



# STRONGKEY™

## TELLARO SB2

### YUBICO YUBIKEY 5C NFC USER'S GUIDE FOR WINDOWS 11

**NOTE:** This document is for StrongKey customers, employees, suppliers and partners who will interact with the StrongKey Production SB2 cluster ("SB2PROD") for business operations.



## COPYRIGHTS AND NOTICES

Copyright 2001–2026 StrongAuth, Inc. (d/b/a StrongKey), 21060 Homestead Rd Suite 222 Cupertino CA 95014, U.S.A. All rights reserved.

StrongAuth, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more U.S. patents or pending patent applications in the U.S. and in other countries. U.S. Government Rights—Commercial software. Government users are subject to the StrongAuth, Inc. standard license agreement and applicable provisions of the Federal Acquisition Regulations and its supplements. This distribution may include materials developed by third parties. StrongAuth, StrongKey, StrongKey Lite, StrongKey CryptoCabinet, StrongKey CryptoEngine, StrongKey FIDO Server, StrongKey Tellaro, StrongKey Tellaro Small Business Security Bundle (SB2), the StrongAuth logo, the StrongKey logo, the StrongKey Lite logo, the StrongKey CryptoCabinet logo and the StrongKey CryptoEngine logo are trademarks or registered trademarks of StrongAuth, Inc. or its subsidiaries in the U.S. and other countries.

Products covered by and information contained in this publication are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical or biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.



## GETTING STARTED: YUBICO YUBIKEY 5C NFC & SB2PROD PLATFORM

This guide will help you set up your Yubico Yubikey 5C NFC by installing the necessary software and drivers. It also covers how to configure your PC to access the StrongKey Production SB2 cluster ("SB2PROD").

The SB2PROD platform allows you to:

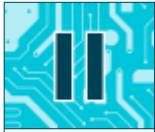
- Securely share information with StrongKey using the SKCC app.
- Download Tellaro software releases via the SKCD app.
- Access new secure services as StrongKey expands its customer support tools.

The StrongKey Support Team



## PREREQUISITES

- Windows 11
- Microsoft (MS) Edge Browser, version 128.0.3351.7
- Yubikey 5C NFC
- Internet connection
- USB-C port or USB-C-to-USB-A adapter



# TABLE OF CONTENTS

A	<a href="#"><u>Installing the Yubico Authenticator Application</u></a>	4
B	<a href="#"><u>Installing the Yubikey Minidriver for Windows 11</u></a>	14
C	<a href="#"><u>Importing SB2 Root CA &amp; SB2 Subordinate CA Certificates into Microsoft Trustore</u></a>	22
D	<a href="#"><u>Accessing an SB2PROD Invitation Link URL</u></a>	53
AP	<a href="#"><u>Appendix: Changing a Yubico Yubikey 5C NFC Personal Identification Number (PIN)</u></a>	71

# SECTION A



STRONGKEY

## A1

## INSTALLING THE YUBICO AUTHENTICATOR APPLICATION

The Yubico Authenticator application is necessary to use the Yubico Yubikey 5C NFC Security Key.

## A2

## DOWNLOAD YUBICO AUTHENTICATOR APPLICATION

Download the Yubico Authenticator for 64-bit systems from <https://www.yubico.com/products/yubico-authenticator/#h-download-yubico-authenticator>. Click Download now.



The screenshot shows the Yubico website's product page for the Yubico Authenticator. The page features a dark blue header with the Yubico logo and navigation links. Below the header, the title 'Yubico Authenticator' is displayed, followed by the tagline 'The safest authenticator app experience across mobile and desktop'. A prominent 'Download now' button is highlighted with a red rectangular box. The background of the page shows a smartphone and a laptop displaying the authenticator application interface.



# WINDOWS YUBICO AUTHENTICATOR APPLICATION

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

The screenshot shows the Yubico website's download page. At the top, there is a navigation bar with the Yubico logo and menu items: Why Yubico, Products, Solutions, Industries, Resources, and Support. On the right side of the navigation bar, there are links for Contact Sales, Resellers, and Support, along with a search icon, a Subscribe button, and a Store button. Below the navigation bar, the page is organized into sections for different operating systems: Linux, Mac, Windows, Android, and iOS. Each section contains a list of download links. The link 'Download for Windows directly here (64-bit)' is highlighted with a red rectangular box.

English  Contact Sales Resellers Support 

**yubico** Why Yubico Products Solutions Industries Resources Support Q [Subscribe](#) [Store](#)

**Linux**

- [Download for Linux directly here](#)

**Mac**

- [Download from macOS AppStore](#)
- [Download for Mac directly here](#)

**Windows**

- [Download from Microsoft app store](#)
- [Download for Windows directly here \(64-bit\)](#)

**Android**

- [Android Download \(on Google Play\)](#)

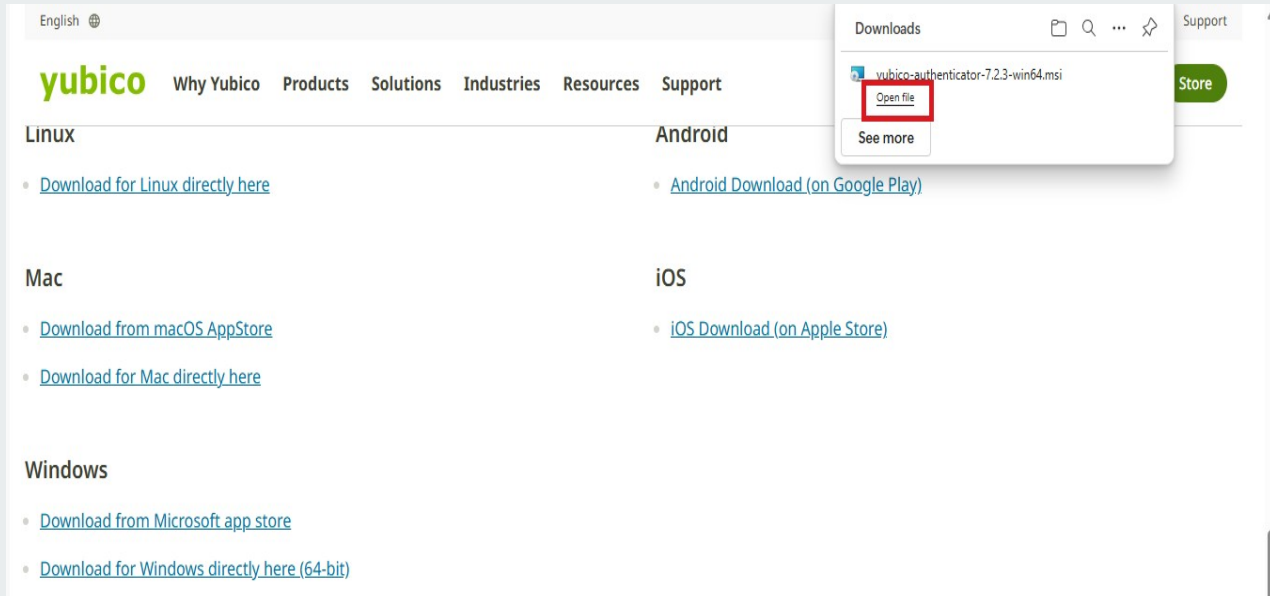
**iOS**

- [iOS Download \(on Apple Store\)](#)



# OPENING THE YUBICO AUTHENTICATOR APPLICATION FILE

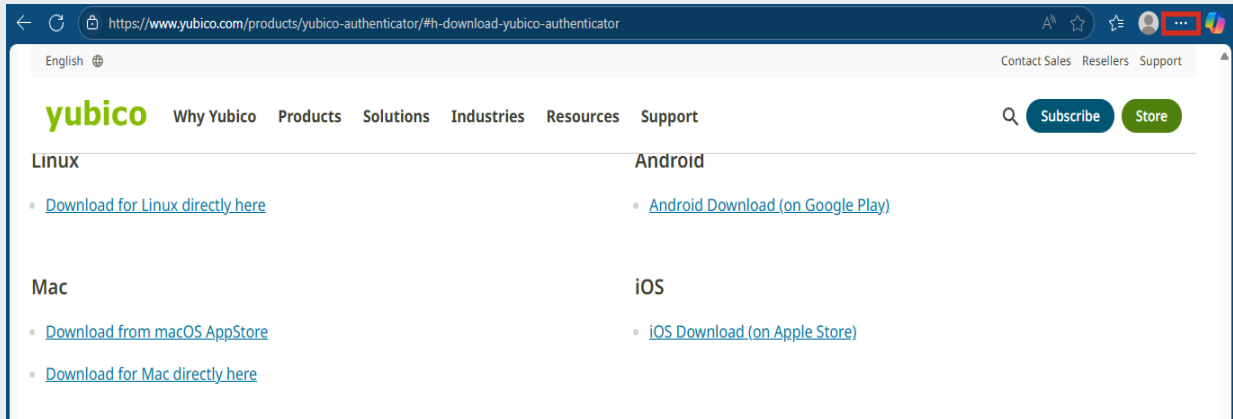
After clicking the download link, MS Edge will display a pop-up confirming the Authenticator application file has been successfully downloaded and ready for installation. Click the open file link.





# NO POP-UP WINDOW? NO PROBLEM

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.





# CLICK DOWNLOADS

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

The screenshot shows a web browser window displaying the Yubico website. The website has a navigation menu with links for 'Why Yubico', 'Products', 'Solutions', 'Industries', 'Resources', and 'Support'. Below the navigation, there are four sections: 'Linux', 'Mac', 'Windows', and 'Android'. Each section contains a list of download links. The 'Downloads' option in the browser's menu is highlighted with a red box.

English

**yubico** Why Yubico Products Solutions Industries Resources Support

**Linux**

- [Download for Linux directly here](#)

**Mac**

- [Download from macOS AppStore](#)
- [Download for Mac directly here](#)

**Windows**

- [Download from Microsoft app store](#)
- [Download for Windows directly here \(64-bit\)](#)

**Android**

- [Android Download \(on Google Play\)](#)

**iOS**

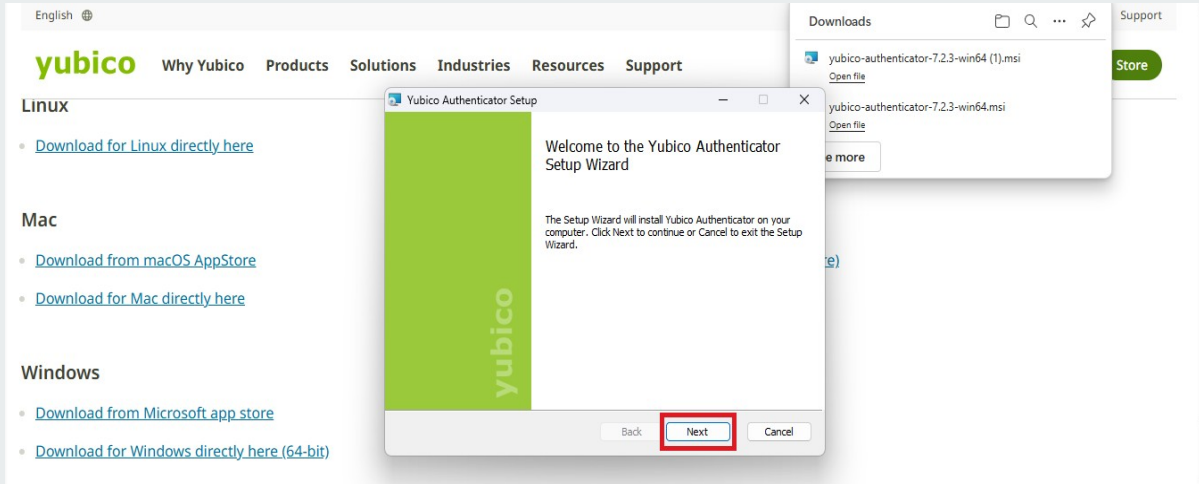
- [iOS Download \(on Apple Store\)](#)

New tab Ctrl+T  
New window Ctrl+N  
New InPrivate window Ctrl+Shift+N  
Zoom - 100% + ↺  
Favorites Ctrl+Shift+O  
Collections Ctrl+Shift+Y  
History Ctrl+H  
Shopping  
**Downloads Ctrl+J**  
Apps  
Extensions  
Performance  
Passwords  
Secure Network  
Delete browsing data Ctrl+Shift+Delete



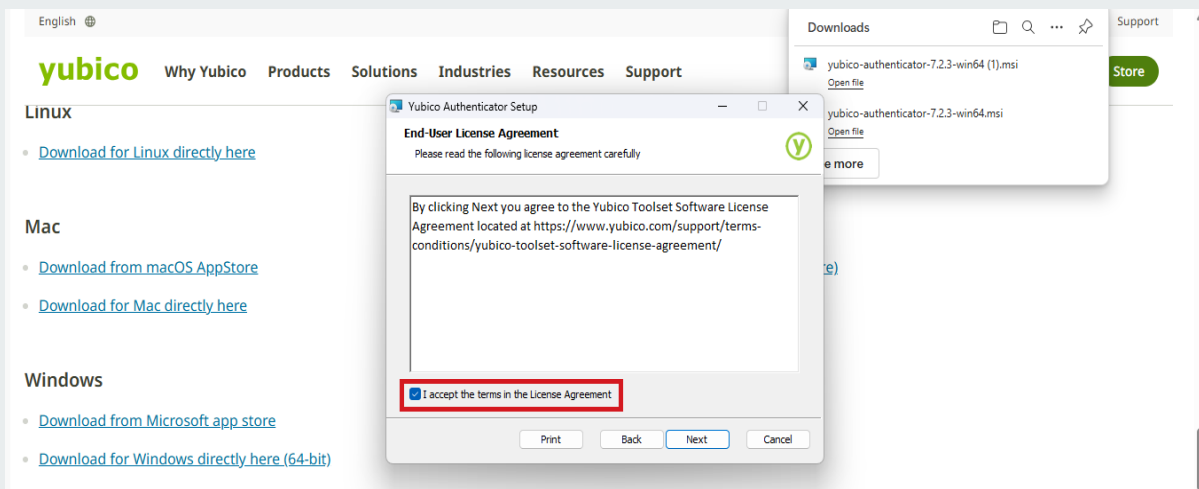
# YUBICO AUTH SETUP WIZARD

A Setup Wizard window will appear, Click Next.



# YUBICO AUTHENTICATOR APPLICATION TERMS & CONDITIONS

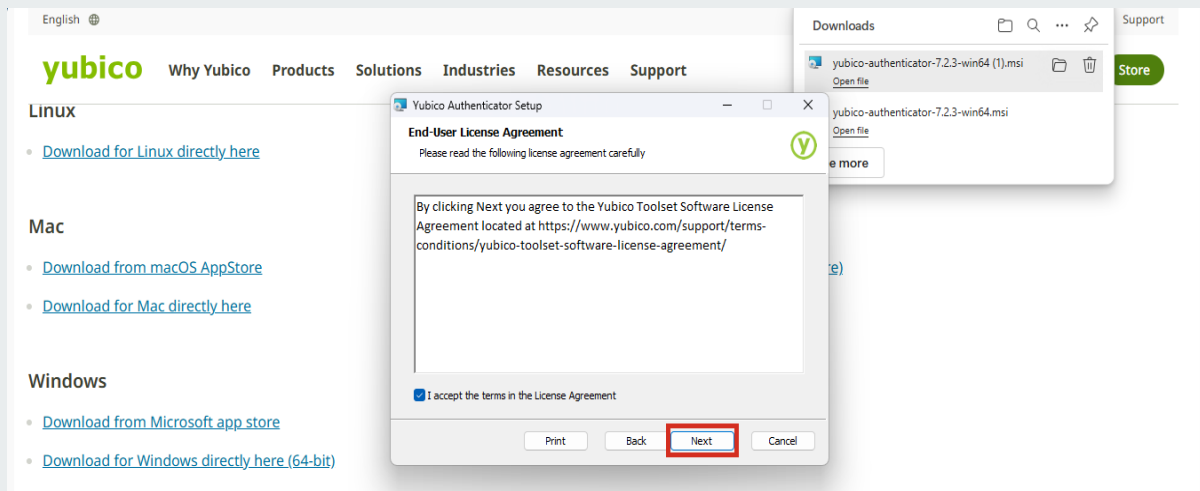
Accept the terms of the end-user license agreement.



A9

# YUBICO AUTHENTICATOR APPLICATION TERMS & CONDITIONS

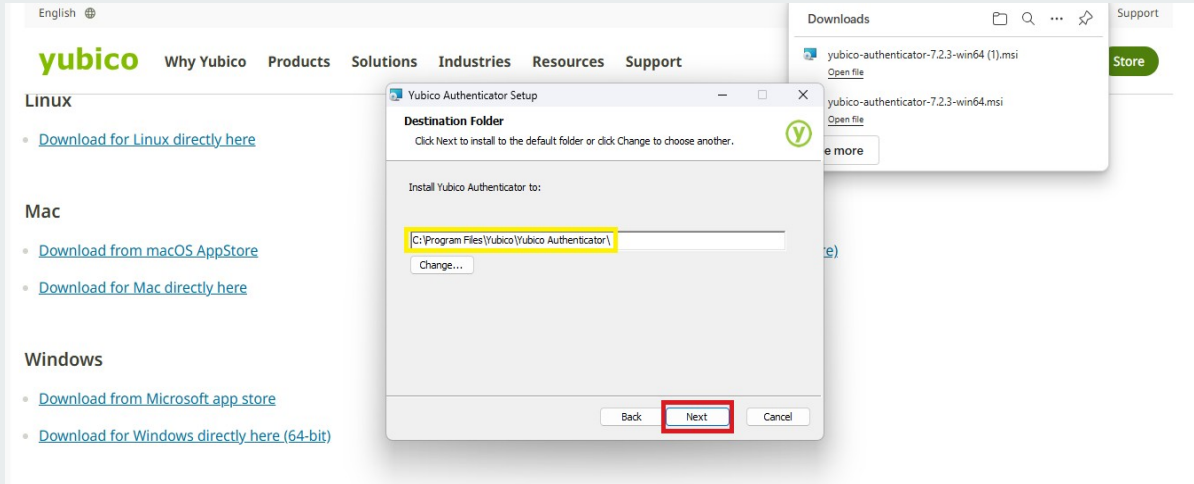
Click Next on the end-user license agreement window.



# A10

## SELECT DESTINATION FOLDER

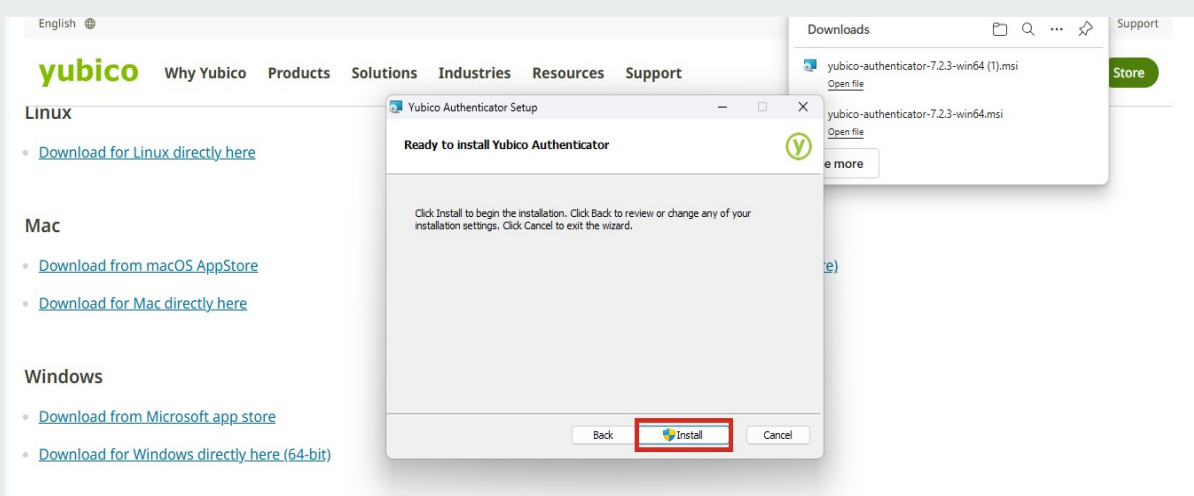
Use the default Destination Folder and Click Next.



# A11

## READY TO INSTALL

Click Install.



## A12

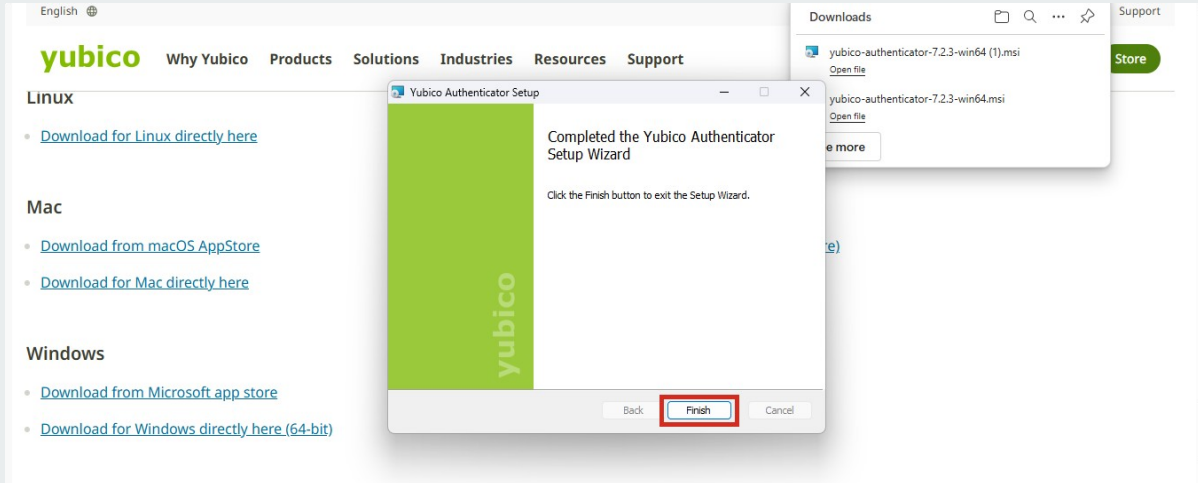
# PERMISSION TO MAKE CHANGES

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

## A13

# FINISH THE INSTALL

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



# SECTION B



**STRONGKEY**

**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.



# DOWNLOAD THE YUBIKEY MINIDRIVER

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

English View site information Contact Sales Resellers Support

**yubico** Why Yubico Products Solutions Industries Resources Support

[Manager CLI \(ykman\) User Manual.](#)

The YubiKey Smart Card Minidriver enables users and administrators to use the native Windows interface for certificate enrollment, managing the YubiKey smart Card PIN, and smart card authentication on Windows.

By downloading, you agree to the [Yubico website terms and conditions of use](#) as well as each download's respective license.

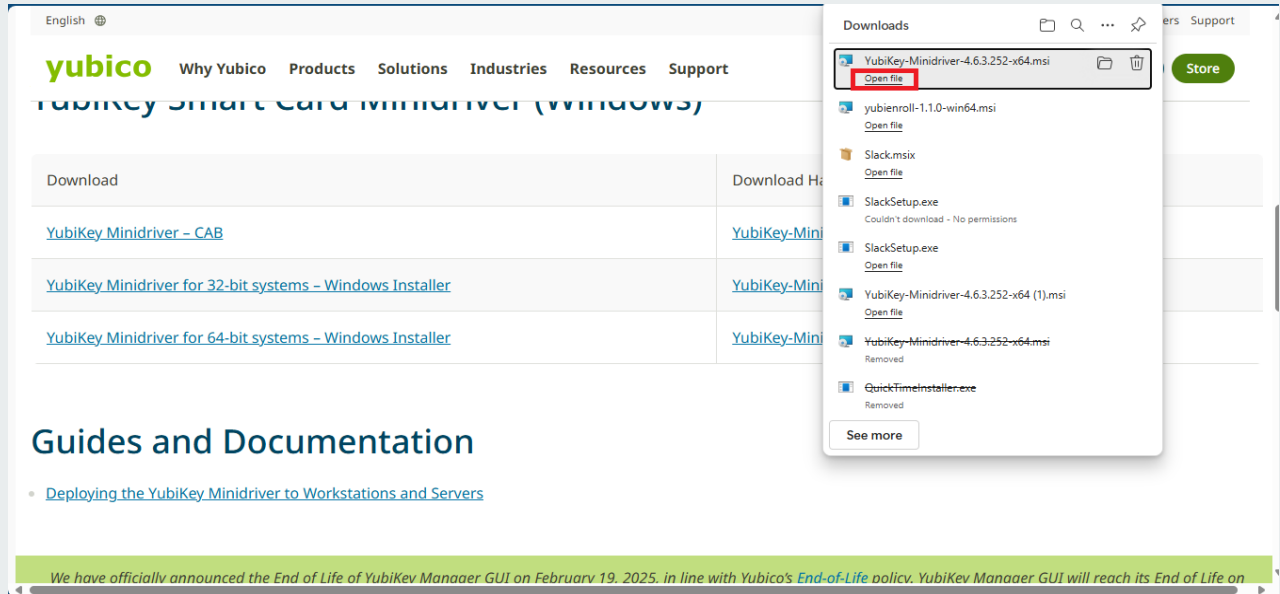
## YubiKey Smart Card Minidriver (Windows)

Download	Download Hash
<a href="#">YubiKey Minidriver - CAB</a>	<a href="#">YubiKey-Minidriver-4.6.3.252.cab.sha256</a>
<a href="#">YubiKey Minidriver for 32-bit systems - Windows Installer</a>	<a href="#">YubiKey-Minidriver-4.6.3.252-x86.msi.sha256</a>
<a href="#">YubiKey Minidriver for 64-bit systems - Windows Installer</a>	<a href="#">YubiKey-Minidriver-4.6.3.252-x64.msi.sha256</a>



# OPENING THE YUBIKEY MINIDRIVER FILE

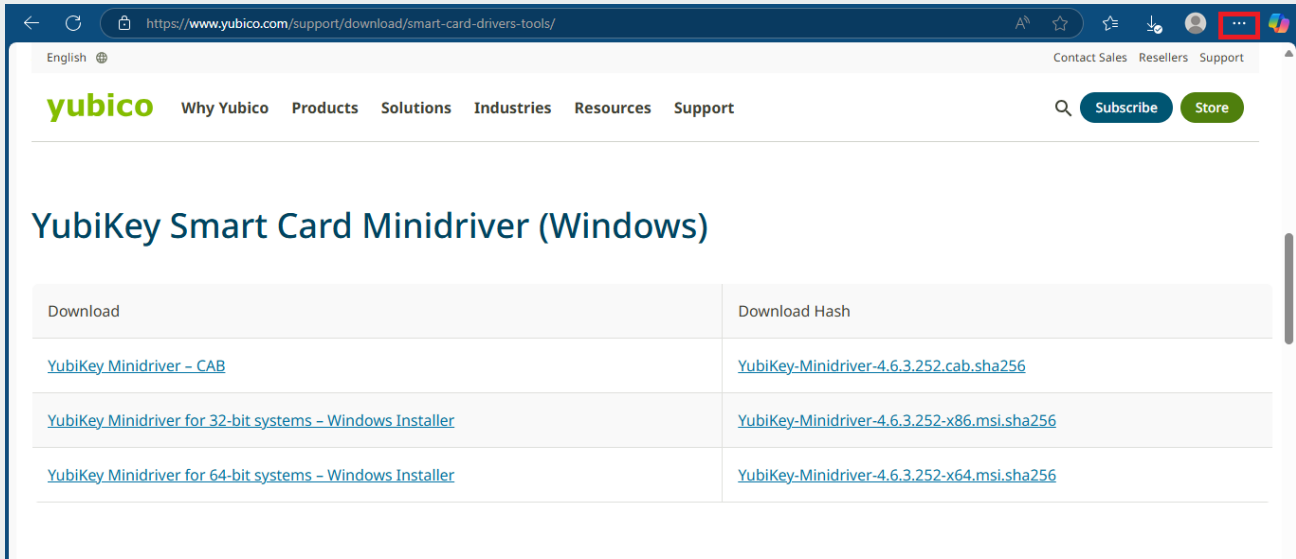
After clicking the download link, Edge browser will display a pop-up confirming the Minidriver file has been successfully downloaded and ready for installation. Click the open file link.





# 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.





# CLICK DOWNLOADS

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

The screenshot shows a web browser window displaying the Yubico website. The page title is "YubiKey Smart Card Minidriver (Windows)". Below the title is a table with two columns: "Download" and "Download Hash". The table contains three rows of download links and their corresponding hashes. A Chrome menu is open on the right side of the browser, and the "Downloads" option is highlighted with a red box. The menu also shows other options like "New tab", "New window", "Zoom", "Favorites", "History", "Shopping", "Apps", "Extensions", "Browser essentials", "Delete browsing data", "Print", "Split screen", "Screenshot", "Find on page", and "More tools".

Download	Download Hash
<a href="#">YubiKey Minidriver - CAB</a>	<a href="#">YubiKey-Minidriver-4.6.3.2</a>
<a href="#">YubiKey Minidriver for 32-bit systems - Windows Installer</a>	<a href="#">YubiKey-Minidriver-4.6.3.2</a>
<a href="#">YubiKey Minidriver for 64-bit systems - Windows Installer</a>	<a href="#">YubiKey-Minidriver-4.6.3.2</a>

Guides and Documentation



# INSTALLING THE YUBIKEY MINIDRIVER

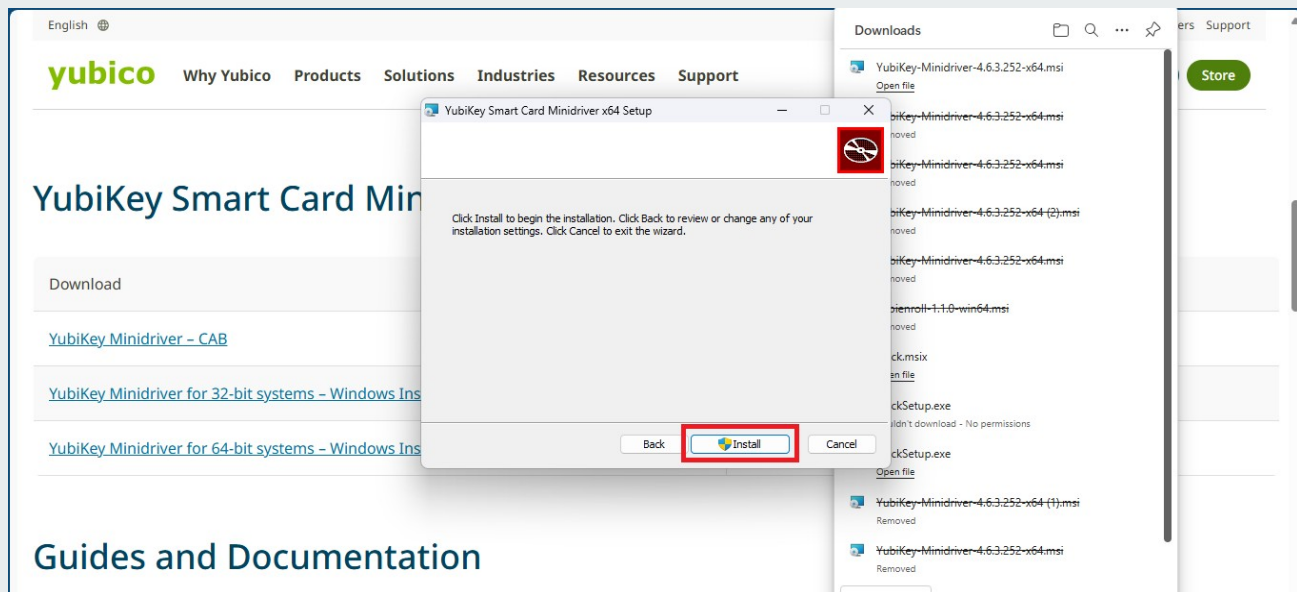
A Setup Wizard pop-up will open – Click **Next**.

The screenshot shows the Yubico website with a 'YubiKey Smart Card Minidriver x64 Setup Wizard' dialog box overlaid. The dialog box has a title bar that reads 'YubiKey Smart Card Minidriver x64 Setup' and a close button. The main content of the dialog box says 'Welcome to the YubiKey Smart Card Minidriver x64 Setup Wizard' and provides instructions: 'The Setup Wizard allows you to change the way YubiKey Smart Card Minidriver x64 features are installed on your computer or to remove it from your computer. Click Next to continue or Cancel to exit the Setup Wizard.' At the bottom of the dialog box, there are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a red rectangular box. In the background, the Yubico website is visible, showing the 'YubiKey Smart Card Minidriver' page with a 'Download' section and a 'Downloads' folder window open in the top right corner.

**B7**

## CONTINUE INSTALLING THE YUBIKEY MINIDRIVER

On the next pop-up window – Click Install.

**B8**

## PERMISSION TO MAKE CHANGES

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



# FINISH THE INSTALL

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

The screenshot shows the Yubico website with a 'YubiKey Smart Card Minidriver x64 Setup Wizard' window overlaid. The wizard window displays the message: 'Completed the YubiKey Smart Card Minidriver x64 Setup Wizard. Click the Finish button to exit the Setup Wizard.' The 'Finish' button is highlighted with a red box. In the background, the website's navigation menu includes 'Why Yubico', 'Products', 'Solutions', 'Industries', 'Resources', and 'Support'. A 'Downloads' window is also visible, showing a list of files including 'YubiKey-Minidriver-4.6.3.252-x64.msi'.



# SECTION C



**STRONGKEY**

## C1

### **IMPORTING SB2 ROOT CA & SB2 SUBORDINATE CA CERTIFICATES INTO TRUSTSTORE**

When using Security Keys with digital certificates for authentication to an SB2 site, the SB2 Root Certificate Authority (CA) certificate of the site is a critical component in establishing trust between your browser and the site. It ensures the digital certificate on your Security Key was issued by that SB2 site and is currently valid.



# ACCESS THE SB2PKI PAGE

All required CA certificates are available for download from the SB2 PKI page at <https://www.strongkey.com/sb2pki>.

<https://www.strongkey.com/sb2pki>

**STRONGKEY**

Welcome to the **StrongKey Tellaro Small Business Security Bundle (SB2)**

This page provides information to help you get started working with SB2  
If you have any questions, please send an e-mail to [getsecure@strongkey.com](mailto:getsecure@strongkey.com)

**SB2 Production CA Certificates**

- Download Root CA
- Download Sub CA 1
- Download Sub CA 2

**How To Configure CA Certificates**

**Swissbit Security Keys**

HTML:	Windows 10	Windows 11	macOS
PDF:	Windows 10	Windows 11	macOS
Video:	Windows 10	Windows 11	macOS

**Yubikey Security Keys**

HTML:	Windows 10	Windows 11	macOS
-------	------------	------------	-------



# SB2 CA CERTIFICATES

On the SB2 PKI page, the following digital certificate files are available – they must be downloaded by clicking their individual **Download** buttons:

- **Download Root CA** (SB2ProdRootCA.crt)
- **Download Sub CA 1** (SB2ProdSubordinateCA1.crt)
- **Download Sub CA 2** (SB2ProdSubordinateCA2.crt)

**STRONGKEY**

Welcome to the **StrongKey Tellaro Small Business Security Bundle (SB2)**

This page provides information to help you get started working with SB2  
If you have any questions, please send an e-mail to [getsecure@strongkey.com](mailto:getsecure@strongkey.com)

**SB2 Production CA Certificates**

- Download Root CA
- Download Sub CA 1
- Download Sub CA 2

**How To Configure CA Certificates**

**Swissbit Security Keys**

HTML:	Windows 10	Windows 11	macOS
PDF:	Windows 10	Windows 11	macOS
Video:	Windows 10	Windows 11	macOS

**Yubikey Security Keys**

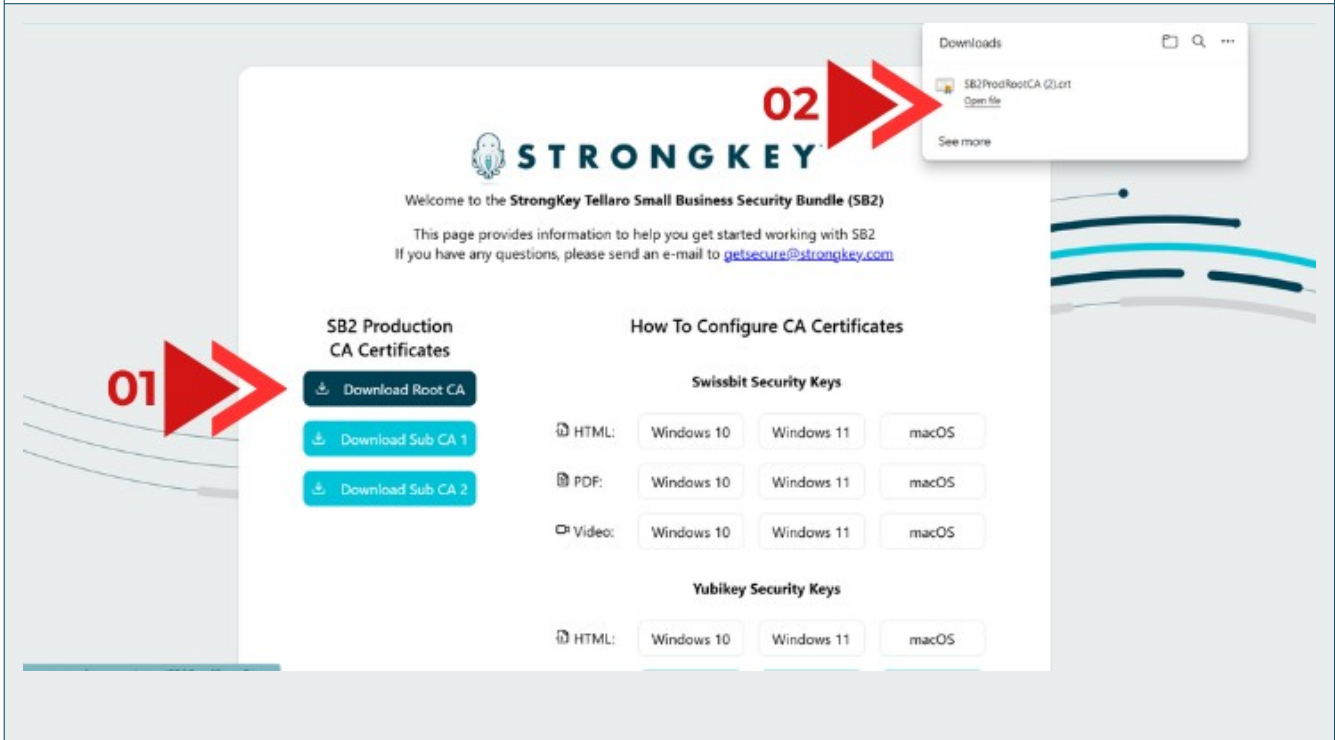
HTML:	Windows 10	Windows 11	macOS
-------	------------	------------	-------

# C4

## DOWNLOADING THE SB2 ROOT CA

First, click the **Download Root CA** button (1). The download will begin automatically, and you'll see a dialog box confirming the file name once the process is complete (2).

**REPEAT** this process for the Sub CA 1 and Sub CA 2 certificates.





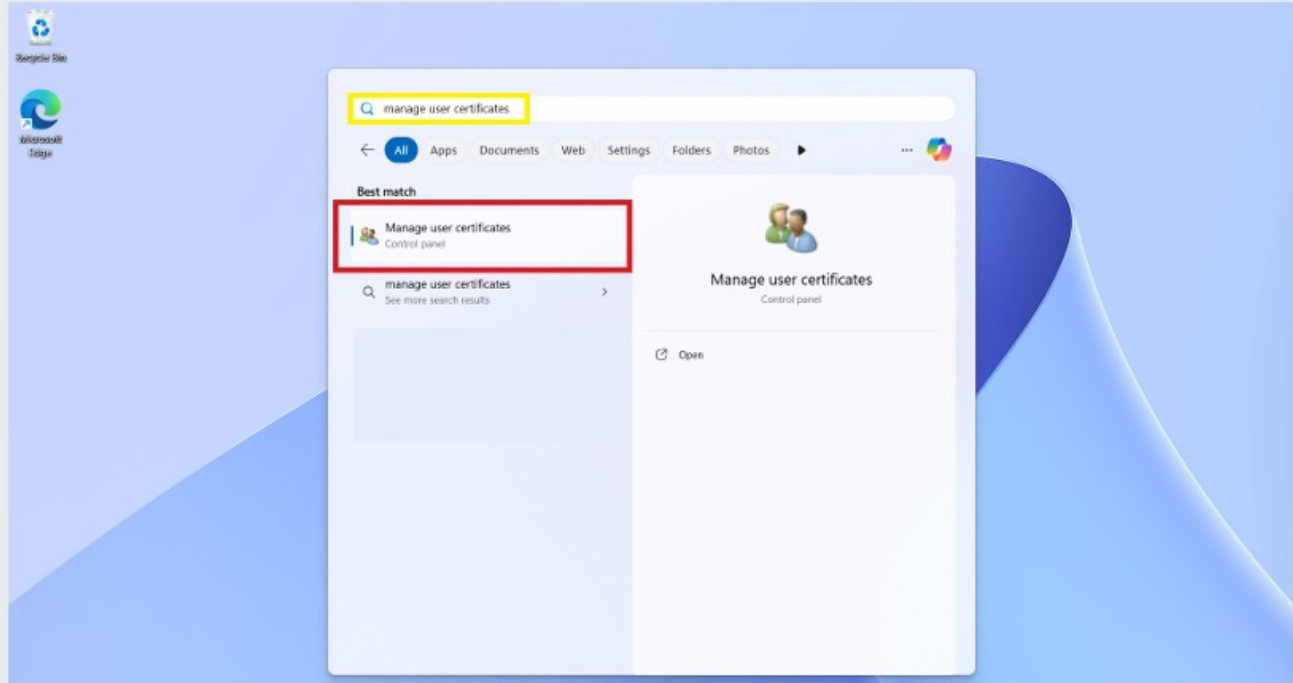
## NAVIGATE TO THE WINDOWS START ICON

After clicking the Windows Start icon, search for **Manage user certificates** to find the settings application for overseeing and configuring security certificates, including importing. Next, select the **Manage user certificates** application.



### NOTE

The **Manage user certificates** application is also known as **certmgr** (short for Certificate Manager). In this document, these terms are used interchangeably.

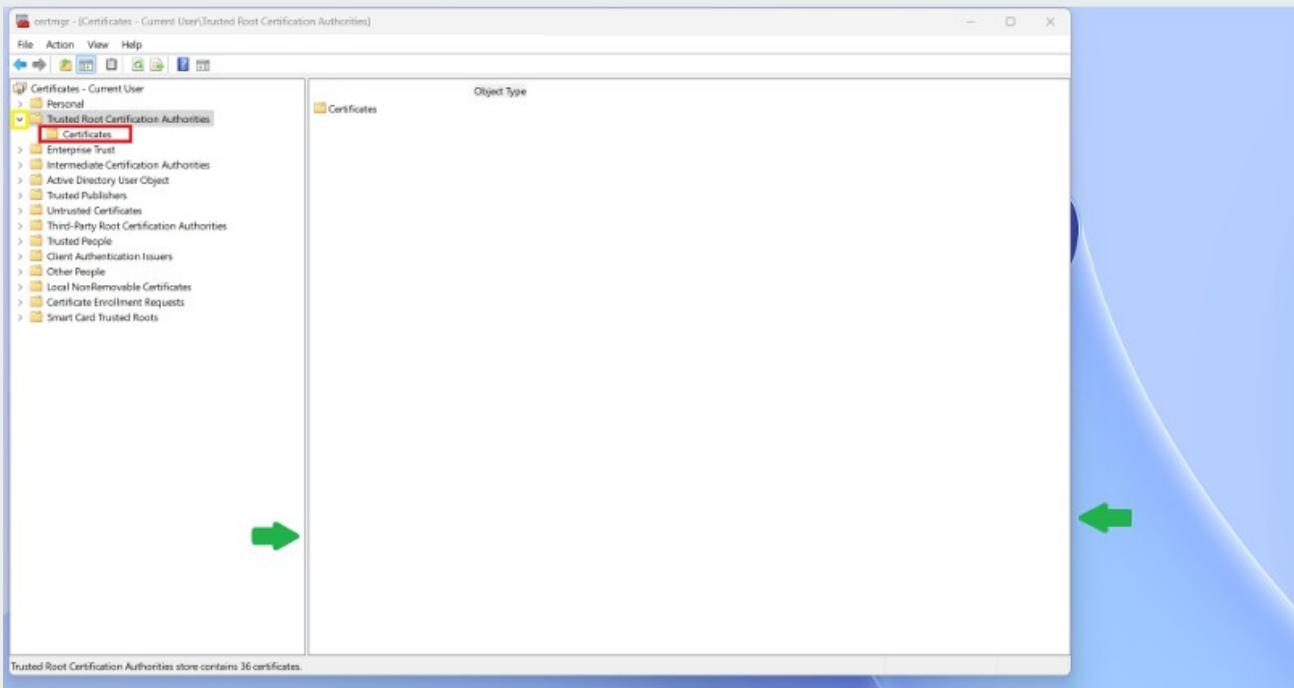




# OPEN TRUSTED ROOT CERTIFICATION AUTHORITIES FOLDER

To begin, expand the **certmgr** 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.

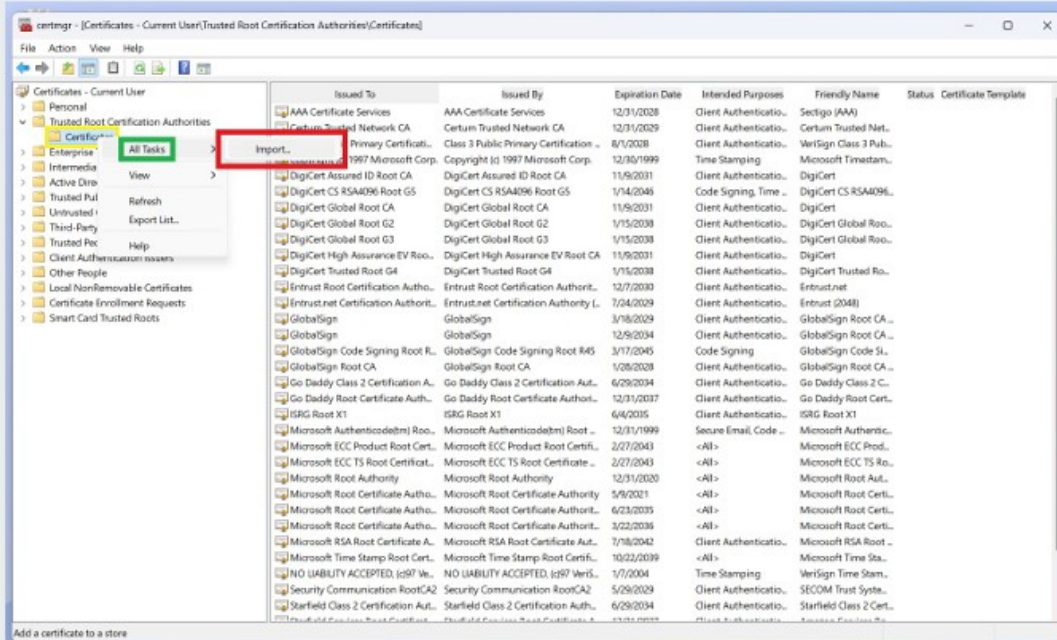




# INITIATE THE SB2 ROOT CERTIFICATE IMPORT

Right-click the **Certificates** folder to open the context menu.

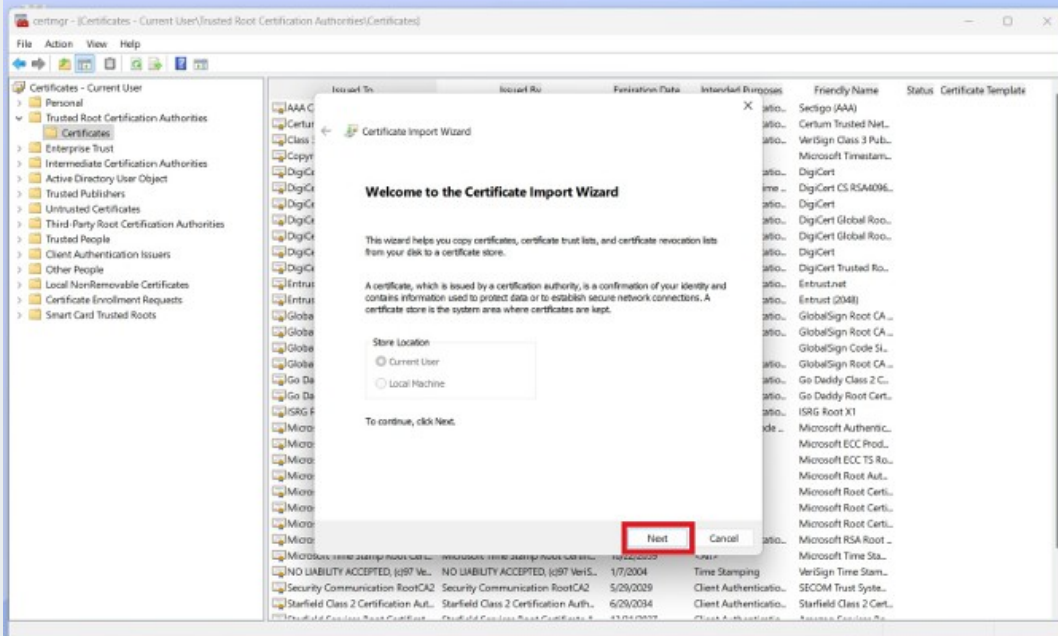
Select **All Tasks**, and click **Import** to start the Certificate Import Wizard.





# CERTIFICATE IMPORT WIZARD

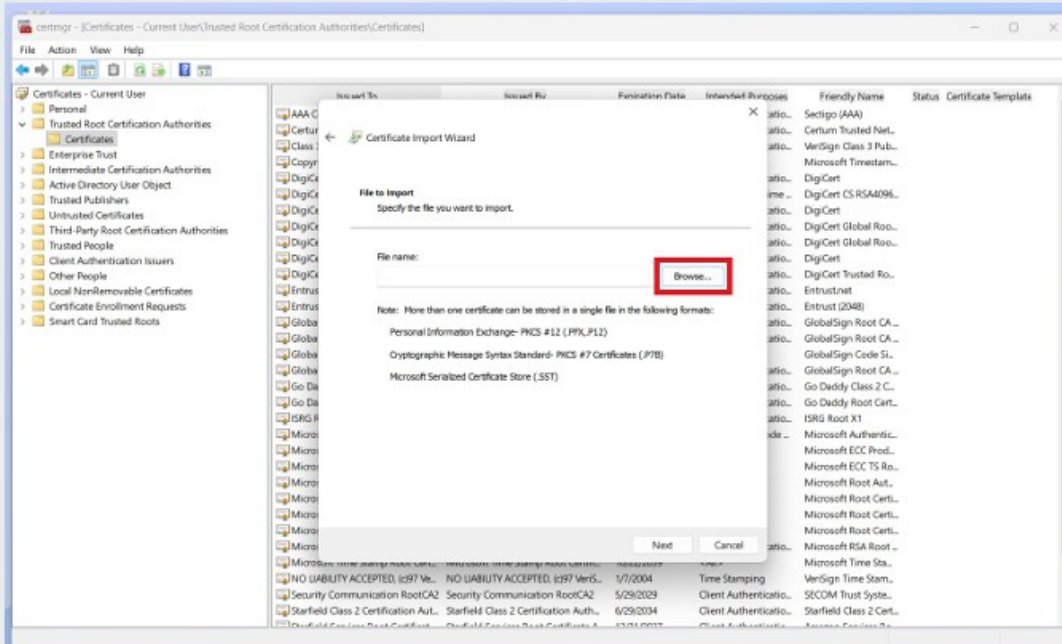
The Certificate Import Wizard will open. Click Next to proceed.





# LOCATE THE SB2 ROOT CA CERTIFICATE

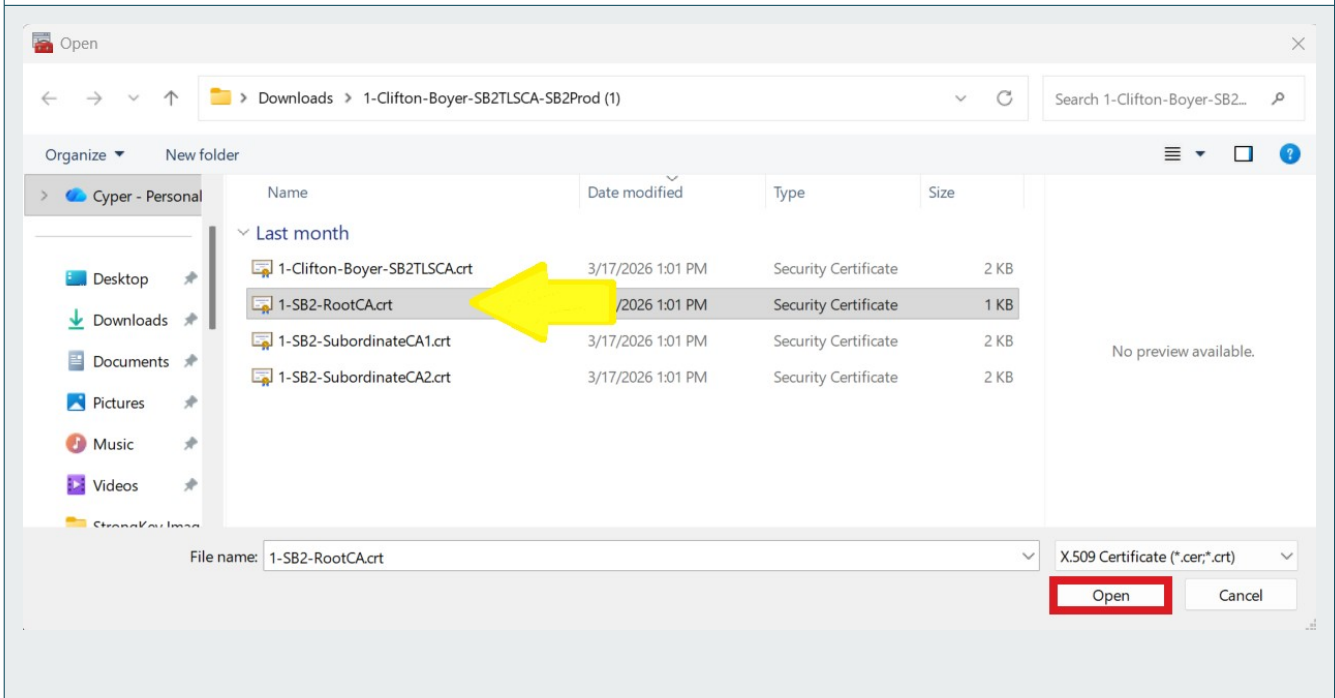
Click the **Browse** button to locate the SB2 Root CA certificate file.





## OPEN THE SB2 ROOT CA CERTIFICATE

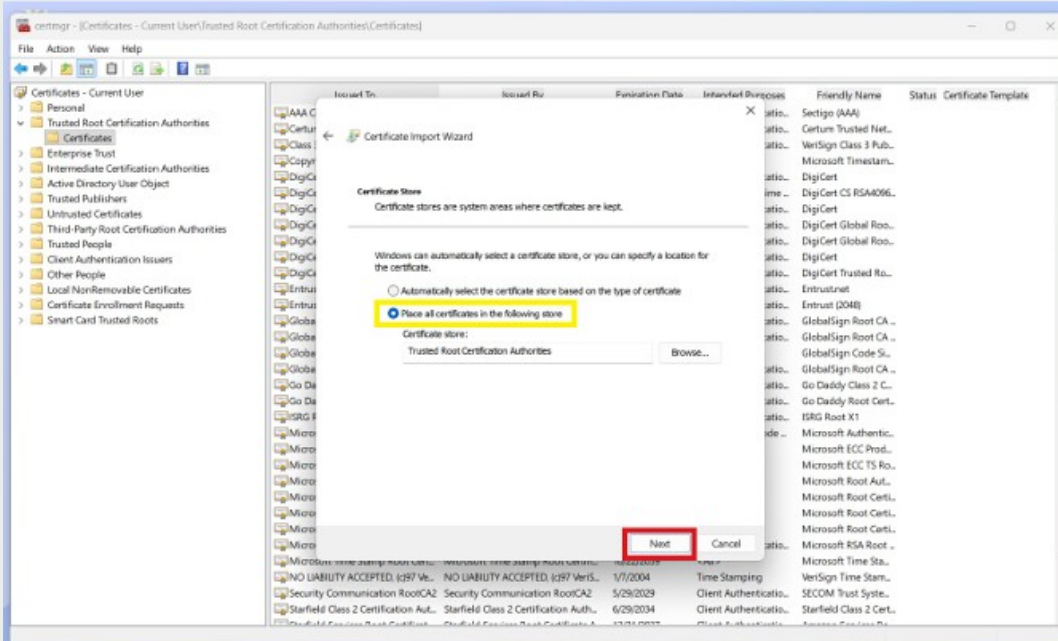
To find the SB2 Root CA Certificate, go to the **SB2ProdRootCA.crt** file's location, which is typically the **Downloads** folder. Once the **SB2ProdRootCA.crt** is located, select it and **click Open**.





# SELECT CERTIFICATE STORE

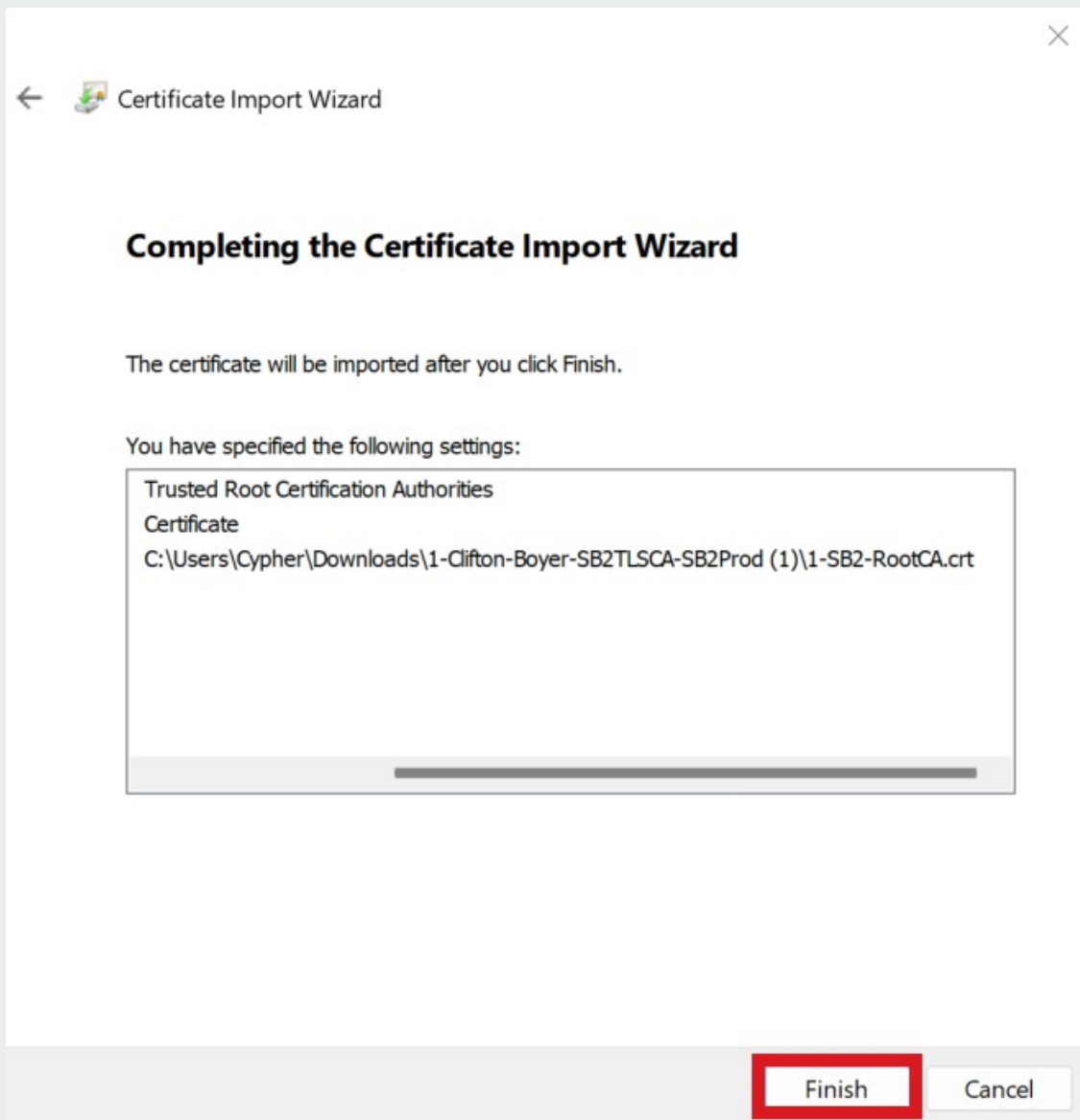
Ensure the *Certificate Store* field indicates the digital certificate will be added to the **Trusted Root Certification Authorities** store before clicking **Next** to continue.





# 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.





# 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**

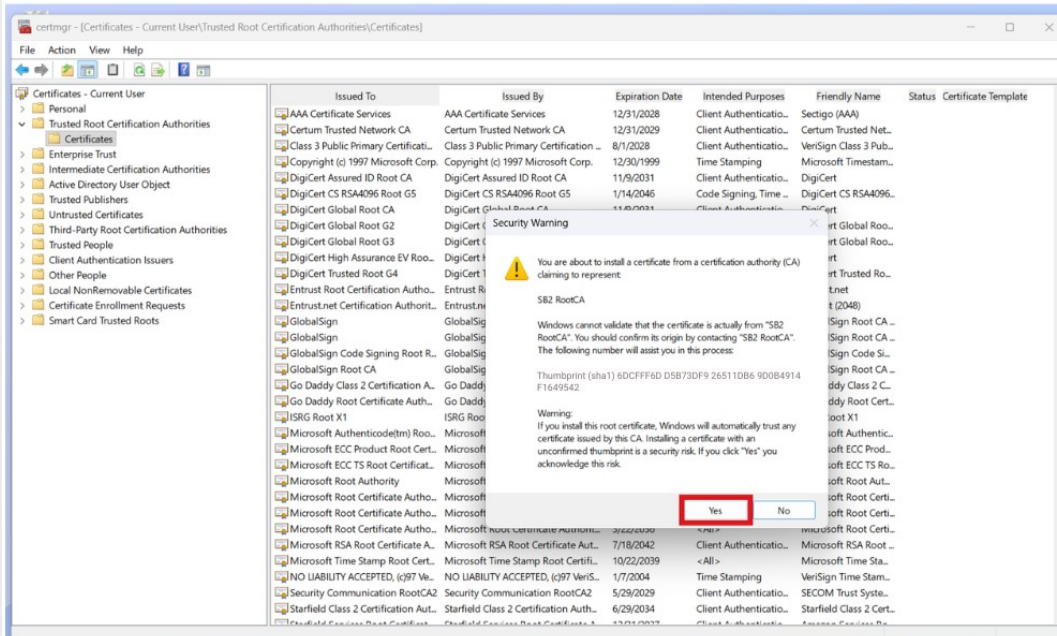
**6DCFFF6D D5B73DF9 26511DB6 9D0B4914 F1649542**

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



**NOTE**

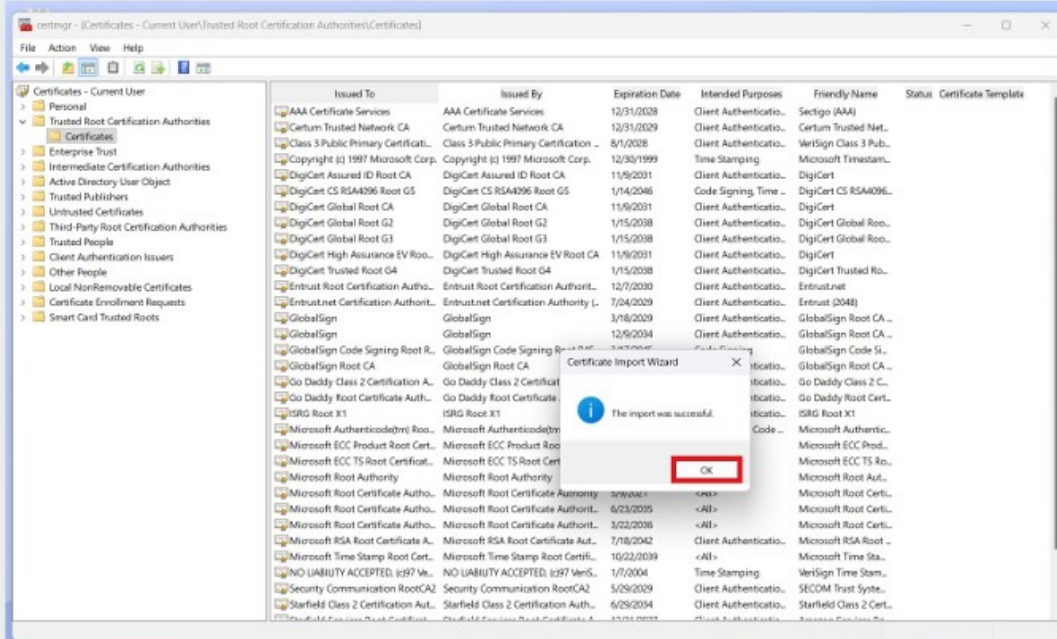
If the Thumbprint of the CA certificate does not match, contact the Administrator of the SB2 site. This step represents the most important step in establishing trust in the SB2 platform.





# A SUCCESSFUL IMPORT

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



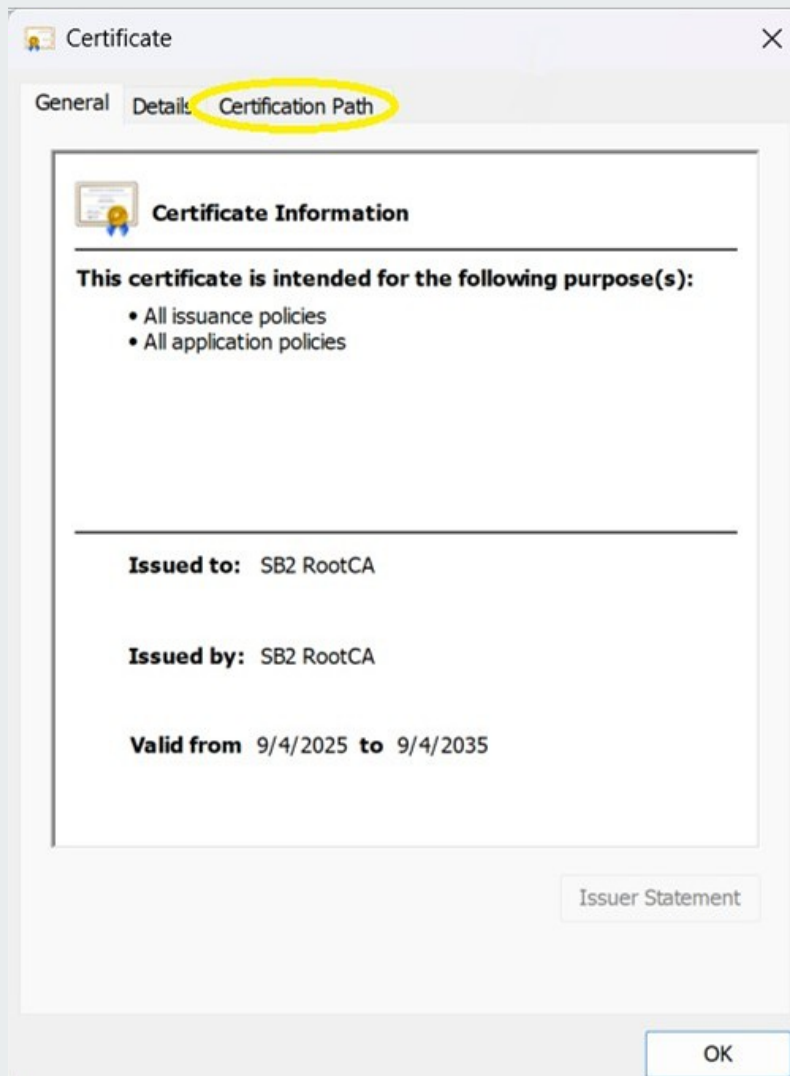


# VERIFY SB2 ROOT CA IN CERTIFICATES LIST

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

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem.
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authentication...	DigiCert		
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authentication...	DigiCert Global Roo...		
DigiCert Global Root G3	DigiCert Global Root G3	1/15/2038	Client Authentication...	DigiCert Global Roo...		
DigiCert High Assurance EV Root...	DigiCert High Assurance EV Root CA	11/9/2031	Client Authentication...	DigiCert		
DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authentication...	DigiCert Trusted Ro...		
Entrust Root Certification Autho...	Entrust Root Certification Authorit...	12/7/2030	Client Authentication...	Entrust.net		
Entrust.net Certification Autho...	Entrust.net Certification Authority (...	7/24/2029	Client Authentication...	Entrust (2048)		
GlobalSign	GlobalSign	3/18/2029	Client Authentication...	GlobalSign Root CA ...		
GlobalSign	GlobalSign	12/9/2034	Client Authentication...	GlobalSign Root CA ...		
GlobalSign Code Signing Root R...	GlobalSign Code Signing Root R45	3/17/2045	Code Signing	GlobalSign Code S...		
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Client Authentication...	GlobalSign Root CA ...		
Go Daddy Class 2 Certification A...	Go Daddy Class 2 Certification Aut...	6/29/2034	Client Authentication...	Go Daddy Class 2 C...		
Go Daddy Root Certificate Auth...	Go Daddy Root Certificate Authorit...	12/31/2037	Client Authentication...	Go Daddy Root Cert...		
ISRG Root X1	ISRG Root X1	6/4/2035	Client Authentication...	ISRG Root X1		
Microsoft Authenticode(m) Roo...	Microsoft Authenticode(m) Root ...	12/31/1999	Secure Email, Code ...	Microsoft Authentic...		
Microsoft ECC Product Root Cert...	Microsoft ECC Product Root Certifi...	2/27/2043	<All>	Microsoft ECC Prod...		
Microsoft ECC TS Root Certificat...	Microsoft ECC TS Root Certificate ...	2/27/2043	<All>	Microsoft ECC TS Ro...		
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...		
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authority	5/8/2021	<All>	Microsoft Root Certi...		
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authorit...	6/23/2035	<All>	Microsoft Root Certi...		
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authorit...	3/22/2036	<All>	Microsoft Root Certi...		
Microsoft RSA Root Certificate A...	Microsoft RSA Root Certificate Aut...	7/18/2042	Client Authentication...	Microsoft RSA Root ...		
Microsoft Time Stamp Root Cert...	Microsoft Time Stamp Root Certifi...	10/22/2039	<All>	Microsoft Time Sta...		
NÖ LIABILITY ACCEPTED, (c97) Ve...	NÖ LIABILITY ACCEPTED, (c97) Veri...	1/7/2004	Time Stamping	VeriSign Time Stam...		
SB2 RootCA	SB2 RootCA	9/4/2035	<All>	<None>		
Secigo Public Server Authentica...	Secigo Public Server Authentication...	3/21/2046	Client Authentication...	Secigo Public Serve...		
Security Communication RootCA2	Security Communication RootCA2	5/29/2029	Client Authentication...	SECOM Trust Syste...		
SSL.com EV Root Certification Au...	SSL.com EV Root Certification Auth...	5/30/2042	Client Authentication...	SSL.com EV Root Cer...		
SSL.com Root Certification Auth...	SSL.com Root Certification Authorit...	2/12/2041	Client Authentication...	SSL.com Root Certifi...		
Starfield Class 2 Certification Aut...	Starfield Class 2 Certification Auth...	6/29/2034	Client Authentication...	Starfield Class 2 Cert...		
Starfield Services Root Certificat...	Starfield Services Root Certificate A...	12/31/2037	Client Authentication...	Amazon Services Ro...		
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root F...	3/14/2032	Code Signing	<None>		
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Thawte Timestampi...		
USERTrust RSA Certification Auth...	USERTrust RSA Certification Author...	1/18/2038	Client Authentication...	Setigo		

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:



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

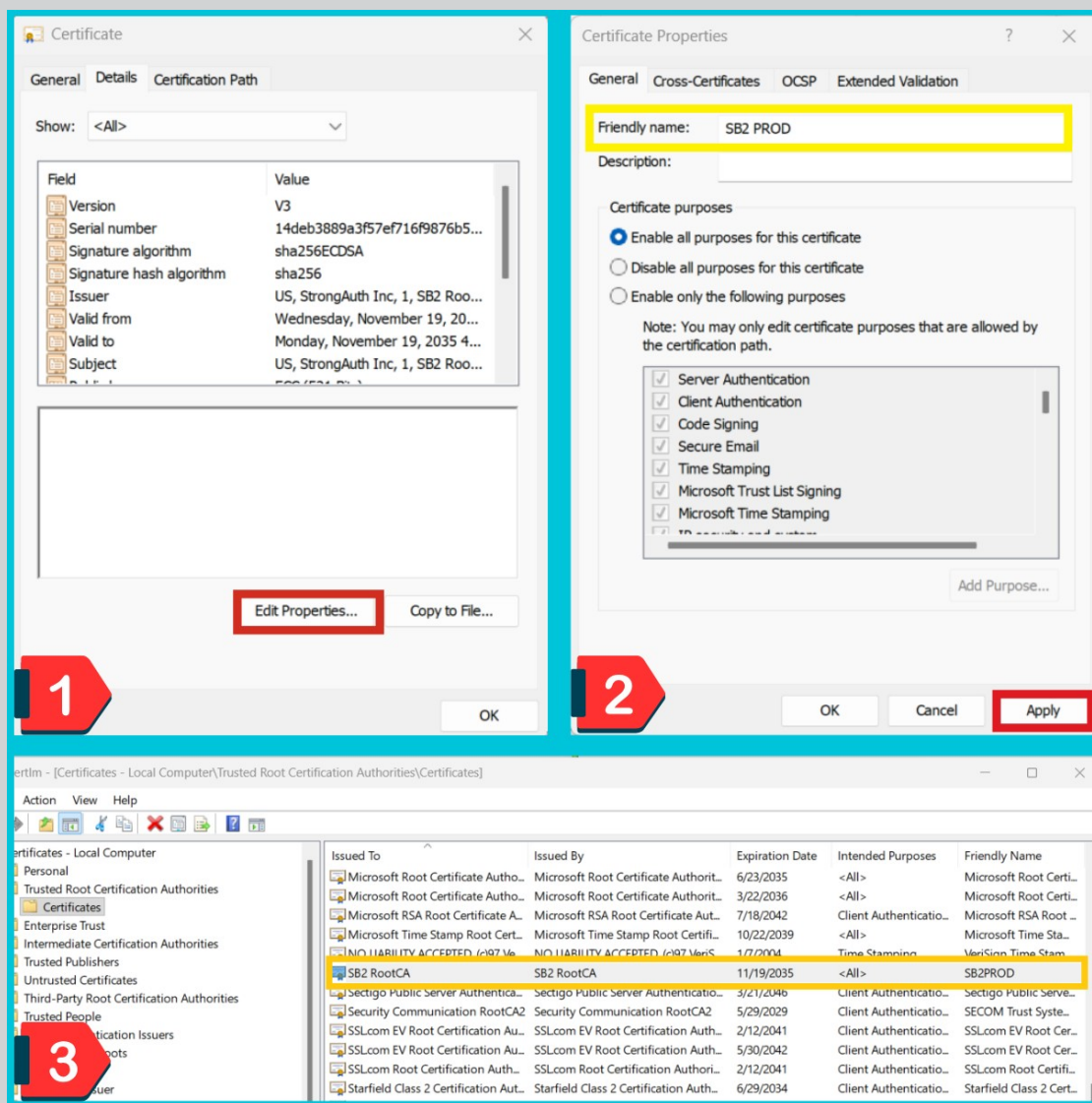
- That the certificate symbol in the **Certification Path** sub-panel at the top does not have any yellow warning symbol associated with it, and
- The **Certificate status** sub-panel at the bottom should state that “This certificate is OK.”



Follow these steps to create a *Friendly name* for the SB2 Root CA:

1. Choose the Details tab.
2. Click Edit Properties (image 1).
3. Add name in Friendly name field (image 2).
4. Click Apply then Click OK to finish.

Friendly names make identifying RootCAs easier in the certificates list (image 3).

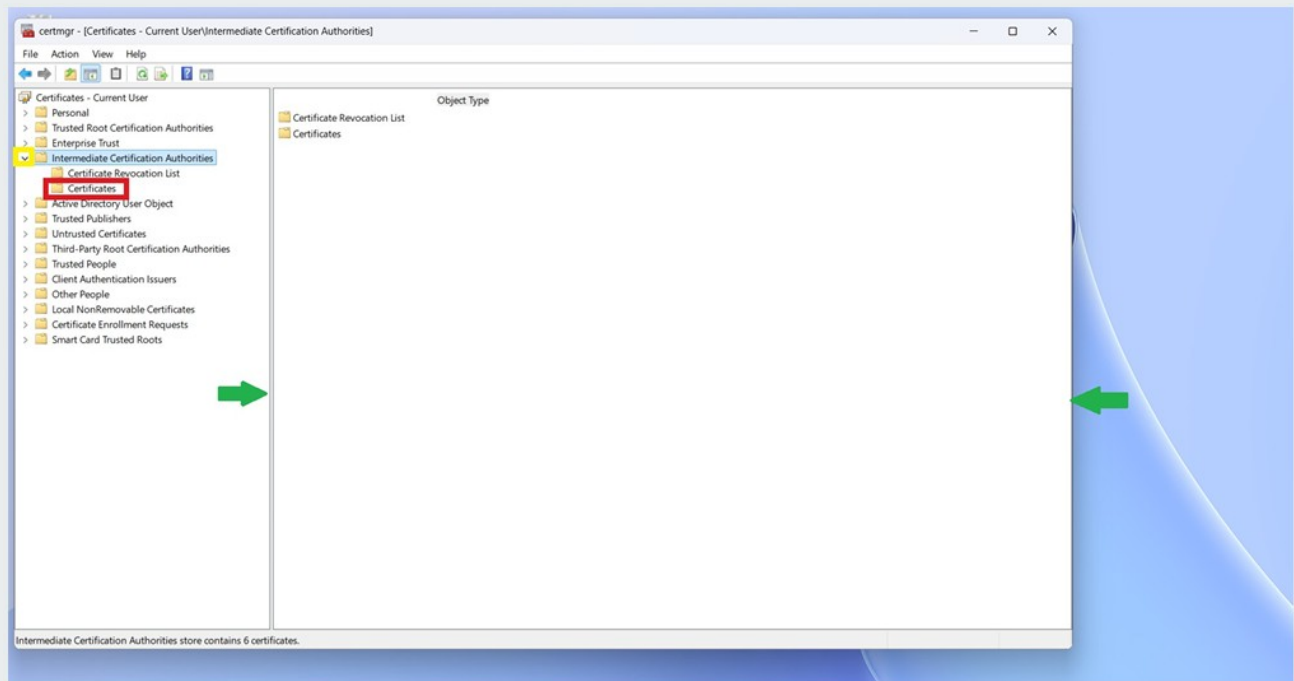




## INTERMEDIATE CERTIFICATION AUTHORITIES FOLDER

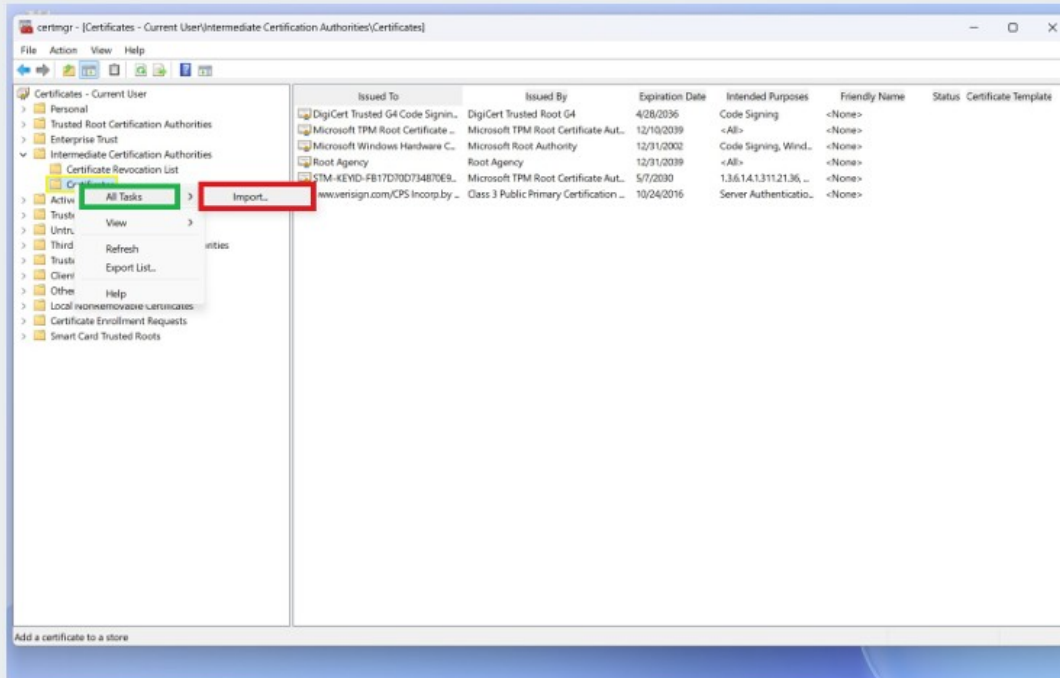
Just as you imported the SB2PROD Root CA certificate, you will now import the two SB2PROD Subordinate CA (aka SubCA) certificates. The SubCA certificates play a vital role in establishing the “certificate chain of trust” between the digital certificate on your Security Key and the SB2 site.

Return to the **certmgr** application. Next, click the **arrow** (yellow box) next to the **Intermediate Certification Authorities** folder to expand it, revealing the **Certificates** (red box) folder.



# INITIATING THE SB2 SUBORDINATE CA CERTIFICATE IMPORT

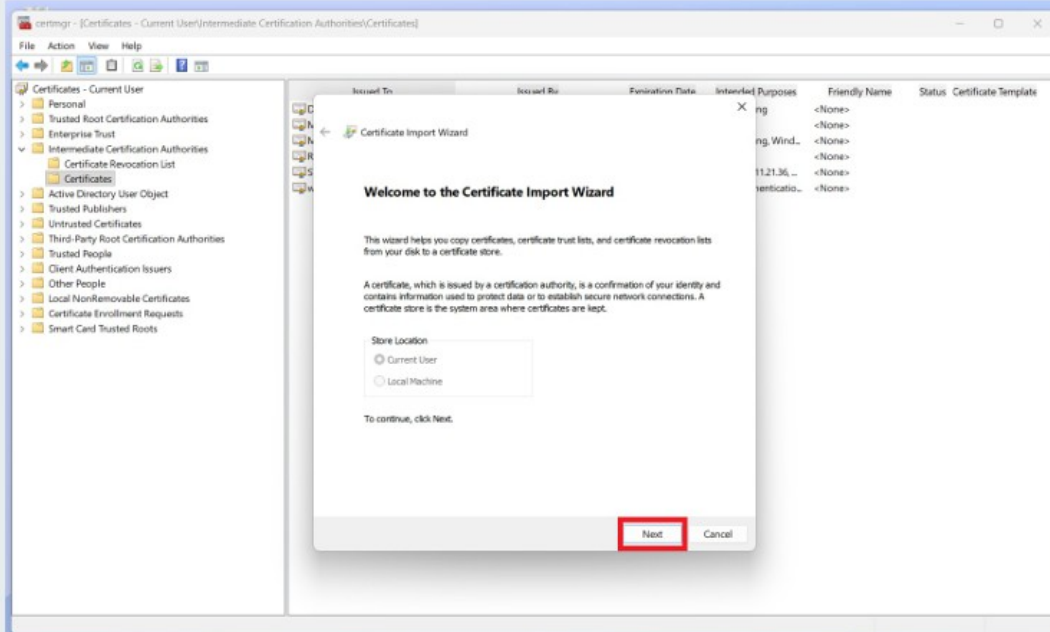
To begin, right-click the **Certificates** folder to open the context menu. From there, select **All Tasks**, and then click **Import** to start the **Certificate Import Wizard**.





# CERTIFICATE IMPORT WIZARD

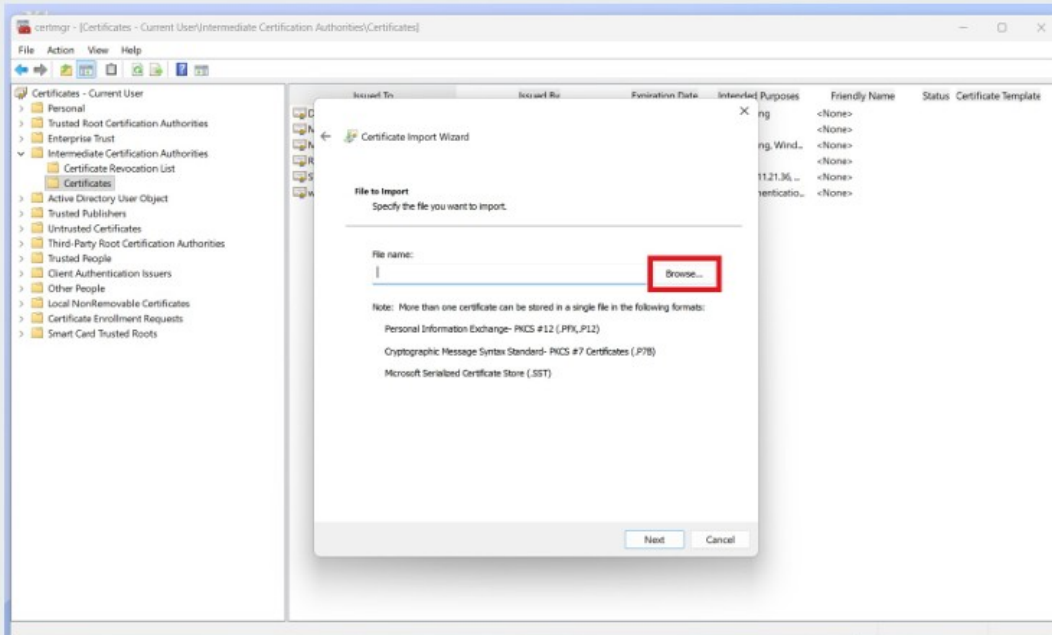
The Certificate Import Wizard will open. Click **Next** to proceed.





# LOCATE SUBORDINATE SB2 CA 1 CERTIFICATE FOR IMPORTING

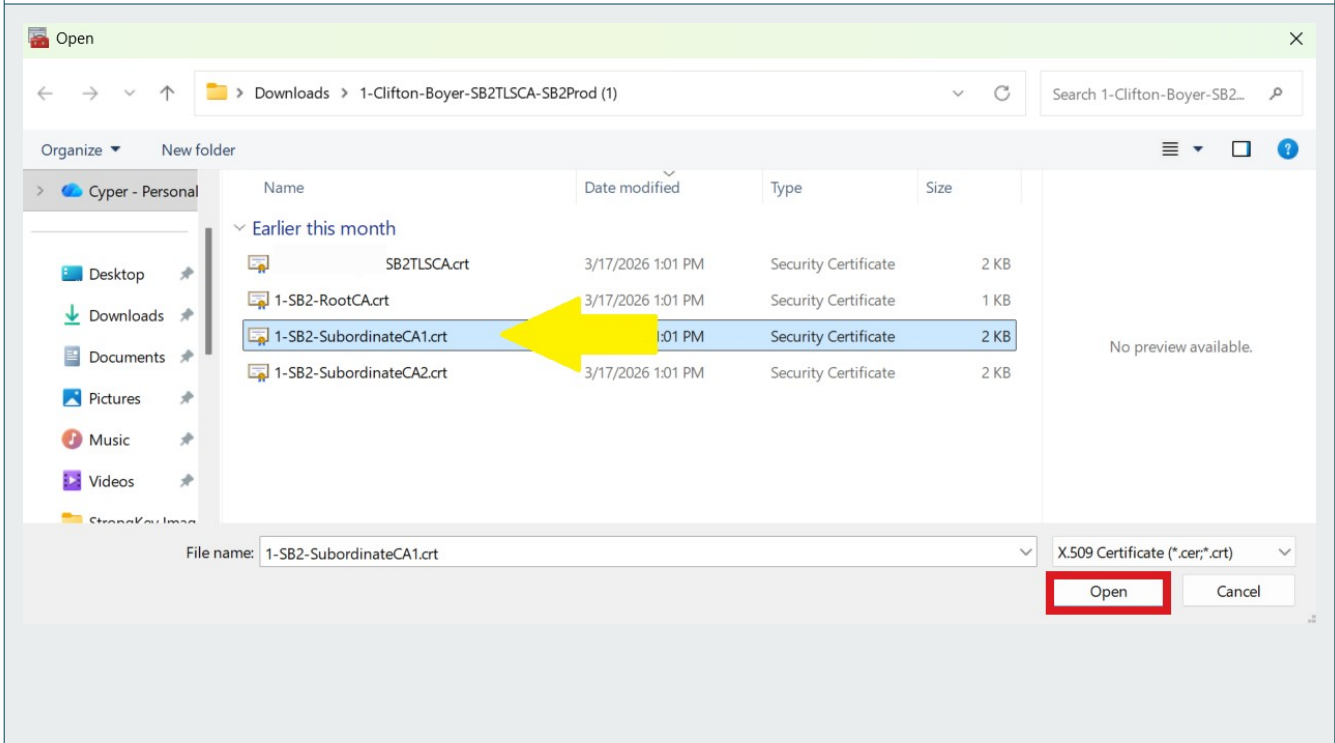
Click the **"Browse"** button to navigate to and select the Subordinate CA certificate file.





# OPEN THE SUBORDINATE SB2PROD CA 1 CERTIFICATE

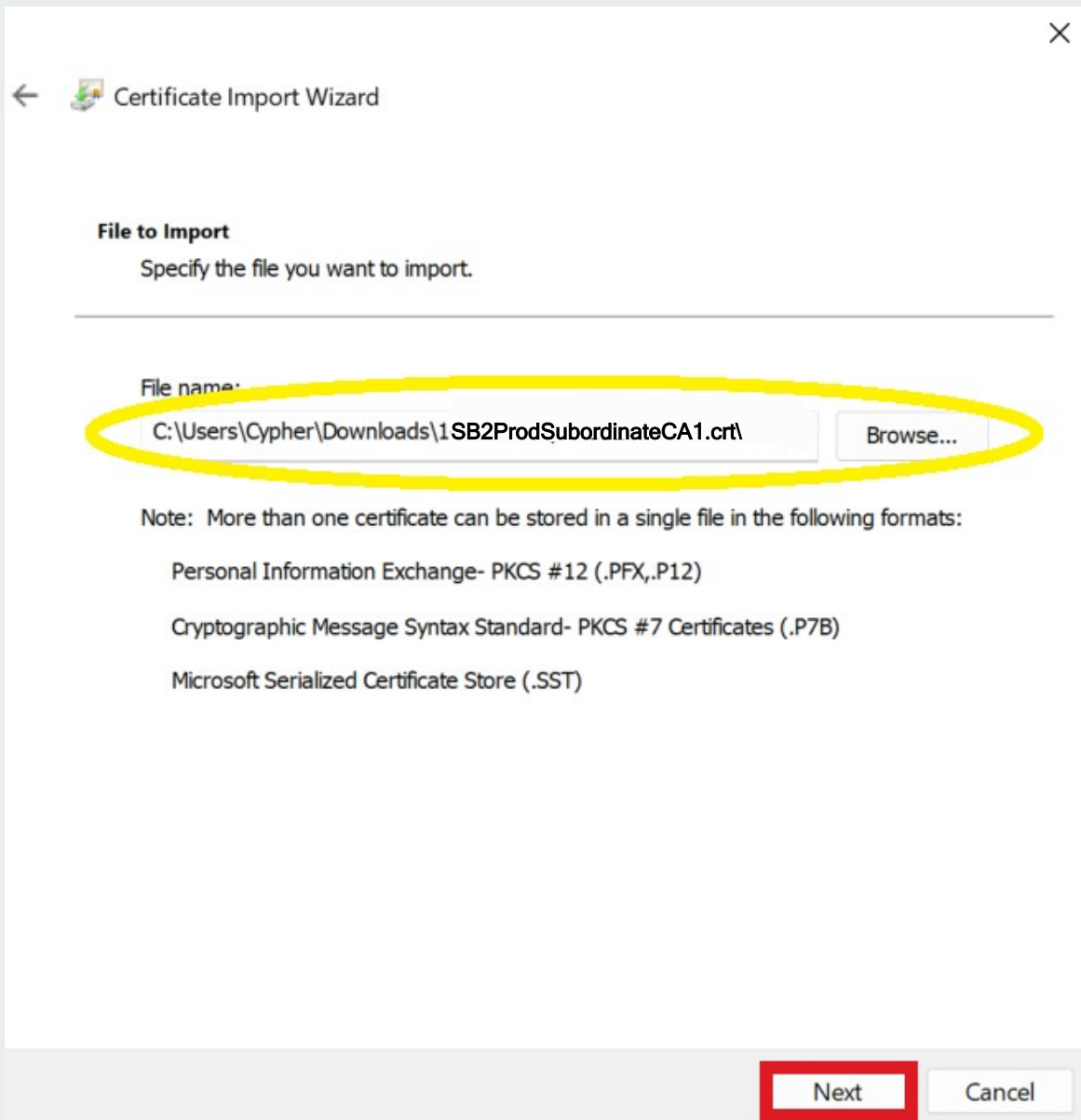
To find the SB2ProdSubordinateCA1.crt certificate file, go to the file's location, which is typically the Downloads folder. Once the SB2ProdSubordinateCA1.crt file (yellow arrow) is located, select it and click Open.





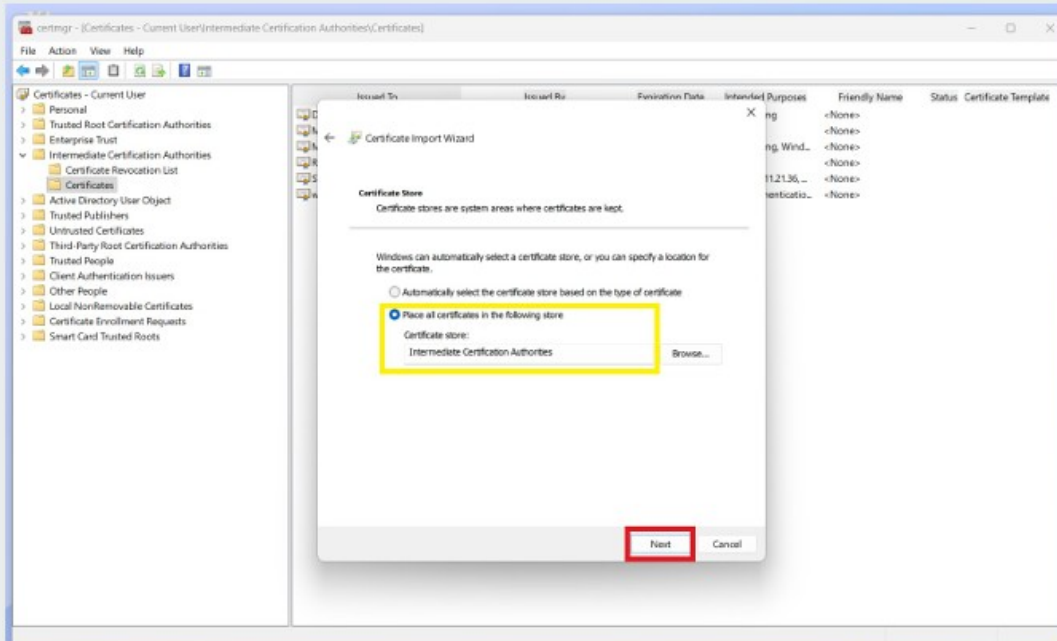
## SB2PROD SUBORDINATE CA 1 CERTIFICATE FILE SELECTED

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.



The image shows a screenshot of the 'Certificate Import Wizard' dialog box. The title bar reads 'Certificate Import Wizard' with a back arrow and a close button. The main content area is titled 'File to Import' and contains the instruction 'Specify the file you want to import.' Below this is a 'File name:' label followed by a text input field containing the path 'C:\Users\Cypher\Downloads\1SB2ProdSubordinateCA1.crl'. To the right of the input field is a 'Browse...' button. A yellow oval highlights the input field and the 'Browse...' button. Below the input field, there is a 'Note' section with the text: 'Note: More than one certificate can be stored in a single file in the following formats:'. This is followed by three bullet points: 'Personal Information Exchange- PKCS #12 (.PFX,.P12)', 'Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)', and 'Microsoft Serialized Certificate Store (.SST)'. At the bottom right of the dialog, there are two buttons: 'Next' (highlighted with a red rectangle) and 'Cancel'.

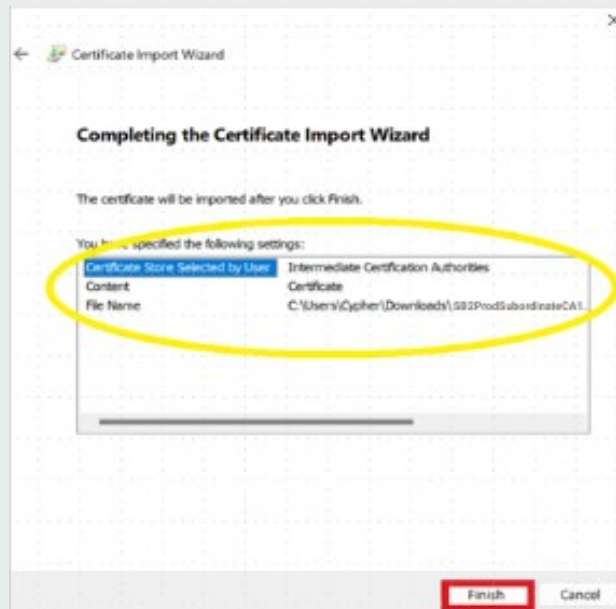
Choose “Place all certificates in the following store” and ensure the certificate is added to the **Intermediate Certification Authorities** certificate store. Click **Next** to continue.





## FINISH IMPORTING THE SB2 SUBORDINATE CA 1 CERTIFICATE

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





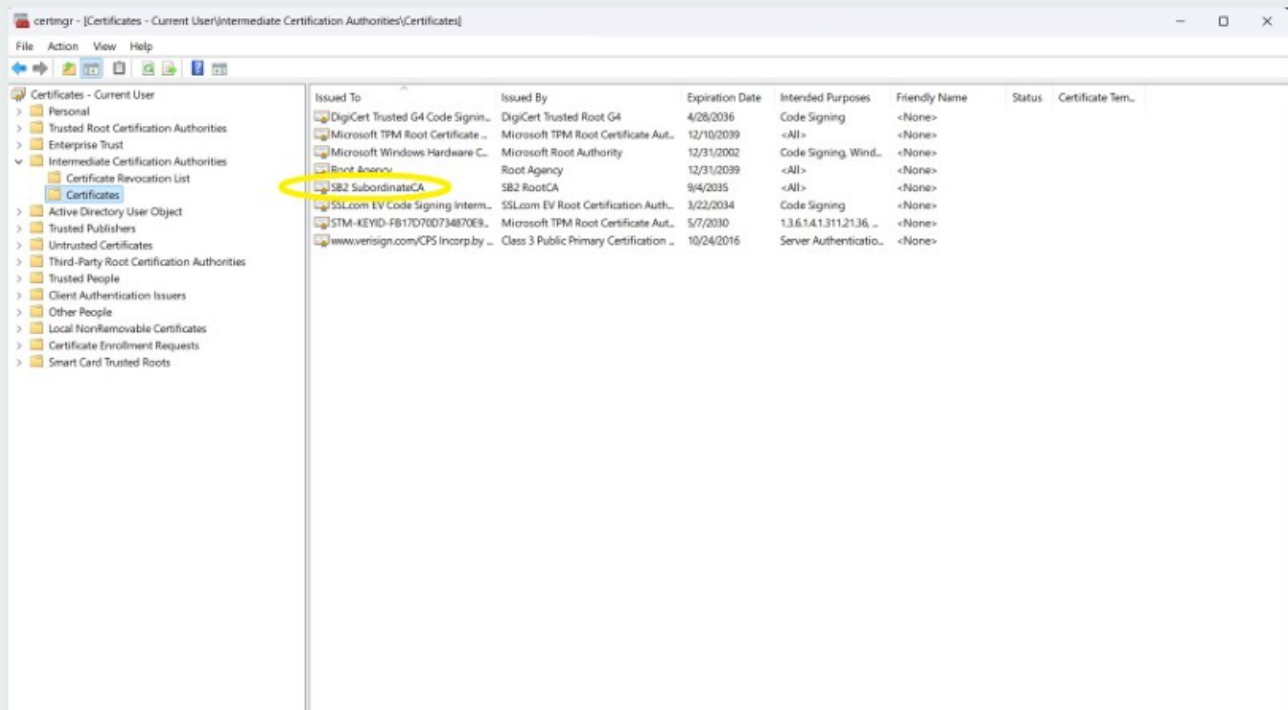
## A SUCCESSFUL IMPORT

Once the SB2 Subordinate CA 1 certificate is imported successfully, a confirmation message will appear. Click OK to continue.



## VERIFY SB2 SUBORDINATE CA 1 IN CERTIFICATES LISTS

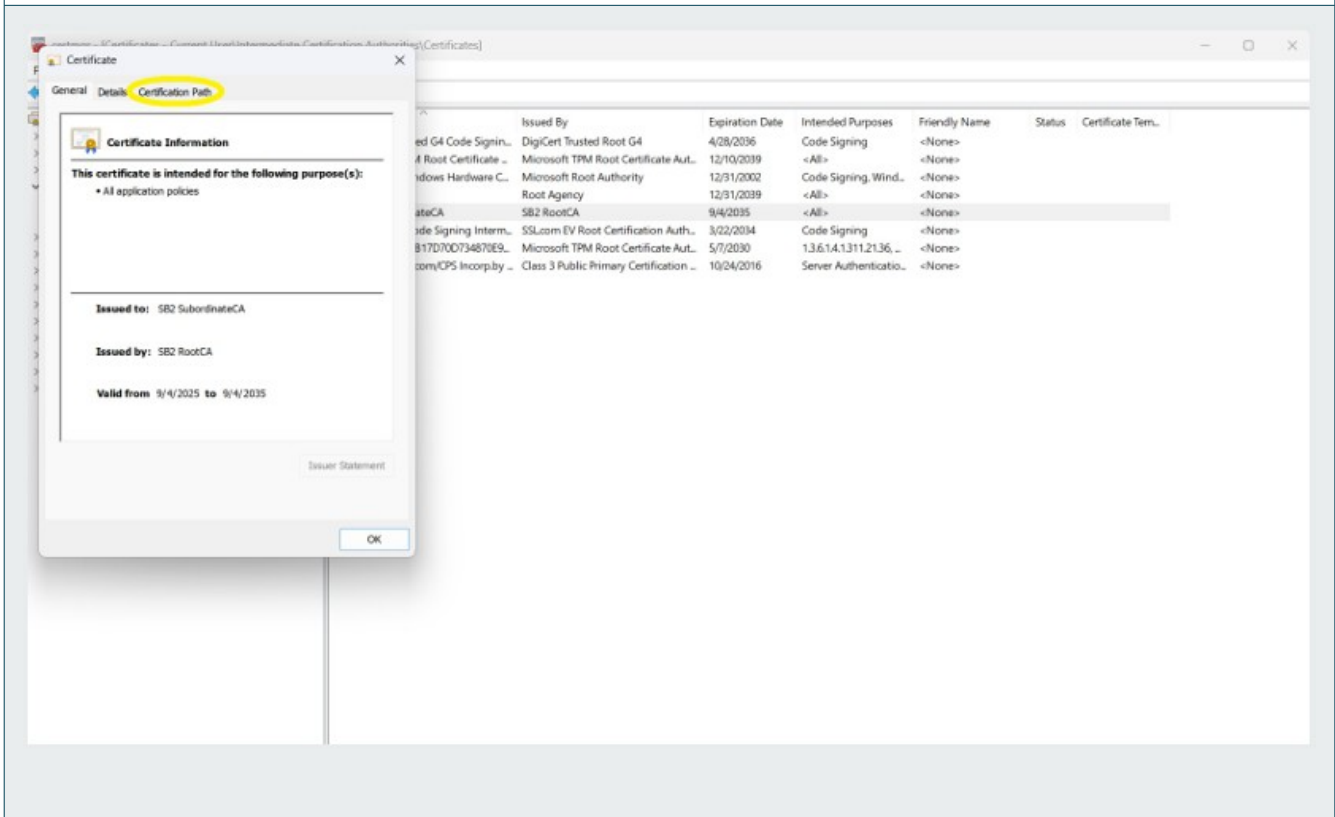
After the SB2 Subordinate CA 1 Certificate has been successfully imported, it will appear in the Intermediate Certification Authorities list as illustrated below:





# VERIFY SB2 SUBORDINATE CA 1 - 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:

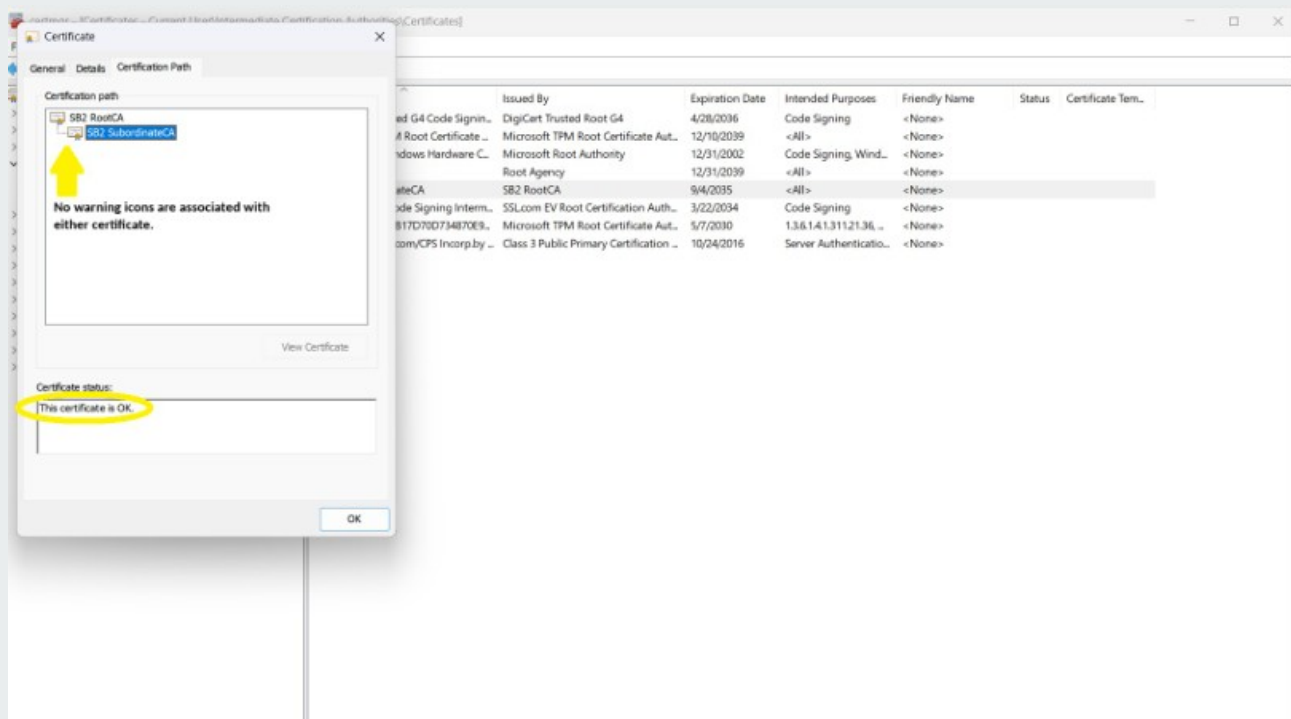




## VERIFY SB2 SUBORDINATE CA 1 - PART 2

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 in 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.”

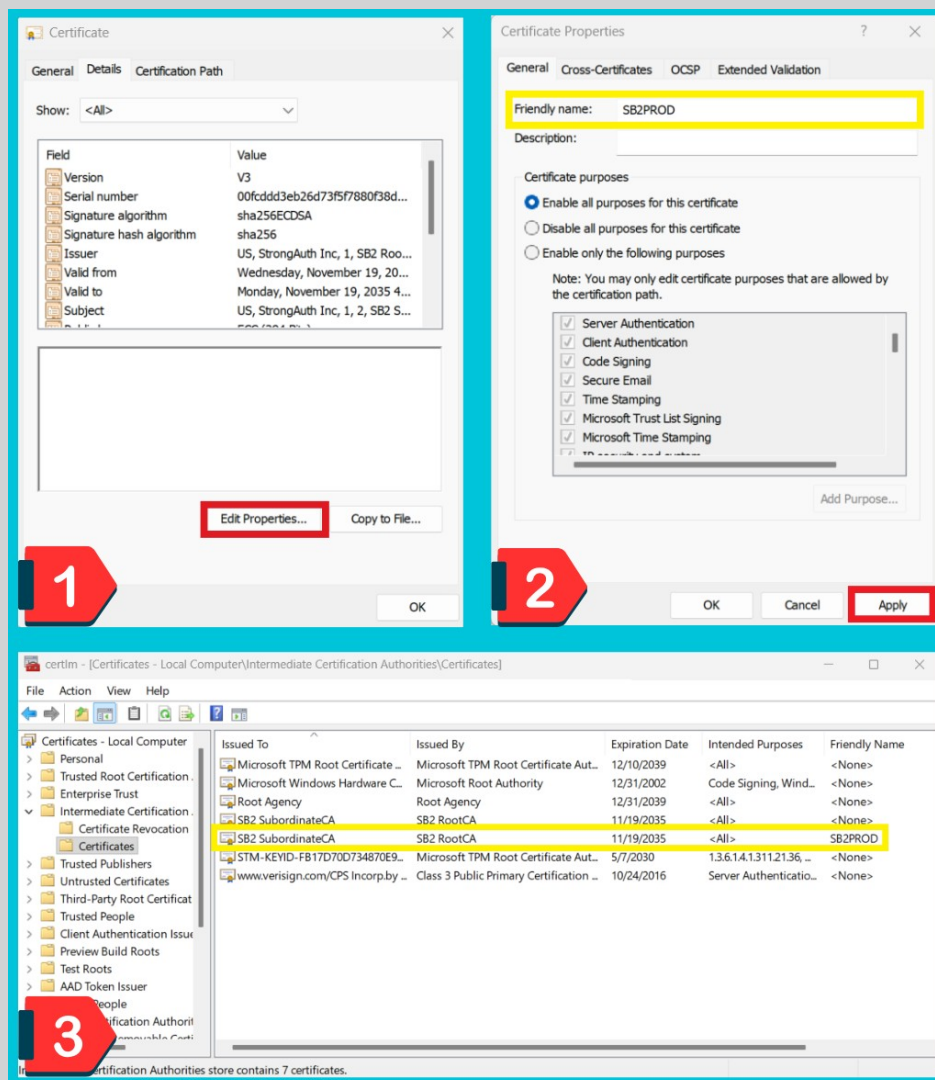


# VERIFY SB2 SUBORDINATE CA 1: PART 3

Follow these steps to create a *Friendly name* for the SB2 Subordinate CA 1:

1. Choose the Details tab.
2. Click Edit Properties (image 1).
3. Add name in Friendly name field (image 2).
4. Click Apply then Click OK to finish.

Friendly names make identifying SubordinateCAs easier in the certificates list (image 3).



**C32**

## IMPORT THE SB2 SUBORDINATE CA 2 CERTIFICATE

Import the SB2 Sub CA 2 certificate by repeating steps [C19](#) - [C31](#). Remember to verify the Sub CA 2 certificate is selected during the process.

**C33**

## RESTART THE COMPUTER

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



# SECTION D



STRONGKEY

D1

## ACCESSING SB2PROD INVITATION LINK

This section will review the steps of accessing the invitation link you received to register a FIDO credential with your Yubikey 5C NFC Security Key with the SB2PROD site.

You must have the Yubikey 5C NFC Security Key – **with Security Key PIN** and the SB2PROD Invitation URL that was sent to you for the FIDO registration process.

D2

## PLUG IN THE YUBIKEY 5C NFC SECURITY KEY

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



## 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.





## 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.

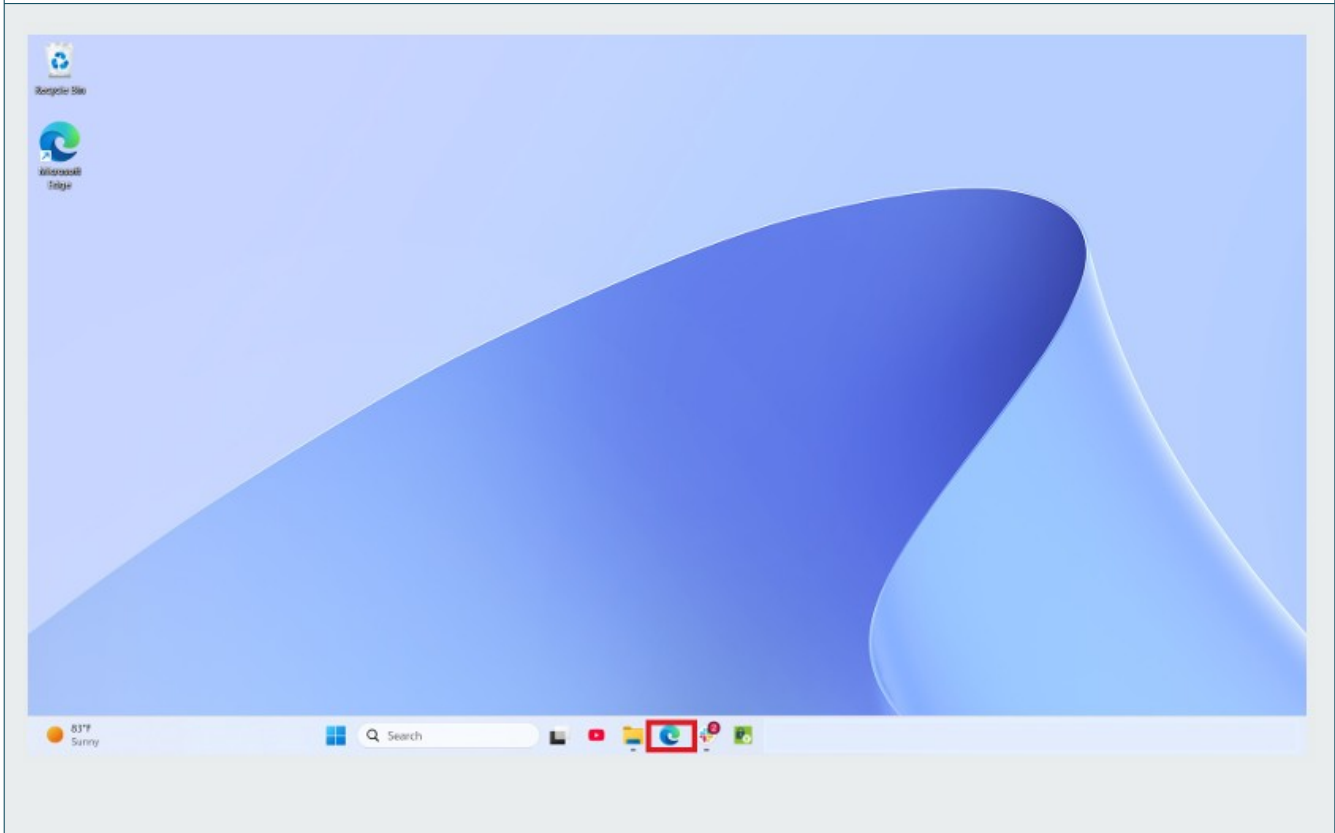
The provided USB adapter pictured below.





## OPEN THE EDGE BROWSER

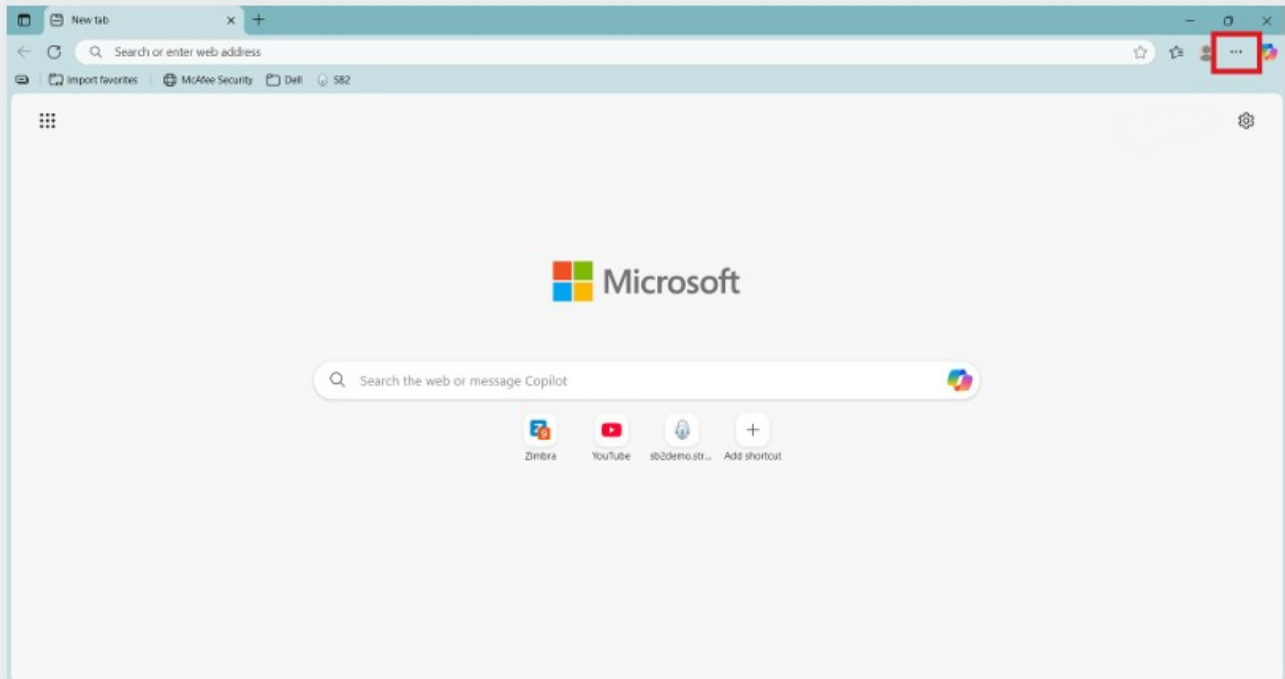
To begin, access the Edge browser by selecting its icon from the Windows taskbar.





# FIND THE EDGE BROWSER DROP DOWN MENU

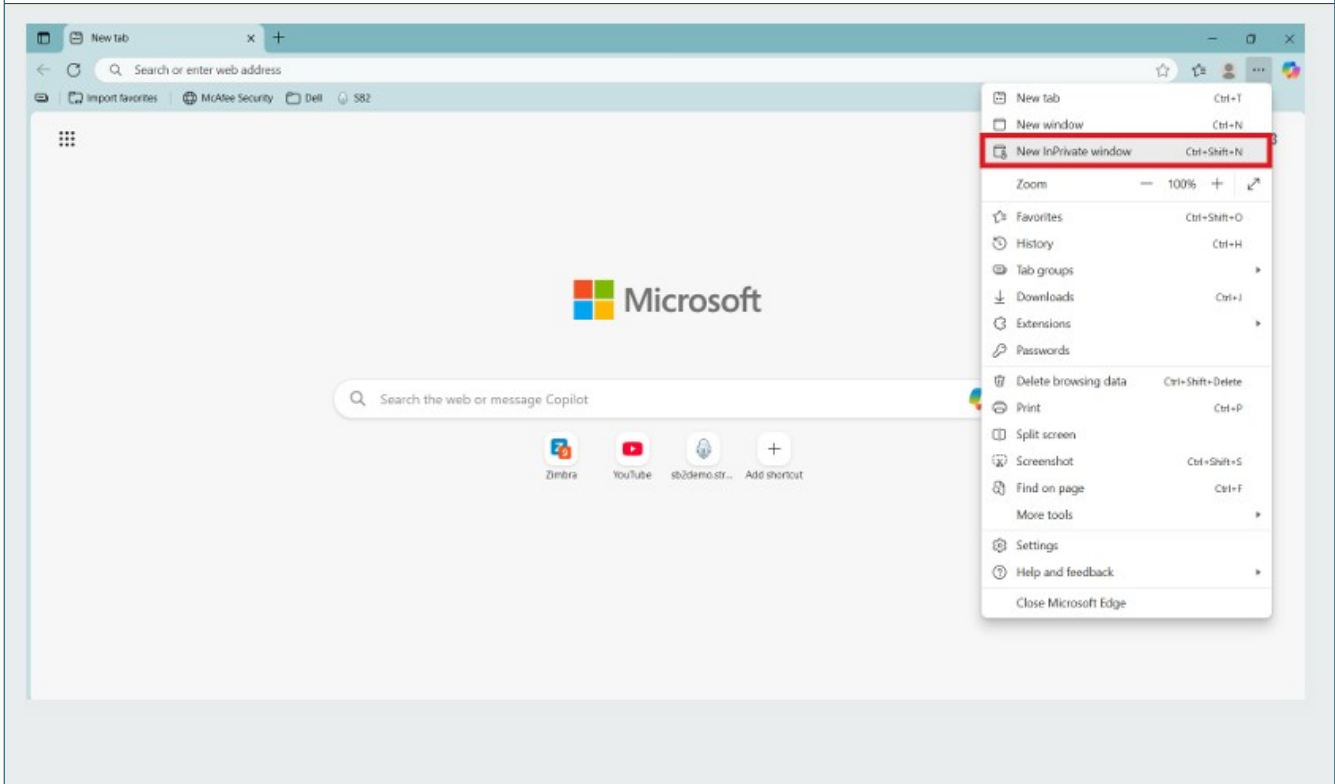
Locate the three-dots icon on the right side of the screen and select it.





# OPEN A NEW InPRIVATE WINDOW

Always use Edge InPrivate mode to access the SB2PROD platform URL (<https://sb2.strongkey.com>).





## SB2PROD PLATFORM URL

In the InPrivate browser address bar, enter the provided SB2PROD Platform invitation link. You will receive the link in an email from a member of the StrongKey Team.



### NOTE

The SB2 registration invite 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://sb2.strongkey.com/sb2/register?  
hash=3d500dec79f6ec257ebddcc56hj78ff1f2d31d557d4c7bf5654](https://sb2.strongkey.com/sb2/register?hash=3d500dec79f6ec257ebddcc56hj78ff1f2d31d557d4c7bf5654)



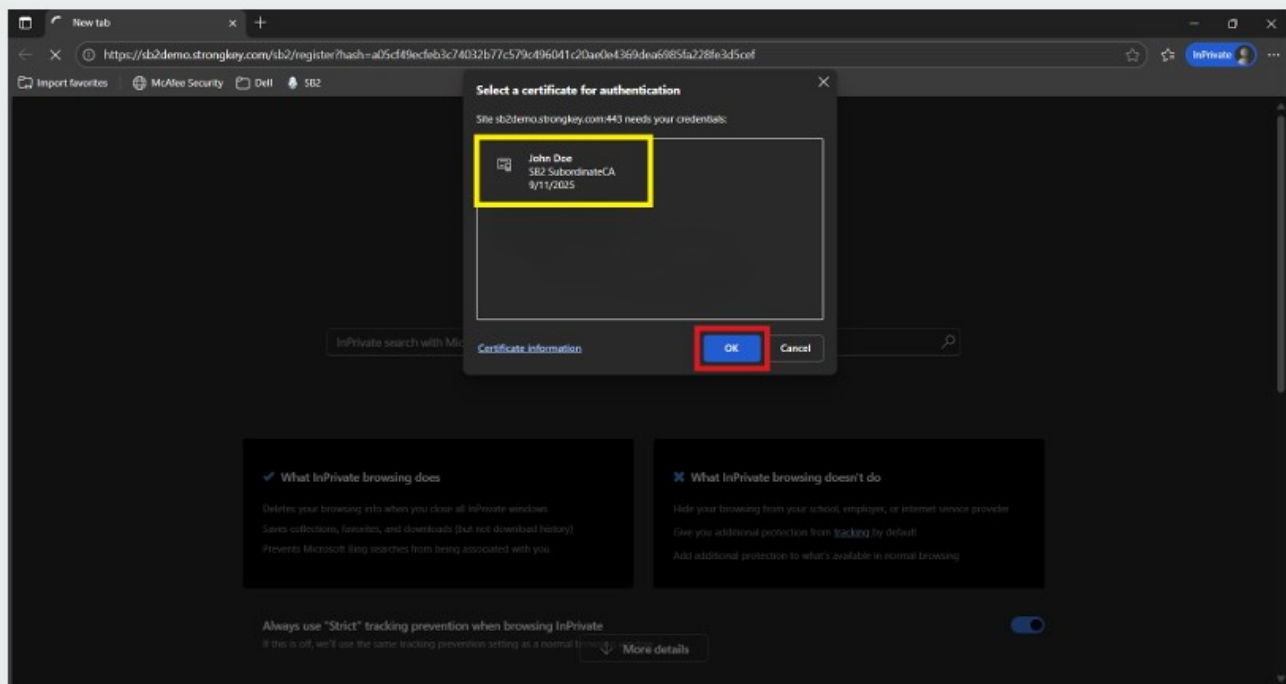
## SELECT THE CERTIFICATE

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 PROD site. Select the presented certificate and **click OK** to proceed.



### NOTE

You will only see 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 [support@strongkey.com](mailto:support@strongkey.com) for support.

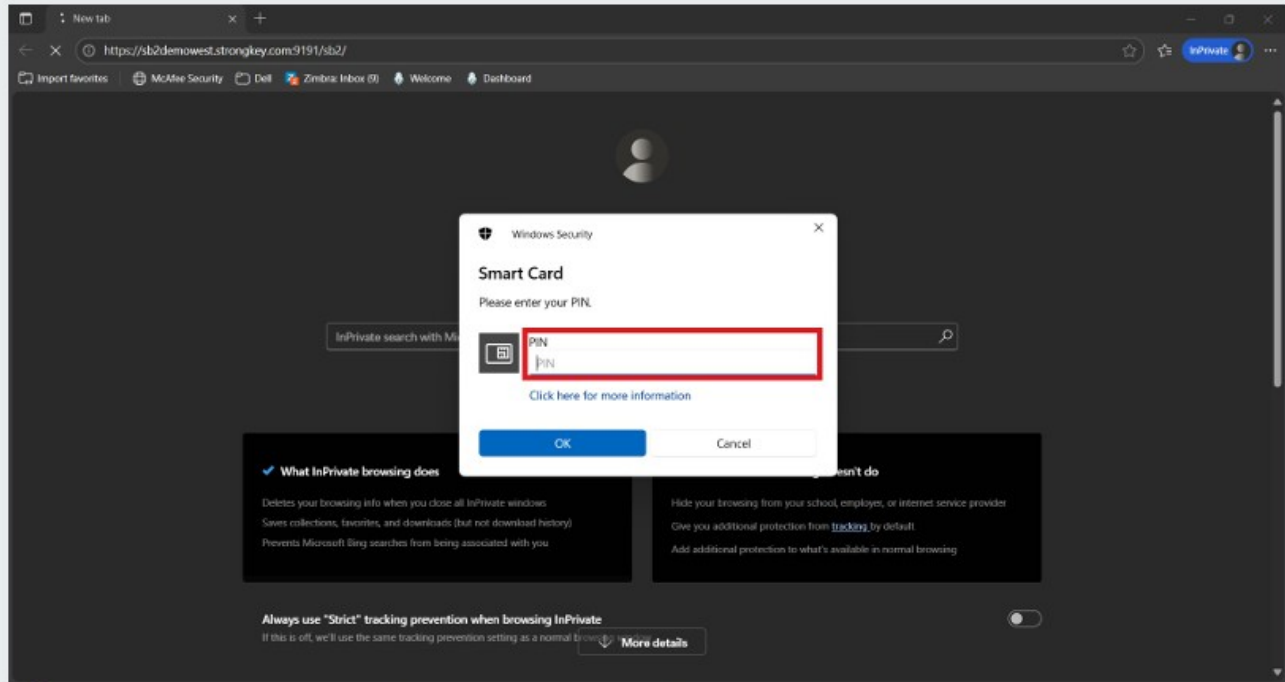




## ENTER SECURITY KEY PIN

The next dialog box will prompt for the Yubikey 5C NFC's 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 PIN, refer to the [Appendix](#) of this guide.





# SB2 PLATFORM 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, some details of your digital certificate information will be displayed (Cypher’s critical details have been redacted to protect his privacy.).
- Legal disclosures for the SB2 platform are located in the middle section. You must scroll all the way to the bottom and agree to the terms disclosed before you may continue with this process.
- Use the right-hand panel to nickname your Security Key. This makes it easier to identify each key if you use more than one.

**STRONGKEY™ SB2**

**Your Digital Certificate**

[Learn More](#)

Username  
cboyer

Full Name  
Clifton Boyer

Organization  
StrongAuth Inc

E-Mail  
clifton.boyer@strongkey.com

Serial No.  
55:CD7D5B7A7474B7D797AC64481E728  
4:27:1E:00

Valid  
Thu Mar 08 16:52:08 EST 2025 - Wed Mar 05  
22:03:33 EST 2031

Other +

**Disclosures**

If you agree with the terms presented here, check the box below and register your Security Key. You agree to:

8. Users who are uncertain about which Personal Data is mandatory are welcome to contact the Owner.


9. The Owner takes appropriate security measures to prevent unauthorized access, disclosure, modification, or unauthorized destruction of the Data.

10. The Data concerning the User is collected to allow the Owner to provide its Service, comply with its legal obligations, respond to enforcement requests, protect its rights and interests, detect any malicious or fraudulent activity, as well as the following: User data management, Registration and authentication.

11. User Data Management: This type of

**Your Security Key**

You were provided with a Security Key (resembling the following image), containing a digital certificate enabling you to see this site. The Security Key will also be used to register a new FIDO credential to authenticate you.



You may give the Security Key a nickname below – such as “JD’s vault credential” or “John Doe’s access key” – to distinguish it from additional Security Keys you may already own and/or acquire in the future.

When you select Register below, you will be prompted for a PIN to the Security Key, and to touch the metal surface with a blinking LED on the Security Key.

Name



# TERMS & 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.



## GIVE SECURITY KEY 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), such as:

- John's Yubikey 5C Security Key for sb2.strongkey.com
- Yubikey for sb2.strongkey.com

The screenshot displays the StrongAuth registration interface. On the left, a user profile for Clifton Boyer is shown, with the email address redacted and labeled "INTENTIONALLY BLURRED FOR YOUR PROTECTION". A red arrow points to the "I agree" checkbox. The middle section contains terms of service, including points 8 through 12. The right section, titled "credential to authenticate you.", features an icon of a security key and instructions on how to name it. The "Name" field contains the text "SB2PROD DOCUMENTATION" and is highlighted with a yellow dashed border. Below the field are "Cancel" and "Register" buttons, with a red arrow pointing to the "Register" button. The footer contains the copyright notice: "Copyright © 2001-2026 StrongAuth, Inc. (dba StrongKey)".



# ENTER SECURITY KEY PIN

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



## NOTE

This step is called **User Verification (UV)** in the FIDO ecosystem. It confirms that the SB2PROD platform is interacting with the legitimate Security Key owner by verifying your PIN, which should never be shared. Each time you use your FIDO credential to sign in, you'll complete this UV step as a required security measure.

The screenshot displays the registration interface for a Security Key. On the left, user information for Clifton Boyer is shown, including his organization (StrongAuth Inc), email (clifton.boyer@strongkey.com), and a blurred serial number. A central Windows Security dialog box is open, titled "Save your passkey". It shows the email address and a field for the "Security Key PIN" which is currently masked with dots. A red arrow points to the "OK" button. To the right, the registration steps are visible, including a "Register" button. The bottom of the screen contains the copyright notice: "Copyright © 2001-2026 StrongAuth, Inc. (dba StrongKey)".



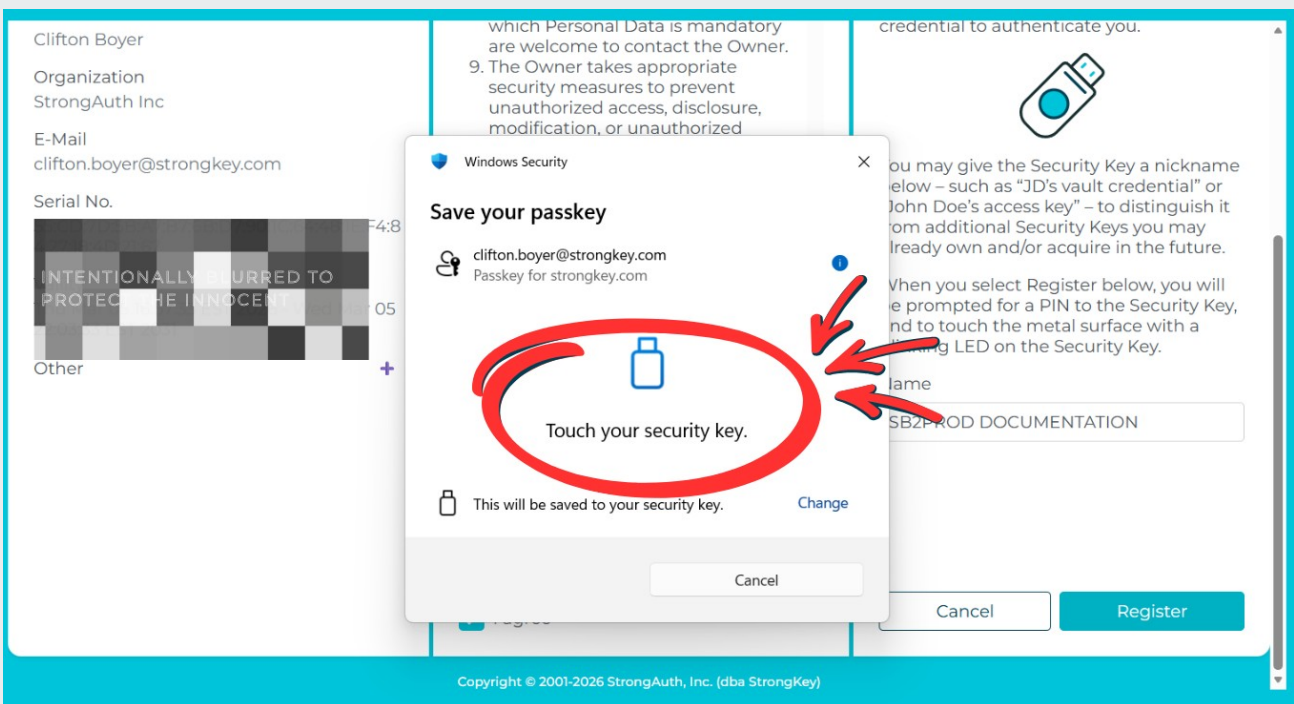
# TOUCH THE SECURITY KEY

To continue adding the credential, 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 is called the “Test of User Presence” (TUP) in the FIDO ecosystem. It ensures that no remote attacker can impersonate you, because they would need both your Security Key and your physical interaction at your computer. Each time you use your FIDO credential to sign in to the SB2 platform, you’ll complete this brief TUP check as a security safeguard.





# SB2PROD CONFIRMATION

Upon successfully adding the credential, a dialog box will confirm the registration action. Click **Continue** to sign-in to SB2PROD.

Clifton Boyer

Organization  
StrongAuth Inc

E-Mail  
clifton.boyer@strongkey.com

INTENTIONALLY OBLURRED TO PROTECT THE INNOCENT

Other +

which Personal Data is mandatory are welcome to contact the Owner.

9. The Owner takes appropriate security measures to prevent unauthorized access, disclosure, modification, or unauthorized destruction of the Data.

10. The Data concerning the User is collected to allow the Owner to provide its Service, comply with its legal obligations, respond to enforcement requests, protect its rights and interests, detect any malicious or fraudulent activity, as well as the following: User data management, Registration and authentication.

11. User Data Management: This type of service allows the Owner to build user profiles by starting from an email address, a personal name, or other information that the User provides to this Application

12. Registration and Authentication: By registering or authenticating, Users allow this Application to identify them and give them access to dedicated services.

I agree

credential to authenticate you.

You will be prompted to assign a Security Key a nickname to be stored in your vault credential of "Job" as an "access key" – to distinguish it from additional Security Keys you may already own and/or acquire in the future.

When you select Register below, you will be prompted for a PIN to the Security Key, and to touch the metal surface with a blinking LED on the Security Key.

Name

SB2PROD DOCUMENTATION

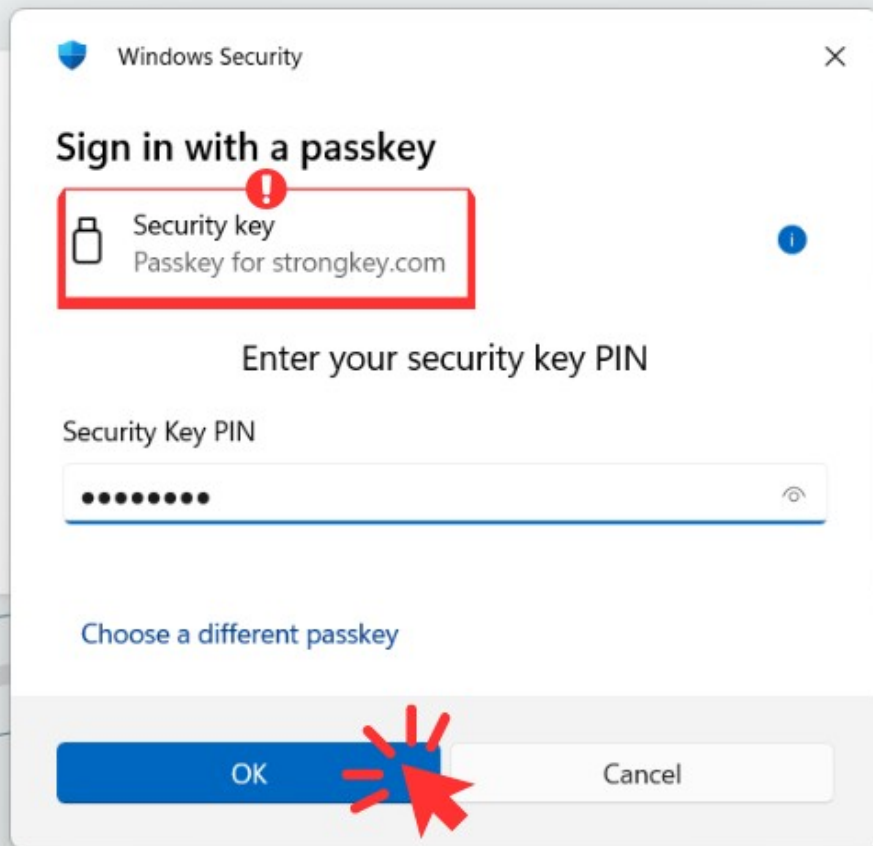
Continue →

**You've successfully registered**  
Click 'Continue' to proceed to the login page.

Copyright © 2001-2026 StrongAuth, Inc. (dba StrongKey)

# D17 SIGNING IN

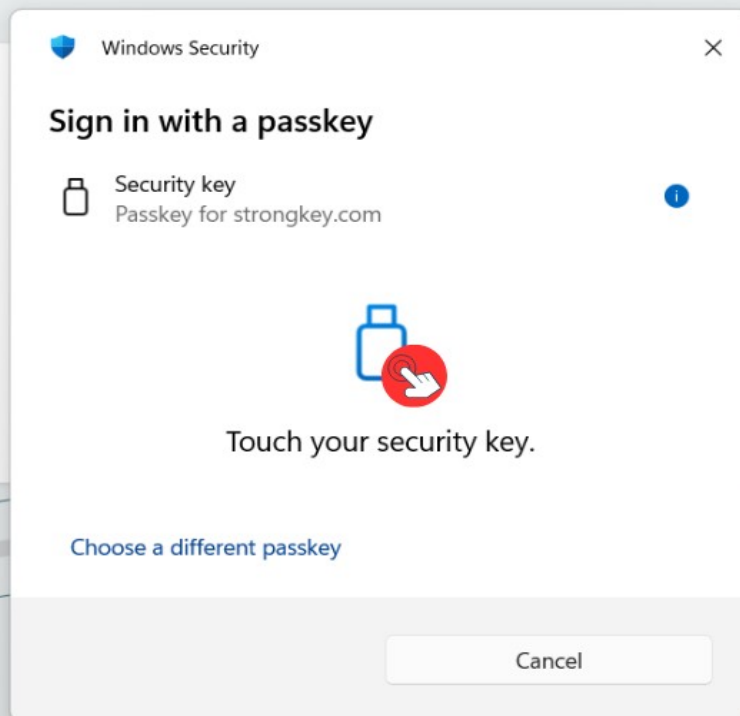
After clicking **Continue**, a prompt will appear prompting you to sign in with the new credential. Verify you are signing in with the Security Key when authenticating to the SB2PROD. Enter your PIN and **Click OK**.





## TEST OF USER PRESENCE (TUP)

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





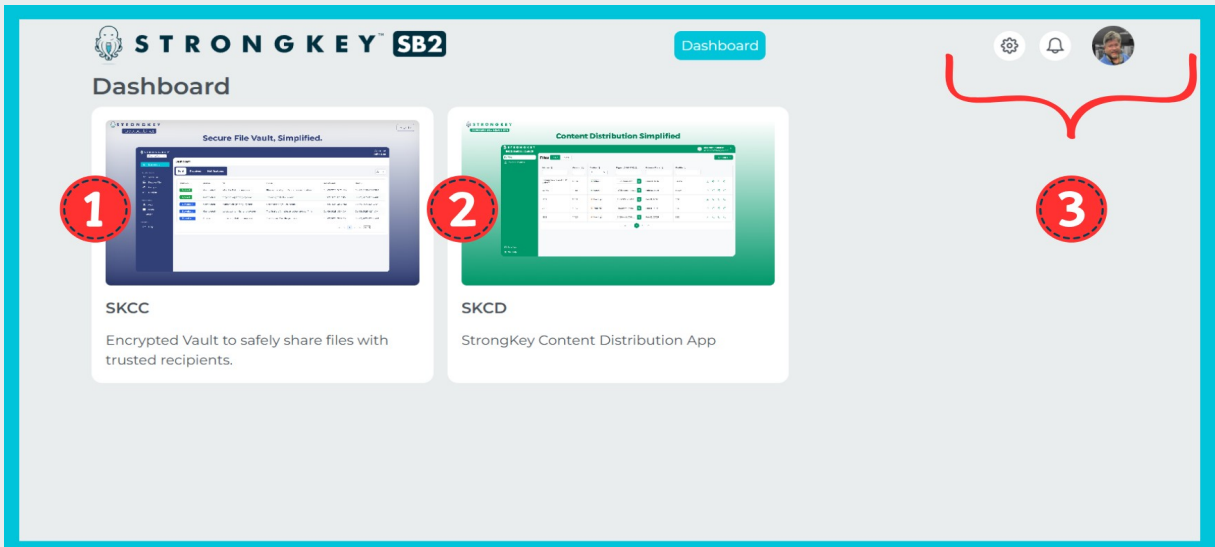
# THE SB2PROD PLATFORM DASHBOARD

CONGRATULATIONS! Your access to the **SB2PROD 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 SB2 users have access to two primary applications and:

1. **StrongKey CryptoCabinet (SKCC):** For securely storing and sharing encrypted files containing sensitive data.
2. **StrongKey Content Distribution (SKCD):** For storing and sharing digitally signed, unencrypted documents.
3. Settings, Notifications and profile picture.

Clicking either image on the SB2 Dashboard opens the application in a new browser tab. Detailed user guides for both SKCC and SKCD are available separately.



**WELL DONE!**

# APPENDIX



**STRONGKEY**

**NOTE: This document is primarily for StrongKey customers, suppliers and partners.**



## COPYRIGHTS AND NOTICES

Copyright 2001–2026 StrongAuth, Inc. (d/b/a StrongKey), 21060 Homestead Rd Suite 222 Cupertino CA 95014, U.S.A. All rights reserved.

StrongAuth, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more U.S. patents or pending patent applications in the U.S. and in other countries. U.S. Government Rights—Commercial software. Government users are subject to the StrongAuth, Inc. standard license agreement and applicable provisions of the Federal Acquisition Regulations and its supplements. This distribution may include materials developed by third parties. StrongAuth, StrongKey, StrongKey Lite, StrongKey CryptoCabinet, StrongKey CryptoEngine, StrongKey FIDO Server, StrongKey Tellaro, StrongKey Tellaro Small Business Security Bundle (SB2), the StrongAuth logo, the StrongKey logo, the StrongKey Lite logo, the StrongKey CryptoCabinet logo and the StrongKey CryptoEngine logo are trademarks or registered trademarks of StrongAuth, Inc. or its subsidiaries in the U.S. and other countries.

Products covered by and information contained in this publication are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical or biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

DOCUMENTATION IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.



## **YUBICO YUBIKEY 5C NFC SECURITY KEY: CHANGING THE PERSONAL IDENTIFICATION NUMBER (PIN)**

**This appendix guides you through changing your PINs on the Yubico Yubikey 5C NFC Security Key.**

## CHANGING A YUBIKEY 5C NFC 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.

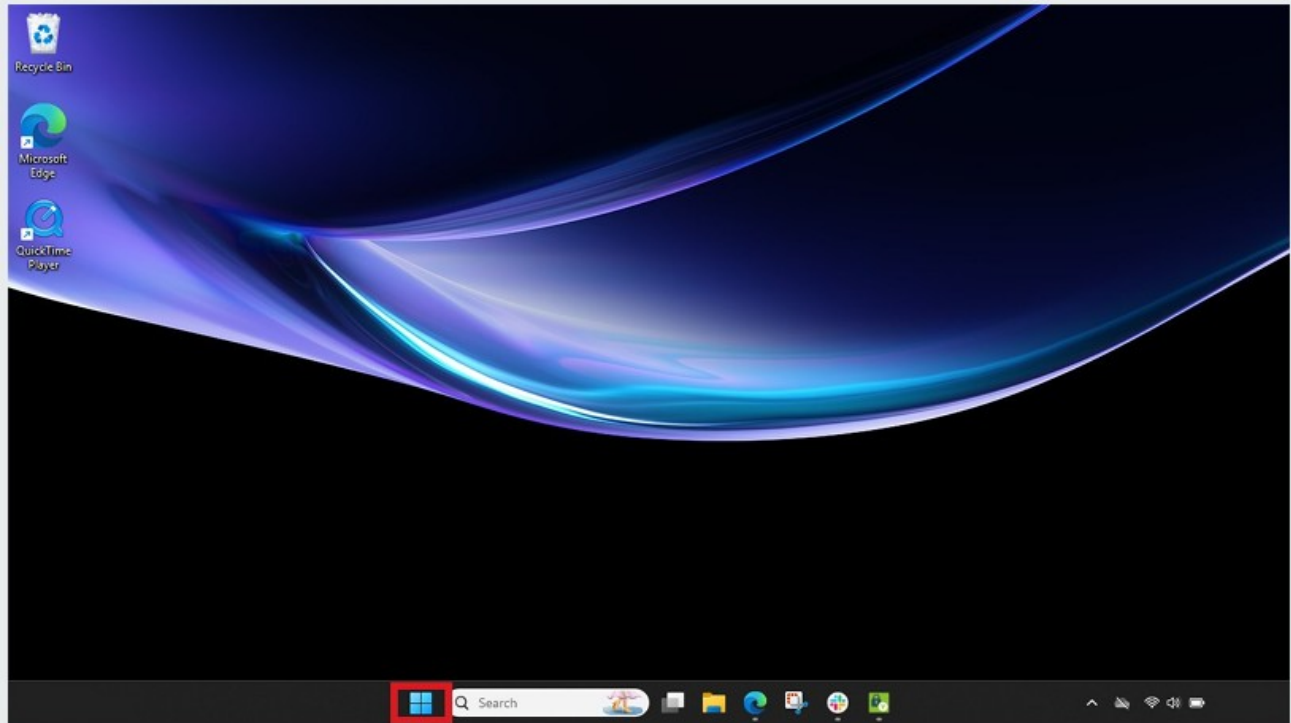
However, StrongKey recommends using the SAME PIN to both containers of the **Security Key** to reduce the burden on users. As long as the **Security Key** is safely in the possession of the legitimate user, and the legitimate user is NOT sharing the PIN to the **Security Key** with anyone, the user will 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 PIV certificate and the other for the FIDO credential.



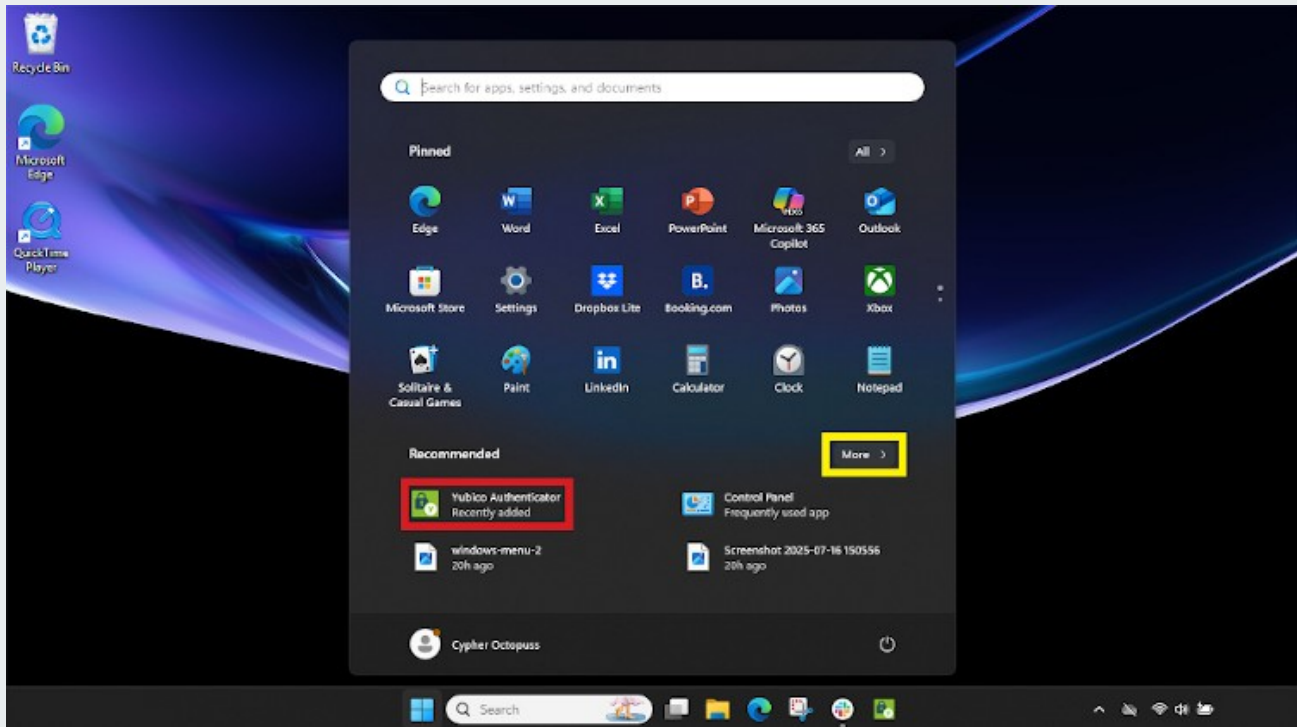
# OPEN THE YUBICO AUTHENTICATOR APPLICATION

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



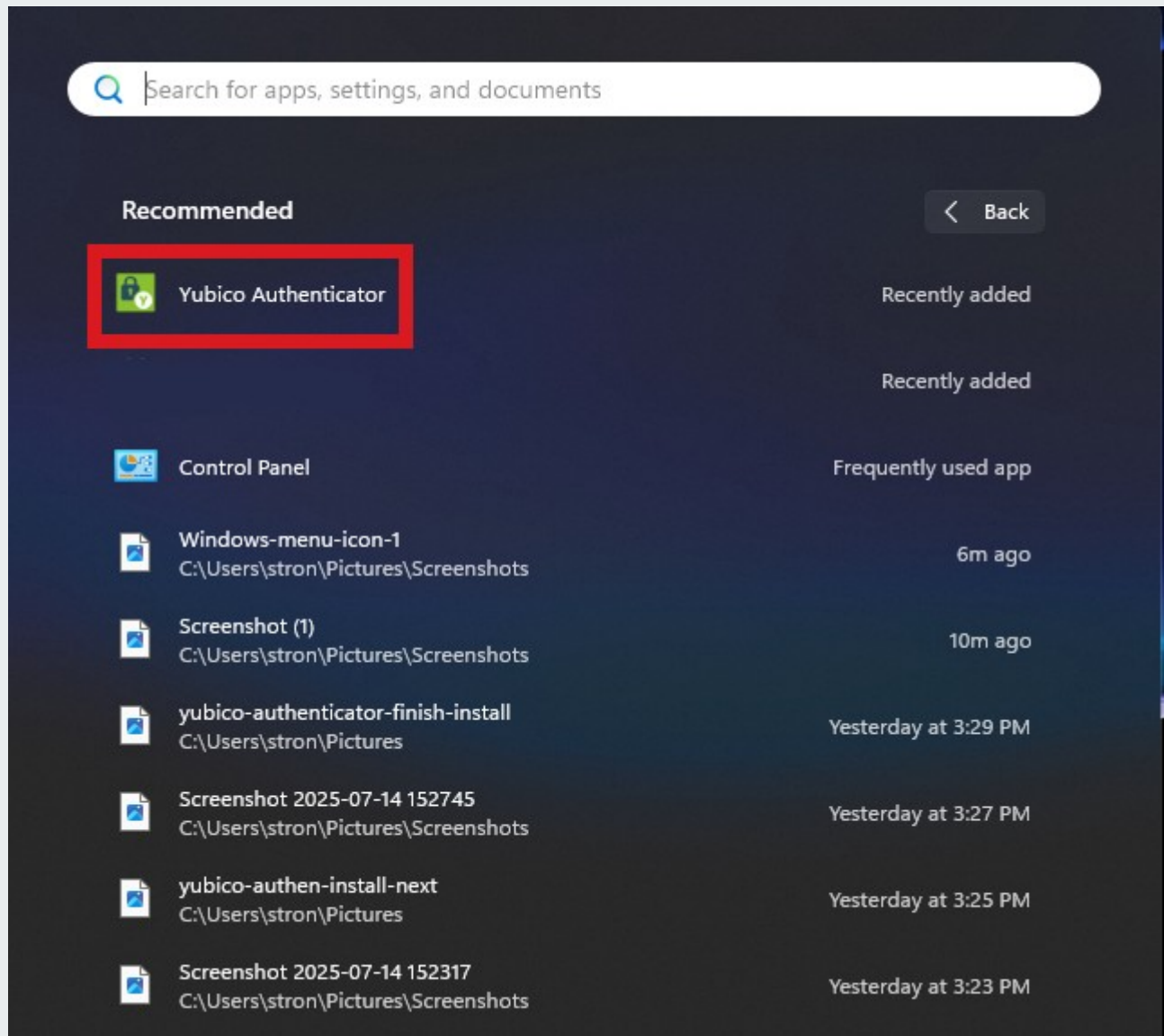
# SELECT YUBICO AUTHENTICATOR

From the menu, select the Yubico Authenticator application. If it does not appear under **Recommended**, click the **More** option on the right to locate the application.



## CLICKING THE “MORE” OPTION

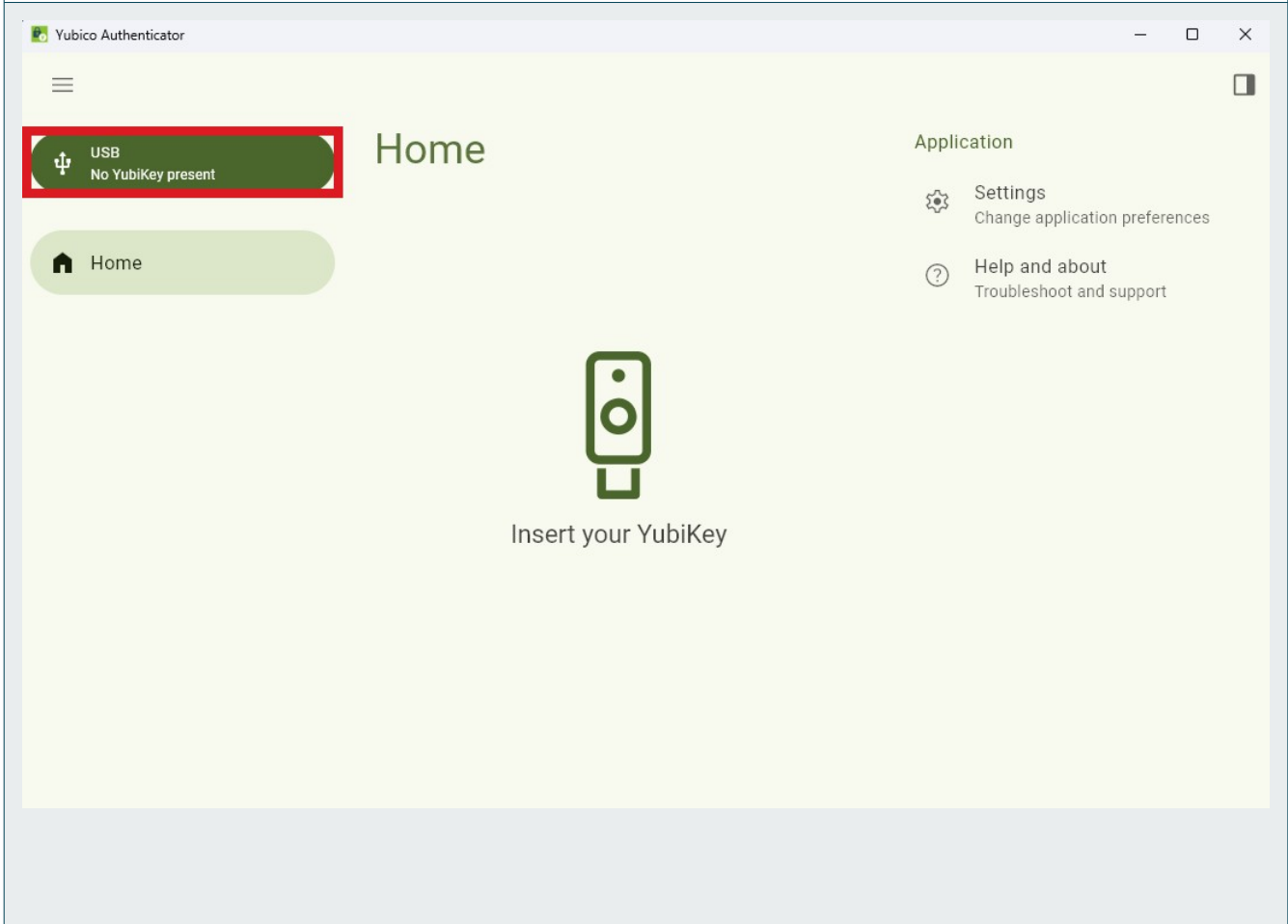
Since the Yubico Authenticator application was recently installed, it will typically appear near the top of the menu list.





# THE YUBICO AUTHENTICATOR APPLICATION

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



# INSERT THE YUBIKEY 5C NFC

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

## AP7

# 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.



AP8

## 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.

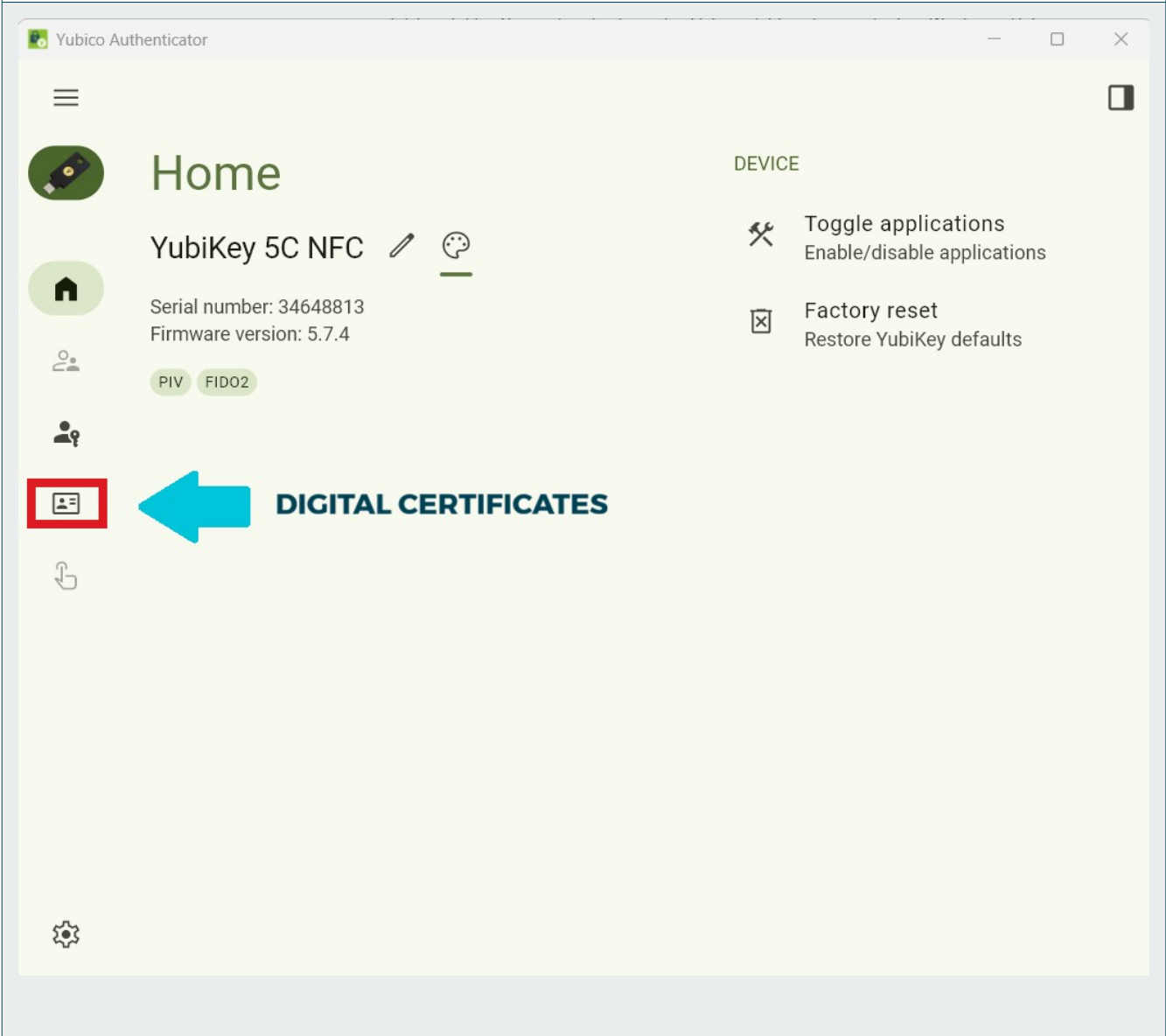
The provided USB adapter pictured below.



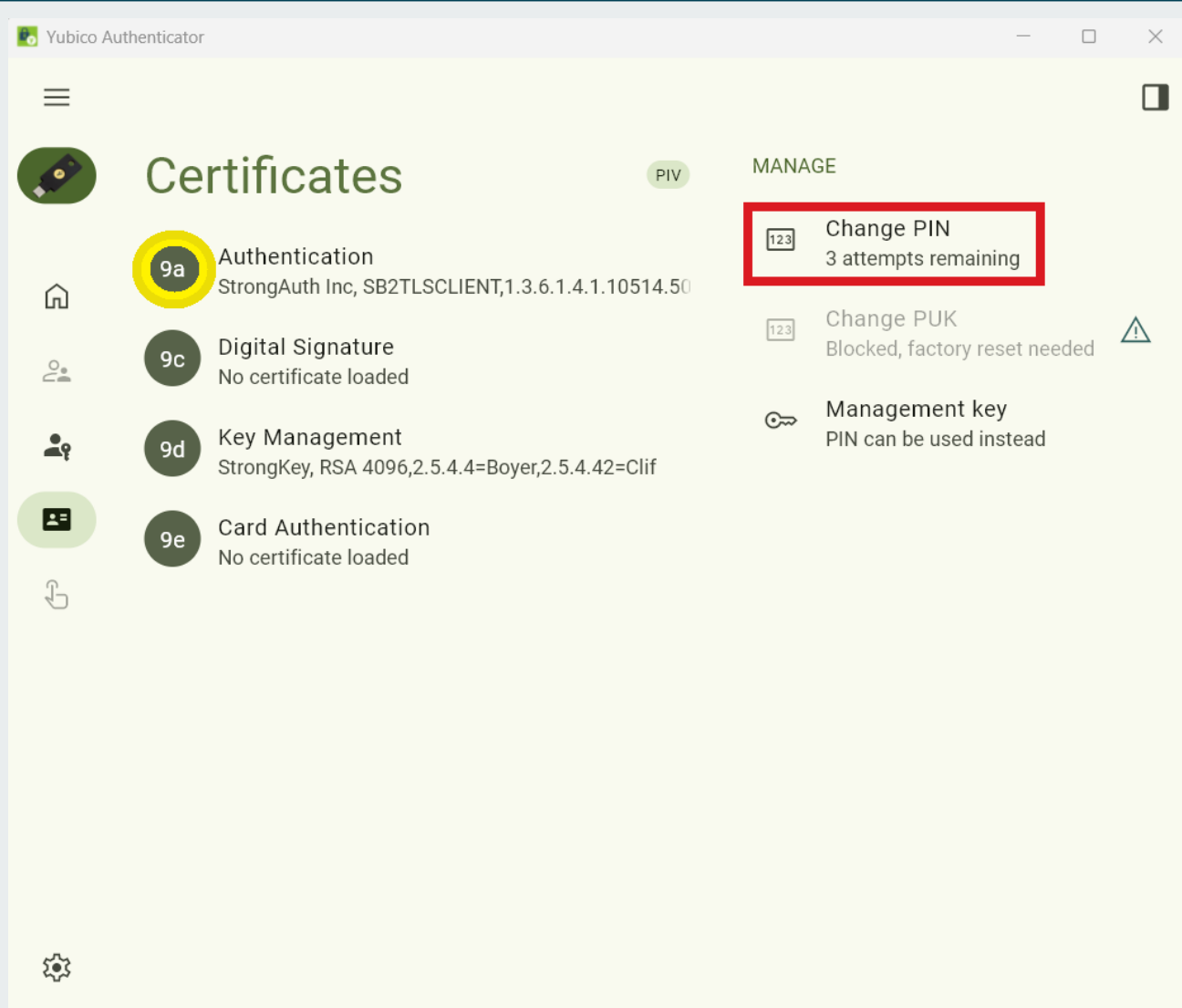


# CHANGING THE DIGITAL CERTIFICATE PIN

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



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



# 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.

Yubico Authenticator

### Change PIN

Current PIN  0/6

New PIN  6/8  
A PIN must be at least 6 characters long.

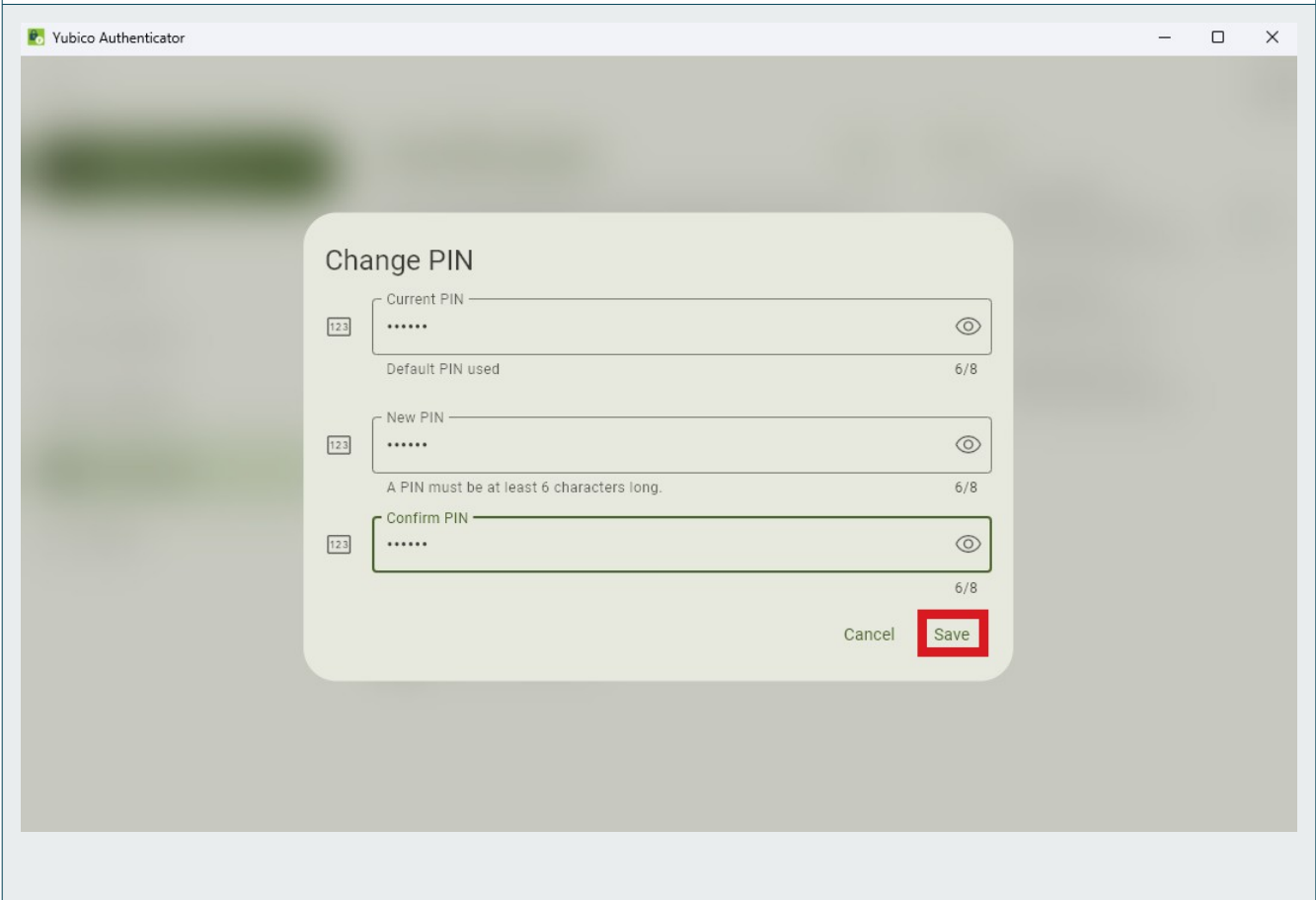
Confirm PIN  6/8

Cancel Save



## 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.





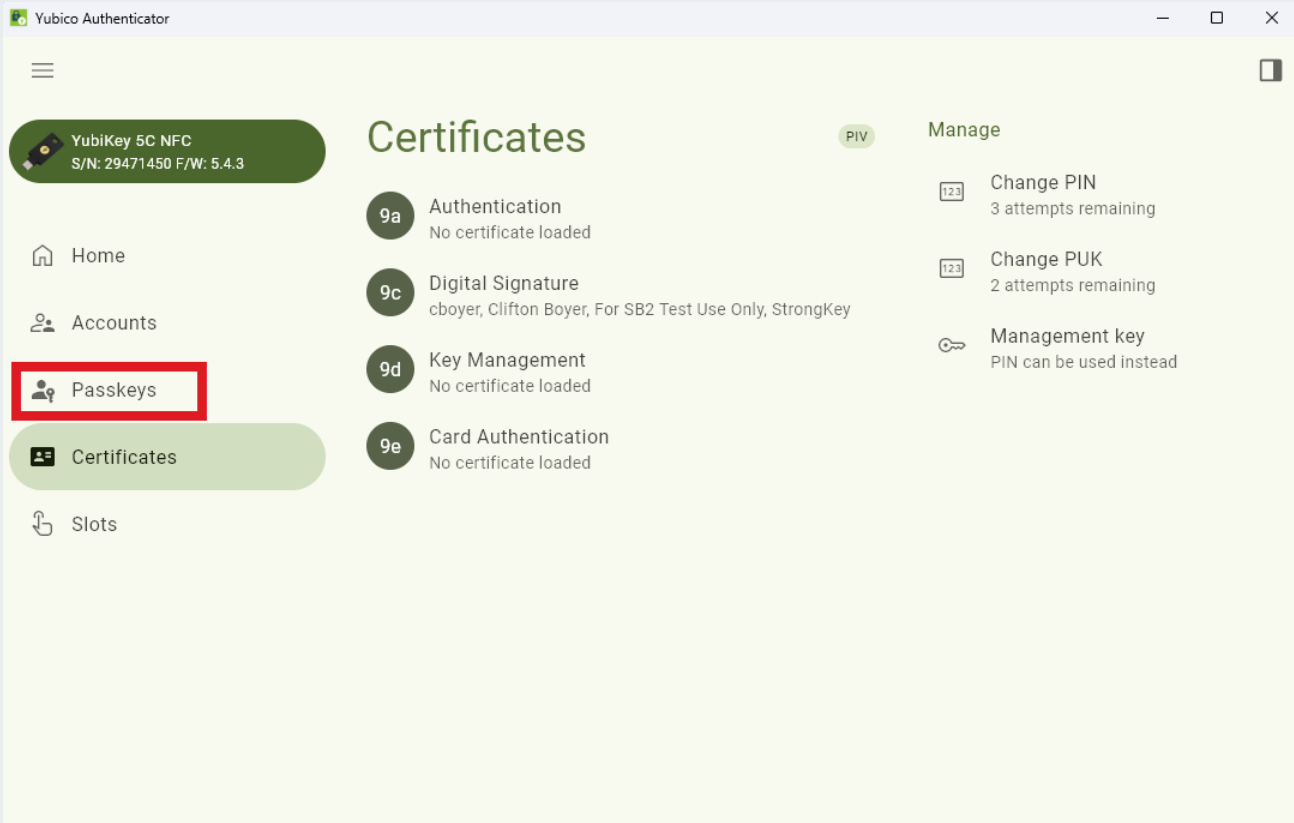
# CHANGING THE FIDO CREDENTIALS PIN

To update the second PIN, click on the **Passkeys** menu option to the left.



**NOTE**

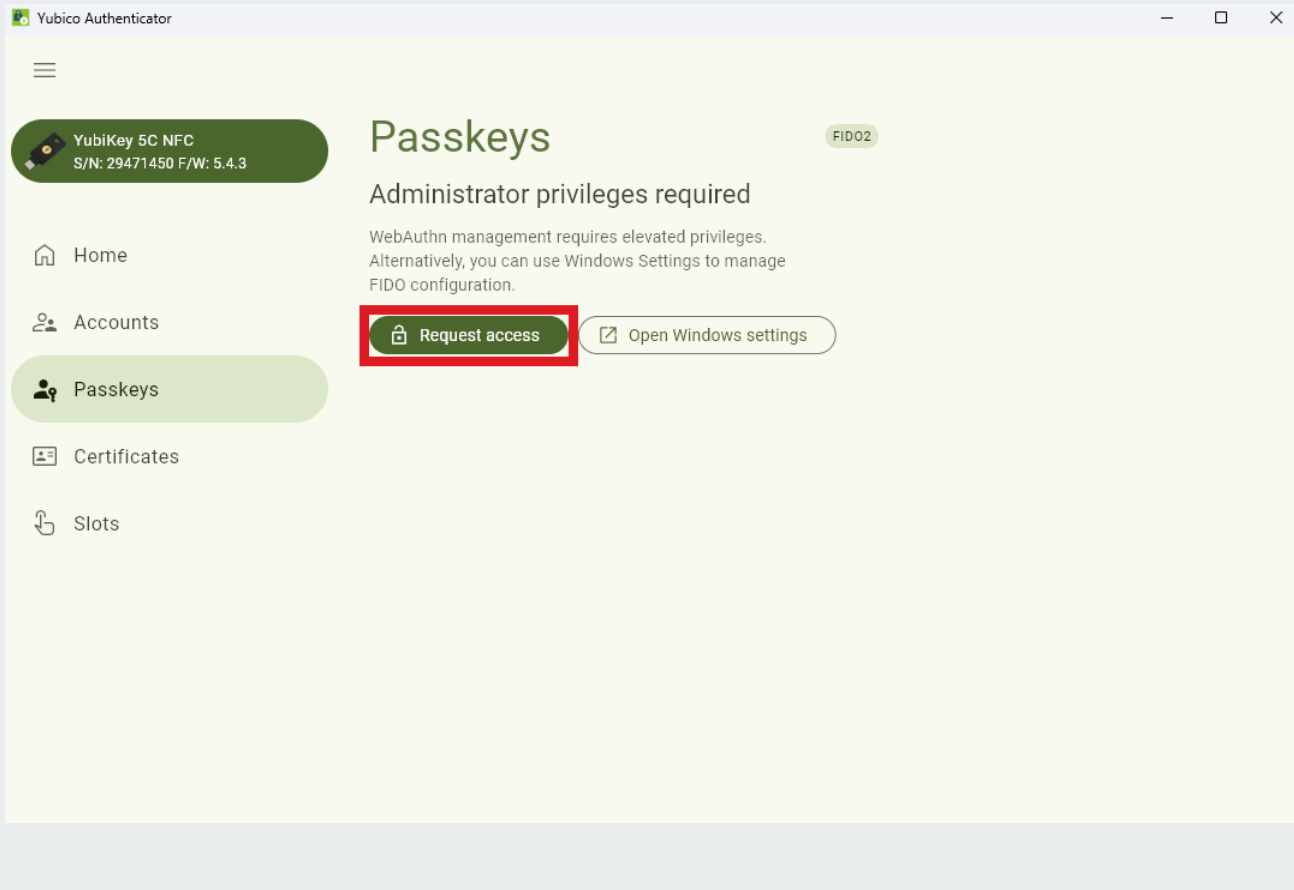
StrongKey recommends using the same PIN for the Security Key.



AP14

## PASSKEYS MENU

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



AP15

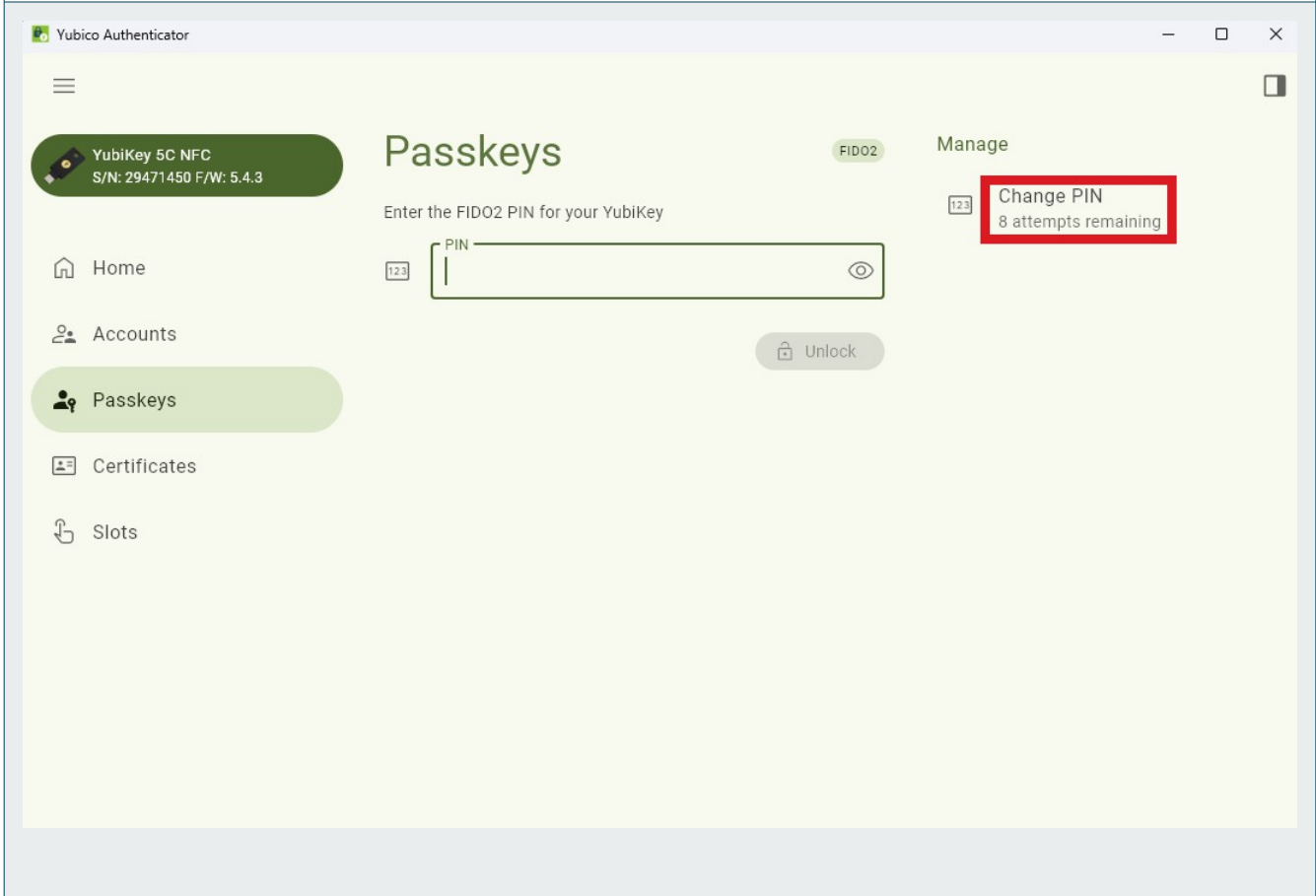
## YUBICO AUTHENTICATOR APPLICATION PERMISSION

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



# CHANGE PIN OPTION

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



## 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.

Yubico Authenticator

Change PIN

Current PIN

New PIN

Confirm PIN

A PIN must be 6-63 characters long and may contain letters, numbers and special characters.

Cancel Save

## AP18 **SUCCESS!**

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

