K33 Demo guide with Microsoft services

Contents

1. Introduction

This document describes how to use FEITIAN's K33 to demo Microsoft's services via HID, BLE and NFC interfaces.

2. Security key management

Note: enrollment of fingerprint needs to be done via USB cable.

Users can manage fingerprints, PIN or reset a security key straight from Settings if the platform is Windows 10 Insider Preview Build 18298 (19H1) and above or 1903 and above via the selection of Sign-in options/Security Key tab.

Note: Reset requires to be done with 10 seconds after powering up, and a touch is needed to prove user presence.

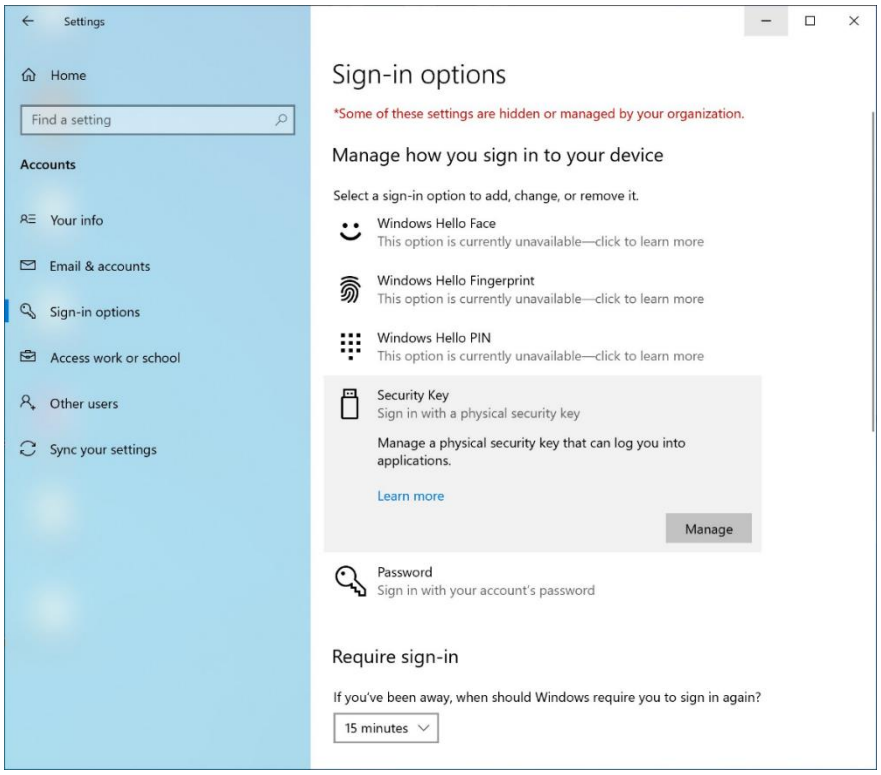


Figure 1 Windows 10 Security Key Settings Page

Users can manage fingerprint, PIN or reset a security key by using FEITIAN's BioPass FIDO2 manager on the Microsoft Store if platform is lower than Insider Build 18298 (19H1) or lower than 1903. This guide will explain enrolling a fingerprint on the BioPass FIDO2 Manager.

Before using the Feitian BioPass FIDO2, users are required to initialize and enroll a fingerprint onto the security key using 'BioPass FIDO2 Manager'. The application can be downloaded via Microsoft Store.

Enroll your first fingerprint.

1) Launch the BioPass FIDO2 Manager and plug in the FEITIAN BioPass FIDO2. Figure 2, see below, will appear.

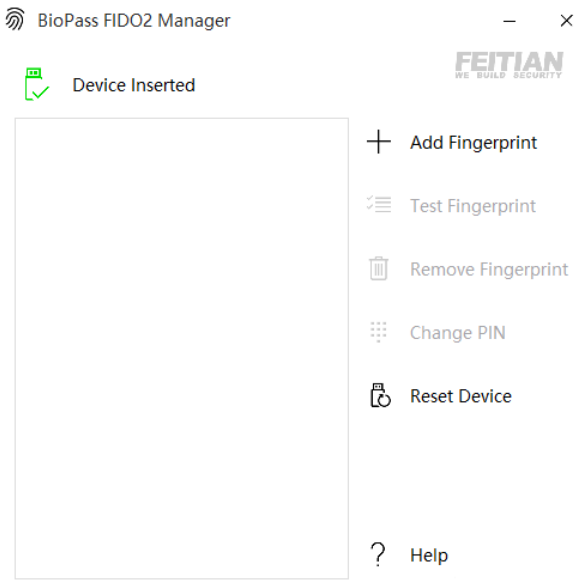


Figure 2 BioPass FIDO2 Manager

2) Click “Add Fingerprint.” You can choose using fingerprint only or set both pin and fingerprint for a verification method as shown in Figure 3. (Once you choose one option, you cannot change to the other option without resetting the device)

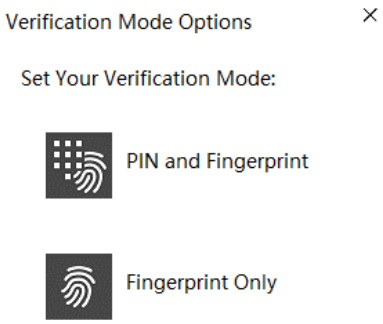


Figure 3 Verification Settings Page

3) If you choose “PIN and Fingerprint,” you will then be prompted to set a PIN. Numbers, letters and special symbols are supported.

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

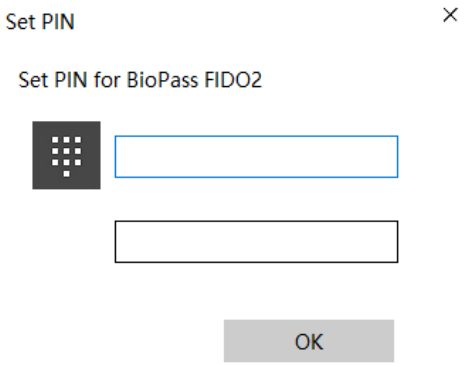


Figure 4 PIN Setup

4) Add a fingerprint by following the instructions.

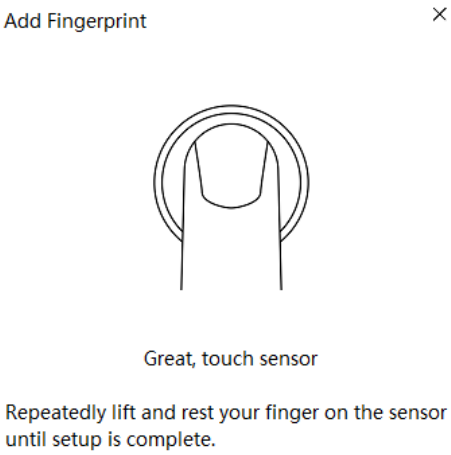


Figure 5 Fingerprint Enrollment

5) After a fingerprint has been successfully enrolled, a fingerprint will be listed in the text box.

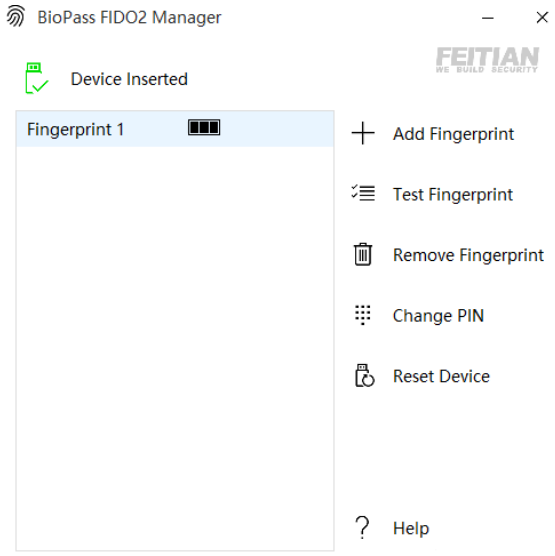


Figure 6 BioPass FIDO2 Manager with Fingerprint Enrolled

6) The BioPass FIDO2 Manager allows you to test your fingerprint, remove your fingerprint and change your pin to enjoy your secure authentication experience.

Test Fingerprint

This function is for the user to test the fingerprint verification.

Note: This testing function will trigger the **block device** procedure mentioned above.

Remove fingerprint

1) Choose the fingerprint you want to delete. (“Fingerprint 2” as shown in Figure 7)

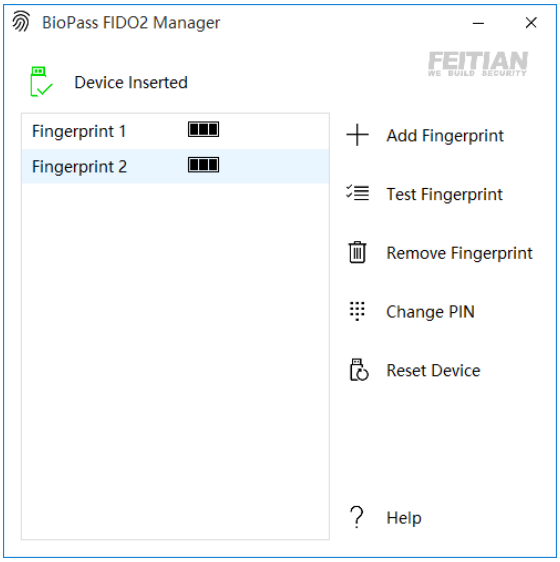


Figure 7 BioPass FIDO2 Manager with Fingerprint Enrolled

2) If a Pin has been enrolled, you will need to choose a verification option

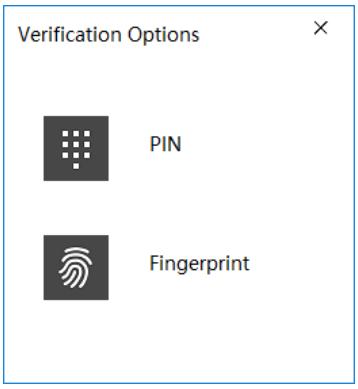


Figure 8 Verification Options

3) After verification, the fingerprint will be removed.

Change Pin

Press “Change PIN” in the BioPass FIDO2 manager to change a PIN.

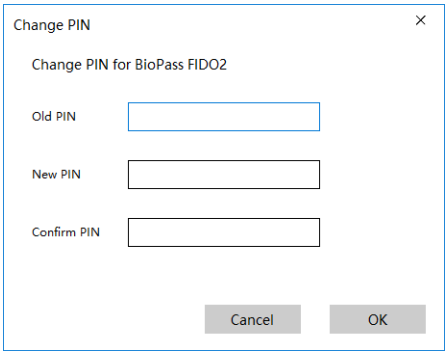


Figure 9 Change PIN

Reset Device

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

This operation need to be done with 10 seconds after the security key is powered up, and a touch is needed to prove user presence.

3. HID interface

K33 security key is plugged into your PC via a USB cable.

3.1 Microsoft account

Requirement: Windows 10 Version 1809 or later and the Microsoft Edge browser

Provision a security key to your Microsoft Account

Go to the Microsoft account page and sign in as you normally would.

Select ***Security > Update***

Figure 10 Microsoft Account Settings Page

Choose ***More security options***.

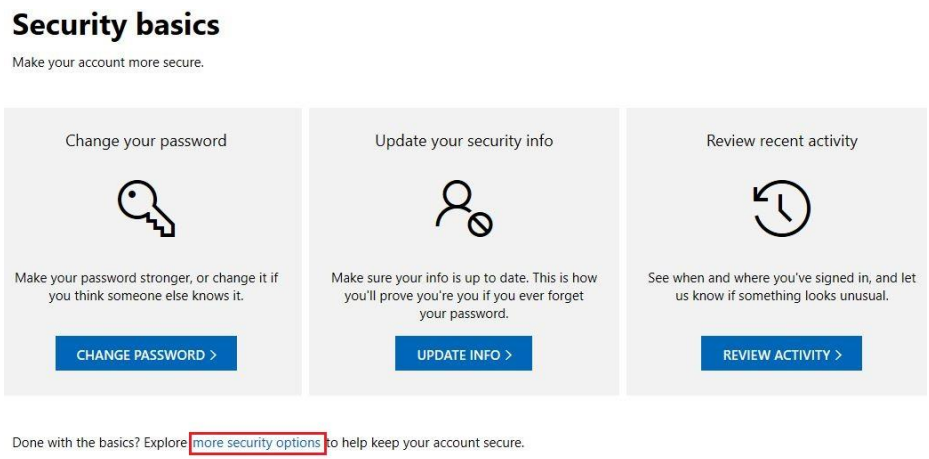


Figure 11 Microsoft Account Basic Security Settings

Under Windows Hello and security keys, select ***Set up a security key.***

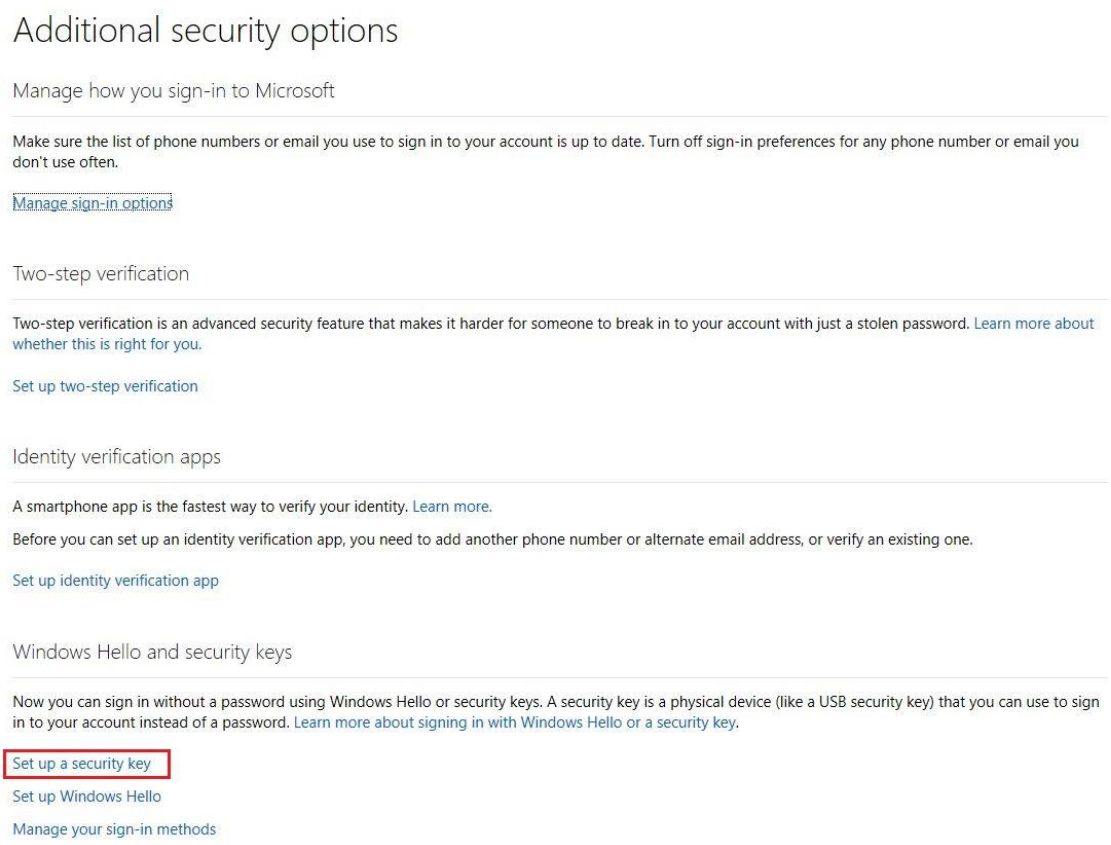


Figure 12 Microsoft Account Security Page

Identify what type of key you have (USB or NFC) and select ***Next***.

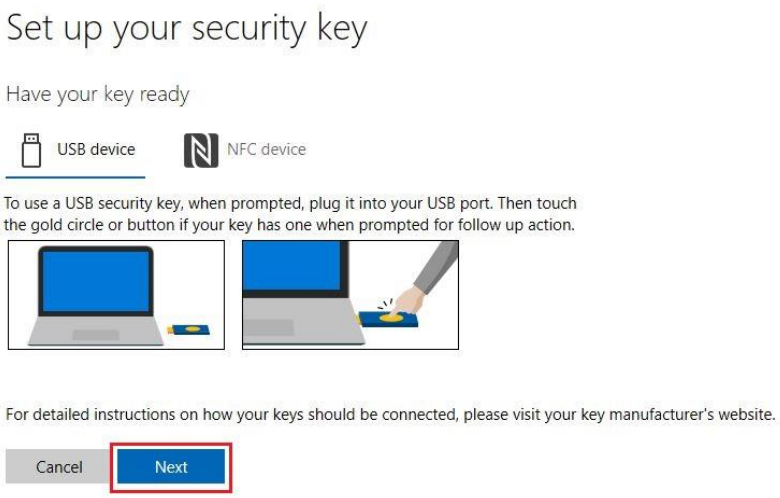


Figure 13 Security Key Setup

You will be redirected to the setup experience where you will insert or tap your key.

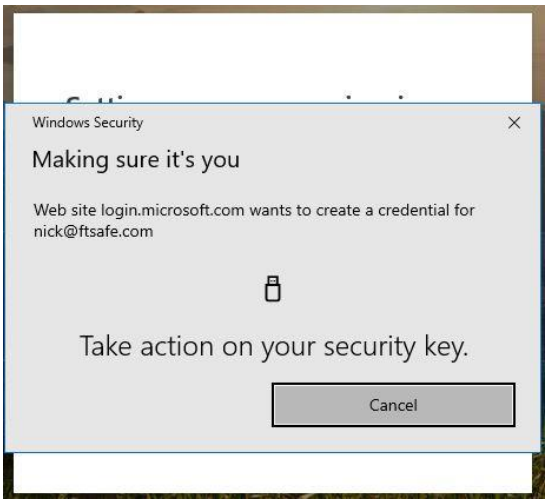


Figure 14 Security Key Setup

Create a PIN (or enter an existing PIN if you have already created one), otherwise if you have already enrolled a fingerprint, you will only need to verify the fingerprint.

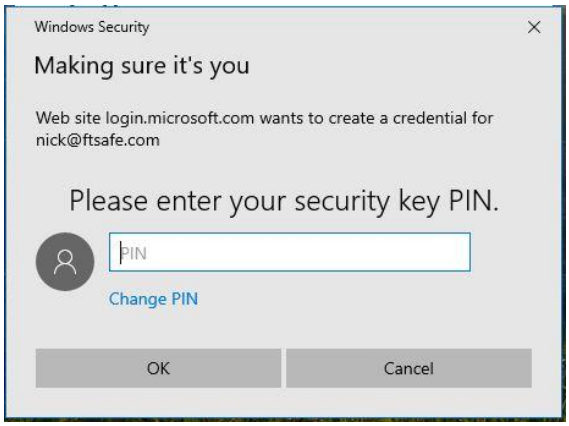


Figure 15 Security Key Setup

Take the follow-up action by touching either the button or gold disk if your key has one (or read the instruction manual to figure out what else it might be).

Name your security key so that you can distinguish it from other keys.

Figure 16 Security Key Setup

Sign out and open Microsoft Edge, select Use Windows Hello or security key instead, and sign in by inserting or tapping your key.

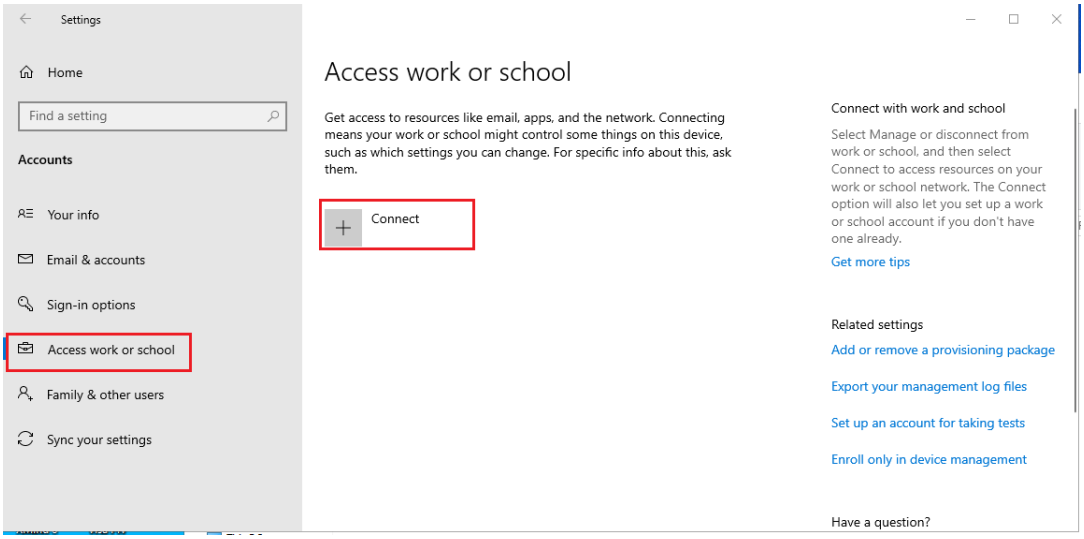
3.2 Windows Hello for business (Azure Active Directory)

Set up shared Windows (Joined AAD)

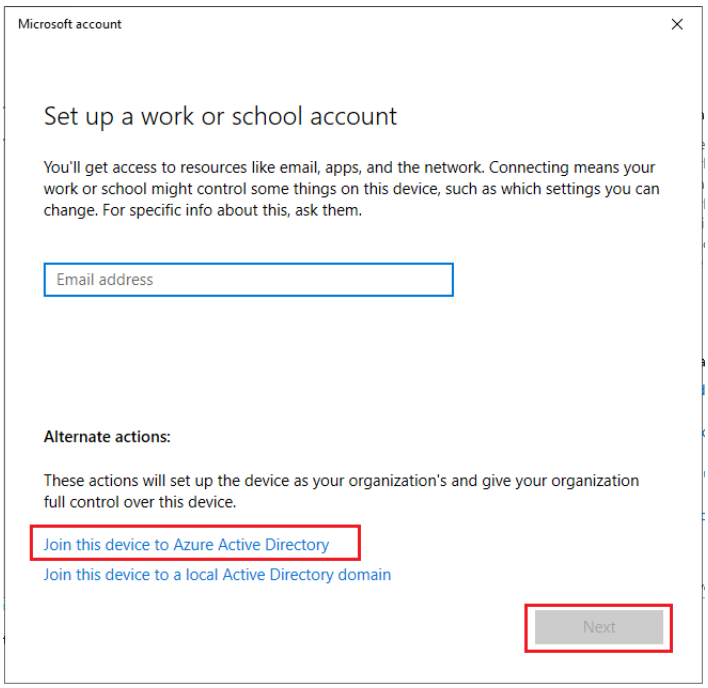
This chapter introduces how we FEITIAN setup the joined PC environment and provisioning a security key to your account.

Requirement: **Windows RS5 or above.**

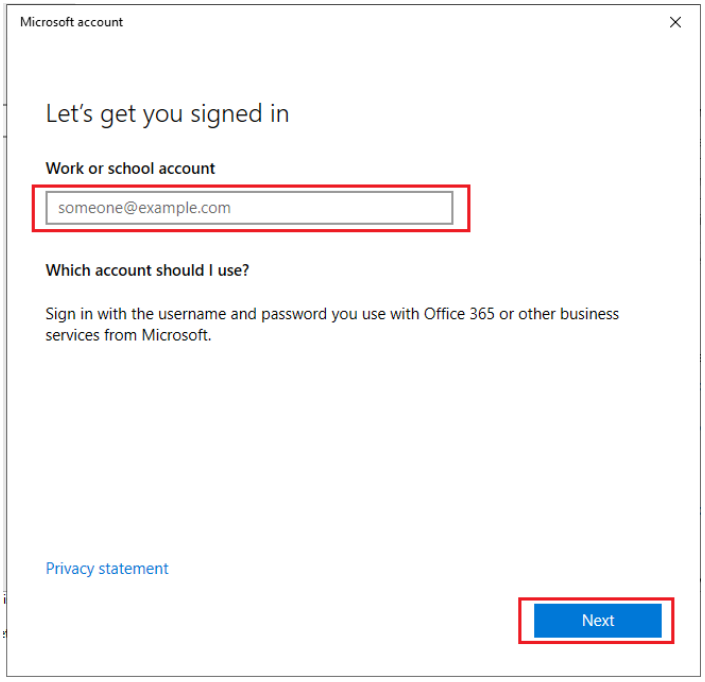
Go to setting's page and click ***'Access work or school'*** selection in ***'Account'***. Click ***'Connect'*** button.

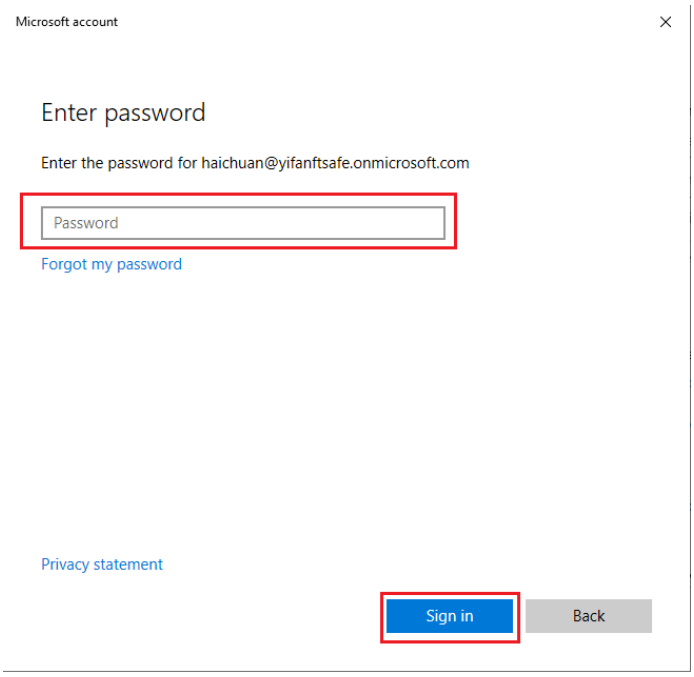


On Pup-up window, click ***'Join this device to Azure Active Directory'*** and click ***'Next'.***

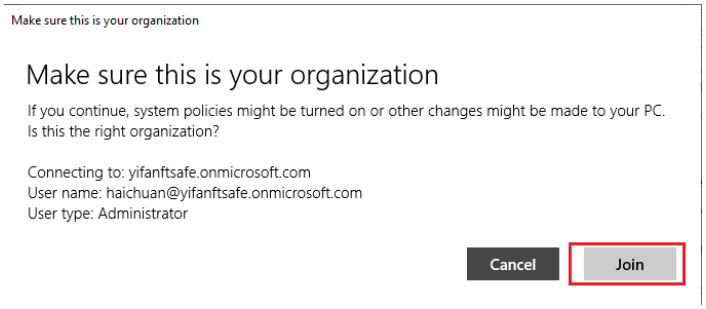


Enter your account and passwords, click ***'Sign in'***.

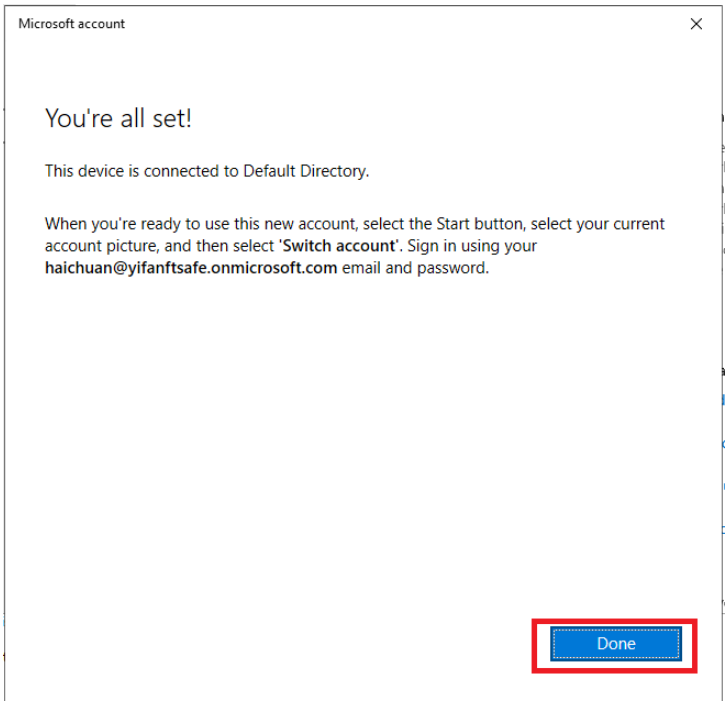




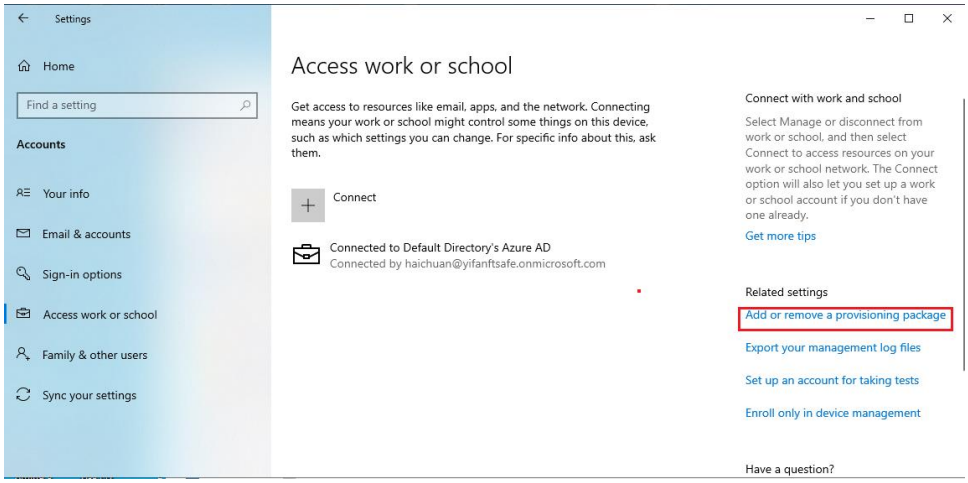
Click ***'Join'***.



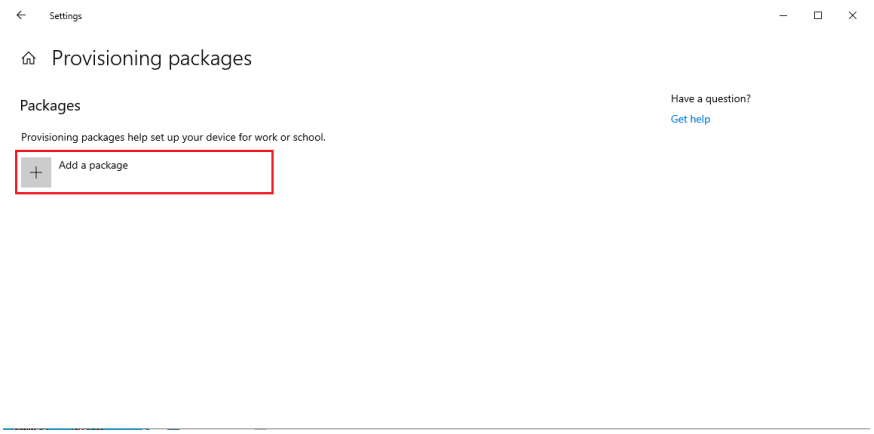
Click ***'Done'*** once you finish the procedures.



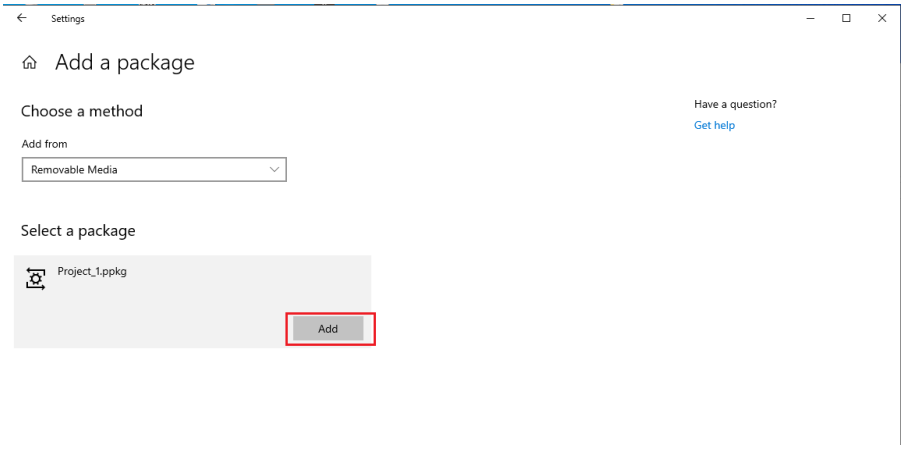
Return the selection of ***'Access work or school'*** and click ***'Add or remove a provisioning package'***.



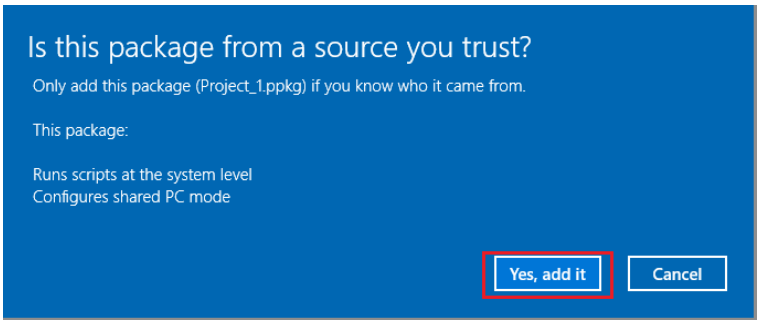
Copy that *.ppkg file to a USB flash disk and click ***'Add a package'***.



Windows will automatically detect the package file and click ***'Add'.***

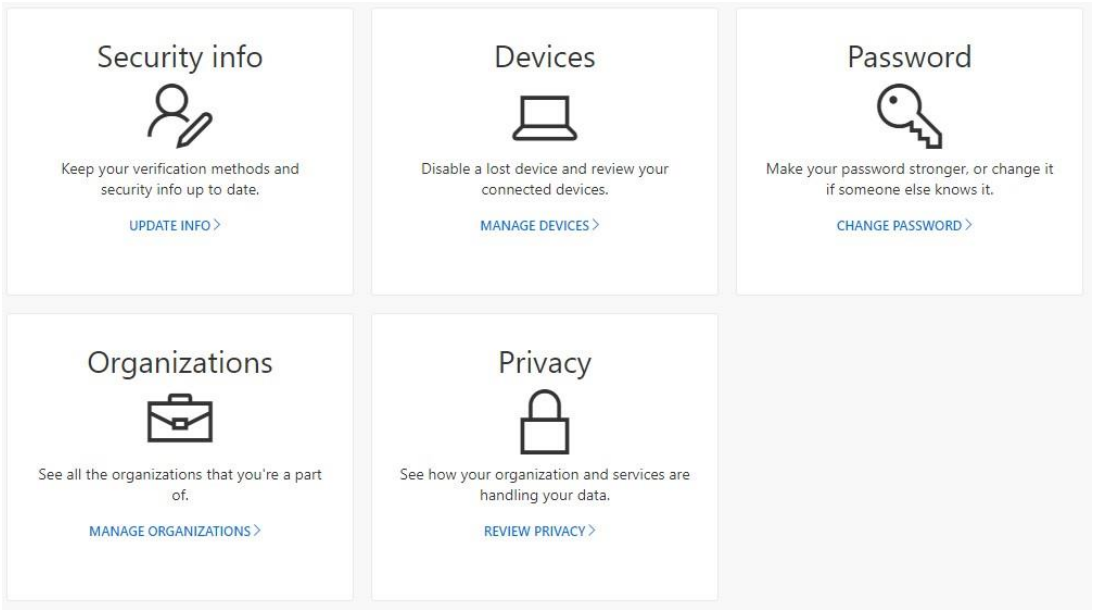


Once finish, click '**Yes, add it**'.

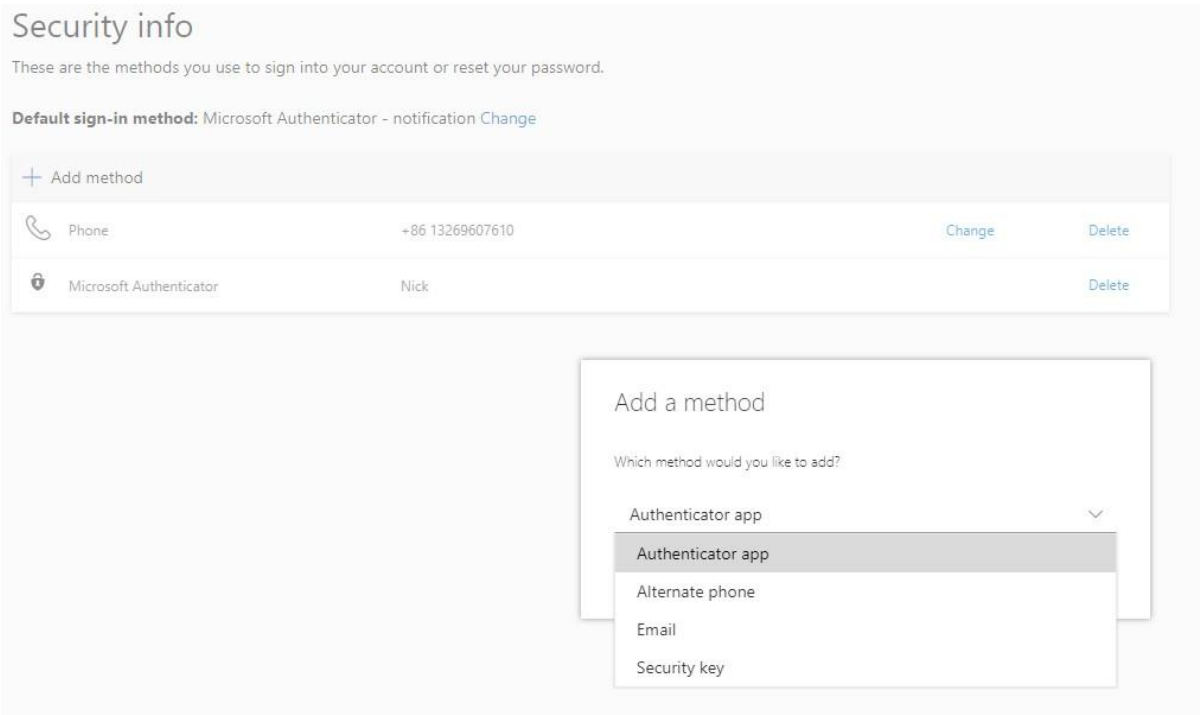


Register a security key to your Azure AD account.

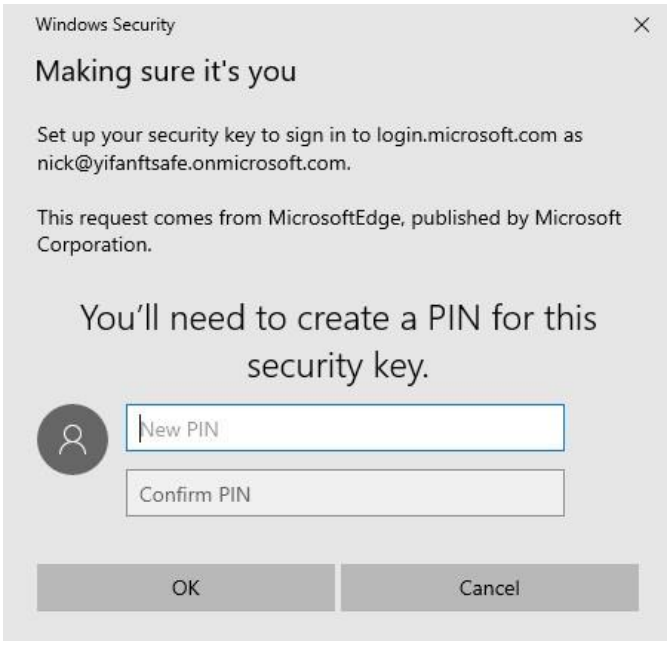
- Browse to ***https://myprofile.microsoft.com*** and sign in if not already using Edge browser.
- Click ***Security Info***
  a. If the user already has at least one Azure Multi-Factor Authentication method registered, they can immediately register a FIDO2 security key.
  b. If they don't have at least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



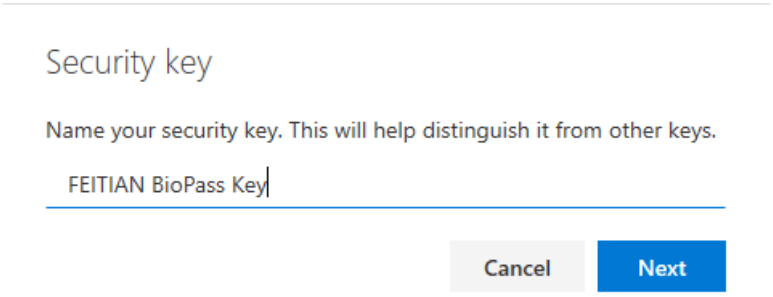
- Add a FIDO2 Security key by clicking ***Add*** method and choosing ***Security key.***



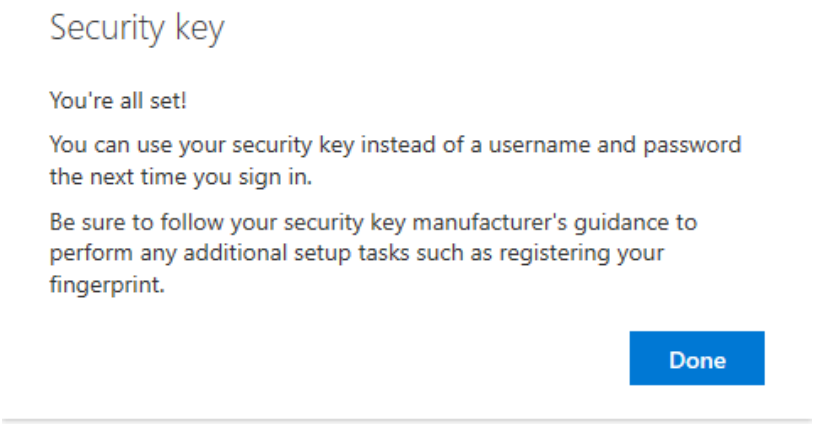
- After clicking ***Add***. Choose USB device or NFC device.
- Insert your key and choose ***Next***.
- A box will appear and ask you to create/enter a PIN for your security key, then perform the required gesture for your key either biometric or touch. During this operation, you may be required to touch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



- 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***.



- Click ***Done*** to complete the process.



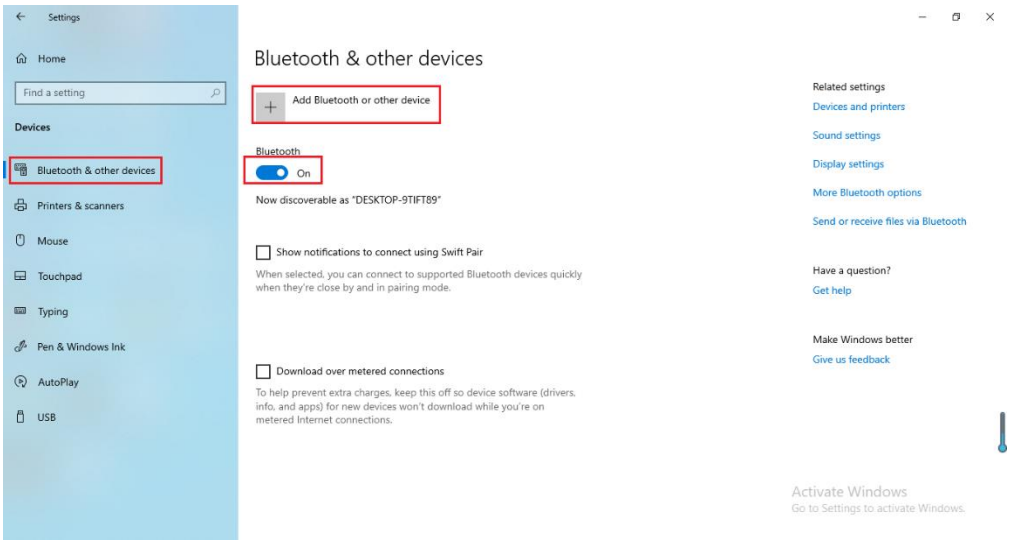
Once all above procedures are done, you can experience logging in your shared PC password-less.

4. BLE interface

Security key talks to PC via BLE interface.

Pair K33 security key to PC

Go to ***Windows Settings/Devices/Bluetooth and other device*** and then click ***'Add Bluetooth or other device'*** after you enable the Bluetooth for both PC and K33.

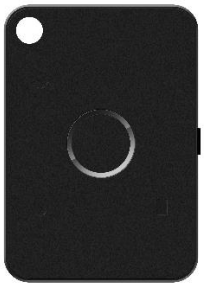


Enable the Bluetooth of K33:

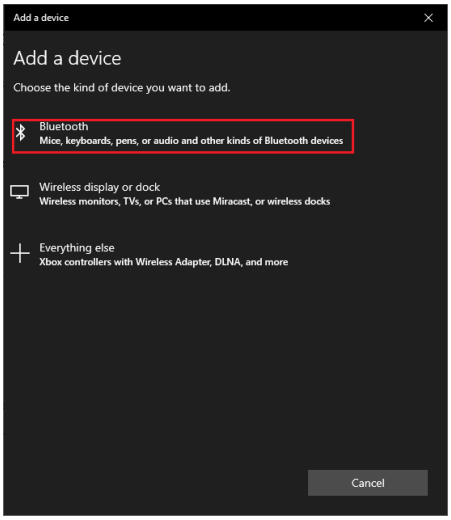
long-press the button of K33 on the right side for about 5 seconds until Bluetooth LED blinks rapidly.

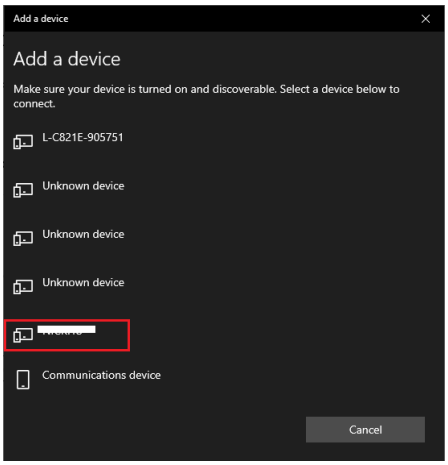
The BLE device paring name should be:

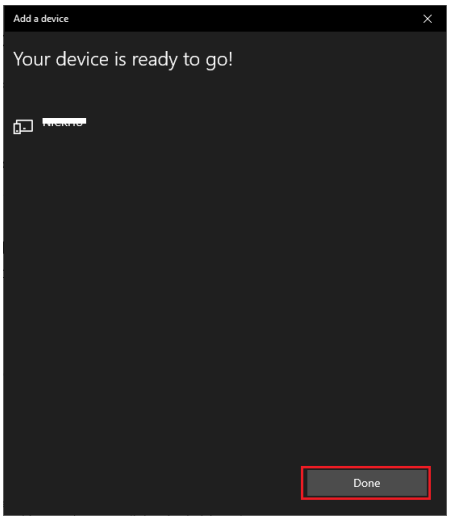
6 digits of characters or FT_6 digits of characters.



Follow the pop-up instruction windows for pairing procedures as below:







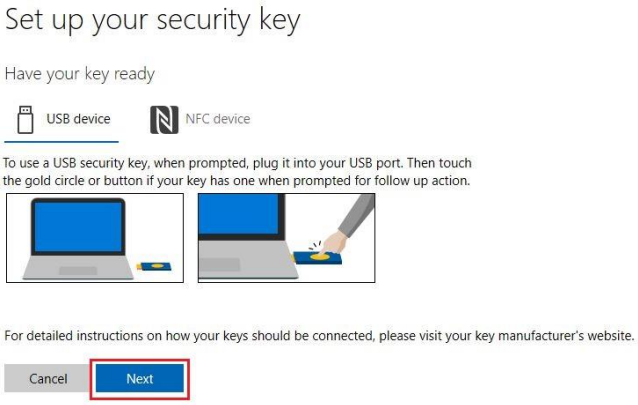
Once it is done, you can now demo K33 with Microsoft services contactless using Bluetooth.

4.1 Microsoft account

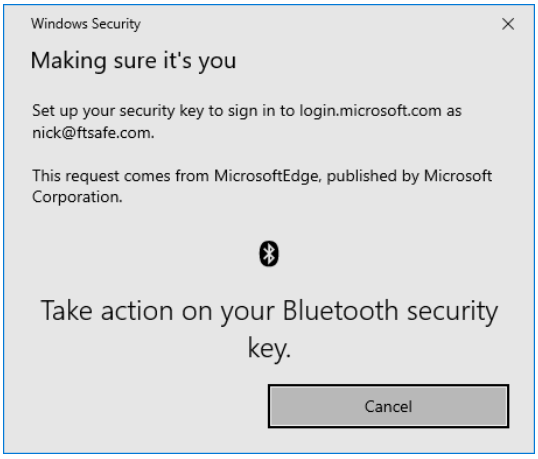
Refer chapter 3.1

Enable the K33's Bluetooth interface by long pressing the button for about 5 seconds before ***setting up your security key***.

Click ***Next*** directly.



The pop-up window requires you to verify your fingerprint if you have enrolled one. Otherwise you will need to input the PIN.



Similarly, before you sign in using the security key via Bluetooth, you will need to activate the Bluetooth of the K33 by long pressing button for 5 seconds.

4.2 Windows Hello for business (Azure Active Directory)

Refer to chapter 3.2.

Please note that Bluetooth of the K33 will need to be activated before the procedures of provisioning security key and Windows signing in.

5. NFC interface

Communication via NFC requires PC support, otherwise, an NFC reader will be needed.

To demo Microsoft account and Windows Hello for business (Azure Active Directory) services via NFC, please refer to the authentication process via HID. No additional steps are required.