

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



HySecurity SSL Certificate Setup Instructions (Cont.)

Home Gate 201 - SmartCNX ×	83 Settings × +			- 0 ×		
$\leftarrow \rightarrow$ C \textcircled{o}	Firefox about:preferences#privacy			☺ ½ ॥\ 🛛 ≡		
🖅 Hynet 🗊 Home Gate 201 🗊 Home G	iate 204 🛛 🐯 IOSiDoor 🛛 🖊 Issues - cnx 😽 Issues - atj	😽 😽 Issues - App iOS 🛛 🖊 Issues - And	droid 🚺 Virginia Mason 🗇 B	ank of America - Ban 📎		
छि General	Anon Frence to instantian and that storage	P Find in	n Settings	Í		
Home	Anow Pirelox to send basklogged crash	reports on your benair Learnin	ore			
Q Search	Security					
Privacy & Security	Certificate Manager X					
Sync	Your Certificates Authentication Dec	sions People Servers	Authorities			
You have certificates on file that identify these certificate authorities						
	Certificate Name	Security Device	1			
	✓ AC Camerfirma S.A.		^			
	Chambers of Commerce Root - 2008	Builtin Object Token				
	Global Chambersign Root - 2008 Builtin Object Token					
	✓ AC Camerfirma SA CIF A82743287					
	Camerfirma Chambers of Commerce Re	es				
	Camerfirma Global Chambersign Root 🛛 Builtin Object Token 🗸 🗸					
	View Edit Trust Import.	Export Delete or Dist	trust OX			
	connections to HTTPS.					
	Learn more					
	Enable HTTPS-Only Mode in all windows Manage					
	C Enable HTTPS-Only Mode in private windows only					
Extensions & Themes	O Don't enable HTTPS-Only Mode					
⑦ Firefox Support						

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**).



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:

	bosts - Notenad					_		×	
	inosis - Notepad							^	
E	le <u>E</u> dit F <u>o</u> rmat <u>V</u> iew <u>H</u> elp								
# #	# Copyright (c) 1993-2009 Microsoft Corp. #								
‡ ‡	<pre># This is a sample HOSTS file used by Microsoft TCP/IP for Windows.</pre> #								
<pre># This file contains the mappings of IP addresses to host names. Each # entry should be kept on an individual line. The IP address should # be placed in the first column followed by the corresponding host name. # The IP address and the host name should be separated by at least one # space. # # Additionally, comments (such as these) may be inserted on individual</pre>									
# #	<pre># lines or following the machine name denoted by a '#' symbol. #</pre>								
# #	For example:								
ŧ	102.54.94.97 rhin	o.acme.com	# source server	r					
ŧ	38.25.63.10 x.ac	me.com	# x client host						
<pre># localhost name resolution is handled within DNS itself. # 127.0.0.1 localhost # ::1 localhost 192.168.1.201 home1.nextgen.com 192.168.1.204 home2.nextgen.com</pre>									
<								>	
			Ln 1, Col 1	100%	Windows (CRLF)	UTF-	8		

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.