ACCESS POINT C9115AXE-EWC

Ardy OCKANDJI

CFA PAYS DE MONTBELIARD RUE DES FRERES LUMIERES

Table des matières

Introduction

Ce document reprend de manière générale, l'ensemble des étapes que j'ai effectuées. C'est un suivi chronologique d'une première approche d'installation et d'un premier contact avec un tel appareil type Cisco. Il sert donc de prise en main rapide ; les équipements Cisco ayant sensiblement des procédures d'administration similaires. En effet, les matériels Cisco sont bien documentés et la plupart des ressources sont disponibles sur Internet avec une grande communauté.

Vous l'aurez compris, je reprends et explique, en quelques mots, toute la configuration que j'ai mise en place. Si vous souhaitez, pour diverses raisons, modifier la configuration en place, veuillez prendre connaissance de mon installation directement à Administration du point d'accès. Si vous désirez uniquement ajouter une borne dans le parc, rendez-vous à Ajout d'une borne (de même modèle potentiellement). Sinon vous pouvez parcourir tout le document !

Bonne lecture et compréhension.

À propos du point d'accès (Cf. fichier pdf)

La série d'Access points sans fil Cisco Catalyst 9115AX est un AP double bande, double simultané, compatible avec la norme 802.11ax pour les entreprises. Cette série d'AP propose des options d'antennes intégrées et externes, conçues pour utiliser à la fois les bandes 2,4 GHz et 5 GHz. Cet access point prend en charge une expérience haute densité (HDX) globale accrue, offrant des performances plus prévisibles pour des applications avancées telles que la vidéo 4K ou 8K, les applications de collaboration haute définition à haute densité, les bureaux entièrement sans fil et l'Internet des objets (IoT). L'access point prend en charge une interopérabilité complète avec les clients 802.11ax et 802.11ac leaders du marché, et permet un déploiement mixte avec d'autres access points et contrôleurs.

Caractéristiques de l'Access point :

- Antennes externes sur les modèles d'Access point 9115AXE (C9115AXE-x et C9115AXE-EWC-x).
- Antennes internes intégrées, omnidirectionnelles en azimut pour les bandes 2,4 GHz (gain maximal de 3 dBi) et 5 GHz (gain maximal de 4 dBi).
- MIMO 4x4 simultané avec quatre flux spatiaux pour les bandes 2,4 GHz et 5 GHz.
- Interfaces matérielles externes comprenant un port Ethernet multi gigabit 100/1000/2500 (RJ-45), une interface console RS-232 via RJ-45, un bouton de récupération (permettant une récupération partielle ou complète de la configuration système), un port USB 2.0 et un indicateur d'état à LED multicolore.
- Technologie Multi user Multiple-Input Multiple-Output (MU-MIMO) avec 4 flux spatiaux pour la liaison descendante.
- Planification basée sur l'accès multiple par répartition orthogonale de la fréquence (OFDMA) pour la liaison descendante et la liaison montante.

- Réutilisation spatiale (également appelée coloration BSS) permettant aux AP et à leurs clients de différencier les BSS, autorisant ainsi davantage de transmissions simultanées.
- Prise en charge du Cisco Catalyst Center pour les expériences mobiles connectées de Cisco, Apple Fast Lane et Cisco Identity Services Engine.
- Roaming AP optimisé pour garantir que les appareils clients s'associent à l'AP dans leur zone de couverture offrant le débit de données le plus rapide disponible.
- Capacités d'égalisation MIMO, qui optimisent les performances et la fiabilité de la liaison montante en réduisant l'impact de la dégradation du signal.

L'AP prend en charge à la fois les déploiements avec contrôleur sans fil intégré Cisco (Cisco Embedded Wireless Controller) et les déploiements légers (utilisant les contrôleurs sans fil Cisco).

Le point d'accès est alimenté en PoE **(standards 802.3af ou 802.3at)**.

Une fois alimenté, le point d'accès peut être administré de trois façons :

- **En console via RJ-45 (9600-8-N-1)**

Vous pouvez utiliser n'importe client (Minicom, PuTTY, etc.).

Se connecter avec username **cisco** ou **webui** password **cisco.**

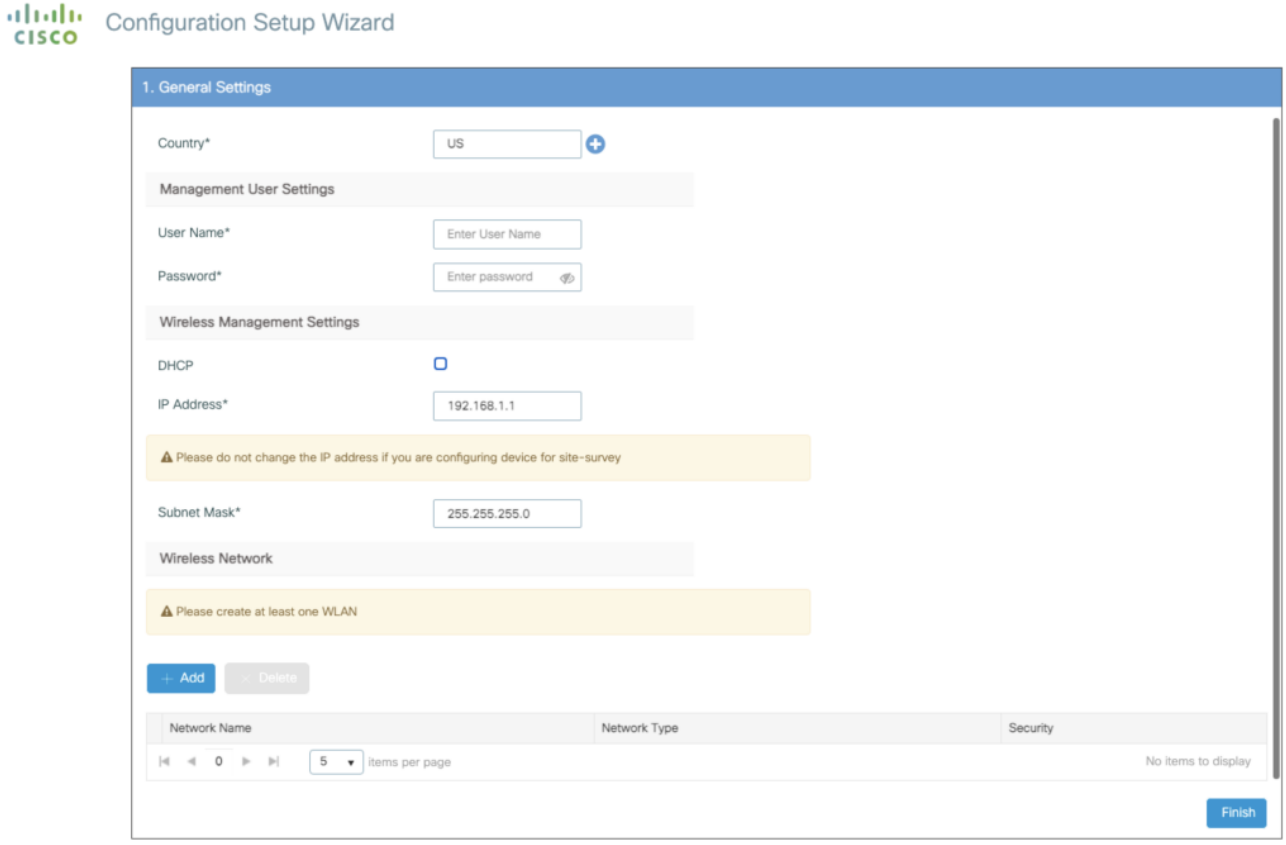
- **Via SSH**

Se connecter en filaire au réseau du point d'accès (DHCP actif). Sinon se mettre en statique dans le réseau **192.168.1.0/24 (ne pas utiliser la première adresse).** L'adresse pour la passerelle par défaut et le DNS est **192.168.1.1** (à préciser obligatoirement).

Ensuite avec un client SSH (Terminal, PuTTY, etc.), se connecter au point d'accès (username **cisco** ou **webui** password **cisco**).

- **Via le Web**

Faire cette manœuvre de nouveau ou utiliser le réseau sans fil diffusé par défaut **CiscoAirProvision-XXXX.** Se connecter avec la clé **password**. Le réseau vous redirige automatiquement vers l'interface web. Sinon, tapez soit « **mywifi.cisco.com** » ou **192.168.1.1** depuis un navigateur.



Remarque : l'ensemble des configurations présentées ici se font hors du réseau. J'ai utilisé la configuration réseau de base de l'AP et je l'ai intégré au réseau de l'entreprise à la fin.

Si vous souhaitez directement travailler en étant connecté au réseau, il vous suffit de réserver une adresse IP pour l'AP ou de modifier uniquement la configuration réseau de base de l'AP afin qu'il soit dans le réseau (IP, masque, DNS, hostname, etc.).

1. Prise en main (0day configuration)

- **0day via console ou SSH**

----------Configuration du nom et d'un utilisateur administrateur----------

WLC7069.5A74.7C78#conf t

WLC7069.5A74.7C78(config)#hostname C9800-EWC

C9800-AP(config)# username **UnNomDutilisateur** privilege 15 password **UnPassword**

----------Configuration du profil des AP----------

C9800-AP(config)#ap profile **NomDuProfil**

C9800-AP(config-ap-profile)#mgmtuser username **UnNomDutilisateur** password 0 **UnPassword** secret 0 **UnPassword (même)**

C9800-AP(config-ap-profile)#end

----------Configuration d'un WLAN----------

C9800-AP(config)# wlan **NomDuProfilWLAN NumeroWLAN(1) NomDuReseauWLAN**

C9800-AP(config-wlan)# no security wpa akm dot1x

C9800-AP(config-wlan)# security wpa psk set-key ascii 0 **CleDuReseauWifi**

C9800-AP(config-wlan)# security wpa akm psk

C9800-AP(config-wlan)# no shutdown

C9800-AP(config-wlan)#end

----------Configuration du profil de stratégie des WLANs----------

C9800-AP#conf t

C9800-AP(config)#wireless profile policy **NomDuProfilWLAN**

C9800-AP(config-wireless-policy)#no central association

C9800-AP(config-wireless-policy)#no central dhcp

C9800-AP(config-wireless-policy)#no central switching

C9800-AP(config-wireless-policy)#http-tlv-caching

C9800-AP(config-wireless-policy)#session-timeout 86400

C9800-AP(config-wireless-policy)#no shutdown

C9800-AP(config-wireless-policy)#end

----------Taguer le WLAN (pour être diffusé) ----------

C9800-AP#conf t

C9800-AP(config)#wireless tag policy **NomPolicyTag**

C9800-AP(config-policy-tag)#wlan **NomDuProfilWLAN** policy **NomDuProfilWLAN**

C9800-AP(config-policy-tag)#end

----------Chiffrement global des mots de passe----------

C9800-AP#conf t

C9800-AP(config)#service password-encryption

C9800-AP(config)#password encryption aes

C9800-AP(config)#key config-key newpass **UnPassword**

C9800-AP(config)#end

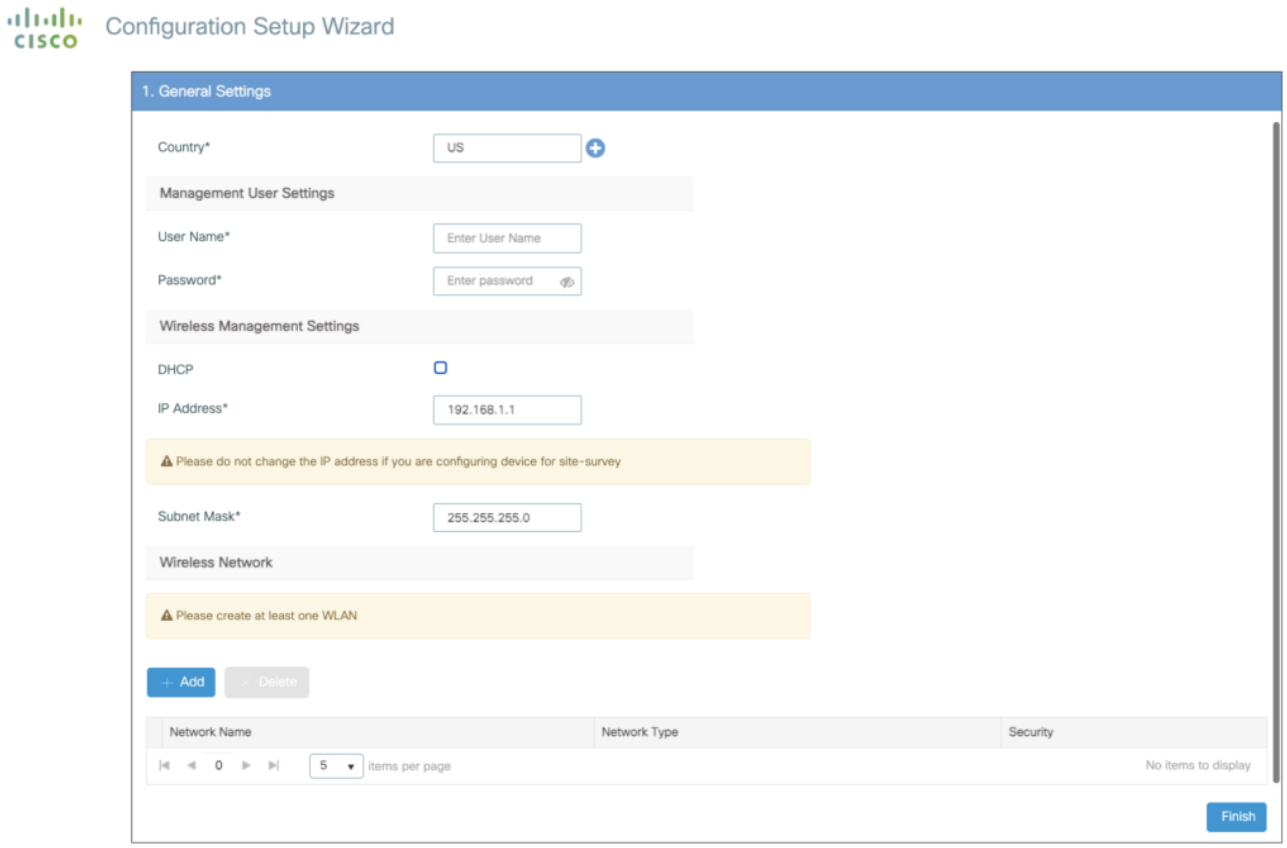
----------Sauvegarde de la configuration----------

C9800-AP# write memory

- **Via Web**

Consiste à se connecter au WLAN par défaut et de suivre les étapes qui vous sont proposées.

Si le WLAN par défaut ne vous donne pas d'adresse en DHCP, connectez-vous en filaire et configurez votre réseau en statique, toujours dans le réseau **192.168.1.0/24.** L'adresse pour la passerelle par défaut et le DNS est **192.168.1.1**.



.

2. Mise à niveau du logiciel

Version de base du système (pour notre matériel) : **Cisco IOS XE Gibraltar 16.12.x**

(Le point d'accès doit être mis à niveau).

Les fichiers binaires se trouve dans **Téléchargements**.

Remarques :

- Pour un même modèle, **C9115AXE-EWC** par exemple, les points d'accès doivent avoir la même version système ;
- Une fois la mise à jour ou la mise à niveau faite sur le contrôleur, elle se répliquera sur tous les points d'accès du parc. Donc à ne faire que sur le contrôleur **C9800-EWC** ;
- S'assurer d'avoir pris assez d'informations avant d'appliquer l'update ou upgrade. Cela peut générer des dysfonctionnements si elle ne concerne pas à la région par exemple.

La mise à niveau peut se faire soit en SSH (pas simple) soit via Web (intuitif)

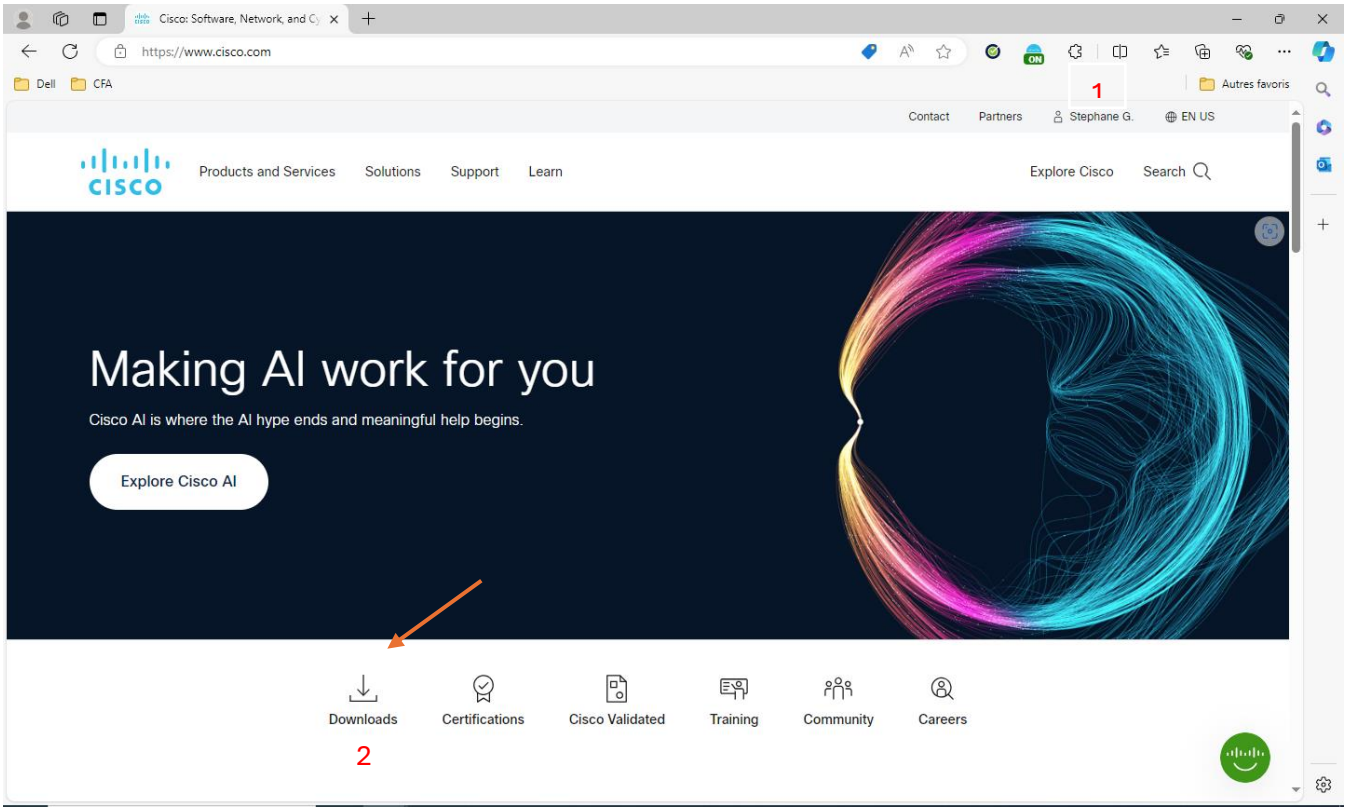
- **Via SSH** (je le mentionne pour information. Les commandées à taper peuvent être retrouvées sur Internet, avec quelques subtilités.)

Cela nécessite :

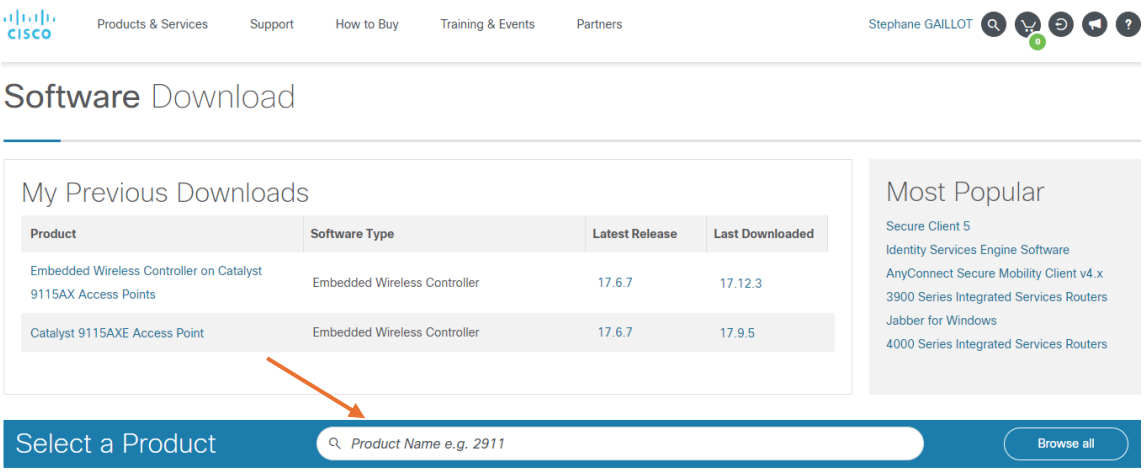
- Un serveur TFTP
- Les images : **ap1g7** (spécifique à notre modèle, C9115AXE) et **C9800-AP-iosxe-wlc.bin** (logiciel de contrôleur embarqué).

Pour télécharger les images :

Se rendre sur https://www.cisco.com, s'authentifier. Après connexion, cliquez sur **« Downloads »**



Vous êtes redirigé vers la page ci-dessous. Là vous pouvez entrer le nom du matériel. Pour nous **Catalyst 9115AXE.**



Choisissez ensuite à la prochaine étape **« Embedded Wireless Controller ».** Puis téléchargez la dernière version. Lors de la saisie de ce document, nos appareils possèdent la version **Cisco IOS XE Software, Version 17.09.05.**

Extraire le fichier téléchargé depuis l'espace de notre compte Cisco.

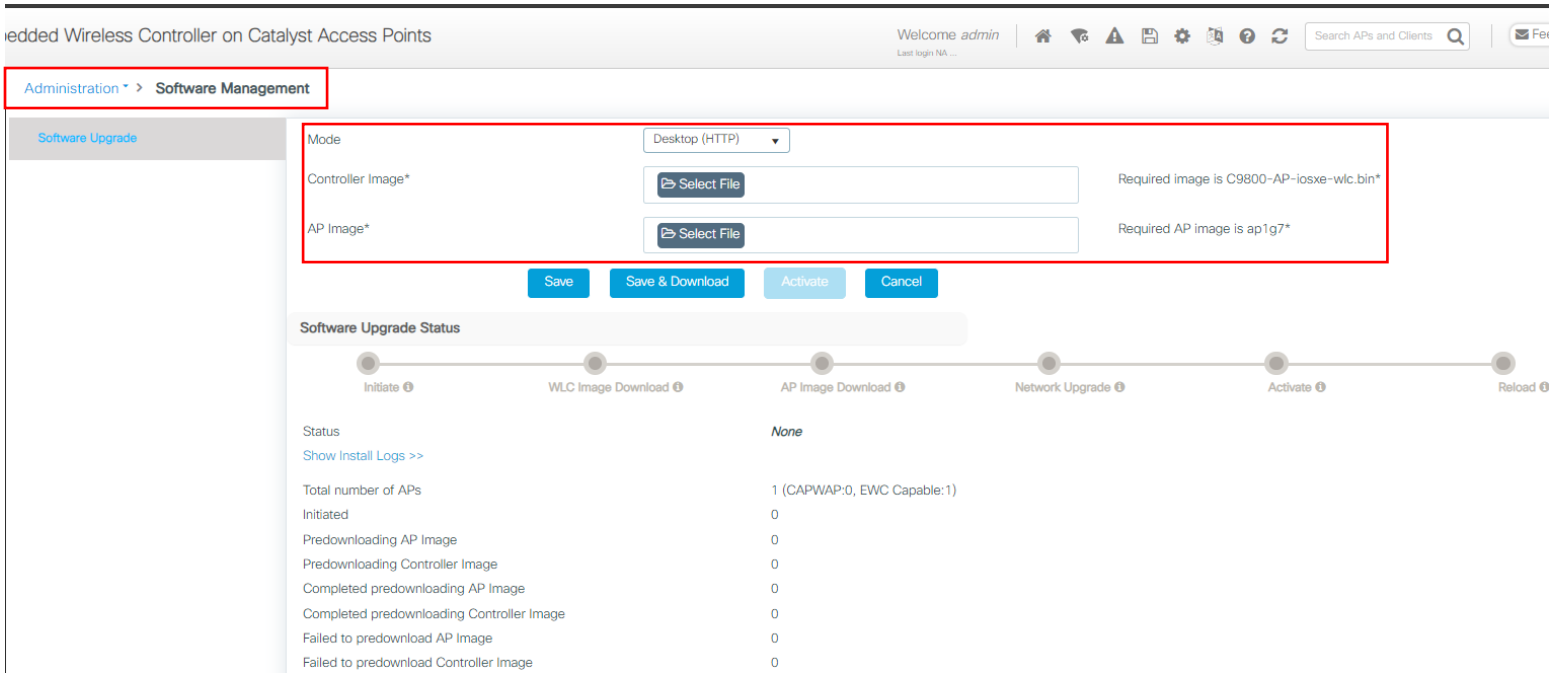
Faire la manipulation de la partie SSH

L'upgrade n'est possible qu'avec un serveur TFTP, dans le même réseau bien sûr, contenant les images : **ap1g7** (spécifique à notre modèle, C9115) et **C9800-AP-iosxe-wlc.bin** (logiciel de contrôleur embarqué).

- **Via le Web**

Se connecter au réseau Wifi, accéder à l'interface Web d'administration. S'authentifier avec les codes d'accès.

Ensuite aller à l'onglet **« Administration »** et choisir **« Software Management »** dans le choix des méthodes, mettre **« Desktop (HTTP) »** puis téléverser les fichiers demandés parmi les téléchargés.



Puis appuyer sur **« Save & Download »**. Lorsque le bouton « **Activate »** sera actif, cliquez dessus et attendre la fin de l'opération. Elle peut durer jusqu'à 15 minutes.

Le point d'accès va redémarrer et vous pourrez passer à la configuration.

3. Administration du point d'accès

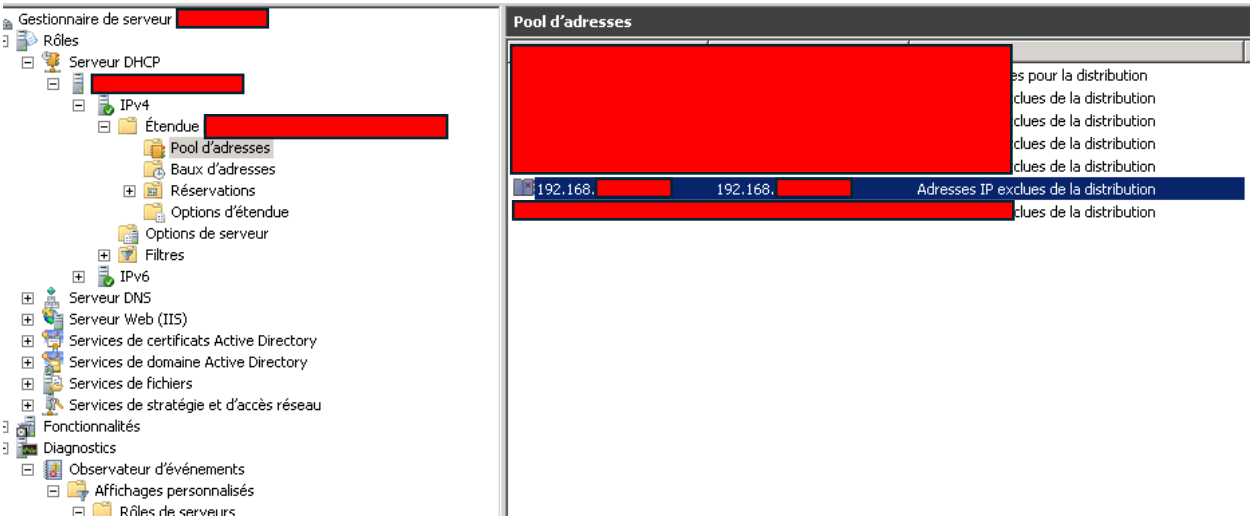
Pour l'installation que j'ai choisie, il est nécessaire d'apporter des modifications au serveur. Je vais donc vous présenter les actions réalisées sur le serveur et le point d'accès. Je dirai brièvement ce qui est fait.

a) Sur le serveur

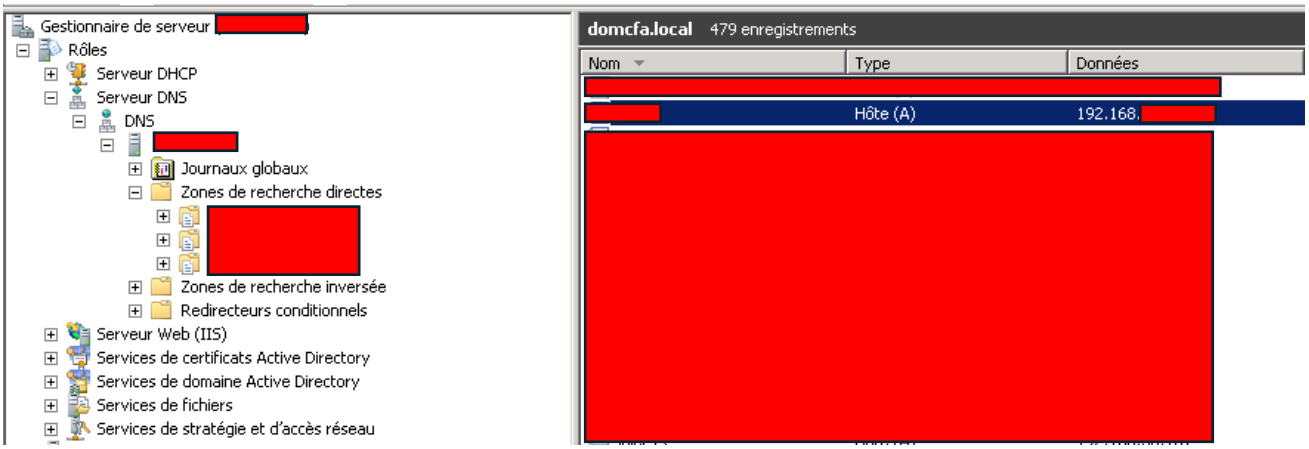
J'ai mis en place un réseau sans fil d'entreprise. Pour cela, je prépare déjà la configuration réseau sur le serveur avec une réservation d'adresse en DHCP et je crée un enregistrement DNS associé à cette adresse.

Réservation d'adresse

Aussi, j'ai exclu une adresse afin qu'aucun autre hôte ne la reçoive. C'est l'adresse de l'interface filaire du point d'accès. On peut le voir ci-dessous.



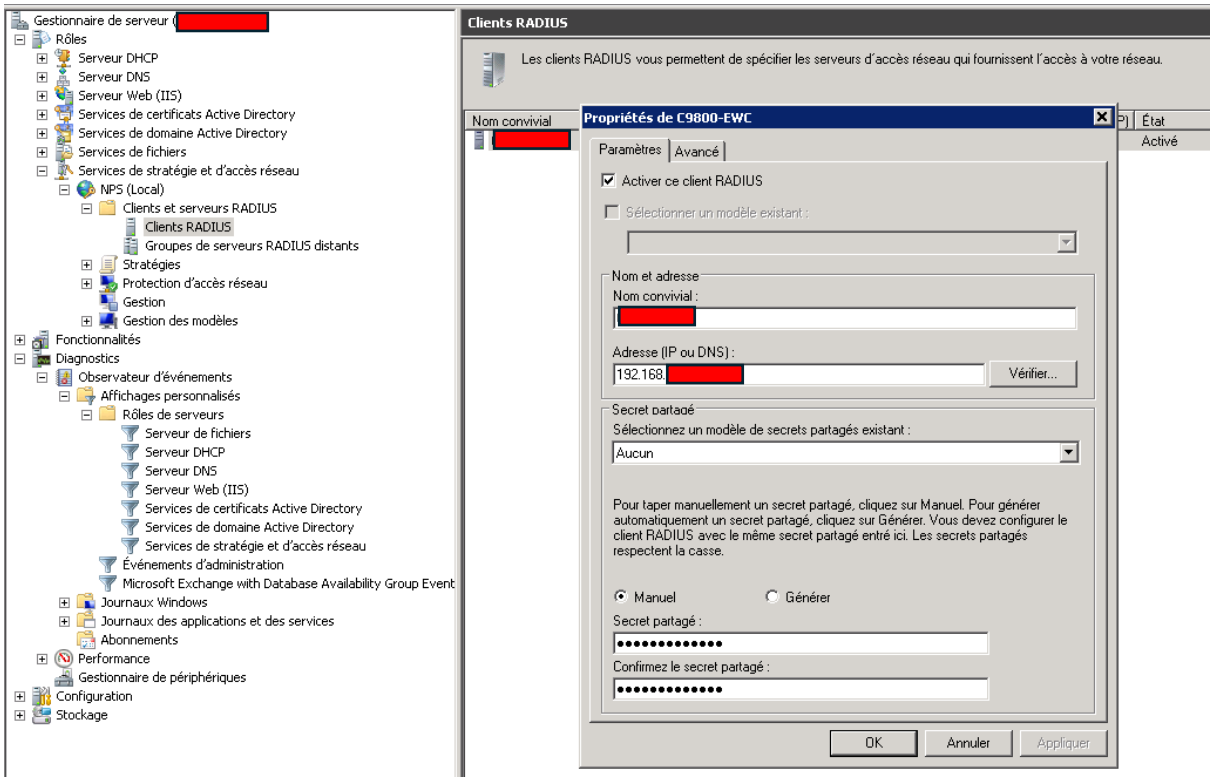
Enregistrement DNS



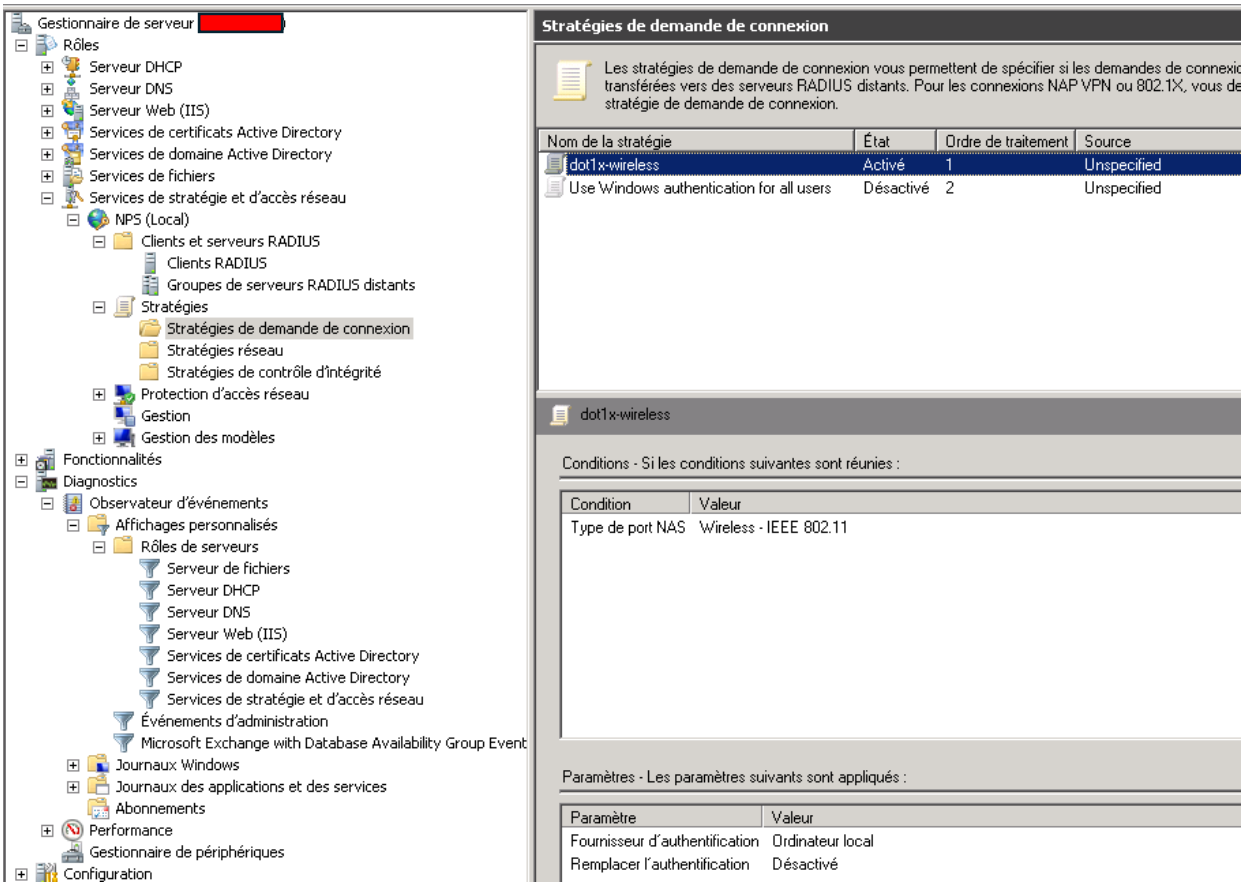
Par la suite, j'ai rajouté un rôle de serveur appelé **« Services de stratégies et d'accès réseau »** (parfois abrégé **NPAS** en anglais). Ce rôle me permet d'ajouter un serveur de stratégie réseau, **RADIUS**. Je peux ainsi configurer un client RADIUS qui est donc le point d'accès.

Le serveur RADIUS va contrôler l'appareil ou l'utilisateur qui demande la connexion au réseau et en fonction de l'identité du demandeur, en respectant la stratégie réseau en place, le serveur autorise ou refuse l'accès. S'il autorise l'accès, il affectera les droits correspondant à l'utilisateur.

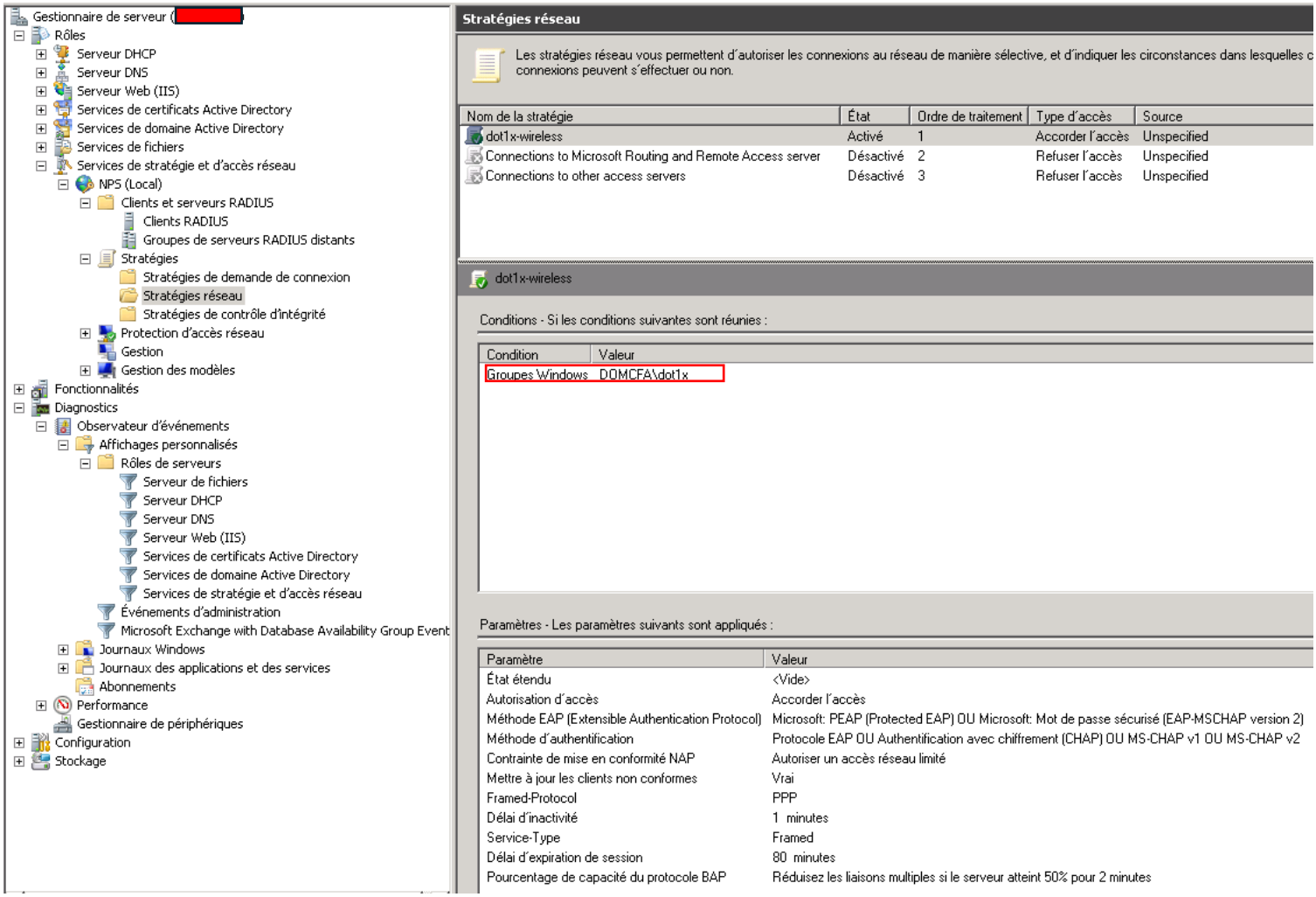
Client RADIUS



Stratégie de demande de connexion

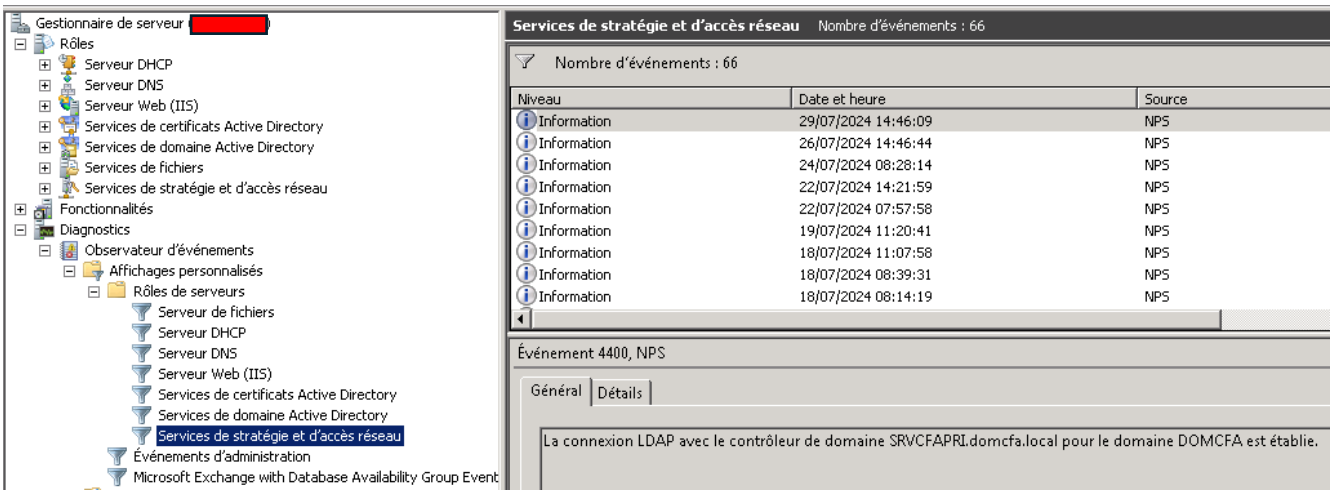


Stratégie réseau

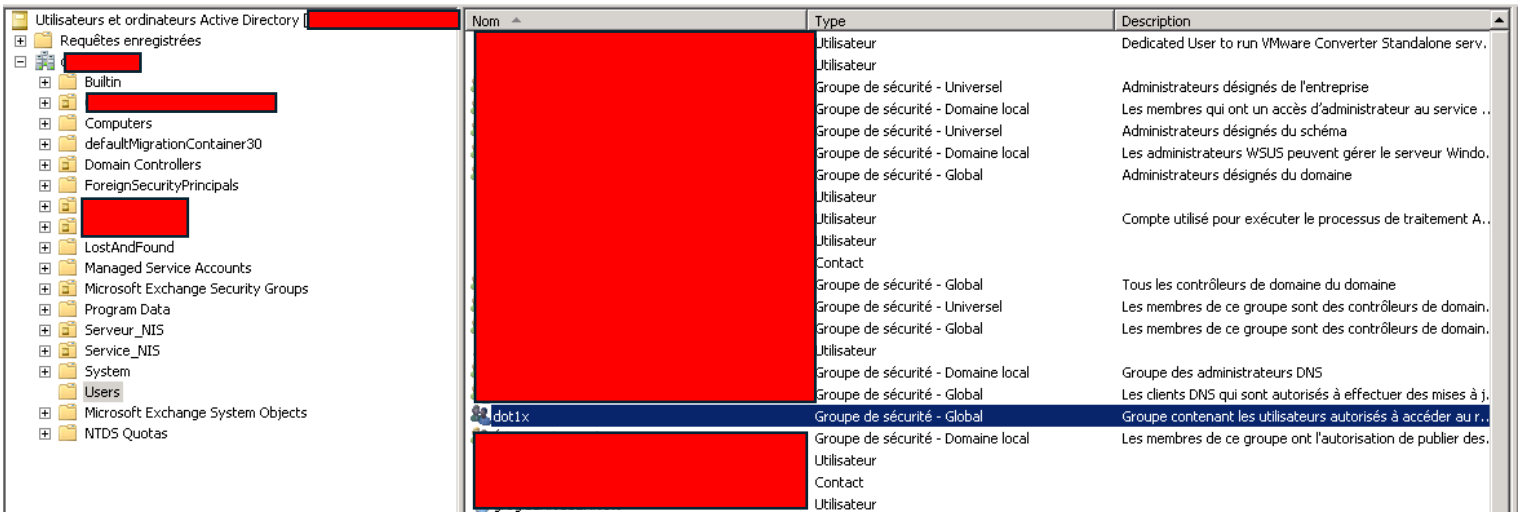


On peut lire la condition que respecte le serveur. L'accès n'est autorisé qu'aux utilisateurs du groupe **« dot1x »**.

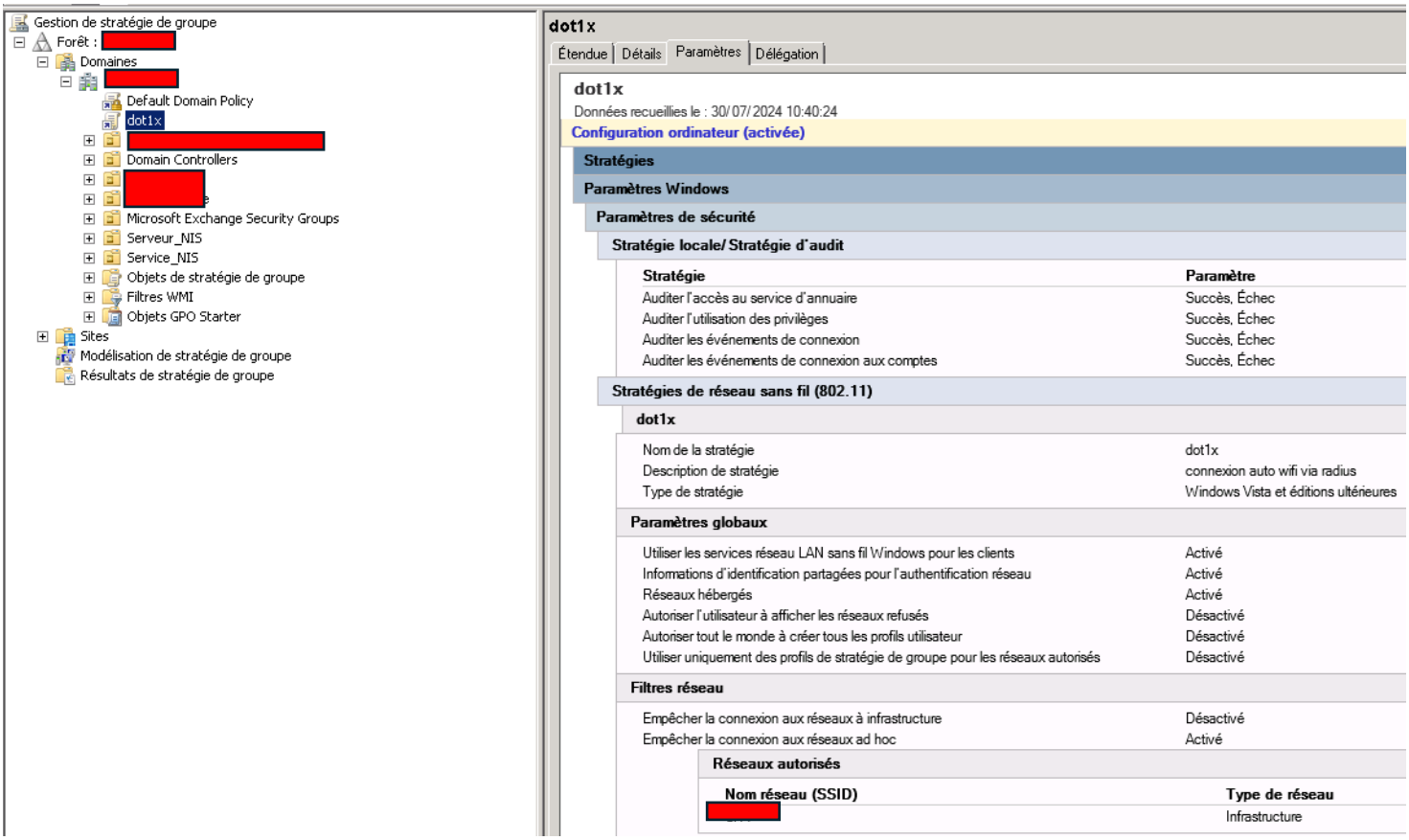
Vous pouvez accéder au log du serveur RADIUS. Voir image ci-dessous. Cela permet de s'assurer du bon fonctionnement du serveur et des échanges entre le client et le serveur. Le fichier de log se trouve dans **C:\Windows\System32\LogFiles**



Le groupe existe dans l'OU **« Users »**, comme vous pouvez voir.



Enfin, j'ai déployé une stratégie qui configure automatiquement le réseau sans fil sur tous les ordinateurs du domaine. Ces ordinateurs (portables ou avec clé Wi-Fi) se connecteront aussi automatiquement au réseau sans fil, s'ils se trouvent à proximité du réseau. Il faudra bien sûr que l'utilisateur qui ouvre sa session sur l'ordinateur, appartienne au groupe **« dot1x »**.

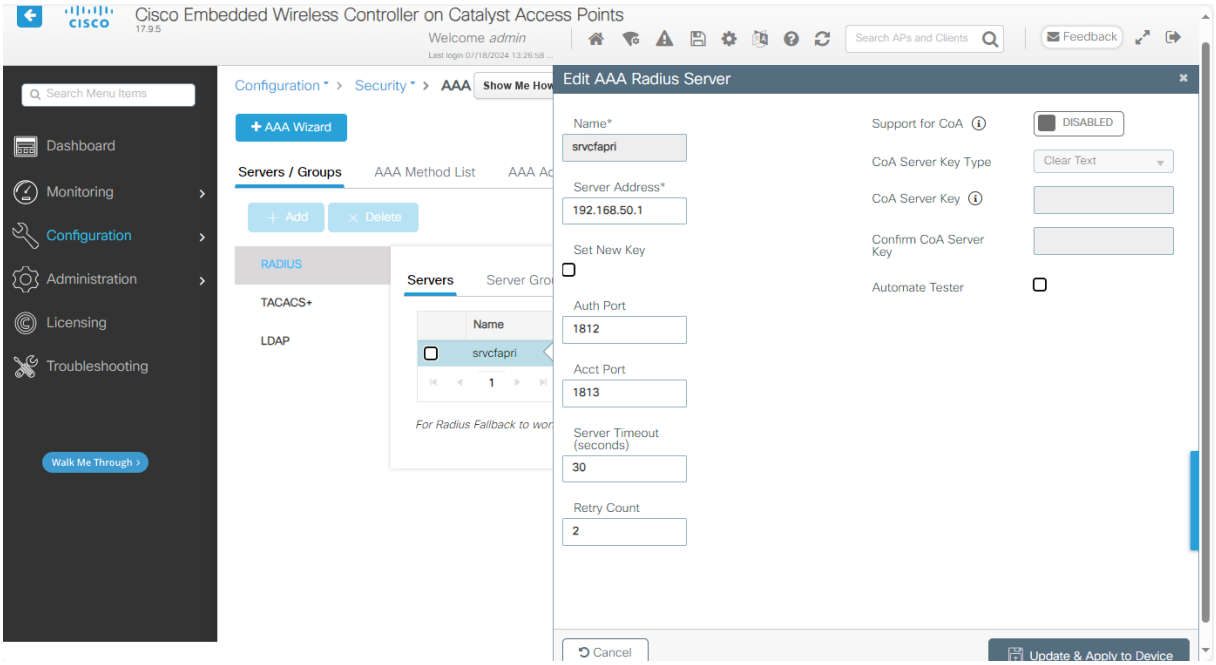


b) Sur le point d'accès

L'administration du point d'accès est assez intuitive. L'interface permet une prise en main rapide et facile.

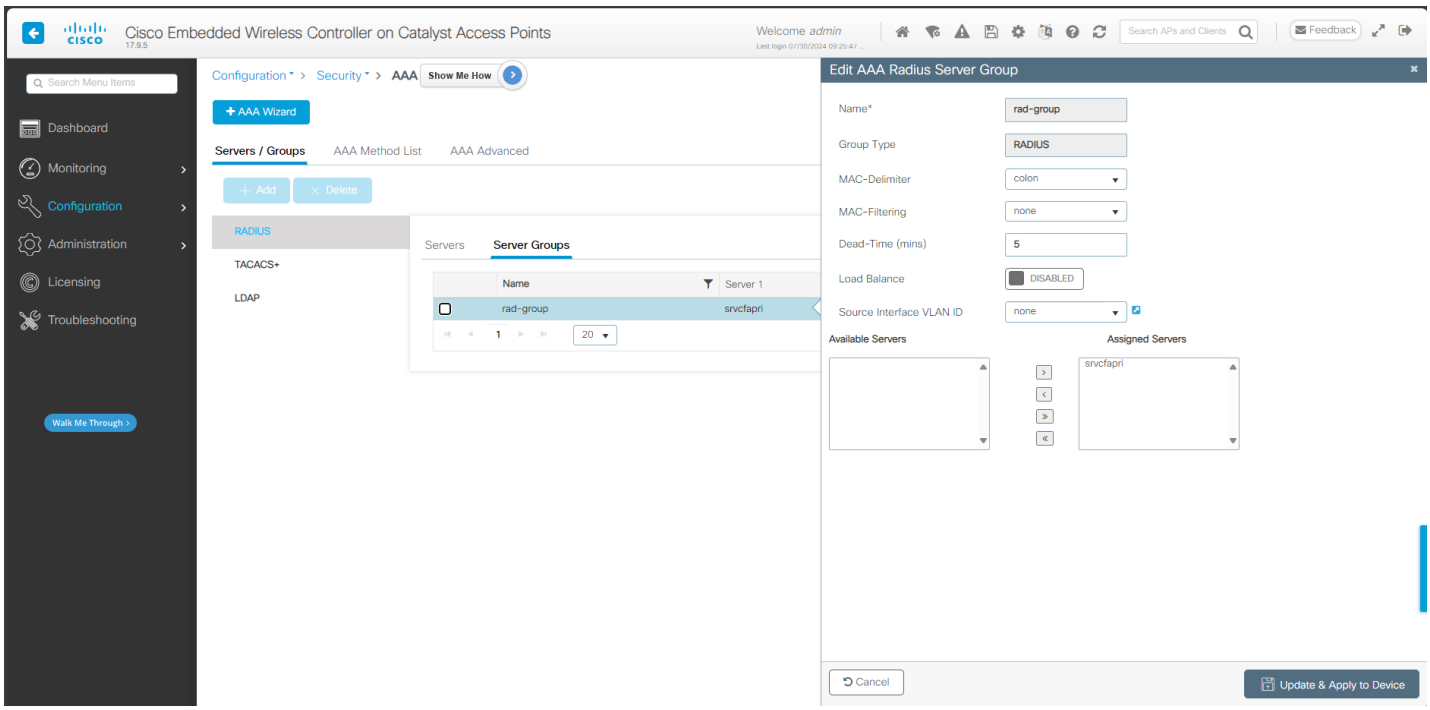
Sur le point d'accès, j'ai essentiellement configuré les informations du serveur RADIUS avec les options qui correspondent (Authentification, Autorisation et Traçabilité).

Serveur RADIUS



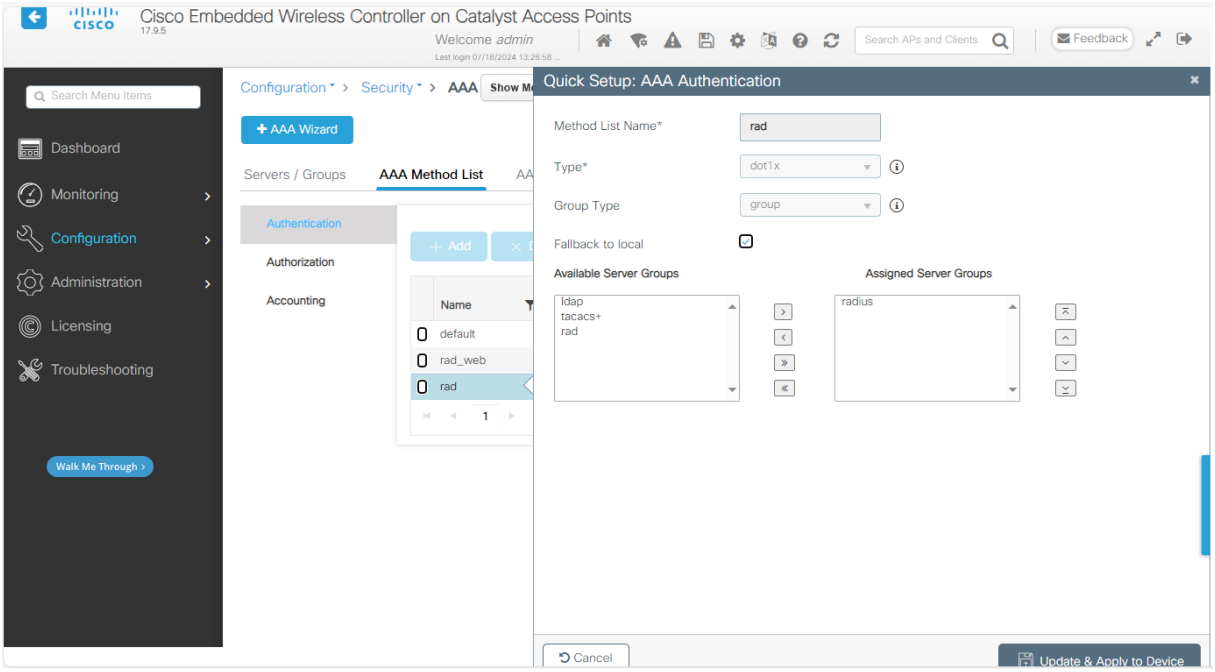
Il y a une clé à entrer. Veillez à entrer la même clé sur le serveur et le point d'accès.

Groupe de serveurs RADIUS



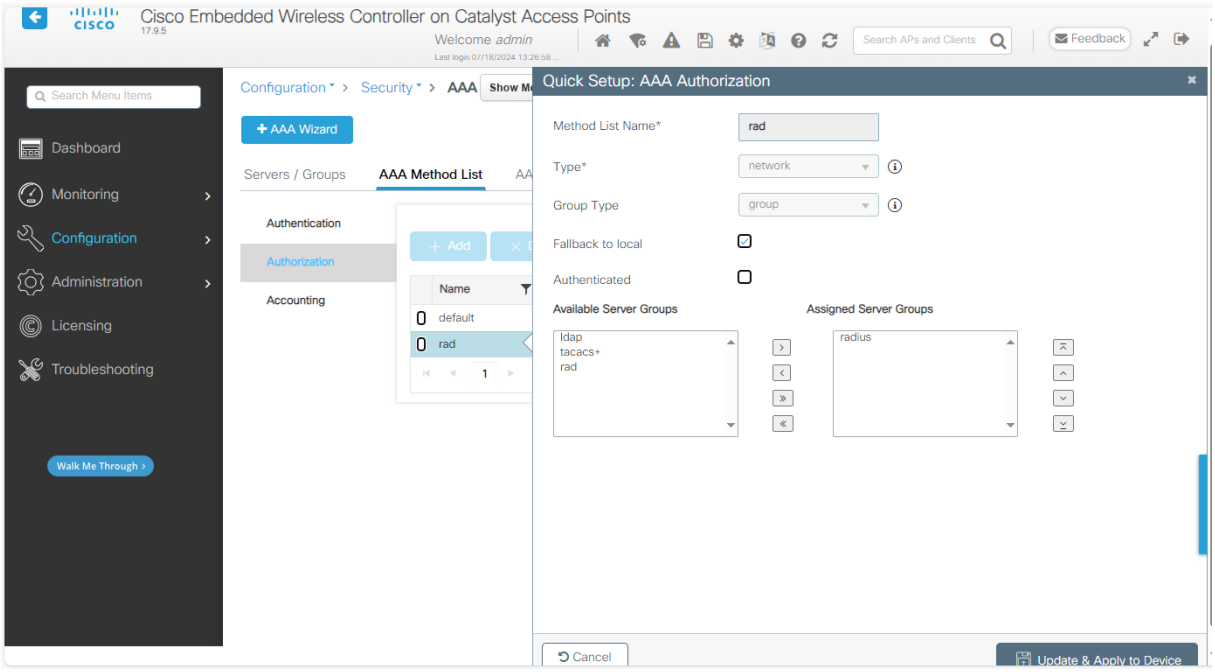
Sélectionnez le serveur RADIUS configuré en amont.

Paramètres pour l'Authentification



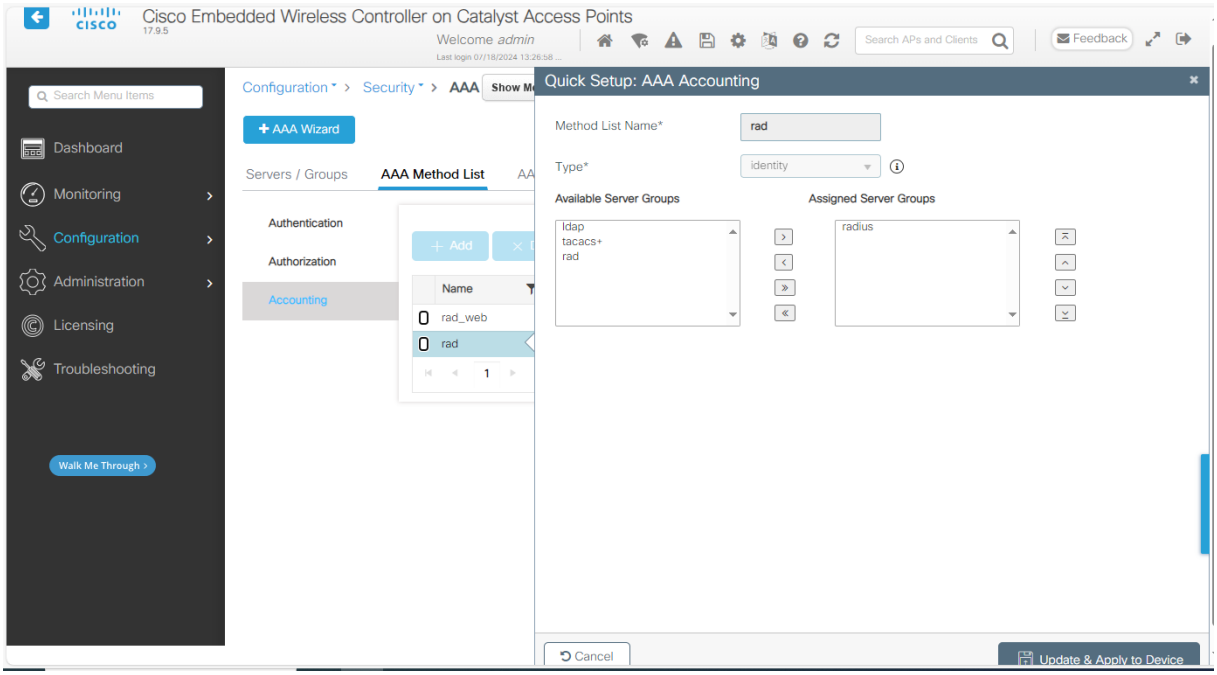
Donnez un nom bien explicite. Ensuite pour le type **« dot1x »** et pour le type de groupe, choisir **« group »**. Cochez la case **« Fallback to local »** et sélectionnez le groupe de serveurs RADIUS créé en amont.

Paramètres pour l'Autorisation

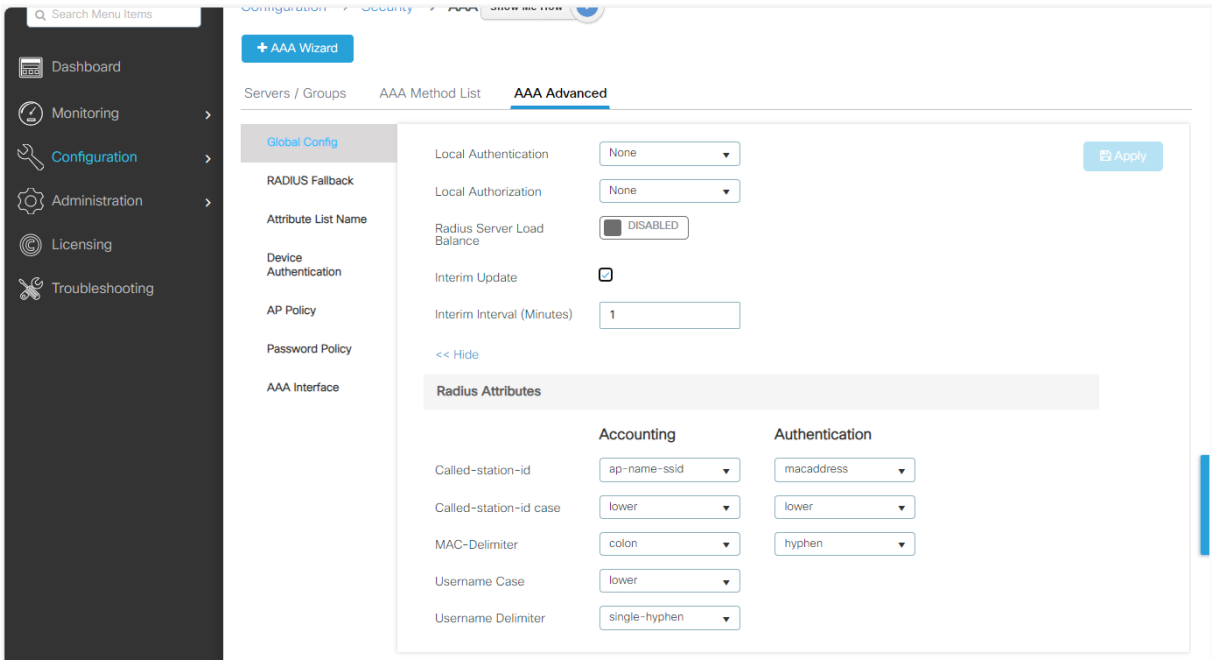


Seule nuance, le type d'autorisation est **« network »** car on autorisera l'accès réseau à l'utilisateur.

Paramètres pour la Traçabilité.



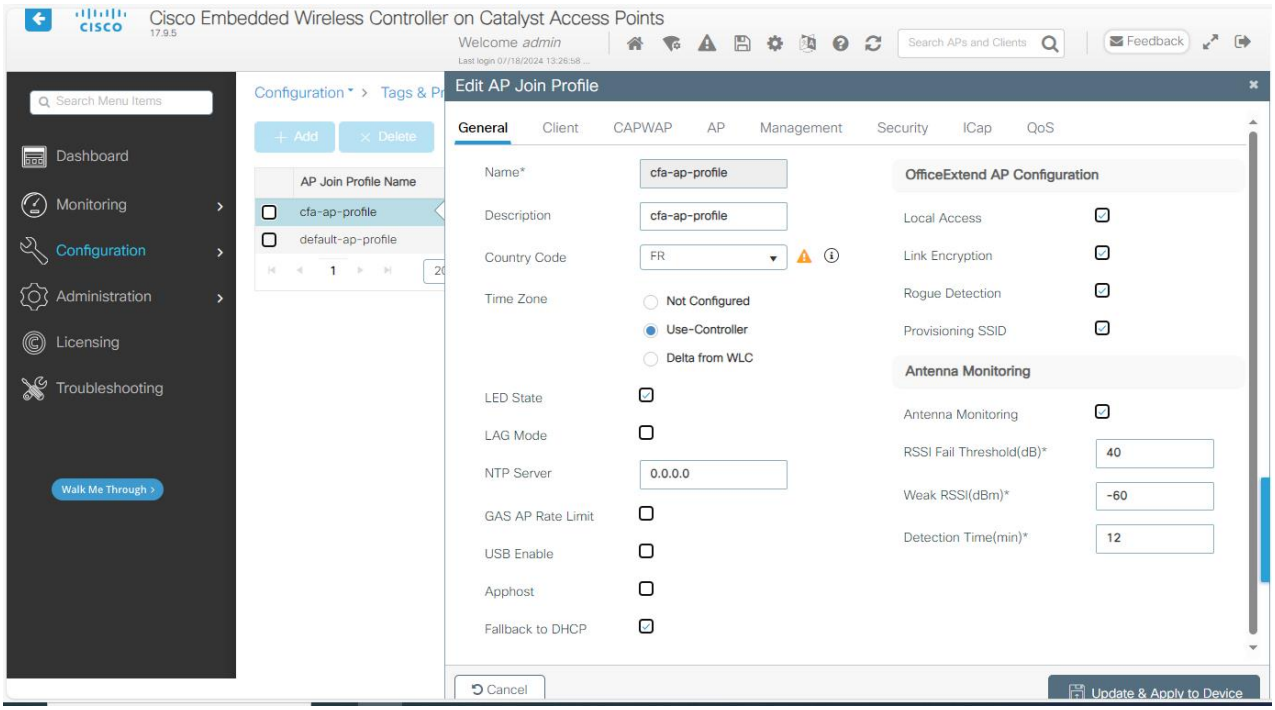
Concrètement, le serveur recueille l'identité du demandeur. D'où le type **« identity »**.



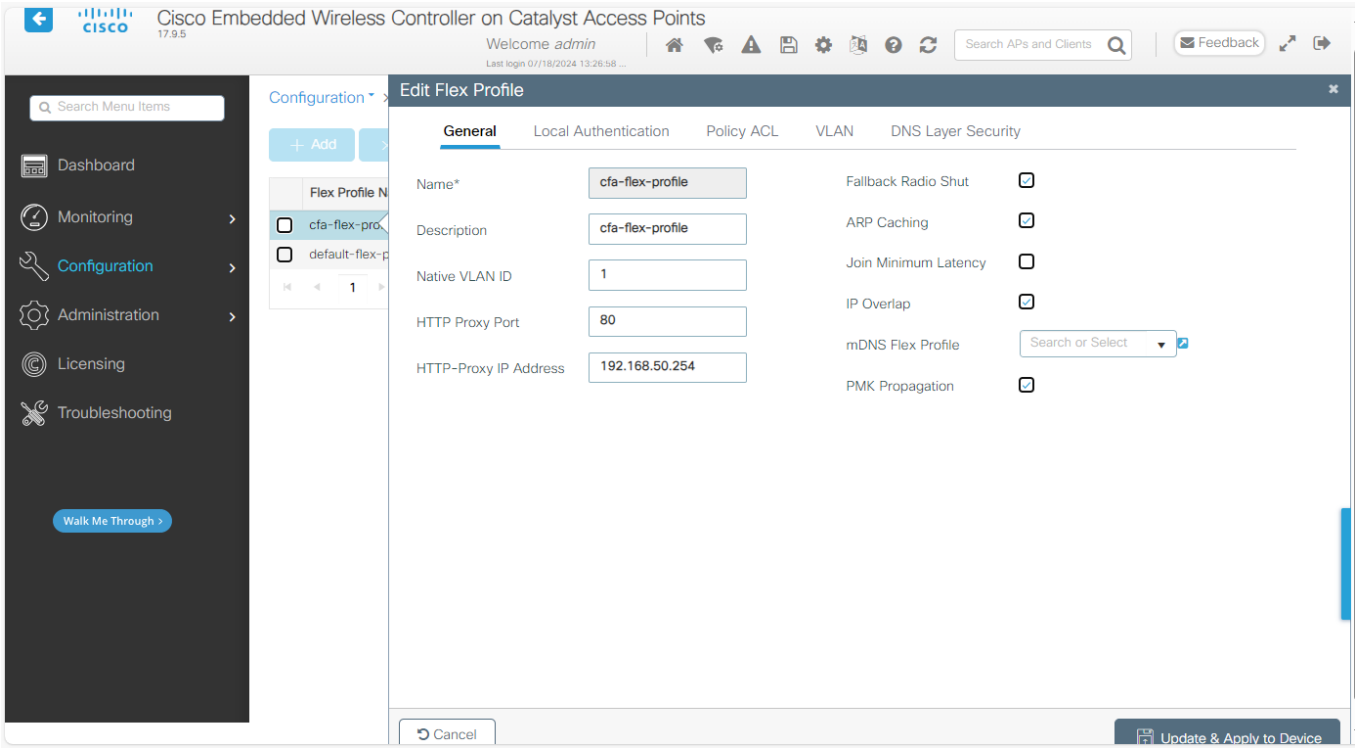
Ci-dessus on indique sous quel format seront affichées les informations du demandeur sur le serveur.

Ensuite j'ai fait toute la partie sans fil. En commençant par configurer les profiles qui correspondent à des stratégies qui s'appliqueront d'abord à **tous les points d'accès** appartenant au parc puis à tous les **réseaux sans fil associés au contrôleur**. Aussi, ces profiles doivent être utilisés et diffusés par le point d'accès (contrôleur) afin que tous les réseaux sans fil soient diffusés. Le point d'accès parle de **« Tag »** pour le réseau sans fil.

Profil à joindre par les APs.

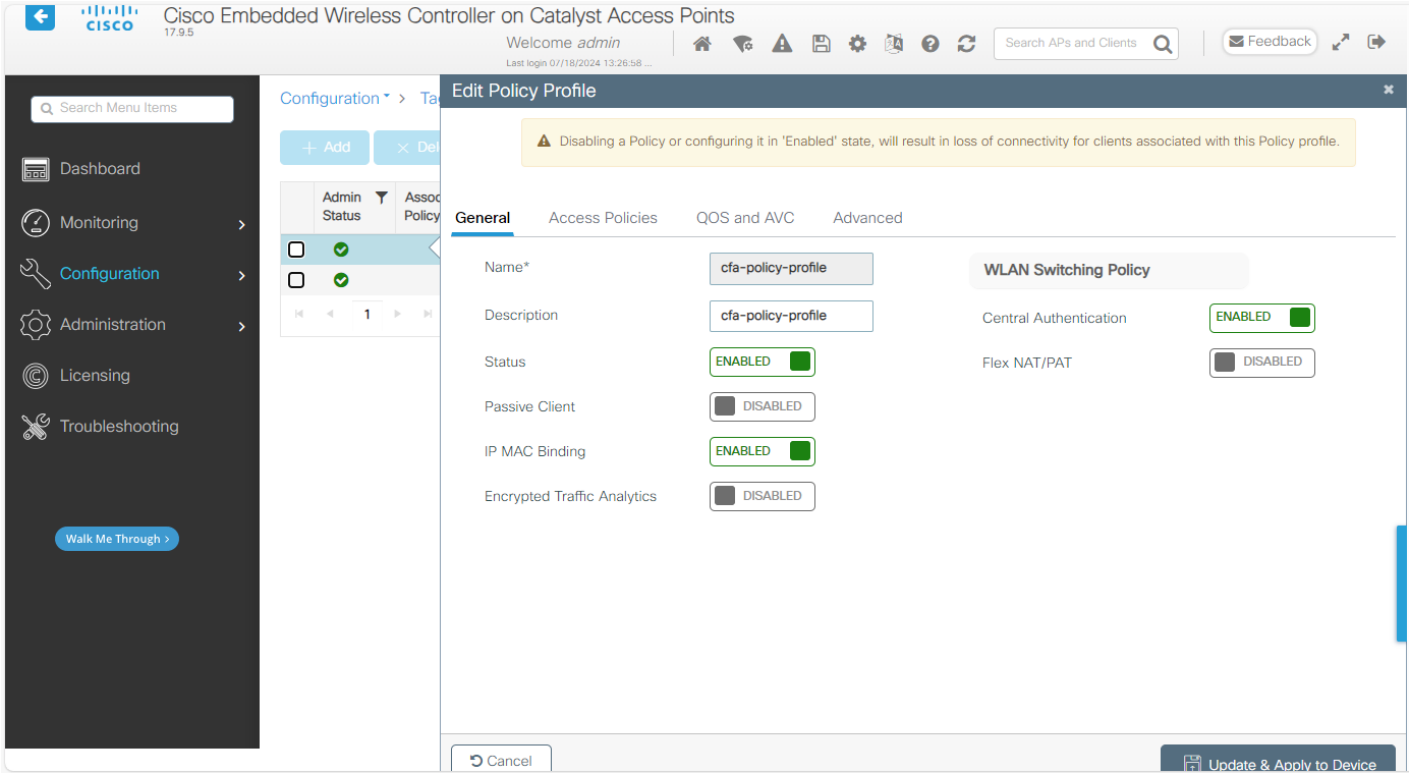


Profil « Flex »



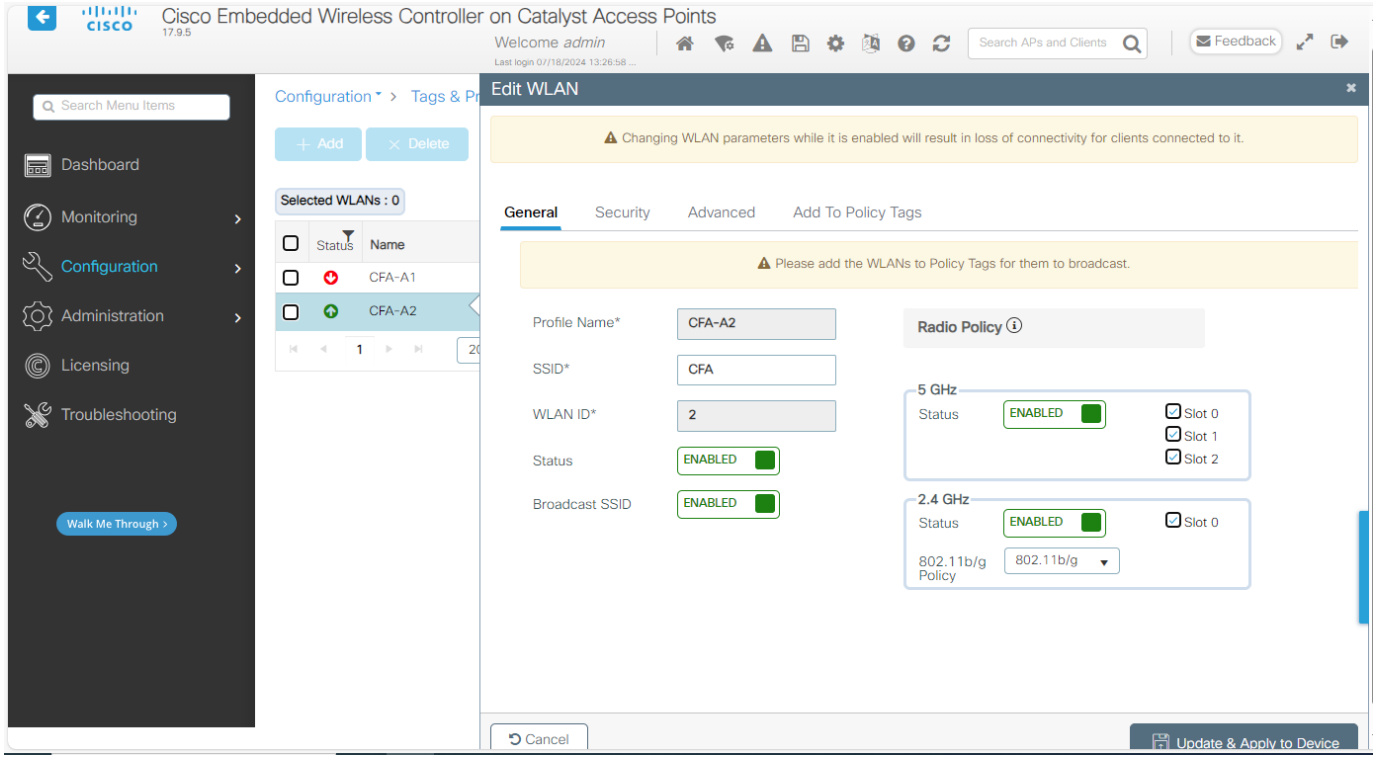
Le profil ci-dessus indique certaines capacités aux APs, comme contrôler l'authentification ou les VLANs.

Profil de stratégie.



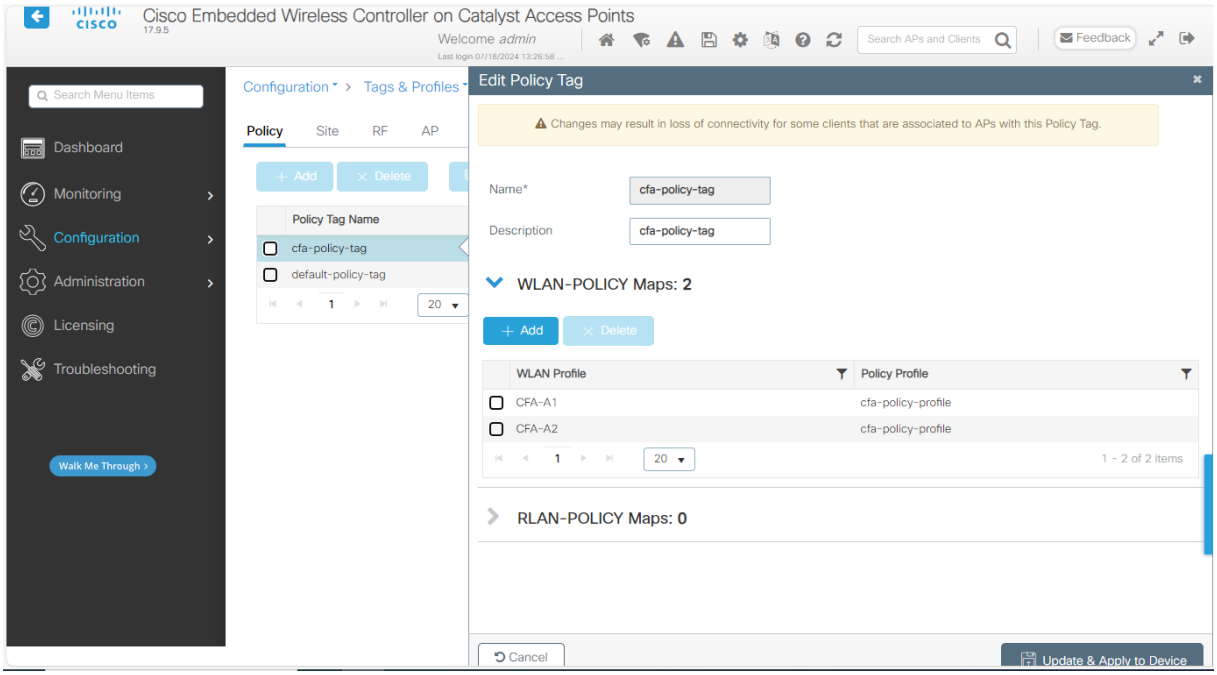
Ici, on indique par exemple à tous les APs du parc (qui appliquent cette stratégie) de ne pas gérer l'authentification en local (puisque c'est le serveur qui s'en occupera). Cela consiste à établir des comportements des APs face aux clients.

Configuration d'un réseau sans fil

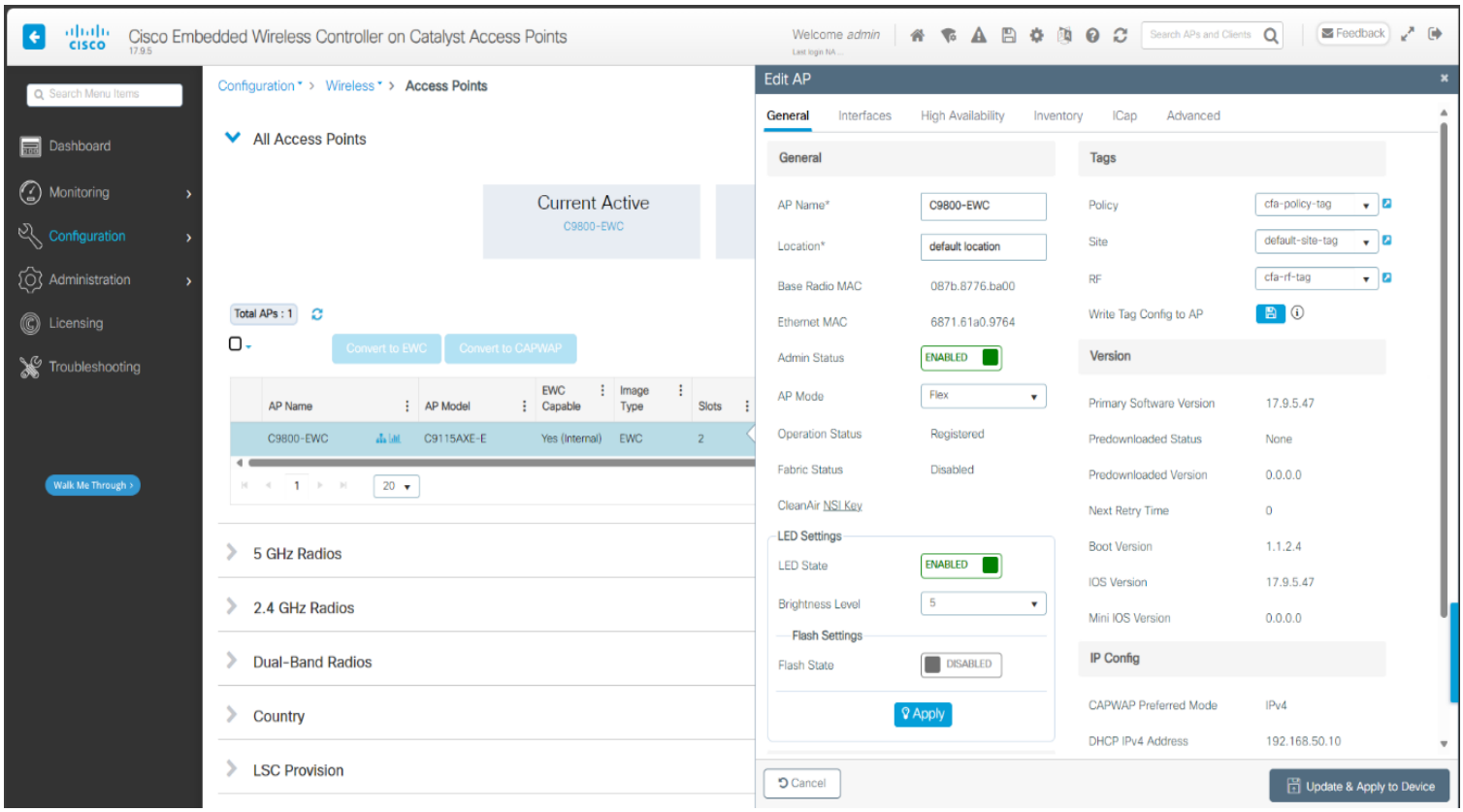


L'image ci-dessus correspond à l'espace dédié pour créer un réseau sans fil que le point d'accès diffusera. N'oubliez pas que pour que la diffusion se fasse, il faut « **taguez** » ce réseau. Autrement dit, l'ajouter au **profil stratégie** (juste ici).

Le tag se fait à cet endroit (image ci-dessous).



L'autre partie de l'administration de l'appareil sans fil consiste à configurer l'interface réseau sans fil. Ce qui correspond réellement au point d'accès.



L'image n'est peut-être pas très lisible, mais à cet endroit on configure le point d'accès **« Edit AP »**.

On :

- Lui donne un **nom** ;
- Lui attribue une configuration IP (ici en DHCP) ;
- Lui affecte les stratégies à utiliser et appliquer ;
- Lui indique certaines propriétés, facultatives mais parfois utiles, sous les autres onglets non illustrés.

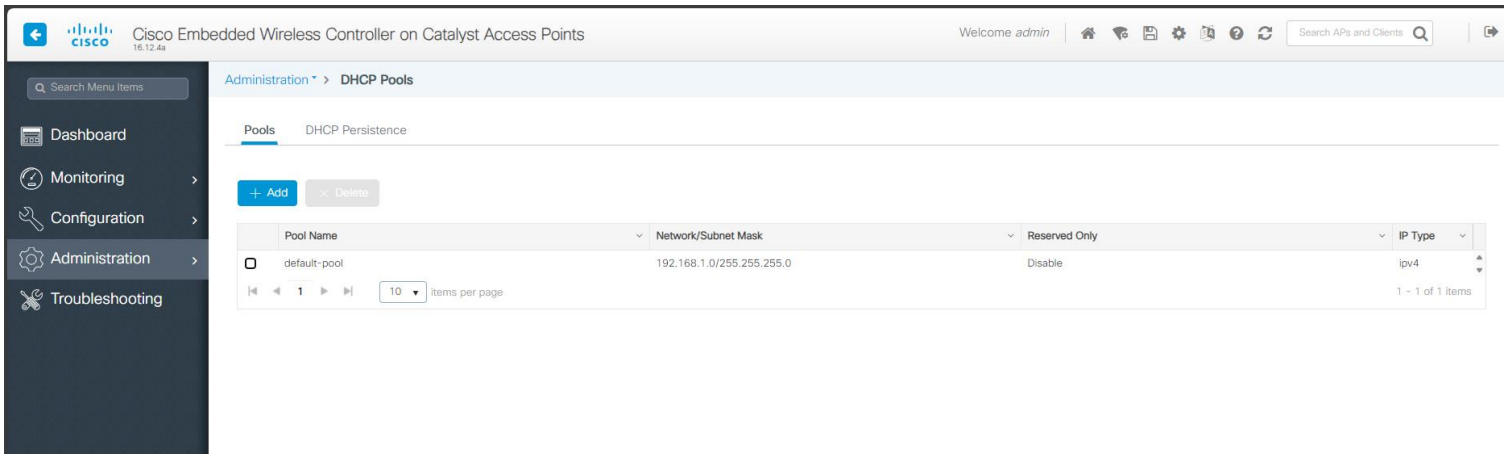
4. Ajout d'une borne (de même modèle potentiellement)

L'ajout d'une borne peut se faire de plusieurs façons différentes. Mais celle que je vais présenter évite toute configuration complexe et facilite l'intégration de la borne dans le parc.

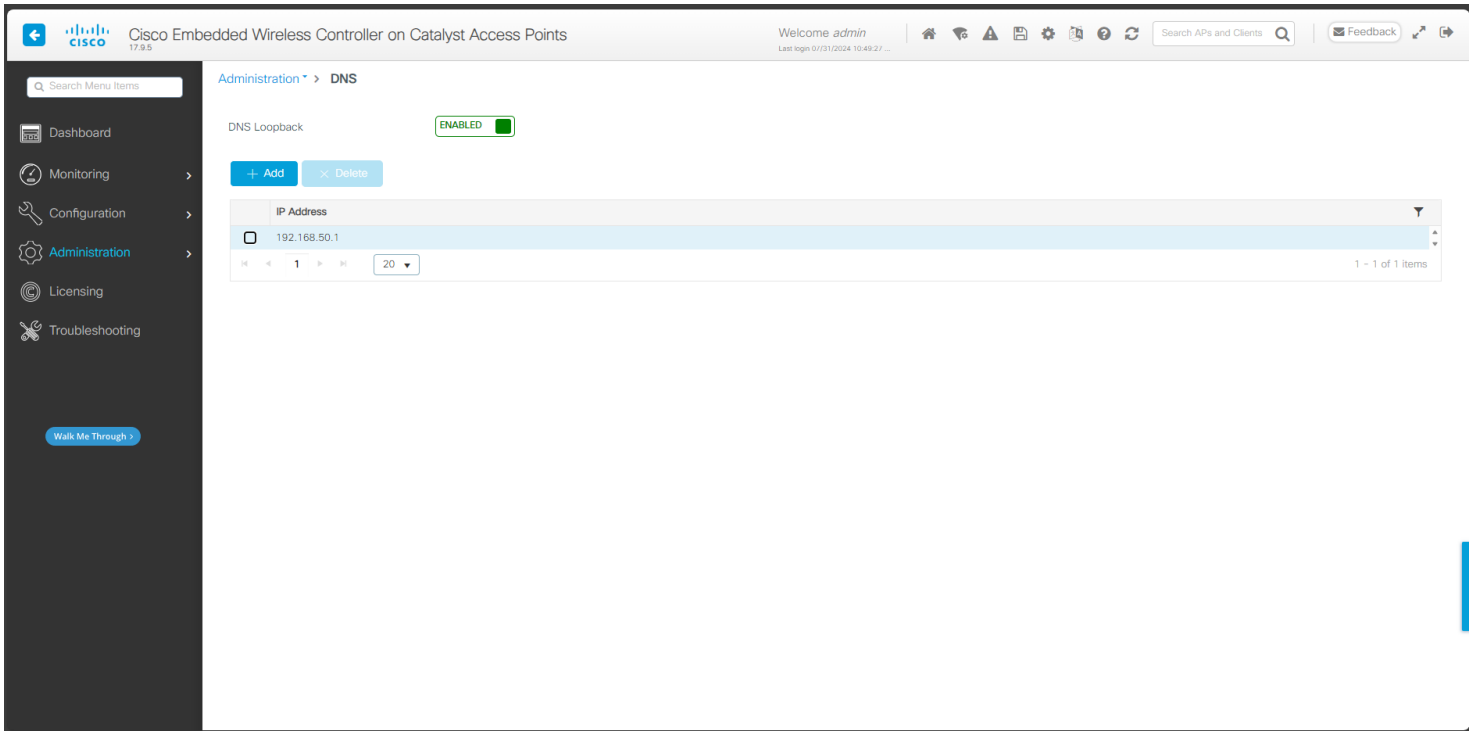
Assurez-vous de le faire dans cet ordre (même si j'ai utilisé une liste à puces).

- Relevez l'adresse MAC de l'AP (à l'arrière) et faite une réservation sur le serveur DHCP.
- Alimenter l'AP hors du réseau : il vous sera demandé de faire la « **0day configuration** ». Voir ici.

Stopper le DHCP interne (**Administration > DNS ;** supprimer le pool par défaut)

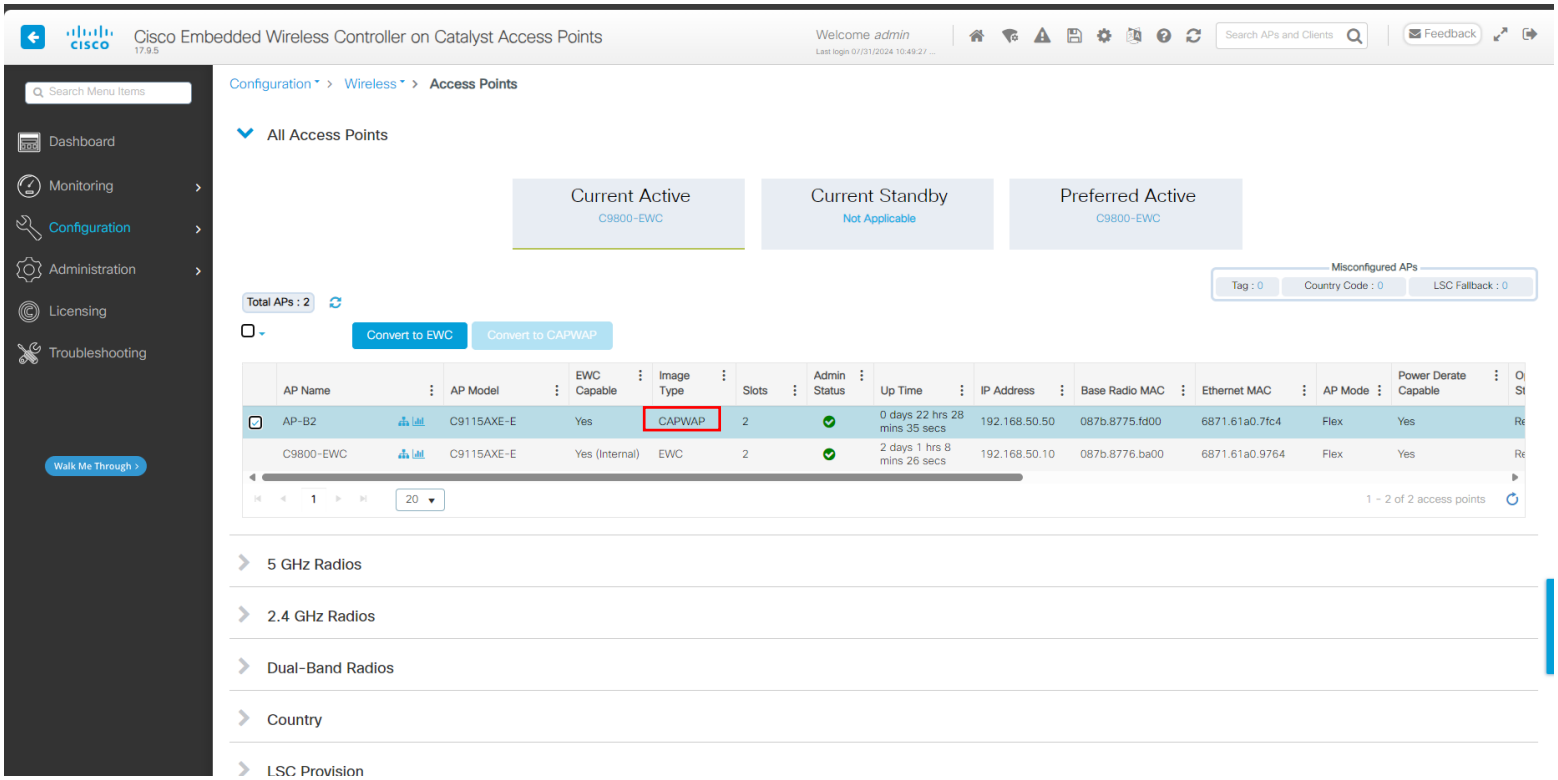


Indiquer le DNS de notre serveur (**Administration > DNS)**



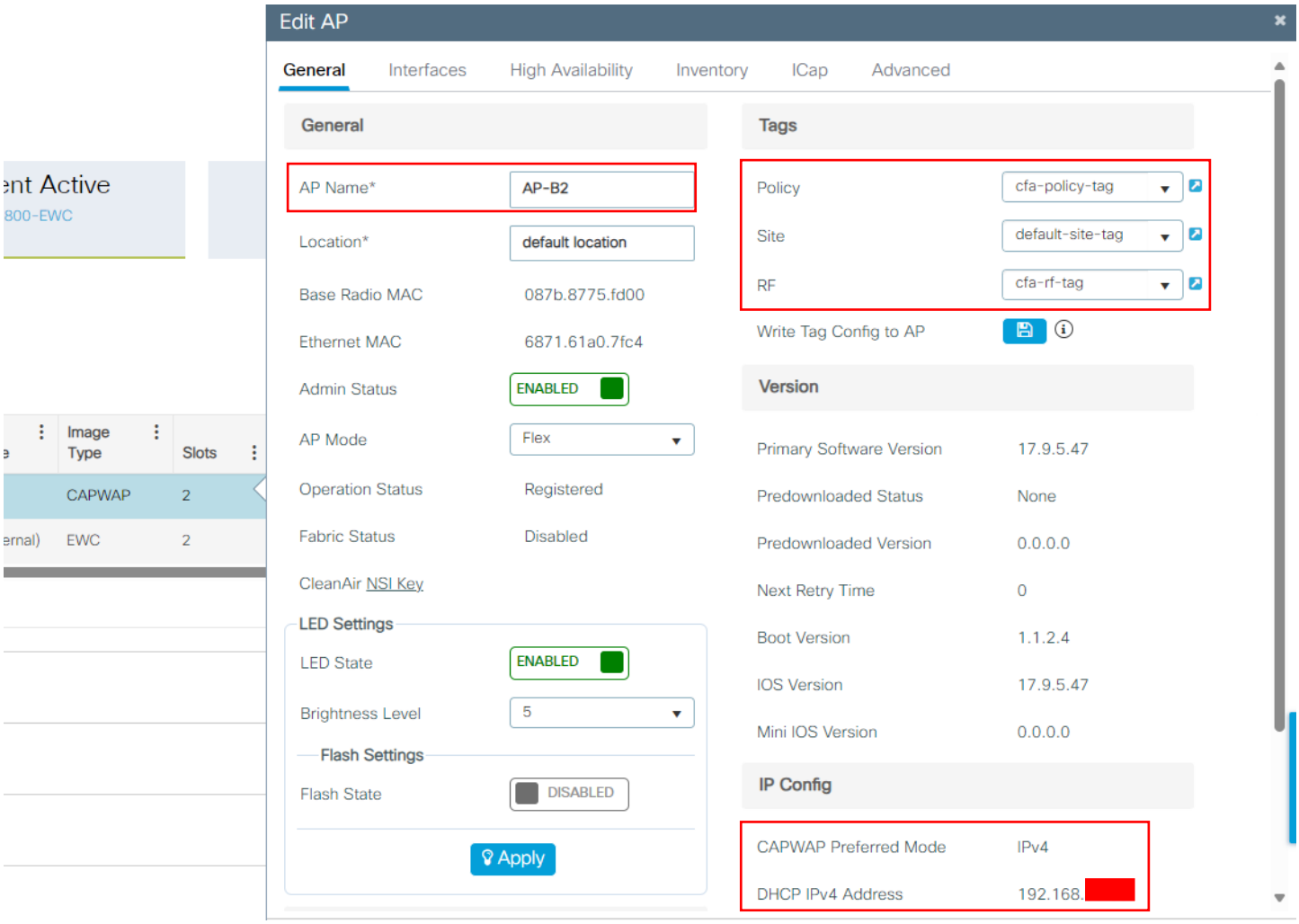
Convertir l'AP en CAPWAP (**Configuration > Wireless > Access Points**)

Après conversion, l'AP ne sera plus accessible. C'est normal. C'est à ce moment qu'il faut le connecter au réseau.

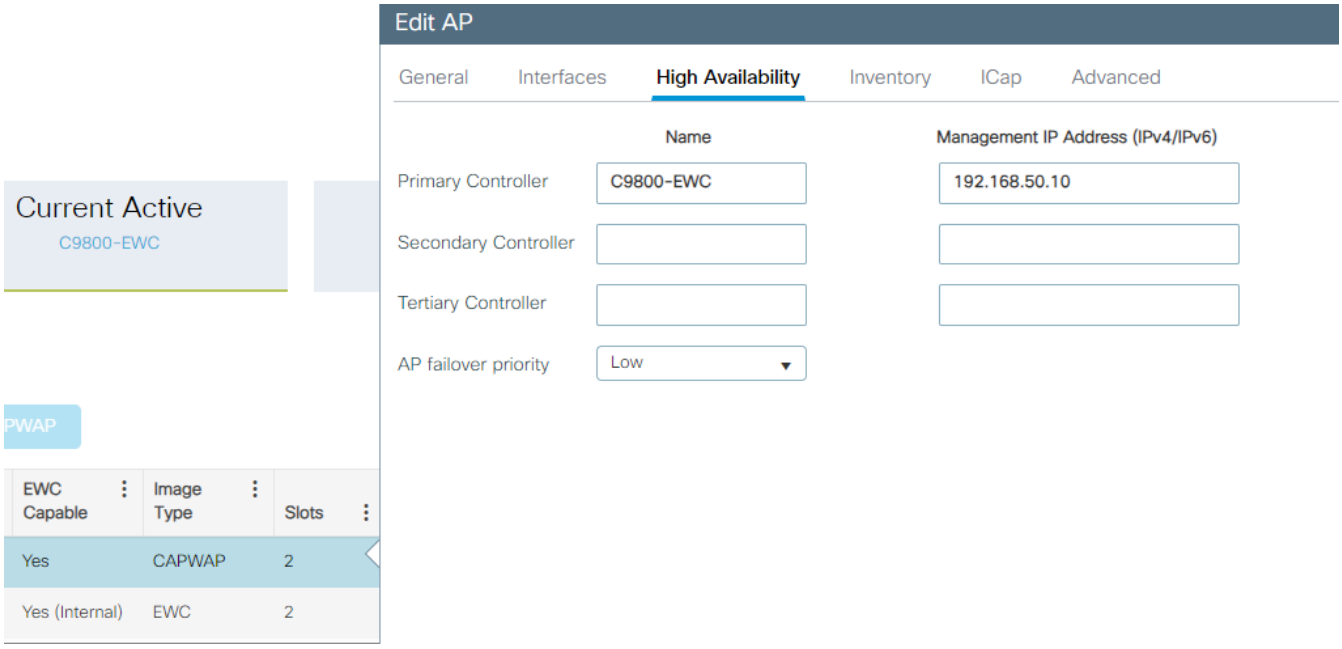


NB : Il faut s'assurer qu'une fois dans le réseau le champ **« Image Type »** correspond bien à **« CAPWAP »**. Vous pourrez le voir en vous connectant sur l'interface de gestion du contrôleur.

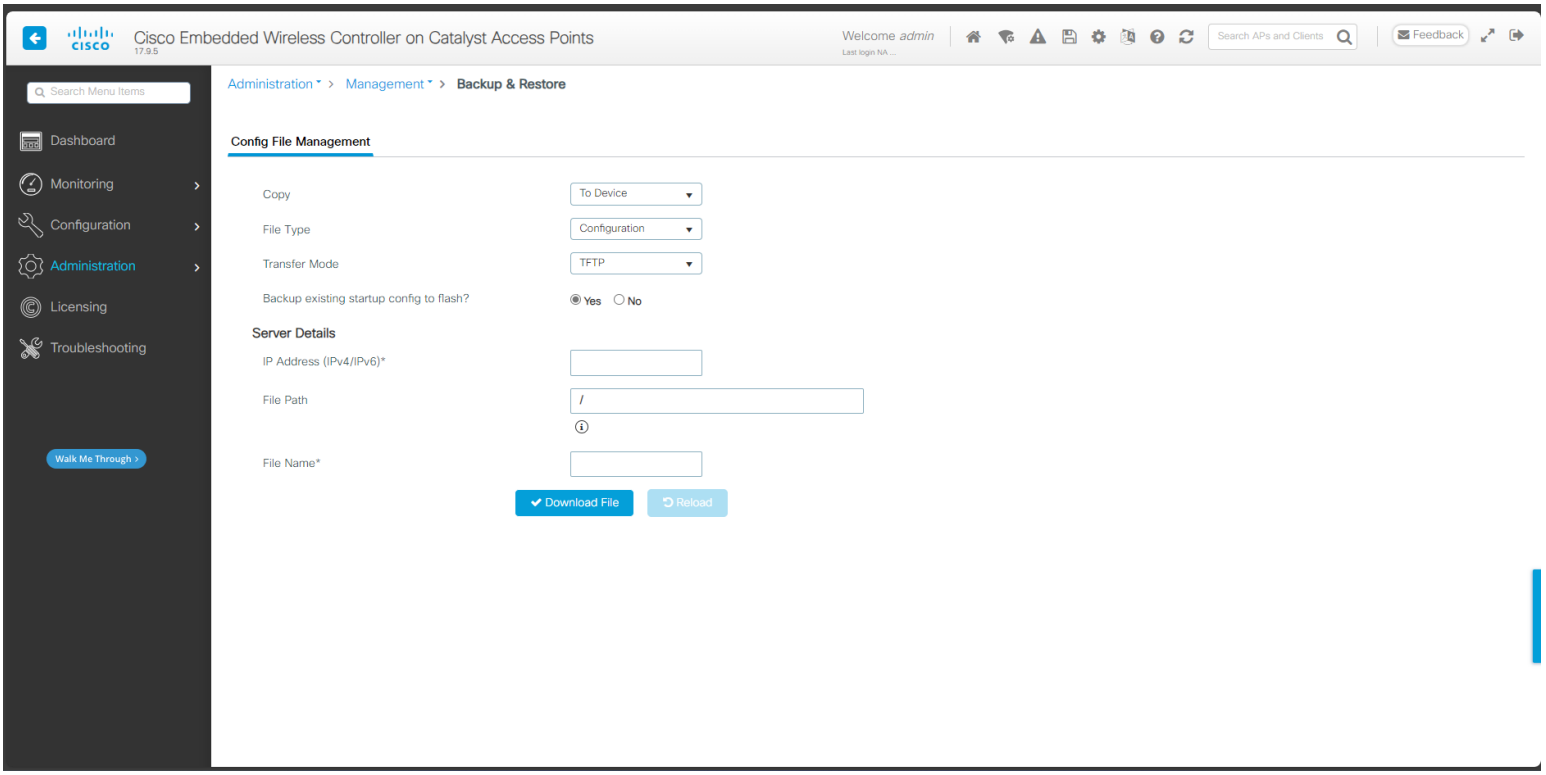
- Modifiez le nom, affectez les stratégies adéquates (choisir **« cfa-... »** dans la liste). Veillez que la configuration IP correspond à la réservation d'adresse faite. Appliquez et sauvegardez.



La partie ci-dessous n’est pas obligatoire. Mais vous pouvez la remplir.



5. Sauvegarde et restauration (Administration > Management, Backup & Restore)



Vous pourrez donc rappeler une configuration antérieure en cas de mauvaise manipulation.

BONNE UTILISATION.