

[Administrator guides](#) > [Adding self-signed SSL certificates for CyberTrace Web](#) > Adding the self-signed certificate as trusted to a browser

Adding the self-signed certificate as trusted to a browser

The procedures in this section show you how to add the self-signed certificates generated during Kaspersky CyberTrace installation to the trusted storage. This will remove the security warnings generated by browsers.

The information in this section is applicable to the situation when a user gains access to CyberTrace Web from the same computer on which CyberTrace Web runs. If the [GUISettings > HTTPServer > ConnectionString](#) element of the Feed Service configuration file refers to an external interface, the CyberTrace Web website will not be considered trusted, because the self-signed certificate can be used only with the `https://127.0.0.1` and `https://localhost` addresses.

To avoid potential security risks, we recommend using a trusted certificate signed by a certificate authority (CA). For more information, see section "[Generating certificates for CyberTrace Web](#)".

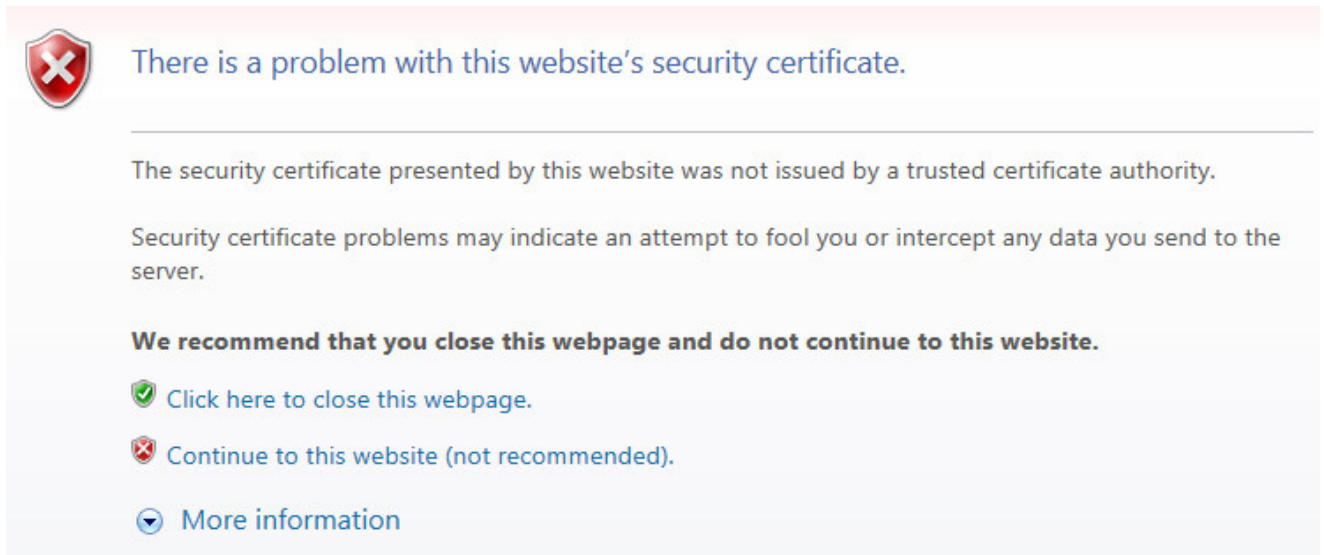
Causing a self-signed certificate to be trusted by a browser (CyberTrace Web is opened in Internet Explorer installed on a Windows system)

Gaining the browser's trust requires that you perform, in sequence, the following three procedures:

To save the certificate to a local file:

1. Open the `https://127.0.0.1` or `https://localhost` address in Internet Explorer.

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



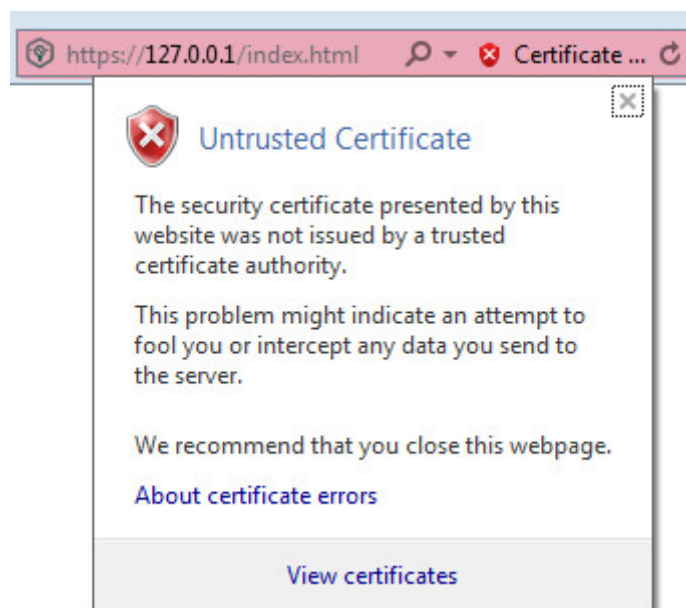
Certificate error message

2. Select the **Continue to this website (not recommended)** link.

The **Certificate Error** message appears in the address bar.

3. Click **Certificate Error**.

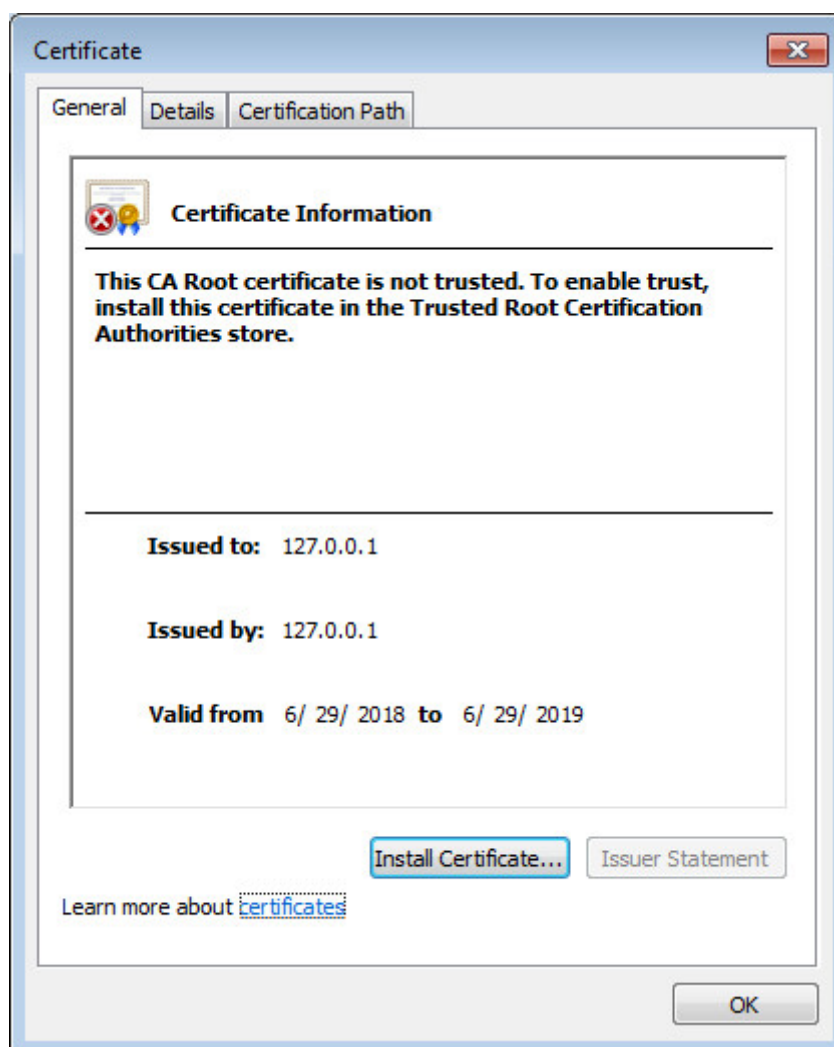
The **Untrusted Certificate** window opens.



Untrusted Certificate window

4. Select the **View certificates** link.

The **Certificate** window opens with information about the CyberTrace certificate.



Certificate window

5. 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

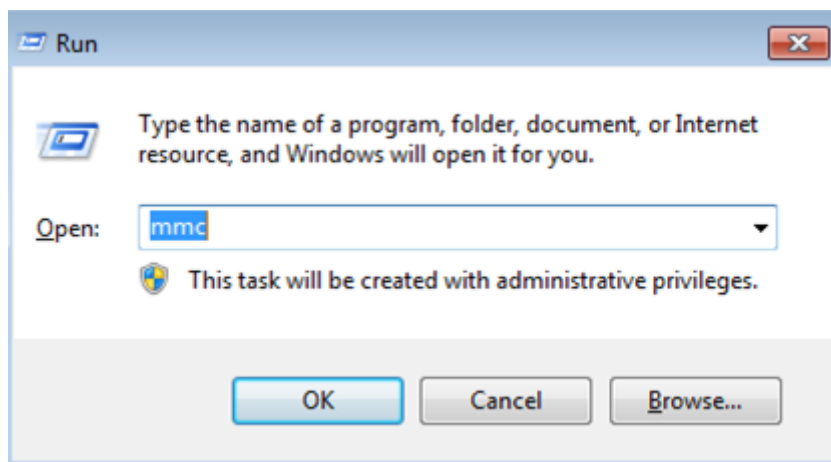
6. Follow the Wizard instructions.

Use the default Wizard settings during the certificate export.

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

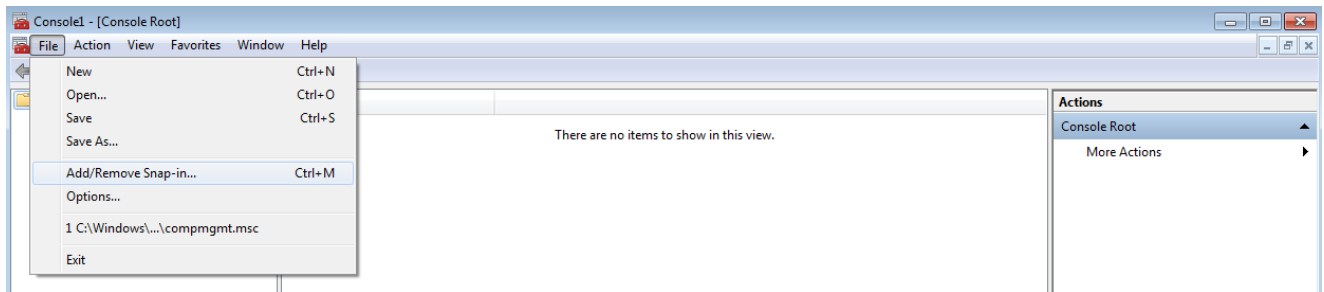
1. From the **Search** box, navigate to the **Run** box, and then enter `mmc`.

You can now run MMC as Administrator.



Running the MMC

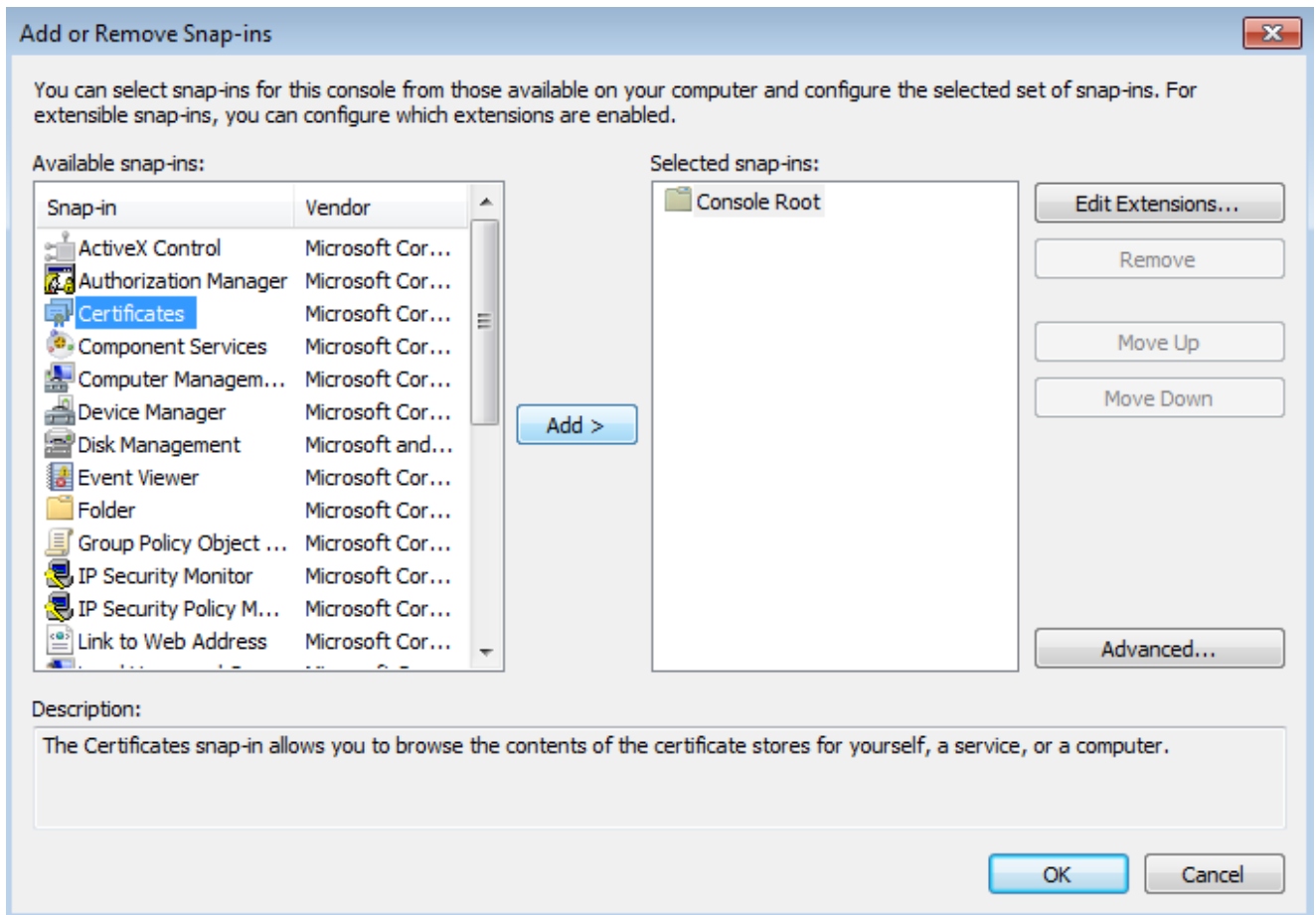
2. In the MMC-based console that opens, select **File > Add/Remove Snap-in**.



Selecting Add/Remove Snap-in

The **Add or Remove Snap-ins** window opens.

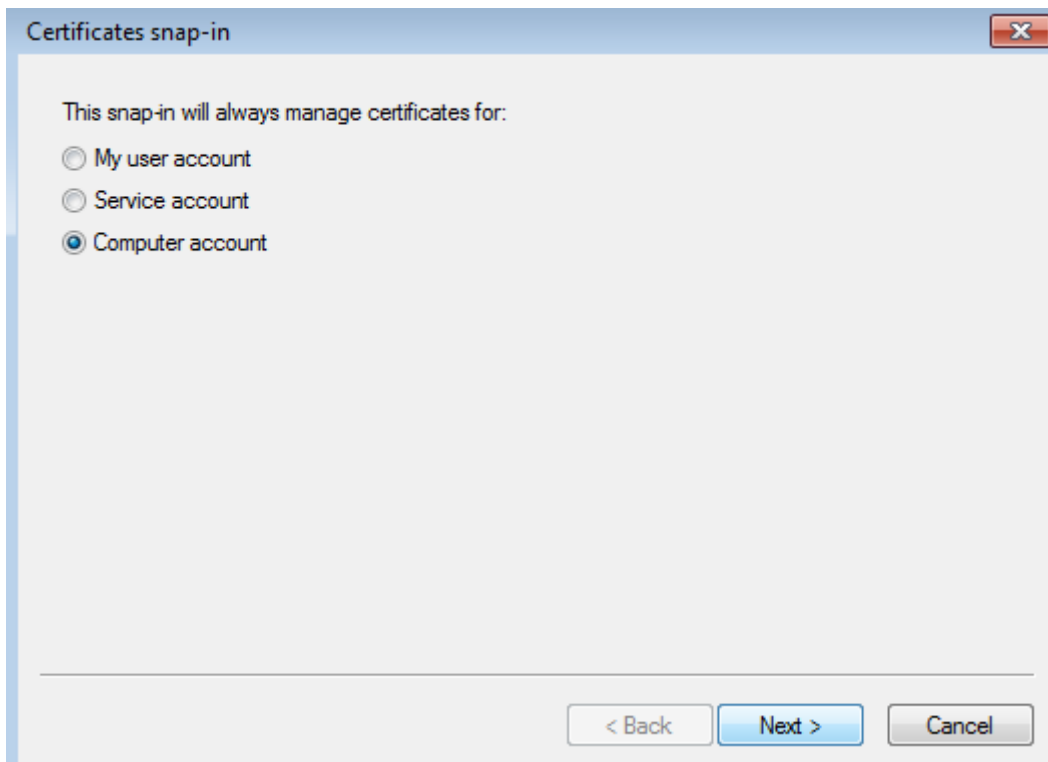
3. In the **Available snap-ins** list, select **Certificates**, and then click **Add**.



Adding a Certificates snap-in

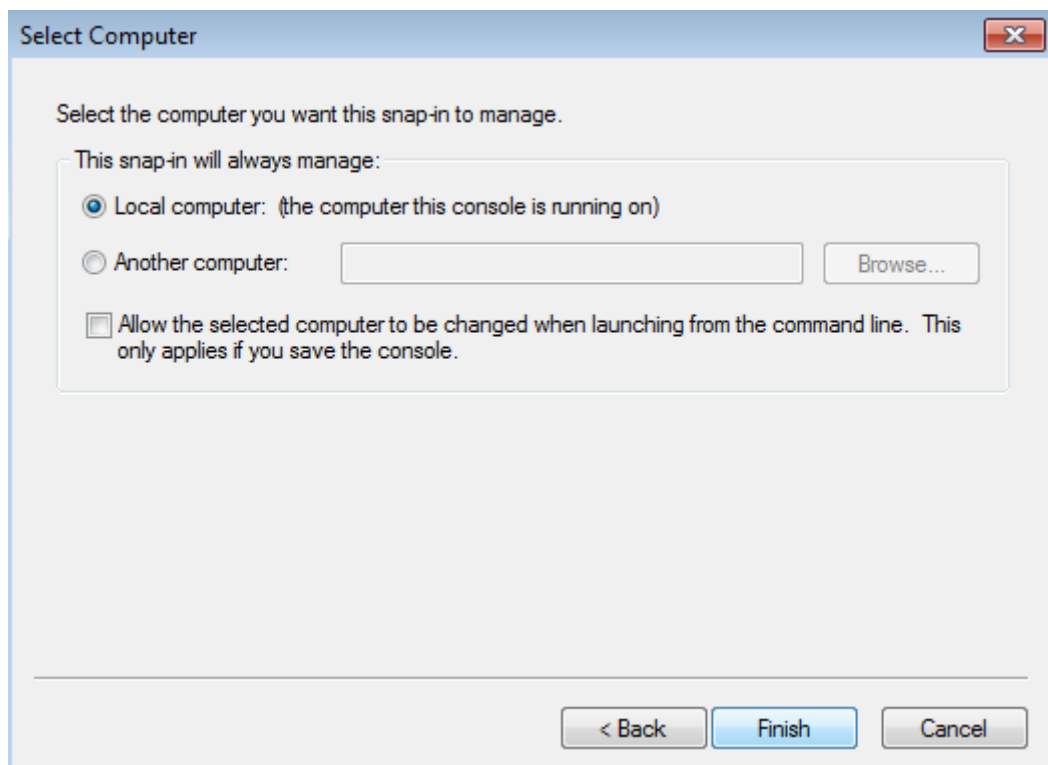
The **Certificates snap-in** window opens.

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



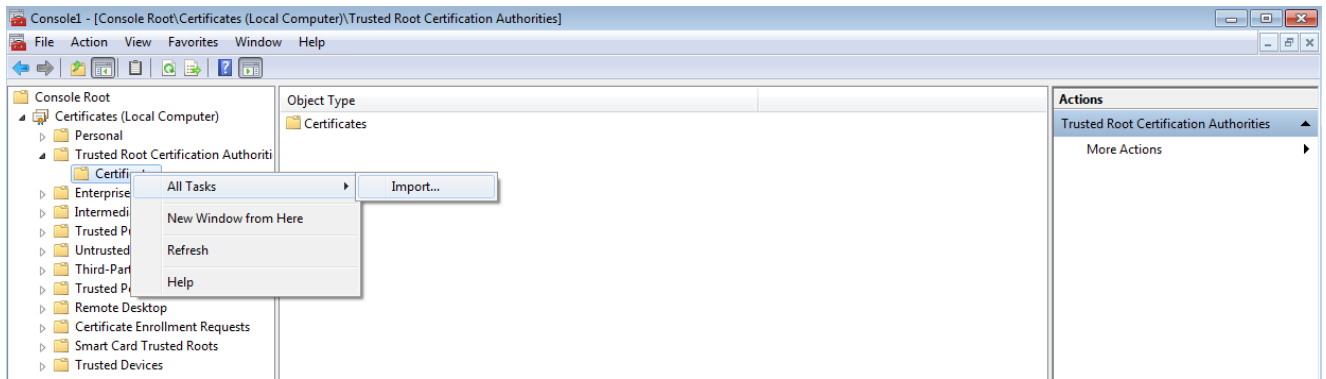
Selecting Computer account

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



Selecting Local computer

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

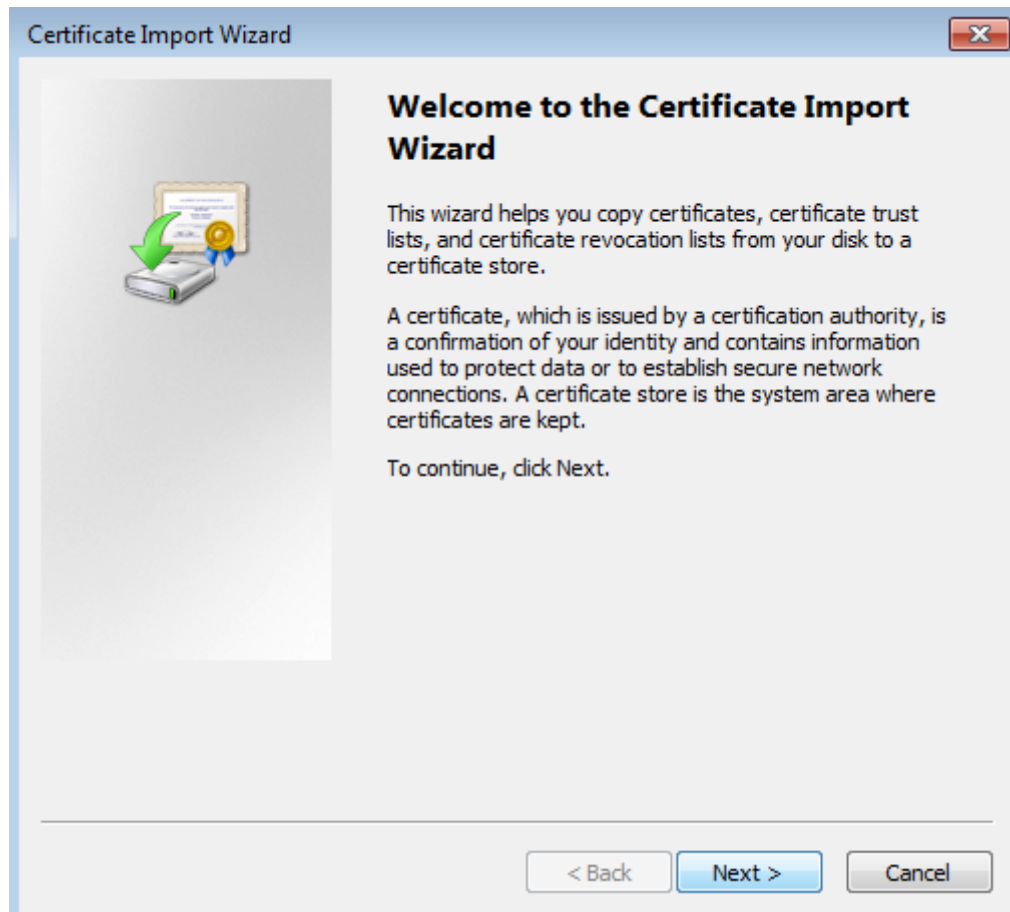


Selecting Import

The Certificate Import Wizard starts.

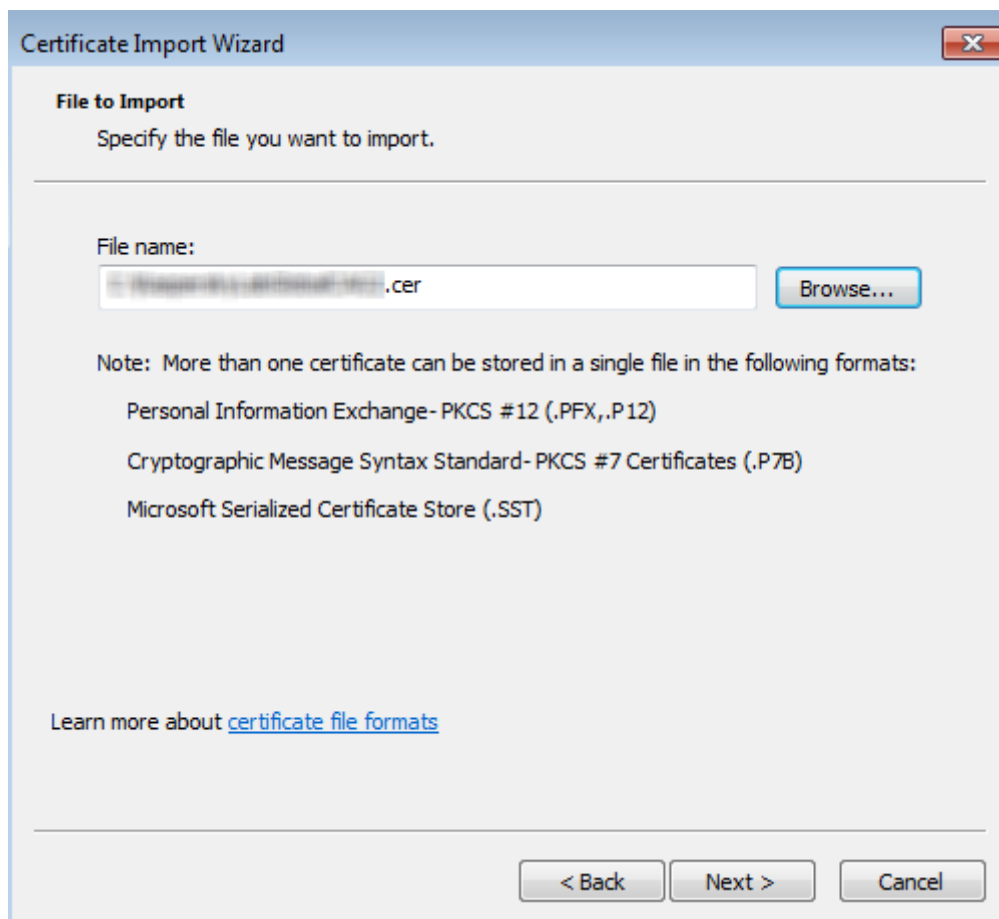
To add the saved certificate to the Trusted Root Certification Authorities store:

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



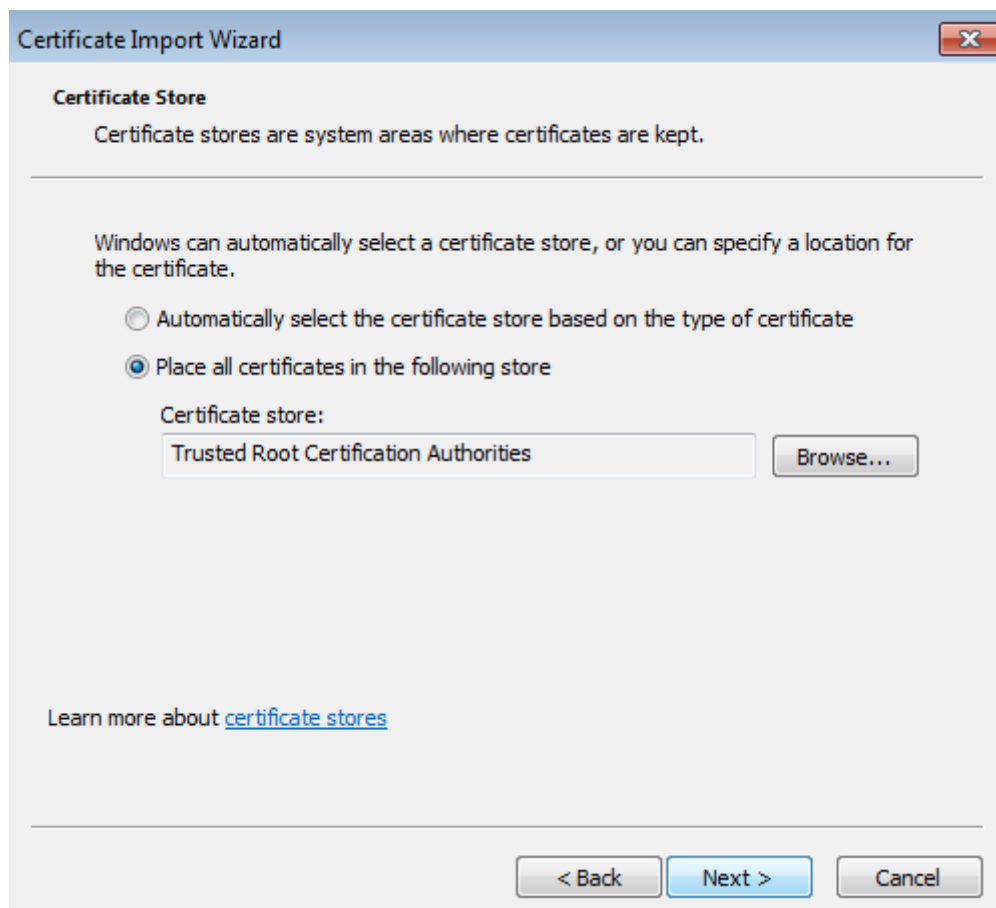
Certificate Import Wizard

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



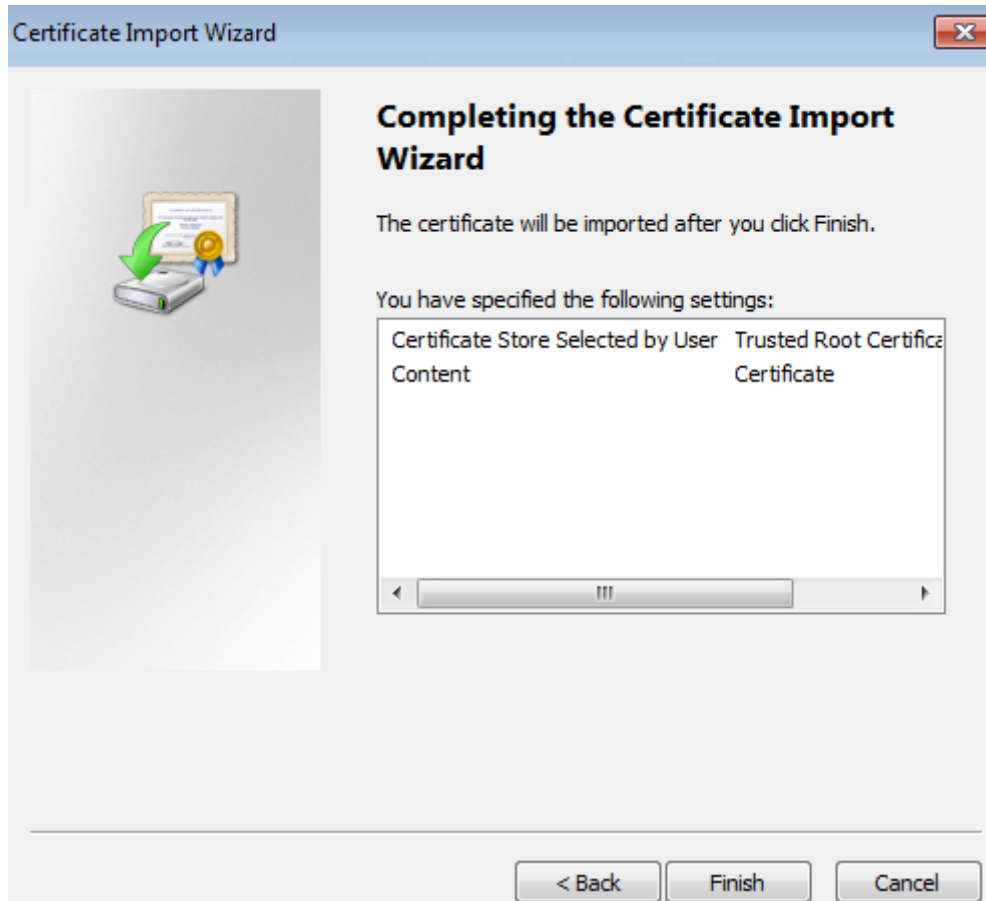
Importing the previously saved certificate

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



Selecting a certificate store

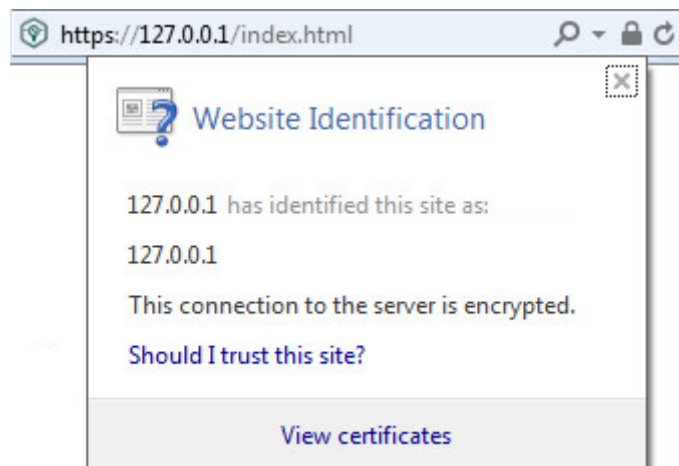
4. On the last page of the Certificate Import Wizard, click **Finish**.



Completing the certificate import

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

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

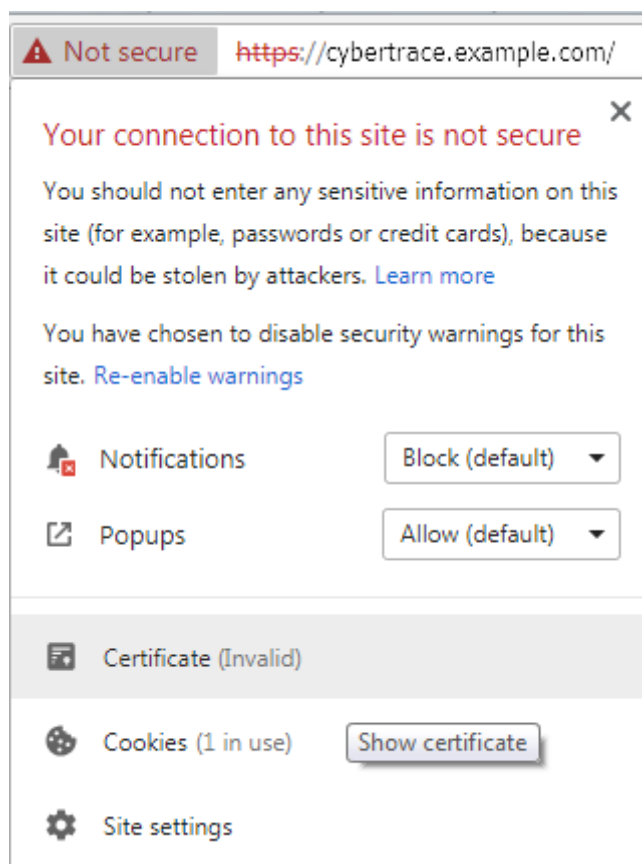


Website identification

Causing a self-signed certificate to be trusted by a browser (CyberTrace Web opens in Google Chrome installed on a Windows system)

To make the self-signed certificate for CyberTrace Web trusted when using Google Chrome:

1. Open the `https://127.0.0.1` or `https://localhost` address in Google Chrome.
A warning is displayed in the address bar that the connection to the site is not secure.
2. Click the **Not secure** message.
A window opens with security details about the website.



Security details

3. Click **Certificate** to view the certificate information. (When the mouse pauses over **Certificate**, a **Show certificate** tooltip appears.)
4. In the **Certificate** window that opens, 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

5. Follow the Wizard instructions.

Use the default Wizard settings during the certificate export.

6. After the certificate is saved to a local disk, open it and add it to the Trusted Root Certification Authorities store, as described in the procedure for Internet Explorer.

7. Restart the browser.

Causing a self-signed certificate to be trusted by a browser (CyberTrace Web opens in Mozilla Firefox)

You add CyberTrace Web to the list of Mozilla Firefox trusted web addresses so that the browser will not display warnings about the certificate.

Causing a self-signed certificate to be trusted by a browser (CyberTrace Web opens in a browser for Linux)

Procedures for using a browser to import a certificate as trusted (on Linux systems) vary depending on the browser and Linux distribution used. But the procedures share common steps: to open the browser settings form and use the form to import the certificate to a store.

To manually cause a self-signed certificate to be trusted by a browser on a Linux system:

1. Create a `/usr/local/share/ca-certificates/` directory if it does not exist on your computer:

```
mkdir /usr/local/share/ca-certificates/
```

2. Copy your root certificate (.crt file) to the created directory:

```
cp <full path to the certificate> /usr/local/share/ca-certificates/
```

3. Update the certificates:

```
sudo update-ca-certificates
```

If you do not have the ca-certificates package, install it with your package manager.

Removing a certificate from the list of trusted ones

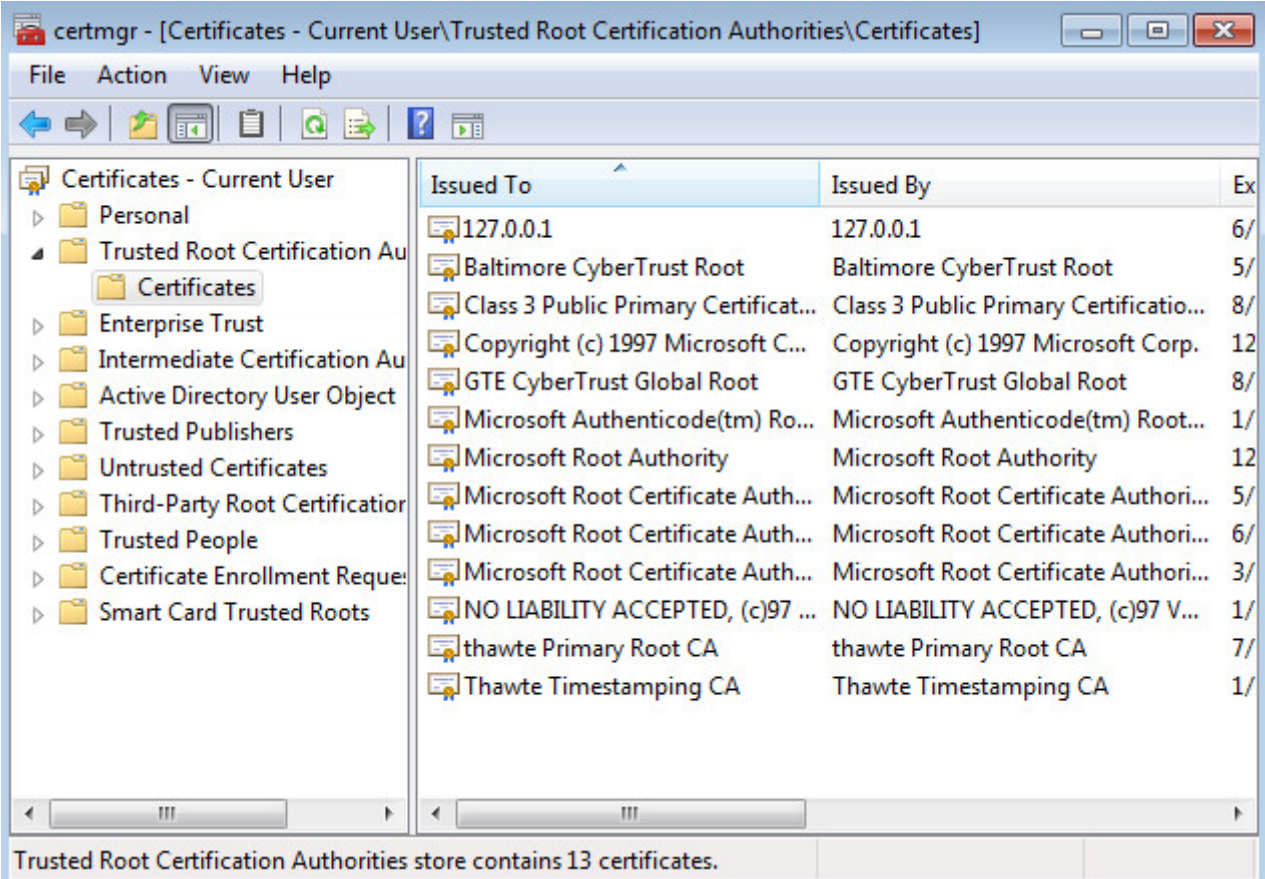
After you have reconfigured or uninstalled CyberTrace, old certificates are no longer used by CyberTrace. You can remove them from the list of trusted certificates.

To remove a certificate from the list of trusted certificates (on Windows):

1. Open the Certificates management console, and then run the following command:

```
certmgr.msc
```

2. In the tree pane, select **Trusted Root Certification Authorities > Certificates**.



Certificates management console

3. In the results pane, right-click the added certificate, and then select **Delete**.

On a Linux system, the removal procedure is performed in a way that is similar to the addition of a certificate: open the list of the trusted certificates and remove those that you do not need.