[Date]

Cisco Catalyst 9800-CL Wireless Controller for Cloud

Migration Contrôleur WiFi Cisco WLC AirOS

Mamadou CAMARA
BTS SIO, SISR

SOMMAIRE :

1. CONTEXTE

Le Contrôleur Cisco WLC AireOS **Cisco Virtual Wireless Controller n'est plus compatible avec certaines AP (Point d'accès). La DSI du CH Esquirol veut migrer vers une nouvelle version Cisco Catalyst 9800-CL Wireless Controller for Cloud.**

2. OBJECTIF

Mise en place d'un contrôleur virtuel **WLC Cisco Catalyst Wireless Controleur 9800.**

Cette solution devra s'adapter au portail captif déjà en place (Utopia) et à une authentification 802.1X NPS Windows Server 2012 (Radius).

3. FONCTIONNEMENT DU CISCO WLC (CAPWAP)

La méthode de communication entre les AP et le contrôleur WLC.

Les bornes Wi-Fi et le contrôleur WLC (Wireless LAN Controleur) communiquent généralement via un protocole appelé **CAPWAP (**Control and Provisioning of Wireless Access Points).

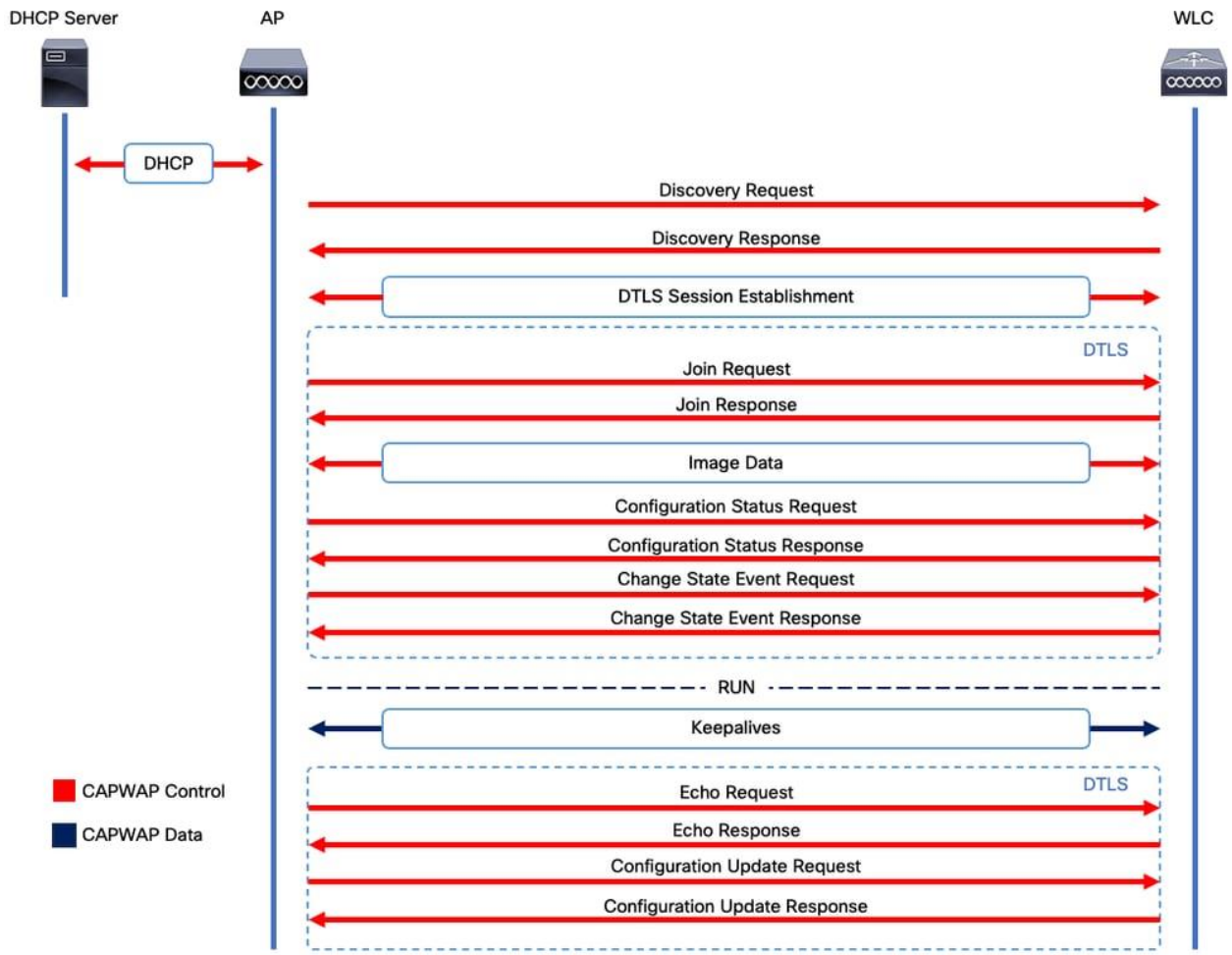
Fonctionnement entre les bornes Wi-Fi et le contrôleur WLC via CAPWAP :

> Lors du démarrage, l'AP contacte le serveur DHCP qui à son tour envoie une configuration IP complète avec notamment l'adresse du Contrôleur WLC en **option 43** (adresse en hexadécimale sous forme de **hex f1.04.[adresse IP du Contrôleur en hexa].**

- **Association initiale** : Lorsque l'AP démarre, il effectue une découverte du contrôleur WLC sur le réseau. Une fois le contrôleur identifié, l'AP établit une association initiale avec le contrôleur pour établir une connexion de découverte.
- **Tunnel CAPWAP** : Une fois l'association établie, l'AP établie un tunnel CAPWAP avec le contrôleur WLC servant un transport des données de contrôle, les informations de configuration et les commandes de gestion entre l'AP et le contrôleur.
- **Echange de données de contrôle** : Une fois le tunnel CAPWAP établi, l'AP envoie périodiquement des informations de surveillance.
- **Configuration et mise à jour** : Le contrôleur WLC envoie les paramètres de configuration à l'AP via le tunnel CAPWAP, tels que les paramètres sécurités, les SSID, les VLANS etc…
- **Gestion du trafic** : Le contrôleur est responsable de la gestion et du contrôle du trafic des AP.

Port de communication : UDP (5246 pour le contrôle de communication et 5247 pour les échanges de données)

3



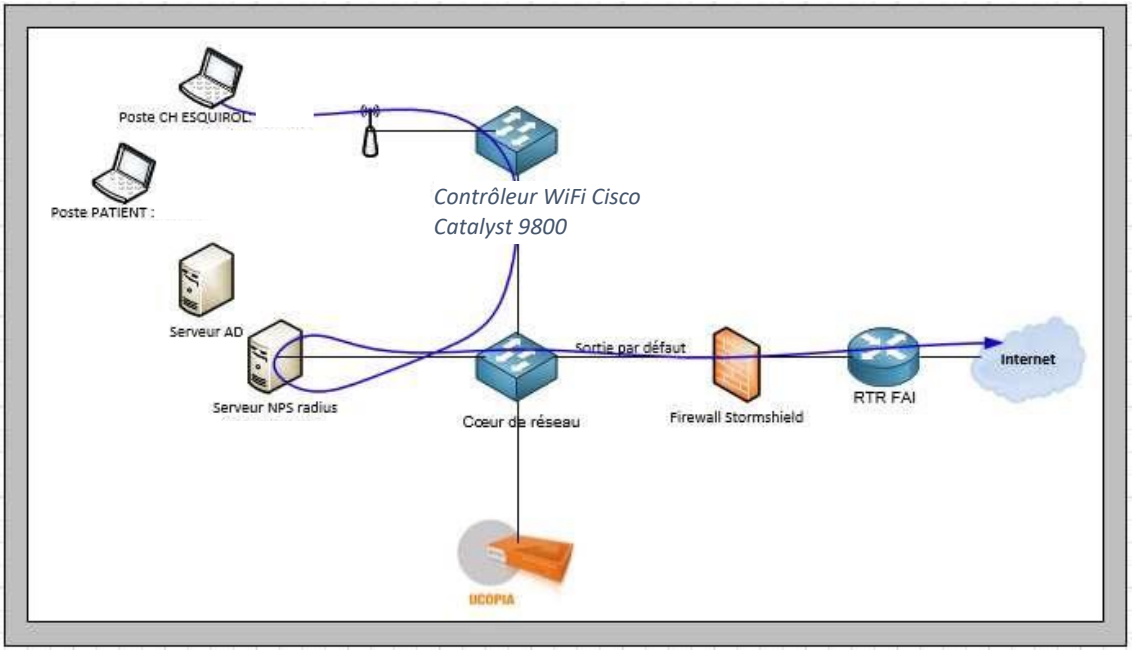
4. L'ARCHITECTURE

L'architecture est basée sur un vlan par SSID avec :

- Le réseau WiFi_PATIENT avec uniquement en niveau 2 jusqu'au portail captif Ucopia,

- Le réseau WiFi_PRO avec une authentification 802.1x, l'authentification est assurée par un serveur 802.1X NPS Windows Server 2012 (Serveur Radius).

- Le réseau WiFi PHARMATIE avec une authentification WiFi WPA 2 PSK + Filtrage et adresse mac

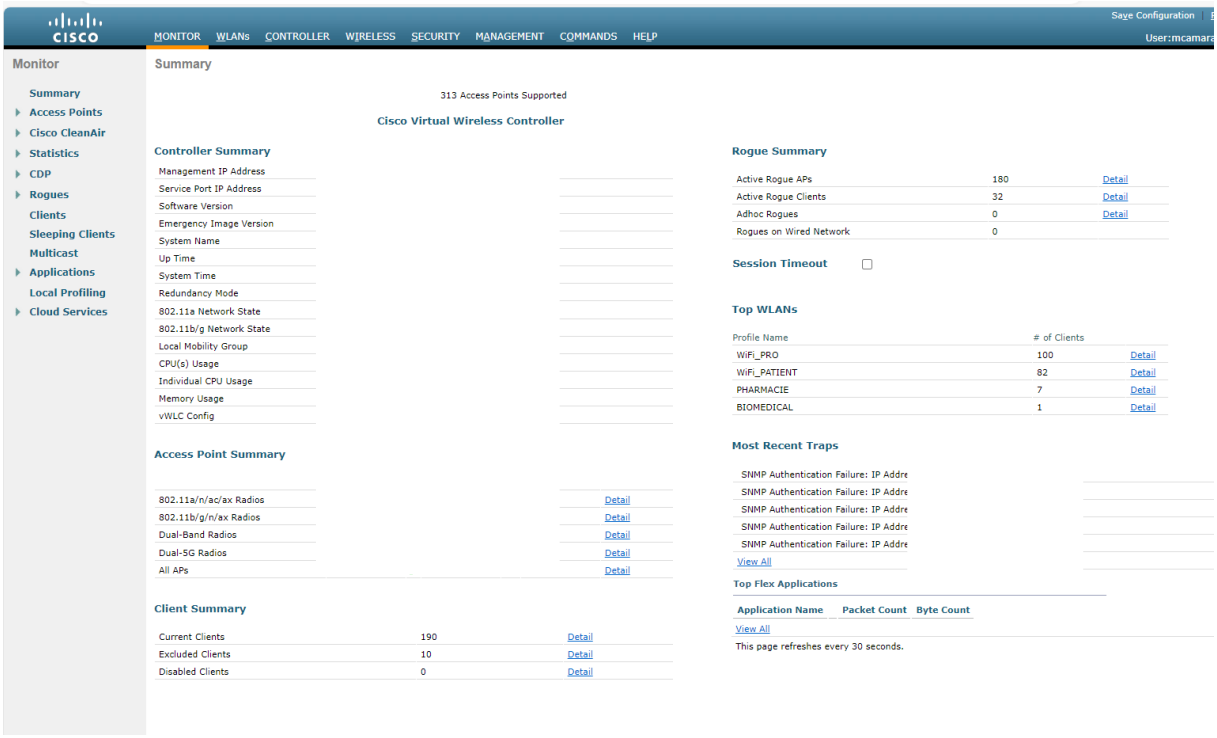


5. Pré-installation

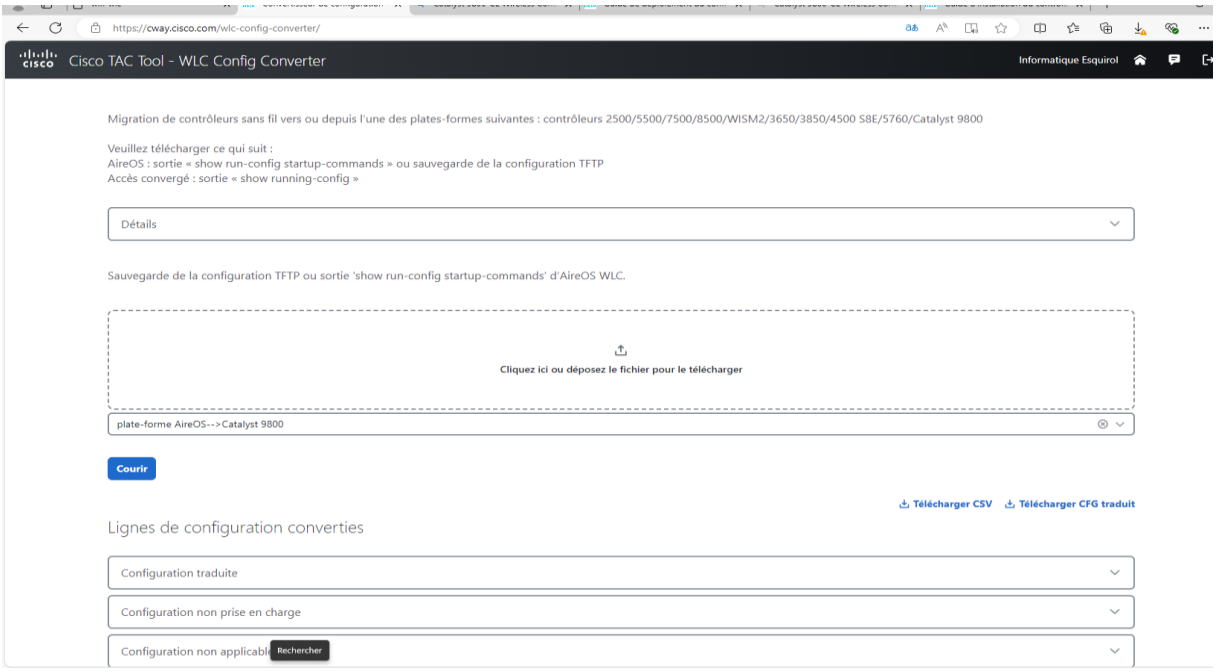
1. Etape 1
   Prise de connaissance de la documentation technique de l'ancien Contrôleur Cisco **WLC AirOS**
2. Prise de connaissance de la configuration de l'ancien contrôleur Cisco **WLC AirOs** depuis l'interface graphique.

- Sauvegarde de la configuration
- Exportation de la configuration

5



- Conversion de la configuration de Cisco **WLC** en **Catalyst 9800-CL** via le site **Cisco TAC Tool Config Converter** : https://cway.cisco.com/wlc-config-converter/



3. Etape 3

Téléchargement de l'image en format OVA du nouveau contrôleur Wi-Fi **Catalyst 9800-CL Wireless Controller for Cloud** depuis le site **Cisco**

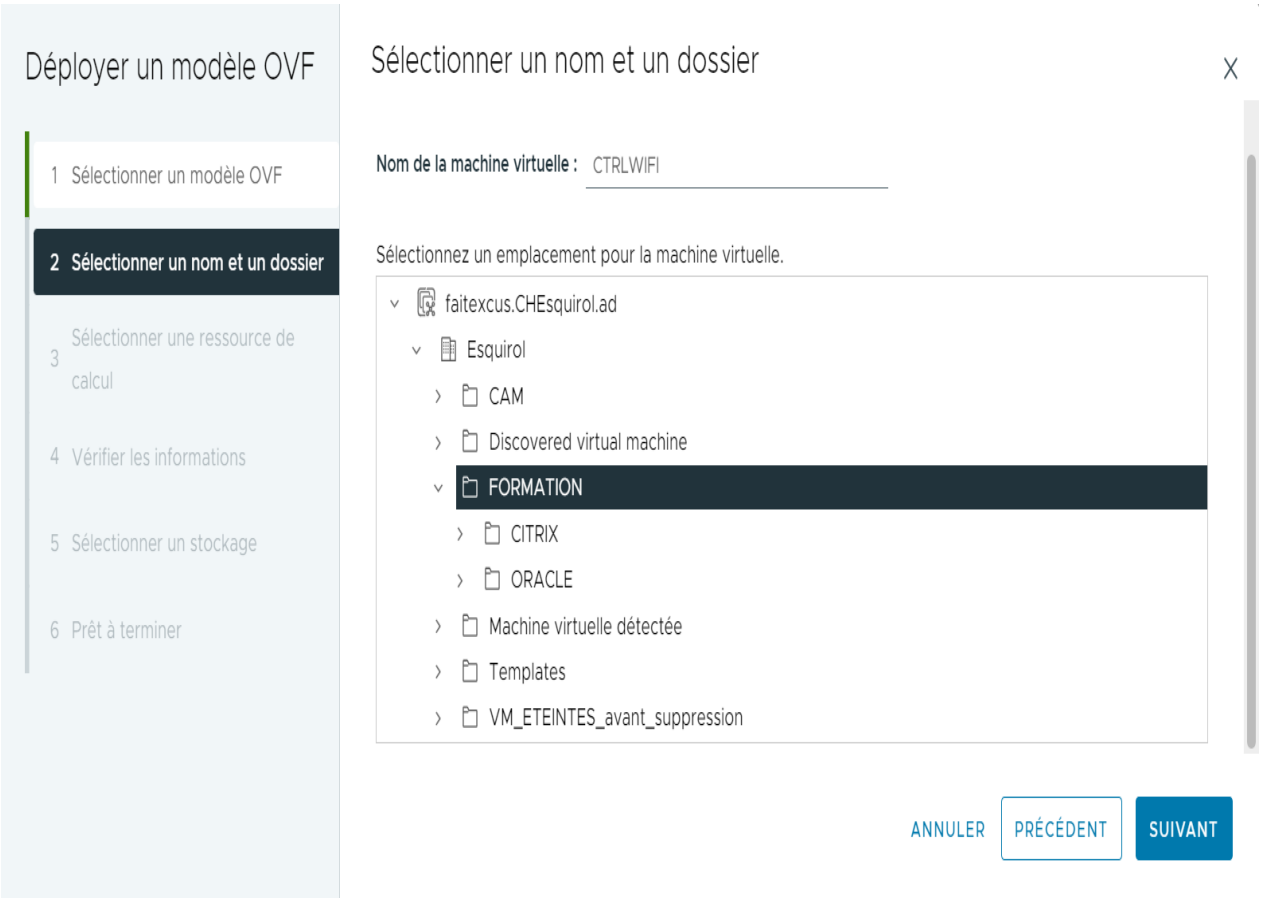
4. Etape 4
Vérification de la compatibilité entre la nouvelle version et l'ancienne :

6. Déploiement et configuration du contrôleur Virtuel sans fil Cisco Catalyst 9800 CL

a. À partir du client vSphere, déployez le modèle OVA 9800-CL.

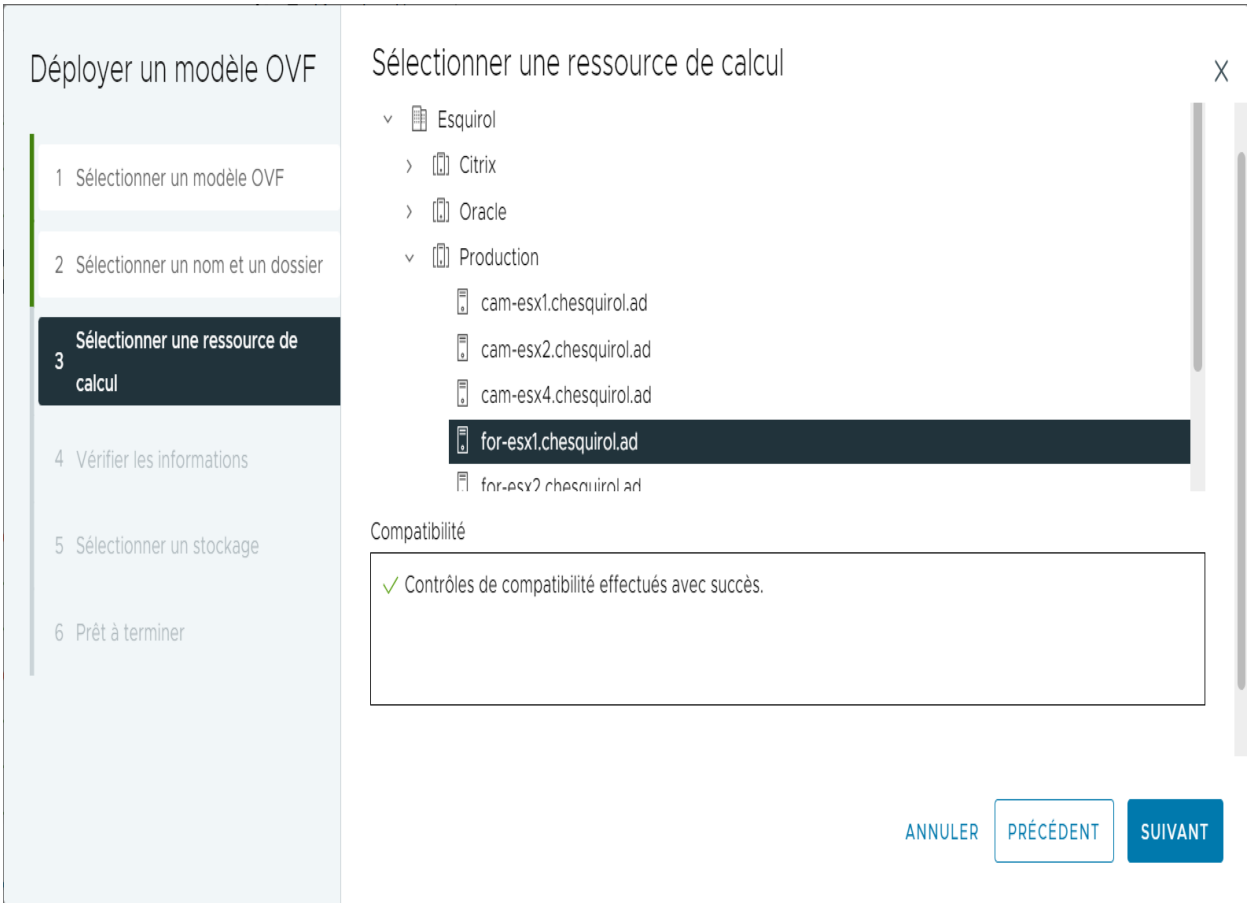
Etape 1 : Déploiement du contrôleur Cisco Catalyst 9800 sur l'hyperviseur VMware

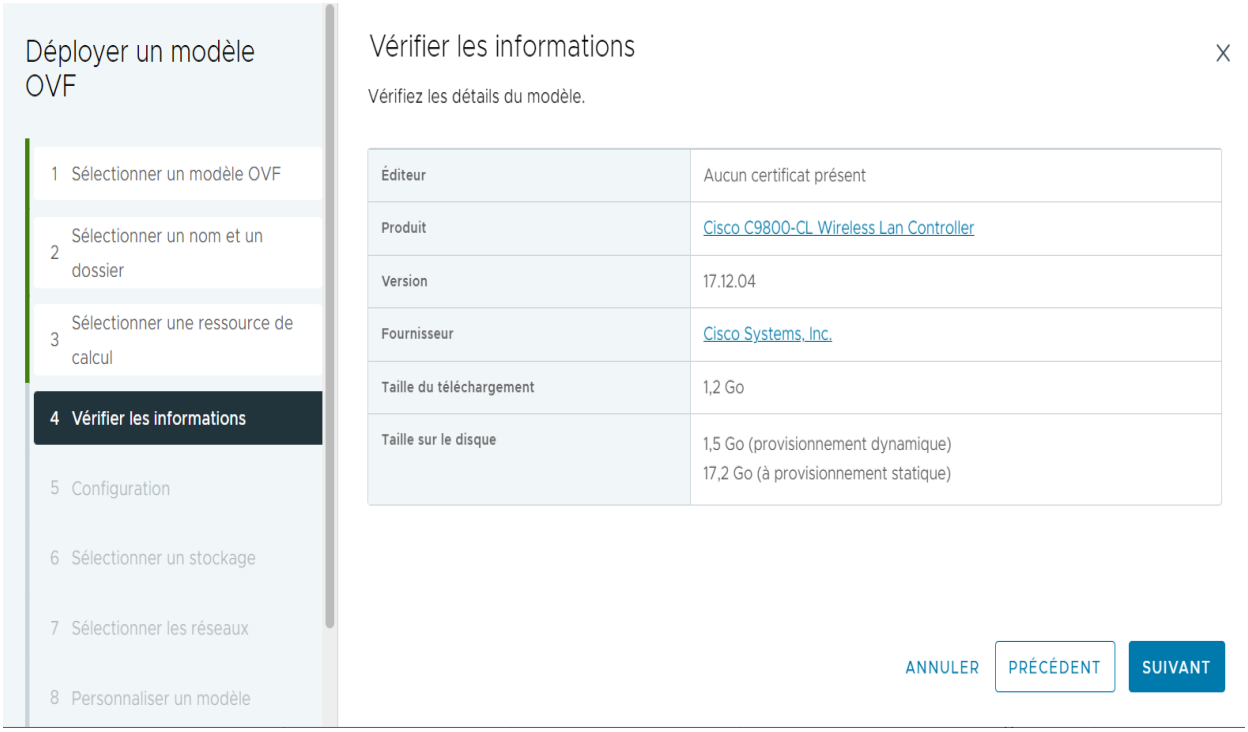
Déployer un modèle OVA/OVF depuis l'hyperviseur VMware (Client vSphere)



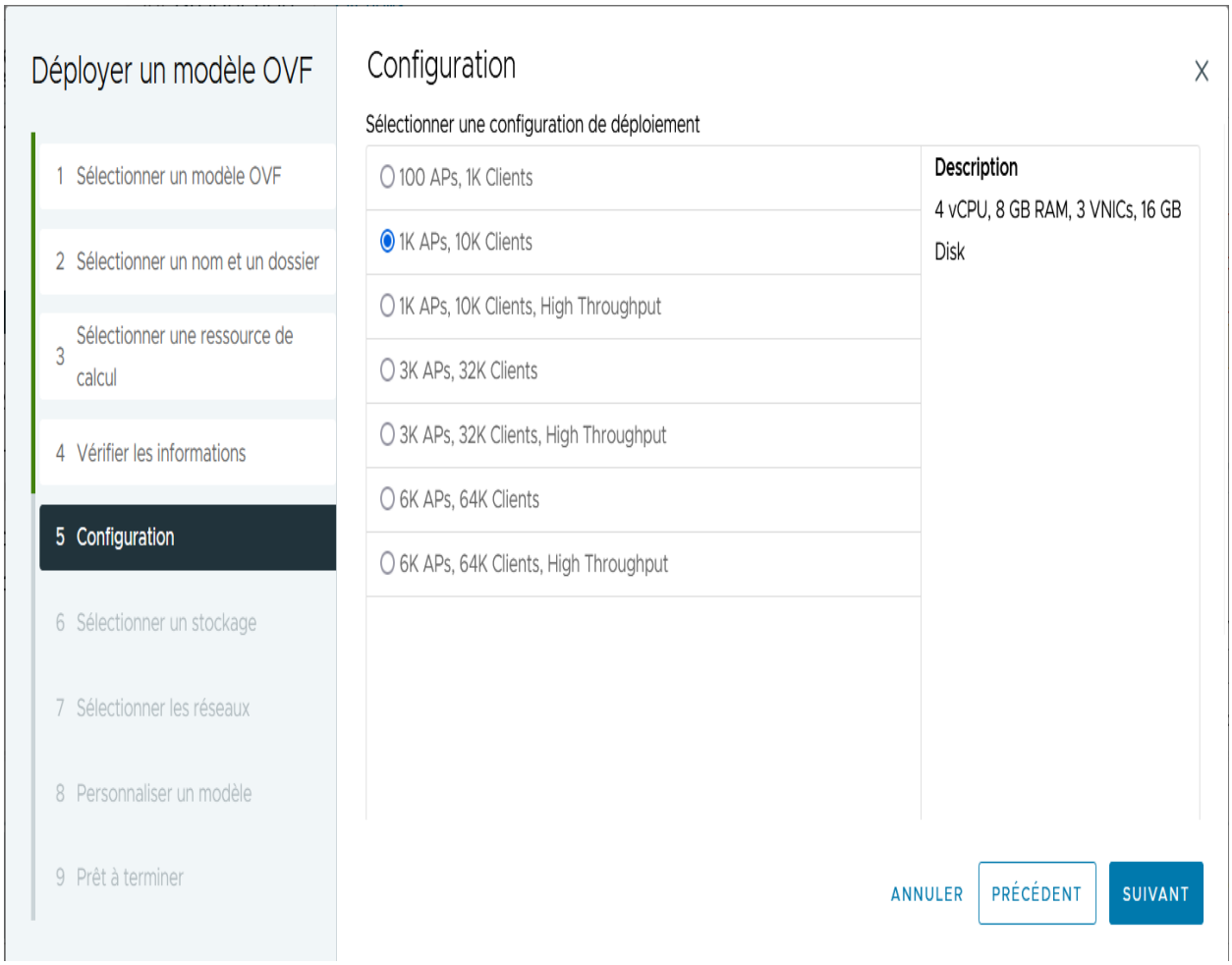
- On sélectionne ensuite une ressource de calcul dans **/Esquirol/Production/**

7


Déployer un modèle OVF
1 Sélectionner un modèle OVF
2 Sélectionner un nom et un dossier
3 Sélectionner une ressource de calcul
4 Vérifier les informations
5 Sélectionner un stockage
6 Prêt à terminer
Sélectionner une ressource de calcul
X
Esquirol
Citrix
Oracle
Production
cam-esx1.chesquirol.ad
cam-esx2.chesquirol.ad
cam-esx4.chesquirol.ad
for-esx1.chesquirol.ad
Compatibilité
✓ Contrôles de compatibilité effectués avec succès.
ANNULER
PRÉCÉDENT
SUIVANT

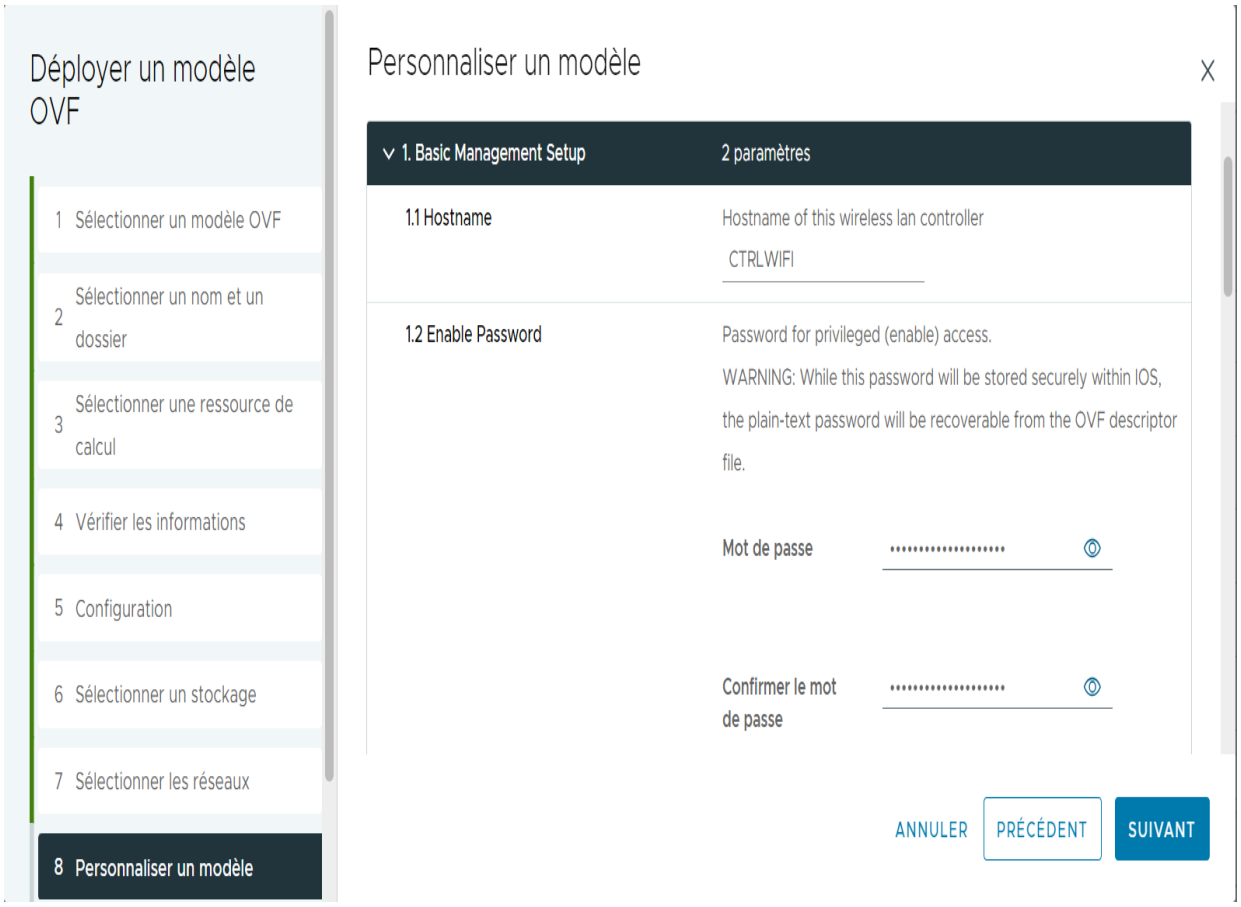

Déployer un modèle OVF
1 Sélectionner un modèle OVF
2 Sélectionner un nom et un dossier
3 Sélectionner une ressource de calcul
4 Vérifier les informations
5 Configuration
6 Sélectionner un stockage
7 Sélectionner les réseaux
8 Personnaliser un modèle
Vérifier les informations
X
Vérifiez les détails du modèle.
Éditeur
Aucun certificat présent
Produit
Cisco C9800-CL Wireless Lan Controller
Version
17.12.04
Fournisseur
Cisco Systems, Inc.
Taille du téléchargement
1,2 Go
Taille sur le disque
1,5 Go (provisionnement dynamique)
17,2 Go (à provisionnement statique)
ANNULER
PRÉCÉDENT
SUIVANT

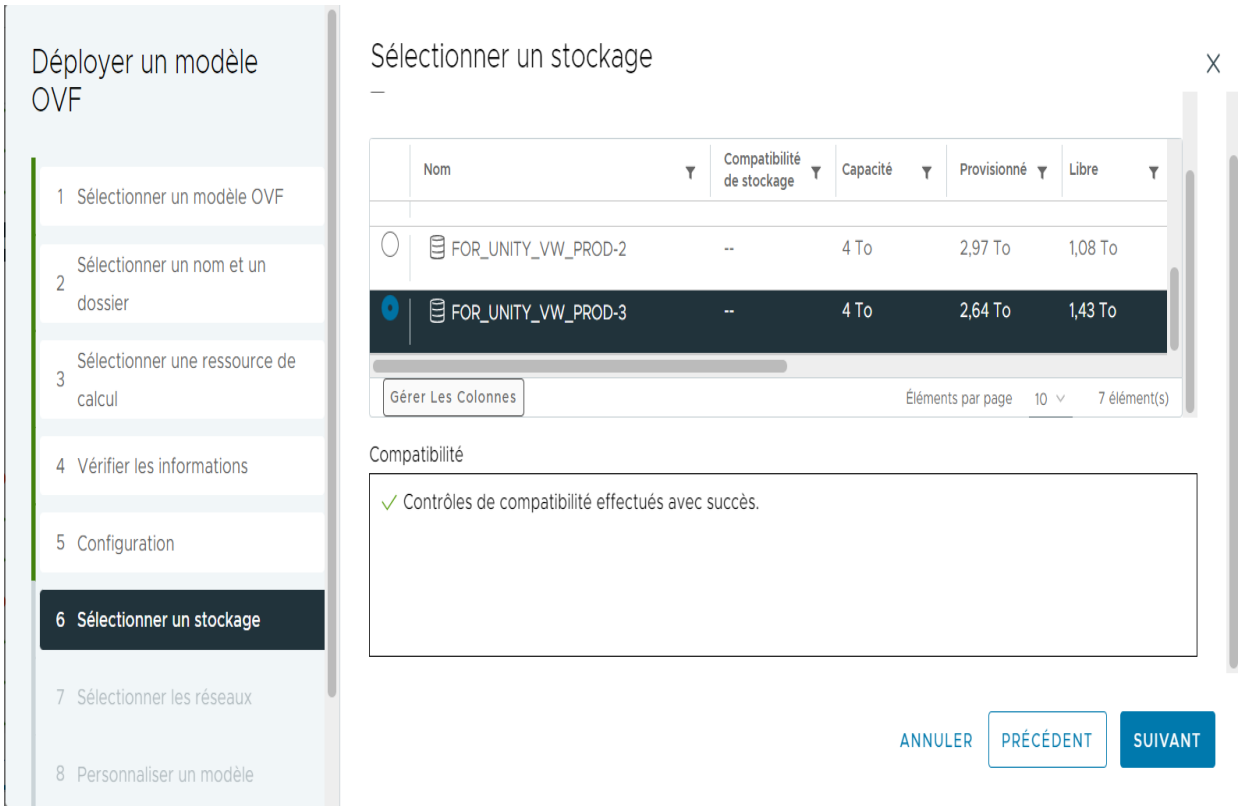
- Le profil du contrôleur choisi étant « **Small** » (Le nombre des APs ne dépasse pas 1000), on choisit 1k APs, 10k Clients pour la configuration de déploiement.



Ensuite créez un mot de passe pour le mode privilégié (Enable password) afin de sécuriser la configuration du contrôleur via le consol.

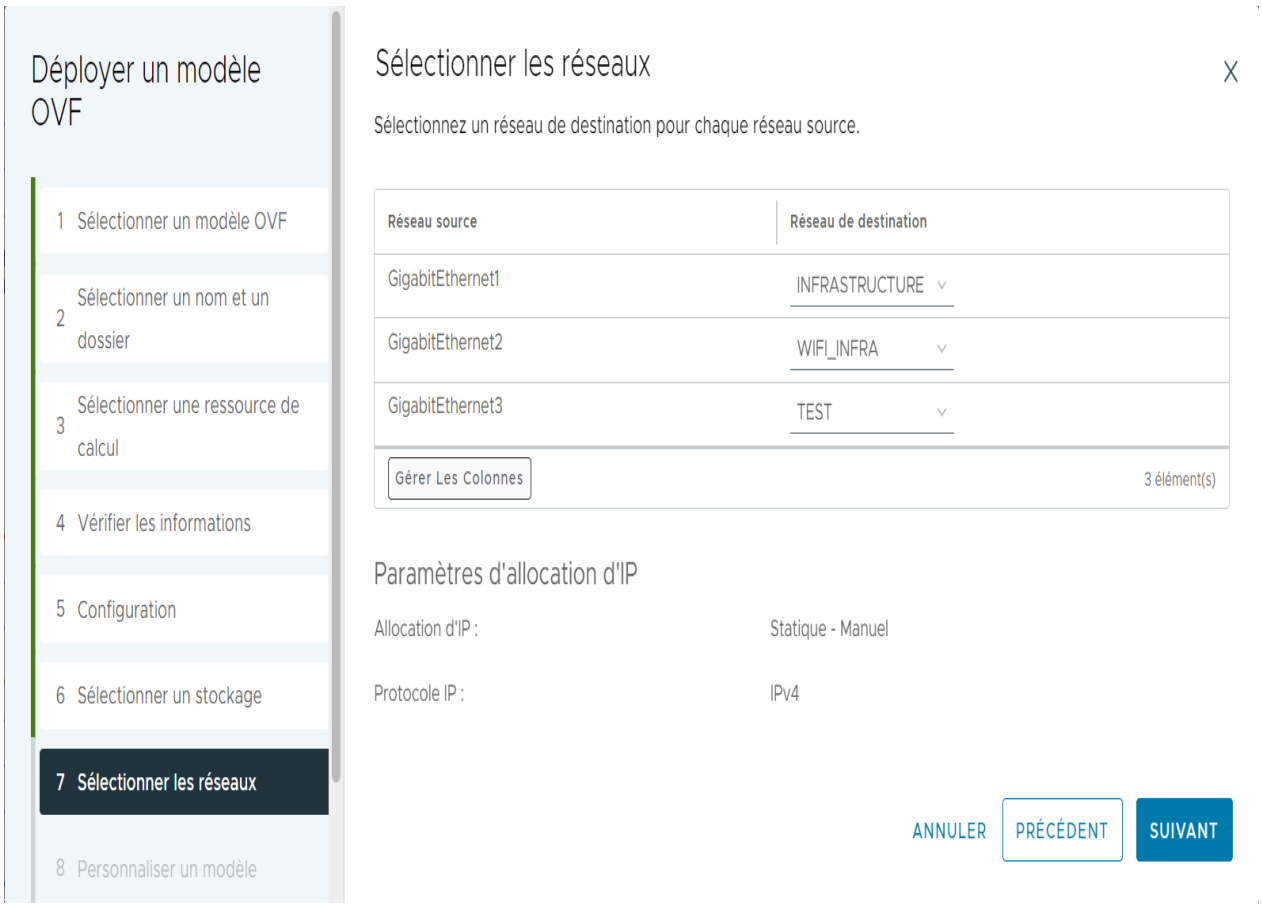
9


Déployer un modèle OVF
1 Sélectionner un modèle OVF
2 Sélectionner un nom et un dossier
3 Sélectionner une ressource de calcul
4 Vérifier les informations
5 Configuration
6 Sélectionner un stockage
7 Sélectionner les réseaux
8 Personnaliser un modèle
Personnaliser un modèle
X
1. Basic Management Setup
2 paramètres
1.1 Hostname
Hostname of this wireless lan controller
CTRLWIFI
1.2 Enable Password
Password for privileged (enable) access.
WARNING: While this password will be stored securely within IOS, the plain-text password will be recoverable from the OVF descriptor file.
Mot de passe
Confirmer le mot de passe
ANNULER
PRÉCÉDENT
SUIVANT


Déployer un modèle OVF
1 Sélectionner un modèle OVF
2 Sélectionner un nom et un dossier
3 Sélectionner une ressource de calcul
4 Vérifier les informations
5 Configuration
6 Sélectionner un stockage
7 Sélectionner les réseaux
8 Personnaliser un modèle
Sélectionner un stockage
X
Nom
Compatibilité de stockage
Capacité
Provisionné
Libre
FOR_UNITY_VW_PROD-2
-- 4 To 2,97 To 1,08 To
FOR_UNITY_VW_PROD-3
-- 4 To 2,64 To 1,43 To
Gérer Les Colonnes
Éléments par page 10
7 élément(s)
Compatibilité
Contrôles de compatibilité effectués avec succès.
ANNULER
PRÉCÉDENT
SUIVANT

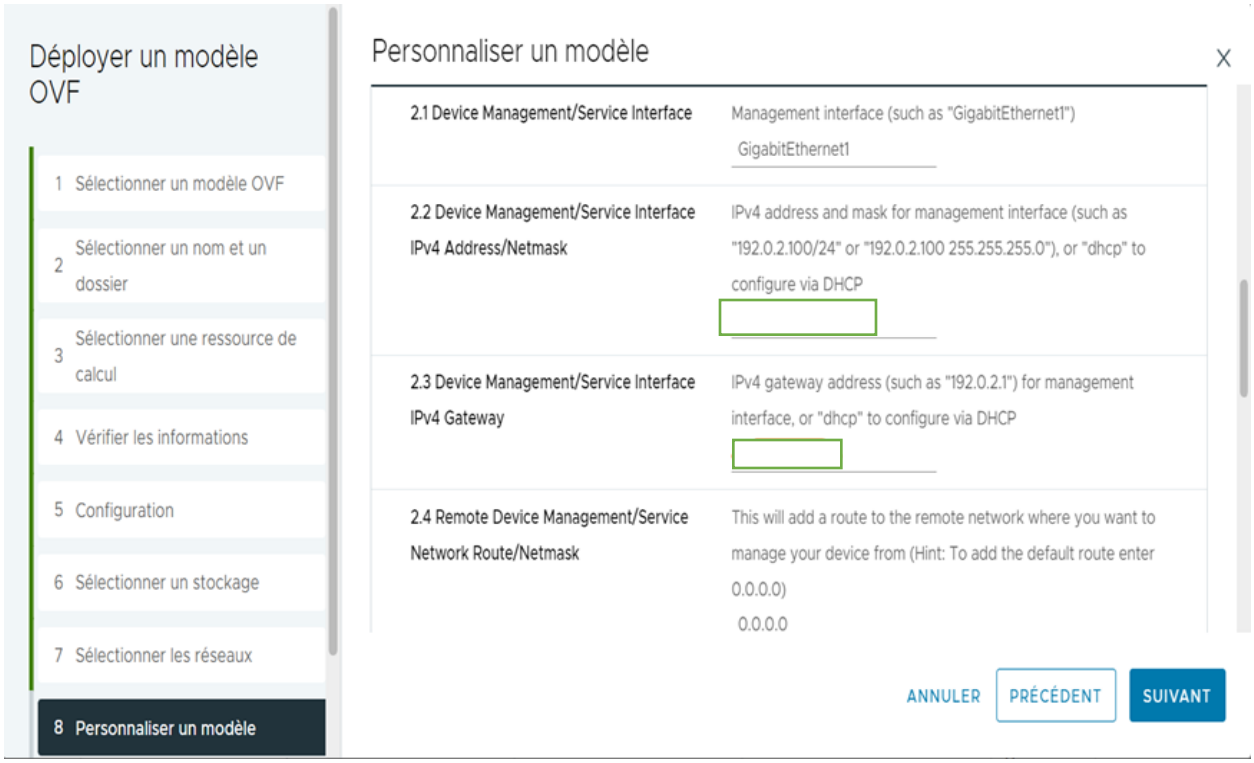
À partir de la liste déroulante de mappage du réseau, attribuez 3 cartes d'interface réseau virtuelle (vNIC) au réseau de destination. Connectez chaque carte à une interface unique.

- **GigabitEthernet 1** à l'interface de gestion des dispositifs et mappée sur le réseau de gestion hors bande (INFRASTRUCTURE).
- **GigabitEthernet 2** à l'interface de gestion sans fil et mappée sur le réseau permettant d'atteindre les points d'accès (AP) et les services. Habituellement, il s'agit d'un **Trunk** pour transporter plusieurs VLAN (WIFI_INFRA).
- **GigabitEthernet 3** à l'interface de haute disponibilité et mappée sur un réseau séparé pour la communication peer-to-peer pour le SSO (Ici, on mappe sur l'interface pour le teste, la haute disponibilité n'étant pas envisagée).

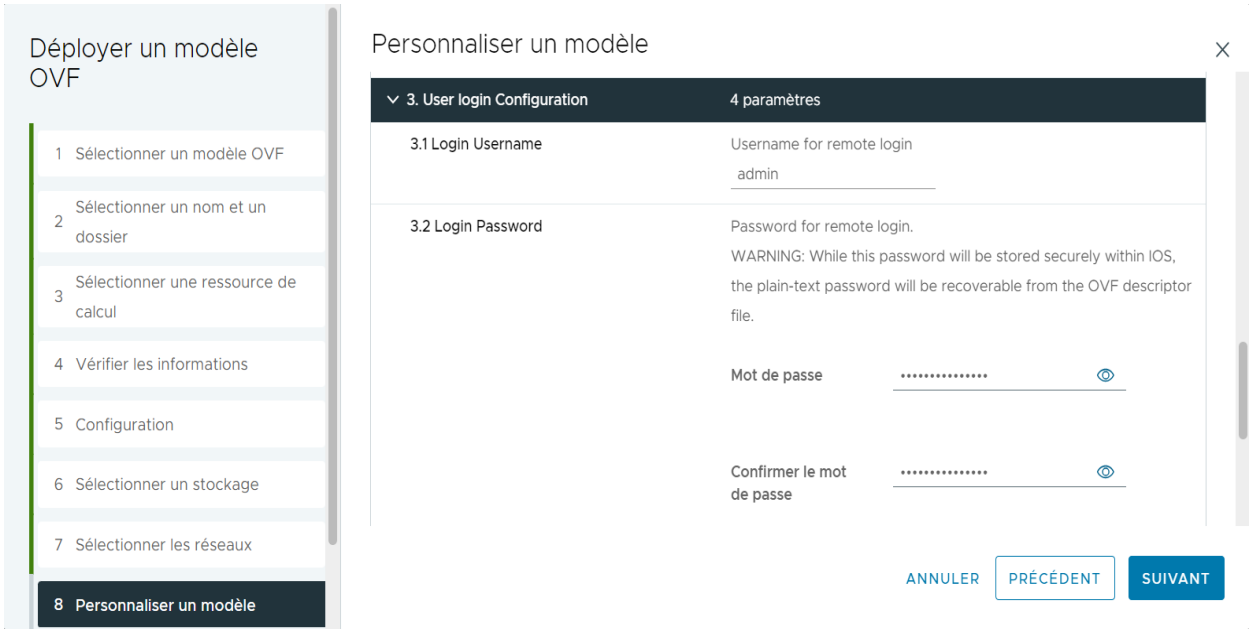


- On indique ensuite l'adresse de l'interface de gestion (pour accéder à l'interface graphique du contrôleur via https://<ip-adresse-contrôleur>)

11



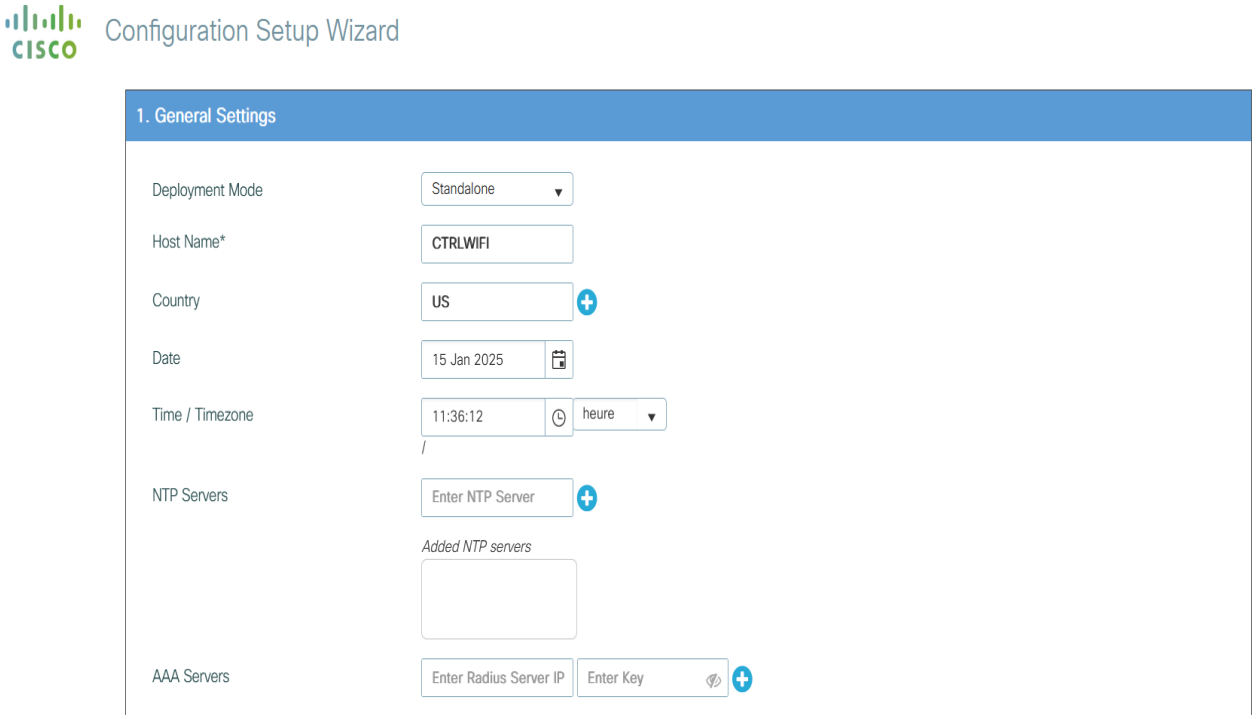
- On Crée un utilisateur admin pour accéder à l'interface graphique du contrôleur WiFi.



12

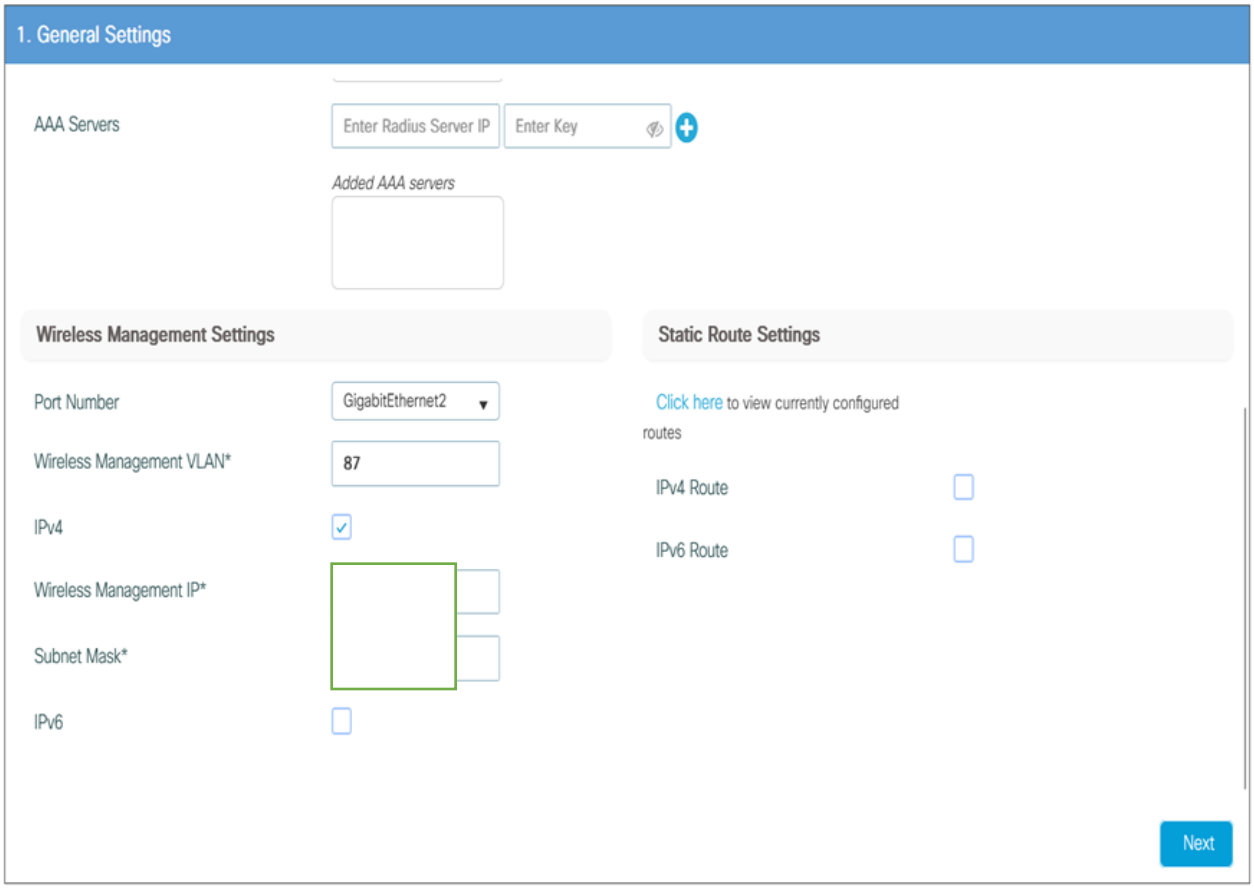
Etape 2 : Configuration du contrôleur Cisco Catalyst 9800 depuis l'interface graphique https://<ip-controleur>

Indiquer le nom du contrôleur, le pays (FR), et l'adresse IP du serveur NTP pour synchroniser l'heure.

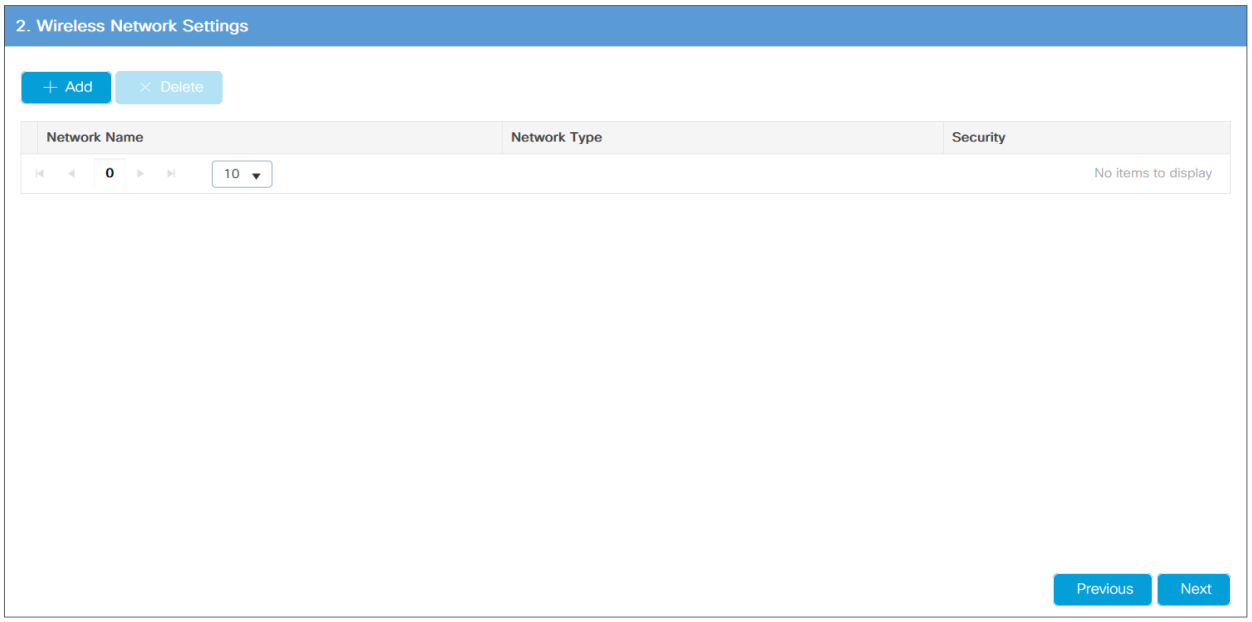


13

- On complétera l'adresse du serveur radius ultérieurement

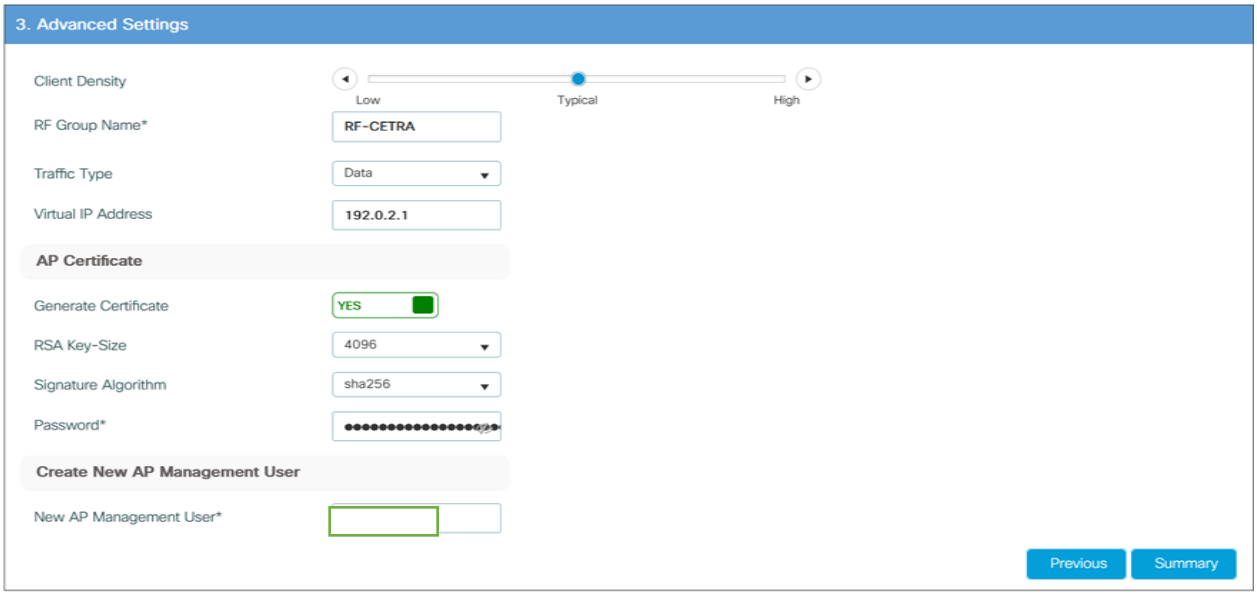


- On complètera cette partie ultérieurement. Cliquer sur **Next**



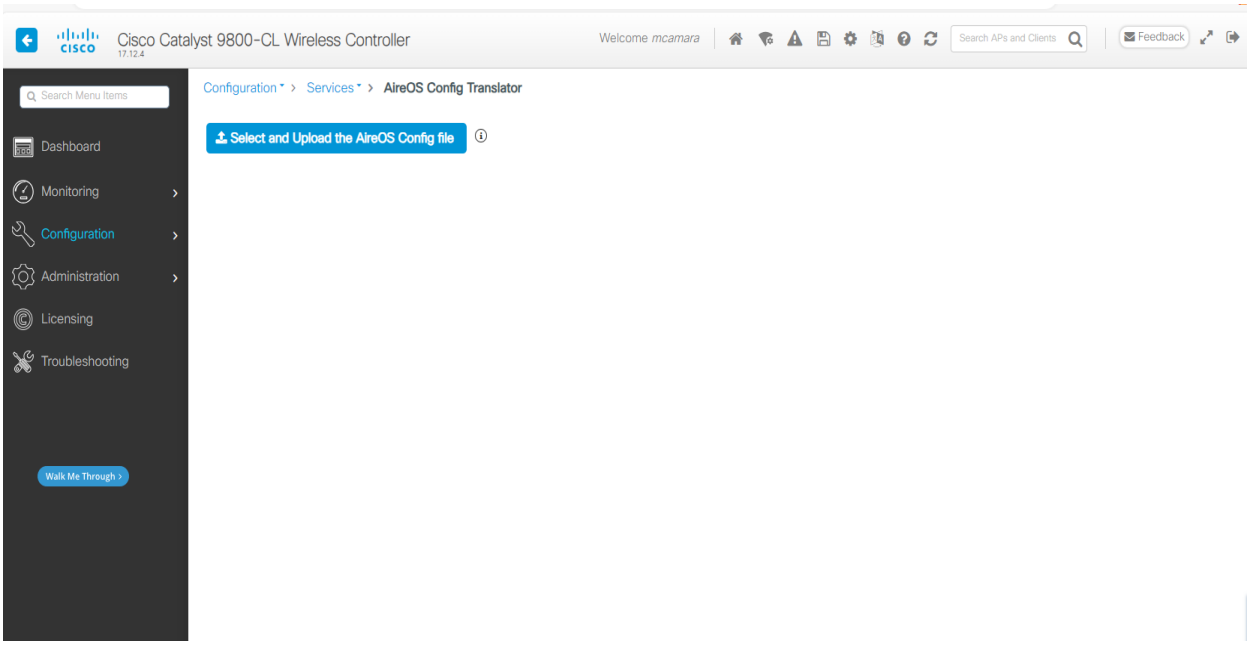
14

- Ensuite, indiquer le **groupe RF** (Radio Frequency Group) pour la gestion des paramètres RF, le **type du trafic** (Data). Laisser l'adresse IP virtuelle du contrôleur par défaut (192.0.2.1).



Etape 3 : déploiement de la configuration de l'ancien contrôleur Cisco WLC AireOS

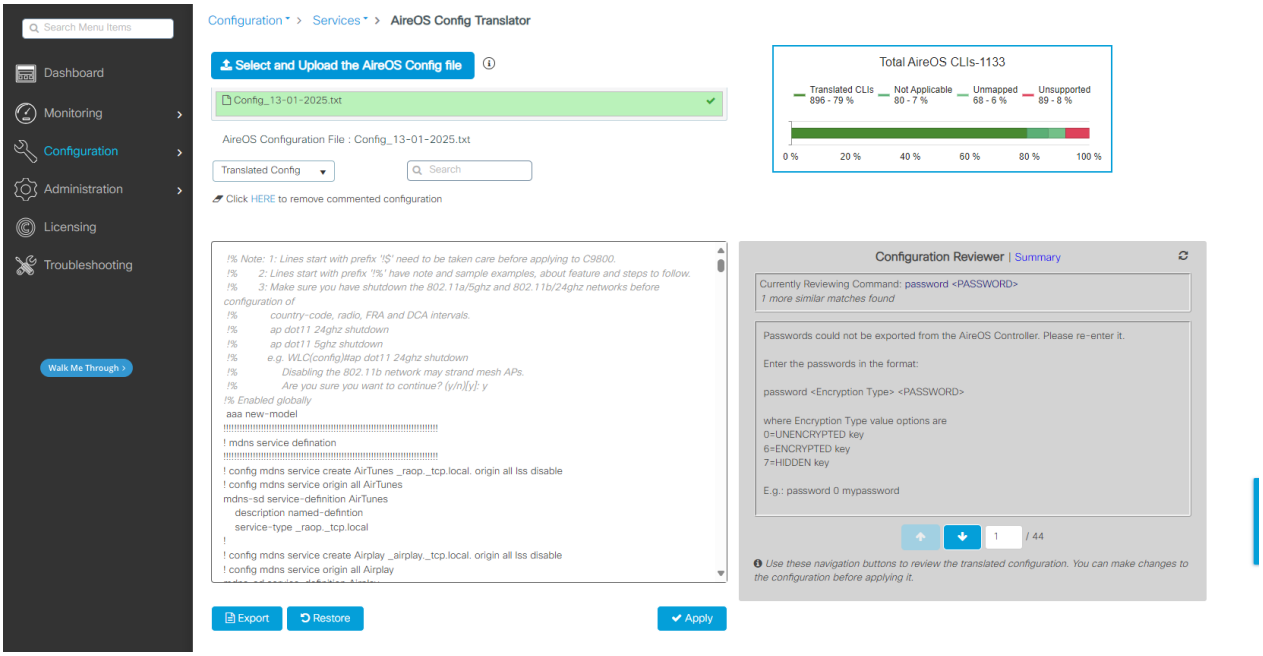
On déploie la configuration depuis **Configuration>Services.**
Ce service permet de transformer la configuration du contrôleur Cisco WLC **AireOS** (ancien contrôleur) en une configuration adapter au contrôleur **Cisco Catalyst 9800-CL.**



15

Une fois le fichier de configuration importé, on ajuste la configuration :

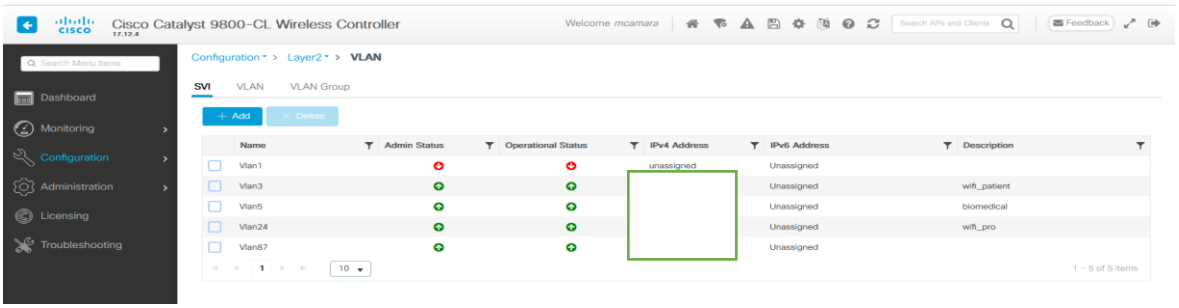
- Adresse IP des interfaces à modifier notamment pour celles de management,
- On indique les mots de passe des utilisateurs crées sur l'ancien contrôleur puisque les mots de passe contenant dans le fichier de configuration de Cisco AireOS ne peuvent pas être importés.
- Les clés du serveur Radius …



- **Problèmes rencontrés** : impossible de déployer la configuration de l'ancien contrôleur Cisco WLC AirOS. Problème d'incompatibilité au niveau de certains éléments notamment les balises entre les deux systèmes.
- **Solutions** : Configuration parallèle à l'ancien contrôleur (SVI, VLAN, WLAN, SSID, Policy & Tag, Flex Groupe, Groupe WLAN…)

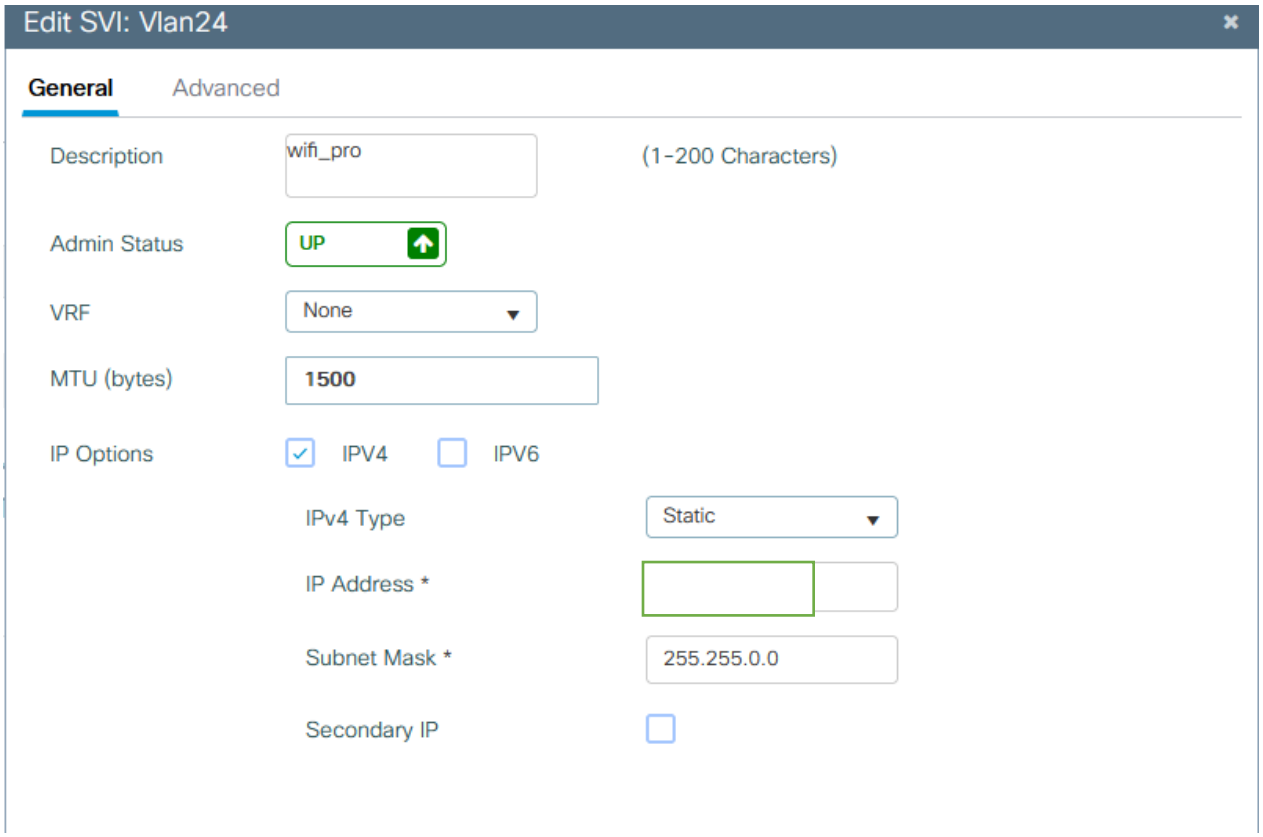
a. Configuration du Contrôleur

- Création des SVI pour les VLANs 3, 5, 24, 87 et 89

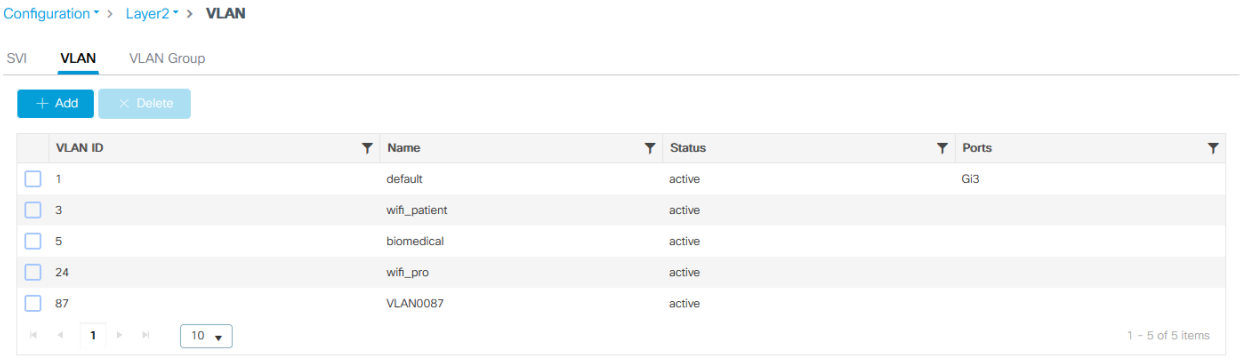


16

Le contrôleur a une interface dans chaque vlan (89, 87, 3, 5 et 24), de façon à pouvoir orienter le trafic (PRO/Patient) en fonction du SSID :



- Création de VLANs
  On crée un VLAN pour chaque SVI



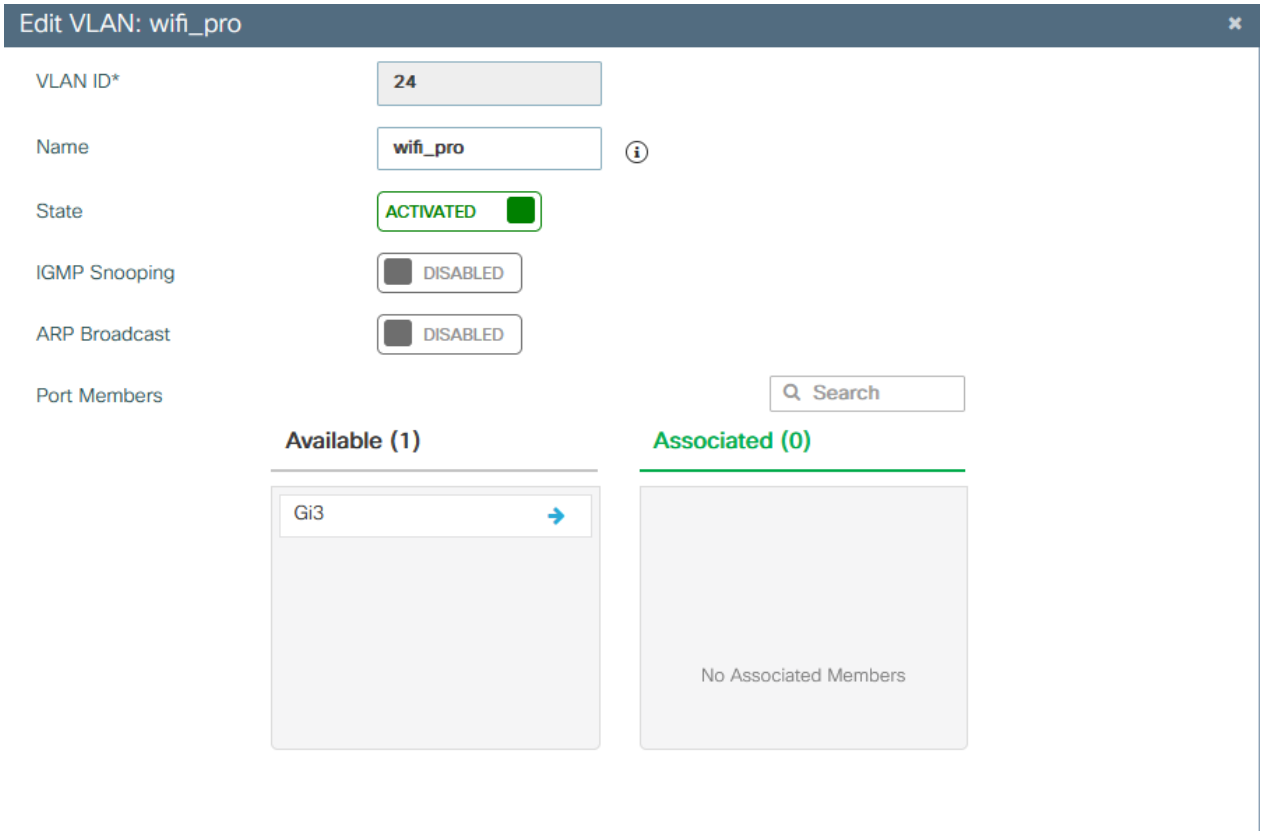
17

Déclarer les VLAN clients :

Avant de commencer la configuration, vous devez ajouter les VLAN nécessaires (VLAN auxquels les clients sans fil sont affectés).

Étape 1. Accédez à **Configuration > Layer2 > VLAN > VLAN > + Add**.

Étape 2. Saisissez les informations requises.

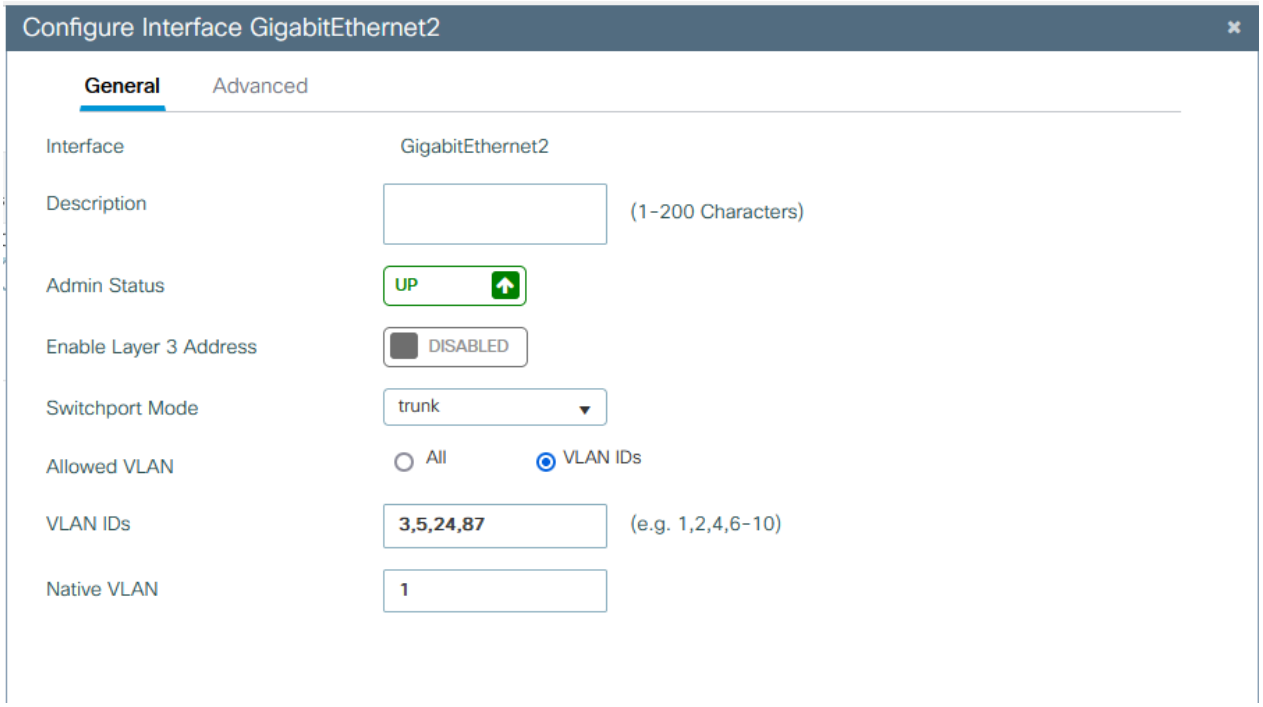


Répétez les étapes 1 et 2 pour tous les VLAN nécessaires. Une fois terminé, vous pouvez passer à l'étape 3.

Étape 3. Vérifiez que les VLAN sont autorisés dans vos interfaces de données.

Accédez à **Configuration > Interface > Ethernet > Nom d'interface > General**. Si vous le voyez configuré comme Allowed Vlan = All, vous avez terminé la configuration. Si vous voyez les ID VLAN autorisés = VLAN, ajoutez les VLAN nécessaires et ensuite cliquez sur **Update & Apply to Device**.
Aucune modification requise :

18



- Serveur Radius :

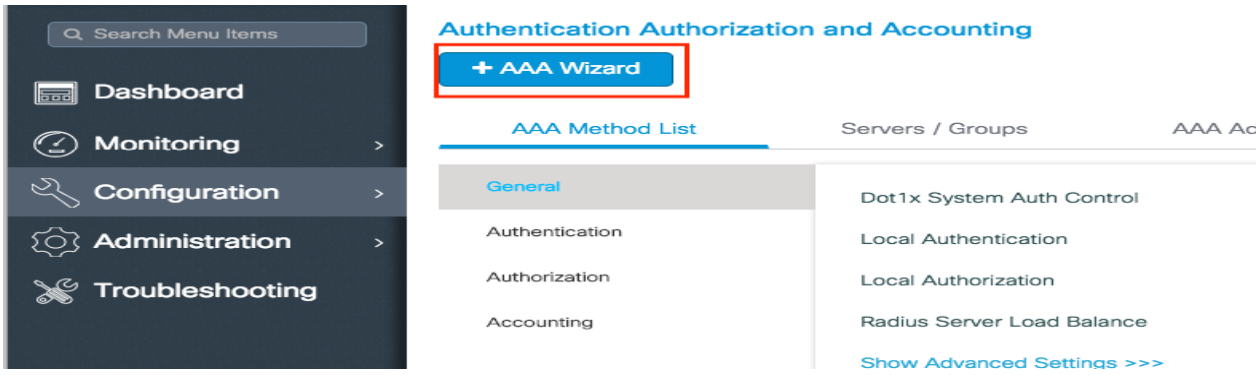
Pour l'installation des WLC Catalyst 9800, vous pouvez utiliser les assistants de configuration disponibles pour vous guider tout au long du processus de configuration.

Si vous devez utiliser des serveurs RADIUS sur votre déploiement, vous pouvez d'abord utiliser l'Assistant AAA, puis choisir entre la configuration sans fil de base ou avancée.

Si vous n'utilisez pas de serveurs RADIUS sur votre déploiement, vous pouvez accéder directement à la configuration sans fil de base ou avancée.

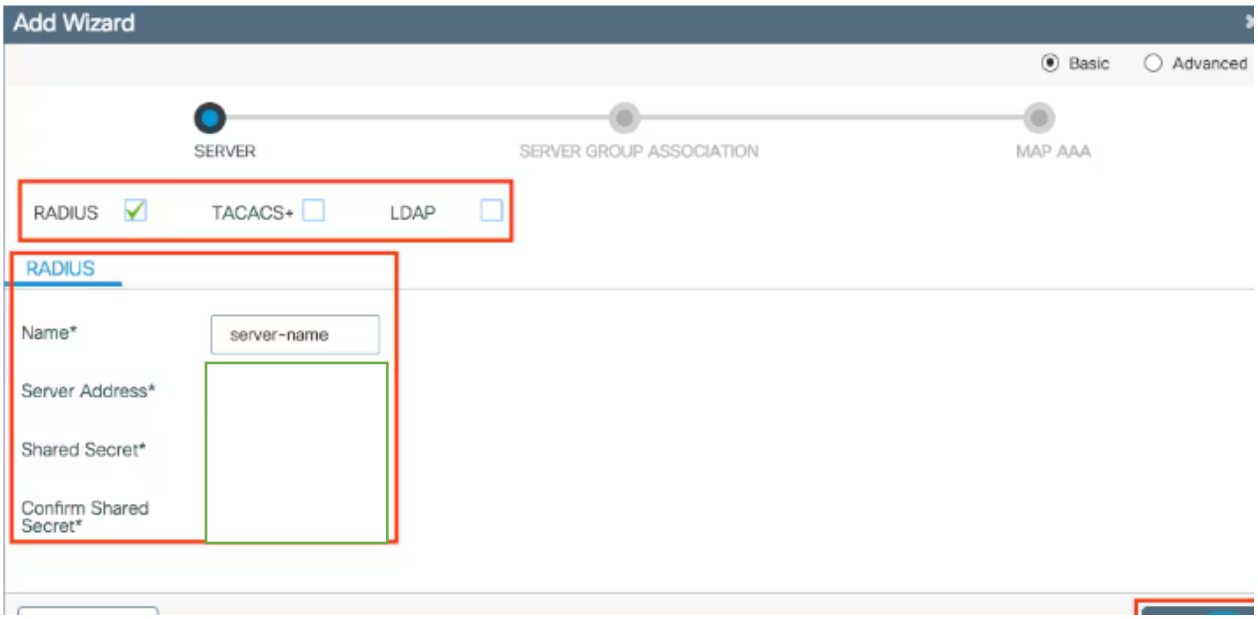
Assistant AAA

Étape 1. Accédez à **Configuration > Security > AAA > + AAA Wizard**.

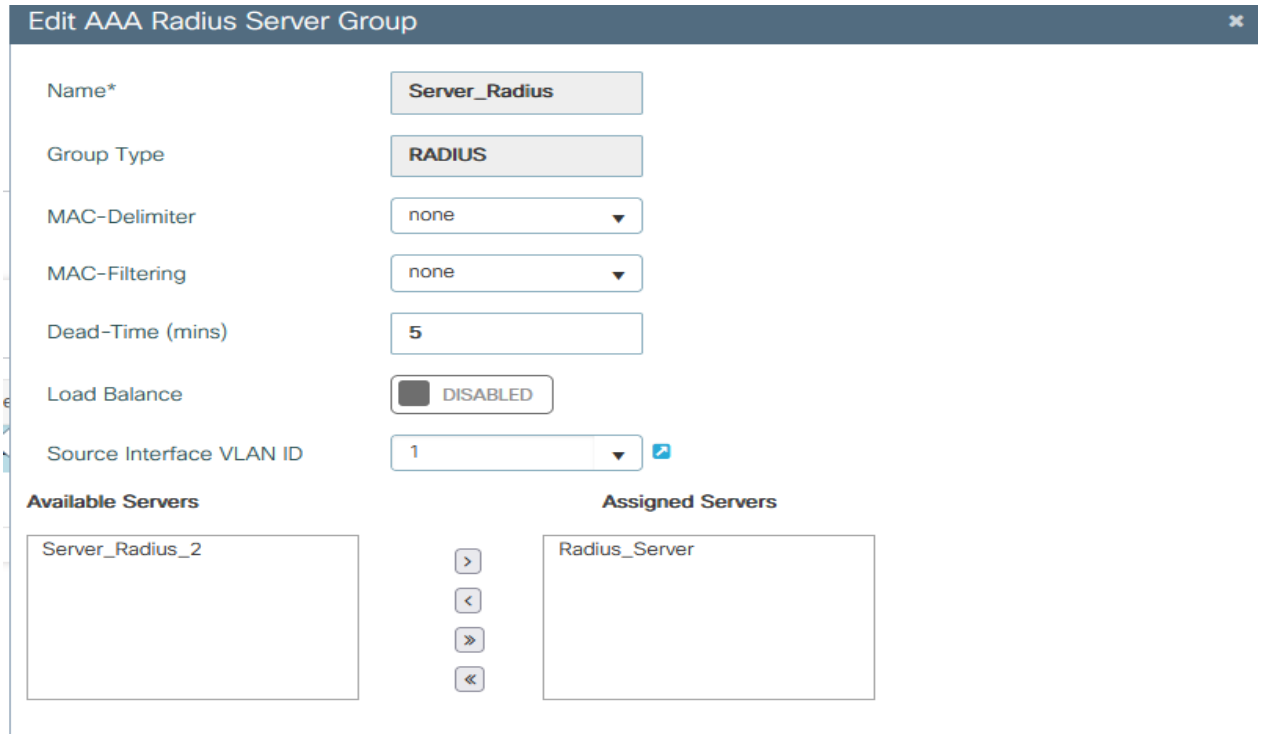


19

Étape 2 : Activez le type de serveurs requis et entrez un nom de serveur (il peut s'agir de l'adresse IP ou de toute autre chaîne), l'adresse IP du serveur et le secret partagé. Après cela, cliquez sur **Next**.



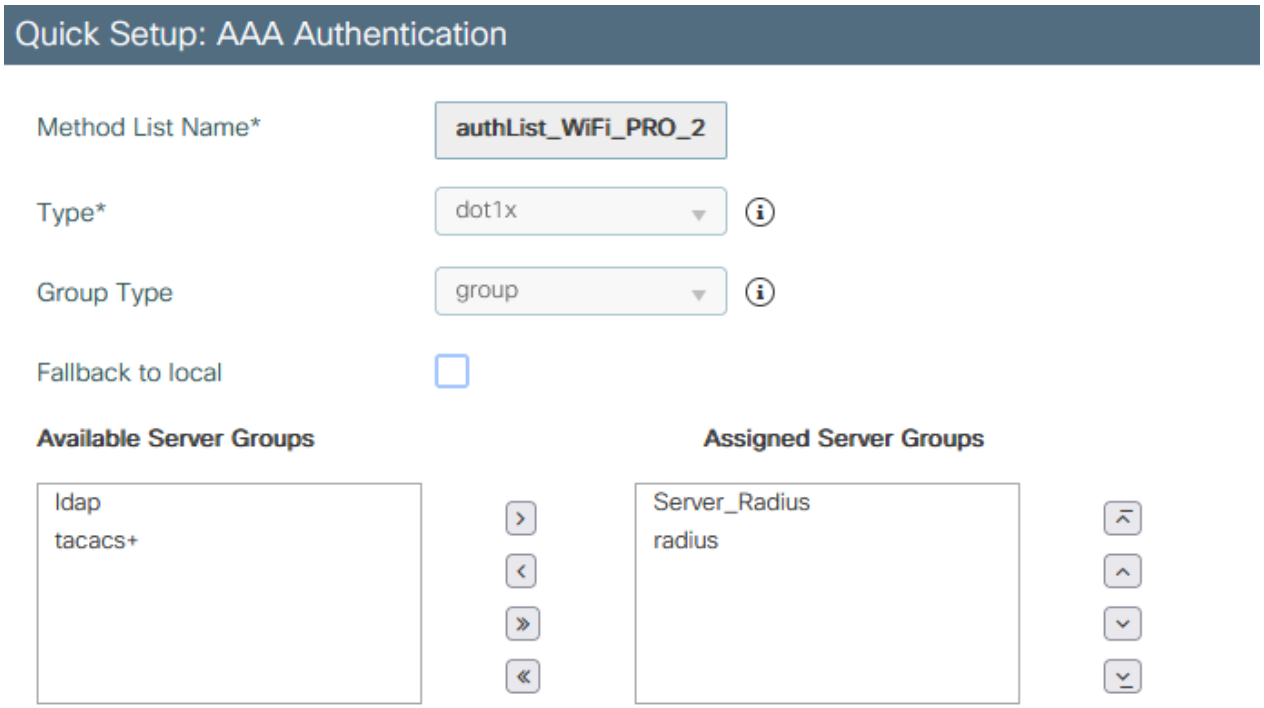
Étape 3. Entrez les informations nécessaires à la création d'un groupe de serveurs. Assurez-vous d'ajouter le serveur spécifié à l'étape précédente aux **serveurs affectés**.



20

Étape 4 : Activez l'authentification et créez une méthode d'authentification.

Accédez à l'onglet **Authentification** et saisissez les informations nécessaires. Une fois terminé, cliquez sur **Save & Apply to Device**



- WLANs (SSID)

WLAN sur les WLC 9800

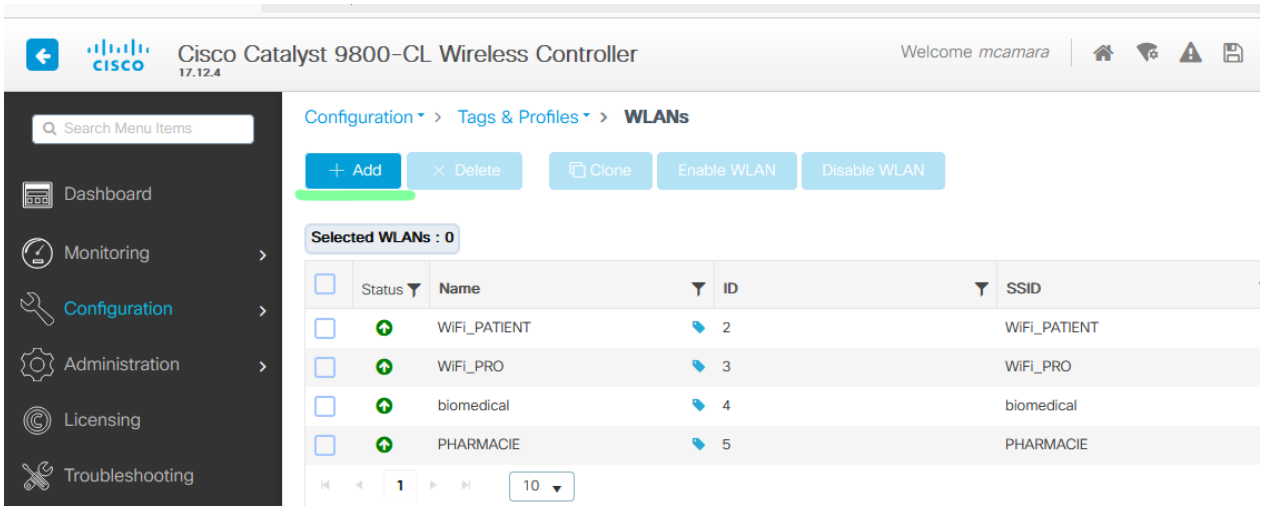
Flux de configuration :

1. Création des SSID

Créez votre SSID

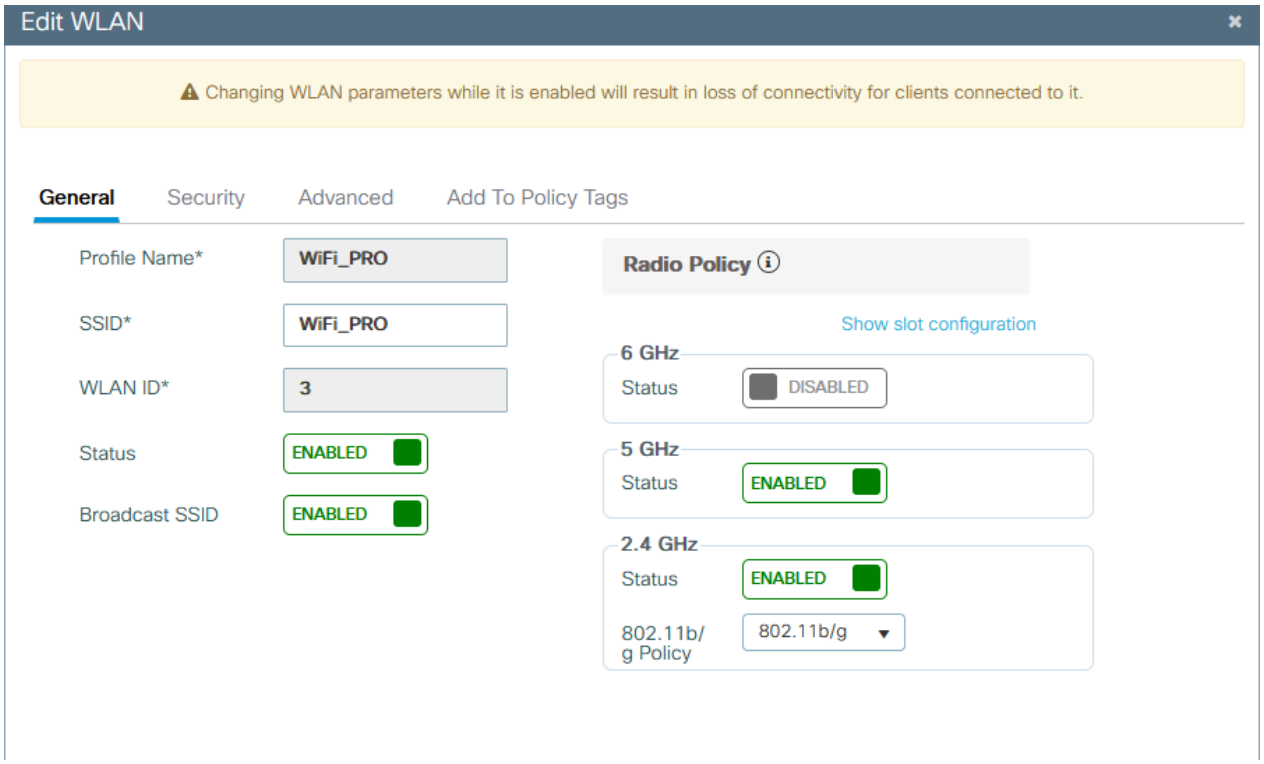
Étape 1. Accédez à **Configuration > Wireless > WLANs > + Add**.

21



- **Création de WLAN pour WiFi_PRO**
  Le SSID WiFi_PRO est configuré avec une authentification 802.1X alors que WiFi_PATIENT n'a pas de sécurité pour pouvoir se connecter, c'est le portail captif ucopia qui remplit ce rôle.

Dans l'onglet ***General,*** Entrez toutes les informations nécessaires (nom SSID, type de sécurité, etc.) et une fois terminé, cliquez sur **Save & Apply to Device**.

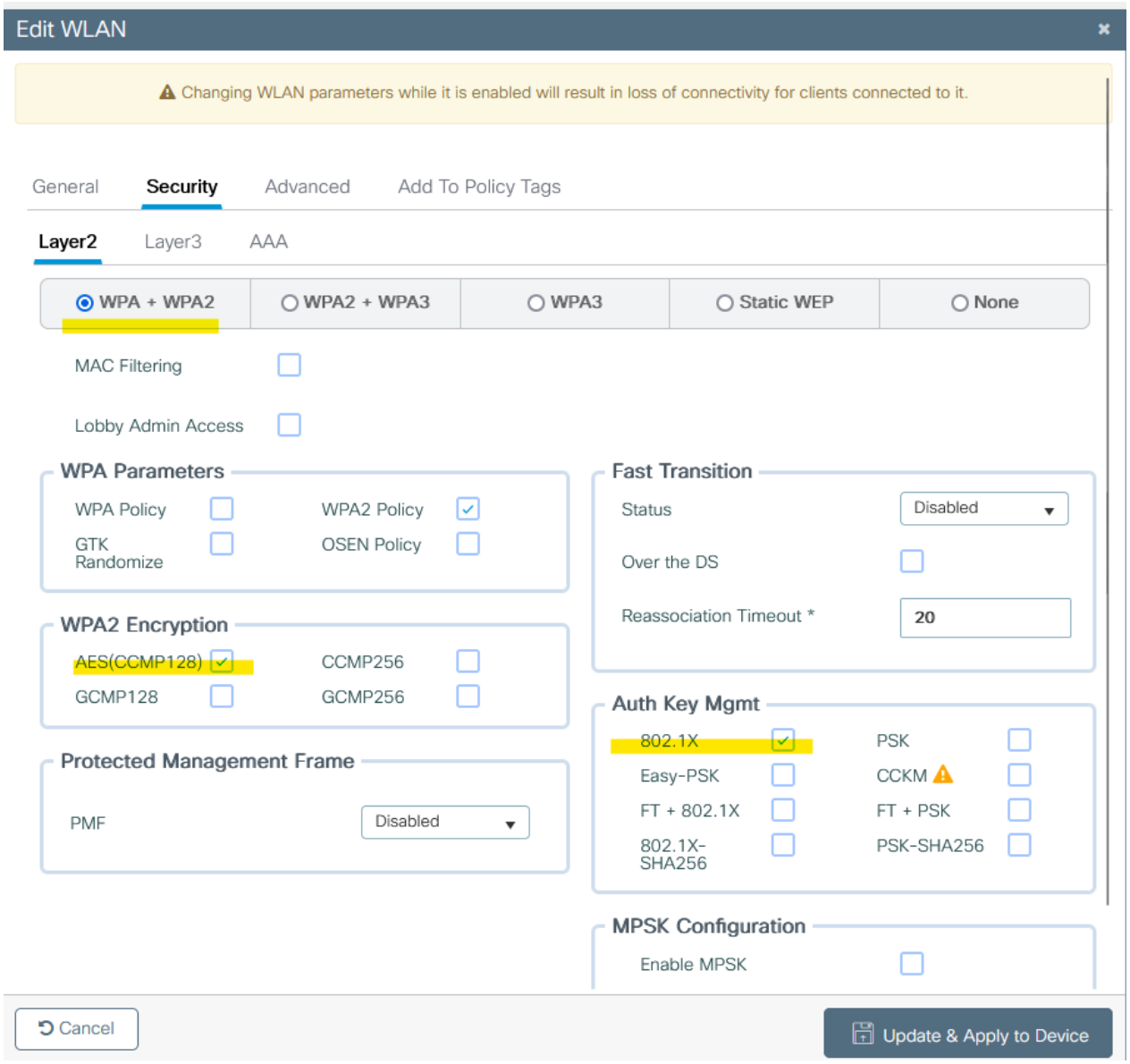


22

Dans l'onglet Security, on précise le type d'authentification.

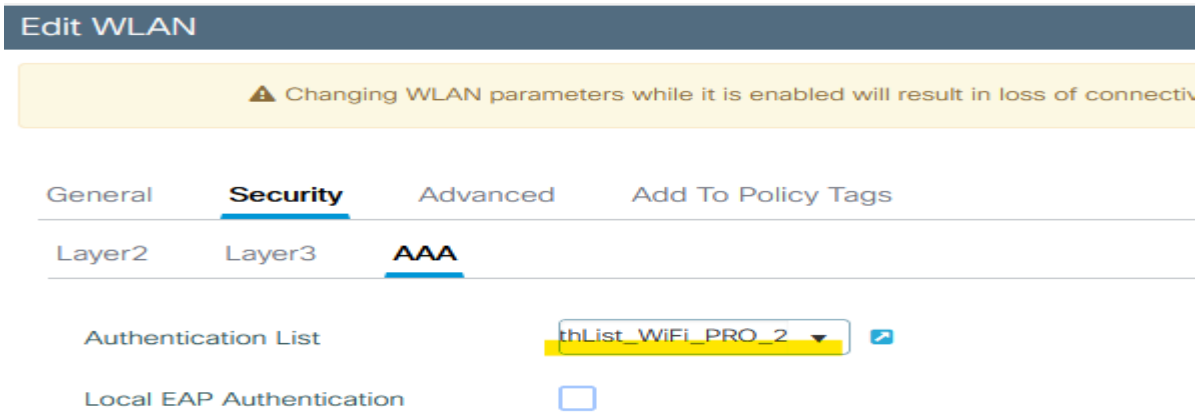
Ce SSID est affecté à l'interface wifi_pro correspondant au vlan 24. L'authentification utilisé est le 802.1x.

Par mesure de sécurité la diffusion du SSID est caché.

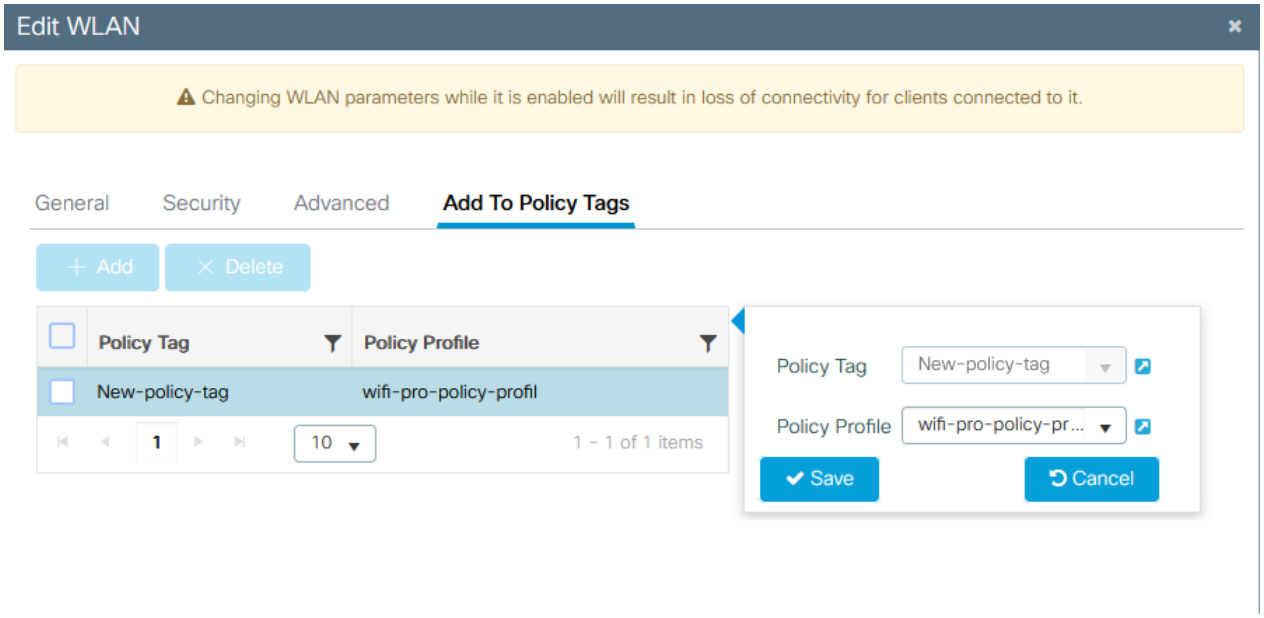


Ensuite, on précise la méthode d'authentification dans la liste déroulante de ***Authentification list***

23



On précise le policy Tags (Stratégie de police) qui permet de gérer finement le comportement, l'accès des utilisateurs et des dispositifs sur le réseau sans fil.



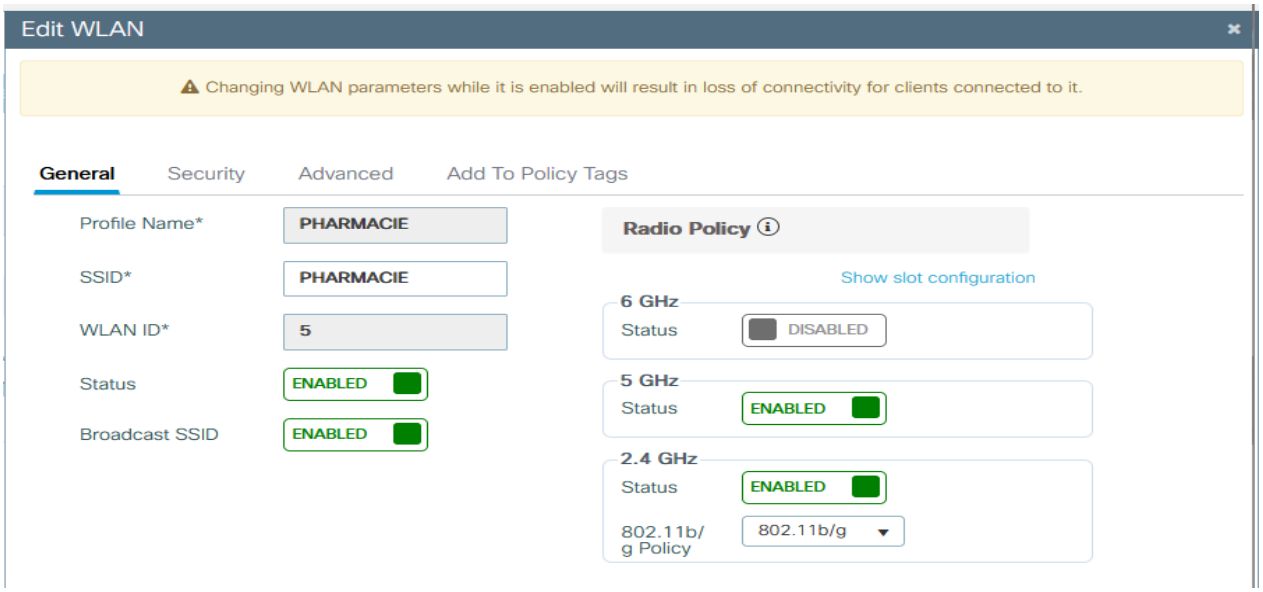
- **Création de WLAN PHARMACIE avec filtrage des adresses MAC**

  Le réseau **wifi Pharmacie** est spécifique et diffusé que dans le bâtiment pharmacie. L'authentification se fait avec une clé **WPA** et déclaration des adresses **MAC** sur le contrôleur wifi.

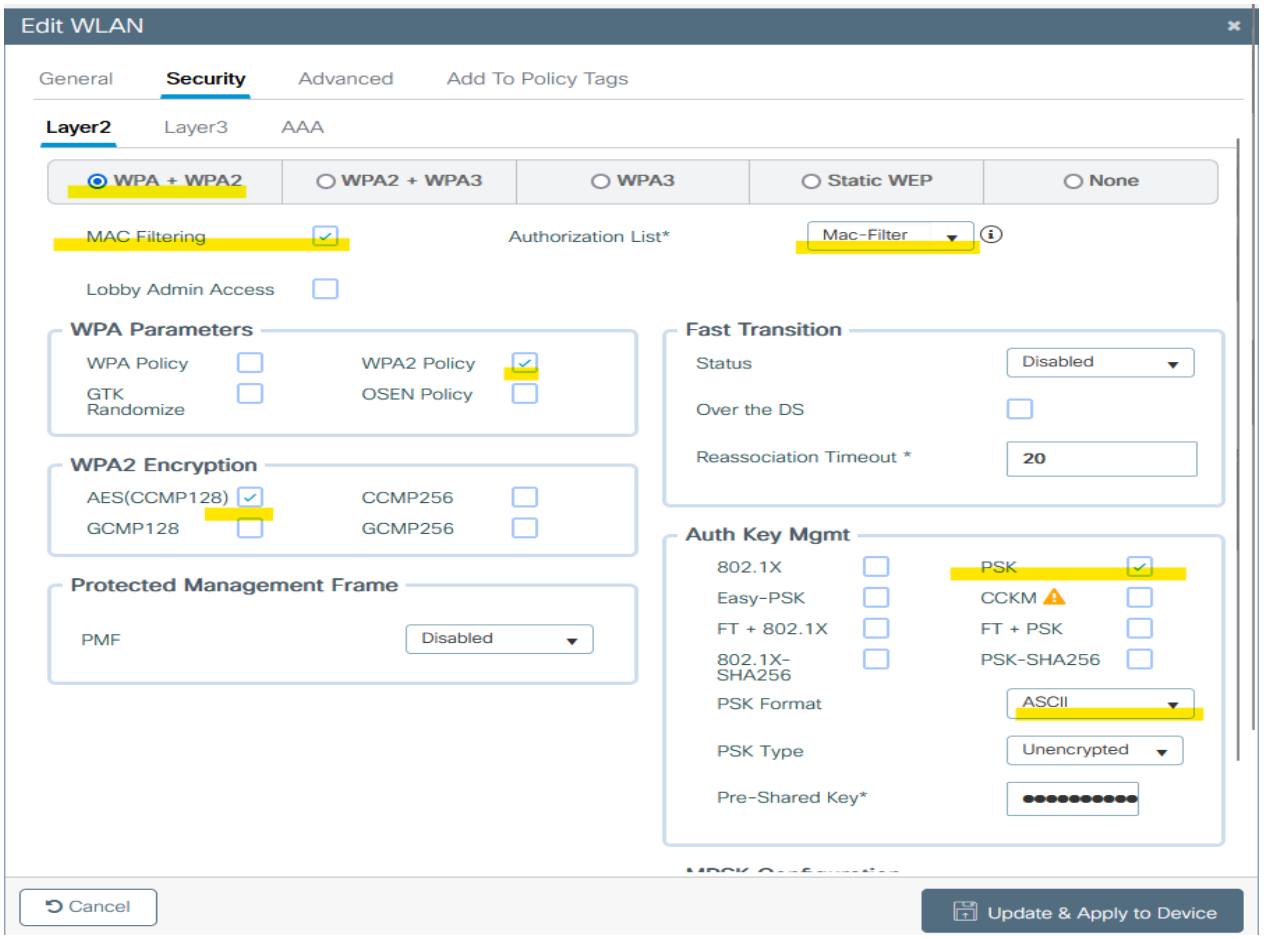
  Etape 1 : Accéder dans **Configuration>Policy&Tags>WLANs ,** puis click sur **+Ajouter**

  On saisit les information nécessaire (SSID, le nom du profil ..)

24

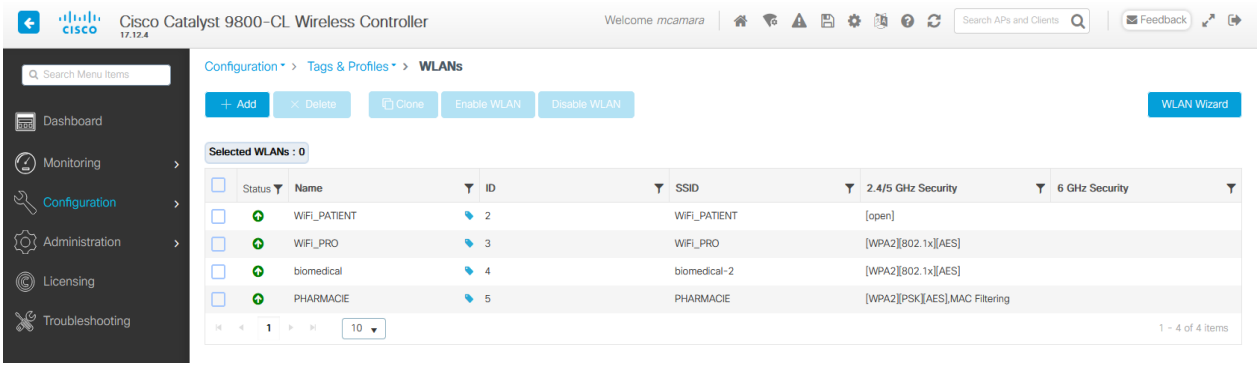


Dans l'onglet ***Security***, activez ***MAC Filtering***. Dans la liste déroulante de ***Authorization List***, sélectionnez la méthode d'autorisation **Mac-Filter** qui sera créée à l'étape suivante (étape 2), ensuite Cliquez sur **Save & Apply to Device.**



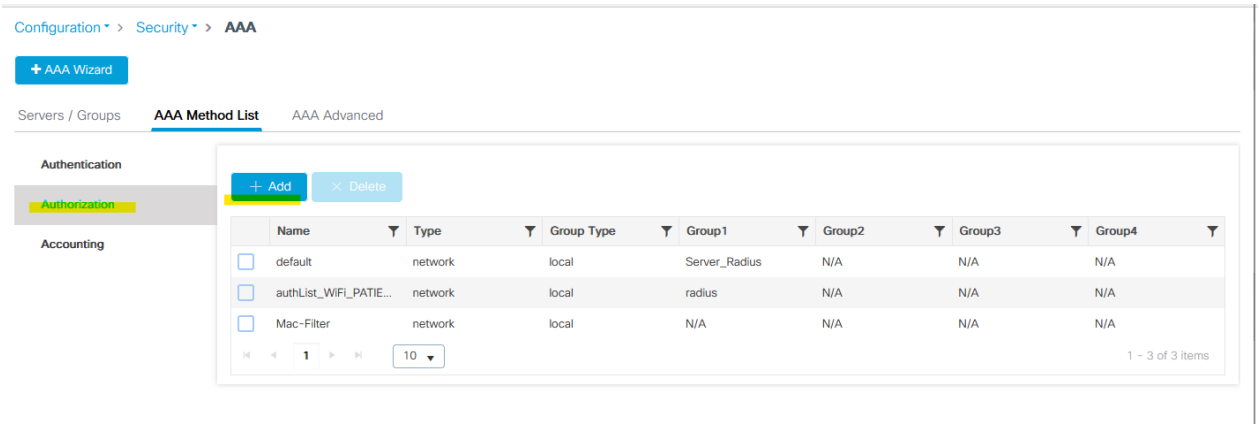
25

Au final, 4 SSID sont crées

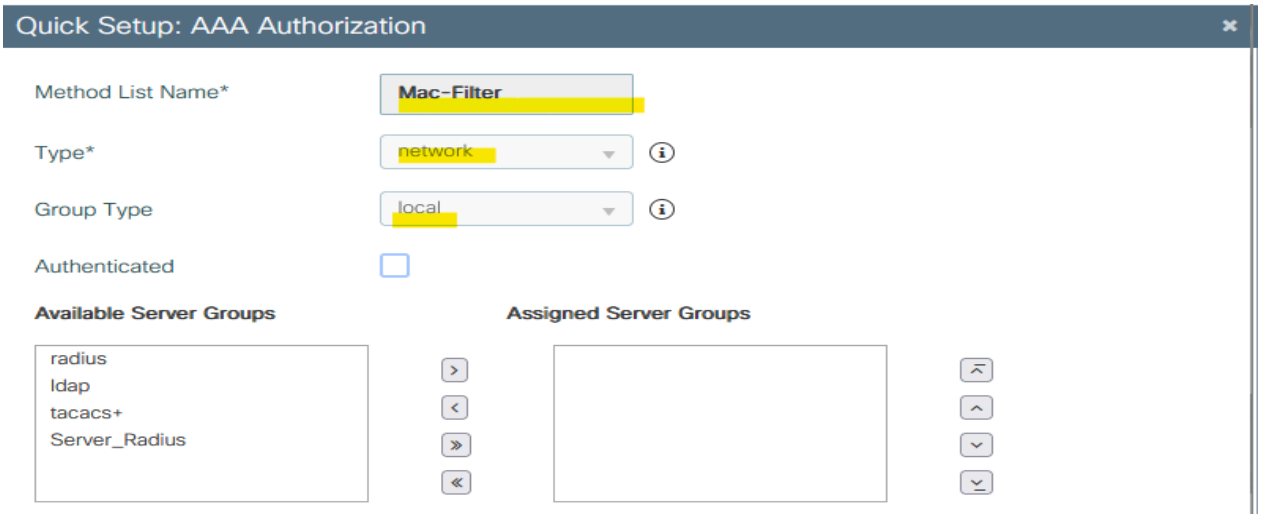


Etape 2 : Créez une méthode de réseau d'autorisation (Filtrage Mac).

Naviguez jusqu'à **Configuration > Security > AAA > AAA Method List > Authorization** > **+ Add** et créez-le.

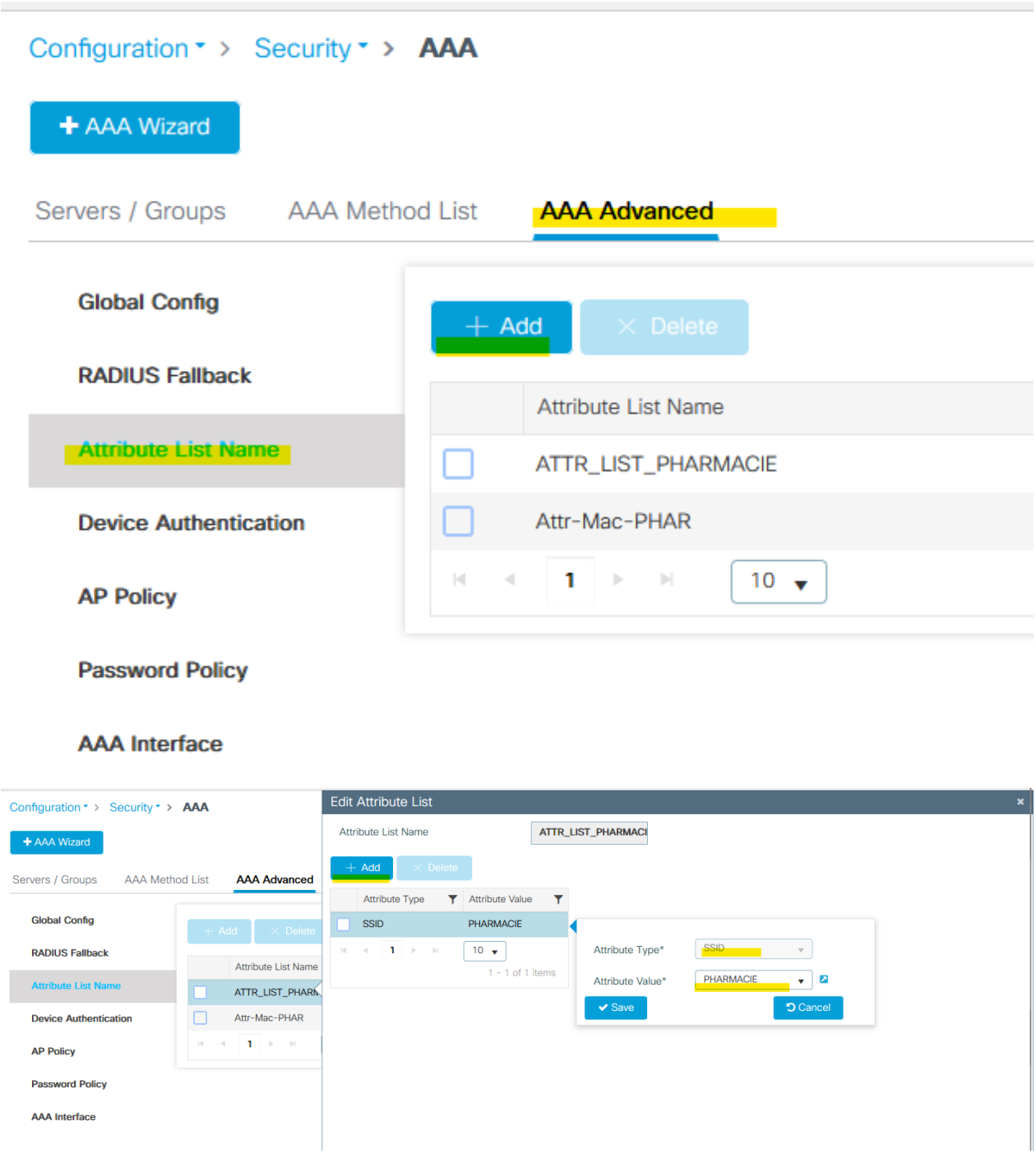


Indiquer le nom de la méthode (Mac-Filter), le type (network) et le groupe en local.



26

Ensuite on crée une attribue dans laquelle on indique le SSID qui nous concerne (**PHARMACIE**).
Accéder à **Configuration** > **Security** > **AAA** >**Attribute Liste Name**> + **Add**

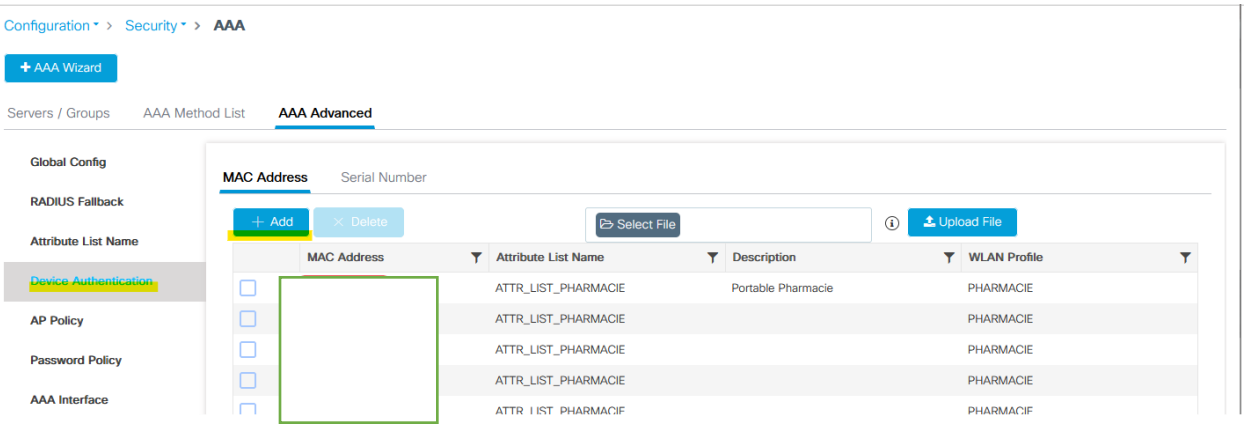


Enregistrez les adresses MAC autorisées.

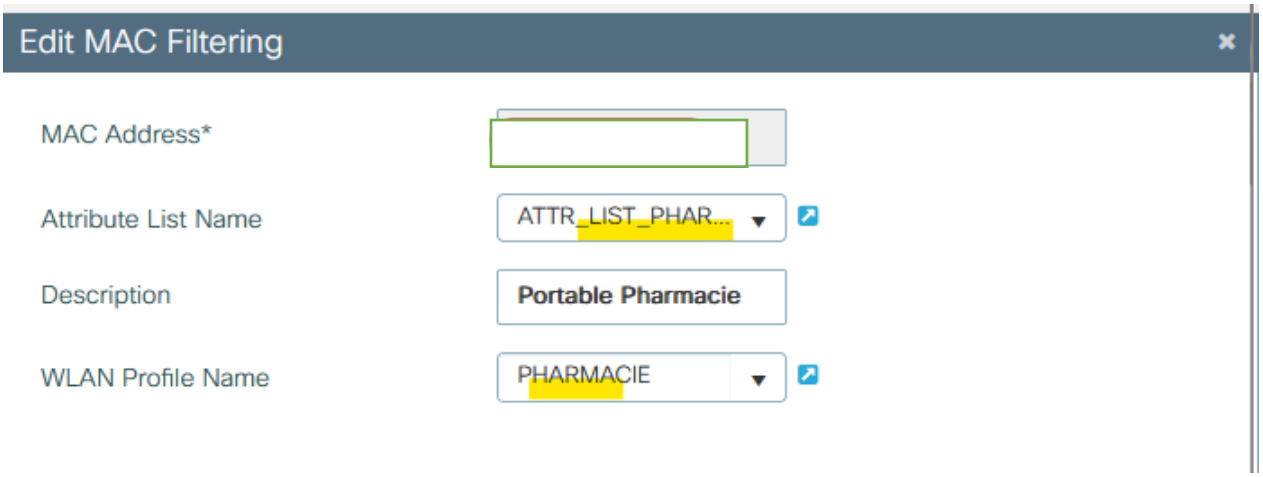
Enregistrez localement les adresses MAC sur le WLC pour l'authentification locale.

27

Accédez à **Configuration > Security > AAA > AAA Advanced > Device Authentication** > + Add



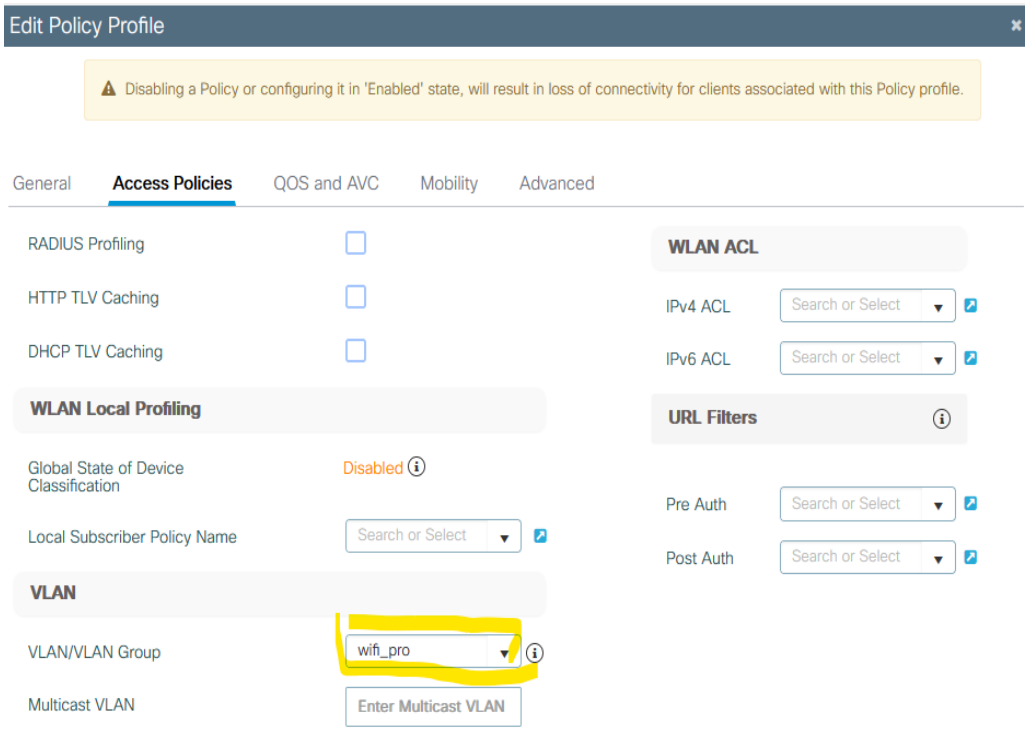
Indiquer l'adresse MAC de la carte Wi-Fi des appareilles que l'on veut autoriser. Dans la liste déroulante de ***Attribute List Name***, choisie celle crée précédemment (ATTR_LIST_PHARMACIE) et indiquer le WLAN auquel on veut appliquer la méthode (PHARMACIE).



2. **Créer/modifier un profil de stratégie**

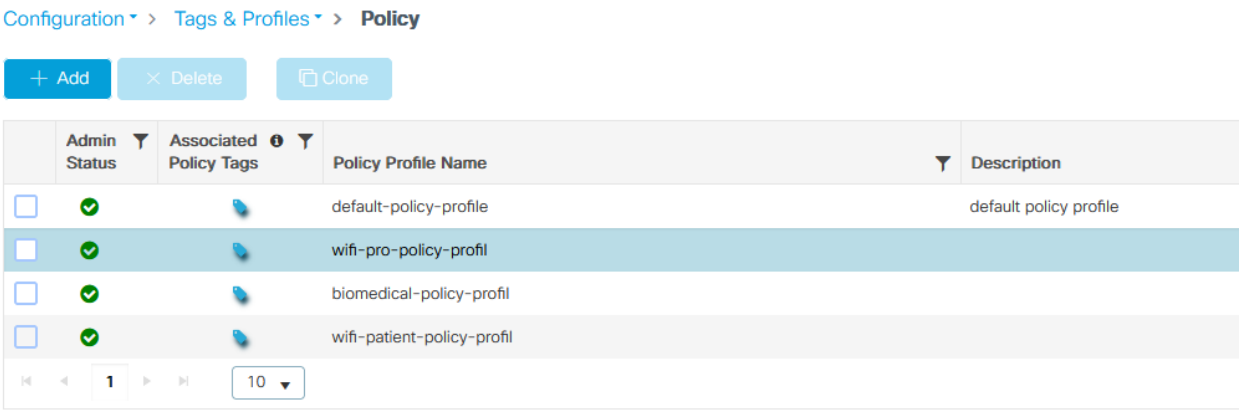
   Étape 1 : Accédez à **Configuration > Tags & Profiles > Policy** Cliquez sur **+ Ajouter** pour en ajouter un nouveau. Assurez-vous qu'il est activé, définissez le VLAN nécessaire et tout autre paramètre que vous souhaitez personnaliser.

28



Étape 2. Une fois terminé, cliquez sur **Enregistrer et appliquer au périphérique**.

Créer en un pour chaque vlan

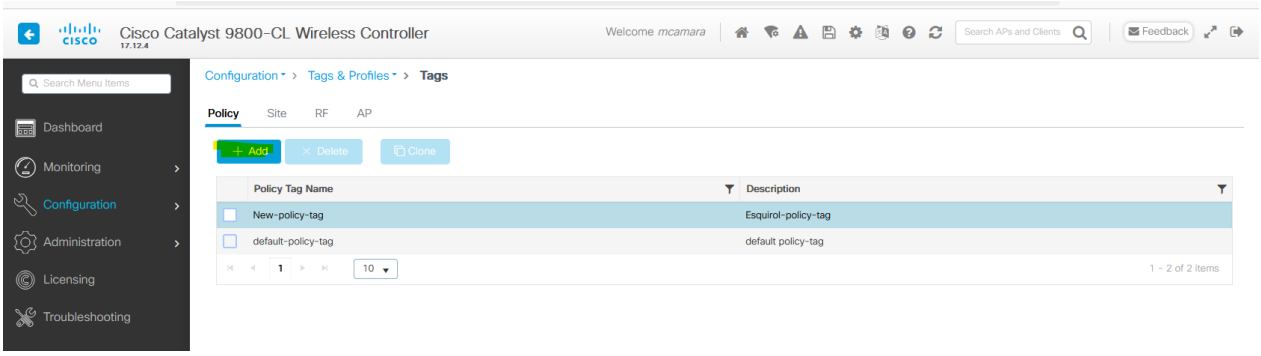


3. Créer/Modifier une balise de stratégie (Lier le SSID au profil de stratégie souhaité)

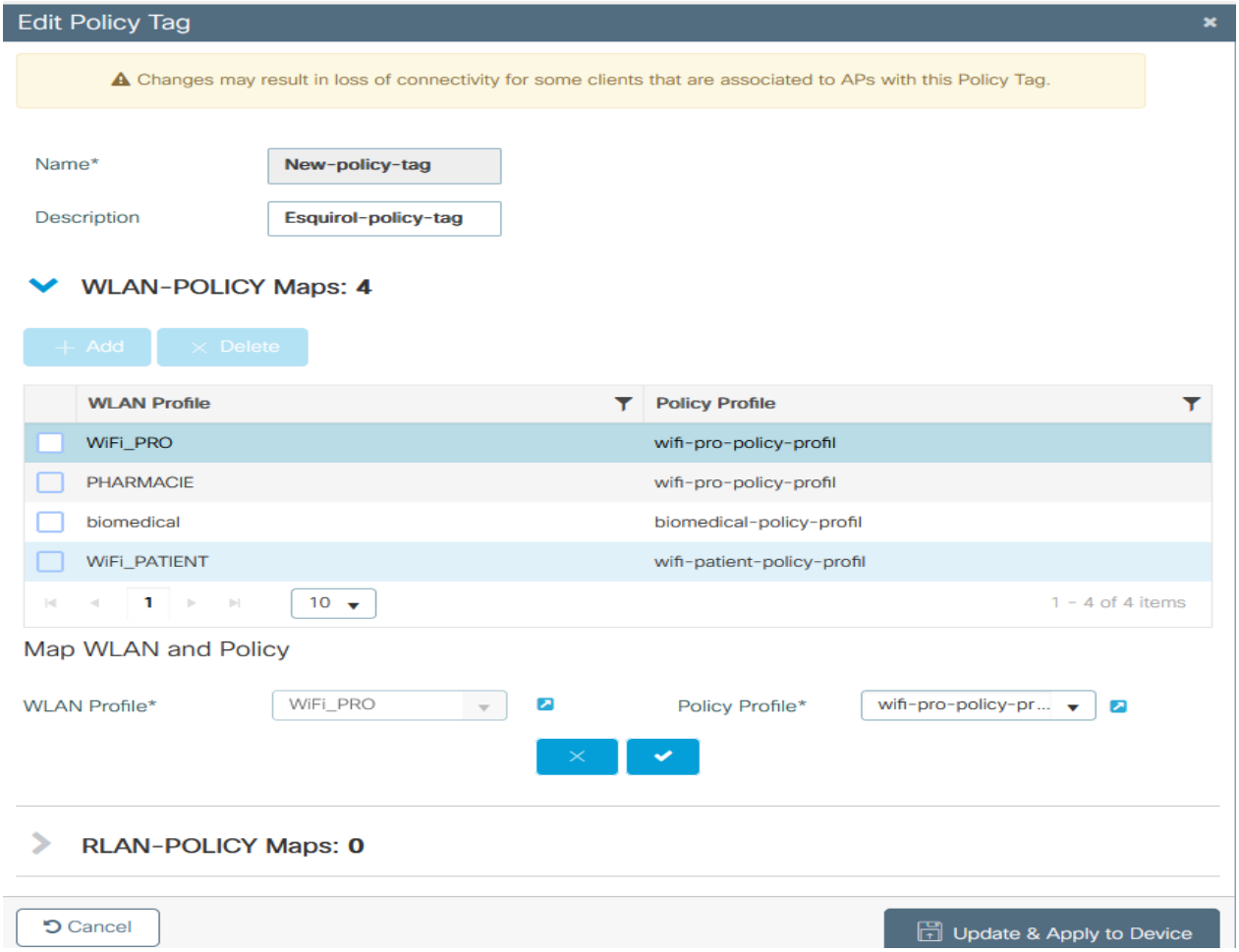
La balise Policy est le paramètre qui vous permet de spécifier quel SSID est lié à quel profil de stratégie.

Étape 1 : Accédez à **Configuration > Tags & Profiles > Tags > Policy**. Sélectionnez le nom d'une balise établie ou cliquez sur **+ Ajouter** pour en ajouter une nouvelle.

29



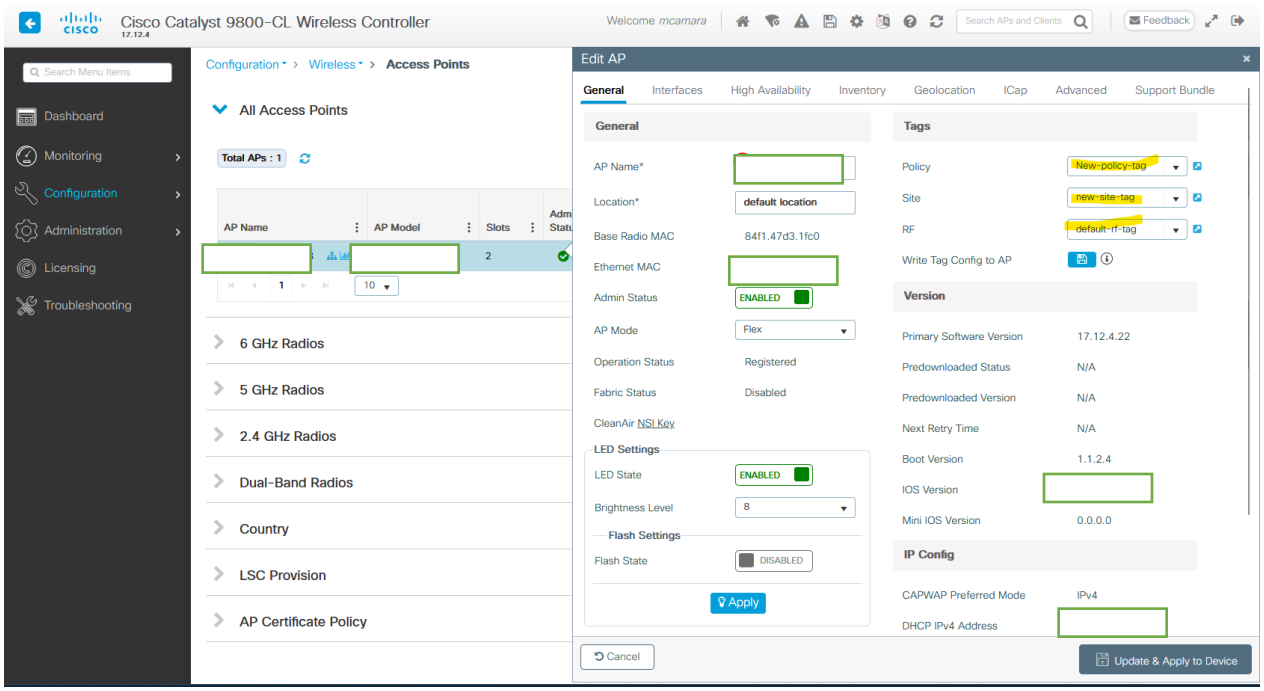
Étape 2 : Dans la **balise de stratégie (WLAN-POLICY Maps)**, cliquez sur **+Add**, dans la liste déroulante, sélectionnez le nom du profil WLAN que vous souhaitez ajouter à la balise de stratégie et au profil de stratégie auxquels vous souhaitez établir une liaison. Ensuite, cliquez sur la coche.



30

- Attribution de balise de stratégie

Vous pouvez attribuer une balise de stratégie directement à un point d'accès ou attribuer la même balise de stratégie à un groupe de points d'accès en même temps. Choisissez celui qui vous convient.



- Paramètres de jonction AP (AP Join Profile) sur les WLC 9800

Le **profil de jonction (AP Join Profile)** est un profil de configuration qui définit les paramètres qu'un point d'accès (AP) utilisera lorsqu'il rejoindra le réseau sans fil. Ce profil spécifie des paramètres comme le mode de fonctionnement de l'AP.

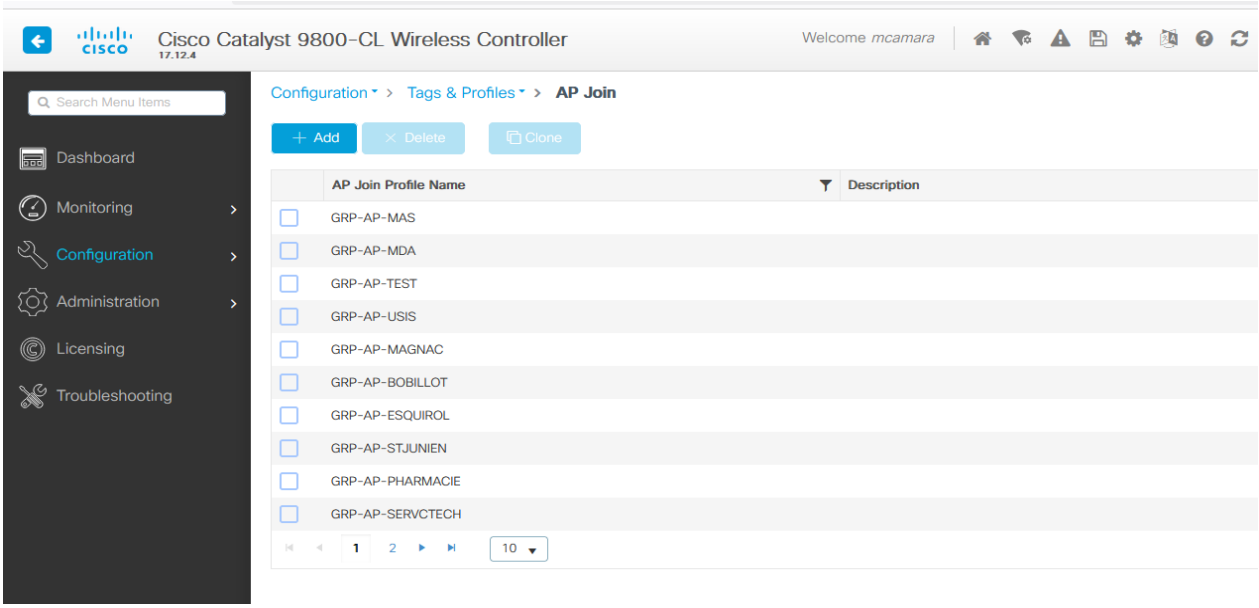
Flux de configuration :

1. **Créer/modifier un profil de jointure AP**

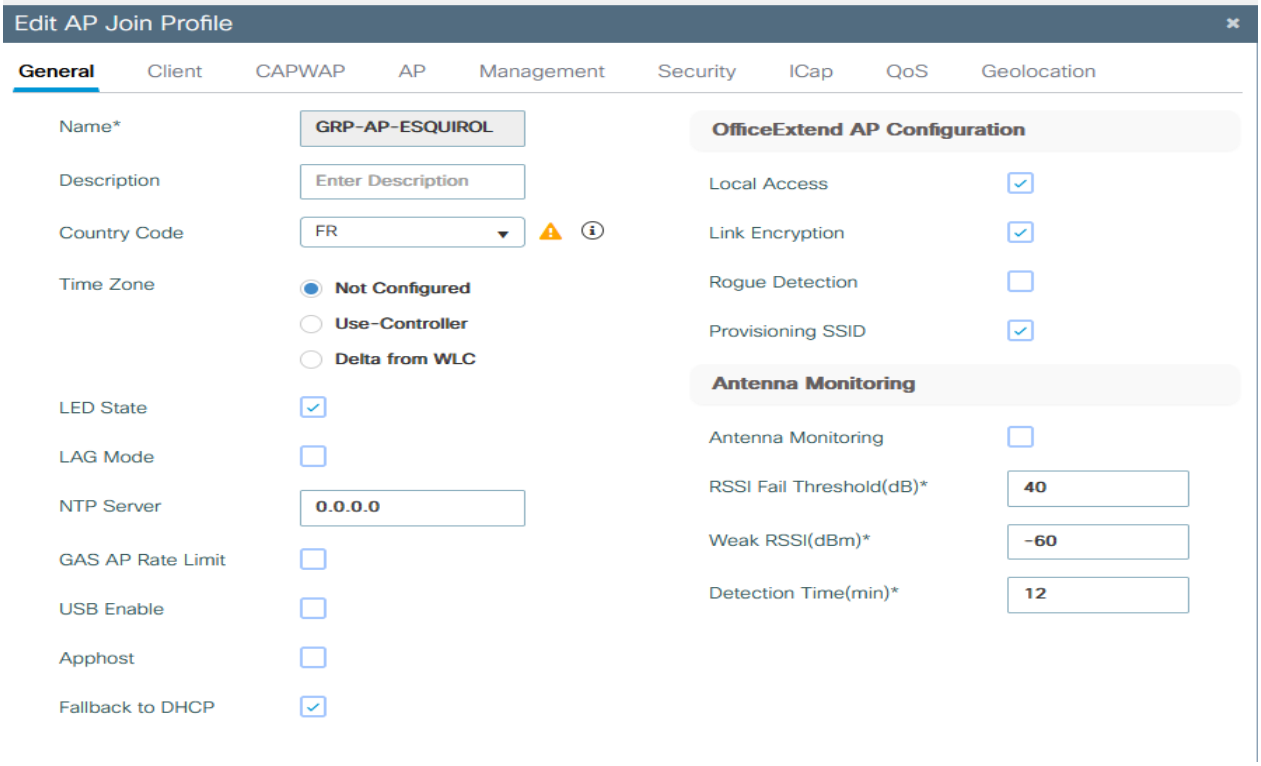
   Étape 1. Accédez à **Configuration > Tags & Profiles > AP Join**.

   Sélectionnez le nom d'un profil établi ou cliquez sur **+ Ajouter** pour en ajouter un nouveau.

31



Étape 2 : Modifiez le profil comme vous le souhaitez. Une fois terminé, cliquez sur **Enregistrer et appliquer au périphérique**.

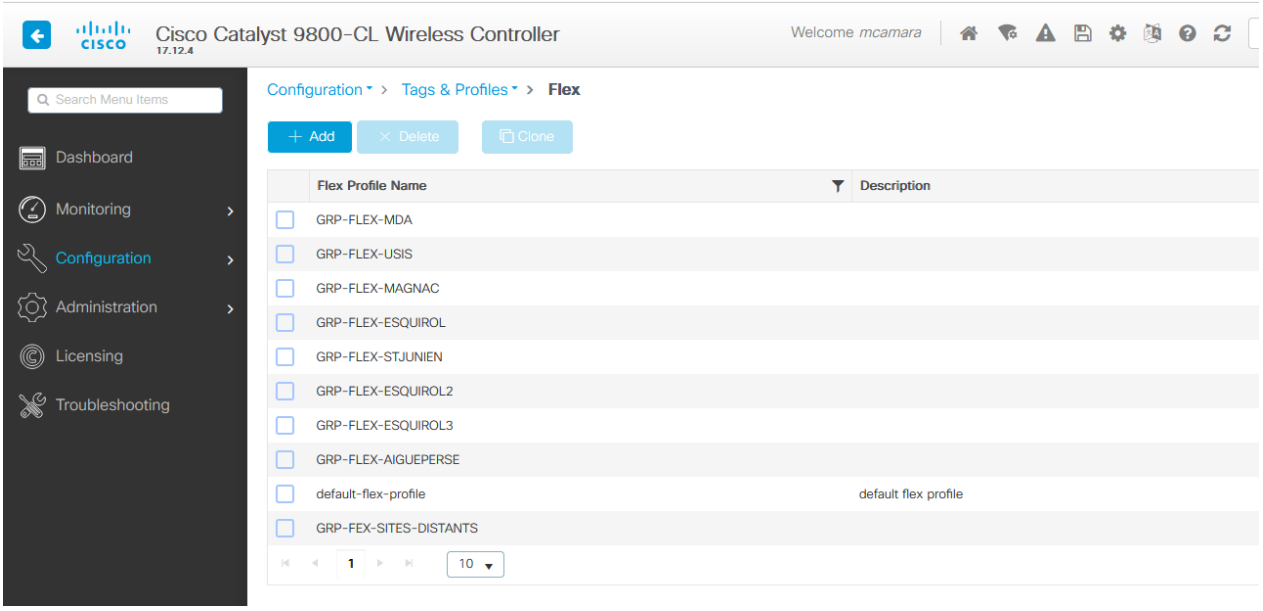


32

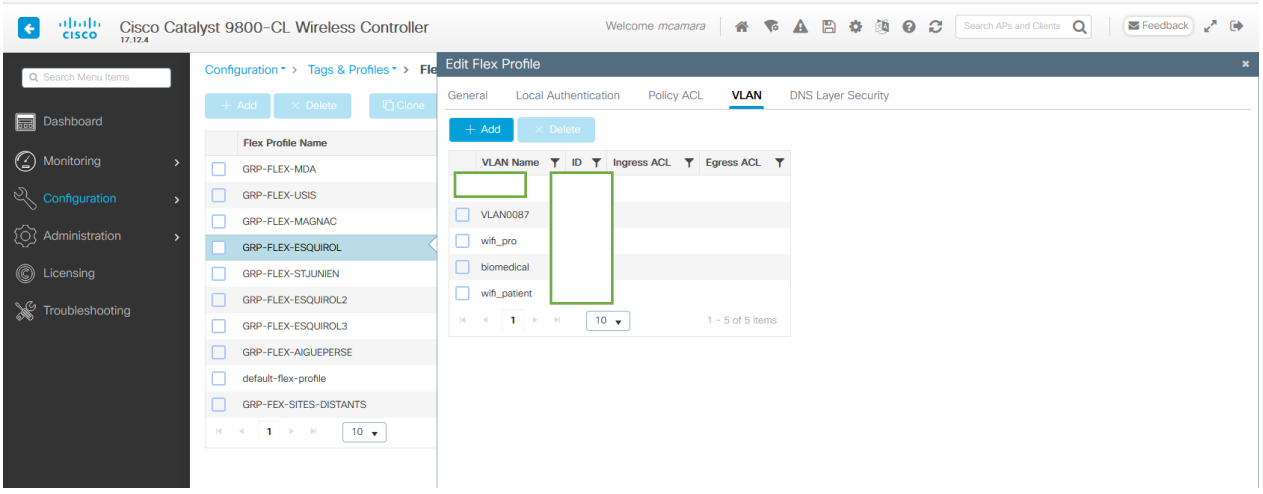
2. Créer/modifier un profil flexible (si AP en mode flexible)

Étape 1. Accédez à **Configuration > Tags & Profiles > Flex**.

Sélectionnez le nom d'un profil établi ou cliquez sur **+ Ajouter** pour en ajouter un nouveau.



Étape 2. Modifiez ou créer le profil comme vous le souhaitez en y ajouter les VLANs crées. Une fois terminé, cliquez sur **Enregistrer et appliquer au périphérique**.

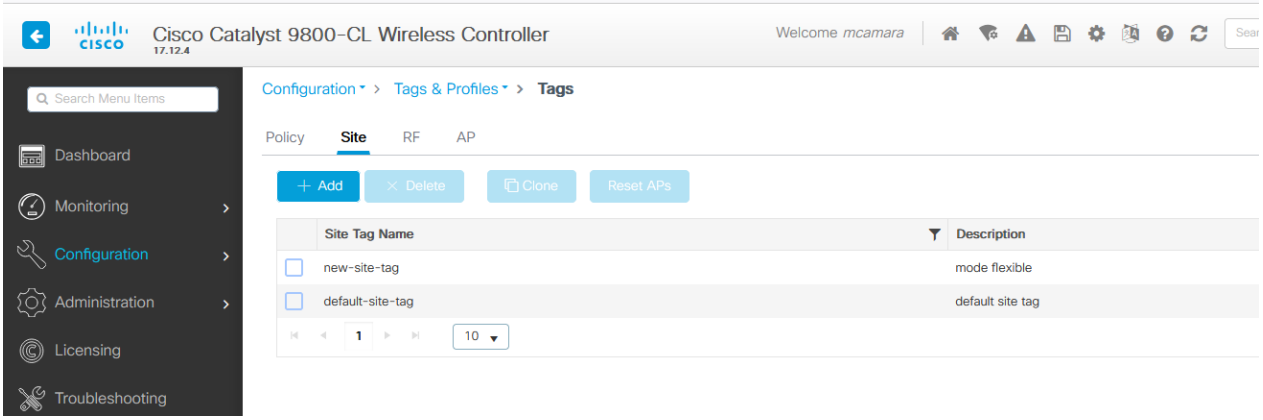


3. Créer/modifier une balise de site

La balise Site est le paramètre qui vous permet de spécifier quelle jointure AP et/ou quel profil Flex est attribué aux AP.

33

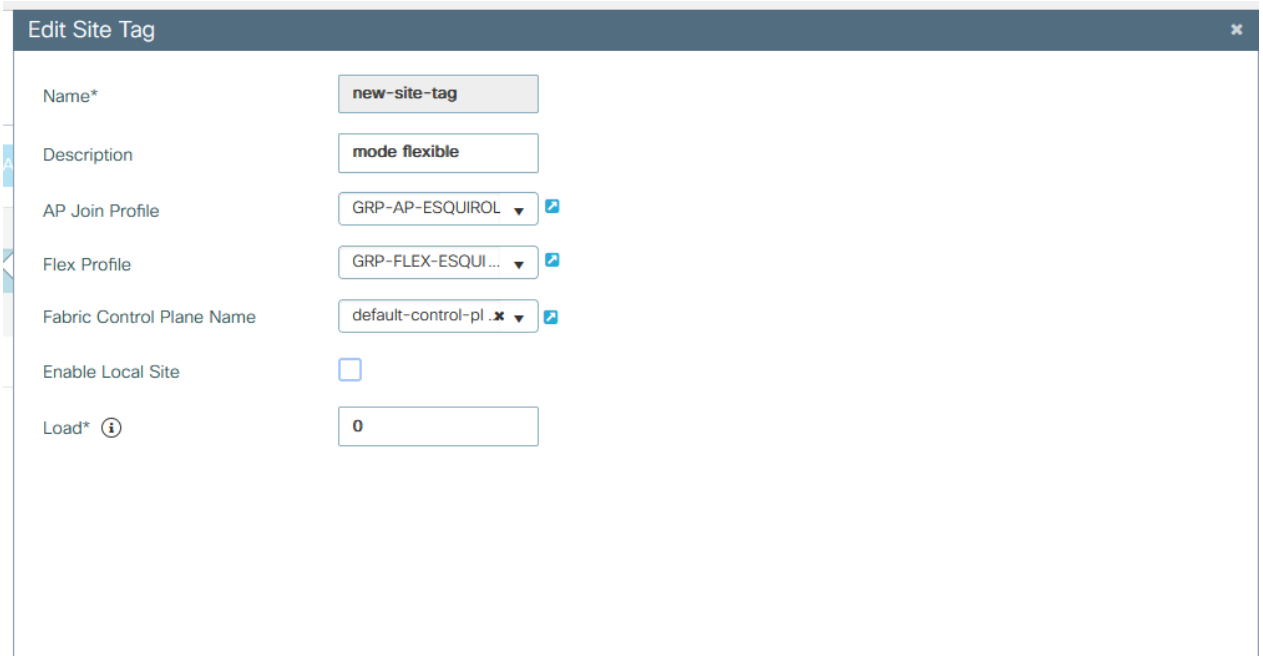
Étape 1 : Accédez à **Configuration > Tags & Profiles > Tags > Site**. Sélectionnez le nom d'un profil établi ou cliquez sur **+ Ajouter** pour en ajouter un nouveau.



Étape 2 : Dans la balise de site, sélectionnez le **profil de jonction AP** que vous voulez ajouter à la balise de site.

Si vous souhaitez convertir les AP (mode de fonctionnement en mode **flexconnect**), désactivez l'option **Enable Local Site (mode Local)**.

Une fois désactivé, vous pouvez également sélectionner un **profil flexible**. Après cela, cliquez sur **Enregistrer et appliquer au périphérique**.



34

N'oubliez pas de maintenir l'option Activer le site local activée si les points d'accès sont prévus pour être utilisés en mode local.

b. Migration des APs (AIR-AP1832I-E-K9) vers Cisco Catalyst 9800 CL

DHCP Option 43 :

Une plage d'adresse IP est activé sur le cœur de réseau pour le vlan 87, afin que les nouveaux points d'accès récupèrent une adresse IP de façon à ce qu'il remonte sur le contrôleur. Une fois le point d'accès récupéré, son IP est figée.

b.1 Problème rencontré : Impossible de déplacer les APs du contrôleur AireOS vers le nouveau contrôleur Catalyst 9800-CL

Le nouveau contrôleur n'accepte pas les AP initialement connectés à l'ancien contrôleur WLC AirOS.

- Échec de la vérification du certificat

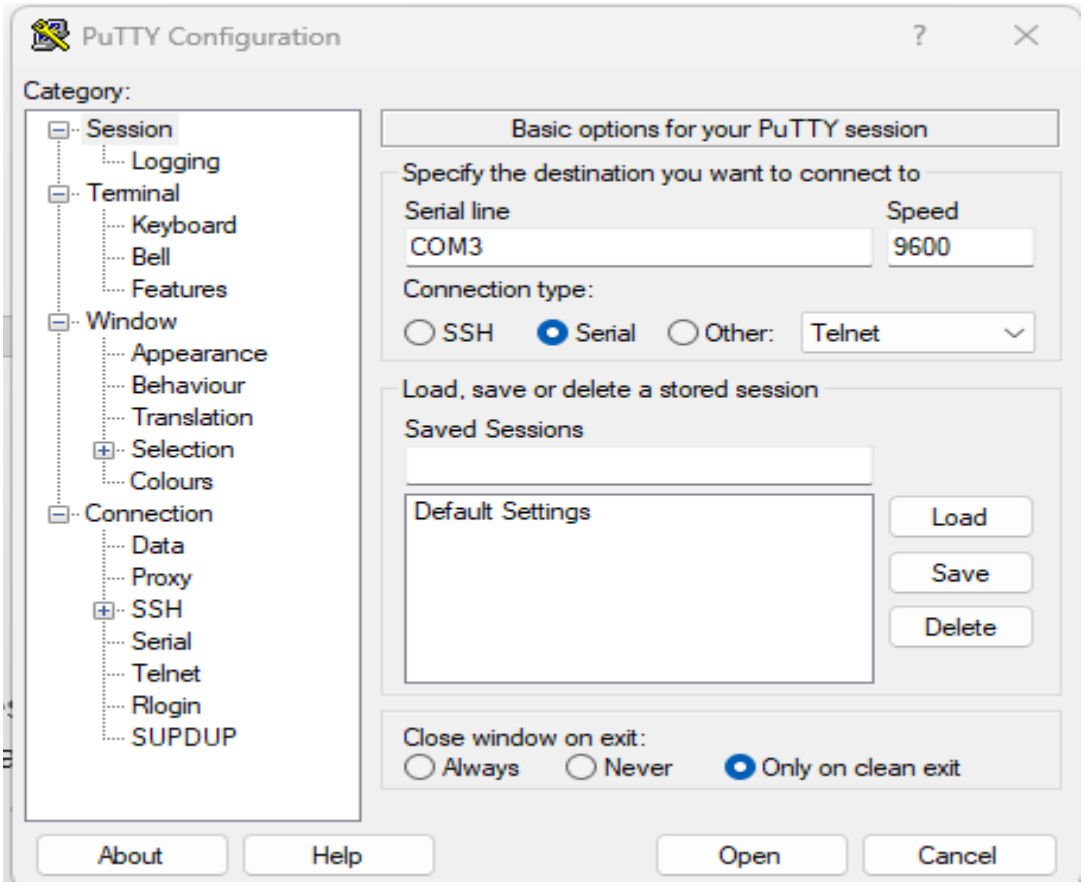
```
] display_verify_cert_status: Verify Cert: FAILED at 1 depth: self signed certificate in certificate chain
[*02/10/2025 12:48:06.1299] X509 OpenSSL Errors...
[*02/10/2025 12:48:06.1299]
[*02/10/2025 12:48:06.1299] NONE
[*02/10/2025 12:48:06.1299]
[*02/10/2025 12:48:06.1299]
[*02/10/2025 12:48:06.1299] dtls_verify_con_cert: Controller certificate verification error
[*02/10/2025 12:48:06.1299] dtls_process_packet: Controller certificate verification failed
[*02/10/2025 12:48:06.1399] sendPacketToDtls: DTLS: Closing connection 0x2b1cca00.
[*02/10/2025 12:48:06.1399]
[*02/10/2025 12:48:06.1399] Going to restart CAPWAP (reason : dtls_rc_connection_closed)...
[*02/10/2025 12:48:06.1399]
[*02/10/2025 12:48:06.1399] DTLS: Error while processing DTLS packet 0x2b23f000.
[*02/10/2025 12:48:06.1399] Restarting CAPWAP State Machine.
```

b.2 Solutions :

1ère Option : Réinitialiser les APs

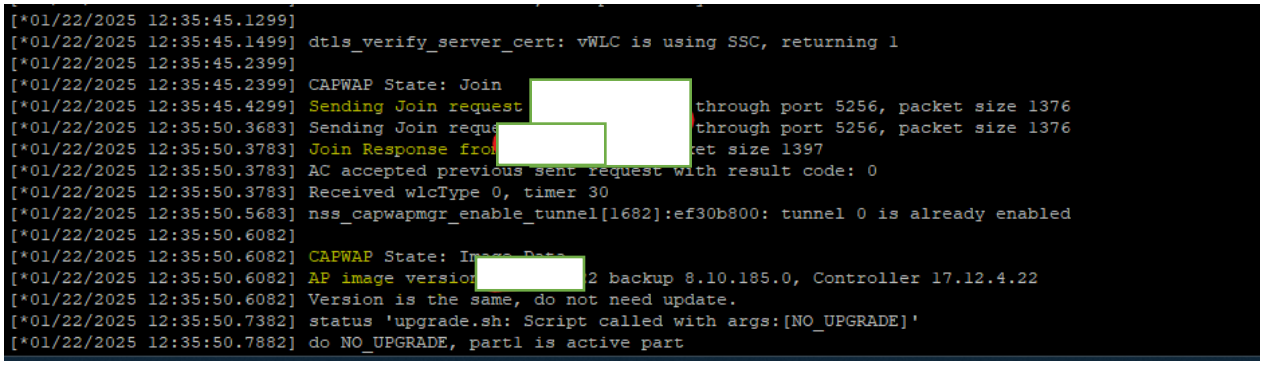
Etape 1 :

- Alimenter le point d'accès via un câble Rj45 (POE)
- Connexion au point d'accès via un câble console
- Connexion au point d'accès via le logiciel PuTTY

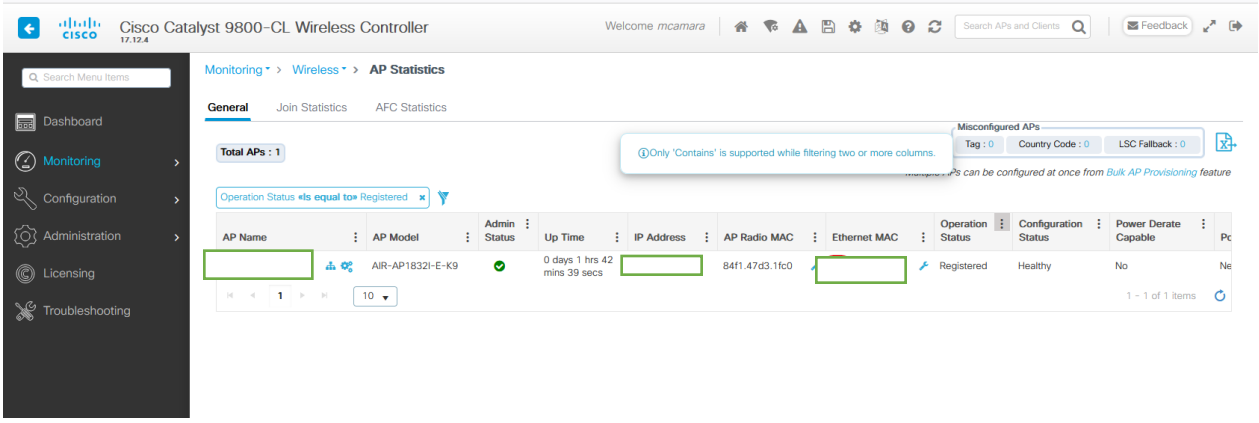


Etape 2 :

- Une fois connecté à l'AP, réinitialiser le avec la commande capwap ap erase all



36



2ème Option : pour une migration massive

Pour résoudre le problème lié aux certificats entre les deux contrôleurs :

Configurez le même token d'authentification sur AireOS et 9800 WLC.

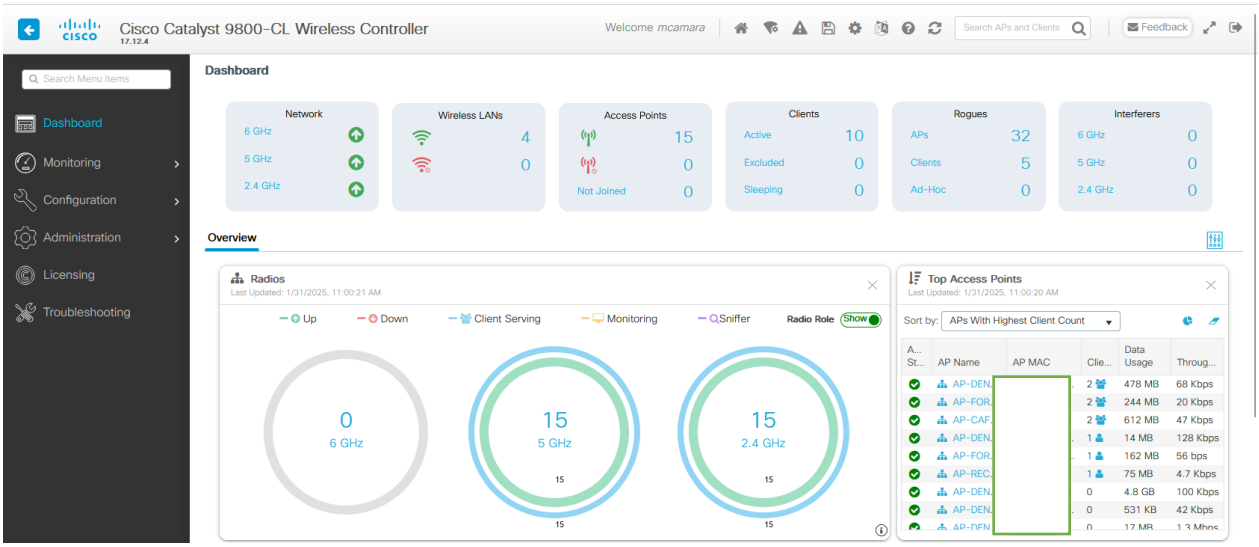
- Assurez-vous que tous les bornes sont associées au WLC AireOS.

- Entrez la commande suivante sur le 9800 **CL** certificate ssc hash validation disable

- Entrez la commande suivante sur **le AireOS** config certificate ssc auth-token « mot-de-passe »

- Entrez la commande suivante sur le **9800** CL wireless management certificate ssc auth-token 0 « mot-de-passe »

- Commencez ensuite à migrer les points d'accès.



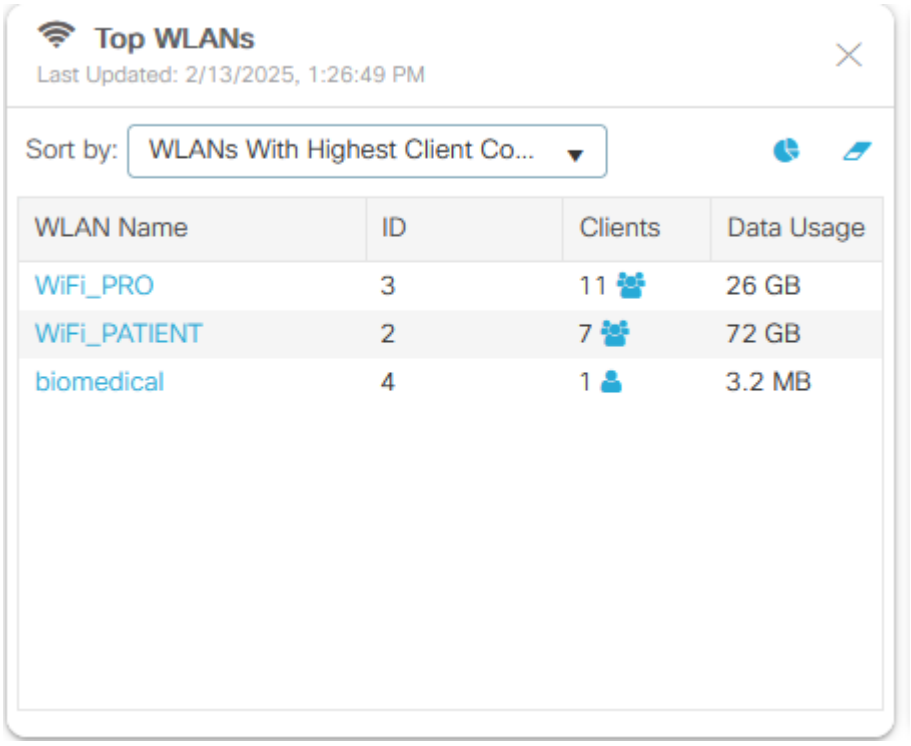
37

7. Test

- Vérification des SSID

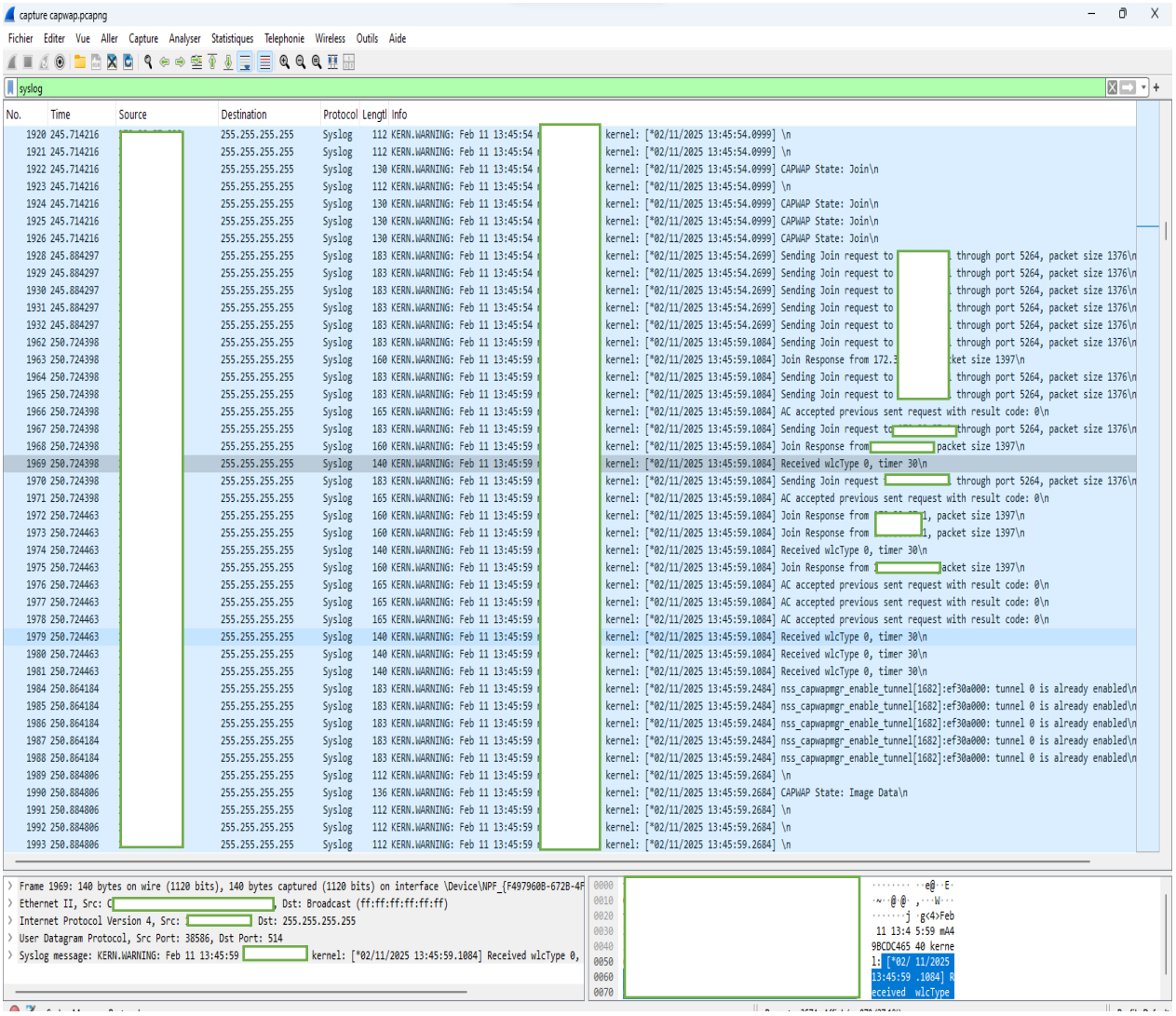
- Pour le WiFi_PATIENT et WiFi_PRO

```
CTRLWIFI#sh wireless client vlan ?
  summary  Show active vlan summary

CTRLWIFI#sh wireless client vlan s
CTRLWIFI#sh wireless client vlan summary
Number of Clients: 11

MAC Address    AP Name                                  Type ID   State            Method     Role       VLAN VLAN name
-------------------------------------------------------------------------------------------------------------------------
               AP                                       WLAN 2    Run              None       Local      3    wifi_patient
               AP                                       WLAN 3    Run              Dot1x      Local      24   wifi_pro
               AP                                       WLAN 2    Run              None       Local      3    wifi_patient
               AP                                       WLAN 3    Run              Dot1x      Local      24   wifi_pro
               AP                                       WLAN 3    Run              Dot1x      Local      24   wifi_pro
               AP                                       WLAN 2    Run              None       Local      3    wifi_patient
               AP                                       WLAN 2    Run              None       Local      3    wifi_patient
               AP                                       WLAN 2    Run              None       Local      3    wifi_patient
               AP                                       WLAN 3    Run              Dot1x      Local      24   wifi_pro
               AP                                       WLAN 3    Run              Dot1x      Local      24   wifi_pro
               AP                                       WLAN 3    Run              Dot1x      Local      24   wifi_pro

CTRLWIFI#
```



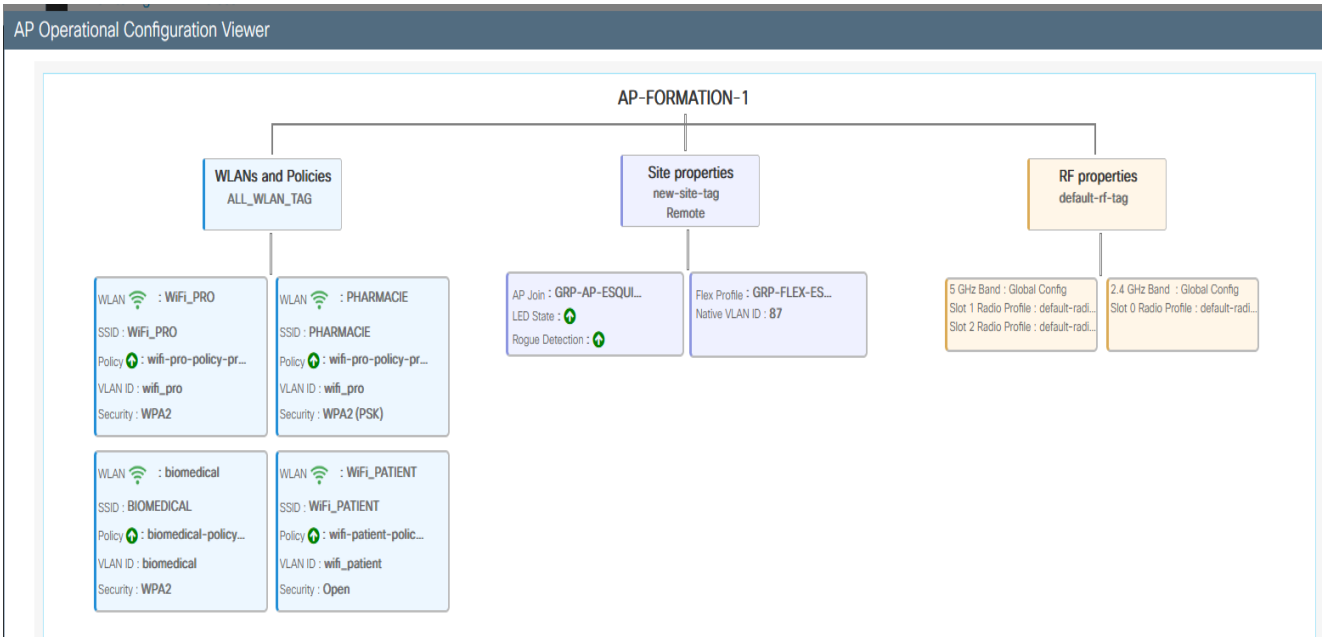
- Wireshark : Capture des trames CAPWAP (entre les APs et le contrôleur 9800 CL)

38


capture capwap.pcapng
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide
syslog
No. Time Source Destination Protocol Lengt Info
1920 245.714216 255.255.255.255 Syslog 112 KERN.WARNING: Feb 11 13:45:54 kernel: [*02/11/2025 13:45:54.0999] \n
1921 245.714216 255.255.255.255 Syslog 112 KERN.WARNING: Feb 11 13:45:54 kernel: [*02/11/2025 13:45:54.0999] \n
1922 245.714216 255.255.255.255 Syslog 130 KERN.WARNING: Feb 11 13:45:54 kernel: [*02/11/2025 13:45:54.0999] CAPWAP State: Join\n
1923 245.714216 255.255.255.255 Syslog 112 KERN.WARNING: Feb 11 13:45:54 kernel: [*02/11/2025 13:45:54.0999] \n
1924 245.714216 255.255.255.255 Syslog 130 KERN.WARNING: Feb 11 13:45:54 kernel: [*02/11/2025 13:45:54.0999] CAPWAP State: Join\n
1925 245.714216 255.255.255.255 Syslog 130 KERN.WARNING: Feb 11 13:45:54 kernel: [*02/11/2025 13:45:54.0999] CAPWAP State: Join\n
1926 245.714216 255.255.255.255 Syslog 130 KERN.WARNING: Feb 11 13:45:54 kernel: [*02/11/2025 13:45:54.0999] CAPWAP State: Join\n
1928 245.884297 255.255.255.255 Syslog 183 KERN.WARNING: Feb 11 13:45:54 kernel: [*02/11/2025 13:45:54.2699] Sending Join request to through port 5264, packet size 1376\n
1929 245.884297 255.255.255.255 Syslog 183 KERN.WARNING: Feb 11 13:45:54 kernel: [*02/11/2025 13:45:54.2699] Sending Join request to through port 5264, packet size 1376\n
1930 245.884297 255.255.255.255 Syslog 183 KERN.WARNING: Feb 11 13:45:54 kernel: [*02/11/2025 13:45:54.2699] Sending Join request to through port 5264, packet size 1376\n
1931 245.884297 255.255.255.255 Syslog 183 KERN.WARNING: Feb 11 13:45:54 kernel: [*02/11/2025 13:45:54.2699] Sending Join request to through port 5264, packet size 1376\n
1932 245.884297 255.255.255.255 Syslog 183 KERN.WARNING: Feb 11 13:45:54 kernel: [*02/11/2025 13:45:54.2699] Sending Join request to through port 5264, packet size 1376\n
1962 250.724398 255.255.255.255 Syslog 183 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.1084] Sending Join request to through port 5264, packet size 1376\n
1963 250.724398 255.255.255.255 Syslog 160 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.1084] Join Response from 172.3 ket size 1397\n
1964 250.724398 255.255.255.255 Syslog 183 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.1084] Sending Join request to through port 5264, packet size 1376\n
1965 250.724398 255.255.255.255 Syslog 183 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.1084] Sending Join request to through port 5264, packet size 1376\n
1966 250.724398 255.255.255.255 Syslog 165 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.1084] AC accepted previous sent request with result code: 0\n
1967 250.724398 255.255.255.255 Syslog 183 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.1084] Sending Join request to through port 5264, packet size 1376\n
1968 250.724398 255.255.255.255 Syslog 160 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.1084] Join Response from packet size 1397\n
1969 250.724398 255.255.255.255 Syslog 140 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.1084] Received wlcType 0, timer 30\n
1970 250.724398 255.255.255.255 Syslog 183 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.1084] Sending Join request through port 5264, packet size 1376\n
1971 250.724398 255.255.255.255 Syslog 165 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.1084] AC accepted previous sent request with result code: 0\n
1972 250.724463 255.255.255.255 Syslog 160 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.1084] Join Response from 1, packet size 1397\n
1973 250.724463 255.255.255.255 Syslog 160 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.1084] Join Response from 1, packet size 1397\n
1974 250.724463 255.255.255.255 Syslog 140 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.1084] Received wlcType 0, timer 30\n
1975 250.724463 255.255.255.255 Syslog 160 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.1084] Join Response from acket size 1397\n
1976 250.724463 255.255.255.255 Syslog 165 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.1084] AC accepted previous sent request with result code: 0\n
1977 250.724463 255.255.255.255 Syslog 165 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.1084] AC accepted previous sent request with result code: 0\n
1978 250.724463 255.255.255.255 Syslog 165 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.1084] AC accepted previous sent request with result code: 0\n
1979 250.724463 255.255.255.255 Syslog 140 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.1084] Received wlcType 0, timer 30\n
1980 250.724463 255.255.255.255 Syslog 140 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.1084] Received wlcType 0, timer 30\n
1981 250.724463 255.255.255.255 Syslog 140 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.1084] Received wlcType 0, timer 30\n
1984 250.864184 255.255.255.255 Syslog 183 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.2484] nss_capwapmgr_enable_tunnel[1682]:ef30a000: tunnel 0 is already enabled\n
1985 250.864184 255.255.255.255 Syslog 183 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.2484] nss_capwapmgr_enable_tunnel[1682]:ef30a000: tunnel 0 is already enabled\n
1986 250.864184 255.255.255.255 Syslog 183 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.2484] nss_capwapmgr_enable_tunnel[1682]:ef30a000: tunnel 0 is already enabled\n
1987 250.864184 255.255.255.255 Syslog 183 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.2484] nss_capwapmgr_enable_tunnel[1682]:ef30a000: tunnel 0 is already enabled\n
1988 250.864184 255.255.255.255 Syslog 183 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.2484] nss_capwapmgr_enable_tunnel[1682]:ef30a000: tunnel 0 is already enabled\n
1989 250.884806 255.255.255.255 Syslog 112 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.2684] \n
1990 250.884806 255.255.255.255 Syslog 136 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.2684] CAPWAP State: Image Data\n
1991 250.884806 255.255.255.255 Syslog 112 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.2684] \n
1992 250.884806 255.255.255.255 Syslog 112 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.2684] \n
1993 250.884806 255.255.255.255 Syslog 112 KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.2684] \n
Frame 1969: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface \Device\NPF_{F497960B-672B-4F
Ethernet II, Src: C , Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: Dst: 255.255.255.255
User Datagram Protocol, Src Port: 38586, Dst Port: 514
Syslog message: KERN.WARNING: Feb 11 13:45:59 kernel: [*02/11/2025 13:45:59.1084] Received wlcType 0,
0000
0010
0020
0030
0040
0050
0060
0070
11 13:4 5:59 mA4
9BCDC465 40 kerne
1: [*02/ 11/2025
13:45:59 .1084] R
eceived wlcType

39

8. Configuration finale :



9. Supervision (Zabbix & Nagios)

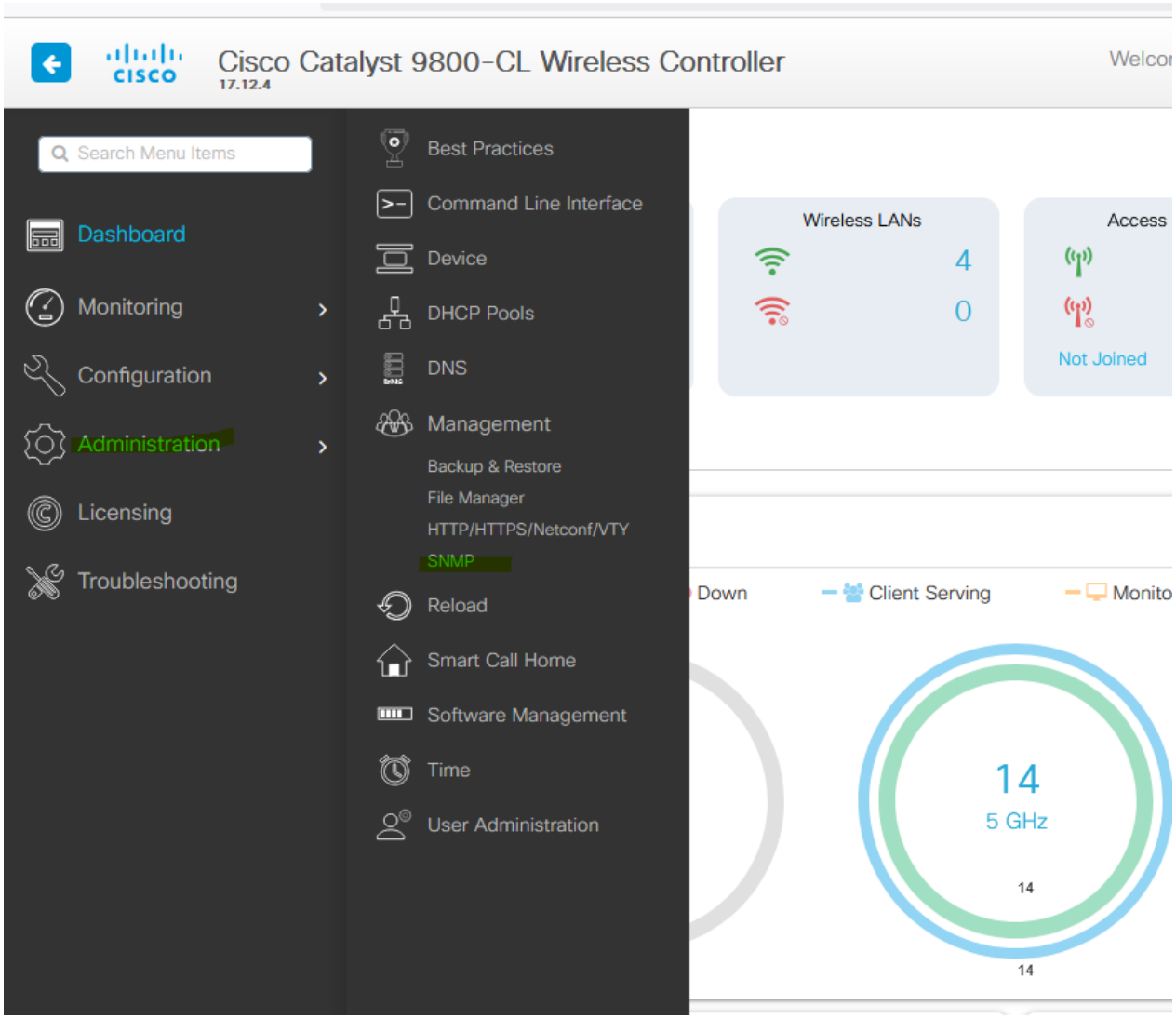
Objectif : Obtenir une vue d'ensemble instantanée sur la disponibilité et l'état de chaque point d'accès du réseau (Esquirol). Cela inclut la connectivité (en ligne/hors ligne) et l'état de chaque AP.

A. Agent SNMP (Contrôleur Catalyst 9800 CL)

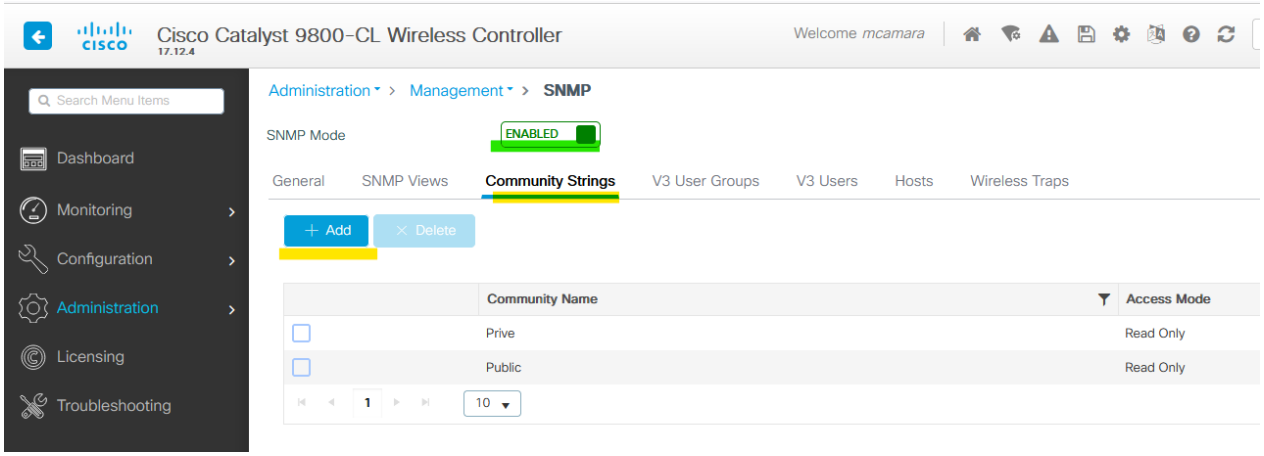
Configuration de l’agent SNMP sur le contrôleur Cisco Catalyst 9800 CL

Aller dans **Administration>SNMP**

40

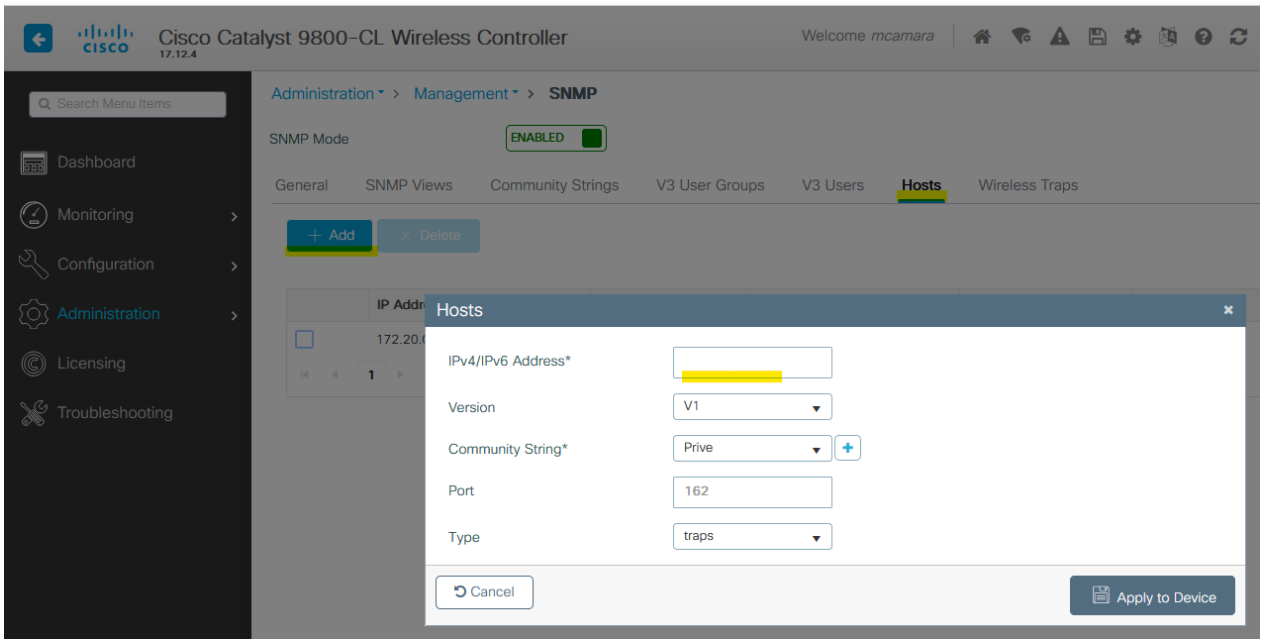


Ensuite dans la section **Community Strings**, on ajoute le deux communautés (Privée et Public)

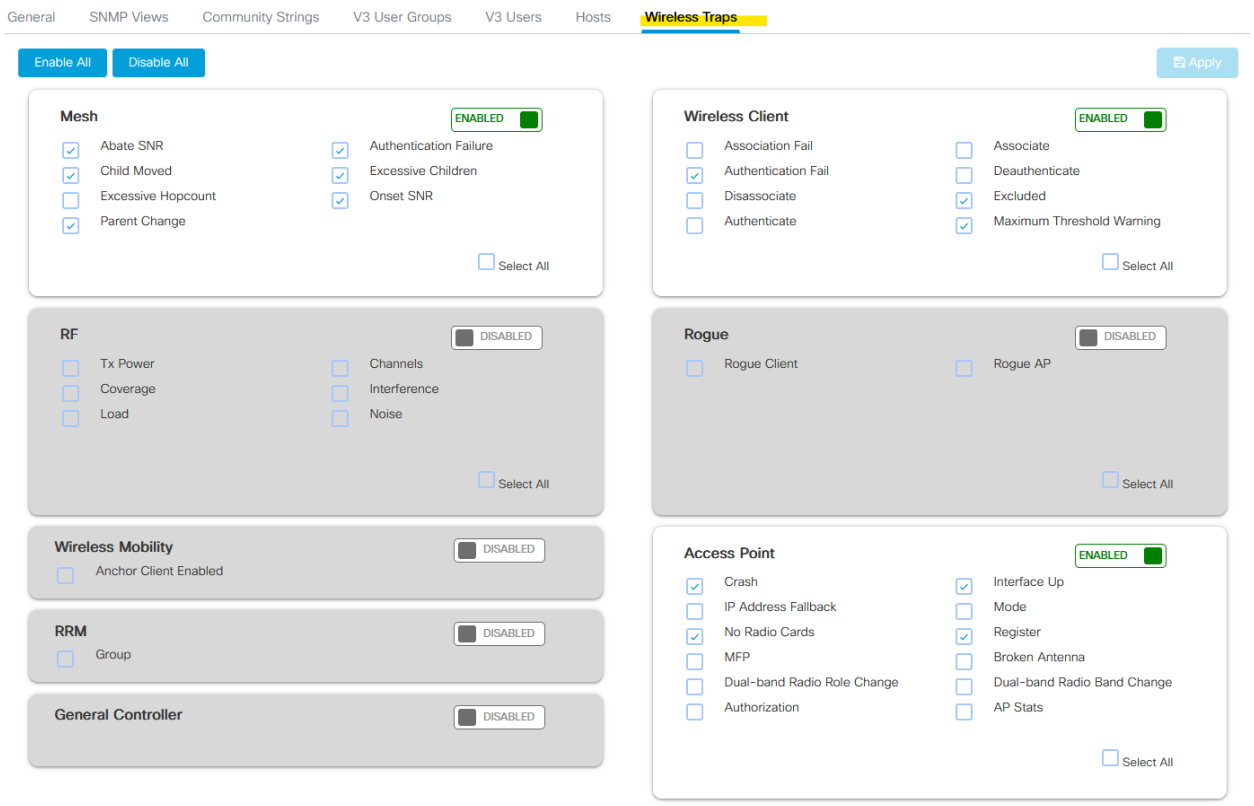


Dans la section **Hosts,** on indique l'adresse IP de **Zabbix** + le port 162

41



Enfin, dans la partie **Wireless Traps**, on active les informations que l'on veut collecter

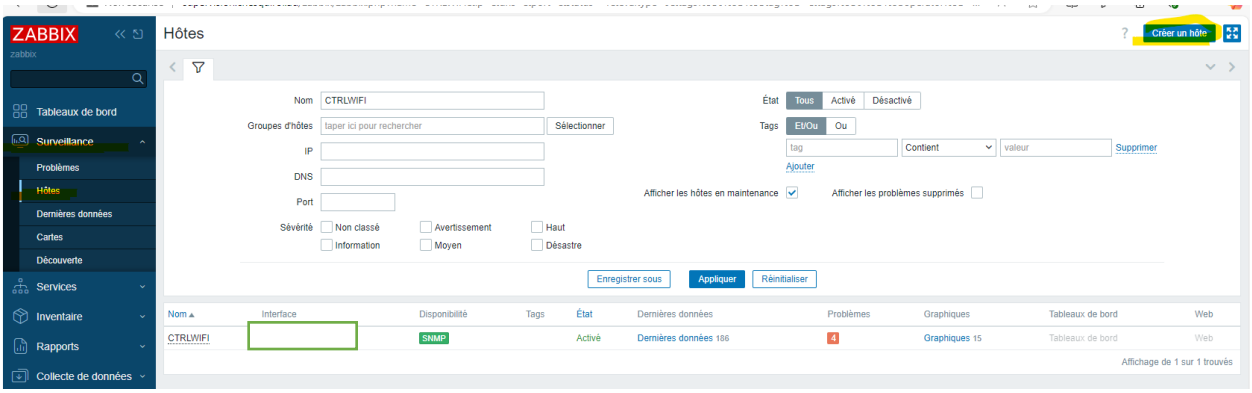


42

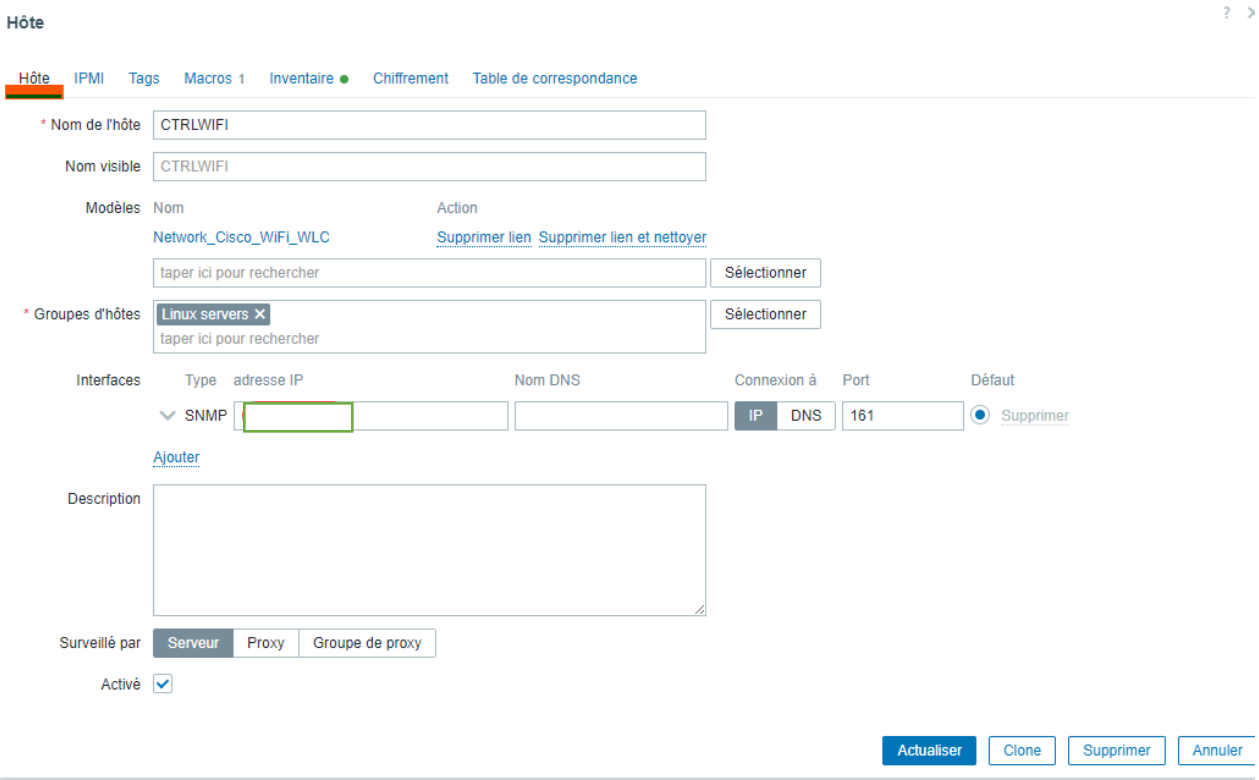
B. Zabbix

Etape 1 : Intégration du contrôleur Catalyst sur Zabbix

Aller dans **Surveillance>Hôtes** et clique sur **créer un hôte**

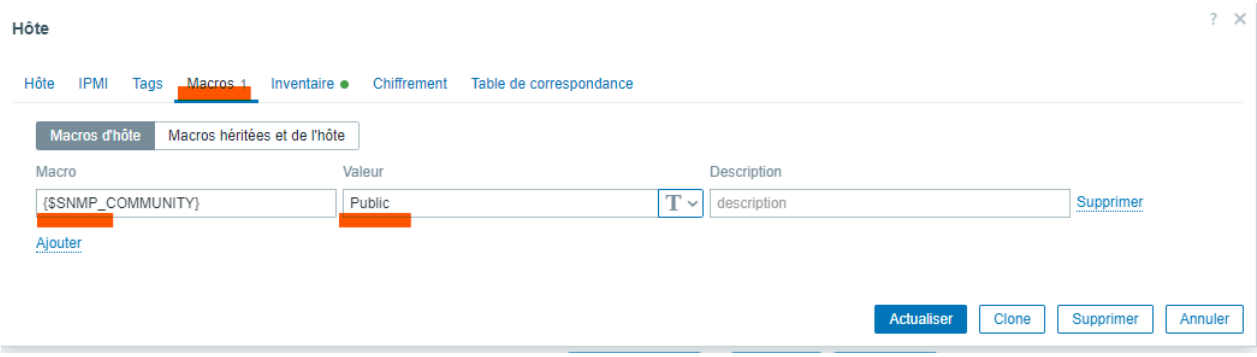


Ensuite, dans la section Hôte, indiquez l'adresse IP du **Contrôleur Wi-Fi Catalyst 9800 CL**



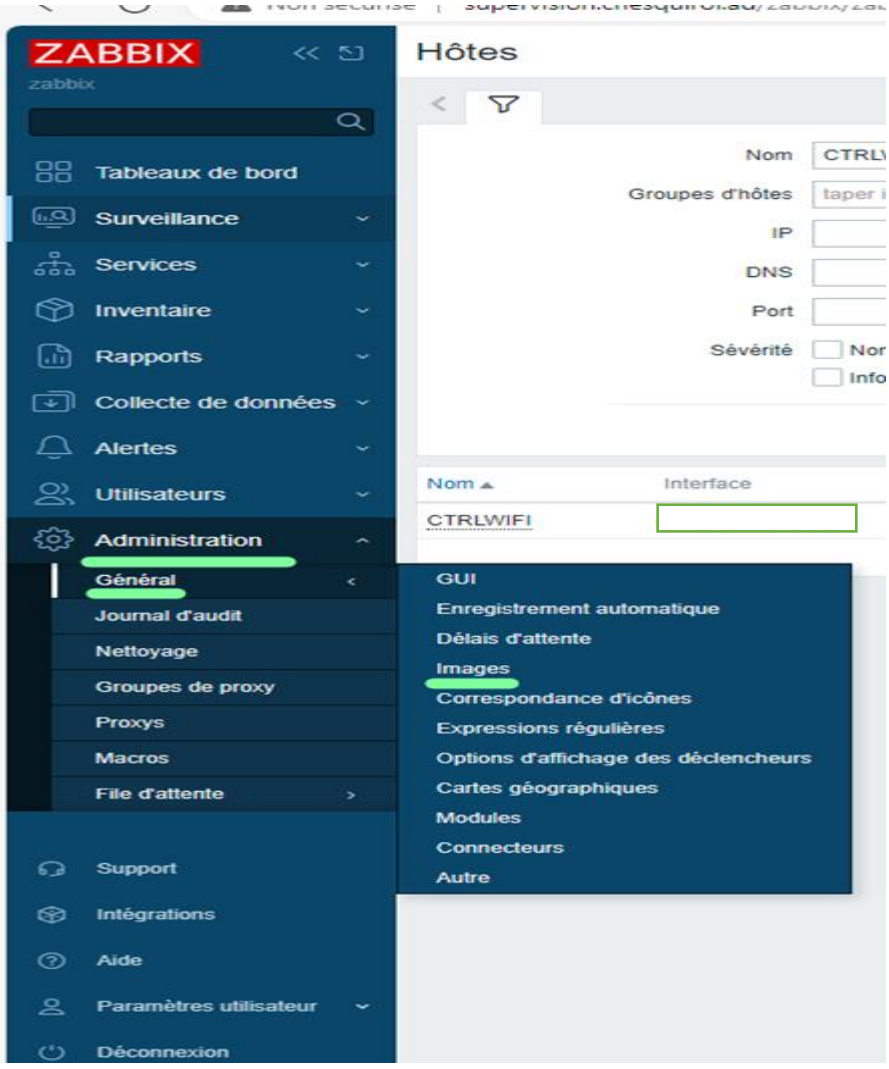
Dans la section **Macro**, on indique la communauté (Public)

43

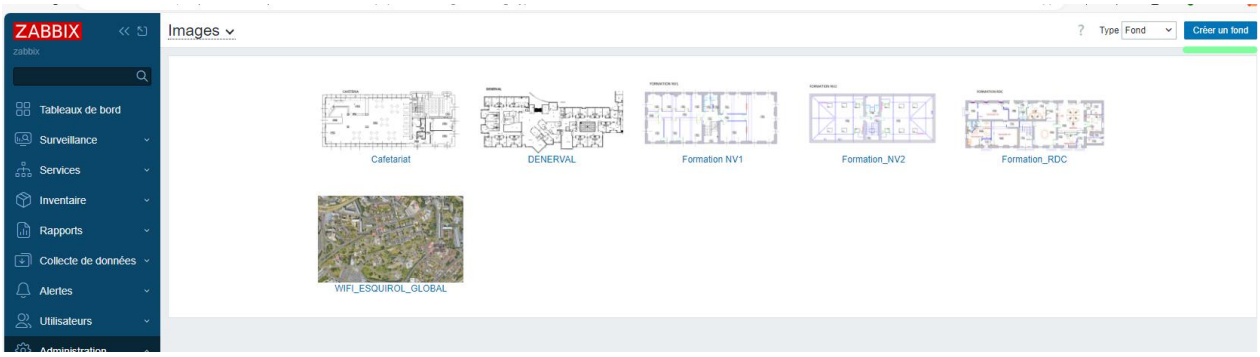


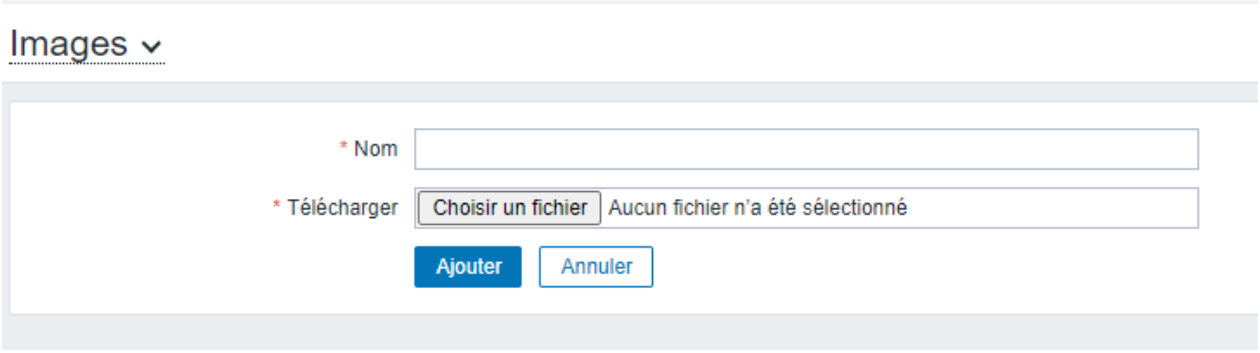
Etape 2 : créer une carte dans Zabbix afin de visualiser l'état des points d'accès (APs)

1. Aller dans l'onglet "**Administration>Général>Images**"
   On importe une image cartographique (plan du lieu où se trouve les APs) dans un premier temps.



44



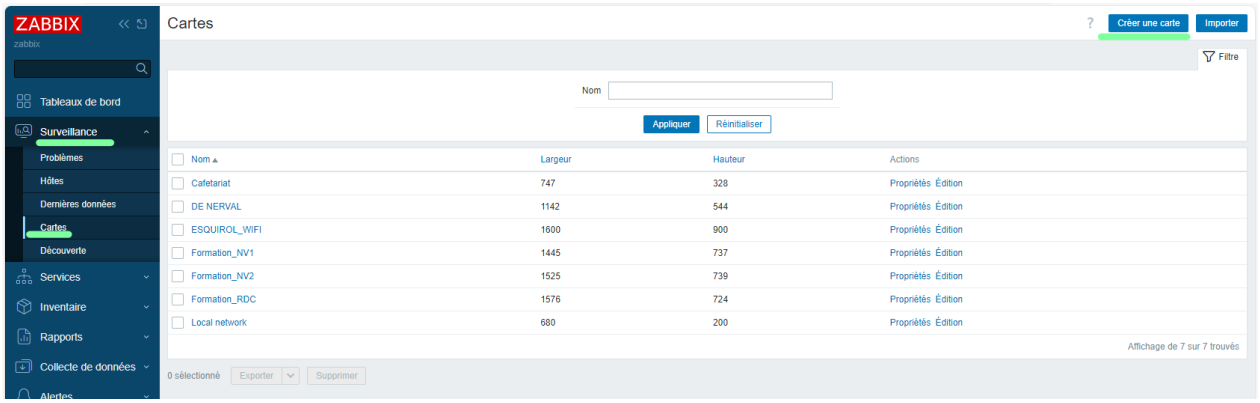


Etape 2 : configuration d'une carte pour les APs

Avant de commencer la configuration de vos cartes sur Zabbix montrant tous les points d'accès (AP), il vous faut d'abord vous assurer que tous les points d'accès y sont bien intégrés avec leurs données de surveillance collectées (comme la disponibilité, la performance, etc.).

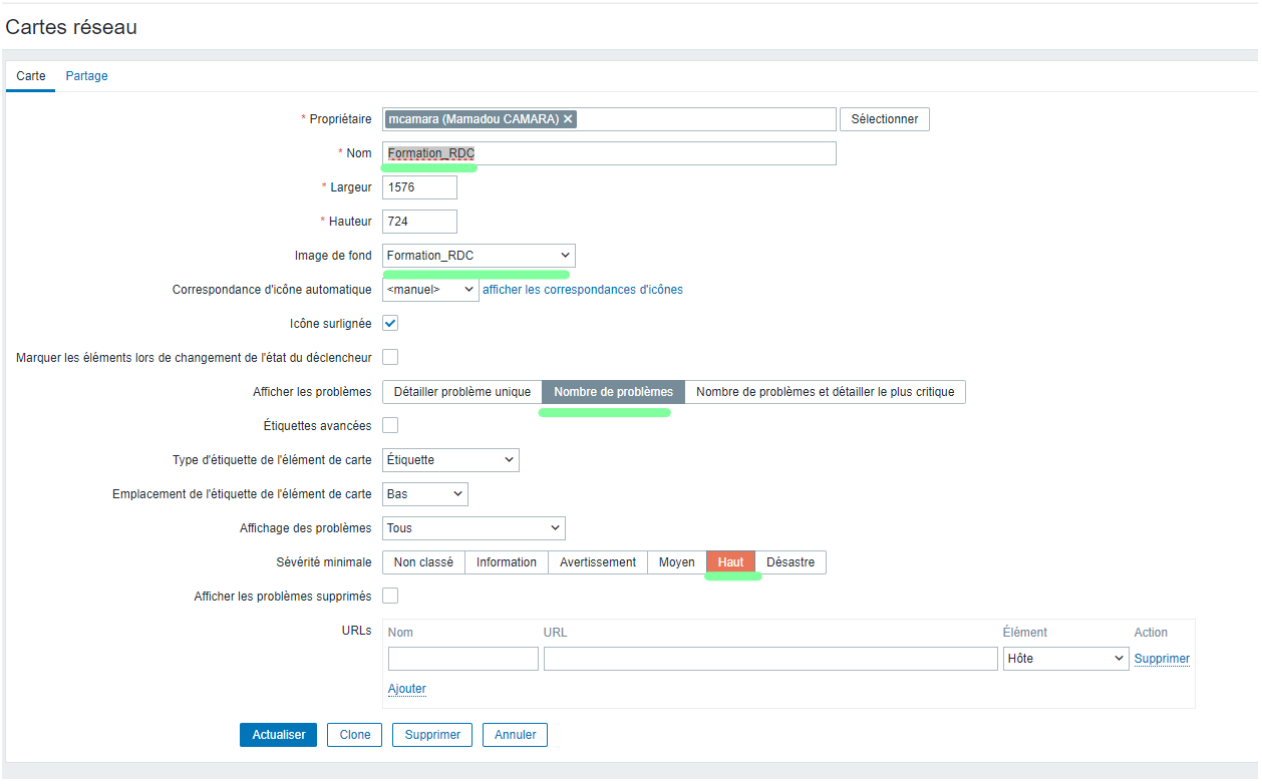
Une fois que les données sont collectées, vous pouvez créer une **carte** pour visualiser l'état de tous les APs. Voici les étapes générales pour réaliser cela :

1. Aller dans **Surveillance/Cartes + Créer une carte**

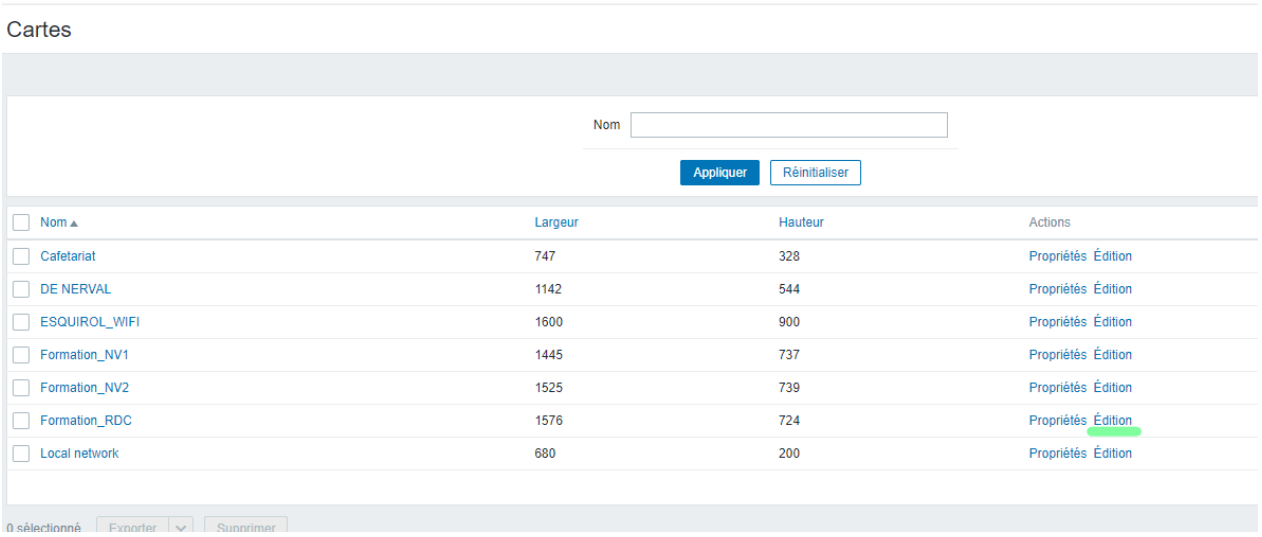


45

Ensuite indiquer le nom de la carte (Bâtiment où se trouve les APs), + l'image cartographique importée précédemment (Formation_RDC)

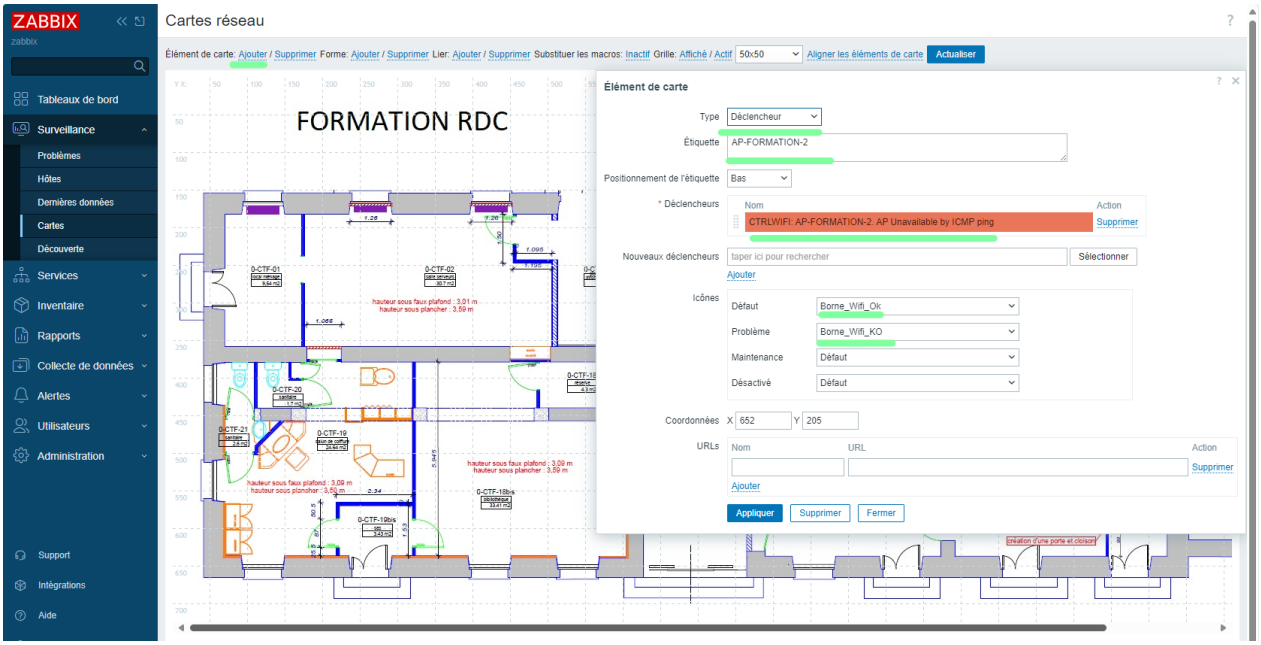


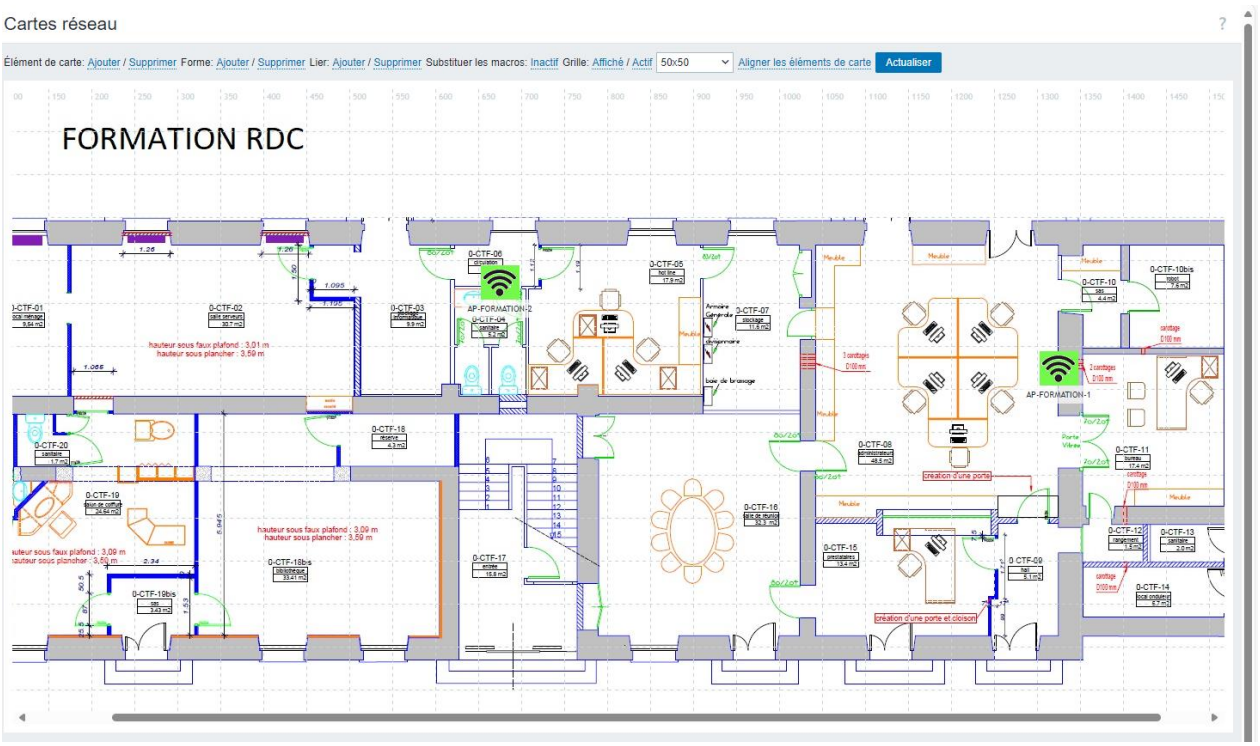
Une fois la carte créée, on clique sur **Editer**



46

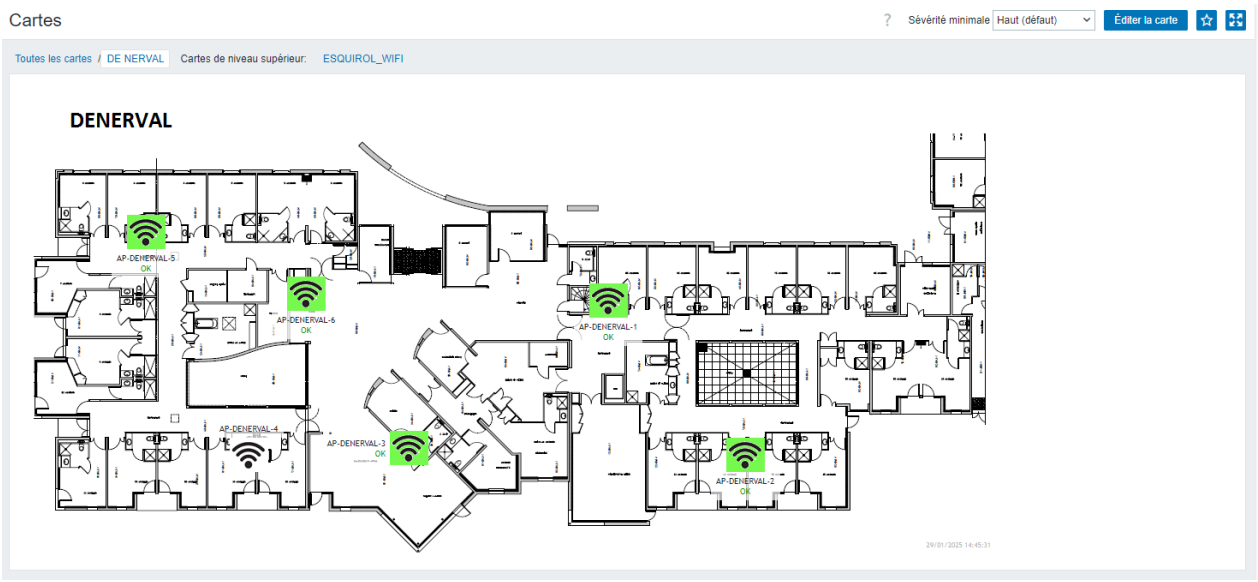
- Créez une carte avec des icônes représentant vos APs.
- Ajoutez un **déclencheur** qui suit l'état de la connectivité pour chaque AP (par exemple, si l'AP est en ligne ou hors ligne).
- Utiliser les icones représentant l'état **(**Disponibilité de l'AP (ping ou autre vérification)) pour refléter l'état actuel de chaque AP.





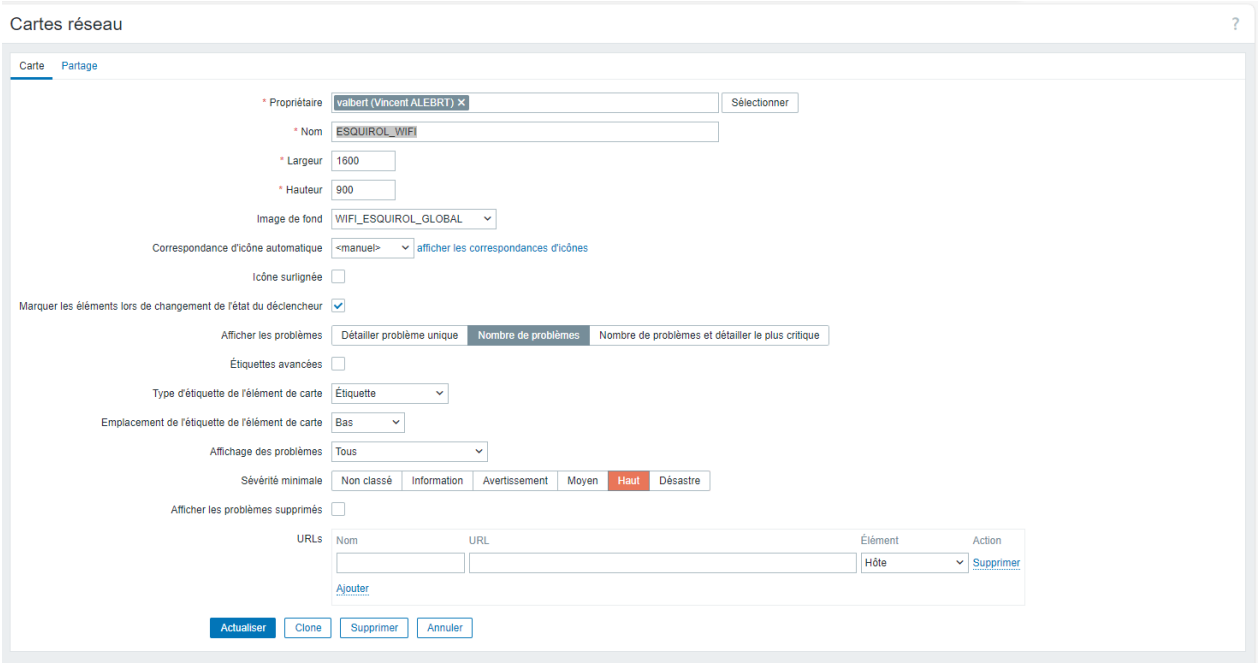
47

On fais pareil pour les autres lieux (Aps)



2. Carte pour tous les APs du CH Esquirol (Satellite)

Aller dans **Surveillance>Cartes + Créer une carte**

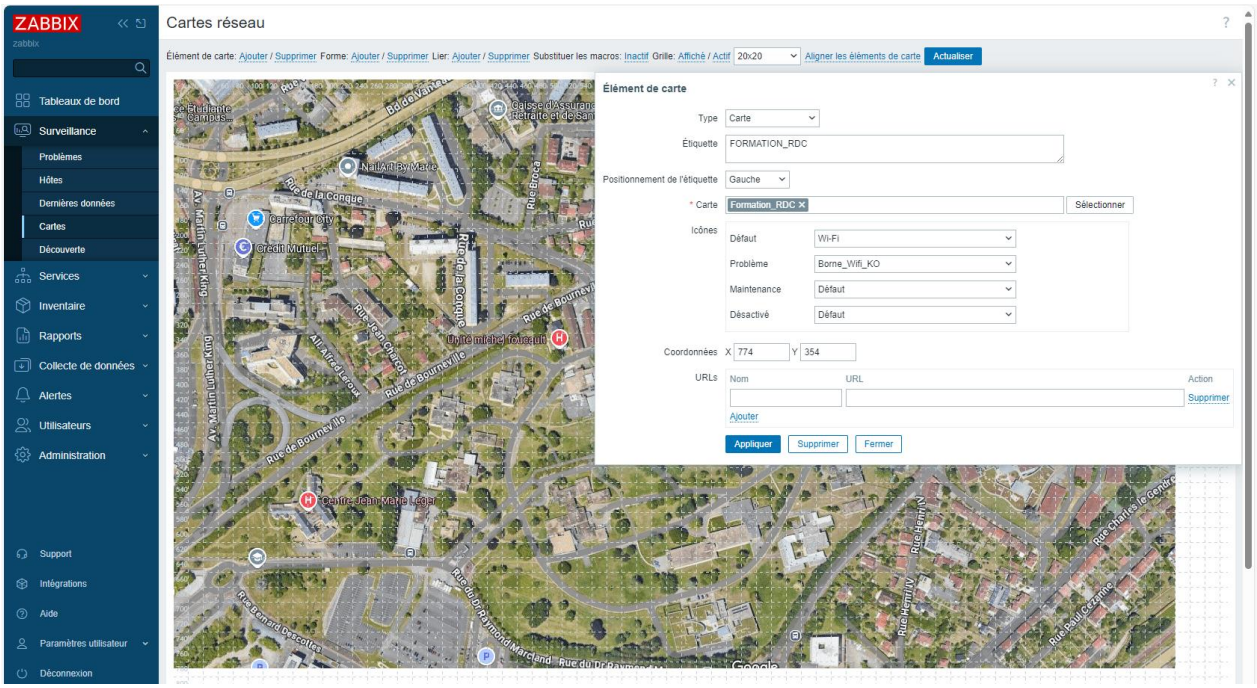


48

Ensuite indiquer le nom de la carte (Esquirol_WiFi), l'image cartographique du site de CH Esquirol (Satellite).

Une fois la carte créée, on clique sur **Editer, + Ajouter** (Elément de la carte).

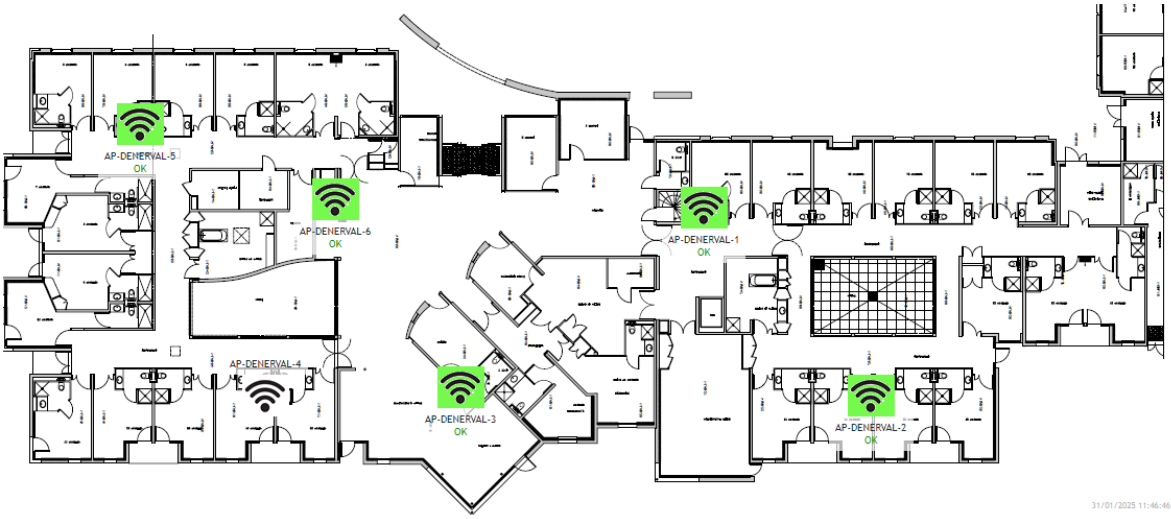
Ensuite on indique le type (Carte), l'étiquette (Le nom du bâtiment où se trouves les APs)



49

On peut vérifier l'état de tous les APs (Bâtiment par bâtiment) depuis la carte (**ESQUIROL_WIFI**)

DENERVAL



50