

# HƯỚNG DẪN SỬ DỤNG VINCSS FIDO2<sup>®</sup> FINGERPRINT CHO WINDOWS/macOS

**Ngày:** 15/07/2021

**Số hiệu:** CSS-IP-PUB-FIDO2-210715-020

**Phiên bản:** 1.0

**Phân loại tài liệu:** Tài liệu công bố

**Thực hiện:** Trung tâm Sản phẩm, VinCSS

**CÔNG TY TNHH DỊCH VỤ AN NINH MẠNG VINCSS**

Số 7 Đường Bằng Lăng 1, Khu đô thị sinh thái Vinhomes Riverside, Phường Việt Hưng,  
Quận Long Biên, Thành phố Hà Nội.

## THEO DÕI PHIÊN BẢN

Phiên bản	Ngày	Người thực hiện	Vị trí	Liên hệ	Ghi chú
1.0	15/07/2021				Khởi tạo tài liệu



# MỤC LỤC

<b>THEO DÕI PHIÊN BẢN .....</b>	<b>2</b>
<b>MỤC LỤC .....</b>	<b>3</b>
<b>I. THÔNG TIN SẢN PHẨM .....</b>	<b>5</b>
<b>I.1. Thông tin chung.....</b>	<b>5</b>
<b>I.2. Ý nghĩa của các đèn hiệu .....</b>	<b>6</b>
<b>II. QUẢN LÝ MÃ PIN VÀ VÂN TAY .....</b>	<b>6</b>
<b>II.1. Nền tảng Windows.....</b>	<b>7</b>
II.1.1. Kết nối với máy tính.....	7
III.1.1.1. Sử dụng qua kết nối USB .....	7
III.1.1.2. Sử dụng qua kết nối NFC .....	7
III.1.1.3. Sử dụng qua kết nối Bluetooth .....	7
II.1.2. Tạo mã PIN mới .....	9
II.1.3. Thay đổi mã PIN .....	11
II.1.4. Thêm vân tay .....	13
II.1.5. Xóa vân tay.....	15
II.1.6. Thiết lập cài đặt gốc .....	16
<b>II.2. Nền tảng macOS .....</b>	<b>19</b>
II.2.1. Kết nối với máy tính.....	19
II.2.2. Tạo mới mã PIN .....	19
II.2.3. Thay đổi mã PIN .....	20
II.2.4. Thêm vân tay .....	21
II.2.5. Xóa vân tay.....	23
II.2.6. Quản lý dữ liệu đăng nhập .....	24
II.2.7. Thiết lập cài đặt gốc .....	25
<b>III. XÁC THỰC KHÔNG MẬT KHẨU VỚI VINCSS FIDO2® FINGERPRINT .....</b>	<b>26</b>
<b>III.1. Windows 10 .....</b>	<b>26</b>
III.1.1. Cấu hình trên hệ thống Azure AD.....	26
III.1.1.1. Cấu hình Azure AD .....	26
III.1.1.2. Đăng nhập Windows 10 sử dụng FIDO2 với provisioning packages .....	27
III.1.1.3. Đăng ký khóa xác thực cho tài khoản Azure AD .....	28
III.1.1.4. Kết nối User vào Azure Work Account.....	35
III.1.2. Đăng nhập Windows 10 .....	37
III.1.2.1. Sử dụng qua kết nối Bluetooth .....	38
III.1.2.2. Sử dụng qua kết nối USB .....	38
III.1.2.3. Sử dụng qua kết nối NFC .....	39
<b>III.2. Tài khoản Microsoft.....</b>	<b>40</b>
III.2.1. Đăng ký khóa bảo mật.....	40
III.2.2. Đăng nhập .....	40
III.2.2.1. Sử dụng qua kết nối Bluetooth .....	40

III.2.2.2.	Sử dụng qua kết nối USB .....	41
III.2.2.3.	Sử dụng qua kết nối NFC .....	41
<b>III.3.</b>	<b>VinCSS OVPN Client.....</b>	<b>42</b>
III.3.1.	Sử dụng qua kết nối Bluetooth.....	43
III.3.2.	Sử dụng qua kết nối USB.....	43
III.3.3.	Sử dụng qua kết nối NFC.....	44
<b>III.4.</b>	<b>Xác thực 2 yếu tố tài khoản Facebook.....</b>	<b>45</b>
III.4.1.	Đăng ký khoá bảo mật.....	45
III.4.1.1.	Sử dụng qua kết nối Bluetooth. ....	46
III.4.1.2.	Sử dụng qua kết nối USB .....	47
III.4.1.3.	Sử dụng qua kết nối NFC .....	47
III.4.2.	Xác thực 2 yếu tố với dịch vụ Facebook.....	48
III.4.2.1.	Sử dụng qua kết nối Bluetooth. ....	48
III.4.2.2.	Sử dụng qua kết nối USB .....	49
III.4.2.3.	Sử dụng qua kết nối NFC .....	49
<b>III.5.</b>	<b>Xác thực 2 yếu tố với Twitter .....</b>	<b>50</b>
III.5.1.	Đăng ký khoá bảo mật.....	50
III.5.1.1.	Sử dụng qua kết nối Bluetooth. ....	51
III.5.1.2.	Sử dụng qua kết nối USB .....	51
III.5.1.3.	Sử dụng qua kết nối NFC .....	51
III.5.2.	Xác thực 2 yếu tố với dịch vụ Twitter.....	52
III.5.2.1.	Sử dụng qua kết nối Bluetooth. ....	53
III.5.2.2.	Sử dụng qua kết nối USB .....	54
III.5.2.3.	Sử dụng qua kết nối NFC .....	54
<b>III.6.</b>	<b>Xác thực 2 yếu tố với Google .....</b>	<b>54</b>
III.6.1.	Đăng ký khoá bảo mật.....	54
III.6.1.1.	Sử dụng qua kết nối USB .....	57
III.6.1.2.	Sử dụng qua kết nối NFC .....	57
III.6.2.	Xác thực 2 yếu tố với dịch vụ Google.....	58
III.6.2.1.	Sử dụng qua kết nối USB .....	58
III.6.2.2.	Sử dụng qua kết nối NFC .....	59

## I. THÔNG TIN SẢN PHẨM



Hình ảnh VinCSS FIDO2® Fingerprint

### I.1. Thông tin chung

Thông tin	Chi tiết
Tên sản phẩm	VinCSS FIDO2® Fingerprint
USB	USB Type-C
Bluetooth	Bluetooth Low Energy 4.0
NFC	ISO7816/ISO14443
Hệ điều hành hỗ trợ	Windows, MacOS, Linux, Android, iOS
Tiêu chuẩn xác thực	Passwordless, Strong Two Factor, Strong Multi-Factor
Chứng chỉ	FIDO2 Certified
Giao thức hỗ trợ	WebAuthn, FIDO2 CTAP1, FIDO2 CTAP2, Universal 2nd Factor (U2F)
Trình duyệt hỗ trợ	Google Chrome, Mozilla Firefox, Apple Safari, Microsoft Edge, Microsoft Edge Chromium
Thuật toán mã hóa	ECC p256
Kiến trúc CPU	32-bit ARM® Cortex™-M4
Số lượng tài khoản có thể lưu	50
Số lượng vân tay có thể lưu	5
Đèn LED báo hiệu	RGB Led
Độ phân giải cảm biến	508 dpi
Tỉ lệ chấp nhận sai FAR	<0.0002%
Cân nặng	

Thông tin	Chi tiết
Kích thước sản phẩm	
Dung lượng/Loại pin	25mA, Lithium-ion Battery
Thời lượng pin	5-7 days
Nguồn điện sử dụng	5V/1A
Nhiệt độ hoạt động	-10°C ~ 60°C

## I.2. Ý nghĩa của các đèn hiệu

Đèn hiệu của VinCSS FIDO® Fingerprint sẽ cho người dùng biết trạng thái hiện tại của pin, trạng thái đang sạc pin, hoặc chế độ hoạt động.

Tín hiệu	Ý nghĩa	Trạng thái
Nháy đèn đỏ ba lần liên tiếp	Sắp hết pin, cần sạc	Đang sử dụng Bluetooth hoặc NFC.
Đèn bật màu hổ phách	Khoá đang được sạc	Đang kết nối với USB
Đèn bật màu xanh lá cây	Khoá đã sạc đầy	Đang kết nối với USB
Đèn bật màu xanh nước biển	Bật chế độ Bluetooth, và khoá đã được kết nối với một thiết bị Bluetooth	Đang sử dụng Bluetooth
Đèn nháy sáng màu xanh nước biển	Khoá bảo mật vào chế độ ghép nối	Đang sử dụng Bluetooth
Đèn bật màu tím	Đã kích hoạt NFC	Đang sử dụng NFC
Nhấp nháy nhanh với đèn màu trắng	Khoá bảo mật đang trong quá trình xử lý và yêu cầu người dùng tương tác.	Yêu cầu người dùng xác nhận bằng cách chạm vào cảm biến vân tay

## II. QUẢN LÝ MÃ PIN VÀ VÂN TAY

Việc đặt mã PIN cho VinCSS FIDO2® Fingerprint là yêu cầu bắt buộc để có thể thêm/xóa vân tay, nhằm đảm bảo an toàn cho thiết bị, tránh trường hợp thêm vân tay trái phép, thử vân tay quá nhiều lần hoặc xóa vân tay từ người lạ. Trường hợp người dùng cần tạo mới, thay đổi mã PIN/vân tay hoặc reset thiết bị VinCSS FIDO2® Fingerprint thì có thể thực hiện theo các bước dưới đây.

## II.1. Nền tảng Windows

### II.1.1. Kết nối với máy tính

#### II.1.1.1. Sử dụng qua kết nối USB

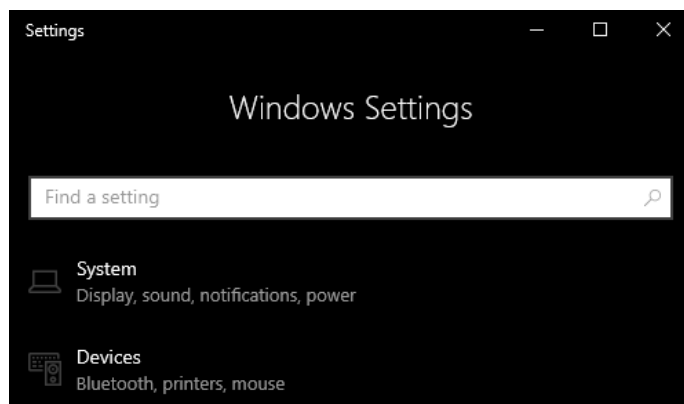
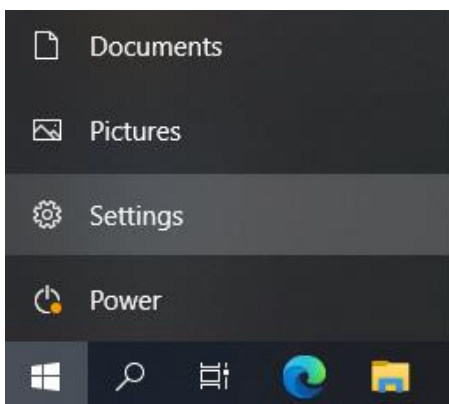
Tiến hành kết nối khoá bảo mật VinCSS FIDO2® Fingerprint vào máy tính thông qua dây USB, đảm bảo rằng khoá bảo mật đang **không** trong chế độ Bluetooth hoặc NFC. Nếu đèn LED nhấp đỏ 3 lần liên tiếp cho biết mức pin đang ở dưới 20%, đèn LED màu hồng phách cho biết khoá bảo mật đang được sạc, đèn LED màu xanh lá cây cho biết pin đã được sạc đầy. Khoá bảo mật VinCSS FIDO2® Fingerprint có thể được sử dụng khi đang sạc.

#### II.1.1.2. Sử dụng qua kết nối NFC

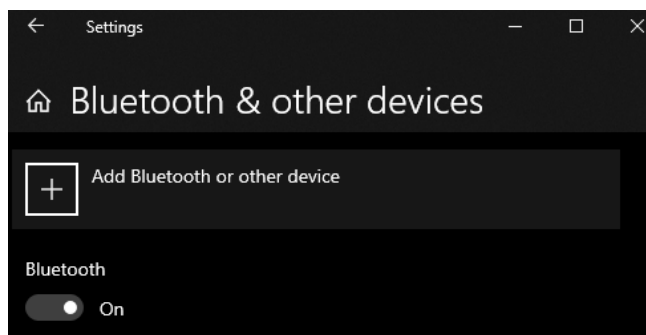
Tiến hành đặt khoá bảo mật VinCSS FIDO2® Fingerprint lên đầu đọc NFC. Khi đèn LED màu tím, có thể sử dụng tính năng NFC.

#### II.1.1.3. Sử dụng qua kết nối Bluetooth

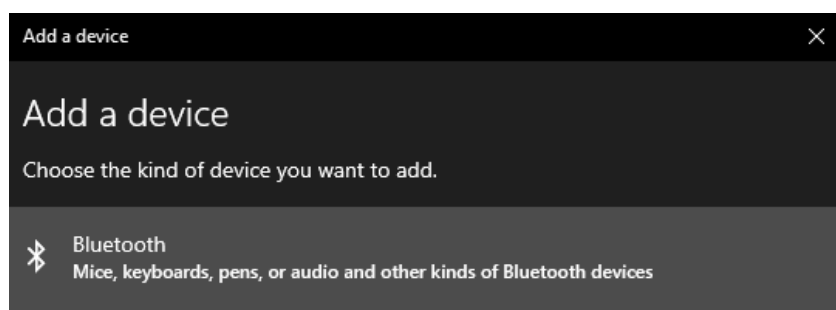
- Tại trạng thái tắt (không có đèn sáng), chuyển khoá bảo mật VinCSS FIDO2® Fingerprint vào chế độ kết nối Bluetooth bằng cách giữ cảm biến vân tay trong 2 giây. Khi đèn LED chuyển sang màu xanh lá, có thể sử dụng tính năng Bluetooth.
- Nếu đèn LED xanh lục không nhấp nháy, thực hiện giữ cảm biến vân tay trong vòng 4 giây để chuyển sang chế độ ghép đôi.
- Truy cập **Windows > Settings > Devices > Bluetooth & other devices**.



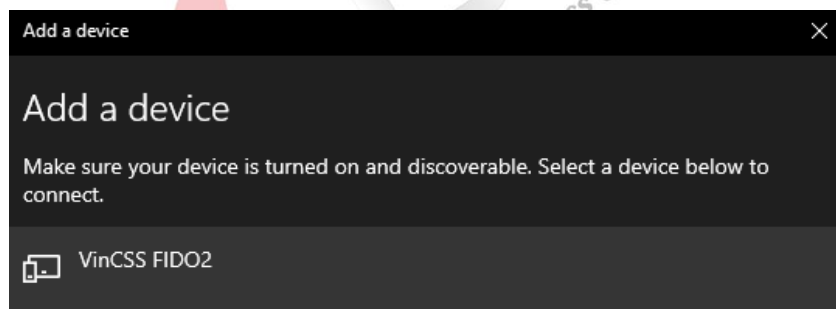
- Tại mục **Bluetooth** chọn **On**, sau đó chọn **Add Bluetooth or other device**.



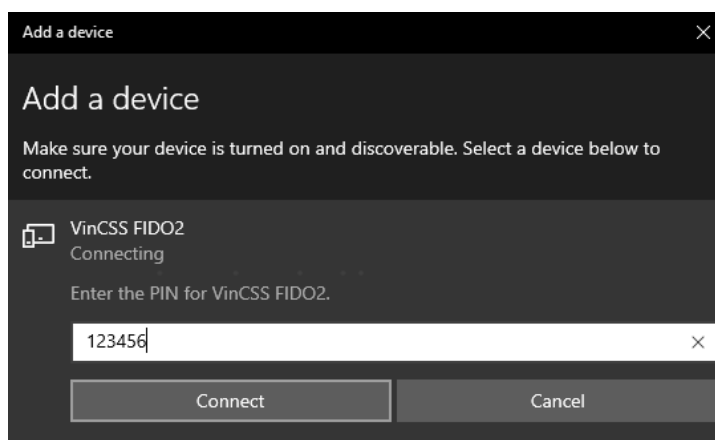
- Tại mục **Add a device**, chọn **Bluetooth**.



- Chọn thiết bị có tên **VinCSS FIDO2**.

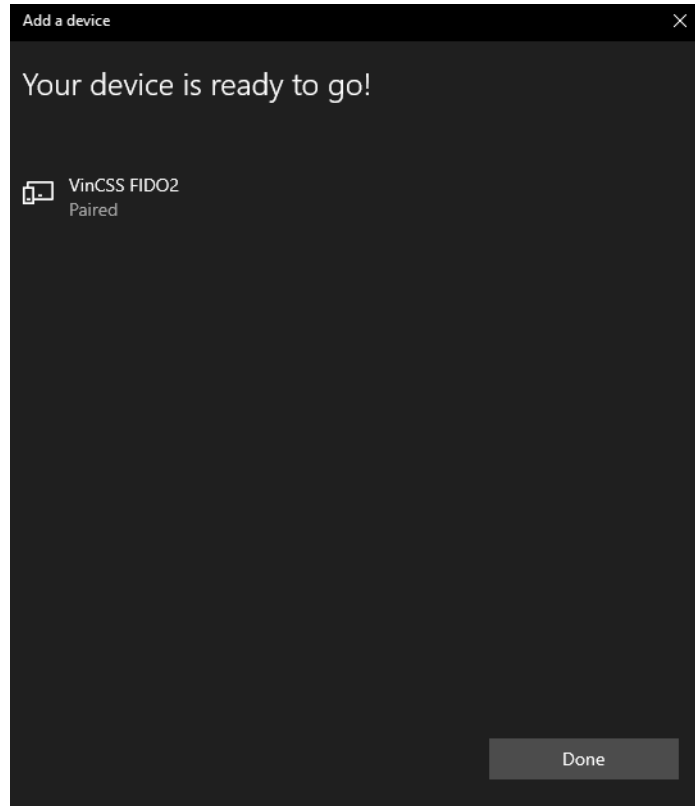


- Nhập mã ghép đôi để kết nối (Mã ghép đôi được ghi ở mặt sau của khóa).

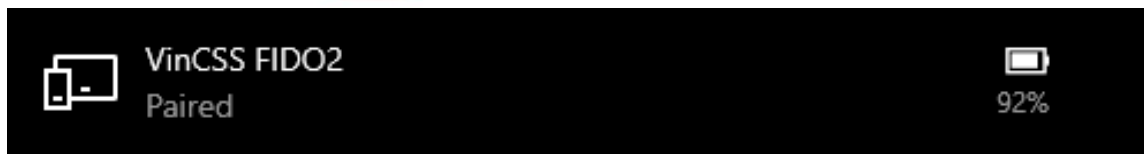




- Kết nối thành công. Nhấn **Done** để kết thúc.



- Sau khi kết nối thành công, trong danh sách thiết bị sẽ hiển thị khóa bảo mật VinCSS FIDO2® Fingerprint và dung lượng pin còn lại của khóa. Trên khóa sẽ hiển thị đèn LED xanh lục.

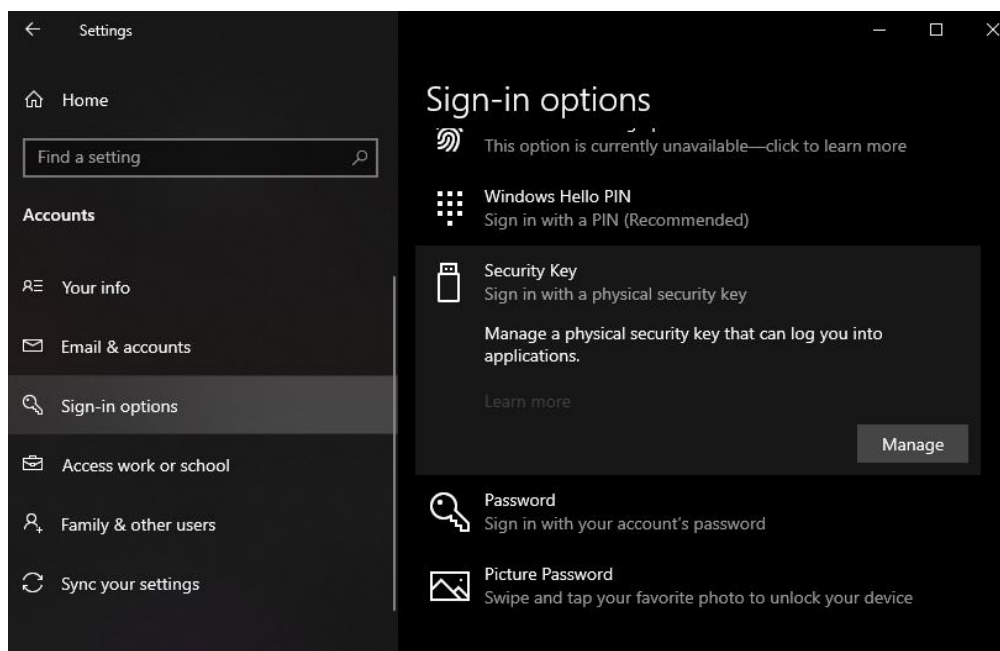


**Lưu ý:**

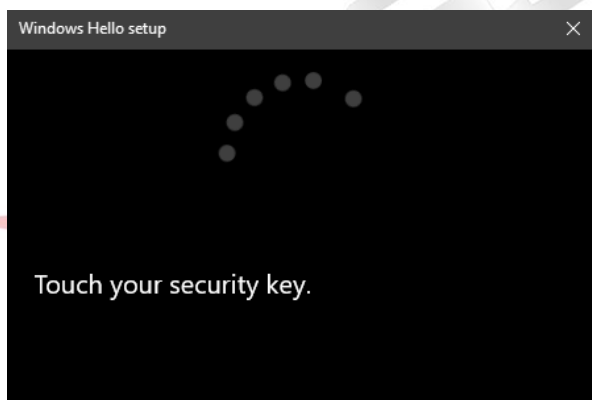
- Trong trường hợp muốn ghép nối với thiết bị mới, thực hiện nhấn giữ cảm biến vân tay trong vòng 4 giây khi khóa xác thực đang được bật.
- Nếu không có hoạt động xác thực trong 90 giây, đèn LED sẽ tắt, khóa tự chuyển vào chế độ Sleep.

### II.1.2. Tạo mã PIN mới

- Truy cập **Start > Settings**.
- Chọn **Account > Sign-in options > Security Key**, sau đó nhấn vào nút **Manage**.



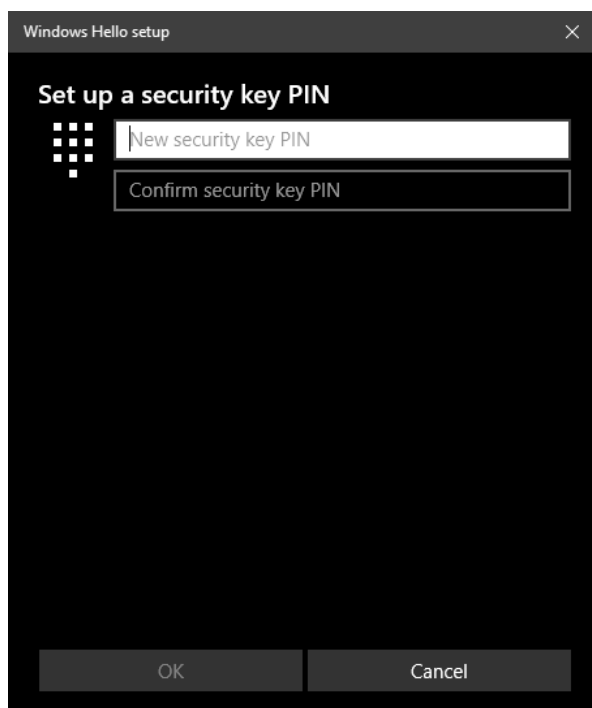
- **Chạm** vào cảm biến vân tay trên khóa bảo mật.



- Mặc định ban đầu, VinCSS FIDO2® Fingerprint không có mã PIN, để tạo mã PIN mới, tại mục **Security Key PIN**, nhấn vào **Add** để thêm mã PIN cho khóa bảo mật.

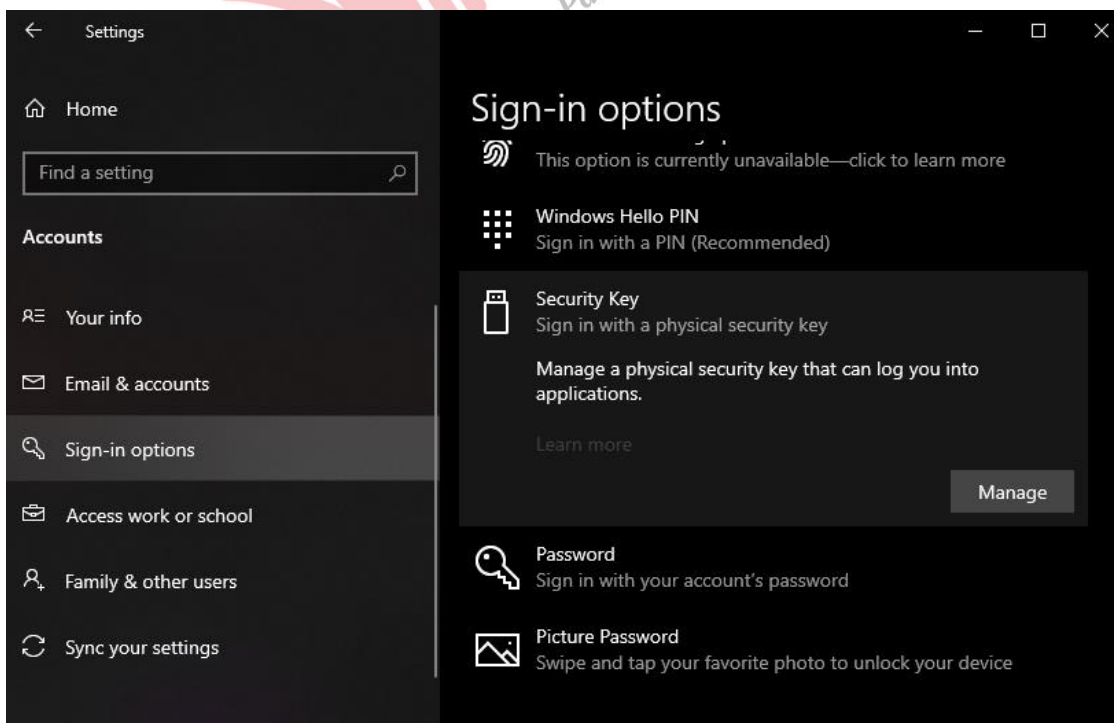


- Điền vào thông tin mã PIN mới, sau đó chọn **OK**.

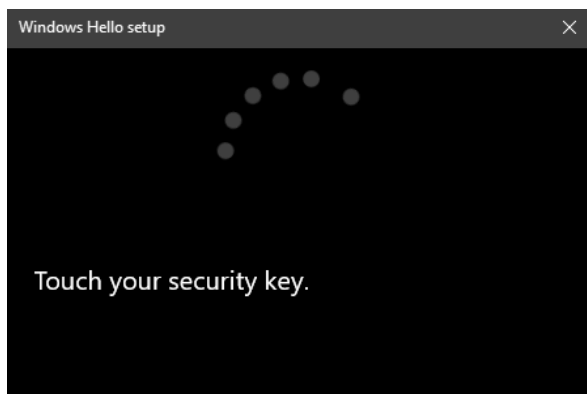


### II.1.3. Thay đổi mã PIN

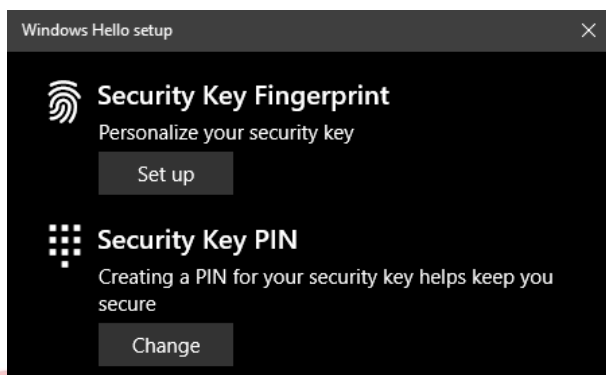
- Truy cập **Start > Settings**.
- Chọn **Account > Sign-in options > Security Key**. Sau đó chọn **Manage**.



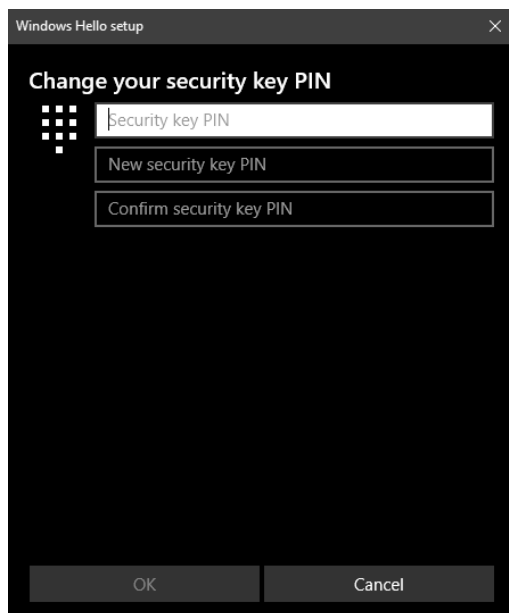
- **Chạm** vào cảm biến vân tay trên khóa bảo mật.



- Tại mục **Security Key PIN**, nhấn vào **Change** để thay đổi mã PIN của khóa bảo mật.



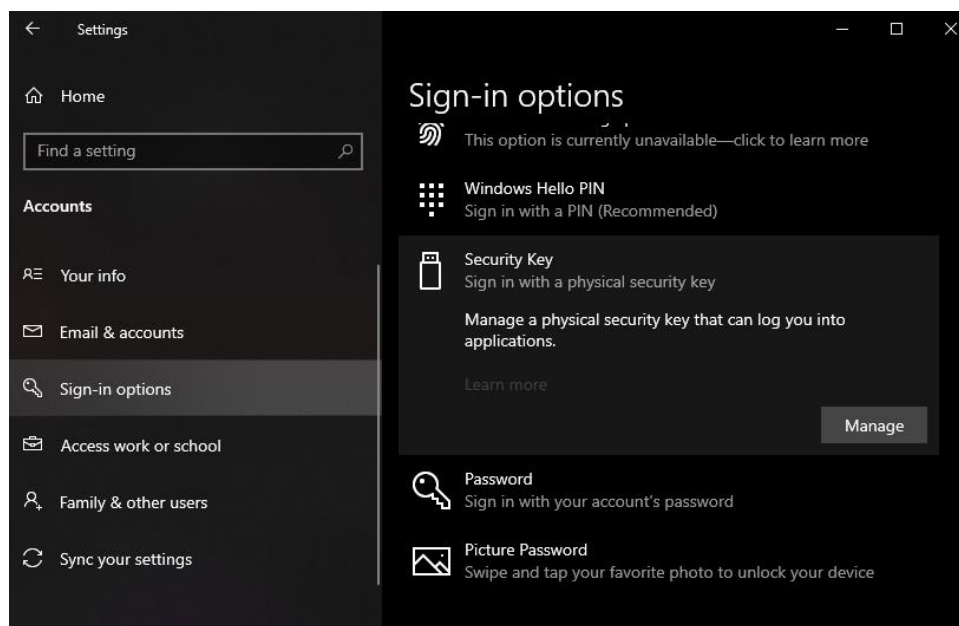
- Điền các thông tin theo thứ tự: mã PIN cũ, mã PIN mới, xác nhận mã PIN mới. Sau đó nhấn **OK**.



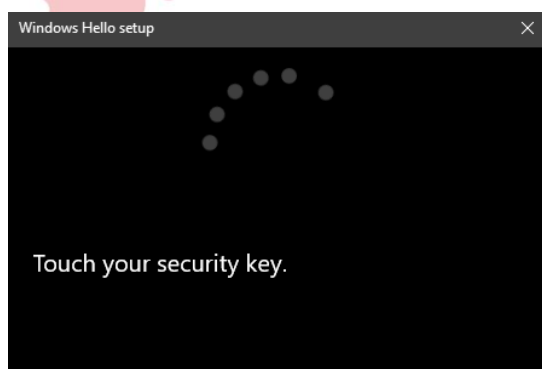
#### II.1.4. Thêm vân tay

Sau khi tạo mã PIN cho VinCSS FIDO2® Fingerprint thành công, người dùng có thể thêm vân tay cho thiết bị (tối đa 5 vân tay). Thực hiện các bước như sau:

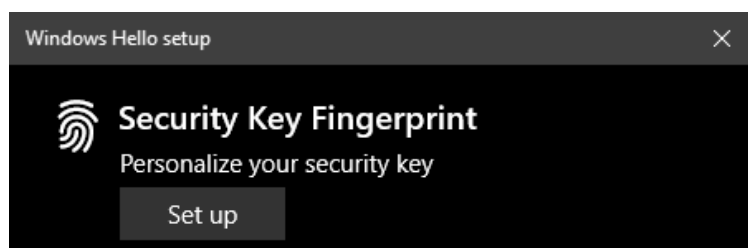
- Truy cập **Start > Settings**.
- Chọn **Account > Sign-in options > Security Key**. Sau đó nhấn vào nút **Manage**.



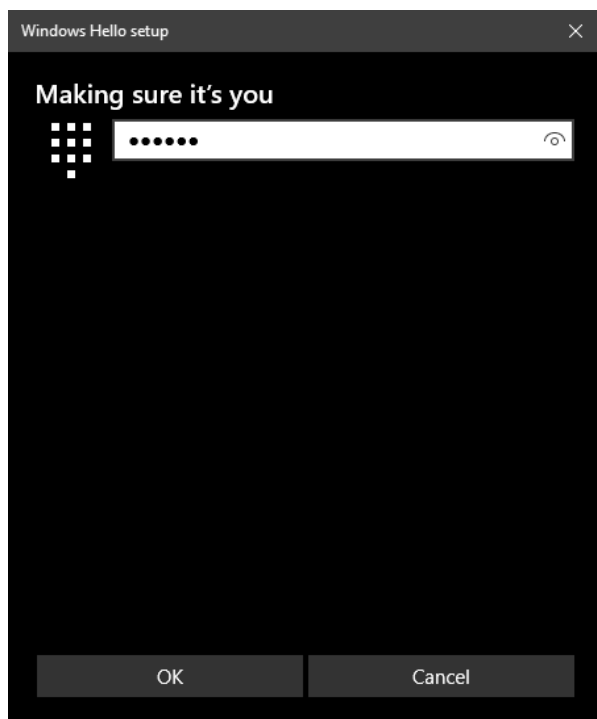
- **Chạm** vào cảm biến vân tay trên khóa bảo mật.



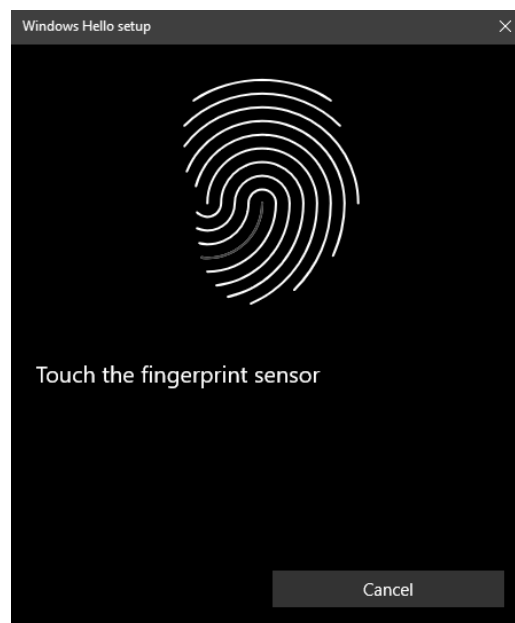
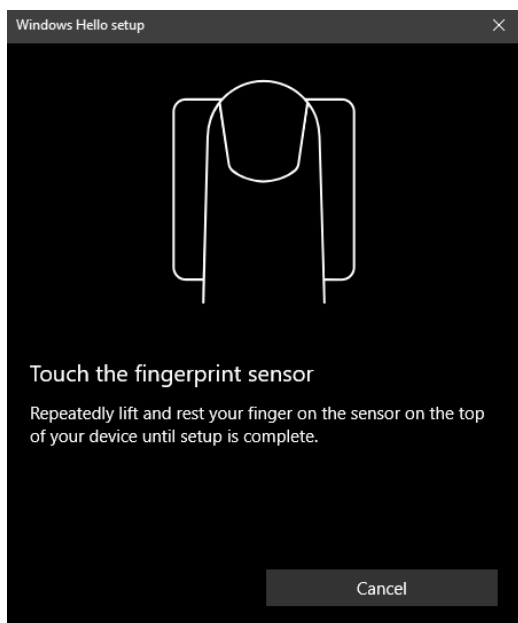
- Tại mục **Security Key Fingerprint**, nhấn **Set up**.



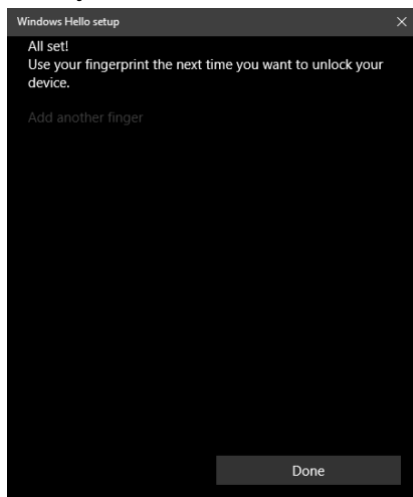
- Điền mã PIN (đã tạo ở bước trên), sau đó nhấn **OK**.



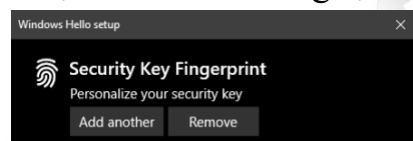
- Khi trên màn hình hiển thị như hình và trên thiết bị nháy đèn trắng, tiến hành quét vân tay bằng cách chạm ngón tay vào cảm biến vân tay, sau đó nhả tay ra khỏi cảm biến vân tay khi khóa bảo mật hiển thị đèn màu xanh lá (thực hiện 5 lần).



- Sau khi quét xong vân tay, nhấn **Done** để kết thúc.



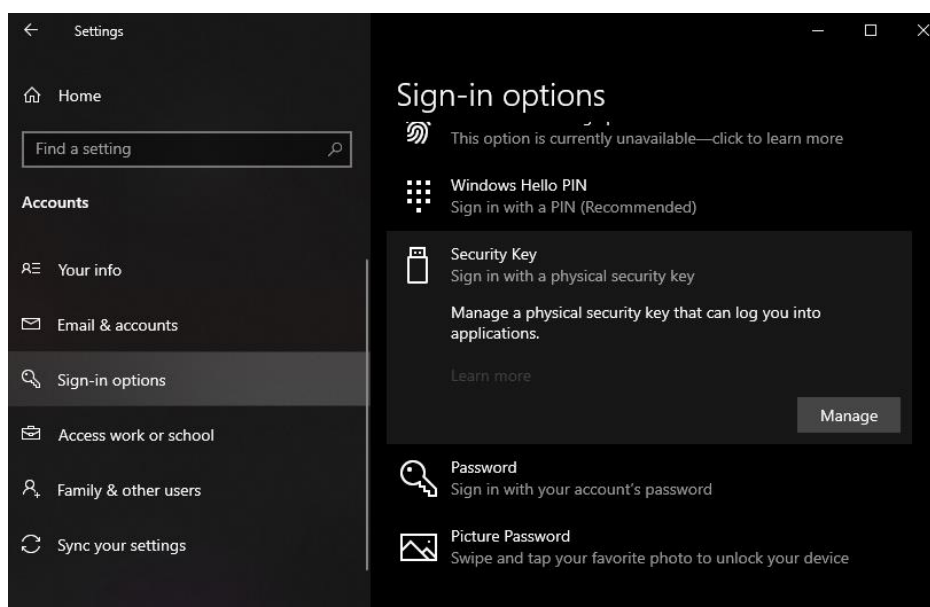
- Để thêm vân tay khác, tại mục **Security Key Fingerprint**, chọn **Add another**, sau đó thực hiện các bước tương tự như trên.



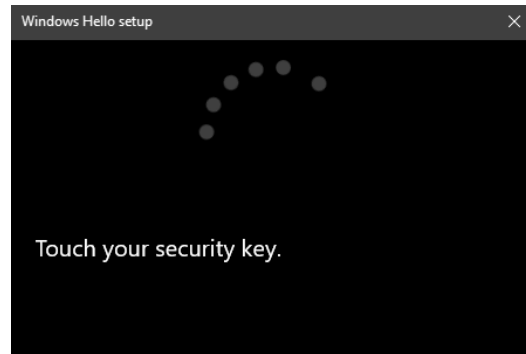
### II.1.5. Xóa vân tay

Hiện hệ điều hành Windows chưa hỗ trợ xóa từng dấu vân tay trên khóa bảo mật, chỉ có thể xóa toàn bộ dấu vân tay. Các bước thực hiện như sau:

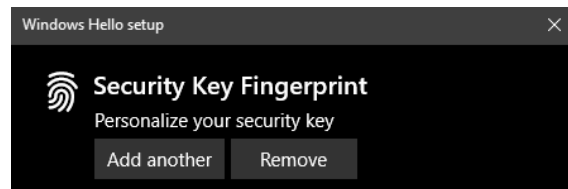
- Truy cập **Start > Settings**.
- Chọn **Account > Sign-in options > Security Key**, sau đó nhấn vào nút **Manage**.



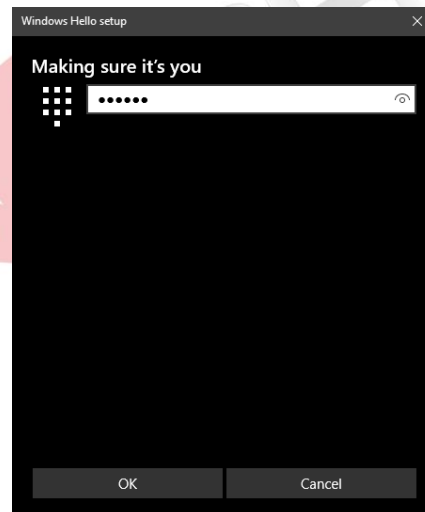
- **Chạm** vào cảm biến vân tay trên khóa bảo mật.



- Tại mục **Security Key Fingerprint**, chọn **Remove**.



- Điền mã PIN (đã tạo ở bước trên), sau đó nhấn **OK**.



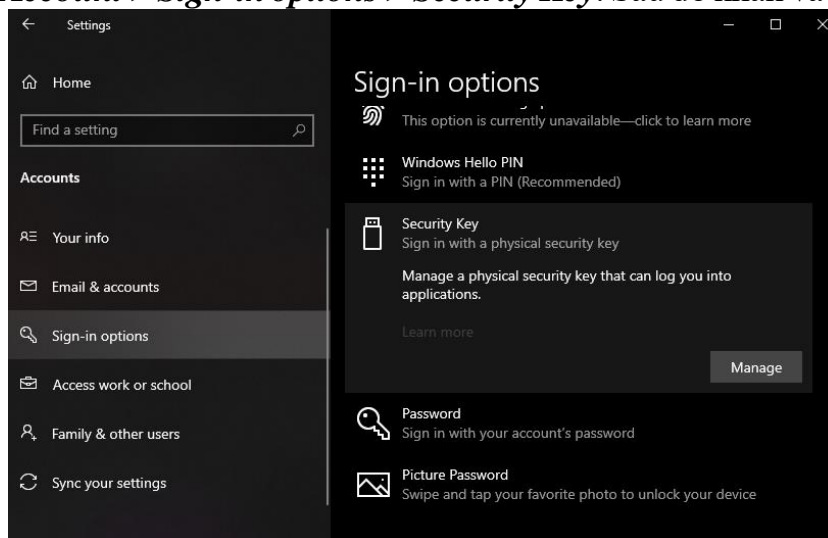
### II.1.6. Thiết lập cài đặt gốc

Trong trường hợp quên mã PIN của VinCSS FIDO2® Fingerprint, người dùng có thể reset thiết bị, tuy nhiên điều này sẽ khiến các dịch vụ đã đăng ký trước đó không thể xác thực được nữa. Sau khi reset, thiết bị trở thành khóa bảo mật mới, vì vậy cần đăng ký lại các dịch vụ để có thể xác thực. Trong trường hợp nhập sai mã PIN nhiều lần (trên 8 lần) thì thiết bị sẽ bị khóa vĩnh viễn, người dùng bắt buộc phải reset để có thể sử dụng lại khóa bảo mật VinCSS FIDO2® Fingerprint như một thiết bị mới.

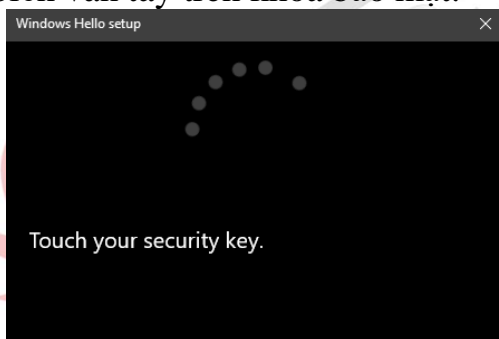


Để reset VinCSS FIDO2® Fingerprint, người dùng thực hiện các bước sau:

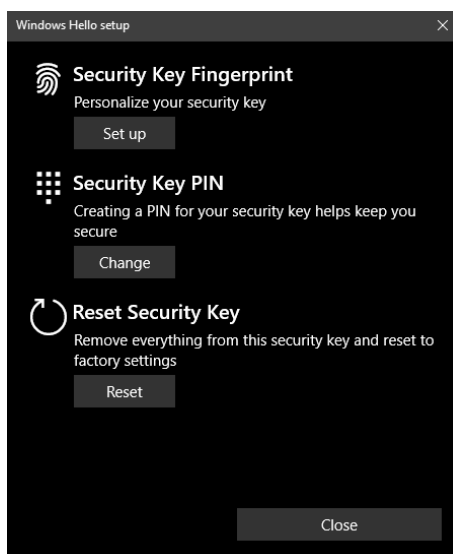
- Truy cập **Start > Settings**.
- Chọn **Account > Sign-in options > Security Key**. Sau đó nhấn vào nút **Manage**.



- **Chạm** vào cảm biến vân tay trên khóa bảo mật.



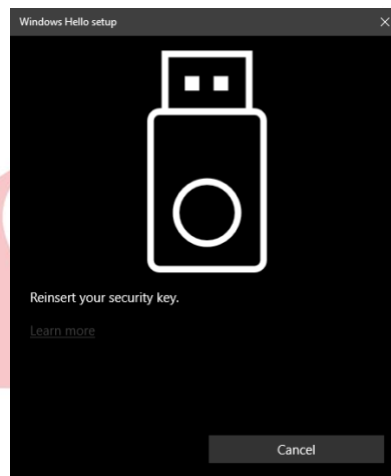
- Tại mục **Reset Security Key**, nhấn **Reset**.



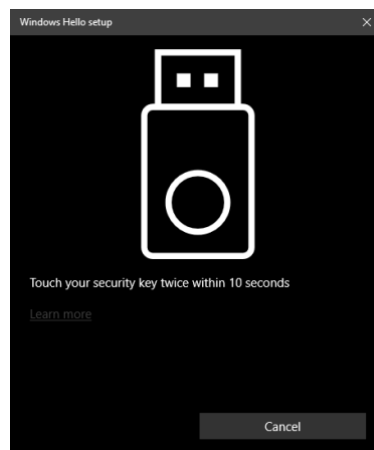
- Nhấn ***Proceed*** để tiến hành Reset khóa bảo mật VinCSS FIDO2® Fingerprint.



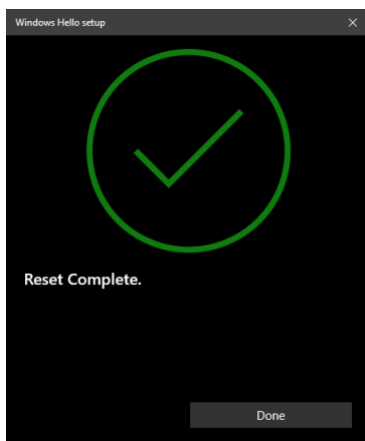
- Rút khóa bảo mật VinCSS FIDO2® Fingerprint ra khỏi máy tính, sau đó cắm lại.



- Khi hiện đèn màu trắng tay trên khóa bảo mật VinCSS FIDO2® Fingerprint, chạm 2 lần vào cảm biến vân tay khoảng 10s.



- Reset khóa bảo mật thành công.



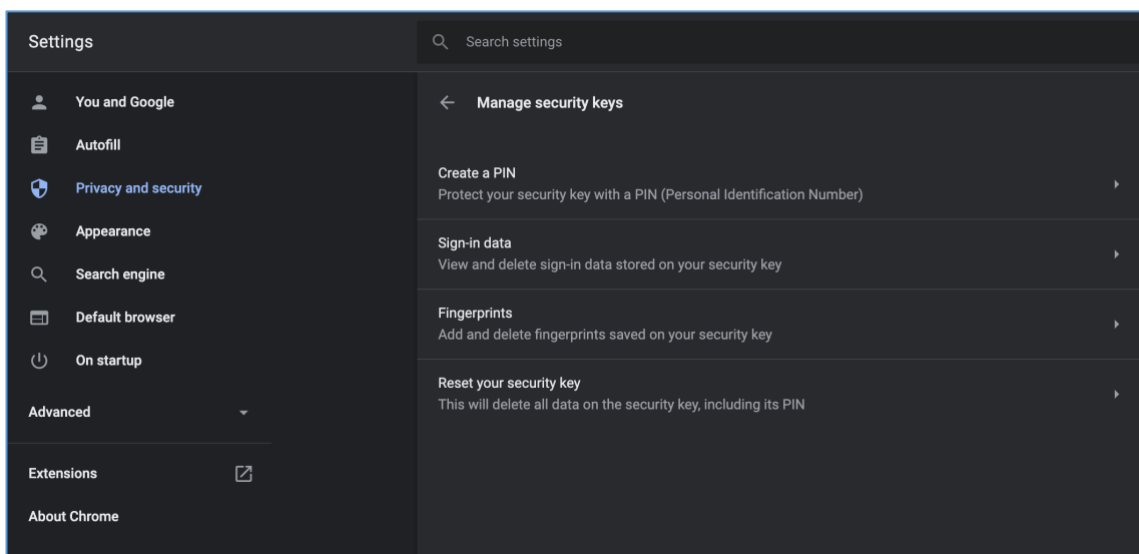
## II.2. Nền tảng macOS

### II.2.1. Kết nối với máy tính

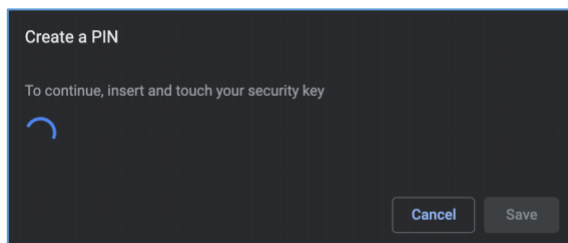
Tiến hành kết nối khoá bảo mật VinCSS FIDO2® Fingerprint vào máy tính thông qua dây USB. Nếu đèn LED nhấp đỏ 3 lần liên tiếp cho biết mức pin đang ở dưới 20%, đèn LED màu hồng phách cho biết khoá bảo mật đang được sạc, đèn LED màu xanh lá cây cho biết pin đã được sạc đầy. Khoá bảo mật VinCSS FIDO2® Fingerprint có thể được sử dụng khi đang sạc.

### II.2.2. Tạo mới mã PIN

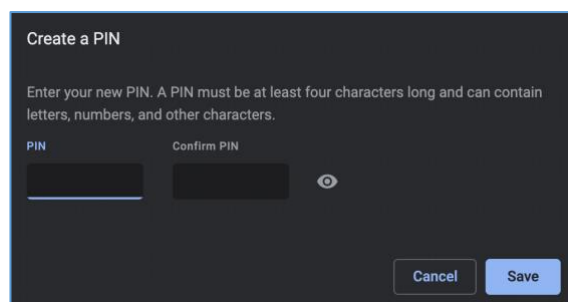
- Mở trình duyệt Chrome, chọn **Setting > Privacy and security > More > Manage security keys**.



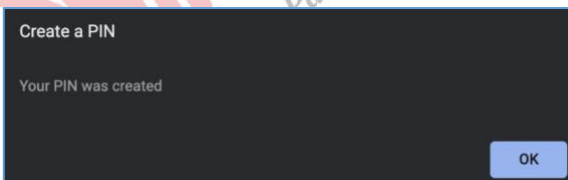
- Mặc định ban đầu, khóa bảo mật VinCSS FIDO2® Fingerprint không có mã PIN, để tạo mới mã PIN cho VinCSS FIDO2® Fingerprint, trên giao diện *Manage security keys*, chọn **Create a PIN** và chạm vào cảm biến vân tay trên VinCSS FIDO2® Fingerprint để xác nhận.



- Tiếp theo, nhập mã PIN và xác nhận lại rồi nhấn **Save** để tạo mã PIN.

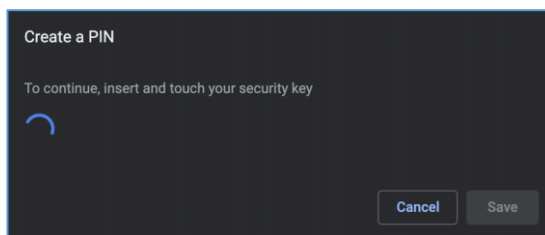


- Nhấn **OK** để hoàn thành việc tạo mã PIN cho VinCSS FIDO2® Fingerprint.

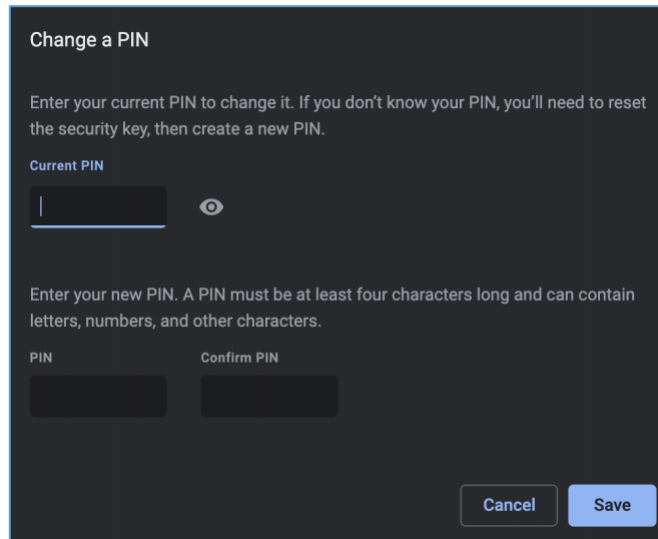


### II.2.3. Thay đổi mã PIN

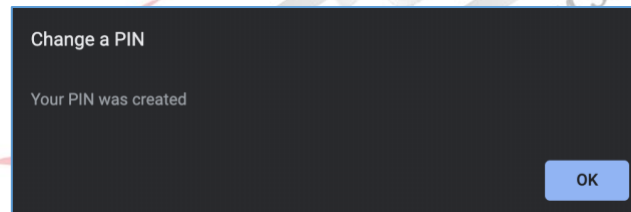
- Để thay đổi mã PIN cho VinCSS FIDO2® Fingerprint, trên giao diện *Manage security keys* (mở trình duyệt Chrome, chọn **Setting > Privacy and security > More > Manage security keys**), chọn **Create a PIN** và chạm vào cảm biến vân tay trên thiết bị để xác nhận.



- Tại cửa sổ **Change a PIN** nhập mã PIN hiện tại đang sử dụng, ở phía dưới nhập mã PIN mới cần thay đổi và xác nhận lại, sau đó chọn **Save** để thay đổi.



- Nhấn **OK** để hoàn thành việc thay đổi mã PIN cho VinCSS FIDO2® Fingerprint.

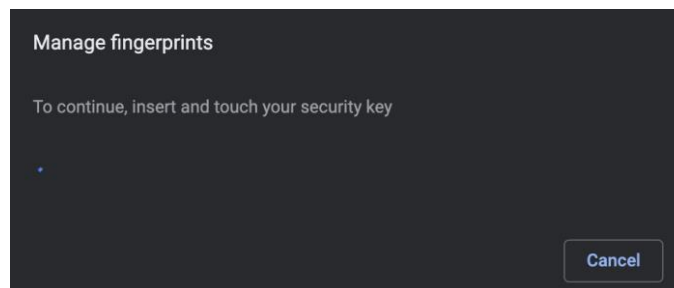


#### II.2.4. Thêm vân tay

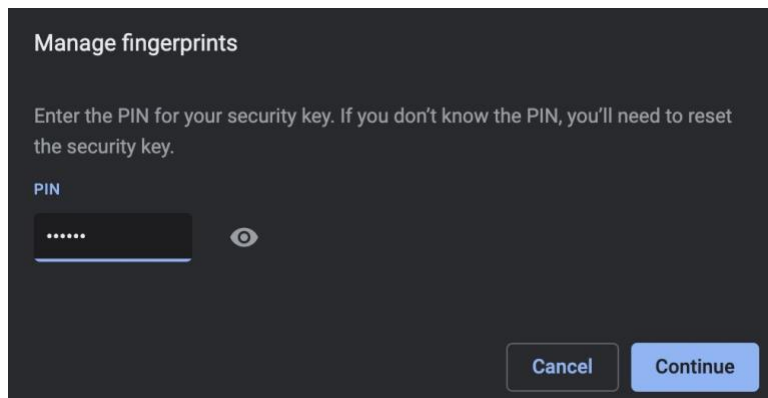
Sau khi tạo mã PIN cho VinCSS FIDO2® Fingerprint thành công, người dùng có thể thêm vân tay cho thiết bị (tối đa **5** vân tay).

Thực hiện các bước như sau:

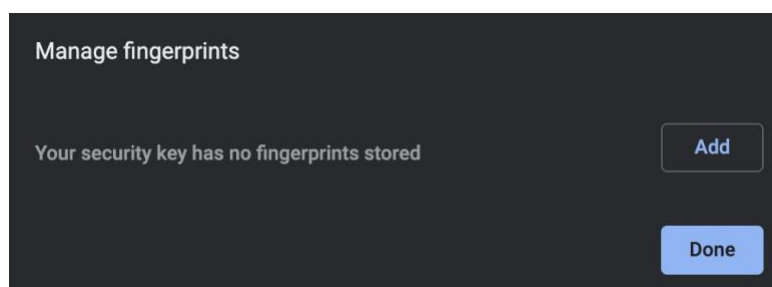
- Trên giao diện **Manage security keys** (mở trình duyệt *Chrome*, chọn **Setting** > **Privacy and security** > **More** > **Manage security keys**), chọn **Fingerprints**, sau đó chạm vào cảm biến vân tay trên khóa bảo mật.



- Điền mã **PIN** (đã tạo ở bước trên), sau đó nhấn **Continue** để tiếp tục.



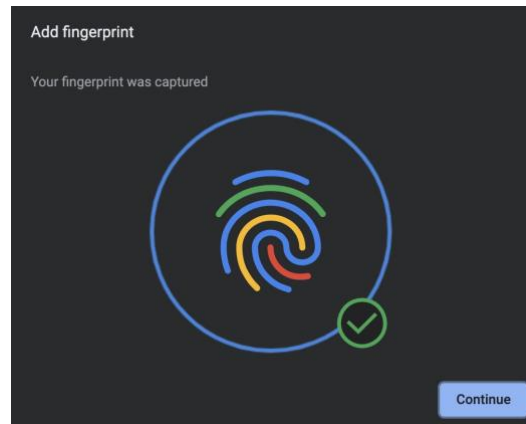
- Để thêm vân tay cho khóa bảo mật, nhấn **Add**.



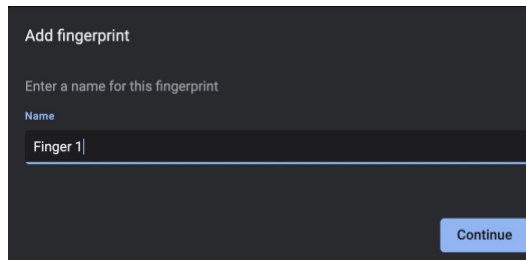
- Khi trên màn hình hiển thị như hình và trên thiết bị nháy đèn trắng, tiến hành quét vân tay bằng cách chạm ngón tay vào cảm biến vân tay, sau đó nhả tay ra khỏi cảm biến vân tay khi khóa bảo mật hiển thị đèn màu xanh lá. Tiến hành quét vân tay nhiều lần để nhận diện vân tay tốt hơn.



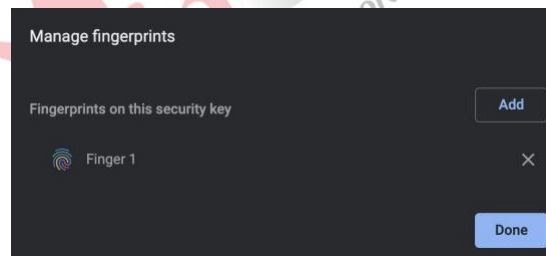
- Sau khi quét xong vân tay, nhấn **Continue** để tiếp tục.



- Đặt tên cho vân tay (tối đa 30 ký tự không dấu), sau đó nhấn **Continue** để tiếp tục.

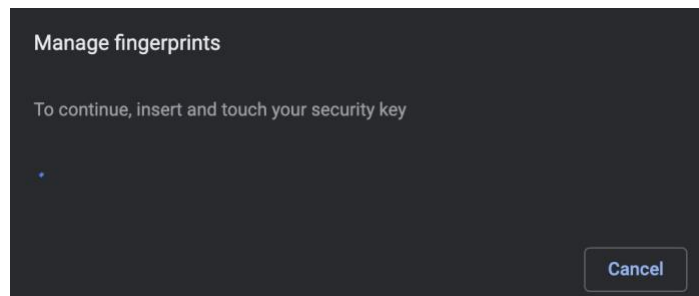


- Nhấn **Add** để tiếp tục thêm vân tay, hoặc nhấn **Done** để kết thúc.

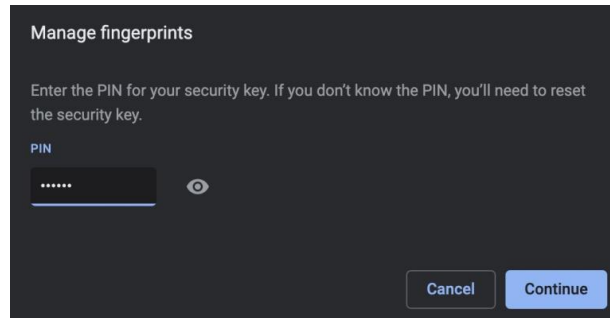


## II.2.5. Xóa vân tay

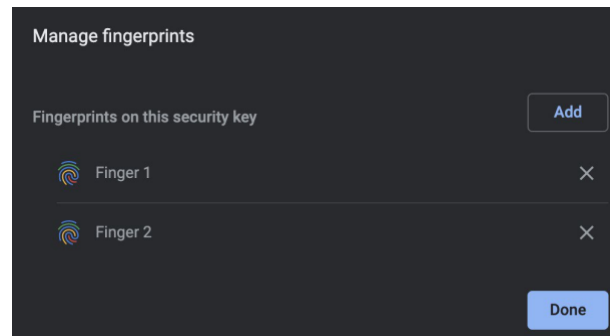
- Trên giao diện **Manage security keys** (mở trình duyệt Chrome, chọn **Setting > Privacy and security > More > Manage security keys**), chọn **Fingerprints**, sau đó chạm vào cảm biến vân tay trên khóa xác thực.



- Điền mã PIN (đã tạo ở bước trên), sau đó nhấn **Continue** để tiếp tục.

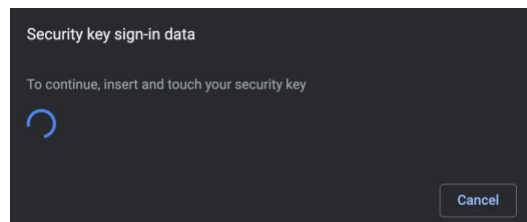


- Trên màn hình sẽ hiển thị danh sách vân tay đã được đăng ký trên khóa bảo mật. Nhấn vào biểu tượng chữ “X” tại mỗi vân tay tương ứng để xóa vân tay đã đăng ký.

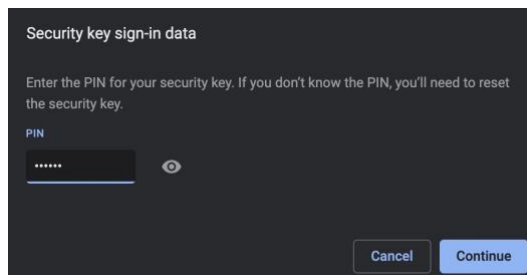


## II.2.6. Quản lý dữ liệu đăng nhập

- Trên giao diện **Manage security keys** (mở trình duyệt Chrome, chọn **Setting > Privacy and security > More > Manage security keys**), chọn **Sign-in data**, sau đó chạm vào cảm biến vân tay trên khóa xác thực.

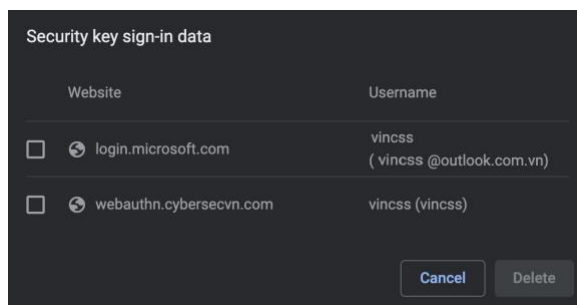


- Điền mã PIN (đã tạo ở bước trên), sau đó nhấn **Continue** để tiếp tục.

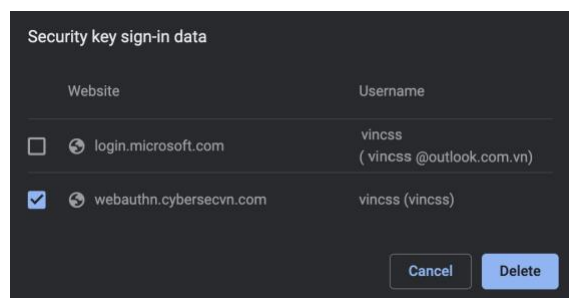




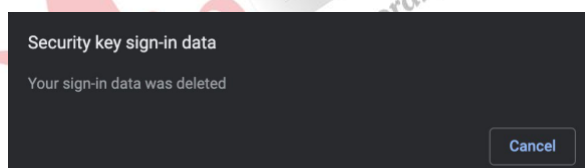
- Trên màn hình sẽ hiển thị danh sách dữ liệu đăng nhập, bao gồm tên website và tên đăng nhập.



- Để xóa dữ liệu đăng nhập, nhấn chọn vào ô vuông ở đầu mỗi dòng, sau đó nhấn **Delete**.



- Sau khi xóa xong, nhấn **Cancel** để kết thúc.



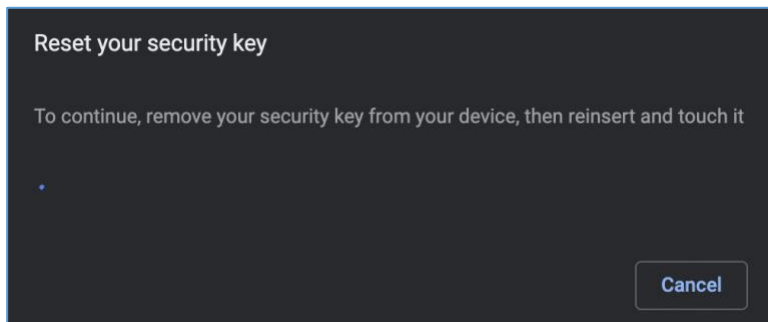
### II.2.7. Thiết lập cài đặt gốc

Trong trường hợp quên mã PIN của VinCSS FIDO2<sup>®</sup> Fingerprint, người dùng có thể reset thiết bị, tuy nhiên điều này sẽ khiến các dịch vụ đã đăng ký trước đó không thể xác thực được nữa. Sau khi reset, thiết bị trở thành khóa bảo mật mới, vì vậy cần đăng ký lại các dịch vụ để có thể xác thực. Trong trường hợp nhập sai mã PIN nhiều lần (trên 8 lần) thì thiết bị sẽ bị khóa vĩnh viễn, người dùng bắt buộc phải reset để có thể sử dụng lại khóa bảo mật VinCSS FIDO2<sup>®</sup> Fingerprint như một thiết bị mới.

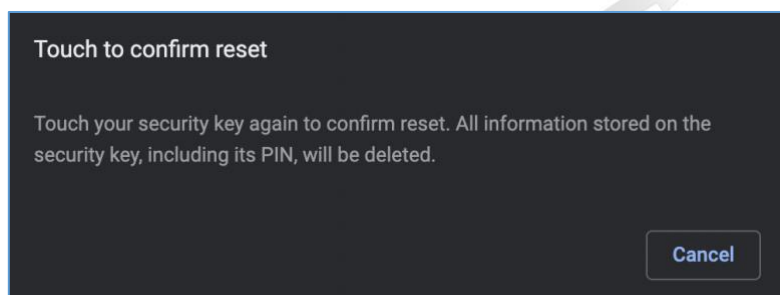
Để reset VinCSS FIDO2<sup>®</sup> Fingerprint, thực hiện các bước sau:

- Trên giao diện **Manage security keys** (mở trình duyệt Chrome, chọn **Setting** > **Privacy and security** > **More** > **Manage security keys**), chọn **Reset your**

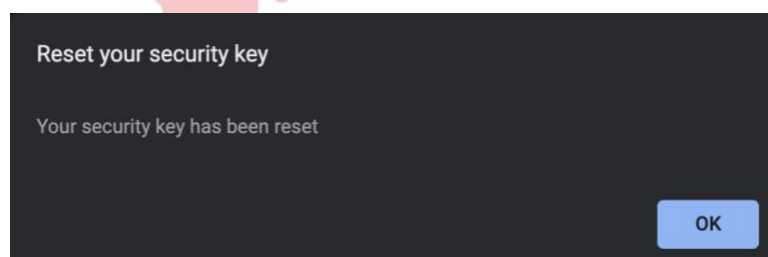
**security keys**, sau đó rút khóa bảo mật VinCSS FIDO2® Fingerprint ra khỏi máy tính và cắm lại. Chạm vào cảm biến vân tay trên VinCSS FIDO2® Fingerprint để xác nhận.



- Chạm tiếp vào cảm biến vân tay trên VinCSS FIDO2® Fingerprint lần nữa để xác nhận việc reset VinCSS FIDO2® Fingerprint.



- Quá trình reset thành công. Nhấn **OK** để kết thúc.



### III. XÁC THỰC KHÔNG MẬT KHẨU VỚI VINCSS FIDO2® FINGERPRINT

#### III.1. Windows 10

##### III.1.1. Cấu hình trên hệ thống Azure AD

###### III.1.1.1. Cấu hình Azure AD

- Truy cập vào đường link sau:  
[https://portal.azure.com/#blade/Microsoft\\_AAD\\_IAM/AuthenticationMethodsMenuBlade/AdminAuthMethods](https://portal.azure.com/#blade/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/AdminAuthMethods)

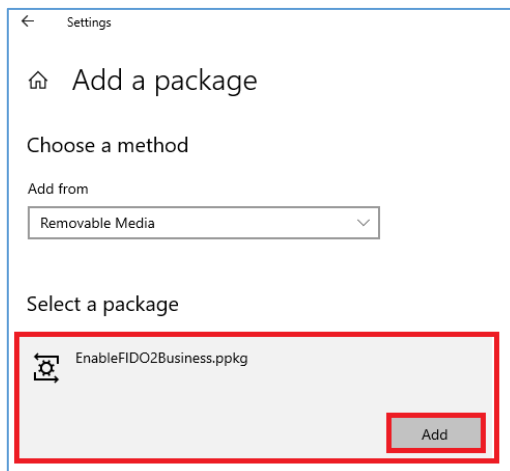
- Chọn **Method FIDO2 Security Key**, sau đó chọn các cấu hình như sau:

The screenshot shows the Windows FIDO2 Security Key settings. At the top, there is a table with columns: Method, Target, and Enabled. The table lists three methods: FIDO2 Security Key (All users, Yes), Microsoft Authenticator passwordless sign-in (No), and Text message (No). Below the table is a section titled 'FIDO2 Security Key settings' with a dropdown arrow. Under this section, there are three main areas: 'ENABLE' with a 'Yes' button selected, 'TARGET' with 'All users' selected, and 'GENERAL' with 'Allow self-service set up' set to 'Yes', 'Enforce attestation' set to 'No', 'Enforce key restrictions' set to 'No', and 'Restrict specific keys' set to 'Allow'. At the bottom, there is a section for 'KEY RESTRICTION POLICY' with 'Enforce key restrictions' set to 'No' and 'Restrict specific keys' set to 'Allow'. There is also a section for 'Add AAGUID' with a right arrow and a note 'No AAGUIDs have been added.'

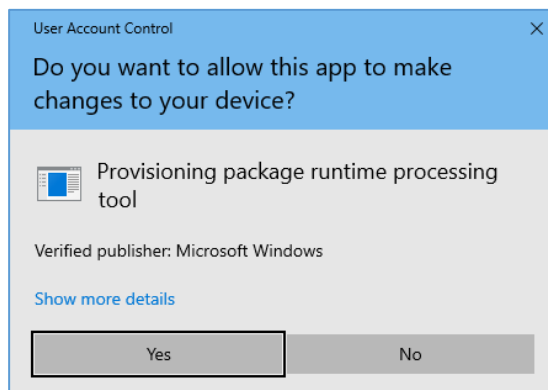
- Nhấn **Save** để lưu lại cấu hình.

### III.1.1.2. Đăng nhập Windows 10 sử dụng FIDO2 với provisioning packages

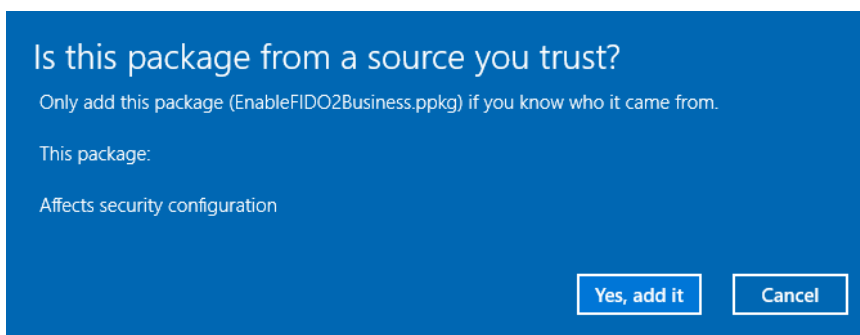
- Chuyển tải 2 file **EnableFIDO2Business.cat** và **EnableFIDO2Business.ppkg** được VinCSS cung cấp vào thiết bị lưu trữ.
- Kết nối thiết bị lưu trữ đó với máy tính cần kích hoạt tính năng FIDO2, sau đó truy cập vào **Settings > Accounts > Access work or school > Add or remove a provisioning package > Add a package**, chọn vào gói và nhấn **Add**.



- Chọn **Yes**.

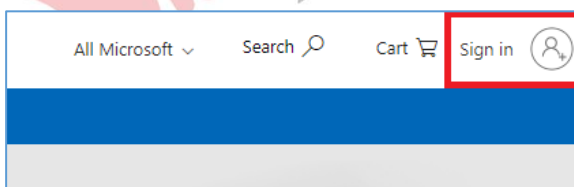


- Chọn **Yes, add it**.

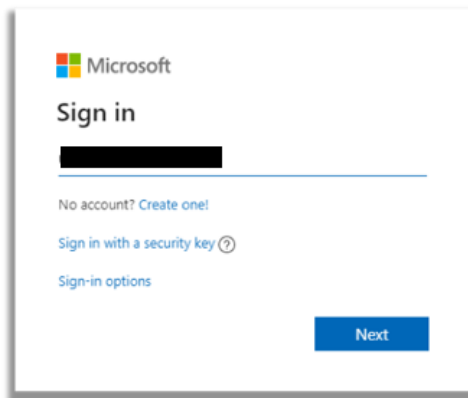


### III.1.1.3. Đăng ký khóa xác thực cho tài khoản Azure AD

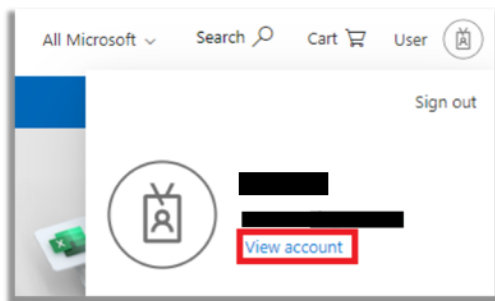
- Truy cập <https://microsoft.com>, chọn **Sign in**.



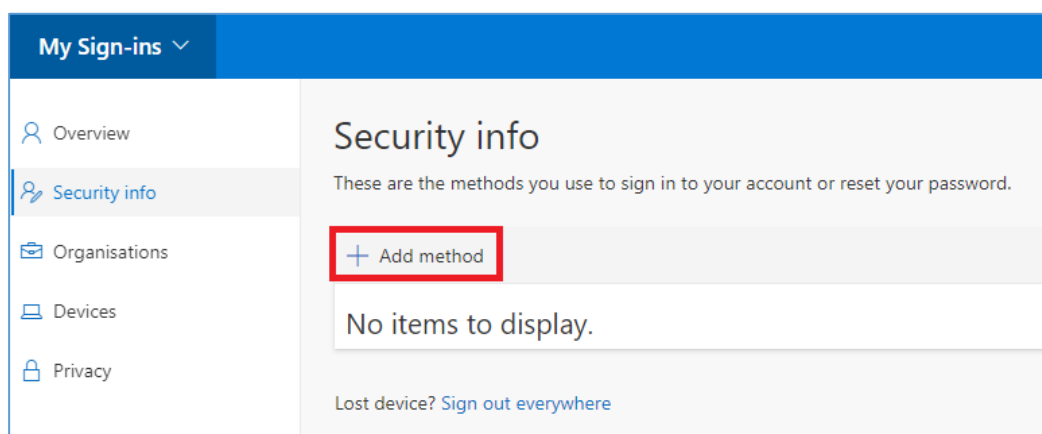
- Nhập thông tin account AD (username/password) để đăng nhập.



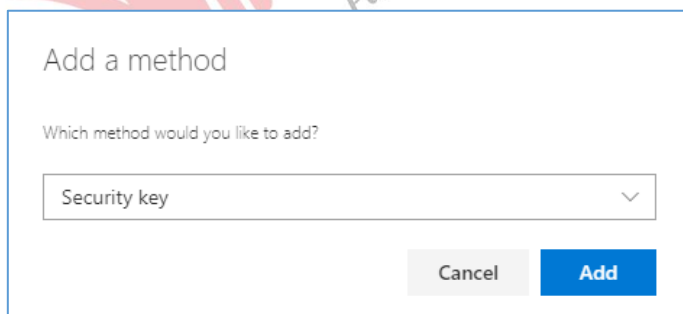
- Sau khi đăng nhập thành công, Chọn **View account** để tiến hành cấu hình.



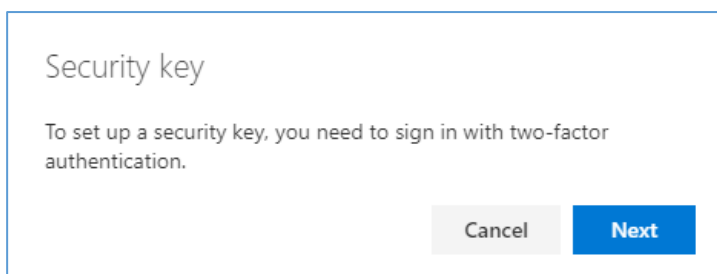
- Chọn mục **Security info** > **Add method** để thêm tùy chọn đăng nhập.



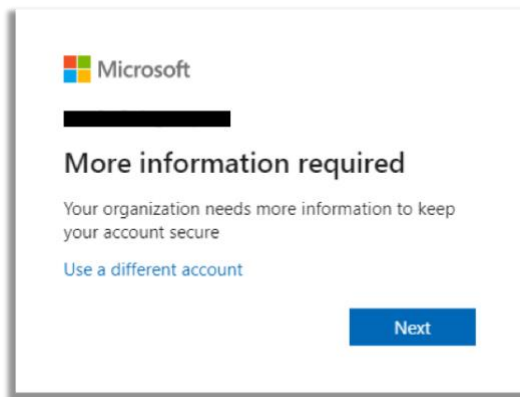
- Trong ô tùy chọn, chọn **Security key** và nhấn nút **Add**.



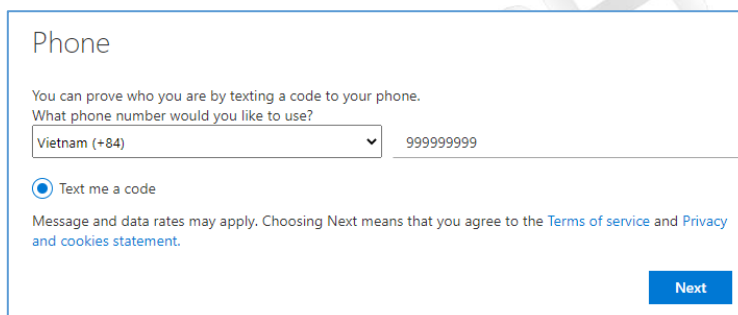
- Bấm **Next** kích hoạt chế độ xác thực hai lớp.



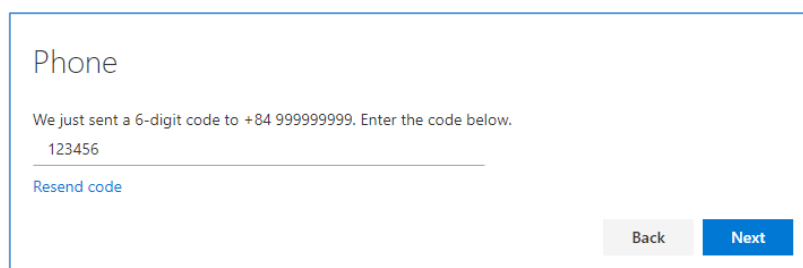
- Chọn **Next** để tiếp tục.



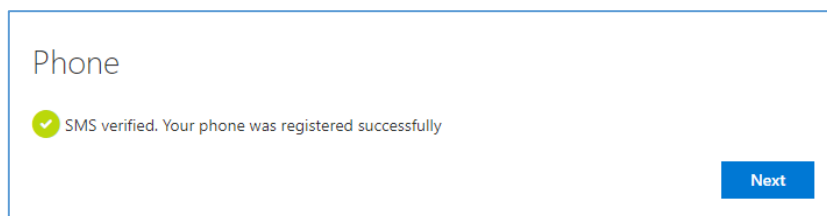
- Tùy chọn: Nếu bạn không đăng ký số điện thoại từ trước, làm theo các bước sau đây:
  - o Cung cấp mã quốc gia và số điện thoại để nhận mã code xác thực.

A screenshot of the "Phone" setup screen. The title is "Phone". Below it, it says "You can prove who you are by texting a code to your phone." and "What phone number would you like to use?". There is a dropdown menu showing "Vietnam (+84)" and a text input field containing "999999999". Below that is a radio button labeled "Text me a code" which is selected. At the bottom, it says "Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#)". At the bottom right is a blue button labeled "Next".

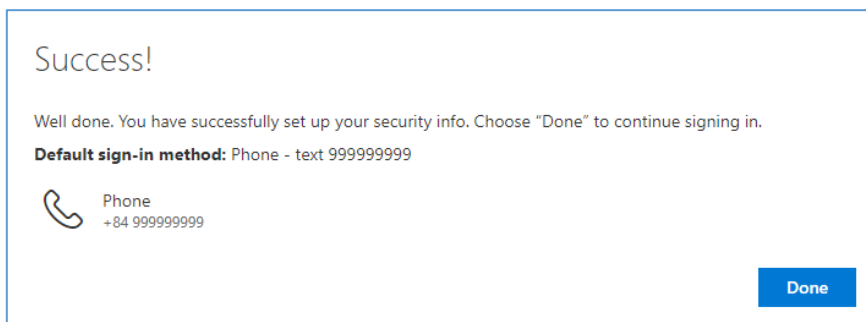
- o Nhập mã 6 số nhận được qua tin nhắn điện thoại.

A screenshot of the "Phone" screen. The title is "Phone". Below it, it says "We just sent a 6-digit code to +84 999999999. Enter the code below." There is a text input field containing "123456". Below that is a link "Resend code" in blue. At the bottom right are two buttons: "Back" (disabled) and "Next" (active).

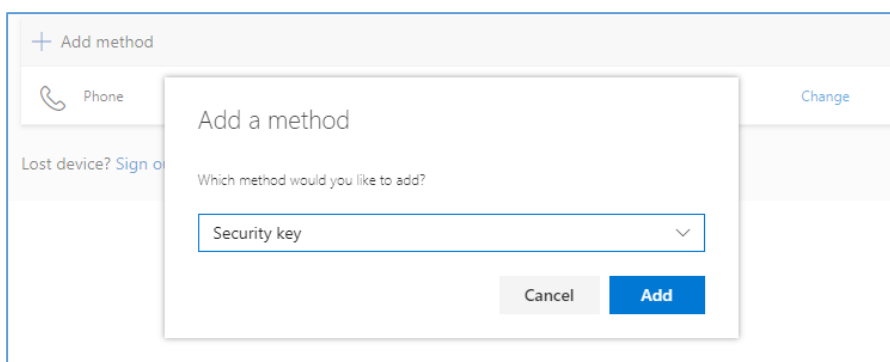
- o Nhấn **Next** để tiếp tục.

A screenshot of the "Phone" screen. The title is "Phone". Below it, there is a green checkmark icon followed by the text "SMS verified. Your phone was registered successfully". At the bottom right is a blue button labeled "Next".

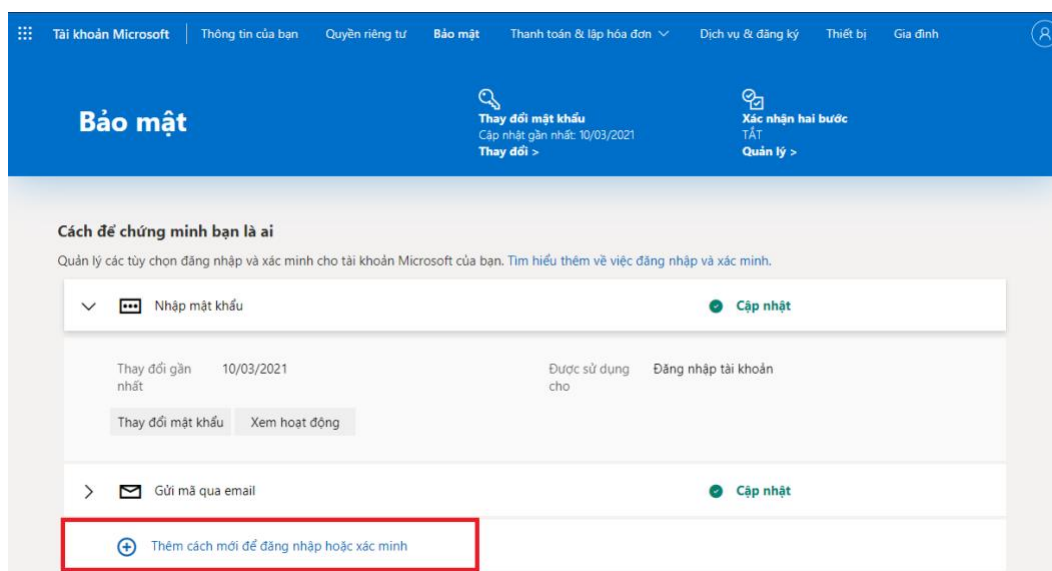
- Xác nhận lại thông tin đã đăng ký, nhấn **Done** để quay lại trang Security info.



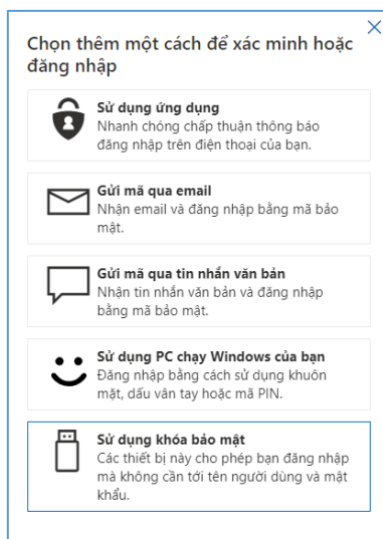
- Chọn **Add method** → **Security key**, sau đó nhấn **Add**.



- Truy cập <https://microsoft.com>, sau đó đăng nhập tài khoản Microsoft.
- Tiếp tục truy cập: <https://account.live.com/proofs/Manage/additional>, sau đó chọn **Thêm cách mới để đăng nhập hoặc xác minh**.

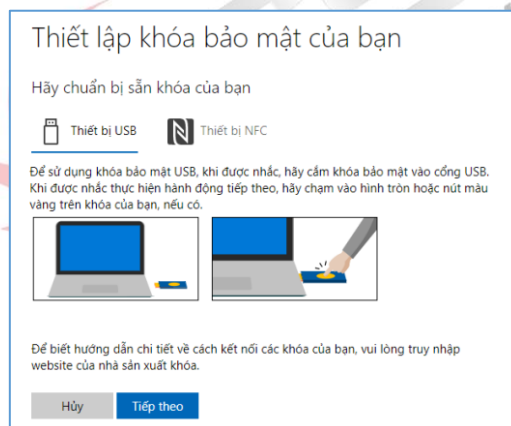


- Chọn **Sử dụng khóa bảo mật**.

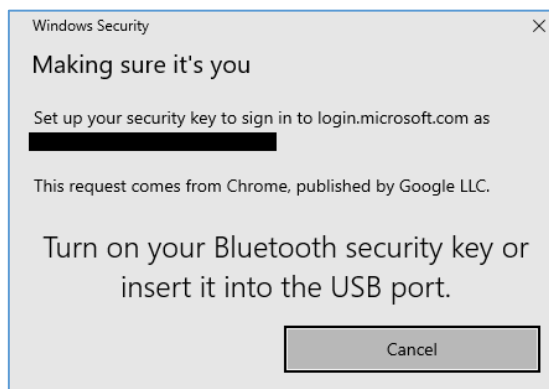


*Sử dụng qua kết nối Bluetooth.*

- Chọn **Thiết bị USB**.

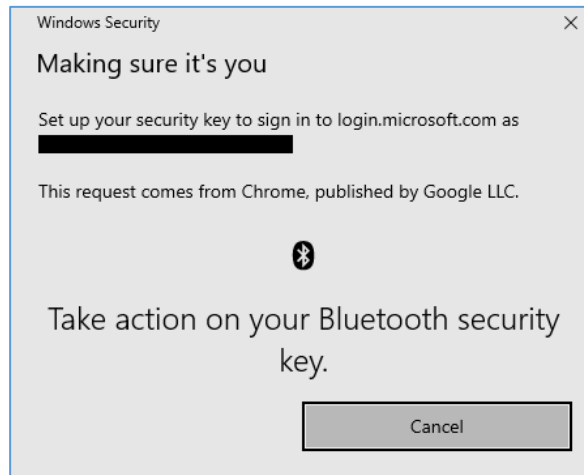


- Kết nối khoá bảo mật với máy tính thông qua kết nối Bluetooth.



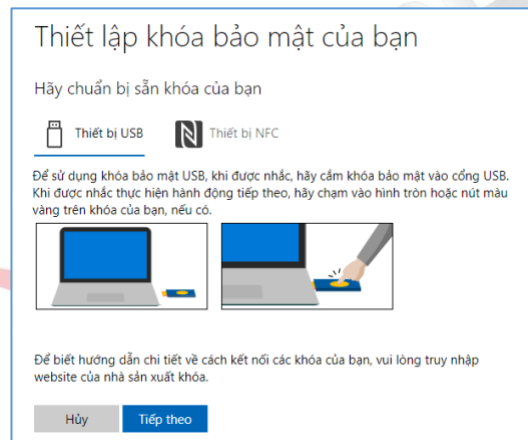


- Quét dấu vân tay khi nhận được thông báo.

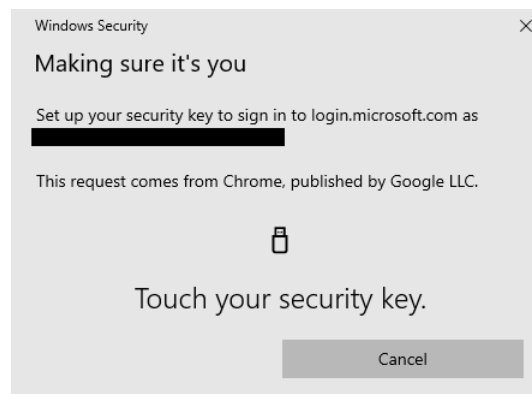


### Sử dụng qua kết nối USB

- Chọn **Thiết bị USB**.

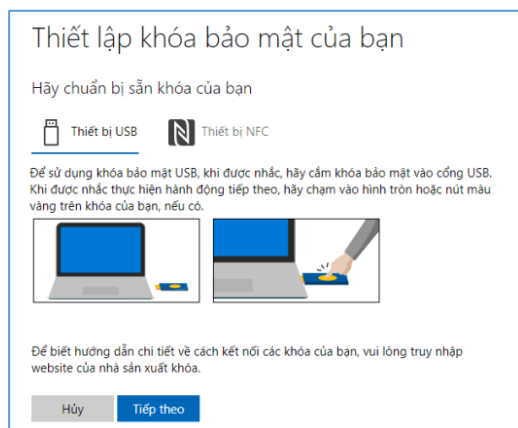


- Kết nối khoá bảo mật với máy tính thông qua kết dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

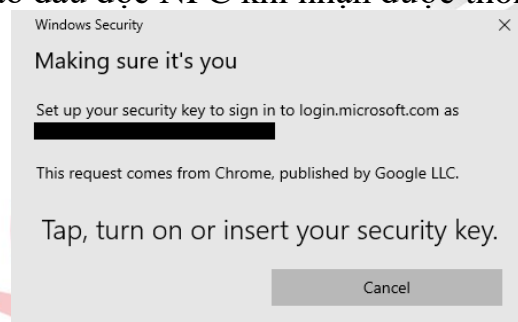


## Sử dụng qua kết nối NFC

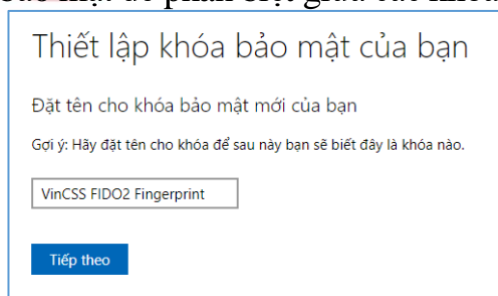
- Chọn **Thiết bị NFC**.



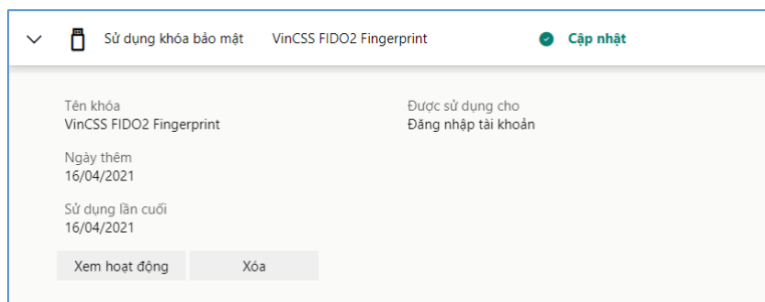
- Kết nối khoá bảo mật với máy tính thông qua kết dây kết nối NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



- Đặt tên cho khóa bảo mật để phân biệt giữa các khóa. Sau đó nhấn **Tiếp theo**.

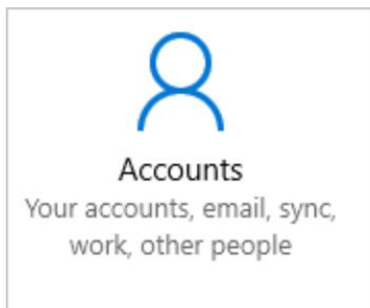


- Thêm khóa bảo mật thành công. Khóa sẽ được hiển thị trong danh sách.

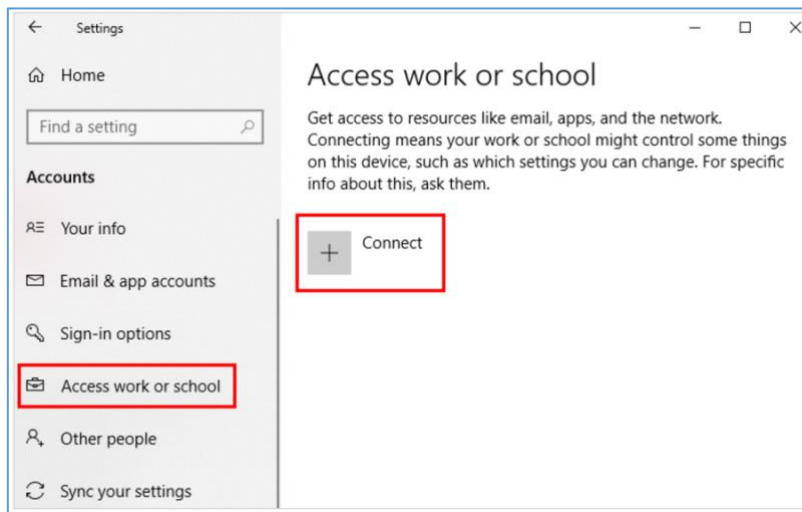


#### III.1.1.4. *Kết nối User vào Azure Work Account*

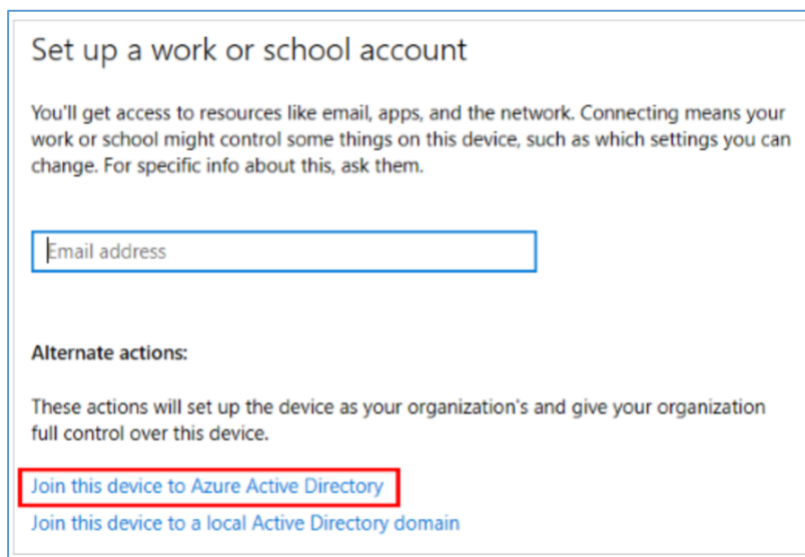
- Trên máy tính Windows, chọn **Settings > Account**.



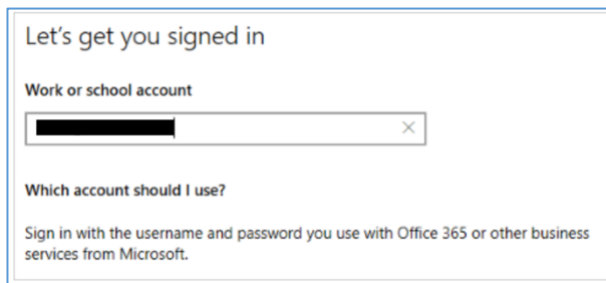
- Chọn **Access work or school > Connect**.



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



- Nhập thông tin account AD (username/password).

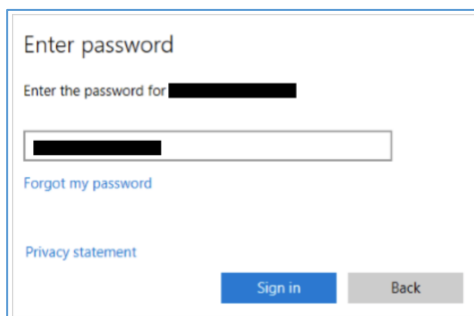


Let's get you signed in

Work or school account

Which account should I use?

Sign in with the username and password you use with Office 365 or other business services from Microsoft.



Enter password

Enter the password for

Forgot my password

Privacy statement

Sign in Back

- Xác thực thông qua điện thoại.



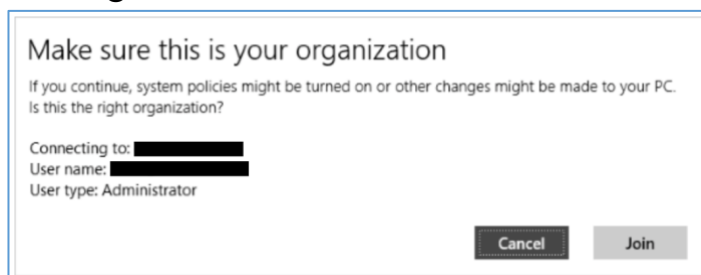
Help us protect your account

We've sent a notification to your mobile device. Please respond to continue.

Use a different verification option

Next Back

- Kiểm tra lại thông tin, sau đó chọn **Done**.

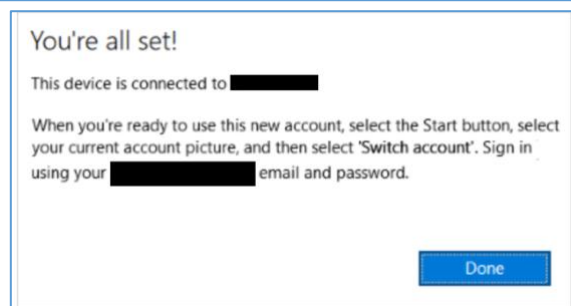


Make sure this is your organization

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: User name: User type: Administrator

Cancel Join



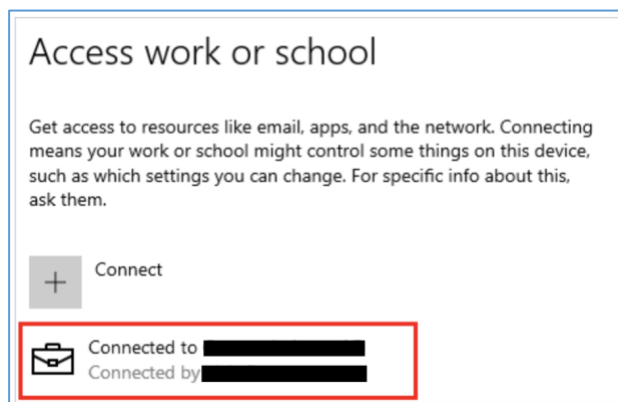
You're all set!

This device is connected to

When you're ready to use this new account, select the Start button, select your current account picture, and then select 'Switch account'. Sign in using your email and password.

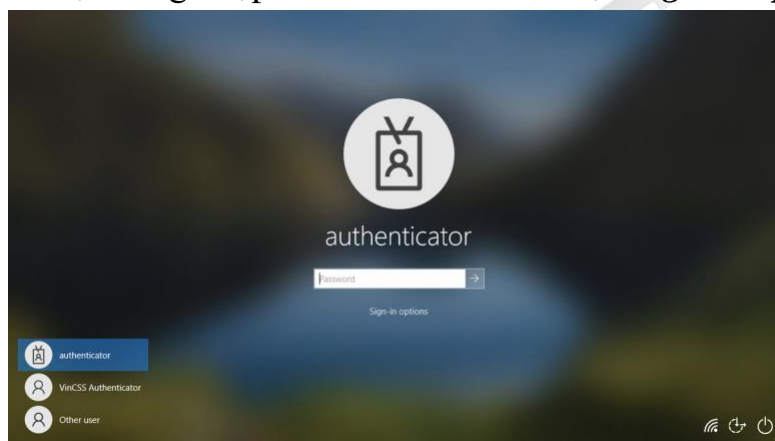
Done

- Kết nối thành công.

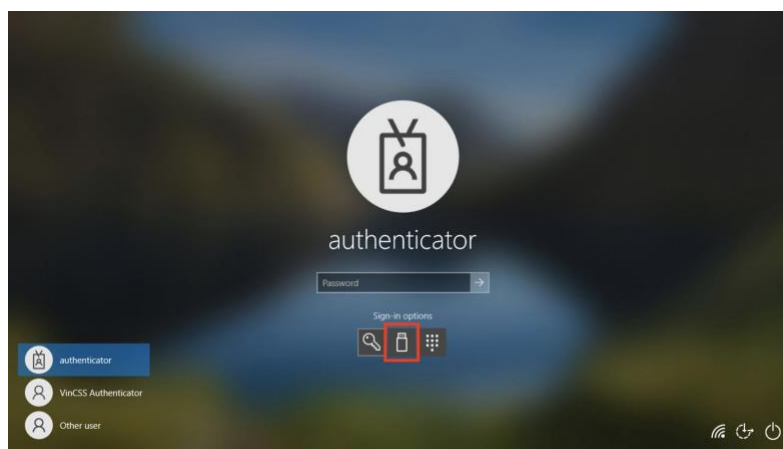


### III.1.2. Đăng nhập Windows 10

- Trên giao diện đăng nhập vào Windows 10, chọn *Sign-in options*.

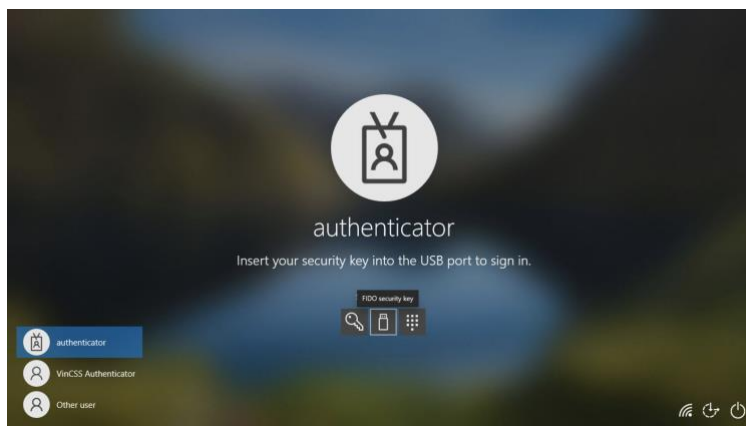


- Để lựa chọn đăng nhập Windows 10 với khoá bảo mật VinCSS FIDO2® Fingerprint thông qua kết nối Bluetooth.

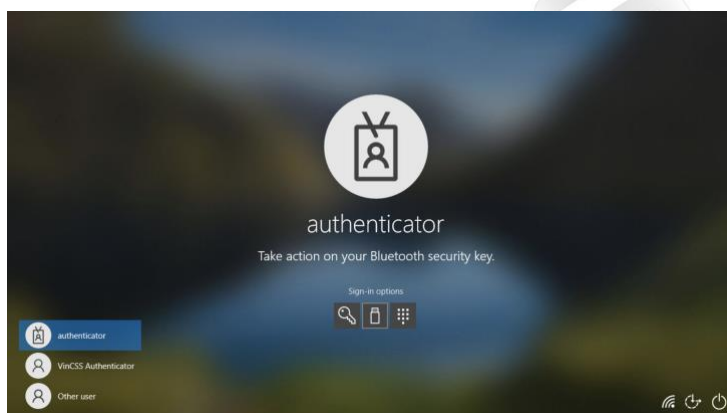


### ***III.1.2.1. Sử dụng qua kết nối Bluetooth***

- Kết nối khoá bảo mật với máy tính thông qua kết nối Bluetooth.

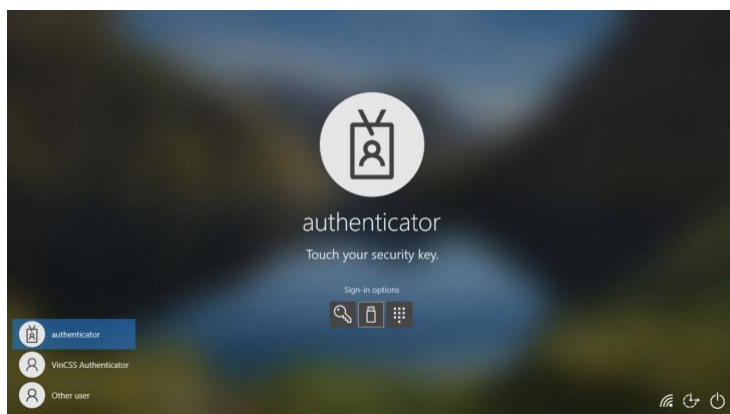


- Quét vân tay khi nhận được thông báo.



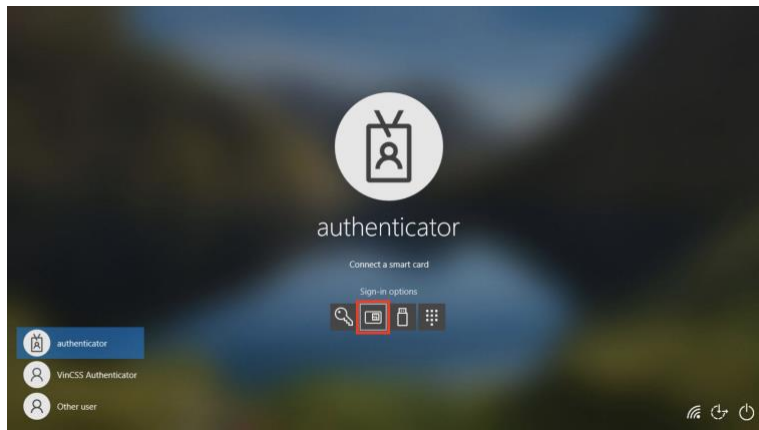
### ***III.1.2.2. Sử dụng qua kết nối USB***

Kết nối khoá bảo mật với máy tính thông qua kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

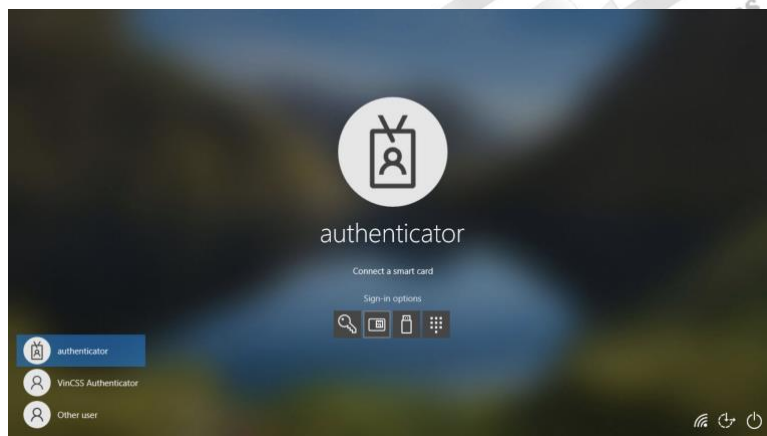


### III.1.2.3. Sử dụng qua kết nối NFC

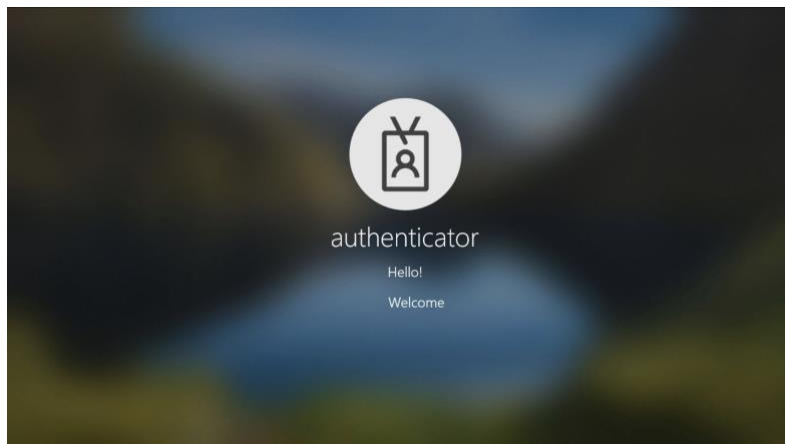
- Để lựa chọn đăng nhập Windows 10 với khoá bảo mật VinCSS FIDO2® Fingerprint thông qua kết nối NFC, chọn biểu tượng smart card như hình bên dưới.



- Kết nối khoá bảo mật với máy tính thông qua kết nối NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



- Đăng nhập thành công.



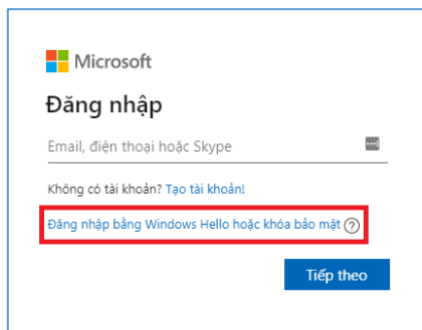
## III.2. Tài khoản Microsoft

### III.2.1. Đăng ký khóa bảo mật

- Tham chiếu mục III.1.1.3.

### III.2.2. Đăng nhập

- Truy cập <https://microsoft.com>, chọn **Đăng nhập**.
- Chọn **Đăng nhập bằng Windows Hello hoặc khóa bảo mật**.

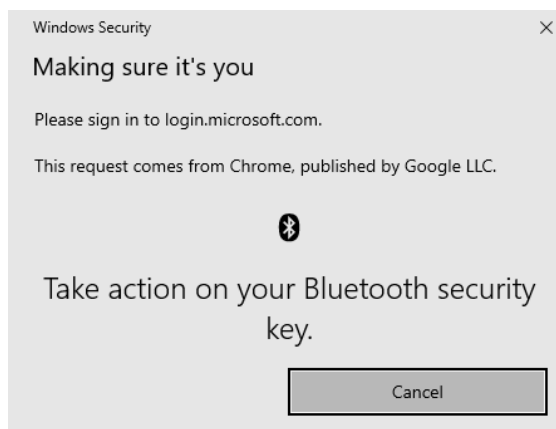


#### III.2.2.1. Sử dụng qua kết nối Bluetooth

- Kết nối khóa bảo mật với máy tính thông qua kết nối Bluetooth.



- Quét dấu vân tay khi nhận được thông báo.





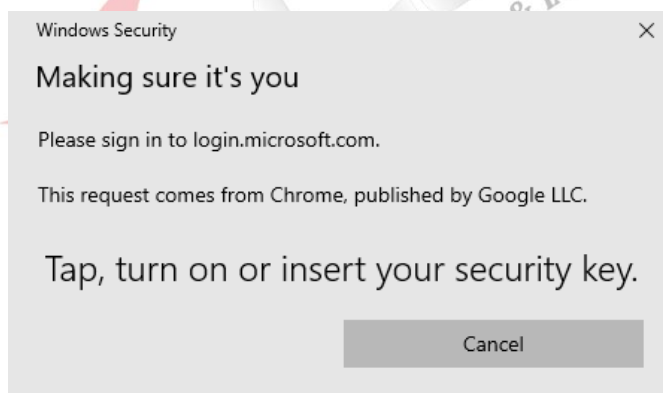
### III.2.2.2. Sử dụng qua kết nối USB

Kết nối khoá bảo mật với máy tính thông qua kết dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

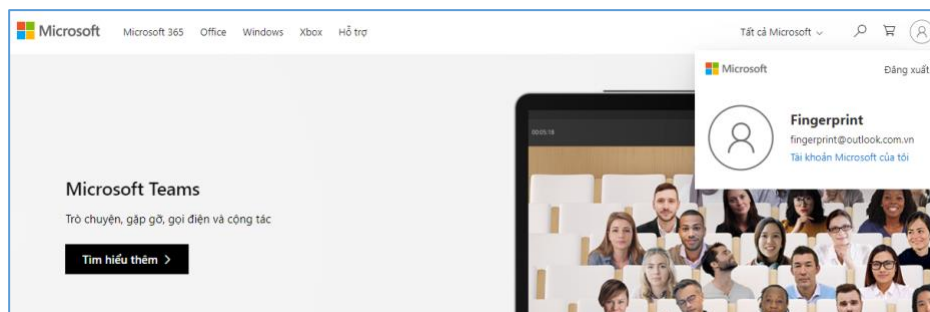


### III.2.2.3. Sử dụng qua kết nối NFC

- Kết nối khoá bảo mật với máy tính thông qua kết dây kết nối NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.

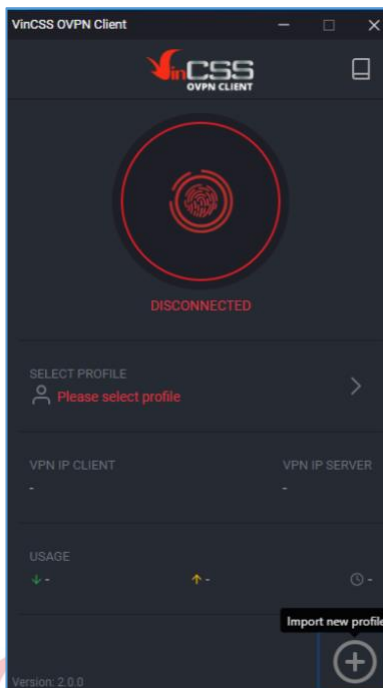


- Đăng nhập thành công.

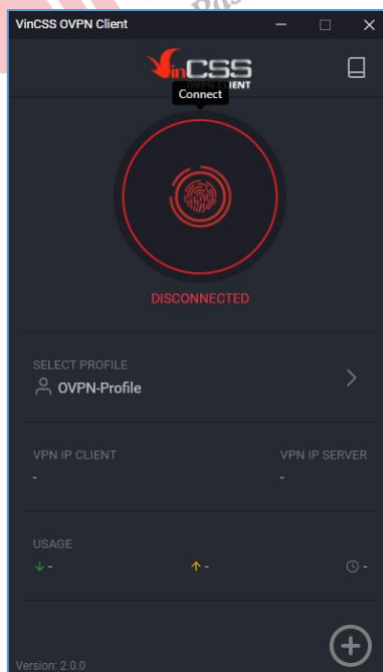


### III.3. VinCSS OVPN Client

- Mở ứng dụng VinCSS OVPN Client, trên giao diện chọn **Import new profile**.

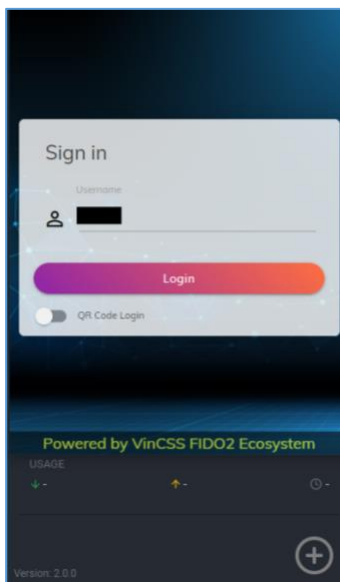


- OVPN profile đã được thêm, tiến hành kết nối VPN, nhấn vào biểu tượng vân tay trên giao diện ứng dụng.



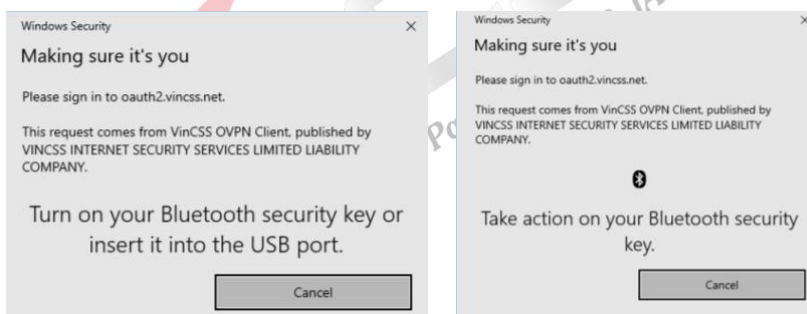
- Nhập **Username** sau đó chọn **Login**. Tiếp theo kết nối khoá bảo mật

## VinCSS FIDO2® Fingerprint vào máy tính.



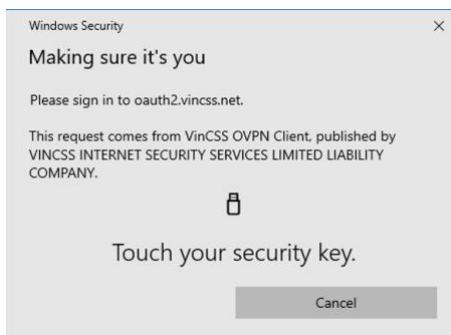
### III.3.1. Sử dụng qua kết nối Bluetooth.

Kết nối khoá bảo mật với máy tính thông qua kết nối Bluetooth, quét dấu vân tay khi nhận được thông báo.



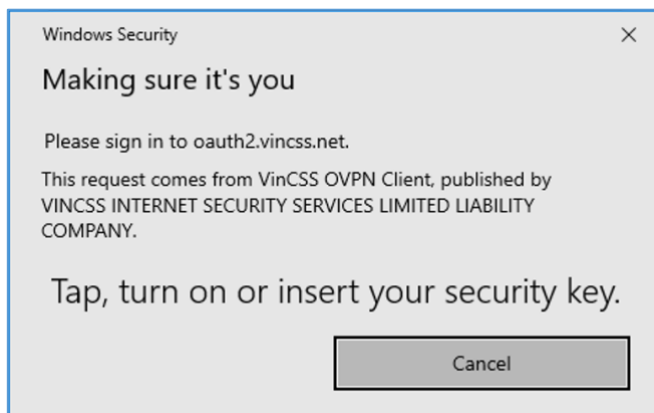
### III.3.2. Sử dụng qua kết nối USB

Kết nối khoá bảo mật với máy tính thông qua kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

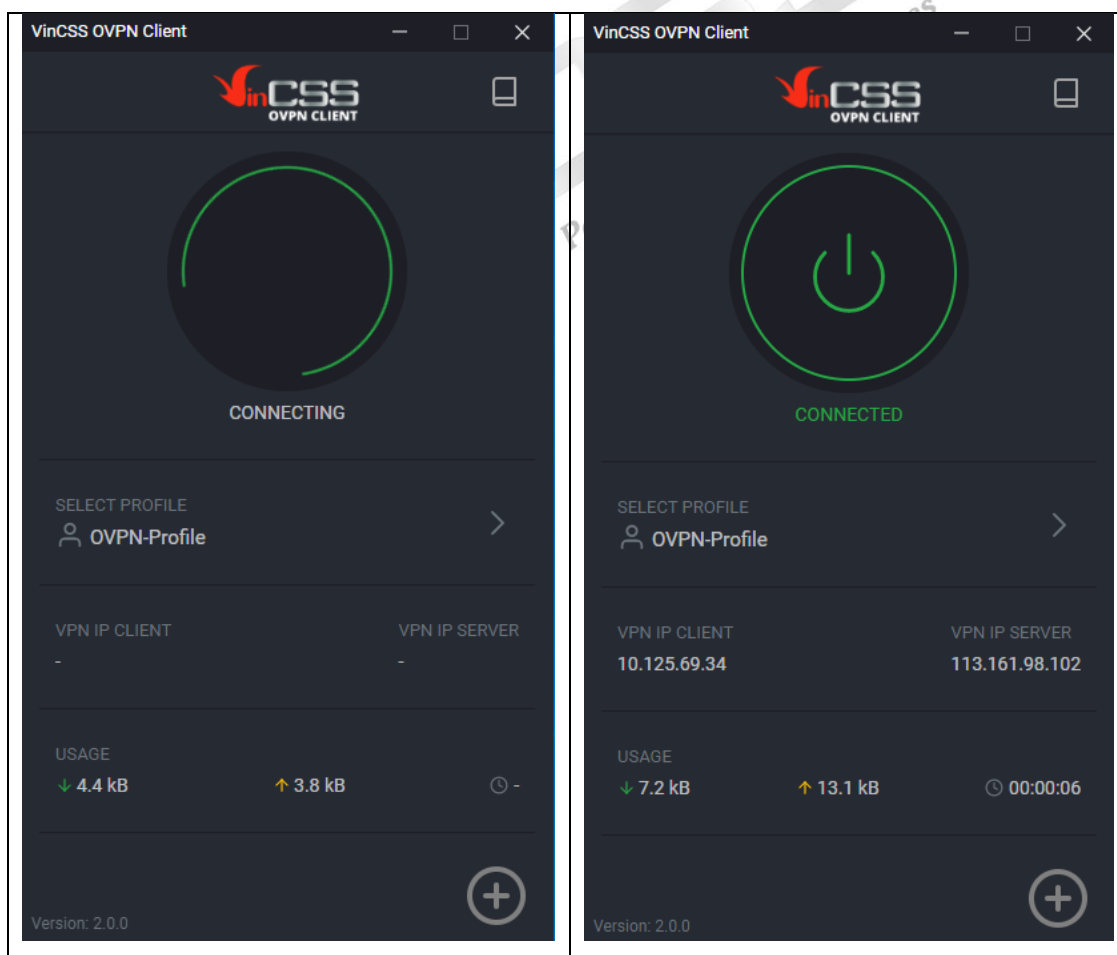


### III.3.3. Sử dụng qua kết nối NFC.

- Kết nối khoá bảo mật với máy tính thông qua kết dây kết nối NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



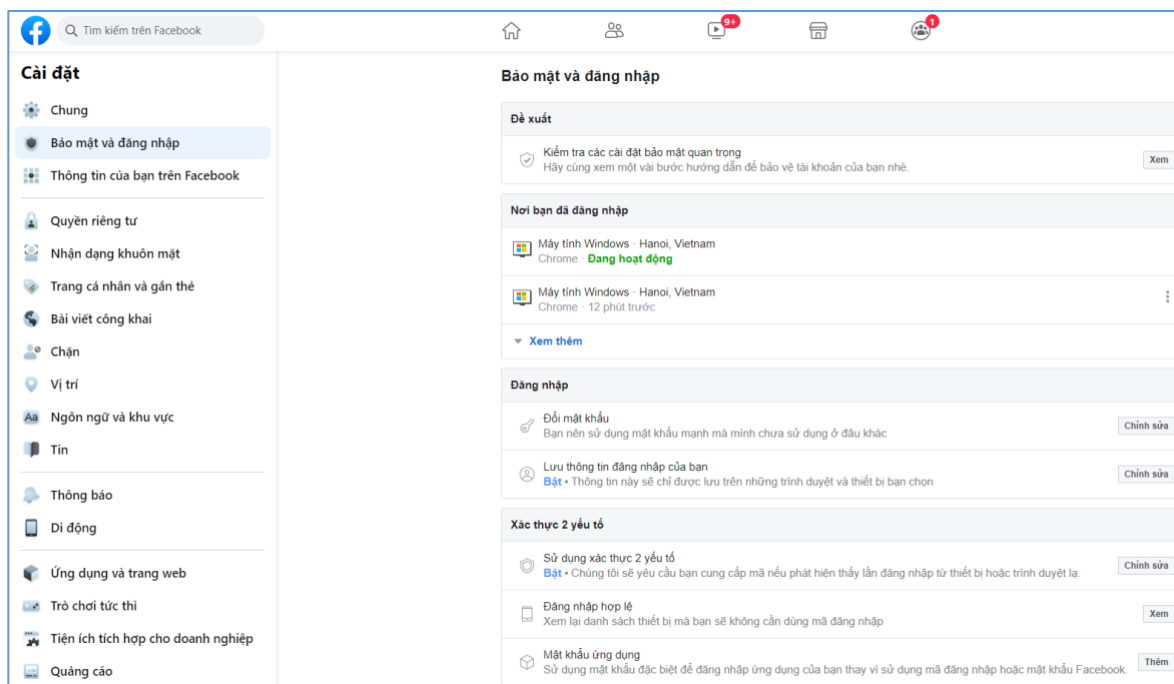
- Quá trình kết nối được tiến hành khi người dùng xác thực thành công. Kết nối VPN thành công, trên giao diện ứng dụng hiển thị trạng thái **CONNECTED**.



### III.4. Xác thực 2 yếu tố tài khoản Facebook

#### III.4.1. Đăng ký khoá bảo mật

- Đăng nhập vào <https://www.facebook.com>, sau đó vào phần **Cài đặt** và chọn **Bảo mật và đăng nhập** bên menu trái. Tại mục **Xác thực 2 yếu tố**, chọn thay đổi thiết lập **Sử dụng xác thực 2 yếu tố**.



- Nếu chưa bật xác thực 2 yếu tố trước đó, người dùng được yêu cầu phải bổ sung phương thức xác thực qua OTP trên ứng dụng Google Authenticator hoặc SMS. Ví dụ dưới đây cho nhận mã OTP qua SMS.



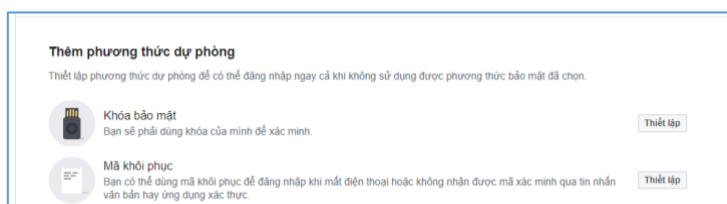
- Nhập mã đã gửi về trên điện thoại.



- Xác nhận thành công.



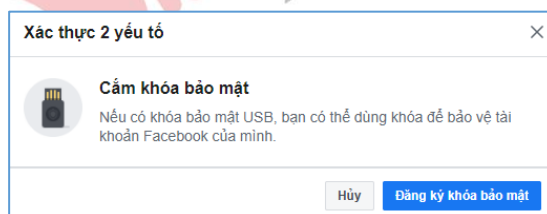
- Tại mục **Thêm phương thức dự phòng**, chọn **Khóa bảo mật (thiết lập)**.



- Chọn **Đăng ký khoá bảo mật**.

#### III.4.1.1. Sử dụng qua kết nối Bluetooth.

- Sau đó kết nối khoá bảo mật VinCSS FIDO2® Fingerprint vào máy tính thông qua Bluetooth.



- Quét vân tay khi nhận được thông báo.



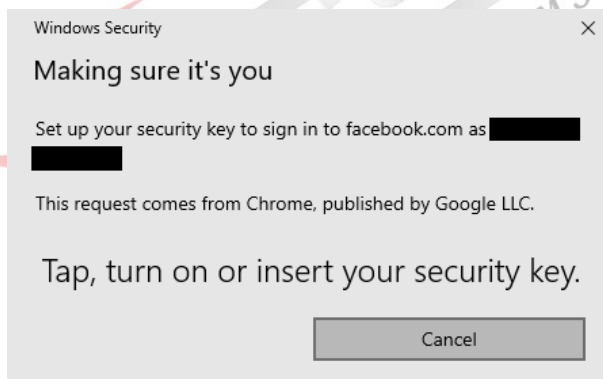
### III.4.1.2. Sử dụng qua kết nối USB

Kết nối khoá bảo mật với máy tính thông qua kết dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

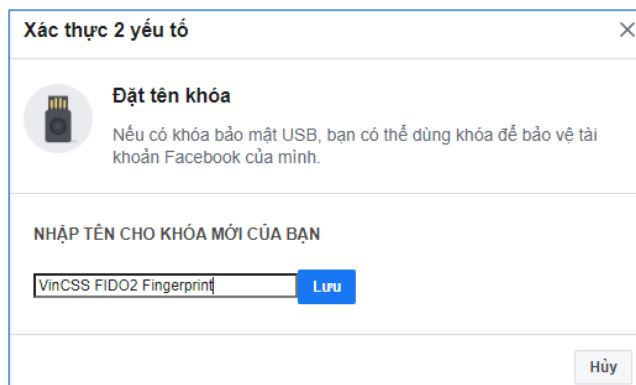


### III.4.1.3. Sử dụng qua kết nối NFC

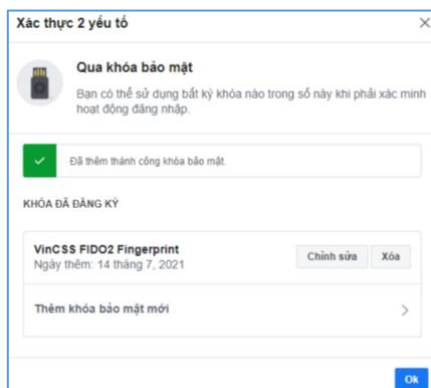
- Kết nối khoá bảo mật với máy tính thông qua kết dây kết nối NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



- Đặt tên cho khoá bảo mật để phân biệt giữa các khoá, sau đó nhấn **Lưu** để lưu lại thông tin khoá.



- Thông tin khoá bảo mật đã được đăng ký thành công.

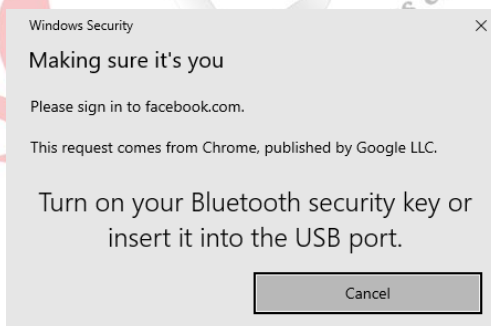


### III.4.2. Xác thực 2 yếu tố với dịch vụ Facebook

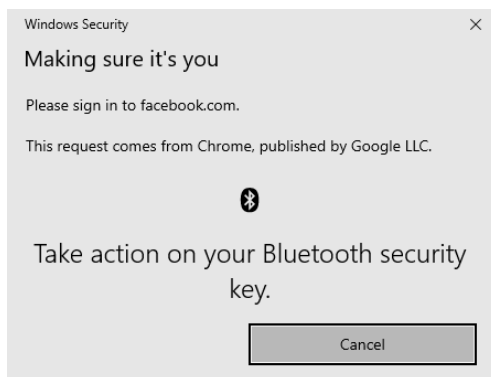
- Truy cập <https://www.facebook.com> rồi đăng nhập với username và password.
- Sau khi xác thực với mật khẩu, trình duyệt yêu cầu người dùng thực hiện xác thực bằng khóa bảo mật.

#### III.4.2.1. Sử dụng qua kết nối Bluetooth.

- Kết nối khoá bảo mật với máy tính thông qua kết nối Bluetooth.



- Quét vân tay khi nhận được thông báo.





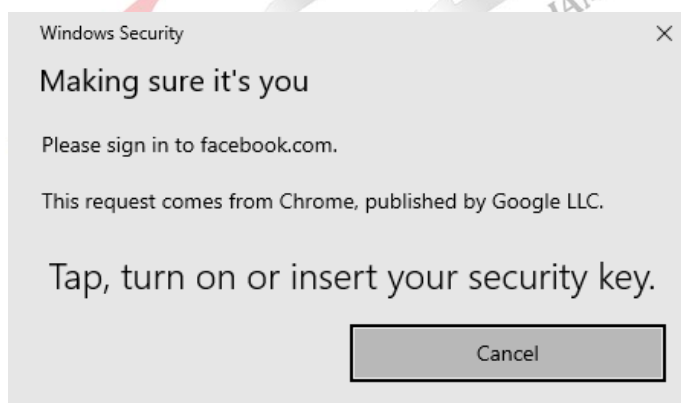
### III.4.2.2. Sử dụng qua kết nối USB

Kết nối khoá bảo mật với máy tính thông qua kết dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.



### III.4.2.3. Sử dụng qua kết nối NFC

- Kết nối khoá bảo mật với máy tính thông qua kết dây kết nối NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



- Xác thực thành công.

**Nhớ trình duyệt**

Khi đã lưu trình duyệt, nếu đăng nhập lại cũng từ trình duyệt này thì bạn sẽ không phải nhập mã xác minh nữa.

☐ Lưu trình duyệt

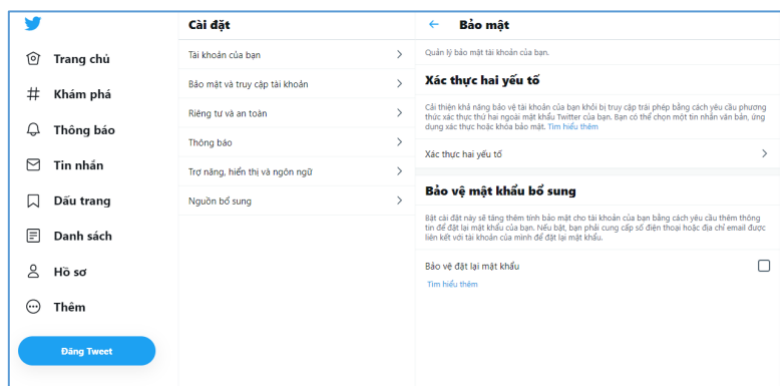
☒ Đừng lưu

**Tiếp tục**

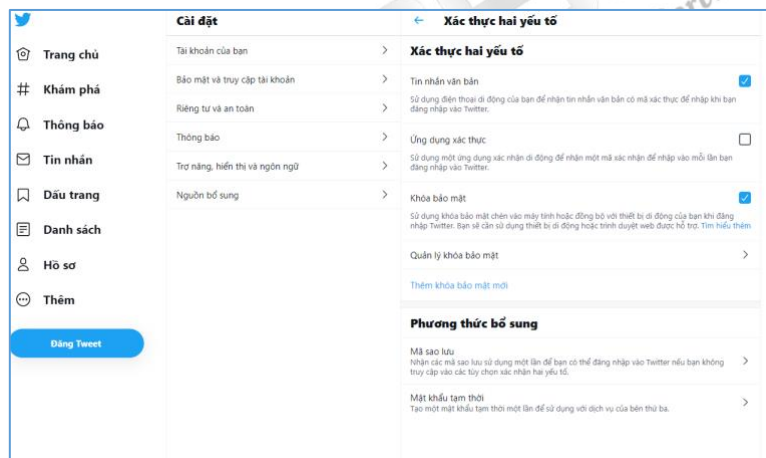
### III.5. Xác thực 2 yếu tố với Twitter

#### III.5.1. Đăng ký khoá bảo mật

- Đăng nhập vào <https://twitter.com>, sau đó vào phần **Thêm** chọn **Cài đặt và riêng tư** bên menu trái. Tại mục **Bảo mật và truy cập tài khoản**, chọn thay đổi thiết lập **Xác thực 2 yếu tố**.



- Chọn mục **Thêm khoá bảo mật mới**.

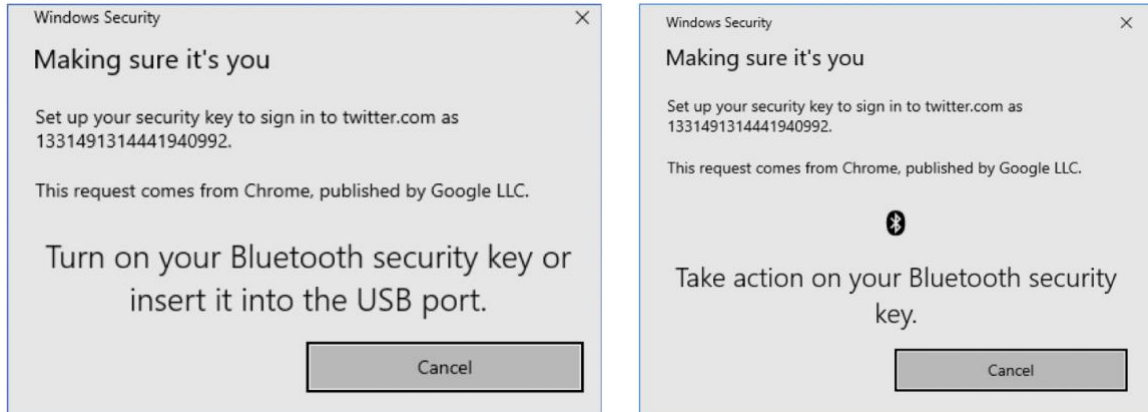


- Chọn **Bắt đầu** để thiết lập khoá bảo mật.



### ***III.5.1.1. Sử dụng qua kết nối Bluetooth.***

Kết nối khoá bảo mật VinCSS FIDO2® Fingerprint với máy tính thông qua Bluetooth. Quét vân tay khi nhận được thông báo.



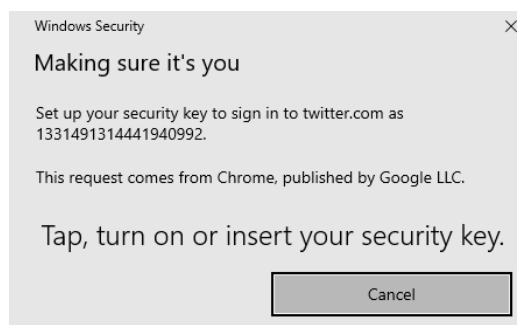
### ***III.5.1.2. Sử dụng qua kết nối USB***

Kết nối khoá bảo mật với máy tính thông qua kết dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

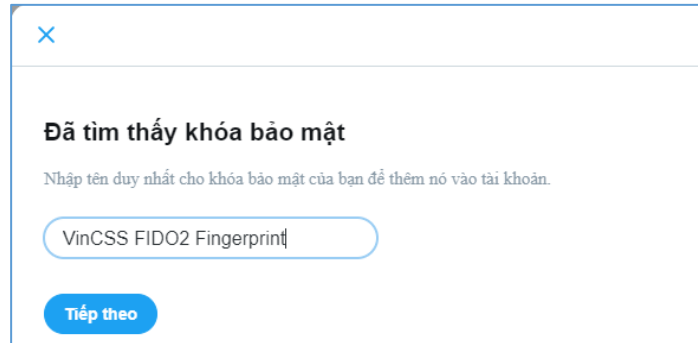


### ***III.5.1.3. Sử dụng qua kết nối NFC***

- Kết nối khoá bảo mật với máy tính thông qua kết dây kết nối NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.

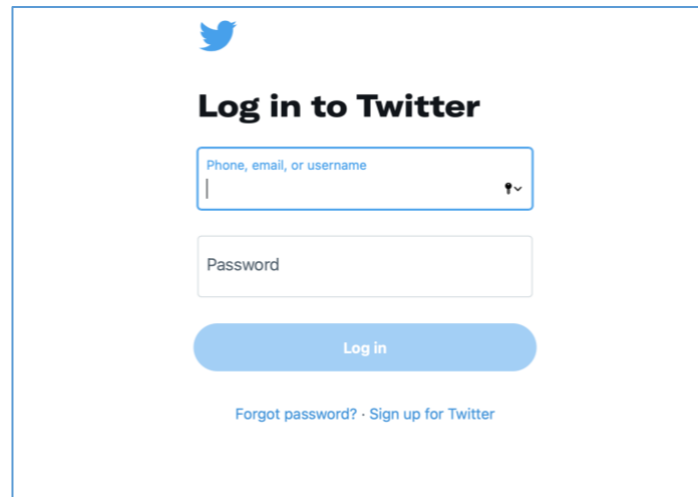


- Đặt tên cho khóa bảo mật để phân biệt giữa các khóa. Sau đó nhấn **Tiếp theo**.



### III.5.2. Xác thực 2 yếu tố với dịch vụ Twitter

- Truy cập <https://www.twitter.com> rồi đăng nhập với username và password.



- Sau khi xác thực với password, chọn **Chọn phương thức xác thực hai yếu tố khác**.



- Chọn **Khoá bảo mật**.

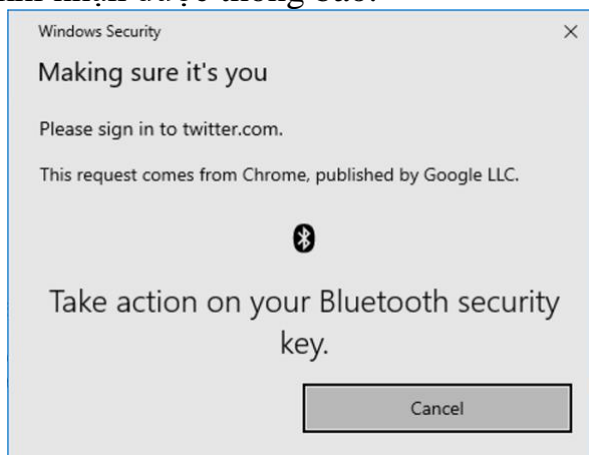


### III.5.2.1. Sử dụng qua kết nối Bluetooth.

- Người dùng kết nối khoá bảo mật VinCSS FIDO2® Fingerprint với máy tính thông qua Bluetooth.



- Quét vân tay khi nhận được thông báo.



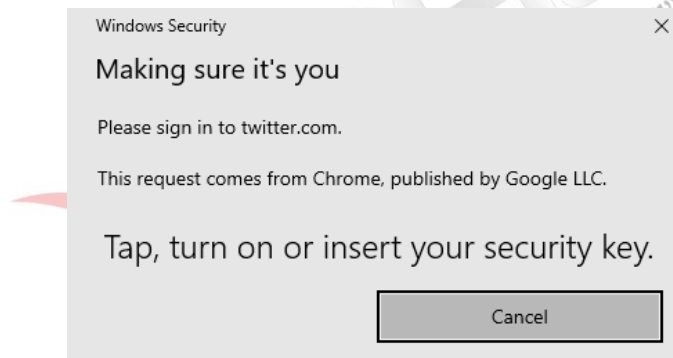
### III.5.2.2. Sử dụng qua kết nối USB

Kết nối khoá bảo mật với máy tính thông qua kết dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.



### III.5.2.3. Sử dụng qua kết nối NFC

- Kết nối khoá bảo mật với máy tính thông qua kết dây kết nối NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



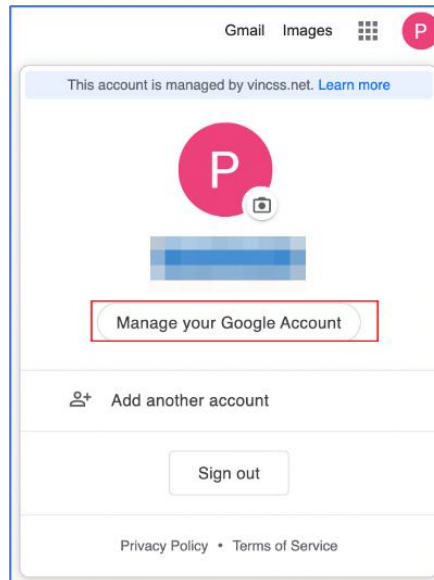
## III.6. Xác thực 2 yếu tố với Google

### III.6.1. Đăng ký khoá bảo mật

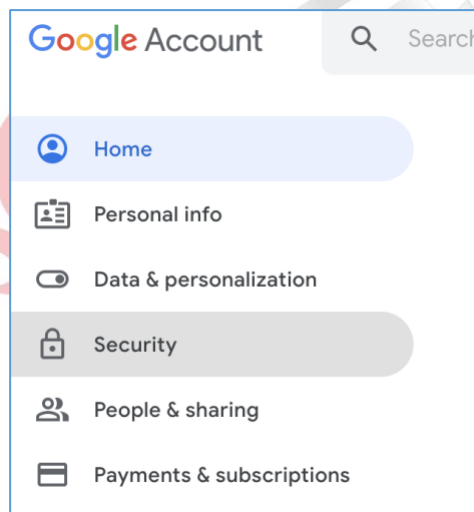
- Truy cập vào <https://accounts.google.com>, đăng nhập với username và mật khẩu.



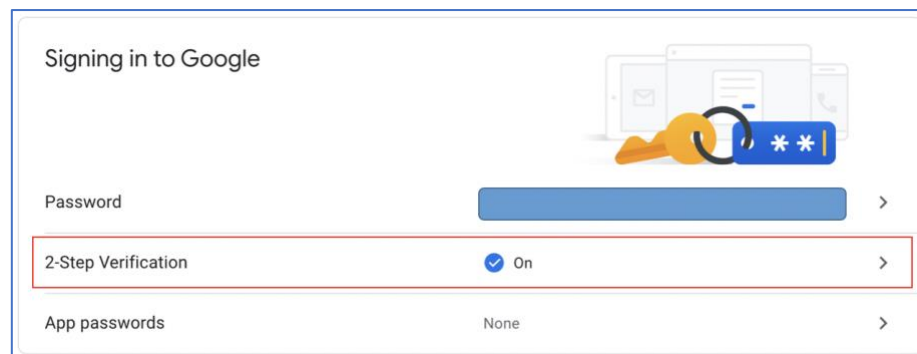
- Bấm vào biểu tượng account gốc trên bên phải, chọn **Manage your Google Account**.



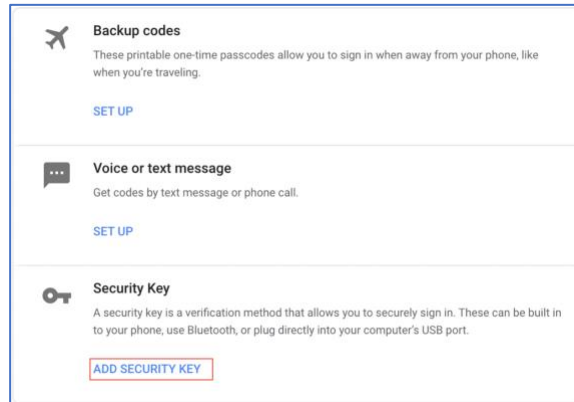
- Chọn mục **Security** tại menu bên trái.



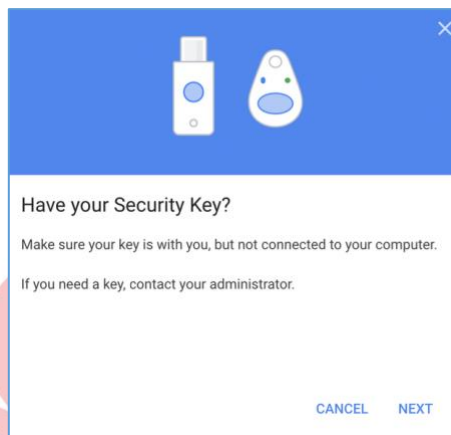
- Chọn mục **2-Step Verification** để thiết lập xác thực hai yếu tố.



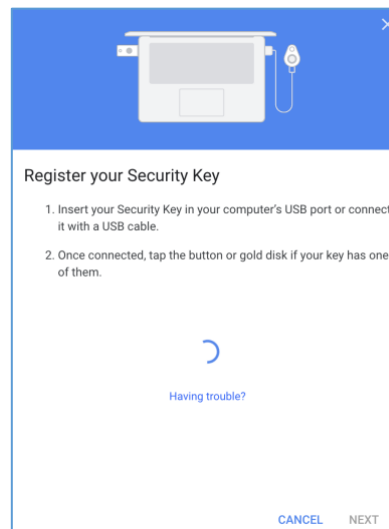
- Chọn **ADD SECURITY KEY** từ danh sách các phương thức xác thực.



- Chọn **Next** để khai báo khóa bảo mật.



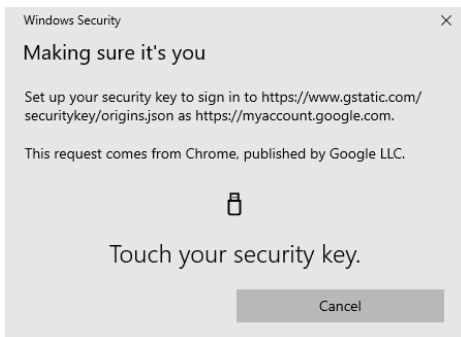
- Khi xuất hiện màn hình **Register your Security Key**, kết nối VinCSS FIDO2® Fingerprint vào máy tính.





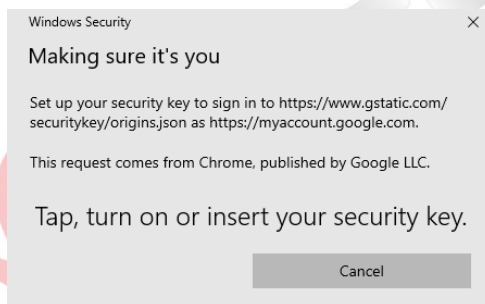
### III.6.1.1. Sử dụng qua kết nối USB

Kết nối khoá bảo mật với máy tính thông qua kết dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

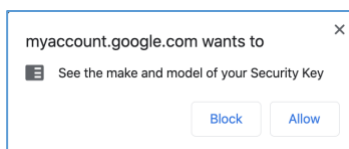


### III.6.1.2. Sử dụng qua kết nối NFC

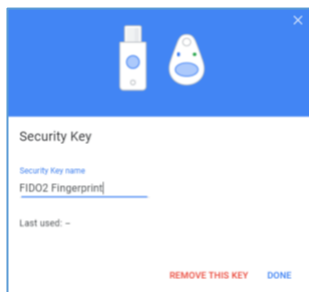
- Kết nối khoá bảo mật với máy tính thông qua kết dây kết nối NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



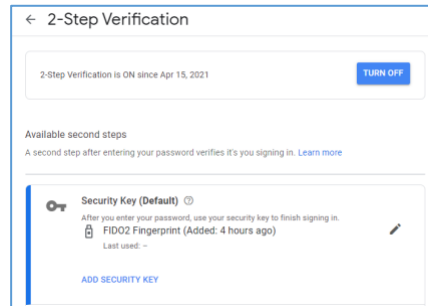
- Tại bước này, trình duyệt có thể yêu cầu được truy xuất thông tin của khóa bảo mật, chọn **Allow** để tiếp tục.



- Đặt tên cho thiết bị khóa bảo mật để dễ phân biệt trong trường hợp người dùng sử dụng đồng thời nhiều khóa, nhấn **Done** để xác nhận.

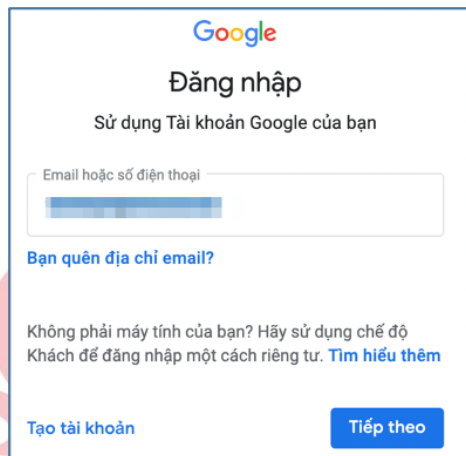


- Hoàn thành đăng ký, từ thời điểm này mọi dịch vụ của Google yêu cầu người dùng đăng nhập phải xác thực với cả mật khẩu và khóa bảo mật



### III.6.2. Xác thực 2 yếu tố với dịch vụ Google

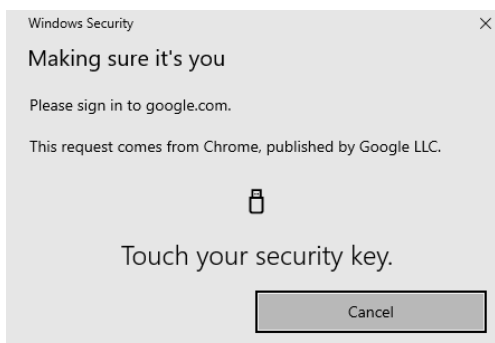
- Truy cập vào <https://accounts.google.com> rồi đăng nhập bằng username và mật khẩu.



- Sau khi xác thực với mật khẩu, trình duyệt yêu cầu người dùng thực hiện xác thực bằng khóa bảo mật.

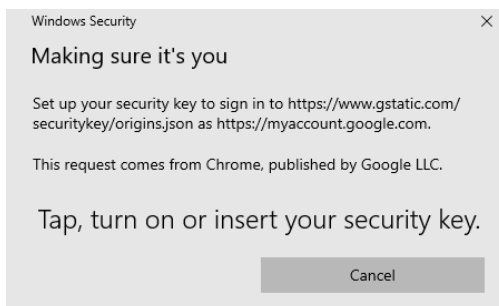
#### III.6.2.1. Sử dụng qua kết nối USB

Người dùng kết nối VinCSS FIDO2® Fingerprint vào máy tính thông qua kết nối USB. Chạm vào phần quét vân tay trên khoá bảo mật VinCSS FIDO2® Fingerprint khi nhận được thông báo.



### **III.6.2.2. Sử dụng qua kết nối NFC**

- Kết nối khoá bảo mật với máy tính thông qua kết dây kết nối NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



- Quá trình đăng nhập thành công, người dùng vào được tài khoản.

