



Panini VisionE Certificate Importation

May 2023

This guide is provided for the convenience of BankUnited Remote Deposit Capture customers utilizing the Panini VisionE scanner. The document was prepared by Fiserv and contains instructions relating to the installation of security certificates and configuration of third-party hardware and software. Information is subject to change by the applicable provider.

Contents

- Introduction..... 3
 - Importing the security certificate..... 3
- Windows..... 3
- Windows: Firefox 7
- Apple/Mac..... 9
- Apple/Mac: Firefox..... 12

This document has been created by Fiserv and is classified FISERV-CONFIDENTIAL. This document is restricted to the received party and not to be forwarded or transferred without the approval of Fiserv.

© 2023 Fiserv Inc. or its affiliates. All rights reserved.

This material is proprietary to and published by Fiserv, Inc. for the sole benefit of its clients. Reproduction, distribution, disclosure and use are expressly prohibited, except as authorized by license, or with the explicit written approval of Fiserv, Inc. The information contained herein is subject to change without notice. In no event will Fiserv be responsible for any direct, indirect, special or consequential damages resulting from the use of this information. No warranties, either express or implied, are granted or extended by this document. Great care should be taken to ensure than any use of this information complies at all times with all applicable laws, rules and regulations.

Introduction

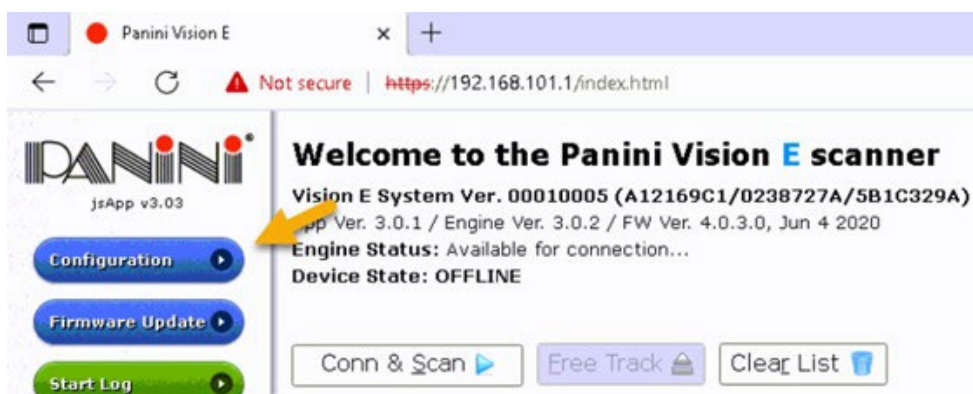
This document describes the process of importing the security certificate from the Panini VisionE manually.

Importing the security certificate

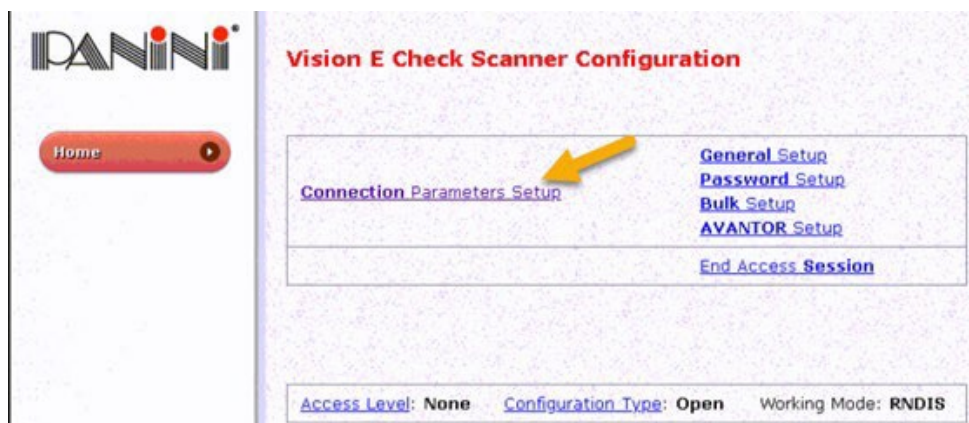
For Windows, you can automatically import the certificate by running the installation package for the VisionE (Fiserv_Panini_VisionE_3.25.2.exe).

Windows

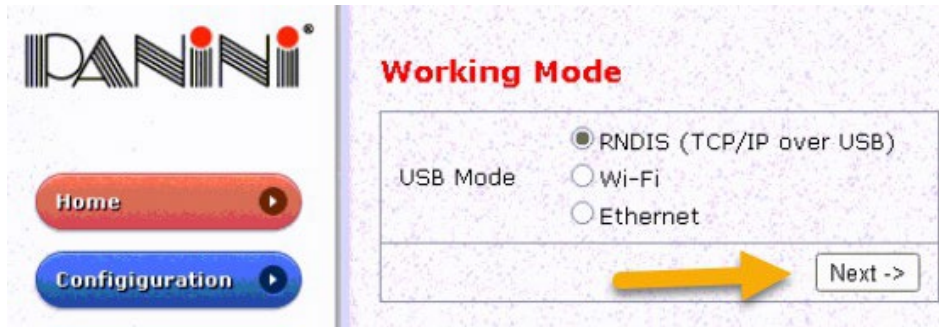
1. Open the browser and navigate to the scanner 192.168.101.1, 192.168.102.1, or 192.168.103.1.
2. Click on **Configuration** option in the upper left corner.



3. Click the **Connection Parameters Setup** link.



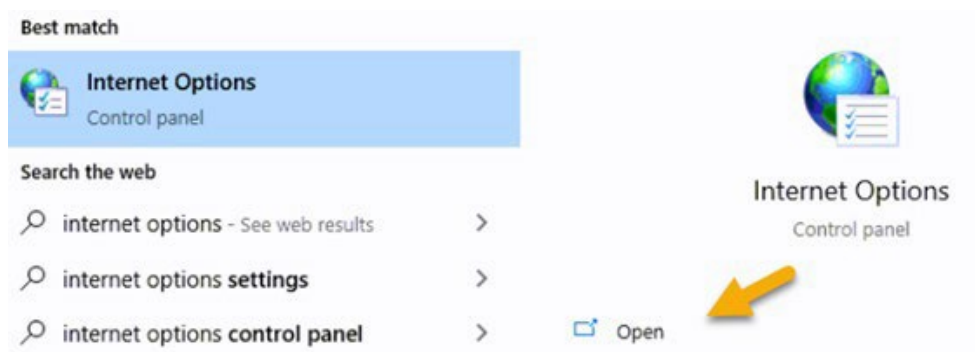
4. Click **Next**.



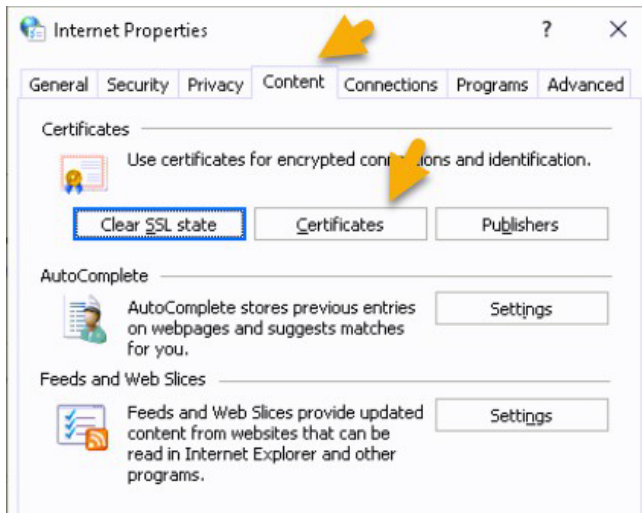
5. Scroll to the bottom of the next page and click the **Root CA Certificate Download (PEM Format)** link.



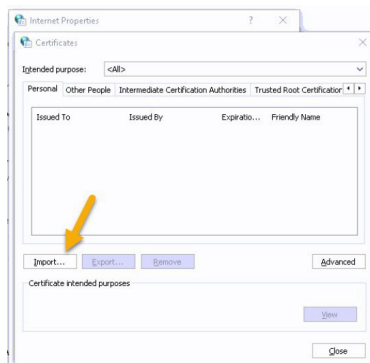
6. Once the certificate file has been downloaded, open the **Start** menu, search for the Internet Options, and then click **Open**.



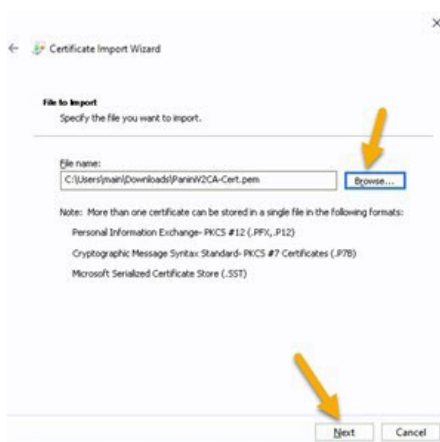
7. Once the **Internet Properties** window opens, click on the **Content** tab, and then **Certificates**.



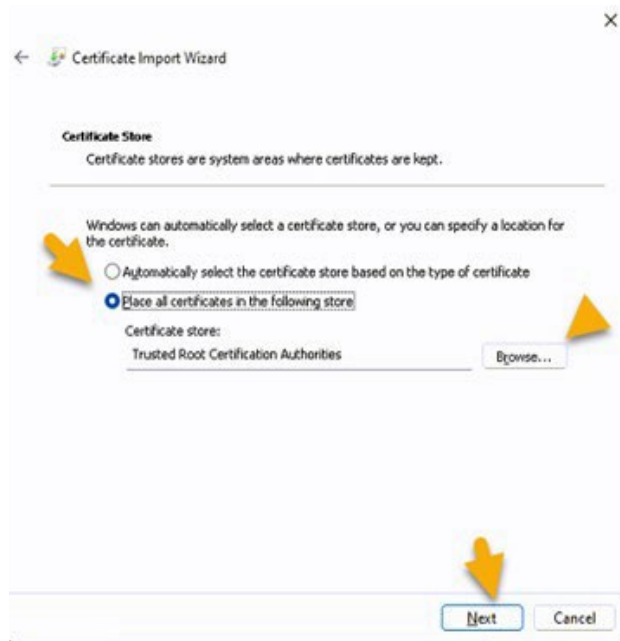
8. Click **Import**.



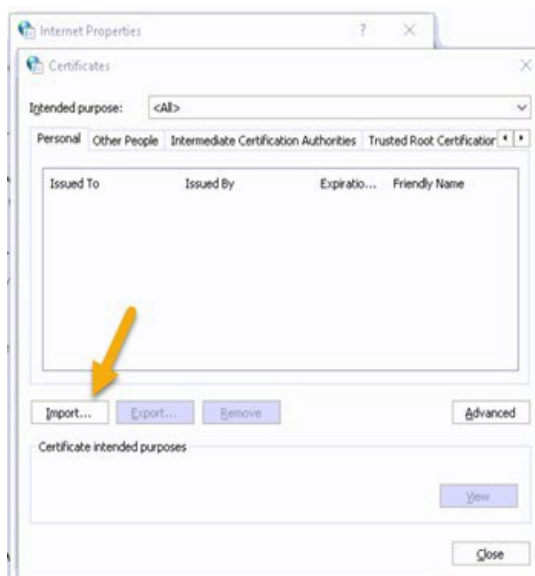
9. Once the new window opens, click **Next**, on the next page click on **Browse**, and go to the folder where the certificate file was saved (normally in the downloads folder by default).



10. Once you select the certificate file and click **Next**, the Certificate Store page displays.
 - a. Click the **Place all certificates in the following store** radio button and then click **Browse**.



- b. Select the **Trusted Root Certification Authorities** option and click **OK**. Once that has been selected and back to the Certificate Import Wizard, click Next.

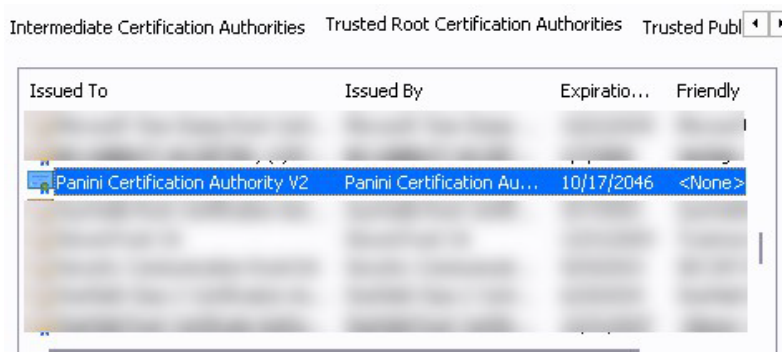


11. Once you import it successfully, a message displays accordingly.

12. To verify that it has been imported, close and re-open the Certificate store, go to the **Trusted Root Certification Authorities** tab, and scroll down to the “P” area of the **Issue To** column.

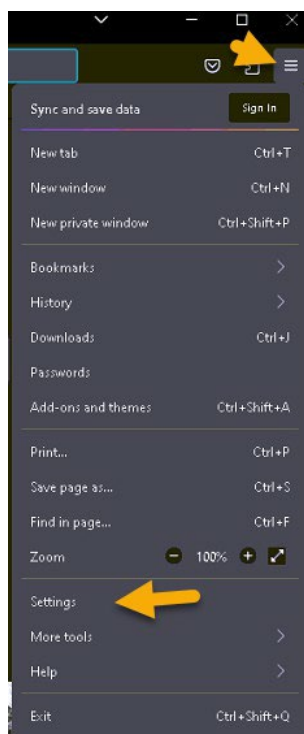
You will find a Panini Certification Authority entry there.

Example –

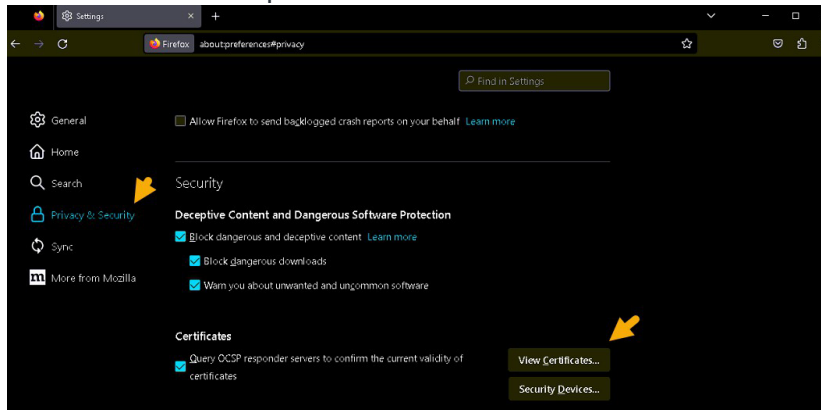


Windows: Firefox

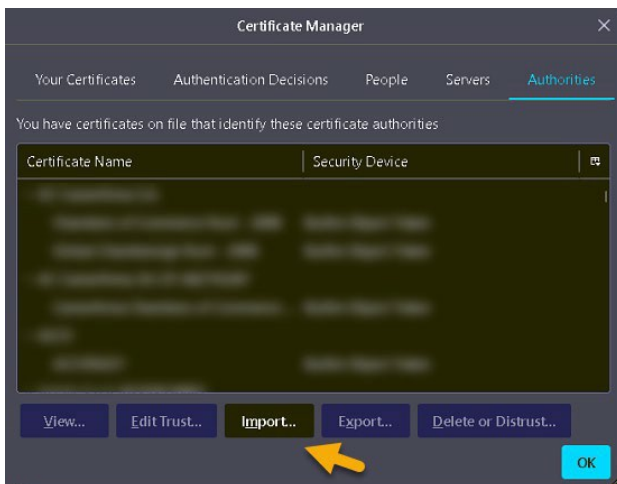
1. To get the certificate, follow the same process as mentioned in the above steps.
2. Once the certificate has been downloaded from the scanner, open Firefox, go to the menu in the upper right corner and then click **Settings**.



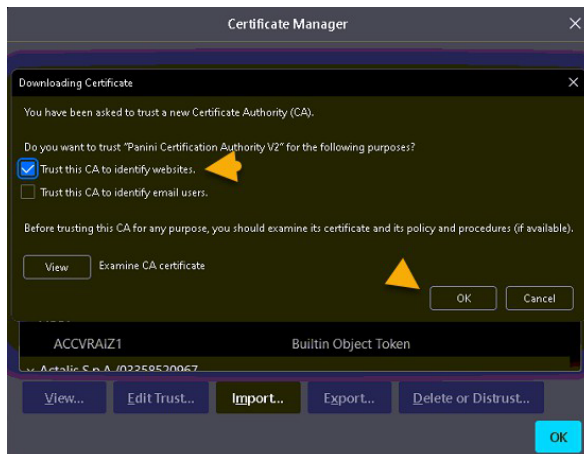
3. In the **Settings** menu, click **Privacy & Security**, scroll down, and then click on the **View Certificates** option.



4. Once the **Certificate Manager** opens, click on the **Authorities** tab, then click **Import**



5. Once the new window opens, navigate to where the certificate file was saved.
 - a. Select the file and click **Open**.
 - b. On the next screen titled **Downloading Certificate**, check the **Trust this CA to identify websites** box as that allows the certificate to work with with SCO, and then click **OK**.

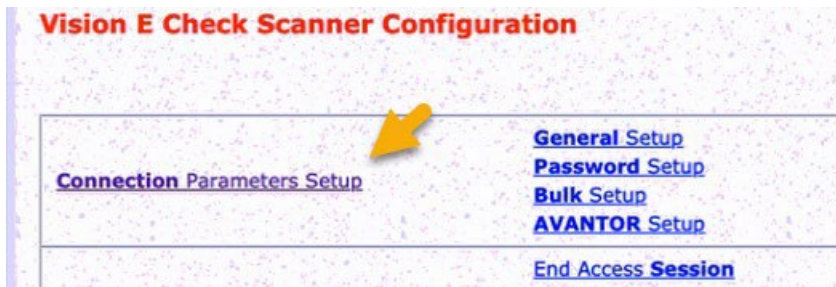


Apple/Mac

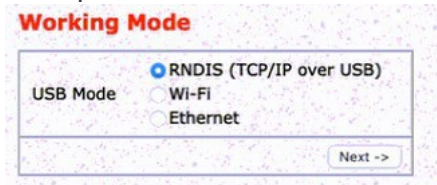
1. Connect the scanner and navigate to it in the browser using 192.168.101.1. Once connected, click **Configuration** in the upper left corner.



2. Click the **Connection Parameters Setup** link.



3. Select the **RNDIS (TCP/IP over USB)** connection method that is being used for this example, and then click **Next**.

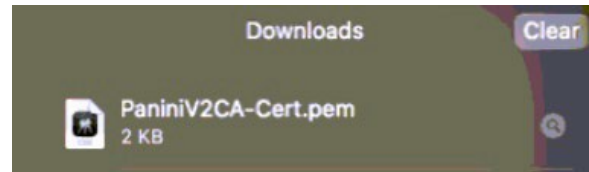
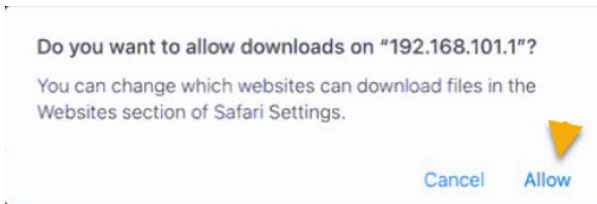


4. On the **Connection Parameters** screen, scroll to the bottom to the **HTTPS** section. Keep it as **Default certificate**, and then click on the **Root CA Certificate Download (PEM Format)** link.



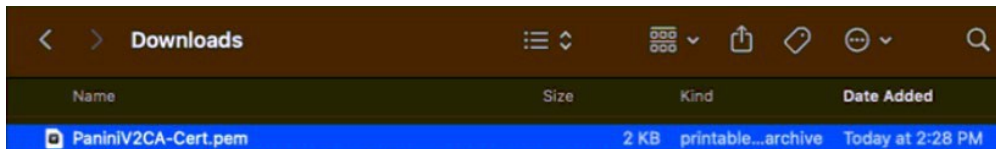
5. In a **Do you want to allow downloads from the scanner address** prompt, click **Allow**.

This downloads the certificate.



6. Open a Finder window and navigate to where the certificate was stored. In this example, it is in the Downloads folder.

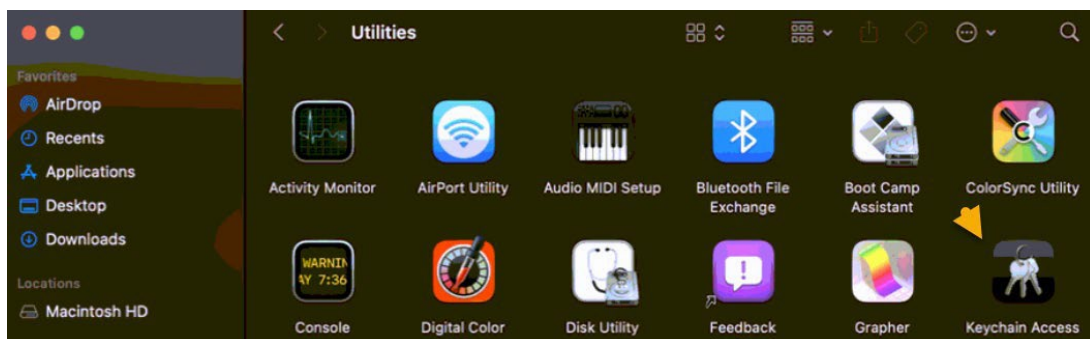
Search the file named **PaniniV2CA-Cert.pem**.



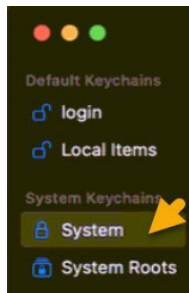
7. Double-click on the file to start the import process.

When prompted, enter the Mac password to allow it to be imported into the Keychain.

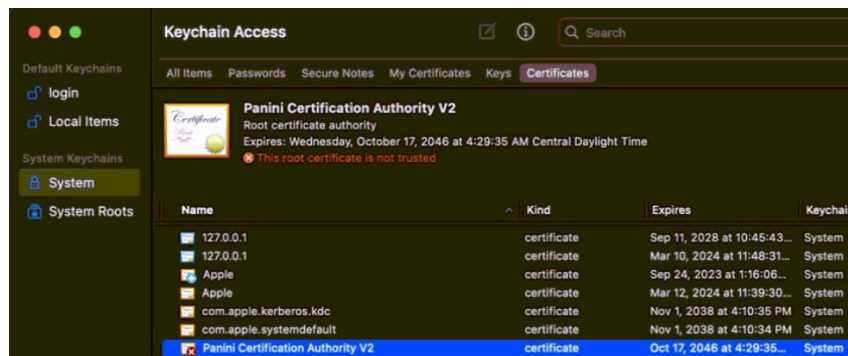
8. Go to **Applications -> Utilities**, and open **Keychain Access**.



9. Once Keychain Access has been opened, navigate to the **System** option under **System Keychains** (both on the left side).

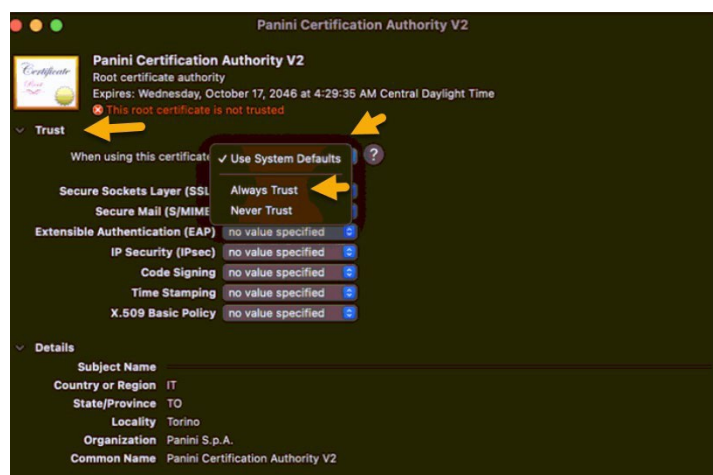


10. In the main area in that section, click the **Certificates** tab. You will find the **Panini Certification Authority V2** there that you import



11. Double-click or right-click on the **Panini Certification Authority V2** and open the certificate. Expand the pre-collapsed **Trust** section at the top.

At the top of that section, change the **When using this certificate** section from **Use System Defaults** to **Always Trust**.

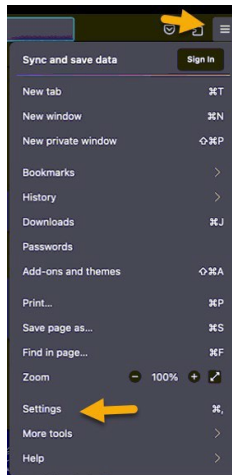


12. Close the window where you will be prompted to enter the Mac password again. This is to allow the change and to save it.
13. Enter the system password and click **Update Settings**.

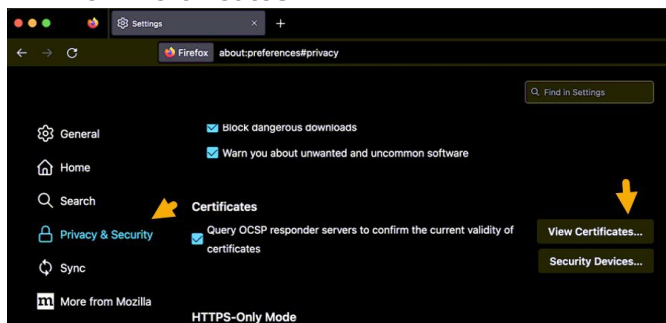


Apple/Mac: Firefox

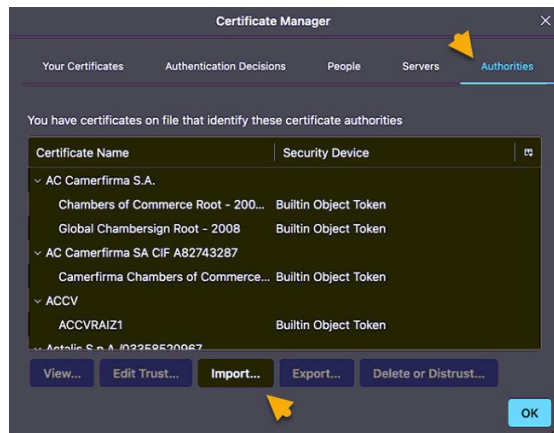
1. To download the certificate, follow the same process as the above steps for Mac.
2. Once it has been downloaded, open Firefox, click in the menu in the upper right, and then click on **Settings**.



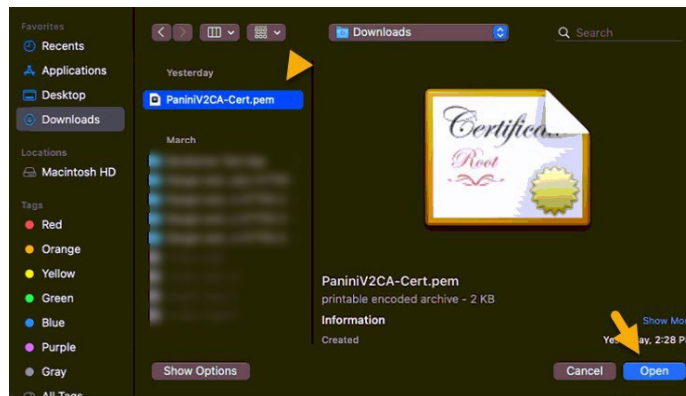
3. Click **Privacy & Security** on the left side, scroll to the bottom, and then click on the **View Certificates...** button.



- Once the **Certificate Manager** window opens, click the **Authorities** tab, and then click the **Import...** button.



- Once the next window opens, navigate to where the certificate was saved (commonly in the Downloads folder), and select the **PaniniV2CA-Cert.pem** file. Then click **Open**.



- On the next screen, check the **Trust this CA to identify websites.** box as that will allow the scanner to communicate with SCO, and then click **OK**.

