



STRONGKEY TELLARO SB2

The Yubico Yubikey 5C NFC User's Guide for macOS

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

THE YUBIKEY 5C NFC AND THE SB2 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

II

PREREQUISITES

- macOS 13 and above
- Safari 26.0.1
- 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	Importing SB2 Root CA & SB2 Subordinate CA Certificates into macOS Keychain Access	6
C	Accessing an SB2PROD Invitation Link URL	17
AP	Appendix: Changing a Yubico YubiKey 5C NFC Personal Identification Number (PIN)	31



SECTION A

A1

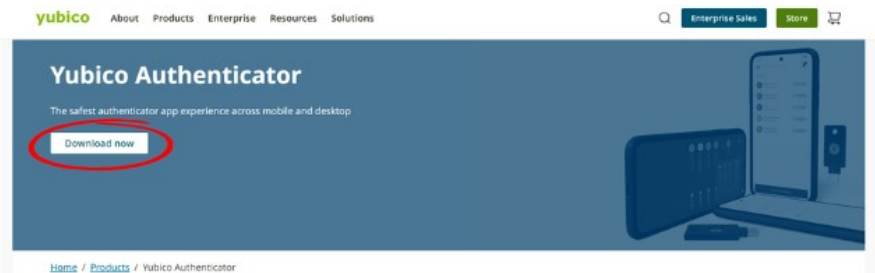
INSTALLING THE YUBICO AUTHENTICATOR APPLICATION

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

A2

DOWNLOAD YUBICO AUTHENTICATOR APPLICATION

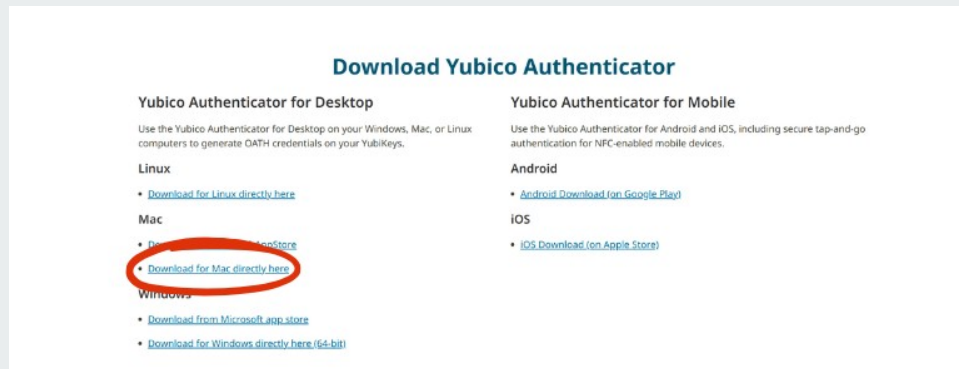
Download the Yubico Authenticator for macOS systems from <https://www.yubico.com/products/yubico-authenticator/#h-download-yubico-authenticator>. Click **Download now**.



A3

WINDOWS YUBICO AUTHENTICATOR APPLICATION

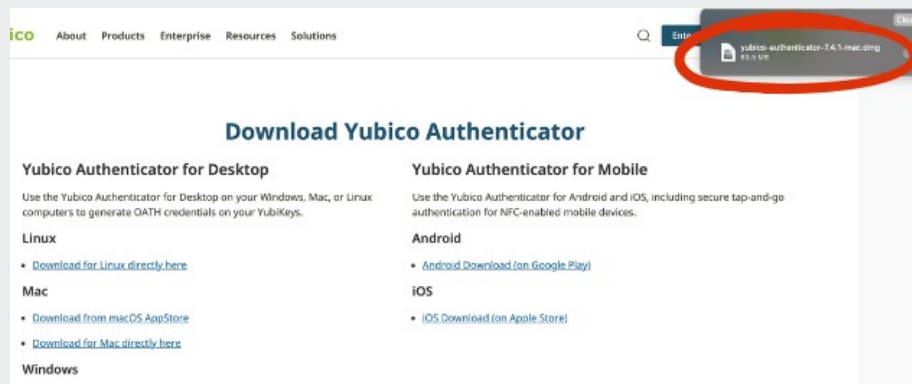
Select Download for Windows directly here (64-bit). **Click it to start download.**



A4

OPENING THE YUBICO AUTHENTICATOR APPLICATION

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



A5

MOVE AUTHENTICATOR APP TO THE APPLICATIONS FOLDER

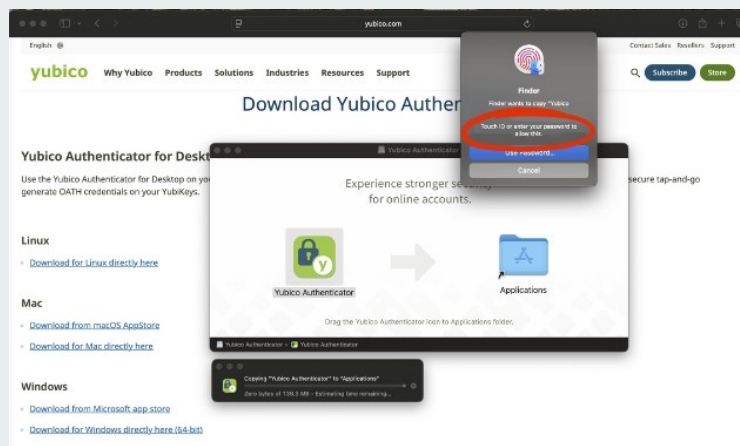
When the installer window appears, Drag the Yubico Authenticator icon to the Applications folder.



A6

AUTHENTICATE TO COMPLETE INSTALLATION

After dragging the **Yubico Authenticator** application to the **Applications** folder, macOS will prompt for **TouchID** or **Mac Account Password** to continue and complete the installation.





SECTION B

B1

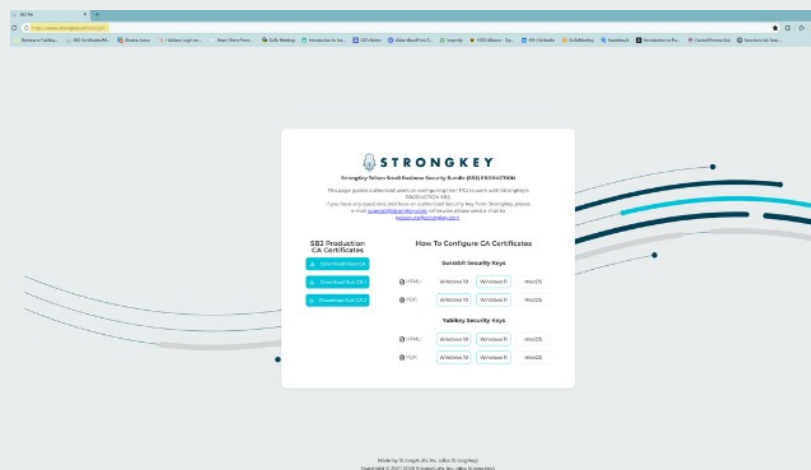
IMPORTING SB2 ROOT CA & SB2 SUBORDINATE CA CERTIFICATES ON macOS KEYCHAIN ACCESS

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.

B2

ACCESS THE SB2PKI PAGE

All required CA certificates are available for download from the SB2PKI page at <https://www.strongkey.com/sb2pki>.



B3

SB2 CA CERTIFICATES

Next, download the three SB2 Production CA certificates from the left side of the page.

NOTE

Download the certificates starting with the Root CA.

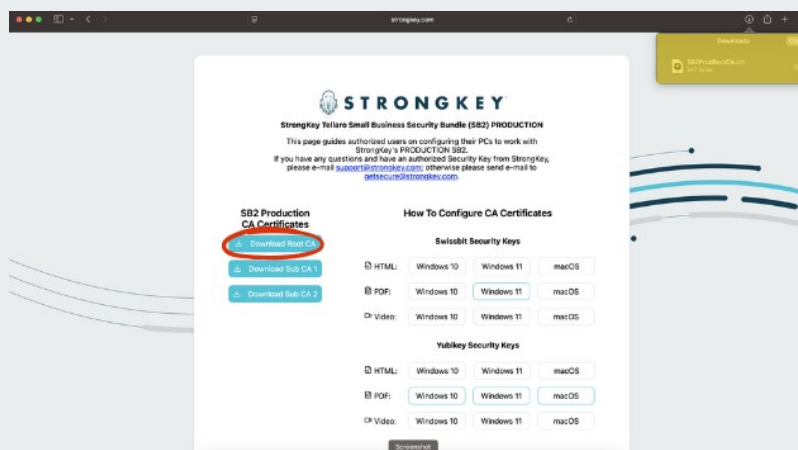


B4

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.

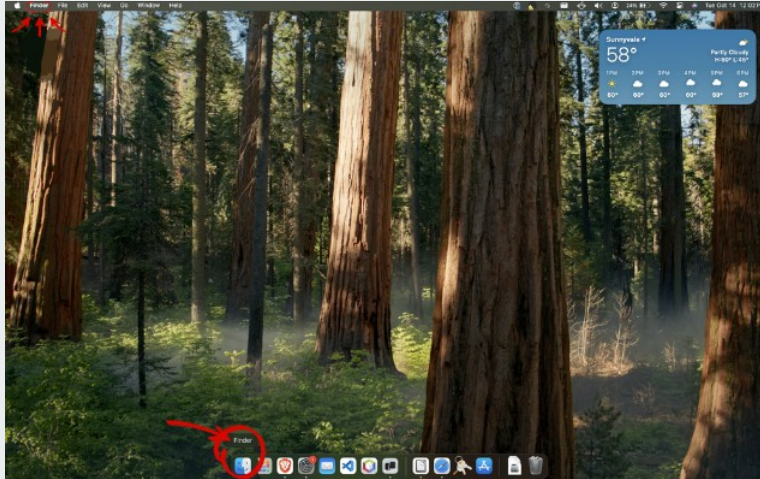
REPEAT this process for the Sub CA 1 and Sub CA 2 certificates.



B5

ACCESS macOS FINDER

To get started installing the certificates, open the **Finder** application by clicking its icon in the **Dock** or by selecting it from the menu in the upper left corner of your screen.



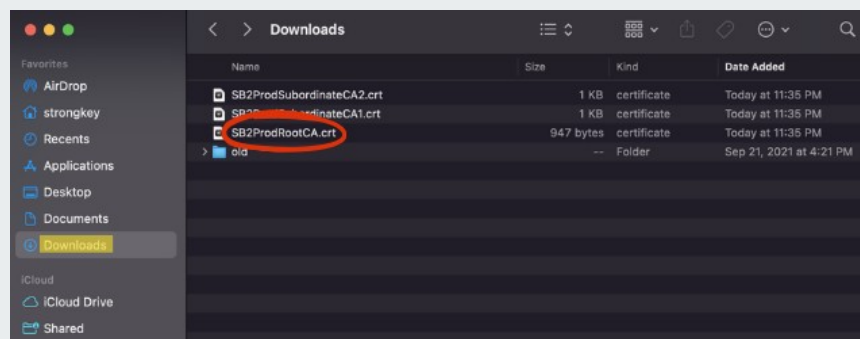
B6

LOCATE DOWNLOADED SB2 ROOT CA FILE

Navigate to the **Downloads** folder in **Finder**. Locate the **SB2 Root CA** file and **right-click** it.

NOTE

Please note that your specific **SB2 certificate** files may have a different name. Ensure you know the correct file name before proceeding.



Launch **Keychain Access** by searching with **Spotlight** [⌘ + Space] (refer to Image 1), or by navigating to **Applications** in **Finder** (see Image 2).

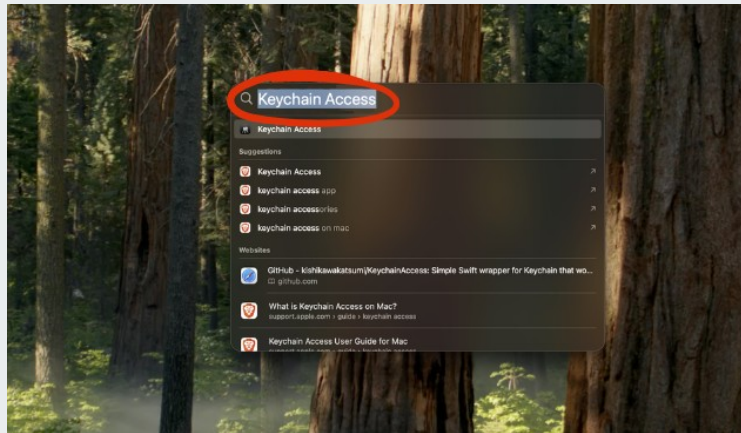


Image 1

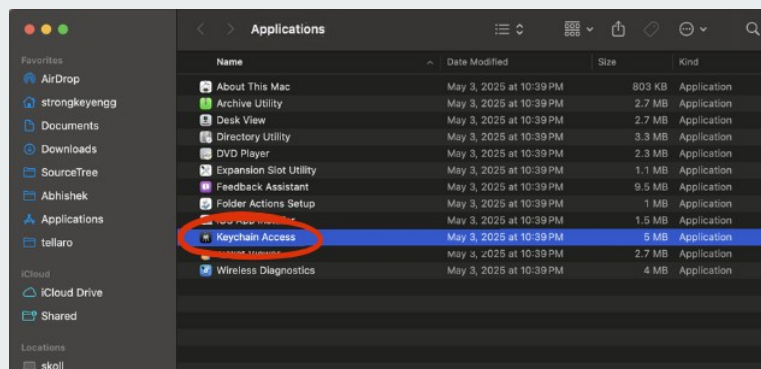
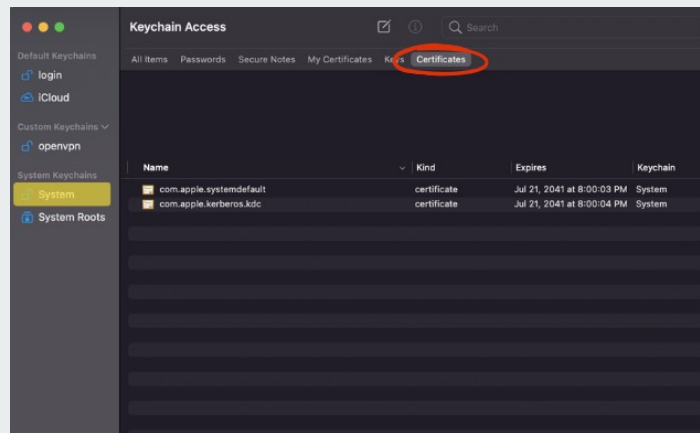


Image 2

B8

NAVIGATING IN THE KEYCHAIN ACCESS APPLICATION

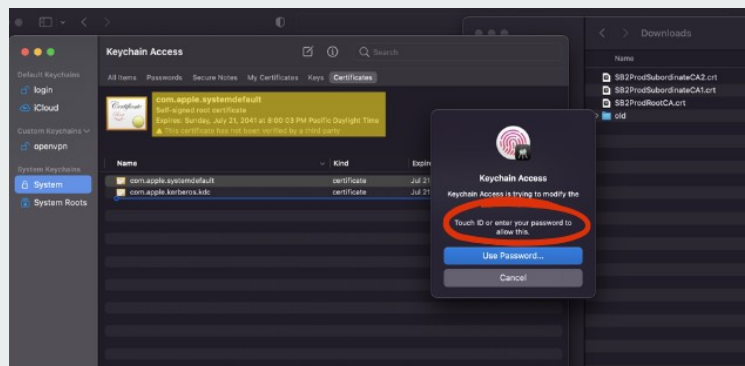
After launching the **KeyChain Access** application, the following screen appears. Select **System** in the sidebar, followed by **Certificates** in the top menu.



B9

IMPORTING CERTIFICATES

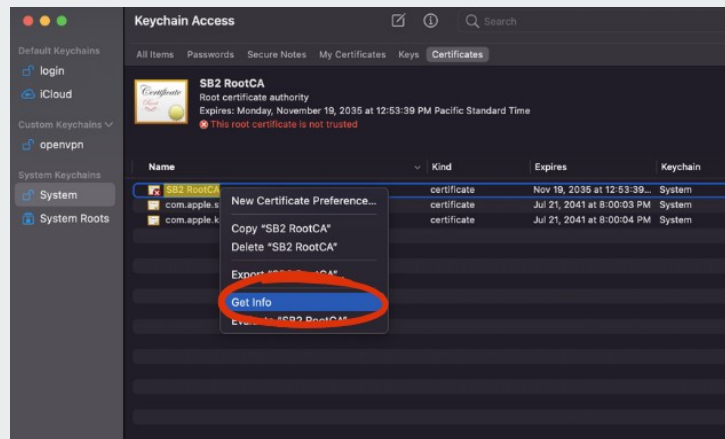
Next, drag the **Root Certificate** into the **Keychain Access** window to begin the certificate import process. The macOS will prompt you to authenticate using Touch ID or an account password to complete the import.



B10

ACCESS THE SB2 ROOTCA CERTIFICATE

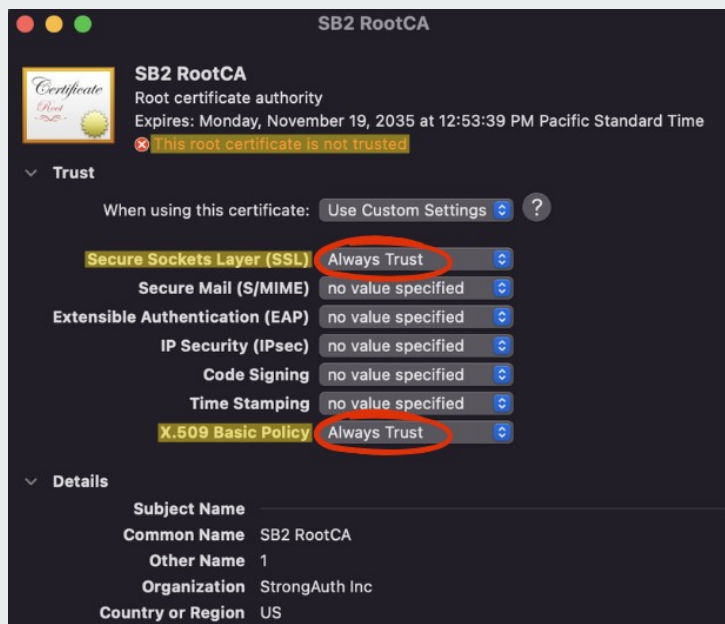
Right-click on the imported **SB2 RootCA** certificate, then select **Get Info** to view its details.



B11

TRUST THE SB2 ROOTCA CERTIFICATE

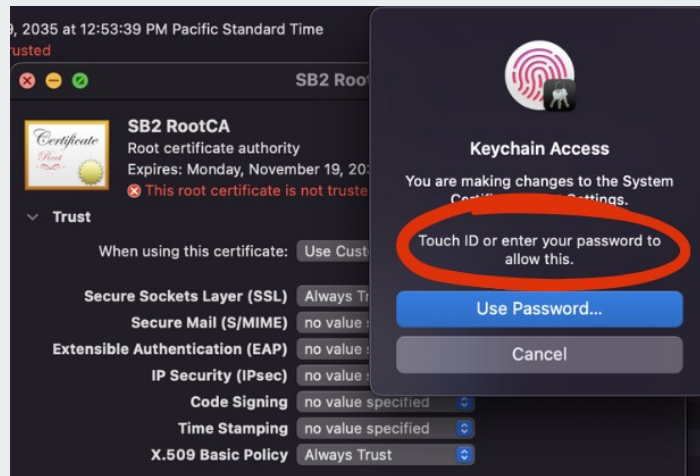
To view the **Trust** details, click the down arrow next to the **Trust** option. Then, select **Always Trust** for both **Secure Sockets Layer (SSL)** and **X.509 Basic Policy**.



B12

AUTHENTICATING THE CHANGES TO THE SB2 ROOTCA CERTIFICATE

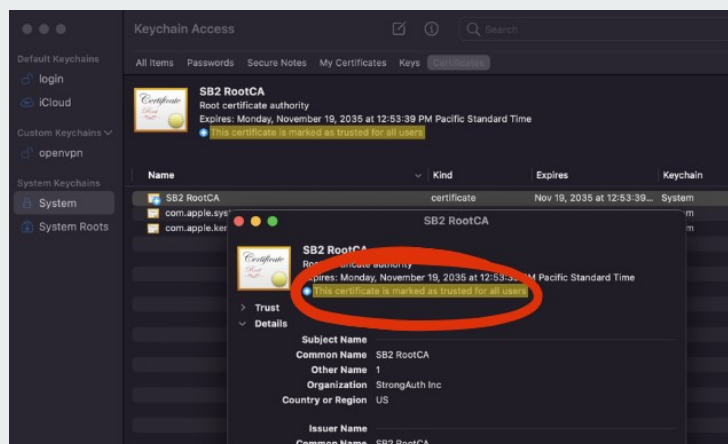
After the SB2 RootCA **Get Info** window is closed, macOS prompts for authentication, using either **Touch ID** or the **macOS account password**, to confirm changes to the Trust settings.



B13

CONFIRMING THE TRUST CHANGES

Click **Next** to continue. To confirm the trust settings, **right-click** the SB2 RootCA certificate and select **Get Info**. A successful import and **trust** is indicated by the message: *"This certificate is marked as trusted for all users."*



ACCESSING THE DOWNLOADED SUBORDINATE ROOT CERTIFICATE FILES

To get started, launch **Keychain Access** by searching with **Spotlight** [⌘ + Space] (refer to Image 1), or by navigating to **Applications** in **Finder** (see Image 2).

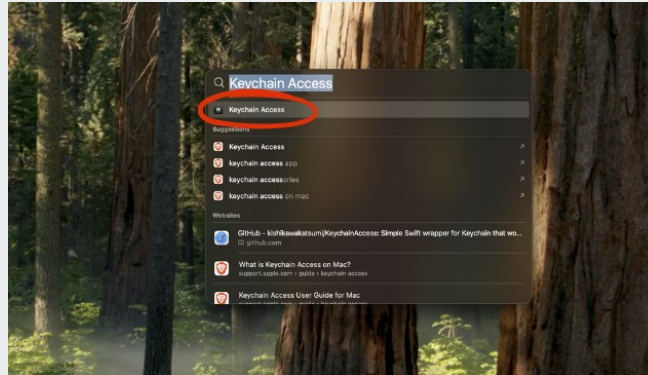


Image 1

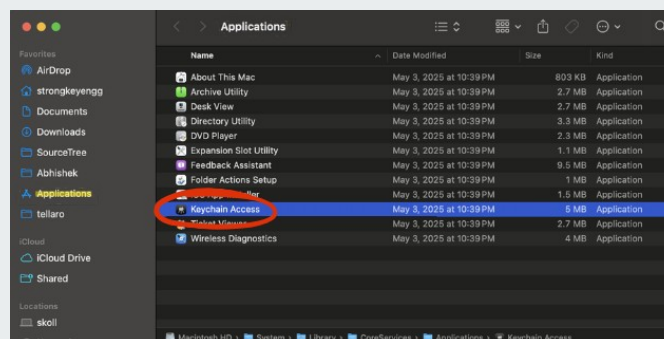
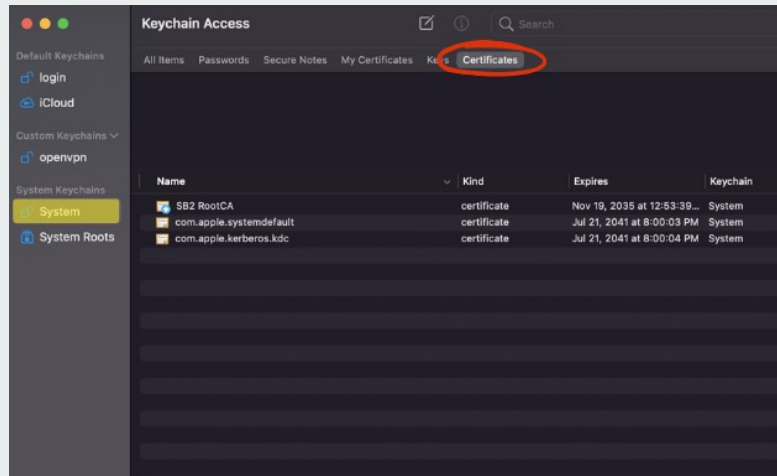


Image 2

B15

NAVIGATING IN THE KEYCHAIN ACCESS APPLICATION

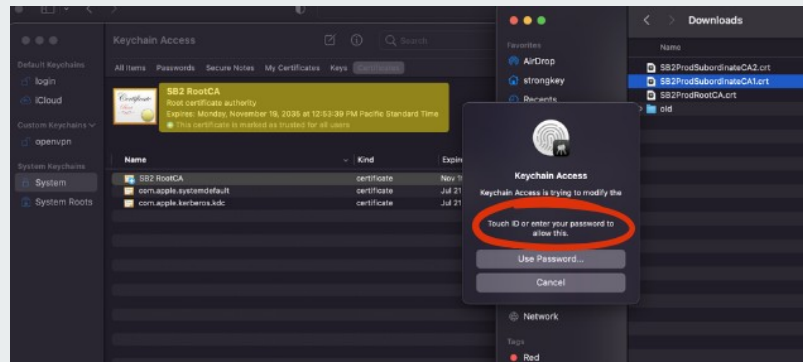
After launching the **KeyChain Access** application, the following screen appears. Select **System** in the sidebar, followed by **Certificates** in the top menu.



B16

IMPORTING CERTIFICATES

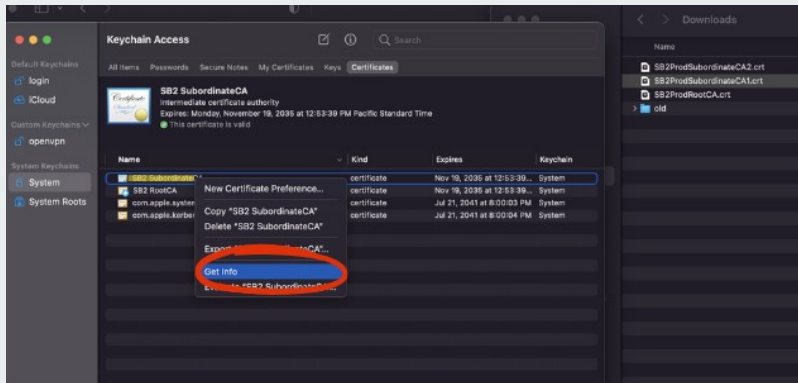
Next, drag the **SB2-SubordinateCA.crt** file into the **Keychain Access** window to begin the certificate import process. The macOS will prompt you to authenticate using Touch ID or an account password to complete the import.



B17

ACCESS THE SB2 SUBORDINATE CA CERTIFICATE DETAILS

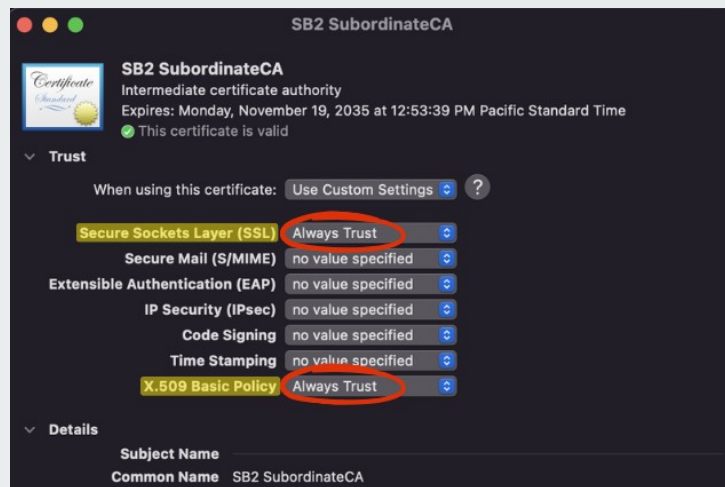
Right-click on the imported **SB2 SubordinateCA** certificate, then select **Get Info** to view its details.



B18

TRUST THE SB2 SUBORDINATE CA CERTIFICATE

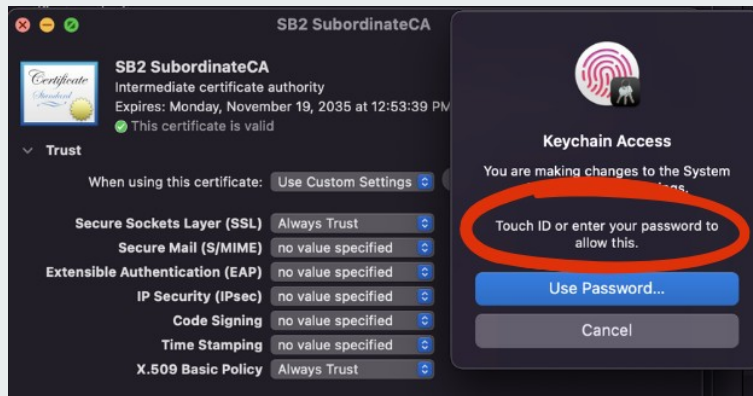
To view the **Trust details**, click the **down arrow** next to the **Trust** option. Then, select **Always Trust** for both **Secure Sockets Layer (SSL)** and **X.509 Basic Policy**.



B19

AUTHENTICATING THE CHANGES TO THE SB2 SUBORDINATE CA

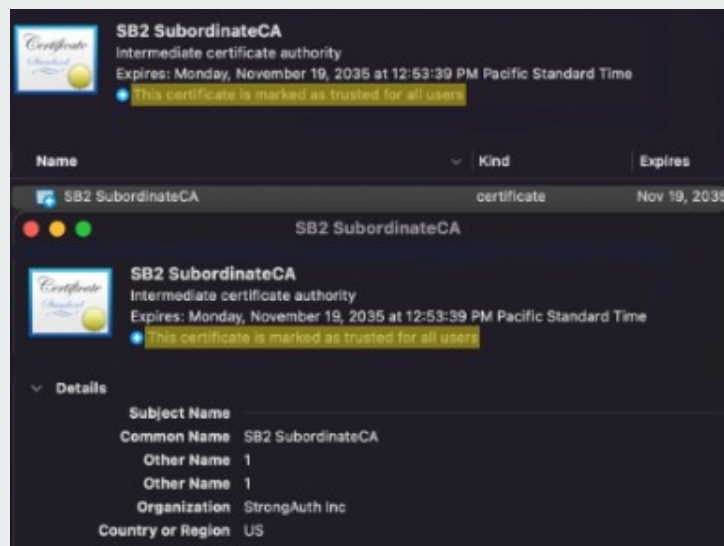
After the SB2 SubordinateCA **Get Info** window is closed, macOS prompts for authentication, using either **Touch ID** or the **macOS account password**, to confirm changes to the trust settings.



B20

CONFIRMING THE TRUST CHANGES

To confirm the trust settings, **right-click** the SB2 SubordinateCA certificate and select **Get Info**. A successful import and trust is indicated by the message: ***"This certificate is marked as trusted for all users."***





SECTION C

C1

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.

C2

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).

C3

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.



C4

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.

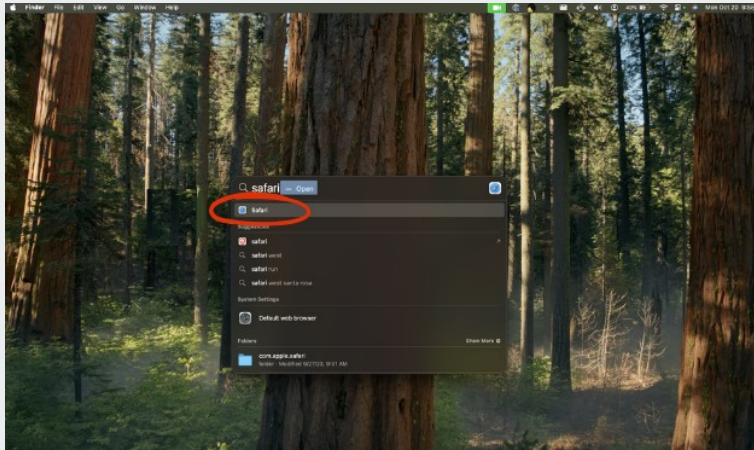
The provided USB adapter pictured below.



C5

OPEN THE SAFARI BROWSER

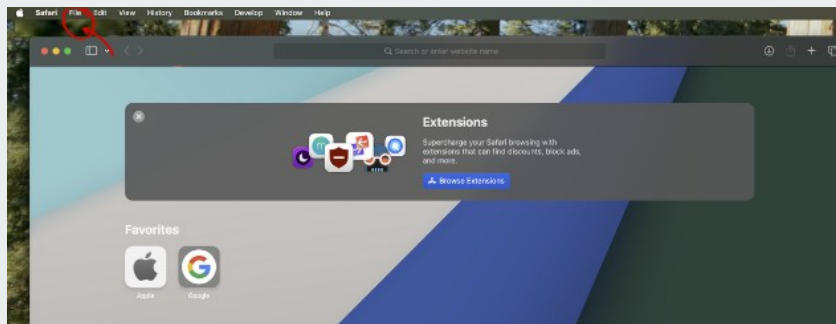
To begin, access the Safari browser by searching with **Spotlight** [⌘ + Space].



C6

LOCATE THE FILE MENU

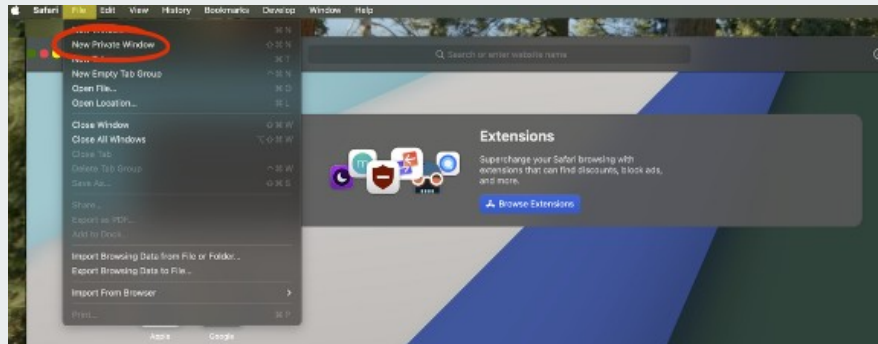
In the top left corner of the menu bar, click the File menu to proceed.



C7

OPEN A NEW PRIVATE WINDOW

Always use Private mode in the Safari browser to access the SB2PROD platform URL (<https://sb2.strongkey.com>).



C8

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)

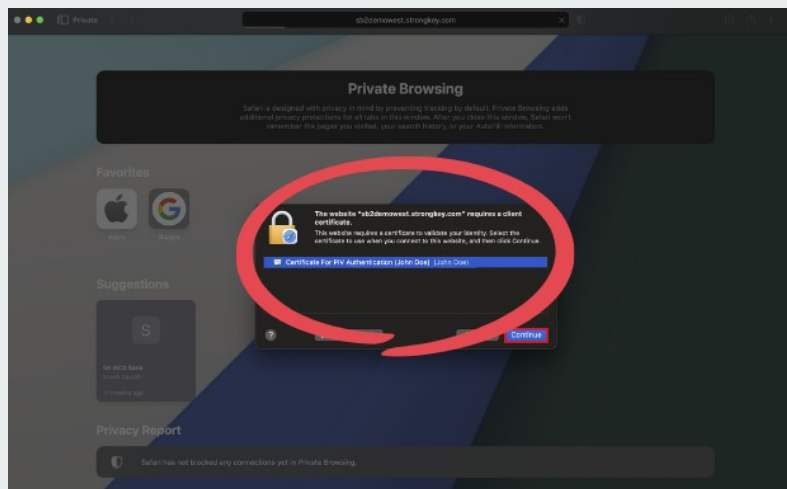
C9

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.

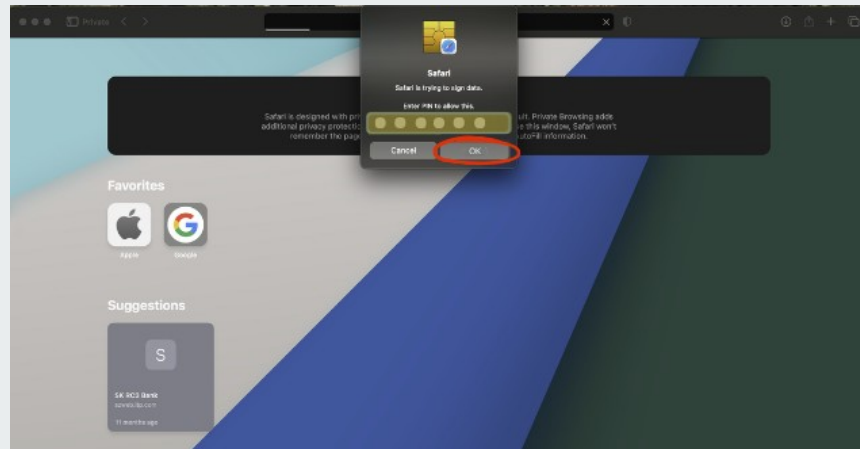
NOTE

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.



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

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

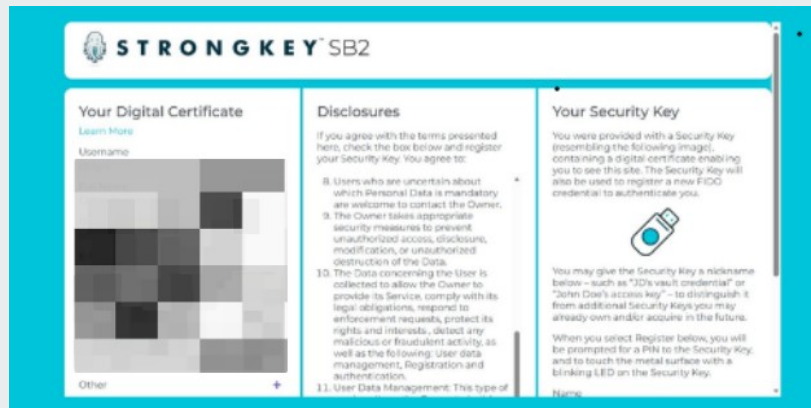


C11

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 (Critical details have been redacted to protect 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.



C12

TERMS & CONDITIONS

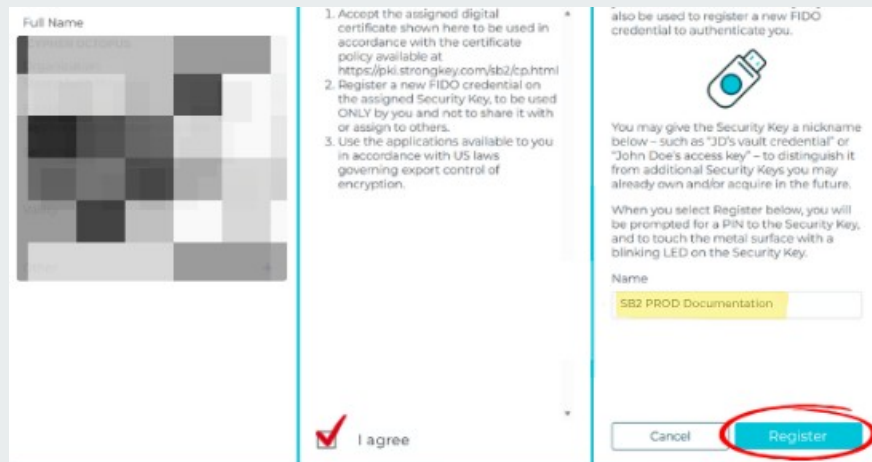
Review and accept the terms and conditions in the **Disclosures** panel. The “**I agree**” box must be checked before proceeding with Security Key registration.

C13

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:

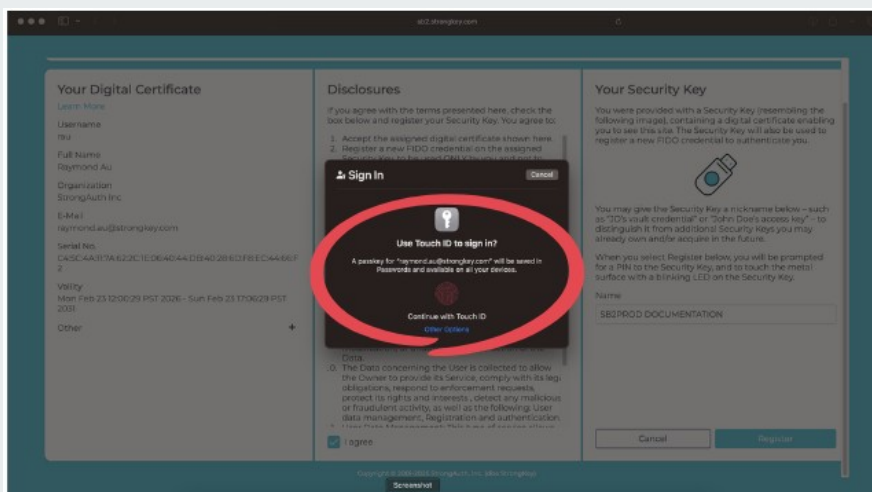
- John's YubiKey 5C Security Key for sb2.strongkey.com
- YubiKey for sb2.strongkey.com



C14

CONTINUE SETUP

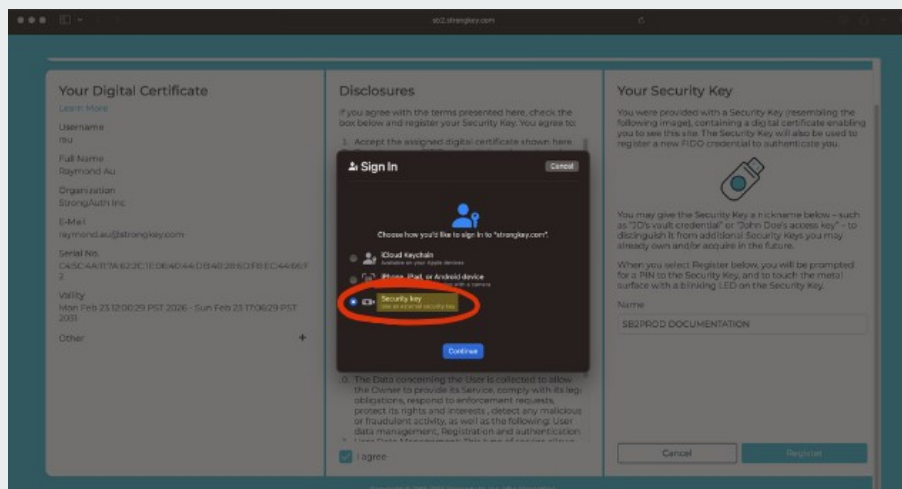
A dialog box will appear to confirm continuation of the setup process, authorizing the current device to also access the SB2PROD website. **Touch your Security Key** to proceed.



C15

SELECT SECURITY KEY

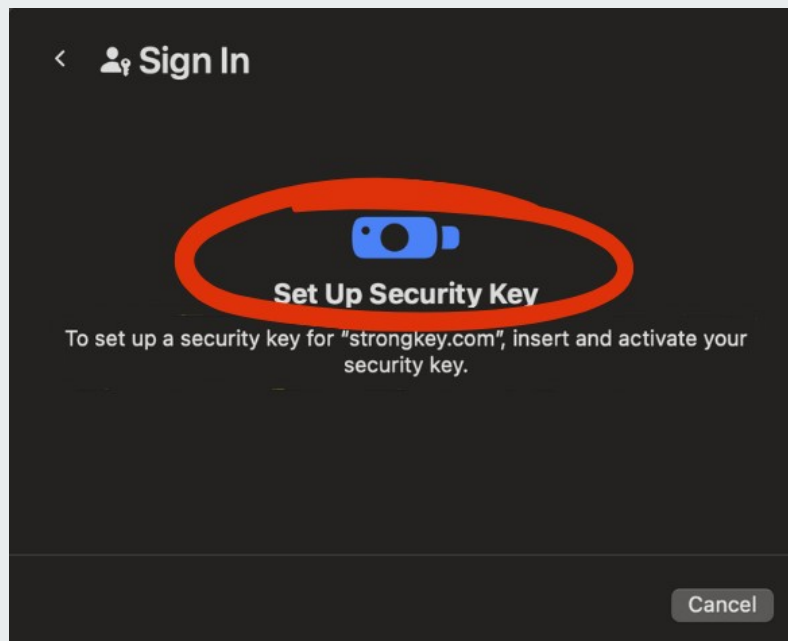
Next, select the **Security Key** for location of where the credential is stored. It is important to verify this location as the Security Key. **Click Continue** to proceed.



C16

SECURITY KEY SETUP

Confirm the SB2PROD login by touching the blinking LED on your security key's metal contact.



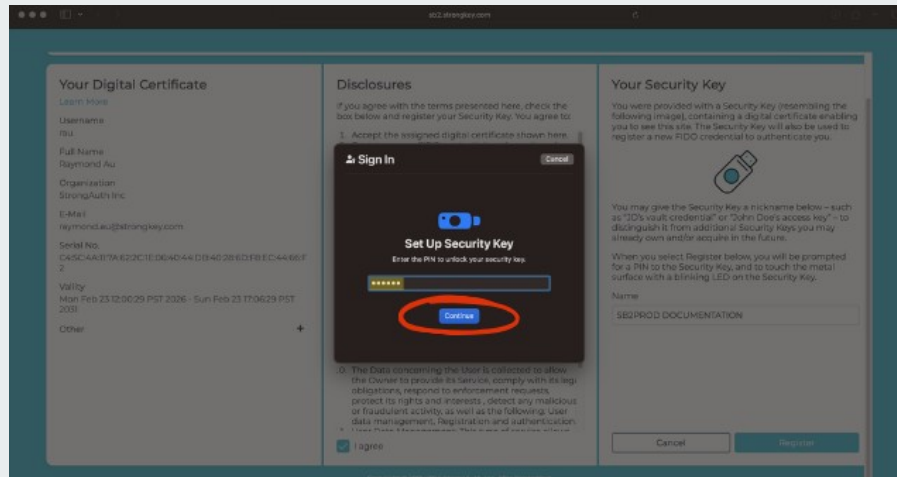
C17

ENTER SECURITY KEY PIN

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

NOTE

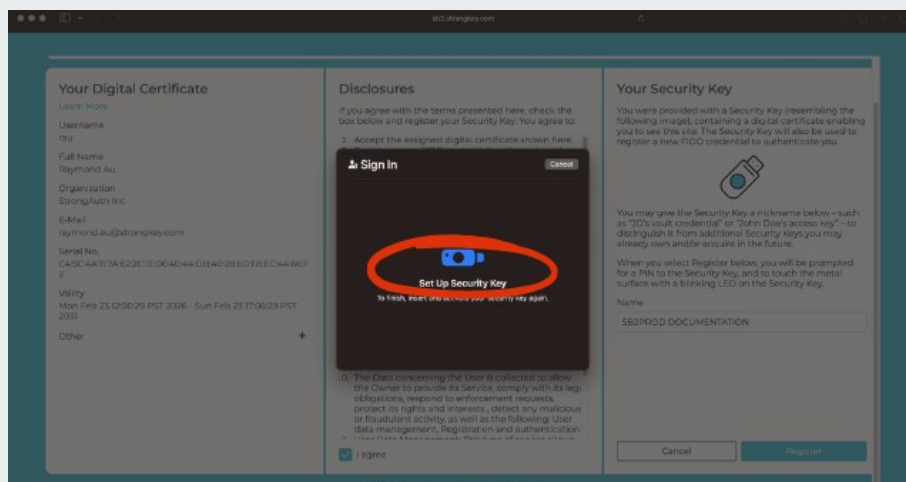
This step is called **User Verification (UV)** in the FIDO ecosystem. It confirms that the SB2PROD platform is interacting with the legitimate Security Key owner by verifying your PIN, which should never be shared. Each time you use your FIDO credential to sign in, you'll complete this UV step as a required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



C18

TOUCH THE SECURITY KEY

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



C19

SB2PROD CONFIRMATION

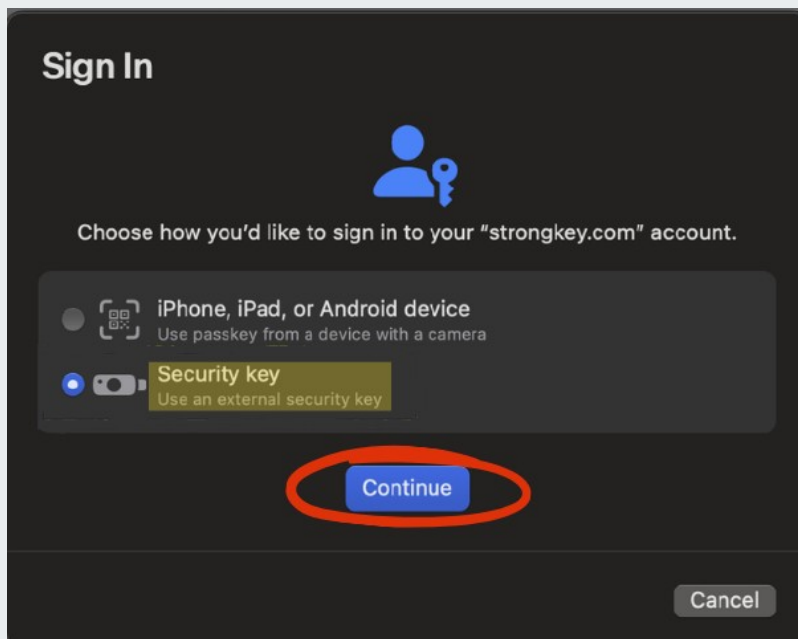
Upon successfully adding the credential, a dialog box will confirm the registration action. Click **Continue** to sign-in to the SB2 platform.



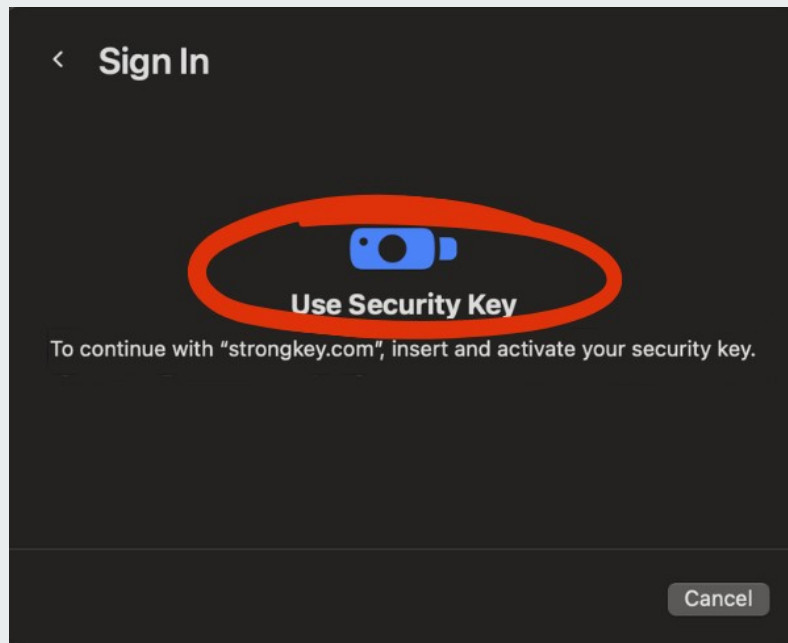
C20

SELECT SECURITY KEY

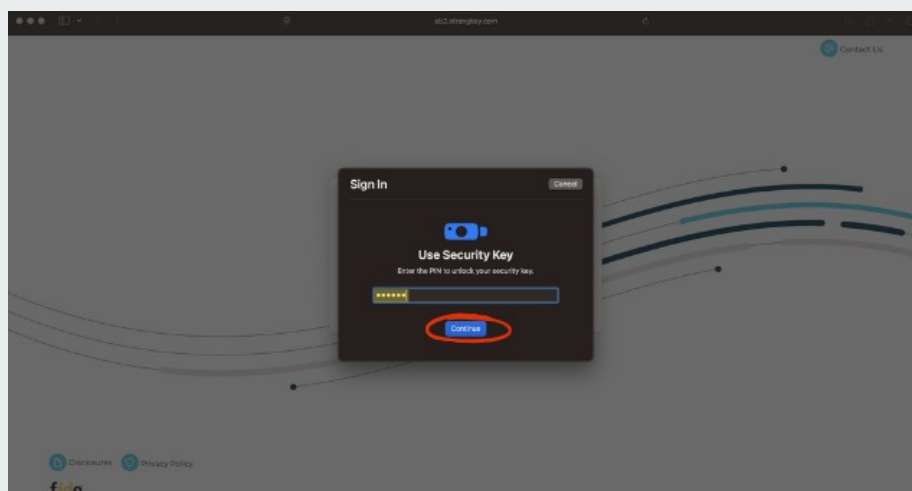
After clicking **Continue**, a prompt will appear prompting you to sign in with the new credential. Make sure you choose the **Security Key** when authenticating to the SB2PROD platform, and click **Continue**.



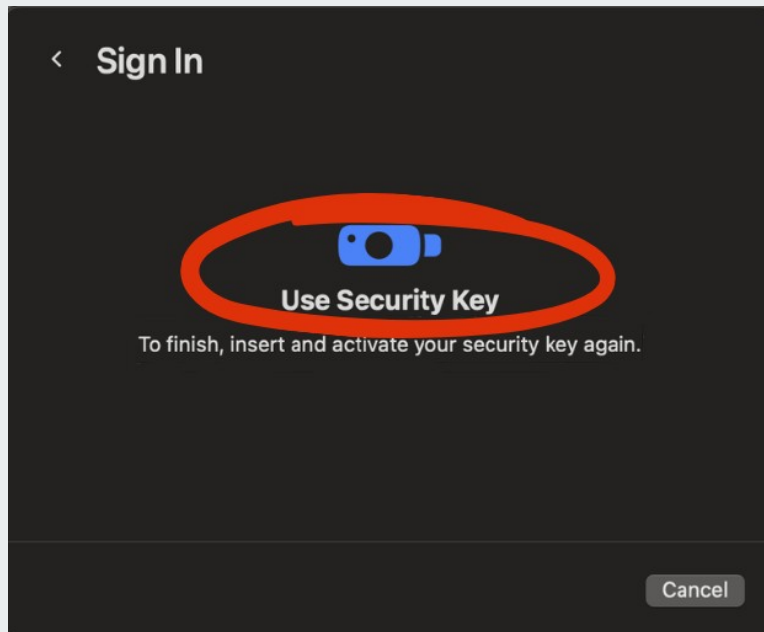
The next dialog box will ask you to activate your Security Key. Please insert now.



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



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.

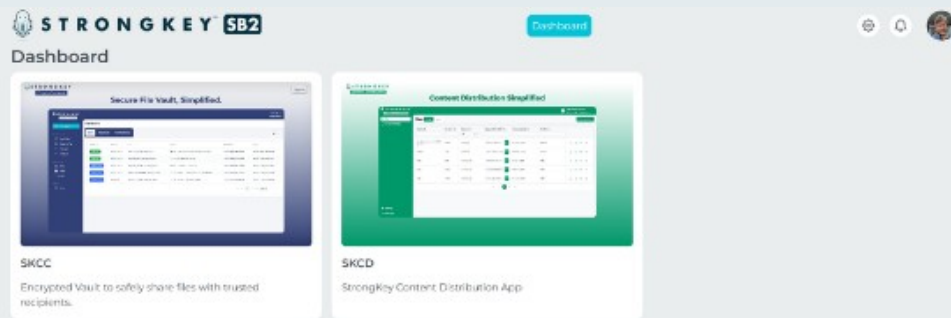


CONGRATULATIONS! Your access to the **SB2PROD Platform** has been successfully established, and your Security Key with your new FIDO credential is registered. Your account name is displayed on the right side of the screen. You may click the gear icon to edit your profile.

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.

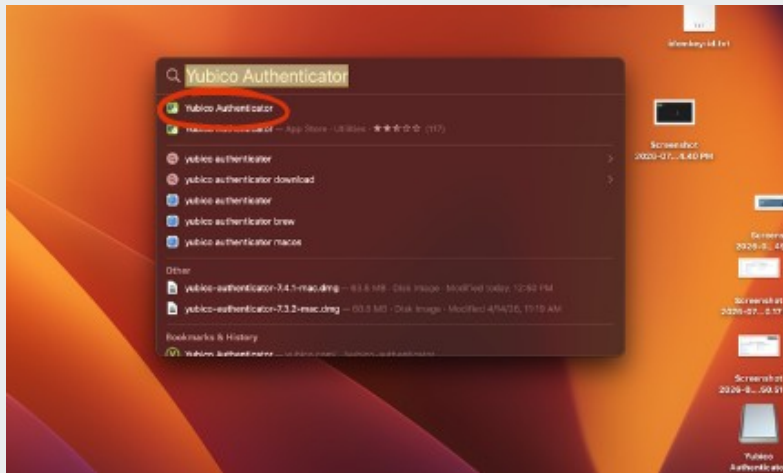
However, StrongKey recommends using the SAME PIN to both containers of the **Security Key** to reduce the burden on users. As long as the **Security Key** is safely in the possession of the legitimate user, and the legitimate user is NOT sharing the PIN to the **Security Key** with anyone, the user will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

OPENING THE YUBICO AUTHENTICATOR APPLICATION

To begin, open the **Yubico Authenticator** application by searching for it with **Spotlight** (⌘ + Space) or locating it in **Finder's** Applications folder.



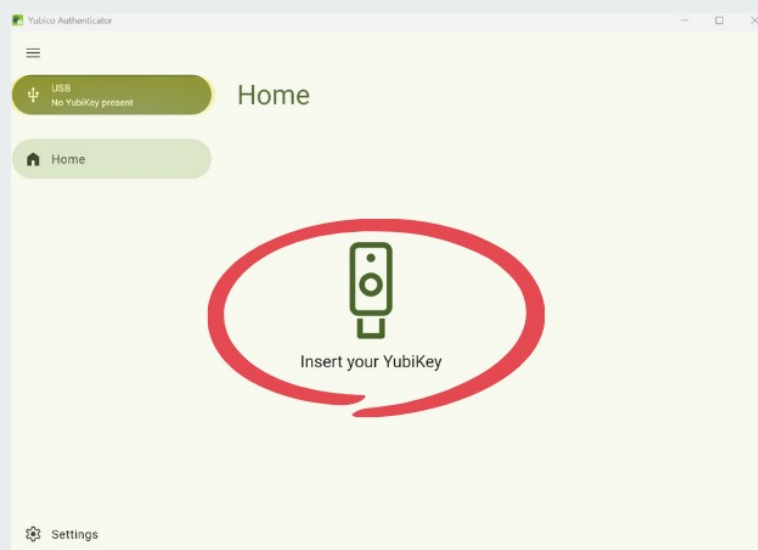
AP3

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.



AP4

INSERT THE YUBIKEY 5C NFC

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

AP5

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.



AP6

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.

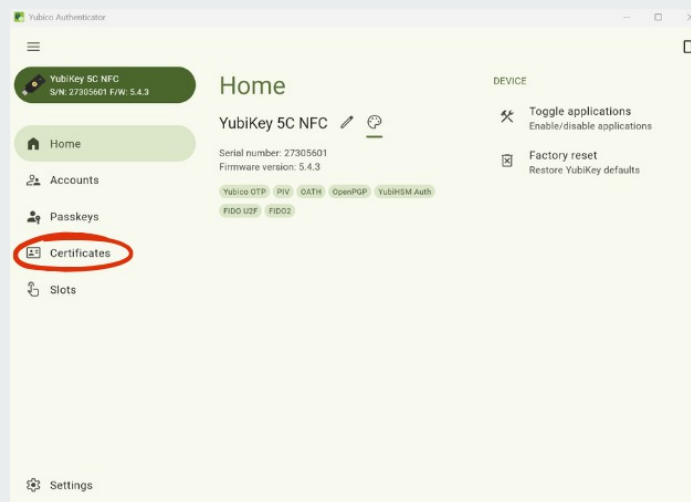
The provided USB adapter pictured below.



AP7

CHANGING THE DIGITAL CERTIFICATE PIN

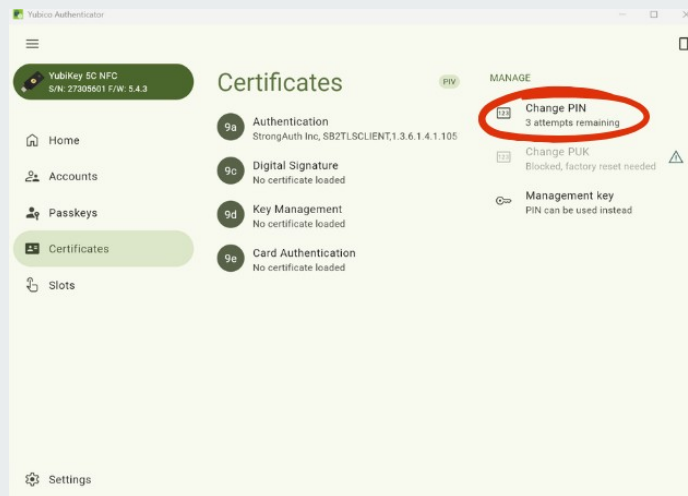
Plugging in the key loads the home screen. Navigate to the left and click the **Certificates** icon from the menu.



AP8

CHANGE PIN

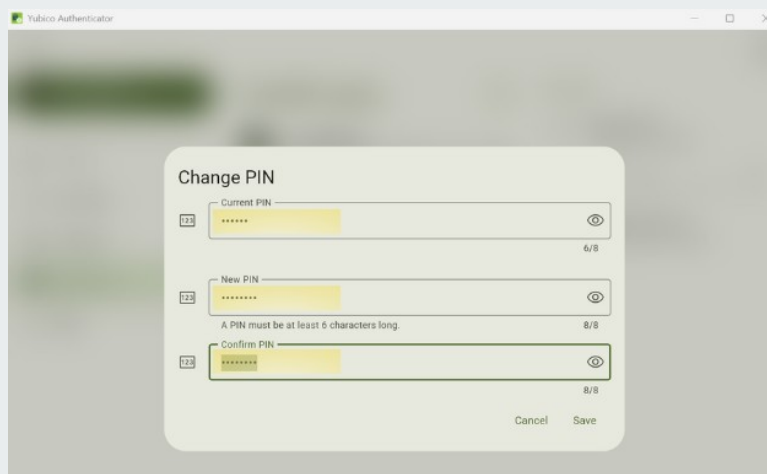
Select the **Change PIN** option from the **Manage** menu on the right.



AP9

ENTER PIN INFORMATION

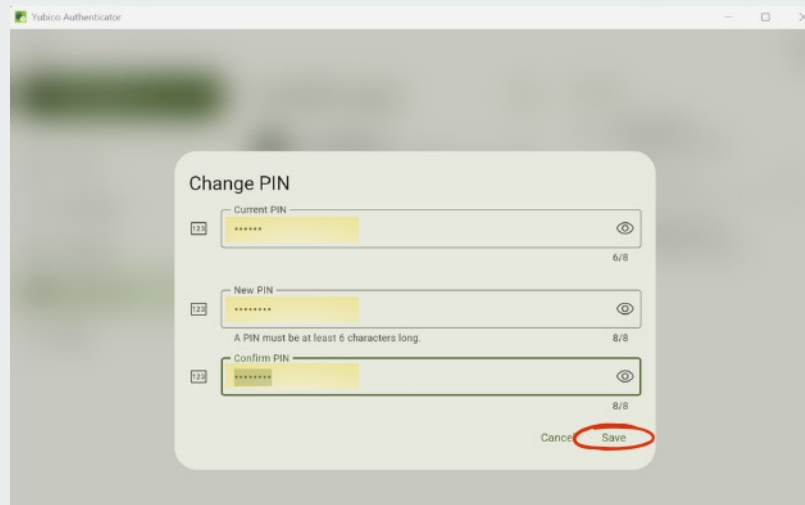
- In the top field, enter the **default PIN: 123456**.
- Enter the new PIN in the middle field. The PIN must contain 6 to 8 characters.
- Re-enter the new PIN in the final field to confirm.



AP10

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.



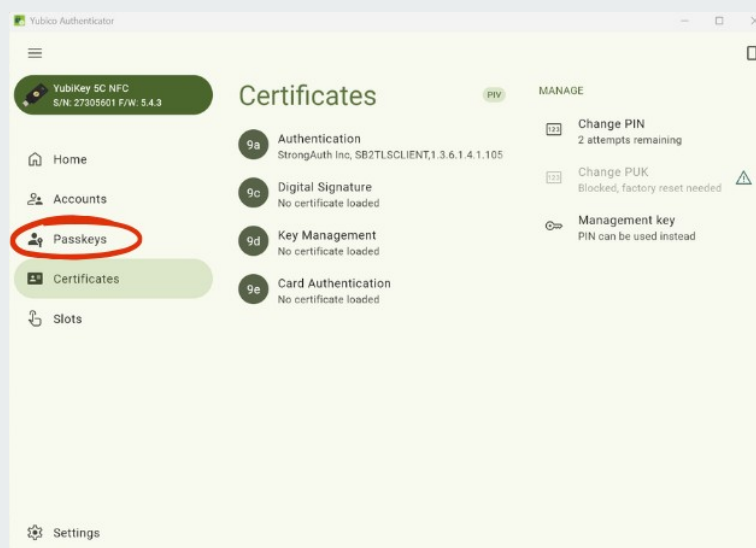
AP11

CHANGING THE FIDO CREDENTIALS PIN

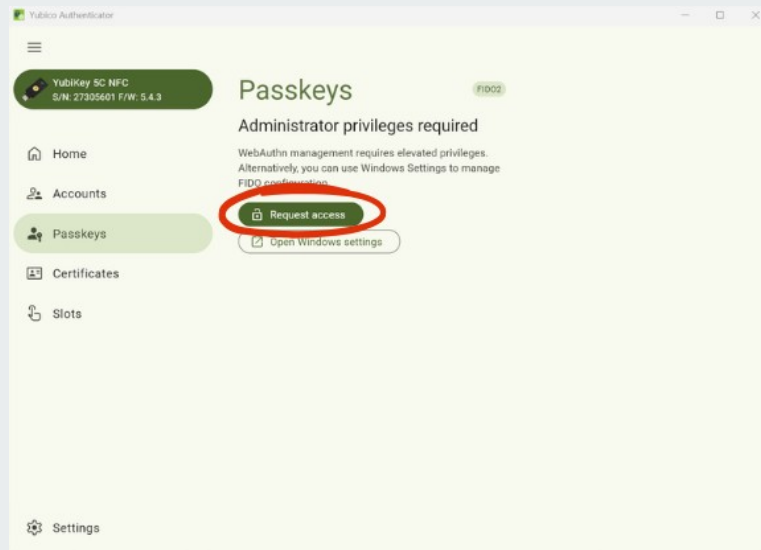
To update the second PIN, click on the **Passkeys** menu option to the left.

NOTE

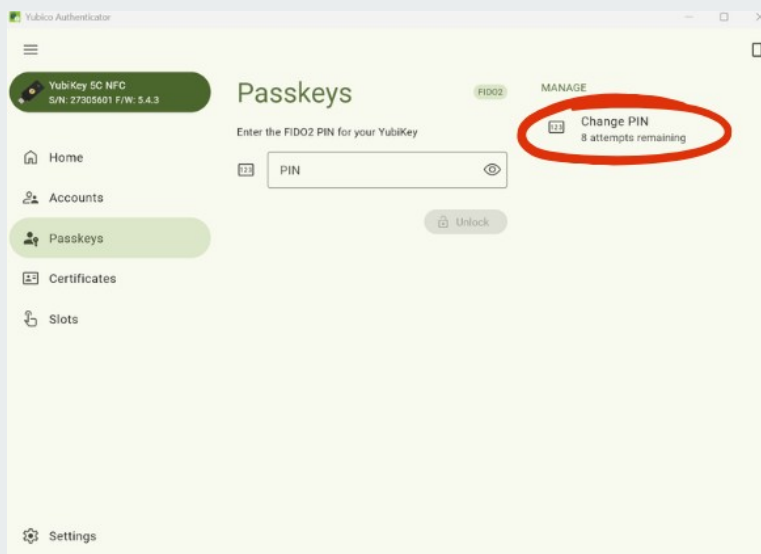
StrongKey recommends using the same PIN for the Security Key.



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



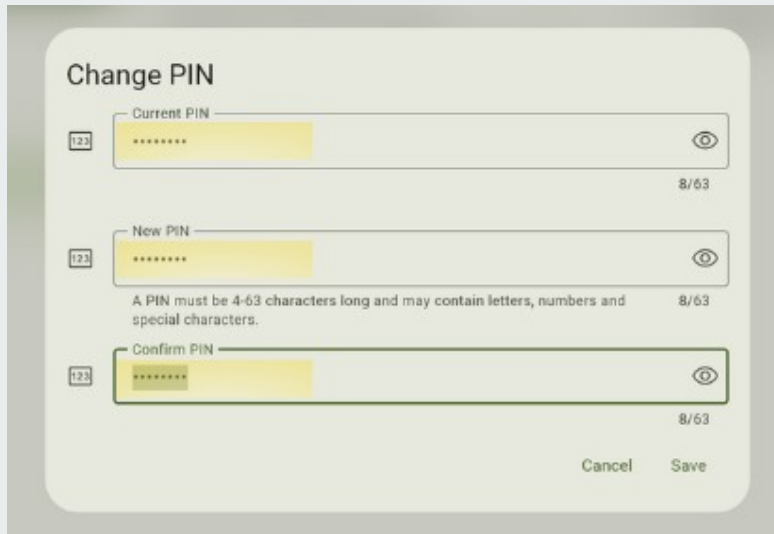
Select the **Change PIN** option located on the right of the screen.



AP14

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.



AP15

SUCCESS!

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

