T110/T20
User Manual

V1.2

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

0. Before Using the TrustKey Security Keys

1. How to Use TrustKey Security Keys

2. Appendix

0. Before Using the TrustKey Security Keys

1. Precautions before using a security key

- You need to register security key's PIN before use. The detailed steps to writing PIN will be in Section 1.4 or 1.5

- Please choose the correct USB port for your security key (USB-A or USB-C)

- Check the version of your device including Windows PC, Macs, Android 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 Browsers		Support all chromium-based web browsers (Recommend to use the latest version)

1. How to Use TrustKey Security Keys

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 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/B210H 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. What is the Security Key's PIN?

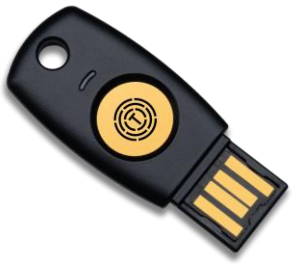
The PIN is similar to the password but used differently. The password is a shared secret between the user and the server. The client system asks the user to type in the password and sends the password information to the server for verification. Unlike the password, the PIN is not sent to the server;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

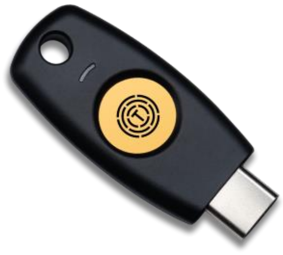
The PIN is needed for fingerprint enrolment and modification. It is also used for backup authentication when fingerprint authentication failed.

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

3. Introduction to Security Key

1) Product Specification

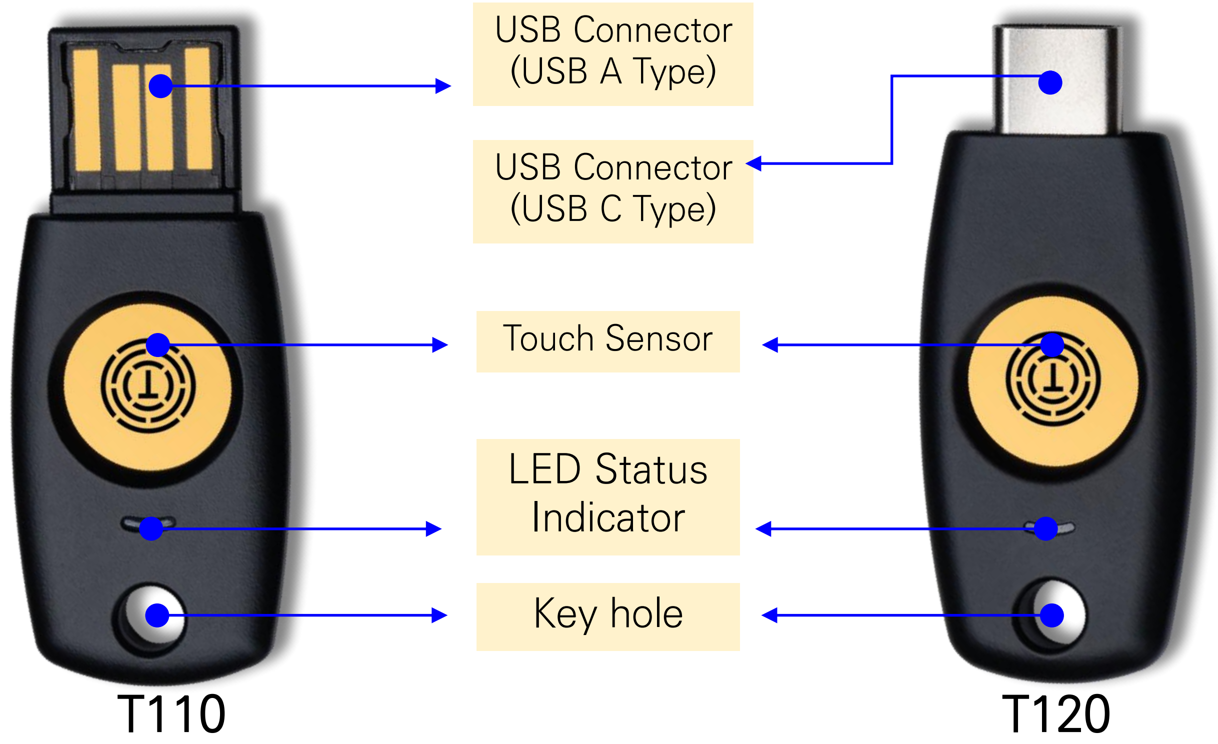




Product Name	T110	T120
Model Name	eTA310	eTA320
USB Type	Type A	Type C
Color	Black	Black
Authentication Action	PIN+Touch	PIN+Touch
Operation Temp	−20℃ ~ +60℃	−20℃ ~ +60℃
Storage Temp	−40℃ ~ +85℃	−40℃ ~ +85℃
HOTP, TOTP	O	O
Device Type	HID Device	HID Device
Status Indicator	White Color LED	White Color LED
Material	Polycarbonate (Touch area: Gold plate)	Polycarbonate (Touch area: Gold plate)
FIDO Protocol	FIDO2, U2F	FIDO2, U2F
FIDO Security Level	Level 1	Level 1
Certification	KC, CE, FCC	KC, CE, FCC
Size	17.8x41.89x3.8 (mm)	17.8x41.6x4.6 (mm)
Weight	2.9g	2.9g

3. Introduction to Security Key

2) Basic Features of Your TrustKey



USB Connector (USB A Type)

USB Connector (USB C Type)

Touch Sensor

LED Status Indicator

Key hole

T110

T120

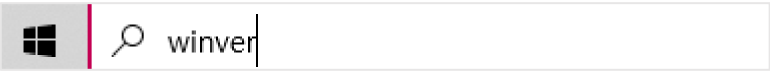
- ### LED Status Indicator

Color	Status	Description	Action
□ White	ON	① Key Connection Success ② Authentication Success	
	Blinking	Waiting for touch recognition	
	OFF	Key Connection Fail	Reinsert the key or change the USB port

4. Setting Up Security Key in Windows

1) Windows Version Check

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



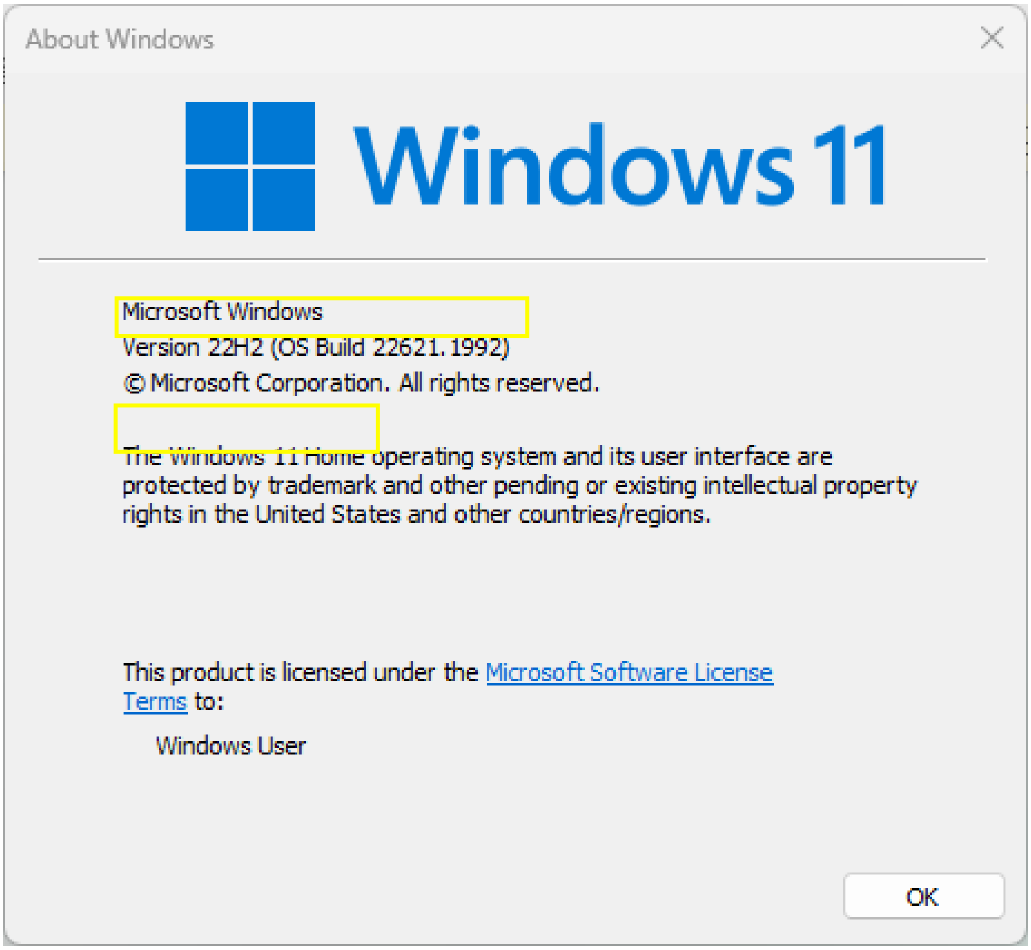
winver

2. Please check the Windows Product Name(①) and version(②).

✓ Available

① Product Name : Windows 10
Home, Professional, Enterprise
Windows 11
Home, Pro, Pro for Workstation, Enterprise

②Version : [19H1] OS build 18298 or later



About Windows

Windows 11

Microsoft Windows
Version 22H2 (OS Build 22621.1992)
© Microsoft Corporation. All rights reserved.

The Windows 11 Home 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

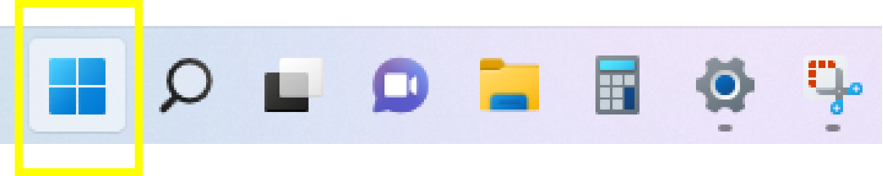
OK

**If your Windows version is earlier than 18298, then you need to upgrade. To update, please refer to the Microsoft Windows Help desk.*

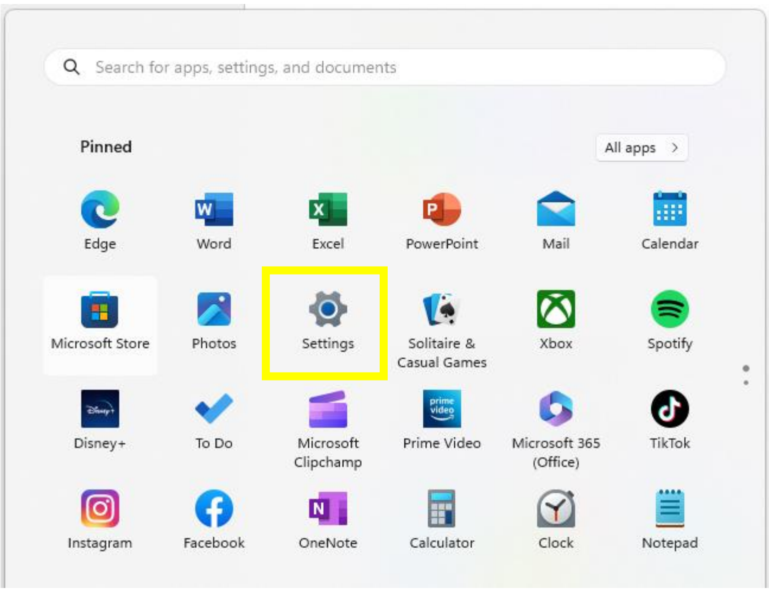
4. Setting Up Security Key in Windows

2) Setting up New PIN [Windows11 Home version 22H2 OS 22621]

1. Click the [**Start**] button on your desktop's taskbar.



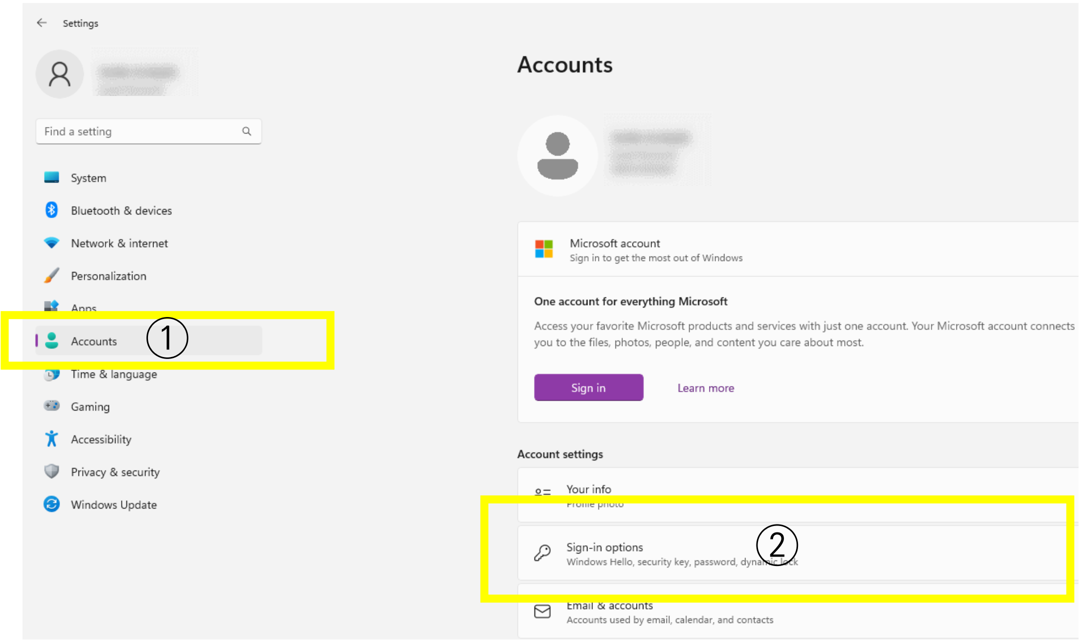
2. Find and launch [**Settings**] from the Start screen.



4. Setting Up Security Key in Windows

2) Setting up New PIN [Windows11 Home version 22H2 OS 22621]

3. From Settings, Click [①**Accounts**] – [②**Sign-in options**]



Microsoft account
Sign in to get the most out of Windows

One account for everything Microsoft

Access your favorite Microsoft products and services with just one account. Your Microsoft account connects you to the files, photos, people, and content you care about most.

Account settings

Your info
Profile photo

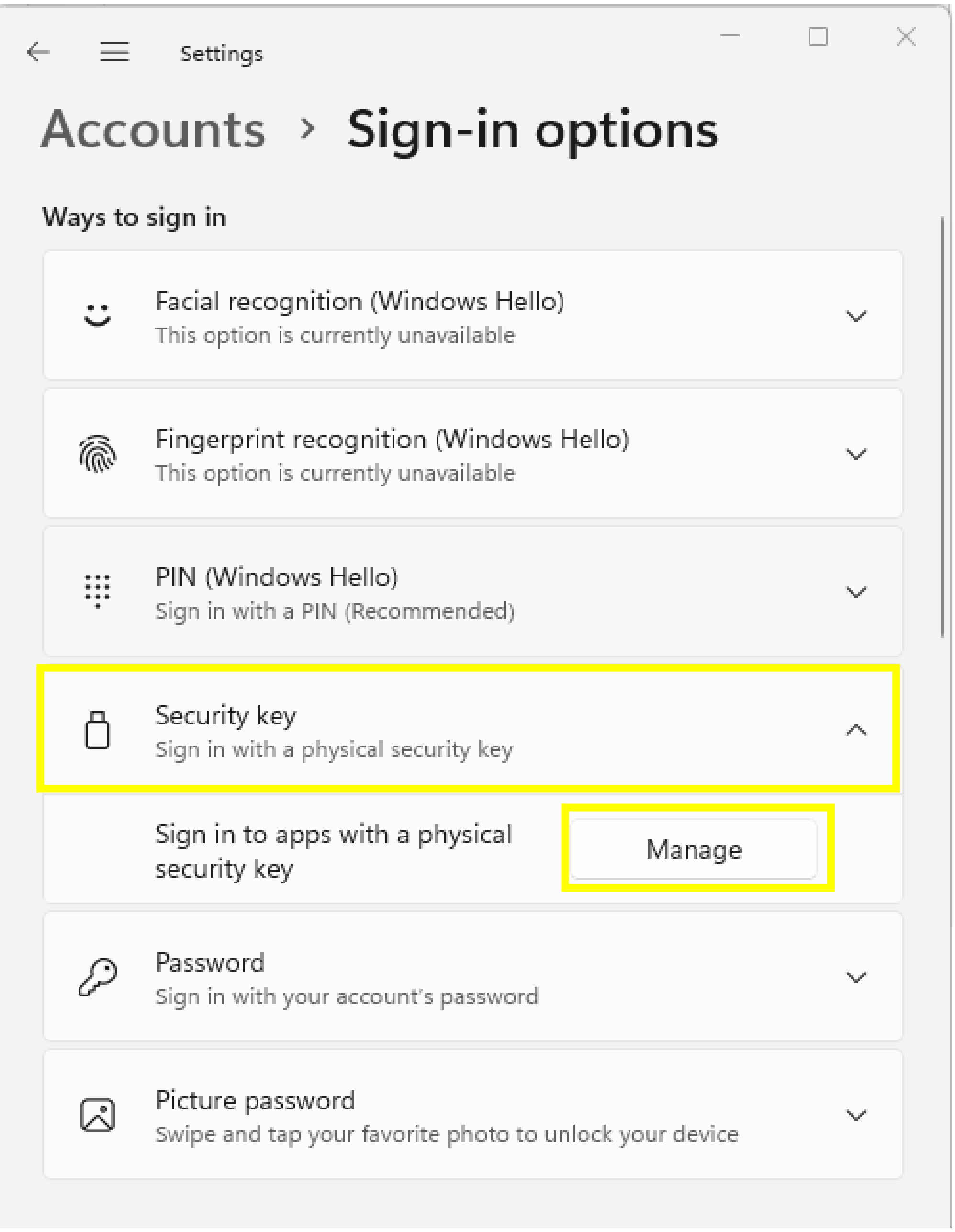
Sign-in options
Windows Hello, security key, password, dynamic lock

Email & accounts
Accounts used by email, calendar, and contacts

4. Setting Up Security Key in Windows

2) Setting up New PIN [Windows11 Home version 22H2 OS 22621]

4. Make sure the [**Manage**] button is enabled in [**Security Key**], then click the [**Manage**] button.



Settings

Accounts › Sign-in options

Ways to sign in

Facial recognition (Windows Hello)
This option is currently unavailable

Fingerprint recognition (Windows Hello)
This option is currently unavailable

PIN (Windows Hello)
Sign in with a PIN (Recommended)

Security key
Sign in with a physical security key

Sign in to apps with a physical security key

Manage

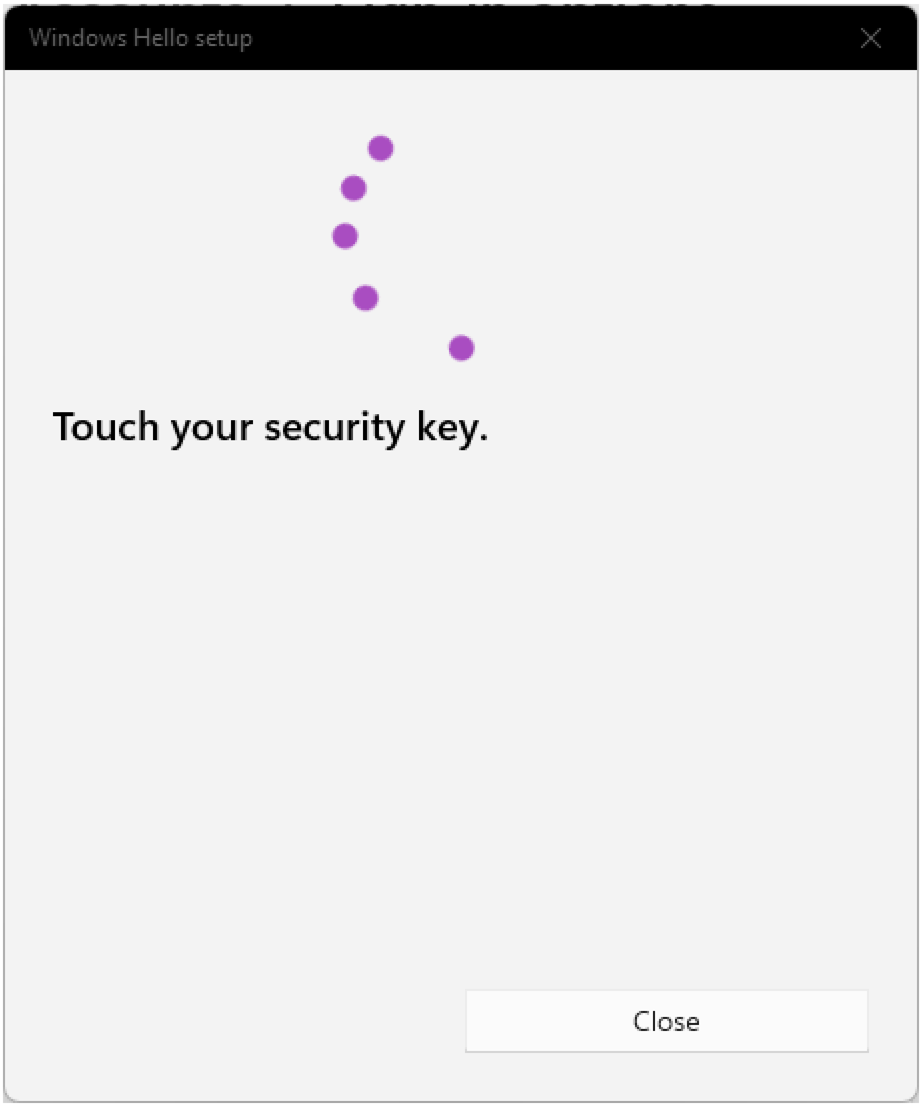
Password
Sign in with your account's password

Picture password
Swipe and tap your favorite photo to unlock your device

4. Setting Up Security Key in Windows

2) Setting up New PIN [Windows11 Home version 22H2 OS 22621]

5. When you insert the T110/T120 into the USB port, the white LED indicator lights up.
The white LED indicator on the security key flashes as the Windows Hello installation window appears, as shown in the figure below. At this point, touch the touch sensor on the security key.

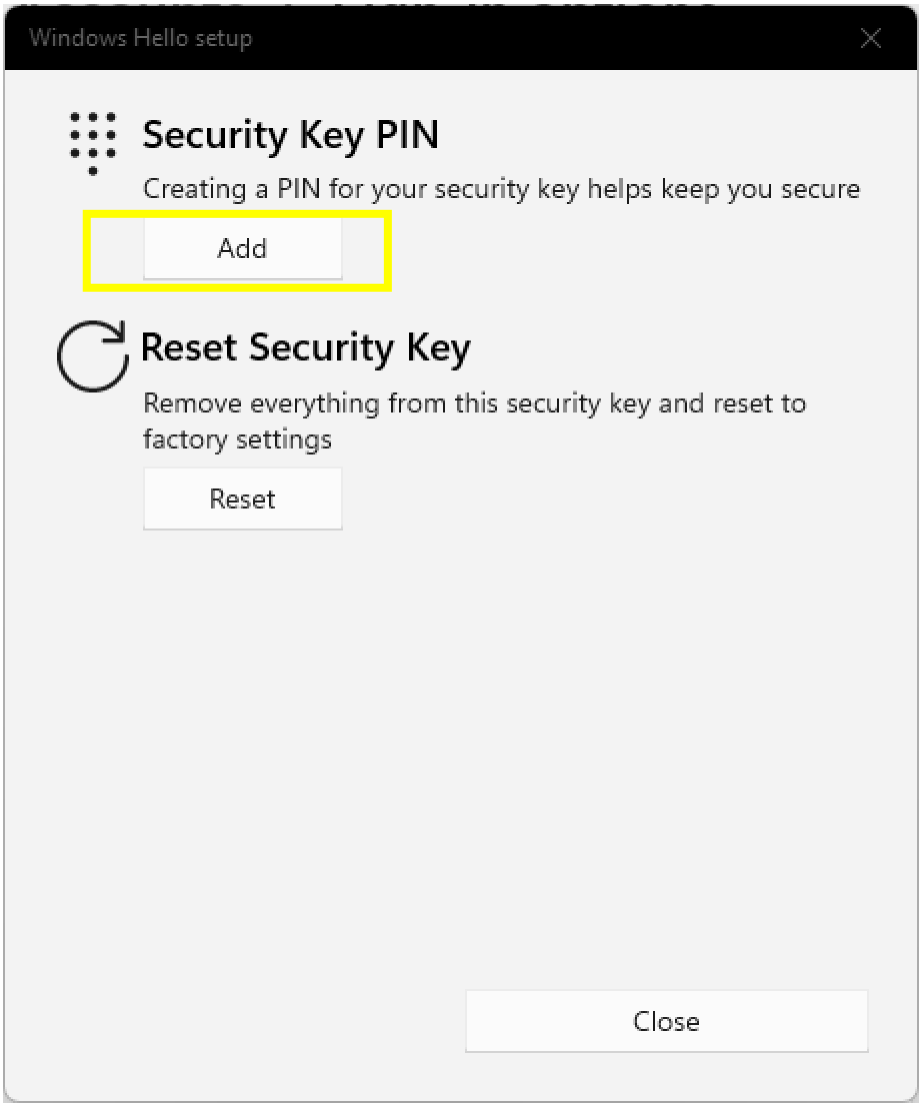


Touch your security key.

4. Setting Up Security Key in Windows

2) Setting up New PIN [Windows11 Home version 22H2 OS 22621]

6. Click [Add] button of Security Key PIN



Windows Hello setup

Security Key PIN

Creating a PIN for your security key helps keep you secure

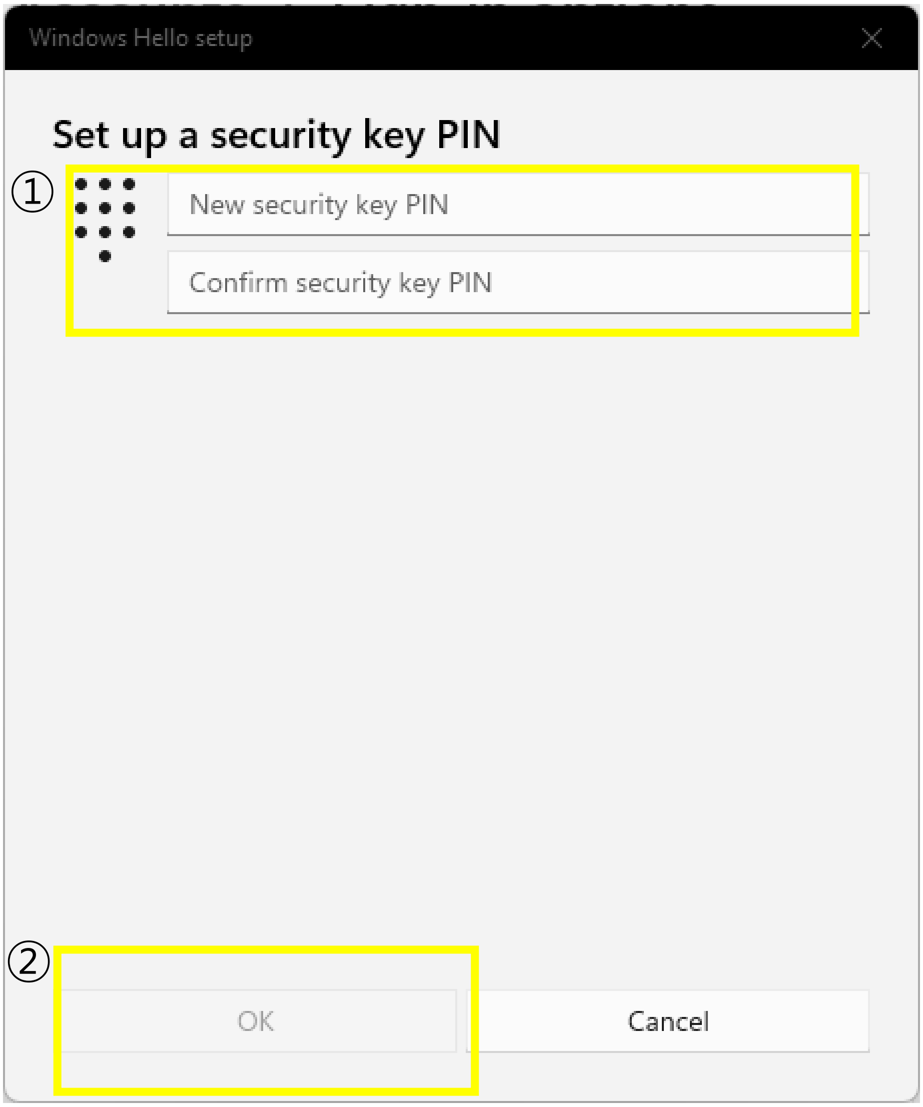
Reset Security Key

Remove everything from this security key and reset to factory settings

4. Setting Up Security Key in Windows

2) Setting up New PIN [Windows11 Home version 22H2 OS 22621]

7. Enter your security key PIN, then click [OK] button to complete PIN registration.
(we recommend using 4~63 alphanumeric characters, upper and lower letters, numbers, and special characters).

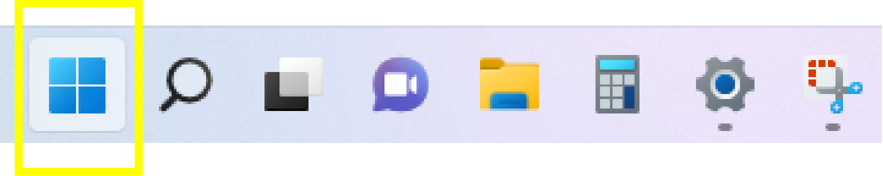


4. Setting Up Security Key in Windows

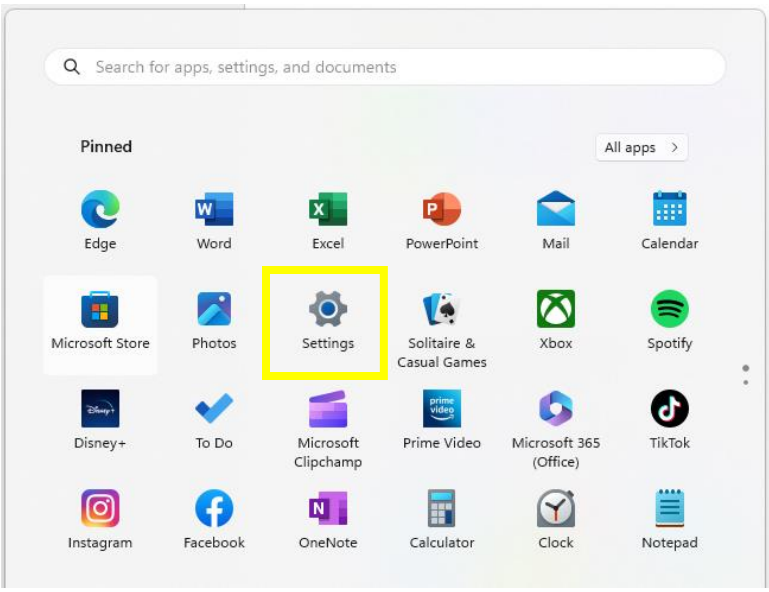
3) How to delete PIN [Windows11 Home version 22H2 OS 22621]

Notice!
The process of deleting a PIN is the same as a factory reset, which means that all data and credentials in the security key are lost.

1. Click the [**Start**] button on your desktop's taskbar.



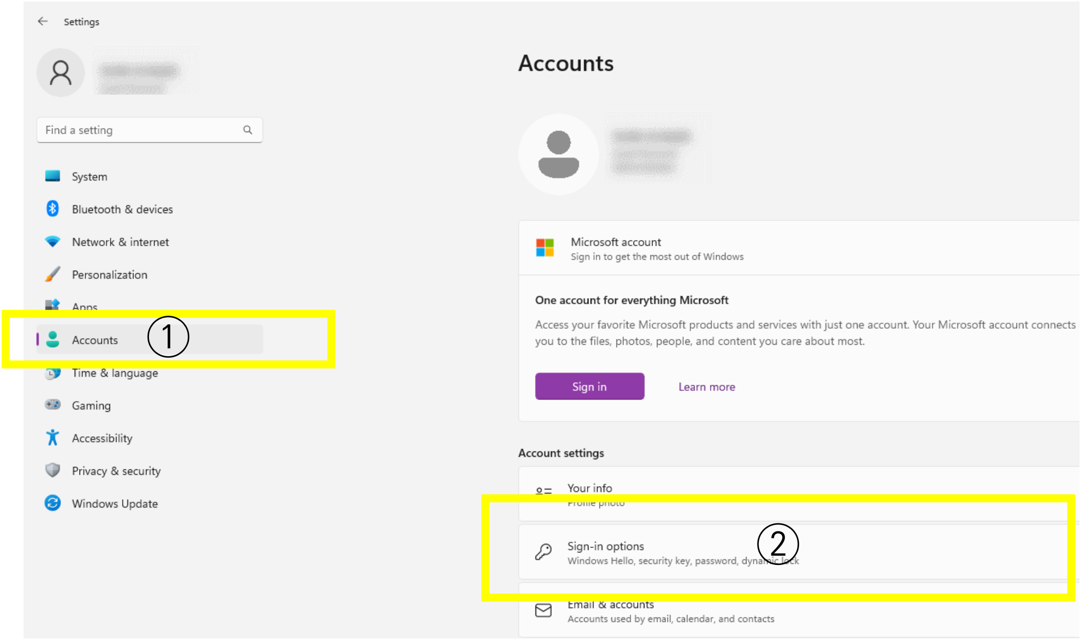
2. Find and launch [**Settings**] from the Start screen.



4. Setting Up Security Key in Windows

3) How to delete PIN [Windows11 Home version 22H2 OS 22621]

3. From Settings, Click [①**Accounts**] – [②**Sign-in options**]



Microsoft account
Sign in to get the most out of Windows

One account for everything Microsoft

Access your favorite Microsoft products and services with just one account. Your Microsoft account connects you to the files, photos, people, and content you care about most.

Your info
Profile photo

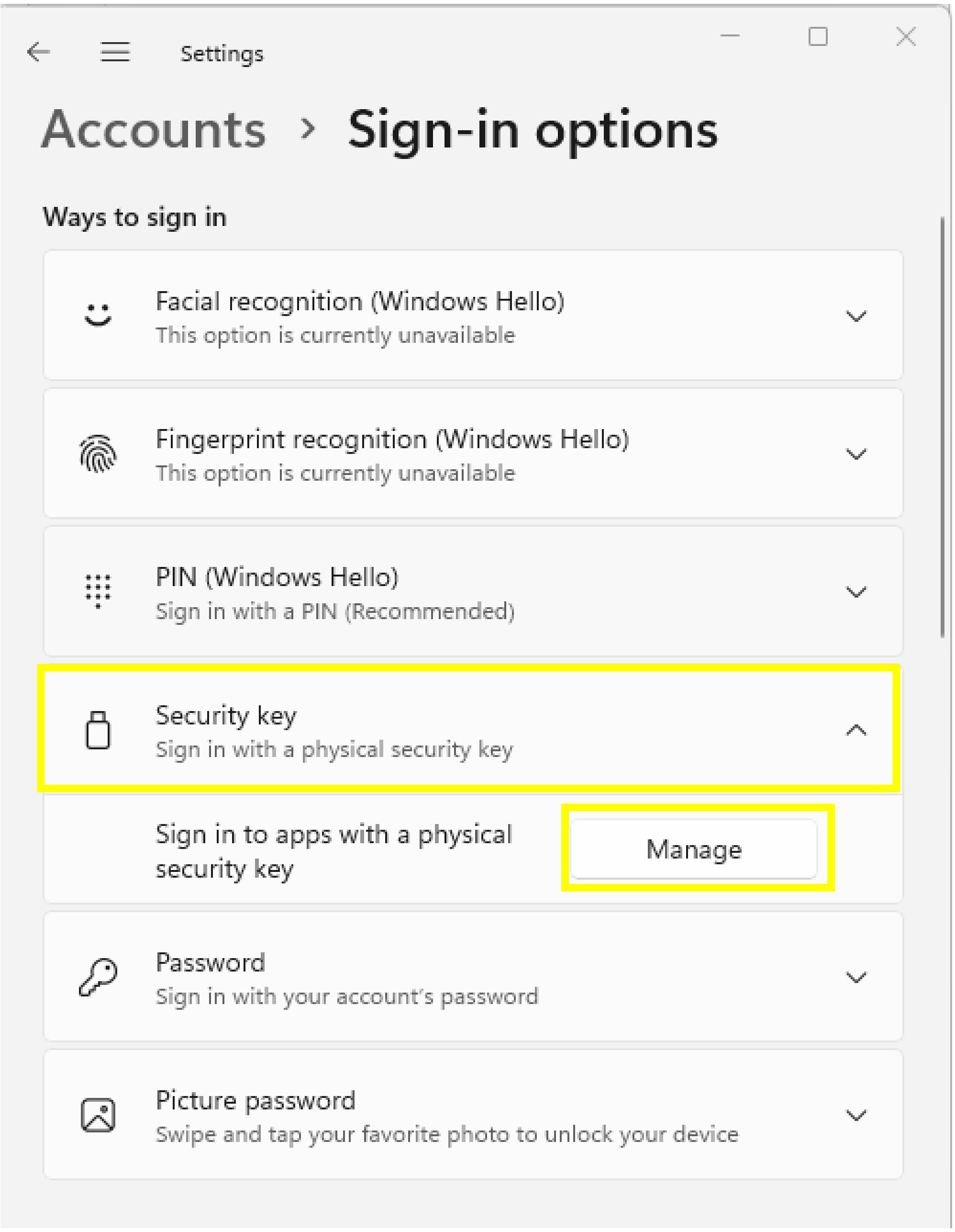
Sign-in options
Windows Hello, security key, password, dynamic lock

Email & accounts
Accounts used by email, calendar, and contacts

4. Setting Up Security Key in Windows

3) How to delete PIN [Windows11 Home version 22H2 OS 22621]

4. Make sure the [**Manage**] button is enabled in [**Security Key**], then click the [**Manage**] button.



Settings

Accounts › Sign-in options

Ways to sign in

Facial recognition (Windows Hello)
This option is currently unavailable

Fingerprint recognition (Windows Hello)
This option is currently unavailable

PIN (Windows Hello)
Sign in with a PIN (Recommended)

Security key
Sign in with a physical security key

Sign in to apps with a physical security key

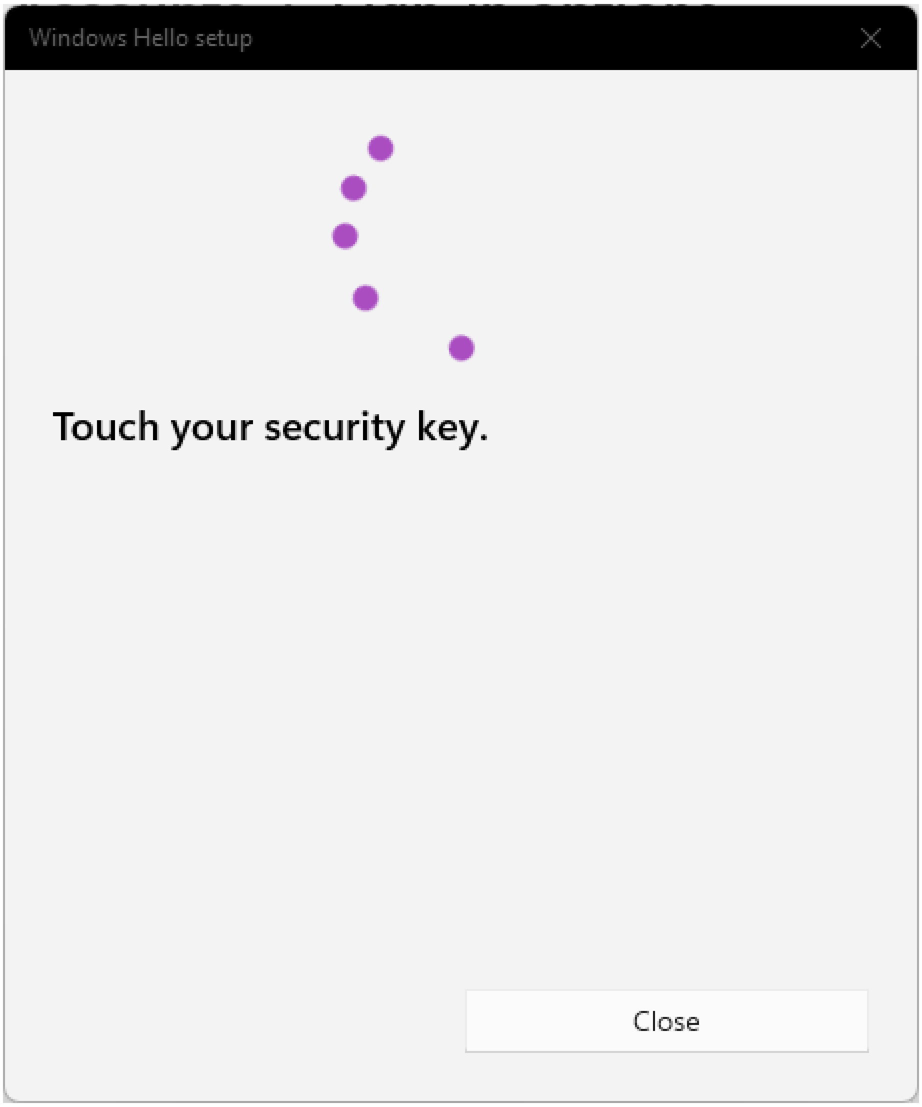
Password
Sign in with your account's password

Picture password
Swipe and tap your favorite photo to unlock your device

4. Setting Up Security Key in Windows

3) How to delete PIN [Windows11 Home version 22H2 OS 22621]

5. When you insert the T110/T120 into the USB port, the white LED indicator lights up.
The white LED indicator on the security key flashes as the Windows Hello installation window appears, as shown in the figure below. At this point, touch the touch sensor on the security key.



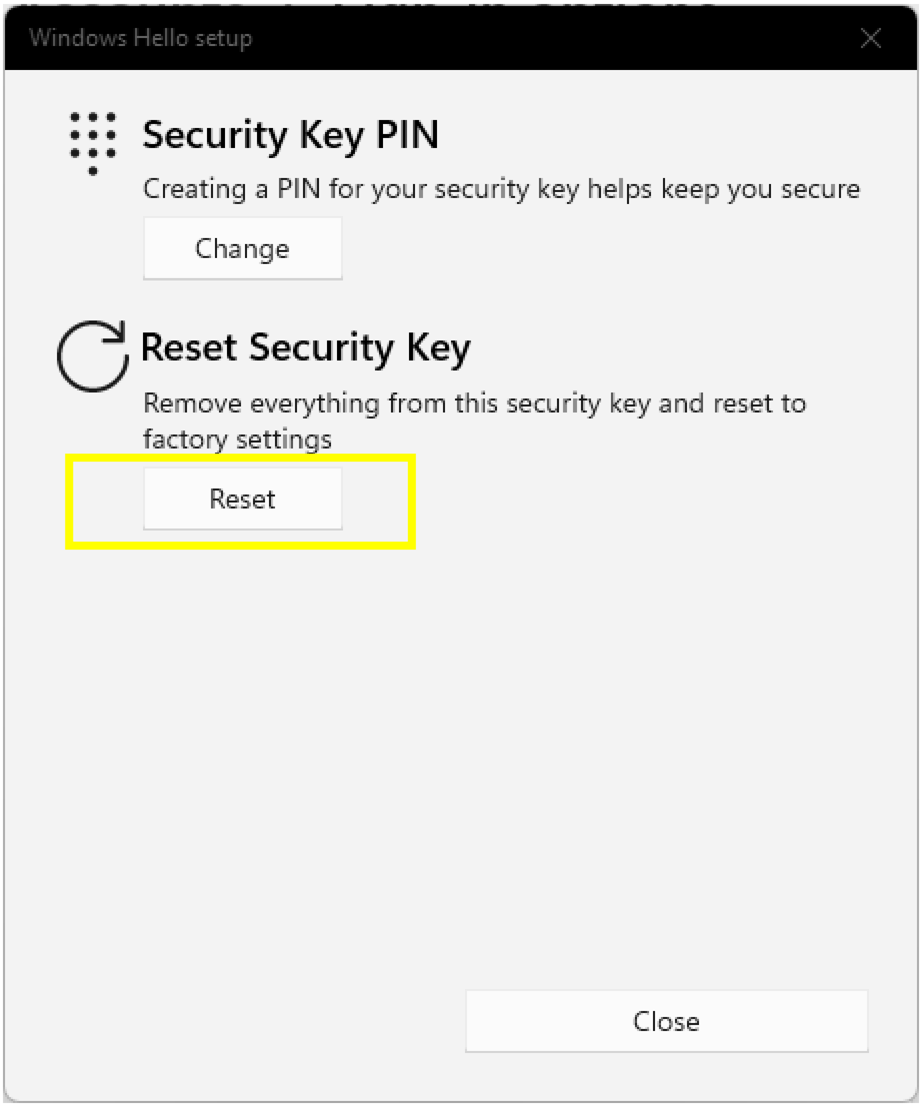
Windows Hello setup

Touch your security key.

4. Setting Up Security Key in Windows

3) How to delete PIN [Windows11 Home version 22H2 OS 22621]

6. Click the [**Reset**] button under 'Reset security key' as shown below.



Windows Hello setup

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

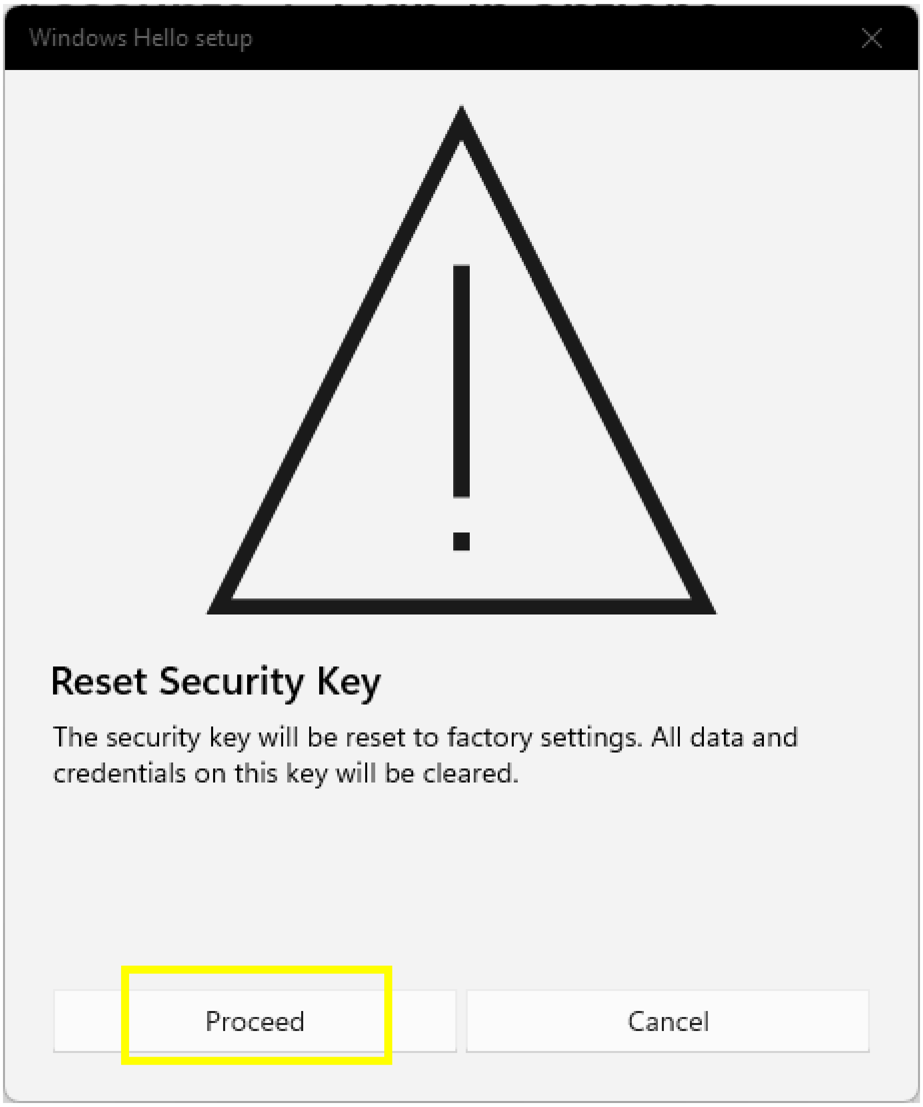
Reset

Close

4. Setting Up Security Key in Windows

3) How to delete PIN [Windows11 Home version 22H2 OS 22621]

7. Click [Proceed] button.



Windows Hello setup

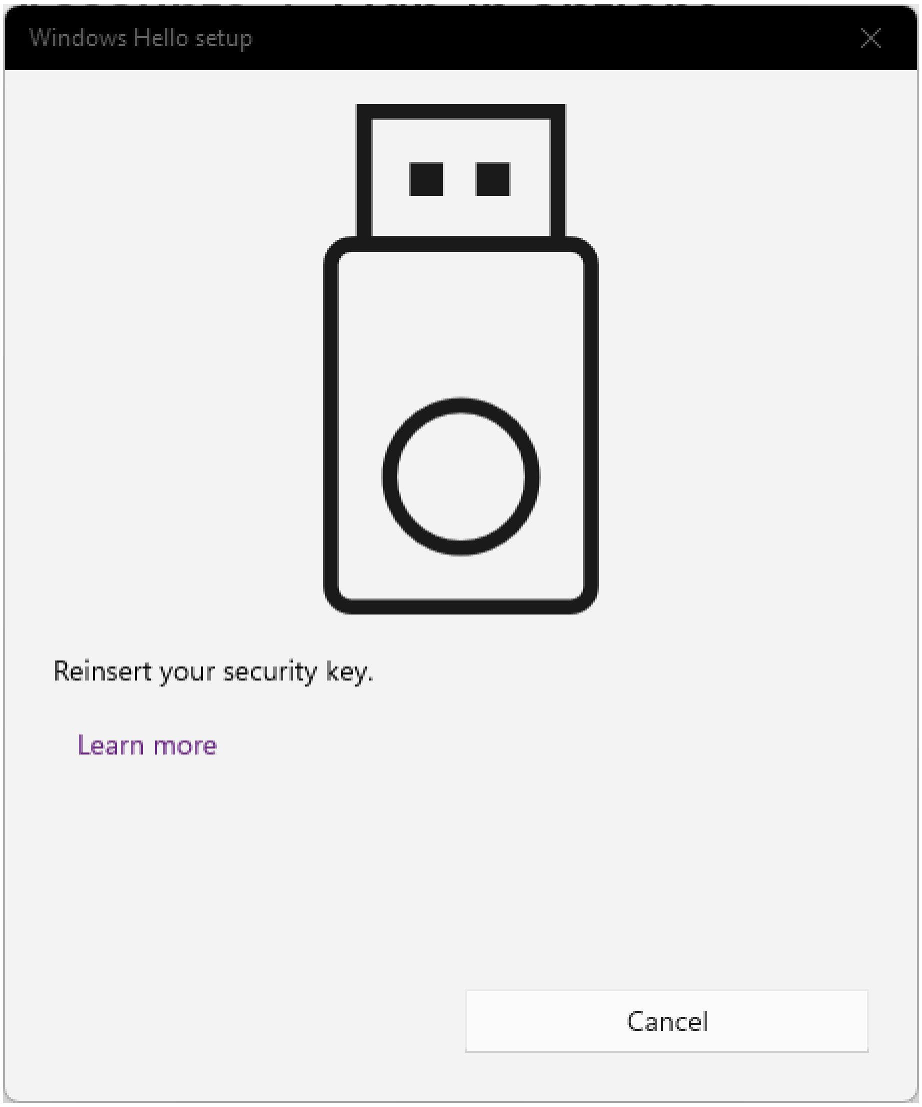
Reset Security Key

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

4. Setting Up Security Key in Windows

3) How to delete PIN [Windows11 Home version 22H2 OS 22621]

8. Please reinsert your security key.

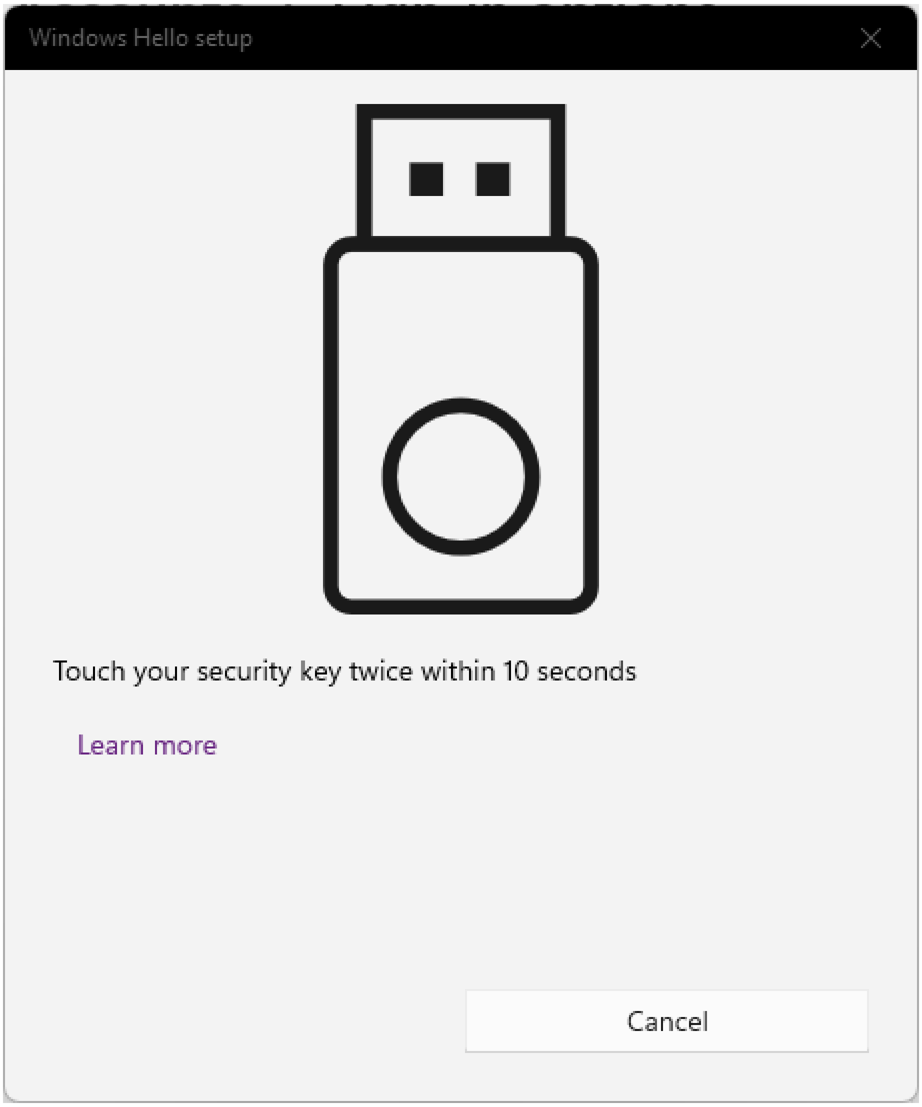


Windows Hello setup

Reinsert your security key.

3) How to delete PIN [Windows11 Home version 22H2 OS 22621]

9. When the LED indicator flashes white, touch the security key's touch sensor twice within 10 seconds. If it times out, reinsert the security key and touch it twice.

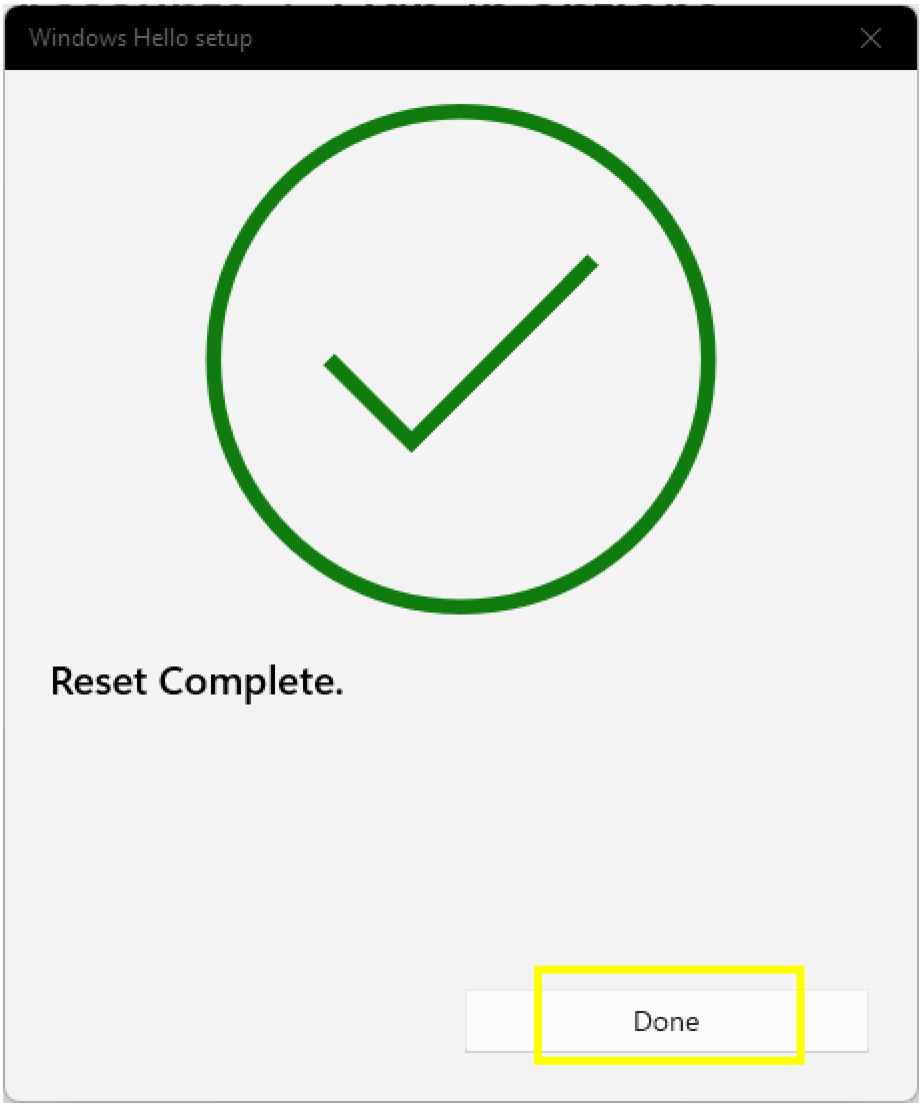


Touch your security key twice within 10 seconds

4. Setting Up Security Key in Windows

3) How to delete PIN [Windows11 Home version 22H2 OS 22621]

10. Click the [Done] button to remove everything from the security key and complete the factory reset.

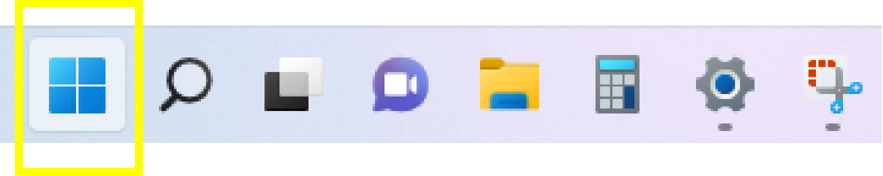


Reset Complete.

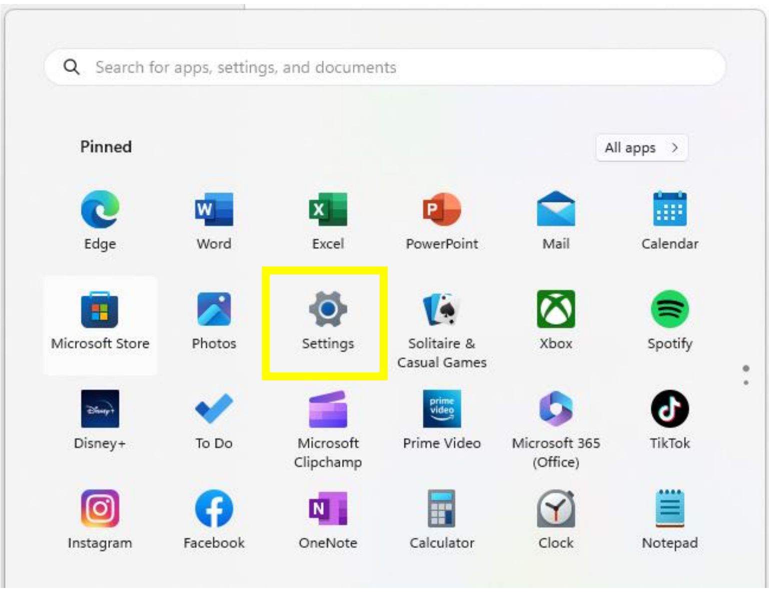
4. Setting Up Security Key in Windows

4) How to change PIN [Windows11 Home version 22H2 OS 22621]

1. Click the [**Start**] button on your desktop's taskbar.



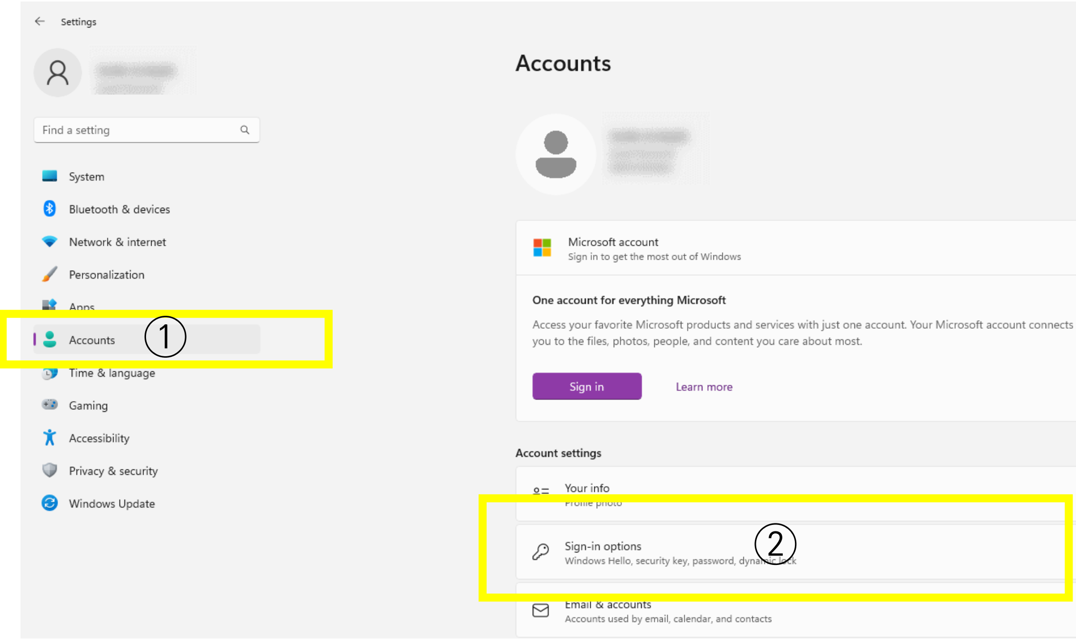
2. Find and launch [**Settings**] from the Start screen.



4. Setting Up Security Key in Windows

4) How to change PIN [Windows11 Home version 22H2 OS 22621]

3. From Settings, Click [①**Accounts**] – [②**Sign-in options**]



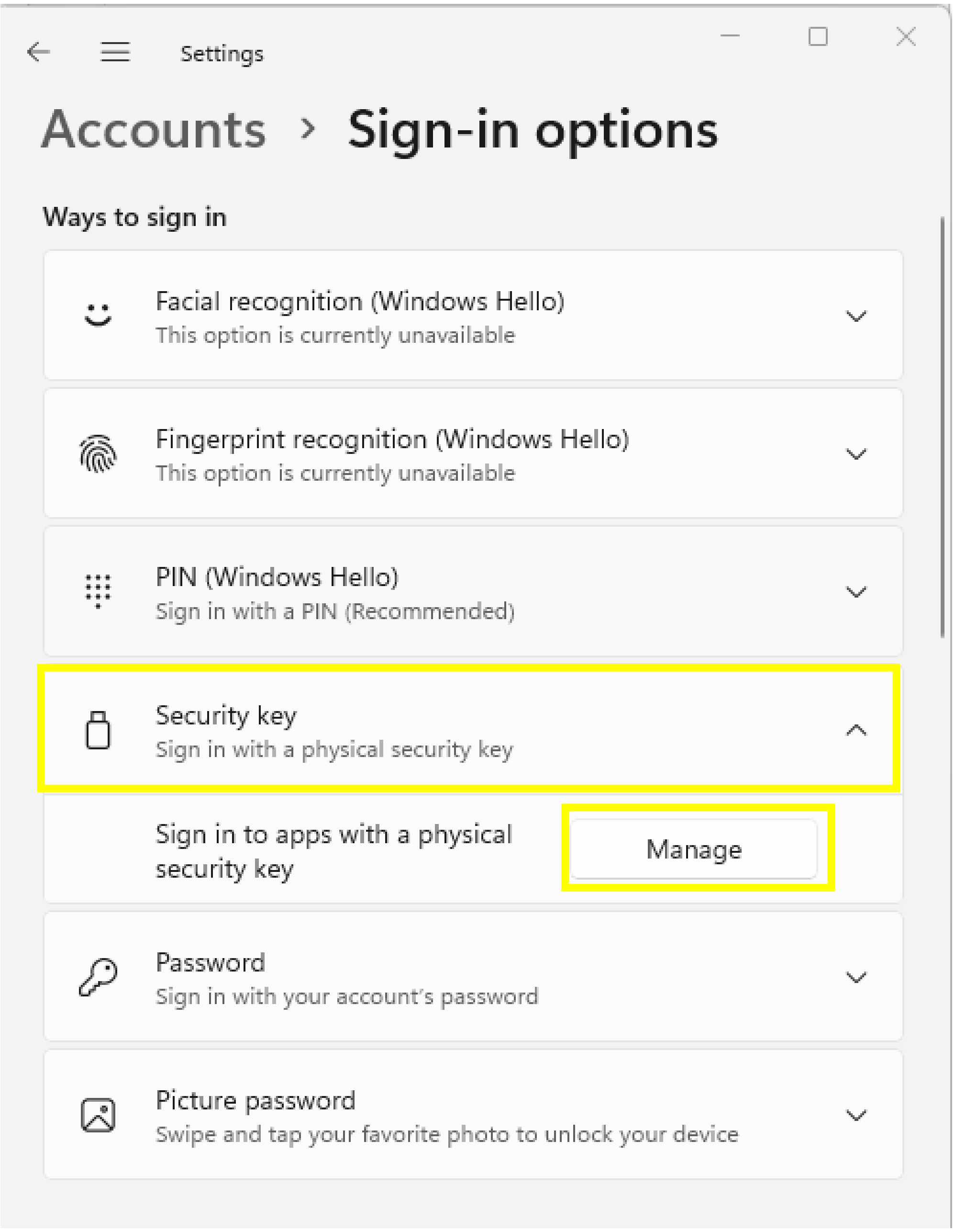
One account for everything Microsoft

Access your favorite Microsoft products and services with just one account. Your Microsoft account connects you to the files, photos, people, and content you care about most.

4. Setting Up Security Key in Windows

4) How to change PIN [Windows11 Home version 22H2 OS 22621]

4. Make sure the [**Manage**] button is enabled in [**Security Key**], then click the [**Manage**] button.



Accounts › Sign-in options

Ways to sign in

Facial recognition (Windows Hello)
This option is currently unavailable

Fingerprint recognition (Windows Hello)
This option is currently unavailable

PIN (Windows Hello)
Sign in with a PIN (Recommended)

Security key
Sign in with a physical security key

Sign in to apps with a physical security key

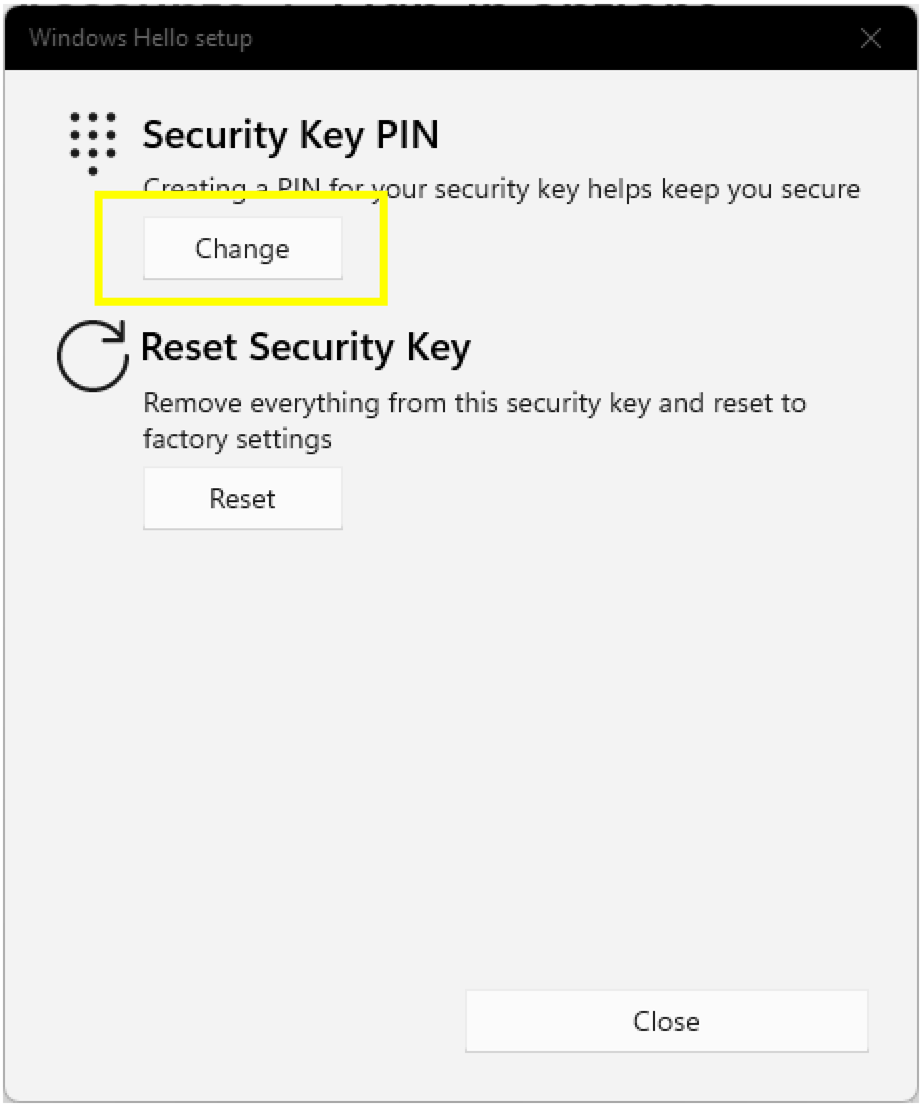
Password
Sign in with your account's password

Picture password
Swipe and tap your favorite photo to unlock your device

4. Setting Up Security Key in Windows

4) How to change PIN [Windows11 Home version 22H2 OS 22621]

5. Click [Change] button of Security Key PIN.



Windows Hello setup

Security Key PIN

Creating a PIN for your security key helps keep you secure

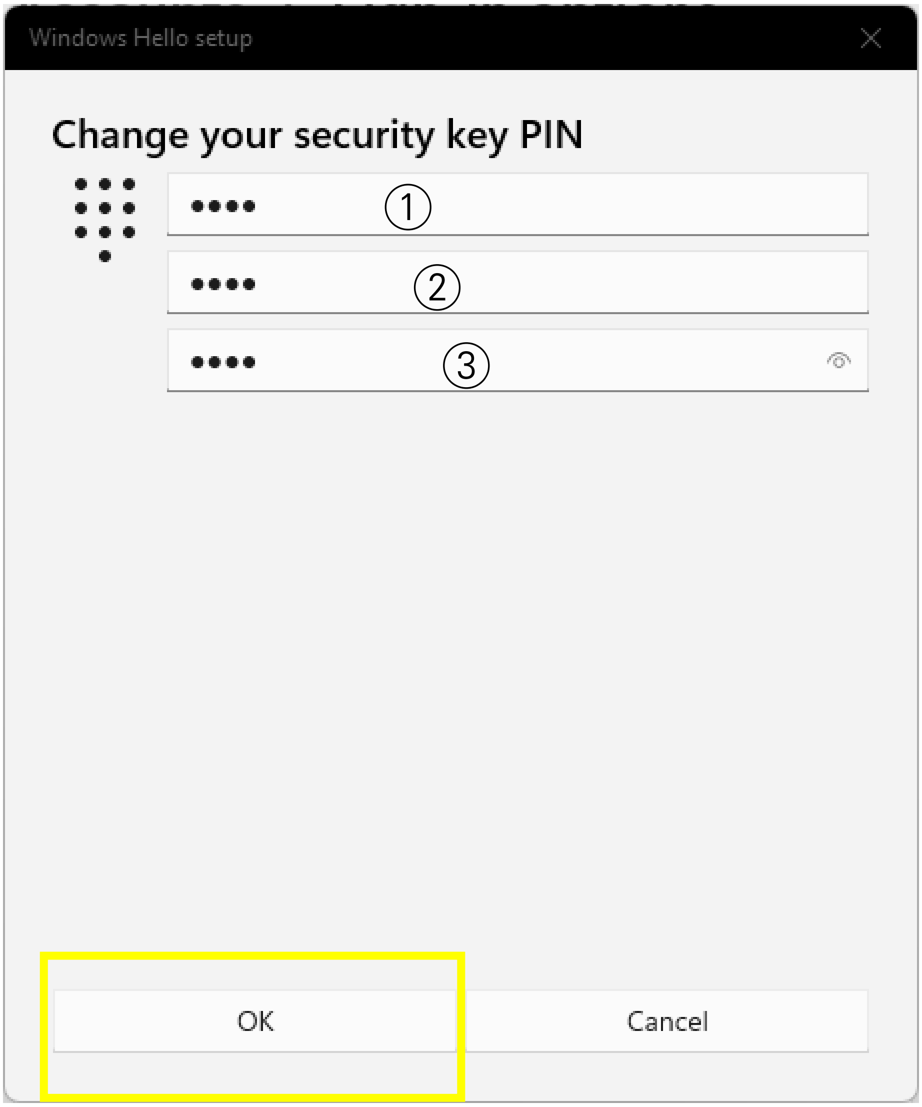
Reset Security Key

Remove everything from this security key and reset to factory settings

4. Setting Up Security Key in Windows

4) How to change PIN [Windows11 Home version 22H2 OS 22621]

6. Enter the security key PIN in field ①, and then enter the new security key PIN in fields ② and ③ below, and click the [OK] button to complete the 'Change your security key PIN'



Windows Hello setup

Change your security key PIN

●●●● ①

●●●● ②

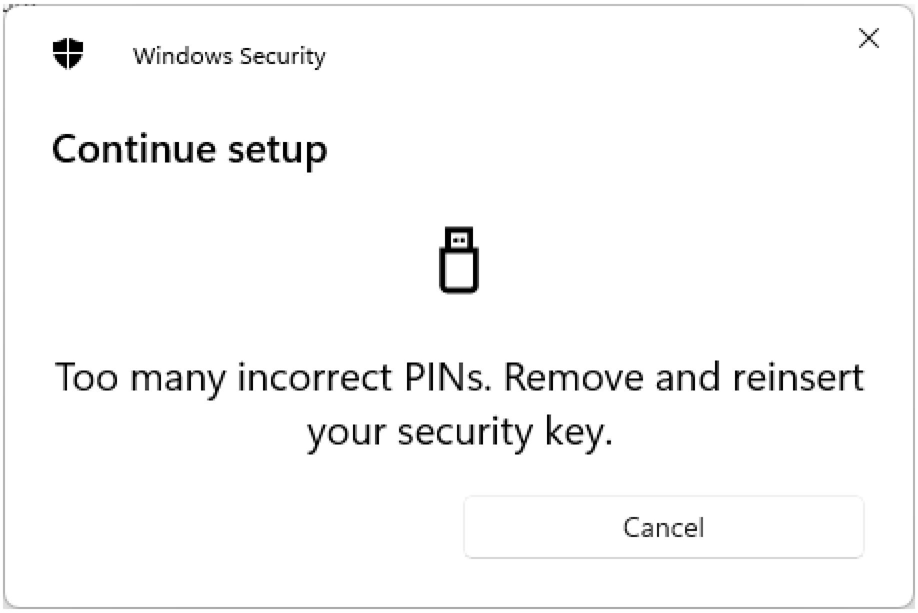
●●●● ③

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

4. Setting Up Security Key in Windows

5) How to Unlock a key [Windows11 Home version 22H2 OS 22621]

1. When the user fails to type the correct PIN four times consecutively, then the below message appears. The User needs to pull out and reinsert the security key and type the correct PIN.



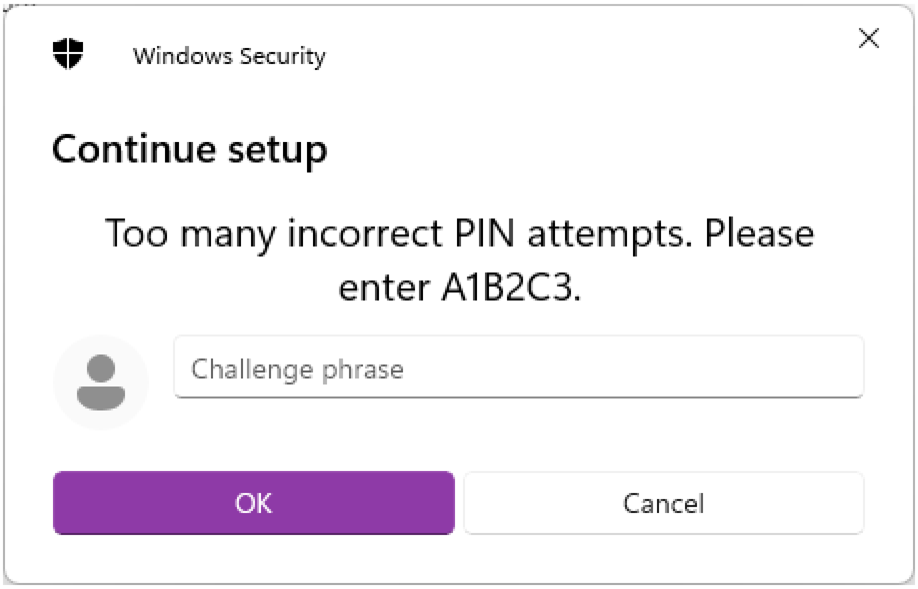
Continue setup

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

4. Setting Up Security Key in Windows

5) How to Unlock a key [Windows11 Home version 22H2 OS 22621]

2. If the user continues to type in incorrect PIN more, the user will get this message.



Windows Security

Continue setup

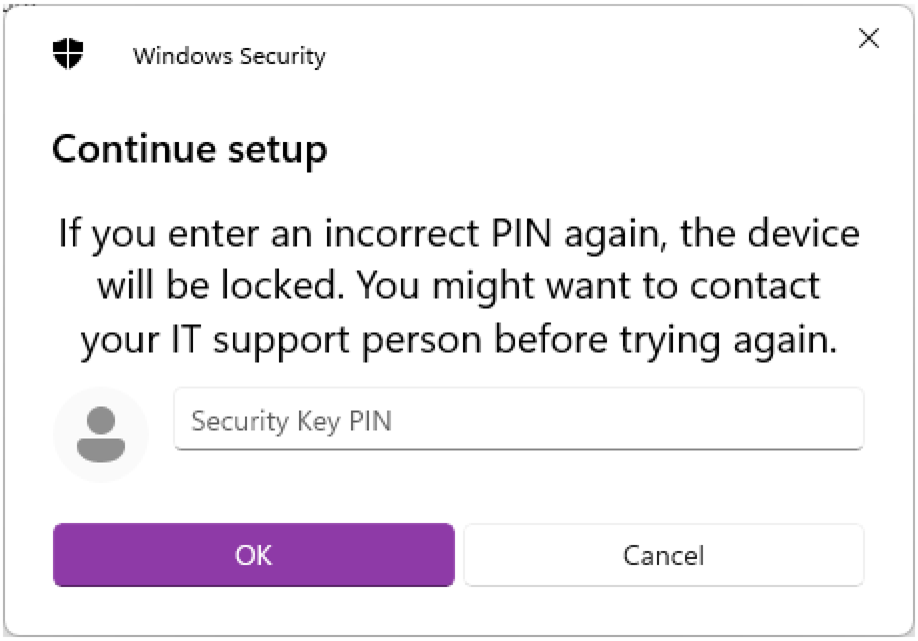
Too many incorrect PIN attempts. Please enter A1B2C3.

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.

4. Setting Up Security Key in Windows

5) How to Unlock a key [Windows11 Home version 22H2 OS 22621]

3. Then, the final warning message pops out.



Windows Security

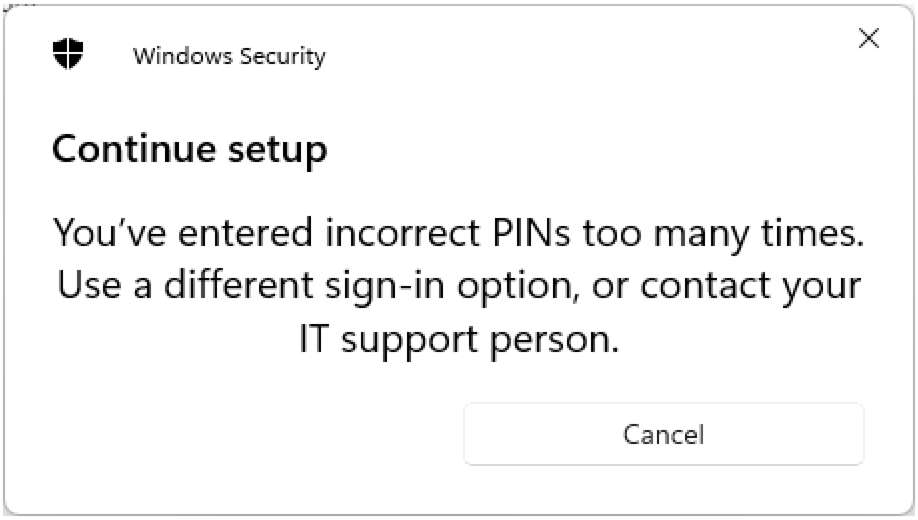
Continue setup

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

4. Setting Up Security Key in Windows

5) How to Unlock a key [Windows11 Home version 22H2 OS 22621]

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



Windows Security

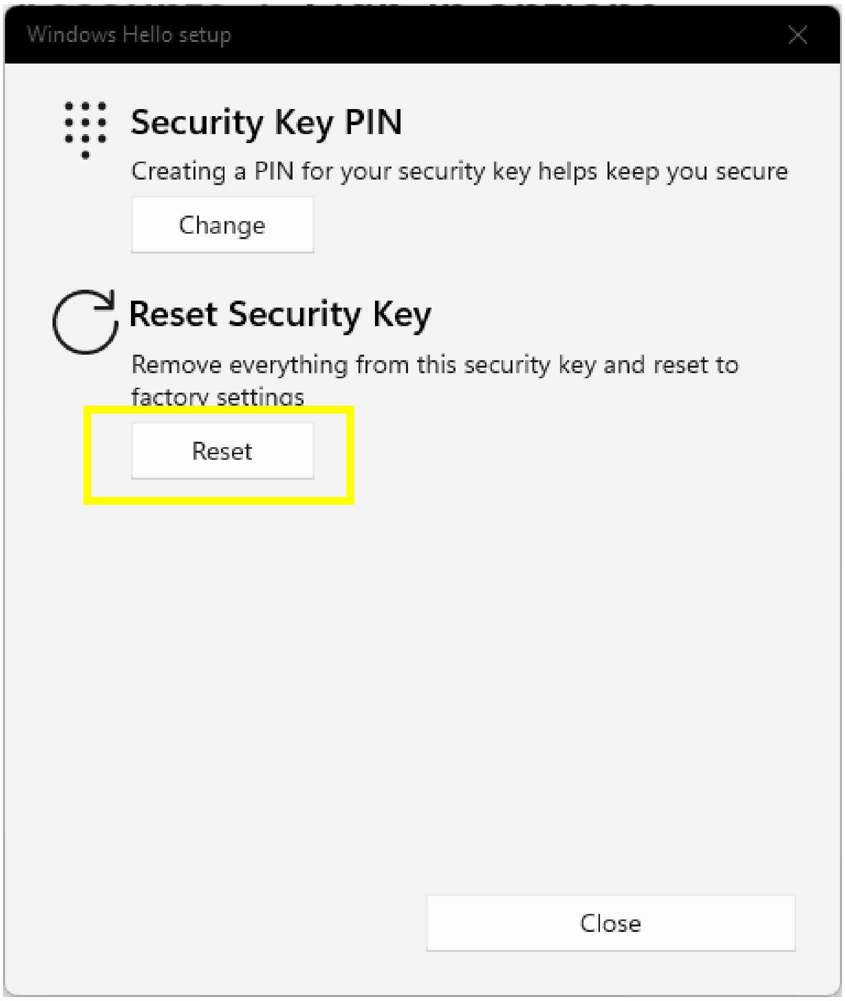
Continue setup

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

4. Setting Up Security Key in Windows

5) How to Unlock a key [Windows11 Home version 22H2 OS 22621]

5. If the security key is fully locked, the following are the steps that you need to take for a factory reset. (page 18~26)
After that, go through the 'Setting up new PIN' process again before using it.(Page 12~17)



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

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.

4. Setting Up Security Key in Windows

6) How to Factory Reset a Key [Windows11 Home version 22H2 OS 22621]

Warning!
A factory reset removes the existing data and all previously created credentials.

The process for '**factory Reset**' and '**deleting a PIN**' is the same.
Go to 17 page to perform a factory reset.

5. Setting Up Security Key in mac OS, Linux

1) macOS, Linux version check

1. Check out the MacOS and Linux versions supported by TrustKey Security Keys below.

Device Platform	Version	Note
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 lat er.

버전 확인 방법

Mac OS : https://support.apple.com/en-us/HT201260

Linux :

①Open [Terminal]

②Enter the following command in [Terminal]

```
cat /etc/*-release
```

③Check the operating system information displayed.

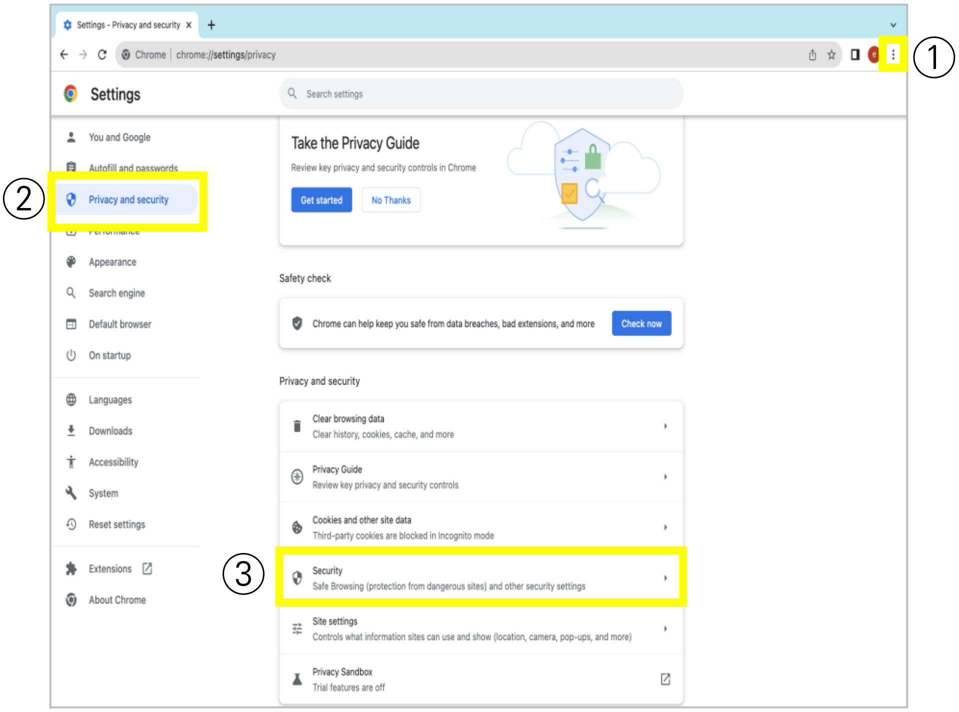
5. Setting Up Security Key in mac OS, Linux

2) Setting up New PIN

Notice!

Registering, changing, and deleting PINs on Mac OS and Linux requires the **Chrome browser**.

1. Using the Chrome browser, sign in your Google Account and ①Press the [**More(⋮)**] button and click **'Settings'** – ②Select [**Privacy and Security**] – ③Select [**Security**]



Take the Privacy Guide

Review key privacy and security controls in Chrome

Chrome can help keep you safe from data breaches, bad extensions, and more

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

Privacy Guide – Review key privacy and security controls

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

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

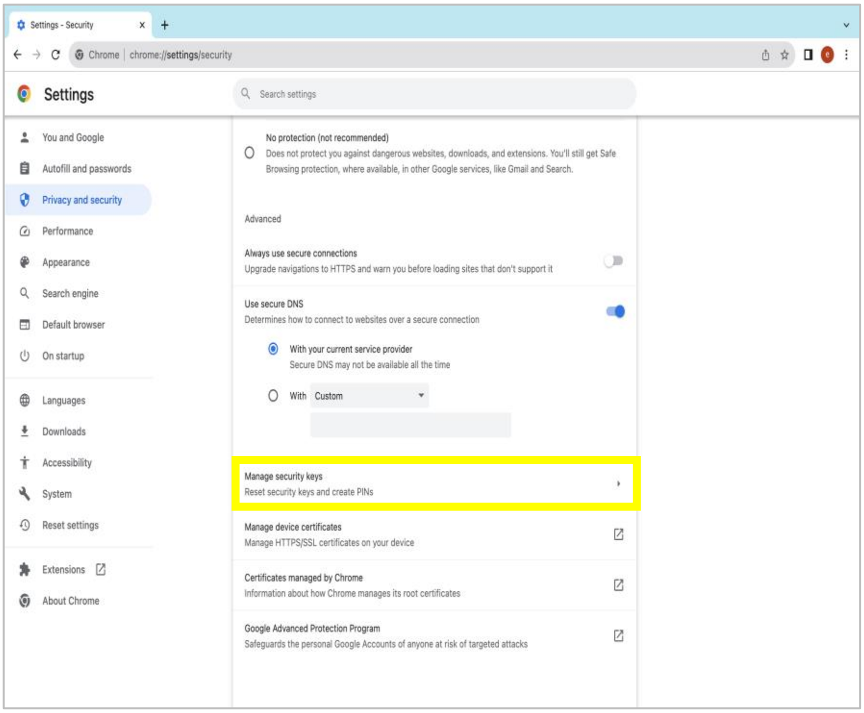
Site settings – Controls what information sites can use and show (location, camera, pop-ups, and more)

Privacy Sandbox – Trial features are off

5. Setting Up Security Key in mac OS, Linux

2) Setting up New PIN

2. Click [**Manage security keys**] in bottom of the page.



○ 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

Always use secure connections
Upgrade navigations to HTTPS and warn you before loading sites that don't support it

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

● With your current service provider
Secure DNS may not be available all the time

○ With Custom

Manage security keys
Reset security keys and create PINs

Manage device certificates
Manage HTTPS/SSL certificates on your device

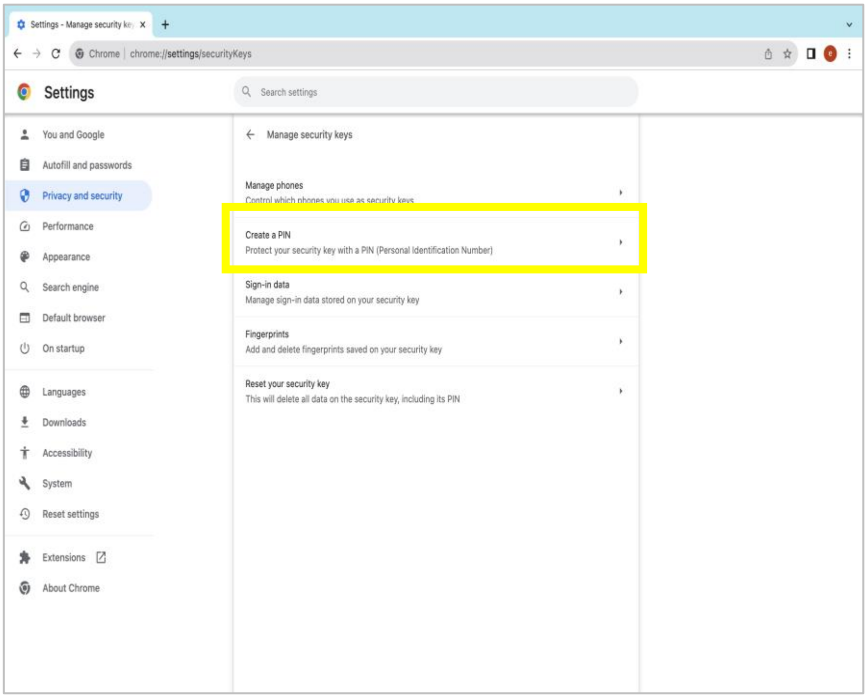
Certificates managed by Chrome
Information about how Chrome manages its root certificates

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

5. Setting Up Security Key in mac OS, Linux

2) Setting up New PIN

3. Choose [**Create a PIN**].



Manage security keys

Manage phones
Control which phones you use as security keys

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

Sign-in data
Manage sign-in data stored on your security key

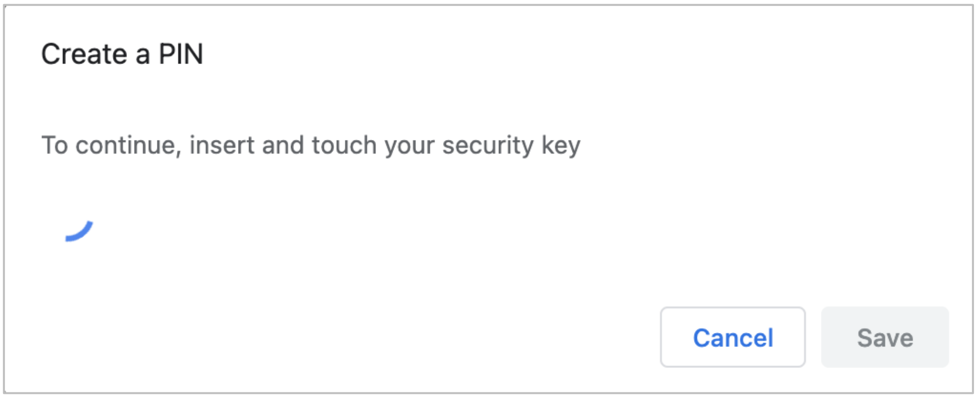
Fingerprints
Add and delete fingerprints saved on your security key

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

5. Setting Up Security Key in mac OS, Linux

2) Setting up New PIN

4. When you insert the T110/T120 into the USB port, the white LED indicator lights up.
At this point, touch the touch sensor on the security key.



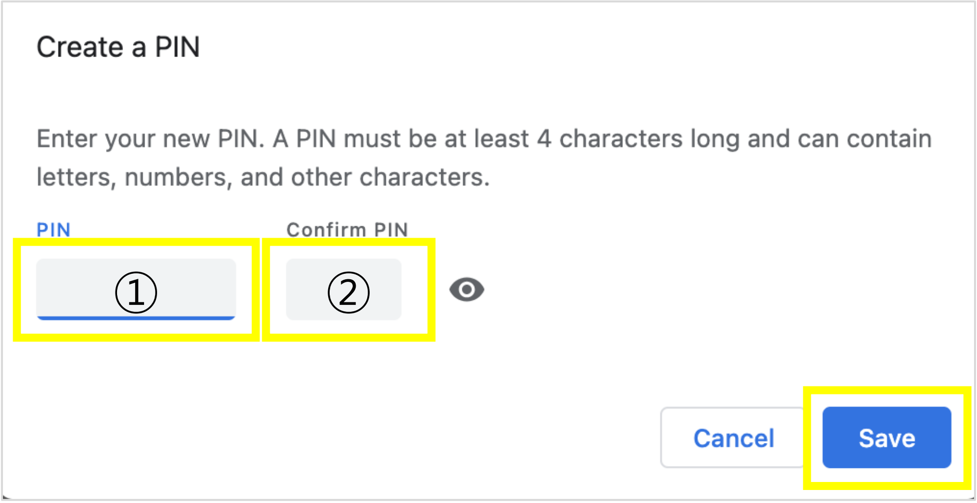
Create a PIN

To continue, insert and touch your security key

5. Setting Up Security Key in mac OS, Linux

2) Setting up New PIN

5. Enter the security key PIN in field ①, and then re-enter the PIN in fields ②. After then click [Save] button to complete the PIN registration.
(A PIN must be at least 4 characters long and can contain letters, numbers, and other characters.)



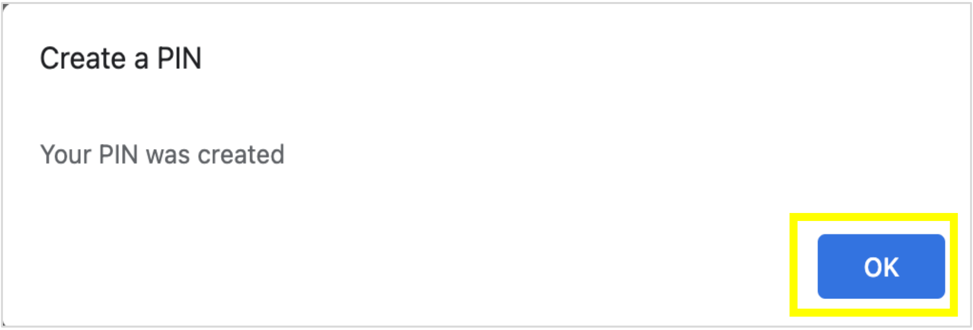
Create a PIN

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

5. Setting Up Security Key in mac OS, Linux

2) Setting up New PIN

6. Click the [OK] button to complete the PIN creation.



Create a PIN

Your PIN was created

5. Setting Up Security Key in mac OS, Linux

3) How to Delete PIN

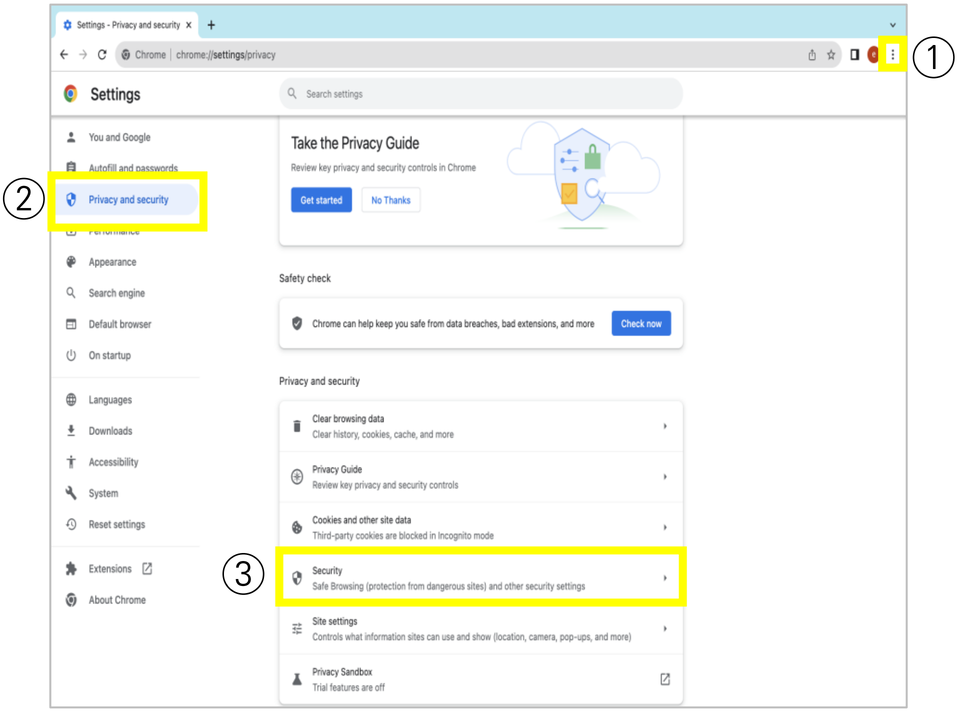
Notice1

The process of deleting a PIN is the same as a factory reset, which means that all data and credentials in the security key are lost.

Notice 2

You must use the Chrome browser to register, change, and delete your PIN on Mac OS and Linux.

1. Using the Chrome browser, sign in your Google Account and ①Press the [**More(⋮)**] button and click **'Settings'** – ②Select [**Privacy and Security**] – ③Select [**Security**]



Take the Privacy Guide

Review key privacy and security controls in Chrome

Safety check

Chrome can help keep you safe from data breaches, bad extensions, and more

Privacy and security

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

Privacy Guide
Review key privacy and security controls

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

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

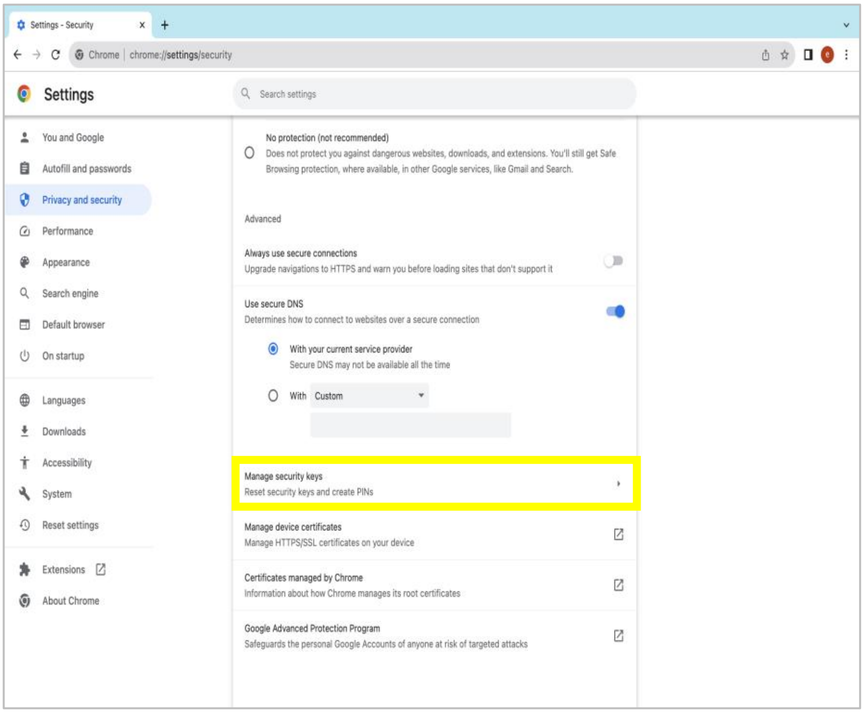
Site settings
Controls what information sites can use and show (location, camera, pop-ups, and more)

Privacy Sandbox
Trial features are off

5. Setting Up Security Key in mac OS, Linux

3) How to Delete PIN

2. Click [**Manage security keys**] in bottom of the page.



○ 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

Always use secure connections
Upgrade navigations to HTTPS and warn you before loading sites that don't support it

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

● With your current service provider
Secure DNS may not be available all the time

○ With Custom

Manage security keys
Reset security keys and create PINs

Manage device certificates
Manage HTTPS/SSL certificates on your device

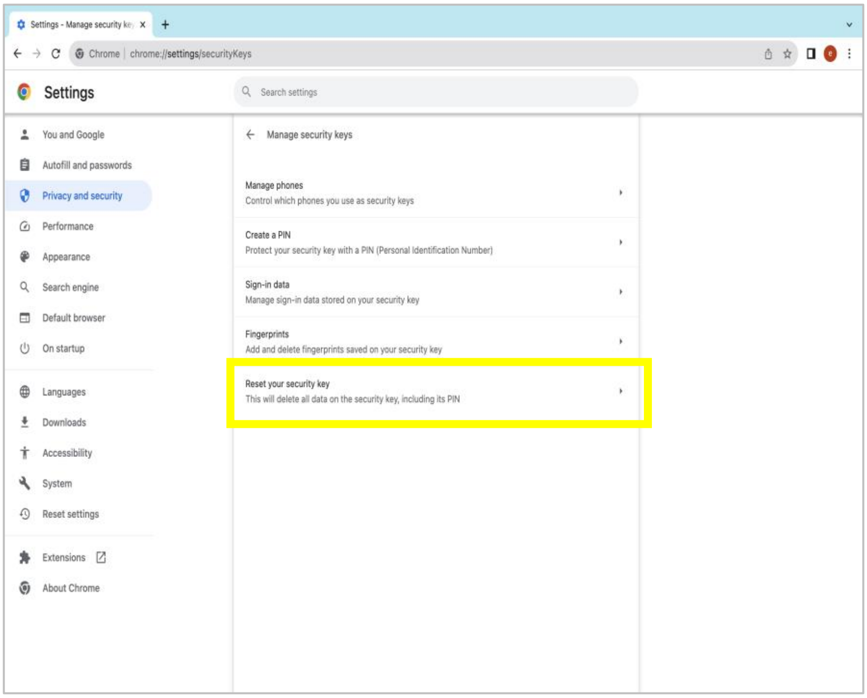
Certificates managed by Chrome
Information about how Chrome manages its root certificates

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

5. Setting Up Security Key in mac OS, Linux

3) How to Delete PIN

3. Choose [Reset your security key].



Manage security keys

Manage phones
Control which phones you use as security keys

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

Sign-in data
Manage sign-in data stored on your security key

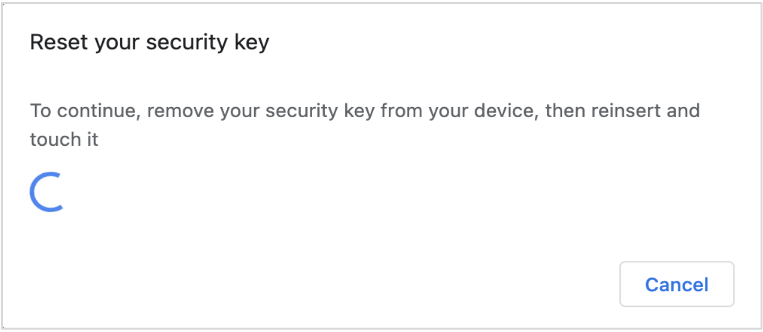
Fingerprints
Add and delete fingerprints saved on your security key

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

5. Setting Up Security Key in mac OS, Linux

3) How to Delete PIN

4. Remove the security key from the USB port, reinsert it, and touch the touch sensor when the white LED flashes.



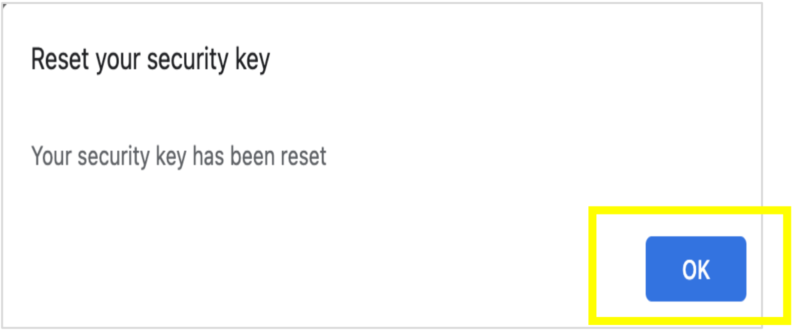
Reset your security key

To continue, remove your security key from your device, then reinsert and touch it

5. Setting Up Security Key in mac OS, Linux

3) How to Delete PIN

5. Click the [OK] button to confirm the deletion of all data stored in the security key.



Reset your security key

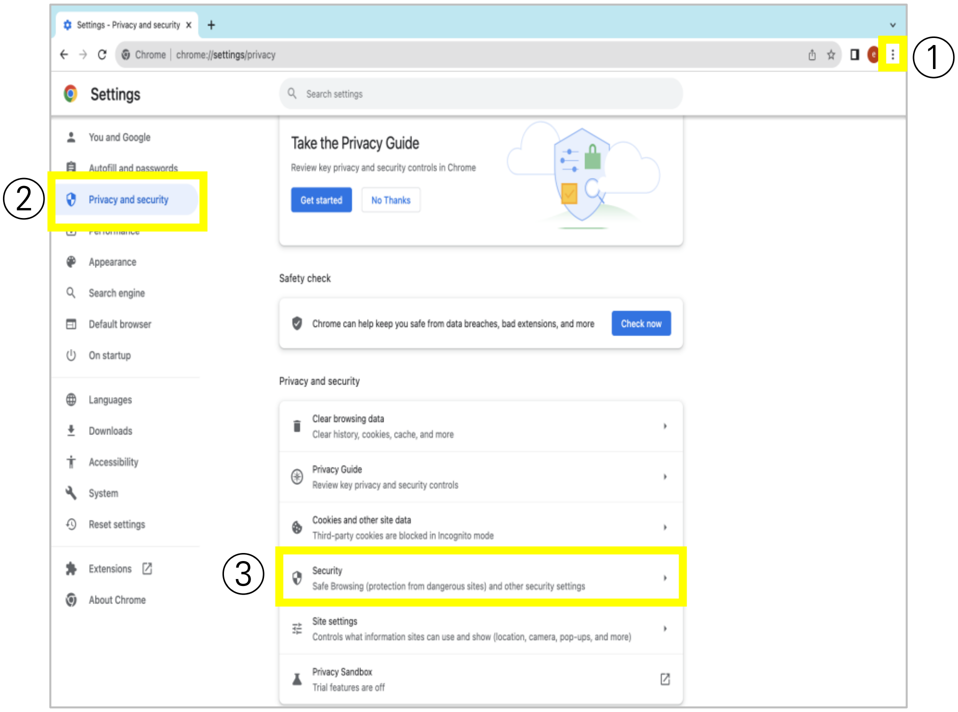
Your security key has been reset

5. Setting Up Security Key in mac OS, Linux

4) How to Change PIN

Notice 1
You must use the Chrome browser to register, change, and delete your PIN on Mac OS and Linux.
Notice 2
You can only change the PIN for security keys that already have a PIN registered.

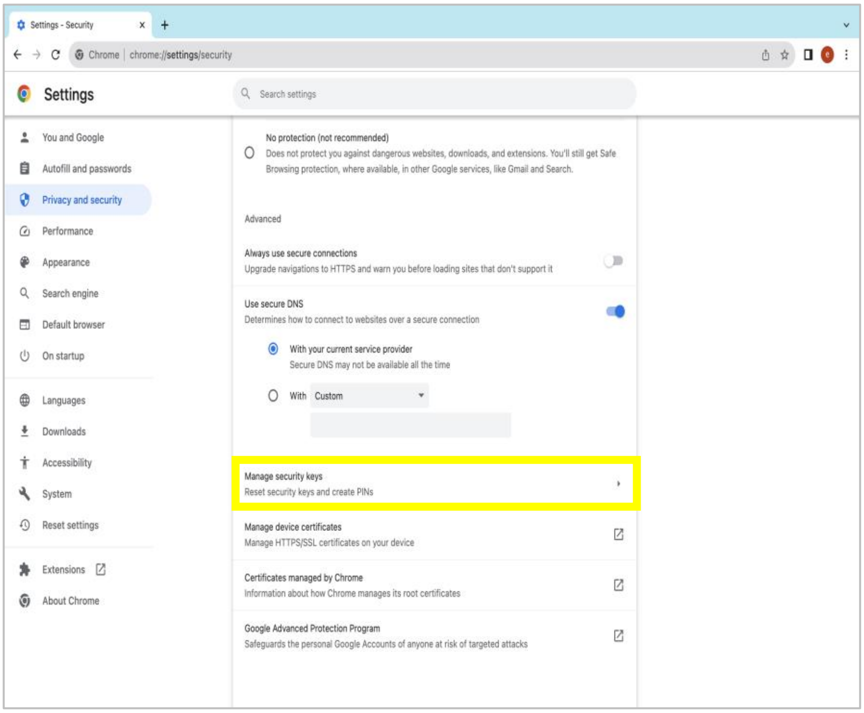
1. Using the Chrome browser, sign in your Google Account and ①Press the [**More(⋮)**] button and click **'Settings'** – ②Select [**Privacy and Security**] – ③Select [**Security**]


Settings - Privacy and security
Chrome | chrome://settings/privacy
①
Settings
Search settings
You and Google
Autofill and passwords
②
Privacy and security
Performance
Appearance
Search engine
Default browser
On startup
Languages
Downloads
Accessibility
System
Reset settings
Extensions
About Chrome
Take the Privacy Guide
Review key privacy and security controls in Chrome
Get started
No Thanks
Safety check
Chrome can help keep you safe from data breaches, bad extensions, and more
Check now
Privacy and security
Clear browsing data
Clear history, cookies, cache, and more
Privacy Guide
Review key privacy and security controls
Cookies and other site data
Third-party cookies are blocked in Incognito mode
③
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 off

5. Setting Up Security Key in mac OS, Linux

4) How to Change PIN

2. Click [**Manage security keys**] in bottom of the page.



○ 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

Always use secure connections
Upgrade navigations to HTTPS and warn you before loading sites that don't support it

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

● With your current service provider
Secure DNS may not be available all the time

○ With Custom

Manage security keys
Reset security keys and create PINs

Manage device certificates
Manage HTTPS/SSL certificates on your device

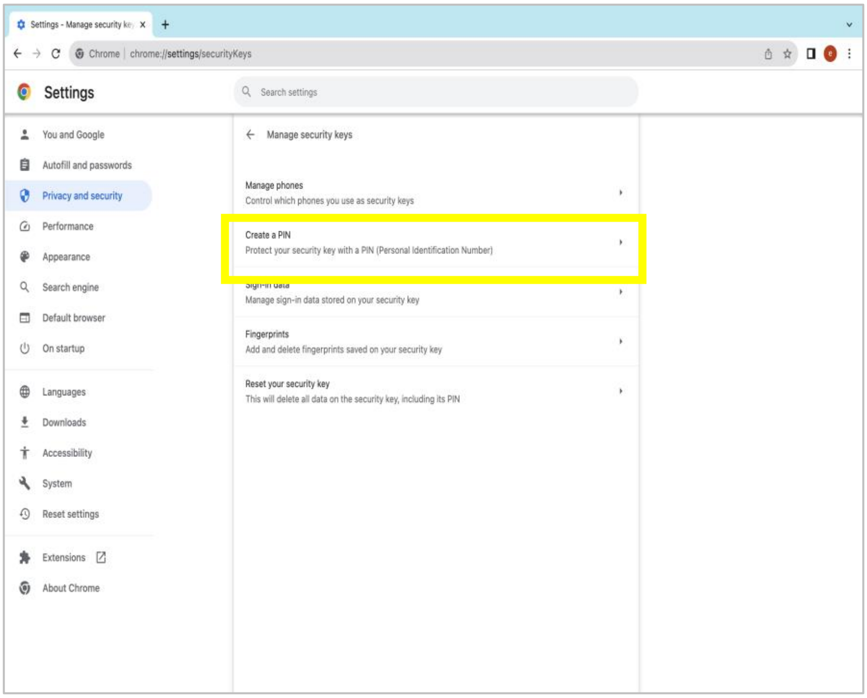
Certificates managed by Chrome
Information about how Chrome manages its root certificates

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

5. Setting Up Security Key in mac OS, Linux

4) How to Change PIN

3. Choose [**Create a PIN**].



Manage security keys

Manage phones
Control which phones you use as security keys

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

Sign-in data
Manage sign-in data stored on your security key

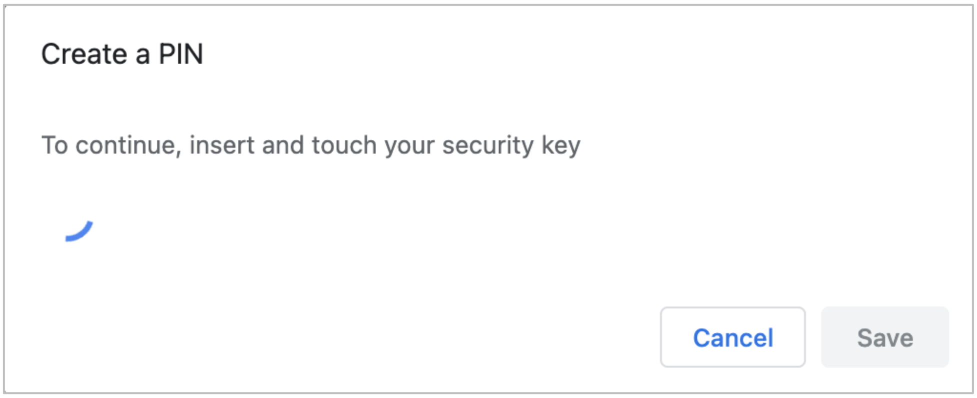
Fingerprints
Add and delete fingerprints saved on your security key

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

5. Setting Up Security Key in mac OS, Linux

4) How to Change PIN

4. When you insert the T110/T120 into the USB port, the white LED indicator lights up.
At this point, touch the touch sensor on the security key.



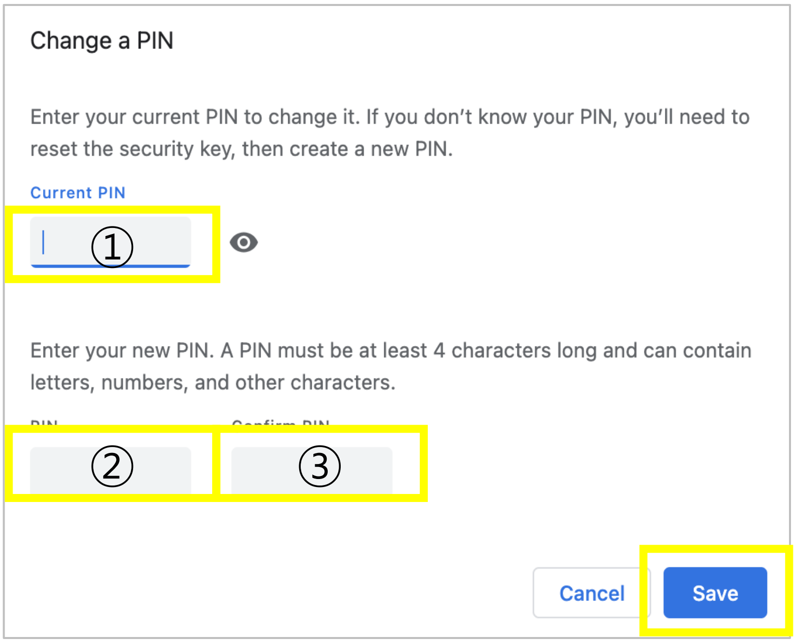
Create a PIN

To continue, insert and touch your security key

5. Setting Up Security Key in mac OS, Linux

4) How to Change PIN

5. Enter the security key PIN in field ①, and then enter the new security key PIN in fields ② and ③ below, and click the [**Save**] button to complete the 'Change your security key PIN'



Change a PIN

Enter your current PIN to change it. If you don't know your PIN, you'll need to reset the security key, then create a new PIN.

Current PIN

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

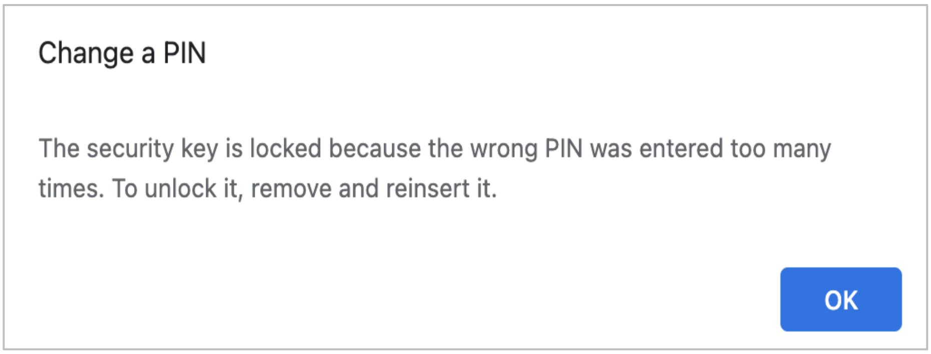
PIN

Confirm PIN

5. Setting Up Security Key in mac OS, Linux

5) How to Unlock a Key

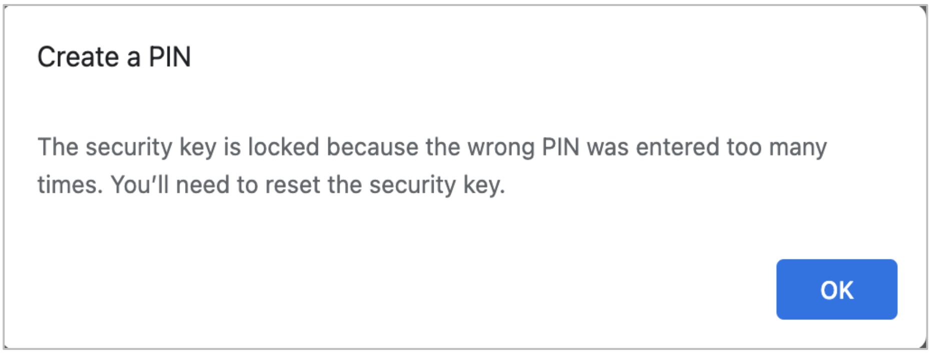
1. When the user fails to type the correct PIN four times consecutively, then the below message appears. The User needs to pull out and reinsert the security key and type the correct PIN.



Change a PIN

The security key is locked because the wrong PIN was entered too many times. To unlock it, remove and reinsert it.

2. If the user types the incorrect PIN for the last time, the security key is locked. If the security key is completely locked, press the [OK] button to return to the previous step.



Create a PIN

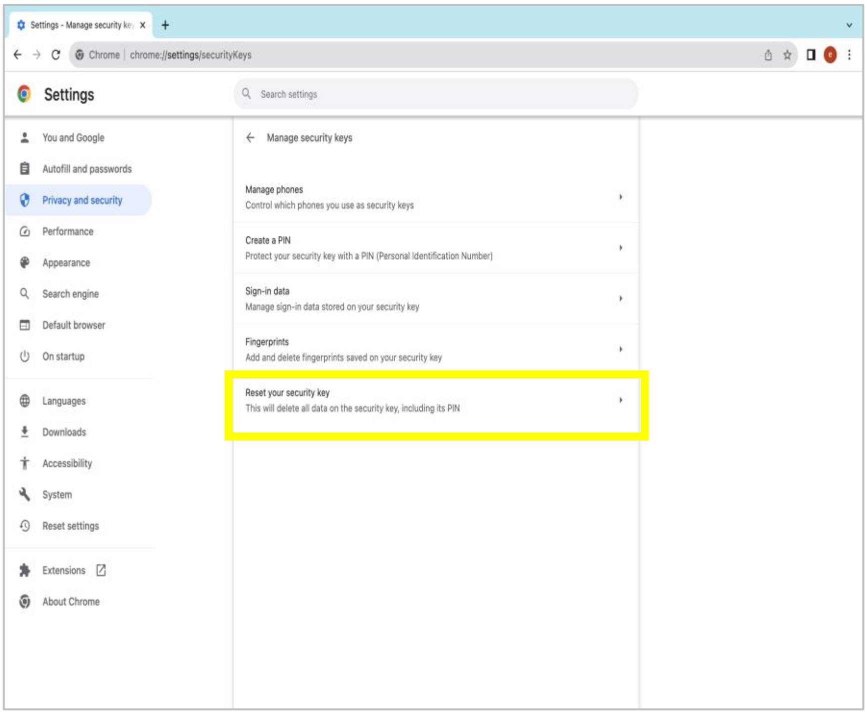
The security key is locked because the wrong PIN was entered too many times. You'll need to reset the security key.

5. Setting Up Security Key in mac OS, Linux

5) How to Unlock a Key

4. Click [**Reset your security key**] to initialize the security key, and then proceed with the security key PIN registration process.

(Reset your security key: page 44, Create a PIN : page 38)



Manage security keys

Manage phones
Control which phones you use as security keys

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

Sign-in data
Manage 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

5. Setting Up Security Key in mac OS, Linux

6) How to Factory Reset a Key

Warning!
A factory reset removes the existing data and all previously created credentials.

The process for '**Factory Reset**' and '**Deleting a PIN**' is the same.
Go to 44 page to perform a factory reset.

6. Setting up Security key in Key Manager at Windows

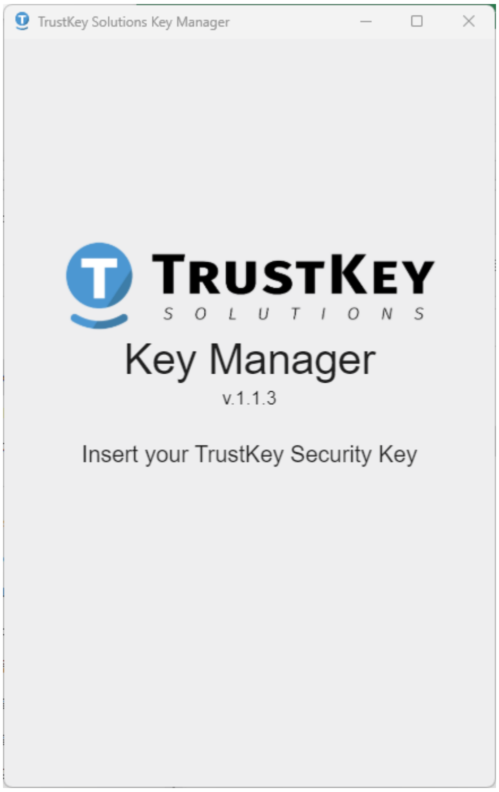
1) Install the Key Manager

*Key Manager is a program to manage PIN for security key as well as registering/managing OTP features of the security key.

1. Make sure that KeyManager™ application is download on your PC.
   Please download the correct version for your OS. For Windows, you can download the file (version 1.1.3)

- file name : Key Manager 1.1.1 Setup (Win)

https://trustkey.kr/sub/support.form



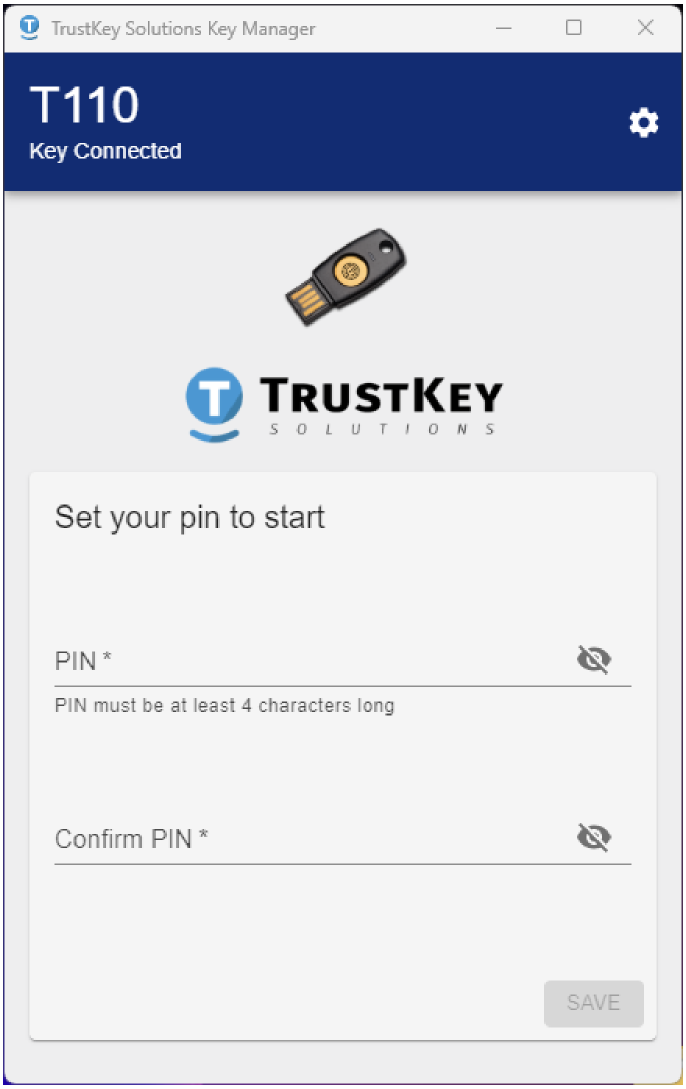
Insert your TrustKey Security Key

6. Setting up Security key in Key Manager at Windows

2) Setting up New PIN

1. Launch KeyManager program and insert T110/T120 into a USB port.

2. Enter PIN and confirm PIN.
   - PIN must be at least four (4) characters long.
   - PIN can be digits, characters, and mixture of them.



Set your pin to start

PIN *

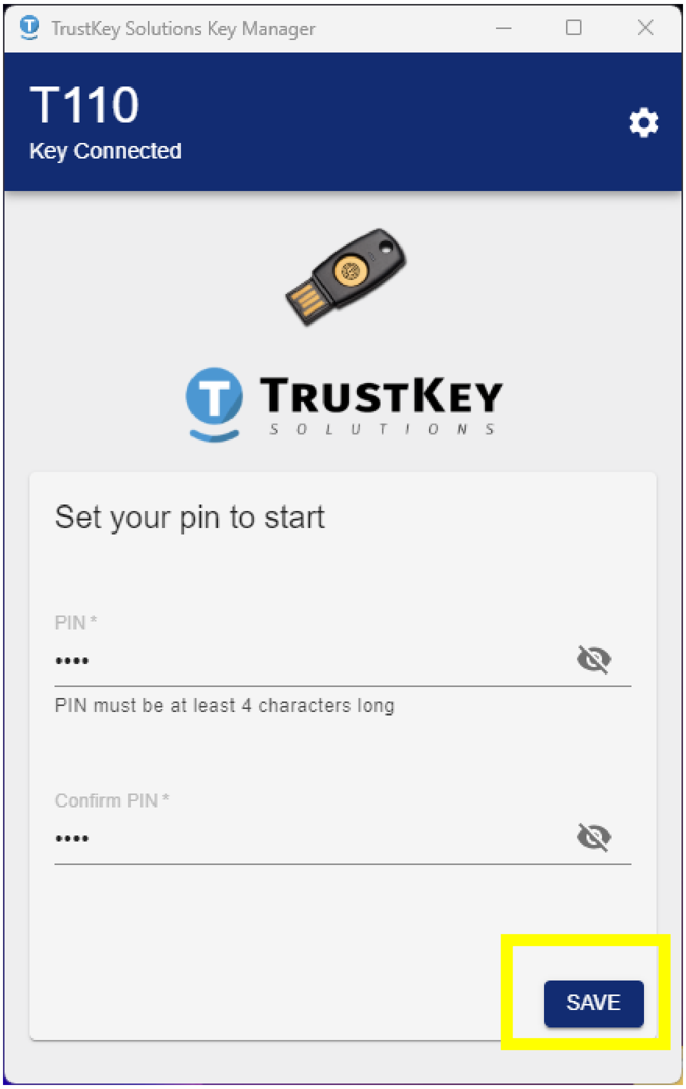
PIN must be at least 4 characters long

Confirm PIN *

6. Setting up Security key in Key Manager at Windows

2) Setting up New PIN

3. Click [SAVE] button.



TrustKey Solutions Key Manager

T110

Key Connected

Set your pin to start

PIN *

••••

PIN must be at least 4 characters long

Confirm PIN *

••••

6. Setting up Security key in Key Manager at Windows

3) How to Delete PIN

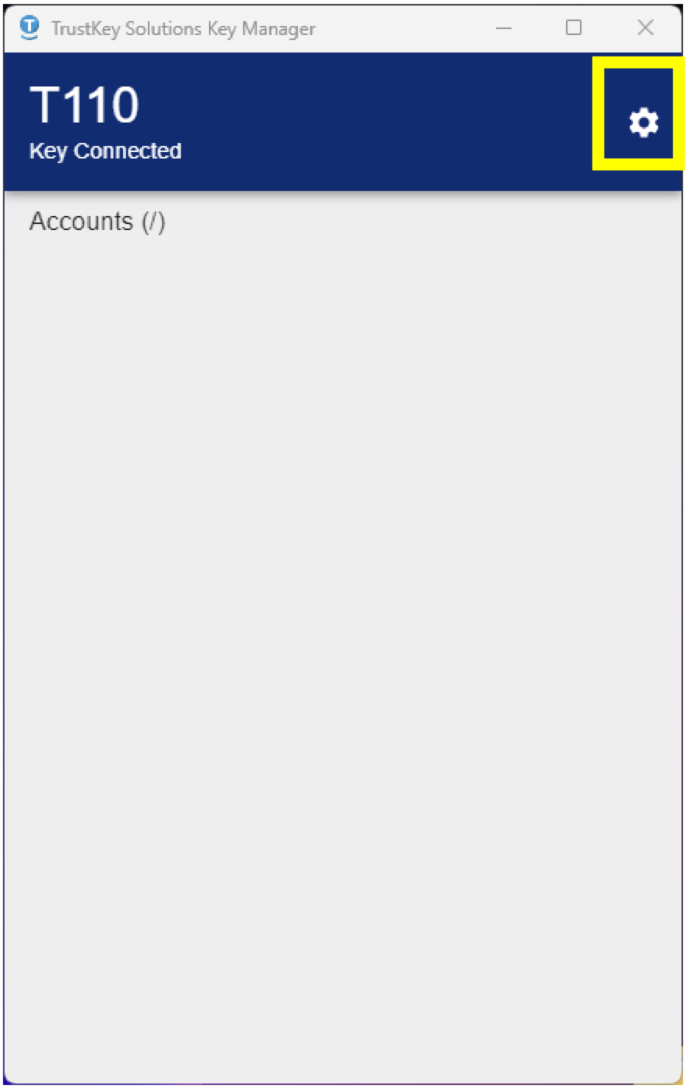
‘Deleting a PIN’ using Key Manager is the same process as the ‘factory reset’.
Go to 66 Page to perform a factory reset.

Note that the factory reset will NOT erase TOTP/HOTP accounts. Please remove all OTP accounts before the factory reset.

6. Setting up Security key in Key Manager at Windows

3) How to Change PIN

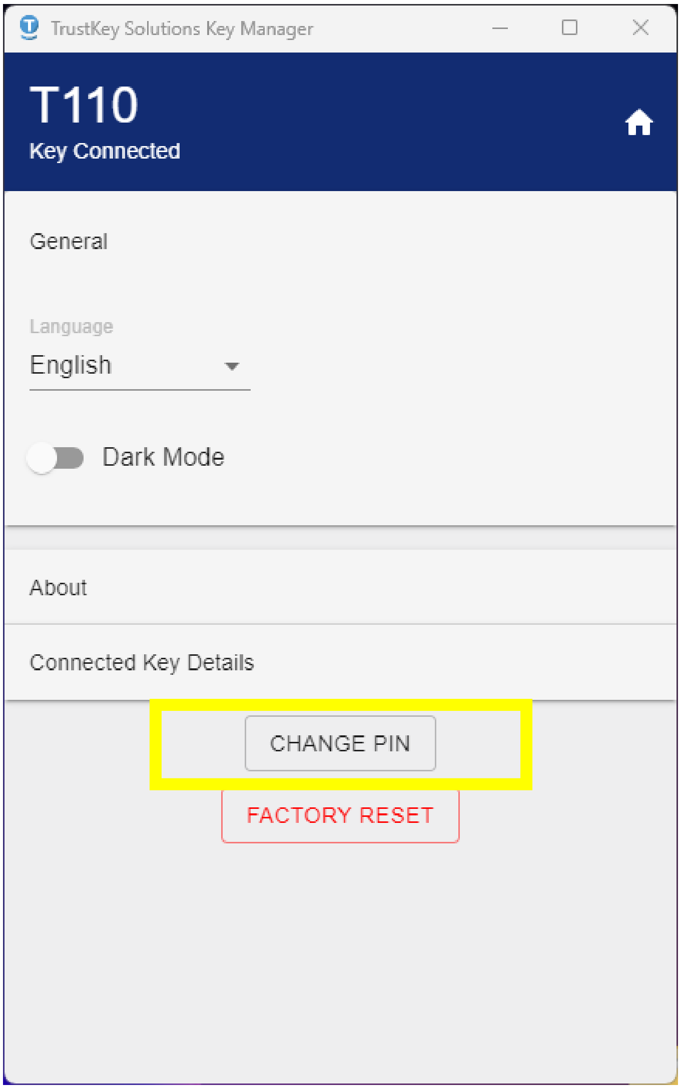
1. Click **[⚙] setup** button.



6. Setting up Security key in Key Manager at Windows

3) How to Change PIN

2. Click [CHANGE PIN] button.



TrustKey Solutions Key Manager

T110

Key Connected

General

Language

English

Dark Mode

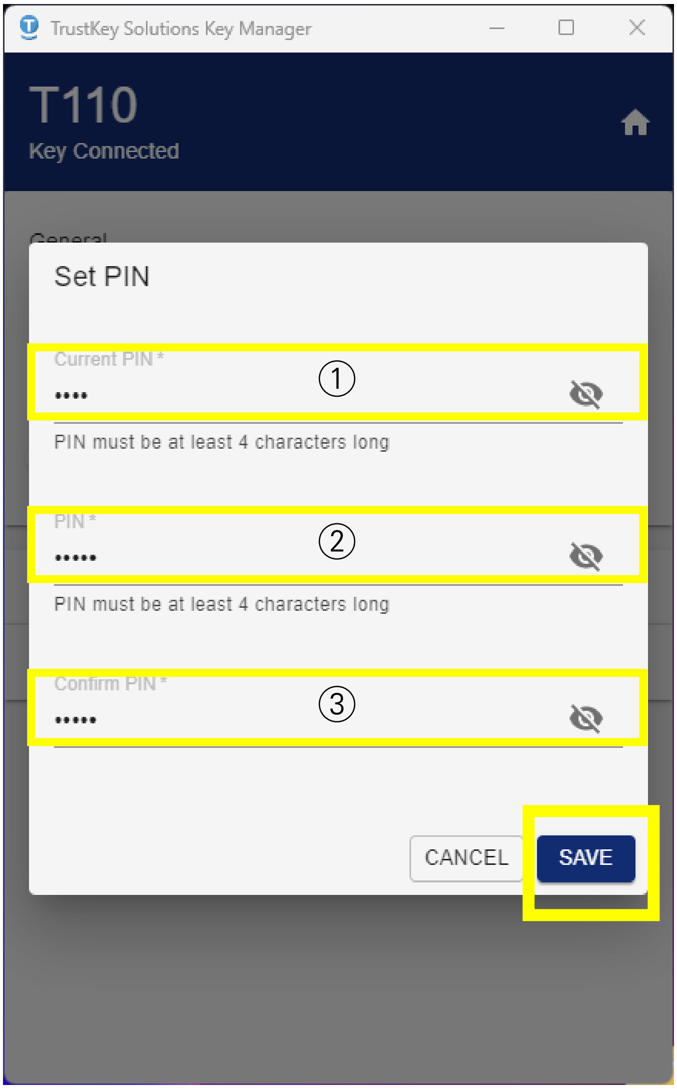
About

Connected Key Details

6. Setting up Security key in Key Manager at Windows

3) How to Change PIN

3. Enter the ① Current PIN, ② PIN (New PIN), ③ Confirm PIN. After then, click [SAVE] button.



Current PIN *: ••••

PIN must be at least 4 characters long

PIN *: •••••

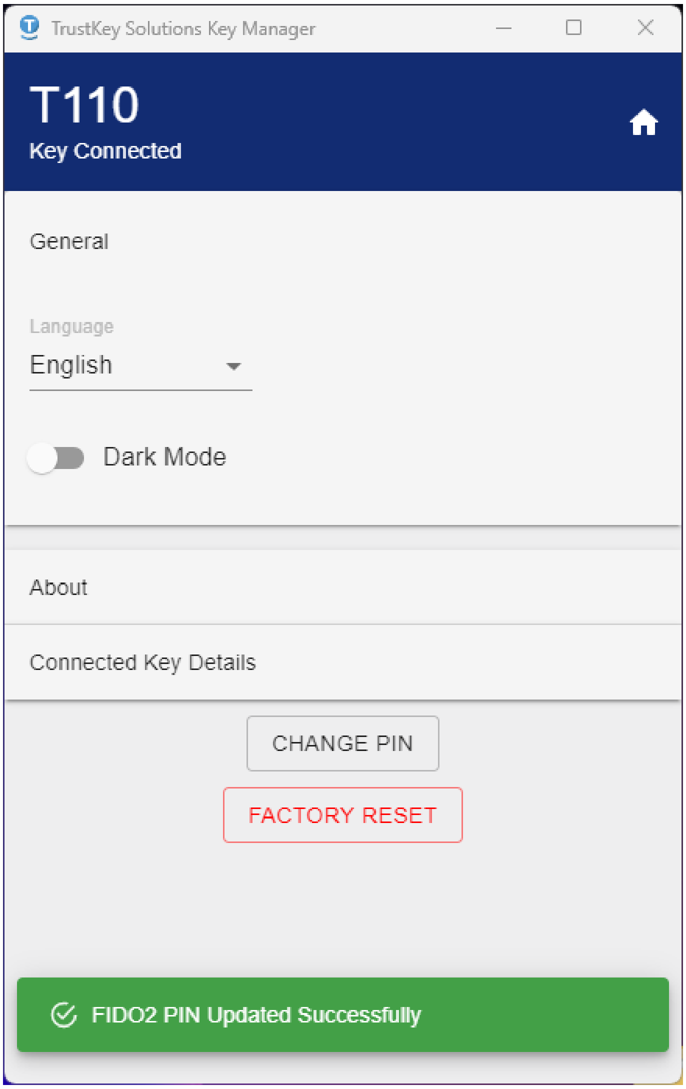
PIN must be at least 4 characters long

Confirm PIN *: •••••

6. Setting up Security key in Key Manager at Windows

3) How to Change PIN

4. You have updated PIN for the security key.

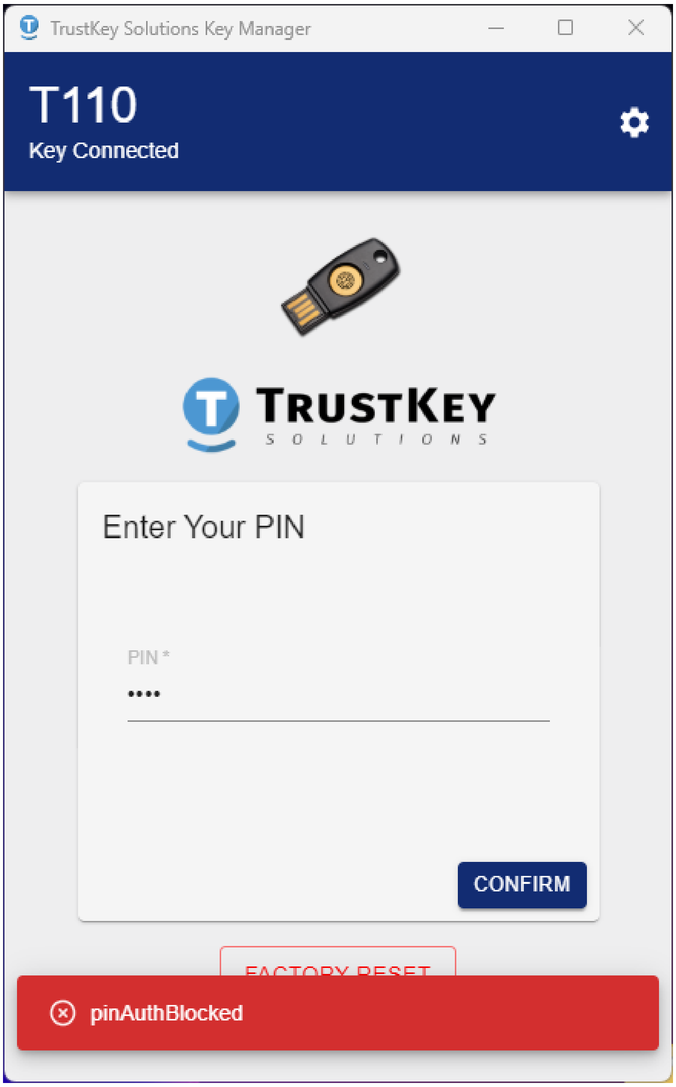


FIDO2 PIN Updated Successfully

6. Setting up Security key in Key Manager at Windows

4) How to Unlock a Key

1. If you enter the wrong PIN **three times** in a row, you will receive a warning message as shown below and the security key will be completely locked. In this case, go to the 66 page to perform a factory reset and proceed with the PIN registration process.



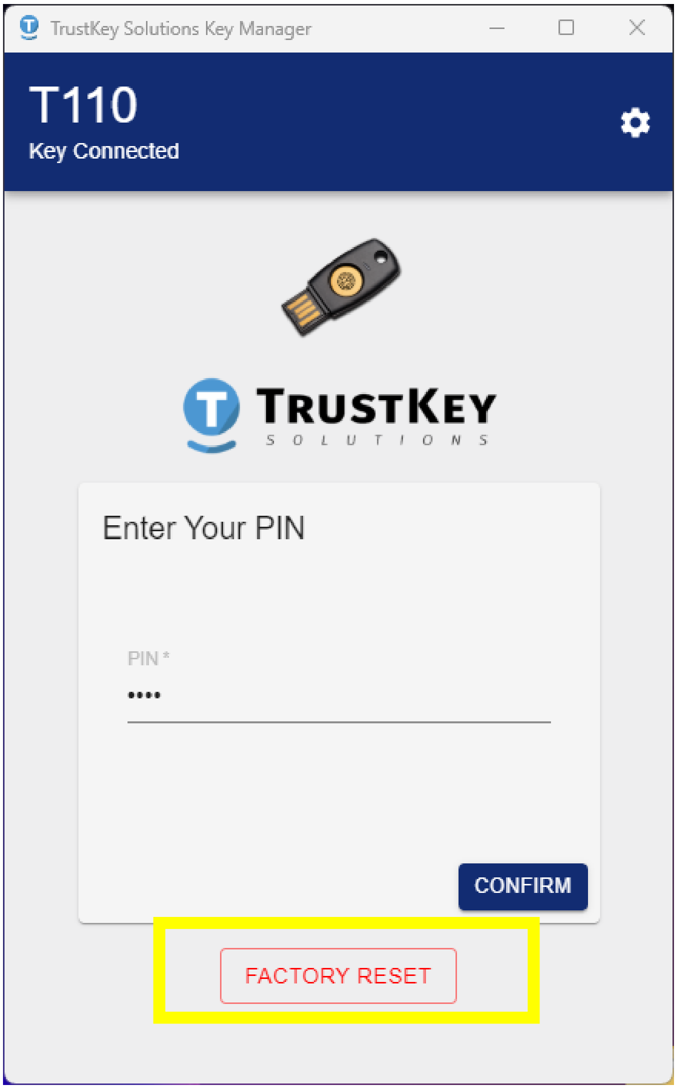
pinAuthBlocked

6. Setting up Security key in Key Manager at Windows

6) How to Factory Reset a Key

1. Click [FACTORY RESET].

This will reset 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.



Enter Your PIN

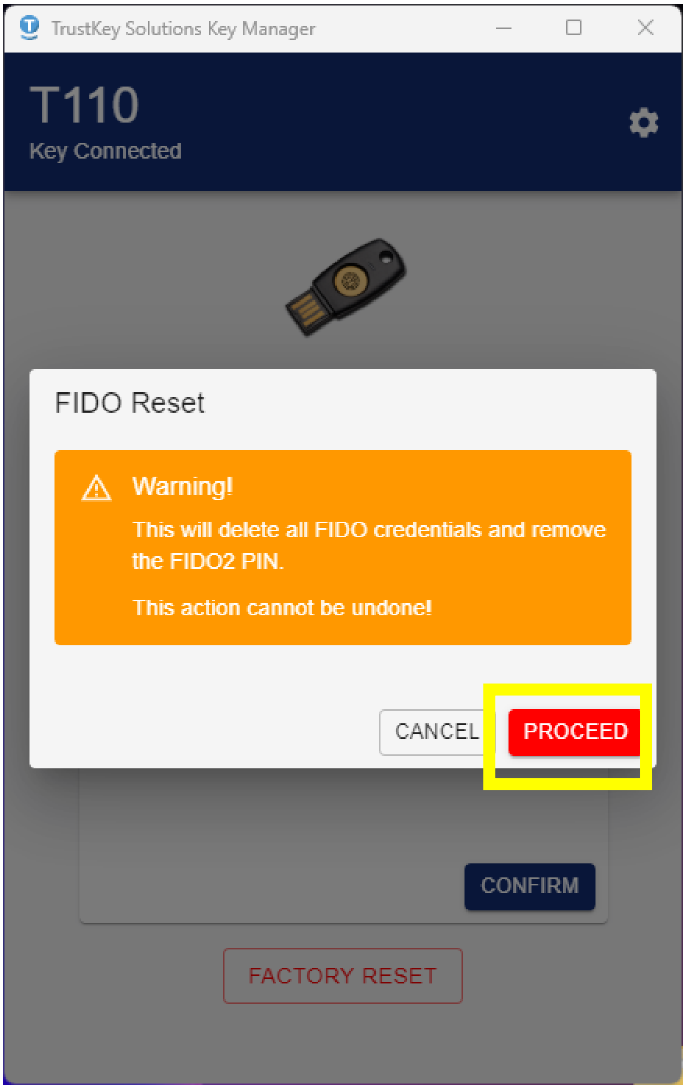
PIN *

••••

6. Setting up Security key in Key Manager at Windows

6) How to Factory Reset a Key

2. Click [PROCEED] button.



FIDO Reset

⚠ Warning!

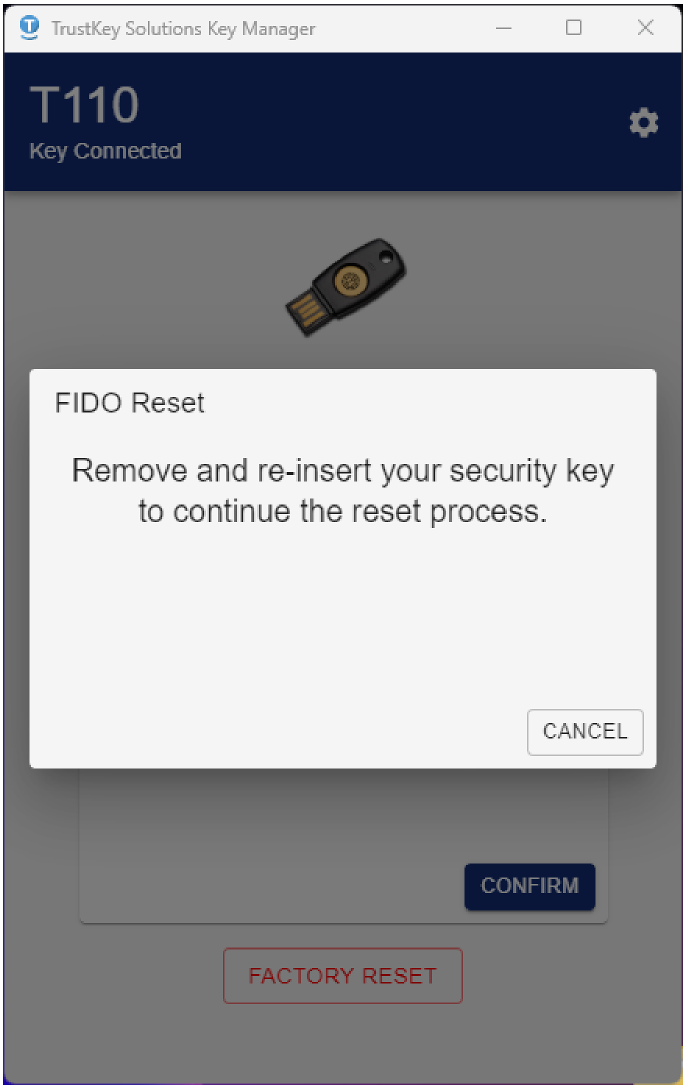
This will delete all FIDO credentials and remove the FIDO2 PIN.

This action cannot be undone!

6. Setting up Security key in Key Manager at Windows

6) How to Factory Reset a Key

3. Remove your security key from USB port.

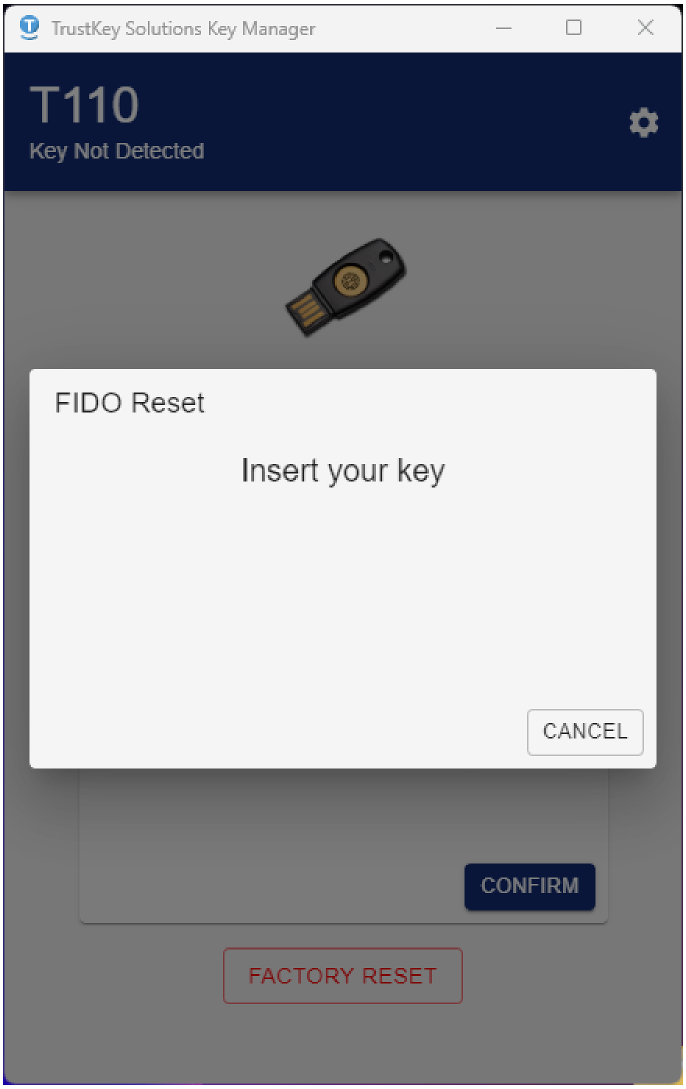


Remove and re-insert your security key to continue the reset process.

6. Setting up Security key in Key Manager at Windows

6) How to Factory Reset a Key

4. Reinsert the security key.



TrustKey Solutions Key Manager

T110

Key Not Detected

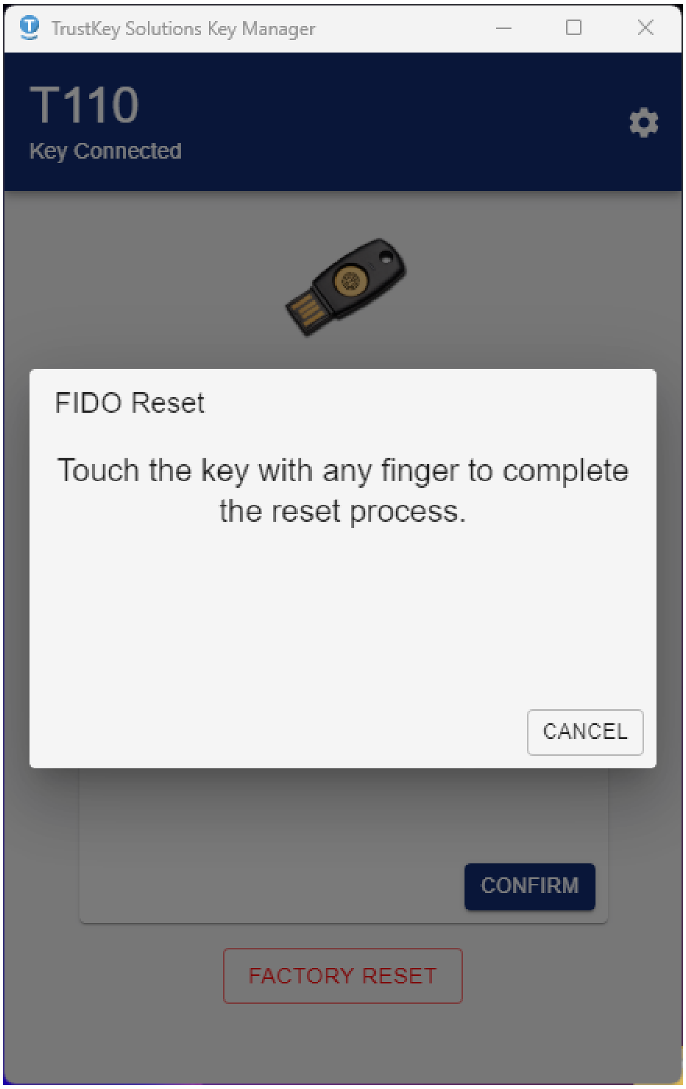
FIDO Reset

Insert your key

6. Setting up Security key in Key Manager at Windows

6) How to Factory Reset a Key

5. Touch the sensor to complete the reset process.



FIDO Reset

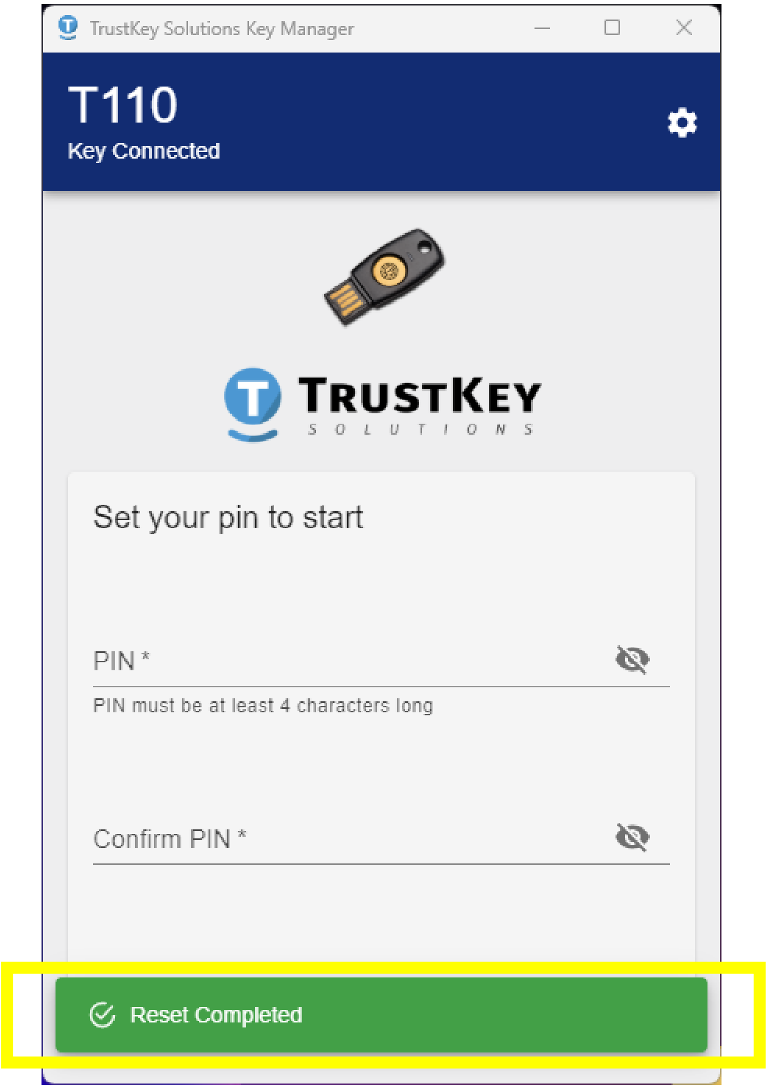
Touch the key with any finger to complete the reset process.

Note:
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.

6. Setting up Security key in Key Manager at Windows

6) How to Factory Reset a Key

5. You have reset security key to factory settings.



T110

Key Connected

Set your pin to start

PIN *

PIN must be at least 4 characters long

Confirm PIN *

Reset Completed

6. Setting up Security key in Key Manager at Windows

OTP (One Time Password) is a user authentication method that uses randomly generated, one-time passwords.
It was introduced to overcome security vulnerabilities caused by repeatedly using the same password by generating a one-time password for each login.

TrustKey FIDO security key 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.

- TOTP (Time based One Time Password)

A time-based, OTP that allows you to authenticate with a password that is valid for a period of time, typically 30 or 60 seconds. It's used by many hardware devices, including GitHub, Google, and Microsoft's Authenticator app, and you can use T110/T120 to generate TOTP passwords through Key Manager.

- HOTP (HMAC based One Time Password)

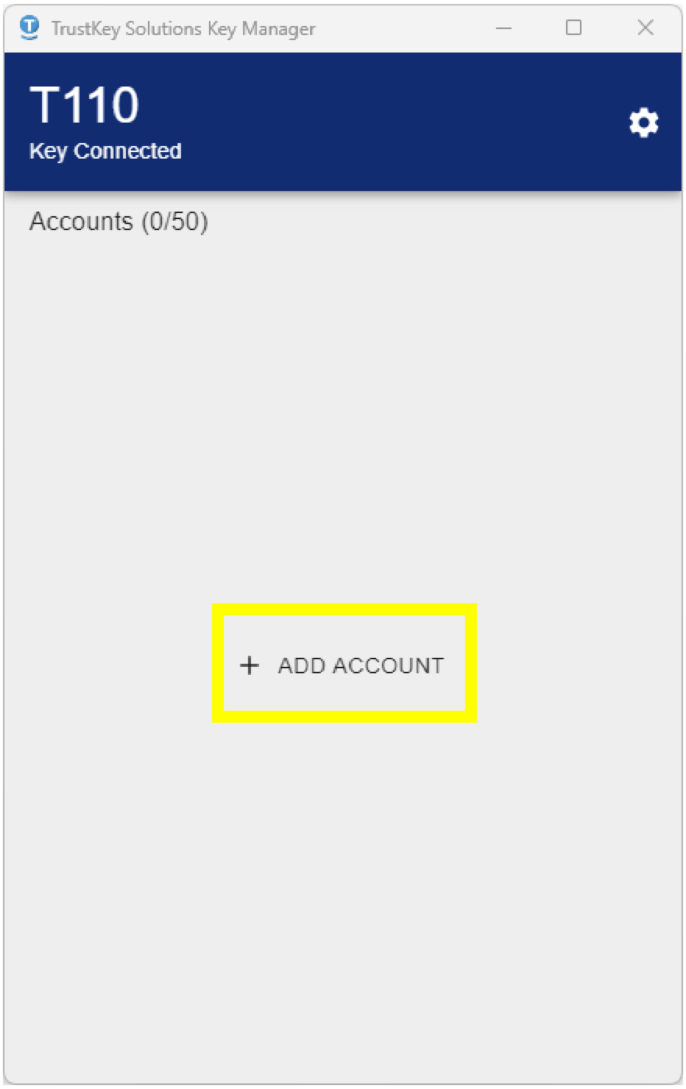
This method allows you to authenticate using a counter-based one-time password generated from a security key. T110/T120 can authenticate and log in to accounts set up with short touch and long touch without using Key Manager.

6. Setting up Security key in Key Manager at Windows

7) Using the TOTP Security Key

① Setting up TOTP accounts using QR scan (GitHub example)

1. Open Key Manager and Click [+ADD ACCOUNT]



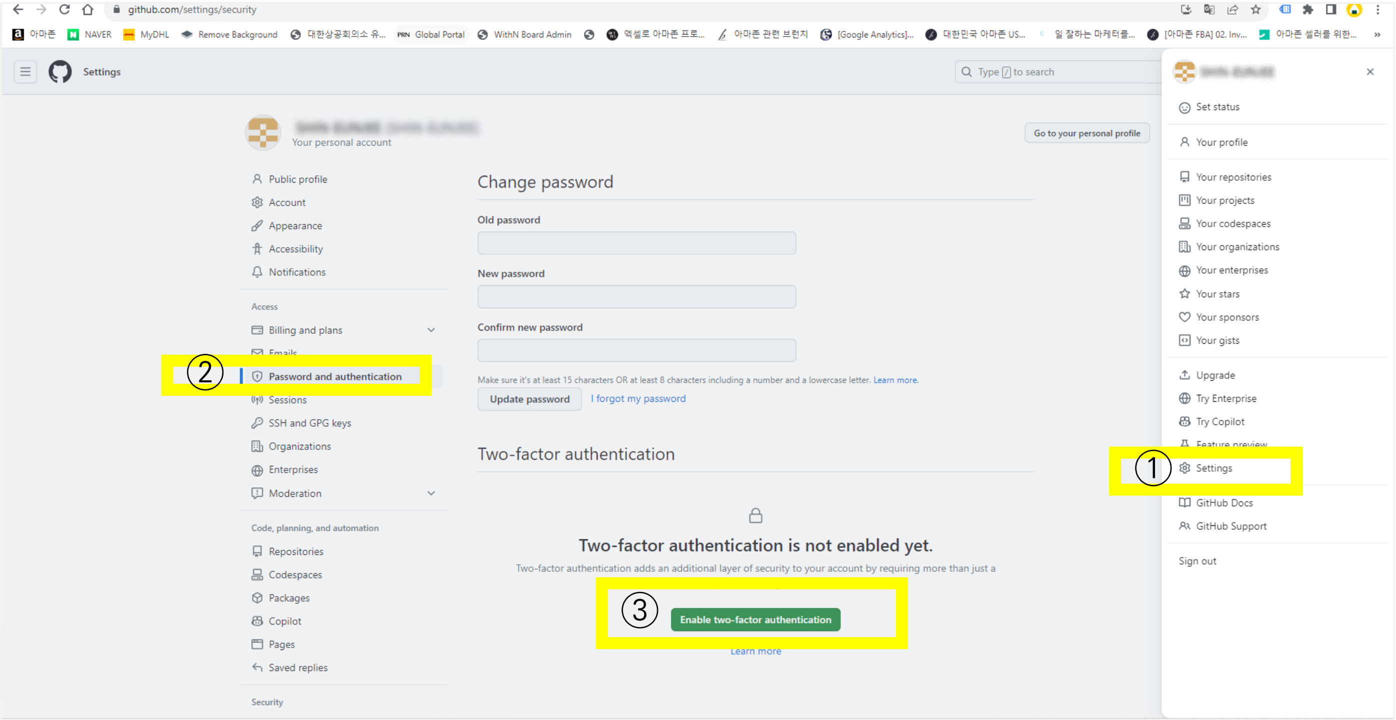
* A GitHub account setup example is given here. The method of setup may be different on other websites.

6. Setting up Security key in Key Manager at Windows

7) Using the TOTP Security Key

① Setting up TOTP accounts using QR scan (GitHub example)

2. After signing in with your ID/PW on GitHub, go to **Settings**(①) – **Password and authentication**(②) – click **Enable two-factor authentication**(③).



github.com/settings/security

Settings

[redacted]
Your personal account

Go to your personal profile

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.

Update password I forgot my password

Two-factor authentication

Two-factor authentication is not enabled yet.

Two-factor authentication adds an additional layer of security to your account by requiring more than just a

Enable two-factor authentication

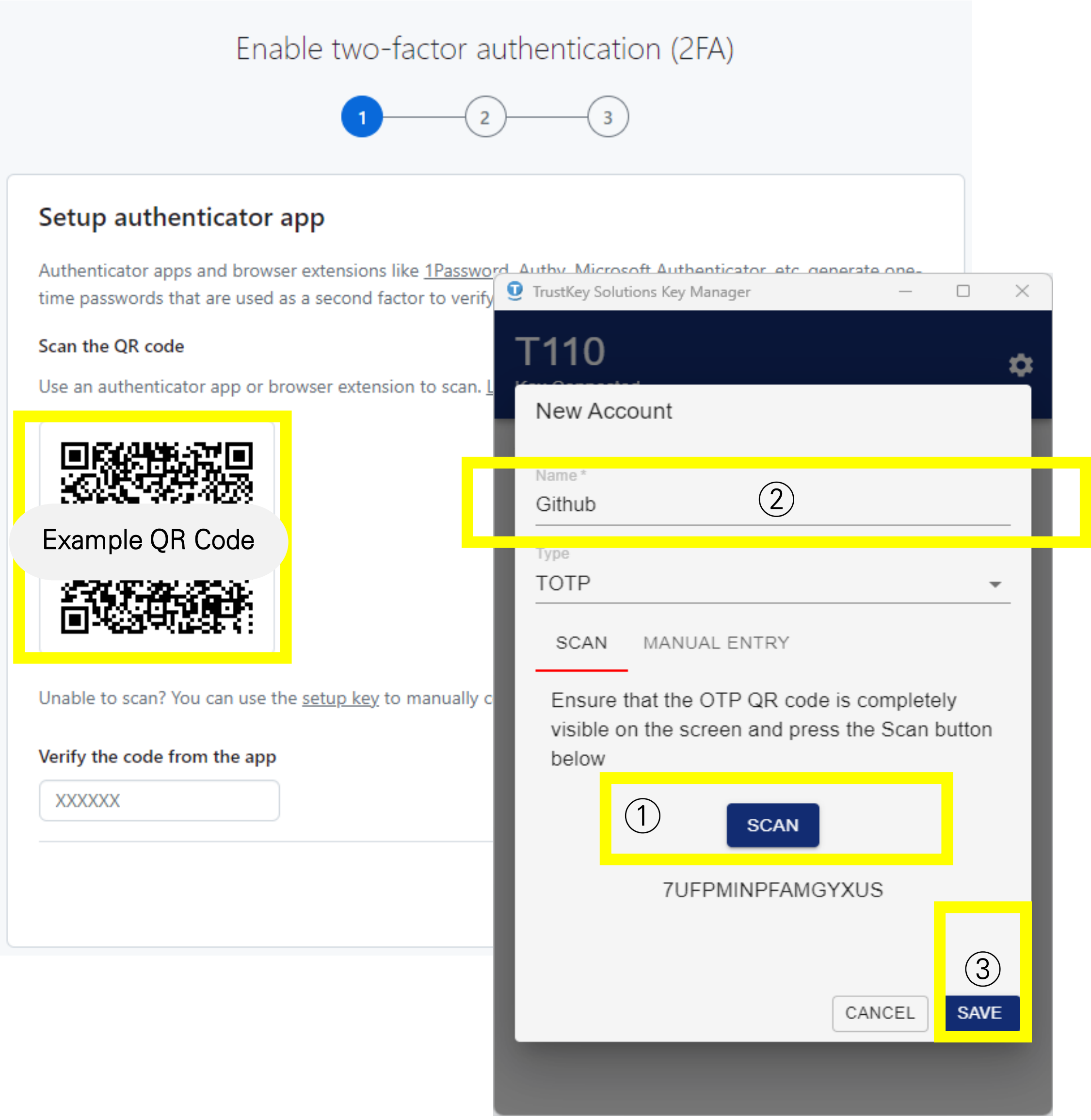
Learn more

6. Setting up Security key in Key Manager at Windows

7) Using the TOTP Security Key

① Setting up TOTP accounts using QR scan (GitHub example)

3. Once the authentication QR code is generated, click the ①[SCAN] button in Key Manager to scan the QR code. Then set a ②Name and click ③[SAVE] button to register a TOTP account on GitHub.



Enable two-factor authentication (2FA)

Setup authenticator app

Authenticator apps and browser extensions like 1Password, Authy, Microsoft Authenticator, etc. generate one-time passwords that are used as a second factor to verify

Scan the QR code

Use an authenticator app or browser extension to scan. L

Unable to scan? You can use the setup key to manually c

Verify the code from the app

XXXXXX

TrustKey Solutions Key Manager

T110

New Account

Name *
Github

Type
TOTP

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

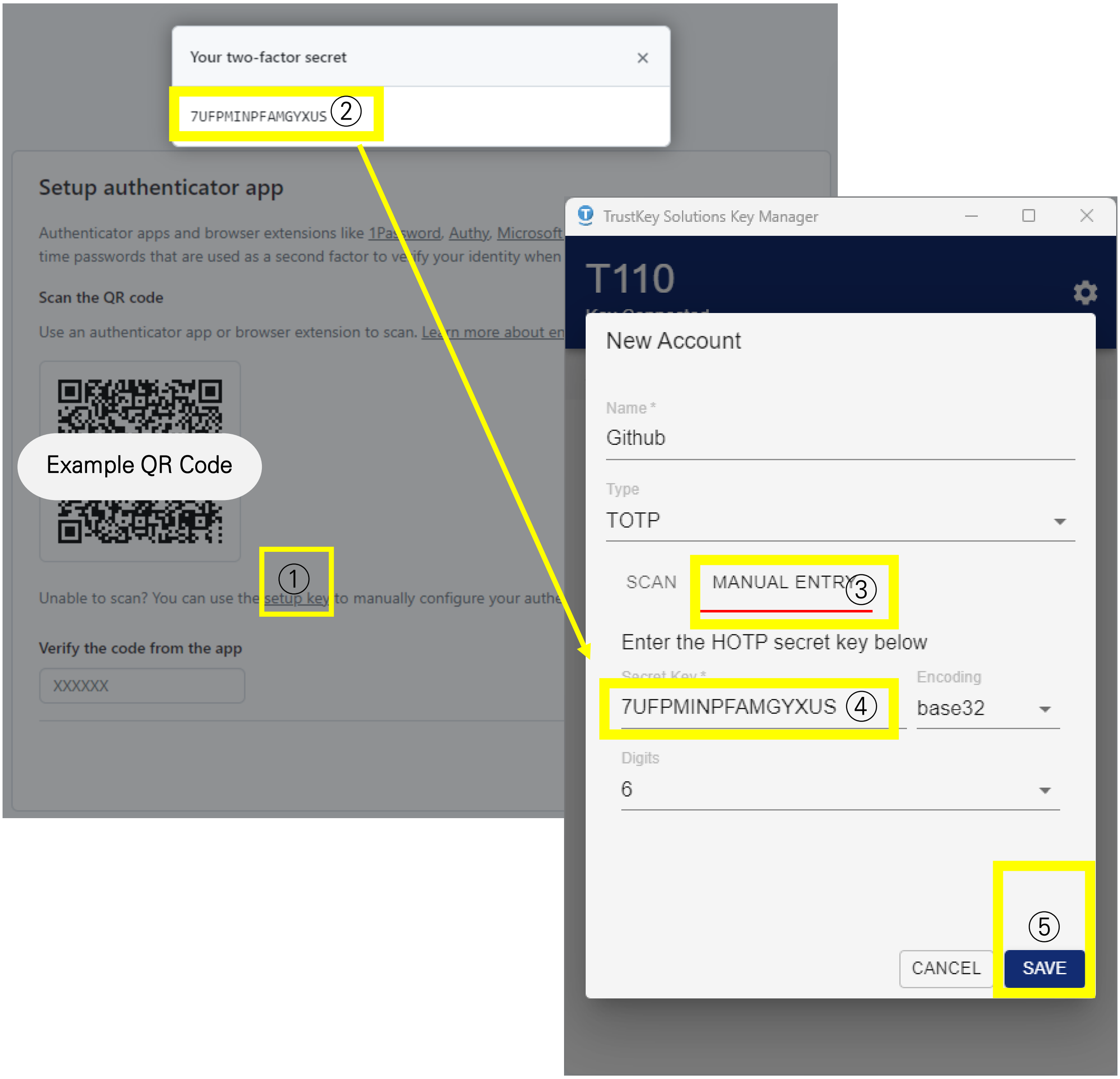
7UFPMINPFAMGYXUS

6. Setting up Security key in Key Manager at Windows

7) Using the TOTP Security Key

② Setting up TOTP accounts using Manual Entry (GitHub example)

1. Instead of using the SCAN button, get the ①②**setup key** and ④enter it in Key Manager via ③'MANUAL ENTRY' and click the ⑤[SAVE] button.



Your two-factor secret

7UFPMINPFAMGYXUS ②

Setup authenticator app

Authenticator apps and browser extensions like 1Password, Authy, Microsoft time passwords that are used as a second factor to verify your identity when

Scan the QR code

Use an authenticator app or browser extension to scan. Learn more about en

Unable to scan? You can use the setup key to manually configure your authe

Verify the code from the app

XXXXXX

TrustKey Solutions Key Manager

T110

New Account

Name *: Github

Type: TOTP

Enter the HOTP secret key below

Secret Key *: 7UFPMINPFAMGYXUS ④

Encoding: base32

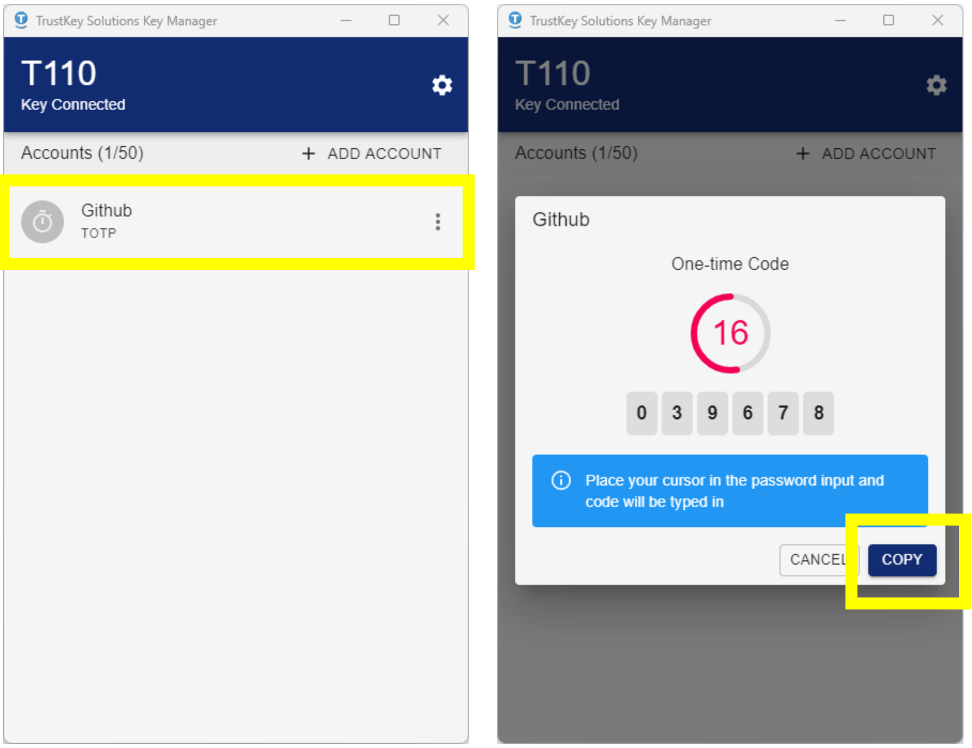
Digits: 6

6. Setting up Security key in Key Manager at Windows

7) Using the TOTP Security Key

① Setting up TOTP accounts using QR scan (GitHub example)

4. After selecting the TOTP account stored in Key Manager, place the cursor in the field where you want to enter the TOTP and touch or click the [COPY] button while the key's LED light is blinking.



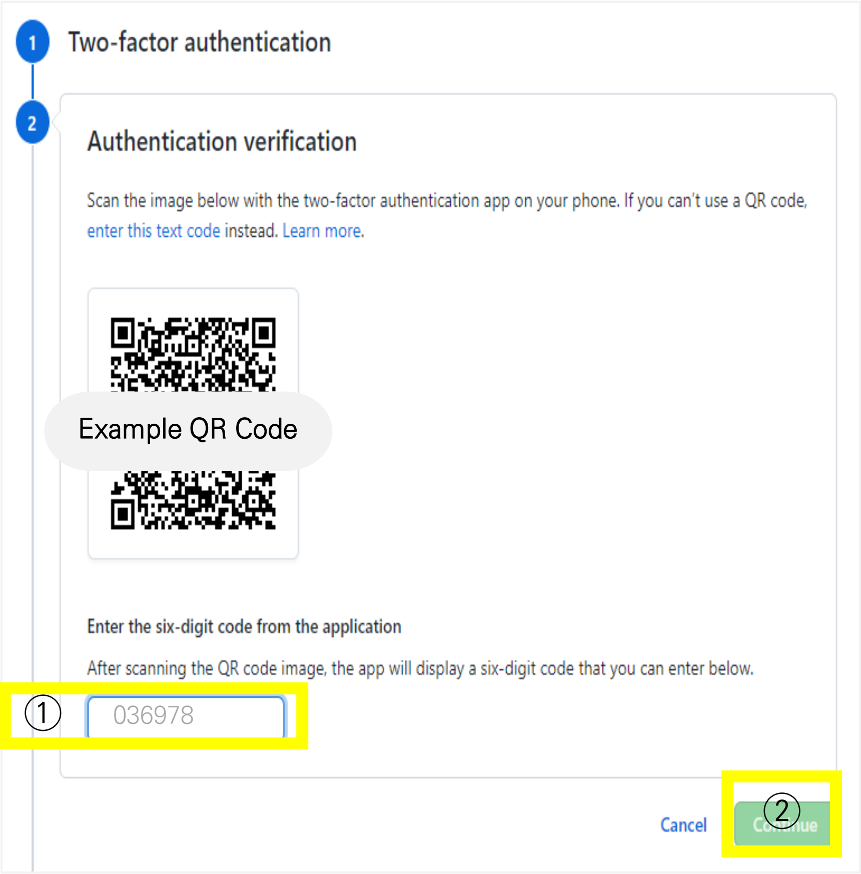
Place your cursor in the password input and code will be typed in

6. Setting up Security key in Key Manager at Windows

7) Using the TOTP Security Key

① Setting up TOTP accounts using QR scan (GitHub example)

5. Github verify the TOTP sequence based on the code given by the QR code.



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.

Example QR Code

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.

① 036978

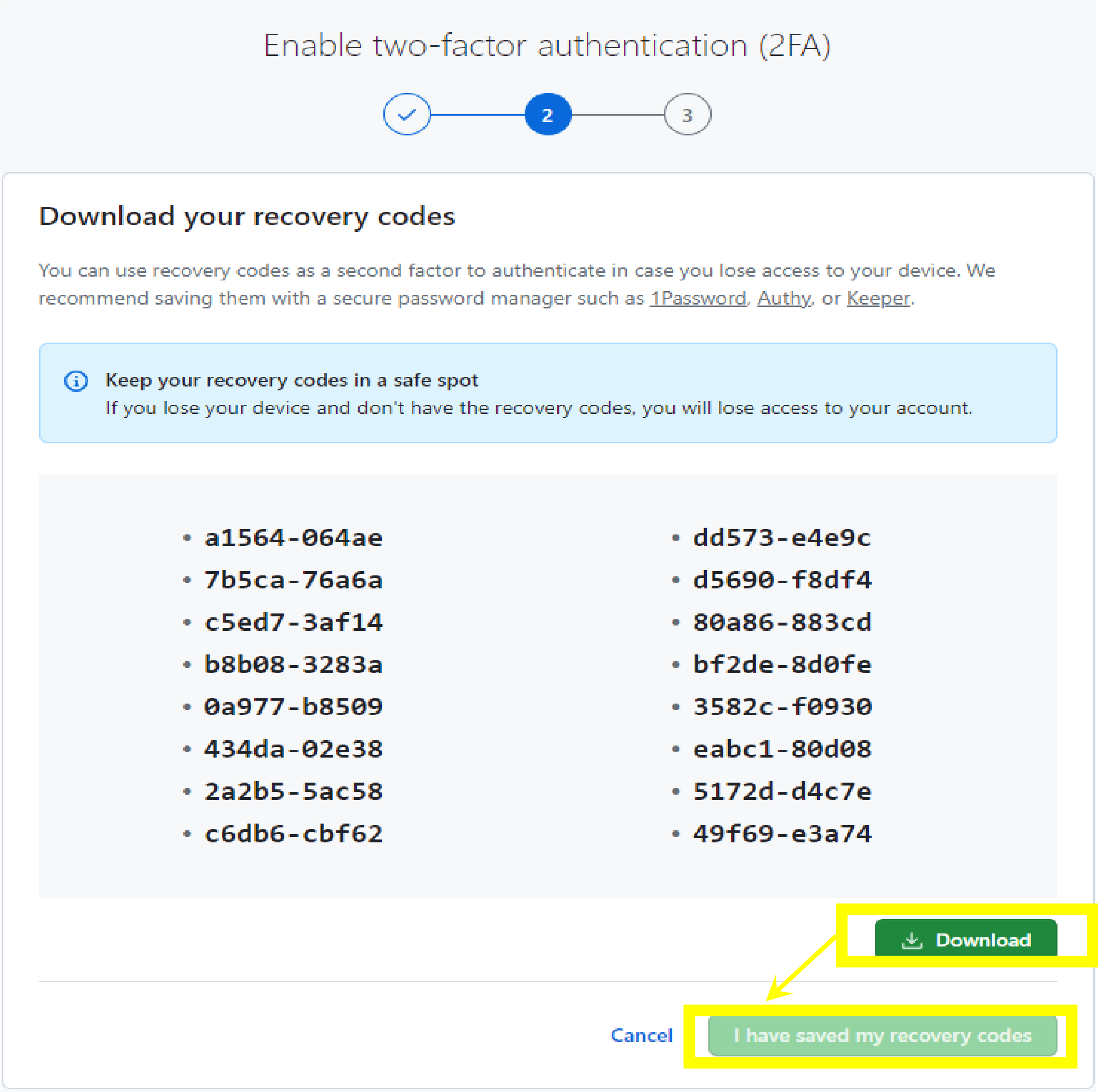
Cancel ② Continue

6. Setting up Security key in Key Manager at Windows

7) Using the TOTP Security Key

① Setting up TOTP accounts using QR scan (GitHub example)

6. After **downloading the recovery codes**, click the **[I have saved my recovery codes]** button to finally activate the two-factor authentication on the Github website.



Enable two-factor authentication (2FA)

Download your recovery codes

You can use recovery codes as a second factor to authenticate in case you lose access to your device. We recommend saving them with a secure password manager such as 1Password, Authy, or Keeper.

Keep your recovery codes in a safe spot
If you lose your device and don't have the recovery codes, you will lose access to your account.

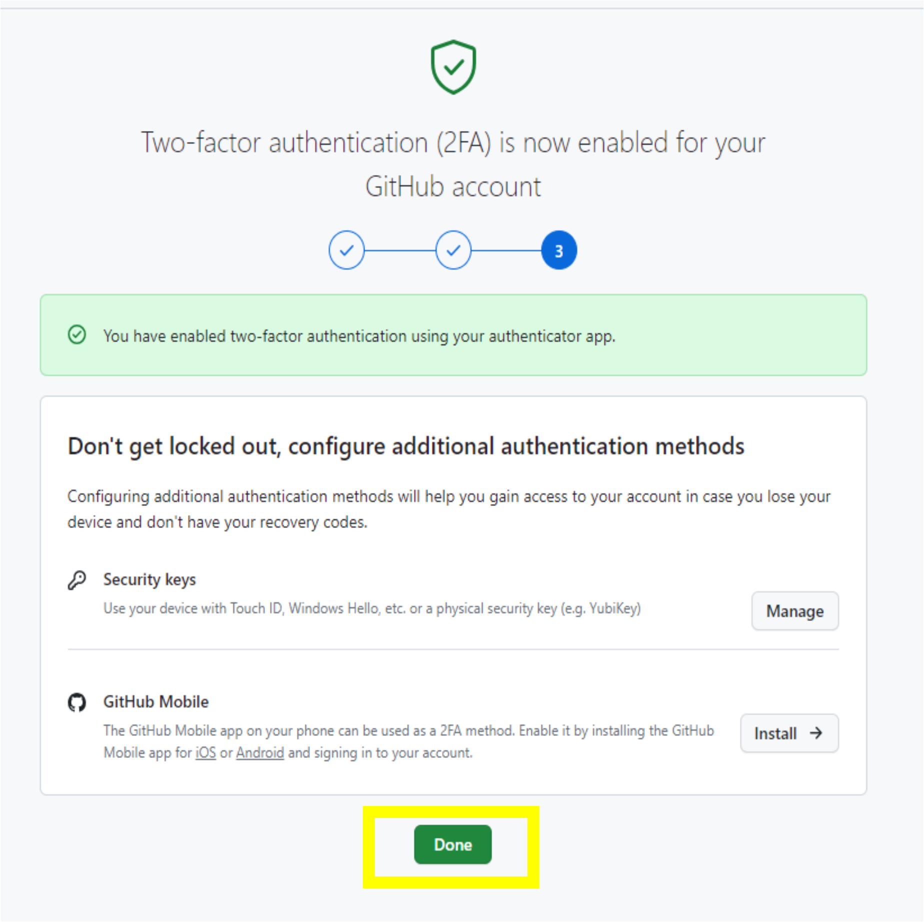
```
• a1564-064ae        • dd573-e4e9c
• 7b5ca-76a6a        • d5690-f8df4
• c5ed7-3af14        • 80a86-883cd
• b8b08-3283a        • bf2de-8d0fe
• 0a977-b8509        • 3582c-f0930
• 434da-02e38        • eabc1-80d08
• 2a2b5-5ac58        • 5172d-d4c7e
• c6db6-cbf62        • 49f69-e3a74
```

6. Setting up Security key in Key Manager at Windows

7) Using the TOTP Security Key

① Setting up TOTP accounts using QR scan (GitHub example)

7. Click the [Done] button to complete the two-factor authentication activation.



Two-factor authentication (2FA) is now enabled for your GitHub account

You have enabled two-factor authentication using your authenticator app.

Don't get locked out, configure additional authentication methods

Configuring additional authentication methods will help you gain access to your account in case you lose your device and don't have your recovery codes.

Security keys

Use your device with Touch ID, Windows Hello, etc. or a physical security key (e.g. YubiKey)

GitHub Mobile

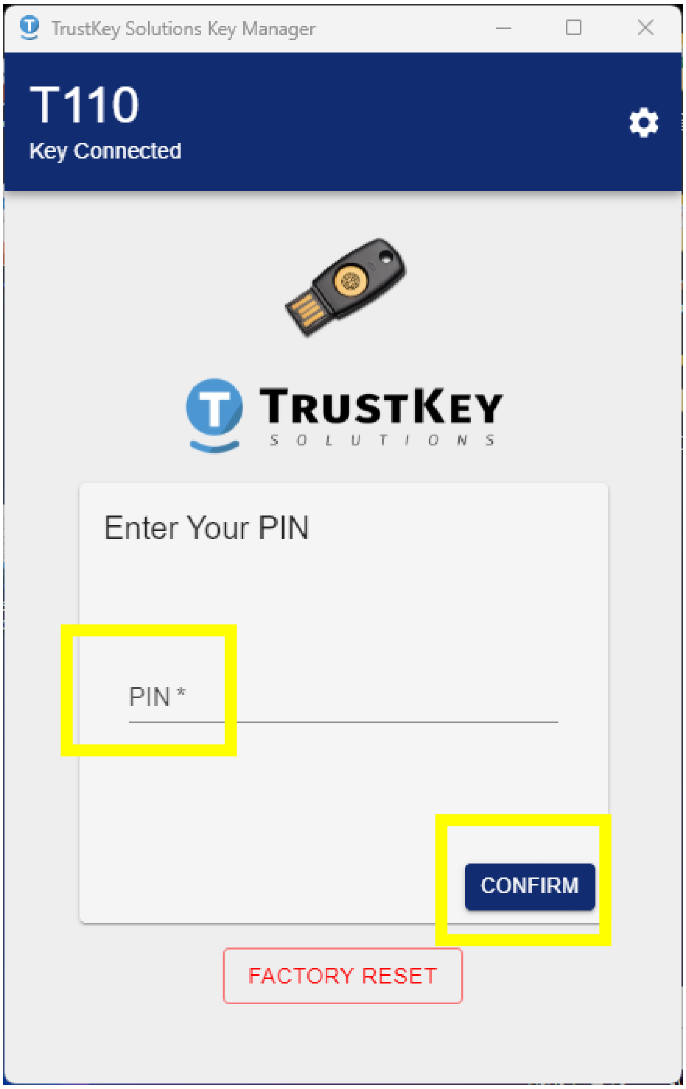
The GitHub Mobile app on your phone can be used as a 2FA method. Enable it by installing the GitHub Mobile app for iOS or Android and signing in to your account.

6. Setting up Security key in Key Manager at Windows

7) Using the TOTP Security Key

③ How to Using a TOTP

1. After logging in with your ID/PW on the website (Github), open Key Manager to insert your T110/T120 and enter your PIN.

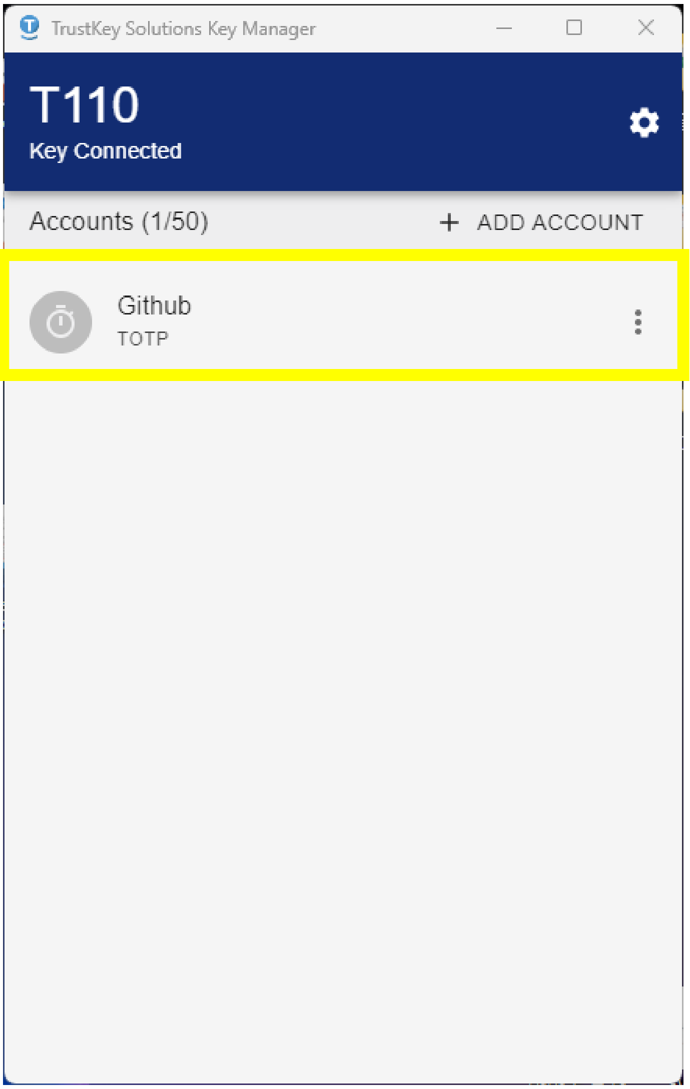


6. Setting up Security key in Key Manager at Windows

7) Using the TOTP Security Key

③ How to Using a TOTP

2. Select the OTP account you registered in Key Manager.

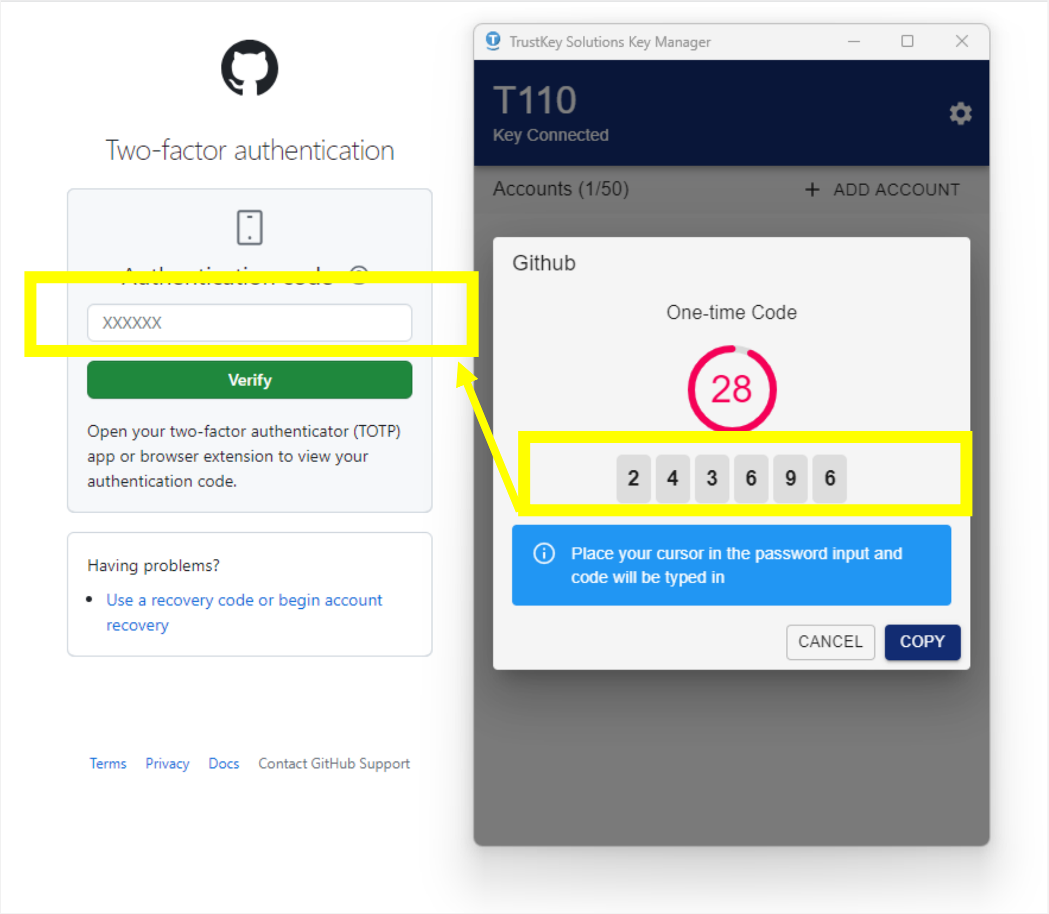


6. Setting up Security key in Key Manager at Windows

7) Using the TOTP Security Key

③ How to Using a TOTP

3. Place the cursor in the TOTP field, touch the sensor while it's flashing, or click [Copy]button. Then paste the copied TOTP code into the TOTP field on the website to complete account authentication and login.



Open your two-factor authenticator (TOTP) app or browser extension to view your authentication code.

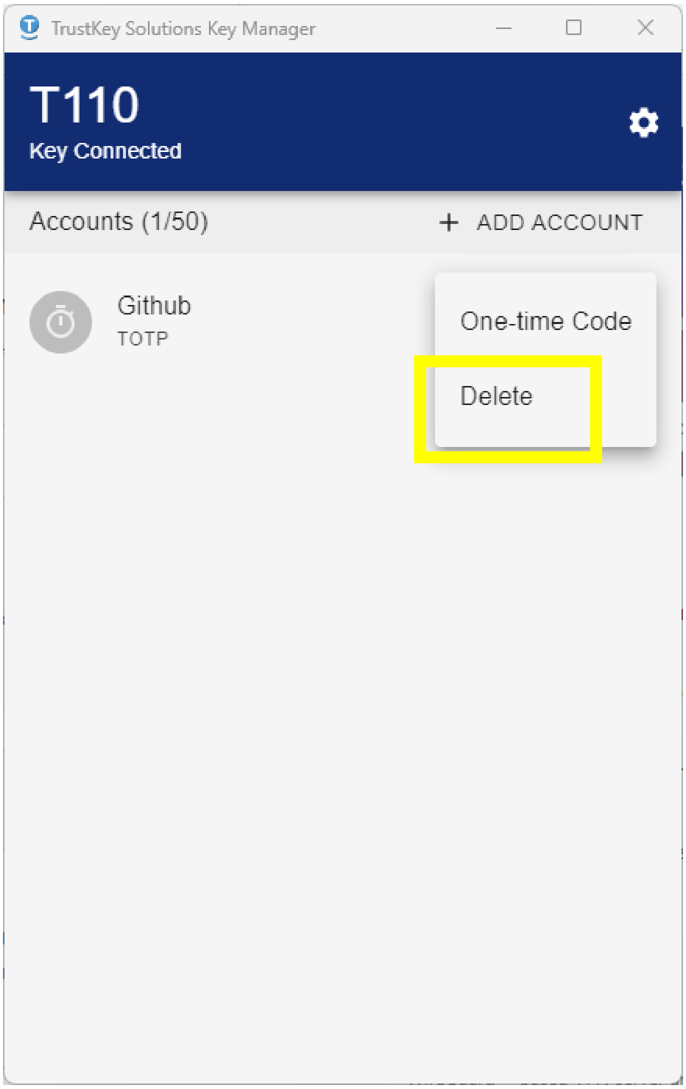
Place your cursor in the password input and code will be typed in

6. Setting up Security key in Key Manager at Windows

7) Using the TOTP Security Key

④ How to Delete a TOTP Slot

1. You can delete a set slot by selecting the [**More(⋮)**] button – [**Delete**] button.

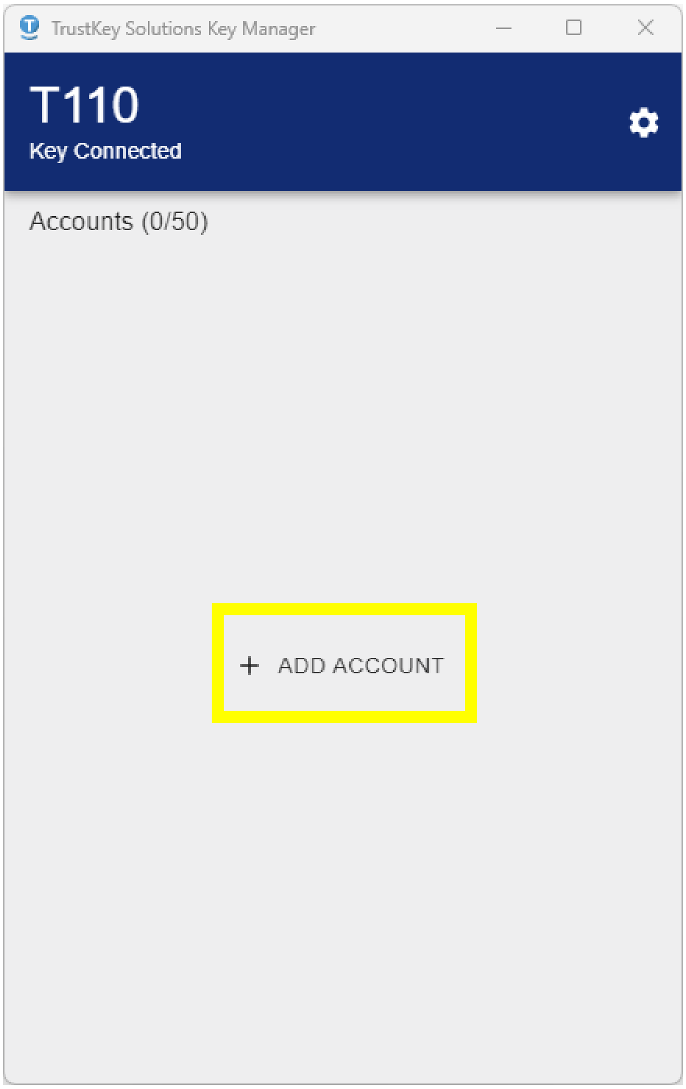


6. Setting up Security key in Key Manager at Windows

8) Using the HOTP Security Key

① Setting Up HOTP accounts (QR Code)

1. Click [+ADD ACCOUNT] button.

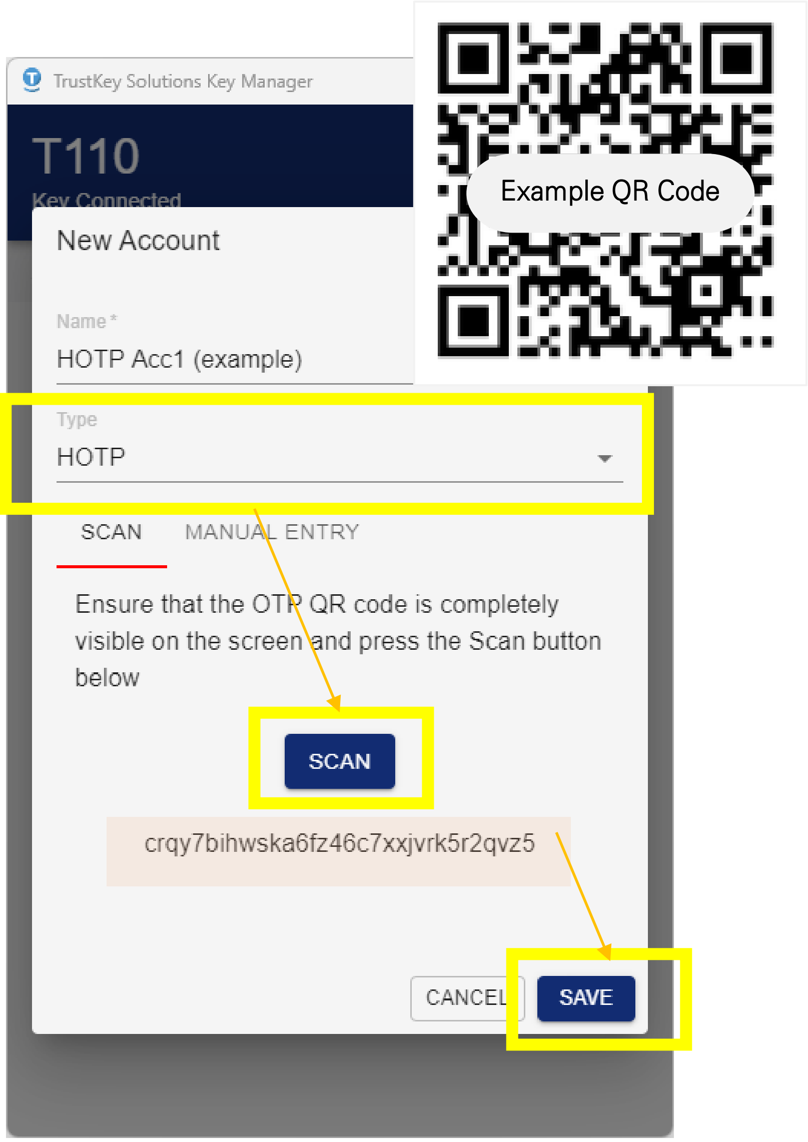


6. Setting up Security key in Key Manager at Windows

8) Using the HOTP Security Key

① Setting Up HOTP accounts (QR Code)

2. You can set up an HOTP account by QR sacn as below. (If the server does not provide a QR code, go to the 88 page to continue the registration)


TrustKey Solutions Key Manager

T110

Key Connected

New Account

Name *

HOTP Acc1 (example)

Type

HOTP

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

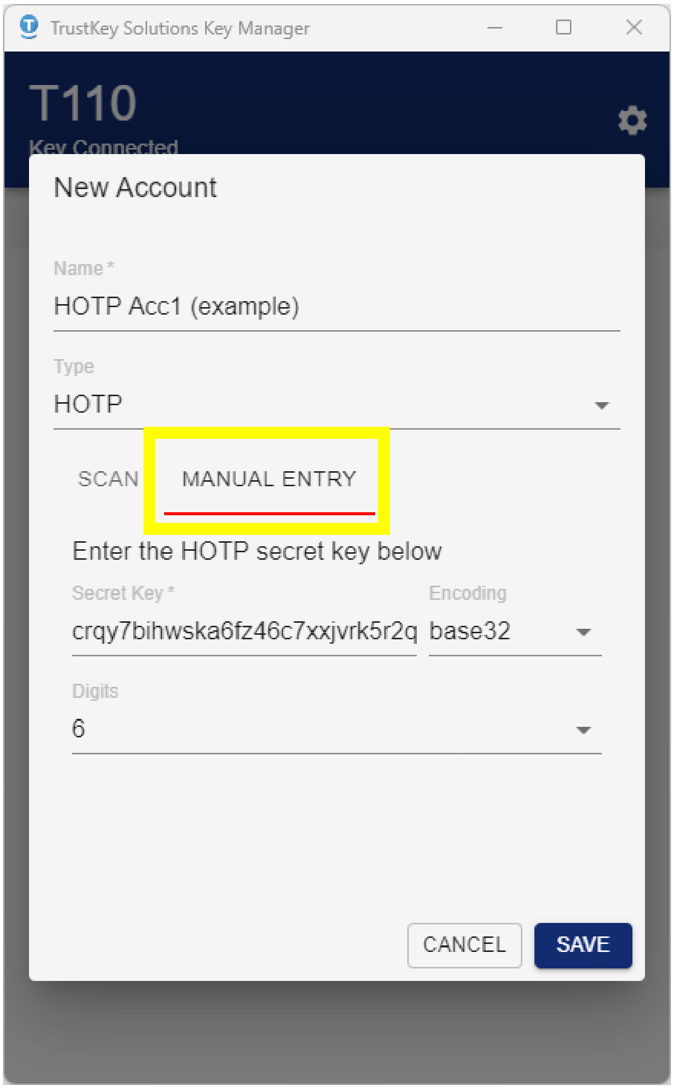
crqy7bihwska6fz46c7xxjvrk5r2qvz5

6. Setting up Security key in Key Manager at Windows

8) Using the HOTP Security Key

② Setting Up HOTP accounts (Manual Entry)

1. If website don't provide a QR code, click ‘MANUAL ENTRY’



TrustKey Solutions Key Manager

T110

Key Connected

New Account

Name *: HOTP Acc1 (example)

Type: HOTP

SCAN | MANUAL ENTRY

Enter the HOTP secret key below

Secret Key *: crqy7bihwska6fz46c7xxjvrk5r2q

Encoding: base32

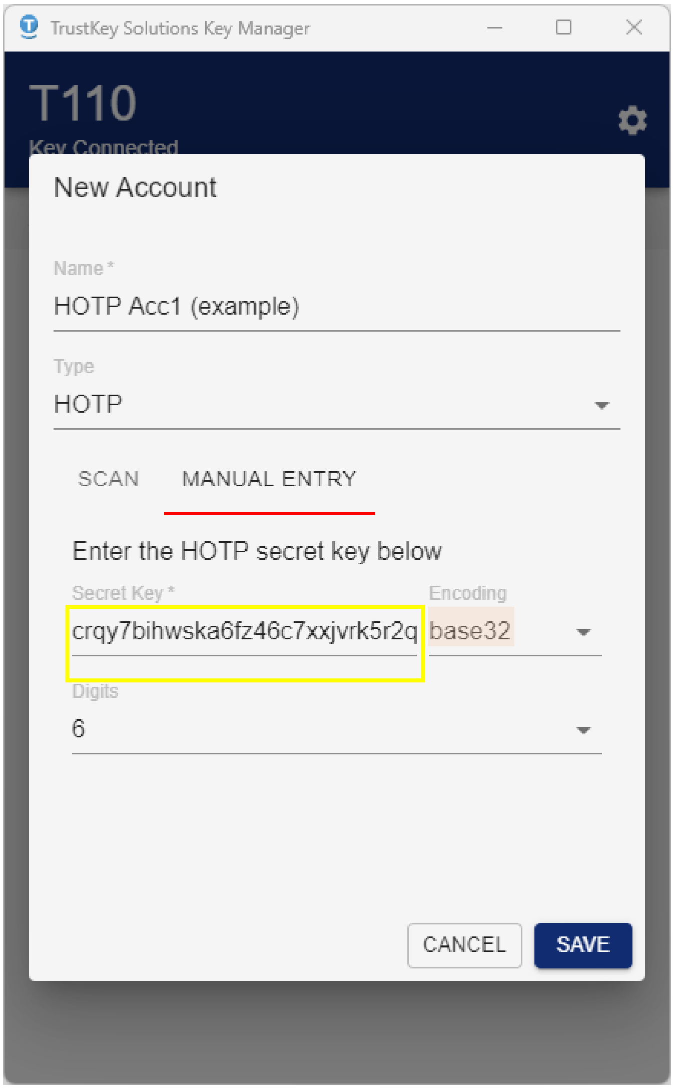
Digits: 6

6. Setting up Security key in Key Manager at Windows

8) Using the HOTP Security Key

② Setting Up HOTP accounts (Manual Entry)

2-2. Input '**Security Key**'. Note that the manual entry data should be in a Base32 format.



New Account

Name *: HOTP Acc1 (example)

Type: HOTP

Enter the HOTP secret key below

Secret Key *: crqy7bihwska6fz46c7xxjvrk5r2q

Encoding: base32

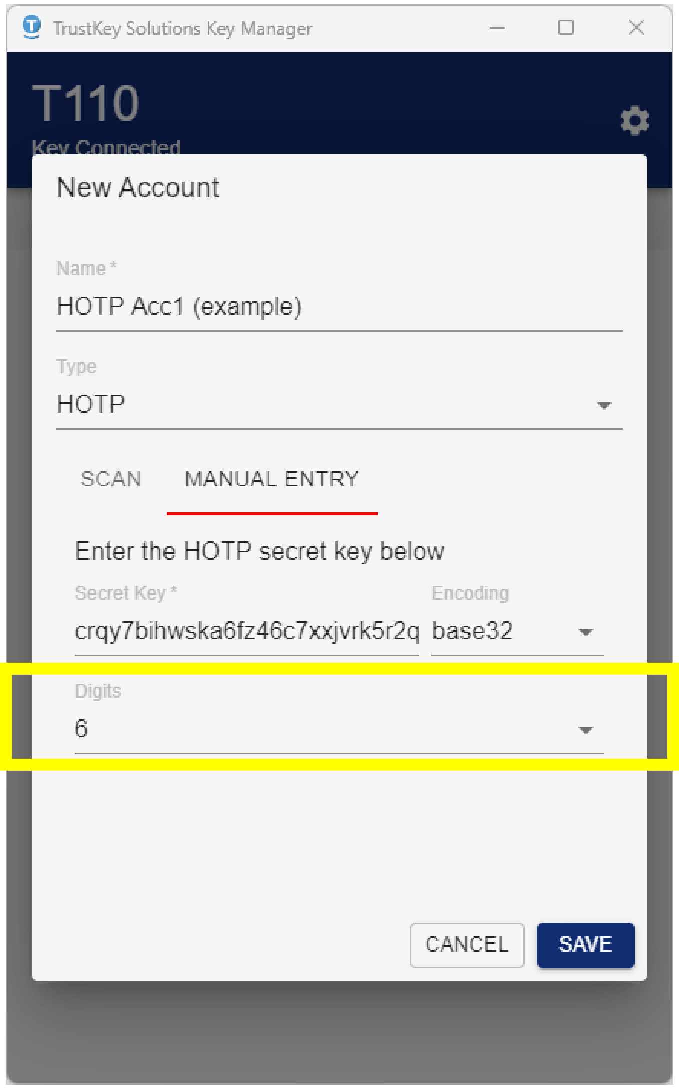
Digits: 6

6. Setting up Security key in Key Manager at Windows

8) Using the HOTP Security Key

② Setting Up HOTP accounts (Manual Entry)

2-3. Select the number of digits (6-8 digits)



Name * HOTP Acc1 (example)

Type HOTP

Enter the HOTP secret key below

Secret Key * crqy7bihwska6fz46c7xxjvrk5r2q

Encoding base32

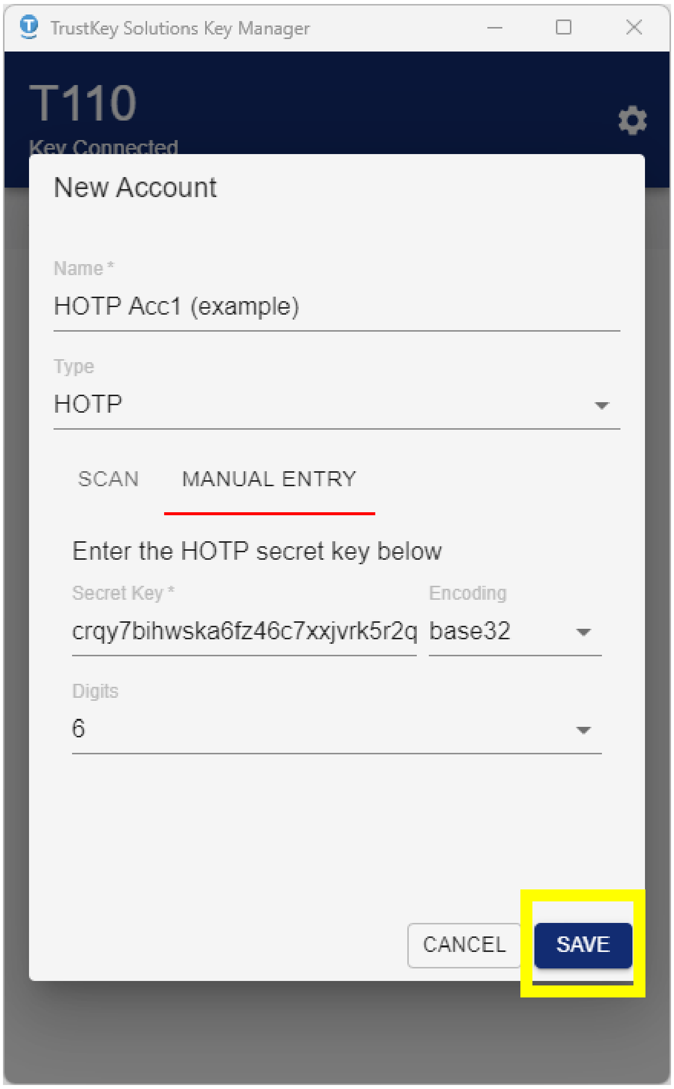
Digits 6

6. Setting up Security key in Key Manager at Windows

8) Using the HOTP Security Key

② Setting Up HOTP accounts (Manual Entry)

2-4. Click [SAVE] button.
Depending on the configured slot HOTP, a long touch or short touch can generate an OTP value directly from the text field.



Name *
HOTP Acc1 (example)

Type
HOTP

Enter the HOTP secret key below

Secret Key *
crqy7bihwska6fz46c7xxjvrk5r2q

Encoding
base32

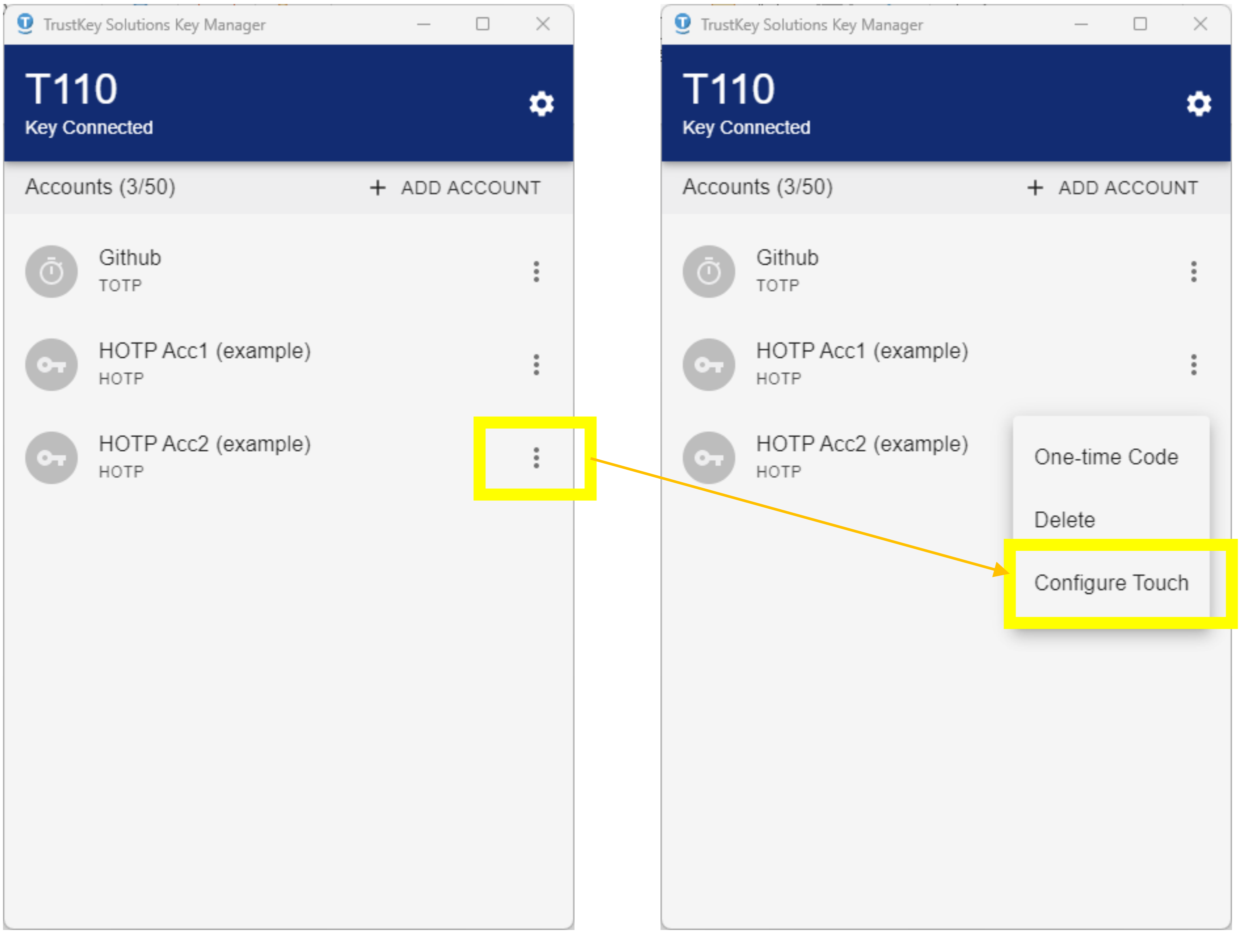
Digits
6

6. Setting up Security key in Key Manager at Windows

8) Using the HOTP Security Key

③ How to Replace a HOTP

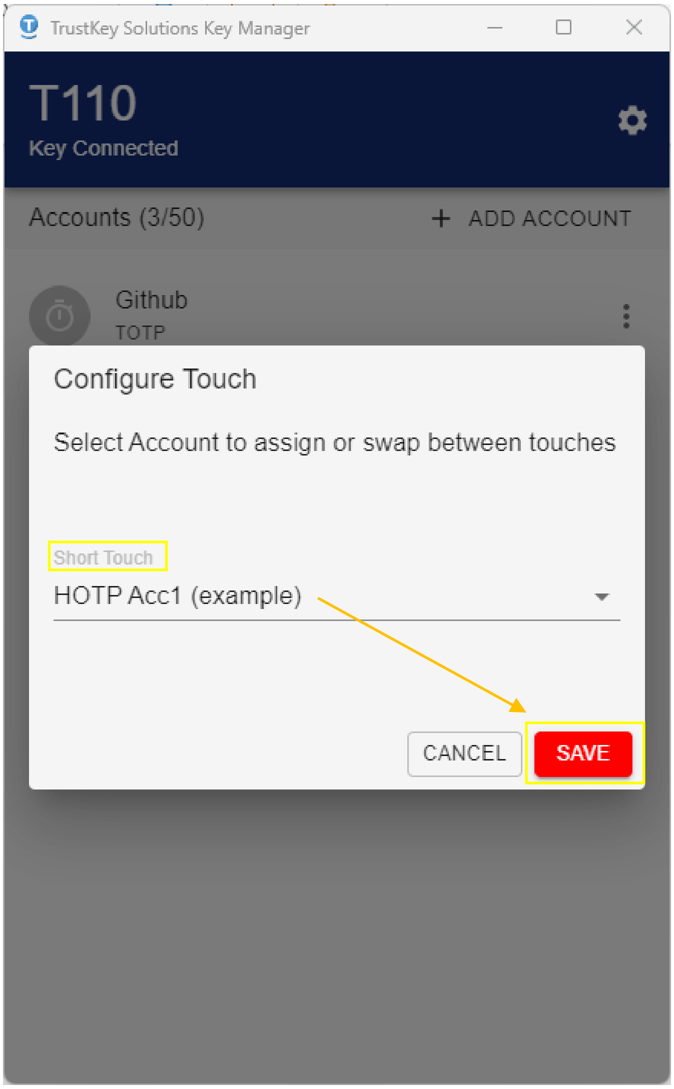
1. You can replace the HOTP settings slot by selecting ‘**Configure Touch**’ for HOTP from the list of accounts.



8) Using the HOTP Security Key

③ How to Replace a HOTP

2 In the 'Short Touch' option, select the HOTP account you want to exchange for the short touch. This will swap the account between the short and long touch.



Configure Touch

Select Account to assign or swap between touches

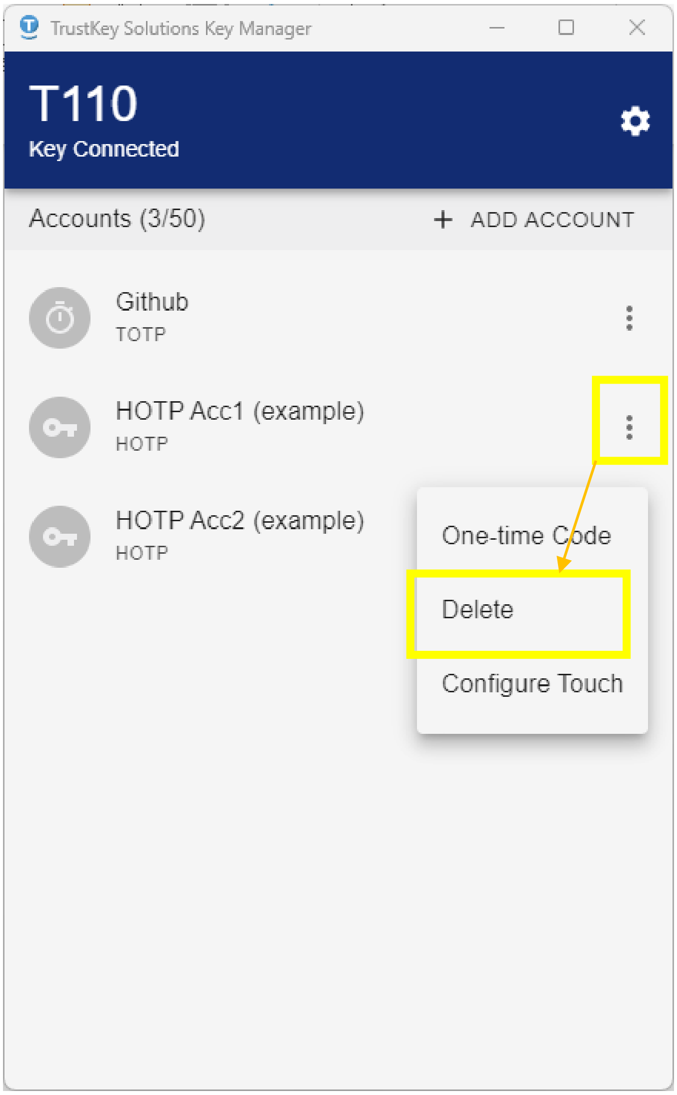
Short Touch: HOTP Acc1 (example)

6. Setting up Security key in Key Manager at Windows

8) Using the HOTP Security Key

④ How to Delete HOTP Slot

1. If you want to delete an account listed in HOTP, you can delete it by clicking **More (⋮)** button, and then click [**Delete**].

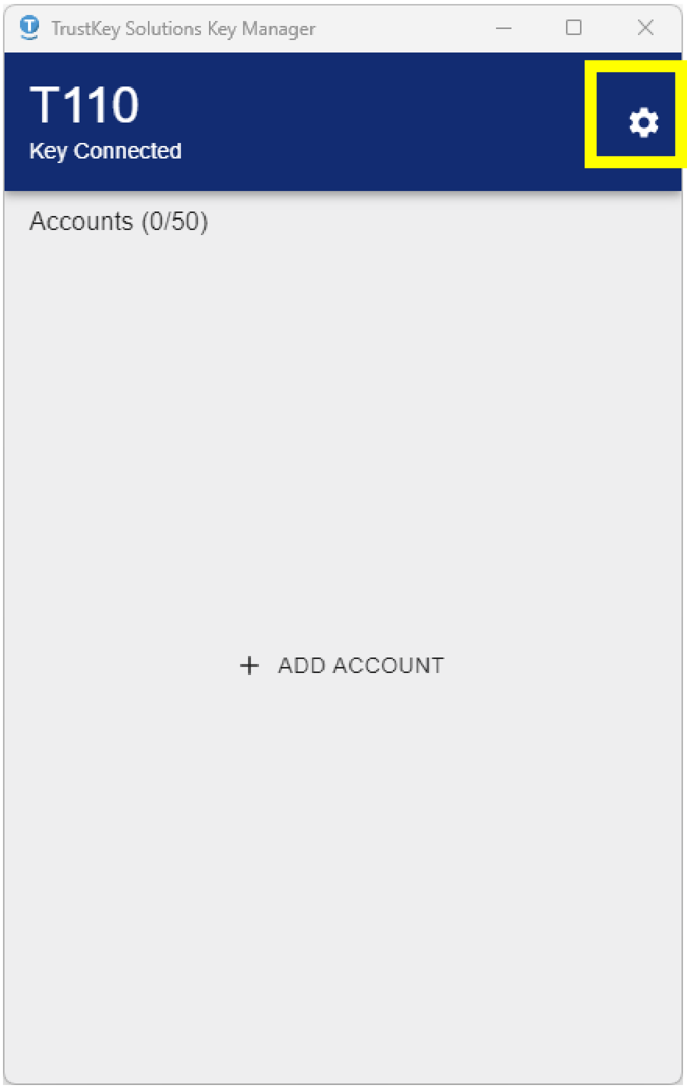


6. Setting up Security key in Key Manager at Windows

9) Setting Up Key Manager

① Language Selection

1. Click [⚙] setup button.

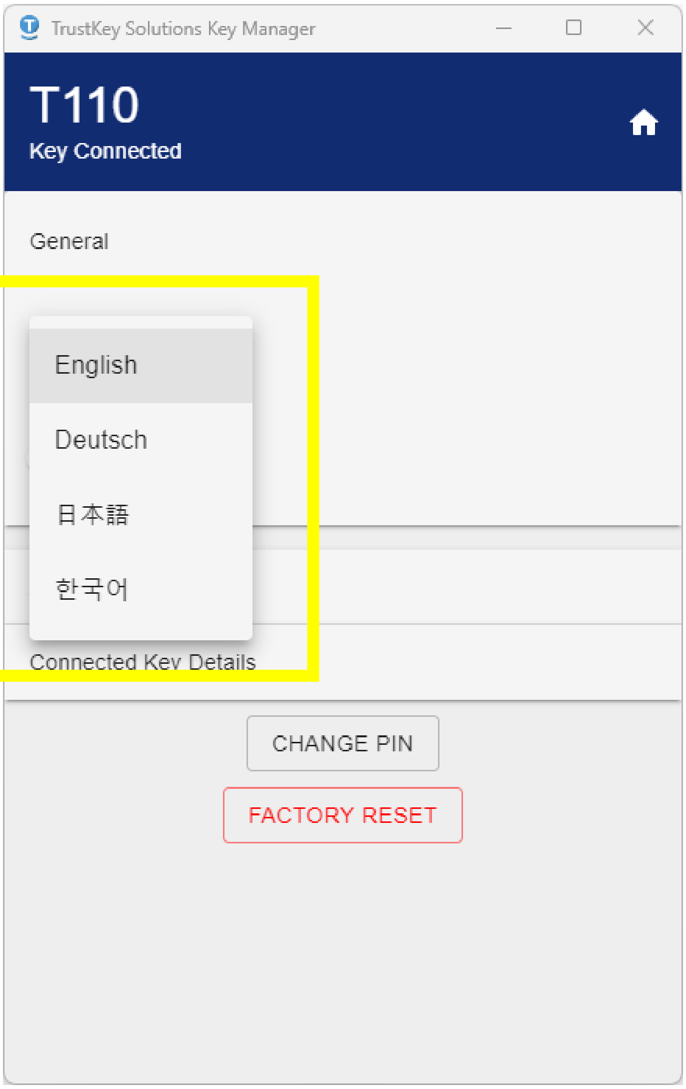


6. Setting up Security key in Key Manager at Windows

9) Setting Up Key Manager

① Language Selection

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

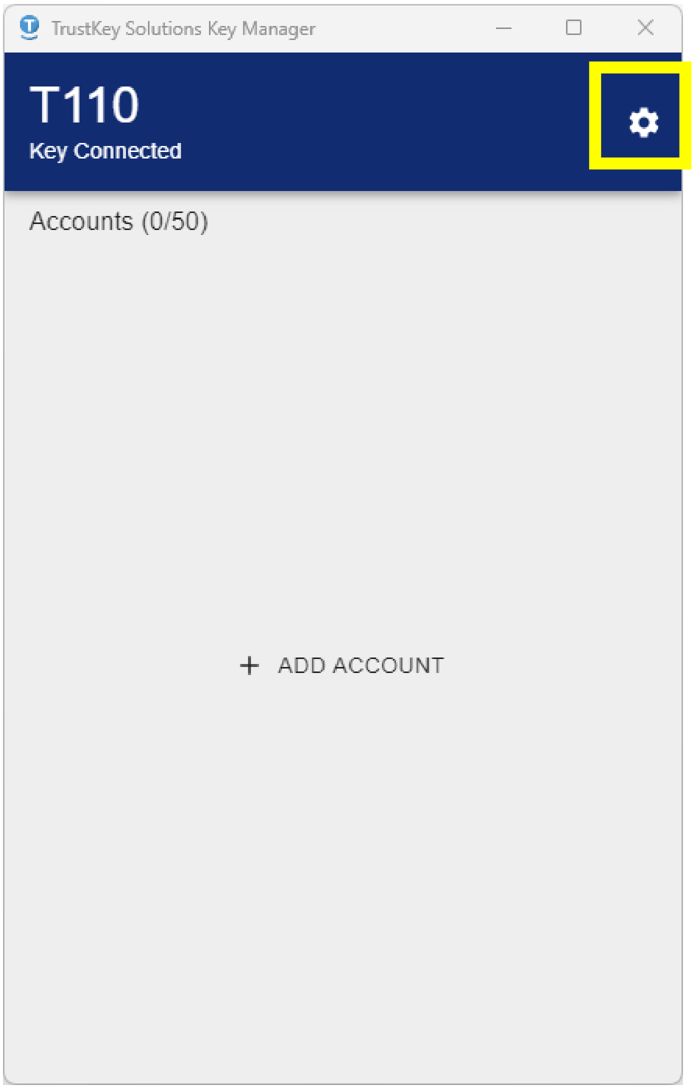


6. Setting up Security key in Key Manager at Windows

9) Setting Up Key Manager

② Dark Mode

1. Click [⚙] setup button.

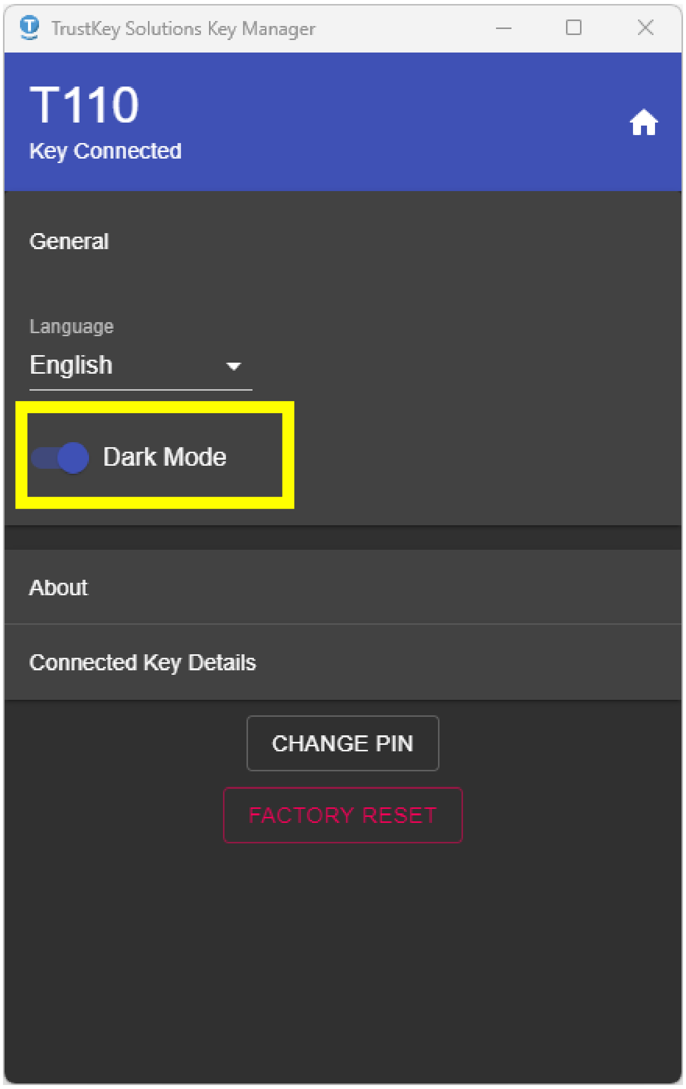


6. Setting up Security key in Key Manager at Windows

9) Setting Up Key Manager

② Dark Mode

2. Tap the [Dark Mode] button to turn it on or off.

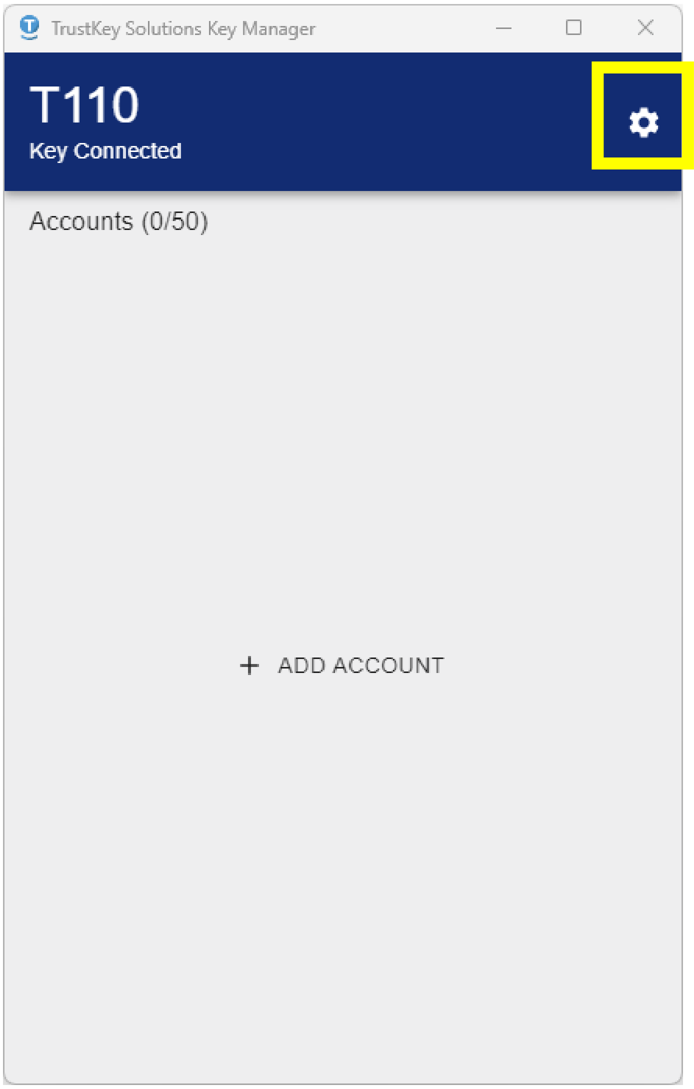


6. Setting up Security key in Key Manager at Windows

9) Setting Up Key Manager

③ Key Manager Version Check

1. Click [⚙] button.

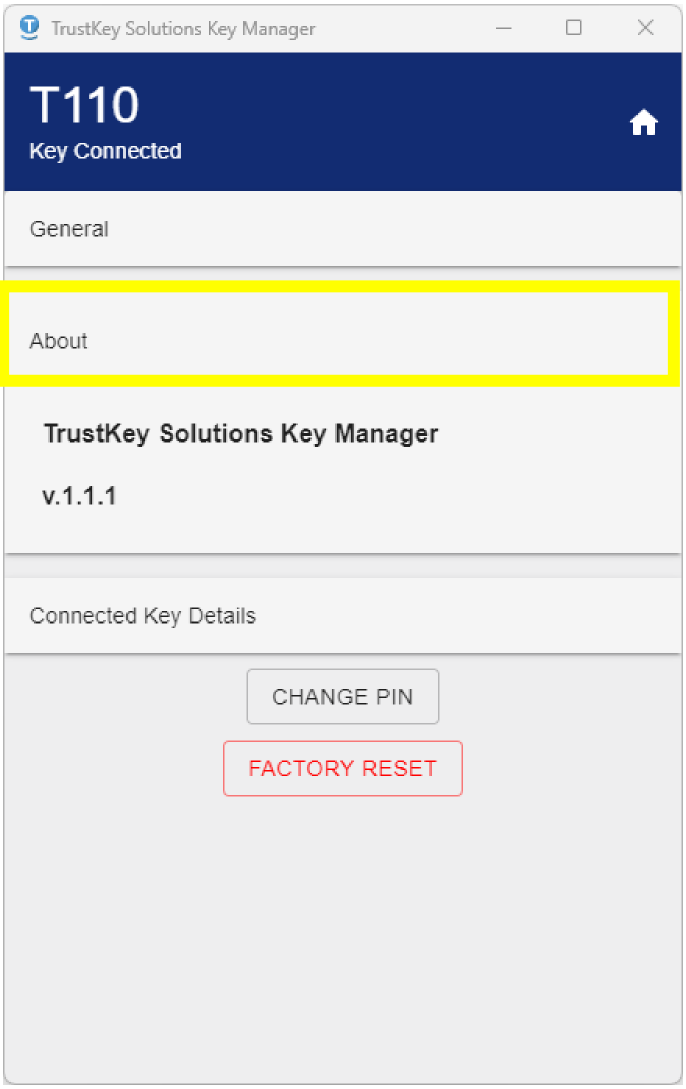


6. Setting up Security key in Key Manager at Windows

9) Setting Up Key Manager

③ Key Manager Version Check

2. Click [**About**].



TrustKey Solutions Key Manager

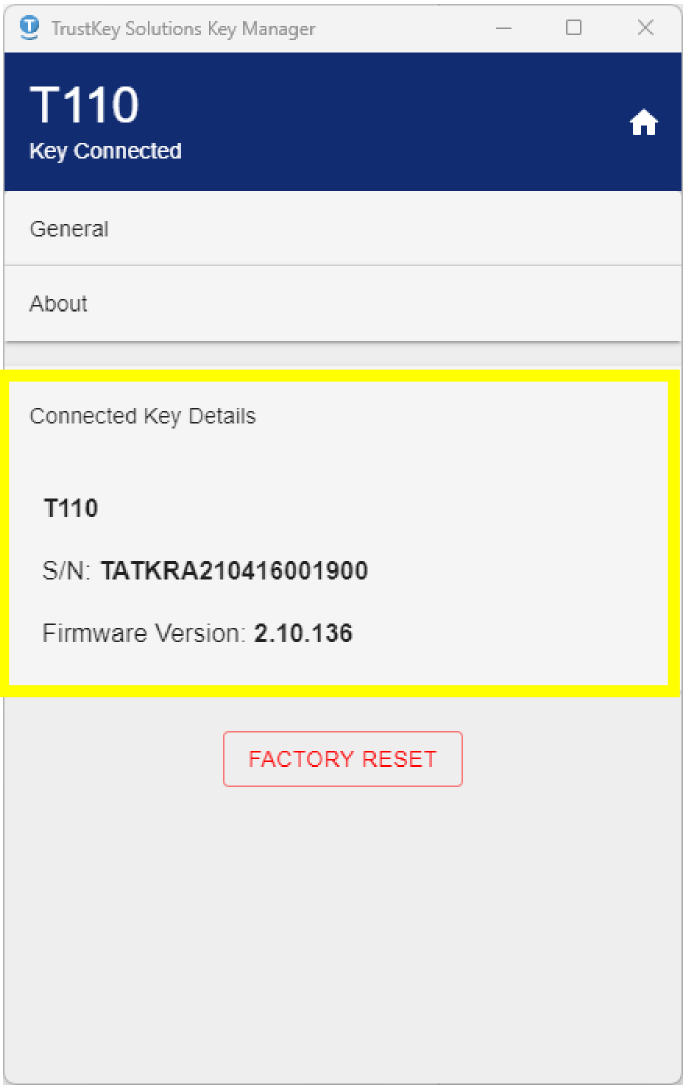
v.1.1.1

6. Setting up Security key in Key Manager at Windows

9) Setting Up Key Manager

④ The connected (inserted) Key Details

This section describes the key serial number and firmware version.



Connected Key Details

T110

S/N: **TATKRA210416001900**

Firmware Version: **2.10.136**

7. Online Usage of the Security Keys

1) Microsoft Azure

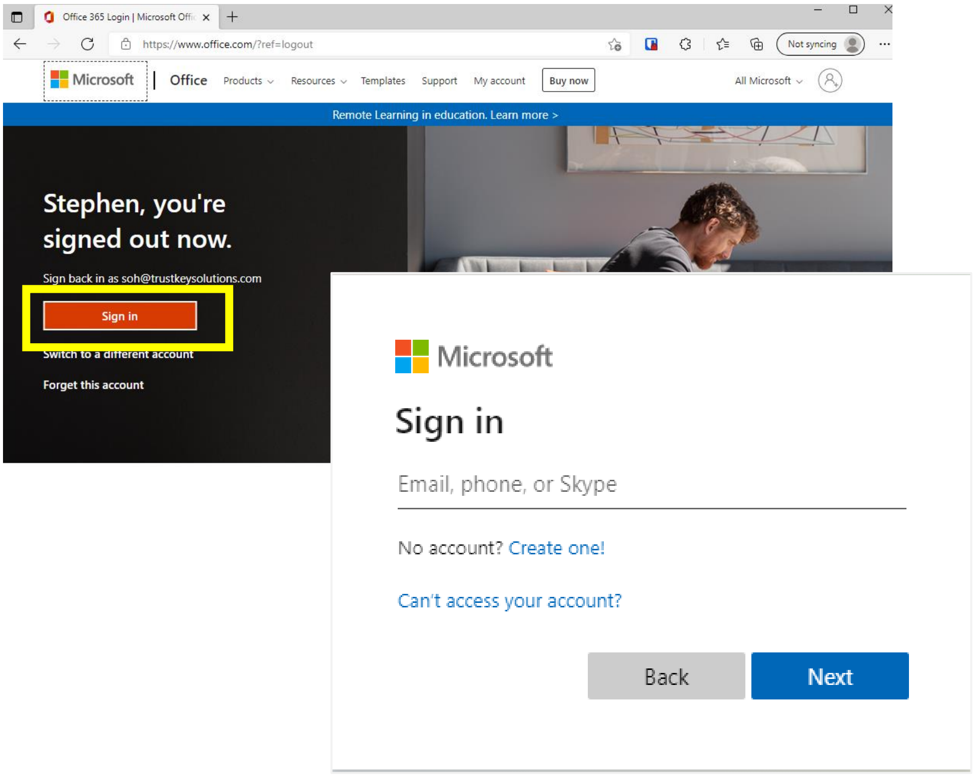
[Azure AD user registration]

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

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

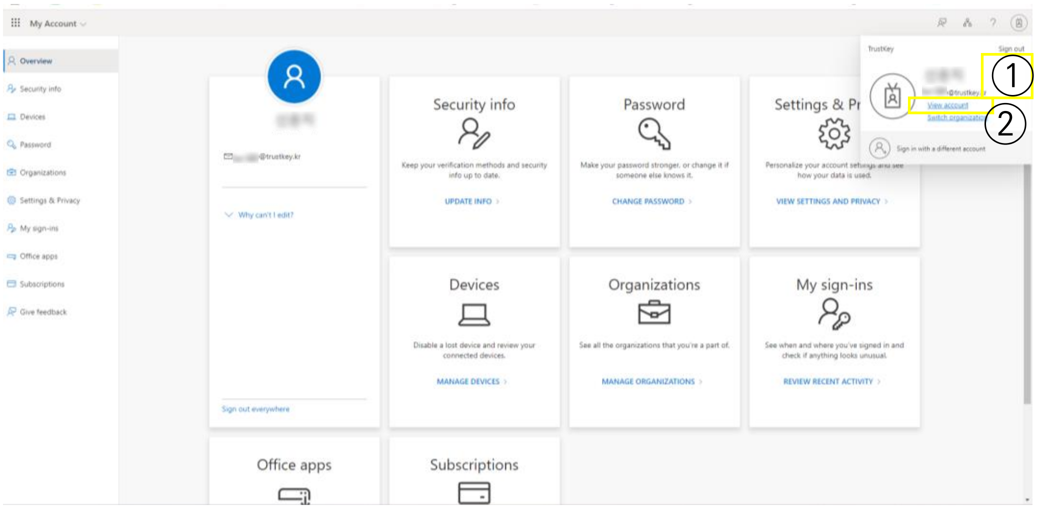
Remote Learning in education. Learn more >

https://www.office.com/?ref=logout

7. Online Usage of the Security Keys

1) Microsoft Azure

2. Click ①‘**Account Manage**’ in the top right corner – Click ②**View account**.



Keep your verification methods and security info up to date.

Make your password stronger, or change it if someone else knows it.

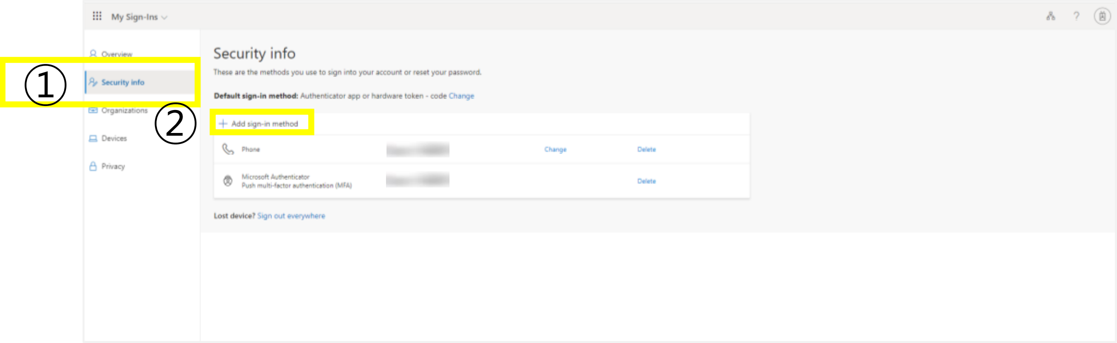
Personalize your account settings and see how your data is used.

Disable a lost device and review your connected devices.

See all the organizations that you're a part of.

See when and where you've signed in and check if anything looks unusual.

3. Select ①**Security info** – ②**+Add method**



Security info

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

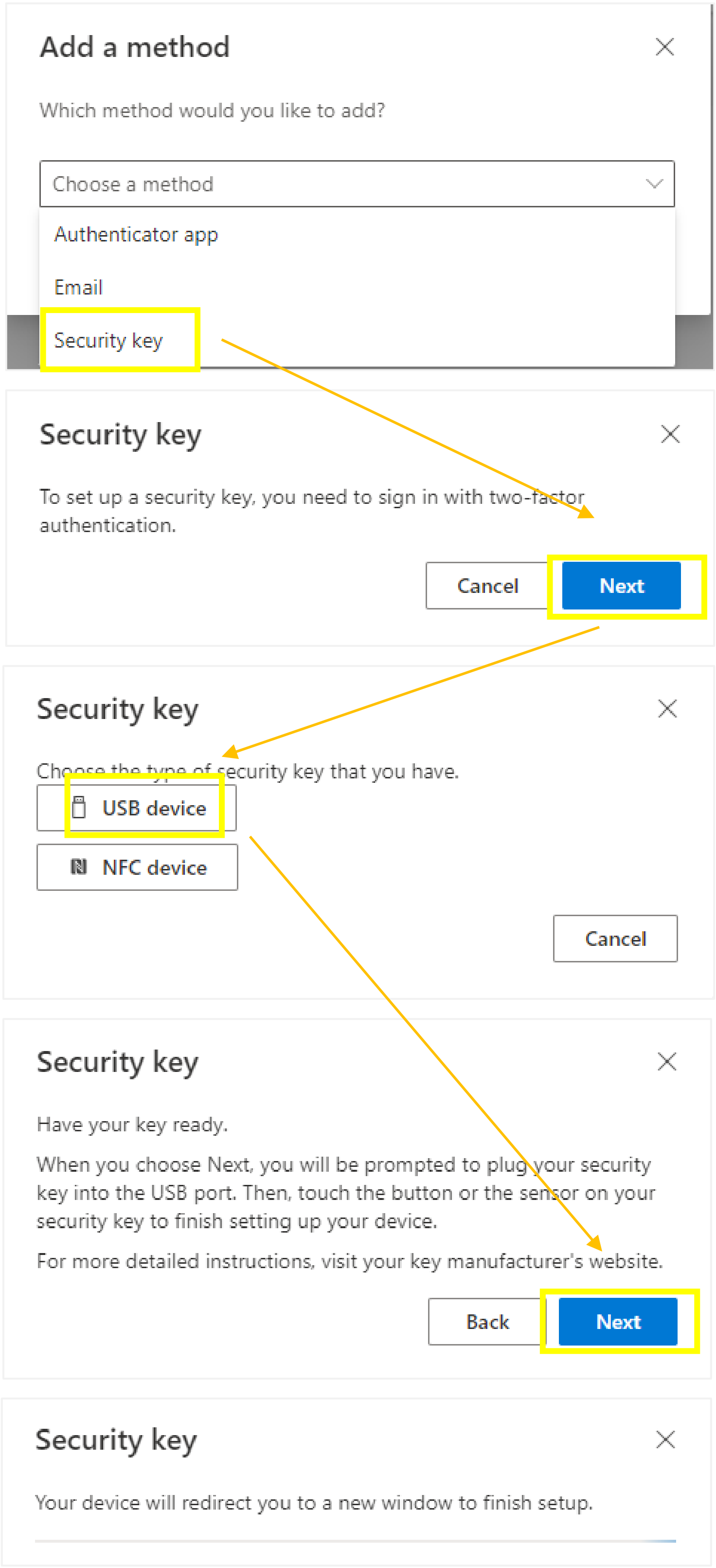
Default sign-in method: Authenticator app or hardware token - code Change

Lost device? Sign out everywhere

7. Online Usage of the Security Keys

1) Microsoft Azure

4. Follow the registration flow.



Add a method

Which method would you like to add?

Security key

To set up a security key, you need to sign in with two-factor authentication.

Security key

Choose the type of security key that you have.

Security key

Have your key ready.

When you choose Next, you will be prompted to plug your security key into the USB port. Then, touch the button or the sensor on your security key to finish setting up your device.

For more detailed instructions, visit your key manufacturer's website.

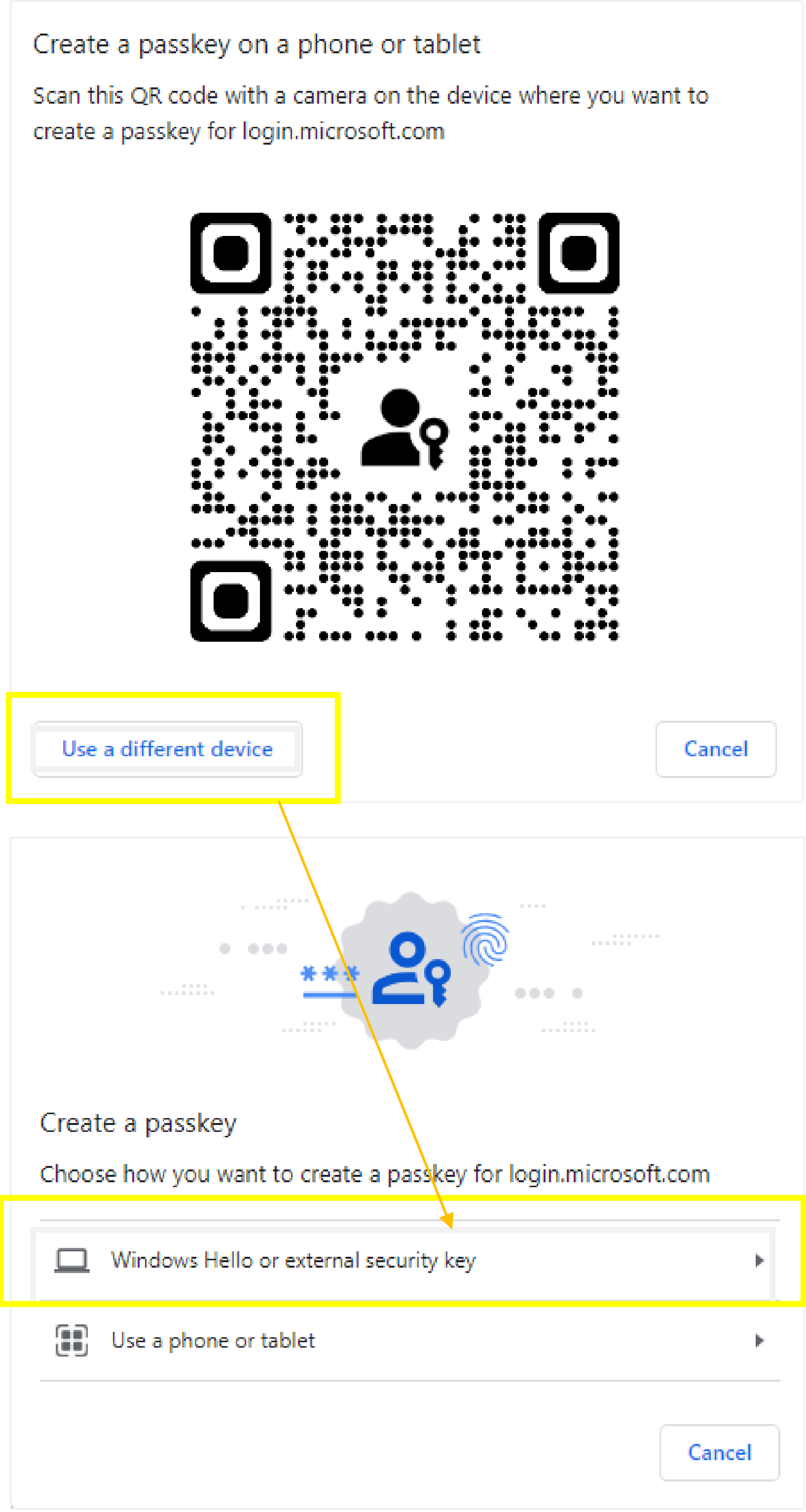
Security key

Your device will redirect you to a new window to finish setup.

7. Online Usage of the Security Keys

1) Microsoft Azure

5. Follow the registration flow.



Create a passkey on a phone or tablet

Scan this QR code with a camera on the device where you want to create a passkey for login.microsoft.com

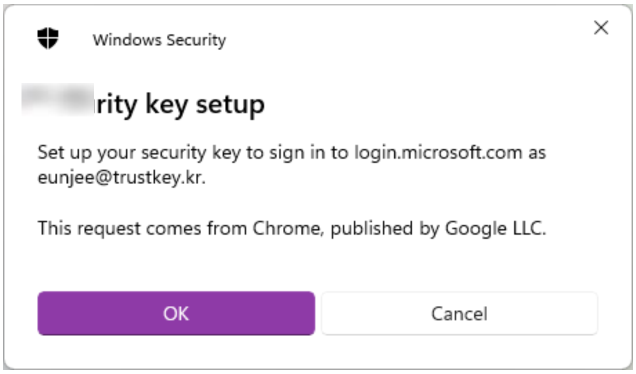
Create a passkey

Choose how you want to create a passkey for login.microsoft.com

7. Online Usage of the Security Keys

1) Microsoft Azure

6. Guide to setting up a security key. Click the [OK] button.

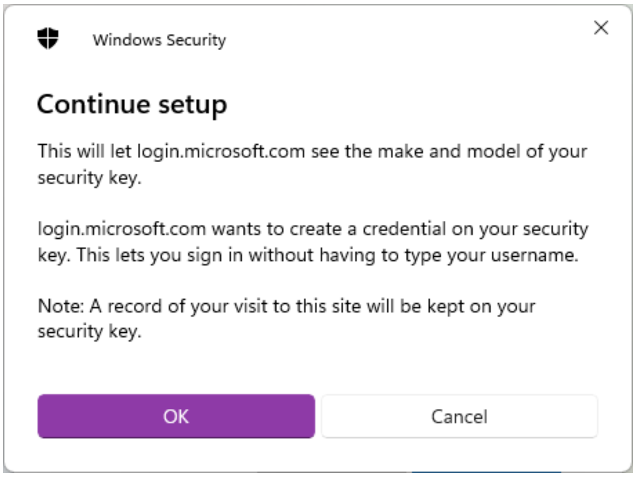


[redacted]rity key setup

Set up your security key to sign in to login.microsoft.com as eunjee@trustkey.kr.

This request comes from Chrome, published by Google LLC.

7. Instructions for generating the key inside the security key. Click [OK]button.



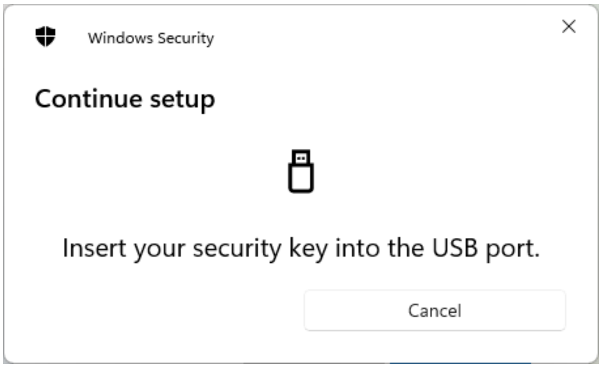
Continue setup

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.

8. Insert T110/T120 security key into the USB port.



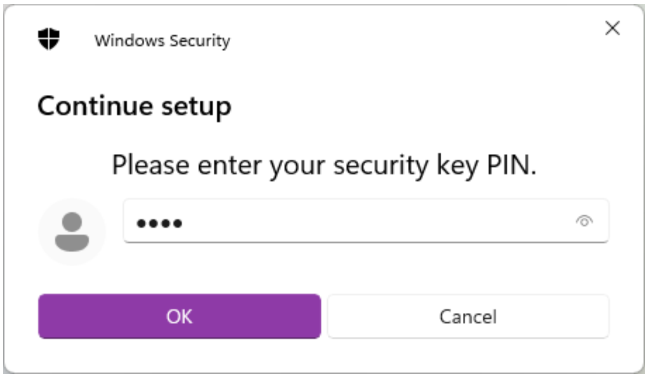
Continue setup

Insert your security key into the USB port.

7. Online Usage of the Security Keys

1) Microsoft Azure

9. Enter your security key PIN – Click [OK] button.



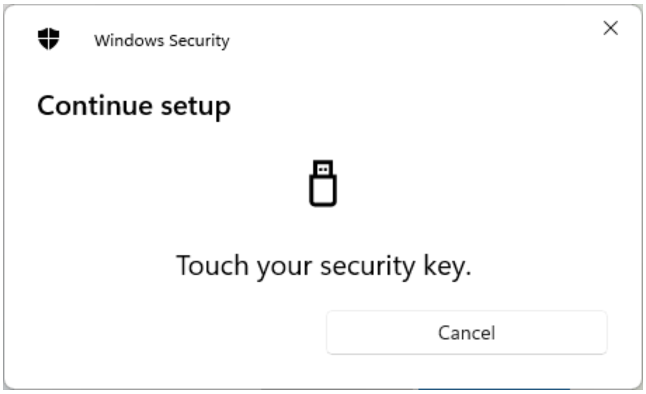
Windows Security

Continue setup

Please enter your security key PIN.

••••

10. When the security key's LED flashes white, touch the security key's touch sensor.

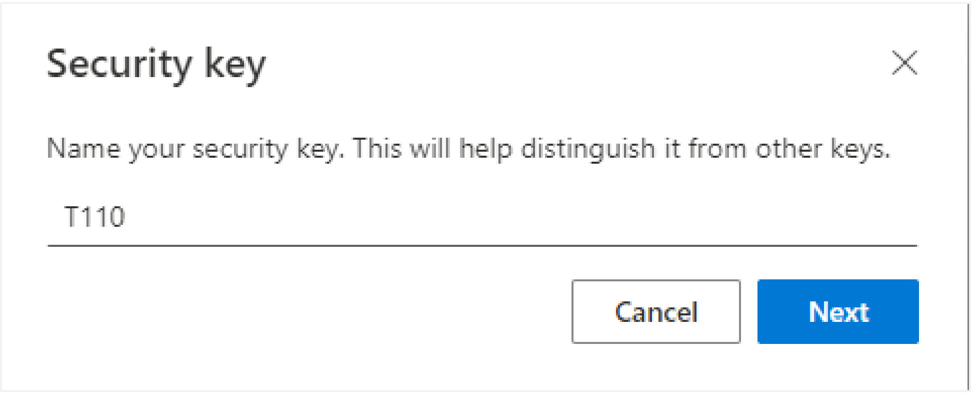


Windows Security

Continue setup

Touch your security key.

11. Enter a name for the security key, and then click the [Next] button.

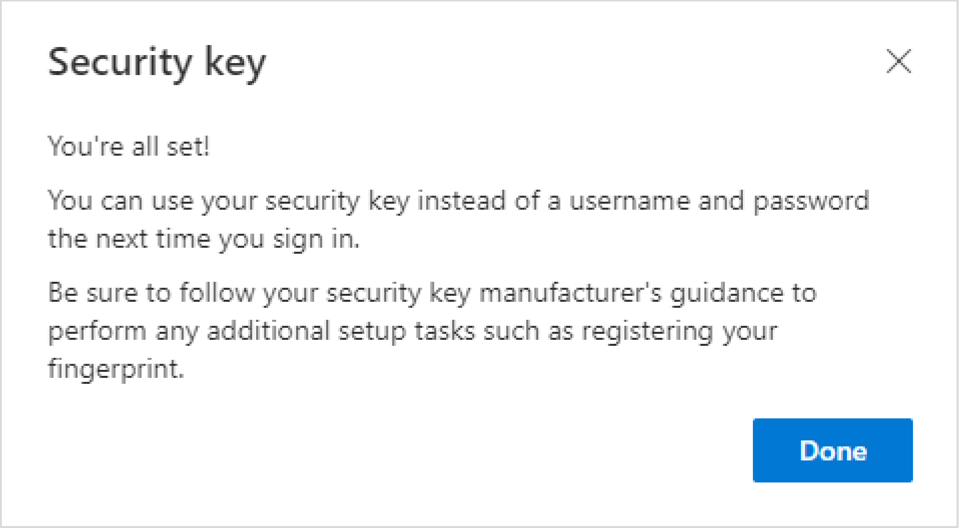


Security key

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

T110

12. Click the [Done] button to complete the security key enrollment.



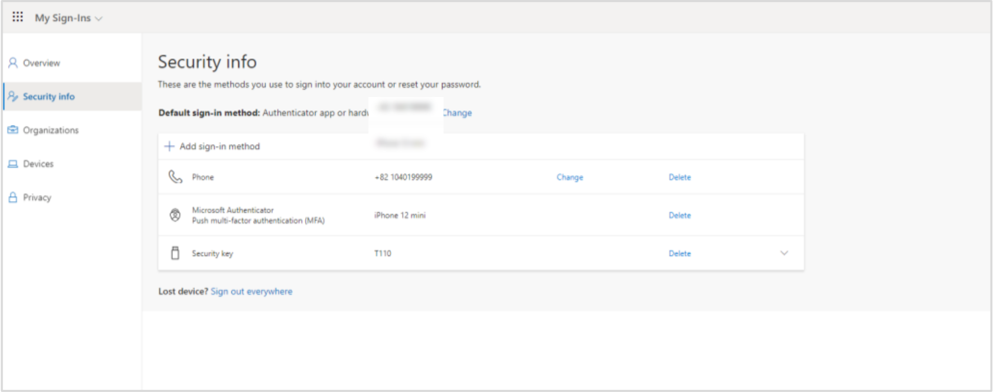
Security key

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.

12–1. You can find your registered secret key in 'Security Information'.



Security info

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

Default sign-in method: Authenticator app or hardw [redacted] Change

+ Add sign-in method

Phone	+82 1040199999	Change	Delete
Microsoft Authenticator Push multi-factor authentication (MFA)	iPhone 12 mini		Delete
Security key	T110		Delete

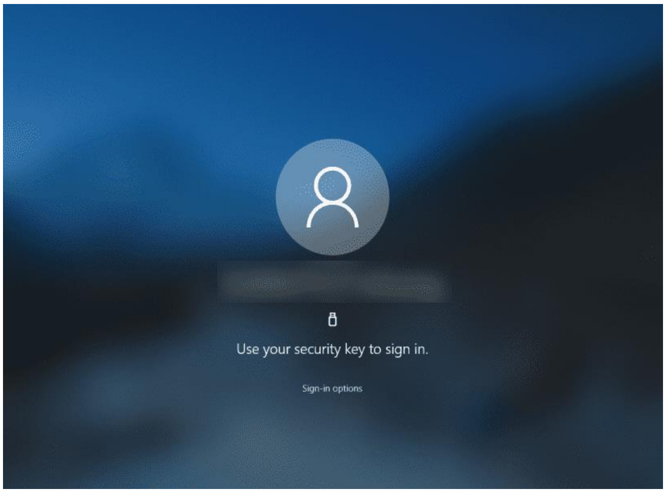
Lost device? Sign out everywhere

7. Online Usage of the Security Keys

1) Microsoft Azure

[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)



[redacted]

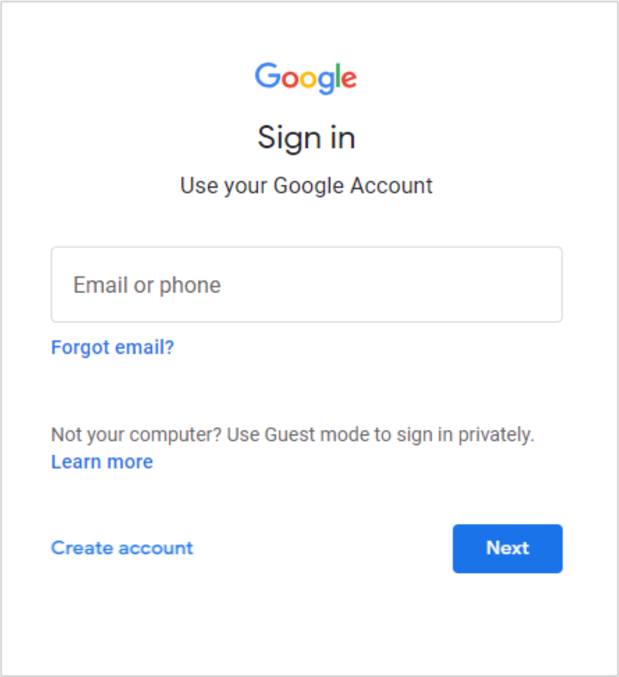
Use your security key to sign in.

7. Online Usage of the Security Keys

2) Google G-suite

[Security Key Registration]

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



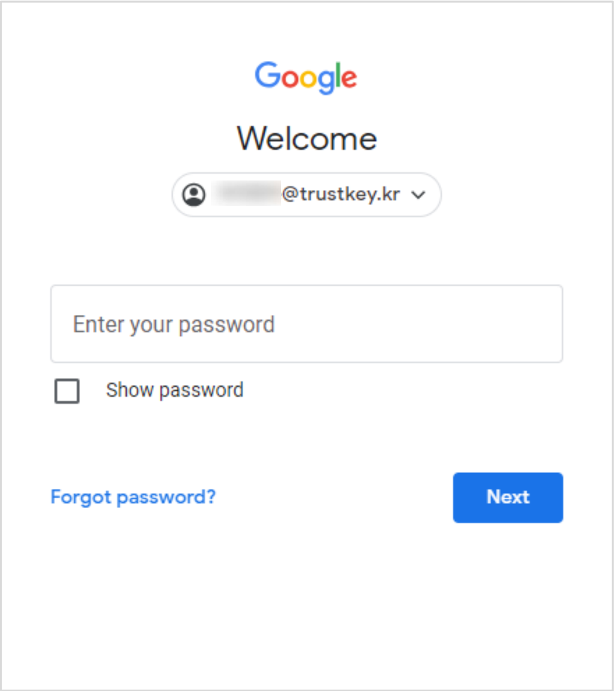
Google

Sign in

Use your Google Account

Email or phone

Not your computer? Use Guest mode to sign in privately. Learn more



Google

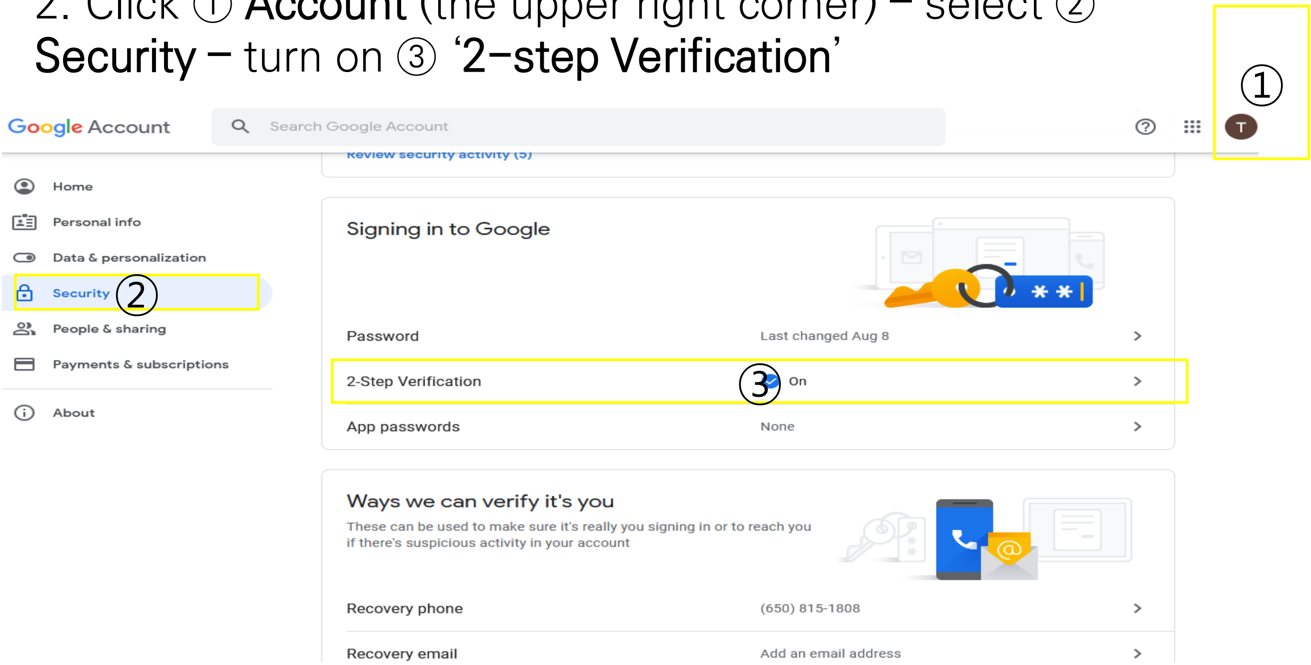
Welcome

[redacted]@trustkey.kr

Enter your password

□ Show password

2. Click ① **Account** (the upper right corner) – select ② **Security** – turn on ③ **'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

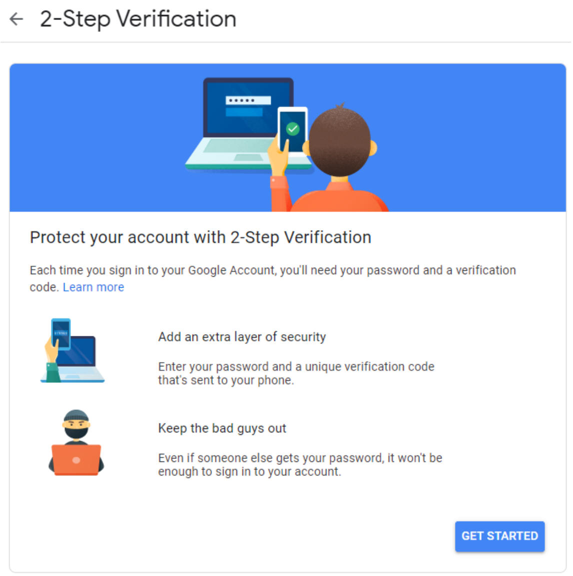
These can be used to make sure it's really you signing in or to reach you if there's suspicious activity in your account

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

7. Online Usage of the Security Keys

2) Google G-suite

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

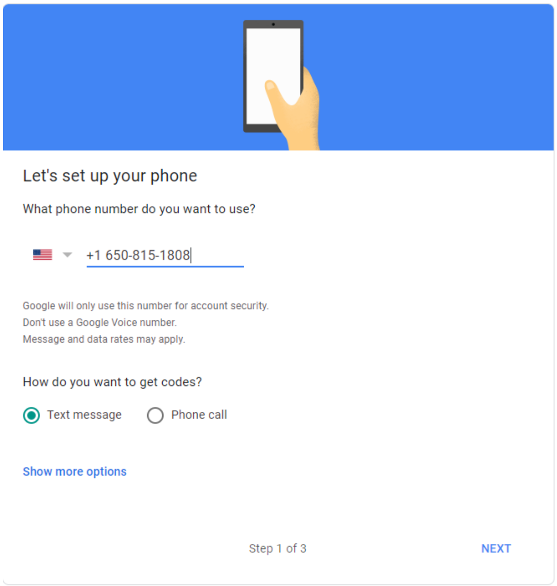
Add an extra layer of security

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.

GET STARTED



Let's set up your phone

What phone number do you want to use?

+1 650-815-1808

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?

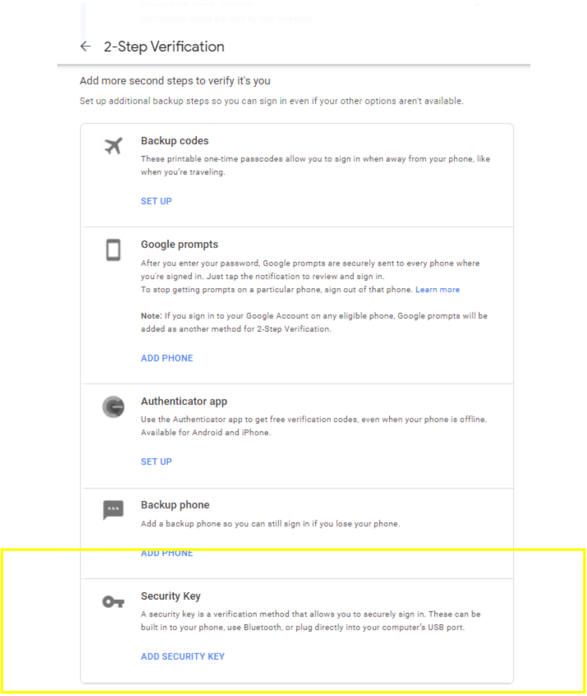
● Text message ○ Phone call

Show more options

Step 1 of 3

NEXT

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.

SET UP

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.

ADD PHONE

Authenticator app

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

SET UP

Backup phone

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

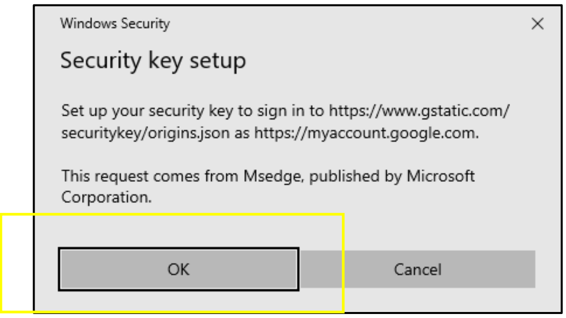
ADD PHONE

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.

ADD SECURITY KEY

5. Follow the browser’s instructions.

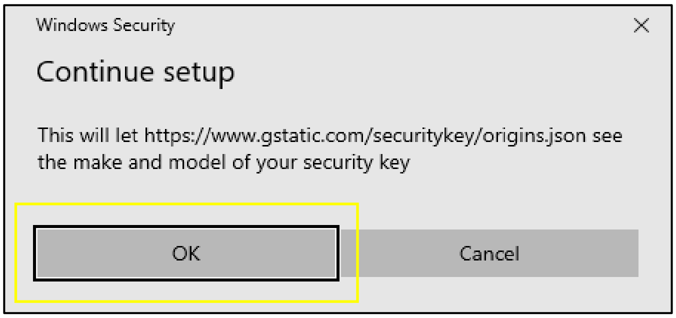


Windows Security

Security key setup

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

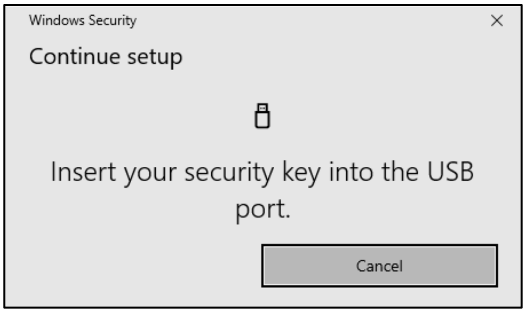
This request comes from Msedge, published by Microsoft Corporation.



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

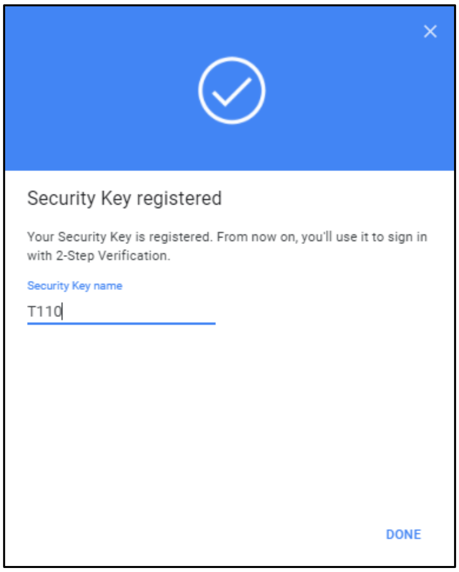
Continue setup

Insert your security key into the USB port.

7. Online Usage of the Security Keys

2) Google G-suite

6. After successful registration, the user needs to name the key.

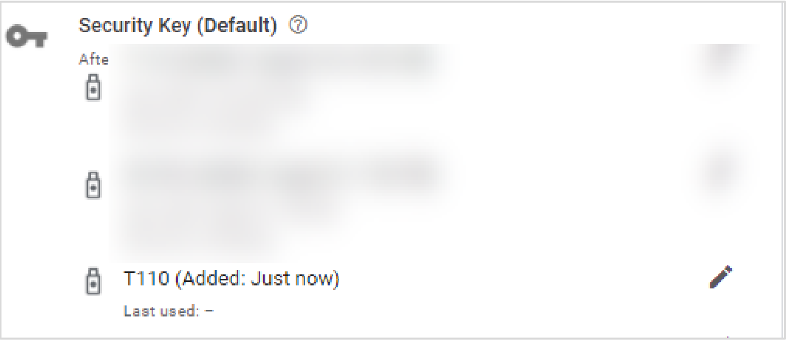


Security Key registered

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)

Afte

T110 (Added: Just now)

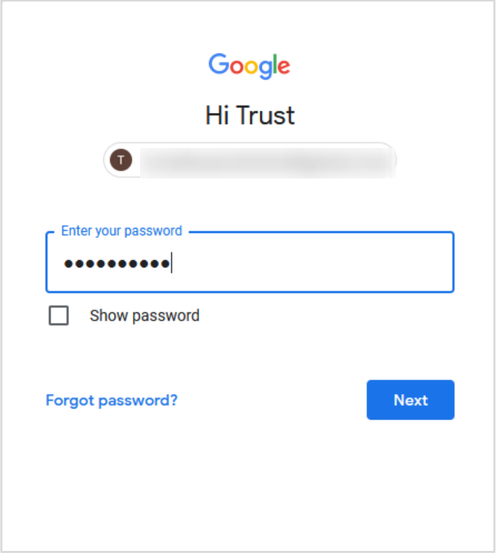
Last used: –

7. Online Usage of the Security Keys

2) Google G-suite

[Sign-in Google using Security Key]

1. The user now can sign in Gmail with the security key.



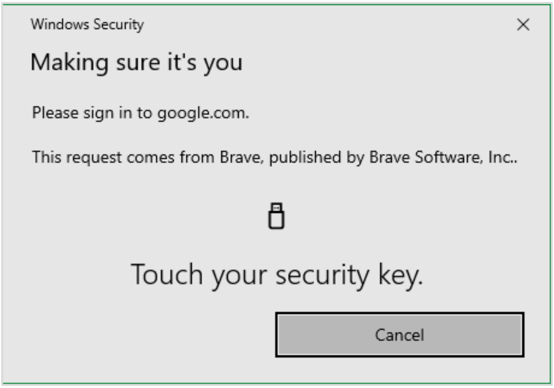
Google

Hi Trust

Enter your password

●●●●●●●●●●●

□ Show password



Windows Security

Making sure it's you

Please sign in to google.com.

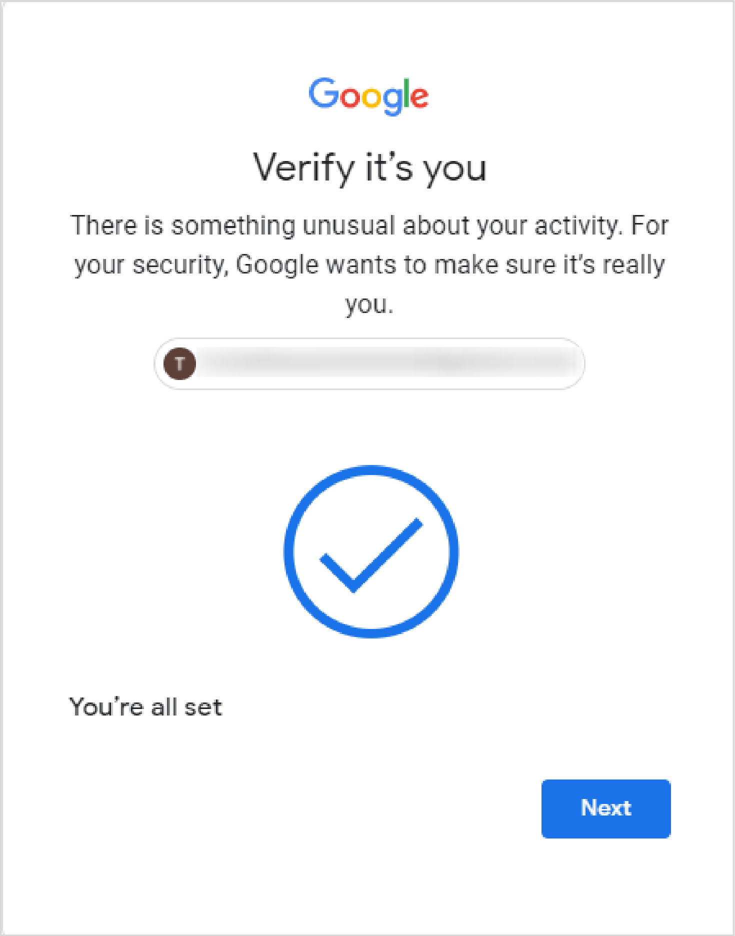
This request comes from Brave, published by Brave Software, Inc..

Touch your security key.

7. Online Usage of the Security Keys

2) Google G-suite

3. Touch the security key to complete login with two-step verification.



Google

Verify it's you

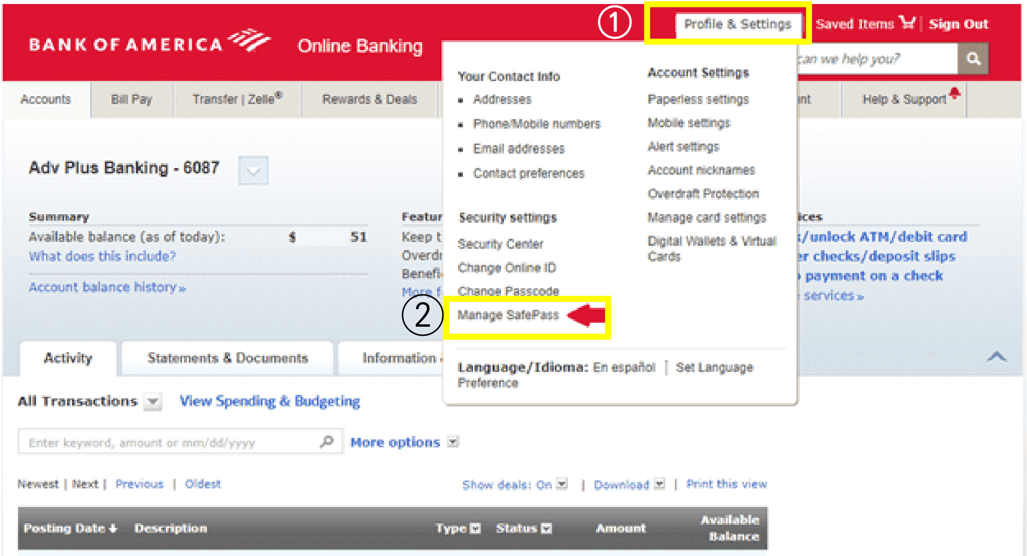
There is something unusual about your activity. For your security, Google wants to make sure it's really you.

You're all set

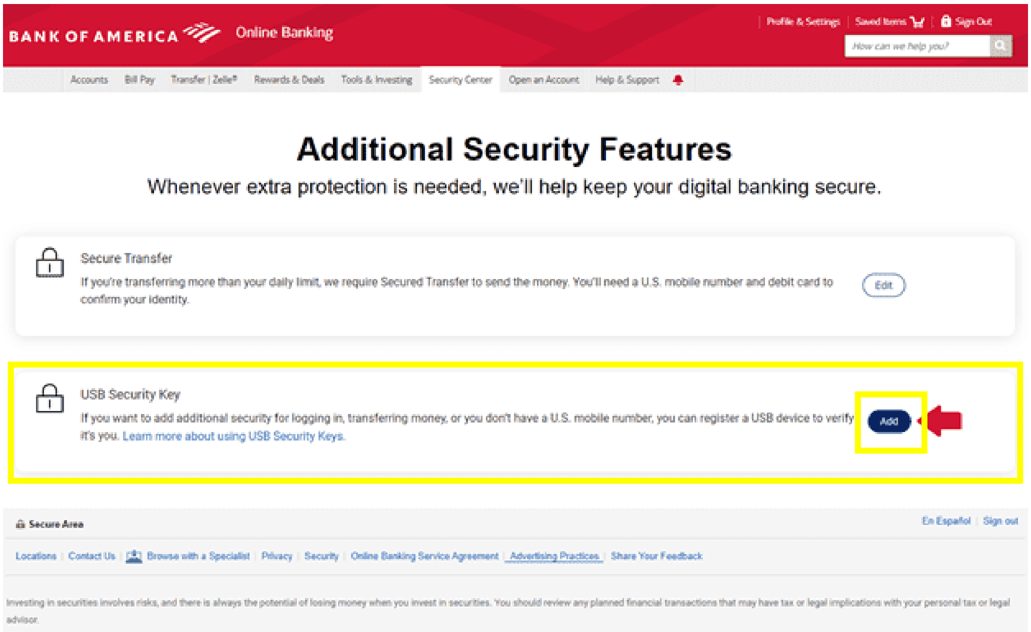
7. Online Usage of the Security Keys

3) Bank of America

1. After logging into your account, select ① **Profile & Setting** – ② **Manager SafePass.**



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.

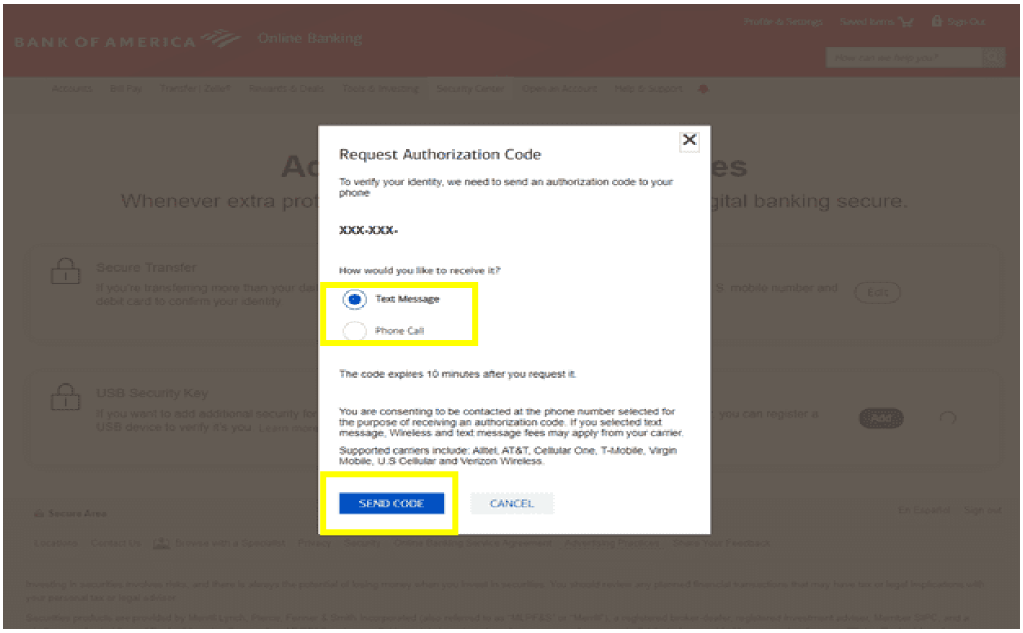
Add
Secure Area
En Español | Sign out
Locations | Contact Us | Browse with a Specialist | Privacy | Security | Online Banking Service Agreement | Advertising Practices | Share Your Feedback

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.

7. Online Usage of the Security Keys

3) Bank of America

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

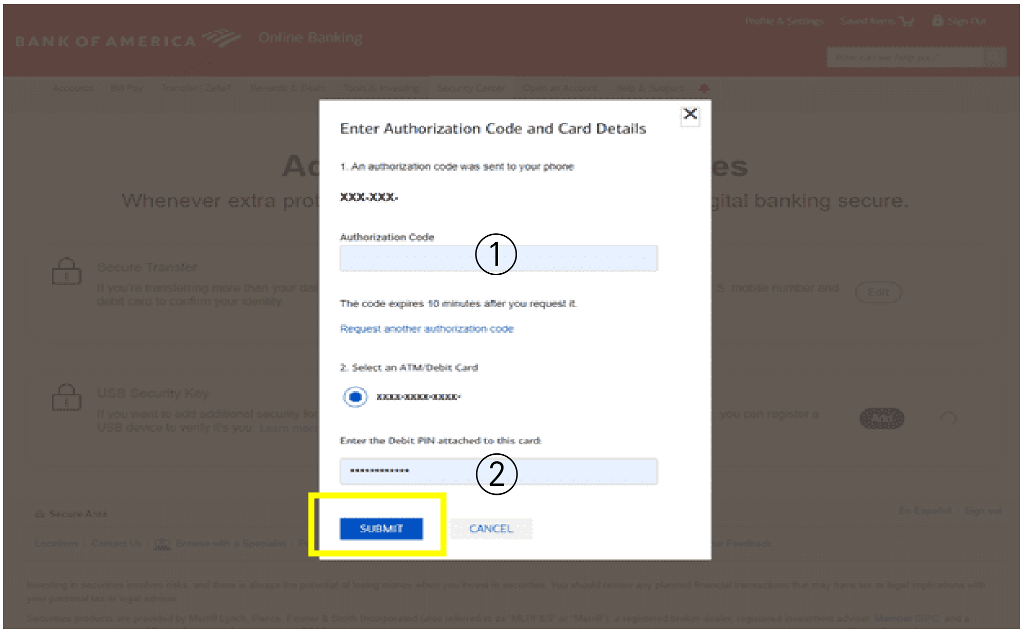
○ Phone Call

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.

4. Enter Authorization Code and Debit PIN then click [SUBMIT] button.



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

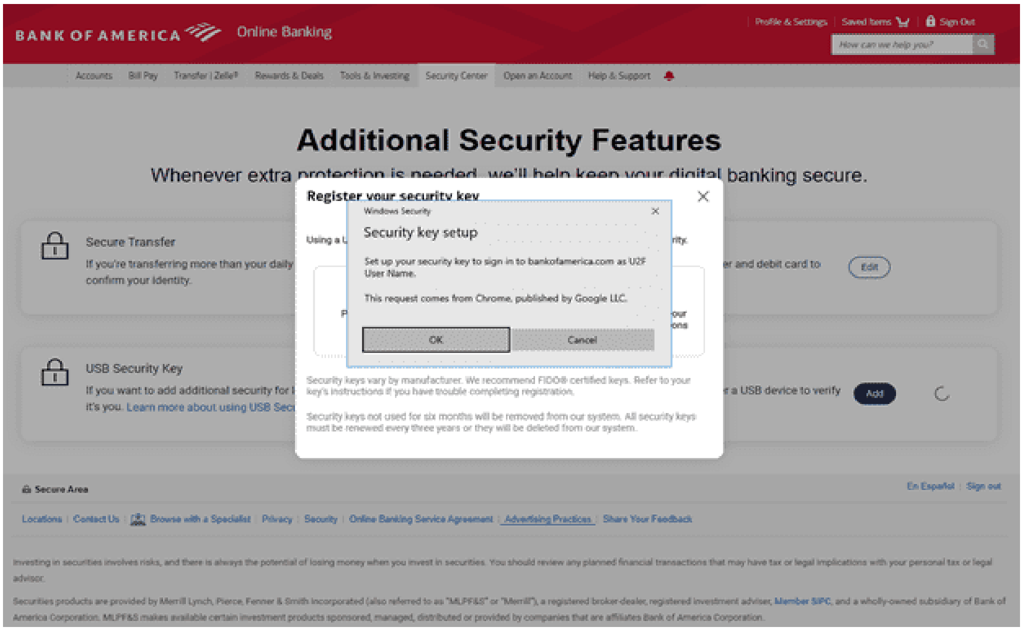
● XXXX-XXXX-XXXX-

Enter the Debit PIN attached to this card:

7. Online Usage of the Security Keys

3) Bank of America

5. Click [OK] to Security key setup popup.



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 ... r a USB device to verify it's you. Learn more about using USB Sec...

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.

OK | Cancel

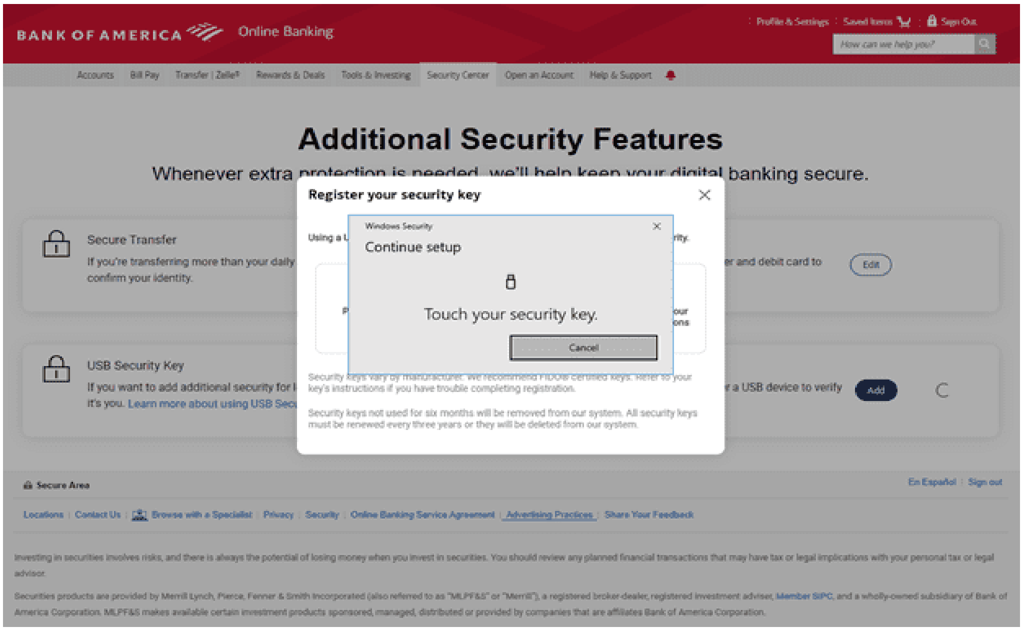
Security keys vary by manufacturer. We recommend FIDO® certified keys. Refer to your key's instructions if you have trouble completing registration.

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.

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.

6. Insert your security key and the touch the security key's sensor.



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 ... r a USB device to verify it's you. Learn more about using USB Sec...

Register your security key

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.

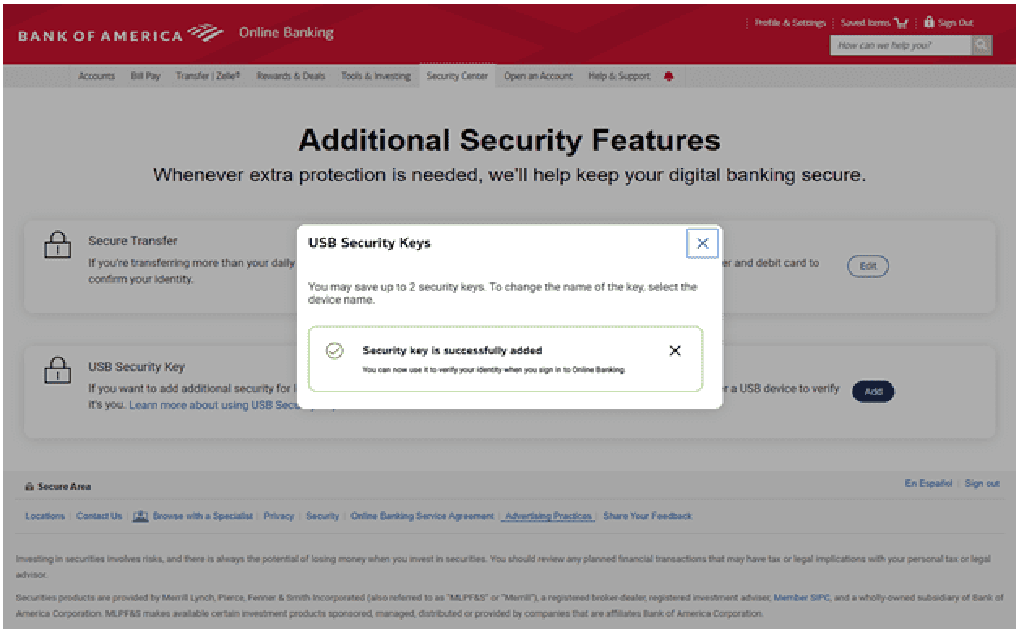
Investing in securities involves risks, and there is always the potential of losing money when you invest in securities. You should review any planned financial transactions that may have tax or legal implications with your personal tax or legal advisor.

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.

7. Online Usage of the Security Keys

3) Bank of America

7. 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.

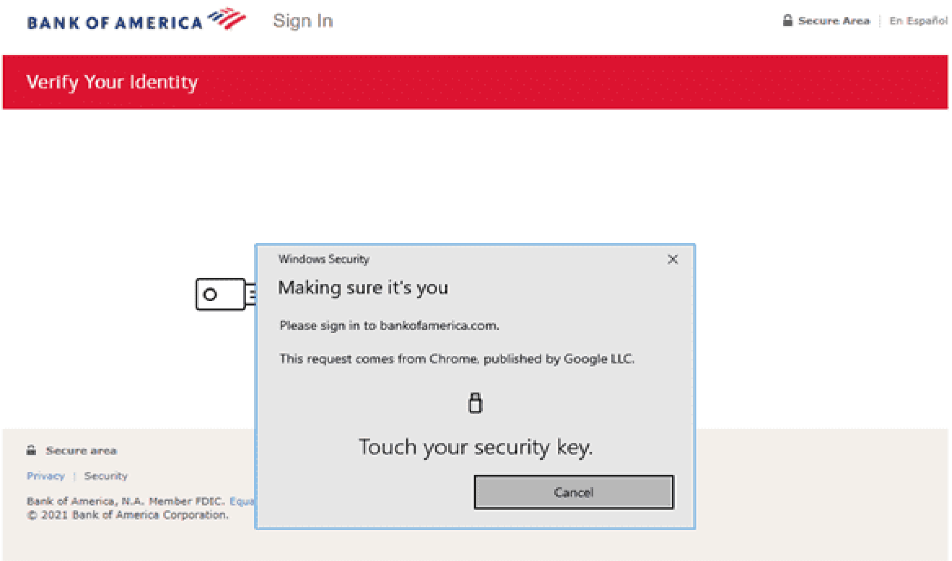
Security key is successfully added

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.

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



Verify Your Identity

Making sure it's you

Please sign in to bankofamerica.com.

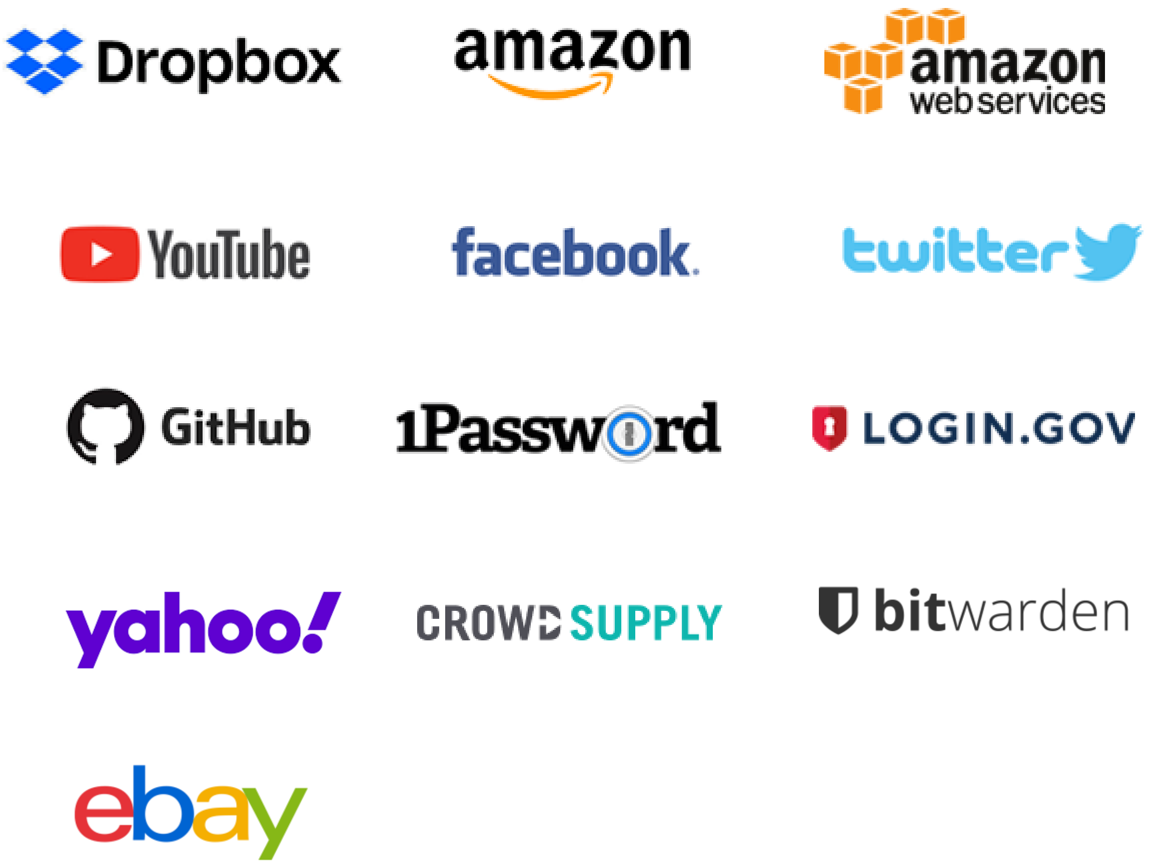
This request comes from Chrome, published by Google LLC.

Touch your security key.

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

7. Online Usage of the Security Keys

4) Other Online Services



Support is subject to change depending on the site operator's policy.

For more information, see the TrustKey homepage!
https://trustkey.kr/en/sub/support_app.form

2. Appendix

1. FAQ

Using T-Series Security Keys

1. How do you enroll your fingerprint to the T-series seuciryt key?
   T-series does not support fingerprint enrolment. Please use TrustKey G and B series security keys (G310H and G320H, B210 and B210H).
2. How many resident keys do T-Series keys hold?
   T-Series keys can hold up to 150 resident keys.
3. How many TOTP accounts can T-series support?
   T-Series keys can hold up to 50 TOTP accounts.
4. Can I use T110 or T120 for Bank of America?
   Yes. T-series (T110/T120) supports Bank of America authentication mechanism.
5. 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.
6. 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

1. Which OS does Key Manager support?
   Key Manager supports Windows, macOS, and Linux
2. 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.
3. 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.
4. 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.

1. FAQ

T-Series Security Key Features

1. 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 in to Azure joined Windows PC online or offline/airplane mode.

2. 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.**

3. 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.

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.)

4. Manufacturer Information

Manufacturer

Manufacturer	TrustKey Co., Ltd.
Technical Support	TEL : +82-2-556-7878 / email : support@trustkey.kr
Webpages	www.trustkey.kr/
Addresses	(06236) 2F, 14, Teheran-ro 22-gil, Gangnam-gu, Seoul, Korea

Copyright

5. 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

TrustKey H.Q Customer Service

+82-2-556-7878

- Please provide the model number of the TrustKey security key you are using and the symptoms of the error so we can provide a faster and more accurate response.

Contact Us [Online]

trustkey.kr/en/sub/support.form

- Download the latest user manuals and applications for your product.

trustkey.kr/en/sub/contactus.form

- You can make sales/technical support and after-sales service inquiries about our products online.