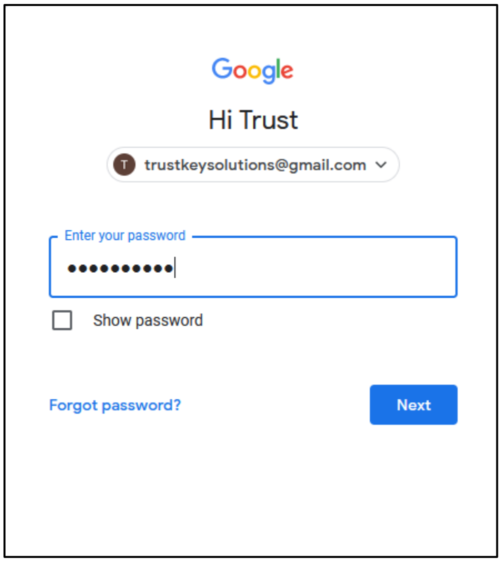
After you enter your password, use your security key to finish signing in.

T110 (Added: August 23, 8:30 AM)
Last used: 2 minutes ago
Chrome on Windows

G310H (Added: August 9, 7:56 PM)
Last used: August 9, 7:56 PM

T110 (Added: Just now)
Last used: –

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



Google

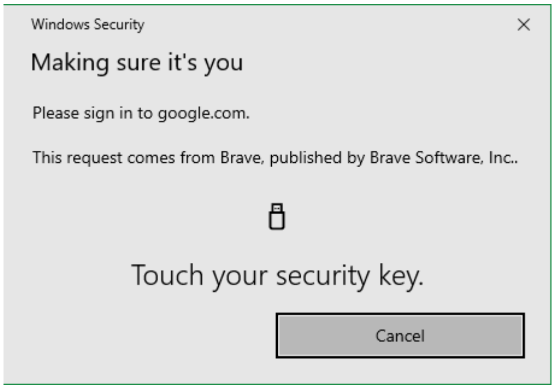
Hi Trust

trustkeysolutions@gmail.com

Enter your password

••••••••••

□ Show password



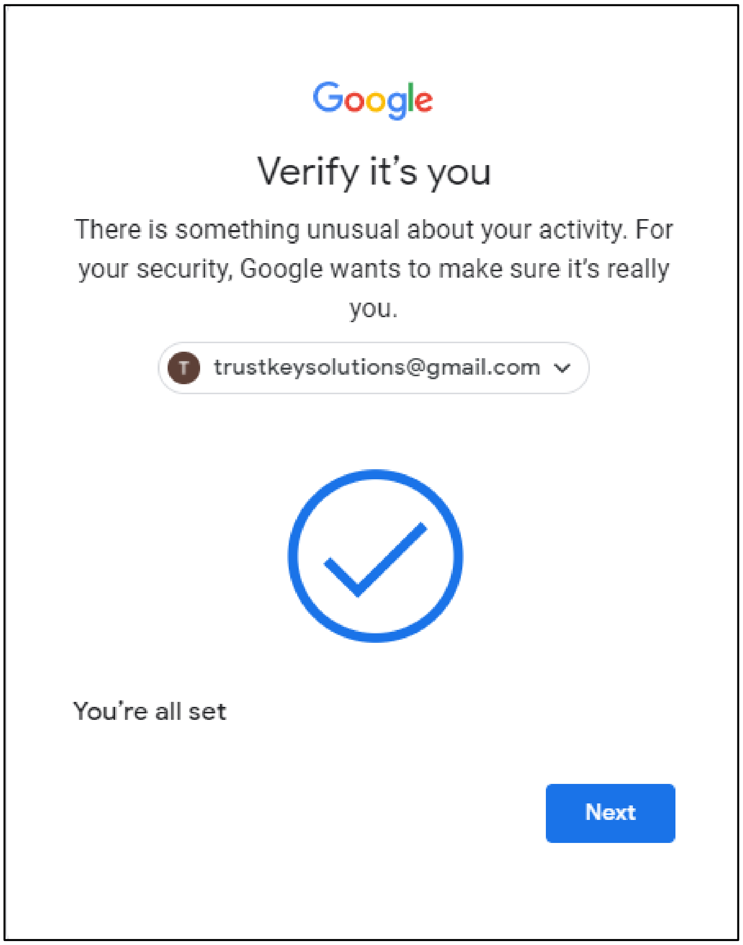
Windows Security

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.



Google

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 the 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.

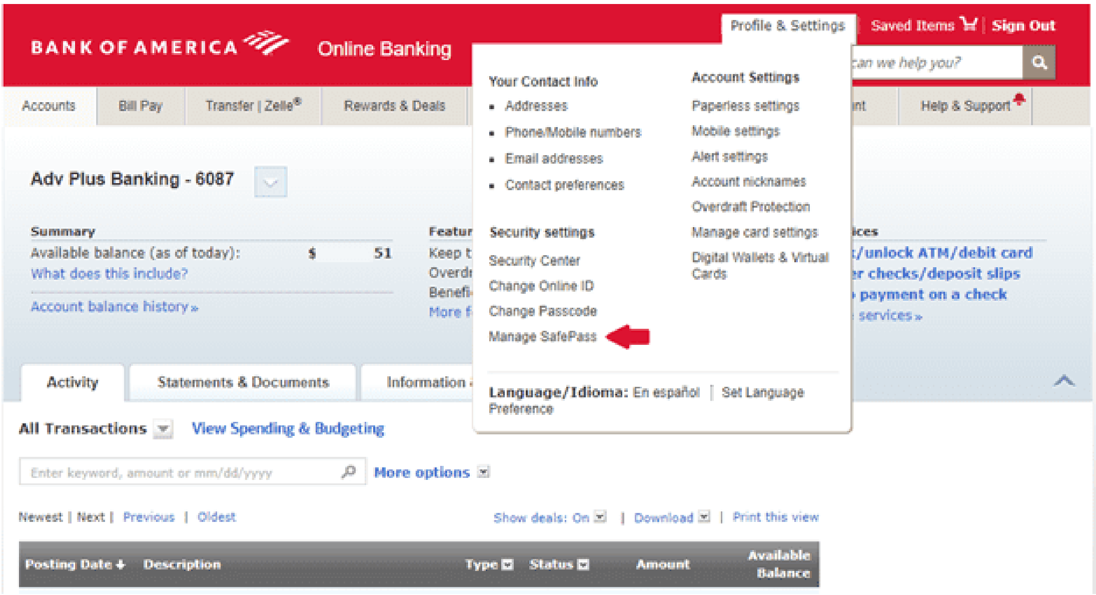
~~Bank of America allows customers to increase the protection of online accounts with new Security Key feature.~~

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.

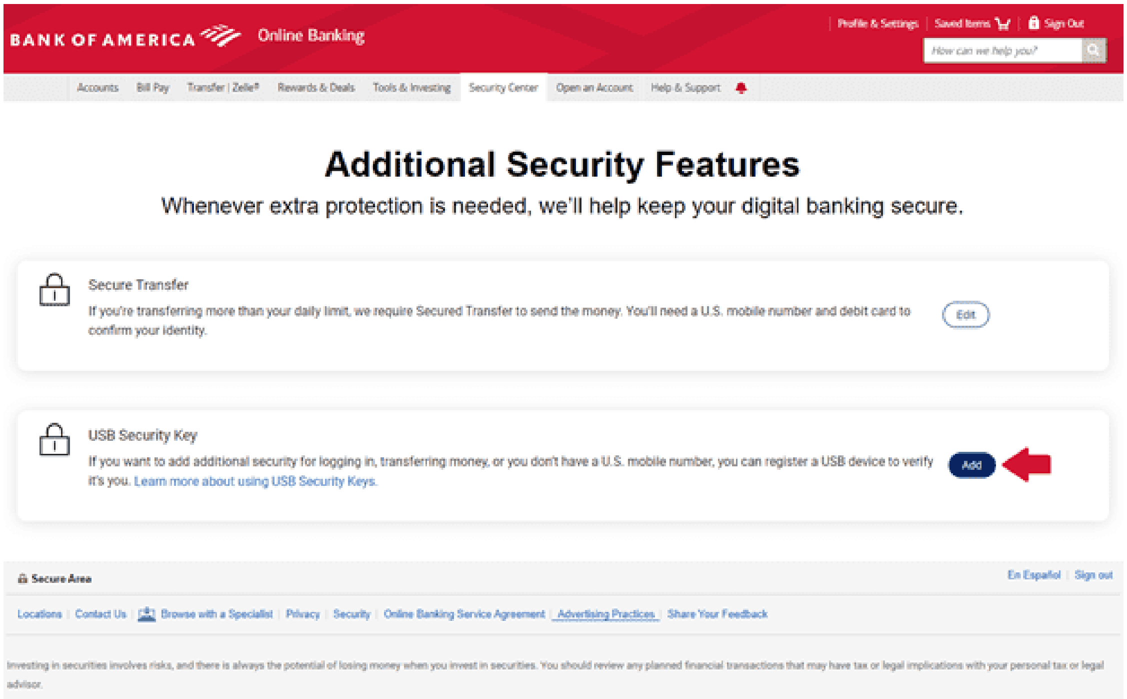
SafePass has long been Bank of America's solution to provide an additional layer of security against unauthorized transactions. However, SafePass only allows customers to use mobile authentication with a one-time code. With the introduction of the Secured Transfer feature, Bank of America has managed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

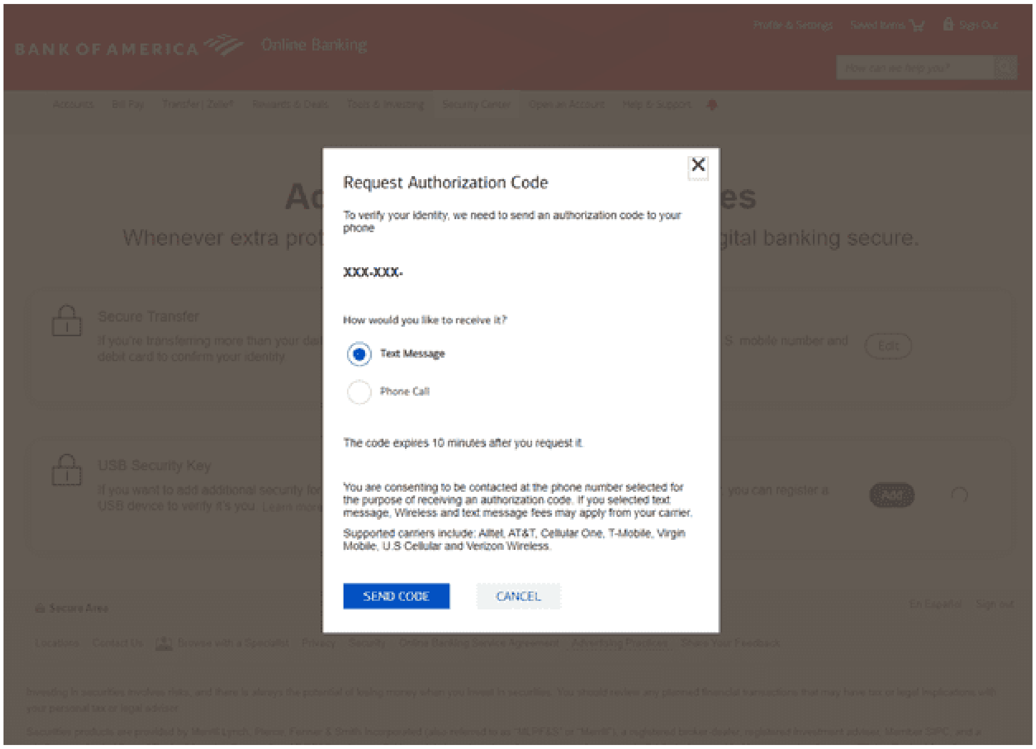
USB Security Key

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

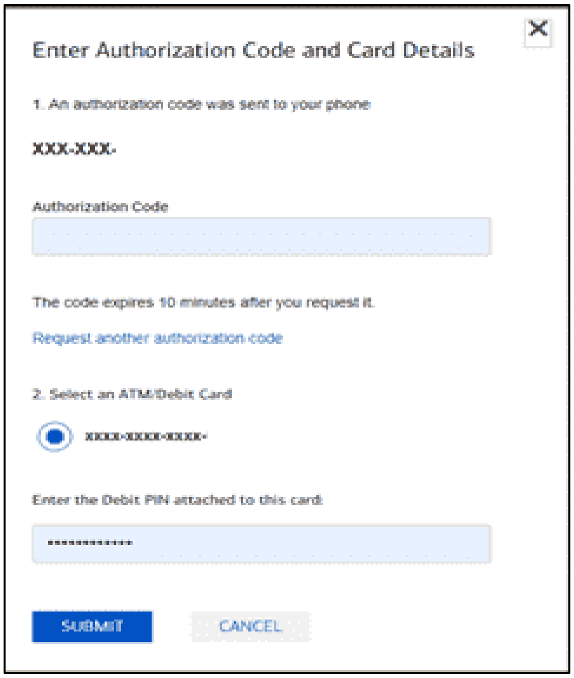
○ Phone Call

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

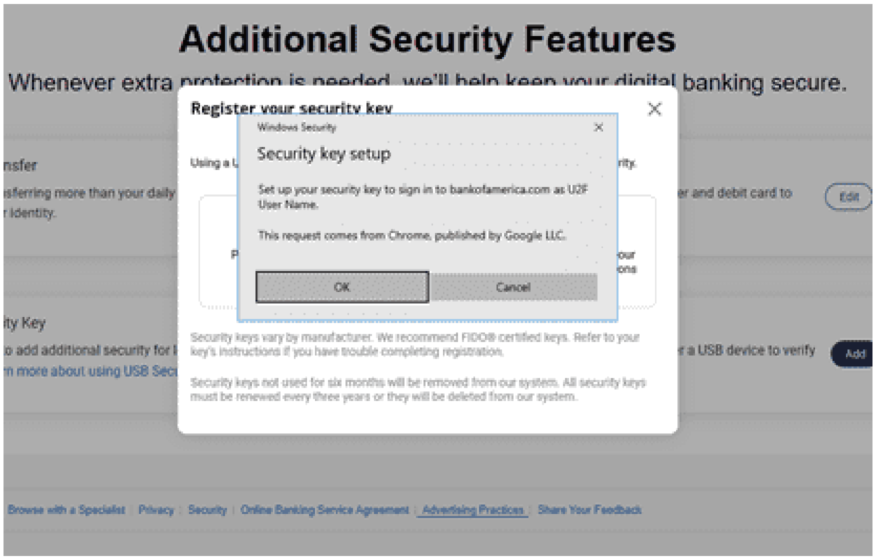
2. Select an ATM/Debit Card

● XXXX-XXXX-XXXX-

Enter the Debit PIN attached to this card:

****

Step 5: Click OK on the 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.

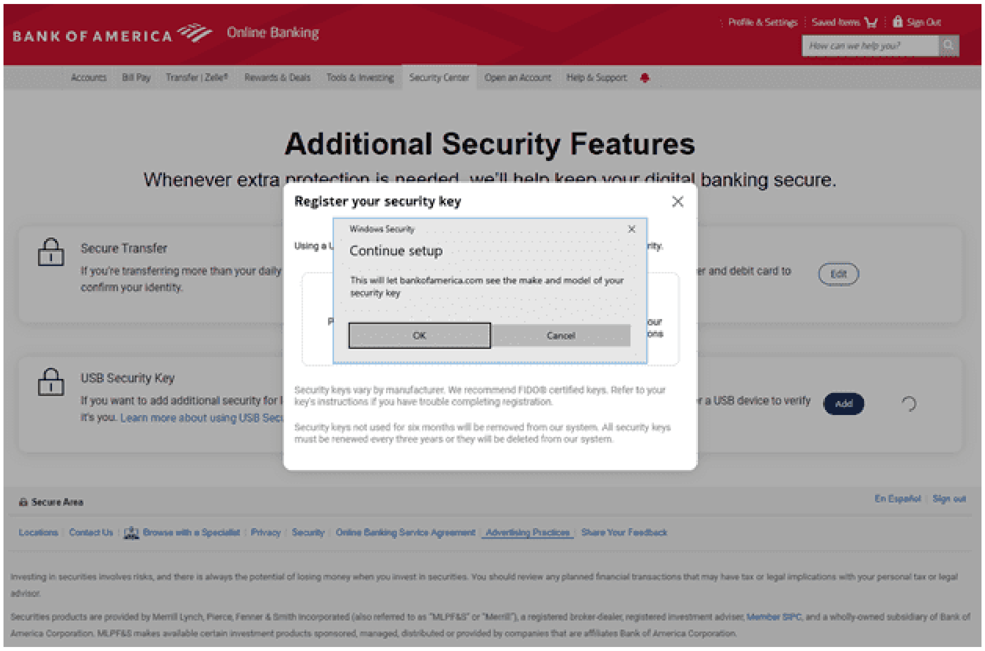
This request comes from Chrome, published by Google LLC.

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.

nsfer
sferring more than your daily
r identity.
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 give access to Bank of America in seeing, making, and modeling your security key on their site



Additional Security Features

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

Register your security key

Windows Security

Continue setup

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

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.

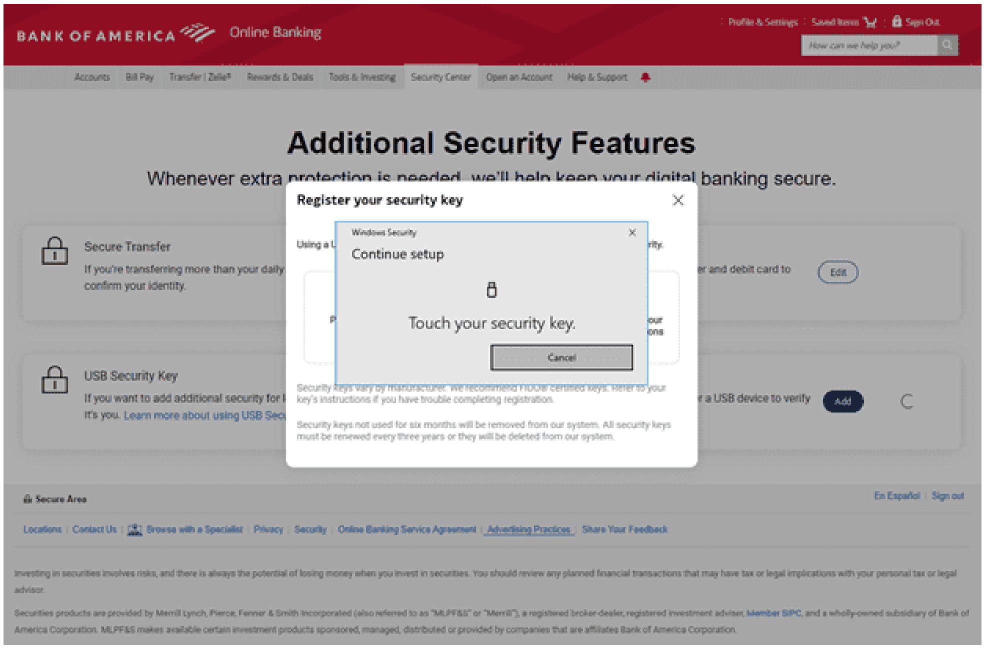
Secure Transfer

If you're transferring more than your daily ... confirm your identity.

USB Security Key

If you want to add additional security for ... it's you. Learn more about using USB Sec...

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



Additional Security Features

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

Register your security key

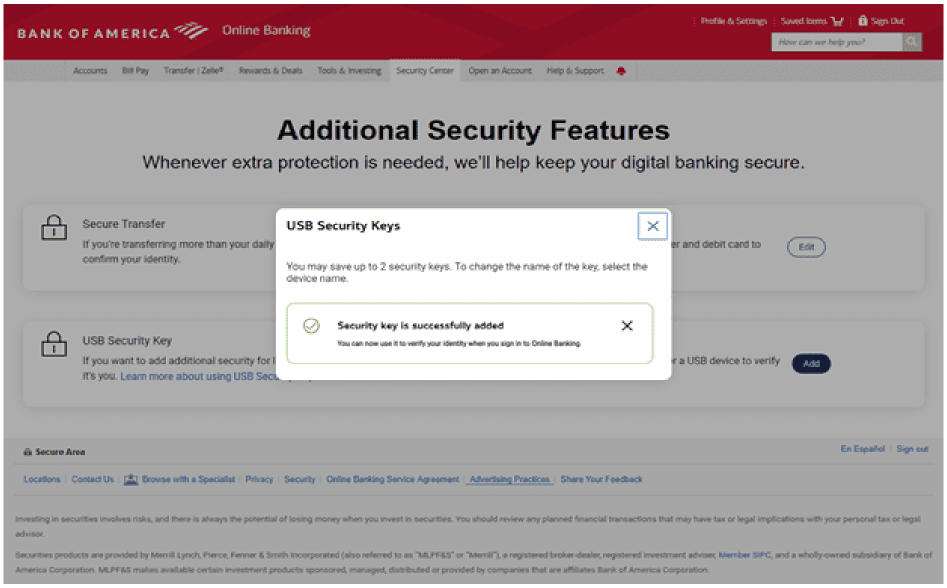
Windows Security

Continue setup

Touch your security key.

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.

Step 8: If successful, you will see the message that shows the 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 I … 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.

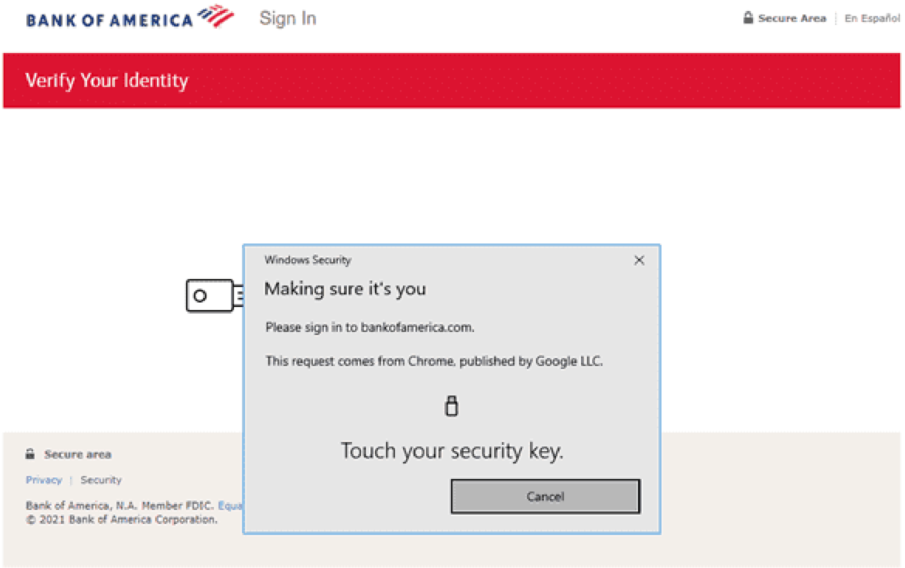
Security key is successfully added

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: 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

Appendix

1. Frequently Asked Questions

Using T-Series Security Keys

How do you enroll your fingerprint to the T-Series security key?

T-series does not support fingerprint enrolment. Please use TrustKey G-series security keys (G310H and G320H).

How many resident keys do T-Series keys hold?

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

How many TOTP accounts can T-series support?

T-Series keys can hold up to 50 TOTP accounts.

Can I use T110 or T120 for Bank of America?

Yes. T-series (T110/T120) supports Bank of America authentication mechanism.

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 T-Series security key with Windows PC, Mac?

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

Which web browsers do you support?

T-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.

T-Series Security Key Features

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

T-Series security keys fully support Microsoft Azure AD. It can be used to sign into Azure joined Windows PC online or offline/airplane mode.

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

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

Can I use the security key on different computers?

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

Misc.

Which certification level do you have?

T-Series security key is Security Level-1 certified security key from FIDO Alliance. However, G-series is the world's first authentication device to achieve FIDO2 Level 2 security certification by satisfying secure operating environment requirements by the FIDO Alliance. The differences between T-series and G-series include fingerprint sensors and associated fingerprint recognition algorithms. Therefore, T-series is as secure as G-series. It's a matter of getting certification from 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?

No. T110 and T120 do not support Windows Hello.

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) eWBM Inc. dba TrustKey Solutions (USA)
Technical support	Korea: TEL : +82-02-556-7878 / email : support@trustkey.kr USA: TEL: (214) 865-9354 Email: support@trustkeysolutions.com
Webpages	Korea: www.trustkey.kr USA: www.trustkeysolutions.com
Addresses	Korea: (06236) 2F, 14, Teheran-ro 22-gil, Gangnam-gu, Seoul USA: 2100 Alamo Rd Suite T, Richardson, TX 75080

Copyright