

ACCESS POINT C9115AXE-EWC

Ardy OCKANDJI

CFA PAYS DE MONTBELIARD RUE DES FRERES LUMIERES

Table des matières

Introduction	2
À propos du point d'accès.....	2
1. Prise en main.....	5
Via Console	5
Via Web.....	6
2. Mise à niveau.....	7
Via SSH	7
Via Web.....	9
3. Administration du point d'accès	11
a) Sur le serveur	11
DHCP	
DNS	
RADIUS	
GPO	
b) Sur le point d'accès	16
Paramétrage RADIUS	
Paramétrage des stratégies et profils	
Paramétrage de l'interface sans fil du contrôleur	
4. Ajout d'une borne	23
5. Sauvegarde & restauration	26

Introduction

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

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

Bonne lecture et compréhension.

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

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

Caractéristiques de l'Access point :

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

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

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

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

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

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

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

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

- **Via SSH**

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

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

- **Via le Web**

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

1. General Settings

Country*

Management User Settings

User Name*

Password*

Wireless Management Settings

DHCP ☐

IP Address*

⚠ Please do not change the IP address if you are configuring device for site-survey

Subnet Mask*

Wireless Network

⚠ Please create at least one WLAN

+ Add

- Delete

Network Name	Network Type	Security
<div> <div>⏪</div> <div>⏩</div> <div>0</div> <div>⏪</div> <div>⏩</div> <div>5</div> <div>Items per page</div> </div> <div>No items to display</div>		

Finish

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

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

1. Prise en main (0day configuration)

- 0day via console ou SSH

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

```
WLC7069.5A74.7C78#conf t
```

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

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

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

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

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

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

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

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

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

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

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

```
C9800-AP(config-wlan)# no shutdown
```

```
C9800-AP(config-wlan)#end
```

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

```
C9800-AP#conf t
```

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

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

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

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

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

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

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

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

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

```
C9800-AP#conf t
```

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

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

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

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

C9800-AP#conf t

C9800-AP(config)#service password-encryption

C9800-AP(config)#password encryption aes

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

C9800-AP(config)#end

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

C9800-AP# write memory

- **Via Web**

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

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

1. General Settings

Country*
US

Management User Settings

User Name*
Enter User Name

Password*
Enter password

Wireless Management Settings

DHCP
☐

IP Address*
192.168.1.1

⚠ Please do not change the IP address if you are configuring device for site-survey

Subnet Mask*
255.255.255.0

Wireless Network

⚠ Please create at least one WLAN

Add
Delete

Network Name	Network Type	Security
5 items per page		
No items to display		

Finish

2. Mise à niveau du logiciel

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

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

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

Remarques :

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

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

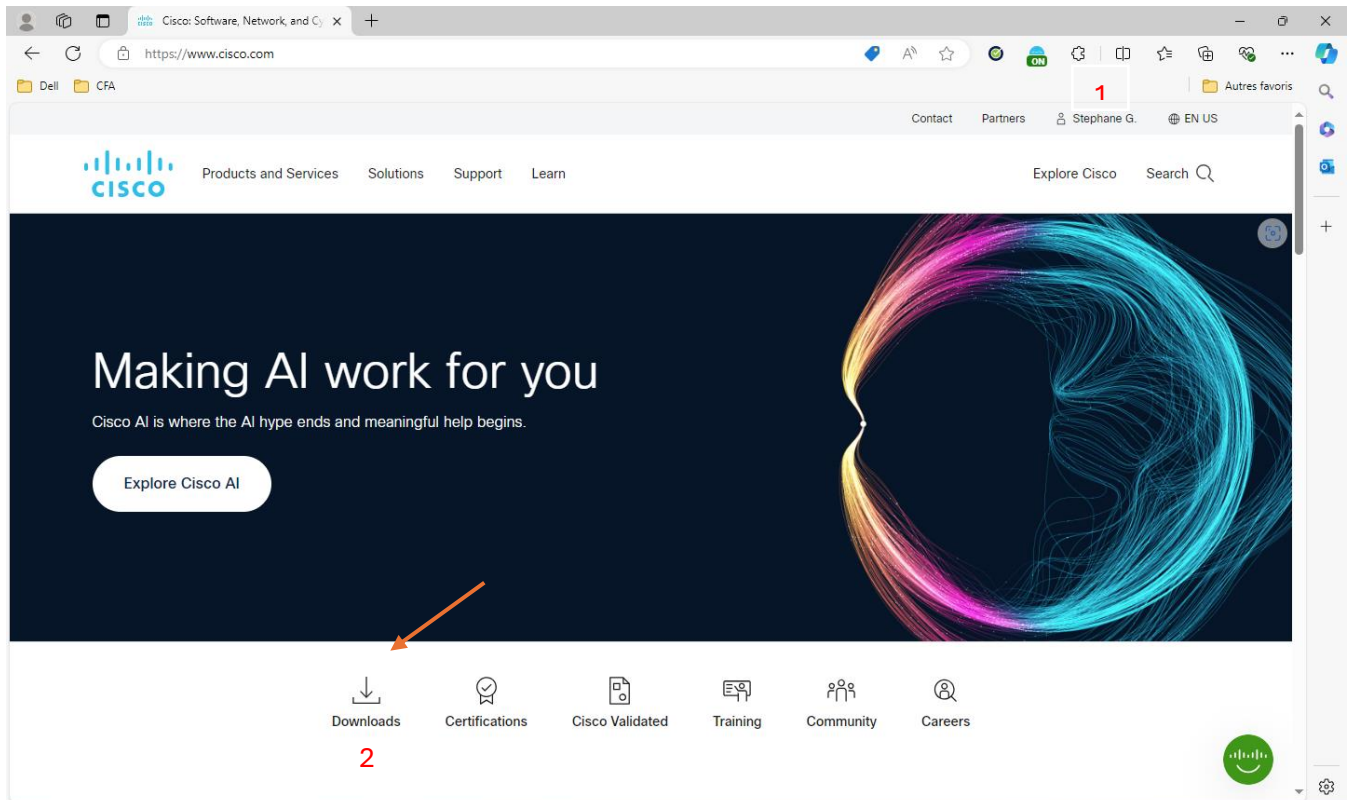
- **Via SSH** (je le mentionne pour information. Les commandes à taper peuvent être retrouvées sur Internet, avec quelques subtilités.)

Cela nécessite :

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

Pour télécharger les images :

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



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

Products & Services Support How to Buy Training & Events Partners

Stephane GAILLOT

Software Download

My Previous Downloads

Product	Software Type	Latest Release	Last Downloaded
Embedded Wireless Controller on Catalyst 9115AX Access Points	Embedded Wireless Controller	17.6.7	17.12.3
Catalyst 9115AXE Access Point	Embedded Wireless Controller	17.6.7	17.9.5

Most Popular

- Secure Client 5
- Identity Services Engine Software
- AnyConnect Secure Mobility Client v4.x
- 3900 Series Integrated Services Routers
- Jabber for Windows
- 4000 Series Integrated Services Routers

Select a Product

Browse all

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

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

Faire la manipulation de la partie [SSH](#)

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

- **Via le Web**

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

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

edded Wireless Controller on Catalyst Access Points

Welcome admin
Last login NA ...

Administration > Software Management

Software Upgrade

Mode
Desktop (HTTP)

Controller Image*
Select File
Required image is C9800-AP-iosxe-wlc.bin*

AP Image*
Select File
Required AP image is ap1g7*

SaveSave & DownloadActivateCancel

Software Upgrade Status

InitiateWLC Image DownloadAP Image DownloadNetwork UpgradeActivateReload

Status
Show Install Logs >>

Total number of APs
Initiated
Predownloading AP Image
Predownloading Controller Image
Completed predownloading AP Image
Completed predownloading Controller Image
Failed to predownload AP Image
Failed to predownload Controller Image

None
1 (CAPWAP:0, EWC Capable:1)
0
0
0
0
0
0
0

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

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

10

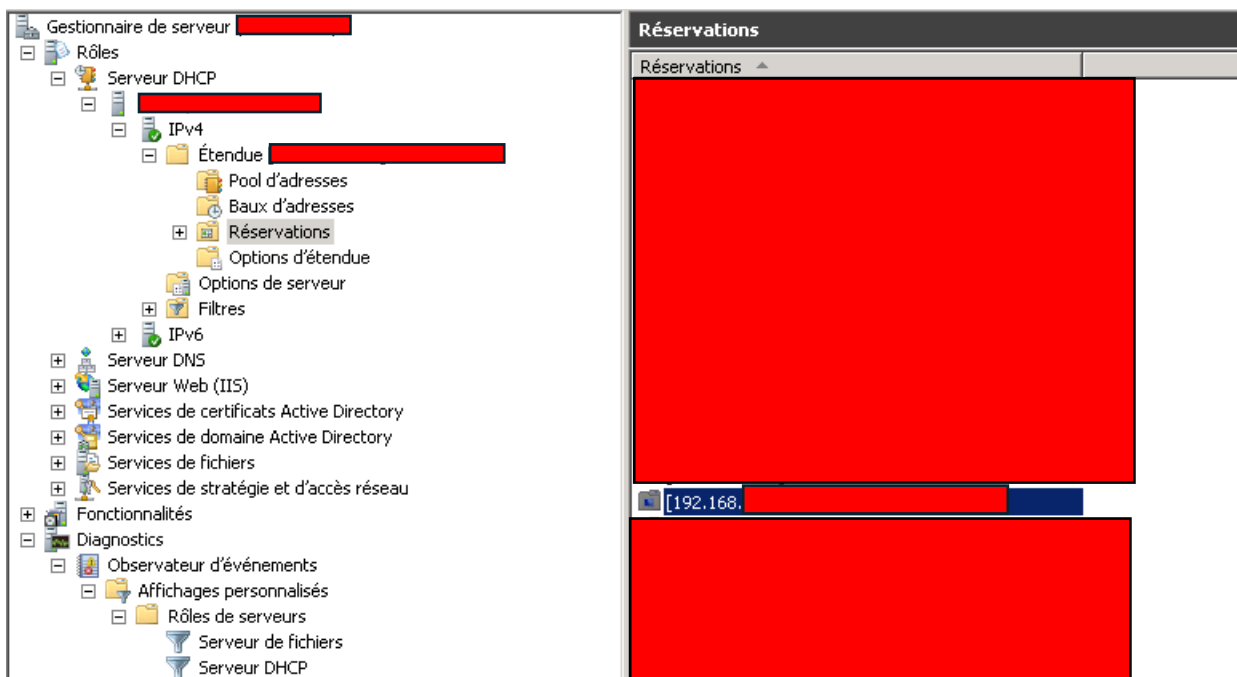
3. Administration du point d'accès

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

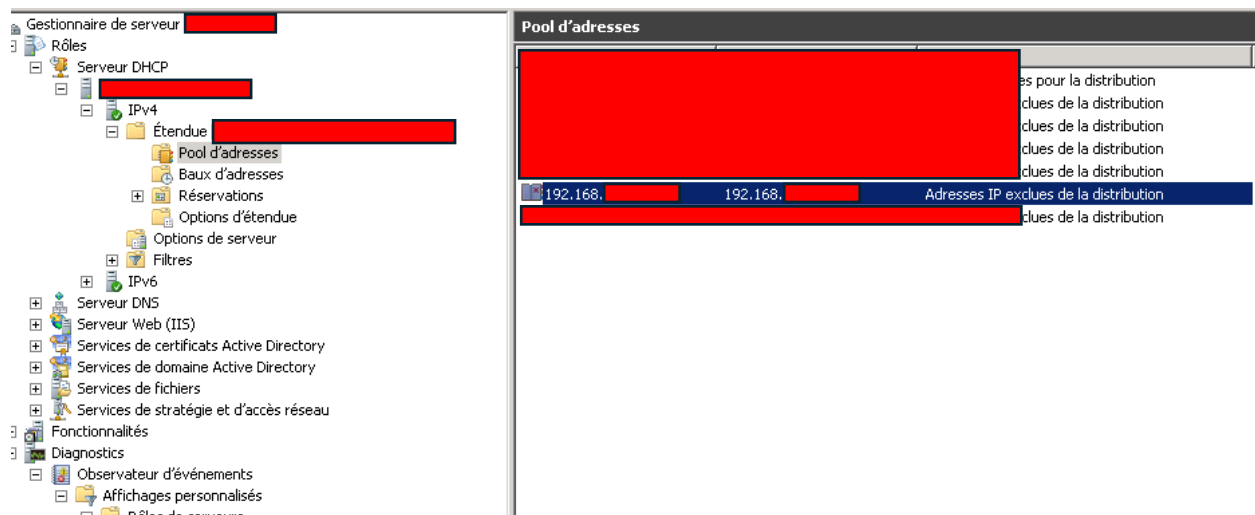
a) Sur le serveur

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

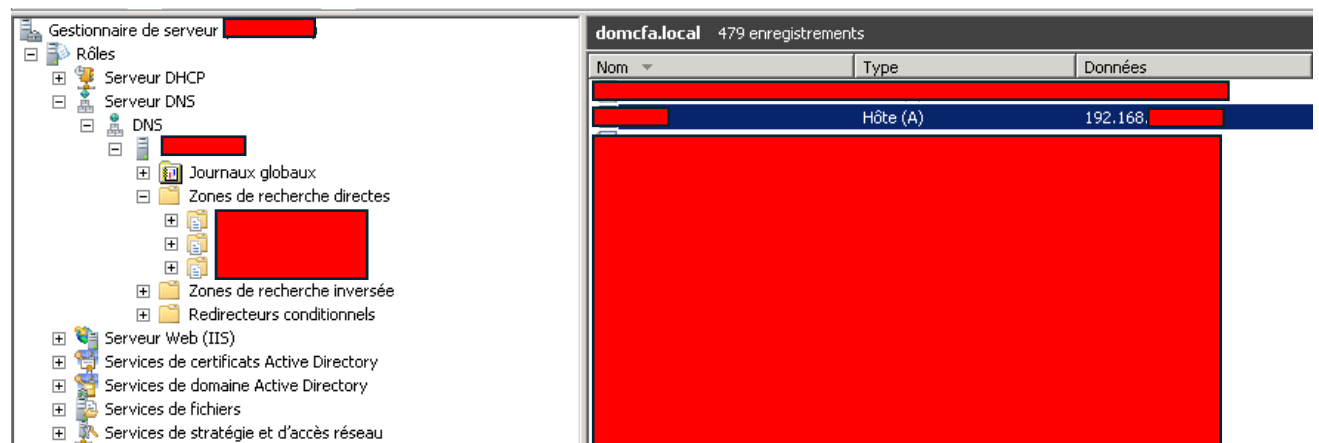
Réservation d'adresse



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



Enregistrement DNS



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

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

Client RADIUS

The screenshot shows the Windows Server Management console on the left, with the 'Clients RADIUS' configuration window open on the right. The window title is 'Propriétés de C9800-EWC'. It has two tabs: 'Paramètres' (selected) and 'Avancé'. The 'Paramètres' tab contains the following fields:

- ☒ Activer ce client RADIUS
- ☐ Sélectionner un modèle existant :
- Nom et adresse:
 - Nom convivial: [redacted]
 - Adresse (IP ou DNS): 192.168 [redacted] [Vérifier...]
- Secret partagé:
 - Sélectionnez un modèle de secrets partagés existant : Aucun
 - Manuel (selected) / Générer
 - Secret partagé : [redacted]
 - Confirmez le secret partagé : [redacted]

Buttons at the bottom: OK, Annuler, Appliquer.

Stratégie de demande de connexion

The screenshot shows the Windows Server Management console on the left, with the 'Stratégies de demande de connexion' configuration window open on the right. The window title is 'Stratégies de demande de connexion'. It contains a list of connection request policies and a detailed view for the 'dot1x-wireless' policy.

Nom de la stratégie	État	Ordre de traitement	Source
dot1x-wireless	Activé	1	Unspecified
Use Windows authentication for all users	Désactivé	2	Unspecified

Below the table, the 'dot1x-wireless' policy is selected, showing its conditions and parameters.

Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur
Type de port NAS	Wireless - IEEE 802.11

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur
Fournisseur d'authentification	Ordinateur local
Remplacer l'authentification	Désactivé

Stratégie réseau

Gestionnaire de serveur ([REDACTED])

- Rôles
 - Serveur DHCP
 - Serveur DNS
 - Serveur Web (IIS)
 - Services de certificats Active Directory
 - Services de domaine Active Directory
 - Services de fichiers
 - Services de stratégie et d'accès réseau
 - NPS (Local)
 - Clients et serveurs RADIUS
 - Clients RADIUS
 - Groupes de serveurs RADIUS distants
 - Stratégies
 - Stratégies de demande de connexion
 - Stratégies réseau
 - Stratégies de contrôle d'intégrité
 - Protection d'accès réseau
 - Gestion
 - Gestion des modèles
- Fonctionnalités
- Diagnostics
 - Observateur d'événements
 - Affichages personnalisés
 - Rôles de serveurs
 - Serveur de fichiers
 - Serveur DHCP
 - Serveur DNS
 - Serveur Web (IIS)
 - Services de certificats Active Directory
 - Services de domaine Active Directory
 - Services de stratégie et d'accès réseau
 - Événements d'administration
 - Microsoft Exchange with Database Availability Group Event
 - Journaux Windows
 - Journaux des applications et des services
 - Abonnements
 - Performance
 - Gestionnaire de périphériques
 - Configuration
 - Stockage

Stratégies réseau

Les stratégies réseau vous permettent d'autoriser les connexions au réseau de manière sélective, et d'indiquer les circonstances dans lesquelles les connexions peuvent s'effectuer ou non.

Nom de la stratégie	État	Ordre de traitement	Type d'accès	Source
dot1x-wireless	Activé	1	Accorder l'accès	Unspecified
Connections to Microsoft Routing and Remote Access server	Désactivé	2	Refuser l'accès	Unspecified
Connections to other access servers	Désactivé	3	Refuser l'accès	Unspecified

dot1x-wireless

Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur
Groupes Windows	DOMCFA\dot1x

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur
État étendu	<Vide>
Autorisation d'accès	Accorder l'accès
Méthode EAP (Extensible Authentication Protocol)	Microsoft: PEAP (Protected EAP) OU Microsoft: Mot de passe sécurisé (EAP-MSCHAP version 2)
Méthode d'authentification	Protocole EAP OU Authentification avec chiffrement (CHAP) OU MS-CHAP v1 OU MS-CHAP v2
Contrainte de mise en conformité NAP	Autoriser un accès réseau limité
Mettre à jour les clients non conformes	Vrai
Framed-Protocol	PPP
Délai d'inactivité	1 minutes
Service-Type	Framed
Délai d'expiration de session	80 minutes
Pourcentage de capacité du protocole BAP	Réduisez les liaisons multiples si le serveur atteint 50% pour 2 minutes

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

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

Gestionnaire de serveur ([REDACTED])

- Rôles
 - Serveur DHCP
 - Serveur DNS
 - Serveur Web (IIS)
 - Services de certificats Active Directory
 - Services de domaine Active Directory
 - Services de fichiers
 - Services de stratégie et d'accès réseau
 - NPS (Local)
 - Clients et serveurs RADIUS
 - Clients RADIUS
 - Groupes de serveurs RADIUS distants
 - Stratégies
 - Stratégies de demande de connexion
 - Stratégies réseau
 - Stratégies de contrôle d'intégrité
 - Protection d'accès réseau
 - Gestion
 - Gestion des modèles
 - Fonctionnalités
 - Diagnostics
 - Observateur d'événements
 - Affichages personnalisés
 - Rôles de serveurs
 - Serveur de fichiers
 - Serveur DHCP
 - Serveur DNS
 - Serveur Web (IIS)
 - Services de certificats Active Directory
 - Services de domaine Active Directory
 - Services de stratégie et d'accès réseau
 - Événements d'administration
 - Microsoft Exchange with Database Availability Group Event
 - Journaux Windows
 - Journaux des applications et des services
 - Abonnements
 - Performance
 - Gestionnaire de périphériques
 - Configuration
 - Stockage

Services de stratégie et d'accès réseau

Nombre d'événements : 66

Nombre d'événements : 66

Niveau	Date et heure	Source
Information	29/07/2024 14:46:09	NPS
Information	26/07/2024 14:46:44	NPS
Information	24/07/2024 08:28:14	NPS
Information	22/07/2024 14:21:59	NPS
Information	22/07/2024 07:57:58	NPS
Information	19/07/2024 11:20:41	NPS
Information	18/07/2024 11:07:58	NPS
Information	18/07/2024 08:39:31	NPS
Information	18/07/2024 08:14:19	NPS

Événement 4400, NPS

Général | Détails

La connexion LDAP avec le contrôleur de domaine SRVCFAPR1.domcfa.local pour le domaine DOMCFA est établie.

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

Utilisateurs et ordinateurs Active Directory	Nom	Type	Description
Requêtes enregistrées		Utilisateur	Dedicated User to run VMware Converter Standalone serv.
Builtin		Utilisateur	
Computers		Groupe de sécurité - Universel	Administrateurs désignés de l'entreprise
defaultMigrationContainer30		Groupe de sécurité - Domaine local	Les membres qui ont un accès d'administrateur au service ..
Domain Controllers		Groupe de sécurité - Universel	Administrateurs désignés du schéma
ForeignSecurityPrincipals		Groupe de sécurité - Domaine local	Les administrateurs WSUS peuvent gérer le serveur Windo.
		Groupe de sécurité - Global	Administrateurs désignés du domaine
		Utilisateur	
LostAndFound		Utilisateur	Compte utilisé pour exécuter le processus de traitement A..
Managed Service Accounts		Utilisateur	
Microsoft Exchange Security Groups		Contact	
Program Data		Groupe de sécurité - Global	Tous les contrôleurs de domaine du domaine
Serveur_NIS		Groupe de sécurité - Universel	Les membres de ce groupe sont des contrôleurs de domain.
Service_NIS		Groupe de sécurité - Global	Les membres de ce groupe sont des contrôleurs de domain.
System		Utilisateur	
Users		Groupe de sécurité - Domaine local	Groupe des administrateurs DNS
Microsoft Exchange System Objects	dot1x	Groupe de sécurité - Global	Les clients DNS qui sont autorisés à effectuer des mises à j.
NTDS Quotas		Groupe de sécurité - Domaine local	Groupe contenant les utilisateurs autorisés à accéder au r..
		Utilisateur	Les membres de ce groupe ont l'autorisation de publier des.
		Contact	
		Utilisateur	

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

Gestion de stratégie de groupe	dot1x
Forêt :	dot1x
Domaines	
Default Domain Policy	
dot1x	
Domain Controllers	
Microsoft Exchange Security Groups	
Serveur_NIS	
Service_NIS	
Objets de stratégie de groupe	
Filtres WMI	
Objets GPO Starter	
Sites	
Modélisation de stratégie de groupe	
Résultats de stratégie de groupe	

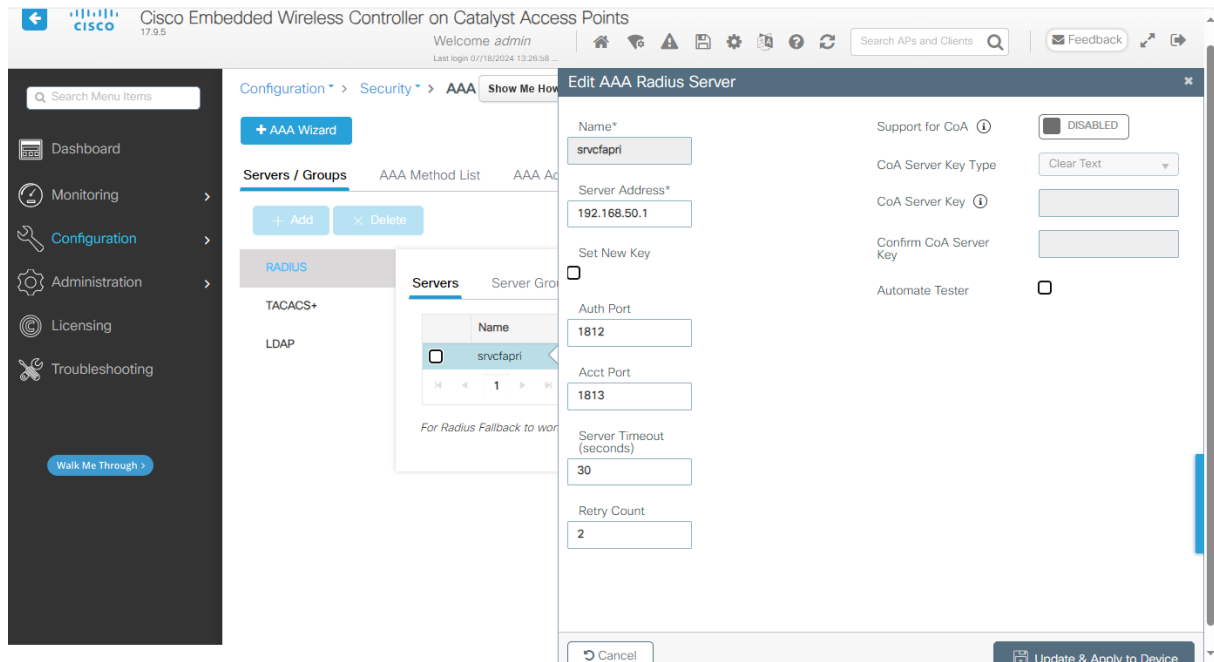
dot1x	
Données recueillies le : 30/07/2024 10:40:24	
Configuration ordinateur (activée)	
Stratégies	
Paramètres Windows	
Paramètres de sécurité	
Stratégie locale/ Stratégie d'audit	
Stratégie	Paramètre
Auditer l'accès au service d'annuaire	Succès, Échec
Auditer l'utilisation des privilèges	Succès, Échec
Auditer les événements de connexion	Succès, Échec
Auditer les événements de connexion aux comptes	Succès, Échec
Stratégies de réseau sans fil (802.11)	
dot1x	
Nom de la stratégie	dot1x
Description de stratégie	connexion auto wifi via radius
Type de stratégie	Windows Vista et éditions ultérieures
Paramètres globaux	
Utiliser les services réseau LAN sans fil Windows pour les clients	Activé
Informations d'identification partagées pour l'authentification réseau	Activé
Réseaux hébergés	Activé
Autoriser l'utilisateur à afficher les réseaux refusés	Désactivé
Autoriser tout le monde à créer tous les profils utilisateur	Désactivé
Utiliser uniquement des profils de stratégie de groupe pour les réseaux autorisés	Désactivé
Filtres réseau	
Empêcher la connexion aux réseaux à infrastructure	Désactivé
Empêcher la connexion aux réseaux ad hoc	Activé
Réseaux autorisés	
Nom réseau (SSID)	Type de réseau
	Infrastructure

b) Sur le point d'accès

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

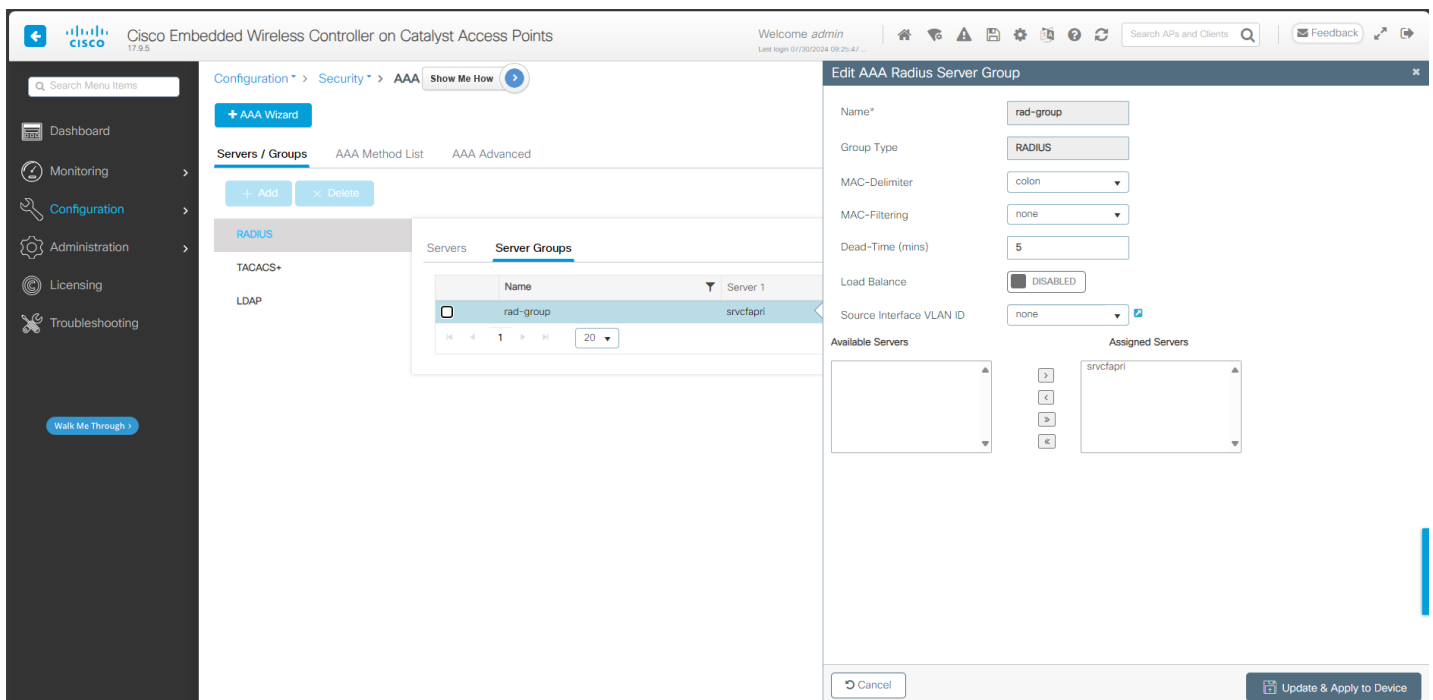
Sur le point d'accès, j'ai essentiellement configuré les informations du serveur RADIUS avec les options qui correspondent (Authentification, Autorisation et Traçabilité).

Serveur RADIUS



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

Groupe de serveurs RADIUS



Sélectionnez le serveur RADIUS configuré en amont.

Paramètres pour l'Authentification

The screenshot shows the 'Quick Setup: AAA Authentication' dialog box. The 'Method List Name*' field is set to 'rad'. The 'Type*' dropdown is set to 'dot1x'. The 'Group Type' dropdown is set to 'group'. The 'Fallback to local' checkbox is checked. The 'Available Server Groups' list contains 'ldap', 'tacacs+', and 'rad'. The 'Assigned Server Groups' list contains 'radius'. The 'Update & Apply to Device' button is visible at the bottom right.

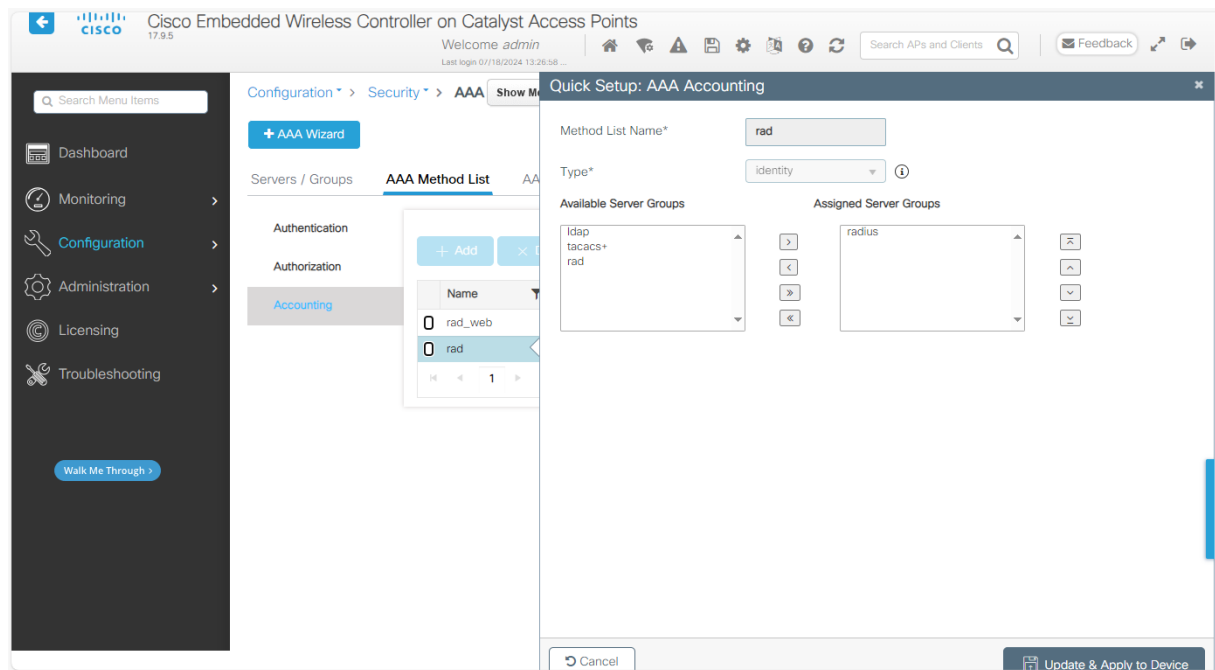
Donnez un nom bien explicite. Ensuite pour le type « **dot1x** » et pour le type de groupe, choisir « **group** ». Cochez la case « **Fallback to local** » et sélectionnez le groupe de serveurs RADIUS créé en amont.

Paramètres pour l'Autorisation

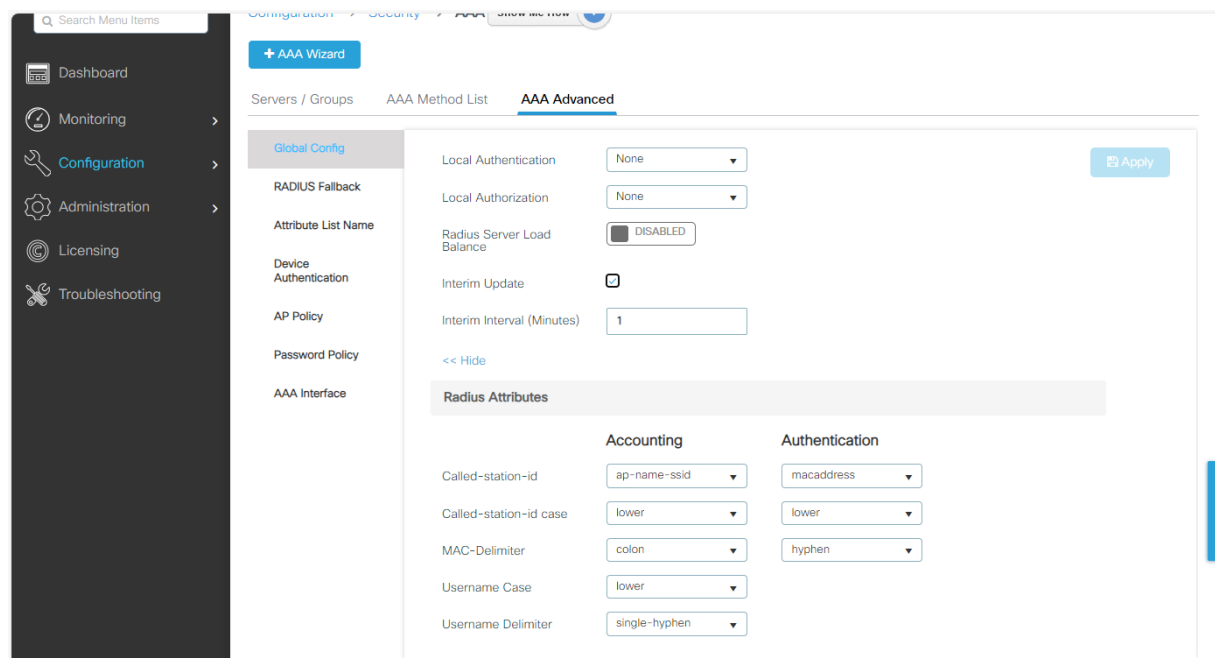
The screenshot shows the 'Quick Setup: AAA Authorization' dialog box. The 'Method List Name*' field is set to 'rad'. The 'Type*' dropdown is set to 'network'. The 'Group Type' dropdown is set to 'group'. The 'Fallback to local' checkbox is checked. The 'Authenticated' checkbox is unchecked. The 'Available Server Groups' list contains 'ldap', 'tacacs+', and 'rad'. The 'Assigned Server Groups' list contains 'radius'. The 'Update & Apply to Device' button is visible at the bottom right.

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

Paramètres pour la Traçabilité.



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



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

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

Profil à joindre par les APs.

The screenshot shows the Cisco Embedded Wireless Controller interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Edit AP Join Profile' and has tabs for General, Client, CAPWAP, AP, Management, Security, ICap, and QoS. The 'General' tab is active, showing fields for Name* (cfa-ap-profile), Description (cfa-ap-profile), Country Code (FR), Time Zone (Use-Controller), LED State (checked), LAG Mode (unchecked), NTP Server (0.0.0.0), GAS AP Rate Limit (unchecked), USB Enable (unchecked), Apphost (unchecked), and Fallback to DHCP (checked). On the right, there are sections for 'OfficeExtend AP Configuration' (Local Access, Link Encryption, Rogue Detection, Provisioning SSID) and 'Antenna Monitoring' (Antenna Monitoring, RSSI Fail Threshold, Weak RSSI, Detection Time). The bottom right has a button 'Update & Apply to Device'.

Profil « Flex »

The screenshot shows the Cisco Embedded Wireless Controller interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Edit Flex Profile' and has tabs for General, Local Authentication, Policy ACL, VLAN, and DNS Layer Security. The 'General' tab is active, showing fields for Name* (cfa-flex-profile), Description (cfa-flex-profile), Native VLAN ID (1), HTTP Proxy Port (80), and HTTP-Proxy IP Address (192.168.50.254). On the right, there are sections for 'Fallback Radio Shut' (checked), 'ARP Caching' (checked), 'Join Minimum Latency' (unchecked), 'IP Overlap' (checked), 'mDNS Flex Profile' (Search or Select), and 'PMK Propagation' (checked). The bottom right has a button 'Update & Apply to Device'.

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

Profil de stratégie.

The screenshot displays the Cisco Embedded Wireless Controller configuration interface. The main window is titled 'Edit Policy Profile' and shows a configuration for a policy profile named 'cfa-policy-profile'. The interface includes a sidebar with navigation options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is divided into tabs: General, Access Policies, QOS and AVC, and Advanced. The 'General' tab is active, showing fields for Name, Description, Status, Passive Client, IP MAC Binding, and Encrypted Traffic Analytics. The 'WLAN Switching Policy' section is also visible, showing 'Central Authentication' as 'ENABLED' and 'Flex NAT/PAT' as 'DISABLED'. A warning message at the top states: 'Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.'

Field	Value
Name*	cfa-policy-profile
Description	cfa-policy-profile
Status	ENABLED
Passive Client	DISABLED
IP MAC Binding	ENABLED
Encrypted Traffic Analytics	DISABLED
Central Authentication	ENABLED
Flex NAT/PAT	DISABLED

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

Configuration d'un réseau sans fil

The screenshot shows the Cisco Embedded Wireless Controller interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Edit WLAN' and displays a configuration form for a WLAN named 'CFA-A2'. The form includes fields for Profile Name, SSID, WLAN ID, Status, and Broadcast SSID. The 'Status' field is set to 'ENABLED'. The 'Radio Policy' section shows the 5 GHz band is enabled and the 2.4 GHz band is also enabled. The 'WLAN ID' is set to 2. The 'Broadcast SSID' is set to 'ENABLED'. A warning message at the top states: 'Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.' The bottom of the form has 'Cancel' and 'Update & Apply to Device' buttons.

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

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

The screenshot shows the Cisco Embedded Wireless Controller interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Edit Policy Tag' and displays a configuration form for a policy tag named 'cfa-policy-tag'. The form includes fields for Name, Description, and a section for 'WLAN-POLICY Maps'. The 'WLAN-POLICY Maps' section shows two maps: 'CFA-A1' and 'CFA-A2', both associated with the 'cfa-policy-profile'. The 'WLAN-POLICY Maps' section has a '+ Add' and '- Delete' button. The bottom of the form has 'Cancel' and 'Update & Apply to Device' buttons.

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

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

On :

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

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

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

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

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

[Voir ici.](#)

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

The screenshot shows the Cisco Embedded Wireless Controller interface. The top navigation bar includes the Cisco logo, version 16.12.4a, and a welcome message for 'admin'. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration (selected), and Troubleshooting. The main content area is titled 'Administration > DHCP Pools'. It features a 'Pools' tab and a 'DHCP Persistence' section. Below these are '+ Add' and 'x Delete' buttons. A table lists the DHCP pools with columns: Pool Name, Network/Subnet Mask, Reserved Only, and IP Type. The table contains one entry: 'default-pool' with Network/Subnet Mask '192.168.1.0/255.255.255.0', Reserved Only 'Disable', and IP Type 'ipv4'. At the bottom of the table, it indicates '1 - 1 of 1 items'.

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

The screenshot shows the Cisco Embedded Wireless Controller interface. The top navigation bar includes the Cisco logo, version 17.9.5, and a welcome message for 'admin'. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, Administration (selected), Licensing, and Troubleshooting. The main content area is titled 'Administration > DNS'. It features a 'DNS Loopback' section with a green 'ENABLED' status indicator. Below this are '+ Add' and 'x Delete' buttons. A table lists the DNS entries with columns: IP Address. The table contains one entry: '192.168.50.1'. At the bottom of the table, it indicates '1 - 1 of 1 items'.

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

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

The screenshot shows the Cisco Embedded Wireless Controller interface. The top navigation bar includes the Cisco logo, version 17.9.5, and a welcome message for 'admin'. The main navigation menu on the left includes Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The 'Configuration' menu is expanded, showing 'Wireless' > 'Access Points'. The 'All Access Points' section displays three status boxes: 'Current Active' (C9800-EWC), 'Current Standby' (Not Applicable), and 'Preferred Active' (C9800-EWC). Below these, there are buttons for 'Convert to EWC' and 'Convert to CAPWAP'. A table lists the access points, with the 'Image Type' column highlighted in red for the 'AP-B2' entry, showing 'CAPWAP'. The table also includes columns for AP Name, AP Model, EWC Capable, Slots, Admin Status, Up Time, IP Address, Base Radio MAC, Ethernet MAC, AP Mode, and Power Derate Capable. Below the table, there are sections for 5 GHz Radios, 2.4 GHz Radios, Dual-Band Radios, Country, and LSC Provision.

AP Name	AP Model	EWC Capable	Image Type	Slots	Admin Status	Up Time	IP Address	Base Radio MAC	Ethernet MAC	AP Mode	Power Derate Capable	On St
AP-B2	C9115AXE-E	Yes	CAPWAP	2	✓	0 days 22 hrs 28 mins 35 secs	192.168.50.50	087b.8775.f000	6871.61a0.7fc4	Flex	Yes	Re
C9800-EWC	C9115AXE-E	Yes (Internal)	EWC	2	✓	2 days 1 hrs 8 mins 26 secs	192.168.50.10	087b.8776.ba00	6871.61a0.9764	Flex	Yes	Re

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

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

ent Active
800-EWC

Image Type	Slots
CAPWAP	2
EWC	2

Current Active
C9800-EWC

EWC Capable	Image Type	Slots
Yes	CAPWAP	2
Yes (Internal)	EWC	2

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

The screenshot shows the Cisco Embedded Wireless Controller (EWC) web interface. The top header displays the Cisco logo, version 17.9.5, and the title 'Cisco Embedded Wireless Controller on Catalyst Access Points'. The user is logged in as 'admin'. The navigation menu on the left includes Dashboard, Monitoring, Configuration, Administration (selected), Licensing, and Troubleshooting. The main content area is titled 'Backup & Restore' and contains a 'Config File Management' section. This section has three dropdown menus: 'Copy' (set to 'To Device'), 'File Type' (set to 'Configuration'), and 'Transfer Mode' (set to 'TFTP'). Below these is a checkbox for 'Backup existing startup config to flash?' with 'Yes' selected. The 'Server Details' section includes input fields for 'IP Address (IPv4/IPv6)*', 'File Path' (containing '/'), and 'File Name*'. At the bottom are 'Download File' and 'Reload' buttons.

Cisco Embedded Wireless Controller on Catalyst Access Points 17.9.5

Welcome admin
Last login N/A ...

Search Menu Items

Administration > Management > Backup & Restore

Config File Management

Copy To Device

File Type Configuration

Transfer Mode TFTP

Backup existing startup config to flash? ☒ Yes ☐ No

Server Details

IP Address (IPv4/IPv6)*

File Path /

File Name*

Download File Reload

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

BONNE UTILISATION.