WLC : Mise en place d’un certificat

>>> Installation d’un certificat délivré par une autorité de certification.

Description :

Le but de cet article est d’expliquer comment générer un CSR depuis le contrôleur wifi, de générer un certificat via une autorité de certification sous Windows Serveur et installer le certificat afin d’obtenir une interface web d’administration du contrôleur wifi en HTTPS avec un certificat signé.

WLC : Mise en place d’un certificat

>>> Installation d’un certificat délivré par une autorité de certification.

Sommaire :

I) Introduction
II) Certificat Racine
1) Vérification du certificat
2) récupération du certificat racine
3) Conversion du certificat racine
4) Installation du certificat racine
5) Vérification du certificat
6) Vérification de l’heure
III) Générer le CSR
IV) Générer et signer le certificat
1) Générer le certificat
2) Conversion du certificat
3) Installation du certificat
V) Vérification du certificat

I) Introduction

Je ne vais pas rappeler comment fonctionne le fonctionnement des certificats, déjà expliqué dans l’article 292.

Voici le résumer de la procédure :

1. Vérifier le certificat en place sur le contrôleur
2. Récupérer le certificat racine de l’autorité de certification
3. Convertir le certificat racine
4. Installer le certificat racine sur le contrôleur
5. Vérifier qu’il est bien installé
6. Générer une demande CSR
7. Générer un certificat sur l’autorité de certification
8. Convertir le certificat
9. Installer le certificat

Informations : Le contrôleur wifi, ne supporte que les certificats de type PEM. Une autorité de certification Windows ne sait malheureusement pas générer de tel certificats. Il vous faudra donc installer OpenSSL sur votre serveur Windows ou sur votre PC afin de convertir les certificats dans le format demandé.

II) Certificat Racine

1) Vérification du certificat

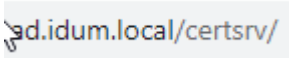
Nous commençons donc par vérifier le certificat en place.
- Connectez-vous sur la page d'administration du contrôleur Wifi.
- Cliquez sur **"Management"** dans la barre du haut.
- Puis cliquez sur **"HTTP-HTTPS"** dans le menu de gauche.
- Vous pouvez observer que le certificat actuel est au nom de Cisco Systems avec un CN "169.254.1.1".



2) récupération du certificat racine

Nous allons maintenant récupérer le certificat racine depuis l'autorité de certification.

- Connectez-vous à l'interface WEB de l'autorité pour moi : "http://ad.idum.local/certsrv" et authentifiez-vous avec un compte ayant les droits de générer les certificats.



- Cliquez sur **"Télécharger un certificat d'autorité de certification, une chaine de certificats ou une liste de révocation des certificats"**.



– Sélectionnez le certificat, sélectionnez la méthode DER, et cliquez sur **"Télécharger la chaine de certificats d'autorité de certification"**.



3) Conversion du certificat racine

Comme expliqué dans l'introduction, le contrôleur wifi de supporte que le format PEM. Il faut donc convertir le certificat racine de P7B en PEM.

– Installez **"OpenSSL"** sur votre PC.
– Puis tapez la commande ci-dessous pour convertir le certificat racine.

```
OpenSSL> pkcs7 -in C:\Certs\CA-root-infra-local.p7b -inform DER -print_certs -text -out C:\Certs\CA-root-infra-local.pem
```

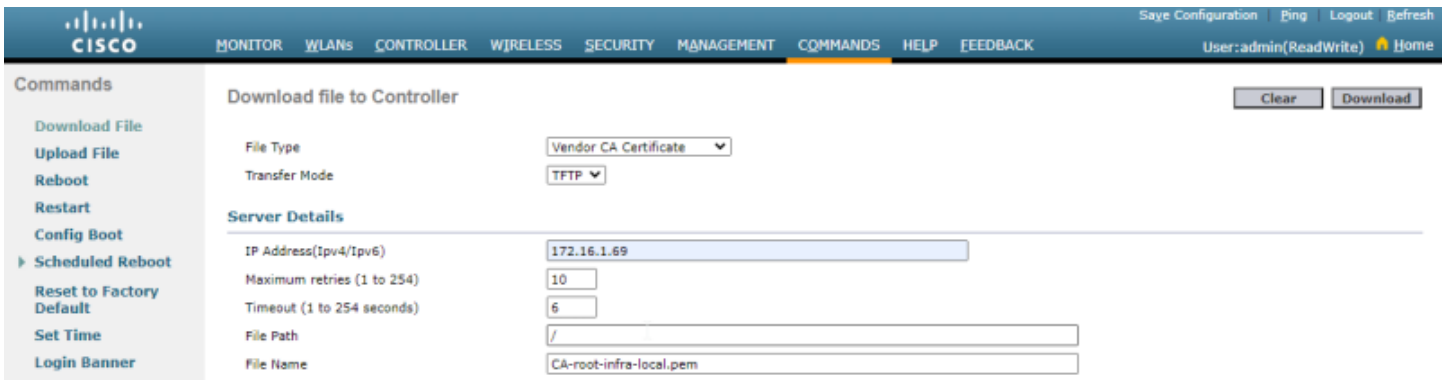
OpenSSL> pkcs7 -in C:\Certs\CA-root-infra-local.p7b -inform DER -print_certs -text -out C:\Certs\CA-root-infra-local.pem

4) Installation du certificat racine

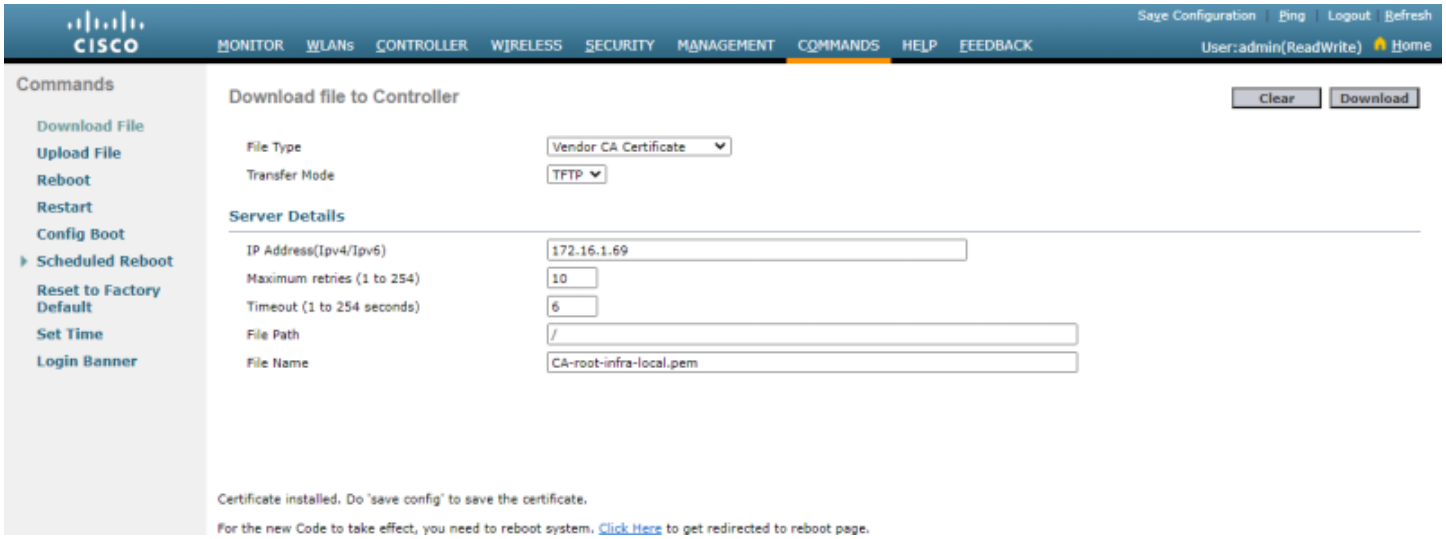
– Retournez sur la page d'administration du contrôleur Wifi.
– Cliquez sur **"Commands"** dans le menu du haut.
– Cliquez sur **"Download File"**.
– Sélectionnez :

- Le file type : **"Vendor CA Certificate"**
- Le type de transfert que vous souhaitez
- L'adresse IP du serveur TFTP ou FTP
- Le chemin
- Et le nom du fichier PEM

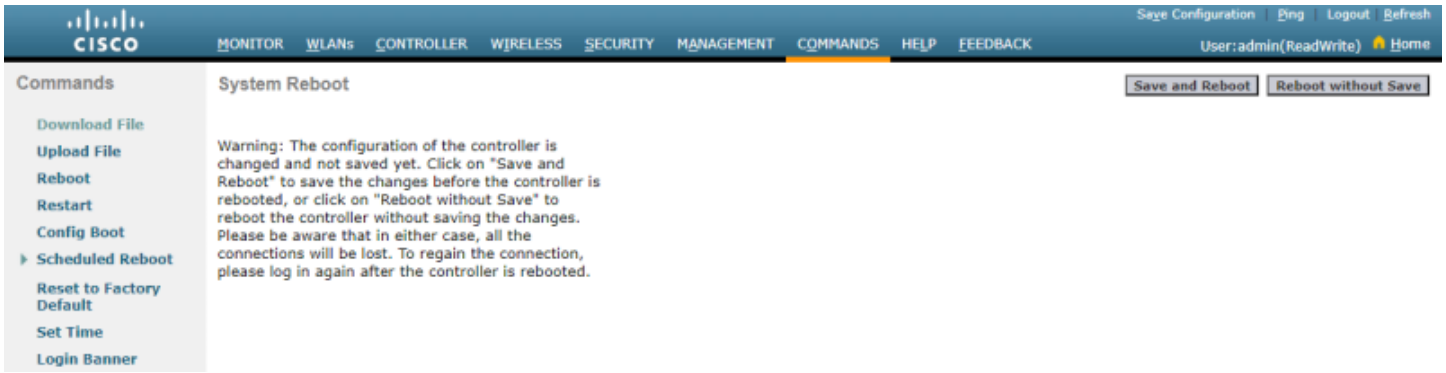
– Cliquez sur **"Download"**.



- Si l'opération se déroule bien, le contrôleur vous demandera de redémarrer.

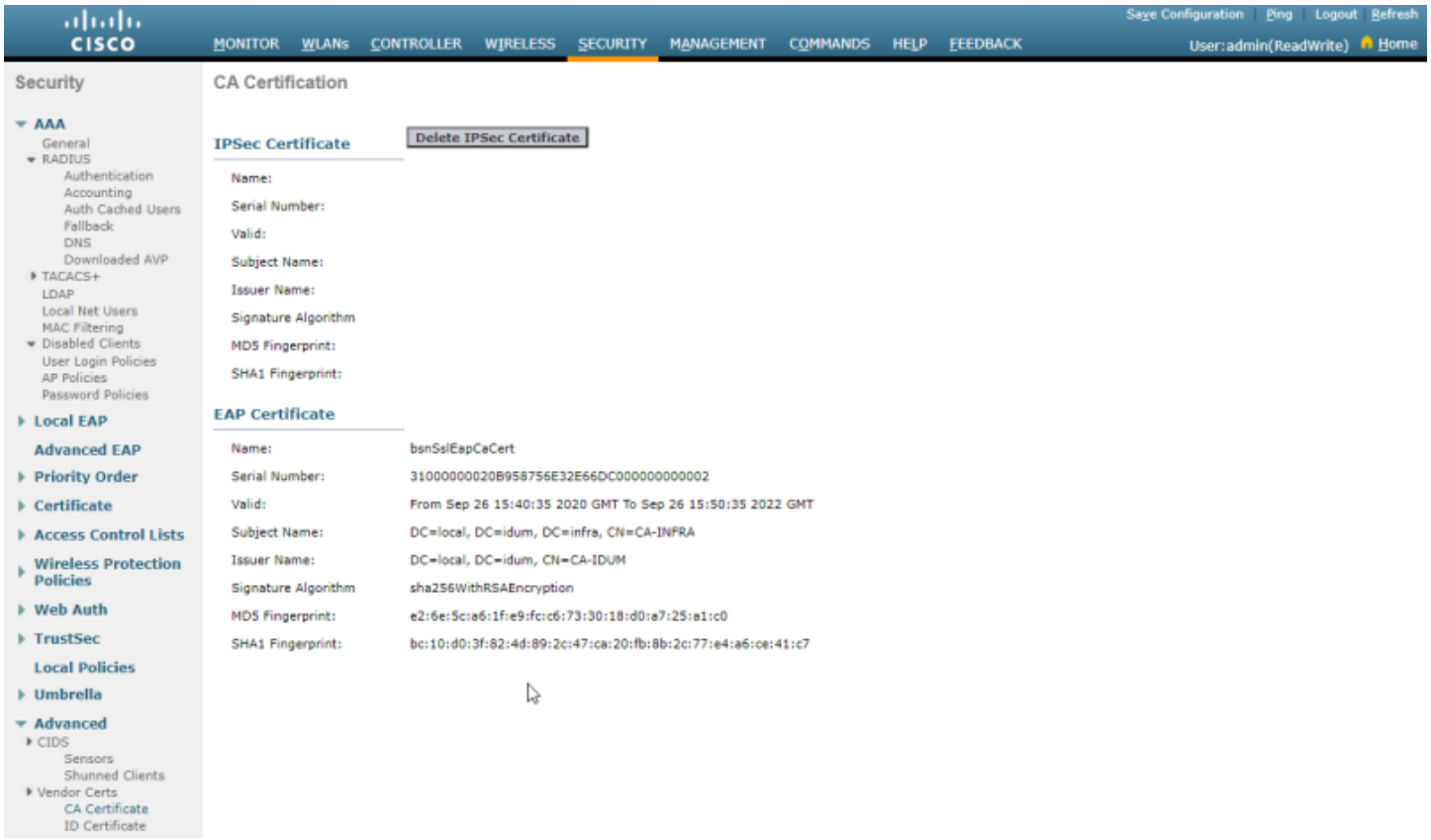


- Cliquez sur **"Save and Reboot"**



5) Vérification du certificat

On vérifie que le certificat racine est bien en place.
- Cliquez sur **"Security"** dans la barre du haut.
- Cliquez sur **"Advanced"** dans le menu de gauche.
- Puis sur **"Vendor Certs"**
- Et enfin sur **"CA certificate"**
- Vous pouvez observer que le certificat est au nom de : **"DC=local, DC=idum, DC=infra, CN=CA-INFRA"**



6) Vérification de l’heure

Pour tout ce qui touche au certificat, l’heure des équipements sont important.

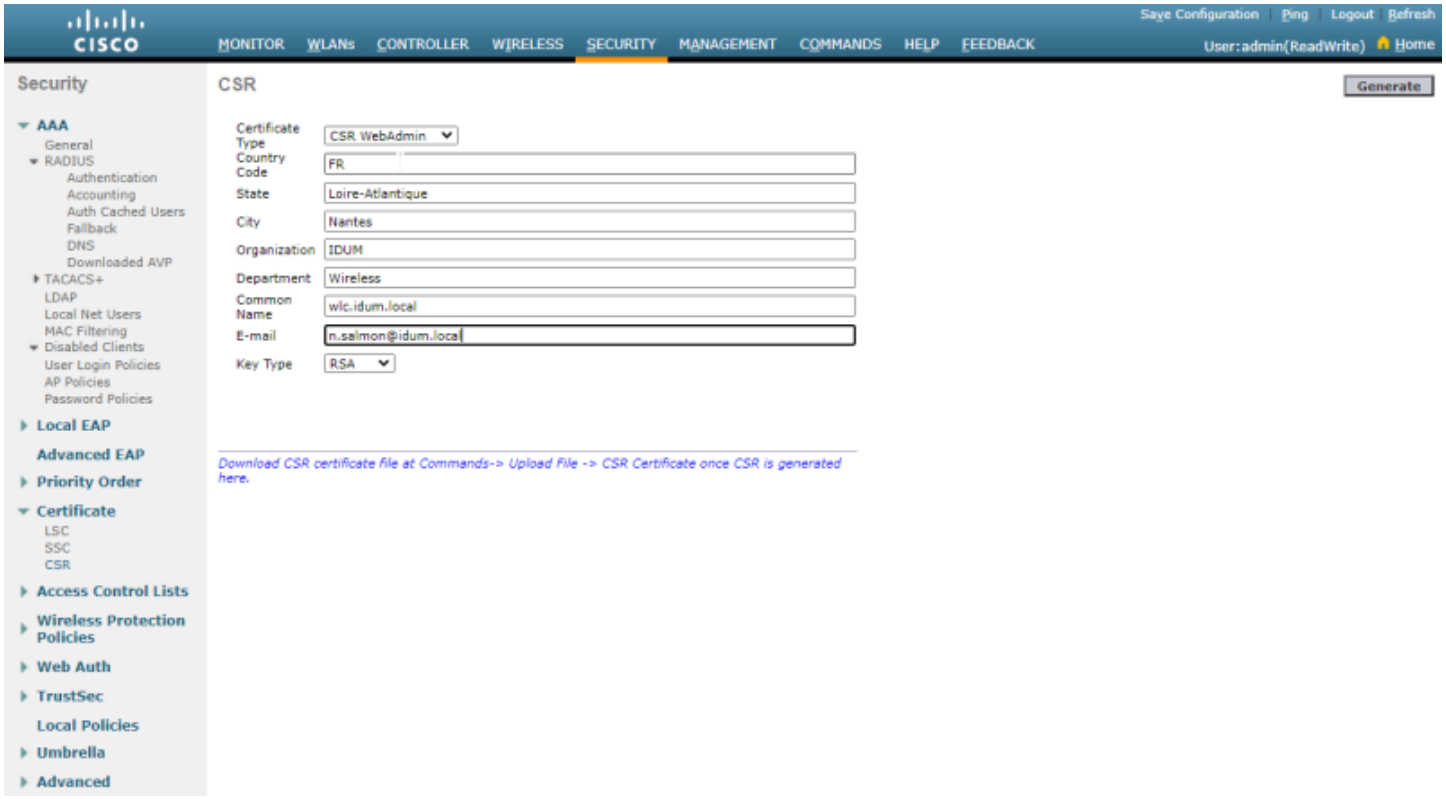
- Cliquez sur **"Commands"** en haut de la page.
- Cliquez sur **"Set Time"**.
- puis vérifiez le **"Current Time"** de votre contrôleur.



III) Générer le CSR

Nous allons maintenant générer la demande de certificat.
- Cliquez sur **"Security"** en haut de la page.
- Cliquez sur **"Certificate"** sur la gauche.
- Puis sur **"CSR"**.
- Sélectionnez le type de certificat : **"CSR WebAdmin"**.
- Remplissez les champs.

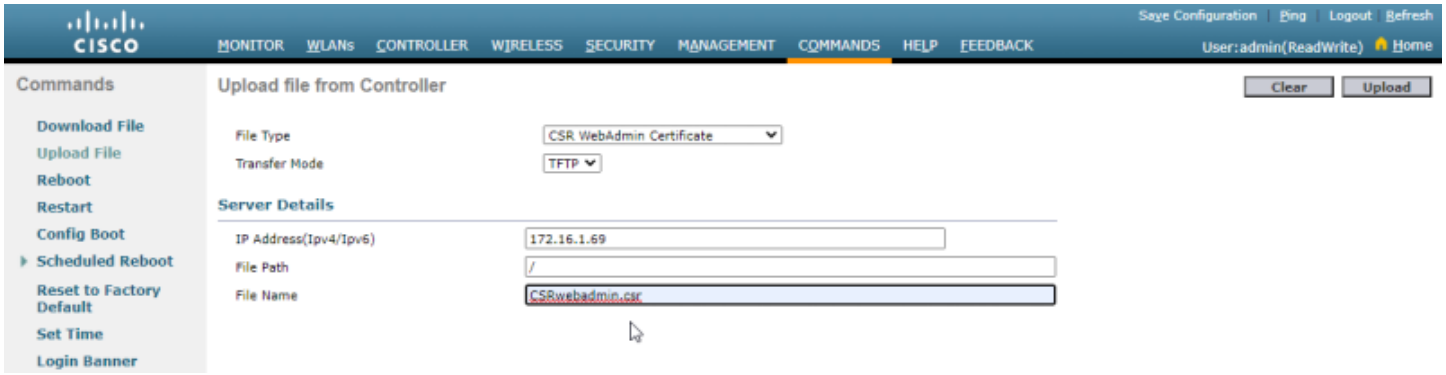
- Et cliquez sur "**Generate**".



- Cliquez sur "**Commands**" en haut de la page.
- Puis sur "**Upload**" à gauche.
- Sélectionnez :

  - Le type de fichier : "**CSR WebAdmin Certificate**"
  - L'adresse IP
  - Le chemin
  - Le nom du fichier

- Puis cliquez sur "**Upload**".



IV) Générer le certificat

1) Générer le certificat

- Retournez sur la page WEB de l'autorité de Certification.
- Cliquez sur "**Demander un Certificat**".



- Cliquez sur **"Soumettez une demande de certificat en utilisant un fichier CMC ou PKCS #10 codé en base 64, ou soumettez une demande en utilisant un fichier PKCS #7 codé en base 64."**



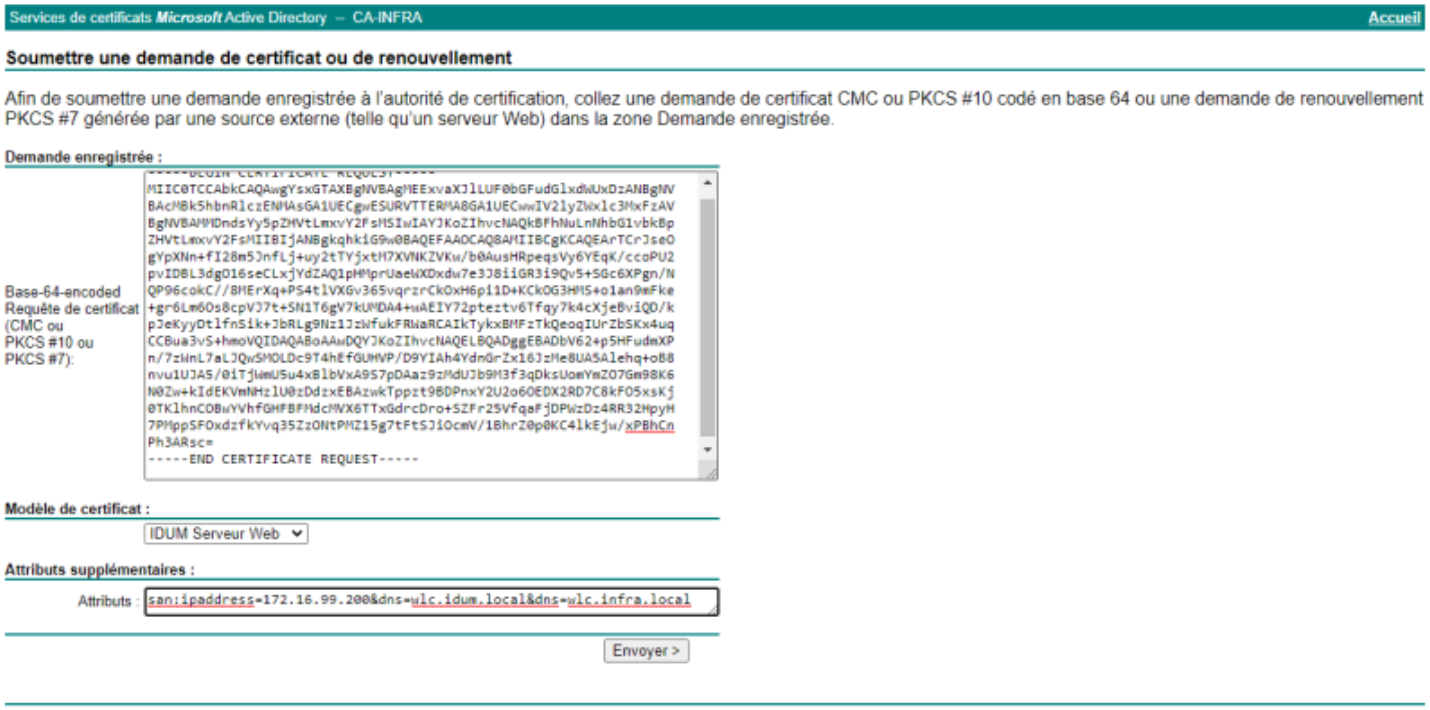
- Ouvrez dans un éditeur de texte le fichier CSR.
- Copiez tout le contenu.
- Collez le contenu dans la zone **"Demande enregistrée"**.
- Sélectionnez le modèle de Certificat.
- Ajoutez les attributs supplémentaires ci-dessous :

```
san:ipaddress=172.16.99.200&dns=wlc.idum.local&dns=wlc.infra.local
```

- Cliquez sur **"Envoyer"**

Pour résumer :
- Spécifiez l'adresse IP du contrôleur de la page administration.
- Spécifiez le nom DNS du contrôleur (nom qui sera utilisé dans le navigateur pour joindre la page d'administration du contrôleur).

Information : Dans mon cas le nom de domaine et idum.local, mais je possède aussi un sous-domaine infra.local



- Sélectionnez la méthode DER, et cliquez sur **"Télécharger la chaine de certificats"**



2) Conversion du certificat

Comme précédemment, utilisez OpenSSL pour convertir le certificat P7B en PEM. Utilisez la commande suivante :

```
OpenSSL> pkcs7 -in C:\Certs\cert_webadmin.p7b -inform DER -print_certs -text -out C:\Certs\Cert_webadmin.pem
```

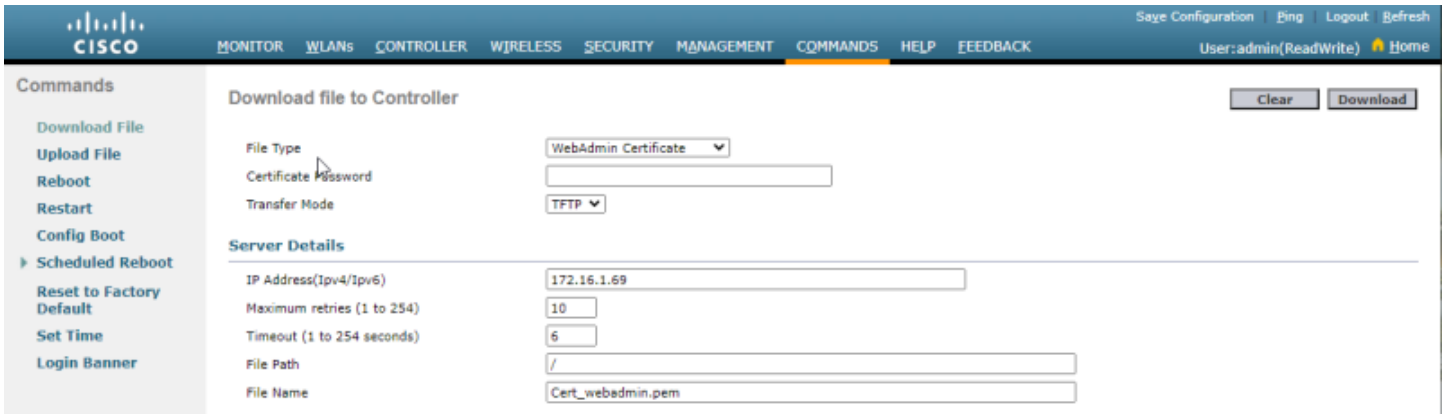
OpenSSL> pkcs7 -in C:\Certs\cert_webadmin.p7b -inform DER -print_certs -text -out C:\Certs\Cert_webadmin.pem

3) Installation du certificat

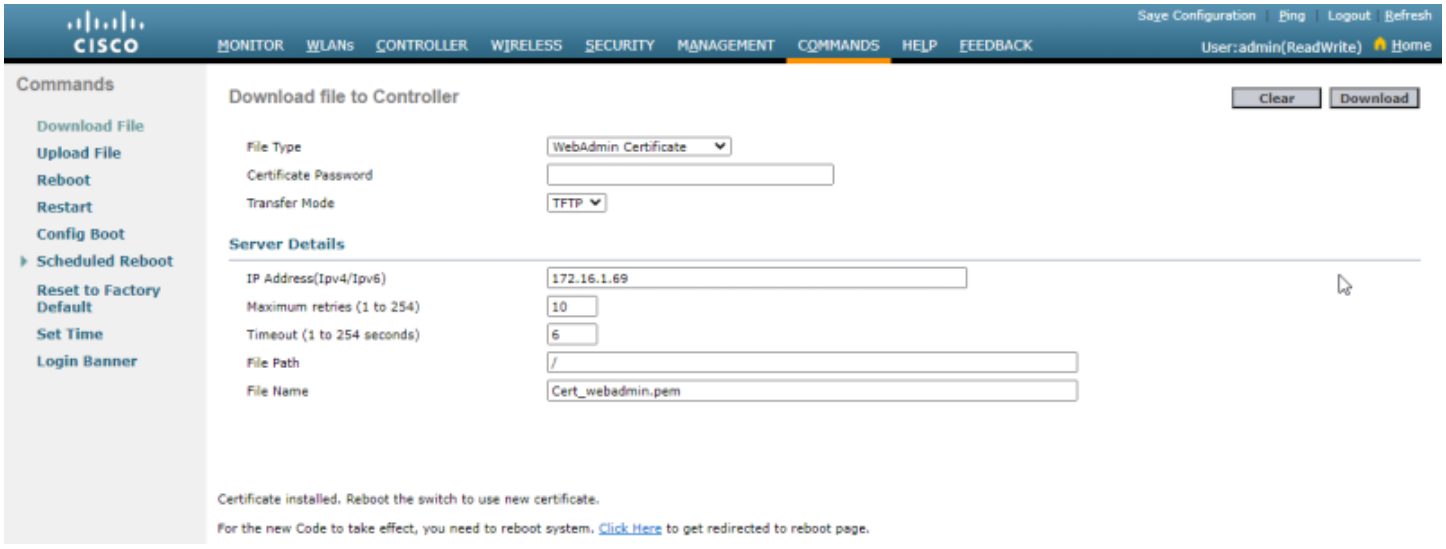
- Dans **"Commands"** en haut de la page, puis dans **"Download File"**.
- Sélectionnez :

- Le file type : **"WebAdmin Certificate"**
- Le type de transfert que vous souhaitez
- L'adresse IP du serveur TFTP ou FTP
- Le chemin
- Et le nom du fichier PEM

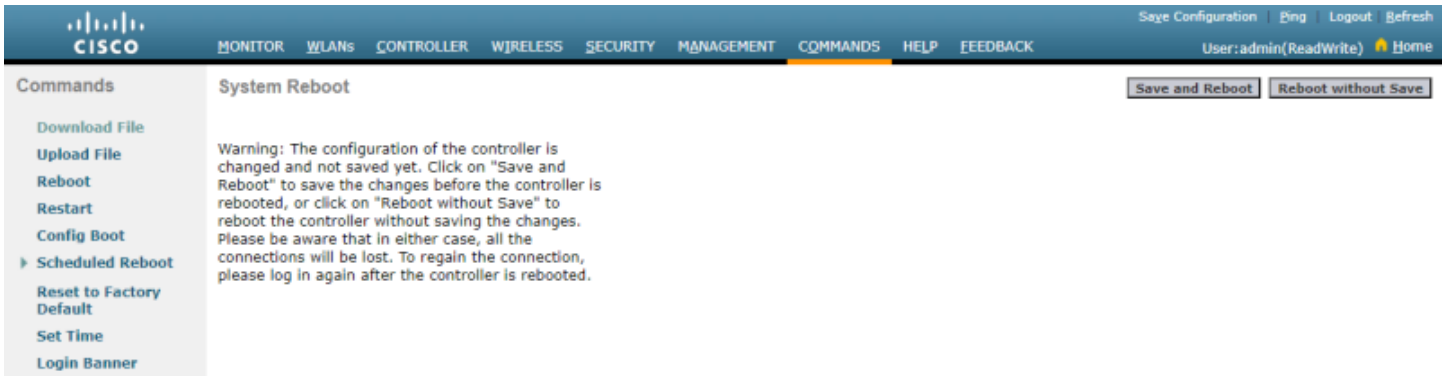
- Cliquez sur **"Download"**



- Si l'opération se déroule bien, le contrôleur vous demandera de redémarrer.



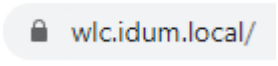
- Cliquez sur **"Save and Reboot"**



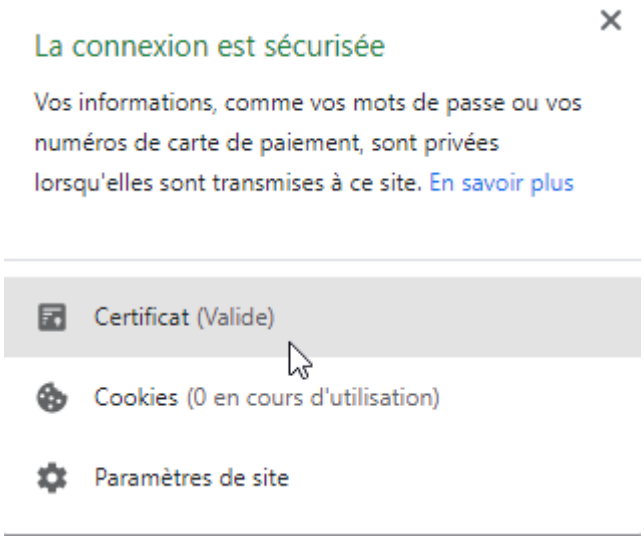
V) Vérification du certificat

Pour conclure cet article, la vérification pour valider que le certificat est bien installé :

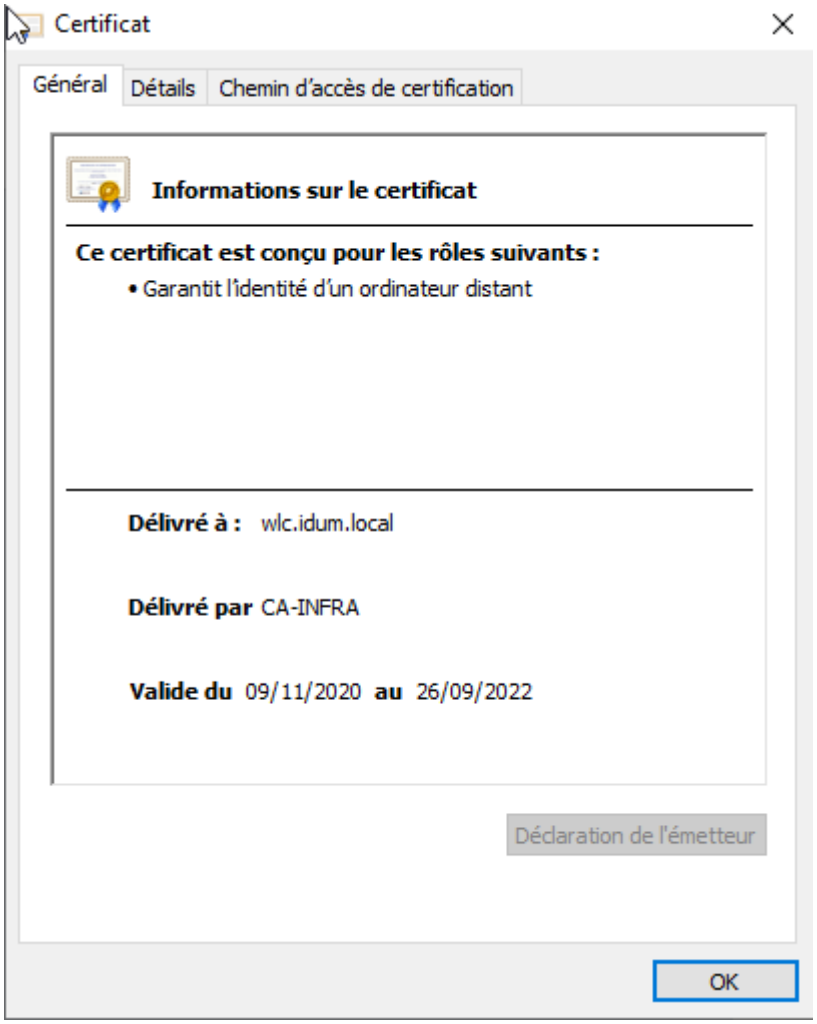
- Attendez que le contrôleur Wifi ait redémarré.
- Fermer et rouvrez le navigateur sur la page administration.
- Vérifier que votre navigateur vous informe bien que le certificat est valide avec un cadenas.



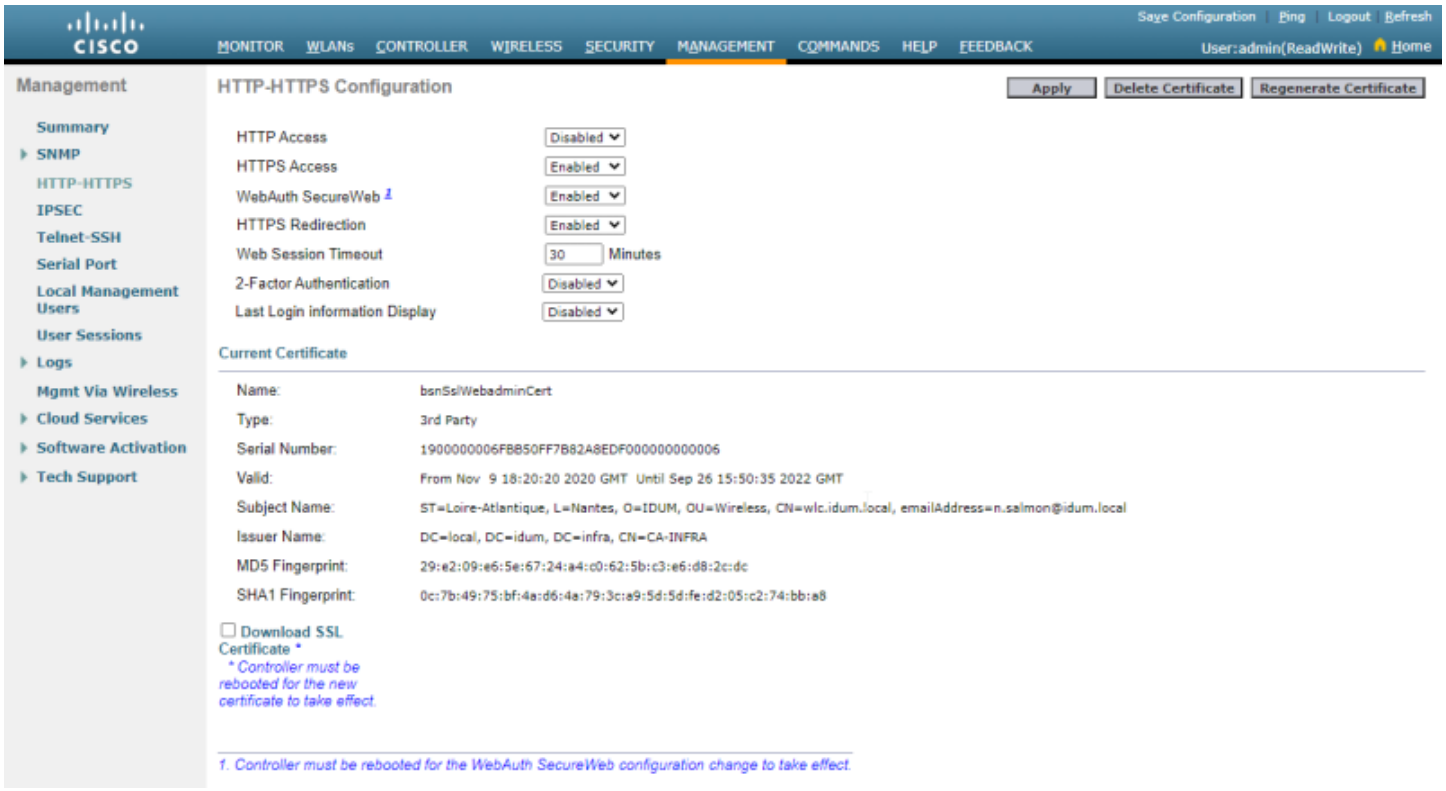
- Cliquez dessus pour voir l'information **"Certificat (valide)"**



- Cliquez dessus afin de voir le détail et vérifier que le certificat est bien signé par votre autorité de certification.



- N'hésitez pas aussi à regarder dans le menu "**Management**" puis "**HTTP-HTTPS**"



Il vous restera à faire la même chose pour le Webauth si vous l'utilisez.

Attention : N'oubliez pas que le certificat Racine doit être installé sur le PC afin de pouvoir authentifier et valider le certificat.