SmartCNX HySecurity SSL Certificate
Setup Instructions

OPERATOR: All operators using SmartCNX H6.04 Firmware **DATE:** 08/12/2021

SUBJECT: Updating the SSL Certificate per new SmartCNX H6.04 Firmware

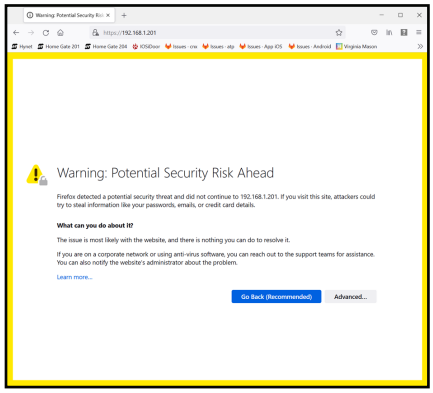
HySecurity SSL Certificate Setup Instructions:

The latest CNX software H6.04 changes the CNX web server to use SSL (https://) with default port 443. Previous versions H6.03 and earlier did not use SSL and defaulted to port 80. These port numbers are defaults but can be changed by the user if needed in the CNX menus.

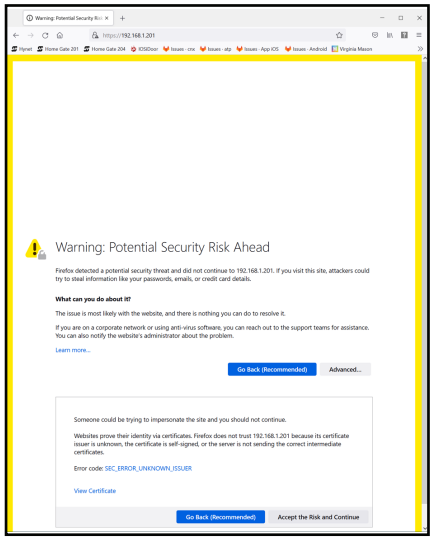
The CNX web server needs an assigned IP address (either manually configured from the CNX menus or using DHCP).

Since the server now uses SSL, you should reach the server by using the assigned IP adress (whatever it is). **EXAMPLE:** if assigned address is **192.168.1.201**, then put **https://192.168.1.201** in your browser's address bar.

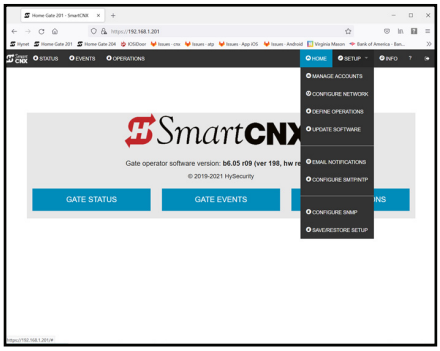
When the server is reached, the browser will warn you that the site may be insecure. You can fix this later and use the CNX SSL certificate, but initially, you must ignore the browser warnings and proceed to the site. Each browser offers a means of bypassing these warnings and going forward to the CNX web server. Below left is an image (**1**) of the Firefox browser's initial warning. Follow the instructions accompanying each screen shot to setup and use the SSL certificate:



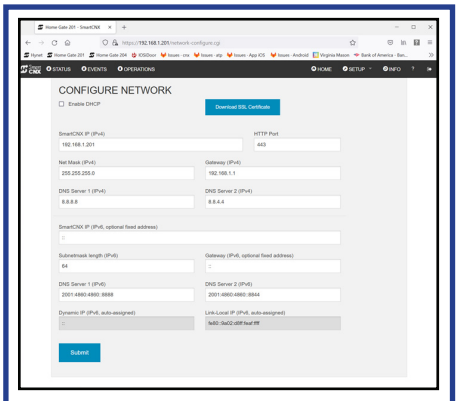
1 Push the "advanced" button (lower right); browser then shows (**2**):



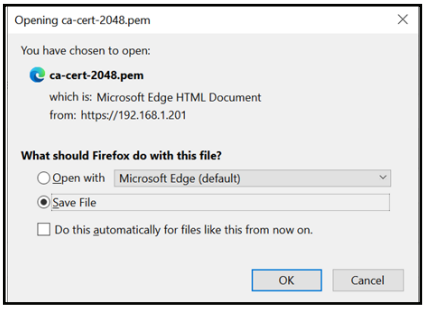
2 Push the "Accept the Risk and Continue" button (lower right) to go to the CNX web server (**3**).



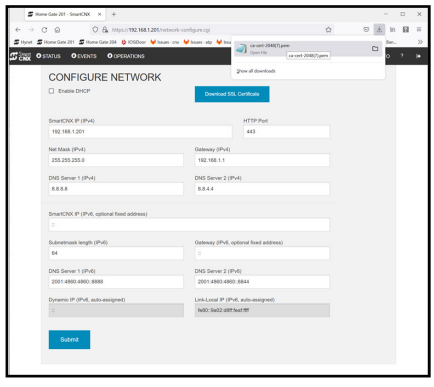
3 Use "SETUP" drop down menu, then navigate to "CONFIGURE NETWORK" page (**4**).



4 Click the "Download SSL Certificate" button to download the HySecurity SSL certificate. This should be placed in the browser's Trusted Root Certification Authorities store (or similarly named store). When you push this button, you should see (**5**):

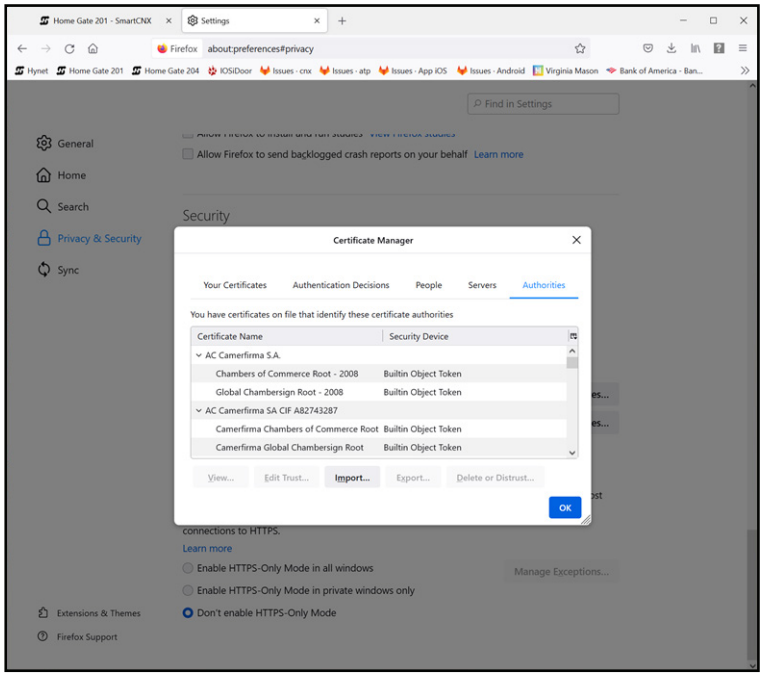


5 Click OK to save the certificate file on your PC. Firefox saves locally and the file can be accessed with the download icon on the address/tool bar. Drag the file to your desktop.



6 Go to the browser's Settings page and select "Privacy & Security". Near the bottom of this page is the "Security" area; push the "View Certificates…" button. The Certificate Manager pops up (**7**):

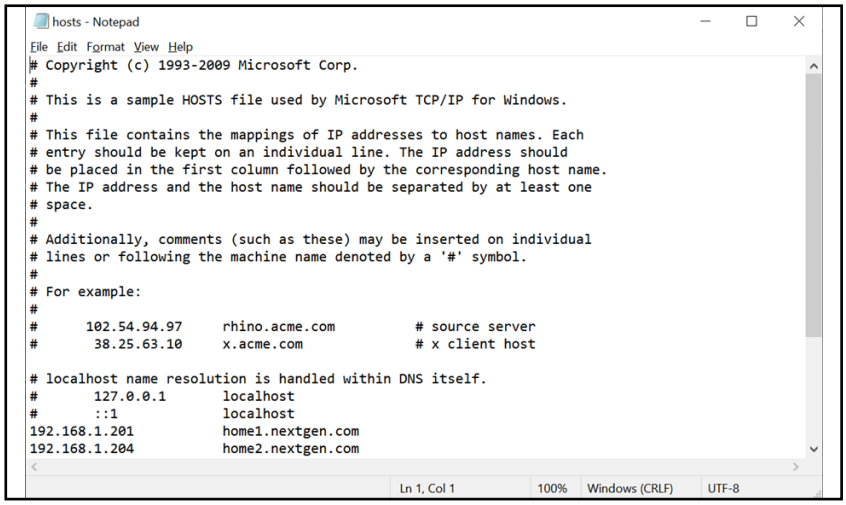
HySecurity SSL Certificate Setup Instructions (Cont.)



7 Under the “authorities” list, push the “import…” button to import the hysecurity certificate on your desktop. Navigate to the file on the desktop and “open” it. Select ok in the next pop-up, and then ok again in the certificate manager pop-up. That completes importing of the hysecurity ssl certificate. You should close the browser for now, and procee to next step (**8**).

8 The next step is to define a URL for the web server address.The HySecurity SSL certificate is known as a “wildcard” certificate. It works with URLs of the format “*.nextgen.com”. You can pick a name for the wildcard but the URL must end in “nextgen.com”.

EXAMPLE: the name “home1.nextgen.com” would be a valid URL with the HySecurity certificate. After deciding a name, you can place this name and IP address into your PC’s “hosts” file. For Windows, this file is found in the following folder: \Windows\System32\drivers\etc. The contents can be edited with a text editor such as Notepad:



NOTICE

One may buy a URL name through a DNS service rather than using the “hosts” file on each PC.

After **Step 8** is complete, you can use the URL in the browser.

EXAMPLE: https://home1.nextgen.com. This will use the HySecurity certificate and a secure SSL connection.