

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




a Hewlett Packard
Enterprise company

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

www.arubanetworks.com

▼ Import Certificates

Import Certificates					
NAME	TYPE	FILENAME	REFERENCES	EXPIRED	
master-ssh-pub-cert	PublicCert	master-ssh-pub-cert	--	--	
root-comodo	TrustedCA	comodorsaaddtrustca.crt	--	--	
comodo-intermediate	IntermediateCA	comodorsaaddtrustca.crt	--	--	
	ServerCert	certificado.pfx	--	--	

+

Step 5


Configure the certificate on the controller and save the config.

General Admin AirWave CPSec Certificates SNMP Logging Profiles **More**

> ALE

▼ General

CAPTIVE PORTAL CERTIFICATE

• Server certificate: 

IDP SERVER CERTIFICATE

Server certificate: default

CONFIGURE SSL/TLS PROTOCOL

SSL protocol: TLSv1 TLSv1.1 TLSv1.2

MON Receivers			
TRANSPORT TYPE	SERVER IP	PROFILE	SECURE
udp	master	default-controller	

+

> Mobility Manager Server

> SMTP

Step 6

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

Certificate Trust List + Add

Filter: Subject contains comodo Go Clear Filter Show 20 records

#	Subject	Validity	Enabled
1.	<input type="checkbox"/> CN=COMODO High-Assurance Secure Server CA,O=COMODO CA Limited,L=Salford,ST=Greater Manchester,C=GB	Valid	Enabled
2.	<input type="checkbox"/> CN=COMODO RSA Certification Authority,O=COMODO CA Limited,L=Salford,ST=Greater Manchester,C=GB	Valid	Enabled
3.	<input type="checkbox"/> CN=COMODO RSA Domain Validation Secure Server CA,O=COMODO CA Limited,L=Salford,ST=Greater Manchester,C=GB	Valid	Enabled

Showing 1-3 of 3 Delete

Step 7

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

Login
Options controlling logging in for self-registered guests.

Enabled: Enable guest login to a Network Access Server

* Vendor Settings:
Select a predefined group of settings suitable for standard network configurations.

Login Method:
Select how the user's network login will be handled.
Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.

* IP Address:
Enter the IP address or hostname of the vendor's product here.

Secure Login: Secure login using HTTPS
Select a security option to apply to the web login process.

Dynamic Address: The controller will send the IP to submit credentials
In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.

Security Hash:
Select the level of checking to apply to URL parameters passed to the web login page.
Use this option to detect when URL parameters have been modified by the user, for example their MAC address.

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
```