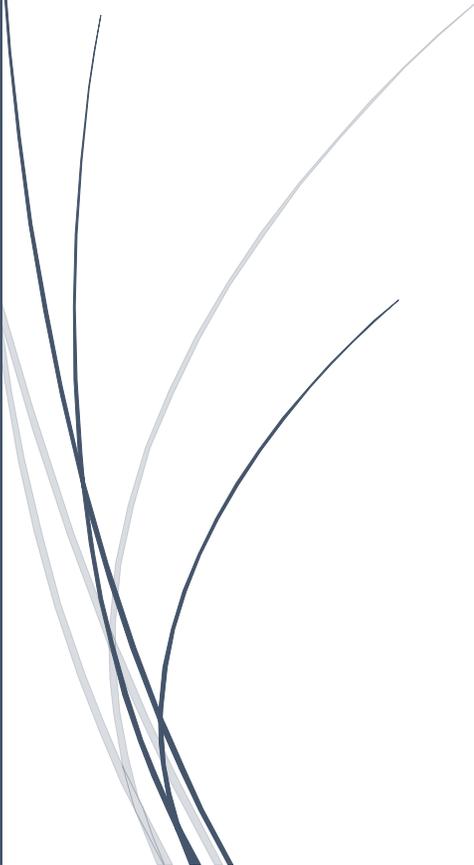




[Date]

Cisco Catalyst 9800-CL Wireless Controller for Cloud

Migration Contrôleur WiFi Cisco WLC
AirOS



Mamadou CAMARA
BTS SIO, SISR

SOMMAIRE :

1. CONTEXTE	3
2. OBJECTIF	3
3. FONCTIONNEMENT DU CISCO WLC (CAPWAP)	3
4. L'ARCHITECTURE	4
5. PRE-INSTALLATION	5
6. DEPLOIEMENT ET CONFIGURATION DU CONTROLEUR VIRTUEL SANS FIL CISCO CATALYST 9800 CL	7
A. À PARTIR DU CLIENT VSPHERE, DEPLOYEZ LE MODELE OVA 9800-CL.	7
ETAPE 1 : DEPLOIEMENT DU CONTROLEUR CISCO CATALYST 9800 SUR L'HYPERVEUR VMWARE	7
ETAPE 2 : CONFIGURATION DU CONTROLEUR CISCO CATALYST 9800 DEPUIS L'INTERFACE GRAPHIQUE HTTPS://<IP-CONTROLEUR>	13
A. CONFIGURATION DU CONTROLEUR	16
• CREATION DE VLANS	17
• SERVEUR RADIUS :	19
• WLANS (SSID)	21
• ATTRIBUTION DE BALISE DE STRATEGIE	31
• PARAMETRES DE JONCTION AP (AP JOIN PROFILE) SUR LES WLC 9800	31
B. MIGRATION DES APs (AIR-AP1832I-E-K9) VERS CISCO CATALYST 9800 CL	35
B.1 PROBLEME RENCONTRE : IMPOSSIBLE DE DEPLACER LES APs DU CONTROLEUR AIREOS VERS LE NOUVEAU CONTROLEUR CATALYST 9800-CL	35
B.2 SOLUTIONS :	35
1^{ERE} OPTION : REINITIALISER LES APs	35
2^{EME} OPTION : POUR UNE MIGRATION MASSIVE	37
7. TEST	38
- VERIFICATION DES SSID	38
- WIRESHARK : CAPTURE DES TRAMES CAPWAP (ENTRE LES APs ET LE CONTROLEUR 9800 CL)	38
8. CONFIGURATION FINALE :	40
9. SUPERVISION (ZABBIX & NAGIOS)	40
A. AGENT SNMP (CONTROLEUR CATALYST 9800 CL)	40

CONFIGURATION DE L'AGENT SNMP SUR LE CONTROLEUR CISCO CATALYST 9800 CL	40
B. ZABBIX	43
ETAPE 1 : INTEGRATION DU CONTROLEUR CATALYST SUR ZABBIX	43
ETAPE 2 : CREER UNE CARTE DANS ZABBIX AFIN DE VISUALISER L'ETAT DES POINTS D'ACCES (APs)	44
ETAPE 2 : CONFIGURATION D'UNE CARTE POUR LES APs	45

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.

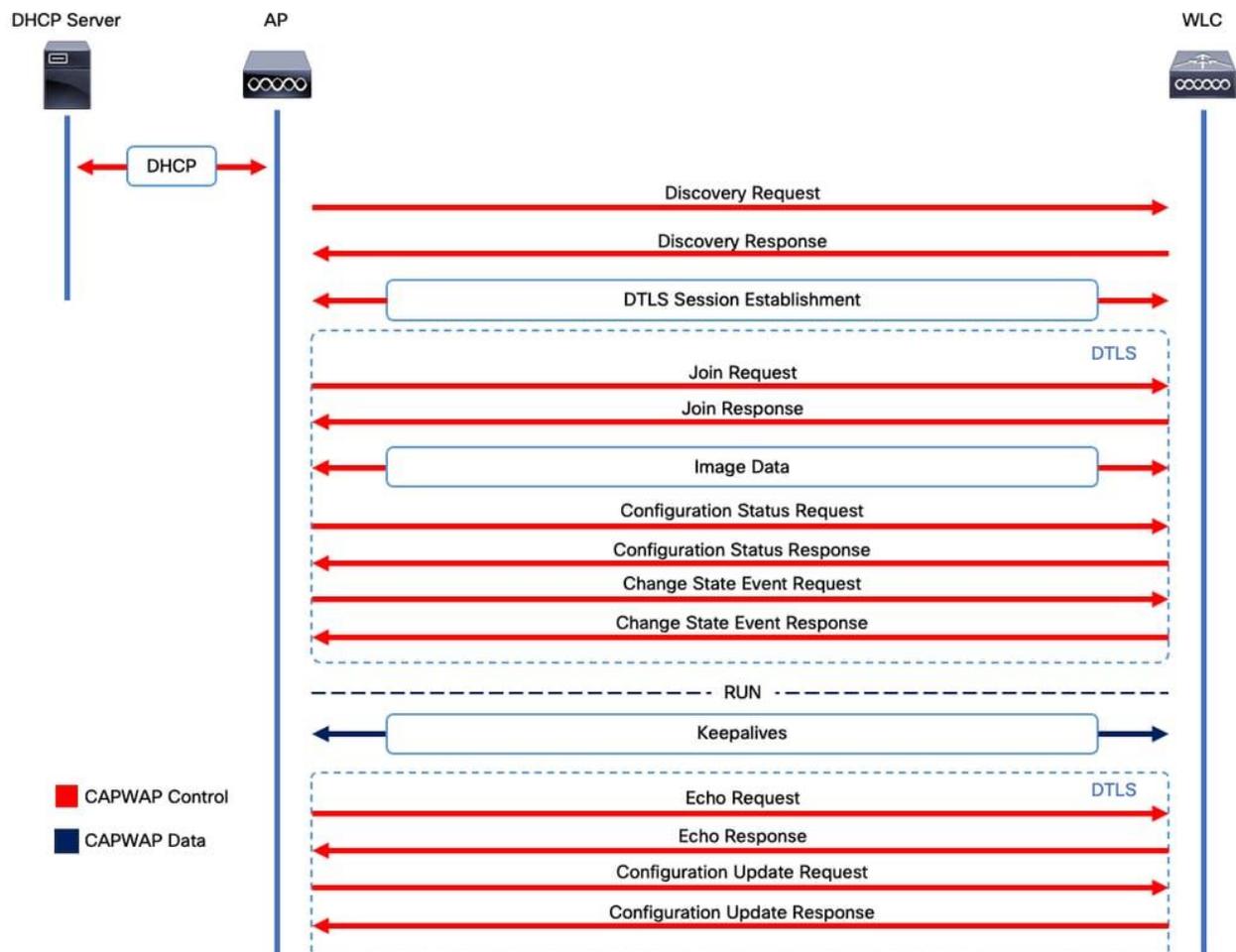
Les bornes Wi-Fi et le contrôleur WLC (Wireless LAN Controleur) communiquent généralement via un protocole appelé **CAPWAP** (Control and Provisioning of Wireless Access Points).

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 établit 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.

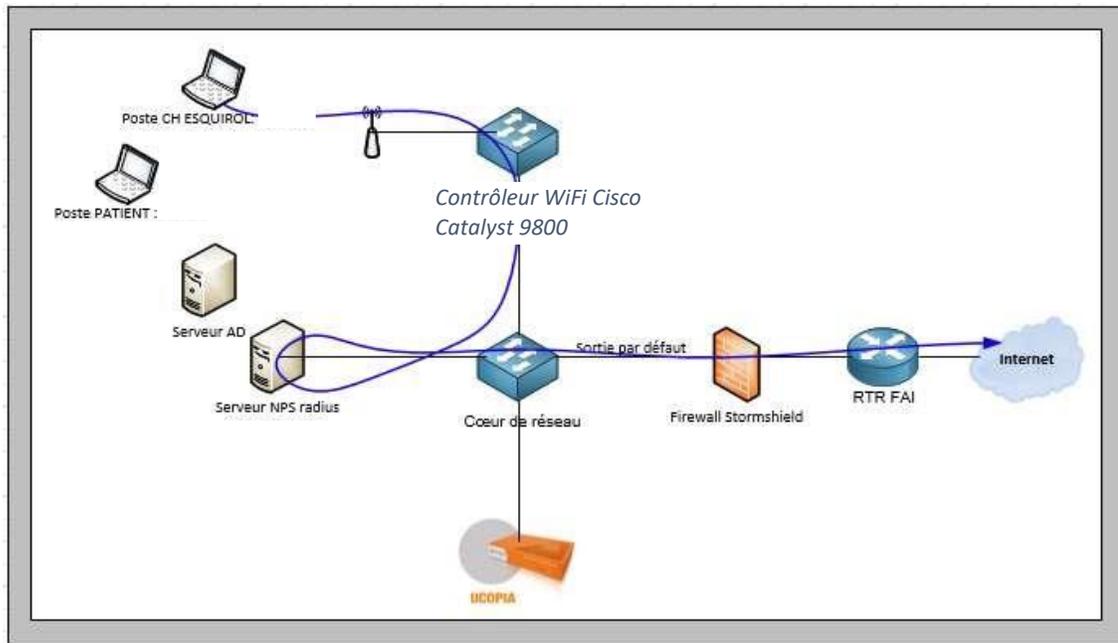
Port de communication : UDP (5246 pour le contrôle de communication et 5247 pour les échanges de données)



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

The screenshot shows the Cisco WLC Monitor interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP. The user is logged in as 'User:mcimara'.

Monitor Summary

313 Access Points Supported
Cisco Virtual Wireless Controller

Controller Summary

Management IP Address	
Service Port IP Address	
Software Version	
Emergency Image Version	
System Name	
Up Time	
System Time	
Redundancy Mode	
802.11a Network State	
802.11b/g Network State	
Local Mobility Group	
CPU(s) Usage	
Individual CPU Usage	
Memory Usage	
vWLC Config	

Access Point Summary

802.11a/n/ac/ax Radios		Detail
802.11b/g/n/ax Radios		Detail
Dual-Band Radios		Detail
Dual-5G Radios		Detail
All APs		Detail

Client Summary

Current Clients	190	Detail
Excluded Clients	10	Detail
Disabled Clients	0	Detail

Rogue Summary

Active Rogue APs	180	Detail
Active Rogue Clients	32	Detail
Adhoc Rogues	0	Detail
Rogues on Wired Network	0	

Session Timeout

Top WLANs

Profile Name	# of Clients	
WIFI_PRO	100	Detail
WIFI_PATIENT	82	Detail
PHARMACIE	7	Detail
BIOMEDICAL	1	Detail

Most Recent Traps

SNMP Authentication Failure: IP Addr	

[View All](#)

Top Flex Applications

Application Name	Packet Count	Byte Count

[View All](#)

This page refreshes every 30 seconds.

- 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/>

The screenshot shows the Cisco TAC Tool - WLC Config Converter website. The page title is "Cisco TAC Tool - WLC Config Converter".

Migration de contrôleurs sans fil vers ou depuis l'une des plates-formes suivantes : contrôleurs 2500/5500/7500/8500/WISM2/3650/3850/4500 SBE/5760/Catalyst 9800

Veuillez télécharger ce qui suit :
AireOS : sortie « show run-config startup-commands » ou sauvegarde de la configuration TFTP
Accès convergé : sortie « show running-config »

Détails

Sauvegarde de la configuration TFTP ou sortie 'show run-config startup-commands' d'AireOS WLC.

Cliquez ici ou déposez le fichier pour le télécharger

plate-forme AireOS-> Catalyst 9800

Courir

[Télécharger CSV](#) [Télécharger CFG traduit](#)

Lignes de configuration converties

Configuration traduite

Configuration non prise en charge

Configuration non applicable [Rechercher](#)

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)

Déployer un modèle OVF

Sélectionner un nom et un dossier

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

Nom de la machine virtuelle : CTRLWIFI

Sélectionnez un emplacement pour la machine virtuelle.

- faitexcus.CHEsquirol.ad
 - Esquirol
 - CAM
 - Discovered virtual machine
 - FORMATION**
 - CITRIX
 - ORACLE
 - Machine virtuelle détectée
 - Templates
 - VM_ETEINTES_avant_suppression

ANNULER PRÉCÉDENT SUIVANT

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

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

- Esquirol
 - Citrix
 - Oracle
 - Production
 - cam-esx1.chesquirol.ad
 - cam-esx2.chesquirol.ad
 - cam-esx4.chesquirol.ad
 - for-esx1.chesquirol.ad**
 - for-esx2.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

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.

Déployer un modèle OVF

- Sélectionner un modèle OVF
- Sélectionner un nom et un dossier
- Sélectionner une ressource de calcul
- Vérifier les informations
- Configuration**
- Sélectionner un stockage
- Sélectionner les réseaux
- Personnaliser un modèle
- Prêt à terminer

Configuration

Sélectionner une configuration de déploiement

<input type="radio"/> 100 APs, 1K Clients	Description 4 vCPU, 8 GB RAM, 3 VNICS, 16 GB Disk
<input checked="" type="radio"/> 1K APs, 10K Clients	
<input type="radio"/> 1K APs, 10K Clients, High Throughput	
<input type="radio"/> 3K APs, 32K Clients	
<input type="radio"/> 3K APs, 32K Clients, High Throughput	
<input type="radio"/> 6K APs, 64K Clients	
<input type="radio"/> 6K APs, 64K Clients, High Throughput	

ANNULER PRÉCÉDENT SUIVANT

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

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

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

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).

Déployer un modèle OVF

- Sélectionner un modèle OVF
- Sélectionner un nom et un dossier
- Sélectionner une ressource de calcul
- Vérifier les informations
- Configuration
- Sélectionner un stockage
- Sélectionner les réseaux**
- Personnaliser un modèle

Sélectionner les réseaux

Sélectionnez un réseau de destination pour chaque réseau source.

Réseau source	Réseau de destination
GigabitEthernet1	INFRASTRUCTURE ▾
GigabitEthernet2	WIFI_INFRA ▾
GigabitEthernet3	TEST ▾

Gérer Les Colonnes 3 élément(s)

Paramètres d'allocation d'IP

Allocation d'IP : Statique - Manuel

Protocole IP : IPv4

[ANNULER](#) [PRÉCÉDENT](#) [SUIVANT](#)

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

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

2.1 Device Management/Service Interface	Management interface (such as "GigabitEthernet") <u>GigabitEthernet1</u>
2.2 Device Management/Service Interface IPv4 Address/Netmask	IPv4 address and mask for management interface (such as "192.0.2.100/24" or "192.0.2.100 255.255.255.0"), or "dhcp" to configure via DHCP <input style="width: 100%;" type="text"/>
2.3 Device Management/Service Interface IPv4 Gateway	IPv4 gateway address (such as "192.0.2.1") for management interface, or "dhcp" to configure via DHCP <input style="width: 100%;" type="text"/>
2.4 Remote Device Management/Service Network Route/Netmask	This will add a route to the remote network where you want to manage your device from (Hint: To add the default route enter 0.0.0.0) <u>0.0.0.0</u>

ANNULER
PRÉCÉDENT
SUIVANT

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

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

3. User login Configuration 4 paramètres

3.1 Login Username	Username for remote login <u>admin</u>
3.2 Login Password	Password for remote login. 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	<input style="width: 100%;" type="password"/>
Confirmer le mot de passe	<input style="width: 100%;" type="password"/>

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

Prêt à terminer

GigabitEthernet2	WIFI_INFRA
GigabitEthernet3	TEST
Paramètres d'allocation d'IP	
Protocole IP	IPv4
Allocation d'IP	Statique - Manuel
Personnaliser un modèle	
Propriétés	
1.1 Hostname = CTRLWIFI	
2.1 Device Management/Service Interface = GigabitEthernet1	
2.2 Device Management/Service Interface IPv4 Address/Netmask =	
2.3 Device Management/Service Interface IPv4 Gateway =	
2.4 Remote Device Management/Service Network Route/Netmask = 0.0.0.0	
3.1 Login Username = admin	
Serial Number for the C9800-CL Instance =	

ANNULER
PRÉCÉDENT
TERMINER

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

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

Configuration Setup Wizard

1. General Settings

Deployment Mode	Standalone ▼	
Host Name*	CTRLWIFI	
Country	US	+
Date	15 Jan 2025	📅
Time / Timezone	11:36:12	🕒 heure ▼
NTP Servers	Enter NTP Server +	
	Added NTP servers	
AAA Servers	Enter Radius Server IP	Enter Key 🔑 +

- On complètera l'adresse du serveur radius ultérieurement

1. General Settings

AAA Servers

Enter Radius Server IP Enter Key  

Added AAA servers

Wireless Management Settings

Port Number: GigabitEthernet2

Wireless Management VLAN*: 87

IPv4:

Wireless Management IP*:

Subnet Mask*:

IPv6:

Static Route Settings

[Click here](#) to view currently configured routes

IPv4 Route:

IPv6 Route:

Next

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

2. Wireless Network Settings

 Add  Delete

Network Name	Network Type	Security
No items to display		

Navigation: << 0 >> 10

Previous **Next**

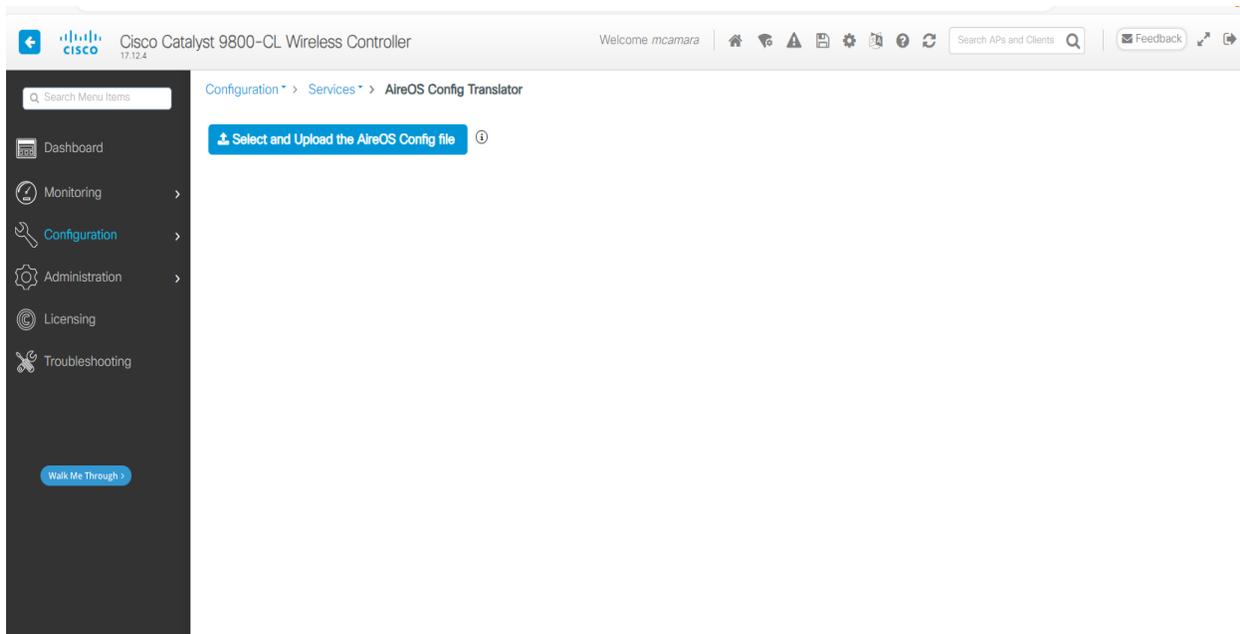
- Ensuite, indiquer le **groupe RF** (Radio Frequency Group) pour la gestion des paramètres RF, le **type du trafic** (Data). Laisser l'adresse IP virtuelle du contrôleur par défaut (192.0.2.1).

The screenshot shows the '3. Advanced Settings' configuration page. It includes a slider for 'Client Density' set to 'Typical'. Below it are input fields for 'RF Group Name*' (RF-CETRA), 'Traffic Type' (Data), and 'Virtual IP Address' (192.0.2.1). A section titled 'AP Certificate' contains a 'Generate Certificate' toggle set to 'YES', 'RSA Key-Size' (4096), 'Signature Algorithm' (sha256), and a 'Password*' field. A 'Create New AP Management User' section has an empty 'New AP Management User*' field. 'Previous' and 'Summary' buttons are at the bottom right.

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**.



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 créés 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

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 :

Edit SVI: Vlan24

General Advanced

Description: (1-200 Characters)

Admin Status:

VRF:

MTU (bytes):

IP Options: IPV4 IPV6

IPv4 Type:

IP Address *:

Subnet Mask *:

Secondary IP:

- Création de VLANs
On crée un VLAN pour chaque SVI

Configuration > Layer2 > VLAN

SVI **VLAN** VLAN Group

VLAN ID	Name	Status	Ports
<input type="checkbox"/> 1	default	active	Gi3
<input type="checkbox"/> 3	wifi_patient	active	
<input type="checkbox"/> 5	biomedical	active	
<input type="checkbox"/> 24	wifi_pro	active	
<input type="checkbox"/> 87	VLAN0087	active	

1 - 5 of 5 items

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.

The screenshot shows the configuration page for a VLAN named 'wifi_pro'. The fields are as follows:

- VLAN ID*: 24
- Name: wifi_pro
- State: ACTIVATED (with a green toggle)
- IGMP Snooping: DISABLED
- ARP Broadcast: DISABLED

Under the 'Port Members' section, there is a search bar and two columns:

- Available (1)**: Contains one entry, 'Gi3', with a blue arrow pointing to the right.
- Associated (0)**: Contains the text 'No Associated Members'.

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 :

Configure Interface GigabitEthernet2

General Advanced

Interface: GigabitEthernet2

Description: (1-200 Characters)

Admin Status: **UP**

Enable Layer 3 Address: DISABLED

Switchport Mode:

Allowed VLAN: All VLAN IDs

VLAN IDs: (e.g. 1,2,4,6-10)

Native VLAN:

- 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.**

The screenshot shows the Cisco configuration interface for "Authentication Authorization and Accounting". On the left is a navigation menu with "Configuration" selected. The main content area shows a table with columns "AAA Method List", "Servers / Groups", and "AAA Ac". A red box highlights the "+ AAA Wizard" button. The table lists methods: General, Authentication, Authorization, and Accounting. Under "General", there are links for "Dot1x System Auth Control", "Local Authentication", "Local Authorization", "Radius Server Load Balance", and "Show Advanced Settings >>>".

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**.

The screenshot shows the 'Add Wizard' interface with three steps: SERVER, SERVER GROUP ASSOCIATION, and MAP AAA. The 'SERVER' step is active. Under 'SERVER', the 'RADIUS' checkbox is checked, while 'TACACS+' and 'LDAP' are unchecked. Below this, the 'RADIUS' section is expanded, showing fields for 'Name*' (with 'server-name' entered), 'Server Address*', 'Shared Secret*', and 'Confirm Shared Secret*'. A red box highlights the 'RADIUS' selection and the 'Name*' field, while a green box highlights the 'Server Address*' and 'Shared Secret*' fields.

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**.

The screenshot shows the 'Edit AAA Radius Server Group' configuration page. Fields include: 'Name*' (Server_Radius), 'Group Type' (RADIUS), 'MAC-Delimiter' (none), 'MAC-Filtering' (none), 'Dead-Time (mins)' (5), 'Load Balance' (DISABLED), and 'Source Interface VLAN ID' (1). Below these are two sections: 'Available Servers' containing 'Server_Radius_2' and 'Assigned Servers' containing 'Radius_Server'. Between these sections are four arrow buttons: a right arrow (>), a left arrow (<), a double right arrow (>>), and a double left arrow (<<).

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

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

Quick Setup: AAA Authentication

Method List Name*

Type* ⓘ

Group Type ⓘ

Fallback to local

Available Server Groups

ldap
tacacs+



Assigned Server Groups

Server_Radius
radius



- 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.**

Cisco Catalyst 9800-CL Wireless Controller 17.12.4

Welcome mcamara

Configuration > Tags & Profiles > WLANs

+ Add × Delete Clone Enable WLAN Disable WLAN

Selected WLANs : 0

<input type="checkbox"/>	Status	Name	ID	SSID
<input type="checkbox"/>	+	WiFi_PATIENT	2	WiFi_PATIENT
<input type="checkbox"/>	+	WiFi_PRO	3	WiFi_PRO
<input type="checkbox"/>	+	biomedical	4	biomedical
<input type="checkbox"/>	+	PHARMACIE	5	PHARMACIE

1 / 10

- **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**.

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General Security Advanced Add To Policy Tags

Profile Name* WiFi_PRO

SSID* WiFi_PRO

WLAN ID* 3

Status ENABLED

Broadcast SSID ENABLED

Radio Policy ⓘ

Show slot configuration

6 GHz
Status DISABLED

5 GHz
Status ENABLED

2.4 GHz
Status ENABLED

802.11b/g Policy 802.11b/g ▼

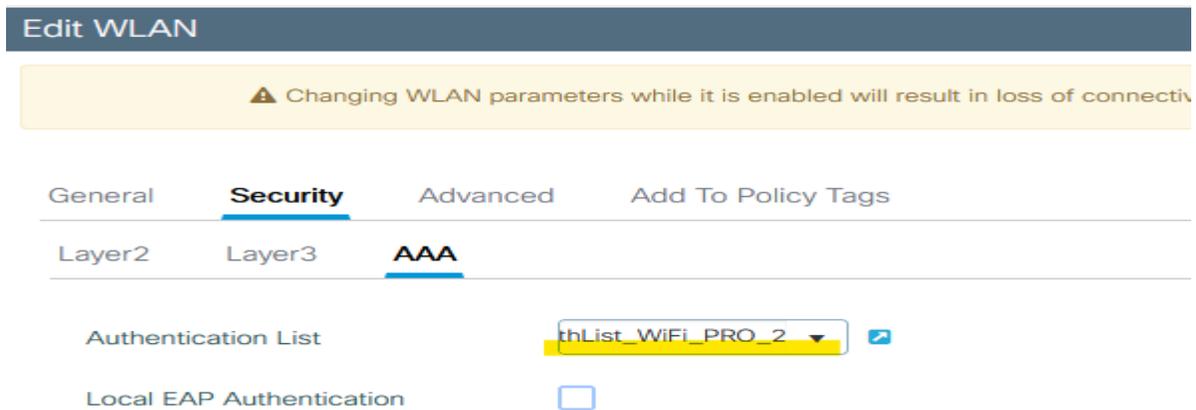
Dans l'onglet Security, on précise le type d'authentification.

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

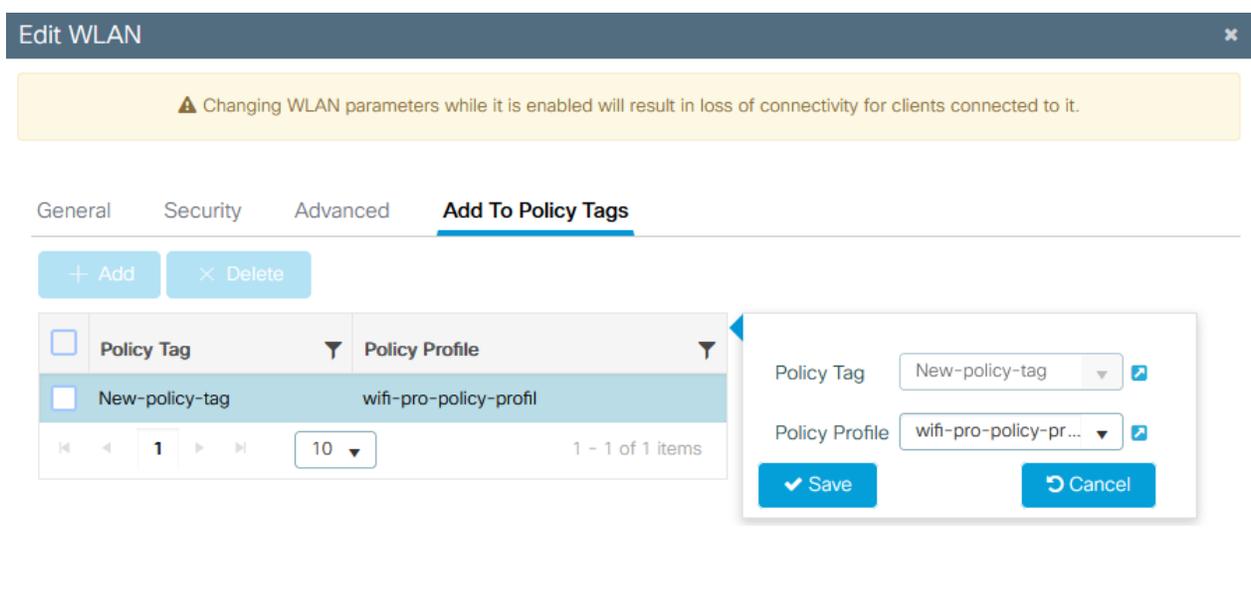
Par mesure de sécurité la diffusion du SSID est caché.

The screenshot shows the 'Edit WLAN' configuration interface. At the top, there is a warning banner: 'Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.' Below this, the 'Security' tab is selected, and the 'Layer2' sub-tab is active. The authentication type is set to 'WPA + WPA2'. Under 'WPA Parameters', 'WPA2 Policy' is checked. Under 'WPA2 Encryption', 'AES(CCMP128)' is selected. Under 'Protected Management Frame', 'PMF' is set to 'Disabled'. Under 'Auth Key Mgmt', '802.1X' is checked. Under 'Fast Transition', 'Status' is 'Disabled' and 'Reassociation Timeout *' is '20'. Under 'MPSK Configuration', 'Enable MPSK' is unchecked. At the bottom, there are 'Cancel' and 'Update & Apply to Device' buttons.

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



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 ..)

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General Security Advanced Add To Policy Tags

Profile Name* PHARMACIE

SSID* PHARMACIE

WLAN ID* 5

Status **ENABLED**

Broadcast SSID **ENABLED**

Radio Policy ⓘ

Show slot configuration

6 GHz Status DISABLED

5 GHz Status **ENABLED**

2.4 GHz Status **ENABLED**

802.11b/g Policy 802.11b/g ▼

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**.

Edit WLAN

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering Authorization List* Mac-Filter ⓘ

Lobby Admin Access

WPA Parameters

WPA Policy WPA2 Policy

GTK Randomize OSEN Policy

WPA2 Encryption

AES(CCMP128) CCMP256

GCMP128 GCMP256

Protected Management Frame

PMF Disabled ▼

Fast Transition

Status Disabled ▼

Over the DS

Reassociation Timeout * 20

Auth Key Mgmt

802.1X PSK

Easy-PSK CCKM ⓘ

FT + 802.1X FT + PSK

802.1X-SHA256 PSK-SHA256

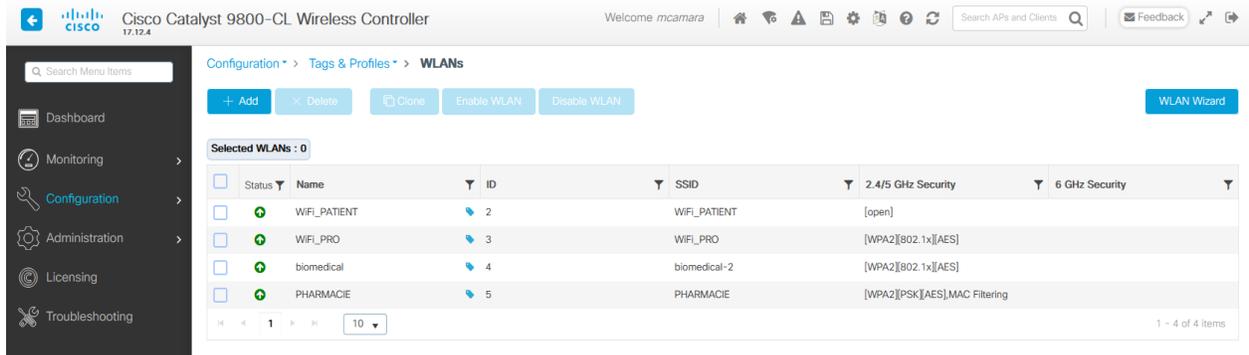
PSK Format ASCII ▼

PSK Type Unencrypted ▼

Pre-Shared Key* ●●●●●●●●

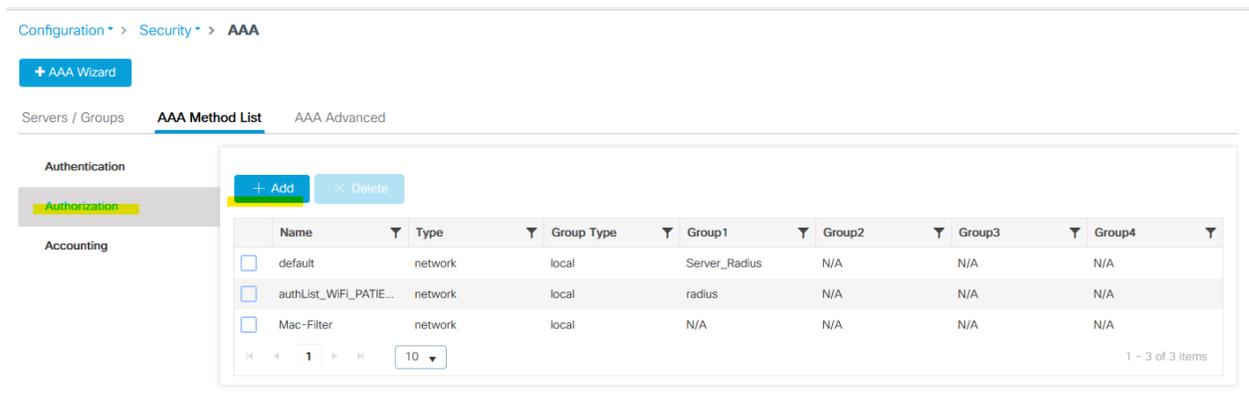
Cancel Update & Apply to Device

Au final, 4 SSID sont créés

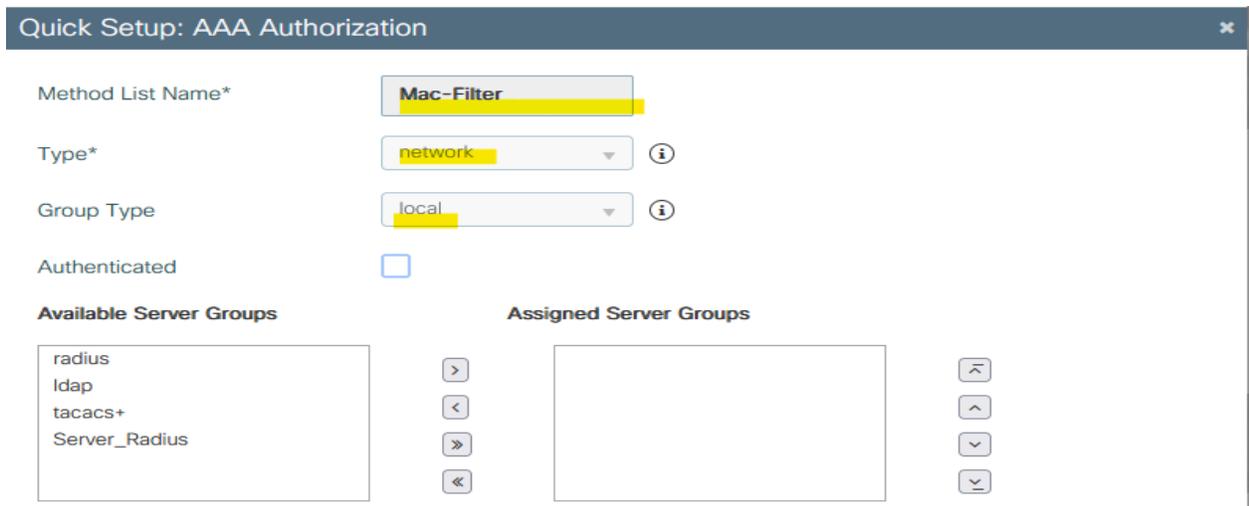


Etape 2 : Créez une méthode de réseau d'autorisation (Filtrage Mac).

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.



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

The screenshot displays the network configuration interface. The breadcrumb navigation is **Configuration > Security > AAA**. The **AAA Advanced** section is active, showing a list of attribute list names: **ATTR_LIST_PHARMACIE** and **Attr-Mac-PHAR**. A modal window titled **Edit Attribute List** is open, showing the configuration for **ATTR_LIST_PHARMACIE**. The **Attribute Type** is set to **SSID** and the **Attribute Value** is **PHARMACIE**. The **Save** button is highlighted.

Enregistrez les adresses MAC autorisées.

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

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

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List **AAA Advanced**

Global Config

RADIUS Fallback

Attribute List Name

Device Authentication

AP Policy

Password Policy

AAA Interface

MAC Address Serial Number

+ Add - Delete Select File Upload File

MAC Address	Attribute List Name	Description	WLAN Profile
<input type="checkbox"/>	ATTR_LIST_PHARMACIE	Portable Pharmacie	PHARMACIE
<input type="checkbox"/>	ATTR_LIST_PHARMACIE		PHARMACIE
<input type="checkbox"/>	ATTR_LIST_PHARMACIE		PHARMACIE
<input type="checkbox"/>	ATTR_LIST_PHARMACIE		PHARMACIE
<input type="checkbox"/>	ATTR_LIST_PHARMACIE		PHARMACIE

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

Edit MAC Filtering

MAC Address*

Attribute List Name

Description

WLAN Profile Name

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.

Edit Policy Profile ✕

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General **Access Policies** QOS and AVC Mobility Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification Disabled ⓘ

Local Subscriber Policy Name

VLAN

VLAN/VLAN Group

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters ⓘ

Pre Auth

Post Auth

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

Créer en un pour chaque vlan

Configuration > Tags & Profiles > Policy

+ Add ✕ Delete 📄 Clone

	Admin Status	Associated Policy Tags	Policy Profile Name	Description
<input type="checkbox"/>	✓		default-policy-profile	default policy profile
<input type="checkbox"/>	✓		wifi-pro-policy-profil	
<input type="checkbox"/>	✓		biomedical-policy-profil	
<input type="checkbox"/>	✓		wifi-patient-policy-profil	

1 / 10

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.

Cisco Catalyst 9800-CL Wireless Controller

Welcome mcamara

Search APs and Clients

Feedback

Configuration > Tags & Profiles > Tags

Policy Site RF AP

+Add Delete Clone

Policy Tag Name	Description
<input checked="" type="checkbox"/> New-policy-tag	Esquirol-policy-tag
<input type="checkbox"/> default-policy-tag	default-policy-tag

1 - 2 of 2 items

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.

Edit Policy Tag

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name*

Description

WLAN-POLICY Maps: 4

+ Add Delete

WLAN Profile	Policy Profile
<input checked="" type="checkbox"/> WiFi_PRO	wifi-pro-policy-profil
<input type="checkbox"/> PHARMACIE	wifi-pro-policy-profil
<input type="checkbox"/> biomedical	biomedical-policy-profil
<input type="checkbox"/> WiFi_PATIENT	wifi-patient-policy-profil

1 - 4 of 4 items

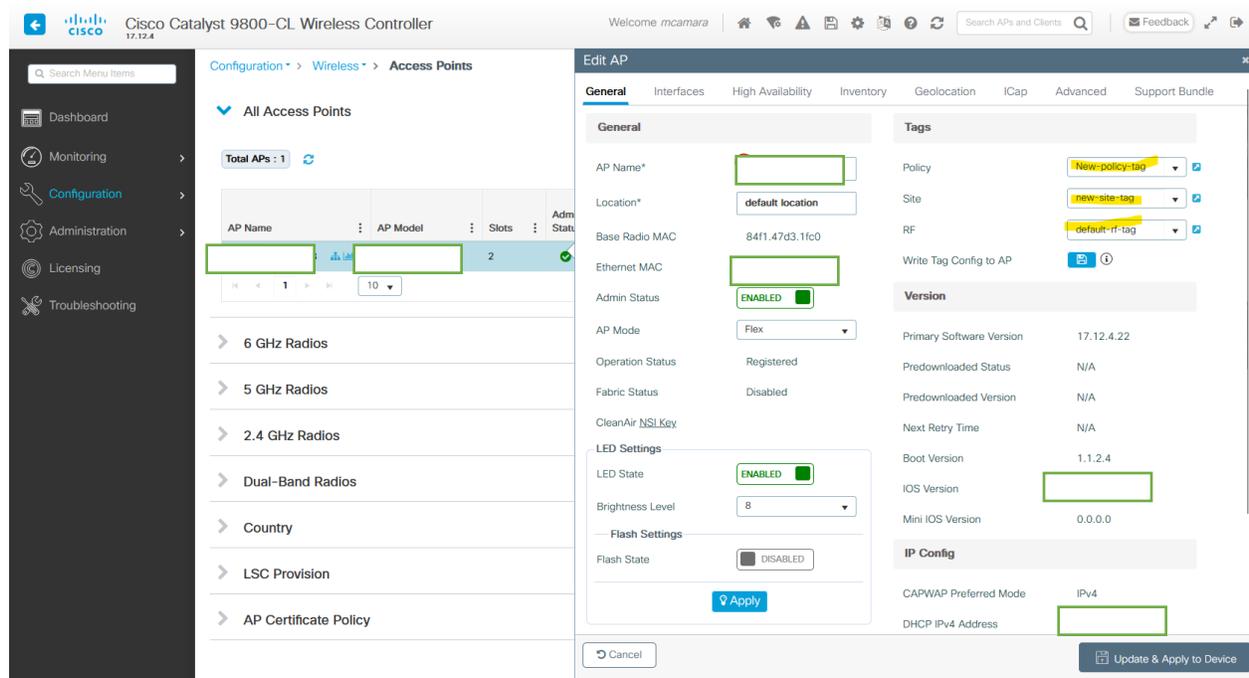
Map WLAN and Policy

WLAN Profile* Policy Profile*

RLAN-POLICY Maps: 0

- 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.

Cisco Catalyst 9800-CL Wireless Controller 17.12.4

Welcome mcamara

Configuration > Tags & Profiles > AP Join

+ Add × Delete Clone

AP Join Profile Name	Description
<input type="checkbox"/> GRP-AP-MAS	
<input type="checkbox"/> GRP-AP-MDA	
<input type="checkbox"/> GRP-AP-TEST	
<input type="checkbox"/> GRP-AP-USIS	
<input type="checkbox"/> GRP-AP-MAGNAC	
<input type="checkbox"/> GRP-AP-BOBILLLOT	
<input type="checkbox"/> GRP-AP-ESQUIROL	
<input type="checkbox"/> GRP-AP-STJUNIEN	
<input type="checkbox"/> GRP-AP-PHARMACIE	
<input type="checkbox"/> GRP-AP-SERVCTECH	

1 2 10

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

Edit AP Join Profile

General Client CAPWAP AP Management Security ICap QoS Geolocation

Name* GRP-AP-ESQUIROL

Description Enter Description

Country Code FR

Time Zone Not Configured
 Use-Controller
 Delta from WLC

LED State

LAG Mode

NTP Server 0.0.0.0

GAS AP Rate Limit

USB Enable

Apphost

Fallback to DHCP

OfficeExtend AP Configuration

Local Access

Link Encryption

Rogue Detection

Provisioning SSID

Antenna Monitoring

Antenna Monitoring

RSSI Fail Threshold(dB)* 40

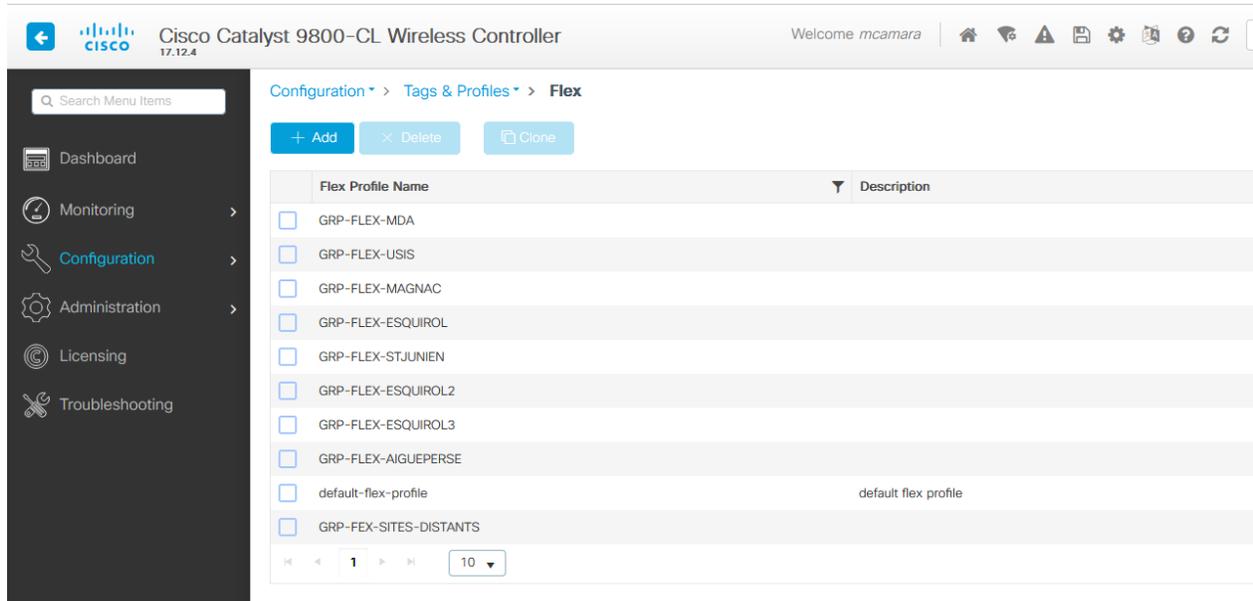
Weak RSSI(dBm)* -60

Detection Time(min)* 12

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

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

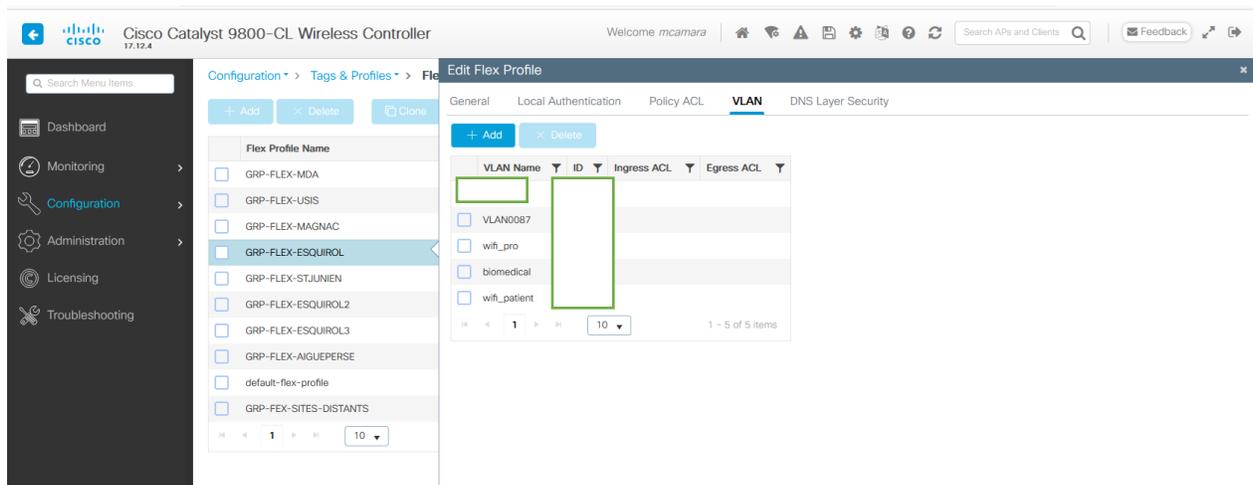
Sélectionnez le nom d'un profil établi ou cliquez sur **+ Ajouter** pour en ajouter un nouveau.



The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The breadcrumb navigation is Configuration > Tags & Profiles > Flex. There are buttons for '+ Add', 'Delete', and 'Clone'. A table lists the following Flex Profile Names and their descriptions:

Flex Profile Name	Description
<input type="checkbox"/> GRP-FLEX-MDA	
<input type="checkbox"/> GRP-FLEX-USIS	
<input type="checkbox"/> GRP-FLEX-MAGNAC	
<input type="checkbox"/> GRP-FLEX-ESQUIROL	
<input type="checkbox"/> GRP-FLEX-STJUNIEN	
<input type="checkbox"/> GRP-FLEX-ESQUIROL2	
<input type="checkbox"/> GRP-FLEX-ESQUIROL3	
<input type="checkbox"/> GRP-FLEX-AIGUEPERSE	
<input type="checkbox"/> default-flex-profile	default flex profile
<input type="checkbox"/> GRP-FEX-SITES-DISTANTS	

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



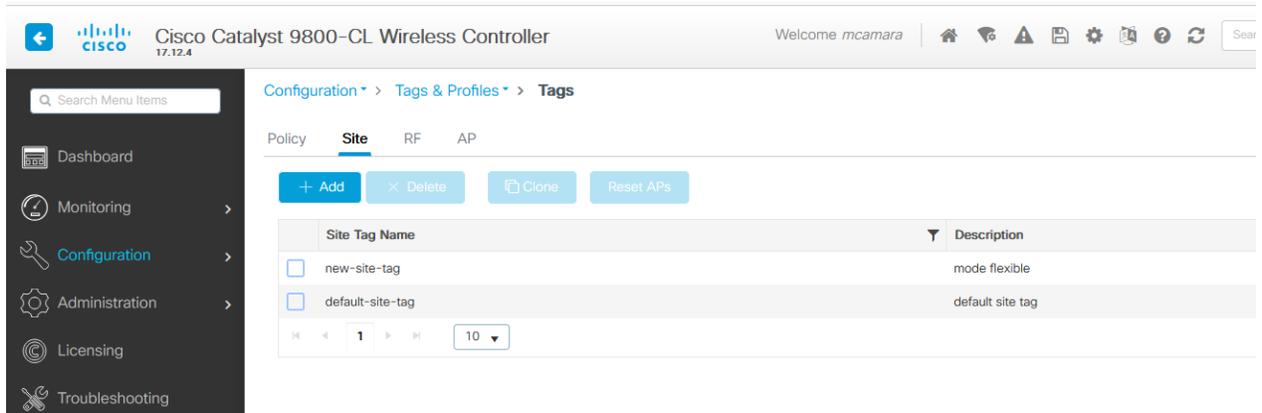
The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface with the 'Edit Flex Profile' dialog box open. The 'VLAN' tab is selected. The dialog box shows a table of VLANs with the following columns: VLAN Name, ID, Ingress ACL, and Egress ACL. The 'VLAN Name' and 'ID' columns are highlighted with green boxes.

VLAN Name	ID	Ingress ACL	Egress ACL
<input type="checkbox"/> VLAN0087			
<input type="checkbox"/> wif_pro			
<input type="checkbox"/> biomedical			
<input type="checkbox"/> wif_patient			

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.

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.



The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller configuration interface. The breadcrumb navigation is Configuration > Tags & Profiles > Tags. The 'Site' tab is selected. There are buttons for '+ Add', 'Delete', 'Clone', and 'Reset APs'. A table lists existing site tags:

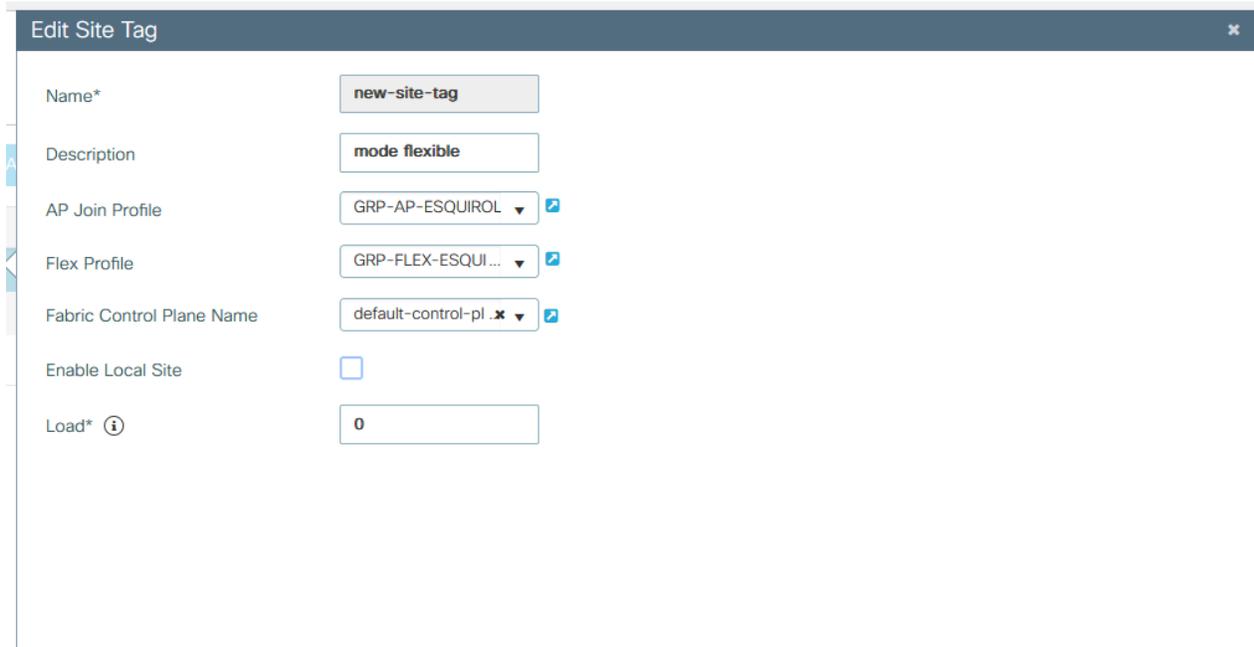
Site Tag Name	Description
<input type="checkbox"/> new-site-tag	mode flexible
<input type="checkbox"/> default-site-tag	default site tag

At the bottom of the table, there are navigation controls showing page 1 of 10.

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**.



The screenshot shows the 'Edit Site Tag' configuration form. The fields are as follows:

- Name*: new-site-tag
- Description: mode flexible
- AP Join Profile: GRP-AP-ESQUIROL
- Flex Profile: GRP-FLEX-ESQUI...
- Fabric Control Plane Name: default-control-pl .x
- Enable Local Site:
- Load*: 0

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

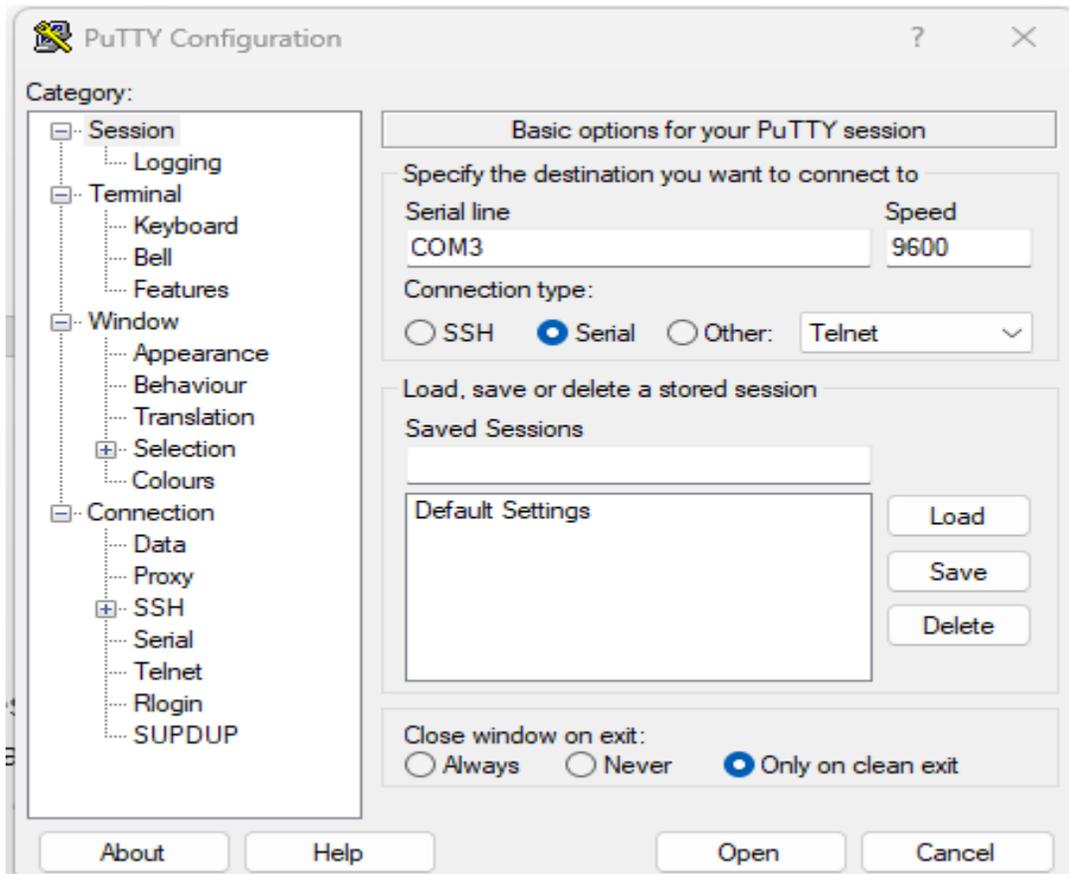
```
] display_verify_cert_status: Verify Cert: FAILED at 1 depth: self signed certificate in certificate chain
[*02/10/2025 12:48:06.1299] X509 OpenSSL Errors...
[*02/10/2025 12:48:06.1299]
[*02/10/2025 12:48:06.1299] NONE
[*02/10/2025 12:48:06.1299]
[*02/10/2025 12:48:06.1299] dtls_verify_con_cert: 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 :

1^{ère} 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`

```
[*01/22/2025 12:35:45.1299]
[*01/22/2025 12:35:45.1499] dtls_verify_server_cert: vWLC is using SSC, returning 1
[*01/22/2025 12:35:45.2399]
[*01/22/2025 12:35:45.2399] CAPWAP State: Join
[*01/22/2025 12:35:45.4299] Sending Join request [redacted] through port 5256, packet size 1376
[*01/22/2025 12:35:50.3683] Sending Join request [redacted] through port 5256, packet size 1376
[*01/22/2025 12:35:50.3783] Join Response from [redacted] et size 1397
[*01/22/2025 12:35:50.3783] AC accepted previous sent request with result code: 0
[*01/22/2025 12:35:50.3783] Received wlcType 0, timer 30
[*01/22/2025 12:35:50.5683] nss_capwapmgr_enable_tunnel[1682]:ef30b800: tunnel 0 is already enabled
[*01/22/2025 12:35:50.6082]
[*01/22/2025 12:35:50.6082] CAPWAP State: Image Data
[*01/22/2025 12:35:50.6082] AP image version [redacted] 2 backup 8.10.185.0, Controller 17.12.4.22
[*01/22/2025 12:35:50.6082] Version is the same, do not need update.
[*01/22/2025 12:35:50.7382] status 'upgrade.sh: Script called with args:[NO_UPGRADE]'
[*01/22/2025 12:35:50.7882] do NO_UPGRADE, part1 is active part
```

2^{ème} 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.

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	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#
```

Top WLANs
Last Updated: 2/13/2025, 1:26:49 PM

Sort by: WLANs With Highest Client Co...

WLAN Name	ID	Clients	Data Usage
WiFi_PRO	3	11	26 GB
WiFi_PATIENT	2	7	72 GB
biomedical	4	1	3.2 MB

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

capture capwap.pcapng

Fichier Editer Vue Aller Capture Analyseur Statistiques Telephone Wireless Outils Aide

syslog

No.	Time	Source	Destination	Protocol	Length	Info
1920	245.714216		255.255.255.255	Syslog	112	KERN.WARNING: Feb 11 13:45:54
1921	245.714216		255.255.255.255	Syslog	112	KERN.WARNING: Feb 11 13:45:54
1922	245.714216		255.255.255.255	Syslog	130	KERN.WARNING: Feb 11 13:45:54
1923	245.714216		255.255.255.255	Syslog	112	KERN.WARNING: Feb 11 13:45:54
1924	245.714216		255.255.255.255	Syslog	130	KERN.WARNING: Feb 11 13:45:54
1925	245.714216		255.255.255.255	Syslog	130	KERN.WARNING: Feb 11 13:45:54
1926	245.714216		255.255.255.255	Syslog	130	KERN.WARNING: Feb 11 13:45:54
1928	245.884297		255.255.255.255	Syslog	183	KERN.WARNING: Feb 11 13:45:54
1929	245.884297		255.255.255.255	Syslog	183	KERN.WARNING: Feb 11 13:45:54
1930	245.884297		255.255.255.255	Syslog	183	KERN.WARNING: Feb 11 13:45:54
1931	245.884297		255.255.255.255	Syslog	183	KERN.WARNING: Feb 11 13:45:54
1932	245.884297		255.255.255.255	Syslog	183	KERN.WARNING: Feb 11 13:45:54
1962	250.724398		255.255.255.255	Syslog	183	KERN.WARNING: Feb 11 13:45:59
1963	250.724398		255.255.255.255	Syslog	160	KERN.WARNING: Feb 11 13:45:59
1964	250.724398		255.255.255.255	Syslog	183	KERN.WARNING: Feb 11 13:45:59
1965	250.724398		255.255.255.255	Syslog	183	KERN.WARNING: Feb 11 13:45:59
1966	250.724398		255.255.255.255	Syslog	165	KERN.WARNING: Feb 11 13:45:59
1967	250.724398		255.255.255.255	Syslog	183	KERN.WARNING: Feb 11 13:45:59
1968	250.724398		255.255.255.255	Syslog	160	KERN.WARNING: Feb 11 13:45:59
1969	250.724398		255.255.255.255	Syslog	140	KERN.WARNING: Feb 11 13:45:59
1970	250.724398		255.255.255.255	Syslog	183	KERN.WARNING: Feb 11 13:45:59
1971	250.724398		255.255.255.255	Syslog	165	KERN.WARNING: Feb 11 13:45:59
1972	250.724463		255.255.255.255	Syslog	160	KERN.WARNING: Feb 11 13:45:59
1973	250.724463		255.255.255.255	Syslog	160	KERN.WARNING: Feb 11 13:45:59
1974	250.724463		255.255.255.255	Syslog	140	KERN.WARNING: Feb 11 13:45:59
1975	250.724463		255.255.255.255	Syslog	160	KERN.WARNING: Feb 11 13:45:59
1976	250.724463		255.255.255.255	Syslog	165	KERN.WARNING: Feb 11 13:45:59
1977	250.724463		255.255.255.255	Syslog	165	KERN.WARNING: Feb 11 13:45:59
1978	250.724463		255.255.255.255	Syslog	165	KERN.WARNING: Feb 11 13:45:59
1979	250.724463		255.255.255.255	Syslog	140	KERN.WARNING: Feb 11 13:45:59
1980	250.724463		255.255.255.255	Syslog	140	KERN.WARNING: Feb 11 13:45:59
1981	250.724463		255.255.255.255	Syslog	140	KERN.WARNING: Feb 11 13:45:59
1984	250.864184		255.255.255.255	Syslog	183	KERN.WARNING: Feb 11 13:45:59
1985	250.864184		255.255.255.255	Syslog	183	KERN.WARNING: Feb 11 13:45:59
1986	250.864184		255.255.255.255	Syslog	183	KERN.WARNING: Feb 11 13:45:59
1987	250.864184		255.255.255.255	Syslog	183	KERN.WARNING: Feb 11 13:45:59
1988	250.864184		255.255.255.255	Syslog	183	KERN.WARNING: Feb 11 13:45:59
1989	250.884806		255.255.255.255	Syslog	112	KERN.WARNING: Feb 11 13:45:59
1990	250.884806		255.255.255.255	Syslog	136	KERN.WARNING: Feb 11 13:45:59
1991	250.884806		255.255.255.255	Syslog	112	KERN.WARNING: Feb 11 13:45:59
1992	250.884806		255.255.255.255	Syslog	112	KERN.WARNING: Feb 11 13:45:59
1993	250.884806		255.255.255.255	Syslog	112	KERN.WARNING: Feb 11 13:45:59

kernel: [*02/11/2025 13:45:54.0999] \n
kernel: [*02/11/2025 13:45:54.0999] \n
kernel: [*02/11/2025 13:45:54.0999] CAPWAP State: Join\n
kernel: [*02/11/2025 13:45:54.0999] \n
kernel: [*02/11/2025 13:45:54.0999] CAPWAP State: Join\n
kernel: [*02/11/2025 13:45:54.0999] CAPWAP State: Join\n
kernel: [*02/11/2025 13:45:54.0999] CAPWAP State: Join\n
kernel: [*02/11/2025 13:45:54.2699] Sending Join request to [redacted] through port 5264, packet size 1376\n
kernel: [*02/11/2025 13:45:54.2699] Sending Join request to [redacted] through port 5264, packet size 1376\n
kernel: [*02/11/2025 13:45:54.2699] Sending Join request to [redacted] through port 5264, packet size 1376\n
kernel: [*02/11/2025 13:45:54.2699] Sending Join request to [redacted] through port 5264, packet size 1376\n
kernel: [*02/11/2025 13:45:59.1084] Sending Join request to [redacted] through port 5264, packet size 1376\n
kernel: [*02/11/2025 13:45:59.1084] Join Response from 172.3[redacted] packet size 1397\n
kernel: [*02/11/2025 13:45:59.1084] Sending Join request to [redacted] through port 5264, packet size 1376\n
kernel: [*02/11/2025 13:45:59.1084] Sending Join request to [redacted] through port 5264, packet size 1376\n
kernel: [*02/11/2025 13:45:59.1084] AC accepted previous sent request with result code: 0\n
kernel: [*02/11/2025 13:45:59.1084] Sending Join request to [redacted] through port 5264, packet size 1376\n
kernel: [*02/11/2025 13:45:59.1084] Join Response from [redacted] packet size 1397\n
kernel: [*02/11/2025 13:45:59.1084] Received wlcType 0, timer 30\n
kernel: [*02/11/2025 13:45:59.1084] Sending Join request to [redacted] through port 5264, packet size 1376\n
kernel: [*02/11/2025 13:45:59.1084] AC accepted previous sent request with result code: 0\n
kernel: [*02/11/2025 13:45:59.1084] Join Response from [redacted], packet size 1397\n
kernel: [*02/11/2025 13:45:59.1084] Join Response from [redacted], packet size 1397\n
kernel: [*02/11/2025 13:45:59.1084] Received wlcType 0, timer 30\n
kernel: [*02/11/2025 13:45:59.1084] Join Response from [redacted] packet size 1397\n
kernel: [*02/11/2025 13:45:59.1084] AC accepted previous sent request with result code: 0\n
kernel: [*02/11/2025 13:45:59.1084] AC accepted previous sent request with result code: 0\n
kernel: [*02/11/2025 13:45:59.1084] AC accepted previous sent request with result code: 0\n
kernel: [*02/11/2025 13:45:59.1084] Received wlcType 0, timer 30\n
kernel: [*02/11/2025 13:45:59.1084] Received wlcType 0, timer 30\n
kernel: [*02/11/2025 13:45:59.1084] Received wlcType 0, timer 30\n
kernel: [*02/11/2025 13:45:59.2484] nss_capwapmgr_enable_tunnel[1682]:ef30a000: tunnel 0 is already enabled\n
kernel: [*02/11/2025 13:45:59.2484] nss_capwapmgr_enable_tunnel[1682]:ef30a000: tunnel 0 is already enabled\n
kernel: [*02/11/2025 13:45:59.2484] nss_capwapmgr_enable_tunnel[1682]:ef30a000: tunnel 0 is already enabled\n
kernel: [*02/11/2025 13:45:59.2484] nss_capwapmgr_enable_tunnel[1682]:ef30a000: tunnel 0 is already enabled\n
kernel: [*02/11/2025 13:45:59.2684] \n
kernel: [*02/11/2025 13:45:59.2684] CAPWAP State: Image Data\n
kernel: [*02/11/2025 13:45:59.2684] \n
kernel: [*02/11/2025 13:45:59.2684] \n
kernel: [*02/11/2025 13:45:59.2684] \n

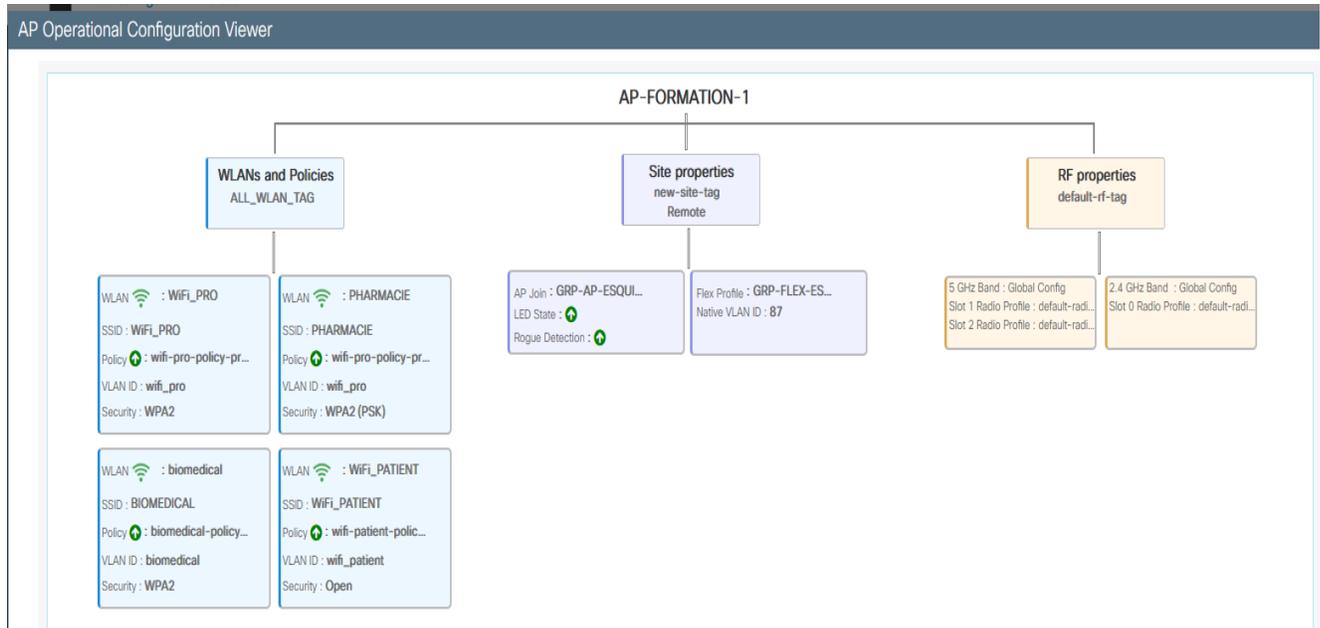
> Frame 1969: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on Interface \Device\NPF_{F4979608-672B-4F...
> Ethernet II, Src: [redacted] Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: [redacted] Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 38586, Dst Port: 514
> Syslog message: KERN.WARNING: Feb 11 13:45:59 [redacted] kernel: [*02/11/2025 13:45:59.1084] Received wlcType 0,

```

0000 [redacted] .....e@-E
0010 [redacted] ..@,.-|...
0020 [redacted] .....j g(4)Feb
0030 [redacted] 11 13:4 5:59 m44
0040 [redacted] 980CD465 40 kenne
0050 [redacted] 1: [*02/ 11/2025
0060 [redacted] 13:45:59 .1084] R
0070 [redacted] eceived wlcType

```

8. Configuration finale :



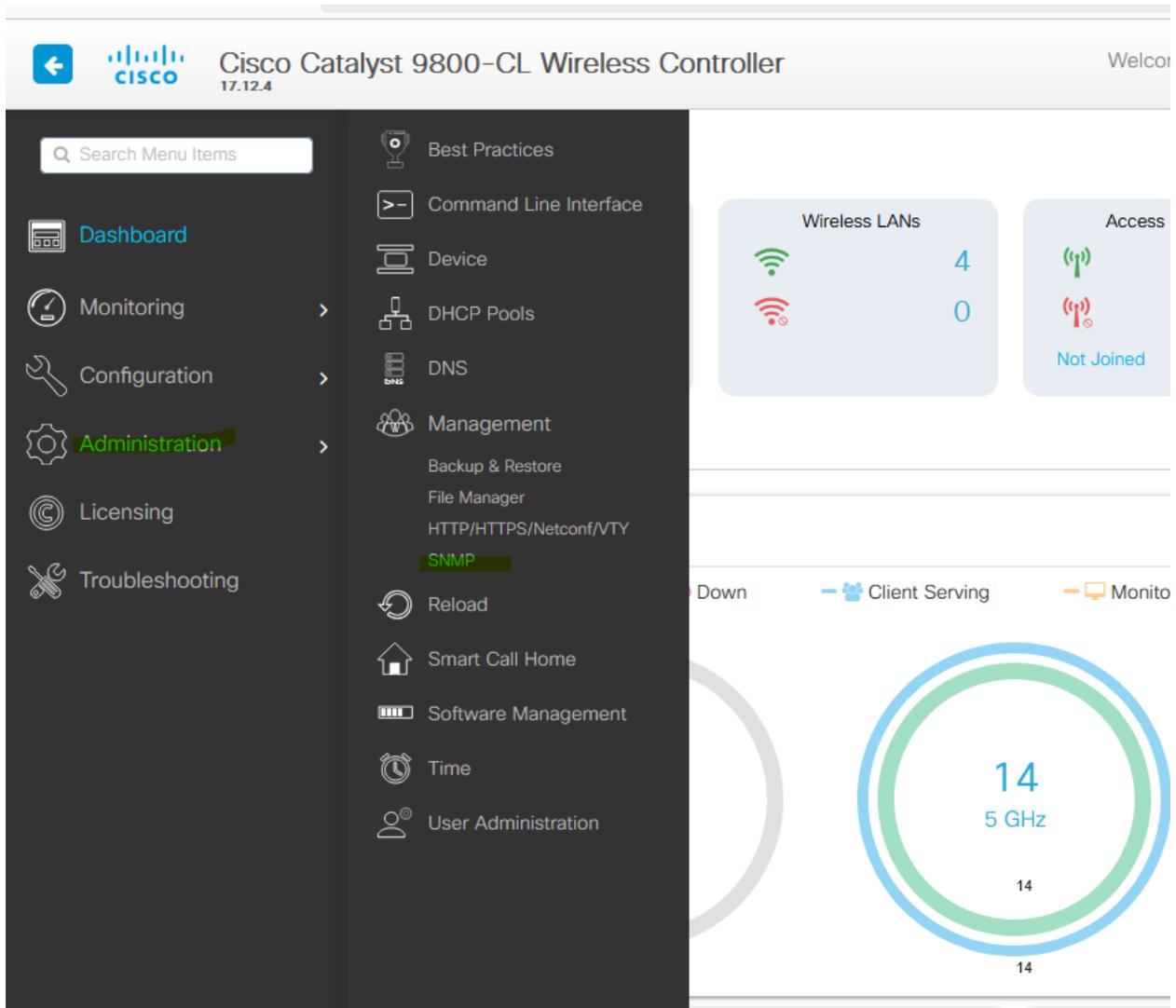
9. Supervision (Zabbix & Nagios)

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

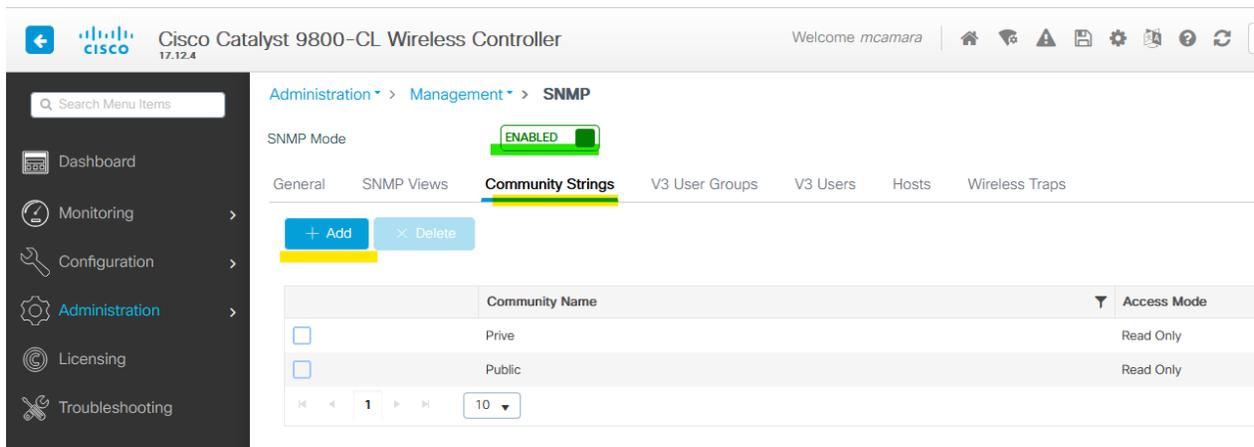
A. Agent SNMP (Contrôleur Catalyst 9800 CL)

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

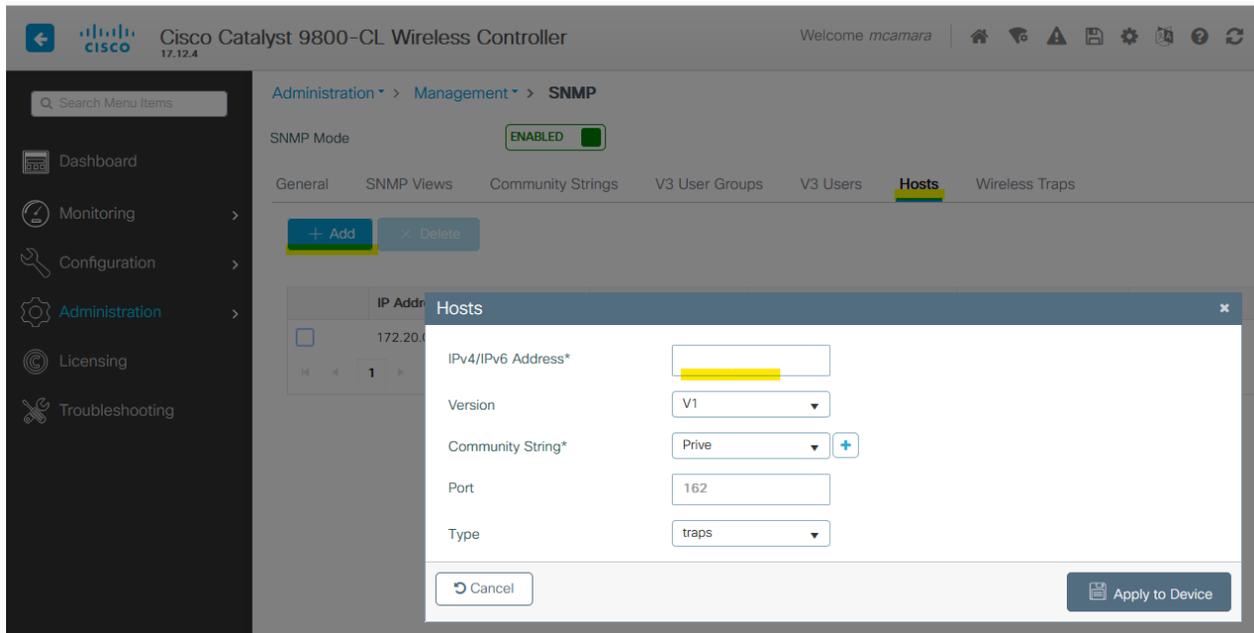
Aller dans **Administration>SNMP**



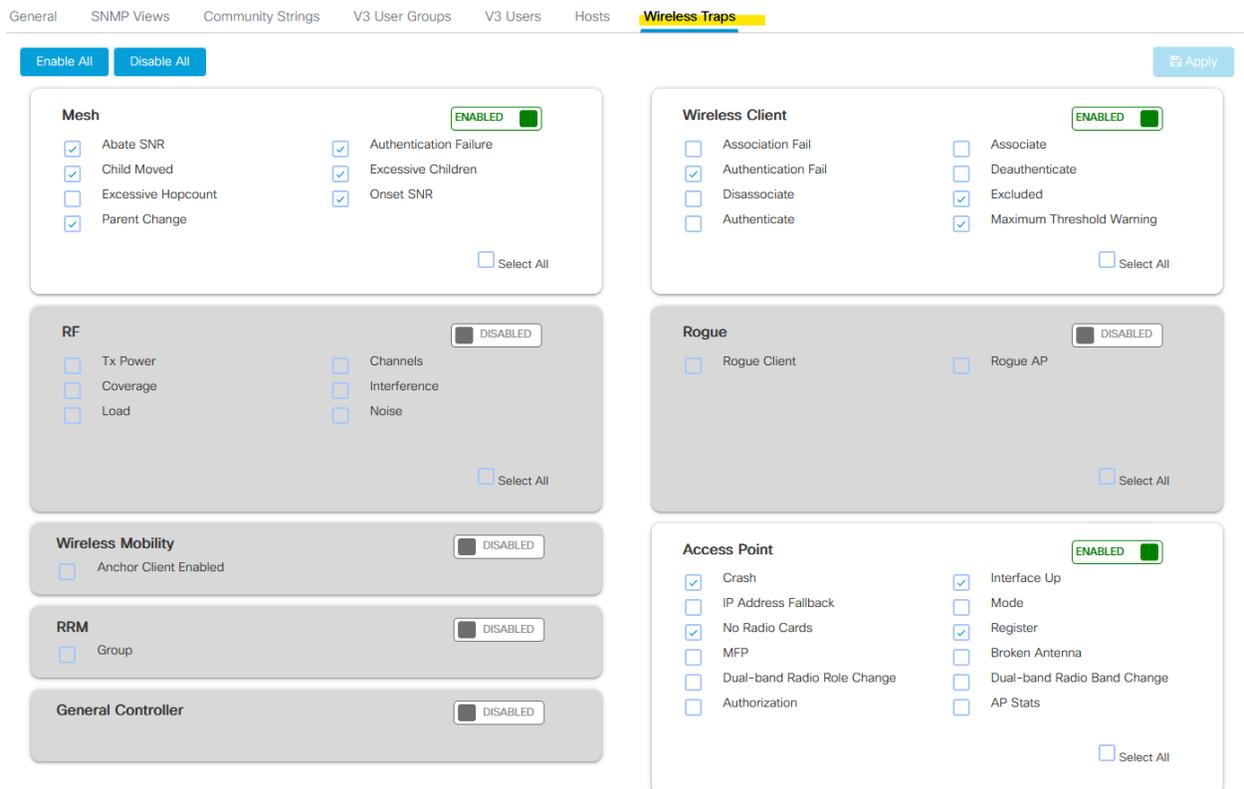
Ensuite dans la section **Community Strings**, on ajoute le deux communautés (Privée et Public)



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



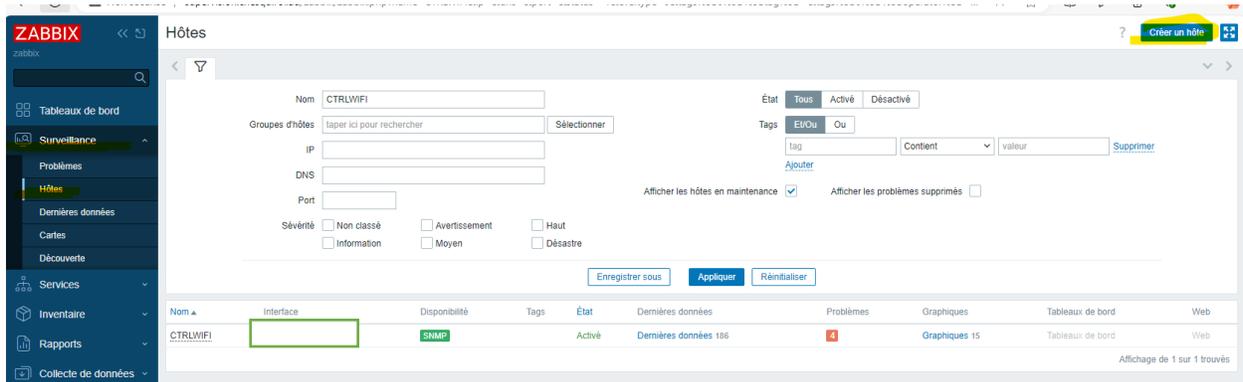
Enfin, dans la partie **Wireless Traps**, on active les informations que l'on veut collecter



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**

Hôte ? >

Hôte | IPMI | Tags | Macros 1 | Inventaire ● | Chiffrement | Table de correspondance

* Nom de l'hôte: CTRLWIFI

Nom visible: CTRLWIFI

Modèles: Nom: Network_Cisco_WiFi_WLC | Action: Supprimer lien | Supprimer lien et nettoyer

* Groupes d'hôtes: Linux servers x

Interfaces:

Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
SNMP			IP DNS	161	Supprimer

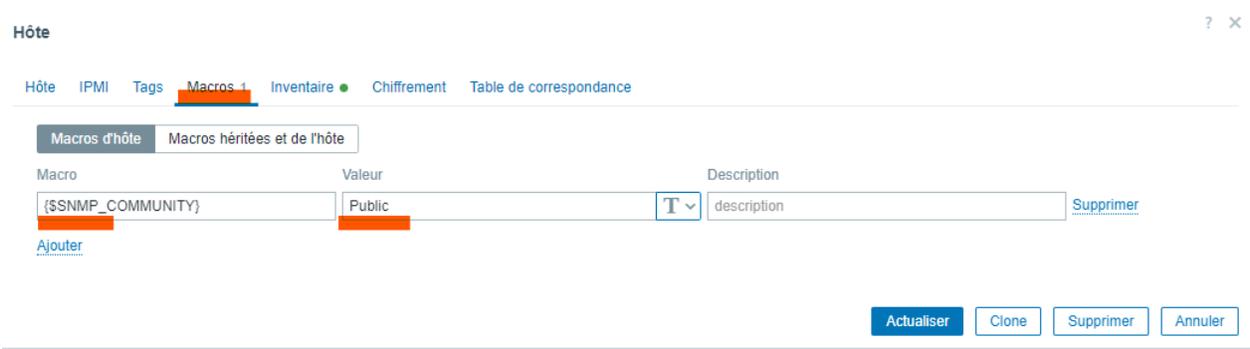
Description:

Surveillé par: Serveur | Proxy | Groupe de proxy

Activé:

Actualiser | Clone | Supprimer | Annuler

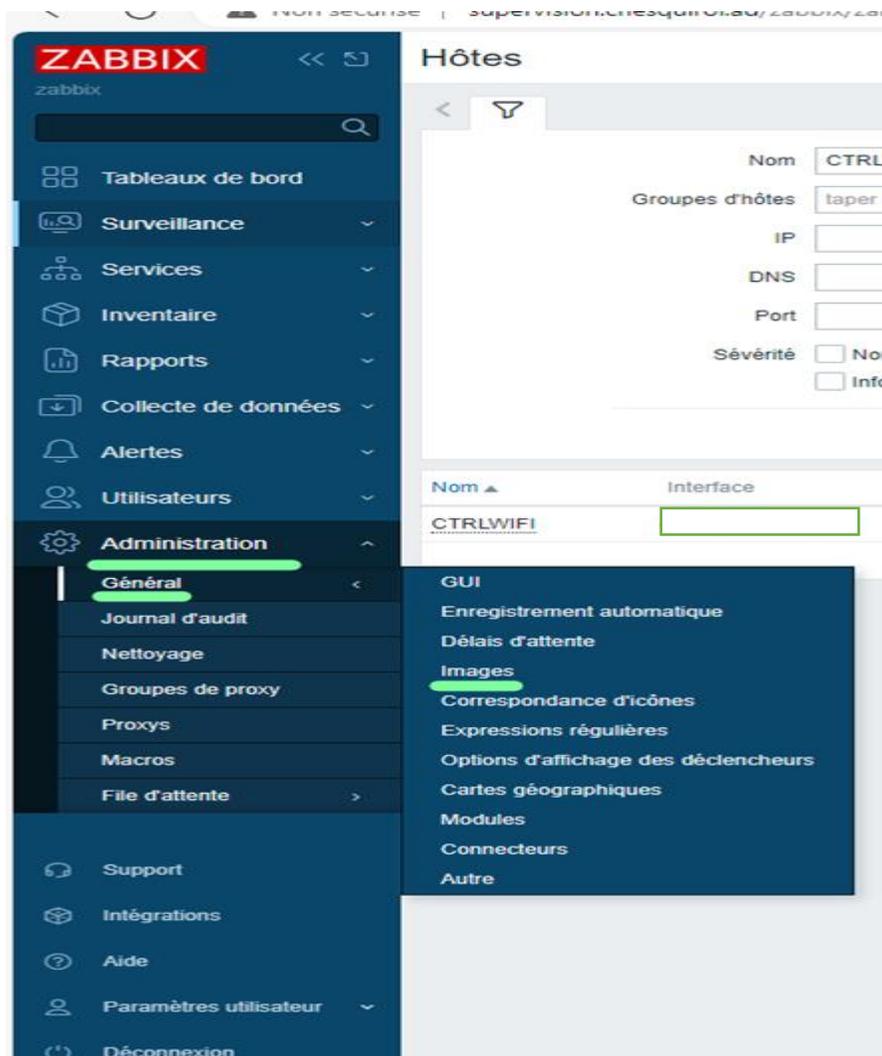
Dans la section **Macro**, on indique la communauté (Public)

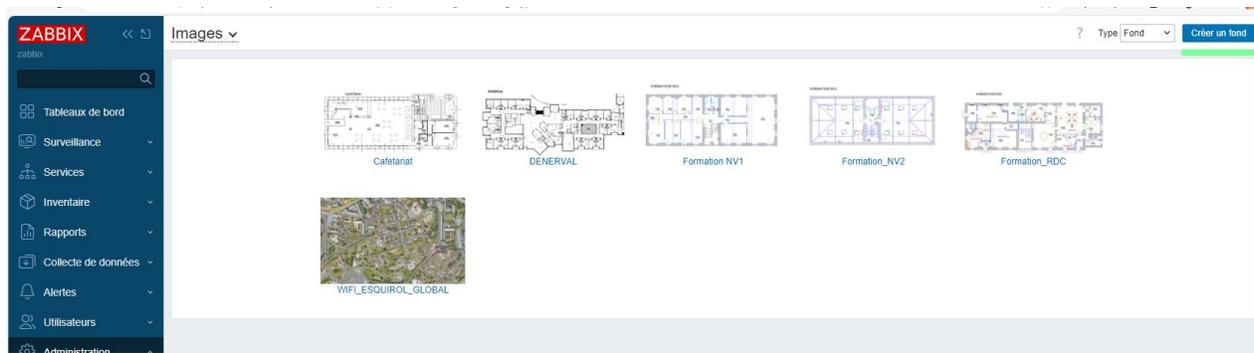


Etape 2 : créer une carte dans Zabbix afin de visualiser l'état des points d'accès (APs)

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.





Images ▾

* Nom

* Télécharger Aucun fichier n'a été sélectionné

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**

Nom	Largeur	Hauteur	Actions
<input type="checkbox"/> Cafetariat	747	328	Propriétés Édition
<input type="checkbox"/> DE NERVAL	1142	544	Propriétés Édition
<input type="checkbox"/> ESQUIROL_WIFI	1600	900	Propriétés Édition
<input type="checkbox"/> Formation_NV1	1445	737	Propriétés Édition
<input type="checkbox"/> Formation_NV2	1525	739	Propriétés Édition
<input type="checkbox"/> Formation_RDC	1576	724	Propriétés Édition
<input type="checkbox"/> Local network	680	200	Propriétés Édition

0 sélectionné Exporter Supprimer

Affichage de 7 sur 7 trouvés

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

Cartes réseau

Carte [Partage](#)

* Propriétaire Sélectionner

* Nom

* Largeur

* Hauteur

Image de fond

Correspondance d'icône automatique [afficher les correspondances d'icônes](#)

Icône surlignée

Marquer les éléments lors de changement de l'état du déclencheur

Afficher les problèmes

Étiquettes avancées

Type d'étiquette de l'élément de carte

Emplacement de l'étiquette de l'élément de carte

Affichage des problèmes

Sévérité minimale

Afficher les problèmes supprimés

Nom	URL	Élément	Action
<input type="text"/>	<input type="text"/>	Hôte	Supprimer

[Ajouter](#)

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

Cartes

Nom

<input type="checkbox"/> Nom ▲	Largeur	Hauteur	Actions
<input type="checkbox"/> Cafetariat	747	328	Propriétés Édition
<input type="checkbox"/> DE NERVAL	1142	544	Propriétés Édition
<input type="checkbox"/> ESQUIROL_WIFI	1600	900	Propriétés Édition
<input type="checkbox"/> Formation_NV1	1445	737	Propriétés Édition
<input type="checkbox"/> Formation_NV2	1525	739	Propriétés Édition
<input type="checkbox"/> Formation_RDC	1576	724	Propriétés Édition
<input type="checkbox"/> Local network	680	200	Propriétés Édition

0 sélectionné

- 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 icônes représentant l'état (Disponibilité de l'AP (ping ou autre vérification)) pour refléter l'état actuel de chaque AP.

ZABBIX Cartes réseau

Élément de carte: Ajouter / Supprimer Forme: Ajouter / Supprimer Lien: Ajouter / Supprimer Substituer les macros: Inactif Grille: Affiché / Actif 50x50 Aligner les éléments de carte Actualiser

FORMATION RDC

Élément de carte

Type: Déclencheur

Étiquette: AP-FORMATION-2

Positionnement de l'étiquette: Bas

* Déclencheurs

Nom	Action
CTRLWIFI: AP-FORMATION-2: AP Unavailable by ICMP ping	Supprimer

Nouveaux déclencheurs

taper ici pour rechercher Sélectionner

Ajouter

Icônes

Défaut: Borne_Wifi_Ok

Problème: Borne_Wifi_KO

Maintenance: Défaut

Désactivé: Défaut

Coordonnées X: 652 Y: 205

URLs

Nom	URL	Action
		Supprimer

Ajouter

Appliquer Supprimer Fermer

Cartes réseau

Élément de carte: Ajouter / Supprimer Forme: Ajouter / Supprimer Lien: Ajouter / Supprimer Substituer les macros: Inactif Grille: Affiché / Actif 50x50 Aligner les éléments de carte Actualiser

FORMATION RDC

0-CTF-01 (3.40m)

0-CTF-02 (3.01m / 3.59m)

0-CTF-03 (3.01m / 3.59m)

0-CTF-04 (3.01m / 3.59m)

0-CTF-05 (3.01m / 3.59m)

0-CTF-06 (3.01m / 3.59m)

0-CTF-07 (3.01m / 3.59m)

0-CTF-08 (3.01m / 3.59m)

0-CTF-09 (3.01m / 3.59m)

0-CTF-10 (3.01m / 3.59m)

0-CTF-11 (3.01m / 3.59m)

0-CTF-12 (3.01m / 3.59m)

0-CTF-13 (3.01m / 3.59m)

0-CTF-14 (3.01m / 3.59m)

0-CTF-15 (3.01m / 3.59m)

0-CTF-16 (3.01m / 3.59m)

0-CTF-17 (3.01m / 3.59m)

0-CTF-18 (3.01m / 3.59m)

0-CTF-19 (3.01m / 3.59m)

0-CTF-20 (3.01m / 3.59m)

0-CTF-21 (3.01m / 3.59m)

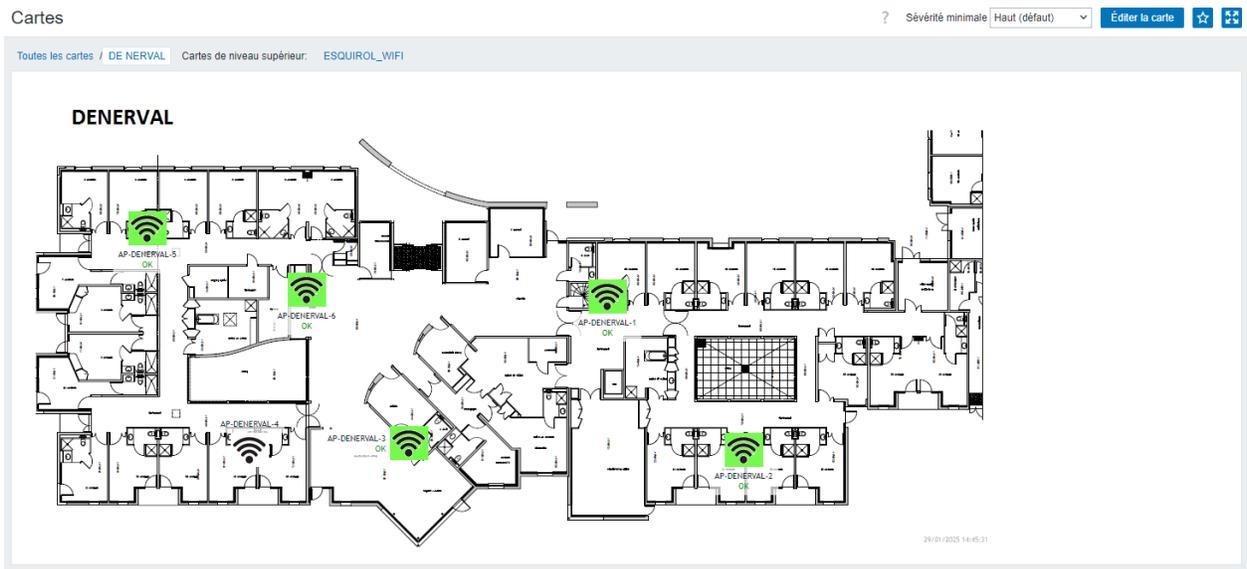
0-CTF-22 (3.01m / 3.59m)

AP-FORMATION-2

AP-FORMATION-1

Installation d'une porte et d'un cloison

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**

Cartes réseau

Carte Partage

* Propriétaire Sélectionner

* Nom

* Largeur

* Hauteur

Image de fond

Correspondance d'icône automatique [afficher les correspondances d'icônes](#)

Icône surlignée

Marquer les éléments lors de changement de l'état du déclencheur

Afficher les problèmes

Étiquettes avancées

Type d'étiquette de l'élément de carte

Emplacement de l'étiquette de l'élément de carte

Affichage des problèmes

Sévérité minimale

Afficher les problèmes supprimés

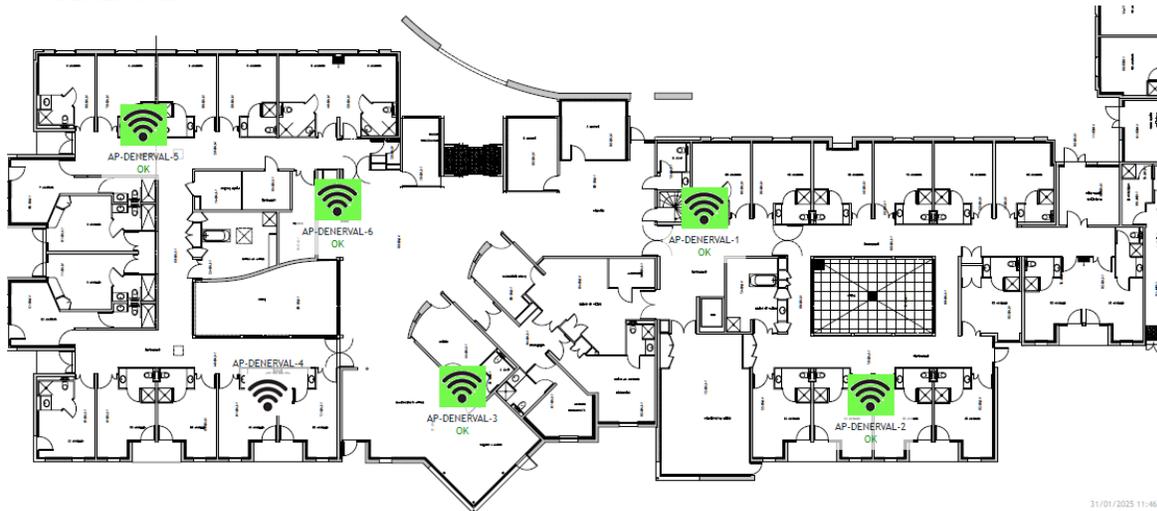
Nom	URL	Élément	Action
<input type="text"/>	<input type="text"/>	Hôte	Supprimer

[Ajouter](#)

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



DENERVAL



31/01/2025 11:40:46