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

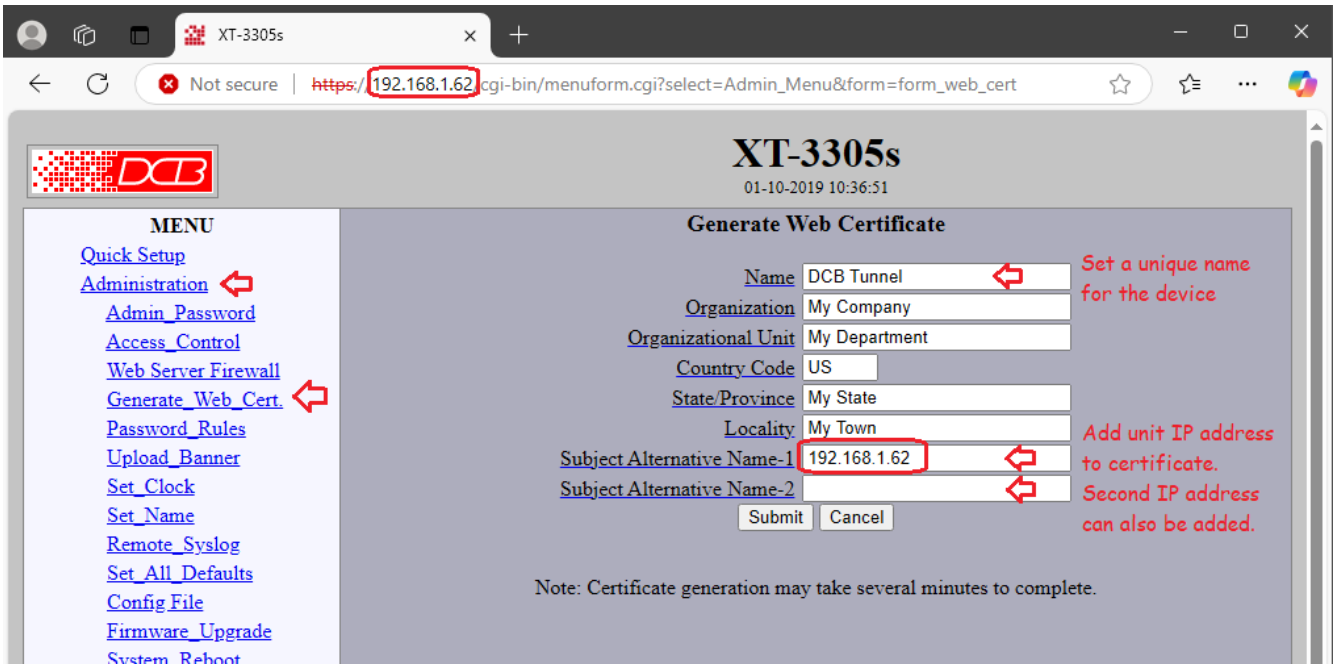
01/27/2025

Introduction

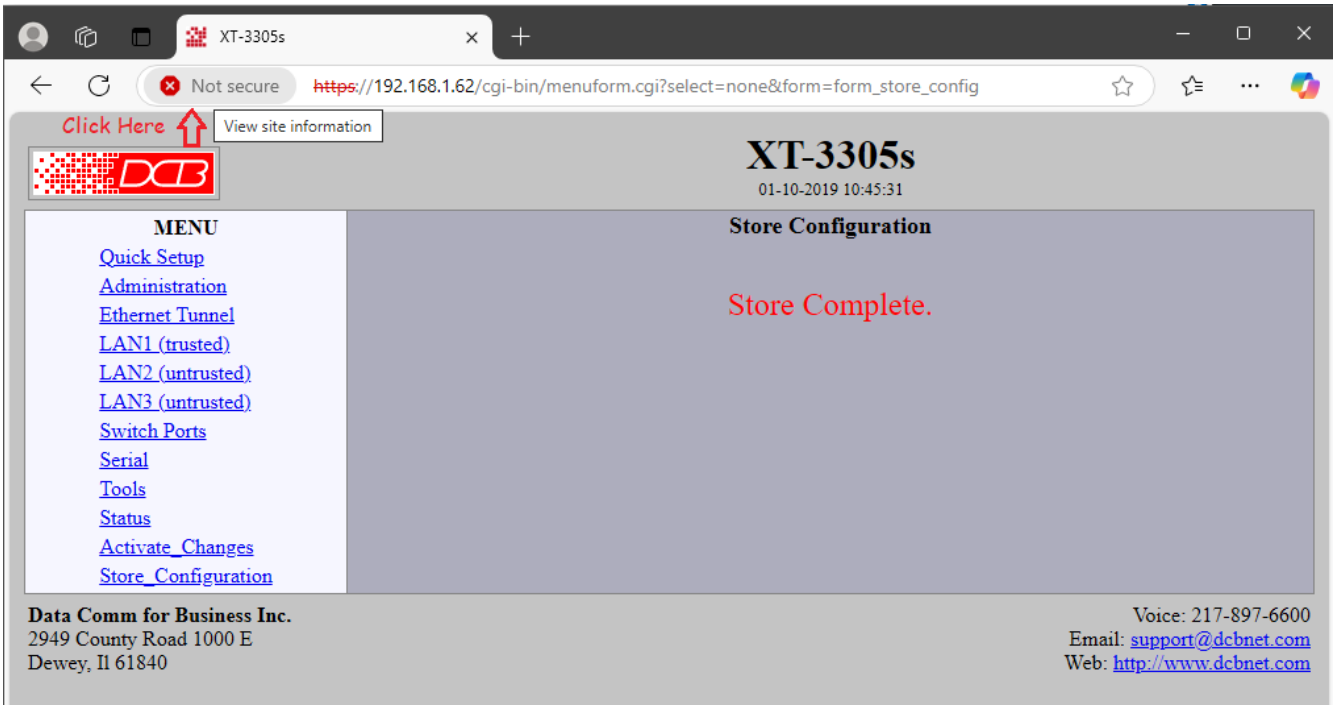
This guide steps through the process of adding a self-signed web certificate to a Windows computer certificate store. The purpose is to eliminate the security warning, displayed by the web browser, when connected to the device. Once the certificate is installed, it can serve as verification that you 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.

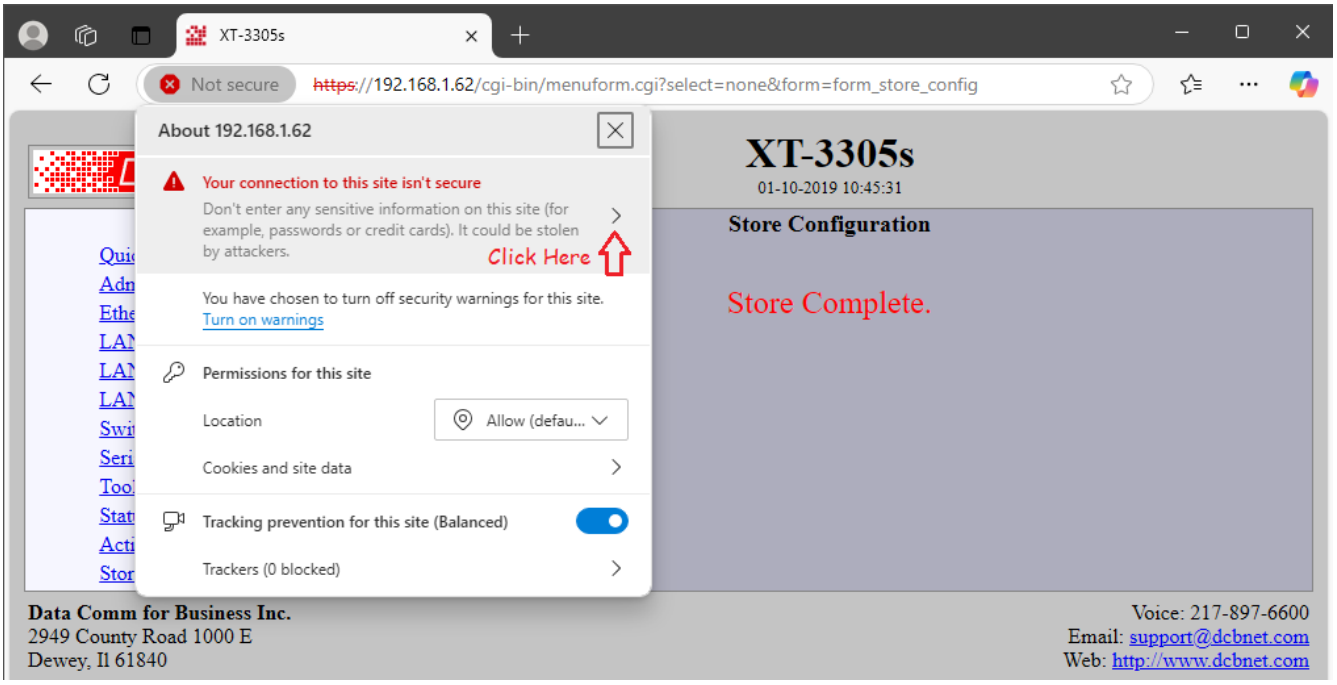
1: Generate a new web certificate for the unit. Give it a unique name and include the unit's IP address in the certificate. Up to two IP addresses may be added. Submit the form and then activate and store the changes. This will result in another security error from the web browser.



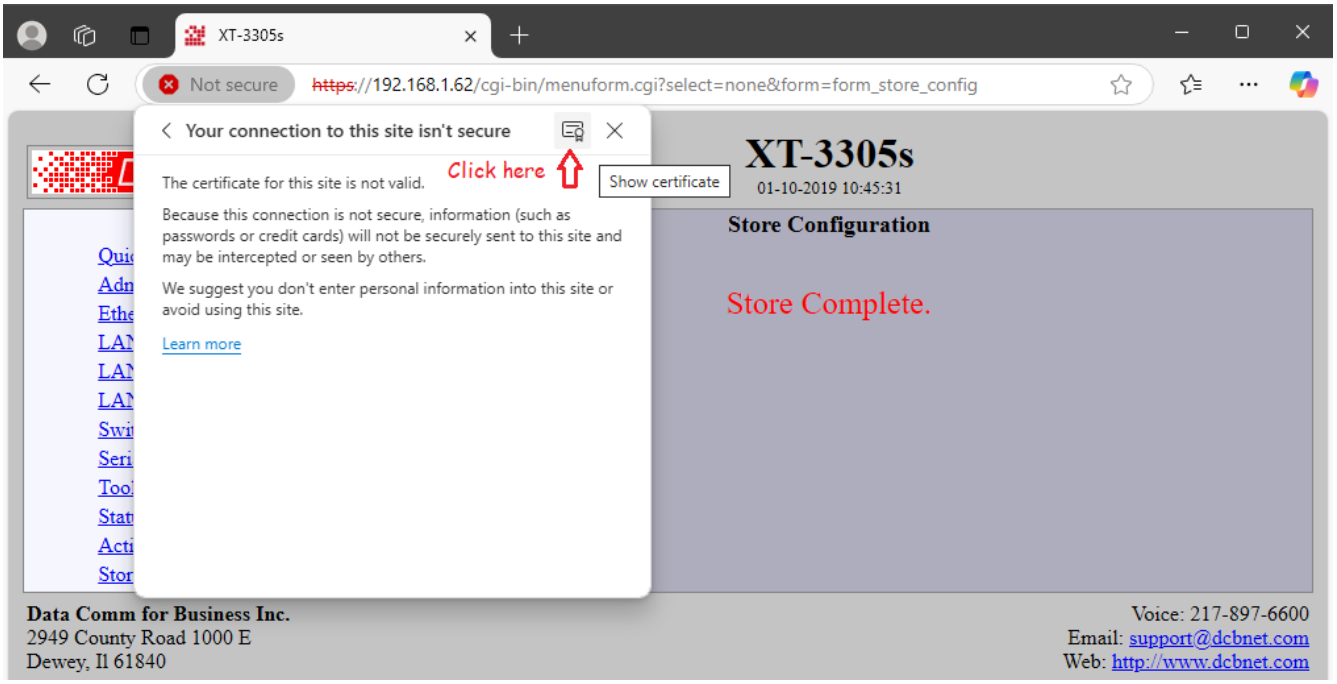
2: Export the unit's web certificate to the local computer. Start by viewing the ***Site Information***.



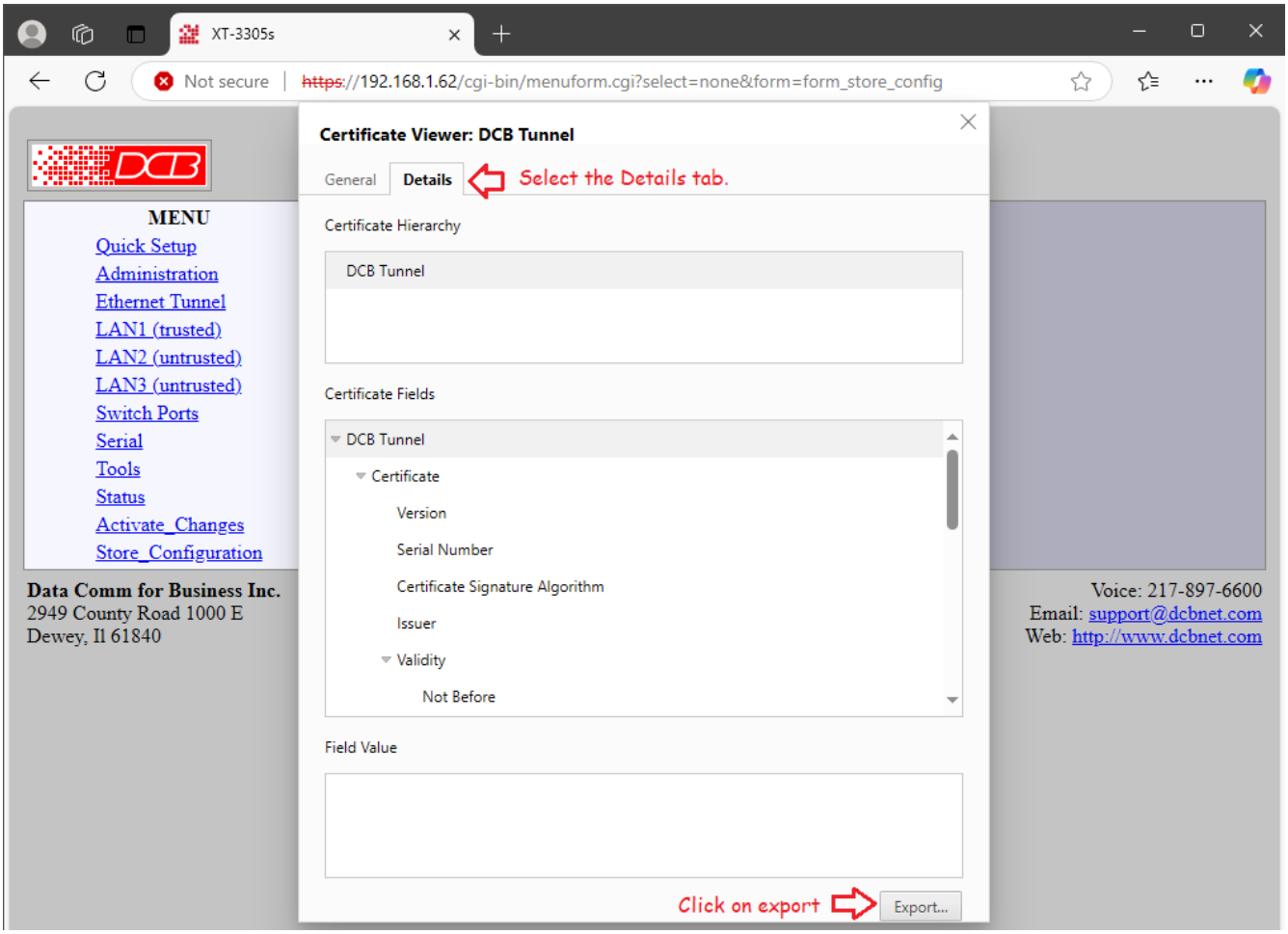
4: View detailed information regarding the warning.



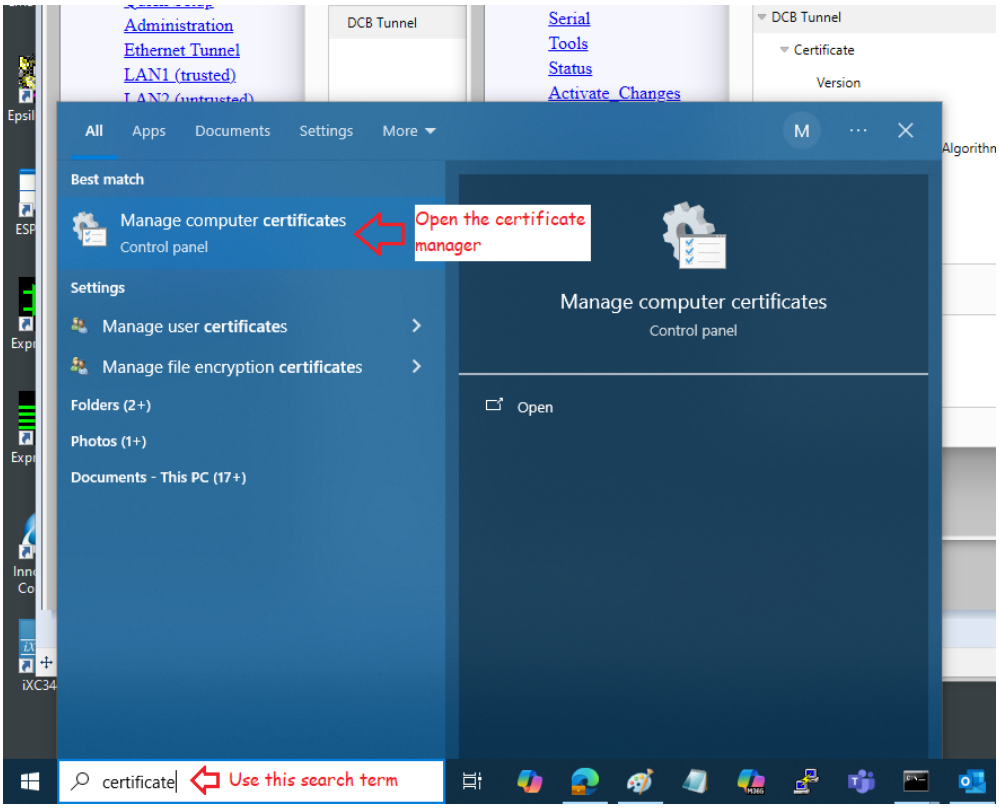
4: View the certificate.



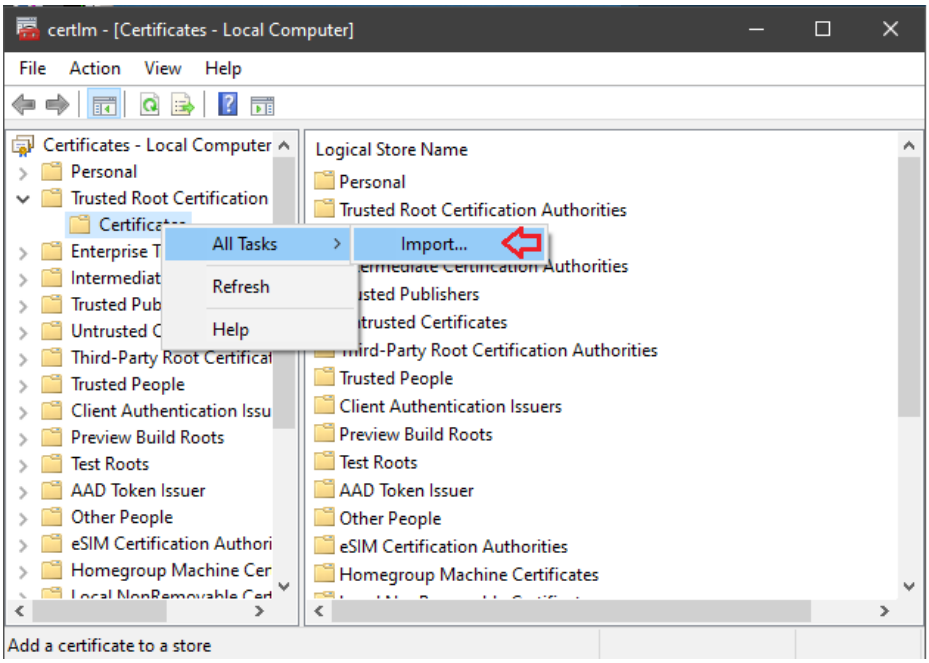
5: The certificate can now be exported to the local PC. Make a note of where the certificate was stored on the PC. The ***Downloads*** folder is the usual location.



6: Open the PC’s certificate manager.



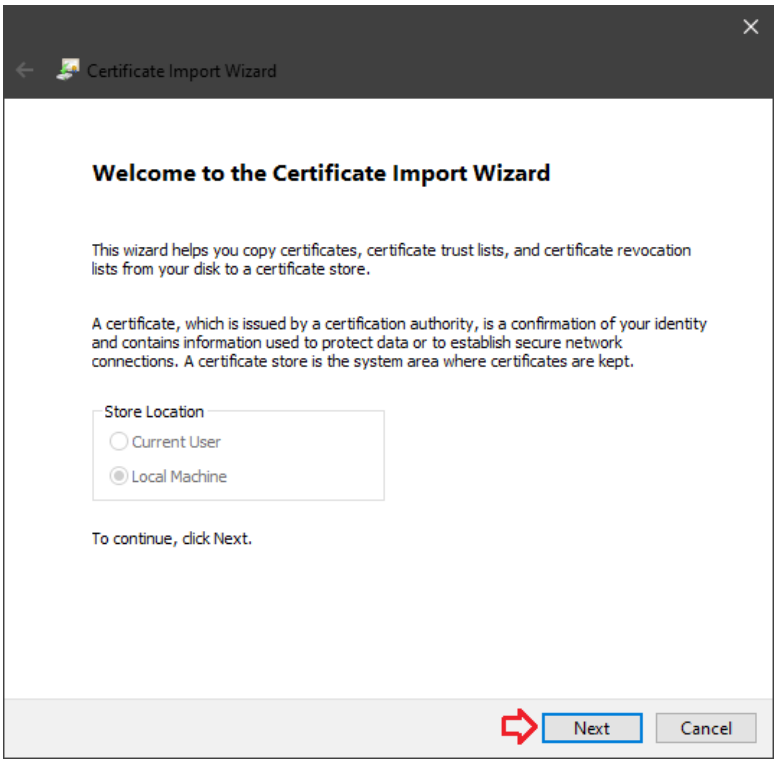
7: Import a certificate to the ***Trusted Root Certifications Authorities***.



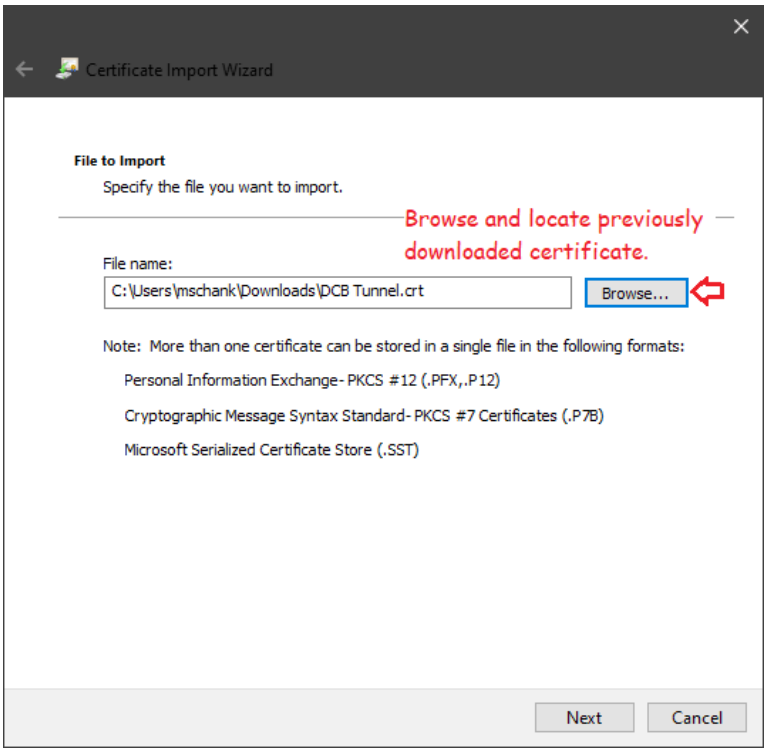
1: Click on Trusted Root Certification to expand.

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

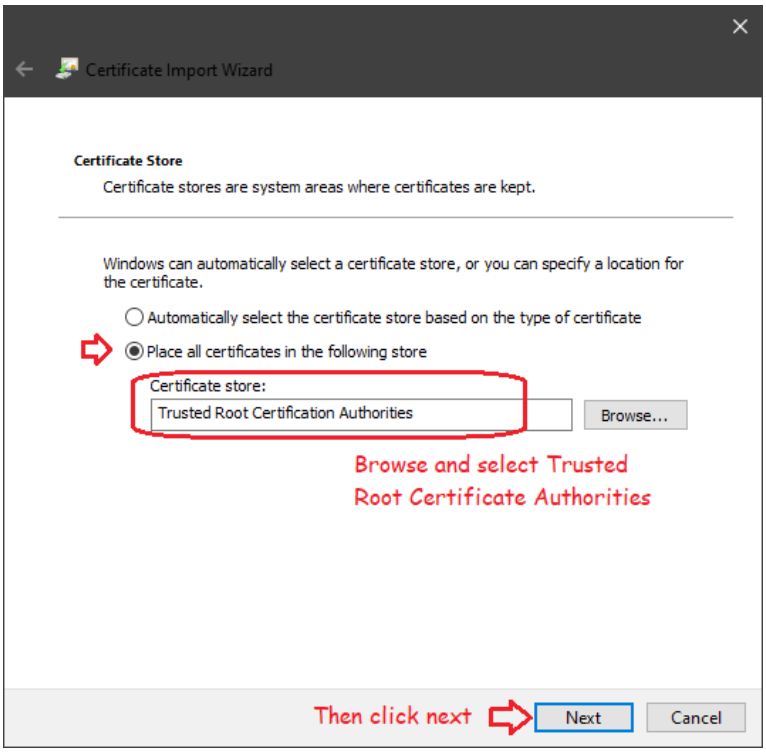
8: The ***Certificate Import Wizard*** will guide you through the process.



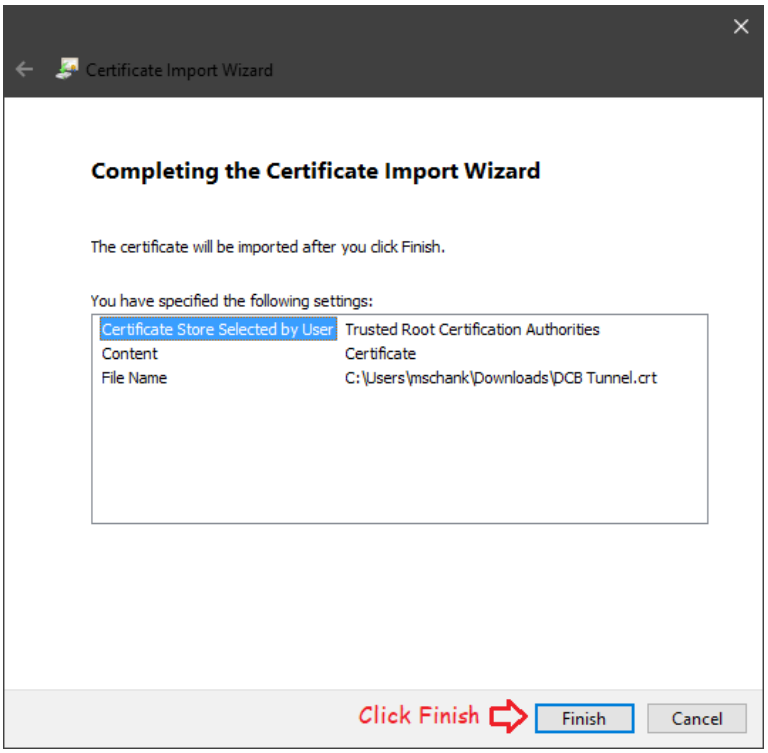
9: Locate and choose the certificate we downloaded from the unit.



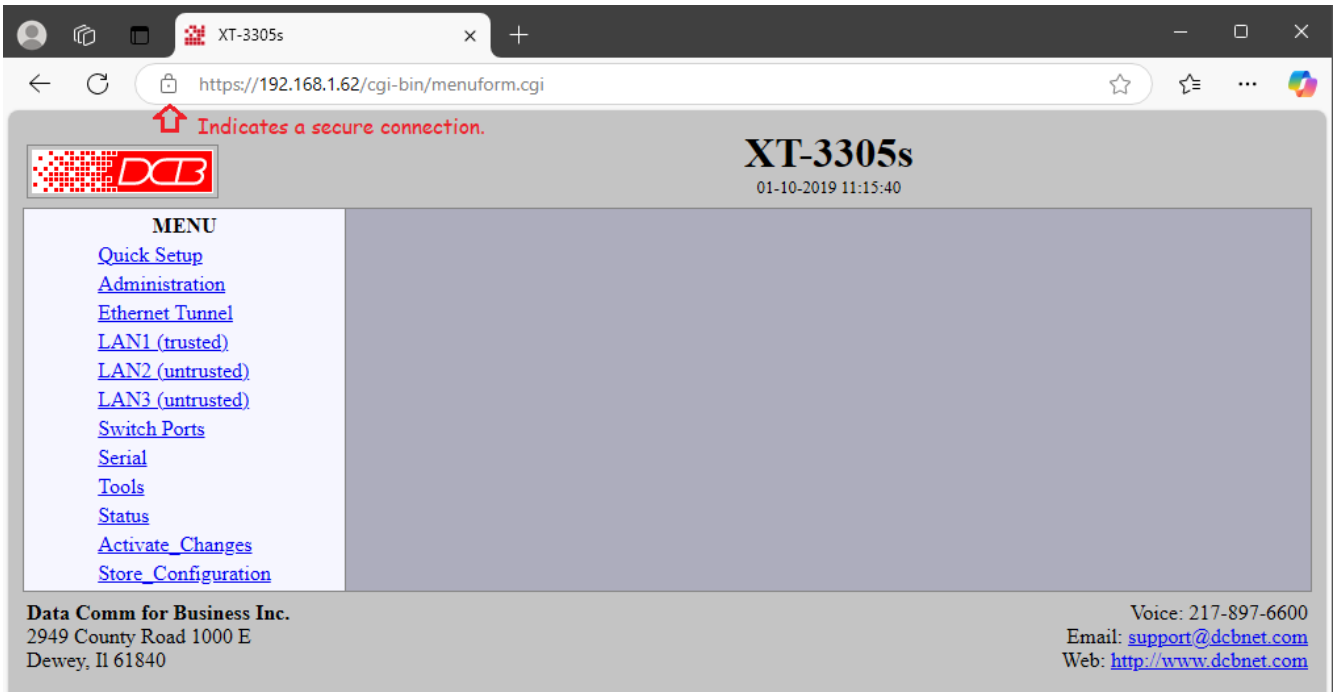
10: Manually select the ***Trusted Root Certification Authorities*** store.



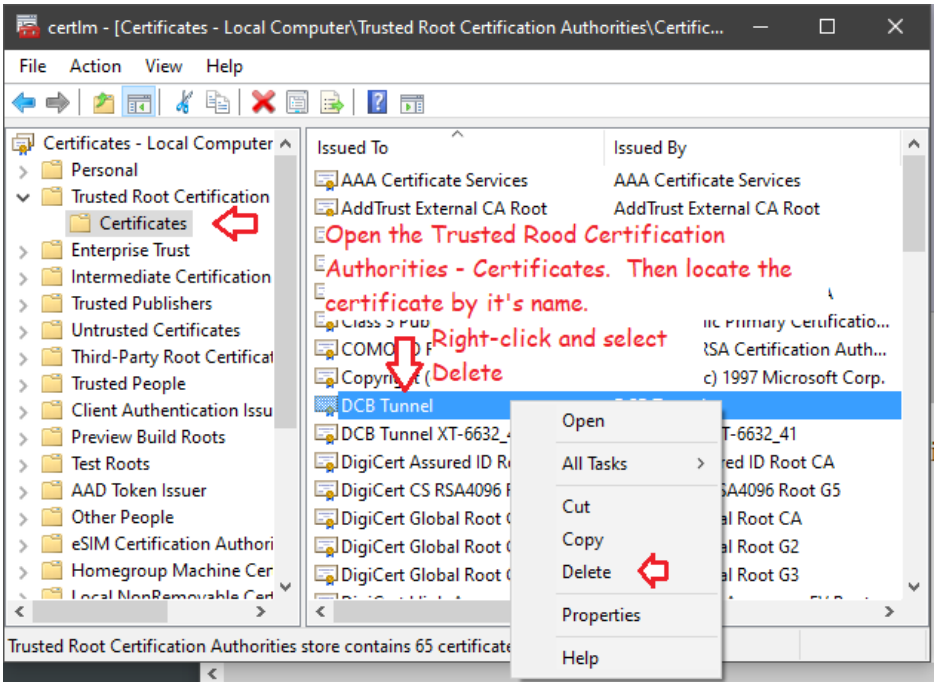
11: Finish the import.



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



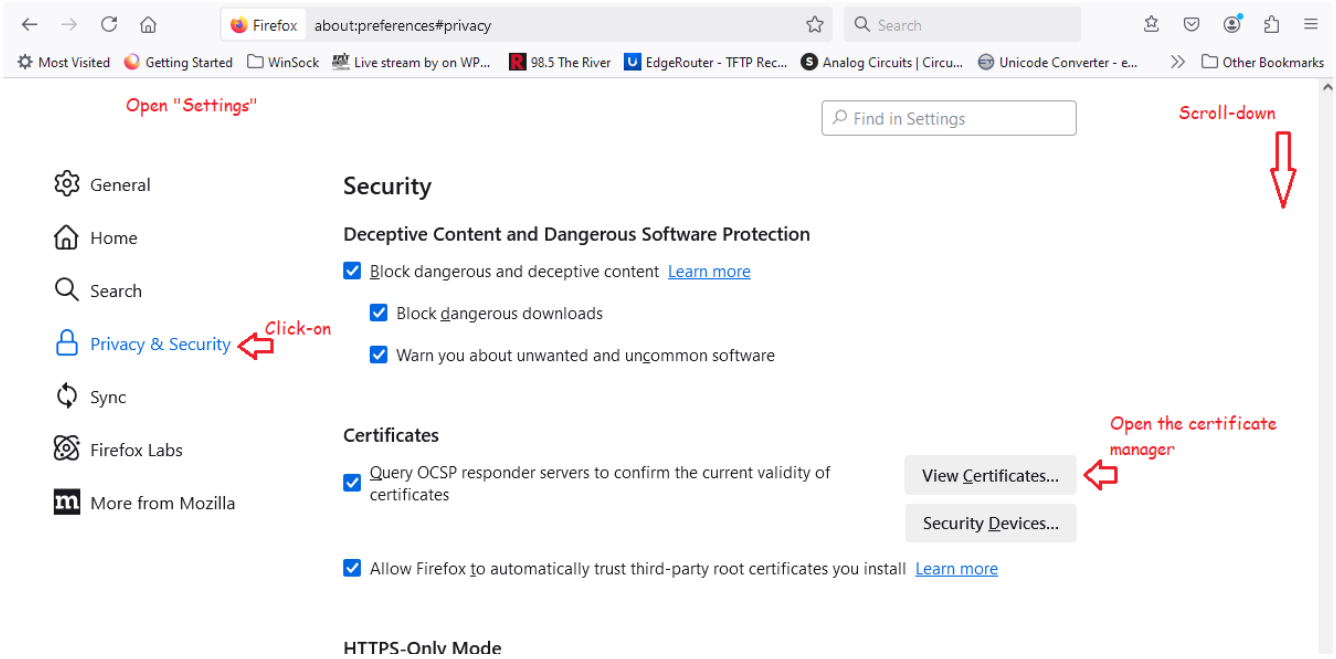
If you have the need to remove or replace a certificate, use the System Certificate Manager to locate the old certificate and to delete it.

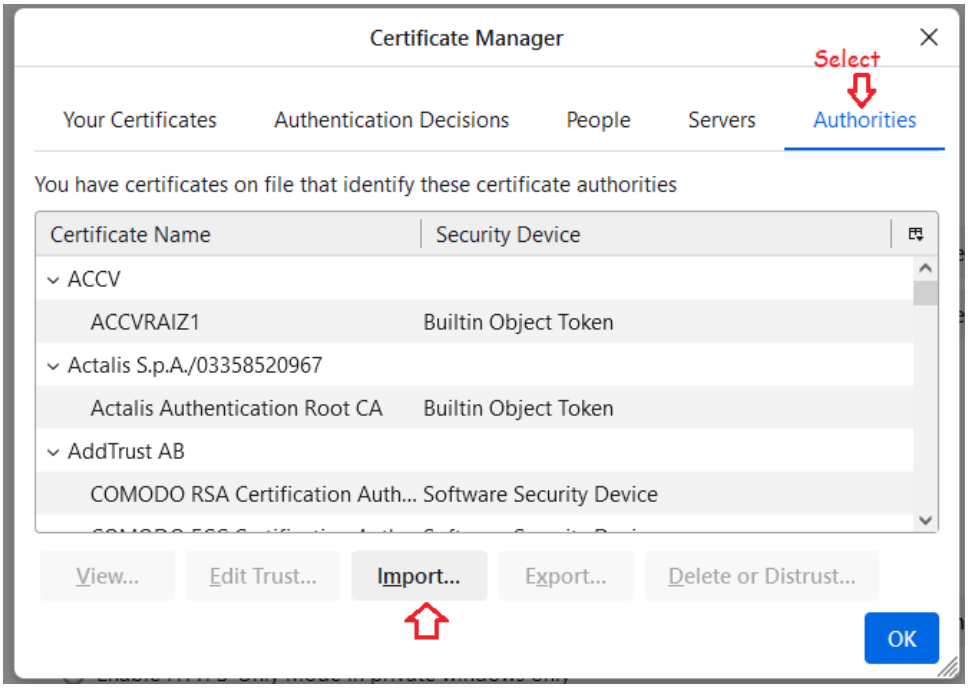


Firefox notes:

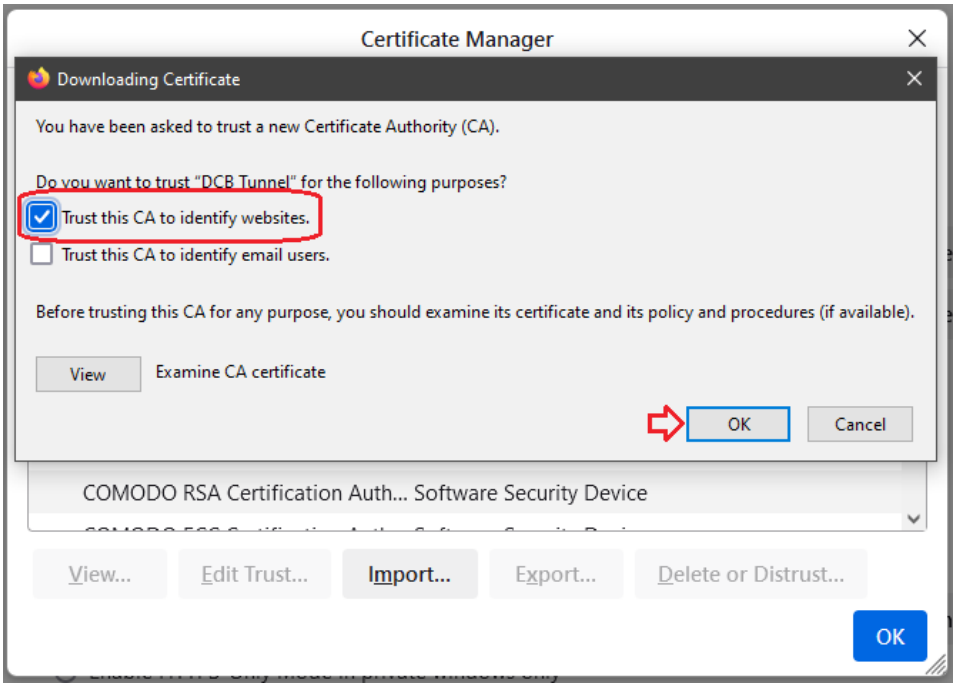
Firefox automatically stores “exceptions” to its certificate store. Once the exception has been added for a site, it will no longer ask for confirmation to continue to a site. However, it will continue to show a padlock with an ‘!’ to indicate an exception has been added fro the site. There is no need 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.

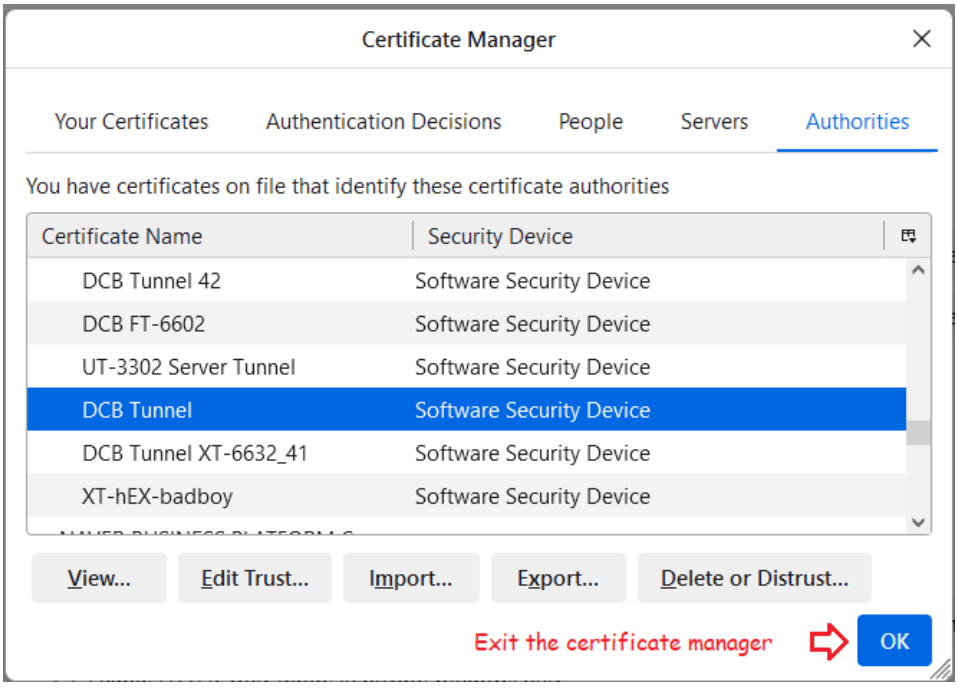




Browse and locate the exported certificate. Use it to identify websites.



Exit the certificate manager.



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