

Security

Certificates Installation Guide

August 31, 2021



Contents

1	Introduction	1
2	Windows	2
2.1	Install Perinet ECC Root CA	2
2.2	Install PKI2go Certificates	7
2.2.1	Install root CA certificates	7
2.2.2	Install Client Certificates	11
3	macOS	14
3.1	Install Perinet ECC Root CA	14
3.2	Install PKI2go Certificates	17
3.2.1	Install root CA certificates	17
3.2.2	Install Client Certificates	18
4	iOS and iPadOS	20
4.1	Install Perinet ECC Root CA	20
4.2	Install PKI2go Certificates	22
4.2.1	Install Root CA Certificates	22
4.2.2	Install Client Certificates	25
5	Linux (Ubuntu, Debian)	26
5.1	Install Perinet ECC Root CA	26
5.2	Install PKI2go Certificates	30
5.2.1	Install root CA certificates	30
5.2.2	Install Client Certificates	33
6	Security Warnings	35
7	Contact & Support	36

1 Introduction

Perinet Smart Components are authenticating themselves with host certificates signed by a **Perinet ECC Root CA** (Perinet Certificate Authority). This proves the originality of a device.

In order to trust Perinet devices and to avoid security warnings or alerts in client browsers, we recommend to download the **Perinet ECC Root CA** from <https://docs.perinet.io> and install it in your system.

In case you decide to ignore the warnings, this is an alternative with low security risks, as the communication between your web browser and the Smart Components is still encrypted, even if not authenticated.

However, as security is fundamental in IoT, Perinet also provides a portable Public Key Infrastructure (PKI) called PKI2go, in form of a container in the periMICA. The PKI2go enables highly secured communication between all entities (services and users) of the IoT application, by providing application-specific Certificate Authorities (root CAs) and client certificates.

PKI2go works locally and is independent of your network setup. To take advantage of this high level of security, you need to install two certificates on your local machine. First is the certificate of the trusted signing instance (application Root CA), which will allow your browser to check the identity of the web servers. Second, you need to install a client certificate (admin_pki_container), which gives you administration rights for all services in the application.

This guide provides the installation steps for **Perinet ECC Root CA** and **PKI2go** certificates. It is organized by operating system (OS) and covers the most used web browsers.

In the **Security Warnings** section, we present a few examples of security warnings that can pop up when the **Perinet ECC Root CA** or the **application Root CA** is not properly installed.

***Note:** Despite the fact that the Root CA certificate installation can be skipped, if the mTLS is enabled in periNODEs or in periMICA containers, the installation of the proper client certificate is mandatory in order to access the HTTPS/MQTT servers.*

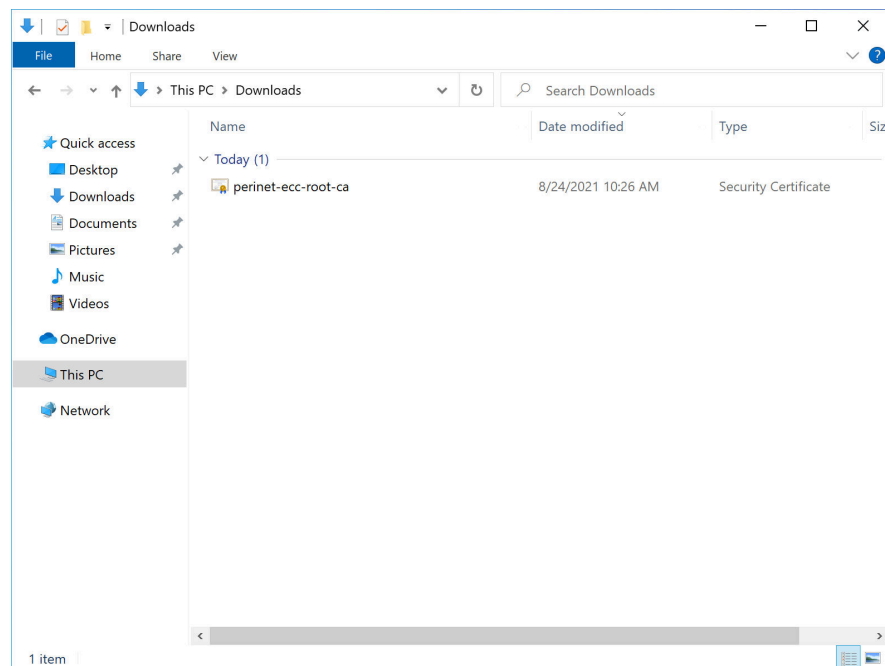
For further information on security concepts, please refer to <https://docs.perinet.io>.

2 Windows

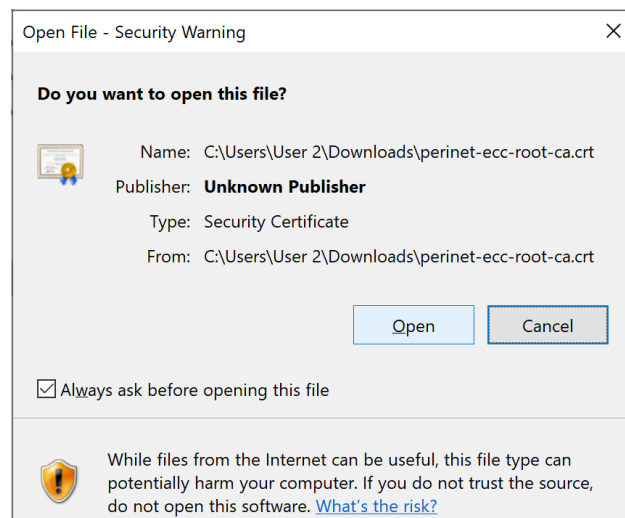
2.1 Install Perinet ECC Root CA

This section describes how to install **Perinet ECC Root CA** certificate on Windows systems.

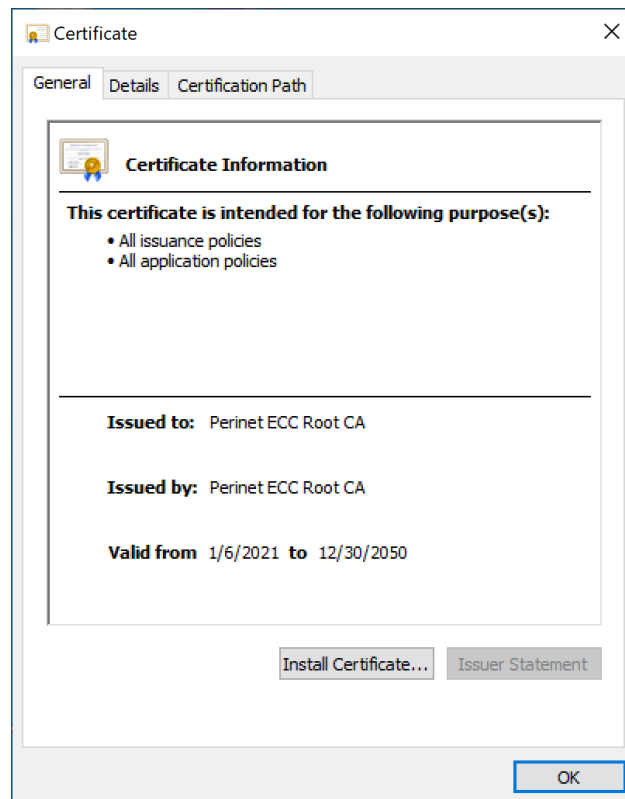
Please download the file from <https://docs.perinet.io>. Double-click on the downloaded certificate file and follow the installation instructions below:



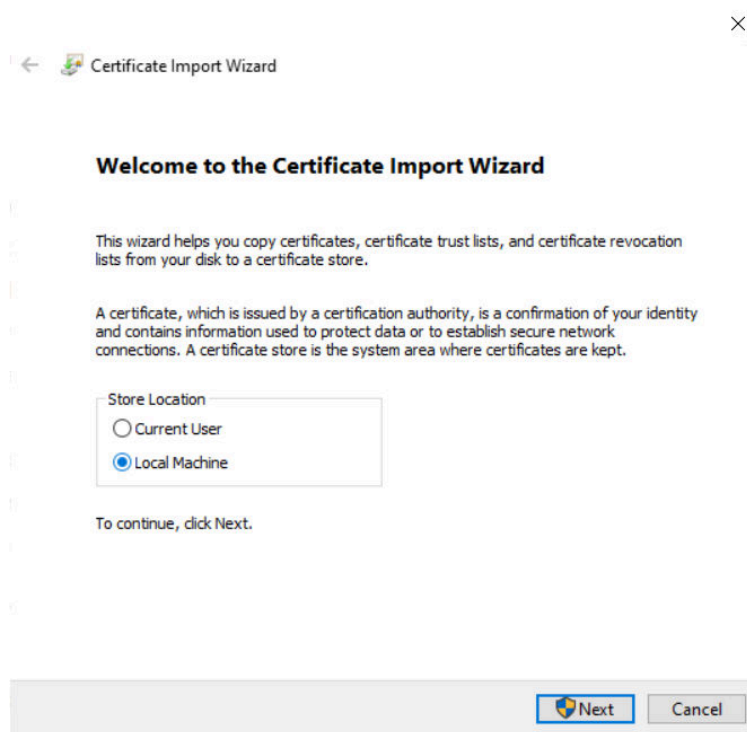
(1) Double Click on *perinet-ecc-root-ca.crt*



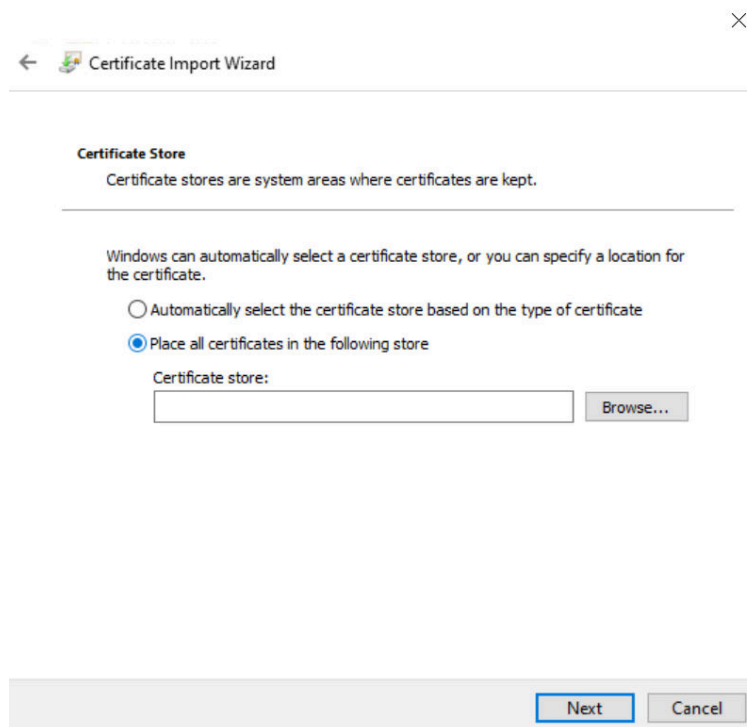
(2) Select *Open*



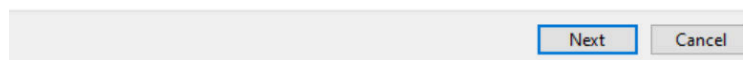
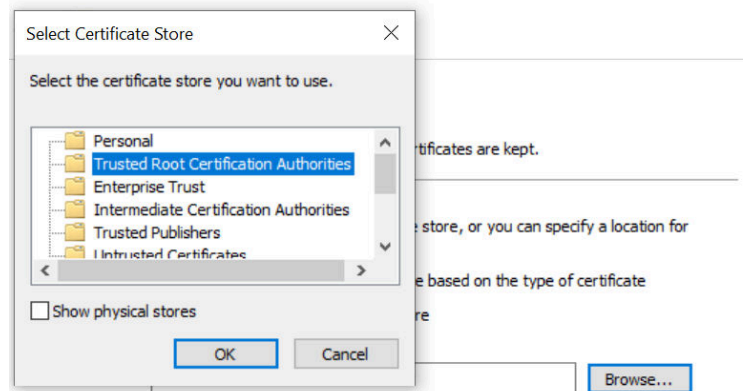
(3) Select *Install Certificate...*



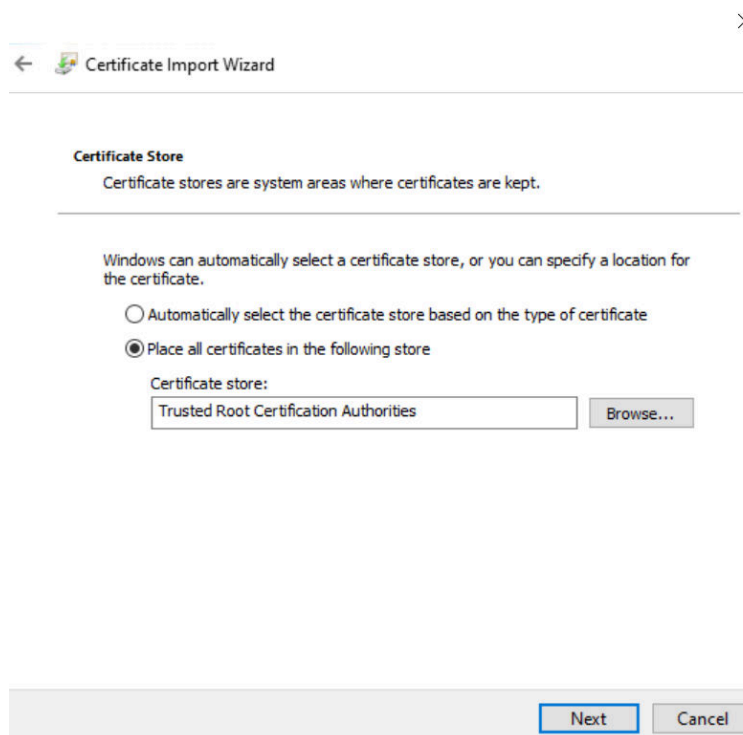
(4) Select *Local Machine*



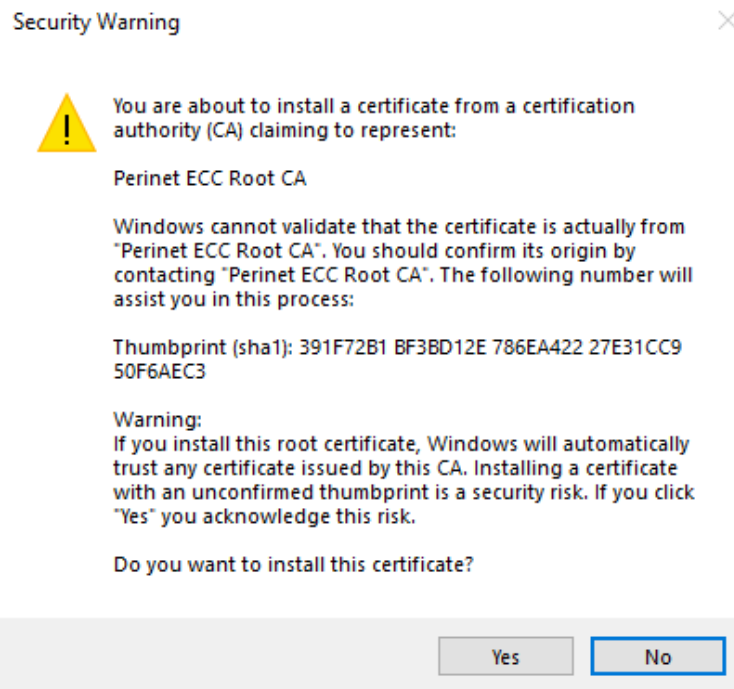
(5) Select *Place all certificates in the following store*



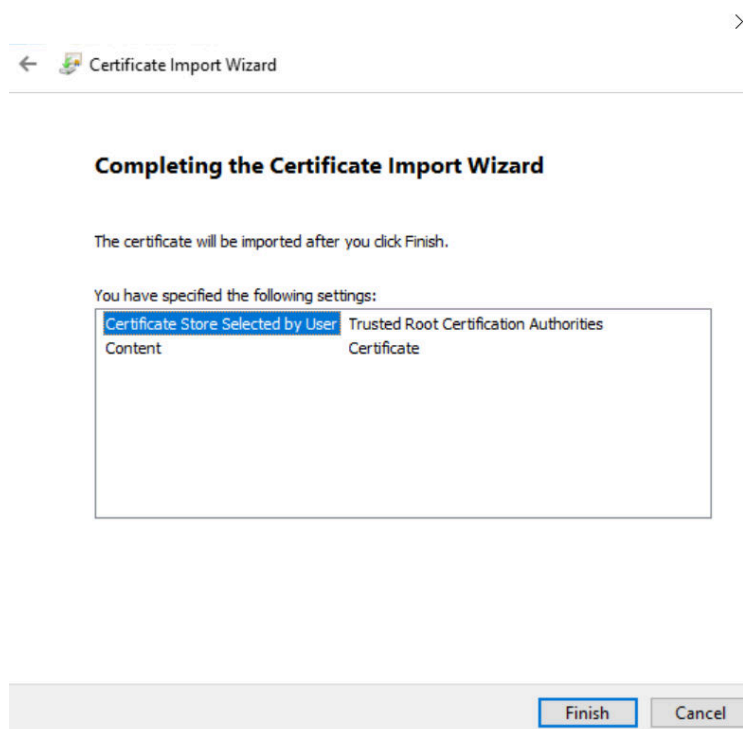
(6) Select *Trusted Root Certification Authorities*



(7) Click *Next*



(8) Click Yes to confirm

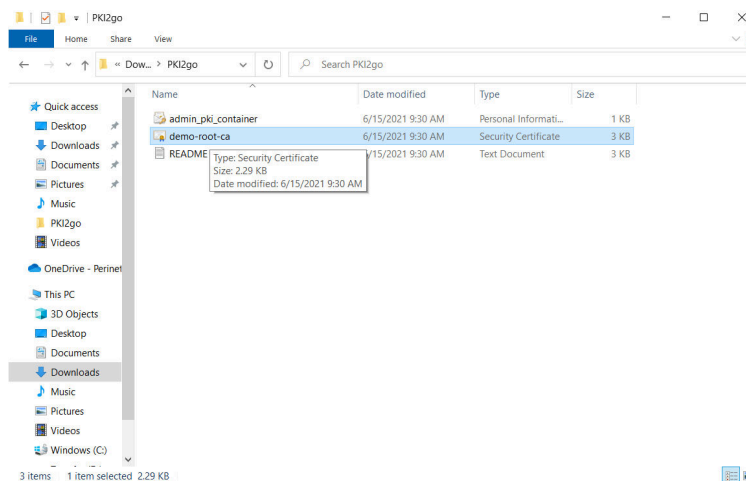


(9) Click *Finish*

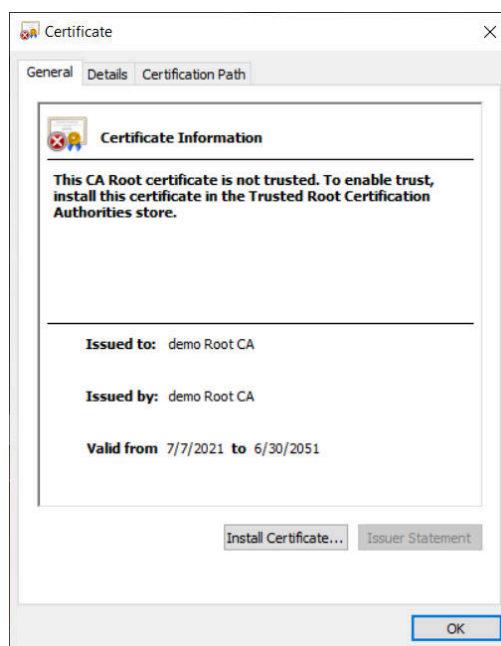
2.2 Install PKI2go Certificates

2.2.1 Install root CA certificates

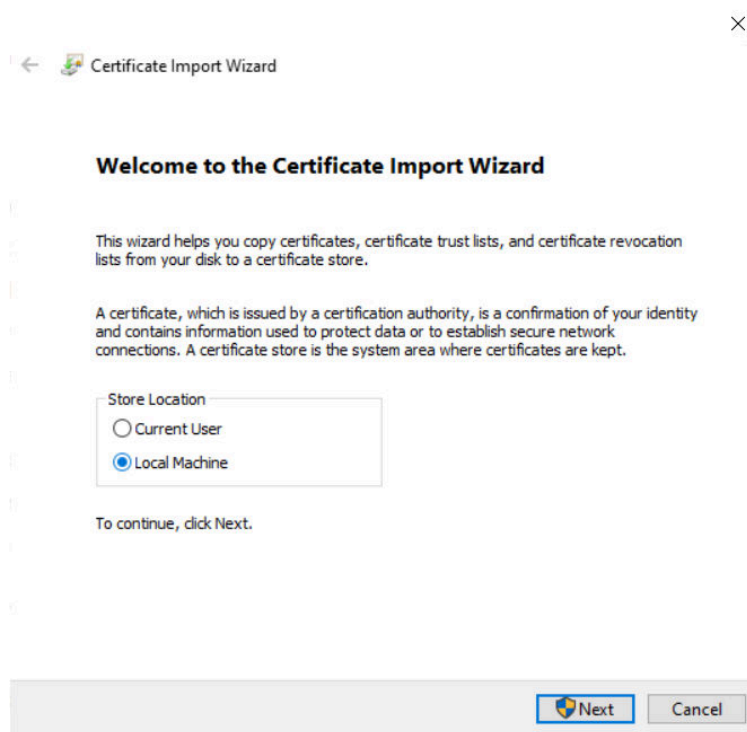
This section describes how to install the certificate generated by PKI2go for the **root Certificate Authority** on Windows systems . Double-click on the downloaded certificate file as shown in the following pictures.



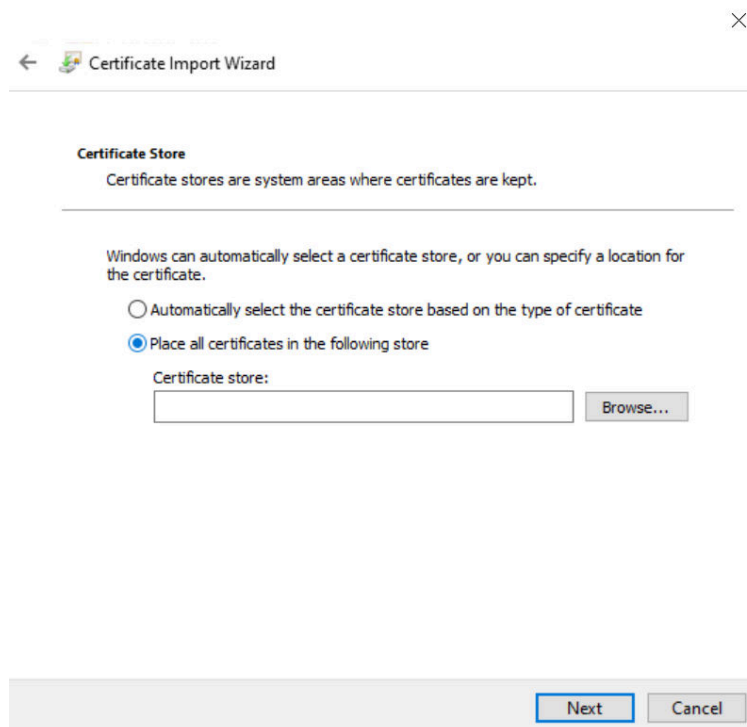
(10) Double Click on *demo-root-ca.crt*



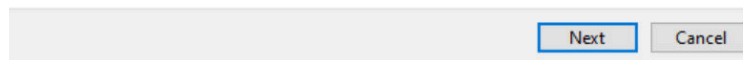
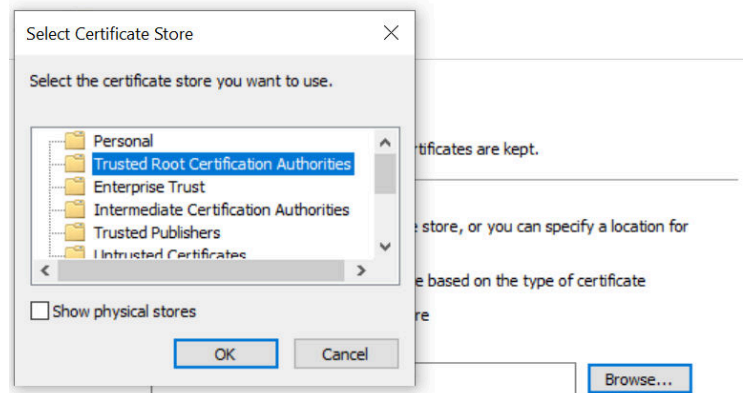
(11) Select *Install Certificate...*



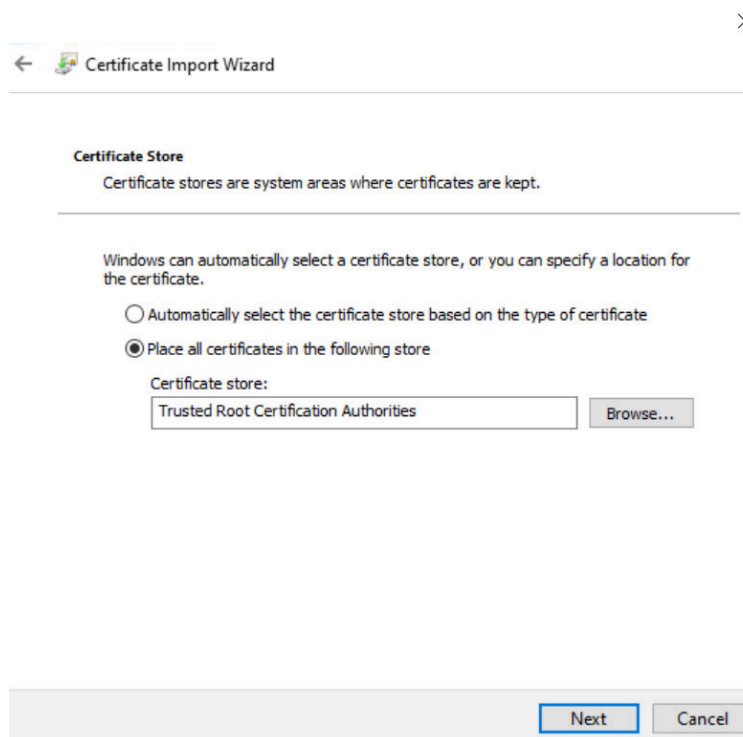
(12) Select *Local Machine*



(13) Select *Place all certificates in the following store*



(14) Select *Trusted Root Certification Authorities*



(15) Click *Next*

Security Warning



You are about to install a certificate from a certification authority (CA) claiming to represent:

demo Root CA

Windows cannot validate that the certificate is actually from "demo Root CA". You should confirm its origin by contacting "demo Root CA". The following number will assist you in this process:

Thumbprint (sha1): 105DEF71 3AB8B219 2A19D630 16F1DA3D 7C8E9A67

Warning:

If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Yes

No

(16) Click Yes to confirm



Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

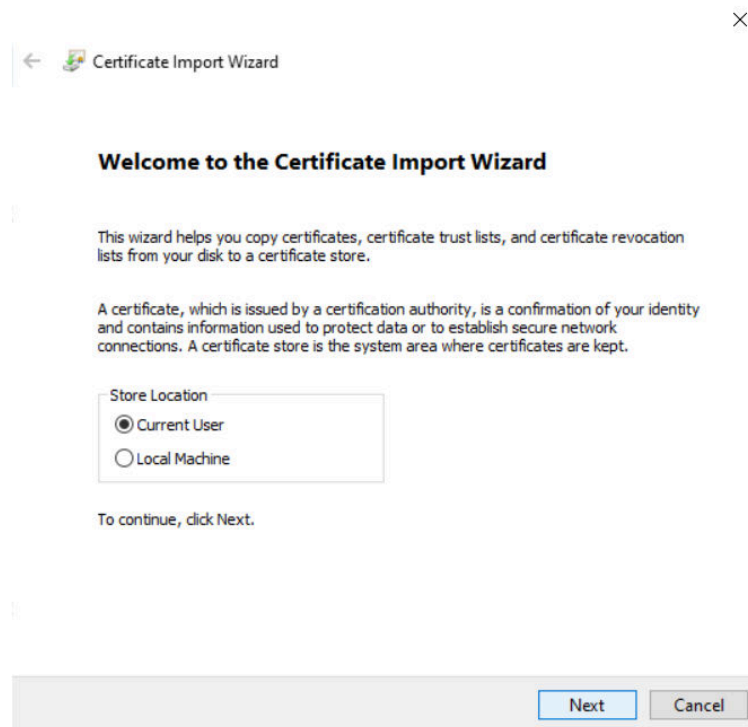
Finish

Cancel

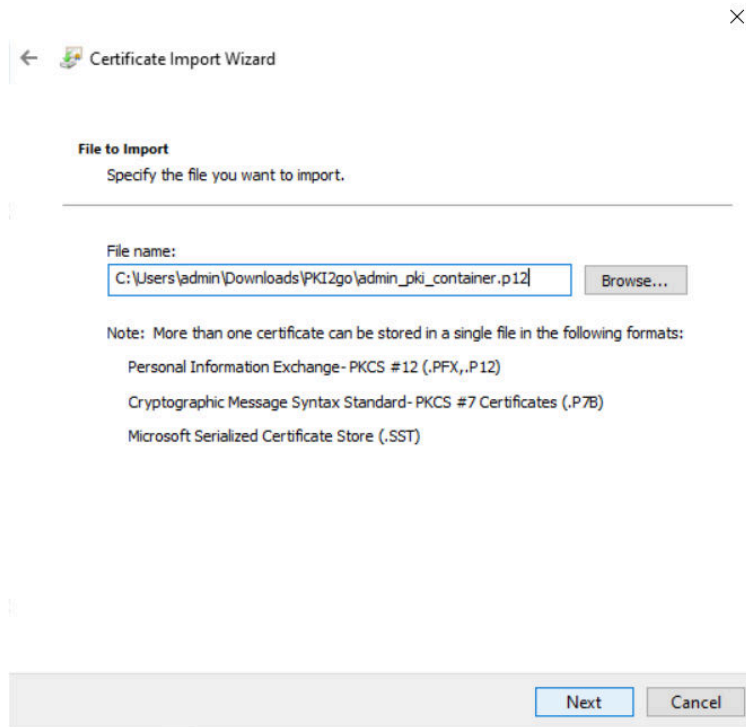
(17) Click *Finish*

2.2.2 Install Client Certificates

Double-click on the certificate with .p12 extension and follow the installation instructions as in the pictures below.



(18) Select *Current User*



← Certificate Import Wizard

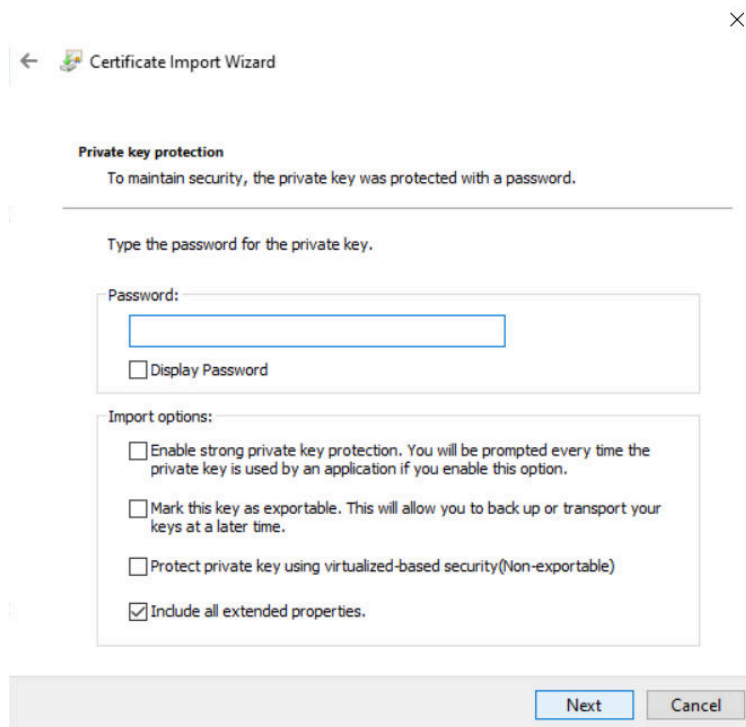
File to Import
Specify the file you want to import.

File name:
C:\Users\admin\Downloads\PKI2go\admin_pki_container.p12 Browse...

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)

Next Cancel

(19) Click *Next*



← Certificate Import Wizard

Private key protection
To maintain security, the private key was protected with a password.

Type the password for the private key.

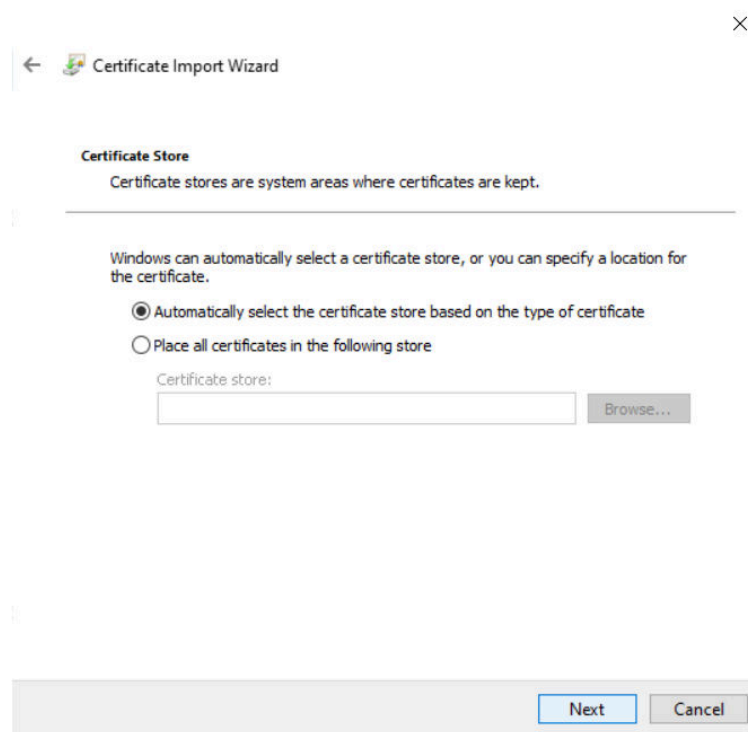
Password:

☐ Display Password

Import options:
☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
☐ Protect private key using virtualized-based security(Non-exportable)
☒ Include all extended properties.

Next Cancel

(20) Type the password: *admin_pki_container*

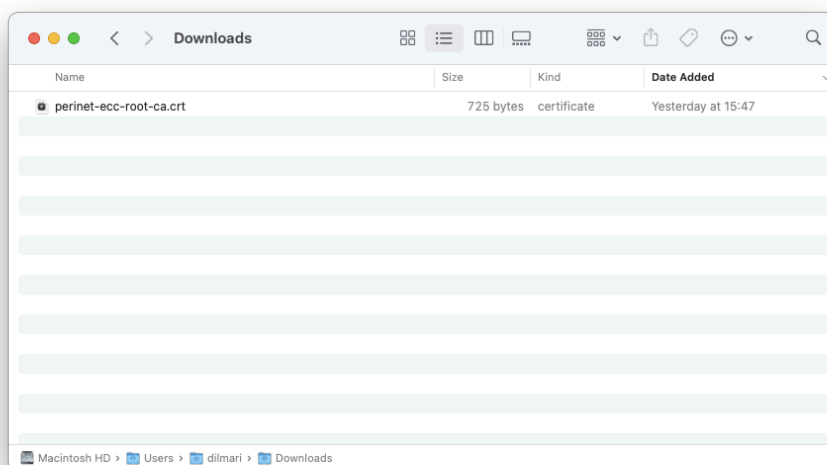


(21) Click *Next*

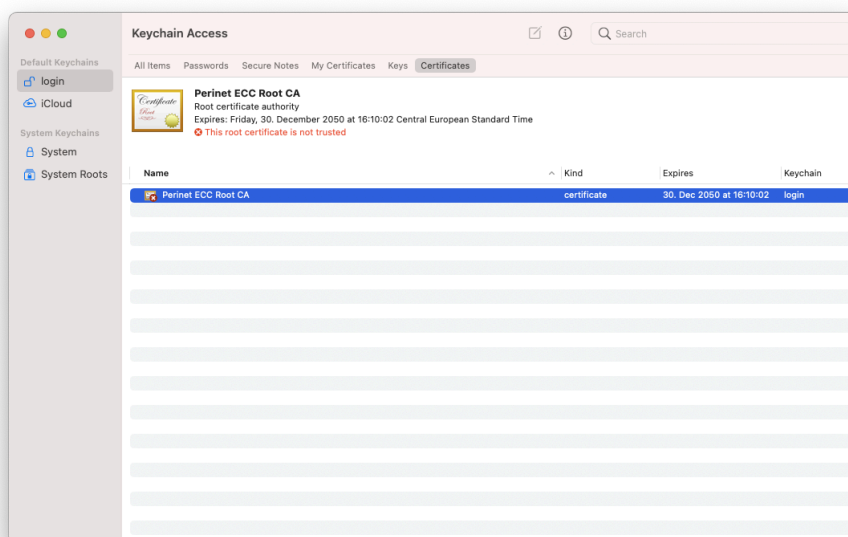
3 macOS

3.1 Install Perinet ECC Root CA

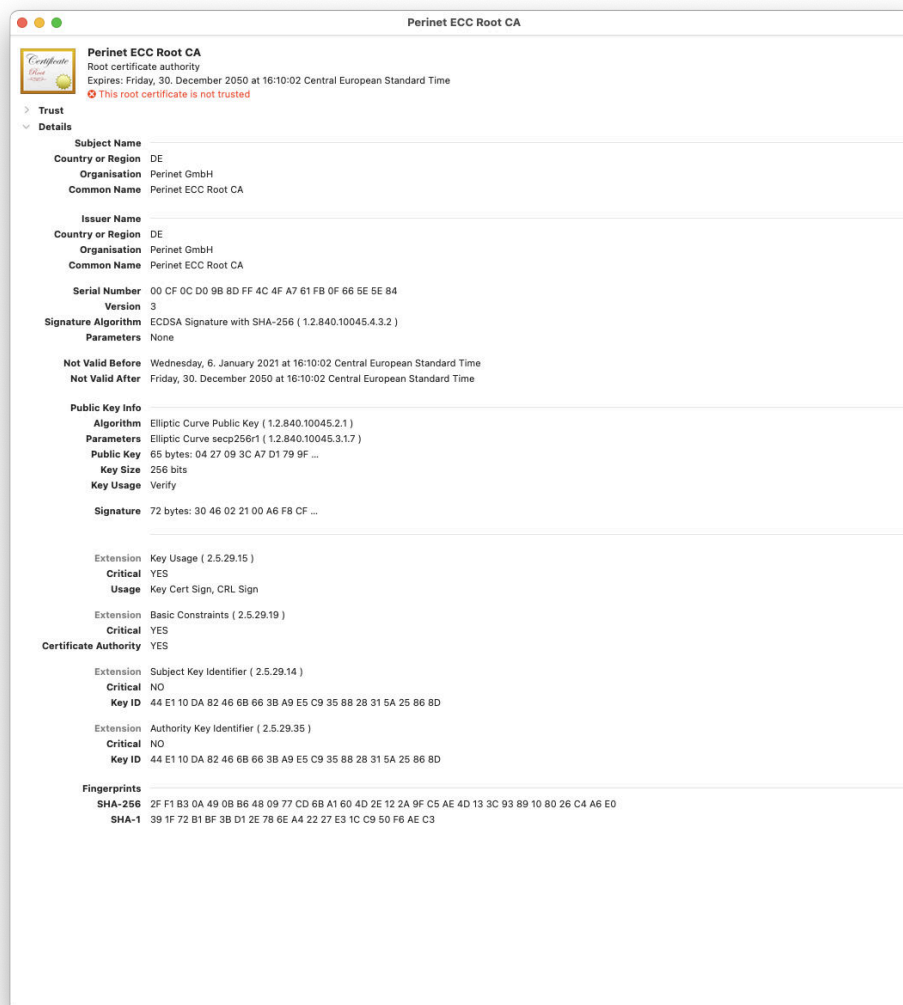
This section describes how to install **Perinet ECC Root CA** on macOS systems. Please download the file from <https://docs.perinet.io>. Double-click on the downloaded certificate file and follow the installation instructions below:



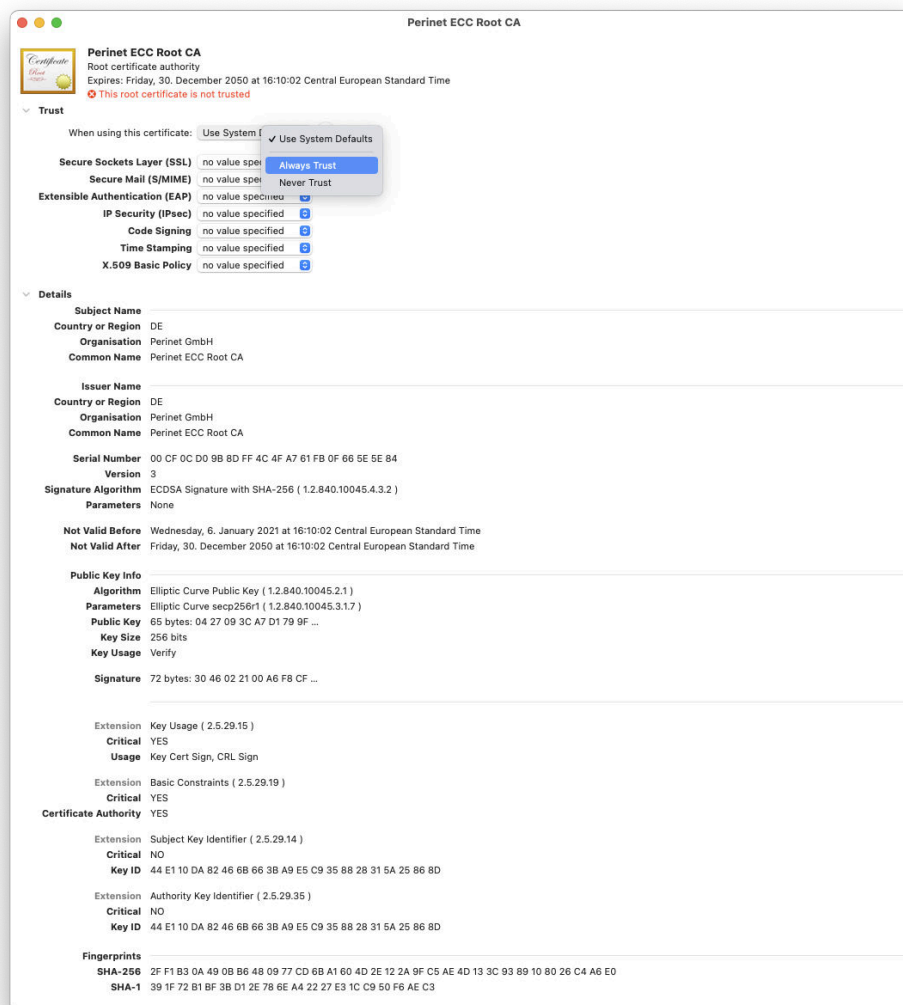
(22) Double-click on *perinet-ecc-root-ca.crt*



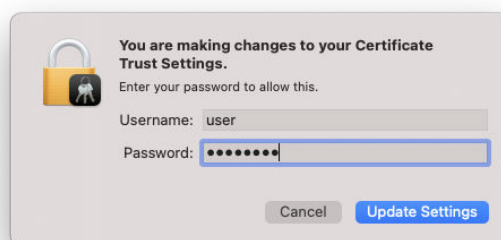
(23) The Keychain Access App will open automatically. Double-click on *Perinet ECC Root CA*



(24) Expand the *Trust* option



(25) Click on *When using this certificate* and select *Always Trust*

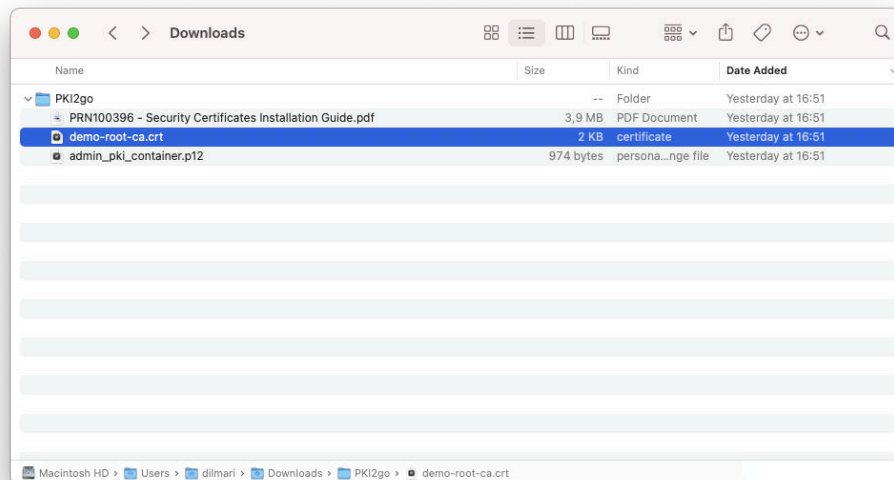


(26) Provide the user credentials and click on *Update Settings*

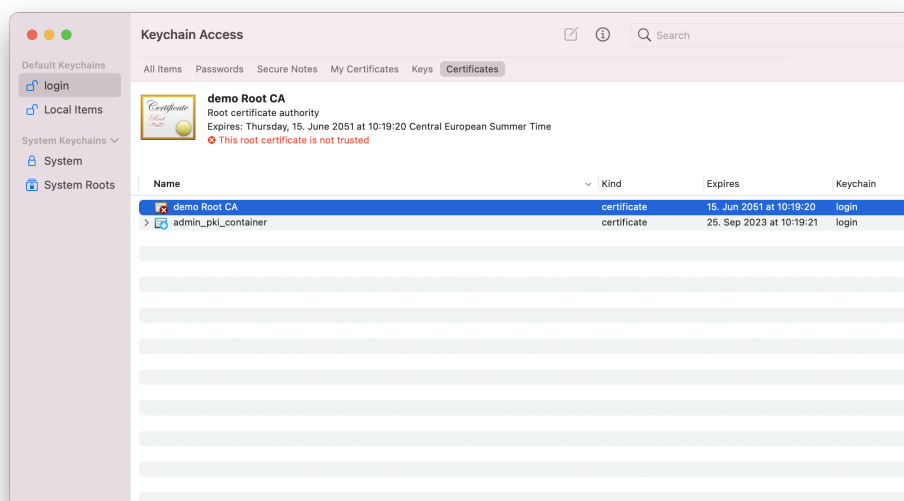
3.2 Install PKI2go Certificates

3.2.1 Install root CA certificates

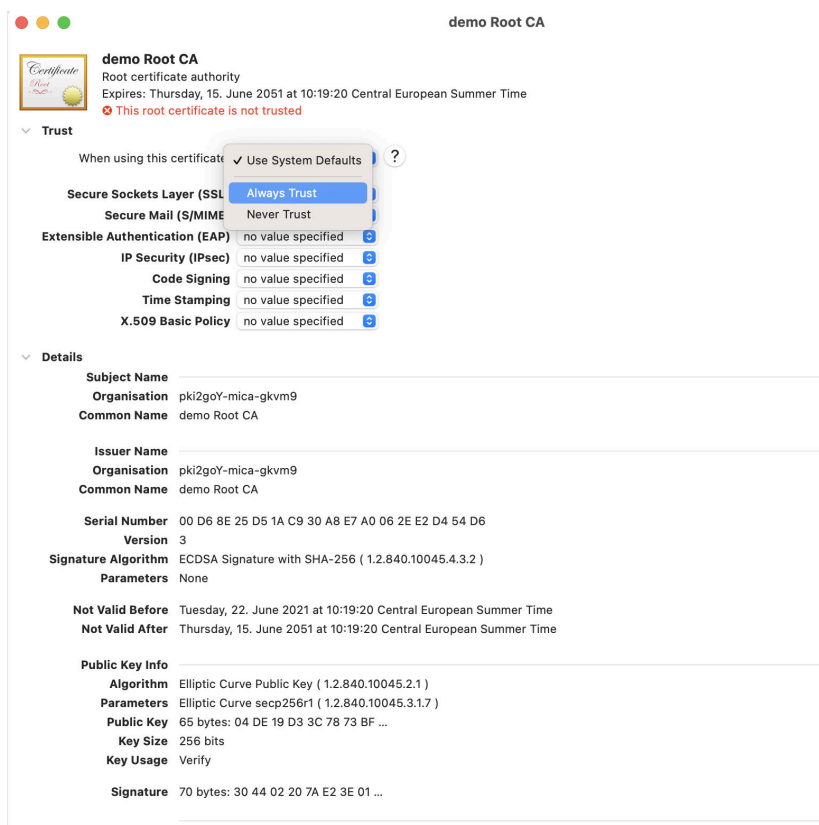
This section describes how to install the certificate generated by PKI2go for the **root Certificate Authority** on macOS. Double-click on the downloaded certificate file as shown in the following pictures.



(27) Double-click on *demo-root-ca.crt*



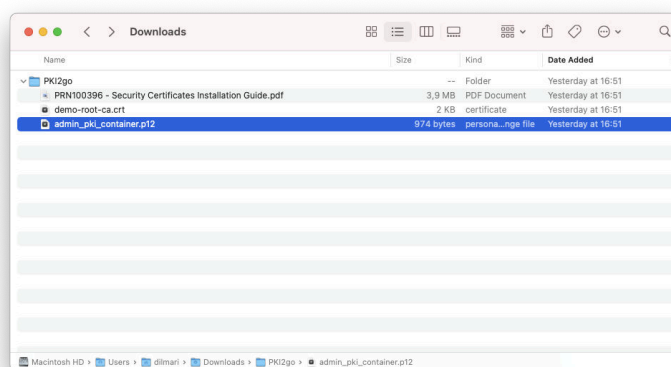
(28) Double-click on *demo Root CA*



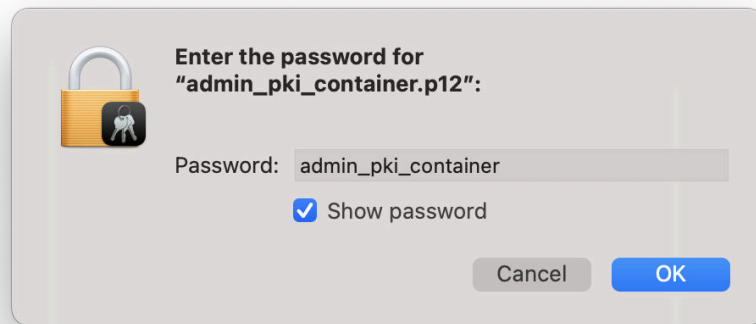
(29) Select Always Trust

3.2.2 Install Client Certificates

Double-click on the certificate with .p12 extension and follow the installation instructions as in the pictures below:



(30) Double-click on the *admin_pki_container_mac_os.p12*



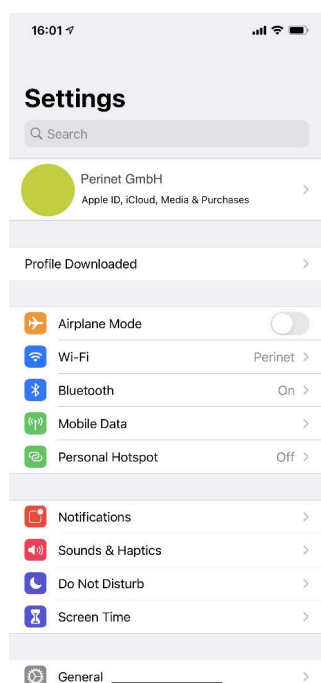
(31) Type the password: *admin_pki_container*

4 iOS and iPadOS

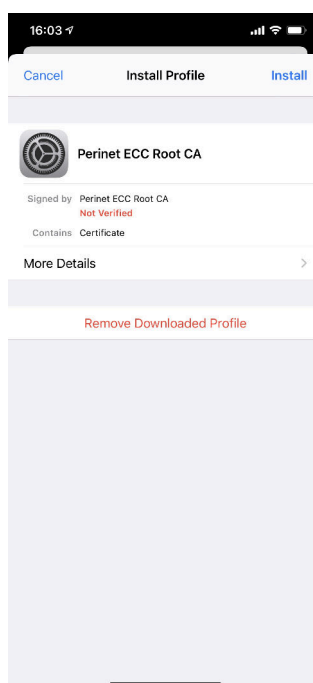
4.1 Install Perinet ECC Root CA

This section describes how to install **Perinet ECC Root CA** certificate on iOS and iPadOS.

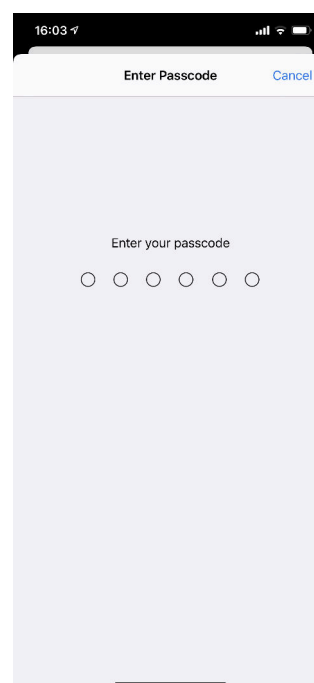
Please download the certificate/profile from <https://docs.perinet.io> and next go to the *Settings* app and follow the installation instructions below:



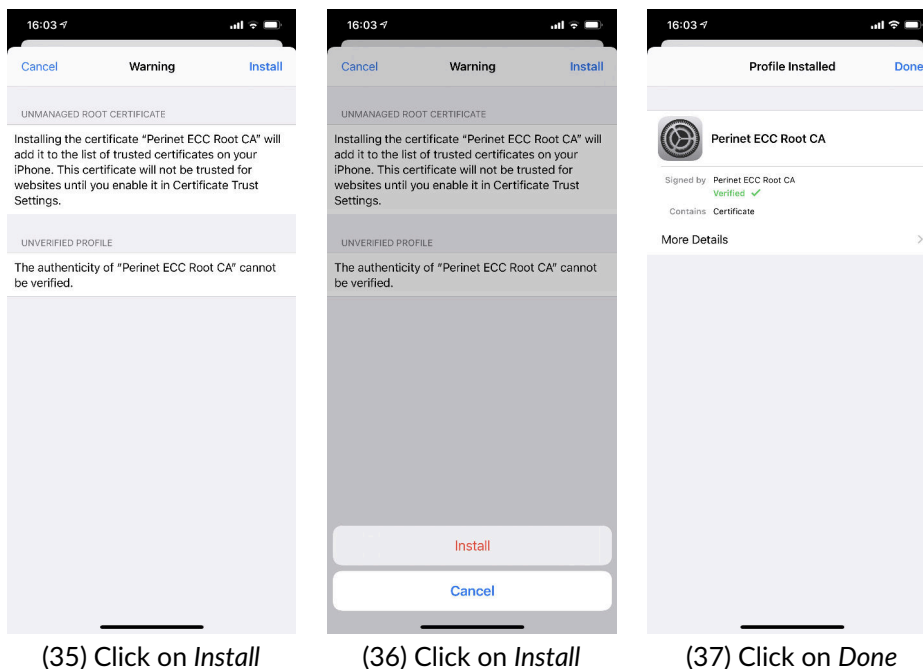
(32) Go to *Profile Downloaded*



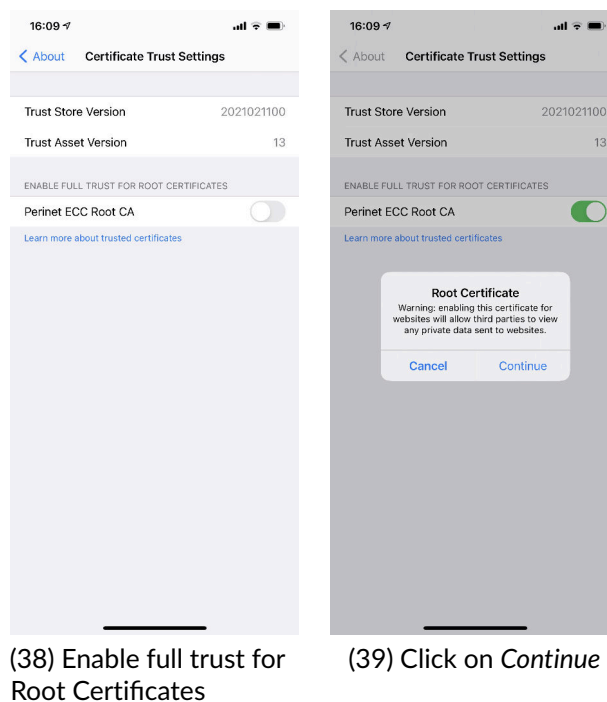
(33) Click on *Install*



(34) Enter your passcode

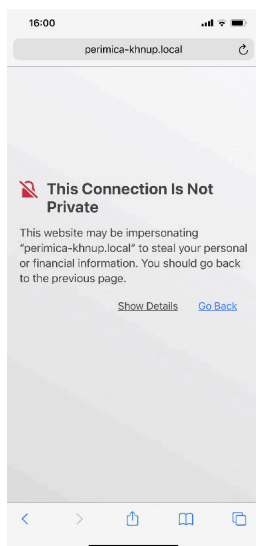


Now the certificate is installed, but not yet trusted. In order to trust the **Perinet ECC Root CA**, open *Settings* → *About* → *Certificate Trust Settings* and follow the instructions in the pictures below:

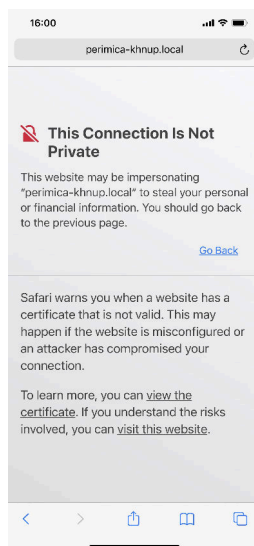


4.2 Install PKI2go Certificates

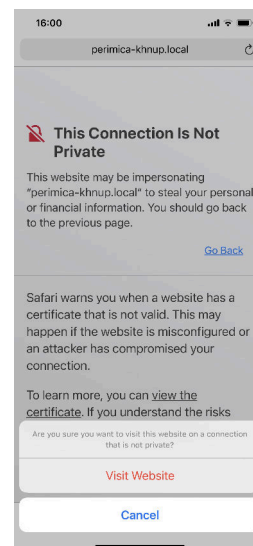
4.2.1 Install Root CA Certificates



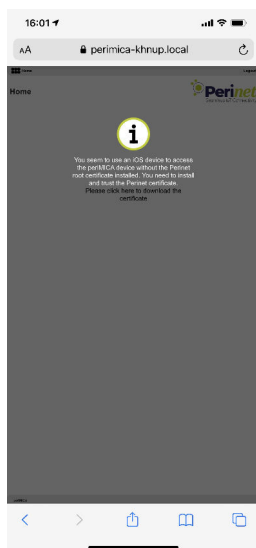
(40) Click on *Show Details*



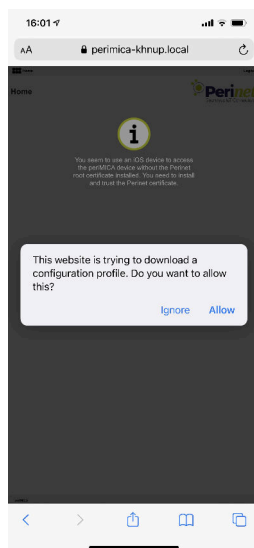
(41) Click on *visit this website*



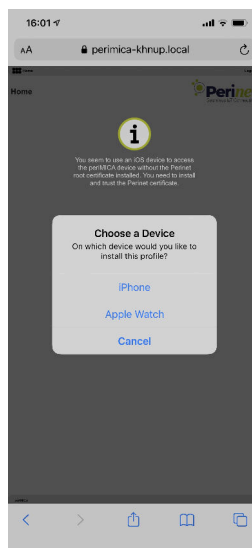
(42) Click on *Visit Website*



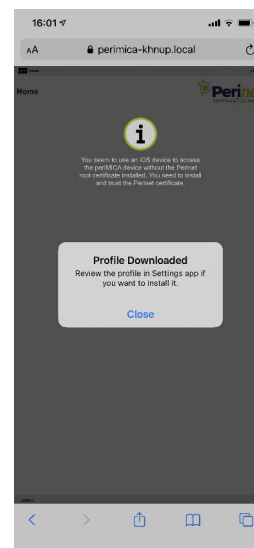
(43) Click on link to download the certificate



(44) Click on *Allow*



(45) Select device

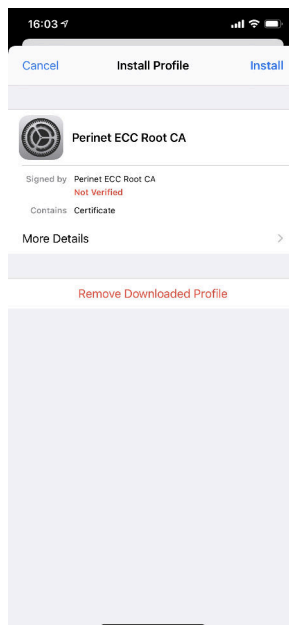


(46) Click on *Close*

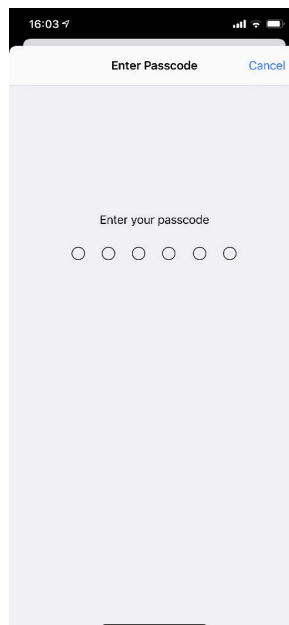
After downloading the certificate, go to the *Settings* app and proceed with the installation as following:



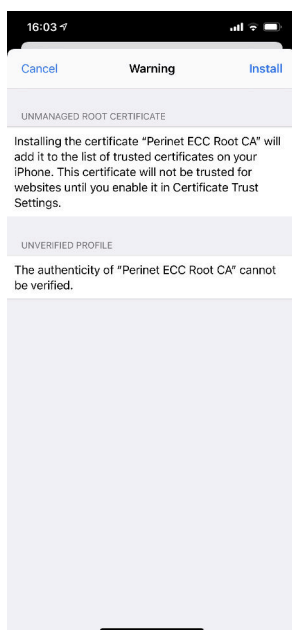
(47) Go to *Profile Downloaded*



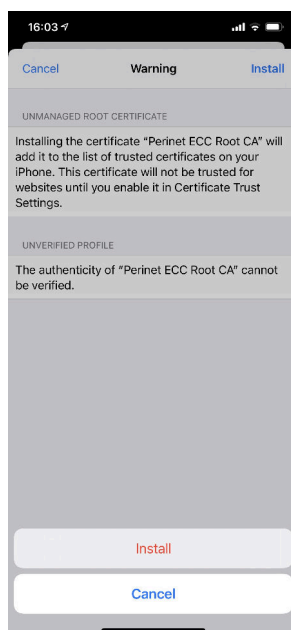
(48) Click on *Install*



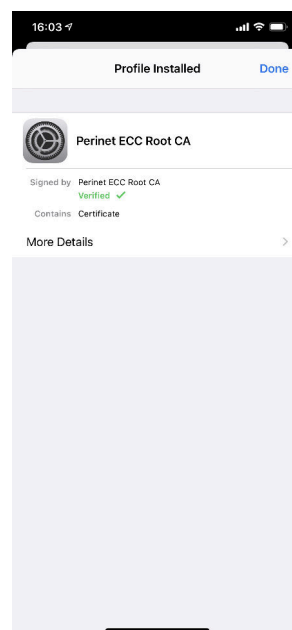
(49) Enter your passcode



(50) Click on *Install*

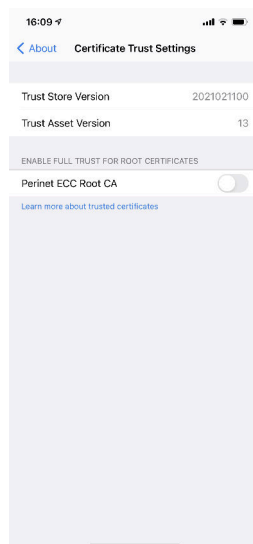


(51) Click on *Install*

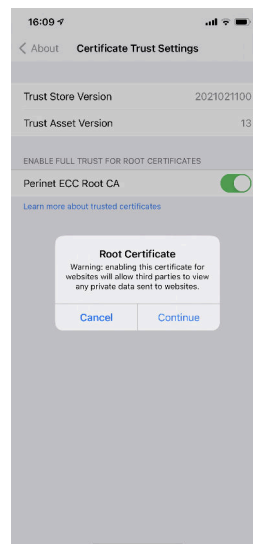


(52) Click on *Done*

Now the certificate is installed, but not yet trusted. In order to trust the **demo Root CA**, open *Settings* → *About* → *Certificate Trust Settings* and follow the instructions in the pictures below:



(53) Enable full trust for Root Certificates



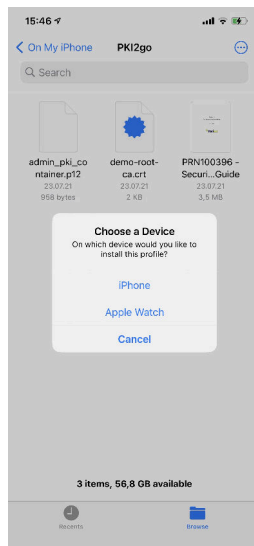
(54) Click on *Continue*

4.2.2 Install Client Certificates

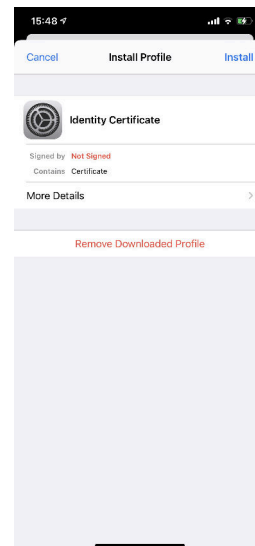
Open the *Files* app and find the downloaded file. Click on the *.p12* and follow the instructions in the pictures below:



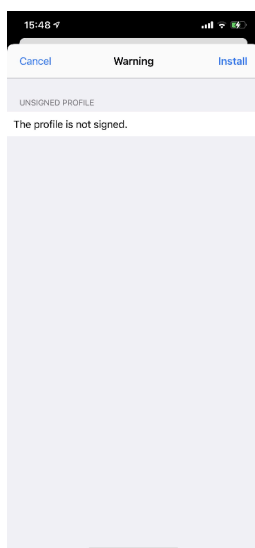
(55) Click on the **.p12** file (*admin_pki_container.p12*)



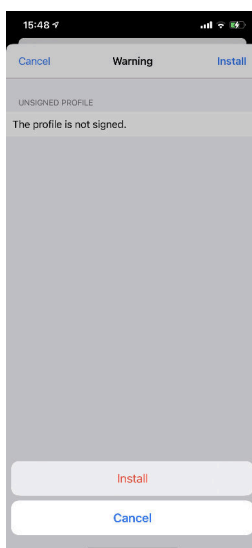
(56) Choose a Device



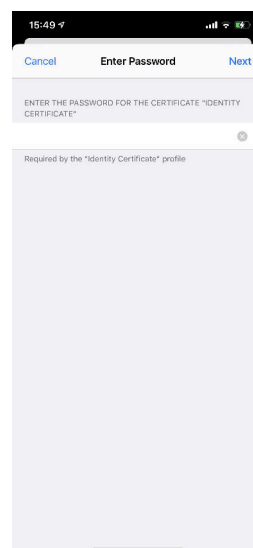
(57) Click on *Install*



(58) Click on *Install*



(59) Click on *Install*

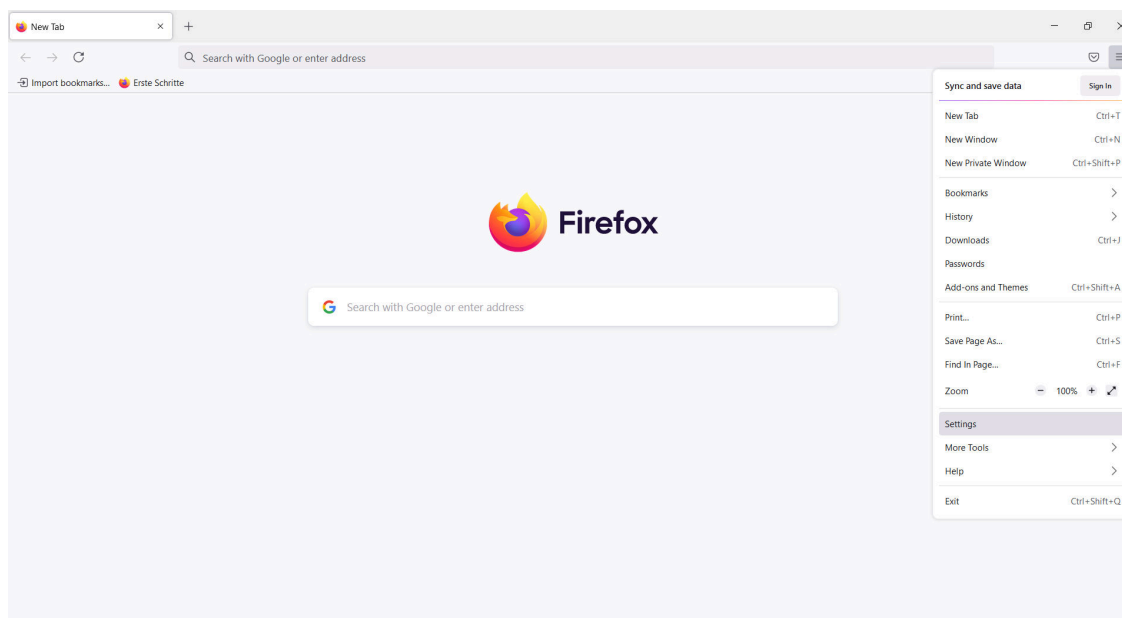


(60) Type the password (*admin_pki_container*) and click on *Next*

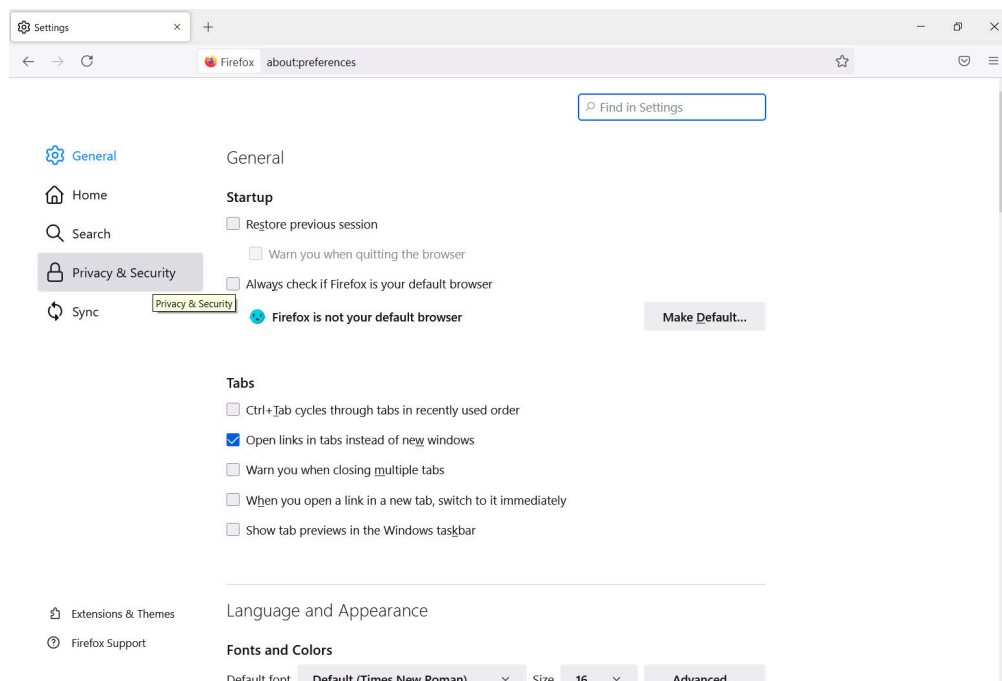
5 Linux (Ubuntu, Debian)

5.1 Install Perinet ECC Root CA

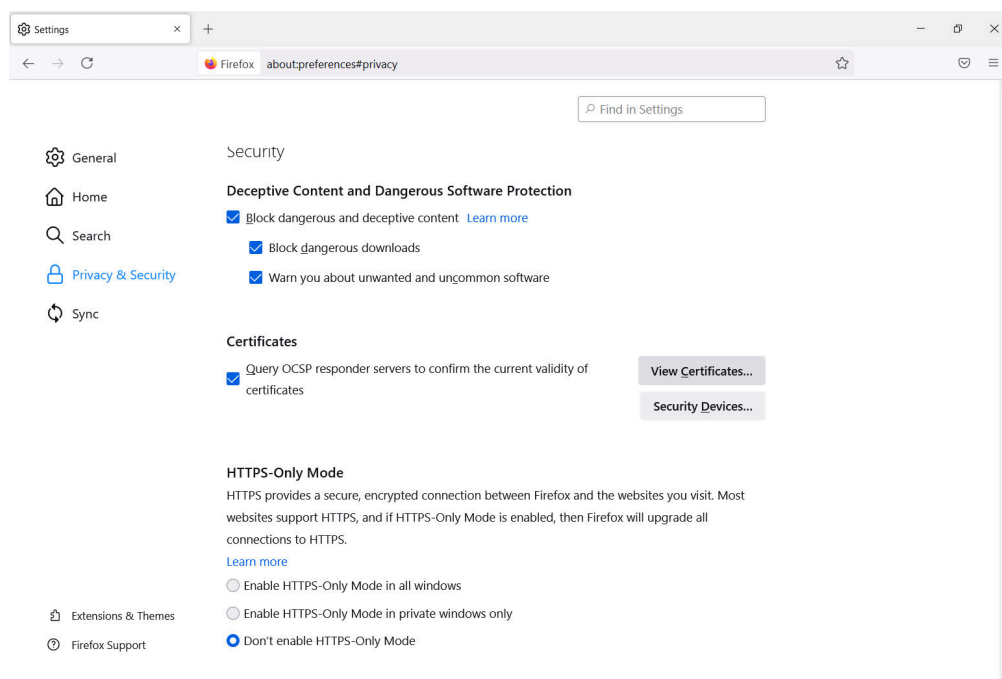
This section describes how to install **Perinet ECC Root CA** certificate on Debian-based systems. The example below is for Firefox browser. Download the file from <https://docs.perinet.io> and follow the installation instructions below:



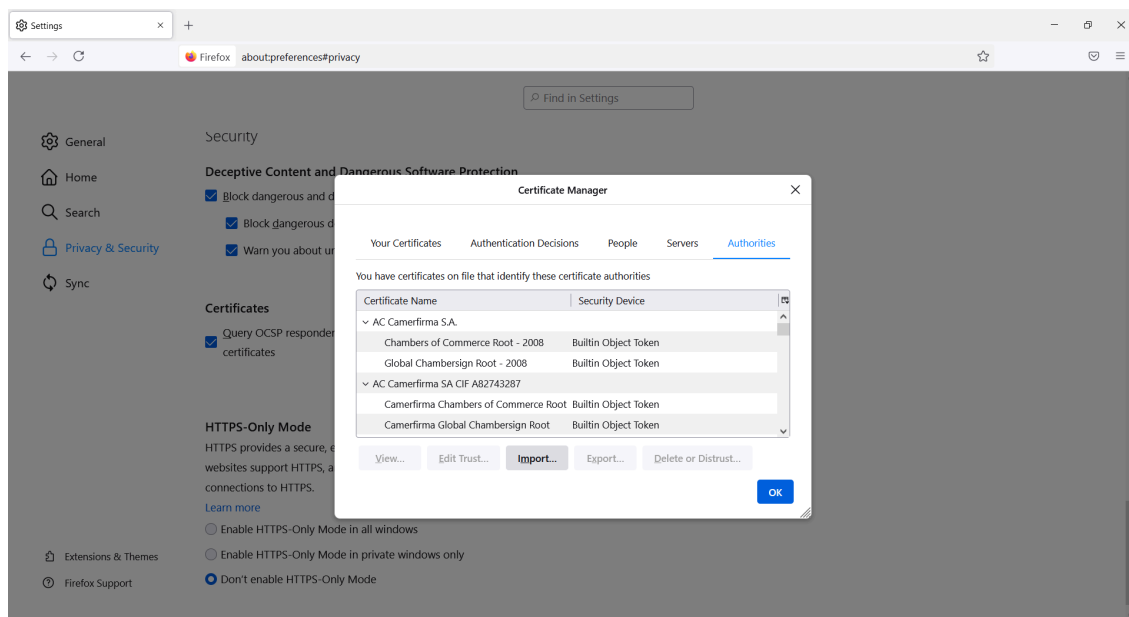
(61) Go to *Settings*



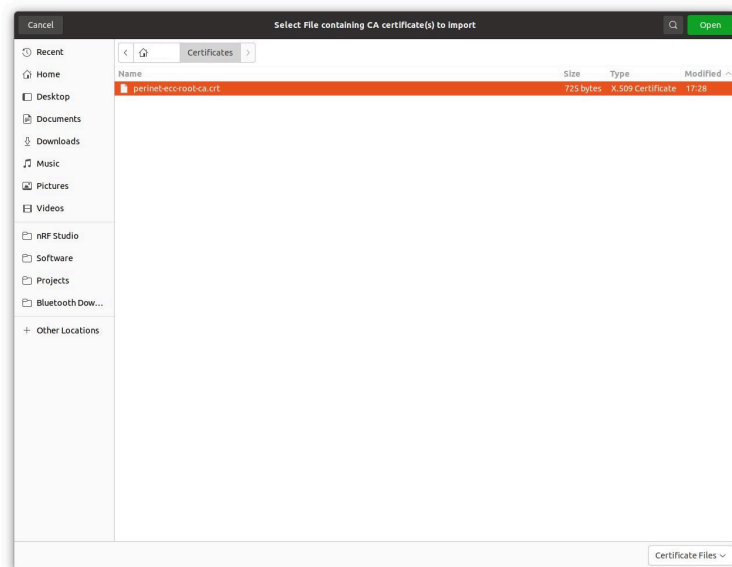
(62) Select *Privacy & Security*



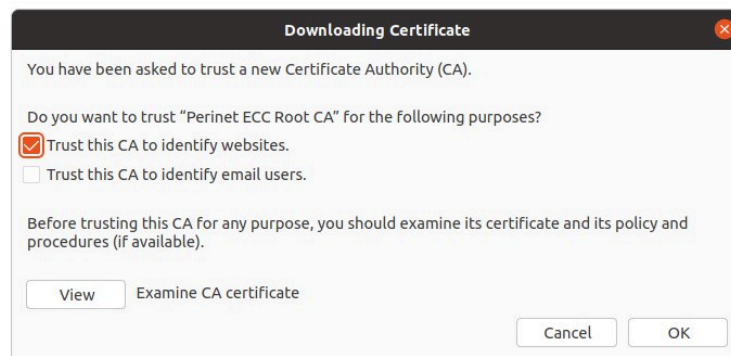
(63) Click on *View Certificates...*



(64) Select **Import...** on **Authorities** tab



(65) Find the file in the system, double-click on the *perinet-ecc-root-ca.crt*

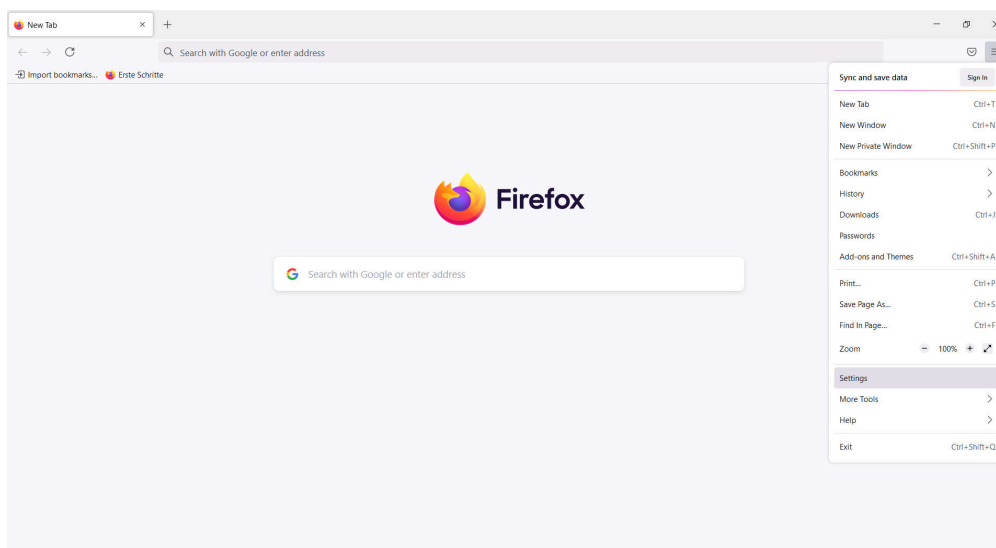


(66) Mark "Trust this CA to identify websites" and click on OK

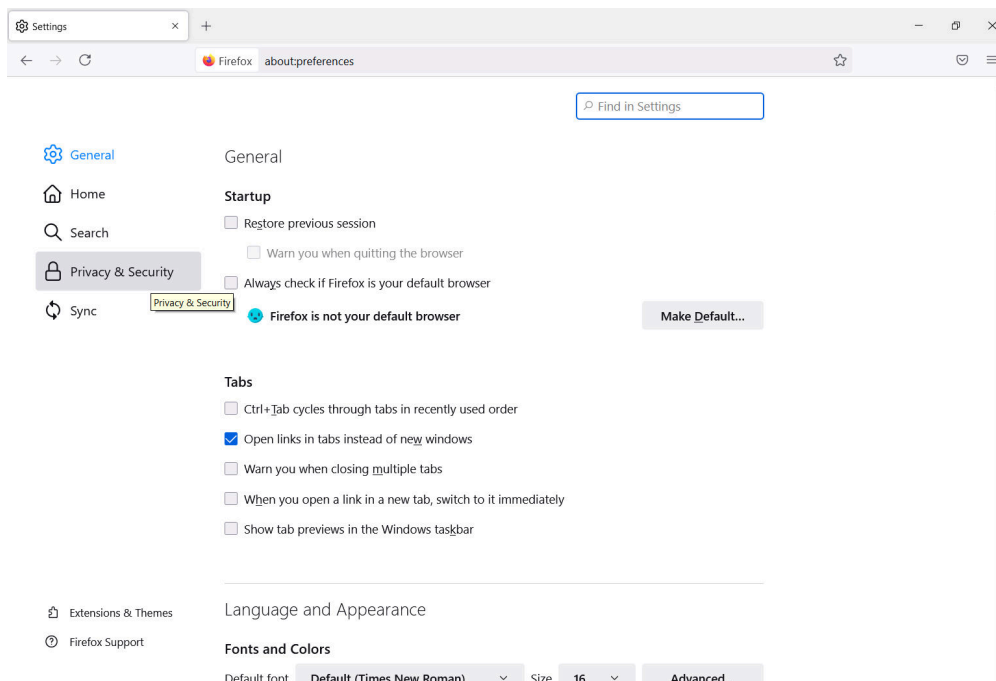
5.2 Install PKI2go Certificates

5.2.1 Install root CA certificates

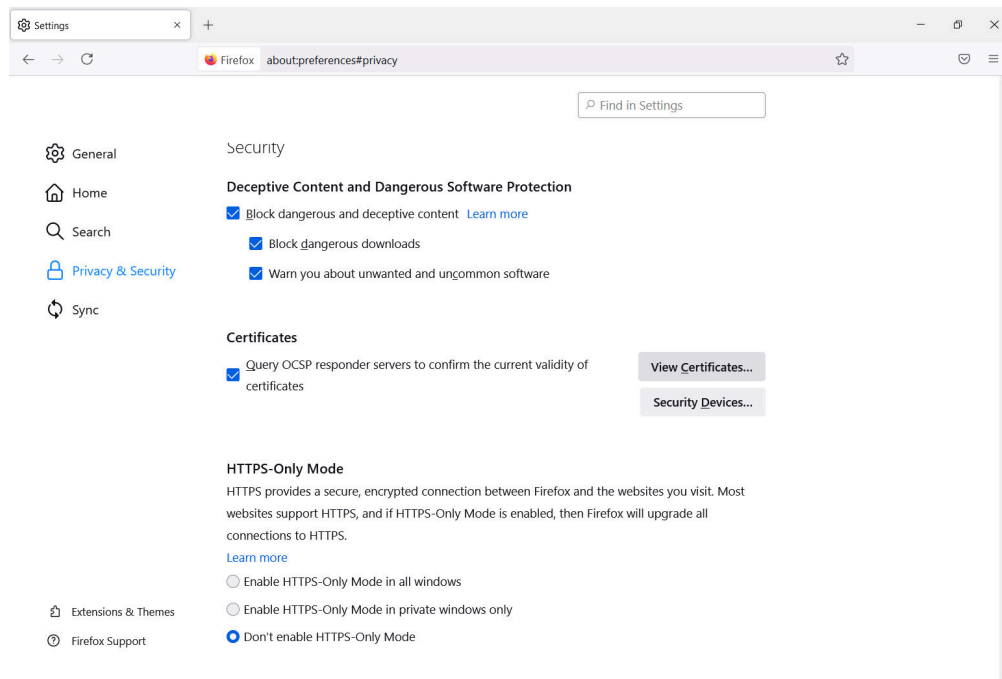
This section describes how to install the certificate generated by PKI2go for the **root Certificate Authority** on Linux (Ubuntu, Debian) systems. The example is for Firefox Browser.



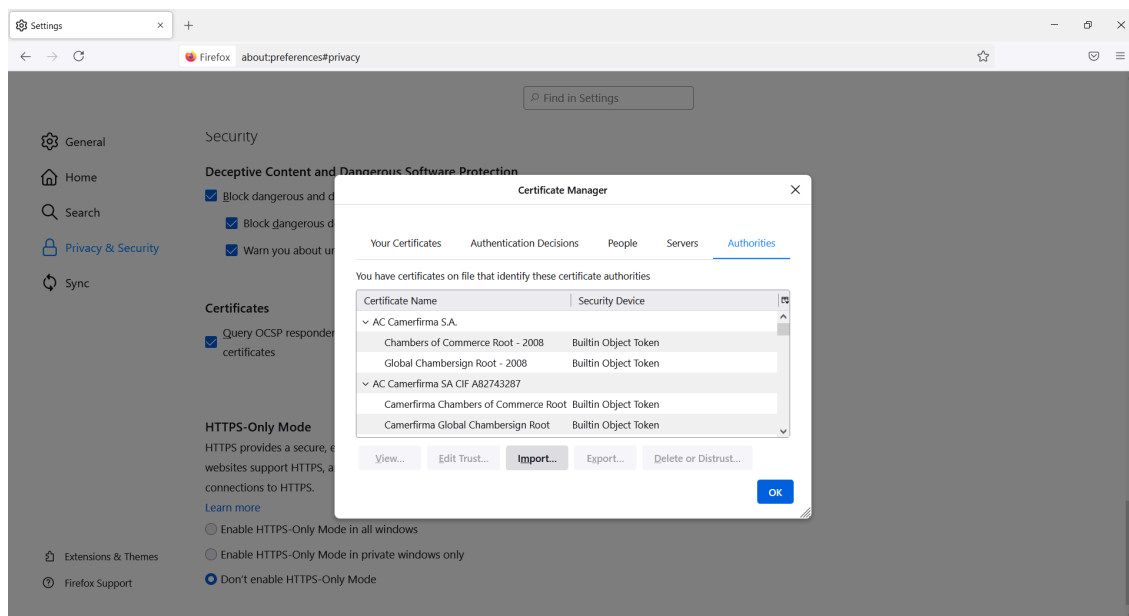
(67) Go to Settings



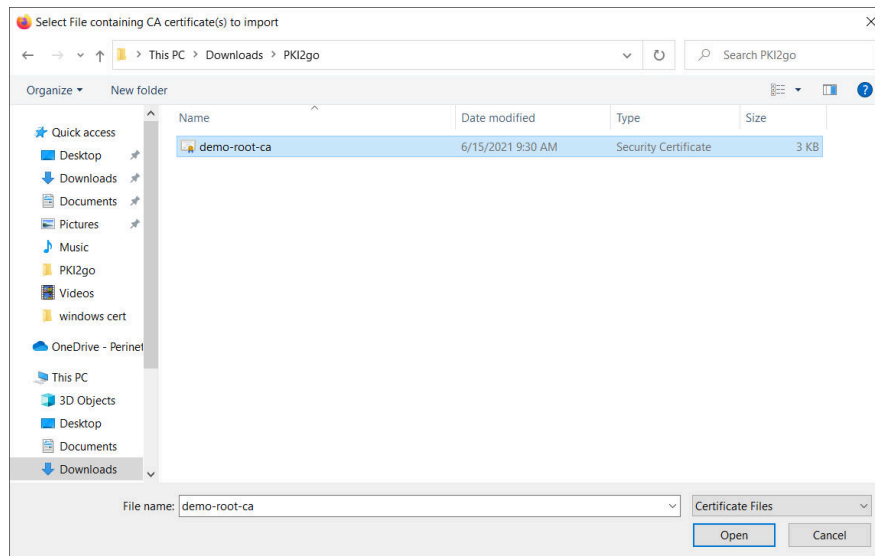
(68) Select Privacy & Security



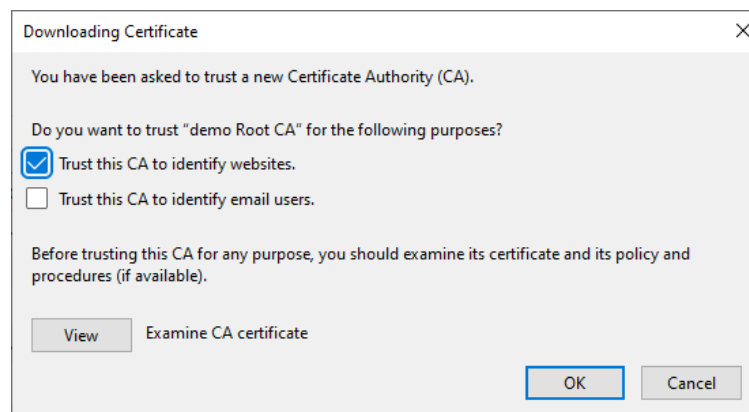
(69) Click on *View Certificates...*



(70) Select *Import...* on *Authorities* tab



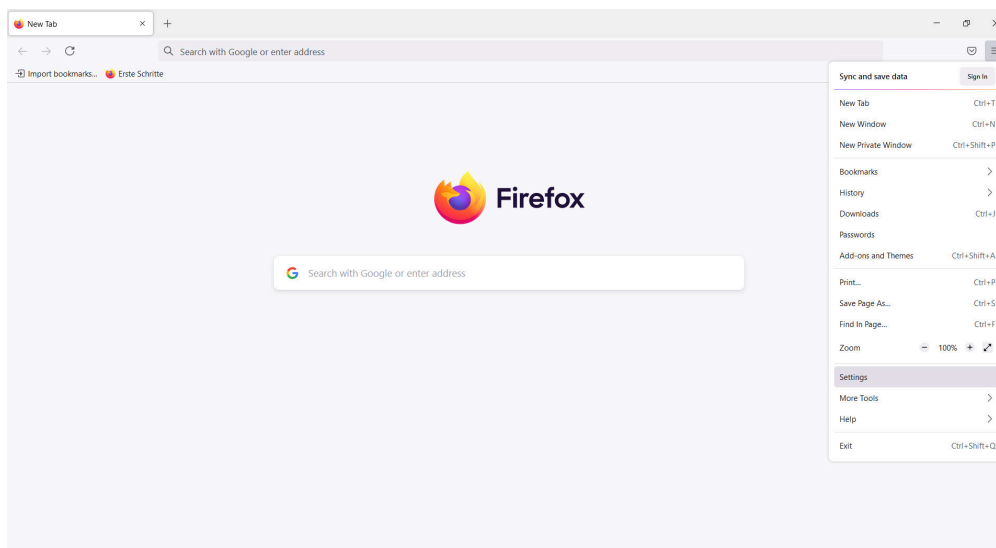
(71) Double-click on the *demo-root-ca.pem*



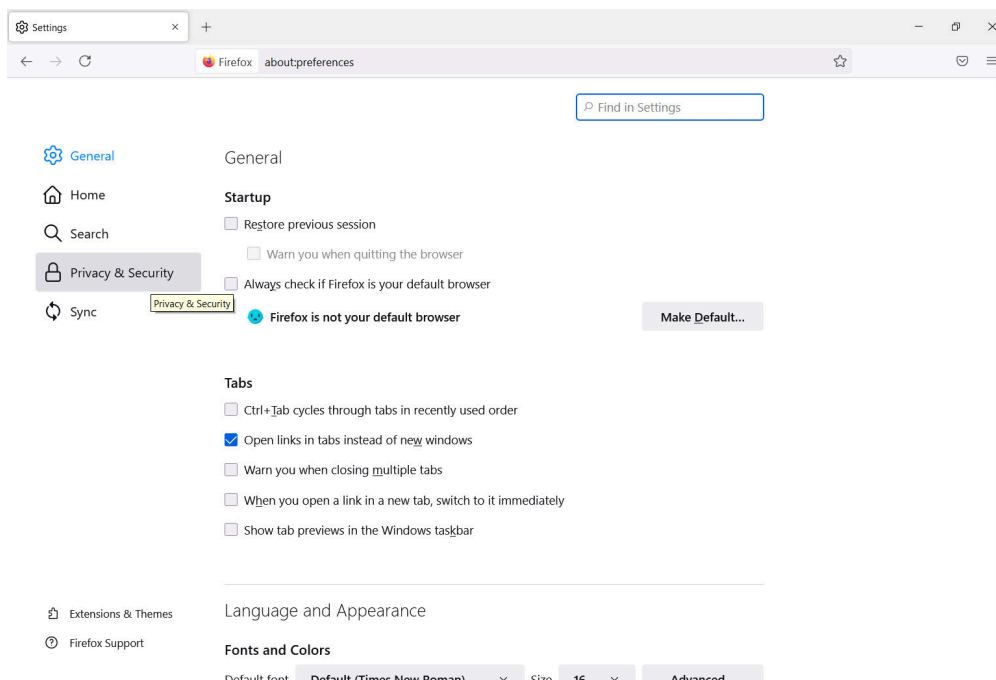
(72) Mark "Trust this CA to identify websites"

5.2.2 Install Client Certificates

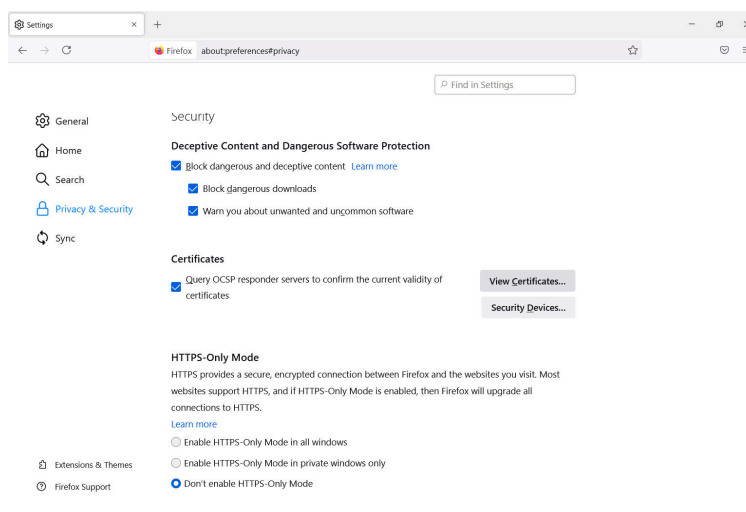
Double-click on the certificate with the .p12 extension and follow the installation instructions below:



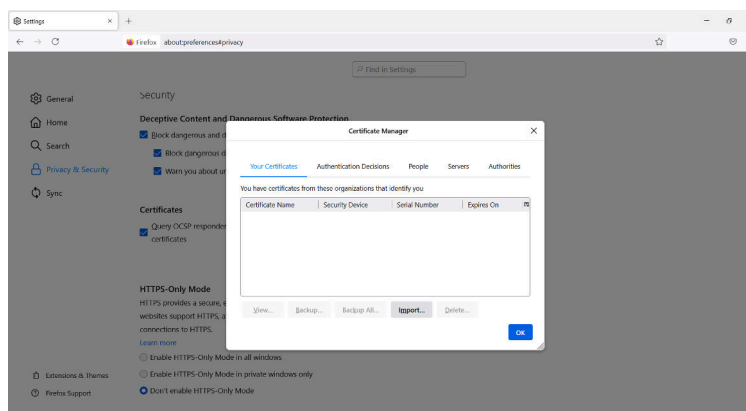
(73) Go to Settings



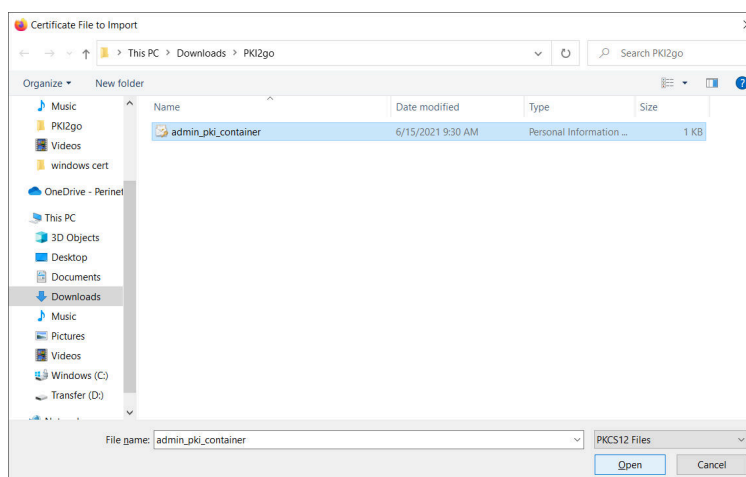
(74) Select Privacy & Security



(75) Click on *View Certificates...*



(76) Select *Import...* on *Your Certificates* tab

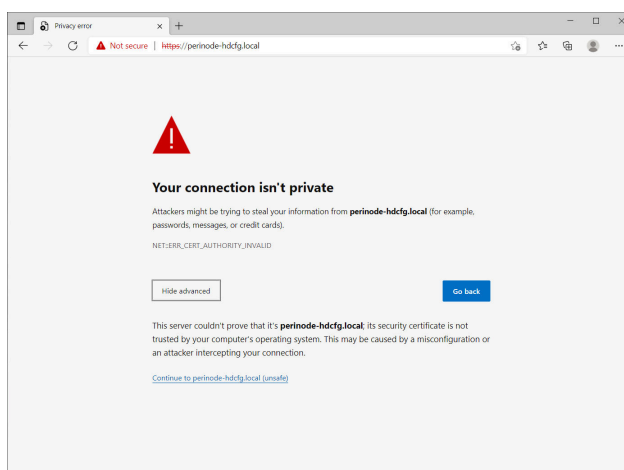


(77) Double-click on the *admin_pki_container.p12*

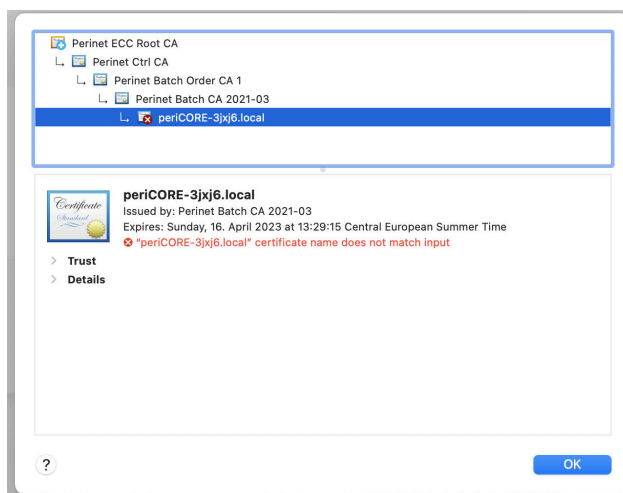
6 Security Warnings

Once the Perinet ECC Root CA or the application Root CA generated by PKI2go certificate is installed correctly in the system, no security warnings or alerts are expected. However, if **Root certificate** is not installed and/or is not marked as trusted by the browser, warnings will be displayed when accessing periNODEs or periMICA containers.

Examples of warning messages that browsers can display:



(78) Edge does not recognize the authority



(79) Safari does not recognize the hostname

7 Contact & Support

For customer support, please call us at **+49 30 863 206 701** or send an e-mail to *support@perinet.io*.

For complete contact information visit us at www.perinet.io

Revision History

Revision	Date	Author(s)	Description
1.0	August 31, 2021	Mihaela Sendrea	Initial release