

# STRONGKEY™

## TELLARO SB2

SWISSBIT iSHIELD KEY 2 PRO USER'S GUIDE FOR macOS

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



## COPYRIGHT & NOTICES

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

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

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

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



## GETTING STARTED: SWISSBIT iSHIELD KEY 2 PRO & SB2PROD PLATFORM

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



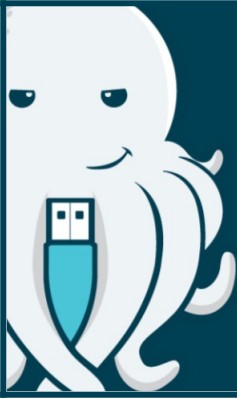
## PREREQUISITES

- 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



# TABLE OF CONTENTS

A	<a href="#"><u>Installing the Swissbit iShield Key Manager</u></a>	4
B	<a href="#"><u>#B1 - importing sb2 root ca sb2</u></a>	14
C	<a href="#"><u>Accessing an SB2PROD Invitation Link</u></a>	36
AP	<a href="#"><u>#Appendix - note: this document is for StrongKey customers</u></a>	58



# 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 SWISSBIT iSHIELD KEY MANAGEMENT KIT (macOS)

To download the iShield Key Management Kit for macOS, go to <https://www.swissbit.com/en/my-swissbit/download-center>. Next, follow these steps:

1. Scroll down to Authentication Products and expand by clicking the plus
2. Select iShield Key 2 (USB-C / NFC)
3. Download iShield Key Management Kit (macOS)

The image is a collage of three screenshots from the Swissbit website, illustrating the steps to download the iShield Key Management Kit for macOS. The screenshots are numbered 1, 2, and 3 with red starburst callouts.

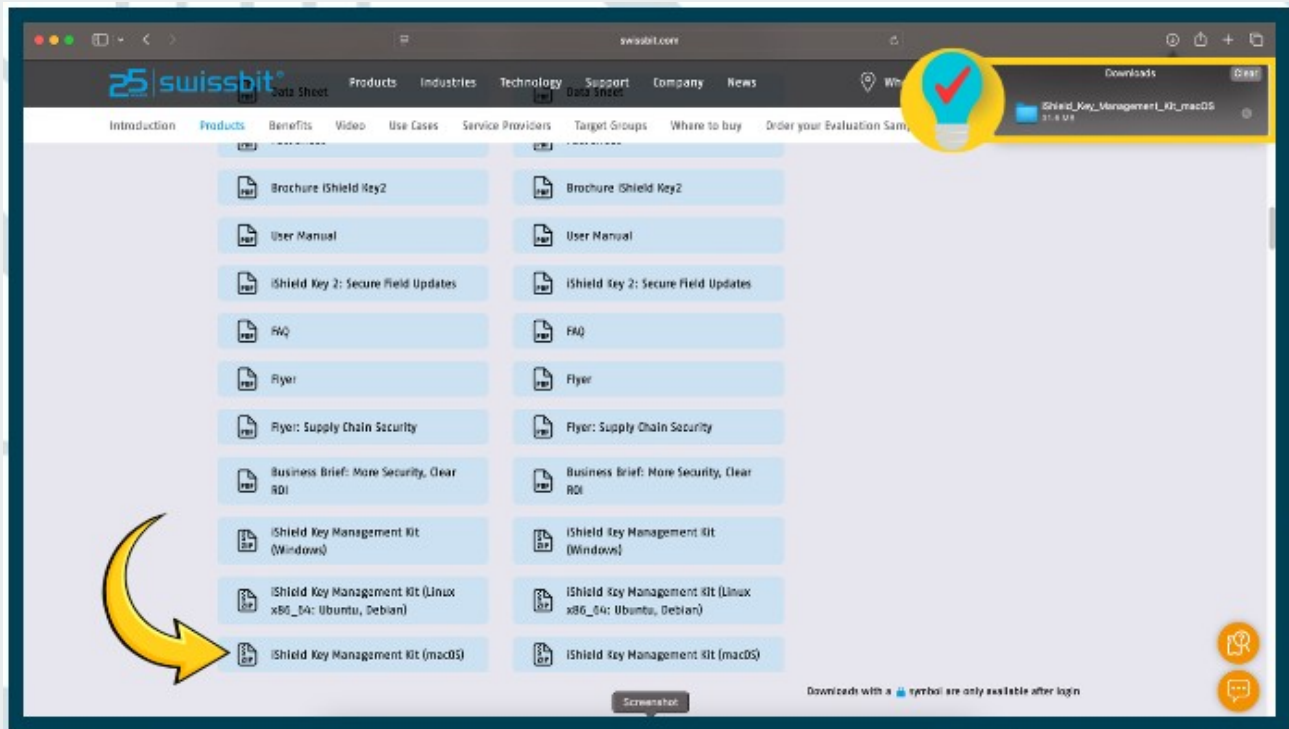
- Step 1:** The first screenshot shows the 'Download Center' page. The search bar contains the URL <https://www.swissbit.com/en/my-swissbit/download-center>. The page title is 'Download Center'. A red starburst with the number '1' is in the top right corner.
- Step 2:** The second screenshot shows the 'Authentication Products' page. The 'iShield Key 2' dropdown menu is expanded, showing 'iShield Key 2 (USB-C / NFC)' and 'iShield Key 2 (USB-A / NFC)'. A red starburst with the number '2' is in the top right corner.
- Step 3:** The third screenshot shows the 'Download Center' page. The 'iShield Key Management Kit (macOS)' option is selected, and a red download icon is visible. A red starburst with the number '3' is in the top right corner.

A large blue square with a white download icon is positioned to the right of the third screenshot.

# A3

## OPENING THE iSHIELD KEY MANAGEMENT KIT (macOS) FILE

After clicking the download link, Safari will display a pop-up confirming the iShield Key Management Kit file has been successfully downloaded and ready for access.



# A4

## OPEN THE macOS FINDER APP



Open **Finder** and select **Downloads** from the **Favorites** sidebar. Locate the ZIP file and **double-click** it to extract its contents (1). After double-clicking, the extracted files will appear in in a blue folder above the ZIP file (2).

The first screenshot shows the 'Downloads' folder in Finder. The file 'iShield\_Key\_Management\_Kit\_macOS.zip' is selected, and a red mouse cursor is hovering over it. A yellow circle highlights the 'Downloads' title in the top bar. A blue star icon with the number '1' is in the top right corner.

Name	Size	Kind
iShield_Key_Management_Kit_macOS.zip	31.6 MB	ZIP archive
ta.key	636 bytes	Keynote
client.conf.yk	424 bytes	Document
cacert.pem	2 KB	printable...
Firefox 136.0.4.dmg	131.3 MB	Disk Image

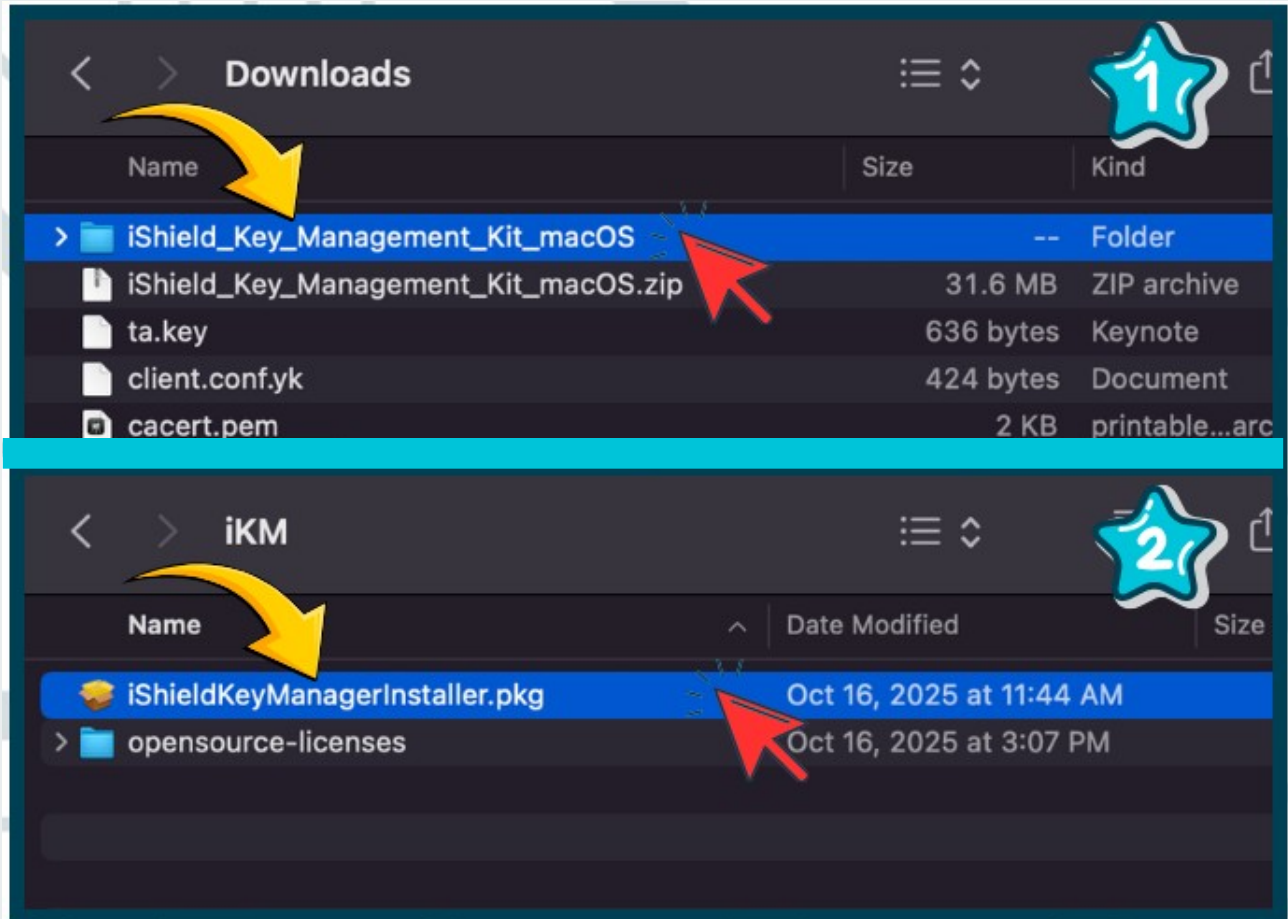
The second screenshot shows the same 'Downloads' folder after the ZIP file has been extracted. A new folder named 'iShield\_Key\_Management\_Kit\_macOS' is now visible at the top of the list, highlighted in blue. A yellow arrow points from the folder name to the first screenshot. A blue star icon with the number '2' is in the top right corner.

Name	Size	Kind
iShield_Key_Management_Kit_macOS	--	Folder
iShield_Key_Management_Kit_macOS.zip	31.6 MB	ZIP archive
ta.key	636 bytes	Keynote
client.conf.yk	424 bytes	Document
cacert.pem	2 KB	printable...

# A5

## LAUNCH THE INSTALLER

Open the iShield\_Key\_Management\_Kit\_macOS folder by **double-clicking** it (image 1). To begin the installation, **double-click** the iShieldKeyManagerinstaller.pkg file to launch the installer.

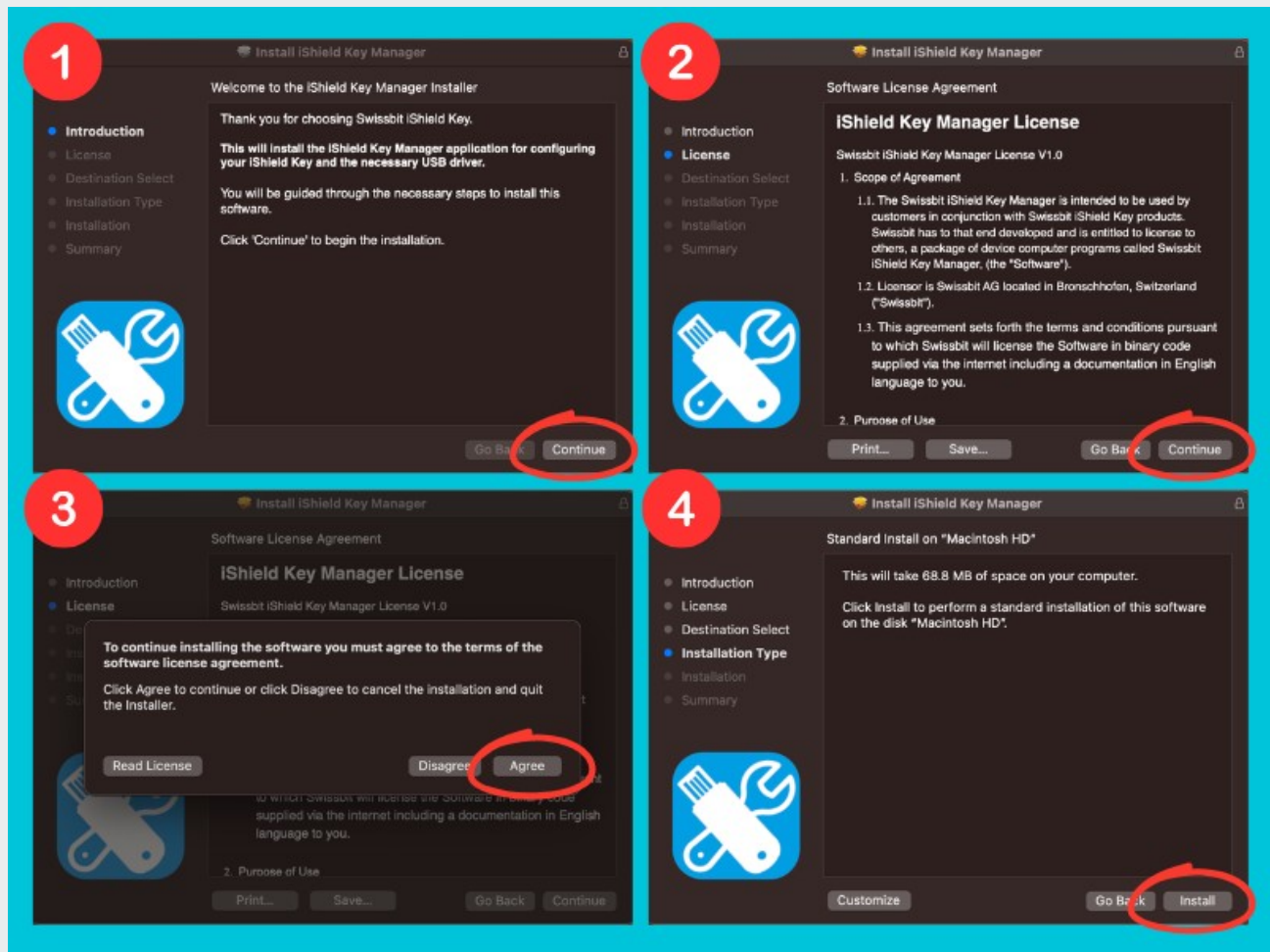


# A6

## iSHIELD KEY MANAGER INSTALL

Follow the onscreen prompts to install the iShield Key Manager Application:

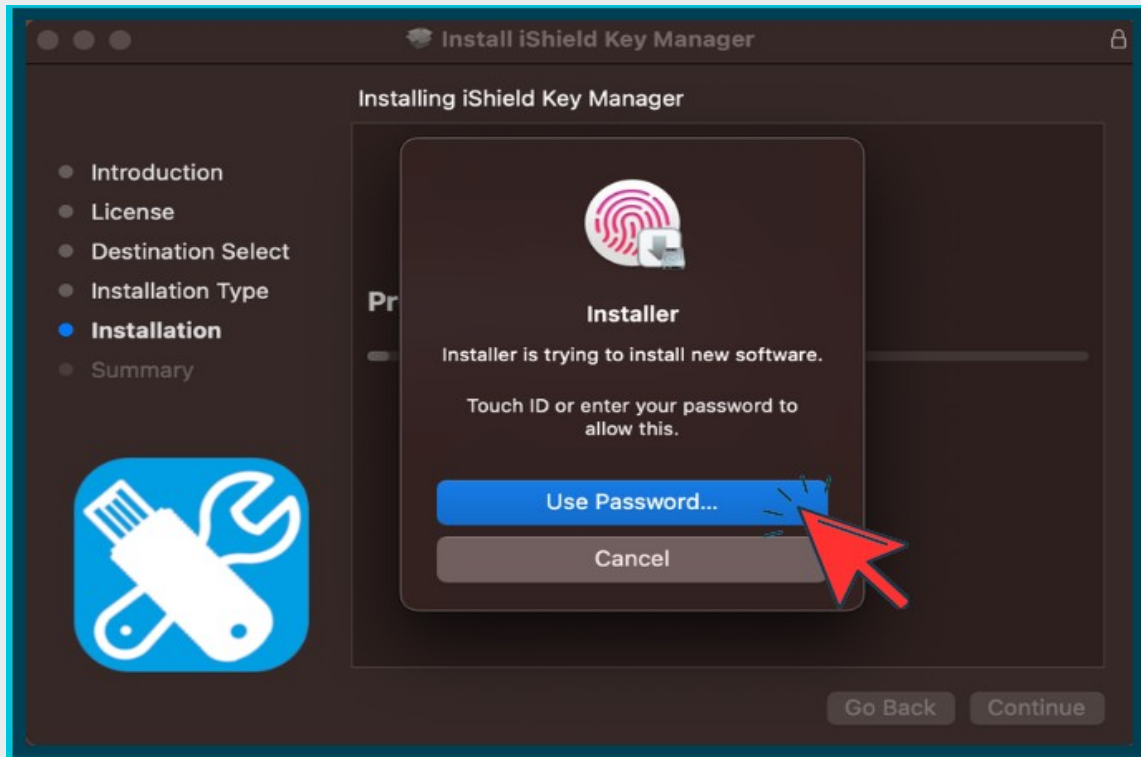
1. Introduction: **Click Continue**
2. License: **Click Continue**
3. Terms of Agreement: **Click Agree**
4. Installation Type: **Verify Standard install and Click Install**



# A7

## ALLOW THE INSTALL

Your Mac will ask permission to install the iShield Key Manager application.  
Click Use Password.



# A8

## ENTER PASSWORD

Enter password and click Install Software.



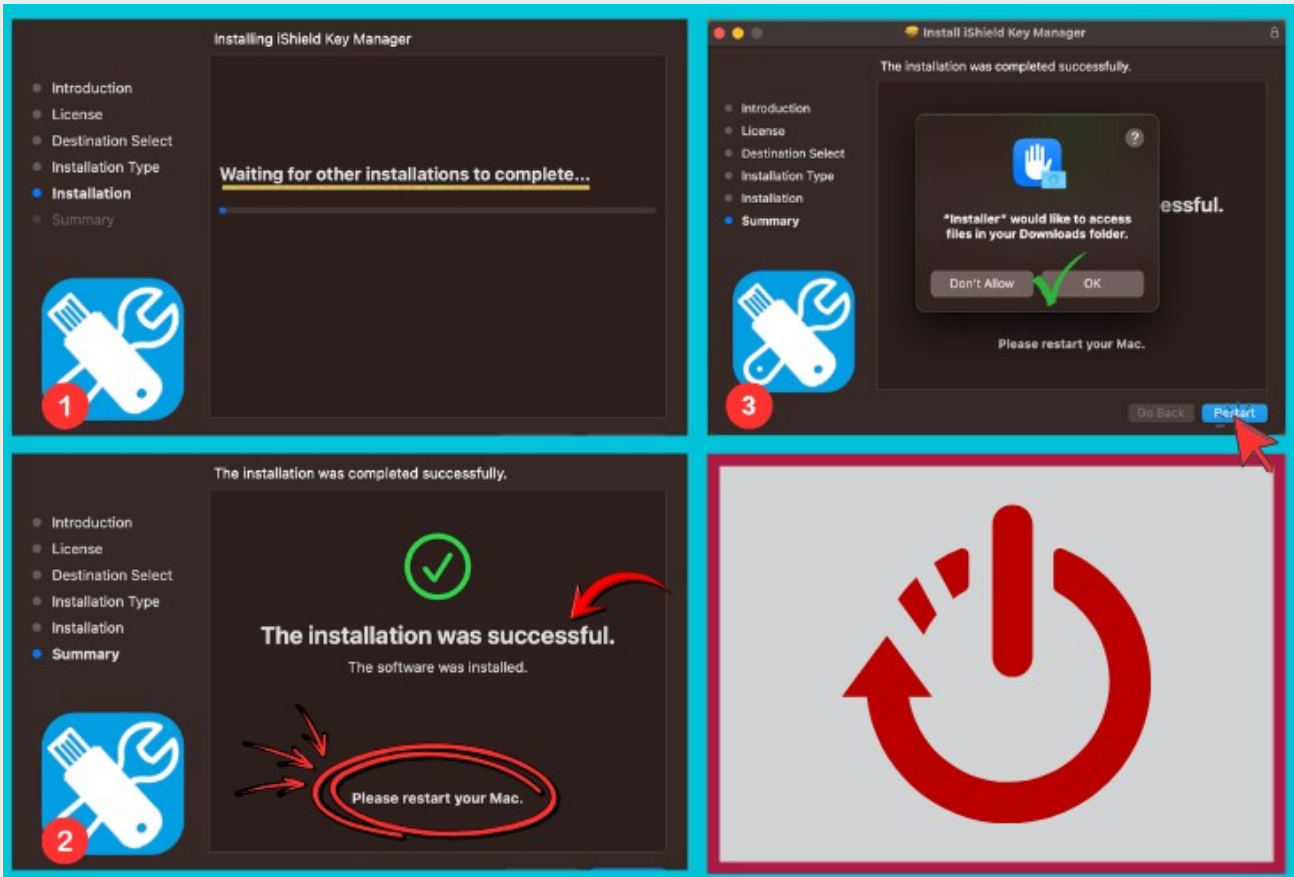
# A9

## FINISH THE INSTALL

Once the progress bar (image 1) finishes, a success message will appear (image 2). Close the installer, save any open work, and restart your computer to complete the setup (image 3).



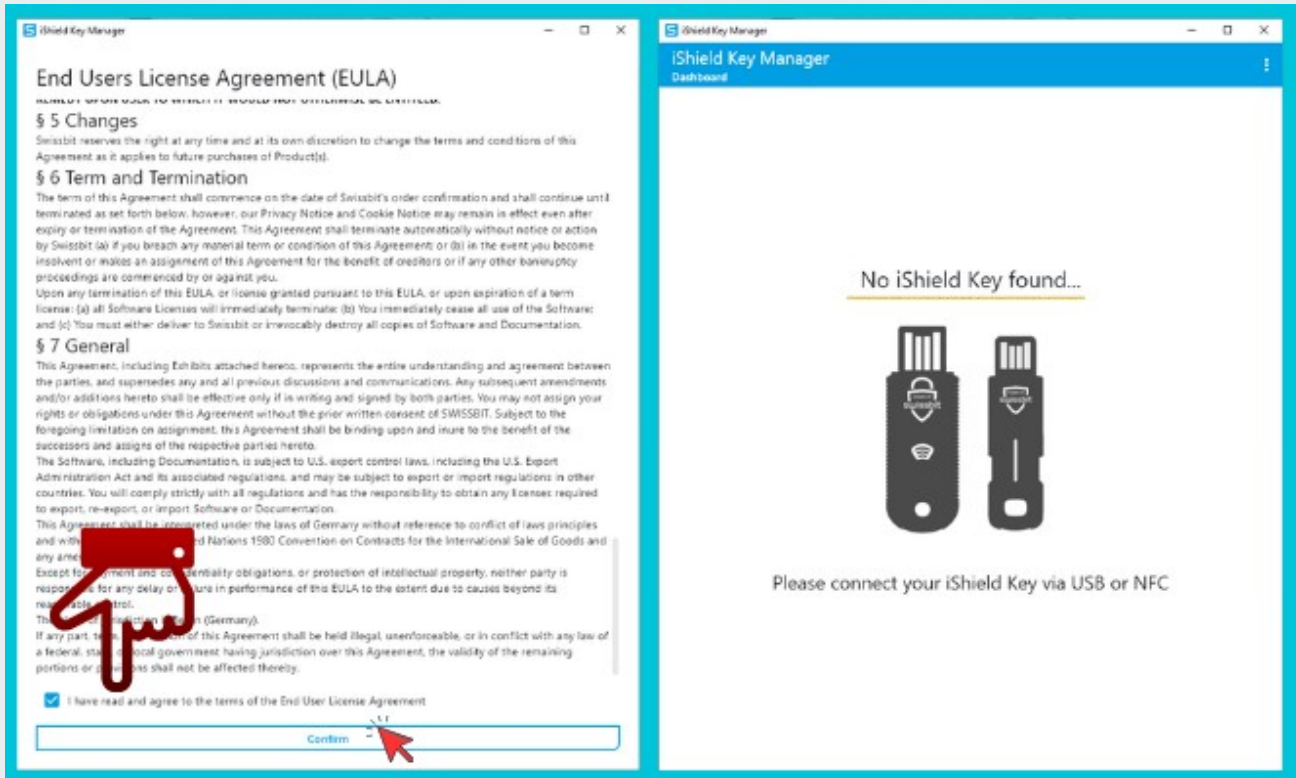
Restarting your computer is a vital step with any software installation. The restart ensures all files are loaded and active.

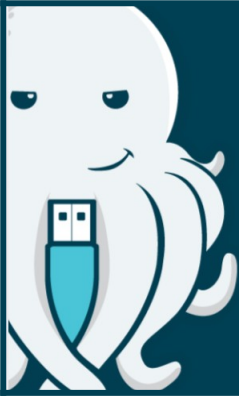


# A10

## OPENING iSHIELD KEY MANAGER FOR THE FIRST TIME

The first time you open iShield Key Manager, review and Agree to the license terms, then click Confirm. The app will then show whether your iShield2 is currently plugged in.





# SECTION B

**B1**

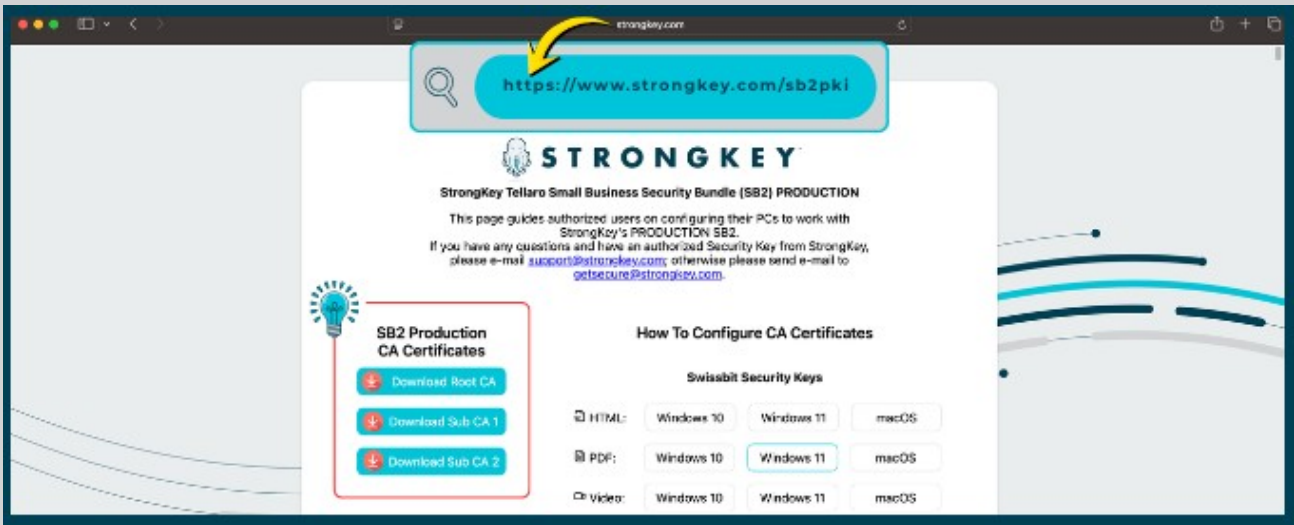
## **IMPORTING SB2 ROOT CA & SB2 SUBORDINATE CA CERTIFICATES ON macOS KEYCHAIN ACCESS**

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>.



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

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

**STRONGKEY**

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

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

**SB2 Production CA Certificates**

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

**How To Configure CA Certificates**

**Swissbit Security Keys**

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

**Yubikey Security Keys**

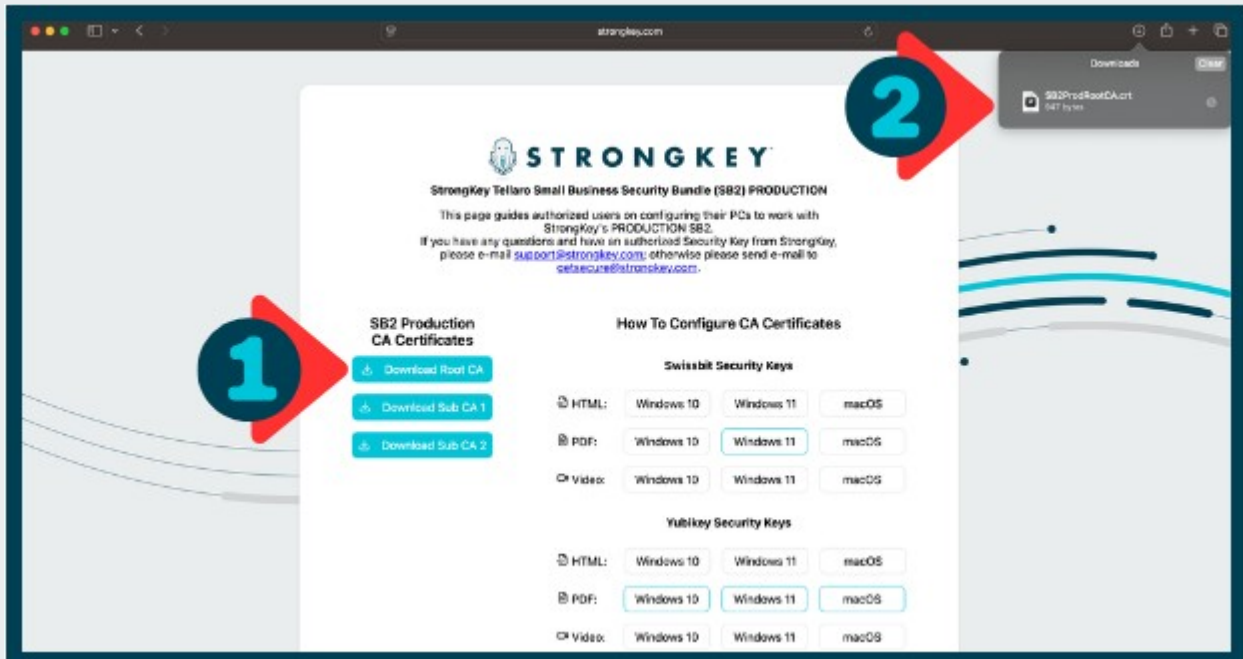
HTML:	Windows 10	Windows 11	macOS
-------	------------	------------	-------

# B4

## DOWNLOADING THE SB2 ROOT CA

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

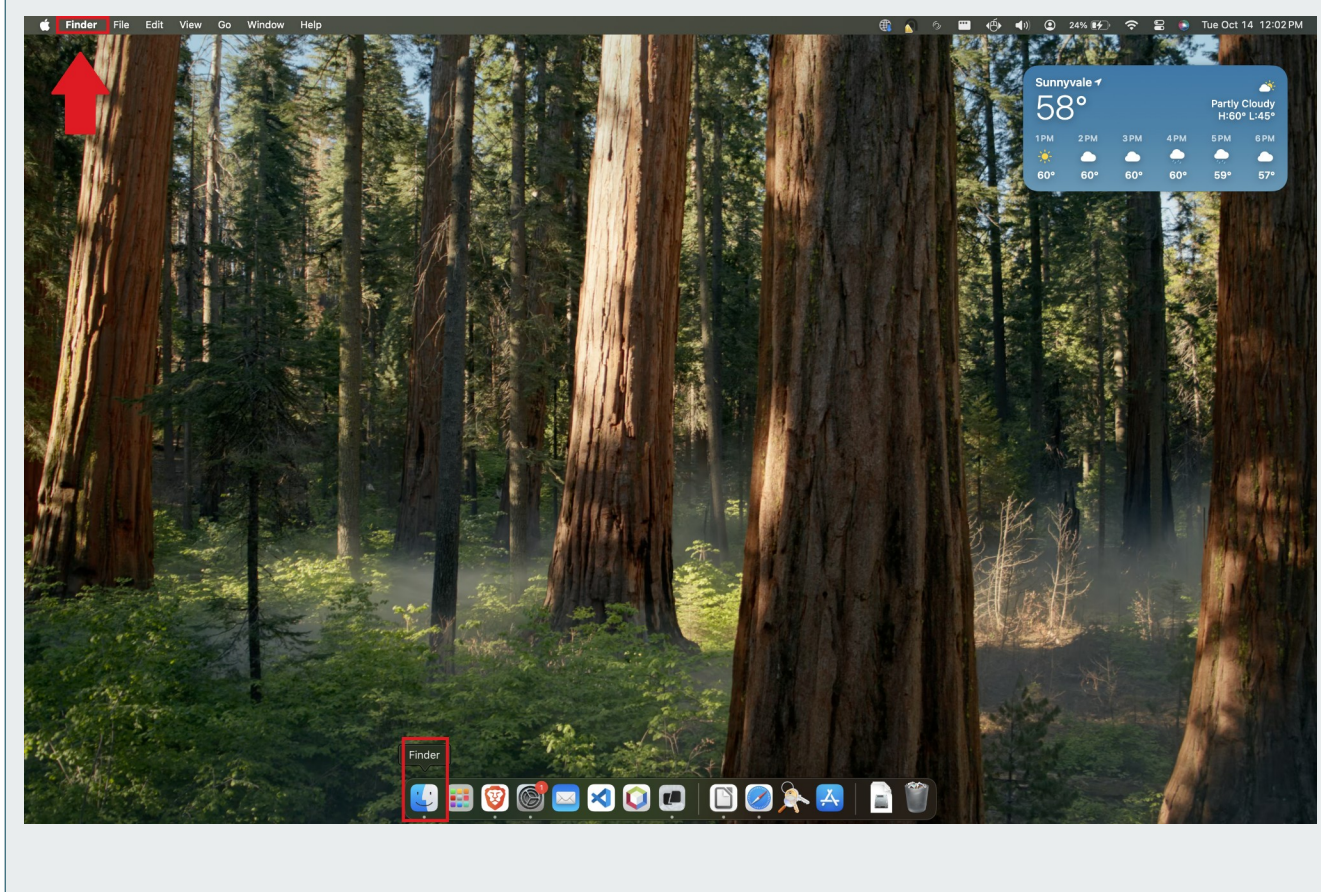
**REPEAT** this process for the Sub CA 1 and Sub CA 2 certificates.



# 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

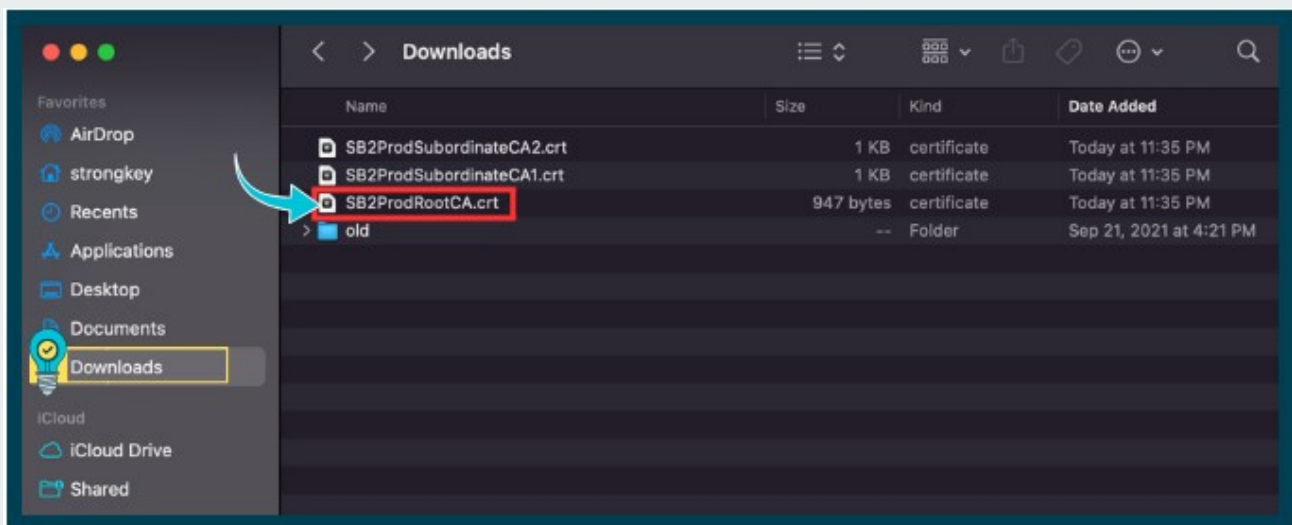
## LOCATE DOWNLOADED SB2 ROOT CA FILE

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

### NOTE



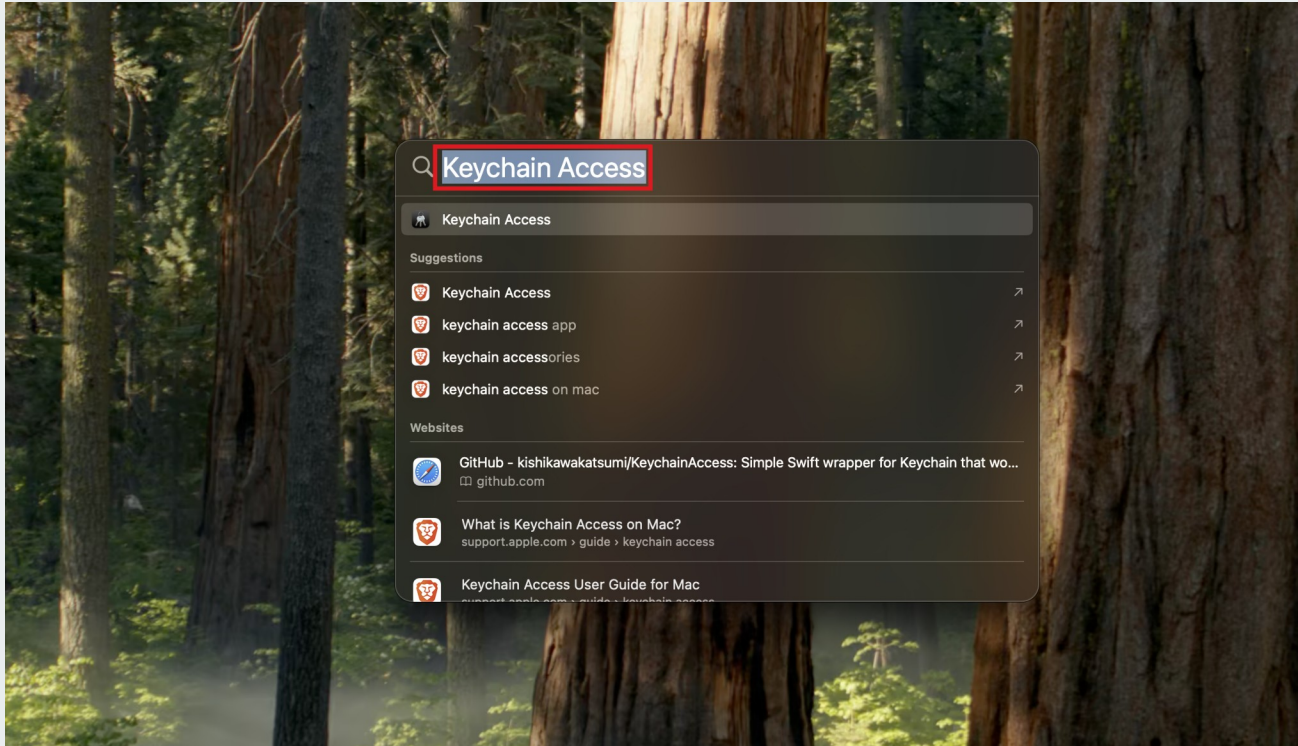
*Please note* that your specific **SB2 certificate files** may have a different name. Ensure you know the correct file name before proceeding.



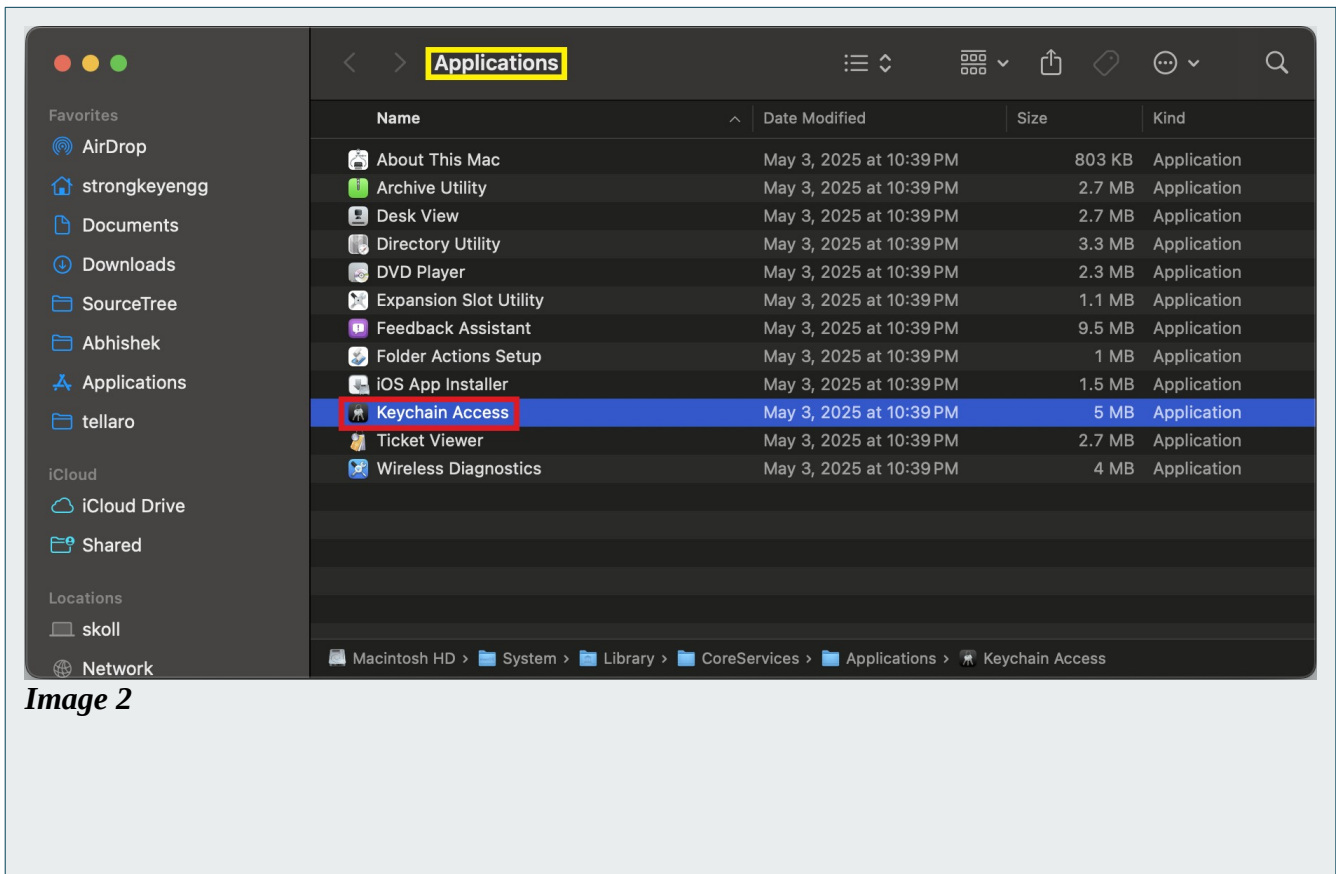
# B7

## 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*

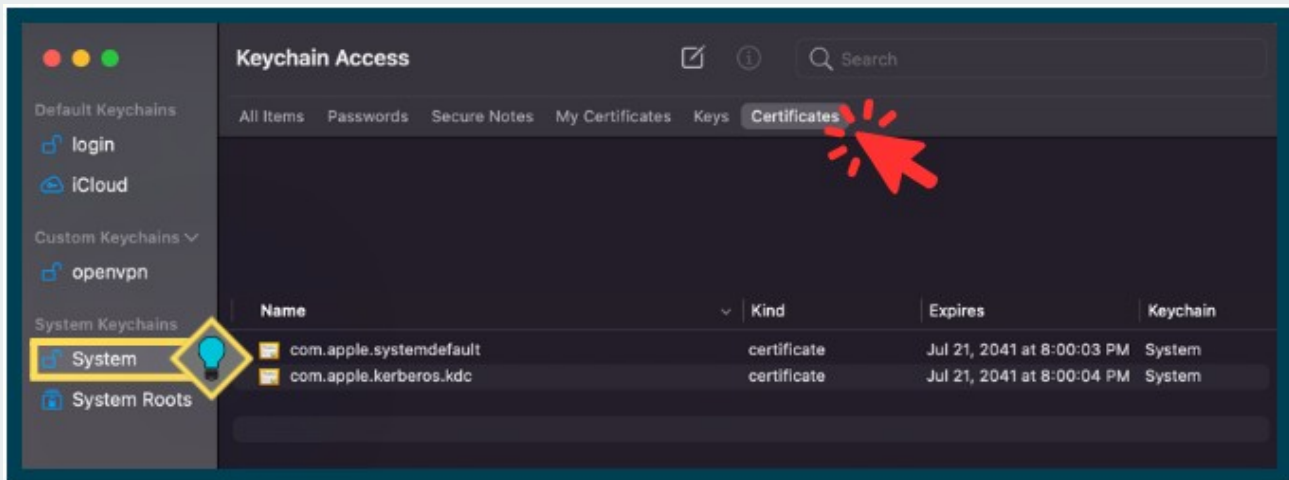


**Image 2**

# B8

## NAVIGATING IN THE KEYCHAIN ACCESS APPLICATION

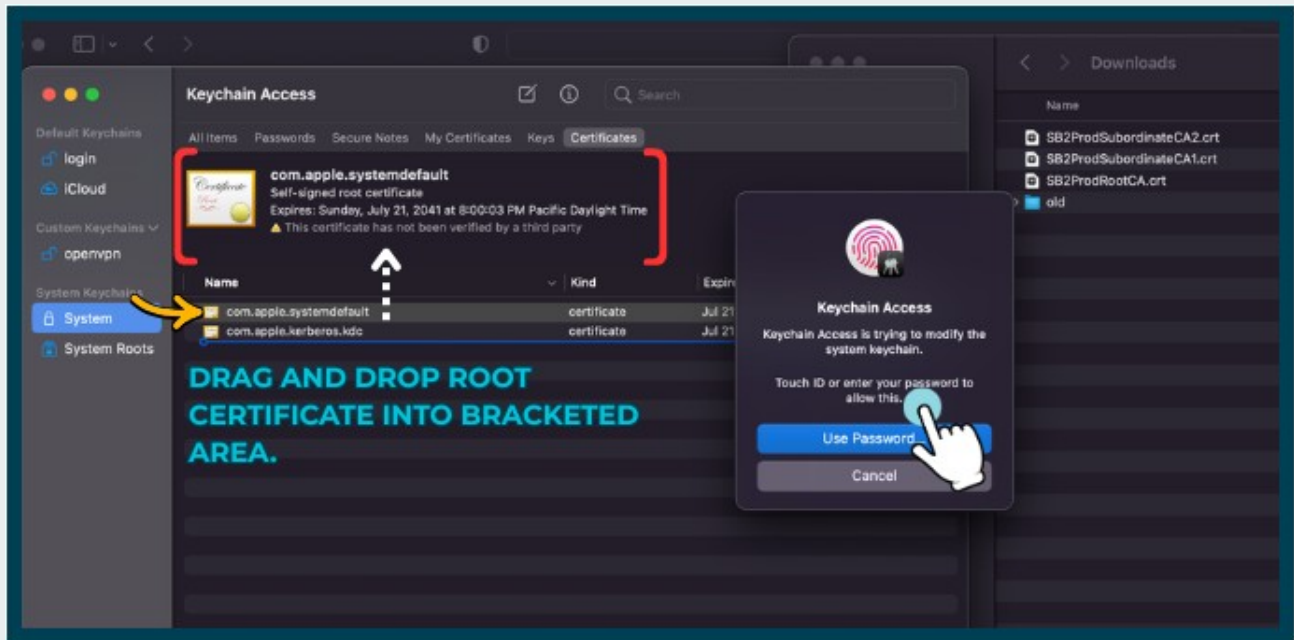
After launching the **KeyChain Access** application, the following screen appears. Select **System** in the sidebar, followed by **Certificates** in the top menu.



# B9

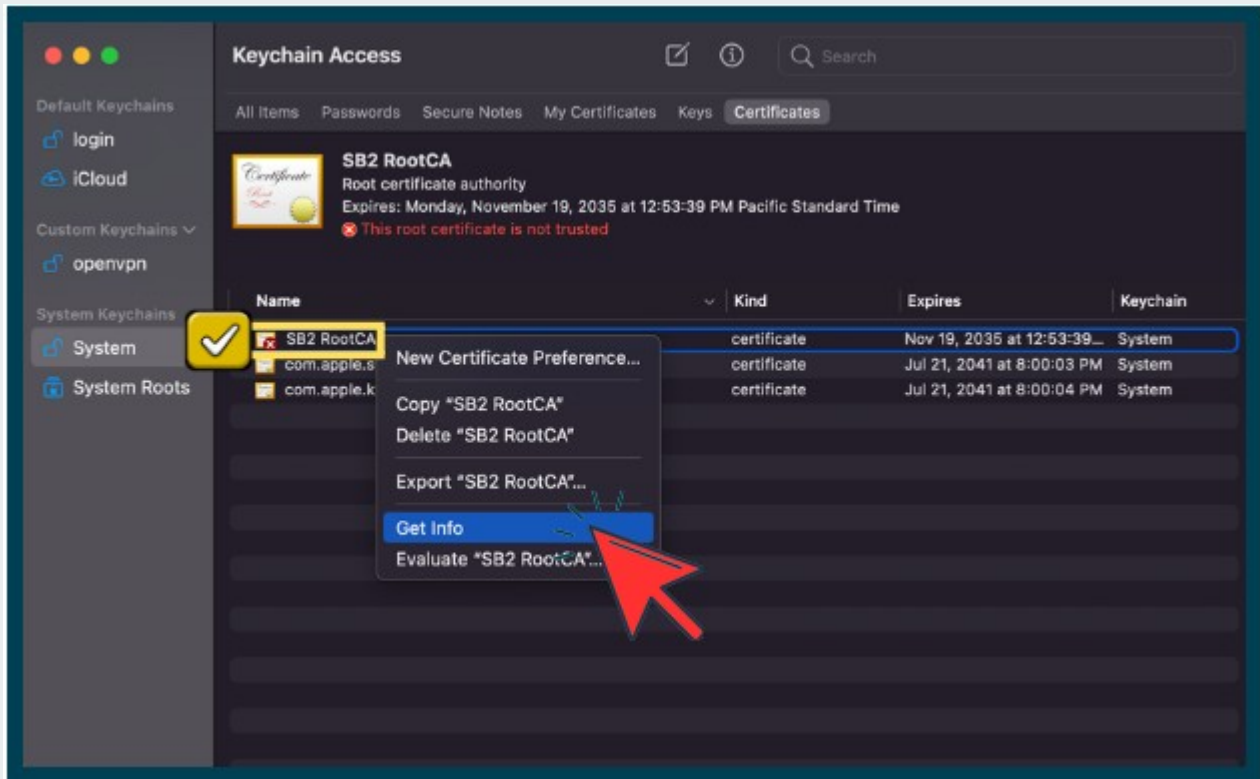
## IMPORTING CERTIFICATES

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.



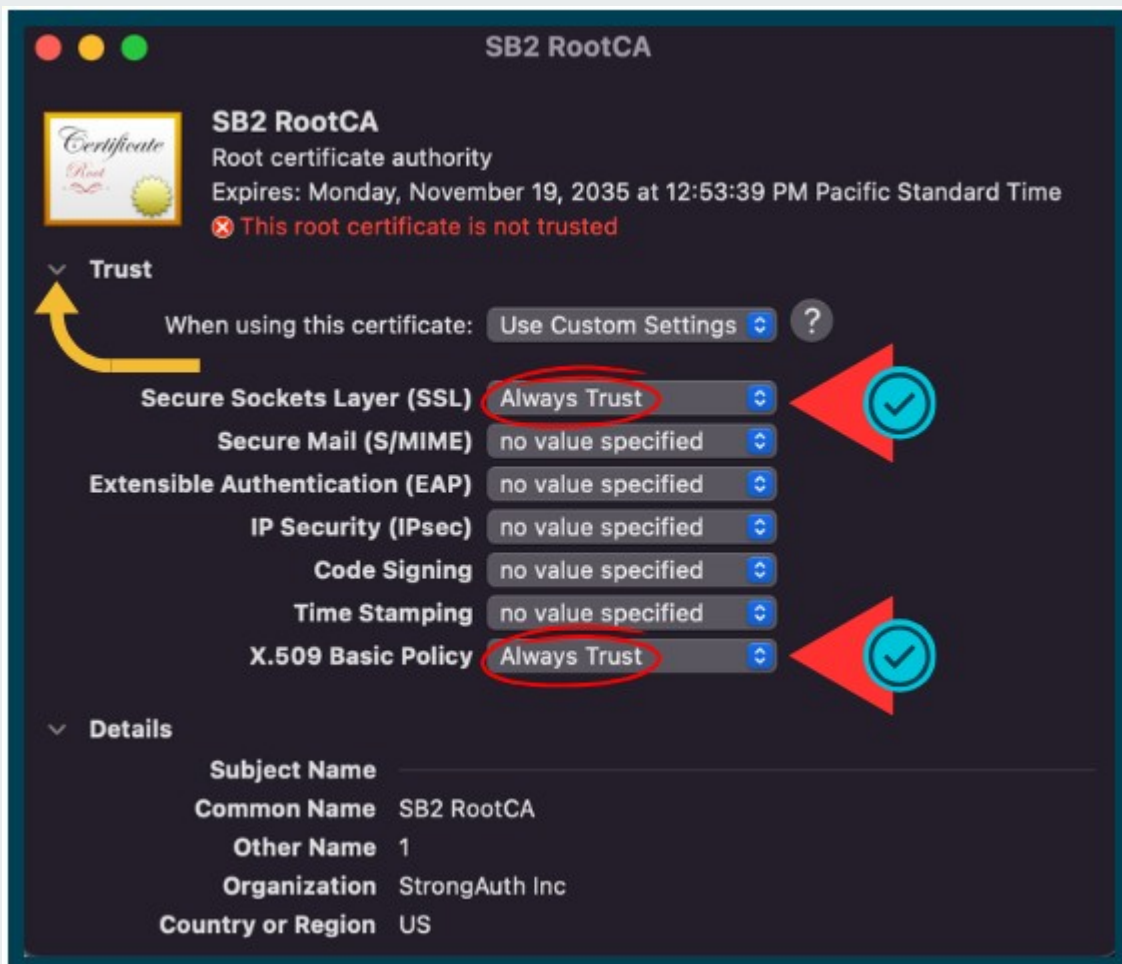
## ACCESS THE SB2 ROOTCA CERTIFICATE

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



## TRUST THE SB2 ROOTCA CERTIFICATE

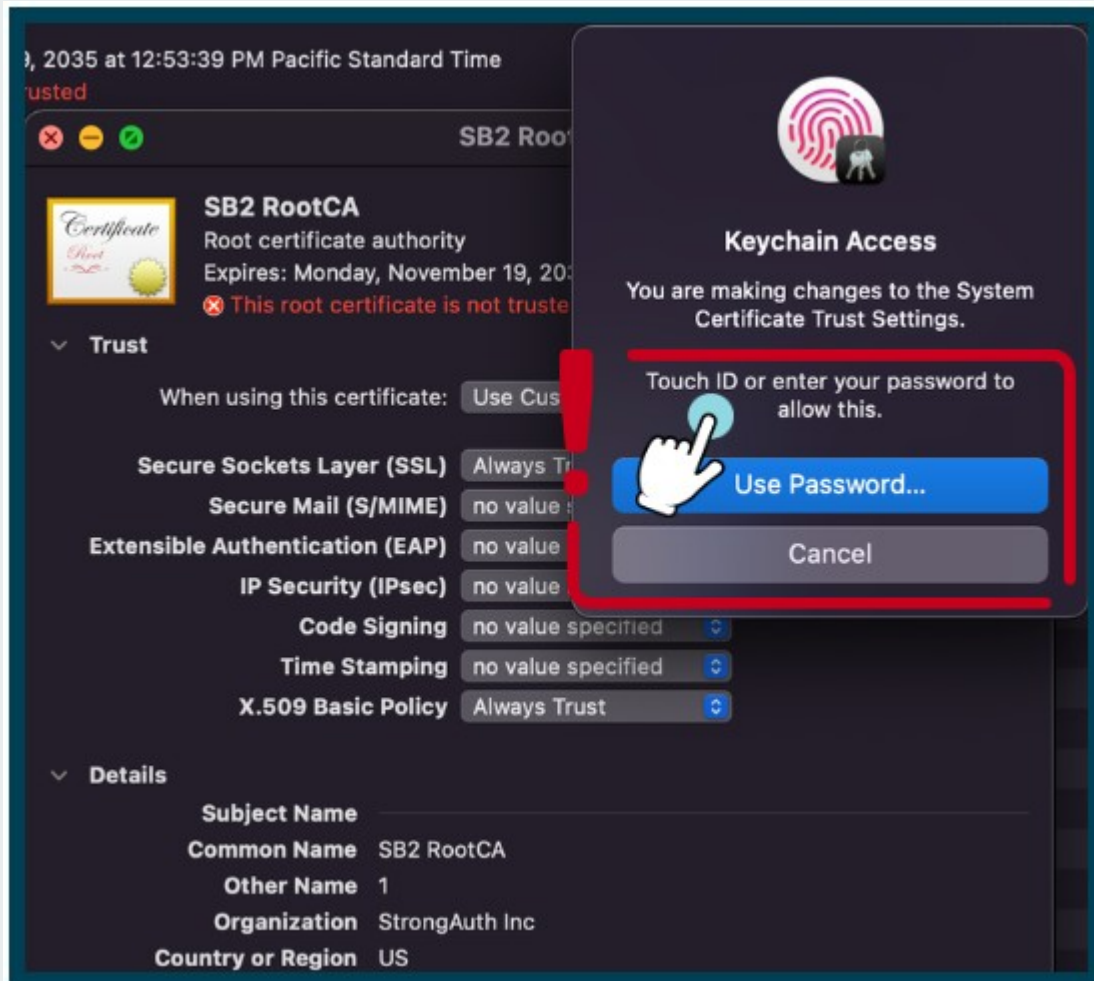
To view the **Trust** details, click the down arrow next to the Trust option. Then, select **Always Trust** for both **Secure Sockets Layer (SSL)** and **X.509 Basic Policy**.



# B12

## AUTHENTICATING THE CHANGES TO THE SB2 ROOTCA CERTIFICATE

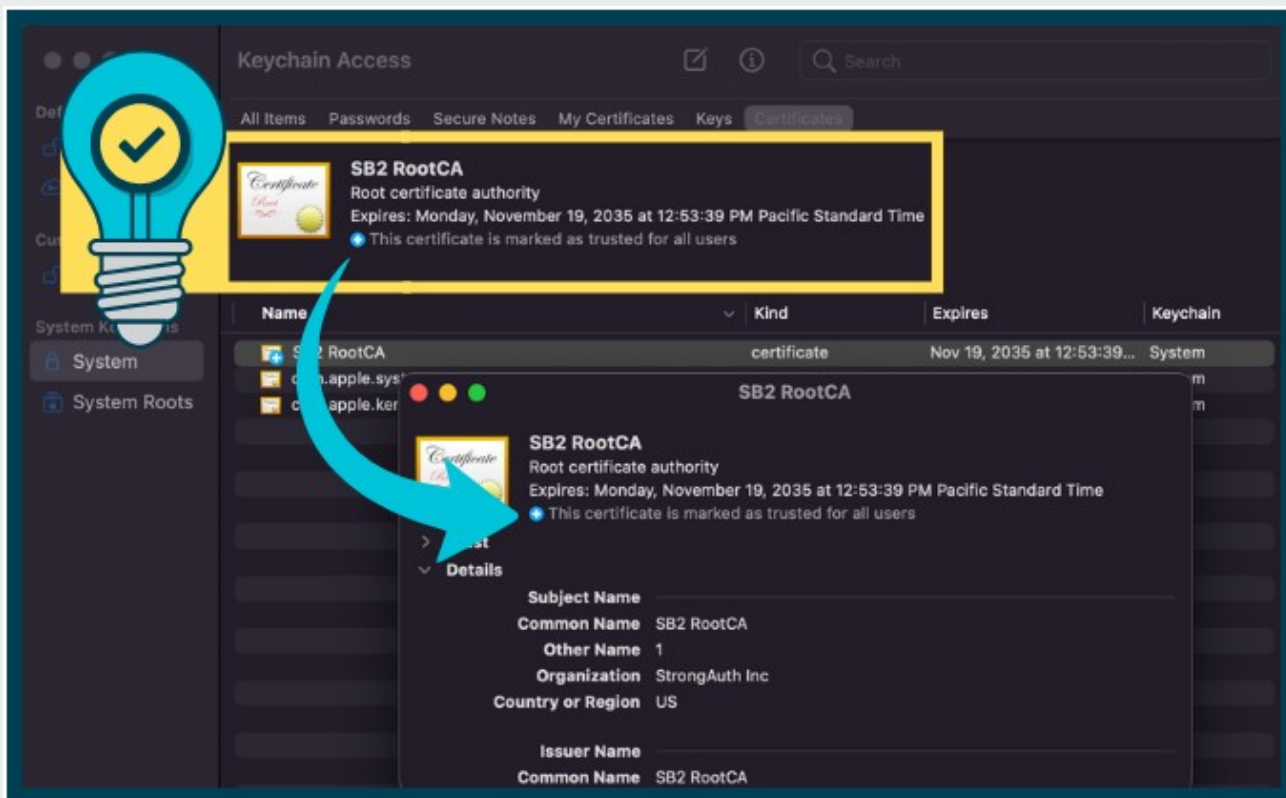
After the SB2 RootCA Get Info window is closed, macOS prompts for authentication, using either Touch ID or the macOS account password, to confirm changes to the Trust settings.



# B13

## CONFIRMING THE TRUST CHANGES

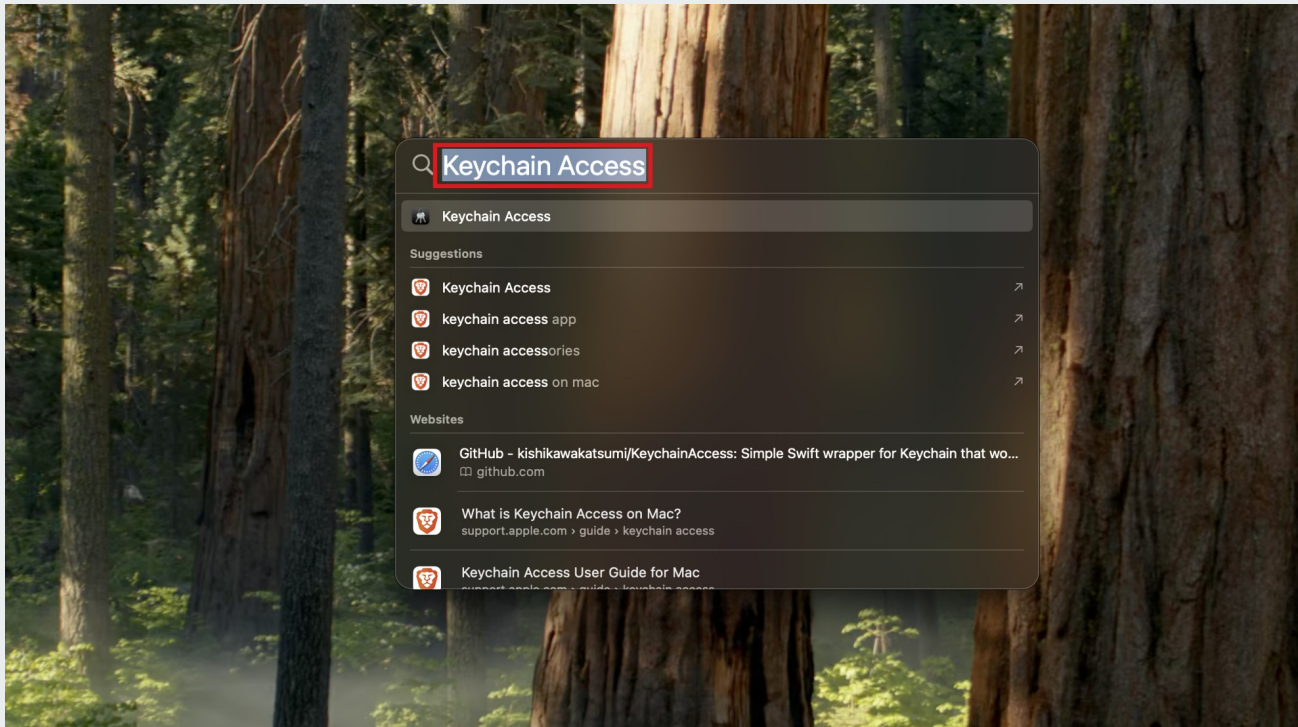
Click **Next** to continue. To confirm the trust settings, **right-click** the SB2 RootCA certificate and select **Get Info**. A successful import and trust is indicated by the message: *“This certificate is marked as trusted for all users.”*



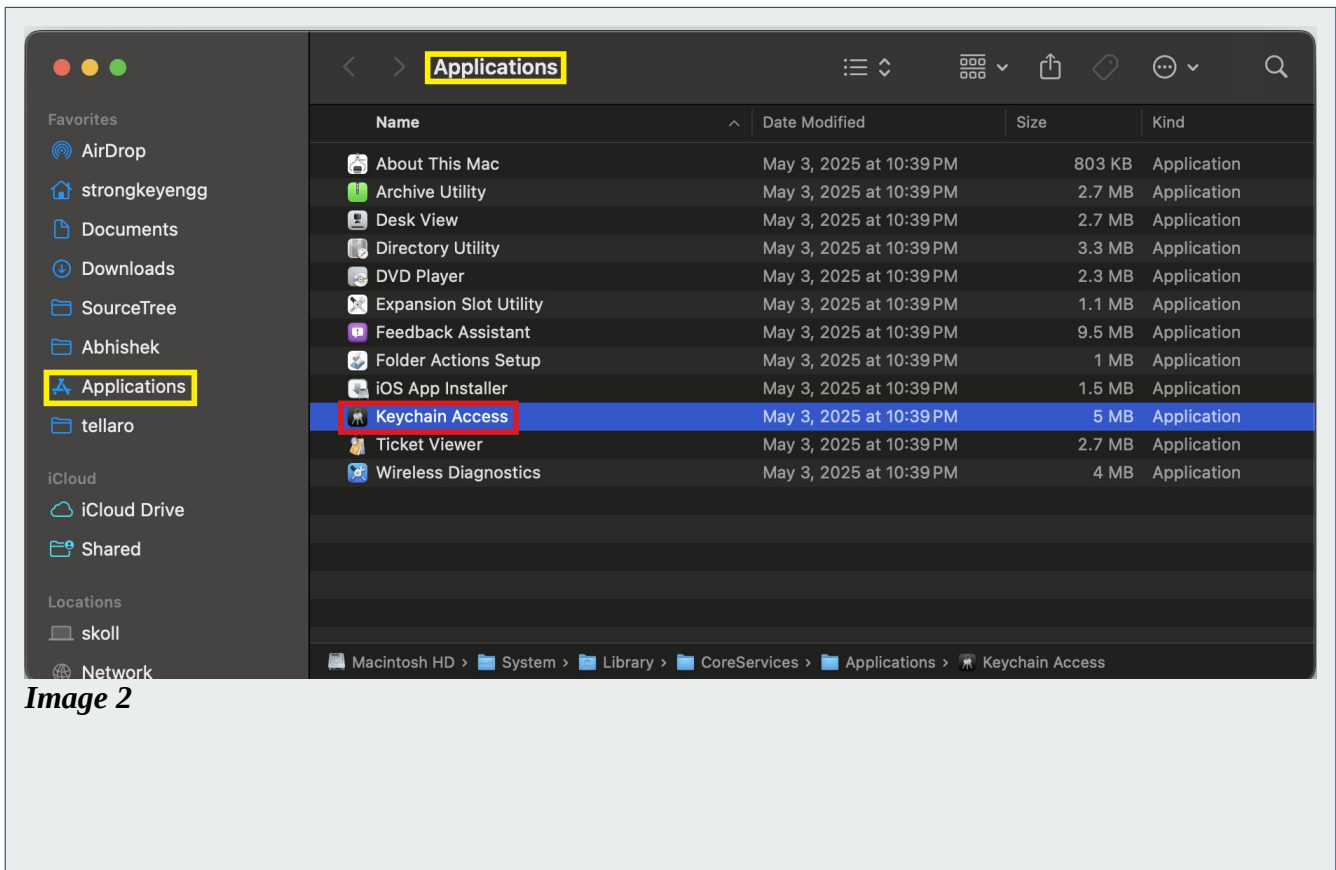
# B14

## 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**

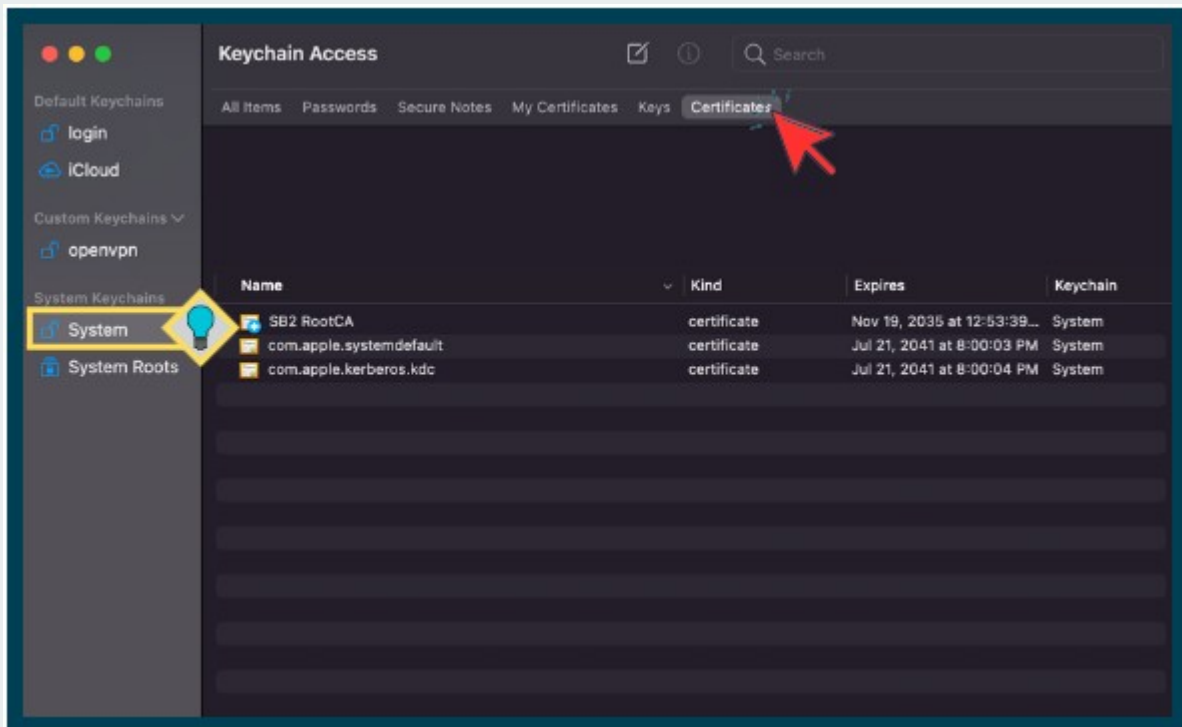


**Image 2**

# B15

## NAVIGATING IN THE KEYCHAIN ACCESS APPLICATION

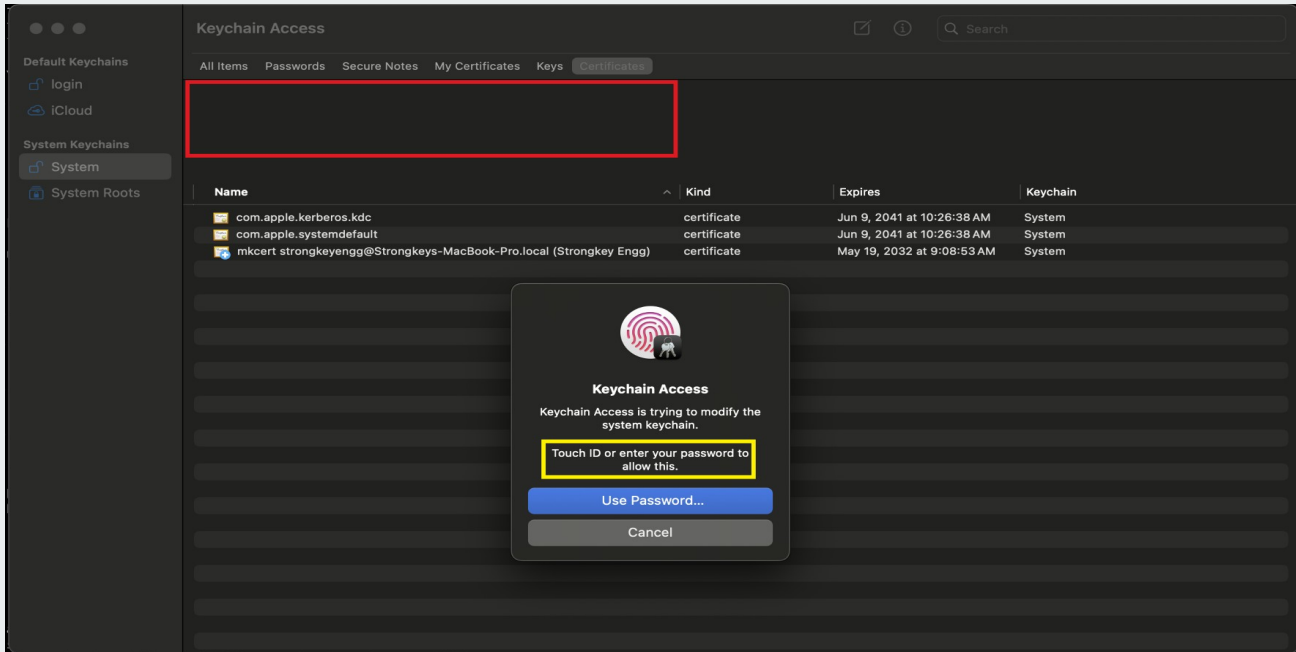
After launching the **KeyChain Access** application, the following screen appears. Select **System** in the sidebar, followed by **Certificates** in the top menu.



# B16

## IMPORTING CERTIFICATES

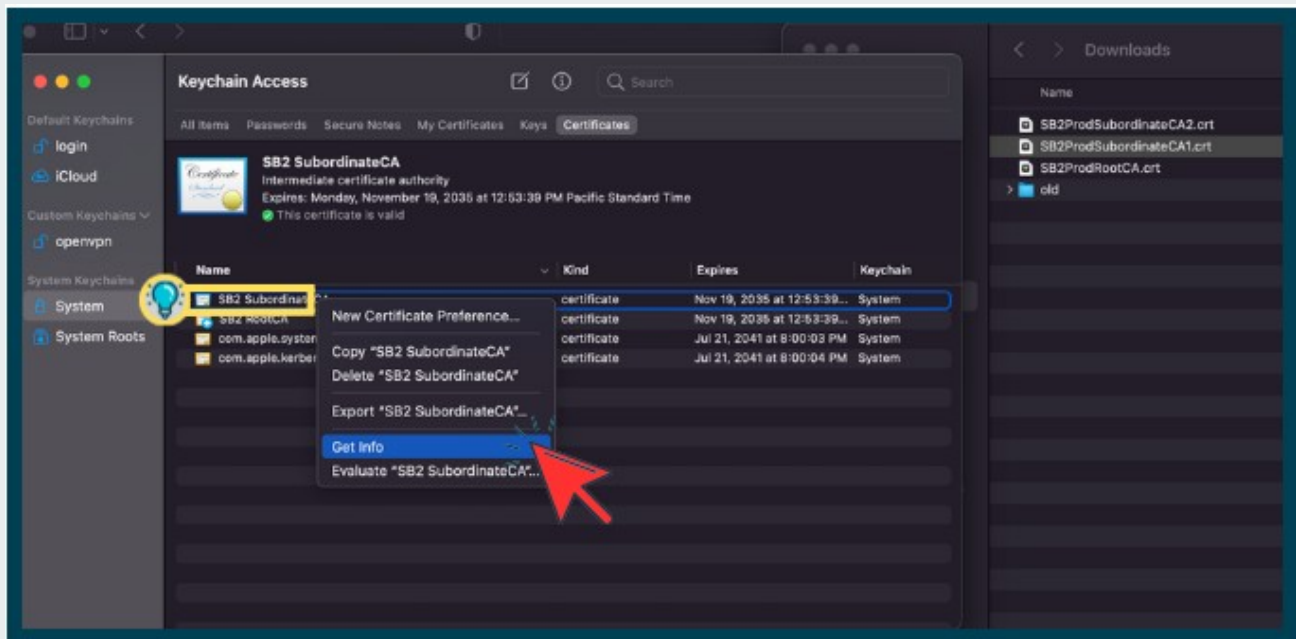
Next, drag the **SB2-SubordinateCA.crt** file into the **Keychain Access** window to begin the certificate import process. The macOS will prompt you to authenticate using Touch ID or an account password to complete the import.



# B17

## ACCESS THE SB2 SUBORDINATE CA CERTIFICATE DETAILS

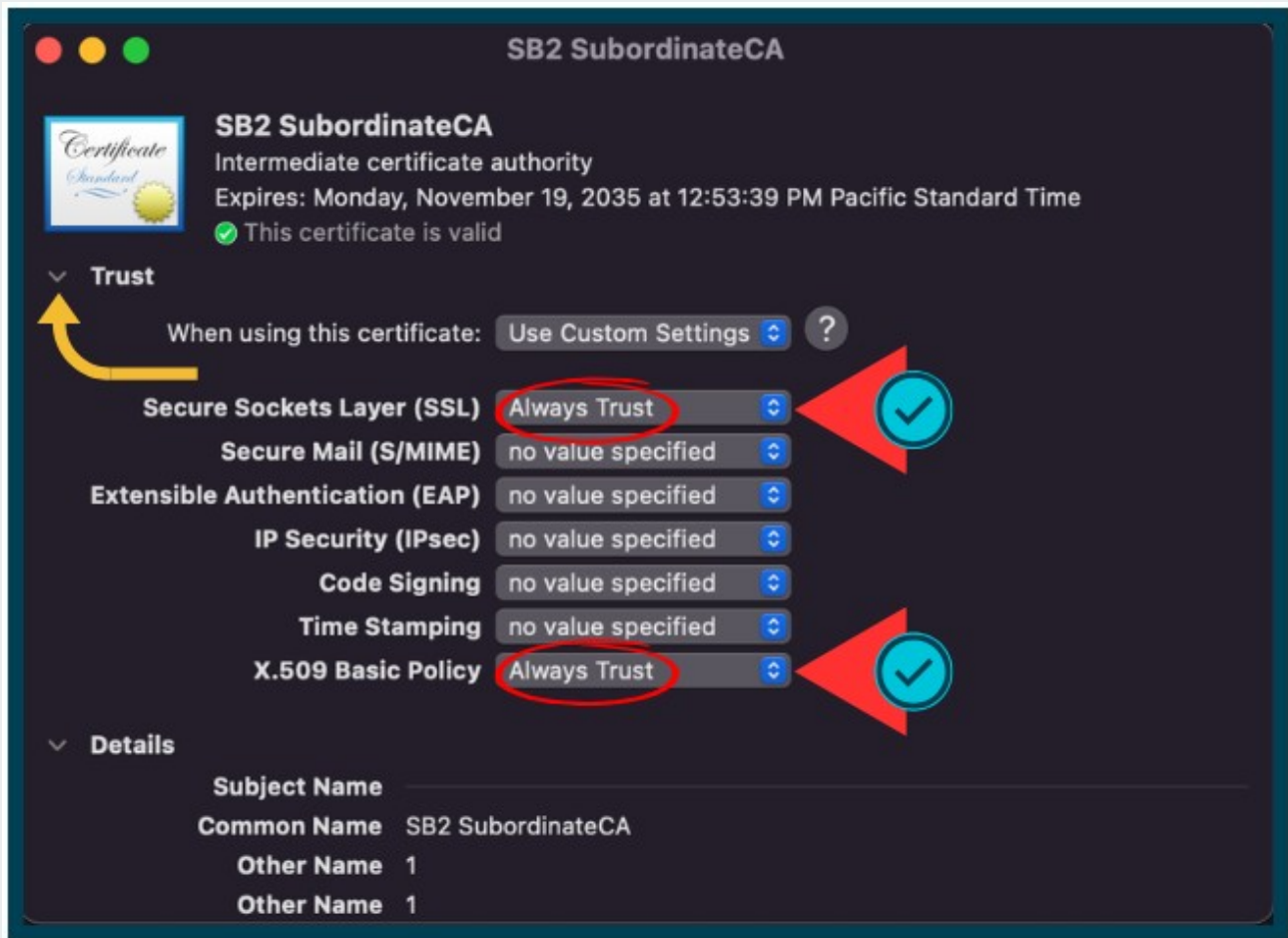
Right-click on the imported SB2 SubordinateCA certificate, then select **Get Info** to view its details.



# B18

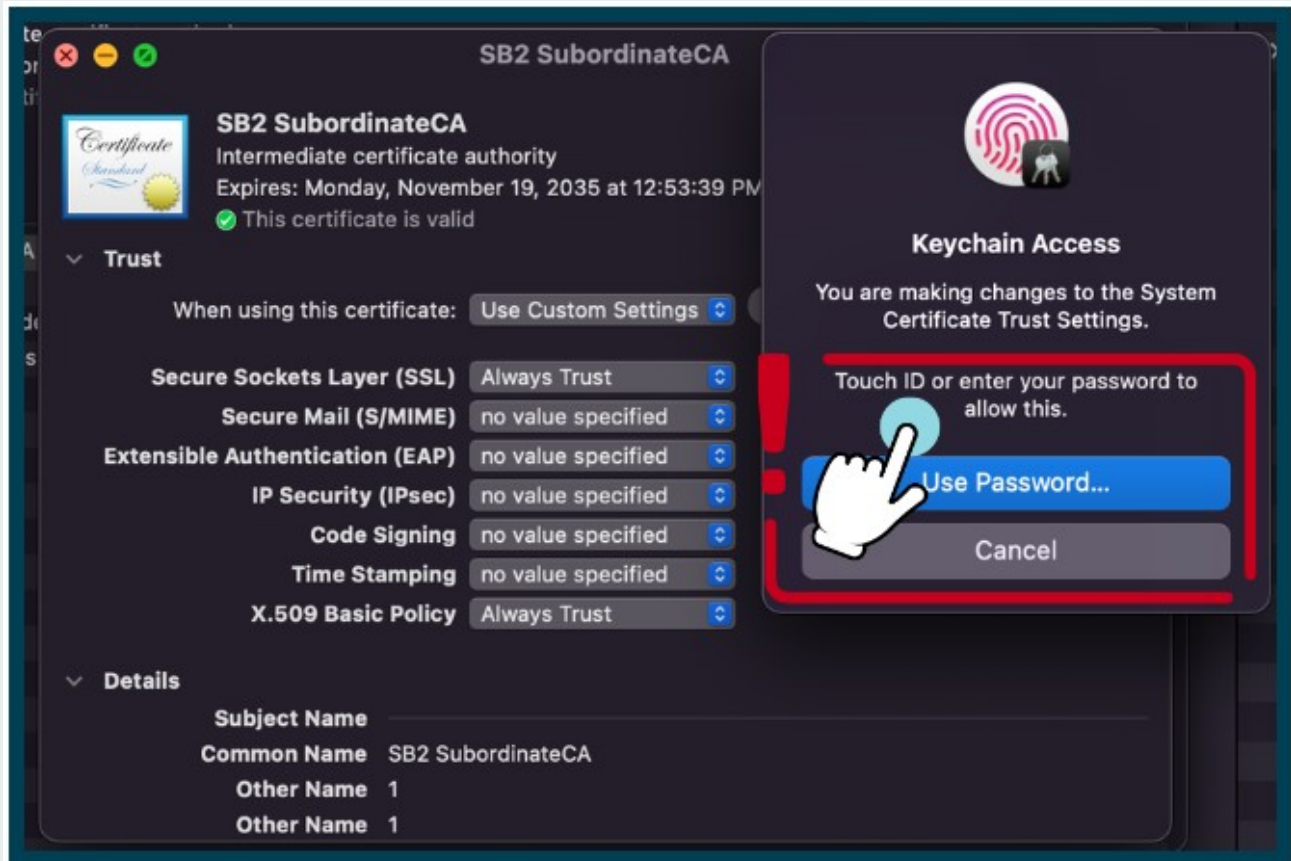
## TRUST THE SB2 SUBORDINATE CA CERTIFICATE

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.

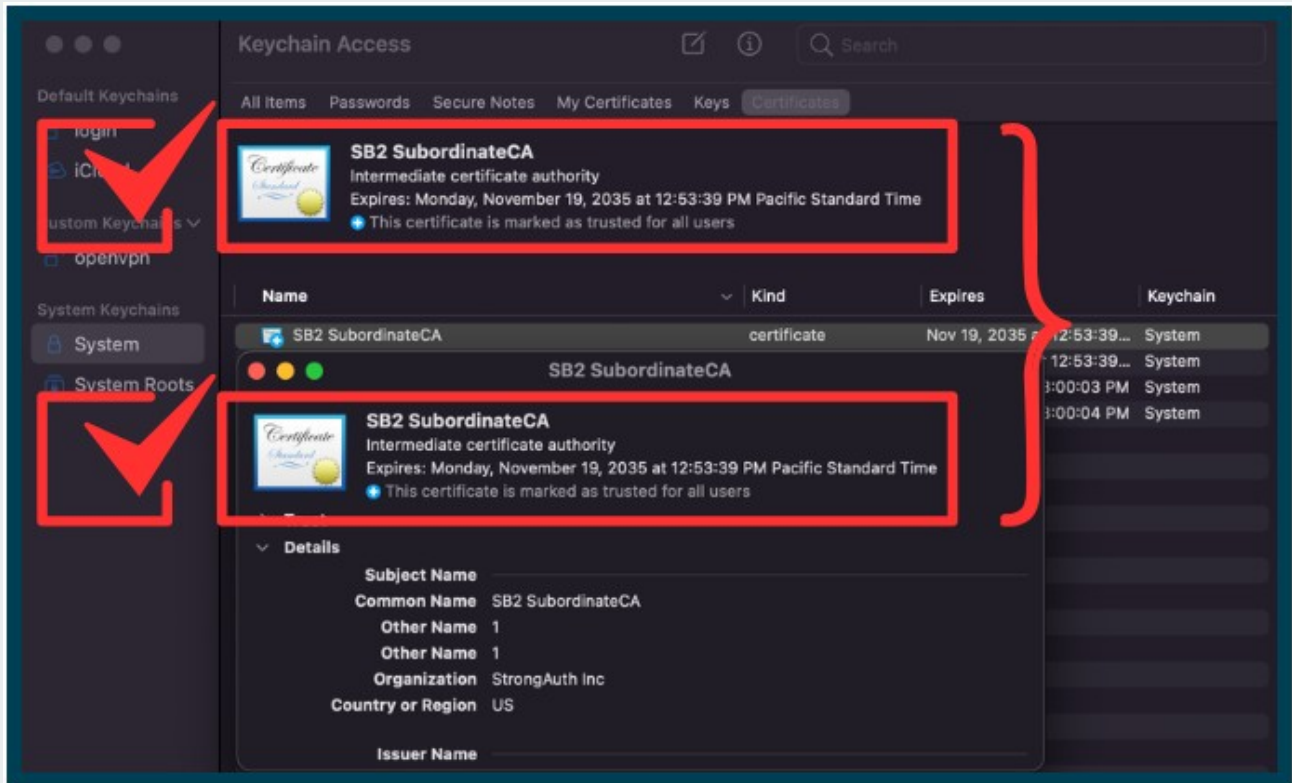


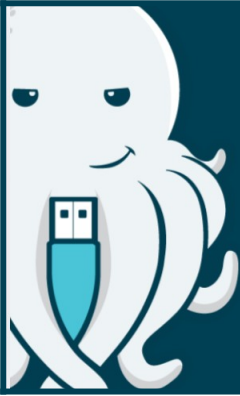
## AUTHENTICATING THE CHANGES TO THE SB2 SUBORDINATE CA

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..



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 iShield2 Security Key with the SB2PROD site.

You must have the 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 ISHIELD2 SECURITY KEY

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



## IDENTIFYING THE USB-C PORT

Locate the USB-C port—typically found along the edge of the computer, it features a compact design with smooth, rounded corners that set it apart from traditional USB-A ports.

The image below shows both a USB-C port and its matching male connector.





## NO USB-C PORT? NO PROBLEM.

With the USB-A to USB-C adapter provided by the Administrator of your SB2 site, simply plug the USB-A end into the computer and insert the Security Key into the USB-C port.

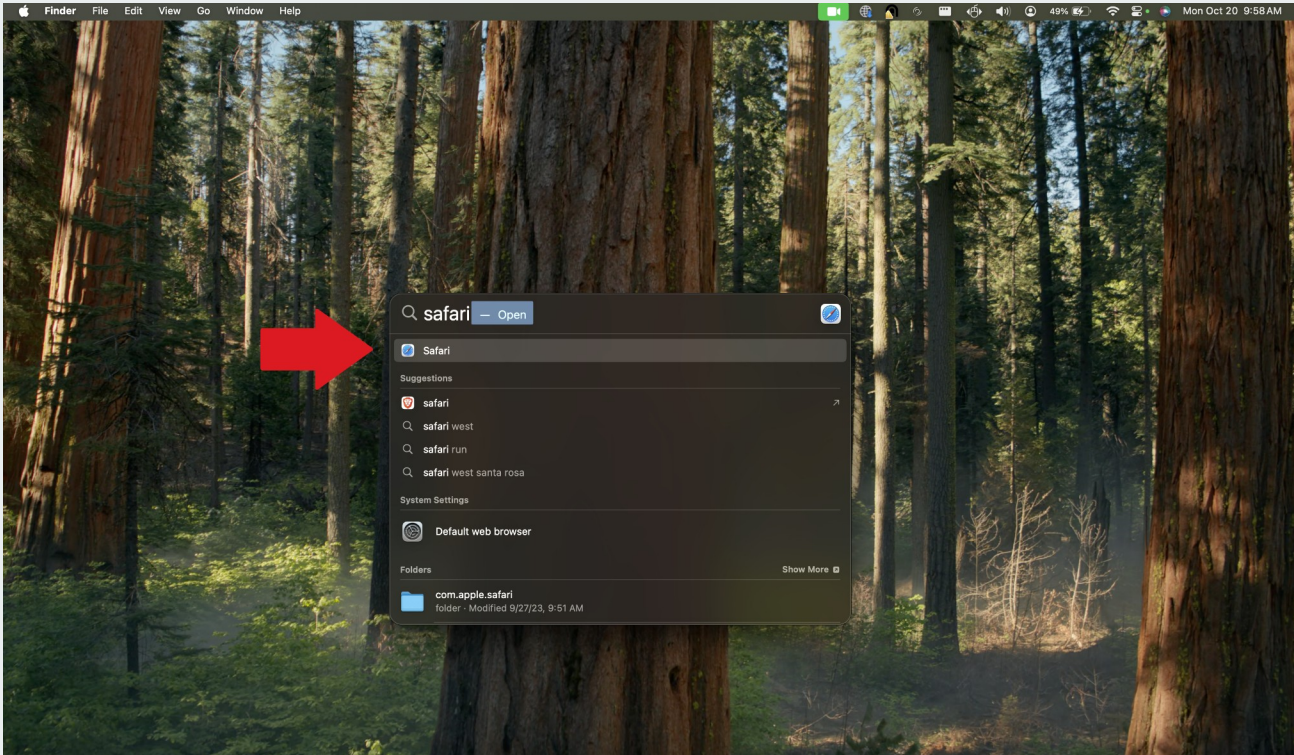
The provided USB adapter pictured below.





# OPEN THE SAFARI BROWSER

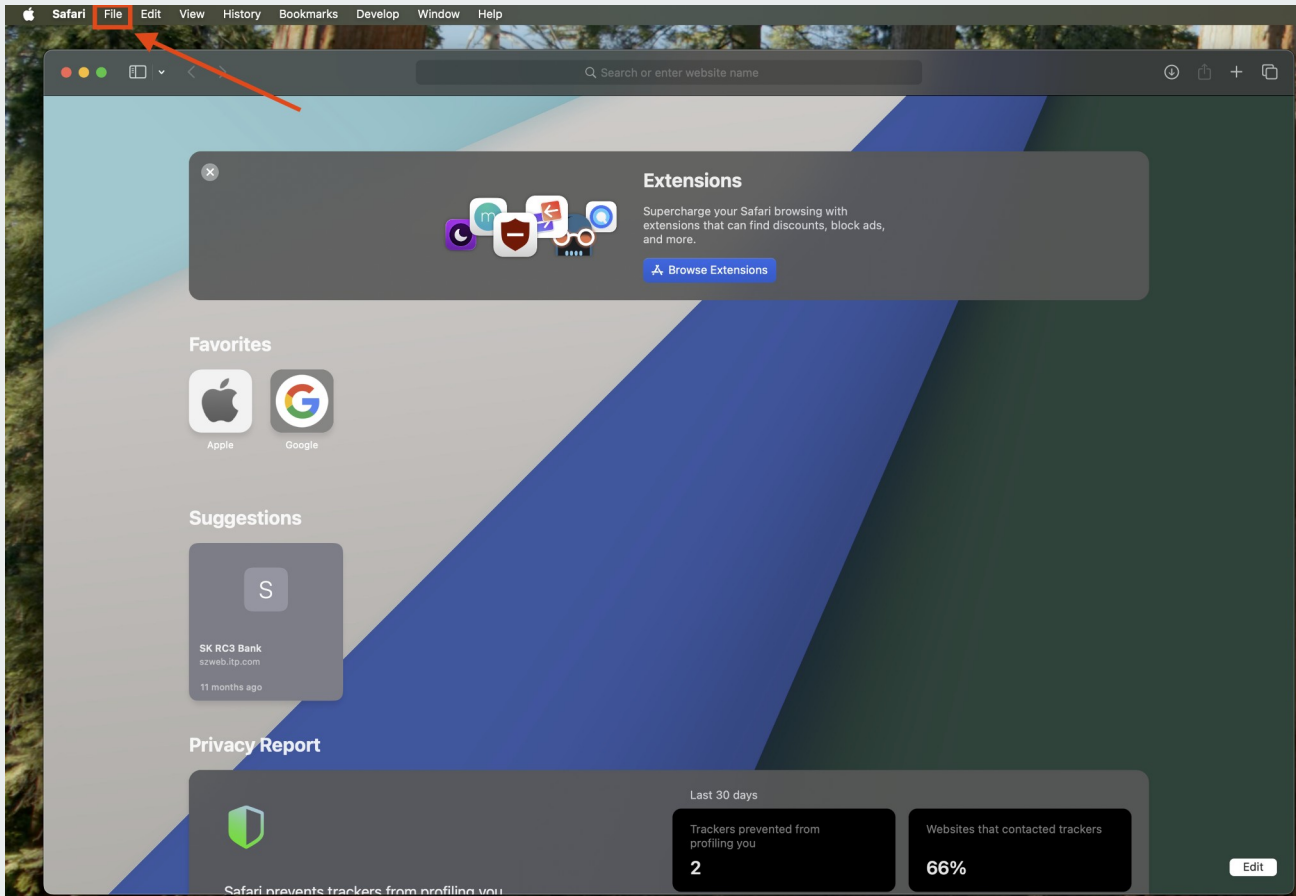
To begin, access the Safari browser by searching with **Spotlight** [⌘ + Space].





# LOCATE THE FILE MENU

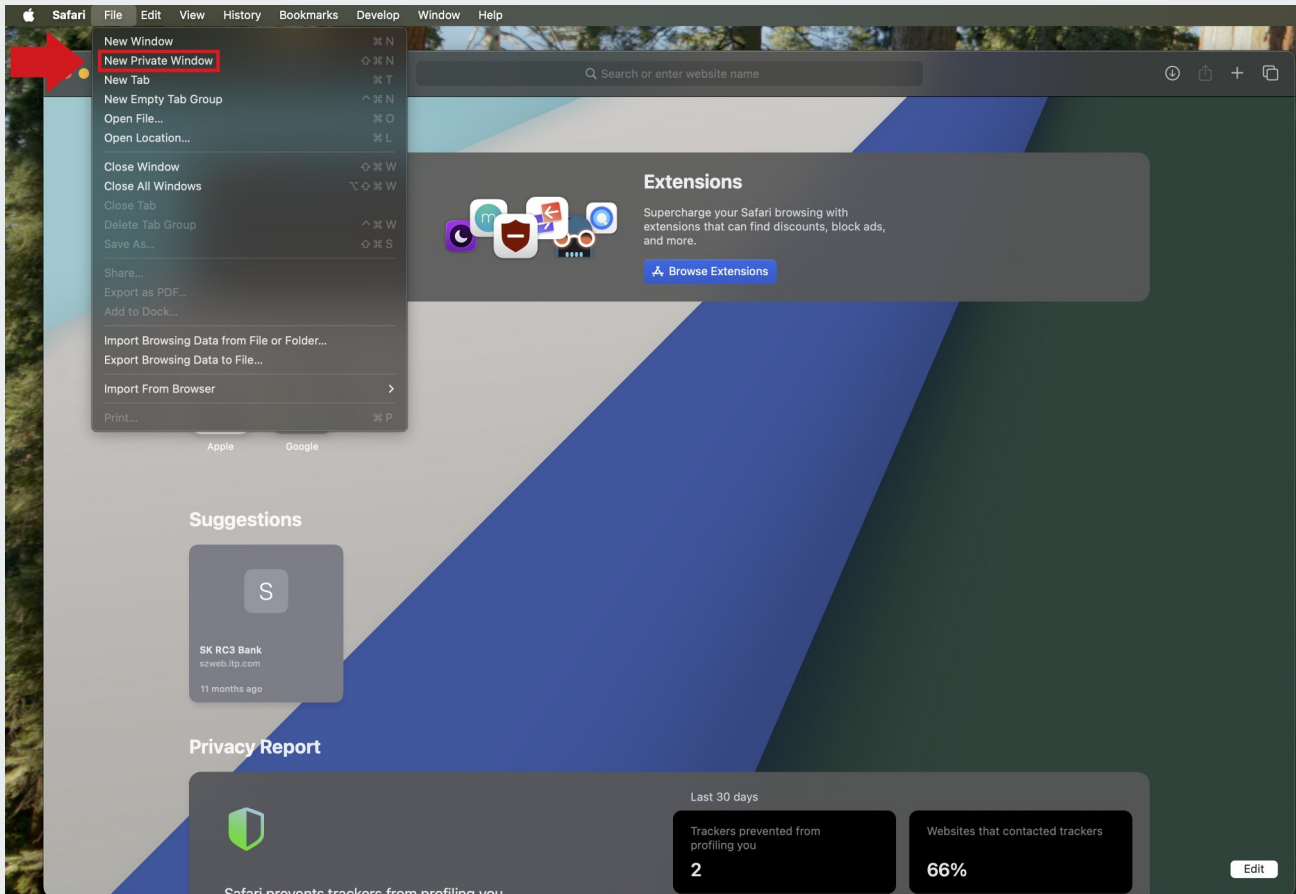
In the top-left corner of the menu bar, click the File menu to proceed.





# OPEN A NEW PRIVATE WINDOW

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





## SB2PROD PLATFORM URL

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

### NOTE



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

[https://sb2.strongkey.com/sb2/register?  
hash=3d500dec79f6ec257ebddcc56hj78ff1f2d31d557d4c7bf5654](https://sb2.strongkey.com/sb2/register?hash=3d500dec79f6ec257ebddcc56hj78ff1f2d31d557d4c7bf5654)



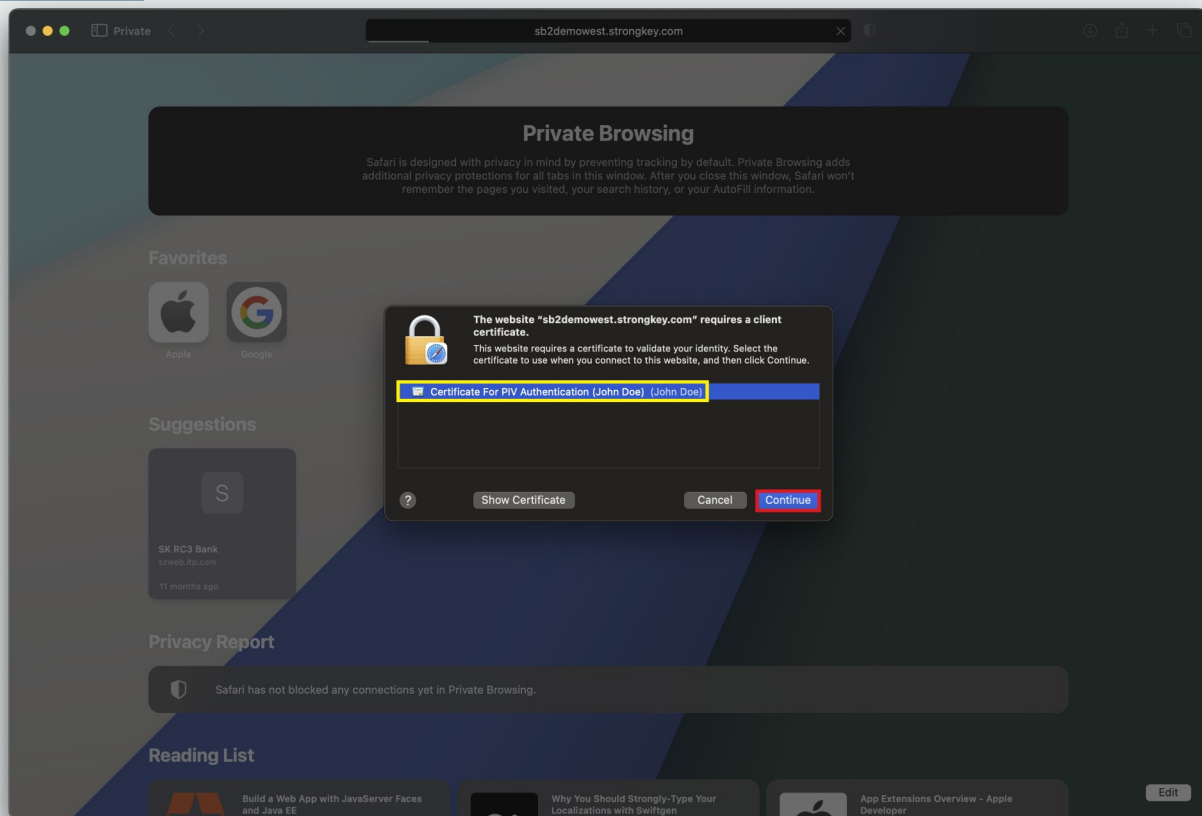
## SELECT THE CERTIFICATE

A pop-up window will display the available certificates (yellow box). The name in the prompt should match your name, as created by the Administrator of the SB2 PROD site. Select the presented certificate and click **Continue** to proceed.

### NOTE



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





## ENTER SECURITY KEY PIN

The next dialog box will prompt for the 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 iShield 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 (Cypher's critical details have been redacted to protect his privacy.).
- Legal disclosures for the SB2 platform are located in the middle section. You must scroll all the way to the bottom and agree to the terms disclosed before you may continue with this process.
- Use the right-hand panel to nickname your Security Key. This makes it easier to identify each key if you use more than one.

**STRONGKEY™ SB2**

**Your Digital Certificate**  
[Learn More](#)  
Username  
cboyer  
Full Name  
Clifton Boyer  
Organization  
StrongAuth Inc  
E-Mail  
clifton.boyer@strongkey.com  
Serial No.  
55:CD:7D:5B:A7:47:4B:D7:91:0C:64:48:1E:74:84:27:1E:0A:00  
Valid Until  
Thu Mar 05 16:52:29 EST 2026 - Wed Mar 05 22:03:33 EST 2031  
Other +

**Disclosures**  
If you agree with the terms presented here, check the box below and register your Security Key. You agree to:  
8. Users who are uncertain about which Personal Data is mandatory are welcome to contact the Owner.  
9. The Owner takes appropriate security measures to prevent unauthorized access, disclosure, modification, or unauthorized destruction of the Data.  
10. The Data concerning the User is collected to allow the Owner to provide its Service, comply with its legal obligations, respond to enforcement requests, protect its rights and interests, detect any malicious or fraudulent activity, as well as the following: User data management, Registration and authentication.  
11. User Data Management: This type of

**Your Security Key**  
You were provided with a Security Key (resembling the following image), containing a digital certificate enabling you to see this site. The Security Key will also be used to register a new FIDO credential to authenticate you.  
  
You may give the Security Key a nickname below – such as “JD’s vault credential” or “John Doe’s access key” – to distinguish it from additional Security Keys you may already own and/or acquire in the future.  
When you select Register below, you will be prompted for a PIN to the Security Key, and to touch the metal surface with a blinking LED on the Security Key.  
Name

# C12

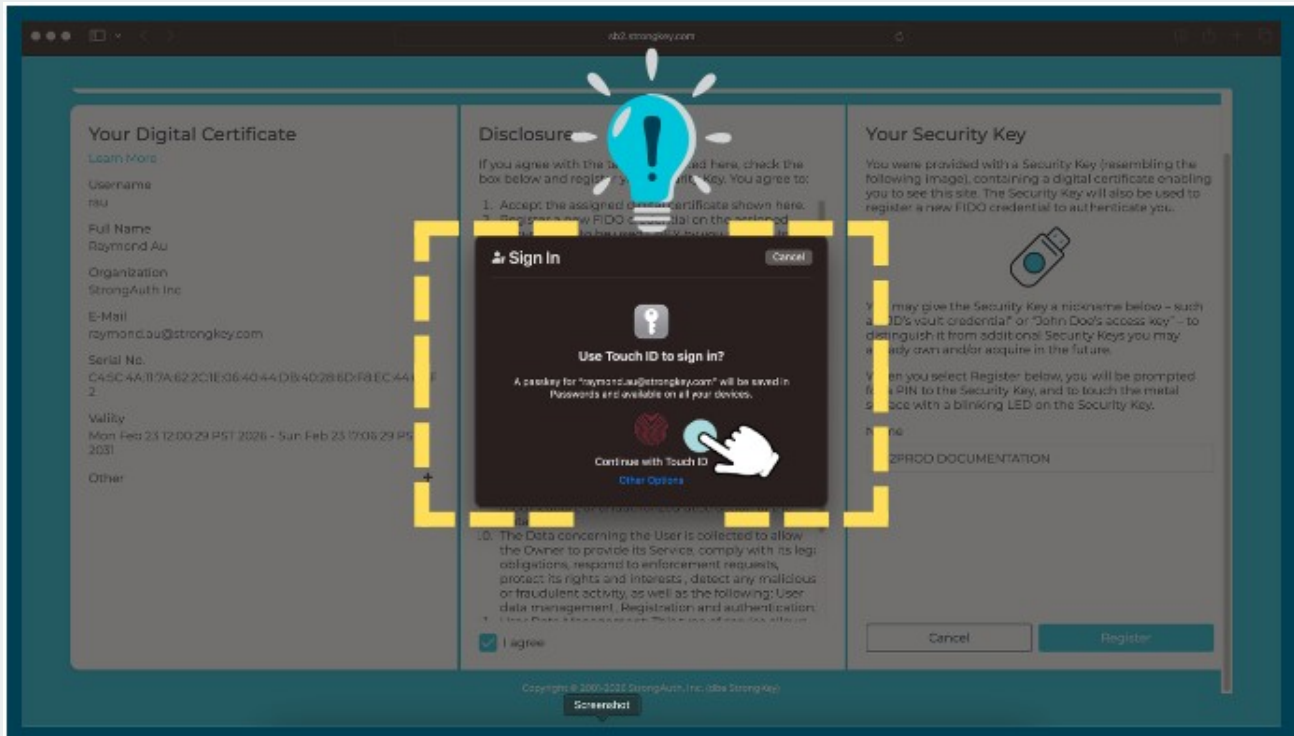
## TERMS & CONDITIONS

Review and accept the terms and conditions in the **Disclosures** panel. The “**I agree**” box must be checked before proceeding with Security Key registration see C13 image).

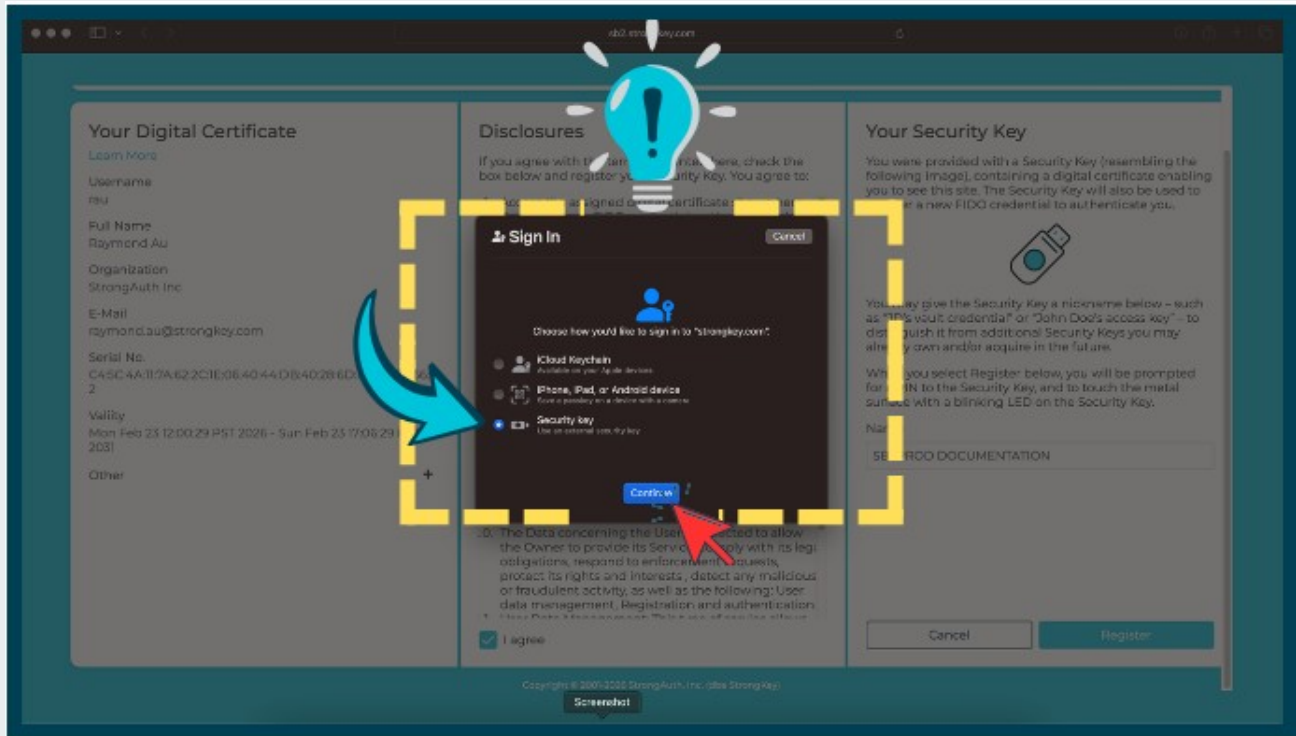


# C14 CONTINUE SETUP

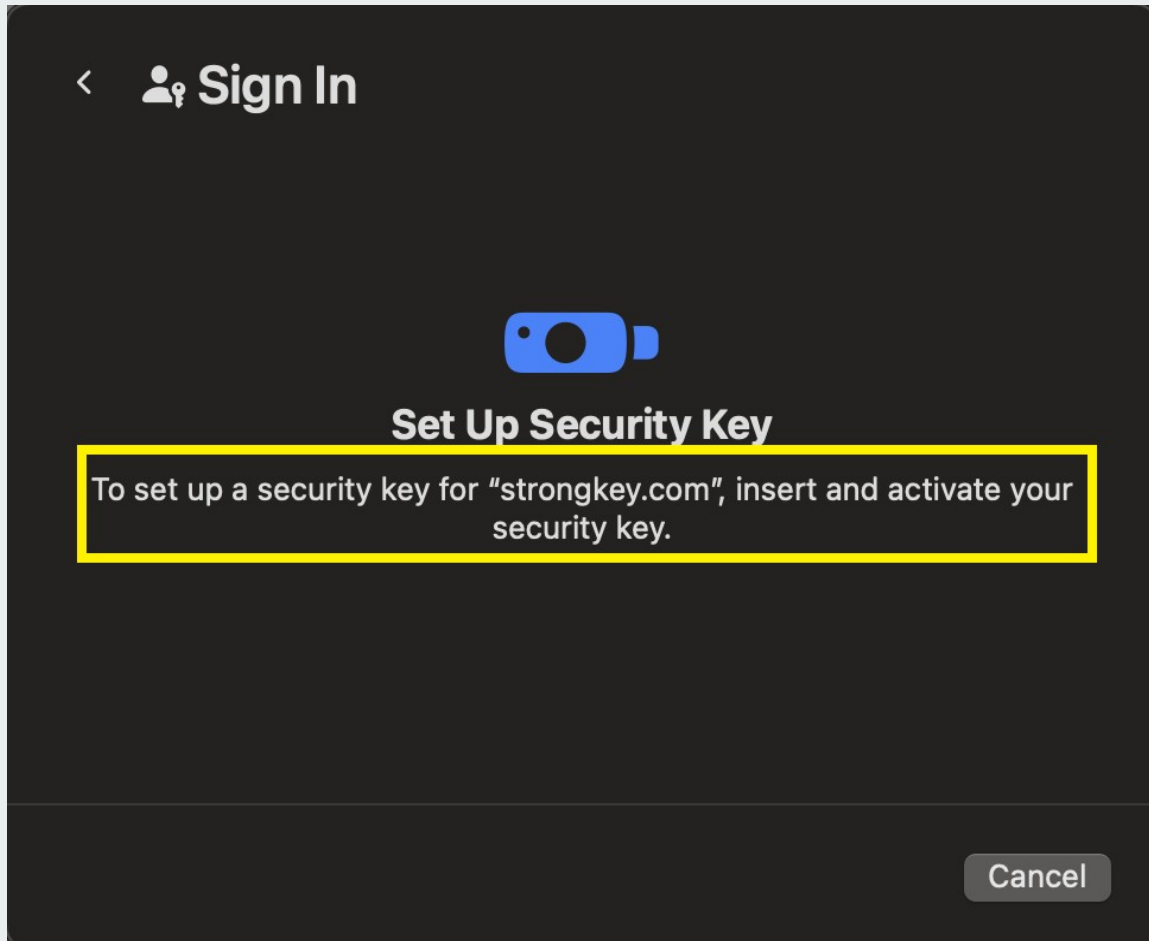
A dialog box will appear to confirm continuation of the setup process, authorizing the current device to also access the SB2PROD website. **Touch your Security Key** to proceed.



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.



Confirm the SB2PROD login by touching the metal contact at the end of the Security Key.



# C17

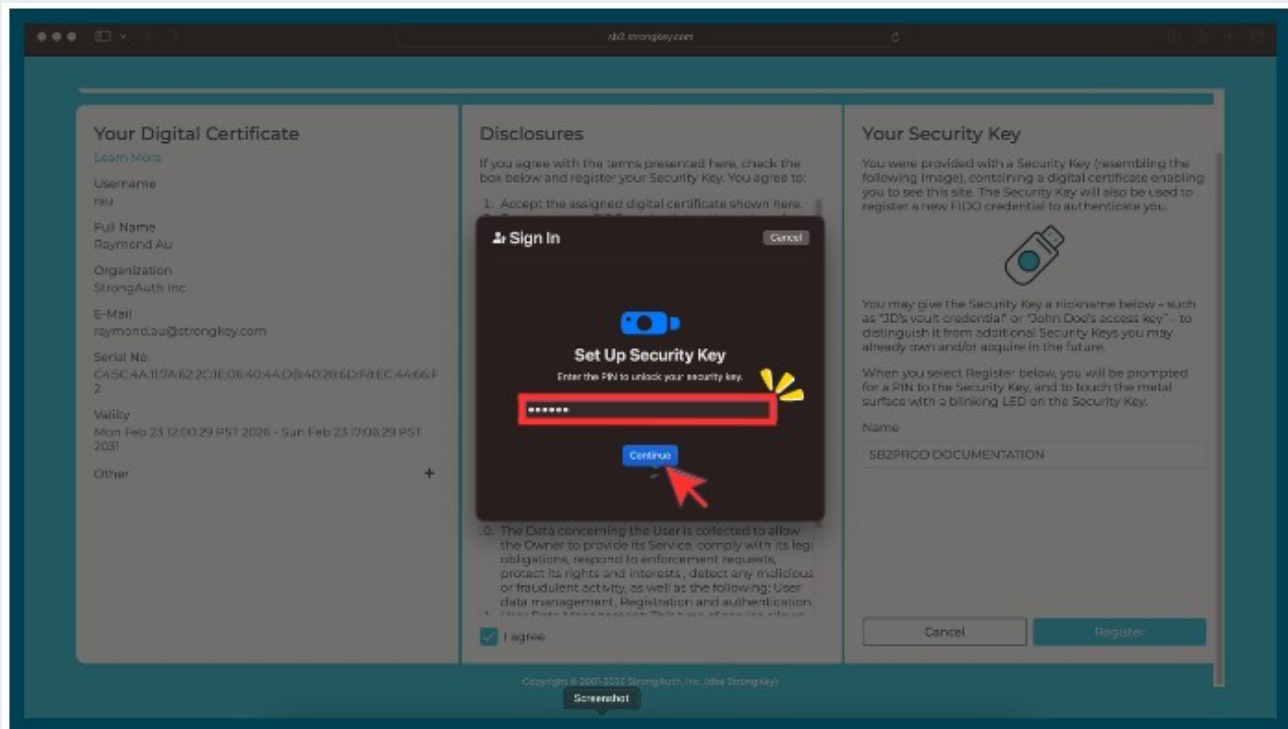
## ENTER SECURITY KEY PIN

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

### 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.



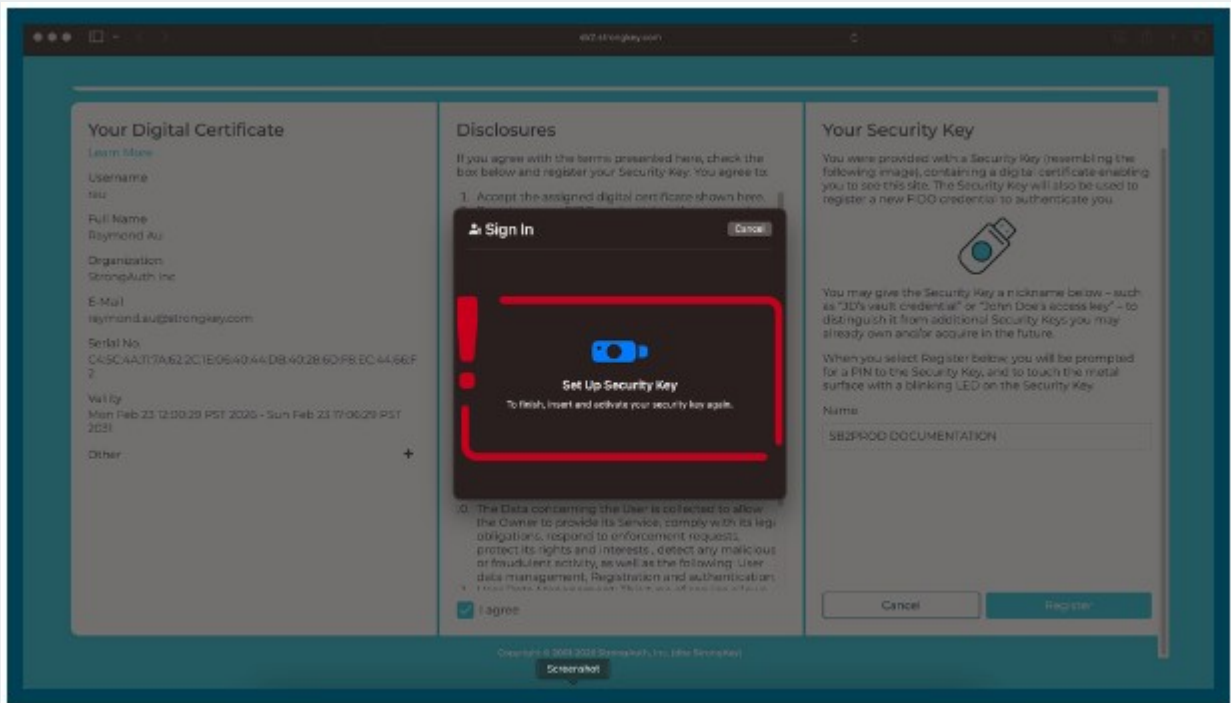
# C18 TOUCH THE SECURITY KEY

To continue the setup, touch the metal contact on the end of the **Security Key** with your finger.

## NOTE



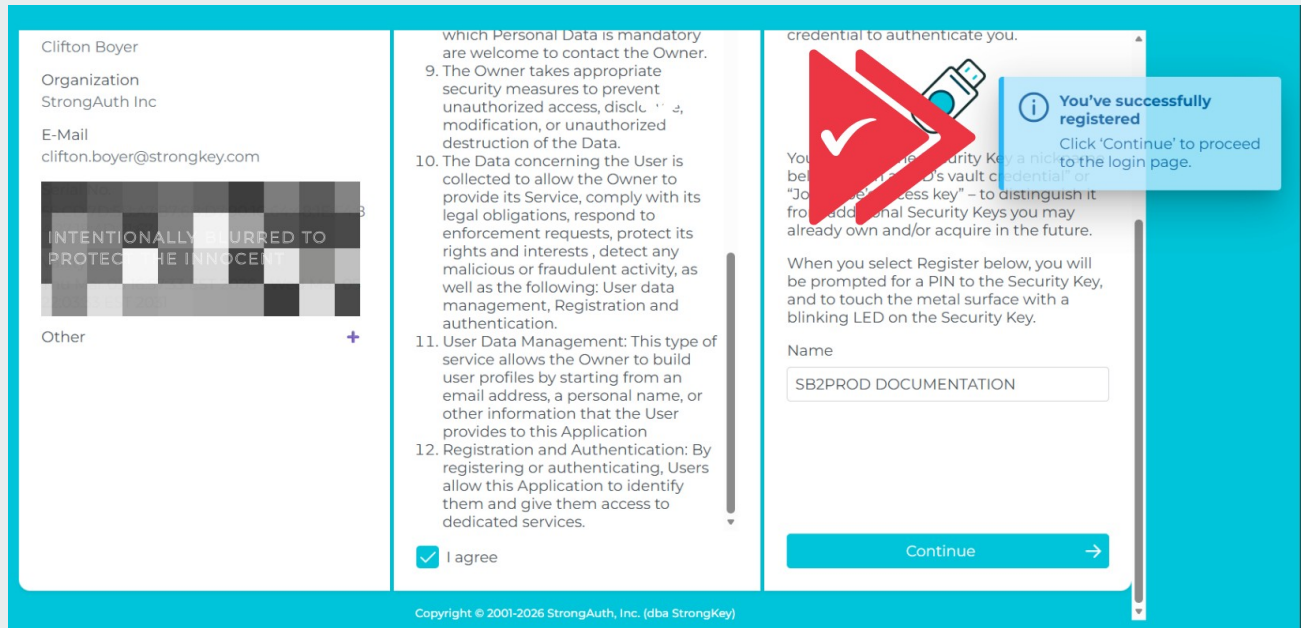
This step is called the “Test of User Presence” (TUP) in the FIDO ecosystem. It ensures that no remote attacker can impersonate you, because they would need both your Security Key and your physical interaction at your computer. Each time you use your FIDO credential to sign in to the SB2 platform, you’ll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





# SB2PROD CONFIRMATION

After touching the security key, SB2PROD will flash a blue message confirming successful registration.






## 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**.

### Sign In



Choose how you'd like to sign in to your "strongkey.com" account.

 iPhone, iPad, or Android device  
Use passkey from a device with a camera

 **Security key**  
Use an external security key

Continue

Cancel

The next dialog box will ask you to activate your Security Key. If not inserted, insert now.

< **Sign In**



**Use Security Key**

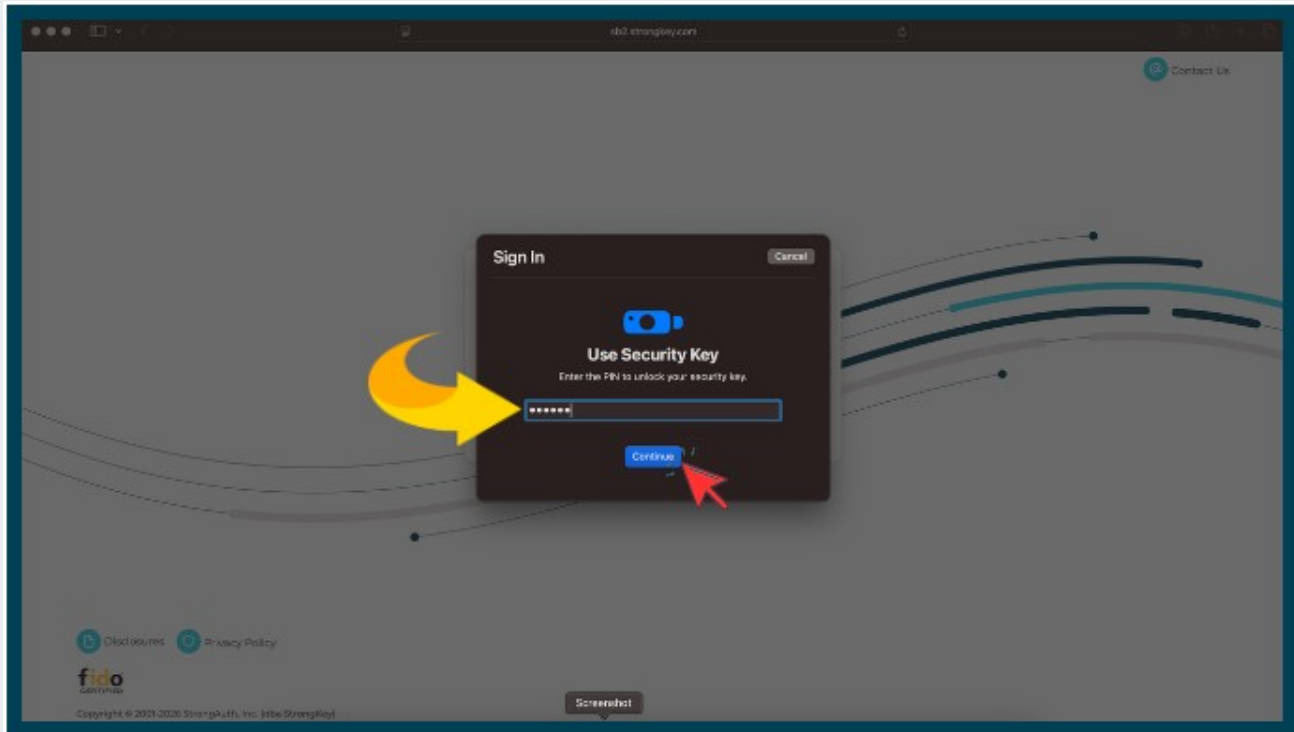
To continue with "strongkey.com", insert and activate your security key.

Cancel



## USER AUTHENTICATION

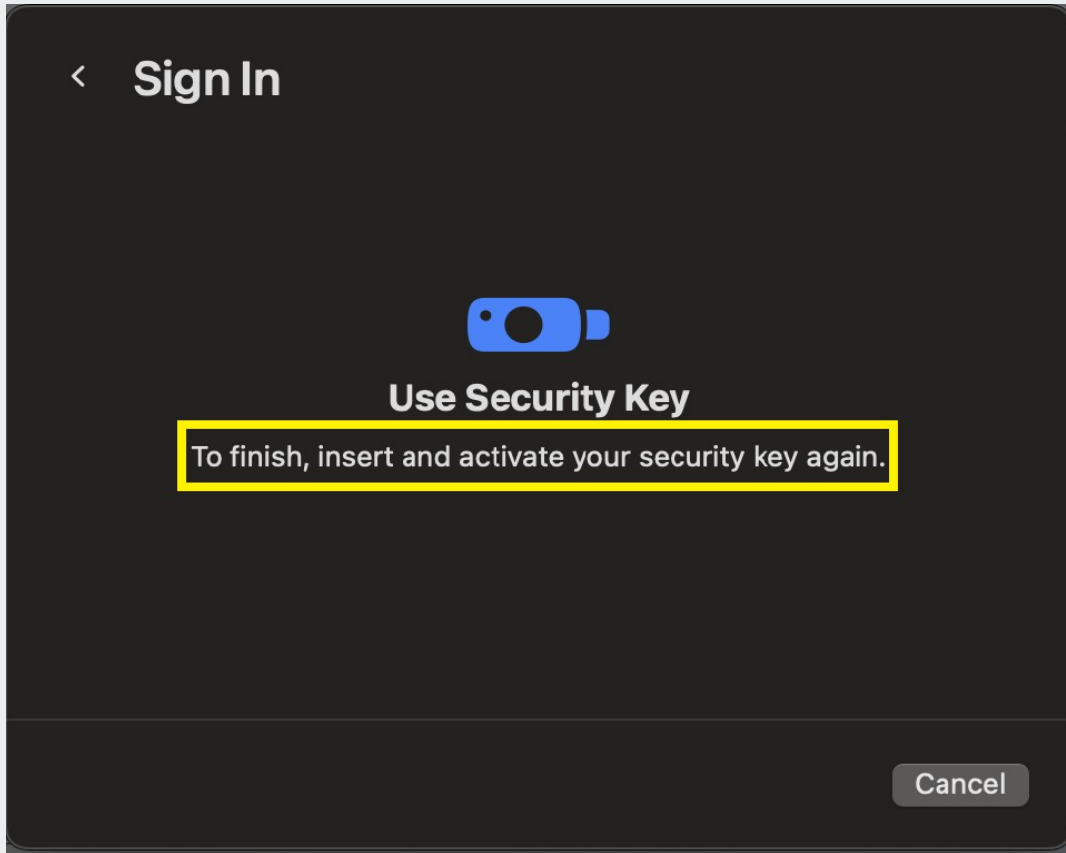
The next dialog box will verify the user. Enter the PIN to the **Security Key** and click **Continue**.





## TEST OF USER PRESENCE (TUP)

To continue the login procedure, touch the metal contact at end 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.





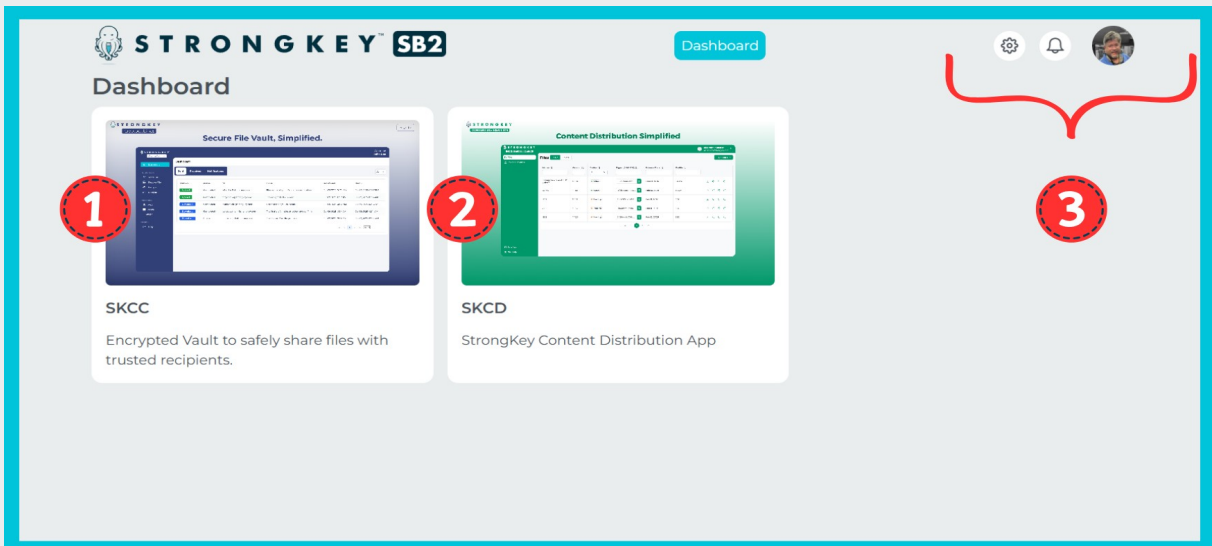
# SB2 PLATFORM DASHBOARD

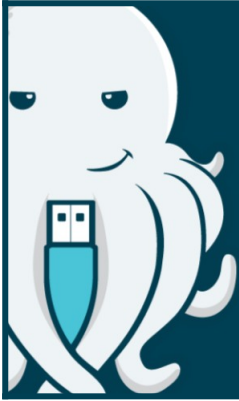
CONGRATULATIONS! Your access to the **SB2PROD Platform** has been successfully established, and your Security Key with your new FIDO credential is registered. Your account name is displayed on the right side of the screen. You may click the gear icon to edit your profile.

All SB2 users have access to two primary applications:

- **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.

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

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



## COPYRIGHT & NOTICES

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

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

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

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



## SWISSBIT iSHIELD KEY 2 PRO: CHANGING THE PERSONAL IDENTIFICATION VERIFICATION (PIV) PIN

This appendix guides you through changing your PINs on the Swissbit iShield Key 2 Pro ("iShield2") Security Key.

### API

## CHANGING A SWISSBIT iSHIELD KEY 2 PRO PIV 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.

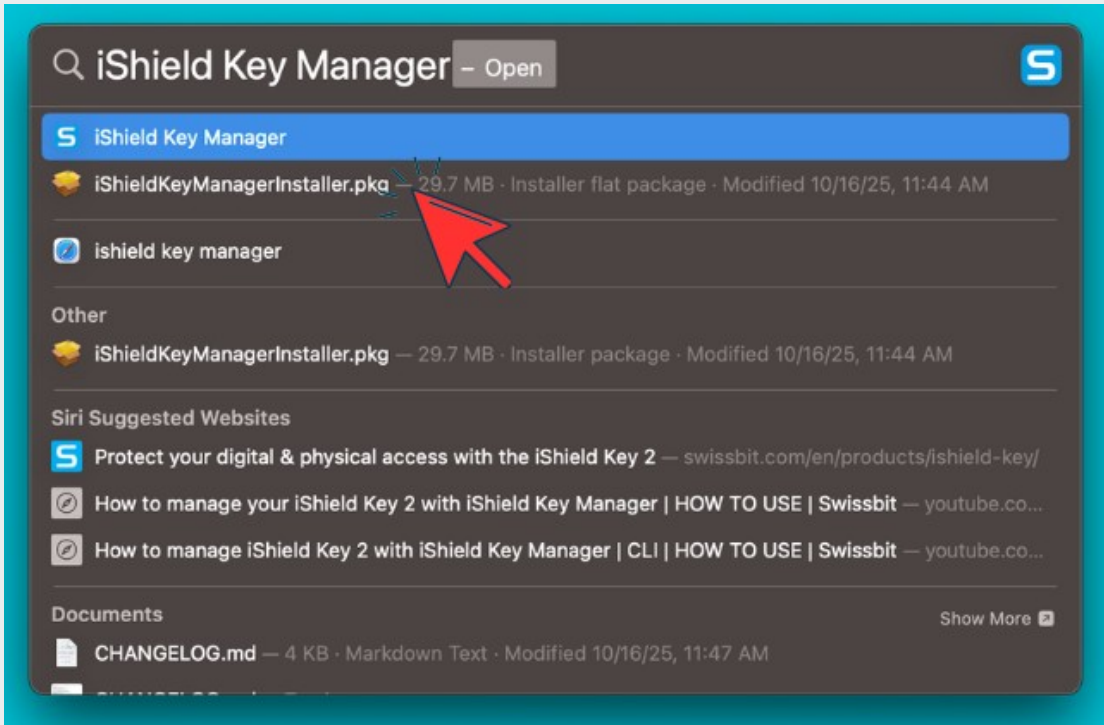
However, StrongKey recommends using the SAME PIN to both containers of the **Security Key** to reduce the burden on users. As long as the **Security Key** is safely in the possession of the legitimate user, and the legitimate user is NOT sharing the PIN to the **Security Key** with anyone, the user will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

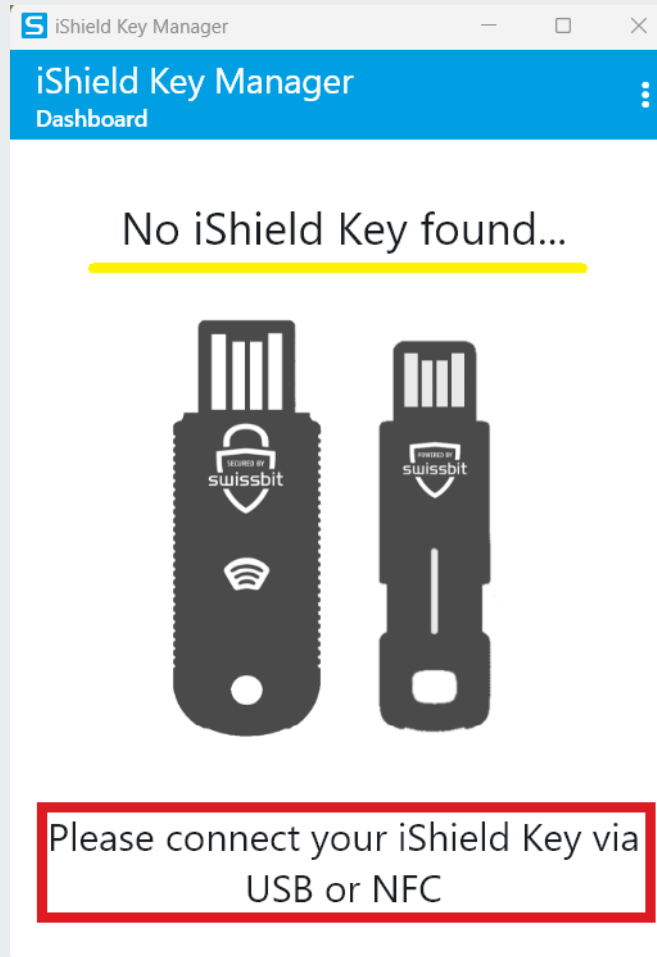
To begin, open the **iShield Key Manager** application by searching for it with **Spotlight** (⌘ + Space) or locating it in **Finder's Applications** folder. **Double-click** to open.



## AP3

# SELECT iSHIELD KEY MANAGER

Upon opening, the application displays the screen shown below and indicates “No iShield Key found”



## 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.



## NO USB-C PORT? NO PROBLEM.

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

The provided USB adapter pictured below.



# CHANGING THE 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**.

The screenshot displays the iShield Key Manager application window. The title bar reads "iShield Key Manager" and the main header is "iShield Key Manager Dashboard".

The interface is divided into several sections:

- Top Left Card:** Features an image of a USB key. Below it, the "Serial Number" is listed as 602782540039 and the "Firmware" as v1.1.2.
- Top Right Card:** Provides instructions: "Alternatively use the Windows settings to manage your FIDO2 PIN: Settings > Account > Sign-in options > Security Key > Manage". It includes a "PIN" field with a "Set PIN" button and a "Factory Reset" field with a "Reset" button.
- Bottom Left Card (Passcode):** Titled "123 Passcode" with the subtitle "HOTPs, TOTP's and Passwords". It has a "Please select a slot" dropdown menu, a "Code" field with a masked input (dots) and icons for visibility, copy, and edit, and a "Version" field showing v3.6.0. A "Details & Settings >" button is at the bottom.
- Bottom Right Card (PIV):** Titled "PIV" with the subtitle "Personal Identity Verification". It shows "X.509 Certificates" with "Installed: 1 / 25" and a "Browse >" button. Below this, the "Version" is listed as "OpenFIPS201 v1.4". A large red arrow points from the "Browse >" button area down to the "Details & Settings >" button at the bottom of the card.

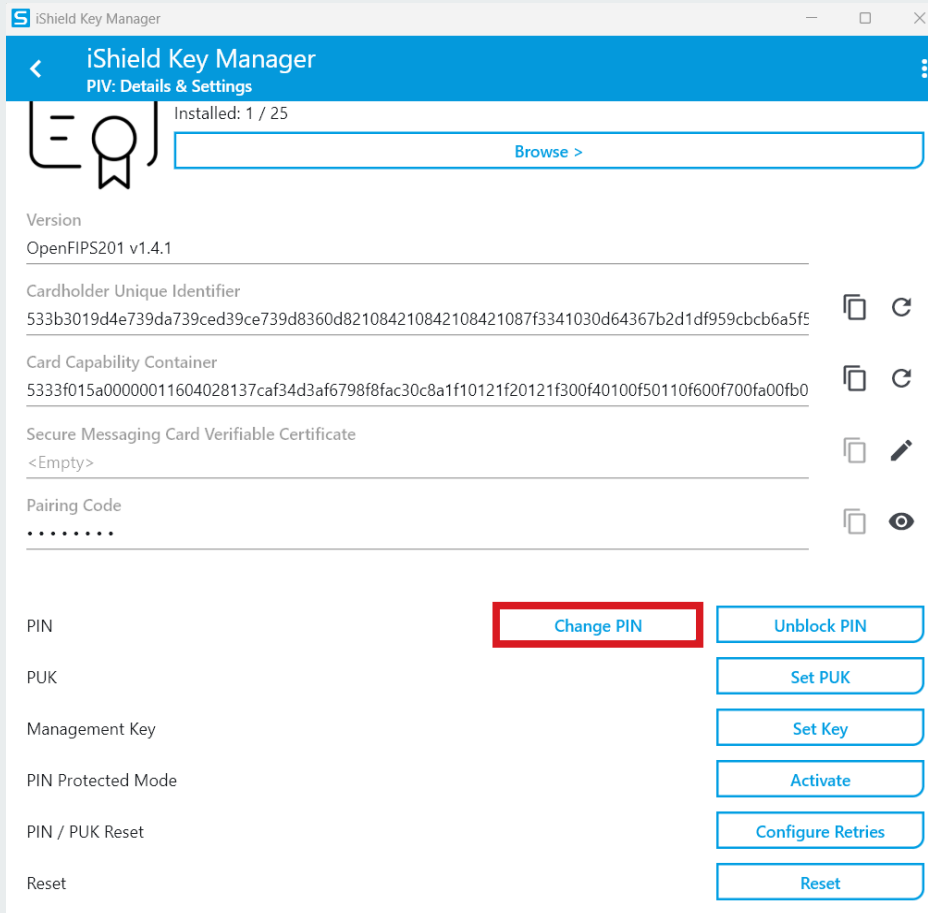
Select the **Change PIN** option.

## 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

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

Change PIV PIN

1 Current PIN

2 New PIN

3 Repeat new PIN

Cancel

Change PIN

## AP10

# SUCCESS!

If the PIN was changed successfully, 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 [AP8 – AP10](#). Start by clicking the **Details & Settings** option.

### NOTE



**StrongKey recommends using the same PIN for the FIDO credential.**


The screenshot shows the iShield Key Manager Dashboard with four main sections:

- iShield Key 2 Pro MIFARE Overview:** Displays a photo of the key and lists the Serial Number (602782540039) and Firmware (v1.1.2).
- FIDO2 Passkeys:** Shows 2/300 passkeys and a **Browse >** button. Below this, it lists the AAGuid (7787a48213e847848a06c7ed49a7aaf4) and Version (1.4.0). A red box highlights the **Details & Settings >** button at the bottom of this section.
- Passcode HOTPs, TOTP and Passwords:** Includes a dropdown menu for "Please select a slot", a code input field with a "Code" label, and a "Version" label.
- PIV Personal Identity Verification X.509 Certificates:** Shows 1/25 certificates installed and a **Browse >** button. It also includes a "Version" label.

# AP12 CHANGE PIN

Click Change PIN.

iShield Key Manager  
FIDO2: Details & Settings

 Passkeys  
2/300  
[Browse >](#)

AAGuid  
7787a48213e847848a06c7ed49a7aaf4

Version  
1.4.0

Supported protocols  
U2F, FIDO 2.0, FIDO 2.1

PIN [Change PIN](#)

Reset [Reset](#)

## AP13 ENTER NEW PIN

1. Enter the default PIN (112233).
2. Enter the new PIN. The PIN must contain 6 to 8 characters.
3. 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).

### Change FIDO2 PIN

1 Current PIN

Force PIN Change

2 New PIN

3 Repeat new PIN

## AP14 SUCCESS!

The display will return to the dashboard, and a notification stating "PIN Reset" will briefly appear on the screen.

