niagara4 Certificates

A certificate is an electronic document that uses a digital signature to bind a public key with a person or organisation. Their primary purpose within Niagara is to verify the identity of a server so that communication can be trusted. Certificates create a chain of trust which consists of multiple components.

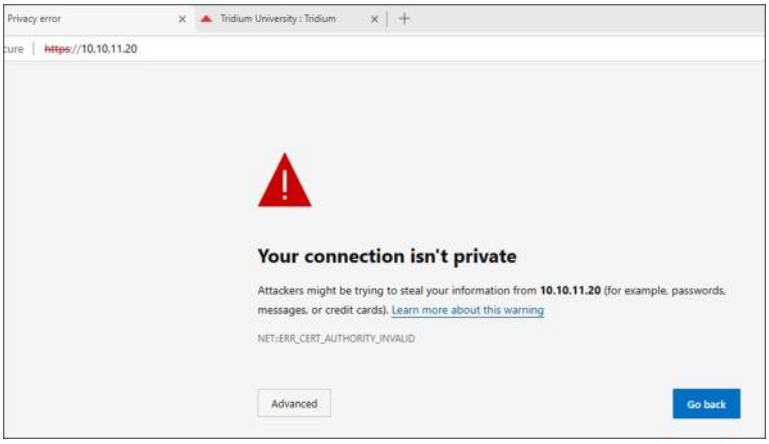
The **RootCA Certificate** is the foundation at the top of the trust hierarchy and acts as an anchor for the subsequent chains of trust. It must be loaded into all participating hosts, stations and browsers.

The **Server Certificate** is a digital file that authenticates a website's identity and enables encrypted communication between the server and a browser via HTTPS to protect data privacy and security.

The Server Certificate uses a **Public Key** that is accessible by anyone to send data, but a **Private Key** is then used to decrypt and view the sent data.

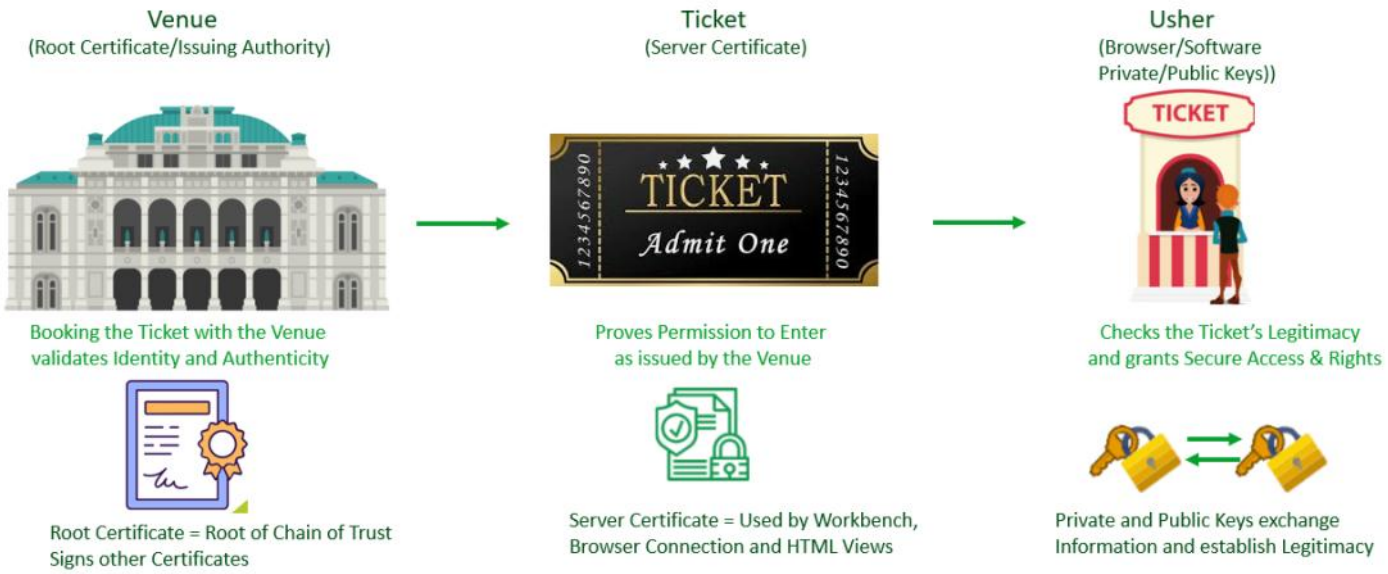
Why Use Certificates

Certificates ensure that all communication is encrypted and therefore hidden from inter-ception and malicious attacks. I Niagara, they also ensure there is no error message when an End User is trying to access the WebPage, warning them that the connection is neither private nor safe.



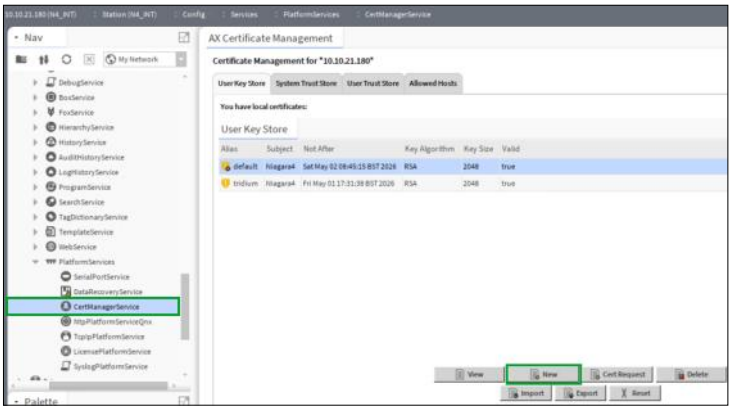
Chain of Trust Simplified

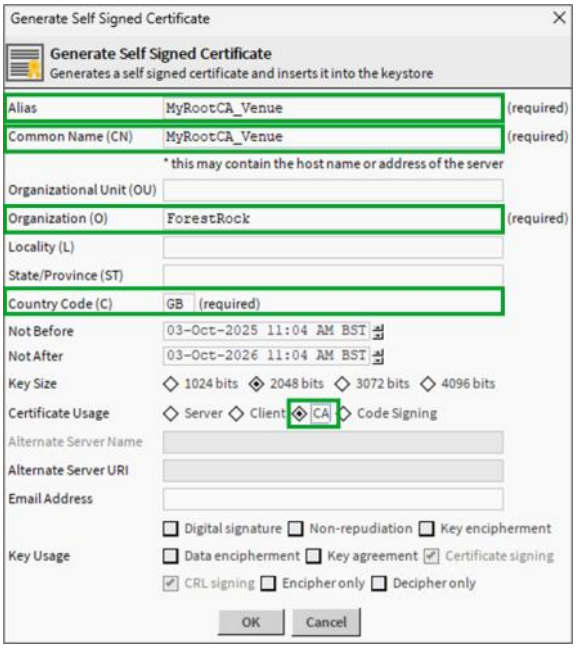
Certificates like a ticket to an event—they prove permission to enter because they have been issued by the venue or events organiser (=RootCA Certificate—Issuing Authority). The ticket itself is the Server Certificate with a unique code or number that is proven to be issued by the venue. The usher at the event on the night embodies the Public and Private keys by checking the ticket's validity and allowing access to the booke seat.



Creating a RootCA Certificate

The CA Certificate is the foundation of the chain of trust and can be created in the station under Config-Services-PlatformServices-CertManagerService. Click NEW in the UserKeyStore to start creating the certificate

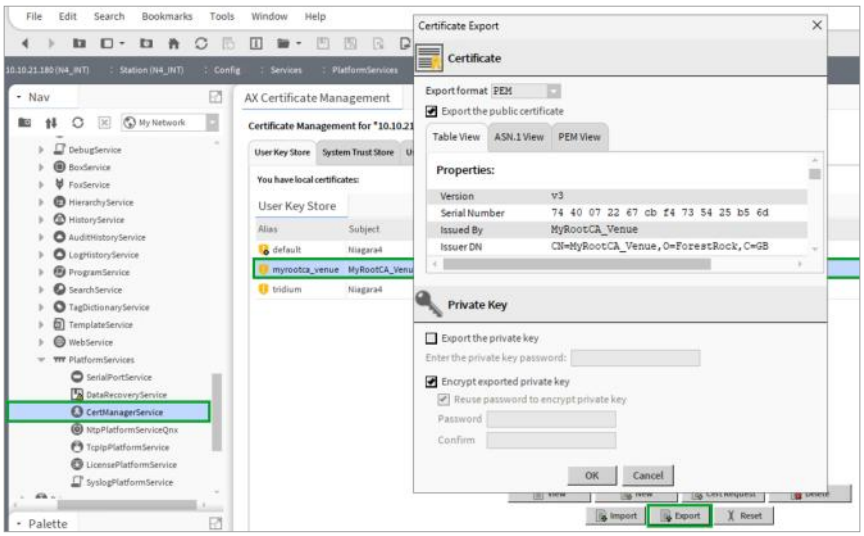




The certificate can be self signed initially, but can also be sent to an official Certificate Signing Authority if heightened security is required by the site.
All fields marked as REQUIRED must be completed, and the CS box ticked for the certificate usage
before clicking OK and moving on to the next step where a password for the Private Key is specified

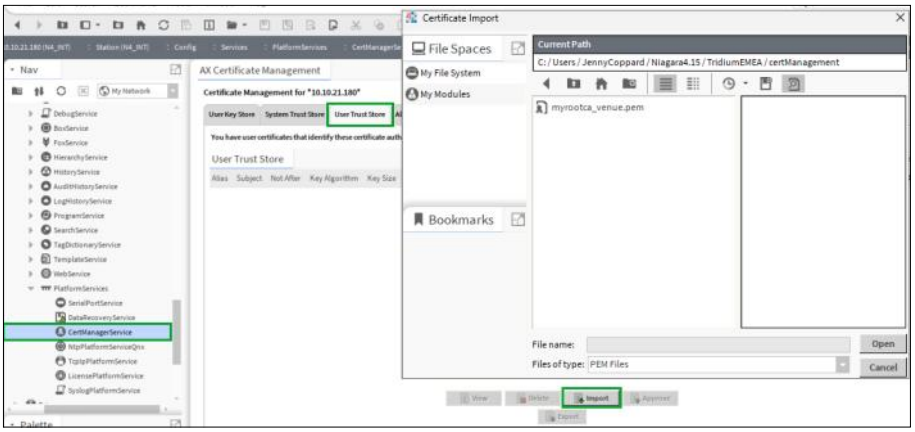
Exporting a RootCA Certificate

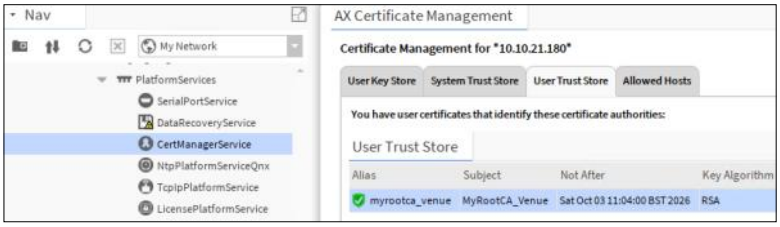
The RootCA certificate has now been created and is visible in the **UserKeyStore** of the CertManagerService, but it is not yet trusted or ready to use in the station. It must be exported to PEM format so it can then be imported to the right places ready to use. The default location for exported PEM files is the **certManagement** folder in UserHome.



Importing a RootCA Certificate to the Station

The RootCA Certificate must be imported into the station.
Navigate to the **UserTrustStore** tab in the CertManagerService and click Import to pick up the PEM file from the certManagement folder in UserHome

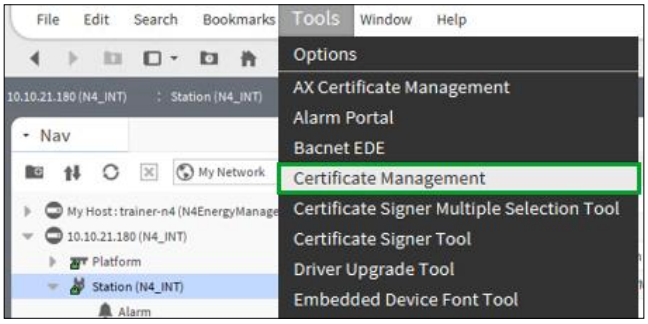


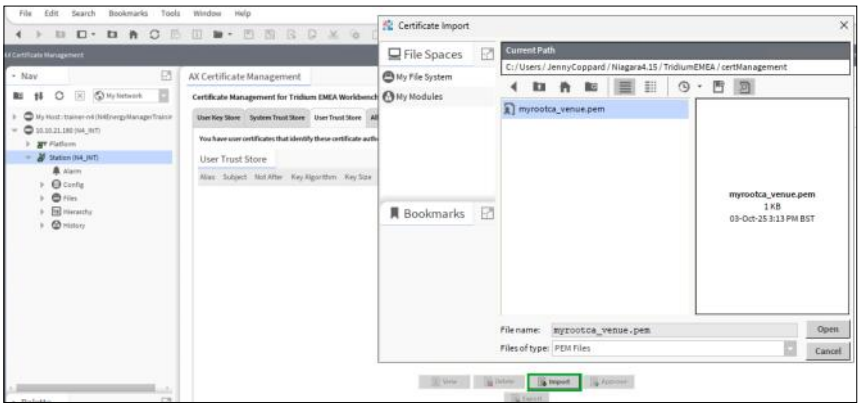


The RootCA Certificate should should then be visible in the UserTrustStore of the station with a green shield to prove it is trusted.

Importing a RootCA Certificate into Workbench

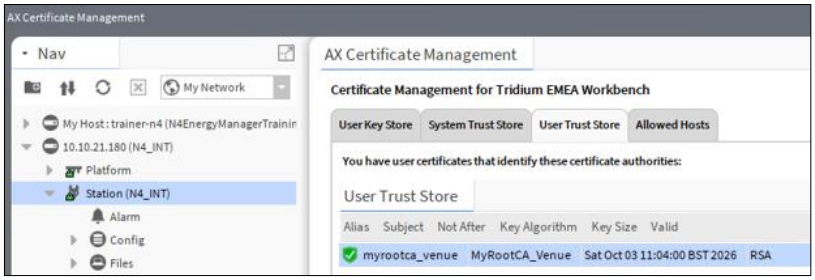
The RootCA Certificate must be also be imported into Workbench itself.
Navigate to **Tools—Certificate Management** from the top menu bar to access the Certificate Management for the Workbench installation on the PC.





Once the Certificat Management for Workbench has been opened, the import process is identical—navigate to the UserTrustStore tab and import the PEM file for the RootCA certificate from the certManagement folder in UserHome.

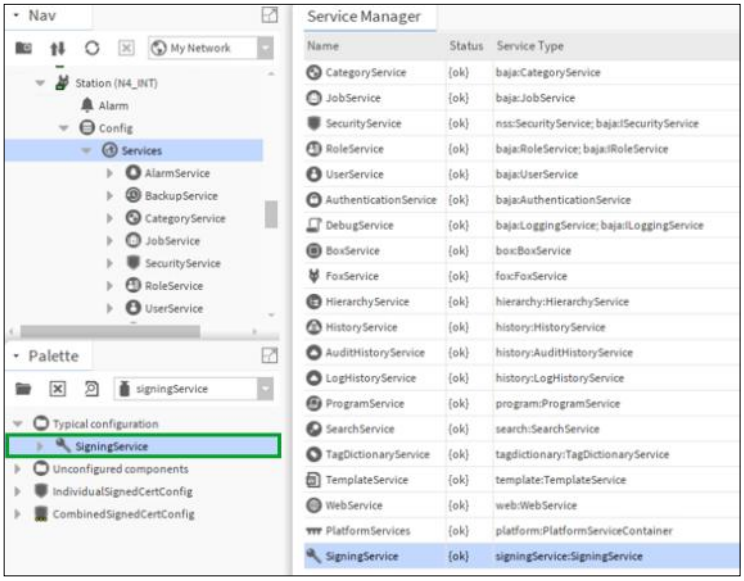
The RootCA Certificate should should then be visible in the UserTrustStore of Workbench with a green shield to prove it is trusted.

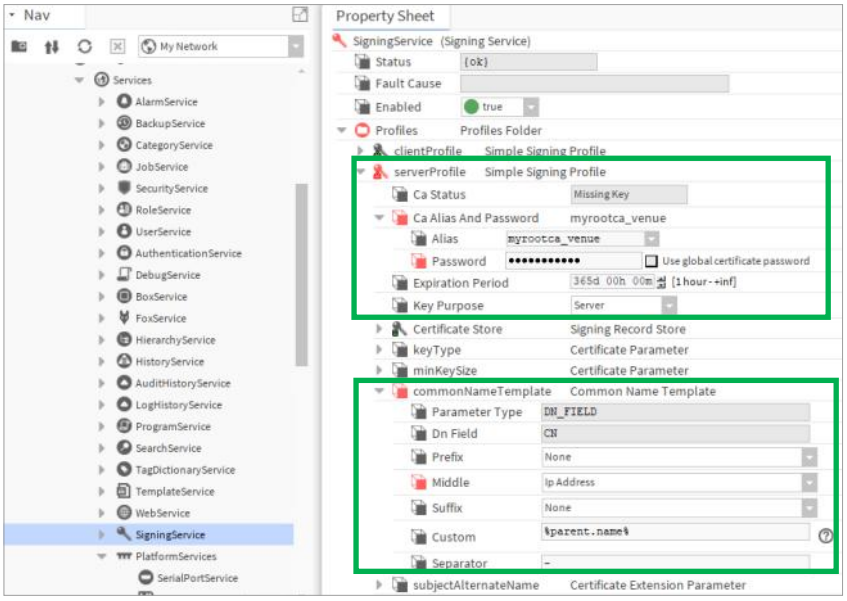


Signing Service

The SigningService helps with the creation and signing of Server Certificates (= Tickets) in Workbench and related stations by ensuring they are linked to and signed by the RootCA certificate.

The SigningService must be manually copied into the list of services in the station from the SigningService palette.





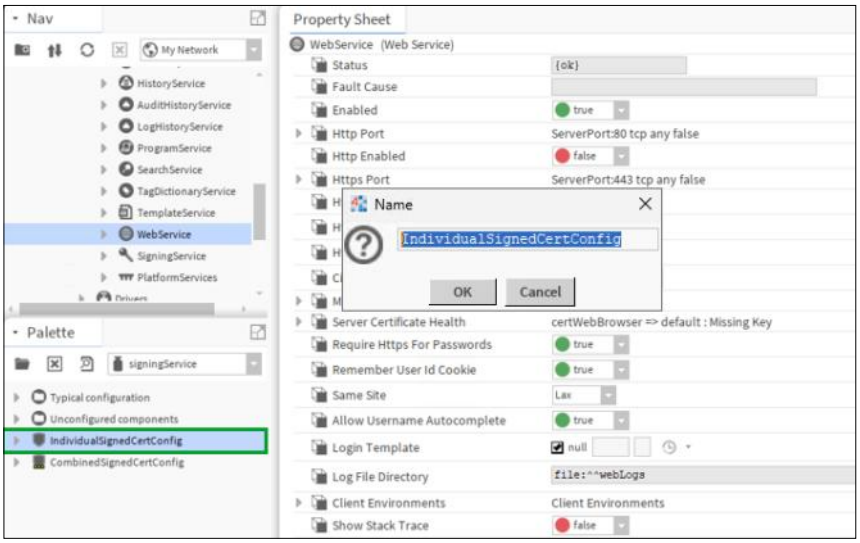
The SigningService must be configured on the PropertySheet to link it to the existing RootCA certificate under the ServerProfiles section using the previously set up password for the PrivateKey. An expiry date must be setup to avoid a security breach.

This ensures that the RootCA will automatically sign any subsequent Server Certificates that are created 'on the fly'.

The CommonNameTemplate must be set to reflect what has been set up in the CA Cert (ie using the IP Address or Host Name for communication)

WebService Configuration

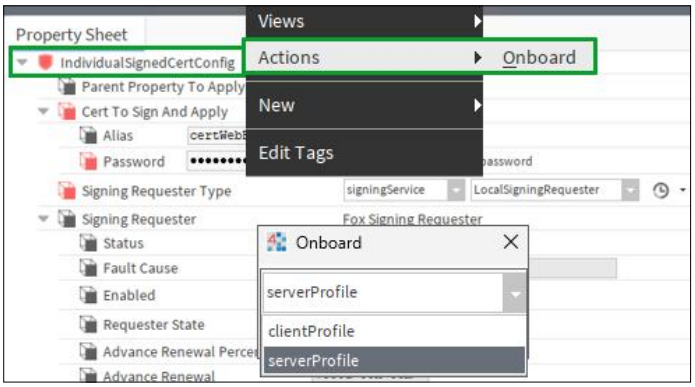
To allow the SigningService to link the Server and CA Certificates in the Web-Service, an **IndividualSignedCertConfig** component must be added to the Web-Service in the station.

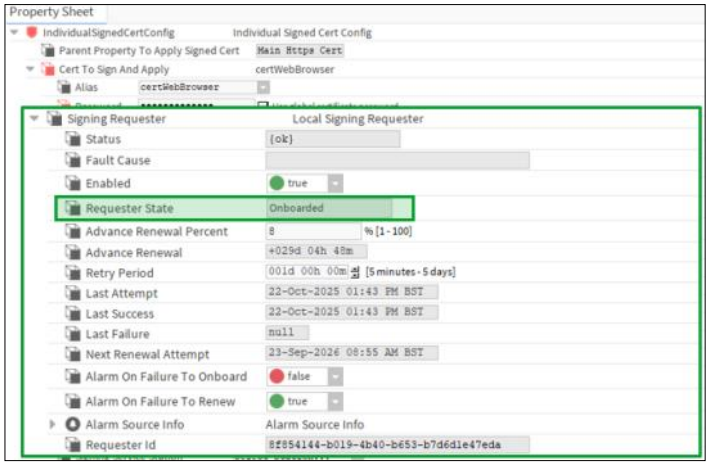


WebService Configuration cont.

The IndividualSignedCertConfig must be set up with the certificate to create, sign and apply, eg certWebBrowser and have the PrivateKey password applied. The SigningRequesterType should be set to SigningService—LocalSigningRequester

Once added and applied, the changes must be saved before the IndividualSignedCertConfig can be onboarded as a **serverProfile**.

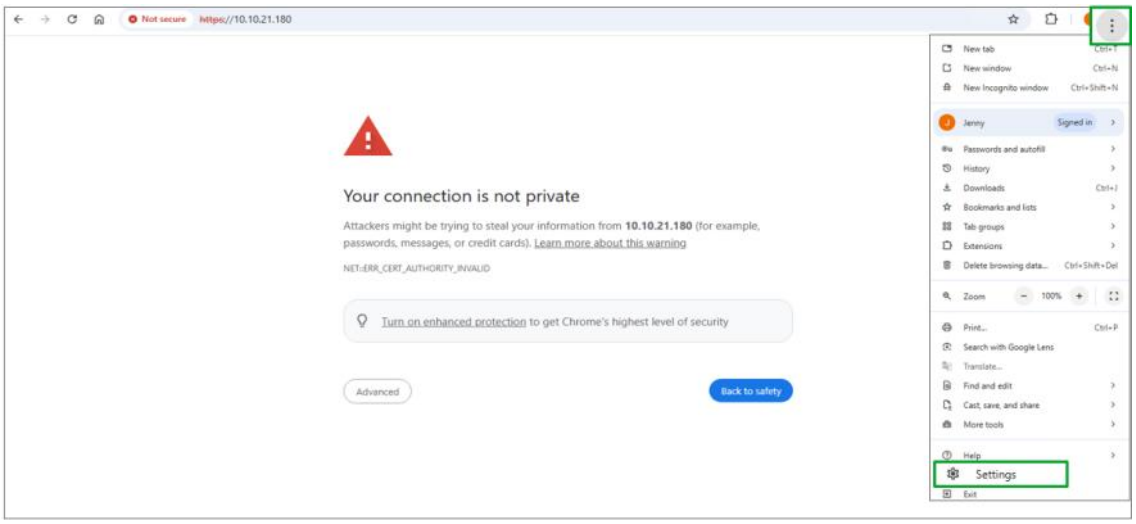




The Requester State will now show as Onboarded and the WebService in the Station is ready to go using the newly set up certificate.

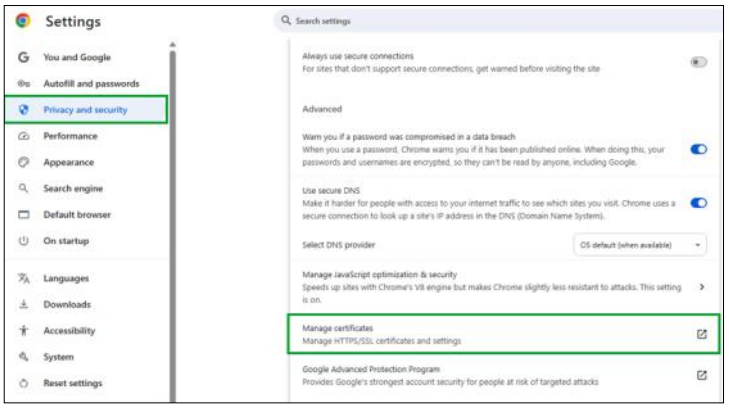
Configuring the Browser

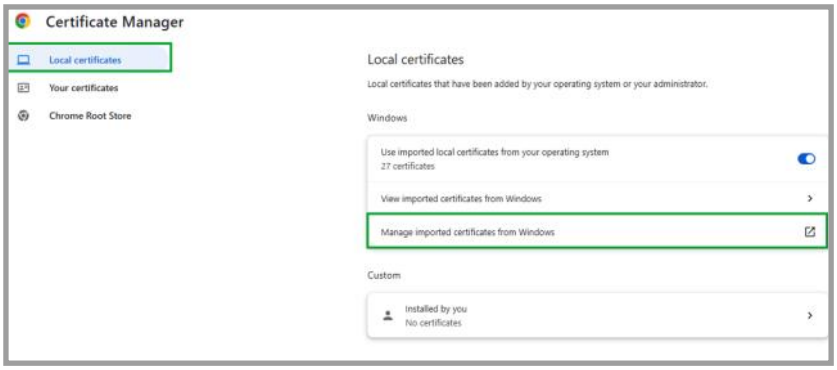
The Browser will also need to be told about the RootCA certificate to ensure that the warning message no longer appears. If using Chrome, select the 3 dots on the top right of the browser window and select Settings to prepare for the certificate upload.



Configuring the Browser

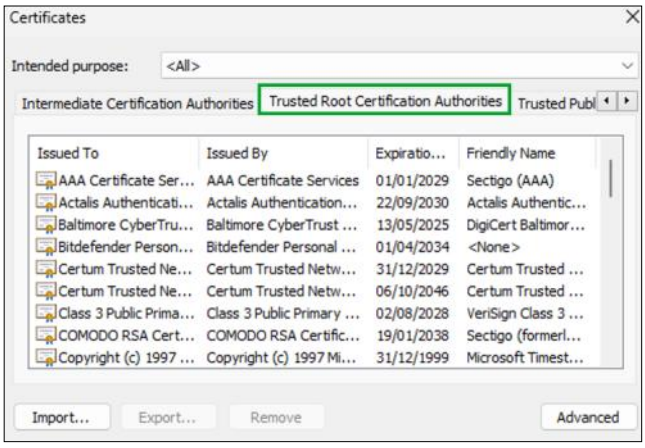
Navigate to **Privacy and Security—Manage Certificates** in the Browser to access the Certificate Manager.

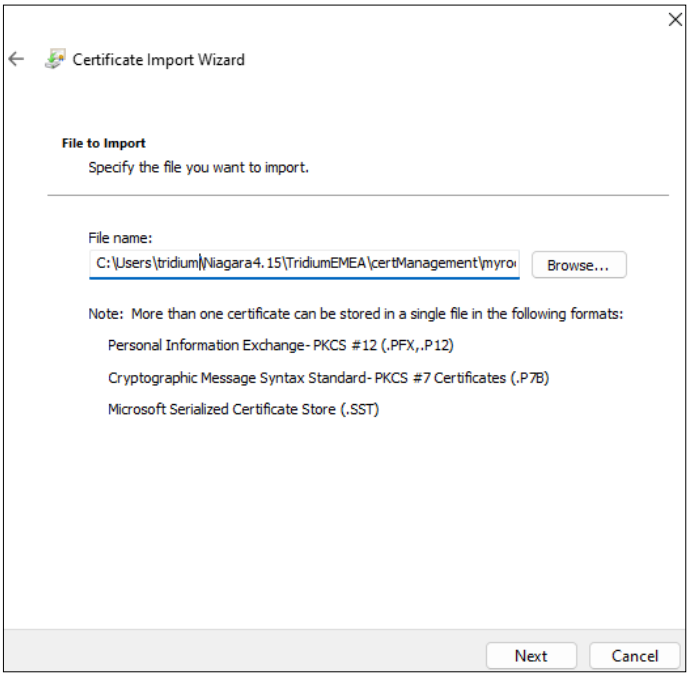




Within the Certificate Manager, select **Local Certificates—Manage Imported Certificates from Windows**.

Navigate to the **Trusted Root Certification Authorities** tab and click Import.





Browse to the certManagement folder in UserHome where the PEM file for the certificate was initially exported to and make sure that **All Files (*.*)** is selected in the file selection popup.
The browser looks for a .cer or .crt by default otherwise and will not find the PEM file.

Configuring the Browser cont.

When logging onto the station via the web browser, the warning will no longer appear because the certificates all match and exchange secure handshakes.