



## Procédure d'installation du WIFI via Radius

# Table des matières

Équipements utilisés .....	3
Réinitialisation des paramètres d'usine .....	3
Configuration de la borne WI-FI .....	4
Création des différents points d'accès WI-FI.....	7
Installation du service radius sur le serveur AD .....	8
Configuration de radius pour une borne WI-FI .....	9
Installation d'une Autorité de certification .....	12
Configuration d'une Autorité de certification .....	13
Sélection du certificat autosigné sur la console NPS.....	15

## 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.

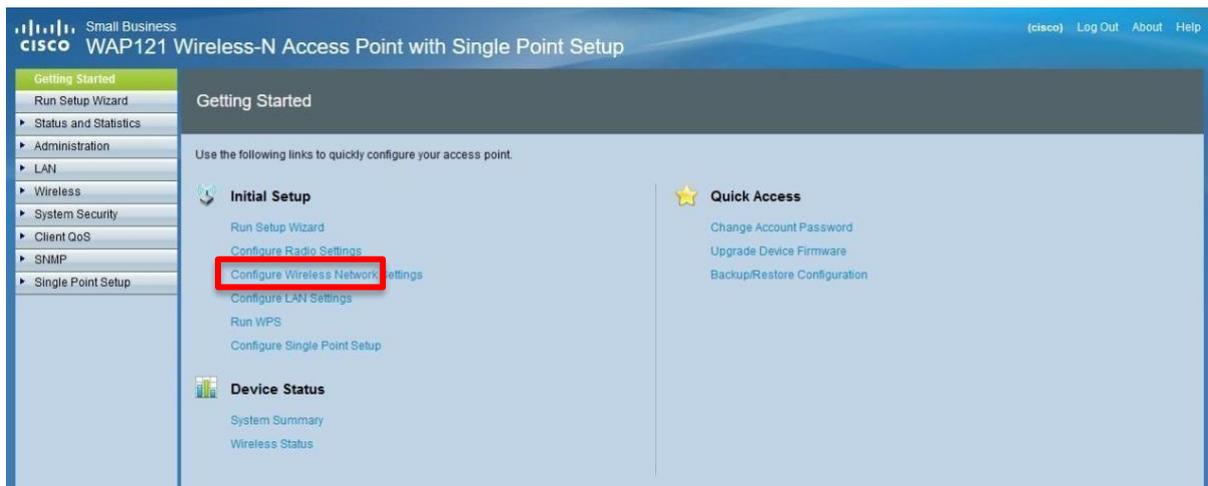
2. Lancez un navigateur Web, tel que Internet Explorer ou Mozilla Firefox. Tapez l'adresse IP statique par défaut 192.168.1.245 dans la barre URL et appuyez sur la touche Entrer. Pour atteindre cette adresse IP, soyez sûr que votre ordinateur est sur le réseau 192.168.1.xxx.

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.

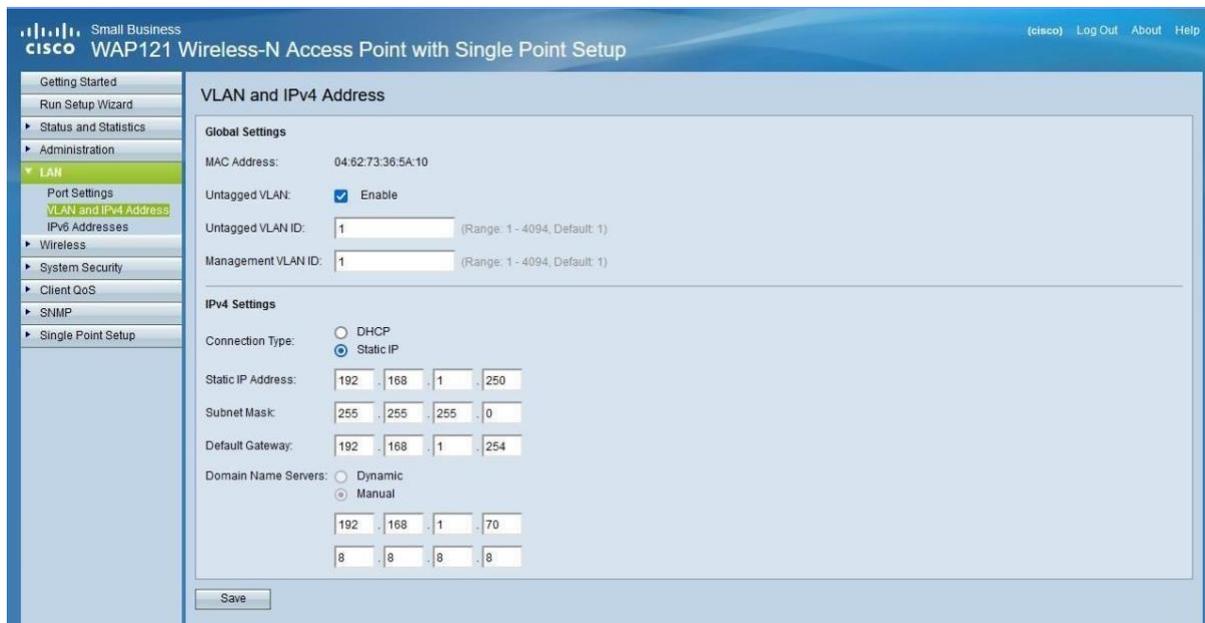
© 2014 Cisco Systems, Inc. All rights reserved.  
Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

## Configuration de la borne WI-FI

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



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



- 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.

- Getting Started
- Run Setup Wizard
- Status and Statistics
- Administration
- LAN
- Wireless
  - Radio**
  - Rogue AP Detection
  - Networks
  - Scheduler
  - Scheduler Association
  - Bandwidth Utilization
  - MAC Filtering
  - WDS Bridge
  - WorkGroup Bridge
  - QoS
  - WPS Setup
  - WPS Process
- System Security
- Client QoS
- SNMP
- Single Point Setup

## Radio

### Global Settings

TSPEC Violation Interval:  Seconds (Range: 0 - 900, 0 = Disable, Default: 300)

### Basic Settings

Radio:  Enable

MAC Address:

Mode:

Channel Bandwidth:

Primary Channel:

Channel:

### Advanced Settings

Short Guard Interval Supported:

Protection:

Beacon Interval:  Milliseconds (Range: 20 - 2000, Default: 100)

DTIM Period:  (Range: 1-255, Default: 2)

Fragmentation Threshold:  Even Numbers (Range: 256 - 2346, Default: 2346)

RTS Threshold:  (Range: 0-2347, Default: 2347)

Maximum Associated Clients:  (Range: 0-200, Default: 200)

Transmit Power:

Fixed Multicast Rate:  Mbps

Rate (Mbps)	54	48	36	24	18	12	11	9	6	5.5	2	1
Supported	<input checked="" type="checkbox"/>											
Basic	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>					

MCS (Data Rate) Settings:	Index	0	1	2	3	4	5	6	7
Enable		<input checked="" type="checkbox"/>							
Index		8	9	10	11	12	13	14	15
Enable		<input checked="" type="checkbox"/>							

Broadcast/Multicast Rate Limiting

Rate Limit:  Packets Per Second (Range: 1 - 50, Default: 50)

Rate Limit Burst:  Packets Per Second (Range: 1 - 75, Default: 75)

TSPEC Mode:

TSPEC Voice ACM Mode:

TSPEC Voice ACM Limit:  Percent (Range: 0 - 70, Default: 20)

TSPEC Video ACM Mode:

TSPEC Video ACM Limit:  Percent (Range: 0 - 70, Default: 15)

TSPEC AP Inactivity Timeout:  Seconds (Range: 0 - 120, 0 = Disable, Default: 30)

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

### Networks

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (5 GHz)  
 Radio 2 (2.4 GHz)

Virtual Access Points (SSIDs)							
	VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	110	invité-yohan	<input checked="" type="checkbox"/>	WPA Personal	Disabled
						<a href="#">Show Details</a>	
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	103	administration-yohan	<input checked="" type="checkbox"/>	None	Disabled
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	100	administration-marin	<input checked="" type="checkbox"/>	None	Disabled
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	30	invité-marin	<input checked="" type="checkbox"/>	WPA Personal	Disabled
						<a href="#">Show Details</a>	

## 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.

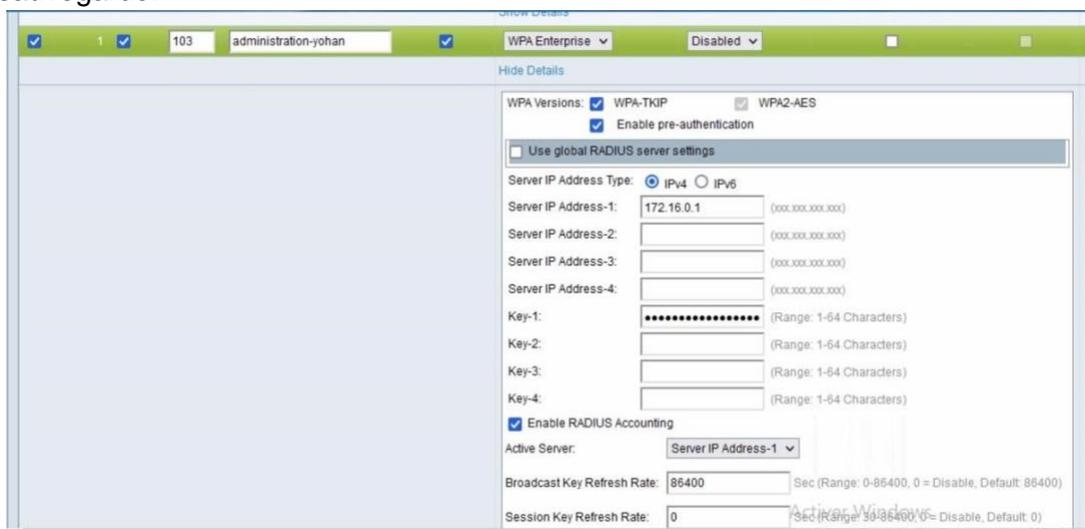


13. Votre premier point d'accès WI-FI est fonctionnel. Il vous suffit de vous connecter à l'aide de la clé pour créer celui-ci.

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

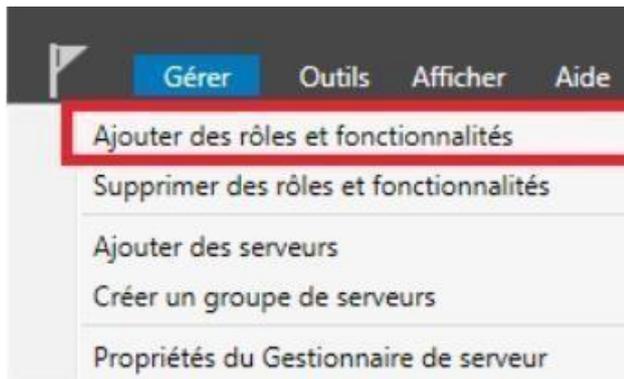
15. On add puis on edit

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.



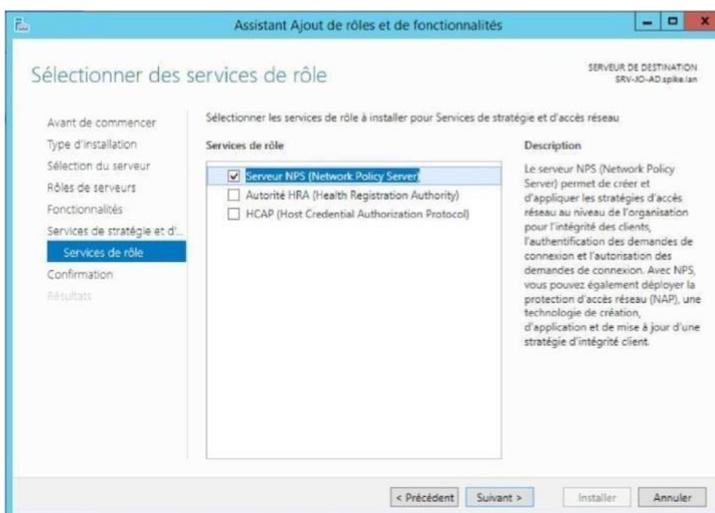
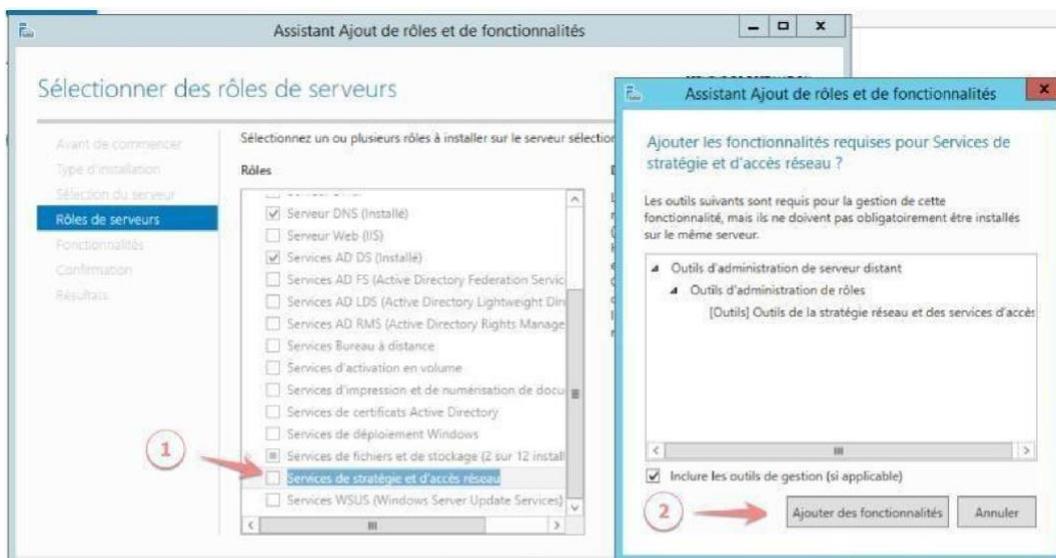
Le point d'accès sera alors visible, mais il ne sera pas possible de la rejoindre nous devons effectuer une manipulation sur le serveur AD. Il pourra ensuite se connecter avec ses identifiants d'entreprise sur la borne WI-FI

## Installation du service radius sur le serveur AD



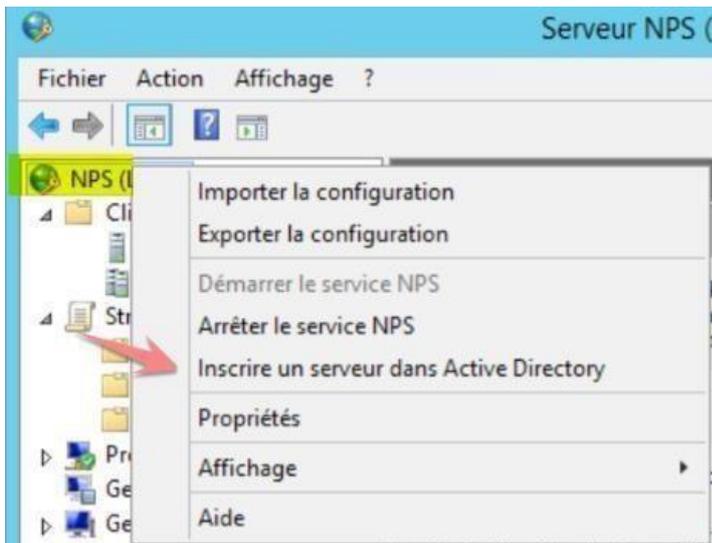
21. Sur le serveur Windows 2019, allez dans le gestionnaire de serveur, cliquez sur « Gérer » puis « Ajouter des rôles et fonctionnalités ».

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



23. Ajout du service de rôle :  
Serveur NPS

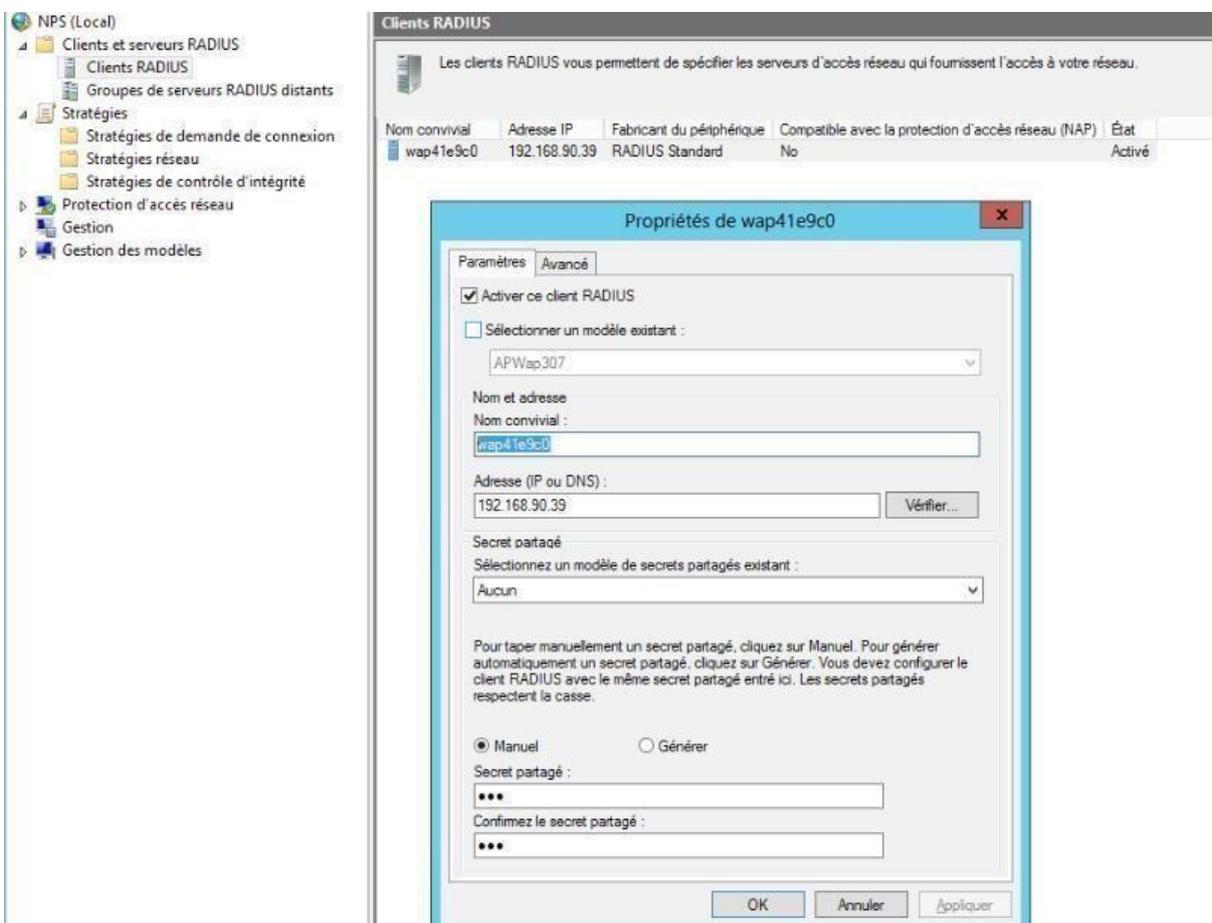
## Configuration de radius pour une borne WI-FI



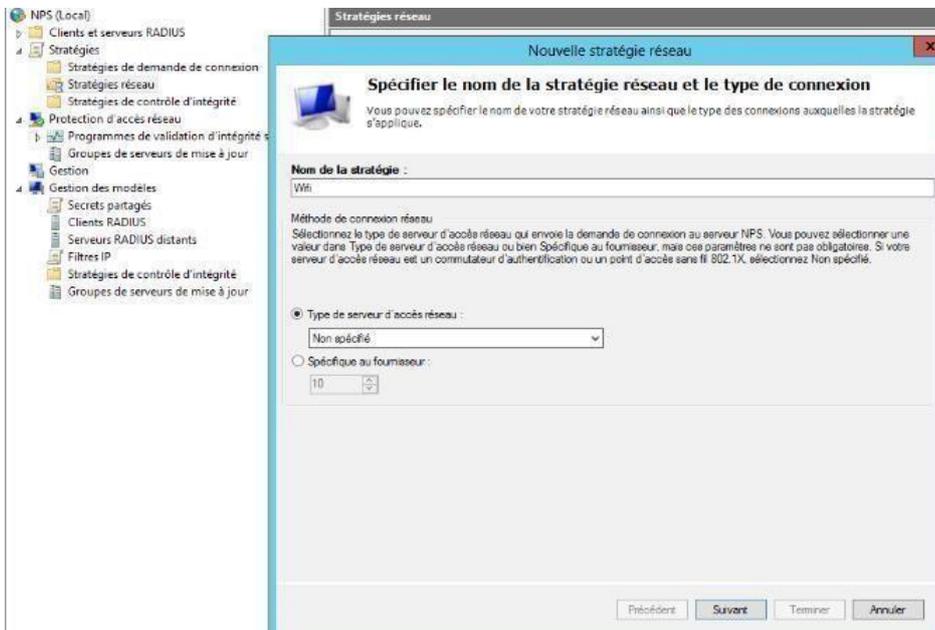
24. Lancez le service et faites un clic droit sur NPS

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

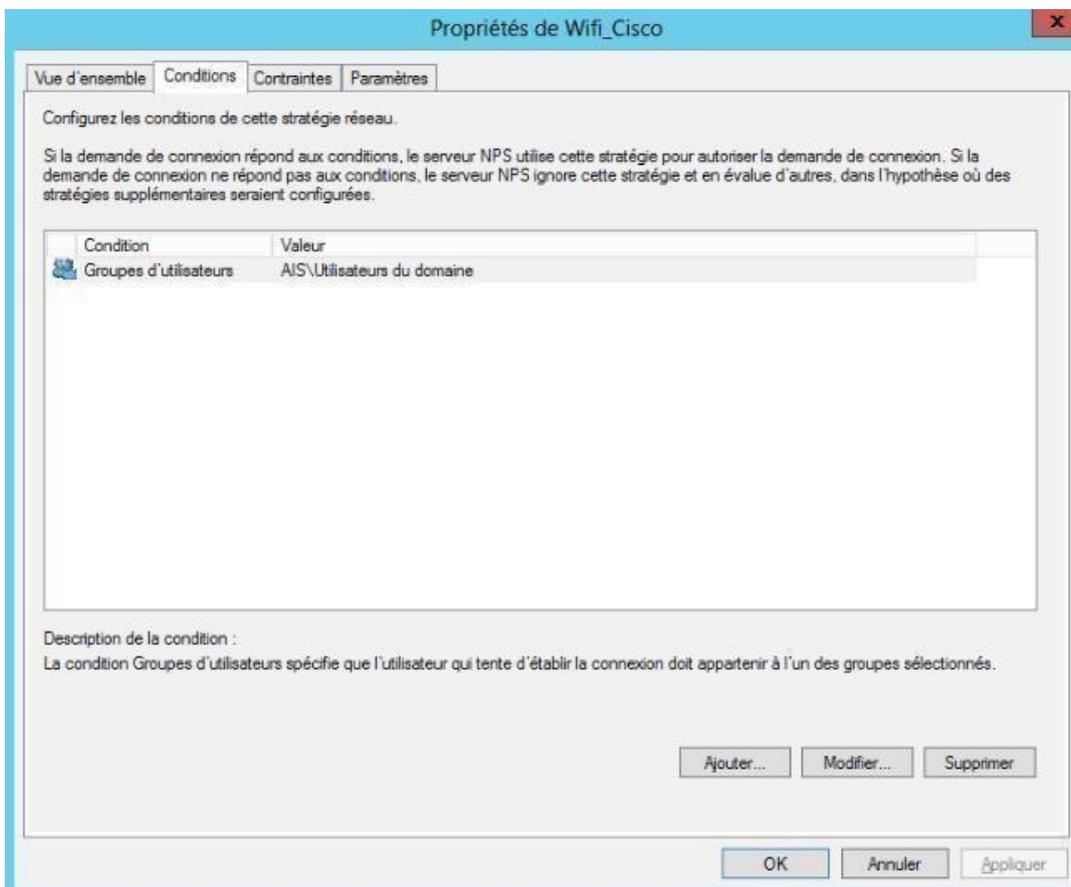
26. Créez un nouveau client radius sur la console NPS, clic droit nouveau Nom de la borne : wap121 adresse de la borne : 192.168.1.250 secret : Que vous avez défini sur la borne en amont



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

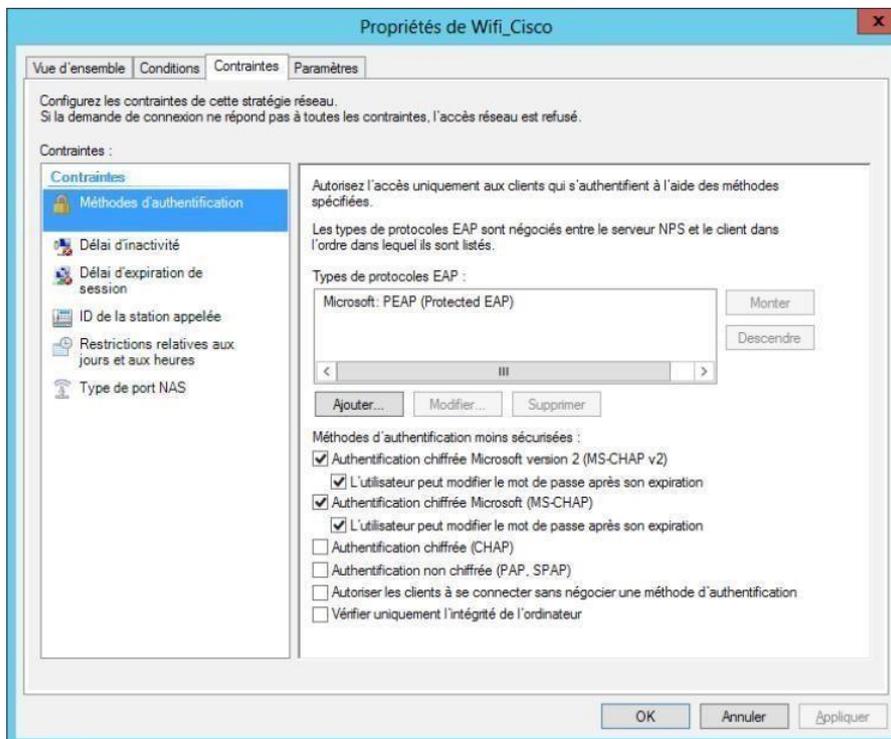


28. Nous ajouterons le Groupe utilisateurs du domaine

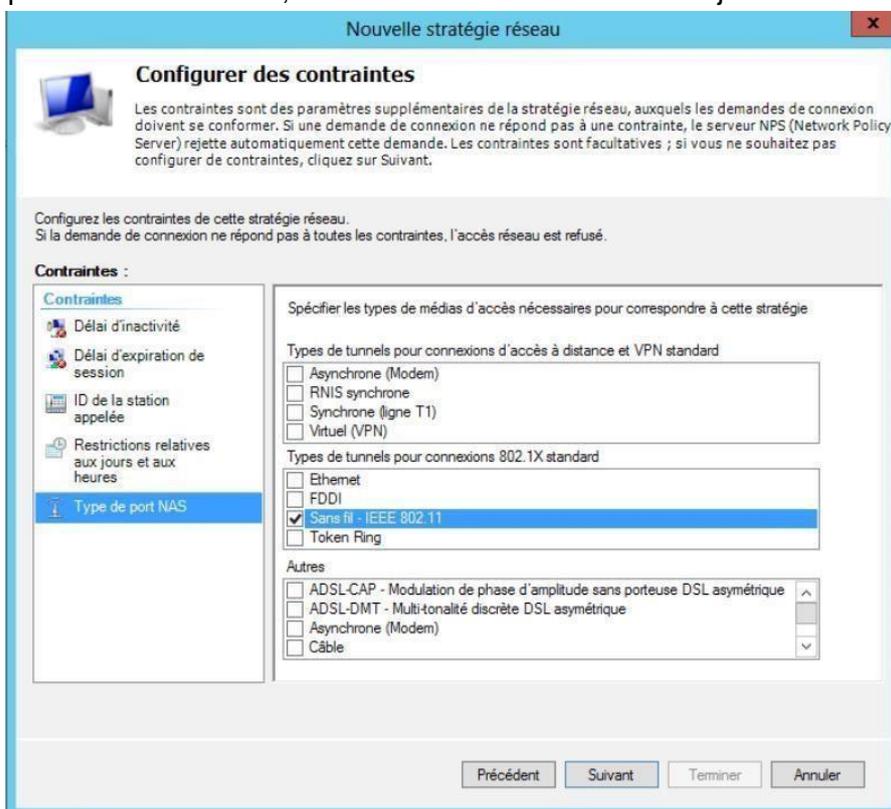


29. Sélectionnez MS-CHAP v2 et MS-CHAP pour authentification par mot de passe.

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

Assistant Ajout de rôles et de fonctionnalités

Sélectionner des rôles de serveurs

SERVEUR DE DESTINATION  
SRV-AD.guilet.fr

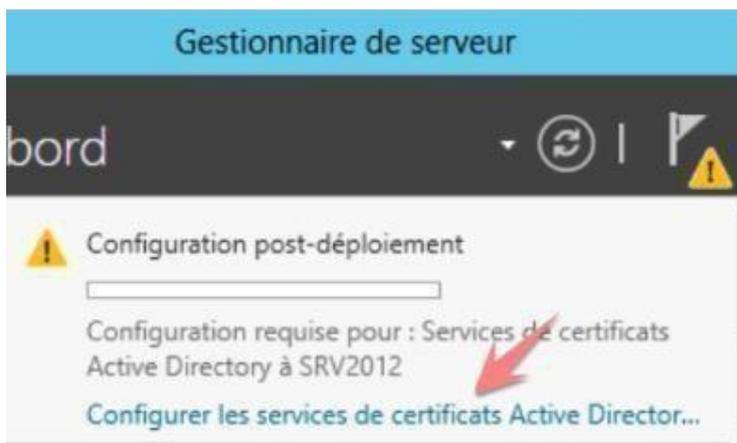
Avant de commencer  
Type d'installation  
Sélection du serveur  
**Rôles de serveurs**  
Fonctionnalités  
Confirmation  
Résultats

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles	Description
<input type="checkbox"/> Accès à distance	L'accès à distance fournit une connectivité transparente via DirectAccess, les réseaux VPN et le proxy d'application Web. DirectAccess fournit une expérience de connectivité permanente et gérée en continu. Le service d'accès à distance (RAS) fournit des services VPN classiques, notamment une connectivité de site à site (filiale ou nuage). Le proxy d'application Web permet la publication de certaines applications HTTP et HTTPS spécifiques de votre réseau d'entreprise à destination d'appareils clients situés hors du réseau d'entreprise. Le routage fournit des fonctionnalités de routage classiques, notamment la traduction d'adresses réseau.
<input type="checkbox"/> Attestation d'intégrité de l'appareil	
<input type="checkbox"/> Contrôleur de réseau	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Serveur de télécopie	
<input checked="" type="checkbox"/> Serveur DHCP (Installé)	
<input checked="" type="checkbox"/> Serveur DNS (Installé)	
<input checked="" type="checkbox"/> Serveur Web (IIS) (16 sur 43 installé(s))	
<input type="checkbox"/> Service Guardian hôte	
<input checked="" type="checkbox"/> Services AD DS (Installé)	
<input type="checkbox"/> Services AD LDS (Active Directory Lightweight Directory Services)	
<input type="checkbox"/> Services AD RMS (Active Directory Rights Management Services)	
<input type="checkbox"/> Services Bureau à distance	
<input type="checkbox"/> Services d'activation en volume	
<input type="checkbox"/> Services d'impression et de numérisation de documents	
<input checked="" type="checkbox"/> Services de certificats Active Directory (1 sur 6 installés)	
<input type="checkbox"/> Services de fédération Active Directory (AD FS)	
<input checked="" type="checkbox"/> Services de fichiers et de stockage (2 sur 12 installés)	
<input checked="" type="checkbox"/> Services de stratégie et d'accès réseau (Installé)	

< Précédent Suivant > Installer Annuler

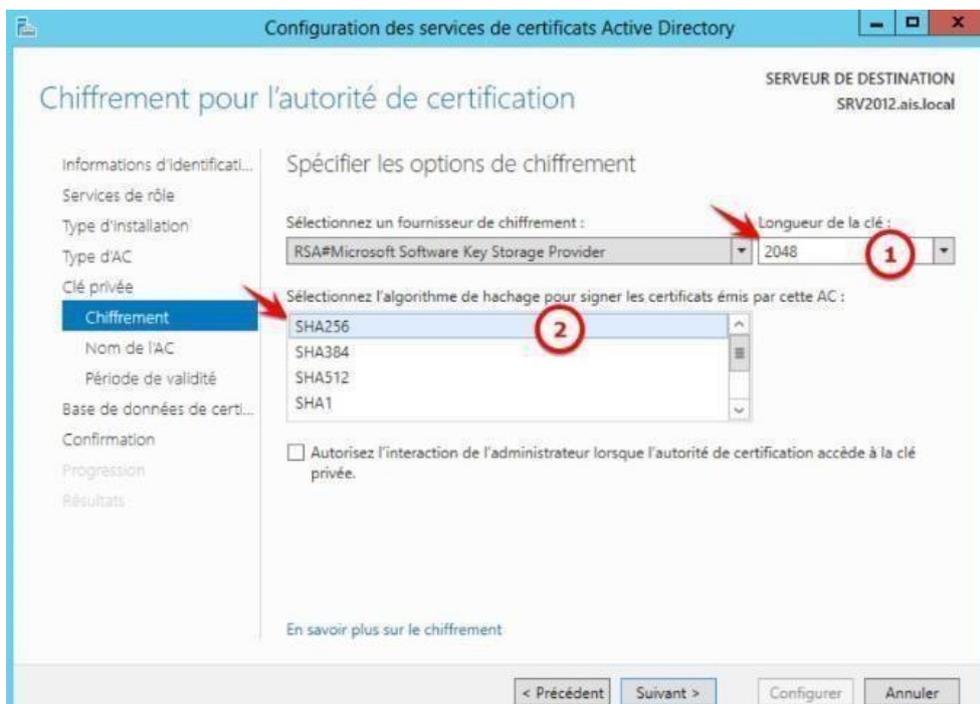
## Configuration d'une Autorité de certification



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

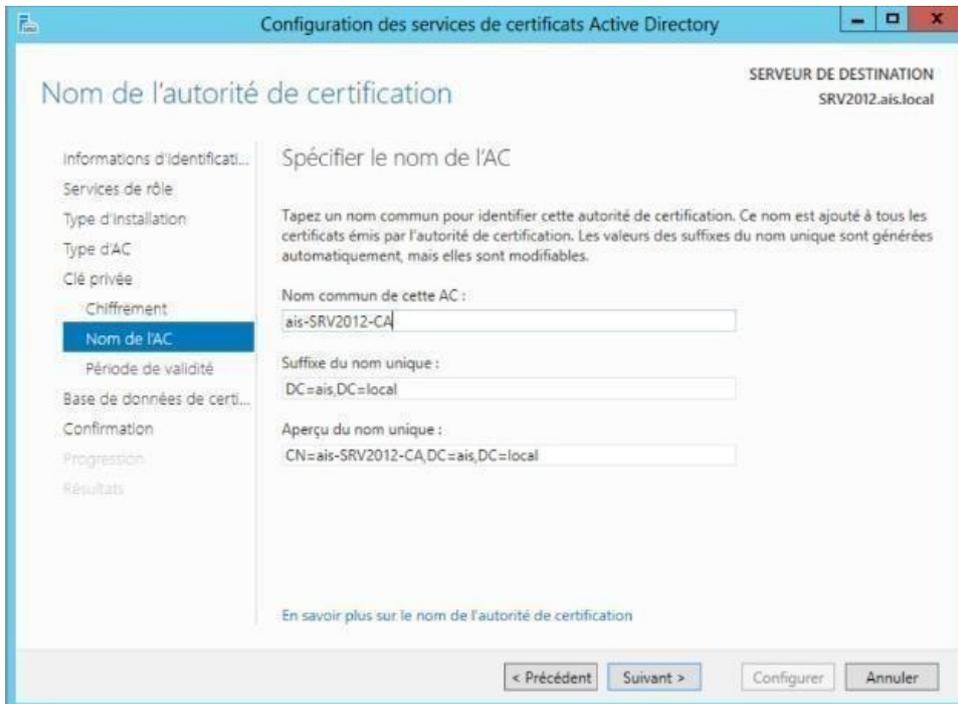
34. Sur la page Services de rôle, sélectionnez Autorité de certification et cliquez sur Suivant.

- 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

