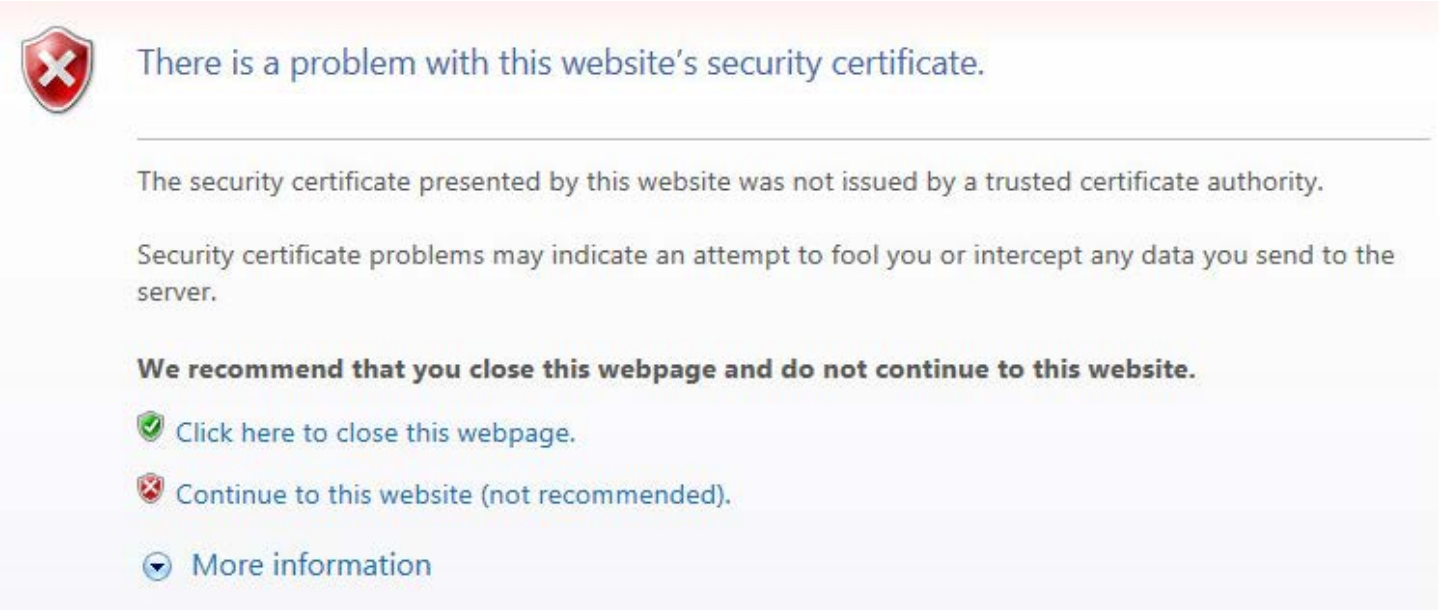
Adding the self-signed certificate as trusted to a browser

Install SSL certificate from an untrusted website into the Certificates snap-in using **IE**

Please read the following contents carefully

1. The browser informs you of a problem with the security certificate of the website.

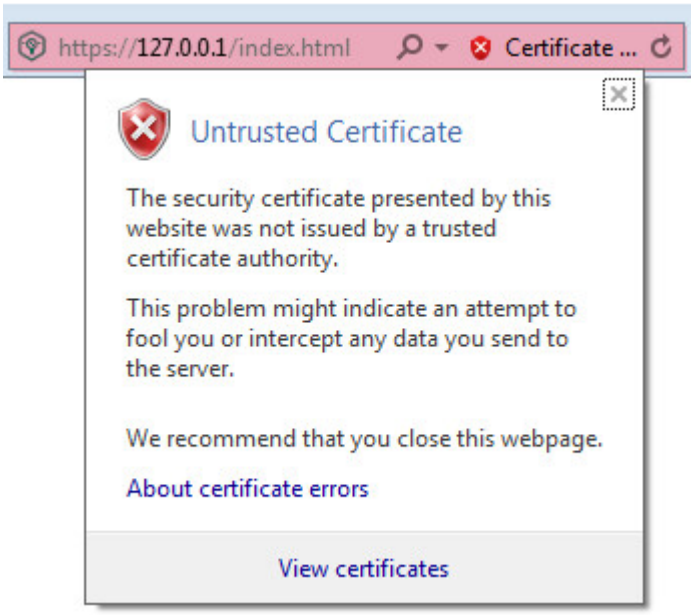


(Untrusted Certificate window)

2.1. Select the **Continue to this website (not recommended)** link. The **Certificate Error** message appears in the address bar.

3.2. Click **Certificate Error.**

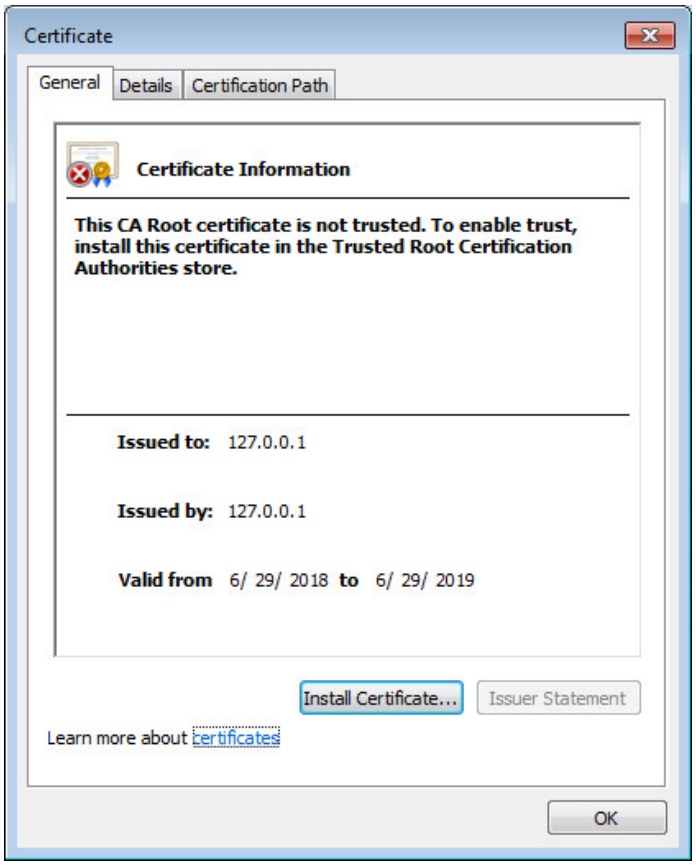
The **Untrusted Certificate** window opens.



(Untrusted Certificate window)

4.3. Select the **View certificates** link.

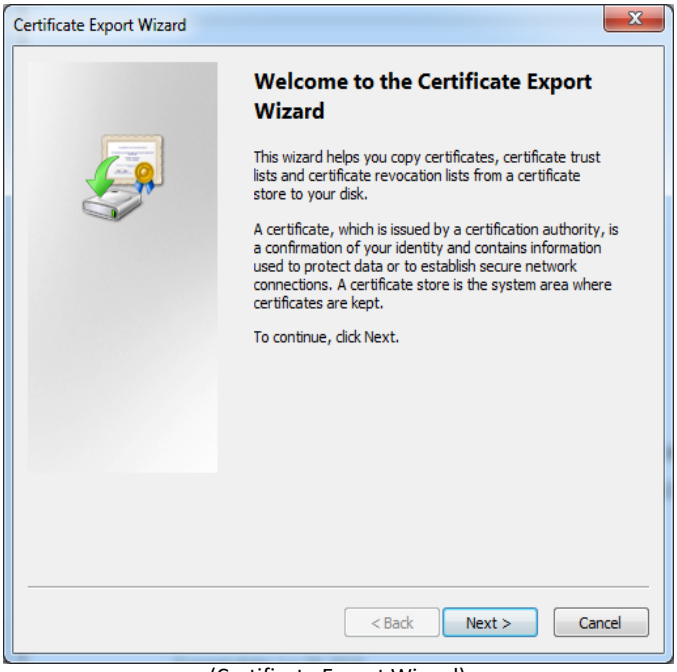
The **Certificate** window opens with information for example about the Kaspersky Cyber Trace certificate.



(Certificate window)

5.4. Select the **Details** tab, and then click **Copy to File** to create a local copy of the certificate.

The Certificate Export Wizard starts.



(Certificate Export Wizard)

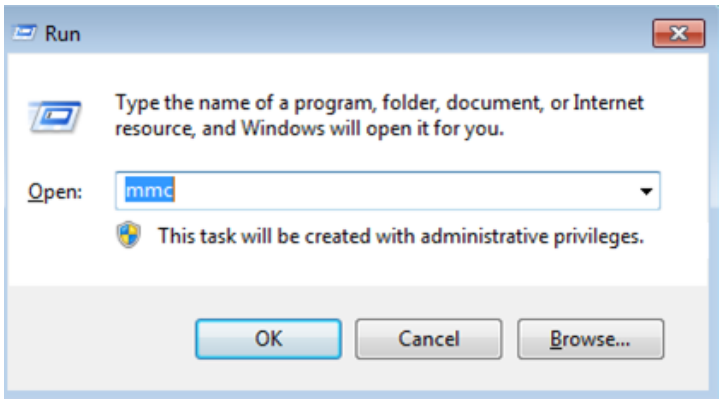
6.5. Follow the Wizard instructions.

Use the default Wizard settings during the certificate export.

To start the certificate import process through Microsoft Management Console (MMC):

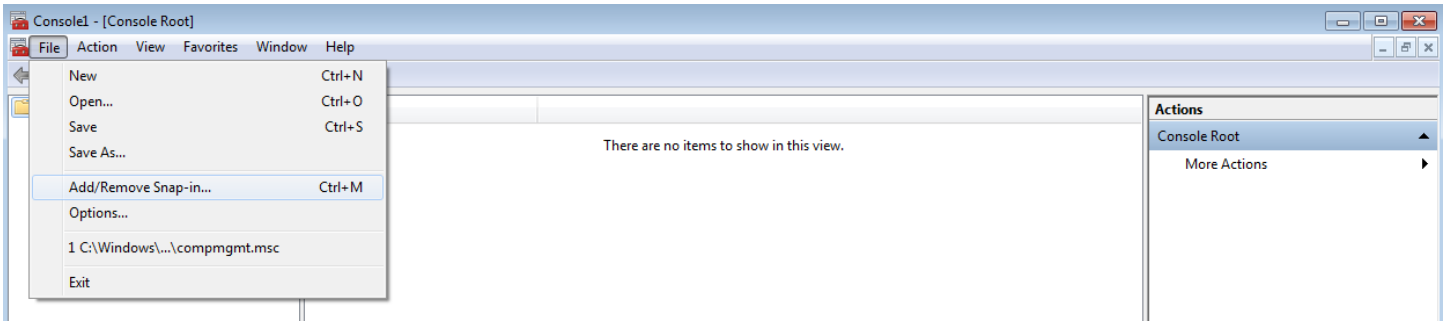
1.1. From the **Search** box, navigate to the **Run** box, and then enter mmc.

You can now run MMC as Administrator.



(Running the MMC)

2.2. In the MMC-based console that opens, select **File => Add/Remove Snap-in**.



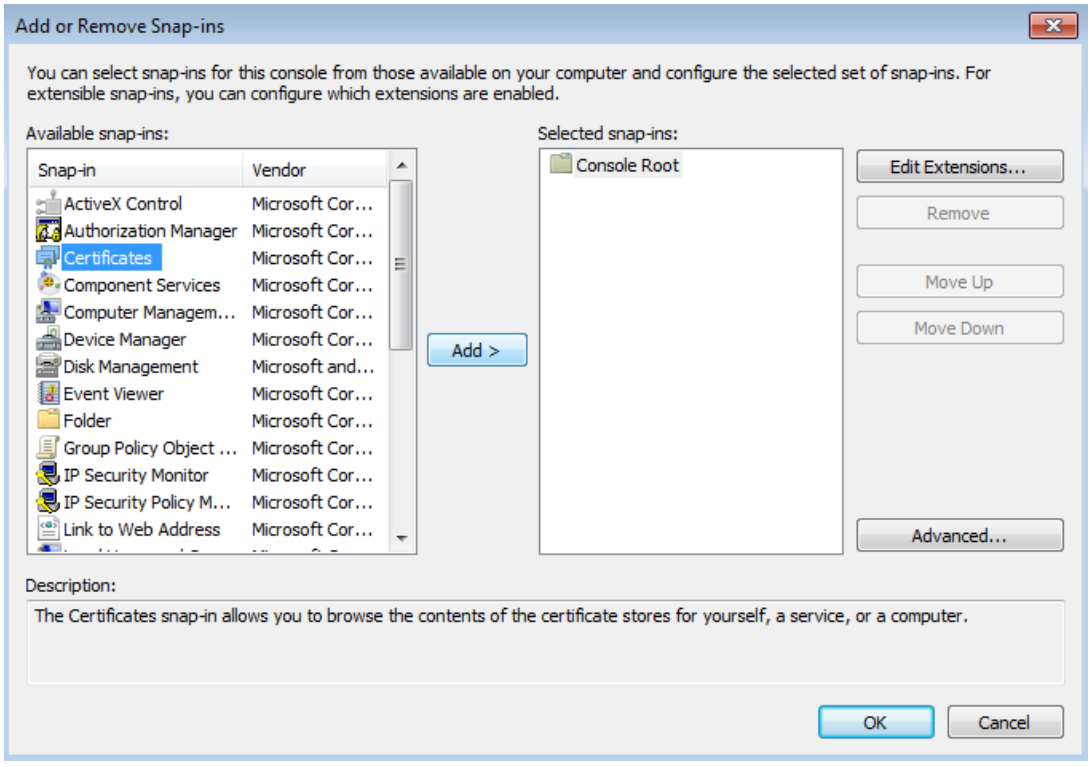
(Selecting Add/Remove Snap-in)

The Add or Remove Snap-ins window opens.

3.3. In the **Available snap-ins** list, select **Certificates**, and then click **Add.**

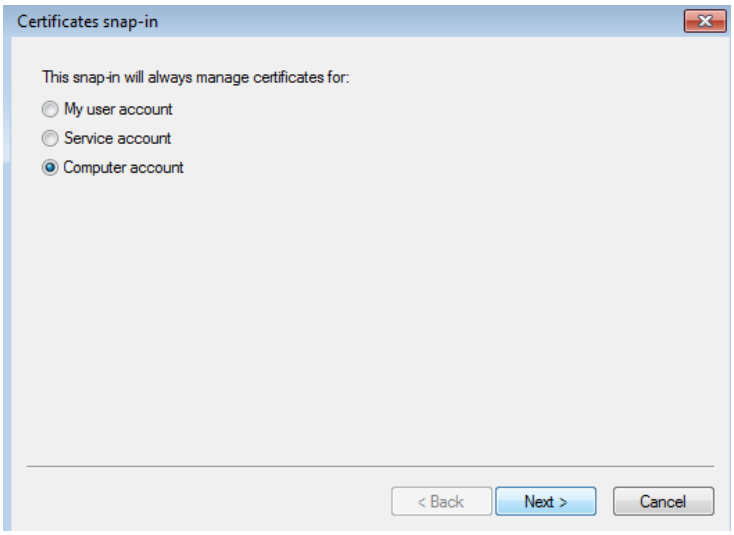
The**Certificates snap**-in window opens.

4.4. Select **Computer account**, and then click **Next**.



(Adding a certificate snap-in)

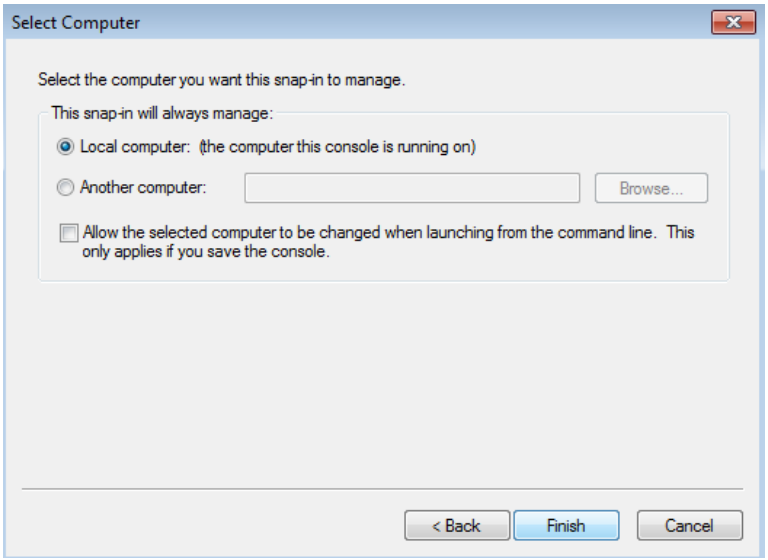
In the **Select Computer** window that opens, click **Finish.**



(Selecting Computer account)

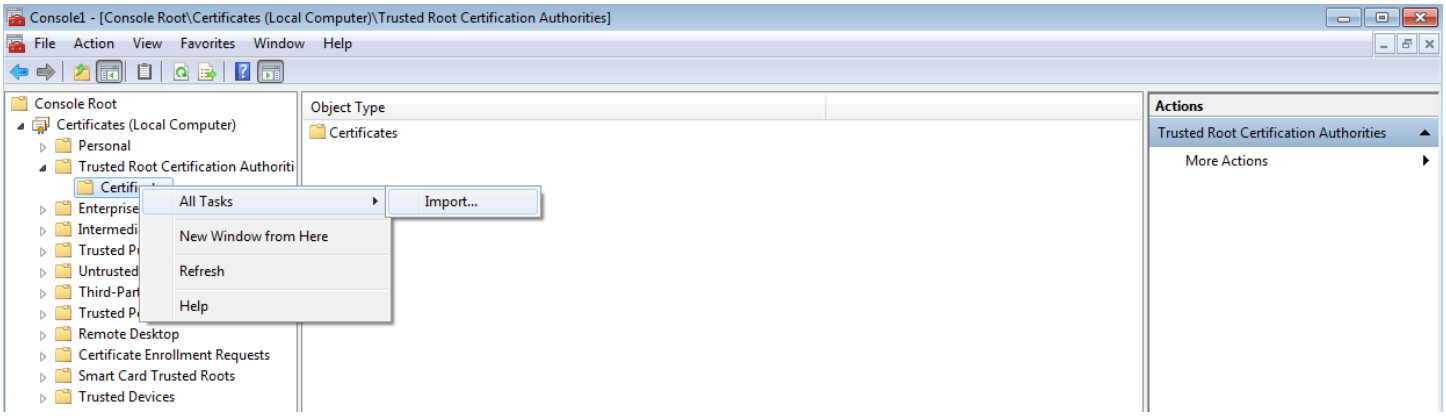
Selecting Local computer

5.5. In the tree pane, select **Certificates (Local Computer)** => **rusted Root Certification Authorities**, right-click **Certificates**, and then select **All Tasks** => **Import**.



(Selecting Local computer)

The Certificate Import Wizard starts.

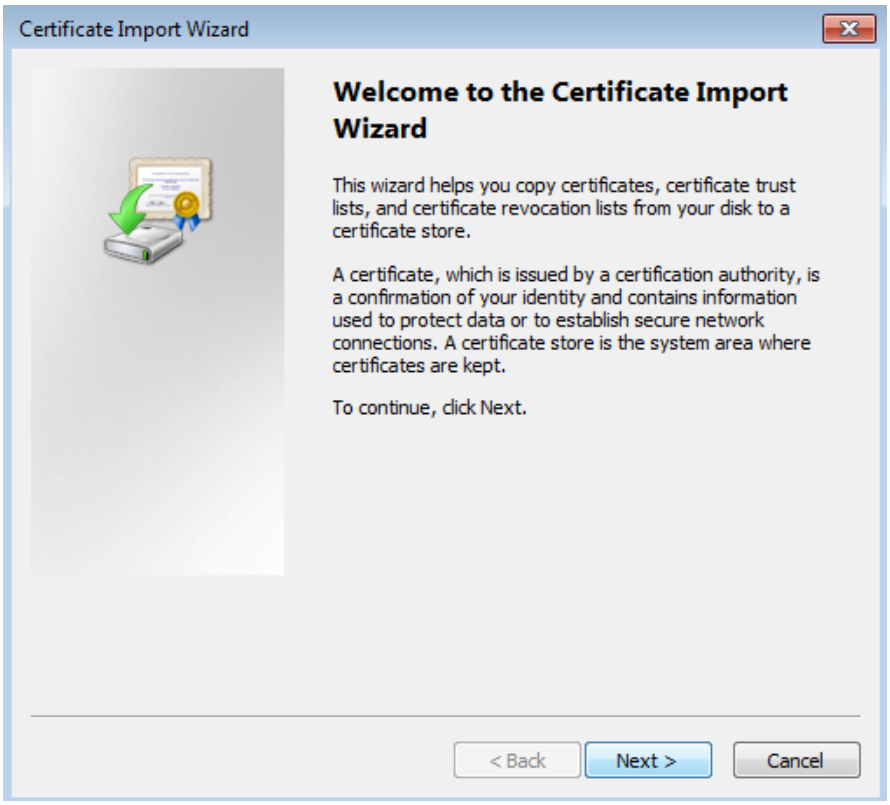


(Selecting Import)

To add the saved certificate to the Trusted Root Certification Authorities store:

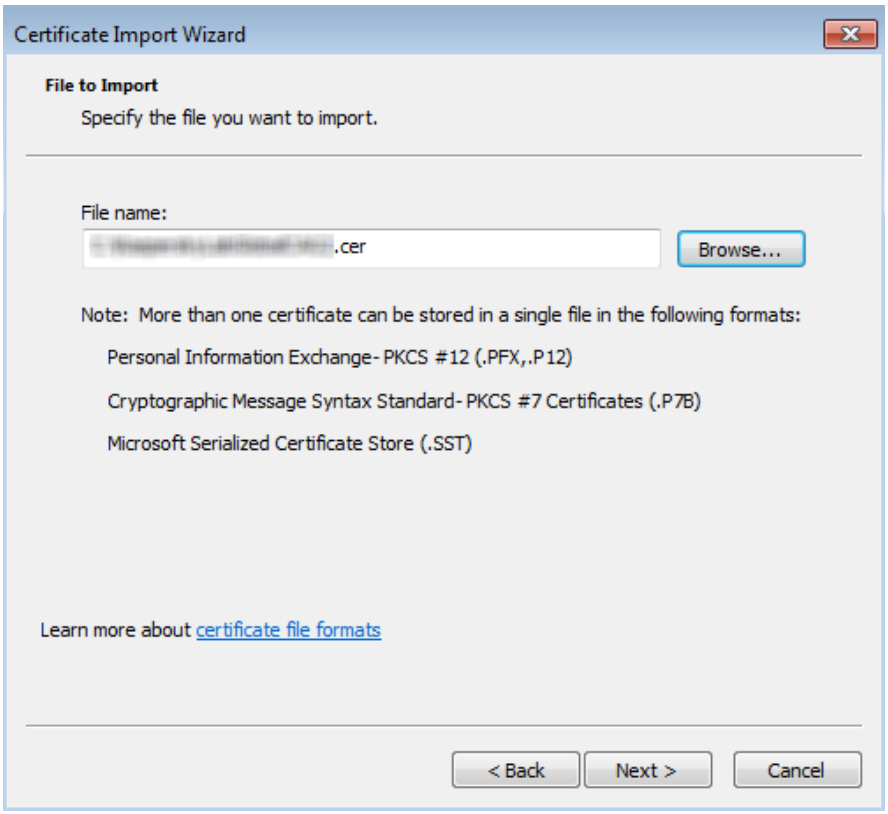
1.1. On the Welcome page of the Wizard, click **Next**.

2.2. Click **Browse** and select the certificate that was saved in the "To make the self-signed certificate for Kaspersky CyberTrace Web trusted when using Internet Explorer:" procedure above.



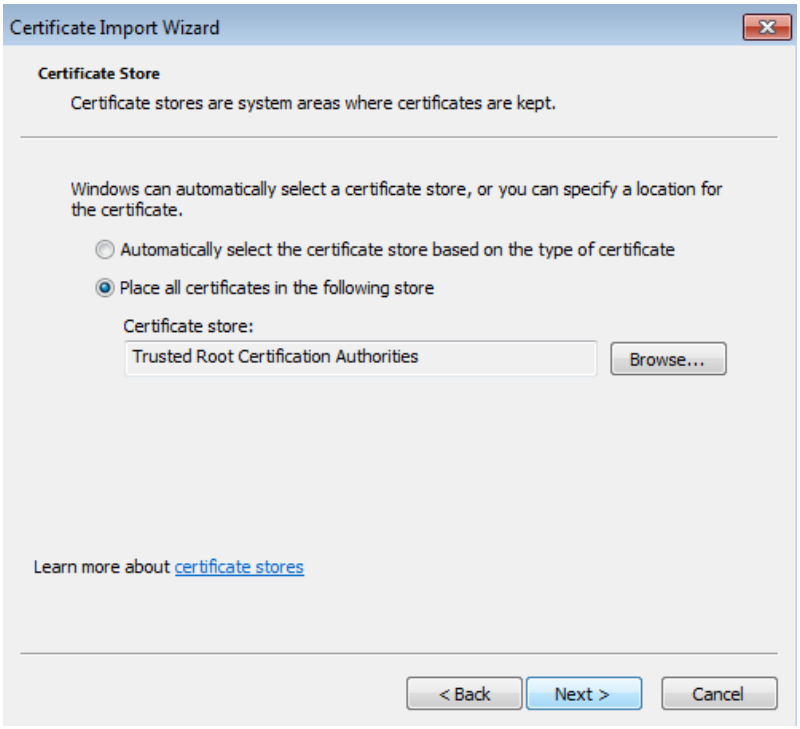
(Certificate Import Wizard)

3.3. On the next page of the Certificate Import Wizard, click **Next**.



(Importing the previously saved certificate)

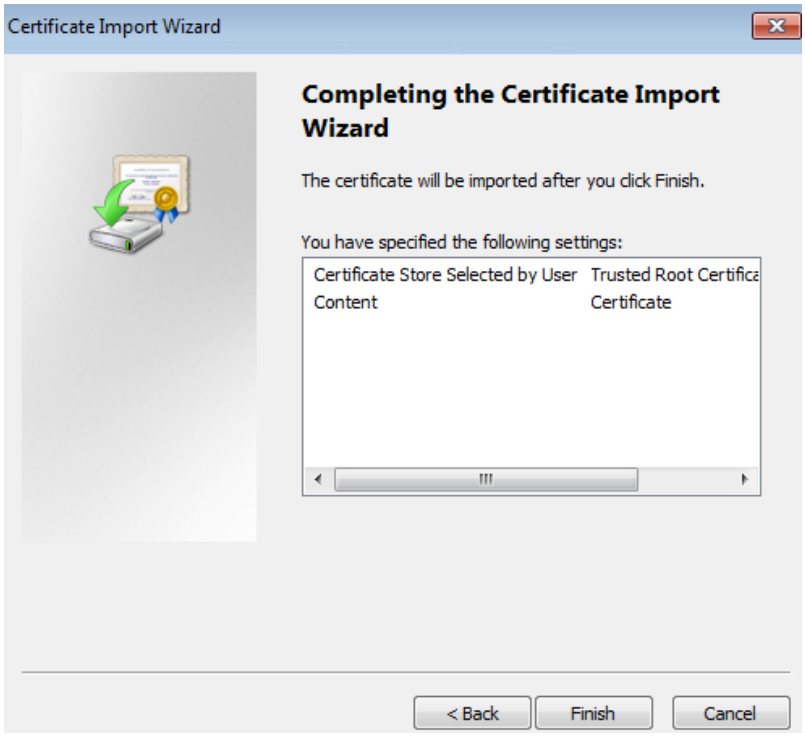
4. On the last page of the Certificate Import Wizard, click **Finish**.



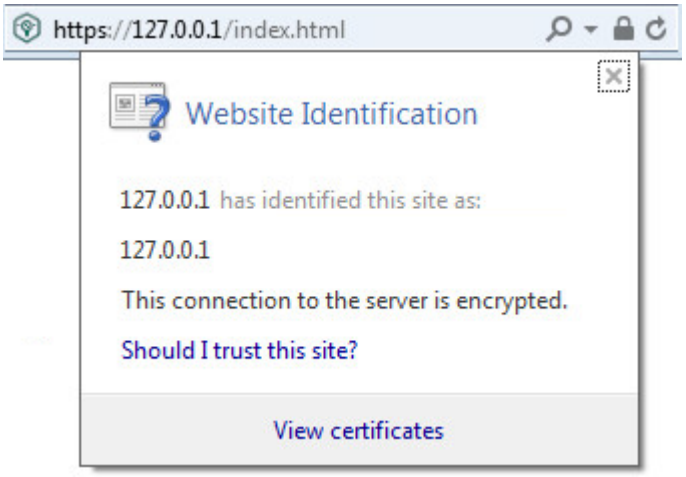
(Selecting a certificate store)

5.5. Close the MMC-based console and restart the browser.

The security problem (untrusted certificate) is resolved, as shown in the figure below.



(Completing the certificate import)



(Website identification)

Ñ@†€