

Password-less Login Microsoft Azure Active Directory with FEITIAN Security Key

Content

- Overview 2
- Manage FEITIAN security keys 2
 - Windows 10 version 1809 or lower 2
 - Non-biometric FEITIAN security keys 2
 - Biometric FEITIAN security keys 2
 - Windows 10 version 1903 or higher 7
- Register FIDO2 security keys to AAD 12

Overview

FEITIAN FIDO2 security keys support newest Microsoft Azure Active Directory passwordless authentication capabilities. This document guides users to manage and register FEITIAN security keys.

Manage FEITIAN security keys

- Windows 10 version 1809 or lower

Non-biometric FEITIAN security keys

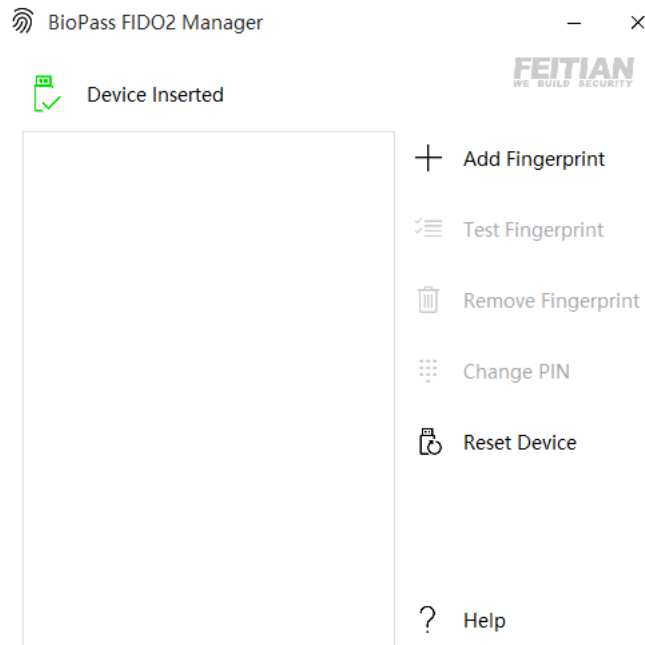
Contact us directly world.sales@ftsafe.com.

Biometric FEITIAN security keys

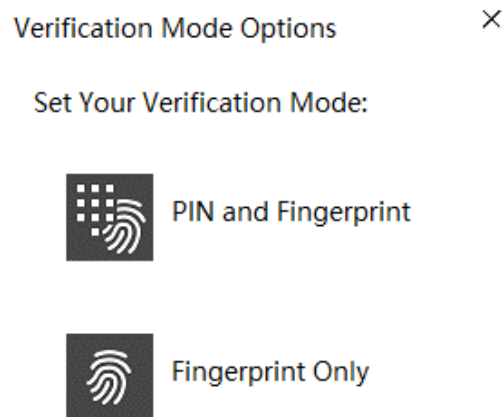
'*BioPass FIDO2 Manager.exe*' is required and can be downloaded via Microsoft store if users are working on Windows 10. Otherwise, the tool is available from FEITIAN official website: <https://ftsafe.com/Support/Resources>. Then the following steps guide you to manage your security keys:

1. Enroll your first fingerprint.

Launch the BioPass FIDO2 Manager and plug in the FEITIAN BioPass FIDO2, you will see the following window:



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



2). Set Pin and then click OK, supports numbers, letters and special symbols.

Note: Setting up a PIN requires user to touch the sensor to prove user presence.

Set PIN

×

Set PIN for BioPass FIDO2

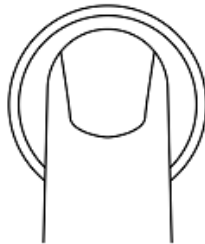


OK

3). Add fingerprint following the instructions.

Add Fingerprint

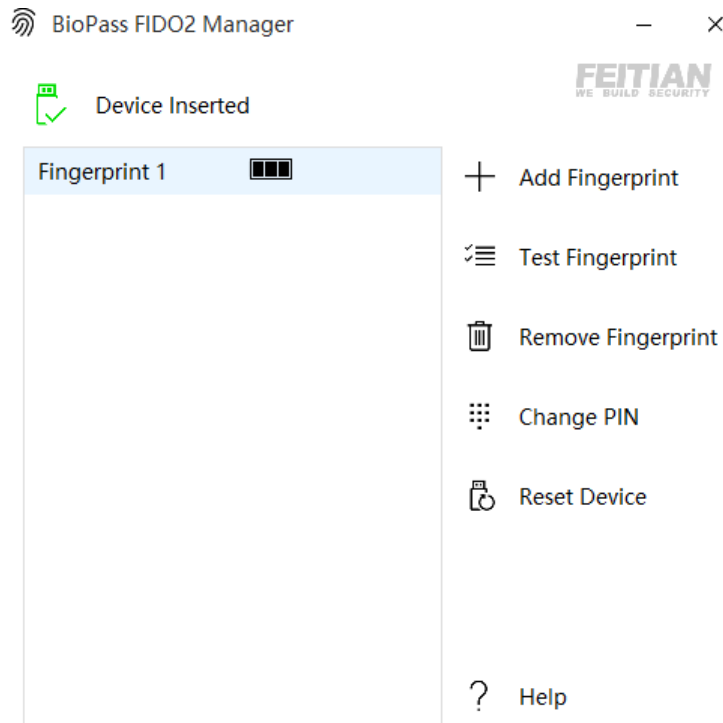
×



Great, touch sensor

Repeatedly lift and rest your finger on the sensor until setup is complete.

4). After the fingerprint successfully enrolled, there should be a fingerprint listed in the text box.



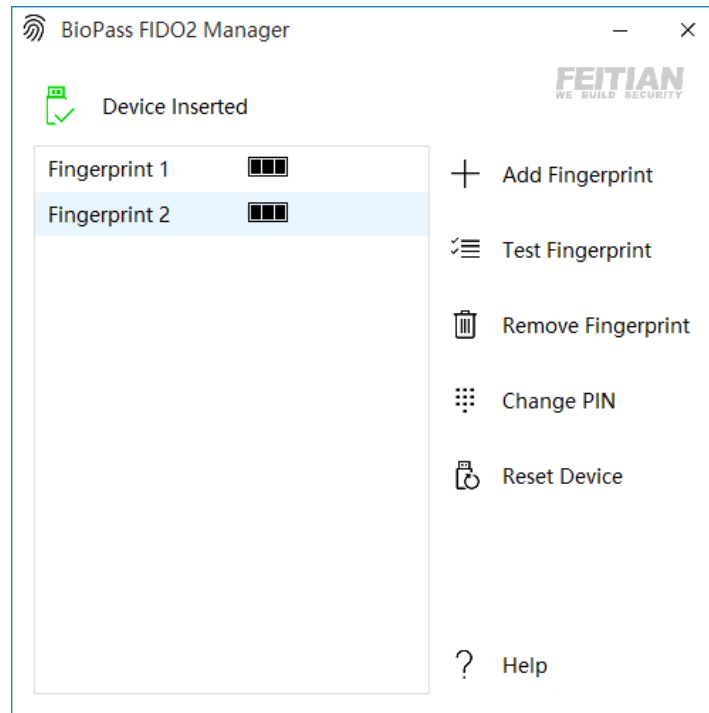
5). Then, you can test your fingerprint, remove your fingerprint and change pin through the BioPass FIDO2 Manager and enjoy your secure authentication experience.

2. Test Fingerprint

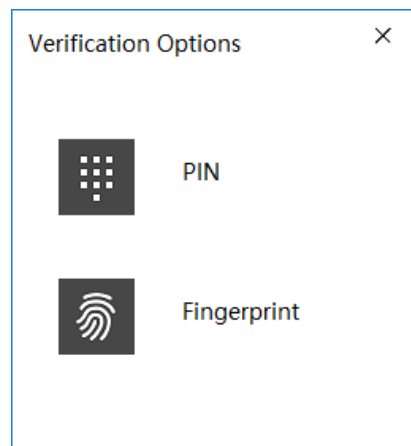
This function is for user to test the fingerprint verification. Note: This testing function will trigger the block device procedure mentioned above.

3. Remove fingerprint

1). Make sure you choose the fingerprint you want to delete. (“Fingerprint 2” as shown in example)



2). If there is a Pin, you need to choose a verification option



3). After verification, the fingerprint will be removed.

4. Change Pin

Just fill in all the text boxes for changing Pin.

A screenshot of a Windows dialog box titled "Change PIN" with a close button (X) in the top right corner. The dialog contains the text "Change PIN for BioPass FIDO2" and three input fields labeled "Old PIN", "New PIN", and "Confirm PIN". At the bottom, there are two buttons: "Cancel" and "OK".

5. Reset Device

Note: when you reset your device, all data stored will be deleted including your credentials.

Note: This needs to be done within 10 seconds after the token is powered up and a touch is needed to prove user presence.

- Windows 10 version 1903 or higher

Users can now set up a security key straight from Settings if the platform is Windows 10 version 1903 or above. In sign-in options/Security key, users are able to manage fingerprint, PIN or reset a security key.

1). Click Manage button, and touch the security key while the LED blinking.

Sign-in options

*Some of these settings are hidden or managed by your organization.

Manage how you sign in to your device

Select a sign-in option to add, change, or remove it.



Windows Hello Face

This option is currently unavailable—click to learn more



Windows Hello Fingerprint

This option is currently unavailable—click to learn more



Windows Hello PIN

This option is currently unavailable—click to learn more



Security Key

Sign in with a physical security key

Manage a physical security key that can log you into applications.


[Learn more](#)


Manage


2). Set up a PIN.

Before enrolling a fingerprint, a PIN is required to add by click Add button.

Windows Hello setup ×

 **Security Key Fingerprint**
Personalize your security key
[Set up](#)

 **Security Key PIN**
Creating a PIN for your security key helps keep you secure
[Add](#)


 **Reset Security Key**
Remove everything from this security key and reset to factory settings
[Reset](#)

[Close](#)

Input your PIN, be noted, the length is limited 4 to 63 characters.


Windows Hello setup ×


Set up a security key PIN




3). Once PIN is set; users are able to enroll their fingerprints by click Set up button.

Windows Hello setup ×

 **Security Key Fingerprint**
Personalize your security key

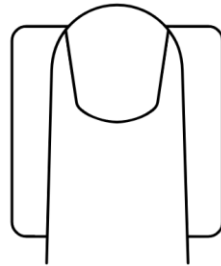
 **Security Key PIN**
Creating a PIN for your security key helps keep you secure

 **Reset Security Key**
Remove everything from this security key and reset to factory settings

After PIN is verified, users may follow the instructions to sample their fingerprint.

Windows Hello setup

×



Touch the fingerprint sensor

Repeatedly lift and rest your finger on the sensor on the top of your device until setup is complete.

Cancel

3). Reset FEITIAN security key.

Please be noted: RESET needs to be done within 10 seconds after the authenticator is powered up, and a touch is needed to prove user presence.

Simply click Reset button.

**Security Key Fingerprint**

Personalize your security key

Add another

Remove

**Security Key PIN**

Creating a PIN for your security key helps keep you secure

Change

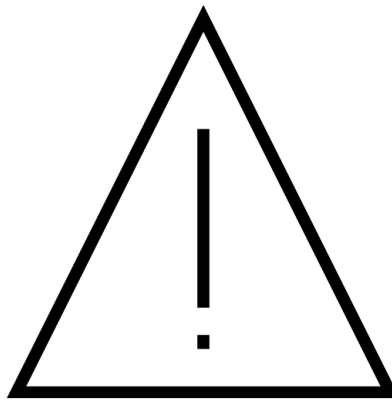
**Reset Security Key**

Remove everything from this security key and reset to factory settings

Reset

Close

Users need to remove the token and re-plug it into PC and then click *Proceed* to continue.

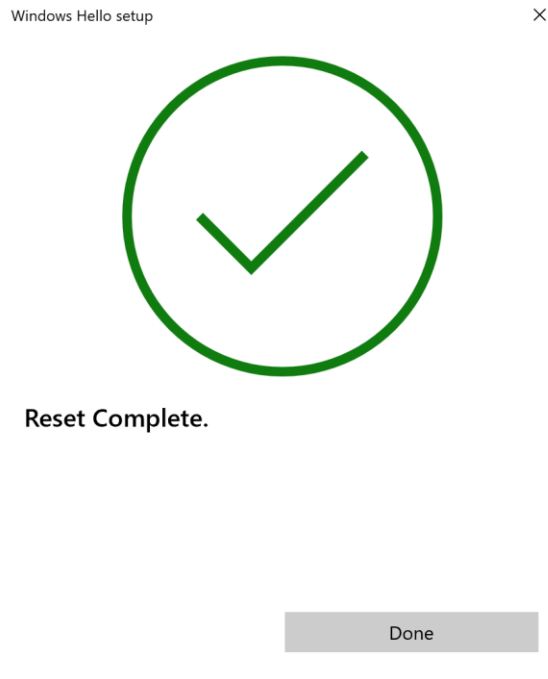
**Reset Security Key**

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

Proceed

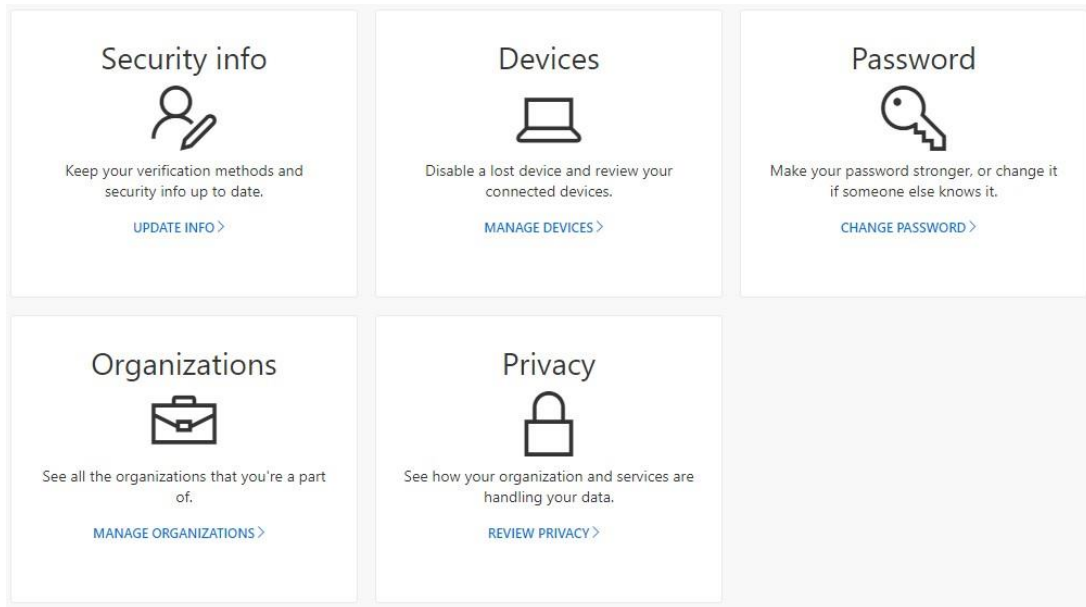
Cancel

Before reset is completed, users need to touch the security key twice within 10 seconds while it is blinking.

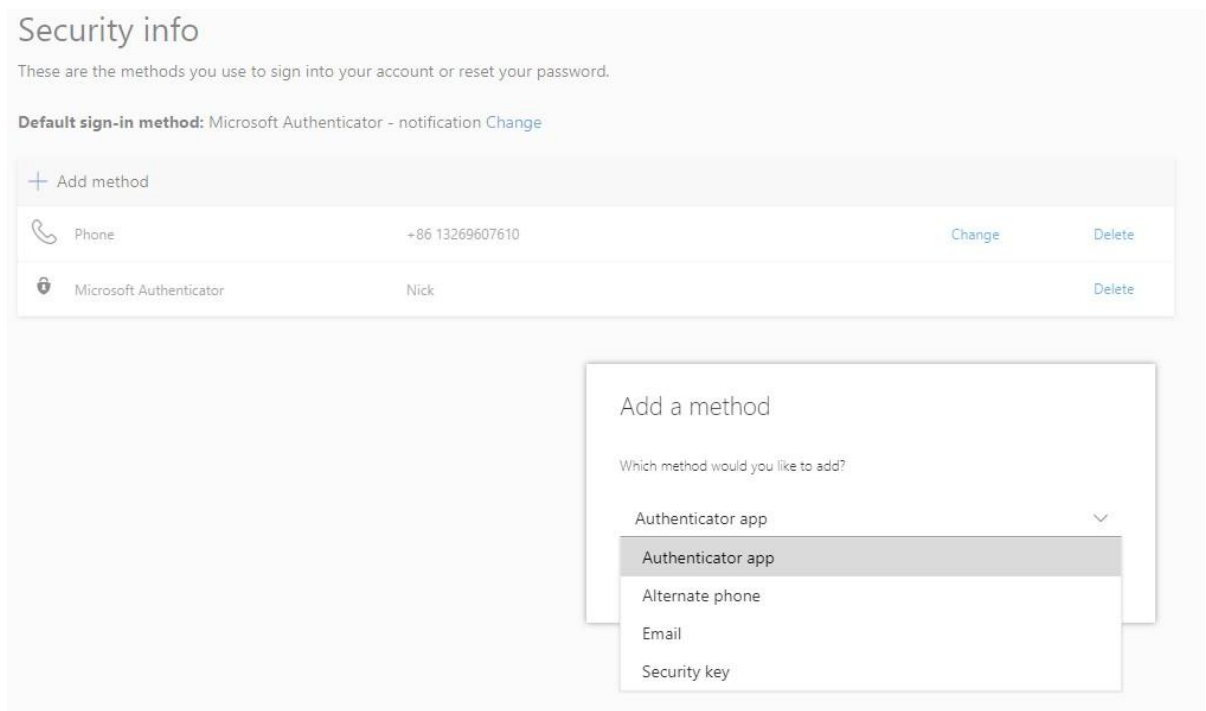


Register FIDO2 security keys to AAD

1. Browse to <https://myprofile.microsoft.com> and sign in if not already using Edge browser.
2. Click *Security Info*
 - a. If the user already has at least one Azure Multi-Factor Authentication method registered, they can immediately register a FIDO2 security key.
 - b. If they don't have at least one Azure Multi-Factor Authentication method registered, they must add one.



3. Add a FIDO2 Security key by clicking Add method and choosing Security key.



4. After clicking Add. Choose USB device or NFC device.

5. Insert your key and choose *Next*.
6. A box will appear and ask you to create/enter a PIN for your security key, then perform the required gesture for your key either biometric or touch. During this operation, you may be required to touch the key twice depending whether you create or enter a PIN.



7. You will be returned to the combined registration experience and asked to provide a meaningful name for your token so you can identify which one if you have multiple. Click *Next*.

Security key

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

FEITIAN BioPass Key

Cancel

Next

8. Click Done to complete the process.

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.

Done
