



STRONGKEY™

TELLARO SB2

SWISSBIT iSHIELD KEY 2 PRO USER'S GUIDE FOR WINDOWS 11

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



COPYRIGHTS AND 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

- Windows 11
- Edge version Browser, 145.0.3800.97
- Swissbit iShield Key 2 Pro
- Internet Connection
- USB-C port or USB-C-to-USB-A adapter

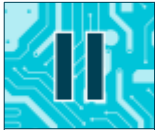


TABLE OF CONTENTS

A	<u>Installing the Swissbit iShield Key Manager</u>	4
B	<u>Installing the Swissbit Minidriver for Windows 11</u>	16
C	<u>Importing SB2 Root CA & SB2 Subordinate CA Certificates into Microsoft Trustore</u>	24
D	<u>Accessing an SB2PROD Invitation Link</u>	55
AP	<u>Appendix: Changing a Swissbit iShield Key 2 Pro Personal Identification Verification (PIV) PIN</u>	73

SECTION A



STRONGKEY

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 (WINDOWS)

To download the iShield Key Management Kit for Windows 11, 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 (Windows)

1

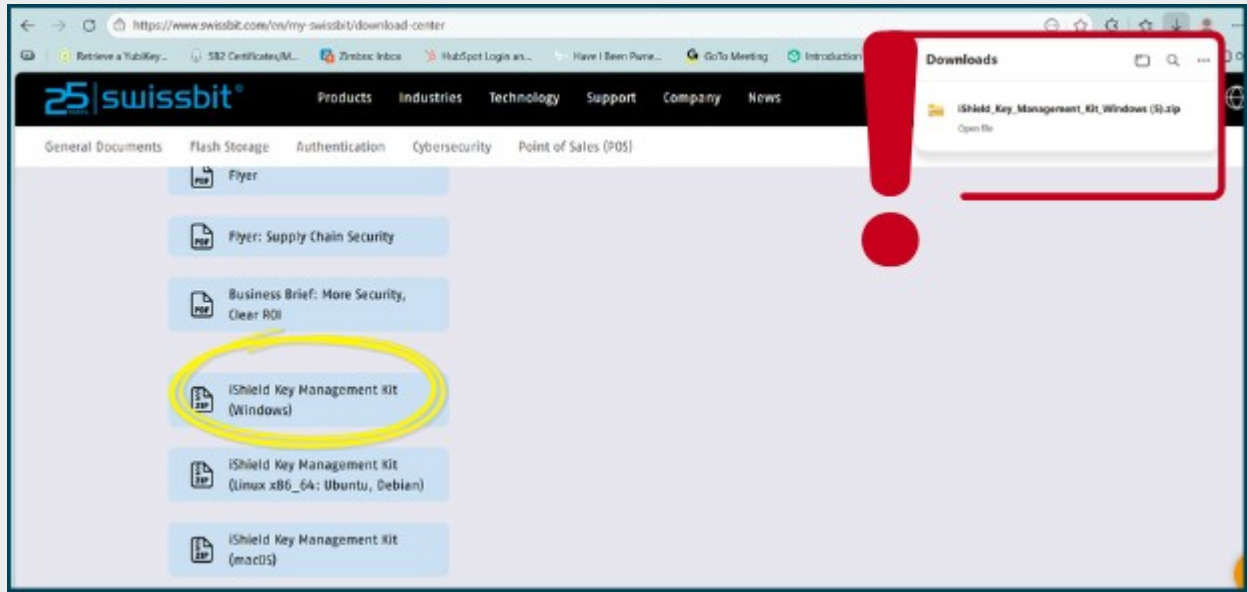
2

3



OPENING THE iSHIELD KEY MANAGEMENT KIT (WINDOWS) FILE

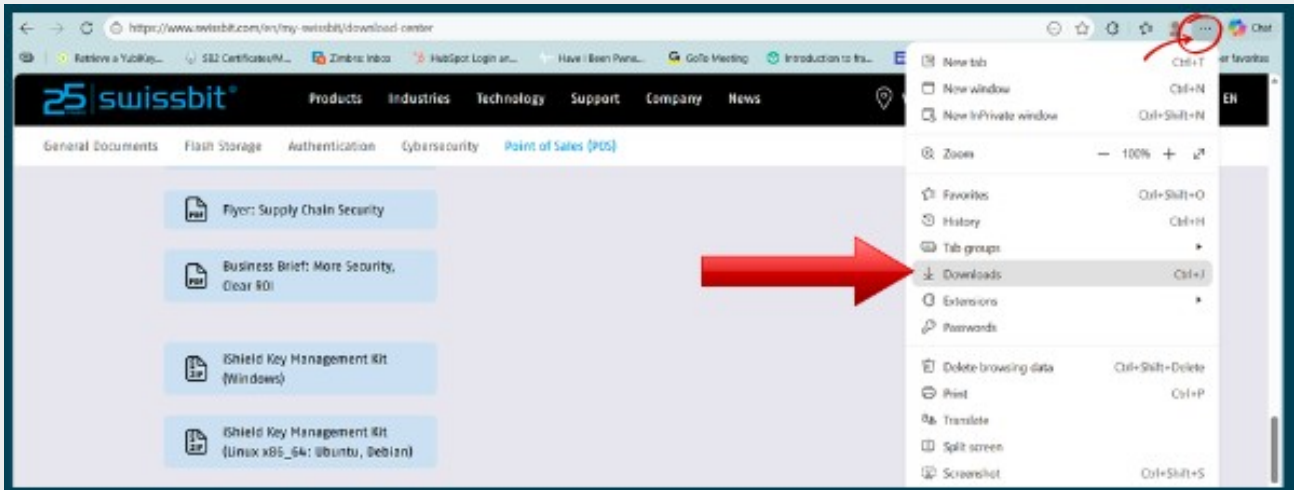
After clicking the download link, MS Edge will display a pop-up confirming the iShield Key Management Kit file has been successfully downloaded and ready for access. **Click the open file link.**





NO POP-UP WINDOW? NO PROBLEM.

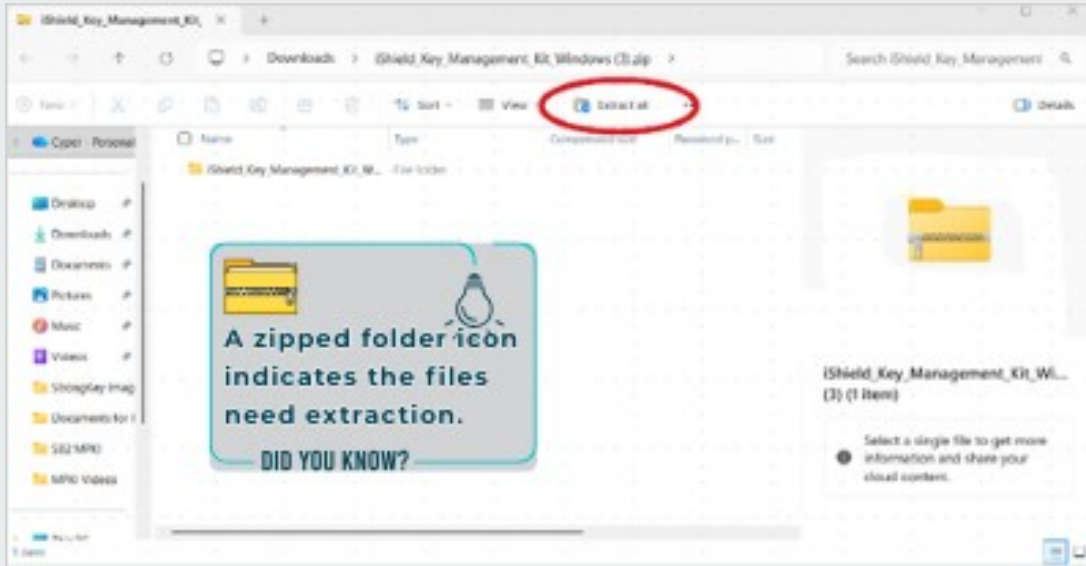
If the pop-up does not appear, or is inadvertently closed, access the downloaded file by clicking the **3-dot** menu on the right side of the MS Edge tool bar. Next, click on **Downloads** in the drop-down menu.





CLICK EXTRACT ALL

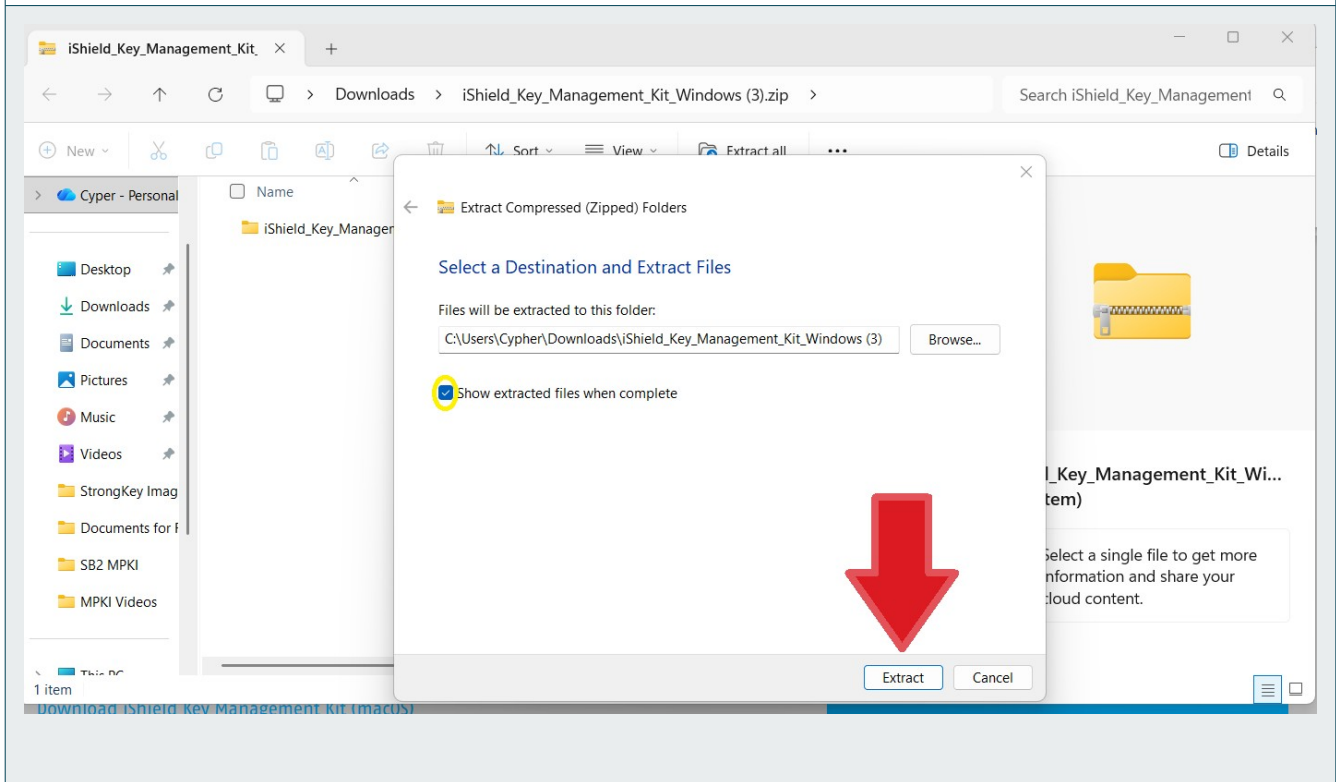
After selecting Downloads, extract the Swissbit files from the ZIP folder. **Click Extract all.**



A6

SELECT DESTINATION FOLDER

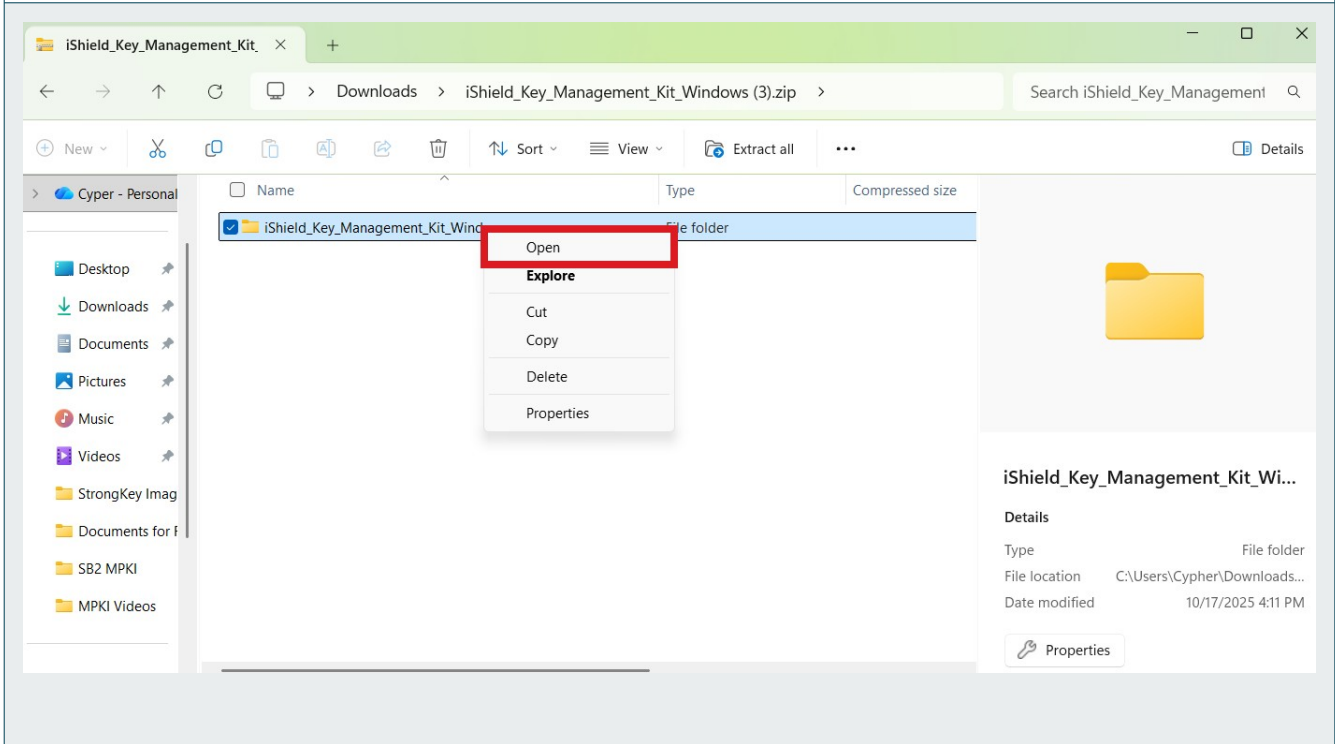
After choosing the destination folder, ensure the 'Show extracted files when complete' option is selected. **Click Extract.**





OPEN FILE

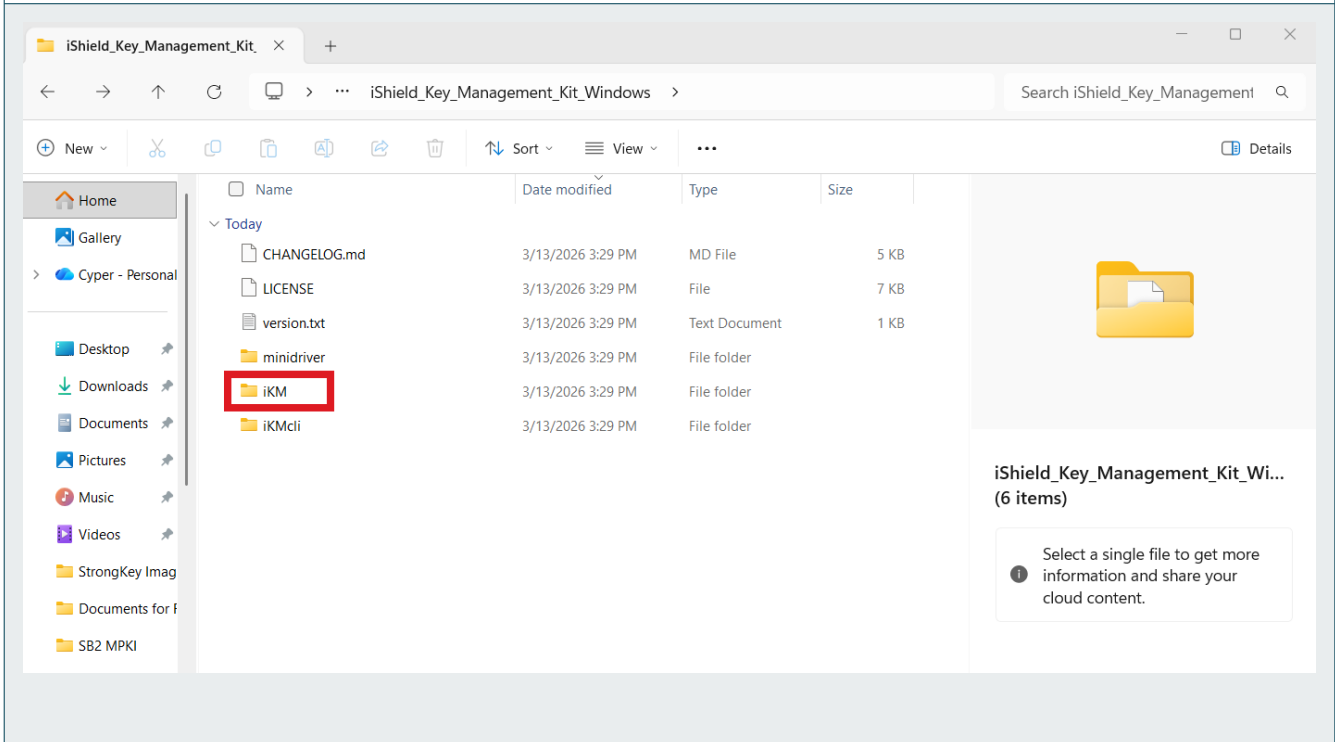
Double-click or Right-click the file to open.





OPEN THE iKM (iSHIELD KEY MANAGER) FOLDER

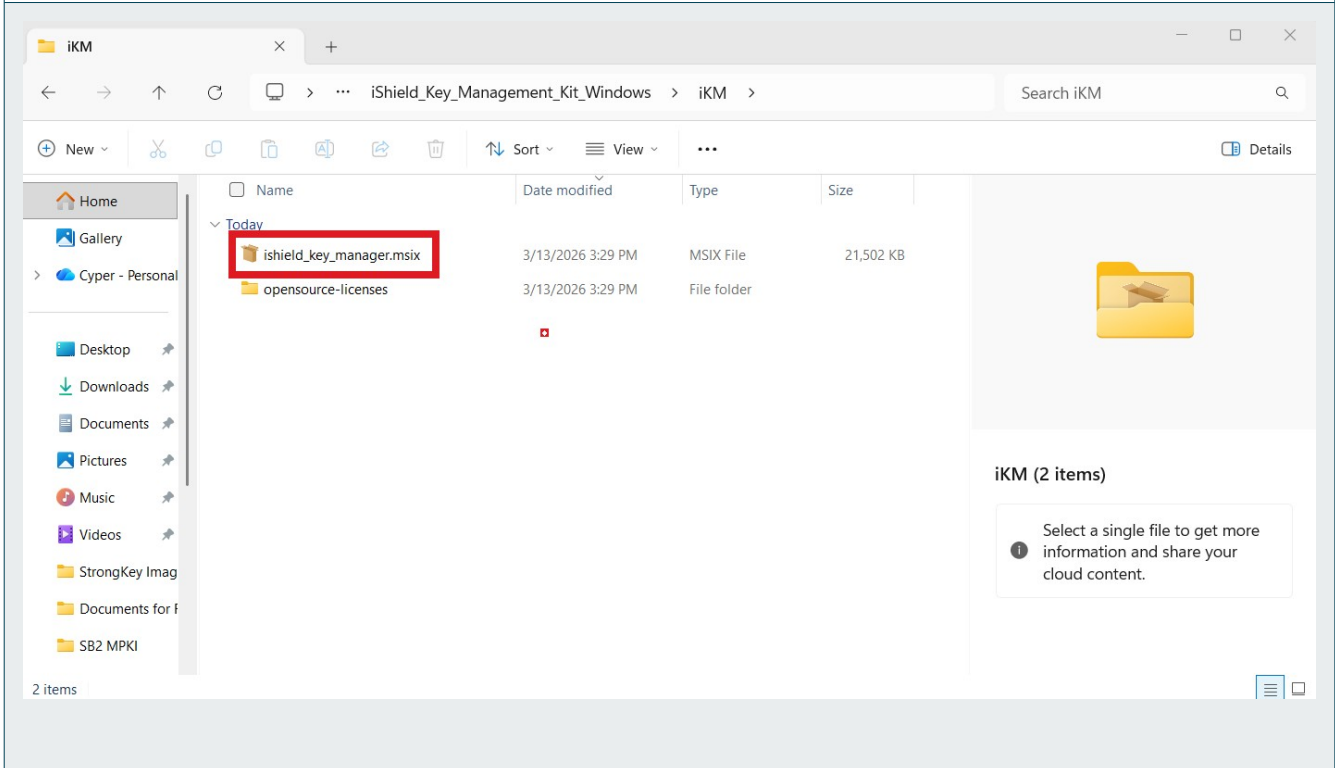
Next, open the iKM folder.





OPEN ISHIELD_KEY_MANAGER.MSIX

Double-click or right-click the “ishield_key_manager.msix” file and follow the prompts.





CLICK INSTALL

Click Install.

Install iShield Key Manager?

Publisher: Swissbit Germany AG

Version: 1.13.1.0

Source: C:\Users\Cypher\Downloads\iShield_Key_Management_Kit_Windows (2)\iShield_Key_Management_Kit_Windows\iKM\ishield_key_manager.msix



Capabilities:

- Uses all system resources
- Access your Internet connection
- Run as administrator

Launch when ready

Install

Cancel



Internet applications can potentially harm your computer. If you do not trust the source, do not install this software. [Learn more](#)



END USERS LICENSE AGREEMENT

Scroll to the bottom of the window and check the box that states you have “read and understand” the terms. **Click Confirm.**

iShield Key Manager

End Users License Agreement (EULA)

agreement as it applies to future purchases of Product(s).

§ 6 Term and Termination

The term of this Agreement shall commence on the date of Swissbit's order confirmation and shall continue until terminated as set forth below, however, our Privacy Notice and Cookie Notice may remain in effect even after expiry or termination of the Agreement. This Agreement shall terminate automatically without notice or action by Swissbit (a) if you breach any material term or condition of this Agreement; or (b) in the event you become insolvent or makes an assignment of this Agreement for the benefit of creditors or if any other bankruptcy proceedings are commenced by or against you.

Upon any termination of this EULA, or license granted pursuant to this EULA, or upon expiration of a term license: (a) all Software Licenses will immediately terminate; (b) You immediately cease all use of the Software; and (c) You must either deliver to Swissbit or irrevocably destroy all copies of Software and Documentation.

§ 7 General

This Agreement, including Exhibits attached hereto, represents the entire understanding and agreement between the parties, and supersedes any and all previous discussions and communications. Any subsequent amendments and/or additions hereto shall be effective only if in writing and signed by both parties. You may not assign your rights or obligations under this Agreement without the prior written consent of SWISSBIT. Subject to the foregoing limitation on assignment, this Agreement shall be binding upon and inure to the benefit of the successors and assigns of the respective parties hereto.

The Software, including Documentation, is subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. You will comply strictly with all applicable export and import regulations and has the responsibility to obtain any licenses required to export, re-export, or import Software and Documentation.

This Agreement shall be interpreted under the laws of Germany without reference to conflict of laws principles and without regard to the United Nations Convention on Contracts for the International Sale of Goods and any amendments thereto.

Except for payment and confidentiality, the protection of intellectual property, neither party is responsible for any delay in performance of this EULA to the extent due to causes beyond its reasonable control.

The place of jurisdiction is Berlin.

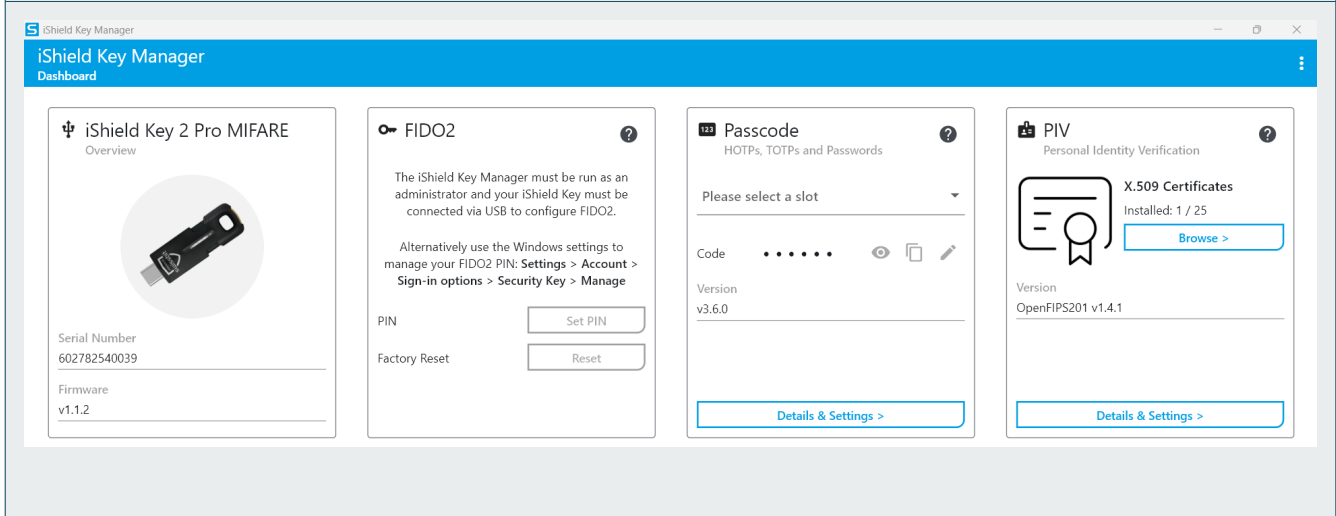
If any part, term, or provision of this Agreement shall be held illegal, unenforceable, or in conflict with any law of a federal, state, or local government having jurisdiction over this Agreement, the validity of the remaining portions or provisions shall not be affected thereby.

I have read and agree to the terms of the End User License Agreement

A12

iSHIELD KEY MANAGER

After clicking “confirm,” the iShield Key Manager will open automatically to the Dashboard. After reviewing, you may close the iShield Key Manager application.



SECTION B



STRONGKEY

B1

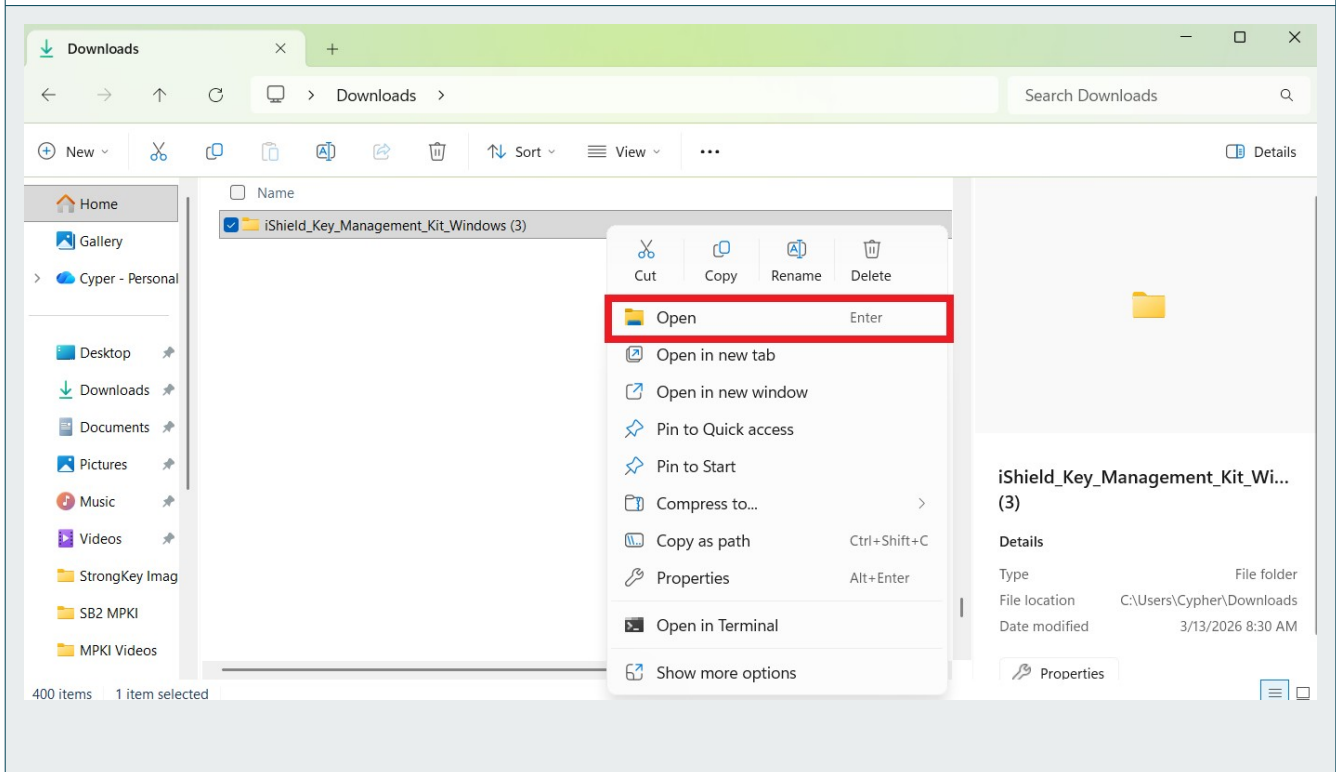
INSTALLING THE SWISSBIT MINIDRIVER FOR WINDOWS 11

This software is essential for enabling the use of a Swissbit iShield2 Security Key on your computer. Before beginning the installation process, please review the process and ensure your computer meets all prerequisites.



OPEN THE iSHIELD FOLDER

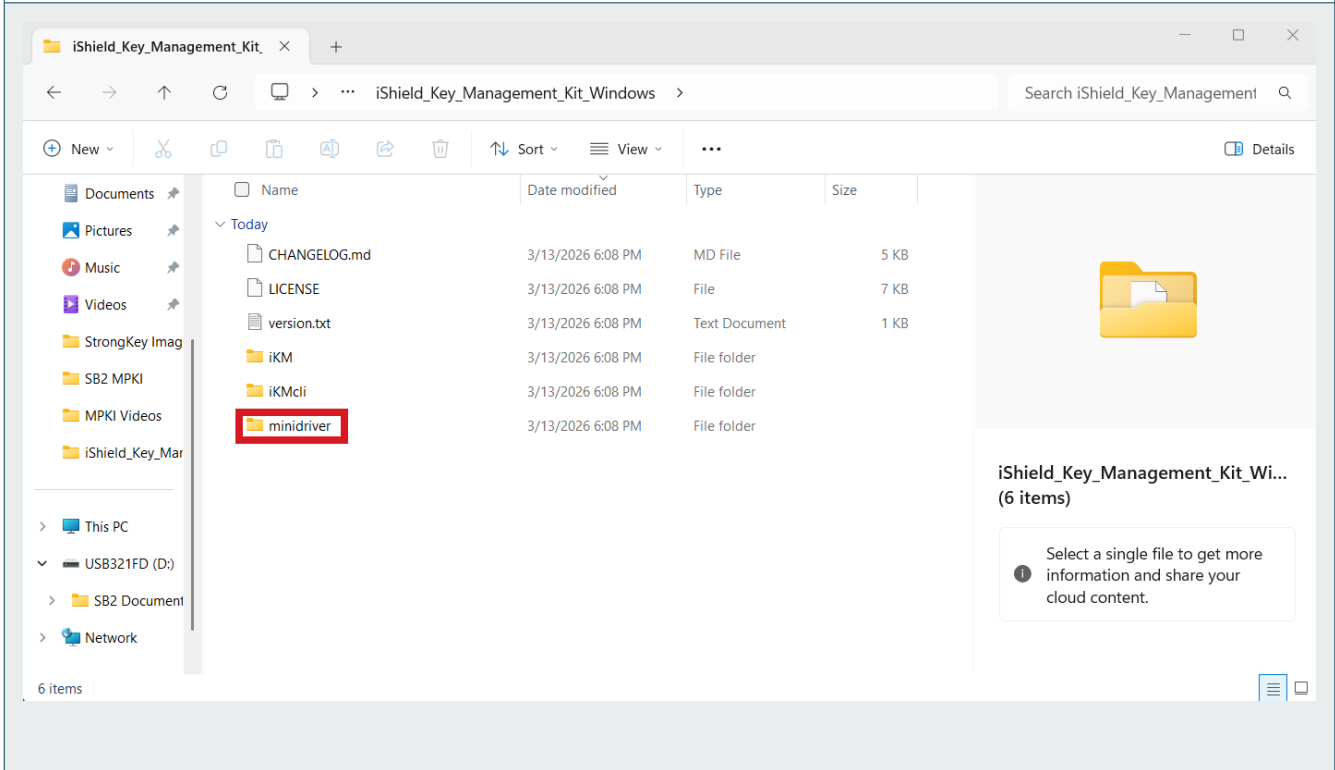
Use File Explorer to return to your Downloads and **Right-click** or **Double-click** the “iShield_Key_Management_Kit_Windows” folder.





OPEN THE MINIDRIVER FOLDER

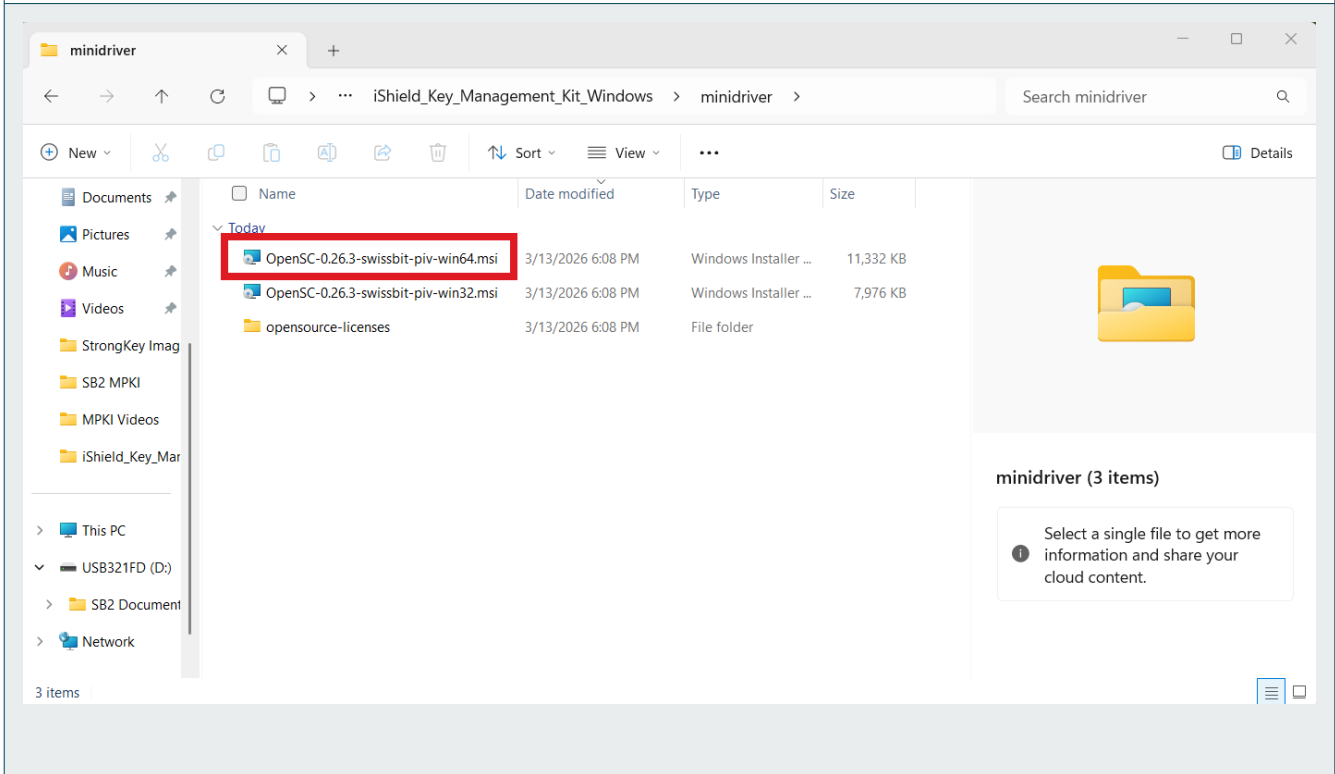
Right-click or Double-click the minidriver folder.





INSTALL THE MINIDRIVER

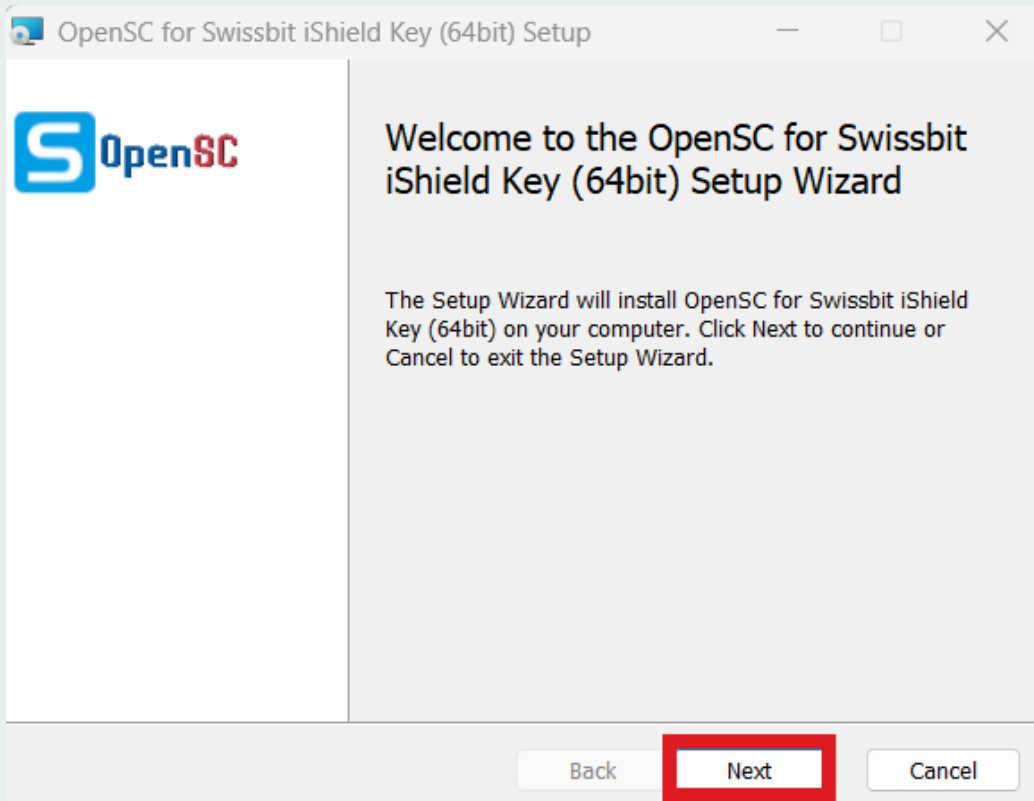
Double-click the OpenSC “win64” minidriver. This will launch the iShield install wizard.





iSHIELD KEY SETUP WIZARD

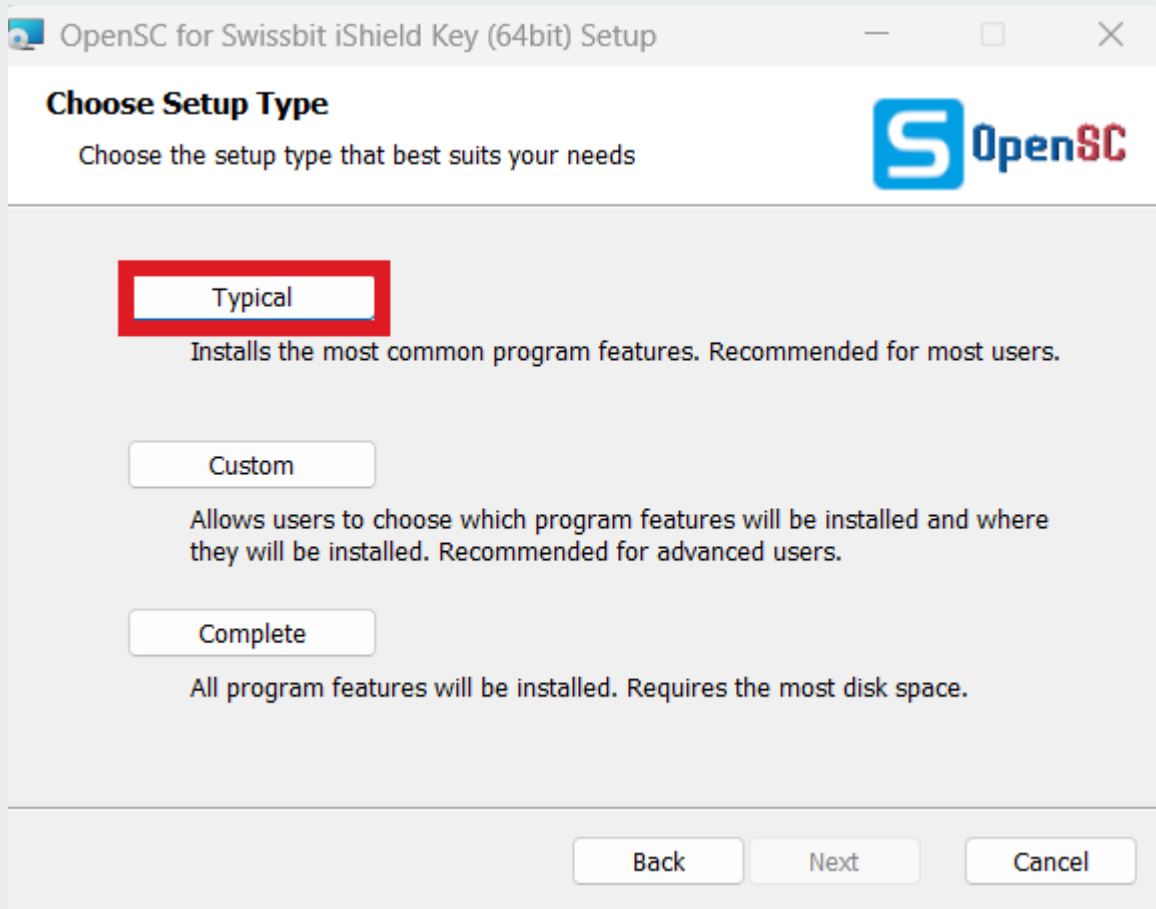
Follow the onscreen prompts. **Click Next.**





SELECT SETUP TYPE

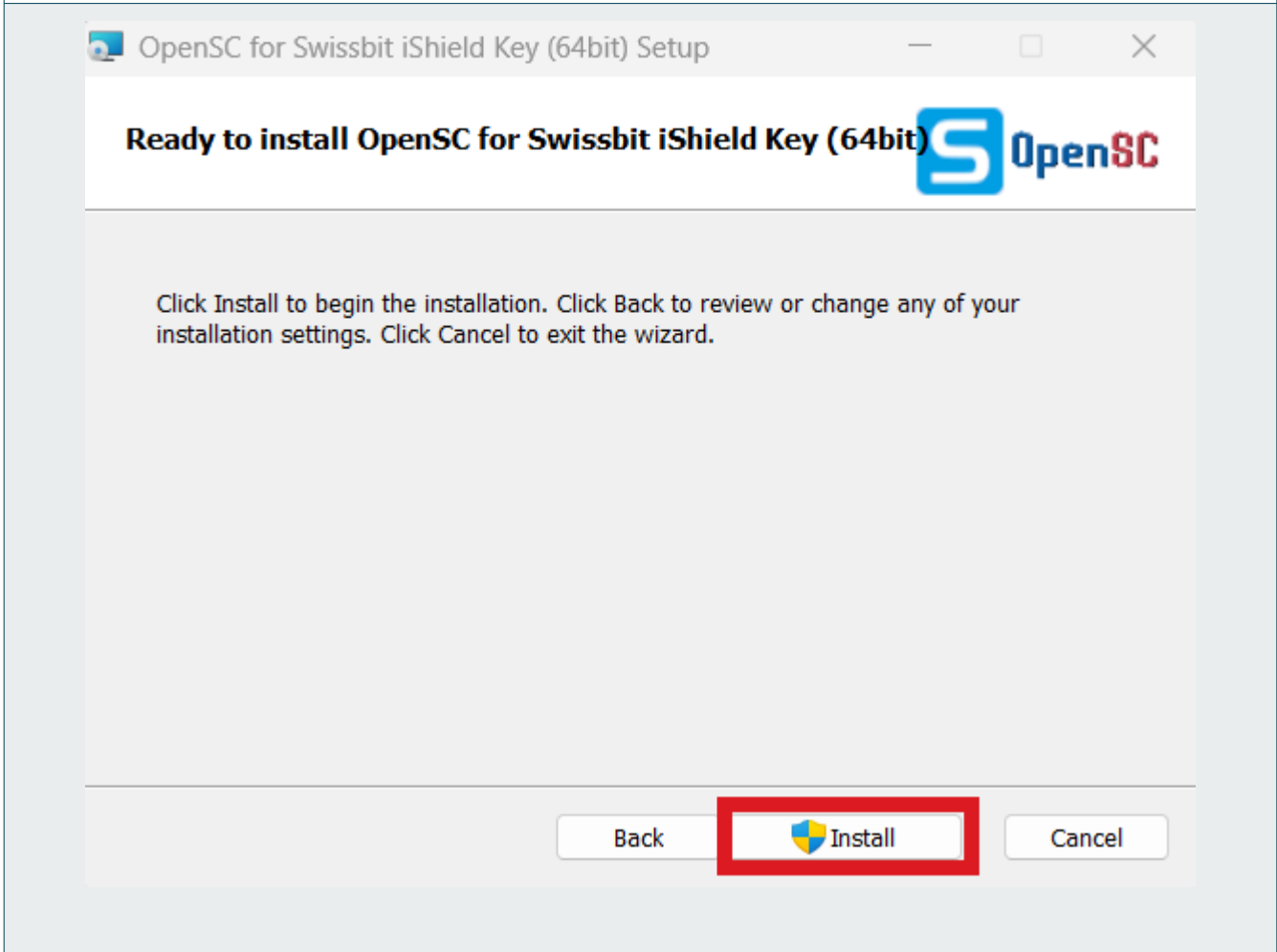
Select Typical.





INSTALL MINIDRIVER

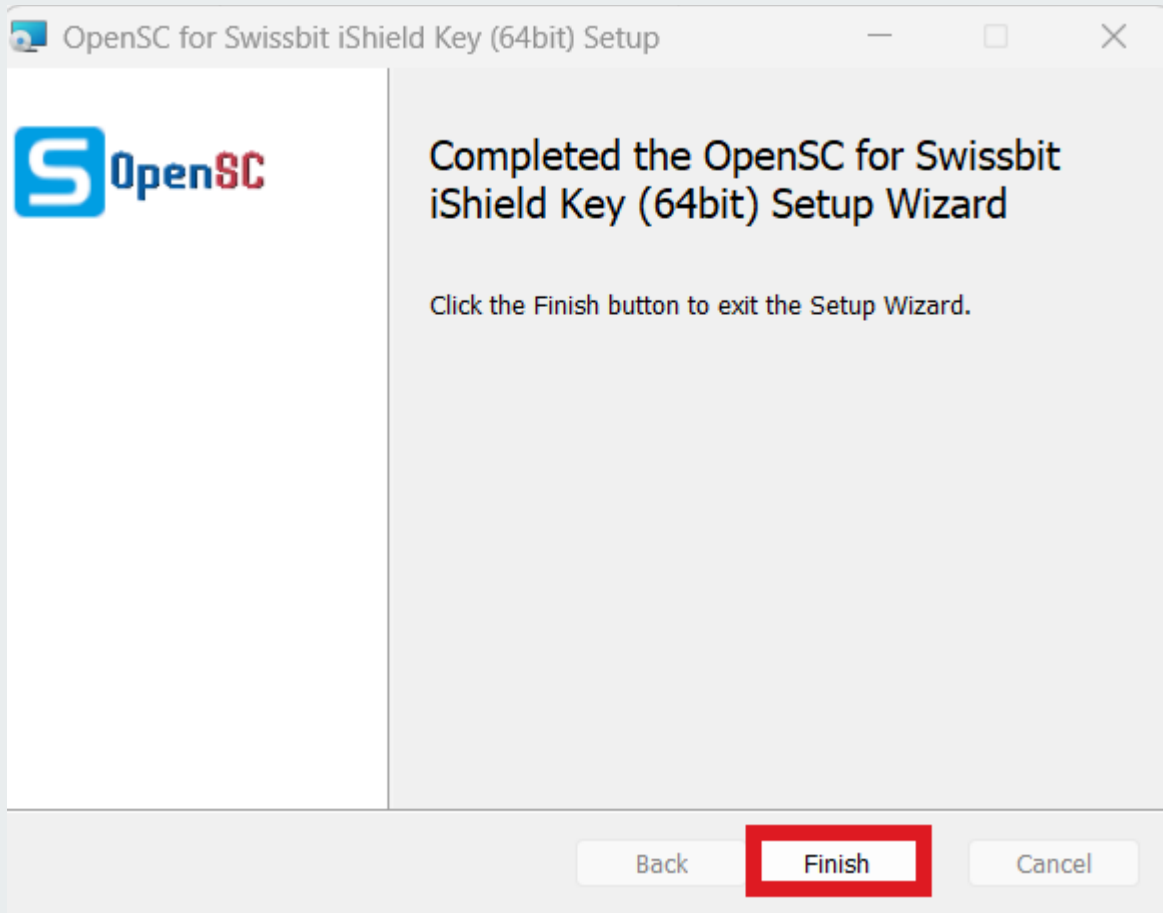
Click **Install**, then approve the prompt allowing the Wizard to make changes to your computer.





FINISH INSTALL

Click Finish. The Swissbit minidriver install is complete.



SECTION C



STRONGKEY

C1

IMPORTING SB2 ROOT CA AND SUBORDINATE CA CERTIFICATES INTO TRUSTSTORE

When using Security Keys with digital certificates for authentication to an SB2 site, the SB2 Root Certificate Authority (CA) certificate of the site is a critical component in establishing trust between your browser and the site. It ensures the digital certificate on your Security Key was issued by that SB2 site and is currently valid.



ACCESS THE SB2 PKI PORTAL

All required CA certificates are available for download from the SB2 PKI portal at <https://www.strongkey.com/sb2pki>. Comprehensive SB2PROD documentation is also accessible through this site.

<https://www.strongkey.com/sb2pki>

STRONGKEY

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

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

SB2 Production CA Certificates

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

How To Configure CA Certificates

Swissbit Security Keys

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

Yubikey Security Keys

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



SB2 CA CERTIFICATES

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

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

The screenshot shows the StrongKey website interface. At the top, the StrongKey logo is displayed with the text "Welcome to the StrongKey Tellaro Small Business Security Bundle (SB2)". Below this, a message states: "This page provides information to help you get started working with SB2. If you have any questions, please send an e-mail to getsecure@strongkey.com".

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

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

Under "Swissbit Security Keys", there are three rows of buttons representing different file formats and operating systems:

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

Under "Yubikey Security Keys", there is one row of buttons:

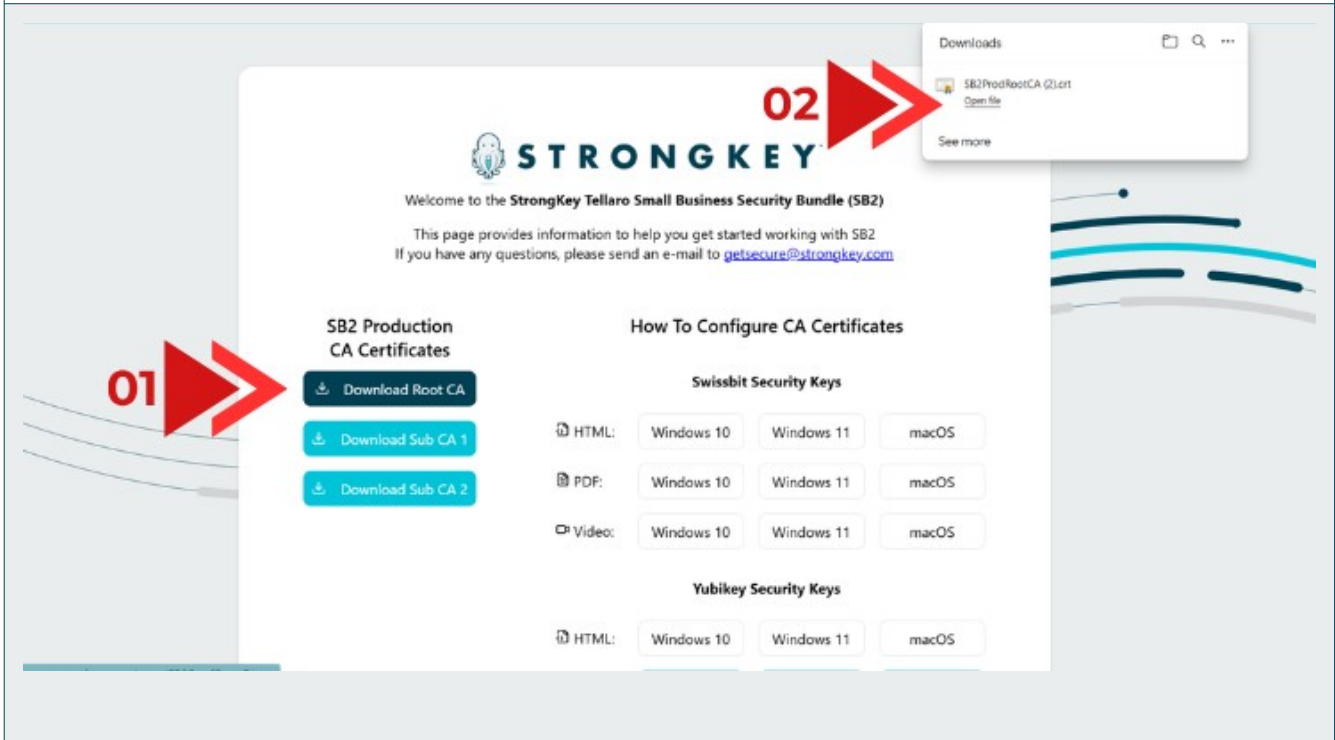
Format	Windows 10	Windows 11	macOS
HTML:	Windows 10	Windows 11	macOS

C4

DOWNLOADING THE SB2 ROOT CA

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

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





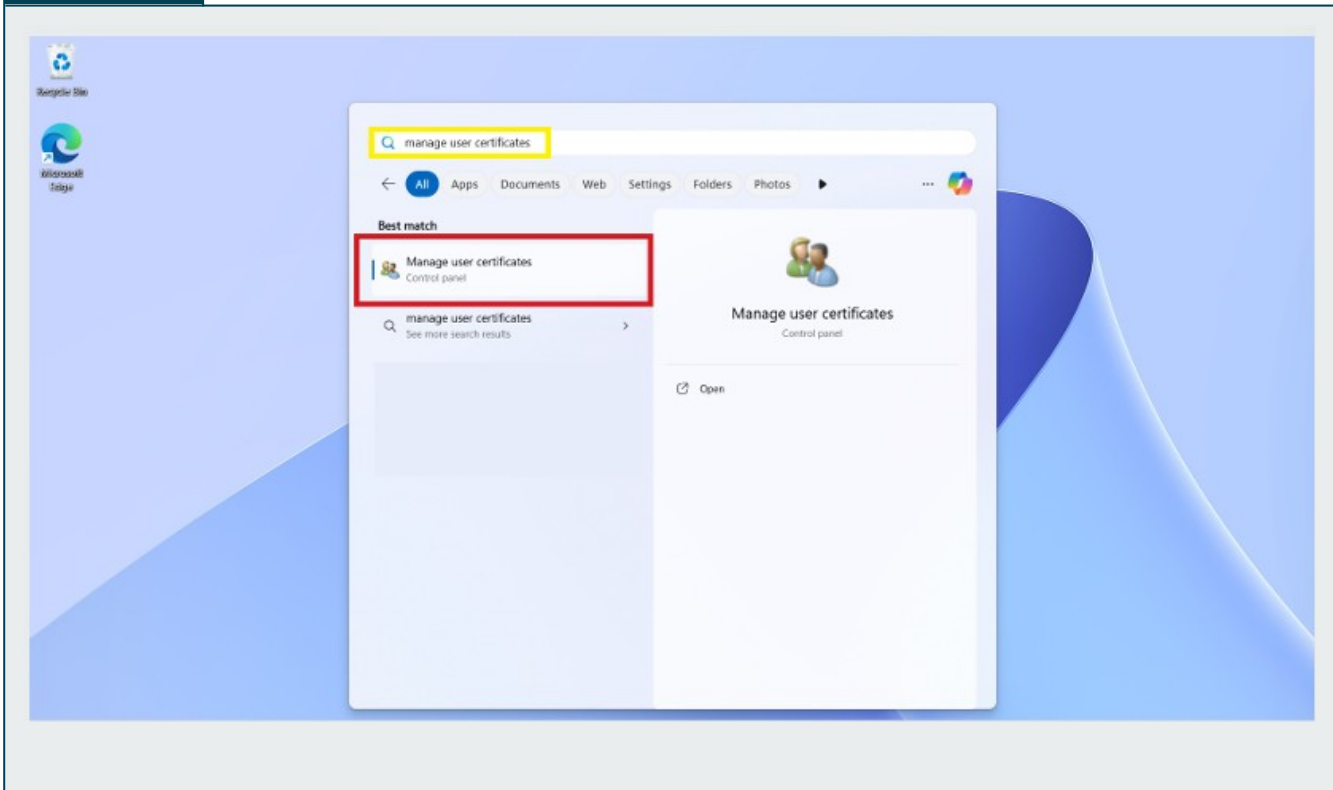
NAVIGATE TO THE WINDOWS START ICON

After clicking the Windows Start icon, search for **Manage user certificates** to find the settings application for overseeing and configuring security certificates, including importing. Next, select the **Manage user certificates** application.



NOTE

The **Manage user certificates** application is also known as **certmgr** (short for Certificate Manager). In this document, these terms are used interchangeably.

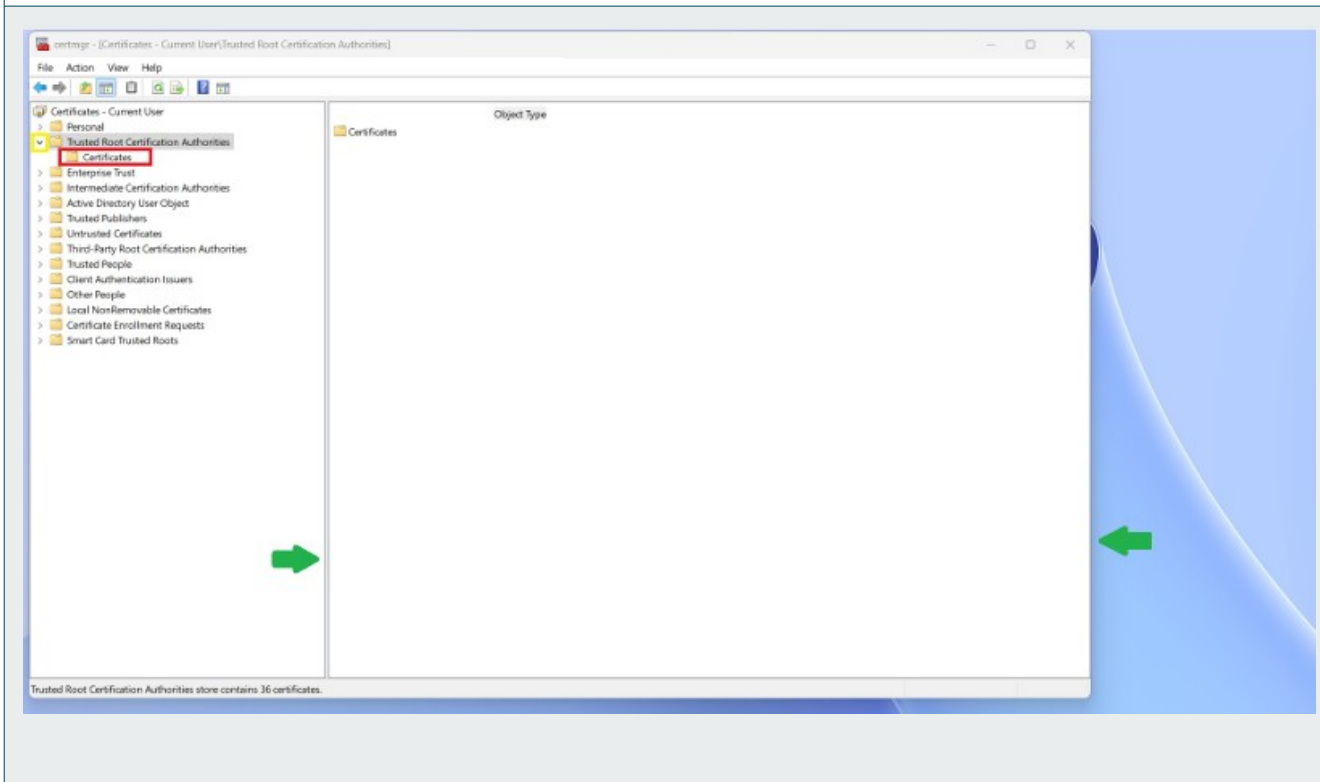




OPEN TRUSTED ROOT CERTIFICATION AUTHORITIES FOLDER

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

Next, click the **arrow** (yellow box) next to the **Trusted Root Certification Authorities** folder to expand it, revealing the **Certificates** (red box) folder.

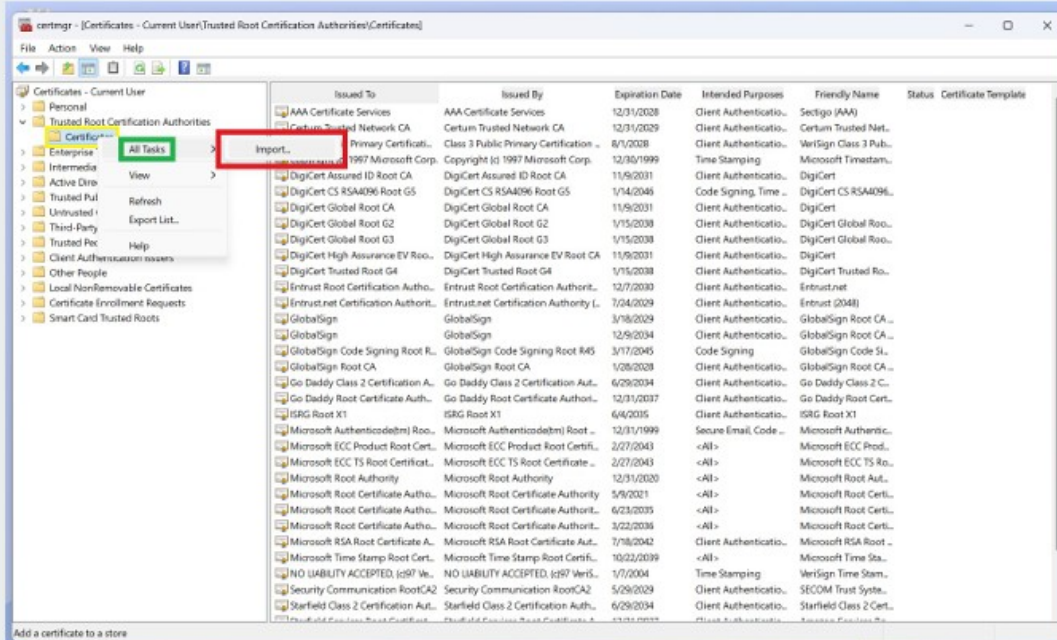




INITIATE THE SB2 ROOT CERTIFICATE IMPORT

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

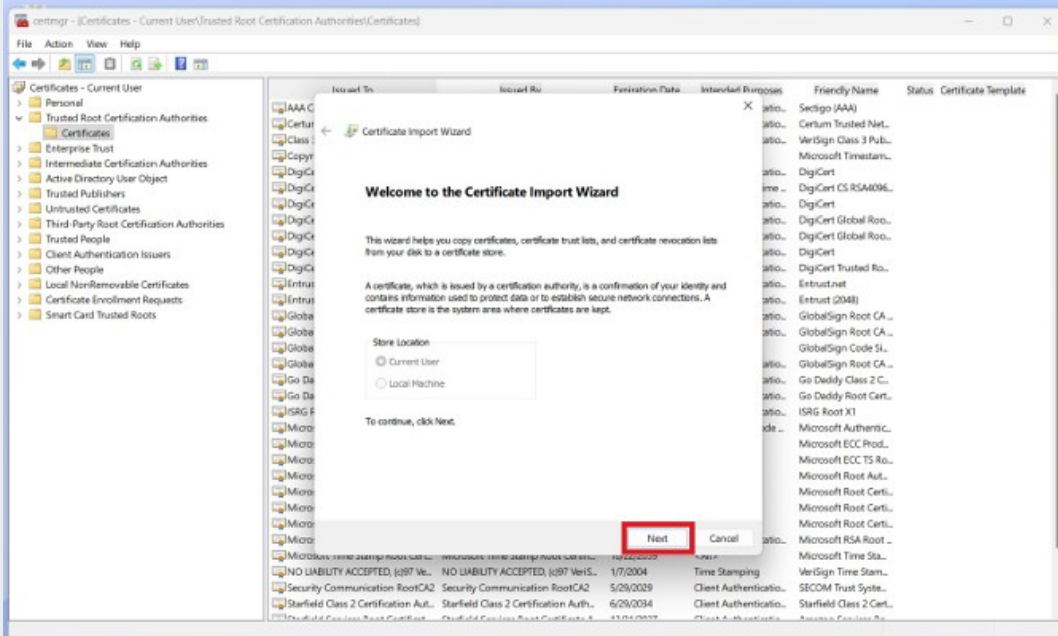
Select **All Tasks**, and click **Import** to start the Certificate Import Wizard.





CERTIFICATE IMPORT WIZARD

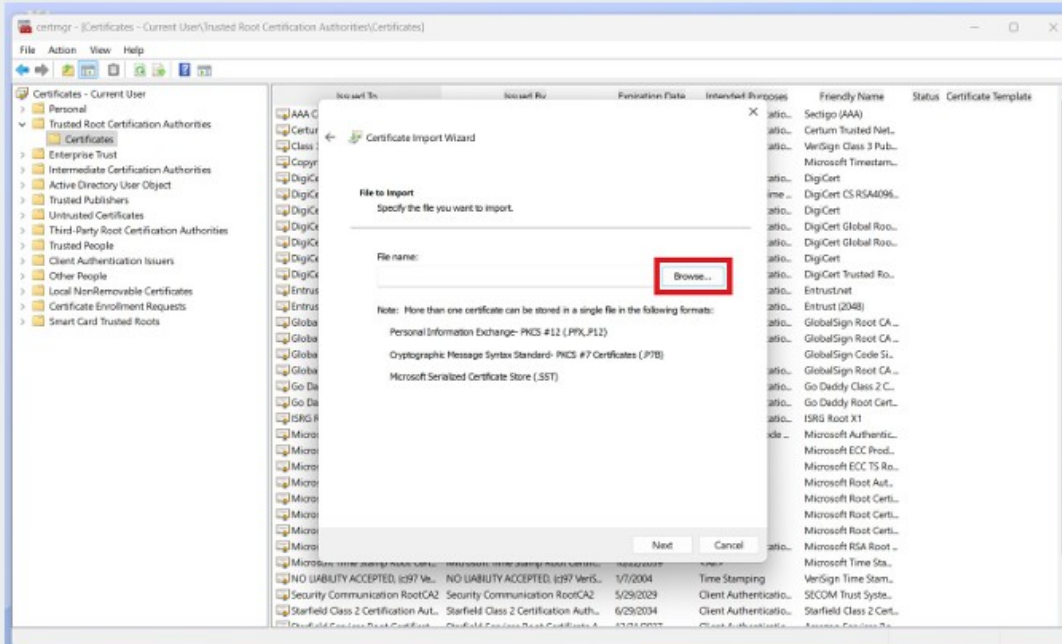
The Certificate Import Wizard will open. Click Next to proceed.





LOCATE THE SB2 ROOT CA CERTIFICATE

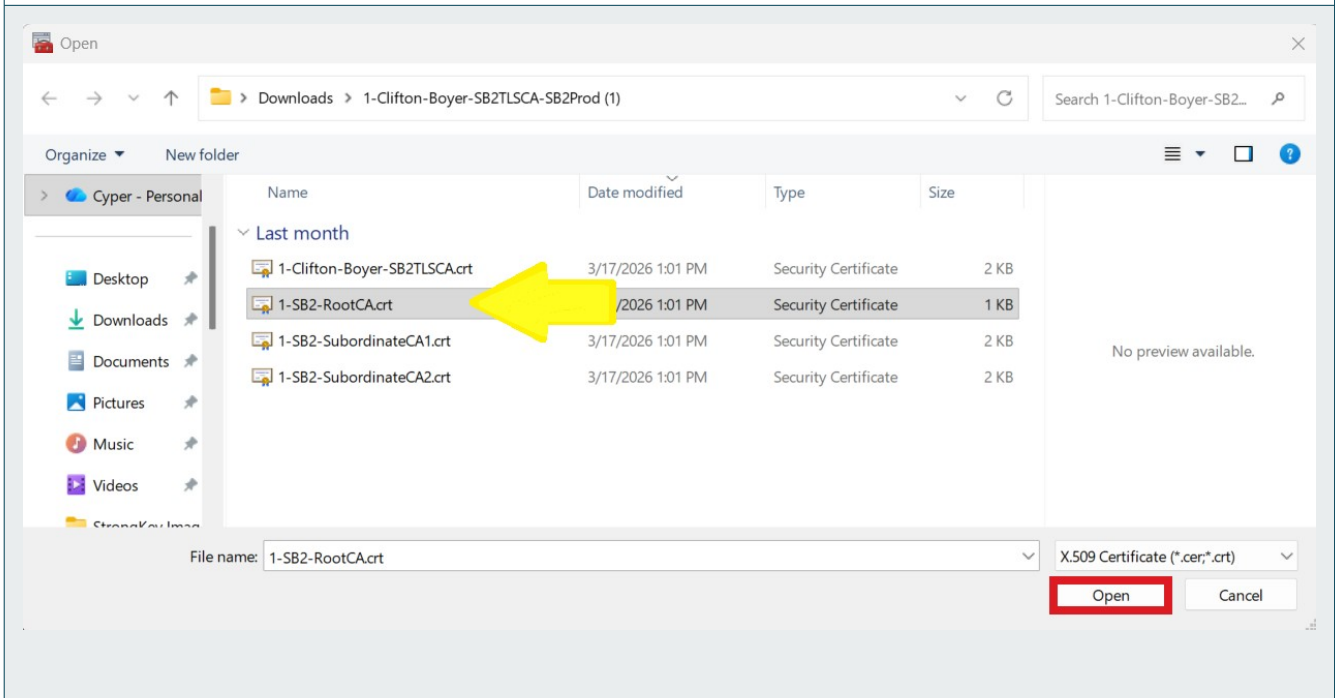
Click the **Browse** button to locate the SB2 Root CA certificate file.





OPEN THE SB2 ROOT CA CERTIFICATE

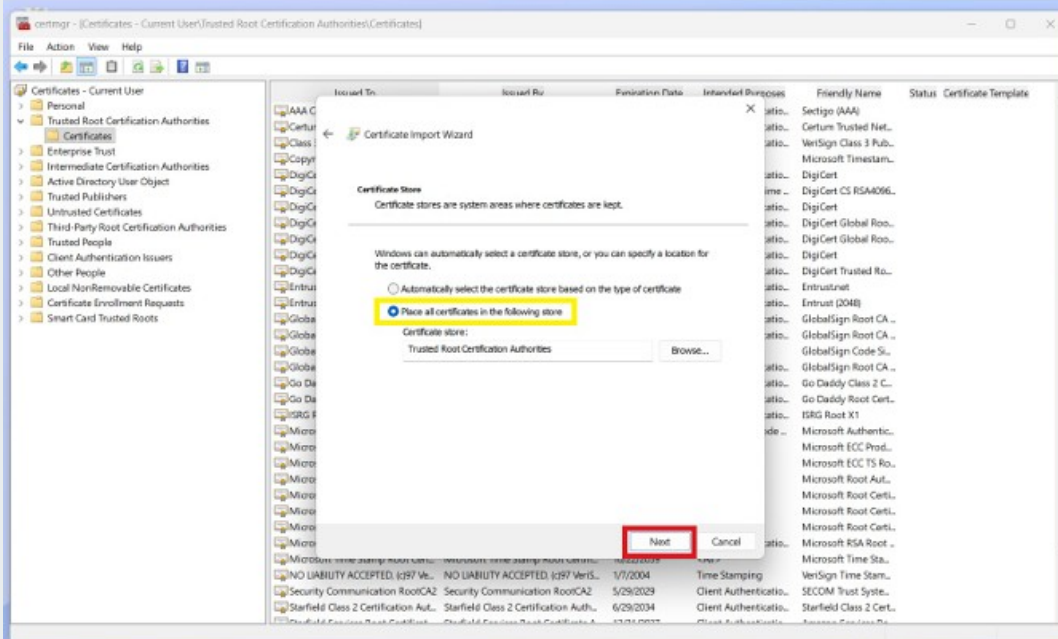
To find the SB2 Root CA Certificate, go to the **SB2ProdRootCA.crt** file's location, which is typically the **Downloads** folder. Once the **SB2ProdRootCA.crt** is located, select it and **click Open**.





SELECT CERTIFICATE STORE

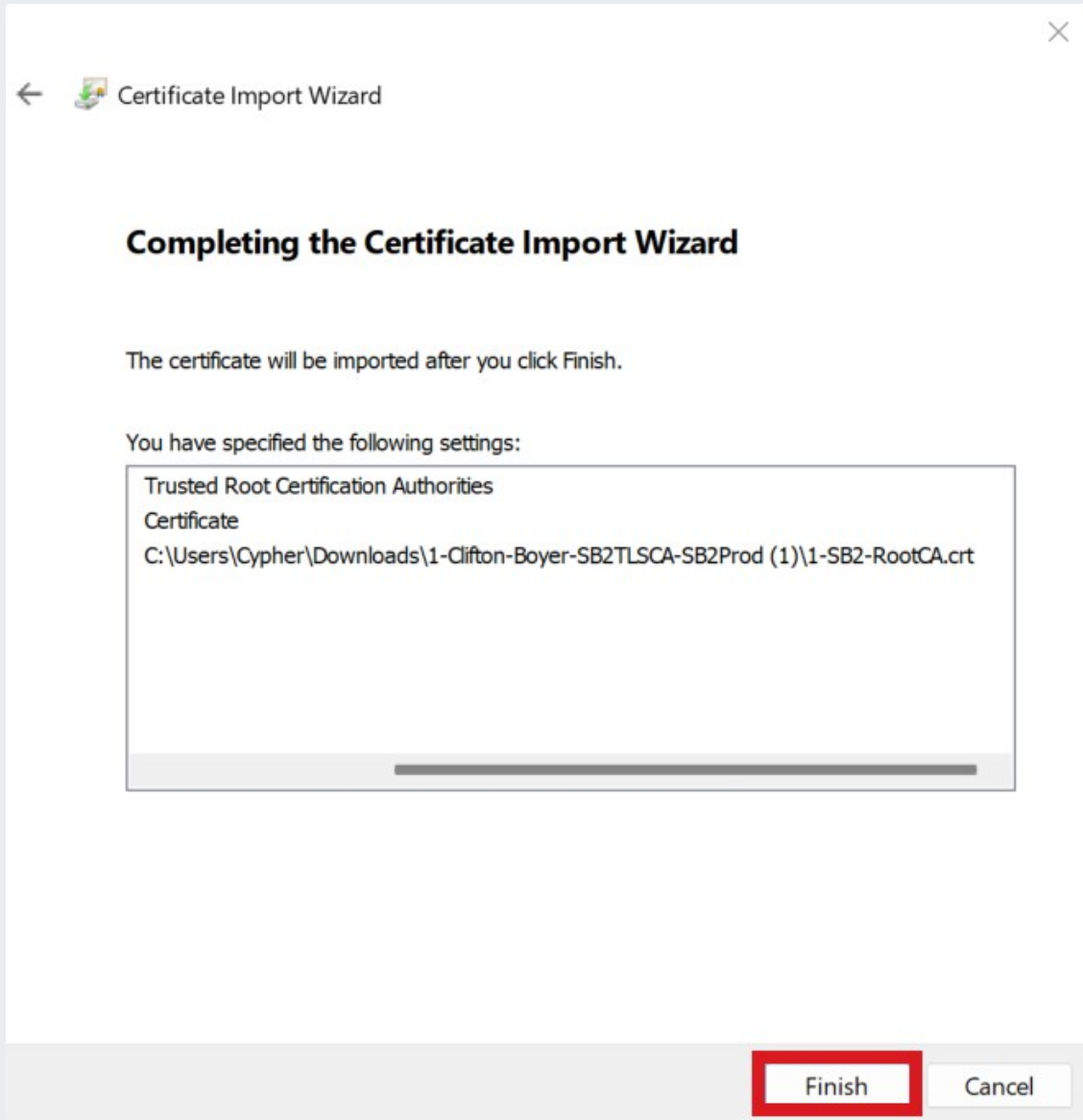
Ensure the *Certificate Store* field indicates the digital certificate will be added to the **Trusted Root Certification Authorities** store before clicking **Next** to continue.





FINISH IMPORTING THE SB2 ROOT CA CERTIFICATE

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





SECURITY WARNING

A security warning will be displayed regarding the Root CA Certificate. Make sure the name of the certificate and the Thumbprint (sha1) shown in the warning window match the content shown here:

SB2 RootCA

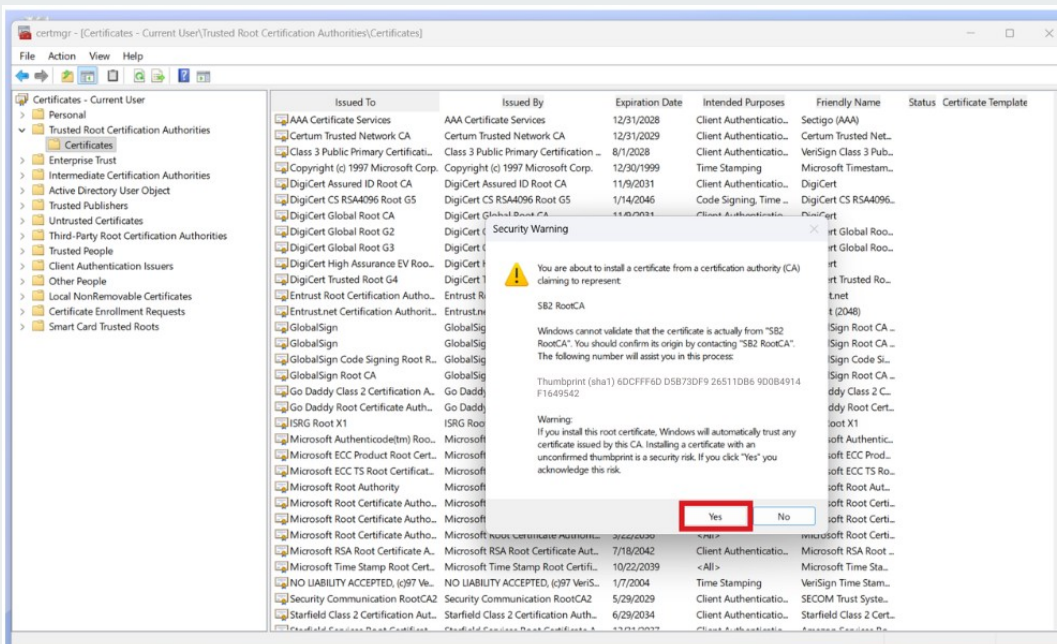
6DCFFF6D D5B73DF9 26511DB6 9D0B4914 F1649542

If it matches *identically*, click **Yes**.



NOTE

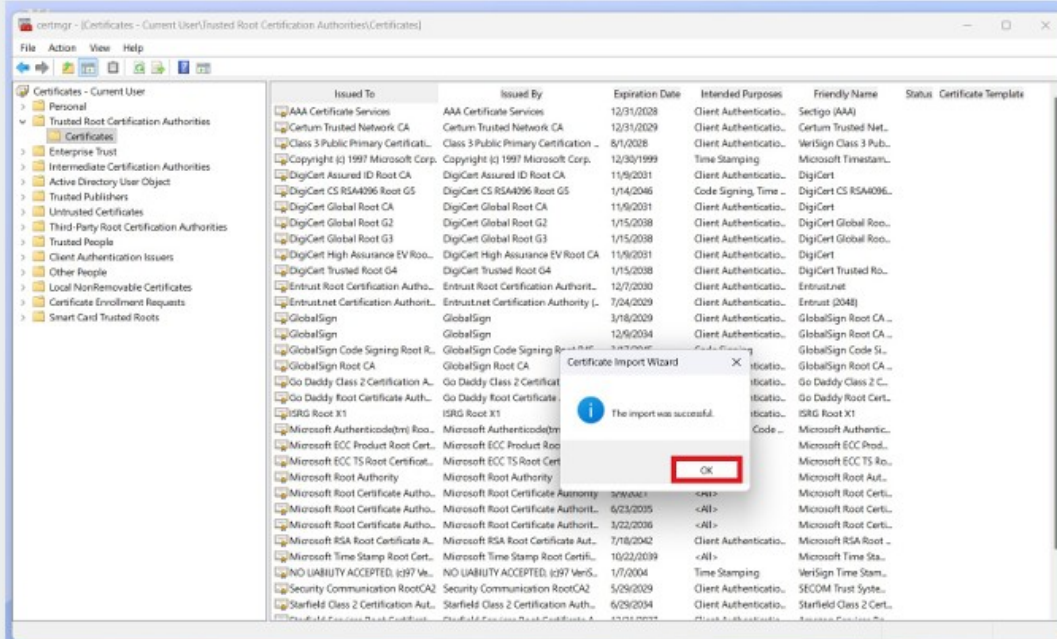
If the Thumbprint of the CA certificate does not match, contact the Administrator of the SB2 site. This step represents the most important step in establishing trust in the SB2 platform.





A SUCCESSFUL IMPORT

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



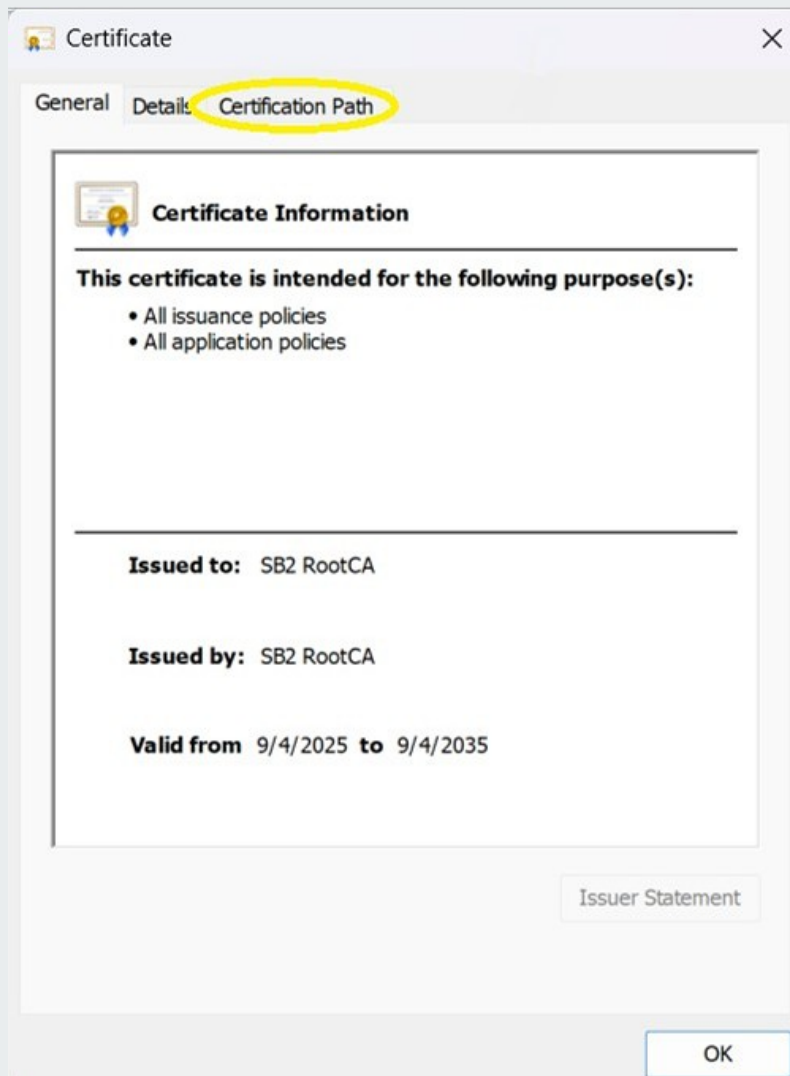


VERIFY SB2 ROOT CA IN CERTIFICATES LIST

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

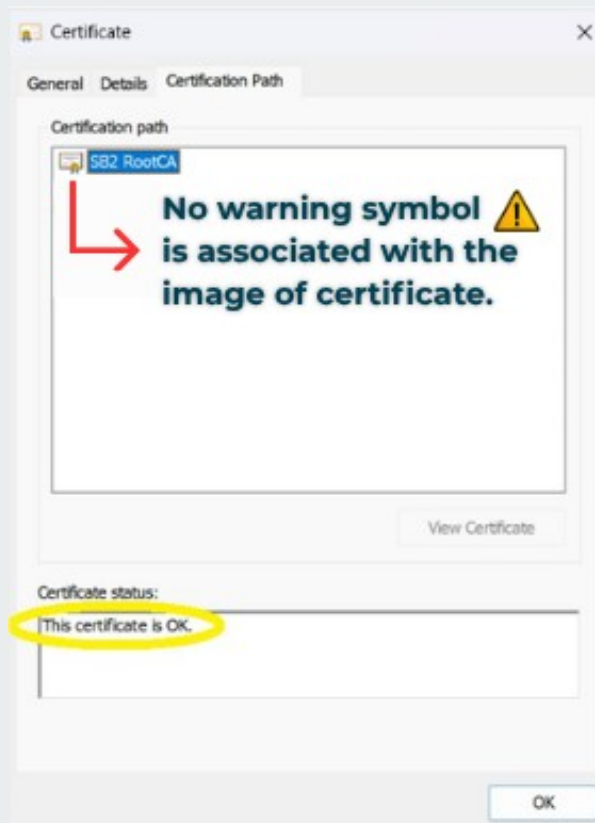
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem.
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authentication...	DigiCert		
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authentication...	DigiCert Global Roo...		
DigiCert Global Root G3	DigiCert Global Root G3	1/15/2038	Client Authentication...	DigiCert Global Roo...		
DigiCert High Assurance EV Root...	DigiCert High Assurance EV Root CA	11/9/2031	Client Authentication...	DigiCert		
DigiCert Trusted Root G4	DigiCert Trusted Root G4	11/5/2038	Client Authentication...	DigiCert Trusted Ro...		
Entrust Root Certification Autho...	Entrust Root Certification Authori...	12/7/2030	Client Authentication...	Entrust.net		
Entrust.net Certification Autho...	Entrust.net Certification Authority (...)	7/24/2029	Client Authentication...	Entrust (2048)		
GlobalSign	GlobalSign	3/18/2029	Client Authentication...	GlobalSign Root CA ...		
GlobalSign	GlobalSign	12/9/2034	Client Authentication...	GlobalSign Root CA ...		
GlobalSign Code Signing Root R...	GlobalSign Code Signing Root R45	3/17/2045	Code Signing	GlobalSign Code S...		
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Client Authentication...	GlobalSign Root CA ...		
Go Daddy Class 2 Certification A...	Go Daddy Class 2 Certification Aut...	6/29/2034	Client Authentication...	Go Daddy Class 2 C...		
Go Daddy Root Certificate Autho...	Go Daddy Root Certificate Authori...	12/31/2037	Client Authentication...	Go Daddy Root Cert...		
ISRG Root X1	ISRG Root X1	6/4/2035	Client Authentication...	ISRG Root X1		
Microsoft Authenticode(m) Roo...	Microsoft Authenticode(m) Root ...	12/31/1999	Secure Email, Code ...	Microsoft Authentic...		
Microsoft ECC Product Root Cert...	Microsoft ECC Product Root Certifi...	2/27/2043	<All>	Microsoft ECC Prod...		
Microsoft ECC TS Root Certificat...	Microsoft ECC TS Root Certificate ...	2/27/2043	<All>	Microsoft ECC TS Ro...		
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...		
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authority	5/8/2021	<All>	Microsoft Root Certi...		
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authority...	6/23/2035	<All>	Microsoft Root Certi...		
Microsoft Root Certificate Autho...	Microsoft Root Certificate Authority...	3/22/2036	<All>	Microsoft Root Certi...		
Microsoft RSA Root Certificate A...	Microsoft RSA Root Certificate Aut...	7/18/2042	Client Authentication...	Microsoft RSA Root ...		
Microsoft Time Stamp Root Cert...	Microsoft Time Stamp Root Certifi...	10/22/2039	<All>	Microsoft Time Sta...		
NO LIABILITY ACCEPTED, (c97) Ve...	NO LIABILITY ACCEPTED, (c97) Veri...	1/7/2004	Time Stamping	VeriSign Time Stam...		
SB2 RootCA	SB2 RootCA	9/4/2035	<All>	<None>		
Secigo Public Server Authentica...	Secigo Public Server Authentication...	3/21/2046	Client Authentication...	Secigo Public Serve...		
Security Communication RootCA2	Security Communication RootCA2	5/29/2029	Client Authentication...	SECOM Trust Syste...		
SSL.com EV Root Certification Au...	SSL.com EV Root Certification Auth...	5/30/2042	Client Authentication...	SSL.com EV Root Cer...		
SSL.com Root Certification Auth...	SSL.com Root Certification Author...	2/12/2041	Client Authentication...	SSL.com Root Certifi...		
Starfield Class 2 Certification Aut...	Starfield Class 2 Certification Auth...	6/29/2034	Client Authentication...	Starfield Class 2 Cert...		
Starfield Services Root Certificat...	Starfield Services Root Certificate A...	12/31/2037	Client Authentication...	Amazon Services Ro...		
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root F...	3/14/2032	Code Signing	<None>		
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Thawte Timestampi...		
USERTrust RSA Certification Auth...	USERTrust RSA Certification Author...	1/18/2038	Client Authentication...	Setigo		

By double-clicking the SB2 Root CA certificate – or **right-clicking** the mouse button and selecting Open, you should see the following window. Select the **Certification Path** tab in this window:



In the **Certification Path** tab of the **SB2 Root CA** certificate, you should be able to confirm these two important attributes of the certificate:

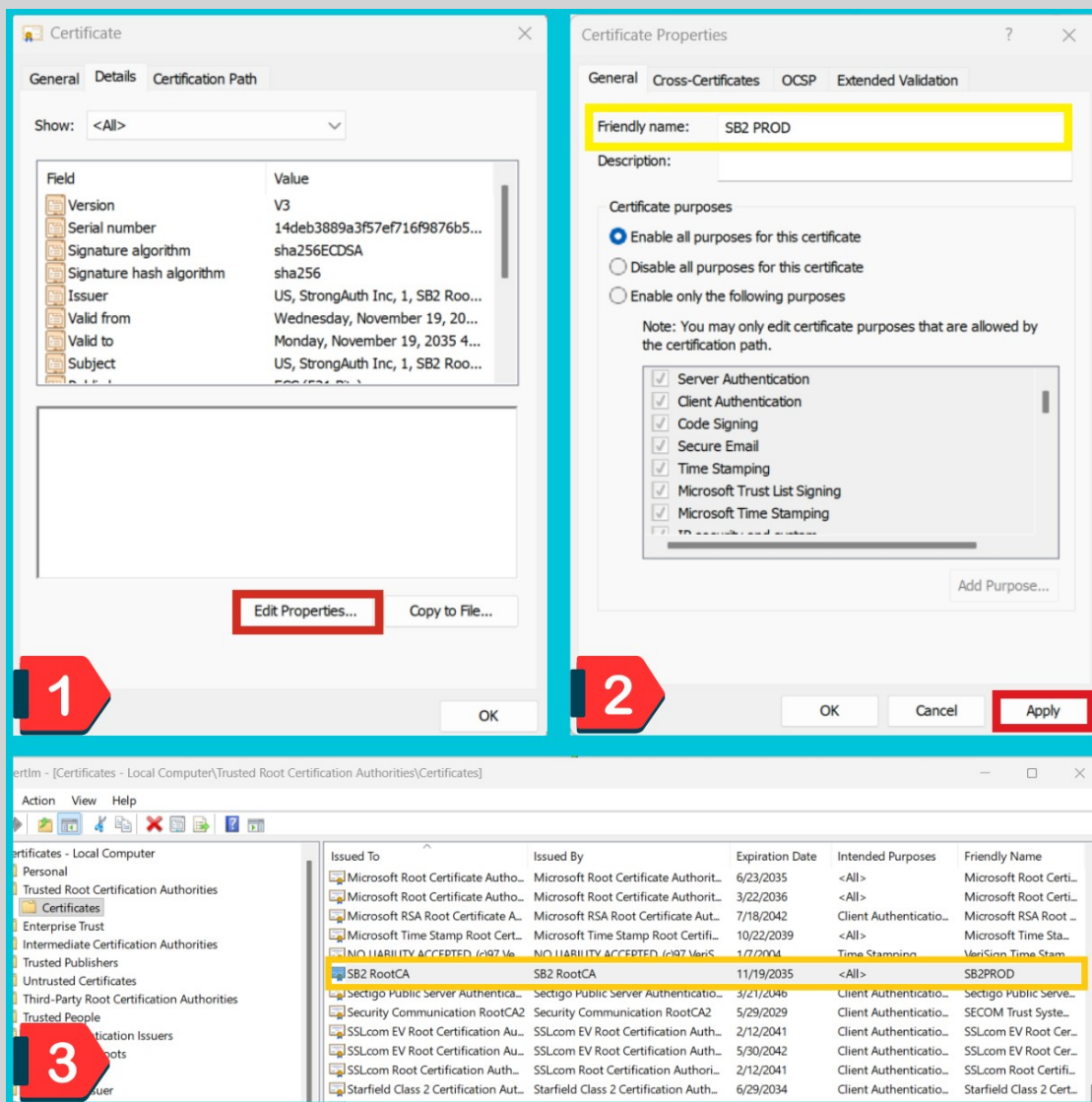
- That the certificate symbol in the **Certification Path** sub-panel at the top does not have any yellow warning symbol associated with it, and
- The **Certificate status** sub-panel at the bottom should state that “This certificate is OK.”



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

1. Choose the Details tab.
2. Click Edit Properties (image 1).
3. Add name in Friendly name field (image 2).
4. Click Apply then Click OK to finish.

Friendly names make identifying Root CAs easier in the certificates list (image 3).

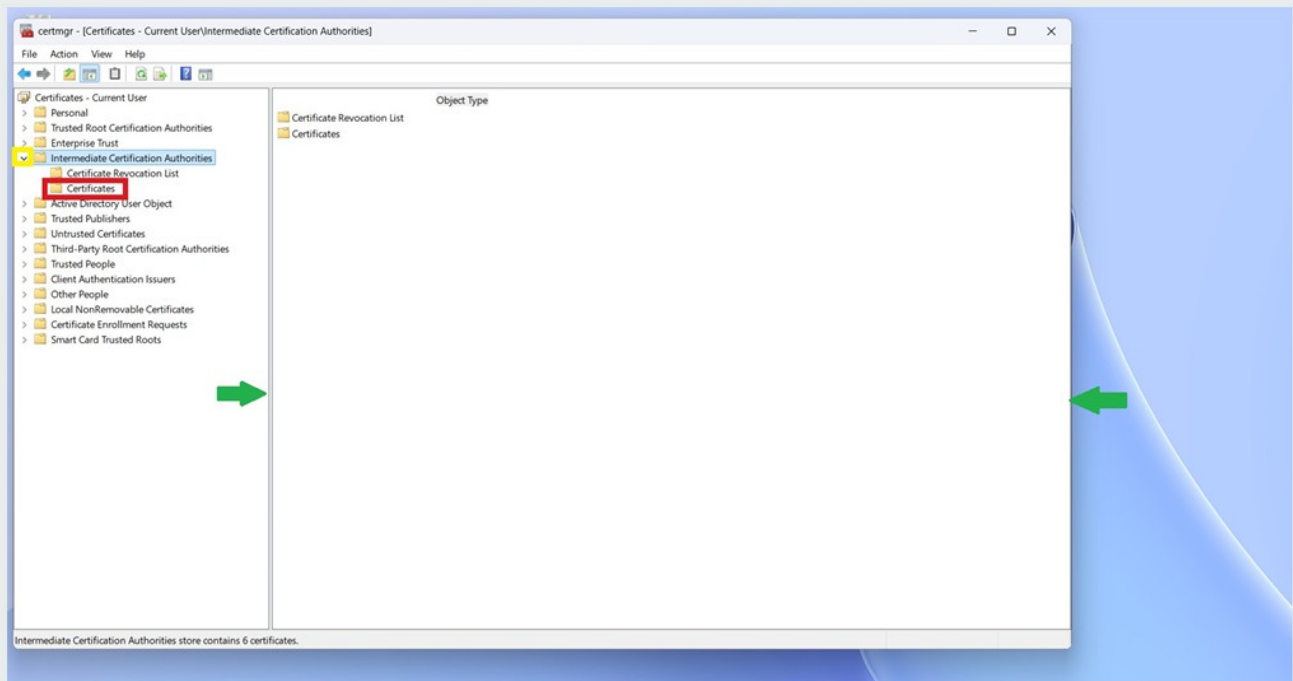




INTERMEDIATE CERTIFICATION AUTHORITIES FOLDER

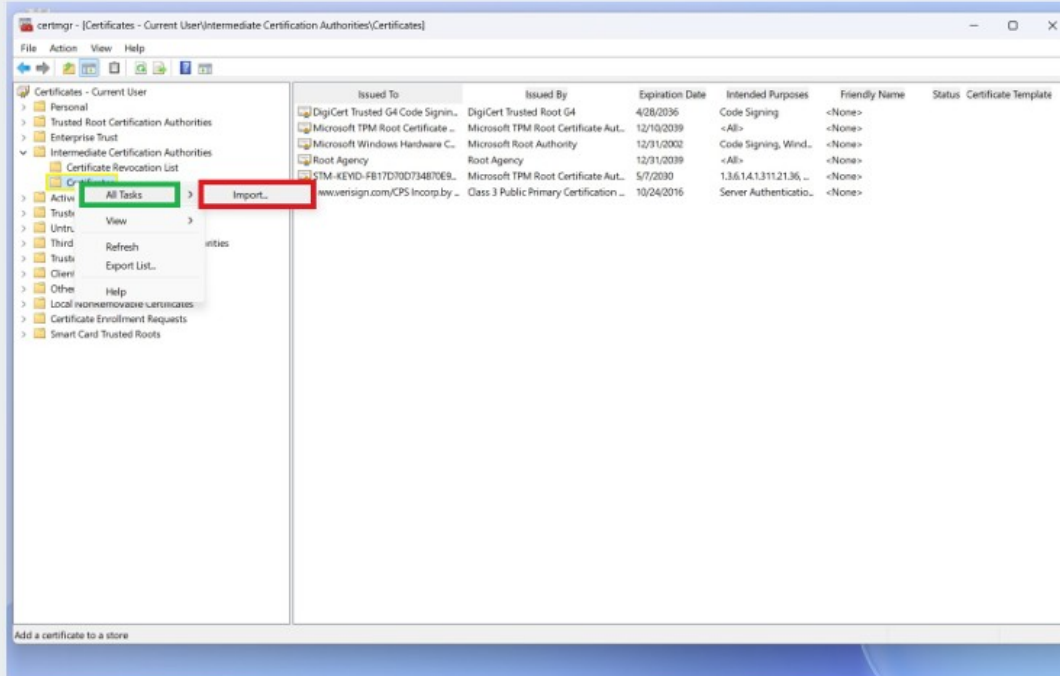
Just as you imported the SB2PROD Root CA certificate, you will now import the two SB2PROD Subordinate CA (aka SubCA) certificates. The SubCA certificates play a vital role in establishing the “certificate chain of trust” between the digital certificate on your Security Key and the SB2 site.

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



INITIATING THE SB2 SUBORDINATE CA CERTIFICATE IMPORT

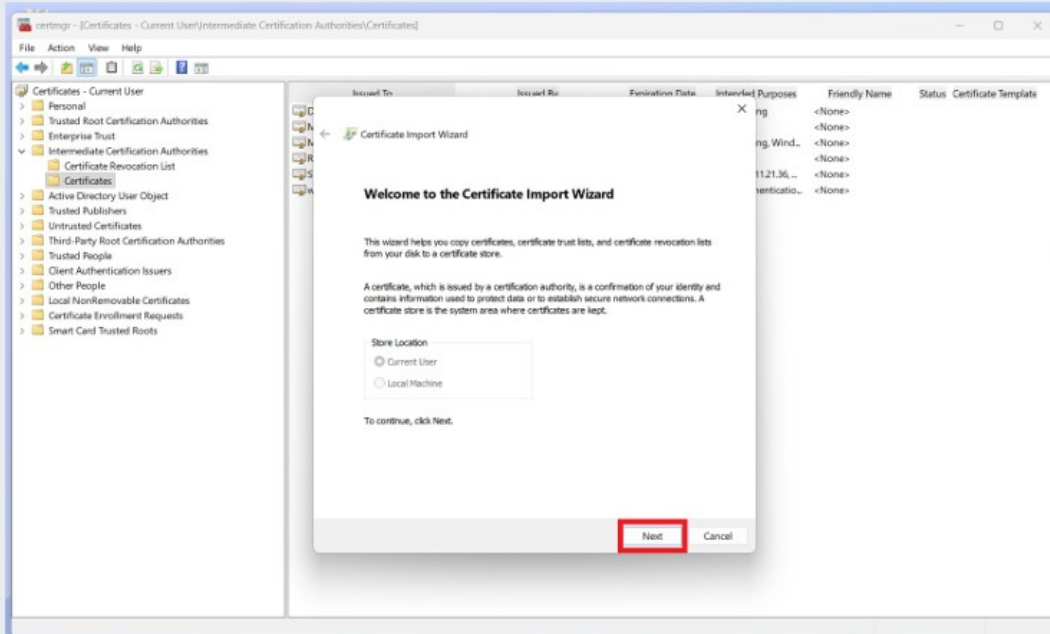
To begin, right-click the **Certificates** folder to open the context menu. From there, select **All Tasks**, and then click **Import** to start the **Certificate Import Wizard**.





CERTIFICATE IMPORT WIZARD

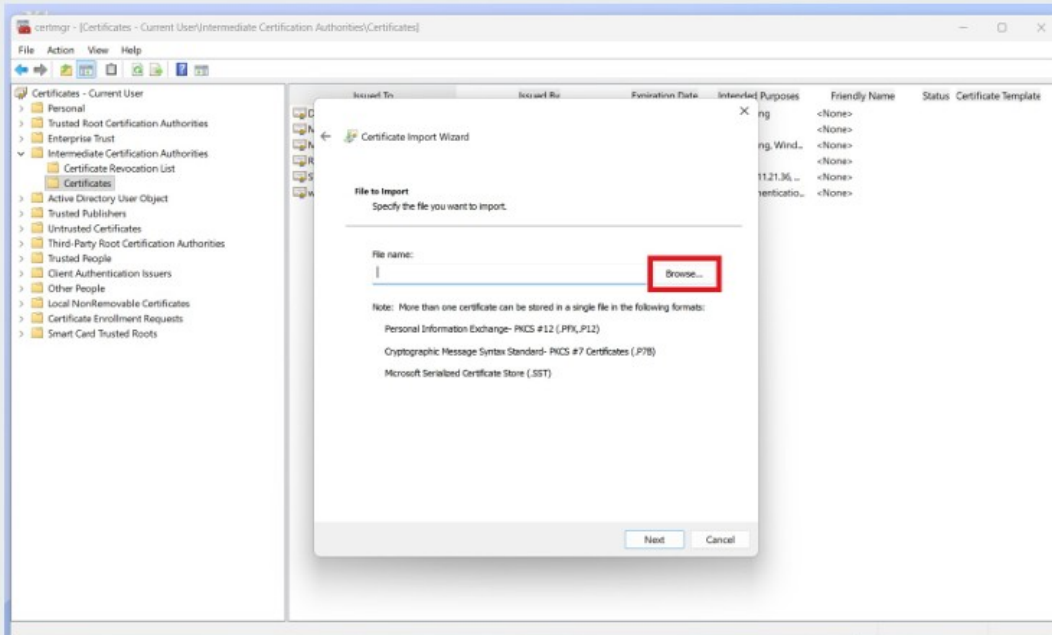
The Certificate Import Wizard will open. Click **Next** to proceed.





LOCATE SUBORDINATE SB2 CA 1 CERTIFICATE FOR IMPORTING

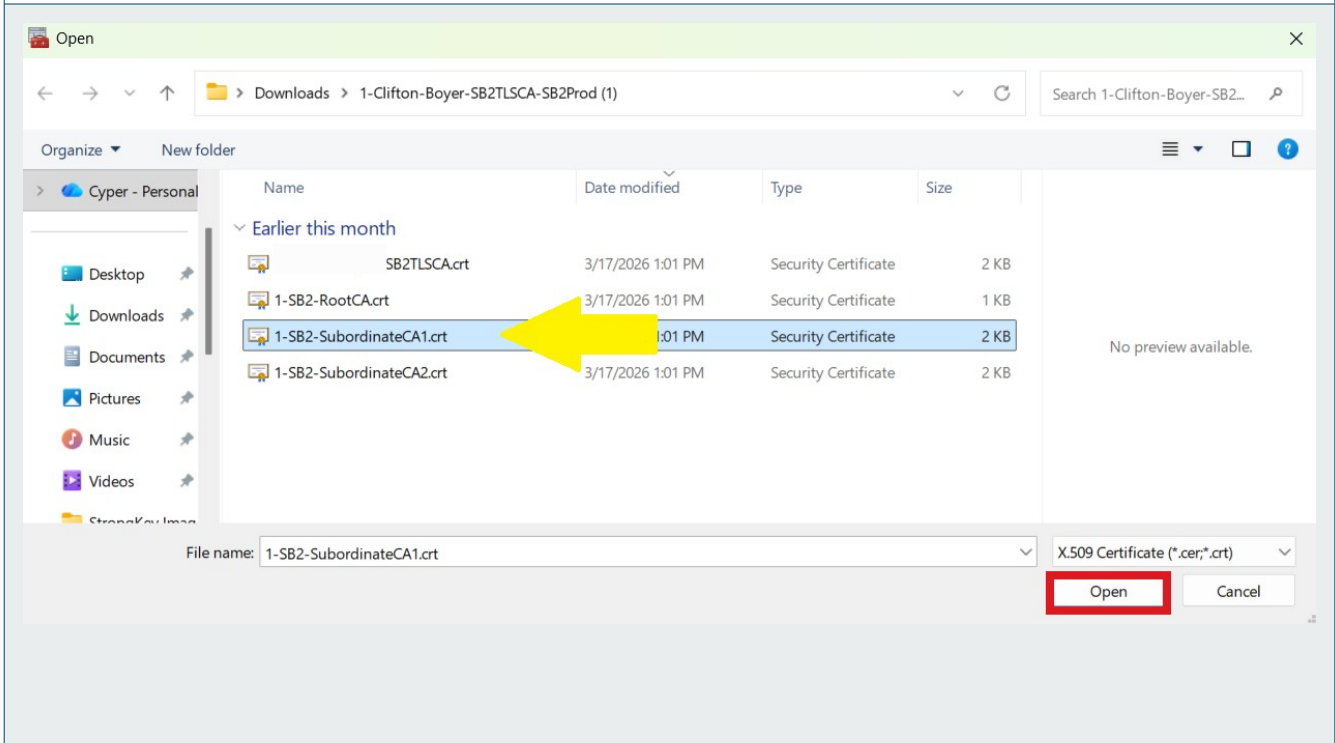
Click the "Browse" button to navigate to and select the Subordinate CA certificate file.





OPEN THE SUBORDINATE SB2PROD CA 1 CERTIFICATE

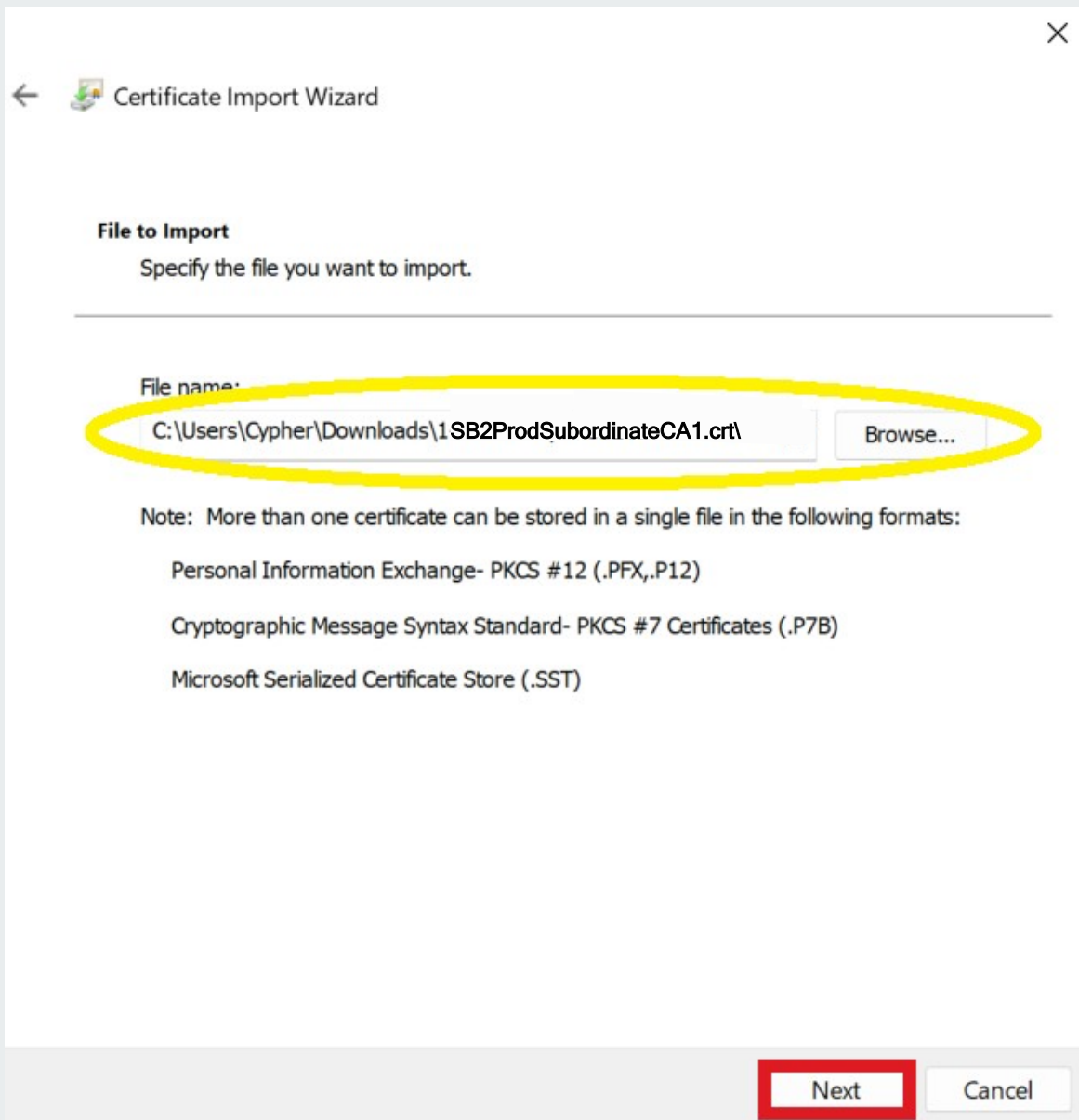
To find the SB2ProdSubordinateCA1.crt certificate file, go to the file's location, which is typically the Downloads folder. Once the SB2ProdSubordinateCA1.crt file (yellow arrow) is located, select it and click Open.



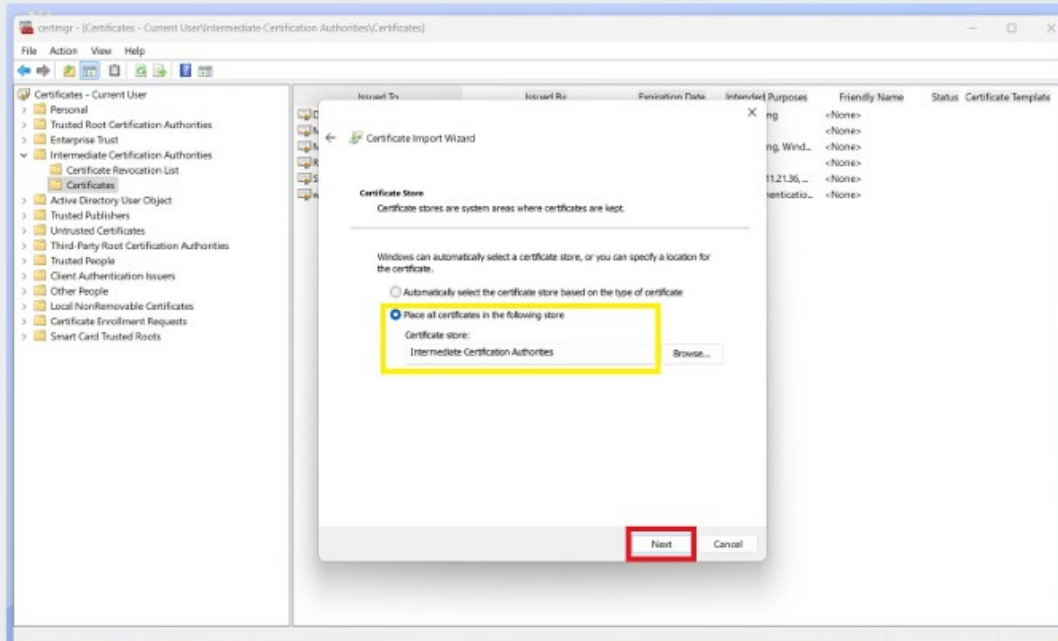


SB2PROD SUBORDINATE CA 1 CERTIFICATE FILE SELECTED

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

A screenshot of the 'Certificate Import Wizard' dialog box. The title bar shows a back arrow, a folder icon, and the text 'Certificate Import Wizard'. The main area is titled 'File to Import' with the instruction 'Specify the file you want to import.' Below this is a 'File name:' label followed by a text input field containing the path 'C:\Users\Cypher\Downloads\1SB2ProdSubordinateCA1.crl'. To the right of the input field is a 'Browse...' button. A yellow oval highlights the input field and the 'Browse...' button. Below the input field is a 'Note' section with the text: 'Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange- PKCS #12 (.PFX,.P12) Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B) Microsoft Serialized Certificate Store (.SST)'. At the bottom right, there are two buttons: 'Next' (highlighted with a red rectangle) and 'Cancel'.

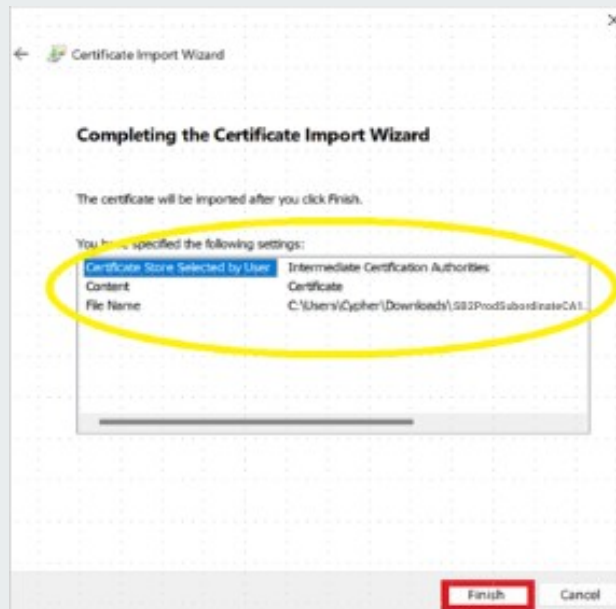
Choose “Place all certificates in the following store” and ensure the certificate is added to the **Intermediate Certification Authorities** certificate store. Click **Next** to continue.





FINISH IMPORTING THE SB2 SUBORDINATE CA 1 CERTIFICATE

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



C27

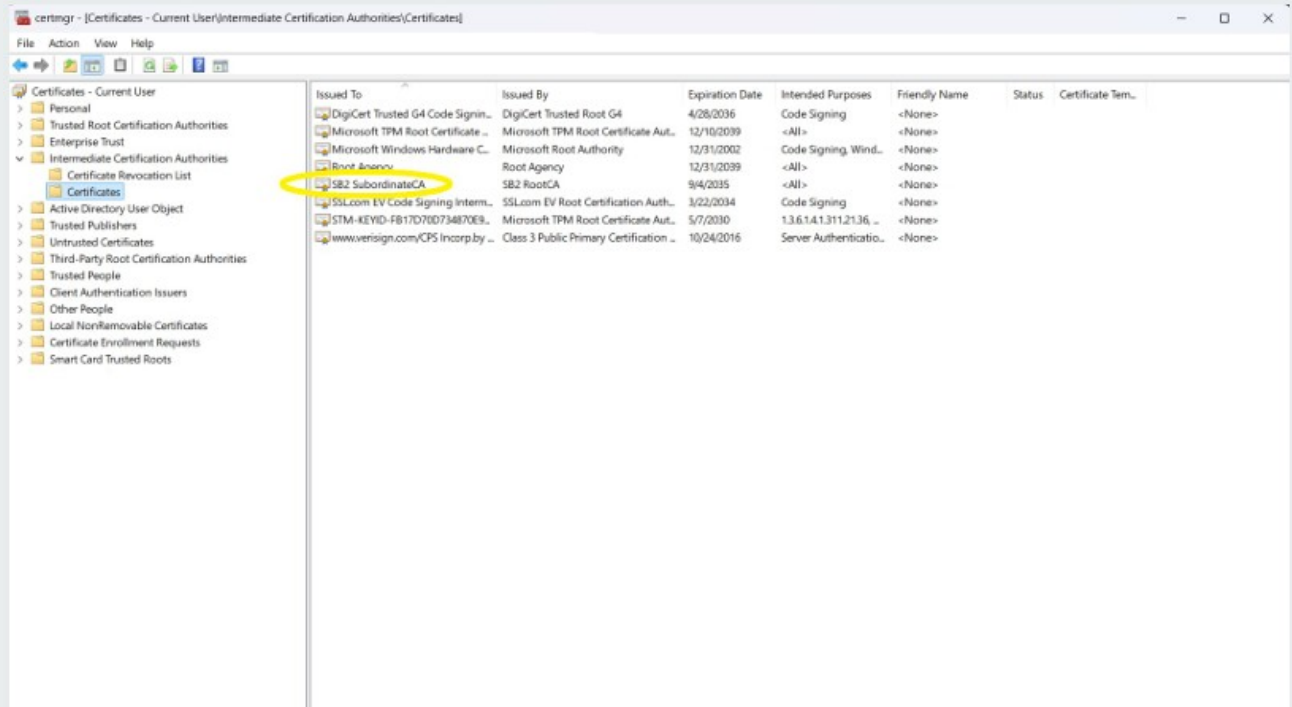
A SUCCESSFUL IMPORT

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

C28

VERIFY SB2 SUBORDINATE CA 1 IN CERTIFICATES LISTS

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



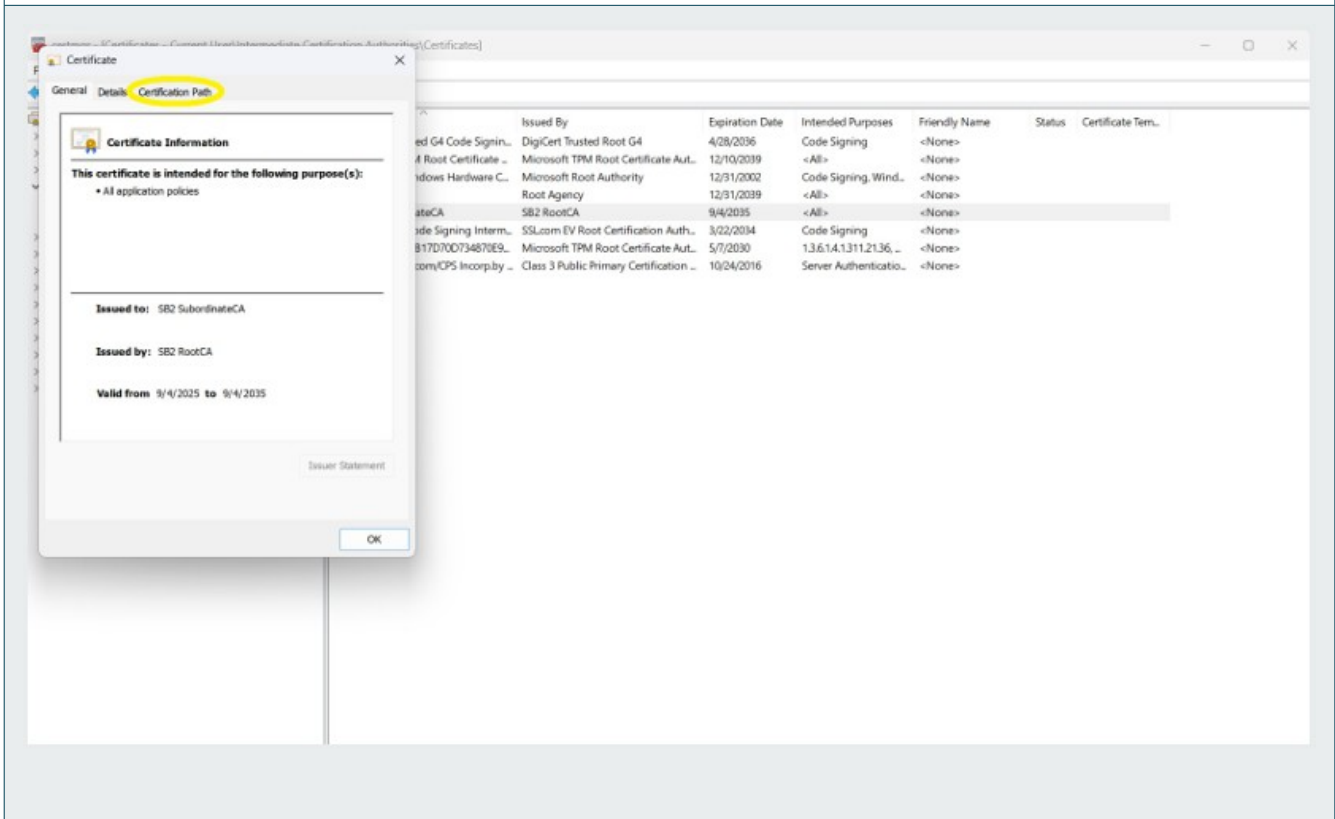
The screenshot shows the Windows Certificates console window titled "certmgr - [Certificates - Current User]Intermediate Certification Authorities(Certificates)". The left pane shows the tree view with "Intermediate Certification Authorities" expanded to "Certificates". The right pane displays a table of certificates. The "SB2 SubordinateCA" entry is highlighted with a yellow circle.

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
DigiCert Trusted G4 Code Signin...	DigiCert Trusted Root G4	4/28/2036	Code Signing	<None>		
Microsoft TPM Root Certificate ...	Microsoft TPM Root Certificate Aut...	12/16/2039	<All>	<None>		
Microsoft Windows Hardware C...	Microsoft Root Authority	12/31/2002	Code Signing, Wind...	<None>		
Root Ass...	Root Agency	12/31/2039	<All>	<None>		
SB2 SubordinateCA	SB2 RootCA	9/4/2035	<All>	<None>		
SSLcom EV Code Signing Intern...	SSLcom EV Root Certification Auth...	3/22/2034	Code Signing	<None>		
STM-KEYID-F817D70D734870E9...	Microsoft TPM Root Certificate Aut...	5/7/2030	1.3.6.1.4.1.311.21.36 ...	<None>		
www.verisign.com/CPS Incorp.by ...	Class 3 Public Primary Certification ...	10/24/2016	Server Authentico...	<None>		



VERIFY SB2 SUBORDINATE CA 1 - PART 1

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

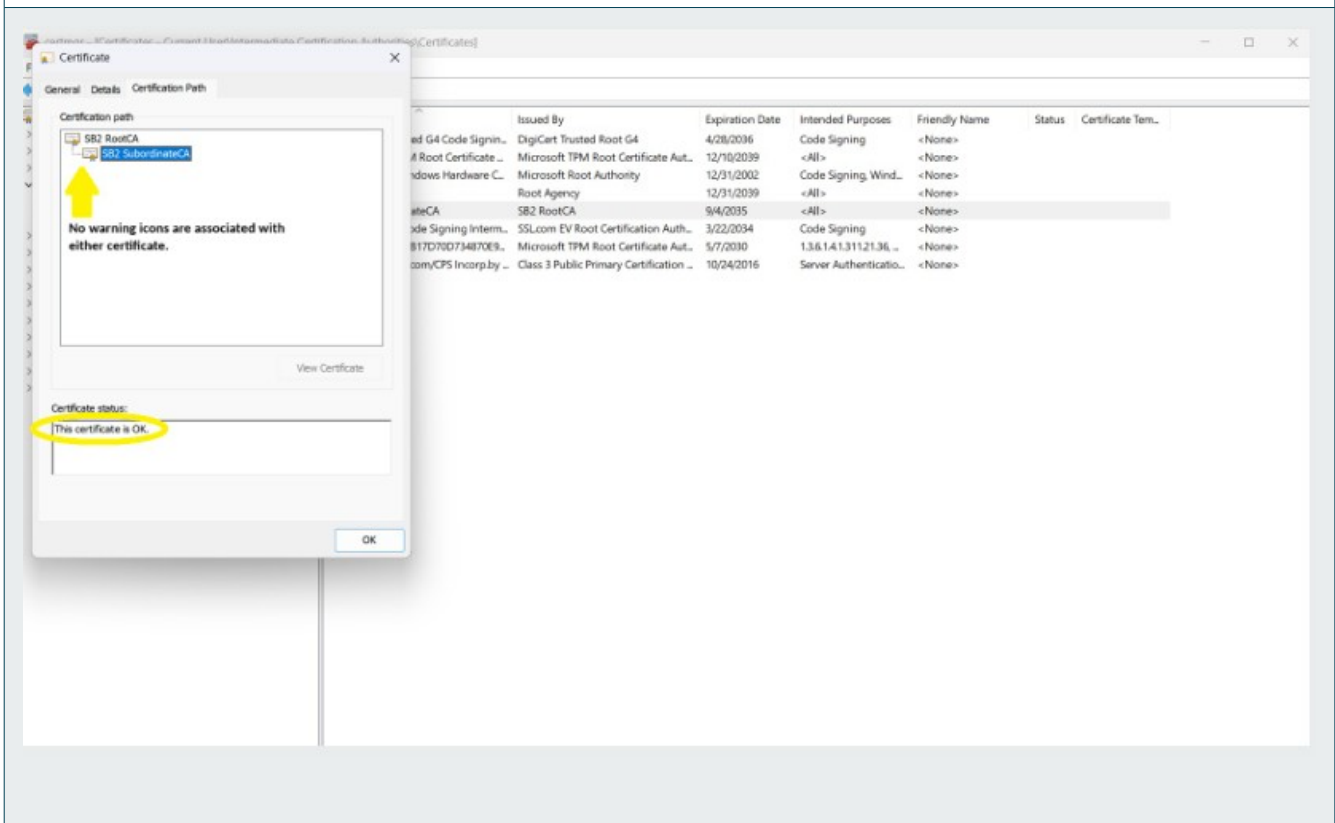




VERIFY SB2 SUBORDINATE CA 1 - PART 2

In the **Certification Path** tab of the **SB2 Subordinate CA** certificate, you should be able to confirm these two important attributes of the certificate:

- That the certificate symbols of the two certificates chained together in the **Certification Path** sub-panel at the top, do not have any yellow warning symbols associated with them, and
- The **Certificate status** sub-panel at the bottom should state that “This certificate is OK.”

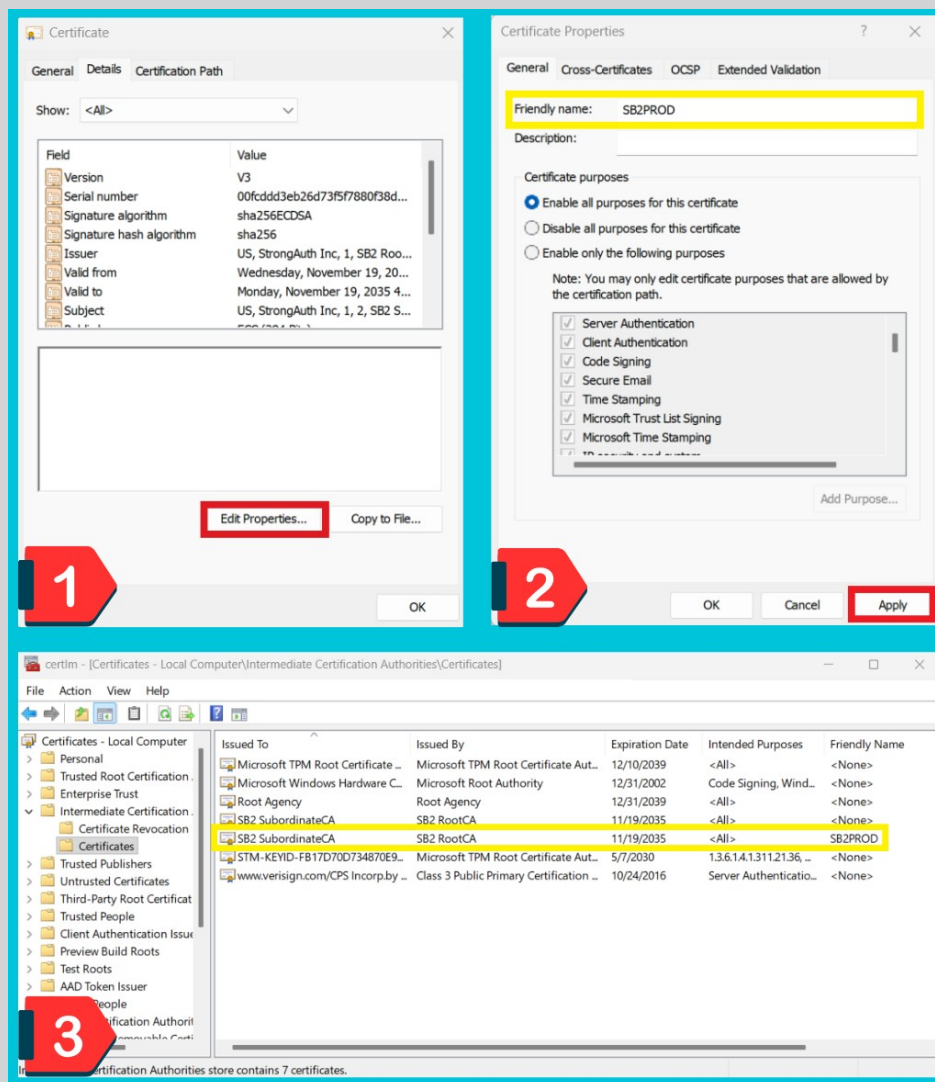


VERIFY SB2 SUBORDINATE CA 1: PART 3

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

1. Choose the Details tab.
2. Click Edit Properties (image 1).
3. Add name in Friendly name field (image 2).
4. Click Apply then Click OK to finish.

Friendly names make identifying SubordinateCAs easier in the certificates list (image 3).



C33

IMPORT THE SB2 SUBORDINATE CA 2 CERTIFICATE

Import the SB2 Sub CA 2 certificate by repeating steps [C20 – C34](#). Remember to verify the Sub CA 2 certificate is selected during the process.

C34

RESTART THE COMPUTER

Save any open files you may have and restart the computer.



SECTION D



STRONGKEY

D1

ACCESSING AN SB2PROD INVITATION LINK

This section will review the steps of accessing the invitation link you received to register a FIDO credential with your Yubikey 5C NFC Security Key with the SB2PROD site.

You must have the Yubikey 5C NFC Security Key – **with Security Key PIN** and the SB2PROD Invitation URL that was sent to you for the FIDO registration process.

D2

PLUG IN THE YUBIKEY 5C NFC SECURITY KEY

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



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.

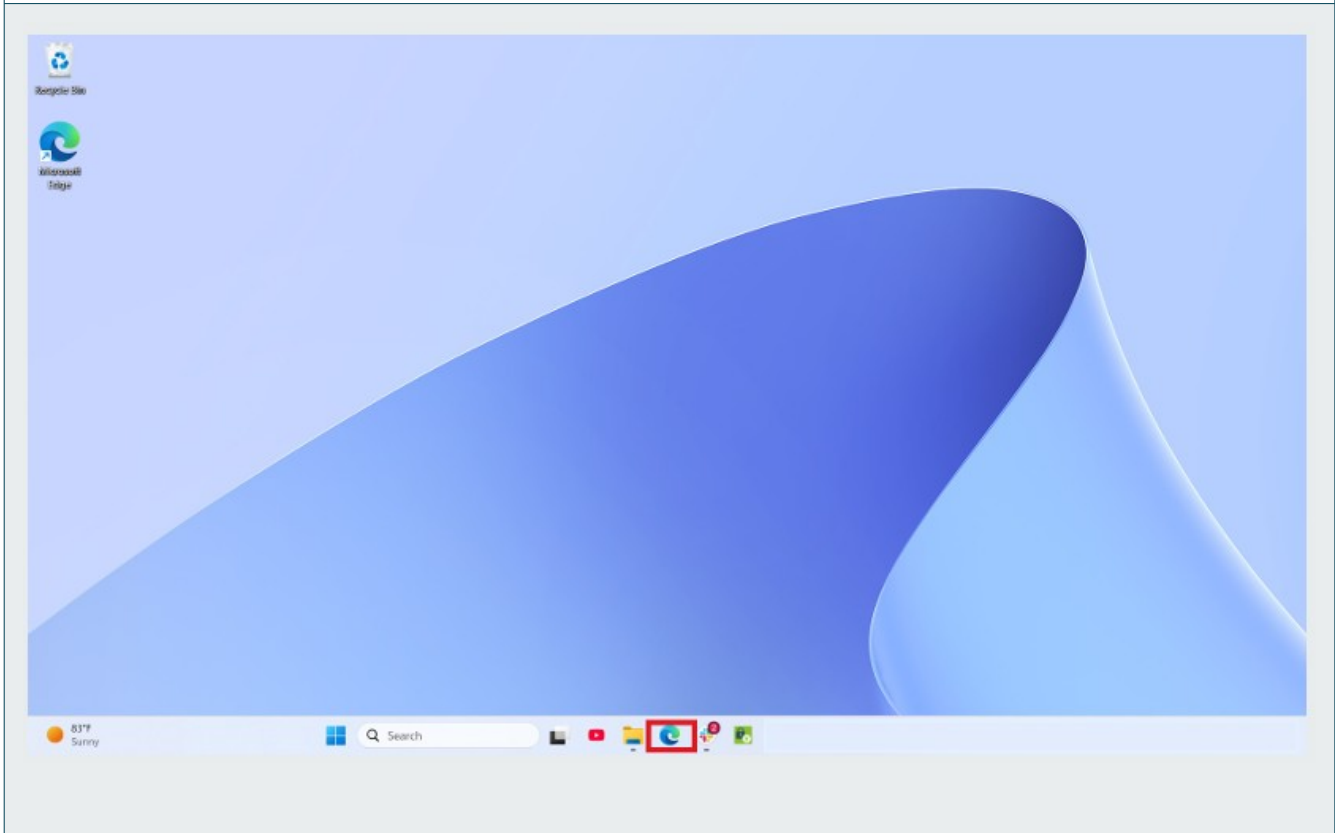
The provided USB adapter pictured below.





OPEN THE EDGE BROWSER

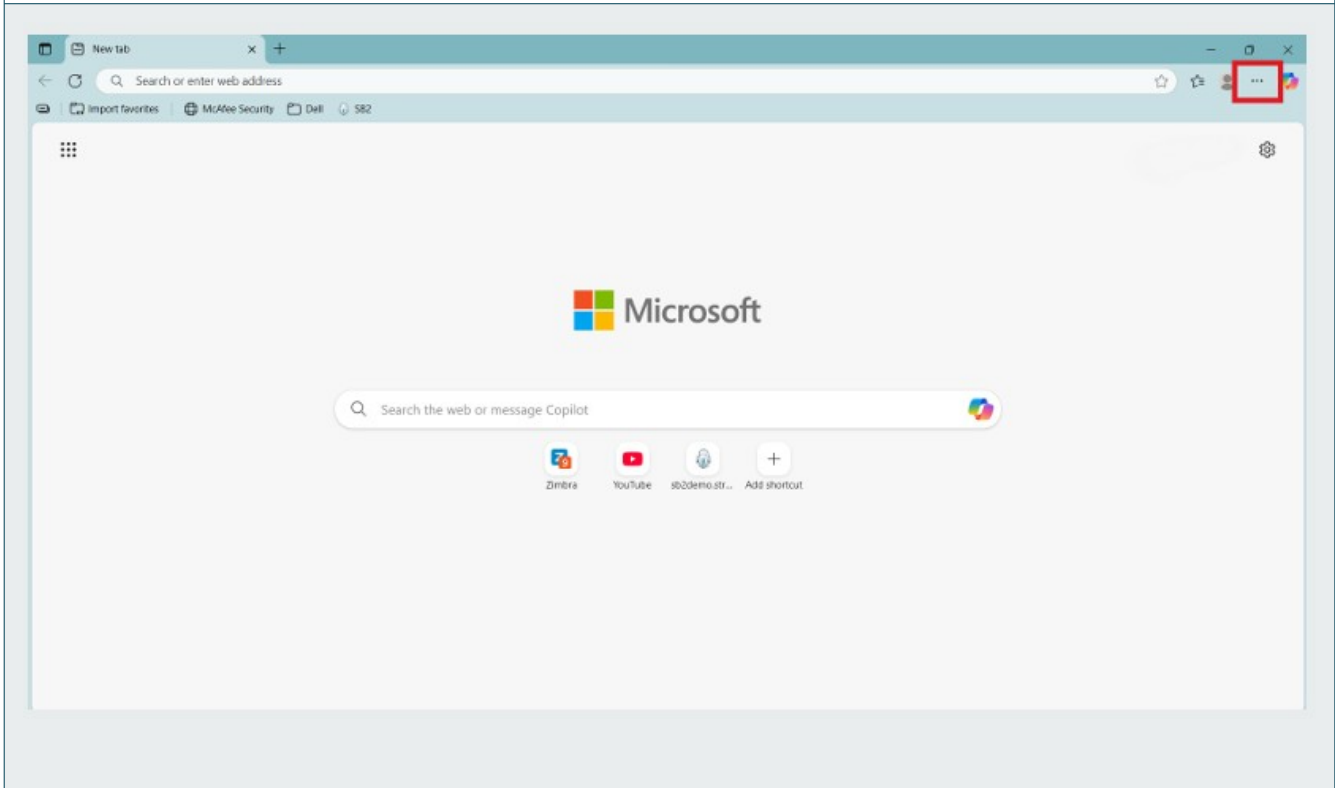
To begin, access the Edge browser by selecting its icon from the Windows taskbar.





FIND THE EDGE BROWSER DROP DOWN MENU

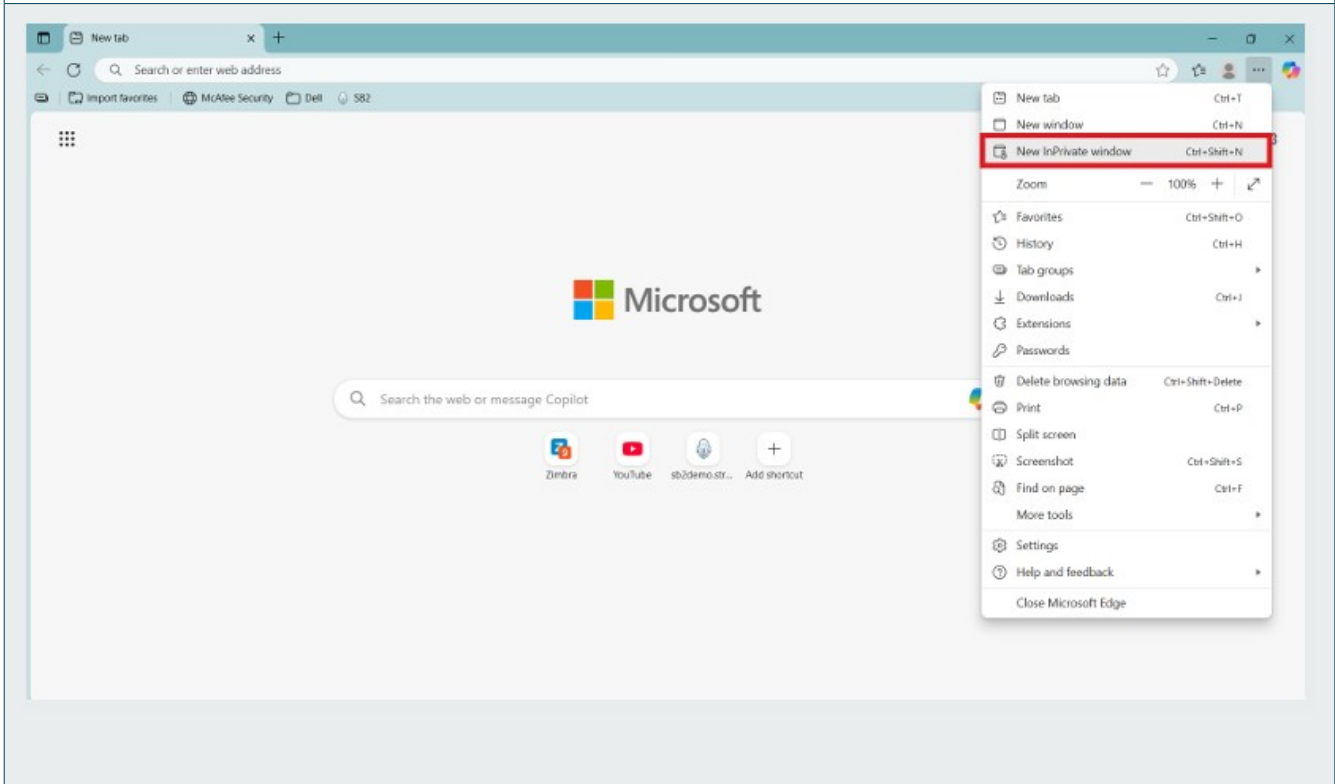
Locate the three-dots icon on the right side of the screen and select it.





OPEN A NEW InPRIVATE WINDOW

Always use Edge InPrivate mode to access the SB2PROD platform URL
<https://sb2.strongkey.com>.



SB2PROD PLATFORM URL

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



NOTE

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

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



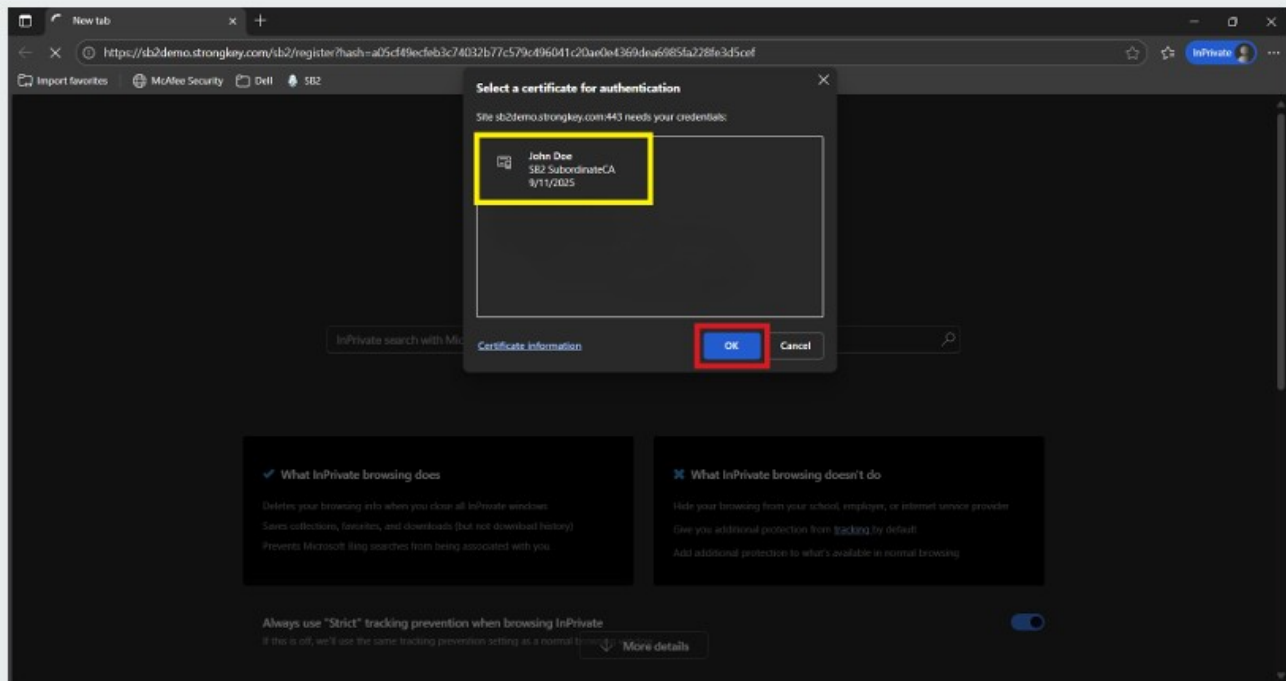
SELECT THE CERTIFICATE

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 such 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 the Administrator of your SB2 PROD site for help.

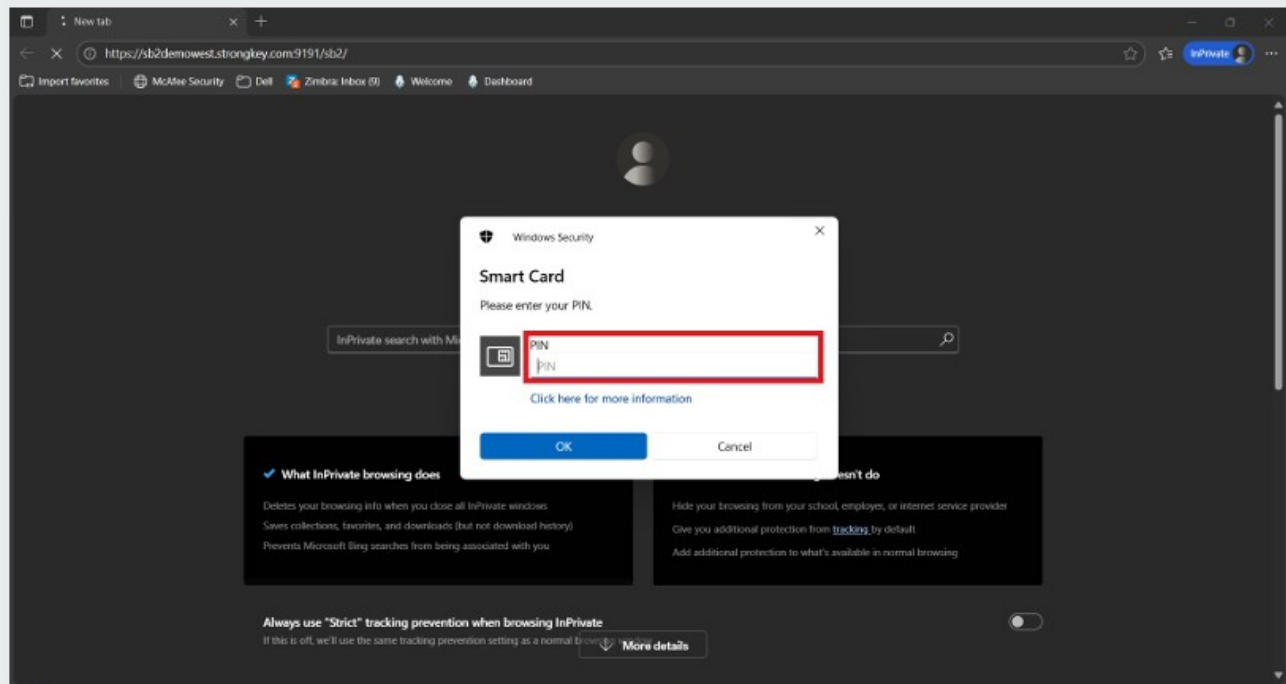




ENTER SECURITY KEY PIN

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

For instructions on changing the iShield Key 2 PIN, refer to the [appendix](#) of this guide.

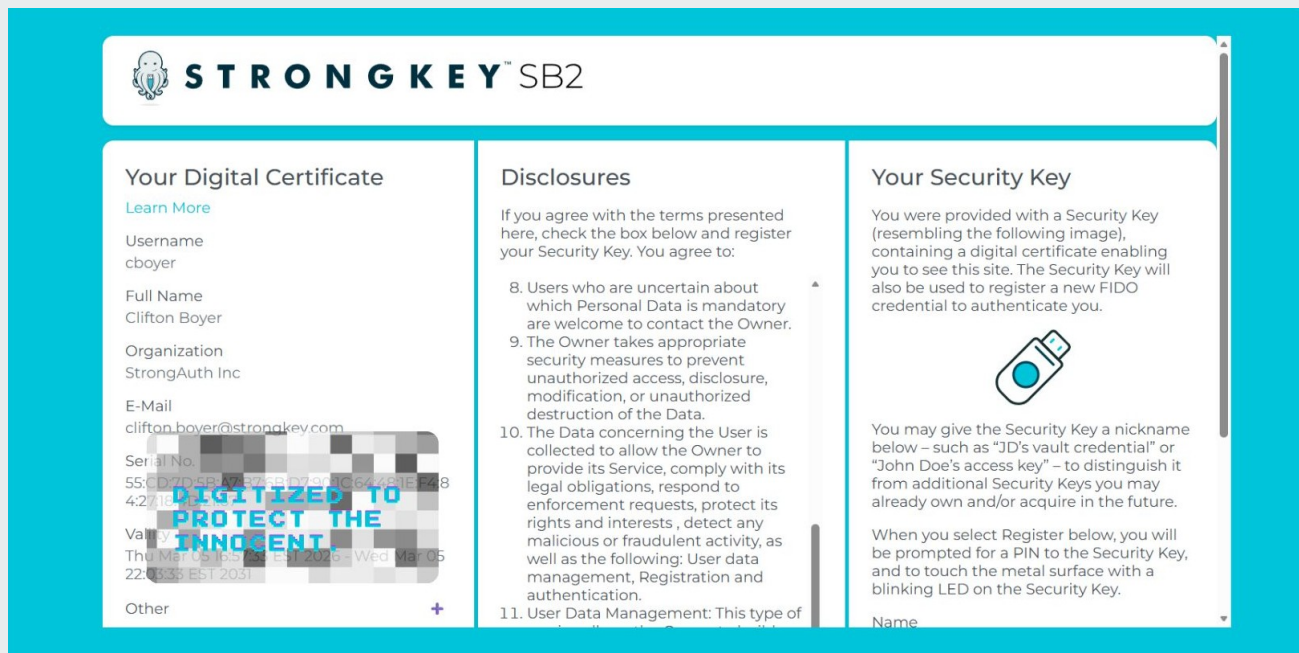




SB2 PLATFORM LANDING PAGE

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.
- 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.



TERMS & CONDITIONS

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



GIVE SECURITY KEY NICKNAME

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

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

Clifton Boyer
Organization
StrongAuth Inc
E-Mail
c
s
5
4
v
t
2
Other +

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 service allows the Owner to build user profiles by starting from an email address, a personal name, or other information that the User provides to this Application
12. Registration and Authentication: By registering or authenticating, Users allow this Application to identify them and give them access to

I agree

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
SB2PROD DOCUMENTATION

Cancel Register

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



ENTER SECURITY KEY PIN

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



NOTE

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

The screenshot displays the registration interface for a Security Key. On the left, user information for Clifton Boyer is shown, including his organization (StrongAuth Inc), email (clifton.boyer@strongkey.com), and a blurred serial number. A central Windows Security dialog box is open, titled "Save your passkey". It shows the email address and a field for the "Security Key PIN", which is highlighted with a yellow circle. A red arrow points to the "OK" button. The background interface includes a "Register" button and a "Cancel" button. At the bottom, there is a copyright notice: "Copyright © 2001-2026 StrongAuth, Inc. (dba StrongKey)".



TOUCH THE SECURITY KEY

To continue adding the credential, touch the metal (brass colored) contact at 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.

The screenshot shows a registration interface for a security key. On the left, user information for Clifton Boyer is displayed. The main area contains a registration form with a 'Register' button. A Windows Security dialog box is overlaid in the center, titled 'Save your passkey'. It shows the email 'clifton.boyer@strongkey.com' and a 'Passkey for strongkey.com'. A red circle highlights the 'Touch your security key.' instruction, with red arrows pointing to the key icon above it. The dialog also includes a 'Change' link and a 'Cancel' button. In the background, a 'Register' button is visible on the right side of the form.



SB2PROD CONFIRMATION

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

Clifton Boyer

Organization
StrongAuth Inc

E-Mail
clifton.boyer@strongkey.com

INTENTIONALLY OBLURRED TO PROTECT THE INNOCENT

Other

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 service allows the Owner to build user profiles by starting from an email address, a personal name, or other information that the User provides to this Application

12. Registration and Authentication: By registering or authenticating, Users allow this Application to identify them and give them access to dedicated services.

I agree

credential to authenticate you.

You will be prompted to select a Security Key a picture of a Security Key in the vault of "Job" - 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

SB2PROD DOCUMENTATION

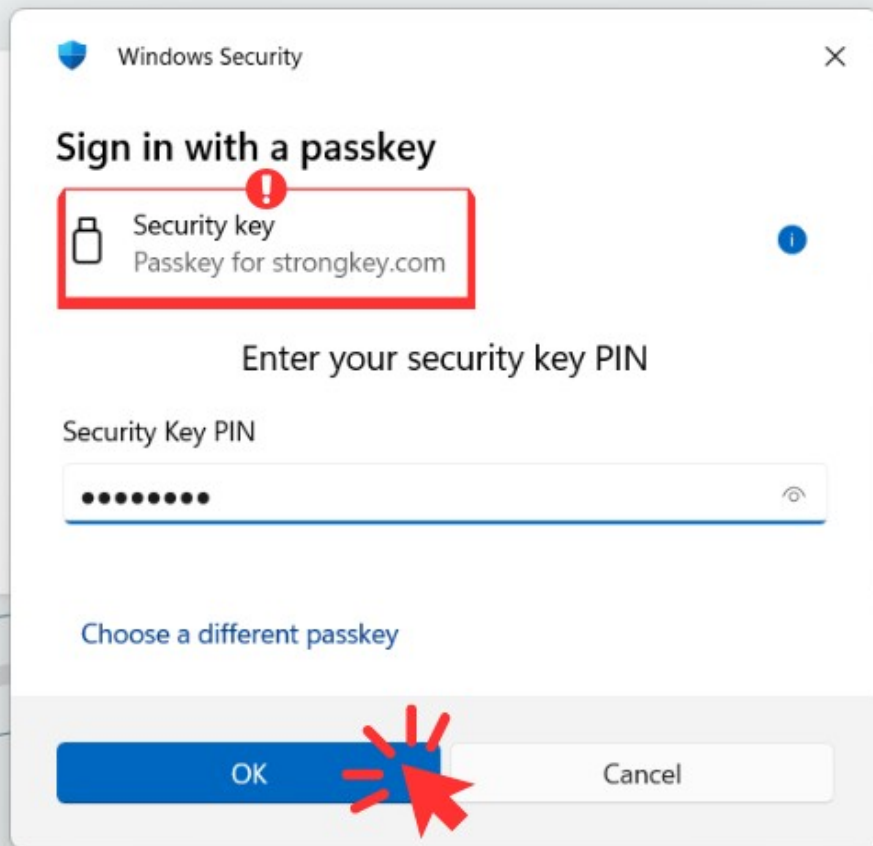
Continue

You've successfully registered
Click 'Continue' to proceed to the login page.

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

D17 SIGNING IN

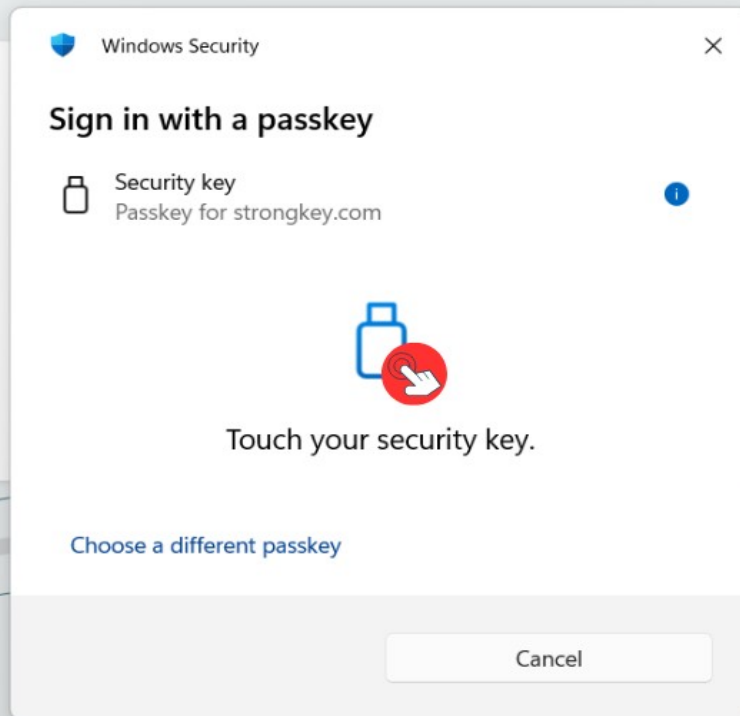
After clicking **Continue**, a prompt will appear prompting you to sign in with the new credential. Verify you are signing in with the Security Key when authenticating to the SB2PROD. Enter your PIN and **Click OK**.





TEST OF USER PRESENCE (TUP)

To continue the login procedure, touch the metal (brass colored) contact at the 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.





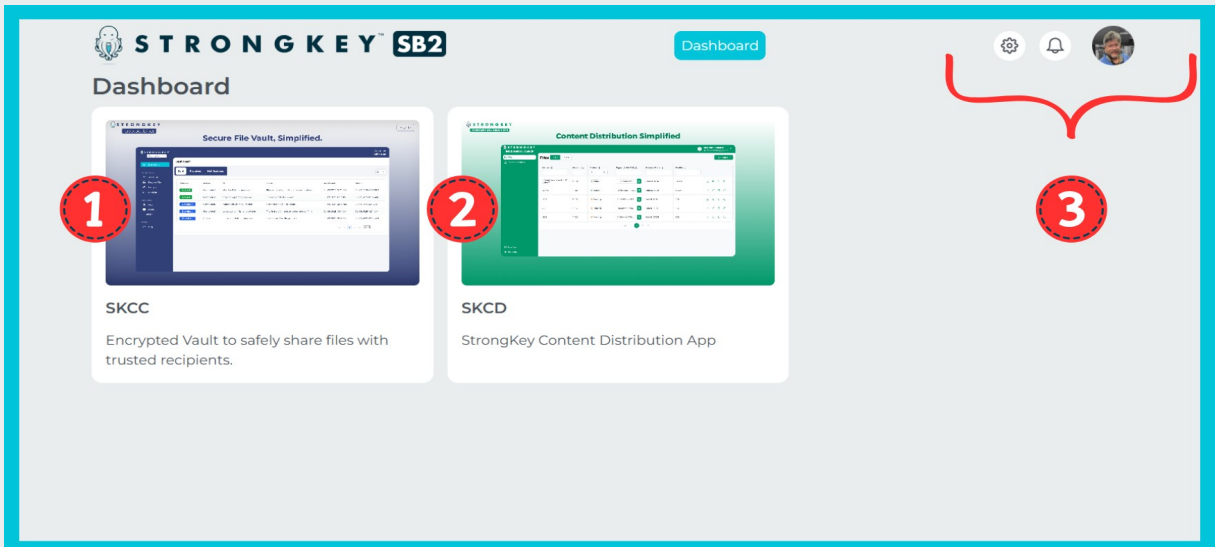
THE SB2PROD PLATFORM DASHBOARD

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

All SB2 users have access to two primary applications and:

1. **StrongKey CryptoCabinet (SKCC):** For securely storing and sharing encrypted files containing sensitive data.
2. **StrongKey Content Distribution (SKCD):** For storing and sharing digitally signed, unencrypted documents.
3. Settings, Notifications and profile picture.

Clicking either image on the SB2 Dashboard opens the application in a new browser tab. Detailed user guides for both SKCC and SKCD are available separately.



WELL DONE!

APPENDIX



STRONGKEY

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



COPYRIGHTS AND 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.



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.

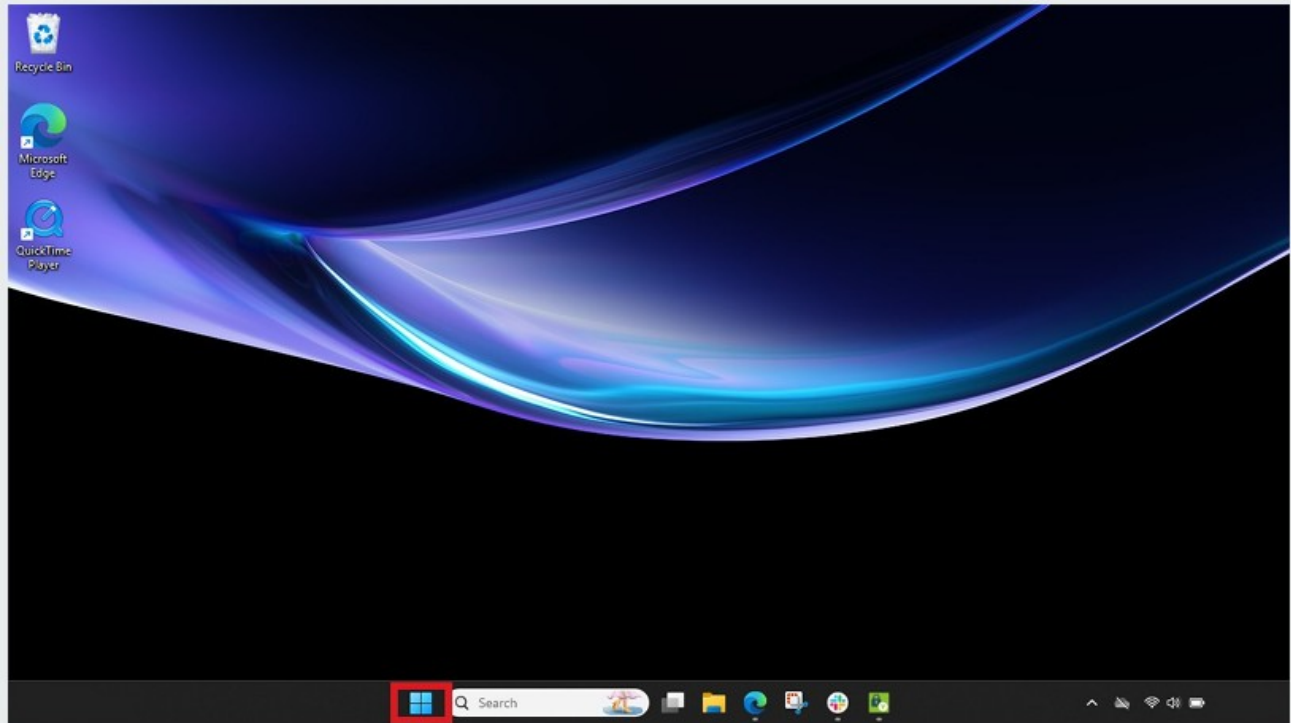
However, StrongKey recommends using the SAME PIN to both containers of the **Security Key** to reduce the burden on users. As long as the **Security Key** is safely in the possession of the legitimate user, and the legitimate user is NOT sharing the PIN to the **Security Key** with anyone, the user will 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, access the iShield Key Manager application by selecting the **Windows start icon** from the Windows taskbar.



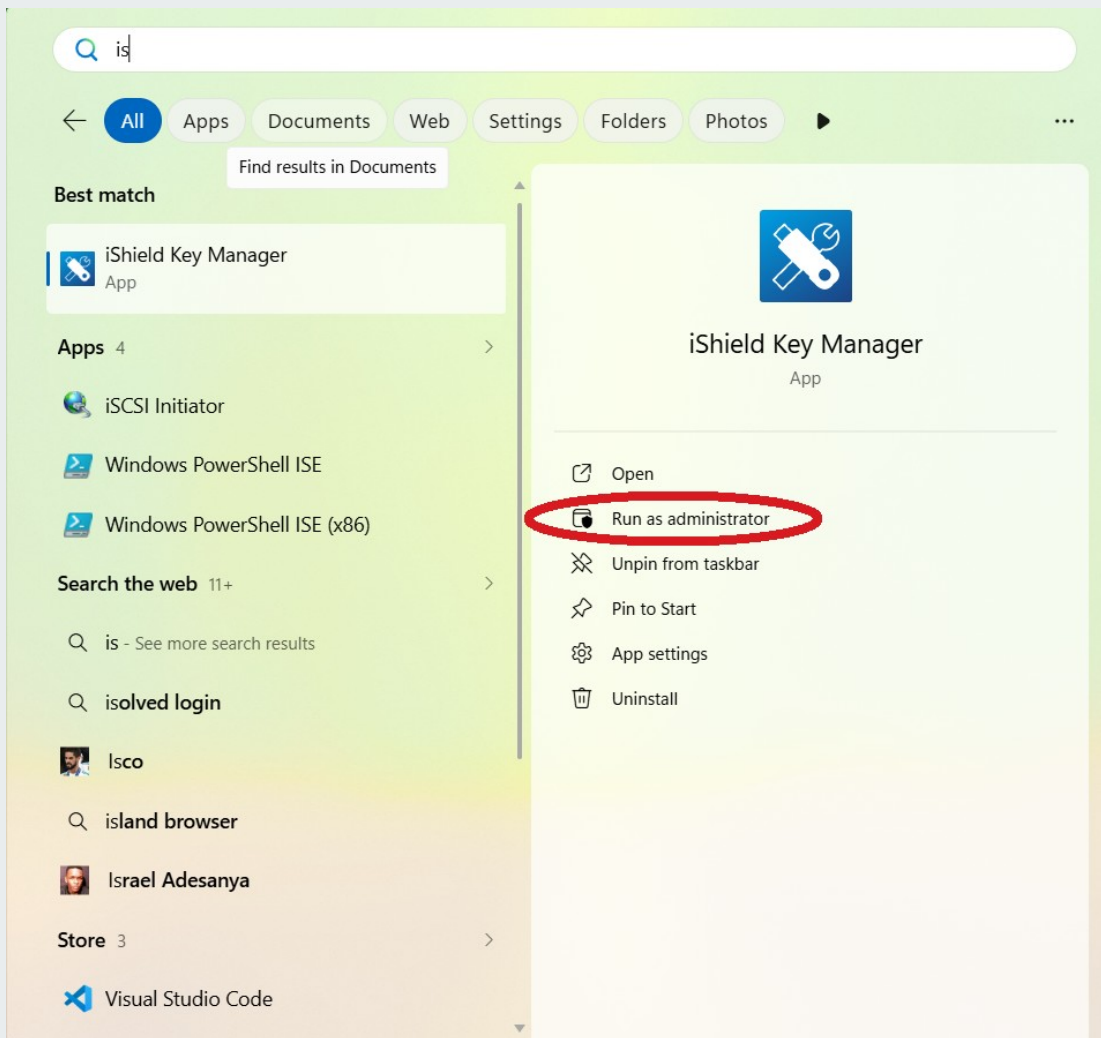
SELECT iSHIELD KEY MANAGER

Search for the iShield Key Manager application. Click **Run as administrator**.



NOTE

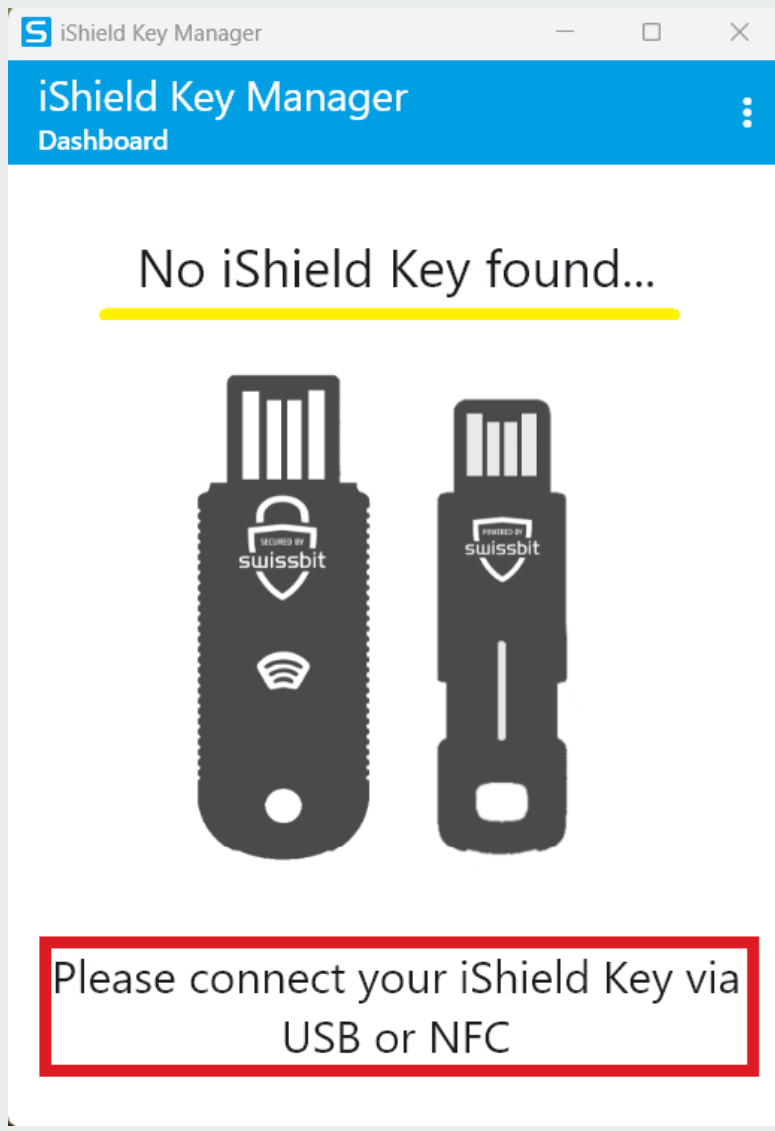
To change your iShield Key's FIDO2 PIN in Windows, you must run the iShield Key Manager as an administrator. Windows requires these elevated permissions to access specific security key settings. If you do not run the app as an administrator, the **Change PIN** settings for the FIDO2 container will remain **inaccessible**.





THE iSHIELD KEY MANAGER APPLICATION

Upon opening, the application displays the screen shown below and indicates **No iShield Key Found.**



AP5

INSERT THE iSHIELD KEY 2 PRO

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

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.



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.





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 shows the iShield Key Manager application interface. The top bar is blue with the text "iShield Key Manager" and "Dashboard". Below this, there are several sections:

- Serial Number:** 602782540039
- Firmware:** v1.1.2
- Passcode:** HOTPs, TOTPs and Passwords. Includes a "Please select a slot" dropdown, a "Code" field with a mask, and a "Version" field showing v3.6.0. A "Details & Settings >" button is at the bottom.
- PIV (Personal Identity Verification):** X.509 Certificates. Installed: 1 / 25. Includes a "Browse >" button and a "Version" field showing OpenFIPS201 v1.4. A "Details & Settings >" button is at the bottom.

A large red arrow points from the "Browse >" button in the PIV section down to the "Details & Settings >" button at the bottom of the PIV section.

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).

The screenshot shows the iShield Key Manager application interface. At the top, the title bar reads "iShield Key Manager" and the subtitle is "PIV: Details & Settings". Below the title bar, there is a navigation menu with a back arrow and a settings icon. The main content area displays the following information:

- Installed: 1 / 25
- Version: OpenFIPS201 v1.4.1
- Cardholder Unique Identifier: 533b3019d4e739da739ced39ce739d8360d821084210842108421087f3341030d64367b2d1df959cbcb6a5f5
- Card Capability Container: 5333f015a00000011604028137caf34d3af6798f8fac30c8a1f10121f20121f300f40100f50110f600f700fa00fb0
- Secure Messaging Card Verifiable Certificate: <Empty>
- Pairing Code:

At the bottom of the screen, there is a list of settings with corresponding buttons:

- PIN: **Change PIN** (highlighted with a red box), Unblock PIN
- PUK: Set PUK
- Management Key: Set Key
- PIN Protected Mode: Activate
- PIN / PUK Reset: Configure Retries
- Reset: Reset

AP10

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

AP11

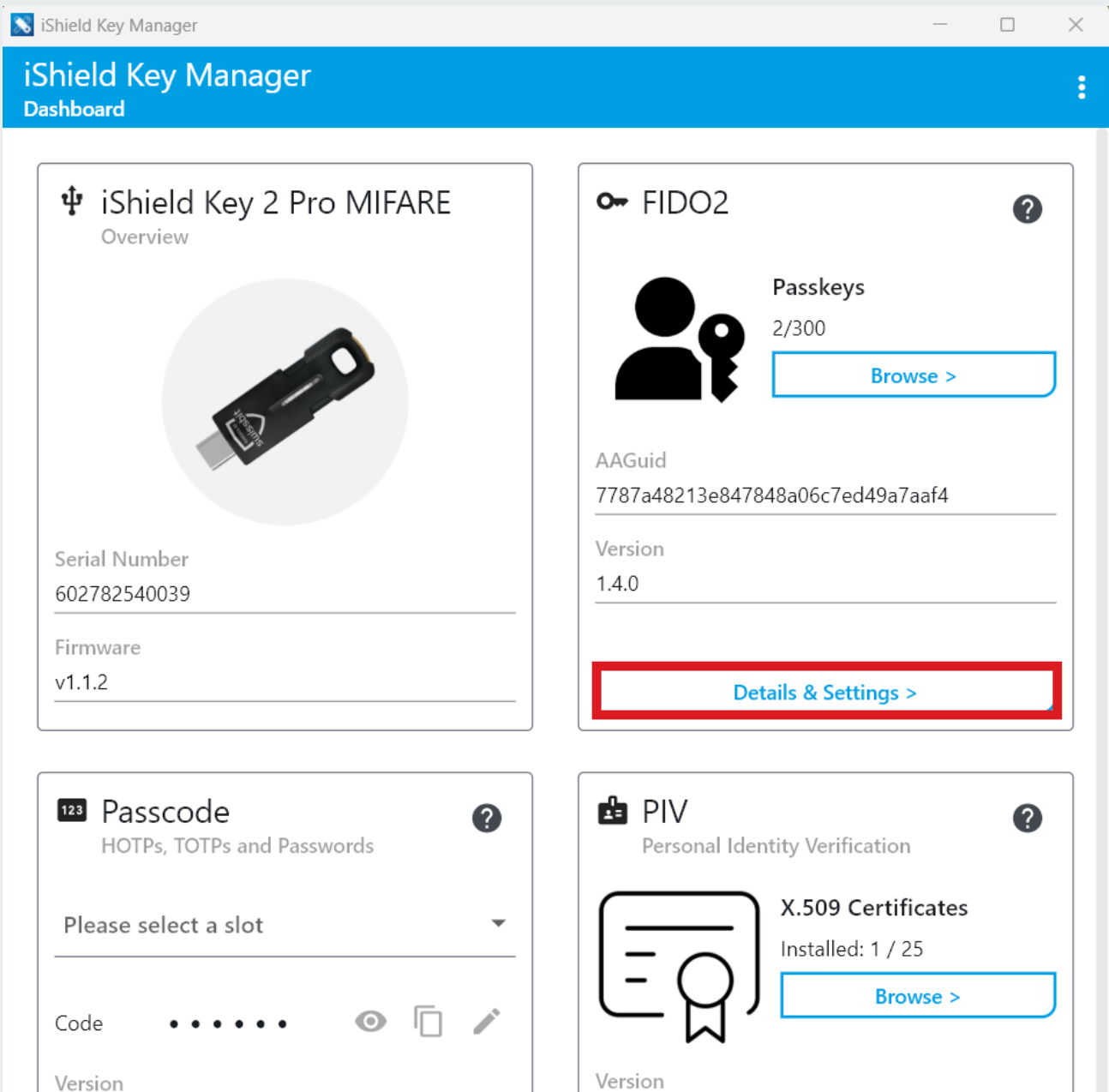
SUCCESS!

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.

AP12

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](#)).






CHANGE PIN

Click Change PIN.

 **iShield Key Manager** 
FIDO2: Details & Settings

 **Passkeys**
2/300

AAGuid
7787a48213e847848a06c7ed49a7aaf4

Version
1.4.0

Supported protocols
U2F, FIDO 2.0, FIDO 2.1

PIN

Reset

AP14 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

Force PIN Change

2

3



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.

