Dylan CHAU
Axel BAUGÉ

2A-SISR

Tests d'intégration Wifi

Date de création : 22/11/2023
Version : 1.0
Pour validation : DSI
A destination : DSI
Mode de diffusion : Intranet
Nombre de pages : 10
Auteur : CHAU Dylan

Métadonnées

Diffusion			
Périmètre de diffusion	Contrôlé	Interne	Libre

Historique des évolutions		
Auteur	Version	Objet de la version et liste des modifications
Dylan Chau	1.0	Initialisation du document

Validation			
Rédacteur		Validateur	
Nom	Date	Nom	Date
Dylan Chau	22/11/2023	DSI	20/12/2023
Date d'application : 13/01/2024			

Table des matières

Prérequis

- Avoir réalisé la procédure d'installation et de configuration du Cisco WAP371.

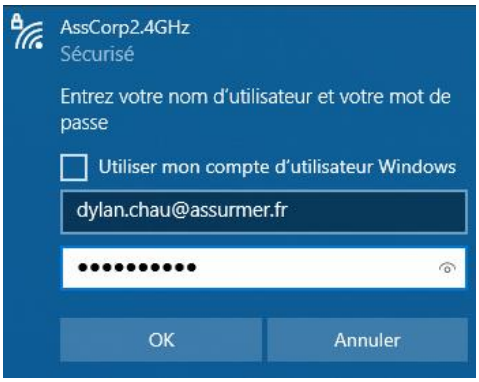
Tests d'intégration Wifi sécurisé et Radius PEAP

1) Test de connexion avec la clé de sécurité

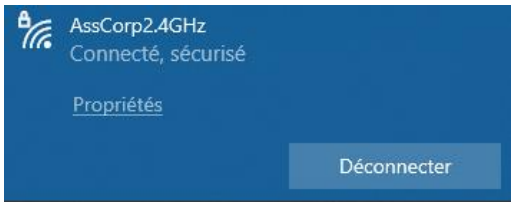
- Sélectionner le point d'accès en WPA-Personal.
- Renseigner la clé de sécurité.
- La connexion fonctionne.

2) Test de connexion avec les identifiants AD

- Sur un poste externe ou interne, se connecter sur le point d'accès avec les identifiants AD.



- Le poste peut se connecter.



- La connexion est bien en PEAP.

Type de sécurité :	WPA2 - Entreprise
Type d'informations de connexion :	Microsoft: PEAP (Protected EAP)

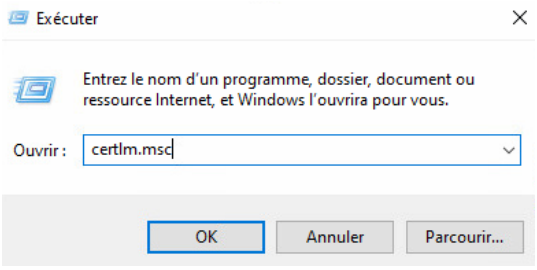
3) Connexion au Wi-Fi Administrateur

- Ajouter le groupe de sécurité « Wifi-Admin » sur un compte.
- Se connecter avec ce compte sur « AssAdminG4 ».
- La connexion fonctionne.
- Sur un autre compte sans le groupe de sécurité, la connexion est impossible.
- Pour chaque point d'accès, vérifier que la bonne adresse IP a été ajoutée.

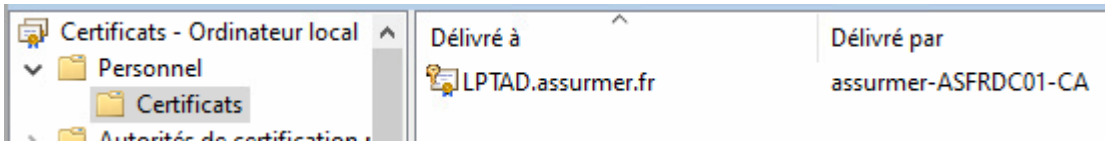
Tests d'intégration axes d'amélioration EAP-TLS

1) Vérification du fonctionnement de la GPO Certificats

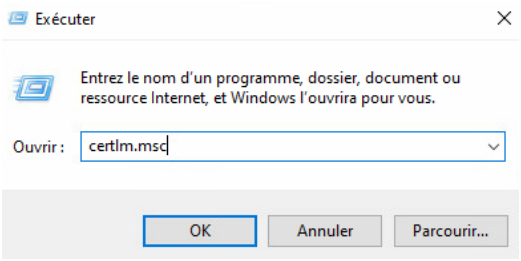
- Après un gpupdate, faire « Windows + R » puis « certlm.msc ».



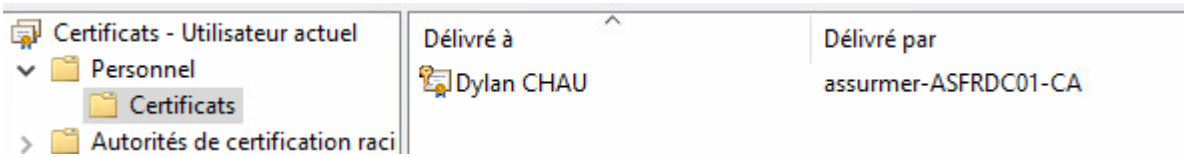
- Le certificat machine apparaît bien.



- Faire « Windows + R » puis « certmgr.msc ».



- Le certificat utilisateur apparaît bien.



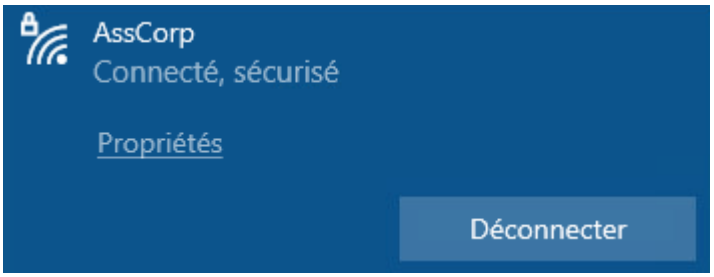
2) Vérification du fonctionnement de la GPO Réseau Wifi

- Après un gpupdate, sur le poste client, connecter une clé wifi.
- Le point d'accès AssCorp apparaît bien.

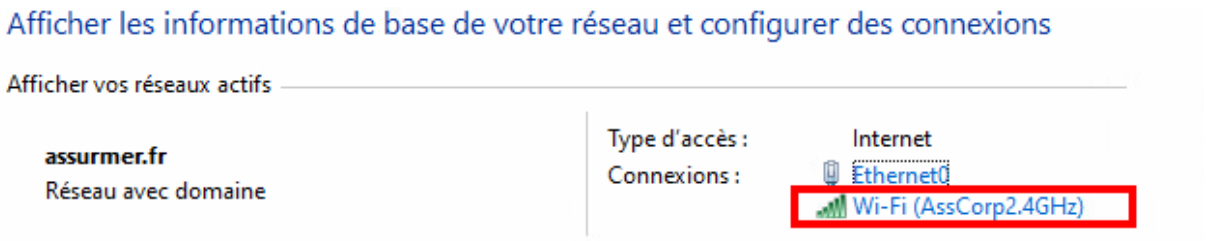
3) Vérification du fonctionnement de la connexion

- Sur le point d'accès, cliquer sur « Se connecter ».

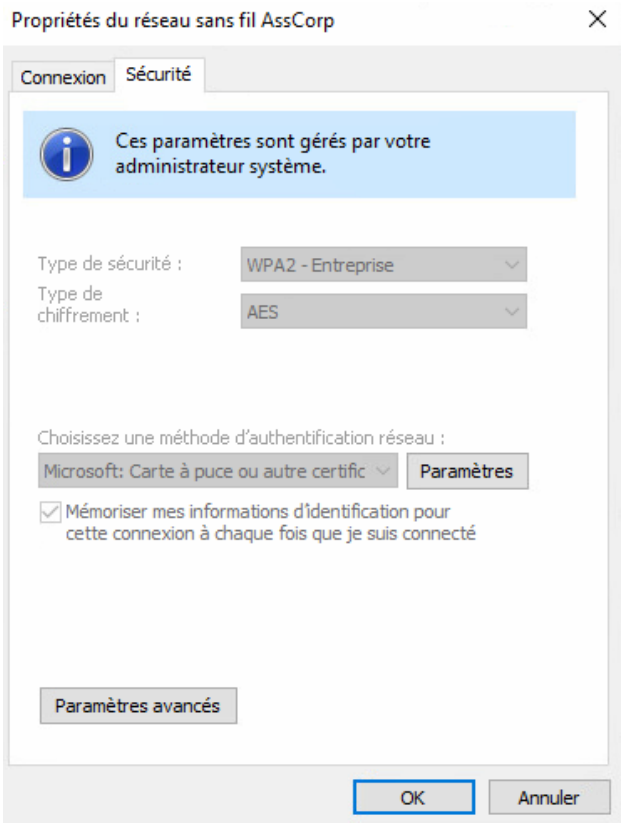
- La connexion fonctionne.



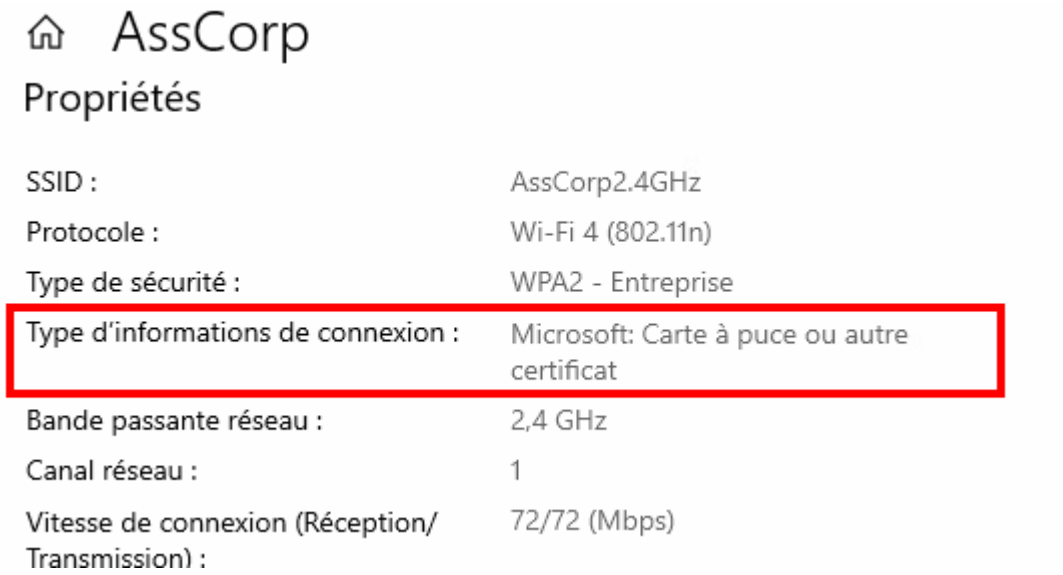
- Dans « Centre Réseau et partage », ouvrir les détails de la connexion Wi-fi.



- Dans les « Propriétés du réseau sans fil », la méthode d'authentification est bien en mode carte à puce ou certificat.

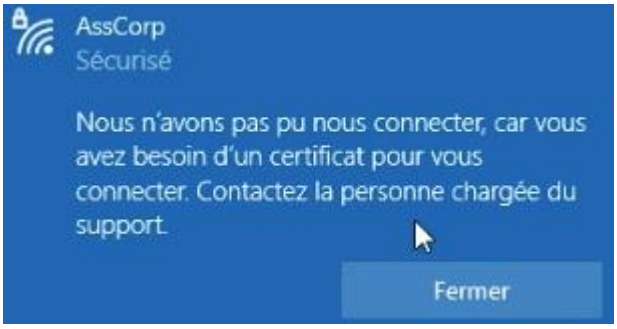


- De même dans les propriétés Windows.

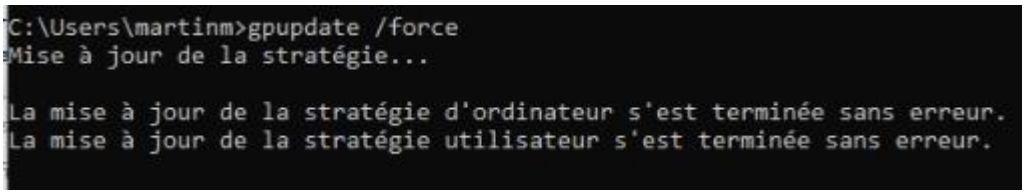


4) Test de suppression des certificats

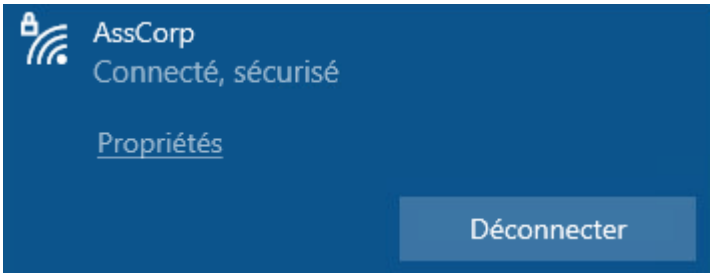
- Supprimer les certificats utilisateur et machine en administrateur dans le magasin de certificat.
- La connexion est désormais impossible.



- Faire la commande gpupdate /force dans cmd pour réimporter les certificats.

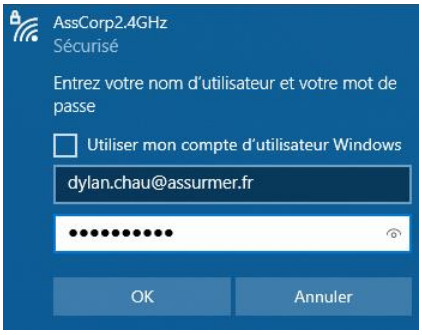


- Réessayer. La connexion est de nouveau possible.

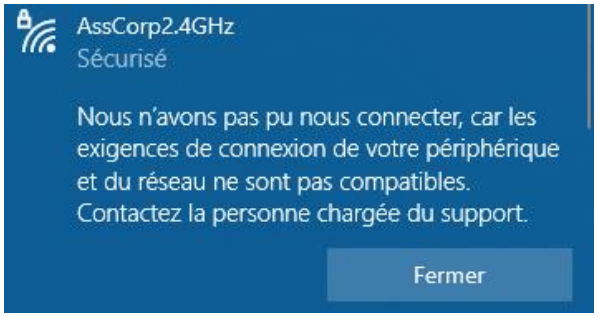


5) Test de connexion avec les identifiants AD

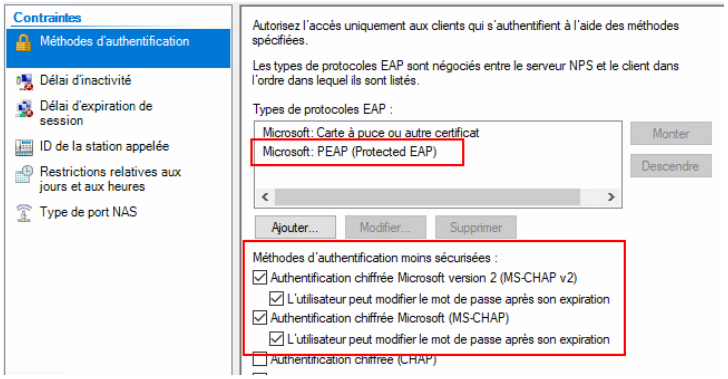
- Sur un poste externe, se connecter sur le point d'accès avec les identifiants AD.



- La connexion est impossible en raison de la stratégie réseau qui ne permet que la connexion à partir d'un certificat.



- Sur la console NPS, ajouter l'authentification PEAP et par mot de passe.



- Réessayer. Le poste externe peut se connecter.