

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.



COPYRIGHT & 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



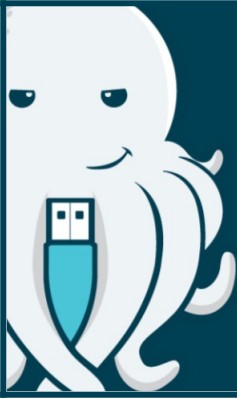
PREREQUISITES

- 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	<u>Installing the Yubico Authenticator Application</u>	4
B	<u>Installing the Yubikey Minidriver for Windows 11</u>	13
C	<u>Importing SB2 Root CA & SB2 Subordinate CA Certificates into Microsoft Trustore</u>	21
D	<u>Accessing an SB2PROD Invitation Link URL</u>	52
AP	<u>Appendix: Changing a Yubico Yubikey 5C NFC Personal Identification Number (PIN)</u>	70



SECTION A

A1

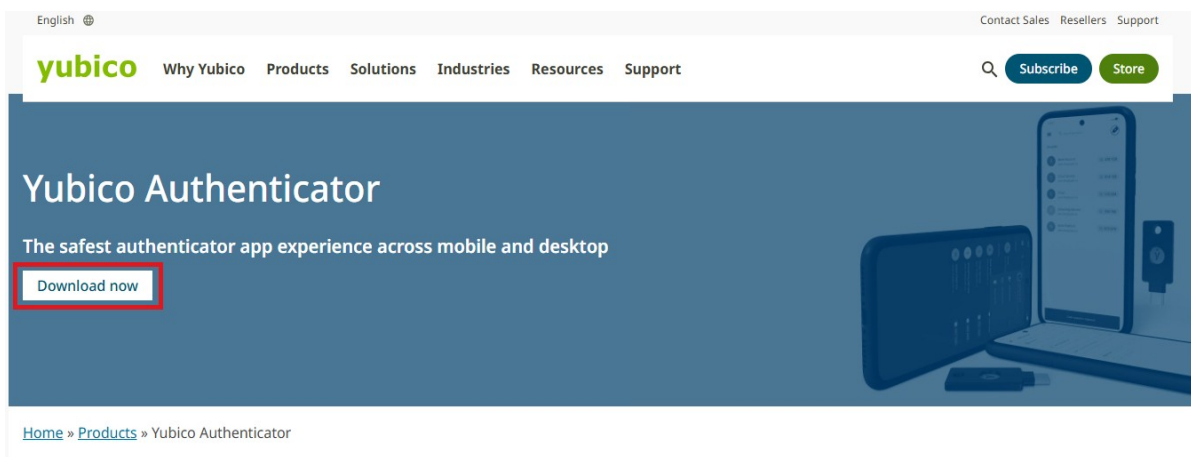
INSTALLING THE YUBICO AUTHENTICATOR APPLICATION

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.







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 one or more 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 \(on Google Play\)](#)

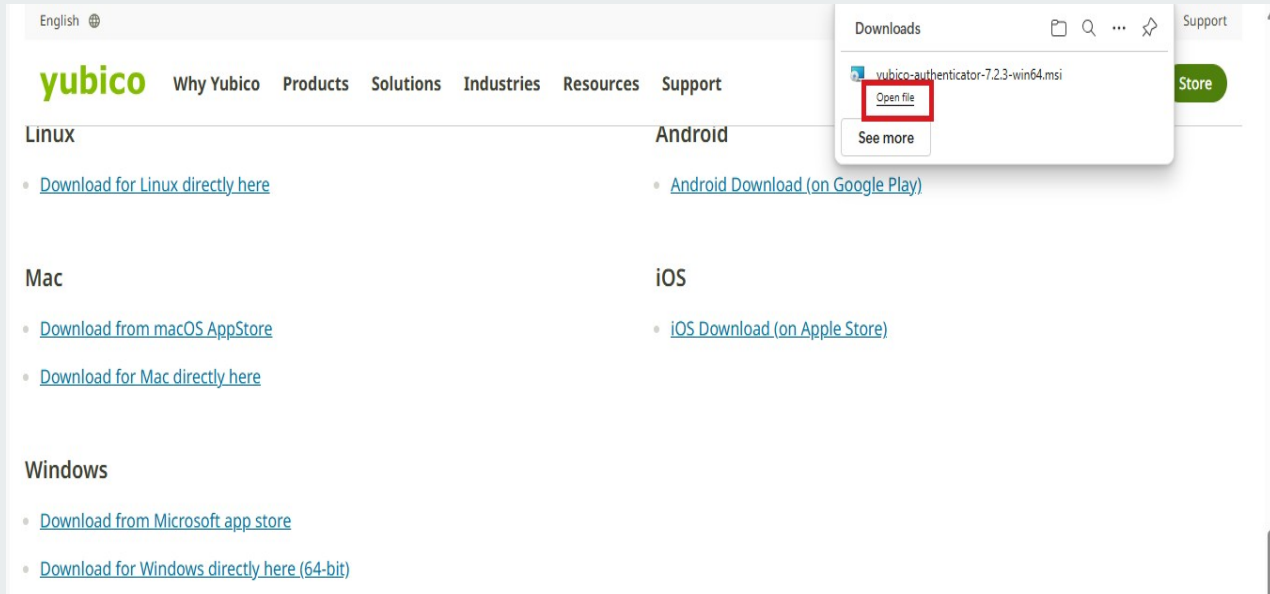
iOS

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

A4

OPENING THE YUBICO AUTHENTICATOR APPLICATION FILE

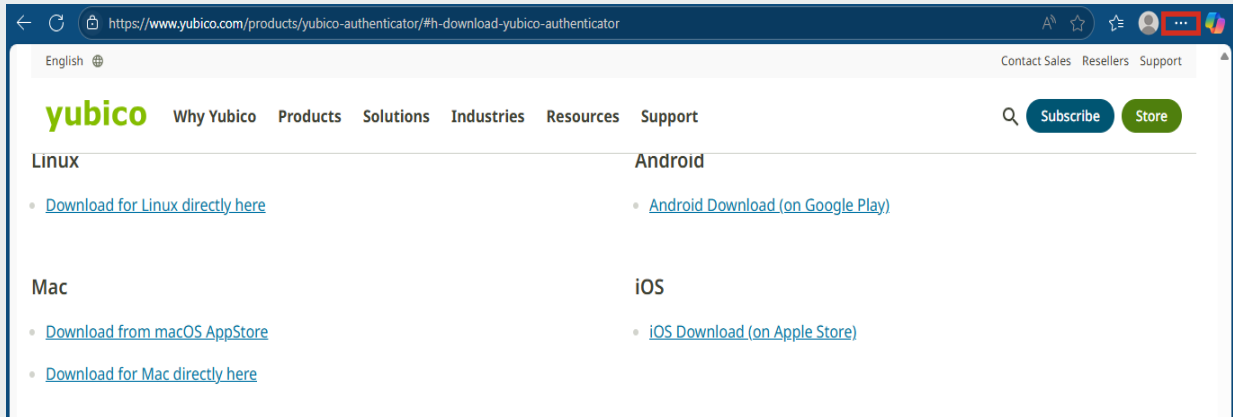
After clicking the download link, MS Edge will display a pop-up confirming the Authenticator application file has been successfully downloaded and ready for installation. Click the open file link.



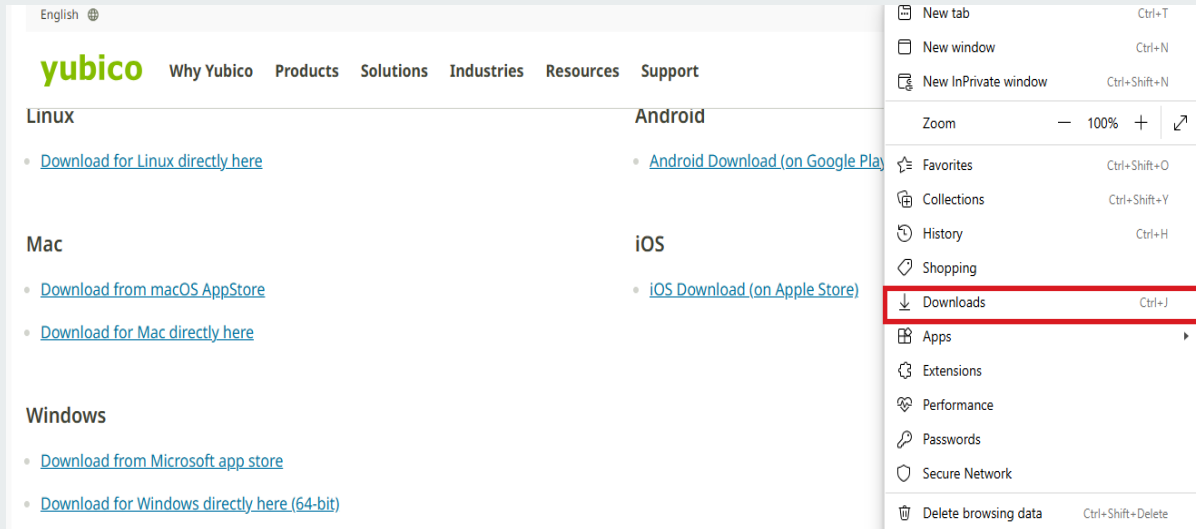
A5

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.



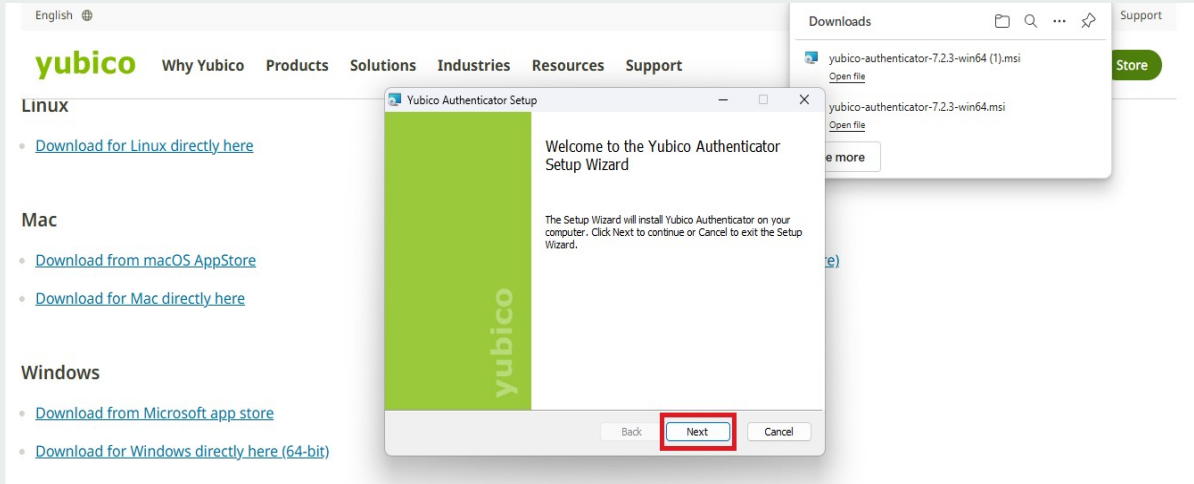
From the drop-down menu, select **Downloads**.



A7

YUBICO AUTH SETUP WIZARD

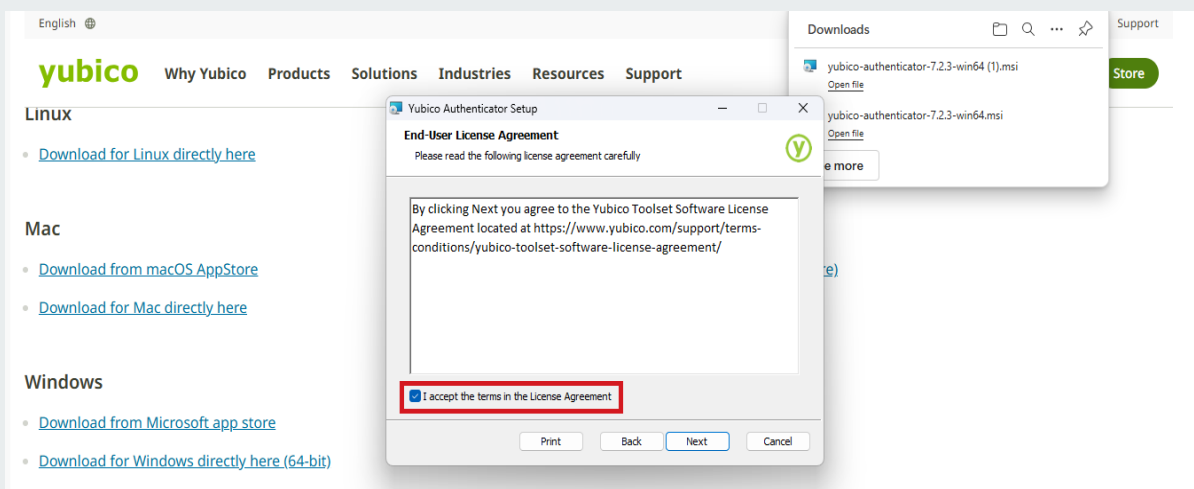
A Setup Wizard window will appear, Click Next.



A8

YUBICO AUTHENTICATOR APPLICATION TERMS & CONDITIONS

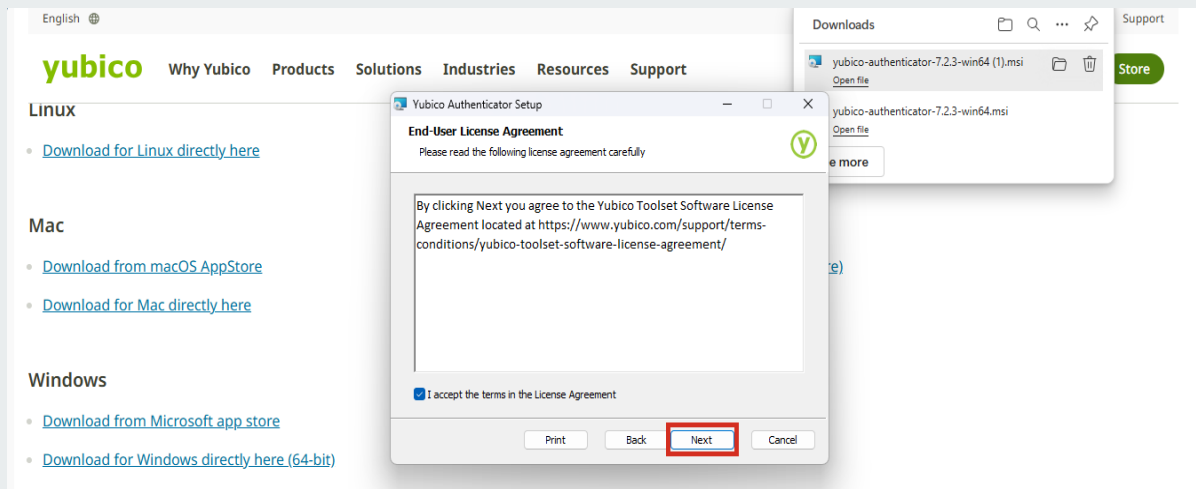
Accept the terms of the end-user license agreement.





YUBICO AUTHENTICATOR APPLICATION TERMS & CONDITIONS

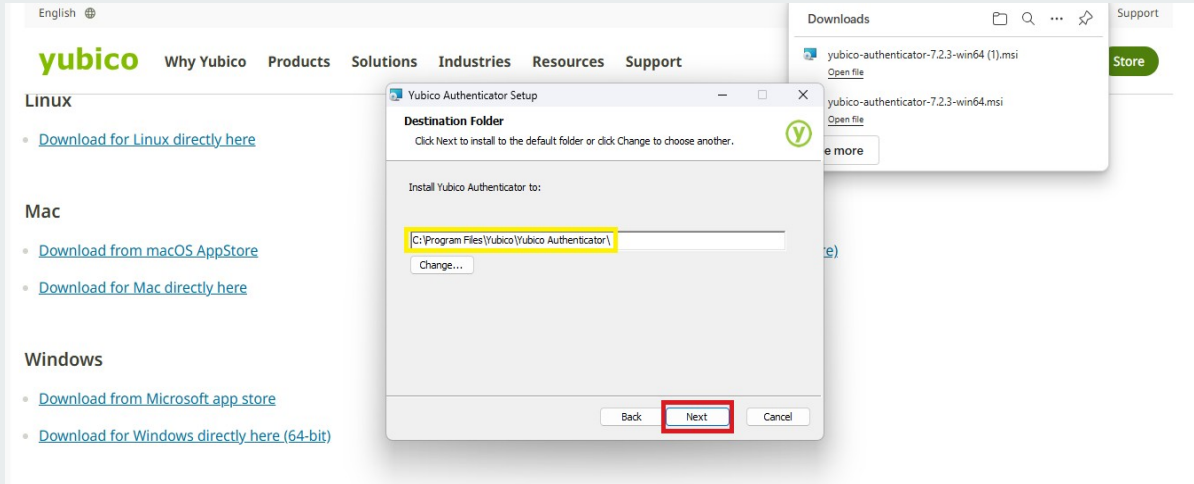
Click Next on the end-user license agreement window.



A10

SELECT DESTINATION FOLDER

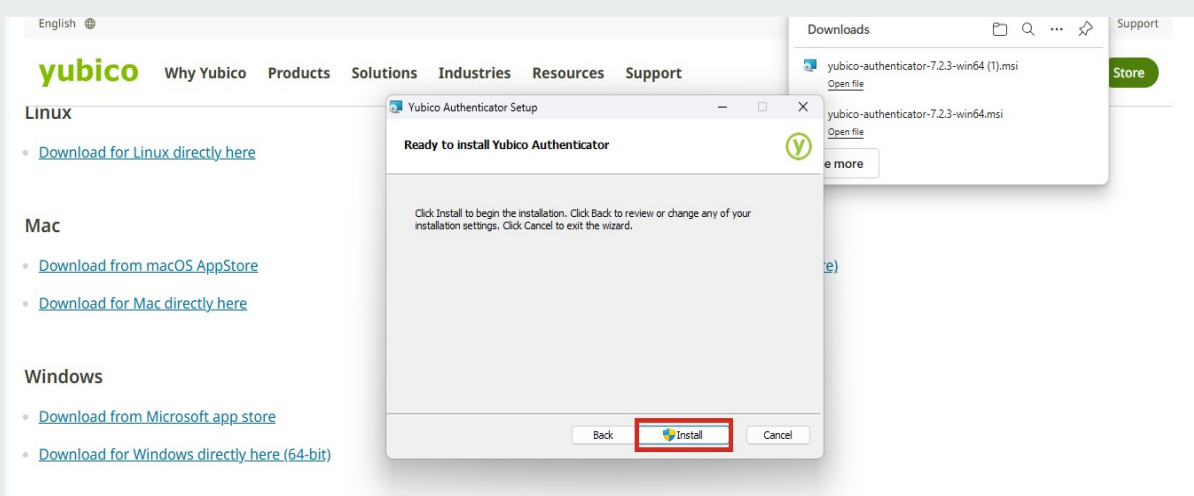
Use the default Destination Folder and Click Next.



A11

READY TO INSTALL

Click Install.

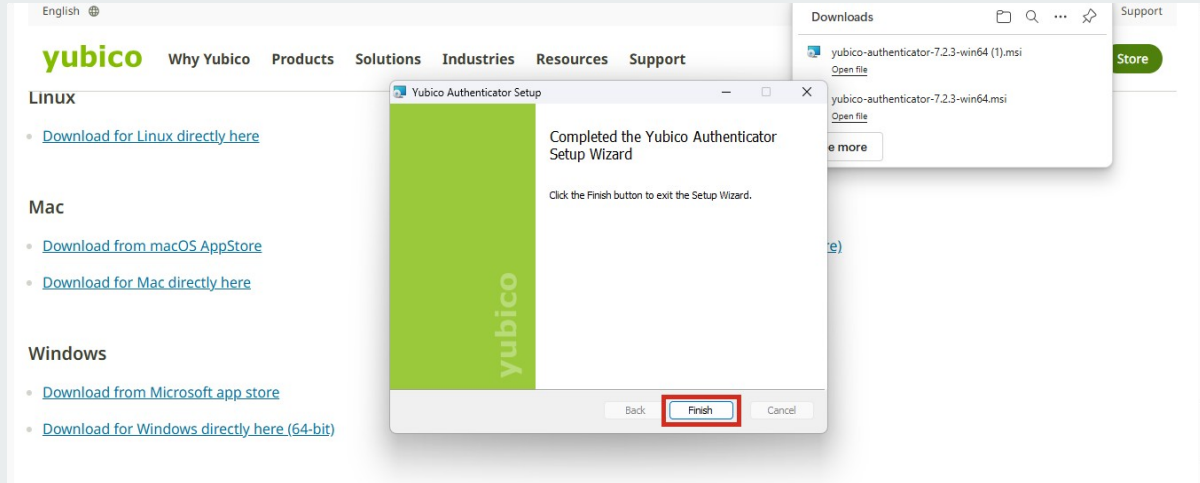


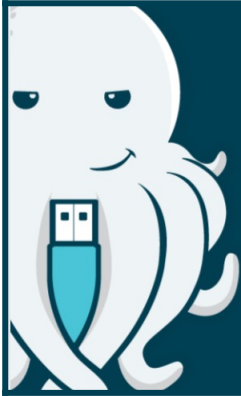
A12 PERMISSION TO MAKE CHANGES

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

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.

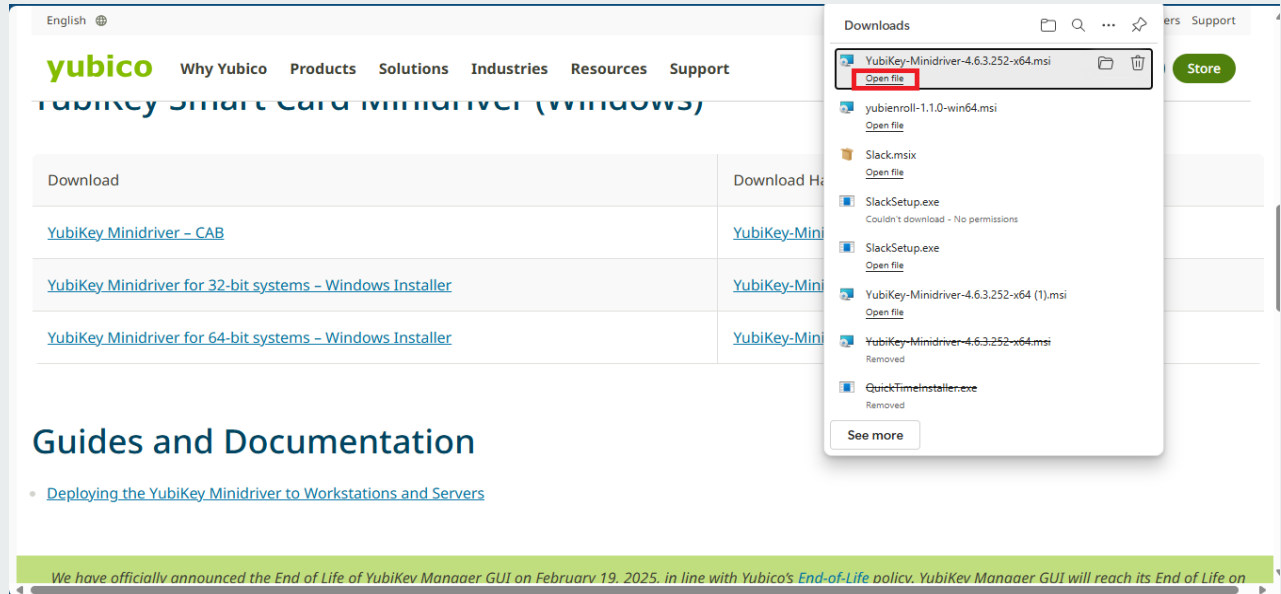
YubiKey Smart Card Minidriver (Windows)

Download	Download Hash
YubiKey Minidriver - CAB	YubiKey-Minidriver-4.6.3.252.cab.sha256
YubiKey Minidriver for 32-bit systems - Windows Installer	YubiKey-Minidriver-4.6.3.252-x86.msi.sha256
YubiKey Minidriver for 64-bit systems - Windows Installer	YubiKey-Minidriver-4.6.3.252-x64.msi.sha256

B3

OPENING THE YUBIKEY MINIDRIVER FILE

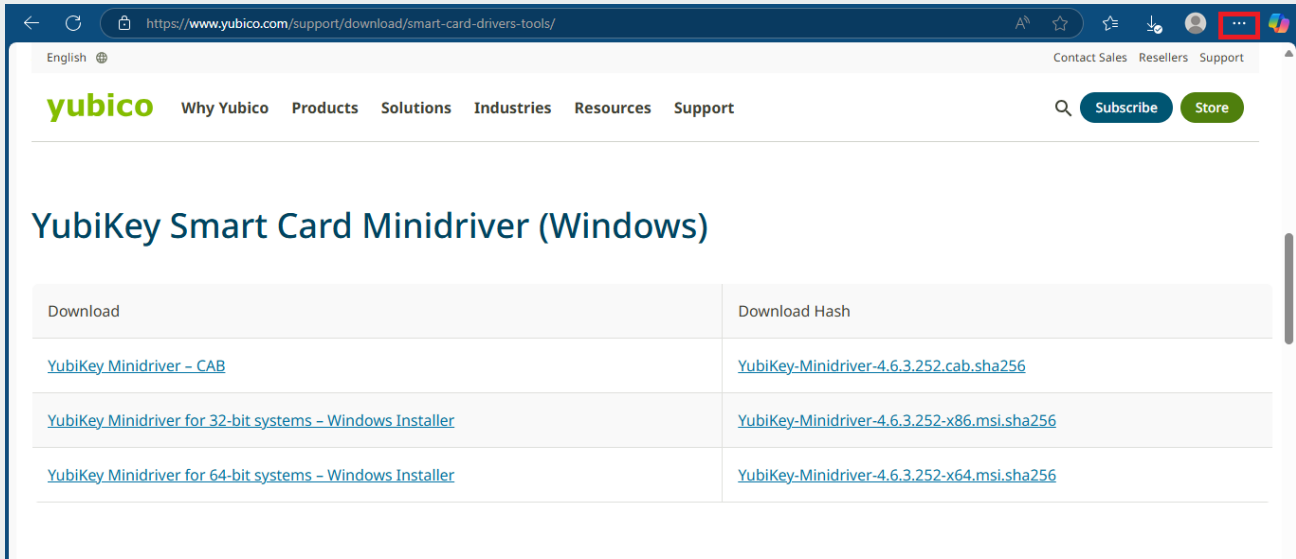
After clicking the download link, Edge browser will display a pop-up confirming the Minidriver file has been successfully downloaded and ready for installation. Click the open file link.



B4

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.



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

The screenshot shows the Yubico website with a browser's drop-down menu open. The 'Downloads' option is highlighted with a red box. The website content includes the Yubico logo, navigation links, and a table of download links for the YubiKey Smart Card Minidriver (Windows).

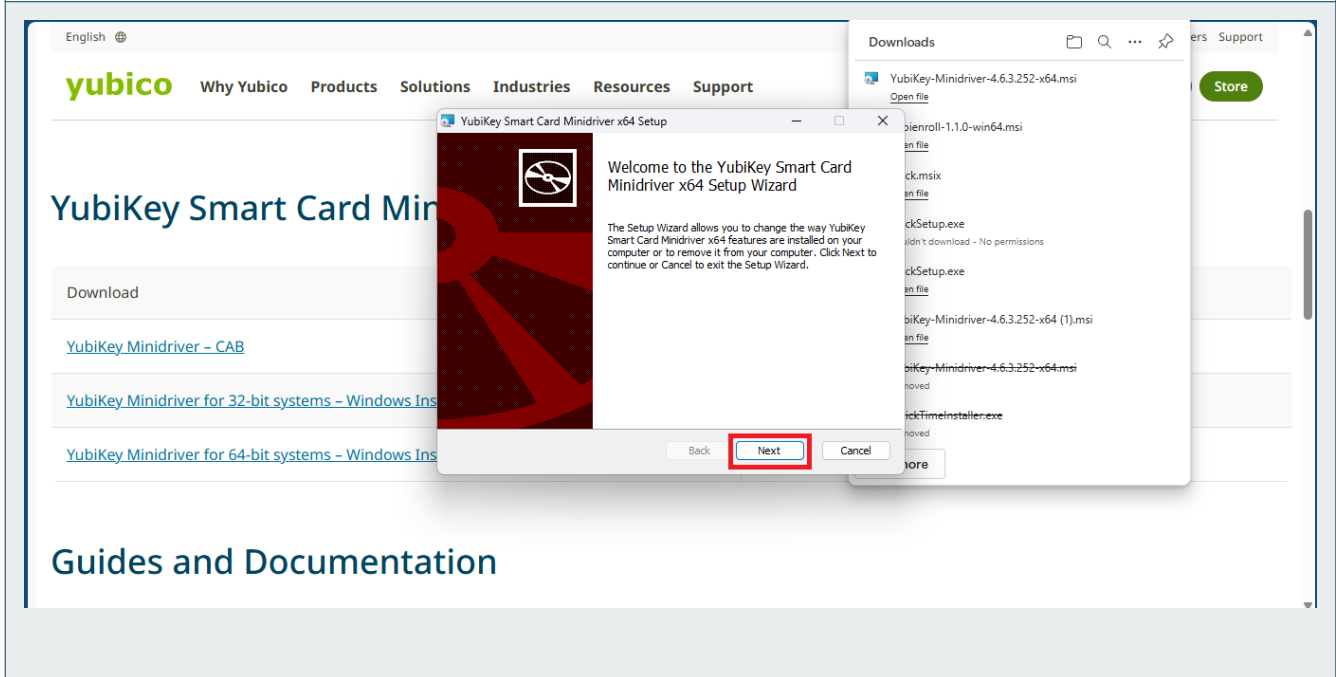
Download	Download Hash
YubiKey Minidriver - CAB	YubiKey-Minidriver-4.6.3.2
YubiKey Minidriver for 32-bit systems - Windows Installer	YubiKey-Minidriver-4.6.3.2
YubiKey Minidriver for 64-bit systems - Windows Installer	YubiKey-Minidriver-4.6.3.2

Guides and Documentation

B6

INSTALLING THE YUBIKEY MINIDRIVER

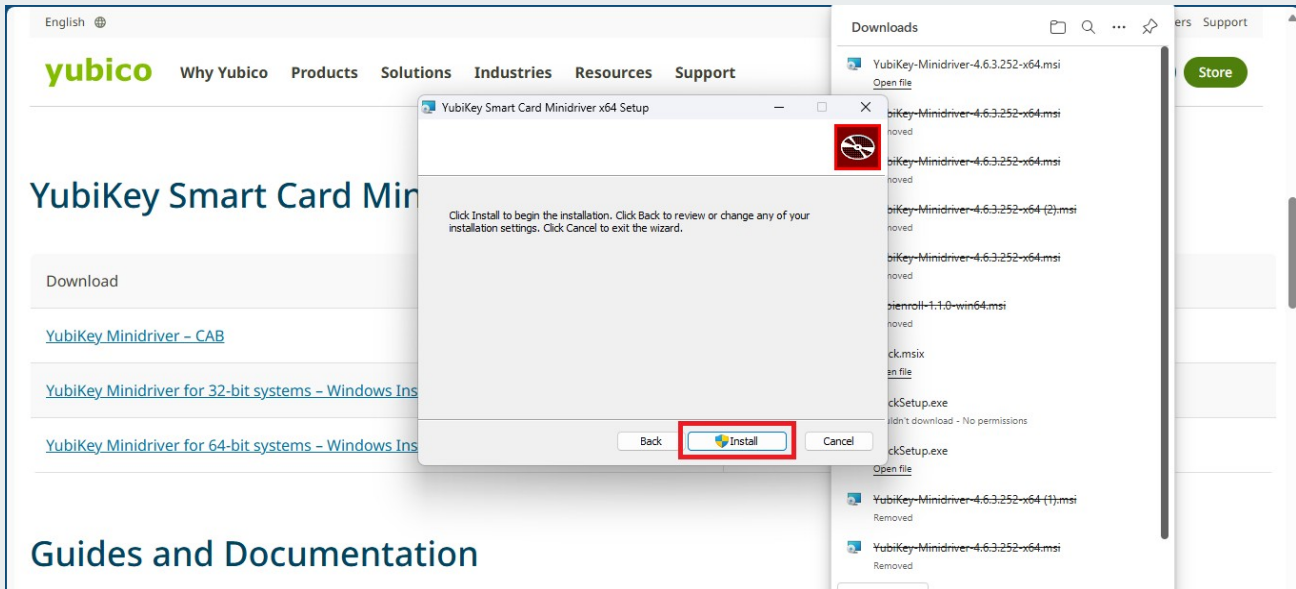
A Setup Wizard pop-up will open – Click **Next**.



B7

CONTINUE INSTALLING THE YUBIKEY MINIDRIVER

On the next pop-up window – Click Install.



B8

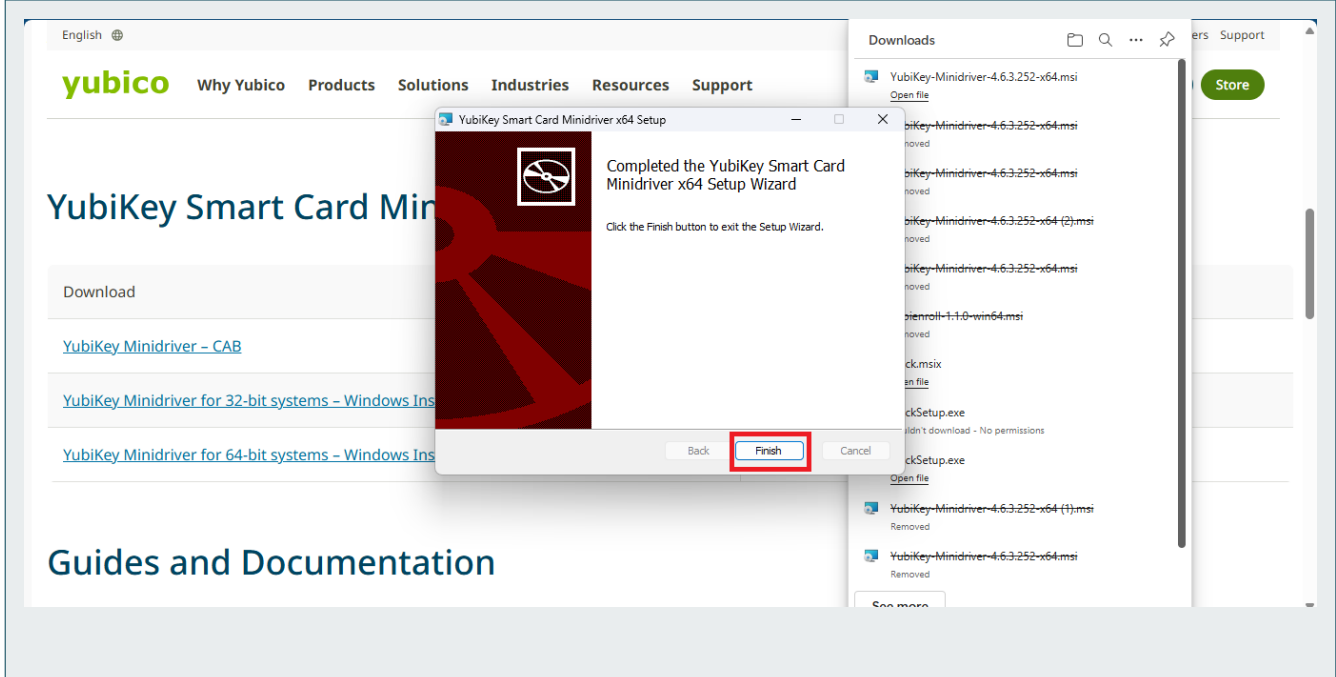
PERMISSION TO MAKE CHANGES

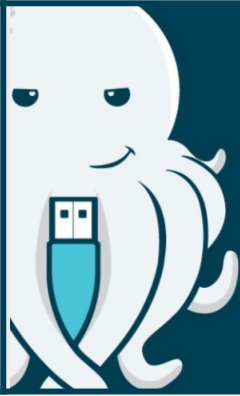
The next pop-up message will ask permission to allow the application to make changes on your computer. Click YES.



FINISH THE INSTALL

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





SECTION C

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

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)

The screenshot shows the StrongKey website interface. At the top, the StrongKey logo is displayed. Below it, a welcome message reads: "Welcome to the StrongKey Tellaro Small Business Security Bundle (SB2)". A sub-header states: "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".

On the left side, there is a section titled "SB2 Production CA Certificates" enclosed in a red-bordered box. It contains three blue buttons with red download icons: "Download Root CA", "Download Sub CA 1", and "Download Sub CA 2". A lightbulb icon is positioned to the right of these buttons.

On the right side, there is a section titled "How To Configure CA Certificates". It is divided into two sub-sections: "Swissbit Security Keys" and "Yubikey Security Keys".

Under "Swissbit Security Keys", there are three rows of buttons. The first row is labeled "HTML:" and has buttons for "Windows 10", "Windows 11", and "macOS". The second row is labeled "PDF:" and has buttons for "Windows 10", "Windows 11", and "macOS". The third row is labeled "Video:" and has buttons for "Windows 10", "Windows 11", and "macOS".

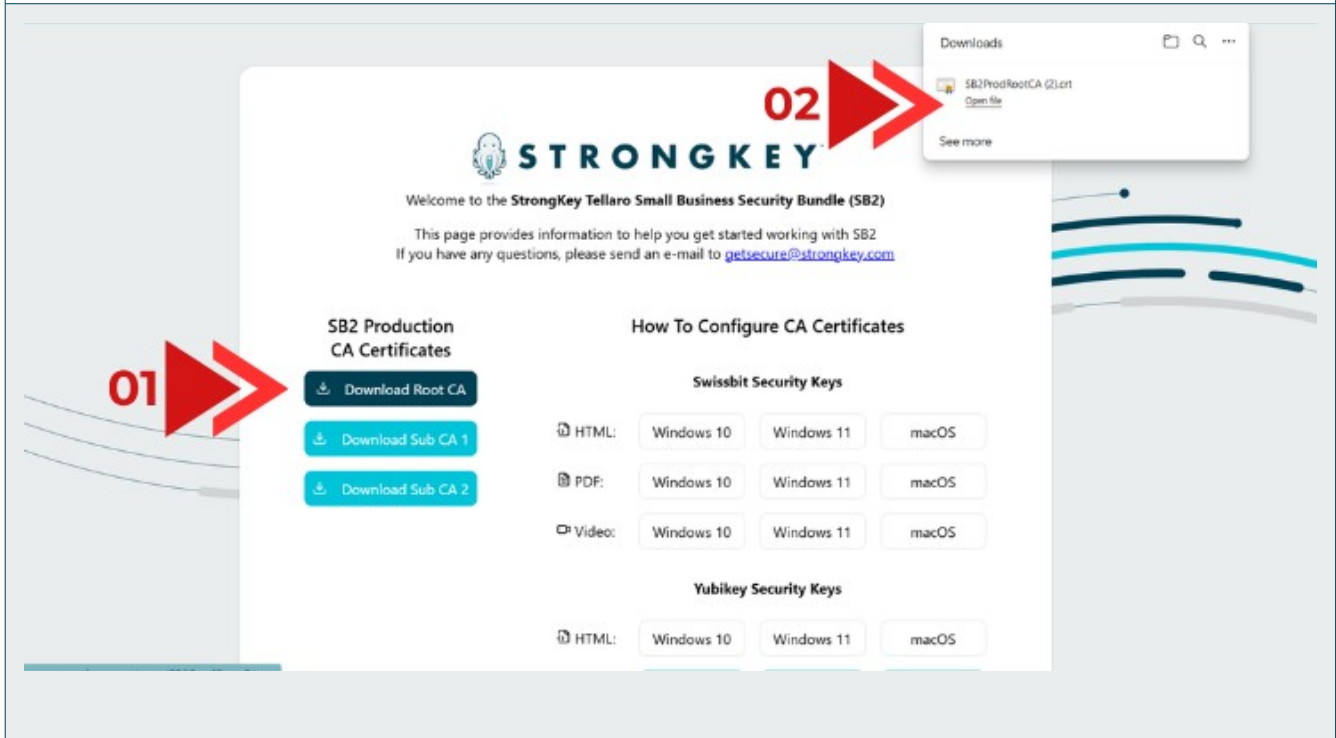
Under "Yubikey Security Keys", there is one row labeled "HTML:" with buttons for "Windows 10", "Windows 11", and "macOS".

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.



C5

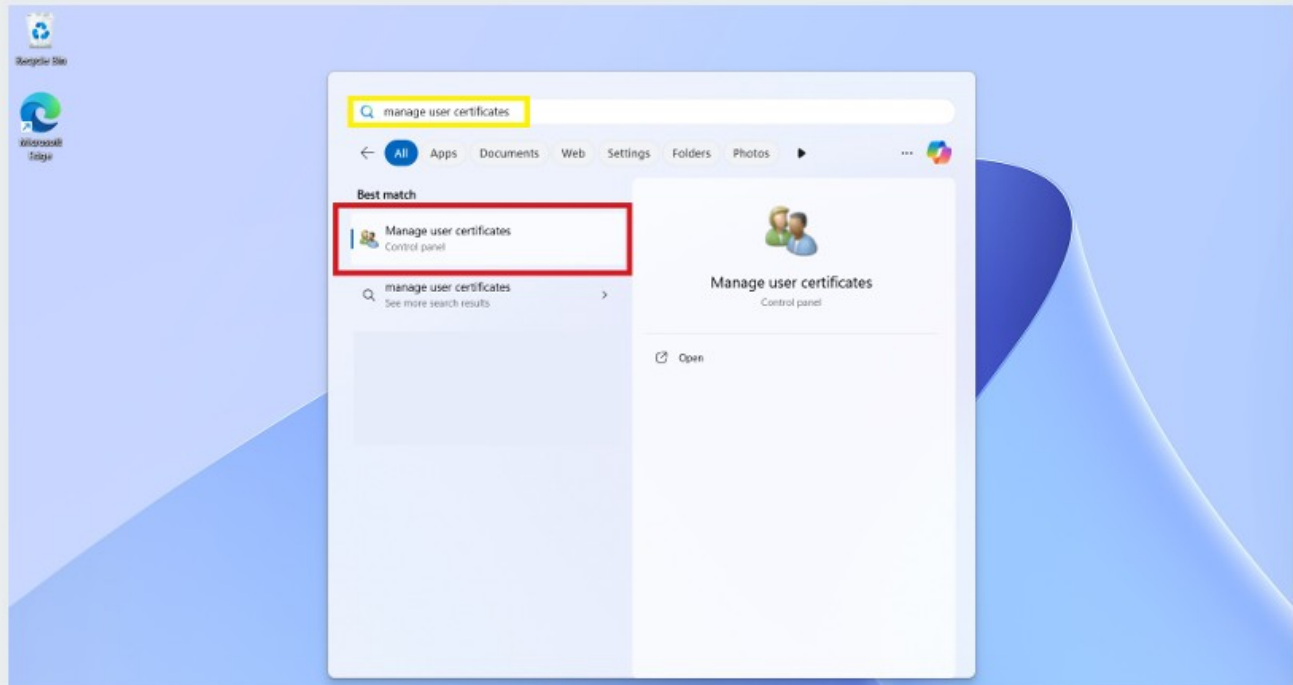
NAVIGATE TO THE WINDOWS START ICON

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.

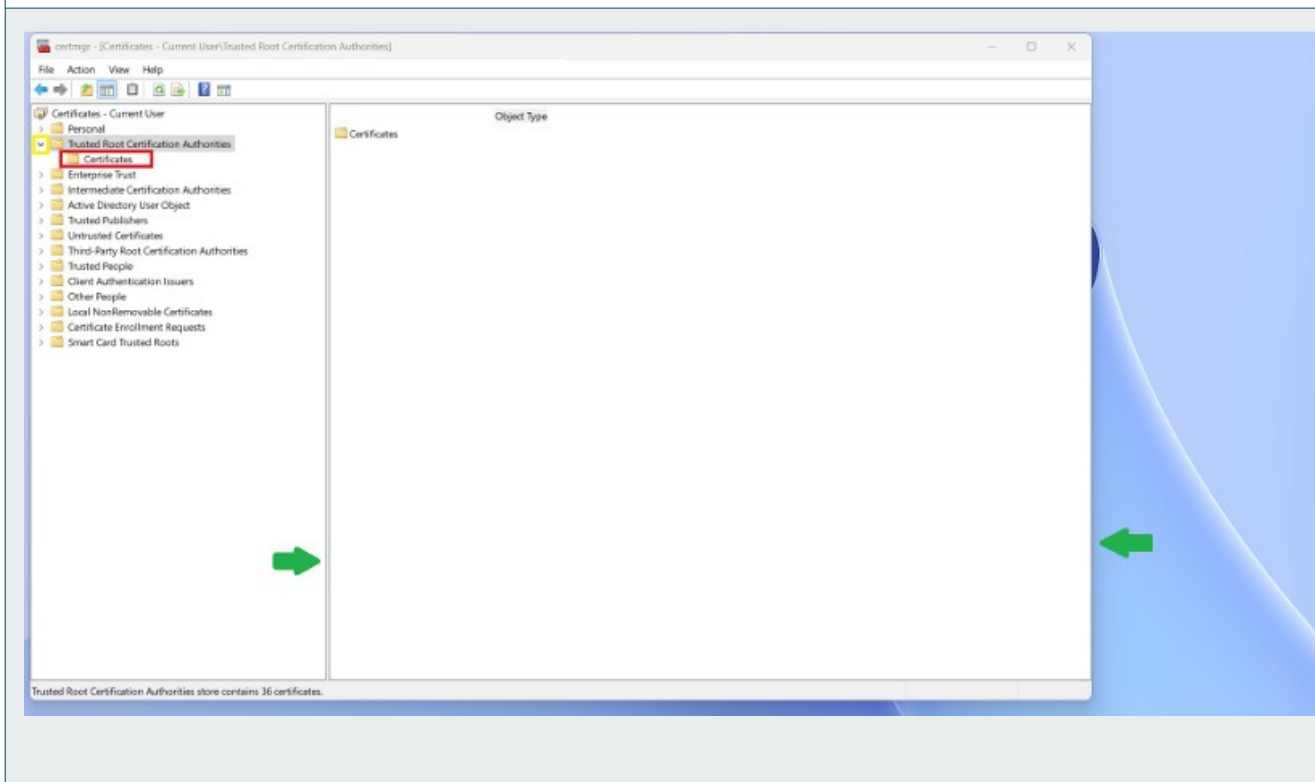


C6

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.

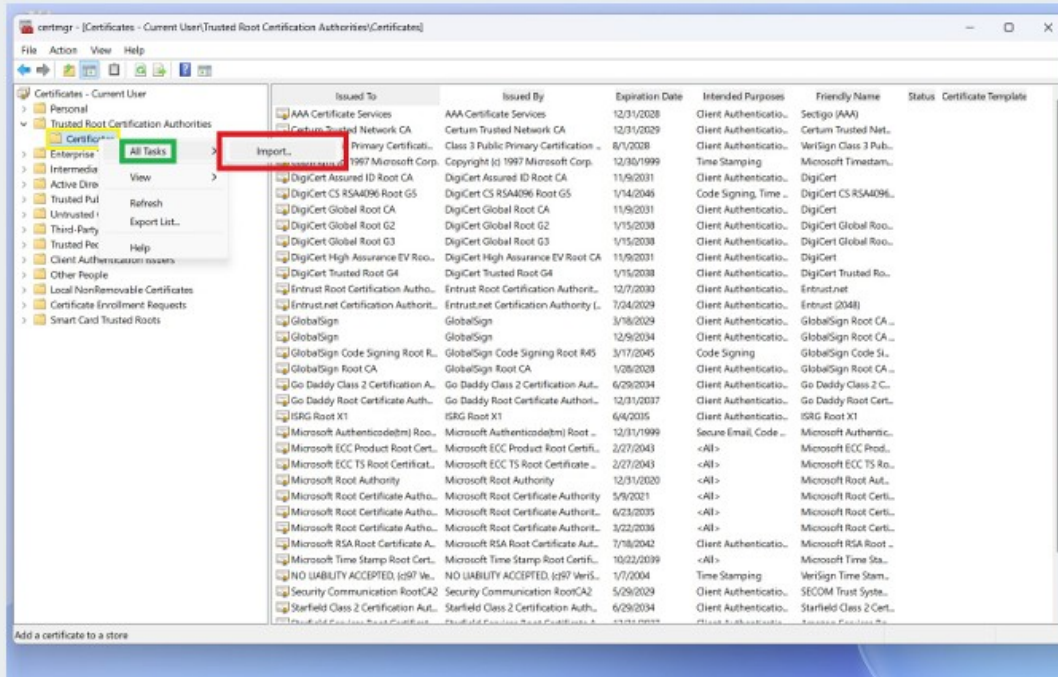


C7

INITIATE THE SB2 ROOT CERTIFICATE IMPORT

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

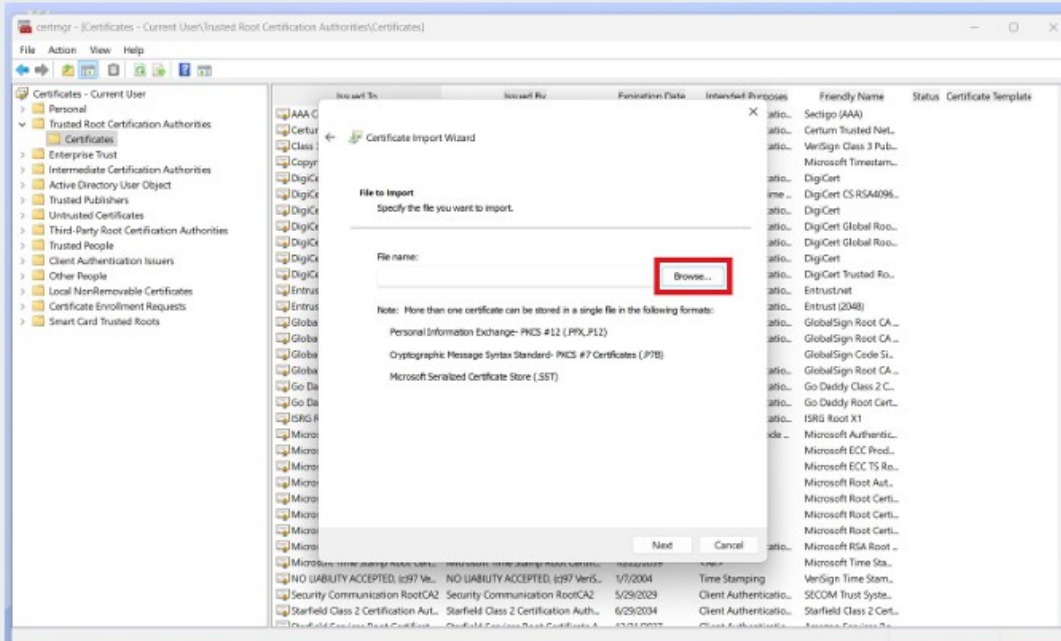
Select **All Tasks**, and click **Import** to start the Certificate Import Wizard.





LOCATE THE SB2 ROOT CA CERTIFICATE

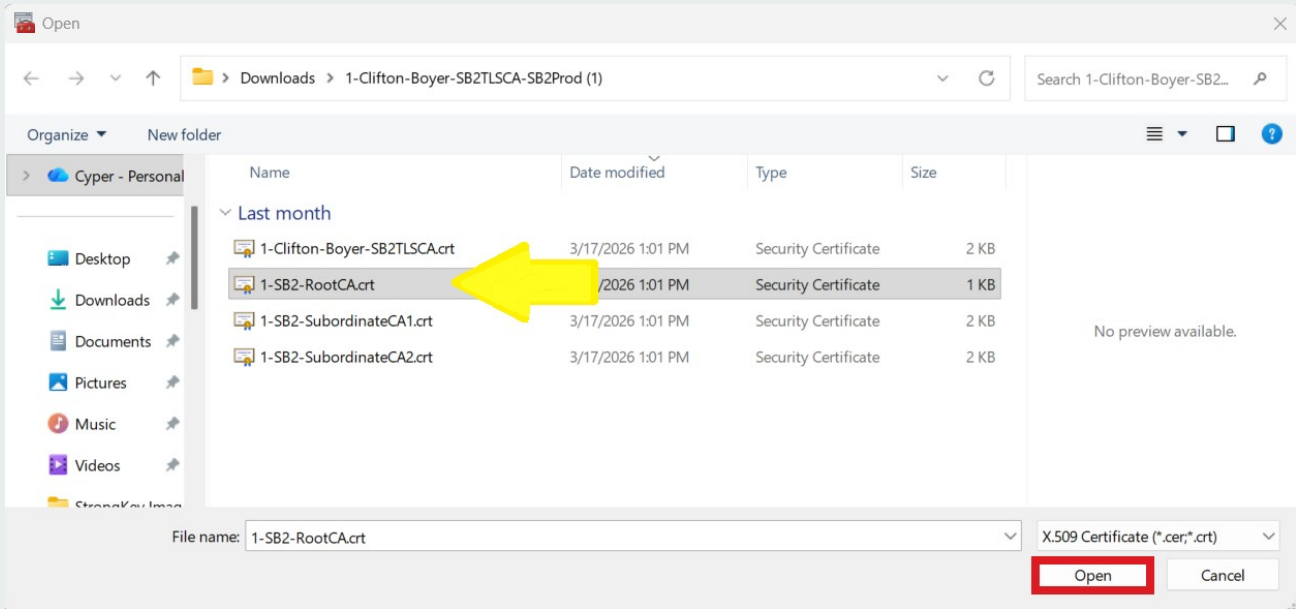
Click the **Browse** button to locate the SB2 Root CA certificate file.





OPEN THE SB2 ROOT CA CERTIFICATE

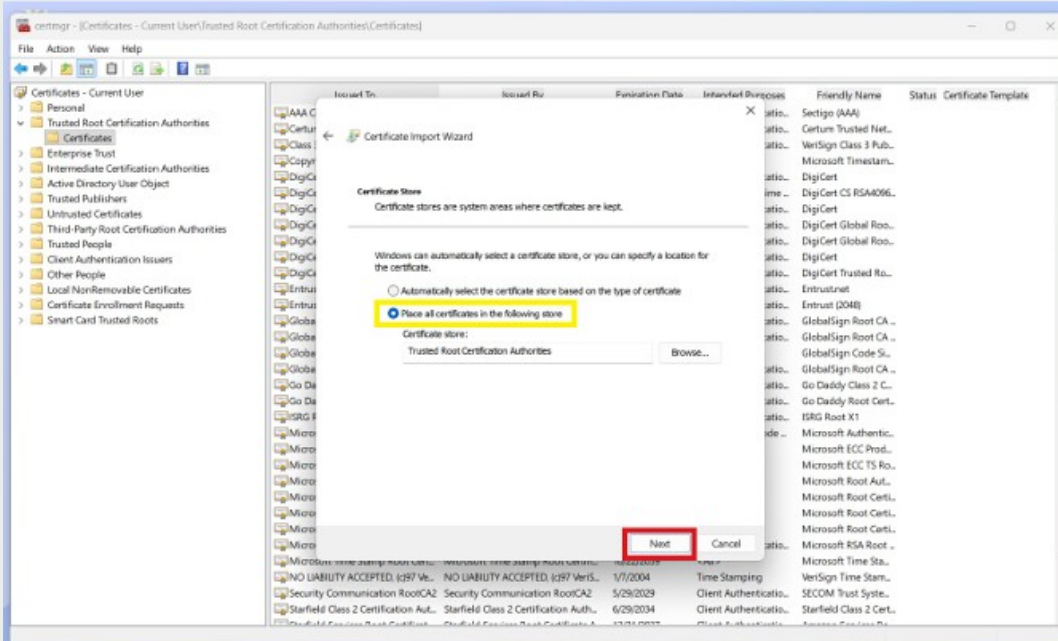
To find the SB2 Root CA Certificate, go to the **SB2ProdRootCA.crt** file's location, which is typically the **Downloads** folder. Once the **SB2ProdRootCA.crt** is located, select it and **click Open**.





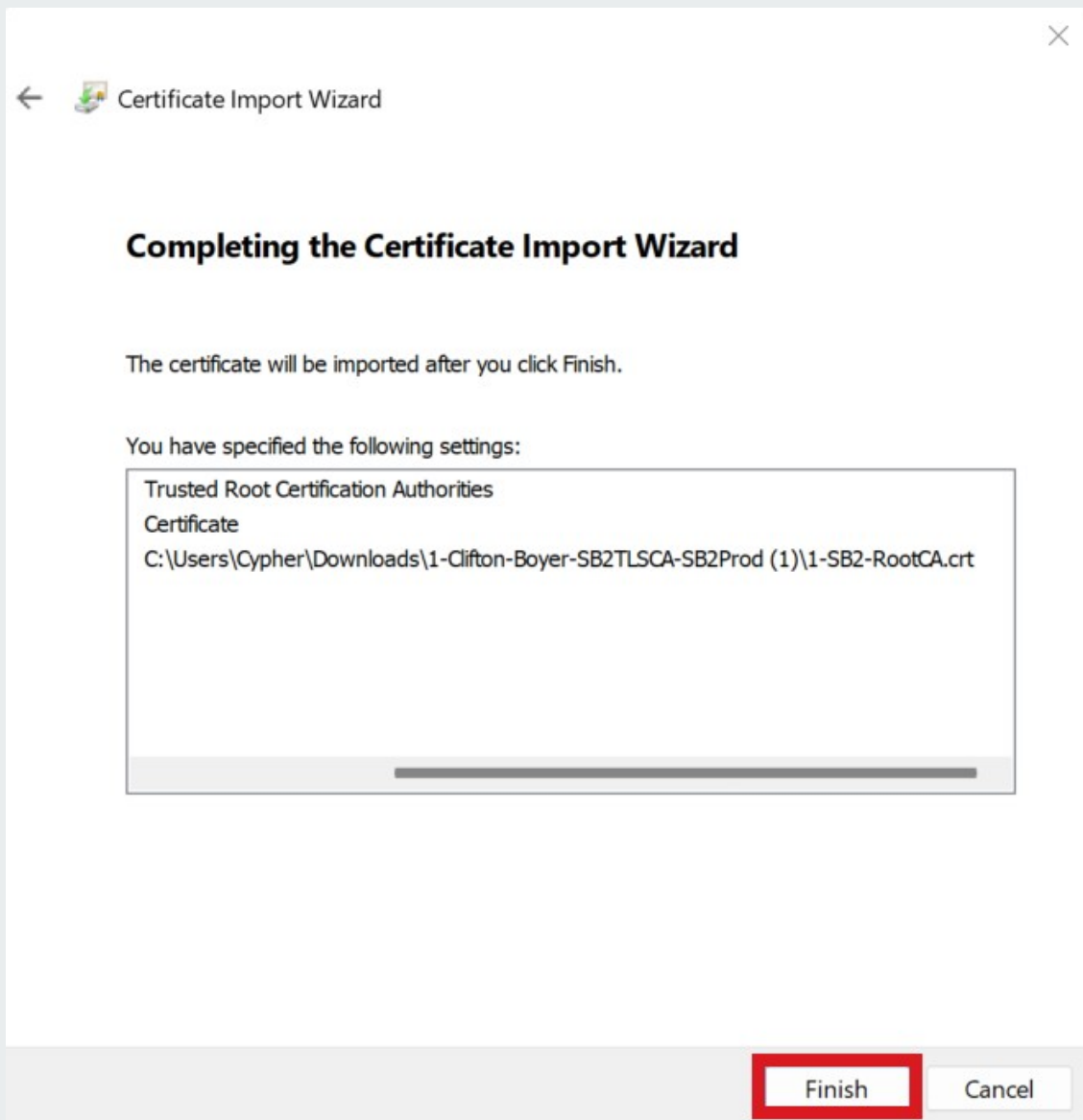
SELECT CERTIFICATE STORE

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.



C13 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.

The screenshot shows the Windows Certificate Manager window with a security warning dialog box overlaid. The dialog box contains the following text:

Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

SB2 RootCA

Windows cannot validate that the certificate is actually from "SB2 RootCA". You should confirm its origin by contacting "SB2 RootCA". The following number will assist you in this process:

Thumbprint (sha1) 6DCFFF6D D5B73DF9 26511DB6 9D0B4914 F1649542

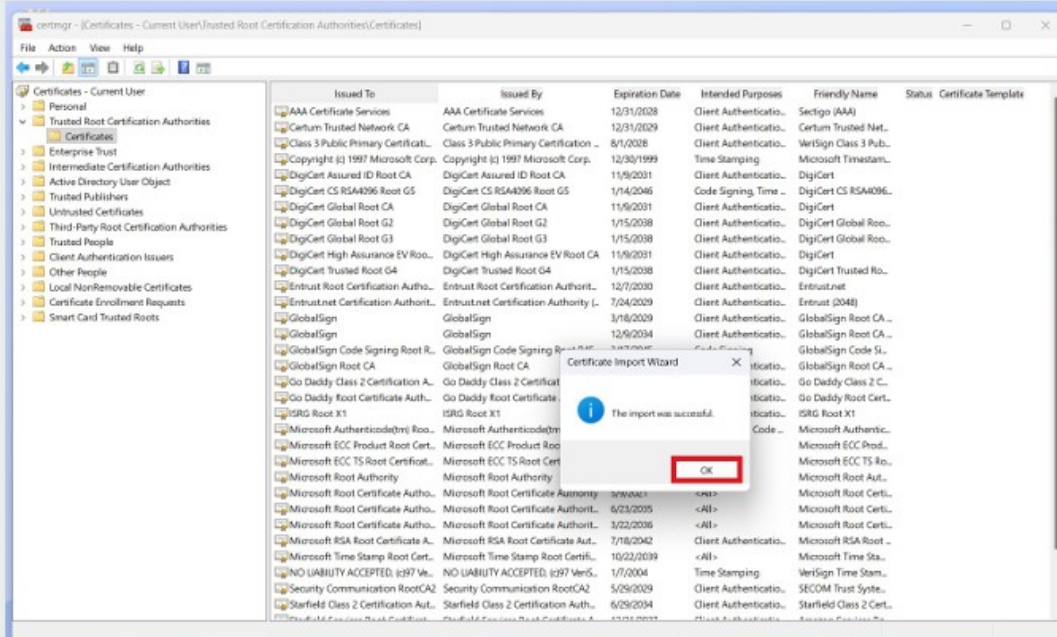
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

At the bottom of the dialog box, there are two buttons: **Yes** and **No**. The **Yes** button is highlighted with a red box.

C14

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

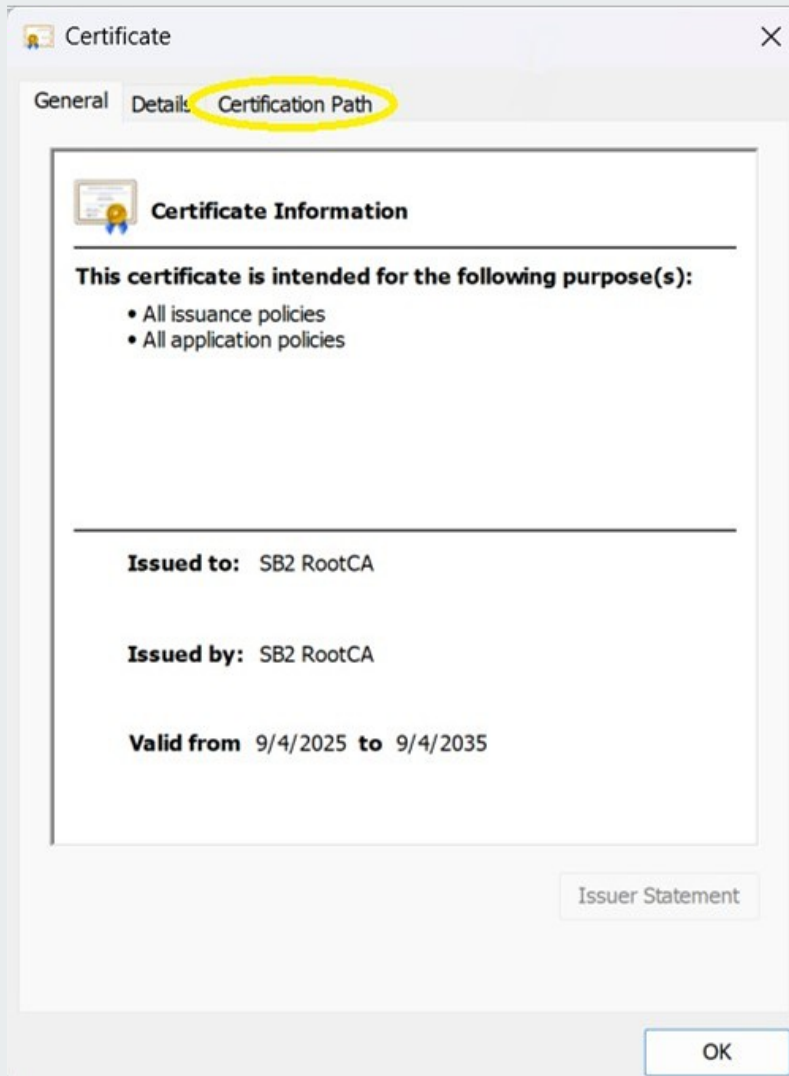
If you scroll down the list of CA certificates on the right-hand side of this window's panel, you will see the **SB2 RootCA** certificate in the list.

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 Autho...	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 Authority...	6/23/2035	<All>	Microsoft Root Certi...		
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authority...	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...		
NO LIABILITY ACCEPTED, (c97) Ve...	NO 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		

C16

VERIFY SB2 ROOT CA: PART 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:



C17

VERIFY SB2 ROOT CA: PART 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:

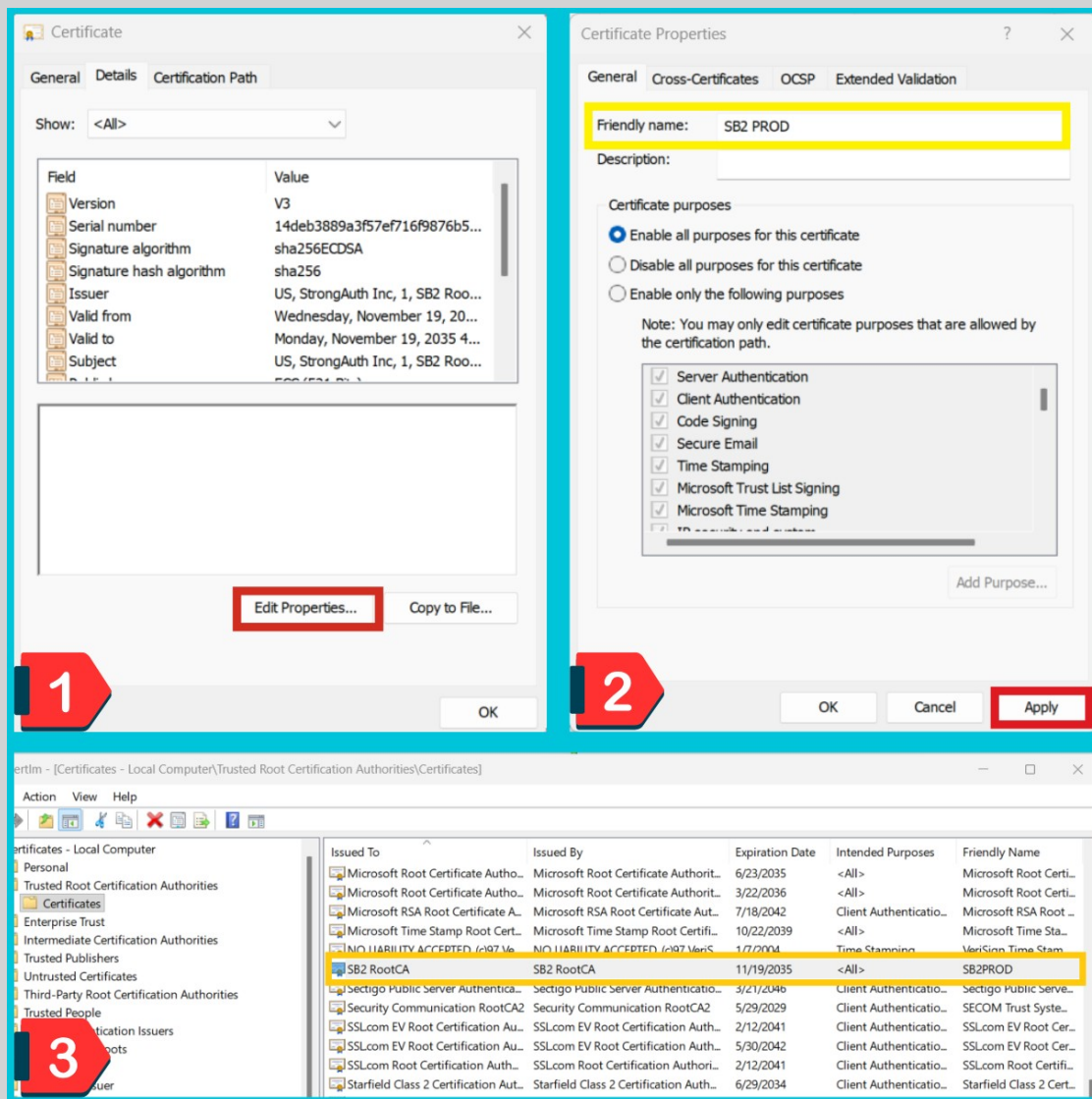
- That the certificate symbol in the **Certification Path** sub-panel at the top does not have any yellow warning symbol associated with it, and
- The **Certificate status** sub-panel at the bottom should state that “This certificate is OK.”



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).

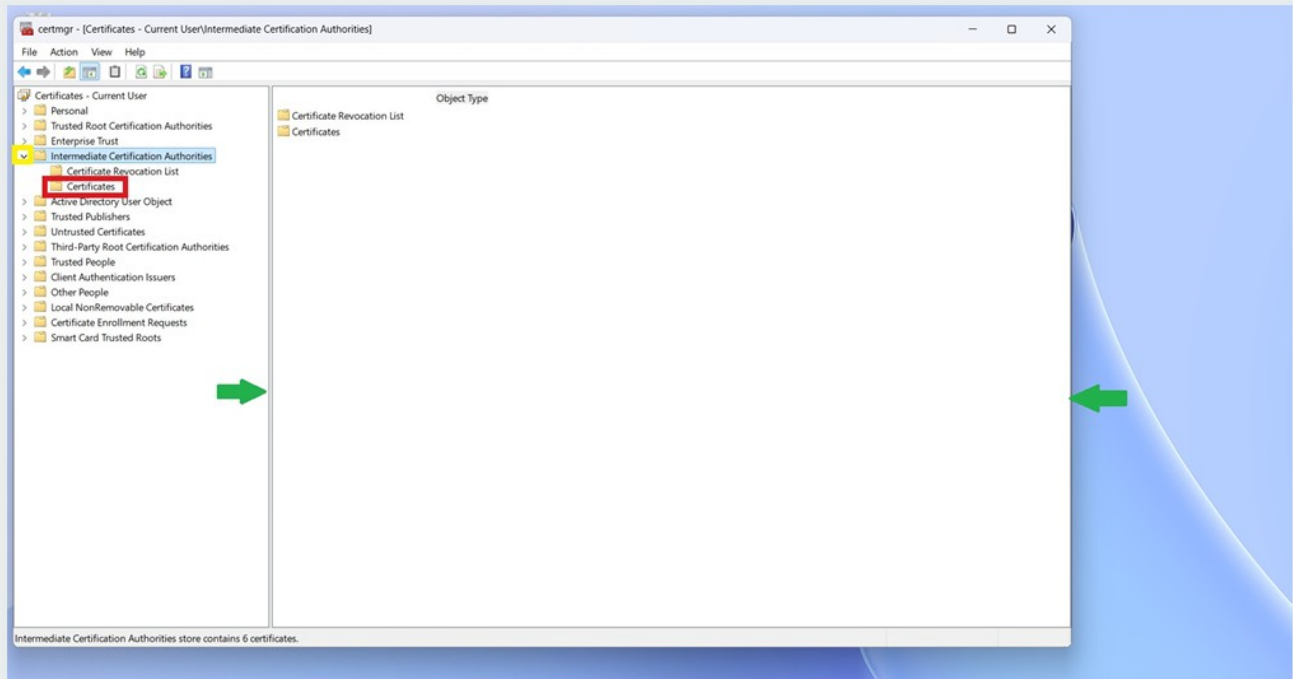


C19

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.

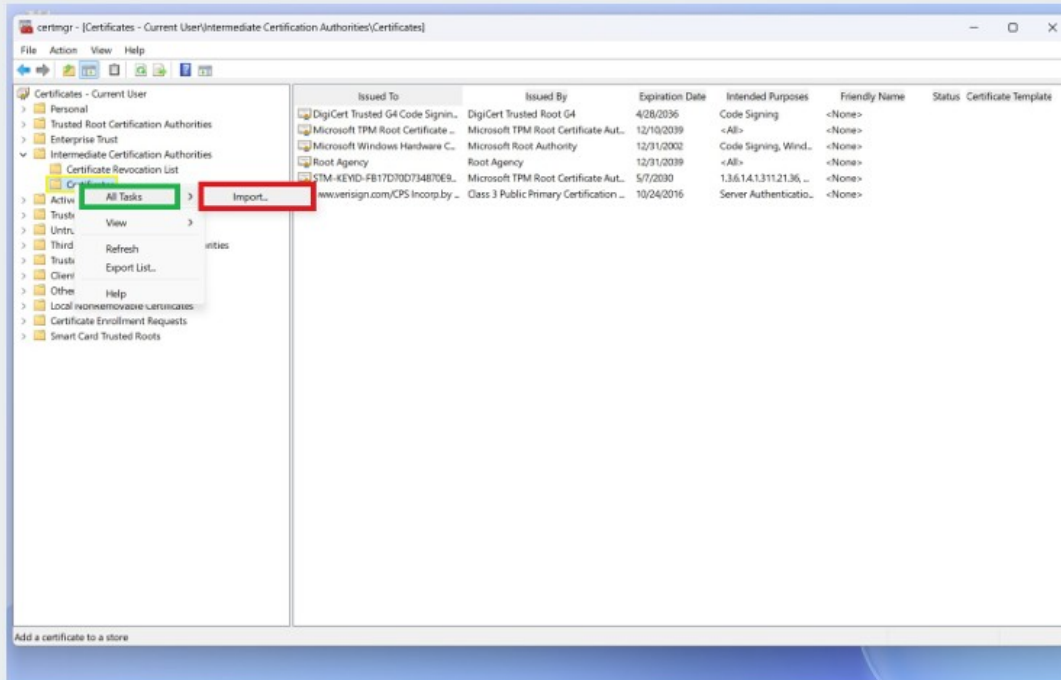
Return to the **certmgr** application. Next, click the **arrow** (yellow box) next to the **Intermediate Certification Authorities** folder to expand it, revealing the **Certificates** (red box) folder.





INITIATING THE SB2 SUBORDINATE CA CERTIFICATE IMPORT

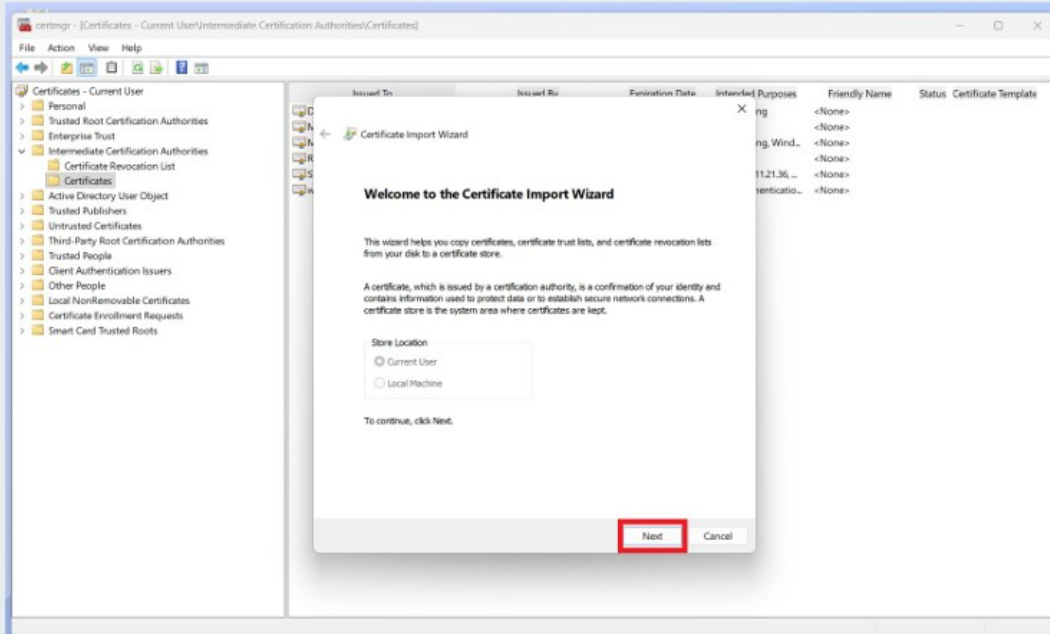
To begin, right-click the **Certificates** folder to open the context menu. From there, select **All Tasks**, and then click **Import** to start the **Certificate Import Wizard**.





CERTIFICATE IMPORT WIZARD

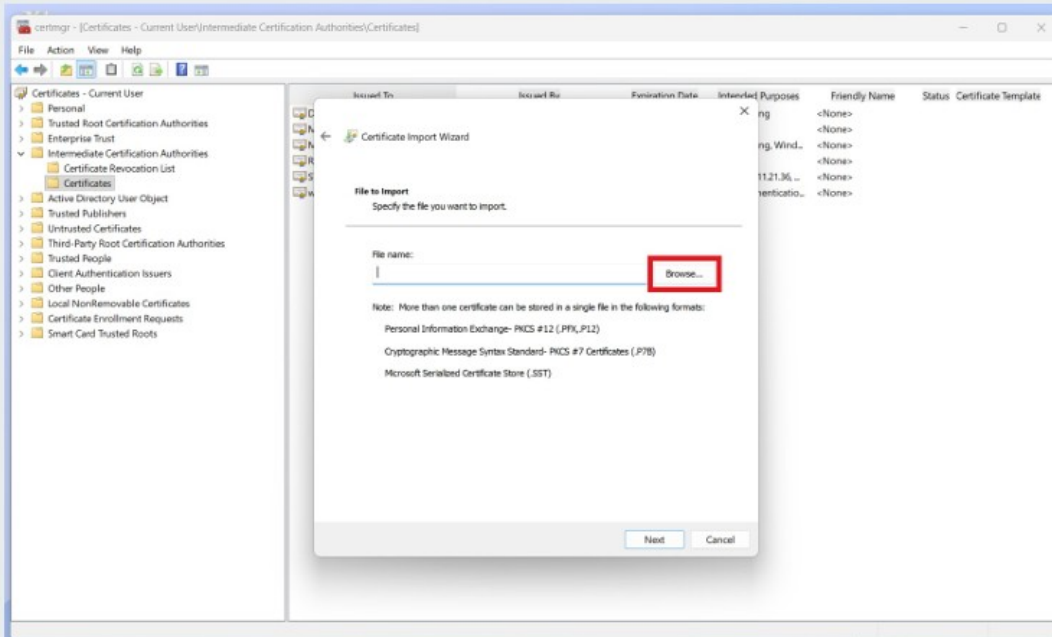
The Certificate Import Wizard will open. Click **Next** to proceed.





LOCATE SUBORDINATE SB2 CA 1 CERTIFICATE FOR IMPORTING

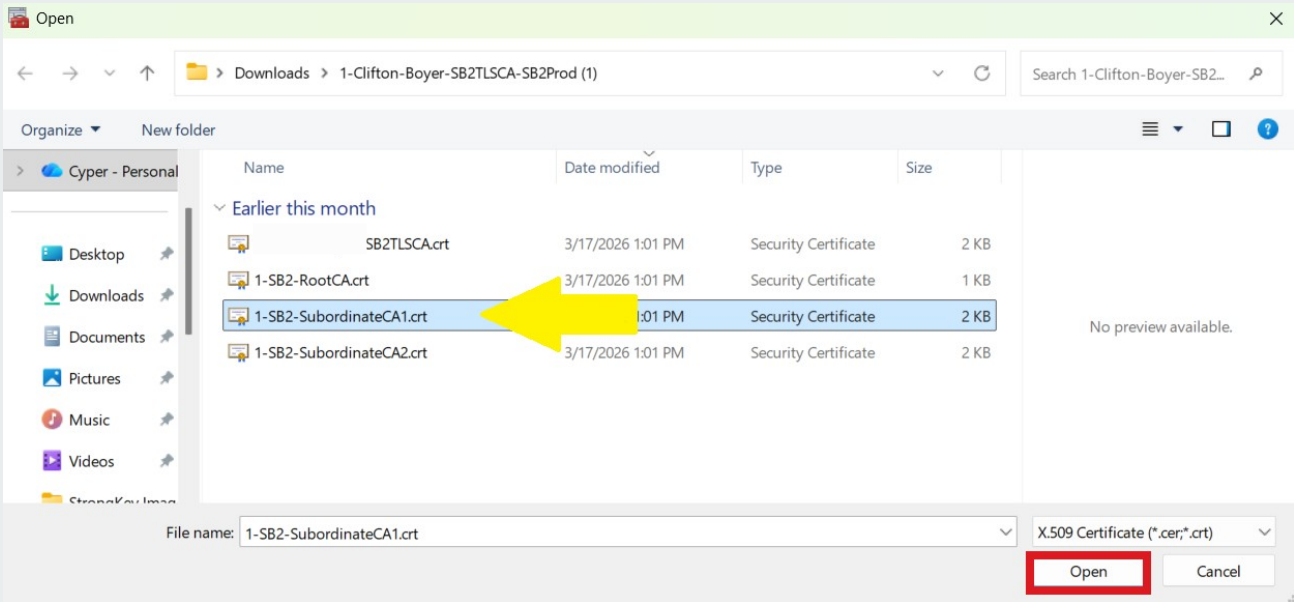
Click the "Browse" button to navigate to and select the Subordinate CA certificate file.





OPEN THE SUBORDINATE SB2PROD CA 1 CERTIFICATE

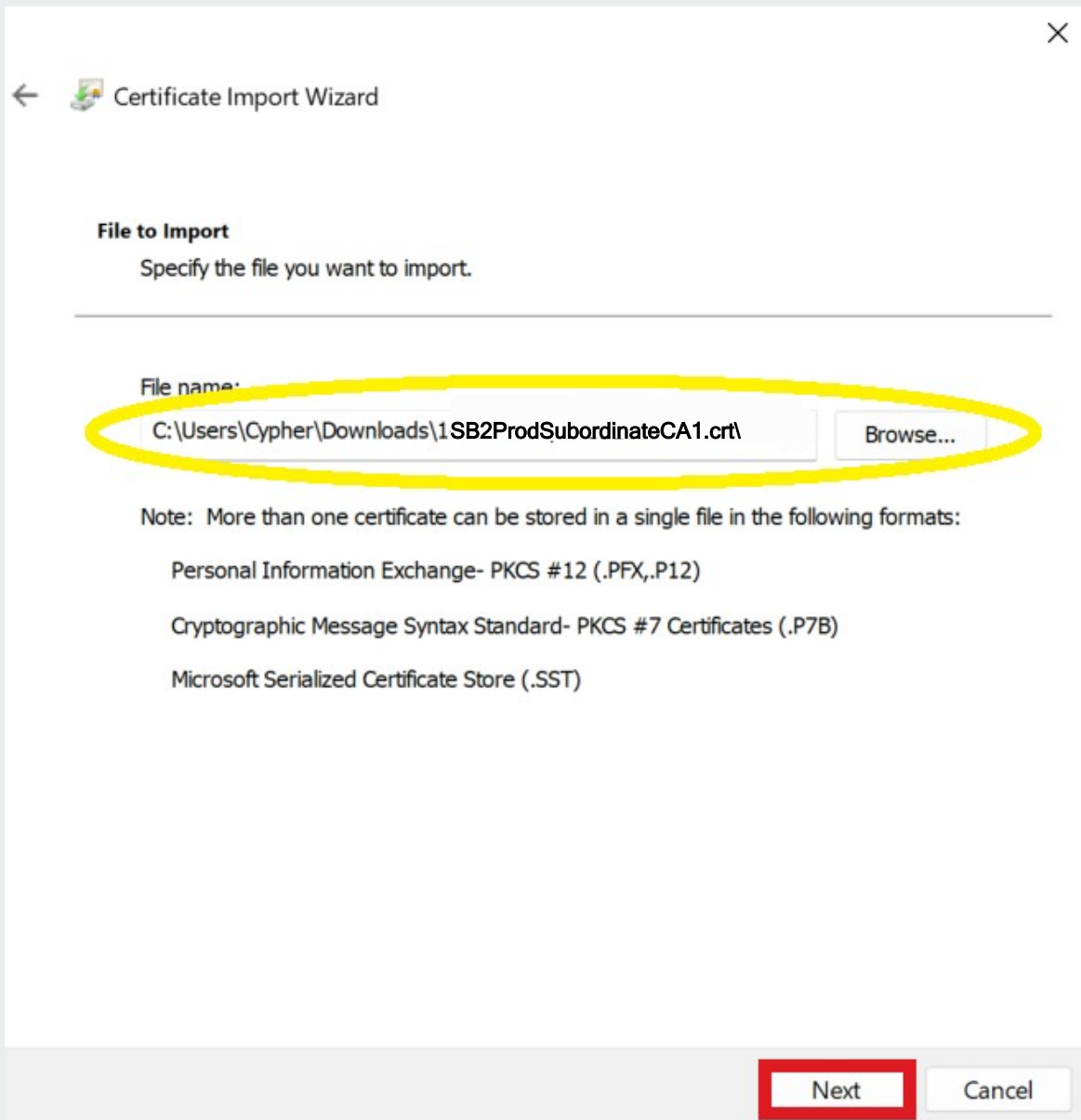
To find the SB2ProdSubordinateCA1.crt certificate file, go to the file's location, which is typically the Downloads folder. Once the SB2ProdSubordinateCA1.crt file (yellow arrow) is located, select it and click Open.





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.

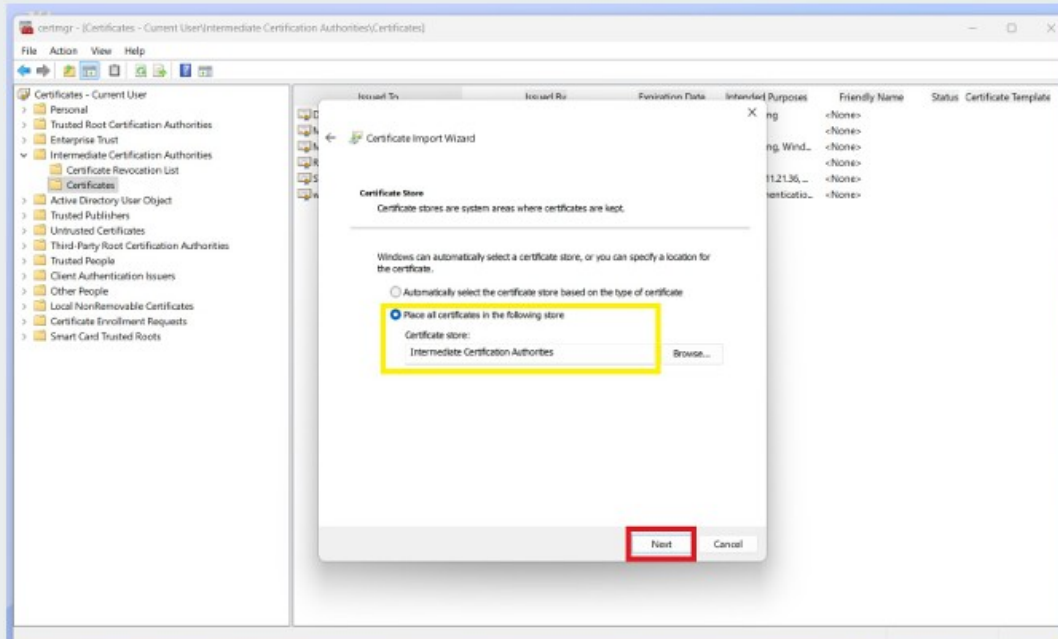


The screenshot shows a 'Certificate Import Wizard' dialog box. The title bar includes a back arrow, a folder icon, and the text 'Certificate Import Wizard'. The main area is titled 'File to Import' with the instruction 'Specify the file you want to import.' Below this is a 'File name:' label and a text 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, a 'Note' states: 'More than one certificate can be stored in a single file in the following formats: 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, there are two buttons: 'Next' (highlighted with a red box) and 'Cancel'.



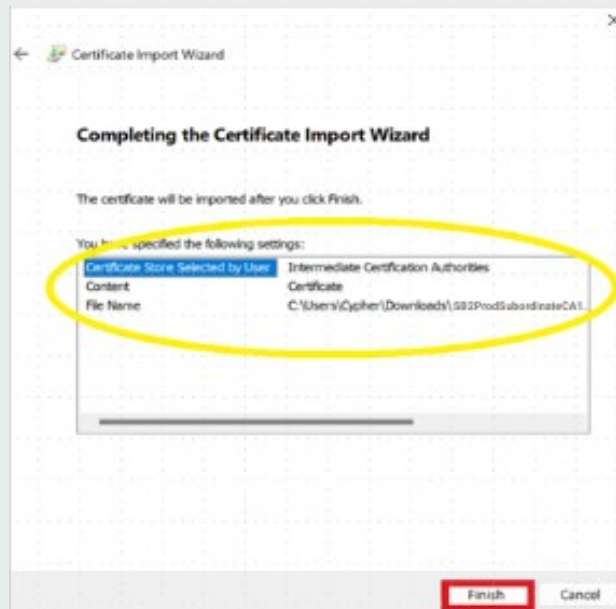
SELECTING CERTIFICATE STORE

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.



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.





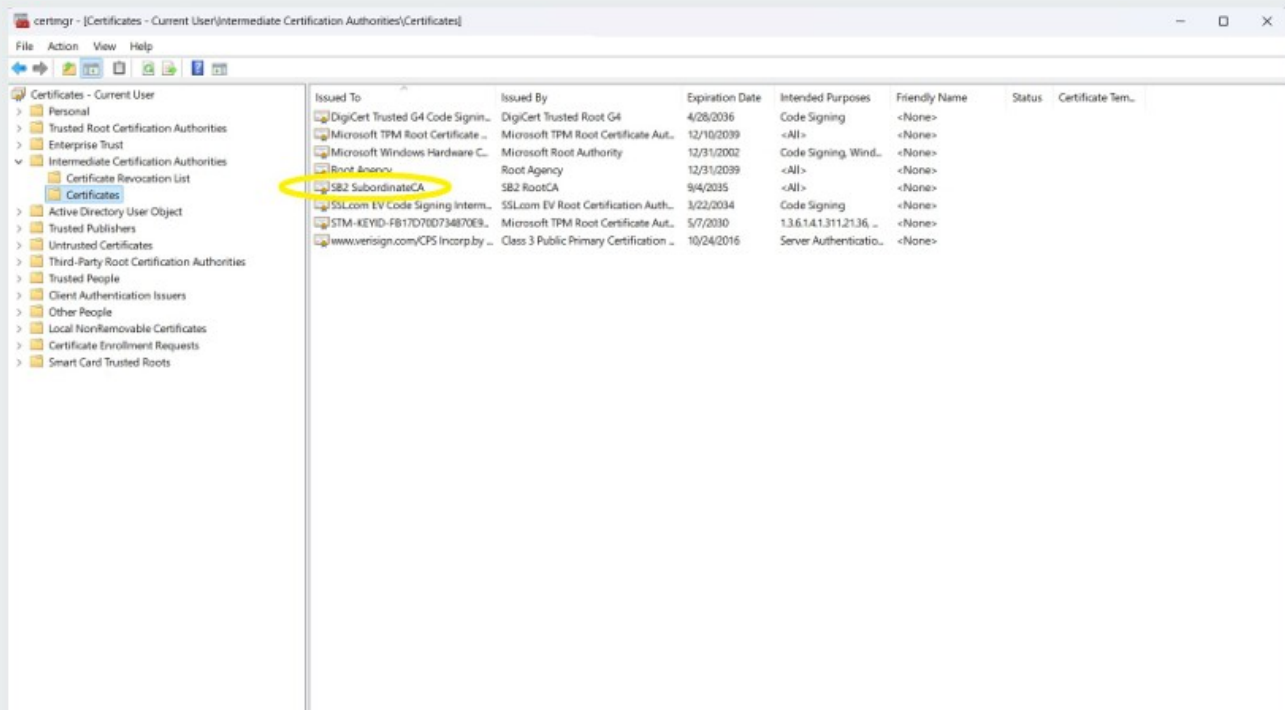
A SUCCESSFUL IMPORT

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

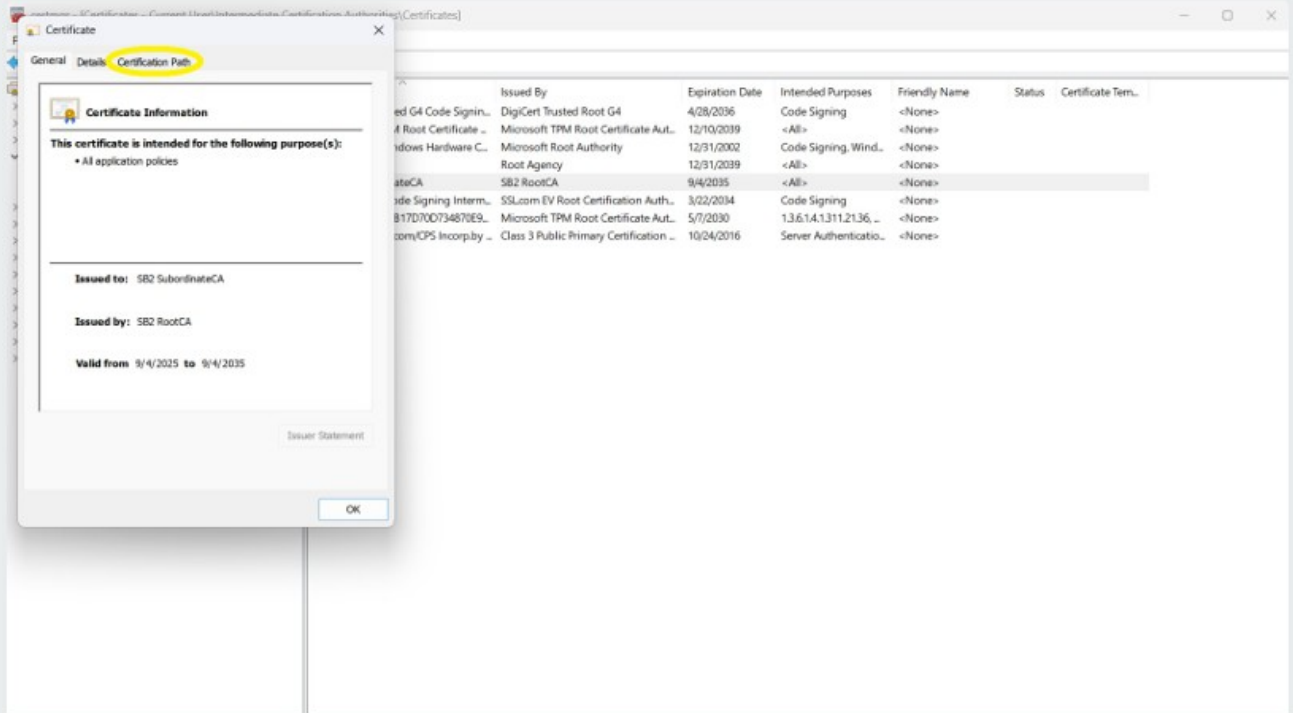
After the SB2 Subordinate CA 1 Certificate has been successfully imported, it will appear in the Intermediate Certification Authorities list as illustrated below:





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:

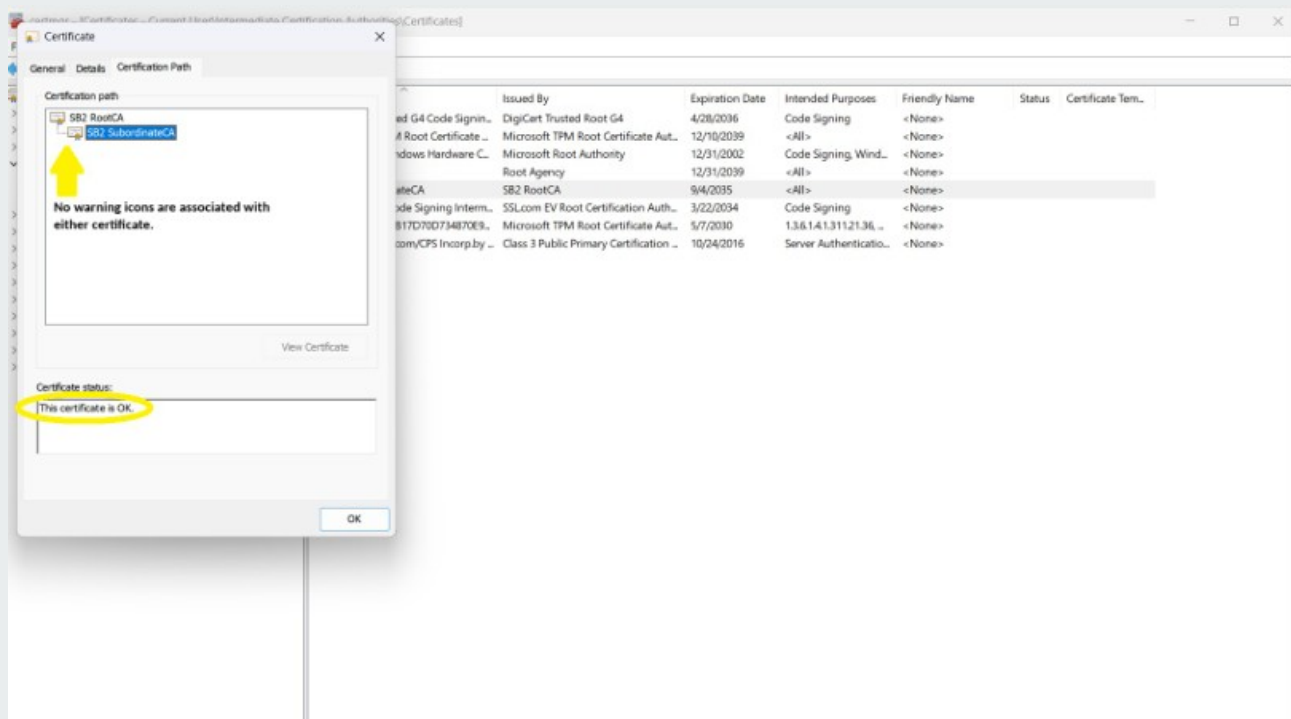


C30

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.”

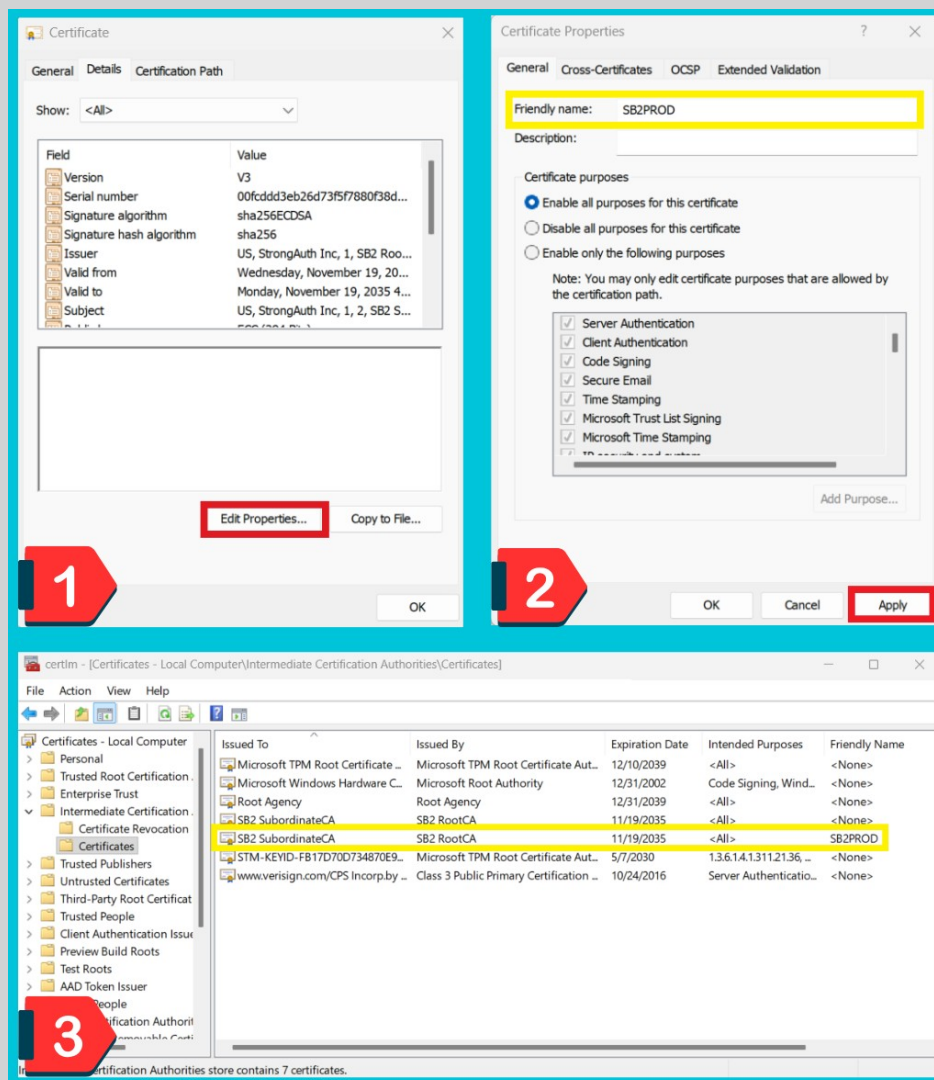


VERIFY SB2 SUBORDINATE CA 1: PART 3

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

It is important to follow these exact steps to restart your computer:

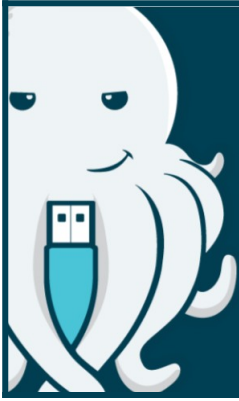
1. **Save** all open work and close all active applications to prevent data loss.
2. **Remove** the Security Key from the USB port.
3. Perform a **full Shut Down** of the computer (avoid "Sleep" or "Hibernate").
4. **Reinsert the Security Key** once the computer has completely powered down.
5. **Power on** the computer to allow the system to automatically find the Security Key and register the new certificates as it starts up.

NOTE



To ensure the operating system recognizes the newly imported digital certificates, you must remove and reinsert the Security Key. This action triggers a required firmware re-initialization to complete the certificate integration process.





SECTION D

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)

D3

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.



D4

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.

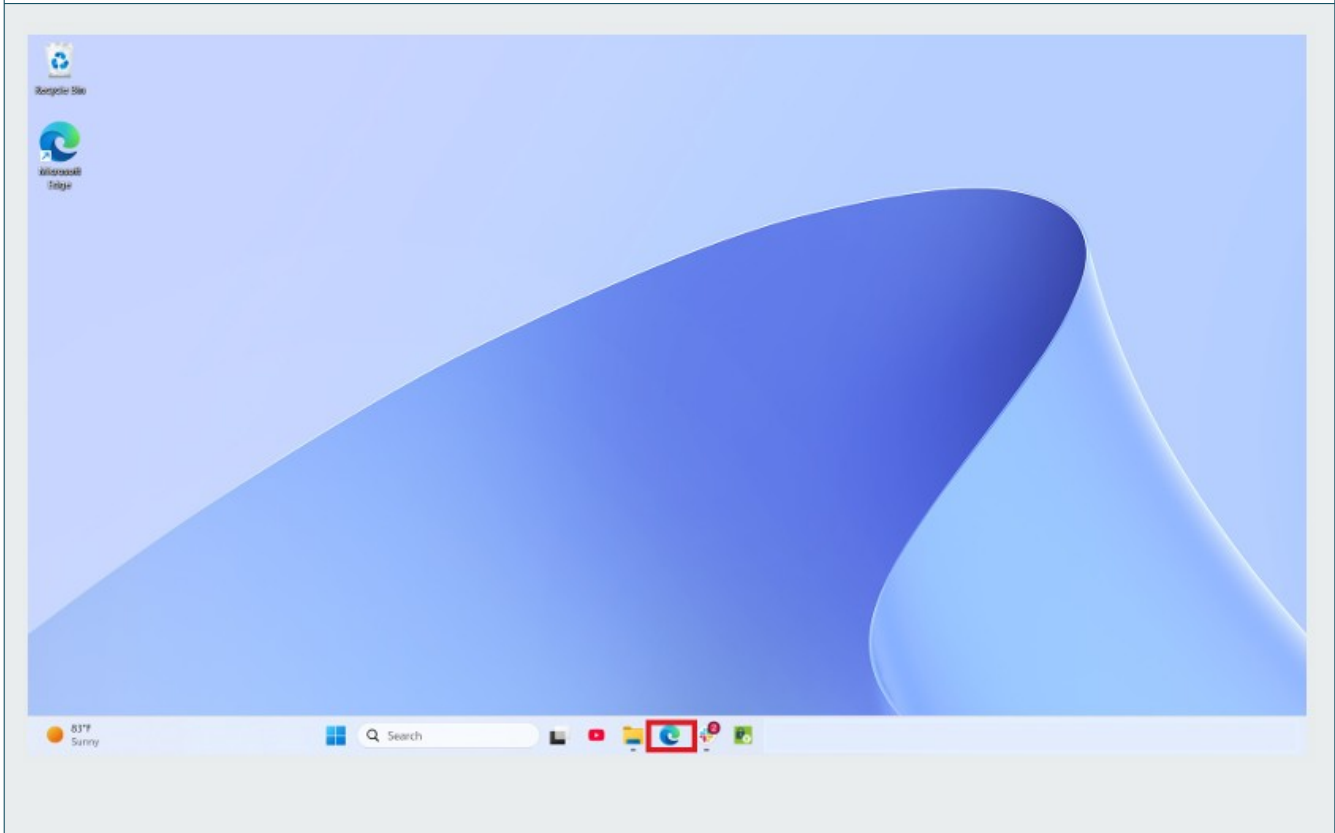
The provided USB adapter pictured below.



D5

OPEN THE EDGE BROWSER

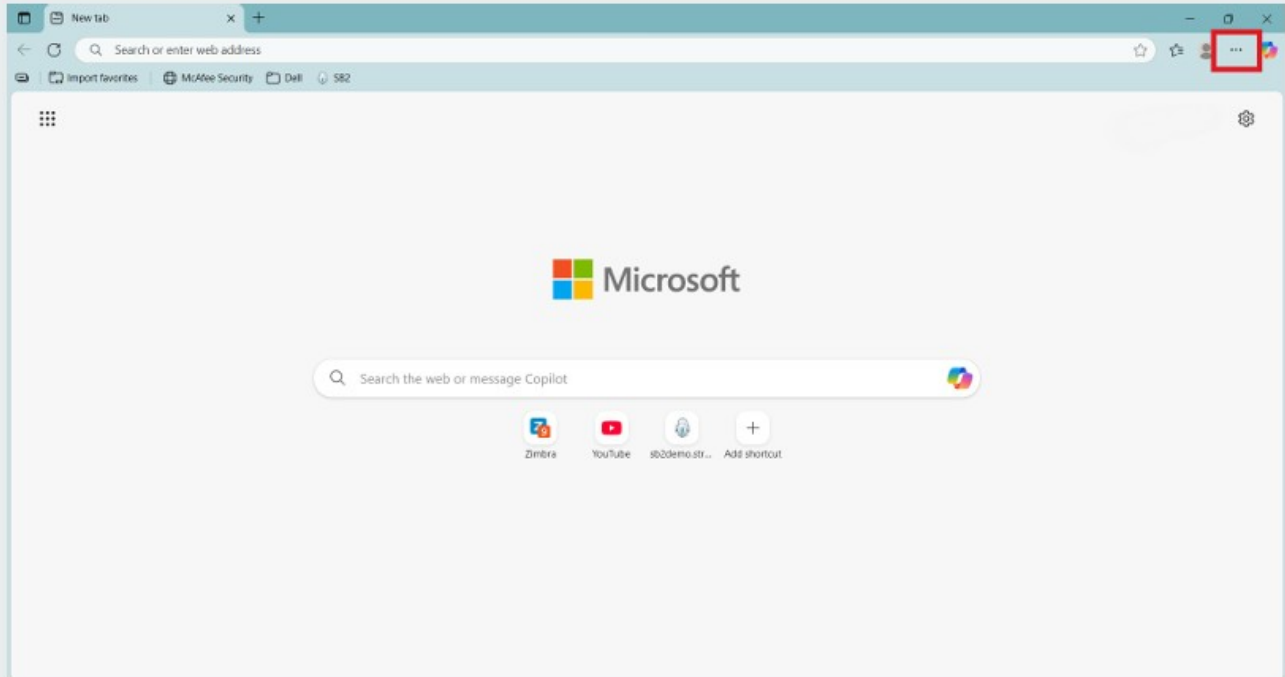
To begin, access the Edge browser by selecting its icon from the Windows taskbar.



D6

FIND THE EDGE BROWSER DROP DOWN MENU

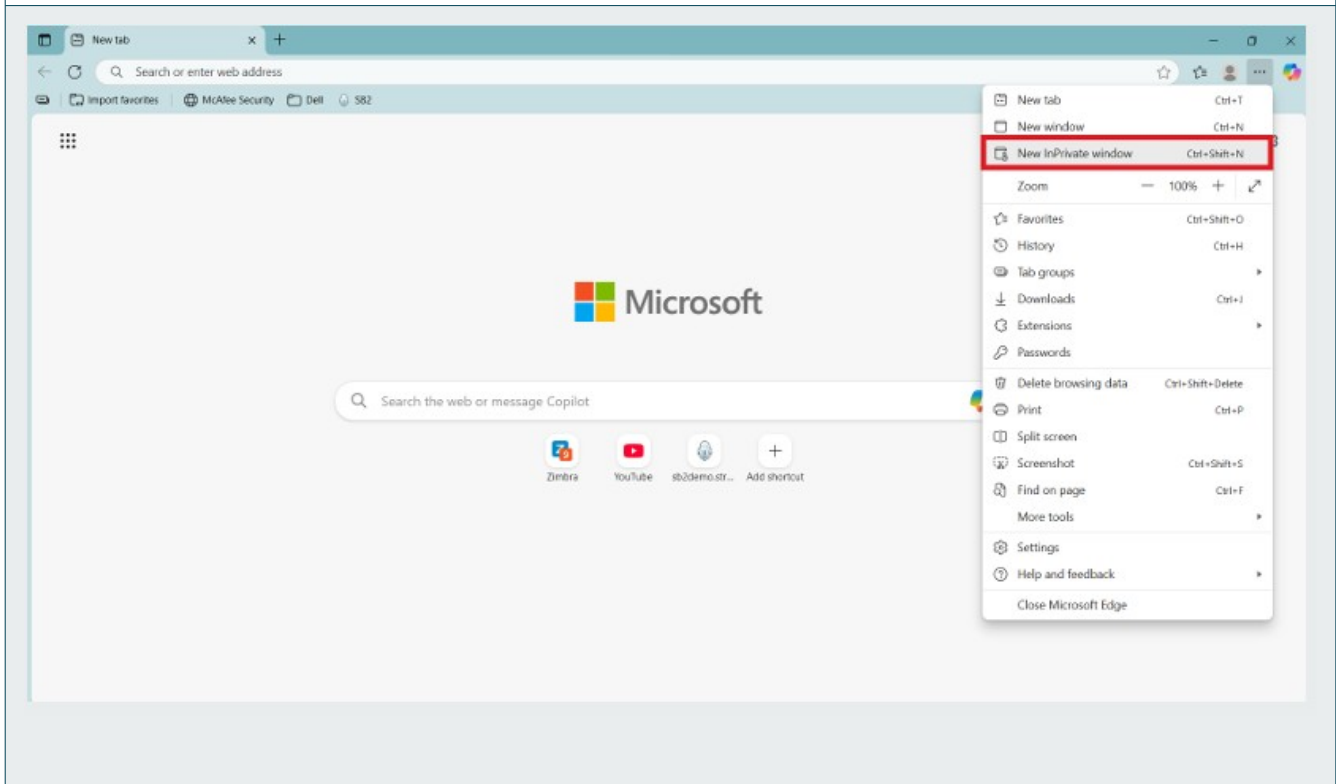
Locate the three-dots icon on the right side of the screen and select it.



D7

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)

D9

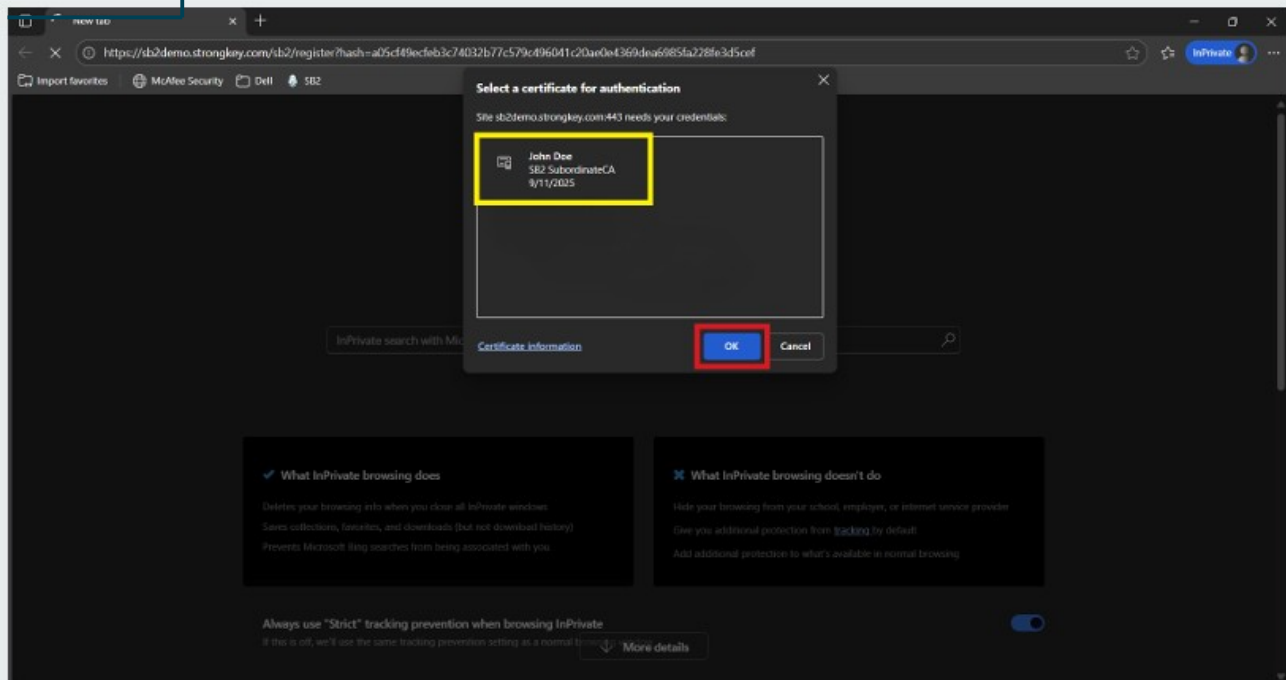
SELECT THE CERTIFICATE

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 for support.

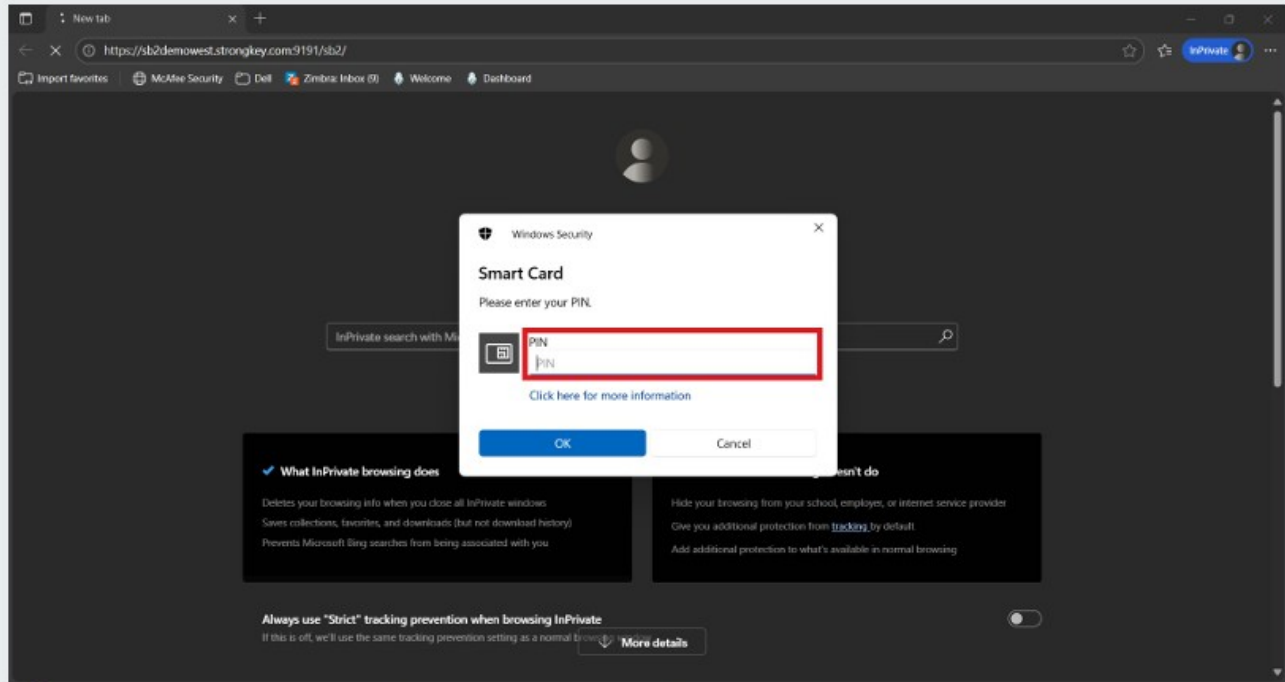




ENTER SECURITY KEY PIN

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.



D11

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.

The screenshot shows the StrongKey SB2 landing page with three main sections:

- Your Digital Certificate:** Includes fields for Username (cboyer), Full Name (Clifton Boyer), Organization (StrongAuth Inc), E-Mail (clifton.boyer@strongkey.com), and a redacted Serial No. A watermark reads "DIGITIZED TO PROTECT THE INNOCENT".
- Disclosures:** Contains a scrollable list of terms, including points 8, 9, 10, and 11. Point 11 is partially visible: "11. User Data Management: This type of".
- Your Security Key:** Features an image of a security key, instructions on nicknaming it, and a "Name" input field.

D12

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 a user registration interface with three main sections:

- User Profile:** Shows the name "Clifton Boyer" and organization "StrongAuth Inc". The email field is redacted with a grey box containing the text "INTENTIONALLY BLURRED FOR YOUR PROTECTION".
- Terms of Service:** A scrollable list of numbered terms (8-12) regarding data management and registration. A green checkmark and the text "I agree" are visible at the bottom of this section.
- Security Key Registration:** Features a USB security key icon and instructions: "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." Below this is a "Name" input field containing "SB2PROD DOCUMENTATION" and a "Register" button. A red arrow points to the "Register" button.

At the bottom of the interface, there is a copyright notice: "Copyright © 2001-2026 StrongAuth, Inc. (dba StrongKey)".

D14 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 shows a Windows Security dialog box titled "Save your passkey" overlaid on a registration screen. The dialog box contains the following text and elements:

- Windows Security logo and title bar.
- Close button (X).
- Section: **Save your passkey**
- Account information: clifton.boyer@strongkey.com Passkey for strongkey.com
- Instruction: **Enter your security key PIN**
- Input field: "Security Key PIN" with a masked PIN (••••••).
- Footer: I agree

The background registration screen shows user information for Clifton Boyer (Organization: StrongAuth Inc, E-Mail: clifton.boyer@strongkey.com) and a "Register" button. A red arrow points to the "OK" button in the dialog box.

D15

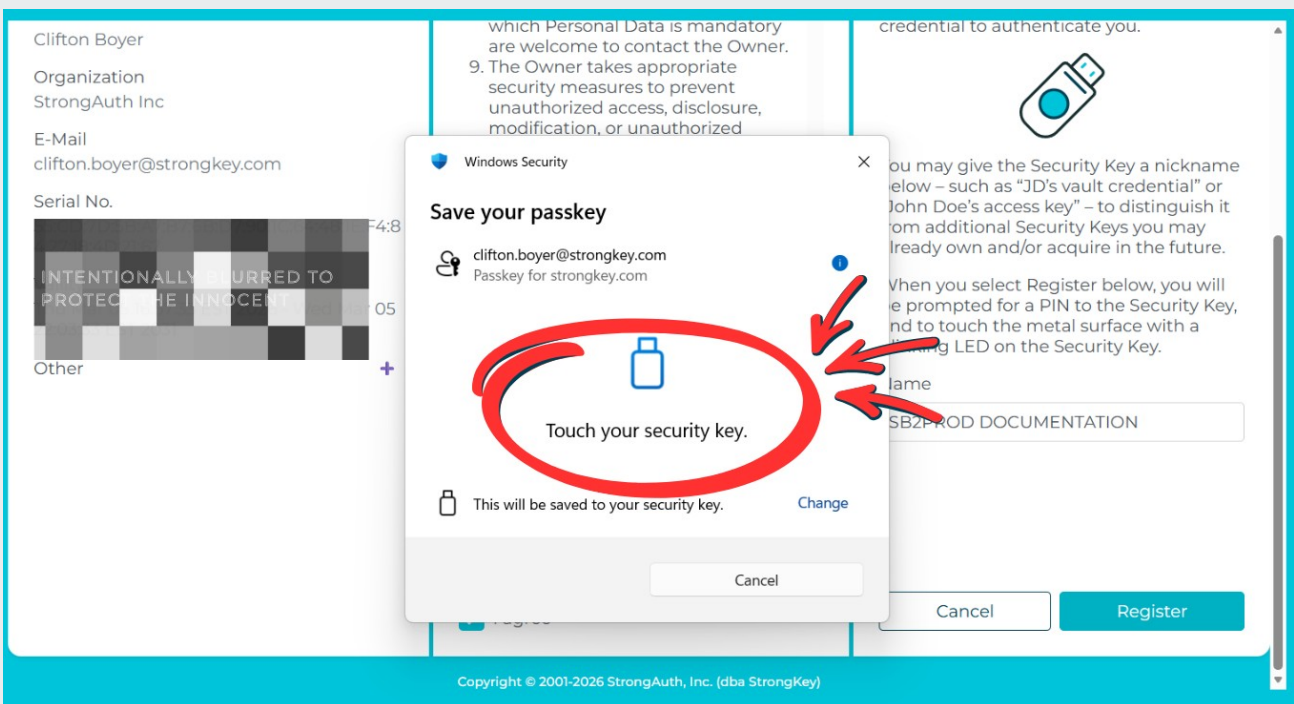
TOUCH THE SECURITY KEY

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.



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

The screenshot shows a registration confirmation dialog box with three main sections:

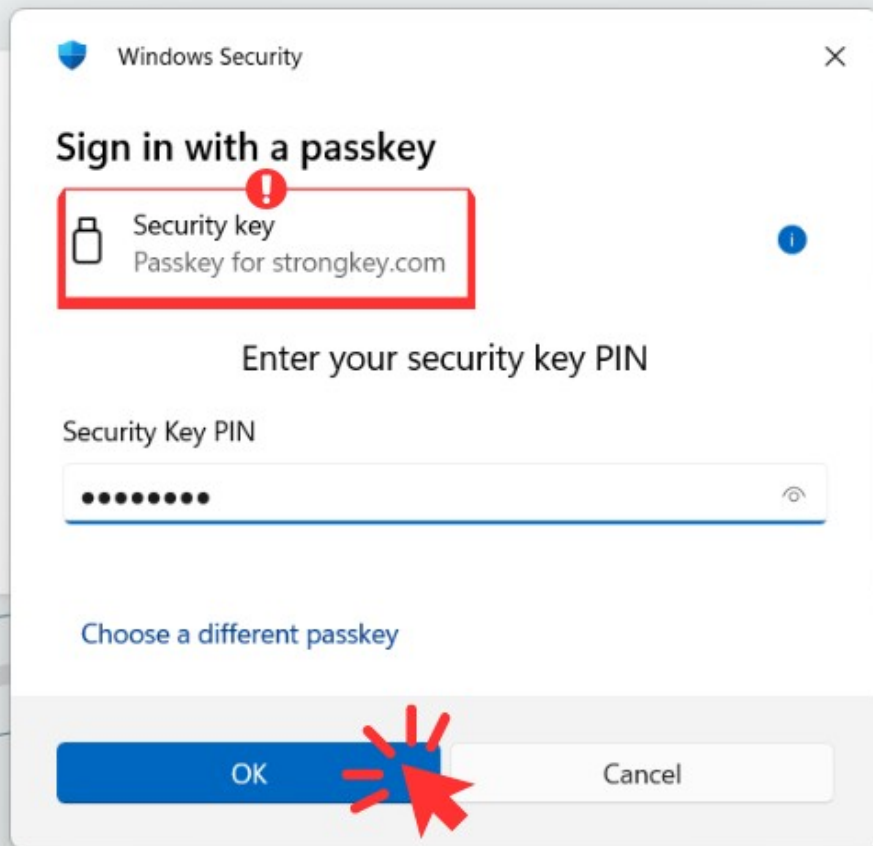
- User Information:** Displays the name "Clifton Boyer", organization "StrongAuth Inc", and email "clifton.boyer@strongkey.com". Below this is a blurred image of a document with the text "INTENTIONALLY OBLURRED TO PROTECT THE INNOCENT" and an "Other" category with a plus sign.
- Terms and Conditions:** Contains numbered paragraphs 9, 10, 11, and 12, along with a checked checkbox labeled "I agree".
- Registration Instructions:** Explains that the user has added a Security Key and provides instructions on how to use it. It includes a "Name" field with the value "SB2PROD DOCUMENTATION" and a "Continue" button with a right-pointing arrow.

A blue notification bubble in the top right corner of the dialog box states: "You've successfully registered. Click 'Continue' to proceed to the login page." A red arrow with a white checkmark points from the notification bubble towards the "Continue" button.

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

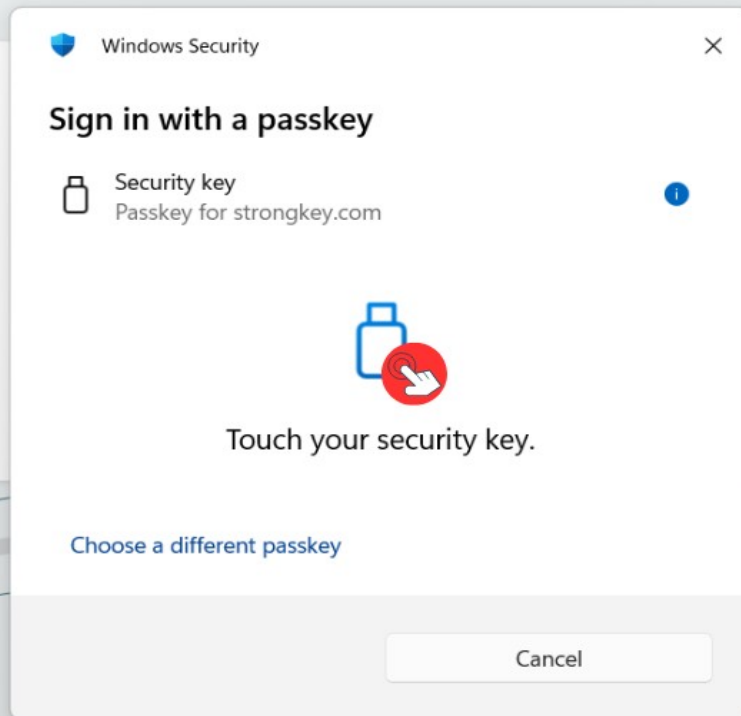
D17 SIGNING IN

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**.



D18 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.



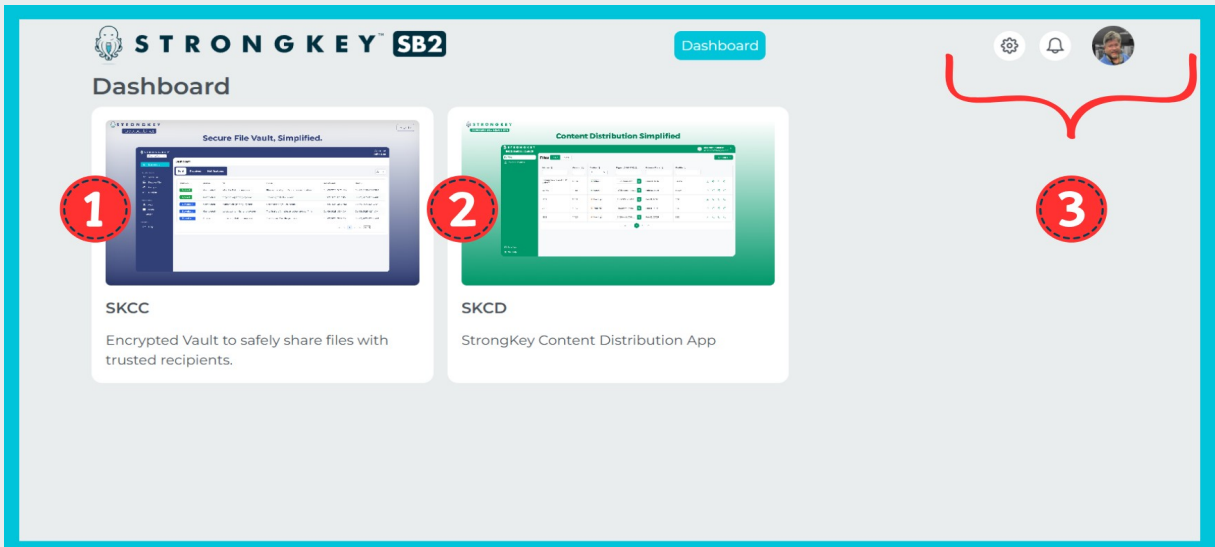
THE SB2PROD PLATFORM DASHBOARD

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.

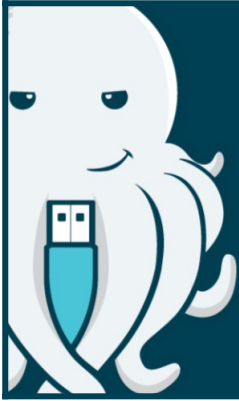
All SB2 users have access to two primary applications and:

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

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



COPYRIGHT & 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.

API

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.

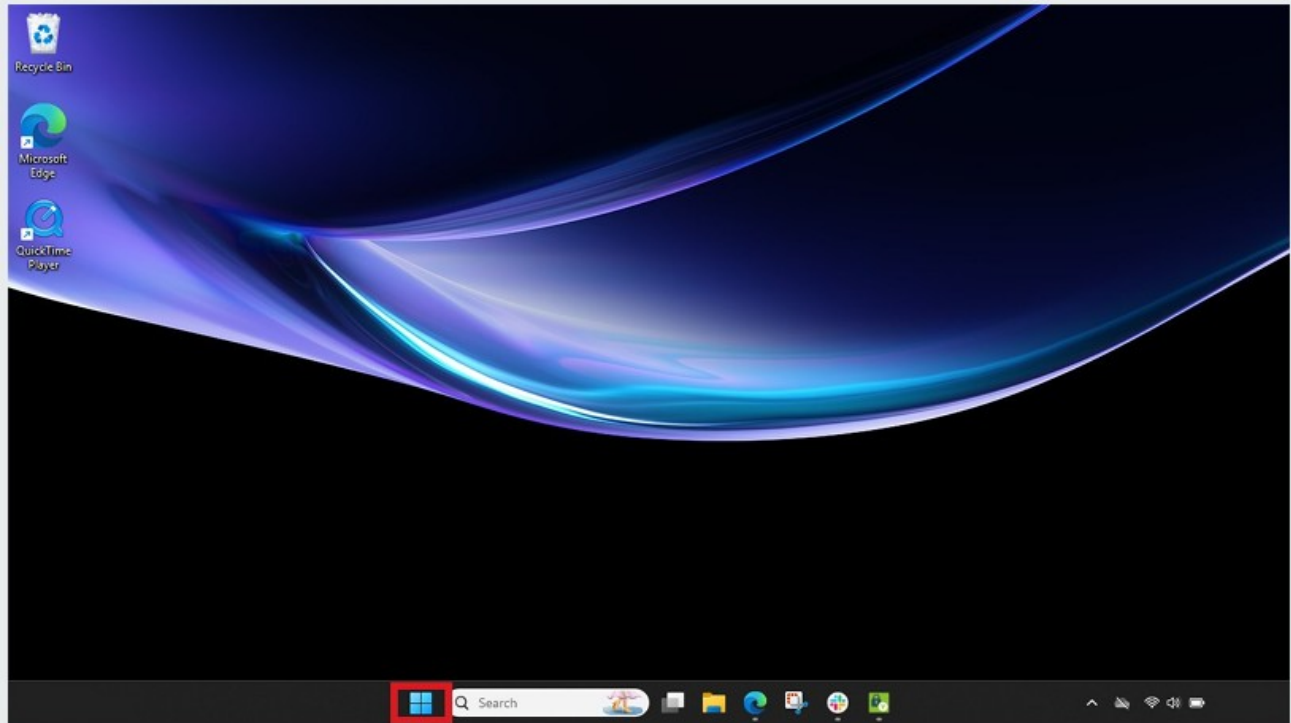
However, StrongKey recommends using the SAME PIN to both containers of the **Security Key** to reduce the burden on users. As long as the **Security Key** is safely in the possession of the legitimate user, and the legitimate user is NOT sharing the PIN to the **Security Key** with anyone, the user will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

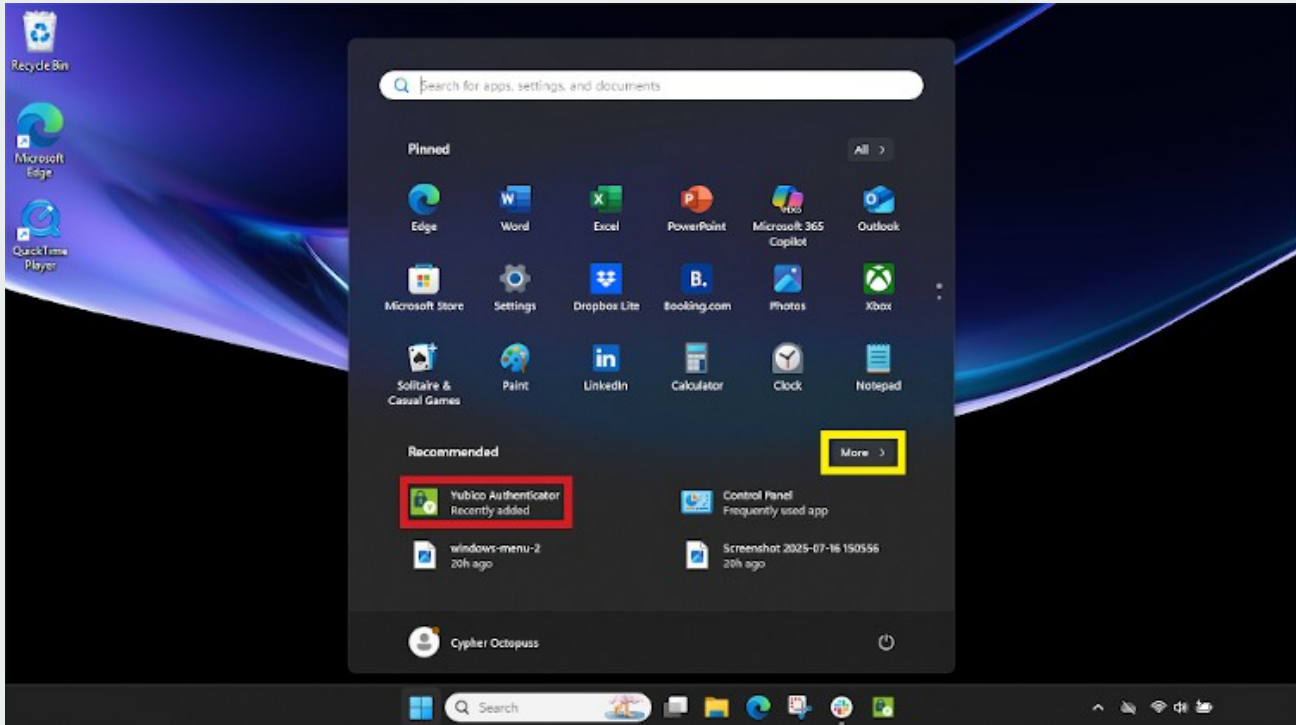
AP2

OPEN THE YUBICO AUTHENTICATOR APPLICATION

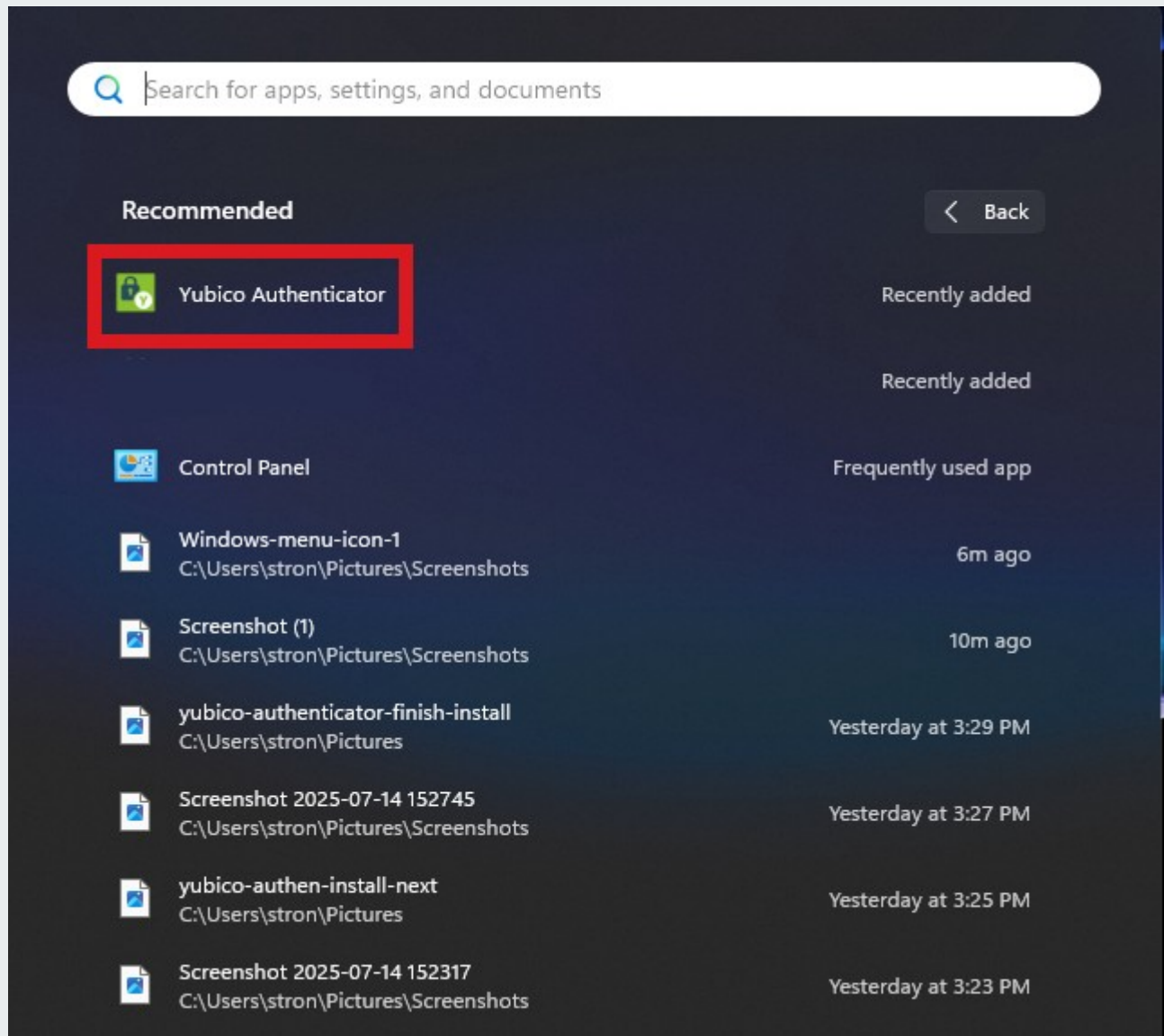
To begin, access the Yubico Authenticator application by selecting the **Windows start icon** from the Windows taskbar.



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.



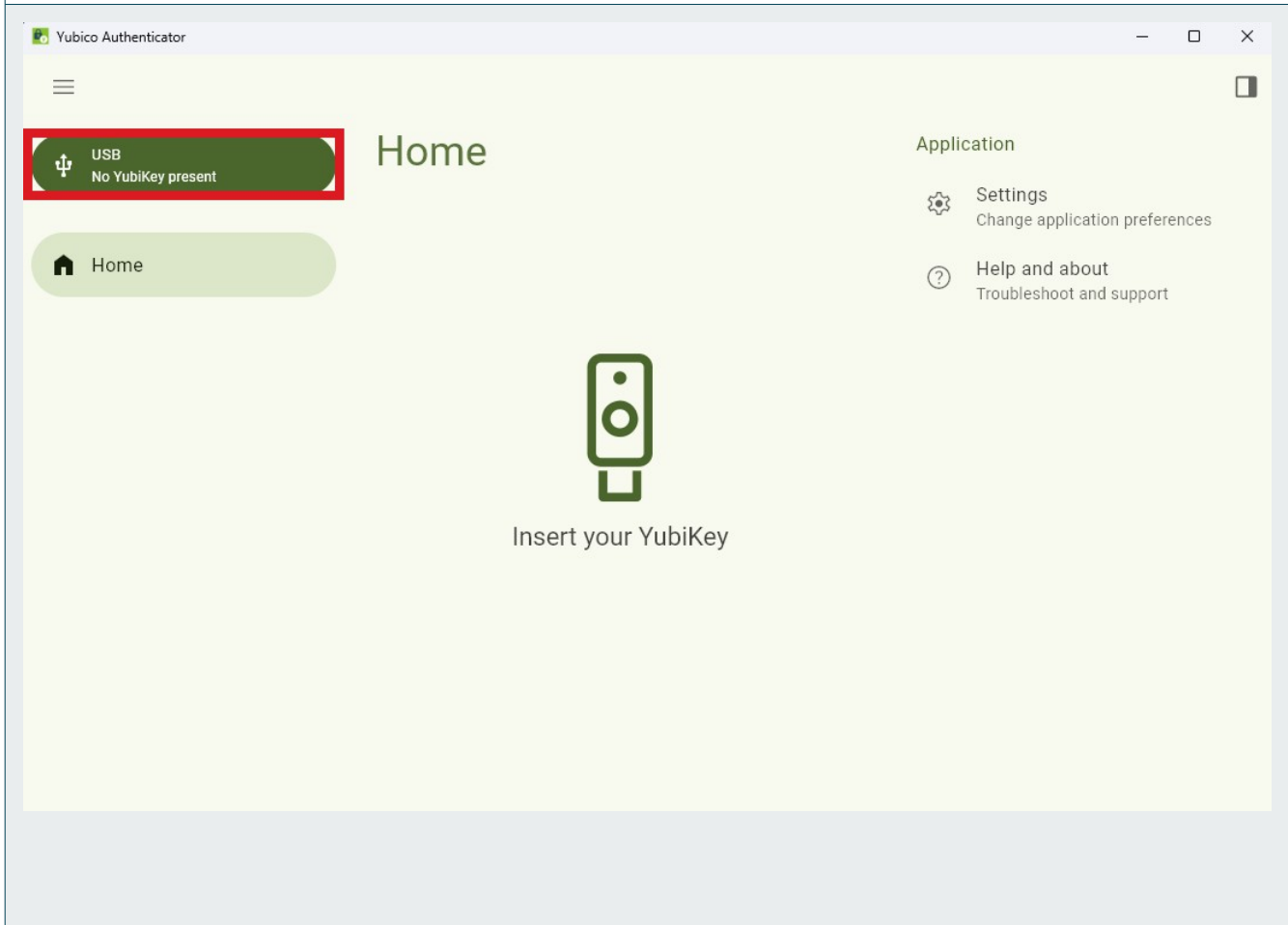
Since the Yubico Authenticator application was recently installed, it will typically appear near the top of the menu list.



AP5

THE YUBICO AUTHENTICATOR APPLICATION

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



AP6

INSERT THE YUBIKEY 5C NFC

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

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.

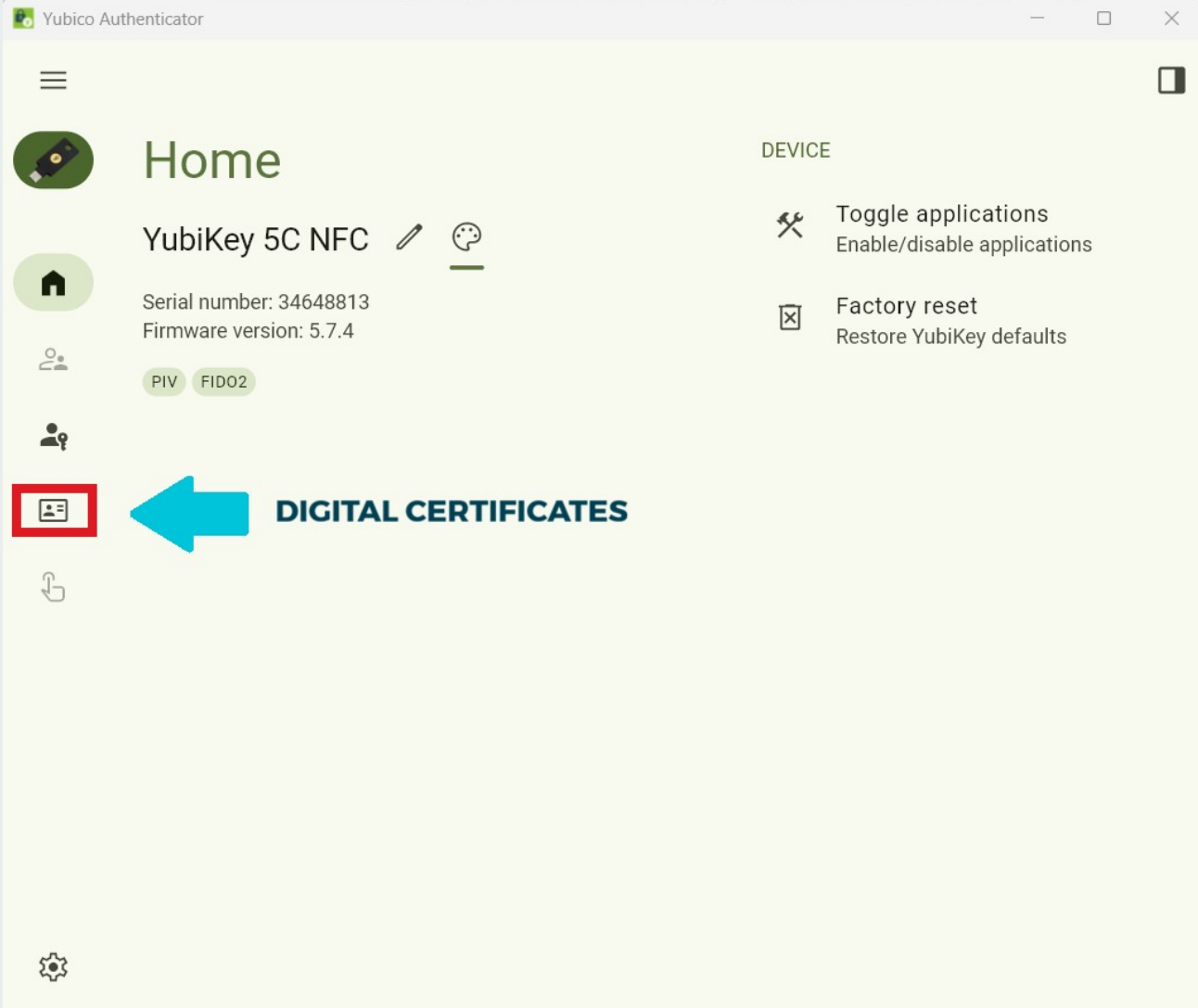
With the provided **USB-A to USB-C adapter**, simply plug the USB-A end into the computer and insert the **Security Key** into the USB-C port.

The provided USB adapter pictured below.

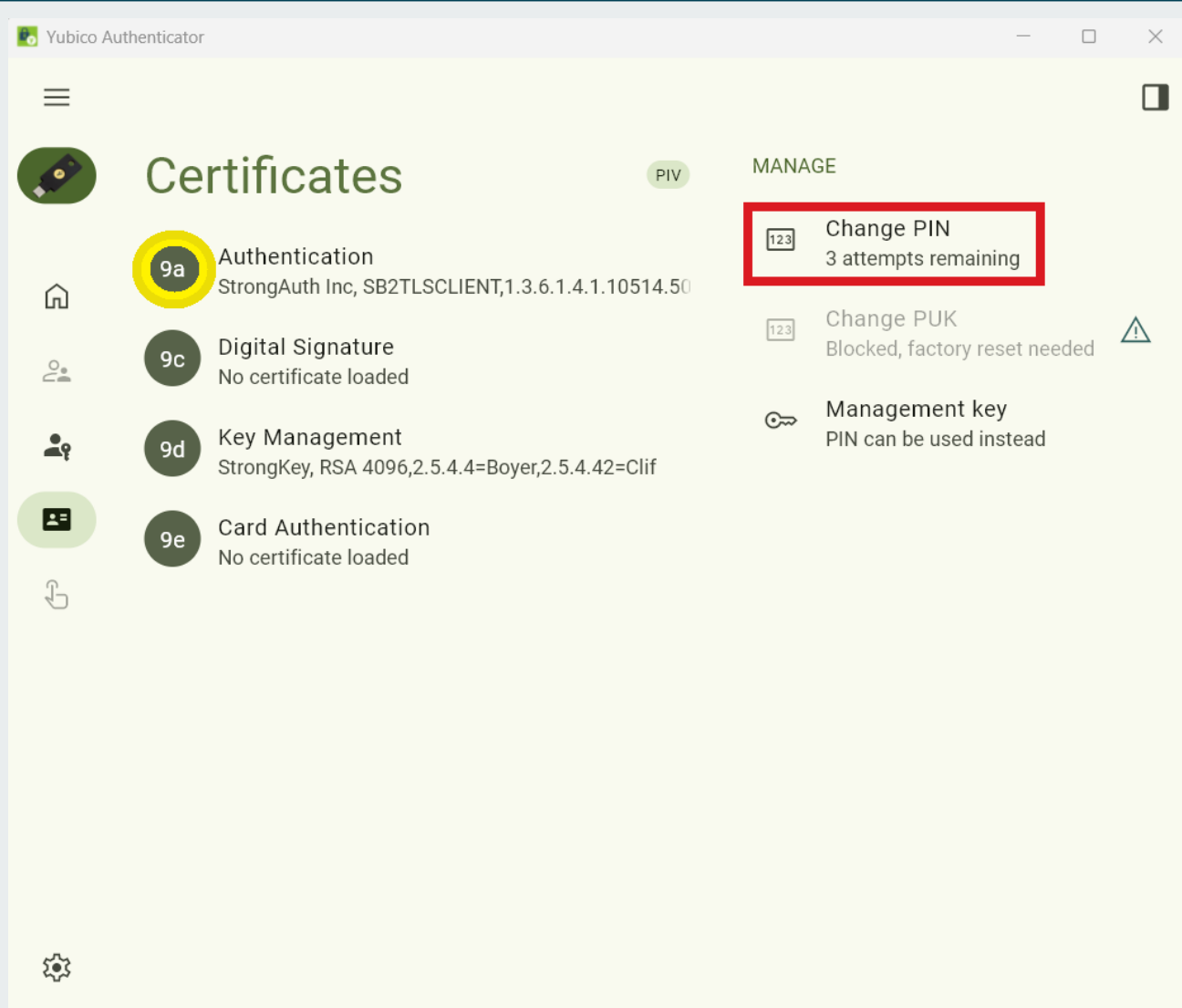


CHANGING THE DIGITAL CERTIFICATE PIN

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.



- 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

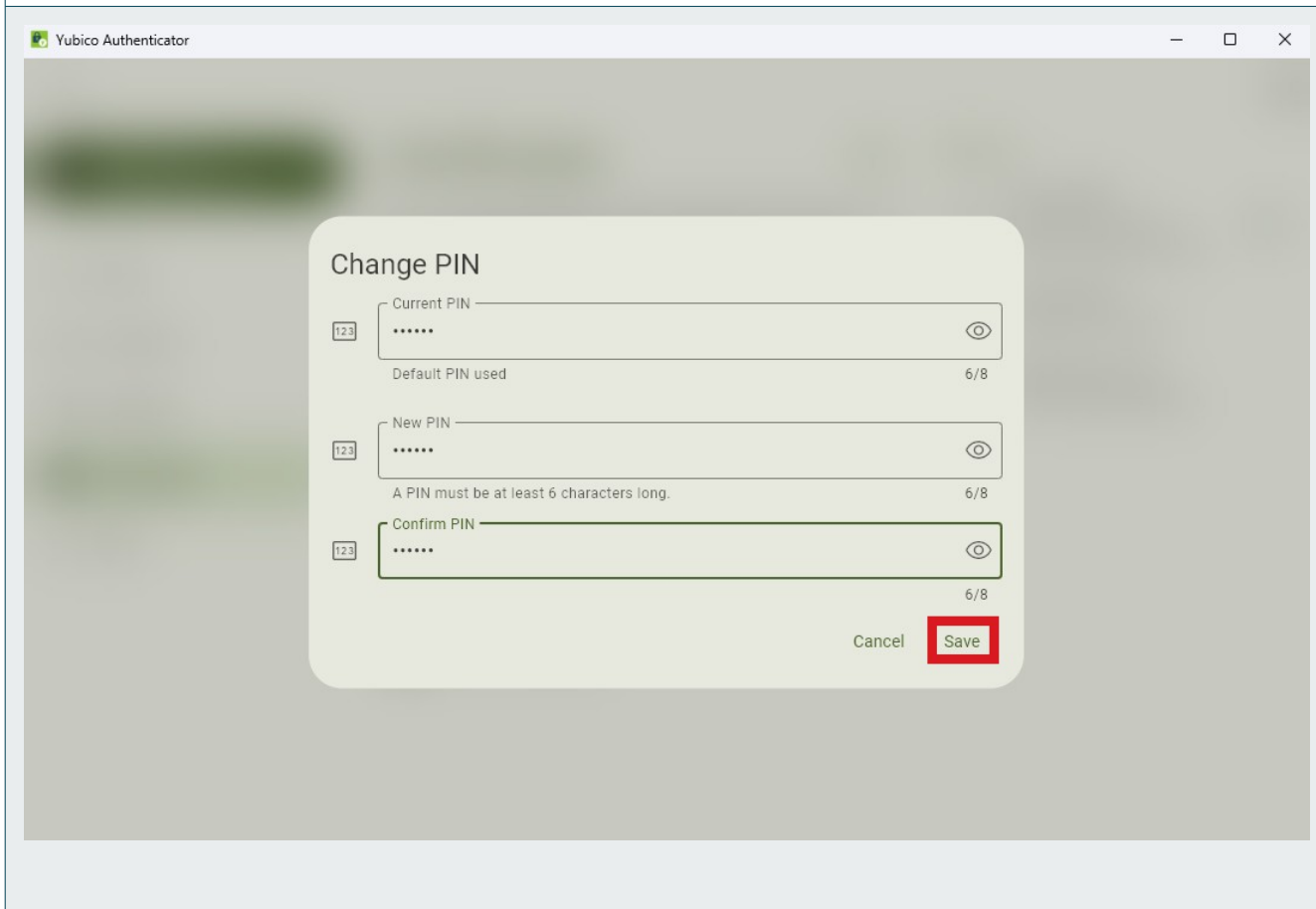
New PIN 6/8
A PIN must be at least 6 characters long.

Confirm PIN 6/8

Cancel Save

AP12 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.



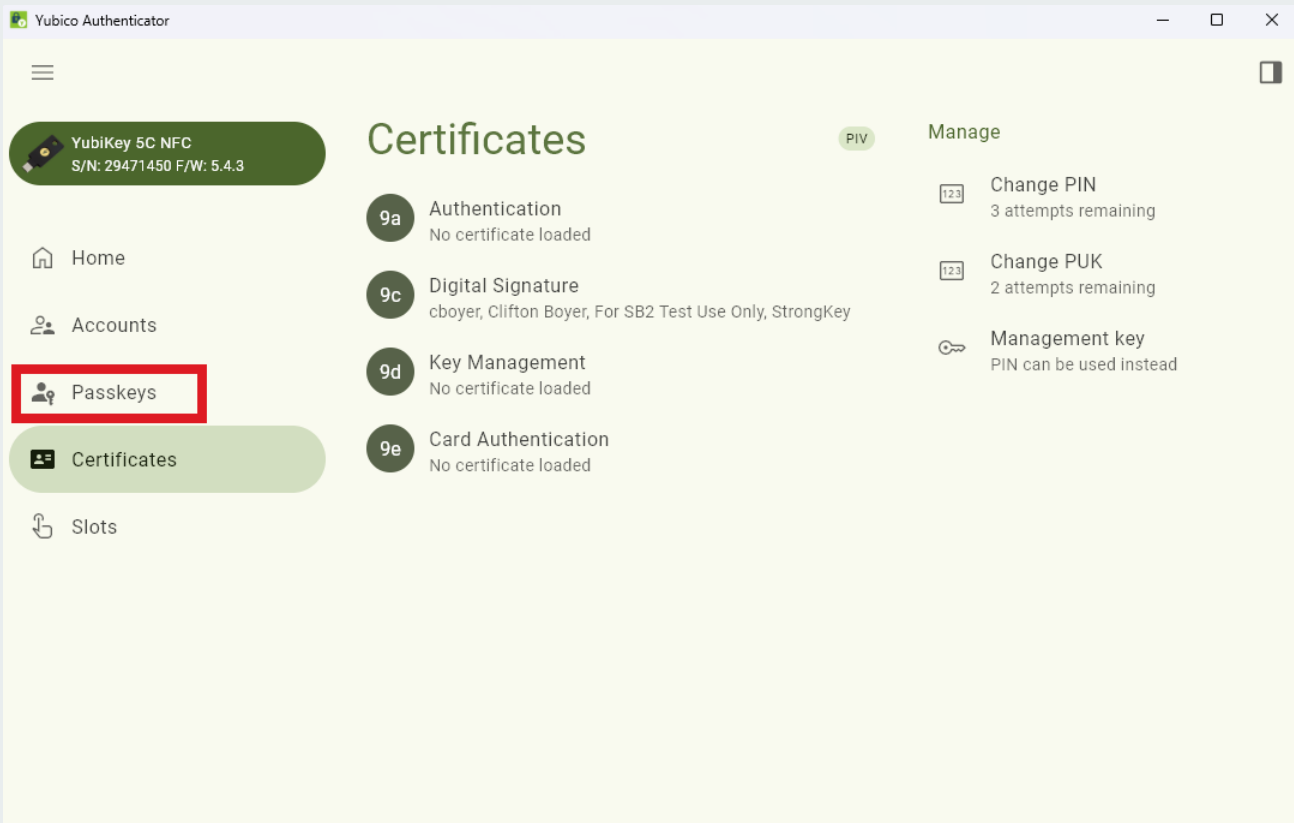
CHANGING THE FIDO CREDENTIALS PIN

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

NOTE



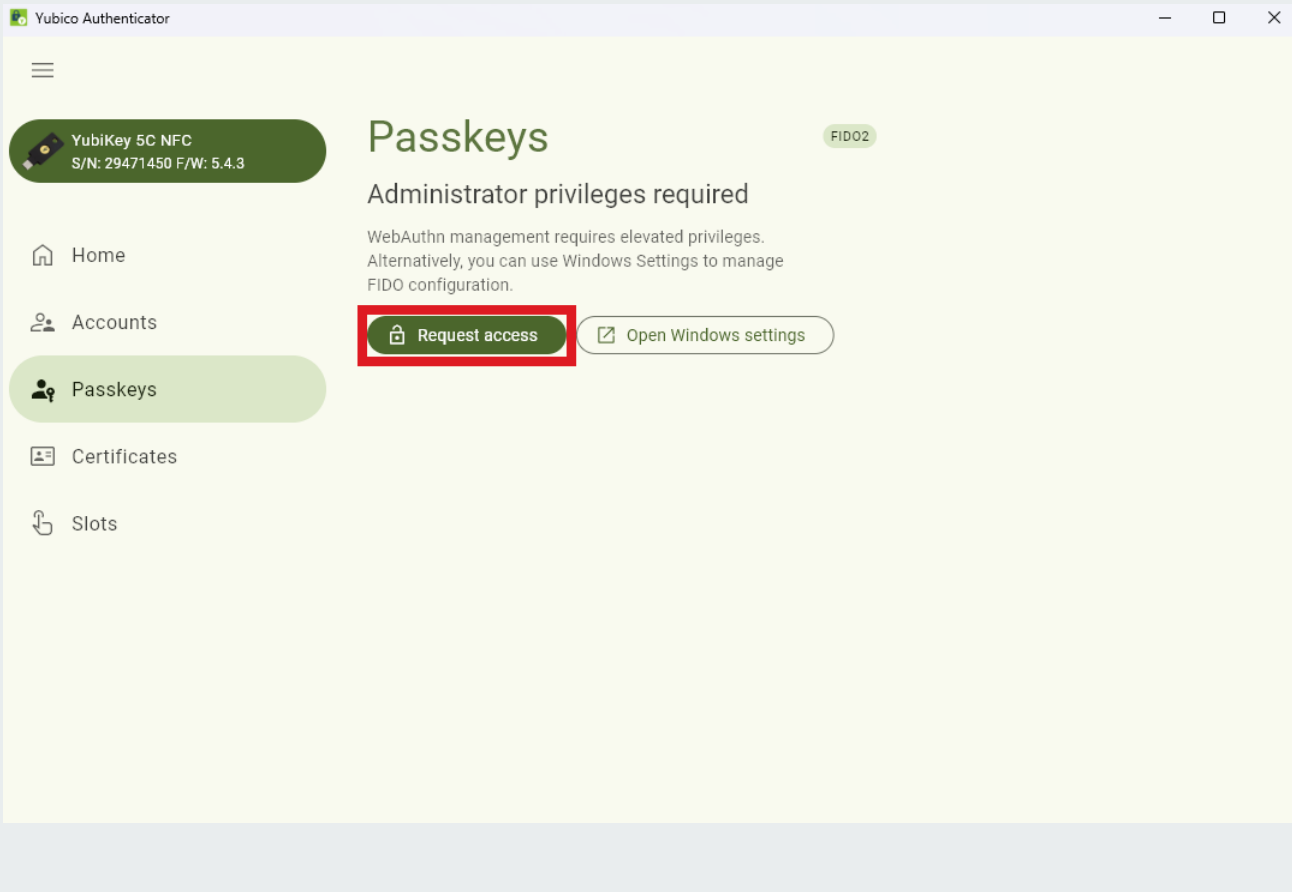
StrongKey recommends using the same PIN for the Security Key.



AP14

PASSKEYS MENU

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

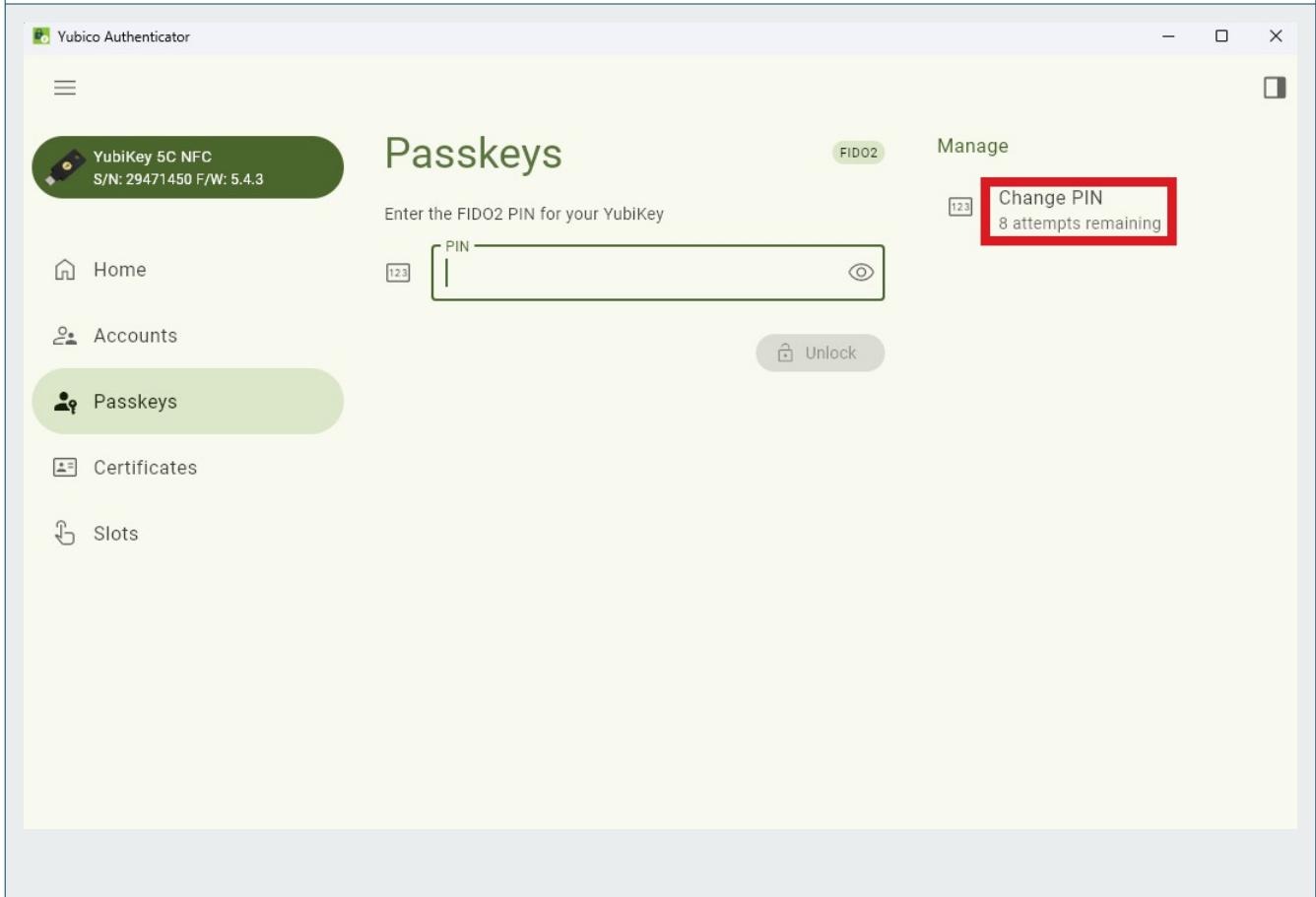


AP15

YUBICO AUTHENTICATOR APPLICATION PERMISSION

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

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.



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.

