



STRONGKEY TELLARO SB2

Yubico YubiKey 5C NFC User's Guide for Windows 10

Version 31

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.

I

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 SB2PROD 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.

The StrongKey Support Team

II

PREREQUISITES

- Windows 10
- Microsoft (MS) Edge Browser, version 146.0.3856.109
- Yubikey 5C NFC
- Internet connection
- USB-C port or USB-C-to-USB-A adapter

III

TABLE OF CONTENTS

A

[Installing the Yubico Authenticator Application](#)

3

B

[Installing the YubiKey Minidriver for Windows 10](#)

9

C

[Importing SB2 Root CA & SB2 Subordinate CA Certificates into Microsoft Trust Store](#)

13

C14

[Security Thumbprint](#)

20

D

[Accessing an SB2PROD Invitation Link URL](#)

36

AP

[Appendix: Changing a Yubico YubiKey 5C NFC Personal Identification Number \(PIN\)](#)

48



SECTION A

A1

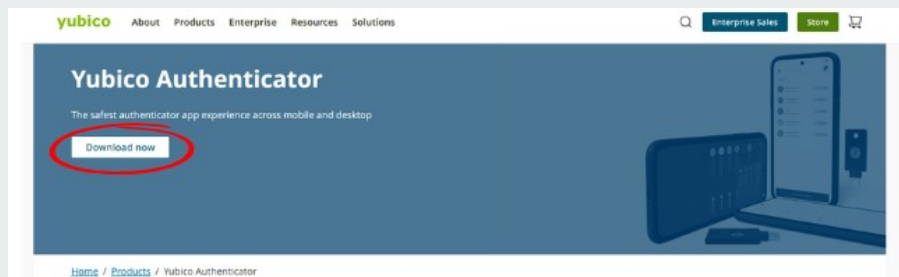
INSTALLING THE YUBICO AUTHENTICATOR APPLICATION

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

A2

DOWNLOAD YUBICO AUTHENTICATOR APPLICATION

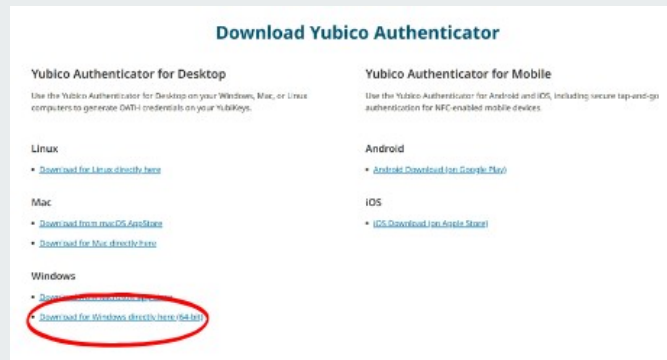
Download the Yubico Authenticator for 64-bit systems from <https://www.yubico.com/products/yubico-authenticator/#h-download-yubico-authenticator>. Click Download now.



A3

WINDOWS YUBICO AUTHENTICATOR APPLICATION

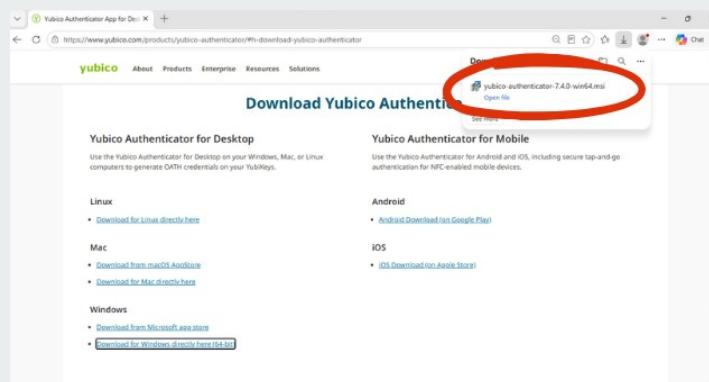
Select Download for Windows directly here (64-bit). **Click it to start download.**



A4

OPENING THE YUBICO AUTHENTICATOR APPLICATION

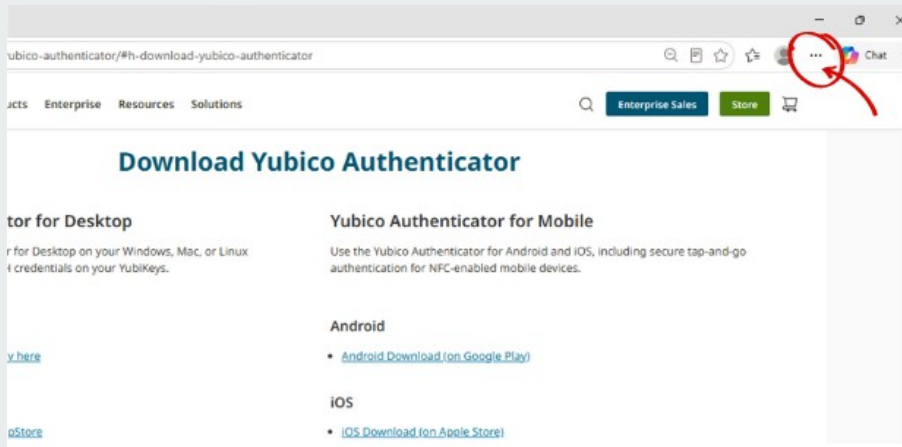
After clicking the download link, MS Edge will display a pop-up confirming the Authenticator application file has been successfully downloaded and ready for installation. **Click the open file link.**



A5

NO POP-UP WINDOW? NO PROBLEM

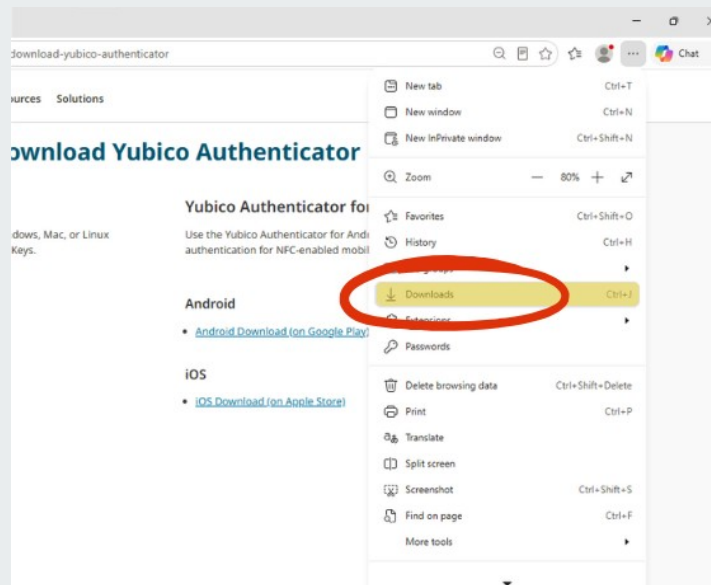
If the pop-up does not appear, or is inadvertently closed, access the downloaded file by clicking the **3-dot menu** on the right side of the MS Edge tool bar.



A6

CLICK DOWNLOADS

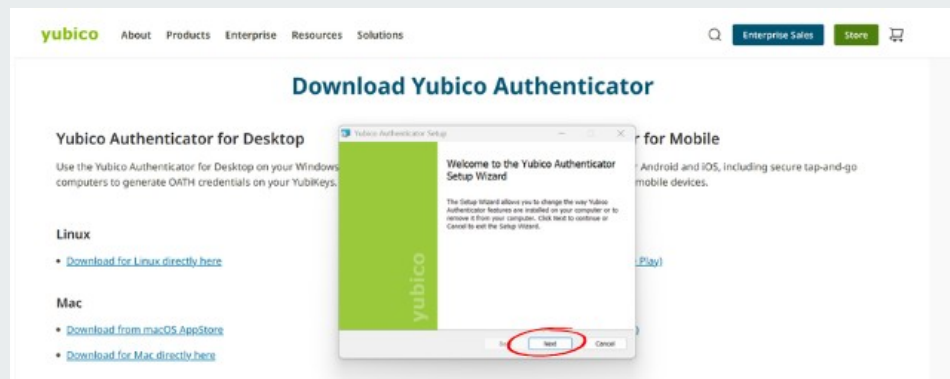
From the drop-down menu, select **Downloads**.



A7

YUBICO AUTHENTICATOR SETUP WIZARD

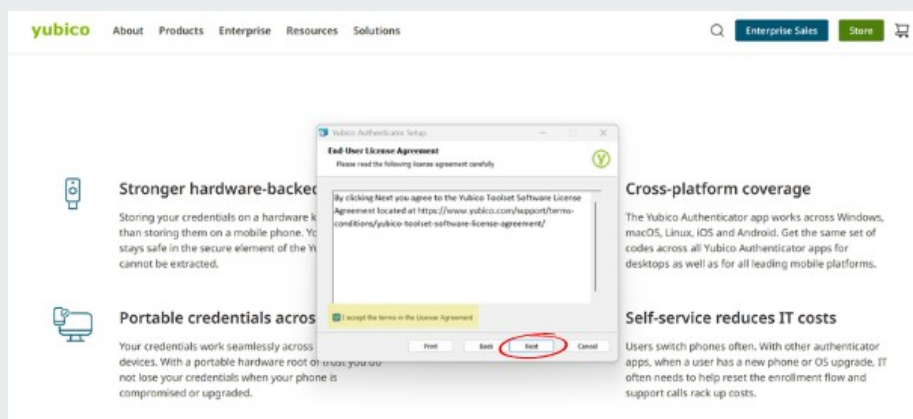
A Setup Wizard window will appear, Click Next.



A8

YUBICO AUTHENTICATOR TERMS & CONDITIONS

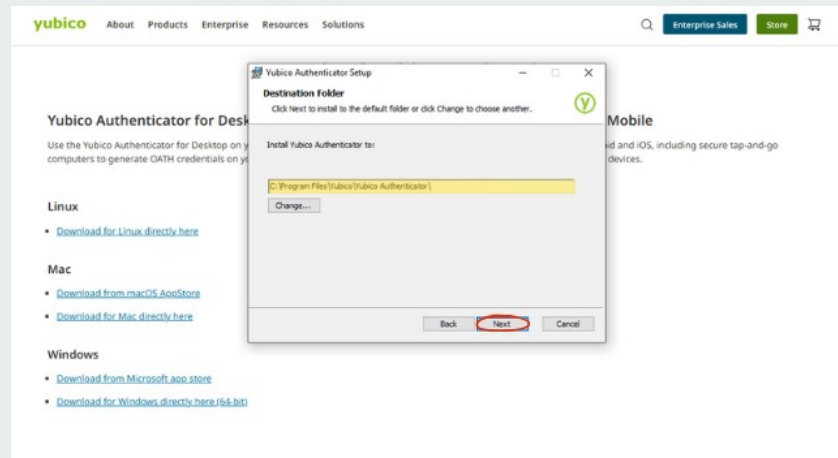
Accept the terms of the end-user license agreement, then click Next.



A9

SELECT DESTINATION FOLDER

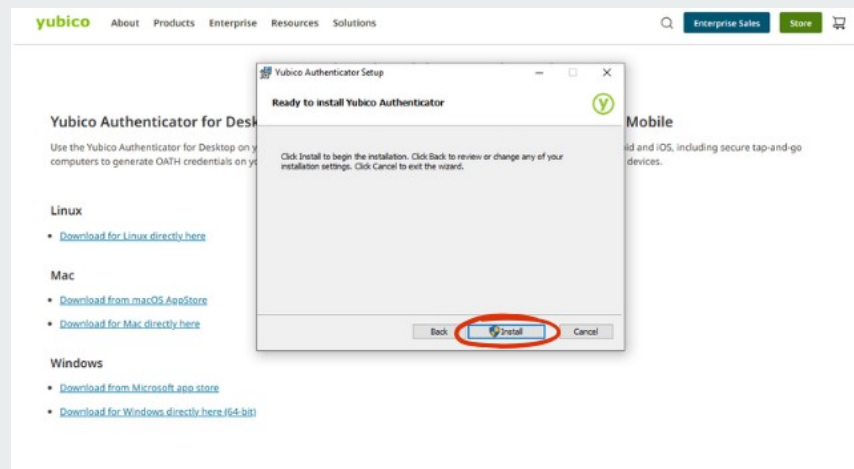
Use the default Destination Folder and Click **Next**.



A10

READY TO INSTALL

Click **Install**.



A11

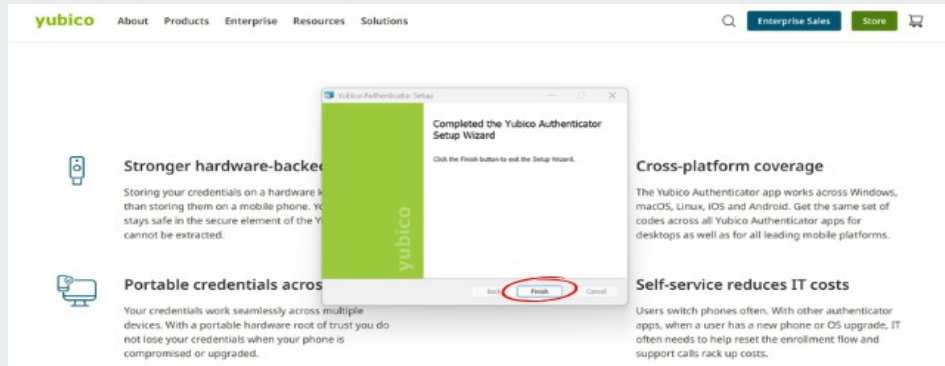
PERMISSION TO MAKE CHANGES

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

A12

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.

B2

DOWNLOAD THE YUBIKEY MINIDRIVER

Download the YubiKey minidriver 64 bit file at:

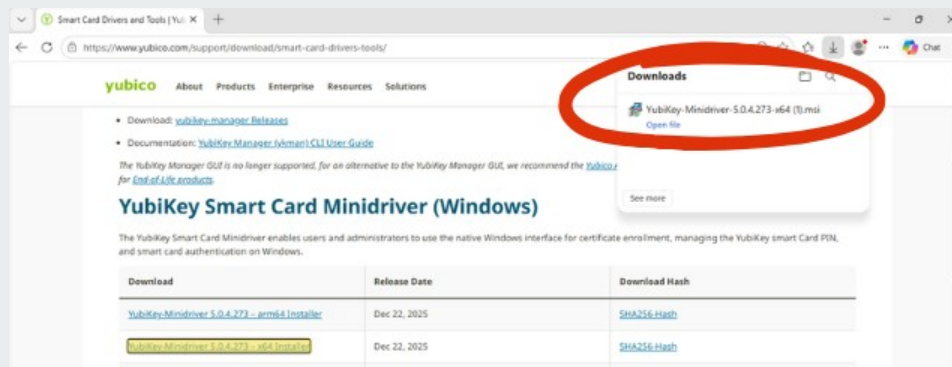
<https://www.yubico.com/support/download/smart-card-drivers-tools/>.

yubico About Products Enterprise Resources Solutions Enterprise Sales Store 		
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.		
Download	Release Date	Download Hash
YubiKey-Minidriver 5.0.4.273 - x64 Installer	Dec 22, 2025	SHA256-Hash
YubiKey-Minidriver 5.0.4.273 - x64 Installer	Dec 22, 2025	SHA256-Hash
YubiKey-Minidriver 5.0.4.273 - x86 Installer	Dec 22, 2025	SHA256-Hash
YubiKey-Minidriver 5.0.4.273 - CAB (x64_arm64_x86)	Dec 22, 2025	SHA256-Hash

B3

OPENING THE YUBIKEY MINIDRIVER FILE

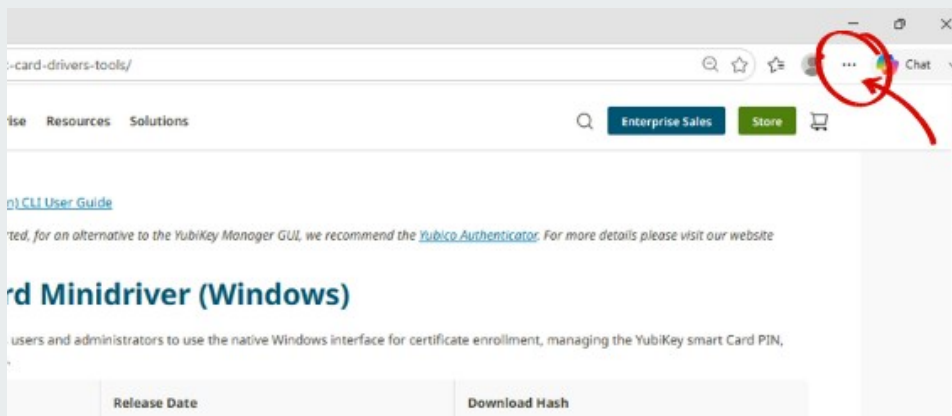
After clicking the download link, Edge browser will display a pop-up confirming the Minidriver file has been successfully downloaded and ready for installation. Click the **Open file link**.



B4

NO POP-UP WINDOW?

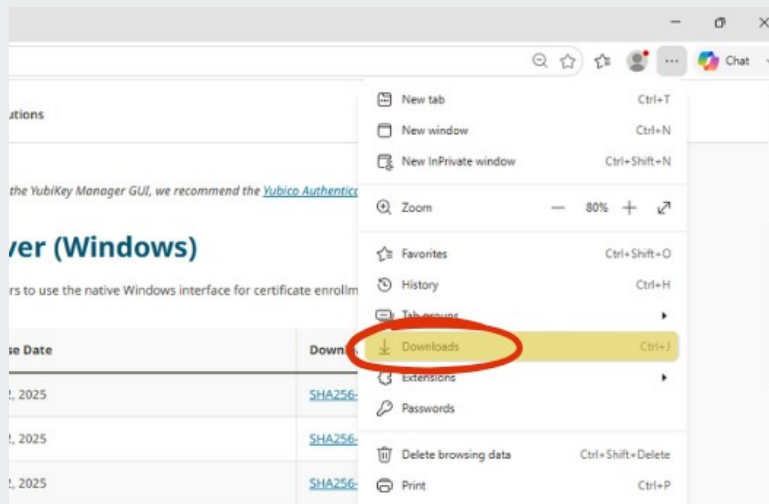
If the pop-up does not appear, or is inadvertently closed, access the downloaded file by clicking the 3-dot menu on the right side of the MS Edge tool bar.



B5

CLICK DOWNLOADS

From the drop-down menu, select **Downloads**. Next, click the **Open file** link under the YubiKey-Minidriver-5.0.4.273-x64.msi file ([see step B3](#)).



B6

INSTALLING THE YUBIKEY MINIDRIVER

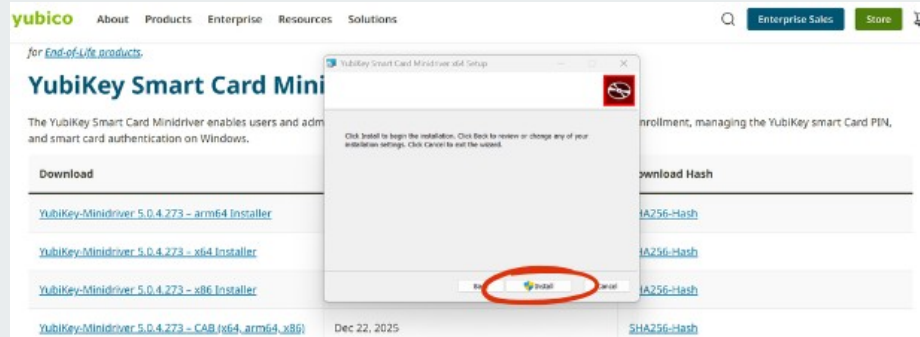
A Setup Wizard pop-up will open – Click **Next**.



B7

CONTINUE INSTALLING THE YUBIKEY MINIDRIVER

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



B8

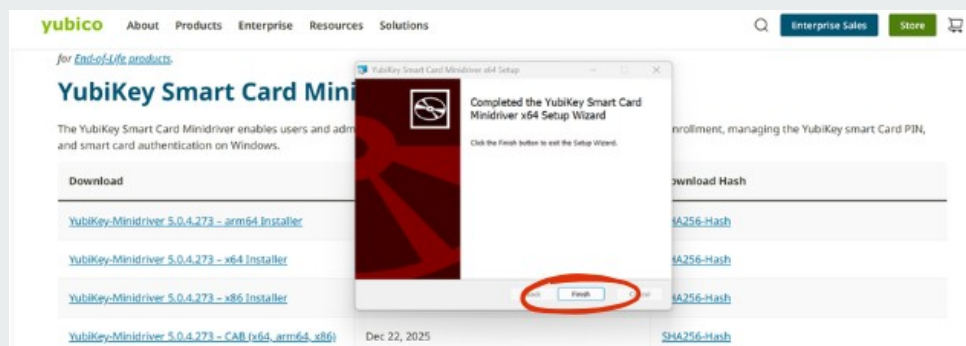
PERMISSION TO MAKE CHANGES

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

B9

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 THE TRUST STORE

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.

C2

ACCESS THE SB2PROD PAGE

All required CA certificates are available for download from the SB2PROD page at <https://www.strongkey.com/sb2pki>.

The screenshot shows the StrongKey website interface for downloading CA certificates. At the top, the StrongKey logo is displayed. Below it, the text reads: "StrongKey Tellaro Small Business Security Bundle (SB2) PRODUCTION". A paragraph follows: "This page guides authorized users on configuring their PCs to work with StrongKey's PRODUCTION SB2. If you have any questions and have an authorized Security Key from StrongKey, please e-mail support@strongkey.com; otherwise please send e-mail to getsecure@strongkey.com."

Under the heading "SB2 Production CA Certificates", there are three download buttons: "Download Root CA", "Download Sub CA1", and "Download Sub CA2".

To the right, under the heading "How To Configure CA Certificates", there are two sections: "Swissbit Security Keys" and "Yubikey Security Keys". Each section has a table of links for HTML and PDF guides for Windows 10, Windows 11, and macOS. The Windows 11 links are highlighted in blue.

Format	Windows 10	Windows 11	macOS
HTML	Windows 10	Windows 11	macOS
PDF	Windows 10	Windows 11	macOS

Format	Windows 10	Windows 11	macOS
HTML	Windows 10	Windows 11	macOS
PDF	Windows 10	Windows 11	macOS

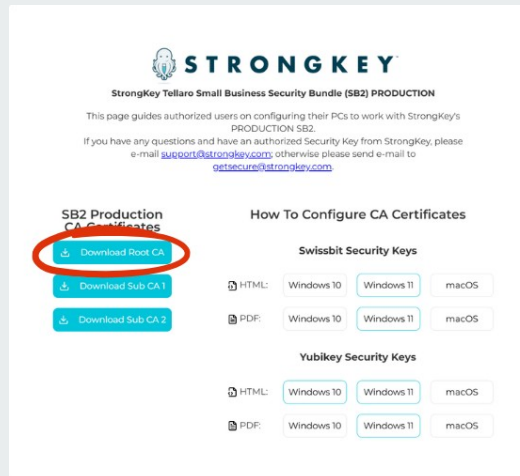
C3

SB2 CA CERTIFICATES

Next, download the three SB2PROD CA certificates from the left side of the page.

NOTE

Download the certificates starting with the Root CA.

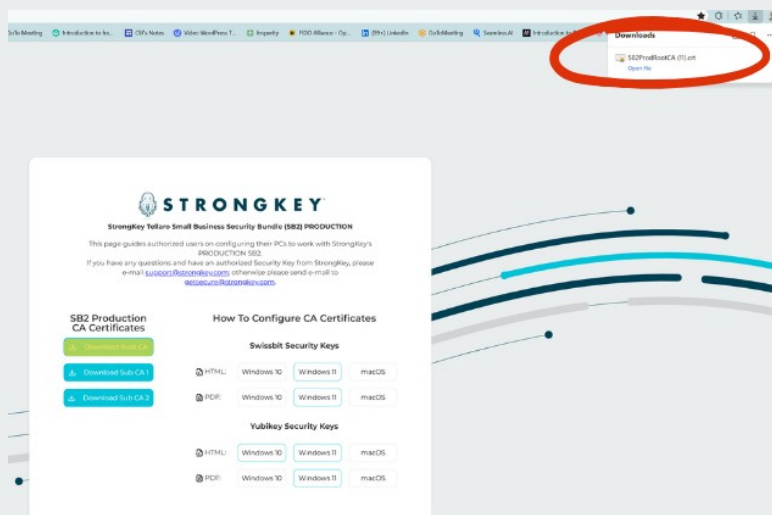


C4

DOWNLOADING THE SB2 ROOT CA

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

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



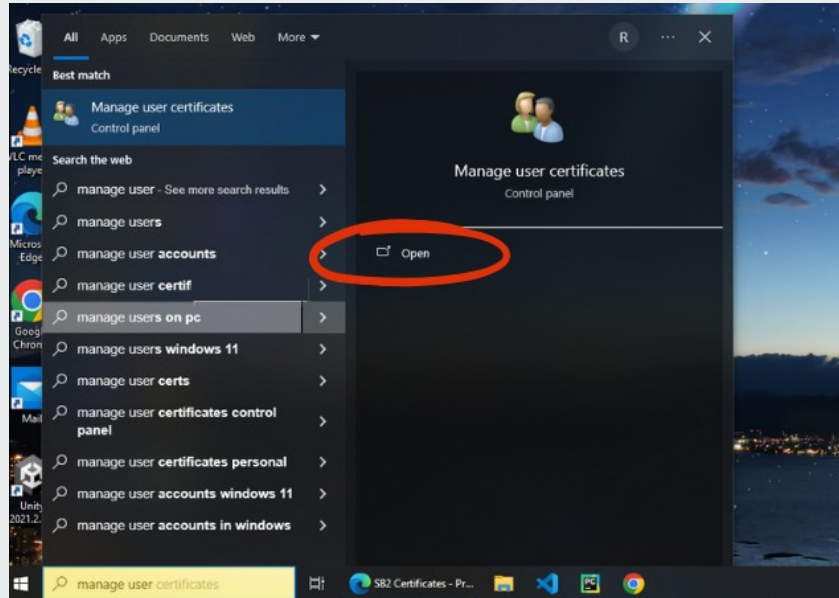
C5

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.

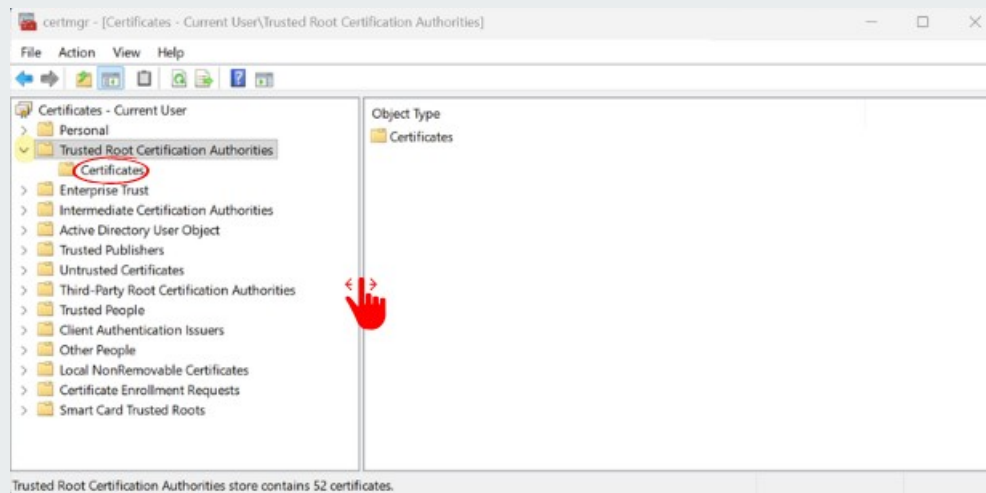


C6

OPEN TRUSTED ROOT CERTIFICATION AUTHORITIES FOLDER

To begin, expand the **certmgr** window by clicking and dragging the borders to a larger size. This will provide a better view of the digital certificates.

Next, click the **down arrow** next to the **Trusted Root Certification Authorities** folder to expand it, revealing the **Certificates** folder.

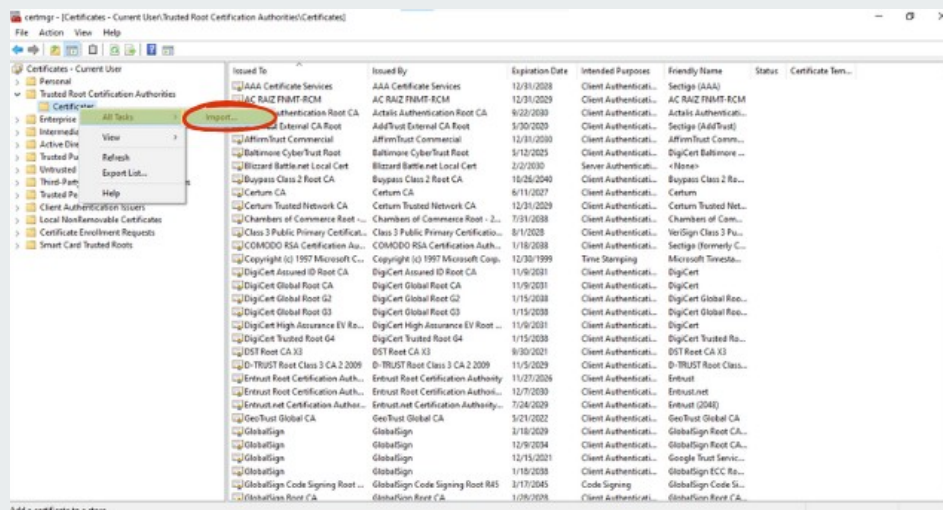


C7

INITIATE THE SB2 ROOT CERTIFICATE IMPORT

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

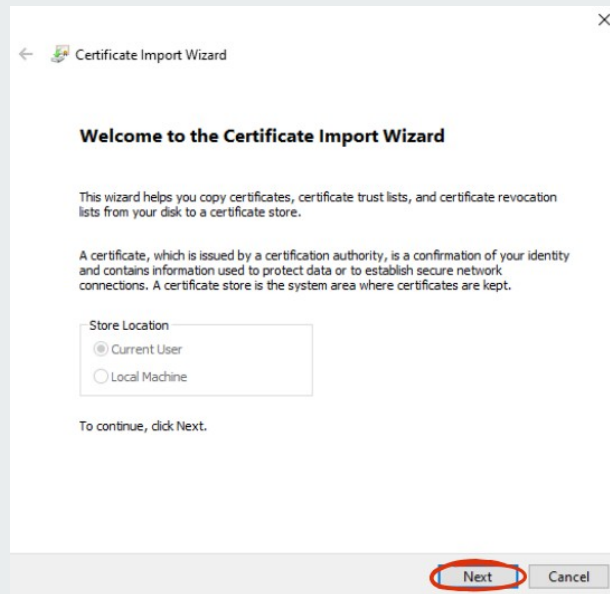
Select **All Tasks**, and click **Import** to start the Certificate Import Wizard.



C8

CERTIFICATE IMPORT WIZARD

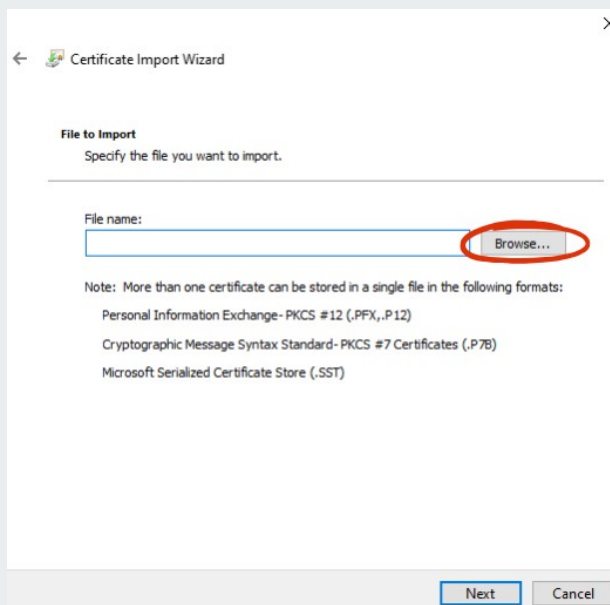
The Certificate Import Wizard will open. Click **Next** to proceed.



C9

LOCATE THE SB2 ROOT CA CERTIFICATE

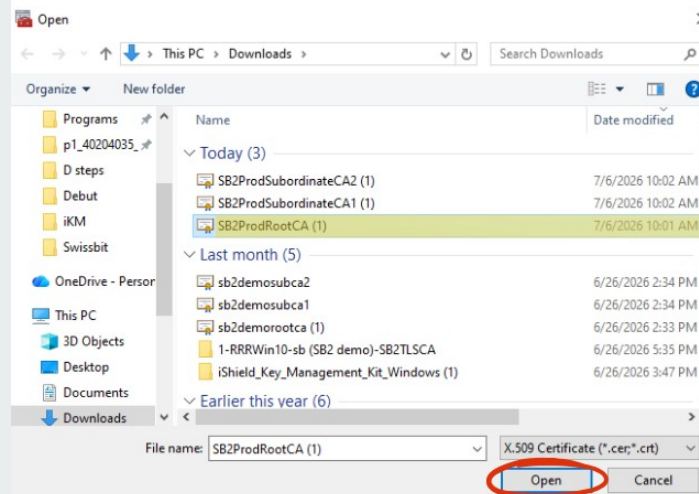
Click the **Browse** button to locate the SB2 Root CA certificate file.



C10

OPEN THE SB2 ROOT CA CERTIFICATE

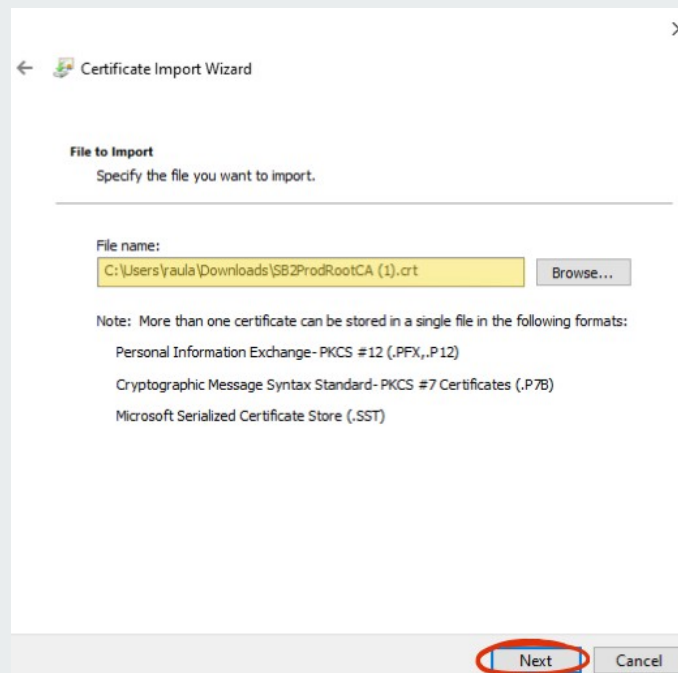
To find the SB2 Root CA Certificate, go to the **sb2prodrootCA.crt** file's location, which is typically the **Downloads** folder. Once the **sb2prodrootCA.crt** is located, select it and **click Open**.



C11

VERIFY THE SB2 ROOT CA CERTIFICATE IS SELECTED

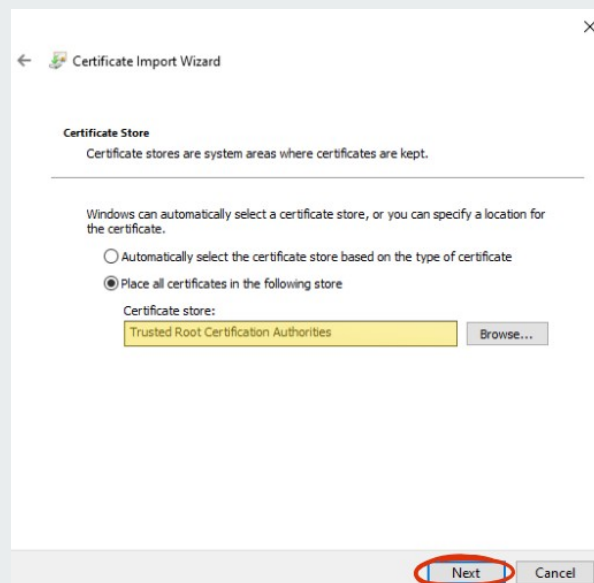
Verify the file being imported is the **sb2prodRootCA** then **click Next**.



C12

SELECT CERTIFICATE STORE

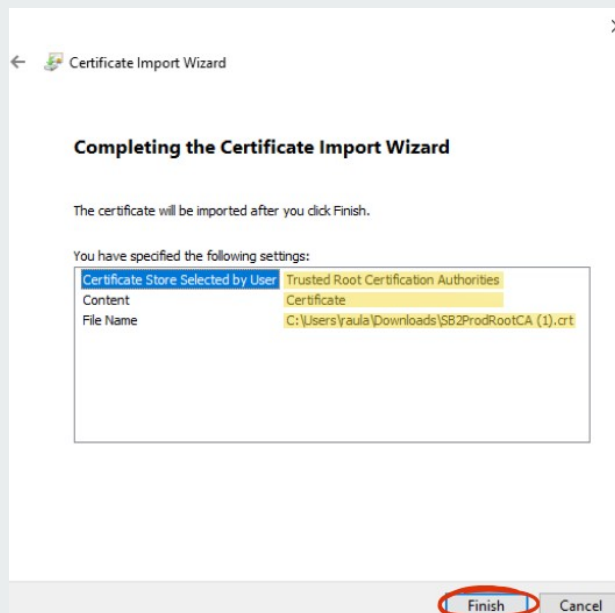
Ensure the *Certificate Store* field indicates the digital certificate will be added to the **Trusted Root Certification Authorities** store before clicking **Next** to continue.



C13

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.



C14

SECURITY THUMBPRINT

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:

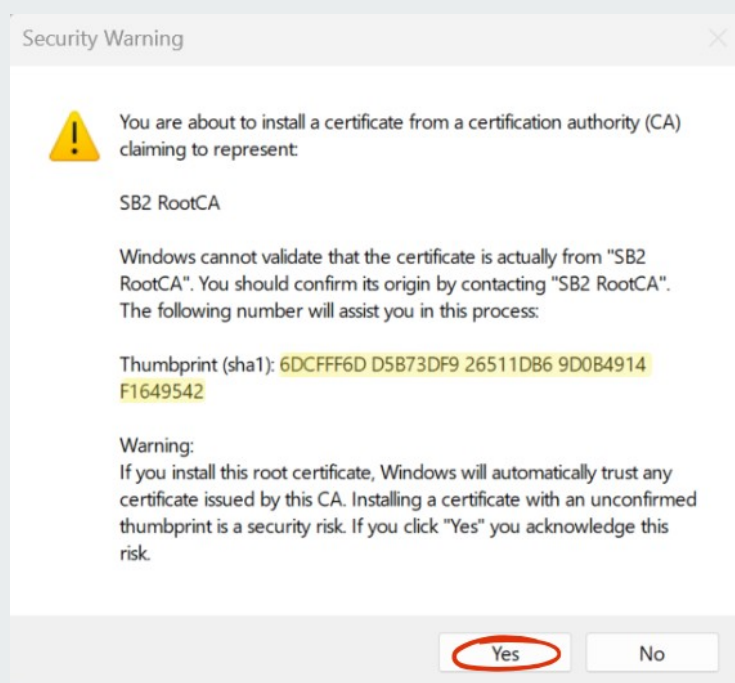
SB2 RootCA

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.



C15

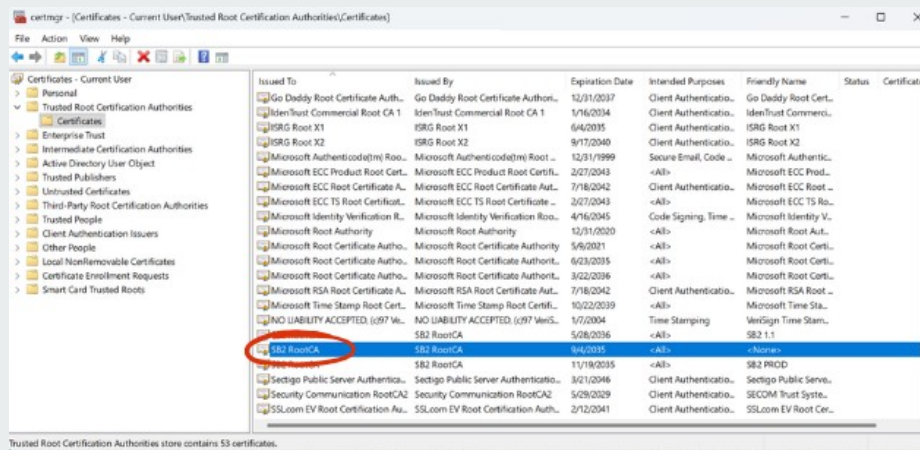
A SUCCESSFUL IMPORT

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

C16

VERIFY SB2 ROOT CA IN CERTIFICATES LIST

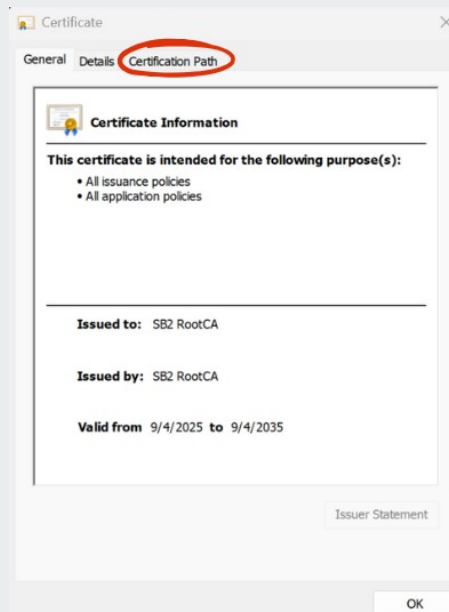
If you scroll down the list of CA certificates on the right-hand side of this window's panel, you will see the **SB2 RootCA** certificate in the list.



C17

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. Click the **Certification Path**.



C18

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.”

Ensure this icon, adjacent to the certificate name, represents a valid certificate.

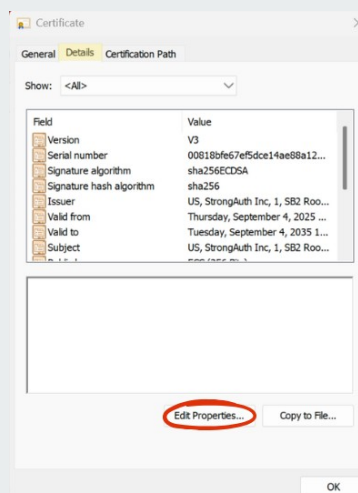


C19

ADDING A FRIENDLY NAME: PART 1

Friendly names make identifying RootCAs easier in the certificates list. Follow these steps to create a ***Friendly name*** for the SB2 Root CA:

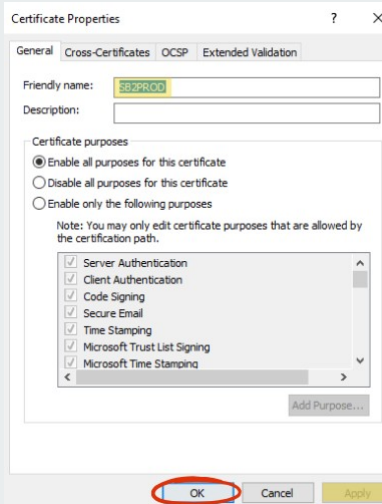
- Choose the Details tab.
- Click Edit Properties.



C20

ADDING A FRIENDLY NAME: PART 2

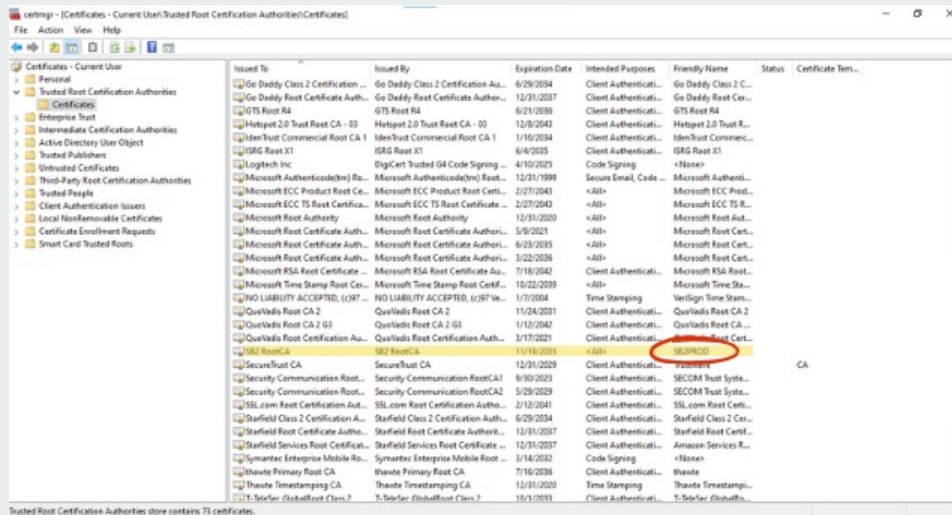
- c) Add name in **Friendly name** field.
- d) Click **Apply** then click **OK** to finish.



C21

VERIFY THE FRIENDLY NAME

Close the Certificate information window. The Friendly name field should now display SB2 DEMO.

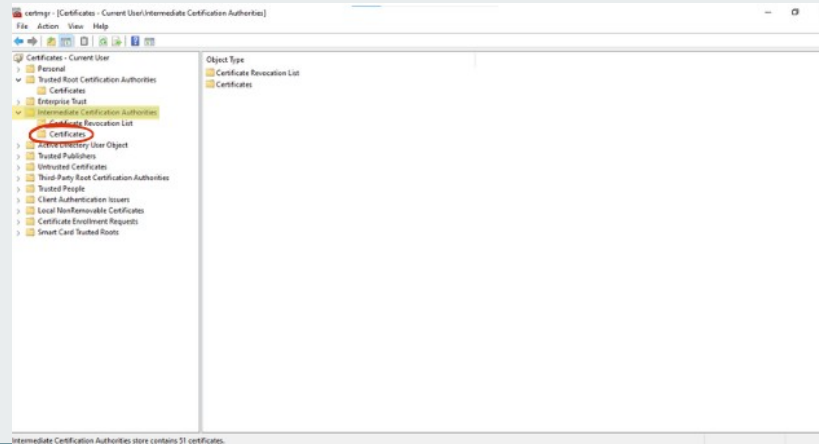


C22

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.

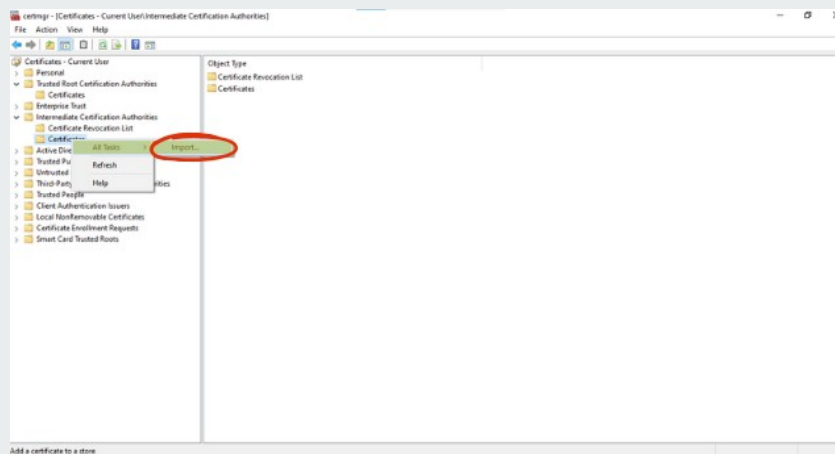
Return to the **certmgr** application. Next, click the **arrow** next to the **Intermediate Certification Authorities** folder to expand it, revealing the **Certificates** folder.



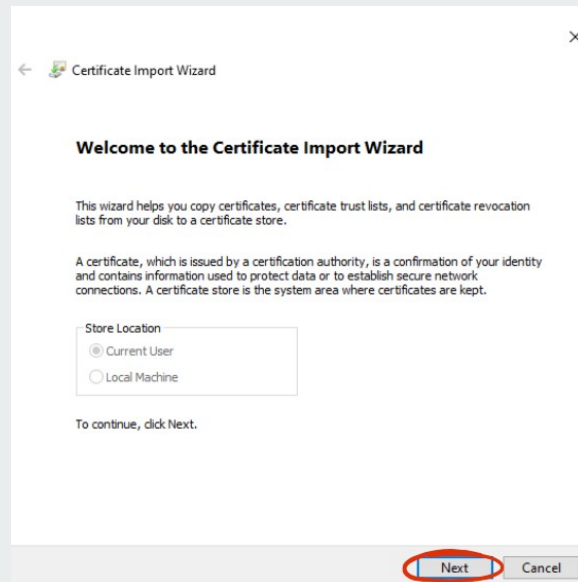
C23

INITIATING SUBORDINATE CA CERTIFICATE IMPORT

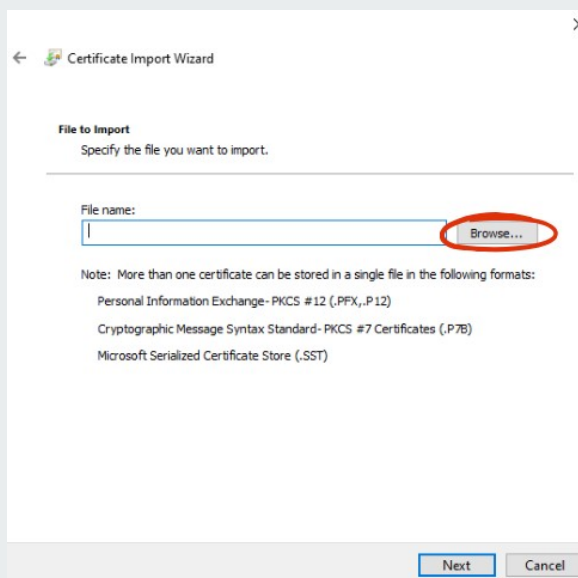
To begin, right-click the **Certificates** folder to open the context menu. From there, select **All Tasks**, and then click **Import** to start the **Certificate Import Wizard**.



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



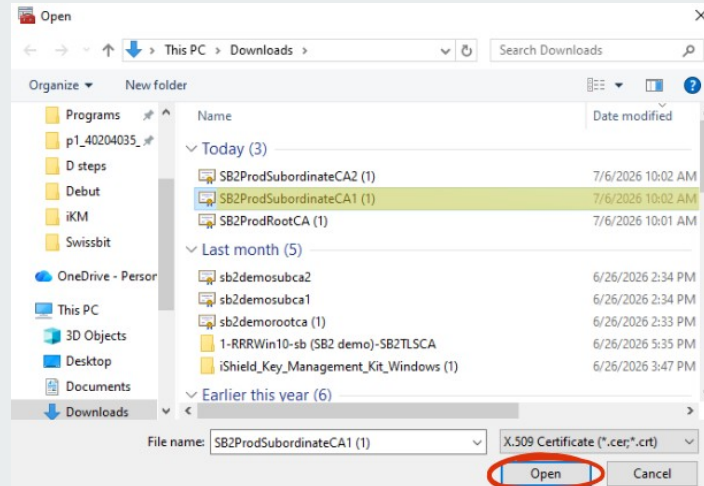
Click the **"Browse"** button to navigate to and select the Subordinate CA certificate file.



C26

OPEN THE SUBORDINATE SB2PROD CA 1 CERTIFICATE

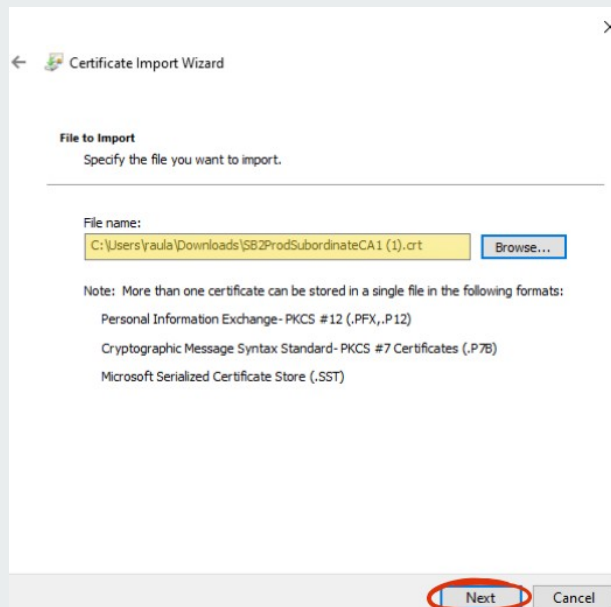
To find the **sb2prodSubCA1.crt** certificate file, go to the file's location, which is typically the Downloads folder. Once the sb2prodSubCA1.crt file is located, select it and **click Open**.



C27

CERTIFICATE VERIFICATION

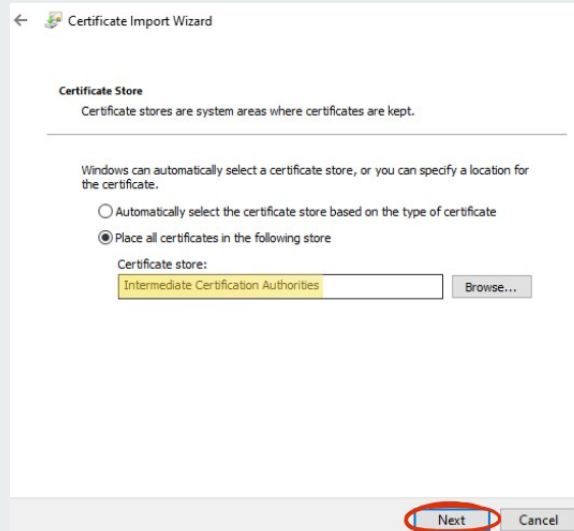
Verify the correct SB2 Subordinate CA Certificate file has been selected. The name of the file will automatically populate the File name field upon selection. **Click Next** to continue.



C28

SELECTING CERTIFICATE STORE

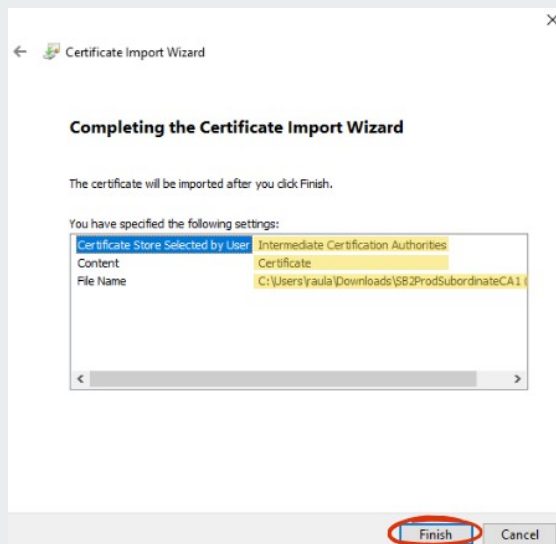
Choose “Place all certificates in the following store” and ensure the certificate is added to the **Intermediate Certification Authorities** certificate store. Click **Next** to continue.



C29

FINISH IMPORTING THE CERTIFICATE

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



C30

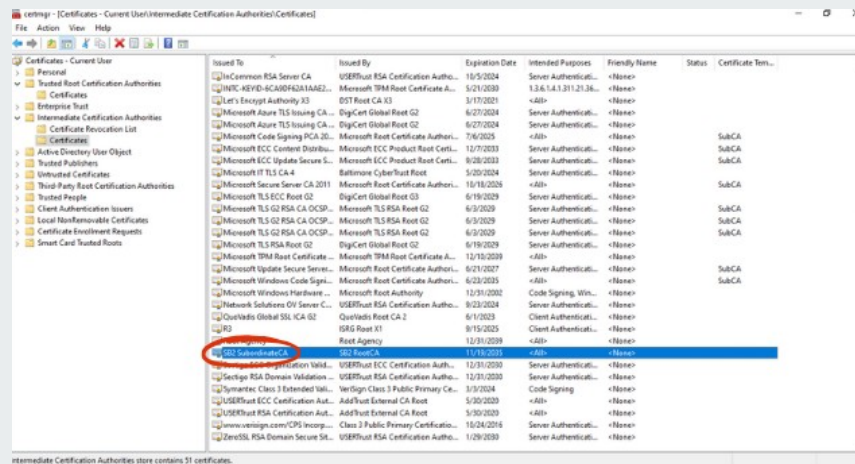
A SUCCESSFUL IMPORT

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

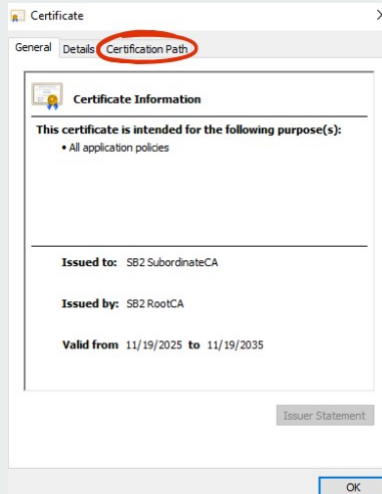
C31

VERIFY SB2 SUBORDINATE CA 1 IS IN CERTIFICATES LISTS

Once the SB2 Subordinate CA 1 certificate is successfully imported, it will appear in the Intermediate Certification Authorities list.



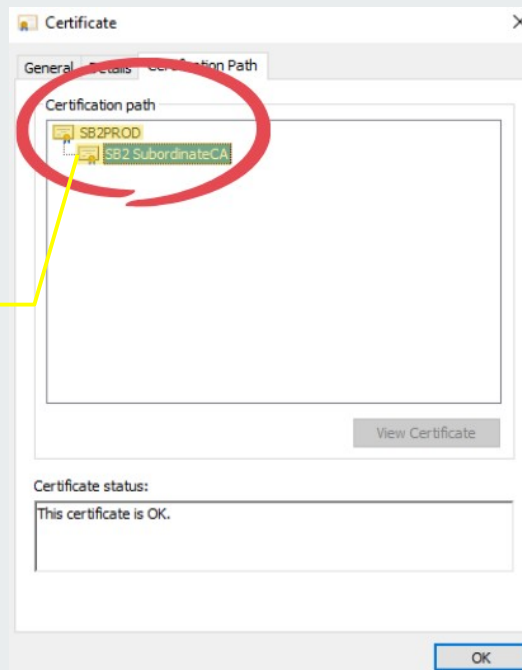
By double-clicking the **SB2 Subordinate CA** certificate – or **right-clicking** the mouse button and selecting **Open**, you should see the following window. Click the **Certification Path** tab.



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.”**

Ensure the two certificates are chained and the adjacent icons represent valid certificates.



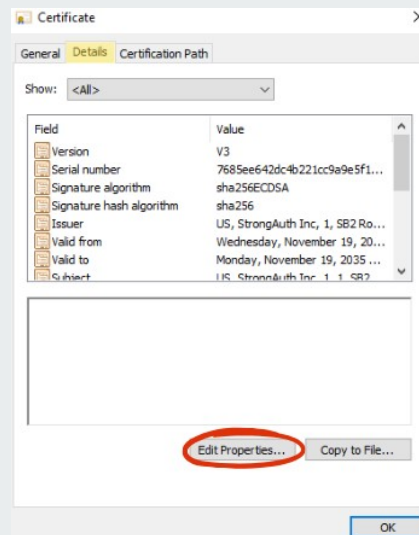
C34

ADDING A FRIENDLY NAME: PART 1

Friendly names make identifying **SubordinateCAs** easier in the certificates list.

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

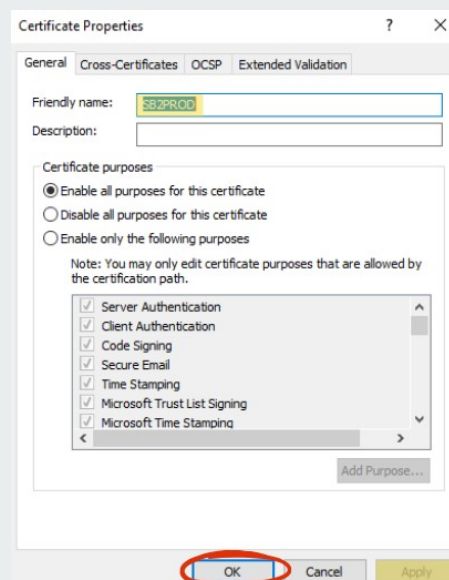
- Choose the Details tab.
- Click Edit Properties.



C35

ADDING A FRIENDLY NAME: PART 2

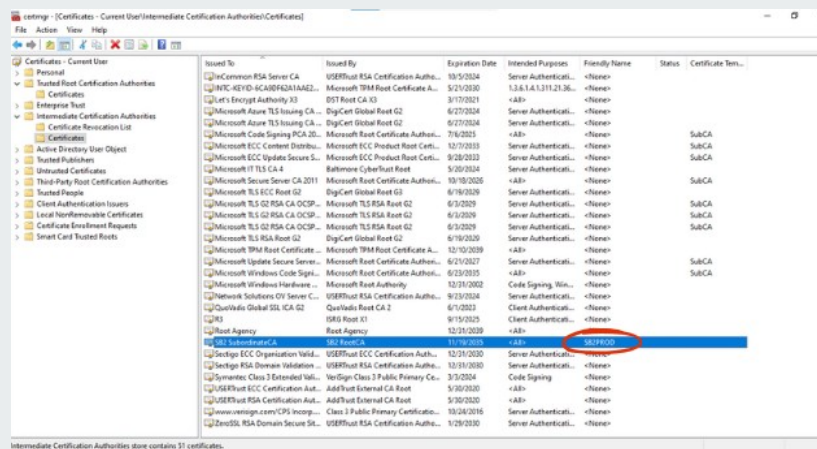
- Add name in **Friendly name** field.
- Click **Apply** then click **OK** to finish.



C36

VERIFY THE FRIENDLY NAME

Close the Certificate information window. The **Friendly name** field should now display SB2PROD.



C37

IMPORT THE SB2 SUBORDINATE CA 2 CERTIFICATE

Import the SB2 Subordinate CA 2 certificate by repeating steps [C22 – C36](#). Remember to verify the Sub CA 2 certificate is selected during the process.

C38

RESTART THE COMPUTER

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

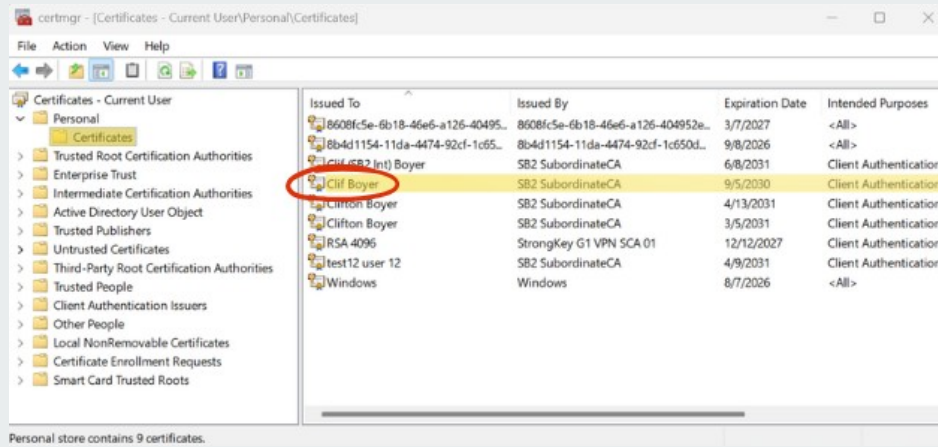
- Save** all open work and close all active applications to prevent data loss.
- Leave** your Security Key (issued by the SB2 site) plugged into the USB port;
- Restart** your computer.

C39

VERIFY YOUR PERSONAL CERTIFICATE - PART 1

Follow these steps to open a Personal Certificate:

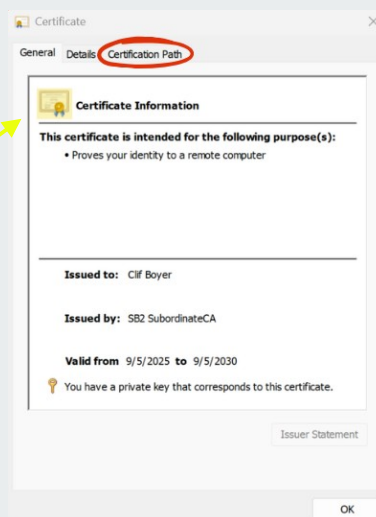
- Open **certmgr** and navigate to the **Personal** folder.
- Click the **arrow** next to the folder to expand it and reveal the **Certificates** subfolder.
- Select an **SB2 Subordinate CA** certificate.
- Double-click** the certificate to open it.



C40

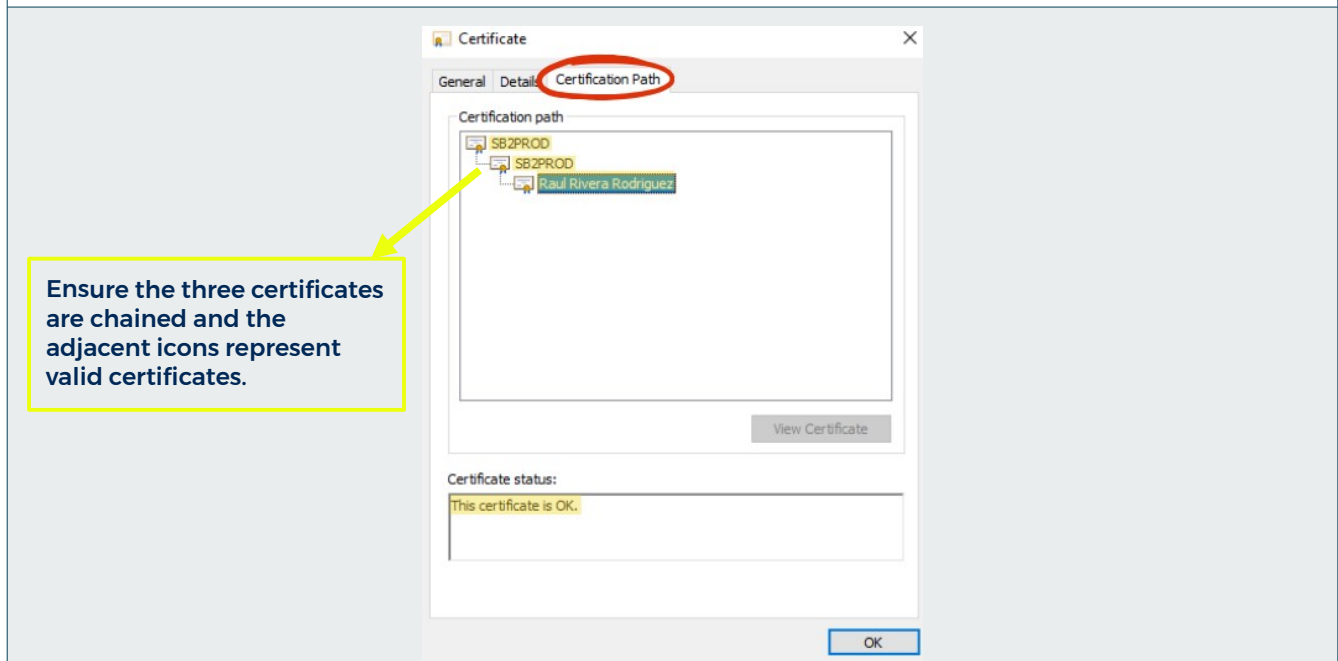
VERIFY YOUR PERSONAL CERTIFICATE - PART 2

Verify that a **certificate** icon appears next to the **Certificate Information** heading, then click the **Certification Path** tab.



Ensure this icon, adjacent to the certificate name, represents a valid certificate.

Verify that a **chain-of-trust** has been established, ending with your **named certificate**. Confirm that the **Certificate status** displays: **The Certificate is OK**.





SECTION D

D1

ACCESSING AN 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.

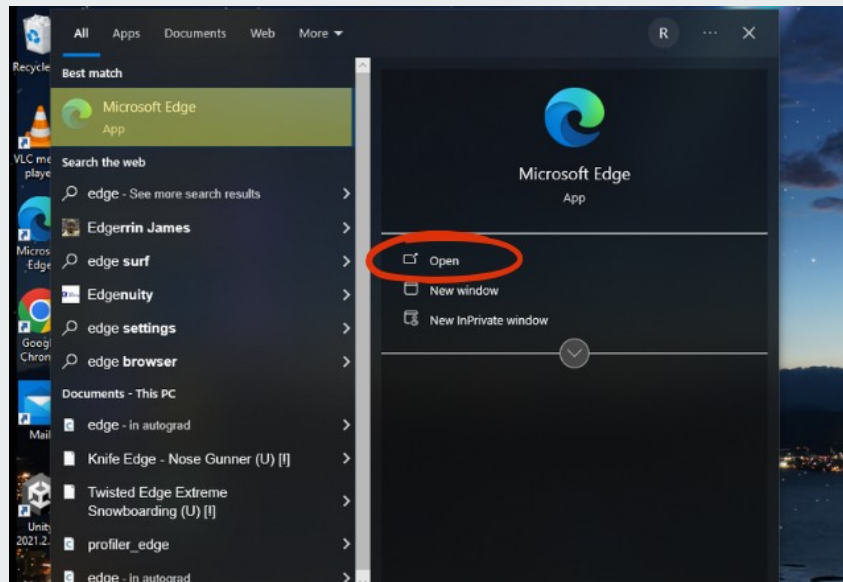
The provided USB adapter pictured below.



D5

OPEN THE EDGE BROWSER

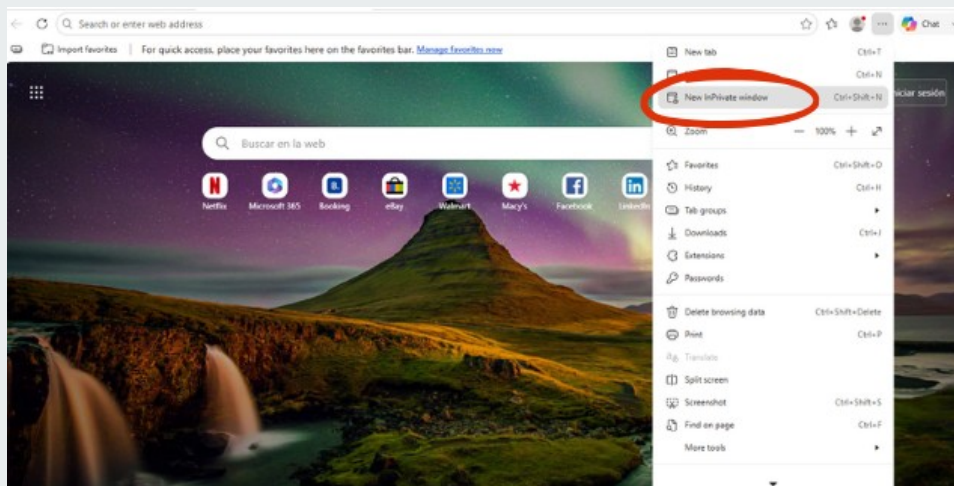
Open the Edge browser.



D6

FIND THE EDGE BROWSER DROP DOWN MENU

Click the three-dot icon in the upper-right corner. Then, select New InPrivate window from the drop-down menu. Always use Edge InPrivate mode to access the SB2PROD platform URL <https://sb2.strongkey.com>.



D7

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 SB2PROD 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=7db88e3055d49b105fca14f2f18a7059d52ef02a9c93cc13a85fd701a1143c1a>

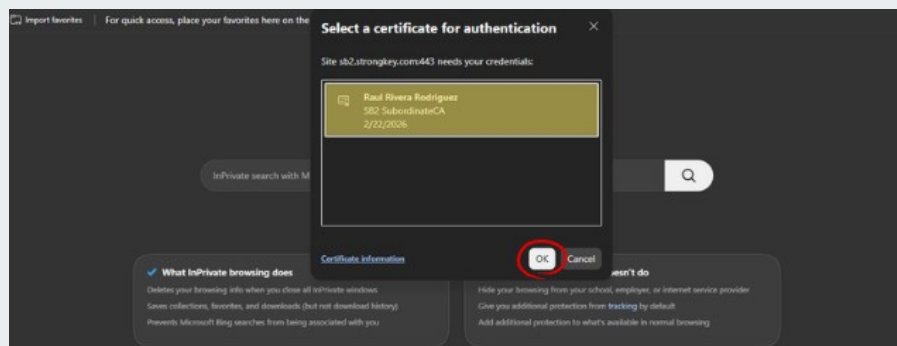
D8

SELECT THE CERTIFICATE

A pop-up window will display the available certificates. The name in the prompt should match your name, as created by the Administrator of the SB2PROD site. Select the presented certificate and **click OK** to proceed.

NOTE

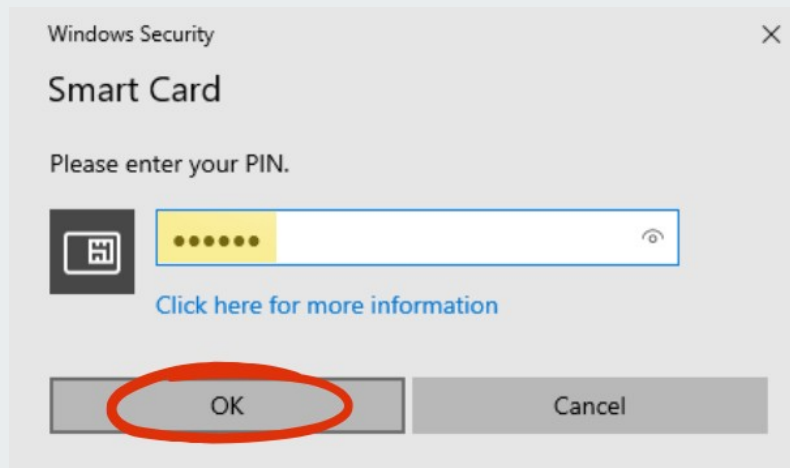
You will only see a certificate prompt if the **SB2 Root CA** and **SB2 Subordinate CA** certificates were imported correctly on your computer. If you do **NOT** see a certificate prompt, please contact support@strongkey.com for help.



D9**ENTER SECURITY KEY PIN**

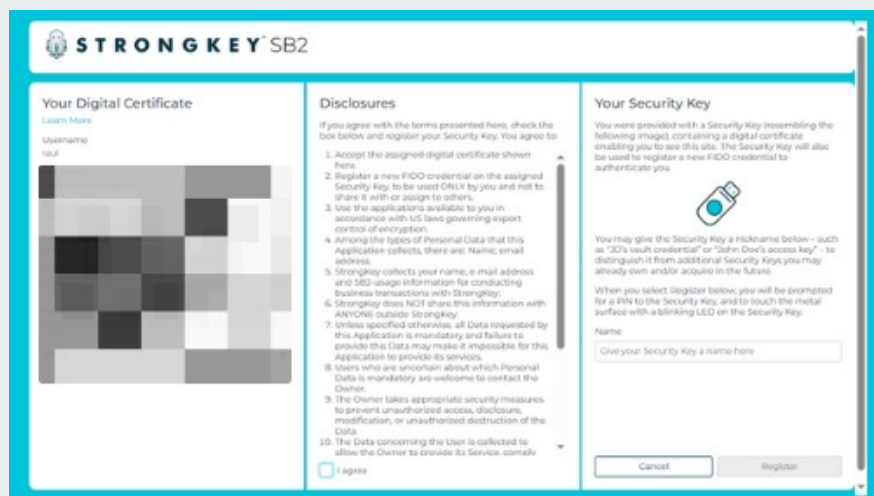
The next dialog box will prompt for the YubiKey 5C NFC's PIN. Enter and click OK to continue. This PIN should have been provided to you by the Administrator of the SB2 site.

For instructions on changing the PIN, refer to the [Appendix](#) of this guide.



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 will be displayed (Critical details have been redacted to protect privacy.).
- Legal disclosures for the SB2 platform are located in the middle section. You must agree to the terms disclosed before continuing with this process.
- Use the right-hand panel to nickname your Security Key. This makes it easier to identify each key if using more than one.



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

D12

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 shows a two-pane interface. The left pane contains a list of terms (10-12) regarding data management and user profiles. The right pane is titled 'You may give the Security Key a nickname below...' and includes a text input field with the placeholder 'sb2PROD.DOCUMENTATION'. Below the input field are 'Cancel' and 'Register' buttons. The 'Register' button is highlighted with a red circle.

D13

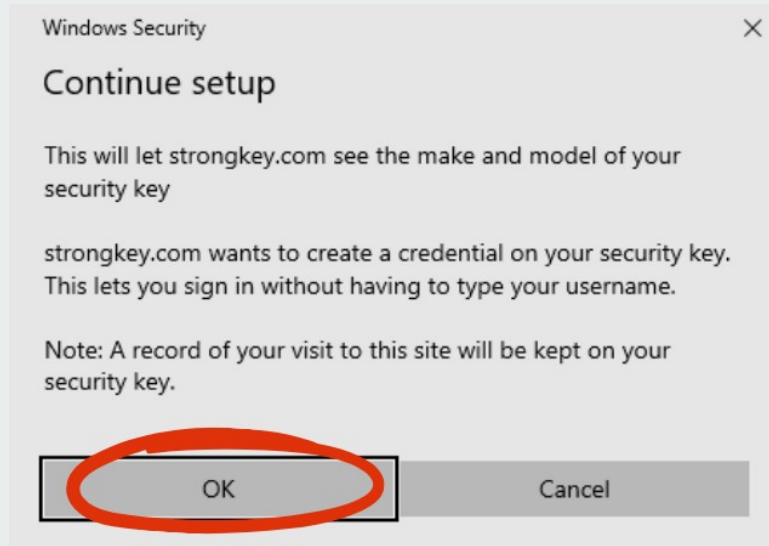
SECURITY KEY SETUP

Click OK.

The screenshot shows a 'Windows Security' dialog box titled 'Security key setup'. The text inside reads: 'Set up your security key to sign in to strongkey.com as rrrwin10yk@strongkey.com. This request comes from Msedge, published by Microsoft Corporation.' At the bottom, there are 'OK' and 'Cancel' buttons. The 'OK' button is highlighted with a red circle.

D14**CONTINUE SETUP**

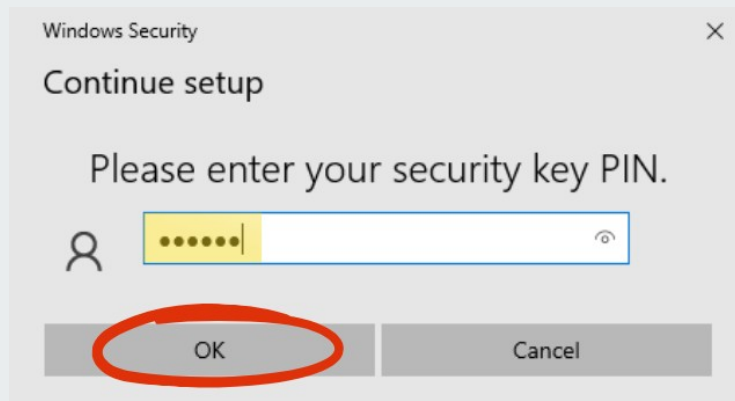
Click OK.

**D15****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.

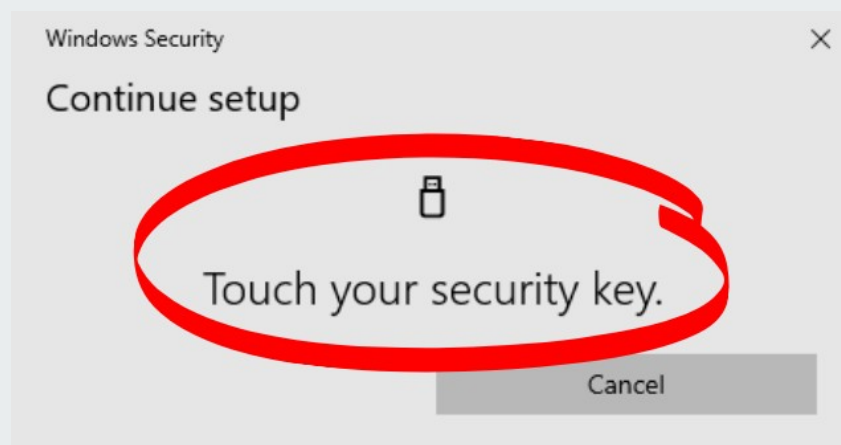


D16**TOUCH THE SECURITY KEY**

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

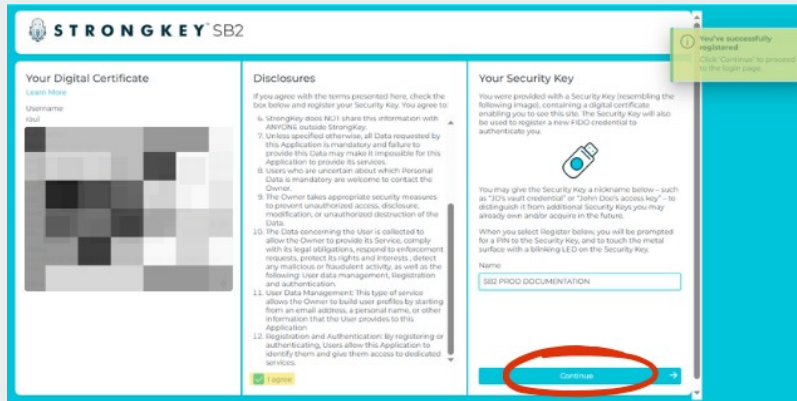
This step is called the “Test of User Presence” (TUP) in the FIDO ecosystem. It ensures that no remote attacker can impersonate you, because they would need both your Security Key and your physical interaction at your computer. Each time you use your FIDO credential to sign in to the SB2 platform, you’ll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



D17

REGISTRATION CONFIRMATION

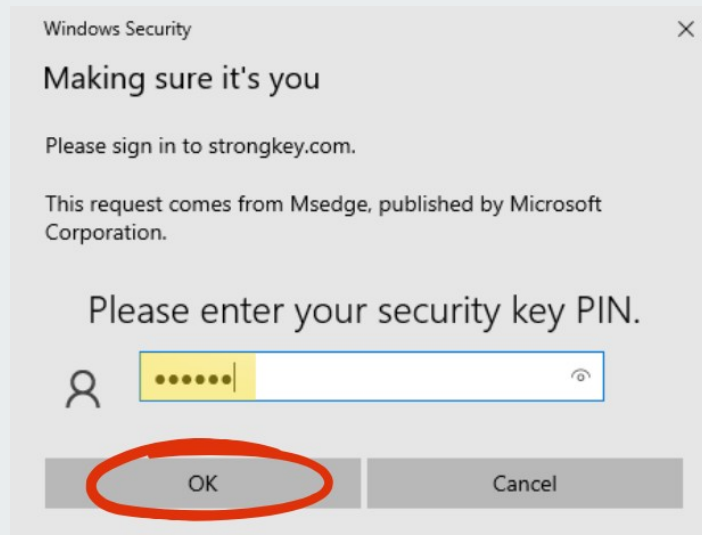
Upon successfully adding the credential, a dialog box will confirm the registration action. Click **Continue** to sign-in to the SB2 platform.



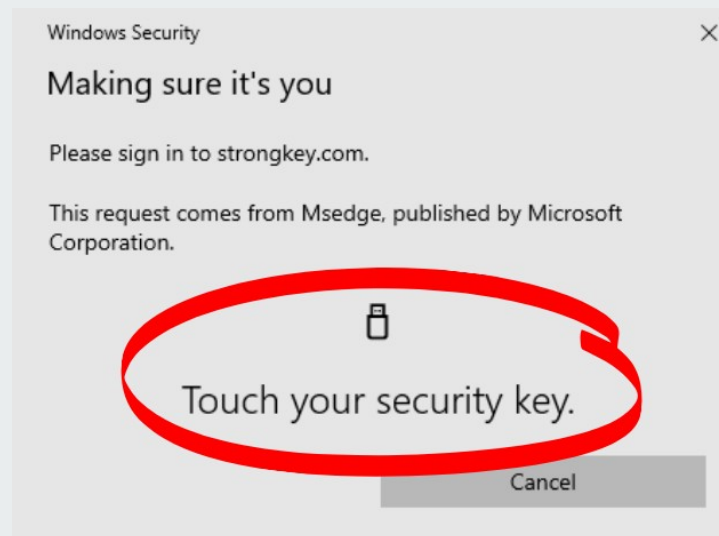
D18

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**.



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.



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:

- **StrongKey CryptoCabinet (SKCC):** For securely storing and sharing encrypted files containing sensitive data.
- **StrongKey Content Distribution (SKCD):** For storing and sharing digitally signed, unencrypted documents.
- 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.





APPENDIX

I

CHANGING PERSONAL IDENTIFICATION NUMBERS (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.

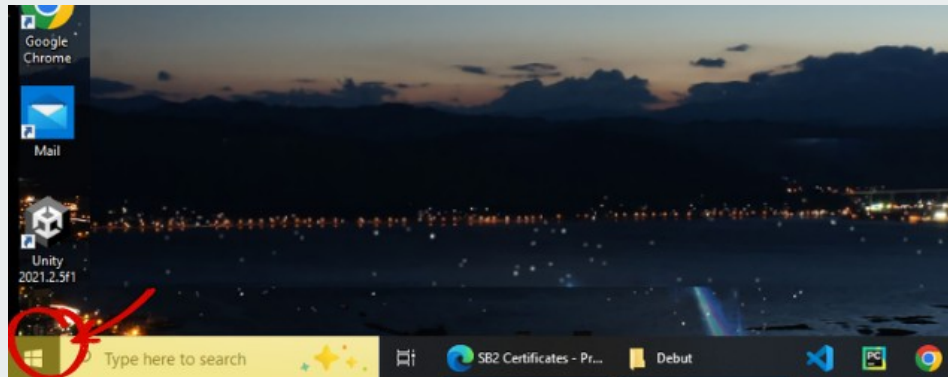
However, StrongKey recommends using the SAME PIN for both containers of the **Security Key** to reduce the burden on users. As long as the **Security Key** is safely in the possession of the legitimate user, and the legitimate user is NOT sharing the PIN to the **Security Key** with anyone, the user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

OPENING THE YUBICO AUTHENTICATOR APPLICATION

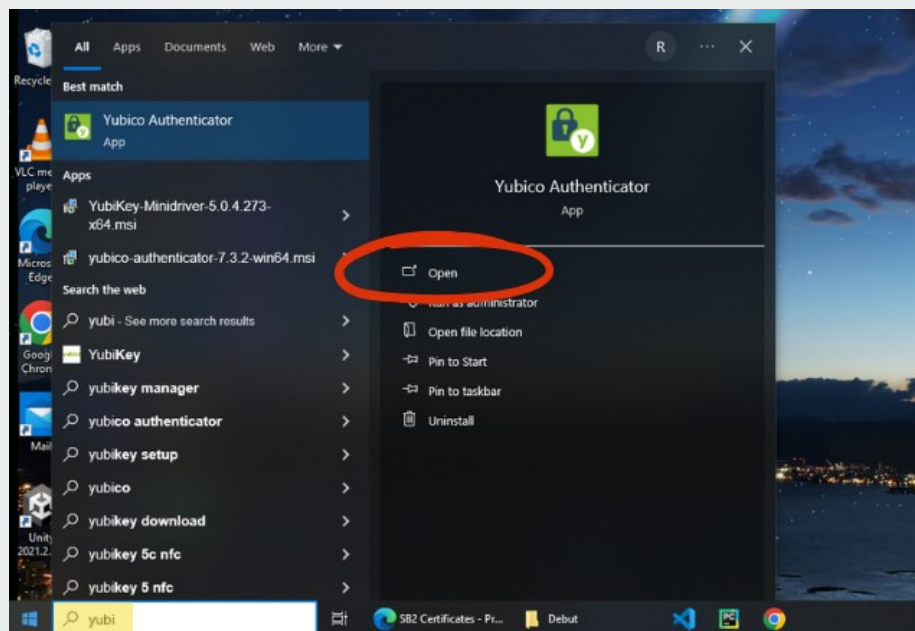
To begin, access the Yubico Authenticator application by clicking the **Windows start icon** from the Windows taskbar.



AP3

SELECT YUBICO AUTHENTICATOR

Search for **Yubico Authenticator** and click **Open** when it appears.



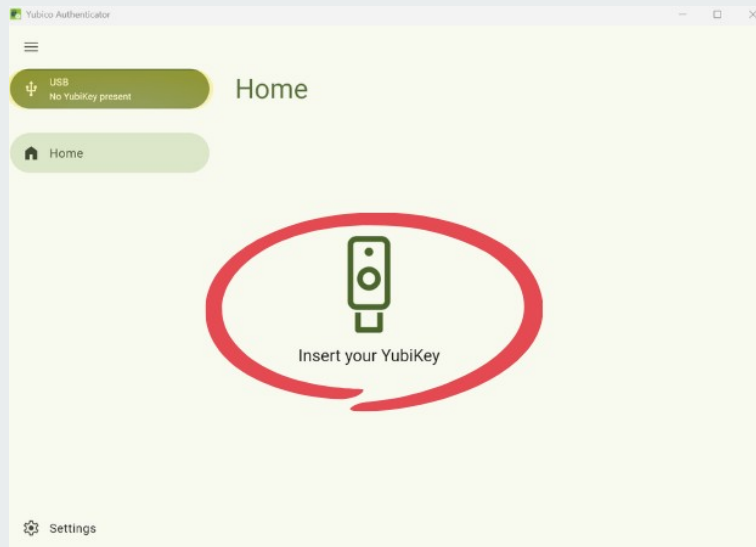
AP4

THE YUBICO AUTHENTICATOR APPLICATION

When you open the application, it displays the messages '**No YubiKey present**' and '**Insert Your YubiKey**'.

NOTE

If the '**No YubiKey present**' message is not visible, expand the application window to ensure all navigation options are clear.



AP5

INSERT THE YUBIKEY 5C NFC

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

AP6

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.



AP7

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.

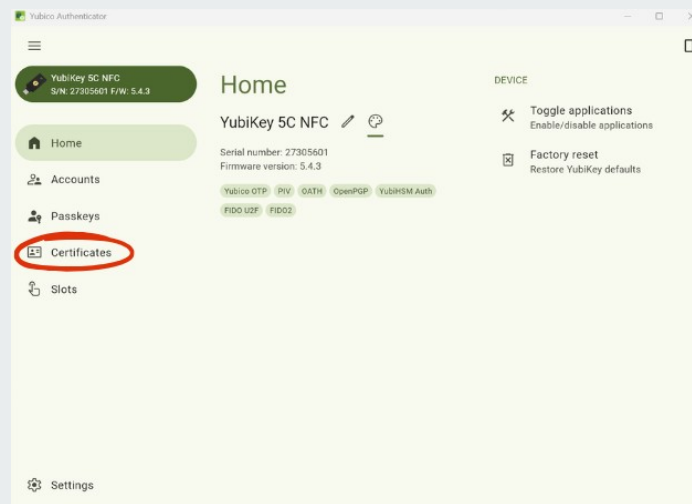
The provided USB adapter pictured below.



AP8

CHANGING THE DIGITAL CERTIFICATE PIN

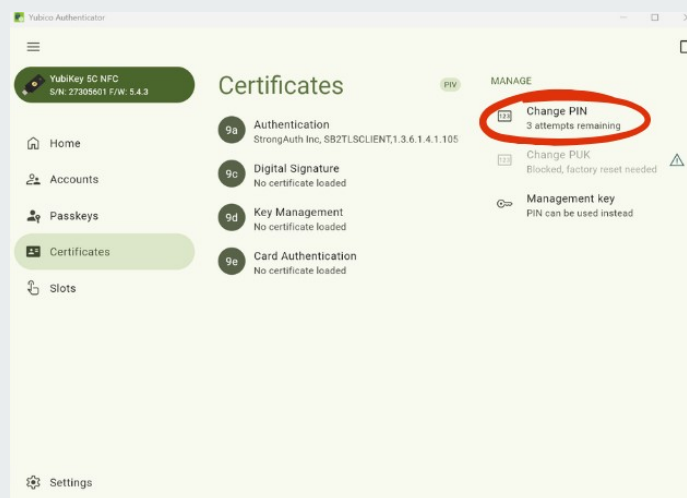
Plugging in the key loads the home screen. Navigate to the left and click the **Certificates** icon from the menu.



AP9

CHANGE PIN

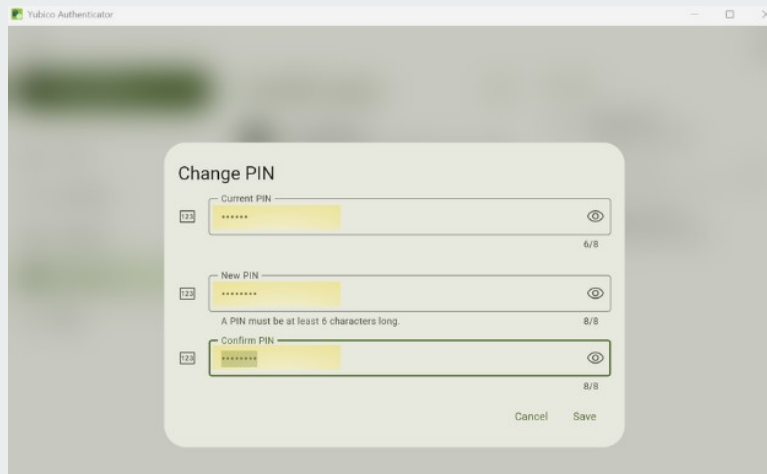
Select the **Change PIN** option from the **Manage** menu on the right.



AP10

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.

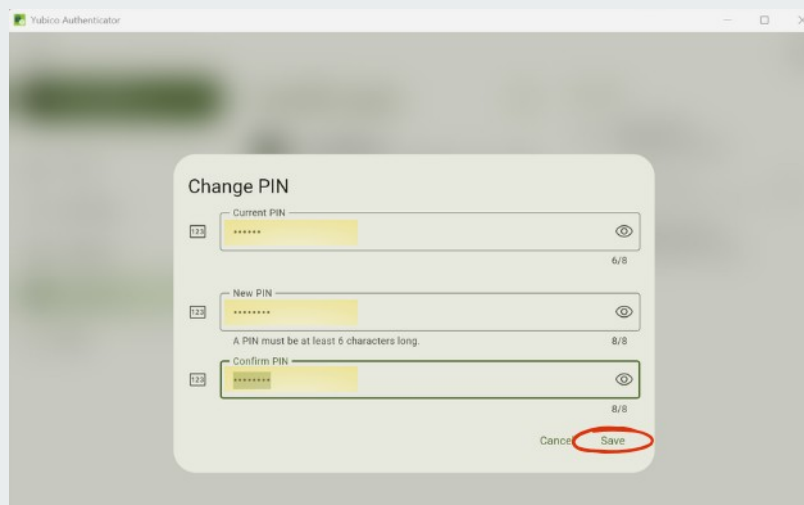


The screenshot shows the 'Yubico Authenticator' application window. In the center is a 'Change PIN' dialog box. It contains three input fields: 'Current PIN', 'New PIN', and 'Confirm PIN'. Each field has a yellow progress bar and a character count (6/8). The 'Current PIN' field is filled with asterisks. The 'New PIN' field is also filled with asterisks, and a message below it states 'A PIN must be at least 6 characters long.' The 'Confirm PIN' field is filled with asterisks. At the bottom right of the dialog box are 'Cancel' and 'Save' buttons.

AP11

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.



This screenshot is identical to the one in AP10, showing the 'Change PIN' dialog box. However, the 'Save' button at the bottom right is circled in red, indicating it is the button to be clicked.

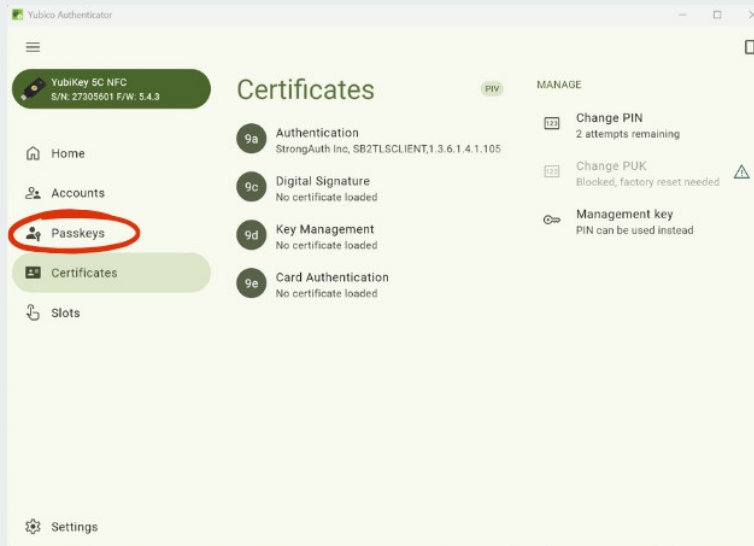
AP12

CHANGING THE FIDO CREDENTIALS PIN

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

NOTE

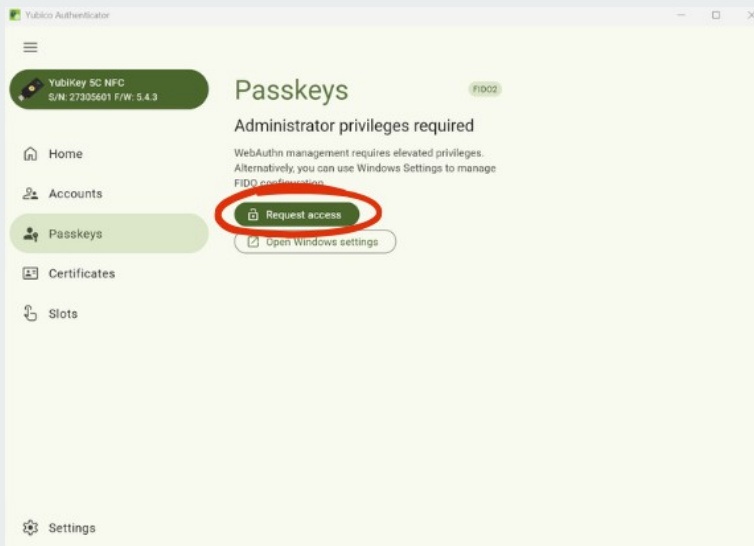
StrongKey recommends using the same PIN for the Security Key.



AP13

PASSKEYS MENU

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



AP14

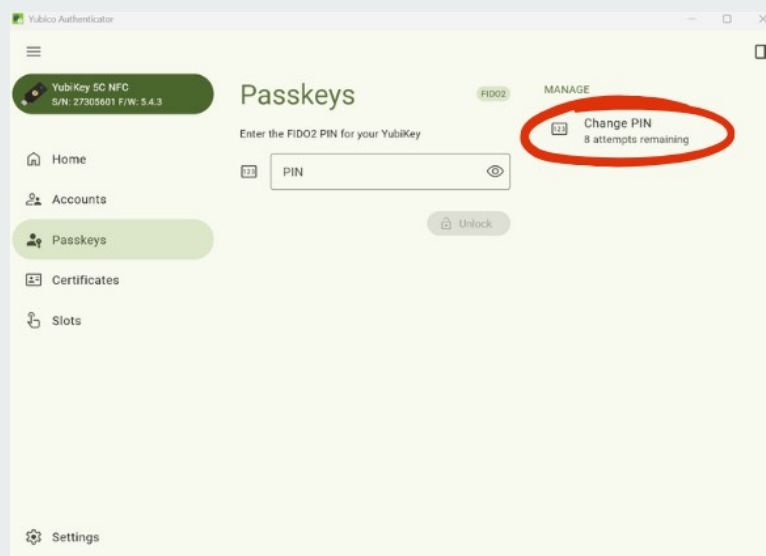
YUBICO AUTHENTICATOR APPLICATION PERMISSION

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

AP15

CHANGE PIN OPTION

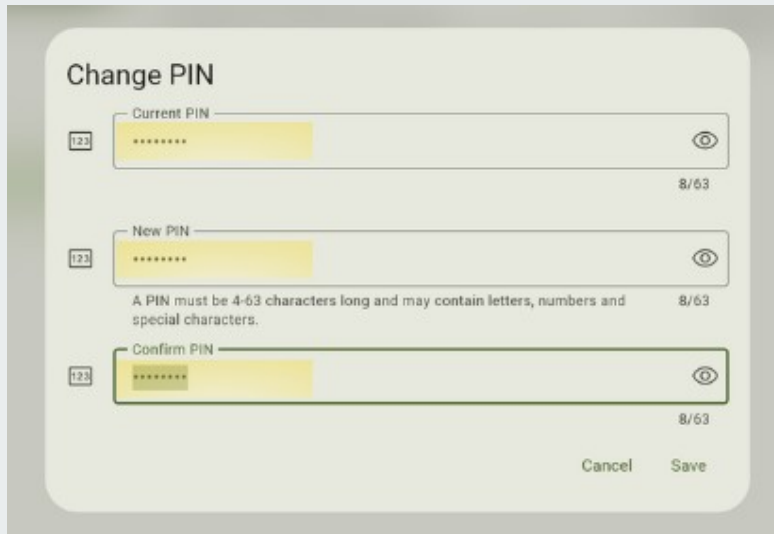
Select the **Change PIN** option located on the right of the screen.



AP16

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.



Change PIN

Current PIN 8/63

New PIN 8/63

A PIN must be 4-63 characters long and may contain letters, numbers and special characters.

Confirm PIN 8/63

Cancel Save

AP17

SUCCESS!

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

