



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
 - a. Server Cert
 - b. Trusted CA Cert
 2. Controller Authentication Configuration
 - a. Configure TLS AAA Profile
 3. AP Configuration
 - a. Add TLS Virtual AP
 4. Client Configuration

1. Certificate Creation

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

a. **Server Cert** – Generate a CSR by going to the Aruba Controller:

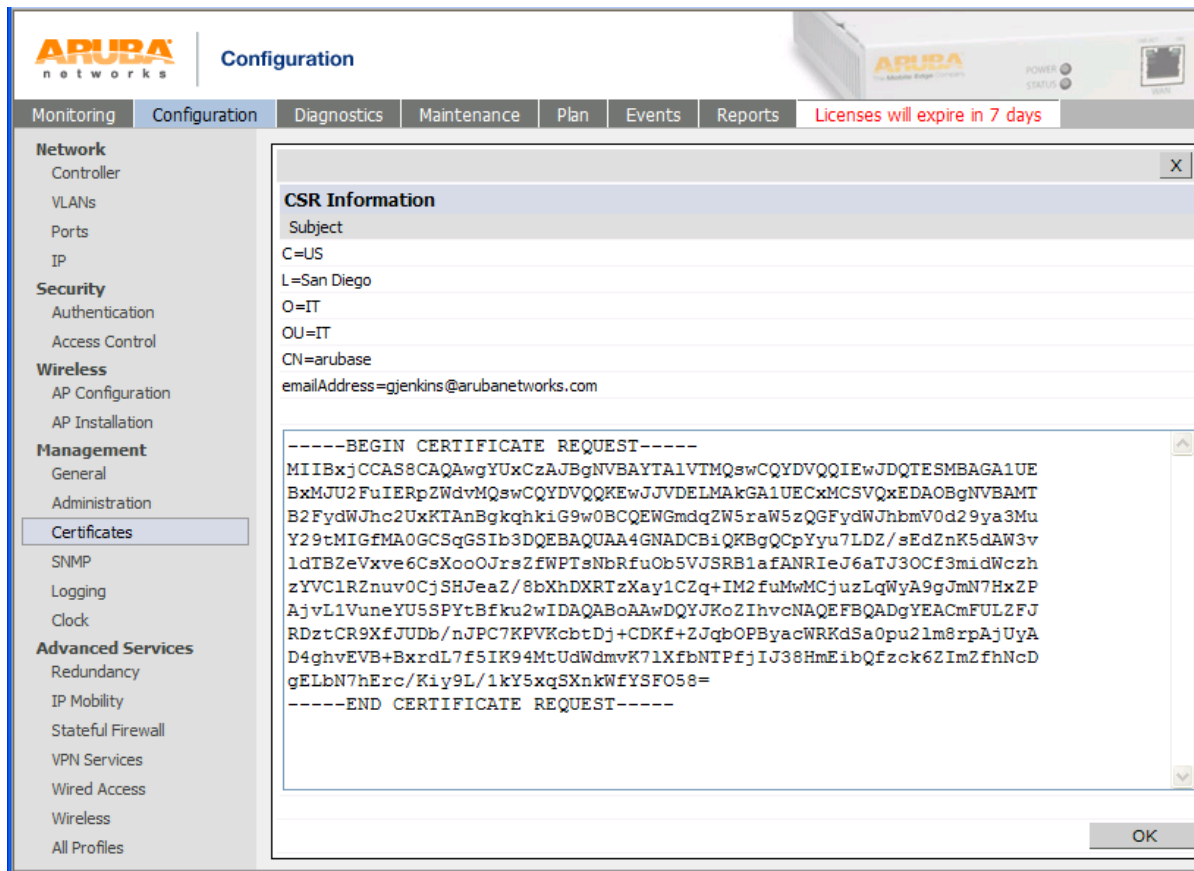
- i. *Configuration > Management > Certificates > CSR*
- ii. Fill in all fields and click > Generate New
- iii. View Current

The screenshot shows the Aruba Configuration web interface. The top navigation bar includes tabs for Monitoring, Configuration, Diagnostics, Maintenance, Plan, Events, Reports, and a license expiration notice. The left sidebar lists various configuration categories like Network, Security, Wireless, Management, and Advanced Services. The main content area is titled 'Management > Certificates > CSR' and contains a form for generating a Certificate Signing Request (CSR). The form includes fields for Key Length (1024), Common Name (arubase), Country (US), State/Province (CA), City (San Diego), Organization (IT), Unit (IT), and Email Address (gjenkins@arubanetwork). At the bottom of the form are buttons for 'Generate New', 'Reset', and 'View Current'.

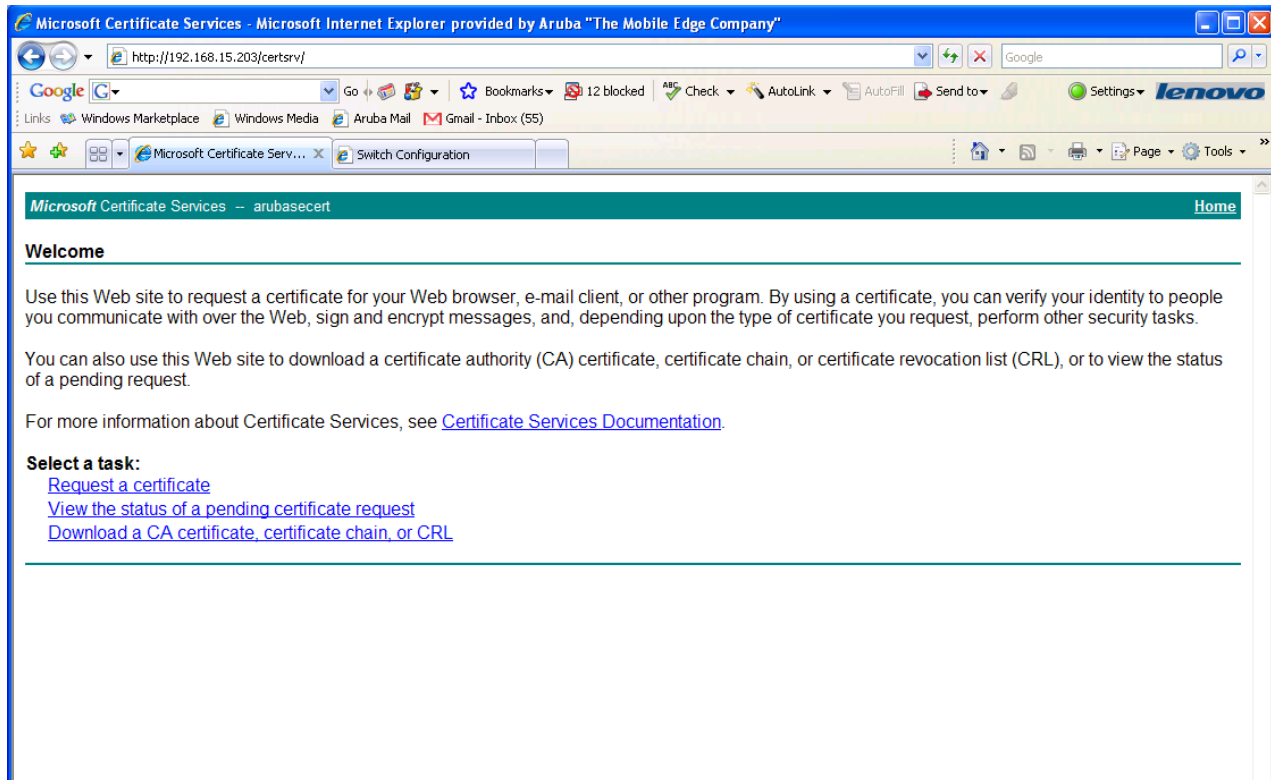
| CSR Information | |
|-----------------|-----------------------|
| Key Length | 1024 |
| Common Name | arubase |
| Country | US |
| State/Province | CA |
| City | San Diego |
| Organization | IT |
| Unit | IT |
| Email Address | gjenkins@arubanetwork |

Generate New Reset View Current

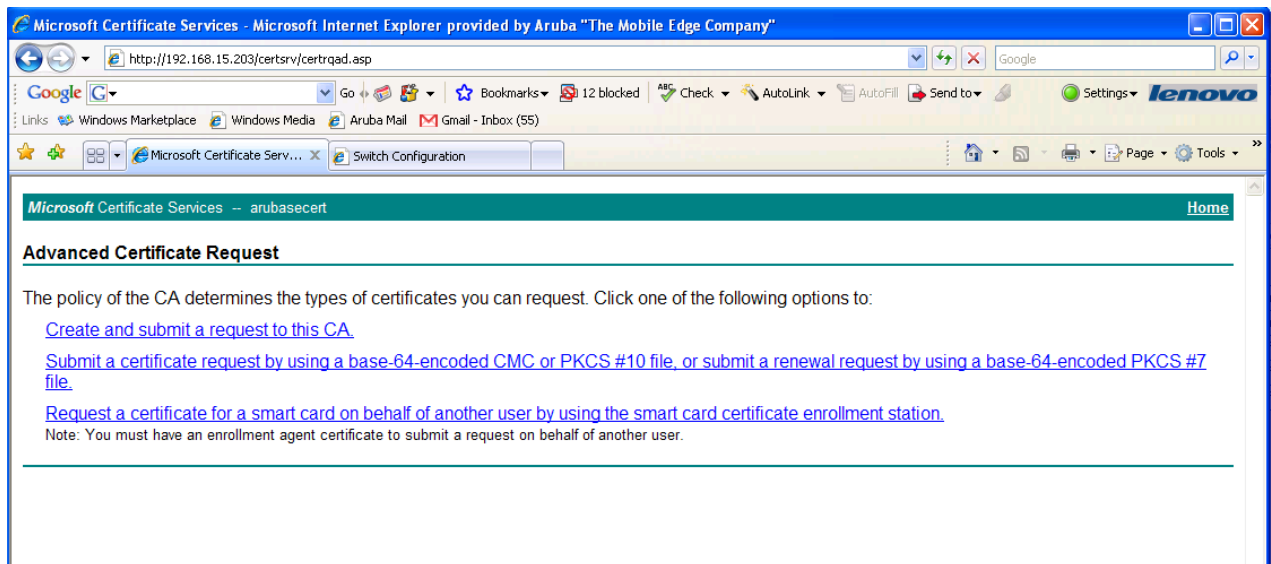
- iv. Copy entire request from “-----BEGIN....” to “...REQUEST-----”



- v. Using your web browser go to your MS Certificate Server with the url of <http://x.x.x/certsrv>
- vi. > Request a certificate



vii. Submit a certificate request by using a base-64-encoded....



viii. Paste in CSR information

Microsoft Certificate Services - Microsoft Internet Explorer provided by Aruba "The Mobile Edge Company"

http://192.168.15.203/certsrv/certrqxt.asp

Google

Go Bookmarks 12 blocked Check AutoLink AutoFill Send to Settings lenovo

Links Windows Marketplace Windows Media Aruba Mail Gmail - Inbox (55)

Microsoft Certificate Serv... Switch Configuration

Microsoft Certificate Services -- arubasecert Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```

zYVC1RZnuv0CjSHJeaZ/8bXhDXRTzXay1CZq+IM2
A3vL1VuneYU5SPYtBfku2wIDAQABoAAwDQYJKoZI
RDZtCR9XfJUDb/nJPC7KPVKcctDj+CDKf+ZJqbOP
D4ghvEVB+BxrdL7f5IK94MtUdWdmvK71XfbNTPfj
gELbN7hErc/Kiy9L/1kY5xqSXnkWfYSFO58=
-----END CERTIFICATE REQUEST-----

```

[Browse for a file to insert.](#)

Certificate Template:

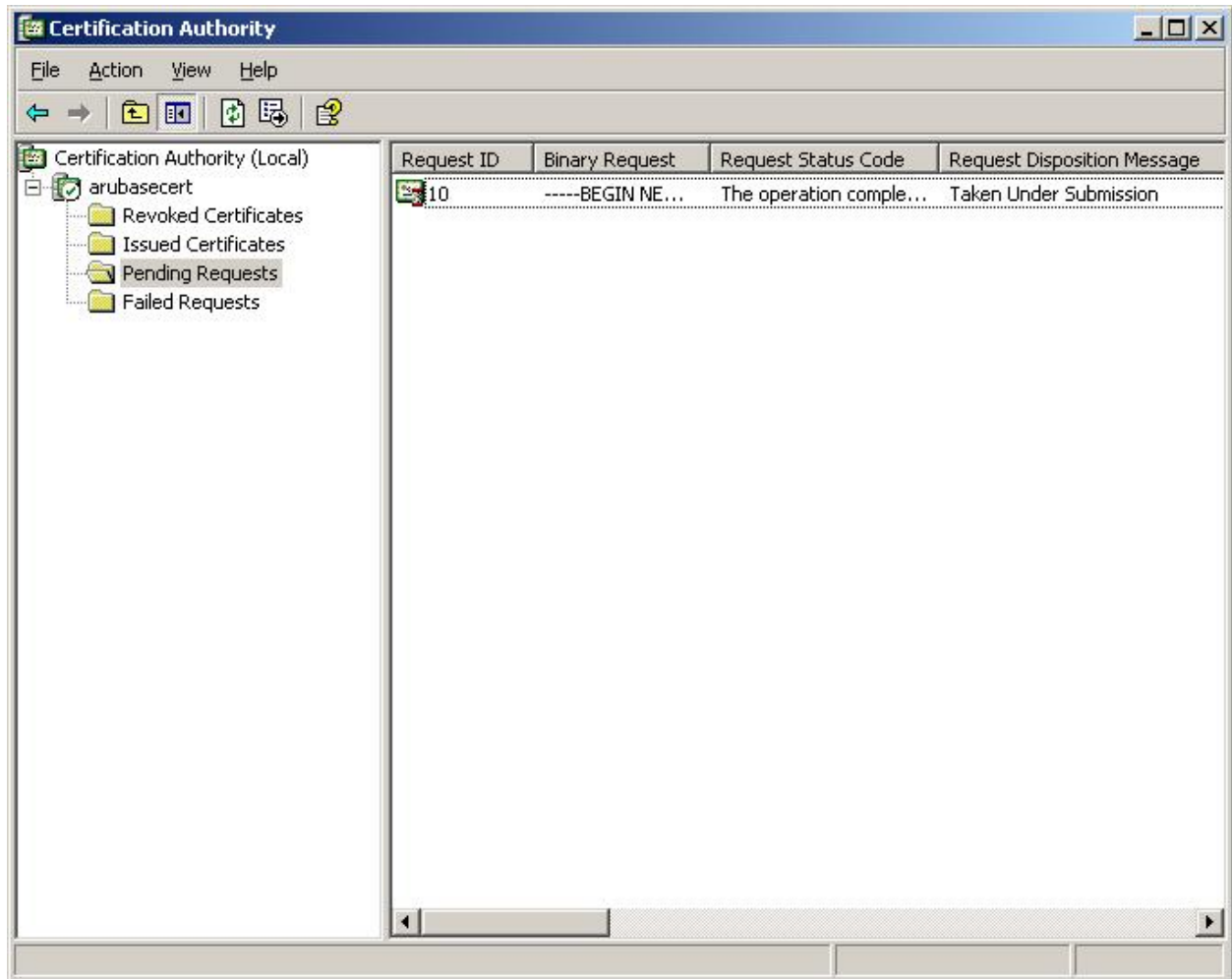
Administrator

Additional Attributes:

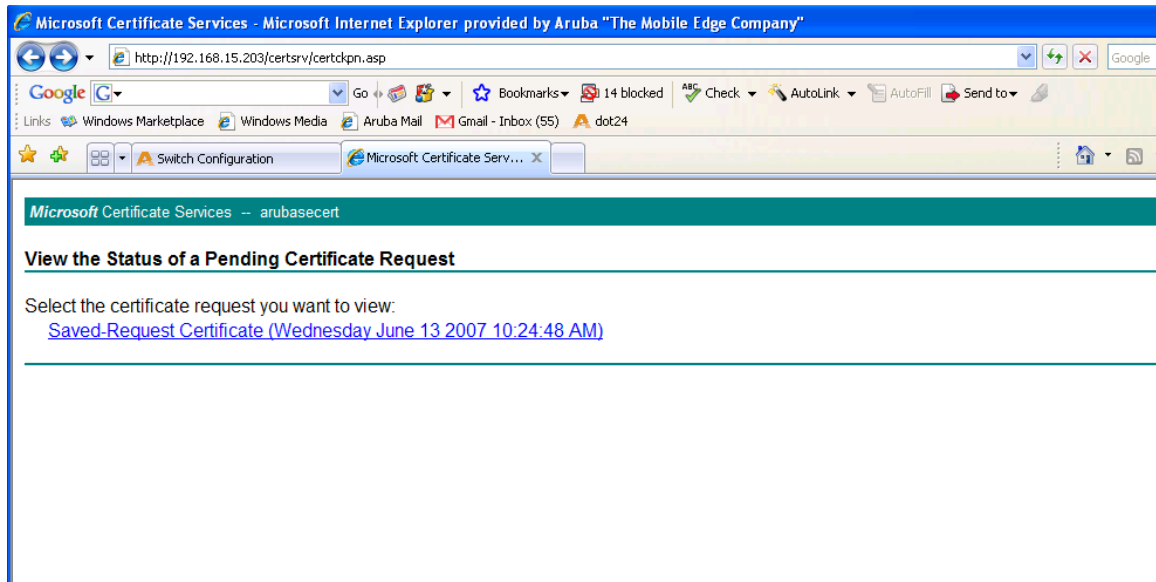
Attributes:

Submit >

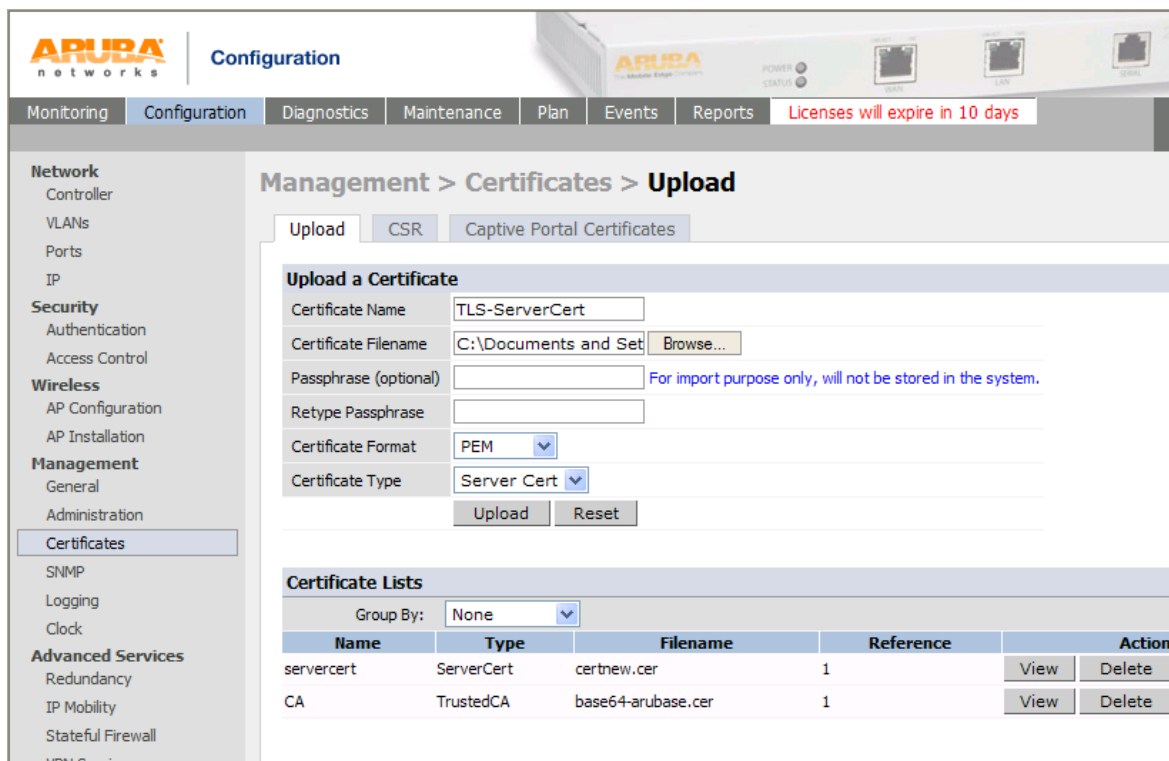
- ix. The Cert Admin will need to approve the pending request via the MS Cert Authority. You do this by right clicking on it and choosing Issue



- x. 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

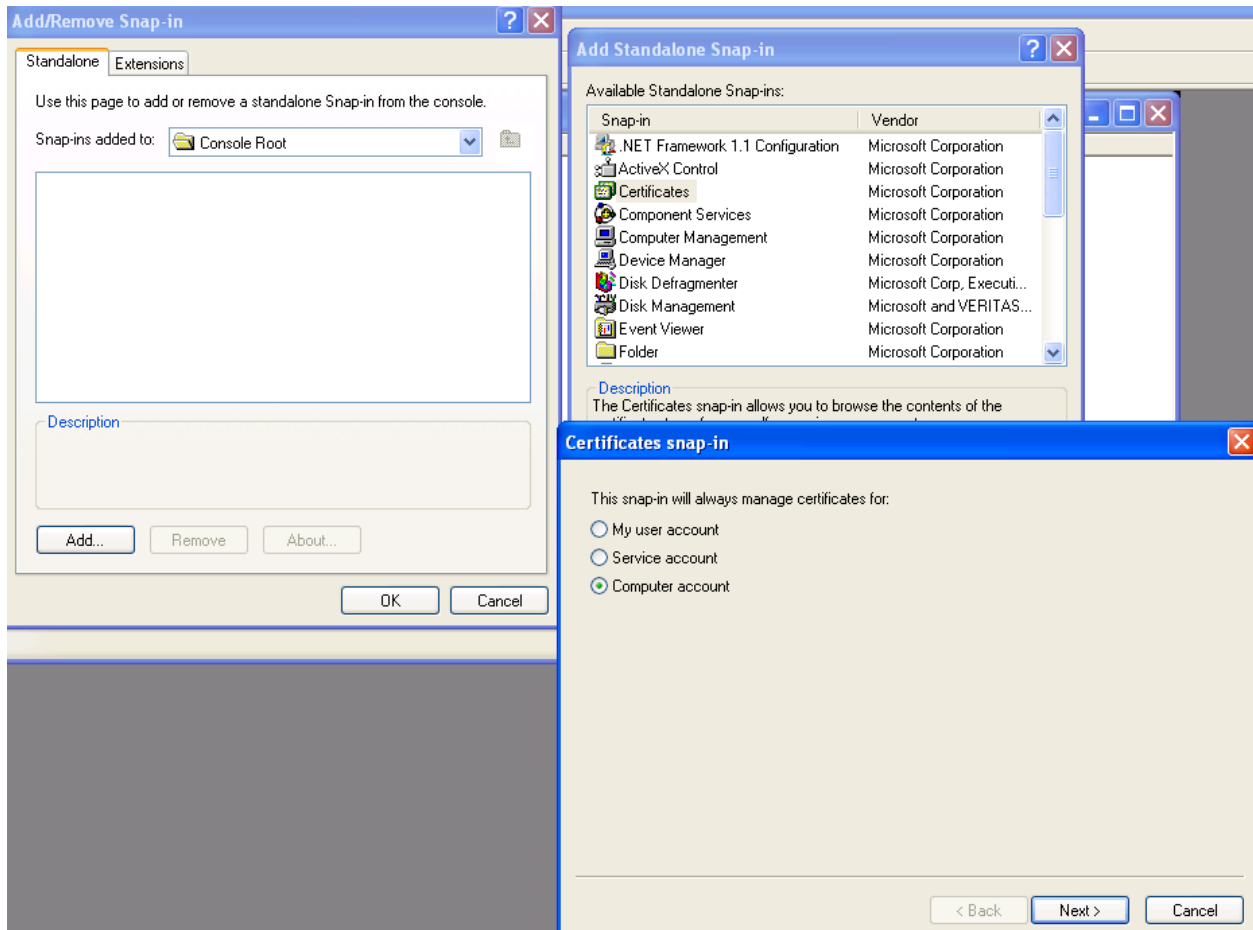


- xi. Upload the Server Cert to the Aruba Controller.
 1. Cert format is PEM
 2. Cert Type is Server Cert

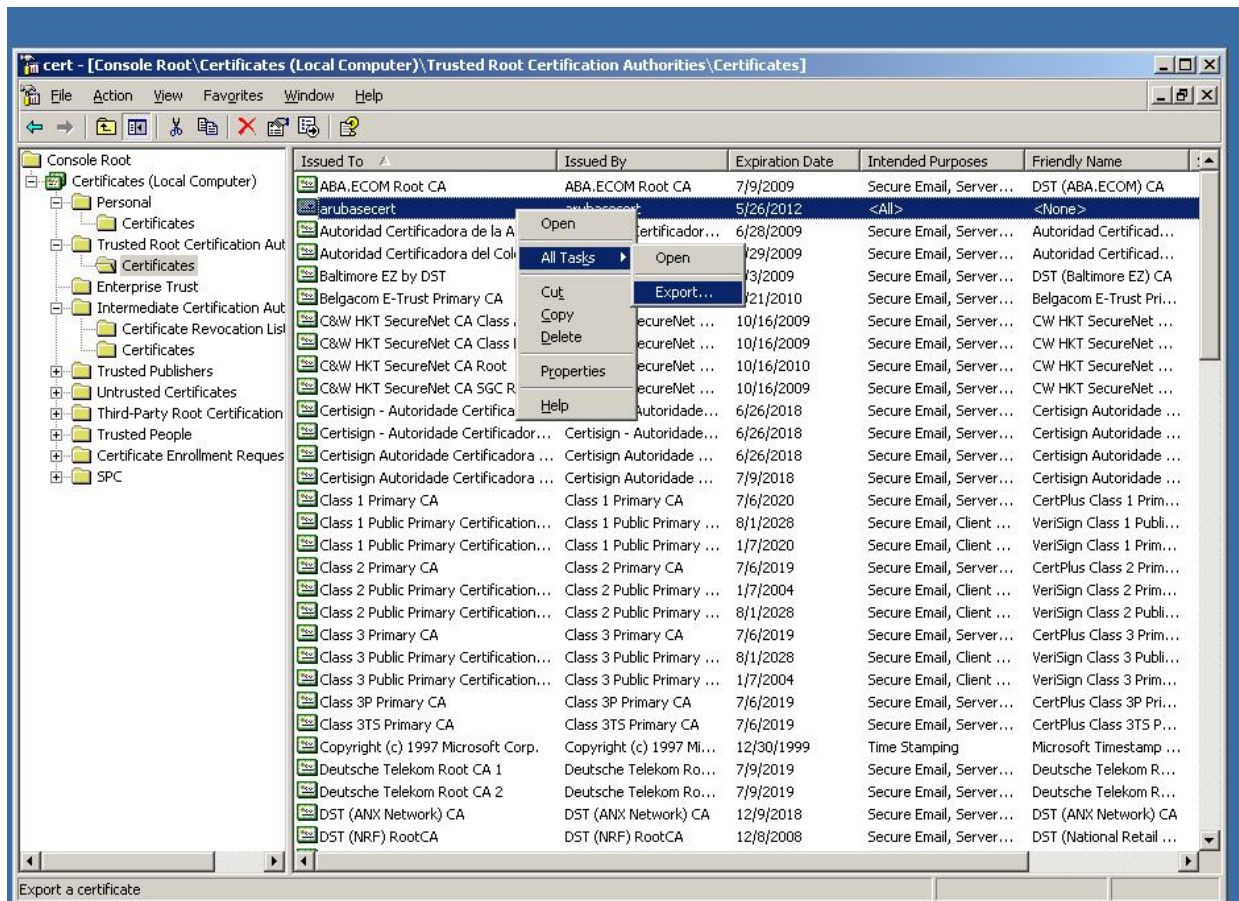


b. Trusted CA Cert

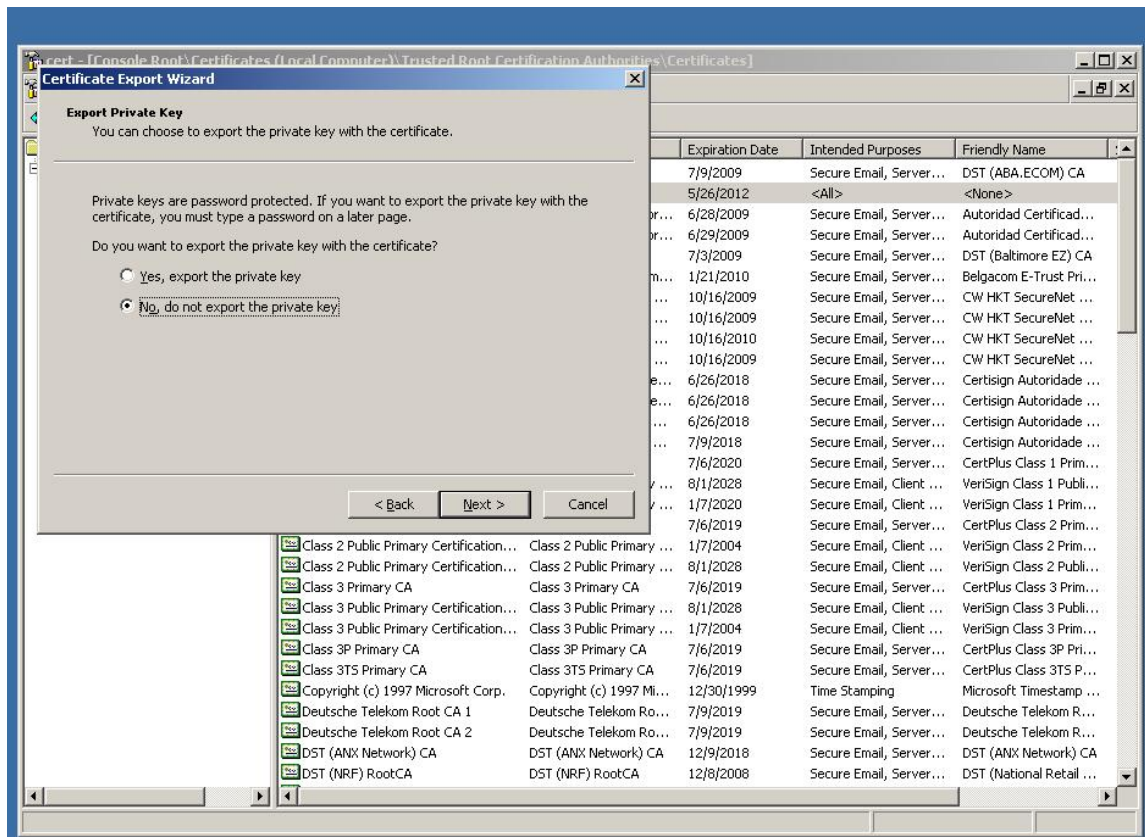
- i. From the Windows 2003 server go to Start> run and type mmc into the run dialog box. This will bring up the mmc console.
- ii. go to File > add snap-in
- iii. Add the Certificate snap-in with Computer account



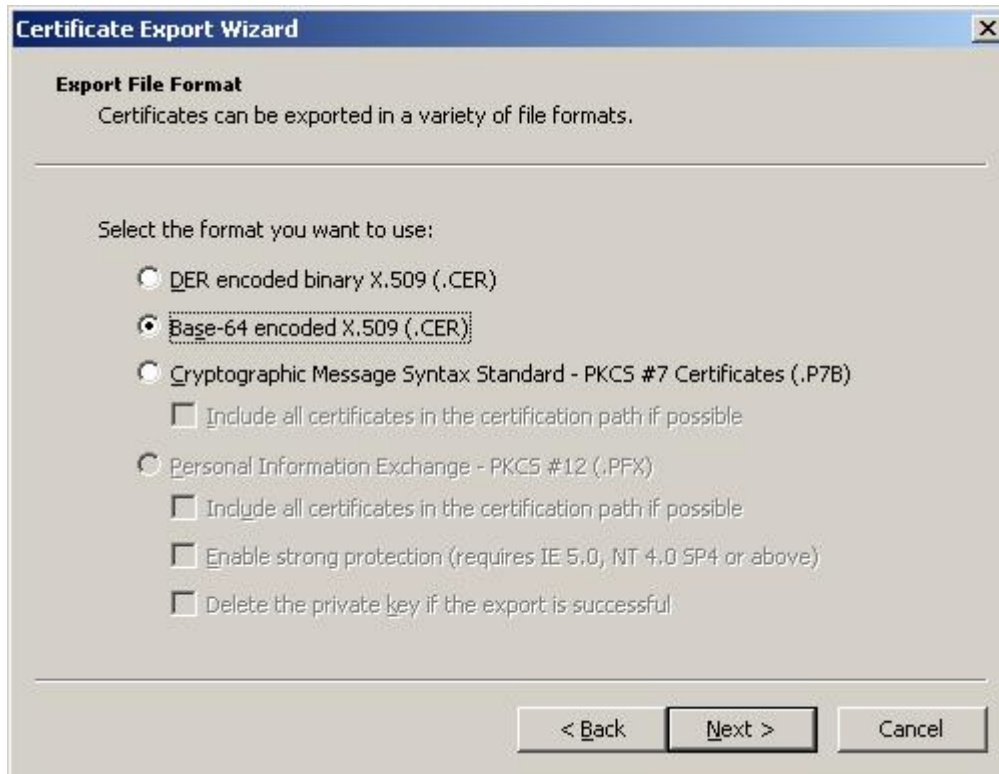
- iv. Under the Trusted Root Cert Auth. find your Cert. This was created during the install of the MS Cert Server.
- v. Right click on it to export it



vi. Export without the private key



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



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

ARUBA networks | Configuration

Monitoring | Configuration | Diagnostics | Maintenance | Plan | Events | Reports | Licenses will expire in 10 days | Save Configuration | Logout jenga

Management > Certificates > Upload

Upload | CSR | Captive Portal Certificates

Upload a Certificate

Certificate Name: CA1

Certificate Filename: C:\Documents and Set [Browse...](#)

Passphrase (optional): [For import purpose only, will not be stored in the system.](#)

Retype Passphrase:

Certificate Format: PEM

Certificate Type: Trusted CA

[Upload](#) [Reset](#)

Certificate Lists

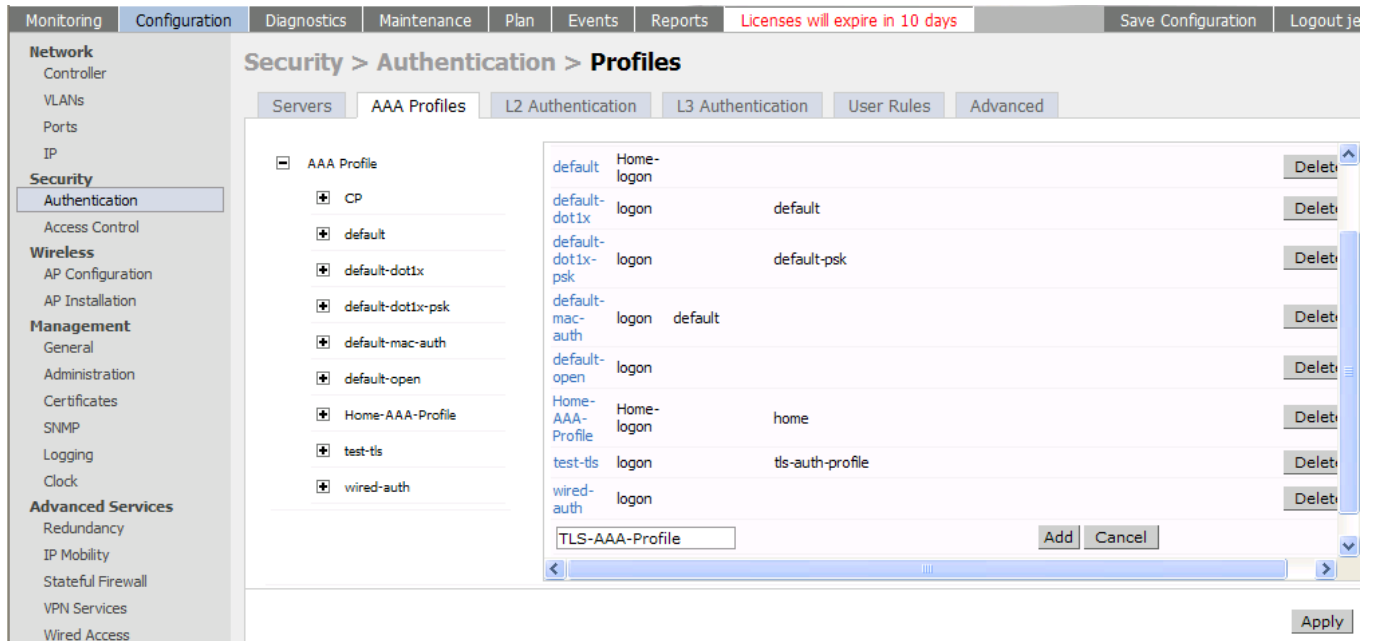
Group By: None

| Name | Type | Filename | Reference | Actions |
|------------|------------|--------------------|-----------|---|
| servercert | ServerCert | certnew.cer | 1 | View Delete |
| CA | TrustedCA | base64-arubase.cer | 1 | View Delete |

Aruba Networks® | E-mail Support

2. Controller Authentication Configuration

- a. Configure TLS AAA Profile
 - i. Go to *Configuration > Security > Authentication > Profiles*
 - ii. Click on add at the bottom and create a new AAA Profile
 - iii. Chose the Initial and Default role you want to use



b. 802.1X Authentication Profile

- i. Create a new 802.1x auth profile
- ii. Enable Termination
- iii. EAP-Type – eap-tls
- iv. Inner EAP-Type – eap-tls
- v. Make sure you Apply before the next step

Security > Authentication > Profiles

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

802.1X Authentication Profile > tls-auth-profile

Basic Advanced

| | |
|--|--|
| Max authentication failures | 0 |
| Enforce Machine Authentication | <input type="checkbox"/> |
| Machine Authentication: Default Machine Role | guest |
| Machine Authentication: Default User Role | guest |
| Reauthentication | <input type="checkbox"/> |
| Termination | <input checked="" type="checkbox"/> |
| Termination EAP-Type | <input checked="" type="checkbox"/> eap-tls <input type="checkbox"/> eap-peap |
| Termination Inner EAP-Type | <input checked="" type="checkbox"/> eap-tls <input type="checkbox"/> eap-mschapv2 <input type="checkbox"/> eap-gtc |

Apply

- vi. Go into the Advanced tab
- vii. Select your CA Cert and your Server Cert
- viii. 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

Security > Authentication > Profiles

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

802.1X Authentication Profile > tls-auth-profile

Basic Advanced

| | | | |
|--|---|----------------------------|--|
| WPA/WPA2 Key Message Retry Count | 3 | Multicast Key Rotation | <input type="checkbox"/> |
| Unicast Key Rotation | <input type="checkbox"/> | Reauthentication | <input type="checkbox"/> |
| Opportunistic Key Caching | <input checked="" type="checkbox"/> | Validate PMKID | <input type="checkbox"/> |
| Use Session Key | <input type="checkbox"/> | Use Static Key | <input type="checkbox"/> |
| xSec MTU | 1300 bytes | Termination | <input checked="" type="checkbox"/> |
| Termination EAP-Type | <input checked="" type="checkbox"/> eap-tls <input type="checkbox"/> eap-peap | Termination Inner EAP-Type | <input checked="" type="checkbox"/> eap-tls <input type="checkbox"/> eap-mschapv2 <input type="checkbox"/> eap-gtc |
| Token Caching | <input type="checkbox"/> | Token Caching Period | 24 hrs |
| CA-Certificate | CA | Server-Certificate | servercert |
| TLS Guest Access | <input checked="" type="checkbox"/> | TLS Guest Role | authenticated |
| Ignore EAPOL-START after authentication | <input type="checkbox"/> | Handle EAPOL-Logoff | <input type="checkbox"/> |
| Ignore EAP ID during negotiation | <input type="checkbox"/> | WPA-Fast-Handover | <input type="checkbox"/> |
| Disable rekey and reauthentication for clients on call | <input type="checkbox"/> | | |

Apply

c. 802.1X Authentication Server Group

- i. 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.

Security > Authentication > Profiles

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

802.1X Authentication Server Group > internal

Save As Reset

| Name | trim-FQDN | match-FQDN | Server-Type | Actions |
|----------|-----------|------------|-------------|-----------------|
| Internal | No | West | Internal | Edit Delete ▲ ▼ |

New

| Priority | Attribute | Operation | Operand | Action | Value | Actions |
|----------|-----------|-----------|---------|--------|-------|---------|
| New | | | | | | |

Apply

Commands View Commands

3. AP Configuration


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

The screenshot shows the Aruba Configuration web interface. The top navigation bar includes tabs for Monitoring, Configuration, Diagnostics, Maintenance, Plan, Events, Reports, and a license expiration notice. The left sidebar lists various configuration categories like Network, Security, Wireless, Management, and Advanced Services. The main content area is titled 'Configuration > AP Group > Edit "TLS"'. It features a 'Profiles' tree on the left with 'Virtual AP' expanded, showing 'TLS' selected. The 'Profile Details' section on the right contains a table for 'Virtual APs' with columns: Name, SSID Profile, VLAN, Forward mode, AAA Profile, Virtual AP enable, and Action. The table has one entry for 'TLS' with 'default' as the SSID Profile, 'N/A' for VLAN and Forward mode, 'TLS-AAA-Profile' for AAA Profile, and 'N/A' for Virtual AP enable. Below the table is an 'Add a profile' section with a 'default' dropdown and an 'Add' button. An 'Apply' button is at the bottom right.

| Profiles | | Profile Details | | | | | | |
|---------------|--|------------------------------|--------------|------|--------------|-----------------|-------------------|--------|
| Wireless LAN | | Virtual APs | | | | | | |
| Virtual AP | | Name | SSID Profile | VLAN | Forward mode | AAA Profile | Virtual AP enable | Action |
| TLS | | TLS | default | N/A | N/A | TLS-AAA-Profile | N/A | Delete |
| RF Management | | Add a profile: default [Add] | | | | | | |
| AP | | | | | | | | |
| QOS | | | | | | | | |
| IDS | | | | | | | | |
| Mesh | | | | | | | | |

- d. Go into the new virtual AP and edit the SSID profile
- e. Add a SSID name
- f. Select WPA and TKIP or WPA2 and AES
- g. Click on save as at the top right and give it a name.
- h. Apply

Note: do not edit the default



ARUBA networks Configuration

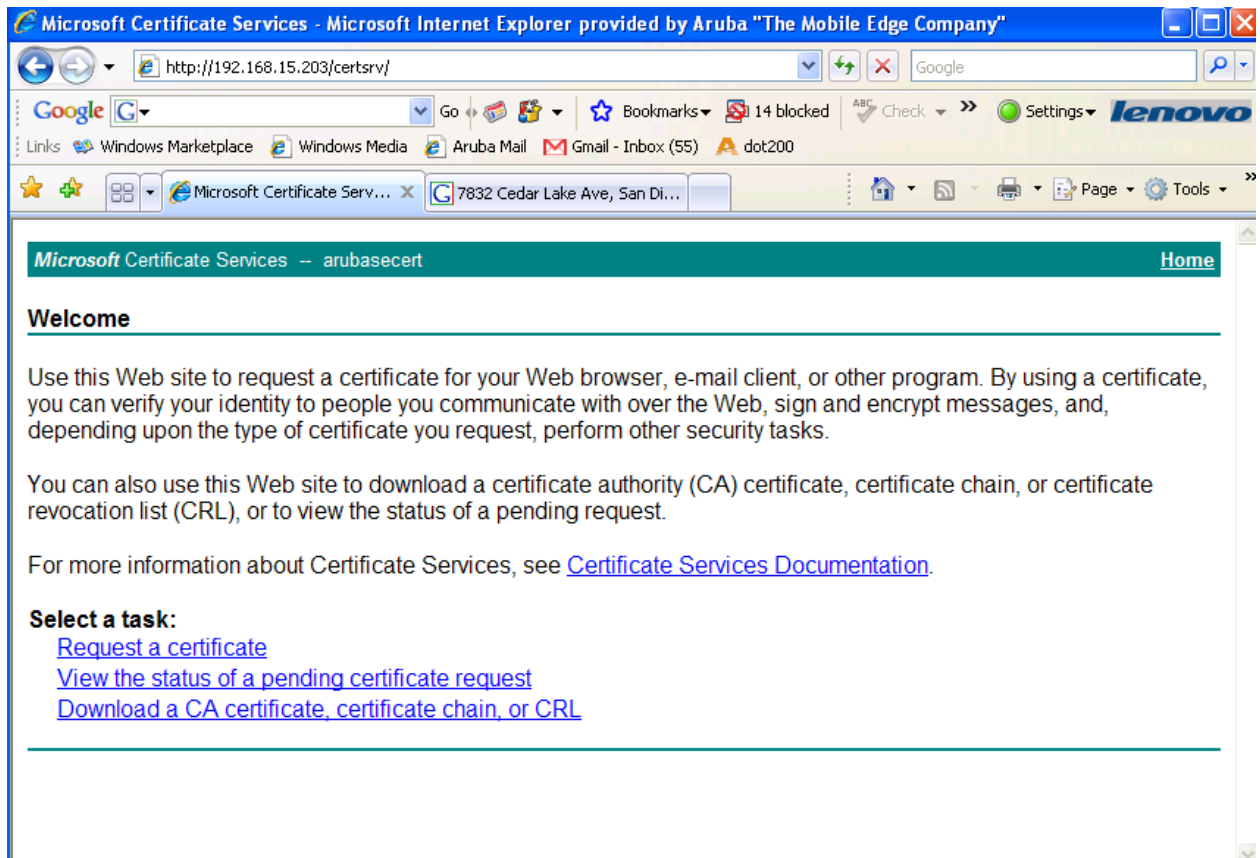
Monitoring Configuration Diagnostics Maintenance Plan Events Reports Licenses will expire in 30 days Save Configuration Logout

Configuration > AP Group > Edit "TLS"

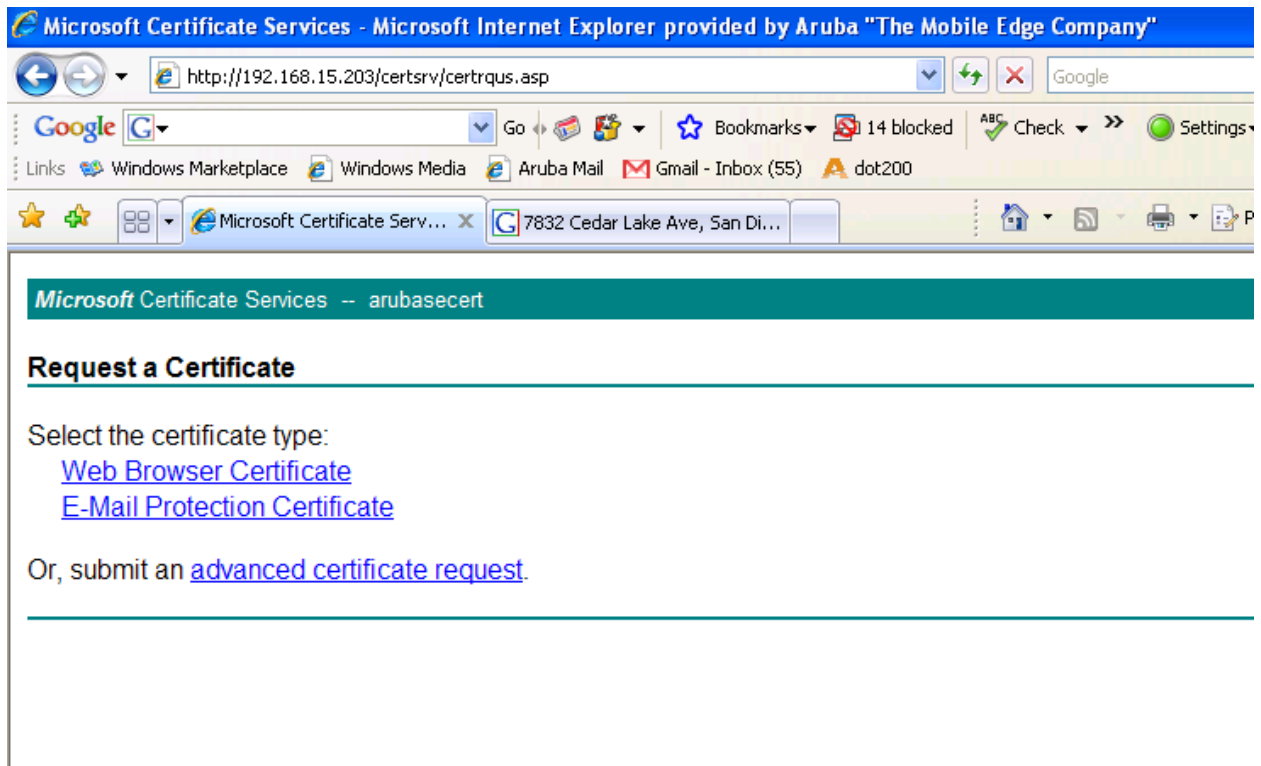
| Profiles | Profile Details |
|---|--|
| <ul style="list-style-type: none"> Wireless LAN <ul style="list-style-type: none"> Virtual AP <ul style="list-style-type: none"> SSID Profile default AAA Profile TLS-AAA-Profile RF Management <ul style="list-style-type: none"> AP QOS IDS Mesh | <p>SSID Profile > --NEW-- TLS-SSID Reset</p> <p>Basic Advanced</p> <p>Network</p> <p>Network Name (SSID) <input type="text" value="aruba-tls"/></p> <p>802.11 Security</p> <p>Network Authentication <input type="radio"/> None <input type="radio"/> 802.1x/WEP <input checked="" type="radio"/> WPA <input type="radio"/> WPA-PSK <input type="radio"/> WPA2 <input type="radio"/> WPA2-PSK</p> <p><input type="radio"/> Mixed</p> <p>Encryption <input checked="" type="radio"/> TKIP</p> <p>Keys</p> <p>Apply</p> |

4. Client Configuration

- From your client web surf to your cert server <http://x.x.x.x/certsrv>
- Click on Request a certificate



c. Select Web Browser Certificate



- d. Fill in form
- e. Submit

Microsoft Certificate Services - Microsoft Internet Explorer provided by Aruba "The Mobile Edge Company"

http://192.168.15.203/certsrv/certrqbi.asp?type=0

Google

Go Bookmarks 14 blocked Check Settings

Links Windows Marketplace Windows Media Aruba Mail Gmail - Inbox (55) dot200

Microsoft Certificate Serv... 7832 Cedar Lake Ave, San Di...

Microsoft Certificate Services -- arubasecert

Web Browser Certificate - Identifying Information

To complete your certificate, type the requested information in the following boxes.

Name:

E-Mail:

Company:

Department:

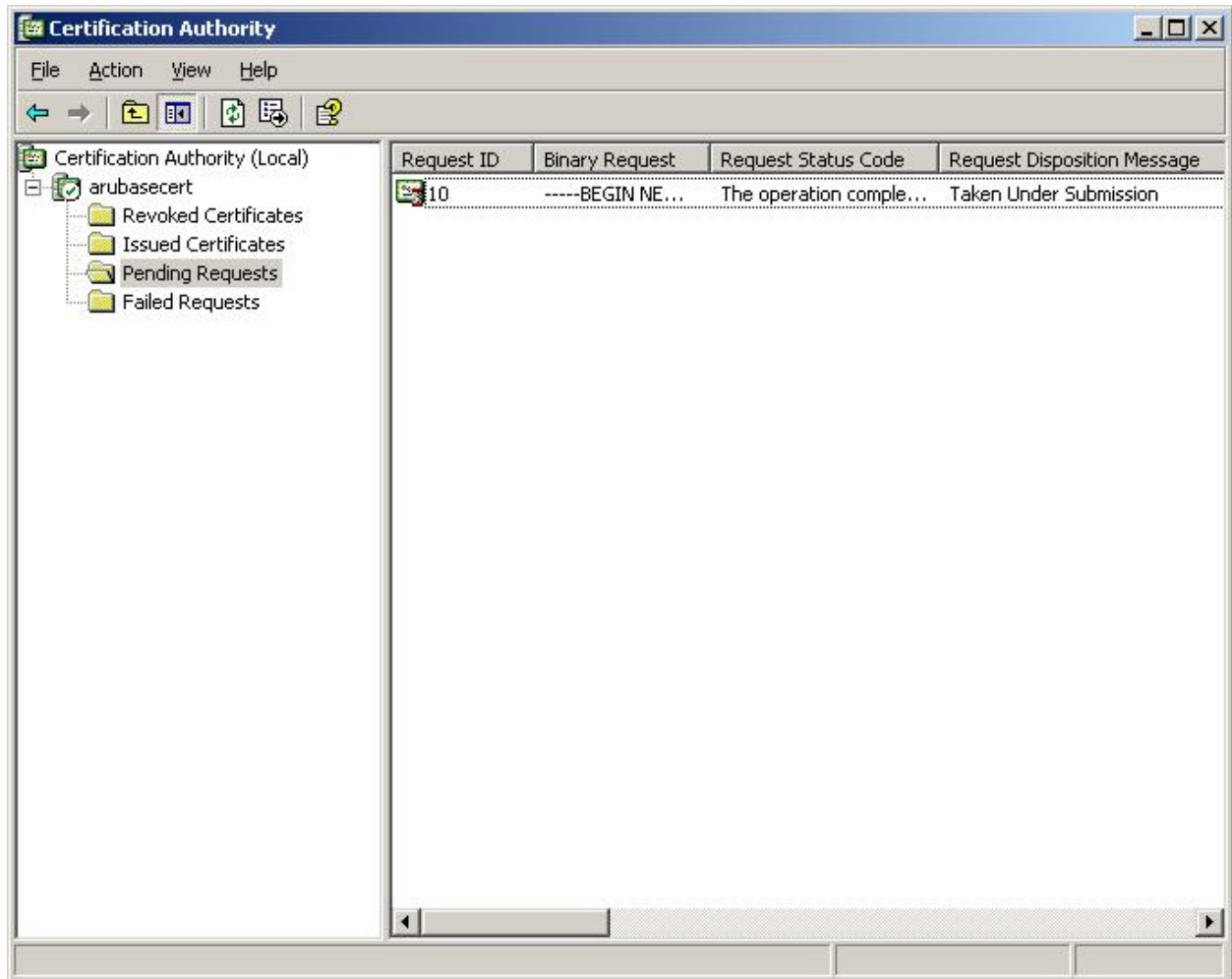
City:

State:

Country/Region:

[More Options >>](#)

- i. 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



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

