STRONGKEY TELLARO SB2

Swissbit iShield Key 2 Pro User's Guide for macOS

Version 31

COPYRIGHT & NOTICES

I SWISSBIT iSHIELD KEY 2 PRO

This guide will help you set up your **Swissbit iShield Key 2 Pro** ("iShield2") 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

I PREREQUISITES

- MacOS 13 and above
- Safari 26.0.1
- Swissbit iShield Key 2 Pro
- Internet Connection
- USB-C port or USB-C-to-USB-A adapter

III TABLE OF CONTENTS

A	Installing the Swisbit iShield Key Manager	4
B	Importing SB2 Root CA & SB2 Subordinate CA Certificates into Microsoft Truststore	13
C	Accessing an SB2PROD Invitation Link URL	24
AP	Appendix: Changing a Swissbit iShield2 Personal Identification Number (PIN)	38

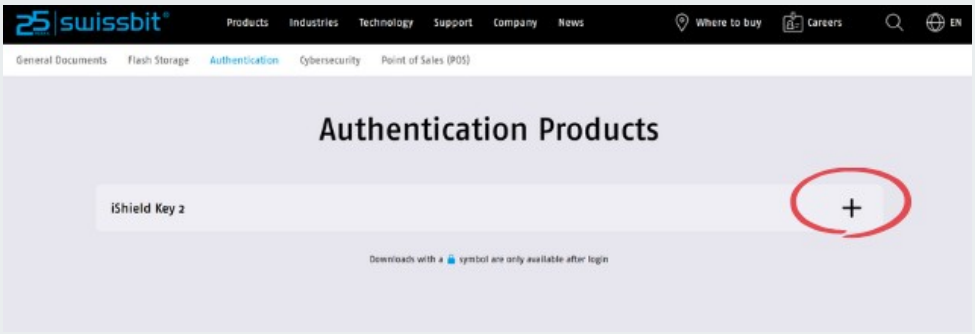
SECTION A

A1 INSTALLING THE SWISSBIT iSHIELD KEY MANAGER

The The Swissbit iShield Key Manager is necessary to use the iShield2 Security Key.

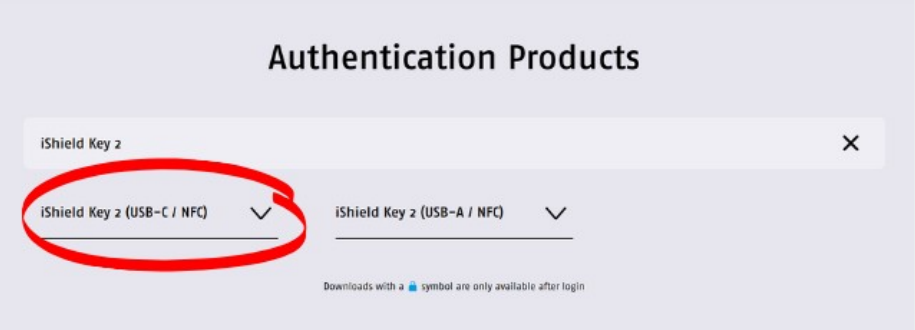
A2 DOWNLOAD iSHIELD KEY MANAGEMENT KIT: PART 1

To download the iShield Key Management Kit for macOS, go to https://www.swissbit.com/en/my-swissbit/download-center. Next, scroll down to Authentication Products and expand by clicking the plus icon.



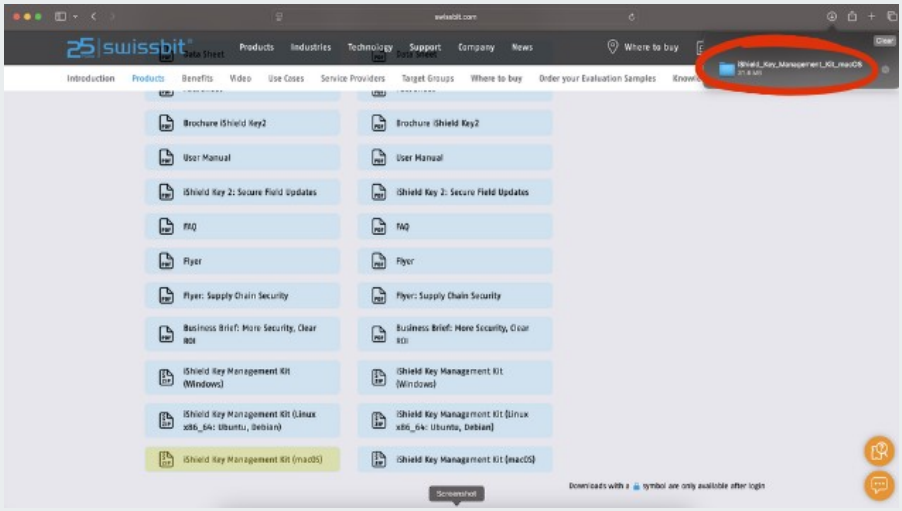
A3 DOWNLOAD SWISSBIT iSHIELD KEY MANAGEMENT KIT: PART 2

Select **iShield Key 2 (USB-C / NFC)** and **click** the **down arrow**.



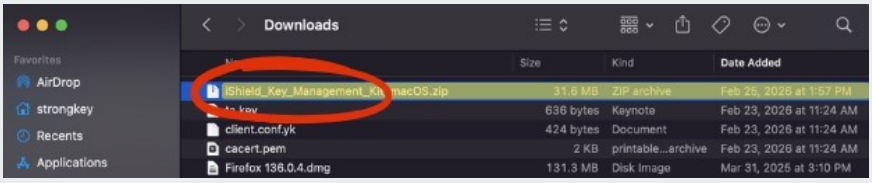
A4 DOWNLOAD SWISSBIT iSHIELD KEY MANAGEMENT KIT: PART 3

Download the **iShield Key Management Kit (macOS) zip file** by clicking the link. When Safari displays a pop-up confirming the download, double-click the **blue file** to initiate install.



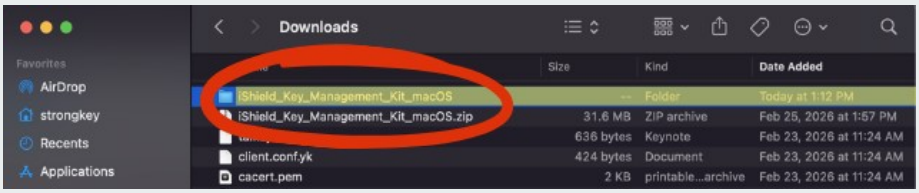
A5 NO POP-UP WINDOW? NO PROBLEM.

If the pop-up does not appear, or is inadvertently closed, access the downloaded file by using **Finder** to access **Downloads**. Double-click the iShield Key Management Zip file to extract the files.



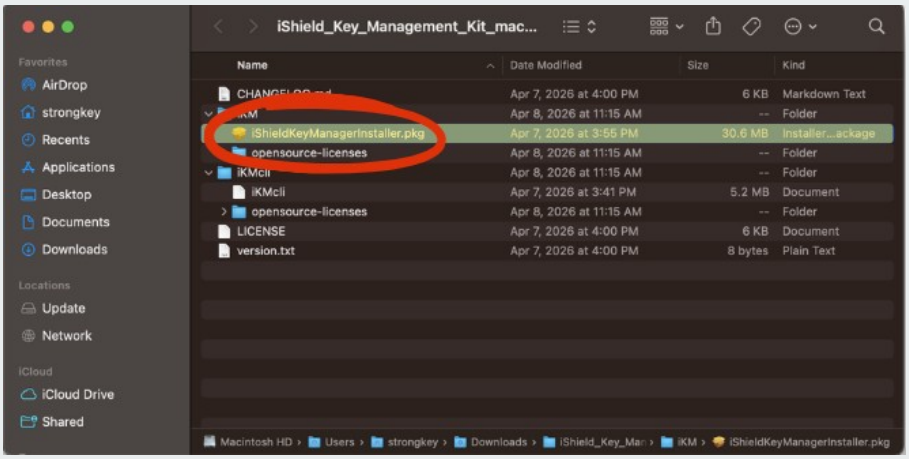
A6 EXTRACTED FILES

Double-clicking the zip file initiates a macOS Archive Utility that automatically extracts the contents of the file. The extracted "iShield" folder appears above the zip file. Double-click the new folder to access the **iShieldKeyManagerInstaller.pkg**.



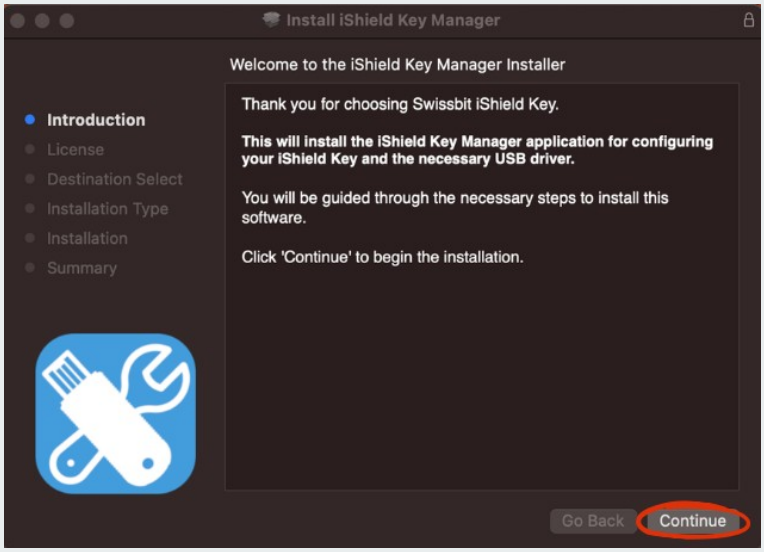
A7 INITIATE iSHIELD INSTALLER

Double-click the **iShieldKeyManagerInstaller.pkg.**



A8 iSHIELD INSTALL

Follow the on-screen prompts to install the iShield Key Manager. **Click Continue**.



A9 ISHIELD KEY MANAGER LICENSE

Click Continue to accept the license agreement.

A10 LICENSE AGREEMENT

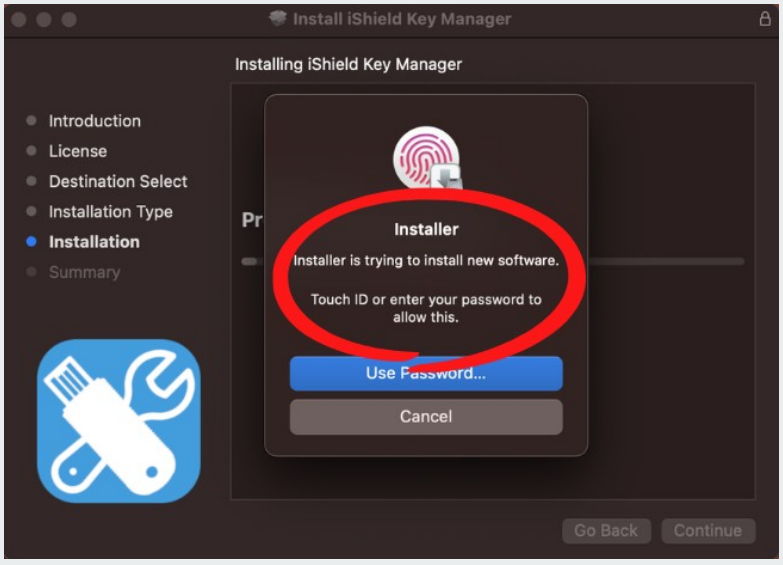
Click Agree to accept agreement and continue installation.

A11 INSTALLATION TYPE

Verify Installation Type is **Standard**. **Click Install**.

A12 AUTHENTICATE TO INSTALL – PART 1

To continue installation, authenticate using **Touch ID** or **Password**. The document example will use a password.

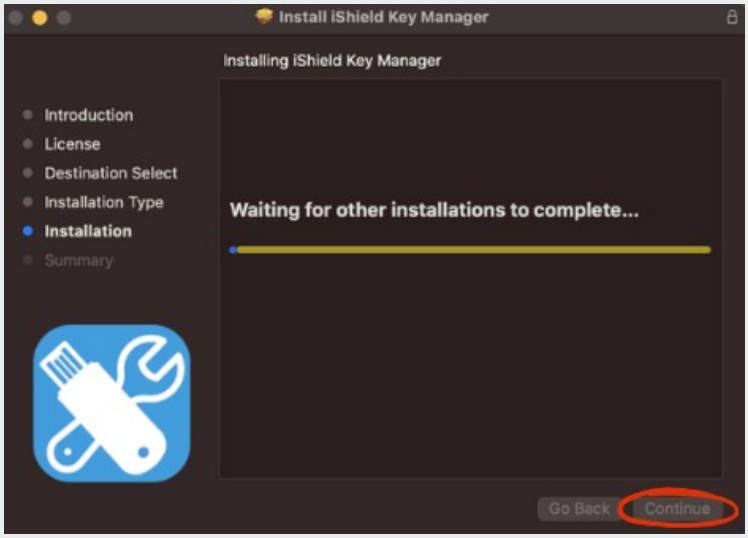


A13 AUTHENTICATE TO INSTALL – PART 2

Enter your **password** and **click Install Software**.

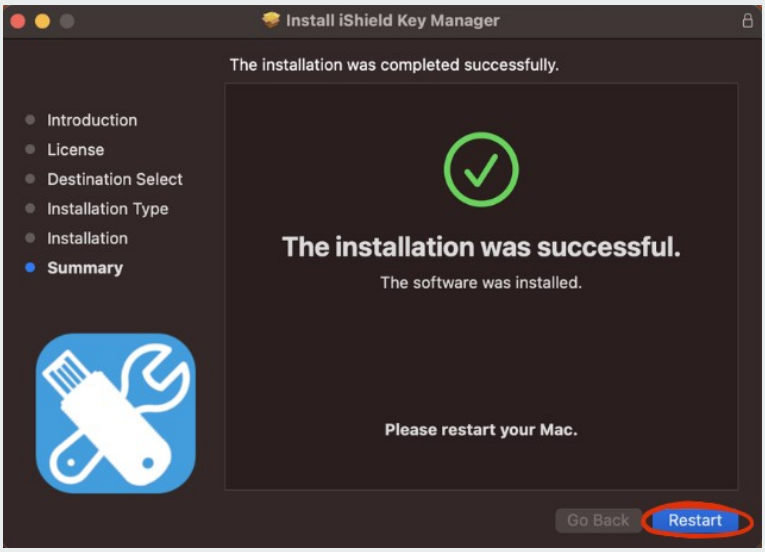
A14 THE INSTALL

When the installation is complete (progress bar will turn blue), the **Continue** button will activate -- **click it**.



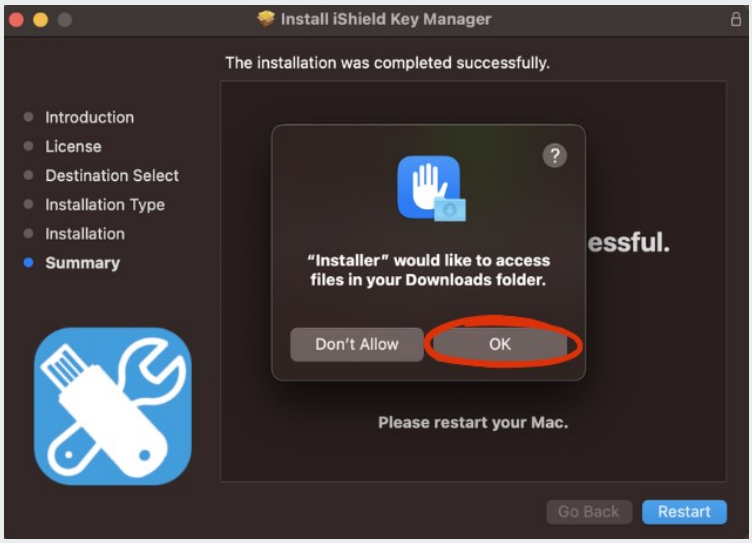
A15 SUCCESSFUL INSTALLATION

After the iShield Key Manager installs successfully, your computer will prompt you to restart. Please save all open documents before proceeding.



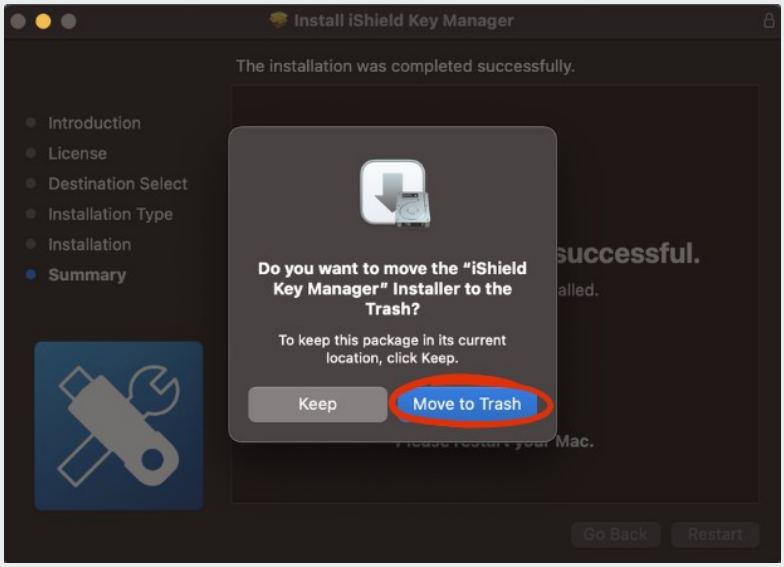
A16 ALLOW ACCESS

Click OK to continue.



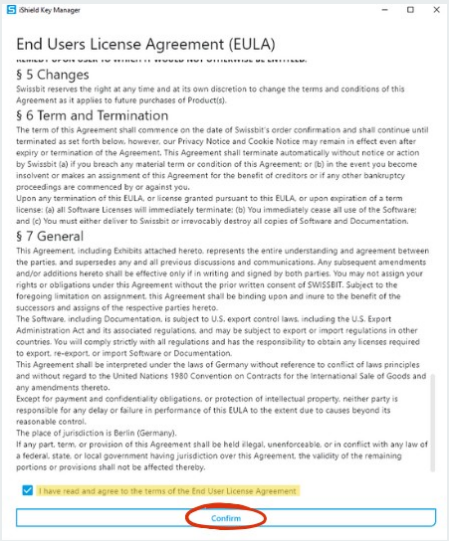
A17 DELETE THE INSTALLER

Click the **Move to Trash** button.



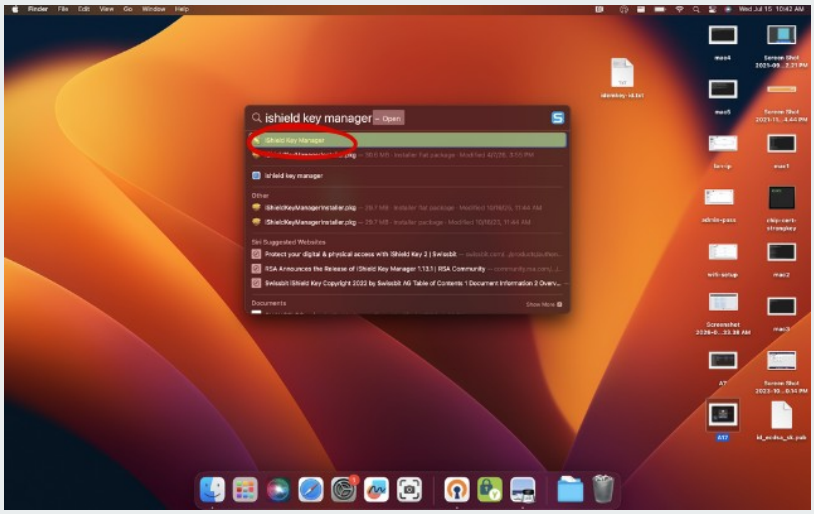
A18 END USER LICENSE AGREEMENT

Check the box that you have read and agree to the terms of the End User License Agreement and click **Confirm.**



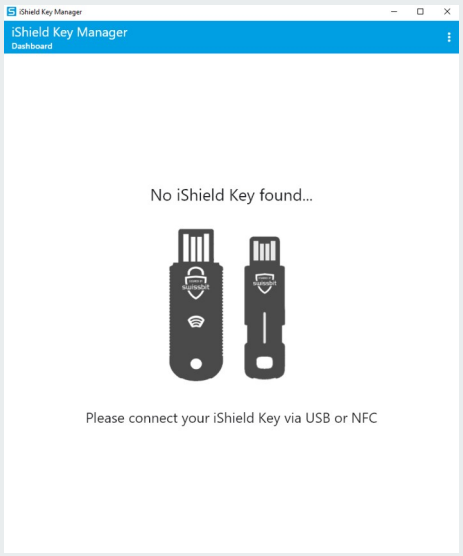
A19 RESTART COMPUTER

After the install is complete, save any open documents and restart the computer. Next, re-open the iShield Key Manager.



A19 SUCCESS

The iShield Key Manager is now ready to use.



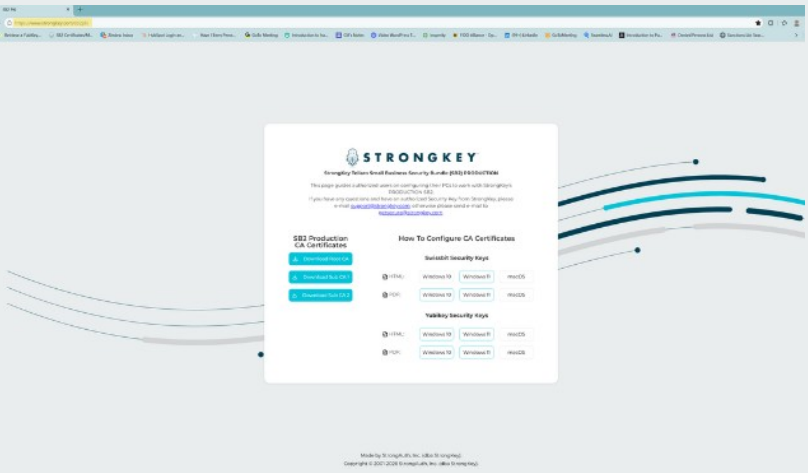
SECTION B

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

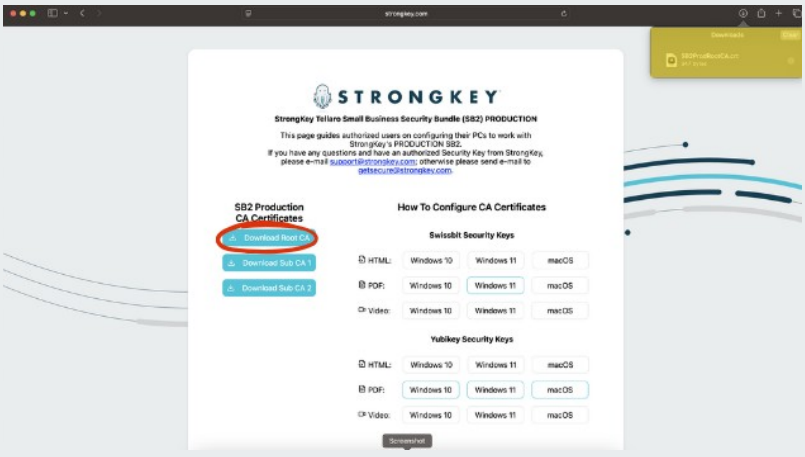
Next, download the three SB2 Production CA certificates from the left side of the page.

NOTE Download the certificates starting with the Root CA.

B4 DOWNLOADING THE SB2 ROOT CA

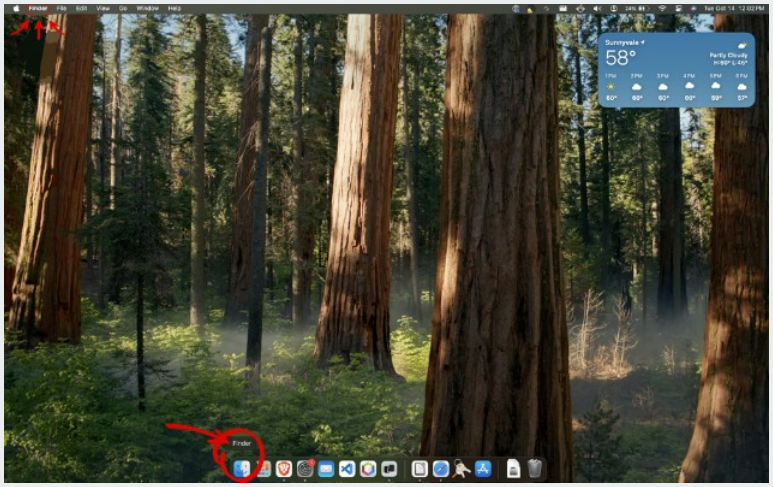
First, click the Download Root CA button. The download will begin automatically, and you'll see a dialog box confirming the file name once the process is complete.

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.

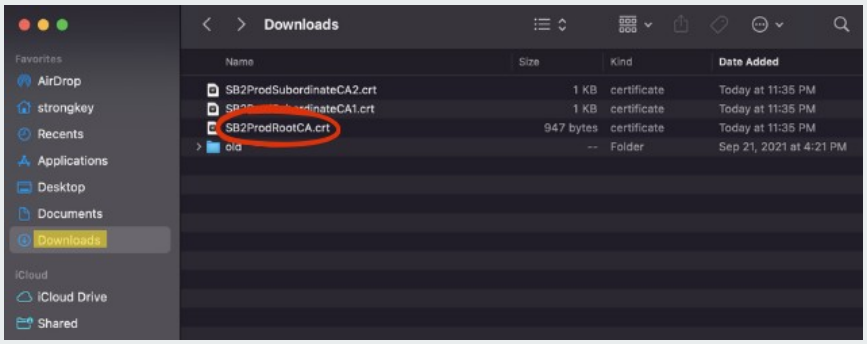


B6 LOCATE DOWNLOADED SB2 ROOT CA FILE

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.



B7 OPEN KEYCHAIN ACCESS

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

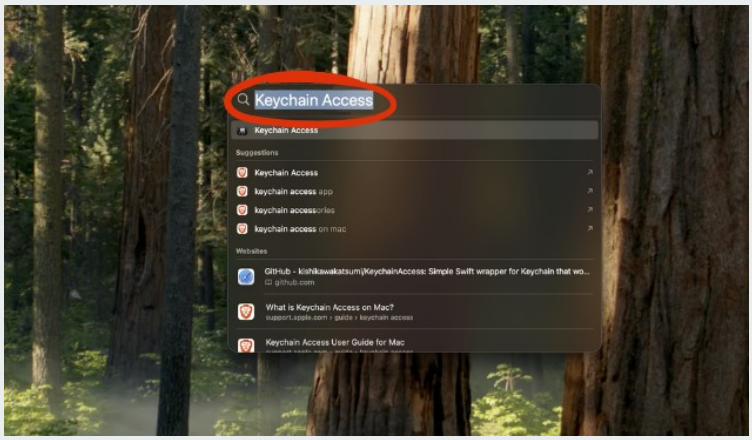


Image 1

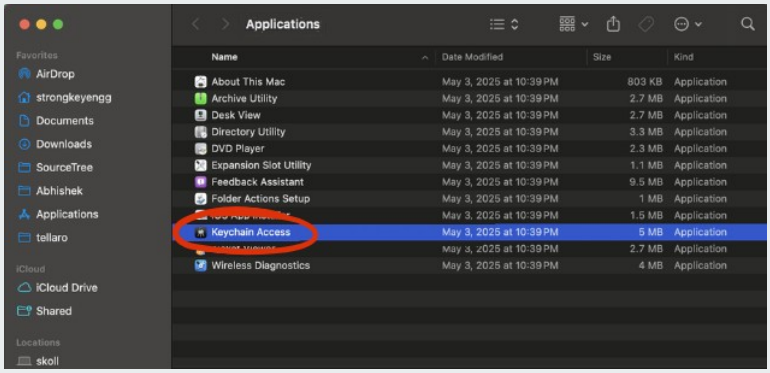
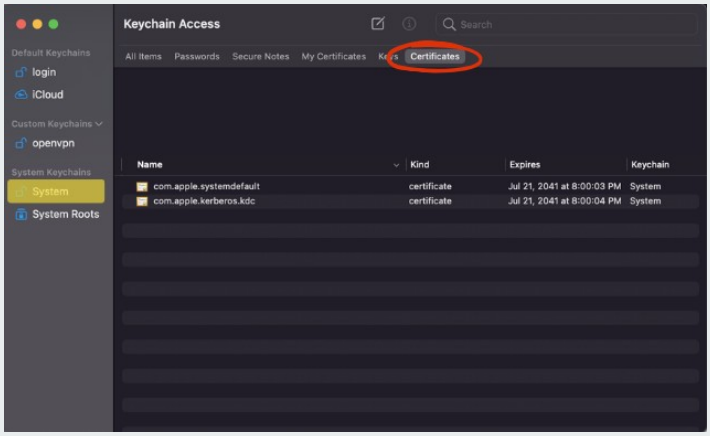


Image 2

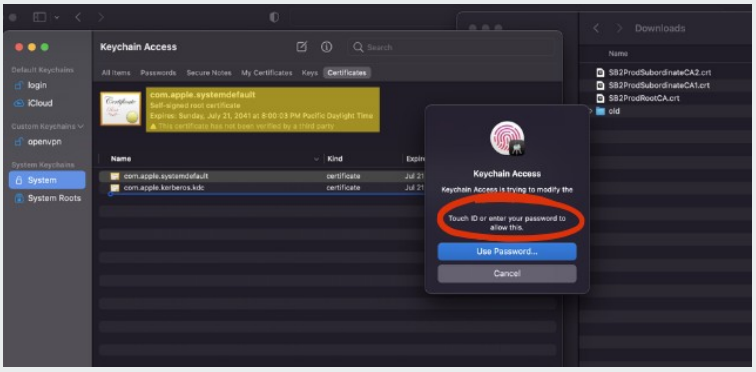
B8 NAVIGATING IN THE KEYCHAIN ACCESS APPLICATION

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



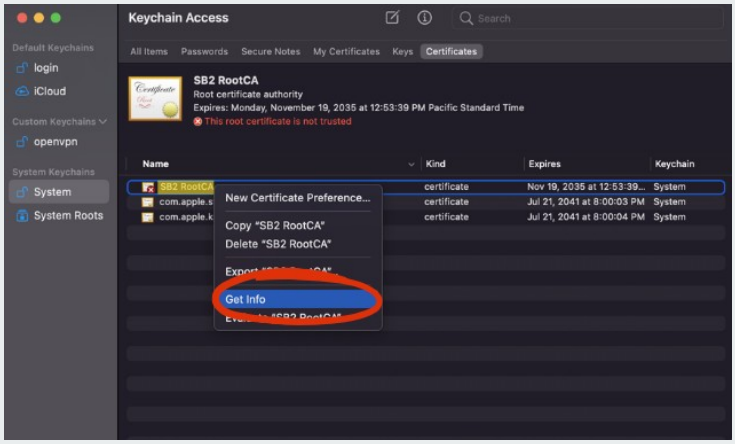
B9 IMPORTING CERTIFICATES

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.



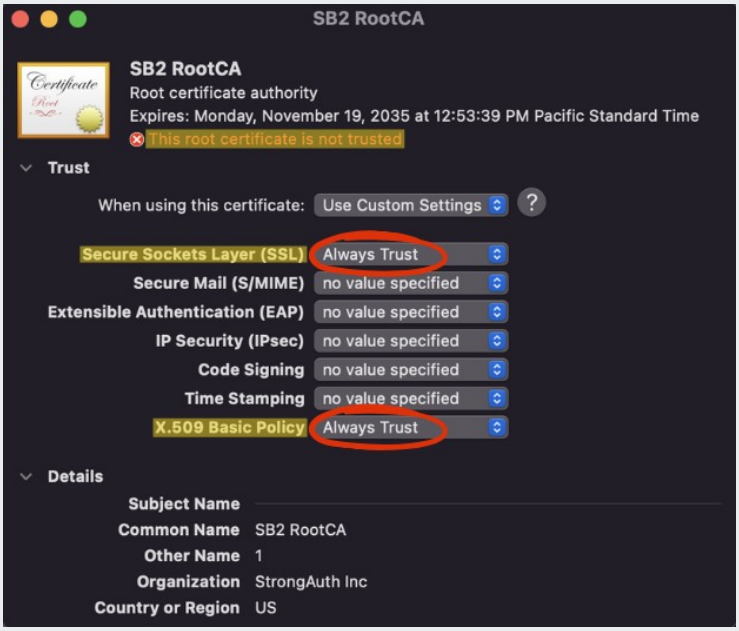
B10 ACCESS THE SB2 ROOTCA CERTIFICATE

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



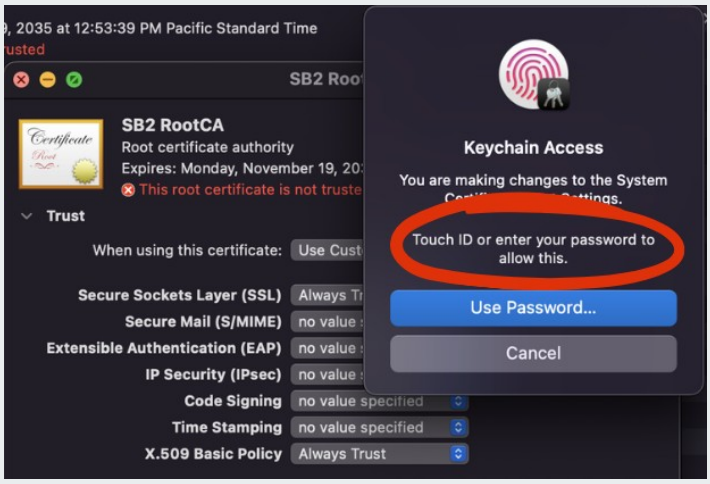
B11 TRUST THE SB2 ROOTCA CERTIFICATE

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**.



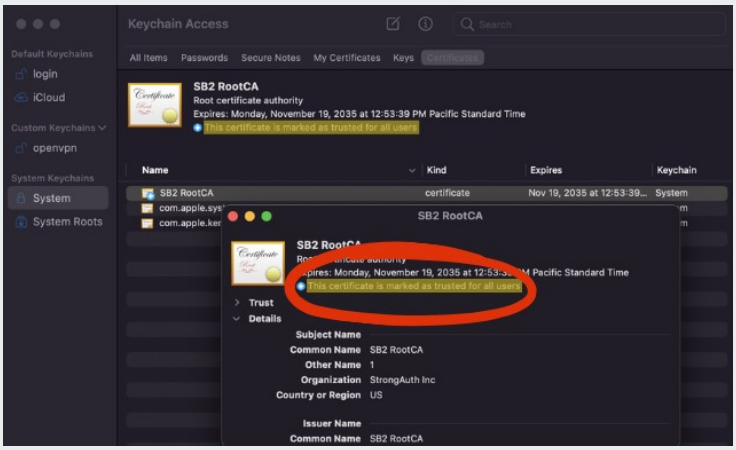
B12 AUTHENTICATING THE CHANGES TO THE SB2 ROOTCA CERTIFICATE

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."***



B14 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).

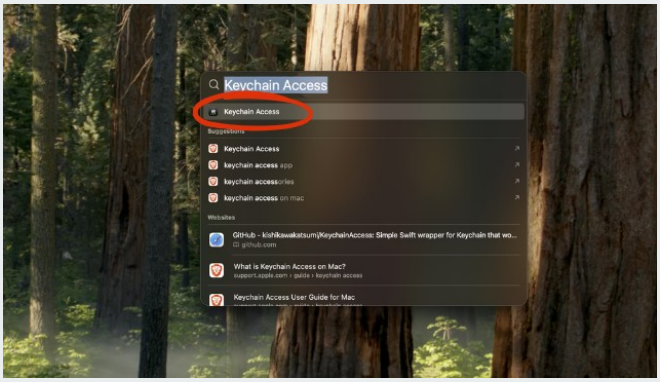


Image 1

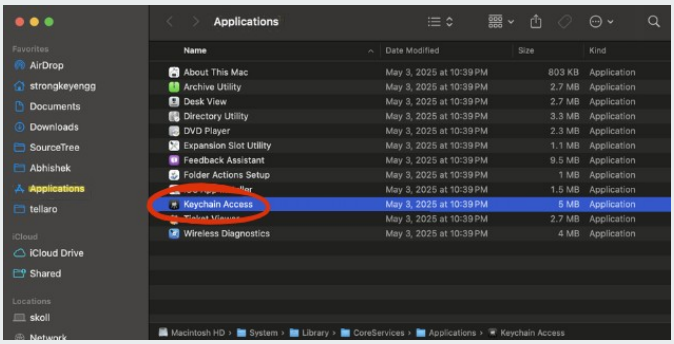
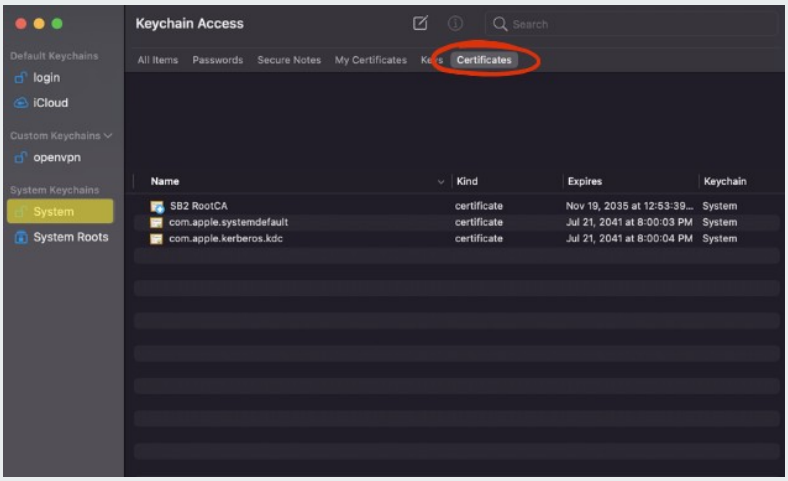


Image 2

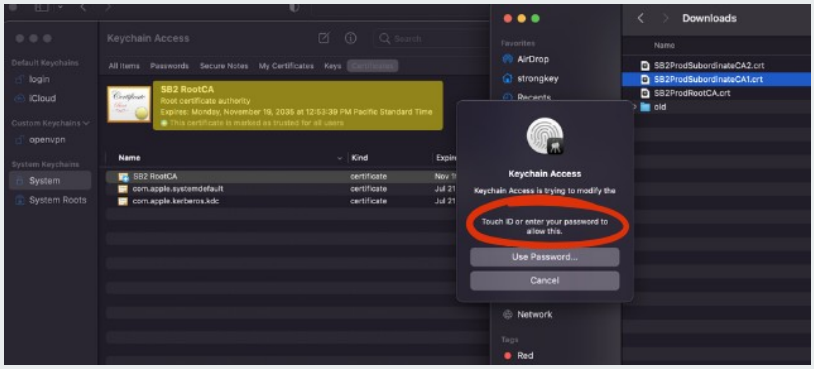
B15 NAVIGATING IN THE KEYCHAIN ACCESS APPLICATION

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



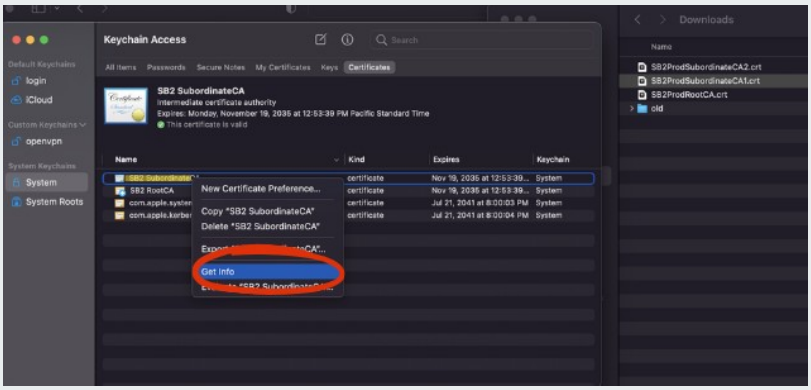
B16 IMPORTING CERTIFICATES

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.



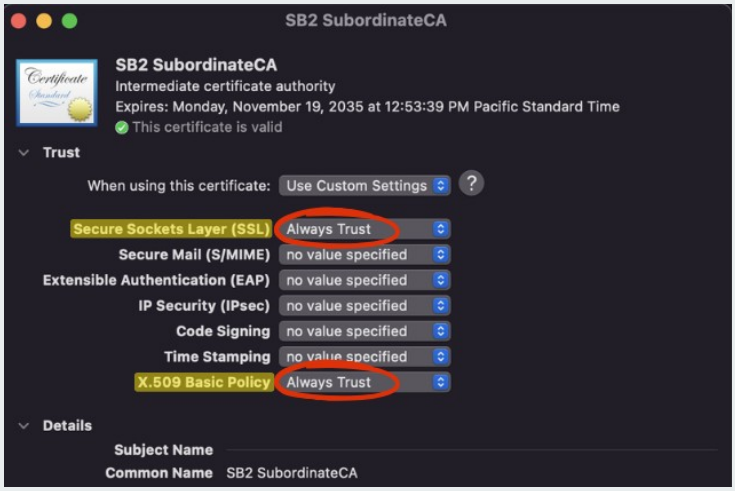
B17 ACCESS THE SB2 SUBORDINATE CA CERTIFICATE DETAILS

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



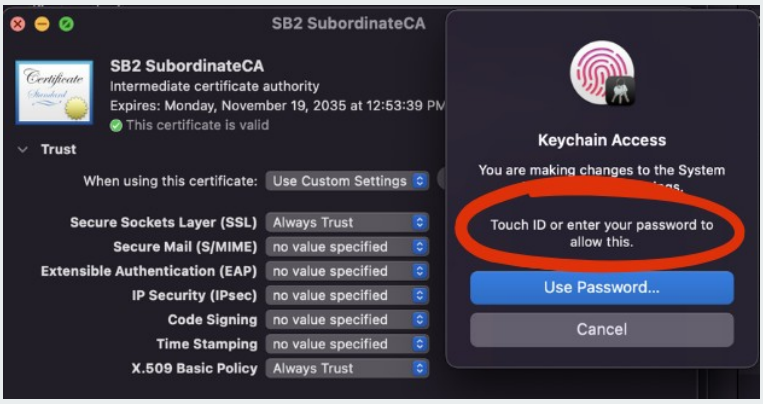
B18 TRUST THE SB2 SUBORDINATE CA CERTIFICATE

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.**



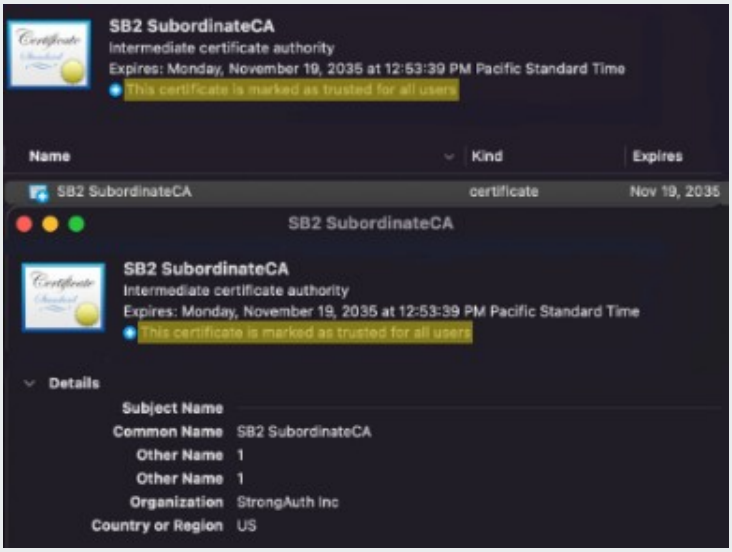
B19 AUTHENTICATING THE CHANGES TO THE SB2 SUBORDINATE CA

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 Swissbit iShield2 Security Key with the SB2PROD site.

You must have the Swissbit iShield2 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 SWISSBIT iSHIELD2 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.

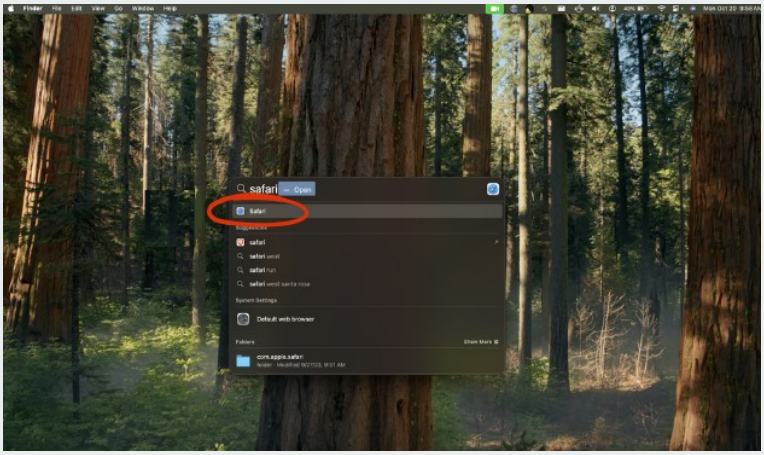
C4 NO USB-C PORT? NO PROBLEM.

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.

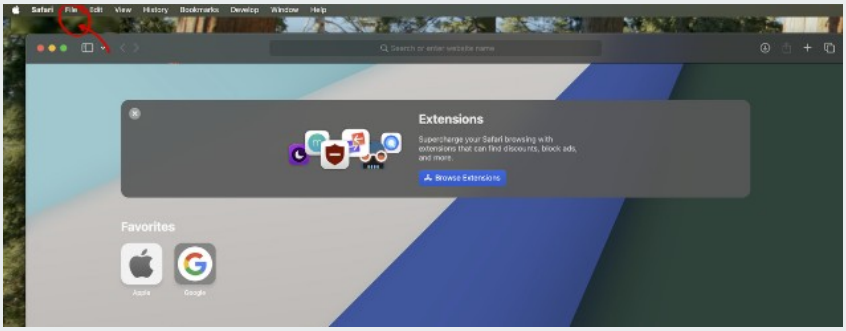
C5 OPEN THE SAFARI BROWSER

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



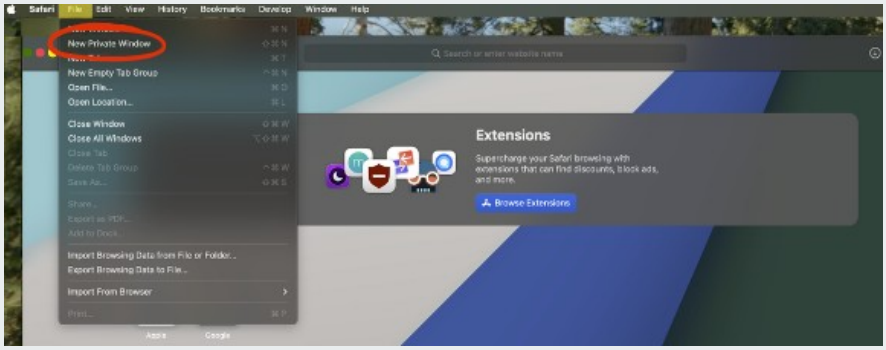
C6 LOCATE THE FILE MENU

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 Sarari 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

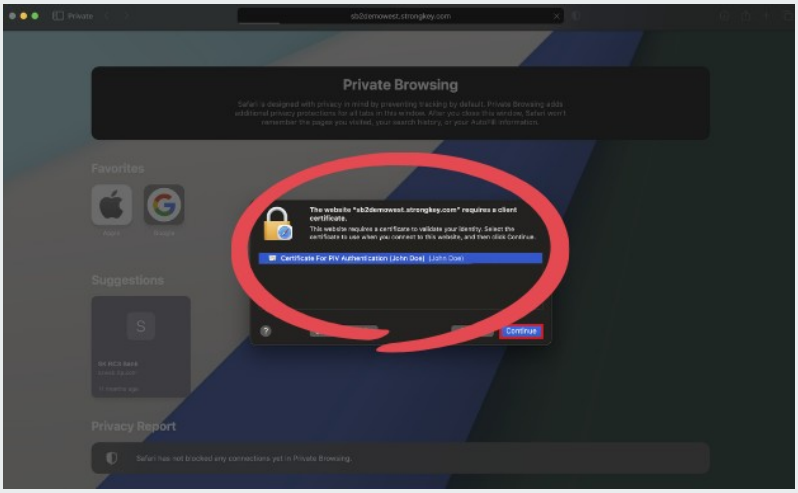
The SB2 registration invite URL is long so it will be advantageous to use the “cut and paste” options. Here is an example of what the URL will look like:

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

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.

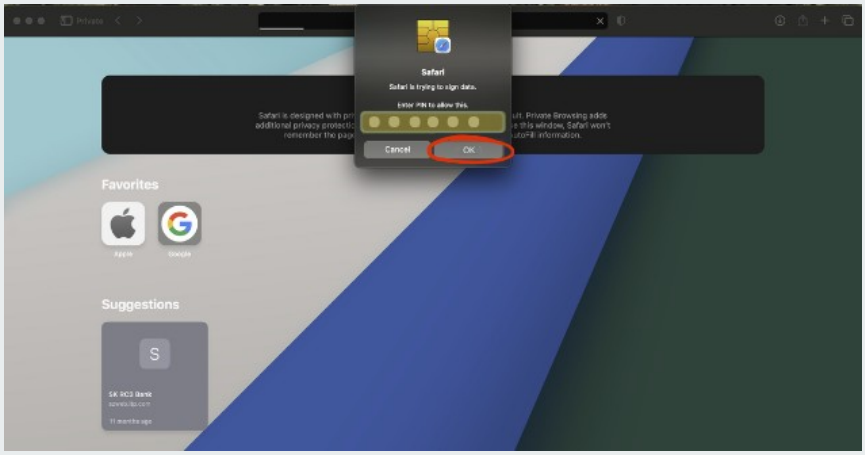
NOTE	You will only see a certificate prompt if the **SB2 Root CA** and **SB2 Subordinate CA** certificates were imported correctly on your computer. If you do **NOT** see a certificate prompt, please contact support@strongkey.com for support.



C10 ENTER SECURITY KEY PIN

The next dialog box will prompt for the iShield2 (aka Smartcard) **PIN**. Enter and **click OK** to continue. This PIN should have been provided by the Administrator of the SB2 platform site.

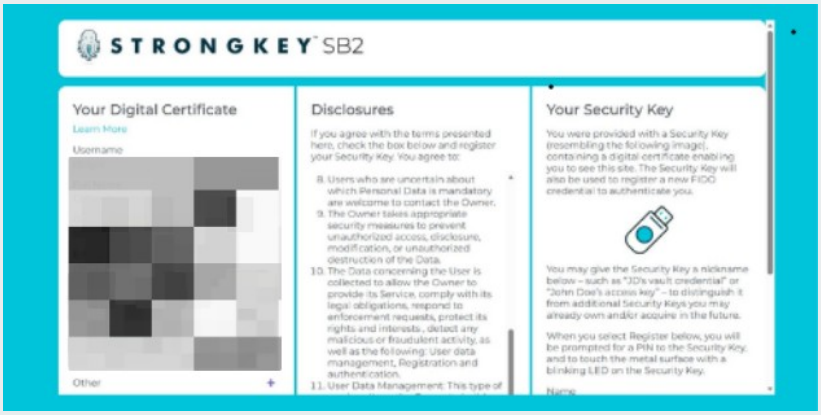
For instructions on changing the iShield2 PIN, refer to the Appendix of this guide.



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.**



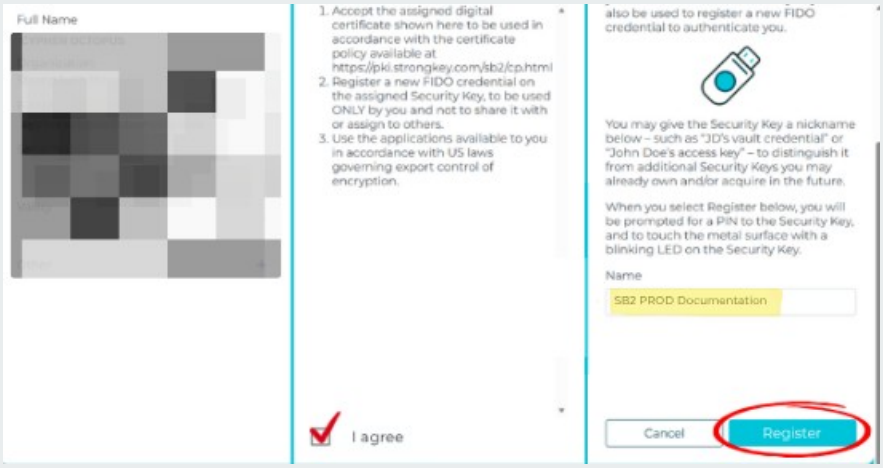
C12 TERMS & CONDITIONS

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

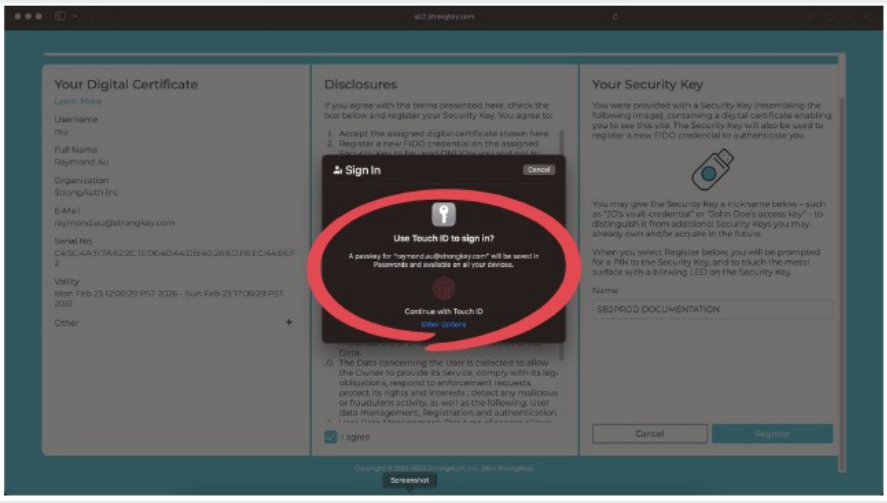
In the Security Key panel on the right, enter a descriptive nickname for the key in the "Name" field. Then select **Register** to complete the process. Names are typically short (up to 16-20 alpha-numeric characters), such as:

- John's Swissbit Security Key for sb2.strongkey.com
- iShield2 for sb2.strongkey.com



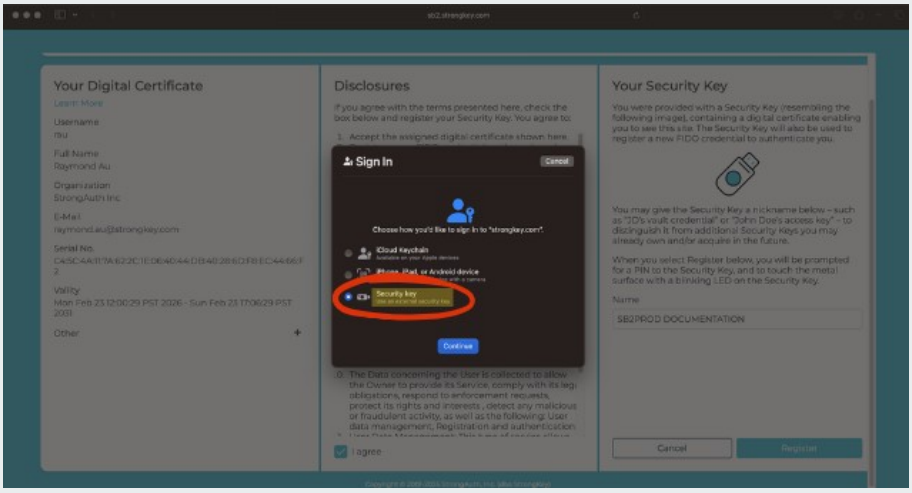
C14 CONTINUE SETUP

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.



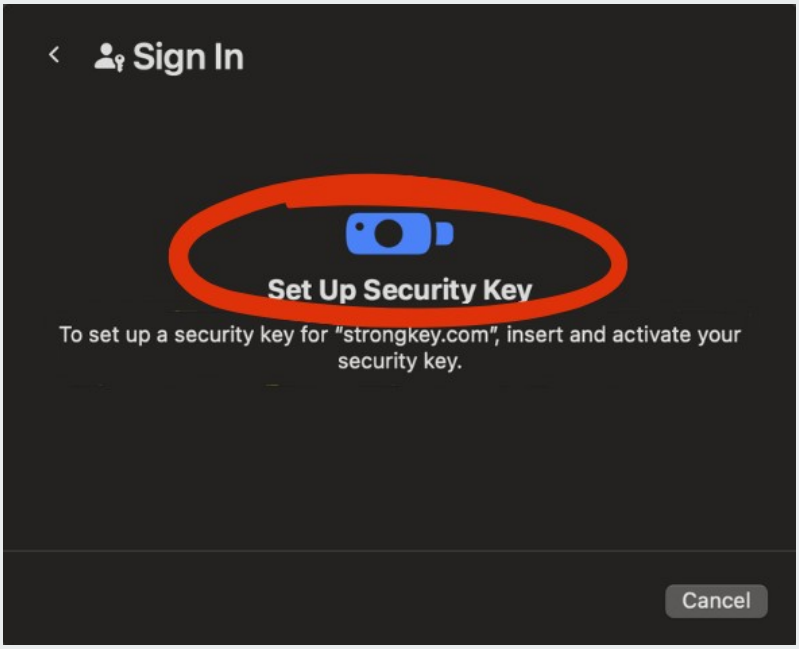
C15 SELECT SECURITY KEY

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.

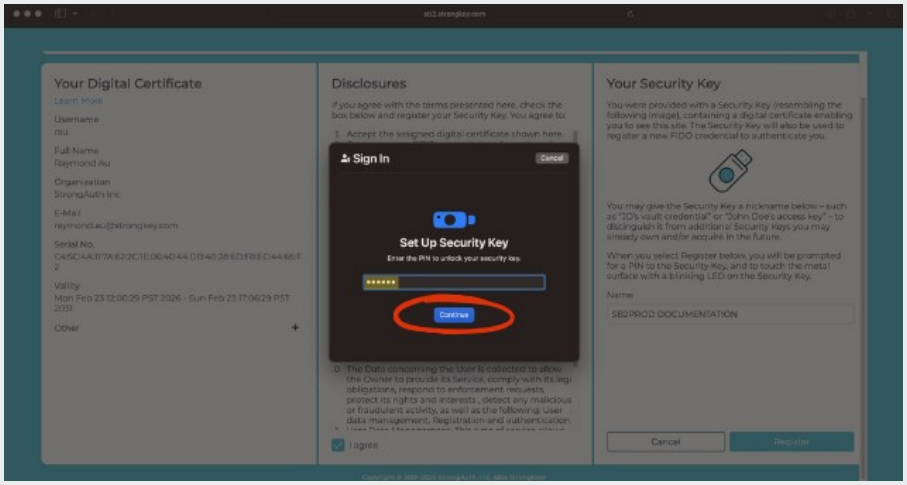


C17 ENTER SECURITY KEY PIN

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

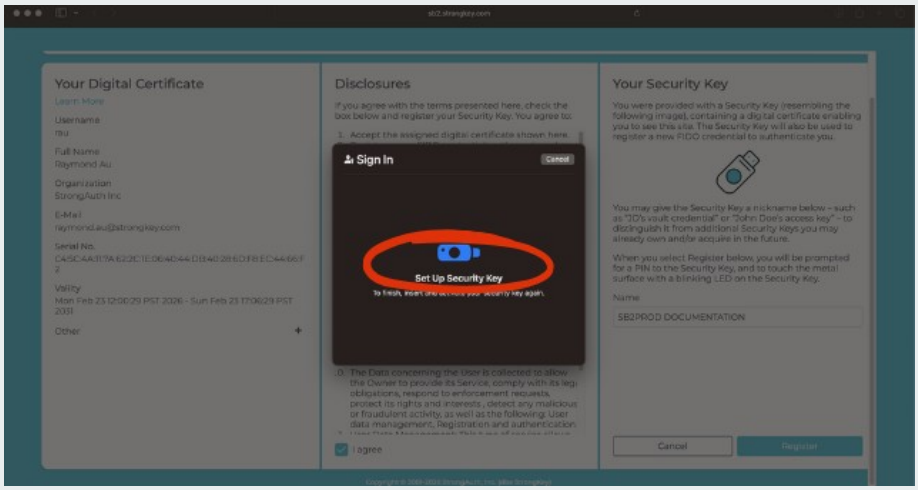
NOTE

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.



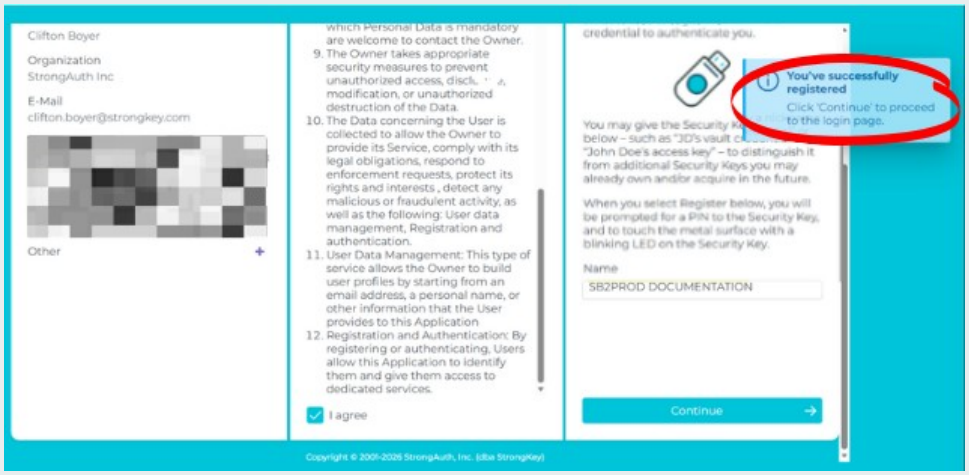
C18 TOUCH THE SECURITY KEY

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.



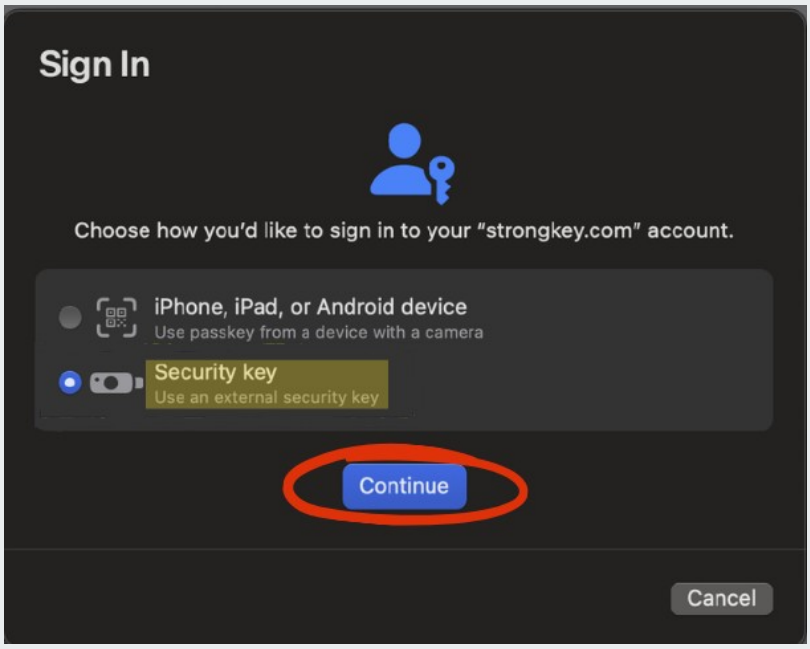
C19 SB2PROD CONFIRMATION

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



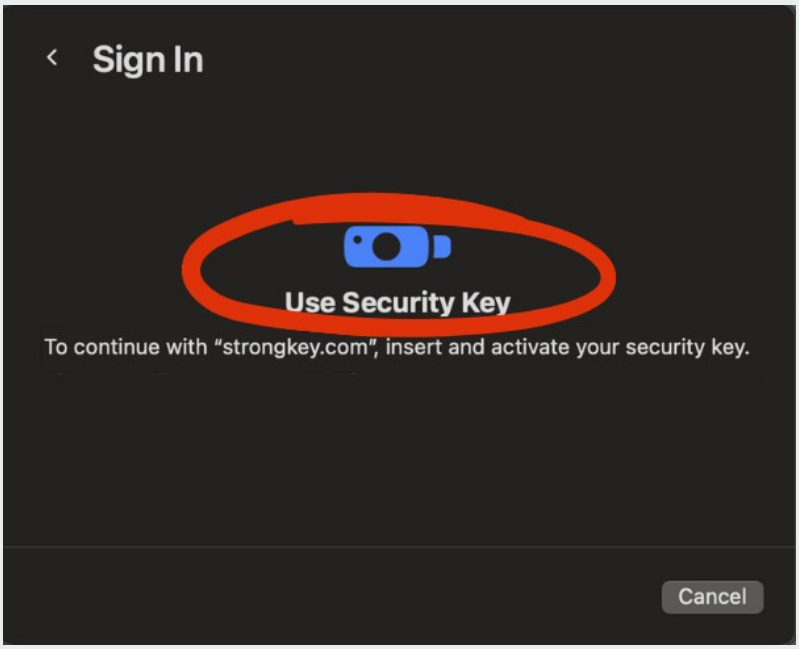
C20 SELECT SECURITY KEY

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.**



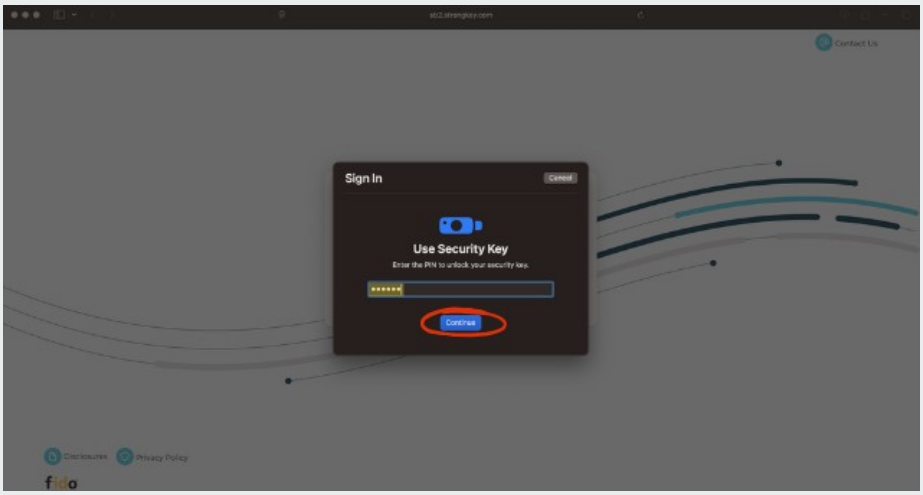
C21 SIGN IN

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



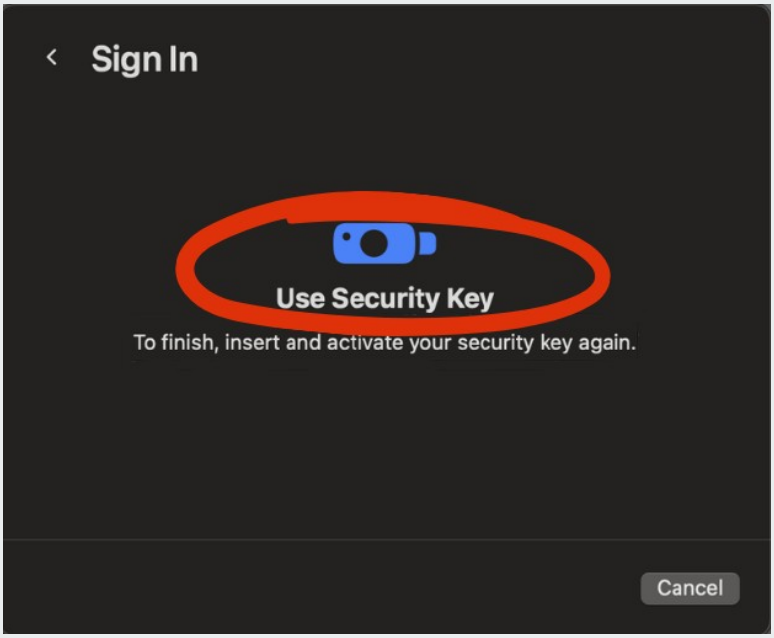
C22 USER AUTHENTICATION

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



C23 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.



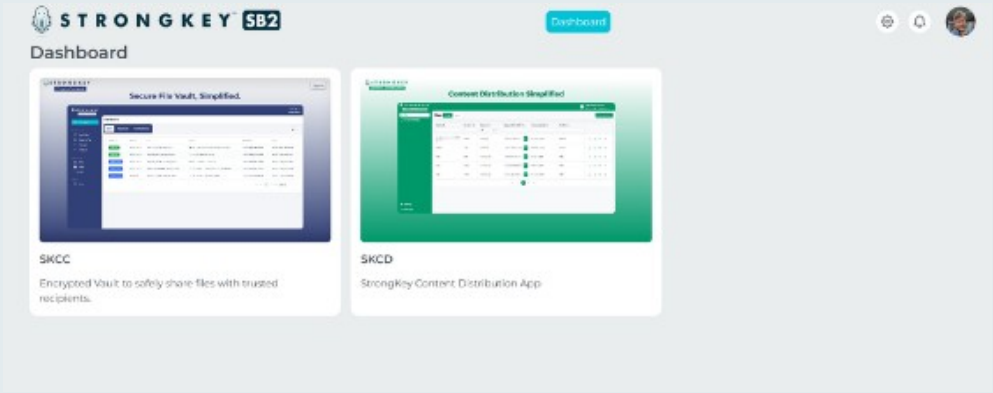
C24 THE SB2PROD PLATFORM DASHBOARD

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:

- **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 iShield2 Security Key.

AP1 CHANGING A SWISSBIT iSHIELD2 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.

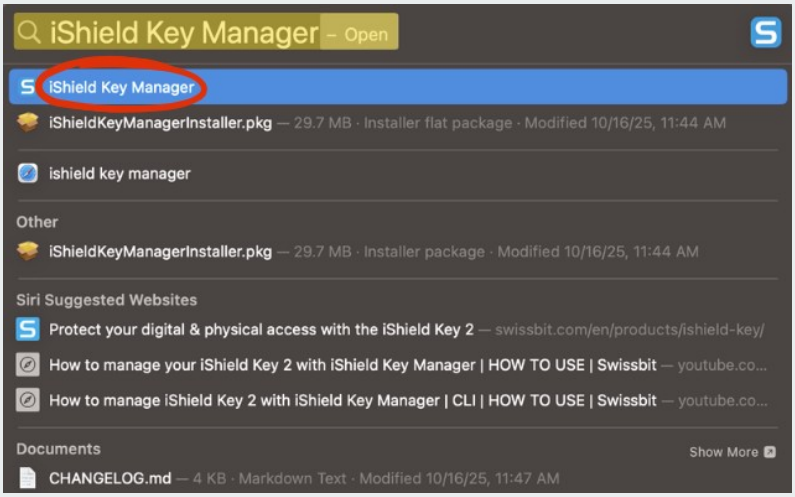
Since the **Security Keys** provided with the SB2 use two different NIST-approved, passwordless authentication protocols, there are two containers for the cryptographic keys used with the protocols. Each container is managed by a separate PIN.

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.

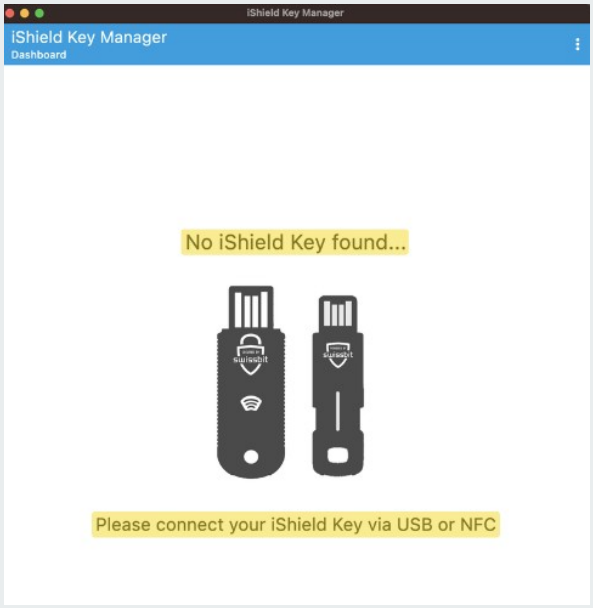
AP2 OPEN THE iSHIELD KEY MANAGER APPLICATION

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



AP3 SELECT iSHIELD KEY MANAGER

When you open the application, it displays the messages **'No iShield Key found'** and **'Please connect your iShield Key via USB or NFC'**.



AP4 INSERT THE iSHIELD2

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.

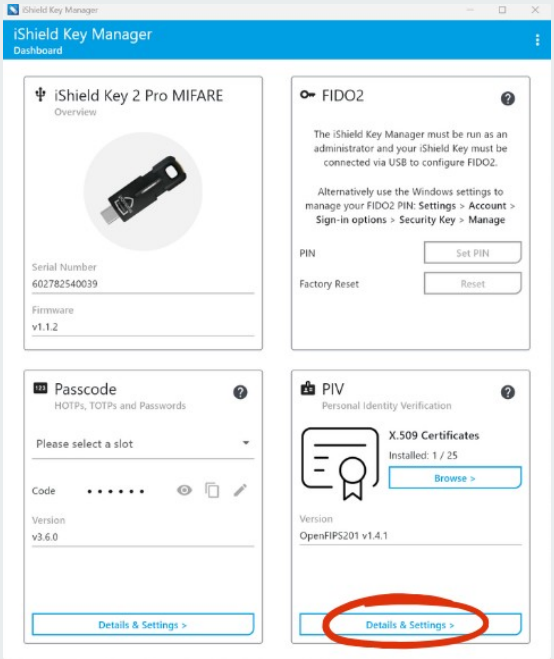
AP6 NO USB-C PORT? NO PROBLEM.

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.

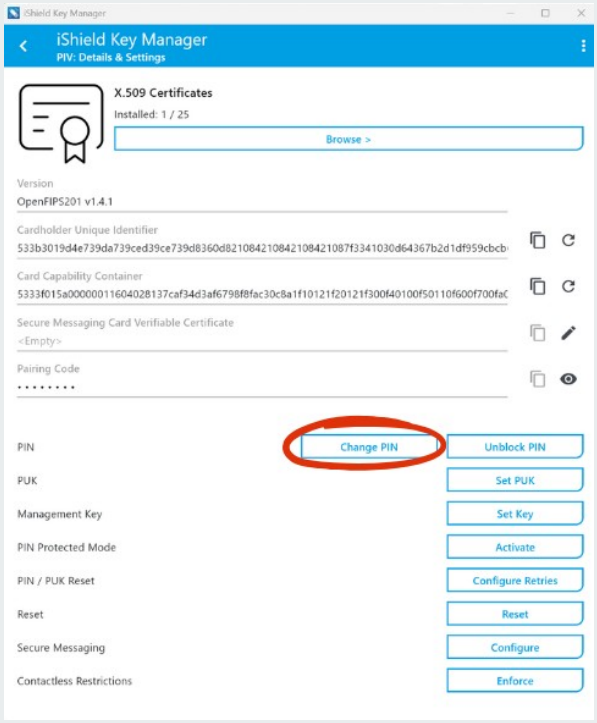
The provided USB adapter pictured below.

AP7 CHANGING PERSONAL IDENTITY VERIFICATION (PIV) PIN

From the home screen, navigate to the lower right-hand side of the screen and open the PIV's **Details & Settings.**

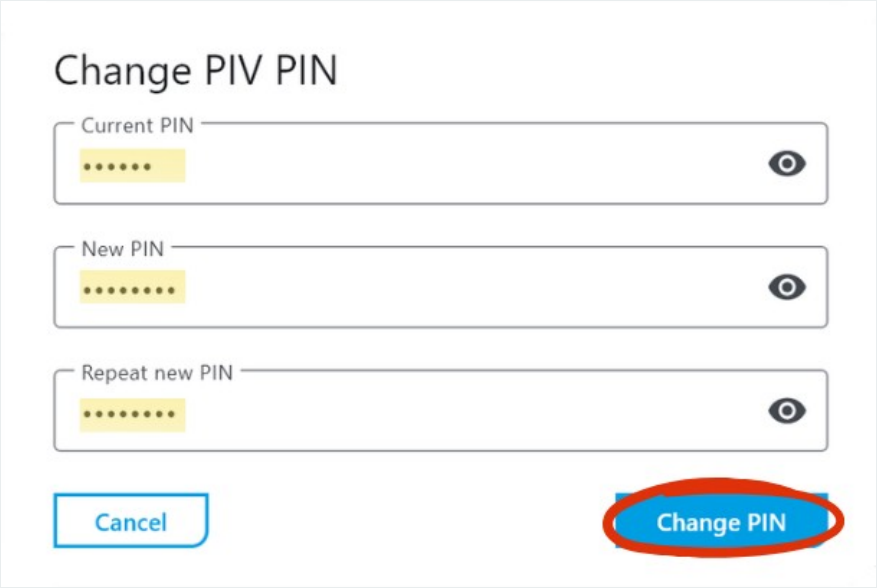


AP8	CHANGE PIN OPTION
Select the **Change PIN** option.	
NOTE	Unless otherwise specified, each PIN on iShield2, must comply with the following rules: • PIN must be at least 6 characters long • 4 identical characters are not permitted (e.g. 2222as), but PIN with 3 identical characters is permitted (e.g. 222asd). • Sequences of numbers are not permitted (e.g. 123456, abcdef).



AP9 ENTER PIN INFORMATION

a) Enter the default PIN **(112233)**.
b) Enter the new PIN. The PIN must contain 6 to 8 characters.
c) Re-enter the new PIN to confirm then click **Change PIN**.

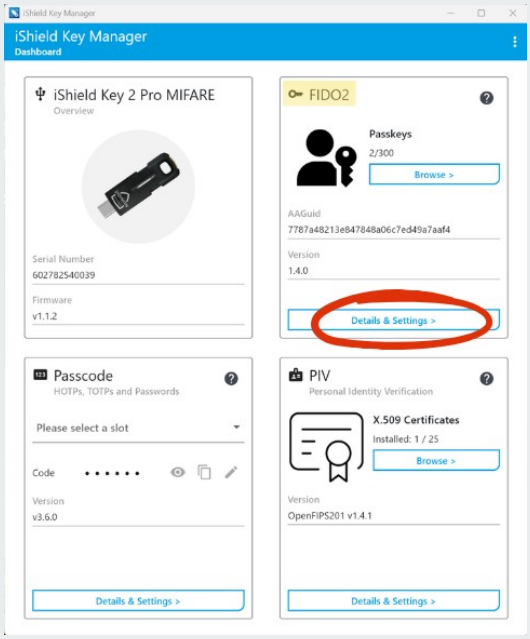


AP10 SUCCESS!

If the PIN was changed succesfully, a confirmation message will appear near the bottom of the application. StrongKey recommends using the same PIN for setting or changing the FIDO PIN.

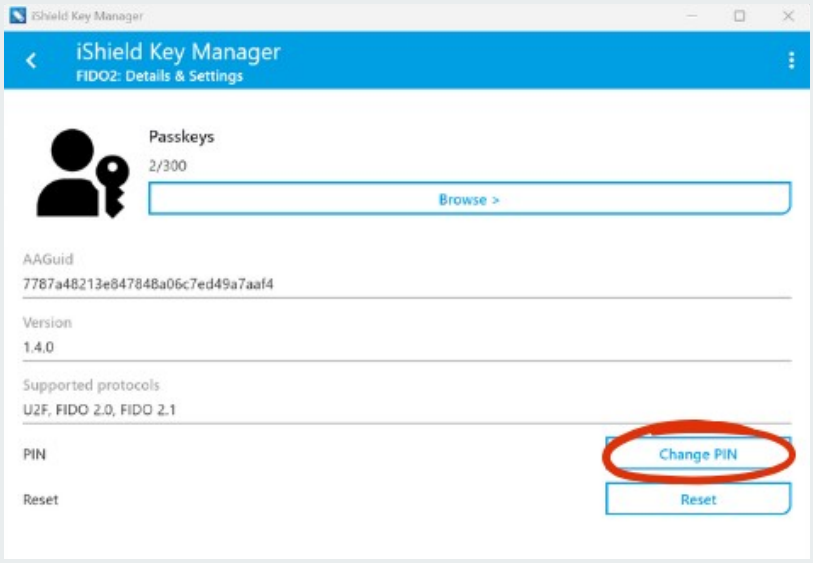
AP11 CHANGING THE FIDO PIN

Changing the PIN for the FIDO2 container uses the same procedure as outlined in steps AP9 – AP11. If the **Details & Settings** button is not accessible, close the iShield Key Manager and reopen but select **Run as administrator** (see Step AP3).



AP12 CHANGE PIN

Click Change PIN.



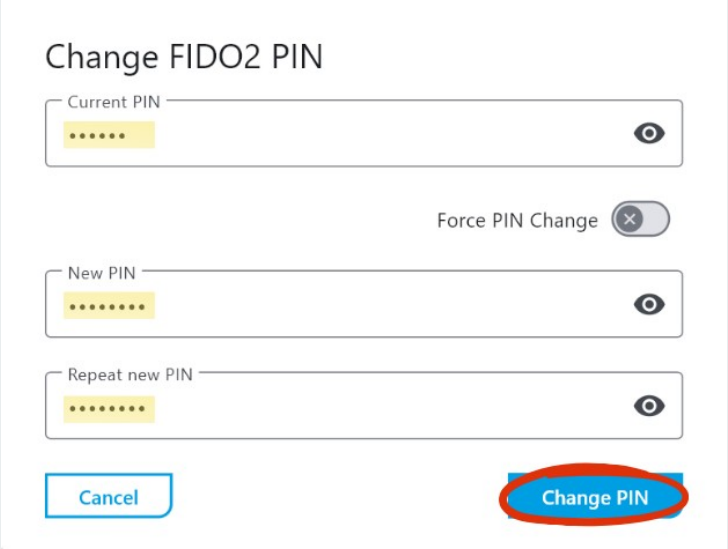
AP13 ENTER NEW PIN

a) Enter the default PIN **(112233)**.
b) Enter the new PIN. The PIN must contain 6 to 8 characters.
c) Re-enter the new PIN to confirm then click Change PIN.

NOTE

Unless otherwise specified, each PIN on iShield2, must comply with the following rules:

- PIN must be at least 6 characters long
- 4 identical characters are not permitted (e.g. 2222as), but PIN with 3 identical characters is permitted (e.g. 222asd).
- Sequences of numbers are not permitted (e.g. 123456, abcdef).



AP14 SUCCESS!

If the PIN was changed succesfully, a confirmation message will appear near the bottom of the application. StrongKey recommends using the same PIN for setting or changing the FIDO PIN.