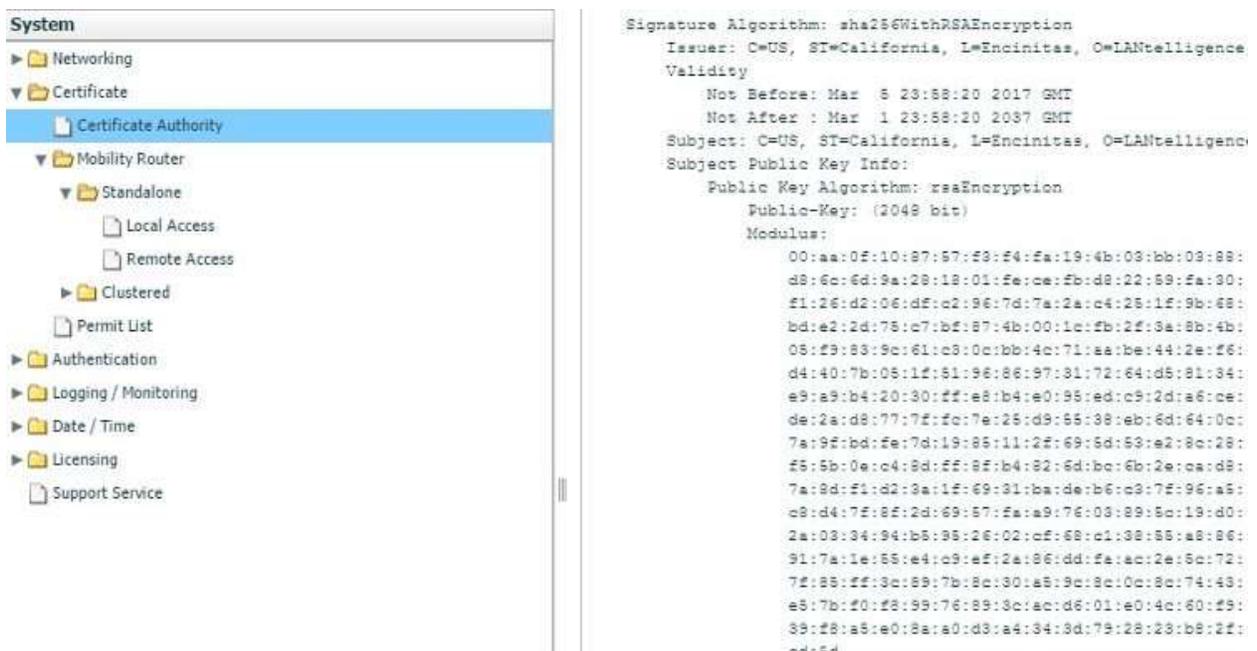


# How to import certificates into ShoreTel Mobility router

Importing certificates into the Mitel (ShoreTel) Connect mobility router is easy if you complete the steps in the right order. In fact, it is faster to do it yourself than waiting on the ShoreTel support line. Read the detailed explanation below and we guarantee that you will succeed.

## Step 1

Create the certificate authority. You will have to generate a self signed certificate authority. Do not use the root CA from your vender here.



The screenshot displays the configuration interface for a ShoreTel Mobility Router. On the left, a tree view under 'System' shows the 'Certificate' folder expanded to 'Certificate Authority'. The 'Certificate Authority' folder is selected and highlighted in blue. Below it, the 'Mobility Router' folder is expanded to show 'Standalone' and 'Clustered' options. The 'Standalone' folder is further expanded to show 'Local Access' and 'Remote Access' options. The 'Remote Access' option is selected. On the right, the configuration details for the Certificate Authority are displayed, including the Signature Algorithm, Issuer, Validity, Subject, and Public Key Information.

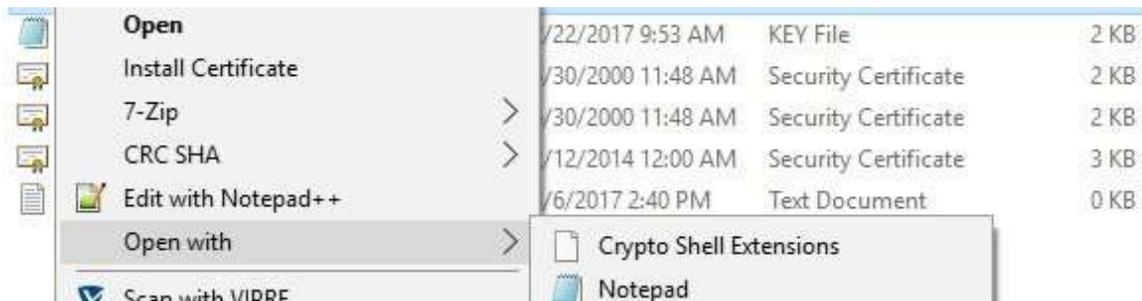
```
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, ST=California, L=Encinitas, O=LANtelligence
Validity
  Not Before: Mar  8 23:58:20 2017 GMT
  Not After : Mar  1 23:58:20 2037 GMT
Subject: C=US, ST=California, L=Encinitas, O=LANtelligence
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  Public-Key: (2048 bit)
  Modulus:
    00:aa:0f:10:97:57:f3:f4:fa:19:4b:09:bb:03:88:
    d8:6c:6d:9a:28:18:01:fe:ce:fb:d8:22:59:fa:30:
    f1:26:d2:06:dF:c2:96:7d:7a:2a:c4:25:1f:9b:68:
    bd:e2:2d:75:c7:bf:87:4b:00:1c:fb:2f:3a:8b:4b:
    05:f9:83:9c:61:c3:0c:bb:4c:71:aa:be:44:2e:f6:
    d4:40:7b:05:1f:51:96:86:97:31:72:64:d5:81:34:
    e9:a9:b4:20:30:ff:e8:b4:e0:98:ed:c9:2d:a6:ce:
    de:2a:d8:77:7f:fc:7e:25:d9:55:38:eb:6d:64:0c:
    7a:9f:bd:fe:7d:19:85:11:2f:69:5d:59:a2:8c:28:
    f5:5b:0e:c4:8d:ff:8f:b4:82:6d:bc:6b:2e:ca:d8:
    7a:8d:f1:d2:3a:1f:69:31:ba:de:b6:c9:7f:96:a5:
    c9:d4:7f:8f:2d:69:57:fa:a9:76:09:89:5c:19:d0:
    2a:02:34:94:b5:95:26:02:cf:68:c1:38:55:a8:86:
    91:7a:1e:55:e4:c9:ef:2a:86:dd:fa:ac:2e:6c:72:
    7f:85:ff:3c:89:7b:8c:30:a5:9c:8c:0c:8c:74:43:
    e5:7b:f0:f8:99:76:89:3c:ac:d6:01:e0:4c:60:f3:
    39:f8:a5:e0:8a:a0:d3:a4:34:3d:79:28:28:b8:2f:
    ~4-~4
```

## Step 2

Open the Remote access certificate page.

## Step 3

The certificates need to be in a text file format. Right click the \*.crt and key files and open with notepad.



## Step 4

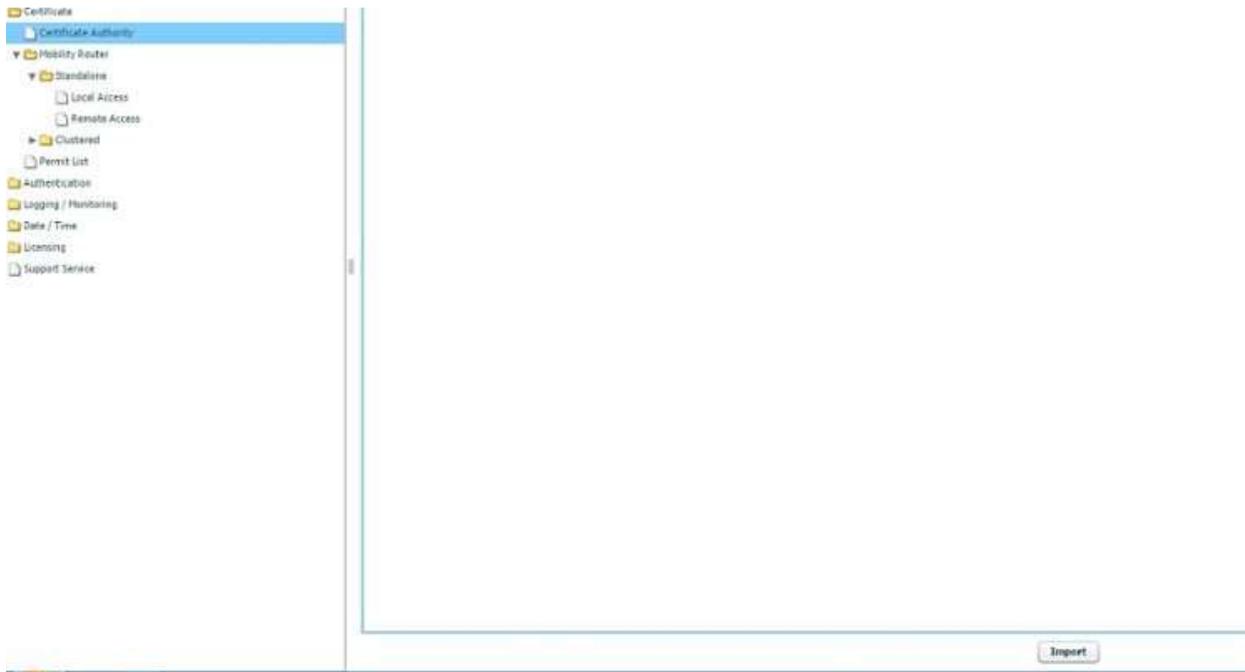
In a blank text file copy the notepad output in the following order. Please note you should copy from the dashes in Begin Certificate all the way to End certificate. The same for the private key.

- Certificate
- Private key
- Trust chain – This may be several certificates in the trust chain. In the example below from Comodo there are three certificates for this piece

Name	Date modified	Type	Size
1) STAR_intelligence_com.crt	2/22/2017 12:00 AM	Security Certificate	2 KB
2) PrivateKey.key	2/22/2017 9:53 AM	KEY File	2 KB
3) AddTrustExternalCARoot.crt	5/30/2000 11:48 AM	Security Certificate	2 KB
3) COMODORSAAAddTrustCA.crt	5/30/2000 11:48 AM	Security Certificate	2 KB
3) COMODORSADomainValidationSecure...	2/12/2014 12:00 AM	Security Certificate	3 KB

## Step 5

Select Import under the remote access page



## Step 6

Copy and paste the text file you created in here and select Import

## Step 7

Repeat the process for local access