

AllinPass FIDO2

Security Key

User Manual

V1.1

Overview

FEITIAN AllinPass FIDO2 K33 is a security key 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.

The AllinPass K33 security key provides users with a strong, user-friendly, passwordless logon experience. The Bluetooth® Certified BLE module embedded in the AllinPass FIDO2 Security Key ensures seamless communication with most mainstream mobile devices and PCs. The NFC communication is fully compliant with the ISO 14443 standard and will work with all compliant smart card readers.

The FEITIAN AllinPass is a FIDO2 certified authenticator which effectively protects users against phishing attacks, MITM attacks, and server credential breaches. The CC EAL 6+ Secure Element embedded in the AllinPass FIDO2 Security Key will also provide strong chip level protection and runs mature algorithms ensuring data security.

FEITIAN AllinPass 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.

Core Features

- Driver free. Recognize as a HID device, no driver needed for Feitian AllinPass FIDO2 to work for Windows Hello.
- Capacitive fingerprint sensor. Fingerprint protected by secure elements.
- Multiple interfaces are supported by AllinPass K33, including USB-A or USB-C (Required a BSU cable), NFC which is fully compliant with the ISO 14443 standard, and BLE that enables users to use it on a mobile application.









AllinPass FIDO2 (K33)

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).

LED Indicators

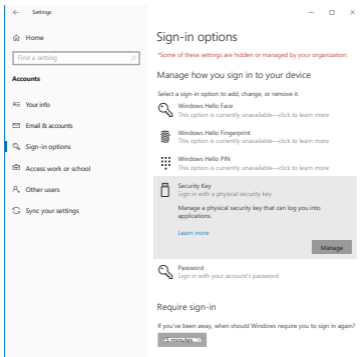
The AllinPass K33 security key has a red LED, a blue LED and a green LED. The red one indicates fail. The green LED means success. And the blue LED is Bluetooth indicator. Besides those, there is an extra light showing the status of battery. The green LED blinks at different frequencies to signal a request for 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
	Blue LED blinks slowly	Bluetooth is in communication mode
	Blue LED blinks rapidly	Bluetooth is in pairing mode

Fingerprint enrollment

Before using the AllinPass K33 security key, fingerprint is always required to be enrolled via a USB cable.

Users can now set up a security key straight from Settings page if the platform is 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.

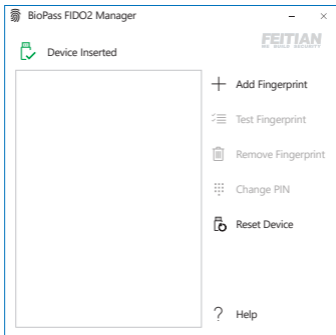


Otherwise, Users can manage fingerprint, PIN or reset a security key by using FEITIAN's BioPass FIDO2 manager if platform is lower than Build 18298 (19H1). It can be downloaded from Microsoft Store or via <https://www.ftsafe.com/download/webdownload/BioPass%20FIDO2%20Manager.exe>.

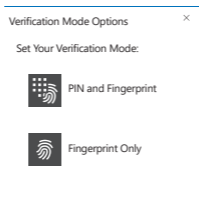
For the first time using Feitian AllinPass FIDO2, users are required to initialize and Enroll the first fingerprint using AllinPass FIDO2 Manager.

Enroll your first fingerprint

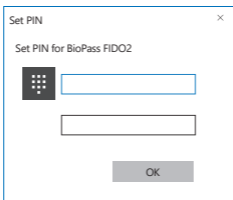
- 1 Launch the BioPass FIDO2 Manager and plug in the FEITIAN AllinPass K33, you will see the following windows:



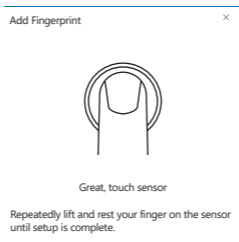
- 2 Click **+ Add Fingerprint** this window will pop up, you can choose to use fingerprint only or to set both pin and fingerprint. (Once you choose one option, you cannot change to another without reset the device)



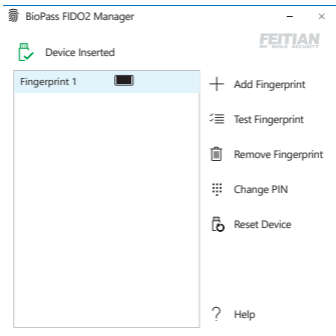
- 3** Set Pin and then click OK. Numbers, letters and special symbols are supported. The PIN has a limitation of 4 to 63 characters.



- 4** Add fingerprint following the instructions.



- 5 After the fingerprint successfully enrolled, there should be a fingerprint listed in the text box.



- 6 Then, users can test their fingerprint, remove the enrolled fingerprints and change pin via the BioPass FIDO2 Manager to enjoy secure authentication experience.

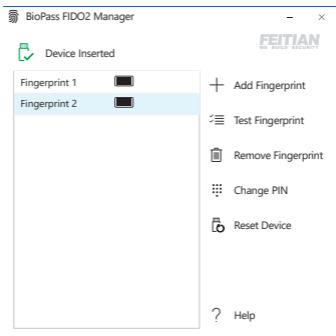
Test Fingerprint

This function is for users to test the fingerprint verification.

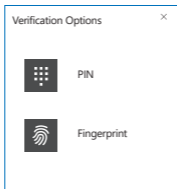
NOTE This testing function will trigger the block device procedure mentioned above.

Remove fingerprint

- 1 Make sure to choose the right fingerprint to delete. ("Fingerprint 2" as shown in example)



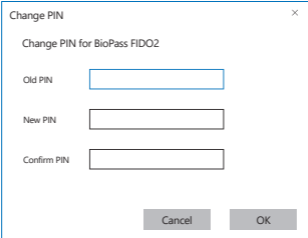
- 2 If there is a Pin, users need to choose a verification option.



- 3 After verification, the fingerprint will be removed.

Change PIN

Just fill in all the text boxes for changing Pins



Change PIN ×

Change PIN for BioPass FIDO2

Old PIN

New PIN

Confirm PIN

Cancel OK

Reset Device

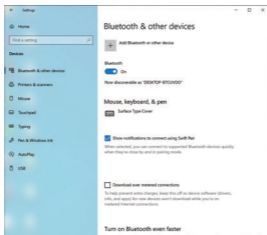
NOTE when you reset your device, all data stored will be deleted including your credentials. And the RESET operation requires to be done within 10 minutes after it is powered up.

Bluetooth pairing

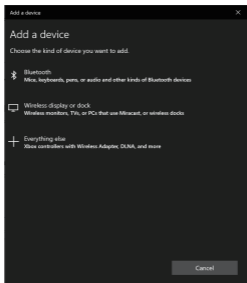
Before using the Bluetooth of AllinPass K33 to do authenticate, the security should be paired with your local host.

Windows 10 host machine:

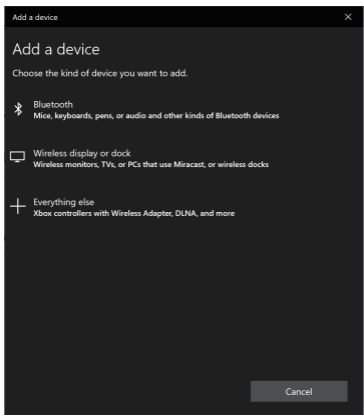
- 1 Go to **'devices'** in Windows settings page and click **'Add Bluetooth or other device'**.



- 2 On the popped up window, choose **'Bluetooth'**.



- 3 Long press the button on the side of AllinPass security key for at least 5 seconds until blue LED blinks rapidly, and choose the device name showed on the popped up window. Then the token is paired to the host machine.



Product Specification

Security Algorithm	ECDSA, SHA256, AES, HMAC, ECDH
Interface	USB-A or USB-C via USB cable, NFC, BLE
Communication Protocol	CTAPHID
Working Voltage	5.0V
Working Current	Stand-by: 80mA
Power	Stand-by: 0.4W
Working Temperature	-10°C - 45°C
Storage Temperature	-20°C - 70°C
Light	Green LED, Red LED, Blue LED
Casing Material	PC, ABS
Size	57*40*6mm

Fingerprint Module

Image Pixel 160 × 180 pixel

DPI 508 DPI

Sensor Service Life More than 200k times

Storage 50 fingerprints

Autonomic Learning Yes

False Accept Rate <0.001%

False Reject Rate <1%

Recognition Time <0.6s(for 120 Finger Points)

Acquisition Time <180 ms

