

**ASSURMER**



ASSURMER

# PROCEDURE DE CONFIGURATION DE RADIUS

Bruno LEVESQUE & Ugo BERNARD

BTS SIO SISR 2B

Réf :	ASSURMER/PROCEDURE/AP8	Doc :	PROCEDURE AP8
Resp.	LEVESQUE, BERNARD	Date :	08/01/2025

## PROCEDURE DE CONFIGURATION DE RADIUS

### ÉTAT DU DOCUMENT

Validé
  En cours de validation
  En projet
  Périmé

### LISTE DES REVISIONS

Version	Date	Auteur	Description de la révision	Page
1	08/01/2024	Bruno Levesque	Création du document et détail de la configuration	14

### REDACTEURS ET APPROBATEURS

	Nom	Fonction	Visa
<b>Rédacteurs</b>	LEVESQUE Bruno Ugo BERNARD	Techniciens Systèmes et Réseaux	OK
<b>Approbateurs &amp; Signataires</b>	Mme MONSIRE Claire Mr DEGEN Loïc	DSI	
<b>Lecteur</b>	LEVESQUE Bruno Ugo BERNARD	Techniciens Systèmes et Réseaux	OK

Réf :	ASSURMER/PROCEDURE/AP8	Doc :	PROCEDURE AP8
Resp.	LEVESQUE, BERNARD	Date :	08/01/2025

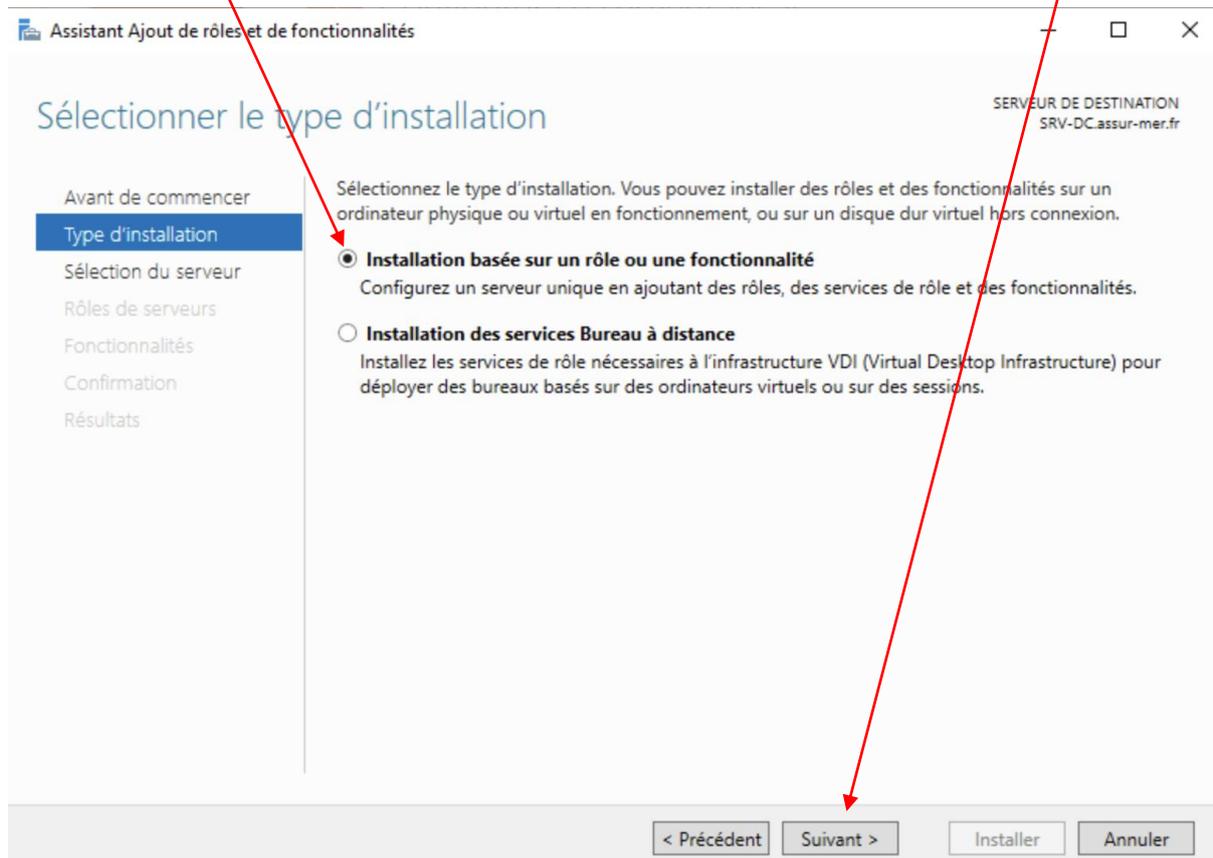
## Table des matières

1.	<b>INSTALLATION DE RADIUS SUR WINDOWS SERVER 2022</b>	<b>3</b>
2.	<b>CONFIGURATION DE LA SOLUTION RADIUS (NPS)</b>	<b>5</b>
3.	<b>MISE EN PLACE DU CERTIFICAT D'AUTHENTIFICATION</b>	<b>10</b>

Réf :	ASSURMER/PROCEDURE/AP8	Doc :	PROCEDURE AP8
Resp.	LEVESQUE, BERNARD	Date :	08/01/2025

## 1. INSTALLATION DE RADIUS SUR WINDOWS SERVER 2022

Sur le gestionnaire de serveur, rendez-vous sur « Ajouter des rôles et des fonctionnalités » et sélectionnez « Installation basée sur un rôle ou une fonctionnalité », enfin, cliquez sur « Suivant ».



Réf :	ASSURMER/PROCEDURE/AP8	Doc :	PROCEDURE AP8
Resp.	LEVESQUE, BERNARD	Date :	08/01/2025

Maintenant, **cliquez** sur « Services de Stratégie et d'accès réseau » puis sur « Suivant ».

Assistant Ajout de rôles et de fonctionnalités

Sélectionner des rôles de serveurs

SERVEUR DE DESTINATION  
SRV-DC.assur-mer.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"/> Contrôleur de réseau	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"/> Hyper-V	
<input type="checkbox"/> Serveur de télécopie	
<input checked="" type="checkbox"/> Serveur DHCP (Installé)	
<input checked="" type="checkbox"/> Serveur DNS (Installé)	
<input type="checkbox"/> Serveur Web (IIS)	
<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)	
<input type="checkbox"/> Services WSUS (Windows Server Update Services)	
<input checked="" type="checkbox"/> Windows Deployment Services (Installé)	

< Précédent Suivant > Installer Annuler

Dorénavant, le service peut être installé, cliquez sur « Installer ». Une fois l'installation terminée, vous pouvez **fermer** cette fenêtre.

Assistant Ajout de rôles et de fonctionnalités

Progression de l'installation

SERVEUR DE DESTINATION  
SRV-DC.assur-mer.fr

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

Afficher la progression de l'installation

**i** Installation de fonctionnalité

Configuration requise. Installation réussie sur SRV-DC.assur-mer.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

**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**.

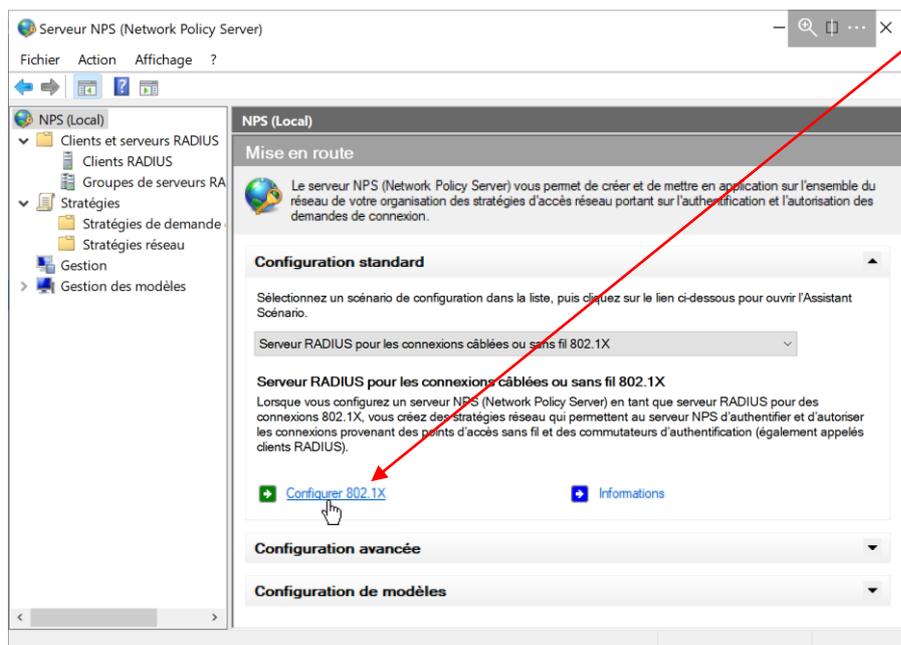
[Exporter les paramètres de configuration](#)

< Précédent Suivant > **Fermer** Annuler

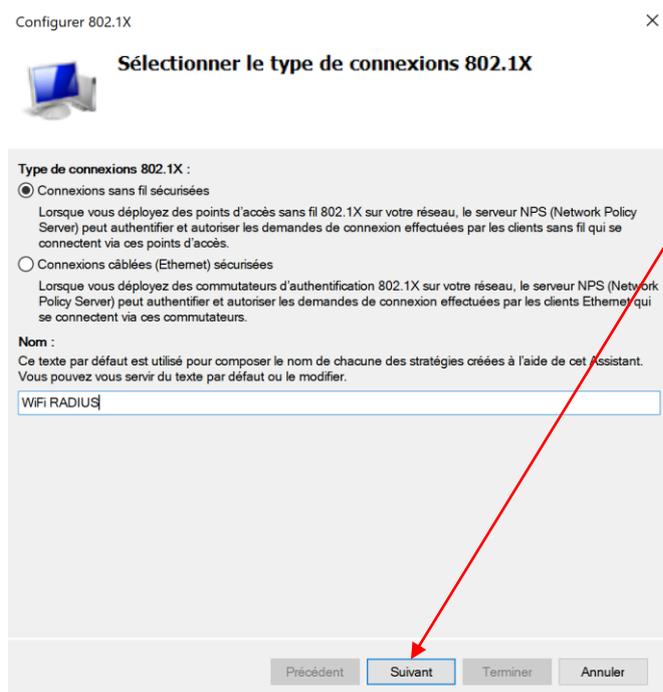
Réf :	ASSURMER/PROCEDURE/AP8	Doc :	PROCEDURE AP8
Resp.	LEVESQUE, BERNARD	Date :	08/01/2025

## 2. CONFIGURATION DE LA SOLUTION RADIUS (NPS)

Dans le gestionnaire de serveur, cliquez sur « Outils » puis ouvrez « Serveur NPS (Network Policy Server) ». Après avoir inscrit un serveur dans Active Directory, cliquez sur « Configurer 802.1X ».



Dans le champ « Nom », inscrivez le nom que vous souhaitez et cliquez sur « Suivant ».



Réf :	ASSURMER/PROCEDURE/AP8	Doc :	PROCEDURE AP8
Resp.	LEVESQUE, BERNARD	Date :	08/01/2025

Vous avez maintenant la possibilité d'ajouter un nom convivial pour votre serveur RADIUS. Renseignez le nom exact de votre borne WiFi. Renseignez également l'adresse IP de votre borne Wi-Fi. Enfin, complétez les champs « Secret partagé » avec un mot de passe robuste.

Nouveau client RADIUS X

Paramètres Avancé

Activer ce client RADIUS

Sélectionner un modèle existant :

Nom et adresse

Nom convivial :  
wapdde480

Adresse (IP ou DNS) :  
172.16.0.10 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

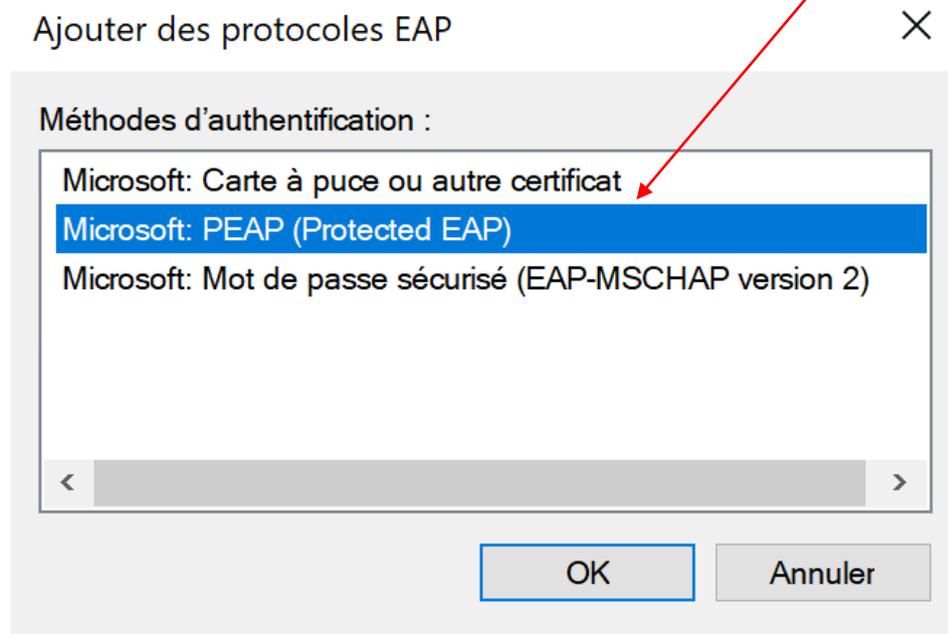
Secret partagé :  
●●●●●●●●

Confirmez le secret partagé :  
●●●●●●●●

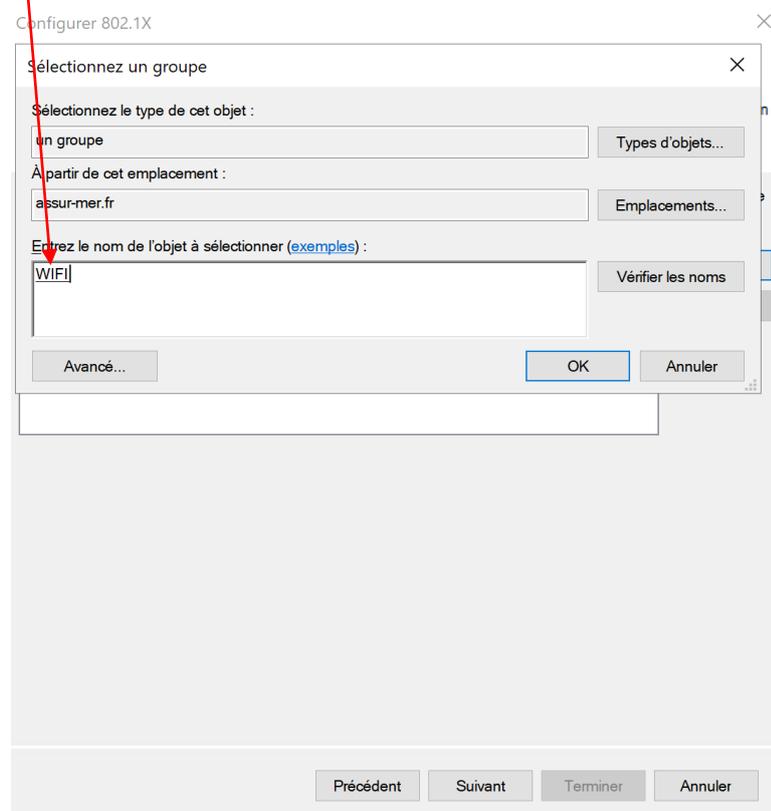
OK Annuler

Réf :	ASSURMER/PROCEDURE/AP8	Doc :	PROCEDURE AP8
Resp.	LEVESQUE, BERNARD	Date :	08/01/2025

Vous devez maintenant choisir une méthode d'authentification. Sélectionnez « Microsoft PEAP ».



Ajoutez maintenant l'Unité d'Organisation créée à cet effet pour le WiFi.



Réf :	ASSURMER/PROCEDURE/AP8	Doc :	PROCEDURE AP8
Resp.	LEVESQUE, BERNARD	Date :	08/01/2025

Les stratégies de demande et de réseau sont maintenant créées.

Stratégies réseau

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

Nom de la stratégie	État	Ordre de traitement	Type d'accès
WIFI RADIUS	Activé	1	Accorder l'accès
Connexions au serveur Microsoft de Routage et Accès distants	Activé	2	Refuser l'accès
Connexions à d'autres serveurs d'accès	Activé	3	Refuser l'accès

WIFI RADIUS

Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur
Type de port NAS	Sans fil - Autre OU Sans fil - IEEE 802.11
Groupes Windows	ASSUR-MERIWIFI

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur
-----------	--------

Stratégies de demande de connexion

Les stratégies de demande de connexion vous permettent de spécifier si les demandes de connexion sont traitées localement ou si elles sont transférées vers des serveurs RADIUS distants.

Nom de la stratégie	État	Ordre de traitement	Source
WIFI RADIUS	Activé	1	Non spécifié
Utiliser l'authentification Windows pour tous les utilisateurs	Activé	1000000	Non spécifié

Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur
-----------	--------

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur
-----------	--------

Réf :	ASSURMER/PROCEDURE/AP8	Doc :	PROCEDURE AP8
Resp.	LEVESQUE, BERNARD	Date :	08/01/2025

Dorénavant, sur la console d'administration de la borne WiFi, **renseignez** l'IP de votre serveur AD dans l'onglet « RADIUS Server » et le secret partagé.

WAP371 Wireless-AC/N Dual Radio Access Point with Single Point Setup

**RADIUS Server**

Server IP Address Type:  IPv4  IPv6

Server IP Address-1:  (xxx.xxx.xxx.xxx)

Server IP Address-2:  (xxx.xxx.xxx.xxx)

Server IP Address-3:  (xxx.xxx.xxx.xxx)

Server IP Address-4:  (xxx.xxx.xxx.xxx)

Key-1:  (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

Réf :	ASSURMER/PROCEDURE/AP8	Doc :	PROCEDURE AP8
Resp.	LEVESQUE, BERNARD	Date :	08/01/2025

### 3. MISE EN PLACE DU CERTIFICAT D'AUTHENTIFICATION

Ajoutez maintenant des services de certificats Active Directory. Dans l'onglet « Services de rôle », **cochez** « Autorité de certification ».

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION  
SRV-DC.assur-mer.fr

Services de rôle

Informations d'identificati... Sélectionner les services de rôle à configurer

Autorité de certification

Inscription de l'autorité de certification via le Web

Répondeur en ligne

Service d'inscription de périphériques réseau

Service Web Inscription de certificats

Service Web Stratégie d'inscription de certificats

En savoir plus sur les rôles de serveur AD CS

< Précédent Suivant > Configurer Annuler

Dans l'onglet « Nom de l'AC », **renseignez** les informations afin de joindre votre Active Directory puis cliquez sur « Suivant ».

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION  
SRV-DC.assur-mer.fr

Nom de l'autorité de certification

Informations d'identificati... 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 :  
assur-mer-SRV-DC-CA

Suffixe du nom unique :  
DC=assur-mer,DC=fr

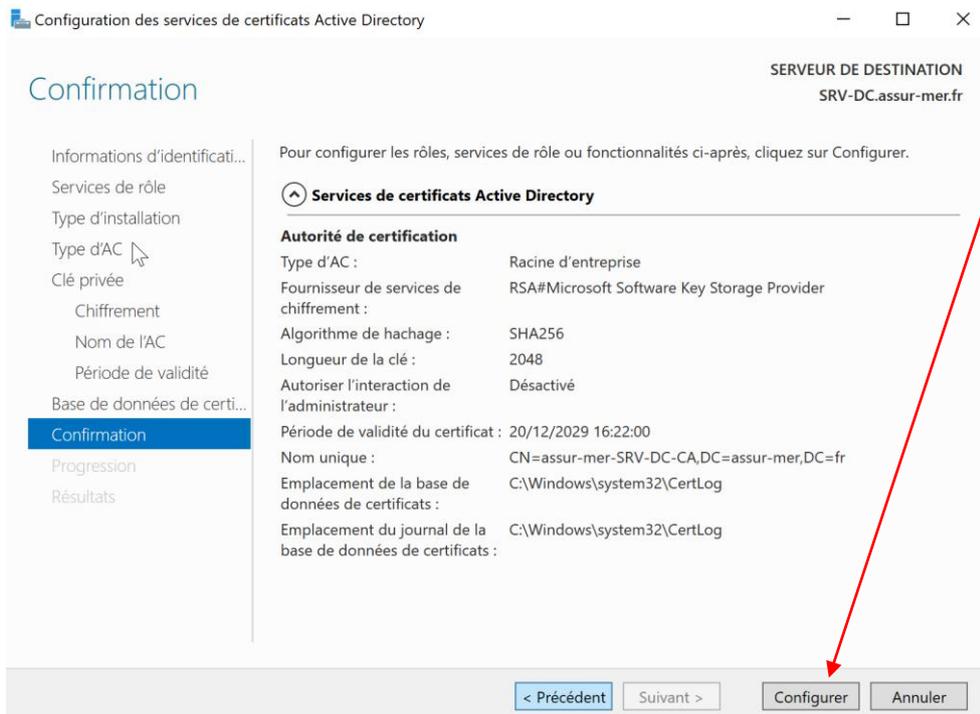
Aperçu du nom unique :  
CN=assur-mer-SRV-DC-CA,DC=assur-mer,DC=fr

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

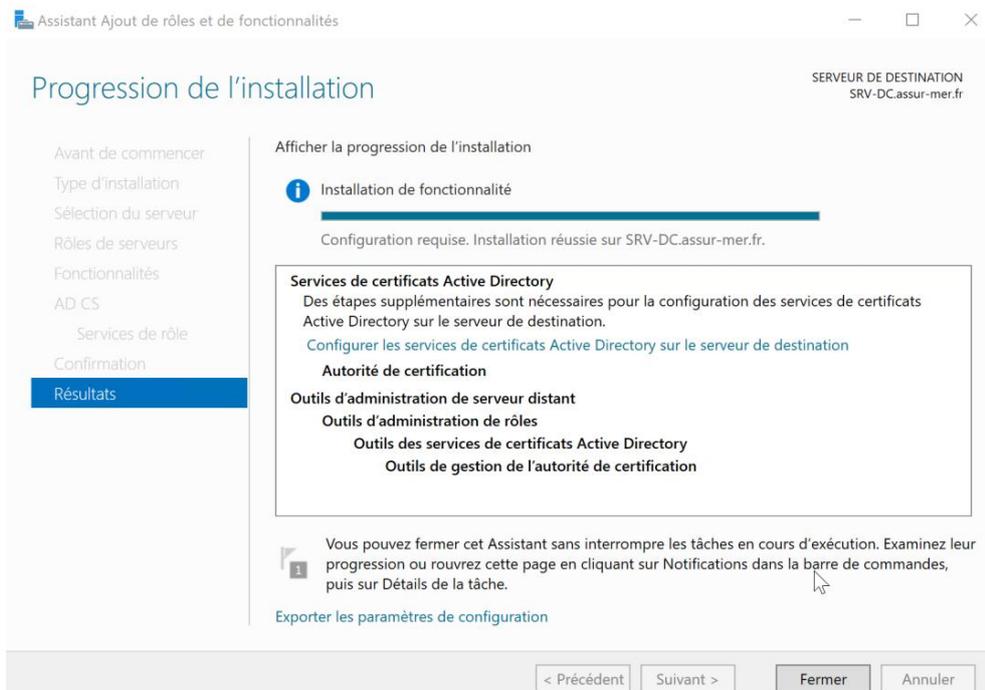
< Précédent Suivant > Configurer Annuler

Réf :	ASSURMER/PROCEDURE/AP8	Doc :	PROCEDURE AP8
Resp.	LEVESQUE, BERNARD	Date :	08/01/2025

Vérifiez maintenant les informations précédemment renseignées puis **cliquez** sur « Configurer ».

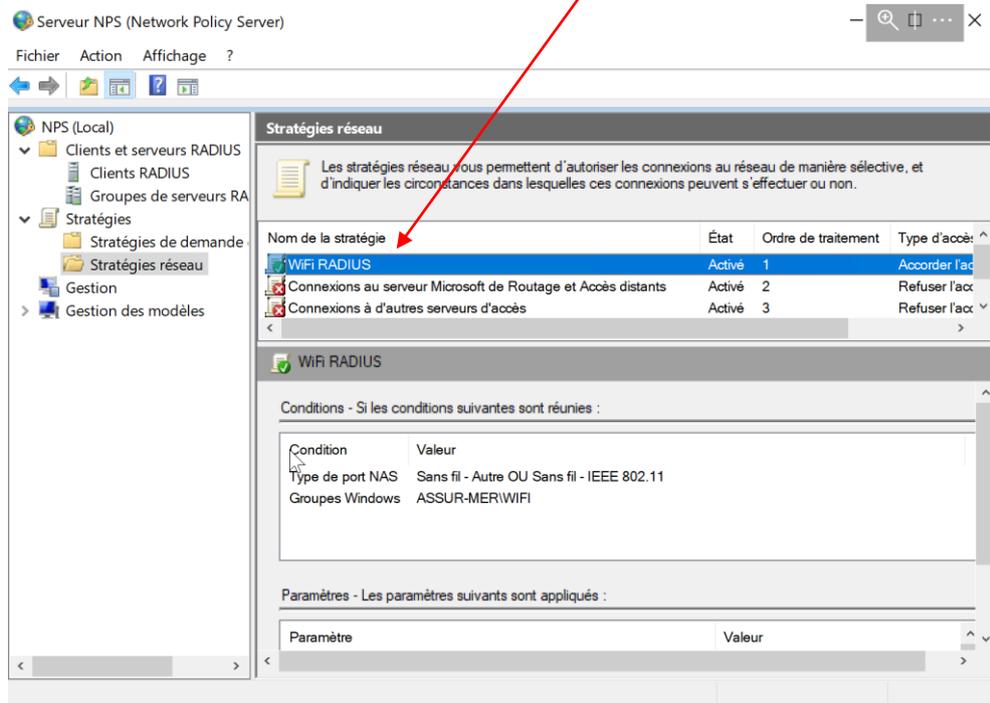


Une fois l'installation de la fonctionnalité terminée, vous pouvez fermer cette fenêtre.

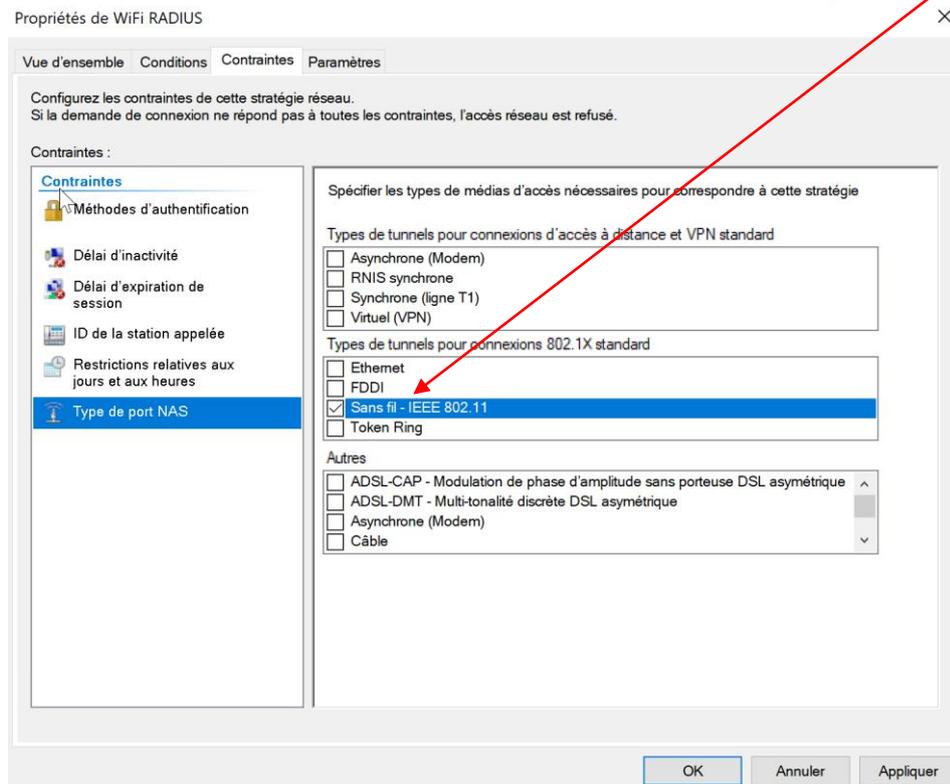


Réf :	ASSURMER/PROCEDURE/AP8	Doc :	PROCEDURE AP8
Resp.	LEVESQUE, BERNARD	Date :	08/01/2025

Retournez maintenant dans l'outil NPS, double-cliquez sur le nom de votre stratégie.



Rendez-vous maintenant dans l'onglet « Contraintes » de cette fenêtre et sélectionnez « Sans fil – IEEE 802.11 ».



Réf :	ASSURMER/PROCEDURE/AP8	Doc :	PROCEDURE AP8
Resp.	LEVESQUE, BERNARD	Date :	08/01/2025

Toujours dans l'onglet « Contraintes », dans « Méthodes d'authentification », ajoutez le type de protocole EAP, sélectionnez votre SRV-DC et cliquez sur « OK ».

Propriétés de WiFi RADIUS

Vue d'ensemble Conditions Contraintes Paramètres

Configurez les contraintes de cette stratégie réseau.  
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.

Contraintes :

**Contraintes**

- Méthodes d'authentification
- Délai d'inactivité
- Délai d'expiration de session
- ID de la station appelée
- Restrictions relatives aux jours et aux heures
- Type de port NAS

Autorisez l'accès uniquement aux clients spécifiés.

Les types de protocoles EAP sont négligés dans l'ordre dans lequel ils sont listés.

Types de protocoles EAP :

Microsoft: PEAP (Protected EAP)

Ajouter... Modifier...

Méthodes d'authentification moins sécurisées

- Authentification chiffrée Microsoft
  - L'utilisateur peut modifier le mot de passe
- Authentification chiffrée Microsoft
  - L'utilisateur peut modifier le mot de passe
- Authentification chiffrée (CHAP)
- Authentification non chiffrée (PAP)
- Autoriser les clients à se connecter

Modifier les propriétés EAP Protégé

Sélectionnez le certificat que le serveur doit utiliser comme preuve de son identité auprès du client. Un certificat configuré pour EAP Protégé dans la stratégie de demande de connexion remplacera ce certificat.

Certificat délivré à : SRV-DC.assur-mer.fr

Nom convivial : SRV-DC.assur-mer.fr

Émetteur : assur-mer-SRV-DC-CA

Date d'expiration : 20/12/2025 16:15:36

Activer la reconnexion rapide  
 Déconnecter les clients sans chiffrement forcé

Types EAP

Mot de passe sécurisé (EAP-MSCHAP version 2)

Monter Descendre

Ajouter Modifier Supprimer OK Annuler

OK Annuler Appliquer

Enfin, nous pouvons voir que le certificat est valide pour une durée certaine.

Propriétés des cartes à puce ou des autres certificats

Ce serveur s'identifie auprès des appelants avant que la connexion ne soit réalisée. Sélectionnez le certificat que vous voulez qu'il utilise comme preuve d'identité.

Certificat délivré à : assur-mer-SRV-DC-CA

Nom convivial : assur-mer-SRV-DC-CA

Émetteur : assur-mer-SRV-DC-CA

Date d'expiration : 20/12/2029 16:23:10

OK Annuler