

TRUSTKEY
BioManager

User Manual

Ver 3.3

Contents

- 1. **Overview** [3](#)

- 2. **LED Indicators** [4](#)

- 3. **How to Use BioManager™** [5](#)
 - Install TrustKey BioManager™ [5](#)
 - How to Enroll Fingerprint [6](#)
 - How to Add Additional Fingerprint Information [11](#)
 - How to Remove Fingerprints [14](#)
 - How to Change PIN [16](#)
 - How to Factory Reset [18](#)
 - How to Unlock When PIN Code Verification Fails [24](#)
 - How to Unlock Fingerprint Recognition Fails [29](#)
 - BioManager™ Version Number and Product Image [31](#)

- 4. **Windows 10 Security Key Manager** [33](#)

- 5. **FCC Warning Statements** [34](#)

Overview

TRUSTKEY's G-series security key is a FIDO2 certified authenticator designed based on TRUSTKEY's powerful microprocessor MS500 and a fingerprint sensor with a world-leading fingerprint recognition algorithm.

G-series keys support the new FIDO2 standard so that one can enjoy the benefit of fast login with a strong protection against phishing, account takeover and many other online attacks.

The user needs to run TrustKey BioManager™ application to enroll your fingerprints on the key. You can download the application from our website:

<https://www.trustkeysolutions.com/support/BioManager/>

LED Indicators

The device LED has the following colors : Red, Green, Blue, Light blue, Amber and White.

▪ Common Mode



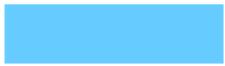
- Device connected
- Fingerprint recognition successful



- Waiting for fingerprint (blinking)



- Device locked due to fingerprint failure (non-blinking)
- Operation failure (blinking)



- Waiting for finger touch in Factory Reset Mode (blinking)

▪ FIDO2 Mode



- FIDO2 login ready (blinking)

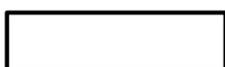


- FIDO2 login ready using device without registered fingerprint (blinking)

▪ U2F Mode



- U2F login ready (blinking)

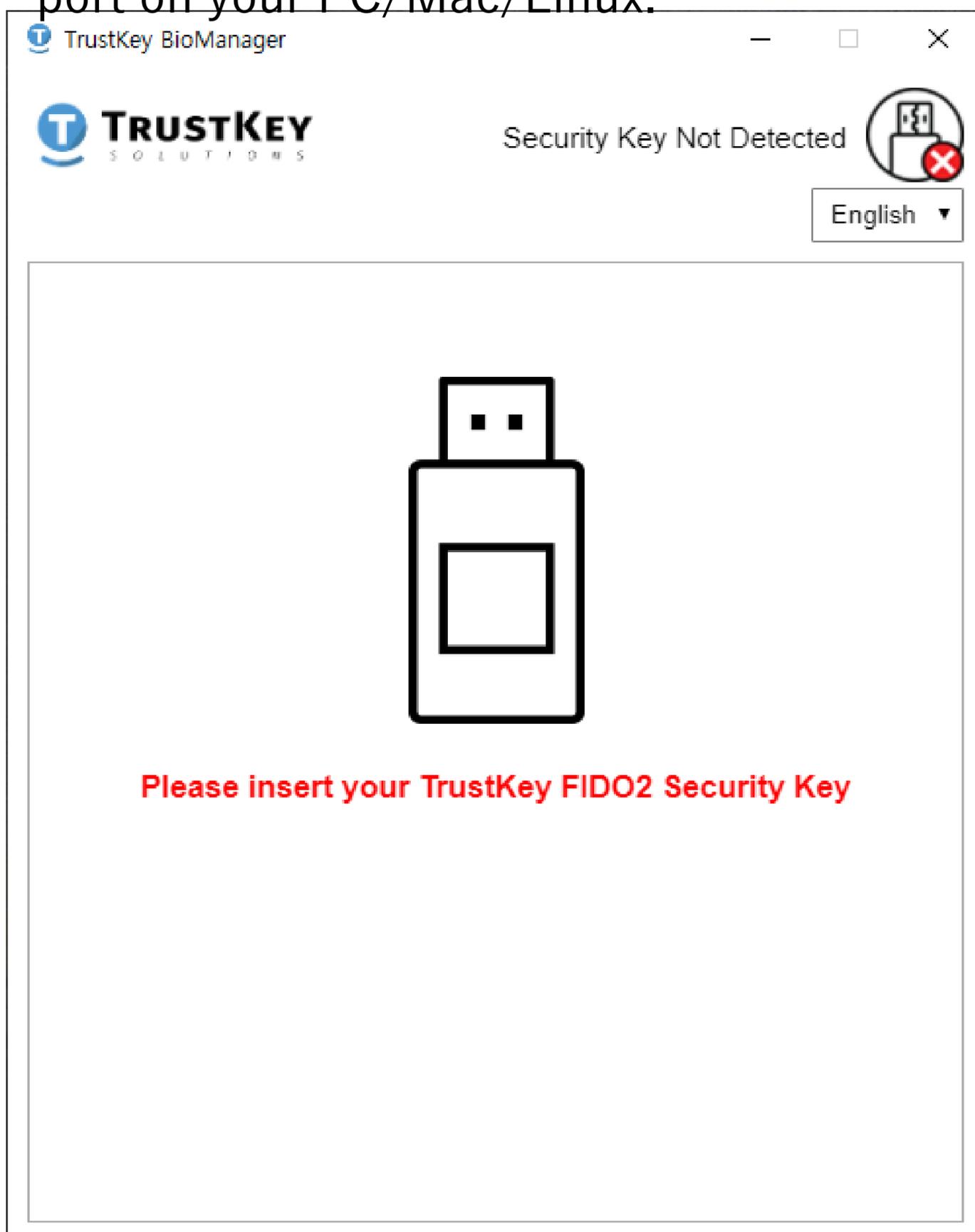


- U2F login ready using device without registered fingerprint (blinking)

Install

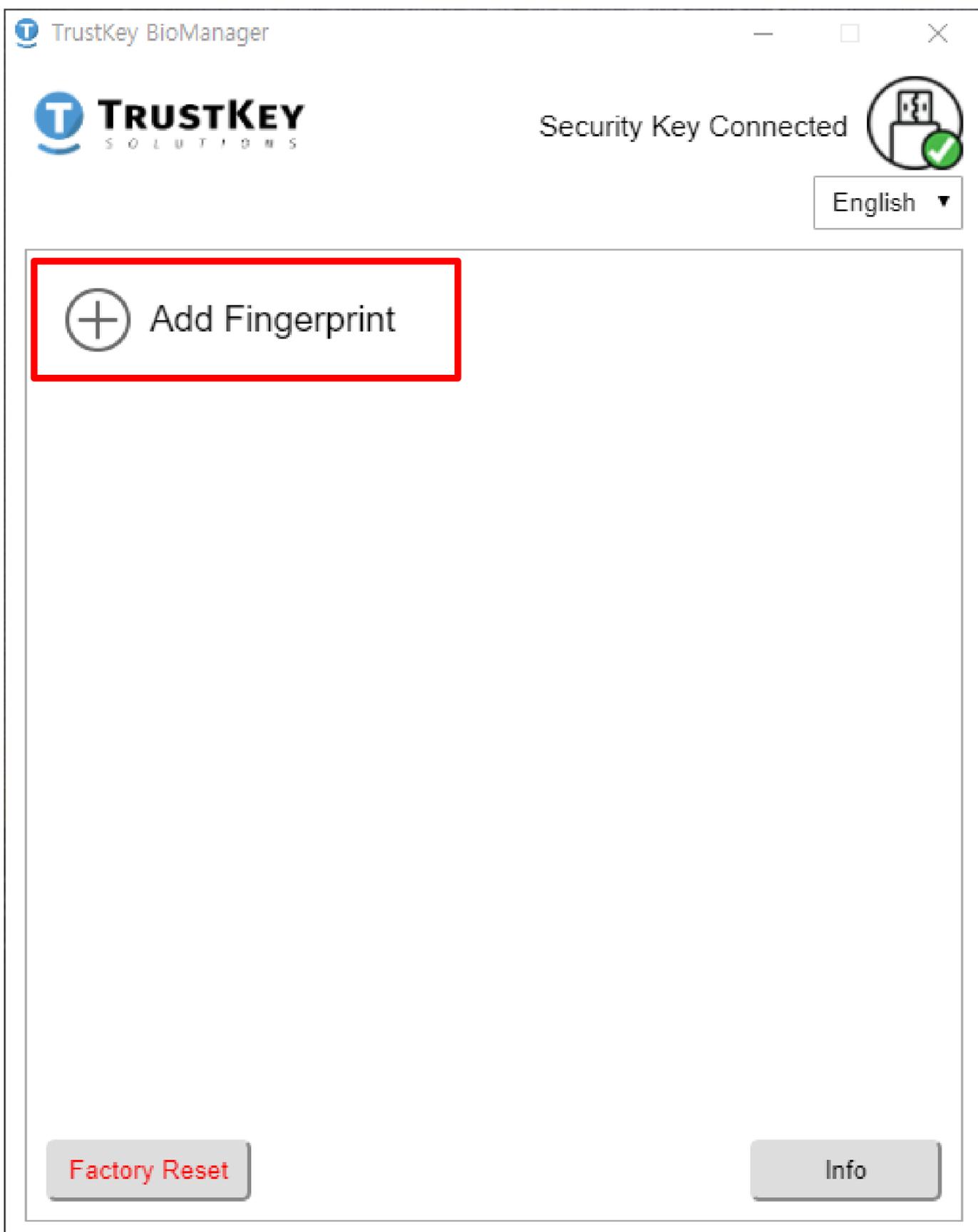
TrustKey BioManager™

1. Make sure that TrustKey BioManager™ application is downloaded on your PC/Mac/Linux.
<https://www.trustkeysolutions.com/support/BioManager/>
2. Launch the TrustKey BioManager™ application. If you see the following screen, plug your G-series security key into the USB port on your PC/Mac/Linux.



How to Enroll Fingerprint

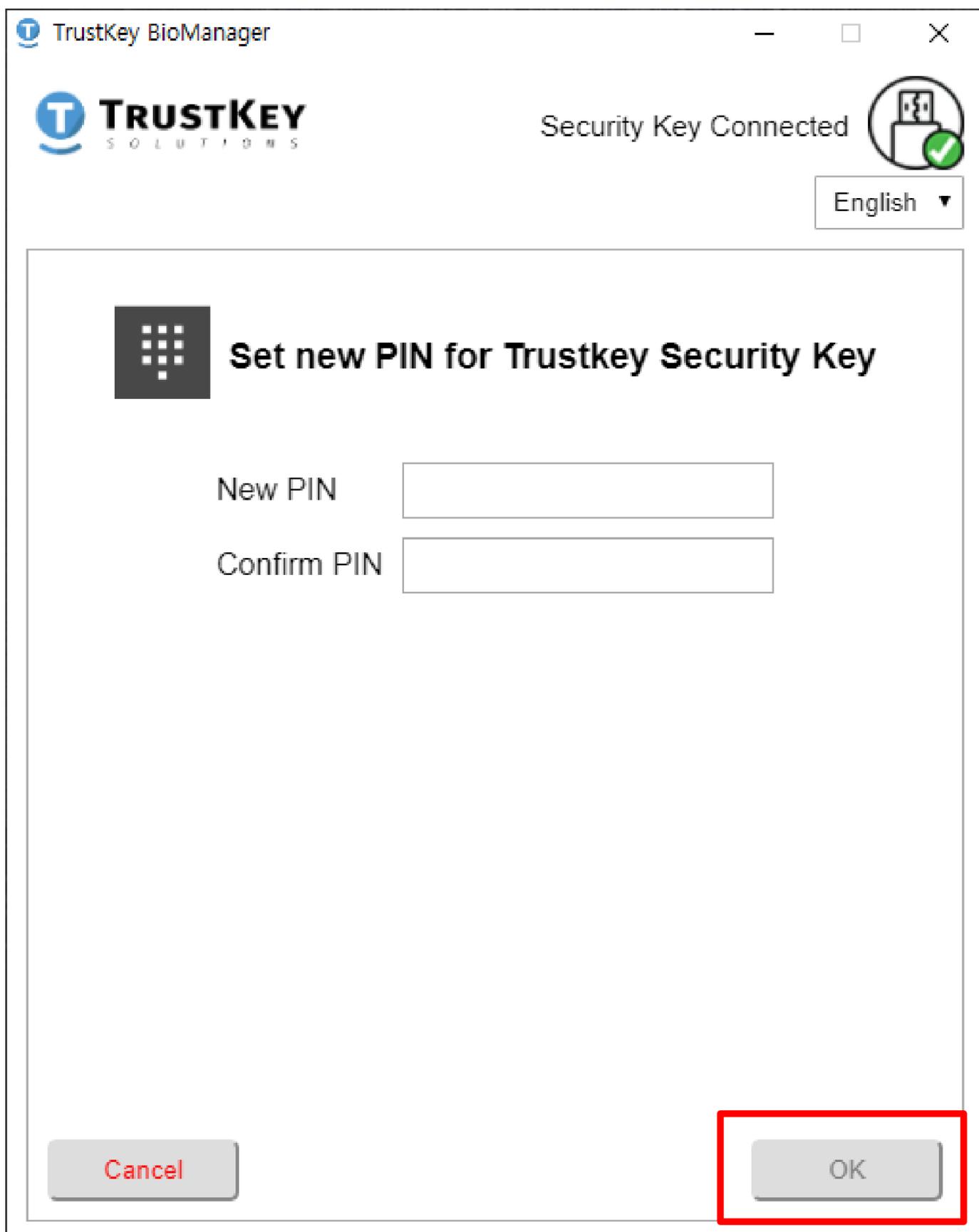
1. Click the ⊕ **Add Fingerprint** and the enrollment process will start. (Up to 3 fingerprints can be added.)



How to Enroll Fingerprint

2. Create a PIN and then click **OK**.

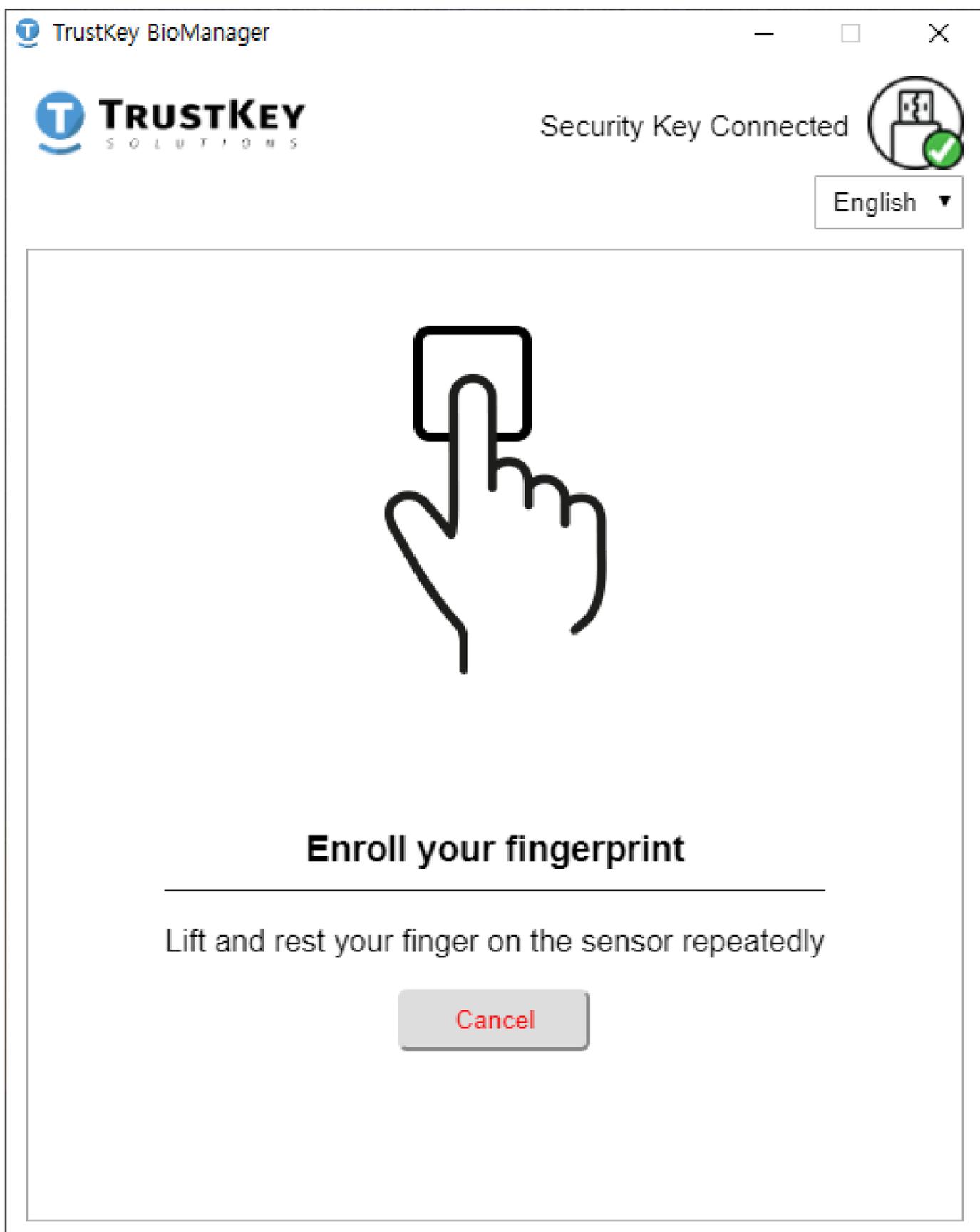
(PIN code must be at least 4 characters and maximum 64 characters long.)



The screenshot shows the TrustKey BioManager application window. The title bar reads "TrustKey BioManager". The interface includes the TrustKey logo, the text "Security Key Connected" with a USB key icon and a green checkmark, and a language dropdown menu set to "English". The main content area is titled "Set new PIN for Trustkey Security Key" and features a grid icon. Below the title are two input fields: "New PIN" and "Confirm PIN". At the bottom of the window, there are two buttons: "Cancel" on the left and "OK" on the right. The "OK" button is highlighted with a red rectangular border.

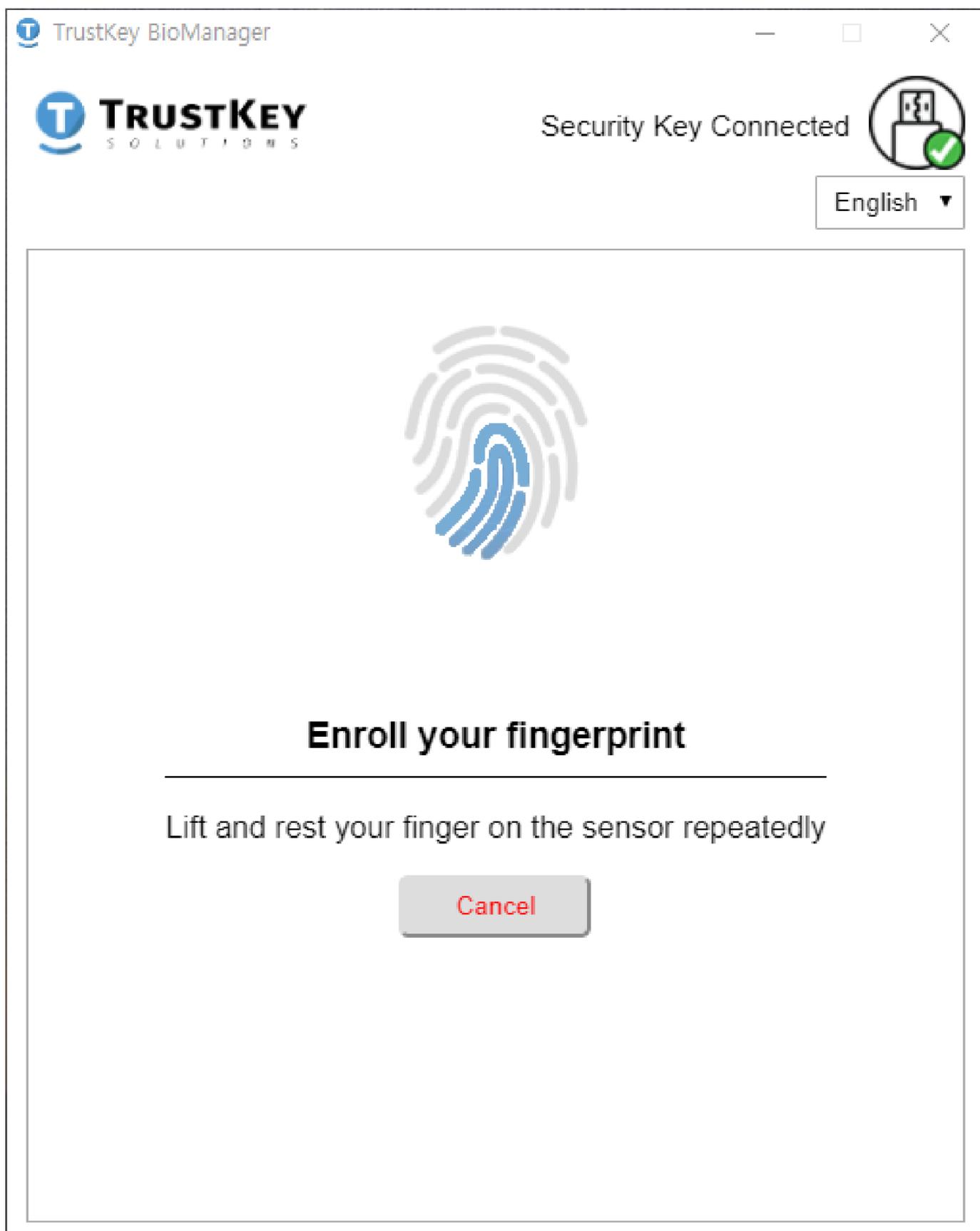
How to Enroll Fingerprint

3. When **blue** color LED is blinking, start enrolling your fingerprint following instructions on the screen.



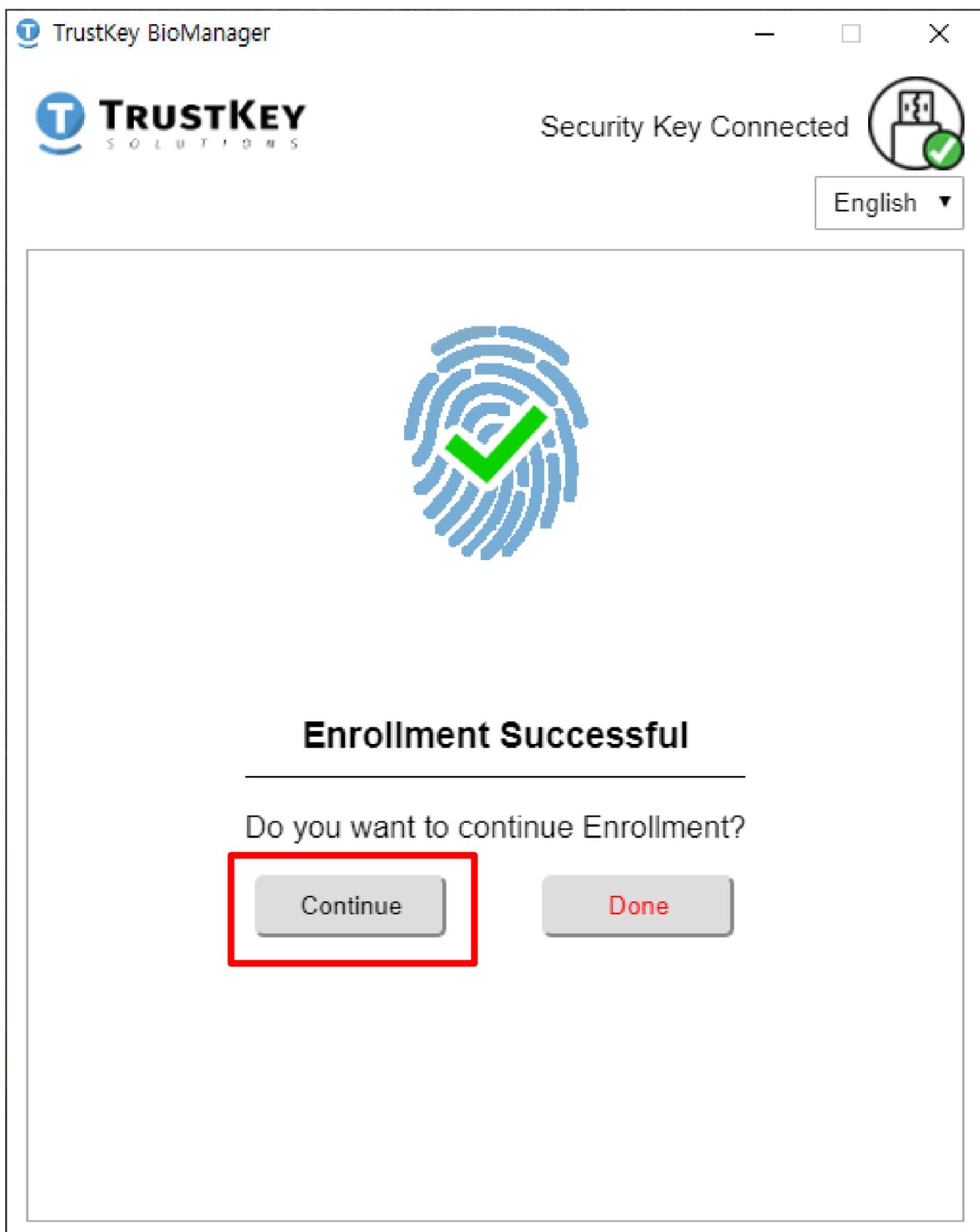
How to Enroll Fingerprint

4. Lift and rest your finger on the sensor repeatedly.



How to Enroll Fingerprint

5. Continue to lift and rest your finger on the sensor repeatedly until it is completed.



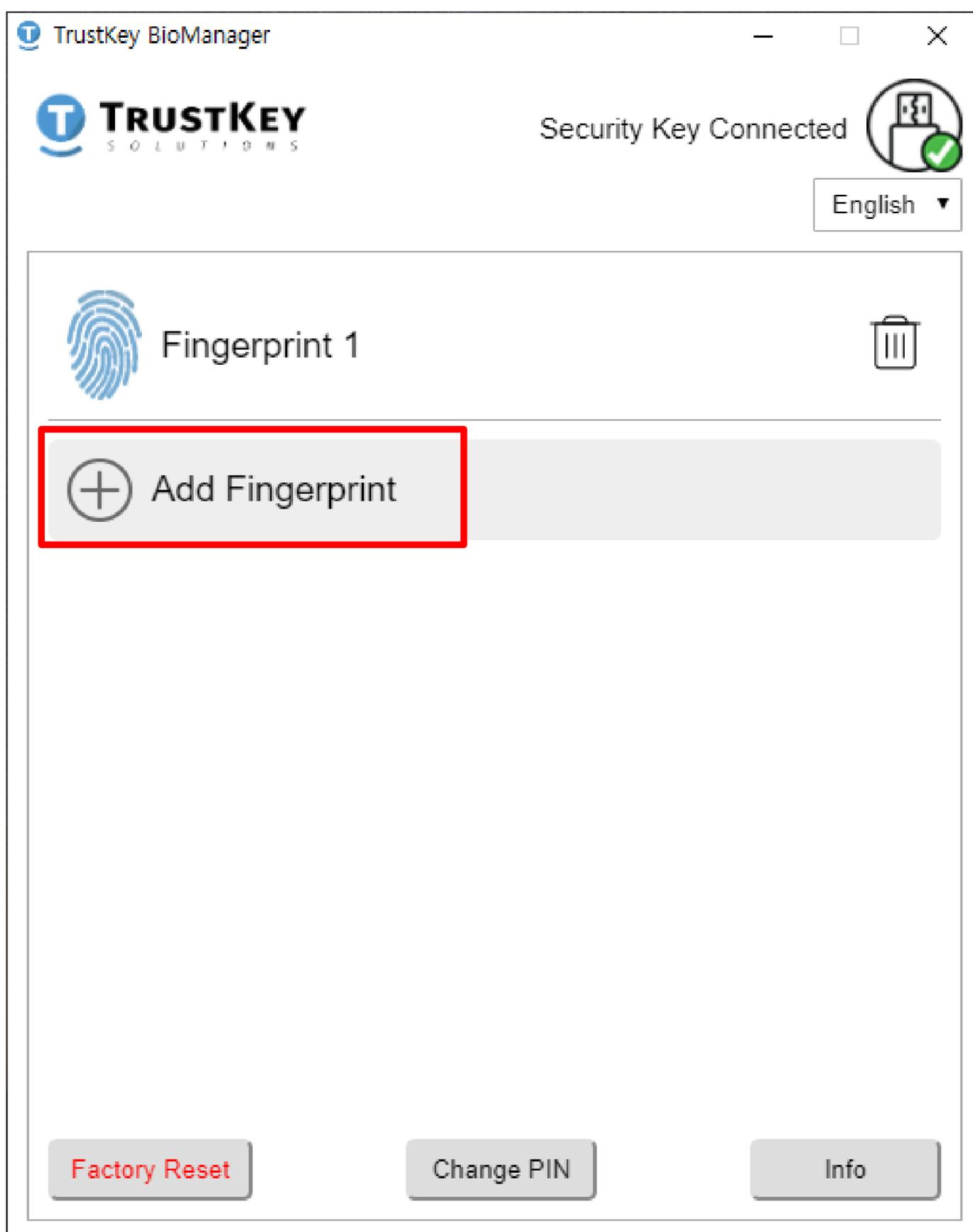
NOTE :

Click **Continue** button if you want to add another fingerprint. Or click 'Done' button if you want to stop enrolling.

*When you continue enrolling, no additional PIN code is required.

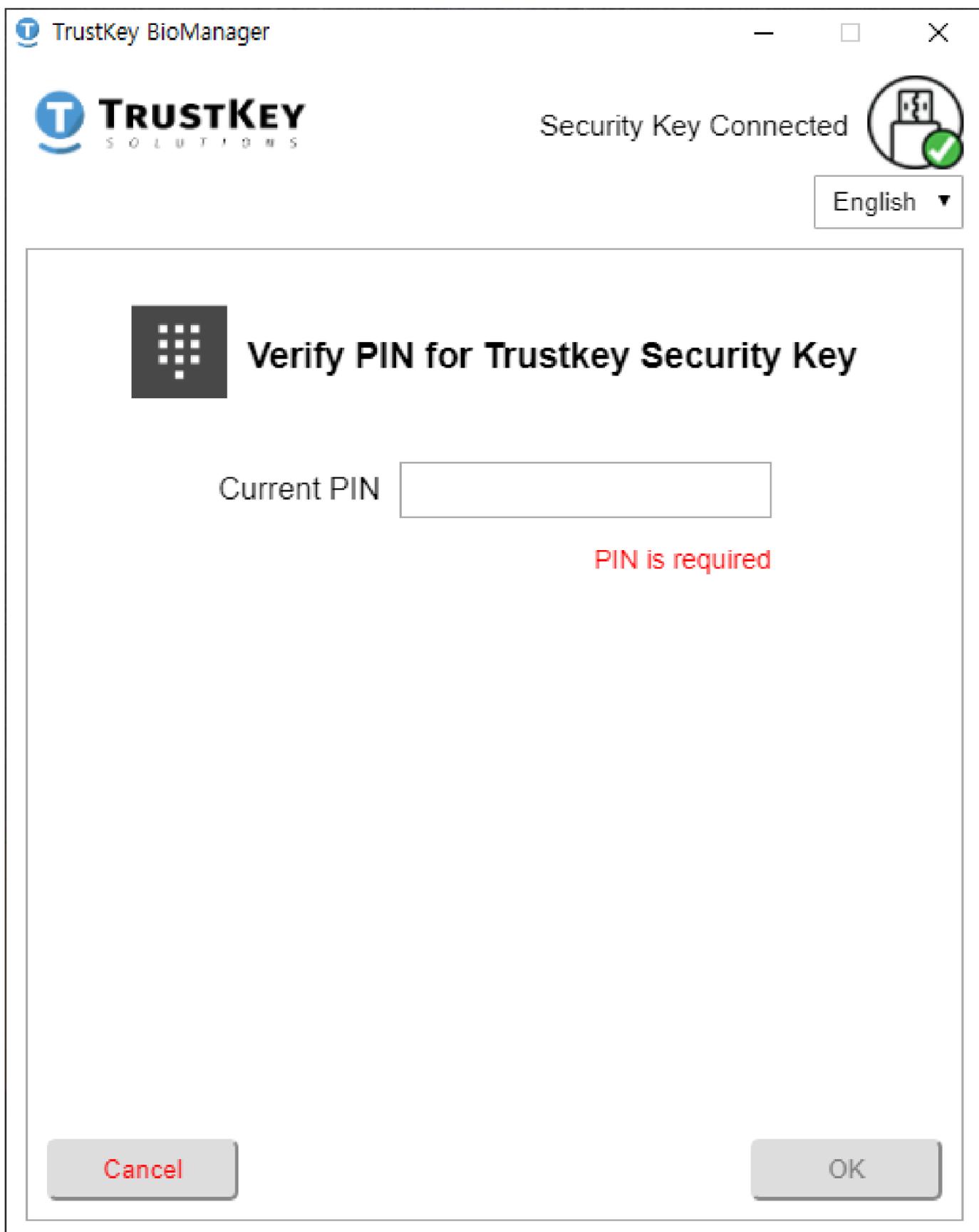
How to Add Additional Fingerprint Information

1. It is possible to add additional fingerprint(s). When you click the **⊕ Add fingerprint** you will be asked to verify your PIN code.



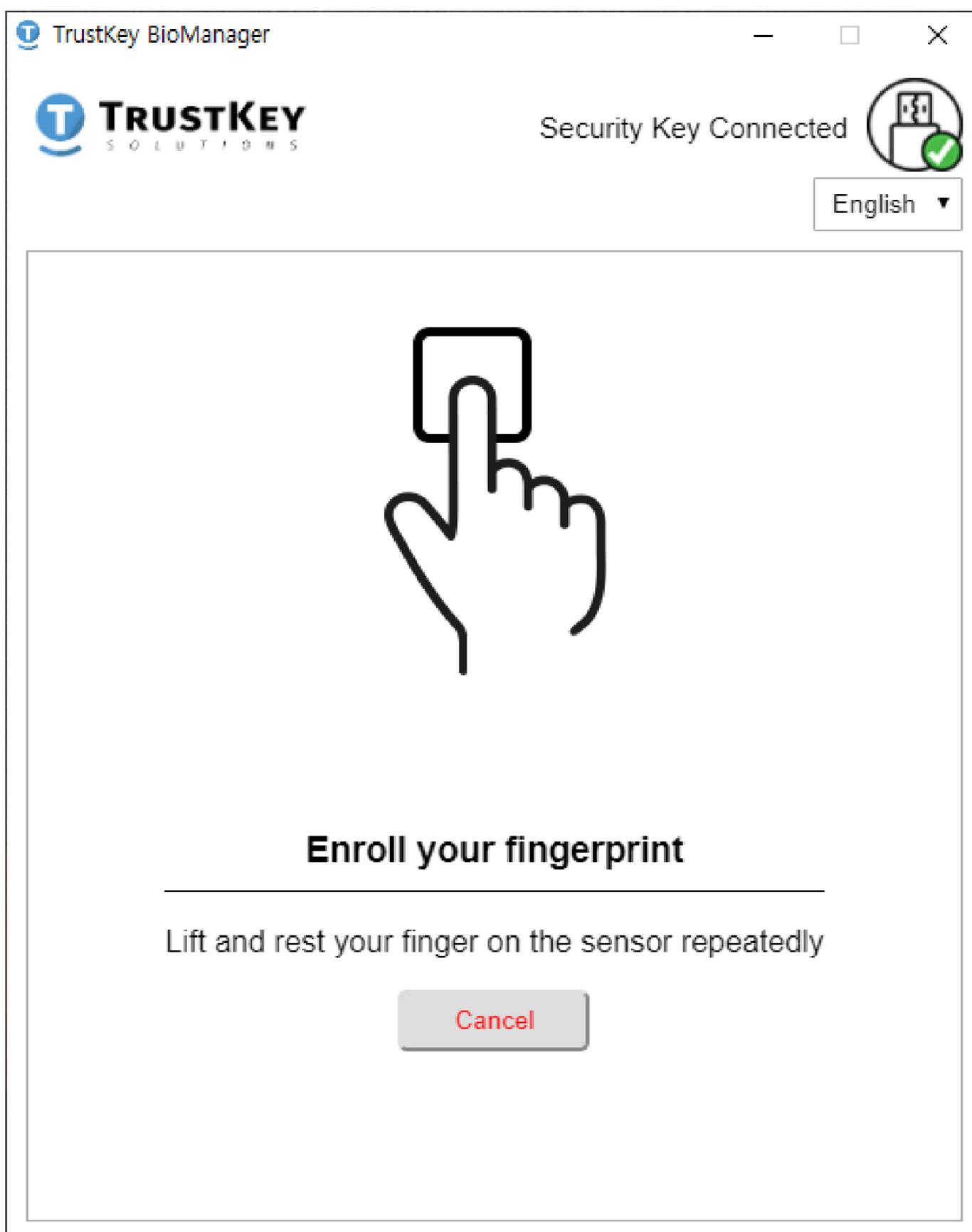
How to Add Additional Fingerprint Information

2. Once the PIN is verified, the enrollment process will start. (Total of 3 fingerprints can be enrolled.)



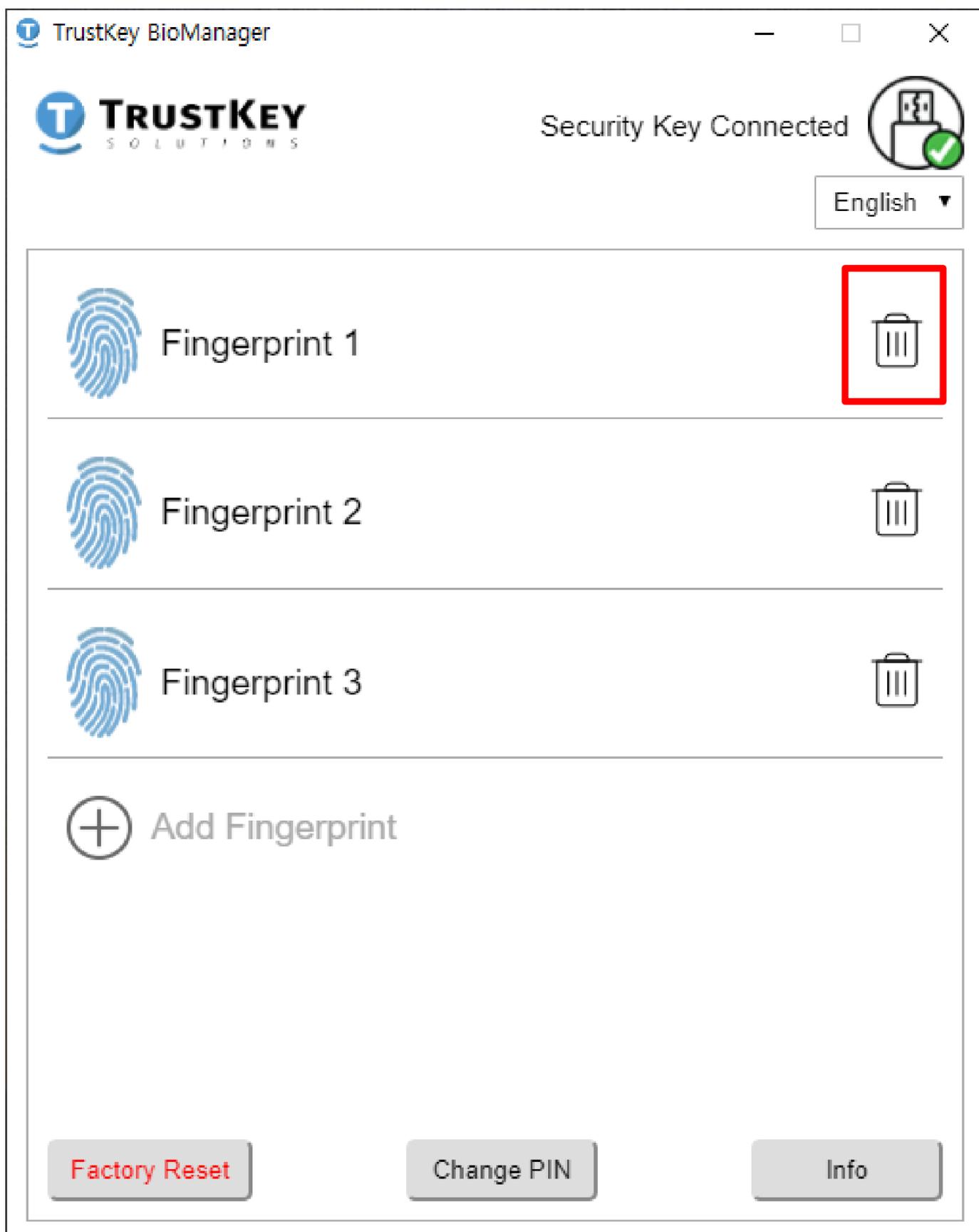
How to Add Additional Fingerprint Information

3. When **blue** color LED is blinking, start enrolling your fingerprint following instructions on the screen.



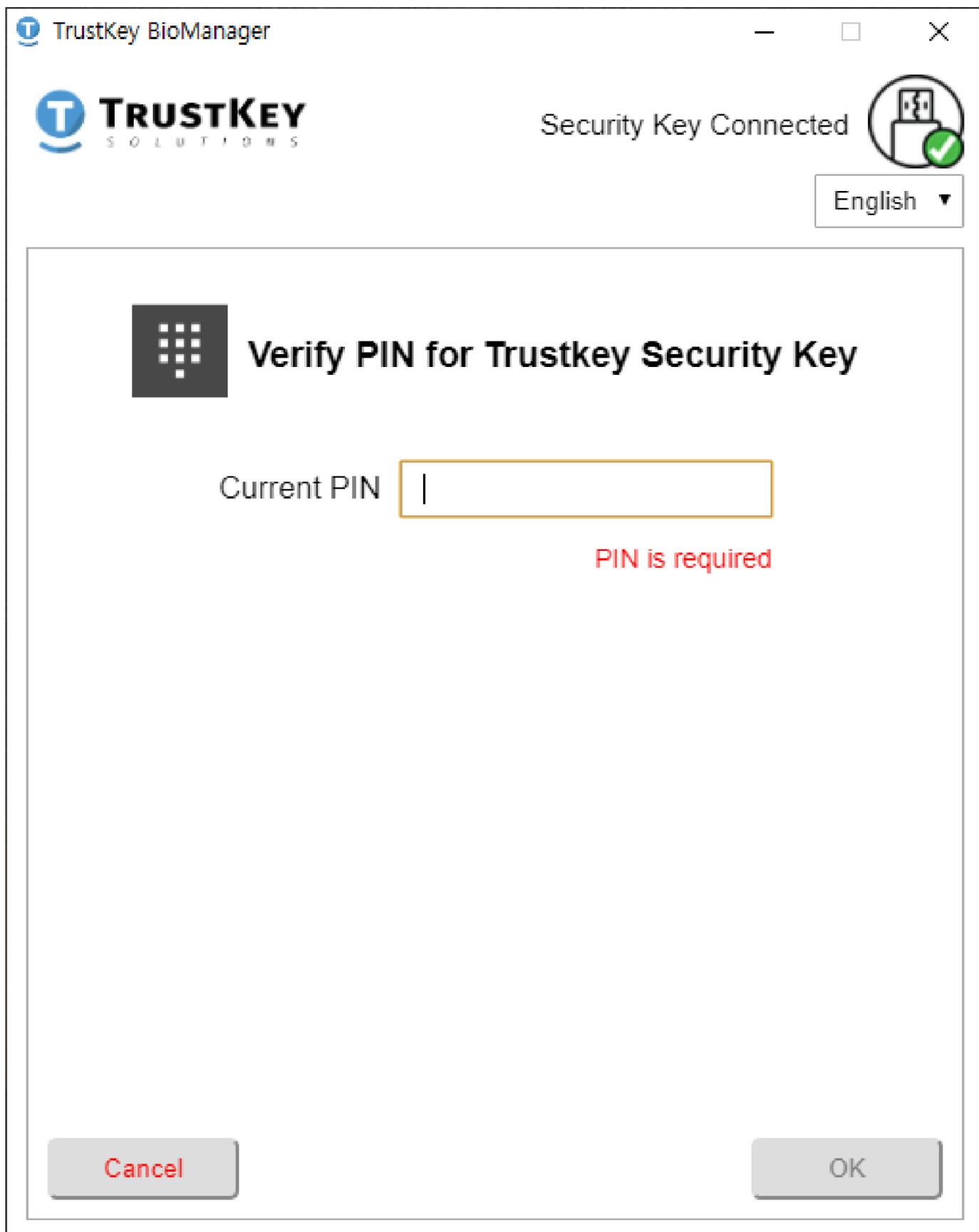
How to Remove Fingerprints

1. Click the trash bin()to remove registered fingerprint.



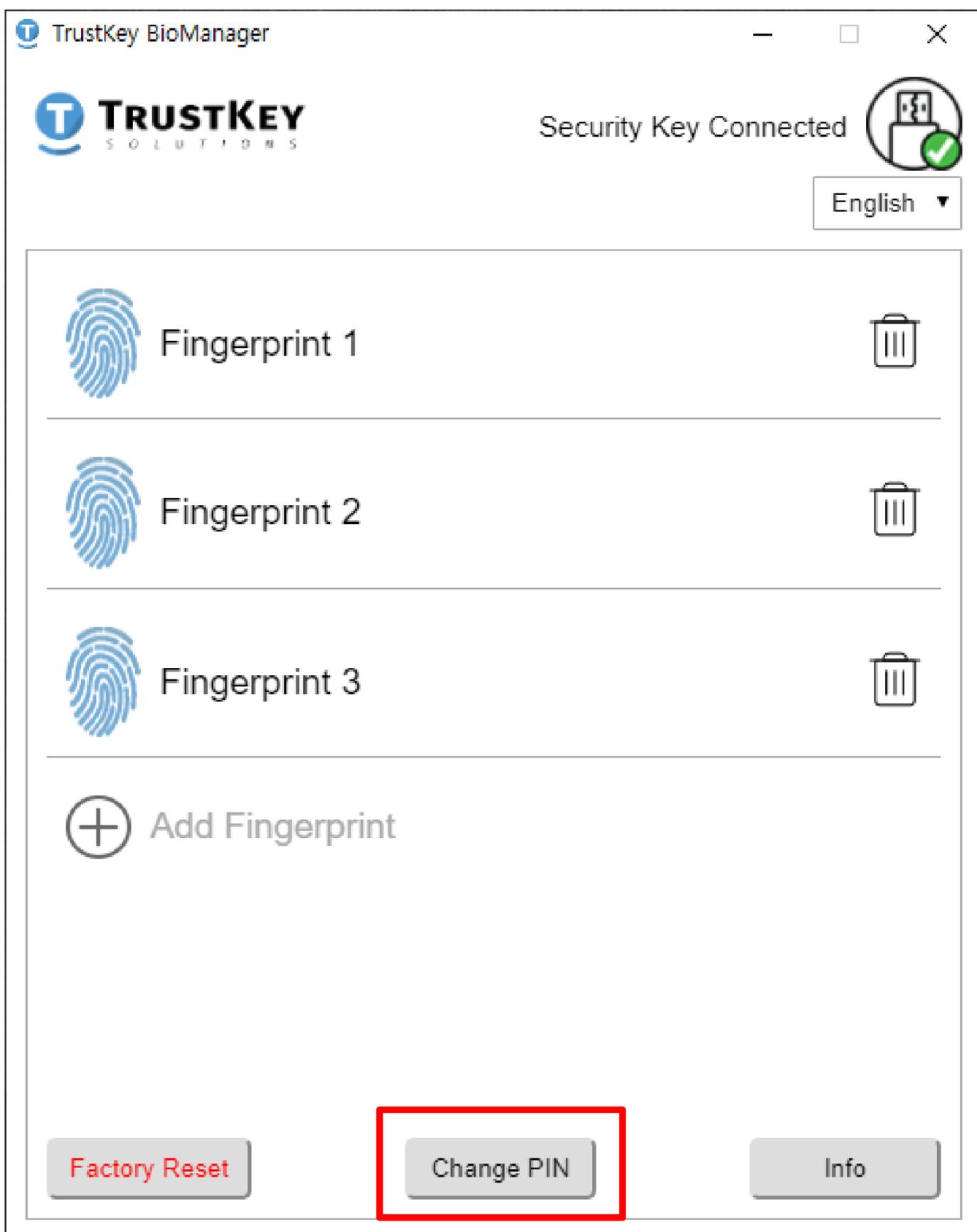
How to Remove Fingerprints

2. Enter the PIN code to remove the fingerprint data.



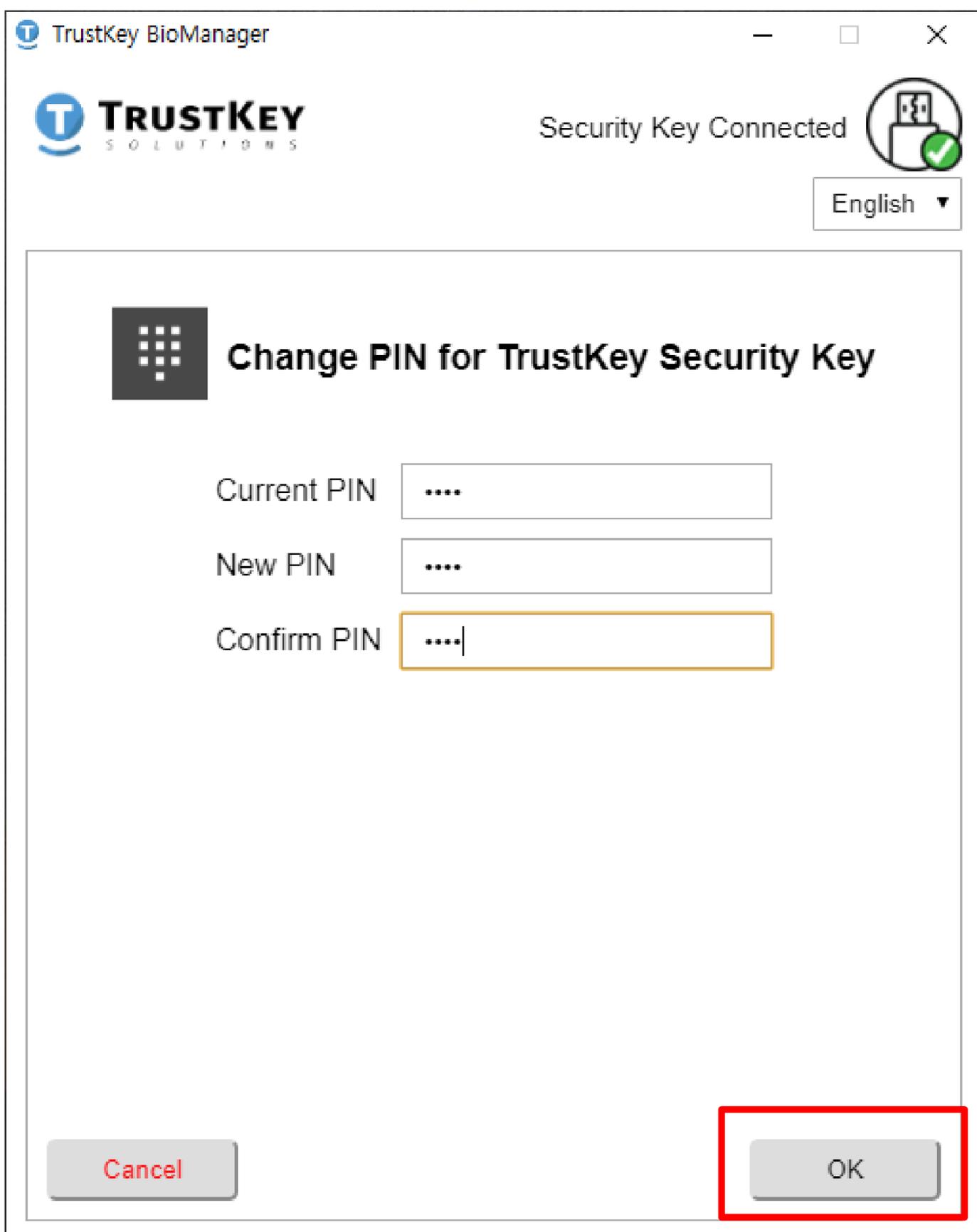
How to Change PIN

1. Click **Change PIN** button to change the PIN code.



How to Change PIN

2. Enter the current PIN code and then enter the new PIN code and click **OK** button.



TrustKey BioManager

TRUSTKEY
SOLUTIONS

Security Key Connected 

English ▾

Change PIN for TrustKey Security Key

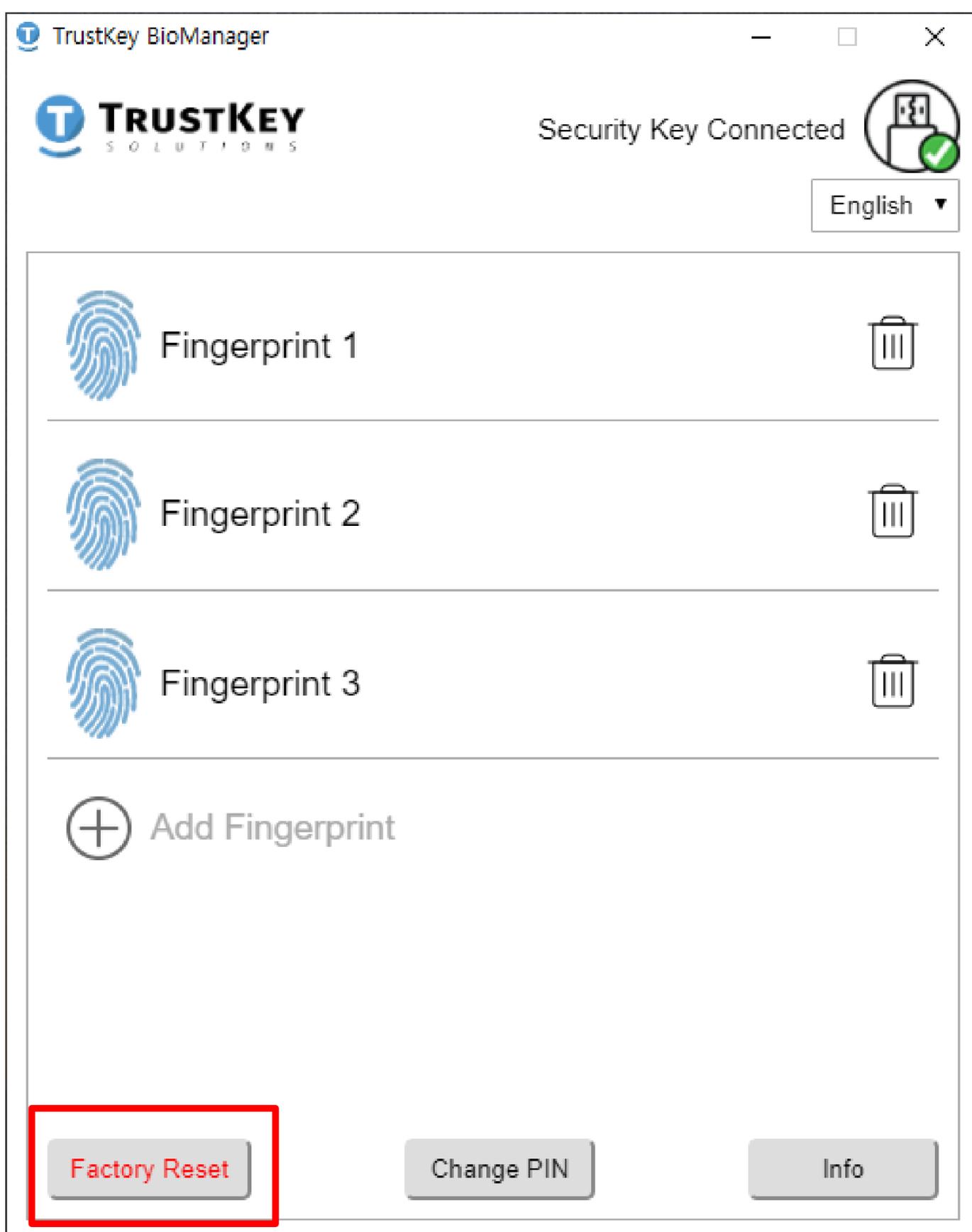
Current PIN

New PIN

Confirm PIN

How to Factory Reset

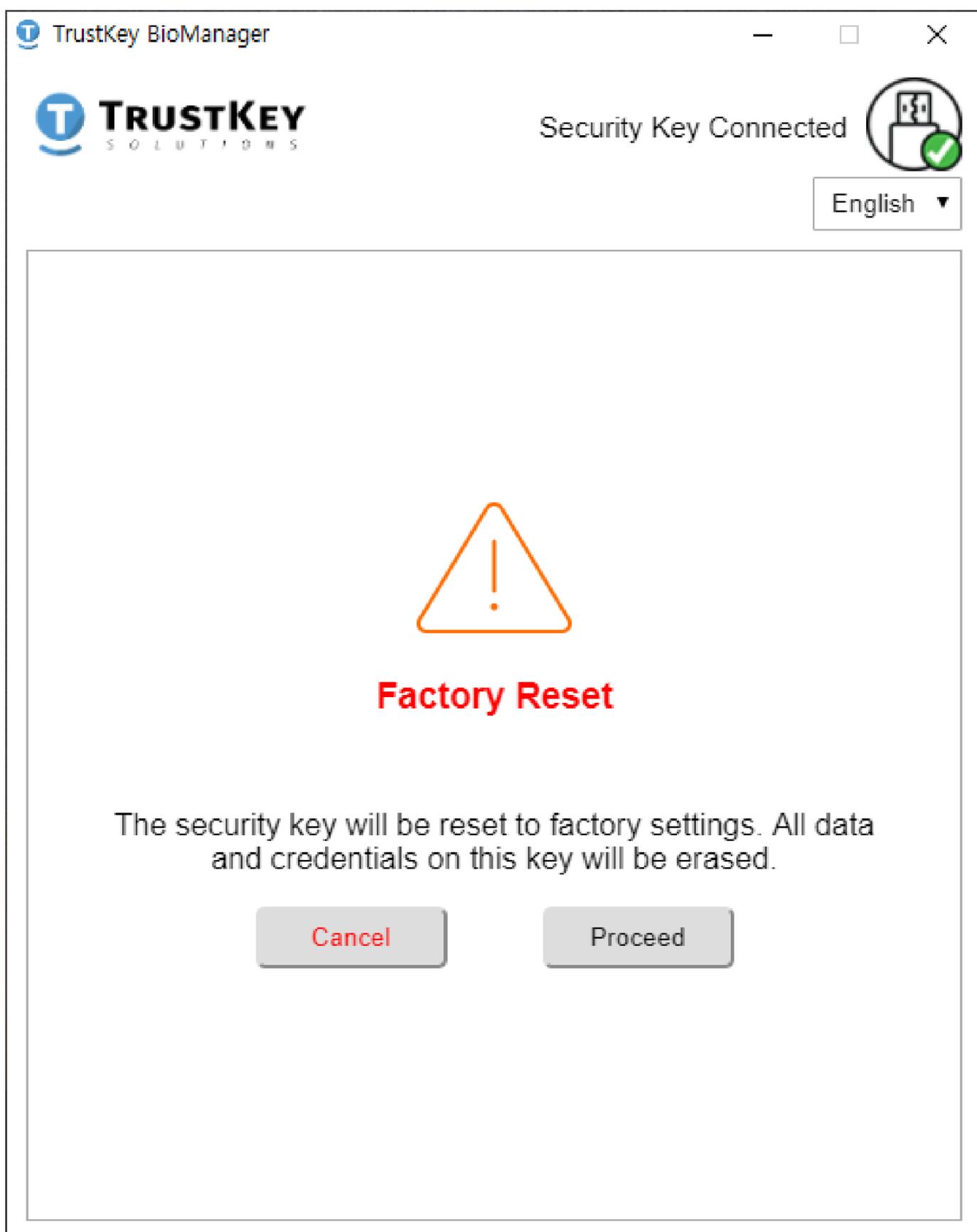
1. Click **Factory Reset** button to reset the security key to initial factory settings.



WARNING : all data and credentials on the key will be lost

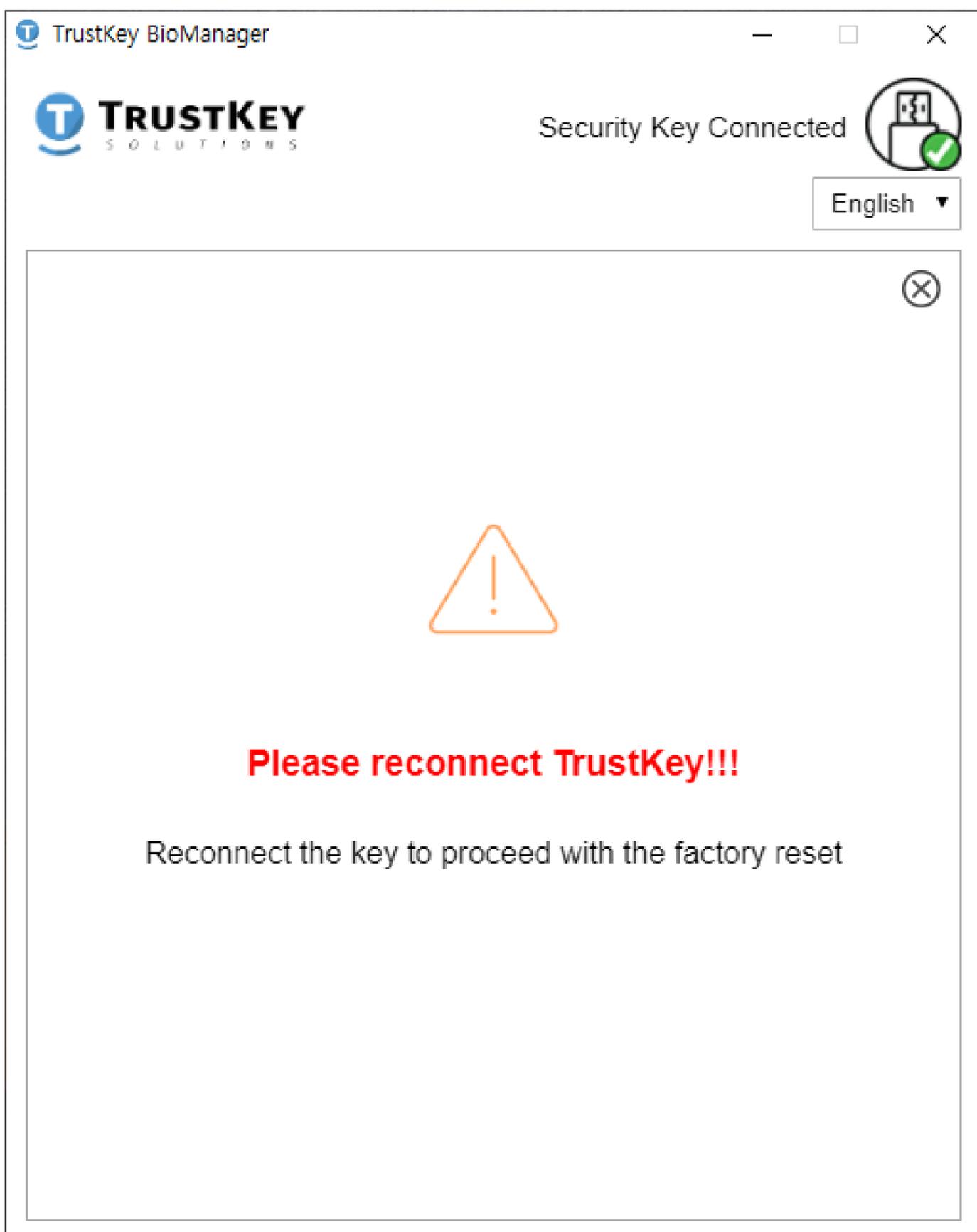
How to Factory Reset

2. Click **Proceed** button to start the Factory Reset.



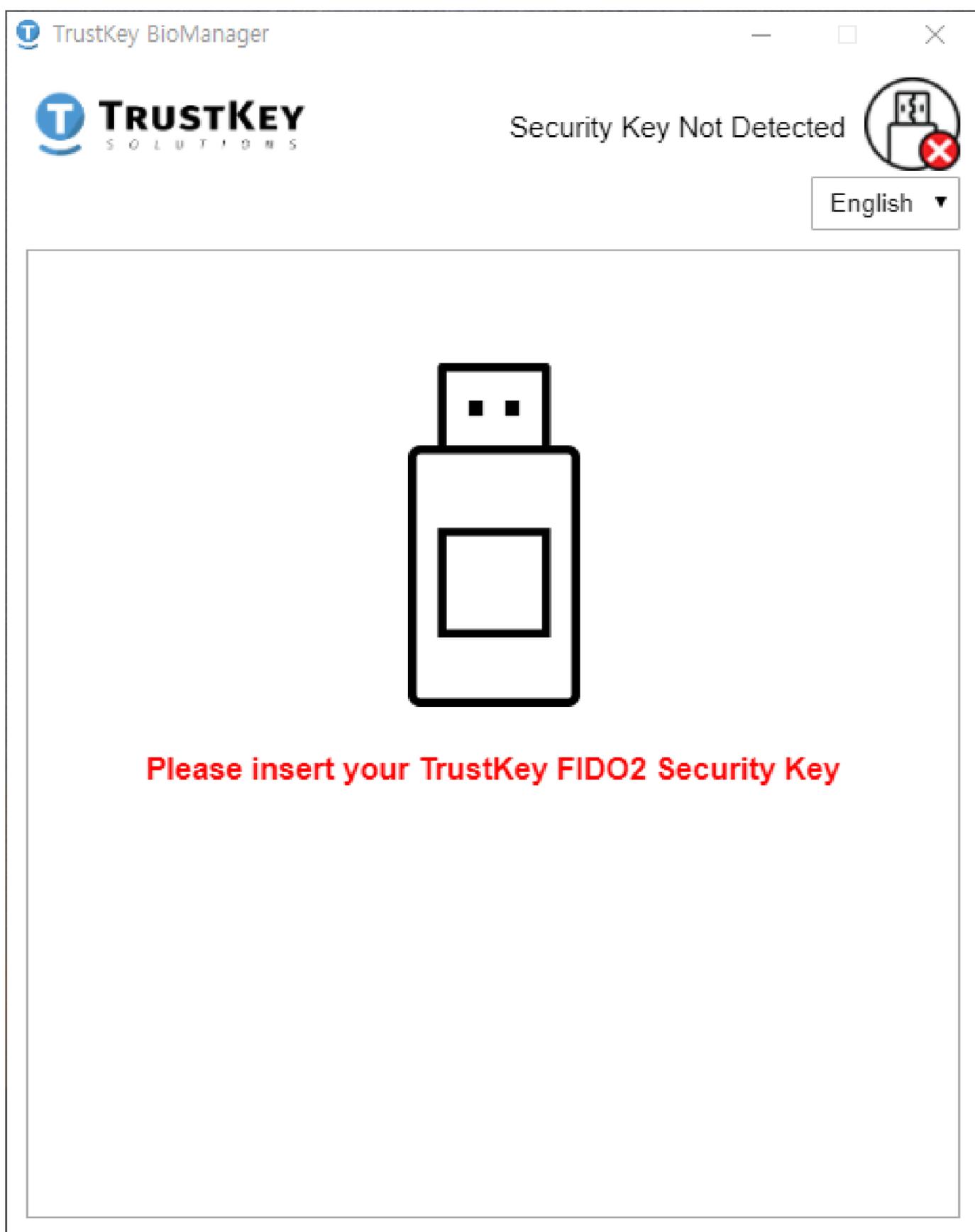
How to Factory Reset

3. Remove the security key from USB port.



How to Factory Reset

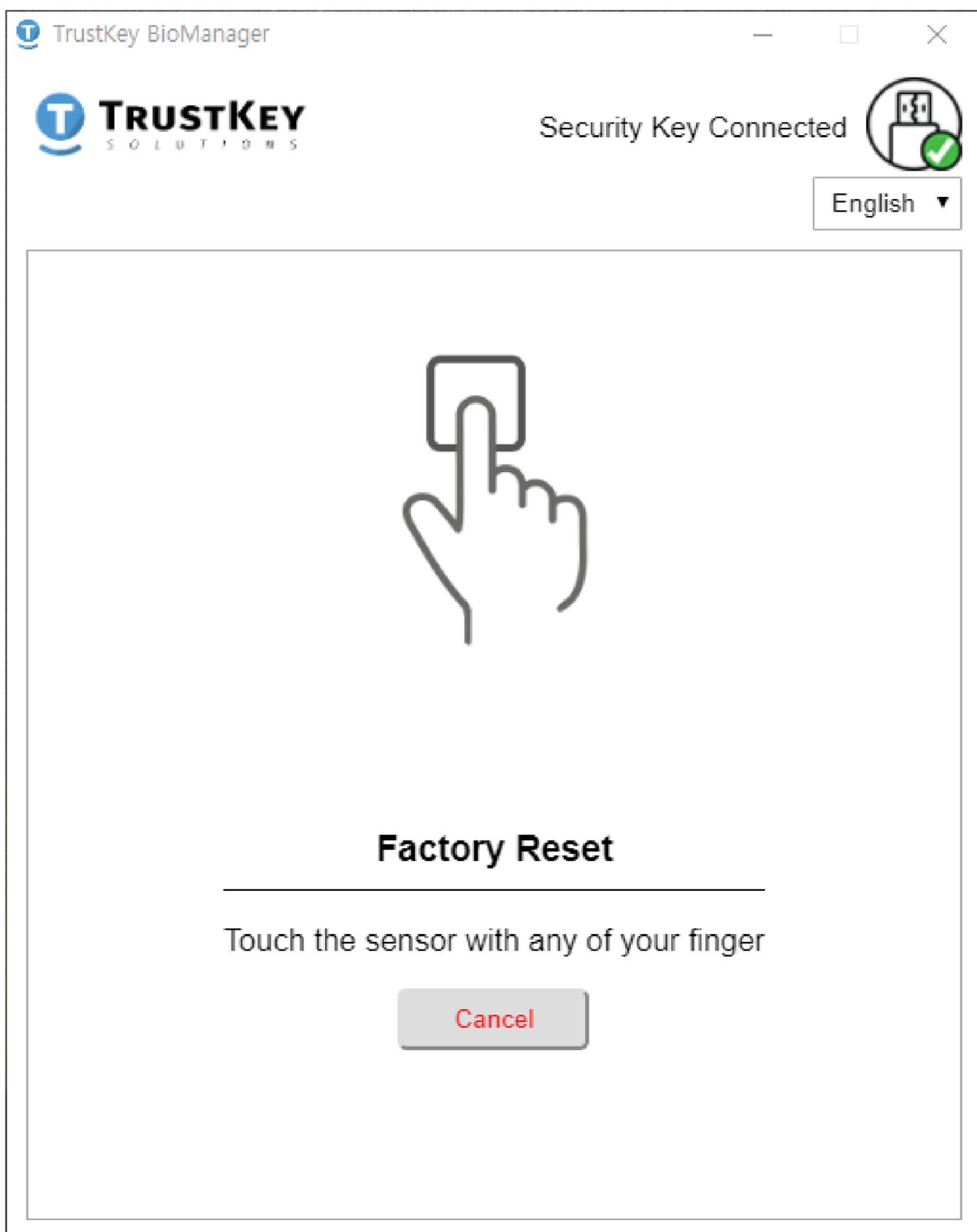
4. Insert the security key into USB port.



WARNING : After re-inserting the security key, make sure to touch the fingerprint sensor within 10 seconds to continue “Factory Reset” process. Otherwise, repeat the whole procedure from the beginning.

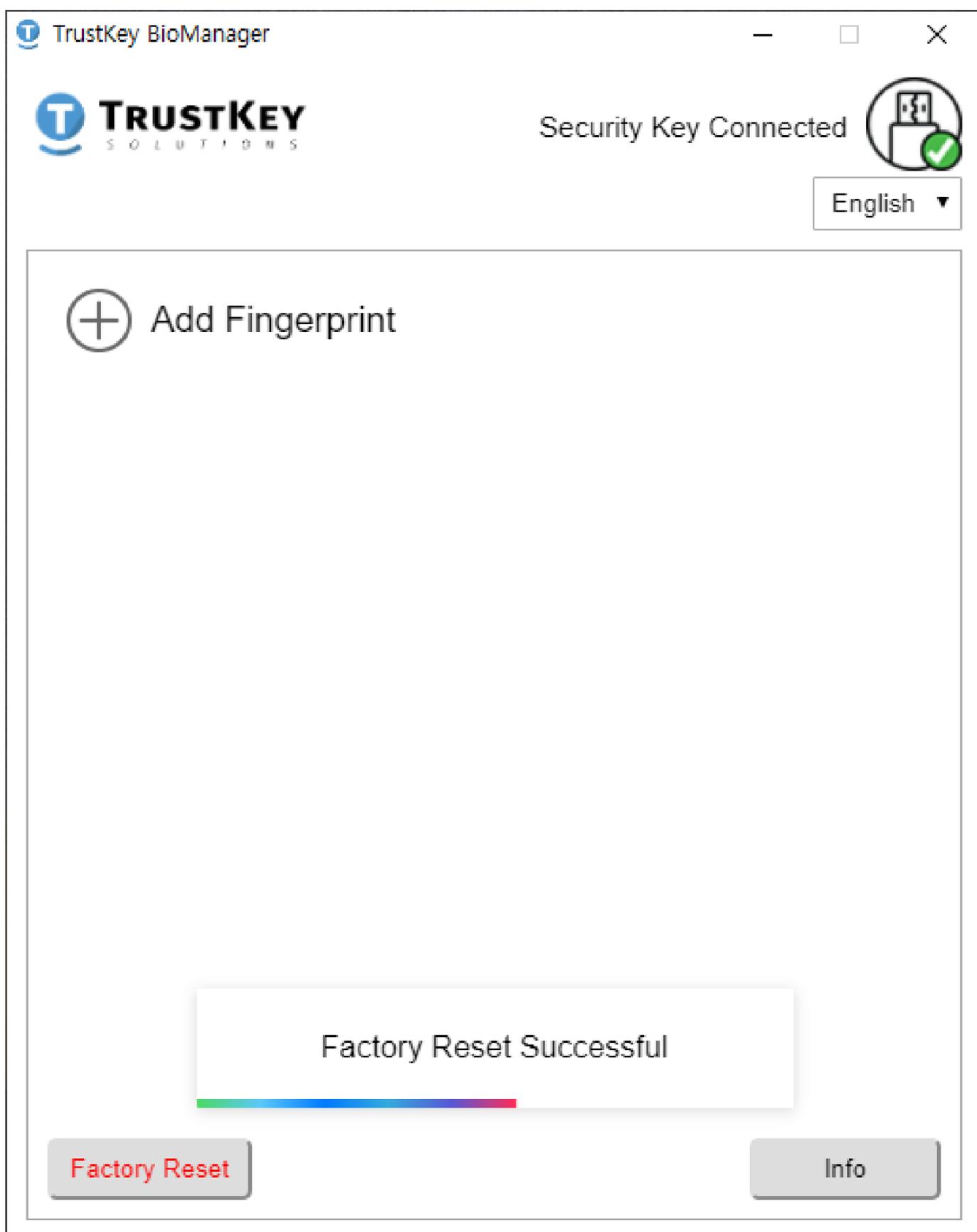
How to Factory Reset

5. If **blue** color LED begins blinking touch the sensor with any of your fingers for the final confirmation.



How to Factory Reset

6. Factory Reset Successful!



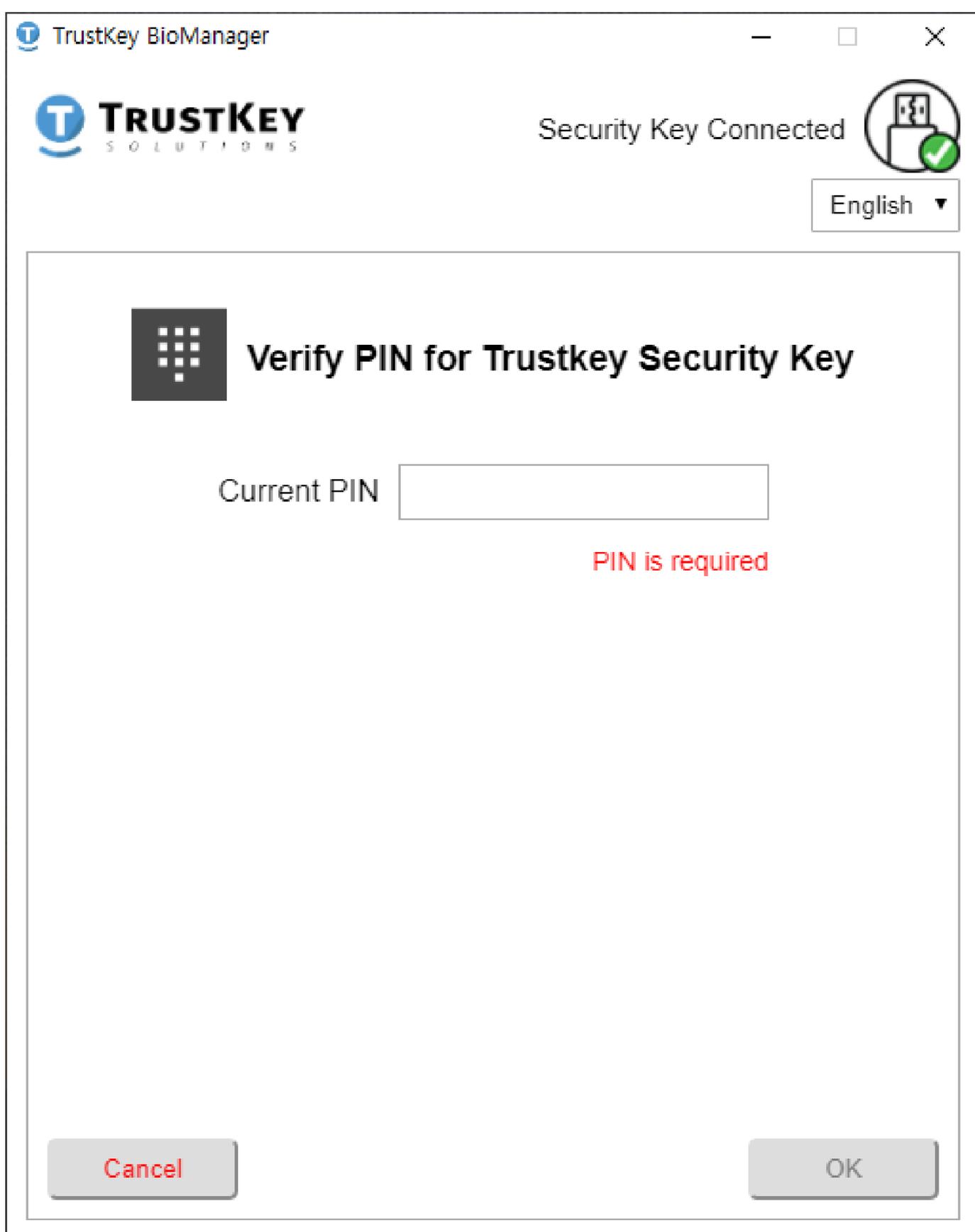
How to Unlock When PIN Code Verification Fails

WARNING :

If the PIN code verification is failed 8 times in a row, Factory Reset is required to unlock the security key. All stored data and credentials will be lost after the Factory reset.

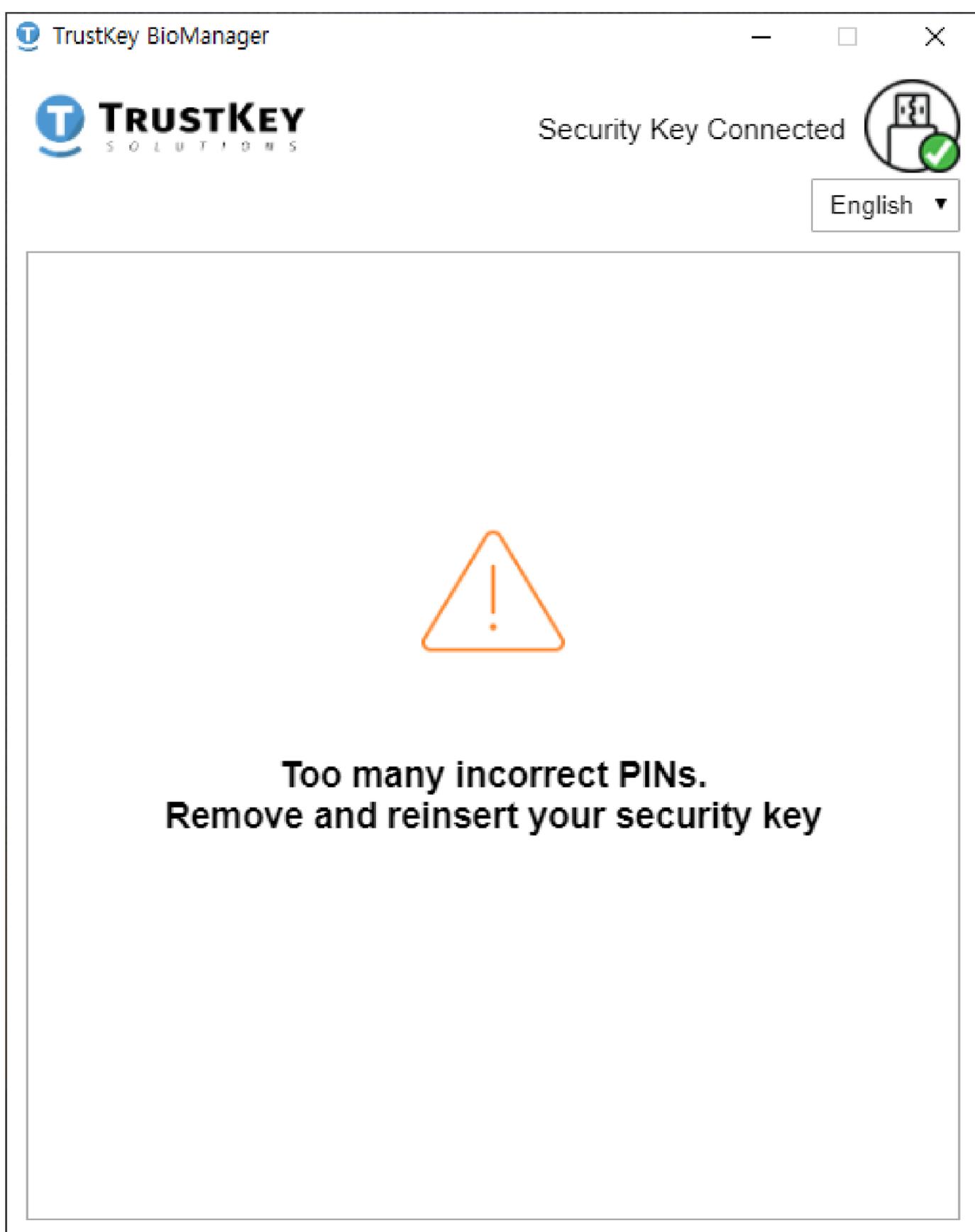
How to Unlock When PIN Code Verification Fails

1. If the PIN code entered doesn't match the below screen will be shown.



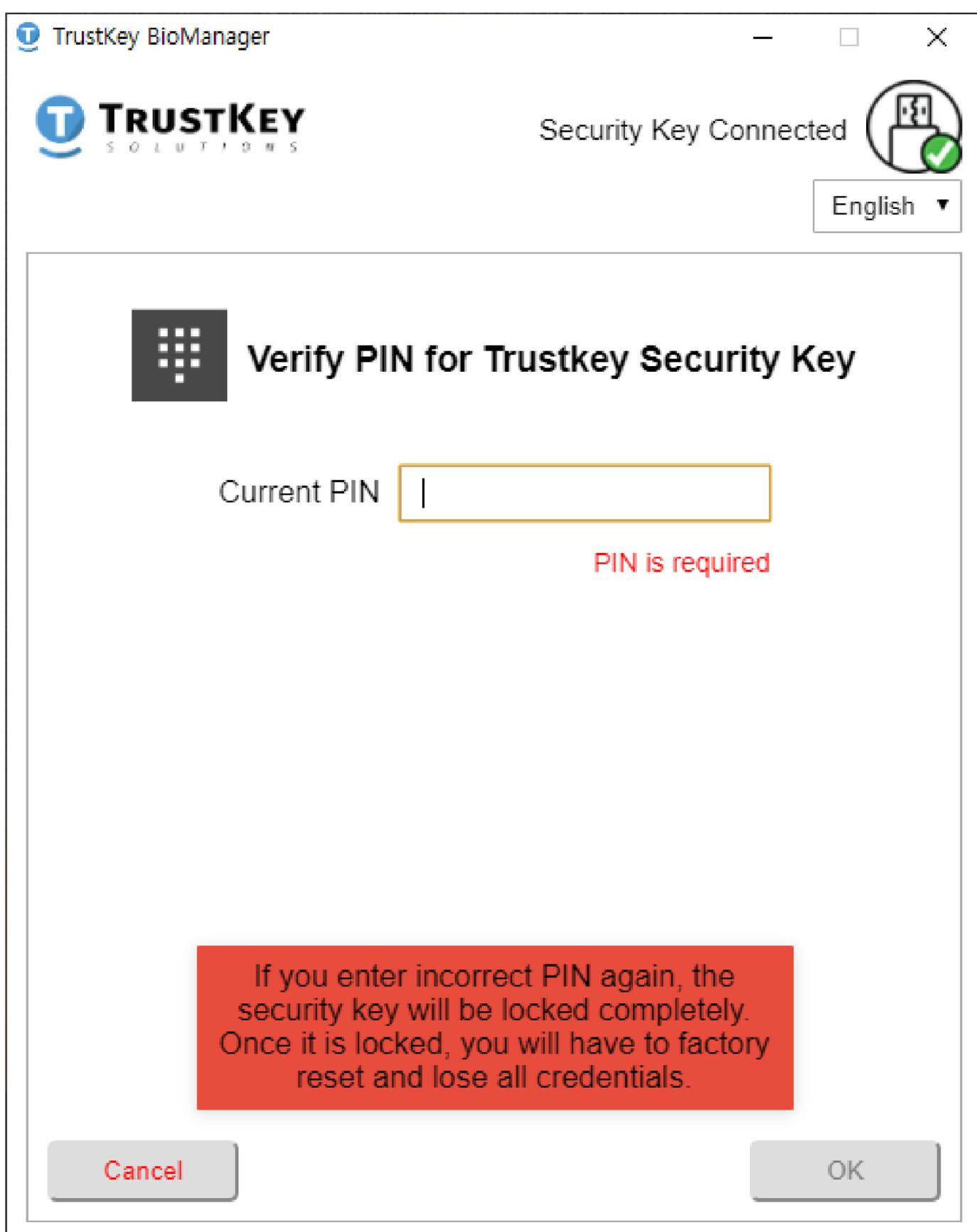
How to Unlock When PIN Code Verification Fails

2. If the PIN verification fails three consecutive times, the user should take out and re-insert the key to try again.



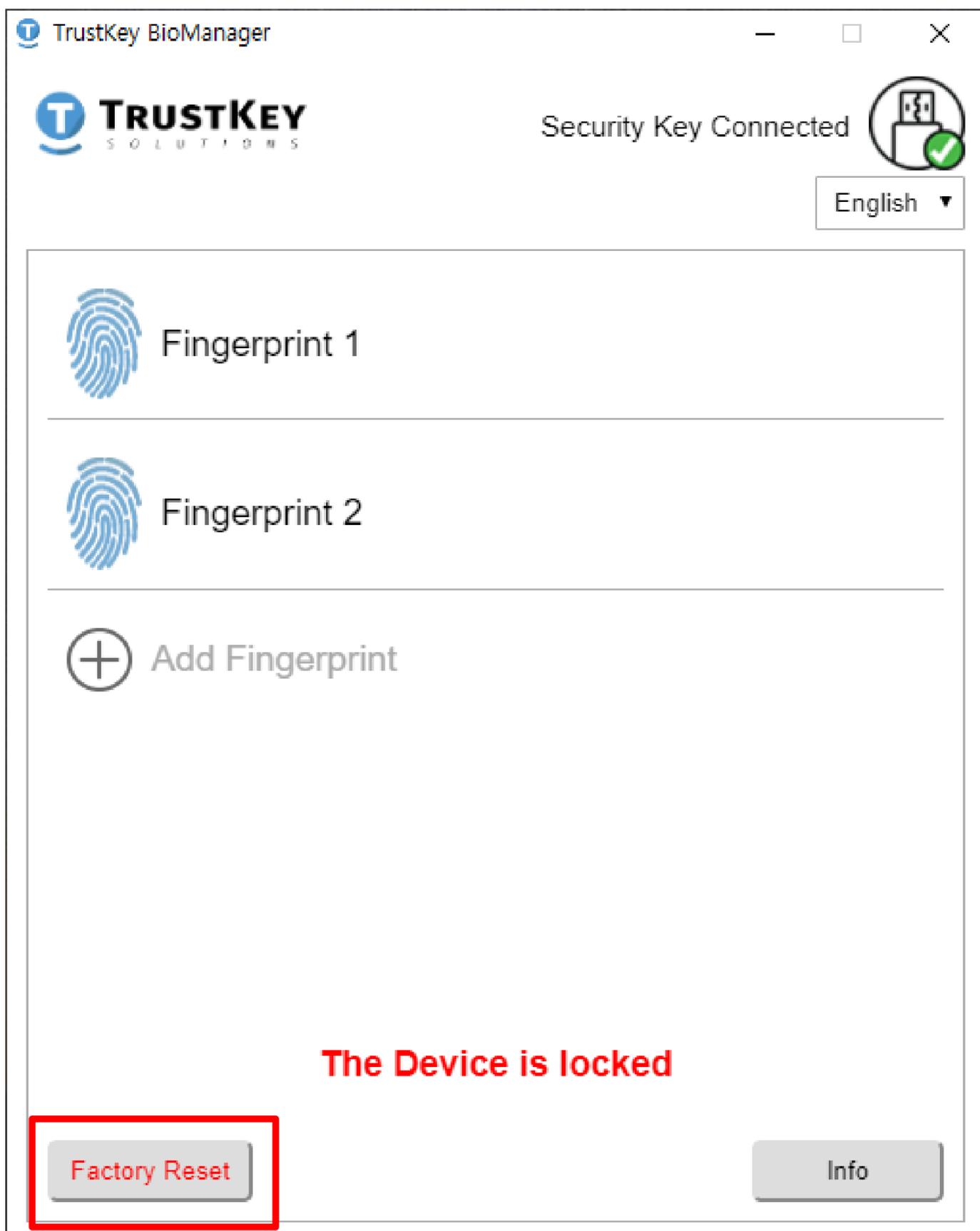
How to Unlock When PIN Code Verification Fails

3. After the 7th PIN verification trial fails, the warning message will be shown as below. If the correct PIN is entered the warning message will be removed.



How to Unlock When PIN Code Verification Fails

4. If the PIN is entered incorrectly for the 8th time in a row, then the device will be locked completely. Once the device is locked by PIN verification failure it should be factory reset and all stored data will be lost including credentials.



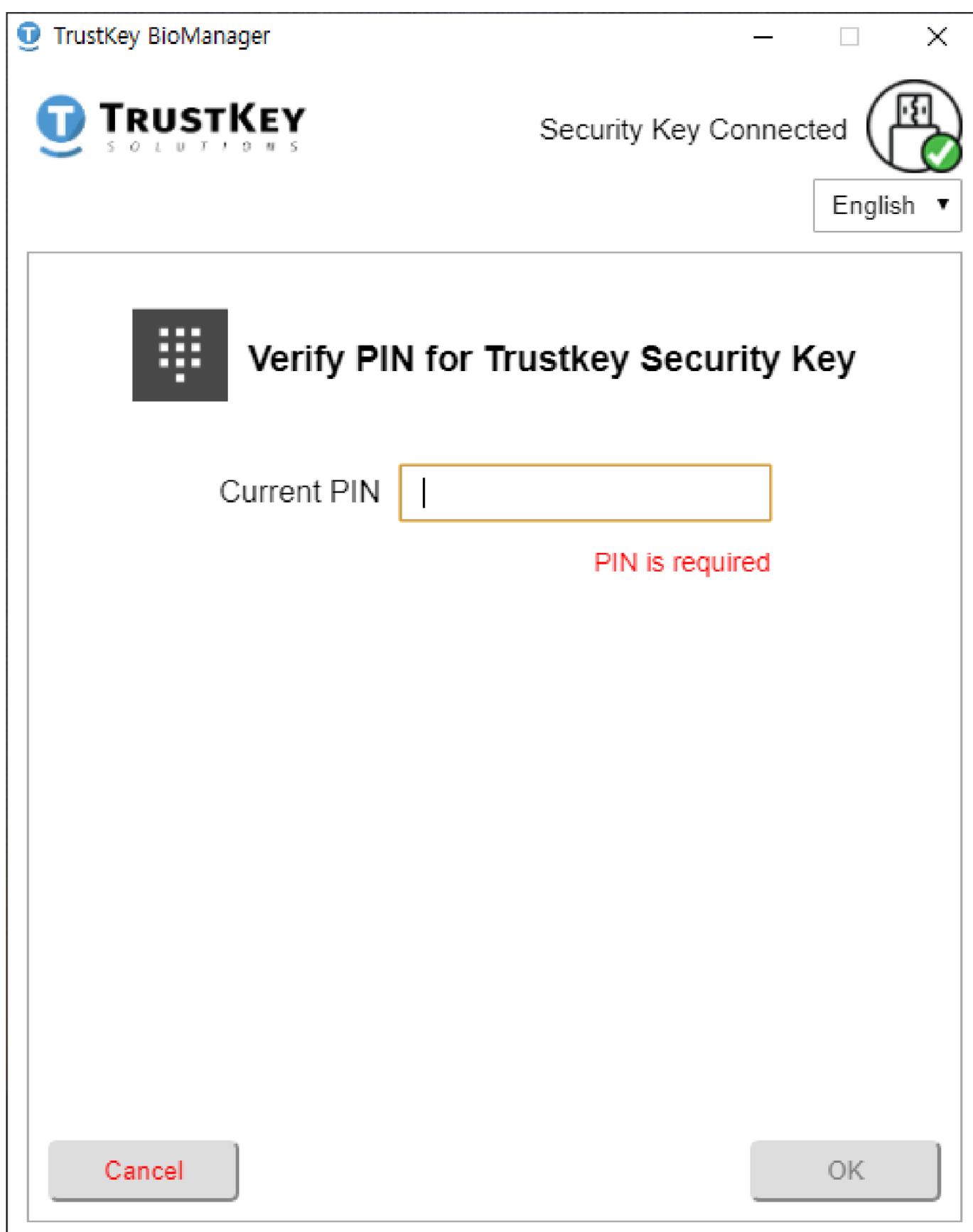
How to Unlock Fingerprint Recognition Fails

WARNING

- For security reasons, TRUSTKEY's G-series security key will be completely locked if the registered fingerprint fails 15 times in a row.
- If the "RED" light is turned on the device, please run BioManager™. Make sure all other web applications are closed before running BioManager™.
- When BioManager™ is running, it will ask for you to enter PIN code to unlock the device.
- After you entered the correct PIN code, your devices is now unlocked successfully.

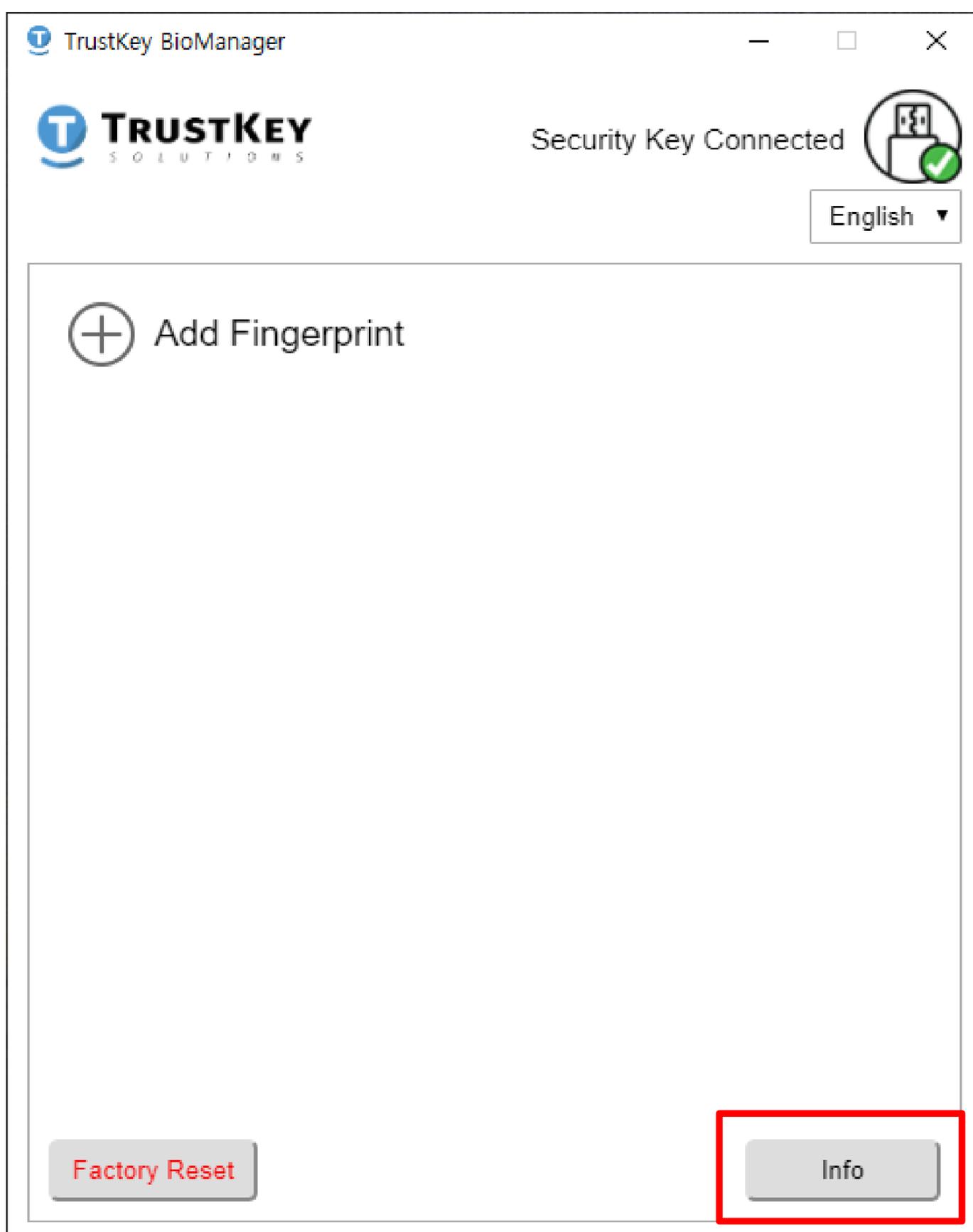
How to Unlock Fingerprint Recognition Fails

1. Unlock the device by entering the correct PIN code.



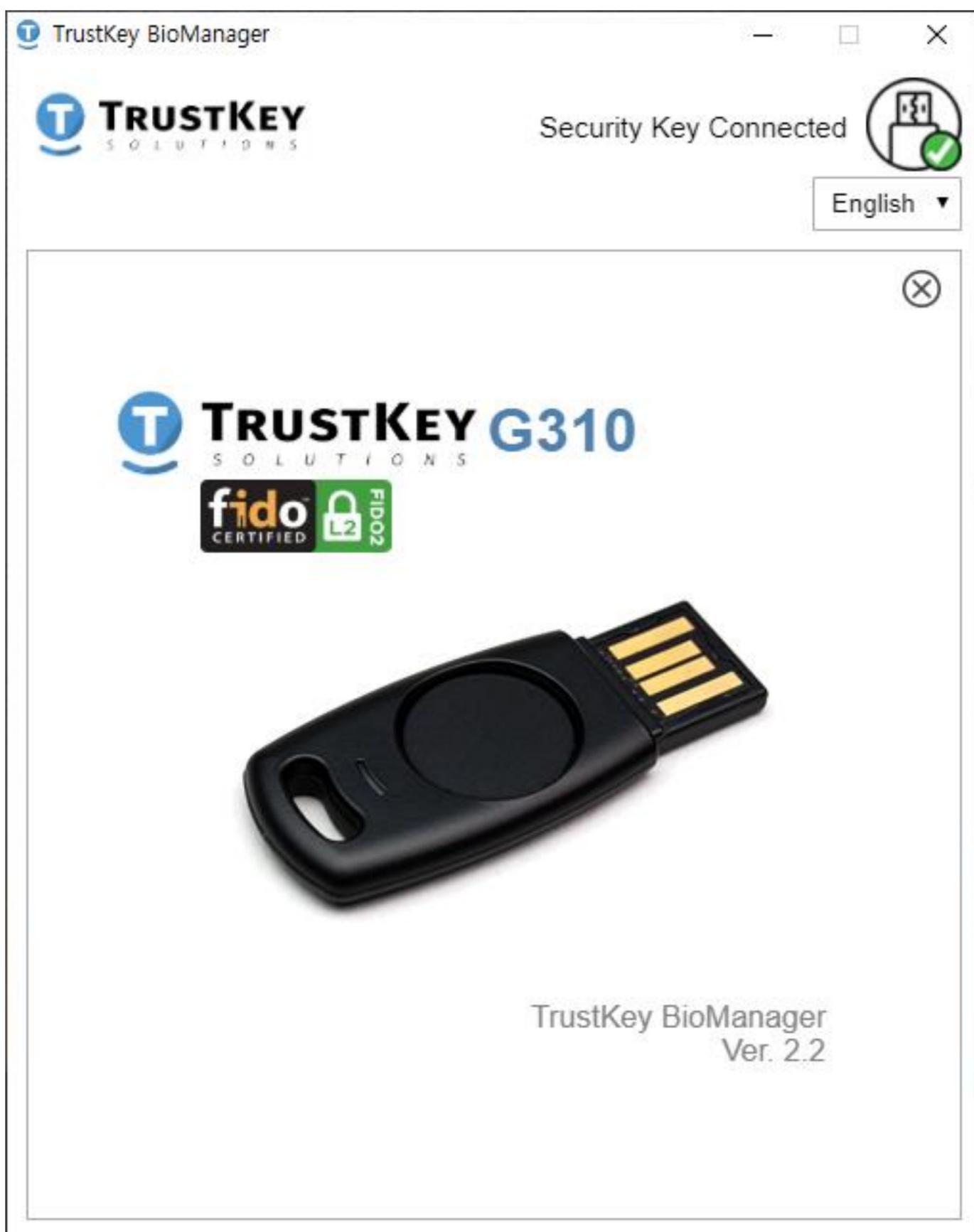
BioManager™ Version Number and Product Image

1. Insert your device into the USB port in your PC/Mac and then click the **Info** button.



BioManager™ Version Number and Product Image

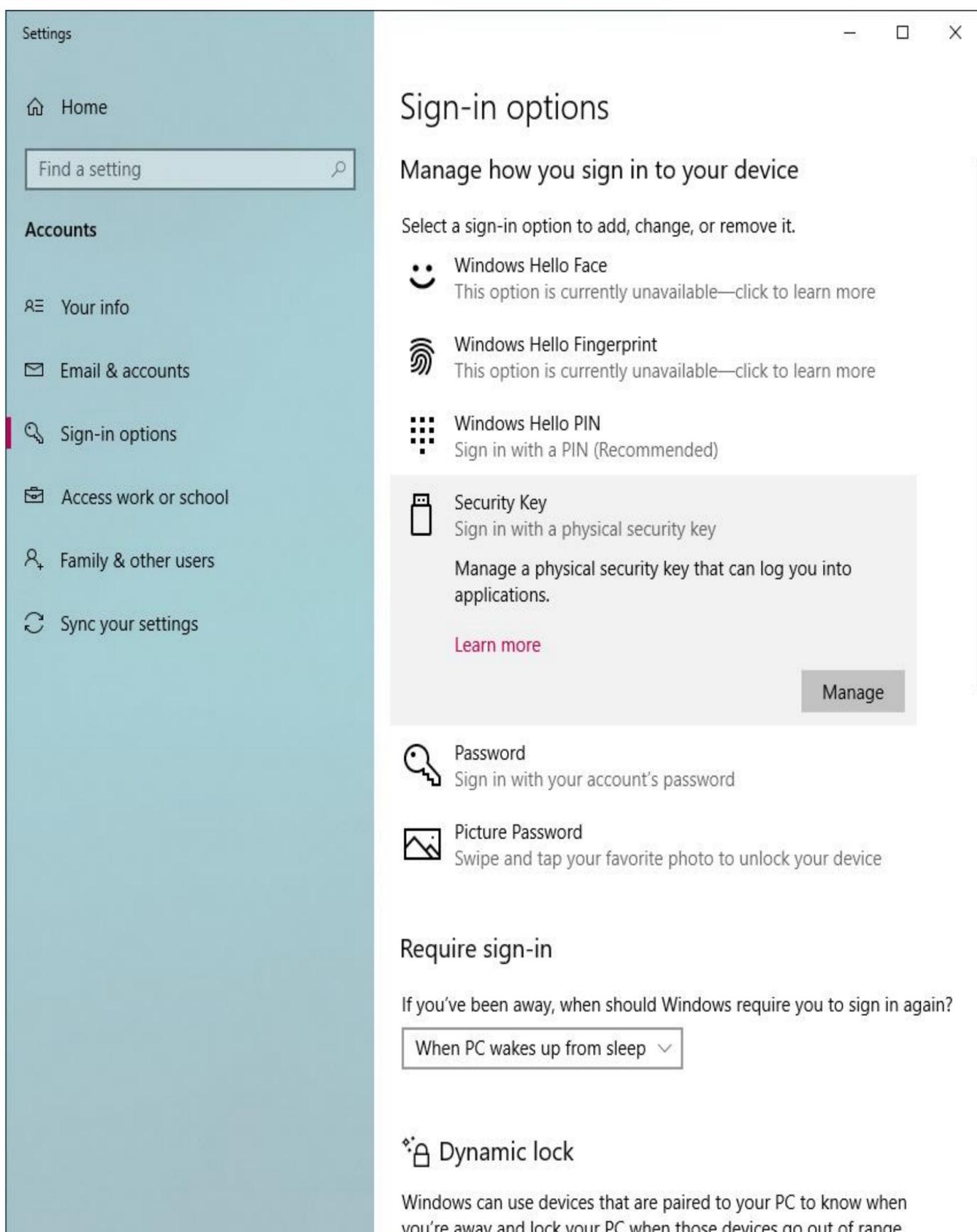
2. If you press **Info** button, then it will show the product image and the BioManager™ version number.



This is an example image when using G310

Windows 10 Security Key Manager

TRUSTKEY's security keys can be set up from systems settings panel on computers running on Windows 10 insider preview build 18298 [19H1] or above. In sign-in settings/ Security Key, Fingerprints and PIN can be managed (add/delete) and the security key can be reset to factory setting if necessary.



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 and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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 : G-series Security Key (eFA310, eFA320)

Responsible Party – U.S. Contact Information

TRUSTKEY Solutions

3101 Park Blvd Palo Alto, CA 94306

+1 408 471 6849