

14/02/2024



# Réalisation professionnelle

La mise en place d'une solution  
Wifi Sécurisée

*Procédure d'installation et de  
configuration d'une solution Radius  
et d'un WPA2 Enterprise*

I. **Procédure d'installation et de configuration  
d'une solution Radius et d'un WPA2 Enterprise**



# PROCEDURE INSTALLATION ET CONFIGURATION SERVICE RADIUS

Réf : ASSURMER-PROC2024-0007

Version : 001

Date d'application : 14.02.2024

Page 2 sur 16

OBJET	DIFFUSION
Cette procédure a pour objet de décrire l'installation et la configuration d'un serveur Radius et d'un réseau Wifi WPA2 Enterprise	- En interne, DSI

	Page
Page de garde	1/16
➤ <b>Prérequis</b>	<b>2/16</b>
➤ <b>Lexique</b>	<b>2/16</b>
➤ <b>Mise en place du RADIUS sur la borne Cisco</b>	<b>3/16</b>
➤ <b>Installation et configuration du services AD CS</b>	<b>4/16</b>
➤ <b>Installation et configuration du service NPS (RADIUS)</b>	<b>8/16</b>

## Rédaction

**Lucas Evieux**  
Technicien Informatique

## Relecteur

**Elouan COTTIN**  
Technicien Informatique

**Tristan Bouvier**  
Technicien Informatique

## Approbation

**Elouan COTTIN**  
Technicien Informatique

**Tristan Bouvier**  
Technicien Informatique

## Prérequis

La mise en place de la solution Wifi sécurisée nécessite :

- Un serveur Windows 2022 avec AD DS, DHCP et DNS.
- Une borne Cisco WAP271.
- Un appareil permettant de se connecter au Wi-Fi.

## Lexique

**1** : Action à réaliser

**2** : L'action effectuée doit afficher

## Mise en place du RADIUS sur la borne Cisco

Dans "System Security" puis "RADIUS Server" et entrer les informations suivantes :

The screenshot shows the "RADIUS Server" configuration page in a Cisco management interface. On the left is a navigation menu with "System Security" expanded to show "RADIUS Server". The main area contains the following fields:

- Server IP Address Type:  IPv4,  IPv6
- Server IP Address-1: 172.16.0.1 (placeholder: xxx.xxx.xxx.xxx)
- Server IP Address-2: (placeholder: xxx.xxx.xxx.xxx)
- Server IP Address-3: (placeholder: xxx.xxx.xxx.xxx)
- Server IP Address-4: (placeholder: xxx.xxx.xxx.xxx)
- Key-1: [masked] (Range: 1 - 64 Characters)
- Key-2: (Range: 1 - 64 Characters)
- Key-3: (Range: 1 - 64 Characters)
- Key-4: (Range: 1 - 64 Characters)
- RADIUS Accounting:  Enable

A "Save" button is located at the bottom of the configuration area.

L'adresse IP doit correspondre au future serveur RADIUS et la clé à la clé qui sera créer avec le serveur RADIUS.

Ensuite dans « Wireless » et « Networks », et ajoutez un point d'accès en « WPA Enterprise » avec les paramètres suivant:

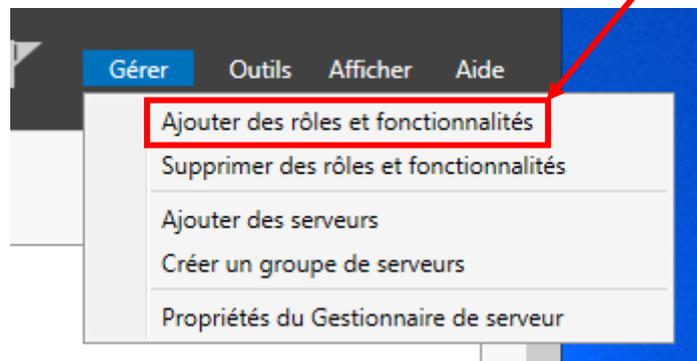
The screenshot shows the "WPA Enterprise" configuration page in a Cisco management interface. A red box highlights the top navigation bar with the following items: "199", "llot.05-Lan-2.4GHz", "WPA Enterprise", and "RADIUS". Below this, the "WPA Versions" section is expanded to show "WPA Enterprise" settings:

- WPA Versions:  WPA-TKIP,  WPA2-AES
- Enable pre-authentication
- Use global RADIUS server settings
- Server IP Address Type:  IPv4,  IPv6
- Server IP Address-1: 0.0.0.0 (placeholder: xxx.xxx.xxx.xxx)
- Server IP Address-2: (placeholder: xxx.xxx.xxx.xxx)
- Server IP Address-3: (placeholder: xxx.xxx.xxx.xxx)
- Server IP Address-4: (placeholder: xxx.xxx.xxx.xxx)
- Key-1: [masked] (Range: 1-64 Characters)
- Key-2: (Range: 1-64 Characters)
- Key-3: (Range: 1-64 Characters)

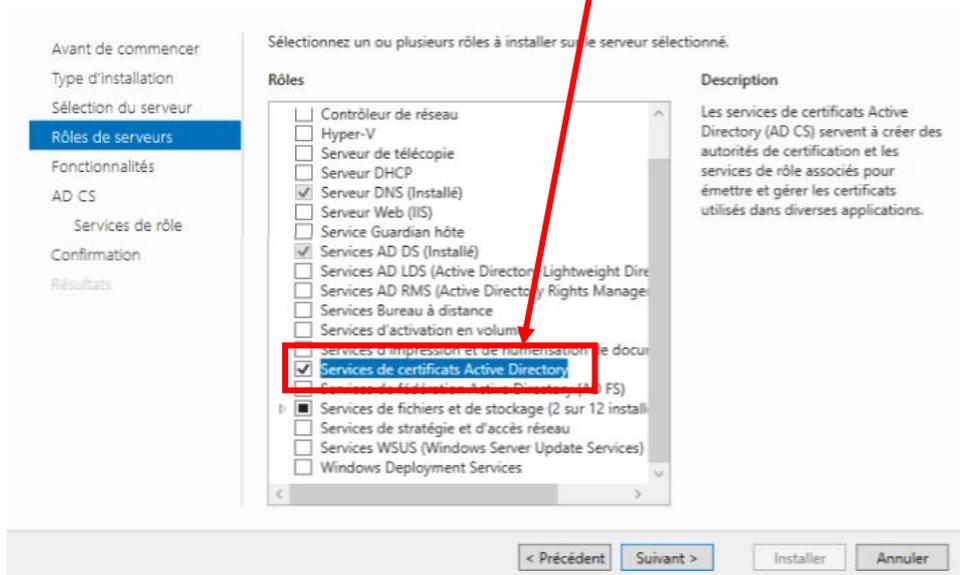
## Installation et configuration des services AD CS

Pour commencer, installer le rôle AD CS qui permet de générer un certificat pour les postes client connectés en Wifi ainsi que pour le service NPS.

Dans le gestionnaire de serveur, appuyer sur « Gérer » puis « Ajouter des rôles et des fonctionnalités »



Faire "Suivant" deux fois, puis cocher "Services de certificats Active Directory" et faire "Suivant" encore trois fois



Cocher ensuite « Autorité de certification », et faites « Suivant »

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

AD CS

**Services de rôle**

Confirmation

Résultats

Sélectionnez les services de rôle à installer pour Services de certificats Active Directory

Services de rôle

- Autorité de certification**
- Inscription de l'autorité de certification via le Web
- Répondeur en ligne
- Service d'inscription de périphérique réseau
- Service Web Inscription de certificats
- Service Web Stratégie d'inscription de certificats

Description

Une autorité de certification sert à émettre et gérer des certificats. Plusieurs autorités de certification peuvent être liées pour former une infrastructure à clé publique.

< Précédent Suivant > Installer Annuler

Cocher la case pour redémarrer automatiquement le serveur, puis faire "Installer"

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

AD CS

Services de rôle

**Confirmation**

Résultats

Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.

- Redémarrer automatiquement le serveur de destination, si nécessaire**

Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.

Outils d'administration de serveur distant

- Outils d'administration de rôles
- Outils des services de certificats Active Directory
- Outils de gestion de l'autorité de certification

Services de certificats Active Directory

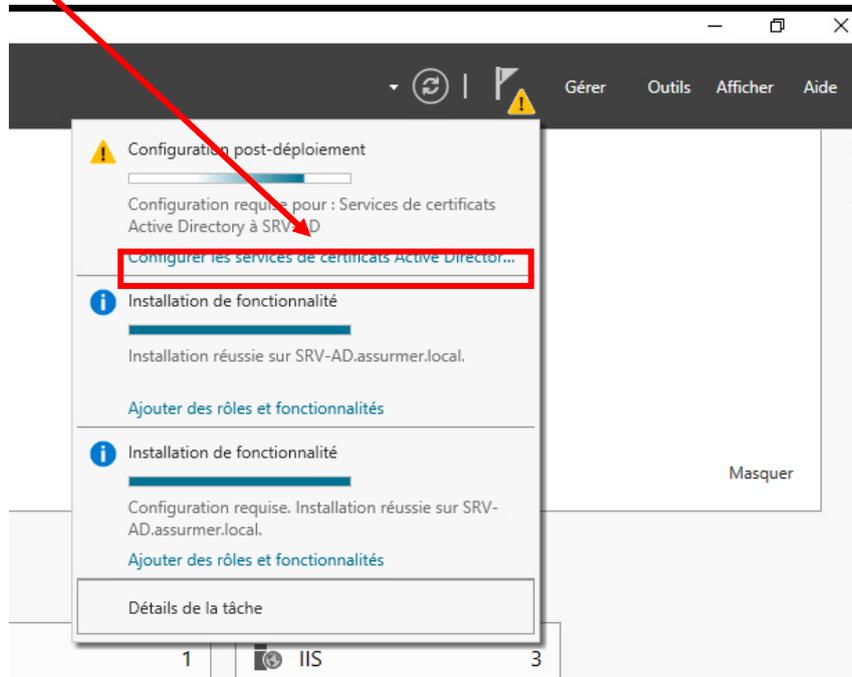
- Autorité de certification

Exporter les paramètres de configuration

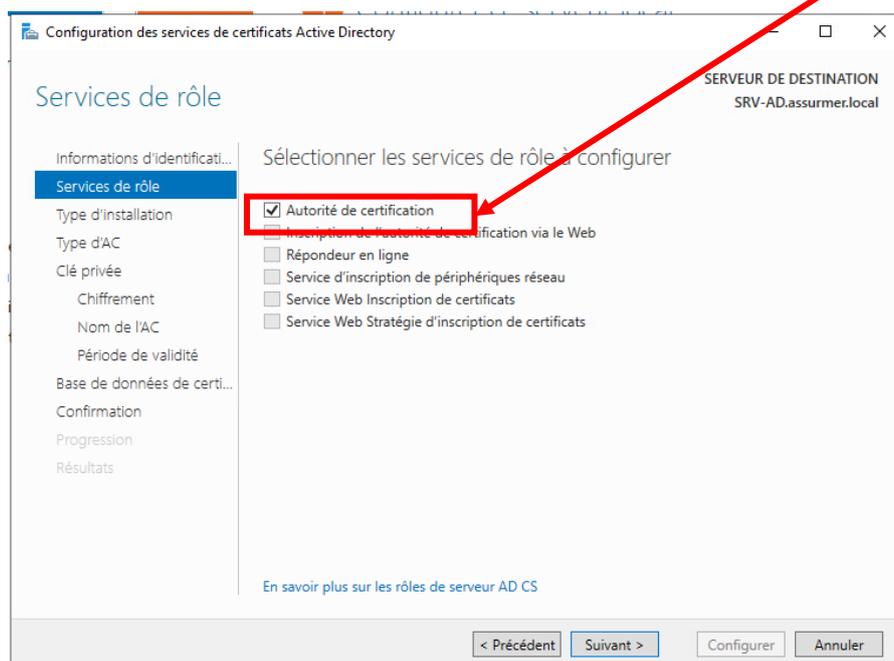
Spécifier un autre chemin d'accès source

< Précédent Suivant > Installer Annuler

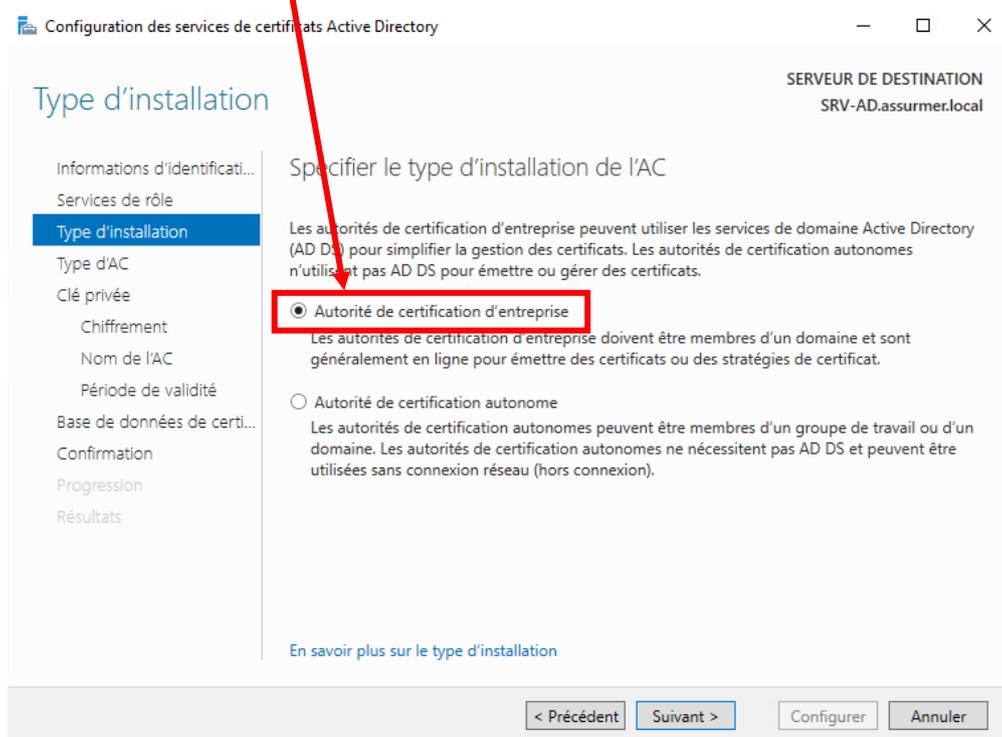
Une fois l'installation finie, retournez sur le Gestionnaire de serveur et cliquez sur « Configurer les services de certificats AD »



Faire "Suivant" une fois en laissant les paramètres par défaut, puis cocher "Autorité de certification" et continuer.

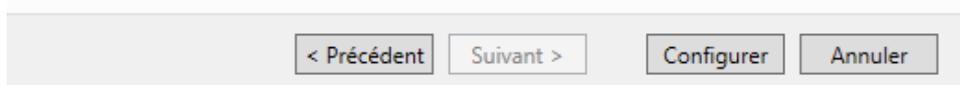


Cocher « Autorité de certification d'entreprise » puis faire « Suivant »



Faire « Suivant » en laissant les paramètres par défaut sur chaque étape.

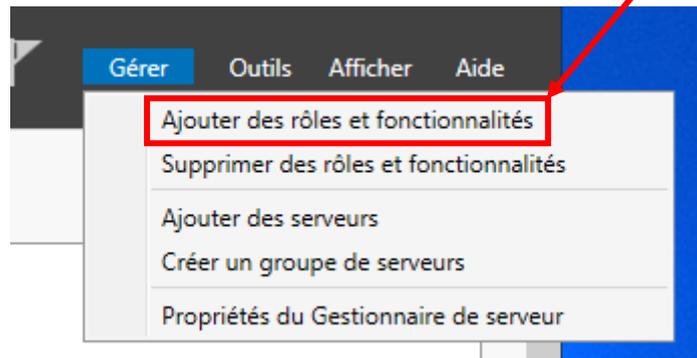
Une fois arrivé à l'étape « Confirmation », cliquez simplement sur « Configurer »



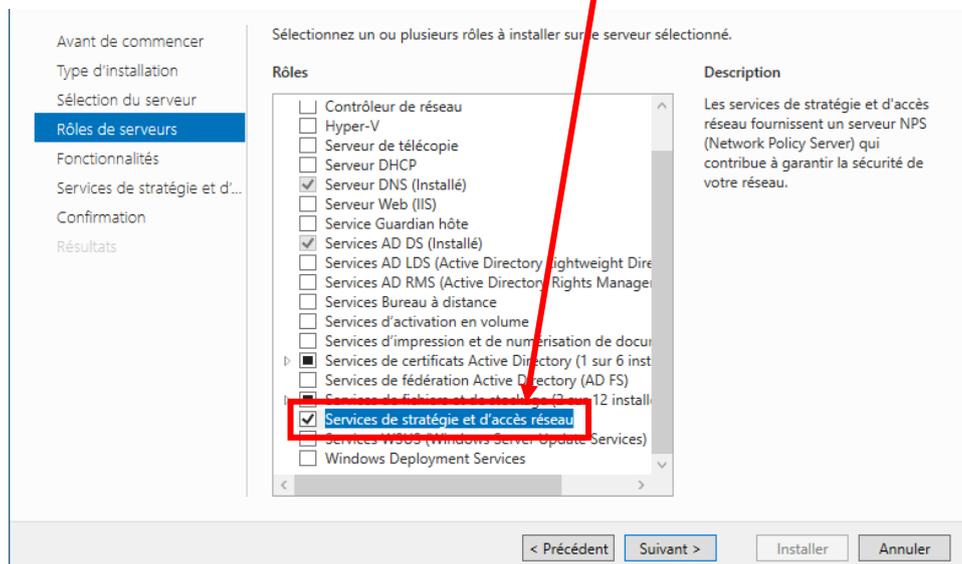
La configuration de l'ADCS est désormais finie.

## Installation et configuration du service NPS (RADIUS)

Dans le gestionnaire de serveur, appuyer sur « Gérer » puis « Ajouter des rôles et des fonctionnalités »

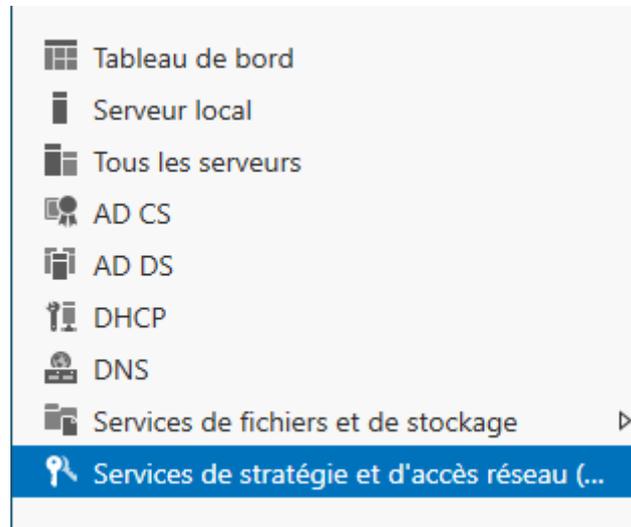


Faire « Suivant » deux fois, puis cocher « Services de stratégie et d'accès réseau »

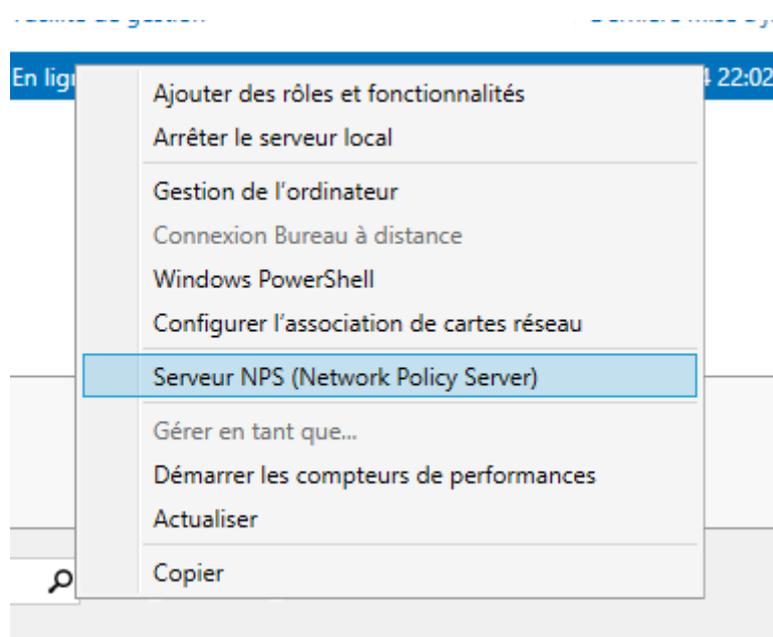


Faire « Suivant » jusqu'à l'installation du service.

Cliquer sur « Services de stratégie et d'accès réseau »



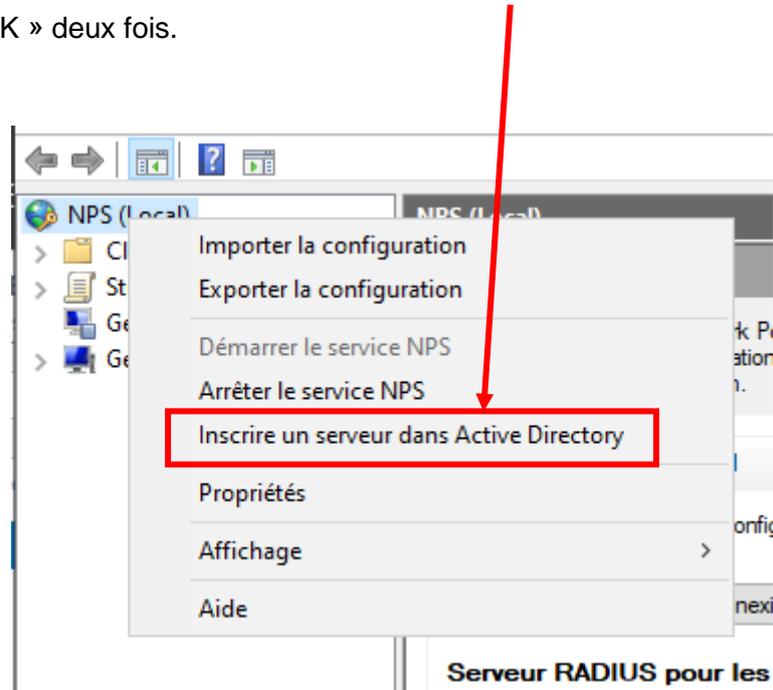
Faire un clic droit sur le serveur, puis cliquer sur « Serveur NPS »



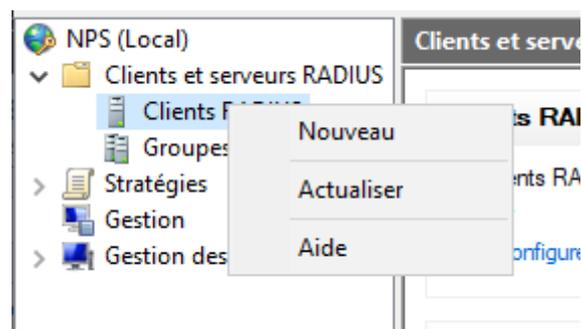
Une nouvelle fenêtre s'ouvre.

Faire clic droit sur « NPS (Local) », puis « Inscrire un serveur dans AD ».

Appuyer sur « OK » deux fois.



Ensuite, aller dans le dossier "Clients et serveurs RADIUS", faire un clic droit sur "Clients RADIUS" puis "Nouveau"



Ajouter les informations comme vu ci-dessous, puis appuyer « OK »

Propriétés de WAP731

Paramètres Avancé

Activer ce client RADIUS

Sélectionner un modèle existant :

Nom et adresse

Nom convivial : WAP731

Adresse (IP ou DNS) : 192.168.0.25 Vérifier...

Secret partagé

Sélectionnez un modèle de secrets partagés existant : Aucun

Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.

Manuel  Générer

Secret partagé : .....

Confirmez le secret partagé : .....

OK Annuler Appliquer

Aller sur « NPS (Local) », puis passer la configuration standard en « 802.1X ». Ensuite « Configurer 802.1X ».

NPS (Local)

- Clients et serveurs RADIUS
  - Clients RADIUS
  - Groupes de serveurs RA
- Stratégies
- Gestion
- Gestion des modèles

NPS (Local)

Mise en route

Le serveur NPS (Network Policy Server) vous permet de créer et de mettre en application sur l'ensemble du réseau de votre organisation des stratégies d'accès réseau portant sur l'authentification et l'autorisation des demandes de connexion.

Configuration standard

Sélectionnez un scénario de configuration dans la liste, puis cliquez sur le lien ci-dessous pour ouvrir l'Assistant Scénario.

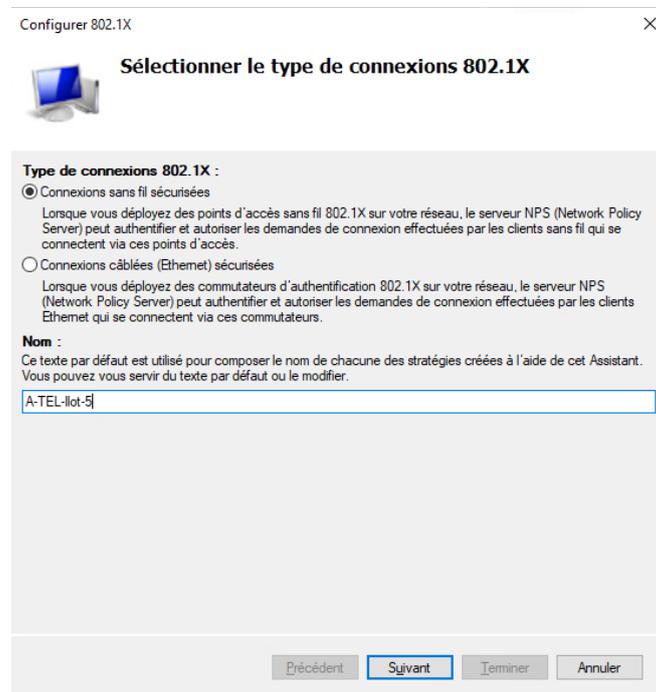
Serveur RADIUS pour les connexions câblées ou sans fil 802.1X

**Serveur RADIUS pour les connexions câblées ou sans fil 802.1X**

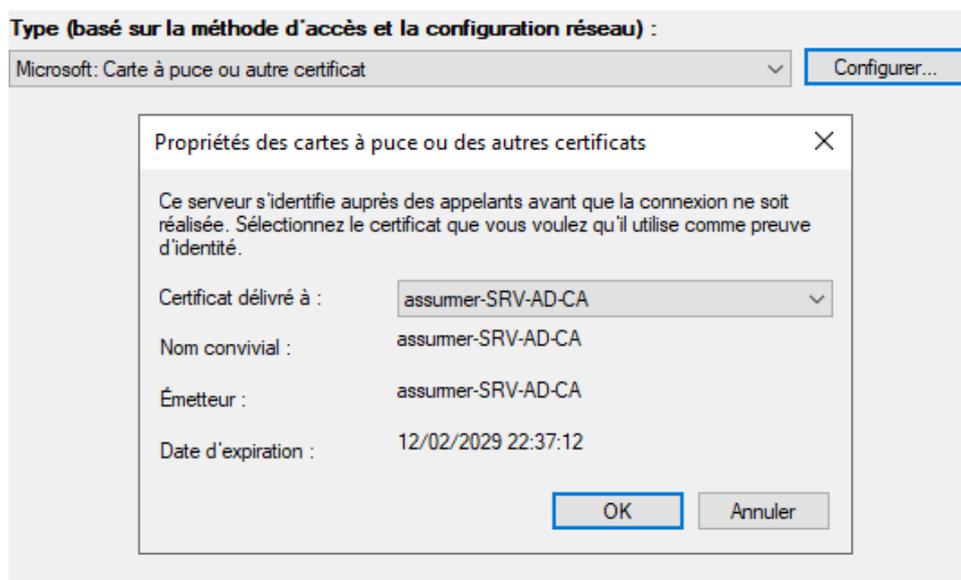
Lorsque vous configurez un serveur NPS (Network Policy Server) en tant que serveur RADIUS pour des connexions 802.1X, vous créez des stratégies réseau qui permettent au serveur NPS d'authentifier et d'autoriser les connexions provenant des points d'accès sans fil et des commutateurs d'authentification (également appelés clients RADIUS).

Configurer 802.1X Informations

Une nouvelle fenêtre s'ouvre. Cocher « Connexion sans fil sécurisées » puis donner un nom et faire "Suivant" deux fois



Cliquer sur « Configurer », puis choisir l'AD CS comme certificat et continuer



Faire « ajouter », et sélectionner le groupe “Utilisateurs du domaine”.

Appuyer “OK” puis “Suivant”

Pour sélectionner des groupes d'utilisateurs, cliquez sur Ajouter. Si aucun groupe n'est sélectionné, cette stratégie s'applique à tous les utilisateurs.

Groupes

Sélectionnez un groupe

Sélectionnez le type de cet objet :

À partir de cet emplacement :

Entrez le nom de l'objet à sélectionner (exemples) :

Refaites « Suivant » une fois, puis « Terminer »

Configurer 802.1X

 **Fin de la configuration des nouvelles connexions câblées/sans fil sécurisées IEEE 802.1X et des clients RADIUS**

Vous avez créé les stratégies suivantes et configuré les clients RADIUS ci-dessous.

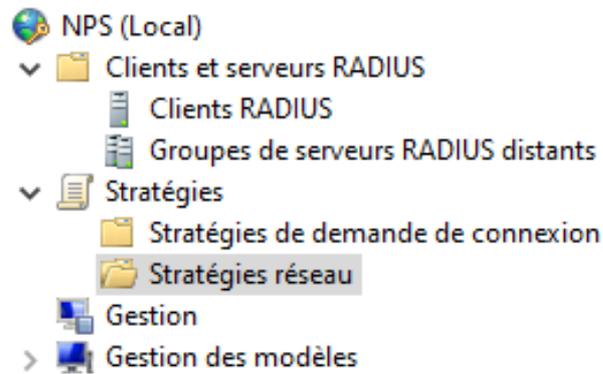
- Pour afficher les détails de la configuration dans votre navigateur, cliquez sur Détails de la configuration.
- Pour modifier la configuration, cliquez sur Précédent.
- Pour enregistrer la configuration et fermer cet Assistant, cliquez sur Terminer.

**Stratégie de demande de connexion :**  
A-TEL-Ilot-5

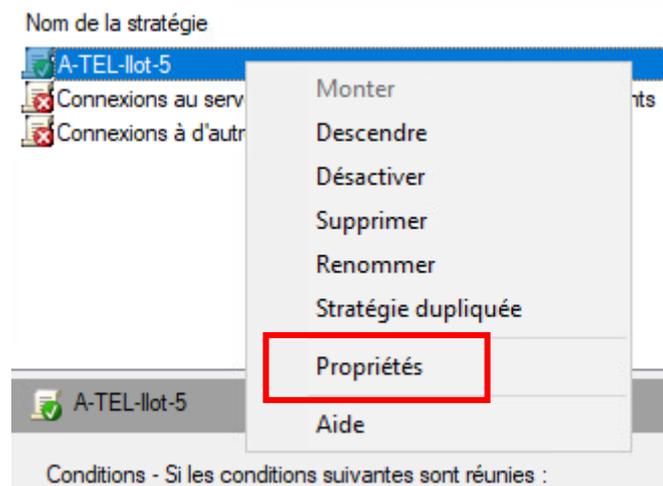
**Stratégies réseau :**  
A-TEL-Ilot-5

[Détails de la configuration](#)

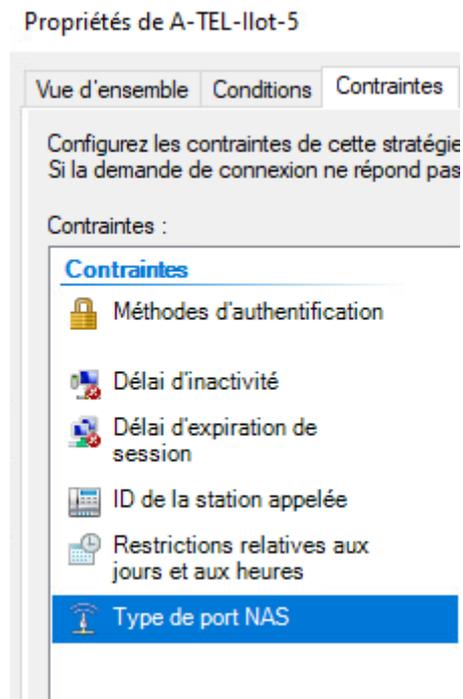
Aller dans “Stratégies”, et “Stratégies réseau”



Faire un clic droit puis “Propriétés” sur “WI-FI\_TEST”



Dans « Contraintes » puis « Type de port NAS »,



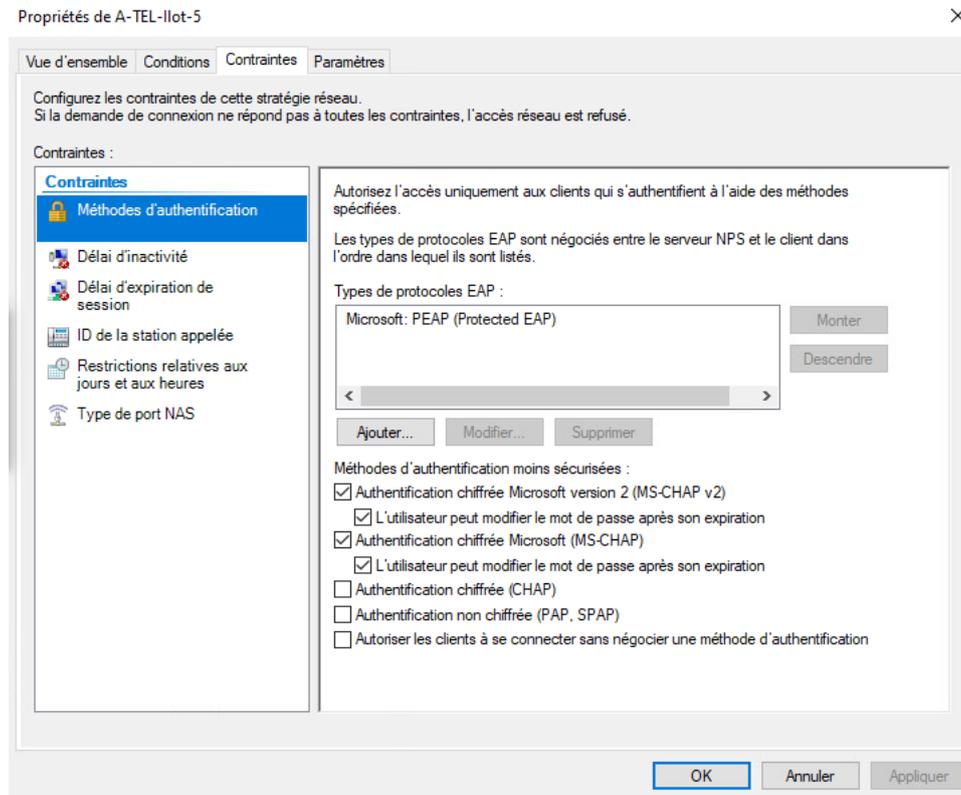
Cocher "Sans fil – IEEE 802.11" dans "Types de tunnels 802.1X" et "Sans fil – Autre" dans "Autres"

Types de tunnels pour connexions 802.1X standard	
<input type="checkbox"/>	Ethernet
<input type="checkbox"/>	FDDI
<input checked="" type="checkbox"/>	Sans fil - IEEE 802.11
<input type="checkbox"/>	Token Ring

Autres	
<input type="checkbox"/>	RNIS asynchrone V.120
<input type="checkbox"/>	RNIS synchrone
<input checked="" type="checkbox"/>	Sans fil - Autre
<input type="checkbox"/>	SDSL - DSL symétrique

Dans « Méthodes d'authentification », cliquer sur « Ajouter » puis sélectionner « Microsoft : PEAP (Protected EAP) »



“Appliquer” et terminer par appuyer sur “OK”.

La configuration est désormais terminée.