Trusted Certificate and Browser Configuration Guide

Overview

The purpose of this guide is to provide a step-by-step tutorial on how to configure, and utilize, trusted certificates for HTTPS communications for video device and web browser connections.

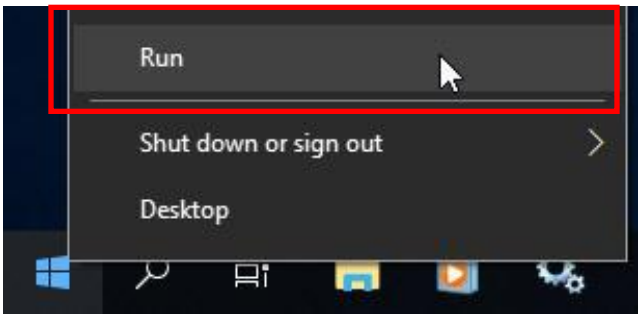
Prior to Starting:

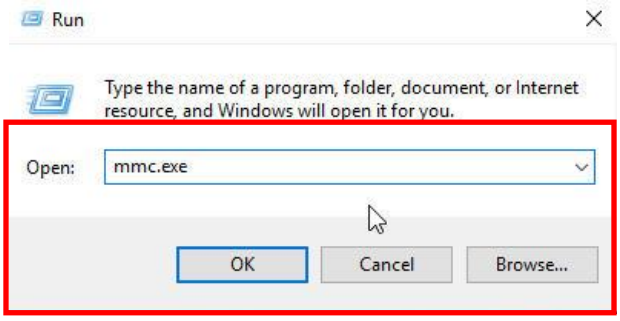
This guide is based on Bosch Configuration Manager 6.01 in conjunction with Bosch video devices configured with firmware 6.51. The example configuration is performed on a "Windows 10" PC with administrative privileges.

Microsoft Management Console (MMC):

For specific configurations, validation, and troubleshooting purposes you should know how to create an MMC snap-in with access to the local machines "certificate store"

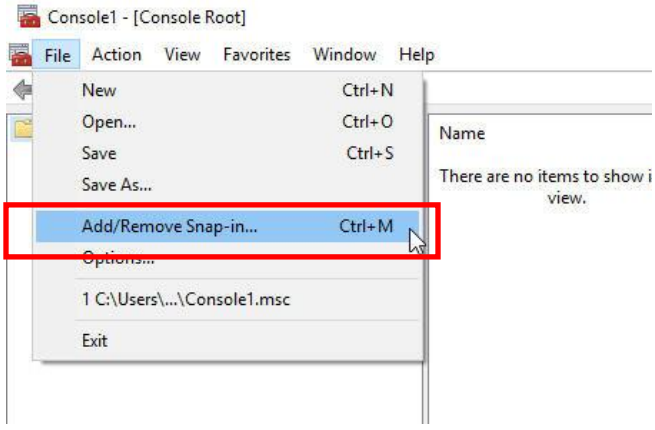
- Right click the "Windows Start" tab select run. From the run menu type "mmc.exe" and select "OK"



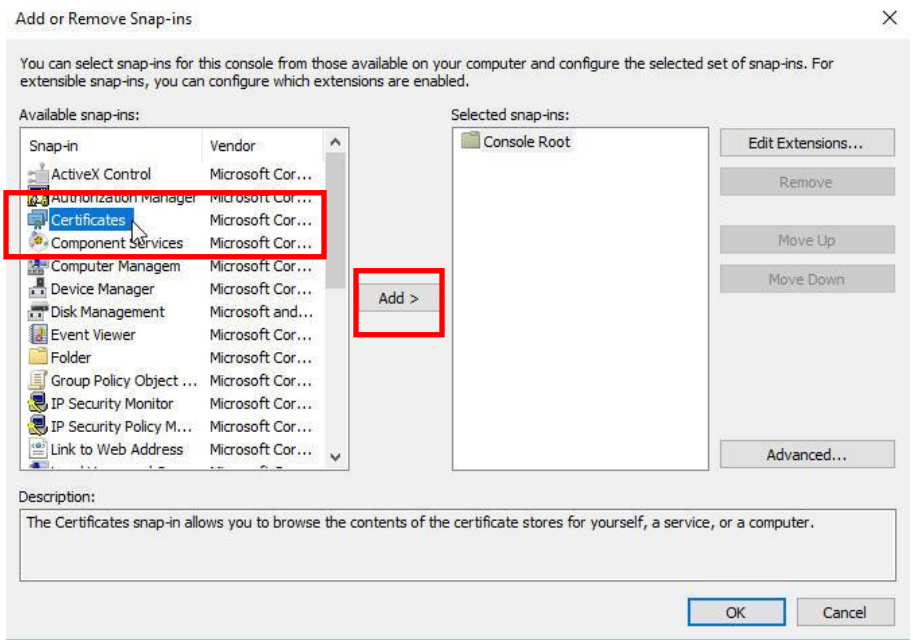


Once the default MMC opens select "File":

- "Add/ Remove Snap-in…."

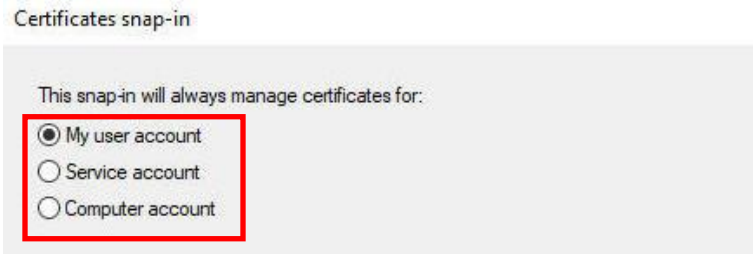


- Once the "Add or Remove Snap-ins" pop-up menu appears, select "Certificates" and then "Add"

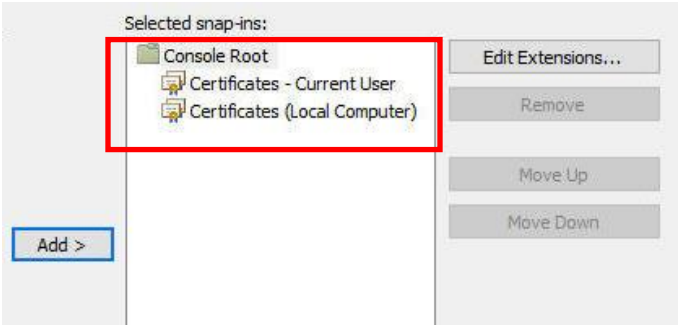


After selecting "Add" you will be required to select the desired account.

- Select "My user account"
- Repeat the process to add "Computer account"



When finished you should have "two" snap-ins



Note: When finished creating the MMC you will be prompted to save. Save it as "cert.msc" to the "Desktop"

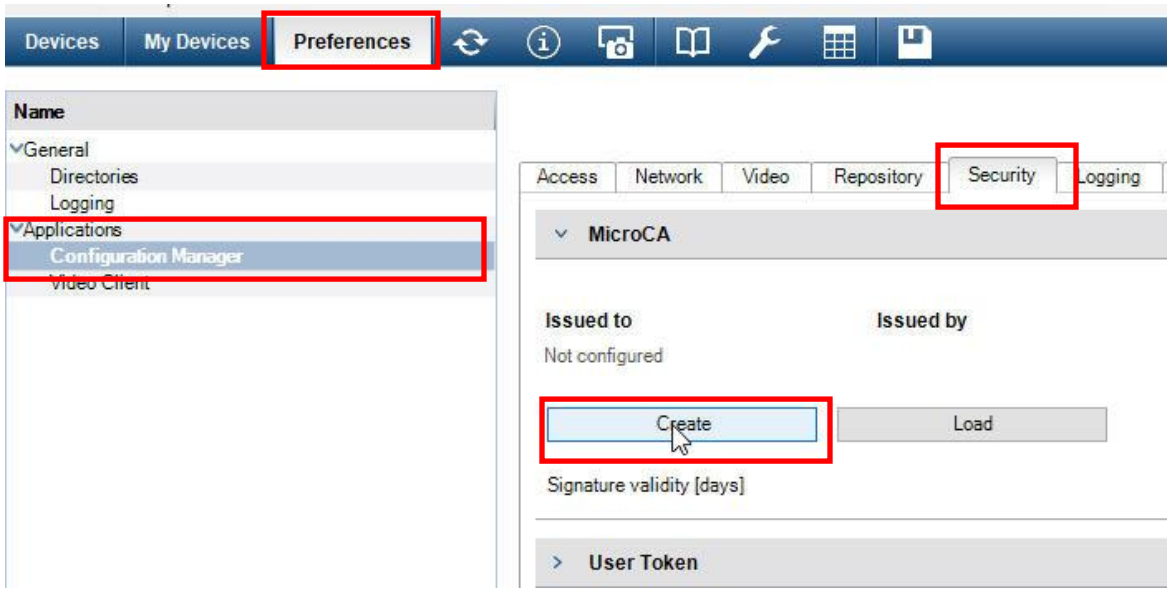
Bosch Configuration Manager Micro Certificate Authority (CA):

Bosch Configuration Manager features and built in Micro **C**ertificate **A**uthority (CA) that allows you to create *Root Certificates*, as well as sign *Certificate-Signing-Requests (CSR)* from system devices.

Creating a "Root Certificate"

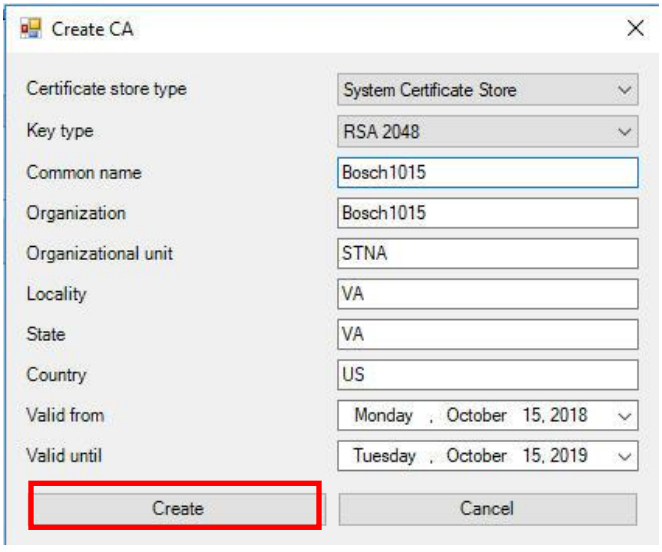
Open Bosch Configuration Manager and navigate to the "Preferences" tab, "Applications", "Configuration Manager" and select the "Security" tab:

- Select the "Create" tab



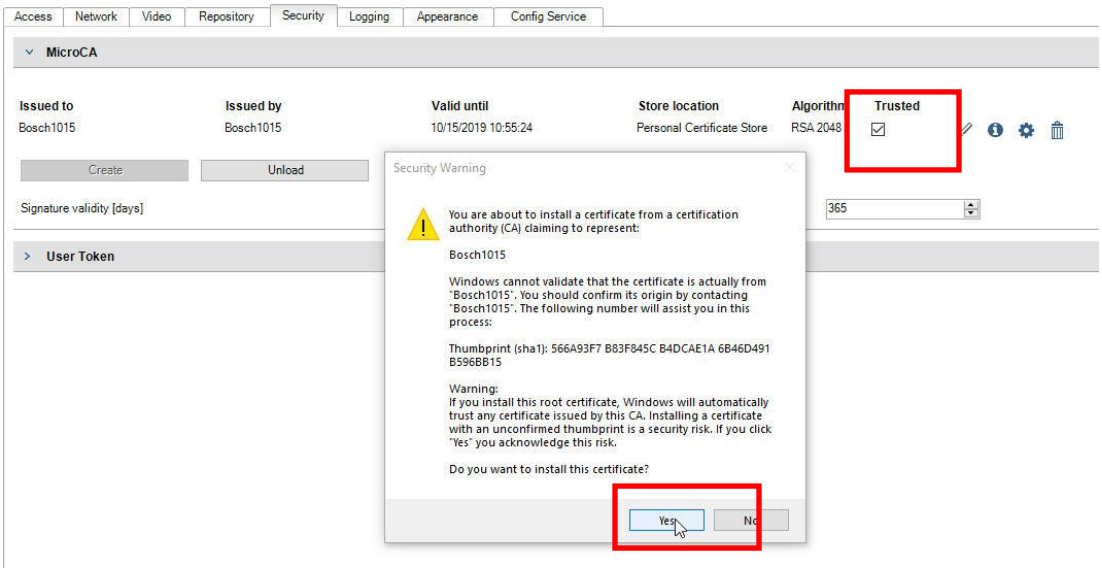
The "Create CA" menu should appear. Select the following:

- Store type: *System Certificate Store*
- RSA 2048
- *Common Name* must be a minimum of 5 characters in length
- All site information should be unique
- Select "Create"



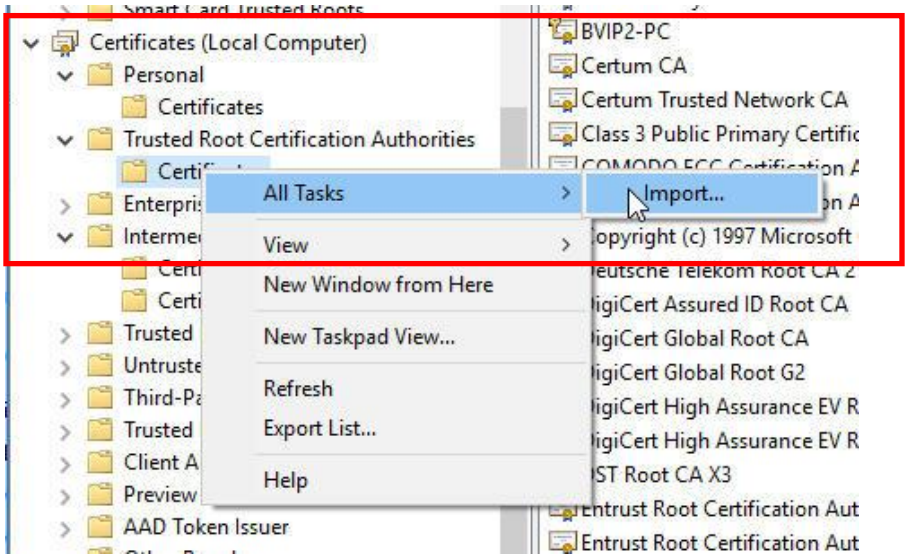
After the certificate is created select the "Trusted" check box in the certificate menu, then select the "Yes" option in the "Security Warning" pop up menu:

- This will add the certificate to the local machines "Certificate Store"



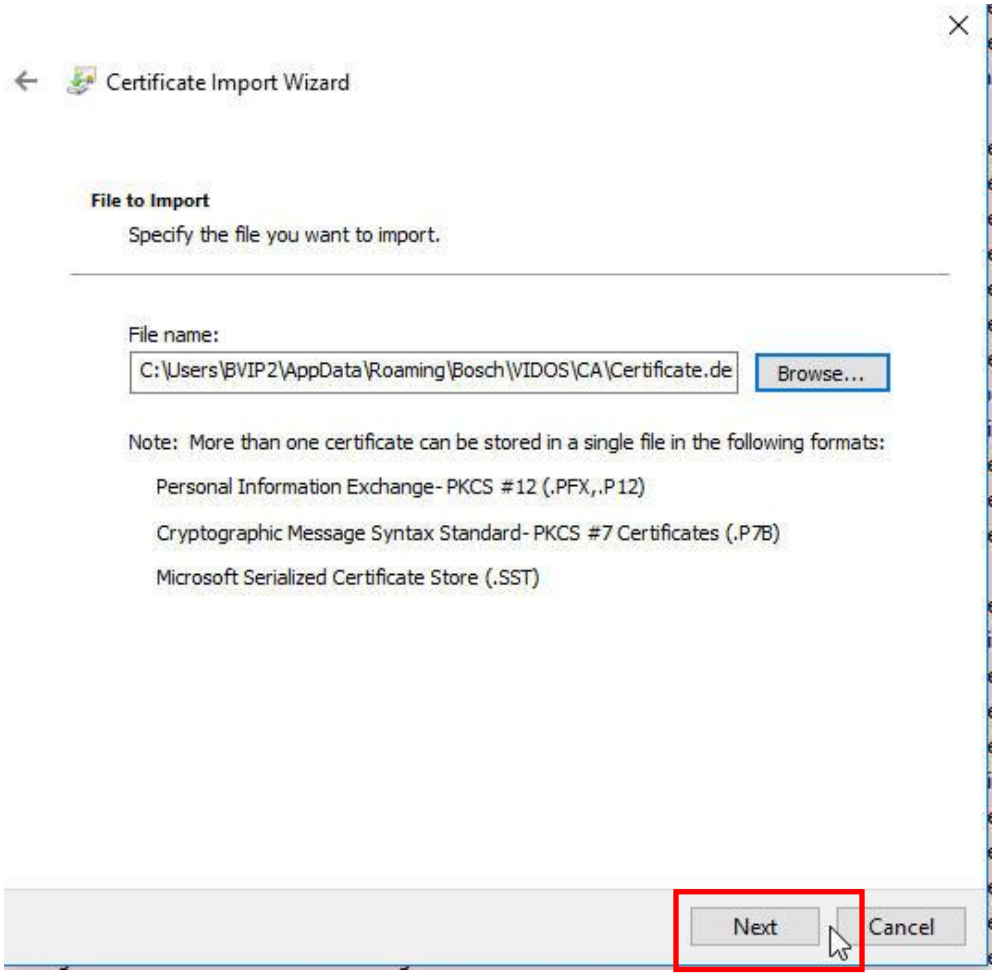
Typically this will add the certificate to the "Current User" certificate store. If the local machine is going to be used by multiple users you may want to add the root certificate to the "Local Computer" Certificate Store.

- Open the MMC shortcut you saved to your desktop
- Navigate to "Certificates (Local Computer)" , "Trusted Certificate Authorities" , and "Certificates"
- Right click "Certificates" and select "All Tasks" and "Import..."



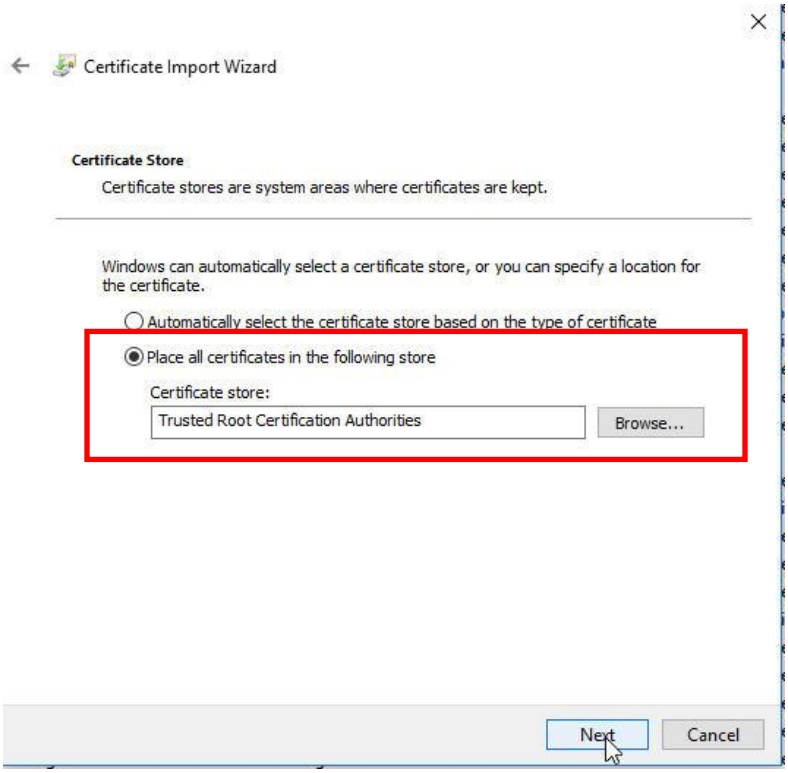
This will open the "Certificate Import Wizard". Your first step is to navigate to the location of the root certificate you just created. By default the MicroCA certificate store is located at the following location:

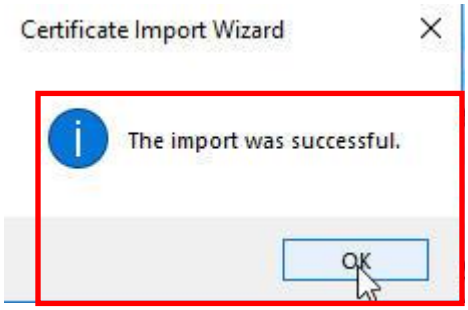
- C:\Users\"username"\AppData\Roaming\Bosch\VIDOS\CA
- Once located, select "Next"



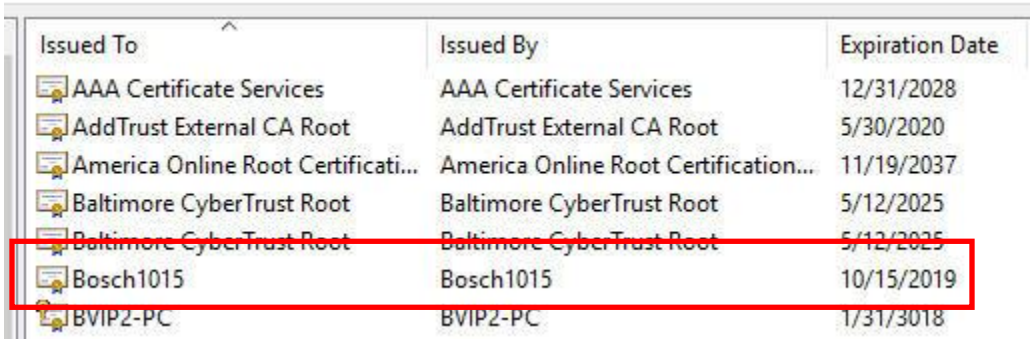
After selecting "Next", ensure that the certificate will be placed in the "Trusted Root Certificate Authorities" store.

- Select next
- Select finished on the last page
- You should receive a "The import was successful" message, select "OK"





You should now see the newly imported certificate in the certificate list.

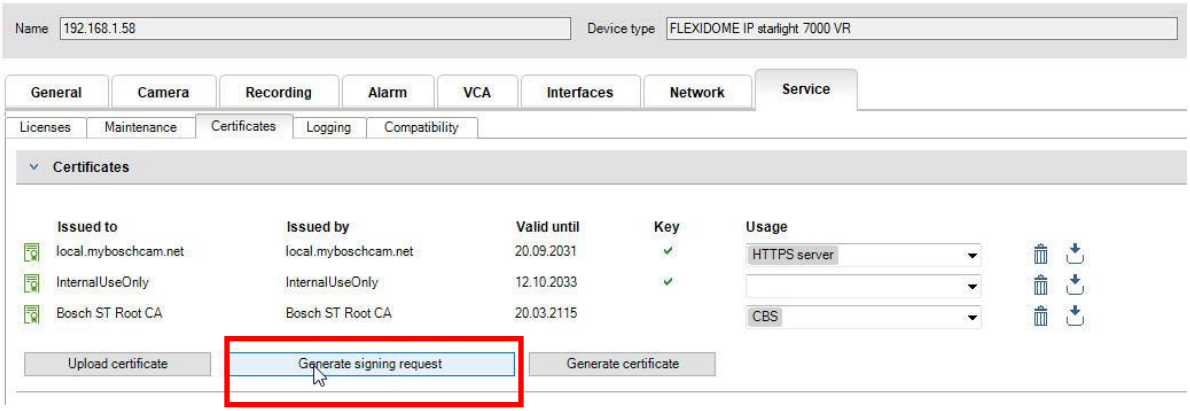


Issued To	Issued By	Expiration Date
AAA Certificate Services	AAA Certificate Services	12/31/2028
AddTrust External CA Root	AddTrust External CA Root	5/30/2020
America Online Root Certificati...	America Online Root Certification...	11/19/2037
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025
Bosch1015	Bosch1015	10/15/2019
BVIP2-PC	BVIP2-PC	1/31/3018

Signing Camera Certificates

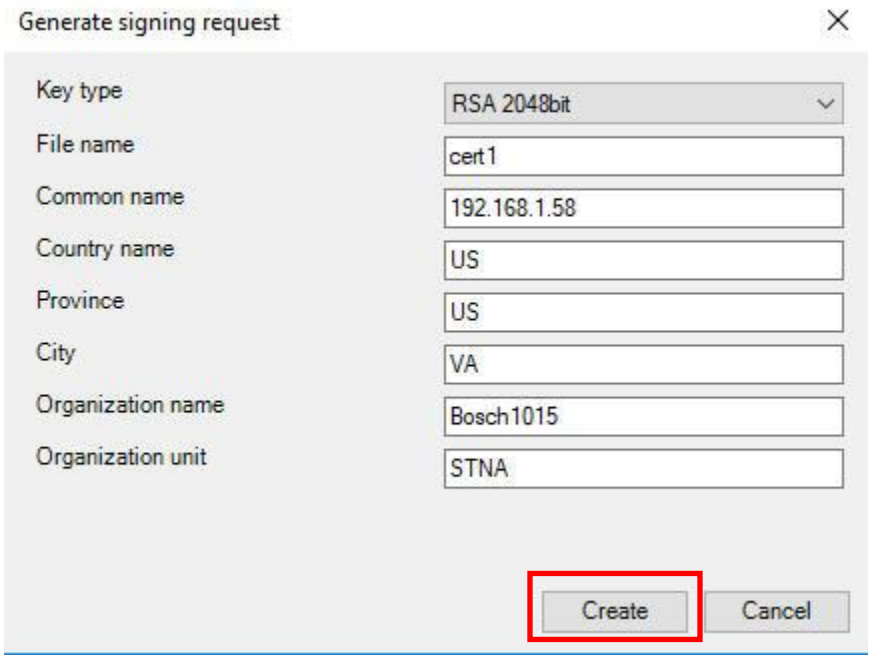
All Bosch video devices come equipped with a "root certificate". From Configuration Manager, the devices tab, select the desired camera. Once the device has been "highlighted" in the device tree:

- Select the "Services" tab
- Select the "Certificates" sub tab
- Select "Generate signing request"



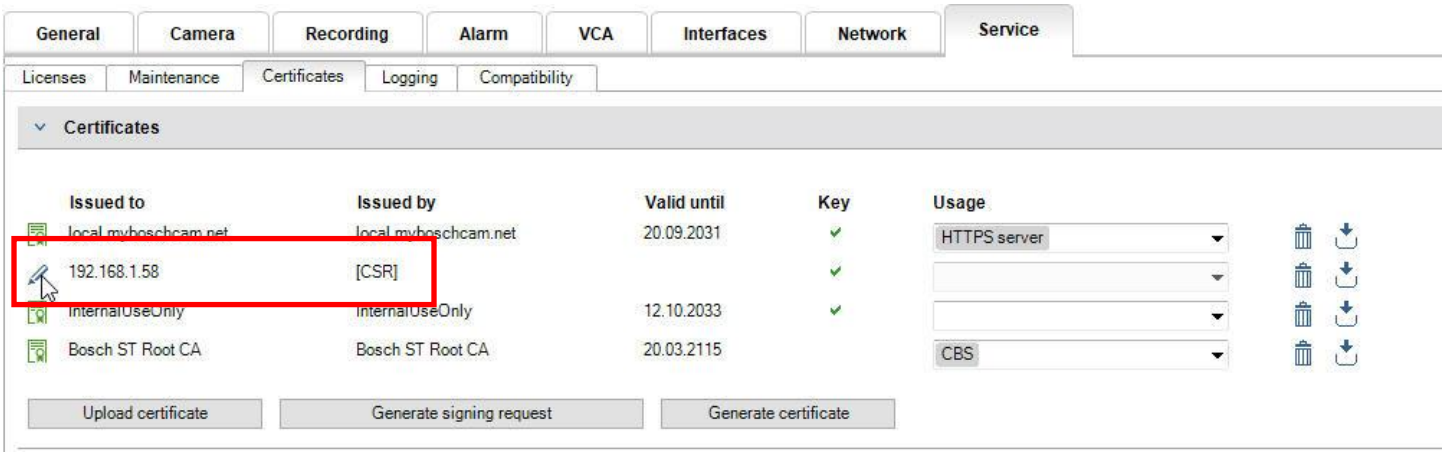
The "Generate signing request pop-up menu should appear. The base information from the Micro-CA Root Certificate should auto filled into the "Signing Request".

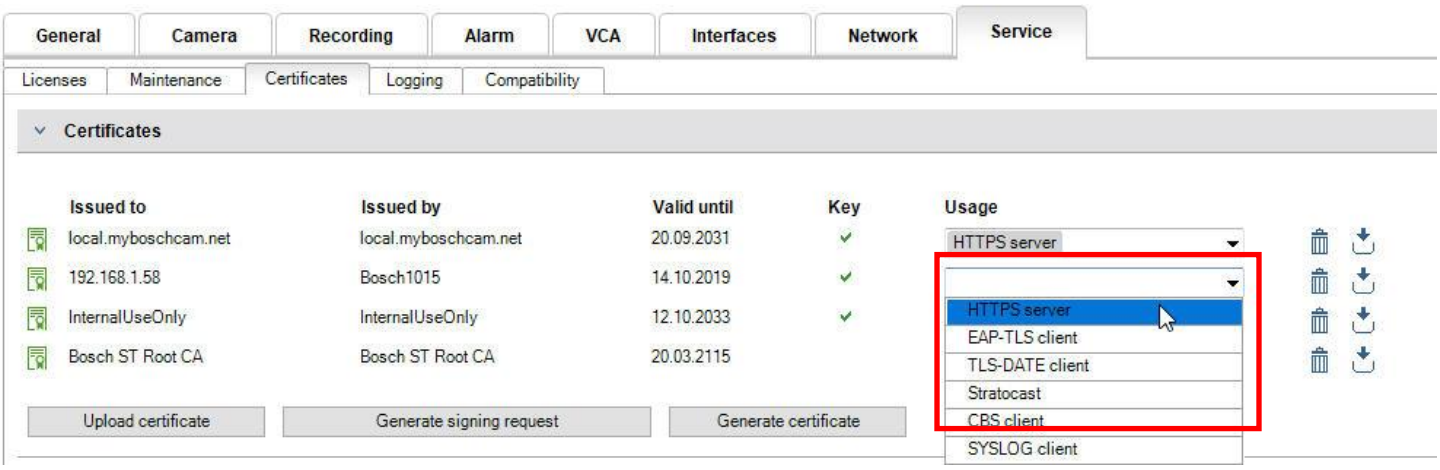
- Ensure the "Key Type" matches what was utilized for the root certificate: RSA 2048bit
- Select "Create"



After the signing request has been generated, you will see the CSR and a "pencil" icon. Select the "pencil icon

- The Micro-CA will automatically sign the CSR
- The CSR will automatically convert to a signed certificate in the menu
- From the "Usage" dropdown menu select "HTTPS server"
- Select "Save"





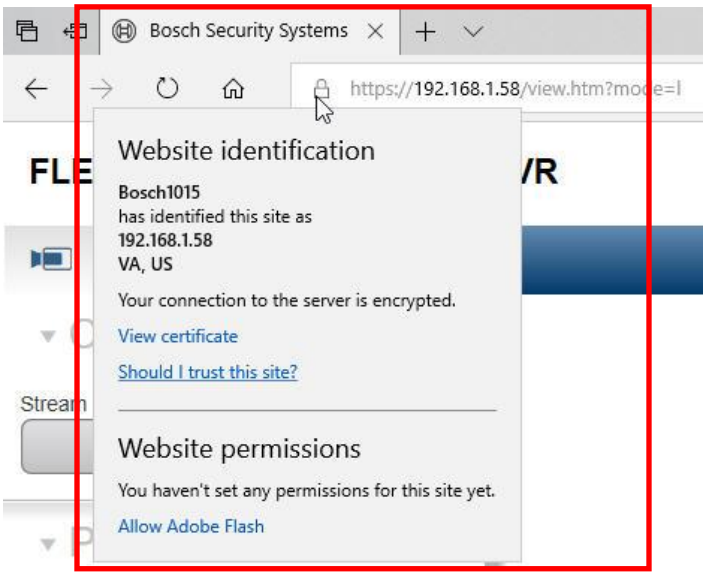
Note: Multiple cameras can be selected simultaneously, and CSRs can be generated in parallel, which will then all appear in the "Certificates" menu as shown above.

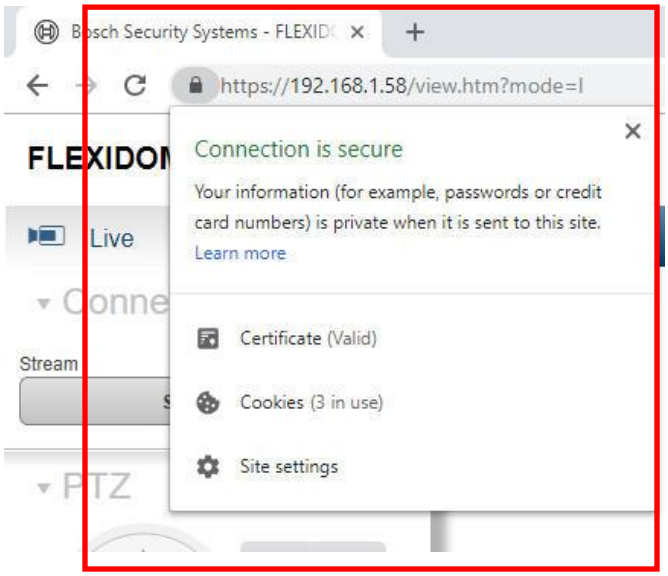
- *Select all desired cameras in the "My Devices" menu, and perform the same procedure as outlined above*

Microsoft Edge and Chrome

Navigating to any of the configured video devices utilizing either *Microsoft Edge* or *Chrome* web browsers will only require "account login"

- HTTPS should show secure and no certificate errors

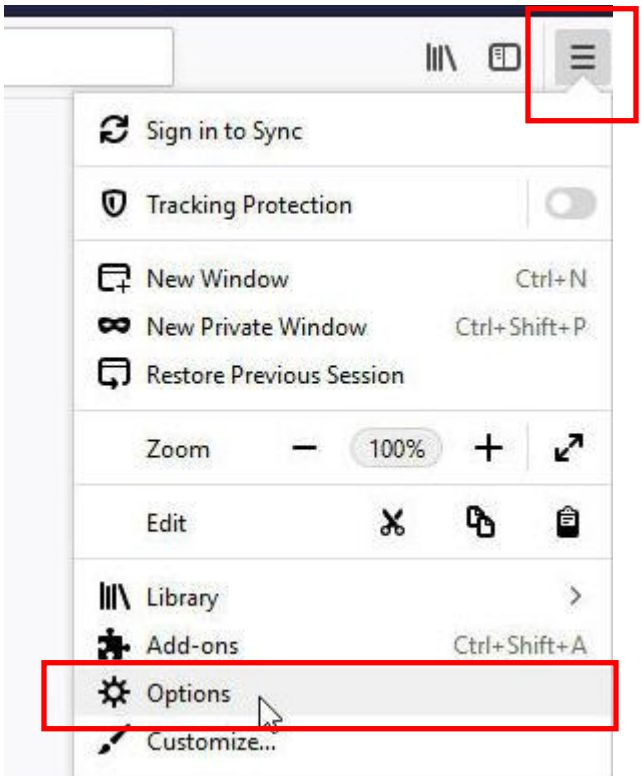


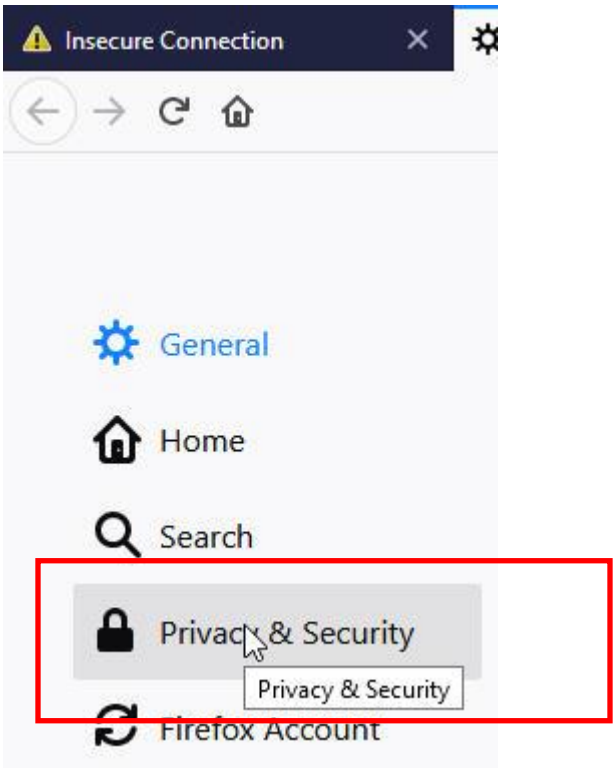


Firefox

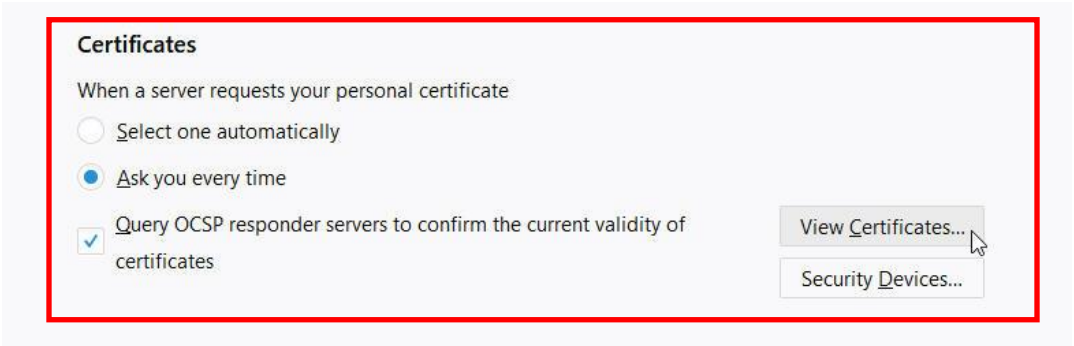
Firefox does not read the "Windows Certificate Store". Root certificates must be manually added to the Browser

- Open Firefox and select the menu icon in the top left hand corner of the browser, then select the "Options" submenu
- From the "Options menu" select "Privacy & Security"



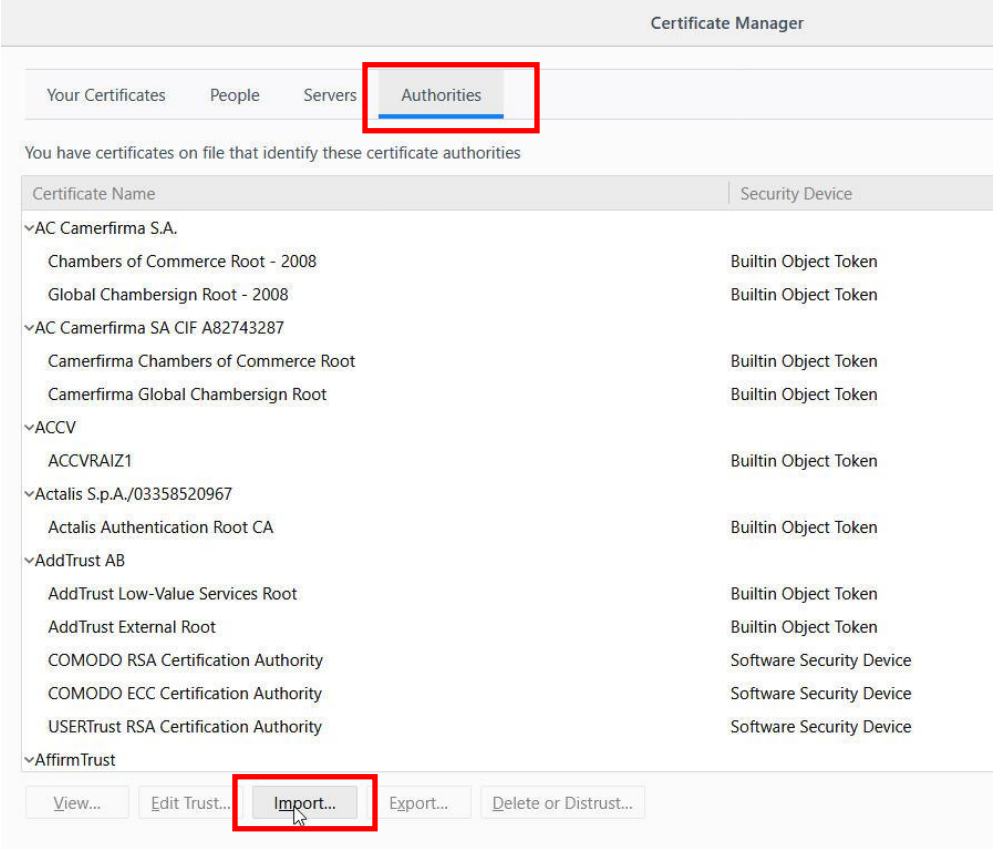


From the bottom most portion of the "Privacy & Security page select "View Certificates"



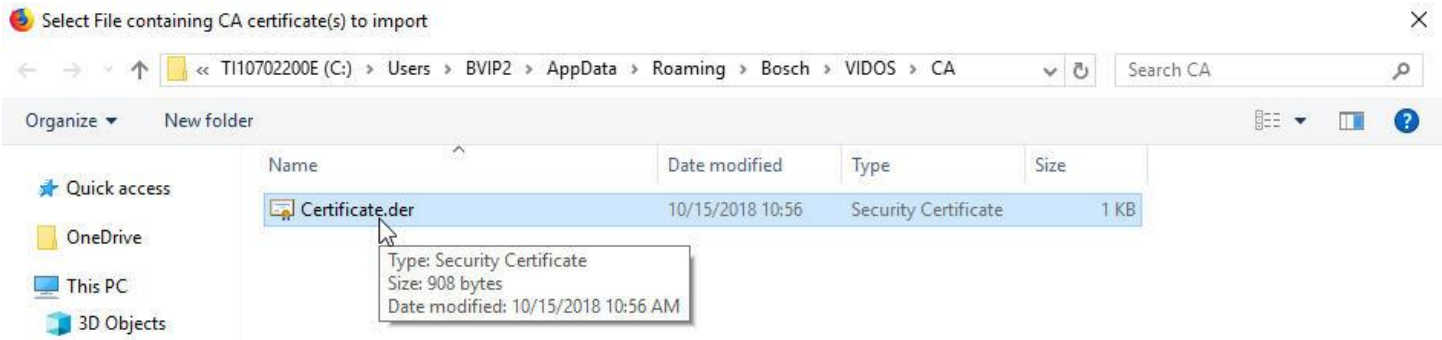
The "Certificate Manager" menu should open:

- Select the "Authorities" Tab
- Select "Import"



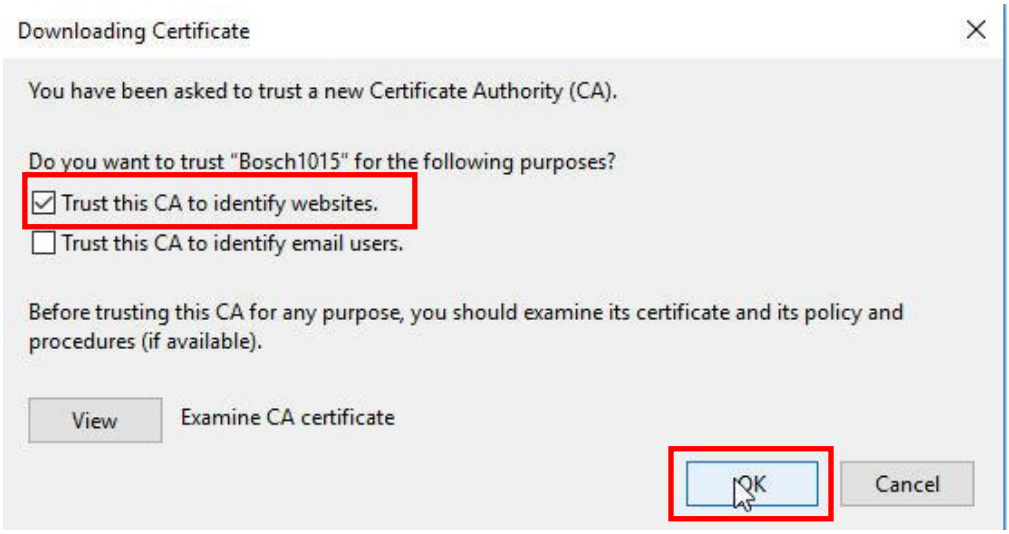
You will need to navigate to the location of the root certificate you created earlier:

- C:\Users\"username"\AppData\Roaming\Bosch\VIDOS\CA



After selecting the root certificate you will receive a "Downloading Certificate" pop-up menu

- Select "Trust this CA to identify websites."
- Select "OK"



Navigating to any of the configured video devices utilizing either *Firefox* will only require "account login"

- HTTPS should show secure and no certificate errors