

BioPass FIDO2

Security Key

User Manual

V1.1

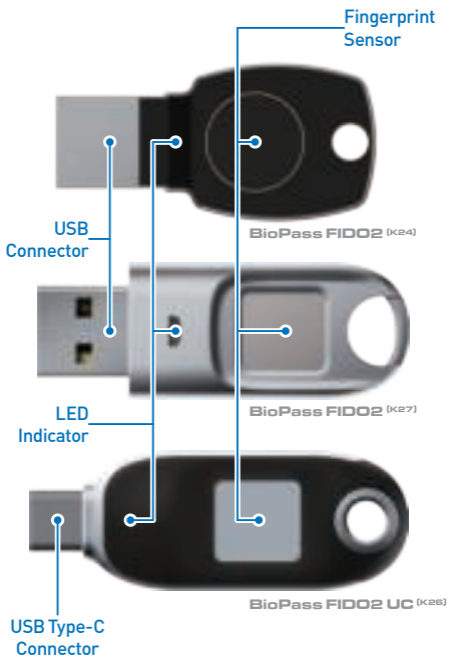
Overview

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



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

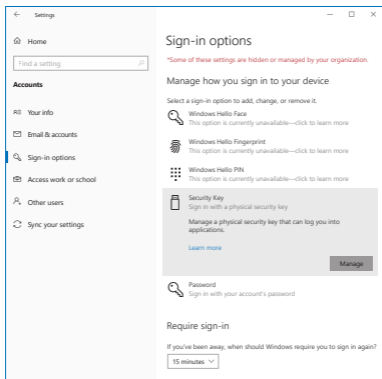


Green LED blinks rapidly

Need to verify fingerprint

Windows 10 Security Key Manager

Users can now set up a security key straight from System Settings Panel on computers running on Windows 10 Insider Preview Build 18298 (19H1) or above. In sign-in settings/Security key, users are able to manage fingerprint, PIN or reset a security key.:



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).

FEITIAN BiPass FIDO2 Manager

Users can manage fingerprint, PIN or reset a security key by using FEITIAN's BioPass FIDO2 manager on computers running on Windows 10 lower than Build 18298 (19H1).

For the first time using FEITIAN BioPass FIDO2 Security Key, users are required to initialize and enroll the first fingerprint via BioPass FIDO2 Manager App. The app can be downloaded from Microsoft Store or the following link:
<https://www.microsoft.com/store/productId/9P2ZJPWK3PXW>



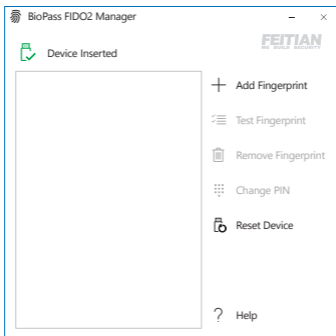
BioPass FIDO2 Manager
Feitian Technologies Co., Ltd.
Free
Get the app >

Warning:

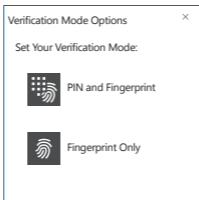
For security concern, the key will be blocked if user fail to verify fingerprint 15 times (3 times per retry × 5 retry counts) in a row. User can only unlock via reset device (All stored data will be lost).

Enroll Fingerprint

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

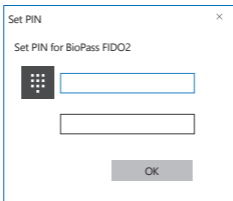


- 2 Click **+** Add Fingerprint . If the Security Key is being used for the first time or just been reset, a window will pop up to let you choose whether to use fingerprint only or both PIN and fingerprint to verify your operations:

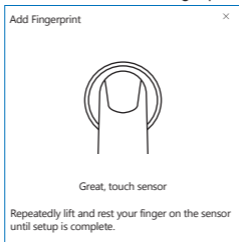


NOTE Once you choose one option, you cannot change to another without reset the device

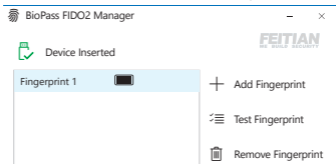
If you choose to use PIN and fingerprint, you will be informed to set a new PIN. PIN value can contain numbers, letters and special symbols.




3 Follow the instructions to add fingerprint.

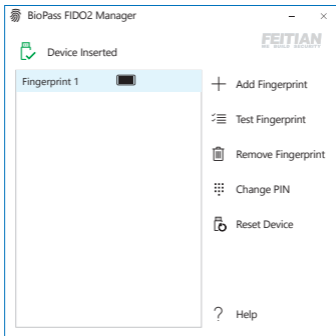


4 After been successfully enrolled, the fingerprint will be listed in main window. Now you can test your fingerprint, remove your fingerprint and change PIN (if set) through the BioPass FIDO2 Manager App and enjoy your secure authentication experience.



Test Fingerprint


- 1 Select the fingerprint you want to test and click  to test if this fingerprint is verified.

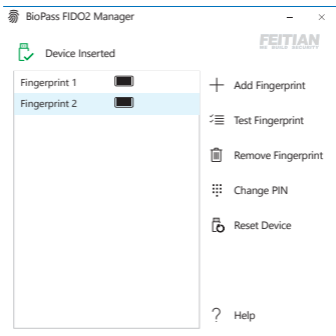


- 2 Follow the instructions to test the fingerprint.

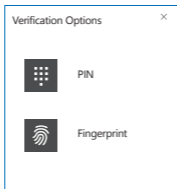
NOTE This testing function will trigger the device block mechanism if user fail to verify fingerprint 15 times (3 times per retry × 5 retry counts) in a row. User can only unlock via reset device (All stored data will be lost).

Remove fingerprint

- 1 Select the fingerprint you want to remove and click  Remove Fingerprint. ("Fingerprint 2" as shown in example)



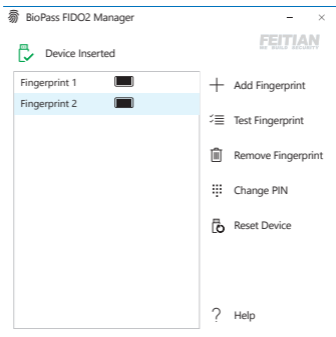
If there is a PIN, you need to choose a verification option.



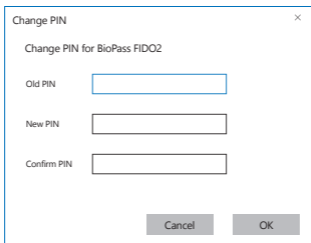
- 2 After verification, the fingerprint will be removed.

Change PIN

- 1 Click  Change PIN.




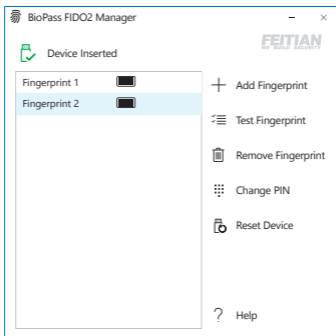
- 2 Fill in all the text boxes then click "OK" to change PIN.



The screenshot shows a "Change PIN" dialog box with a close button in the top right corner. The title is "Change PIN" and the subtitle is "Change PIN for BioPass FIDO2". There are three text input fields labeled "Old PIN", "New PIN", and "Confirm PIN". At the bottom of the dialog, there are two buttons: "Cancel" and "OK".

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	42.3 × 20.8 × 4.5 mm ^{K24} 51 × 18 × 6.5 mm ^{K27} 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 50 fingerprints

Autonomic Learning Yes

False Accept Rate <0.001%

False Reject Rate <1%

Recognition Time <0.6 sec

Acquisition Time <180 ms

