



Présentation & procédure d'installation de Radius :

Présentation de RADIUS :

Le serveur RADIUS possède le rôle de l'authentification, il accorde ou refuse donc les accès à la borne WIFI selon les stratégies d'authentifications mises en place

Prérequis :

- 1 Serveur Windows serveur 2019
- 1 Serveur AD
- 1 Routeur
- 1 Borne WIFI

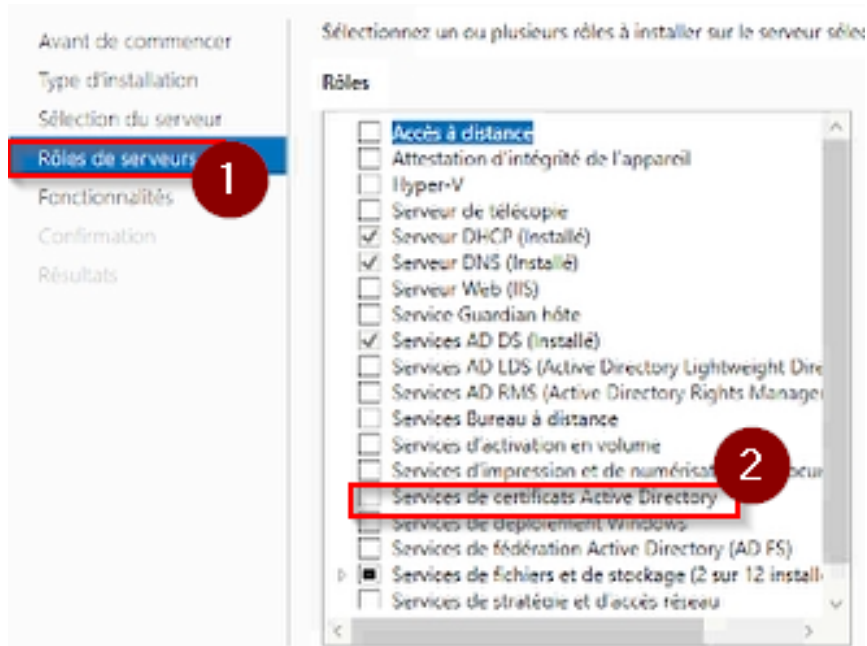
Installation de radius :

Se rendre sur le gestionnaire de serveur de serveur Windows server 2019 puis se rendre dans "gérer" puis "ajouter des rôles et fonctionnalités".

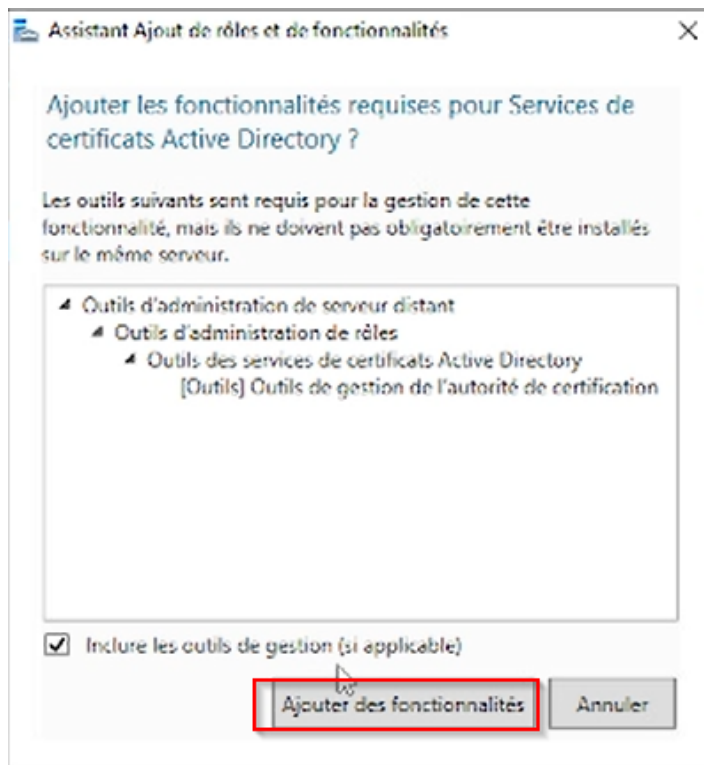




Se rendre sur “Rôles de serveurs” puis sélectionner “Services de certificats Active Directory” .

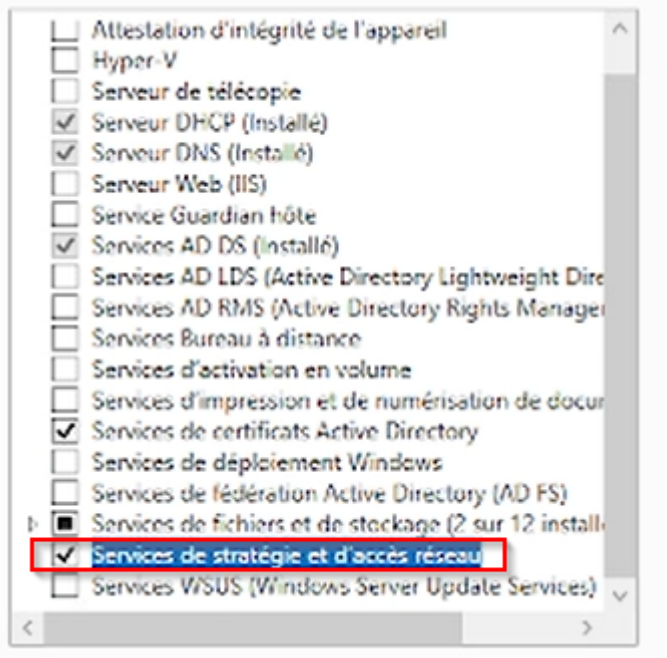


Cliquer sur “ajouter des fonctionnalités” .

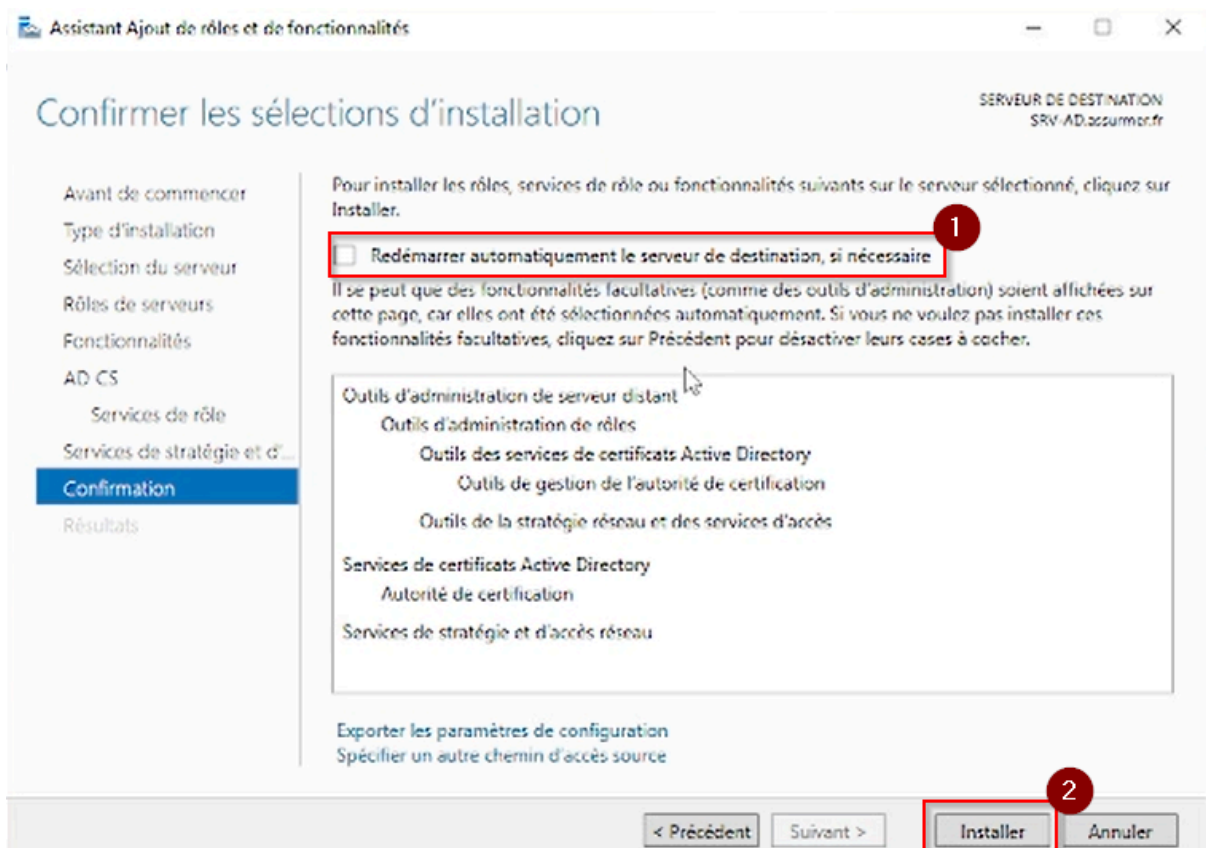




Sélectionner “Services de stratégies d'accès réseau”.



Cliquer sur “suivant” jusqu’à avoir cette page et cliquer sur “redémarrer automatiquement le serveur de destination, si nécessaire” puis cliquer sur “installer”.





Une fois l'installation terminée cliquer sur "fermer".

Assistant Ajout de rôles et de fonctionnalités

Progression de l'installation

SERVEUR DE DESTINATION
SRV-AD.assumer.fr

- Avant de commencer
- Type d'installation
- Sélection du serveur
- Rôles de serveurs
- Fonctionnalités
- AD CS
 - Services de rôle
 - Services de stratégie et d'...
 - Confirmation
 - Résultats**

Afficher la progression de l'installation

i Installation de fonctionnalité

Configuration requise. Installation réussie sur SRV-AD.assumer.fr.

Services de certificats Active Directory
Des étapes supplémentaires sont nécessaires pour la configuration des services de certificats Active Directory sur le serveur de destination.
Configurer les services de certificats Active Directory sur le serveur de destination

Autorité de certification

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
- Outils de la stratégie réseau et des services d'accès

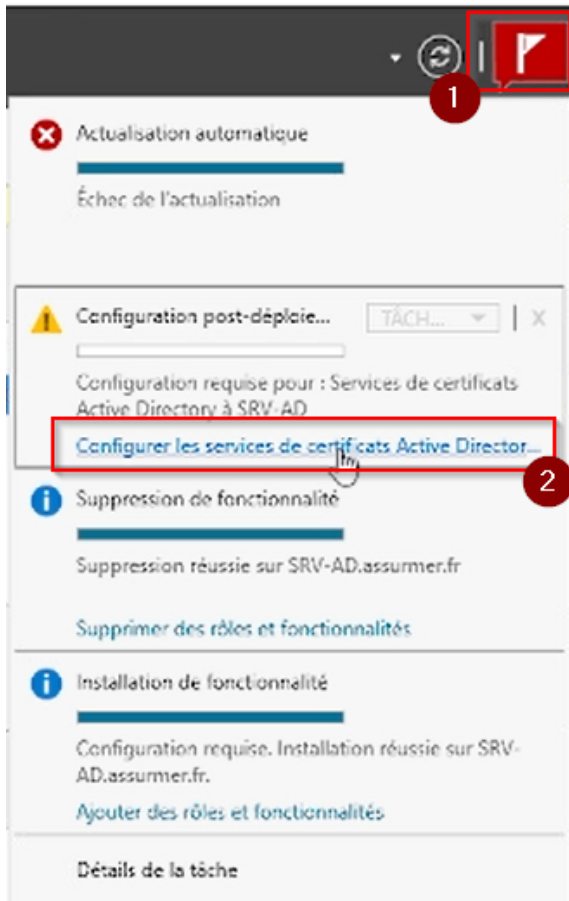
i Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.

Exporter les paramètres de configuration

< Précédent Suivant > **Fermer** Annuler



Se rendre sur le logo du drapeau puis cliquer sur “configurer les services de certificats Active Directory”.





Cliquer sur "suivant".

Configuration des services de certificats Active Directory

Informations d'identification

SERVEUR DE DESTINATION
SRV-AD.assumer.fr

Informations d'identificat...

Services de rôle

Confirmation

Progression

Résultats

Spécifier les informations d'identification pour configurer les services de rôle

Pour installer les services de rôle suivants, vous devez être membre du groupe Administrateurs local :

- Utiliser l'autorité de certification autonome
- Inscription de l'autorité de certification via le Web
- Répondeur en ligne

Pour installer les services de rôle suivants, vous devez être membre du groupe Administrateurs d'entreprise :

- Autorité de certification d'entreprise
- Service Web Stratégie d'inscription de certificats
- Service Web Inscription de certificats
- Service d'inscription de périphériques réseau

Informations d'identification : ASSURMER\Administrateur

Modifier...

En savoir plus sur les rôles de serveur AD CS

< Précédent

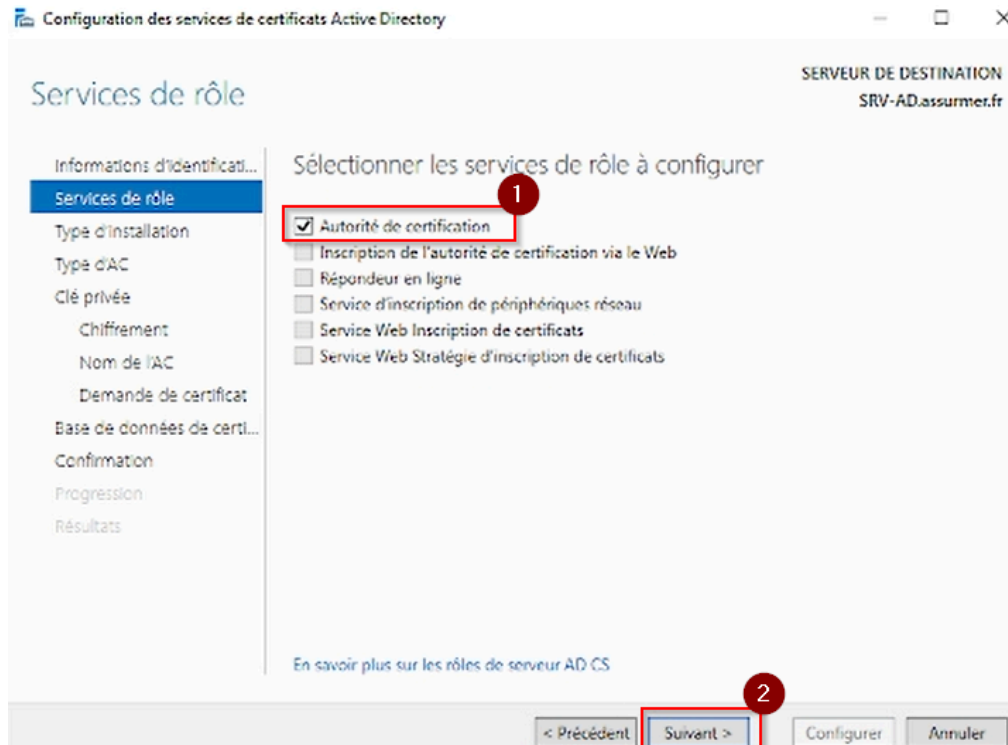
Suivant >

Configurer

Annuler



Sélectionner “Autorité de certification” puis cliquer sur “suivant”.





Sélectionner “Autorité de certification d’entreprise” et cliquer sur “suivant”.

Configuration des services de certificats Active Directory

SERVEREUR DE DESTINATION
SRV-AD.assumer.fr

Type d'installation

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Demande de certificat
Base de données de certi...
Confirmation
Progression
Résultats

Spécifier le type d'installation de l'AC

Les autorités de certification d'entreprise peuvent utiliser les services de domaine Active Directory (AD DS) pour simplifier la gestion des certificats. Les autorités de certification autonomes n'utilisent pas AD DS pour émettre ou gérer des certificats.

- Autorité de certification d'entreprise**
Les autorités de certification d'entreprise doivent être membres d'un domaine et sont généralement en ligne pour émettre des certificats ou des stratégies de certificat.
- Autorité de certification autonome**
Les autorités de certification autonomes peuvent être membres d'un groupe de travail ou d'un domaine. Les autorités de certification autonomes ne nécessitent pas AD DS et peuvent être utilisées sans connexion réseau (hors connexion).

En savoir plus sur le type d'installation

< Précédent **Suivant >** Configurer Annuler



Sélectionner “Autorité de certificat secondaire” et cliquer sur “suivant”.

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION
SRV-AD.assumer.fr

Type d'autorité de certification

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Demande de certificat
Base de données de certi...
Confirmation
Progression
Résultats

Spécifier le type de l'AC

Lorsque vous installez les services de certificats Active Directory (AD CS), vous créez ou étendez une hiérarchie d'infrastructure à clé publique (PKI). Une autorité de certification racine se trouve au sommet de la hiérarchie PKI et émet ses propres certificats auto-signés. Une autorité de certification secondaire reçoit un certificat de l'autorité de certification de rang plus élevé dans la hiérarchie PKI.

Autorité de certification racine
Les autorités de certification racines sont les premières voire les seules autorités de certification configurées dans une hiérarchie PKI.

Autorité de certification secondaire
Les autorités de certification secondaires nécessitent une hiérarchie PKI établie et sont autorisées à émettre des certificats par l'autorité de certification de rang plus élevé dans la hiérarchie.

En savoir plus sur le type d'autorité de certification

< Précédent **Suivant >** Configurer Annuler



Sélectionner "Créer une clé privée" et cliquer sur "suivant".

Clé privée

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Demande de certificat
Base de données de certi...
Confirmation
Progression
Résultats

SERVER DE DESTINATION
SRV-AD.assumer.fr

Spécifier le type de la clé privée

Pour générer et émettre des certificats aux clients, une autorité de certification doit posséder une clé privée.

Créer une clé privée
Utilisez cette option si vous n'avez pas de clé privée ou pour en créer une.

Utiliser la clé privée existante
Utilisez cette option pour garantir la continuité avec les certificats émis antérieurement lors de la réinstallation d'une AC.

Sélectionner un certificat et utiliser sa clé privée associée
Sélectionnez cette option s'il existe un certificat sur cet ordinateur ou pour importer un certificat et utiliser sa clé privée associée.

Sélectionner une clé privée existante sur cet ordinateur
Sélectionnez cette option si vous avez conservé les clés privées d'une installation antérieure ou pour utiliser une clé privée d'une autre source.

En savoir plus sur la clé privée

< Précédent **Suivant >** Configurer Annuler



Mettre les mêmes paramètres et cliquer sur "suivant".

Configuration des services de certificats Active Directory

Chiffrement pour l'autorité de certification

SERVEUR DE DESTINATION
SRV-AD.assumer.fr

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Demande de certificat
Base de données de certi...
Confirmation
Progression
Résultats

Spécifier les options de chiffrement

Sélectionnez un fournisseur de chiffrement : RSA#Microsoft Software Key Storage Provider Longueur de la clé : 2048

Sélectionnez l'algorithme de hachage pour signer les certificats émis par cette AC :

- SHA256
- SHA384
- SHA512
- SHA1

Autorisez l'interaction de l'administrateur lorsque l'autorité de certification accède à la clé privée.

En savoir plus sur le chiffrement

< Précédent **Suivant >** Configurer Annuler

Cliquer sur "suivant".

Configuration des services de certificats Active Directory

Nom de l'autorité de certification

SERVEUR DE DESTINATION
SRV-AD.assumer.fr

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Demande de certificat
Base de données de certi...
Confirmation
Progression
Résultats

Spécifier le nom de l'AC

Tapez un nom commun pour identifier cette autorité de certification. Ce nom est ajouté à tous les certificats émis par l'autorité de certification. Les valeurs des suffixes du nom unique sont générées automatiquement, mais elles sont modifiables.

Nom commun de cette AC :
assumer-SRV-AD-CA-2

Suffixe du nom unique :
DC=assumer,DC=fr

Aperçu du nom unique :
CN=assumer-SRV-AD-CA-2,DC=assumer,DC=fr

En savoir plus sur le nom de l'autorité de certification

< Précédent **Suivant >** Configurer Annuler



Cliquer sur "suivant".

Configuration des services de certificats Active Directory

Demande de certificat

SERVEUR DE DESTINATION
SRV-AD.assumer.fr

Informations d'identifiants...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Demande de certificat
Base de données de certi...
Confirmation
Progression
Résultats

Demander un certificat auprès d'une AC parente

Vous devez demander un certificat à une autorité de certification parente afin d'autoriser cette autorité de certification secondaire à émettre des certificats. Vous pouvez obtenir un certificat à partir d'une autorité de certification en ligne ou vous pouvez stocker votre demande dans un fichier avant de l'envoyer à l'autorité de certification parente.

Envoyer une demande de certificat à une AC parente :

Sélectionner :
 Nom de l'AC
 Nom de l'ordinateur
AC parente : Sélectionner...

Enregistrer une demande de certificat dans un fichier de l'ordinateur cible :

Nom du fichier :

i Vous devez obtenir manuellement un certificat de l'AC parente pour que cette AC soit opérationnelle.

[En savoir plus sur la demande de certificat](#)

< Précédent **Suivant >** Configurer Annuler

Cliquer sur "suivant".

Configuration des services de certificats Active Directory

Base de données de l'autorité de certification

SERVEUR DE DESTINATION
SRV-AD.assumer.fr

Informations d'identifiants...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Demande de certificat
Base de données de certi...
Confirmation
Progression
Résultats

Spécifier les emplacements des bases de données

Emplacement de la base de données de certificats :

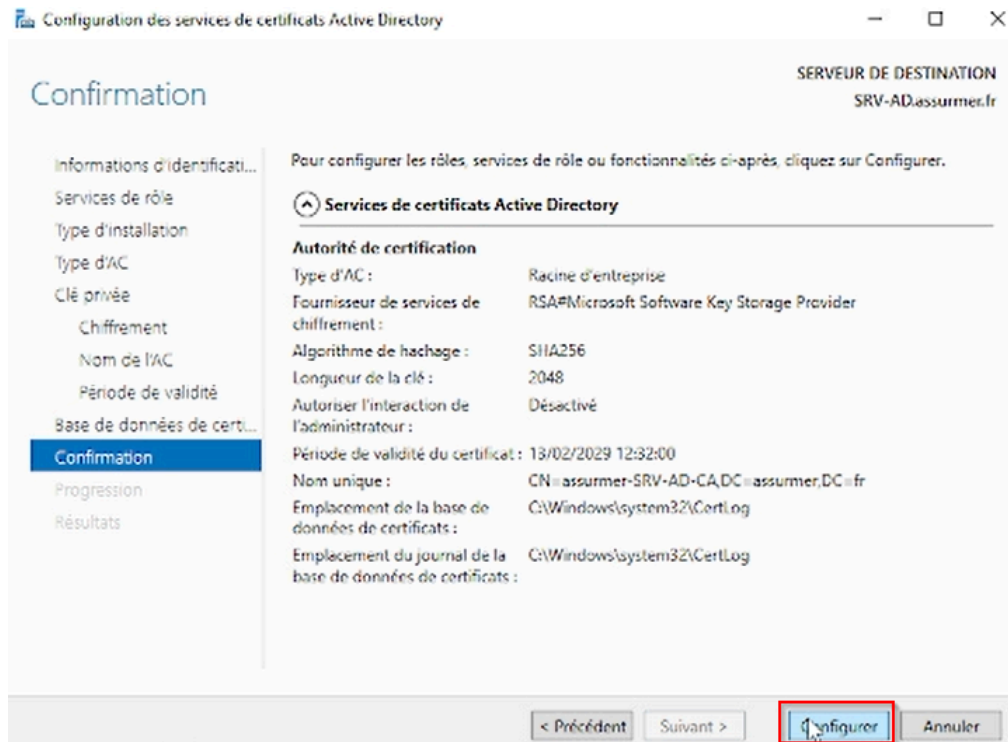
Emplacement du journal de la base de données de certificats :

[En savoir plus sur la base de données de l'autorité de certification](#)

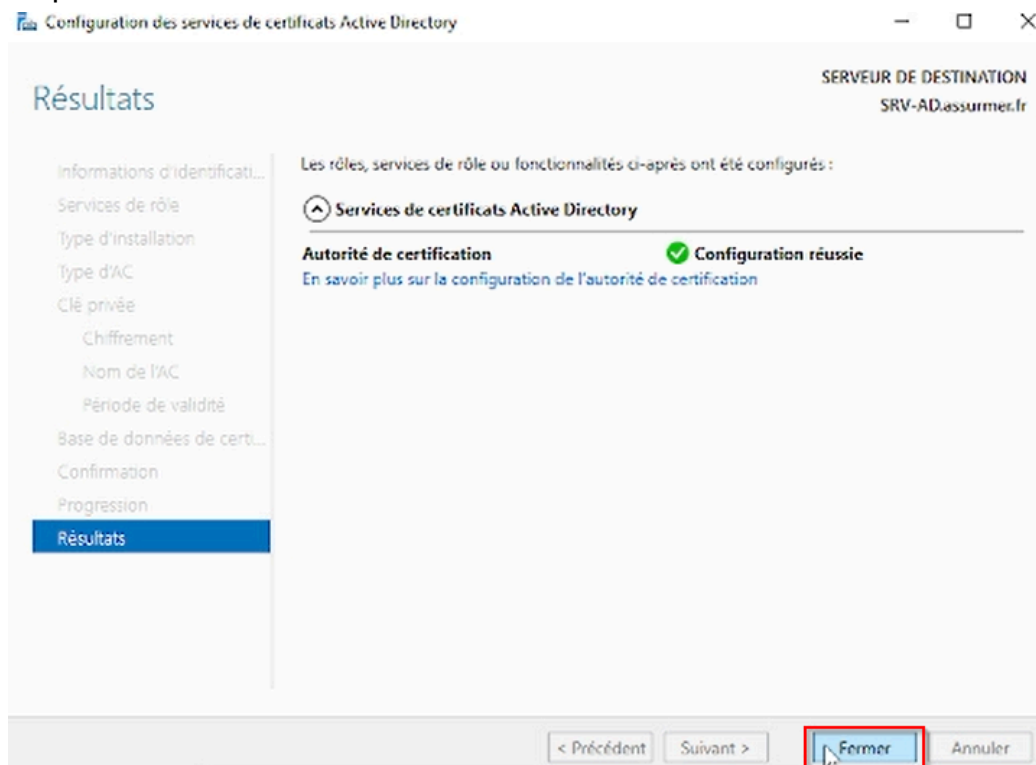
< Précédent **Suivant >** Configurer Annuler



Cliquer sur "Configurer".

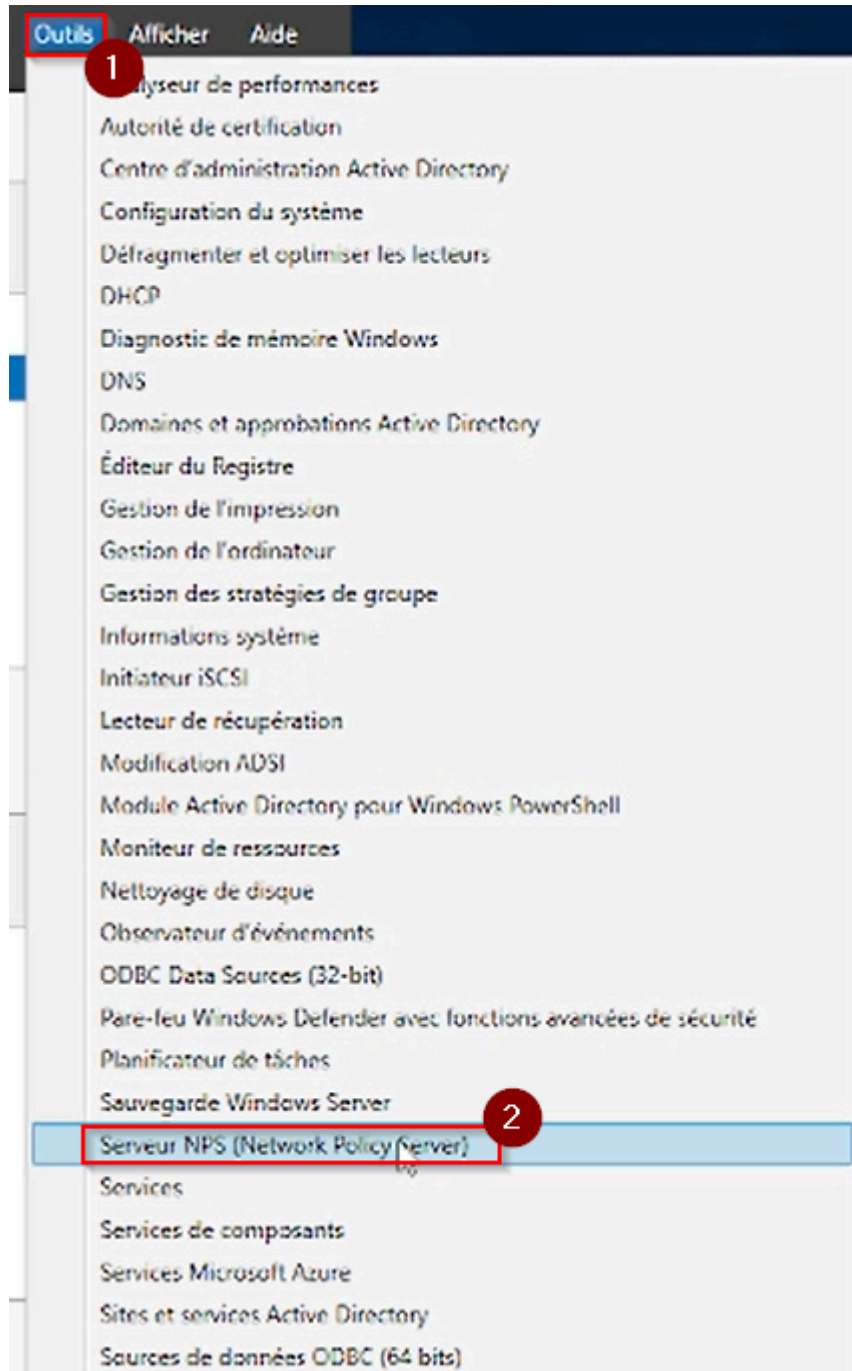


Cliquer sur "fermer".



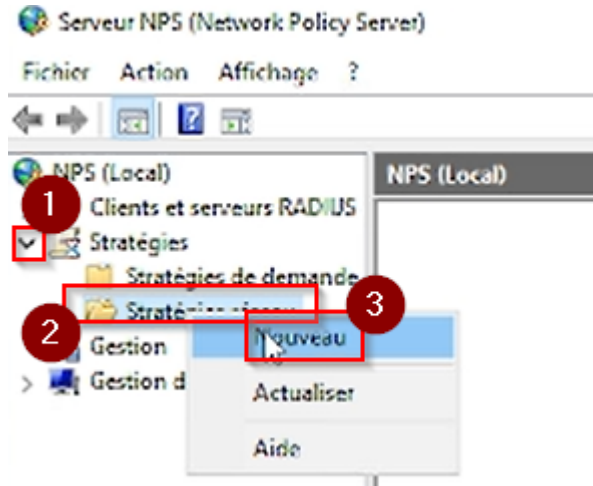


Cliquer sur "Outils" puis sur "Serveur NPS (Network Policy Server)".

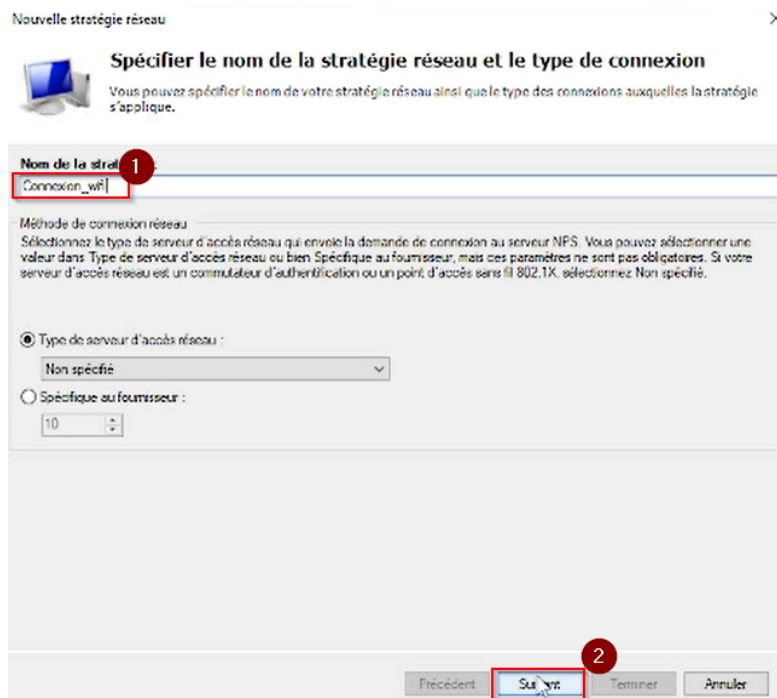




Dérouler le menu, faire un clic droit sur "Stratégie de réseau" puis cliquer sur "nouveau".

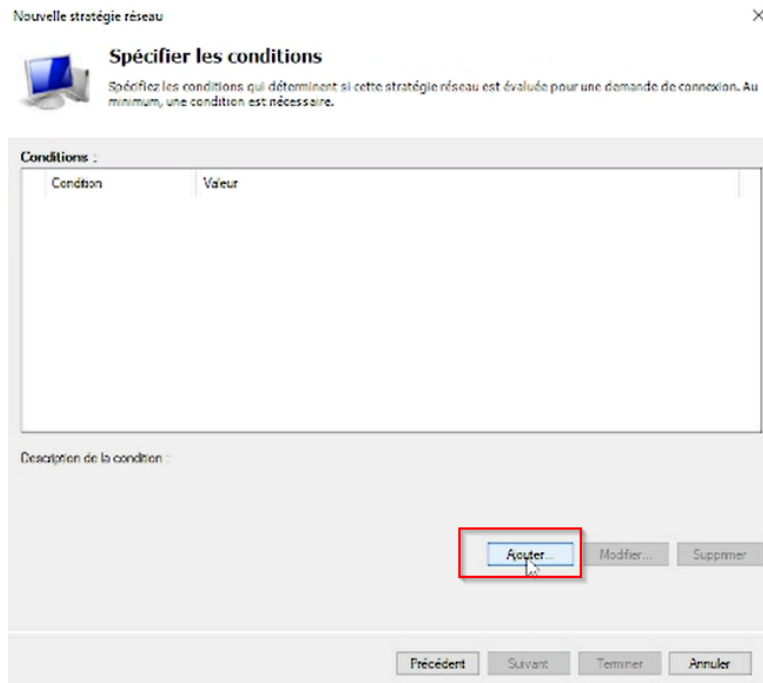


Donner un nom à la stratégie et cliquer sur "suivant".

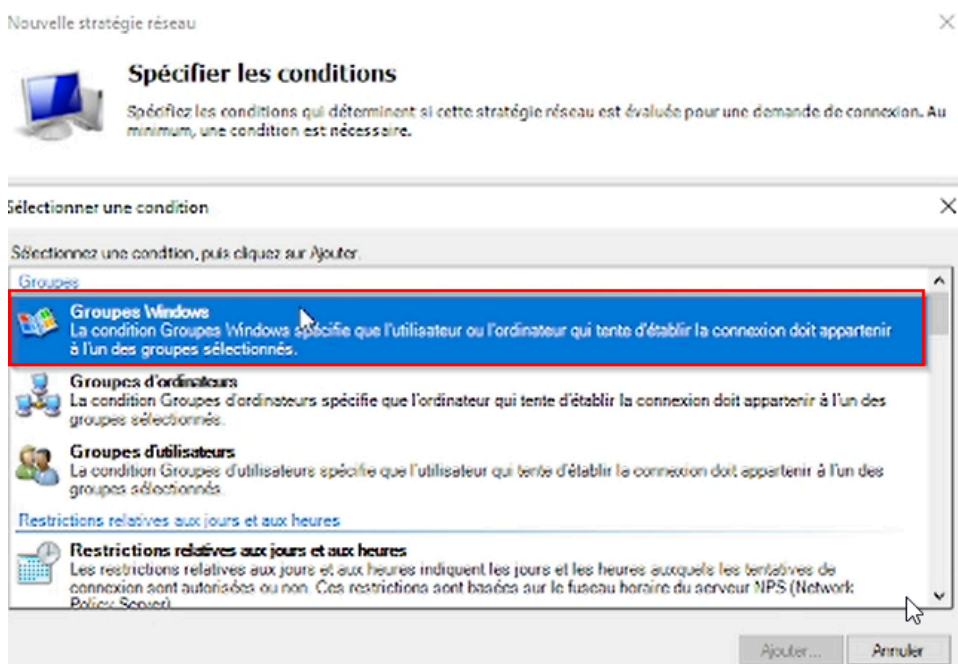




Cliquer sur "ajouter".

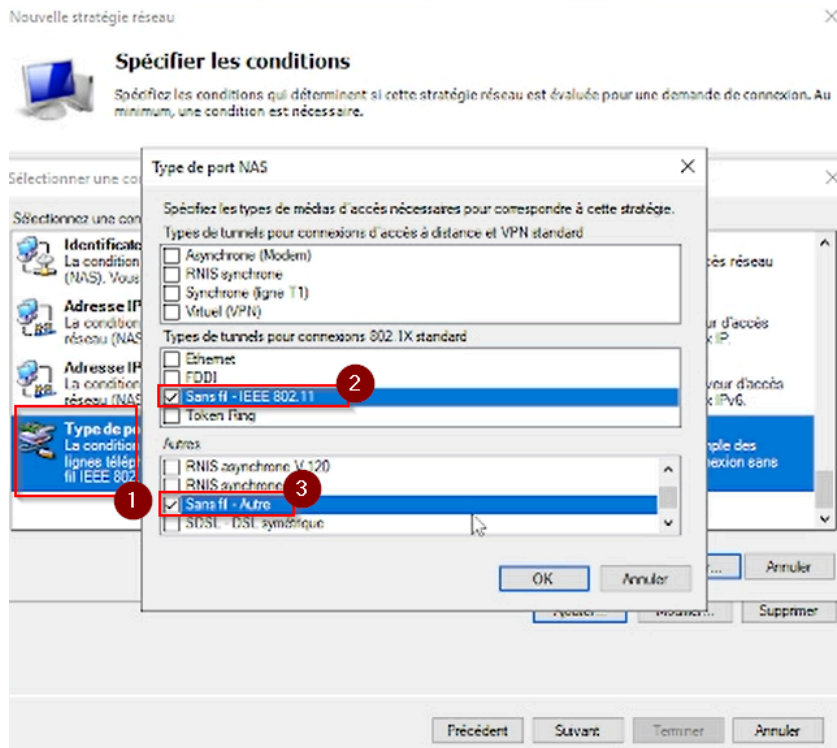


Cliquer sur "Groupe Windows" et sélectionner le groupe d'utilisateur qui pourra se connecter au WIFI.

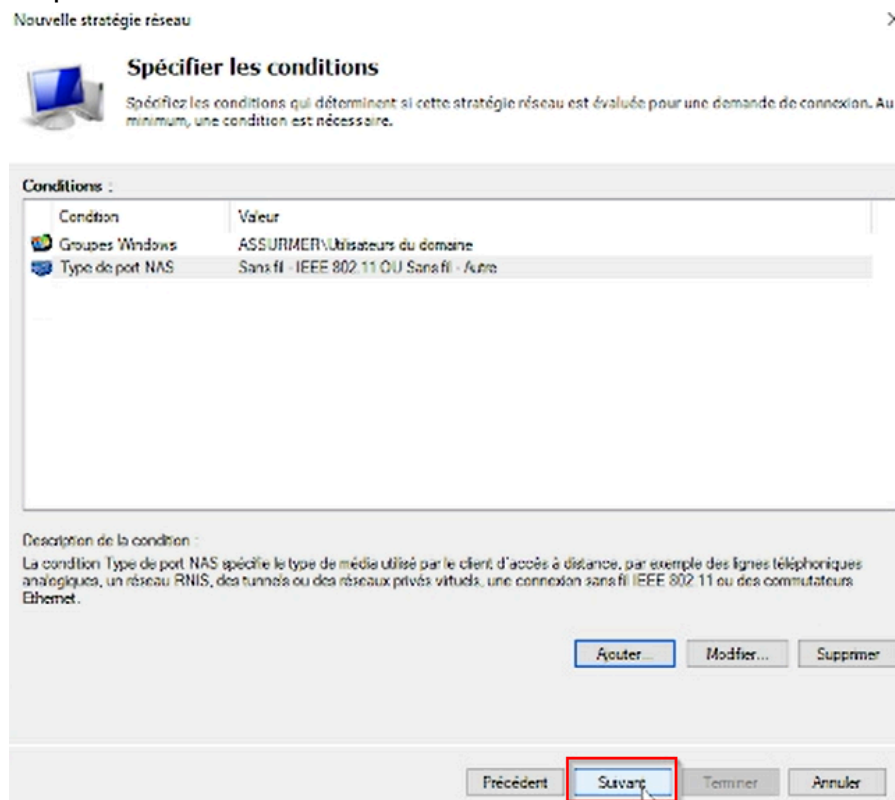




Cliquer sur “Type de port NAS” et sélectionner “Sans-fil IEEE 802.11” et “Sans-fil Autre”.



Cliquer sur “suivant”.





Cliquer sur "suivant".

Nouvelle stratégie réseau

Spécifier l'autorisation d'accès

Effectuez la configuration nécessaire pour accorder ou refuser l'accès réseau si la demande de connexion correspond à cette stratégie.

Accès accordé
Accordez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.

Accès refusé
Refusez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.

L'accès est déterminé par les propriétés de numérotation des utilisateurs (qui remplacent la stratégie NPS)
Choisissez selon les propriétés de numérotation utilisateur si les tentatives de connexion des clients répondent aux conditions de la stratégie.

Précédent **Suivant** Terminer Annuler

Cliquer sur "ajouter" puis sélectionner "Microsoft PEAP (Protected EAP)" puis cliquer sur "suivant".

Nouvelle stratégie réseau

Configurer les méthodes d'authentification

Configurez une ou plusieurs des méthodes d'authentification nécessaires pour que la demande de connexion corresponde à cette stratégie. Pour l'authentification EAP, vous devez configurer un type EAP.

Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.

Types de protocoles EAP :

1 Ajouter

Ajouter des protocoles EAP

Méthodes d'authentification :

- Microsoft: Carte à puce ou autre...
- 2** Microsoft: PEAP (Protected EAP)
- Microsoft: Mot de passe/gourde (EAP-MSCHAP version 2)

OK Annuler

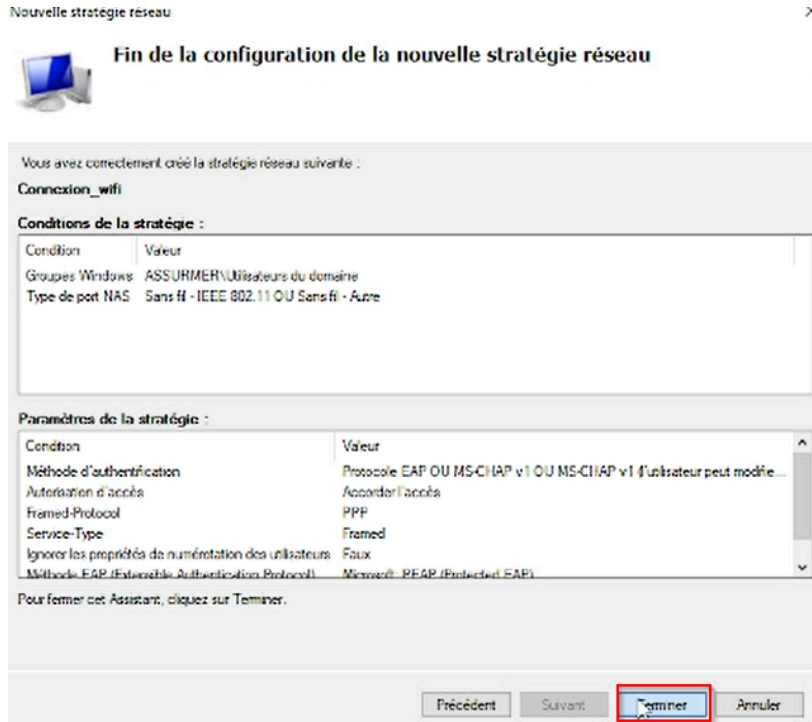
Méthodes d'authentification

- Authentification chiffrée Microsoft
- L'utilisateur peut modifier le mot de passe après sa connexion
- Authentification chiffrée Microsoft
- L'utilisateur peut modifier le mot de passe après sa connexion
- Authentification chiffrée (CIAP)
- Authentification non chiffrée (PAP, SPAP)
- Autoriser les clients à se connecter sans négocier une méthode d'authentification.

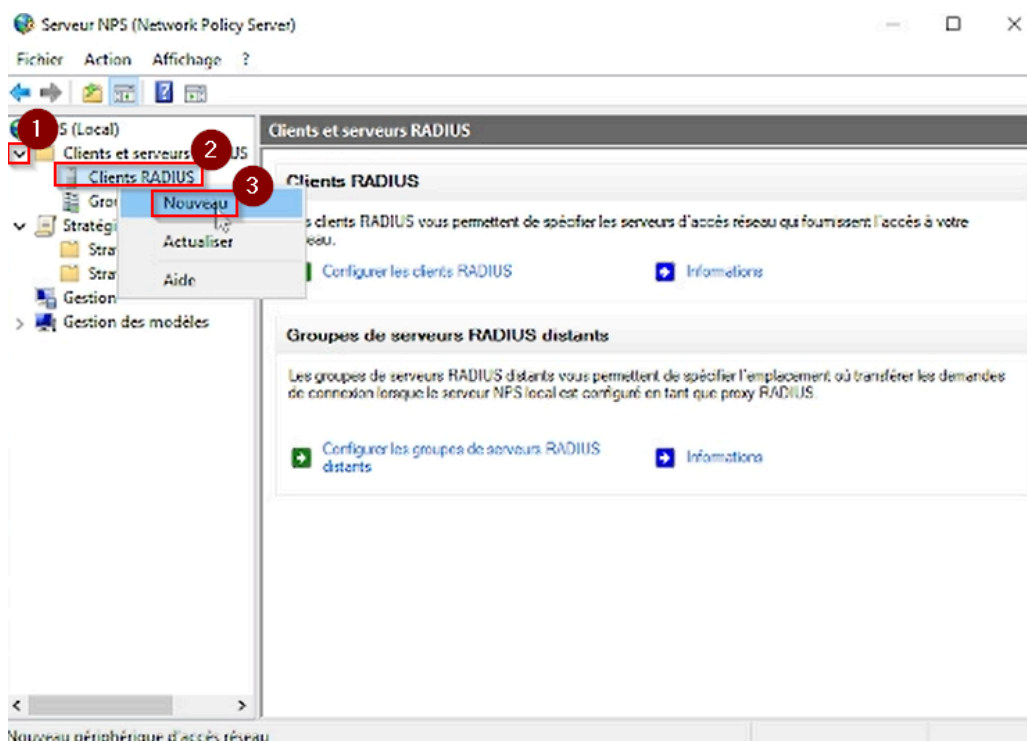
Précédent **3** Suivant Terminer Annuler



Cliquer sur “suivant” jusqu’à arriver à cette fenêtre et cliquer sur “terminer”.



Dérouler le menu et faire un clic droit sur “client RADIUS” et cliquer sur “Nouveau”.





Mettre un nom, ainsi que l'IP de la borne WI-FI et créer un mot de passe robuste.

Nouveau client RADIUS

Paramètres Avancé

Activer ce client RADIUS

Sélectionner un modèle existant :

Nom et adresse

Nom convivial
Borne_01

Adresse (IP ou DNS) :
172.16.0.10

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

Se rendre sur la page de configuration de la borne, aller dans la catégorie "RADIUS SERVER" et rentrer l'ip du serveur RADIUS ainsi que le mot de passe robuste en laissant le port par défaut et cliquer sur SAVE

Getting Started
Run Setup Wizard
Status and Statistics
Administration
LAN
Wireless
system Security
RADIUS Server
802.1X Supplicant
Password Complexity
WPA-PSK Complexity
Quality of Service
ACL
SNMP

RADIUS Server

Server IP Address Type: IPv4 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	172.16.0.1	1812
2			1812
3			1812
4			1812

Enable RADIUS Accounting

Save