Creating Your Own Signed Web Certificates Using OpenSSL

Topic Covered

Featured Brands

lumbergautomation A BELDEN BRAND
HIRSCHMANN A BELDEN BRAND
TOFINO SECURITY A BELDEN BRAND
GarrettCom A BELDEN BRAND

Phone: **1.800.BELDEN1**

www.belden.com

General Information

1 Signed Web Certificates Description:

1.1.1 What are website certificates?

If an organization wants to have a secure website that uses encryption, it needs to obtain a site, or host, certificate. There are two elements that indicate that a site uses encryption:

- a closed padlock, which, depending on your browser, may be located in the status bar at the bottom of your browser window or at the top of the browser window between the address and search fields
- a URL that begins with "https:" rather than "http:"

By making sure a website encrypts your information and has a valid certificate, you can help protect yourself against attackers who create malicious sites to gather your information. You want to make sure you know where your information is going before you submit anything.

If a website has a valid certificate, it means that a certificate authority has taken steps to verify that the web address actually belongs to that organization. When you type a URL or follow a link to a secure website, your browser will check the certificate for the following characteristics:

1. the website address matches the address on the certificate
2. the certificate is signed by a certificate authority that the browser recognizes as a "trusted" authority

If the browser senses a problem, it may present you with a dialog box that claims that there is an error with the site certificate. This may happen if the name the certificate is registered to does not match the site name, if you have chosen not to trust the company who issued the certificate, or if the certificate has expired. You will usually be presented with the option to examine the certificate, after which you can accept the certificate forever, accept it only for that particular visit, or choose not to accept it. The confusion is sometimes easy to resolve (perhaps the certificate was issued to a particular department within the organization rather than the name on file). If you are unsure whether the certificate is valid or question the security of the site, do not submit personal information. Even if the information is encrypted, make sure to read the organization's privacy policy first so that you know what is being done with that information .

1.1.2 Can you trust a certificate?

The level of trust you put in a certificate is connected to how much you trust the organization and the certificate authority. If the web address matches the address on the certificate, the certificate is signed by a trusted certificate authority, and the date is valid, you can be more confident that the site you want to visit is actually the site that you are visiting. However, unless you personally verify that certificate's unique fingerprint by calling the organization directly, there is no way to be absolutely sure.

When you trust a certificate, you are essentially trusting the certificate authority to verify the organization's identity for you. However, it is important to realize that certificate authorities vary in how

strict they are about validating all of the information in the requests and about making sure that their data is secure. By default, your browser contains a list of more than 100 trusted certificate authorities. That means that, by extension, you are trusting all of those certificate authorities to properly verify and validate the information. Before submitting any personal information, you may want to look at the certificate.

1.1.3 How do you check a certificate?

There are two ways to verify a web site's certificate in Internet Explorer or Firefox. One option is to click on the padlock icon. However, your browser settings may not be configured to display the status bar that contains the icon. Also, attackers may be able to create malicious websites that fake a padlock icon and display a false dialog window if you click that icon. A more secure way to find information about the certificate is to look for the certificate feature in the menu options. This information may be under the file properties or the security option within the page information. You will get a dialog box with information about the certificate, including:

- Who issued the certificate - You should make sure that the issuer is a legitimate, trusted certificate authority (you may see names like VeriSign, Thawte, or Entrust). Some organizations also have their own certificate authorities that they use to issue certificates to internal sites such as intranets.
- Who the certificate is issued to - The certificate should be issued to the organization who owns the web site. Do not trust the certificate if the name on the certificate does not match the name of the organization or person you expect.
- Expiration date - Most certificates are issued for one or two years. One exception is the certificate for the certificate authority itself, which, because of the amount of involvement necessary to distribute the information to all of the organizations who hold its certificates, may be ten years. Be wary of organizations with certificates that are valid for longer than two years or with certificates that have expired.

2 Initial Preparation

Gather the information, tools and equipment needed to complete this task. The example values given in this document are not meant to be thought of as recommended as each installation is unique and has its own requirements.

2.1 Tools and equipment:

2.1.1 Cables

2.1.1.1 DX, 10XTS Console

Console cable DB9 to DB9 for systems with serial port (**Model CONSOLE-CBLQD**) or

Console cable DB9 to USB for systems with only USB ports **(Model CONSOLE-CBLQU)**

RJ45 Ethernet cable

Pin	Name	Dir.	Description
1	DCD	In	Data Carrier Detect from DCE.
2	RXD	In	Receive Data from DCE.
3	TXD	Out	Transmit Data to DCE.
4	DTR	Out	Data Terminal Ready to DCE.
5	GND	Power Reference	Signal Ground.
6	DSR	In	Data Set Ready from DCE.
7	RTS	Out	Request To Send.
8	CTS	In	Clear to Send.
9	RI	In	Ring Indicator from DCE.

DB9 Console port pin assignments DX, 10XTS

2.1.2 Software

Terminal Server Software for a Windows PC supporting serial and SSH connections to access the MNS, MNS-DX, INOS CLI;

Recommended, not supplied by Belden.

Examples: TeraTerm (http://en.osdn.jp/projects/ttssh2/releases/)

Putty (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html)

Internet Browsers used to access the MNS, MNS-DX, INOS Graphical User Interface, hereafter called the GUI.

Examples: Firefox (https://www.mozilla.org/)

Chrome (https://www.google.com/chrome/)

OpenSSL is a toolkit that can be installed on a Windows or Linux system.

Cygwin is one option for a Linux install on a Windows system, this will be used for this document.

CygWin (http://www.cygwin.org/)

These are third party software and as such are not supported by Belden.

2.1.3 Laptop or Desktop Personal Computer required

These devices are not supplied nor supported by Belden

2.2 Information to get before starting:

This information may be supplied by your IT department or the network administrator for the network where the MNS, MNS-DX, INOS system will be installed.

2.2.1 IP address assigned to the Management Interface

Example Value Used: 192.168.1.2 (Default address for MNS, MNS-DX and INOS devices)

2.3 Special Note for DX Firmware Versions 4.1.0 and above

The following changes for the management station feature were done during implementation of Zero Touch Provisioning required by Industrial HiVision software.

Current default behavior for the management station is:

- By default SNMP V3 is enabled, and a default user of manager is configured.
- If no management station IP is configured, then the device will process the SNMP queries from all IP addresses. (This was done as the IP address of Industrial HiVision Software could be any address)
- If a management station IP is configured, the device will process the SNMP queries only from the IP addresses of the listed management stations.

3 Connecting to the DUT

3.1 Console Port Connections

The console port of the DX/XTS is an DB9 connector that can be located on either the front or rear of the system. It is always located with the LED indicators (power, activity or connectivity)

Use the appropriate cable to connect from the laptop to the console port. Start the Terminal program installed on your PC (TeraTerm in this document), select the appropriate serial port (this will vary from system to system depending on the cable and the adapter used) and configure the serial port properties as follows:

- 38400 Baud rate
- 8 Data bits
- 1 Stop bit
- No Parity
- No Flow Control

After completing this and hitting the enter key you should see a **login:** prompt. The default username and password is **manager**.

3.2 SSH Connections

Before connecting to the Ethernet port on the DUT the IP address of the Laptop/PC must be set to be in the same subnet as the default IP of the DUT, **in this example it is set to 192.168.1.2 mask 255.255.255.0.**

Only Ethernet port 6 is enabled when the DX/XTS is first powered up. The default address is 192.168.1.2.

Some Terminal Server software will take what seems a long time to make the first connection, do not despair a lot of back and forth occurs just this once and usually once all this has completed you will be asked to accept a key (not accepting this key will not allow you to login).

After this you will see a **login:** prompt. The default username and password is **manager**.

NOTE: Remember that once the IP address of the DUT has been changed this initial SSH connection will no longer be valid and a new session with the new address must be started to continue.

3.3 Web/GUI Connections

Before connecting to the Ethernet port on the DUT the IP address of the Laptop/PC must be set to be in the same subnet as the default IP of the DUT, **in this example it is set to 192.168.1.1 mask 255.255.255.0.**

Only Ethernet port 6 is enabled when the DX/XTS is first powered up. The example address is 192.168.1.2 and a secure connection is required. Thus the URL/Address to access will be **https://192.168.1.2**.

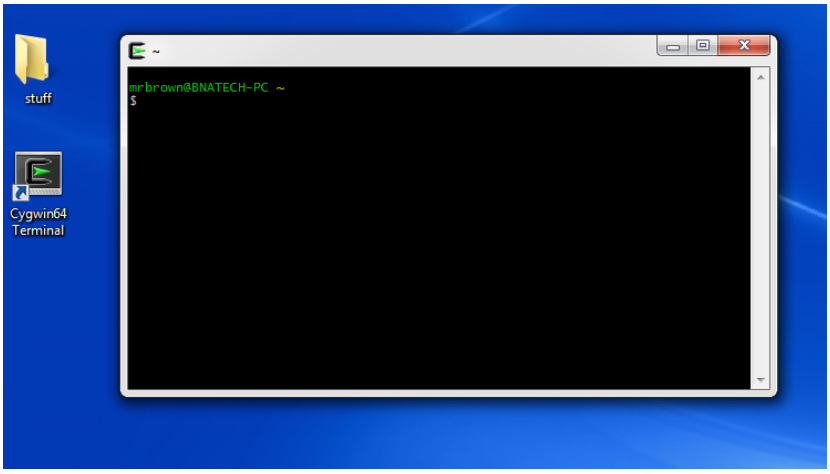
NOTE: All newer web browsers and all older browsers that have all of the security updates installed are configured by default to reject self-signed certificates (these certificates are used to setup the SSL secure connection). However you are offered as the user the opportunity to bypass this block and continue to the web page. You will be required to do this for the DUT.

After this you will see a **login:** screen. The default username and password is **manager**.

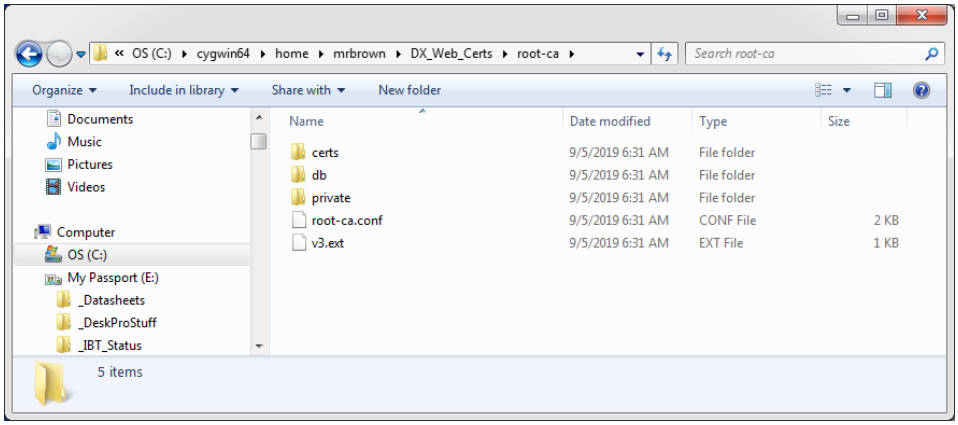
4 Using OpenSSL to Create a Certificate Authority

4.1 First Step Open the CygWin Terminal

If you feel comfortable the most cost effective method of creating signed certificates for installation on DX/XTS systems is to create your own root/Certificate Authority. This can be done using OpenSSL and for this How To, Cygwin is installed to allow running OpenSSL in Linux on a Windows System. The default installation of CygWin includes OpenSSL and the Linux file structure is easily accessible using Windows Explorer.



CygWin Desktop Icon and open Linux Terminal



Windows Explorer showing access to CygWin Linux Folders

The Folders and Files required by OpenSSL are also shown in this picture. The procedure to create both will be covered in the next section.

4.2 Second Step Create OpenSSL Configuration Files and Directories

- **Example of OpenSSL Configuration File [root-ca.conf]**

```
[default]
name = dxroot-ca
domain_suffix = TSBelden.com
aia_url = http://$name.$domain_suffix/$name.crt
crl_url = http://$name.$domain_suffix/$name.crl
ocsp_url = http://ocsp.$name.$domain_suffix:9080
default_ca = ca_default
name_opt = utf8,esc_ctrl,multiline,lname,align
[ca_dn]
countryName = "US"
organizationName = "Belden"
commonName = "DXRoot CA"
[ca_default]
home = .
database = $home/db/index
serial = $home/db/serial
crlnumber = $home/db/crlnumber
certificate = $home/$name.crt
private_key = $home/private/$name.key
RANDFILE = $home/private/random
new_certs_dir = $home/certs
unique_subject = no
copy_extensions = none
```

```
default_days = 18000

default_crl_days = 365

default_md = sha256

policy = policy_c_o_match


[policy_c_o_match]

countryName = match

stateOrProvinceName = optional

organizationName = match

organizationalUnitName = optional

commonName = supplied

emailAddress = optional


[req]

default_bits = 2048

encrypt_key = yes

default_md = sha256

utf8 = yes

string_mask = utf8only

prompt = no

distinguished_name = ca_dn

req_extensions = ca_ext


[ca_ext]

basicConstraints = critical,CA:true

keyUsage = critical,keyCertSign,cRLSign
```

```
subjectKeyIdentifier = hash

[sub_ca_ext]

authorityInfoAccess = @issuer_info

authorityKeyIdentifier = keyid:always

basicConstraints = critical,CA:true,pathlen:0

crlDistributionPoints = @crl_info

extendedKeyUsage = clientAuth,serverAuth

keyUsage = critical,keyCertSign,cRLSign

nameConstraints = @name_constraints

subjectKeyIdentifier = hash

[crl_info]

URI.0 = $crl_url

[issuer_info]

caIssuers;URI.0 = $aia_url

OCSP;URI.0 = $ocsp_url

[name_constraints]

permitted;DNS.0=example.com

permitted;DNS.1=example.org

excluded;IP.0=0.0.0.0/0.0.0.0

excluded;IP.1=0:0:0:0:0:0:0:0/0:0:0:0:0:0:0:0
```

The Following Items in this configuration file need to be changed for your specific location and corporate requirements.

The Sections from the above file the changes are made in are surrounded by []

```
[default]

name = dxroot-ca

domain_suffix = TSBelden.com
```

```
[ca_dn]
countryName = "US"
organizationName = "Belden"
commonName = "DXRoot_CA"
[ca_default]
default_days = 18000
default_md = sha256
[req]
default_bits = 2048
encrypt_key = yes
default_md = sha256
```

- **Example of OpenSSL Configuration File [v3.ext]**

```
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment,
dataEncipherment
[ dn ]
CN = 96.233.66.244
[ req_ext ]
subjectAltName = @alt_names
[ alt_names ]
DNS.1 = 96.233.66.244
IP.1 = 96.233.66.244
```

The IP Addresses in the v3.ext file should be the IP address of the DX the end certificate is to be signed for. The v3.ext file is NOT used as part of creating the root/Certificate Authority.

The above files can be created using any Text Editing software (NOT Microsoft Word).
The file format should be Linux compatible (LF NOT CR/LF for end of line).
The above files (root-ca.conf and v3.ext) should be placed in a folder to be used to hold both the root certificate and keys as well as all signed keys for use in the DX/XTS systems. This folder should be in the CygWin home folder of the user who installed CygWin.

- **Creating the Folders required by OpenSSL and checking OpenSSL is installed correctly**

```
mrbrown@BNATECH-PC ~

$ cd DX_Web_Certs

mrbrown@BNATECH-PC ~/DX_Web_Certs

$ ls -l

total 5

-rwxr-xr-x 1 mrbrown None 1728 Aug 30 08:26 root-ca.conf

-rwxr-xr-x 1 mrbrown None  282 Sep  4 06:32 v3.ext

mrbrown@BNATECH-PC ~/DX_Web_Certs

$ mkdir root-ca

mrbrown@BNATECH-PC ~/DX_Web_Certs

$ cd root-ca

mrbrown@BNATECH-PC ~/DX_Web_Certs/root-ca

$ mkdir certs db private

mrbrown@BNATECH-PC ~/DX_Web_Certs/root-ca

$ chmod 700 private

mrbrown@BNATECH-PC ~/DX_Web_Certs/root-ca

$ touch db/index

mrbrown@BNATECH-PC ~/DX_Web_Certs/root-ca

$ openssl rand -hex 16 > db/serial

mrbrown@BNATECH-PC ~/DX_Web_Certs/root-ca

$ echo 1001 > db/crlnumber
```

```
mrbrown@BNATECH-PC ~/DX_Web_Certs/root-ca
$ cp ../root-ca.conf .
mrbrown@BNATECH-PC ~/DX_Web_Certs/root-ca
$ cp ../v3.ext .
mrbrown@BNATECH-PC ~/DX_Web_Certs/root-ca
$ ls -l
total 5
drwxr-xr-x+ 1 mrbrown None    0 Sep  5 06:31 certs
drwxr-xr-x+ 1 mrbrown None    0 Sep  5 06:31 db
drwx------+ 1 mrbrown None    0 Sep  5 06:31 private
-rwxr-xr-x  1 mrbrown None 1728 Sep  5 06:31 root-ca.conf
-rwxr-xr-x  1 mrbrown None  282 Sep  5 06:31 v3.ext
mrbrown@BNATECH-PC ~/DX_Web_Certs/root-ca
$ openssl version
OpenSSL 1.1.1c  28 May 2019
```

4.3 Third Step Create the CA/Root Certificate and Keys

The following steps need to be done only once to create a CA/Root certificate used to sign any number of certificate requests created by the installed base of DX/XTS systems in your network.

```
mrbrown@BNATECH-PC ~/DX_Web_Certs/root-ca
$ openssl req -new -config root-ca.conf -out dxroot-ca.csr -keyout private/dxroot-ca.key
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'private/dxroot-ca.key'
```

```
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
mrbrown@BNATECH-PC ~/DX_Web_Certs/root-ca
$ openssl ca -selfsign -config root-ca.conf -in dxroot-ca.csr -out dxroot-ca.crt  -extensions ca_ext
Using configuration from root-ca.conf
Enter pass phrase for ./private/dxroot-ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            60:fb:ce:7c:b1:92:a0:e4:f6:4e:27:40:01:09:22:0e
        Issuer:
            countryName               = US
            organizationName          = Belden
            commonName                = DXRoot CA
        Validity
            Not Before: Sep  5 13:12:08 2019 GMT
            Not After : Dec 16 13:12:08 2068 GMT
        Subject:
            countryName               = US
            organizationName          = Belden
            commonName                = DXRoot CA
```

```
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        RSA Public-Key: (2048 bit)
        Modulus:
            00:d9:f7:8c:d5:e5:84:67:55:57:d5:95:c3:13:de:
            96:9d:cf:e2:b4:3e:71:17:e7:08:41:ac:63:c5:9d:
            a1:48:85:d4:34:4a:40:5d:98:fd:9b:69:d0:01:f6:
            45:3d:c4:a7:73:79:ba:b7:b0:66:7e:09:b0:e7:4c:
            77:51:d7:5f:ed:71:a8:1f:90:45:df:b5:b1:26:46:
            d7:09:5e:24:db:6c:17:03:b1:4d:9c:4e:b7:24:71:
            d6:af:4c:b6:90:b5:e9:ac:5b:55:ff:db:87:79:c3:
            a3:17:4b:72:96:e3:63:76:3c:4f:4c:5f:25:80:dd:
            34:75:7a:f2:aa:42:ae:43:50:99:2f:47:3f:58:05:
            8e:0e:ea:3b:22:27:4e:b6:d3:33:23:06:fb:7f:0d:
            8b:a1:76:34:a2:75:bf:c2:18:93:77:c0:6a:be:19:
            71:03:b4:25:ce:1f:3b:4d:61:2c:60:f7:bf:77:3f:
            1d:df:bc:e5:05:48:6a:12:c8:19:14:b1:5e:f2:ed:
            38:45:32:51:f2:db:a0:7f:ee:57:49:16:77:d3:69:
            c7:fe:82:08:af:c3:16:a7:9c:1e:8f:b8:29:7e:69:
            c4:36:b1:c5:30:98:e3:f9:ec:d6:11:90:e4:75:21:
            43:e7:73:67:d0:a4:6d:0f:d1:71:0c:8c:2b:76:fe:
            b7:c5
        Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Basic Constraints: critical
        CA:TRUE
```

```
        X509v3 Key Usage: critical
            Certificate Sign, CRL Sign
        X509v3 Subject Key Identifier:
            E6:74:E8:2A:5E:2B:A2:6D:23:95:8F:3B:A1:A1:15:5F:DF:65:C4:CA
Certificate is to be certified until Dec 16 13:12:08 2068 GMT (18000 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated


mrbrown@BNATECH-PC ~/DX_Web_Certs/root-ca
$ ls -l
total 21
drwxr-xr-x+ 1 mrbrown None    0 Sep  5 09:12 certs
drwxr-xr-x+ 1 mrbrown None    0 Sep  5 09:12 db
-rw-r--r--  1 mrbrown None 4163 Sep  5 09:12 dxroot-ca.crt
-rw-r--r--  1 mrbrown None 1041 Sep  5 09:10 dxroot-ca.csr
drwx------+ 1 mrbrown None    0 Sep  5 09:08 private
-rwxr-xr-x  1 mrbrown None 1728 Sep  5 06:31 root-ca.conf
-rwxr-xr-x  1 mrbrown None  282 Sep  5 06:31 v3.ext


mrbrown@BNATECH-PC ~/DX_Web_Certs/root-ca
$
```

The pass phrase used above [Enter PEM pass phrase:] should be treated the same as any other password and only kept in either a password lock box or Encrypted file.

5 Using the DX/XTS to Create a Certificate Request

5.1 First Step Check Network Connectivity

Ping from the CygWin PC to the DX you want to create the certificate request on

C:\Users\mrbrown>ping 96.233.66.245

Pinging 96.233.66.245 with 32 bytes of data:

Reply from 96.233.66.245: bytes=32 time=1ms TTL=63

Reply from 96.233.66.245: bytes=32 time=1ms TTL=63

Reply from 96.233.66.245: bytes=32 time=1ms TTL=63

Ping statistics for 96.233.66.245:

Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milliseconds:

Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\mrbrown>ping 96.233.66.245

Pinging 96.233.66.245 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 96.233.66.245:

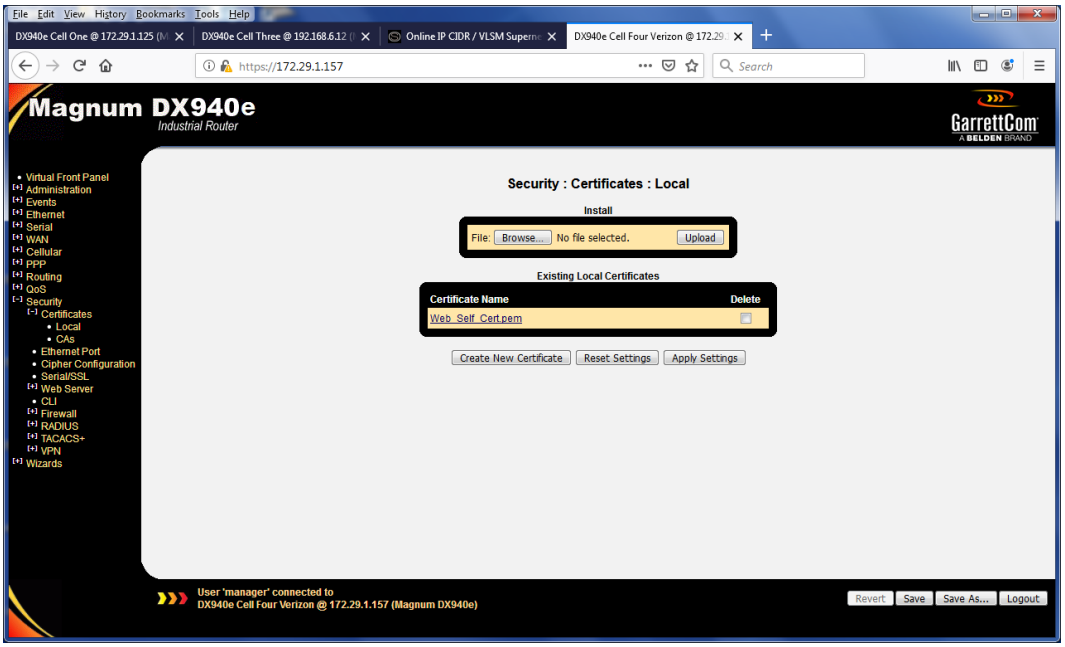
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\mrbrown>

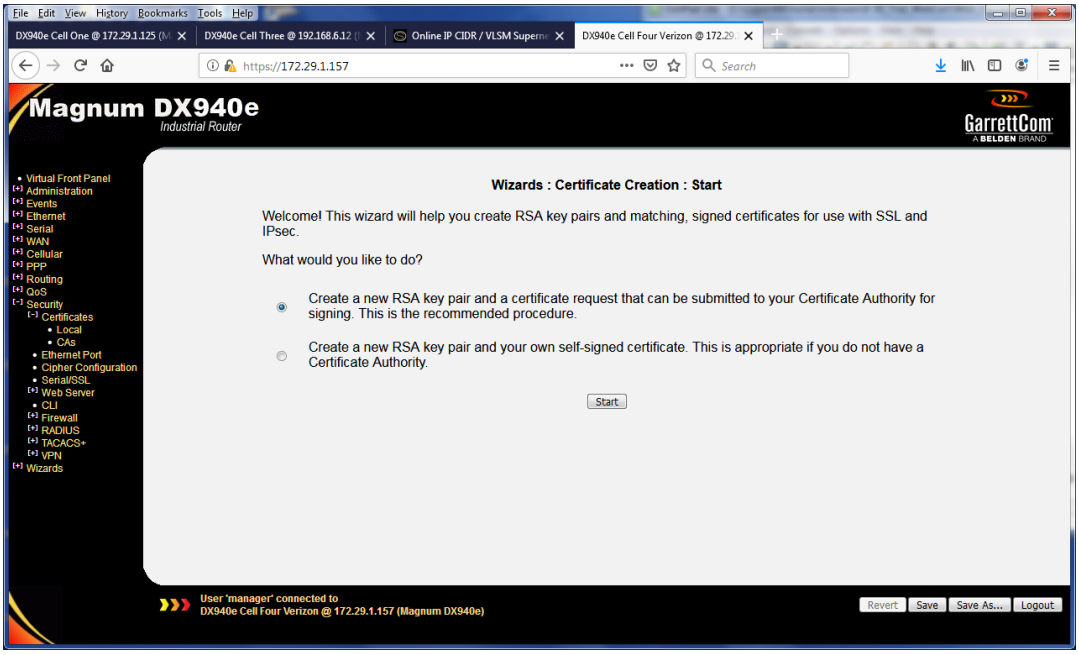
The above is an example of 2 ping requests from the System that hosts the Cygwin OpenSSL installation to the system (DX40 in this example) you want to create the certificate request on. The first shows 4 good ping request/replies, with this result it is time to continue to the next step. The second shows a ping request timeout a timeout indicates a network problem. This network problem needs to be solved before continuing, this document does not cover debugging network problems.

5.2 Second Step Access the DX Certificates Section via the Web/GUI

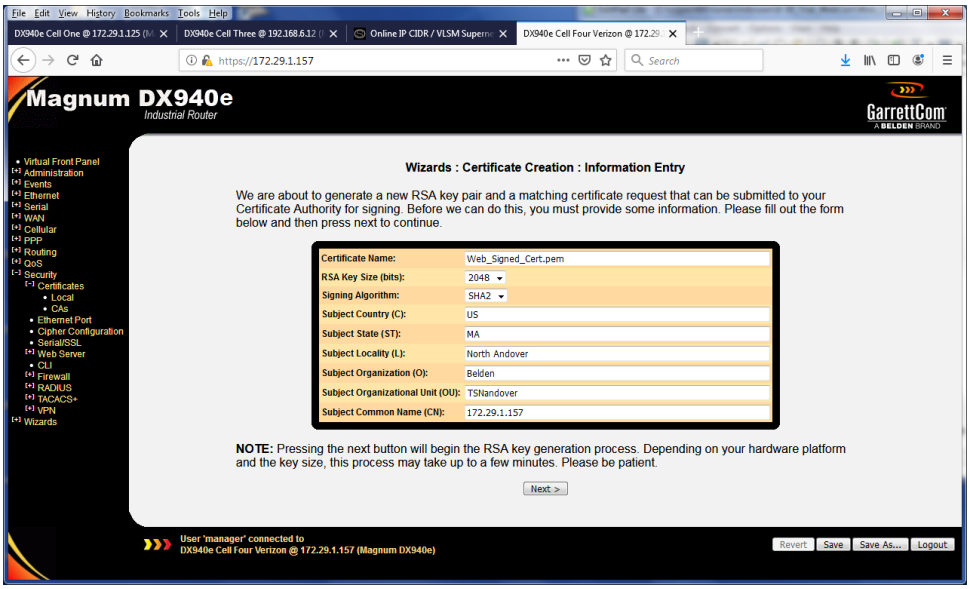
Once you have logged into the DX go to the Security/Certificates/Local



Click on the Create New Certificate Button

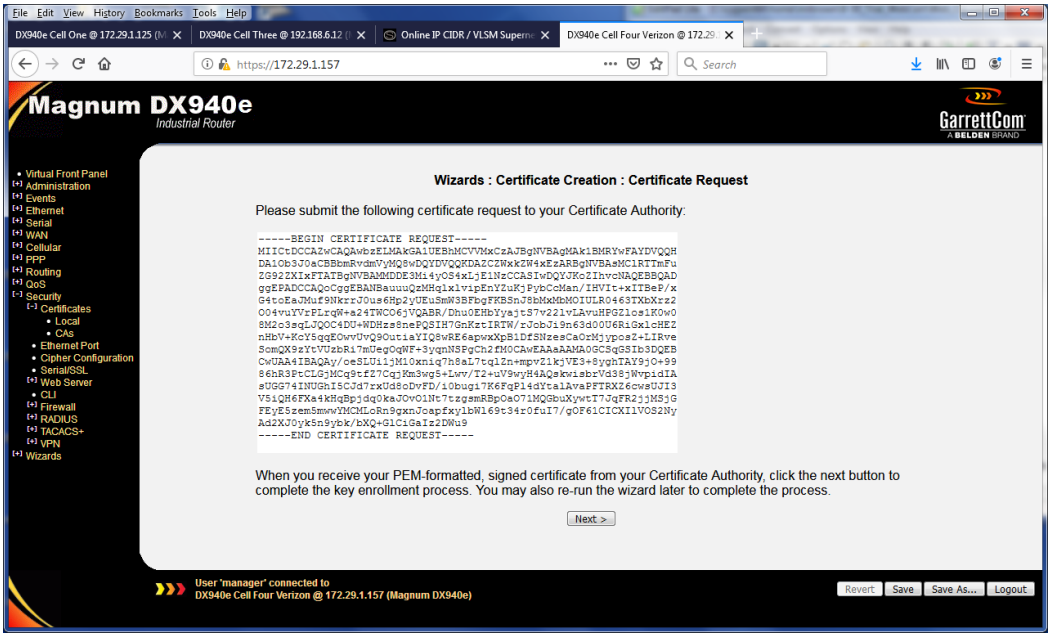


Select Create New Key Pair and Certificate Request then the Start Button

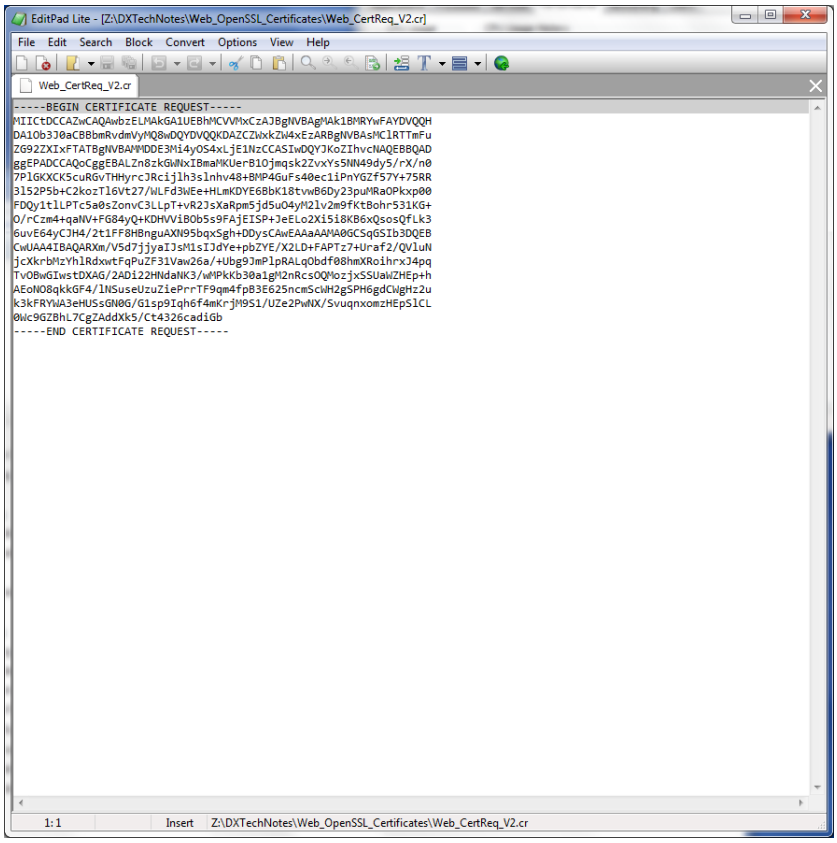


Fill in the Fields on the Information Page, When done click the Next Button

- Certificate name is anything you want but make it unique to the system
- RSA Key Size and Signing Algorithm are recommended to be as shown
- The remaining fields should reflect local requirements
- The Subject Common Name (CN:) is recommended to be the IP address of the DX

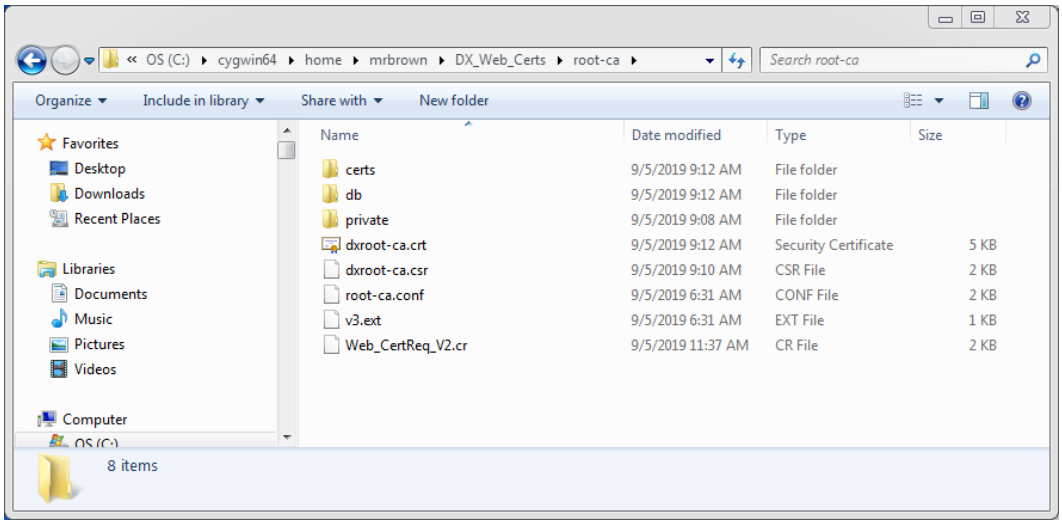


Select the Certificate Request then Copy and Paste into a File Select the Next Button



Certificate Request Pasted in Text Editor

5.3 Third Step, Save the Certificate Request to the CygWin OpenSSL Folder



6 Using OpenSSL CA to Sign a DX/XTS Certificate Request

6.1 Make sure the V3.ext File has the Correct IP Addresses

```
authorityKeyIdentifier=keyid,issuer

basicConstraints=CA:FALSE

keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment


[ dn ]

CN = 172.29.1.157


[ req_ext ]

subjectAltName = @alt_names


[ alt_names ]

DNS.1 = 172.29.1.157

IP.1 = 172.29.1.157
```

172.29.1.157 matches the IP of the DX that generated the Certificate Request

6.2 Sign The DX Certificate Request using OpenSSL

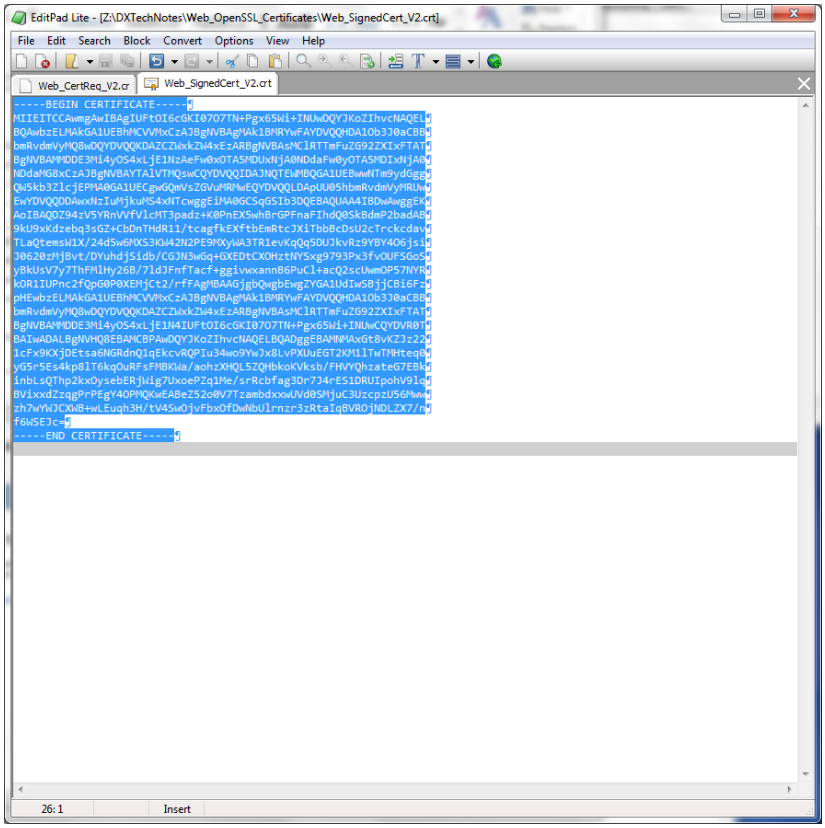
```
mrbrown@BNATECH-PC ~/DX_Web_Certs/root-ca

$ ls -l

total 25

drwxr-xr-x+ 1 mrbrown None    0 Sep  5 09:12 certs

drwxr-xr-x+ 1 mrbrown None    0 Sep  5 09:12 db

-rw-r--r--  1 mrbrown None 4163 Sep  5 09:12 dxroot-ca.crt

-rw-r--r--  1 mrbrown None 1041 Sep  5 09:10 dxroot-ca.csr
```

```
drwx------+ 1 mrbrown None    0 Sep  5 09:08 private

-rwxr-xr-x  1 mrbrown None 1728 Sep  5 06:31 root-ca.conf

-rwxr-xr-x  1 mrbrown None  279 Sep  5 12:00 v3.ext

-rwxr-xr-x  1 mrbrown None 1028 Sep  5 11:37 Web_CertReq_V2.cr



mrbrown@BNATECH-PC ~/DX_Web_Certs/root-ca

$ openssl x509 -req -days 3650 -in Web_CertReq_V2.cr -signkey private/dxroot-ca.key -out
Web_SignedCert_V2.crt  -extfile v3.ext

Signature ok

subject=C = US, ST = MA, L = North Andover, O = Belden, OU = TSNandover, CN = 172.29.1.157

Getting Private key

Enter pass phrase for private/dxroot-ca.key:



mrbrown@BNATECH-PC ~/DX_Web_Certs/root-ca

$ ls -l

total 29

drwxr-xr-x+ 1 mrbrown None    0 Sep  5 09:12 certs

drwxr-xr-x+ 1 mrbrown None    0 Sep  5 09:12 db

-rw-r--r--  1 mrbrown None 4163 Sep  5 09:12 dxroot-ca.crt

-rw-r--r--  1 mrbrown None 1041 Sep  5 09:10 dxroot-ca.csr

drwx------+ 1 mrbrown None    0 Sep  5 09:08 private

-rwxr-xr-x  1 mrbrown None 1728 Sep  5 06:31 root-ca.conf

-rwxr-xr-x  1 mrbrown None  279 Sep  5 12:00 v3.ext

-rwxr-xr-x  1 mrbrown None 1028 Sep  5 11:37 Web_CertReq_V2.cr

-rw-r--r--  1 mrbrown None 1493 Sep  5 12:04 Web_SignedCert_V2.crt



mrbrown@BNATECH-PC ~/DX_Web_Certs/root-ca

      $
```

7 Loading the Signed Certificate onto the DX/XTS

Once the Certificate request is signed the DX/XTS offers a method to cut and paste the contents of the signed request back onto the DX/XTS

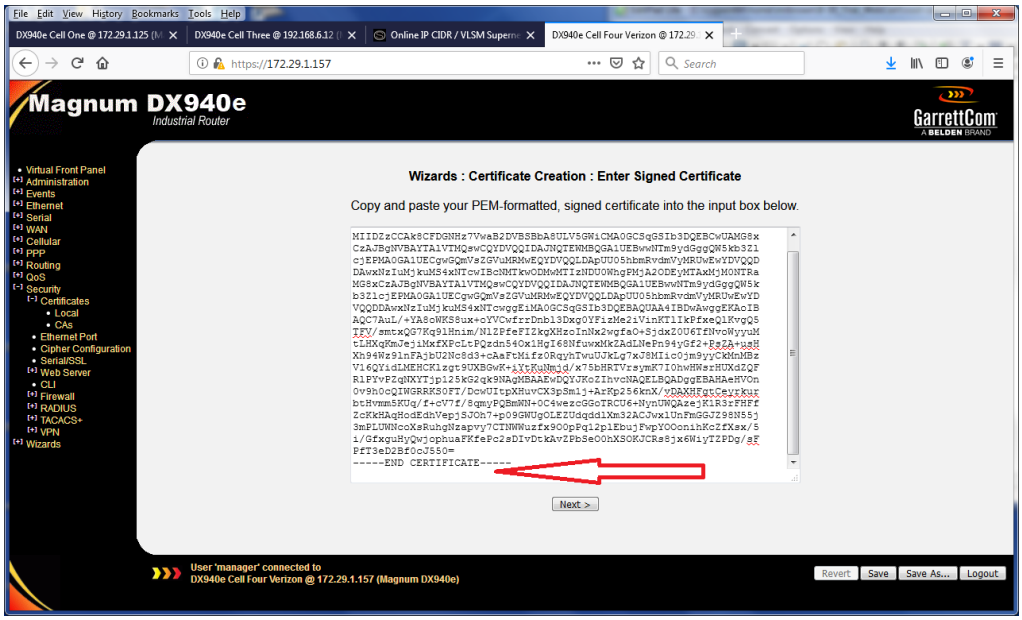
7.1 Open the Signed Certificate in a Text Editor



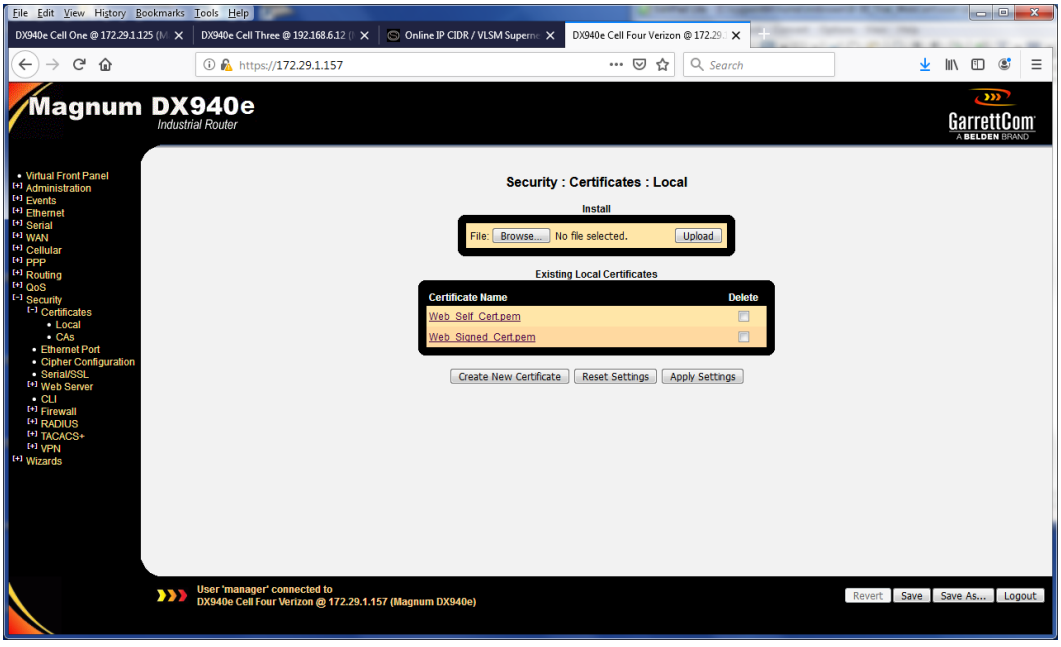
Notice that the last line including the end line character is selected. **THIS IS VERY IMPORTANT**

If all end line characters of the file are not copied over to the DX the process will fail. There will be NO ERROR messages in any DX940/10XTS before Firmware version V4.1.2 or DX940E before firmware version 1.0.3. All other DX systems DX800/DX900/DX1000 will never show an error message, these systems are no longer supported for firmware upgrades.

7.2 Copy and Paste the Signed Certificate into the Empty Box in the DX Window



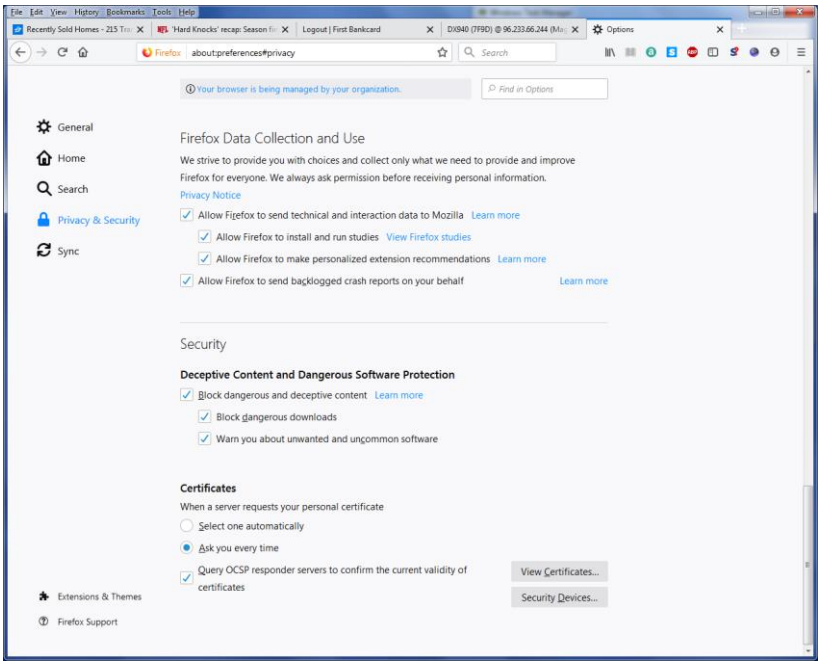
The Red Arrow Points to the empty last line pasted into the window as part of copying the signed certificate. If this empty line is not seen then delete what is in the window and try the copy and paste again. Once the contents of the signed certificate are copied correctly then click on the next button.

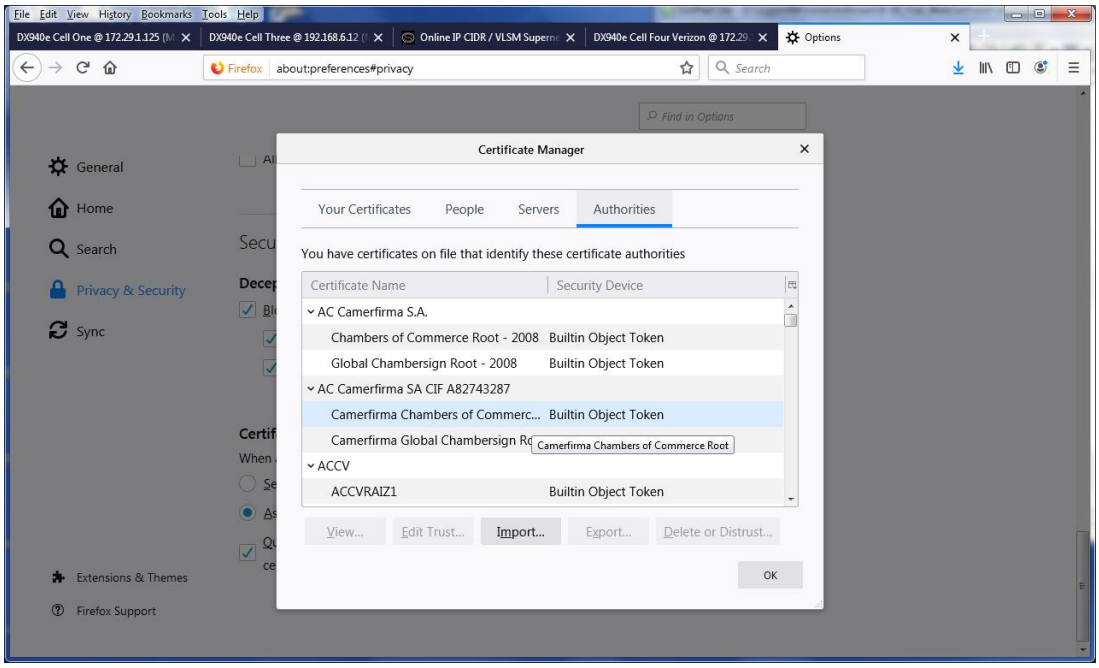


The Signed Certificate is now on the DX/XTS and can be selected for use by the Web Server

7.3 Import the root-ca.crt onto the Browsers Trusted Authorities

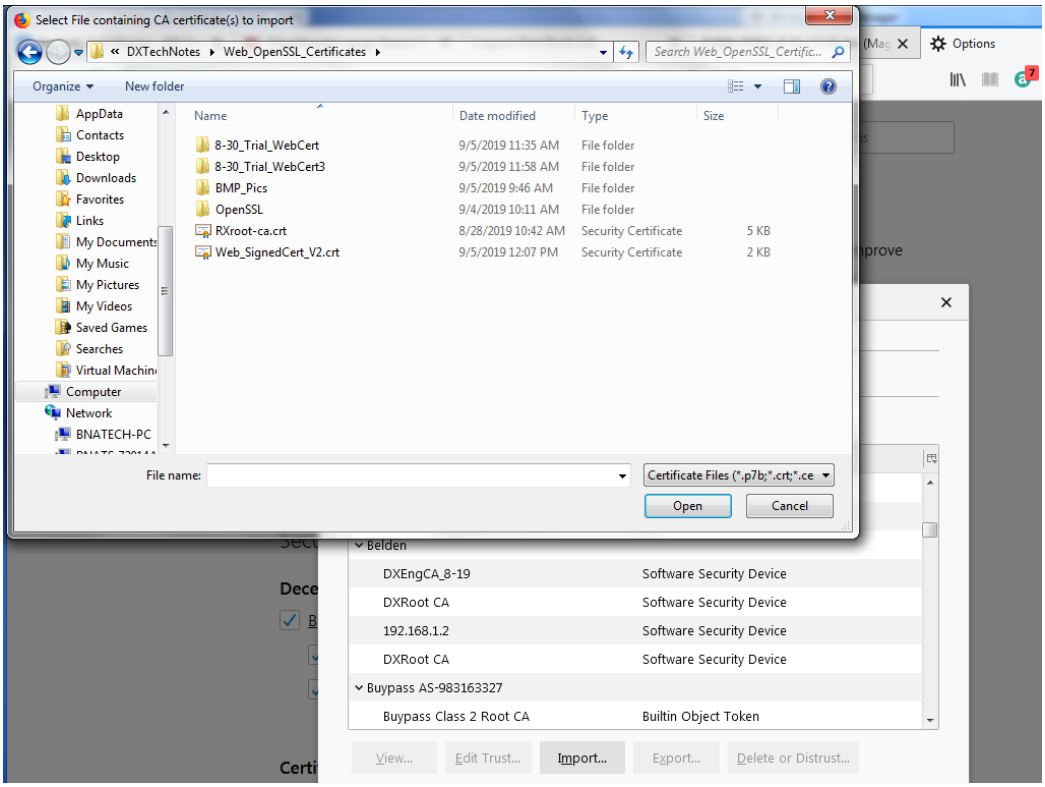
The following Instructions ONLY PERTAIN to the latest release of the Firefox browser your mileage may vary.

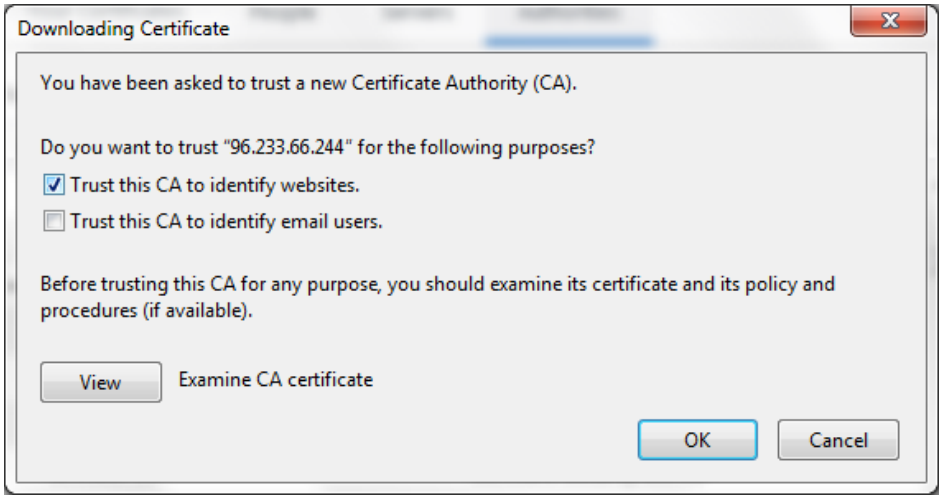




Click on the Hamburger button on the top right of the browser select options, then Privacy and Security. Click on the View Certificates button make sure the Authorities tab is selected.

Click on the Import button and load the root-ca.crt you created in step 4 earlier.

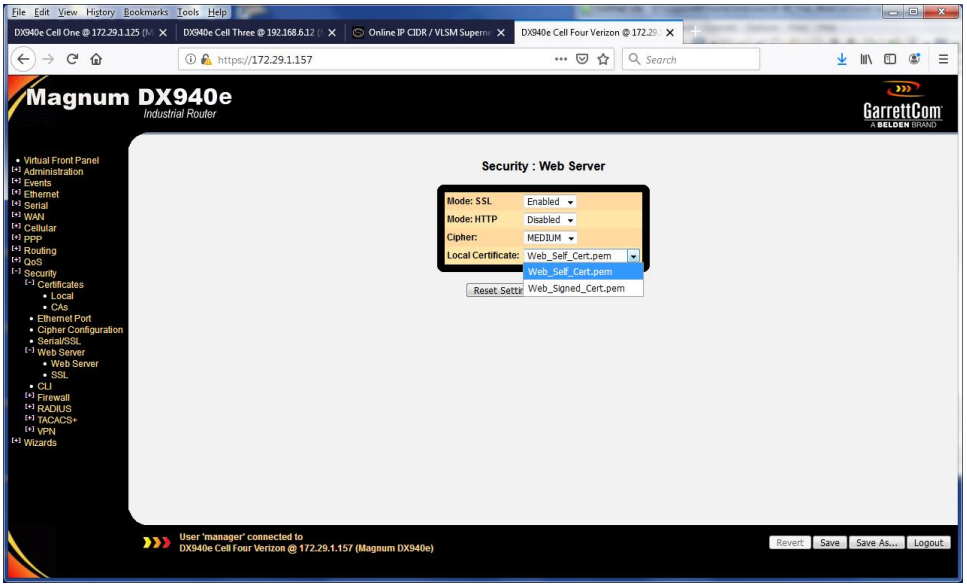




Make sure you click on the Trust this CA to identify websites then click OK

You have now configured the browser to recognize your signed certificates as valid

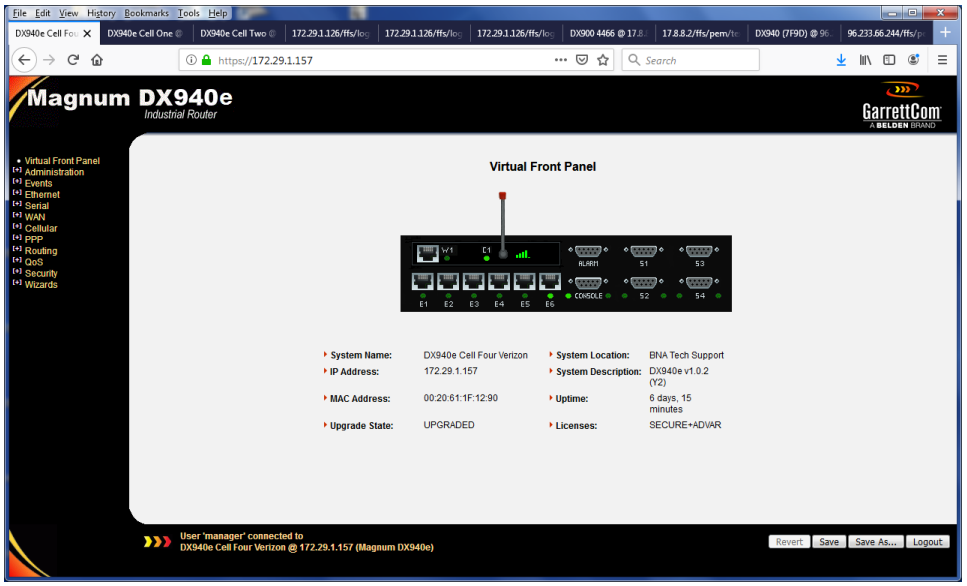
7.4 Change your selected Web Server Certificate to use the Signed Certificate



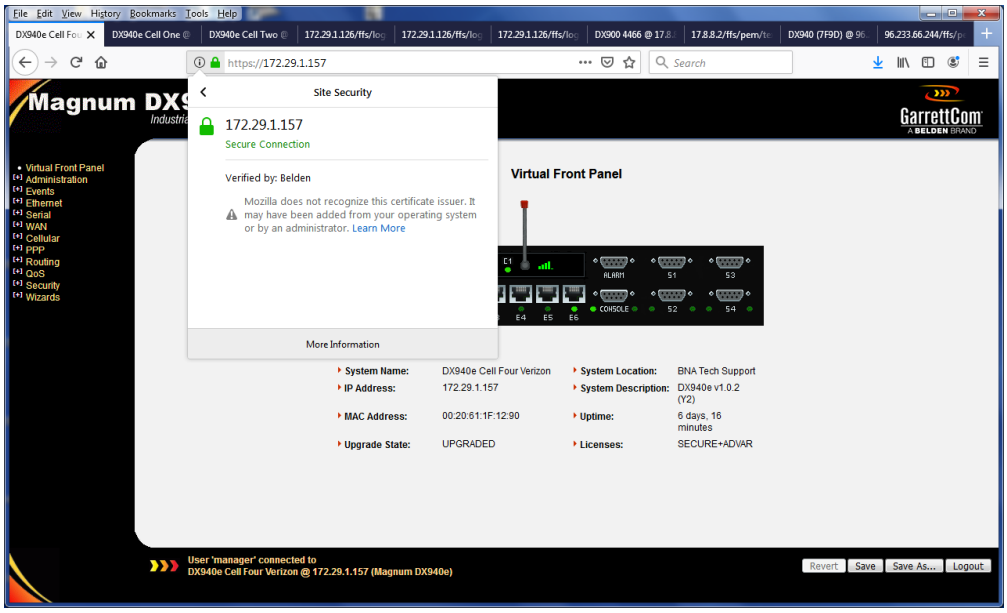
After selecting the signed certificate make sure you click on the apply button

At this point you will most likely lose contact with the DX as the hash has changed with the new certificate. Click on the browser refresh button to reload.

7.5 After Refreshing the Browser Save your changes by Clicking on Save



Note Green Padlock in Address Bar



If you click on the I icon next to the padlock you can see how Firefox now rates the DX webservers HTTPS as secure. This also speeds up login as the browser is no longer warning you as below.