GOAL

Create a certificate, get it signed by a public CA and upload it to the controller to avoid certificates issues when client is redirected to a captive portal. In this case the certificate will be shared by multiple controllers.

Step 1

Create the CSR externally. This method is only needed when the same certificate will be installed in multiple controllers.

In this step, you will need to download the CSR and the private key. i.e. you will use xxx.domain.com

Step 2

Get the CSR signed by a public CA

Step 3

Download the intermediate and the root certificate and combine them. I used openssl to combine the certificates.

```
openssl pkcs12 -export -out certificado.pfx -inkey privateKey.pkey -in CRT-I-GOT-SIGNED-FROM-PUBLIC-CA -certfile INTERMEDIATE-AND-ROOT-CERTIFICATE
```

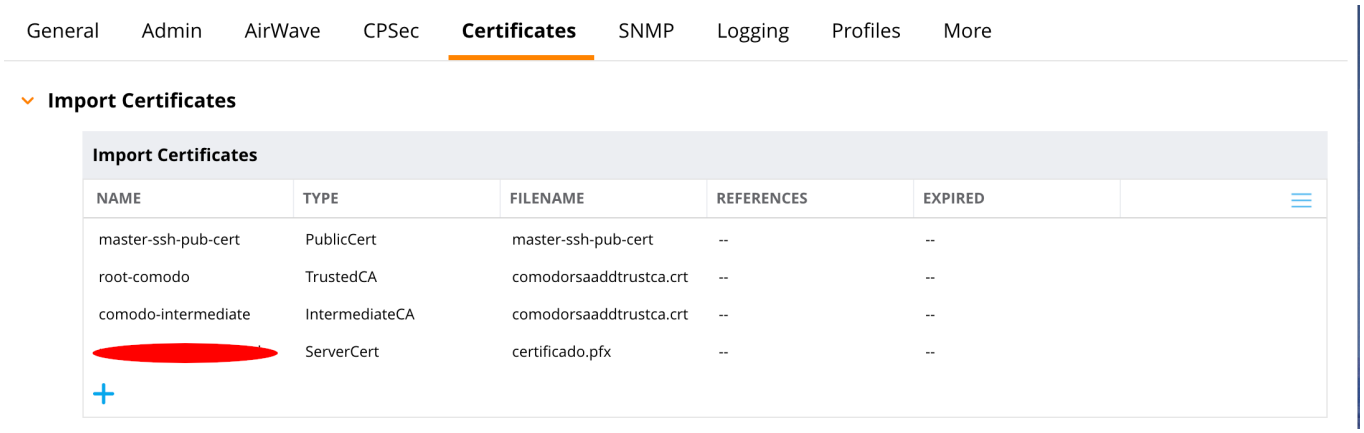
At this point I have the certificate I need to upload to the controller ("certificado.pfx").

Step 4

Upload the certificates to the controller.

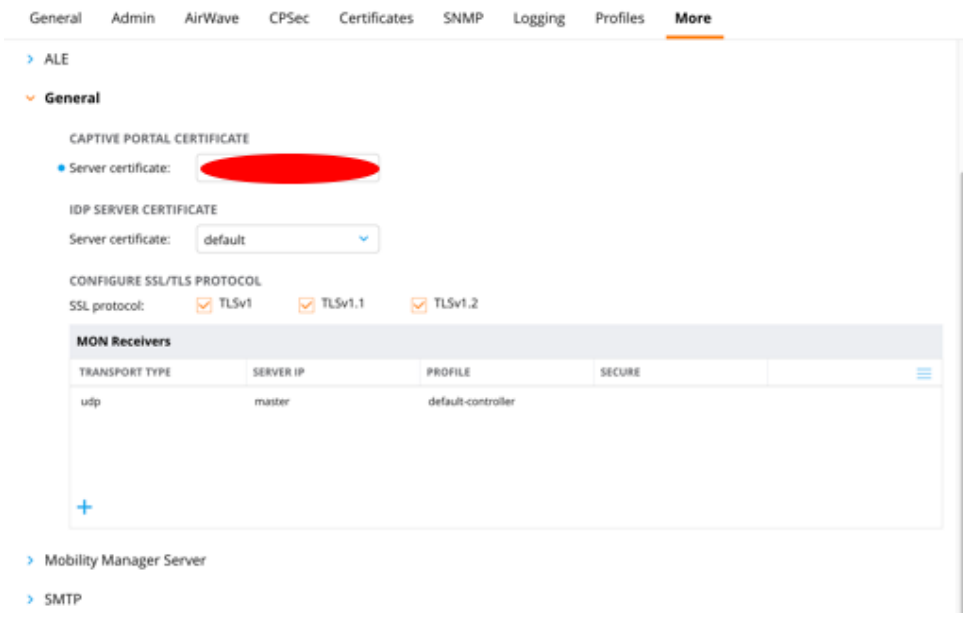
- Upload "certificado.pfx" as ServerCert.
- Upload the intermediate certificate as IntermediateCA
- Upload the root certificate as TrustedCA

3333 Scott Blvd. | Santa Clara, CA 95054
1.844.472.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | info@arubanetworks.com



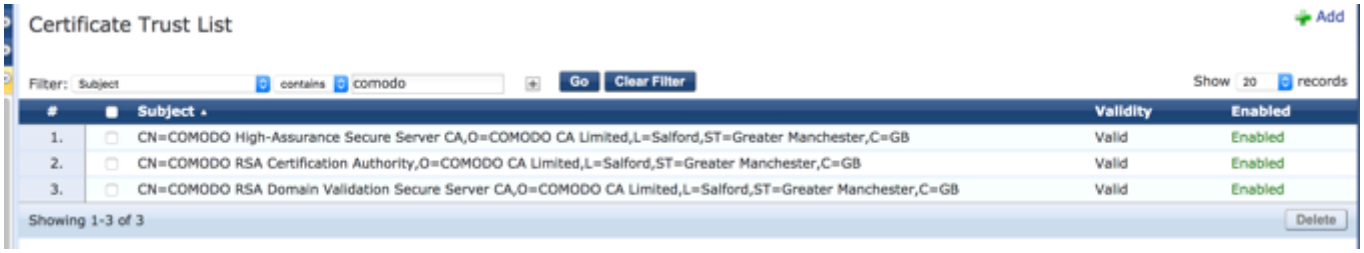
Step 5

Configure the certificate on the controller and save the config.



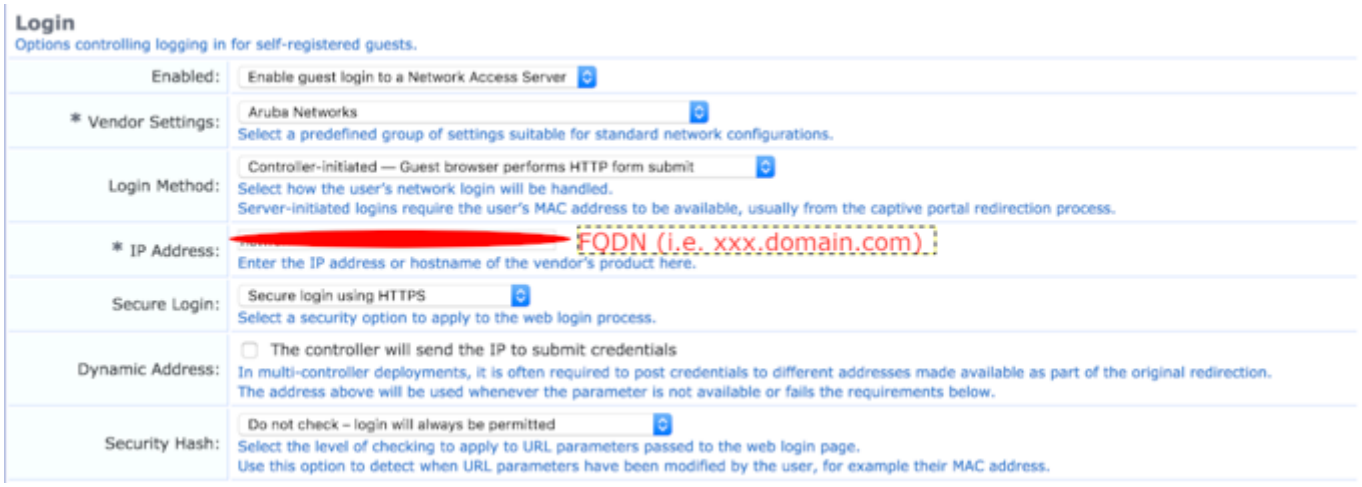
Step 6

On ClearPass the root and intermediate certificate should be uploaded and marked as trusted (In my case it is COMODO)



Step 7

Modify the IP address on the Guest captive portal page to the FQDN that has been created.



When the form is completed and the user hits the “Log in” button, the guest user will perform a HTTP post to xxx.domain.com.

Step 8

Test it.

Please note that an entry on the DNS has **not** been added. The controller will hijack the DNS request and will respond with its own IP address.

```
nslookup xxx.domain.com
Server:         10.10.160.10
Address:        10.10.160.10#53

Non-authoritative answer:
Name:   xxx.domain.com
Address: 10.10.150.210
```