BioPass FIDO2

Security Key

User Manual

V1.2

FEITIAN
WE BUILD SECURITY

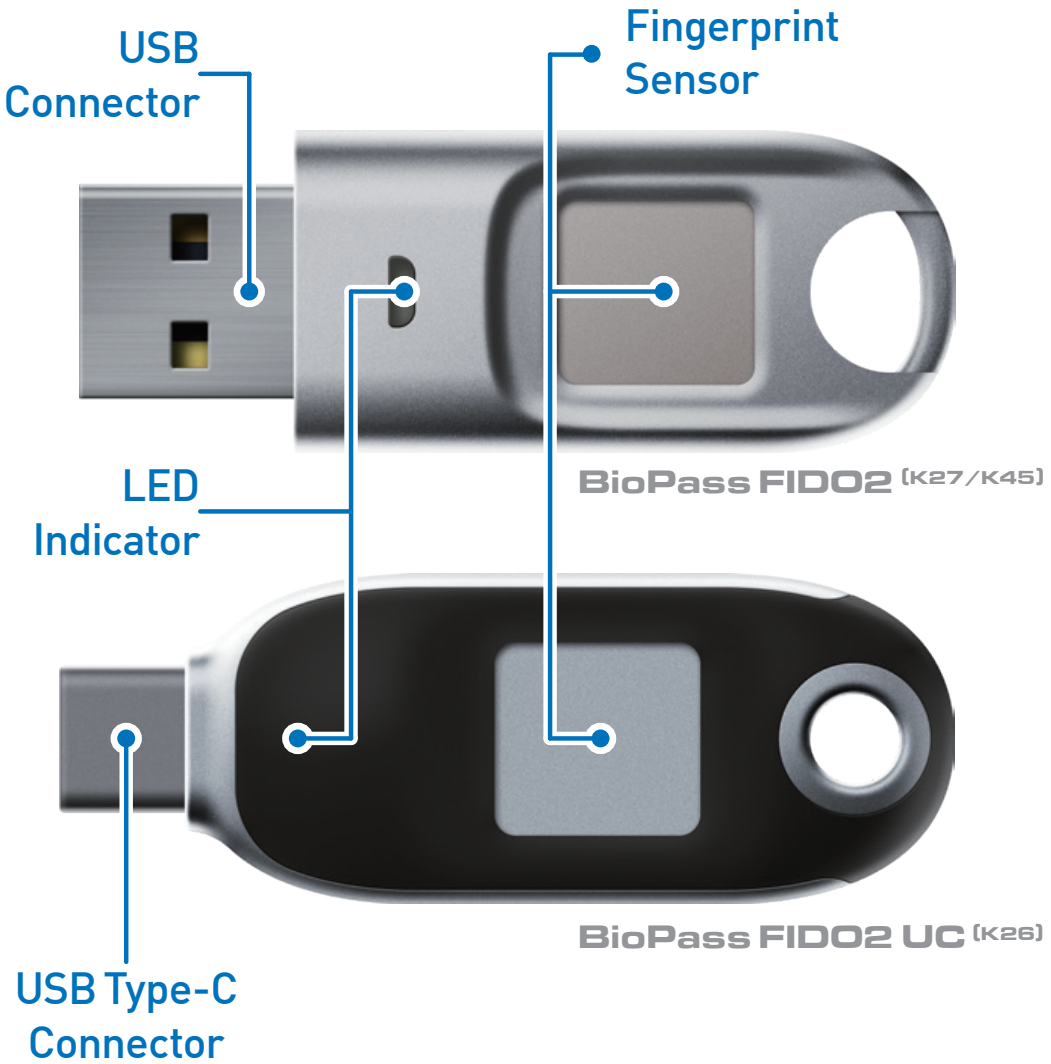
Overview

FEITIAN BioPass security key FIDO2 is built on FIDO2.0 Specification which promoted by FIDO alliance to replace traditional password using biometric or add a second factor to reduce the complexity of traditional password scheme.

FEITIAN BioPass FIDO2 is recommend by Microsoft as the security key for windows hello. For now, we can support the Azure enterprise deployment to provide security and usability. Since FIDO2.0 is submitted to W3C for standardization, most platforms will support FIDO2.0 authentication.

The embedded high-performance FPC fingerprint sensor will ensure fluent user experience with low FRR and FAR. Once enrolled, fingerprint information will only be processed inside the key and protected by security chip embedded, which significantly reduces the risk of fingerprint leaking.

Diagram


USB
Connector
Fingerprint
Sensor
BioPass FIDO2 (K27/K45)
LED
Indicator
BioPass FIDO2 UC (K26)
USB Type-C
Connector

LED Indicators

BioPass security key has a red and a green LED. The red one indicates fail. The green LED means success. The green LED blinks at different frequencies to signal a request for a user presence or user verification. The behavior of green LED is controlled by the options of command sent from client. For example, if client sends a command with uv=true, the green LED will blink rapidly.

Green LED ON	Fingerprint Verification success / user present / Power up
Red Led ON	Fingerprint Verification fail / user absent
Green LED blinks slowly	Need to touch
Green LED blinks rapidly	Need to verify fingerprint

Set up Security Keys

The first step after receiving security key is to set up the PIN and Fingerprint of the security key, there are serval available tools that can be used for set up security key listed below:

NOTE: **It is recommended to set up the security key first before provision security key to web services.**

Windows built-in Security Key Manager

Availability: This tool is a system built-in security key manager which is available in Windows 19H1 and above.

Users are able to set the PIN of security key, add fingerprint, remove fingerprints and reset the security keys.

This tool can be found in “Settings” => “Accounts” => “Sign-in options” => “Security Key”

Chrome built-in Security Key Manager

Availability: This tool is available in the latest Chrome browser in macOS and Linux core system.

Users can find this tool in “Chrome Settings” => “Privacy and security” => “Manage security keys” This tool offers user possibilities for manage PIN, fingerprint and credentials inside the security key and reset the device.

FEITIAN BioPass FIDO2 Manager

Availability: Windows 7, Windows 10 Build 18H2 and below, macOS and Linux.

The latest Windows and Linux version can be downloaded at:
https://www.ftsafe.com/Support/Resources

NOTE: For security concern, the key will be blocked if user fail to verify fingerprint 15 times (3 times per retry × 5 retry counts) in a row. User can only unlock via reset device (All stored data will be lost).

Provision your Security key With web services:

The first step of using FIDO authentication is to provision security keys into your account. For most web services, it is required to register your security key on PC via USB. To provision the security key with your account, please follow the steps below:

Step1:
Authenticate you account as normal with PC and a WebAuthN supported browser.

Step2:
Go to account settings – sign in methods – set upsecurity keys(Normally it is under 2-step verification or something similar)

Step3:
Plug in the security key and follow the pop upinstructions.

Authenticate to Web services

After provisioning the security key via PC, user can authenticate to their account passwordlessly or as a strong second factor with the security key. The steps of authenticate to account may be different across web services and platforms.

For Passwordless Authentication, user can click "sign-in with security key" in the sign in window, then follow the pop up instruction of authentication.

Two Step Authenticcation, users are required to type authentication with username and password as usual, then the two step verification window will pop up, user follow the pop up instruction to finish authentication.

For detailed instructions and supported services, please see the following website:
https://www.ftsafe.com/article/620.html

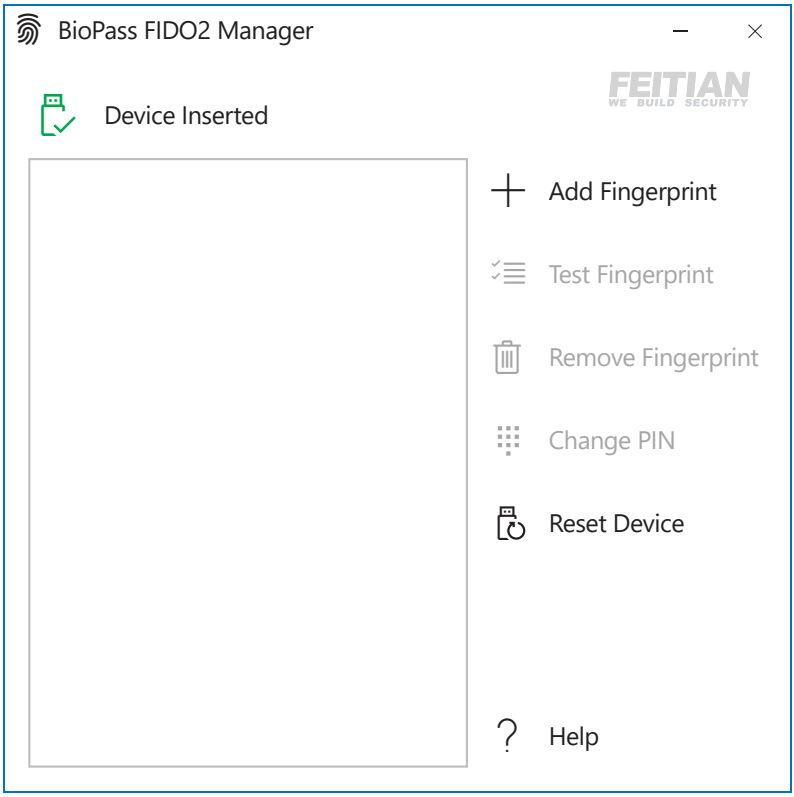
BiPass FIDO2 Manager

This section provides a detailed guide ofFEITIAN BioPass FIDO2 Manager, users using Windows 10 (1809 and below), windows7, Linux and MacOS can use this tool for fingerprint provisioning. MacOS usercan download this tool from APP Store. The latest Windows and Linux version canbe downloaded at:
https://www.ftsafe.com/Support/Resources

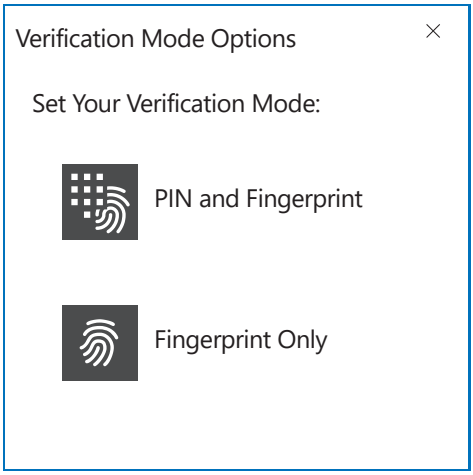
Warning:
For security concern, the key will be blocked if user fail to verify fingerprint 15 times (3 times per retry × 5 retry counts) in a row. User can only unlock via reset device (All stored data will be lost).

Enroll Fingerprint

❶ Plug in your BioPass FIDO2 Security Key and launch BioPass FIDO2 Manager App, the following window should appear:

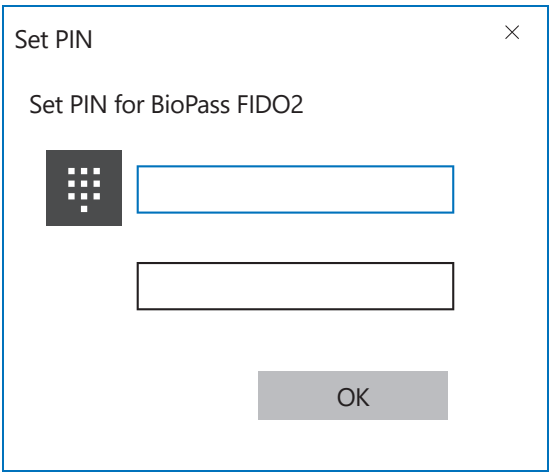


❷ Click Add Fingerprint . If the Security Key is being used for the first time or just been reseted, a window will pop up to let you choose wether to use fingerprint only or both PIN and fingerprint to verify your operations:

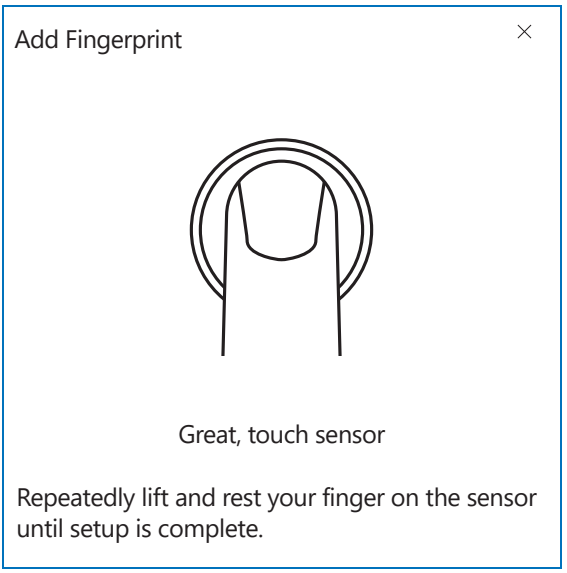


NOTE **Once you choose one option, you cannot change to another without reset the device**

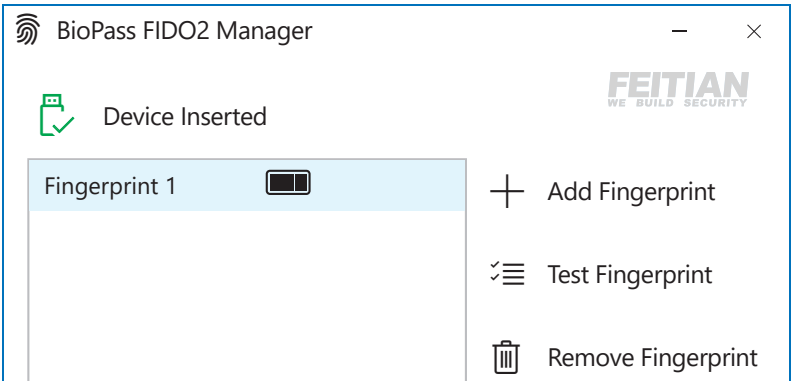
If you choose to use PIN and fingerprint, you will be informed to set a new PIN. PIN value can contain numbers, letters and special symbols.



❸ Follow the instructions to add fingerprint.

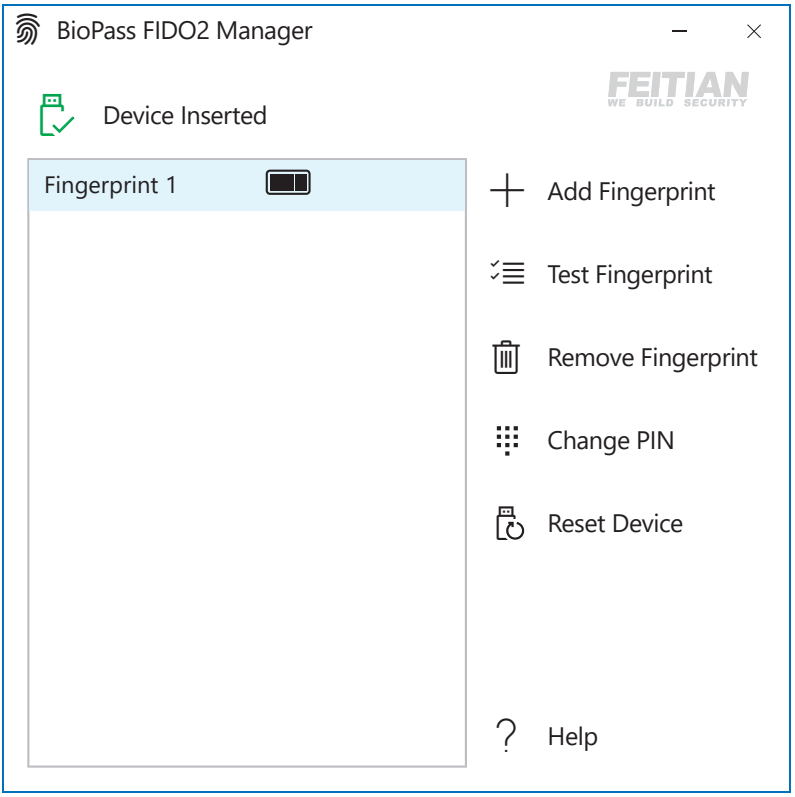


❹ After been successfully enrolled, the fingerprint will be listed in main window. Now you can test your fingerprint, remove your fingerprint and change PIN (if set) through the BioPass FIDO2 Manager App and enjoy your secure authentication experience.



Test Fingerprint

❶ Select the fingerprint you want to test and click Test Fingerprint to test if this fingerprint is verified.

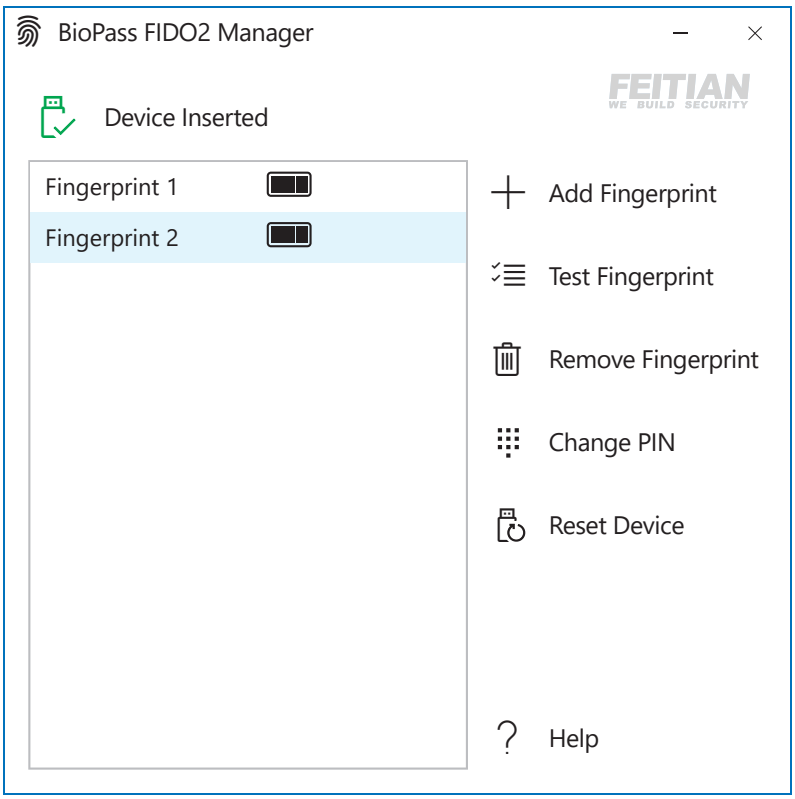


❷ Follow the instructions to test the fingerprint.

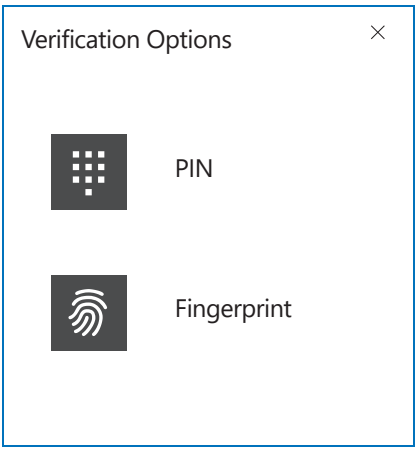
NOTE **This testing function will trigger the device block mechanism if user fail to verify fingerprint 15 times (3 times per retry × 5 retry counts) in a row. User can only unlock via reset device (All stored data will be lost).**

Remove fingerprint

❶ Select the fingerprint you want to remove and click Remove Fingerprint. (“Fingerprint 2” as shown in example)



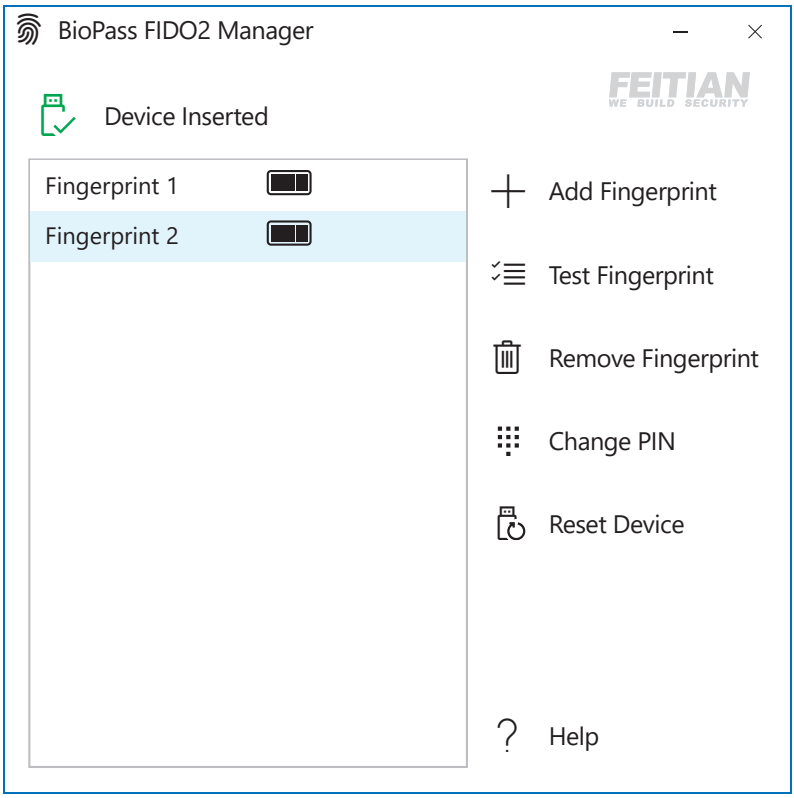
If there is a PIN, you need to choose a verification option.



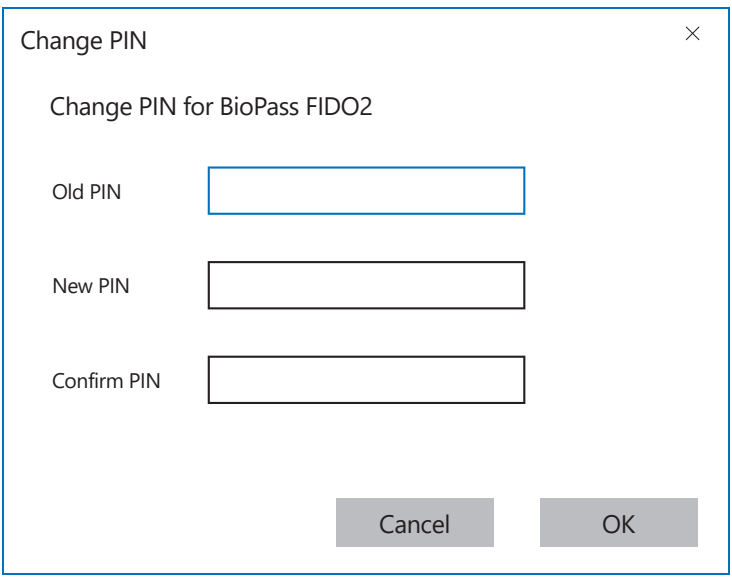
❷ After verification, the fingerprint will be removed.

Change PIN

❶ Click Change PIN .

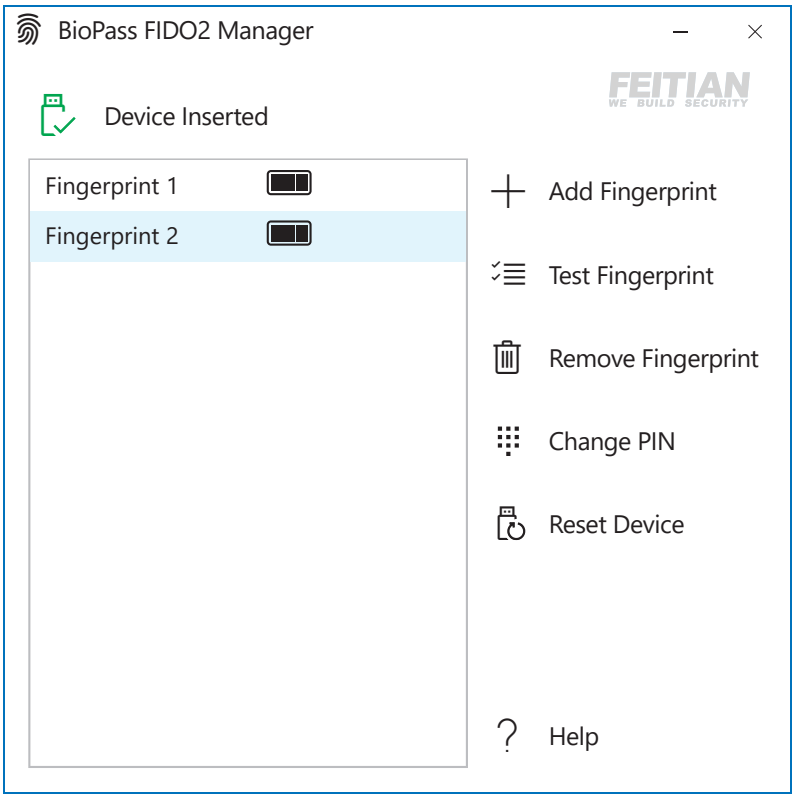


❷ Fill in all the text boxes then click “OK” to change PIN.



Reset Device

Click Reset Device .



NOTE **Once reseted, all data including your credentials stored inside the Security Key will be deleted .**

Specification
Security Key

Standard	FIDO2
Security Algorithm	ECDSA, SHA256, AES, HMAC, ECDH
Interface	USB Type-A / USB Type-C
Communication Protocol	CTAPHID
Working Voltage	5.0V
Working Current	34mA Standby 44mA Peak
Power	0.17W Standby 0.22W Peak
Working Temperature	-10 ~ 50 °C (14 ~ 122 °F)
Storage Temperature	-20 ~ 70 °C (-4 ~ 158 °F)
Fingerprint Sensor	FPC Fingerprint Sensor
Indicator	Green LED, Red LED
Casing Material	Zinc Alloy and Plastic (PC+ABS)
Size	51 × 18 × 6.5 mm K27/K45 50.9 × 18.5 × 7 mm K26

Specification
Fingerprint Module

Resolution	160 × 180 pixel
Definition	508 DPI
Sensor Service Life	Over 200,000 times
Storage	Up to 50 fingerprints
Autonomic Learning	Yes
False Accept Rate	<0.001%
False Reject Rate	<1%
Recognition Time	<0.6 sec
Acquisition Time	<180 ms

www.ftsafe.com

FEITIAN
WE BUILD SECURITY