Procédure d’installation du WIFI via Radius

Table des matières

Équipements utilisés

-WAP371
-Cable RJ45
-Ordinateur portable
-Un serveur AD, DHCP, DNS préconfigurer
-Un switch

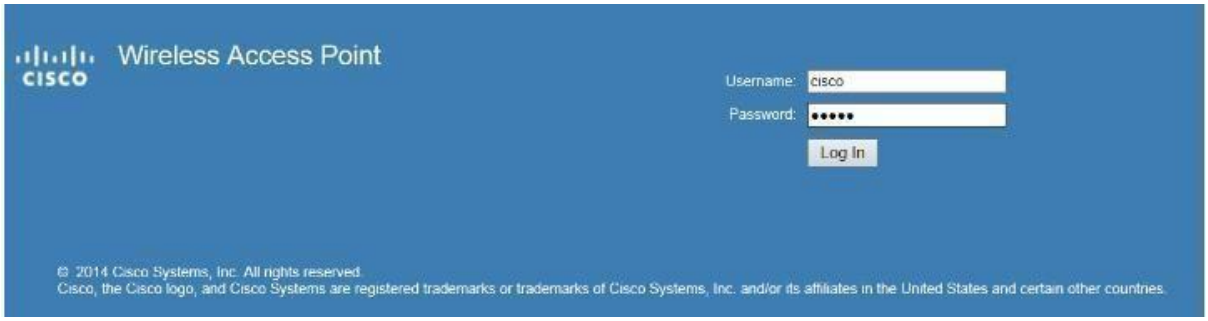
Réinitialisation des paramètres d'usine

1. Appuyer sur le bouton de réinitialisation situé au fond du périphérique pendant approximativement dix secondes avec une broche.

Les recharges de Point d'accès sont placées en configuration par défaut.

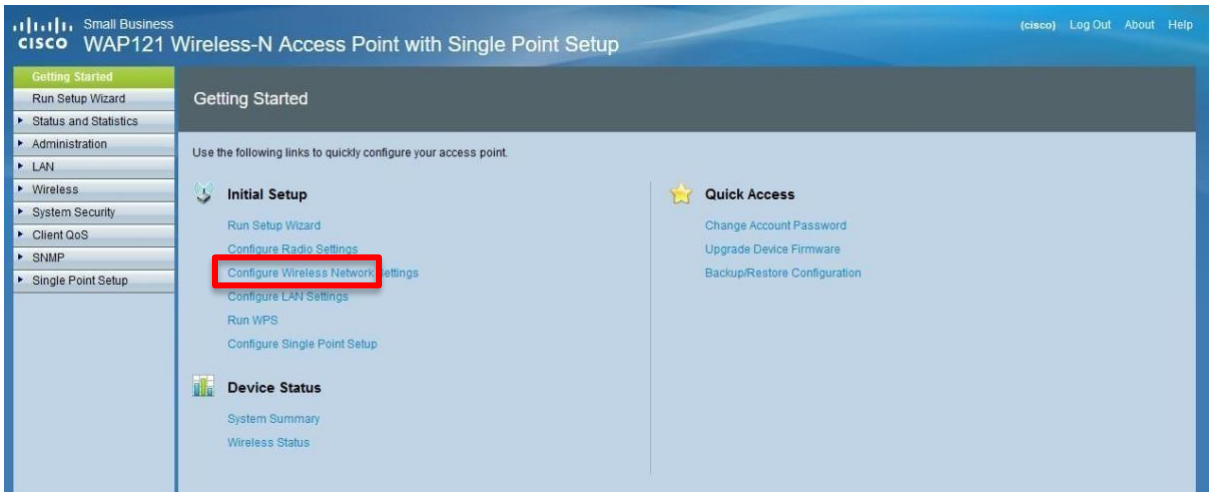
2. Lancez un navigateur Web, tel que Internet Explorer ou Mozilla Firefox. Tapez l'adresse IP statique par défaut 192.168.1.245 dans la barre URL et appuyez sur la touche Entrer. Pour atteindre cette adresse IP, soyez sûr que votre ordinateur est sur le réseau 192.168.1.xxx.

3. Procédure de connexion avec les qualifications par défaut. Le nom d'utilisateur par défaut est Cisco, et le mot de passe par défaut est Cisco.

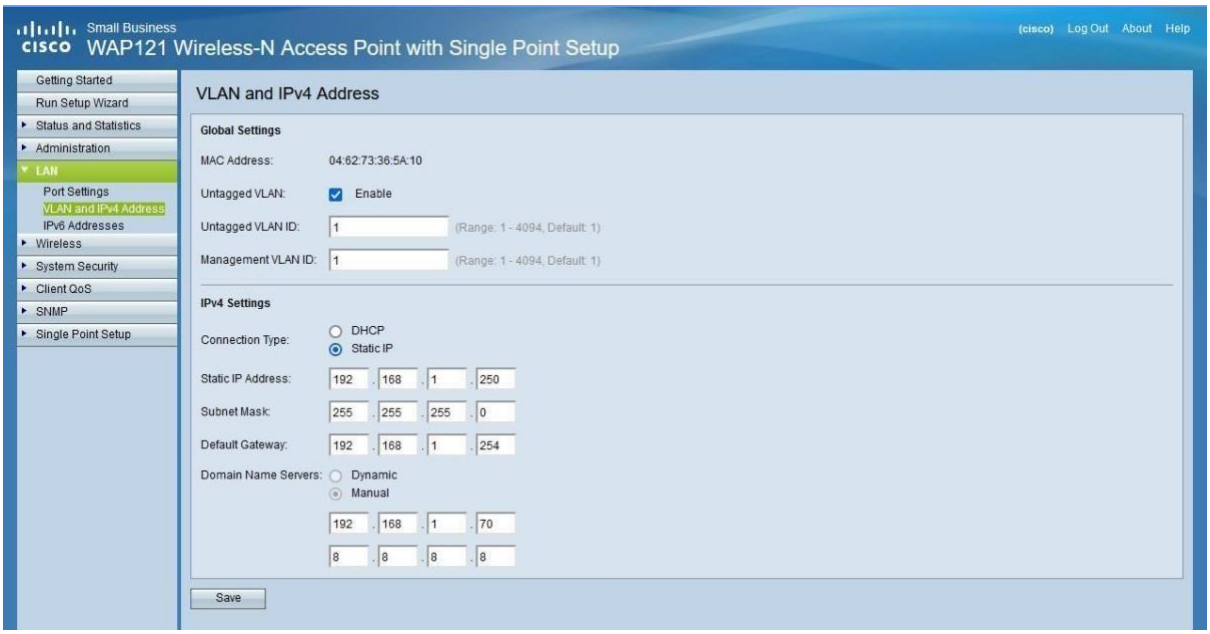


Configuration de la borne WI-FI

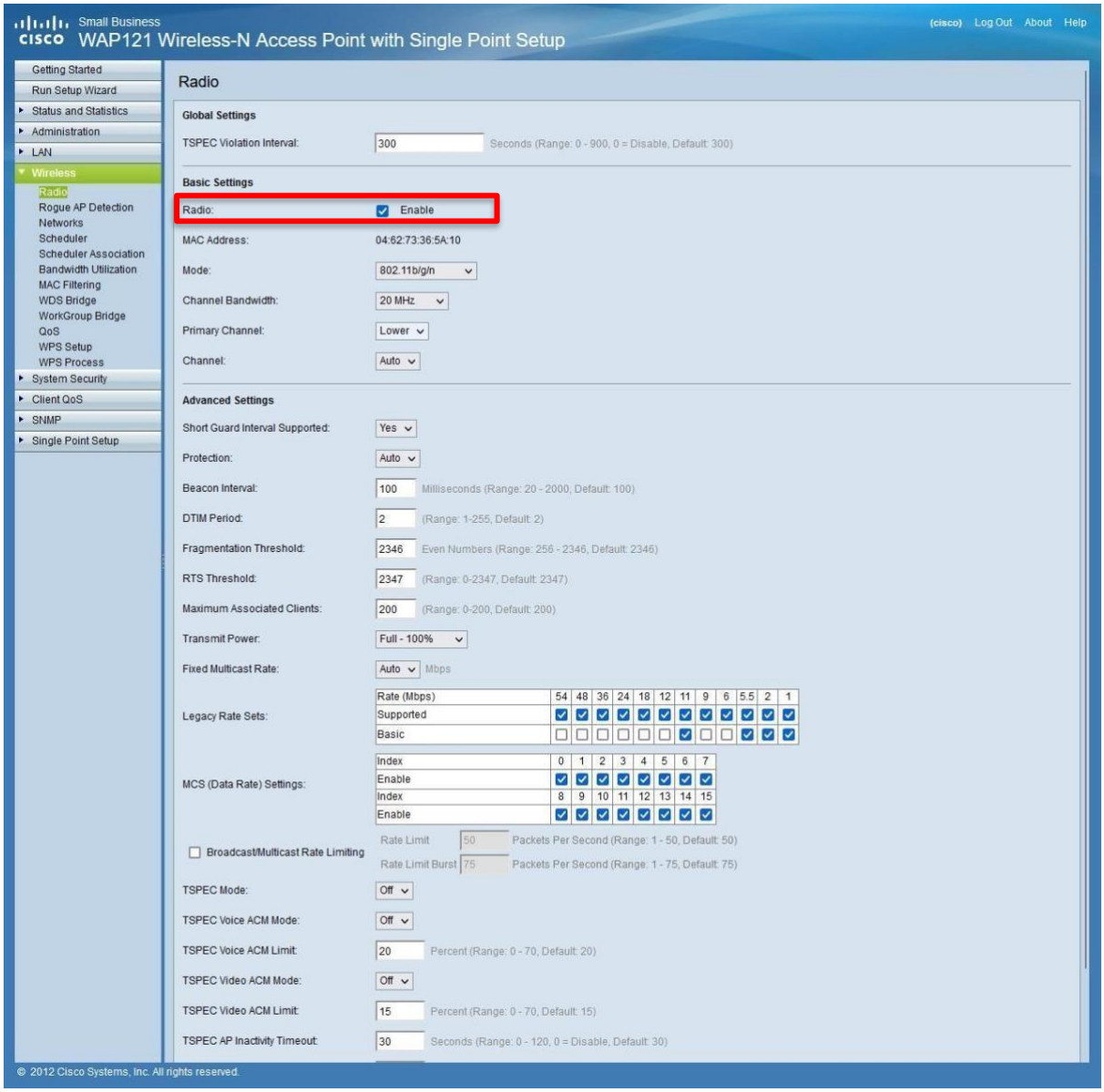
4. Une fois installée, connectez-vous et cliquez sur Configure LAN Settings



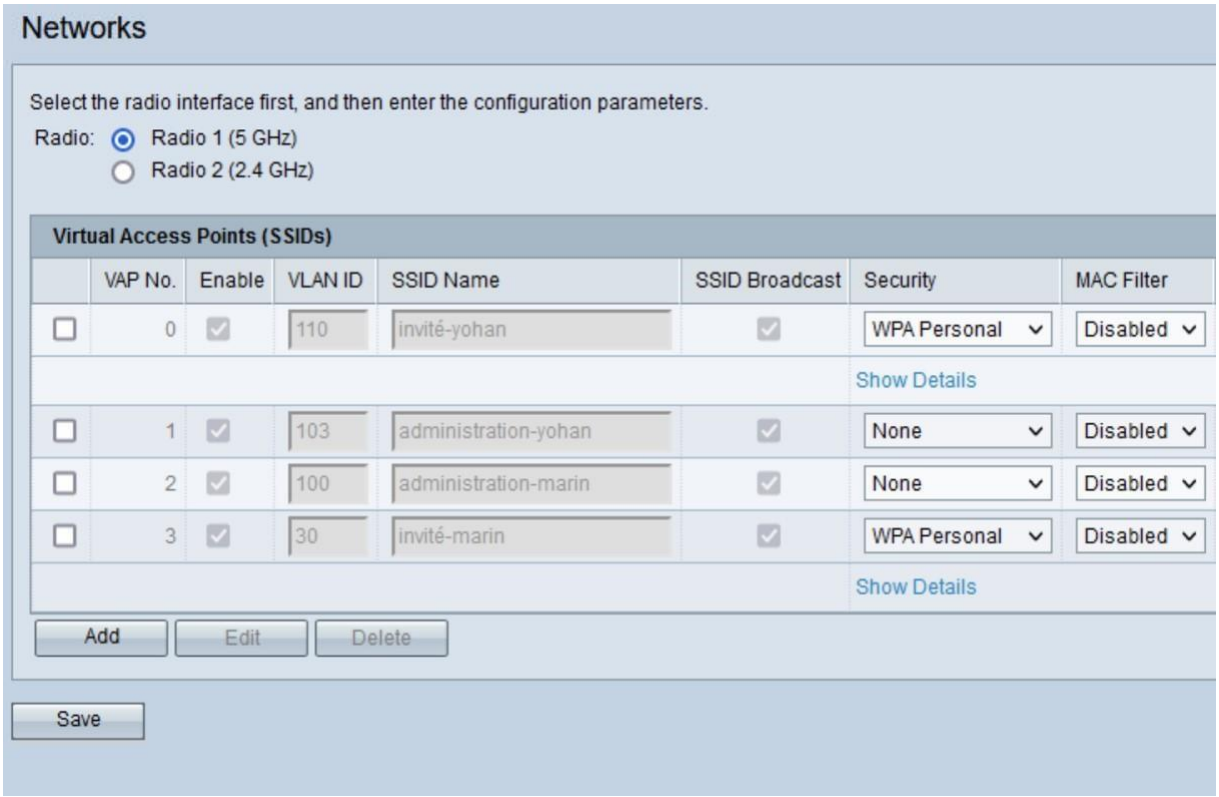
5. Configurer l'IPv4 statique de la borne, le masque, la passerelle, le DNS de votre réseau et éventuellement indiqué lui VLAN si votre switch et configuré avec des vlans



6. Après cela, retournez à l'accueil et cliquez sur Configure Radio Setting. Activez l'option Radio, nous laisserons les paramètres par défaut, mais nous serons amenés à les modifier plus tard pour des questions d'optimisation selon l'environnement de la borne WI-FI.

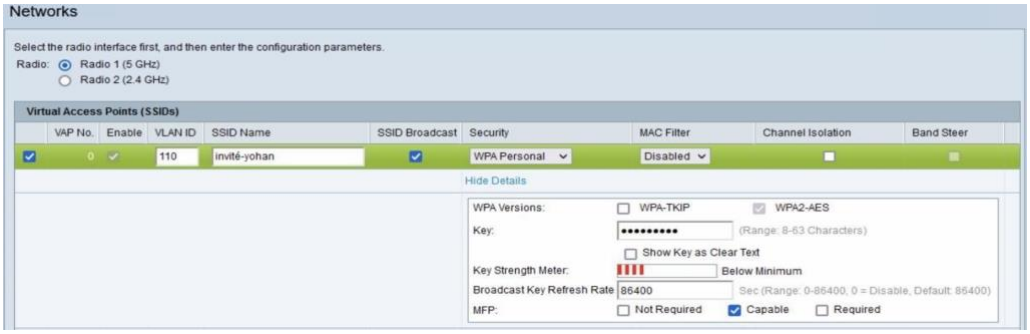


7. Retournez au menu et cliquez maintenant sur Configure Wireless Network Settings



Création des différents points d'accès WI-FI

11. Cliquez sur le point d'accès par défaut puis sur Edit
12. Indiquez le vlan à utiliser si c'est le cas donner un SSID au point d'accès, laissez cocher le SSID Broadcast. Enfin, pour le premier point d'accès on utilise la sécurité WPA Personal. Ensuite nous définissons la clé puis on sauvegarde.

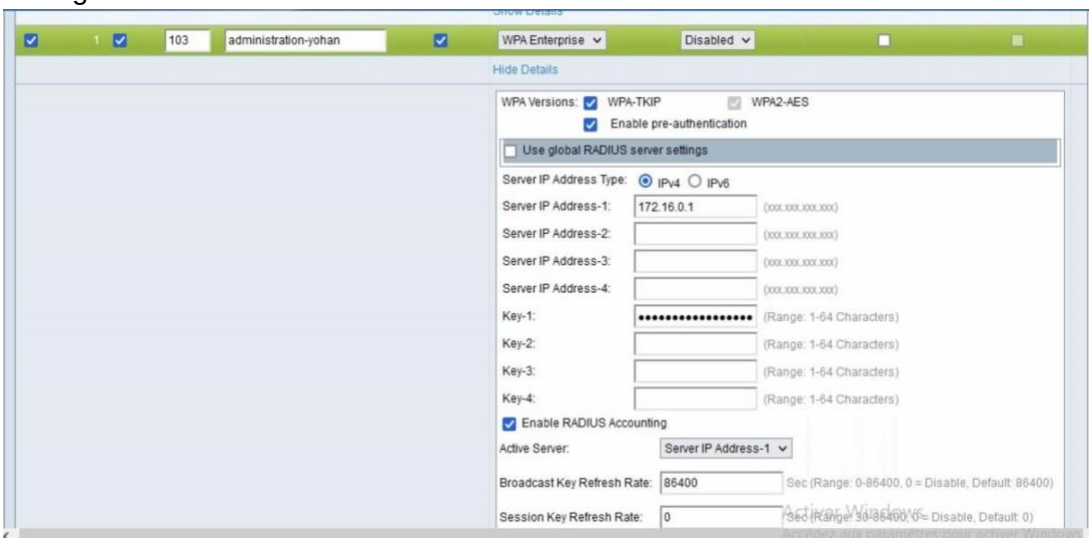


13.Votre premier point d'accès WI-FI est fonctionnel. Il vous suffit de vous connecter à l'aide de la clé pour créer celui-ci.

14.Nous allons créer un point d'accès WI-FI d'entreprise

15.On add puis on edit

16. Indiquer le vlan à utiliser si c'est le cas donner un SSID au point d'accès, laissez cocher le SSID Broadcast. Enfin, pour le premier point d'accès on utilise la sécurité WPA Entreprise. Ensuite nous définissons l'adresse IP ou point nos service AD, DHCP … éventuellement sa réplication et une clé puis on sauvegarde.

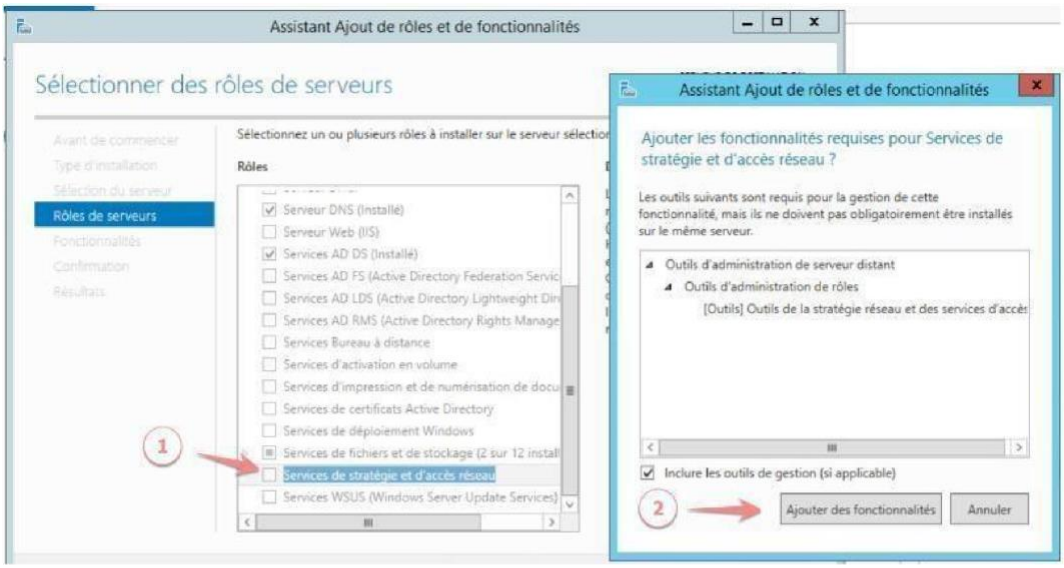


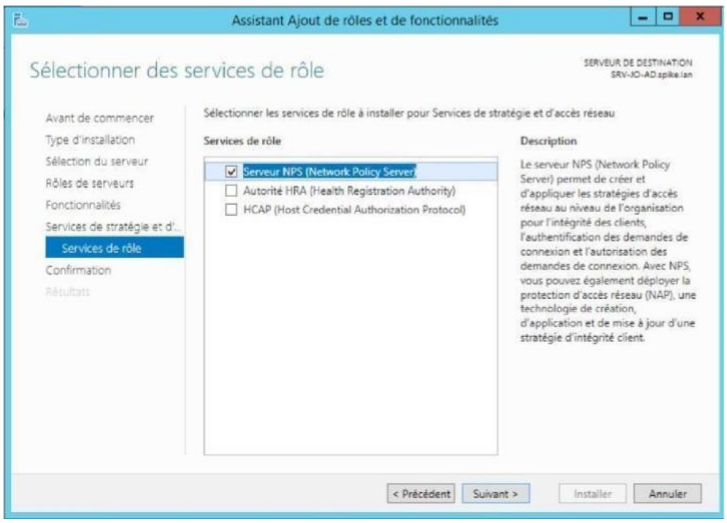
Le point d'accès sera alors visible, mais il ne sera pas possible de la rejoindre nous devons effectuer une manipulation sur le serveur AD. Il pourra ensuite se connecter avec ses identifiants d'entreprise sur la borne WI-Fi

Installation du service radius sur le serveur AD

21. Sur le serveur Windows 2019, allez dans le gestionnaire de serveur, cliquez sur « Gérer » puis « Ajouter des rôles et fonctionnalités ».

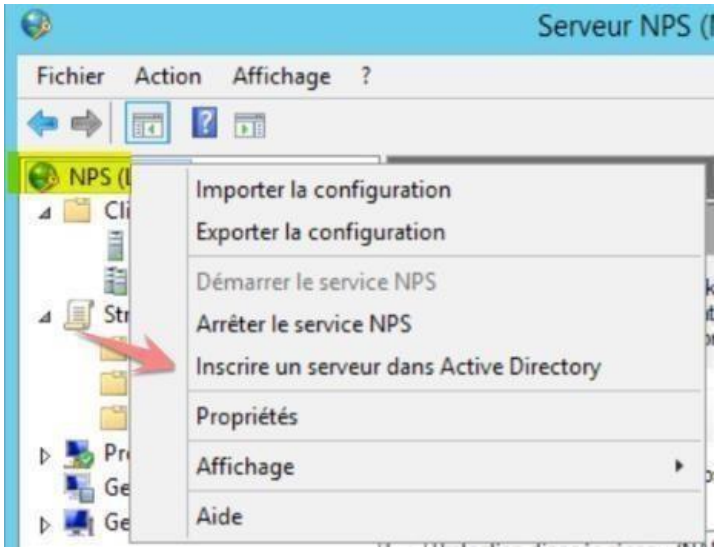
22. Sélectionner le rôle services de stratégie et d'accès réseau et ajouter des fonctionnalités





23. Ajout du service de rôle : Serveur NPS

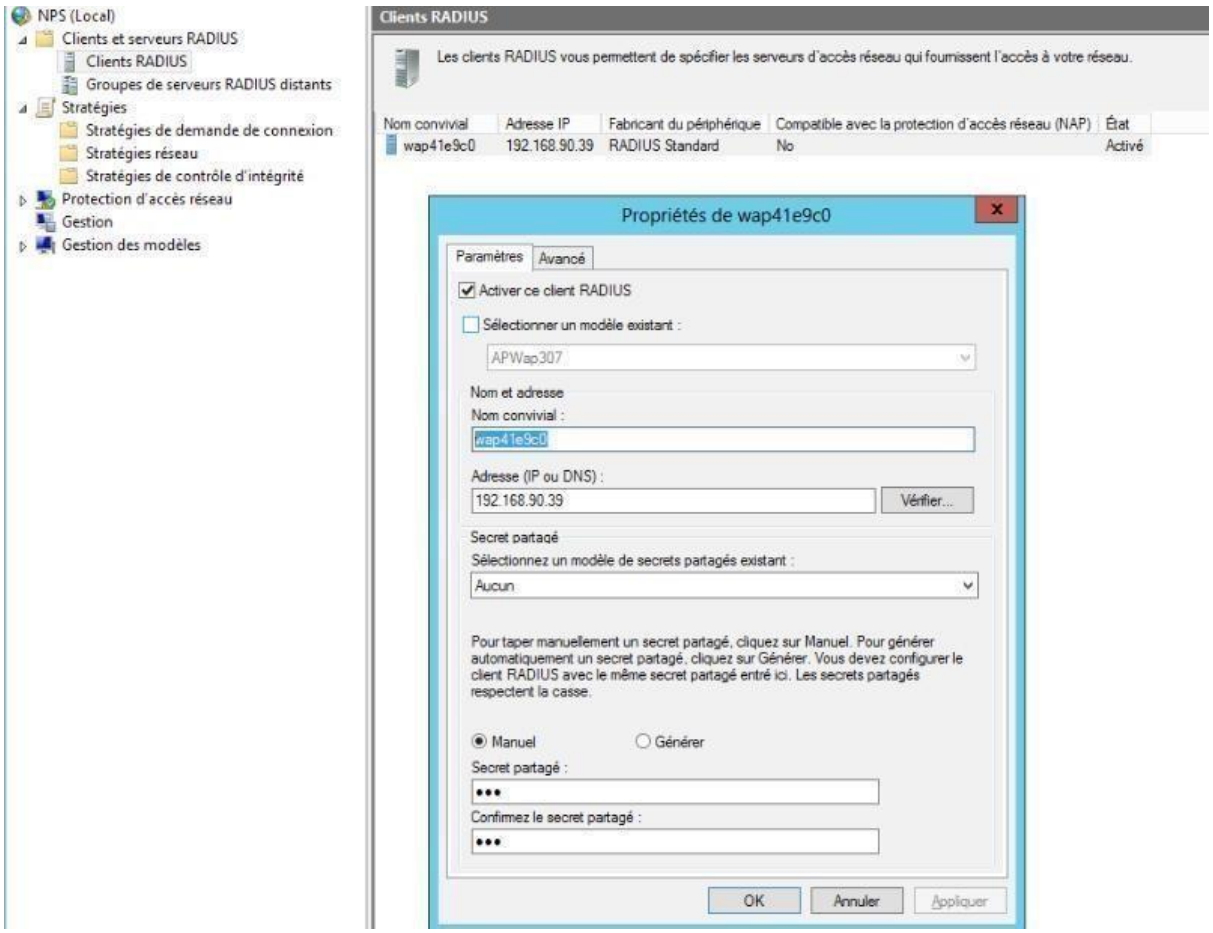
Configuration de radius pour une borne WI-FI



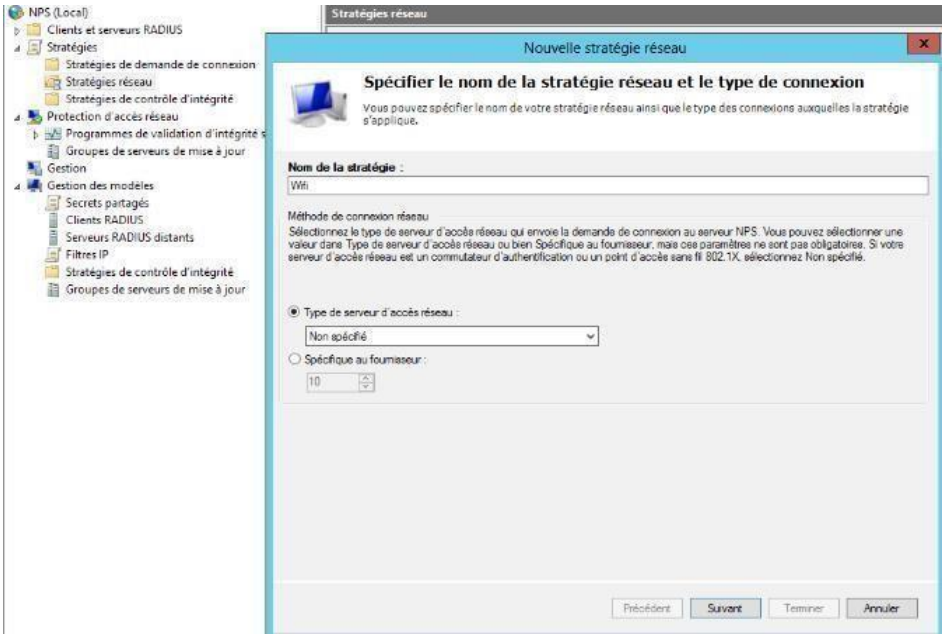
24.Lancez le service et faites un clic droit sur NPS

25.Inscrivez le serveur dans l'Active directory sinon il sera impossible de définir les conditions liées aux groupes/utilisateurs dans la stratégie d'accès distant

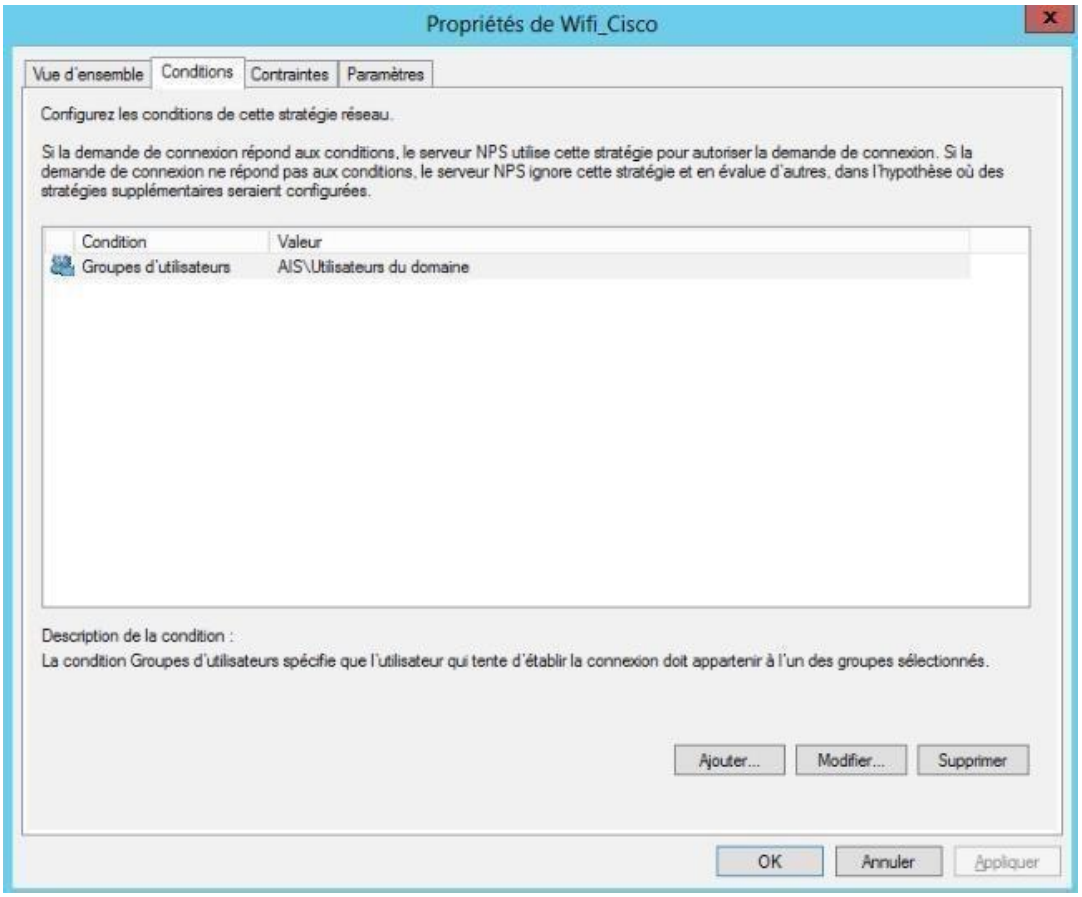
26.Créez un nouveau client radius sur la console NPS, clic droit nouveau Nom de la borne : wap121 adresse de la borne : 192.168.1.250 secret : Que vous avez défini sur la borne en amont



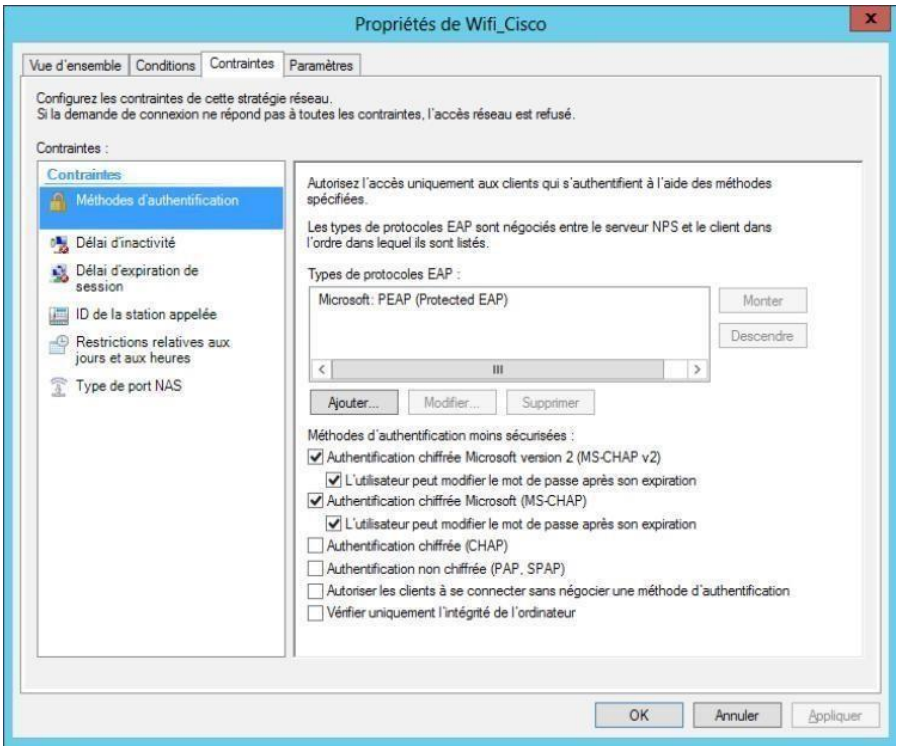
27. Configuration de la stratégie réseau nouvelle stratégie réseau – nom de la stratégie : Wifi



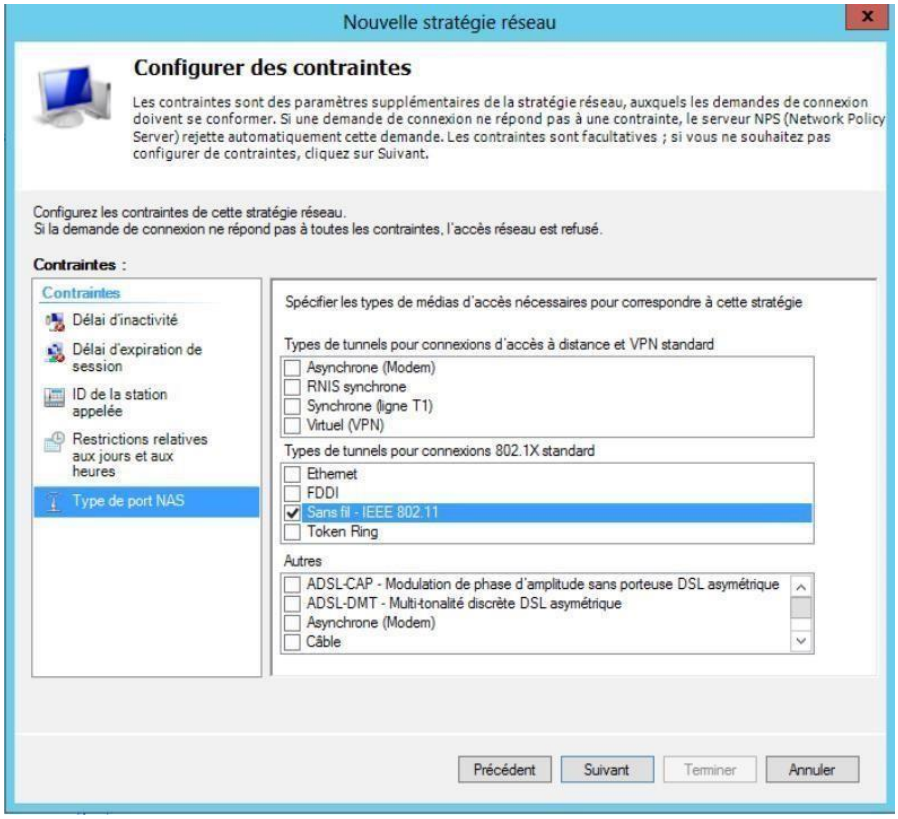
28. Nous ajouterons le Groupe utilisateurs du domaine



29. Sélectionnez MS-CHAP v2 et MS-CHAP pour authentification par mot de passe.
30. Montez Le protocole Extended Authentication Protocol. Il sert pour le transport des données nécessaire à l'authentification.

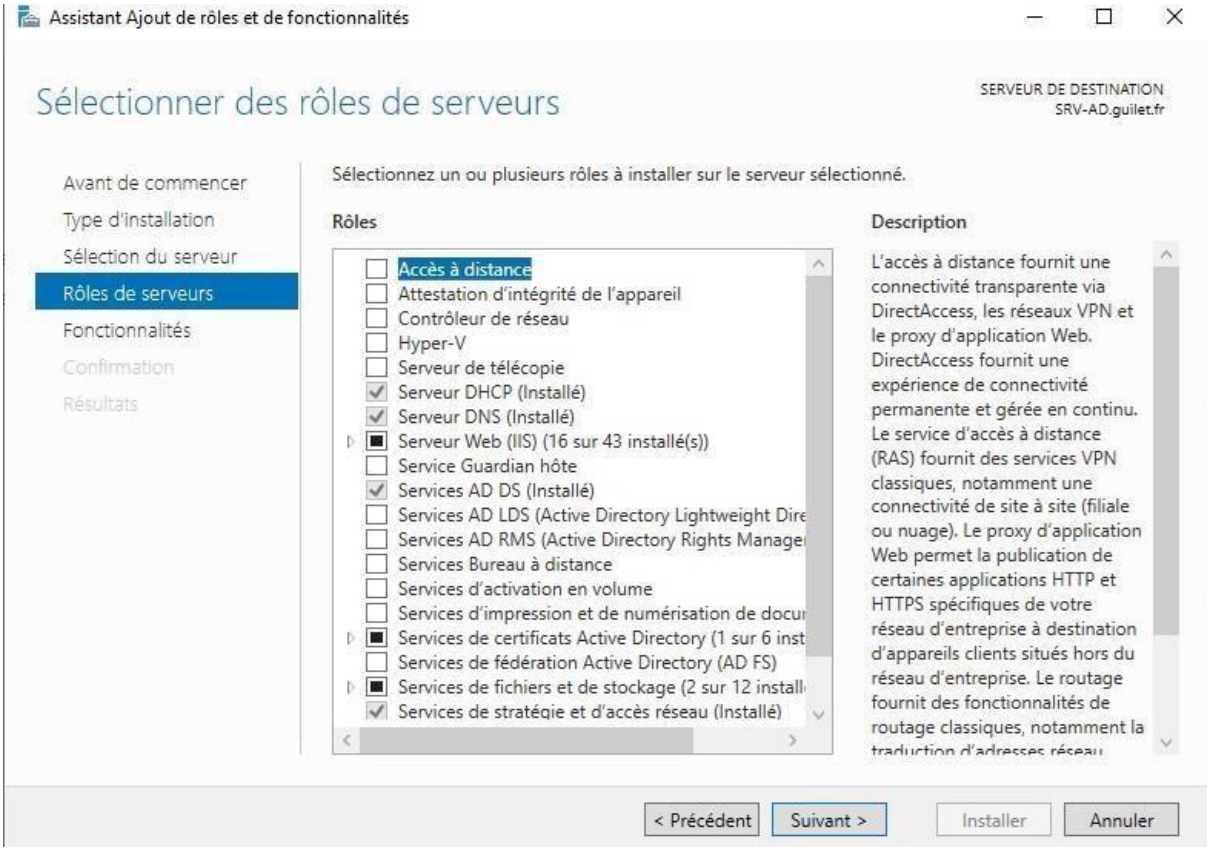


31. Type de port NAS - dans rubrique 801.1X , sélectionnez Sans fil – IEEE 802.11 si ce n'est pas un accès sans fil, la demande de connexion est rejetée.

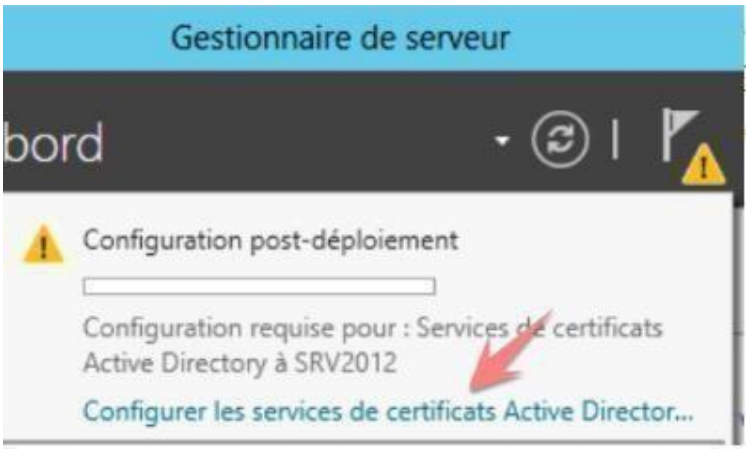


Installation d’une Autorité de certification

32. Installez les rôles adcs et outil de gestion. Suivant<suivant<installer



Configuration d'une Autorité de certification



33. Démarrez le gestionnaire de serveur, et cliquez sur l'icône drapeau en haut à droite pour démarrer la configuration.

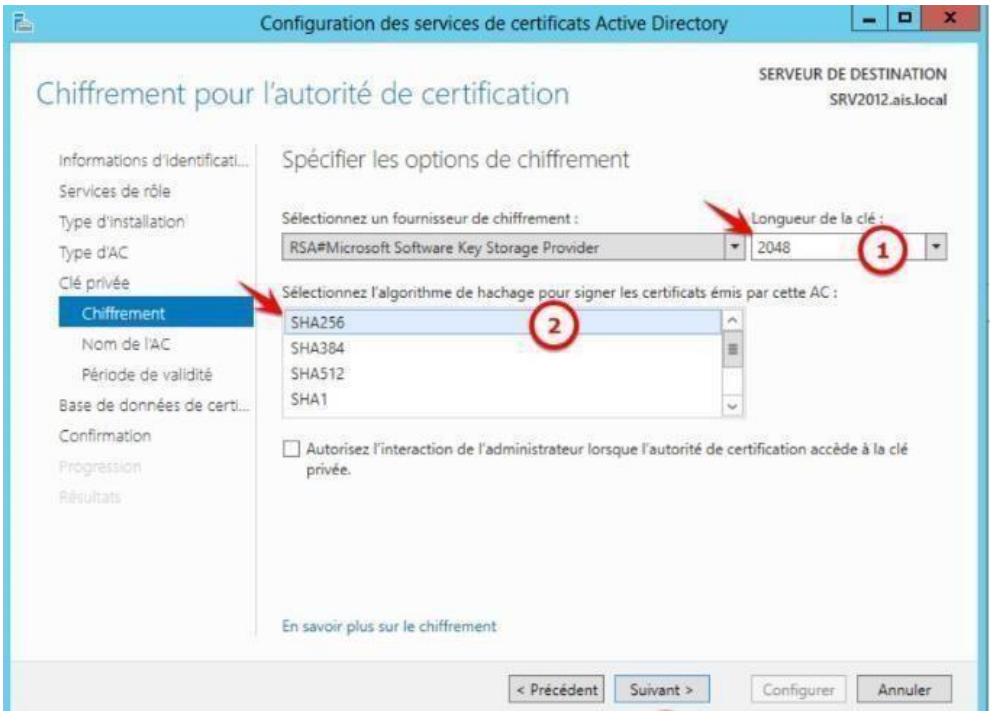
34. Sur la page Services de rôle, sélectionnez Autorité de certification et cliquez sur Suivant.

• Sur la page Type d'installation, sélectionnez Autorité de certification d'entreprise et cliquez sur Suivant.

• Sur la page Type d'autorité de certification, sélectionnez Autorité de certification racine Sur la page Clé privée, sélectionnez Créer une nouvelle clé privée et cliquez sur Suivant.

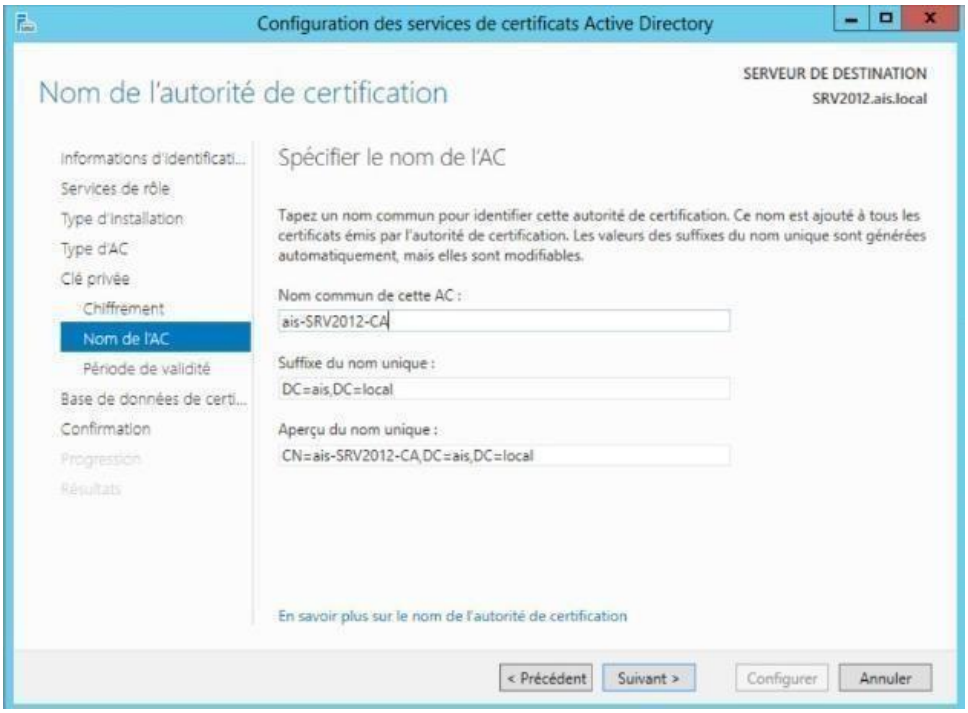
• Sur la page Chiffrement, entrez les informations comme suit. (Recommandation NIST et globalsign : longueur de clé minimal 2048 et algorithme SHA256)

•



35. Sur la page Nom de l'autorité de certification, acceptez les valeurs par défaut et cliquez sur Suivant.

36. Donnez un nom au certificat



37. Sur la page Période de validité, par défaut la valeur est de 5 années, cliquez sur Suivant.
38. Sur la page Base de données de certificats, cliquez sur Suivant.
39. Sur la page Confirmation, passez en revue les informations fournies et cliquez sur Configurer.

Sélection du certificat autosigné sur la console NPS

40. Console NPS – stratégie d'accès réseau – propriétés de la stratégie wifi onglet contraintes

41. Sélectionnez Microsoft PEAP, puis Modifier afin de sélectionner le certificat serveur autosigné.

42. Cliquez sur OK pour valider