

Starter Kit Plus

Security Certificates Installation Guide

February 10, 2022



Contents

1	Introduction	3
2	Windows	4
2.1	Install demo-root-ca.crt	4
2.2	Install admin_pki_container.p12	8
3	macOS	11
3.1	Install demo-root-ca.crt	11
3.2	Install admin_pki_container.p12	13
4	iOS and iPadOS	14
4.1	Install demo-root-ca.crt	14
4.2	Install admin_pki_container.p12	17
5	Linux (Ubuntu, Debian)	18
5.1	Install demo-root-ca.crt	18
5.2	Install admin_pki_container.p12	22
6	Troubleshooting	25
7	Contact & Support	26

1 Introduction

Perinet Smart Components and periMICA containers received in this kit are authenticating themselves with certificates signed by a **demo root CA** that was created by Perinet for demonstration purposes.

Client certificates are used for providing access control, in order to keep both data communication and configuration of the network devices secure.

To access the Smart Components and the containers included in the Starter Kit Plus, please install the two security certificates downloaded from the **GettingStarted** container. Please go to the section of your operating system in this guide and follow the indicated steps to install the *demo-root-ca.crt* and the *admin_pki_container.p12* certificates.

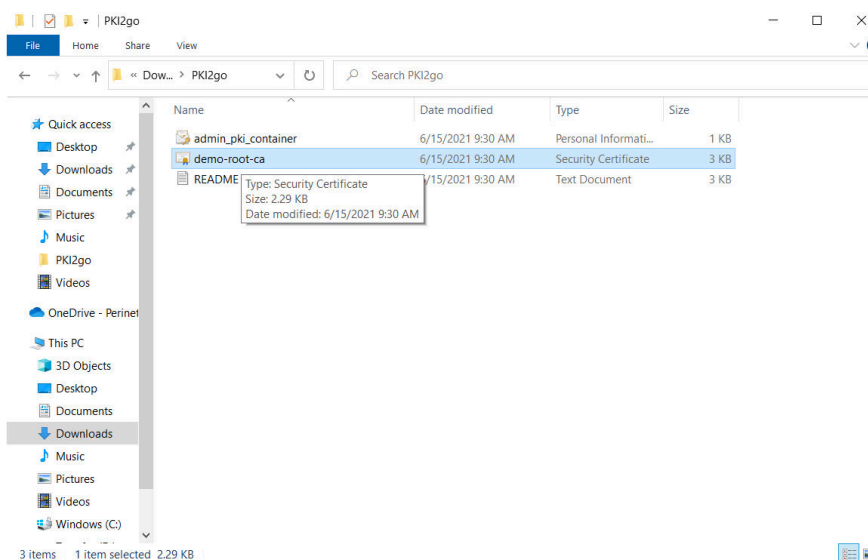
For further information on security concepts, please refer to <https://docs.perinet.io>.

2 Windows

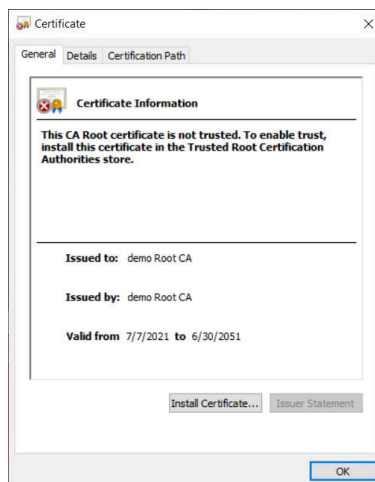
This section describes how to install **demo-root-ca.crt** and **admin_pki_container.p12** certificates on Windows systems.

2.1 Install demo-root-ca.crt

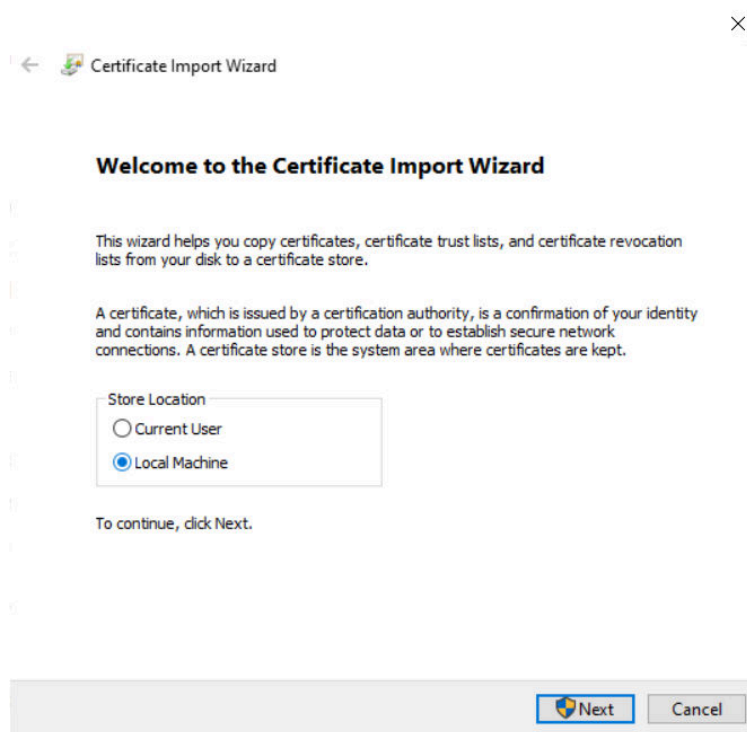
Double-click on the file and follow the installation instructions below:



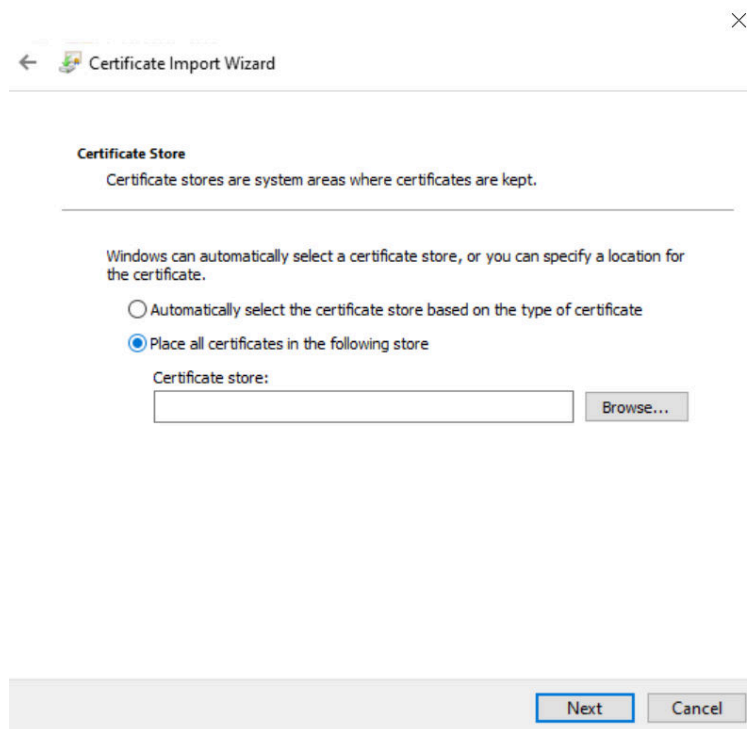
(1) Double Click on *demo-root-ca.crt*



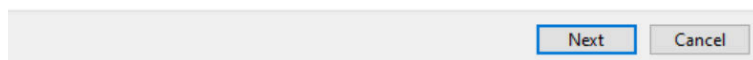
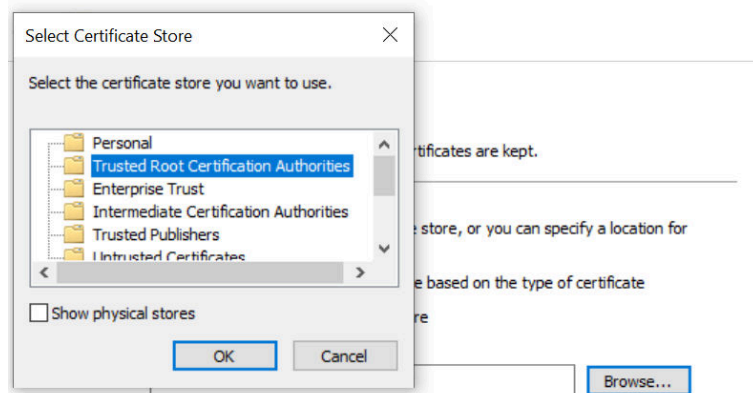
(2) Select *Install Certificate...*



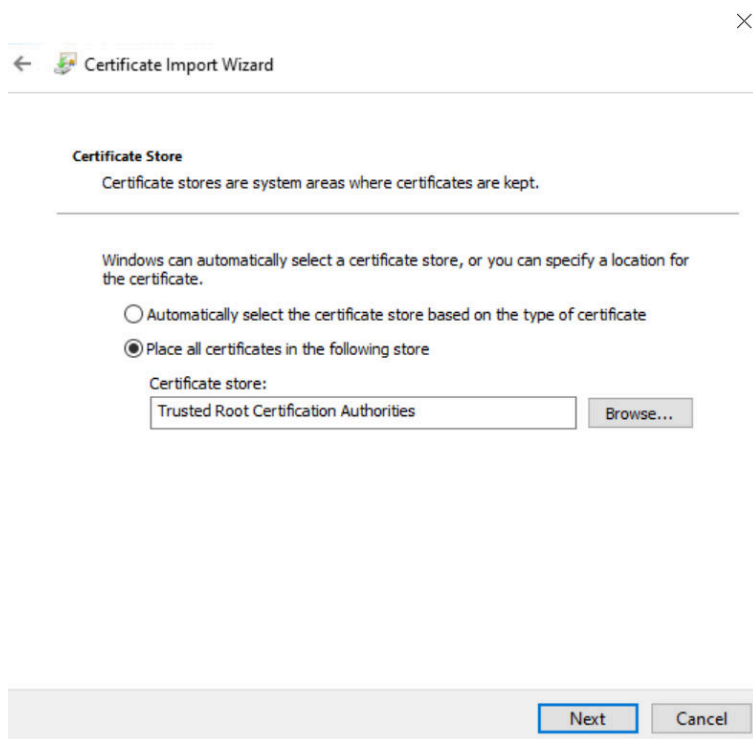
(3) Select *Local Machine*



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



(5) Select *Trusted Root Certification Authorities*



(6) 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

(7) 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

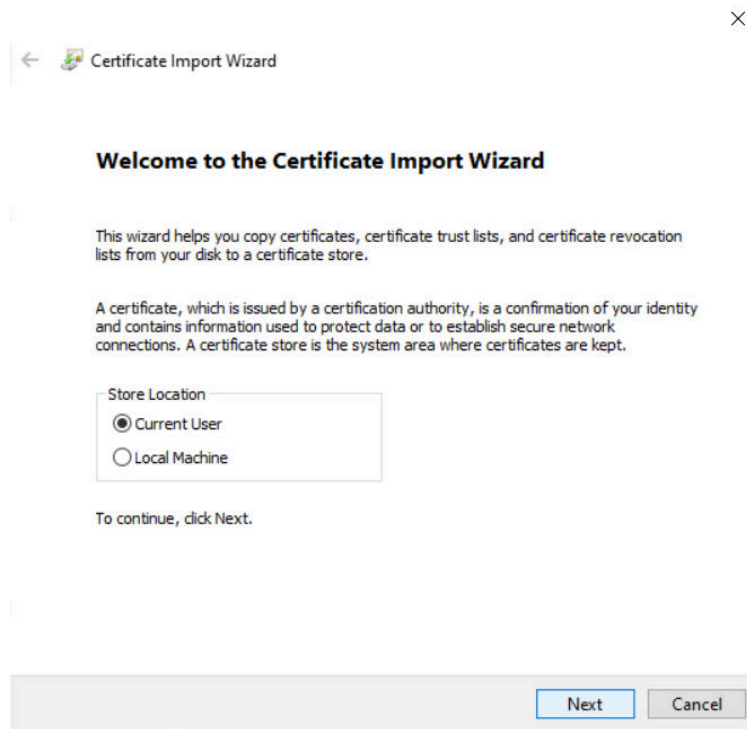
Finish

Cancel

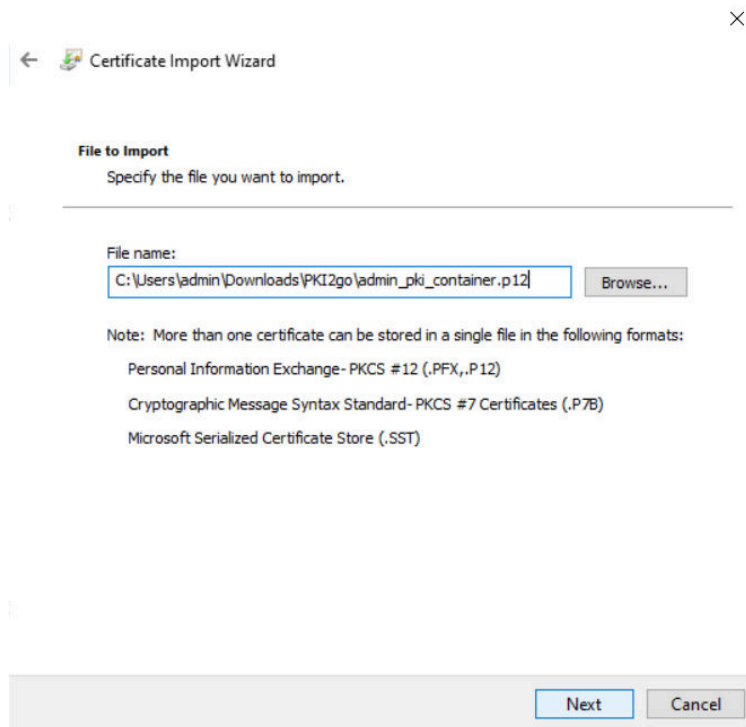
(8) Click *Finish*

2.2 Install admin_pki_container.p12

Double-click on the *admin_pki_container.p12* file and follow the installation instructions below:



(9) Select *Current User*



← Certificate Import Wizard

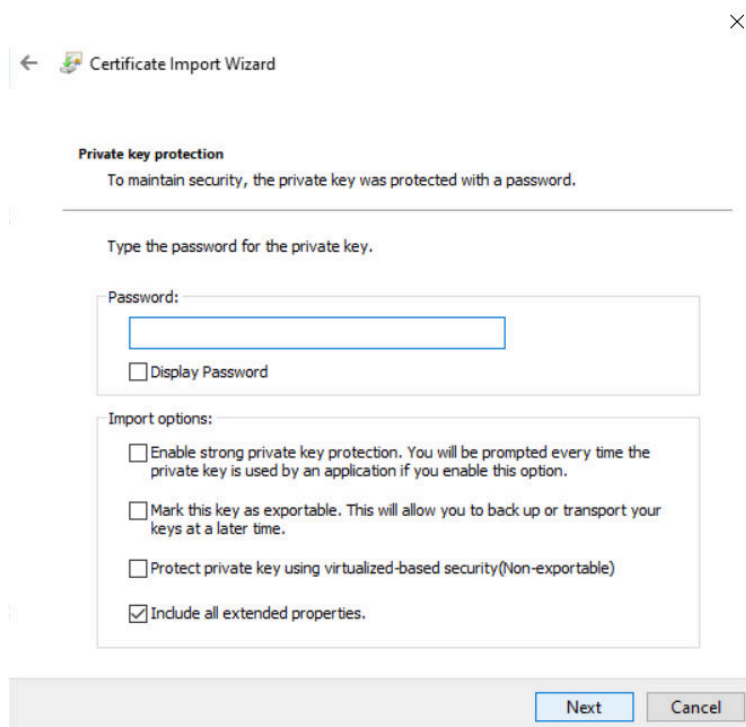
File to Import
Specify the file you want to import.

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

(10) 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.

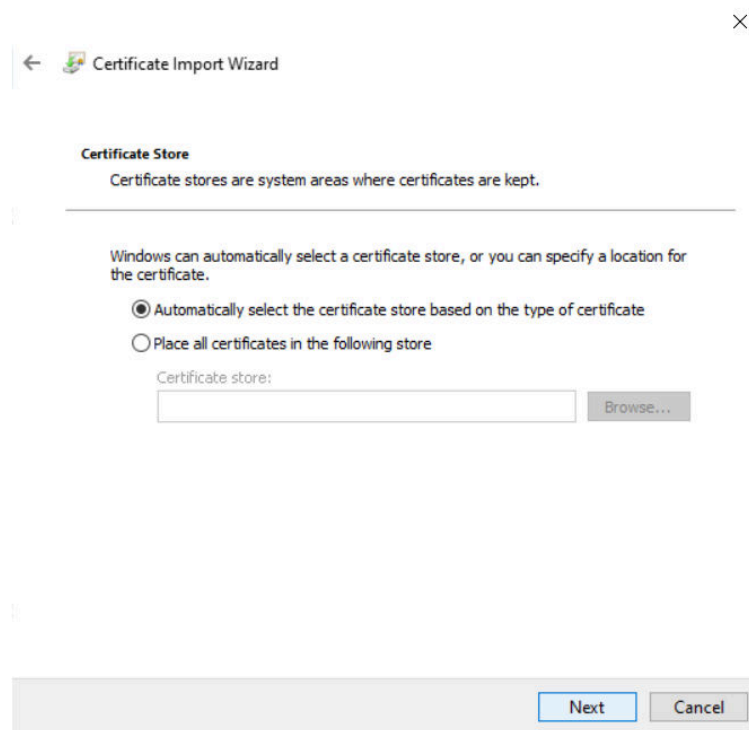
Password:

☐ 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

(11) Type the password: *admin_pki_container*



(12) Click Next

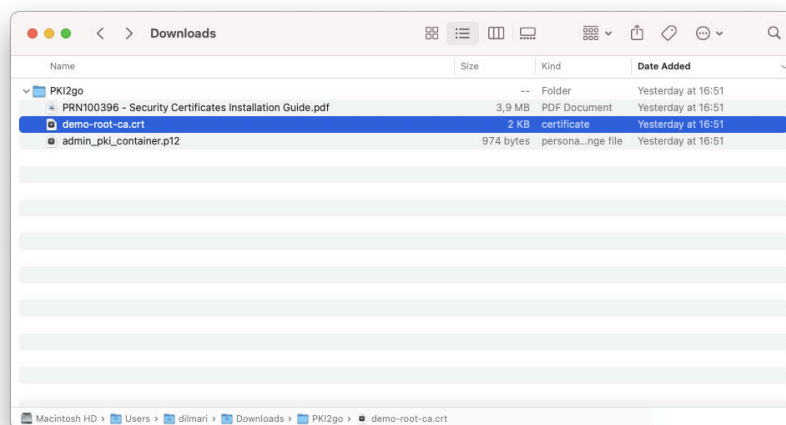
Note: Please restart your browser after installing the certificates.

3 macOS

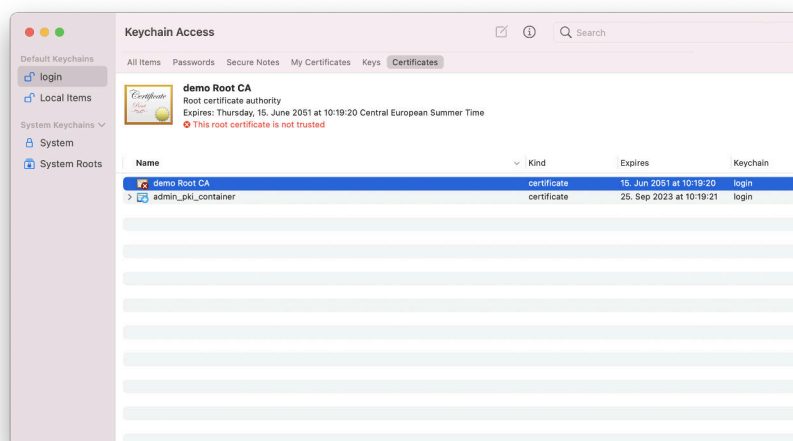
This section describes how to install **demo-root-ca.crt** and **admin_pki_container.p12** certificates on macOS systems.

3.1 Install demo-root-ca.crt

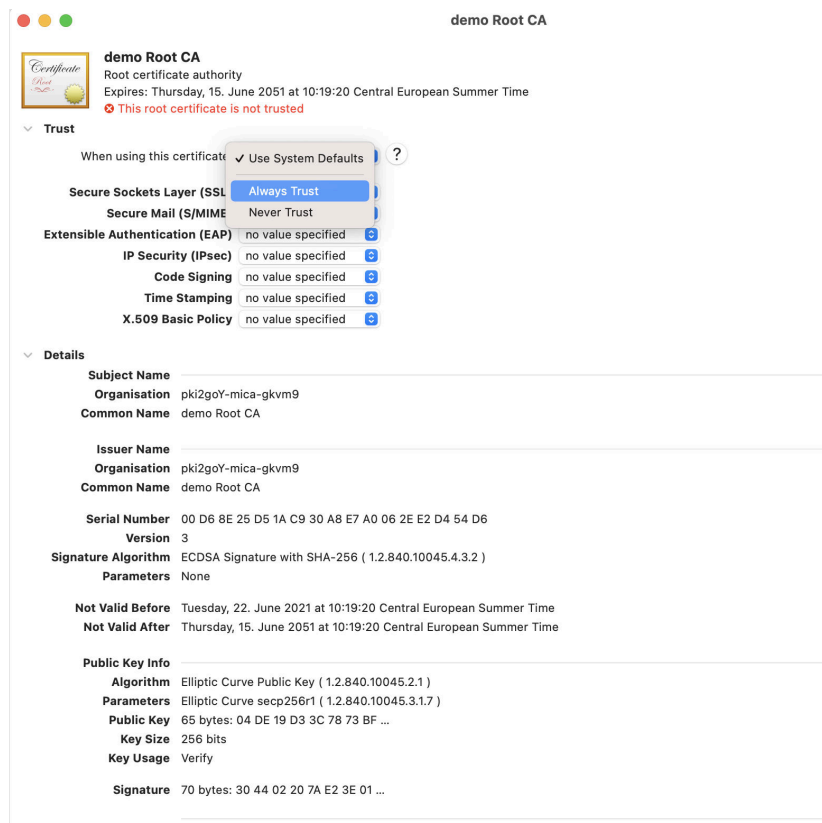
Double-click on the file and follow the installation instructions below:



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



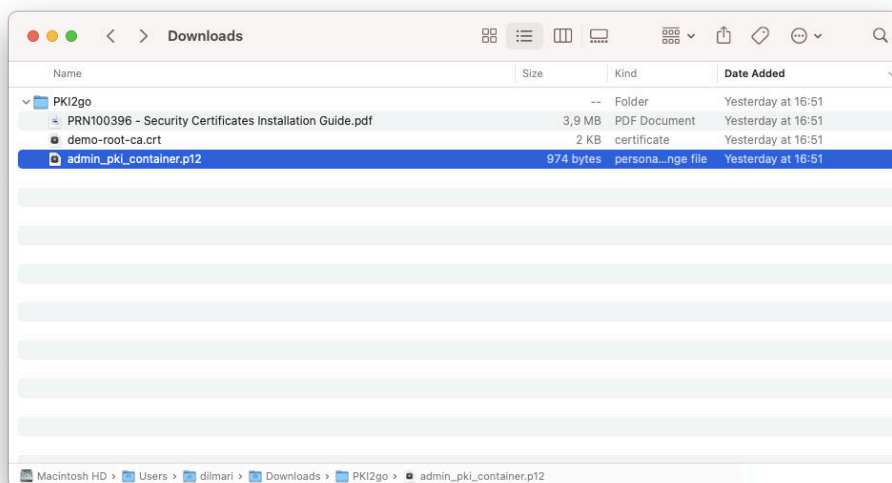
(14) Double-click on *demo Root CA*



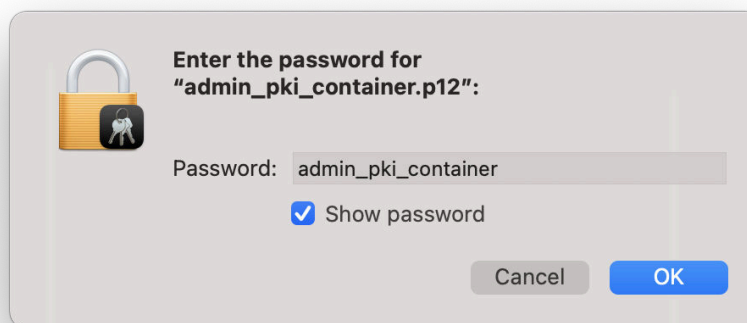
(15) Select Always Trust

3.2 Install admin_pki_container.p12

Double-click on the *admin_pki_container.p12* file and follow the installation instructions below:



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



(17) Type the password: *admin_pki_container*

Note: Please restart your browser after installing the certificates.

4 iOS and iPadOS

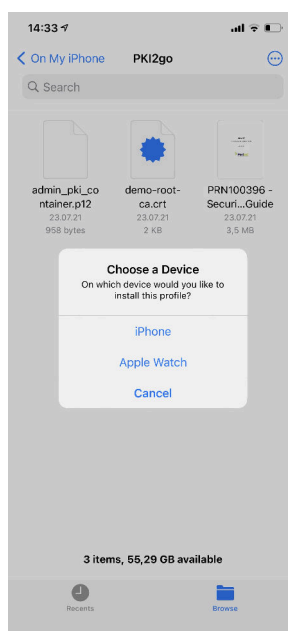
This section describes how to install **demo-root-ca.crt** and **admin_pki_container.p12** certificates on iOS and iPadOS systems.

4.1 Install demo-root-ca.crt

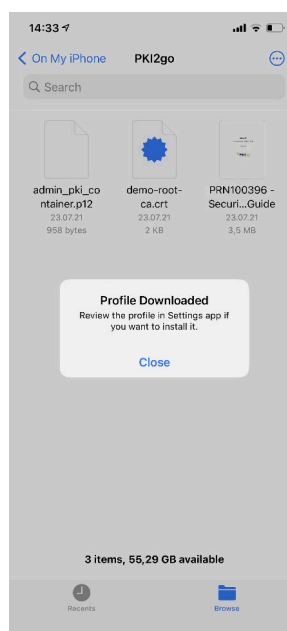
Open the **Files** app, find the downloaded folder **PKI2go** and click on **demo-root-ca.crt**. Then follow the instructions according to the pictures below:



(18) Click on **demo-root-ca.crt**

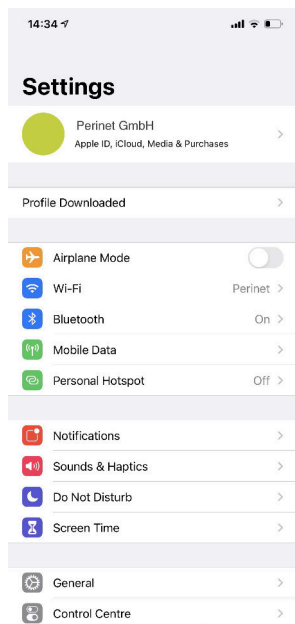


(19) Choose the device

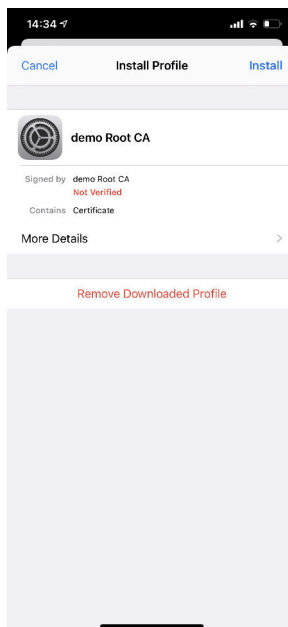


(20) Click on **Close**

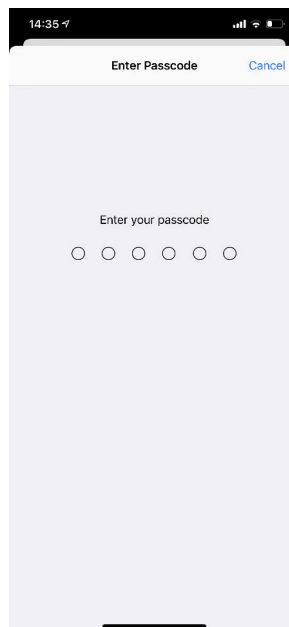
Open the **Settings** app and follow the installation instructions below:



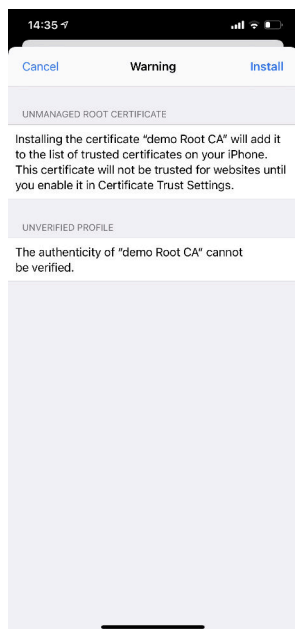
(21) Click on *Profile Downloaded*



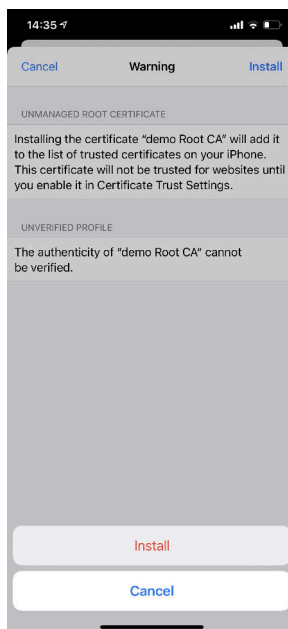
(22) Click on *Install*



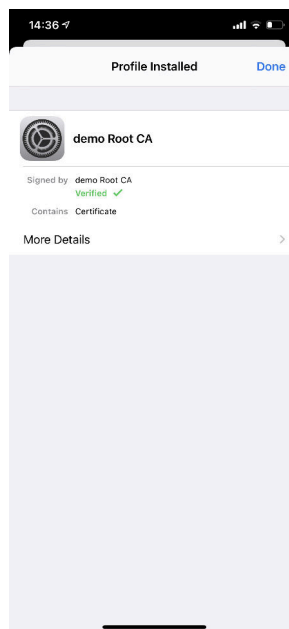
(23) Enter the passcode (user passcode)



(24) Click on *Install*

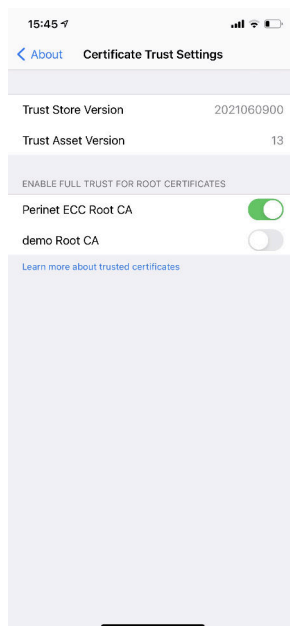


(25) Click on *Install*

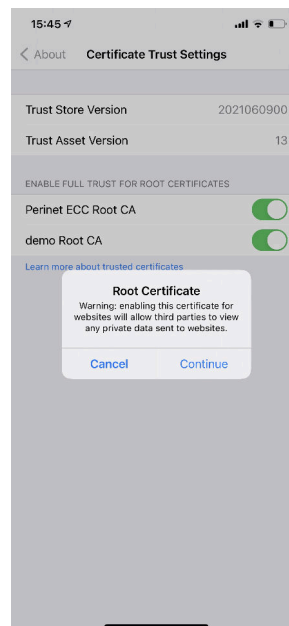


(26) Click on *Done*

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:



(27) Enable the demo Root CA



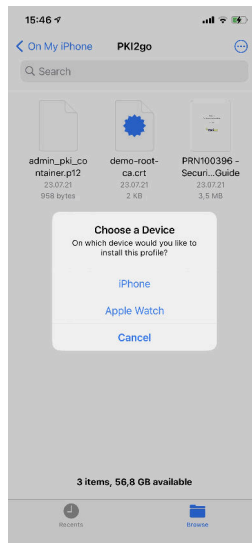
(28) Click on *Continue*

4.2 Install admin_pki_container.p12

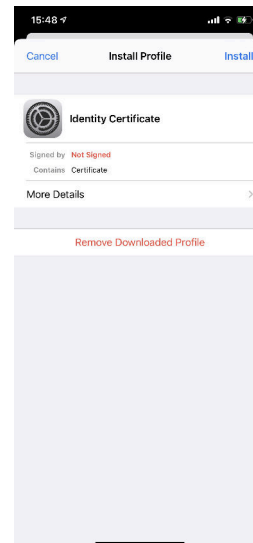
Open the *Files* app and find the downloaded file. Click on the **admin_pki_container.p12** and follow the installation instructions:



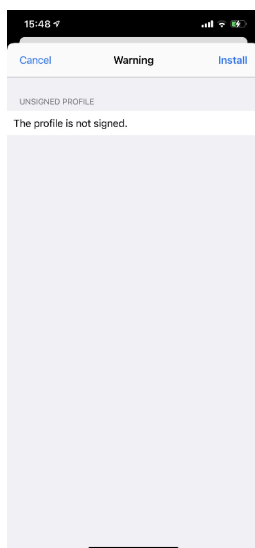
(29) Click on *admin_pki_container.p12*



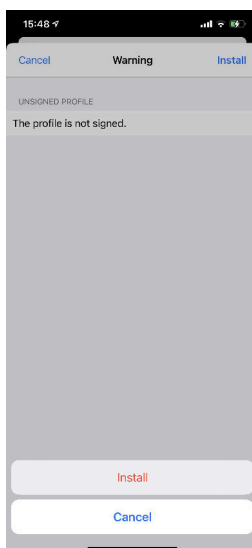
(30) Choose a Device



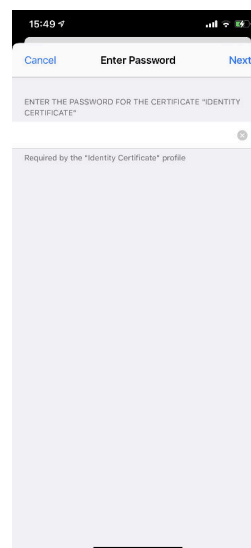
(31) Click on *Install*



(32) Click on *Install*



(33) Click on *Install*



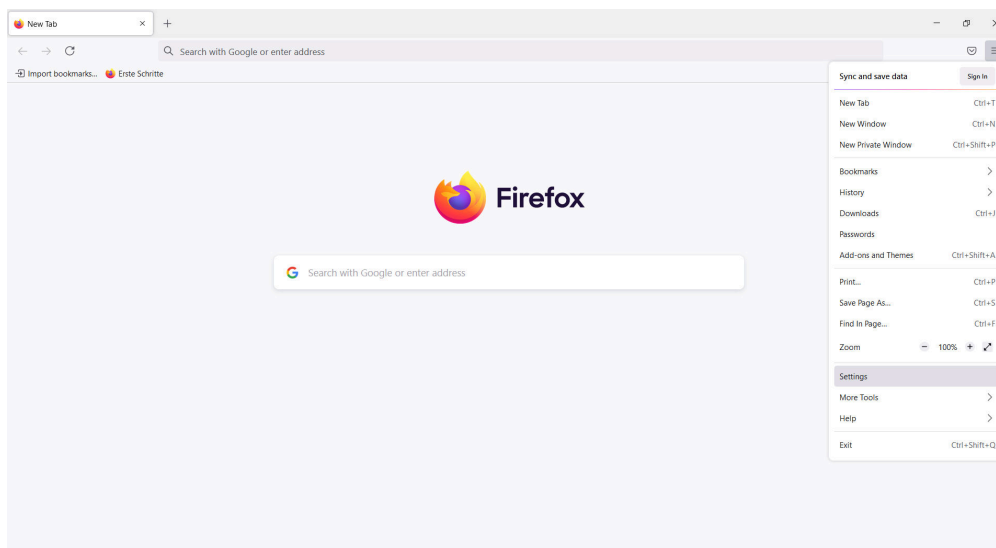
(34) Type the password (*admin_pki_container*) and click on *Next*

5 Linux (Ubuntu, Debian)

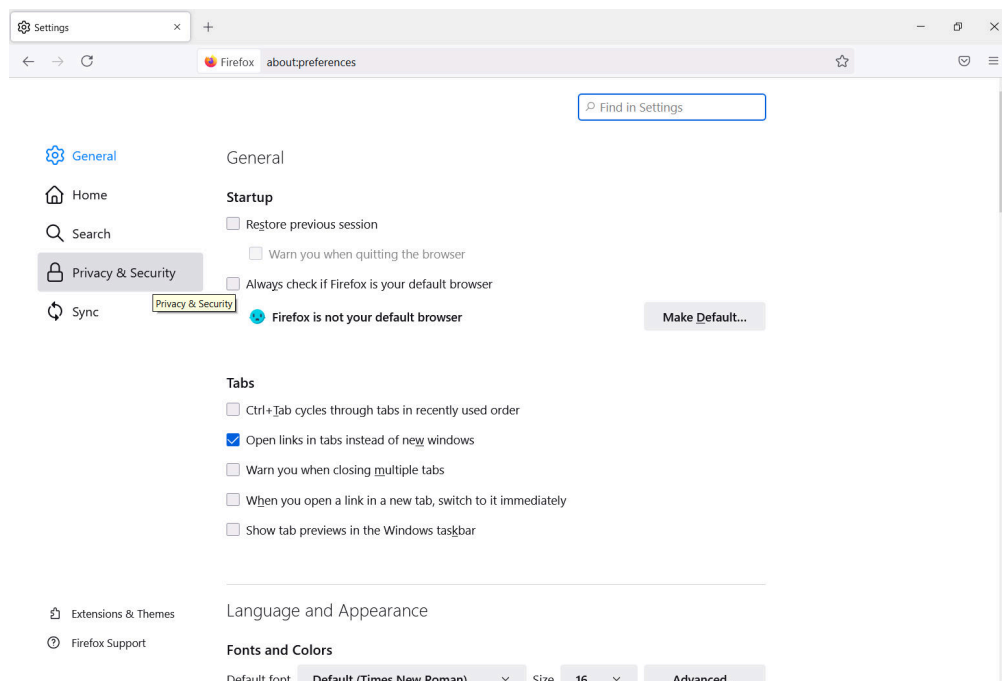
This section describes how to install **demo-root-ca.crt** and **admin_pki_container.p12** certificates on Linux (Ubuntu, Debian) systems. The example below is for Firefox browser:

5.1 Install demo-root-ca.crt

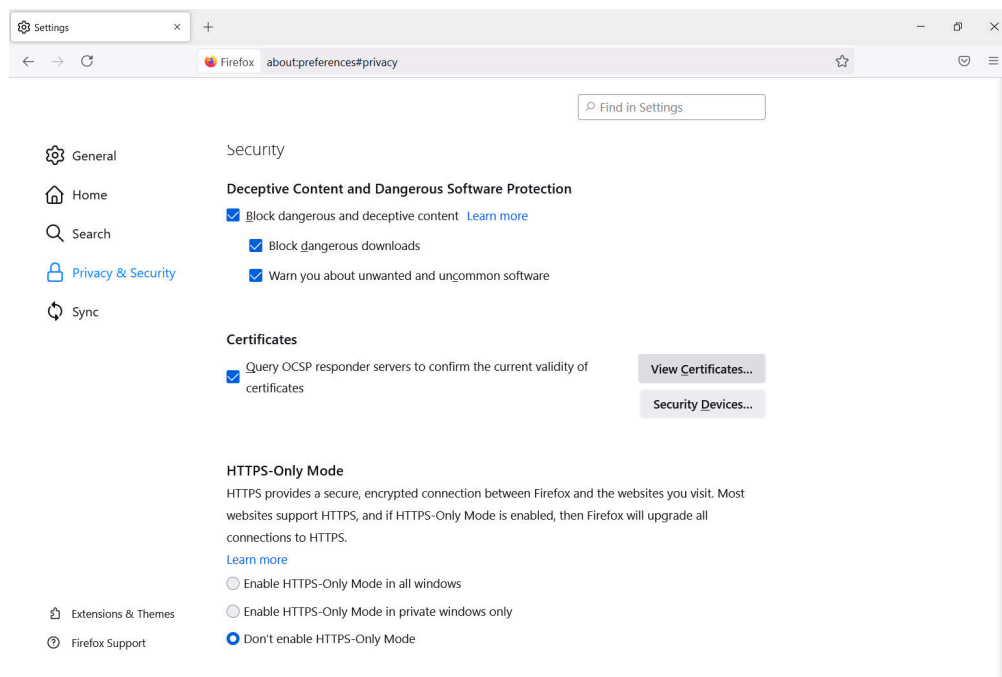
In the Menu, go to **Settings** and follow the installation instructions below:



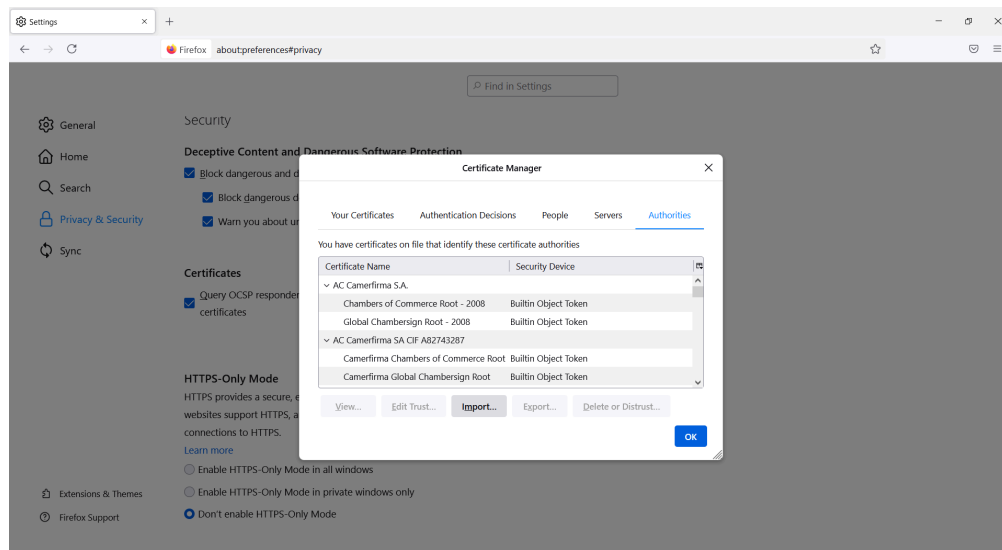
(35) Go to *Settings*



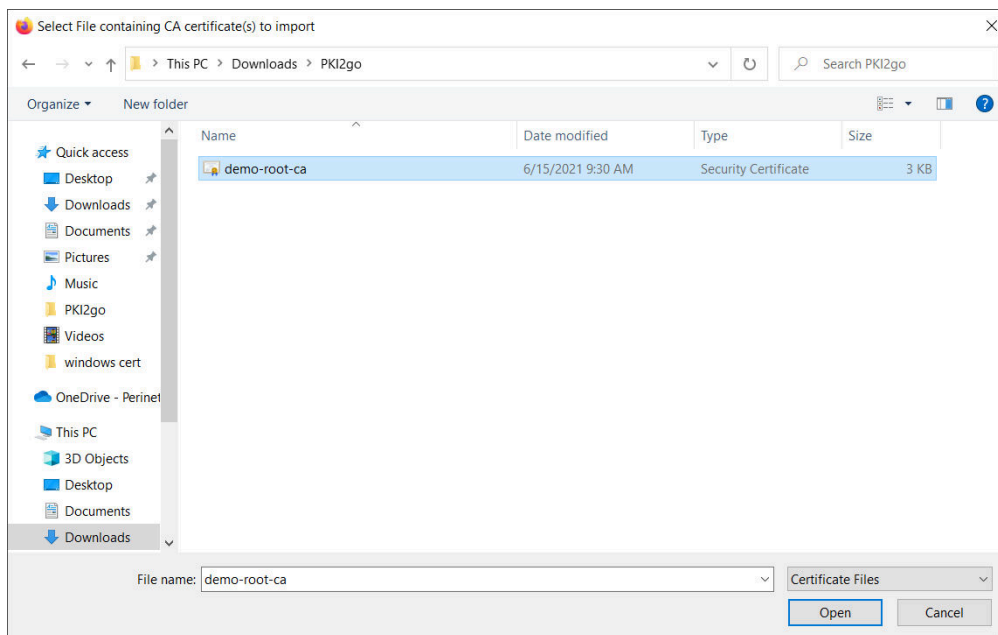
(36) Select *Privacy & Security*



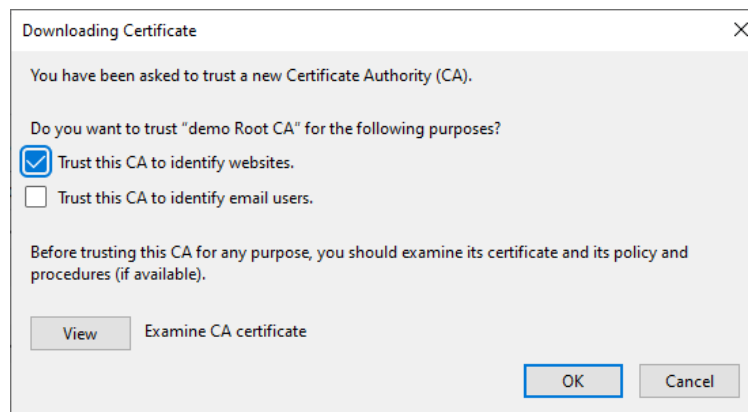
(37) Click on *View Certificates...*



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



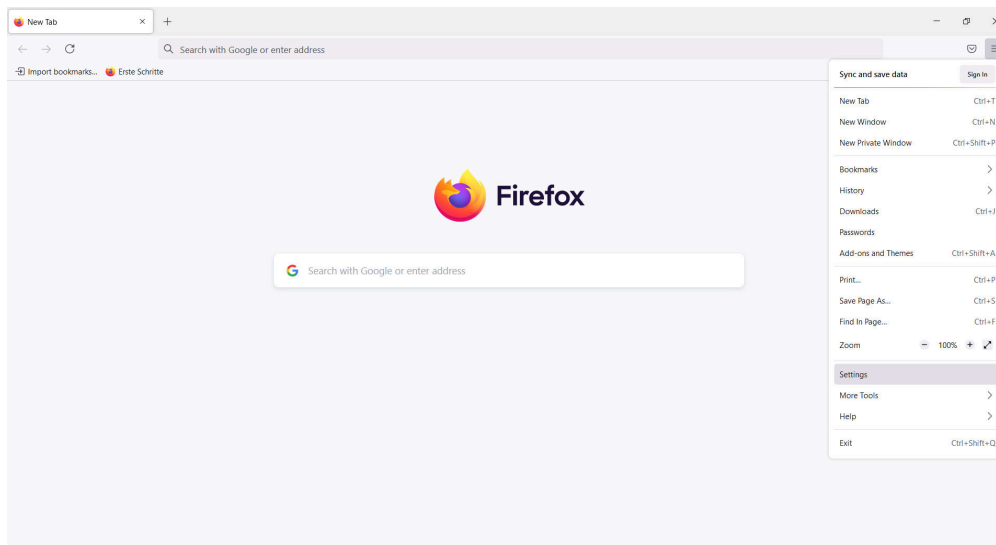
(39) Double-click on the *demo-root-ca.crt*



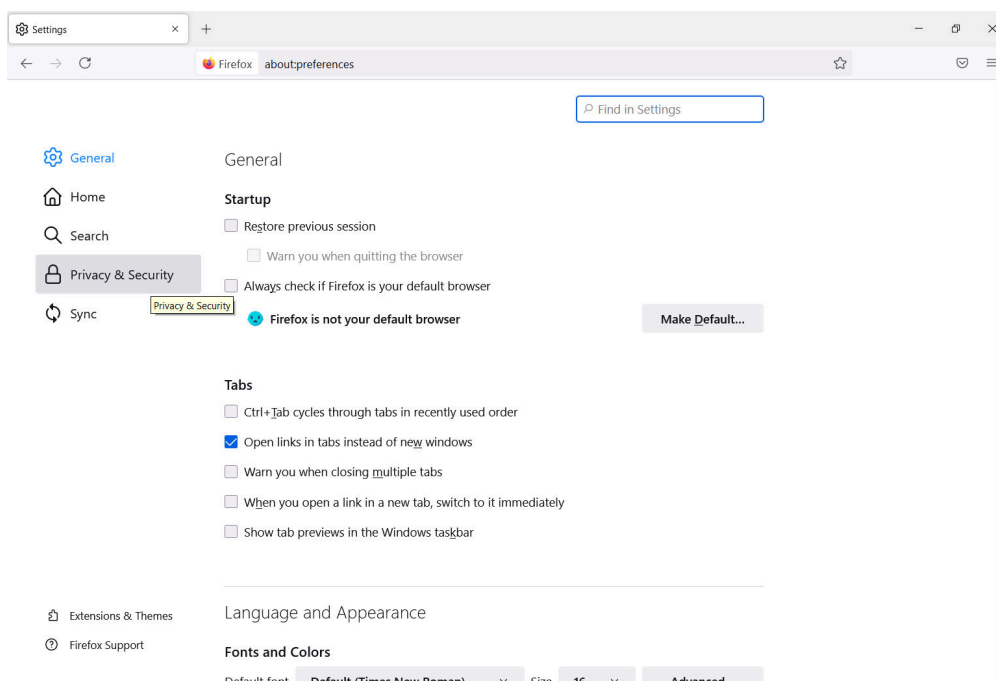
(40) Mark *Trust this CA to identify websites*

5.2 Install admin_pki_container.p12

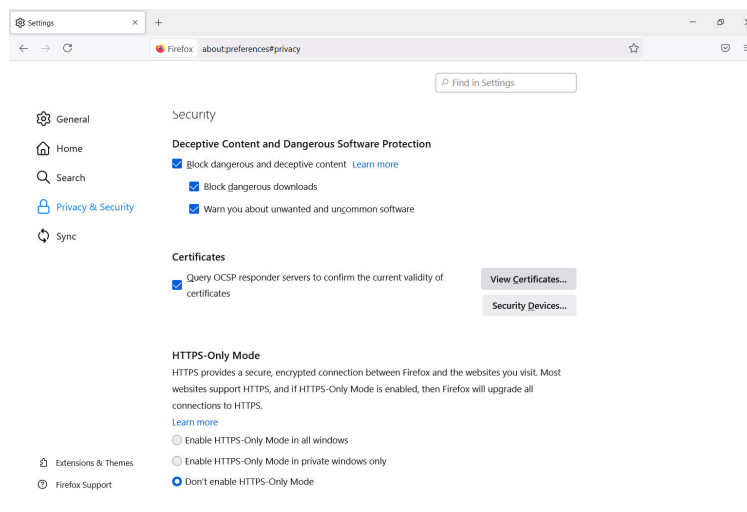
Double-click on *admin_pki_container.p12* and follow the installation instructions below.



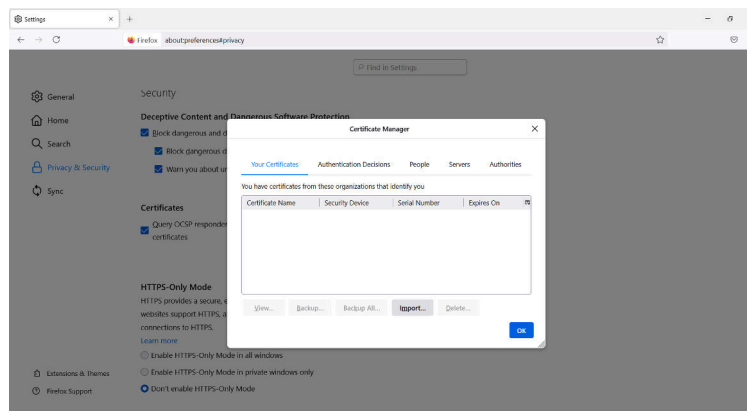
(41) Go to Settings



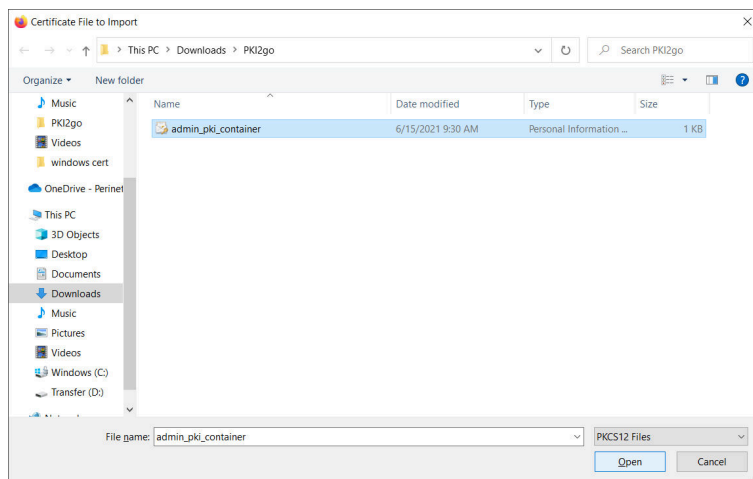
(42) Select Privacy & Security



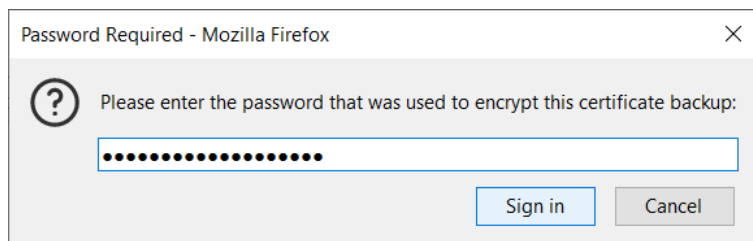
(43) Click on *View Certificates...*



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



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



(46) Type the password *admin_pki_container* and click *Sign in*

Note: Please restart your browser after the certificates installation.

6 Troubleshooting

- Browsers can cache SSL certificates in order to speed up the access. But caching can cause issues, because a protected server will refuse the connection if the browser sent the incorrect certificate. In that case, refreshing the web page might help. If the problem still occurs, make sure to have the correct client certificates imported and restart the browser.
- When the periMICA is not able to reach any NTP (Network Time Protocol) server, its Time & Date are not automatically synchronized and it can generate security errors when trying to access the containers installed. To fix this problem you can configure the Time & Date manually in *periMICA Homepage* → *Settings* → *Time & Date*.

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	February, 9, 2022	Dilmari Seidel Heuer	Initial release