

SafeDNS Root Certificate For HTTPS Pages

About the certificate

Root certificate or **SSL certificate** is the main part of the website security. SSL certificate is required for the correct operation of sites with a secure (HTTPS) connection. If you have issues with displaying the SafeDNS block page (your internet browser shows a message "Unable to access the site"), you need to download a SafeDNS certificate and configure it to use in your browser.

Please note that the certificate should be installed on each end device where you want HTTPS pages to display correctly.

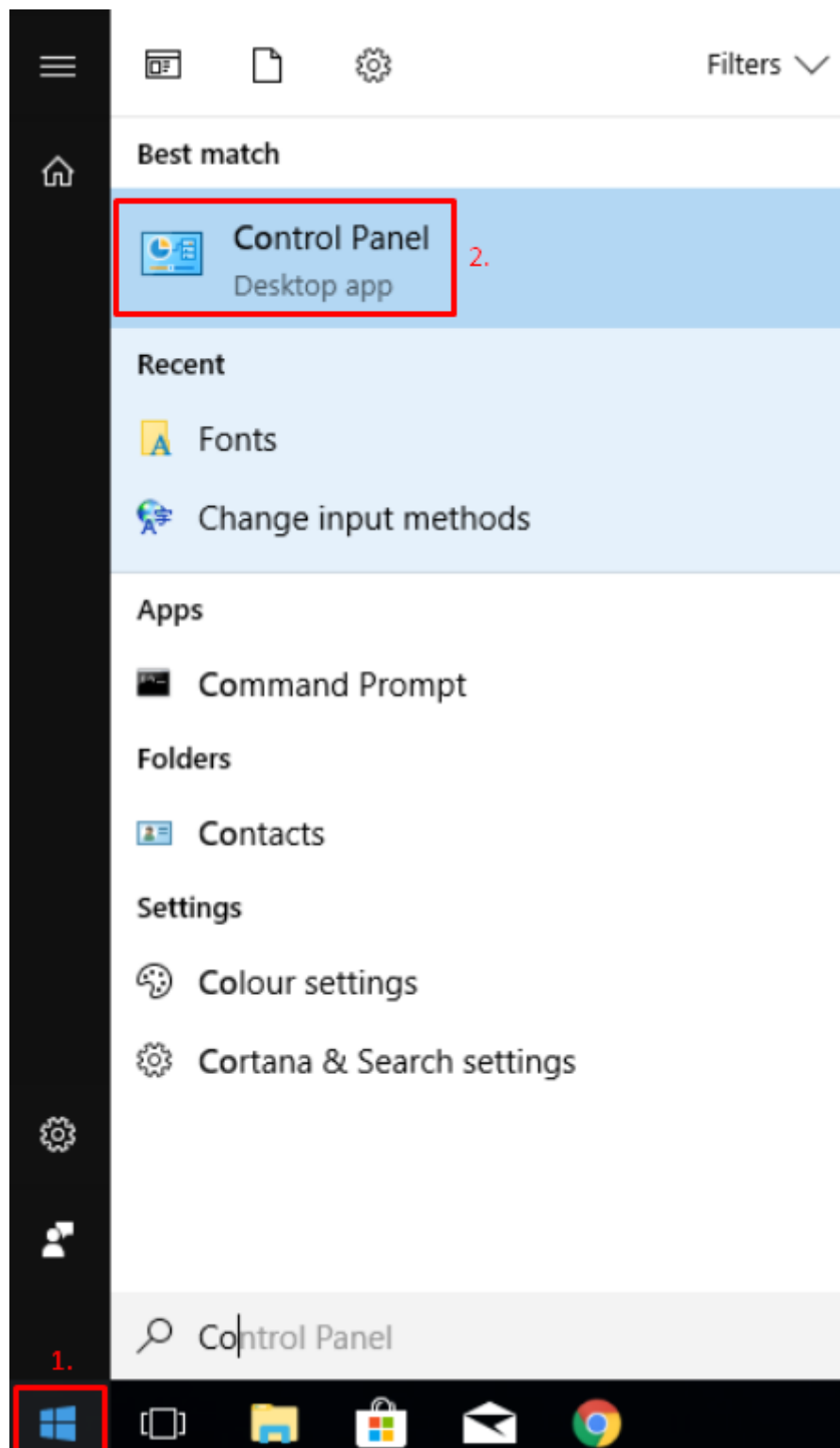
[Download SafeDNS certificate](#)

If the browser starts installing the certificate after you click on the button, cancel it, right-click on the button and choose "**Save as...**"

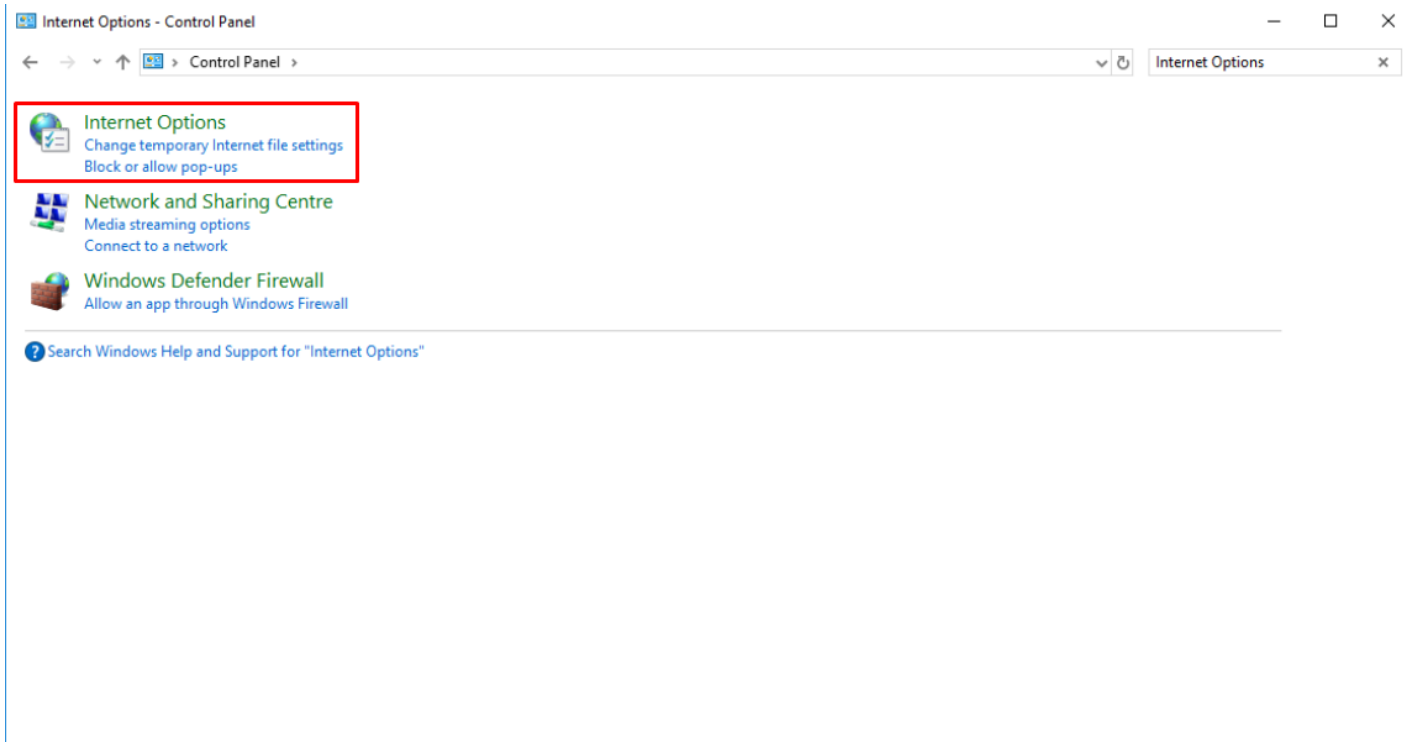
Windows (Chrome, Edge, Opera browsers)

For Mozilla Firefox, see the next section.

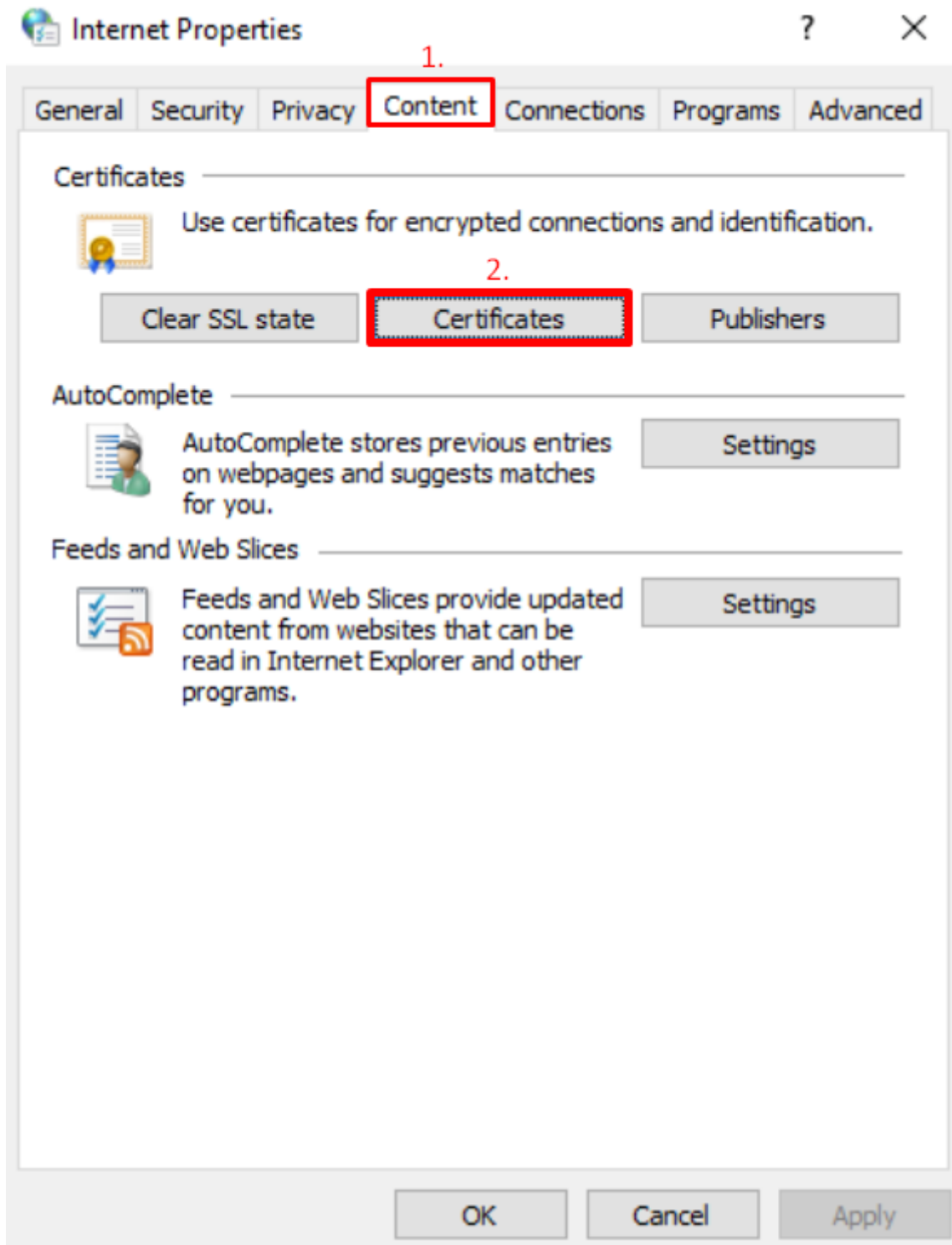
1. Open the **Start menu**, type in '**Control Panel**', and open the suggested app.



2. Open **Internet Options**.



3. Navigate to the **Content** tab and click **Certificates**.



4. Navigate to the **Trusted Root Certification Authorities** tab, and click **Import**.

Intended purpose:

<All>

1.



Intermediate Certification Authorities

Trusted Root Certification Authorities

Trusted Publ



Issued To	Issued By	Expiry Date	Friendly Name
AddTrust External ...	AddTrust External CA...	30/05/2020	The USERTrust ...
Baltimore CyberTru...	Baltimore CyberTrust ...	12/05/2025	DigiCert Baltimor...
Certum CA	Certum CA	11/06/2027	Certum
Certum Trusted Ne...	Certum Trusted Netw...	31/12/2029	Certum Trusted ...
Class 3 Public Prima...	Class 3 Public Primary ...	01/08/2028	VeriSign Class 3 ...
Copyright (c) 1997 ...	Copyright (c) 1997 Mi...	30/12/1999	Microsoft Timest...
DigiCert Global Roo...	DigiCert Global Root CA	10/11/2031	DigiCert
DigiCert High Assur...	DigiCert High Assuran...	10/11/2031	DigiCert
Equifax Secure Cer...	Equifax Secure Certifi...	22/08/2018	GeoTrust

2.

Import...

Export...

Remove

Advanced

Certificate intended purposes

View

Close

5. Click **Next** in **Certificate Import Wizard**.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Next

Cancel

6. Click **Browse** and select a downloaded SafeDNS certificate file.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Users\user\Downloads\safedns.crt

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 Serialised Certificate Store (.SST)

Next

Cancel

7. Make sure that the certificate is placed in the store **Trusted Root Certification Authorities**.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

☐ Automatically select the certificate store based on the type of certificate

☒ Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Browse...

Next

Cancel

8. Close the window by clicking on **Finish**.



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
File Name	C:\Users\user\Downloads\safedns.crt

Finish

Cancel

9. Click on **Yes** when **Security Warning** appears.



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

SafeDNS Root CA

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

Thumbprint (sha1): 49C17FA5 6FD8927D 3C6C45EA 8AD1B7B1 C79AC494

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

10. Close Certificate Import Wizard by clicking **OK**.

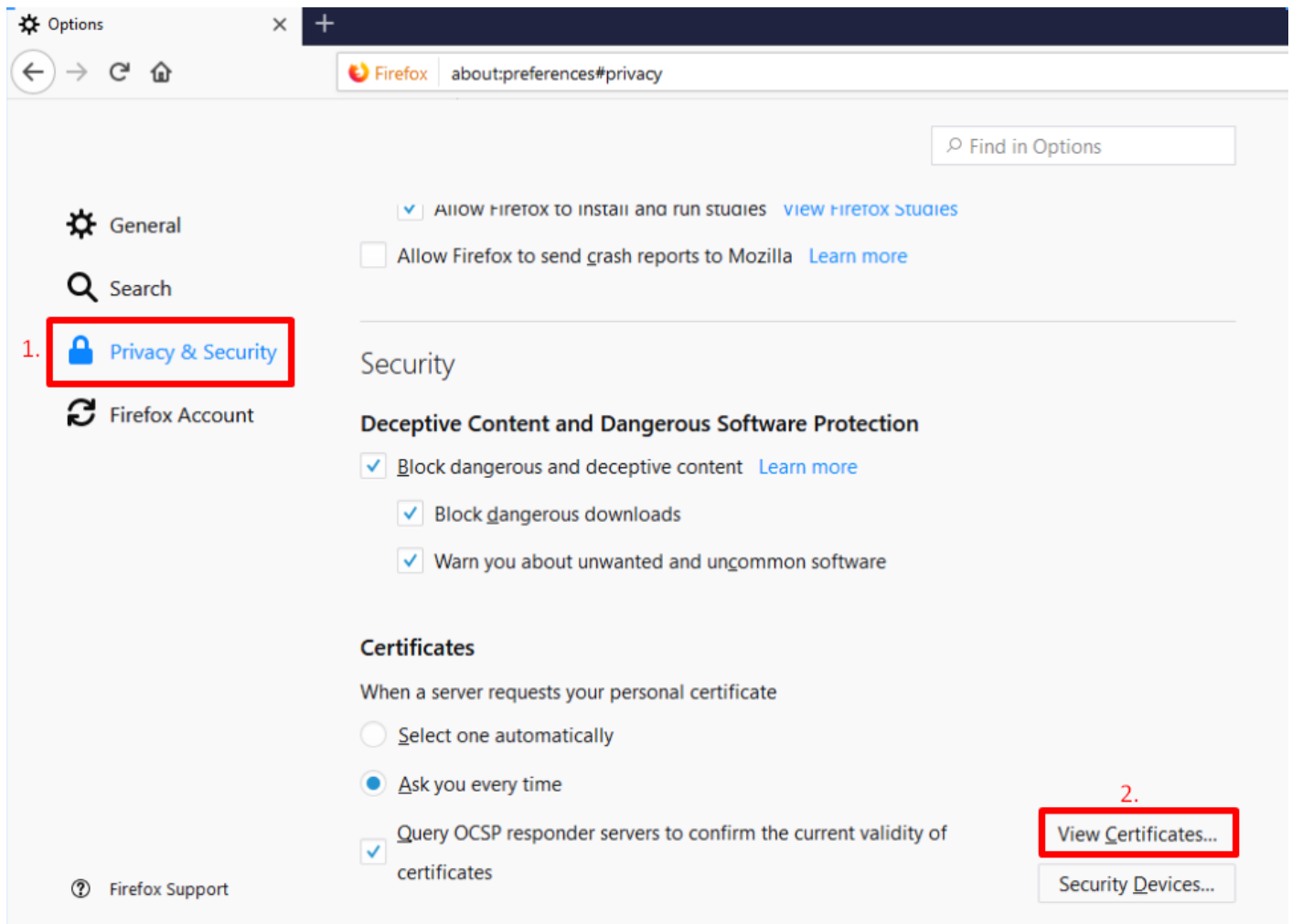


The import was successful.

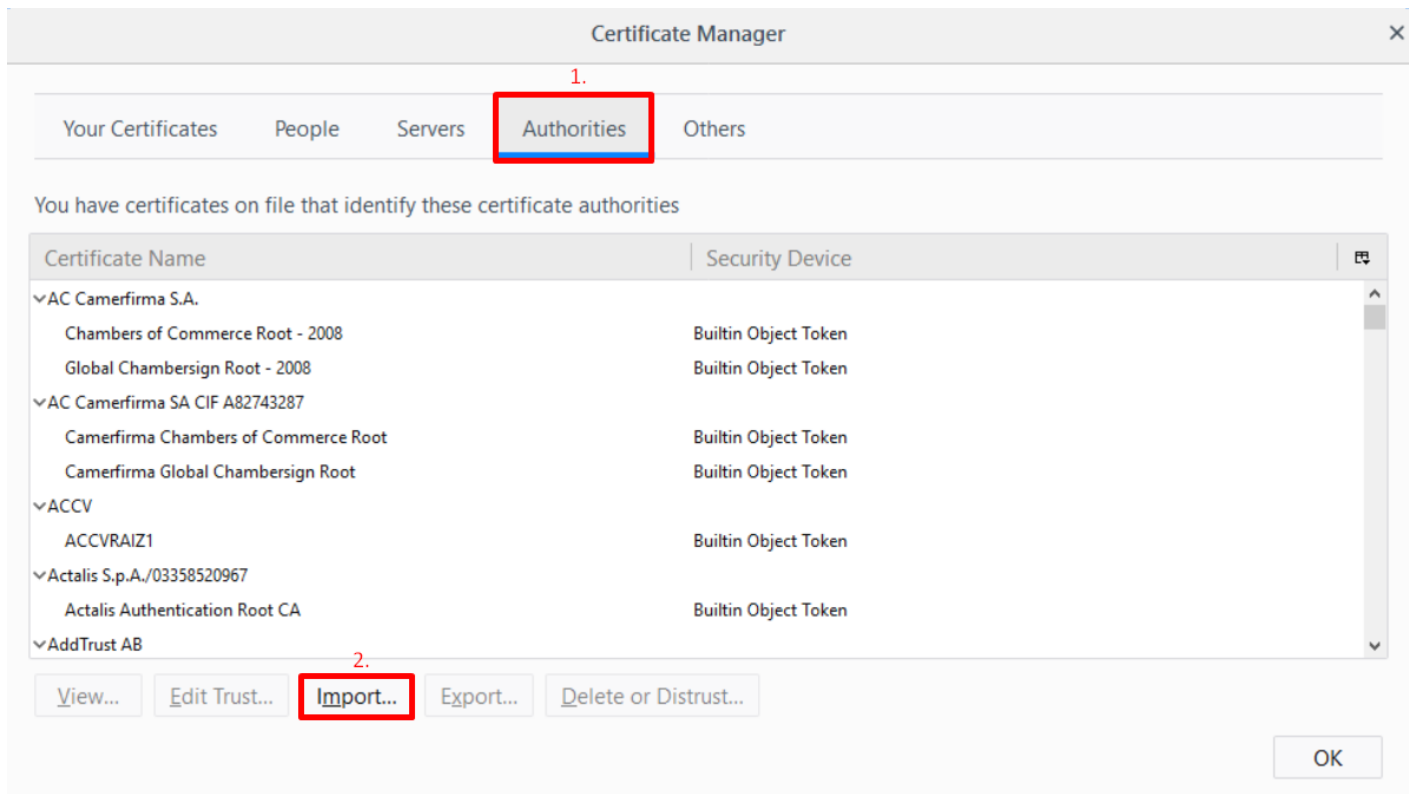
OK

Mozilla Firefox (all platforms)

1. Click on the **Menu button** in the top right corner of the browser and select **Settings**.
2. Choose **Privacy & Security** in the left menu, scroll to the bottom of the page, and click **View Certificates**.



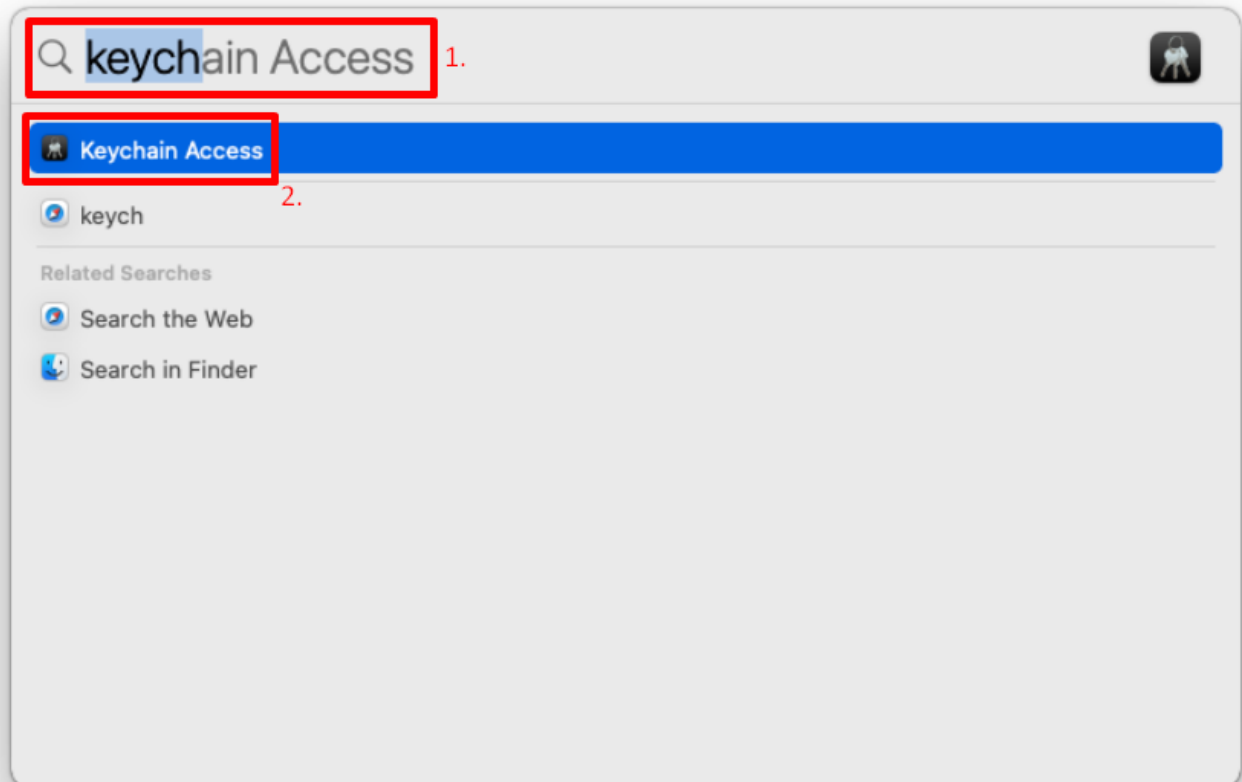
3. Select the **Authorities** tab and click **Import**.



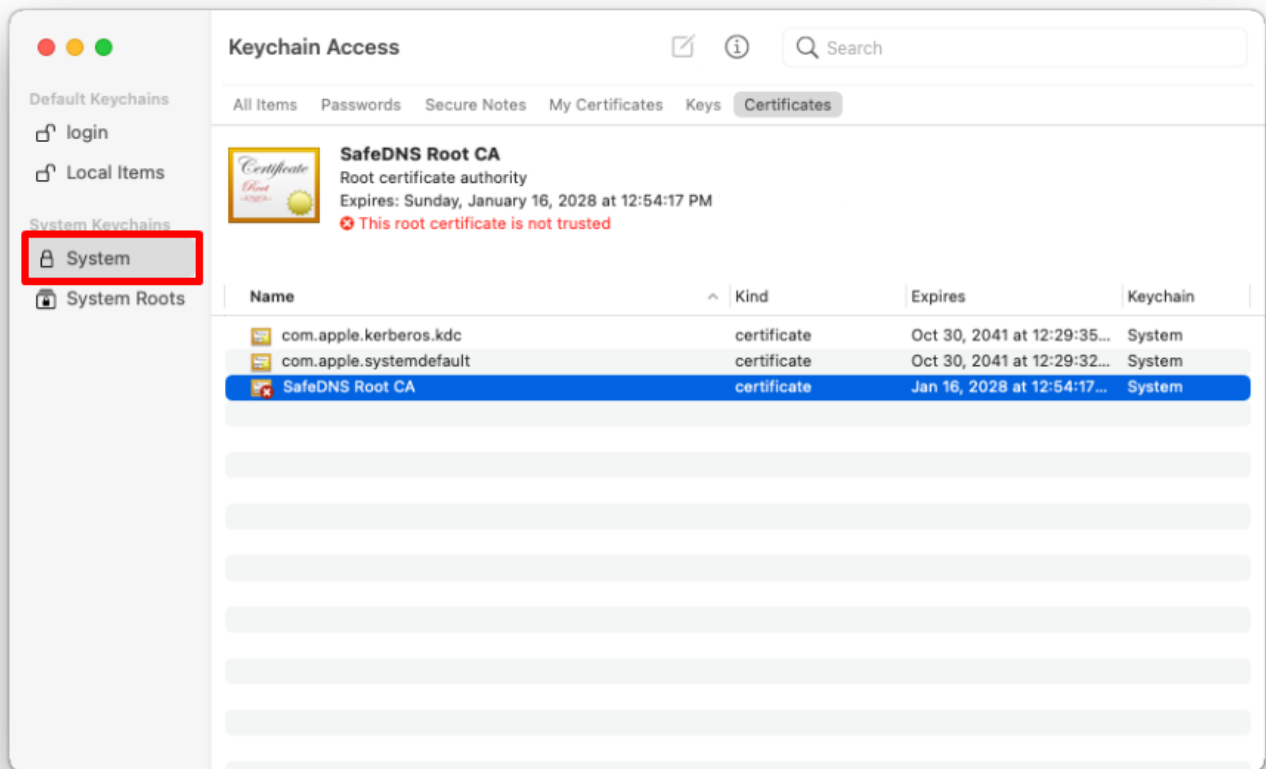
4. Select the downloaded SafeDNS Certificate, tick the box **Trust this CA to identify websites**, and click **OK**.

Mac OSX

1. Press the hotkey **CTRL + SPACE** and type '**Keychain**' in the Spotlight search. Open the **Keychain Access** application.

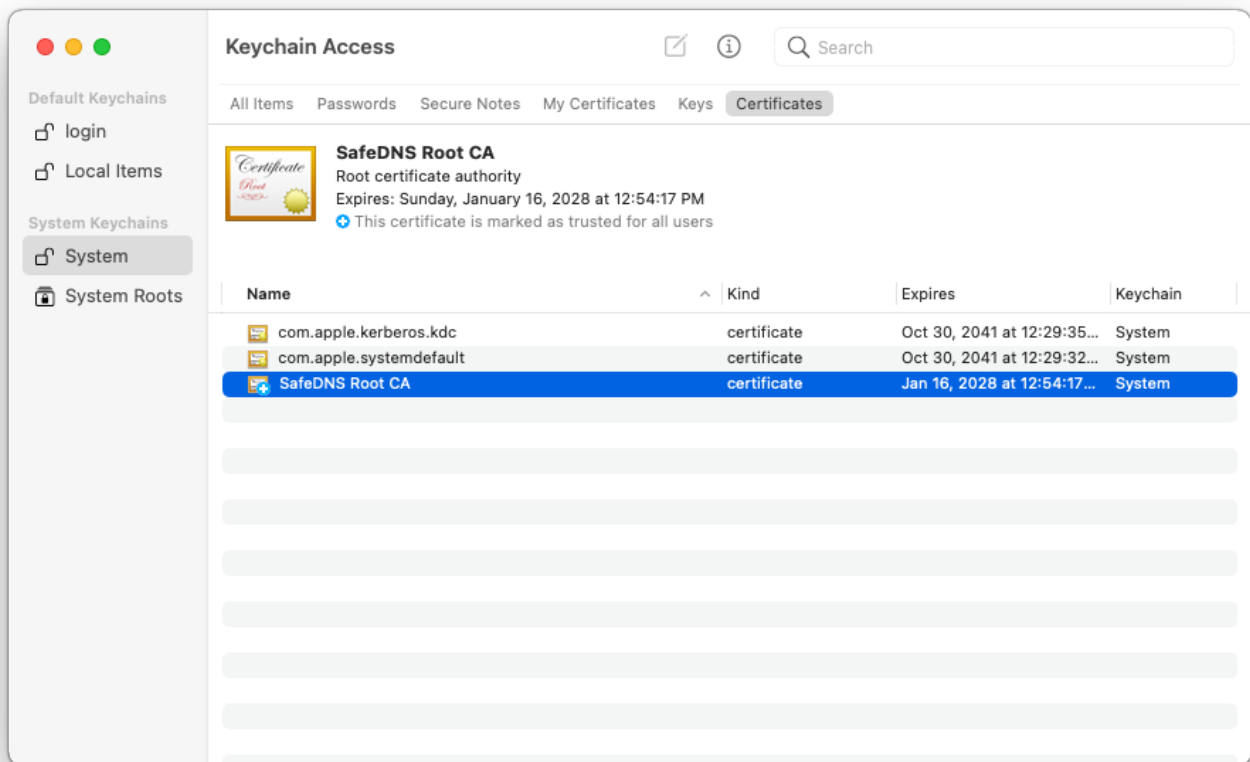


2. Navigate to **Login > System**.

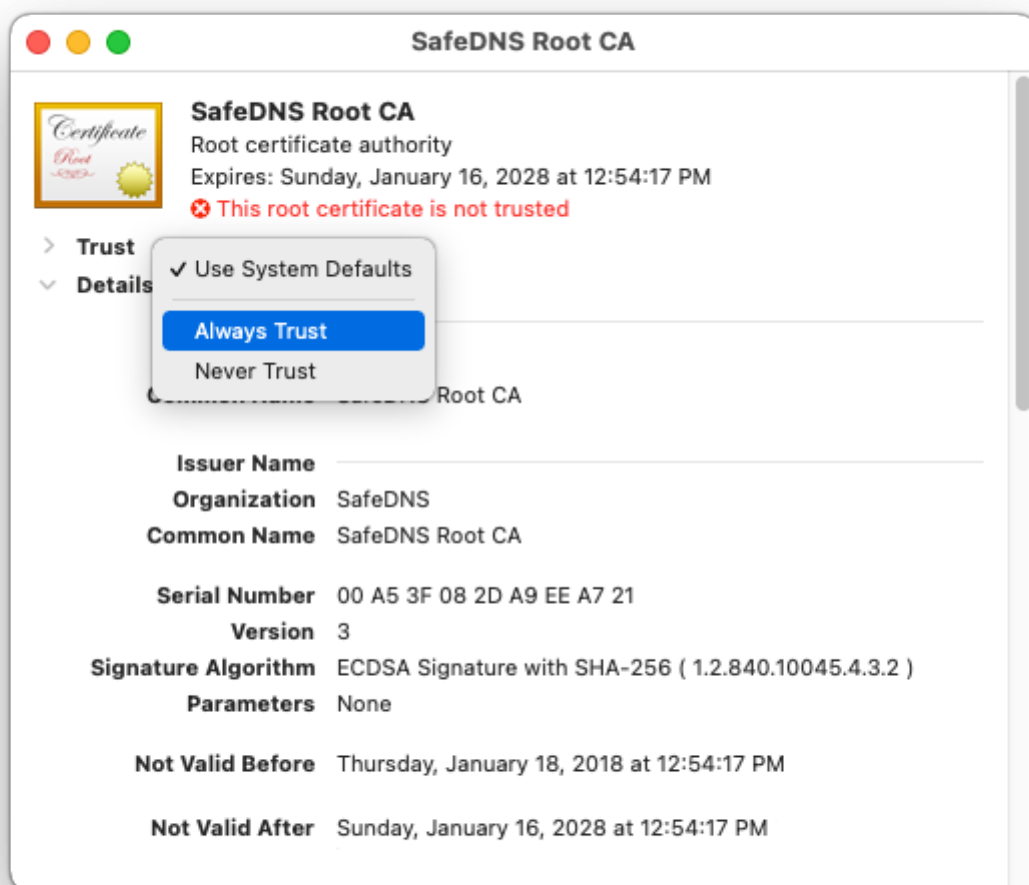


3. Drag and drop the downloaded SafeDNS certificate on the right side of the Keychain Access application where the rest of the certificates are stored.

4. Double-click on the SafeDNS certificate and select **Properties certificate**. In the opened window, choose when to use this certificate, and select '**Always trust**'. Close the window.

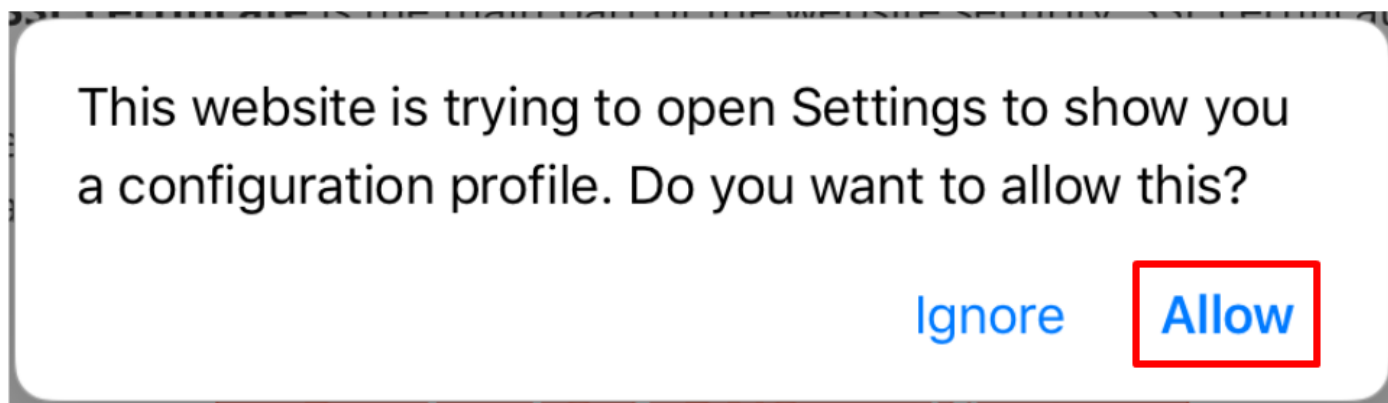


5. Make sure that the SafeDNS certificate is marked as trusted for this account in the Keychain Access application.

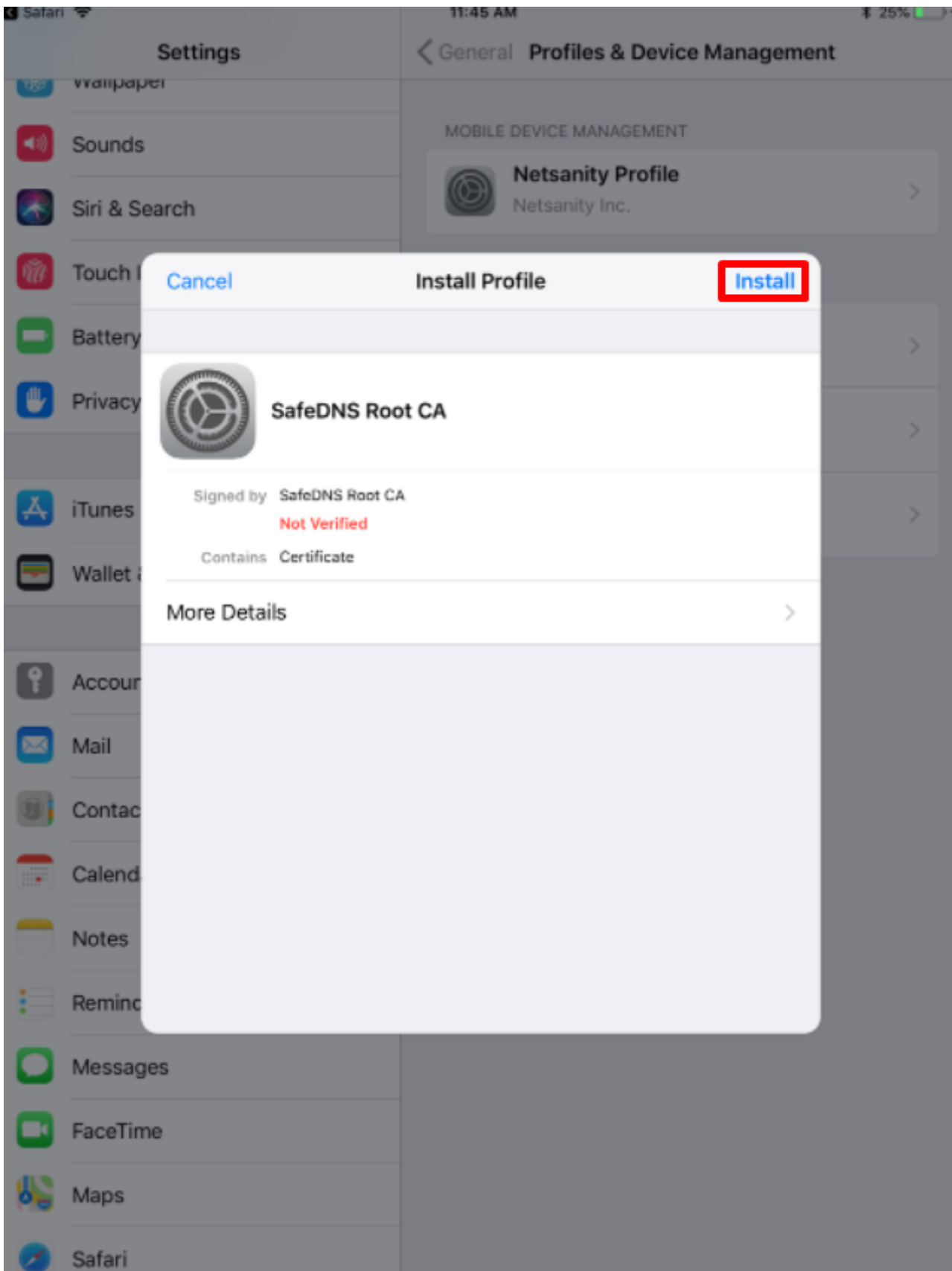


iPhone and iPad

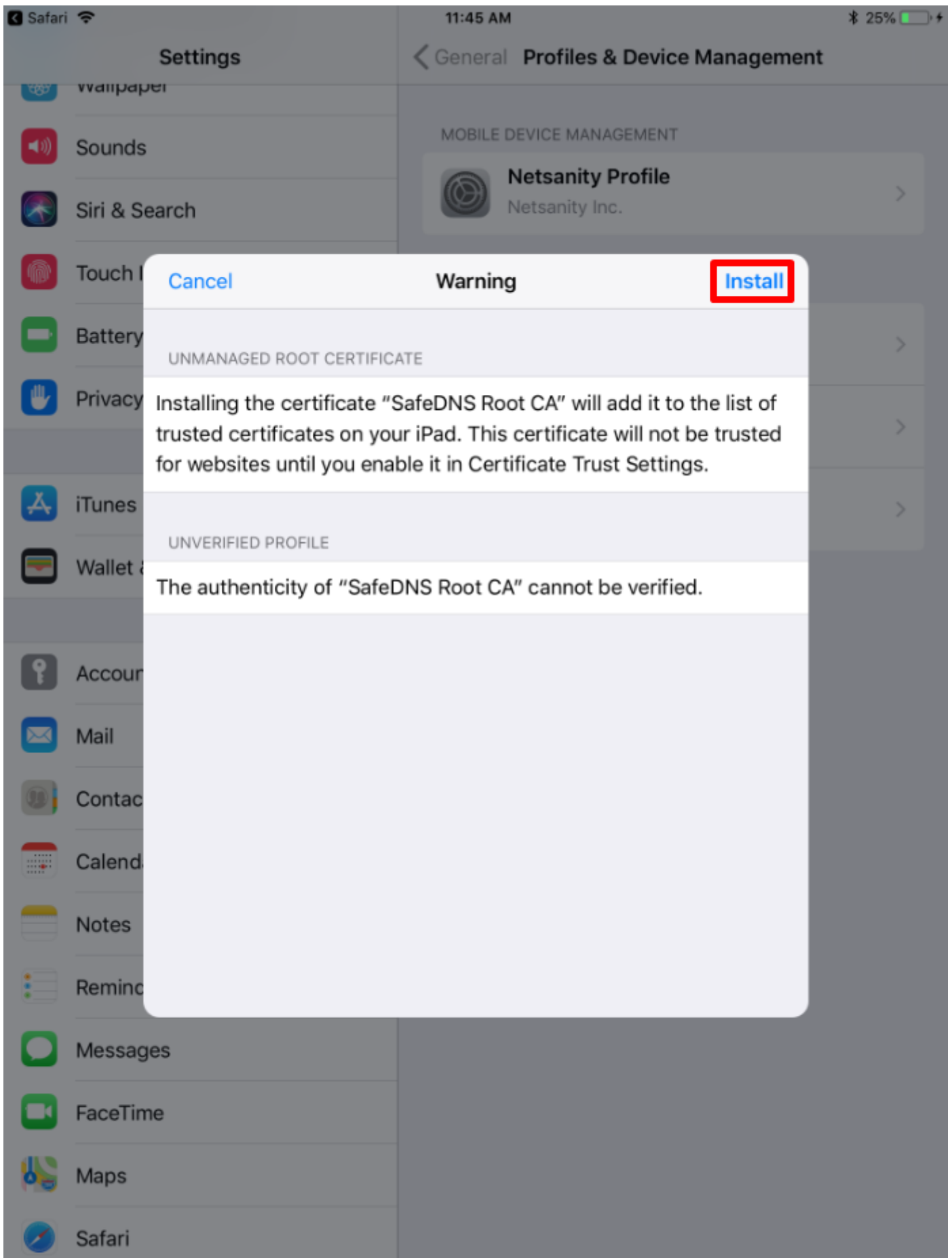
1. Download the **SafeDNS certificate**.
2. **Allow** the website to open **Settings**.



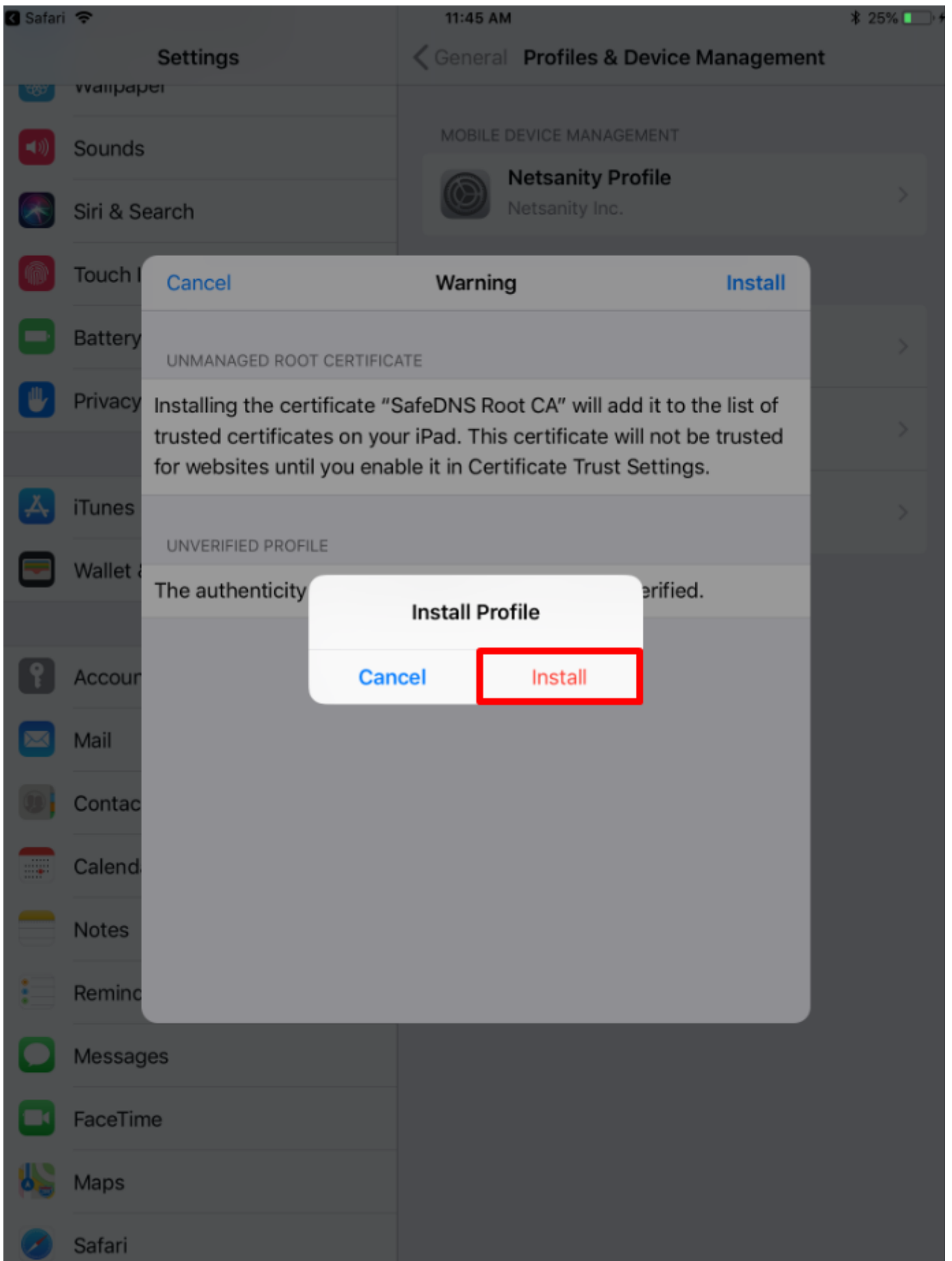
3. Tap **Install**.



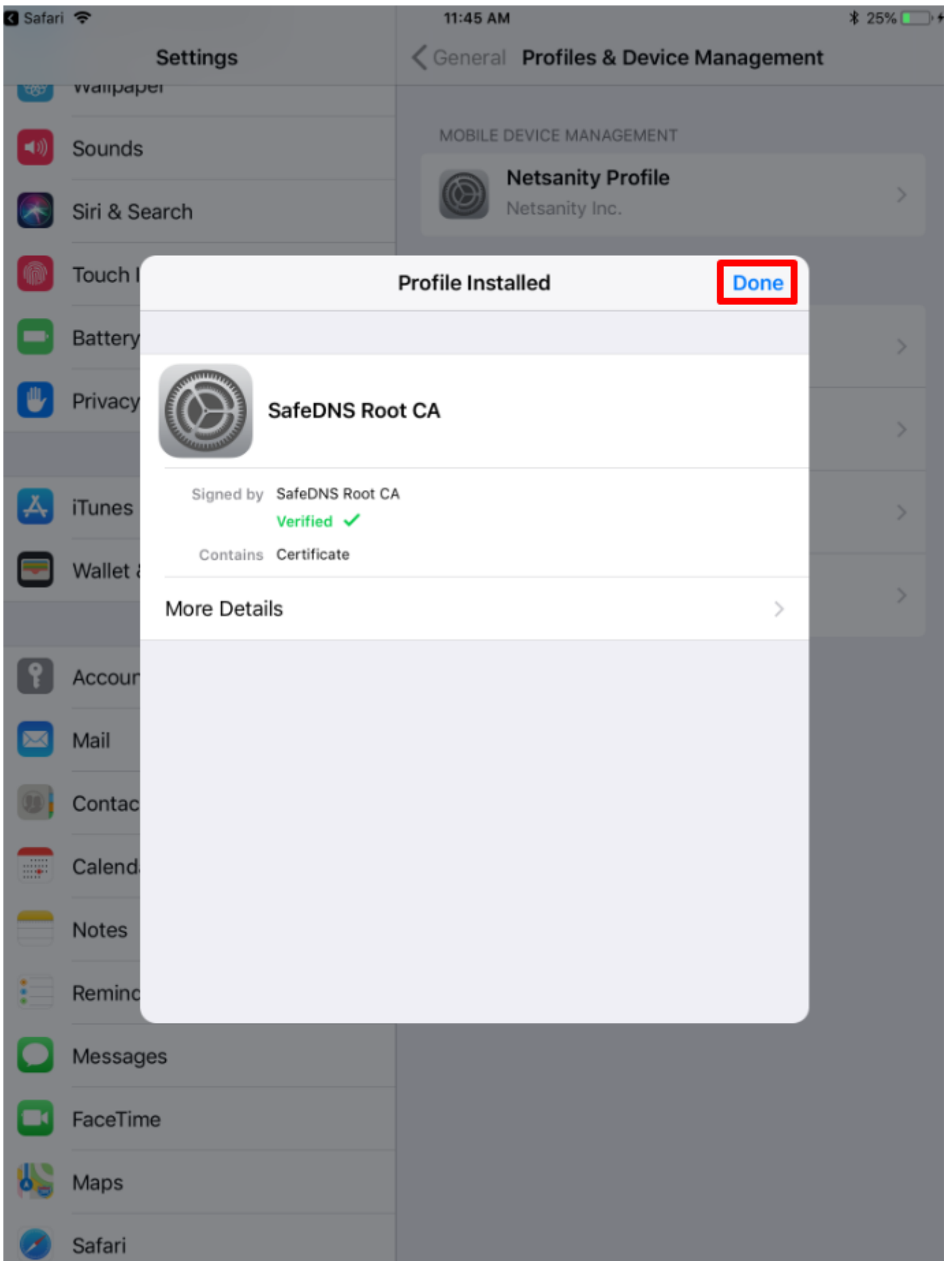
4. Tap on **Install** in the system warning window.



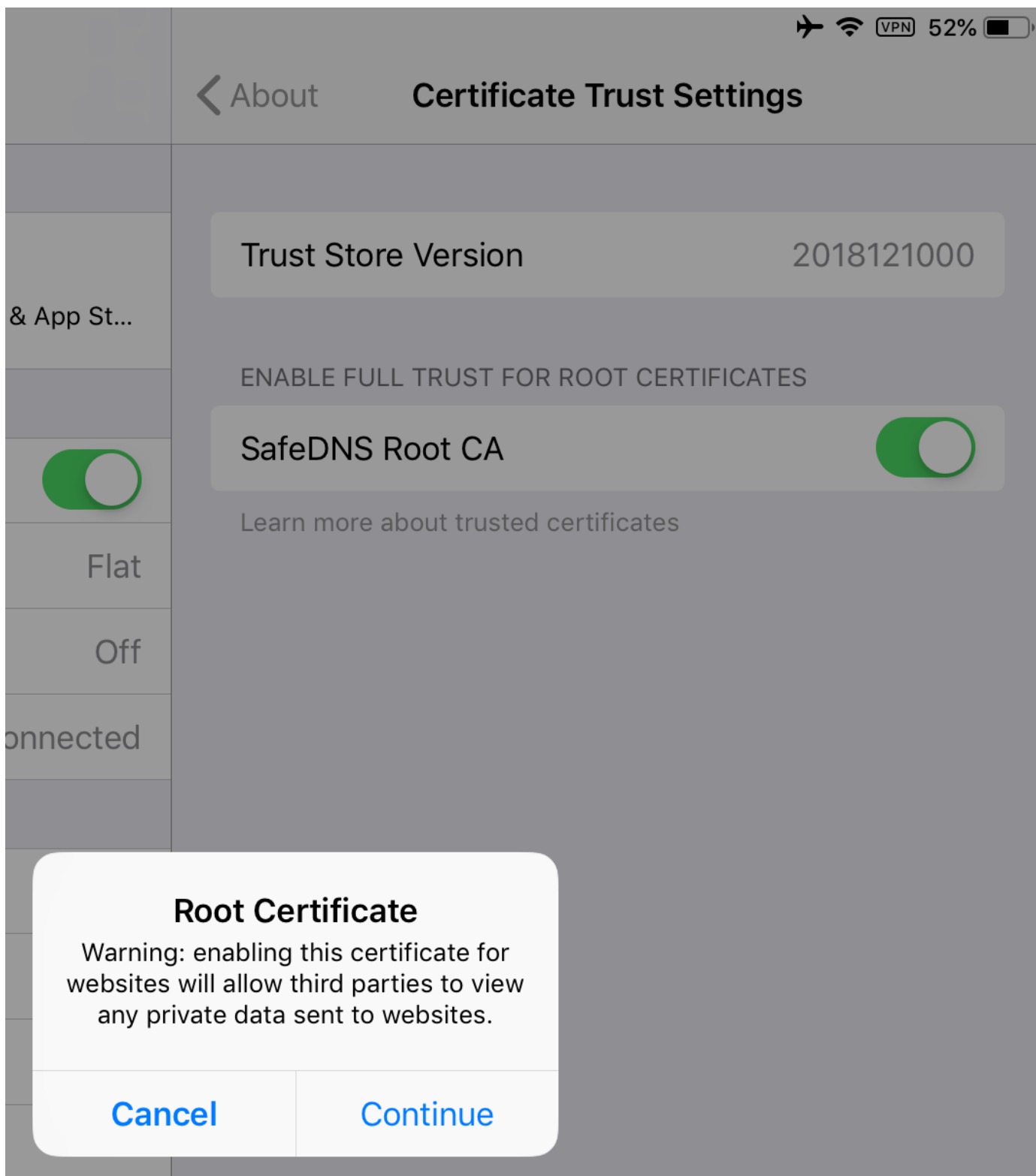
5. Tap **Install** in the confirmation window.



6. Tap **Done**.



7. Navigate to Settings > General > About > Certificate Trust Settings
8. Enable full trust for the SafeDNS Root CA certificate

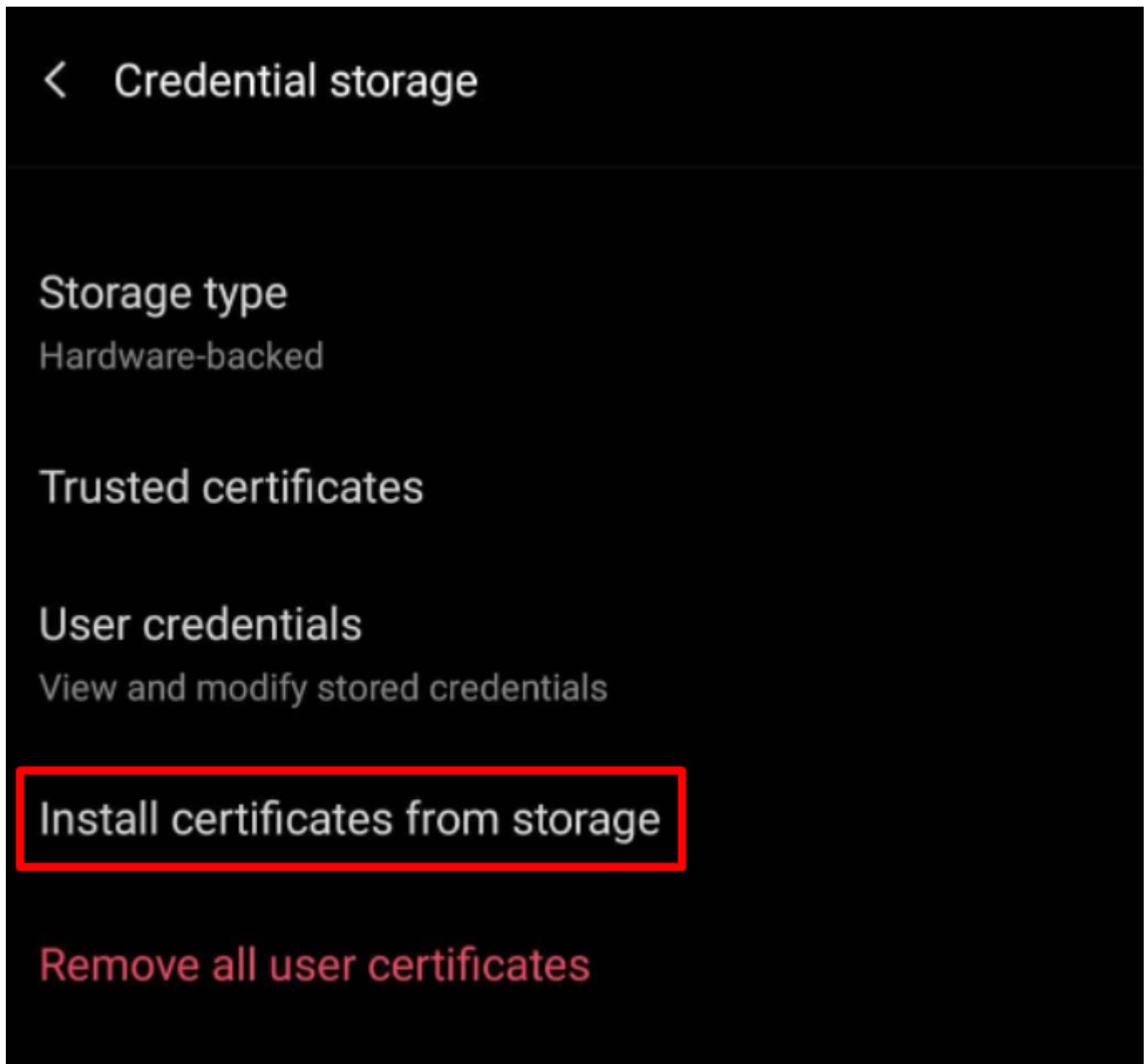


Android

Menu items and the system interface might be different on your device.

1. Open the Settings app.

2. Start typing "certificate" in the search box.
3. Choose the option related to the certificate installation, a new window will open.
4. Choose "Install certificates from storage".



5. Press "CA certificate".

< Install a certificate

CA certificate

VPN & app user certificate

Wi-Fi certificate

6. Follow the on-screen instructions to install the certificate.

Chromebooks and Google Workspace

In case the .crt certificate is not accepted, export it as a .pem file and import it into Workspace Admin.

Troubleshooting

If you don't see the block page on HTTPS pages after the certificate installation, or there is a browser warning about an invalid certificate, please, try reinstalling the certificate.

If the issue remains, [contact our technical support team](#)

Revision #6

Created 28 August 2022 23:23:47

Updated 25 September 2024 06:03:41 by Val Redman