NETWORK TECHNOLOGIES INCORPORATED
1275 Danner Dr Tel:330-562-7070
Aurora, OH 44202 Fax:330-562-1999
www.networktechinc.com

# Creation of Custom x509 Certificates for ENVIROMUX Series Products

The ENVIROMUX family of products is designed to be configurable with security to limit access to their web interface controls. The ENVIROMUX includes a default x.509 certificate. However, this procedure will help you create your own custom x.509 certificate to use with this feature. This procedure was created using CentOS and OpenSSL.

**Note: Do not disable access to the ENVIROMUX web interface using http before you verify that the https client authentication works properly (see last page).**

## I. Using Self-Signed Certificates for ENVIROMUX Series Products

We can use self-signed certificates to access ENVIROMUX products with HTTPS with a self-signed root certificate authority. In this procedure, our root certificate authority needs to be explicitly added to every PC as trusted authority, to access the product page.

### 1. Creating a Self-Signed Certificate Authority using OpenSSL

An example SSL configuration file to use can be found here: **http://www.networktechinc.com/download/openssl.cnf**
When using this document, make a copy of the current default openssl configuration file and replace it with the file above.

#### a. Creating the Certificate Management Files and Directories

The following directories are made for organizing the files being used and generated. These directories are also used for other procedures in the document.

1. Create directory "ntiCA" in /usr/local/ssl for ntiCA certificate management and change to that directory. If you prefer, this directory name can be set to any other name like MyCompanyCA. Make sure the **`openssl.cnf`** file is edited to match the changes to the folder name. The **`openssl.cnf`** file can usually be found in /usr/local/openssl/openssl.cnf on local installations of OpenSSL.

```
# mkdir /usr/local/ssl/ntiCA
# cd /usr/local/ssl/ntiCA
```

Create the following directories in the ntiCA directory: **(The number sign (#) is the command prompt, not part of the command.)**

```
# mkdir CA
# mkdir server
# mkdir server/certificates
# mkdir server/requests
# mkdir server/keys
# mkdir user
# mkdir user/certificates
# mkdir user/requests
# mkdir user/keys
```

Perform the following commands in the ntiCA directory:

```
# cd /usr/local/ssl/ntiCA
# touch index.txt
# echo "01" > serial
```

#### b. Creating the CA Key and Certificate

The general process for creating a certificate includes:

1. Creating a private CA key
2. Creating a certificate request
3. Creating and signing a certificate from the certificate request

1. Create the private CA key:

```
# cd /usr/local/ssl/ntiCA
# openssl genrsa -out ./CA/ntiCA.key 2048
Generating RSA private key, 2048 bit long modulus
.....++++++
......++++++
e is 65537 (0x10001)
```

2. Create the CA certificate signing request:

```
# openssl req -sha512 -new -key ./CA/ntiCA.key -out ./CA/ntiCA.csr
```

```
You are about to be asked to enter information that will be incorporated into your certificate
request.
    What you are about to enter is what is called a Distinguished Name or a DN.
    There are quite a few fields but you can leave some blank
    For some fields there will be a default value,(indicated by the characters "[ ]")
    If you enter '.', the field will be left blank.
  -----
    Country Name (2 letter code) [US]:US
    State or Province Name (full name) [OH]:OH
    Locality Name (eg, city) []:
    Organization Name (eg, company) [NTI]:NTI
    Organizational Unit Name (eg, section) []:
    Common Name (eg, YOUR name) [NTI CA]:NTI CA
    Email Address [sales@ntigo.com]:sales@ntigo.com

    Please enter the following 'extra' attributes
    to be sent with your certificate request
    . []:
    . []:
```

3. Self-sign the CA certificate:

```
# openssl x509 -req -sha512 -days 3650 -in ./CA/ntiCA.csr -out ./CA/ntiCA.crt
-signkey ./CA/ntiCA.key
Signature ok
subject=C = US, ST = OH, O = NTI, CN = NTI CA, emailAddress = sales@ntigo.com
Getting Private key
```

### c. Verifying the CA certificate contents

At this point we have our self-signed CA certificate and our CA key, which will be used to sign the ENVIROMUX certificates that we create. To verify the certificate contents, use the following command:

```
# openssl x509 -in ./CA/ntiCA.crt -text
```

The output should look similar to this:

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            b2:ce:14:9d:bf:52:f5:1f
    Signature Algorithm: sha512WithRSAEncryption
        Issuer: C = US, ST = OH, O = NTI, CN = NTI CA, emailAddress = sales@ntigo.com
        Validity
            Not Before: Dec  4 20:00:24 2018 GMT
            Not After : Dec  1 20:00:24 2028 GMT
        Subject: C = US, ST = OH, O = NTI, CN = NTI CA, emailAddress = sales@ntigo.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b0:43:2b:de:93:7b:ac:1f:24:96:9d:e9:98:26:
                    44:bc:cb:7e:04:ec:c2:64:da:60:59:a1:c8:b7:42:
                    52:04:b7:b2:91:b1:10:db:ea:04:25:52:14:8b:52:
                    a4:7f:5a:fc:08:65:c6:77:44:8b:48:27:71:68:00:
                    c2:09:a2:b4:4a:3d:f9:3c:f8:d0:69:24:e8:44:b8:
                    07:57:e1:57:2d:0e:9b:2f:3e:df:4c:71:00:45:bb:
                    ff:2d:a6:7f:11:2d:34:ca:f2:07:f5:79:f0:4f:9b:
                    d8:d3:ad:04:3b:3c:56:07:25:c1:be:fe:09:03:8a:
                    6e:4d:72:82:ad:67:22:2c:54:1b:d5:69:5b:2b:67:
                    1f:12:f5:98:ef:a4:10:1d:56:83:13:ca:8d:d7:2f:
                    c5:0a:da:d5:3b:30:25:9a:2c:6f:8c:94:c1:69:35:
                    e2:38:9b:1b:37:53:ff:d6:2d:3e:d9:1c:7a:03:b3:
                    71:a6:76:16:f4:eb:35:2a:f2:86:6f:40:d9:cc:6e:
                    59:31:ef:94:11:cf:cc:52:9d:eb:8e:06:69:67:ee:
                    86:98:b0:54:11:61:71:aa:ae:19:2a:f3:77:ce:95:
                    2c:a5:87:0d:10:16:b9:5e:88:c8:03:da:d9:6d:90:
                    3b:ca:4c:32:15:0c:ba:05:64:79:c7:4b:b0:7a:f5:
                    26:5d
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha512WithRSAEncryption
         9f:d2:50:61:36:f3:d9:b9:cb:39:5e:31:d6:2a:a8:e4:03:f0:
         e0:65:4d:37:e0:60:cd:71:f5:5a:6d:7d:87:53:6e:2e:8b:3a:
         f2:fb:73:fc:21:51:63:79:8a:2d:5d:a9:c2:a9:47:a1:b3:17:
         9a:2e:5b:8a:7f:29:ab:08:cb:2f:52:70:26:2c:76:2d:2d:07:
         81:cc:84:6f:59:db:f3:be:fe:77:dc:67:6b:5d:ff:b3:17:24:
         bd:f3:c0:cc:83:10:d0:17:67:2d:e5:5b:4b:59:aa:80:fb:ec:
         53:ed:e4:c5:0d:a1:0d:13:b3:0b:ee:a4:c2:f0:d2:a0:29:ef:
         11:f5:6a:29:8b:46:ed:1a:64:2b:93:02:af:0d:7f:83:28:2c:
         a2:11:2e:e6:fc:af:61:d2:df:eb:e2:c0:e2:46:6e:ef:51:6e:
         e1:db:4f:d4:24:2b:6d:63:21:d0:3c:f2:02:6e:d0:63:10:bf:
         1c:9c:bf:31:c8:74:cd:88:51:7b:cc:a6:8d:6d:c1:fb:5c:63:
         8a:dc:74:de:5f:04:d2:2d:b0:5b:c7:65:06:37:c0:42:8d:87:
         22:2e:2d:59:dc:89:6c:e4:32:fe:2f:88:da:42:50:6e:67:3e:
         6c:7c:86:9b:f4:20:60:6b:26:c2:cd:0b:97:d8:e1:f5:f9:c1:
         4c:32:6c:ab
-----BEGIN CERTIFICATE-----
MIIDLjCCAhYCCQCyzhSdv1L1HzANBgkqhkiG9w0BAQ0FADBZMQswCQYDVQQGEwJV
UzELMAkGA1UECBMCT0gxDDAKBgNVBAoTA05USTEPMA0GA1UEAxMGTlRJIENBMR4w
```

```
HAYJKoZIhvcNAQkBFg9zYWxlc0BudGlnby5jb20wHhcNMTgxMjA0MjAwMDI0WhcN
MjgxMjAxMjAwMDI0WjBZMQswCQYDVQQGEwJVUzELMAkGA1UECBMCT0gxDDAKBgNV
BAoTA05USTEPMA0GA1UEAxMGTlRJIENBMR4wHAYJKoZIhvcNAQkBFg9zYWxlc0Bu
dGlnby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCwQyvek3us
HySWnemYJkS8y34E7MJk2mBZoci3QlIEt7KRsRDb6gQlUhSLUqR/WvwIZcZ3RItI
J3FoAMIJorRKPfk8+NBpJOhEuAdX4VctDpsvPt9McQBFu/8tpn8RLTTK8gf1efBP
m9jTrQQ7PFYHJcG+/gkDim5NcoKtZyIsVBvVaVsrZx8S9ZjvpBAdVoMTyo3XL8UK
2tU7MCWaLG+MlMFpNeI4mxs3U//WLT7ZHHoDs3Gmdhb06zUq8oZvQNnMblkx75QR
z8xSneuOBmln7oaYsFQRYXGqrhkq83fOlSylhw0QFrleiMgD2tltkDvKTDIVDLoF
ZHnHS7B69SZdAgMBAAEwDQYJKoZIhvcNAQENBQADggEBAJ/SUGE289m5yzleMdYq
qOQD8OBlTTfgYM1x9VptfYdTbi6LOvL7c/whUWN5ii1dqcKpR6GzF5ouW4p/KasI
yy9ScCYsdi0tB4HMhG9Z2/O+/nfcZ2td/7MXJL3zwMyDENAXZy3lW0tZqoD77FPt
5MUNoQ0TswvupMLw0qAp7xH1aimLRu0aZCuTAq8Nf4MoLKIRLub8r2HS3+viwOJG
bu9RbuHbT9QkK21jIdA88gJu0GMQvxycvzHIdM2IUXvMpo1twftcY4rcdN5fBNIt
sFvHZQY3wEKNhyIuLVnciWzkMv4viNpCUG5nPmx8hpv0IGBrJsLNC5fY4fX5wUwy
bKs=
-----END CERTIFICATE-----
```

## 2. Creating a CA-Signed ENVIROMUX server Certificate (This will need to be done for each ENVIROMUX device.)

The procedure for creating a CA-Signed web server certificate is similar to that for creating the CA certificate except that the device certificate will be signed using the CA key rather than self-signing with a server-specific key.

a. Create the web server private key using a fully qualified DNS name (or IP address).

```
# cd /usr/local/ssl/ntiCA
# openssl genrsa -out ./server/keys/your_device_fqdn_or_ipaddress.key 2048
Generating RSA private key, 2048 bit long modulus
.......++++++
.++++++
e is 65537 (0x10001)
```

b. Create the web server certificate signing request using the same fully qualified DNS name (or IP address) you used for the private key. **It is vitally important** that you set the Common Name value to the fully qualified DNS name of your web server because that's the value that a browser client will verify when it receives the web server's certificate.

```
# openssl req -sha512 -new -key ./server/keys/your_device_fqdn_or_ipaddress.key -
out ./server/requests/your_device_fqdn_or_ipaddress.csr

You are about to be asked to enter information that will be incorporated into your
certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value, (indicated by the characters "[ ]")
If you enter '.', the field will be left blank.
-----
Country Name [US]:US
State or Province Name [OH]:OH
Locality Name []:Aurora
Organization Name [NTI]:NTI
Organizational Unit Name []:
Common Name [NTI CA]:192.168.3.144
Email Address [sales@ntigo.com]:your_name@example.com

Please enter the following 'extra' attributes
```

```
to be sent with your certificate request
. []:
. []:
```

c. Create a file defining the Subject Alternative Name. This extension file extensions.ext can be made with any text editor, and should be added to the /usr/local/ssl/ntiCA directory. This needs to be defined to know for what domains or IP addresses the certificate will be valid. Add the following lines to the **`extensions.ext`** file:

basicConstraints=CA:FALSE

subjectAltName=IP:**<ip_address>**

Replace "**<ip_address>**" with the IP address you plan to use to access the device. Other options are available for specifying this. Below is an example using a DNS:

subjectAltName = DNS:server.example.com

d. Sign the web server certificate with the CA key:

```
# openssl x509 -req –in server/requests/your_device_fqdn_or_ipaddress.csr -CA
CA/ntiCA.crt -CAkey CA/ntiCA.key –CAcreateserial -out your_device_fqdn_or_ipaddress.pem -
days 1024 -extfile extensions.ext
```

```
Signature ok
subject=C = US, ST = OH, L = Aurora, O = NTI, CN = 192.168.3.144, emailAddress =
sales@ntigo.com
Getting CA Private Key
```

To verify the web server certificate contents, use the following command:

```
# openssl x509 -in your_device_fqdn_or_ipaddress.pem -text
```

Key values to look for are:

```
Subject CN=192.168.3.144
Issuer CN=NTI CA
```

## 3. Uploading a Self-Signed Certificate Authority to a ENVIROMUX Device

You should import the "ntiCA.crt" file located in the /usr/local/ssl/ntiCA/CA directory that is generated using this procedure into the ENVIROMUX. To import this file into the ENVIROMUX, you must log into its web interface.

On the ENVIROMUX Web Interface menu Under "Administration" select "Network". In X509 certificates, select "Choose File", select the CA certificate file ntiCA.crt, and click **"Upload CA certificate**".

## 4. Uploading Server Certificate to a ENVIROMUX Device

The NTI ENVIROMUX web server expects the certificate and key as a single file in "PEM" format.

Use the following command to combine certificate and key file to a single file with extension "pem".

```
cat ./server/keys/your_device_fqdn_or_ipaddress.key your_device_fqdn_or_ipaddress.pem >
server.pem
```

On the ENVIROMUX Web Interface menu Under "Administration" select "Network". In X509 certificates, select "Choose File", select the server certificate and key file, and click "Upload **Server certificate and key"**.

The following is an example of what the **`server.pem`** file should look like:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAxKmpFfvWbJymSP2Pos/+NIDQvmoIU4xv2FBZBuOrc+uRKf1D
y2VeFKlMufp2JXMTxSHXCOjyZgVvEH9jb1VORU6WRz2/6VG5hYDqFa8dptC9YJ2S
yRUa6STObwSZCCHMfE6Qxk/1ren59rtckYpygz7/VdcNAhgcoLoIHRoJFTLwONMF
MTt1kW1cNXTSBT//s5jTYOfba7qck1HpSRTPdWOHwajnoyH9t/I/JnFdtJJu3IQN
qnA9G3pQdoi/J3Nug2CNKrSLJutBtTAmLQsJjUlmwg4MvcxpWURATNOWnnGAhuX1
t694QVI8owZ+bycidUjGSmdr3GUQ4i6/97sdeQIDAQABAoIBAEHVle/xDVfwnM3k
bBgRzsRetwJ3VnA5nBtqOlK6RIiavE61JOPK/FKoVjIQAUsKGfOtFeI6sSKr+Ez8
iBn2Eayr4SzaJAuEOznQ7QvzQlbcm/ji5wd/lDGmGFmtzVjmj6CxYE+y5siggfgx
woxKL4l2Jl3jDsy7q6G2hQ7Q72dzvtlEFRBaZvBdQ5LjPCrnZxzQBZGXCMU5/ro9
IwwlXzpKUce0IDG27WqpSFa7DSzwouq8gSkIGNxe643pBGFJYLoz4+00DyFiaete
izqNh9ulhgrwu6AVwO/Mtl5icSdPZgtgQ6Az1/tcT5y89zKyaNHEtXho5jiOvlPi
+iYCyuOCgYEA5jJXHAxcdMzDBsjUln8D1nYr87CSac7DEG4Oo2S1fBL93rUe62Cu
cPuyy8goFFKtmbxdl1dZtxmQww+VMWxZ8jBsH81VexqgkiYgTy1dde/Ih6v94CcU
nFiouWU92BRWt7zf3y6AhrR2bLfUCBrNqscdPCS7QuYKkPlwiCjzUNsCgYEA2rUK
w8u3dOpFEsJYttxv1BHSLVlBN7wsACo2RC9qkevEPAcjMmSCzJpgiA6JpwMlZa9b
AfU1zACtkHkW7gd8Xb7HOJkCpH4FN+YO9SxEWuE/XetznrV4vobPJbzzHHDG7cUb
jvaYcDM6UUQSLPXlUp5RWuwnMAc6FdVJqKT14TsCgYEA1LuO3v/ZbaNRVHLCa7ZD
wK0Cnzj9hcSrZgKfioZmZZxTer4dLd7yNr2UlViLGYTyo9F9GICEC38X1fwPn1YH
pZb0RUuIBLUt0QJk92bwKS6IPkFG5CCZnoccngCe75KUNUbaCTG7W0Fo873KuBa1
HG7YaJ11ZTScbS/nvB1EBuMCgYAXddAUpLebbjYWmw5VHzRHtVmsT6S1S9QUeHK1
wbhWysmT/tgBsdJuDClKrvSJG8dJLxQ+E4WfynrTwol5IwhuLebE5XTpHDOHGYCF
QChc70iS1IzkfBlkpqVV0PzrEhXkr34TSdR0RKp+ySSB+iaNRDpJ3IcfmcbbTLPI
CVnuvQKBgCpS6uxdhXJMd6Wgeutq9gQOQ8Og+VtMWHmIuEXvW9oth+jCKTRmuz3W
S7MgNuljPctusLig+exnUG8fxy467lCk7nAgslDrozGjPpix2BZF5AhuoCwCklwc
3LWF4AnRW4VgcUSTBSzEIOsDai/4oqbz65Ry2ZpXYzn5jpQfQQsc
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIID4TCCAsmgAwIBAgIJAJMjatDg7g/aMA0GCSqGSIb3DQEBCwUAMIGcMQswCQYD
VQQGEwJVUzELMAkGA1UECBMCTOgxDzANBgNVBAcTBkF1cm9yYTEhMB8GA1UEChMY
TmV0d29yayBUZWNobm9sb2dpZXMgSW5jMRQwEgYDVQQLEwtFbmdpbmVlcmluZzEP
MA0GA1UEAxMGTlRJIENBMSUwIwYJKoZIhvcNAQkBFhZqdXN0aW4uZmVycmlAbnRp
Z28uY29tMB4XDTE4MTIwMzE4MzkzNloXDTIxMDkyMjE4MzkzNlowgaIxCzAJBgNV
BAYTAlVTMQswCQYDVQQIEwJPSDEPMA0GA1UEBxMGQXVyb3JhMSEwHwYDVQQKExhO
ZXR3b3JrIFRlY2hub2xvZ2llcyBJbmMxFDASBgNVBAsTC0VuZ2luZWVyaW5nMRUw
EwYDVQQDEwwxOTIuMTY4LjMuNzExJTAjBgkqhkiG9w0BCQEWFmp1c3Rpbi5mZXJy
aUBudGlnby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDEqakV
+9ZsnKZI/Y+iz/40gNC+aghTjG/YUFkG7Stz65Ep/UPLZV4UqUy5+nYlcxPFIdcI
6PJmBVUQf2NvVU5FTpZHPb/pUbmFgOovrx2m0L1gnZLJFRrpJPRvBJkIIcx8TpDG
T/Wt6fn2u1yRinKDPv9V1w0CGByguggdGgkvMvDQ0wUxO3WRbVw1dNIFP/9LmNNg
59trupyTUe1JFM91Y4fBqOejIf238j8mcV2Okm7chA2qcDObelB2iL8nc26DYI0q
tIsm6OG1MCYtCwmNSWbCDgy9zGlZREBMO5aecYCG5fW3r3hBUjyjBn5vJyJ1SMZK
Z2vcZRDiLr/3ux15AgMBAAGjHjAcMAkGA1UdEwQCMAAwDwYDVR0RBAgwBocEwKgD
RzANBgkqhkiG9w0BAQsFAAOCAQEAFM6WKCwdU1ARIKc8tM4bI9GmA7VEC+69CgCo
GkiZ4WBEYfibc265uH7Lz+/z88rdflXW9B5Xc2B2GCzCxPYIwLcHfZpxbf6C7kp2
bs2OHzvCTGluVwm+r51bjmqQZzUQVH5vMZP8ct7HbOZbhtc6KwFRFIW5CZSu1qhn
tfxBEFiQGaR7wNTuEk9B4LJ3ghSNBYC+gPXOCDQSK3taXq1uA5fx08/6QBULQgbA
FzosbstNc7INpqtK9OZUOtwO3HAnr+gZJb3i4XQK5BReUlCLhlKy6X36Px4hf1rh
rf6da7kDfkC0g3x6B1EJzR/Cmazfmutd/AKKpvFT25YKE78jMQ==
-----END CERTIFICATE-----
```


## 5. Accepting a Self-Signed Certificate Authority as Trustworthy

### How to add a Self-Signed Certificate Authority as a Trusted Root Certification Authority on Windows

The browsers must recognize and trust the Certificate Authority created. The following are directions for trusting the newly created CA.

1. Open “Internet Options” in Control Panel
2. Navigate to the “Content” tab.
3. Select the “Certificates” button.
4. Go to the “Trusted Root Certification Authorities” tab
5. Press “Import”
6. Navigate through the prompt. The only option that will need to be modified is selecting the certificate to trust.
7. Restart the preferred browser.

### How to add a Self-Signed Certificate Authority as a Trusted Root Certification Authority on Mozilla Firefox

Mozilla Firefox does not use Window’s Certificate Authorities. For the Firefox browser to recognize your CA, do the following:

1. Open the Mozilla Firefox browser.
2. Type “about:preferences#privacy” in the URL field of the browser.
3. Under “Security” in the “Certificates” section, press the “View Certificates” button.
4. Navigate to the “Authorities” tab.
5. Select “Import”
6. Find your self-made CA and press “Open”

7. Select “Trust this CA to identify websites” and click “OK”.
8. Restart the Firefox browser.

**Note that some of these directions may be slightly different for older versions of Firefox.**

# II. Using External CA Signed Certificates for ENVIROMUX Series Products

## 1. Creating a certificate signing request for External Certificate Authority

A Certificate Signing Request must be provided to an external Certificate Authority like DigiCert, Verisign, or Comodo.

The Certificate Signing Request should be made using the following command:

```
# mkdir thirdparty
# mkdir thirdparty/certificates
# mkdir thirdparty/keys
# openssl genrsa -out ./thirdparty/keys/server.key 2048
# openssl req -sha512 -new -key ./thirdparty/keys/server.key -out
./thirdparty/certificates/server.csr
```

Below is an example of a valid certificate signing request:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDGzCCAgMCAQAwgawxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJPSDEPMA0GA1UE
BxMGQXVyb3JhMSEwHwYDVQQKExhOZXR3b3JrIFRlY2hub2xvZ2llcyBJbmMxFDAS
BgNVBAsTC0VuZ2luZWVyaW5nMR8wHQYDVQQDExZ3d3cubmV0d29ya3RlY2hpbmMu
Y29tMSUwIwYJKoZIhvcNAQkBFhZqdXN0aW4uZmVycmlAbnRpZ28uY29tMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzc1BU6EbJL4hNYj9UfM2EO2qzTHr
c/OUL8kaoZZyExpnK3ekrlGWSTciV3hP4ZY+AlxuYOP5pzWWnIGXzBHgw0XybIgM
/IraRiEzrh8jw+kKUCjcBhP1DQXES7EhX1MDoNyTVEaIXF5Ya8RWJMxisrd4VTfc
eCm3zgUq1HN4rmY4Uj4EN7fsDrT2QppClPKvFiFaFdwAsi7GXA8q2Gffx5mfhPiw
yb5qAPPx78f6wTYk/MeasUDVDC5DHlOL87MfYkMLhc+1tLIOxUSKu0NJYczuC/gO
OAuk+khgkH5gau9t83lCThEI6OkHswNR8P9eHSHTOoOU9XfuOywmpL6ByQIDAQAB
oCkwJwYJKoZIhvcNAQkOMRowGDAJBgNVHRMEAjAAMAsGA1UdDwQEAwIF4DANBgkq
hkiG9w0BAQ0FAAOCAQEAqQ2Es1PHsBrPIDwCLZ/9+4hTCcgTyIXBb6A7TmvLmnzF
JcyC7/78np+jGbhSMbM9Pgh6DJpcTuIgSSDlwzP9JJLGq+SjKn3Lm6tScGCz7YYT
cf6VFtPyCP5GkNVqfZfTApKESj4OtIqM/gVyByQzD1CFL4FIGhRrYXpbbGpoBpj/
C9S1FZT5XjuS/ixbKm/O6GwzO6H6US8PAFMtViSHaOg6i9nhIBWUg7OeOjwBdnTb
JaQpAIF3OrTbQ/iKgXzYb4L9bowExyvP/DldOx7vG9egbi4WJjjIhuOssxFb7Q1J
ODh+Cc7uALD5PhLaUgglhi8a1IgtlIuiPlB1UztZcg==
-----END CERTIFICATE REQUEST-----
```

Upload your CSR to your Certificate Authority to get the certificate.

## 2. Uploading Server Certificate to a ENVIROMUX Device

The NTI ENVIROMUX device expects the certificate and key as a single file in "PEM" format.

The server certificate file with extension “pem” should be received by your external CA after submitting a certificate request. Get your server certificate in a .pem or .cer format. Copy your server certificate into another file and add the device key as shown below.

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAyQ1pnlRkr3r4wlCJi0jYrFW2+bXqv6WrotMyGfIRZaZkLo5J
1whYb/uFcX2Unc/H5X7wDa3gawr6iJki/dVf8X16gpHicrWR+WFAiRs/D7z+B/ew
iaM5vqDMTw5mvAmnNaOsZ3gsOnSEFgiZMewkimJYyyfHjHv2kpW51HekWraa8dVJ
dunAhzeTTcDghxhT2p2hsKxARB5m4DOvjv2aEcxnRixxvDA/2uggxfXJil8SCpAk
qxiJzeqPv+xRvp/jTpI1wlGPmuemJILGs95iFOv8WpUFM3xDR3o8GCuOl8eokEEA
lpWNgiRuQcjjh464z8rbr8lO+FJP0AhEJ7XufwIDAQABAoIBABStQHN8Em7JotO5
HKwqBb4rgonj36SeESzJs5lff9KIbjOrfQSUYyQBJhQp6iLgv5oml+GQREg99M4f
ka2xSBC56uOKxVMuwTh4e/6dwrqHoUiIfKtrEgE84EYxIPettniZwJ1Tipjoar0p
XTf5JTjmLGOYT7lu9kjVBSuIsmpxtn8xNu1po5l1zY/Soy3p38qTKwNJ1n9CnJXo
q9LTnfiGvq7JfRhjHFx4AYKJsZMNE4ZI4WEr4B72wxifpINr0llk0ezrKn5UB+Ug
8nXONonxAlotv7McIM+u4cjv8ww3yTb7Mw5isAS9zeS9eN5ticLLh5yFFJyYKai6
e2HgpEECgYEA7XY94+z2Xy48z5ogQErgHCwFv7wWP6kUObJGkITCygP0N5jqKSuo
pprtpr4gpvH8V78krPASsdXrmm3UyVmrK5z89T0SQMnSls6HX+vfVsHVxmKW3Wa6
BChtA2+YsHPtpFeAYK/rUxh/3rRblFOpTfpiHpmYEWNOwyXT2Jg2HPcCgYEA2L+D
t6HvFnscOdcr1kE2VGEmLgD6ll2eUBp3/6+MrAqgdVqaaBgxuv57sWNS7Ys4Fv7V
EioI/CwDcB4uIIK4mbenW39uu2OZAGceNXOmdOsg97Vxs7GR76tyC9irei6u0HX2
ySpb5L8cB1PevTP058GHVjqhKmSrzQx/URx9ALkCgYEAyhZc6YKa0bnp6svCMrUG
MTON2O9S5O6h1dBQmWFC3OWsizxJ26vaJZ+oLMWVyD4cgRicv8i4QDxL++sIsirr
r3w1EwhcZmLcI5e0Qf/c3Fqt8d2pgtaP7EXzMH9itJiUX85P5PkSDm/FMuTPI1Zn
uYMiyePxNKsNNqsUtToko1UCgYAsRWHX/iFhjB/FyKdRNORt87Hir5x/XfvaDK35
8ZdgBIOltK3ZGSf/M798CfeEQW1hdQd8QE25hBvnqKJvTYP7EcIDNFIfwEYeCPHo
pQiY1PXU4qCovVo7g981gDn2KNbYCWAw0pAWdtp4vK7AIn6hX6wO9sa4a/uTVDwl
CxaVMQKBgFhJvBHD9cKY41kMTYHvNPaXmJAtWlEBMyVkFWAtz+e4C+ojzyLuI34e
TPkk8ivxeZO0c8X241dIBZKbwCLnV3TprvA2UeMui5LjyU0H4AEnzan1H4S2G+Rz
gWWEFZmTlg0R7f7H9uBPpoNjnJzhsAMkBAVgwPJvY6PyoPP0tglR
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDazCCAlogAwIBAgIJAMib9H5kqNSpMA0GCSqGSIb3DQEBCwUAMFkxCzAJBgNV
BAYTAlVTMQswCQYDVQQIEwJPSDEMMAoGA1UEChMDTlRJMQ8wDQYDVQQDEwZOVEkg
Q0ExHjAcBgkqhkiG9w0BCQEWD3NhbGVzQG50aWdvLmNvbTAeFw0xODEyMDQyMDA1
MzhaFw0yMTA5MjMyMDA1MzhaMHExCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJPSDEP
MA0GA1UEBxMGQXVyb3JhMQwwCgYDVQQKEwNOVEkxFjAUBgNVBAMTDTE5Mi4xNjgu
My4xNDQxHjAcBgkqhkiG9w0BCQEWD3NhbGVzQG50aWdvLmNvbTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAMkNaZ5UZK96+MJQiYtI2KxVtvm16r+lq6LT
MhnyEWWmZC6OSdcIWG/7hXF9lJ3Px+V+8A2t4GsK+oiZIv3VX/F9eoKR4nK1kflh
QIkbPw+8/gf3sImjOb6gzE8OZrwJpzWjrGd4LDp0hBYImTHsJIpiWmsnx4x79pKV
udR3pFq2mvHVSXbpwIc3kO3A4IcYU9qdobCsQEQeZuA9L479mhHMZ0YscbwwP9ro
IMX1yYpfEgqQJKsYic3qj7/sUb6f406SNcJRj5rnpiSCxrPeYhdL/FqVBTN8Q0d6
PBgrtJfHqJBBAJaVjYIkbkHI44eOuGfK26/JdPhST9AIRCe17n8CAwEAAaMeMBww
CQYDVR0TBAIwADAPBgNVHREECDAGhwTAqAOQMA0GCSqGSIb3DQEBCwUAA4IBAQBd
CNA7H/4DeYR7Oj13yOmN9ajgRU5XbzETNA1Cr+3w+2YUaJ4cAOdo/e9TLwhTC1pH
E1HKrkFyjag5JEE32PT/Pn+gb++/2U94jw7qatqrcwiboy7ytJCzgEKYOEPjvfUJ
fS1saVbgWmQMGA0LuRr2NLLU9vCYlTpeeTGyC/ve5k3rjOYFACQL5rKa9D7Vgn6r
IwTU13uwvDxP7QzvkgjKuEJkWlg2DlMS3bw2ejAOc9HAl8RCROxm55Z7maRqeLzJ
GLbf3587pCZMQIu21YU9DJ/7ORSN1xdyKQG4KNfOxMHkmuAafqIFp+d8D+3xtVSw
h94zxQI77VarHxLswk3e
-----END CERTIFICATE-----
```

On the ENVIROMUX Web Interface menu Under “Administration” select “Network”. In X509 certificates, select “Choose File”, select the combined server certificate /key file, click **"Upload Server certificate and key"**.

### 3. Uploading External CA Certificate to ENVIROMUX Device:

```
-----BEGIN CERTIFICATE-----
MIIDtjCCAp4CCQDy25JKAce+dDANBgkqhkiG9w0BAQ0FADCBnDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAk9IMQ8wDQYDVQQHEwZBdXJvcmExITAfBgNVBAoTGE5ldHdv
cmsgVGVjaG5vbG9naWVzIEluYzEUMBIGA1UECxMLRW5naW5lZXJpbmcxDzANBgNV
BAMTBk5USSBDQTElMCMGCSqGSIb3DQEJARYWanVzdGluLmZlcnJpQG50aWdvLmNv
bTAeFw0xODEyMDMxODE1NDZaFw0xOTExMjgxODE1NDZaMIGcMQswCQYDVQQGEwJV
UzELMAkGA1UECBMCT0gxDzANBgNVBAcTBkF1cm9yYTEhMB8GA1UEChMYTmV0d29y
ayBUZWNobm9sb2dpZXMgSW5jMRQwEgYDVQQLEwtFbmdpbmVlcmluZzEPMA0GA1UE
AxMGTlRJIENBMSUwIwYJKoZIhvcNAQkBFhZqdXN0aW4uZmVycmlAbnRpZ29tMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtUVXiaF44xtBRQ6if1Ch
evpmQJfxHyQL8KtnGXgAuWk1KNp+3S1culYzlHgMSJU//W/srqnoPh6DmkokhB/r
qYt4KbdeC7t8w4oNX4ltdJzO+7chBBqvoN7DYLS45/OIrTLpaHnbBJPhxsFEREWU
hW1iX14SgTw40X49EfPJdGshORMAEsqwk37JddX440ALrjLcEI82Rv4Mb8EV9oJ8
JyulpWHqfuRVMCn3X/yzHiEP7Dql7nrFjAM8OhmlOJxHizAZQRdqfqHGO09zgrct
qJOQVLMW8amWFn2l3DAzSQdJOrFl1zOx7D2zlBkTYm7gr1E7mzR12uAOfl5OwqEL
2wIDAQABMA0GCSqGSIb3DQEBDQUAA4IBAQBxkTZ3oR7eRLv+Q5U2a4iNj6l/UkW9
loHhu9YtMOpijt/CUeD4q3Cu56i6JNyru4of7Q4ZUSU+jTXxWhh2QCb0+eF+LMEC
NnF/J26pfXQNh3OmQ1KRLq6EpZ5DedSbrRTB/lEO5zm/ChOyY7bOizp/B8+AY4Id
/AU63BULTN2tRL4doNcbEcCtS37YRdRZTJF85es9qlfTKVA4mBYjE5p9bgDzHCdQ
Xliuv5fiELp3O7y7NNLtO9nVRrbzS9YHHmmJORP4j7SPaAxveyFfz93LuQn8kKlw
0dzroXCmGuMVPDilq1Z2ORZVDNw9+AZvk7/lH++EguB5p7y5aP7zpEfN
-----END CERTIFICATE-----
```

Get the certificate of your CA in a *.cer or *.pem format which should be as shown above. Optionally this file may include an intermediate certificate, which would be different from the above root Certificate, in the same file. On the ENVIROMUX Web Interface menu Under “Administration” select “Network”. In X509 certificates, click “Choose File”, select this CA certificate file, and click **"Upload CA certificate"**.

## III. Creating a Client Certificate for ENVIROMUX Series Products

The procedure for creating a client certificate is similar to that for creating the web server certificate.

### 1. Creating a user key

The following instructions create a private key for a user named your_name@example.com. When prompted for the pass phrase, enter a password that you can remember.

```
% cd /usr/local/ssl/ntiCA
% openssl genrsa -des3 -out ./user/keys/your_name@example.com.key 2048
Generating RSA private key, 2038 bit long modulus
...++++++
.....++++++
e is 65537 (0x10001)
Enter pass phrase for ./user/keys/your_name@example.com.key:
Verifying - Enter pass phrase for ./user/keys/your_name@example.com.key:
```

**NOTE: When entering the password, the characters will not be displayed and there will not be an indication of what you typed in. An error message will be printed if you do not type the same password in both prompts.**

### 2. Create the user certificate request

1. The following command creates a certificate request for a user with email address: your_name@example.com and common name your_name. When prompted for the pass phrase for the keys in file ./user/keys/your_name@example.com.key, enter the pass phrase that you used to create the user key (e.g. “password”).

```
% openssl req -sha512 -new -key ./user/keys/your_name@example.com.key -out
./user/requests/your_name@example.com.csr
Enter pass phrase for ./user/keys/your_name@example.com.key:
```

```
You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:US
  State or Province Name (full name) [OH]:OH
  Locality Name (eg, city) []: Aurora
  Organization Name (eg, company) [NTI]:NTI
  Organizational Unit Name (eg, section) []:Engineering
  Common Name (eg, YOUR name) []:your_name
  Email Address [ca@ntigo.com]:your_name@example.com

  Please enter the following 'extra' attributes
  to be sent with your certificate request
  A challenge password []:
  An optional company name []:
```

2. Sign the user certificate request and create the certificate

```
% openssl ca -in ./user/requests/your_name@example.com.csr -cert ./CA/ntiCA.crt -keyfile
./CA/ntiCA.key -out ./user/certificates/your_name@example.com.crt
```

Make sure the following line is in your **openssl.cnf**:

```
unique_subject = "yes"
```

If it is not, you should add it on a separate line using any text editor.

### 3. Check that the request matches the signature

```
Using configuration from /usr/local/openssl/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'US'
stateOrProvinceName   :PRINTABLE:'OH'
localityName          :PRINTABLE:'Aurora'
organizationName      :PRINTABLE:'NTI'
organizationalUnitName:PRINTABLE:'Engineering'
commonName            :PRINTABLE:'your_name'
emailAddress          :IA5STRING:'your_name@example.com'
Certificate is to be certified until Dec  7 14:52:08 2038 GMT (7305 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
```

If you receive an error message like the one below, you still should not have issues with signing the certificate. The index.txt.attr file will be generated.

```
Can't open /usr/local/ssl/ntiCA/index.txt.attr for reading, No such file or directory
3079379152:error:02001002:system library:fopen:No such file or
directory:crypto/bio/bss_file.c:74:fopen('/usr/local/ssl/ntiCA/index.txt.attr','r')
3079379152:error:2006D080:BIO routines:BIO_new_file:no such
file:crypto/bio/bss_file.c:81:
```

### 4. Verifying the user certificate contents

To verify the user certificate contents, you can use the following command:

```
% openssl x509 -in ./user/certificates/your_name@example.com.crt -text
```

## IV. Creating and Importing a Client Certificate for ENVIROMUX Series Products

Web browsers like Firefox and IE can't use the certificates in the PEM format that is generated by OpenSSL . Consequently, we'll need to export the user certificate to file formats that can be imported by web browsers.

### 1. Generating the client certificate in PKCS#12 format

Firefox and Windows support the PKCS#12 certificate format. Use the following command to convert the user certificate to this format.

**NOTE: During the conversion process, you'll be asked for an export password. Enter anything you can remember, but don't let it be empty because the file will contain your private key.**

```
    % openssl pkcs12 -export -clcerts -in ./user/certificates/your_name@example.com.crt -inkey
./user/keys/your_name@example.com.key -out ./user/certificates/your_name@example.com.p12
        Enter pass phrase for ./user/keys/your_name@example.com.key:
        Enter Export Password:
        Verifying - Enter Export Password:
```

Copy the `your_name@example.com.p12` file in the /usr/local/ssl/ntiCA/user/certificates directory to a location where you can access it from your web browser via the file system.

### How to Import a Client Certificate on Windows

The browsers must be able to access the client certificate created. The following are directions for using the newly created client certificate.

1. Open “Internet Options” in Control Panel
2. Navigate to the “Content” tab.
3. Select the “Certificates” button.
4. Go to the “Personal” tab
5. Press “Import”
6. Follow the wizard instructions to select the certificate file
7. Enter the password you used to protect your certificate and private key
8. Import the client certificate into the Personal store.
9. Enter the password you used to protect your certificate and private key
10. Click the imported certificate and then on the View button in the Certificate intended purposes group box. Click the Details tab and then the Edit Properties button. Make sure that the Client Authentication option is checked.

Next time you try to access the ENVIROMUX Web Interface, you will be prompted to use the client certificate.

**NOTE: You will also have to import the CA that was used to sign this client certificate.**

### How to Import a Client Certificate on Mozilla Firefox

The Mozilla Firefox browser does not use Window’s stores to use and trust certificates. The following are directions for trusting the newly created client certificate.

1. Open the Mozilla Firefox browser.
2. Type “about:preferences#privacy” in the URL field of the browser.
3. Under “Security” in the “Certificates” section, press the “View Certificates” button.
4. Navigate to the “Your Certificates” tab.
5. Select “Import”.
6. Make sure you are looking for the correct file type (in the dropdown next to the file name field, the file type should display something that accepts (*.p12) files.
7. Find your client certificate and press “Open”
8. Enter the password you used earlier to generate it and click “OK”.
9. Restart the Firefox browser.

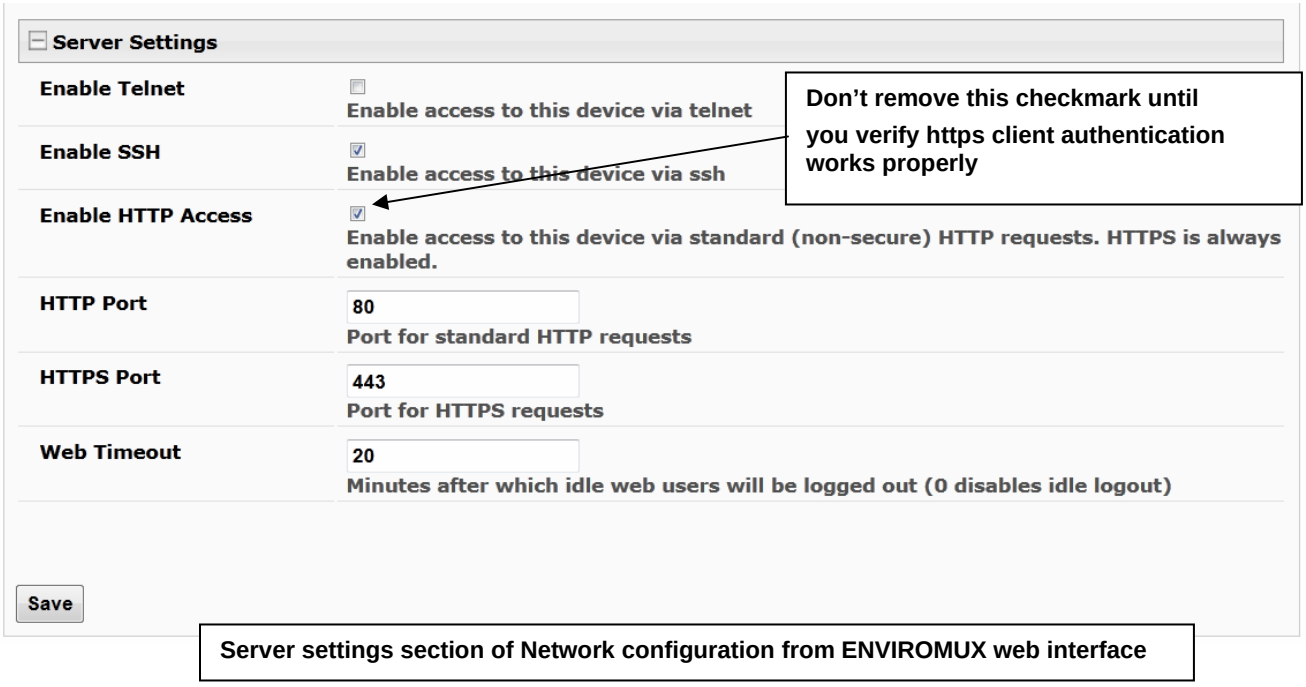
Next time you access the ENVIROMUX Web Interface, you will be prompted to use the client certificate.

**NOTE: You will also have to import the CA that was used to sign this client certificate.**

## V. Configuring an ENVIROMUX Device to Require Client Certificate

On the ENVIROMUX Web Interface menu Under “Administration” select “Security”.
In X509 certificates select the file `ntiCA.crt` and press button "Upload CA certificate".
Select “certificate + login” in the "Mode" field under “User Authentication” to enable the device to ask for a client certificate.
Use https communication.

**Note: Before disabling http be sure to verify https client authentication works properly.**




Server settings section of Network configuration from ENVIROMUX web interface