



DCB, Inc.
2949 CR 1000 E
Dewey, Illinois
61840

217.897.6600 Tel
800.432.2638 Toll Free
217.897.1331
www.dcbnet.com

Adding a Self-Signed Web Certificate to the Certificate Store

01/27/2025

Introduction

This guide steps through the process of adding a self-signed web certificate to a Windows computer certificate store. The purpose is to eliminate the security warning, displayed by the web browser, when connected to the device. Once the certificate is installed, it can serve as verification that you are communicating with **your** device and not an impostor device.

The method here will work with any web browser that utilizes the Window's certificate store. This includes Edge, Explorer, and Chrome. Firefox does not utilize the Window's certificate store. The self-signed certificate can be similarly imported into the Firefox certificate store using it's internal certificate manager. However, it will continue to display a security warning although it will no longer ask for an exception.

1: Generate a new web certificate for the unit. Give it a unique name and include the unit's IP address in the certificate. Up to two IP addresses may be added. Submit the form and then activate and store the changes. This will result in another security error from the web browser.

The screenshot shows a web browser window with the address bar displaying `https://192.168.1.62/cgi-bin/menuform.cgi?select=Admin_Menu&form=form_web_cert`. The page title is "XT-3305s" and the timestamp is "01-10-2019 10:36:51". The main content area is titled "Generate Web Certificate" and contains the following form fields:

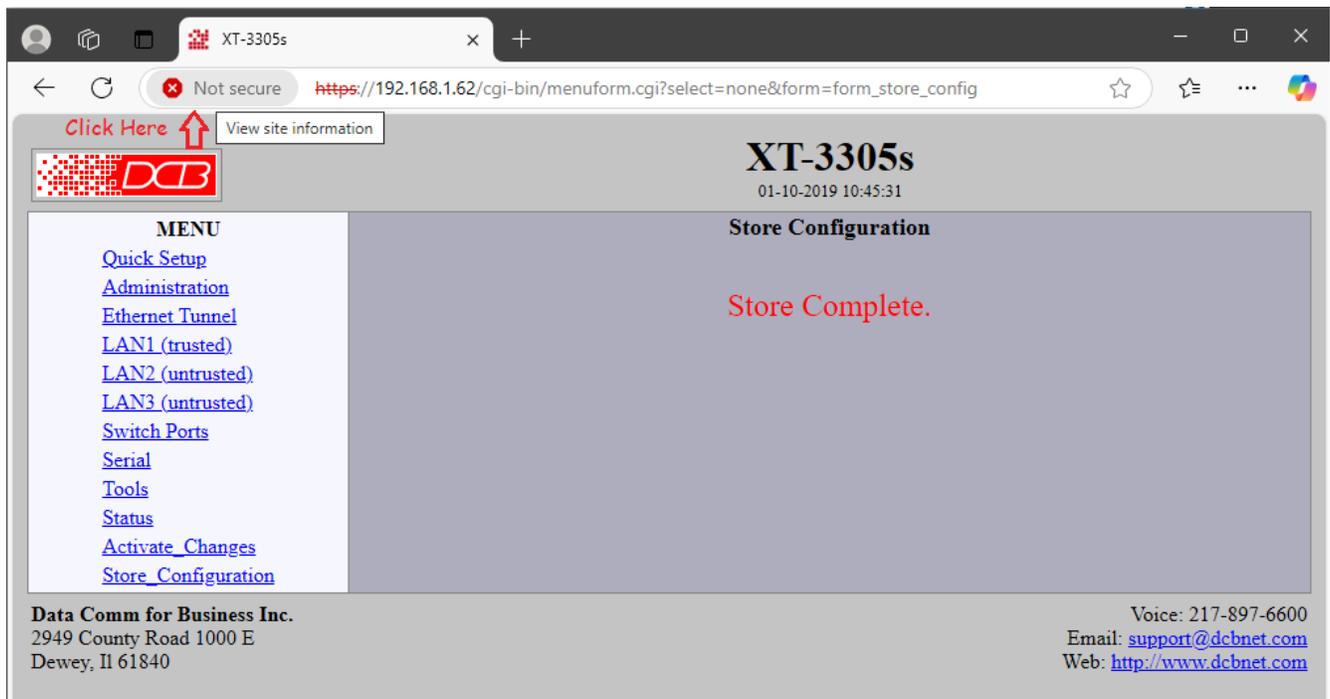
- Name: DCB Tunnel
- Organization: My Company
- Organizational Unit: My Department
- Country Code: US
- State/Province: My State
- Locality: My Town
- Subject Alternative Name-1: 192.168.1.62
- Subject Alternative Name-2: (empty)

Red annotations on the form include:

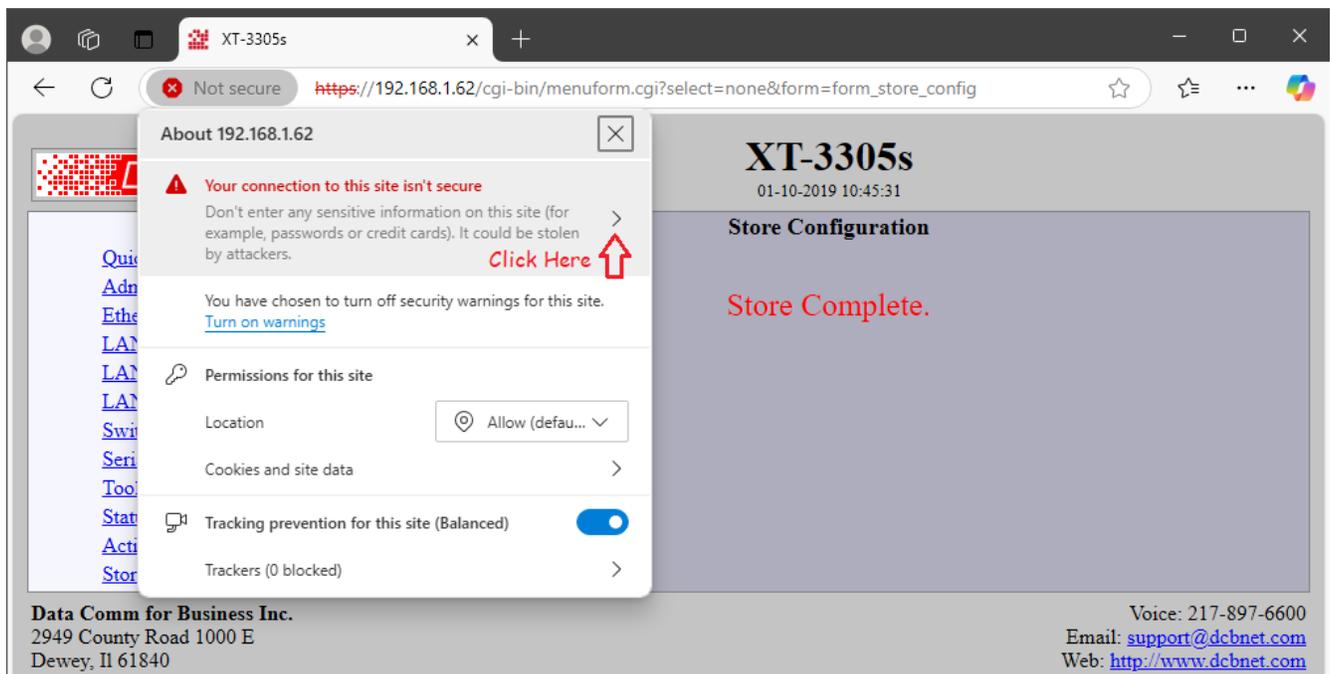
- An arrow pointing to the "Name" field with the text: "Set a unique name for the device".
- An arrow pointing to the "Subject Alternative Name-1" field with the text: "Add unit IP address to certificate. Second IP address can also be added."

At the bottom of the form, there are "Submit" and "Cancel" buttons. A note below the form states: "Note: Certificate generation may take several minutes to complete."

2: Export the unit's web certificate to the local computer. Start by viewing the *Site Information*.



4: View detailed information regarding the warning.



4: View the certificate.

The screenshot shows a web browser window with a security warning overlay. The warning message reads: "Your connection to this site isn't secure". Below this, it states: "The certificate for this site is not valid. Click here ↑ Show certificate". A further explanation says: "Because this connection is not secure, information (such as passwords or credit cards) will not be securely sent to this site and may be intercepted or seen by others. We suggest you don't enter personal information into this site or avoid using this site. Learn more".

The background page is titled "XT-3305s" and "Store Configuration". It displays the date and time "01-10-2019 10:45:31" and a large red message: "Store Complete.".

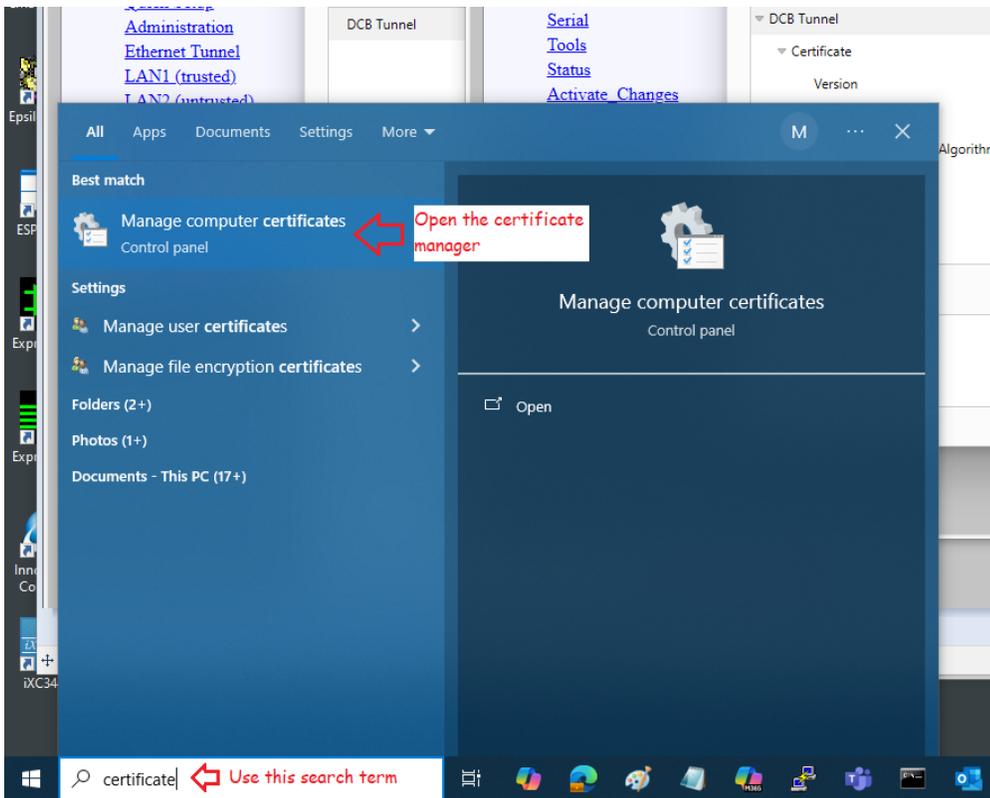
At the bottom of the page, contact information for "Data Comm for Business Inc." is provided: "2949 County Road 1000 E Dewey, IL 61840". On the right side, contact details include: "Voice: 217-897-6600", "Email: support@dcbnet.com", and "Web: <http://www.dcbnet.com>".

5: The certificate can now be exported to the local PC. Make a note of where the certificate was stored on the PC. The **Downloads** folder is the usual location.

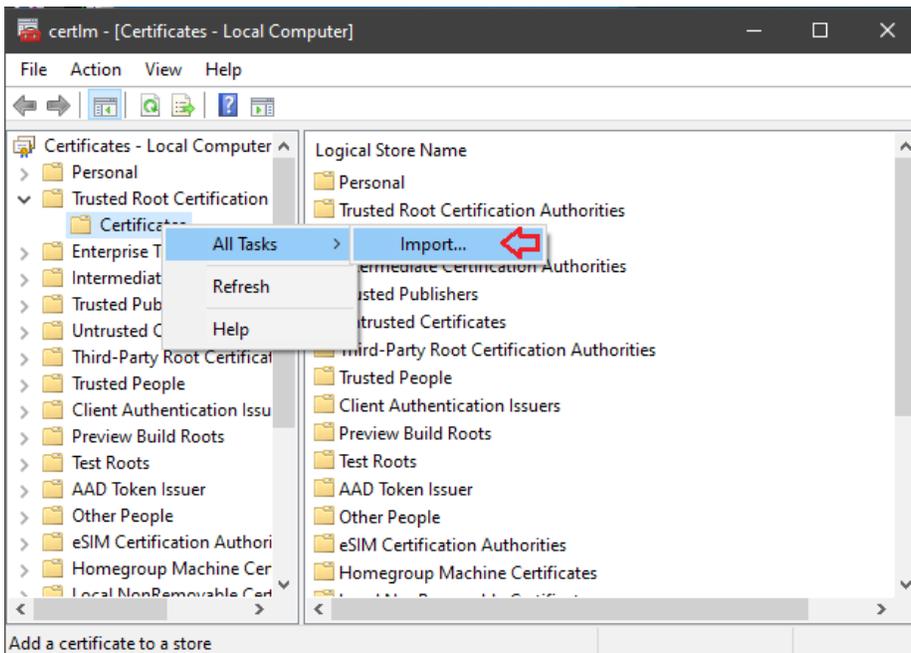
The screenshot displays a web browser window with the following elements:

- Browser Address Bar:** Shows the URL `https://192.168.1.62/cgi-bin/menuform.cgi?select=none&form=form_store_config`.
- Page Header:** Includes the DCB logo and the title "Certificate Viewer: DCB Tunnel".
- Navigation Tabs:** "General" and "Details" tabs are present. A red arrow points to the "Details" tab with the text "Select the Details tab."
- Left Sidebar (MENU):**
 - Quick Setup
 - Administration
 - Ethernet Tunnel
 - LAN1 (trusted)
 - LAN2 (untrusted)
 - LAN3 (untrusted)
 - Switch Ports
 - Serial
 - Tools
 - Status
 - Activate Changes
 - Store Configuration
- Main Content Area:**
 - Certificate Hierarchy:** A list containing "DCB Tunnel".
 - Certificate Fields:** A tree view showing "DCB Tunnel" expanded to "Certificate", which includes fields: "Version", "Serial Number", "Certificate Signature Algorithm", "Issuer", and "Validity" (with "Not Before" listed below).
 - Field Value:** A large empty text box for displaying the certificate's value.
- Bottom Right:** An "Export..." button is visible, with a red arrow pointing to it and the text "Click on export".
- Footer:** Contact information for Data Comm for Business Inc. (2949 County Road 1000 E, Dewey, IL 61840) and support@dcbnet.com is displayed on both the left and right sides.

6: Open the PC's certificate manager.



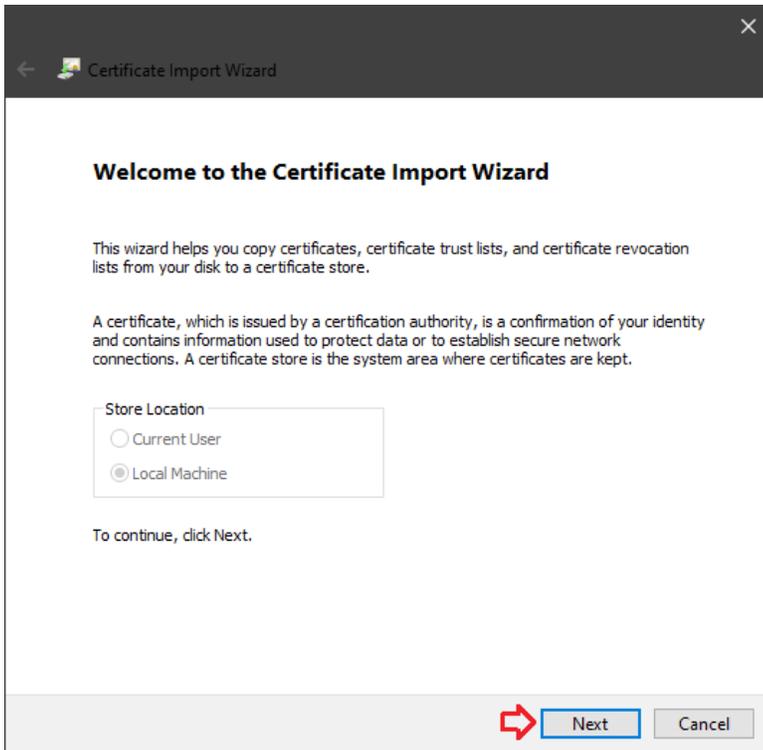
7: Import a certificate to the *Trusted Root Certifications Authorities*.



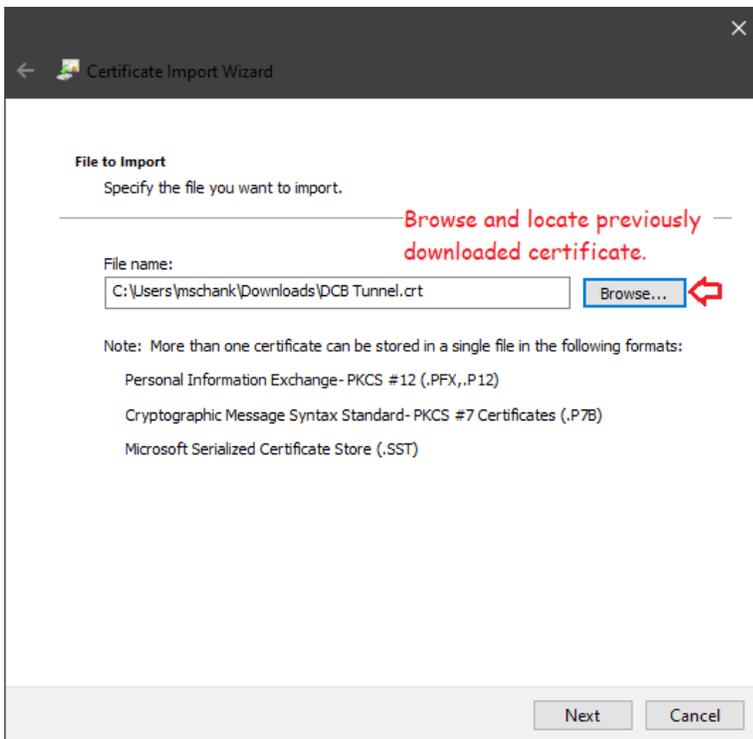
1: Click on Trusted Root Certification to expand.

2: Right-click on Certificates and select All Tasks -> Import

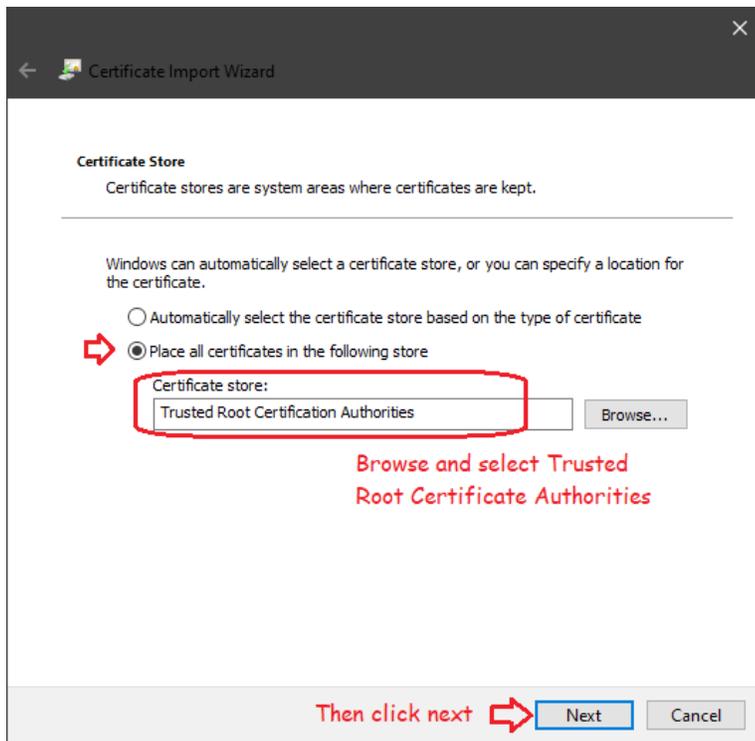
8: The *Certificate Import Wizard* will guide you through the process.



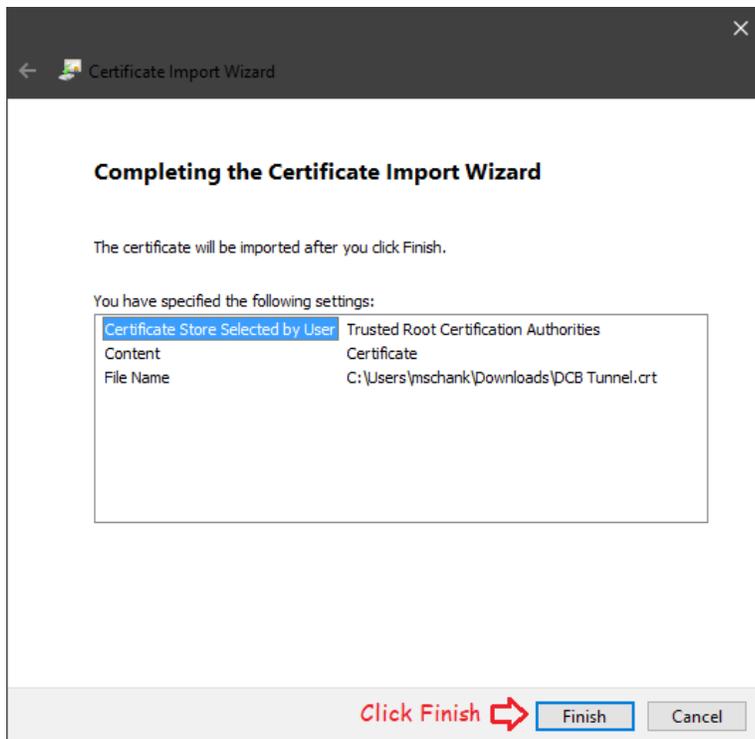
9: Locate and choose the certificate we downloaded from the unit.



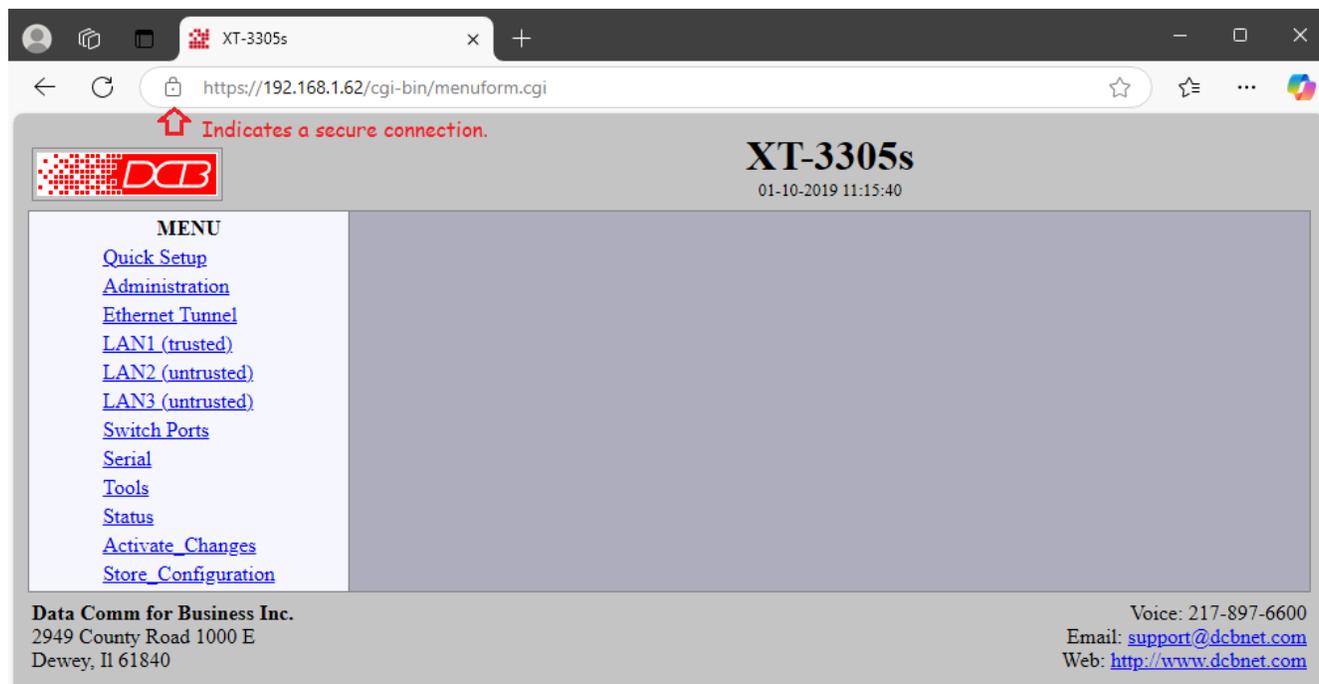
10: Manually select the *Trusted Root Certification Authorities* store.



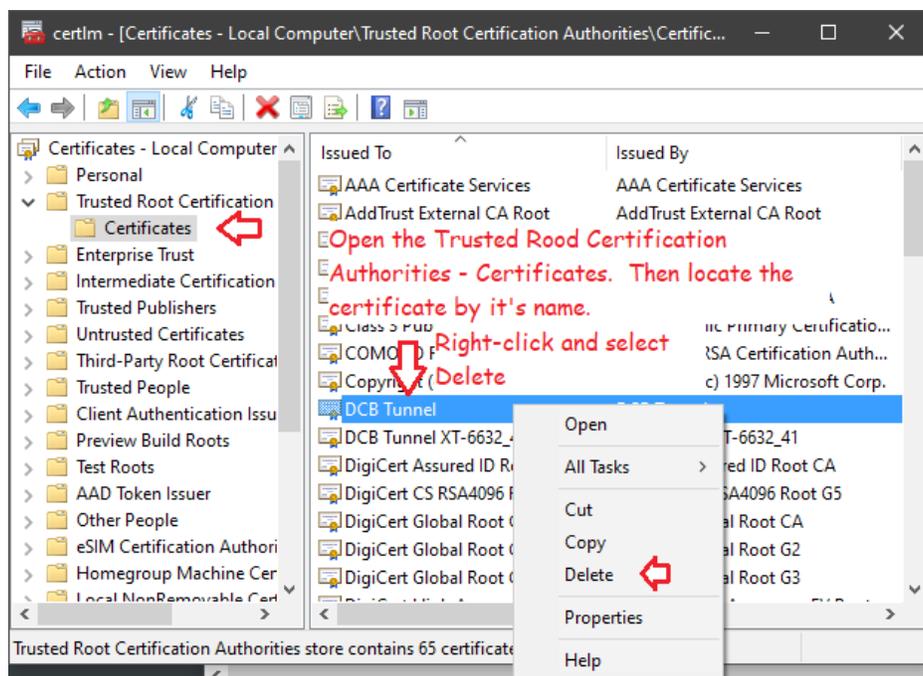
11: Finish the import.



12: The web browser will replace the **Not secure** designation with a padlock icon.



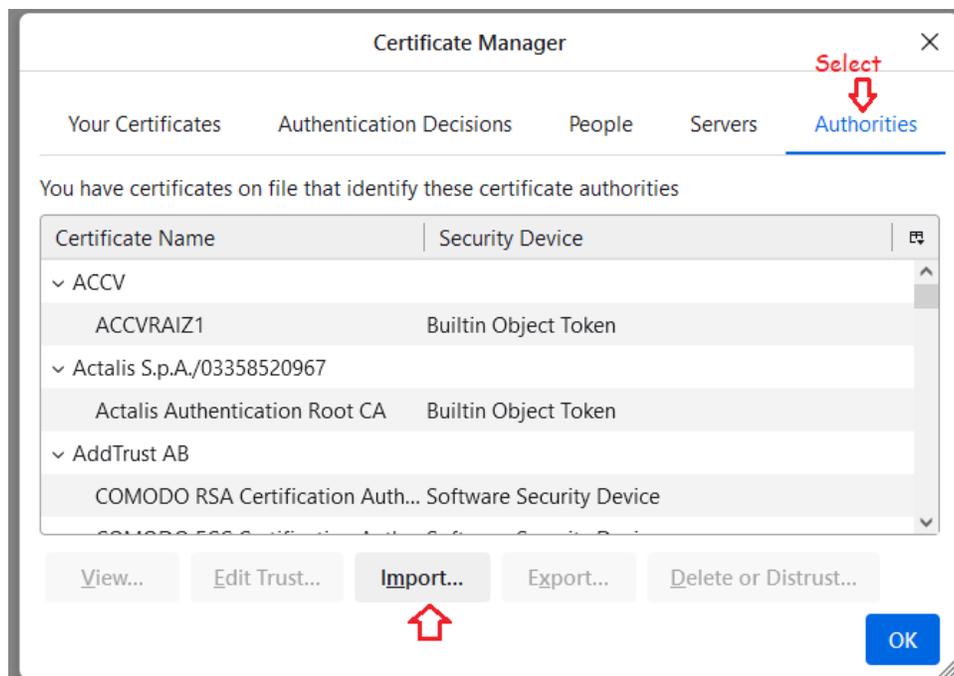
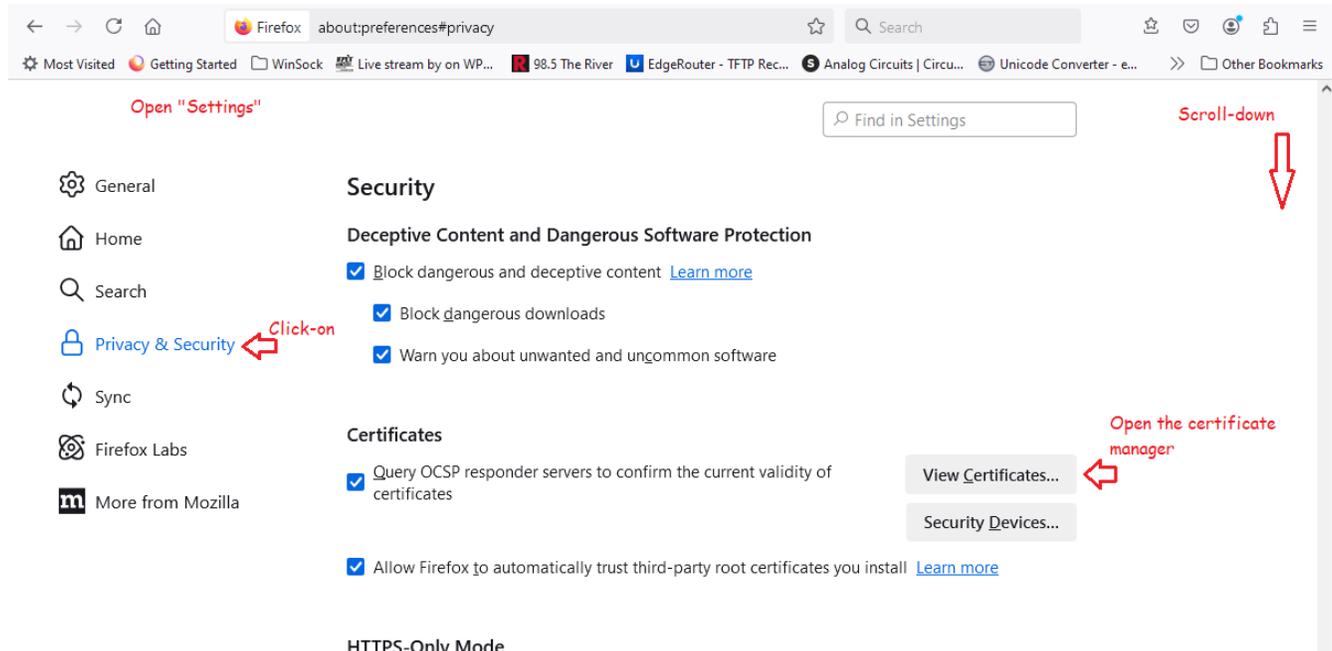
If you have the need to remove or replace a certificate, use the System Certificate Manager to locate the old certificate and to delete it.



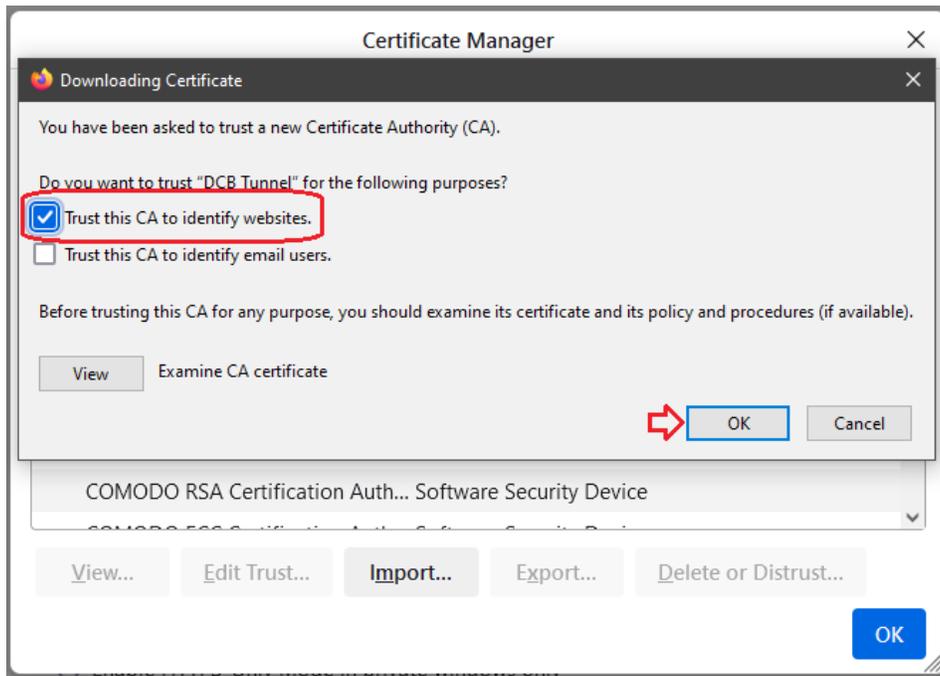
Firefox notes:

Firefox automatically stores “exceptions” to its certificate store. Once the exception has been added for a site, it will no longer ask for confirmation to continue to a site. However, it will continue to show a padlock with an ‘!’ to indicate an exception has been added from the site. There is no need to perform the steps shown below as they do not change the behavior of Firefox. These notes are simply reference of how to access the Firefox certificate manager.

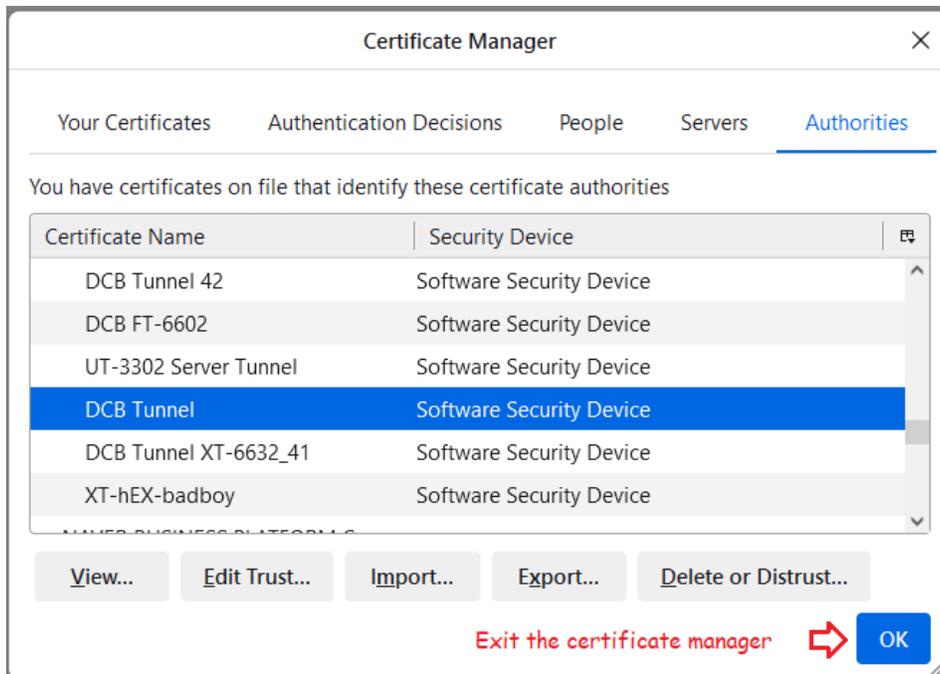
Opening the Firefox certificate manager.



Browse and locate the exported certificate. Use it to identify websites.



Exit the certificate manager.



As always, if you have any problems, phone or email DCB Tech Support.