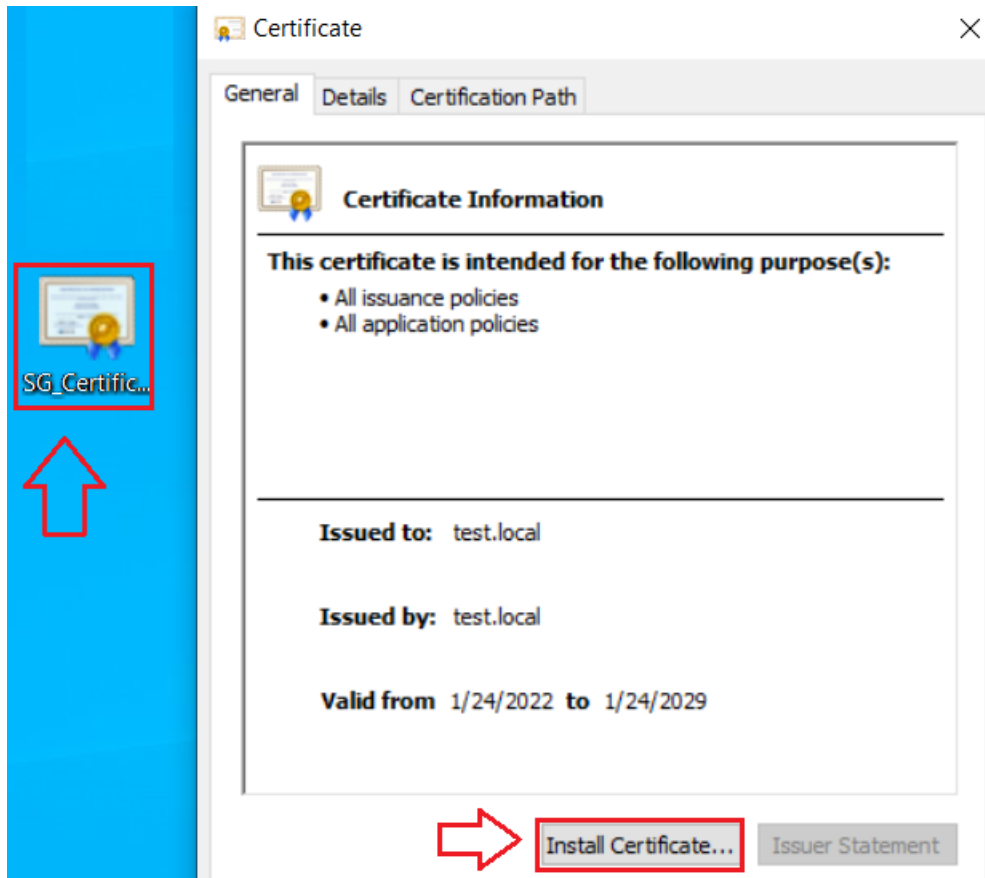


Install Certificate in Client PC:

Double click on **certificate** it will Certificate Windows Click on **Install Certificate...**



Select **Local Machine** and click **Next** to continue.

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.

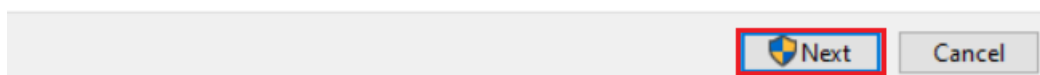
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

Current User

Local Machine

To continue, click Next.



Select **Place all certificate in the following store** and choose Trusted Root Certification Authorities click **Next**.

←  Certificate Import Wizard

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

Just click **Finish** button to end Certificate installation.

←  Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

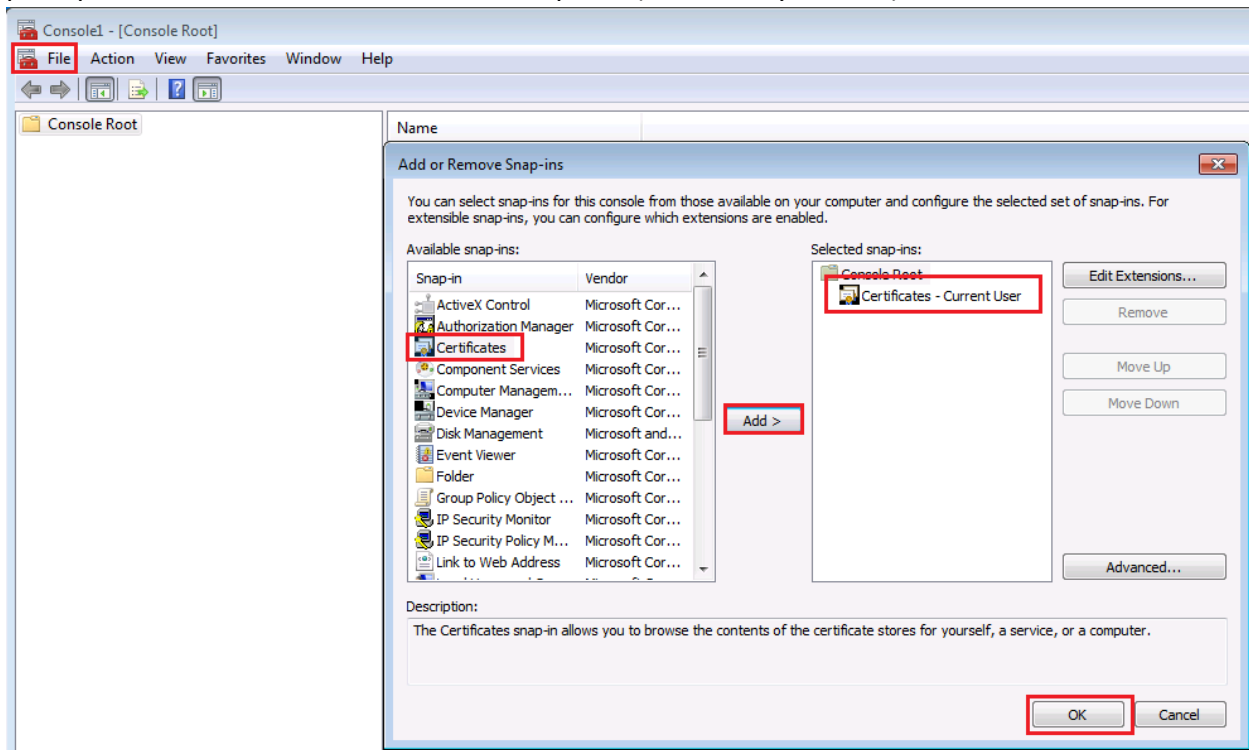
You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

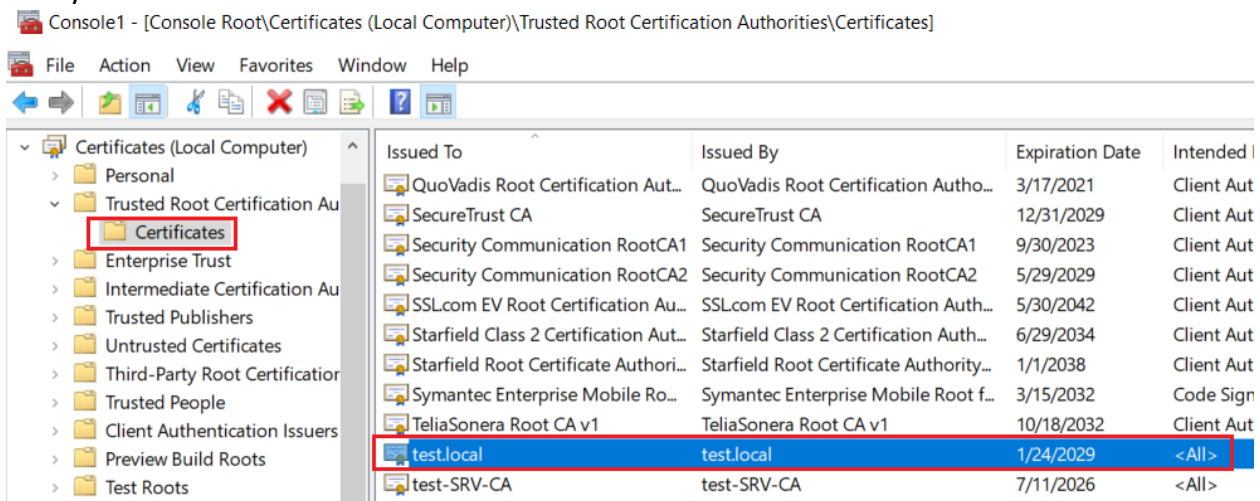
Finish

Cancel

Enter **Start > Run>MMC.exe**. Click **File > Add/Remove Snap-in**. In the Add or Remove Snap-ins window, select **Certificates** and click **Add**. Select the Computer account radio button when prompted and click **Next**. Select Local computer (selected by default) and click **Finish**.



Go to **Certificates –Local Computer > Trusted Root Certification Authorities > Certificates** and Verify that the certificate is install.



Navigate to **Security Profile>SSL/SSH Inspection** double click to edit Deep-Inspection profile.

+ Create New			View	Clone	Delete	Search	Q
Name	Read Only	Comments					
SSL Custom-deep-inspection		Read-only deep inspection profile.					
SSL WIN-Deep-Inspection		Win CRT deep inspection profile.					
SSL certificate-inspection	🔒	Read-only SSL handshake inspection profile.					
SSL custom-deep-inspection		Customizable deep inspection profile.					
SSL deep-inspection	🔒	Read-only deep inspection profile.					
SSL no-inspection	🔒	Read-only profile that does no inspection.					

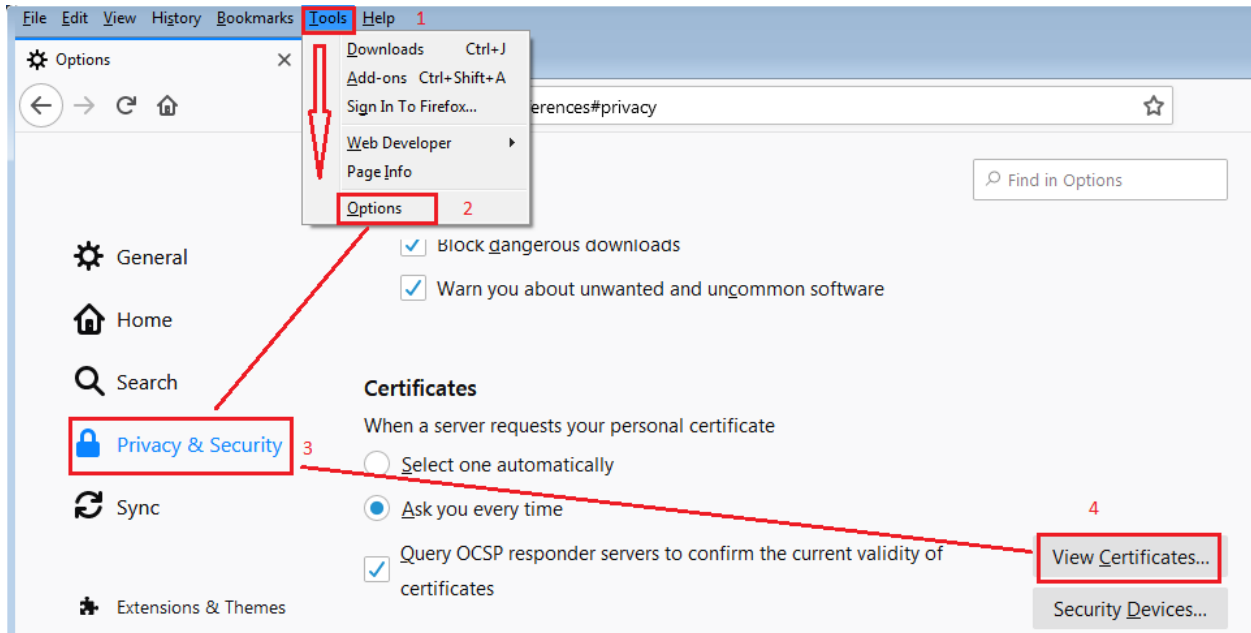
CA certificate click Download **Fortinet_CA_SSL** certificate to your computer.

The screenshot shows the 'Edit SSL/SSH Inspection Profile' page. The left sidebar has 'Security Profiles' selected. The main area shows the profile name 'deep-inspection' and its comments. Under 'SSL Inspection Options', the 'CA certificate' dropdown is set to 'Fortinet_CA_SSL', which is highlighted with a red box and a red arrow. A 'Download' button is also visible next to it.

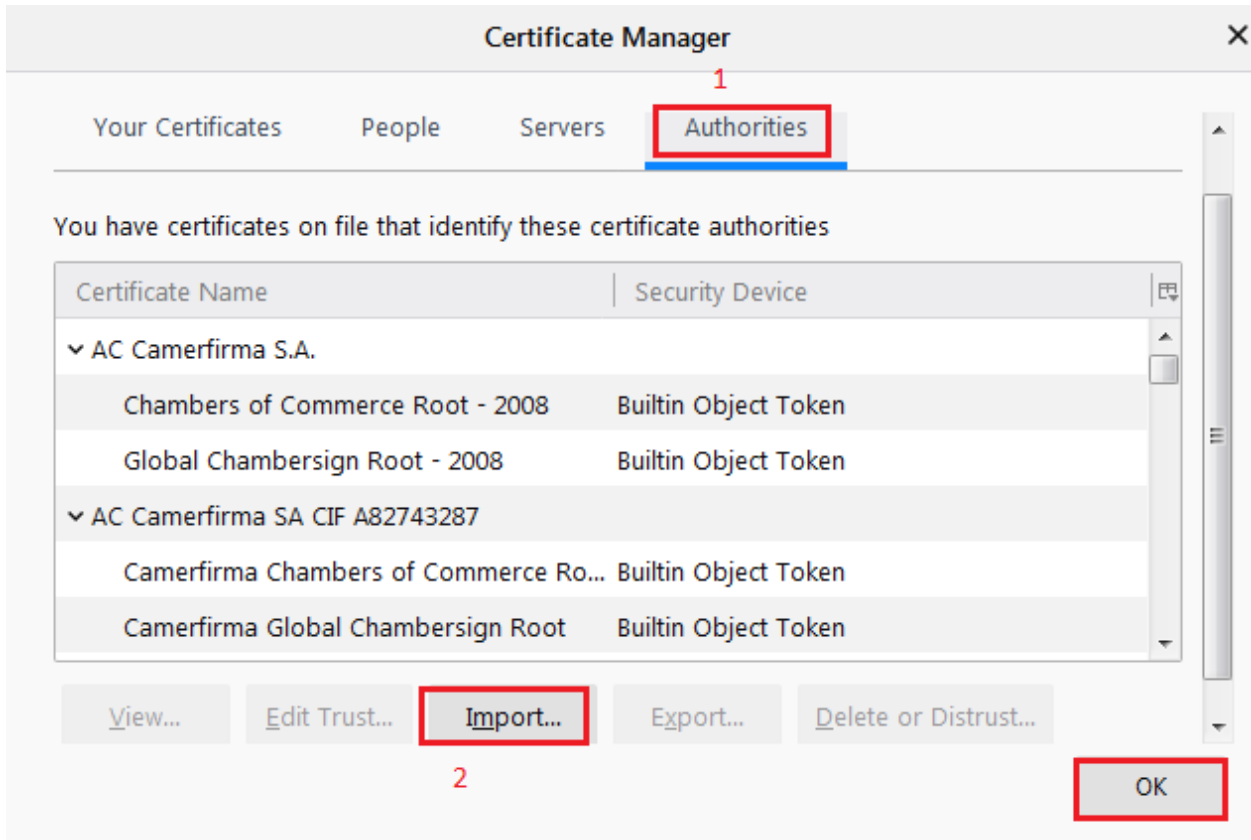
The Certificate is downloaded to your system.

The screenshot shows the Fortinet system tray at the bottom of the interface. It displays the Fortinet logo and version 'v7.0.5'. Below it, a notification for 'Fortinet_CA_SSL.cer' is shown, with a red arrow pointing to it.

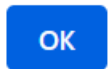
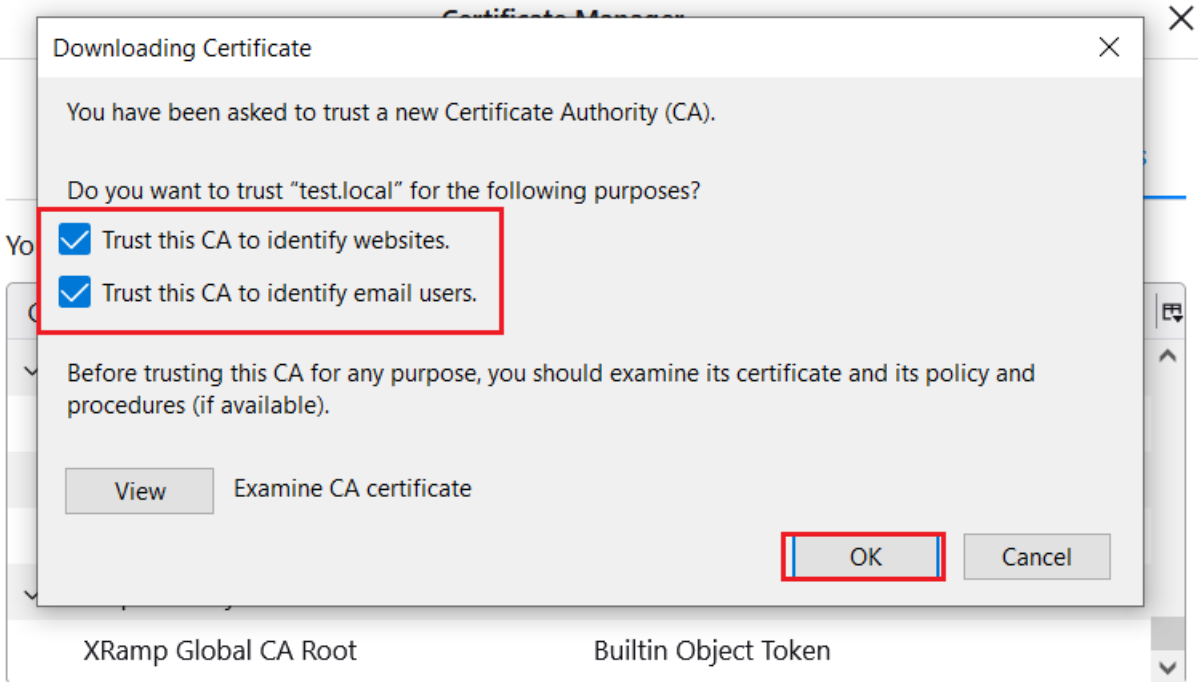
On the web browser (Mozilla Firefox) by going to **Tools > Options**. Go to **Privacy & Security > Certificates > View Certificates**.



Under **Authorities** > click **Import**.



Check Trust this CA to identify websites & Trust this CA to identify email users and Click OK.



Let's verify the certificate is properly imported to Mozilla Browser.

