

EAP-TLS Termination

**Termination of EAP-TLS on Aruba OS 3.1**

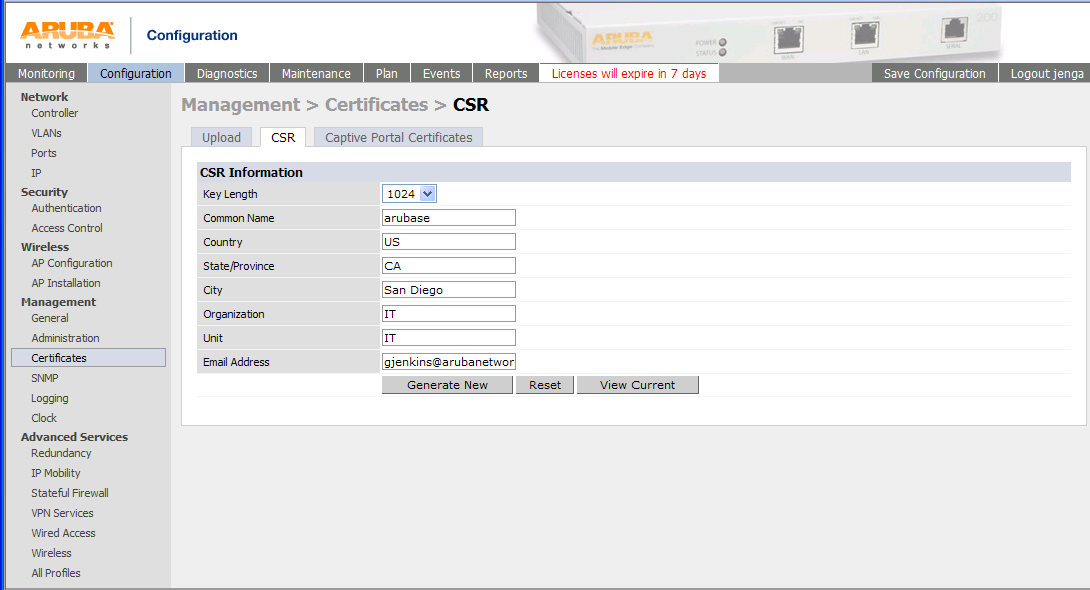
This setup for EAP-TLS termination was do with the following

* Aruba Controller running AOS 3.1 or greater
* Windows 2003 server running a Microsoft Cert Authority, IIS and acting as a Domain Controller
* Juniper Odyssey Access Client

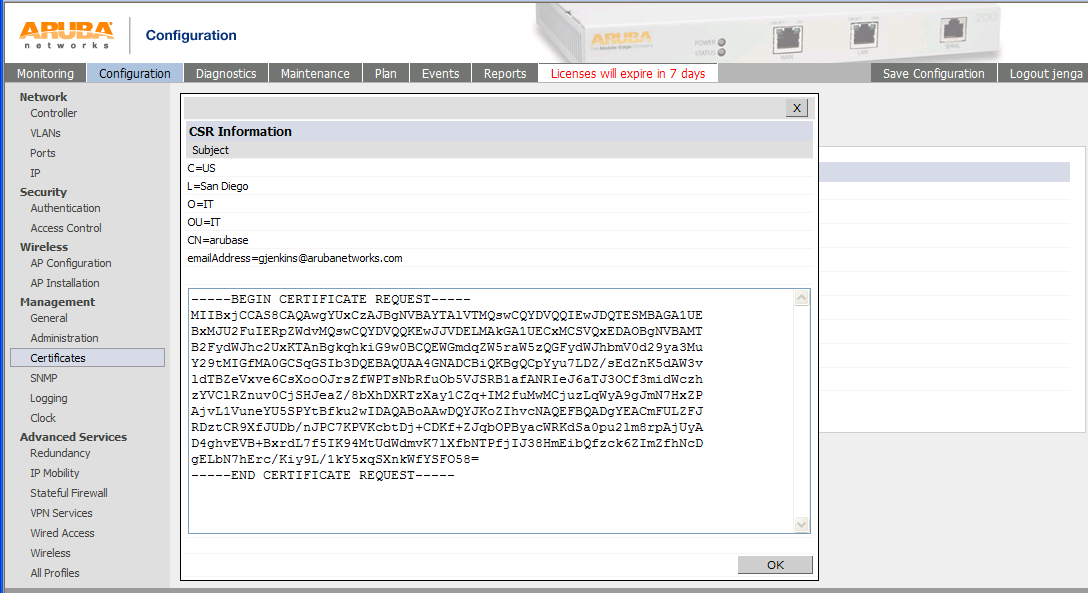
1. Certificate Creation
   1. Server Cert
   2. Trusted CA Cert
2. Controller Authentication Configuration
   1. Configure TLS AAA Profile
3. AP Configuration
   1. Add TLS Virtual AP
4. Client Configuration
5. Certificate Creation

You will need both a Server Cert and a Trusted CA Cert for EAP-TLS.

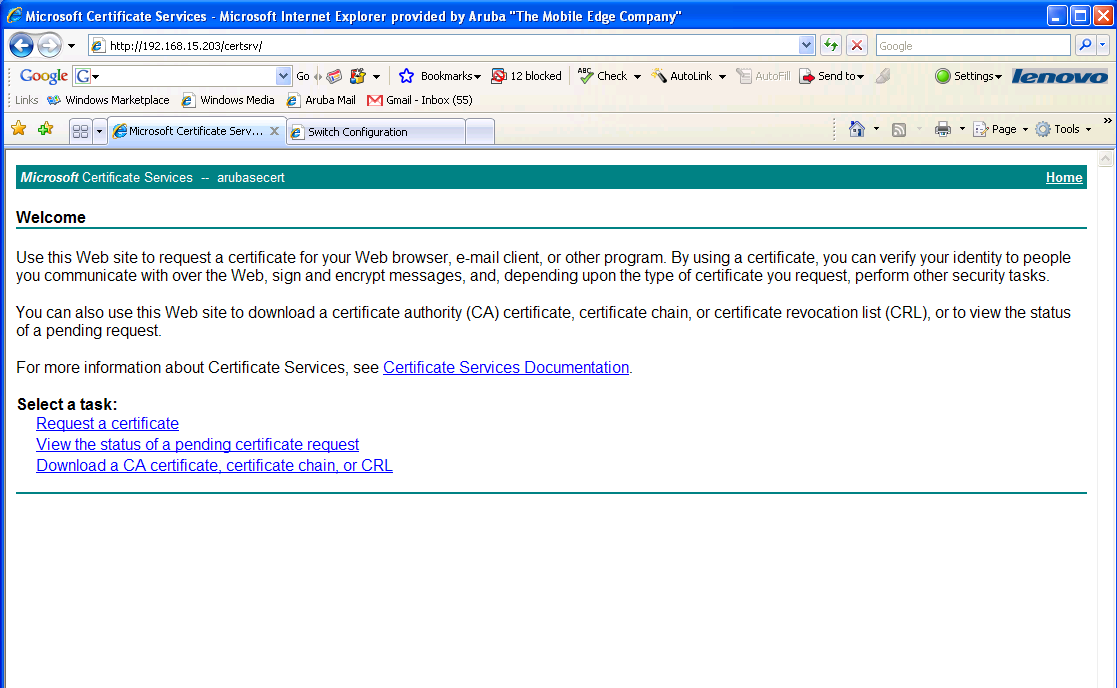
* 1. **Server Cert** – Generate a CSR by going to the Aruba Controller:
     1. Configuration> Management > Certificates > CSR
     2. Fill in all fields and click> Generate New
     3. View Current



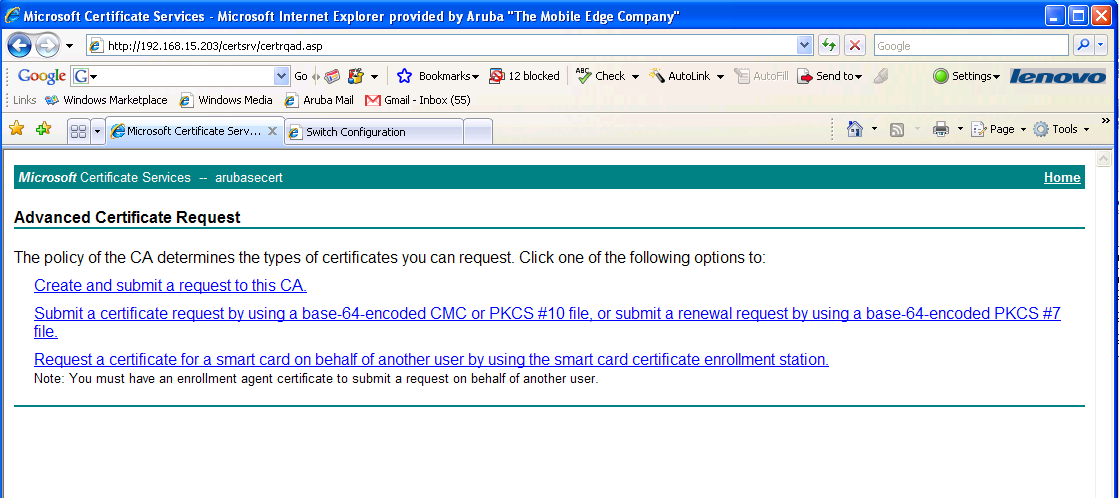
* + 1. Copy entire request from “-----BEGIN….” to “…REQUEST-----“



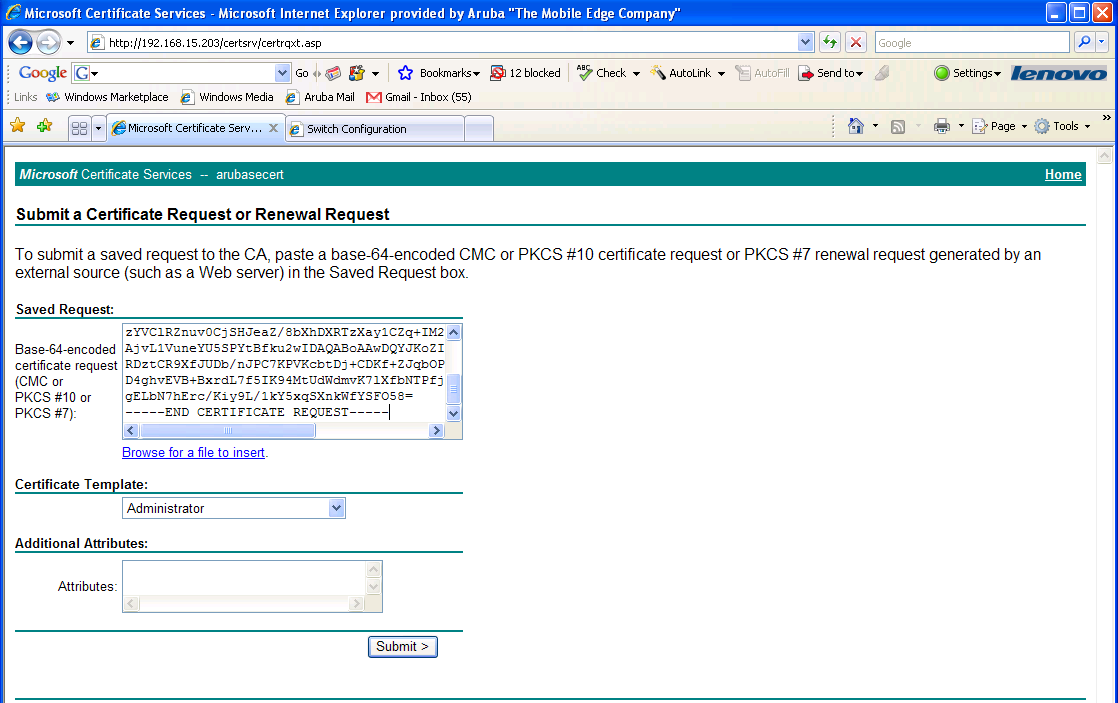
* + 1. Using your web browser go to your MS Certificate Server with the url of <http://x.x.x.x/certsrv>
    2. > Request a certificate



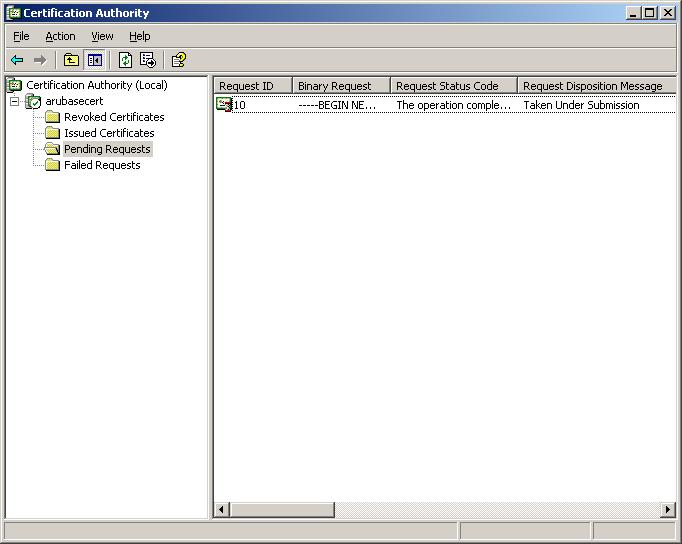
* + 1. Submit a certificate request by using a base-64-encoded….



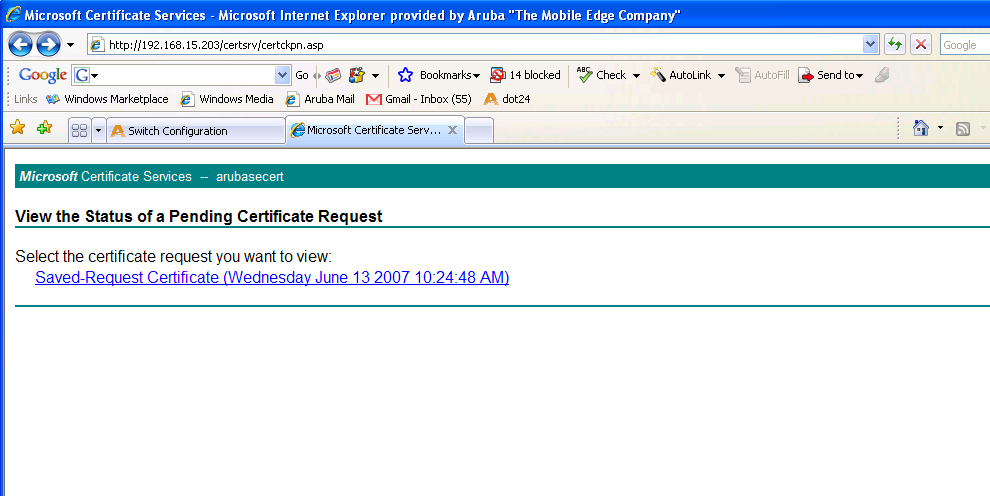
* + 1. Paste in CSR information



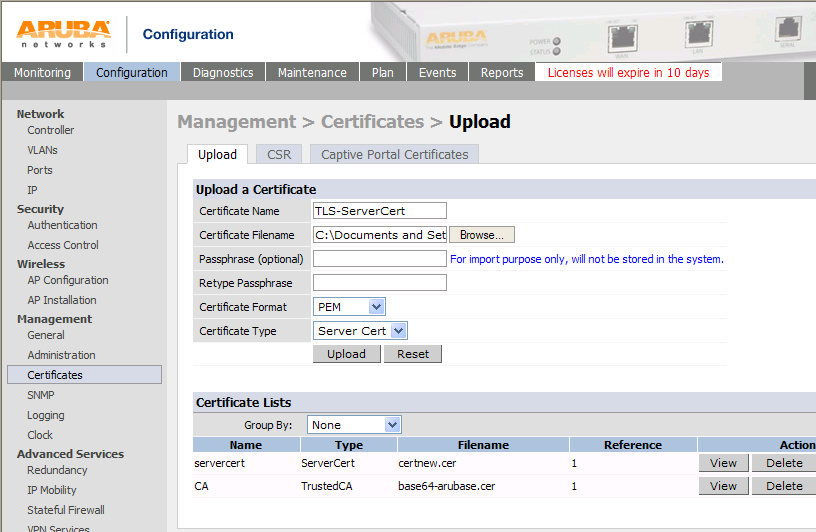
* + 1. The Cert Admin will need to approve the pending request via the MS Cert Authority. You do this by right clicking on it and choosing Issue



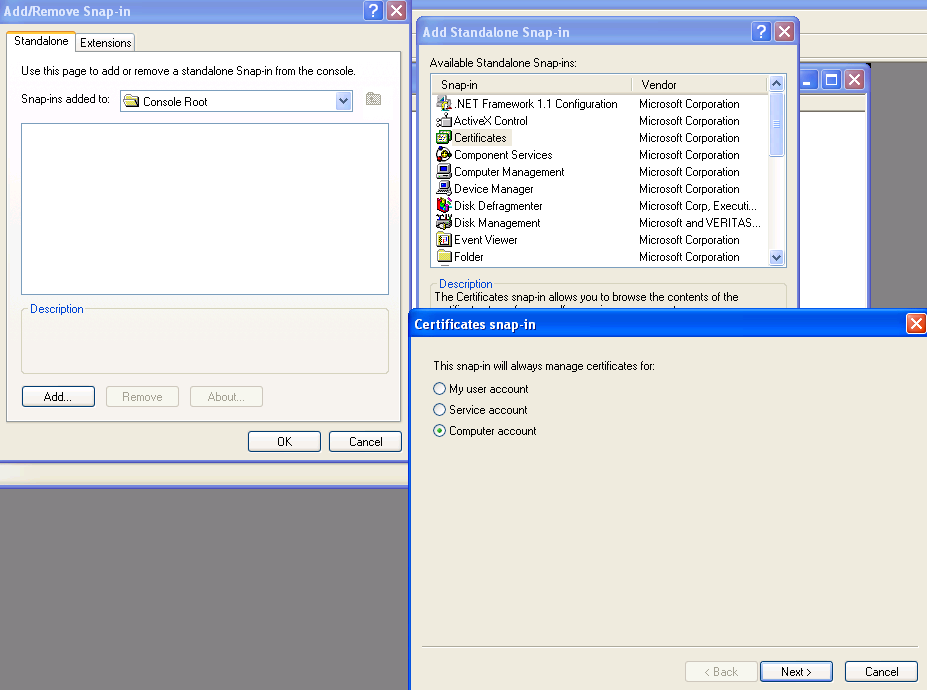
* + 1. You will now be able to web surf back to <http://x.x.x.x/certsrv> and download your cert. You should use a name that tells you it is the Server Cert so you don’t get it mixed up with your CA Cert



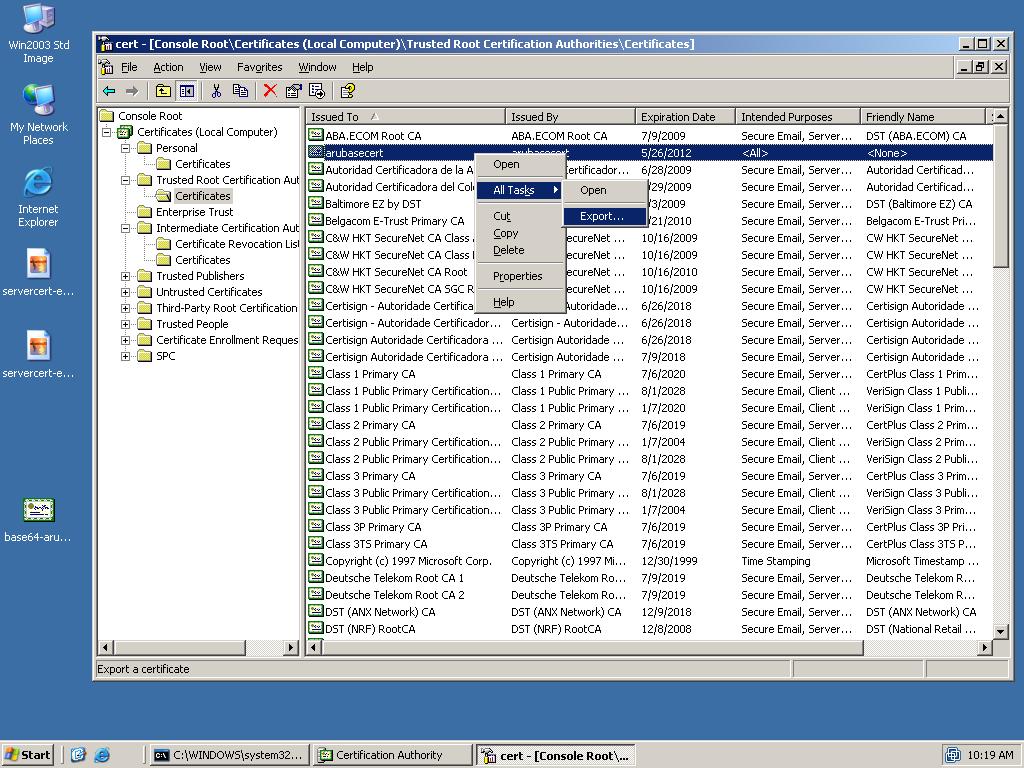
* + 1. Upload the Server Cert to the Aruba Controller.
       1. Cert format is PEM
       2. Cert Type is Server Cert



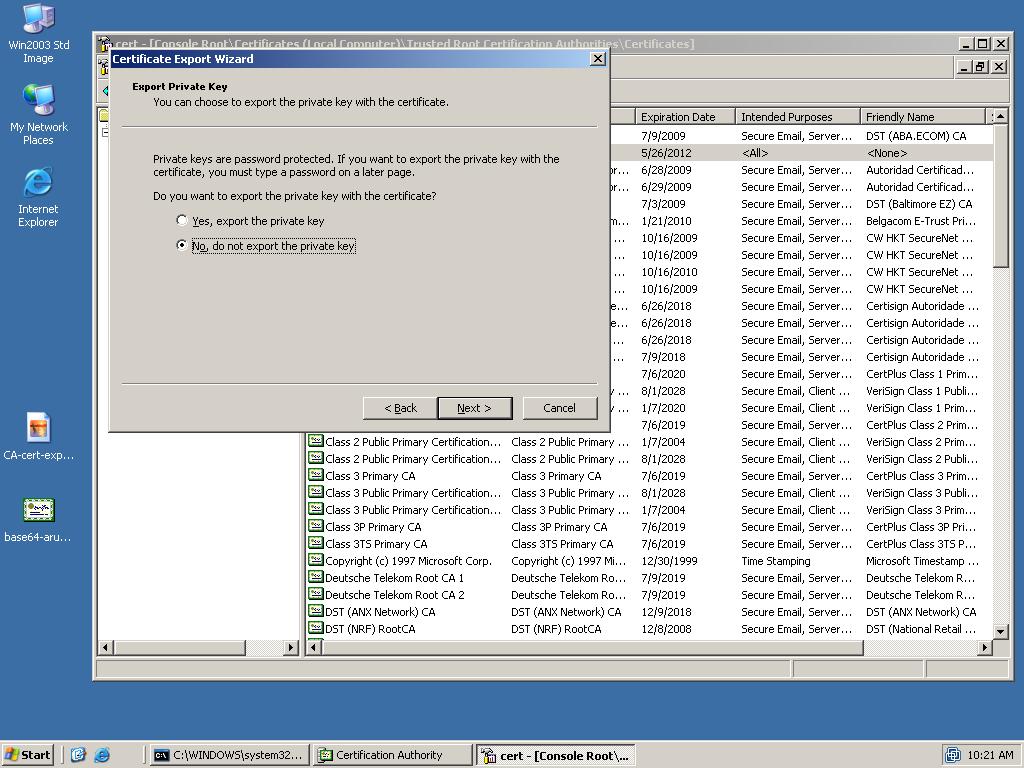
* 1. **Trusted CA Cert**
     1. From the Windows 2003 server go to Start> run and type mmc into the run dialog box. This will bring up the mmc console.
     2. go to File > add snap-in
     3. Add the Certificate snap-in with Computer account

****

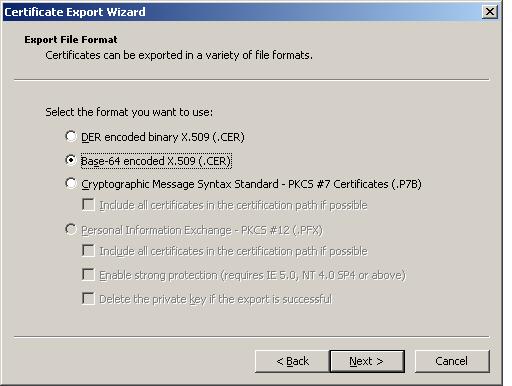
* + 1. Under the Trusted Root Cert Auth. find your Cert. This was created during the install of the MS Cert Server.
    2. Right click on it to export it



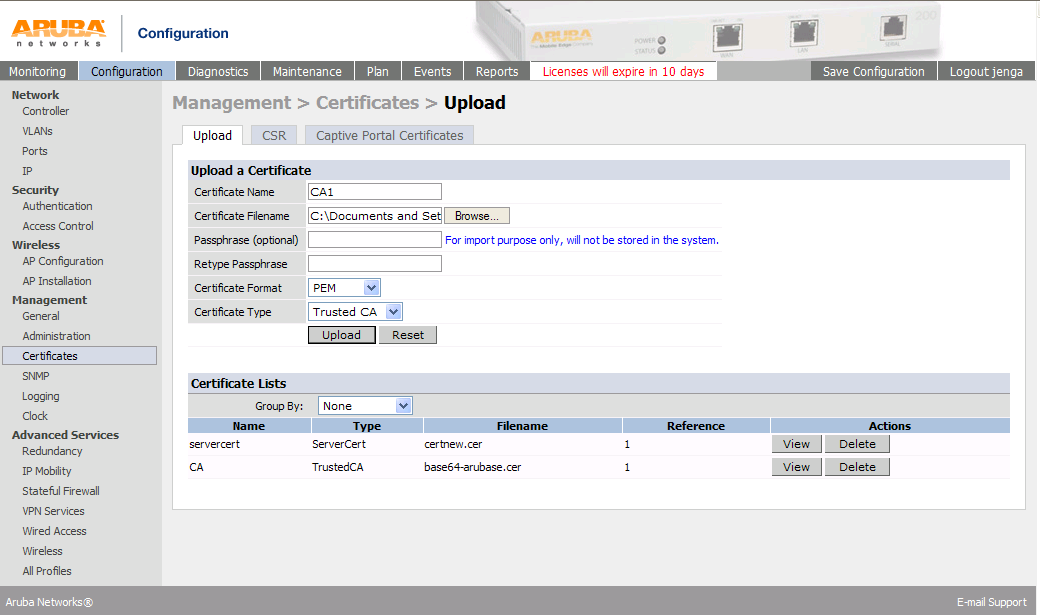
* + 1. Export without the private key



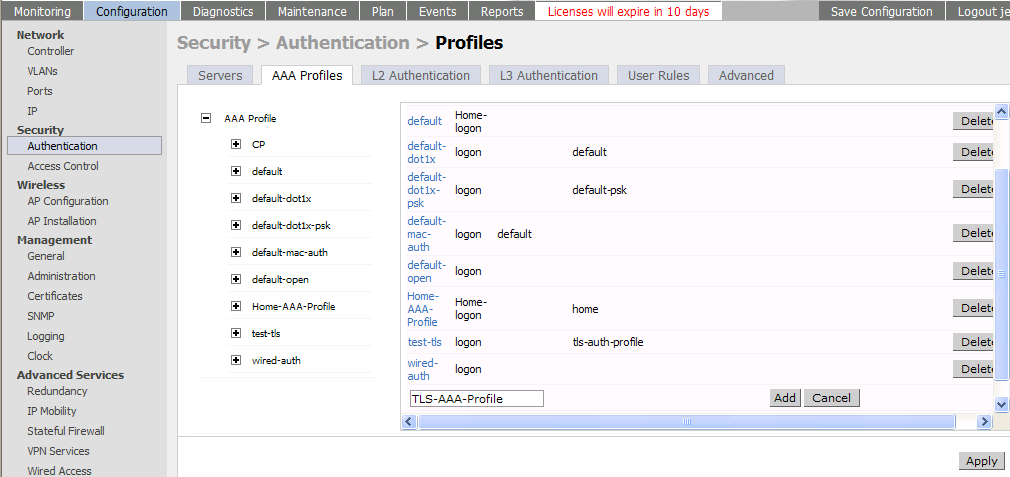
* + 1. Base-64 encoded X.509 format. Again name it with a name so that you know it is the CA Cert.



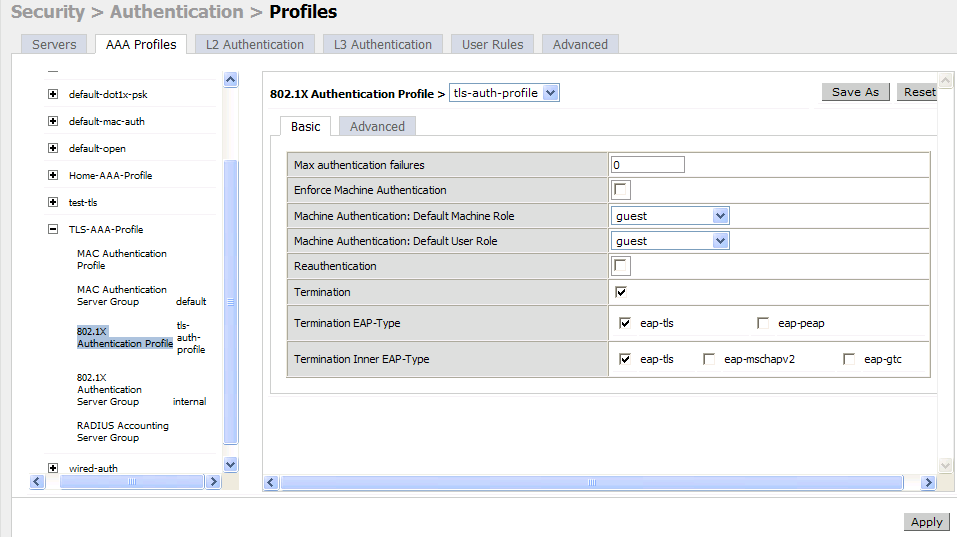
* + 1. Upload the TrustedCA to the Aruba Controller.
       1. Cert format is PEM
       2. Cert Type is Trusted CA



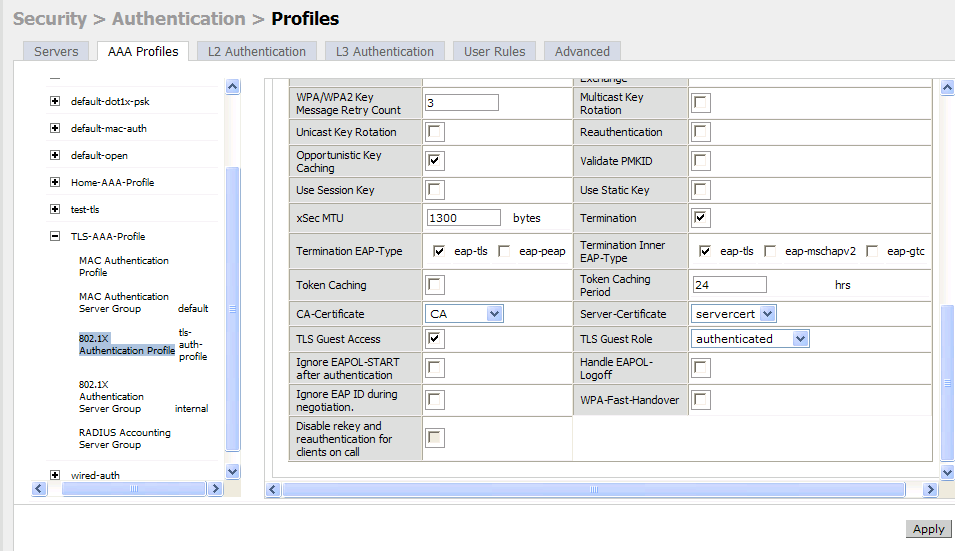
1. **Controller Authentication Configuration**
   1. Configure TLS AAA Profile
      1. Go to Configuration > Security > Authentication > Profiles
      2. Click on add at the bottom and create a new AAA Profile
      3. Chose the Initial and Default role you want to use



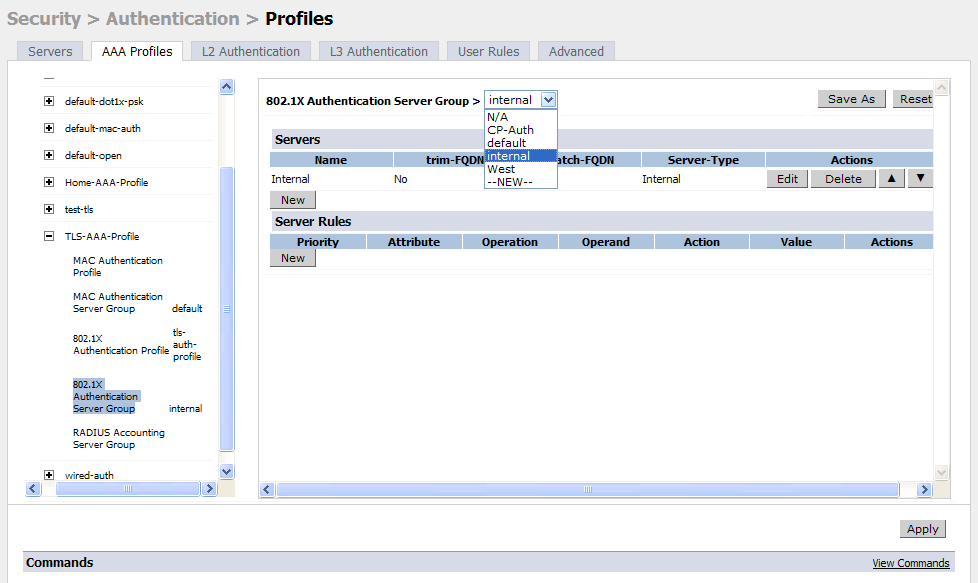
* 1. 802.1X Authentication Profile
     1. Create a new 802.1x auth profile
     2. Enable Termination
     3. EAP-Type – eap-tls
     4. Inner EAP-Type – eap-tls
     5. Make sure you Apply before the next step



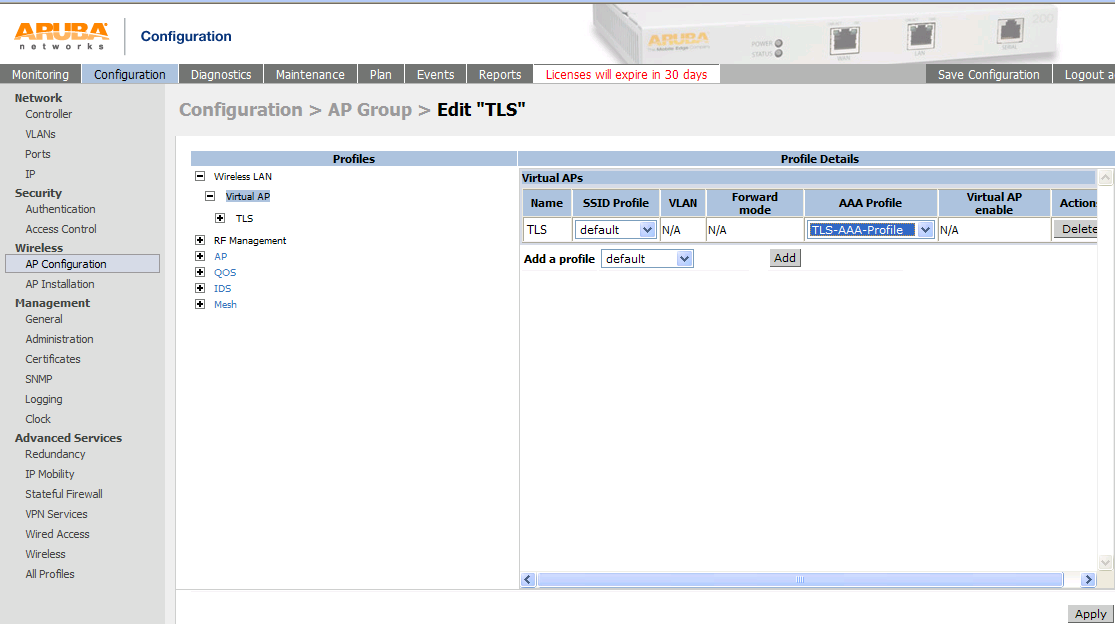
* + 1. Go into the Advanced tab
    2. Select your CA Cert and your Server Cert
    3. If you want a cert based login you will need select TLS Guest Access and a TLS Guest Role. If you do not select this option you will need to tie in some type of Auth Server



* 1. 802.1X Authentication Server Group
     1. Select the internal server as the Auth Server Group. I don’t understand why this is required for Guest TLS but it is. You do not need any usernames or passwords for Guest TLS.

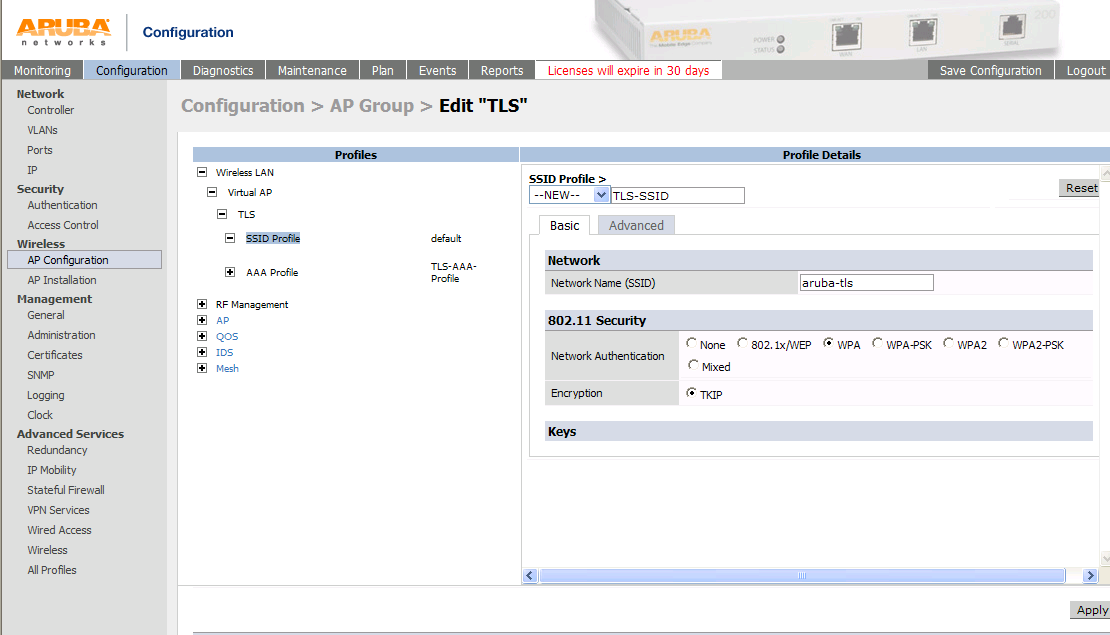


1. **AP Configuration**
   1. Add TLS Virtual AP
   2. under Configuration > AP Group > - add a SSID
   3. From the AAA Profile drop down menu select the TLS profile and apply

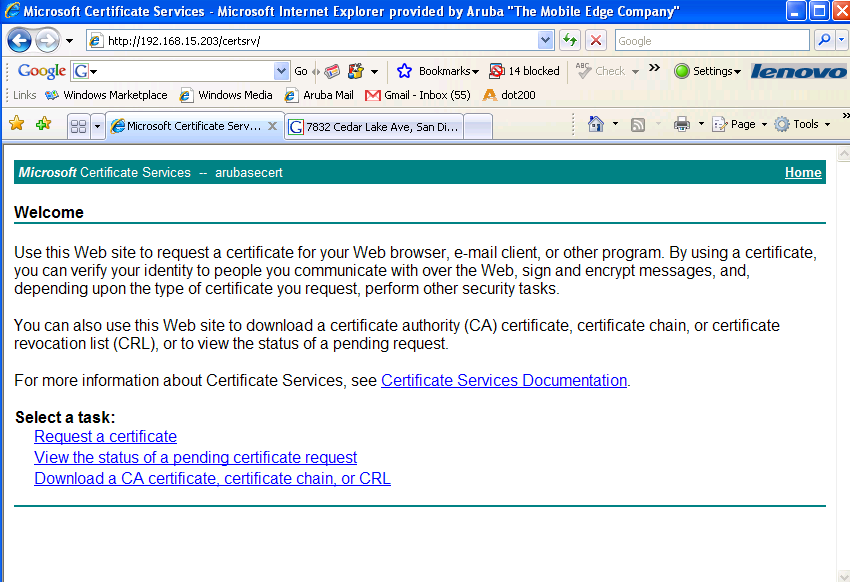


* 1. Go into the new virtual AP and edit the SSID profile
  2. Add a SSID name
  3. Select WPA and TKIP or WPA2 and AES
  4. Click on save as at the top right and give it a name.
  5. Apply

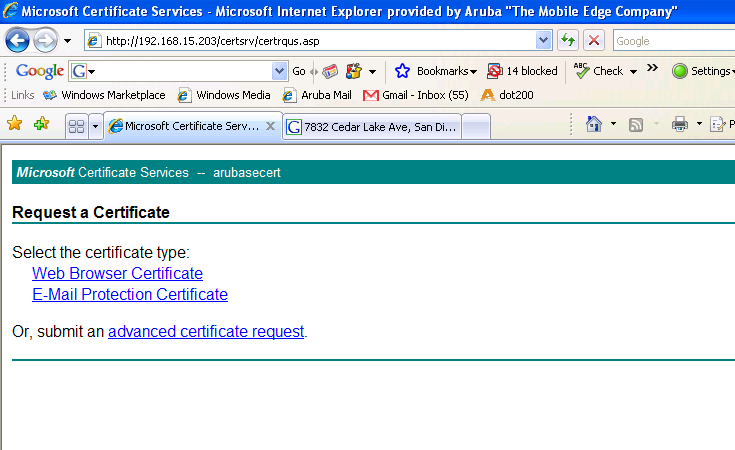
Note: do not edit the default



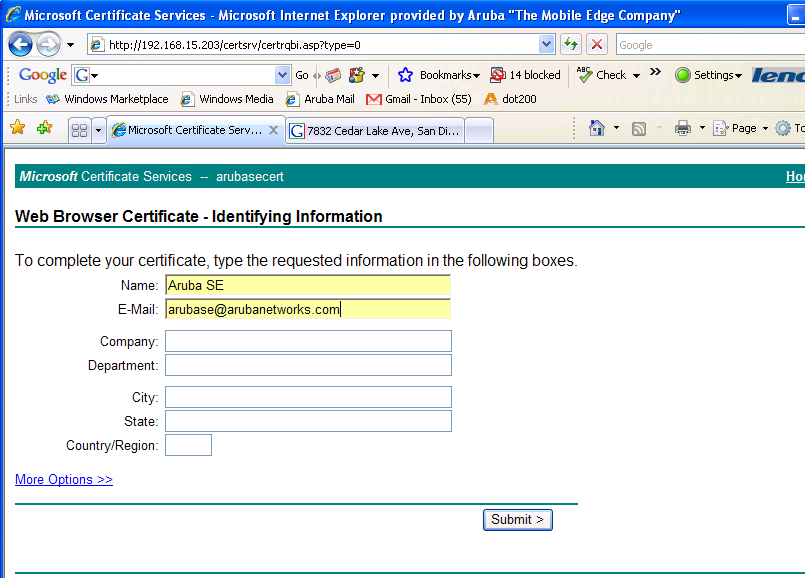
1. Client Configuration
   1. From you client web surf to your cert server <http://x.x.x.x/certsrv>
   2. Click on Request a certificate



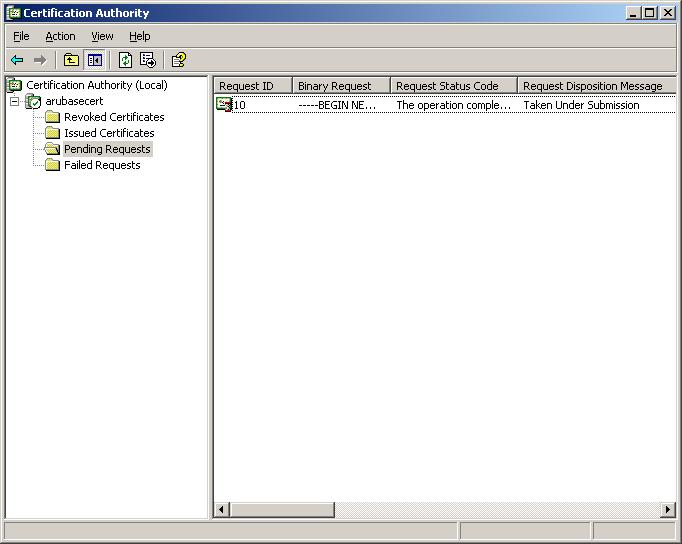
* 1. Select Web Browser Certificate



* 1. Fill in form
  2. Submit



1. The Cert Admin will need to approve the pending request via the MS Cert Authority. You do this by right clicking on it and choosing Issue



1. You will now be able to web surf back to <http://x.x.x.x/certsrv> and install your cert.

