# STRONGKEY™

## Tellaro SB2

# Yubico Yubikey 5C NFC
# User Guide for Windows 10

# I Prerequisites

- Windows 10
- Microsoft (MS) Edge Browser, version 141.0.3537.99
- Yubikey 5C NFC
- Internet connection
- ZIP file issued by an SB2 platform
- USB-C port or USB-C-to-USB-A adapter

# II Table of Contents

## A1 Installing the Yubico Authenticator Application

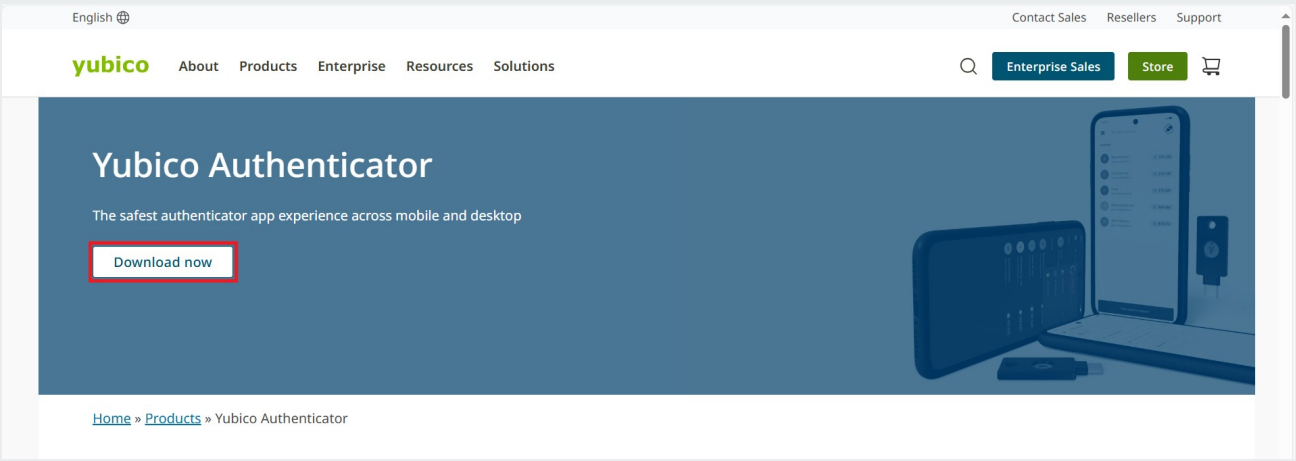
The Yubico Authenticator application is necessary to access and configure the Yubikey 5C NFC Security Key settings and features.

## A2 Prerequisites

- Windows 10
- Microsoft (MS) Edge Browser, version 141.0.3537.99
- Internet connection

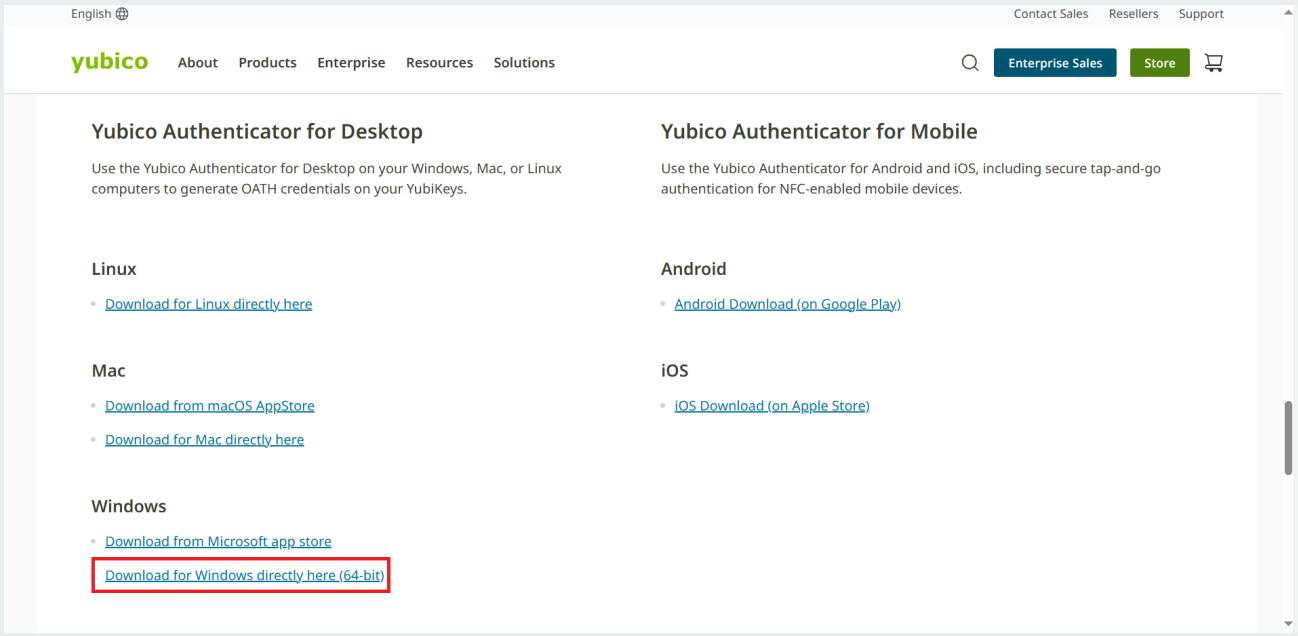
# A3 Download Yubico Authenticator Application

Download the Yubico Authenticator for 64-bit systems from https://www.yubico.com/products/yubico-authenticator. **Click Download now.**



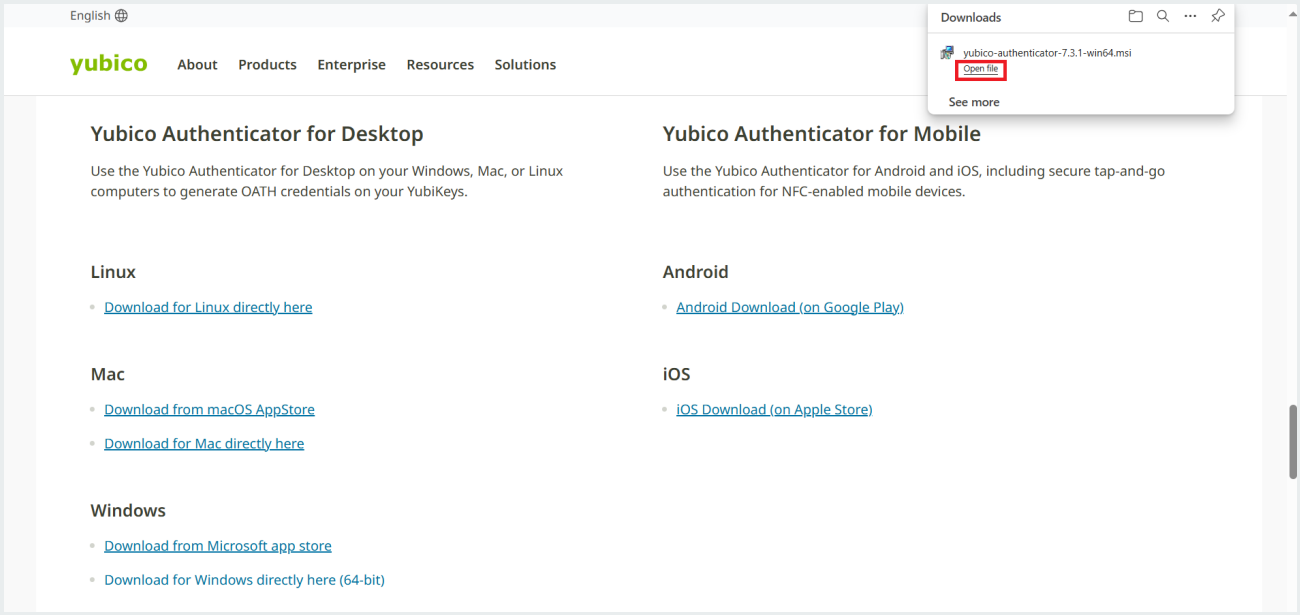
# A4 Windows Yubico Authenticator Application

Select **Download for Windows directly here (64-bit). Click it** to start download.



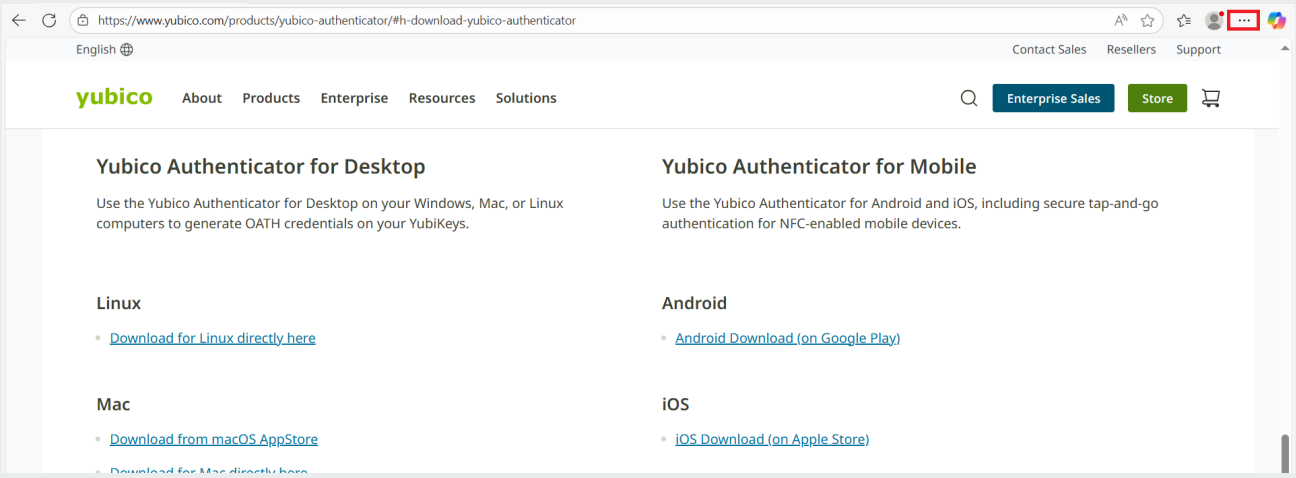
# A5 Opening the Yubico Authenticator Application File

After clicking the download link, MS Edge will display a pop-up confirming the Authenticator application file has been successfully downloaded and ready for installation. **Click the open file link.**



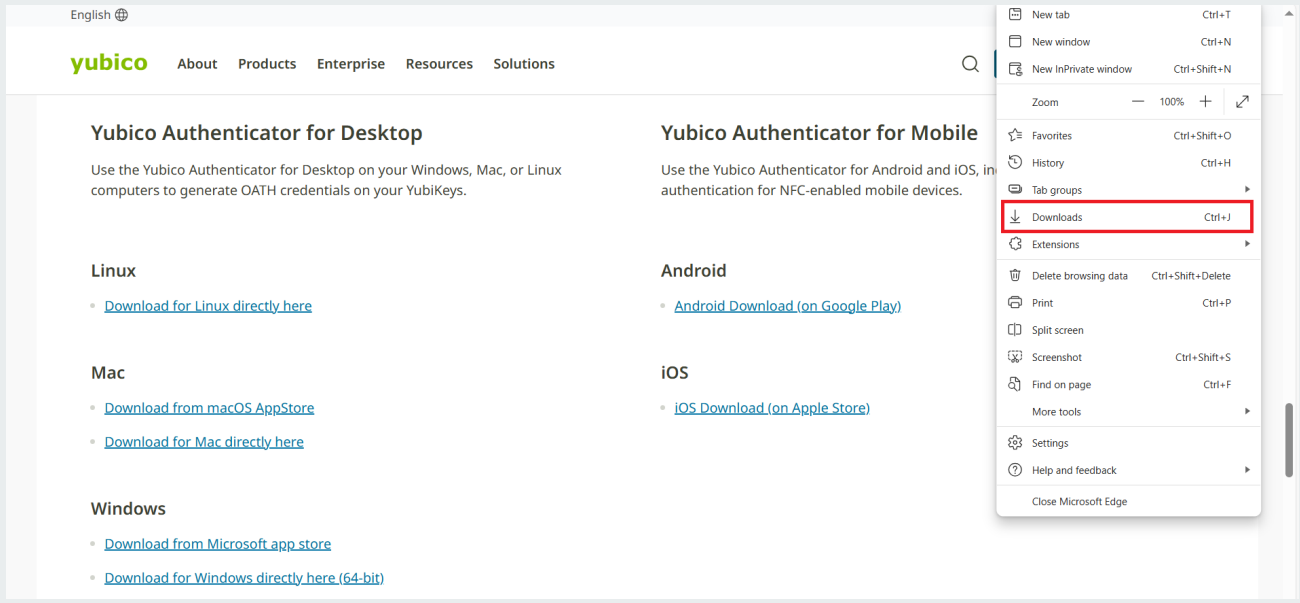
# A6 No pop-up window?

If the pop-up does not appear, or is inadvertently closed, access the downloaded file by clicking the **3-dot menu** on the right side of the MS Edge tool bar.



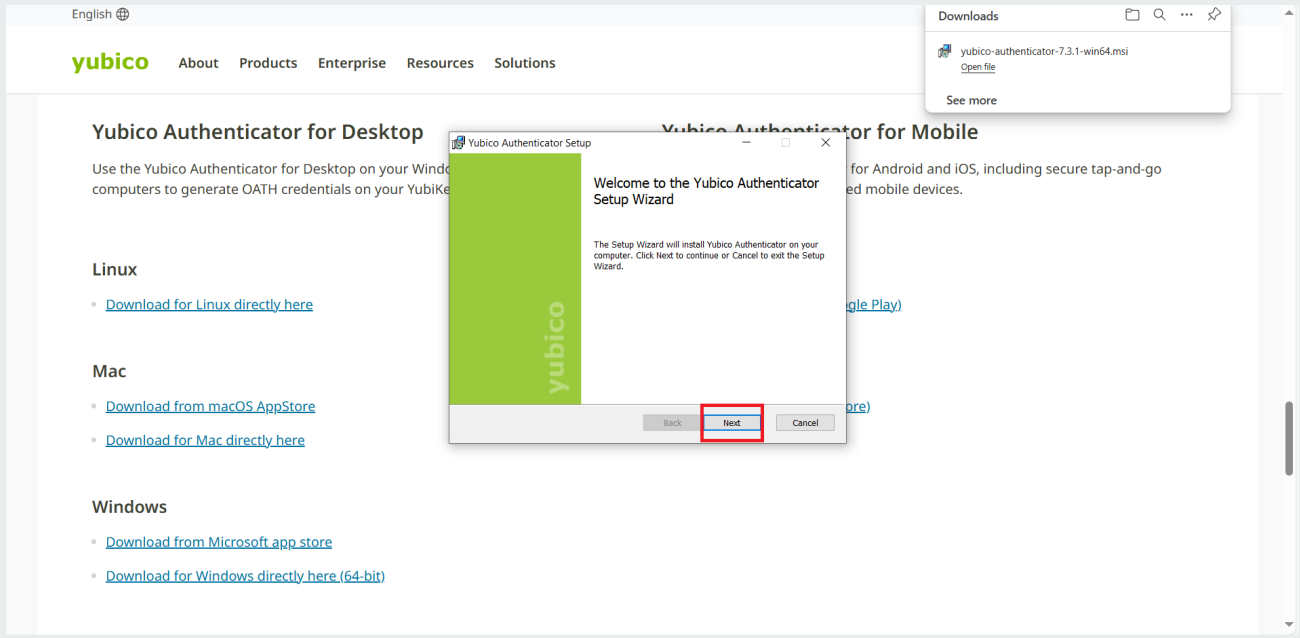
# A7 Click Downloads

From the drop-down menu, select **Downloads.**



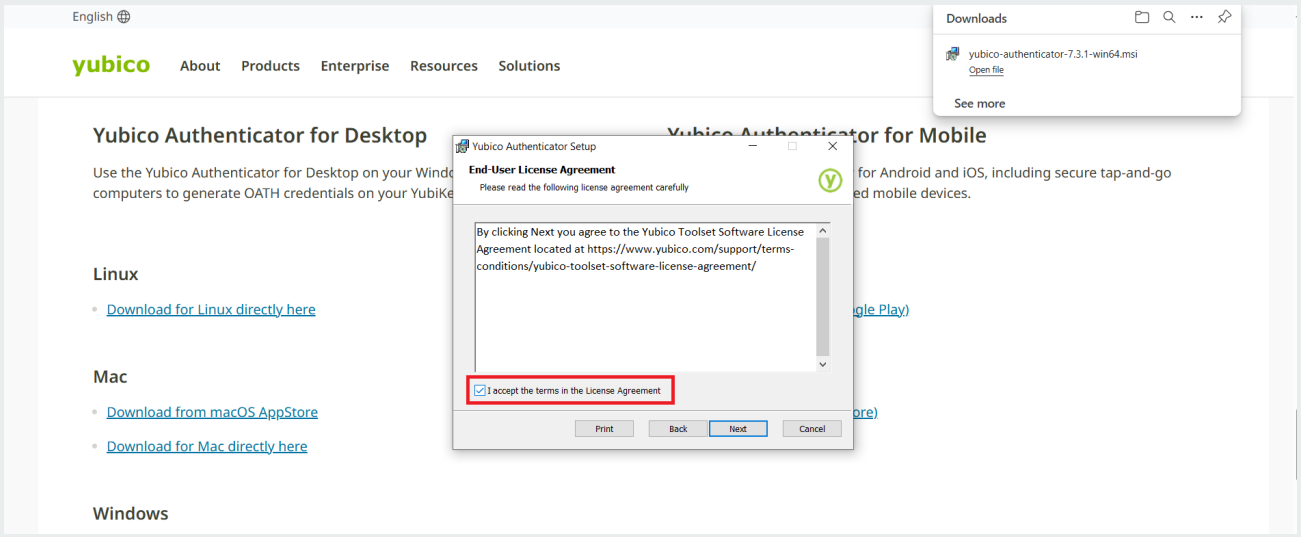
# A8 Yubico Authenticator Setup Wizard

A Setup Wizard window will appear, **Click Next.**



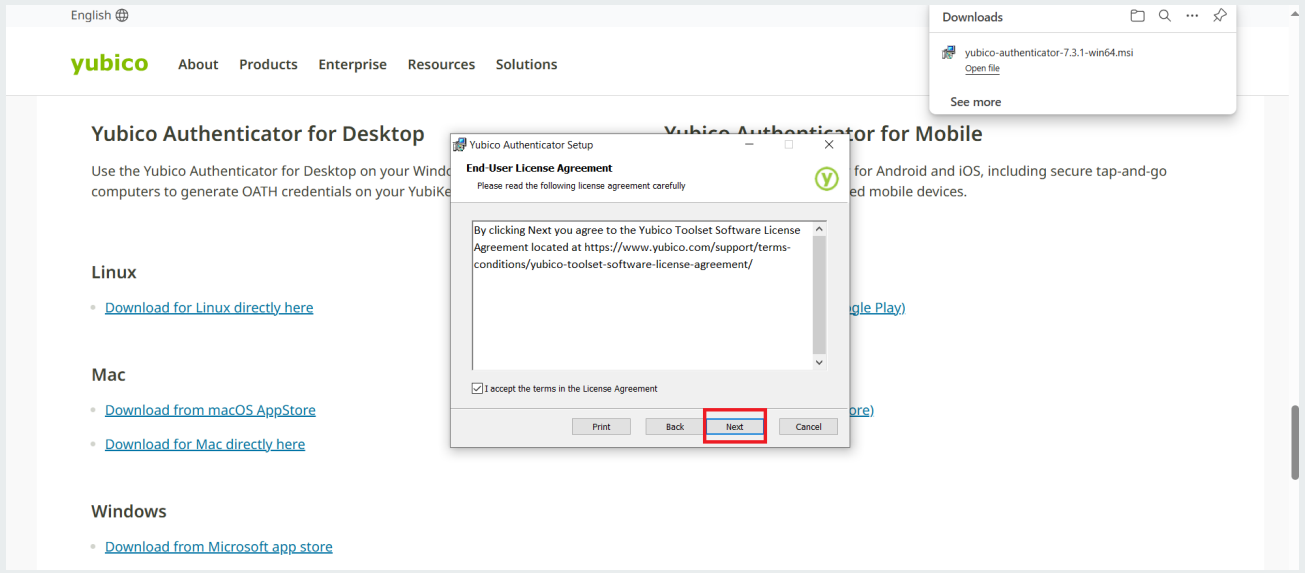
# A9 Yubico Authenticator Application Terms & Conditions

Accept the terms of the end-user license agreement.



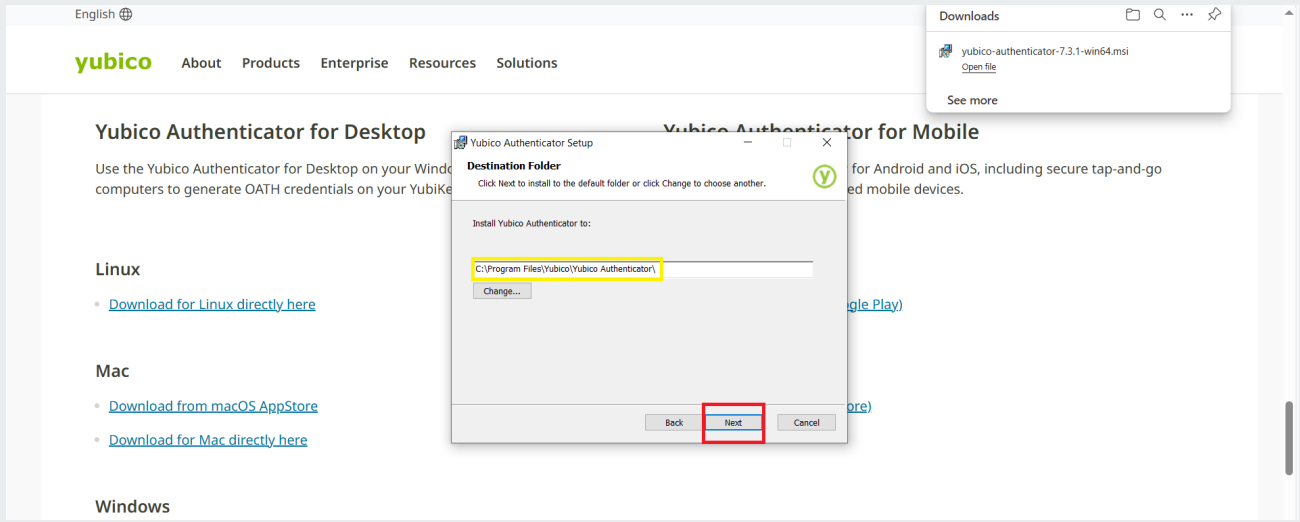
# A10 Yubico Authenticator Application Terms & Conditions

**Click Next** on the end-user license agreement window.



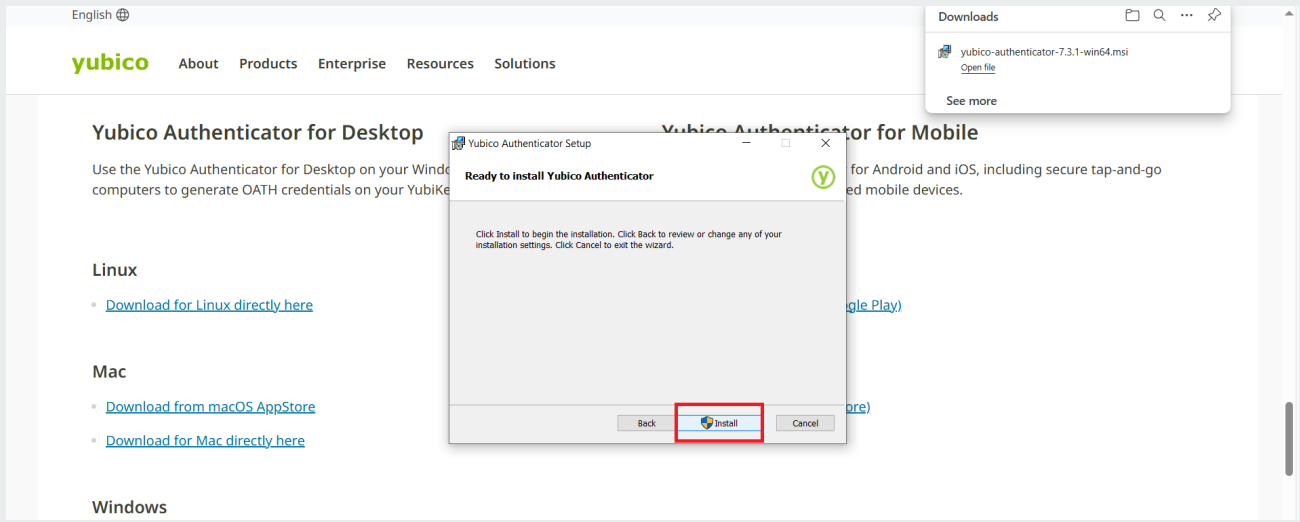
# A11 Select Destination Folder

Use the default Destination Folder and **Click Next.**




# A12 Ready to Install

Click Install.

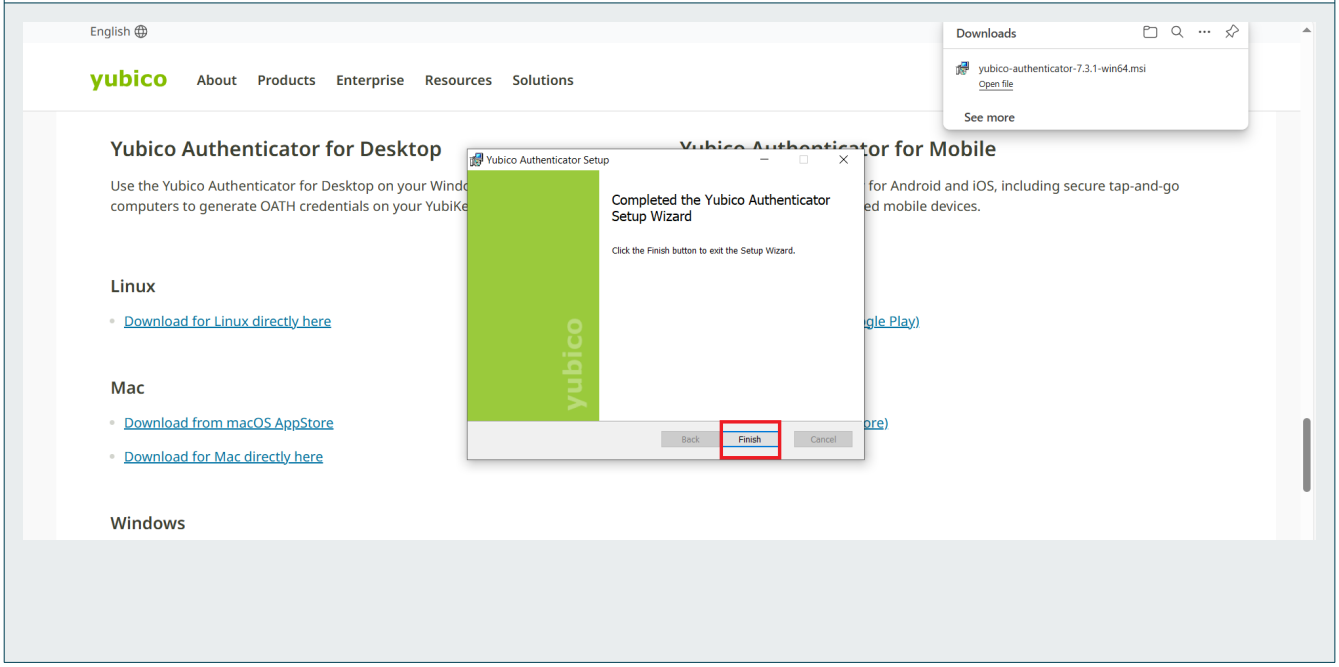


## A13 Permission to make changes

The next pop-up message will ask permission to allow the application to make changes on your computer.  Click **YES**.

## A14 Finish the install

To complete the installation of the Yubico Authenticator application, click **Finish**.




The installation of the Yubico Authenticator application is now complete.

# SECTION B

## B1 Installing the Yubikey Minidriver for Windows

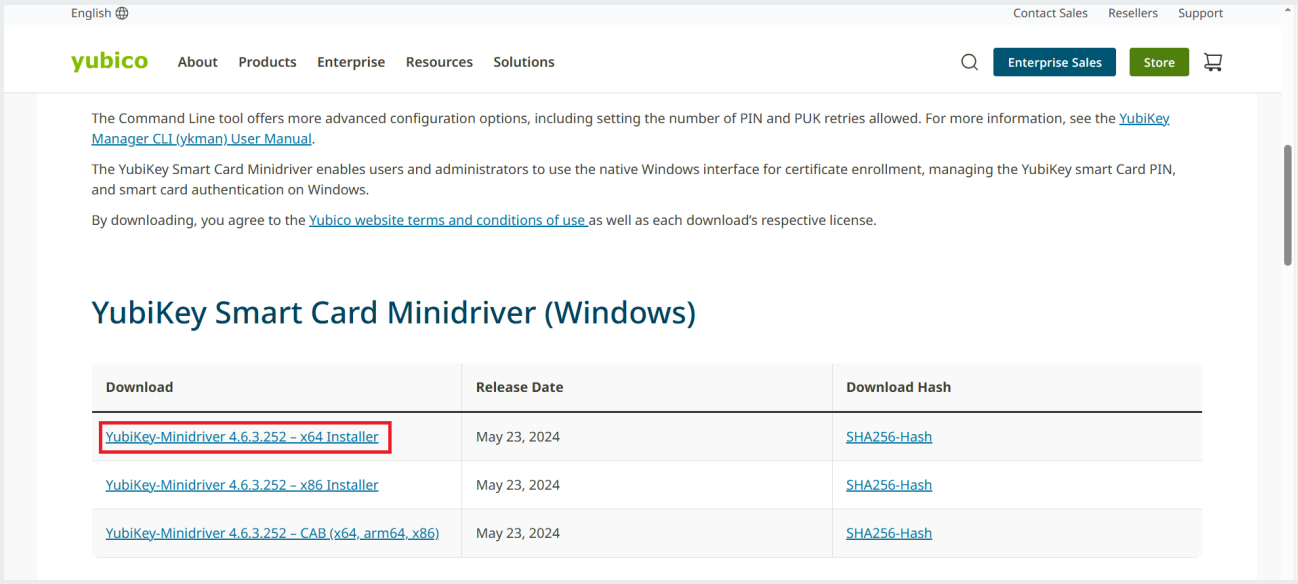
This software is essential for enabling the use of a Yubico Yubikey 5C NFC Security Key on your computer. Before beginning the installation process, please review the process and ensure your computer meets all prerequisites.

## B2 Prerequisites

- Windows 10
- Microsoft (MS) Edge Browser, version 141.0.3537.99
- Internet connection

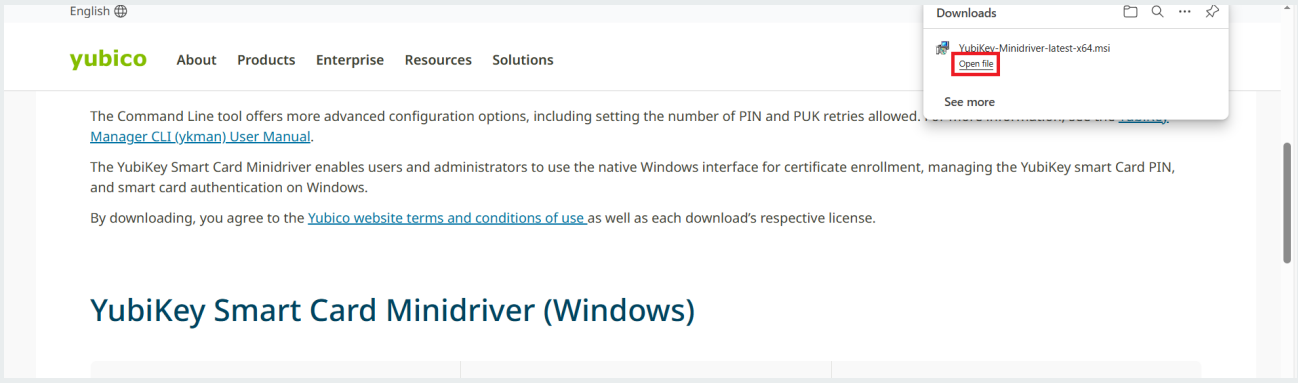
# B3 Download Yubikey Minidriver

Download Yubikey Minidriver for 64-bit systems from
https://www.yubico.com/support/download/smart-card-drivers-tools/



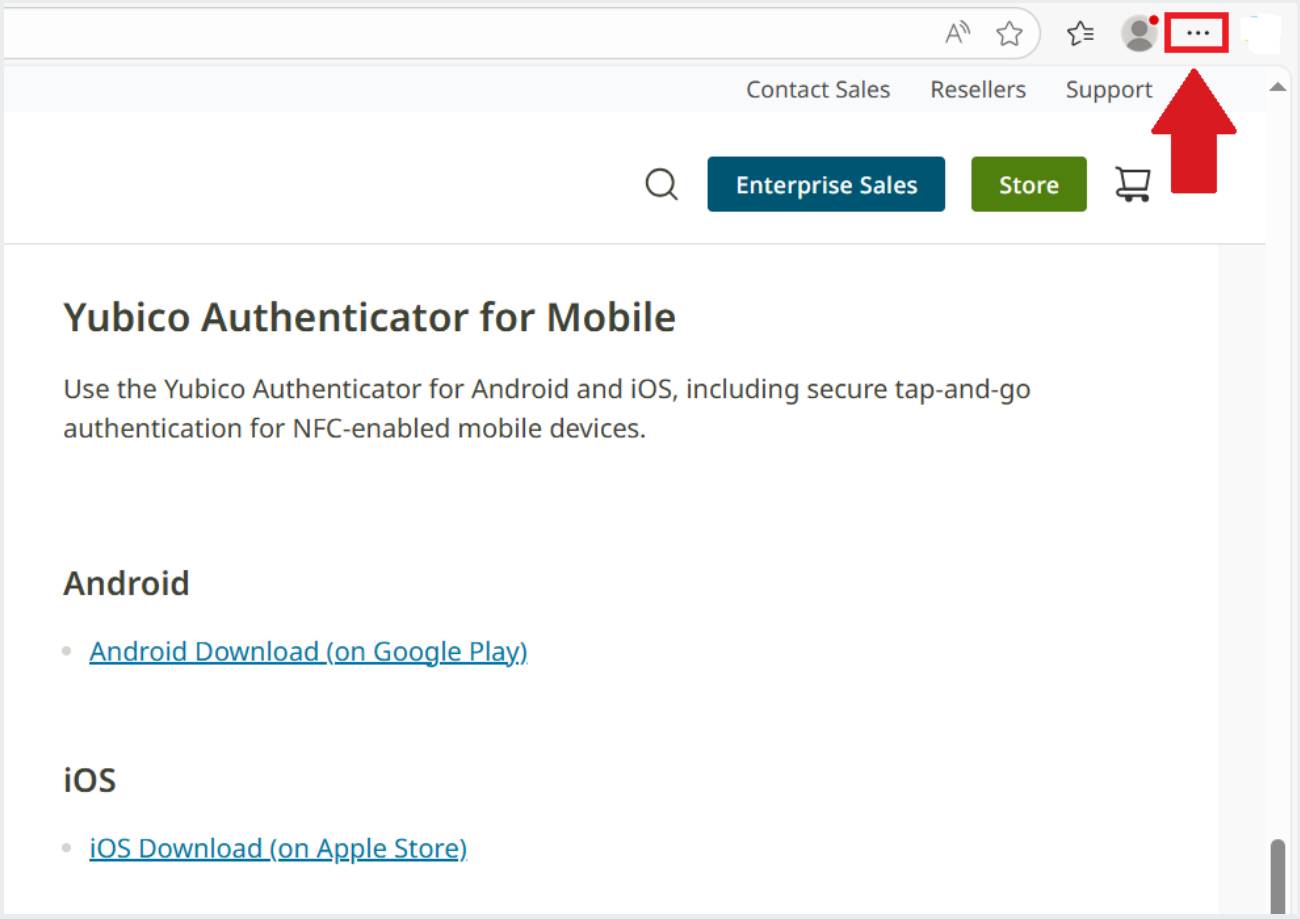
# B4 Opening the Yubikey Minidriver File

After clicking the download link, MS Edge will display a pop-up confirming the Minidriver file has been successfully downloaded and ready for installation.
**Click the open file link.**



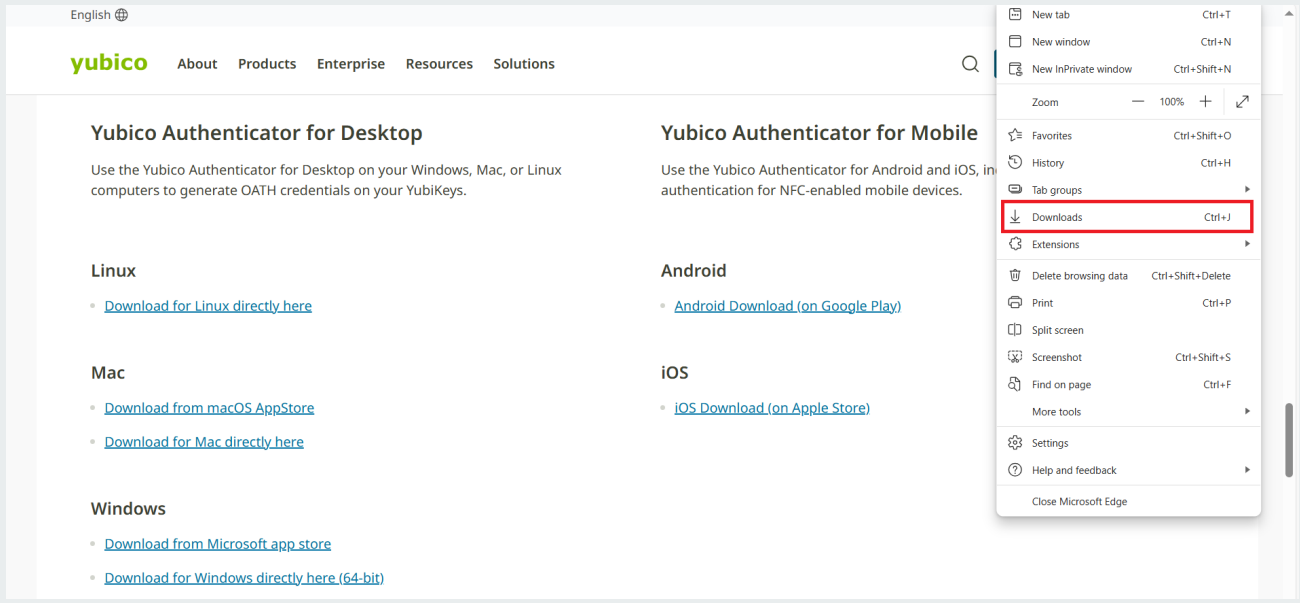
## B5 No pop-up window?

If the pop-up does not appear, or is inadvertently closed, access the downloaded file by clicking the 3-dot menu on the right side of the MS Edge tool bar.



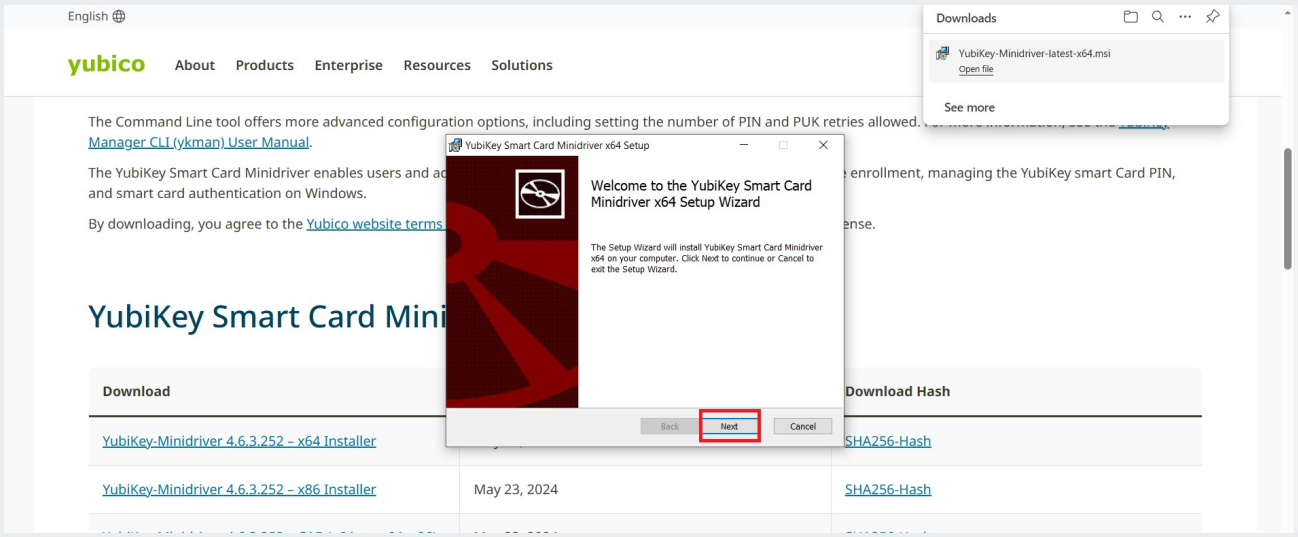
# B6 Click Downloads

From the drop-down menu, select **Downloads.**



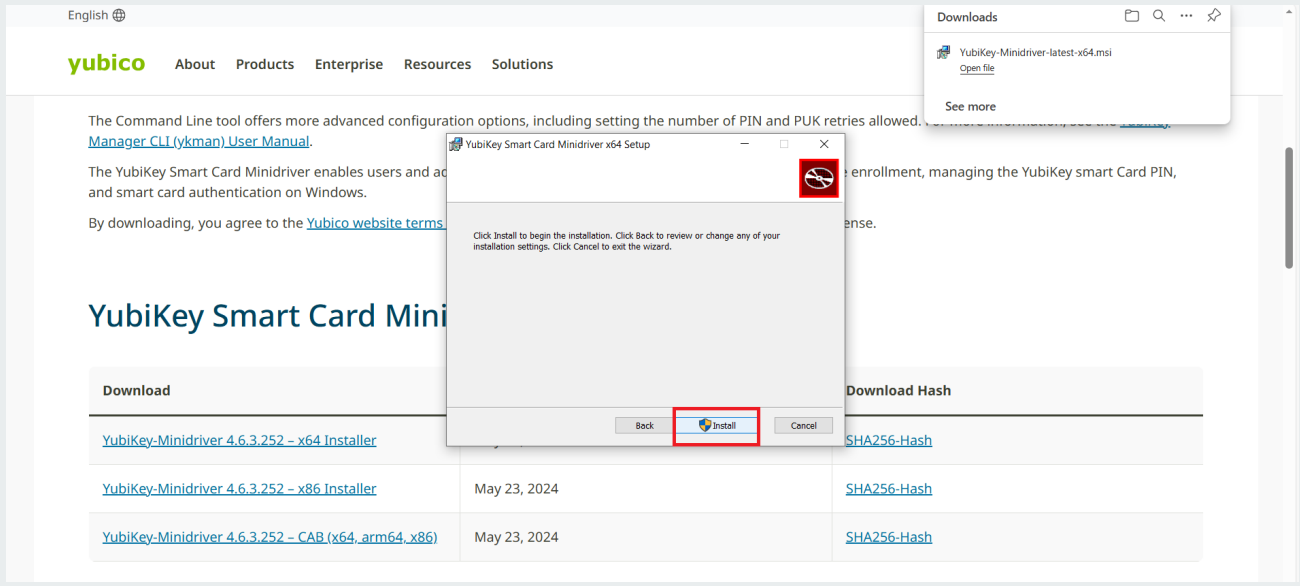
# B7 Installing the Yubikey Minidriver

A Setup Wizard pop-up will open – **Click Next.**



# B8 Continue Installing the Yubikey Minidriver

On the next pop-up window – **Click Install.**

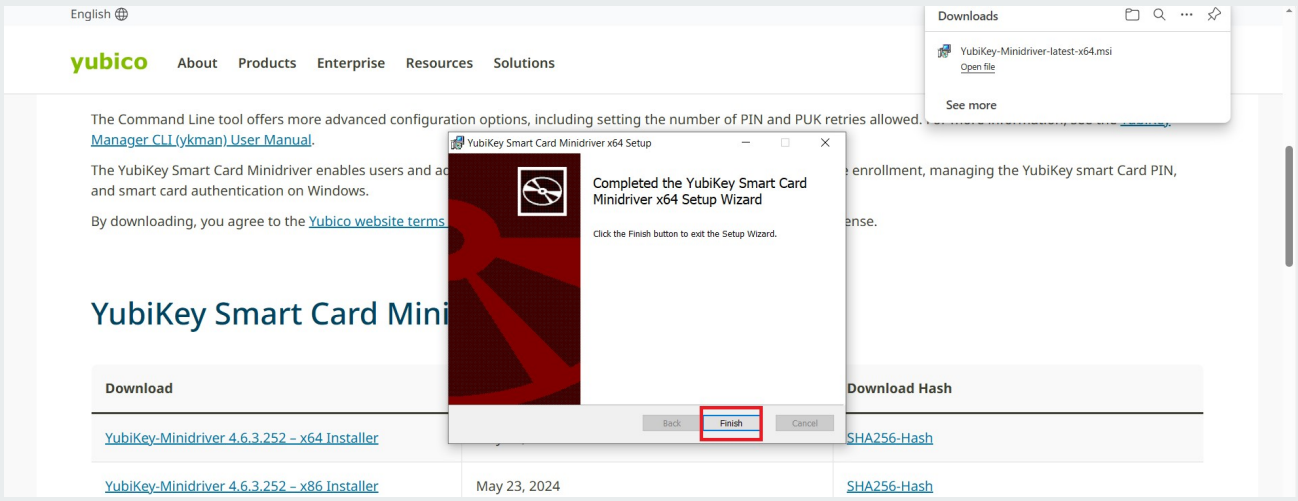



# B9 Permission to make changes

The next pop-up message will ask permission to allow the application to make changes on your computer. **Click YES.**

# B10 Finish the install

To complete the installation of the Yubikey Minidriver, **click Finish.**




The installation of the Yubikey Minidriver is now complete.

# SECTION C

## C1 Importing an SB2 Root CA Certificate into Microsoft Truststore

When using Security Keys with digital certificates for authentication to an SB2 website, the **SB2 Root CA** certificate is the most critical component in establishing trust with that SB2 website. It verifies that the digital certificate on your Security Key was issued by a trusted Certificate Authority specific to the SB2 website—reflecting the unique "root of trust" established for each SB2 deployment worldwide.

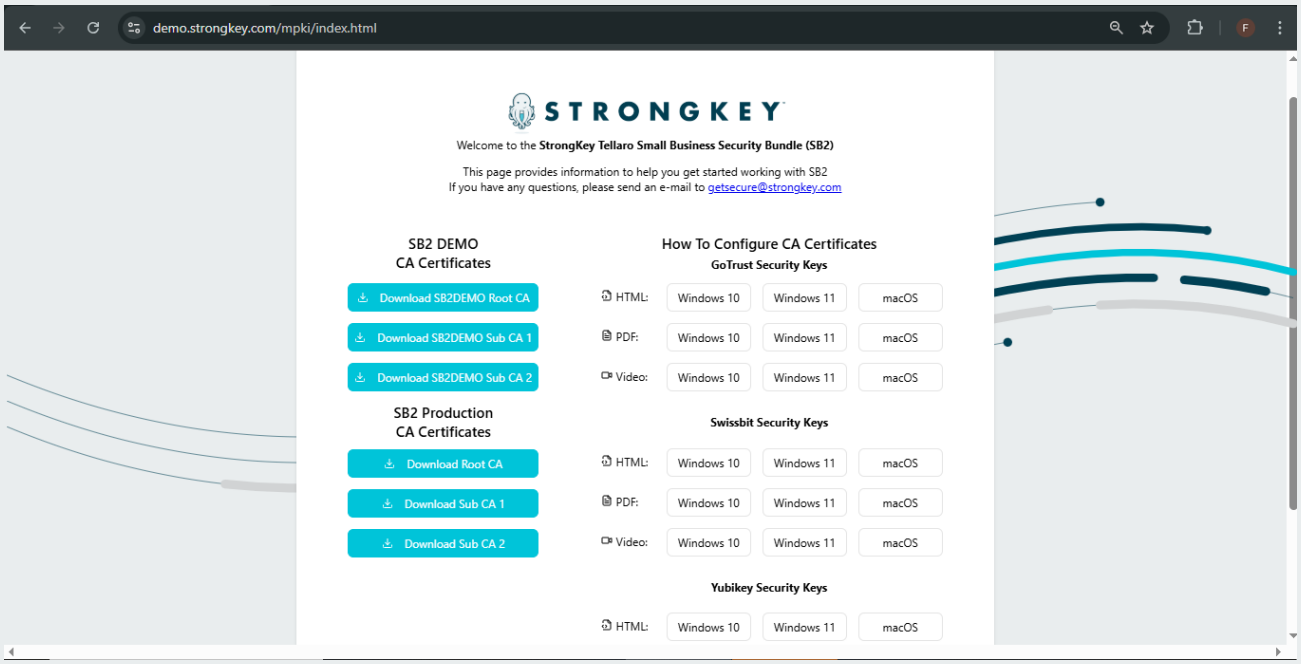
This not only ensures the integrity of the authentication process, but also guarantees that the trust established between the Security Key you were given and the SB2 site, is unique from every other SB2 website in the world. This ensures attackers cannot scale an attack on any other SB2 website even if they managed to compromise one through an insider attack.

## C2 Prerequisites

- Windows 10
- Microsoft (MS) Edge Browser, version 141.0.3537.99
- Internet connection
- Individual CA certificate files downloaded from the MPKI website.
- NOTE: In the event the individual files for the **SB2 Root CA** and **SB2 Subordinate** CA certificates were provided, you may import them directly from the stored location on your computer without the need for the ZIP file – the process is similar, starting from step C7.

# C3 Access the SB2 MPKI Landing Page

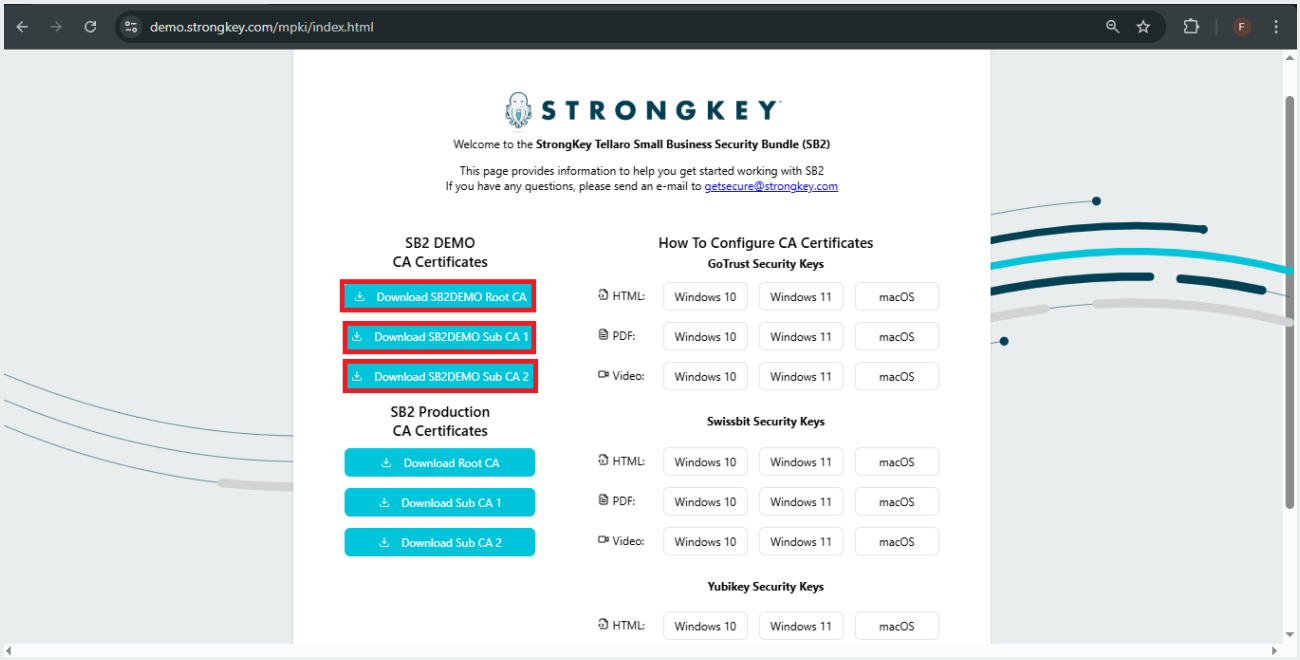
All required CA certificates are available for download from the **SB2 MPKI portal** at https://demo.strongkey.com/mpki. Comprehensive SB2 documentation is also accessible through this site.



# C4 SB2 CA Certificates

At the SB2 MPKI portal, locate the available CA Certificate download options. Each of the following certificate files are required:

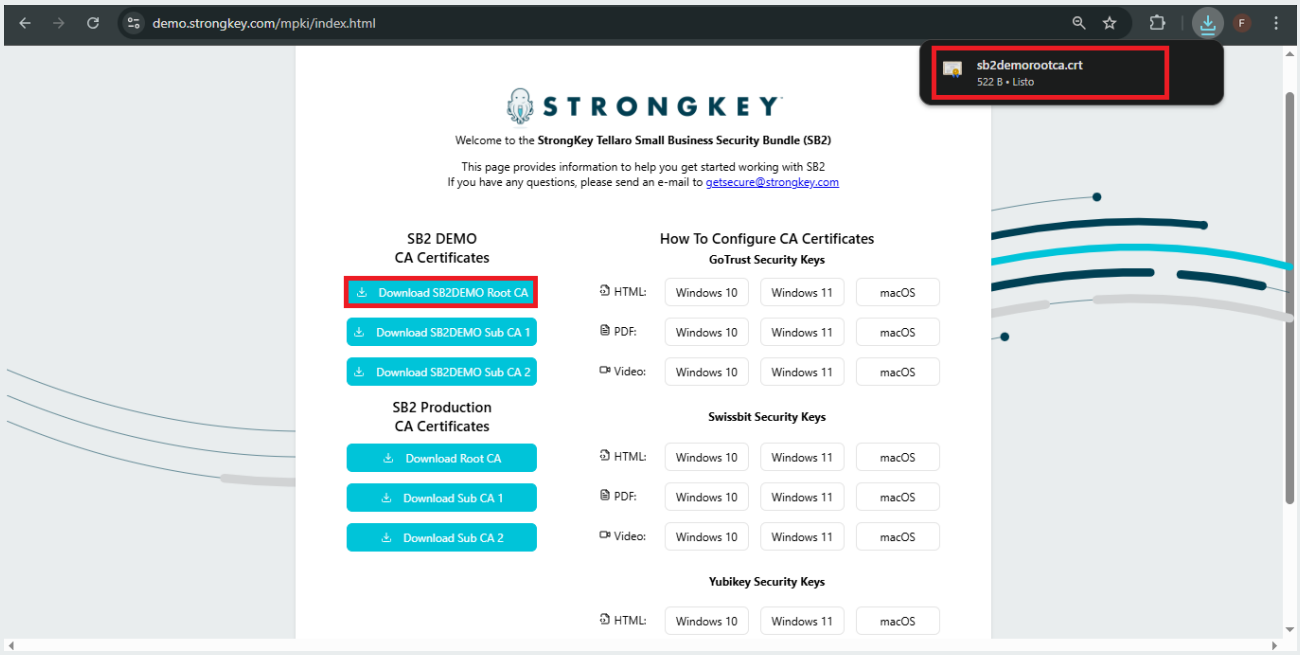
- **SB2DEMO Root CA**
- **SB2DEMO Sub CA1**
- **SB2DEMO Sub CA2**



# C5 Downloading the SB2DEMO Root CA

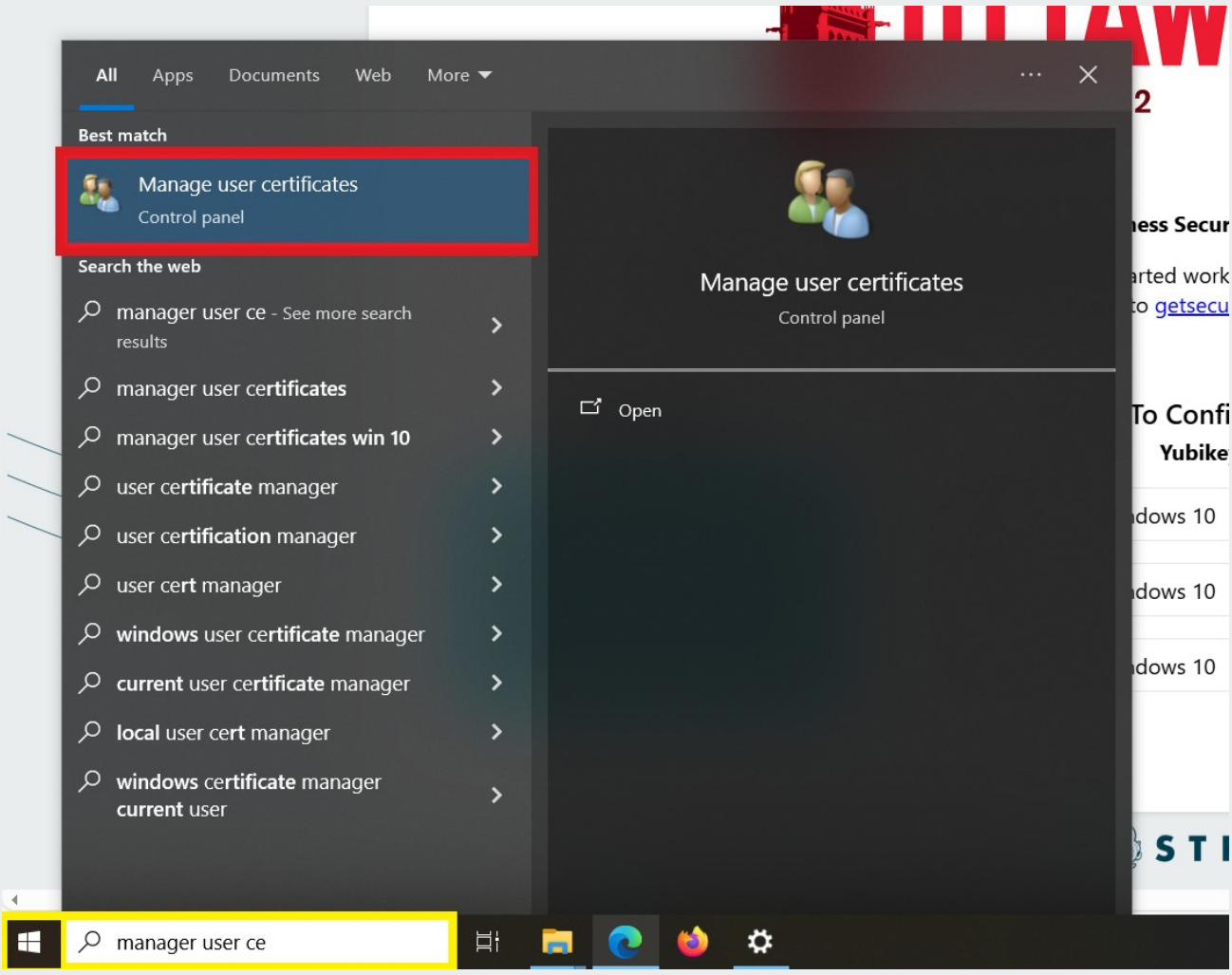
To download the Root CA, **click** the **SB2DEMO Root CA button**. The download will begin automatically, and you'll see a **dialog box** confirming the file name once the process is complete.

Repeat this process for the **SB2DEMO Sub CA1** and the **SB2DEMO Sub CA2** files.



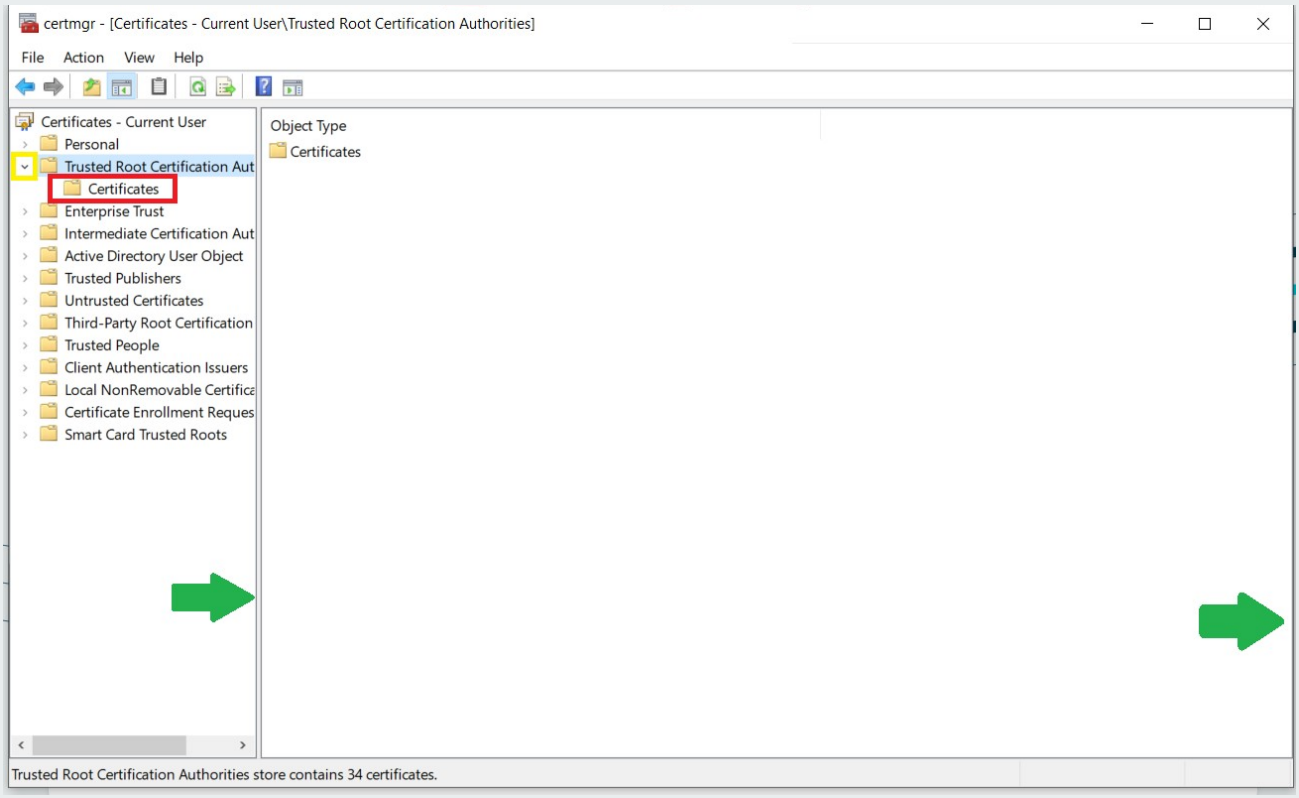
## C6 Navigate to Windows Start Icon:

After clicking the Windows Start icon (or alternatively **clicking** on the search bar at the right of the Windows Start icon), search for **Manage user certificates** to find the settings application for overseeing and configuring security certificates, including importing. From here, select the **Manage user certificates** application.



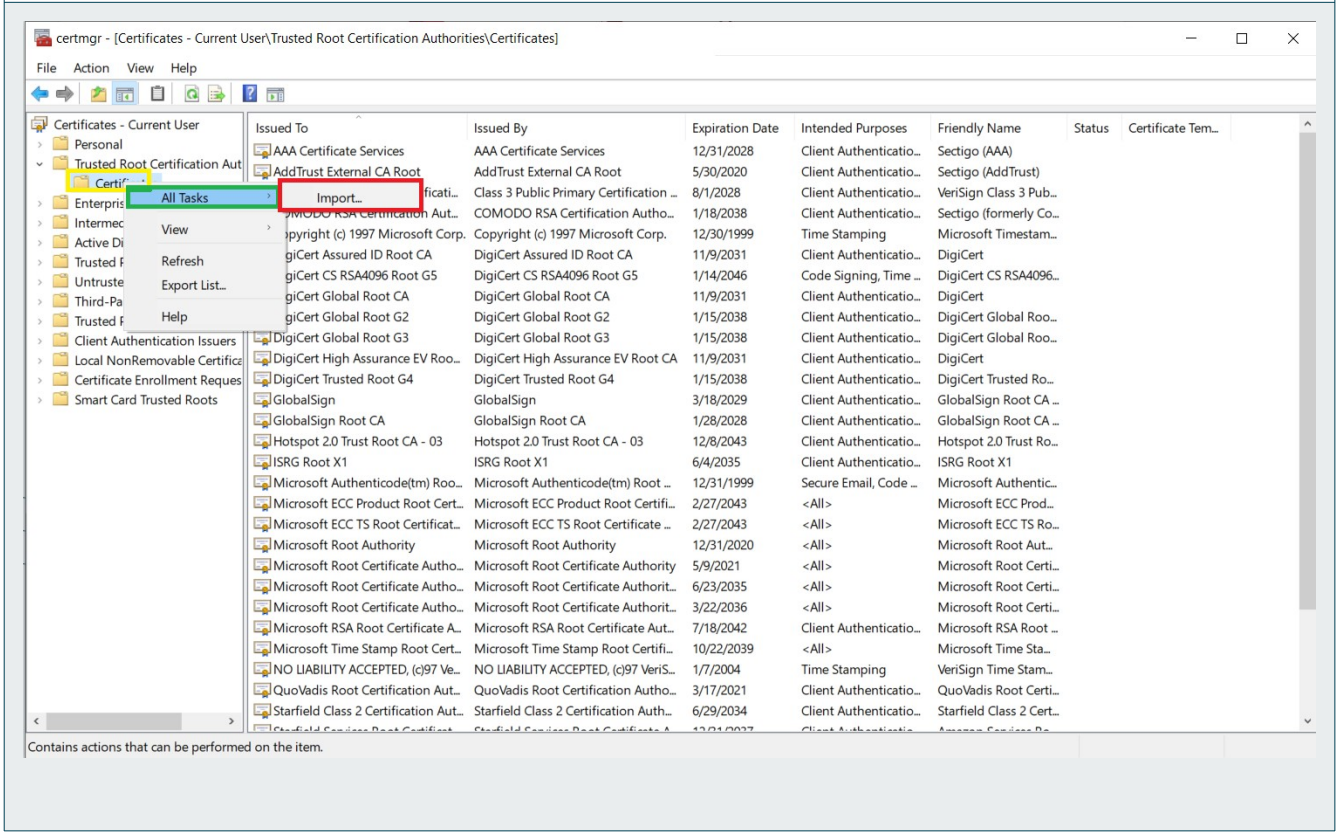
# C7 Open the Trusted Root Certification Authorities Folder

To begin, expand the **Certification Manager** window by clicking and dragging the borders (green arrows) to a larger size. This will provide a better view of the digital certificates. Next, click the **arrow** (yellow box) next to the **Trusted Root Certification Authorities** folder to expand it, revealing the **Certificates** (red box) folder.



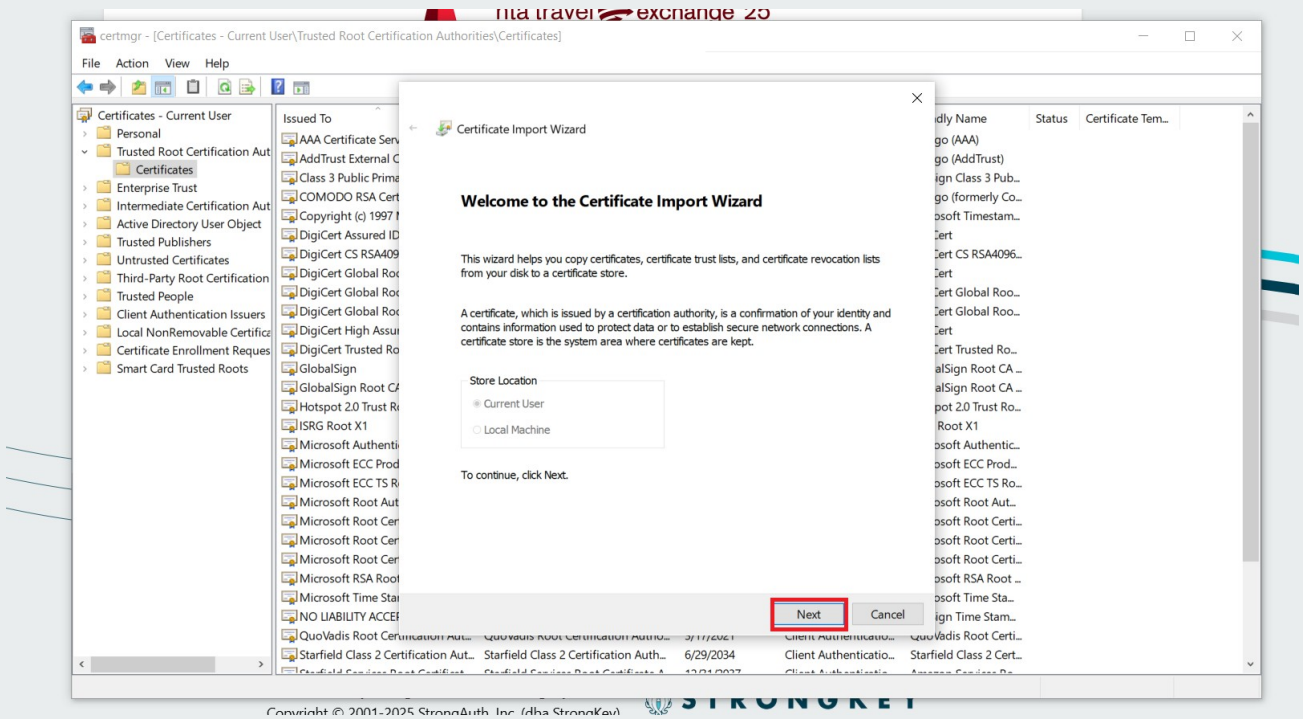
# C8 Initiate the SB2 Root CA Certificate Import

To begin, right-click the **Certificates** folder to open the context menu. From there, select **All Tasks**, and then **click Import** to start the **Certificate Import Wizard**.



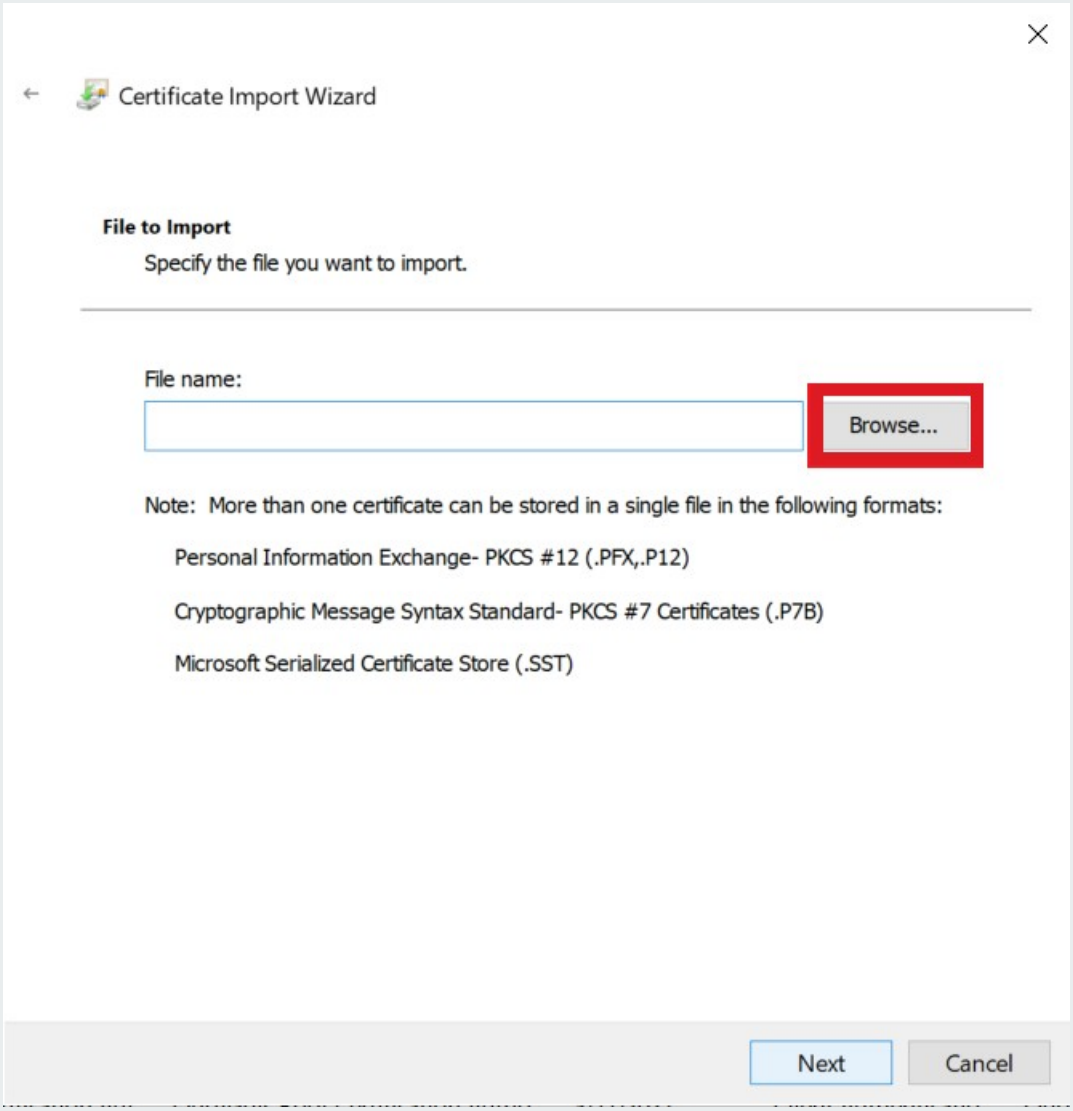
# C9 Certificate Import Wizard

The Certificate Import Wizard will open. **Click Next** to proceed.



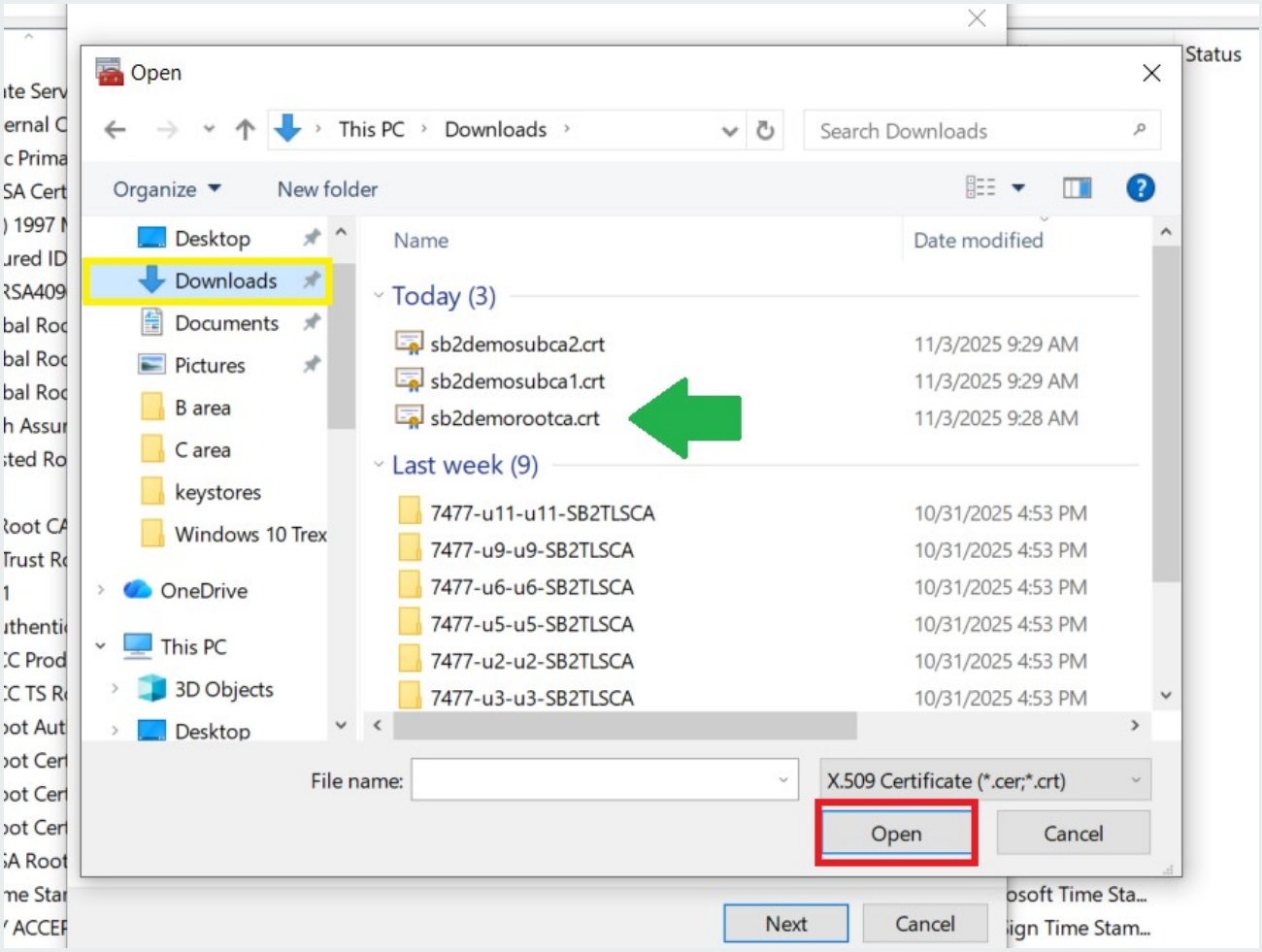
# C10 Locate the SB2 Root CA Certificate

**Click** the **Browse** button to locate the SB2 Root CA certificate file.



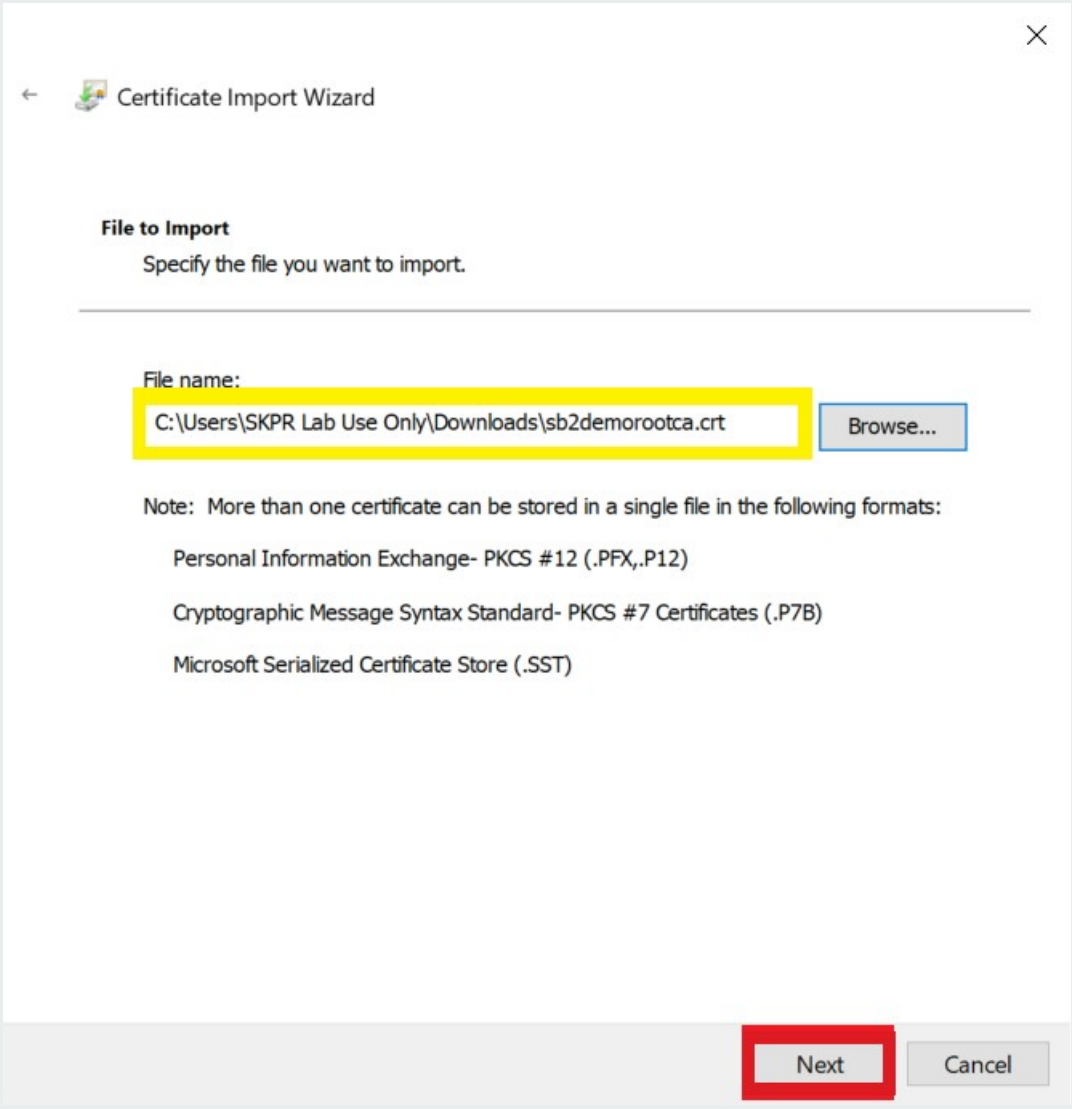
# C11 Open the SB2 Root CA Certificate

To find the SB2 Root CA Certificate, go to the file's location, which is typically the **Downloads** folder. Once the **SB2 Root CA file** is located, **select** it and **click Open**.



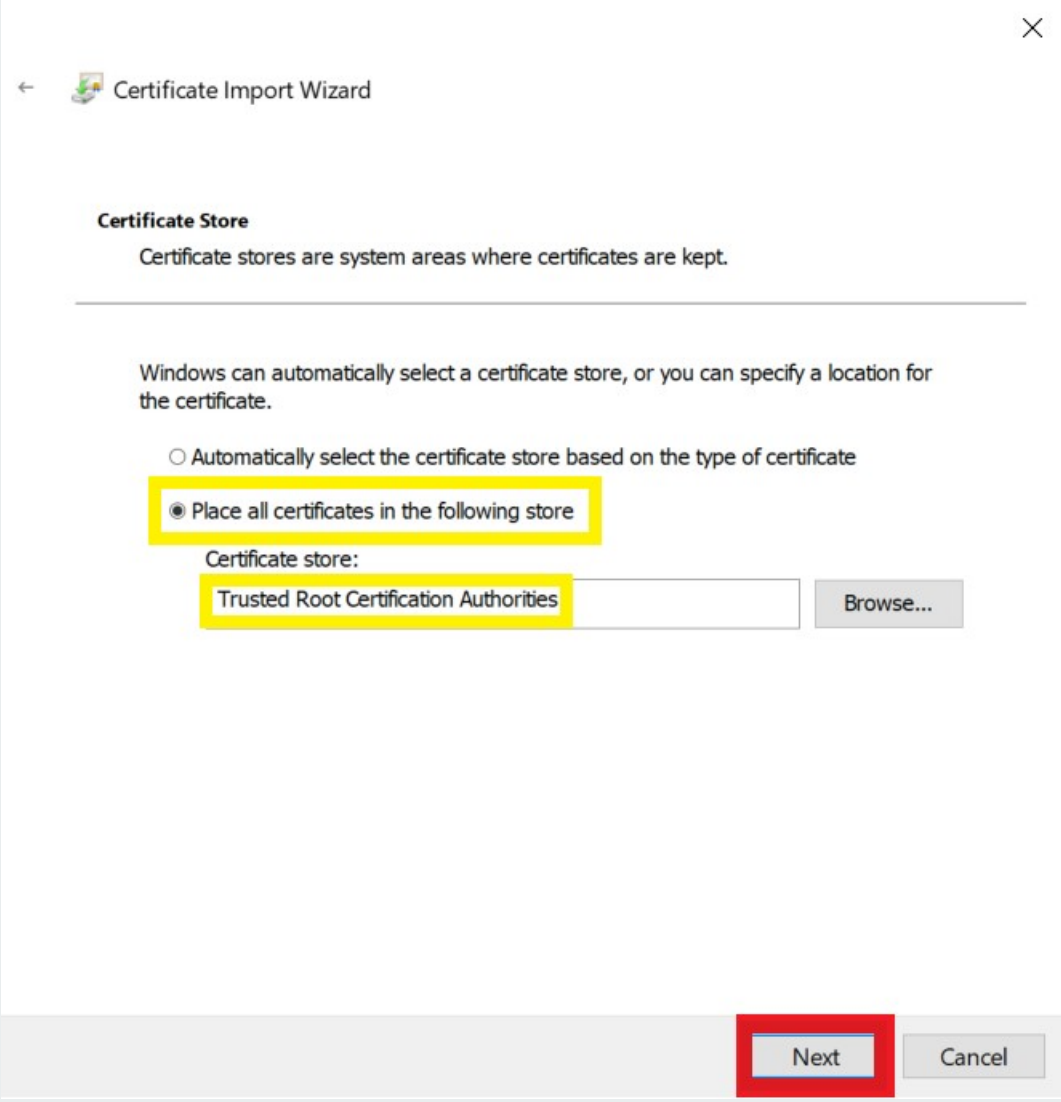
# C12 SB2 Root CA Certificate File selected

Before proceeding, verify the correct **SB2 Root CA Certificate** file has been selected. The name of the file will automatically populate the **"File Name"** field upon selection. **Click Next** to continue.



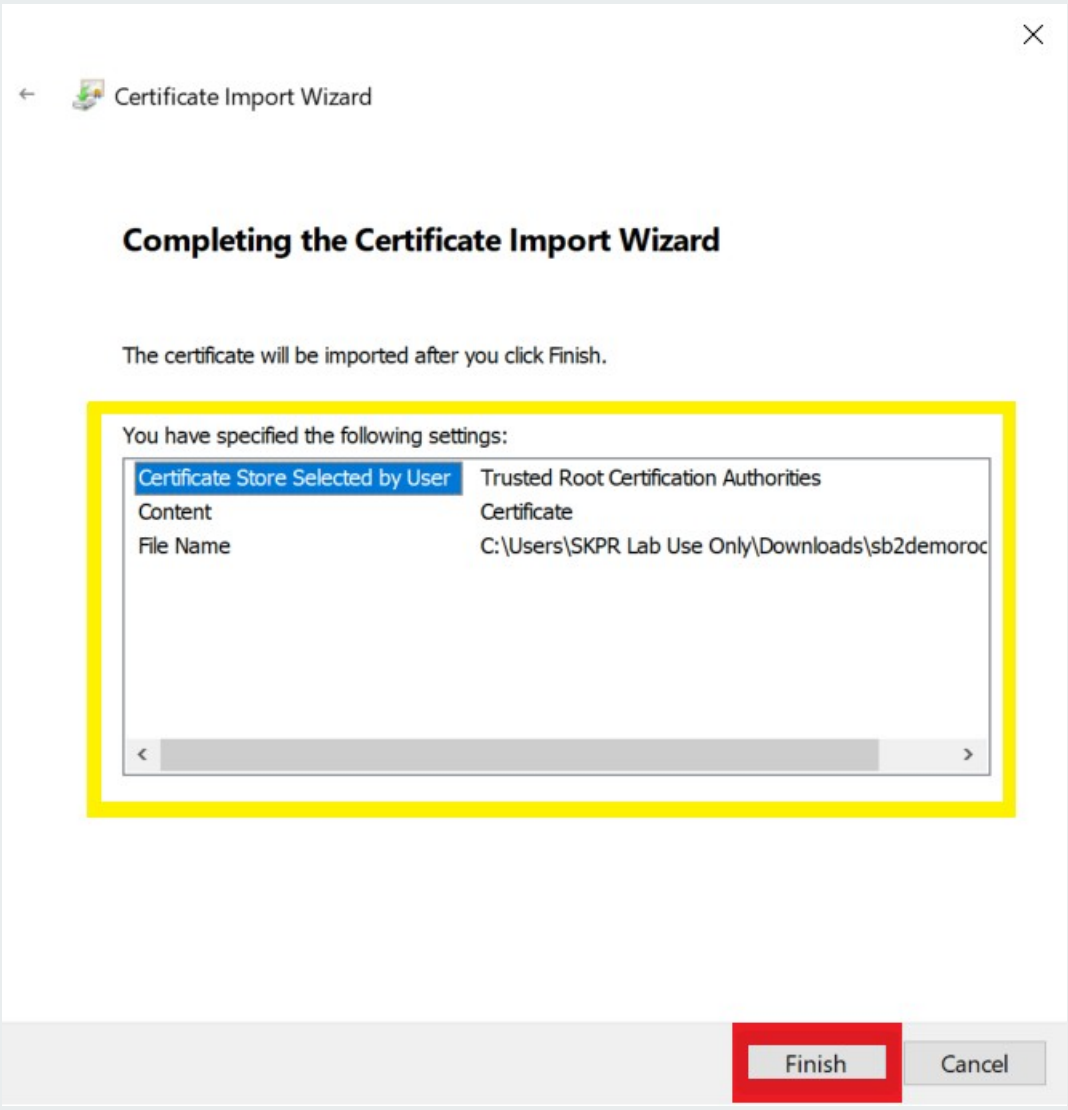
# C13 Select Certificate Store

**Choose** “Place all certificates in the following store” (yellow box) and ensure the certificate is added to the **Trusted Root Certification Authorities** certificate store. **Click Next** to continue.



# C14 Finish Importing the SB2 Root CA Certificate

Review the certificate store name, certificate details, and file name in the next dialog box, then **click Finish** to complete the import process.



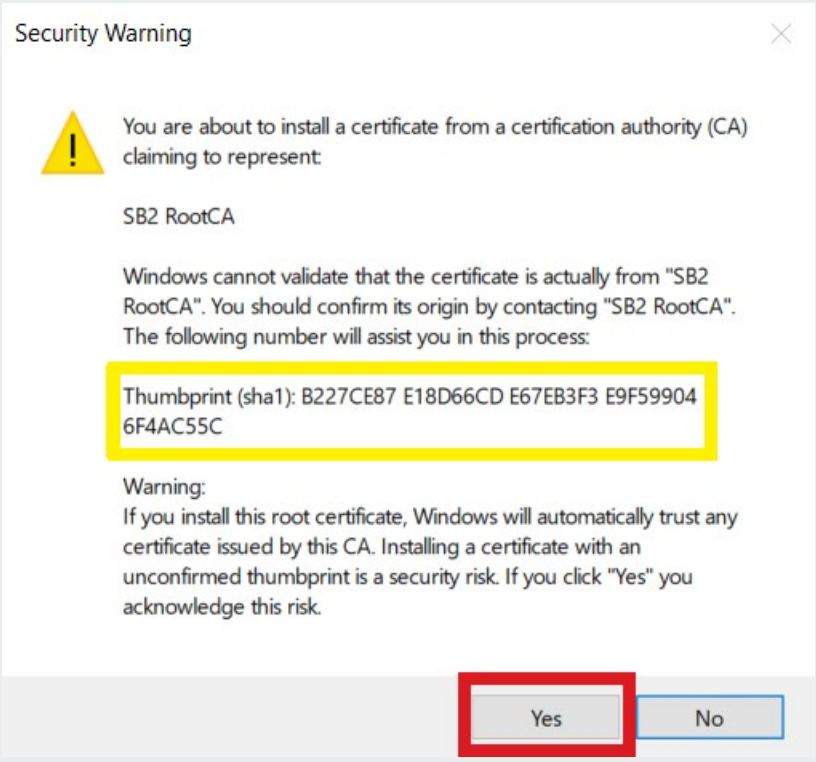
# C15 Security Warning

A security warning will be displayed regarding the Root CA Certificate. Make sure the name of the certificate and the **Thumbprint** (sha1) shown in the warning window match the content shown here:

**SB2 RootCA**
**B227CE87 E18D66CD E67EB3F3 E9F59904 6F4AC55C**

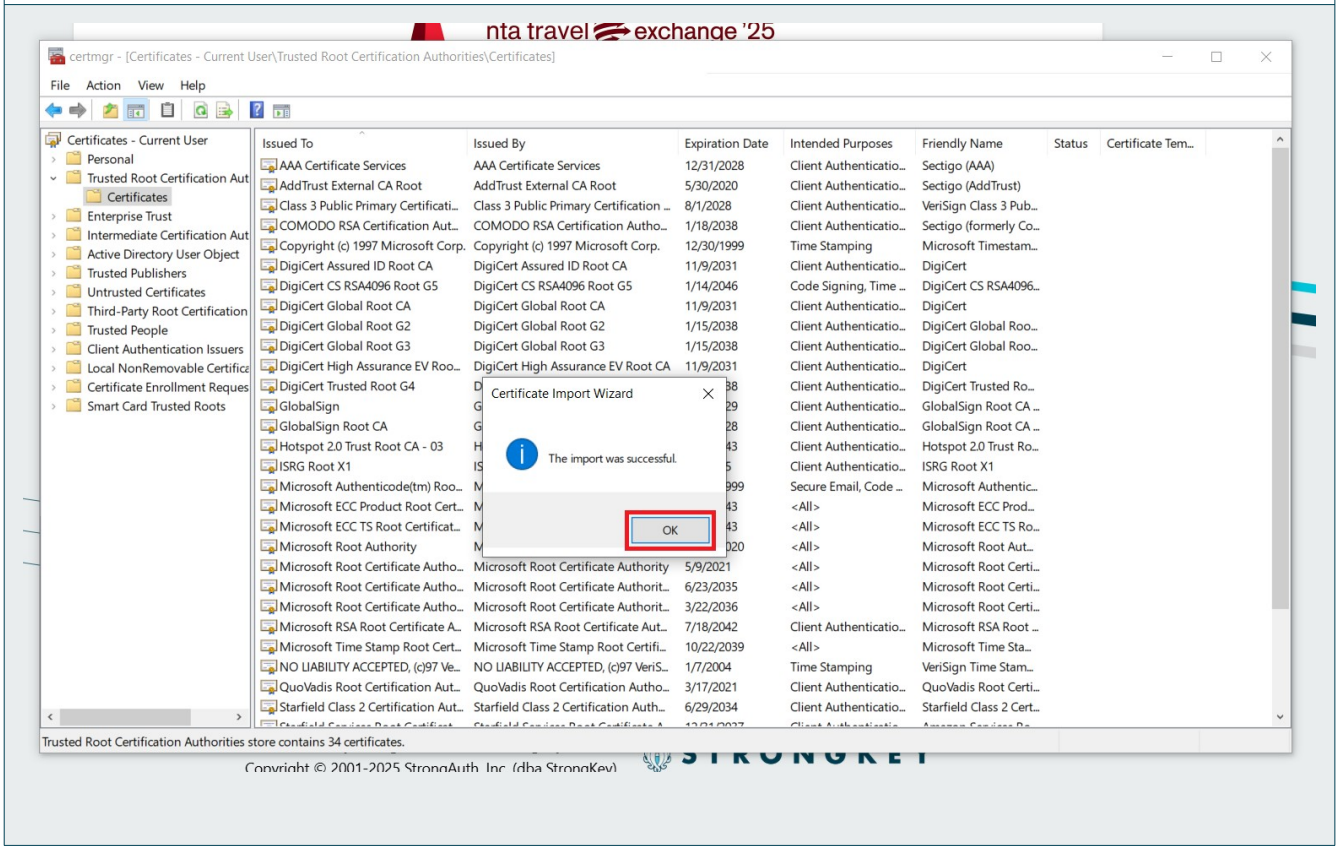
If it matches *identically*, **click Yes.**

NOTE: If the Thumbprint of the CA certificate does not match, get in touch with the Administrator of the SB2 site. This step represents the most important step in establishing trust in the SB2 platform.



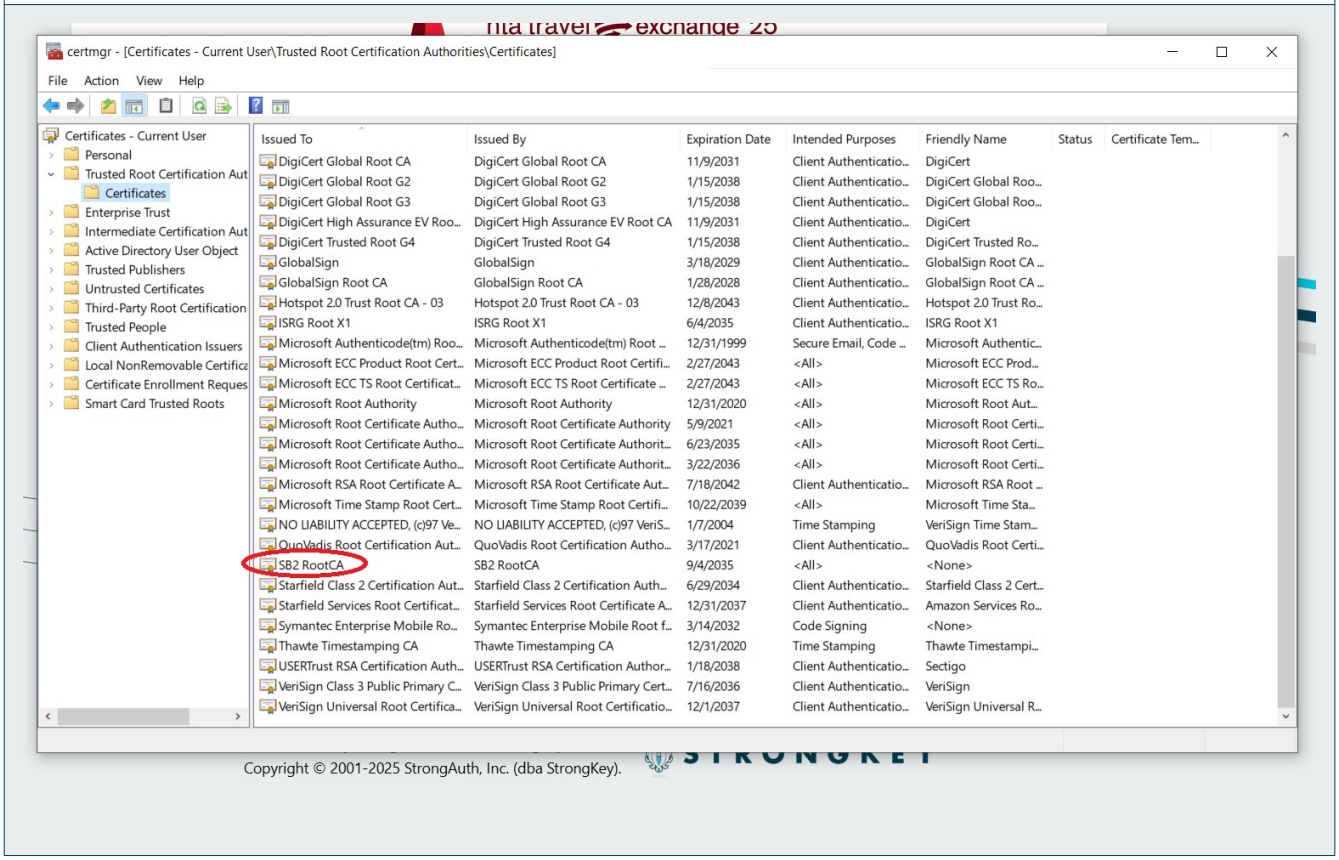
# C16 A Successful Import

Once the **SB2 Root CA Certificate** is imported successfully, a confirmation message will appear. Click **OK** to continue.



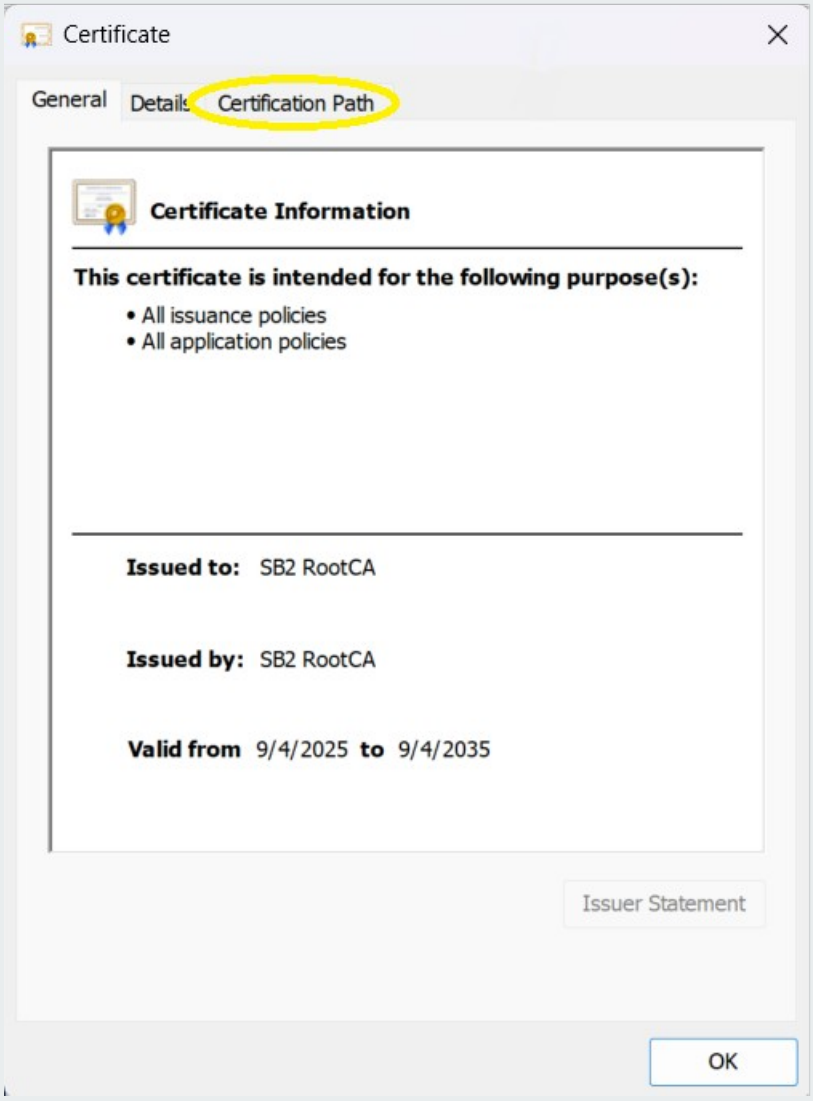
# C17 Verify SB2 Root CA in List of Certificates

If you scroll down the list of CA certificates on the right-hand side of this window's panel, you will see the **SB2 Root CA** certificate in the list.



# C18 Verify SB2 Root CA - 1

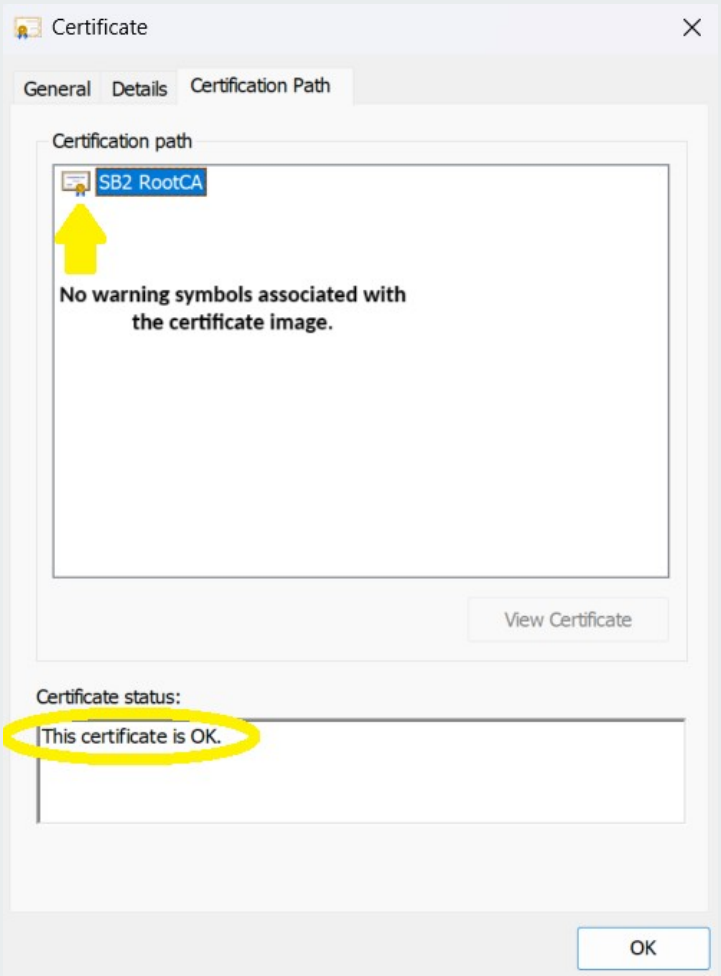
By double-clicking the **SB2 Root CA** certificate – or **right-clicking** the mouse button and selecting **Open**, you should see the following window. Select the **Certification Path** tab in this window:



# C19 Verify SB2 Root CA - 2

In the **Certification Path** tab of the **SB2 Root CA** certificate, you should be able to confirm these two important attributes of the certificate:

- That the certificate symbol in the **Certification Path** sub-panel at the top does not have any yellow warning symbol associated with it, and
- The **Certificate status** sub-panel at the bottom should state that "This certificate is OK."



# SECTION D

## D1 Importing SB2 Subordinate CA Certificate into Microsoft Truststore

Subordinate CA certificates play a vital role within the SB2 platform. They are part of the “certificate chain” establishing trust between the digital certificate on your Security Key and the SB2 Root CA embedded within the SB2 platform.

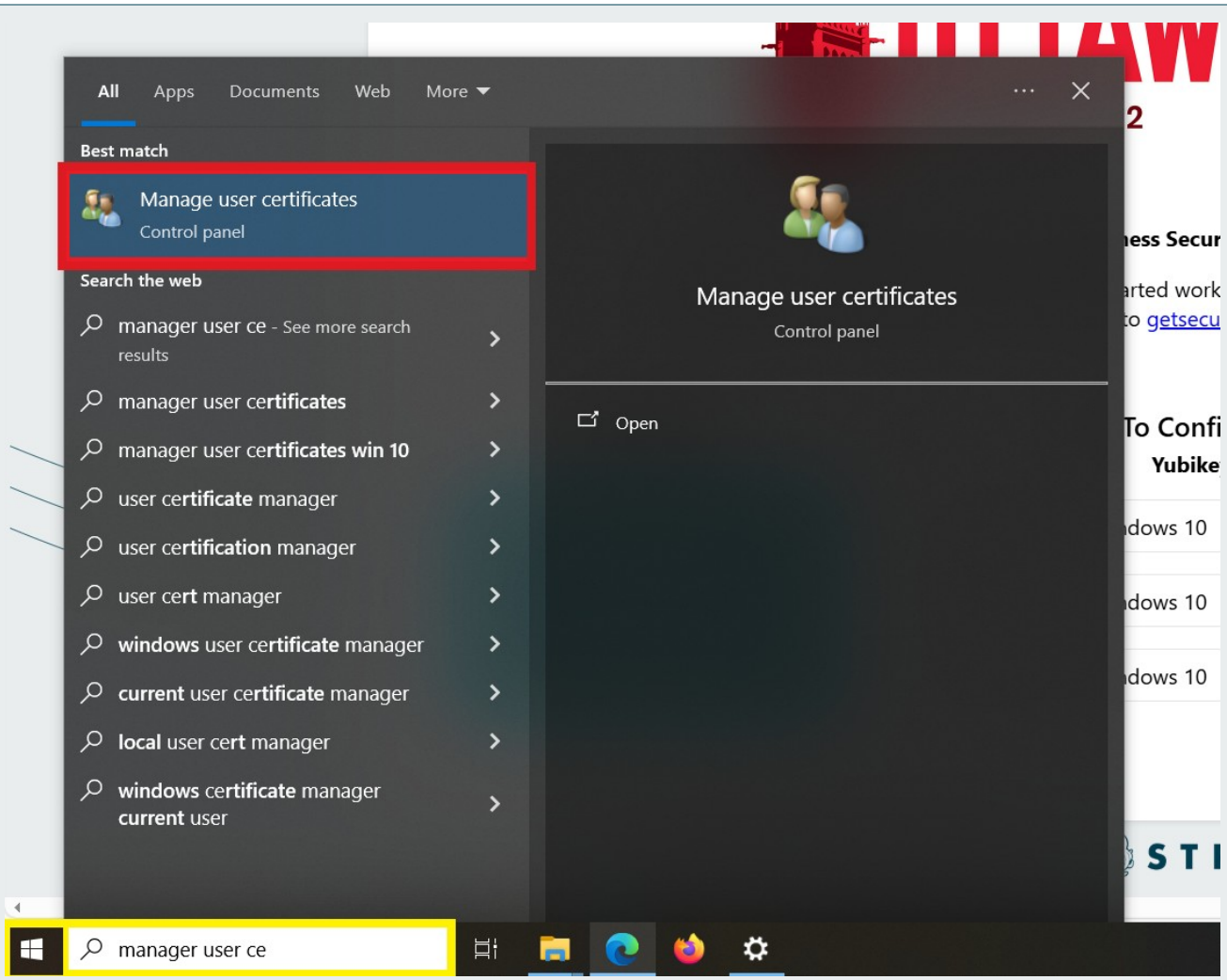
## D2 Prerequisites

- Windows 10
- ZIP File issued by the Administrator of an SB2 platform* at your site; or
- Individual CA certificate files issued by the Administrator of an SB2 platform at your site
- NOTE: In the event the SB2 Administrator provided individual files for the **SB2 Root CA** and **SB2 Subordinate** CA certificates, you may import them directly from the stored location on your computer without the need for the ZIP file – the process is similar, starting from step D5

* If you have not extracted the SB2 ZIP file provided by the Administrator of the SB2 platform, see **Importing an SB2 Root CA Certificate into Microsoft Truststore**, steps C3 – C7.

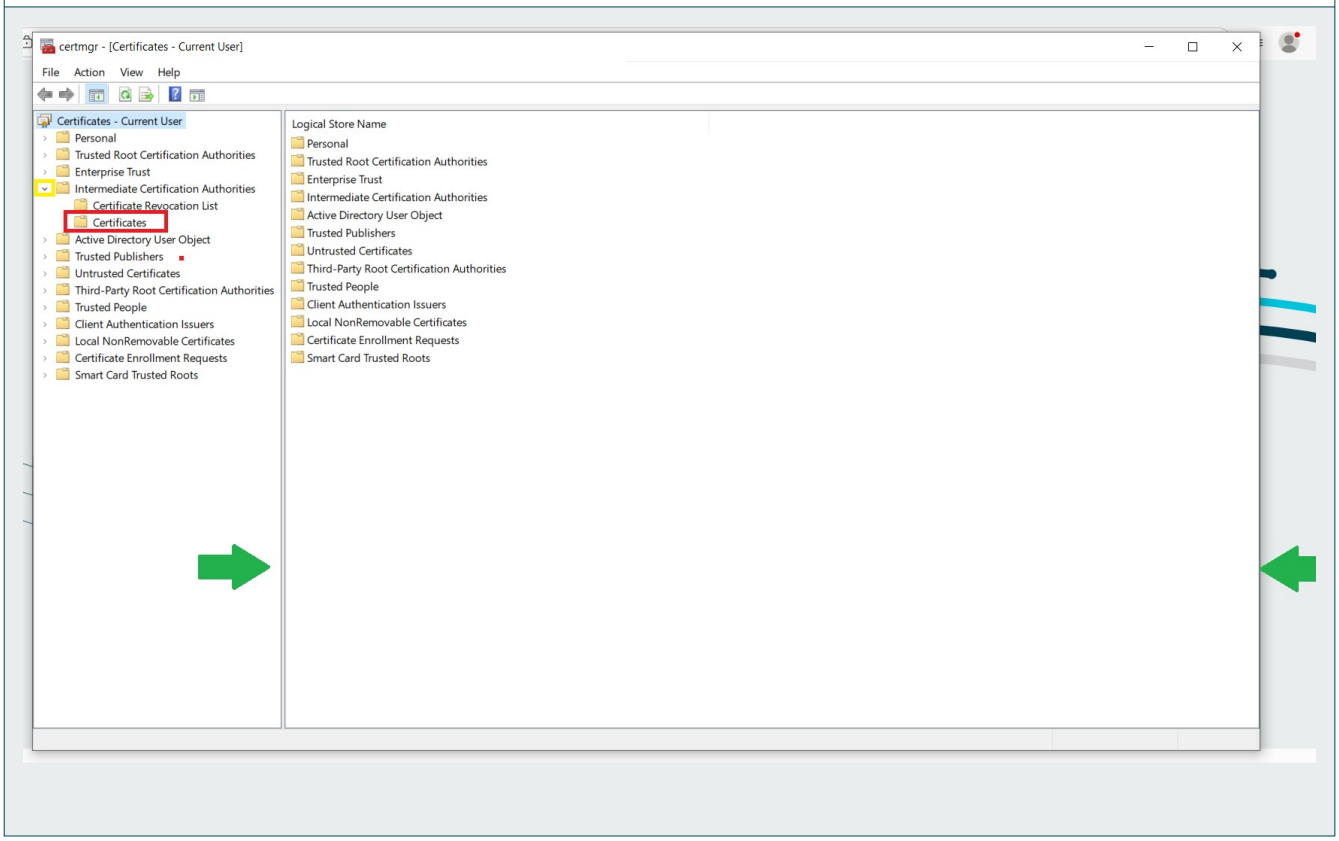
## D3 Navigate to Windows Start Icon:

After clicking the Windows Start icon (or alternatively **clicking** on the search bar at the right of the Windows Start icon), search for **Manage user certificates** to find the settings application for overseeing and configuring security certificates, including importing. From here, select the **Manage user certificates** application.



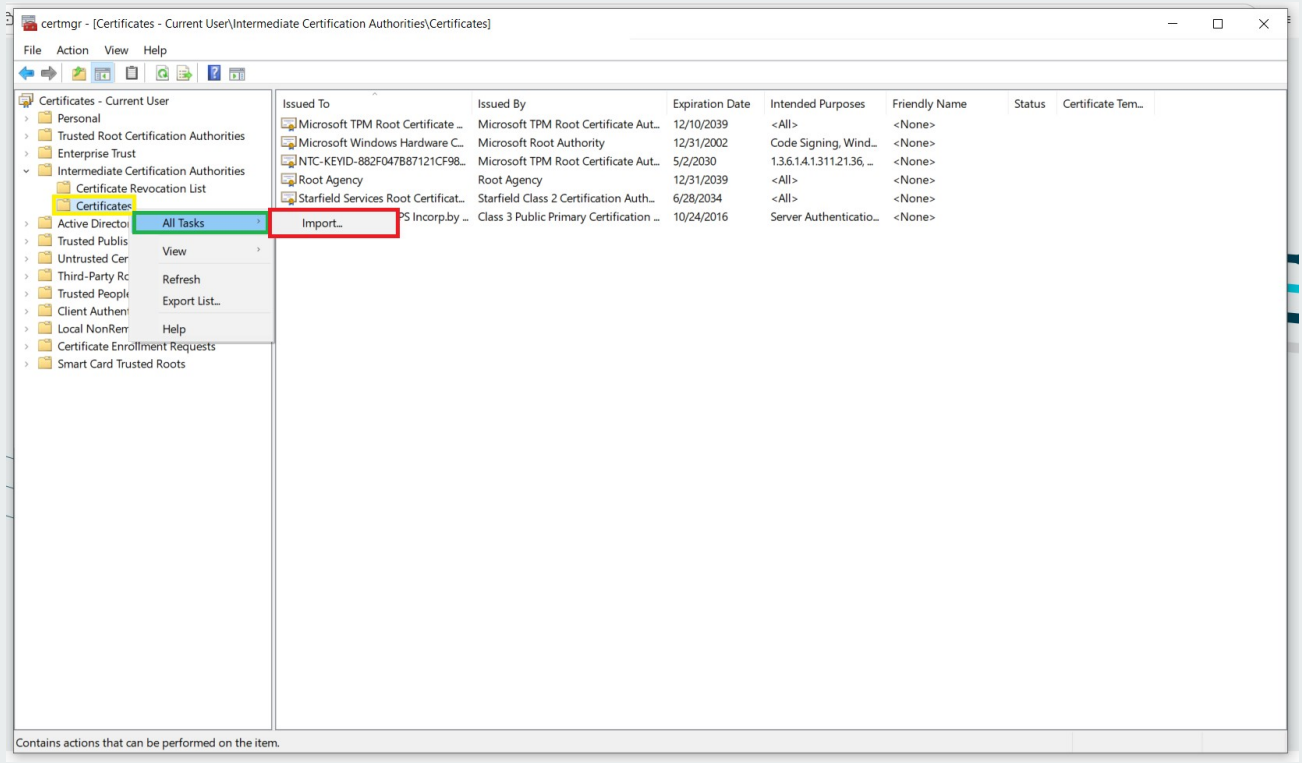
# D4 Open the Intermediate Certification Authorities Folder

To begin, expand the **Certification Manager** window by clicking and dragging the borders (green arrows) to a larger size. This will provide a better view of the security certificates. Next, click the **arrow** (yellow box) next to the **Intermediate Certification Authorities** folder to expand it, revealing the **Certificates** (red box) folder.



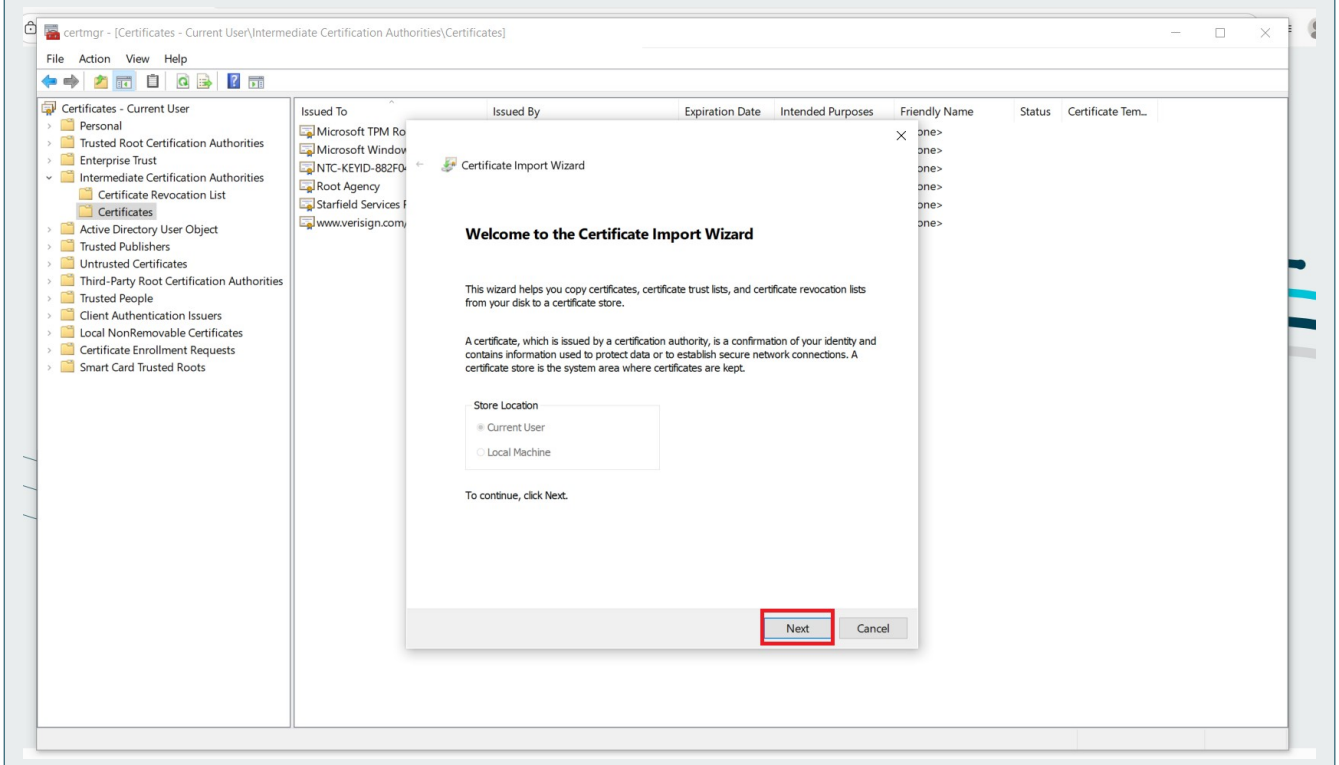
# D5 Initiating the SB2 Subordinate CA Certificate Import

To begin, right-click the **Certificates** folder to open the context menu. From there, select **All Tasks**, and then **click Import** to start the **Certificate Import Wizard**.



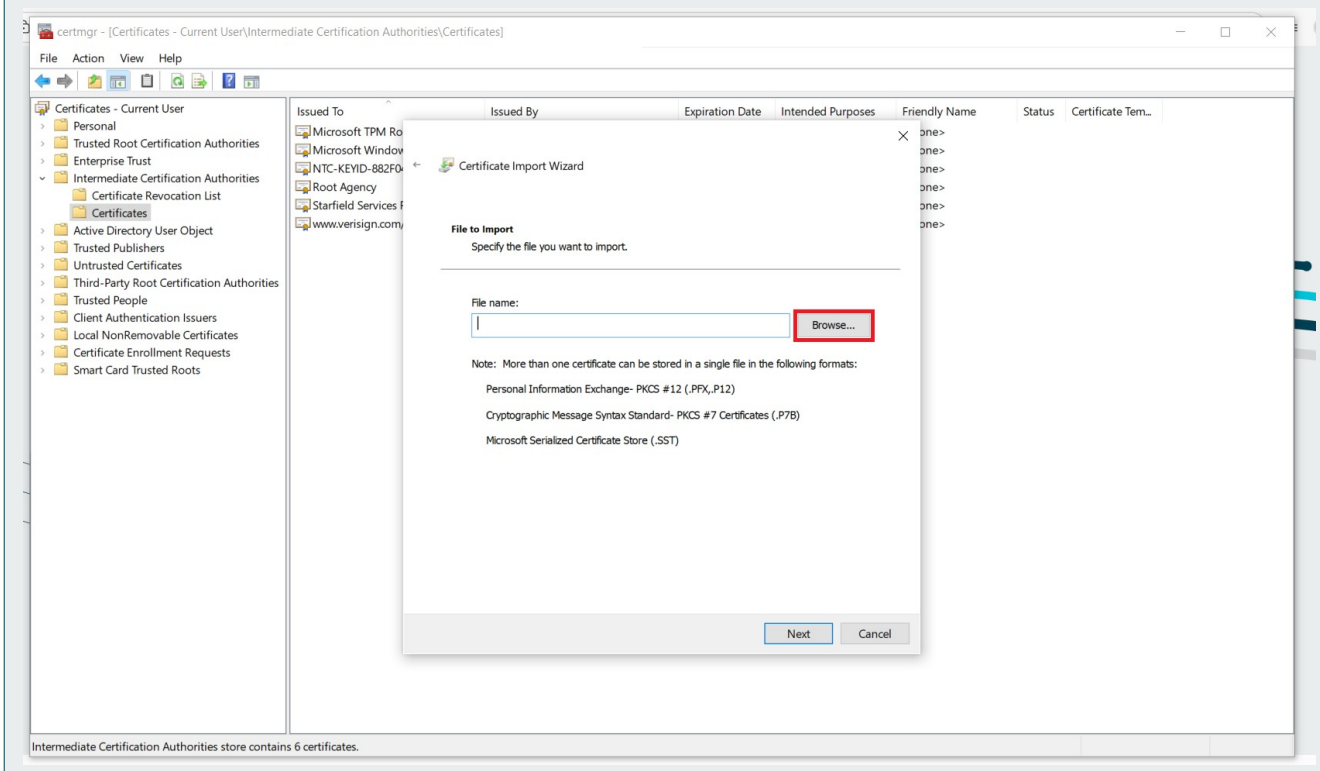
# D6 Certificate Import Wizard

The Certificate Import Wizard will open. **Click Next** to proceed.



# D7 Locate the Subordinate SB2 CA Certificate for Importing

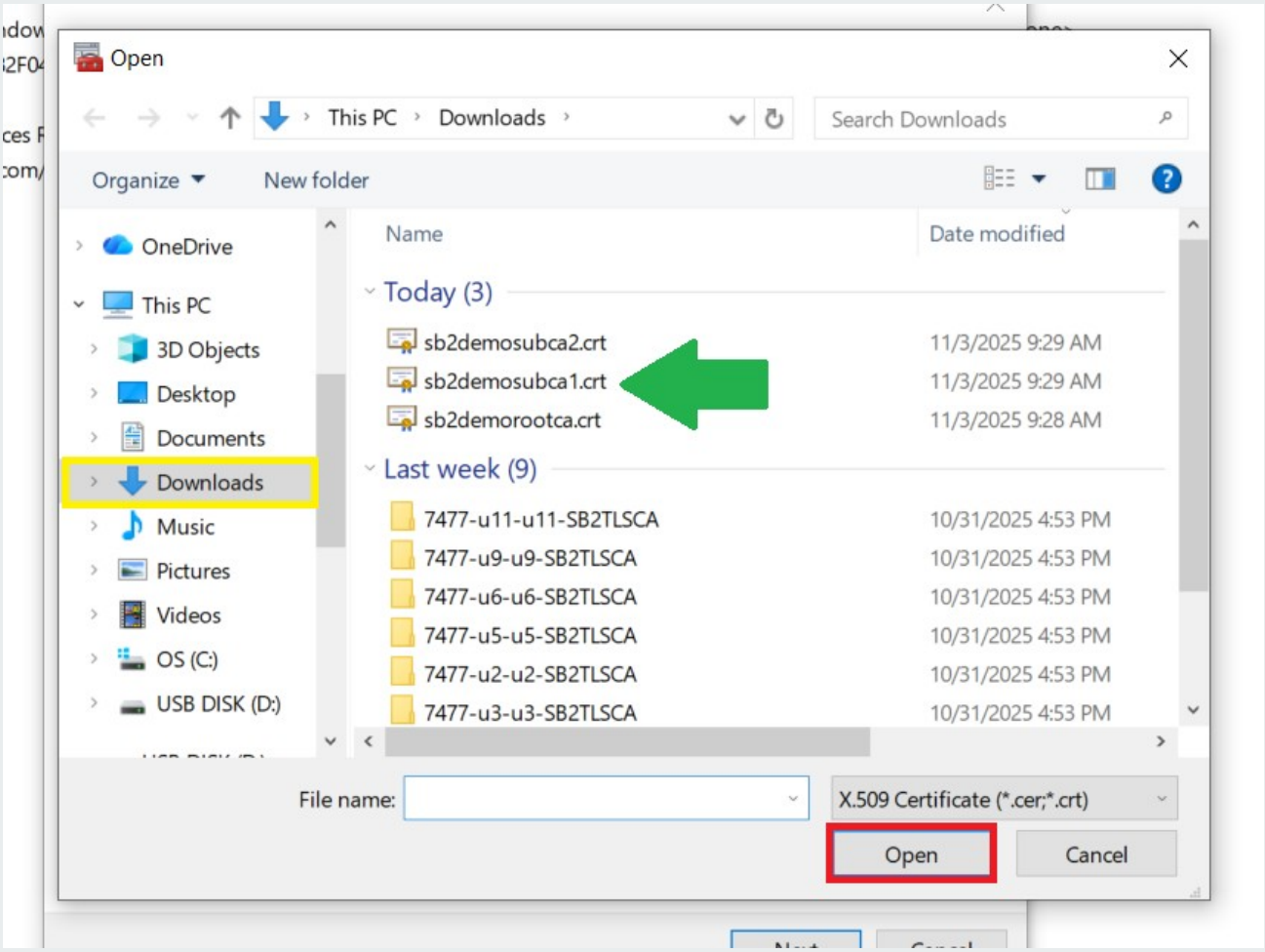
**Click** the **Browse** button to navigate to and select the Subordinate CA certificate file.



# D8 Open the SB2 Subordinate CA Certificate

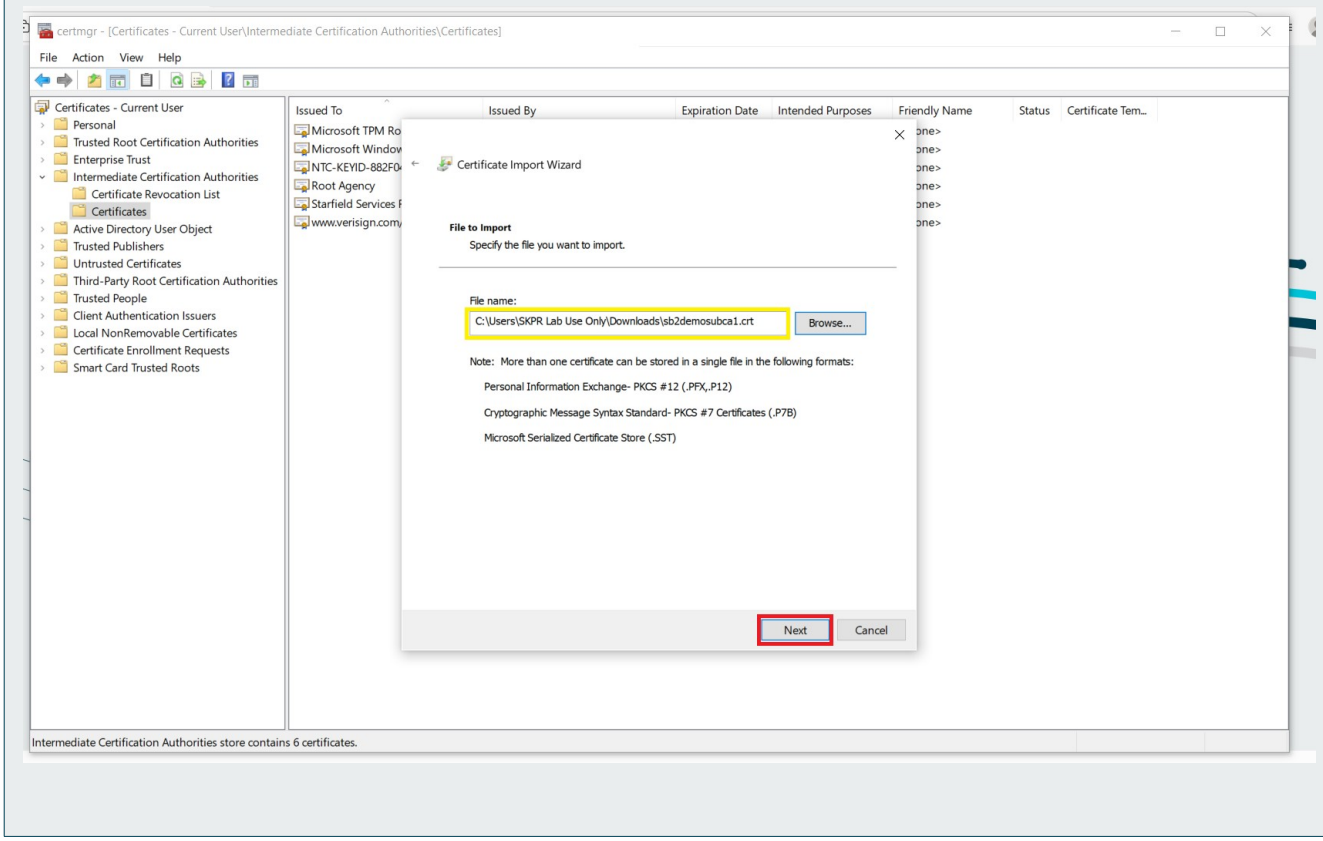
To find the SB2 Subordinate CA Certificate, go to the file's location, which is typically the **Downloads** folder. Once the **SB2 Subordinate CA file** is located, **select** it and **click Open**.

**Please note:** Should the SB2 ZIP file contain more than one **Subordinate CA Certificate**, or if the SB2 Administrator provided more than one **SB2 Subordinate CA** certificate, you must import all of them.



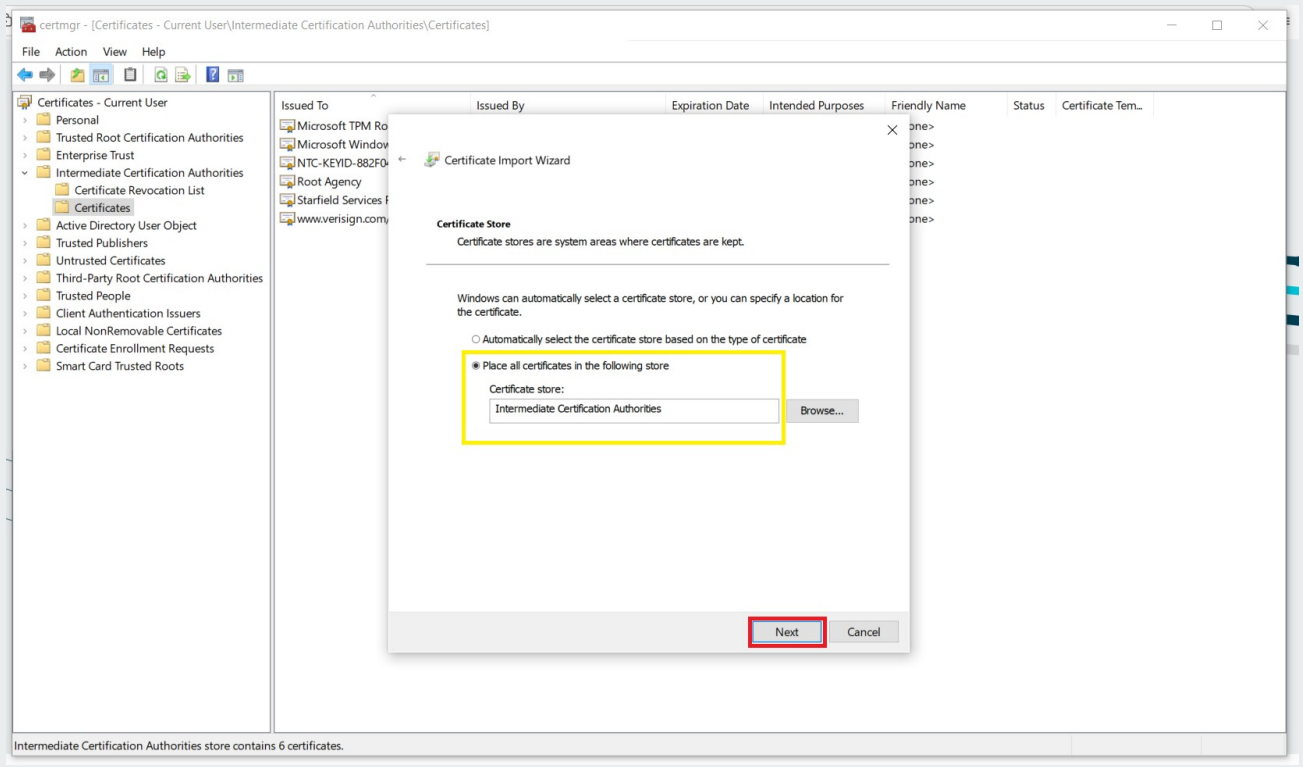
# D9 SB2 Subordinate CA Certificate File selected

Before proceeding, verify the correct **SB2 Subordinate CA Certificate** file has been selected. The name of the file will automatically populate the **File Name** field upon selection. Click **Next** to continue.



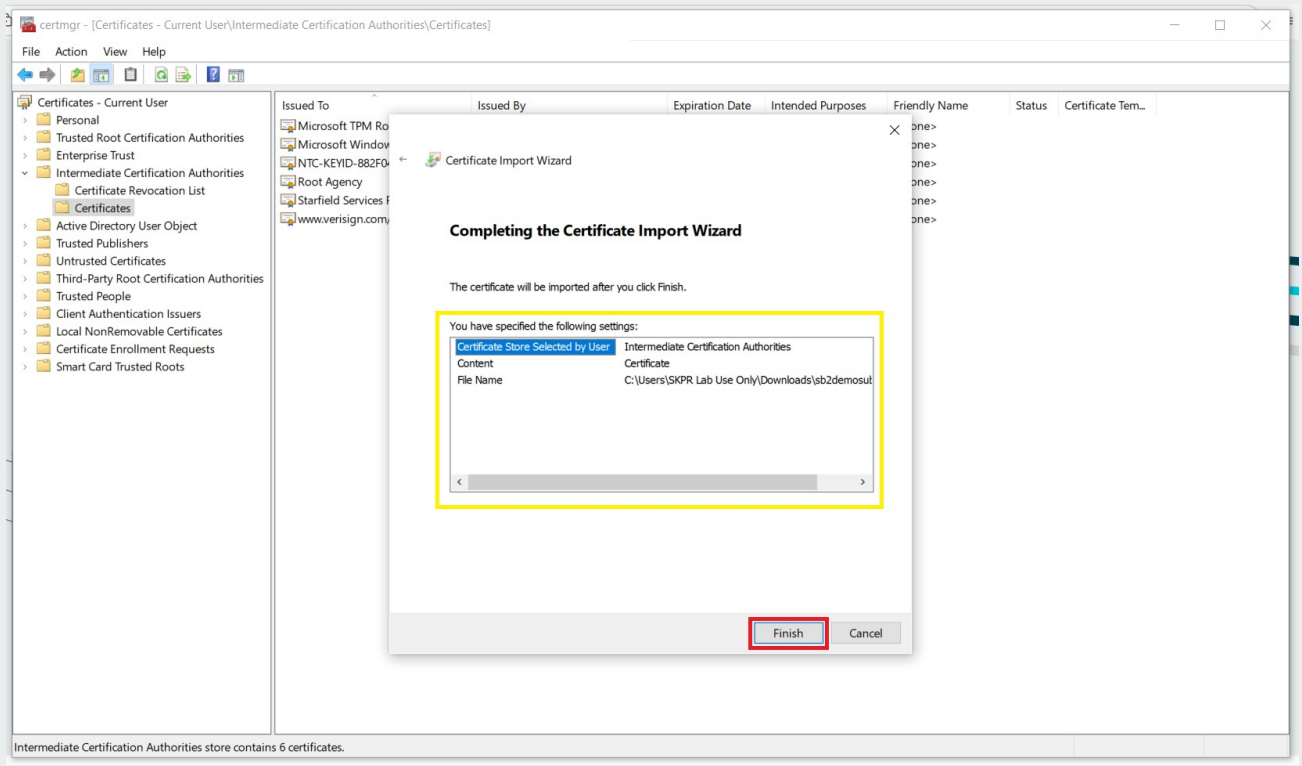
# D10 Selecting Certificate Store

**Choose** “Place all certificates in the following store” and ensure the certificate is added to the **Intermediate Certification Authorities** certificate store. Click **Next** to continue.



# D11 Finish Importing the SB2 Subordinate CA Certificate

Review the certificate store name, certificate details, and file name in the next dialog box, then **click Finish** to complete the import process.

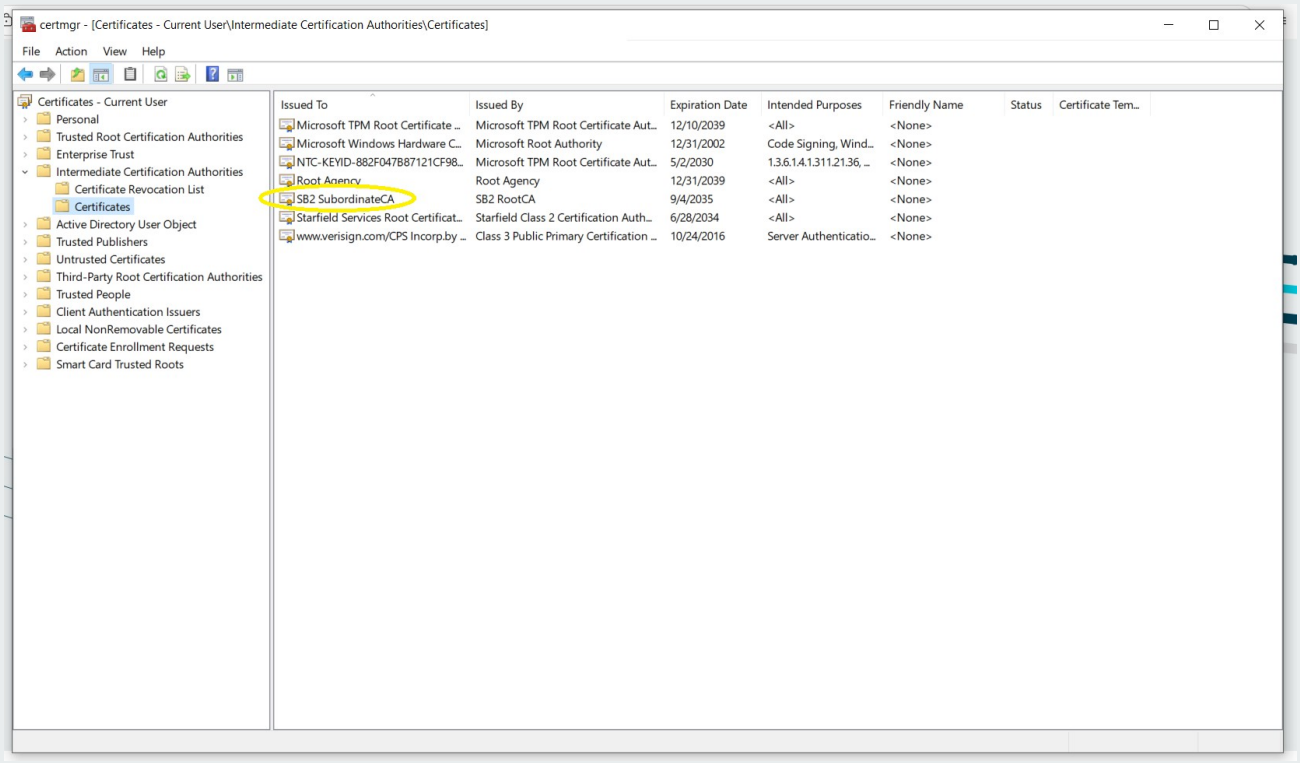



# D12 A Successful Import

Once the **SB2 Subordinate CA Certificate** is imported successfully, a confirmation message will appear. **Click OK** to continue.

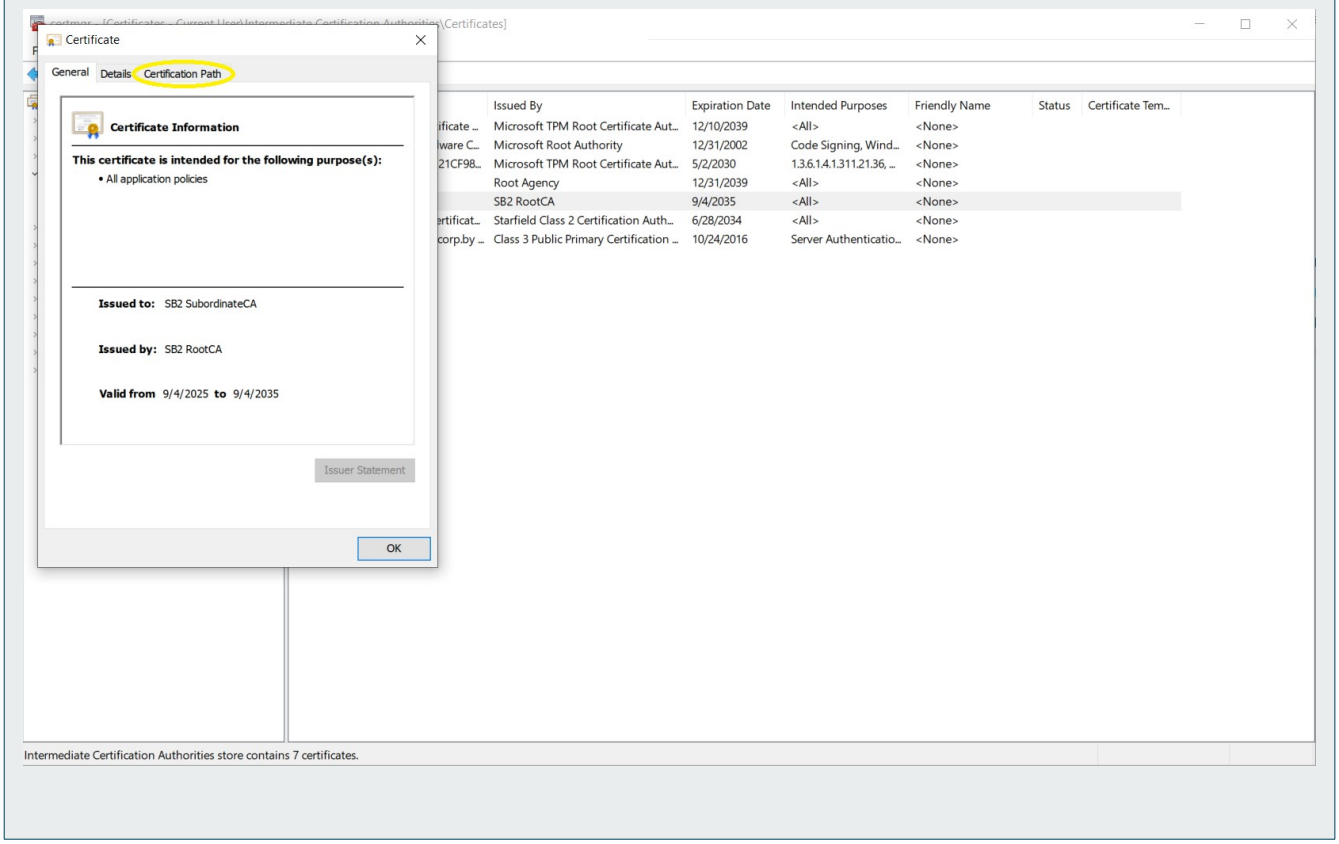
# D13 Verify SB2 Subordinate CA in List of Certificates

After the **SB2 Subordinate CA Certificate** has been successfully imported, it will appear in the **Intermediate Certification Authorities** list as illustrated below:



# D14 Verify SB2 Subordinate CA - Part 1

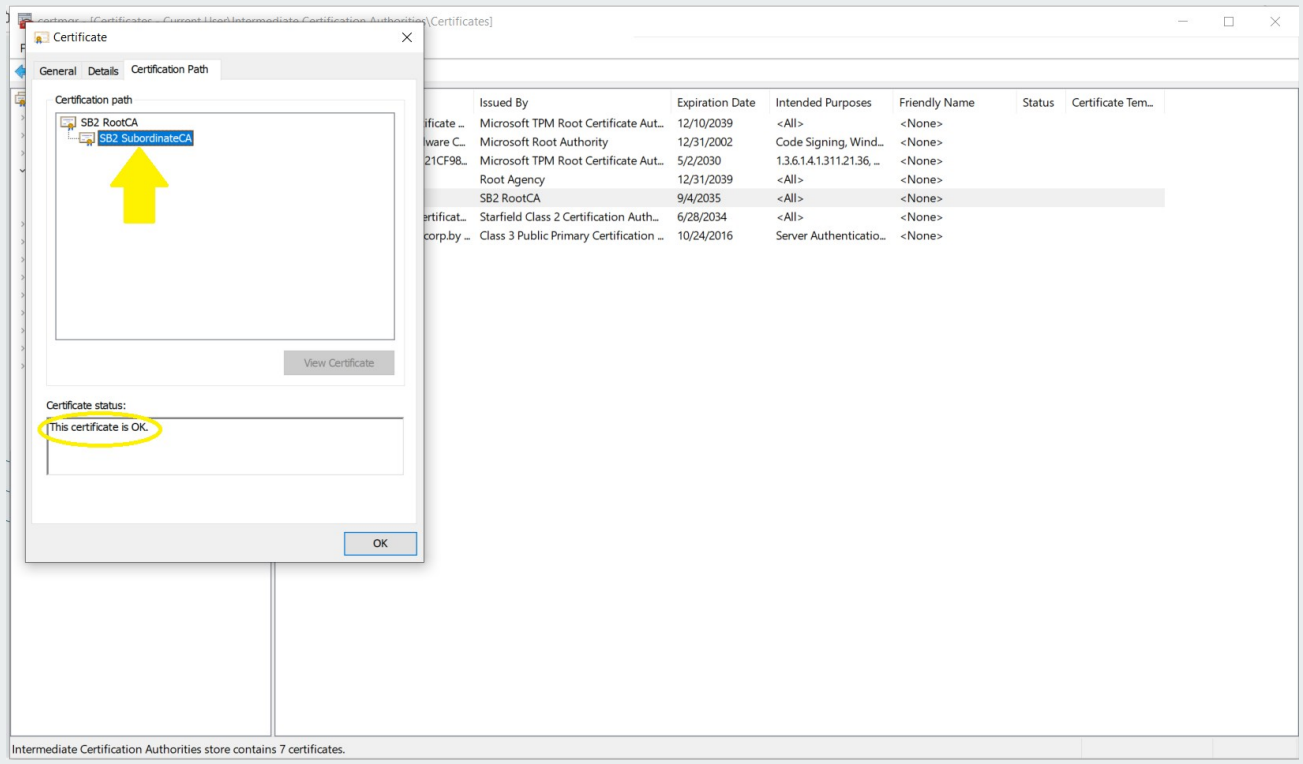
By double-clicking the **SB2 Subordinate CA** certificate – or **right-clicking** the mouse button and selecting **Open**, you should see the following window. Select the **Certification Path** tab in this window:



# D15 Verify SB2 Subordinate CA – Part 2

In the **Certification Path** tab of the **SB2 Subordinate CA** certificate, you should be able to confirm these two important attributes of the certificate:

- That the certificate symbols of the two certificates chained together n the **Certification Path** sub-panel at the top, do not have any yellow warning symbols associated with them, and
- The **Certificate status** sub-panel at the bottom should state that "This certificate is OK."



## D16 Import the SB2DEMO Sub CA2 Certificate

Import the SB2DEMO Sub CA2 certificate by repeating steps D3 - D15.
Remember to verify the Sub CA2 certificate is selected during the process.

## D17 Restart the Computer

Save any open files you may have and restart the computer.

# SECTION E

## E1 Accessing an SB2 Platform URL

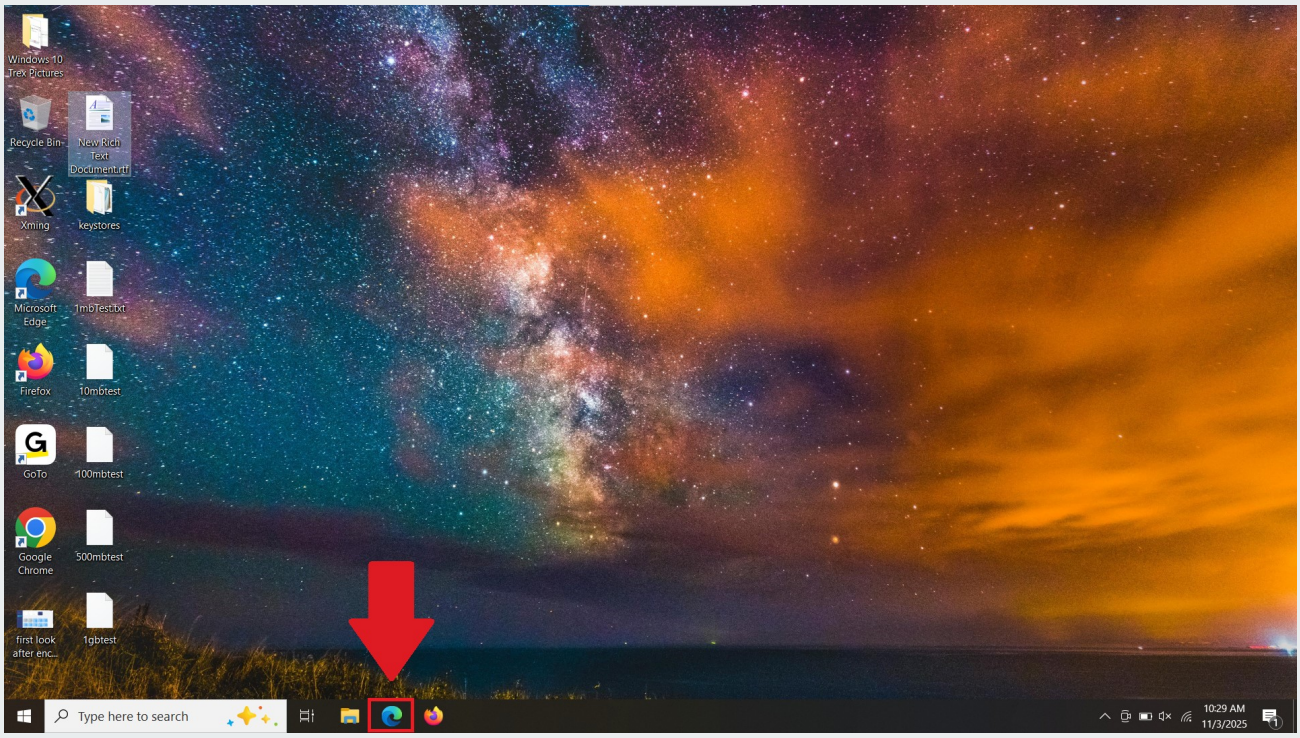
This section will review the steps of accessing an SB2 URL with a Yubikey 5C NFC Security Key.

## E2 Prerequisites

- Windows 10
- Microsoft (MS) Edge Browser, version 141.0.3537.99
- Internet connection
- Yubikey 5C NFC Security Key – with the PIN to the Security Key
- SB2 Platform URL
- USB-C port or USB-C adapter

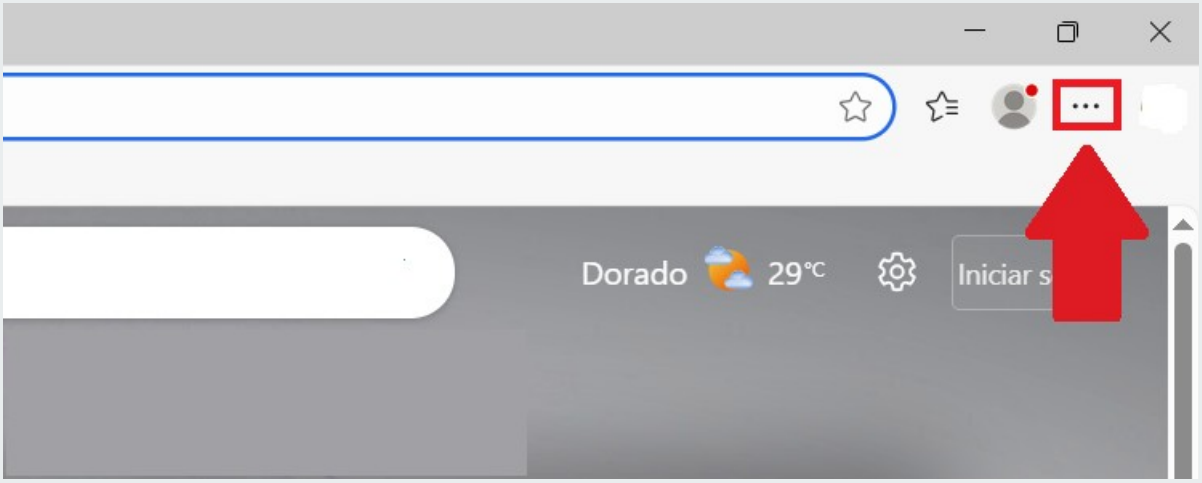
# E3 Open the Edge Browser

To begin, access the Edge browser by selecting its icon from the Windows taskbar.



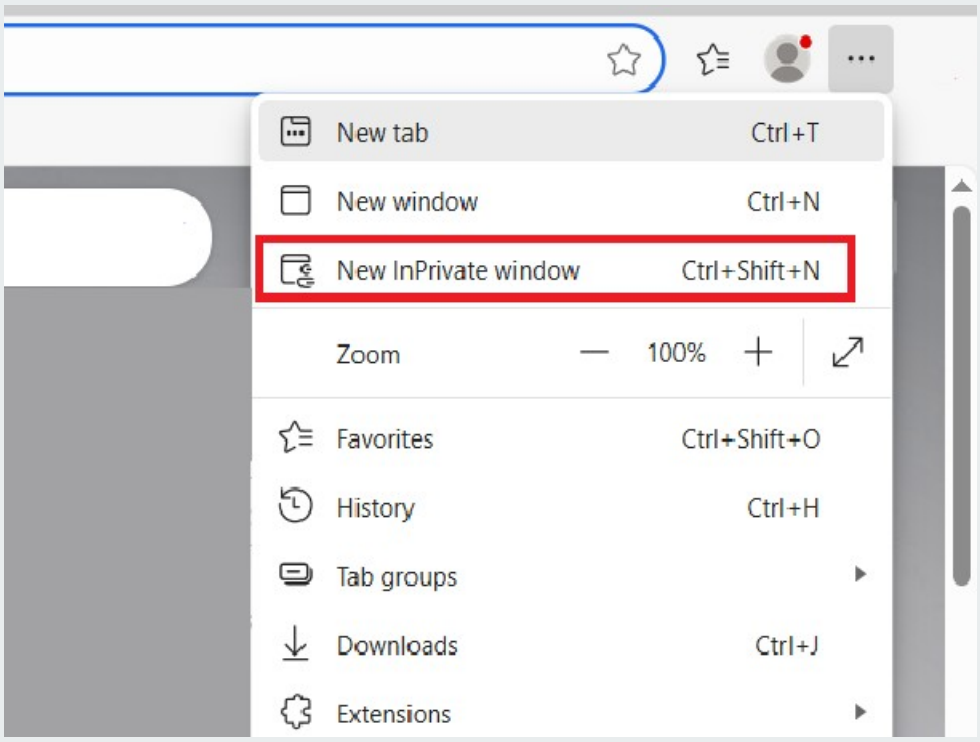
# E4 Find the Edge Drop Down Menu

Locate the three-dots icon on the right side of the screen and select it.



## E5 Open a New InPrivate Window

Access the SB2 URL in Edge's InPrivate window.




## E6 Plug in the Yubikey

Plug the **Security Key** into the USB-C port (or the USB-C to USB-A adapter)

## E7 Identifying the USB-C port

Locate the USB-C port—typically found along the edge of the computer, it features a compact design with smooth, rounded corners that set it apart from traditional USB-A ports.
The image below shows both a USB-C port and its matching male connector.

## E8 No USB-C port? No problem.

With the USB-A to USB-C adapter provided by the Administrator of your SB2 site, simply plug the USB-A end into the computer and insert the Security Key into the USB-C port.

The provided USB adapter pictured below.

## E9 SB2 Platform URL

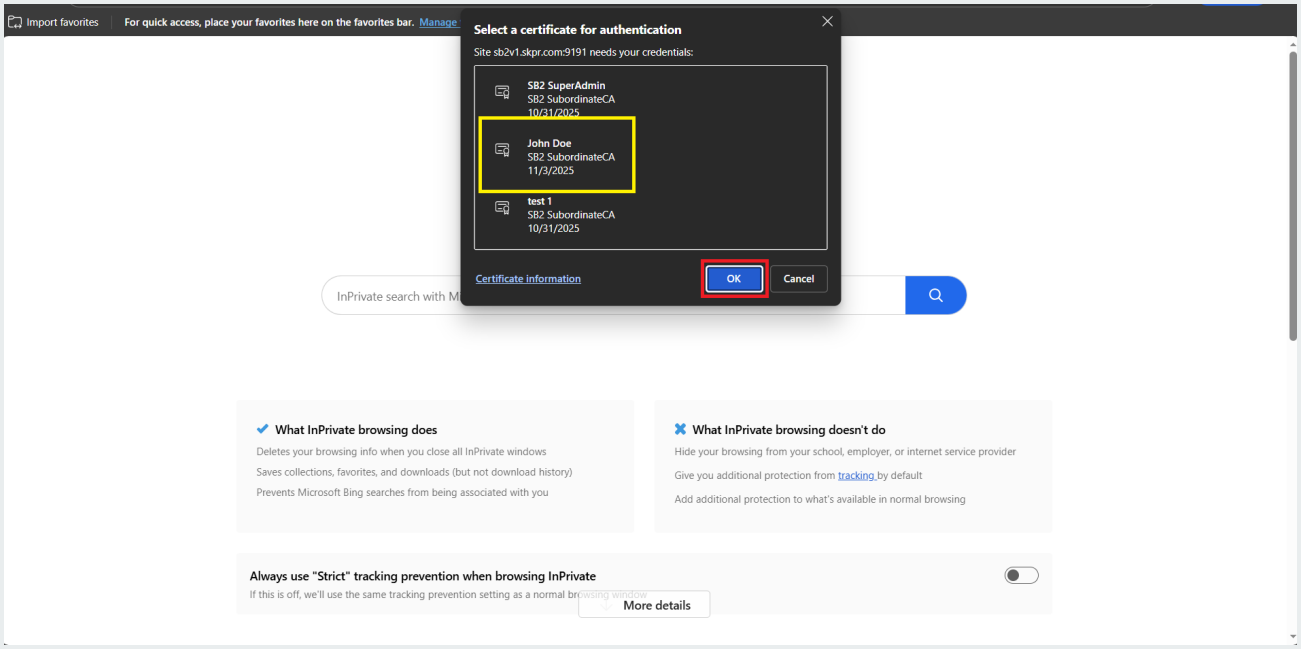
In the InPrivate browser address bar, enter the provided SB2 Demo invitation link. You will receive the link in an email from a member of the StrongKey Team. **Please note**, the URL is long so it will be advantageous to use the "cut and paste" options. Here is an example of what the URL will look like:

•https://sb2demo.strongkey.com:443/sb2/register?hash=3d500dec79f6ec257ebddcc56hj78ff1f2d31d557d4c7bf5654

# E10 Select the Certificate

A pop-up window will display the available certificates (yellow box). The name in the prompt should match your name, as created by the Administrator of the SB2 site. Select the certificate and **click OK** to proceed.

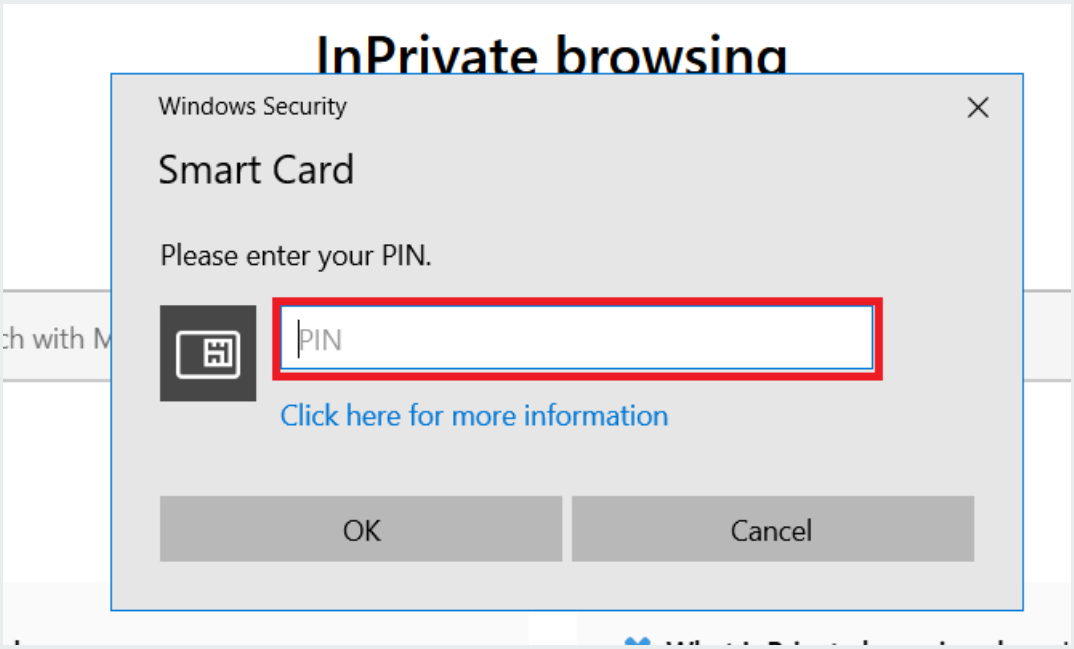
**NOTE**: You will only see such a certificate prompt if the **SB2 Root CA** and **SB2 Subordinate CA** certificates were imported correctly on your computer. If you do NOT see a certificate prompt, please contact the Administrator of your SB2 site for help.



# E11 Enter Security Key PIN

The next dialog box will prompt for the Yubikey 5C NFC (aka Smartcard) PIN. Enter and **click OK** to continue. This PIN should have been provided to you by the Administrator of the SB2 site.

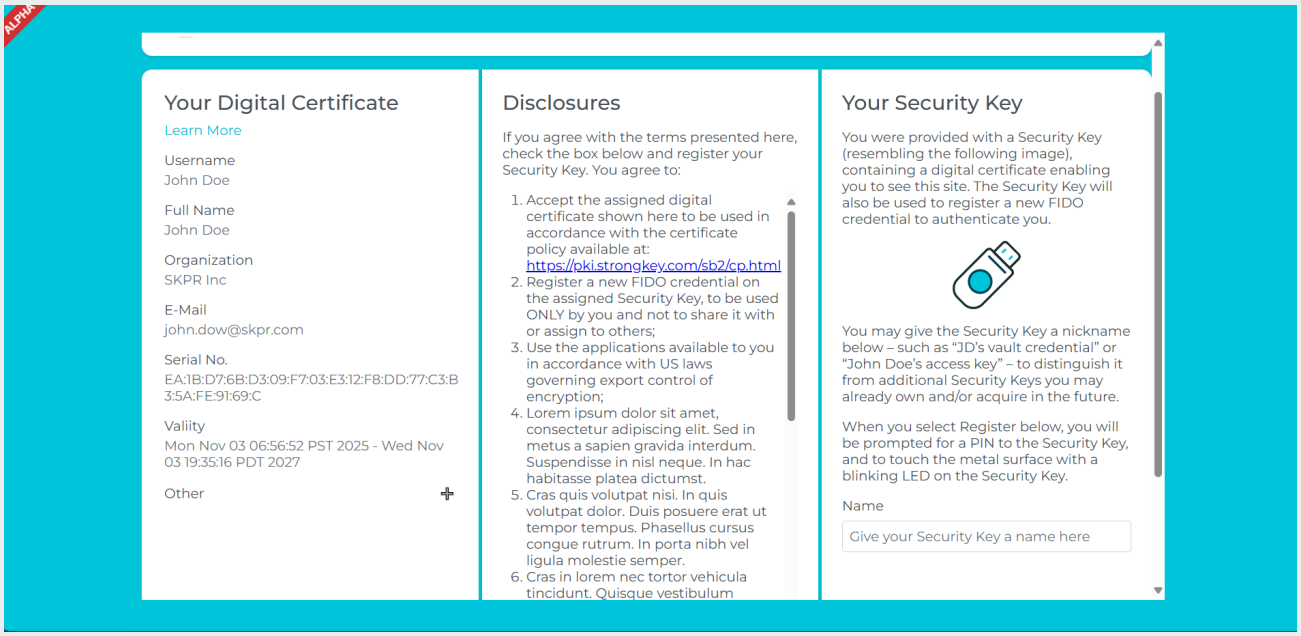
*For instructions on changing the Yubikey PIN, refer to the appendix of this guide.*



# E12 SB2 Landing Page

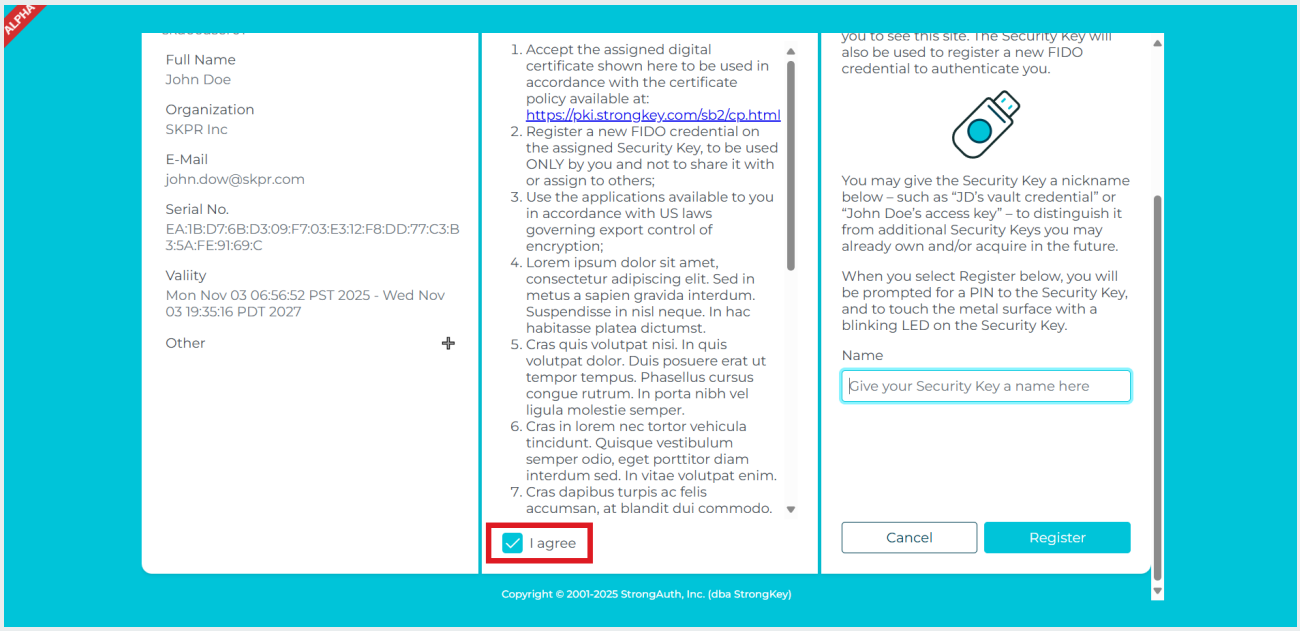
Upon successful authentication with the digital certificate, the following one-time **SB2 Landing Page** will be displayed. This page has three (3) sections:

- On the left-hand side, details of your digital certificate information will be displayed.
- In the middle section are the legal disclosures by the SB2 platform. You must scroll all the way to the bottom and **agree** to the terms disclosed before continuing.
- On the right-hand side, is the option to give your **Security Key** a nickname to distinguish it from other Security Keys.



# E13 Terms and Conditions

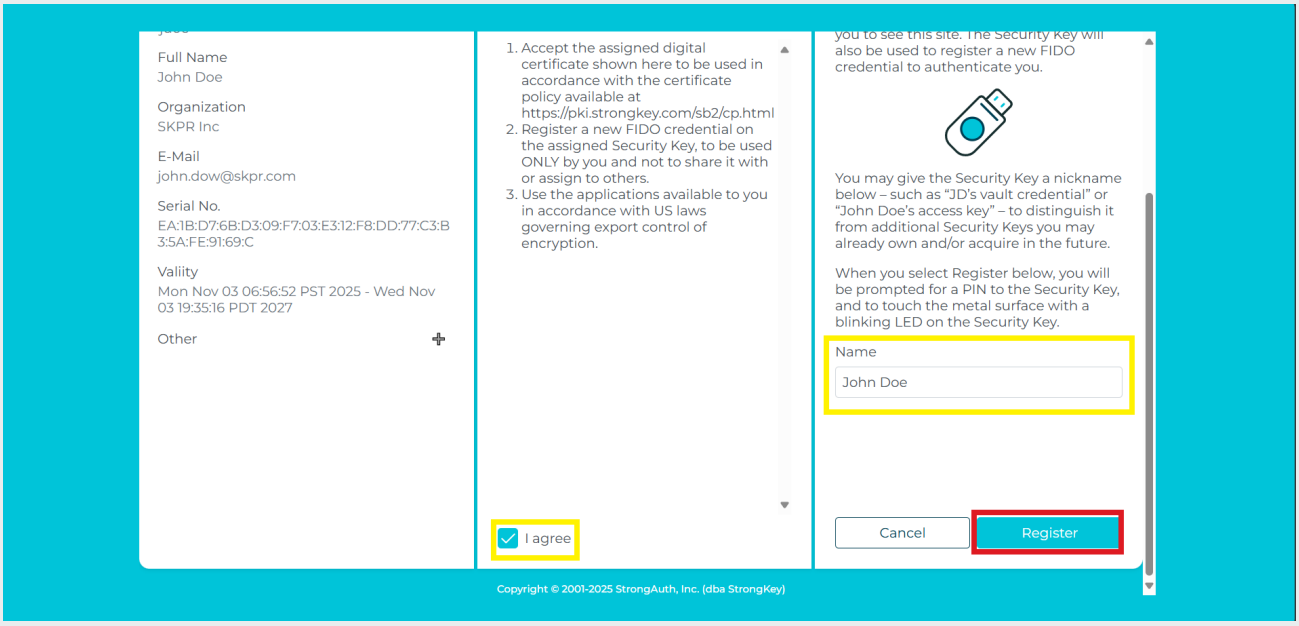
Review and accept the terms and conditions in the **Disclosures** panel. The **"I agree"** box must be checked before proceeding with **Security Key** registration.



# E14 Give the Security Key a Nickname

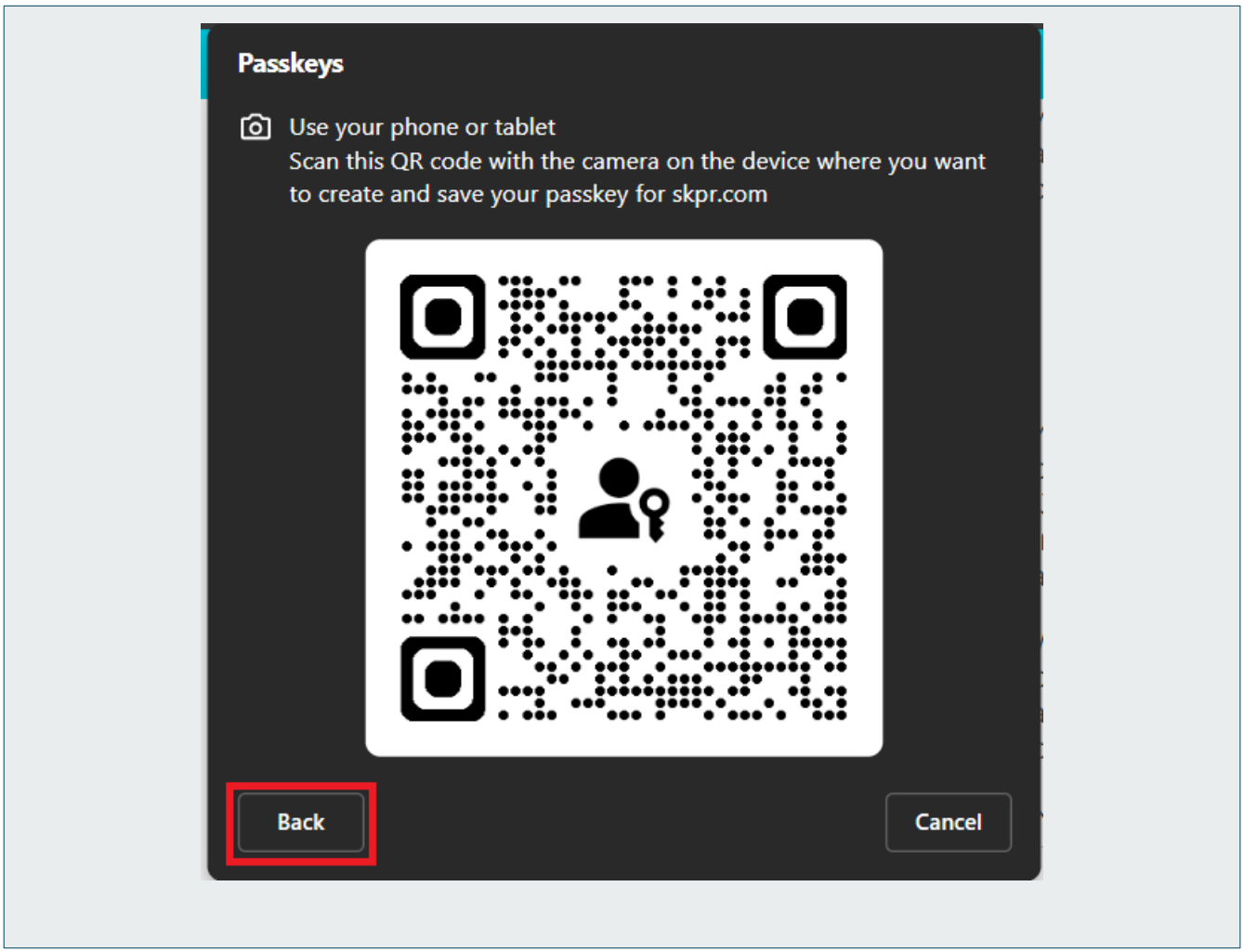
In the Security Key panel on the right, enter a descriptive nickname for the key in the **Name** field. Then select **Register** to complete the process. Names are typically short (up to 16-20 alpha-numeric characters):

- John's SB2 key at mysite.com
- Yubikey for mysite.com SB2



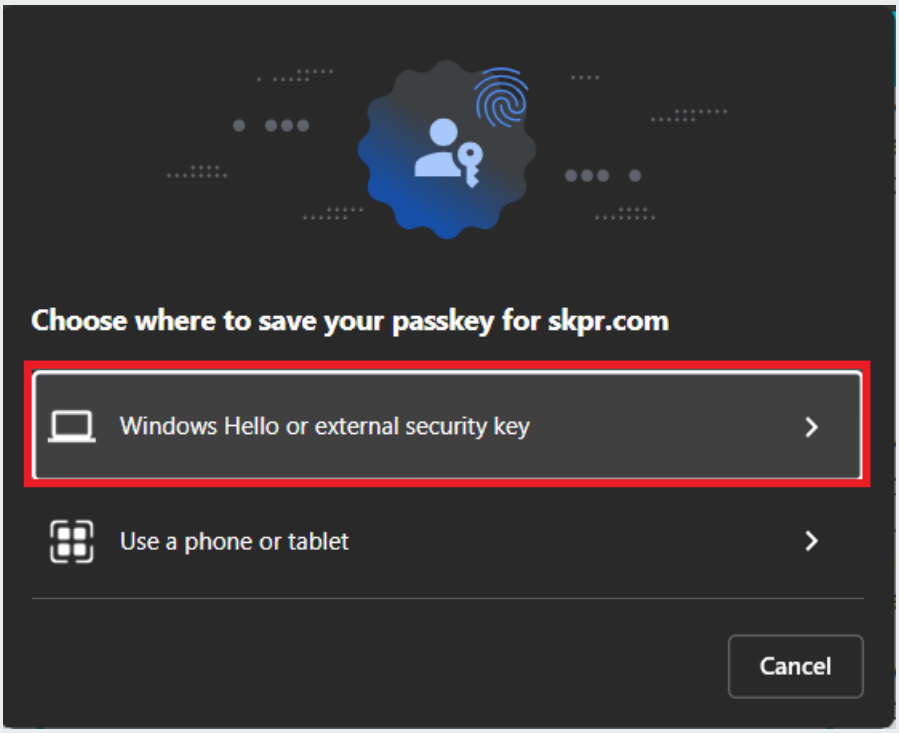

# E15 Save 'Passkeys' Option

A box will appear at the top of the page providing the option to create a Passkey. Do not create a Passkey. **Click** on **Back** to continue.


Passkeys
Use your phone or tablet
Scan this QR code with the camera on the device where you want to create and save your passkey for skpr.com
Back
Cancel

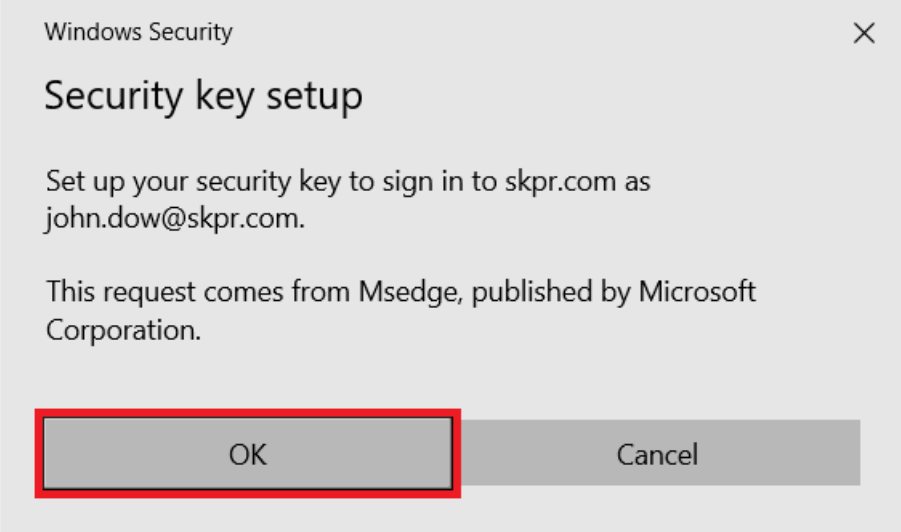
# E16 Select external security key

A box will appear at the top of the page. **Click** on **Windows Hello or external security key** to choose a security key and continue.



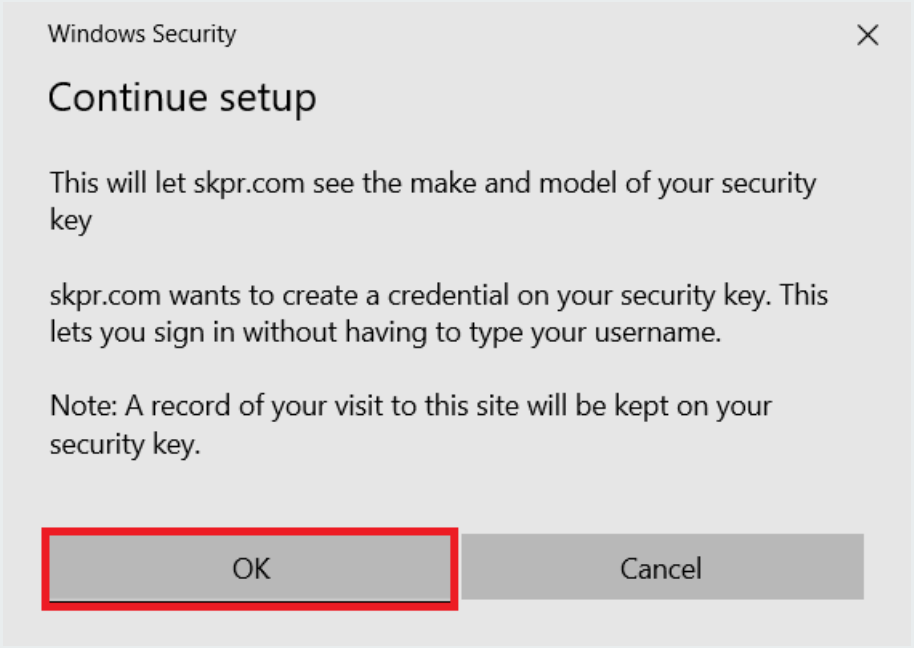
# E17 Security Key Setup

A dialog box will verify the **Security Key** is being setup to login to the SB2 Platform. **Click OK.**



# E18 Continue Setup

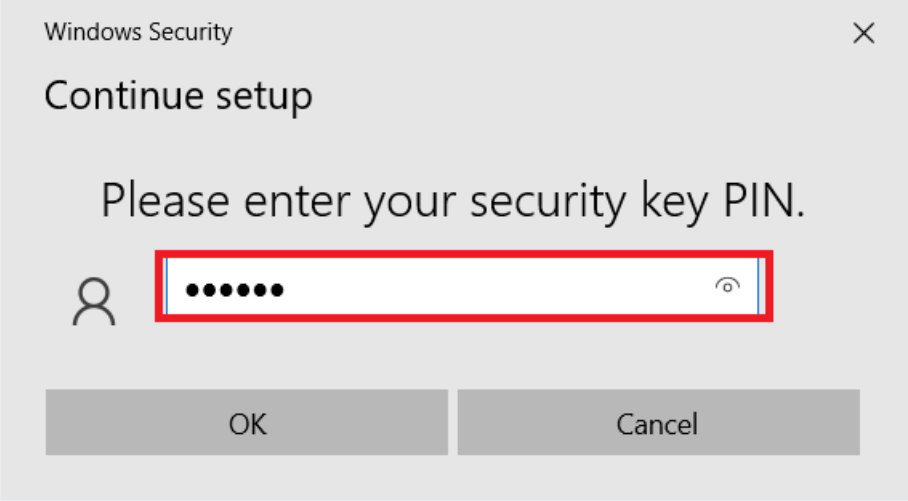
This message is to inform the user the SB2 Platform will create a credential on the **Security Key. Click OK.**



# E19 Enter Security Key PIN

To continue adding a credential to the **Security Key**, enter the PIN and **click OK**.

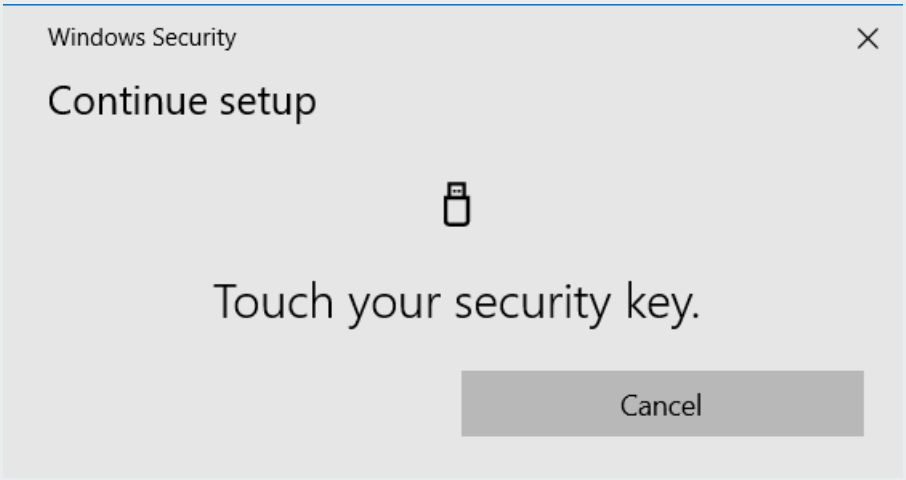
**NOTE:** This step in the process is known as the "**User Verification**" (aka UV) in the FIDO ecosystem. It is a security feature of the FIDO authentication protocol to ensure that the SB2 platform can verify the legitimate owner's PIN of the **Security Key**. SB2 sites will mandate a security policy where the PIN to the **Security Key** is not shared with others. Every time the FIDO credential is used to authenticate you to the SB2 platform, you will be required to perform the UV function as a security precaution.



## E20 Touch the Security Key

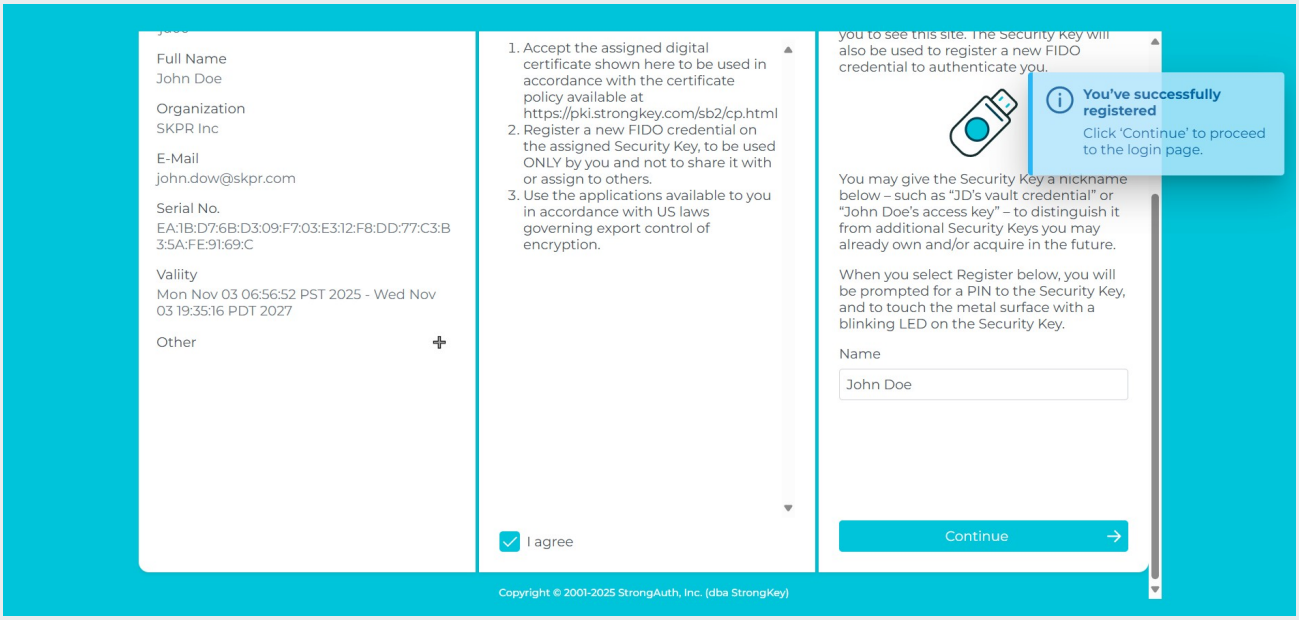
To continue the setup, touch the metal contact visible on the **Security Key** with your finger, it will have a light-emitting diode (aka LED) blinking to indicate where it must be touched.

**NOTE:** This step in the process is known as the "**Test of User Presence**" (aka TUP) in the FIDO ecosystem. It is a security feature of the FIDO authentication protocol to ensure that a remote attacker can never steal your identity from a remote computer since they will neither have a **Security Key** with your FIDO credential nor will they be able to perform the "test of user presence" at your computer (where the FIDO transaction is occurring). Every time the FIDO credential is used to authenticate you to the SB2 platform, you will be required to perform the TUP as a security precaution.



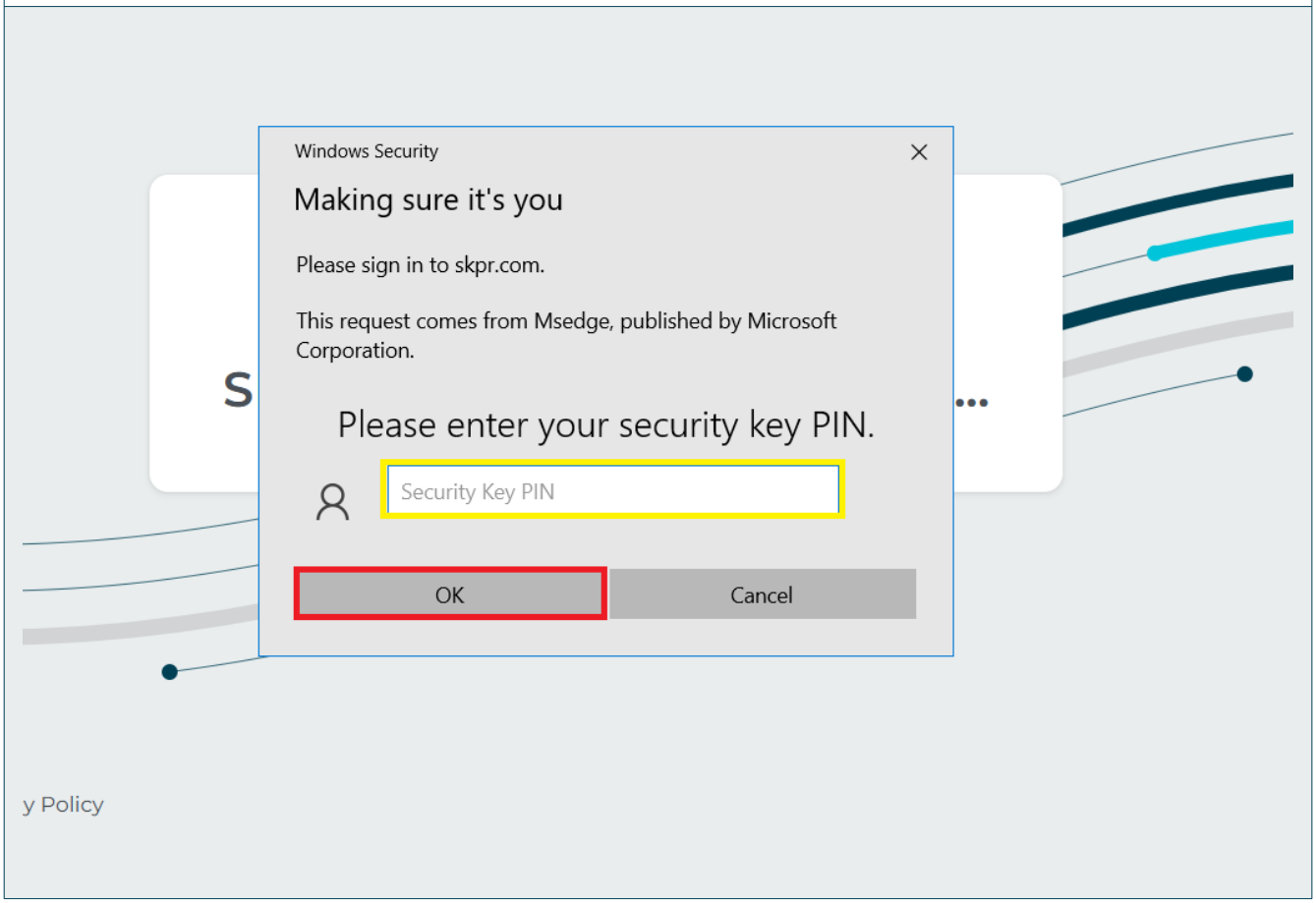
# E21 SB2 Confirmation

After clicking OK, SB2 will flash a blue message confirming successful registration.



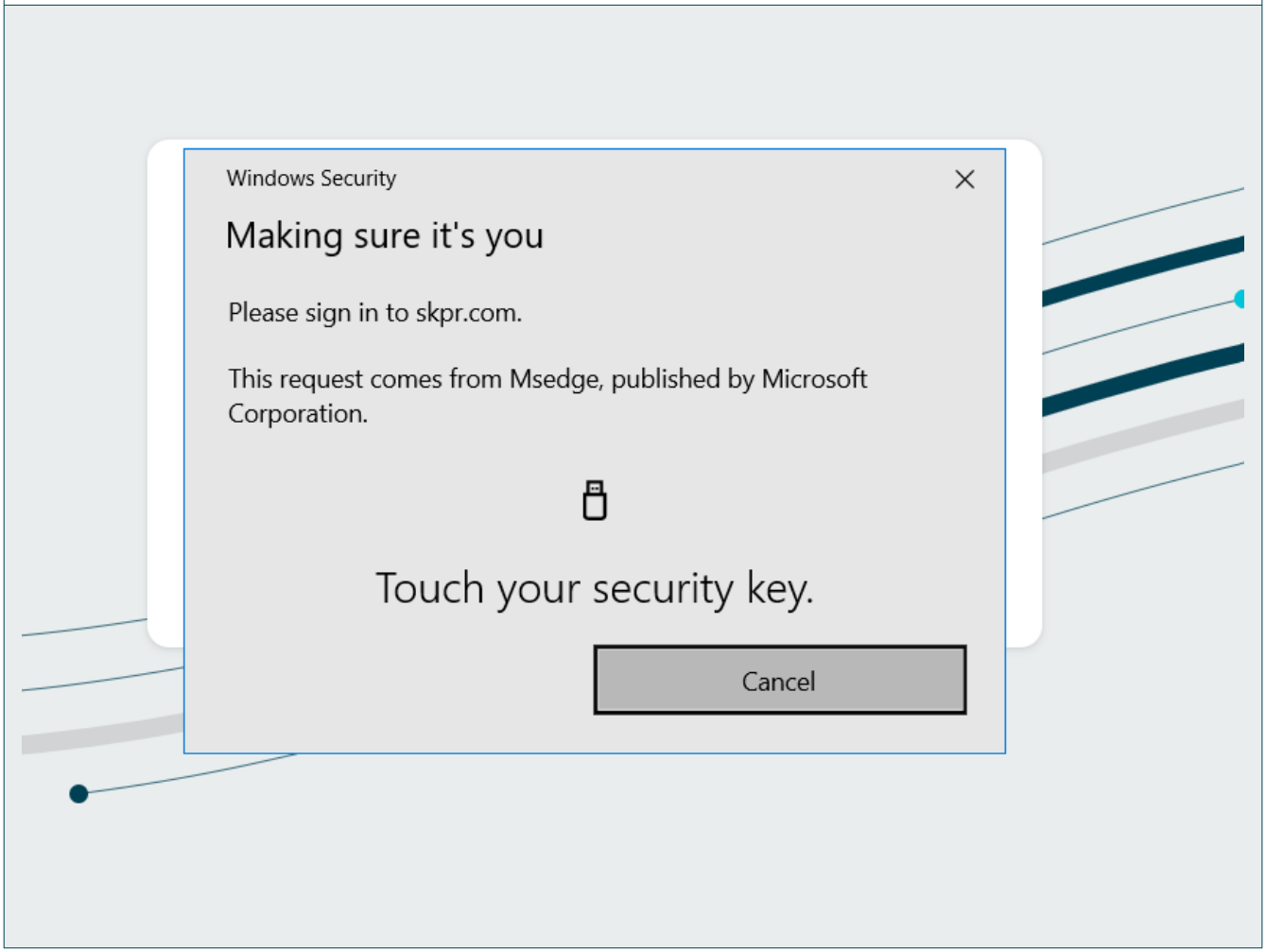
# E22 User Authentication

The next dialog box will verify the user. Enter the PIN to the **Security Key** and **click OK.**



# E23 Test of User Presence

To continue the login procedure, touch the metal contact on top of the **Security Key** where an LED is blinking – this confirms a user is present and attempting to sign in from that computer with a legitimate credential on the **Security Key**.

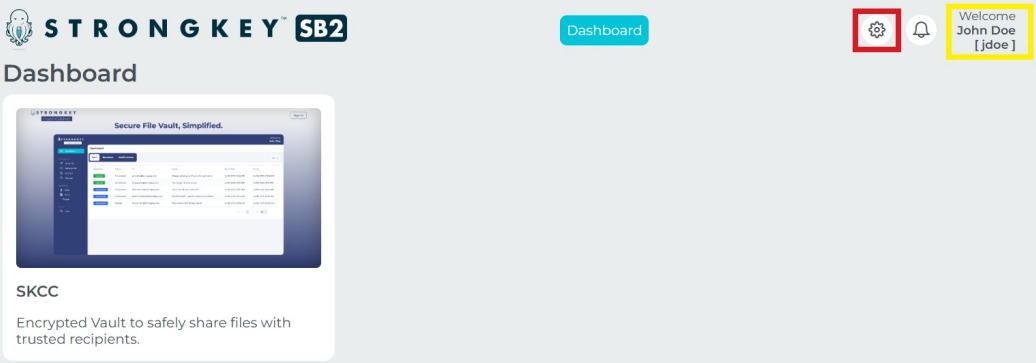


# E24 SB2 Platform Dashboard

CONGRATULATIONS!

Your access to the **SB2 Platform** has been successfully established, and your **Security Key** with your new FIDO credential is registered. Your account name is displayed on the right side of the screen. You may click the gear icon to edit your **profile**.

All users of the SB2 platform have access to a web application – StrongKey CryptoCabinet (SKCC) – that enables the secure storage and sharing of files with sensitive data. Clicking on the SKCC image on the SB2 Dashboard opens a new tab in the browser and presents the SKCC Dashboard. Details on how to use SKCC are provided in separate documents.



# Appendix

STRONGKEY™

# Changing a Yubikey Personal Identification Number (PIN)

# AP1 Changing a Yubikey 5C NFC Personal Identification Number (PIN)

The **Security Key** is a very powerful cybersecurity device and represents the state-of-the-art in multi-factor authentication (MFA) technology that does not use any passwords. The MFA is supported by the:

- **Possession factor** – where the physical possession of the Security Key is essential to the authentication process;
- **Knowledge factor** – where know the PIN to the Security Key is also essential to the authentication process.

Since the **Security Keys** provided with the SB2 use two different NIST-approved, passwordless authentication protocols, there are two containers for the cryptographic keys used with the protocols. Each container is managed by a separate PIN.

However, StrongKey recommends using the SAME PIN to both containers of the **Security Key** to reduce the burden on users. As long as the **Security Key** is safely in the possession of the legitimate user, and the legitimate user is NOT sharing the PIN to the **Security Key** with anyone, the user will be complying with one of the strictest security policies recommended for access control.

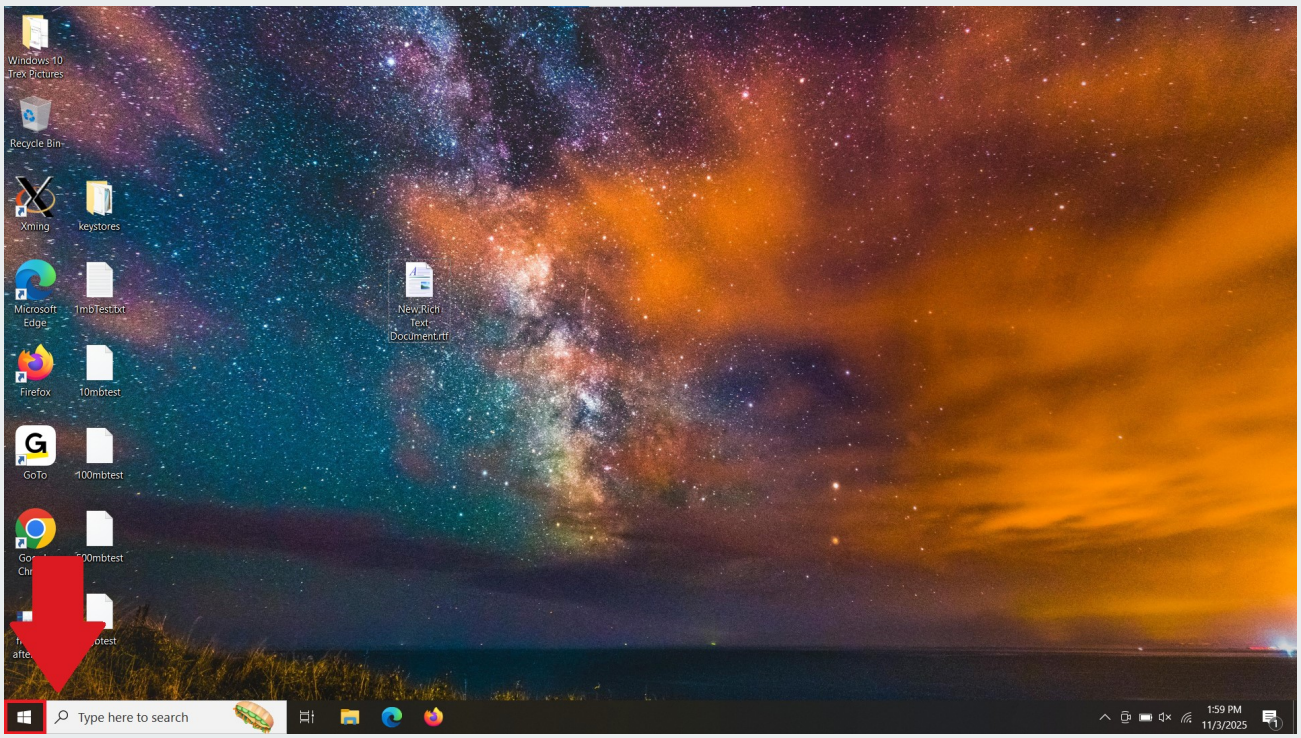
This document outlines the process for changing the two required PINs – one for the digital certificate and the other for the FIDO credential.

# AP2 Prerequisites

- Windows 10
- USB-C port or USB-C adapter
- Yubico Authenticator application

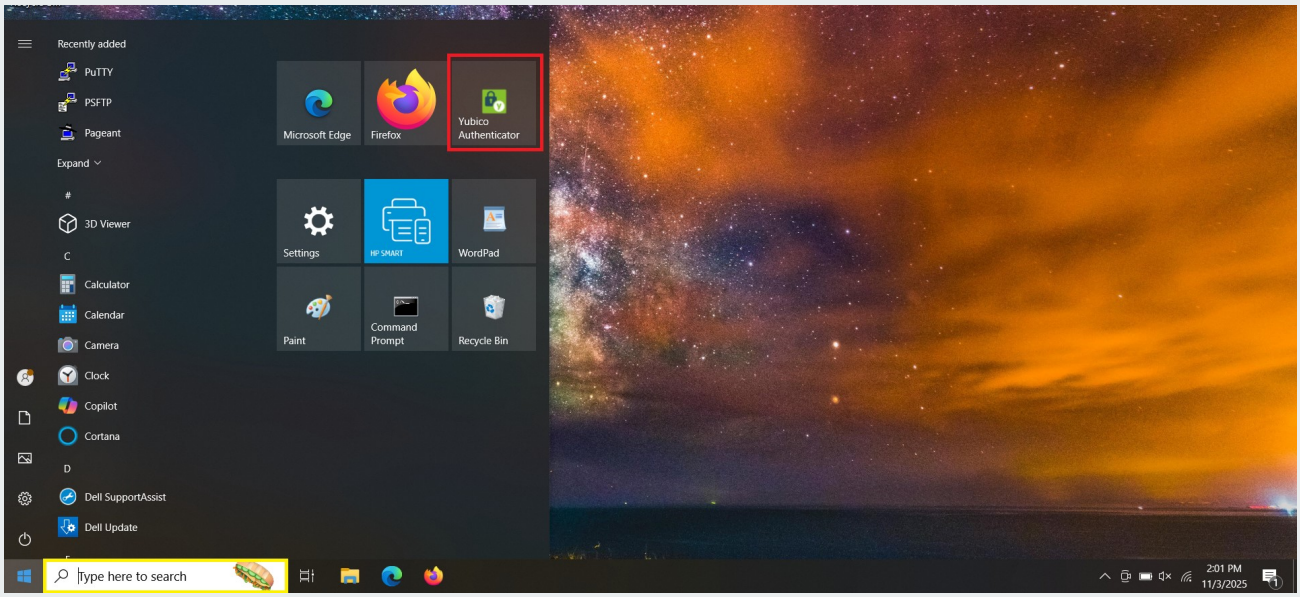
# AP3 Open the Yubico Authenticator Application

To begin, access the Yubico Authenticator application by selecting the **Windows icon** from the Windows taskbar.



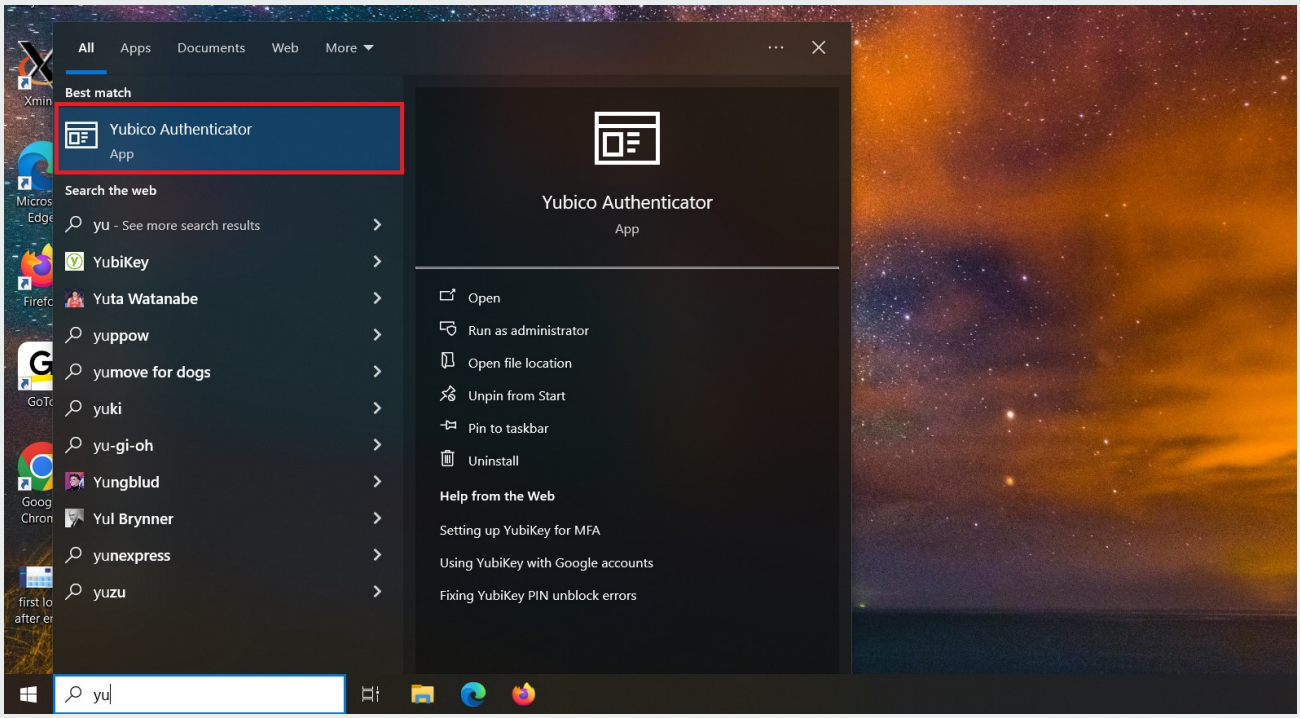
# AP4 Select Yubico Authenticator

From the menu, select the **Yubico Authenticator application**. If it does not appear, type ‘Yubico Authenticator’ in the search bar or scroll down in the recently added tab.



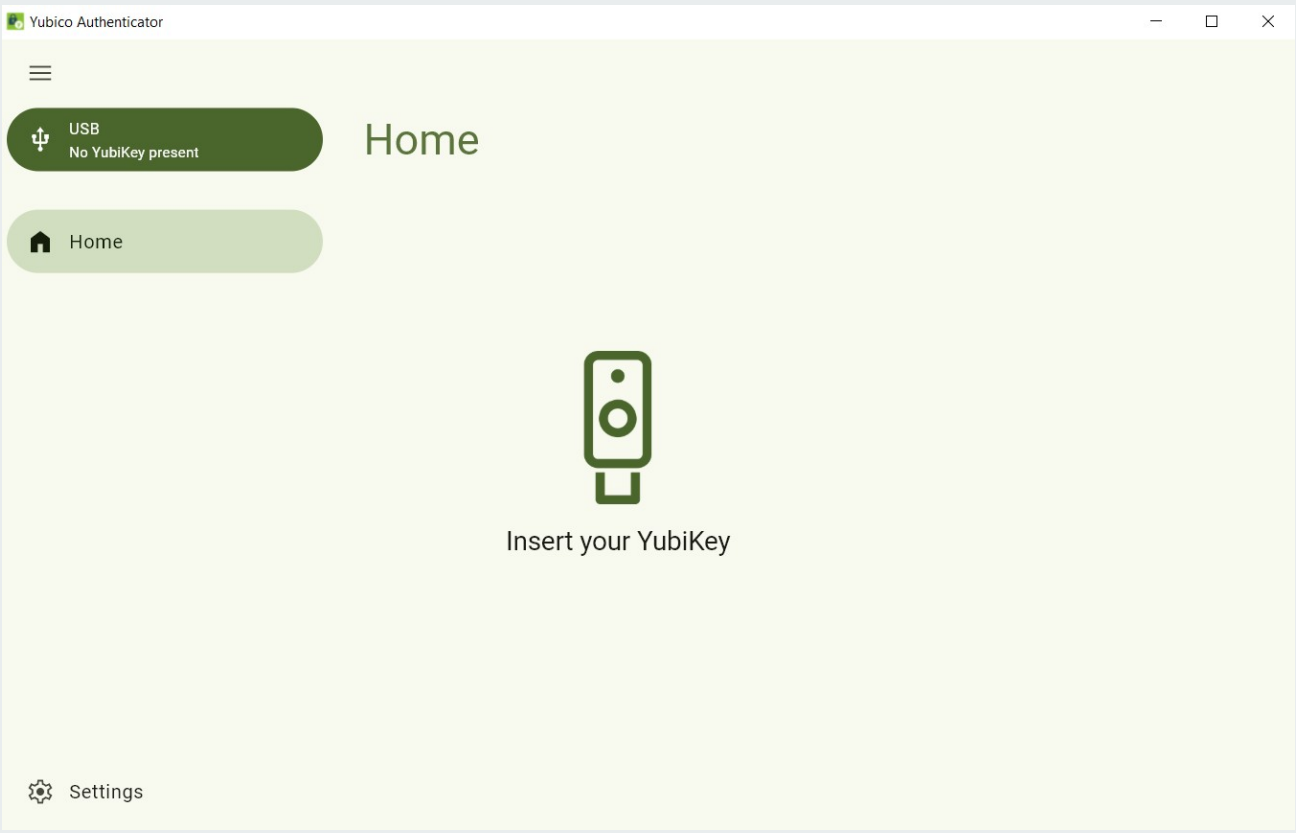
# AP5 Using the search bar

After typing a few letters of Yubico Authenticator, the application will display. Hit **Enter** on the keyboard or **click** on the application name to access.



## AP6 The Yubico Authenticator application

Upon opening, the Authenticator application displays the screen shown below and indicates there is **“No Yubikey Present.”**




## AP7 Insert the Yubikey

Plug the **Security Key** into the USB-C port.

## AP8 Identifying the USB-C port

Locate the **USB-C port**—typically found along the edge of the computer, it features a compact design with smooth, rounded corners that set it apart from traditional USB-A ports. The image below shows both a USB-C port and its matching male connector.

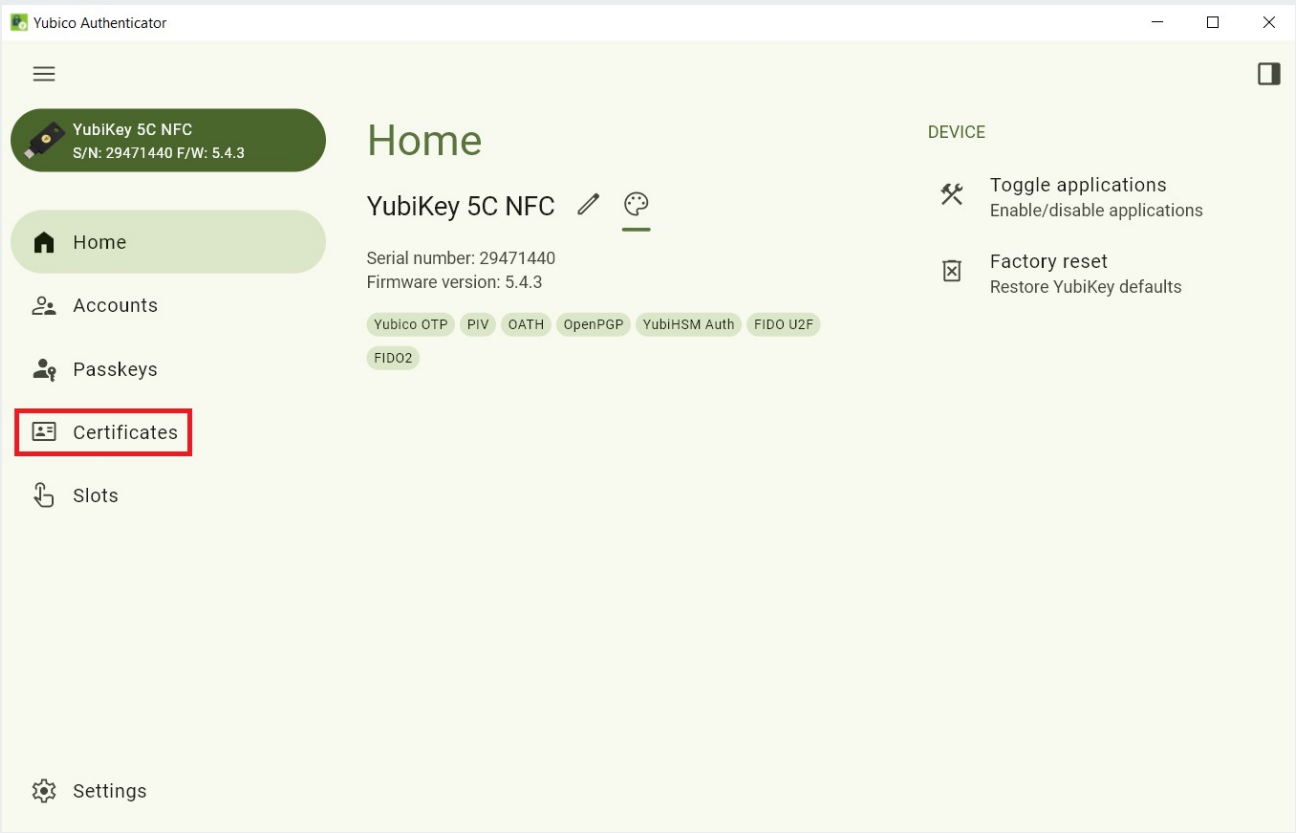
## AP9 No USB-C port? No problem.

With the provided **USB-A to USB-C adapter**, simply plug the USB-A end into the computer and insert the **Security Key** into the USB-C port.

The provided USB adapter pictured below.

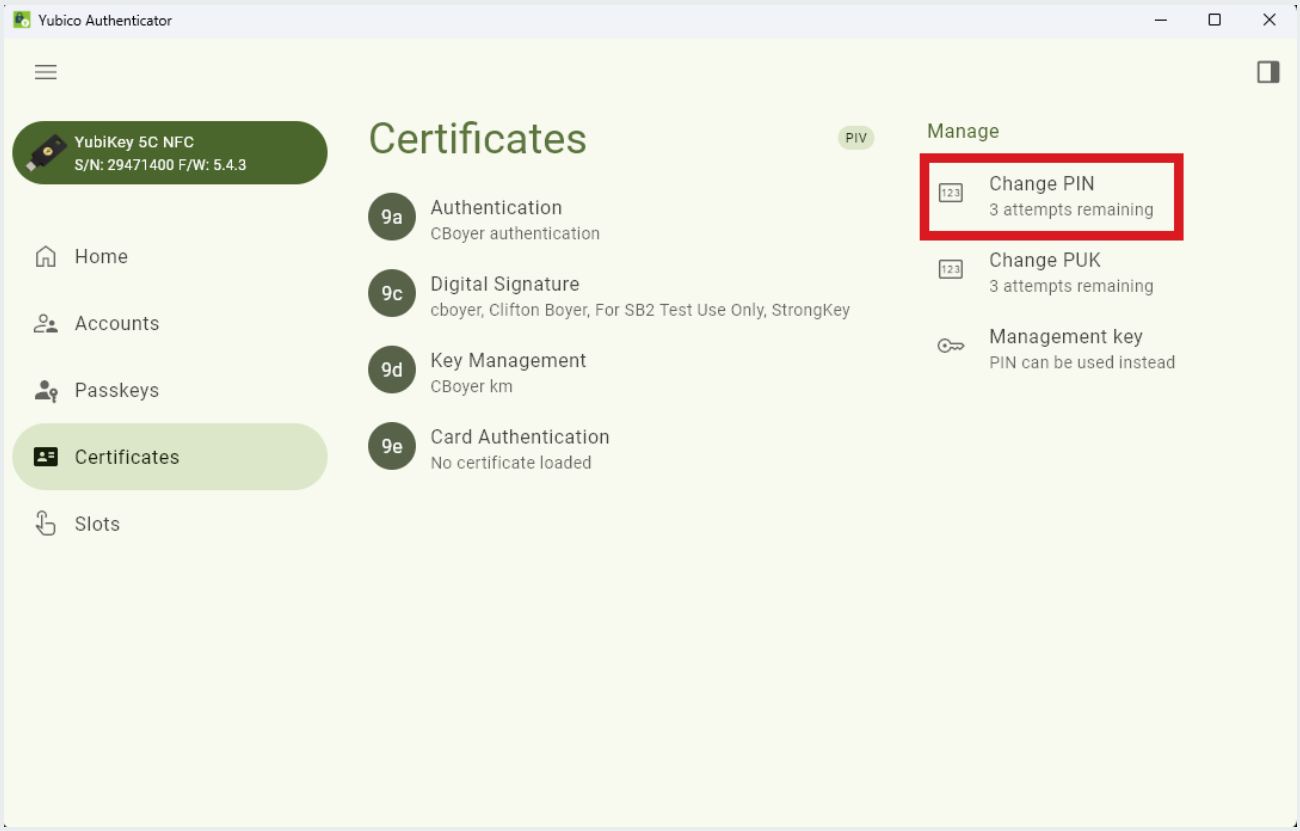
# AP10 Changing the Digital Certificate PIN

From the home screen, navigate to the left and select the **Certificates** option from the menu.



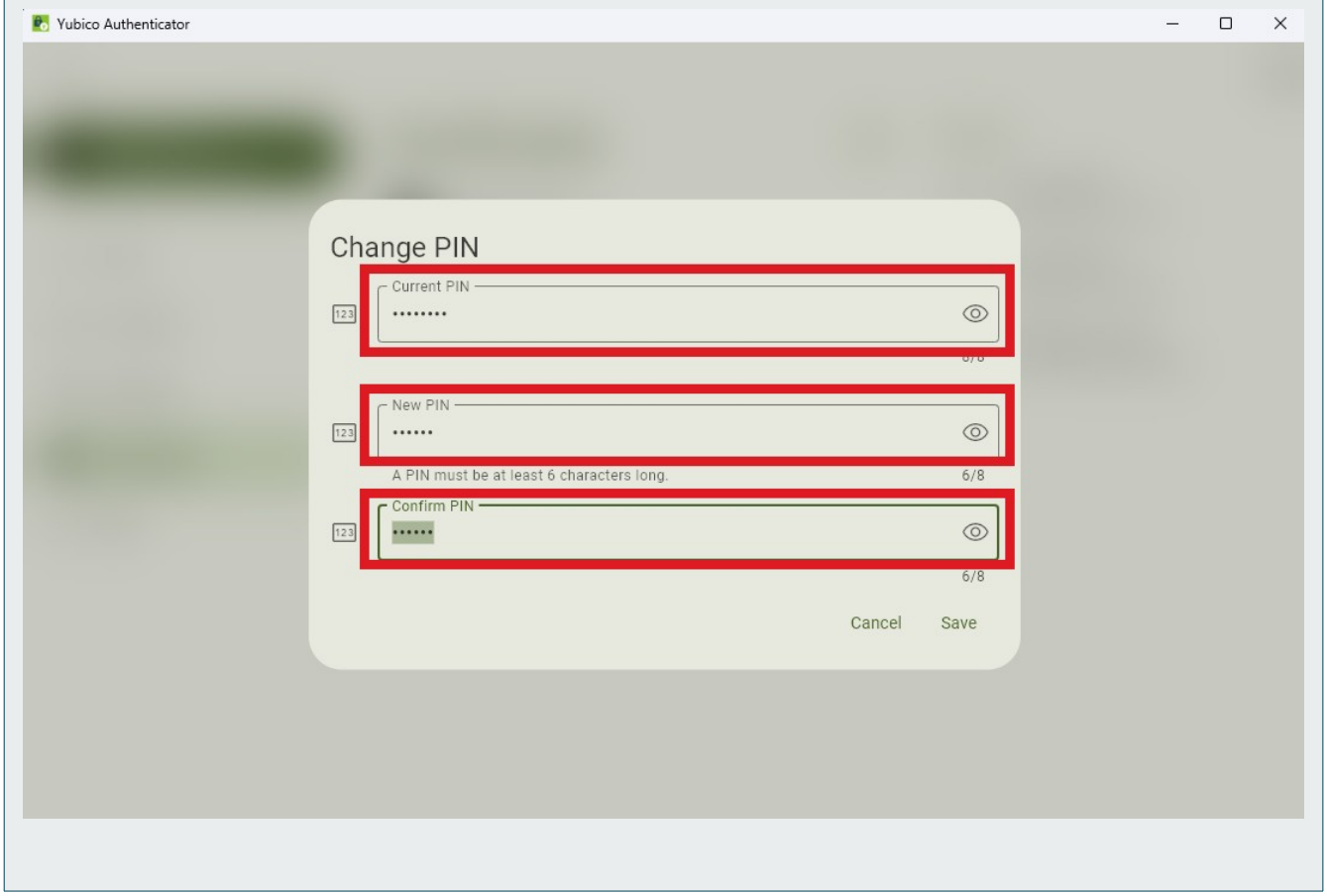
# AP11 Change PIN option

Select the **Change PIN** option from the **Manage** menu on the right.



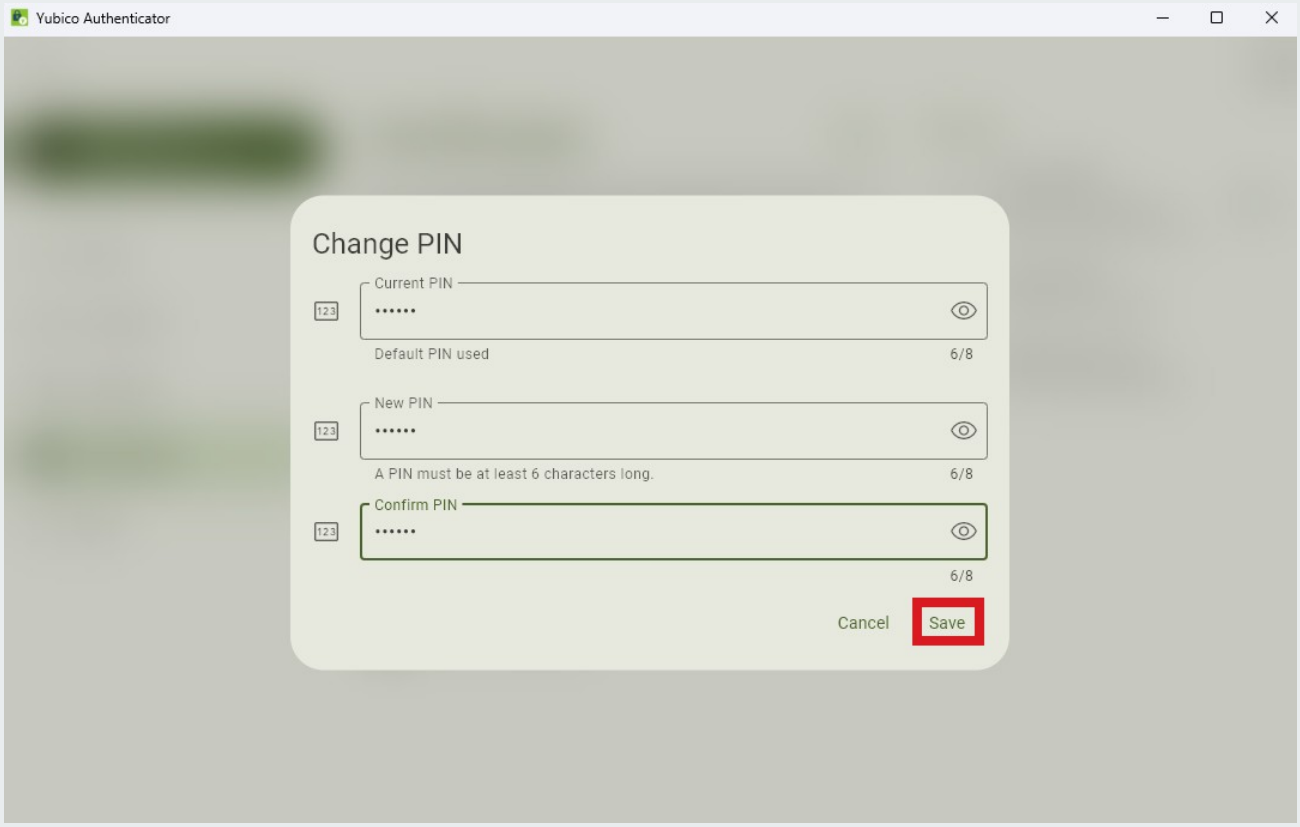
# AP12 Enter PIN information

- In the top field, enter the **default PIN: 123456**.
- Enter the new PIN in the middle field. The PIN must contain 6 to 8 characters.
- Re-enter the new PIN in the final field to confirm.



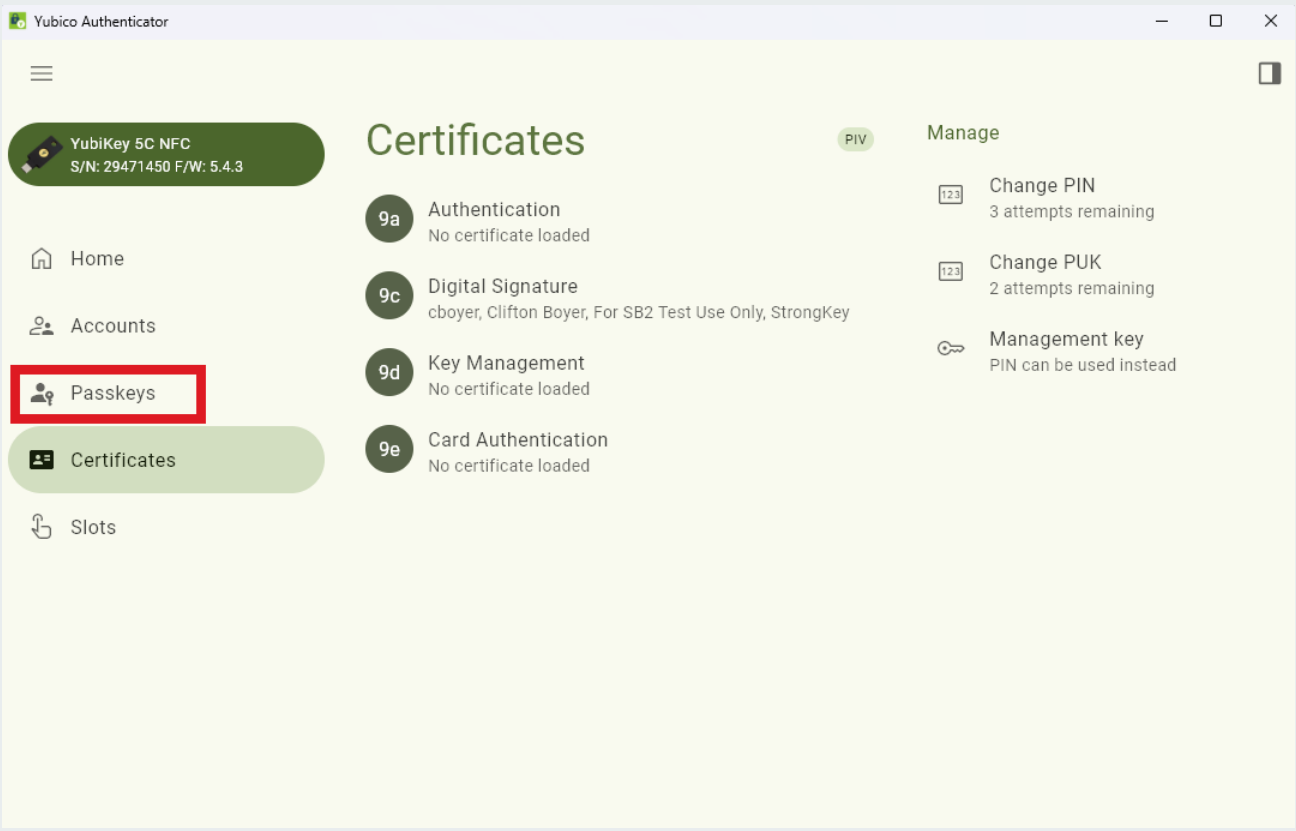
# AP13 Save new PIN

**Click Save.** The application returns to the previous screen. If the process is successful, a “PIN changed” notification briefly appears at the bottom of the screen.



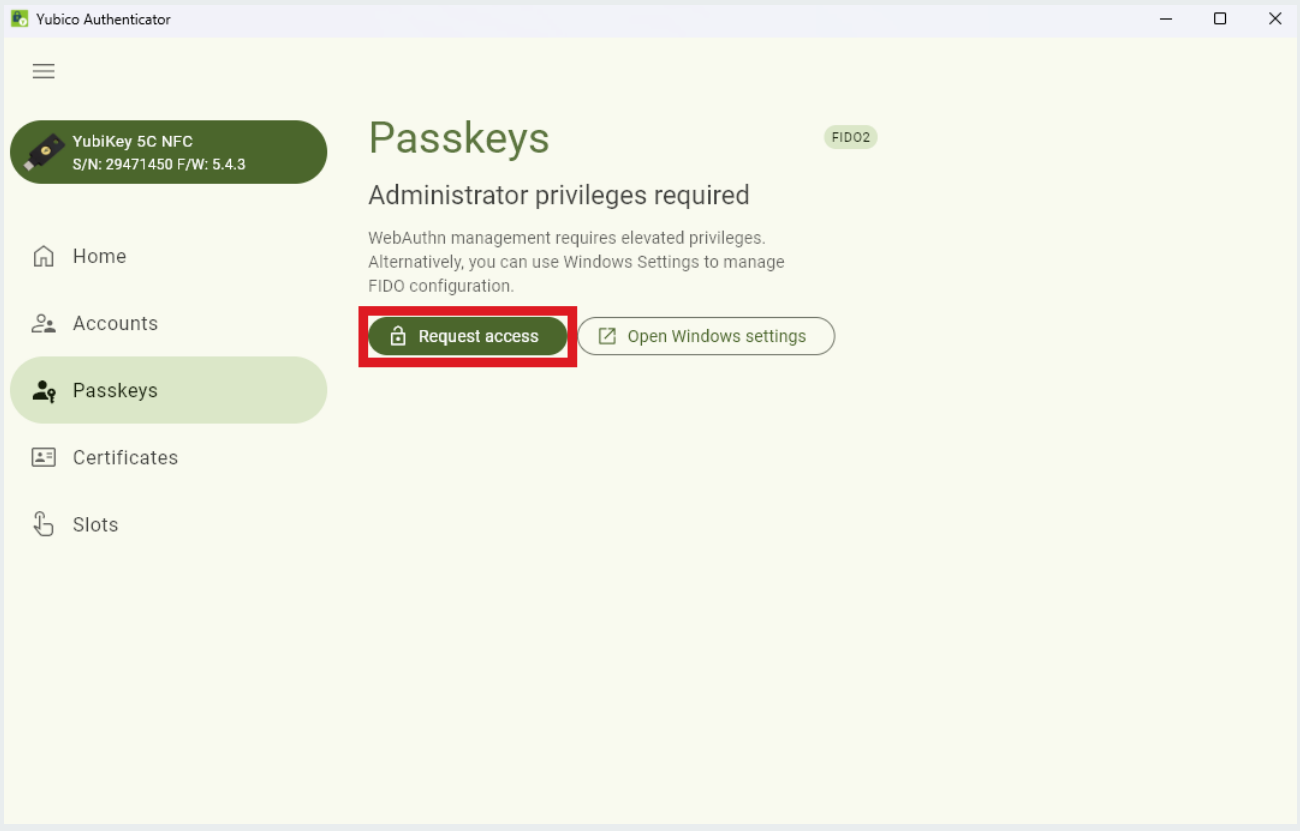
# AP14 Changing the FIDO Credentials PIN

To update the second PIN, click on the **Passkeys** menu option to the left. **NOTE: StrongKey recommends using the same PIN for the Security Key.**



## AP15 Passkeys Menu

In the Passkeys menu, select **Request Access.**

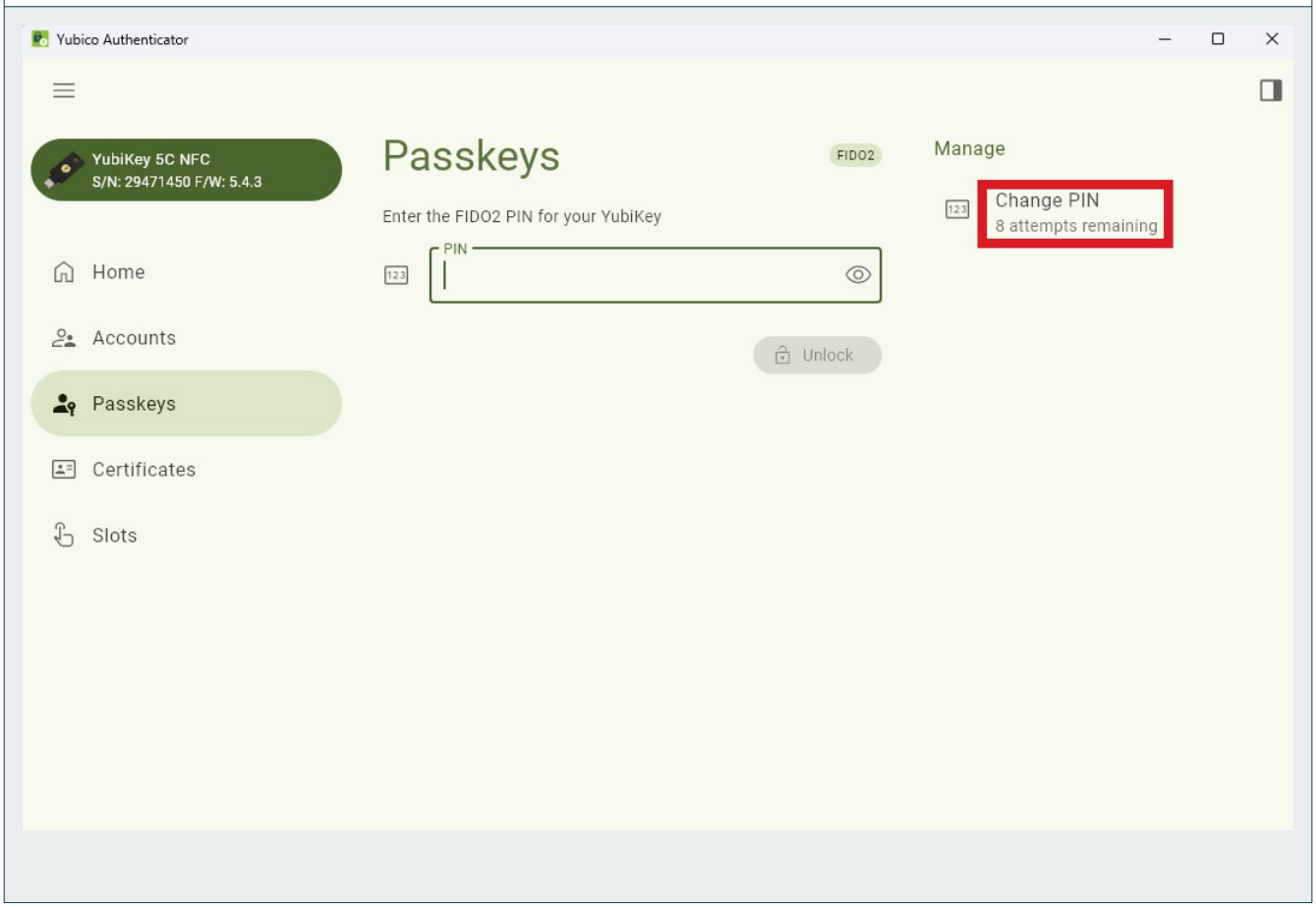



## AP16 Yubico Authenticator Application Permission

The Yubico Authenticator application will ask Windows for permission to implement changes on the computer. **Click yes.**

# AP17 Change PIN option

Select the **Change PIN** option located on the right of the screen.



# AP18 Enter PIN information

- In the text field marked **Current PIN** type in your current PIN. If you have not changed it, it is 123456 by default.
- In the text field marked **New PIN** enter a new PIN of your choice. It must be a minimum of 6, and up to 63 characters.
- In the text field marked **Confirm PIN** enter the same PIN you selected.

## AP19 Success!

The display will return to the **Passkeys** menu, and a notification stating "PIN Reset" will briefly appear at the bottom of the screen.