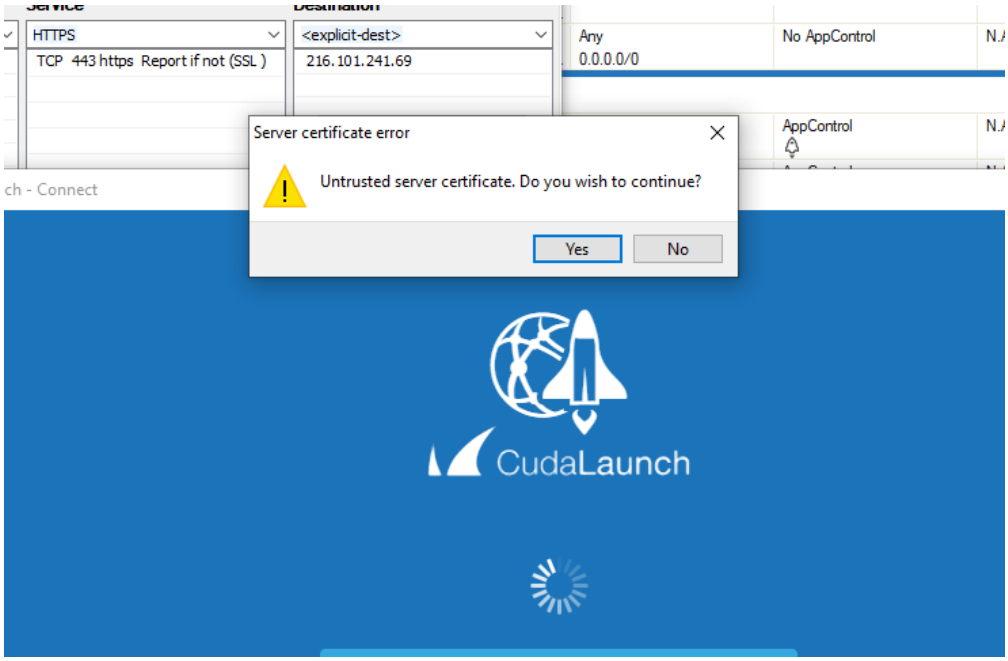
How to Use an External Certificate in CudaLaunch

https://campus.barracuda.com/doc/91987648/

In some cases, end users might receive an “untrusted certificate” pop-up when connecting to CudaLunch. To solve this issue, use an external certificate. If you already have a public certificate chain and key pair, you can just upload the correct certificate and key pair to the CloudGen Firewall. Otherwise, you will have to generate a CSR.



Generate an External Certificate

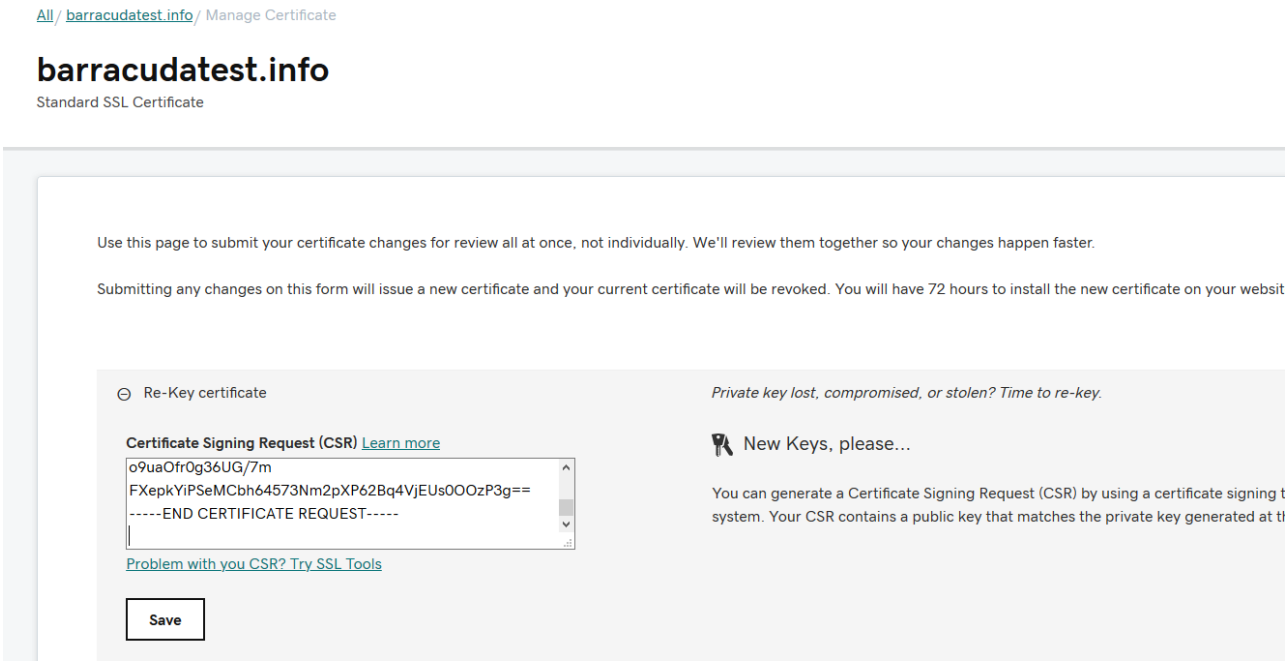
1. Log into the Barracuda CloudGen Firewall via SSH.
2. Use the following command to generate the CSR and the private key:
   - `openssl req -new -newkey rsa:2048 -nodes -keyout domain.key -out domain.csr`
3. Follow the instructions to add information to your CSR. Make sure to add a password to the private key.

   You can use the **`ls`** command once it has been created to view the files in the directory.

```
udatestinfo.key -out barracudatestinfo.csr newkey rsa:2048 -nodes -keyout barrac
Generating a 2048 bit RSA private key
.....................+++
.................................................+++
writing new private key to 'barracudatestinfo.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) [XX]:US
State or Province Name (full name) []:CA
Locality Name (eg, city) [Default City]:Campbell
Organization Name (eg, company) [Default Company Ltd]:Barracuda Sales Engineering
Organizational Unit Name (eg, section) []:SE
Common Name (eg, your name or your server's hostname) []:barracudatest.info
Email Address []:gabe@cudaseteam.org

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:barracuda
An optional company name []:Barracuda
[2020-04-28 18:57 UTC] [-root shell-] [-Barracuda Networks-]
[root@CudaLaunchTest:~]# ls
anaconda-ks.cfg        barracudatestinfo.key   machine
barracudatestinfo.csr  commitinstallation.log  original-ks.cfg
```

4. Use the *down* function to download the CSR and private key pair to your desktop.
   [down] **domain**.key
   [down] **domain**.csr
5. Open the CSR in a text editor, and copy and paste the output into GoDaddy or a similar provider.
   For GoDaddy, this section is located under **Certificates > rekey & manage**.



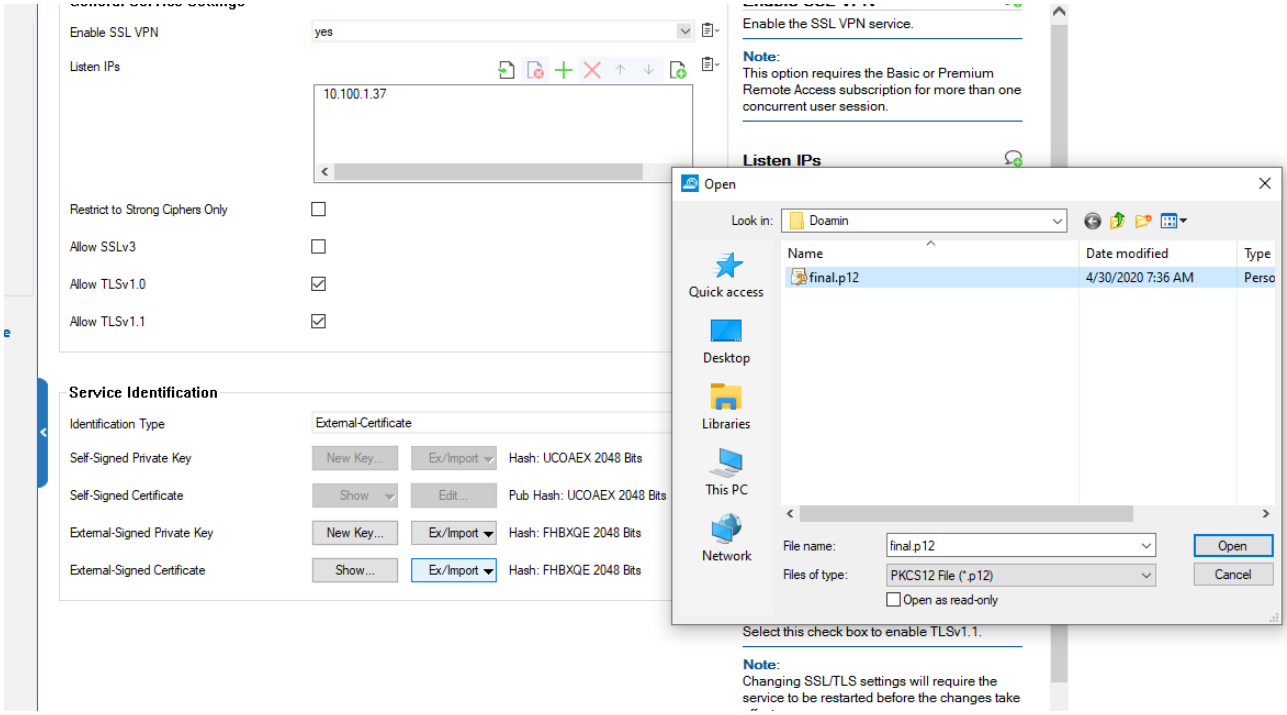
6. Wait a few minutes and then download the new certificate that matches the key pair you generated on the CloudGen Firewall.

Upload the Certificate to the CloudGen Firewall

Upload the certificate chain and your key pair as an external certificate. If you downloaded from GoDaddy, there will be a .crt bundle that includes all the intermediate certificates as an easy-to-upload package.

On the CloudGen Firewall:

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > SSL-VPN**.
2. In the left menu, select **Service Setup**.
3. Click **Ex/Import** and upload the certificate in the **Service Identification** section.



For more information on how to upload certificates, see How to Configure the SSL VPN Service.

Troubleshooting

If uploading the cert file and key separately does not work on the CloudGen Firewall, create a pkcs12 file that contains all the information: cert, intermediaries, and key.

1. Rename your key, certificate, and chain to PEM.
2. Upload key, certificate, and chain to the CloudGen Firewall through the console:
   Run the following command:

- `openssl pkcs12 -export -inkey domain.key -in certfile.pem -certfile bundleofintermediaries.pem -out final.pfx`

3. Use the *down* function:
   - *[down]* `final.pfx`
4. Rename `pfx` to `.p12`

Figures

1. cl_external01.png
2. cl_external02.png
3. cl_external03.png
4. cl_external04.png