

VINCSS FIDO2® FINGERPRINT USER MANUAL



Date: 01/03/2024

Number: CSS-PRD-PQMC-USG-240301-006

Document type: Public document

Written by: Product Department, VinCSS

VINCSS INTERNET SECURITY SERVICES JSC

No 7, Bang Lang 1 Street, Vinhomes Riverside, Viet Hung Ward, Long Bien District, Hanoi.

TABLE OF CONTENT

TABLE OF CONTENT	2
I. PRODUCT INFORMATION.....	6
I.1. General Information.....	6
I.2. Meaning of the LED indicator.....	7
II. MANAGING PIN CODE AND FINGERPRINT	8
II.1. Windows	8
II.1.1. <i>Connecting to computer</i>	8
II.1.1.1 Connecting via USB	9
II.1.1.2 Connecting via NFC	9
II.1.1.3 Connecting via Bluetooth	9
II.1.2. <i>Creating a new PIN</i>	12
II.1.3. <i>Changing PIN</i>	13
II.1.4. <i>Adding fingerprints</i>	15
II.1.5. <i>Removing fingerprints</i>	18
II.1.6. <i>Resetting</i>	19
II.2. macOS.....	23
II.2.1. <i>Creating a new PIN</i>	23
II.2.2. <i>Changing PIN</i>	25
II.2.3. <i>Adding fingerprints</i>	26
II.2.4. <i>Removing fingerprints</i>	28
II.2.5. <i>Managing sign-in data</i>	29
II.2.6. <i>Resetting</i>	31
II.3. Linux	32
II.3.1. <i>USB</i>	32
II.3.2. <i>Bluetooth</i>	33
II.3.2.1. Install Blueman on Ubuntu.....	33
II.3.2.2. Connect to VinCSS FIDO2® Fingerprint	34
III. PASSWORDLESS AUTHENTICATION USING VINCSS FIDO2® FINGERPRINT	34
III.1. Windows	34

III.1.1.	<i>Configuration on Azure AD system</i>	34
III.1.1.1.	Configuration on Azure AD	34
III.1.1.2.	Login Windows 10 using FIDO2 with provisioning packages	35
III.1.1.3.	Register authentication key for Azure AD	36
III.3.2.2.1.	<i>Using via Bluetooth</i>	37
III.3.2.2.2.	<i>Using via USB</i>	39
III.3.2.2.3.	<i>Using via NFC</i>	41
III.1.1.4.	Connect User to Azure Work Account.....	43
III.1.2.	<i>Login Windows</i>	46
III.1.2.1.	Using via Bluetooth.....	46
III.1.2.2.	Using via USB.....	47
III.1.2.3.	Using via NFC.....	47
III.2.	<i>Microsoft account</i>	48
III.2.1.	<i>Register authentication key</i>	48
III.2.1.1.	Using via Bluetooth.....	51
III.2.1.2.	Using via USB.....	53
III.2.1.3.	Using via NFC	54
III.2.2.	<i>Passwordless authentication of Microsoft accounts</i>	56
III.2.2.1.	Using via Bluetooth.....	57
III.2.2.2.	Using via USB.....	58
III.2.2.3.	Using via NFC	58
III.3.	<i>VinCSS OVPN Client</i>	59
III.3.1.	<i>Windows</i>	59
III.3.1.1.	Register for VinCSS FIDO2® Fingerprint security key	59
III.3.1.1.1.	<i>Using via Bluetooth</i>	60
III.3.1.1.2.	<i>Using via USB</i>	61
III.3.1.1.3.	<i>Using via NFC</i>	61
III.3.1.2.	Authentication with VinCSS FIDO2® Fingerprint security key	62
III.3.1.2.1.	<i>Passwordless authentication</i>	65
III.3.1.2.2.	<i>Authentication usernameless</i>	65
III.3.1.2.2.1.	<i>Using via Bluetooth</i>	66
III.3.1.2.2.2.	<i>Using via USB</i>	66
III.3.1.2.2.3.	<i>Using via NFC</i>	67

III.3.2. macOS.....	68
III.3.2.1. Register for VinCSS FIDO2® Fingerprint security key (<i>Only USB connection is supported</i>)	68
III.3.2.2. Authentication with VinCSS FIDO2® Fingerprint security key	69
III.3.2.2.4. Passwordless authentication	72
III.3.2.2.5. Authentication usernameless.....	72
III.3.2.2.2.1. Using via Bluetooth	73
III.3.2.2.2.2. Using via USB	74
III.3.2.2.2.3. Using via NFC	74
III.4. Two-factor authentication for Facebook	75
III.4.1. Register authentication key	75
III.4.1.1. Using via Bluetooth.....	77
III.4.1.2. Using via USB	78
III.4.1.3. Using via NFC	78
III.4.2. Two-factor authentication with Facebook account.....	79
III.4.2.1. Using via Bluetooth.....	80
III.4.2.2. Using via USB	80
III.4.2.3. Using via NFC	81
III.5. Two-factor with Twitter account.....	81
III.5.1. Register authentication key	81
III.5.1.1. Using via Bluetooth.....	83
III.5.1.2. Using via USB	83
III.5.1.3. Using via NFC	84
III.5.2. Two-factor authentication with Twitter account.....	85
III.5.2.1. Using via Bluetooth.....	85
III.5.2.2. Using via USB	86
III.5.2.3. Using via NFC	86
III.6. Two-factor authentication with Google account.....	86
III.6.1. Register authentication key	86
III.6.1.1. Using via Bluetooth.....	92
III.6.1.2. Using via USB	93
III.6.1.3. Using via NFC	93
III.6.2. Two-factor authentication with Google account.....	95

III.6.2.1.	Using via Bluetooth.....	95
III.6.2.2.	Using via USB.....	96
III.6.2.3.	Using via NFC	96
REFERENCES	98



I. PRODUCT INFORMATION



VinCSS FIDO2® Fingerprint

I.1. General Information

Information	Detail
Product name	VinCSS FIDO2® Fingerprint
USB type	USB Type-C
Bluetooth	Bluetooth Low Energy 5.0
NFC	ISO7816/ISO14443
Supported OS	Windows, macOS, Linux, Android, iOS
Authentication Methods	Passwordless, Strong Two Factor, Strong Multi-Factor
Certificate	FIDO2 Certified, FCC, JQA
Supported protocol	WebAuthn, FIDO2 CTAP1, FIDO2 CTAP2, Universal 2nd Factor (U2F)
Supported browser	Google Chrome, Mozilla Firefox, Apple Safari, Microsoft Edge, Microsoft Edge Chromium
Encryption algorithm	ECC p256
CPU	32-bit ARM® Cortex™-M4

Information	Detail
Account storage	50
Fingerprint storage	5
Indicator lights	RGB Led
Fingerprint Sensor resolution	508 dpi
Fingerprint Sensor FAR	< 0.0002%
Fingerprint authentication time	< 1s
Weight	20 gram
Product dimensions	43,5 x 38 x 8 (mm)
Battery	25mAh, Lithium-ion Battery
Battery life	5-7 days (<i>12 authentication times per day</i>)
Standby	4 months
Full charge time	2 hour 30 minutes
Operation Voltage/Current	5V/1A
Material	Heavy-duty high-grade polycarbonate plastic, ensuring product durability
Nhiệt độ hoạt động	-10°C ~ 60°C
Màu sắc	Black, White, Blue
Phụ kiện đi kèm	USB Type – C cable, keychain, holder accessory
Xuất xứ	Việt Nam

I.2. Meaning of the LED indicator

The VinCSS FIDO2® Fingerprint's LED indicator will let you know about current battery state, charging state or working mode. If the LED blinks.

LED indicator	Meaning	State
Blinking red 3 times in a row	The built-in battery is running low and needs to be charged	Using Bluetooth or NFC
Solid amber	The security key is being charged	Connecting with USB
Solid green	The security key is fully charged	Connecting with USB
Solid blue	Bluetooth mode On, the security key is connected to a Bluetooth device	Using Bluetooth
Blinking blue	The security key enters the pairing mode	Using Bluetooth
Blinking purple	NFC activated	Using NFC
Blinking white quickly	The security key is processing request and require user interaction	Requiring user verification by touching the fingerprint sensor

II. MANAGING PIN CODE AND FINGERPRINT

PIN code for VinCSS FIDO2® Fingerprint is required to add/remove fingerprints, in order to ensure the safety of the device and avoid adding unauthorized fingerprints, trying to scan fingerprints many times or fingerprints being deleted from unauthorized users.

Please follow the steps below to create/change PIN, manage fingerprints or reset VinCSS FIDO2® Fingerprint.

II.1. Windows

II.1.1. Connecting to computer

Note: The battery will be set to sleep mode to maintain the battery's standby time longer. For the first time using the NFC/Bluetooth function, users need to, requires the user to make a direct connection via a USB type C cable.

II.1.1.1 Connecting via USB

Plug the VinCSS FIDO2® Fingerprint into your computer using USB cable, make sure the security key is **not** in Bluetooth or NFC working mode. If the LED blinks red 3 times in a row, it indicates low battery level (*below 20%*), while the amber LED indicates the security key is being charged and the green LED indicates the battery is fully charged. The VinCSS FIDO2® Fingerprint security key can be used while charging.

II.1.1.2 Connecting via NFC

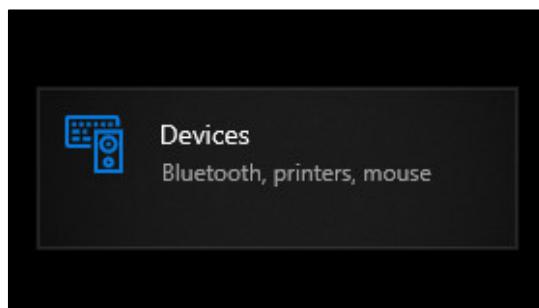
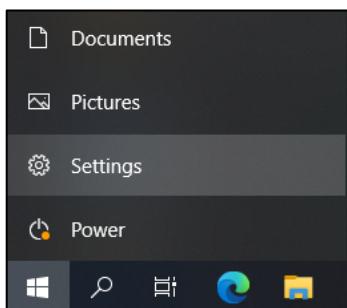
Put VinCSS FIDO2® Fingerprint on the NFC reader. When the LED indicator on the key turns purple, the VinCSS FIDO2® Fingerprint can be used.

Note:

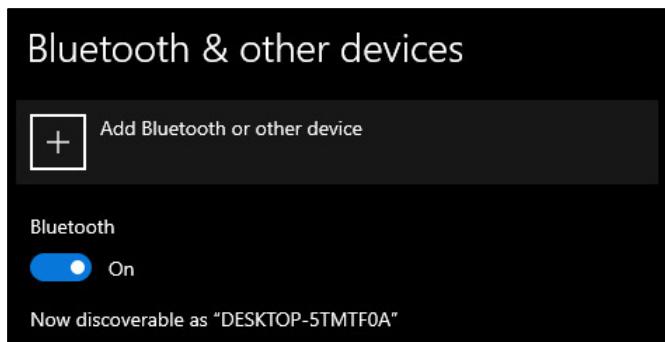
- For iPhone models from iPhone 7/8, iPhone 7/8 Plus and iPhone X: Open the control center, turn on NFC Tag Reader mode, then place the VinCSS FIDO2 Fingerprint security key on the iPhone's front camera, then Move the key down from 1/2 to 2/3 of the security key length. When the light turns purple, it means the NFC connection has been successful.
- For iPhone models from iPhone XS, iPhone XS max and above: you can directly connect the security key to the device according to the instructions above without opening NFC Tag Reader mode at the control center.

II.1.1.3 Connecting via Bluetooth

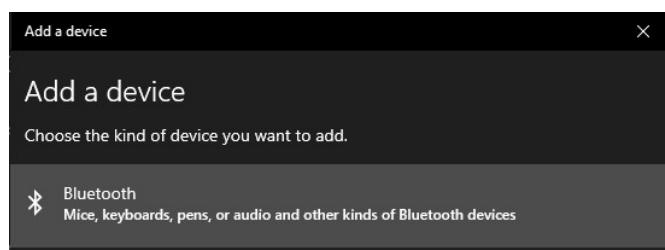
- In the off mode (*no LED indicator*), turn on the Bluetooth mode of the security key by holding down the fingerprint sensor for 5 seconds until the LED indicator on the key turns blue, the security key will connect automatically to the previously connected device.
- If the blue LED doesn't blink, hold the fingerprint sensor for 5 seconds to enter pairing mode.
- Go to **Windows > Settings > Devices**.



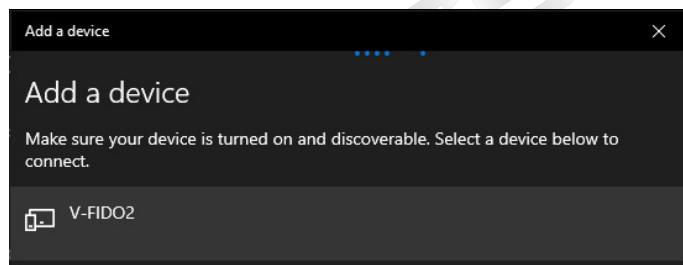
- In the **Bluetooth** section, select **On**, then select **Add Bluetooth or other device**.



- In **Add a device** section, select **Bluetooth**.

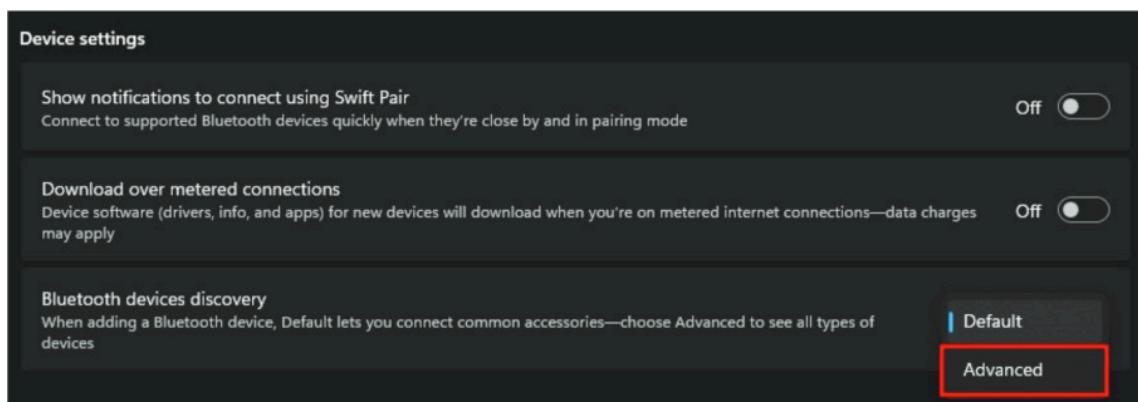


- Select the device named **V-FIDO2**.



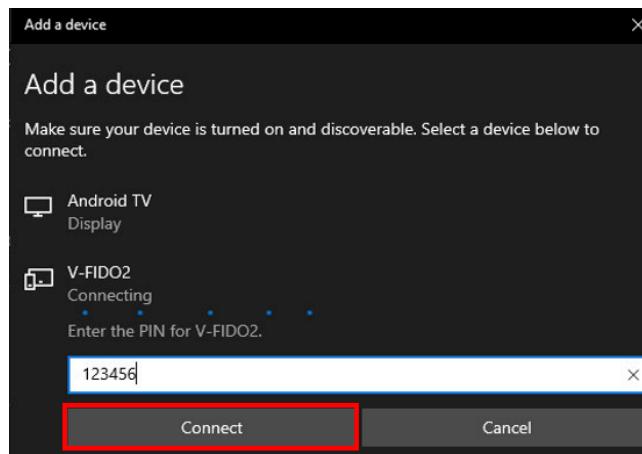
Note: Due to the change in the Bluetooth device visibility policy on Windows 11, the computer may not be able to find the security key. Then, please make changes to the settings as instructed below:

- **Open Settings -> Bluetooth & devices -> Devices -> Device settings.**
- **In the Bluetooth devices discovery section, select *Advanced*.**

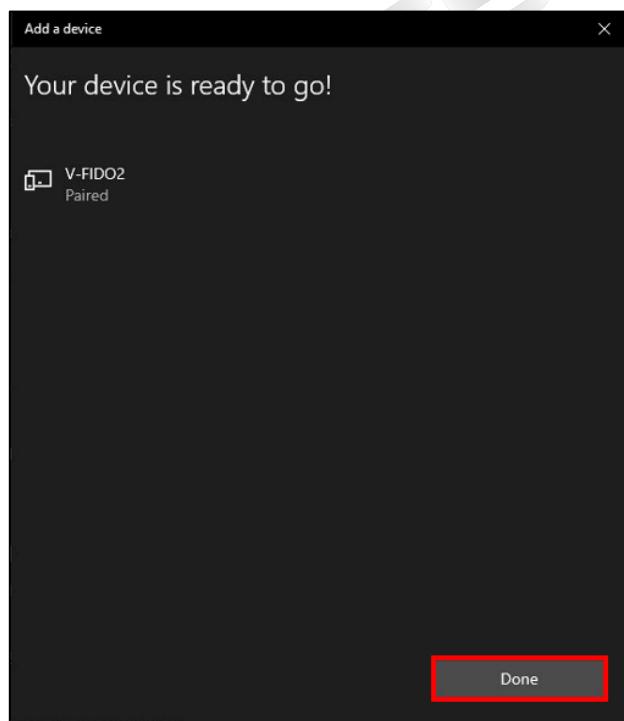


- Enter pairing code to connect. Then click **Connect**.

Note: *The pairing code is a sequence of the last 6 digits taken from serial code (In case the serial code has only the last 5 digits, enter the number “0” at the beginning of the serial. For example: XXX123456 => 123456 or XXX12345 => 012345).*



- Successful connection. Click **Done** to finish.



- After the successful connection, the connected security key and its remaining battery will appear on the device list.

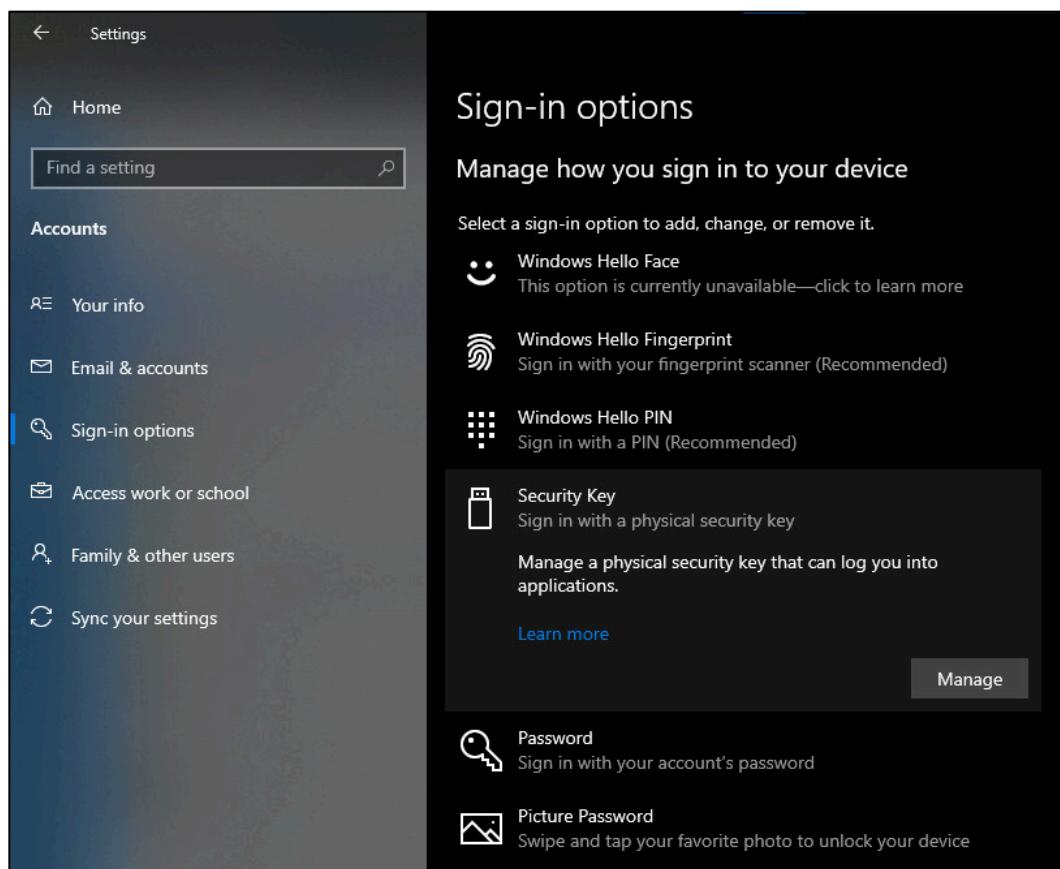


Note:

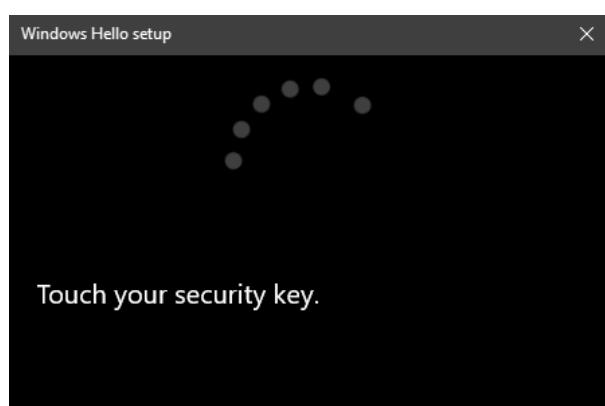
- In case you want to pair with a new device, hold down the fingerprint sensor for 5 seconds while the key is on.
- The security key will automatically disable BLE connection if there is no interaction for 90 seconds..

II.1.2. Creating a new PIN

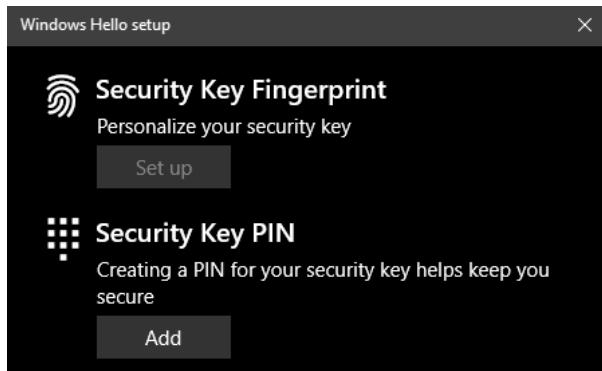
- Go to Start > Settings > Account > Sign-in options > Security Key. Then select Manage button.



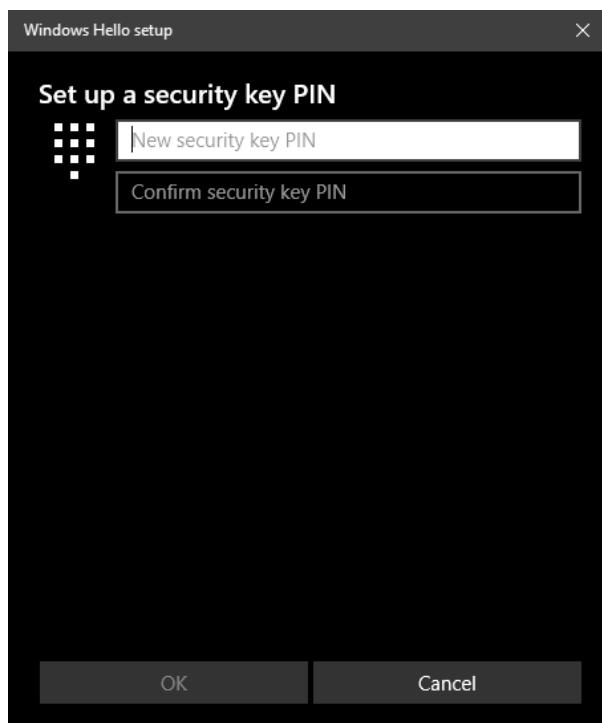
- Touch the fingerprint sensor on the security key.



- By default, VinCSS FIDO2® Fingerprint does not have a PIN. To create a new PIN for the key, in the **Security Key PIN**, click **Add**.

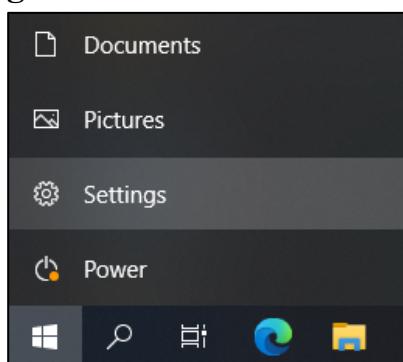


- Type in the new PIN (*From 4 to 63 characters include letters (lowercase, uppercase), numbers and special characters*), then click **OK**.

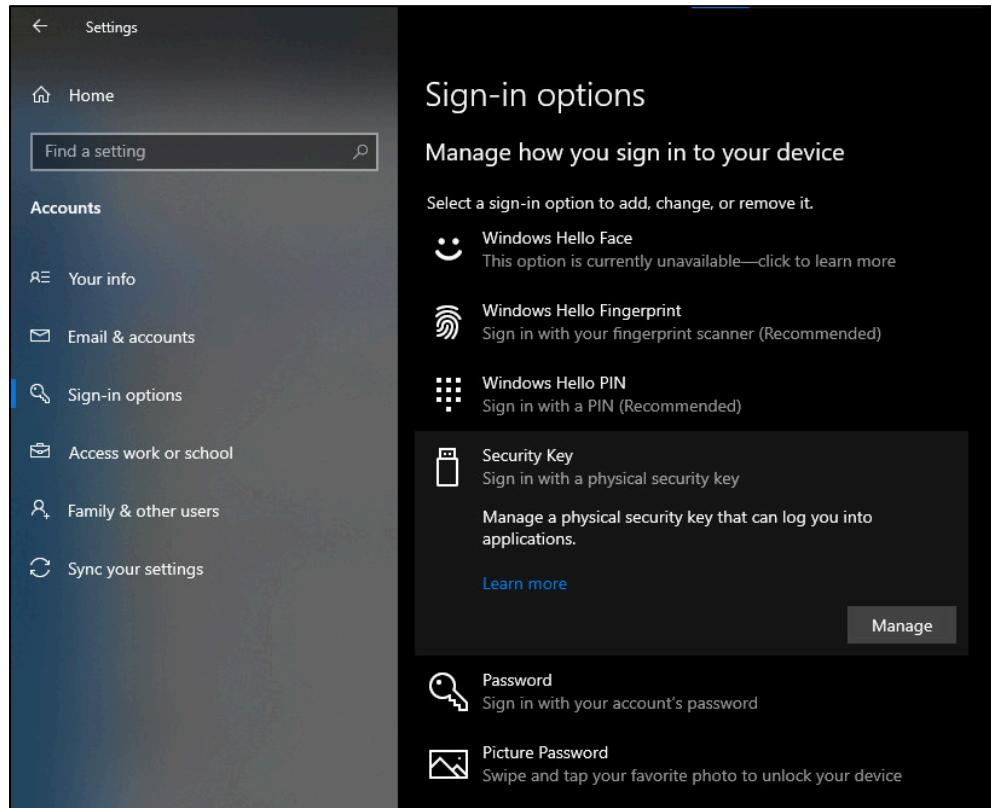


II.1.3. Changing PIN

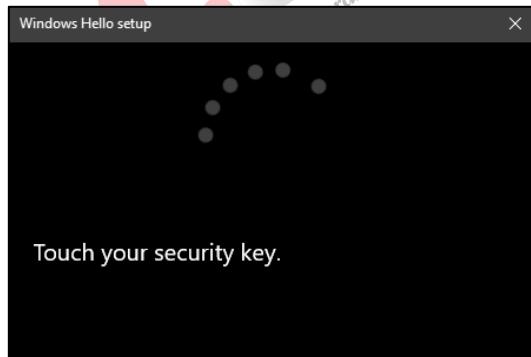
- Go to **Start > Settings**.



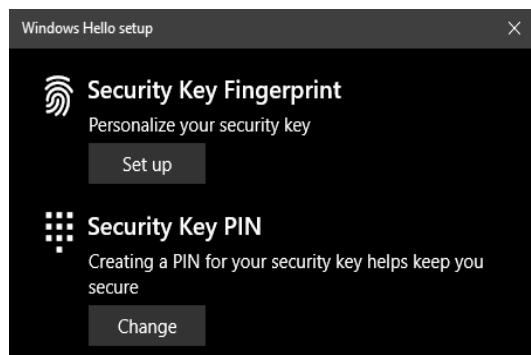
- Select Account > Sign-in options > Security Key. Then select Manage.



- Touch the fingerprint sensor on the security key.



- In Security Key PIN section, select Change to change the PIN code of the security key.



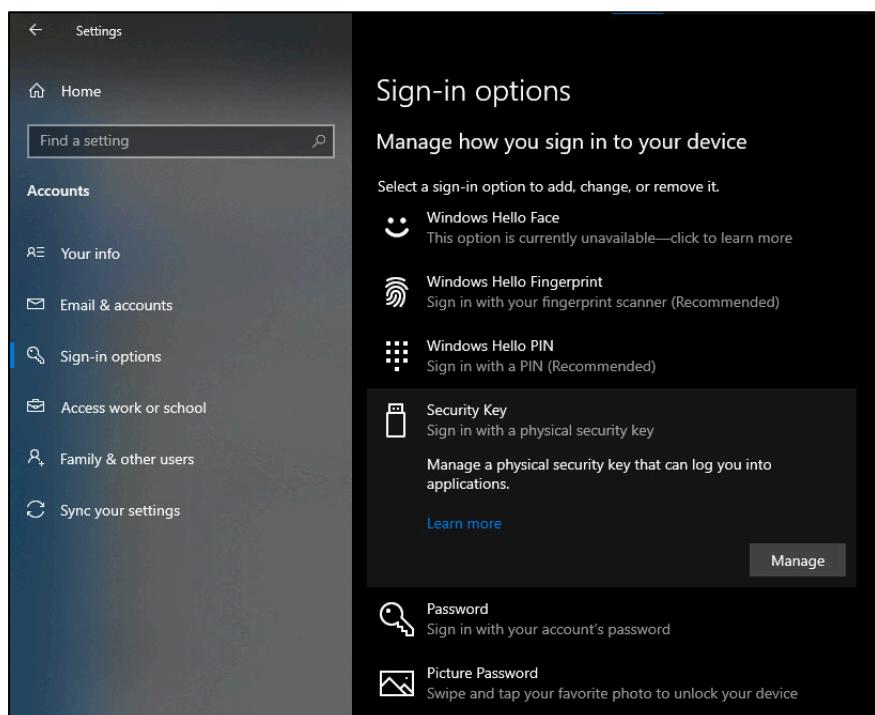
- Fill the information in order: old PIN, new PIN, confirm new PIN (*From 4 to 63 characters include letters (lowercase, uppercase), numbers and special characters*). Then select **OK**.



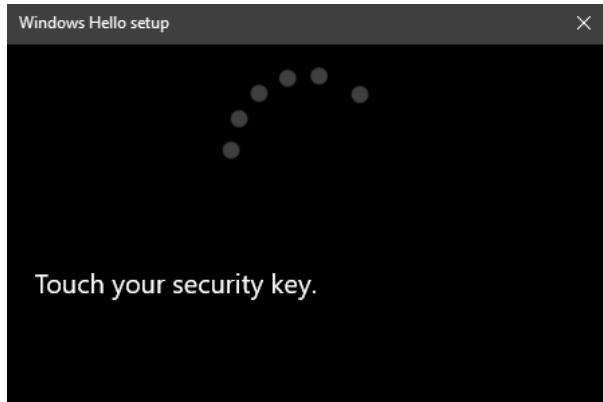
II.1.4. Adding fingerprints

After successfully creating a PIN for VinCSS FIDO2® Fingerprint, users can add fingerprints to the key (*up to 5 fingerprints*). Follow the steps below:

- Go to **Start > Settings > Account > Sign-in options > Security Key**. Then select **Manage**.



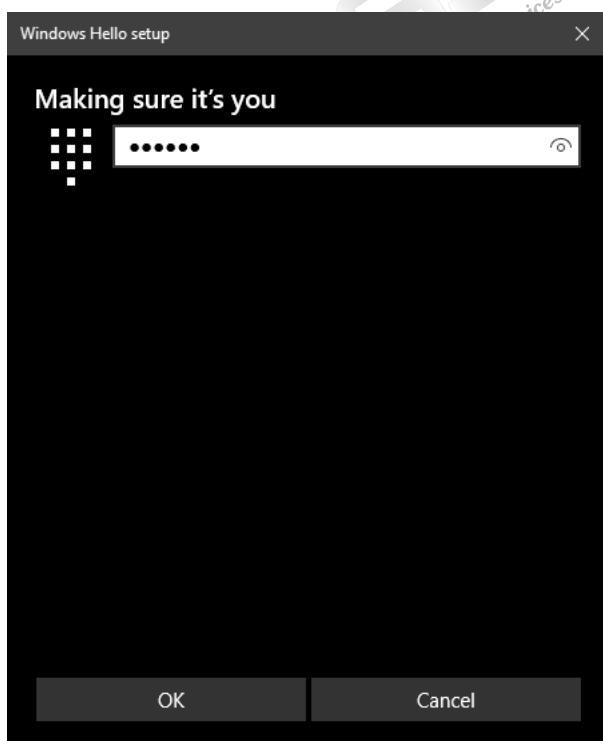
- Touch the fingerprint sensor on the security key.



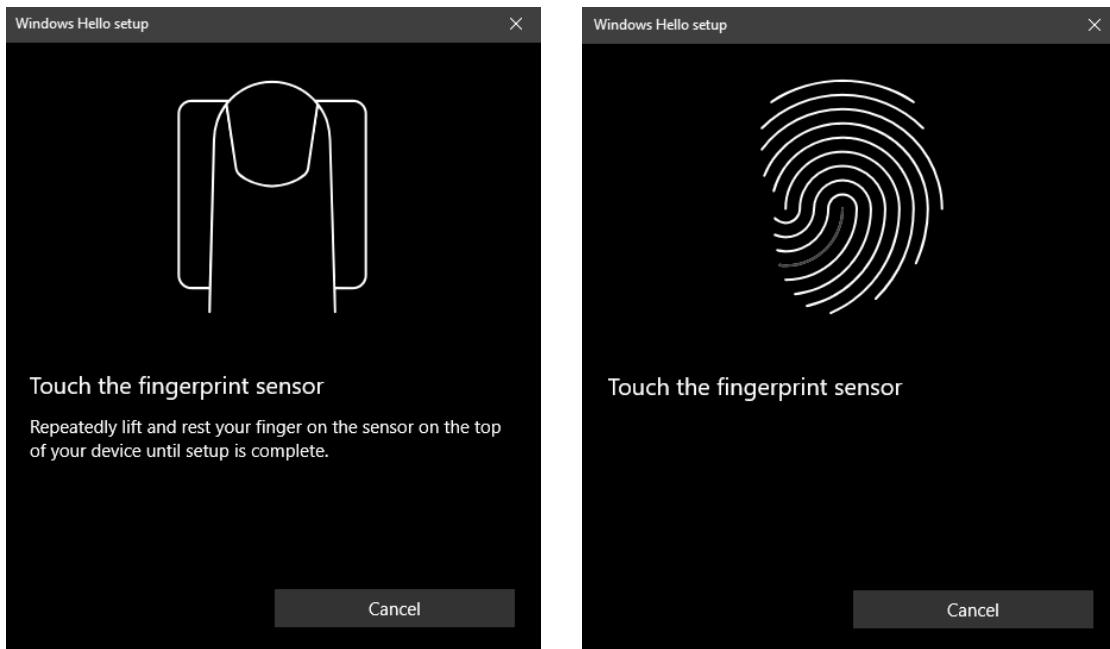
- In Security Key Fingerprint section, select Set up.



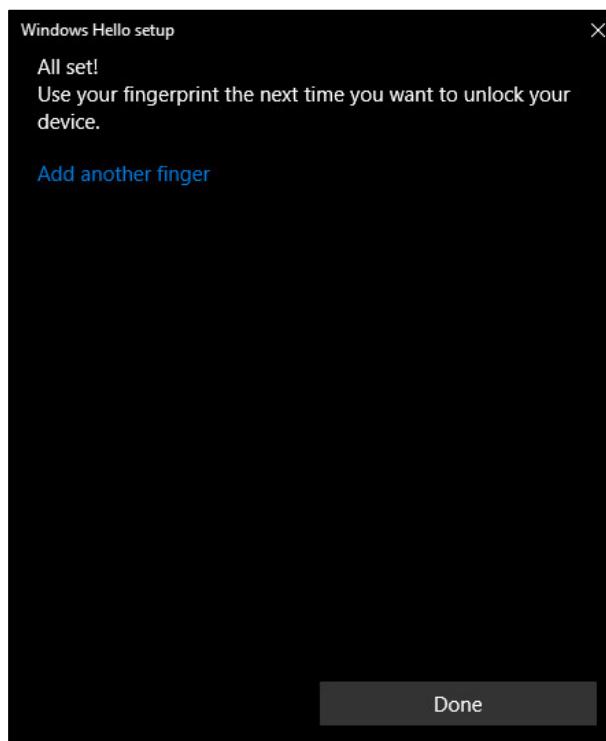
- Enter the PIN (*created in the above step*) then select OK.



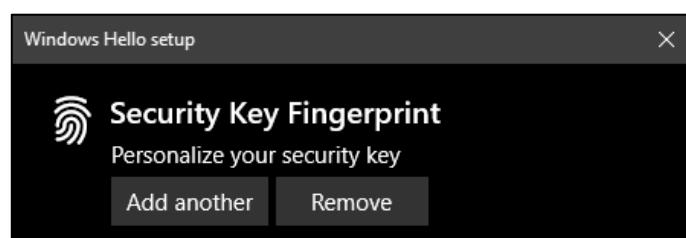
- Conduct fingerprint scanning by touching the fingerprint sensor with your finger until the light shows green, then lift your hand off the sensor (*5 times*).



- After finishing the fingerprint scan, select **Done** to finish.



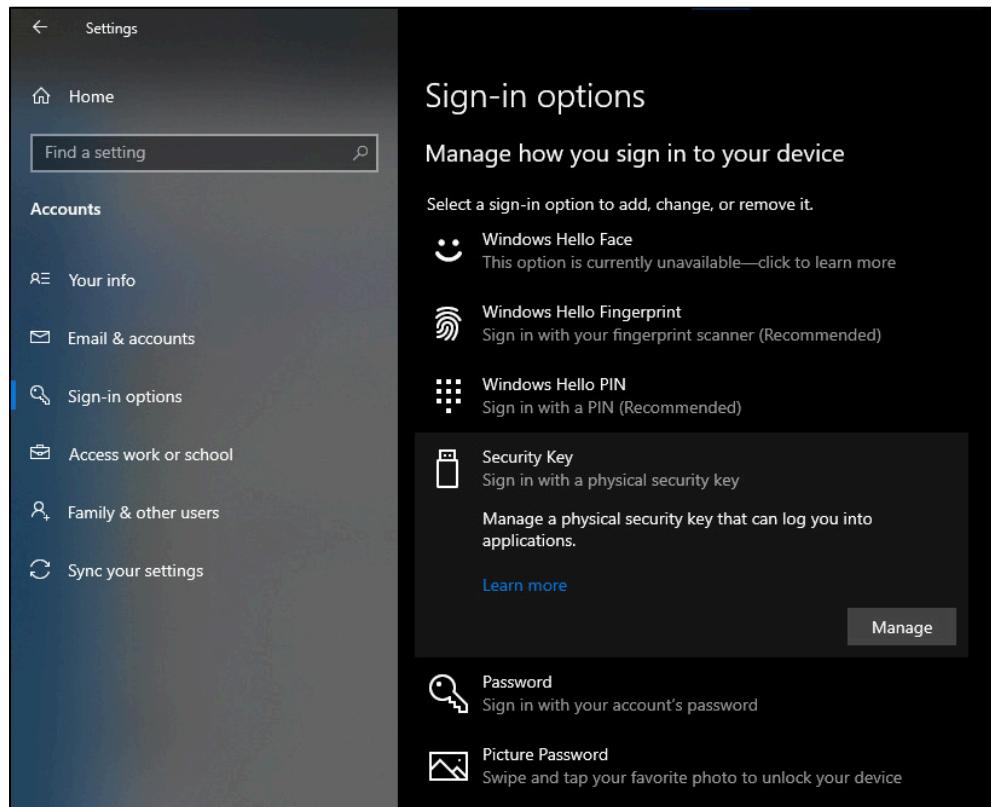
- To add more fingerprints, at **Security Key Fingerprint**, select **Add another**, then do the same steps as above.



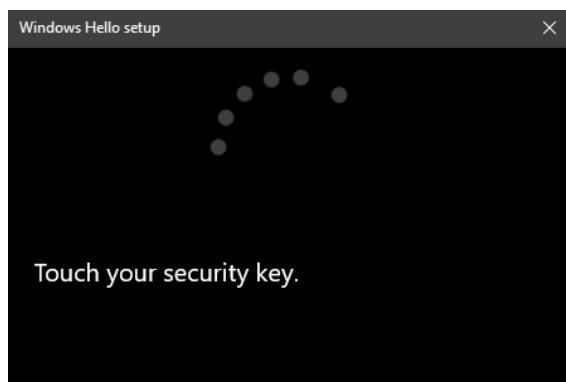
II.1.5. Removing fingerprints

Currently, Windows only allows users to delete all fingerprints on the security at once, not one by one. Follow the steps below:

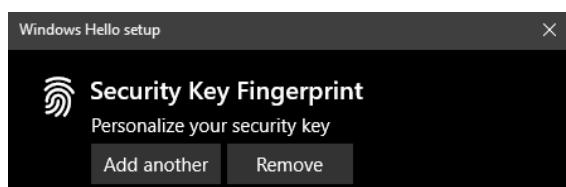
- Go to **Start > Settings > Account > Sign-in options > Security Key**. Then select **Manage** button.



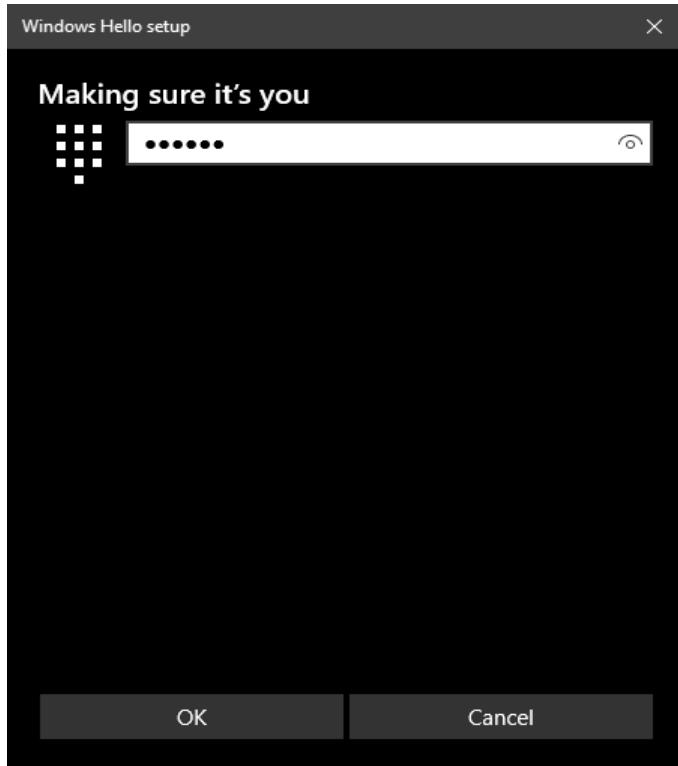
- **Touch** the fingerprint sensor on the security key.



- In **Security Key Fingerprint** section, select **Remove**.



- Enter the PIN (*created in the above step*) then select **OK**.



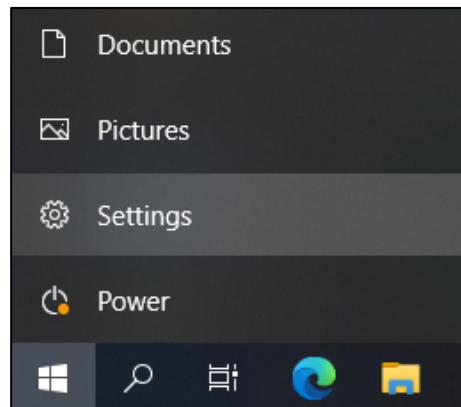
II.1.6. Resetting

In the case of forgetting the PIN of VinCSS FIDO2® Fingerprint, users can reset the key, but this will make the previously registered services unable to authenticate by using the key. After resetting, the device becomes a new security key, so services need to be re-registered to authenticate.

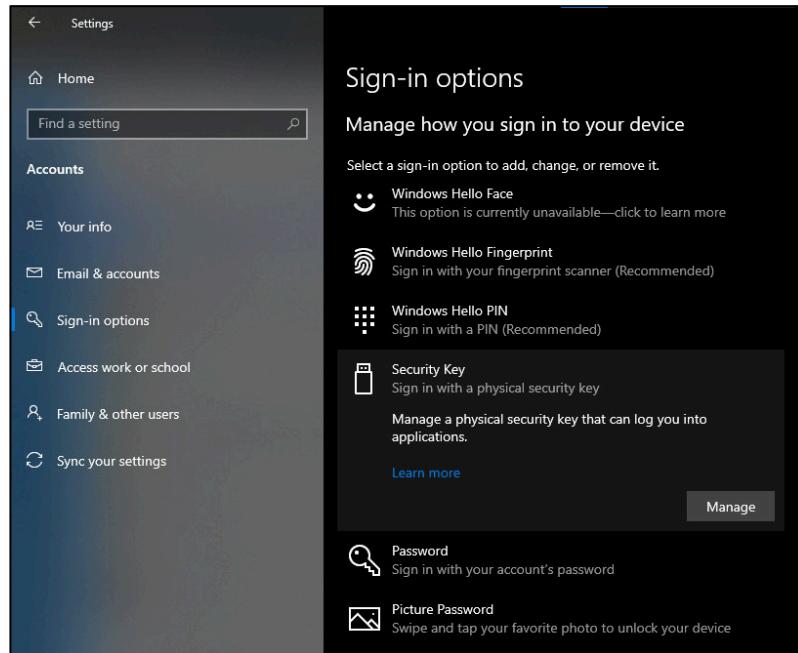
In case the PIN code is entered incorrectly many times (*more than 8 times*), the device will be locked permanently, user will also be forced to reset to use the VinCSS FIDO2® Fingerprint as a new device.

To reset VinCSS FIDO2® Fingerprint, follow the steps below:

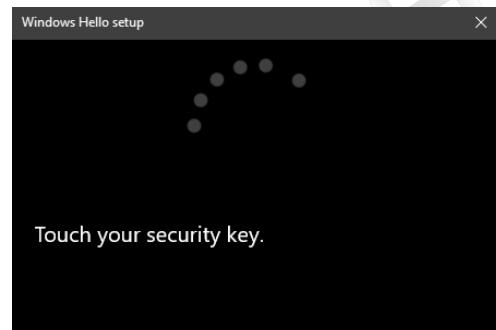
- Go to **Start > Settings**.



- Select Account > Sign-in options > Security Key, then select Manage.



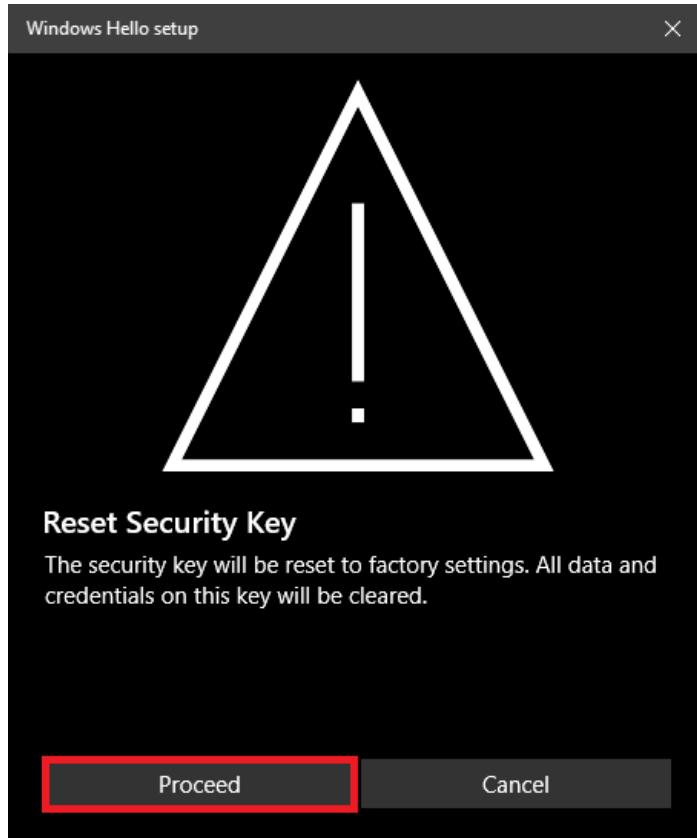
- Touch the fingerprint sensor on the security key.



- In Reset Security Key section, select Reset.



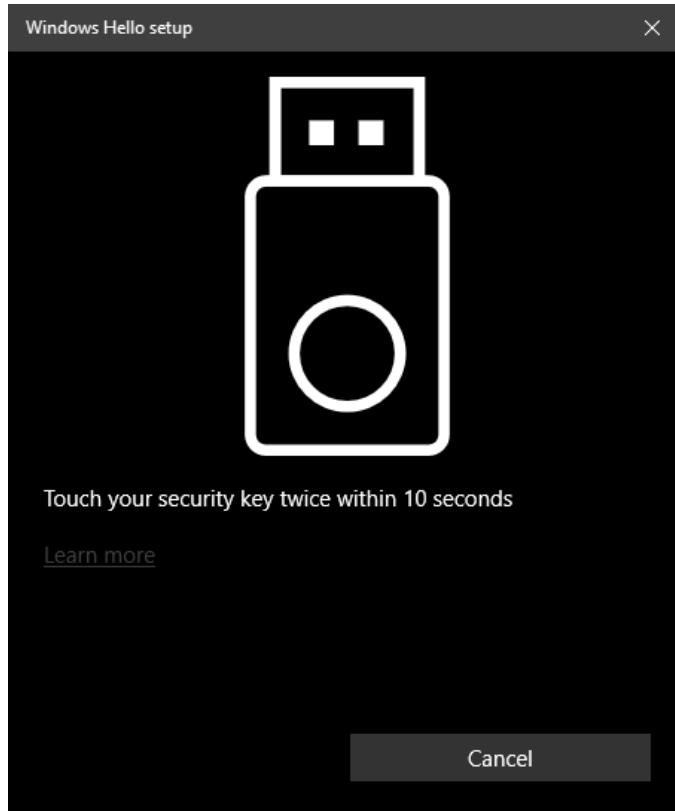
- Select **Proceed** to reset VinCSS FIDO2® Fingerprint.



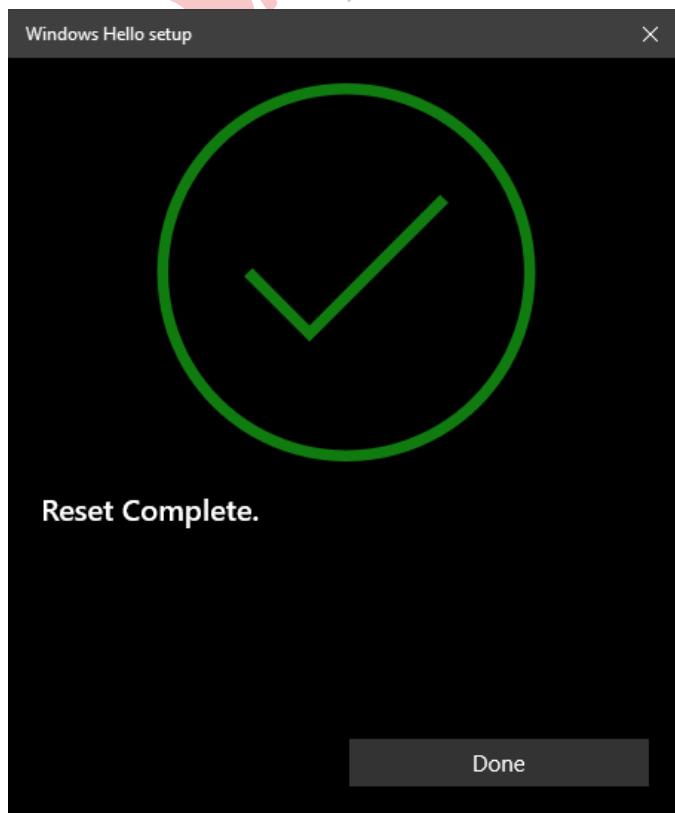
- Unplug the VinCSS FIDO2® Fingerprint, then plug it in again.



- When the white LED indicator appears on VinCSS FIDO2® Fingerprint, touch the fingerprint sensor on your security key twice within 10 seconds.



- After successfully resetting the security key, select **Done** to complete.

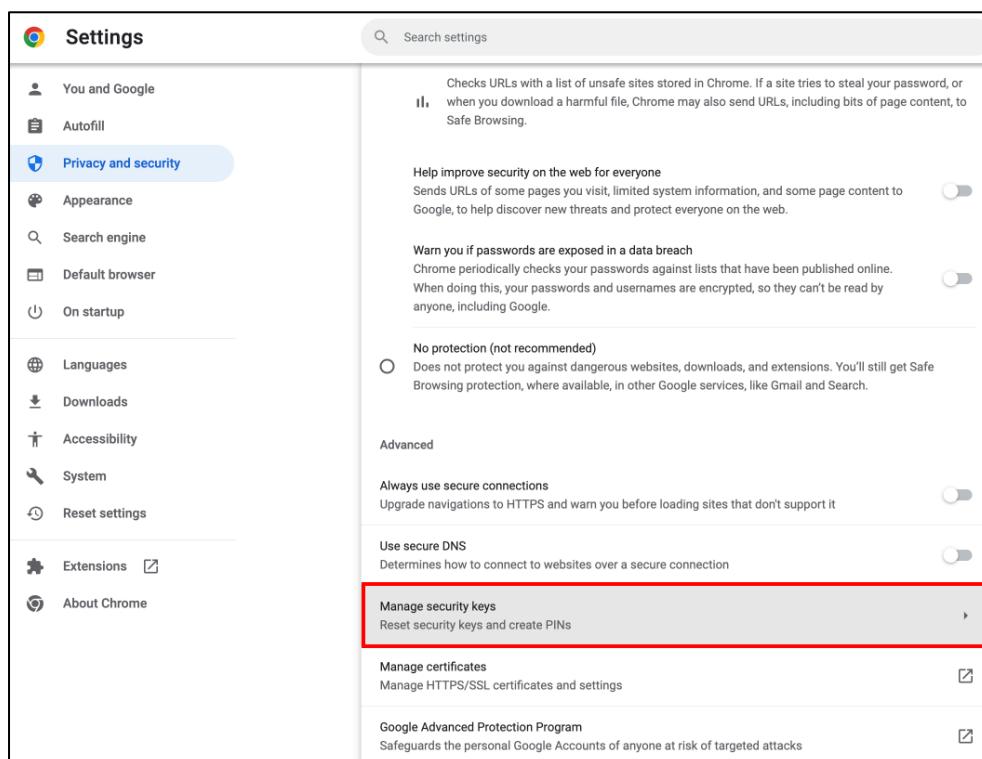


II.2. macOS

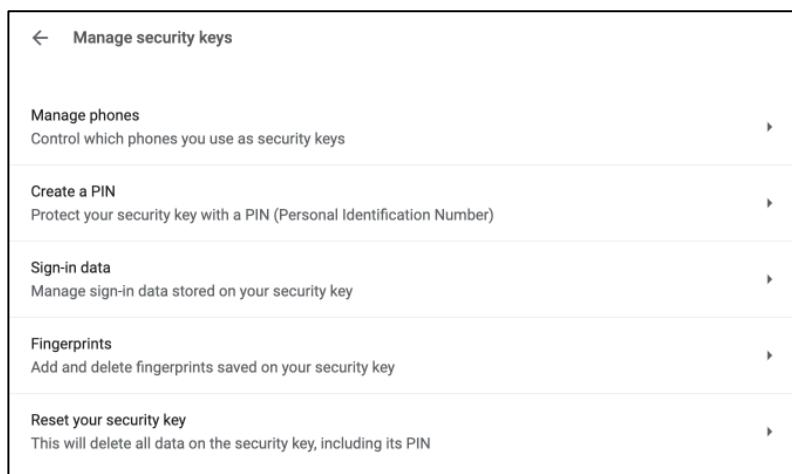
Plug the VinCSS FIDO2® Fingerprint into your computer using USB cable. If the LED blinks red 3 times in a row, it indicates low battery level (*below 20%*), while the amber LED indicates the security key is being charged and the green LED indicates the battery is fully charged. The VinCSS FIDO2® Fingerprint security key can be used while charging.

II.2.1. Creating a new PIN

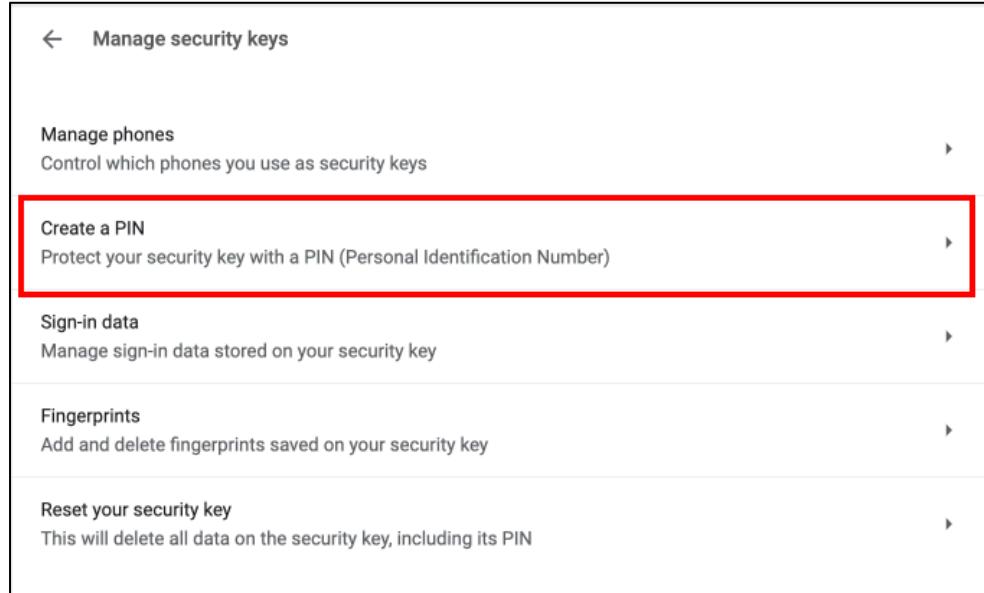
- Open Chrome browser, select **Settings > Privacy and security > Security > Manage security keys.**



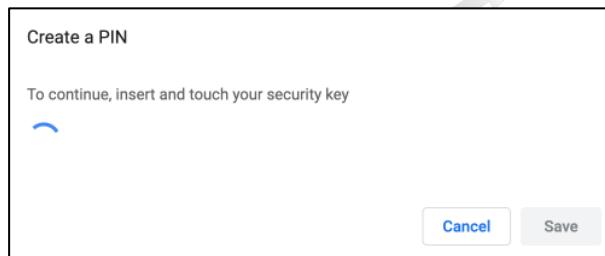
- **Manage security keys** interface is opened.



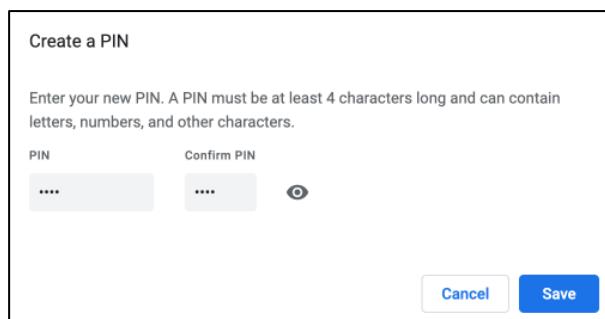
- By default, VinCSS FIDO2® Fingerprint does not have a PIN. To create a new PIN for the key, in the **Manage security keys**, select **Create a PIN**.



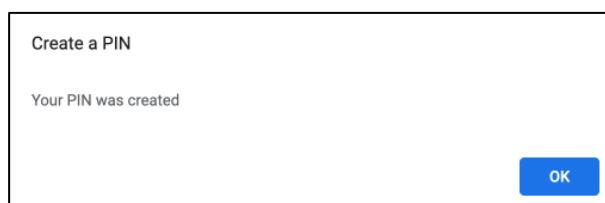
- Touch the fingerprint sensor on VinCSS FIDO2® Fingerprint to confirm.



- Next, enter PIN (*From 4 to 63 characters include letters (lowercase, uppercase), numbers and special characters*) and confirm PIN. Then click **Save** to create a PIN.

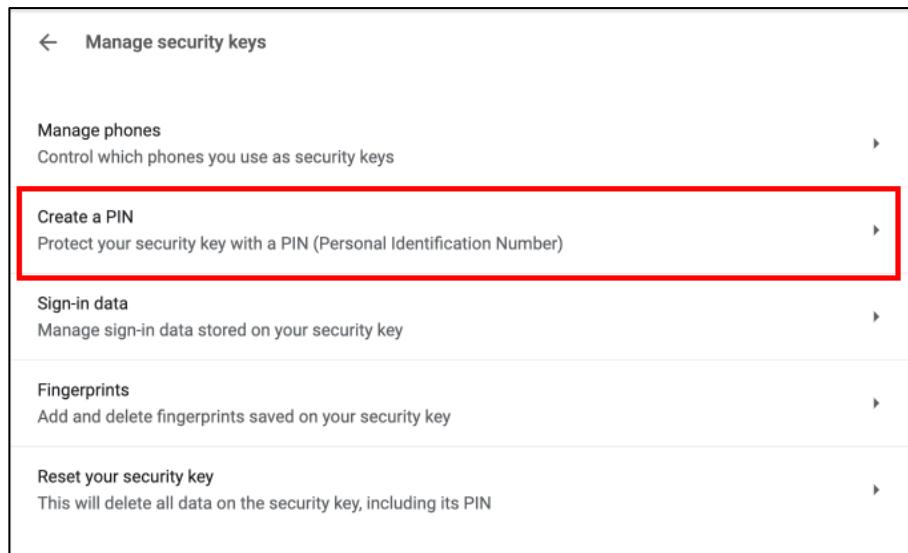


- Click **OK** to complete.

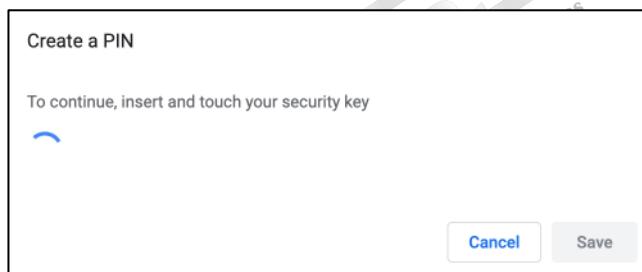


II.2.2. Changing PIN

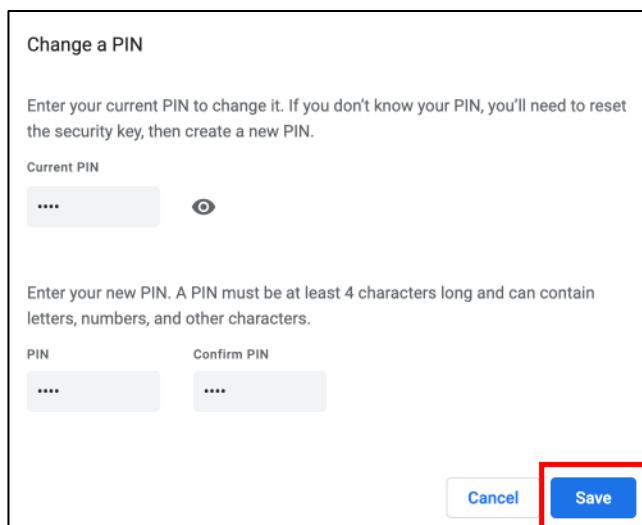
- To change PIN for VinCSS FIDO2® Fingerprint, in **Manage security keys** section (*Open Chrome browser, then select Setting > Privacy and security > Security > Manage security keys*), select **Create a PIN**.



- Touch the fingerprint sensor on the key to confirm.



- In **Change a PIN** section, enter current PIN. At the bottom, enter a new PIN and confirm PIN (*From 4 to 63 characters include letters (lowercase, uppercase), numbers and special characters*), then select **Save** to change.



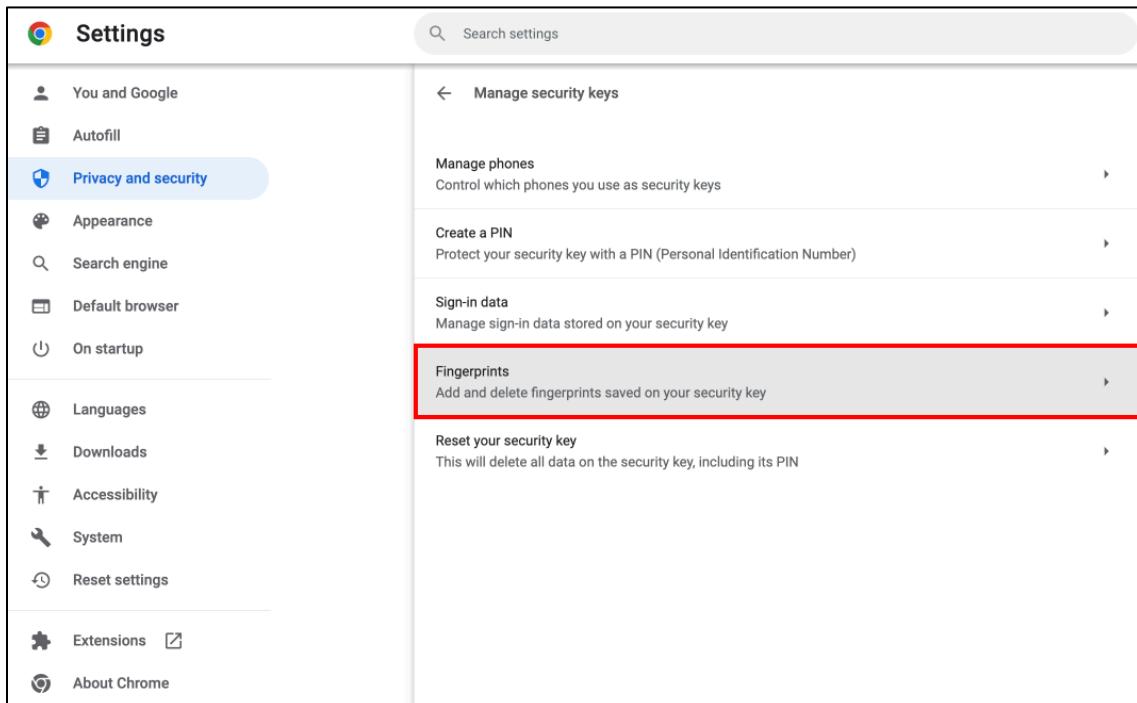
- Click **OK** to finish.



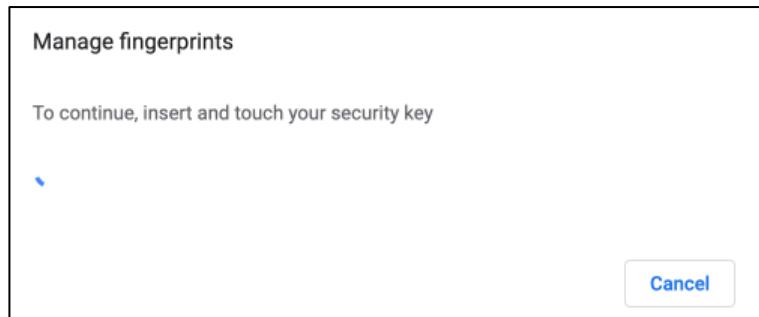
II.2.3. Adding fingerprints

After successfully creating a PIN for VinCSS FIDO2® Fingerprint, users can add additional fingerprints to the key (*up to 5 fingerprints*). Follow the steps below:

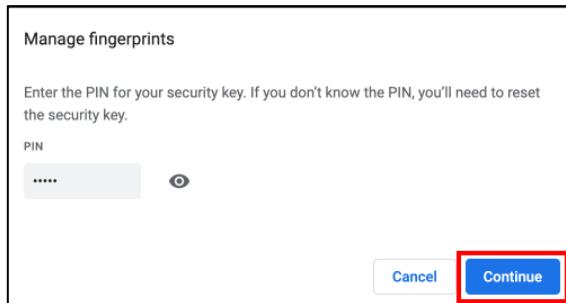
- In **Manage security keys** section (*Open Chrome browser, then select Setting > Privacy and security > Security > Manage security keys*), select **Fingerprints**.



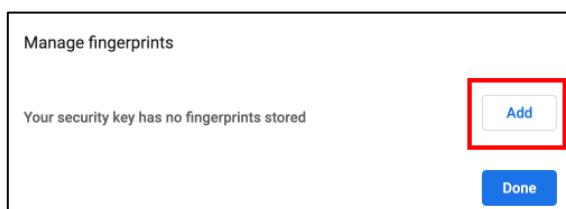
- Touch the fingerprint sensor on the security key.



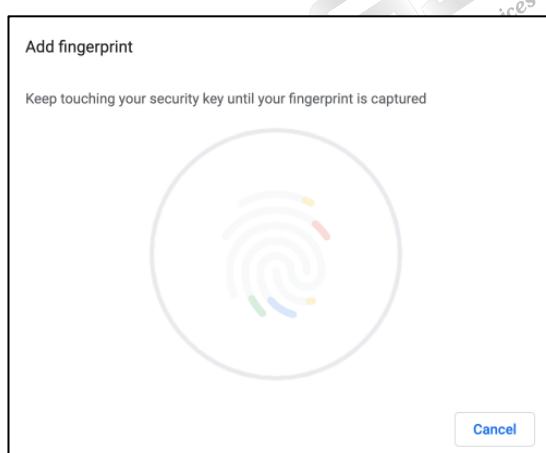
- Enter the PIN (*created in the above step*) then select **Continue**.



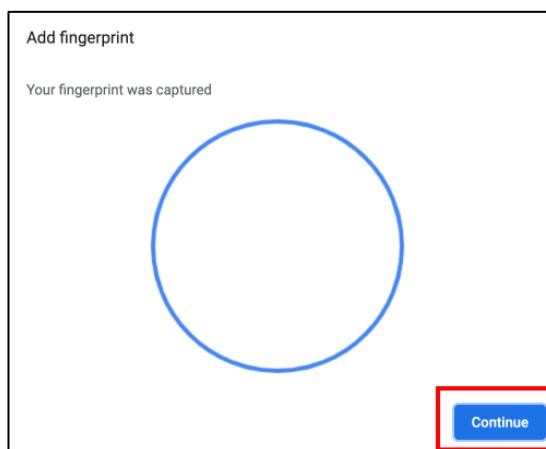
- Click **Add** to add a new fingerprint for the security key.



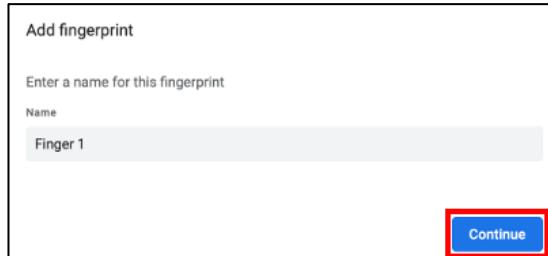
- When the device flashes a white light, scan the fingerprint by touching the fingerprint sensor with your finger until the light shows green, then lift your finger off the sensor (*5 times*).



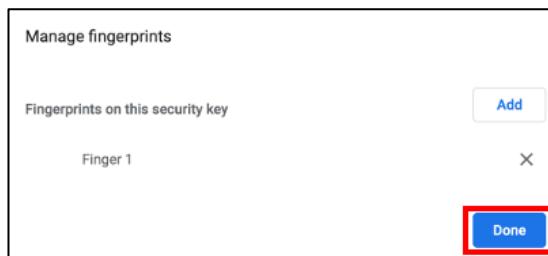
- After scanning fingerprint, click **Continue**.



- Name the fingerprint (*up to 30 unsigned characters*), then click **Continue**.

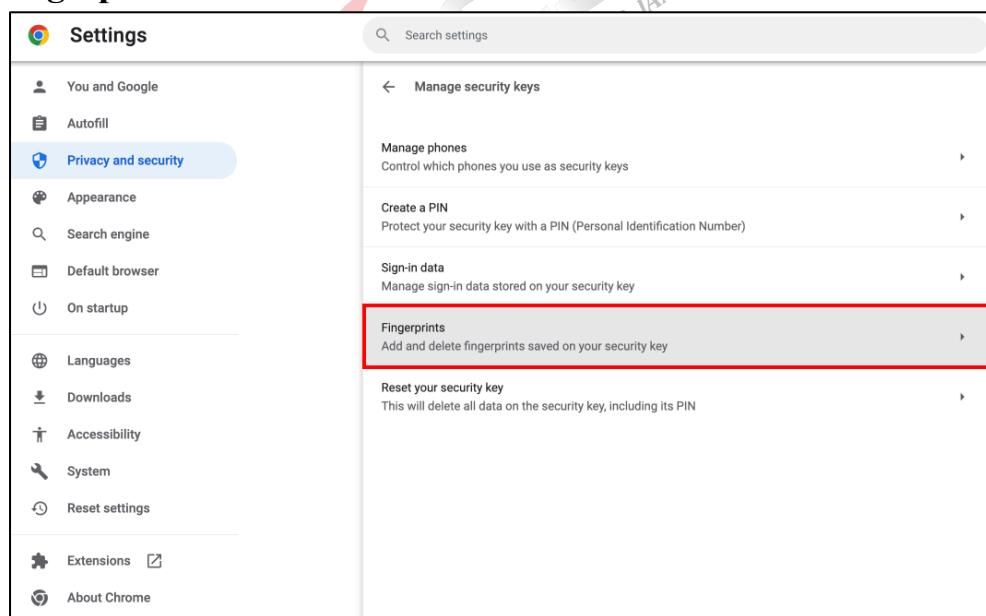


- Select **Add** to continue adding fingerprints, or select **Done** to finish.

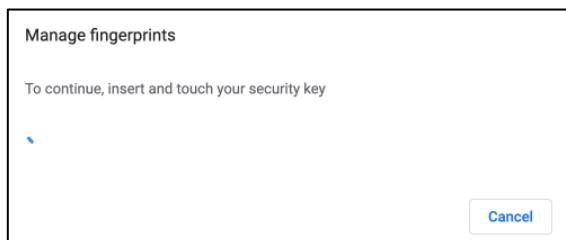


II.2.4. Removing fingerprints

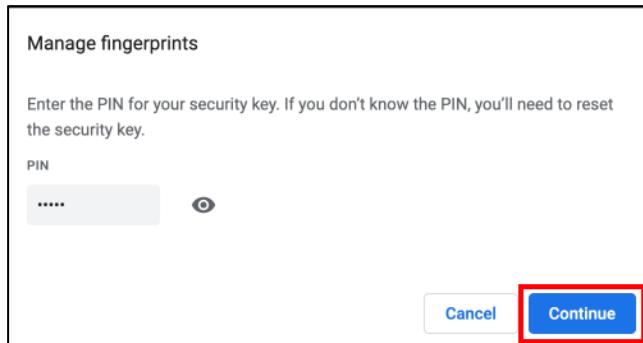
- In **Manage security keys** section (*Open Chrome browser, then select Setting > Privacy and security > Security > Manage security keys*), select **Fingerprints**.



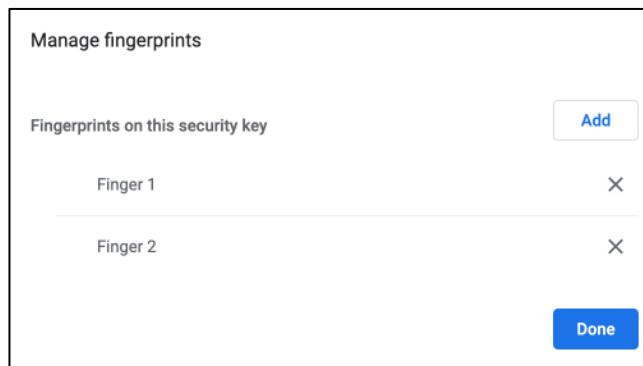
- Touch the fingerprint sensor on the security key.



- Enter the PIN (*created in the above step*) then select **Continue**.

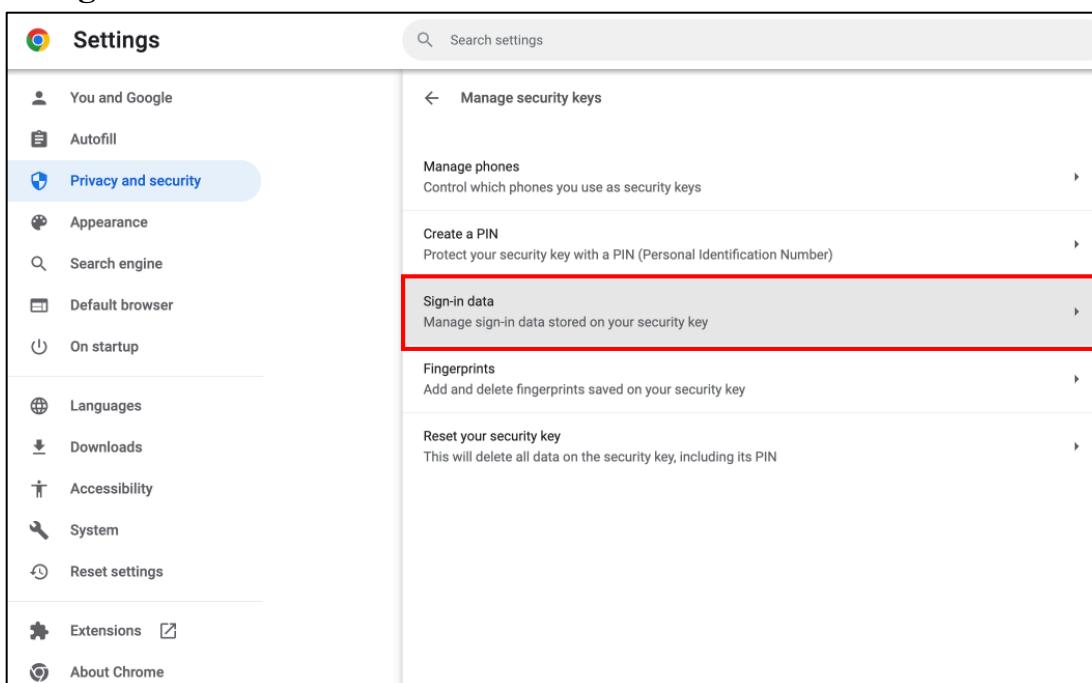


- A list of fingerprints that have been registered on the security key will be displayed. Click on the “X” icon at each corresponding fingerprint to delete.

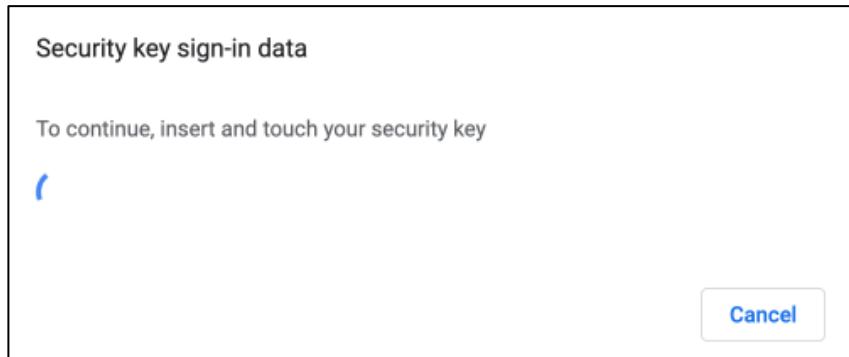


II.2.5. Managing sign-in data

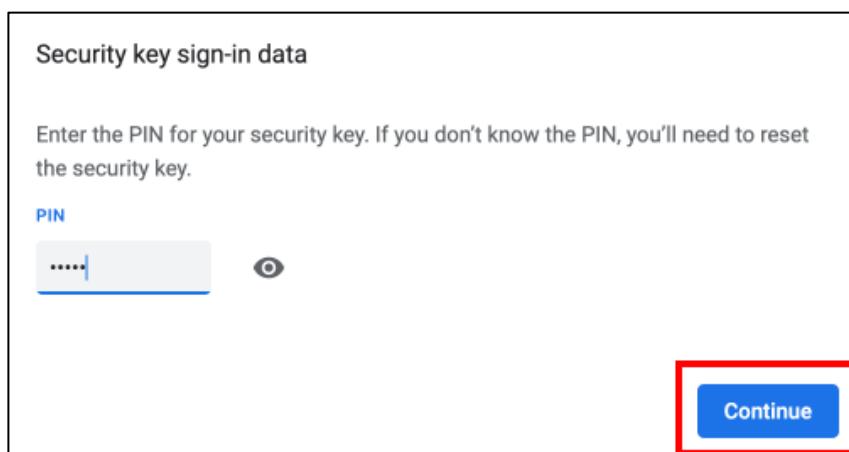
- In **Manage security keys** section (*Open Chrome browser, then select Setting > Privacy and security > Security > Manage security keys*), select **Sign-in data**.



- Touch the fingerprint sensor on the security key.



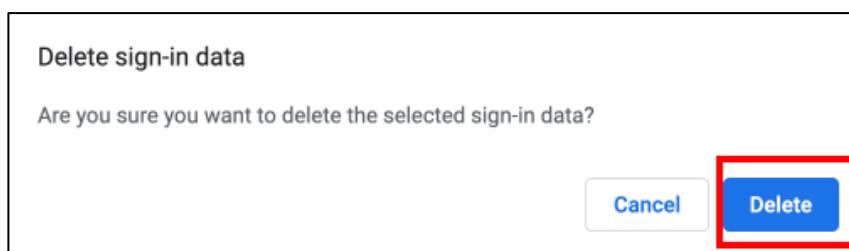
- Enter the PIN (*created in the above step*) then select **Continue**.



- Login data will be listed on the screen, including website and username.



- To delete the login data, click on the icon  at the end of each line. The **Delete sign-in data** dialog box appears. Select **Delete**.



- Complete the process of clearing login data. Return to the **Security key sign-in data** dialog box. Click **Done** to finish.

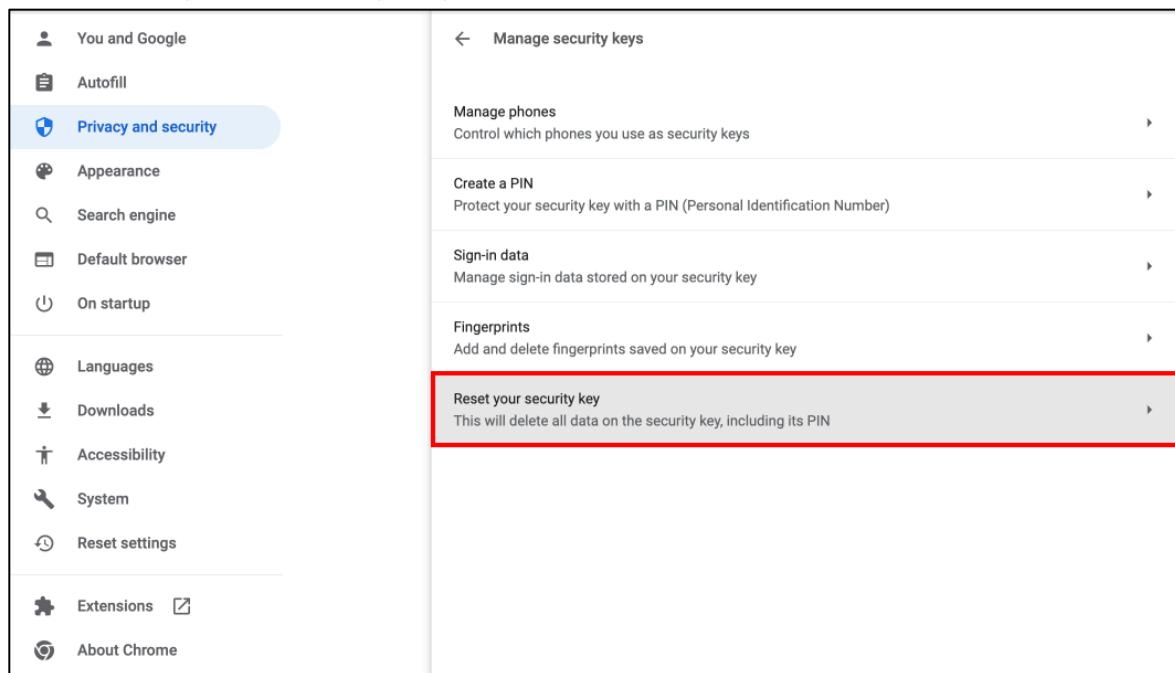


II.2.6. Resetting

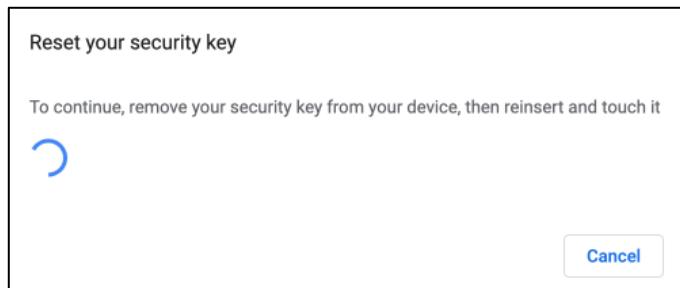
In the case of forgetting the PIN of VinCSS FIDO2® Fingerprint, users can reset the key, but this will make the previously registered services unable to authenticate by using the key. After resetting, the device becomes a new security key, so services need to be re-registered to authenticate. In case the PIN code is entered incorrectly many times (*more than 8 times*), the device will be locked permanently, user will also be forced to reset to use the VinCSS FIDO2® Fingerprint as a new device.

To reset VinCSS FIDO2® Fingerprint, follow the steps below:

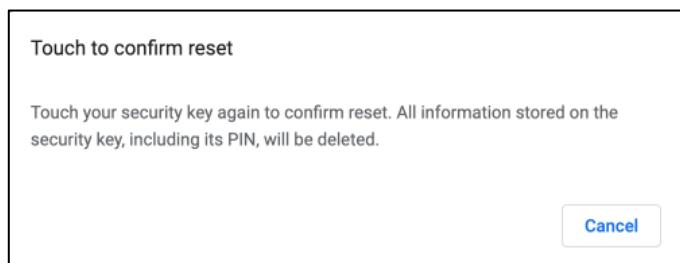
- In **Manage security keys** section (*Open Chrome browser, then select Setting > Privacy and security > Security > Manage security keys*), select **Reset your security key**.



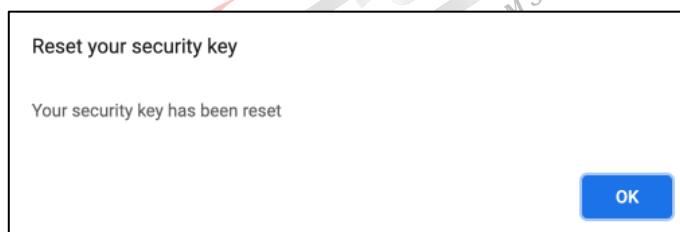
- Unplug VinCSS FIDO2® Fingerprint from the computer and re-plug it. Touch the fingerprint sensor on VinCSS FIDO2® Fingerprint to confirm.



- Touch the fingerprint sensor on VinCSS FIDO2® Fingerprint again to confirm the reset process of VinCSS FIDO2® Fingerprint.



- After successfully resetting the security key, click **OK** to finish.



II.3. Linux

II.3.1. USB

To check the udev version of the device, the user runs the following command in Terminal: **“sudo udevadm –version”**.

From udev version 244 and above, VinCSS FIDO2® Fingerprint authentication is quite supported. If the udev version is lower than 244, to set up the Linux system:

- Verify that **libu2f-udev** is installed on your system.
 - o On Debian and its derivatives (*Ubuntu, Linux Mint, etc.*), check whether libu2f-udev is installed by running the following command in Terminal: “**dpkg -s libu2f-udev**”.
 - o Install by running the following command in Terminal (*If already installed, please skip this step*): **“sudo apt install libu2f-udev”**.

- Copy **99-vincss.rules** into the Linux directory: **/etc/udev/rules.d/**. If this file is already there, ensure that the content looks like the one provided.



- Save your file, and then reboot the system.

Note:

- *If user have set up “udev rules” but the VinCSS FIDO2® Fingerprint security key’s still not working, please contact us for support. The cause might be a conflict of some packages installed on the Linux.*
- *Other operations to manage security keys are performed on Chrome browser (similar to macOS platform - Refer to section [II.2. macOS](#)).*

II.3.2. Bluetooth

Users need to install Blueman Bluetooth Manager software on Ubuntu to be able to pair the VinCSS FIDO2® Fingerprint security key with the device. Users should not pair the security keys with Linux in **Settings/Bluetooth** because the two devices will connect without a PIN code. That makes the security key doesn't work with Bluetooth on Linux.

Pre-requisites to install Blueman on Ubuntu:

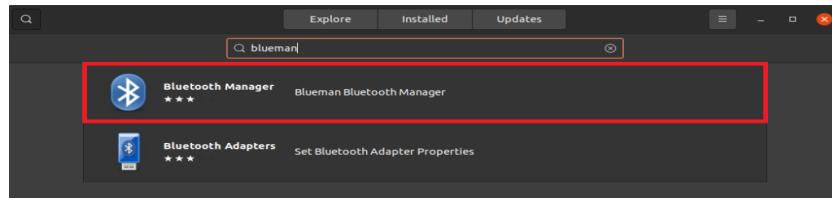
- Ubuntu installed and Running.
- Active Internet Connection to download Blueman.
- Sudo Privileges.
- Inbuilt or External Bluetooth Adapter.

If Bluetooth is not already set up on the system, then first install BlueZ. User can check whether libu2f-udev is installed by running the following command in Terminal: “**dpkg -s bluez**”.

Install: ”**sudo apt install bluez bluez-tools**”

II.3.2.1. Install Blueman on Ubuntu

- via terminal: **sudo apt install blueman**
- via Ubuntu Software center:
 - o Start the Ubuntu Software center.
 - o Search for Blueman. Click on the “Blueman Bluetooth Manager” result.



- Click on Install and provide authentication to install Blueman.

II.3.2.2. Connect to VinCSS FIDO2® Fingerprint

- Turn on Bluetooth Manager.
- Set up a new device via Bluetooth Manager, the PIN Request will appear and users can use the VinCSS FIDO2® Fingerprint on Linux via Bluetooth. (Refer to section [II.2.1. Creating a new PIN](#)).

III. PASSWORDLESS AUTHENTICATION USING VINCSS FIDO2® FINGERPRINT

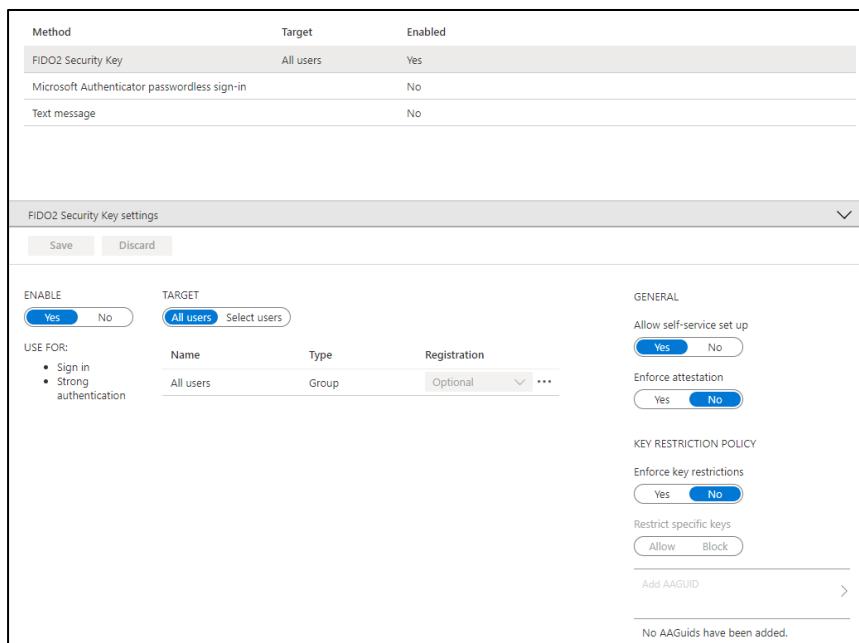
III.1. Windows

Note: Users need an Azure AD account.

III.1.1. Configuration on Azure AD system

III.1.1.1. Configuration on Azure AD

- Go to the link: https://portal.azure.com/#blade/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/AdminAuthMethods
- Select **Method FIDO2 Security Key**, then select the following configurations:



Method	Target	Enabled
FIDO2 Security Key	All users	Yes
Microsoft Authenticator passwordless sign-in		No
Text message		No

FIDO2 Security Key settings

GENERAL

Allow self-service set up: Yes

Enforce attestation: No

KEY RESTRICTION POLICY

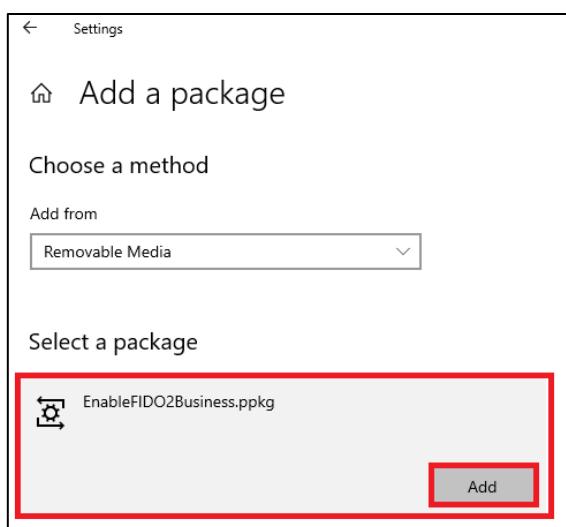
Enforce key restrictions: Yes

Restrict specific keys: Allow

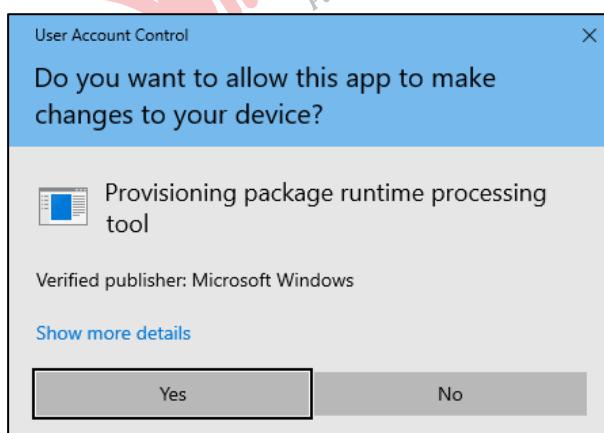
- Click **Save** to save the configurations.

III.1.1.2. Login Windows 10 using FIDO2 with provisioning packages

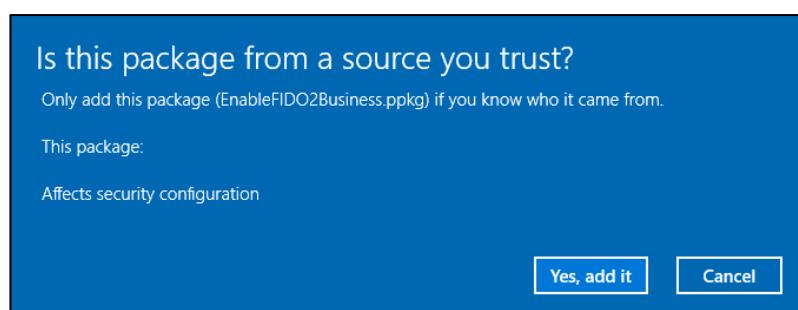
- Transfer 2 files **EnableFIDO2Business.cat** and **EnableFIDO2Business.ppkg** provided by VinCSS to storage device.
- Connect that storage device to the computer needed to enable FIDO, then go to **Settings > Accounts > Access work or school > Add or remove a provisioning package > Add a package**, select package, then click **Add**.



- Select **Yes**.

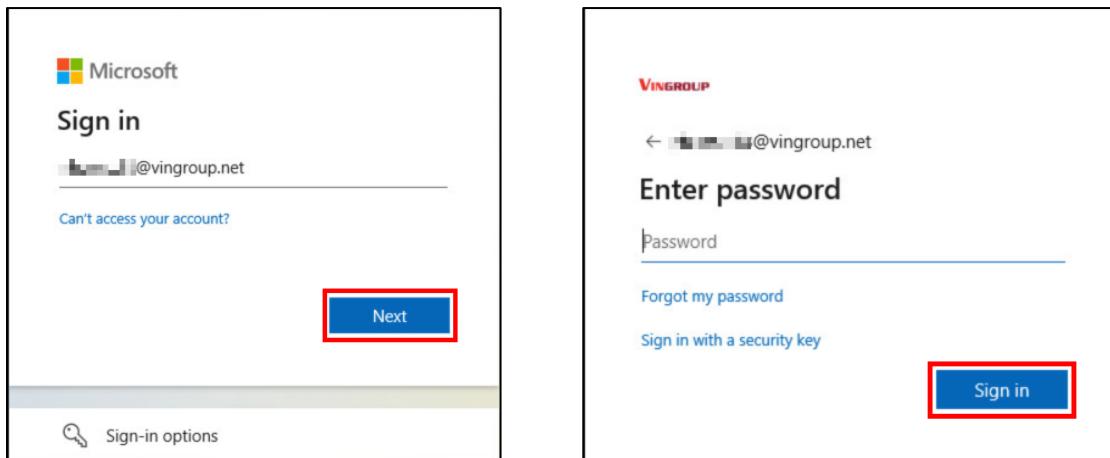


- Select **Yes, add it**.

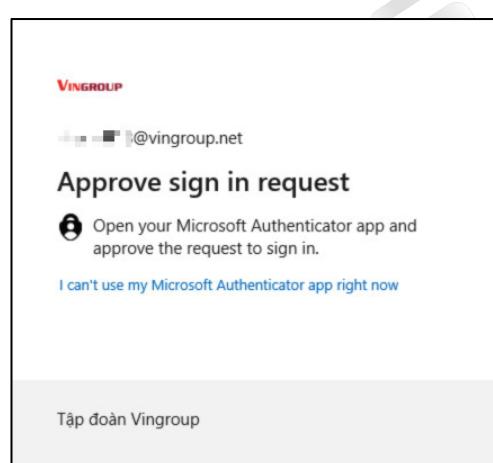


III.1.1.3. Register authentication key for Azure AD

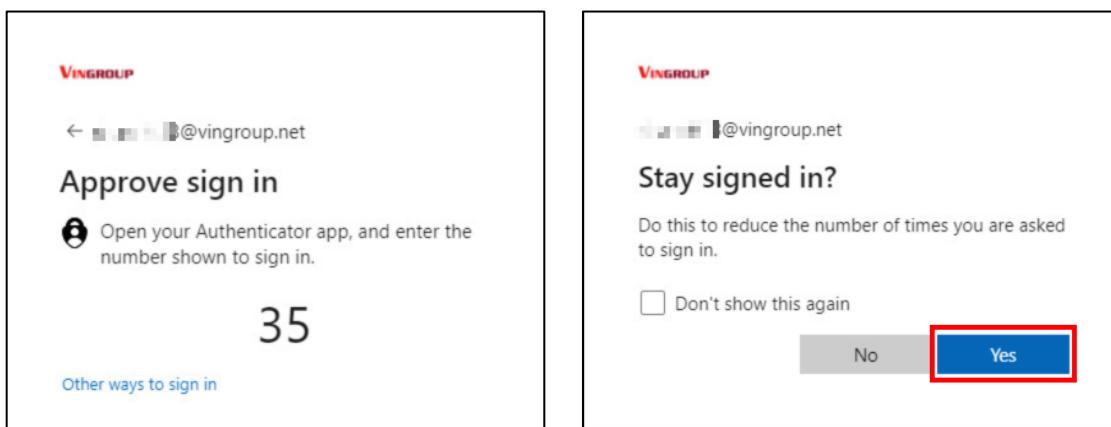
- Go to <https://myaccount.microsoft.com/>, enter AD account information, then click **Next**. Enter the password of the AD account and then select **Sign in**.



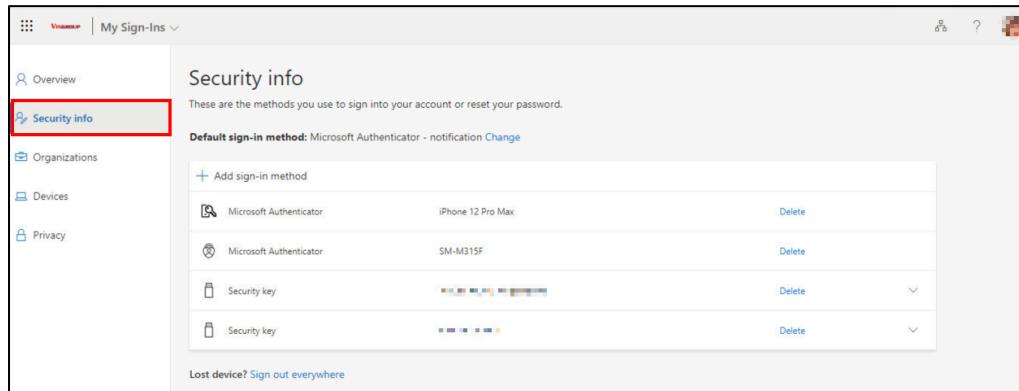
- Authenticate with the Microsoft Authenticator app on your phone.



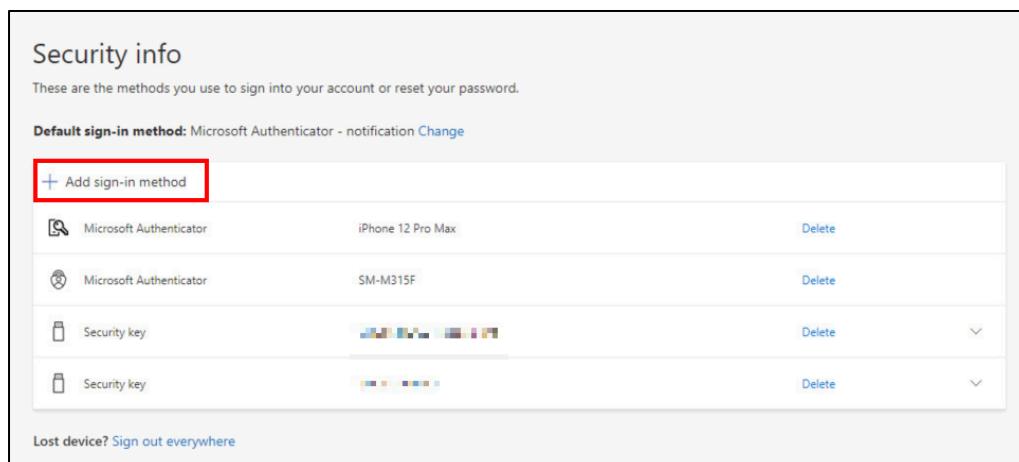
- On the Authenticator app, enter the phone number shown on the computer screen. Click **Yes** to continue logging in.



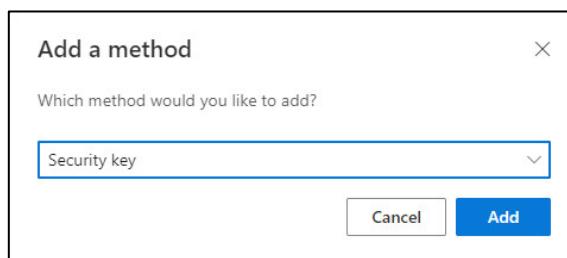
- After successful login, select **My sign-ins > Security info.**



- Select **Add sign-in method.**



- The **Add a method** dialog box appears, select **Security key** and then click **Add**.

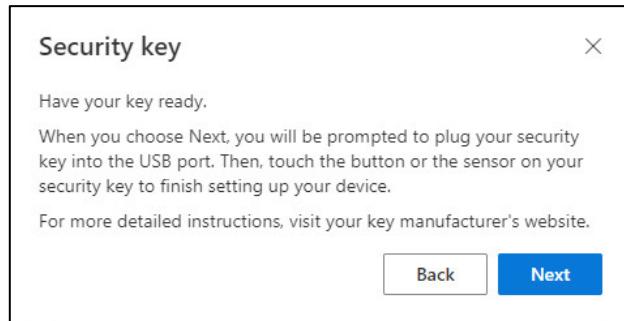


III.3.2.2.1. Using via Bluetooth

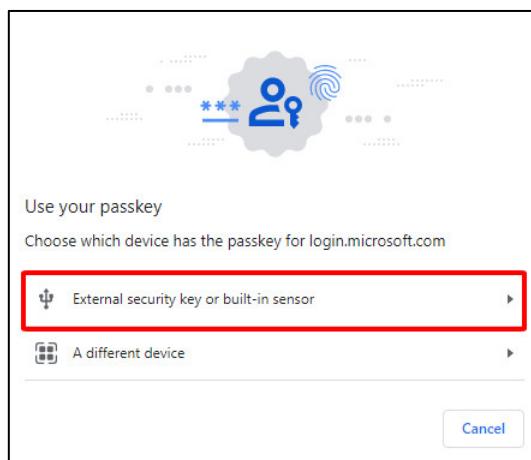
- Select **USB device.**



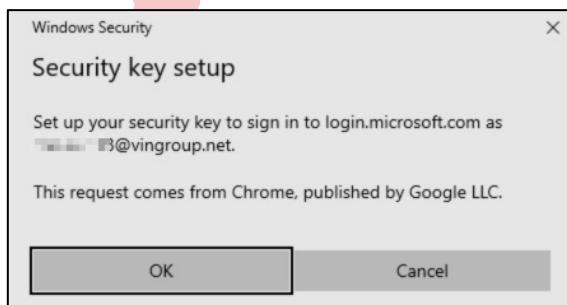
- Select **OK** to continue.



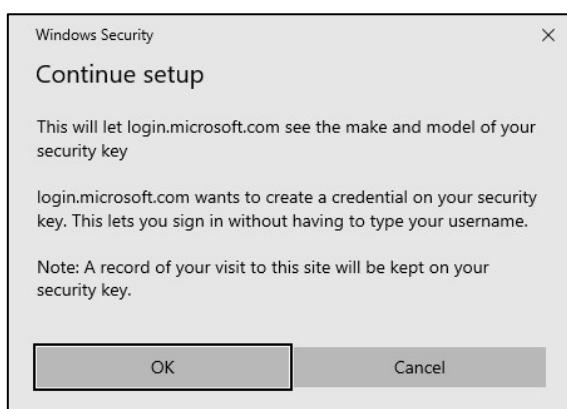
- Select **External security key or built-in sensor** to set up security key.



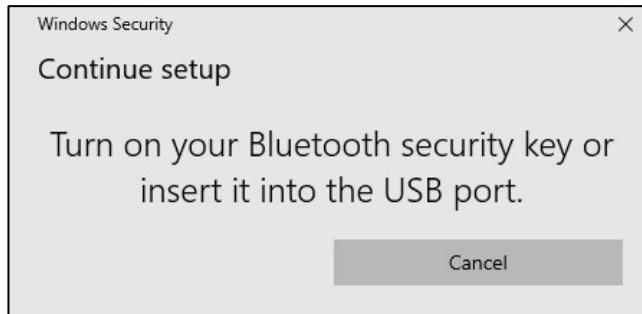
- Select **OK** to continue to set up the security key.



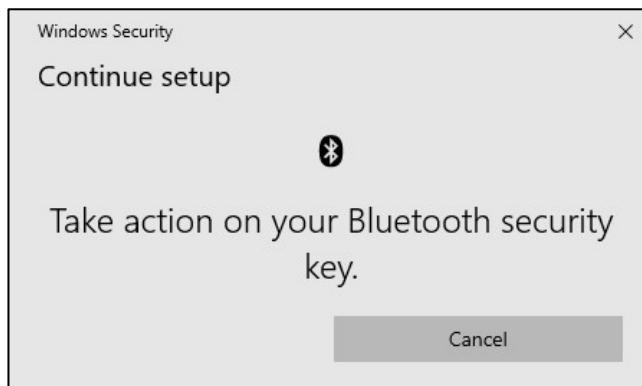
- Select **OK** to continue.



- Connect the VinCSS FIDO2® Fingerprint to your computer via Bluetooth.

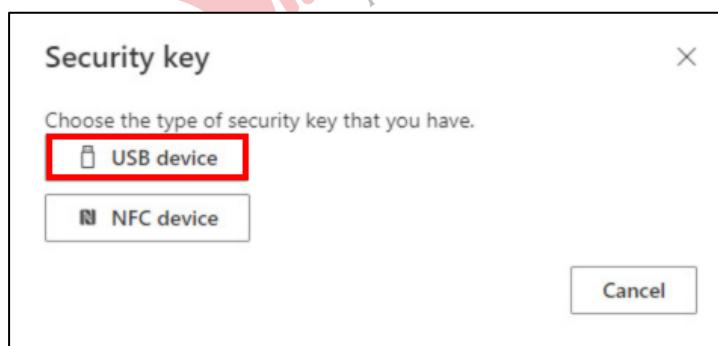


- Scan your fingerprint when receiving notification.

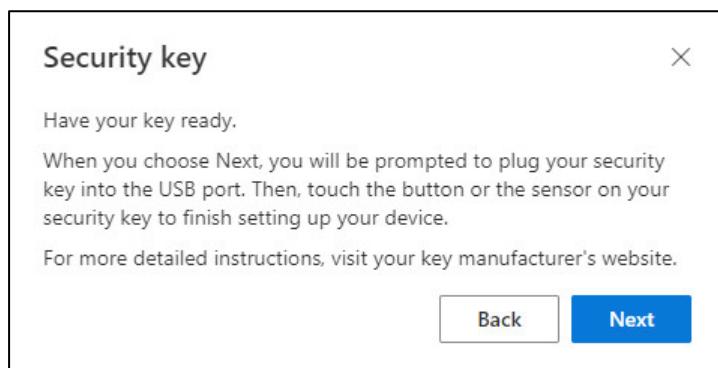


III.3.2.2.2. Using via USB

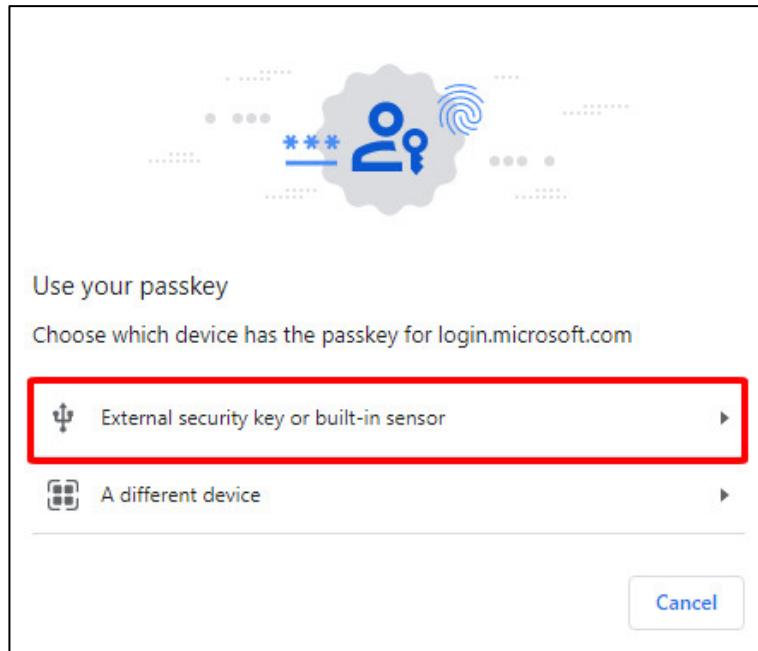
- Select **USB device**, click **Next**.



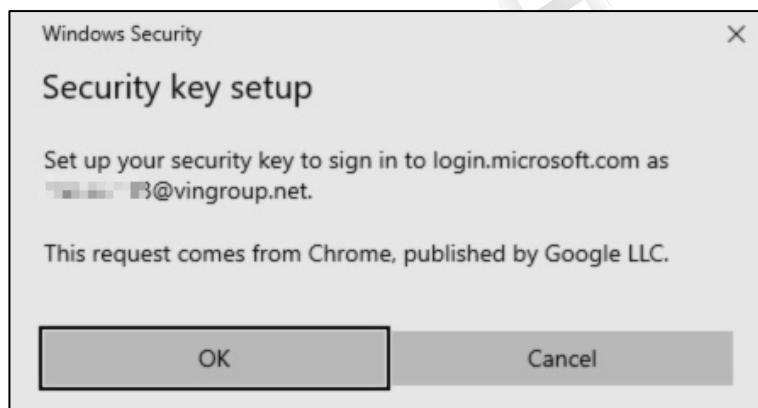
- Select **OK** to continue.



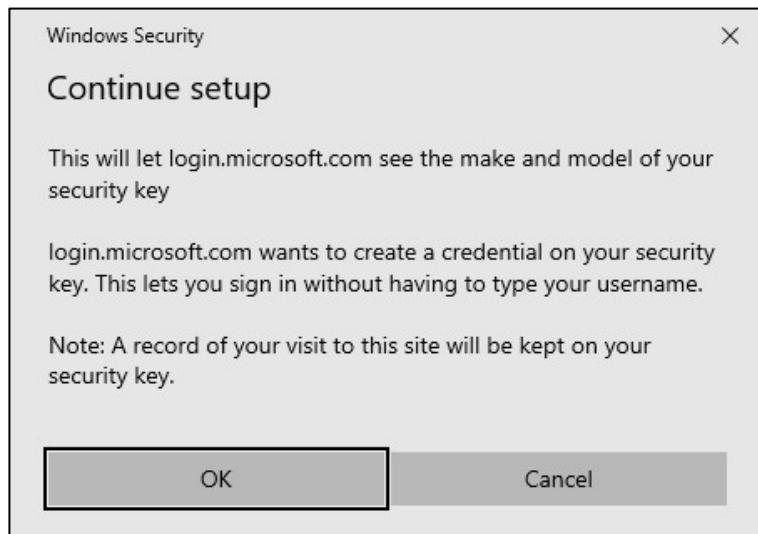
- Select **External security key or built-in sensor** to set up security key.



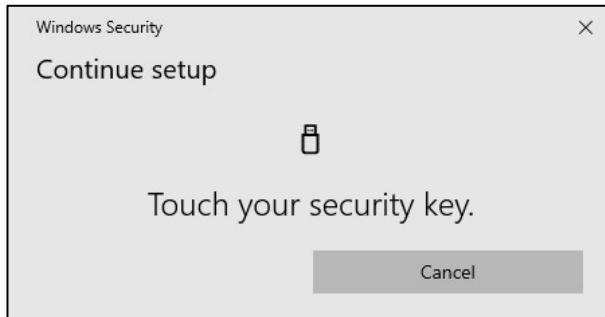
- Select **OK** to continue to set up the security key.



- Select **OK** to continue.



- Connect the VinCSS FIDO2® Fingerprint to the computer via USB, scan your fingerprint on the sensor when receiving the notification.

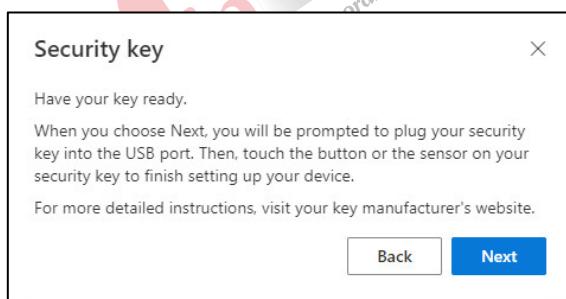


III.3.2.2.3. Using via NFC

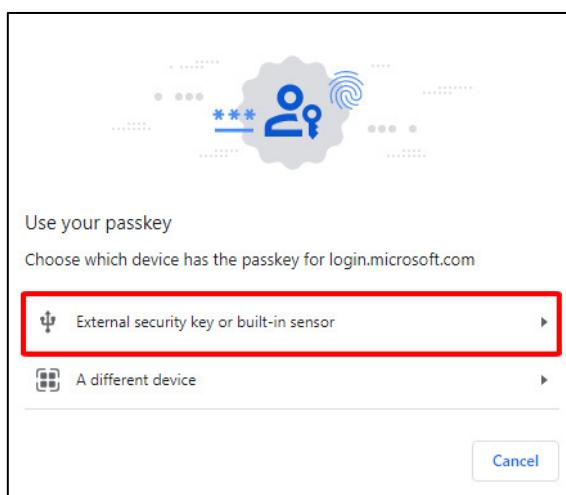
- Select **NFC device**. Click **Next**.



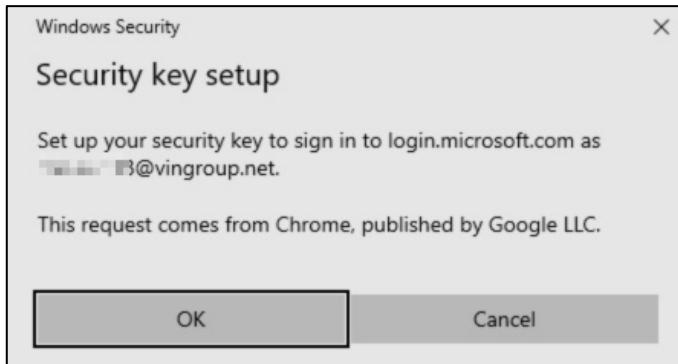
- Select **OK** to continue.



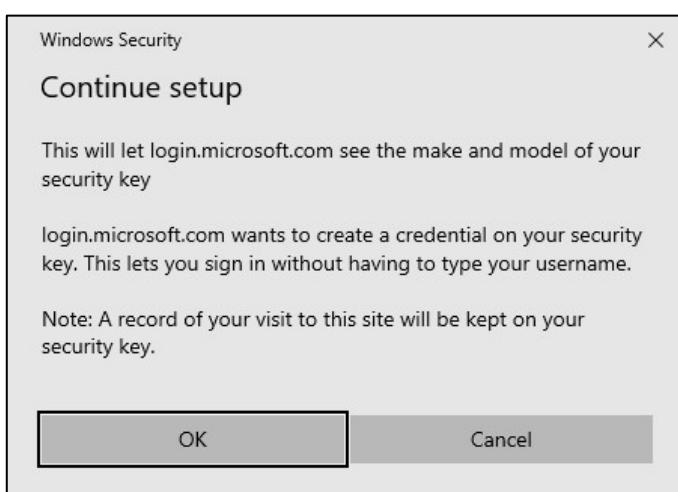
- Select **External security key or built-in sensor** to set up security key.



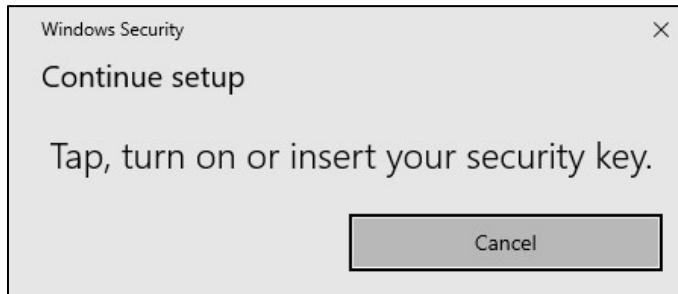
- Select **OK** to continue to set up the security key.



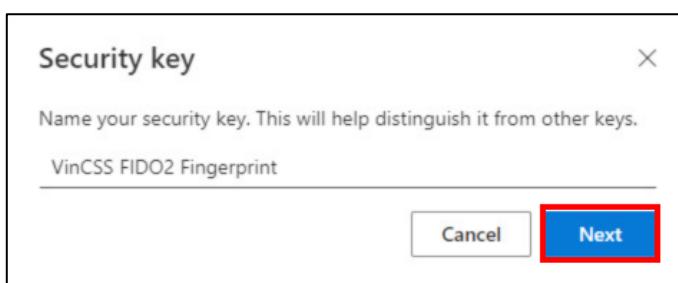
- Select **OK** to continue.



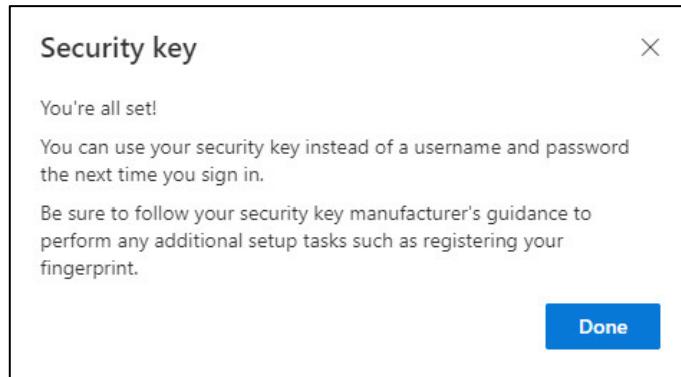
- Connect the key to the NFC reader when receiving the notification, then scan your fingerprint on the sensor.



- Name the security key (*up to 30 characters*) to distinguish the key and then click **Next**.

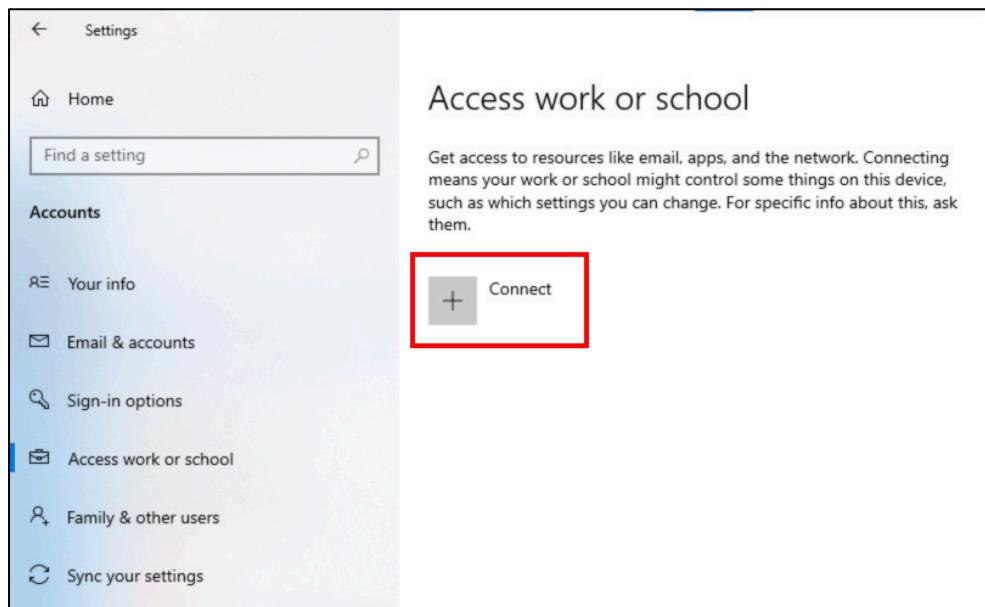


- Click **Done** to complete the Security key registration.

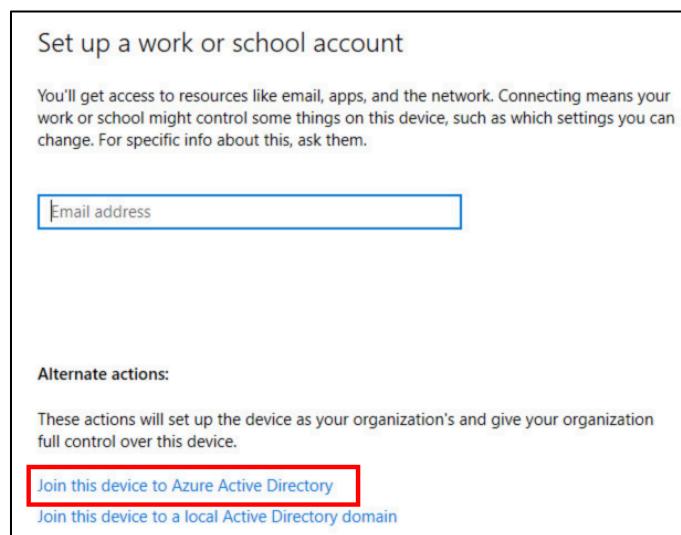


III.1.1.4. Connect User to Azure Work Account

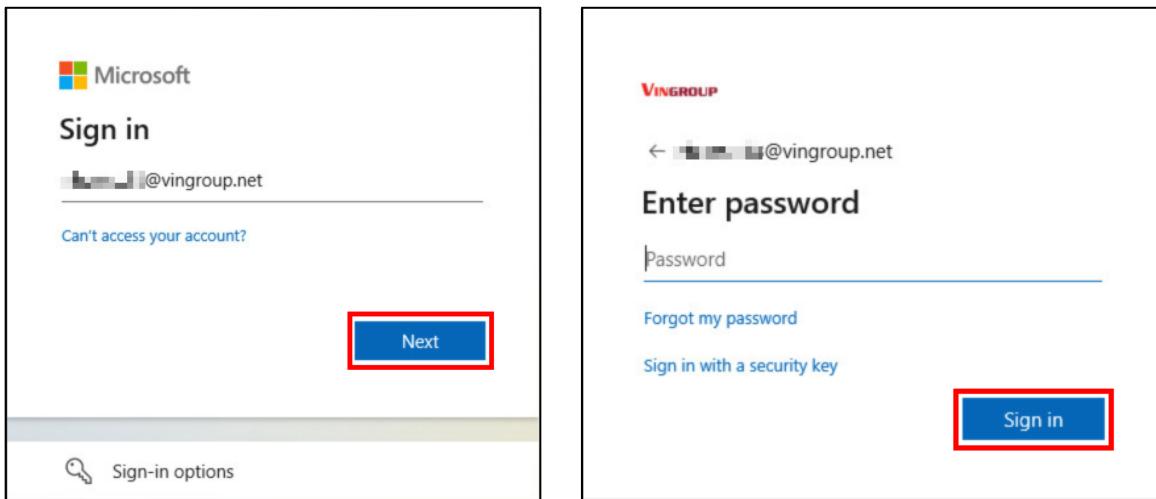
- On Windows, select **Settings > Account > Access work or school > Connect**.



- Select **Join this device to Azure Active Directory**.



- Enter the AD account infomation, then click **Next**. Enter the password of the AD account and then select **Sign in**.



Microsoft Sign in

← [REDACTED]@vingroup.net

Can't access your account?

Next

Sign-in options

VINGROUP

← [REDACTED]@vingroup.net

Enter password

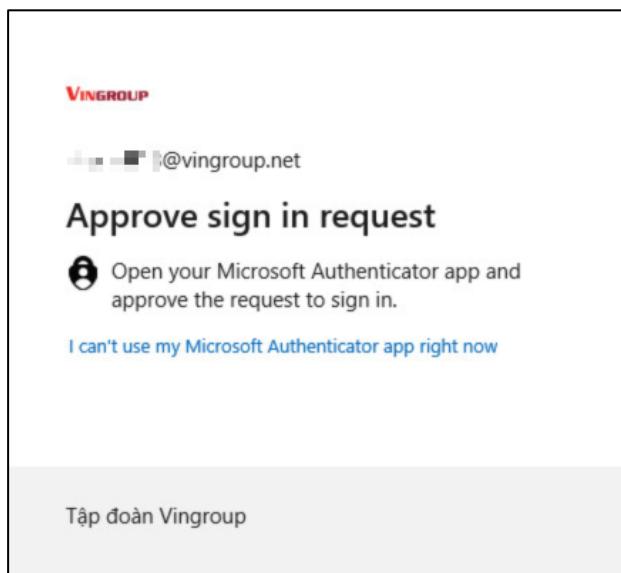
>Password

Forgot my password

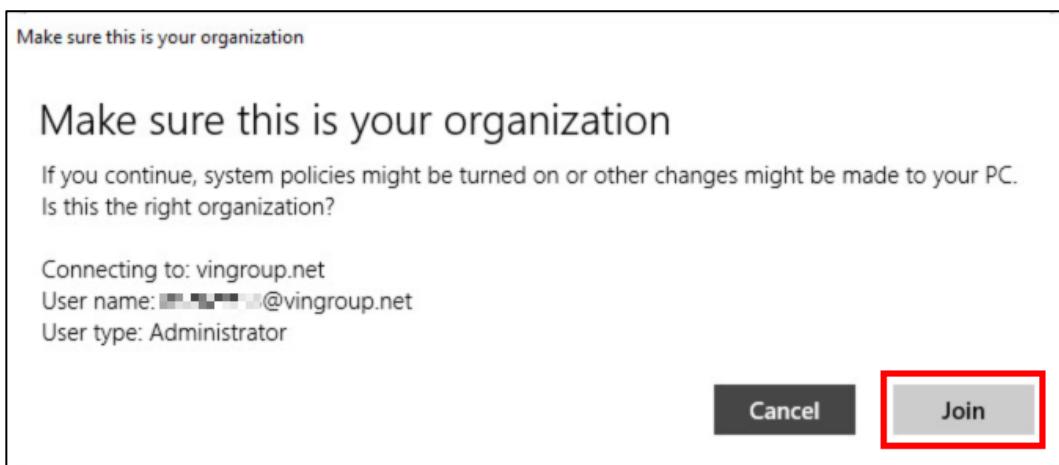
Sign in with a security key

Sign in

- Authenticate with the Microsoft Authenticator app on your phone.



- Check information, then click **Join**.



Make sure this is your organization

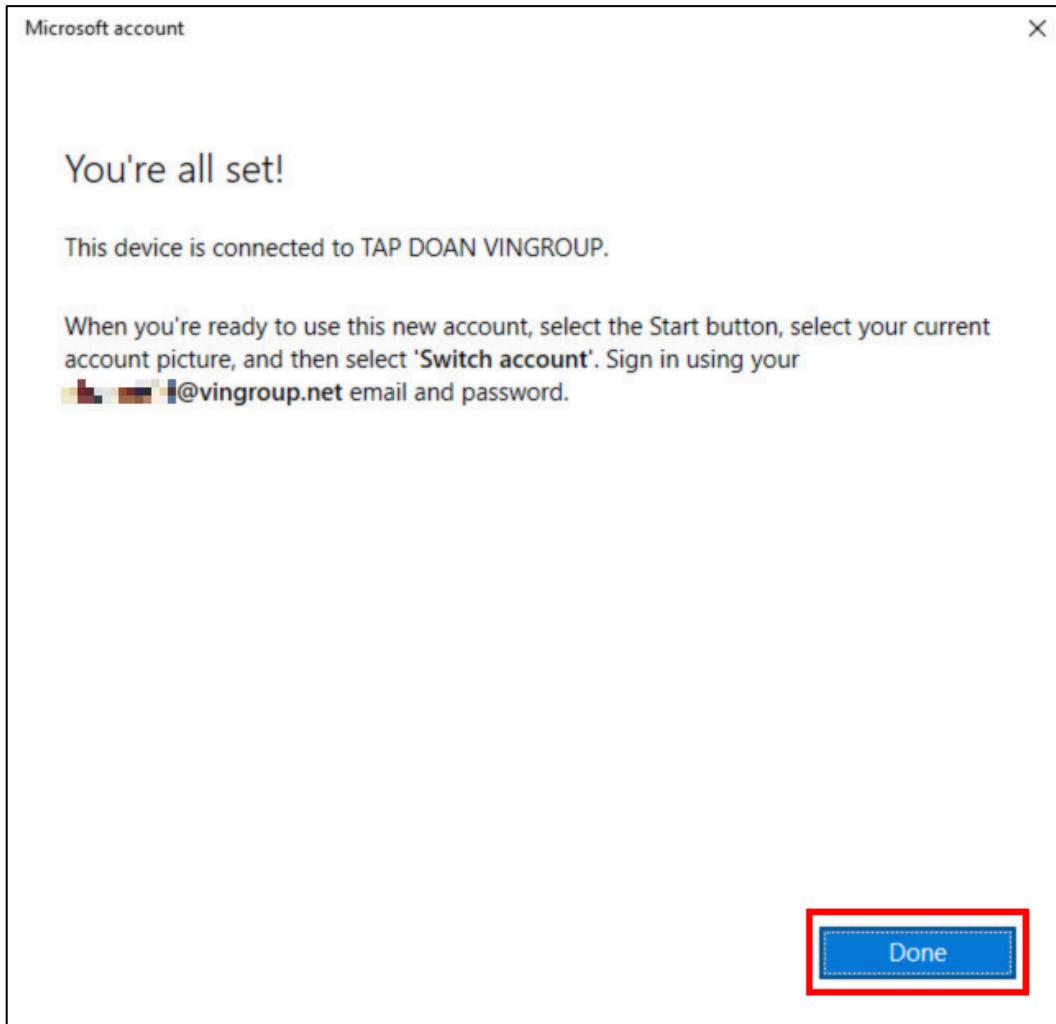
Make sure this is your organization

If you continue, system policies might be turned on or other changes might be made to your PC.
Is this the right organization?

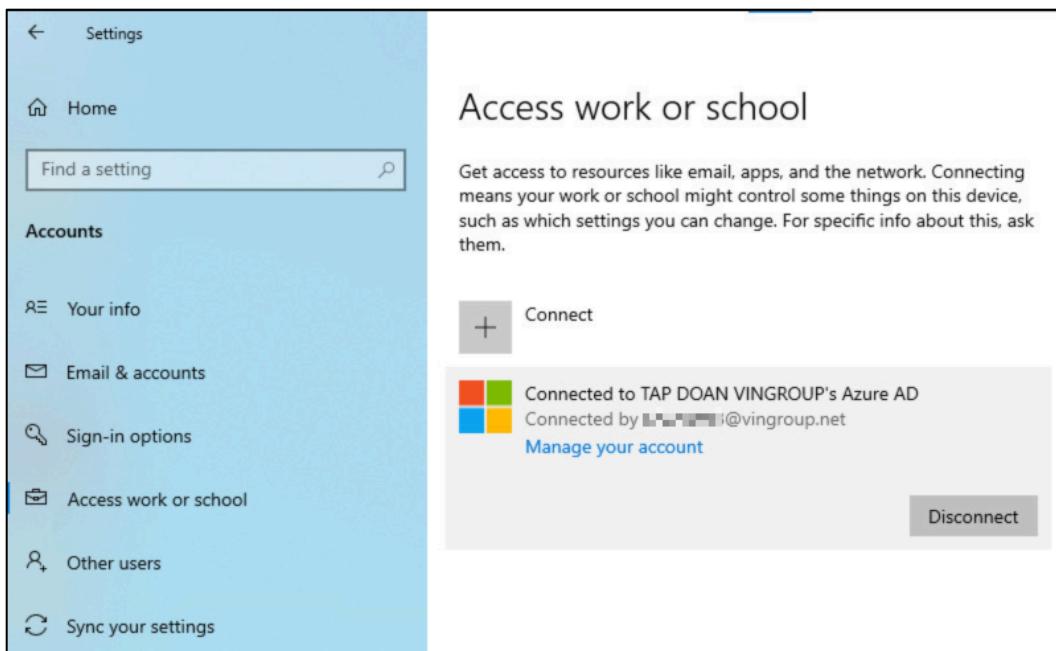
Connecting to: vingroup.net
User name: [REDACTED]@vingroup.net
User type: Administrator

Cancel **Join**

- Click Done to finish.

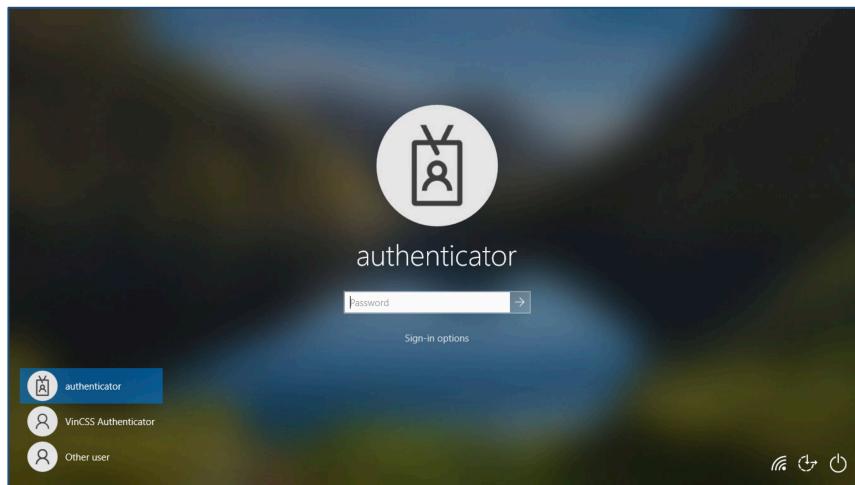


- The connection is successful, the screen shows as below.

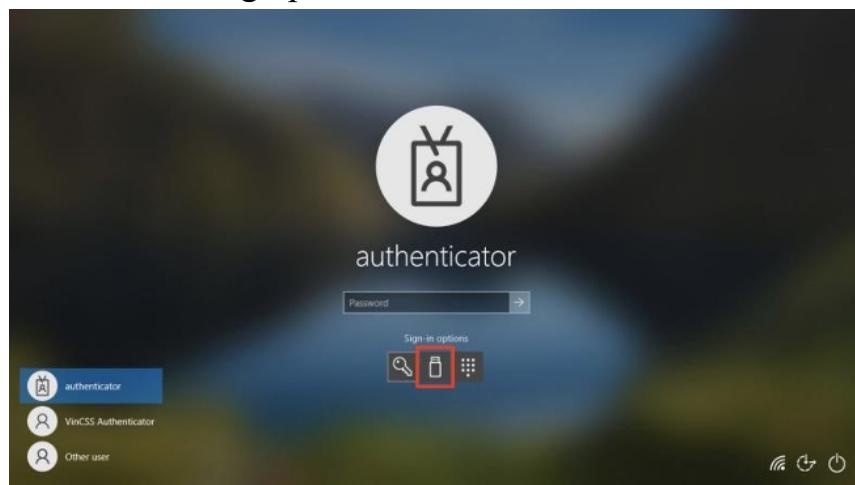


III.1.2. Login Windows

- On Windows 10 sign-in interface, select **Sign-in options**.

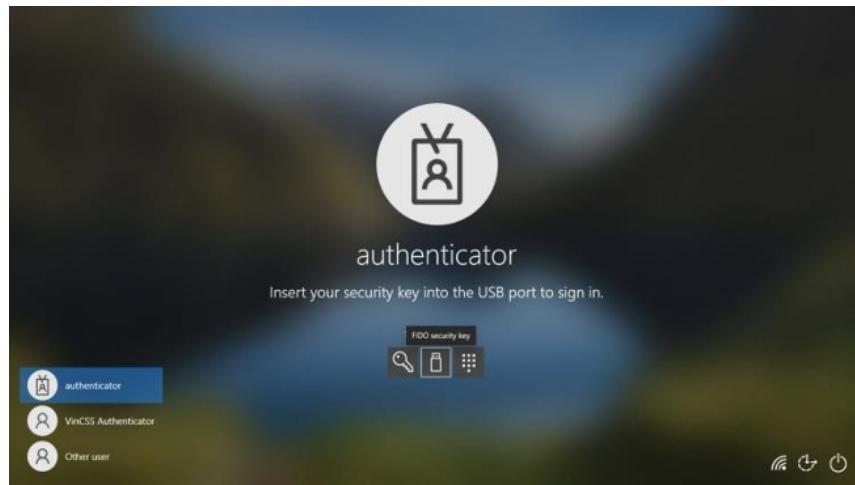


- Select security key icon as shown below to login to Windows 10 with VinCSS FIDO2® Fingerprint via Bluetooth.



III.1.2.1. Using via Bluetooth

- Connect the security key to the computer via Bluetooth.



- Scan your fingerprint when receiving notification.



III.1.2.2. Using via USB

- Connect the security key to the computer via USB, then scan your fingerprint on VinCSS FIDO2® Fingerprint sensor when receiving notification.



III.1.2.3. Using via NFC

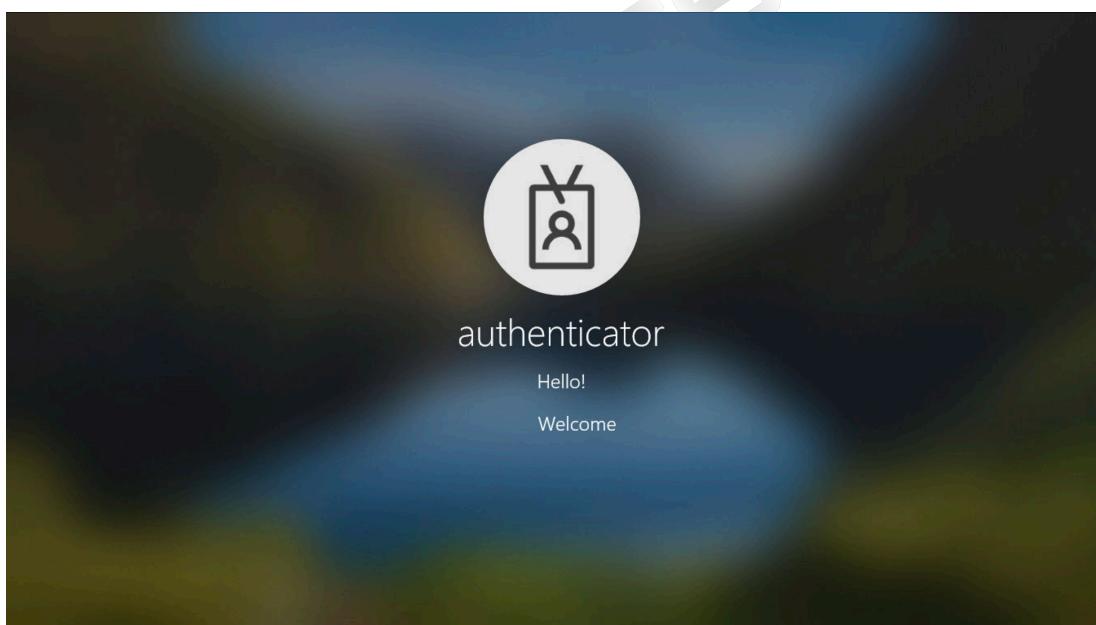
- Select smart card icon as shown below to login Windows 10 with VinCSS FIDO2® Fingerprint via NFC.



- Connect VinCSS FIDO2® Fingerprint to the computer via NFC, then scan your fingerprint on the sensor when receiving notification.



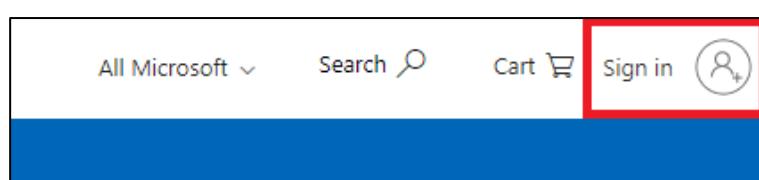
- Log in successfully.



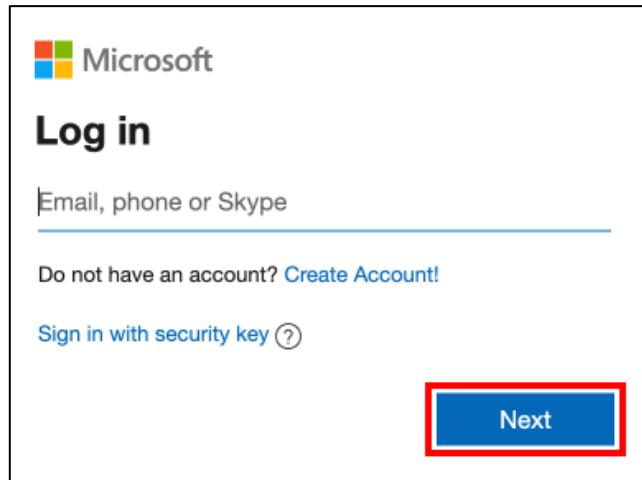
III.2. Microsoft account

III.2.1. Register authentication key

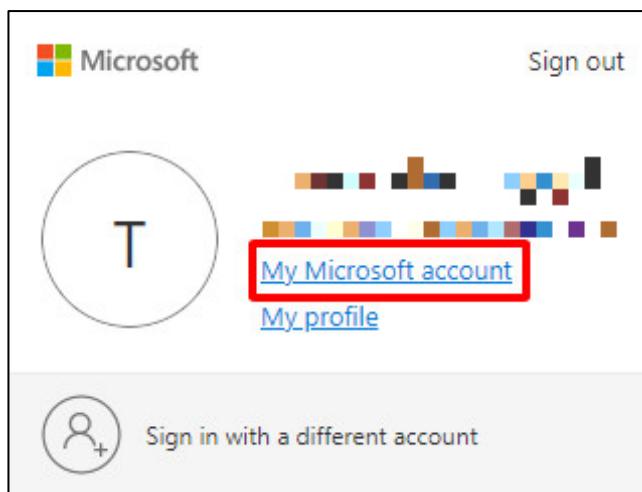
- Go to <https://microsoft.com>, then select **Sign in**.



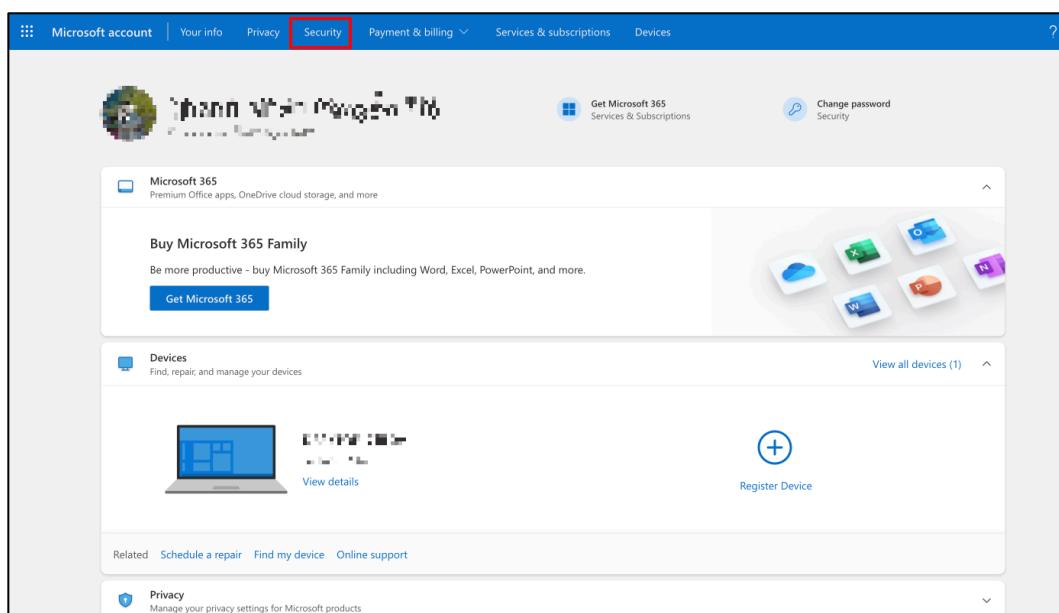
- Enter your account/password information and then click **Next** to log in.



- After successful login, select **My Microsoft account** to configure.

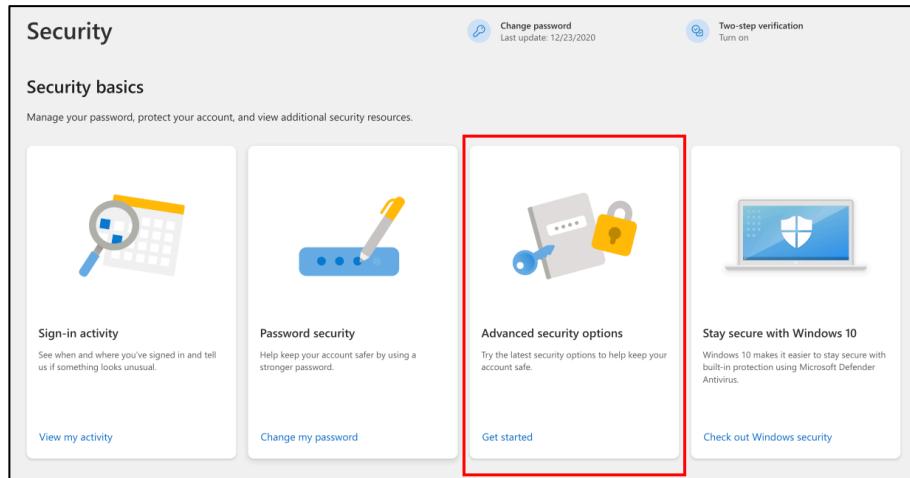


- Select **Security**.

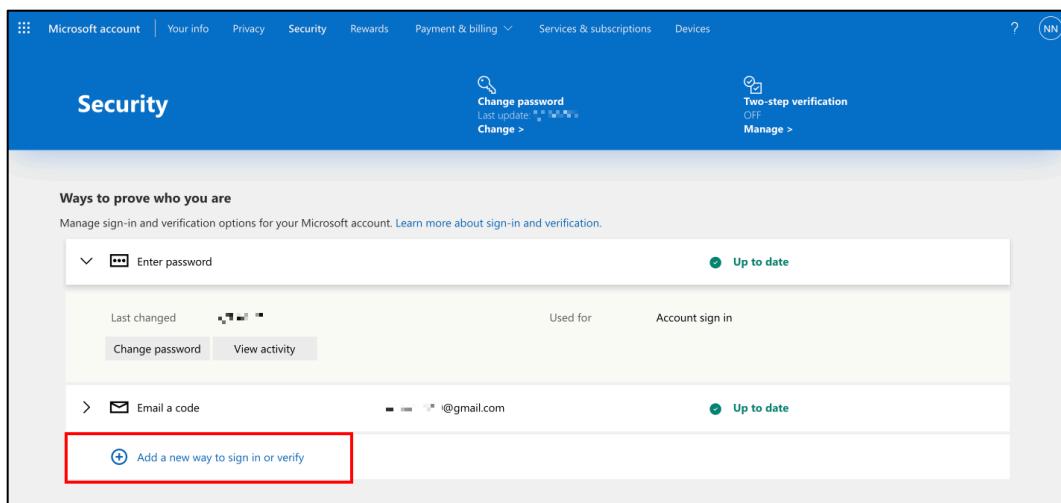


The image shows the Microsoft account dashboard with the "Security" tab selected in the top navigation bar. The main content area displays several sections: "Microsoft 365" (Buy Microsoft 365 Family), "Devices" (Find, repair, and manage your devices), and "Privacy" (Manage your privacy settings for Microsoft products). The "Devices" section includes a "Register Device" button and a "View all devices (1)" link. The "Privacy" section includes links for "Schedule a repair", "Find my device", and "Online support".

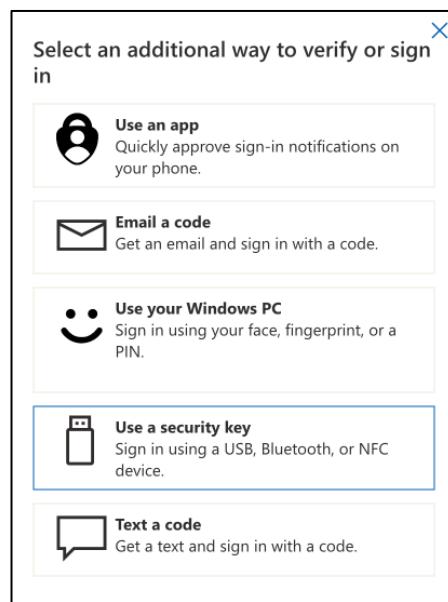
- Select **Advanced security options** to change the security method.



- Select **Add a new way to sign in or verify.**

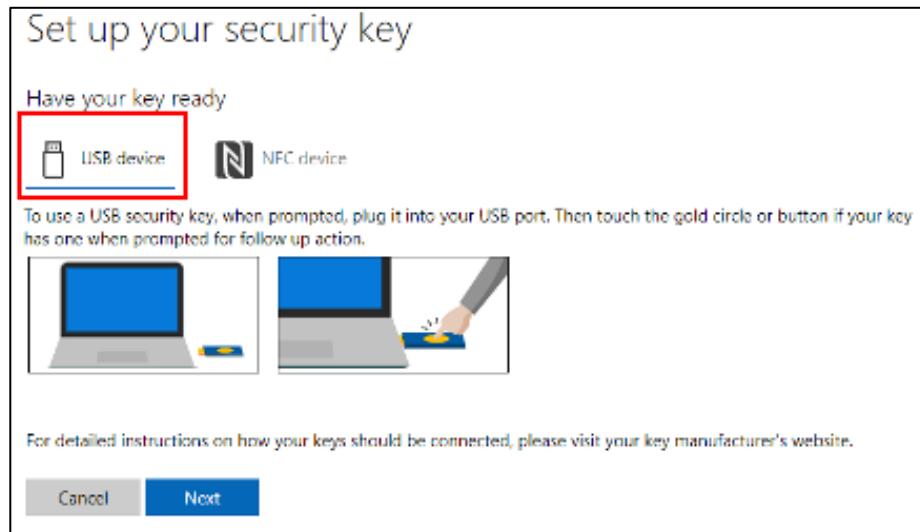


- Select **Use a security key.**

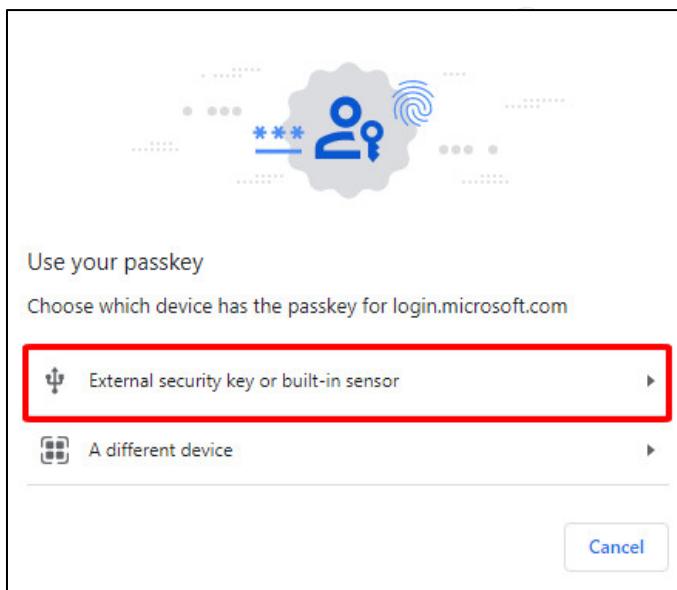


III.2.1.1. Using via Bluetooth

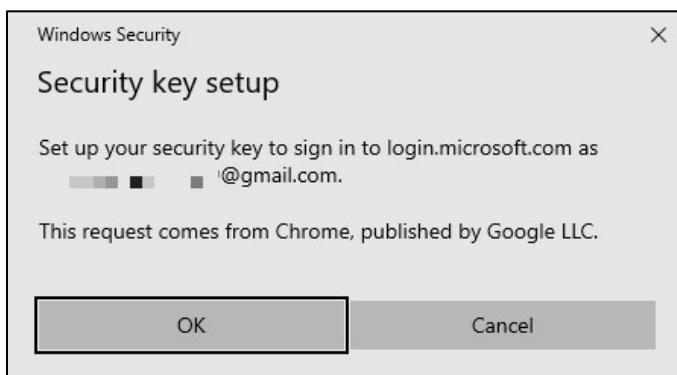
- Select **USB device**, click **Next**.



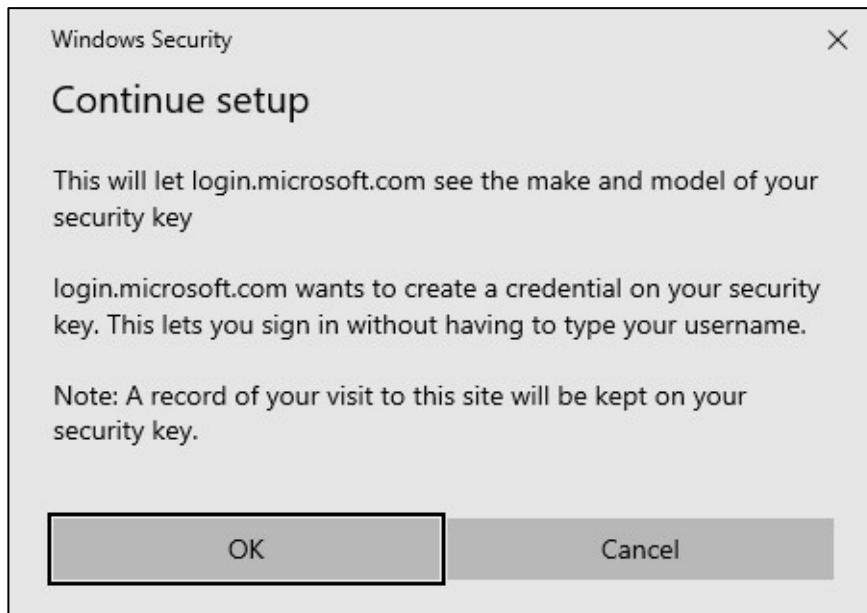
- Select **External security key or built-in sensor** to set up security key.



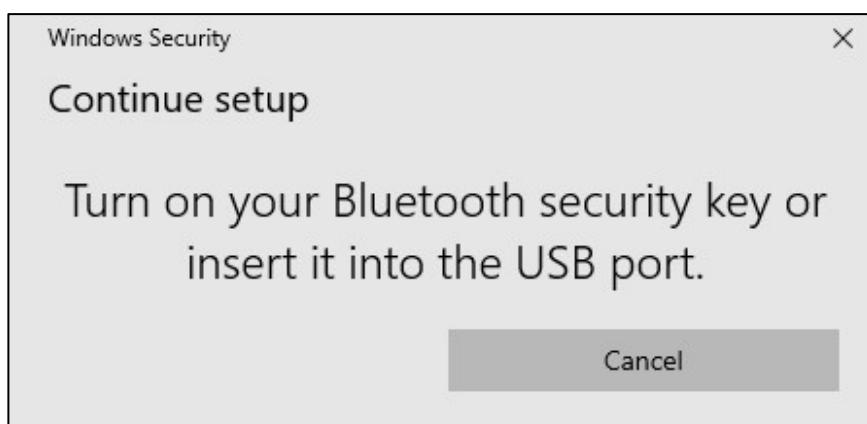
- Select **OK** to continue to set up the security key.



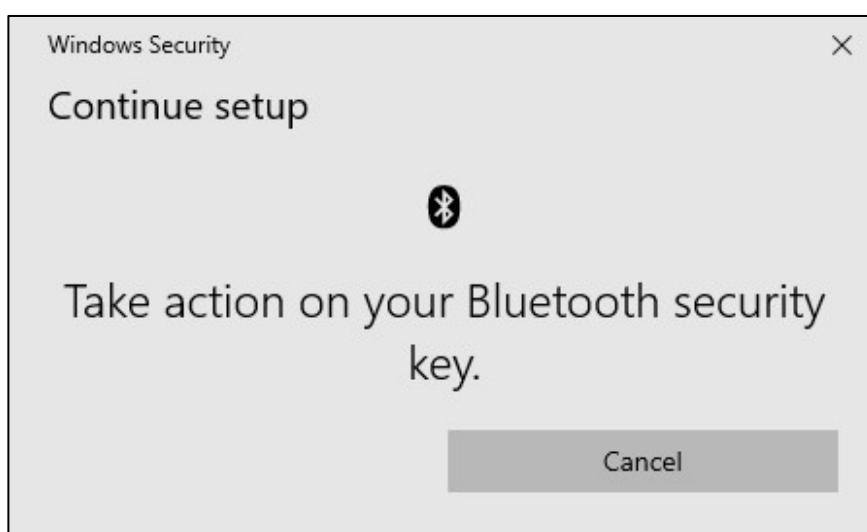
- Select **OK** to continue.



- Connect the VinCSS FIDO2® Fingerprint to your computer via Bluetooth.

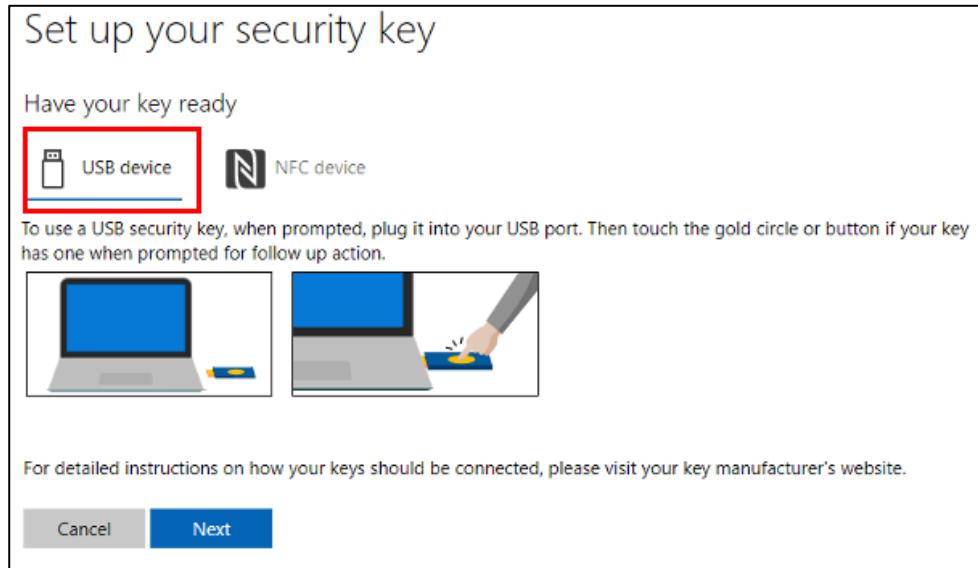


- Scan your fingerprint when receiving notification.

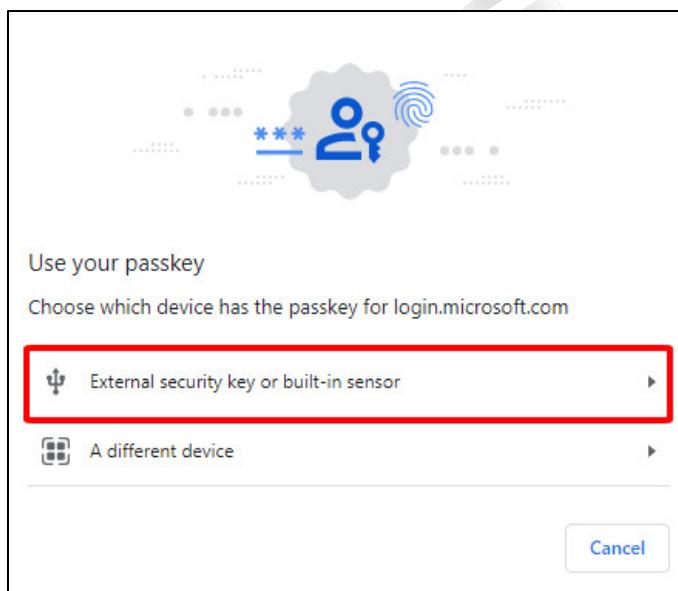


III.2.1.2. Using via USB

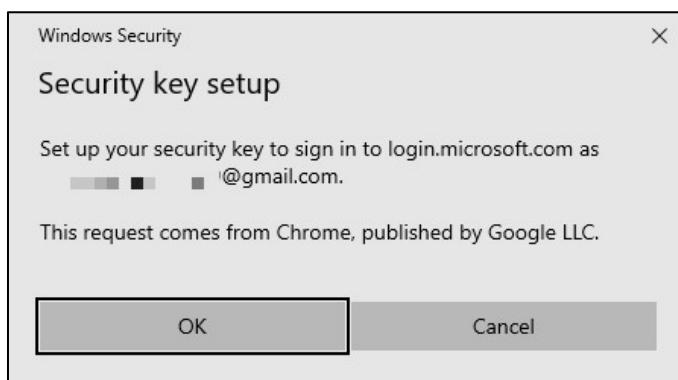
- Select **USB device**, click **Next**.



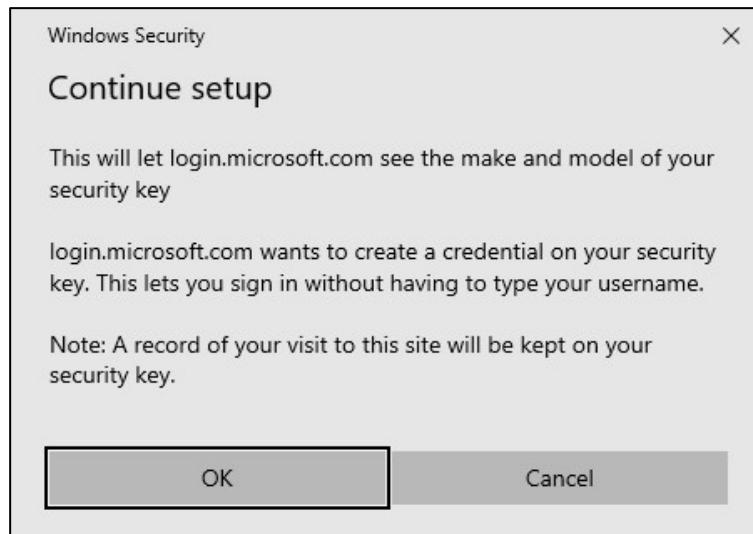
- Select **External security key or built-in sensor** to set up security key.



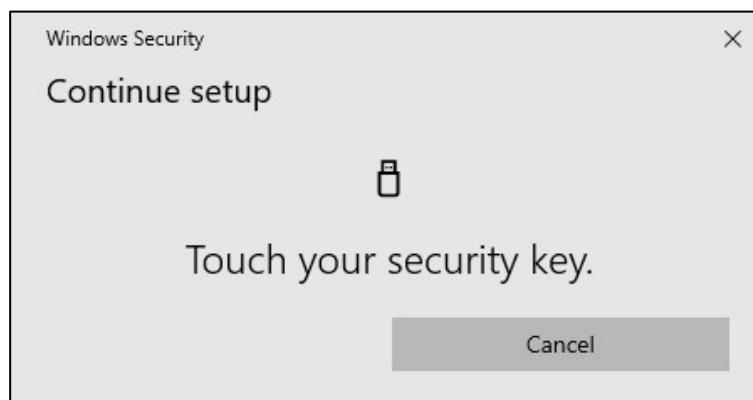
- Select **OK** to continue to set up the security key.



- Select **OK** to continue.

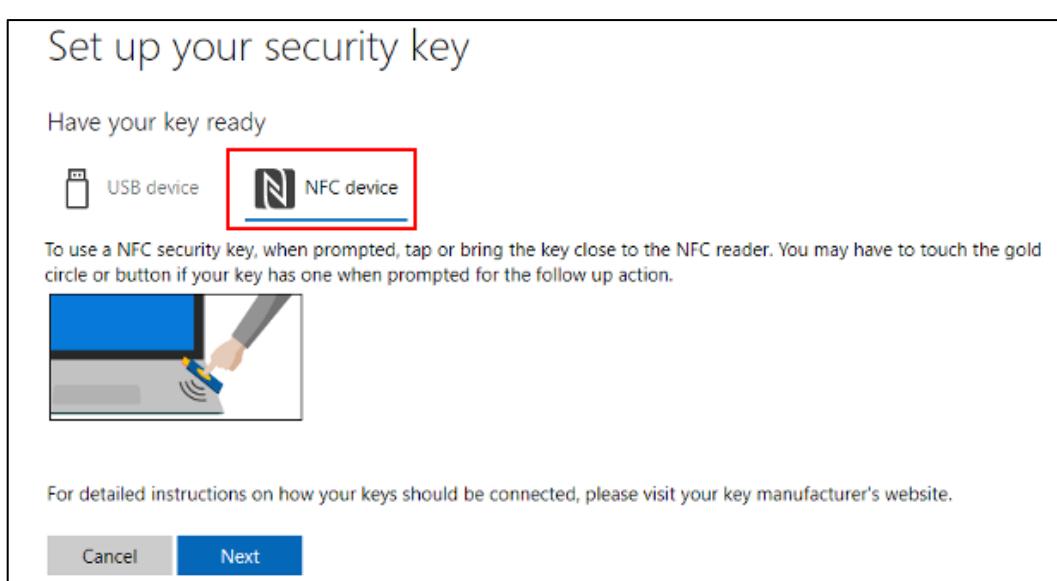


- Connect the VinCSS FIDO2® Fingerprint to the computer via USB, scan your fingerprint on the sensor when receiving the notification.

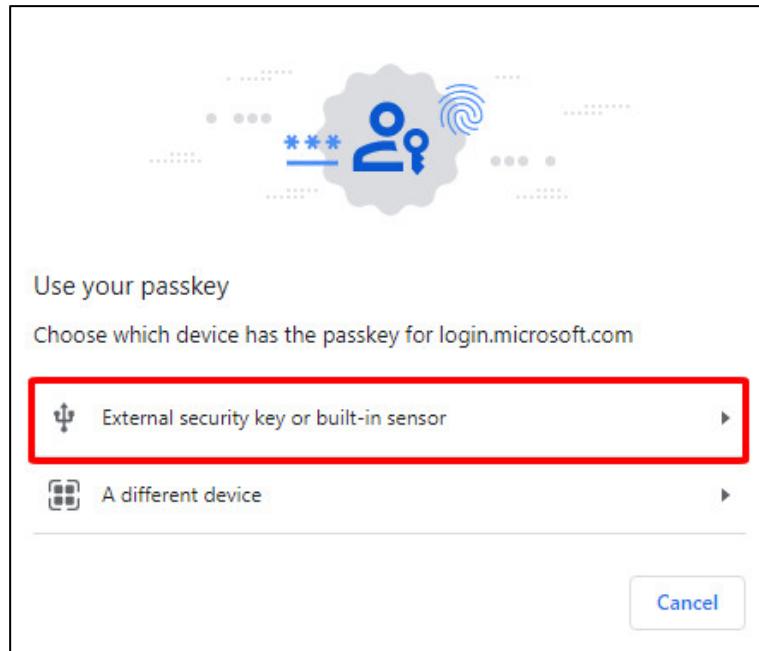


III.2.1.3. Using via NFC

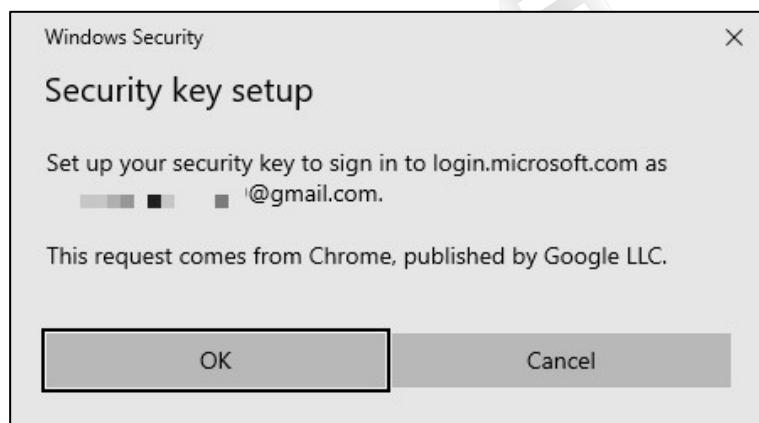
- Select **NFC device**. Click **Next**.



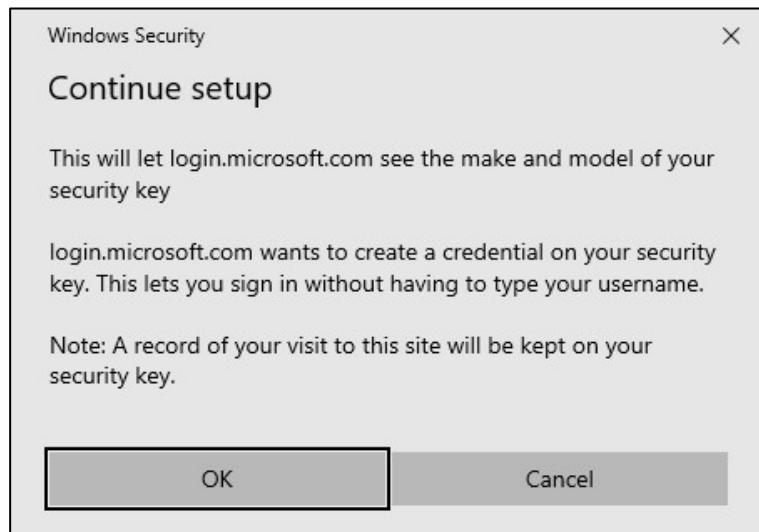
- Select **External security key or built-in sensor** to set up security key.



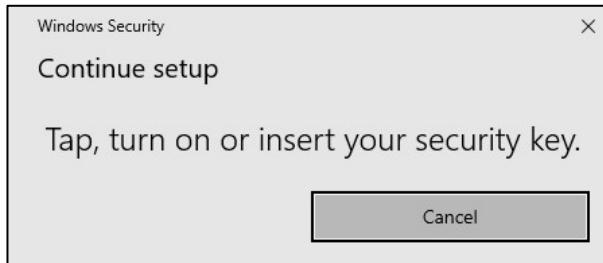
- Select **OK** to continue to set up the security key.



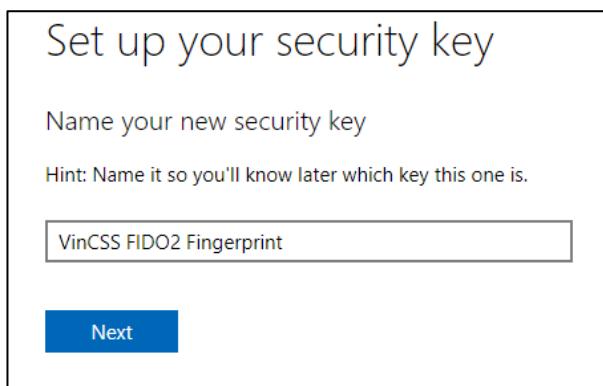
- Select **OK** to continue.



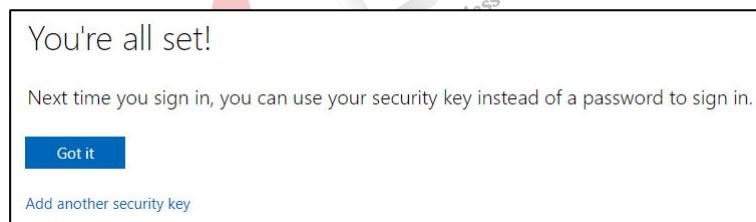
- Connect the key to the NFC reader when receiving the notification, then scan your fingerprint on the sensor.



- Name the security key to distinguish the key, then click **Next**.

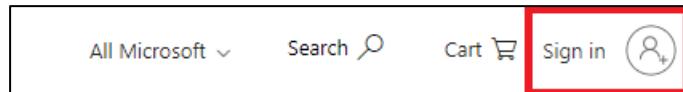


- Click **Got it** to complete the Security key registration.

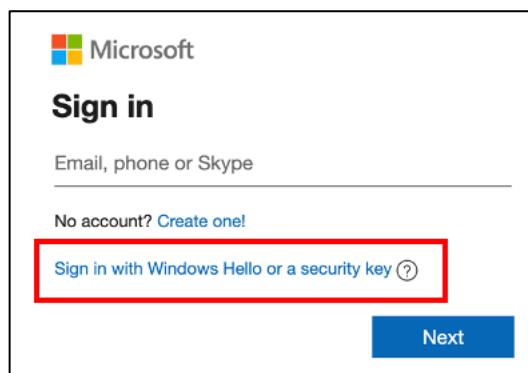


III.2.2. Passwordless authentication of Microsoft accounts

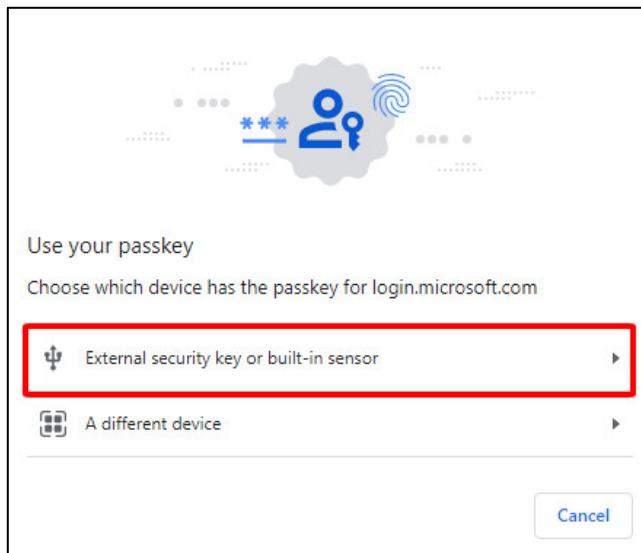
- Access <https://microsoft.com>, click **Login**.



- Select **Sign on with Windows Hello or a security key**.



- Select **External security key or built-in sensor** to log in with the security key.



III.2.2.1. Using via Bluetooth

- Connect the security key to computer via Bluetooth.



- Scan fingerprint when receiving notification.



III.2.2.2. Using via USB

- Connect VinCSS FIDO2® Fingerprint to computer via USB, touch fingerprint scanner on security key when receiving the notification.

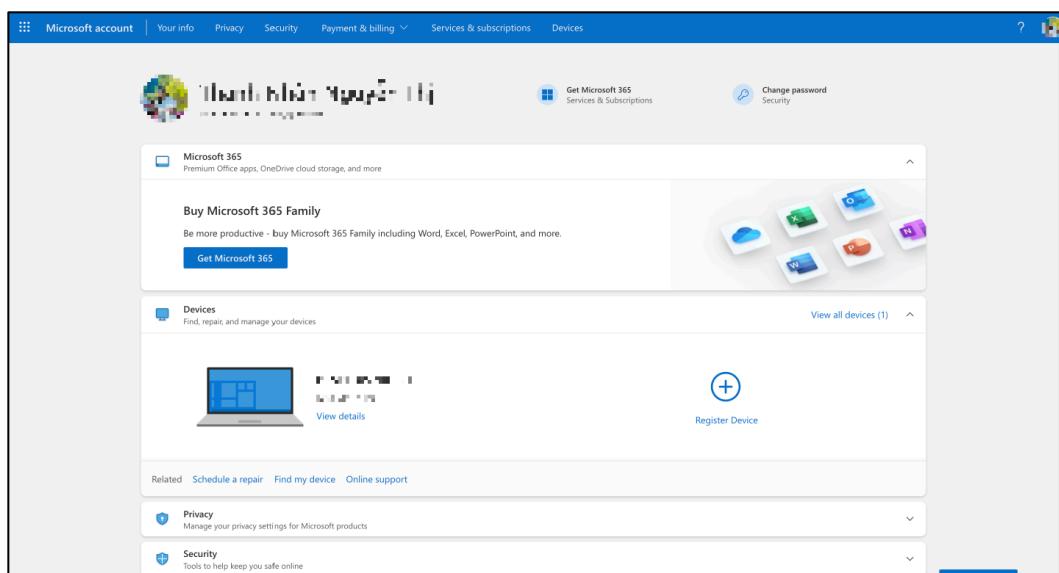


III.2.2.3. Using via NFC

- Connect VinCSS FIDO2® Fingerprint to computer via NFC, touch the security key to NFC reader when receiving notification.



- Log in successfully.

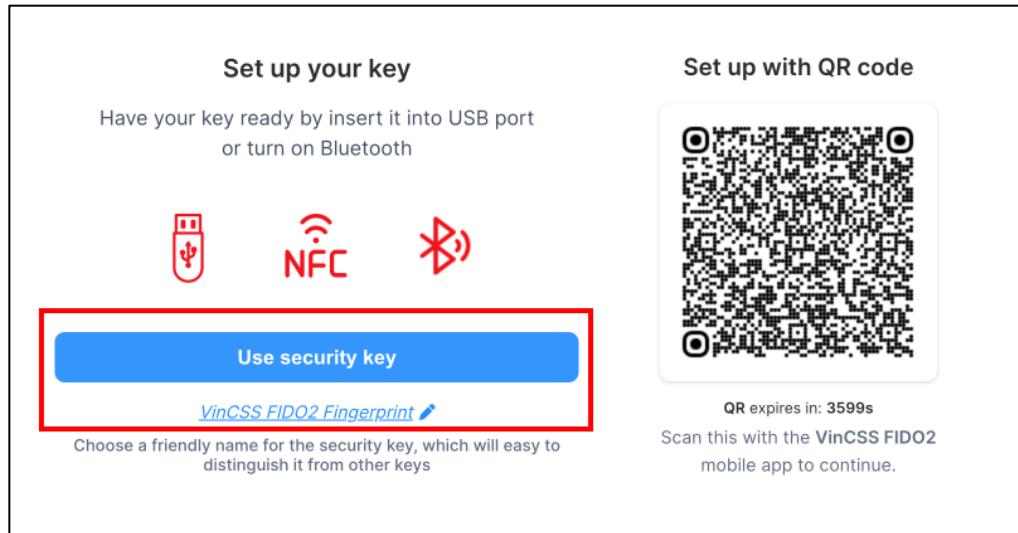


III.3. VinCSS OVPN Client

III.3.1. Windows

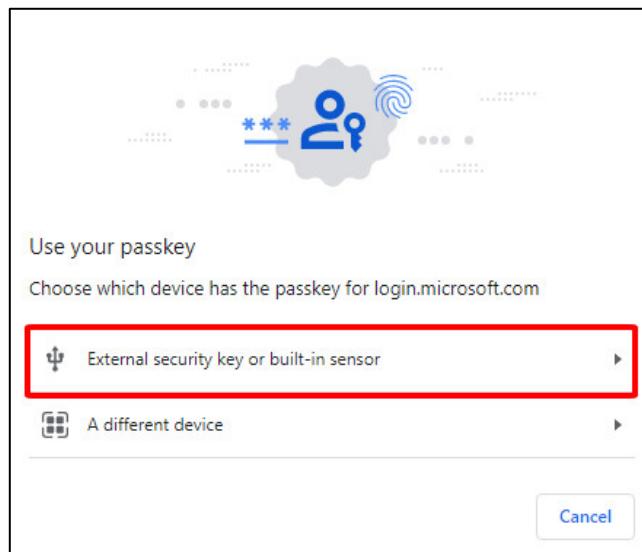
III.3.1.1. Register for VinCSS FIDO2® Fingerprint security key

- Contact administrator to get the key registration link sent to user via email or IM (*valid for 1 hour*). Change the security key name and select **Use security key**.

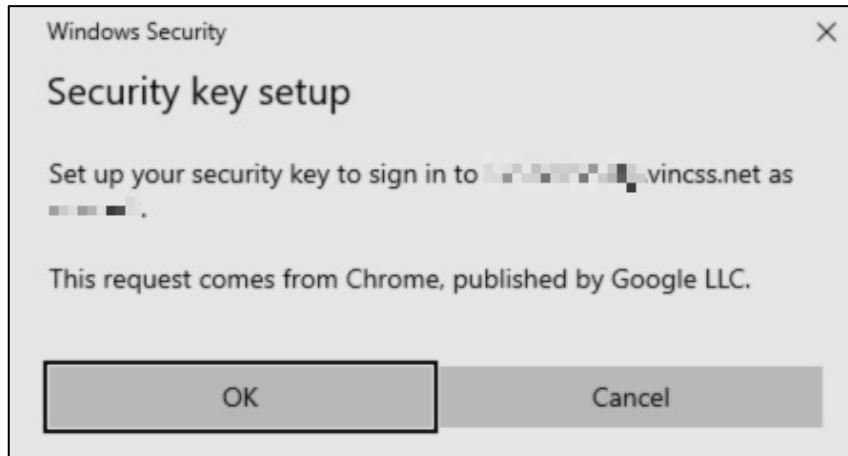


Note: By default, administrator will send a link to register a security key that can be used with all login methods after successfully registering a security key (Passwordless authentication method (Refer to section III. 3.1.2.1.) and anonymous authentication (Refer to section III.3.1.2.2.))

- Select **External security key or built-in sensor** to register the VinCSS FIDO2® Fingerprint security key.



- Select **OK** to continue with the security key registration process.

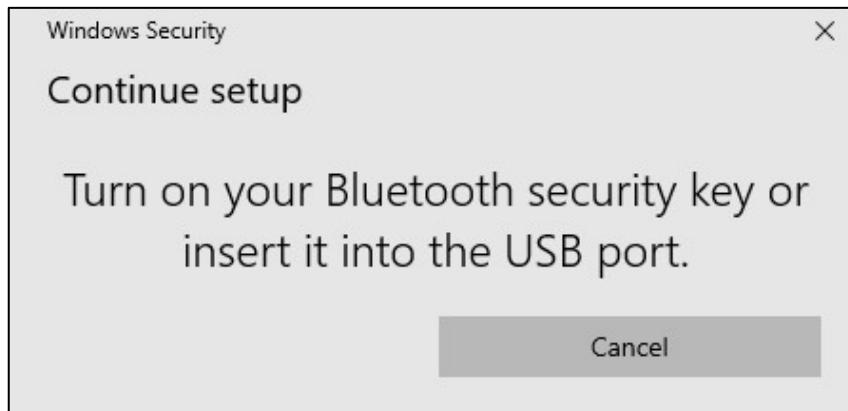


- Click **OK** to continue.

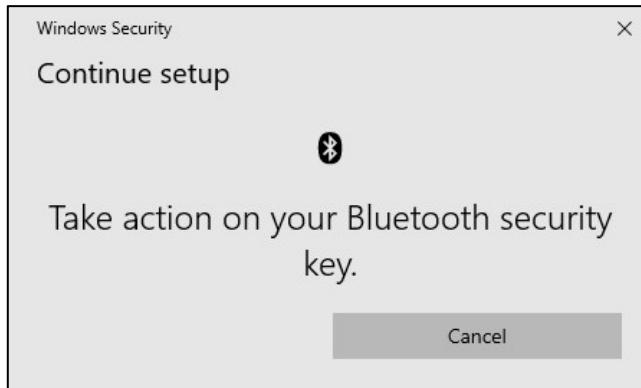


III.3.1.1.1. Using via Bluetooth

- Connect the security key to the computer via Bluetooth connection.

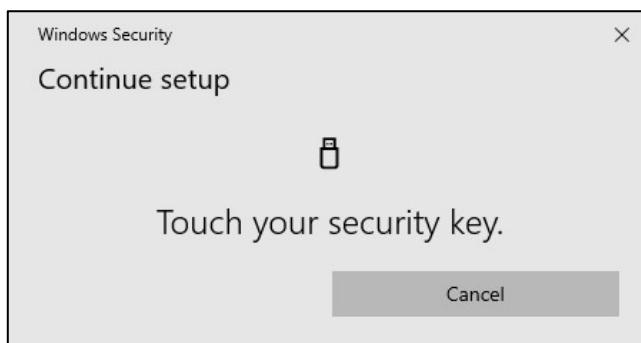


- Scan your fingerprint when you receive a notification.



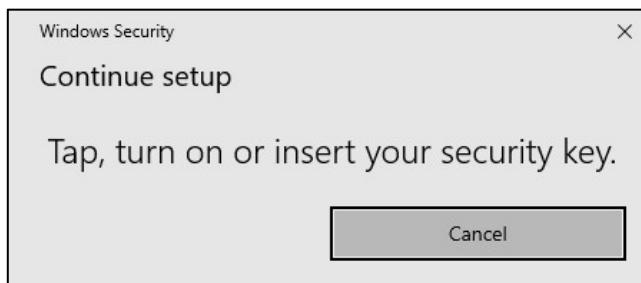
III.3.1.1.2. Using via USB

- Connect the security key to the computer via the USB connection wire, touch the fingerprint scanner on the security key when receiving the notification.

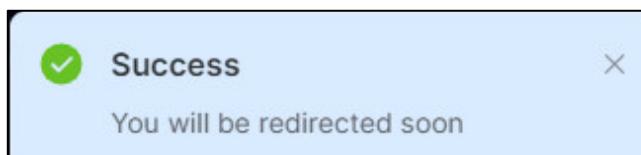


III.3.1.1.3. Using via NFC

- Connect the security key to the computer via the NFC reader, touch the security key to the NFC reader when receiving the notification.

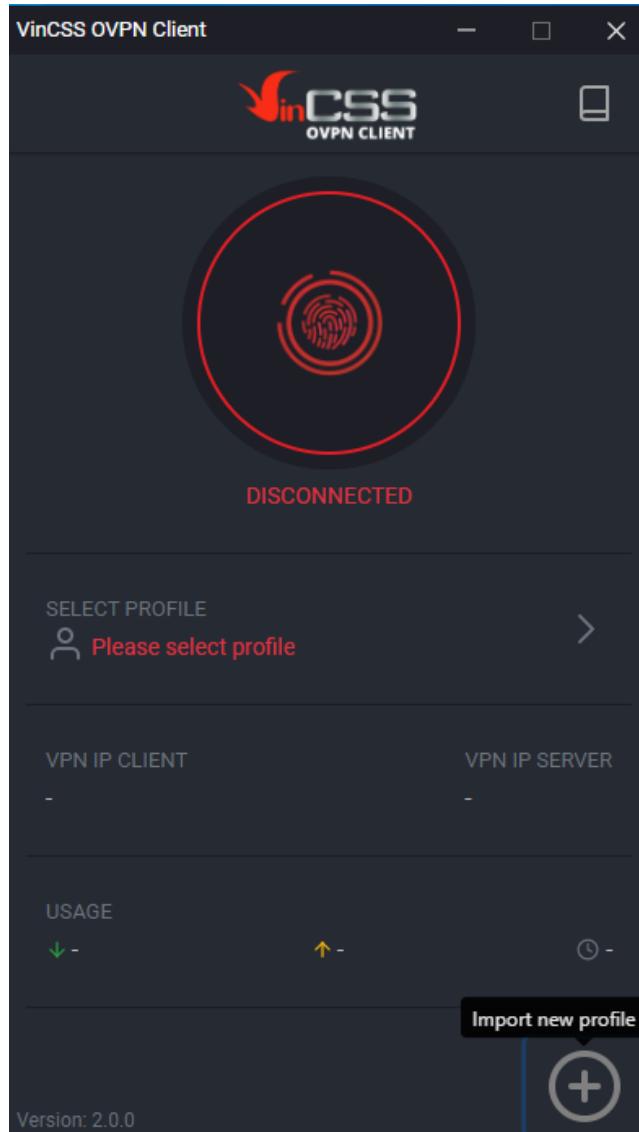


- On the computer screen, a pop-up will appear to notify user that the security key has been successfully registered.

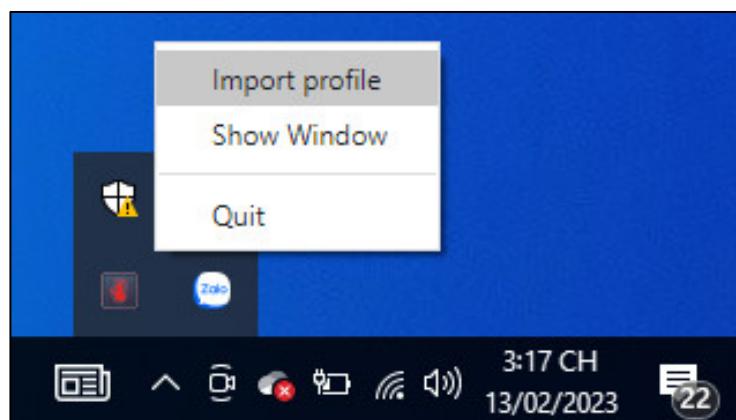


III.3.1.2. Authentication with VinCSS FIDO2® Fingerprint security key

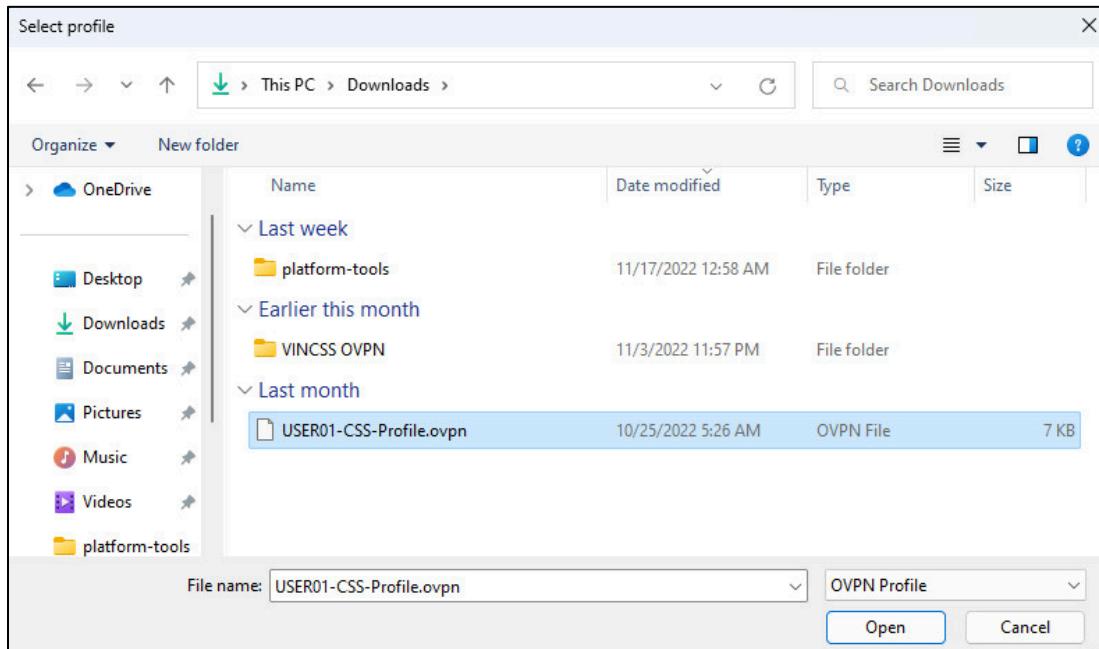
- Open VinCSS OVPN Client, on the interface select **Import new profile**.



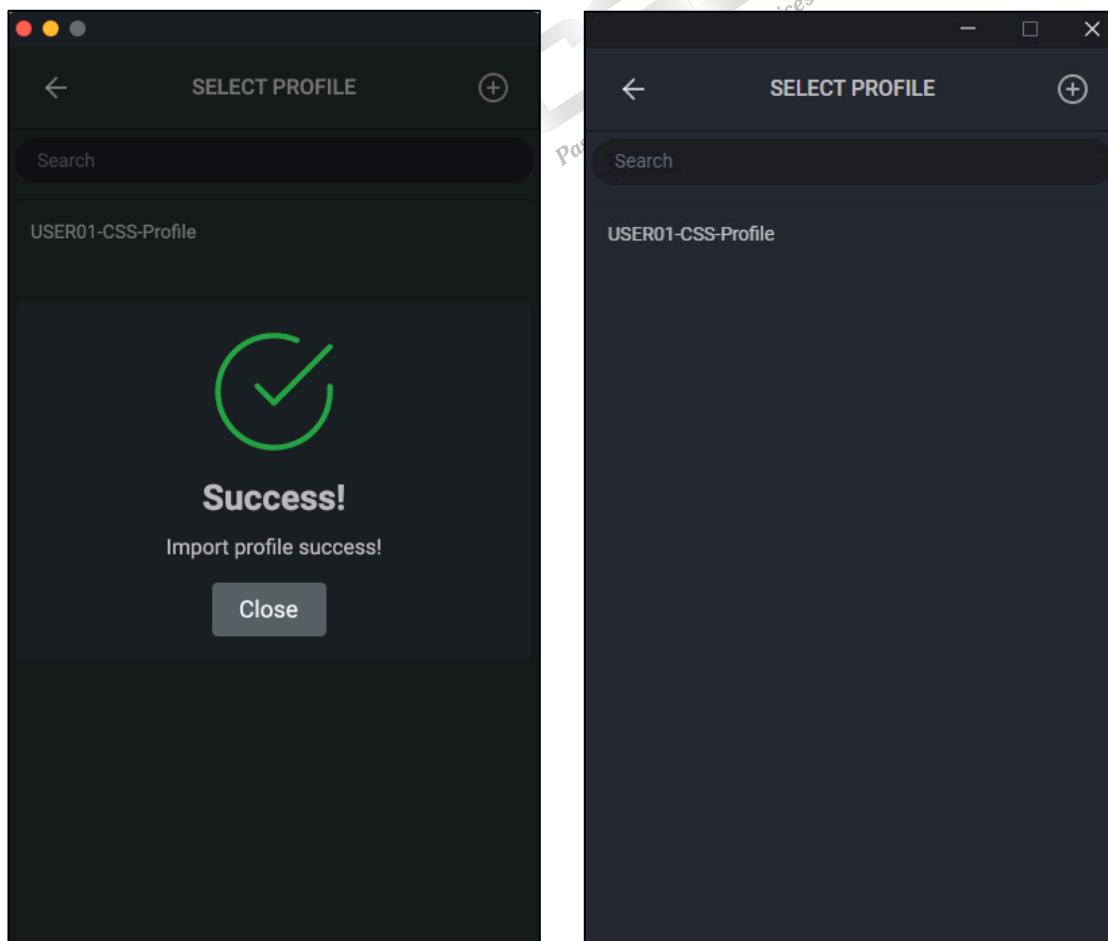
- Or right-click on the VinCSS OVPN Client icon on the taskbar, select **Import profile**.



- Select the profile sent by administrator (*file .ovpn*) and click **Open**.

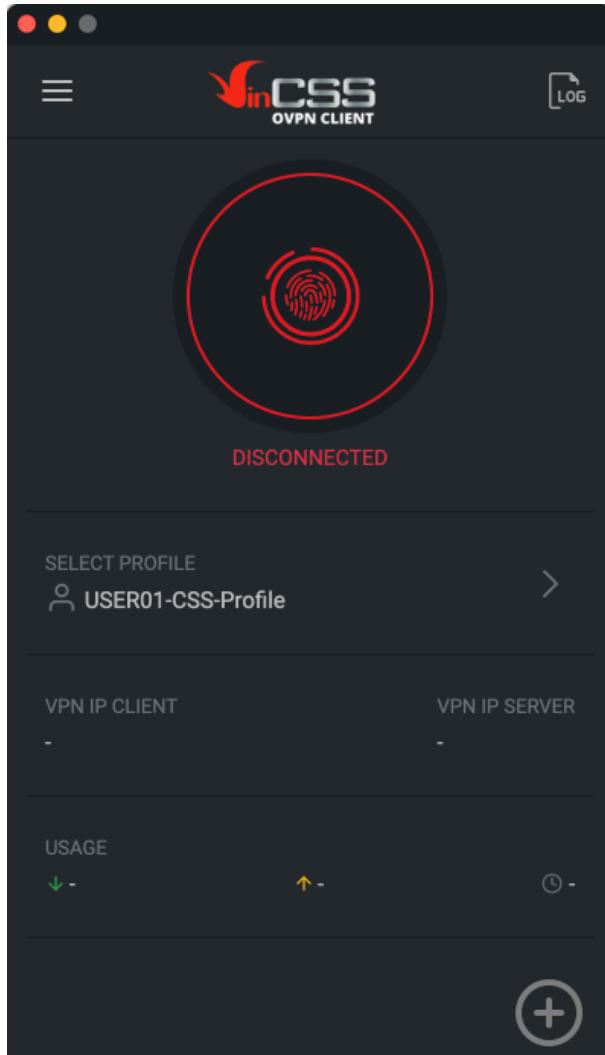


- Profile is added successfully. Click **Close** to close the notification window.
Screen shows profile name on the list.

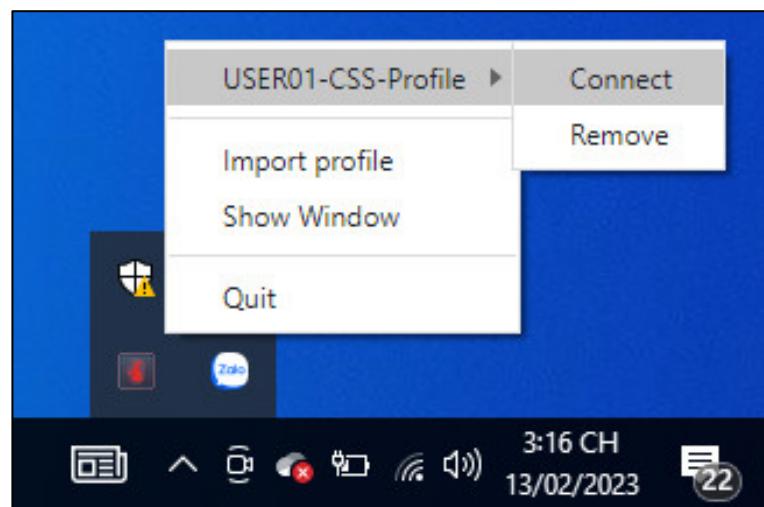


- After adding new profile, click on the fingerprint icon to connect to the VPN.

Click on the fingerprint logo on the application interface

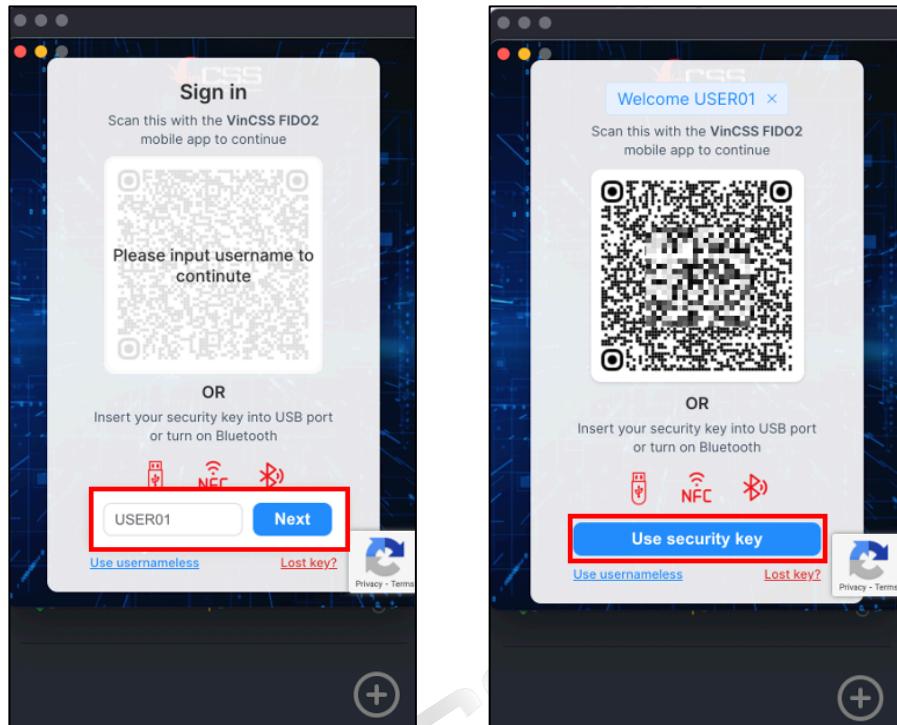


- Or right-click the VinCSS OVPN Client icon in the taskbar, select the VPN profile to connect, then select **Connect**.



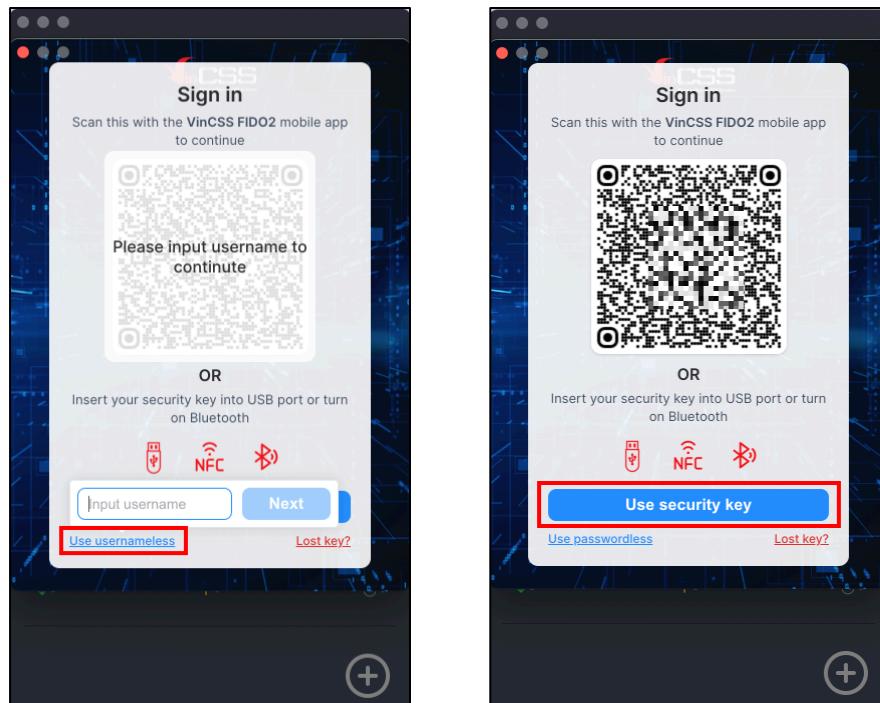
III.3.1.2.1. Passwordless authentication

- Enter **Username** (*not case sensitive*), select **Next**. Then select **Use security key** to continue.



III.3.1.2.2. Authentication usernameless

- Users can choose another login method by selecting **Use usernameless** instead of entering **username** and then selecting **Use security key**.



III.3.1.2.2.1. Using via Bluetooth

- Connect VinCSS FIDO2® Fingerprint to the computer via Bluetooth.



- Scan your fingerprint when receiving the notification.



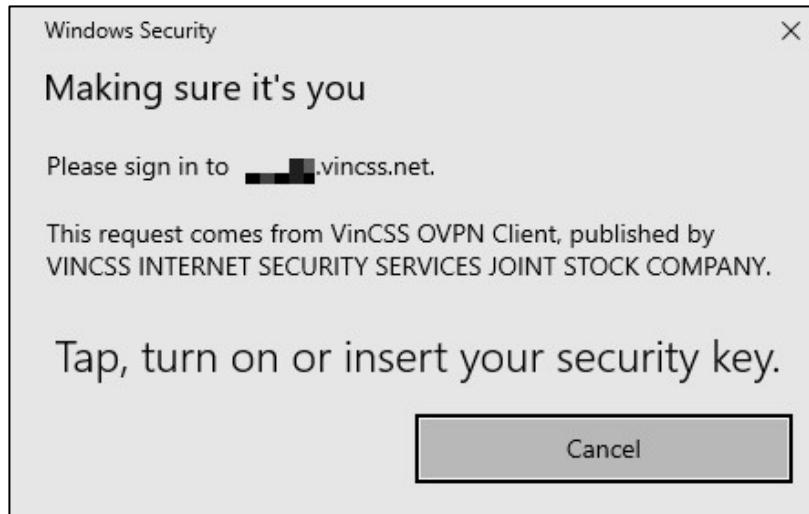
III.3.1.2.2.2. Using via USB

- Connect VinCSS FIDO2® Fingerprint to the computer via USB. Scan fingerprint on security key when receiving notification

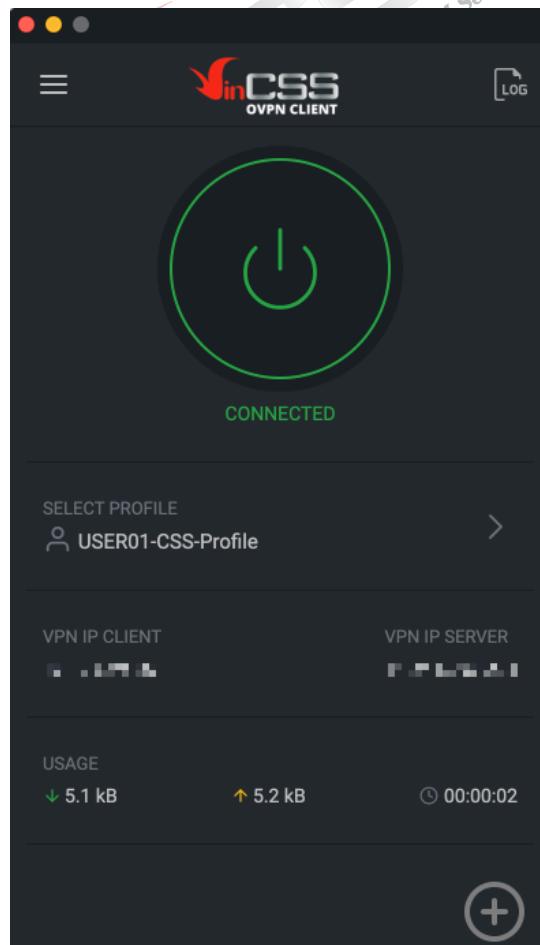


III.3.1.2.2.3. Using via NFC

- Connect VinCSS FIDO2® Fingerprint to the computer via NFC. Touch the key to the NFC reader when receiving the notification.



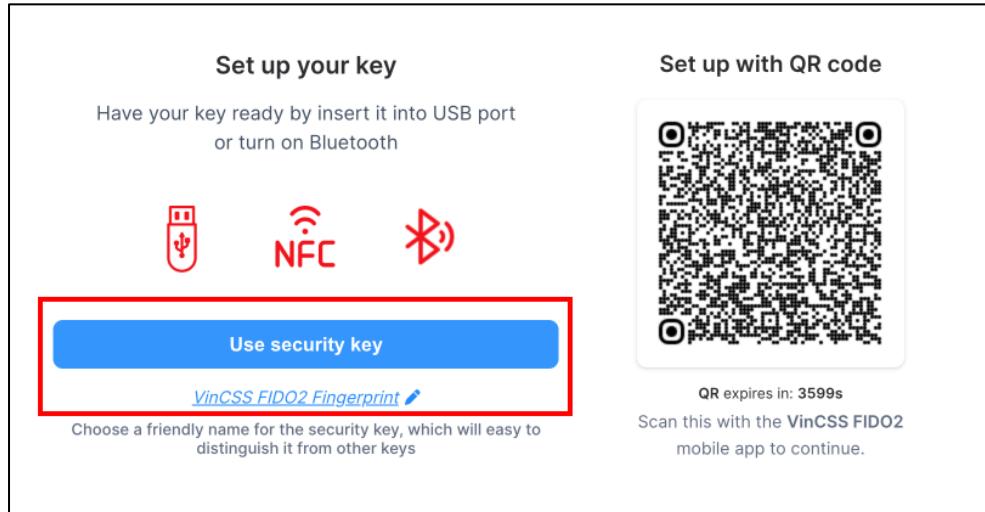
- The connection process is conducted when user authenticates successfully. When VPN is connected successfully, on the application interface shows the status **CONNECTED**.



III.3.2. macOS

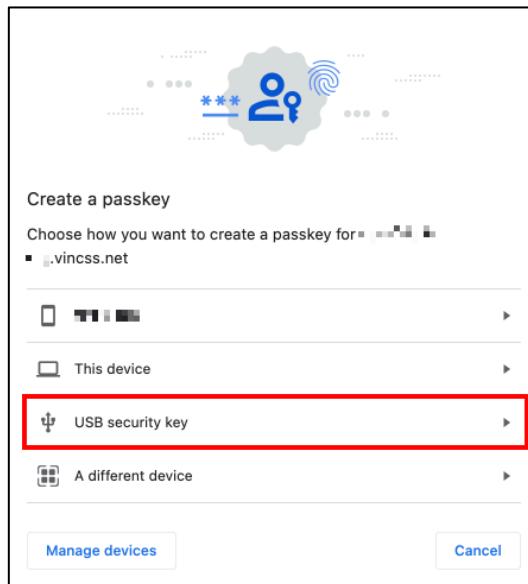
III.3.2.1. Register for VinCSS FIDO2® Fingerprint security key (*Only USB connection is supported*)

- Contact administrator to get the key registration link sent to the user via email or IM (*valid for 1 hour*). Change the security key name and select **Use security key**.

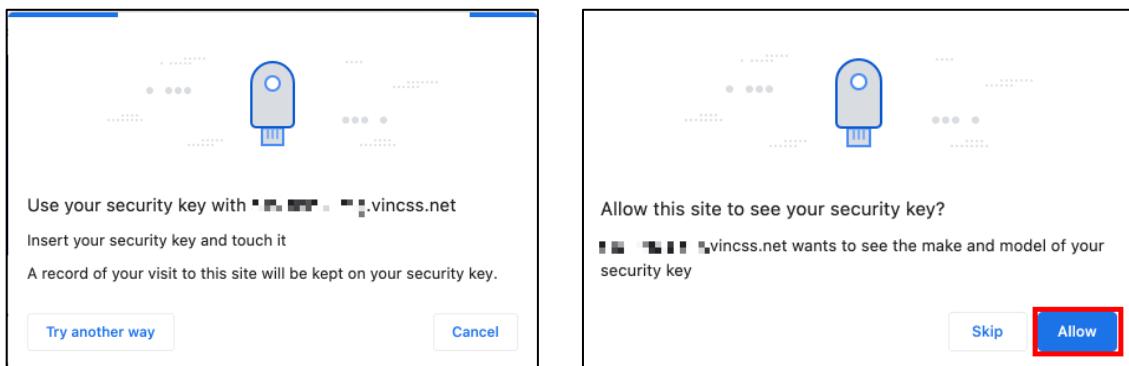


Note: By default, the administrator will send a link to register a security key that can be used with all login methods after successfully registering a security key (Passwordless authentication method (Refer to section III. 3.2.2.1.) and anonymous form of authentication (Refer to section III.3.2.2.2.))

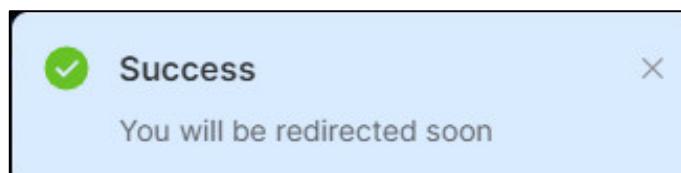
- Select **USB security key** to register with VinCSS FIDO2® Fingerprint security key.



- Touch the fingerprint scanner on the security key when receiving the notification. Then click **Allow** to continue.

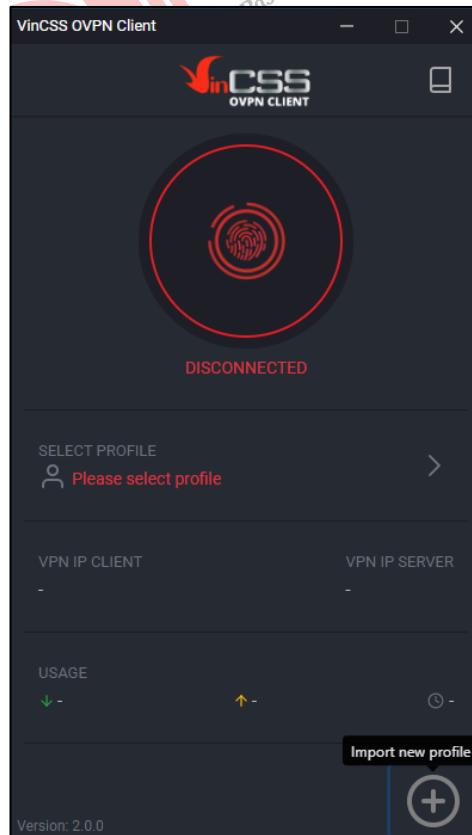


- On the computer screen, a pop-up will appear to notify the user that the security key has been successfully registered.

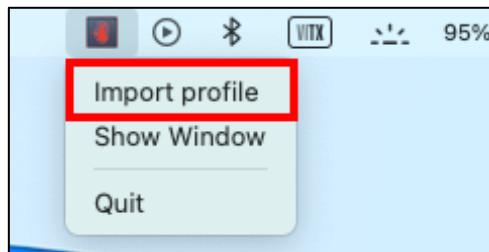


III.3.2.2. Authentication with VinCSS FIDO2® Fingerprint security key

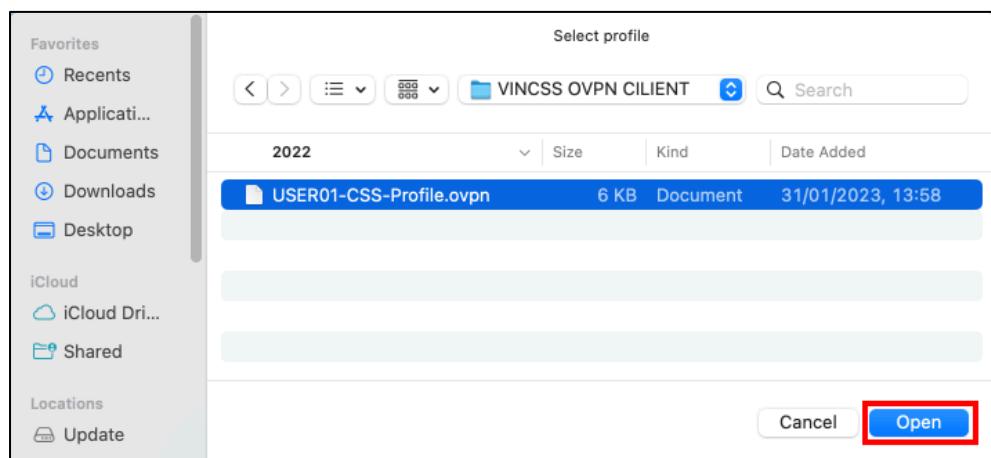
- Open the VinCSS OVPN Client software installed in the machine. On the main interface, click the (+) sign to add a new profile.



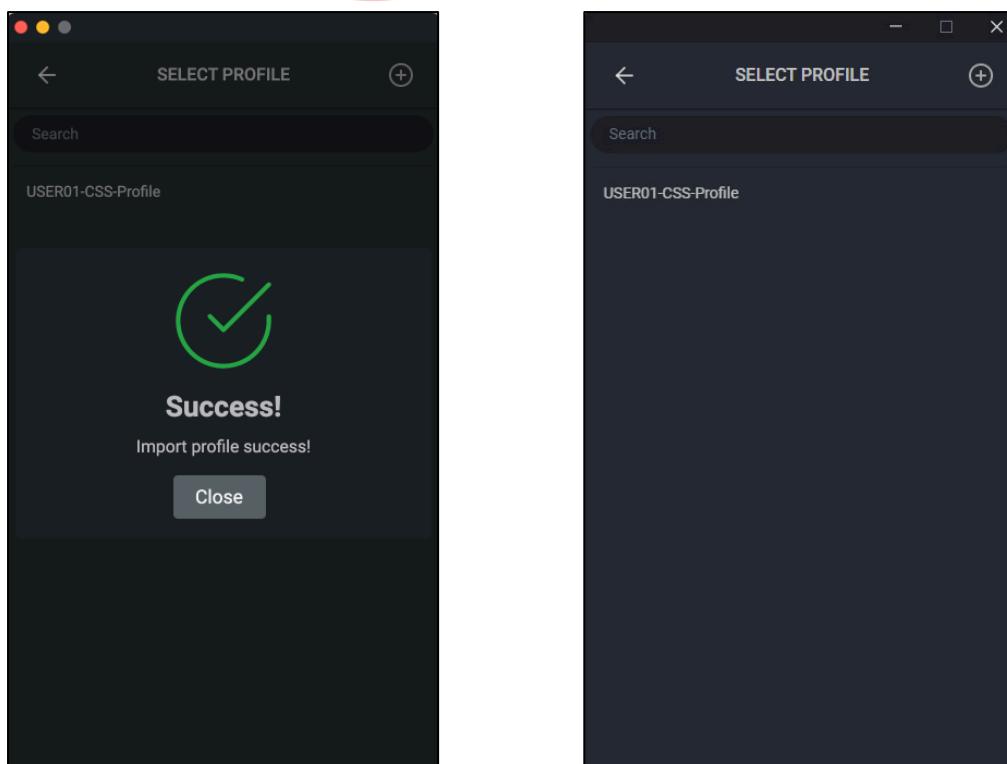
- Or right-click on the VinCSS OVPN Client icon on the taskbar, select **Import profile**.



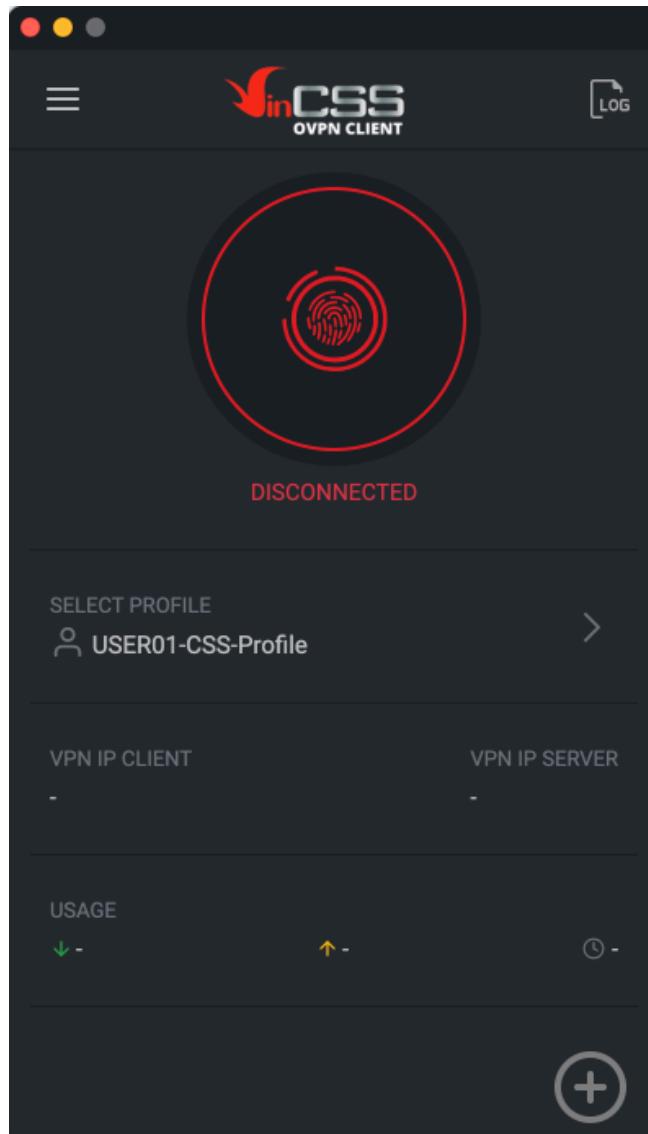
- Select the profile sent by the administrator (*file .ovpn*) and select **Open**.



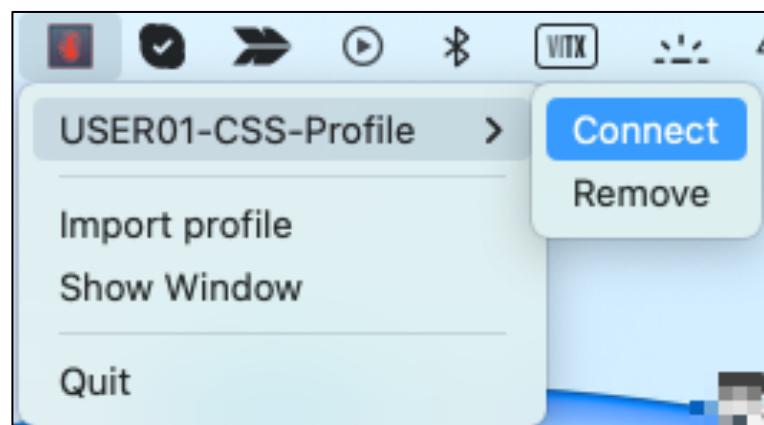
- Profile added successfully, click Close to close the notification window. The screen shows the profile name in the list.



- Click on the red fingerprint icon on the application interface to proceed with the VPN connection.

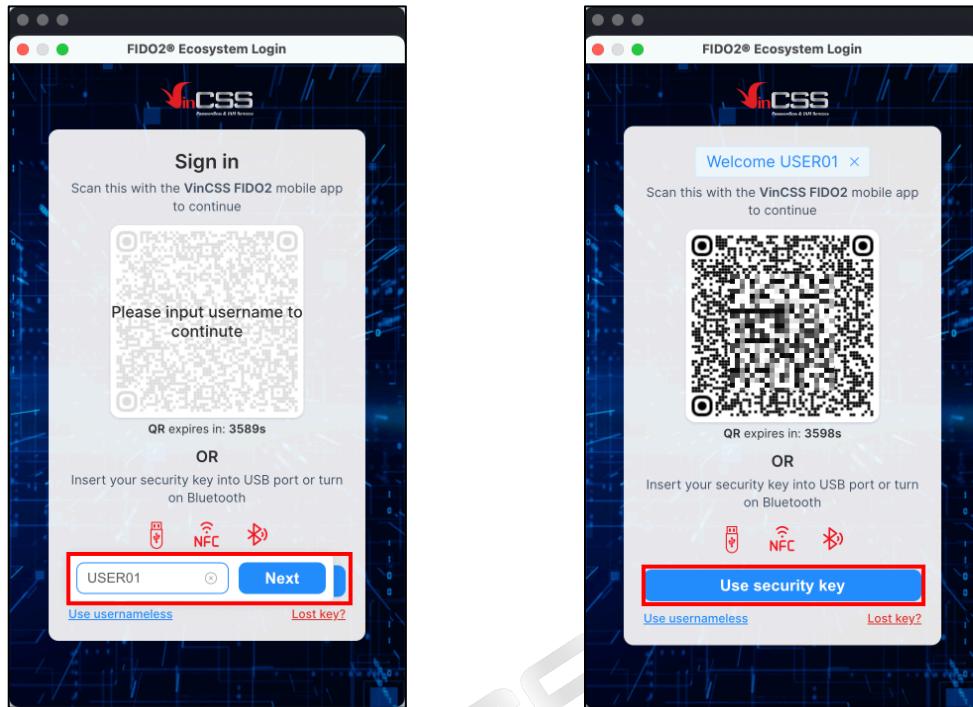


- Or right-click the VinCSS OVPN Client icon in the taskbar, select the VPN profile to connect, then select **Connect**.



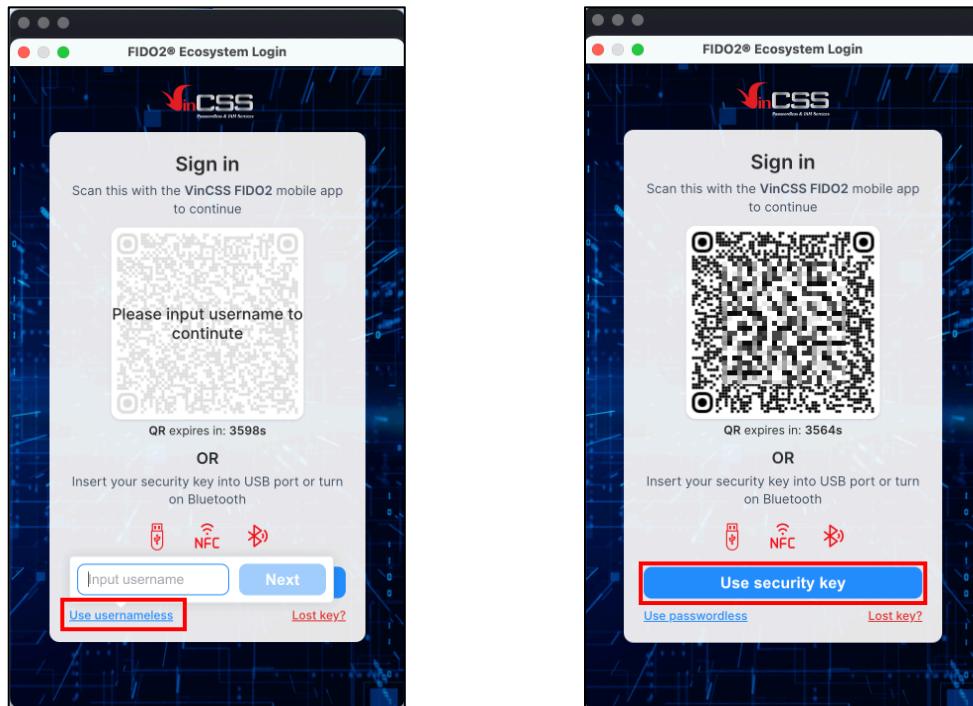
III.3.2.2.4. Passwordless authentication

- Enter **Username** (*case insensitive*), select **Next**. Then select **Use security key** to continue.



III.3.2.2.5. Authentication usernameless

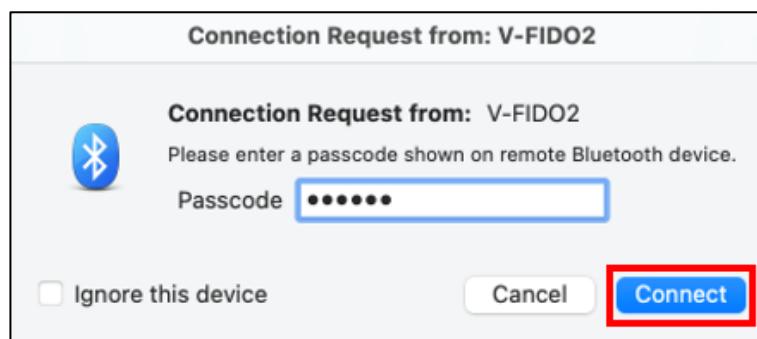
- User can choose another login method by selecting **Use usernameless** instead of entering **username** and then selecting **Use security key**.



III.3.2.2.2.1. Using via Bluetooth

- Touch and hold the fingerprint scanner (*about 5-8 seconds*) of the security key until the indicator light flashes blue. The security key is in the pairing pending state. Enter the pairing code (*The pairing code is the last sequence (5 or 6 digits) of the serial code displayed on the back of the security key*) to connect and then select **Connect**.

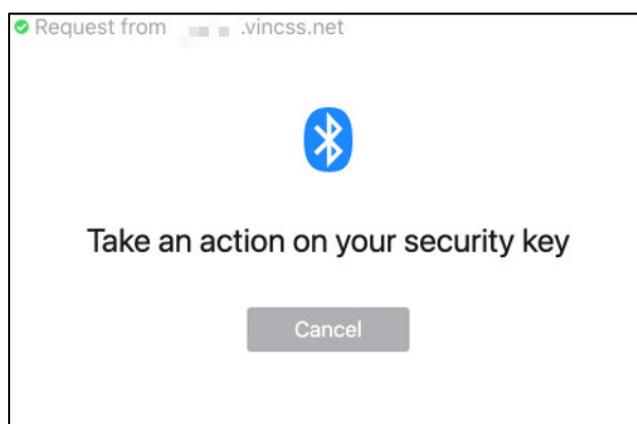
Note: macOS does not support the Bluetooth connection of the security key. The Bluetooth connection of security key can only be supported through VinCSS OVPN Client application at this step.



- Users click on the name of the security key to connect.

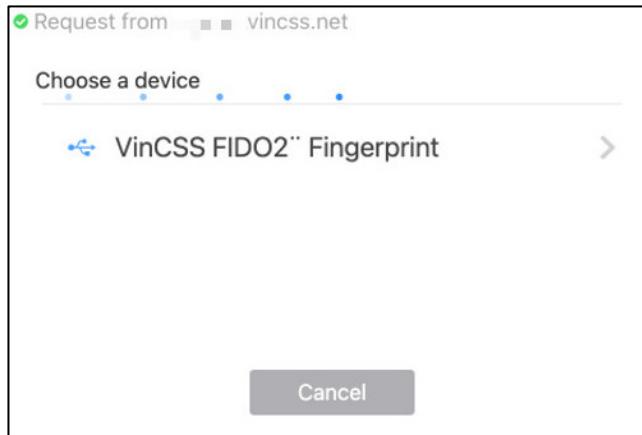


- Scan your fingerprint when you receive a notification.

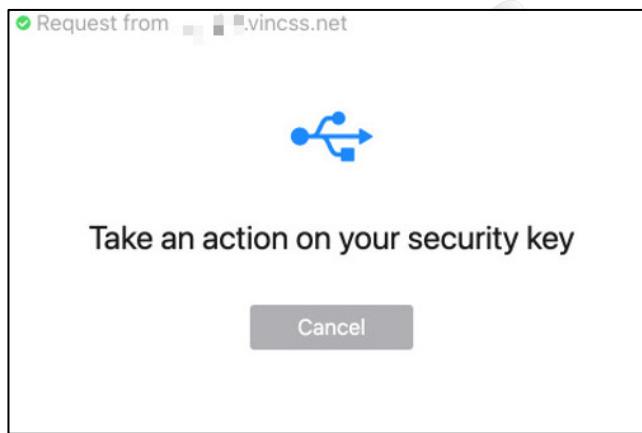


III.3.2.2.2.2. Using via USB

- Connect the security key to the computer via the USB cable. Select the device to connect.



- Touch the fingerprint scanner on the security key when receiving the notification.

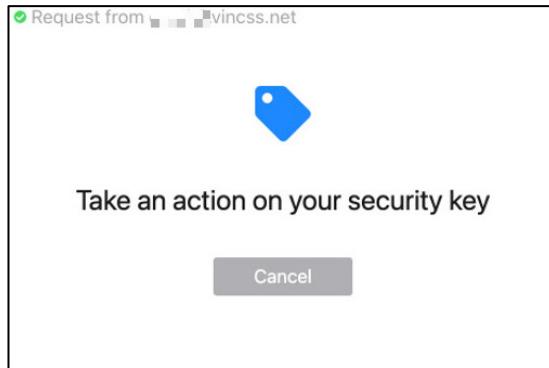


III.3.2.2.2.3. Using via NFC

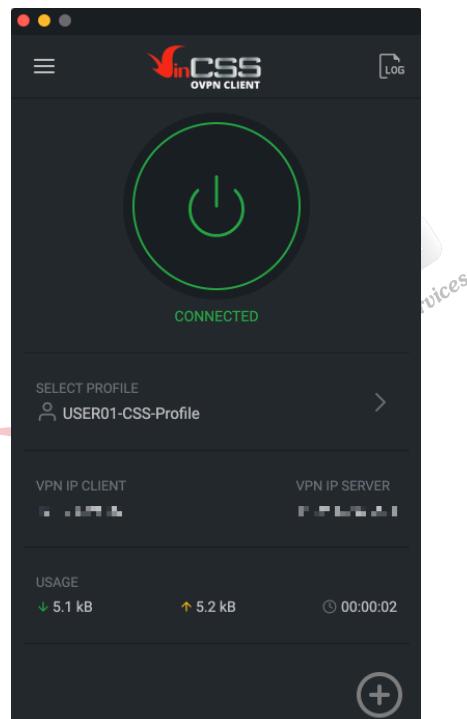
- Connect the security key to the computer via NFC connection, select the device to connect.



- Connect the security key to the NFC reader when receiving a notification.



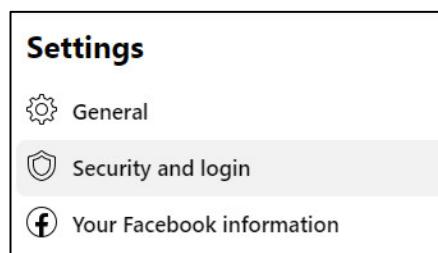
- The connection process is done when user is successfully authenticated. VPN is connected successfully when **CONNECTED** status is displayed on screen.



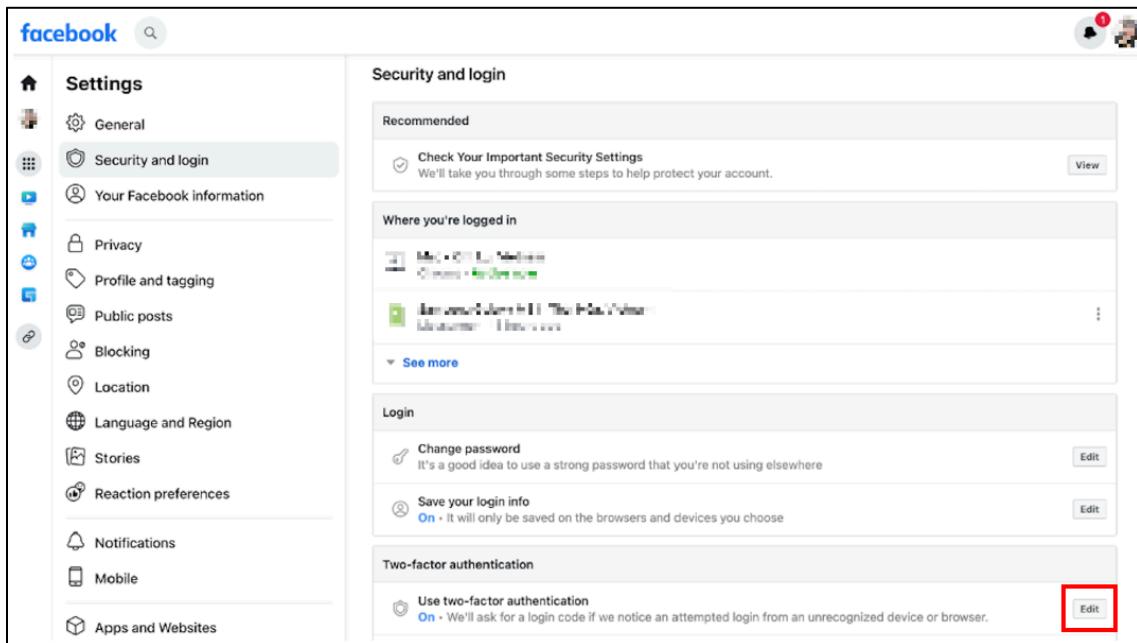
III.4. Two-factor authentication for Facebook

III.4.1. Register authentication key

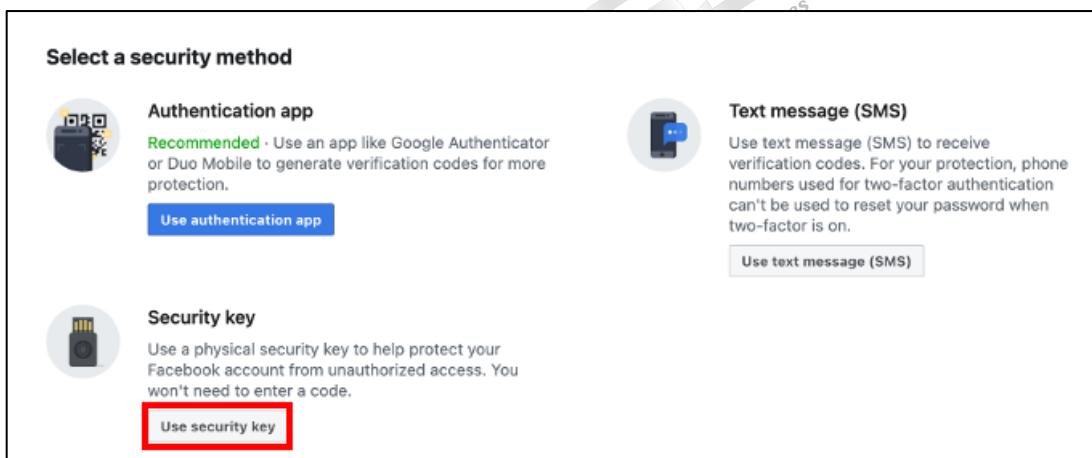
- Login Facebook account at <https://www.facebook.com>, select **Setting > Security and login** on the left menu.



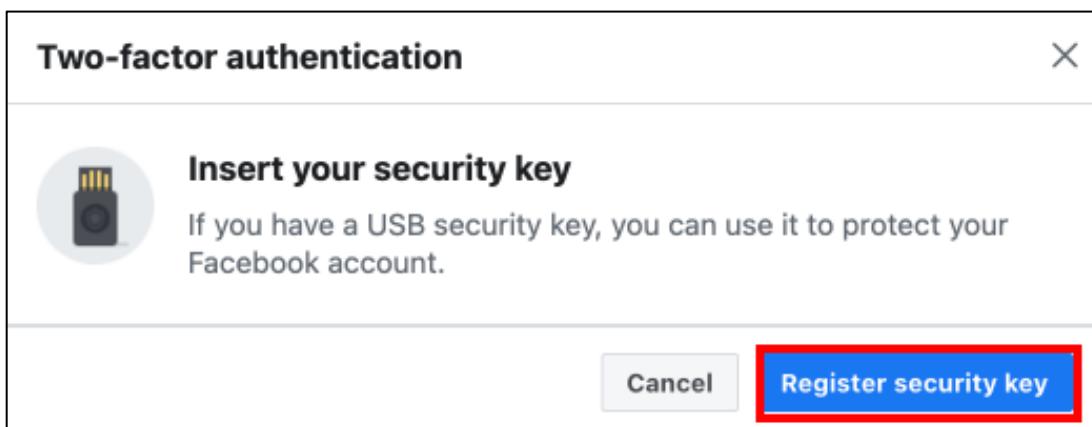
- Edit setting **Use two-factor authentication at Two-factor authentication.**



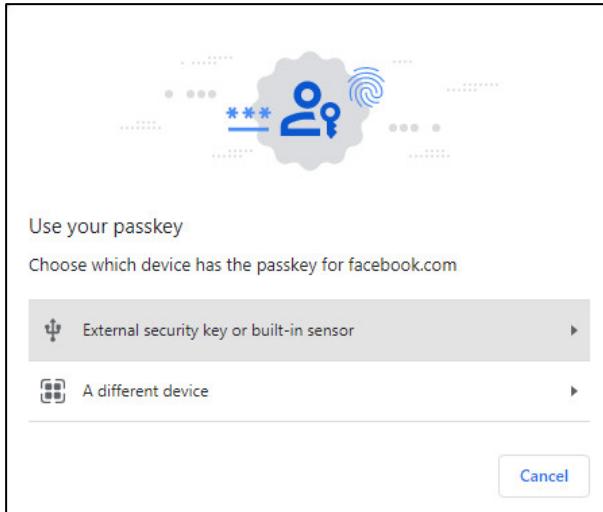
- In the **Select a security method > Use security key.**



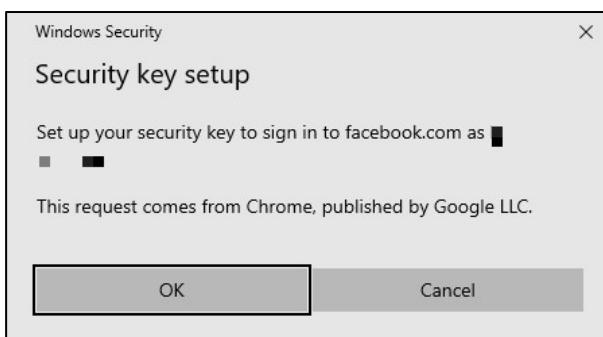
- In the **Two-factor authentication**, select **Register security key**.



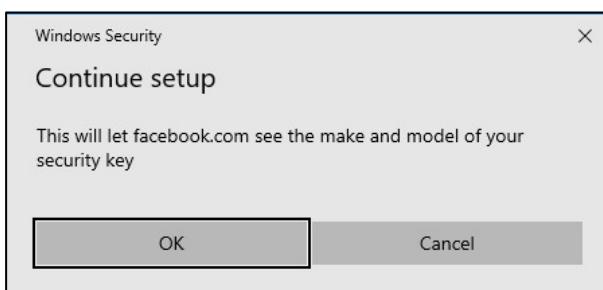
- Select **External security key or built-in sensor** to set up security key.



- To continue with the registration process, press **OK**.

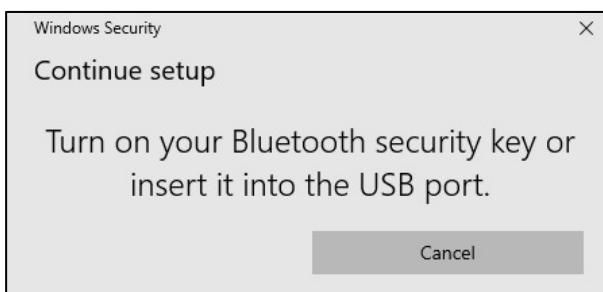


- Select **OK** to continue.

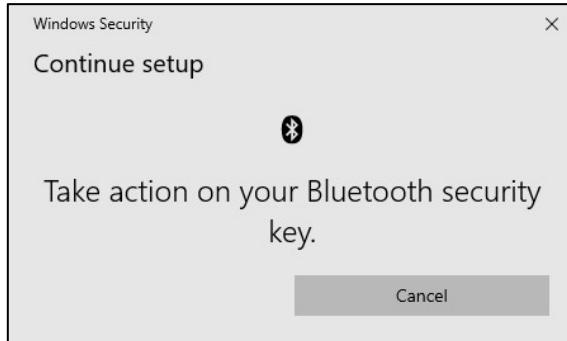


III.4.1.1. Using via Bluetooth

- Connect VinCSS FIDO2® Fingerprint to your computer via Bluetooth.

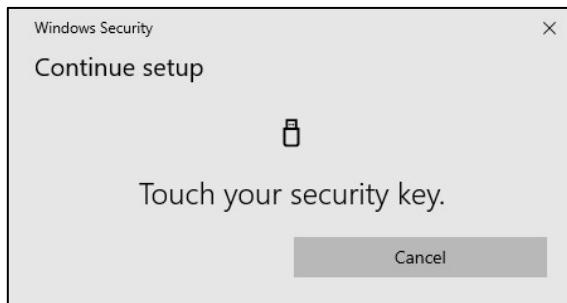


- Scan your fingerprint when receiving notification.



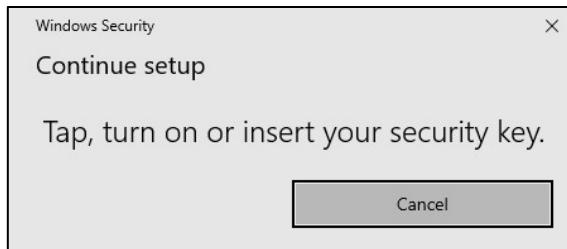
III.4.1.2. Using via USB

- Connect VinCSS FIDO2® Fingerprint to your computer via USB, touch the fingerprint scanner when receiving notification.

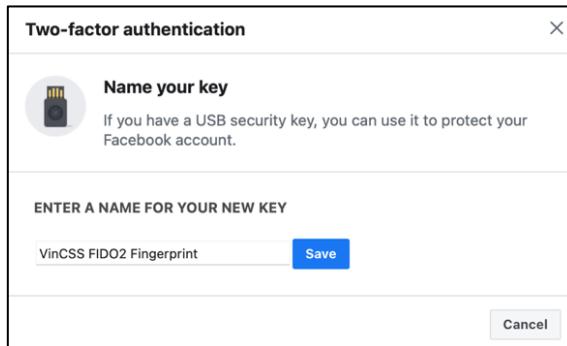


III.4.1.3. Using via NFC

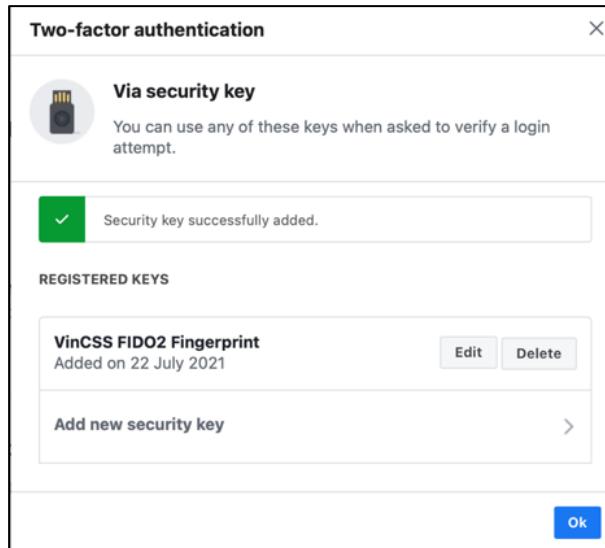
- Connect VinCSS FIDO2® Fingerprint to your computer via NFC, touch the fingerprint scanner when receiving notification.



- Name the security key to distinguish the key, then click **Save**.

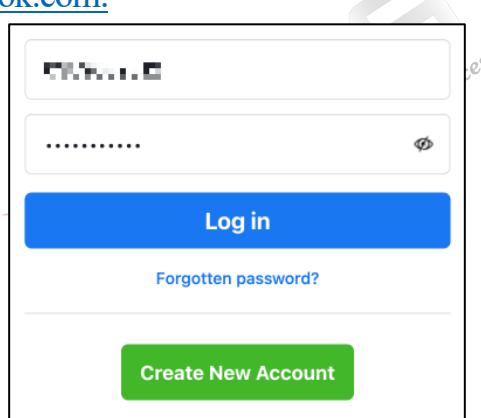


- The security key has been successfully registered.

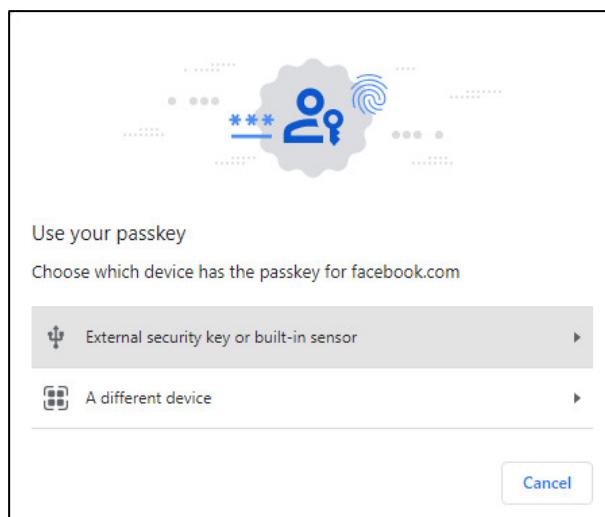


III.4.2. Two-factor authentication with Facebook account

- Log in Facebook account (*username and password*) at <https://www.facebook.com>.



- After that Facebook would request two-factor authentication by security key. Select **External security key or built-in sensor**.



III.4.2.1. Using via Bluetooth

- Connect VinCSS FIDO2® Fingerprint to computer via Bluetooth.



- Scan your fingerprint when receiving notification.



III.4.2.2. Using via USB

- Connect VinCSS FIDO2® Fingerprint to computer via USB, touch finger-print scanner on security key when receiving notification.

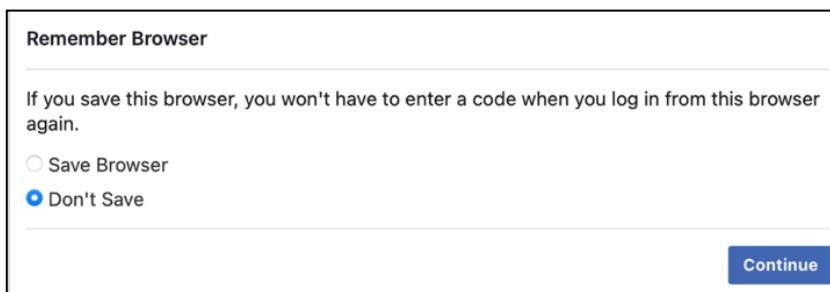


III.4.2.3. Using via NFC

- Connect VinCSS FIDO2® Fingerprint to computer via NFC, touch fingerprint scanner on security key when receiving notification.



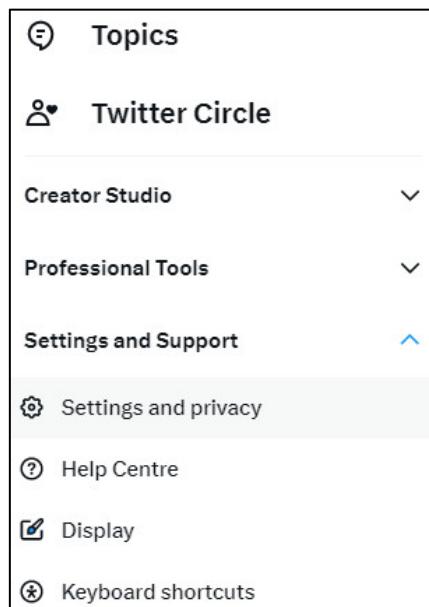
- Authenticate successfully. Select **Don't Save** and click **Next**.



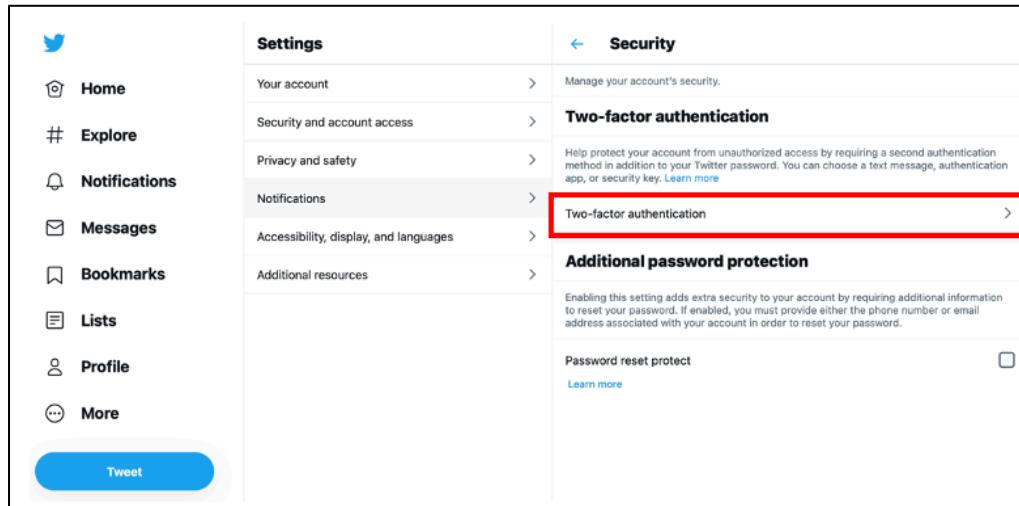
III.5. Two-factor with Twitter account

III.5.1. Register authentication key

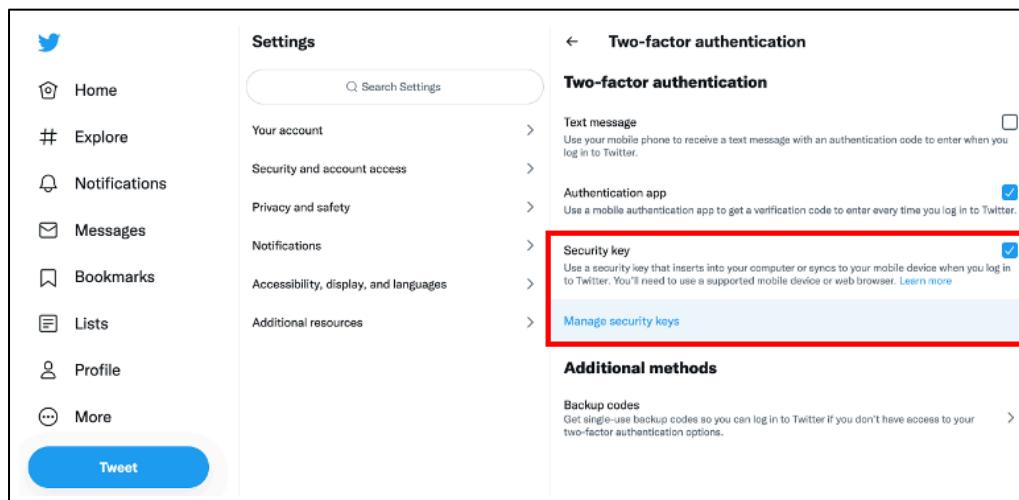
- Access <https://twitter.com>, select **More > Settings and Support > Settings and Privacy**.



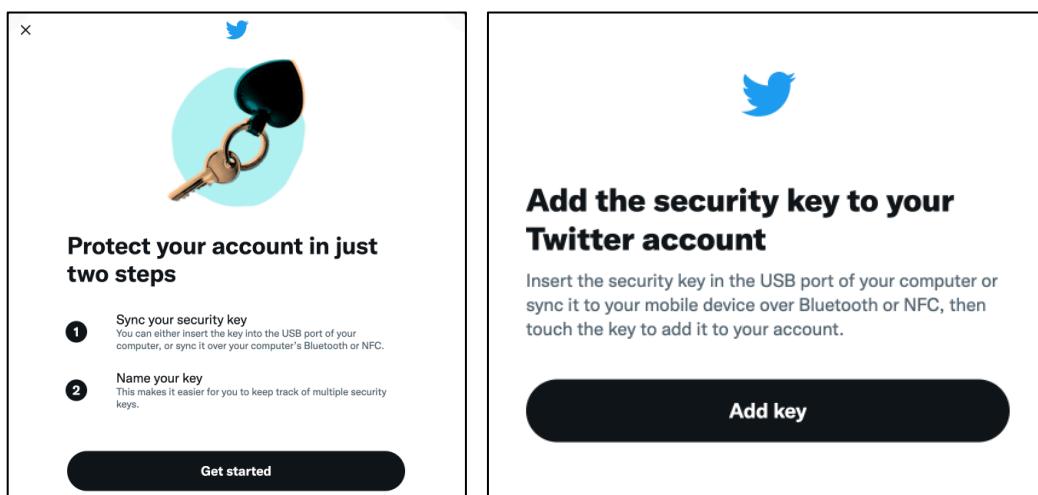
- Select Security and account access > Security> Two-factor authentication



- Select Security keys.



- At the notice board, select Get started > Add key to start the registration process.

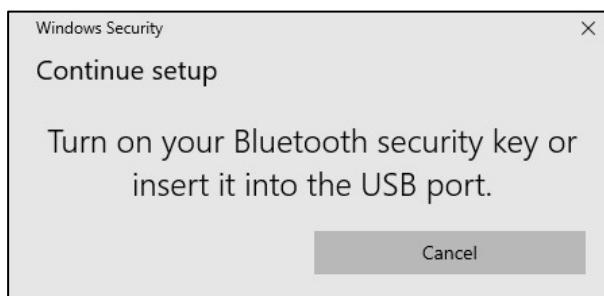


- Click **OK** to continue.

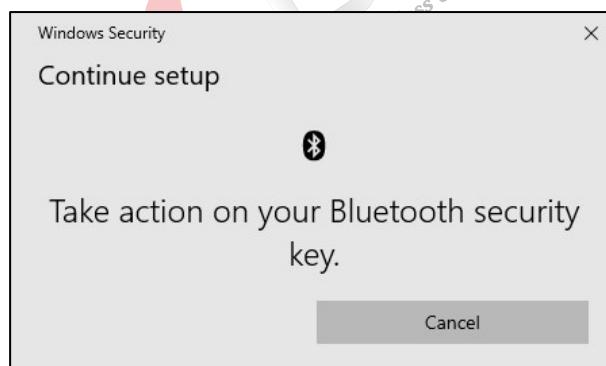


III.5.1.1. Using via Bluetooth

- Connect VinCSS FIDO2® Fingerprint to computer via Bluetooth.

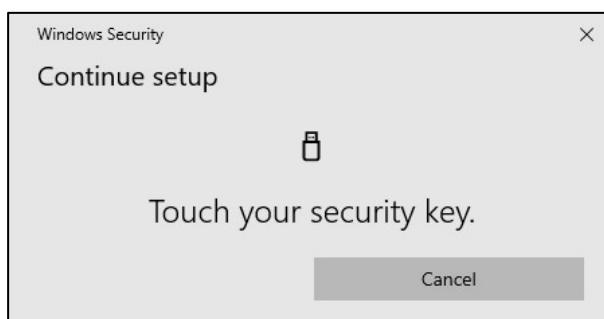


- Touch fingerprint scanner on security key when receiving notification.



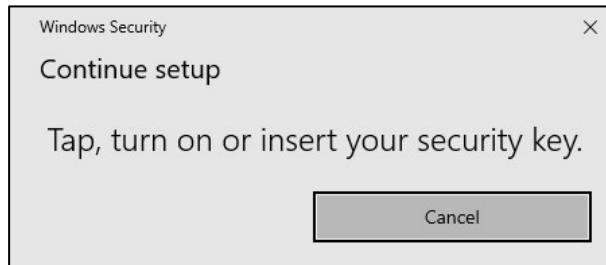
III.5.1.2. Using via USB

- Connect VinCSS FIDO2® Fingerprint to computer via USB, touch fingerprint scanner on security key when receiving notification.

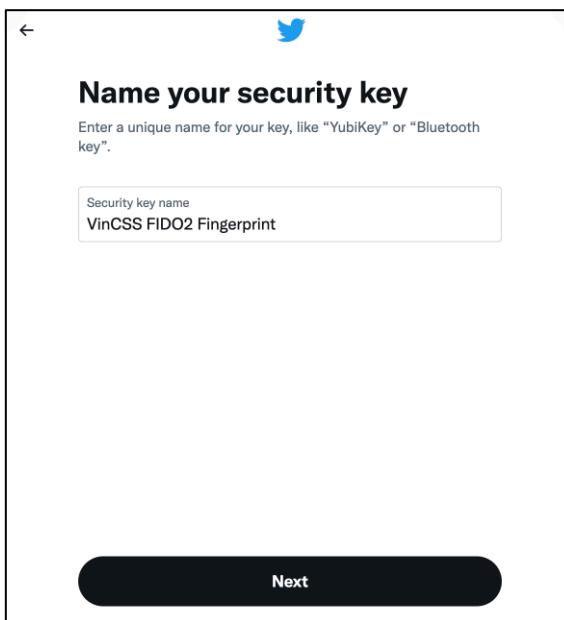


III.5.1.3. Using via NFC

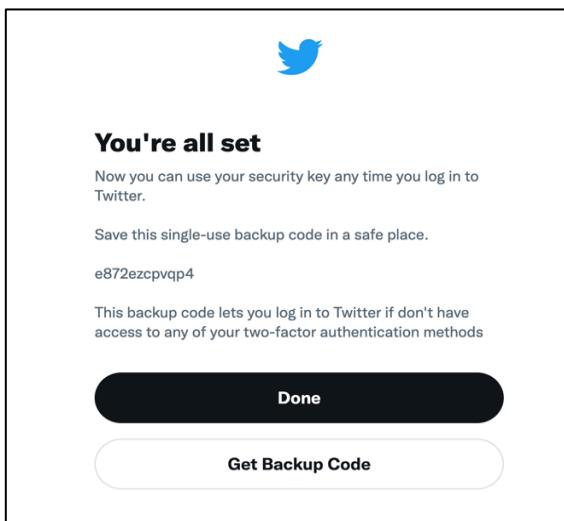
- Connect VinCSS FIDO2® Fingerprint to computer via NFC, touch security key to NFC reader when receiving notification.



- Name the security key to distinguish the key, then click **Next** to save the key information.

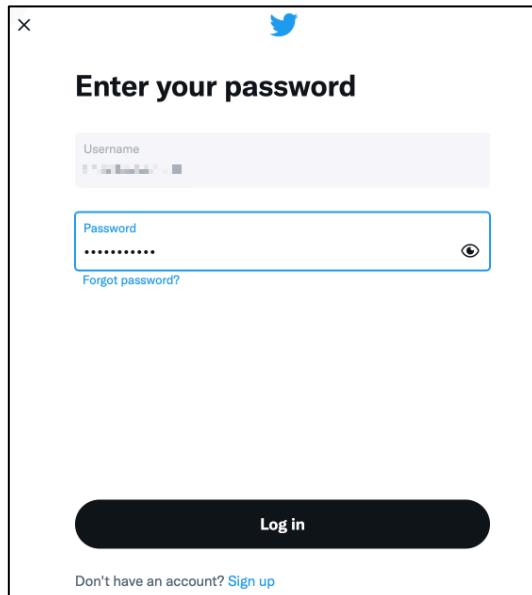


- Security key has been successfully registered. Click **Done** to complete.



III.5.2. Two-factor authentication with Twitter account

- Log in Twitter account at <https://www.twitter.com> by using username and password.



III.5.2.1. Using via Bluetooth

- Connect VinCSS FIDO2® Fingerprint to computer via Bluetooth.



- Scan the fingerprint when receiving notification.



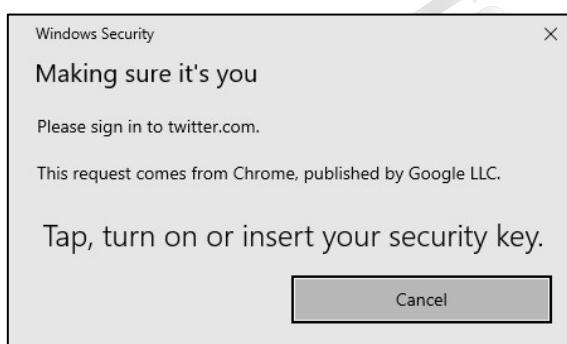
III.5.2.2. Using via USB

- Connect VinCSS FIDO2® Fingerprint to computer via USB, touch on the fingerprint sensor on security key when receiving notification.



III.5.2.3. Using via NFC

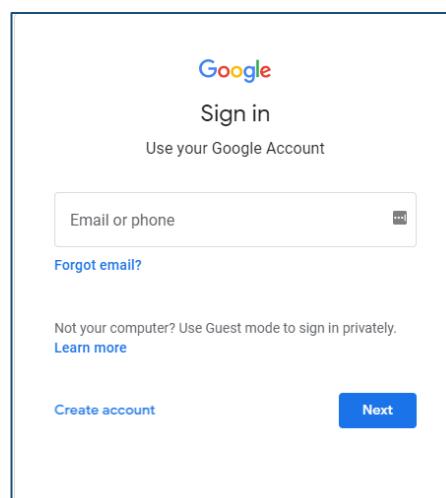
- Connect VinCSS FIDO2® Fingerprint to computer via USB, touch your security key to NFC reader when receiving notification.



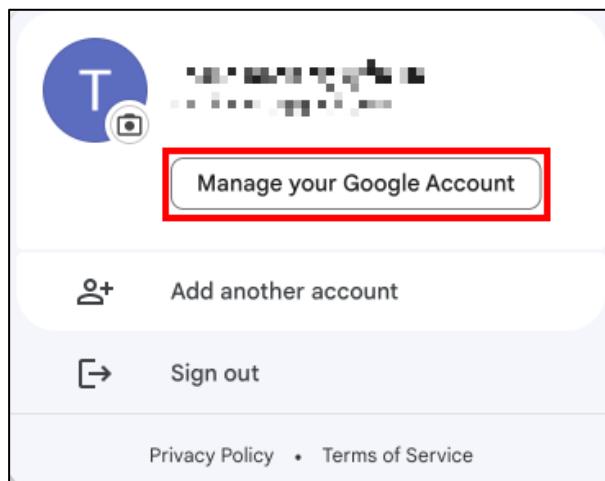
III.6. Two-factor authentication with Google account

III.6.1. Register authentication key

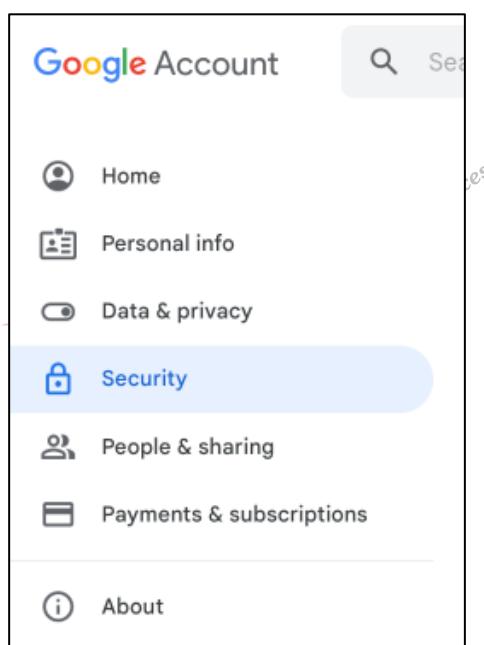
- Log in Google account with username and password at: <https://accounts.google.com>.



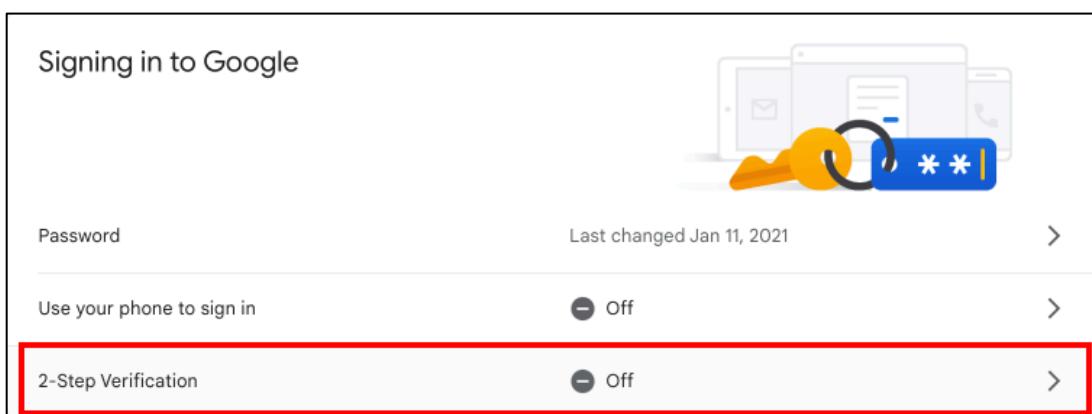
- Click on the account icon in right screen corner, select **Manage your Google Account**.



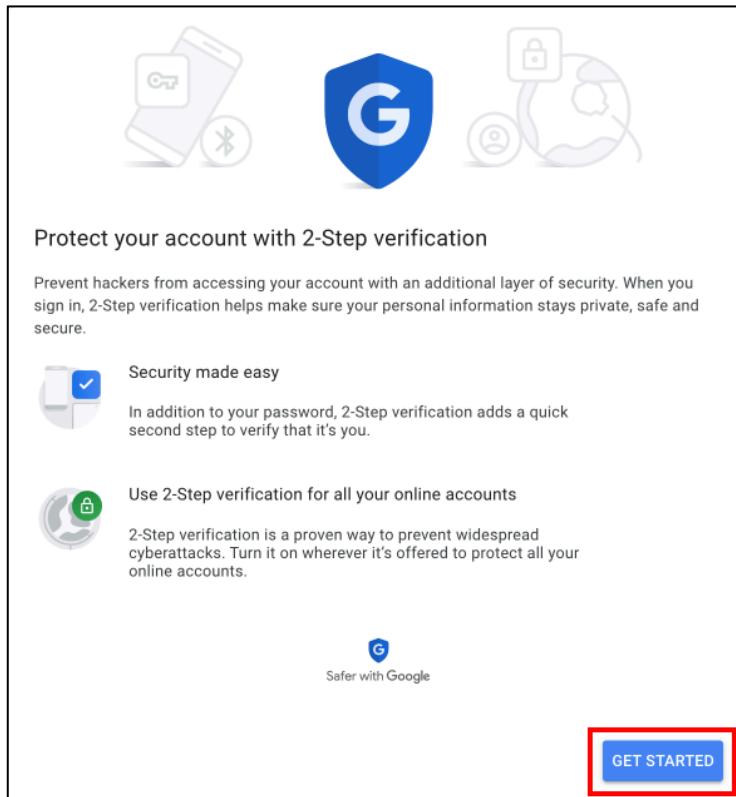
- Select **Security** on left menu.



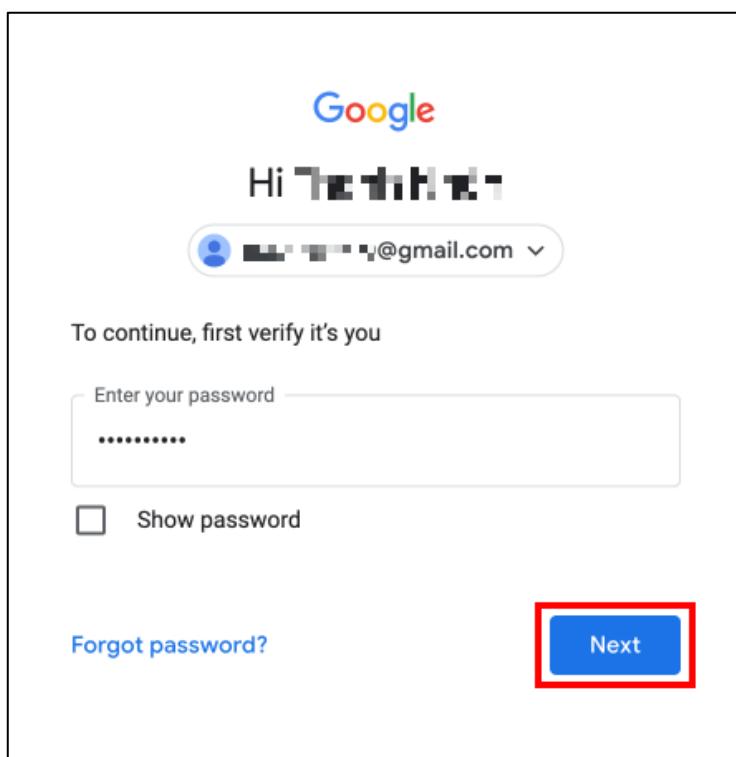
- Select **2-Step Verification** to set up two-factor authentication.



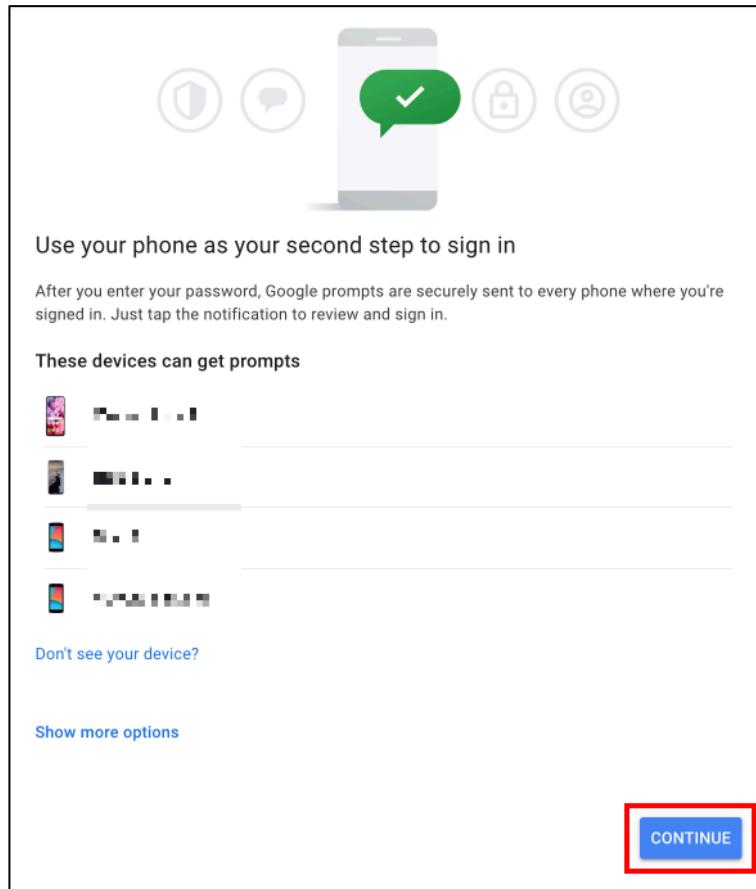
- In case you have not registered for 2-step authentication before, it is necessary to verify the user's identity before setting up the security key. Click **Get Started**.



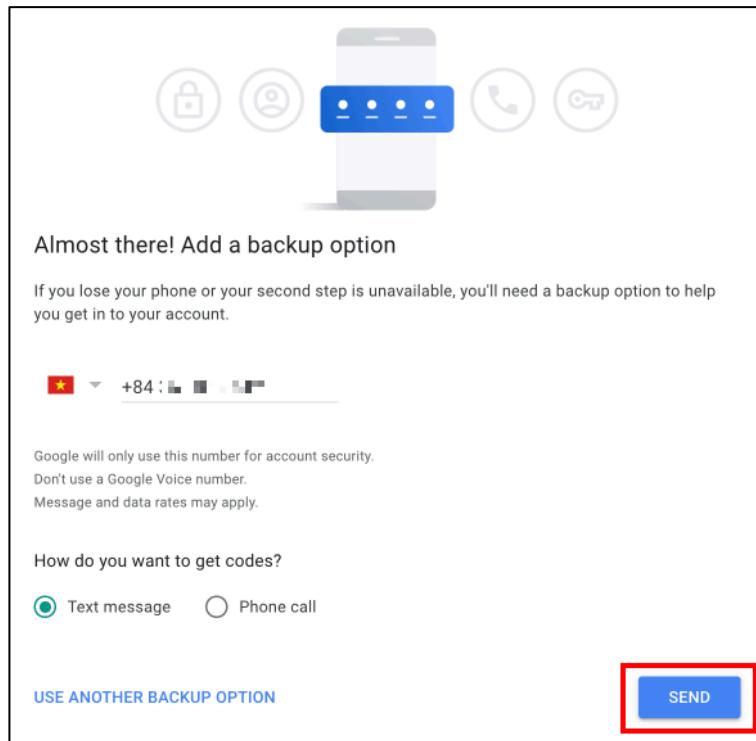
- Enter the password to verify your identity and click **Next**.



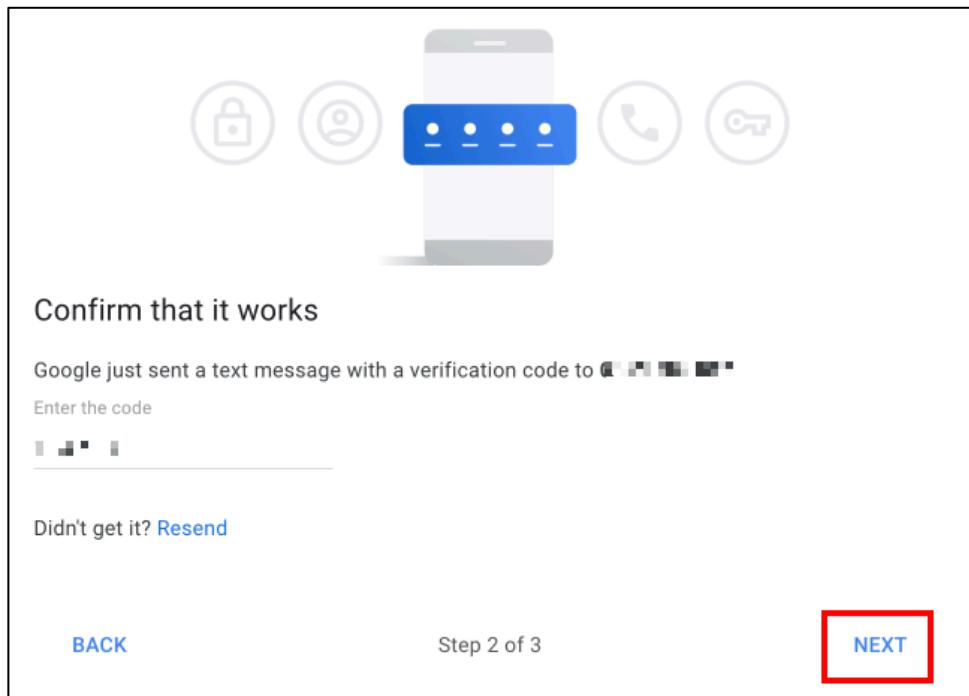
- Click **CONTINUE** to use the phone number as the 2nd step to log in.



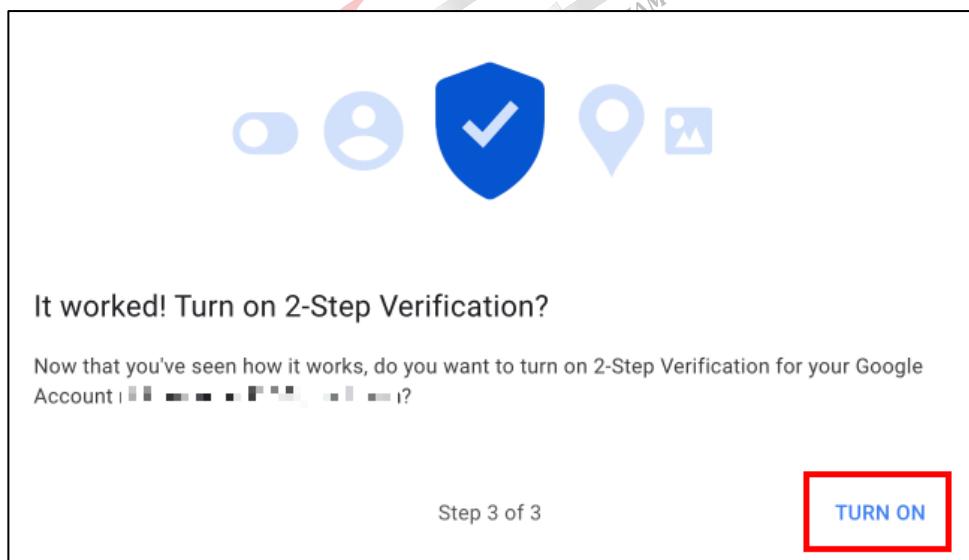
- Enter the phone number and choose how to receive the code and then select **Next** (*default received by text message*).



- Enter the confirmation code sent to the register phone number and then Select **Next**.



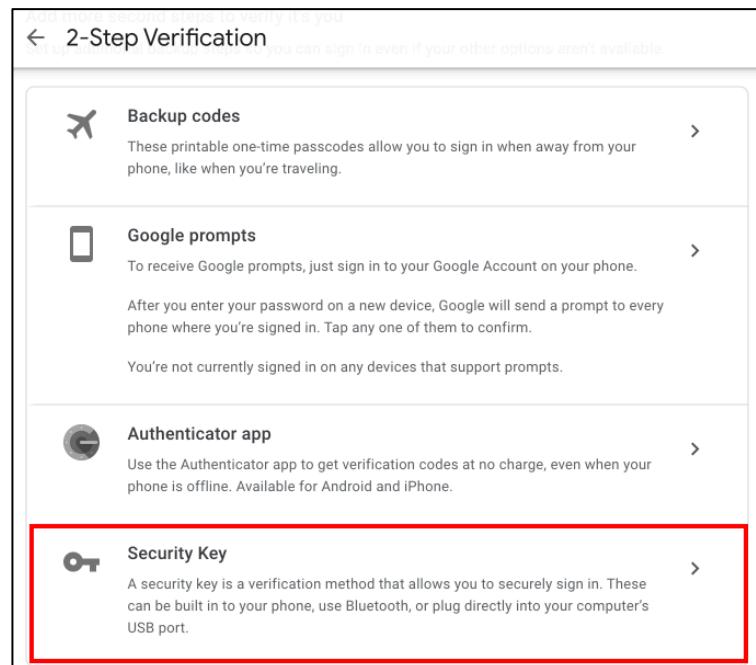
- Click **Turn on** to enable **2-Step Verification**.



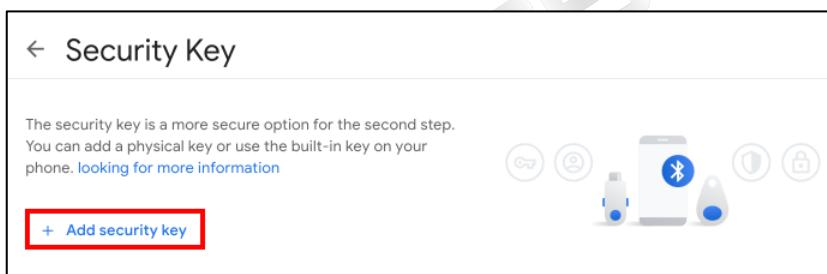
- Complete the verification step.



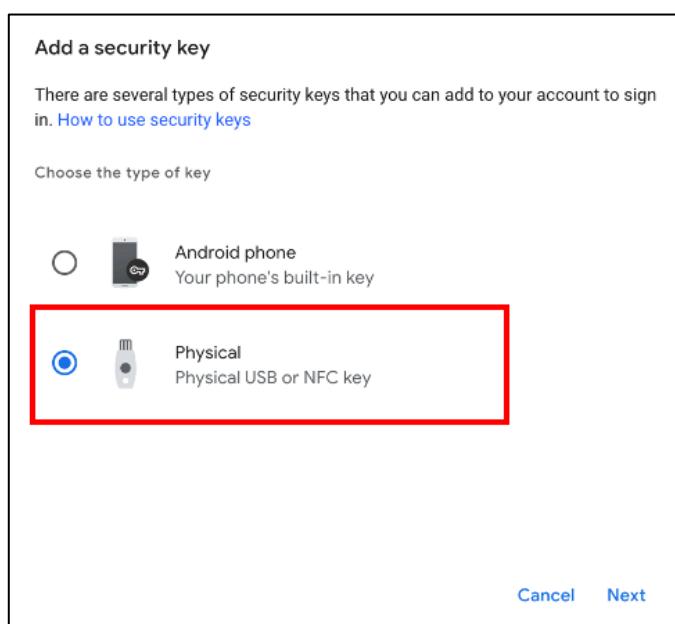
- In the 2-Step Verification, choose **Security Key**.



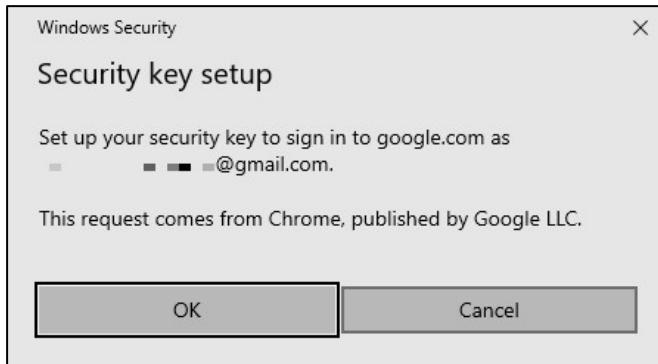
- Select **Add security key**.



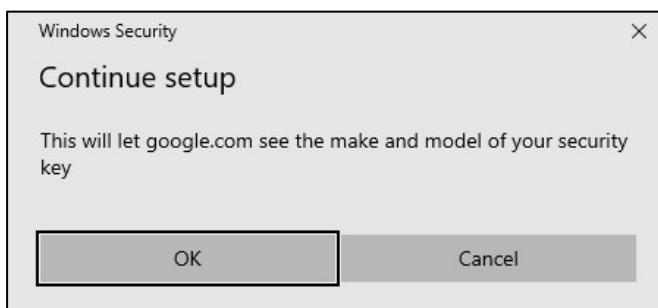
- Select **Physical** and click **Next** to add security key.



- Click **OK** to continue setting up the security key.

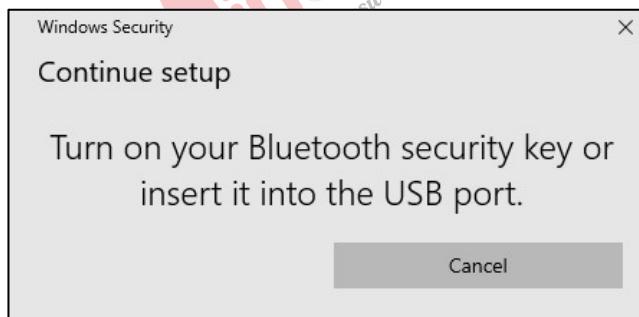


- Click **OK** to continue.

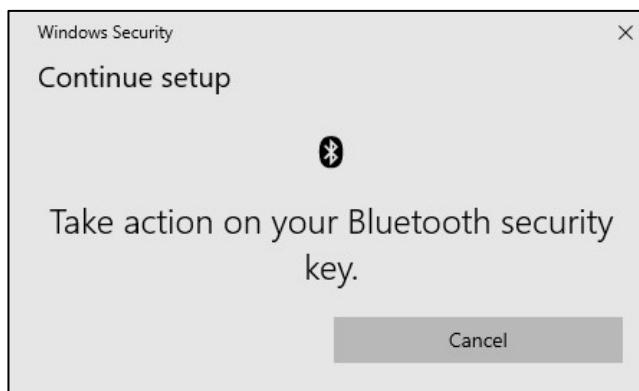


III.6.1.1. Using via Bluetooth

- Connect VinCSS FIDO2® Fingerprint to computer via Bluetooth.

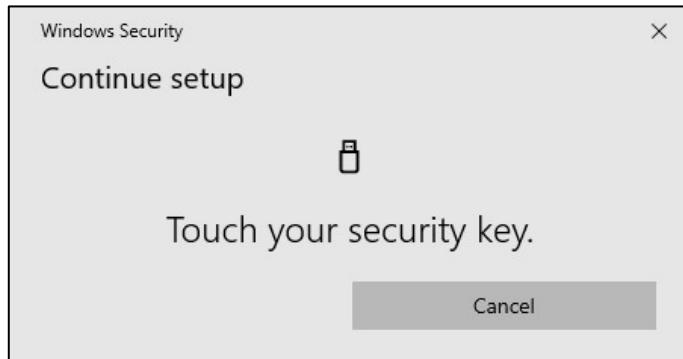


- Touch fingerprint scanner on security key when receiving notification.



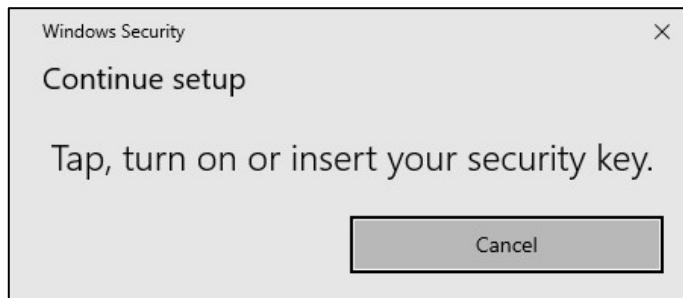
III.6.1.2. Using via USB

- Connect VinCSS FIDO2® Fingerprint to computer via USB, touch finger-print scanner on security key when receiving notification.

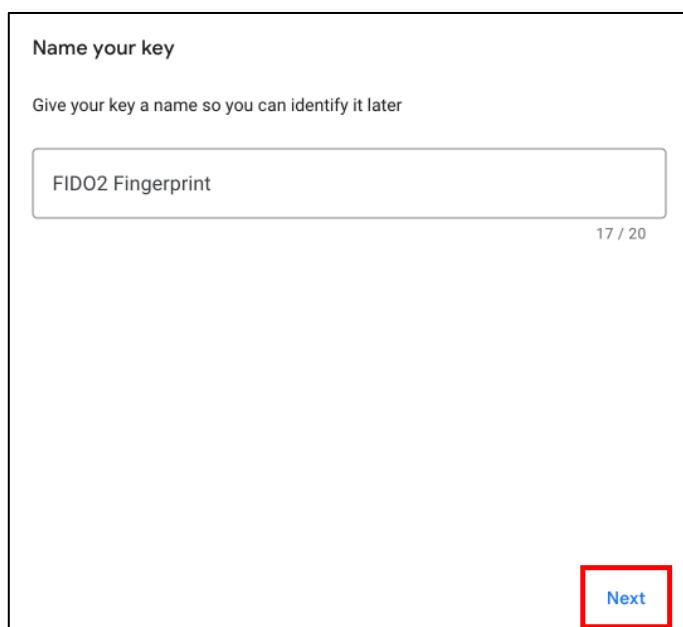


III.6.1.3. Using via NFC

- Connect VinCSS FIDO2® Fingerprint to computer via NFC, touch security key to NFC reader when receiving notification.

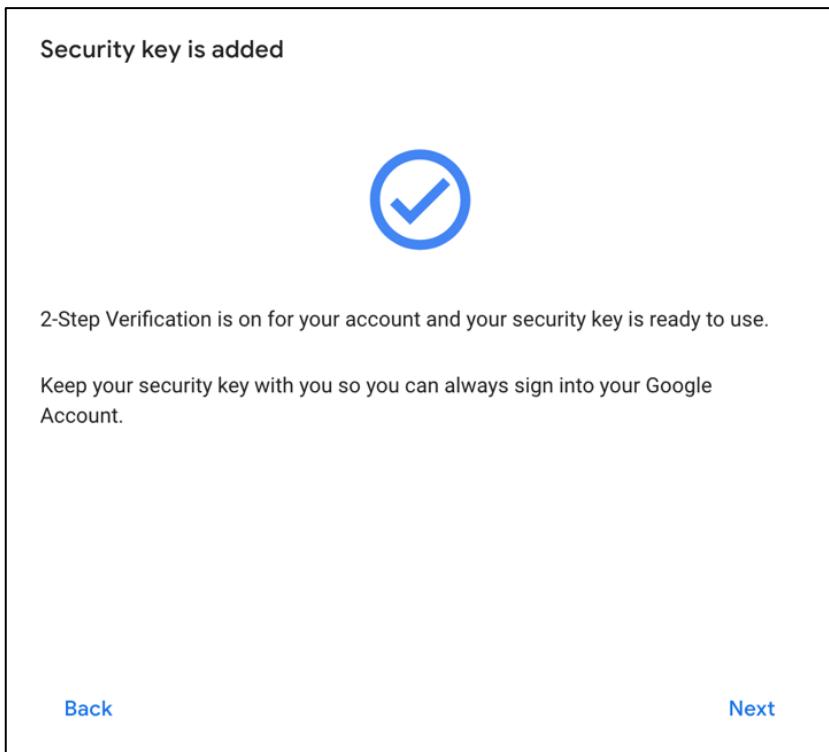


- Name the security key device to distinguish between keys (*up to 20 characters*), and click **Next** to confirm.

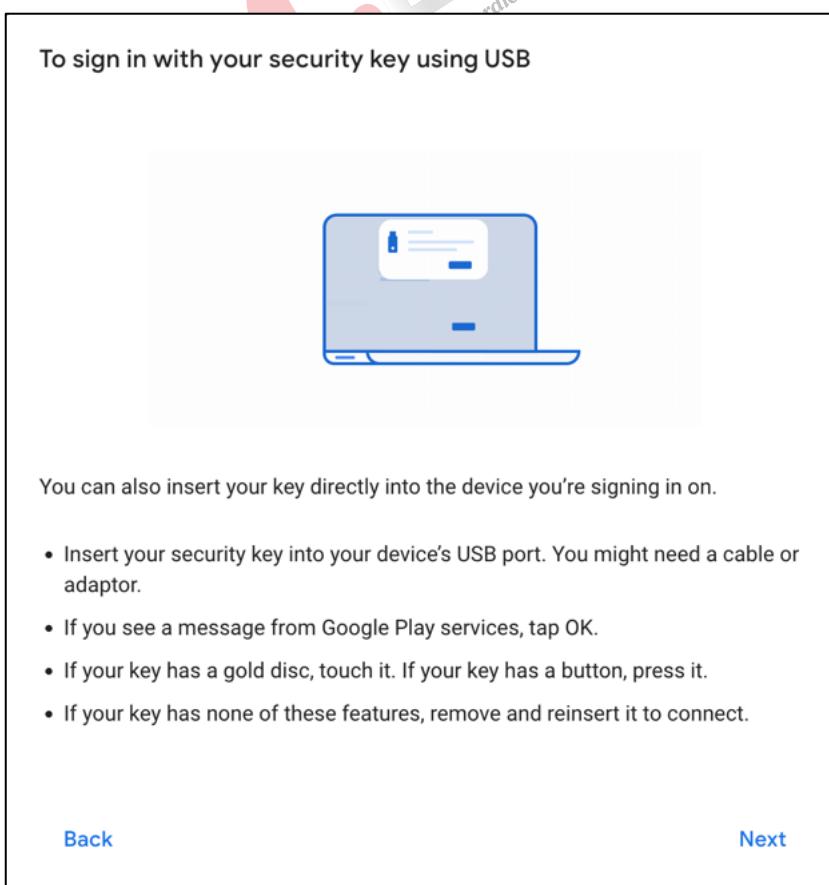


A screenshot of a "Name your key" dialog box. It asks "Give your key a name so you can identify it later" and has a text input field containing "FIDO2 Fingerprint". A character counter "17 / 20" is shown below the input field. A red box highlights the "Next" button at the bottom right.

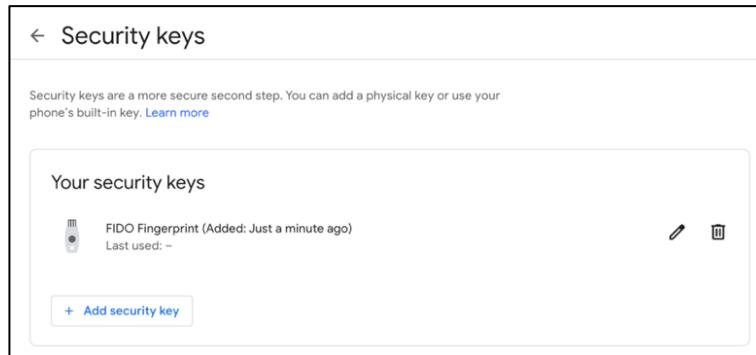
- Select **Next** to complete the security key registration process .



- Select **Next** to complete the registration. After that, all of Google services will require to authenticate with password and security key when user logins.

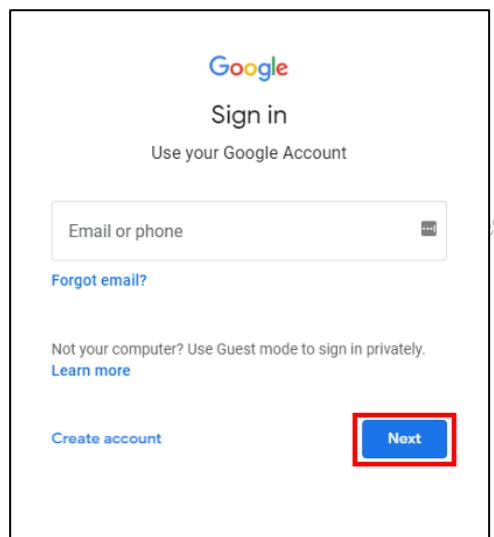


- Sign up successfully.



III.6.2. Two-factor authentication with Google account

- Log in Google account with username and password at <https://accounts.google.com>.



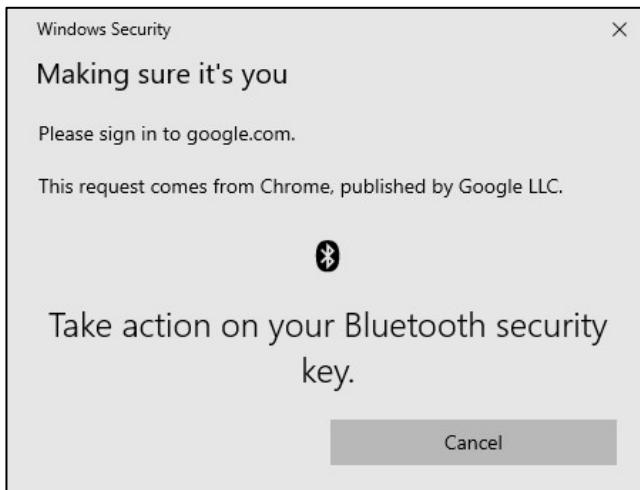
- After authenticating with password, user must authenticate with security key.

III.6.2.1. Using via Bluetooth

- Connect VinCSS FIDO2® Fingerprint to computer via Bluetooth.



- Touch the fingerprint sensor on the security key when receiving notification.



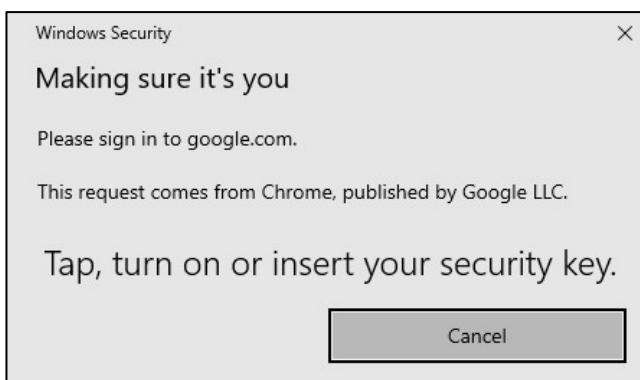
III.6.2.2. Using via USB

- Connect VinCSS FIDO2® Fingerprint to computer via USB. Touch the fingerprint sensor on the security key when receiving notification.

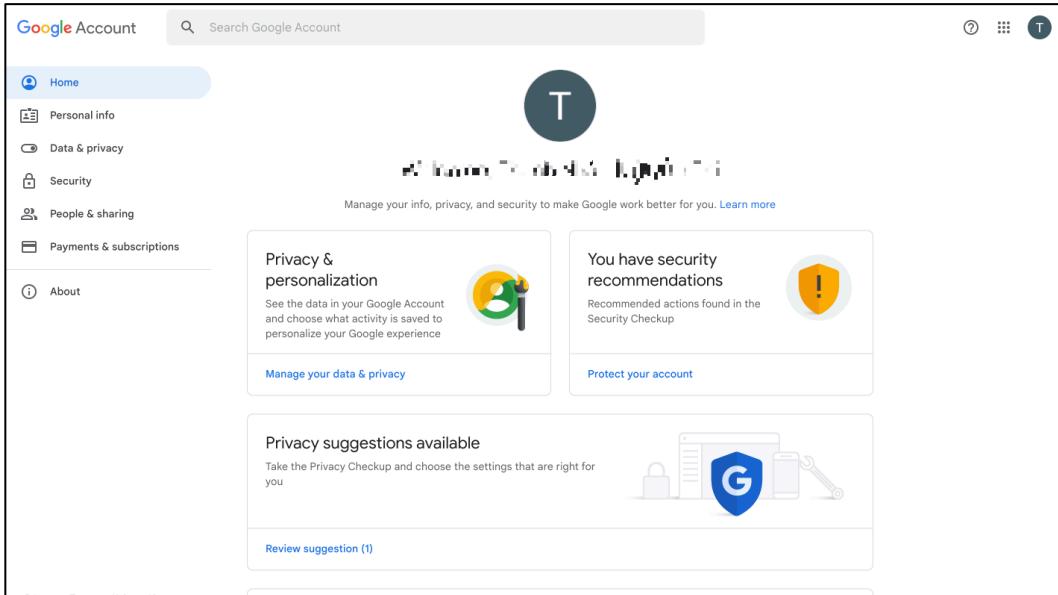


III.6.2.3. Using via NFC

- Connect VinCSS FIDO2® Fingerprint to computer via NFC, touch the security key to NFC reader when receiving notification.



- Log in successfully, user can use Google services.



The screenshot shows the Google Account settings page. On the left, there's a sidebar with links: Home (selected), Personal info, Data & privacy, Security, People & sharing, Payments & subscriptions, and About. The main area has a large circular profile picture placeholder with a 'T'. Below it, there are two main sections: 'Privacy & personalization' and 'You have security recommendations'. The 'Privacy & personalization' section includes a link to 'Manage your data & privacy'. The 'You have security recommendations' section includes a link to 'Protect your account'. At the bottom, there's a section titled 'Privacy suggestions available' with a link to 'Review suggestion (1)'. The background features a watermark for 'VinCSS Passwordless & IAM Services'.

REFERENCES

- VinCSS FIDO2 Ecosystem: <https://passwordless.vincss.net/>
- VinCSS Youtube channel:
https://www.youtube.com/channel/UCNtS_7d4GtyecE2HCpJSr7g
- FAQs: <https://passwordless.vincss.net/en/support>
- VinCSS OVPN Client guide:
<https://github.com/VinCSS-Public-Projects/FIDO2-Public-Documents/tree/main/VinCSS-OVPN-Client>

