



Serveur Radius

Mise en place sur borne wifi

Dans ce dossier, vous trouverez la procédure pour l'installation du serveur Radius et sa mise en place sur une borne wifi

S.VAUGEOIS
08/04/2015

Configuration du serveur 2012 :

- ➔ Tout d'abord, vous devez installer sur le Serveur 2012, les rôles et fonctionnalités suivants :

Services de certificats Active Directory (autorité de certification et Inscription de l'autorité de certification via le Web)

Service de stratégie et d'accès réseau (Serveur NPS)

- ➔ Lorsque vous installez les Services de certificats Active Directory, on va vous demander de configurer ce service, vous devrez le remplir avec les informations suivantes :

Spécifier le type de l'AC : autorité de certification racine

Spécifier le type de la clé privée : Créer une clé privée

Spécifier le nom de l'AC : -nom commun de cette AC : labo-SERVEUR2012-CA

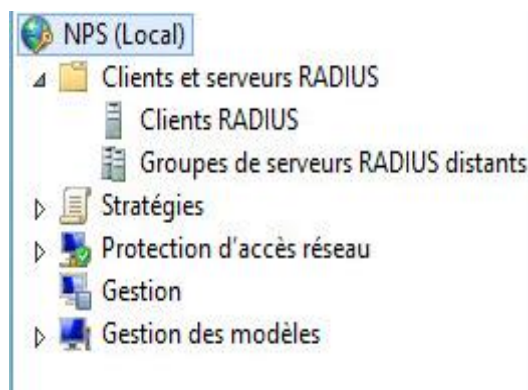
-suffixe du nom unique : DC=labo, DC=sio

-aperçu du nom unique : CN=labo-SERVEUR2012-CA,

DC=labo, DC=sio

Puis confirmer

- ➔ Maintenant, vous devez aller sur le serveur NPS (network policy server) et faire un clic droit sur Client RADIUS et Nouveau :



- ➔ Puis, vous devez remplir les propriétés de la manière suivante, c'est-à-dire le nom convivial (nom donné au client, ici c'est bornewifi17, l'adresse IP qui correspond à l'adresse de la borne wifi, et le mot de passe):

Nouveau client RADIUS

Paramètres Avancé

☒ Activer ce client RADIUS

☐ Sélectionner un modèle existant :

Nom et adresse

Nom convivial : bornewifi17

Adresse (IP ou DNS) : 192.168.17.13 Vénifier...

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

NPS (Local)

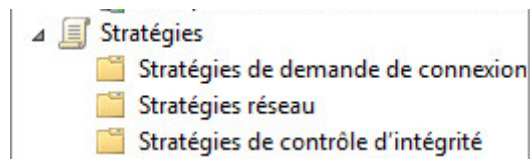
- Clients et serveurs RADIUS
 - Clients RADIUS
 - Groupes de serveurs RADIUS distants
- Stratégies
 - Stratégies de demande de connexion
 - Stratégies réseau
 - Stratégies de contrôle d'intégrité
- Protection d'accès réseau
- Gestion
- Gestion des modèles

Clients RADIUS

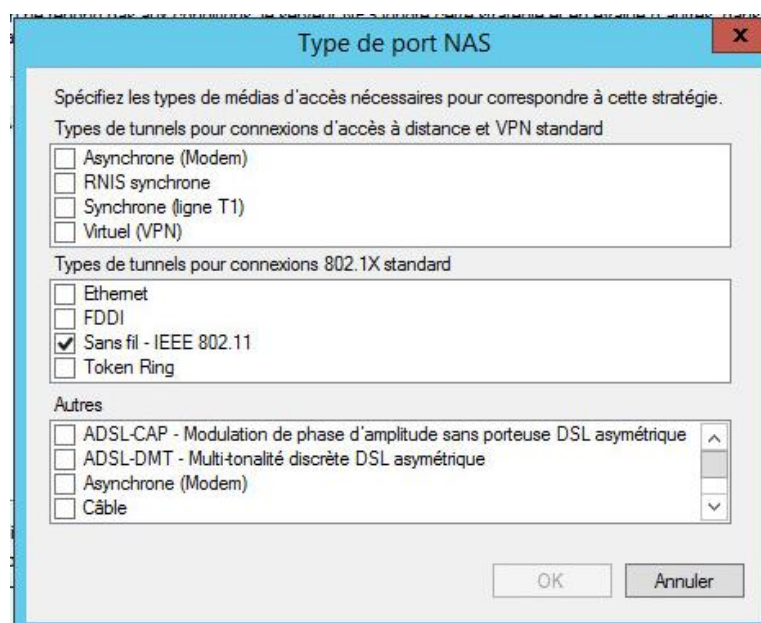
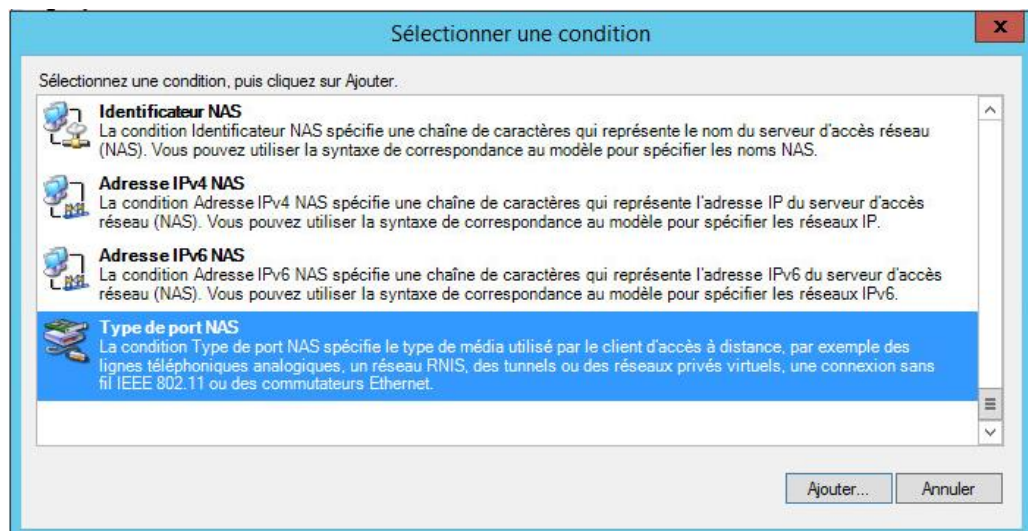
Les clients RADIUS vous permettent de spécifier les serveurs d'accès réseau qui fournissent l'accès à votre réseau.

Nom convivial	Adresse IP	Fabricant du périphérique	Compatible avec la protection d'accès ré
bornewifi17	192.168.17.13	RADIUS Standard	No

- Ensuite, vous devez créer une stratégie réseau en faisant clic droit sur Stratégie réseau et Nouveau :



- Puis, vous devez donner un nom à cette stratégie et choisir les conditions qui sont les suivantes, c'est-à-dire pour la condition (Type de port NAS), dans Type de port NAS, il faut choisir sans fil- IEEE 802.11 (car nous mettons en place une borne wifi):



Condition	Valeur
Type de port NAS	Sans fil - IEEE 802.11

- ➔ Après, vous devez choisir les contraintes suivantes qui sont dans Méthodes d'authentification : Microsoft- Carte à puce ou autre certificat et Microsoft-PEAP (Protected EAP) et dans Type de port NAS, choisir sans fil-IEEE 802.11:

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 qui s'authentifient à l'aide des méthodes spécifiées.

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 :

Microsoft: Carte à puce ou autre certificat
Microsoft: PEAP (Protected EAP)

Monter
Descendre

Ajouter...
Modifier...
Supprimer

Méthodes d'authentification moins sécurisées :

- ☒ Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
 - ☒ L'utilisateur peut modifier le mot de passe après son expiration
- ☒ Authentification chiffrée Microsoft (MS-CHAP)
 - ☒ L'utilisateur peut modifier le mot de passe après son expiration
- ☐ Authentification chiffrée (CHAP)
- ☐ Authentification non chiffrée (PAP, SPAP)
- ☐ Autoriser les clients à se connecter sans négocier une méthode d'authentification
- ☐ Vérifier uniquement l'intégrité de l'ordinateur

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

Spécifier les types de médias d'accès nécessaires pour correspondre à cette stratégie

Types de tunnels pour connexions d'accès à distance et VPN standard

☐ Asynchrone (Modem)
☐ RNIS synchrone
☐ Synchrone (ligne T1)
☐ Virtuel (VPN)

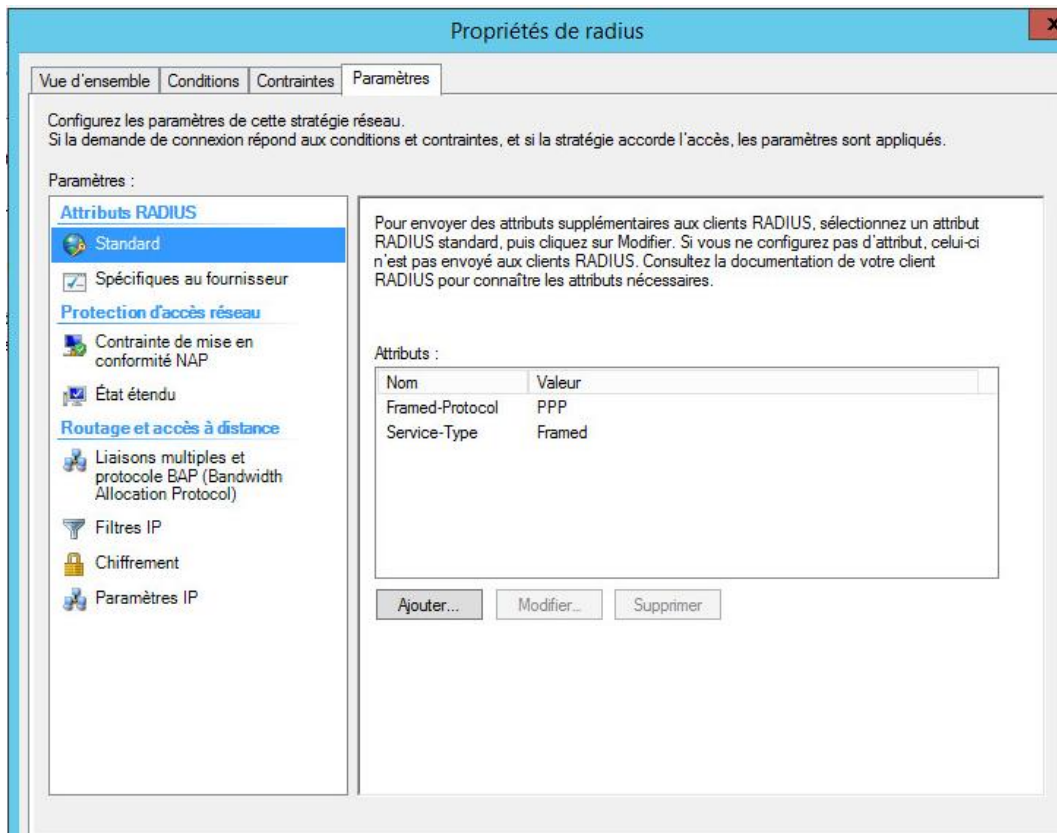
Types de tunnels pour connexions 802.1X standard

☐ Ethernet
☐ FDDI
☒ Sans fil - IEEE 802.11
☐ Token Ring


Autres

☐ ADSL-CAP - Modulation de phase d'amplitude sans porteuse DSL asymétrique
☐ ADSL-DMT - Multi-tonalité discrète DSL asymétrique
☐ Asynchrone (Modem)
☐ Câble

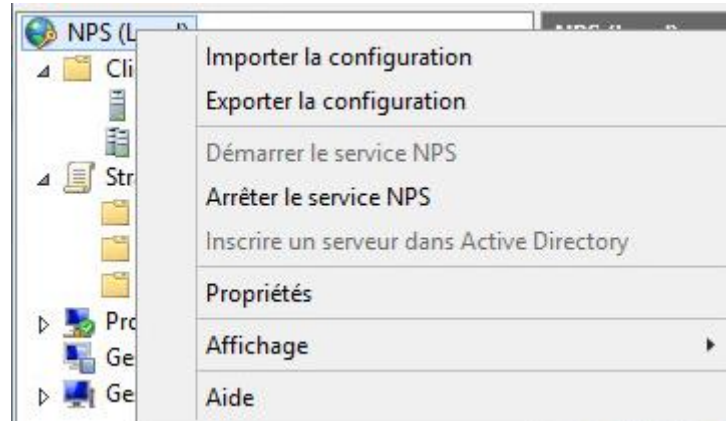
➔ Puis, lorsque vous avez configuré les conditions et les contraintes, vous devez choisir les paramètres :



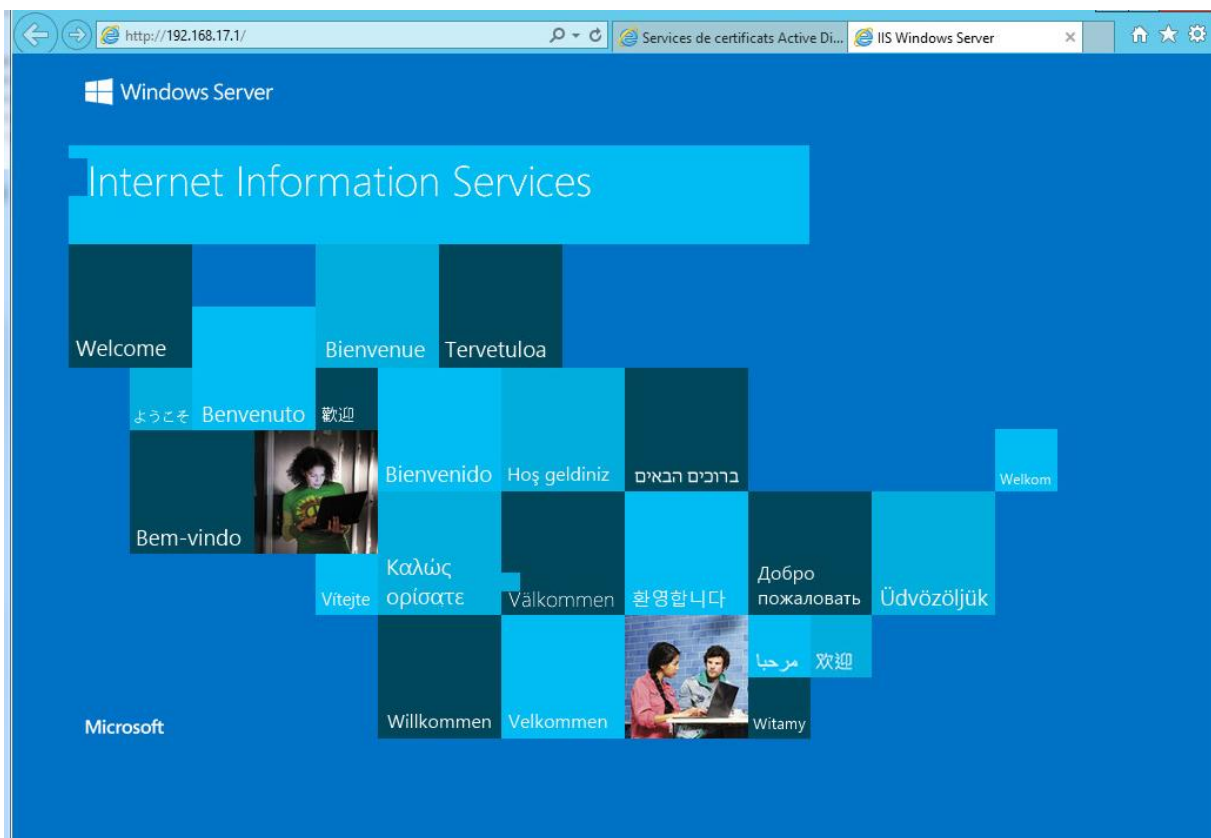
➔ Si la configuration a correctement fonctionné, vous devez voir cela :

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	Source
radius	Activé	1	Accorder l'accès	Non spécifié
Connexions au serveur Microsoft de Routage et Accès distants	Activé	999998	Refuser l'accès	Non spécifié
Connexions à d'autres serveurs d'accès	Activé	999999	Refuser l'accès	Non spécifié

- Ensuite, vous devez intégrer le serveur NPS dans l'Active Directory, en faisant un clic droit sur NPS puis, inscrire un serveur dans Active Directory :



- Puis, vous pouvez maintenant tester si le serveur NPS fonctionne, en allant sur un navigateur web et taper dans l'adresse URL les informations suivantes
<http://192.168.17.1/>



- ➔ Ensuite, vous inscrivez dans la barre URL ceci : <http://192.168.17.1/certsrv> , et vous devez arriver sur une page web qui vous propose différentes tâches à réaliser au niveau des certificats :

Services de certificats *Microsoft* Active Directory — labo-SERVEUR2012-CA Accueil

Bienvenue !

Utilisez ce site Web pour demander un certificat pour votre navigateur Web, votre programme client de messagerie électronique ou un autre programme. En utilisant un certificat, vous pouvez confirmer votre identité aux personnes avec lesquelles vous communiquez sur le Web, signer et chiffrer des messages et, selon le type de certificat que vous demandez, effectuer d'autres tâches sécurisées.

Vous pouvez également utiliser ce site Web pour télécharger un certificat d'autorité de certification, une chaîne de certificats ou une liste de révocation des certificats, ou vous pouvez afficher le statut d'une requête en attente.

Pour obtenir plus d'informations sur les Services de certificats Active Directory, voir [Documentation sur les Services de certificats Active Directory](#).

Sélectionnez une tâche :

- [Demander un certificat](#)
- [Afficher le statut d'une requête de certificat en attente](#)
- [Télécharger un certificat d'autorité de certification, une chaîne de certificats ou une liste de révocation des certificats](#)

- ➔ Sur la page ci-dessus, vous devez choisir « Télécharger un certificat d'autorité, une chaîne de certificats ou une liste de révocation de certificats », vous devez arriver alors sur la page ci-dessous :

Télécharger un certificat d'autorité de certification, une chaîne de certificats ou la liste de révocation des certificats

Pour faire confiance aux certificats émis à partir de cette autorité de certification, installez cette chaîne de certificats d'autorité de certification.

Pour sélectionner un certificat d'autorité de certification, une chaîne de certificats ou une liste de révocation des certificats, sélectionnez un certificat et une méthode de chiffrement.

Certificat de l'autorité de certification :

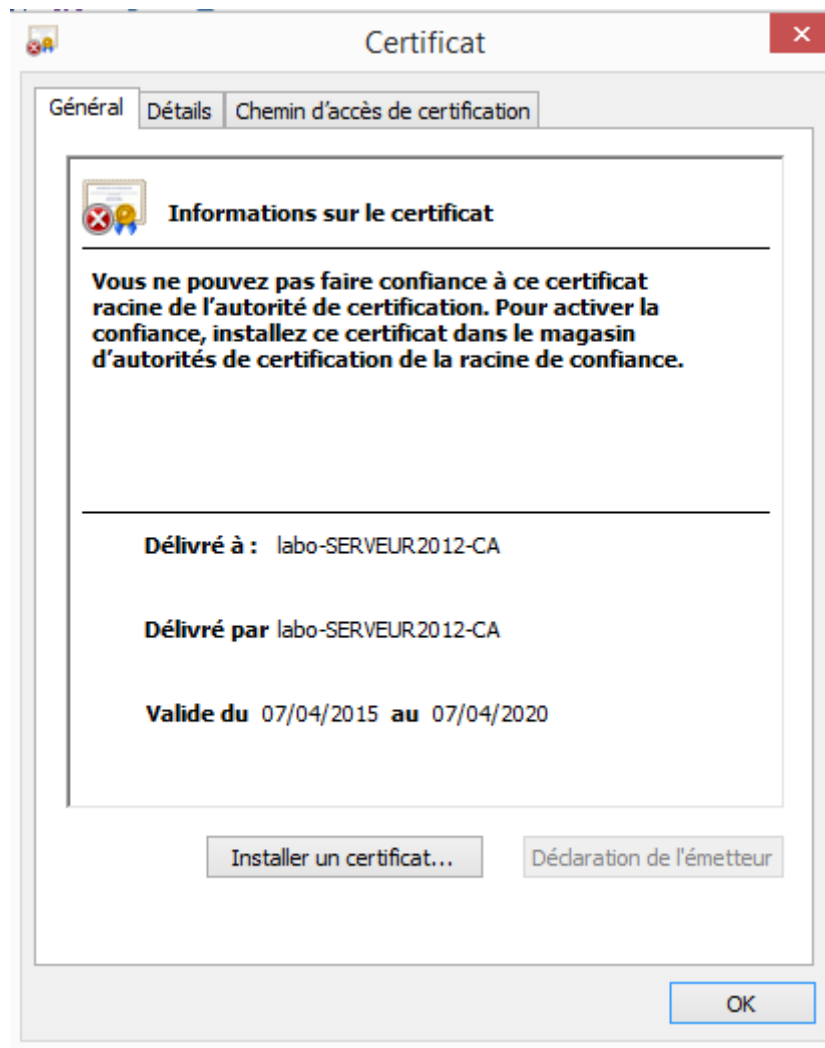
Actuel [labo-SERVEUR2012-CA]

méthode de codage :

☒ DER
☐ Base 64

[Télécharger un certificat de l'autorité de certification](#)
[Télécharger la chaîne de certificats d'autorité de certification](#)
[Télécharger la dernière Liste de révocation des certificats de base](#)
[Télécharger la dernière Liste de révocation des certificats delta](#)

- ➔ Ensuite, vous devez choisir « Télécharger un certificat de l'autorité de certification », cela vous donnera alors un certificat qui vous permettra de donner accès à la wifi aux ordinateurs portables des utilisateurs :



Lorsque vous avez configuré votre serveur, vous devez configurer votre borne wifi, en allant sur l'interface web qui est, dans ce cas précis, 192.168.0.50.

Configuration de la borne Wifi :

- ➔ Dans Home, vous devez remplir les informations suivantes qui sont Mode : Access Point, le SSID qui pour nous est Julien-Solene et l'authentification est WPA2-EAP et le radiusu server qui est l'adresse du serveur que l'on a configuré précédemment, dans notre cas, c'est 192.168.17.1 et inscrire le mot de passe dans Radius (c'est le mot de passe rentré dans la propriété au niveau du client Radius):

The screenshot shows the 'Home' tab of a configuration interface. Under 'Wireless Settings', the following fields are visible: 'Wireless Band' set to 'IEEE802.11g', 'Mode' set to 'Access Point', 'SSID' set to 'Julien-Solene', 'SSID Broadcast' set to 'Enable', 'Channel' set to '6' (with '2.437 GHz' displayed next to it), and 'Authentication' set to 'WPA2-EAP'. A 'Radius Server Settings' section contains: 'Cipher Type' set to 'AES', 'Group Key Update Interval' set to '1800', 'Radius Server' set to '192.168.17.1', 'Radius Port' set to '1812', and 'Radius Secret' masked with dots. At the bottom, 'Radio' is 'On', 'Super G Mode' is 'Disable', and 'Wireless Qos(WMM)' is 'Disable'. Three buttons at the bottom right are labeled 'Apply', 'Cancel', and 'Help' with corresponding icons.

- ➔ Ensuite, vous devez configurer dans LAN Settings, l'adresse IP de la borne Wifi (192.168.17.13), son masque et la passerelle (192.168.17.3) qui correspond dans notre contexte à l'Ipfire :

The screenshot shows the 'Home' tab of a configuration interface. Under 'LAN Settings', the following fields are visible: 'Get IP From' set to 'Static (Manual)', 'IP address' set to '192.168.17.13', 'Subnet Mask' set to '255.255.255.0', and 'Default Gateway' set to '192.168.17.3'. Three buttons at the bottom right are labeled 'Apply', 'Cancel', and 'Help' with corresponding icons.

- ➔ Puis, vous devez configurer le DHCP, en allant dans Advanced et Dynamic Pool Settings, vous allez devoir mettre Enable pour Function, pour indiquer que la borne wifi aura un rôle de serveur DHCP, puis inscrire dans IP AssignedFrom qui l'IP de départ pour les adresses IP distribuées, ensuite, vous devez informer sur le masque, la passerelle, le dns et le nom de domaine/

The screenshot shows a web-based configuration interface for a DHCP server. The top navigation bar has tabs for Home, Advanced (selected), Tools, Status, and Help. Below the navigation bar, there are links for Dynamic Pool Settings, Static Pool Settings, and Current IP Mapping List. The main section is titled 'DHCP Server Control' and contains two sub-sections: 'DHCP Server Control' and 'Dynamic Pool Settings'. The 'Dynamic Pool Settings' section includes the following fields:

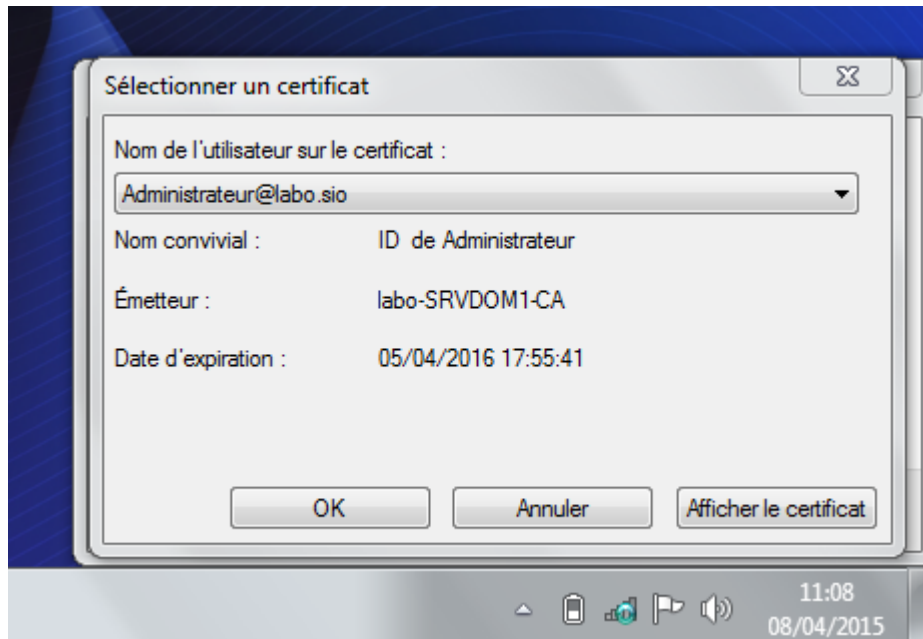
Field	Value
Function Enable/Disable	Enable
IP Assigned From	192.168.17.100
The Range of Pool (1-255)	10
SubMask	255.255.255.0
Gateway	192.168.17.3
Wins	0.0.0.0
DNS	192.168.17.1
Domain Name	labo.sio
Lease Time (60 - 31536000 sec)	3600
Status	ON

At the bottom right of the form, there are three buttons: Apply (with a green checkmark icon), Cancel (with an orange X icon), and Help (with a red plus icon).

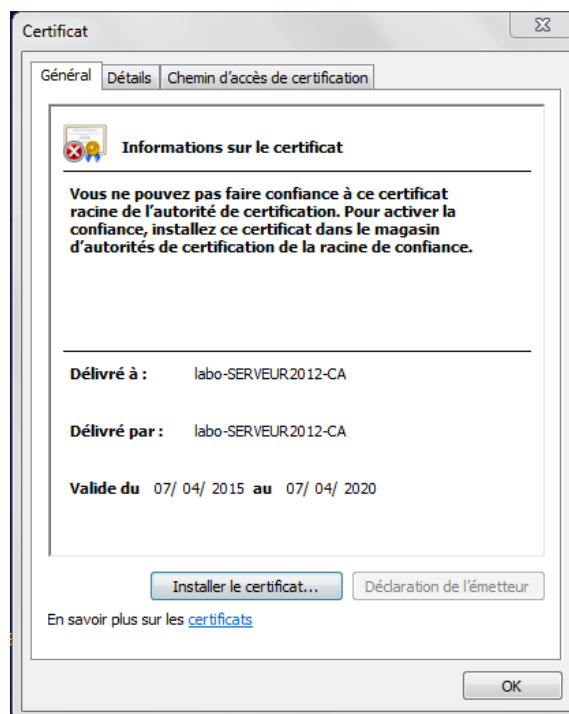
- ➔ Lorsque vous avez configuré la borne Wifi et le serveur, il faut passer au test avec un client. Nous avons pris un ordinateur portable.

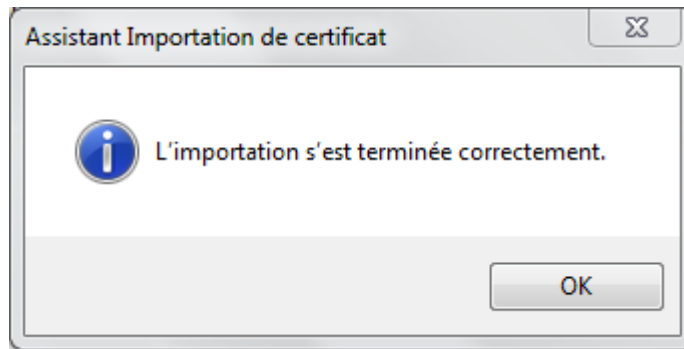
Configuration du client :

- Lorsque vous allez cliquer sur le réseau que vous allez vouloir tester (pour nous, c'est Julien-Solene), on doit vous demander de sélectionner un certificat, vous cliquez sur OK:

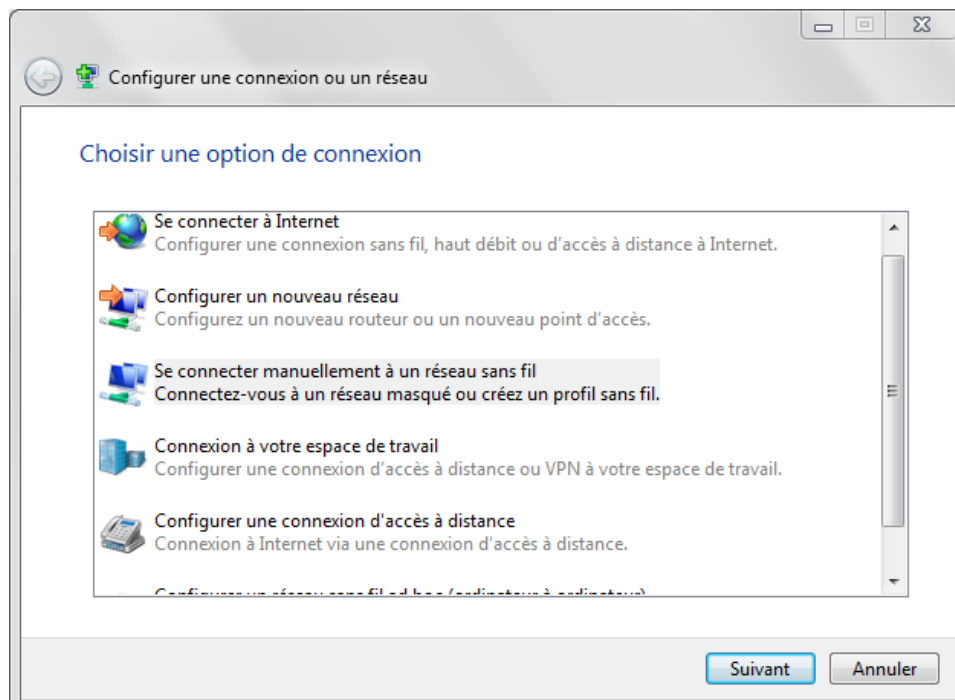


- Quand vous aurez cliqué sur OK, vous allez avoir une page qui va s'ouvrir nommée Certificat et là vous allez devoir cliquer sur Installer le certificat... :

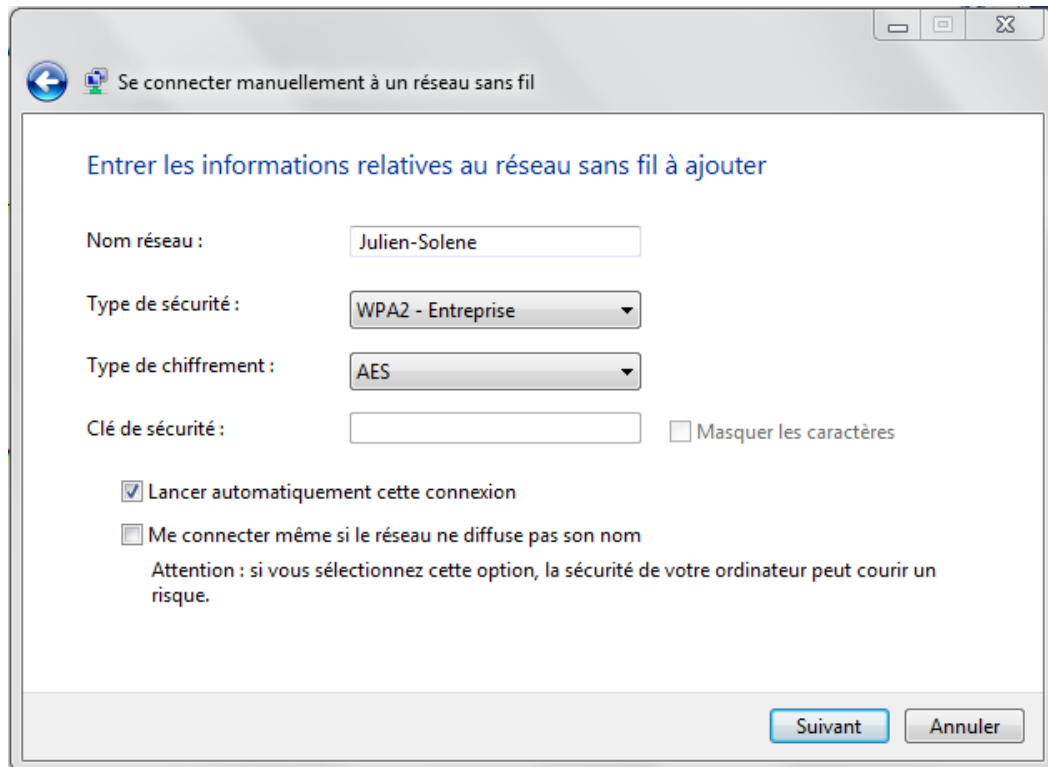




- Lorsque l'importation sera terminée, on vous demandera de choisir un type de connexion, vous allez devoir sélectionner « Se connecter manuellement à un réseau sans fil » :



- ➔ Puis, vous allez devoir rentrer les informations relatives au réseau sans fil à ajouter. Les informations à ajouter sont le nom du réseau (ici c'est Julien-Solene), le type de sécurité (WPA2-Entreprise) :

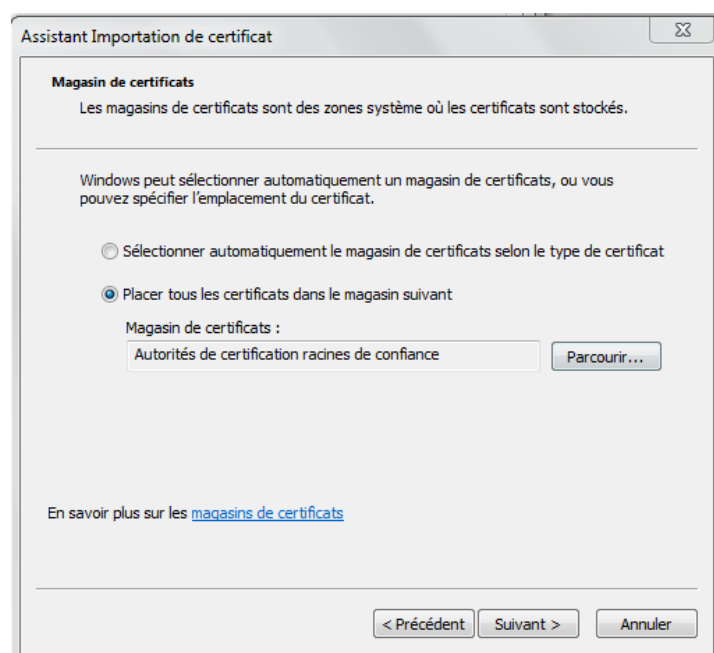


The screenshot shows a Windows dialog box titled "Se connecter manuellement à un réseau sans fil". The main heading is "Entrer les informations relatives au réseau sans fil à ajouter". The form contains the following fields and options:

- Nom réseau : Julien-Solene
- Type de sécurité : WPA2 - Entreprise
- Type de chiffrement : AES
- Clé de sécurité : (empty text box) ☐ Masquer les caractères
- ☒ Lancer automatiquement cette connexion
- ☐ Me connecter même si le réseau ne diffuse pas son nom

Below the second checkbox, there is a warning: "Attention : si vous sélectionnez cette option, la sécurité de votre ordinateur peut courir un risque." At the bottom right, there are two buttons: "Suivant" and "Annuler".

- ➔ Ensuite, vous allez devoir choisir le magasin de certificats, qui est dans « Placer tous les certificats dans le magasin : Autorité de certification racines de confiance » :

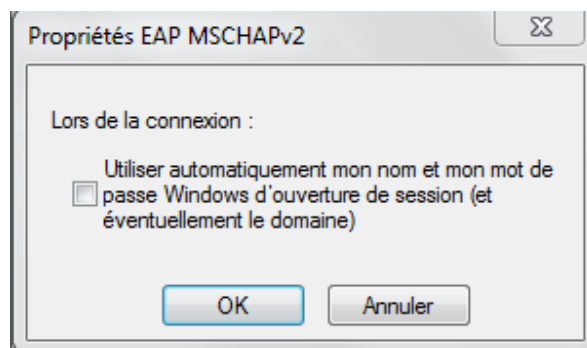
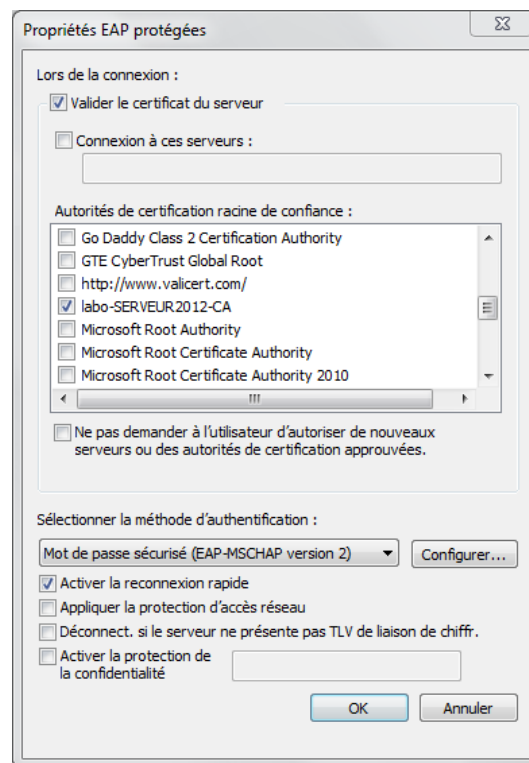


The screenshot shows the "Assistant Importation de certificat" dialog box. The title bar says "Assistant Importation de certificat". The main heading is "Magasin de certificats". Below it, a text box explains: "Les magasins de certificats sont des zones système où les certificats sont stockés." A separator line follows. Below the line, a text box states: "Windows peut sélectionner automatiquement un magasin de certificats, ou vous pouvez spécifier l'emplacement du certificat." There are two radio button options:

- ☐ Sélectionner automatiquement le magasin de certificats selon le type de certificat
- ☒ Placer tous les certificats dans le magasin suivant

Below the second option, there is a label "Magasin de certificats :" followed by a text box containing "Autorités de certification racines de confiance" and a "Parcourir..." button. At the bottom, there is a link: "En savoir plus sur les [magasins de certificats](#)". At the very bottom, there are three buttons: "< Précédent", "Suivant >", and "Annuler".

- ➔ Maintenant, il vous reste à choisir les Propriétés EAP protégées pour l'autorité de certification racines de confiance. Cela correspond au nom de votre certificat :



- ➔ Lorsque vous aurez fait cela, on vous demandera une authentification afin de vérifier si vous faites bien parti du domaine et que vous avez le droit d'y accéder par la wifi :

