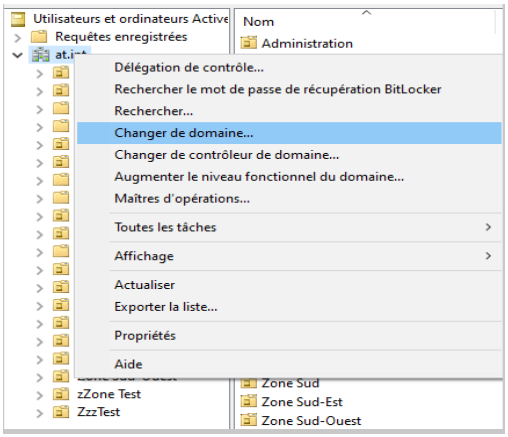
PRÉFET
DU VAL-D'OISE
Liberté
Égalité
Fraternité

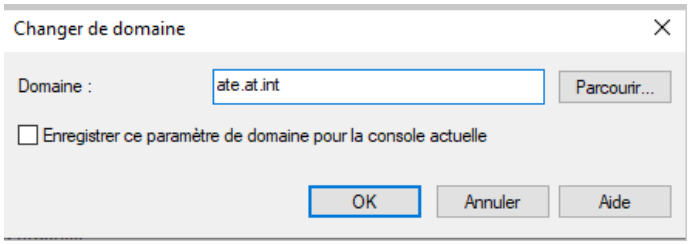
SERVICE INTERMINISTÉRIEL DÉPARTEMENTAL DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION

Création et Mastérisation d'un poste NOEMI DDI

Dans l'Active Directory ATE :

- **L'accès à L'AD ATE se fait depuis l'AD AT :**

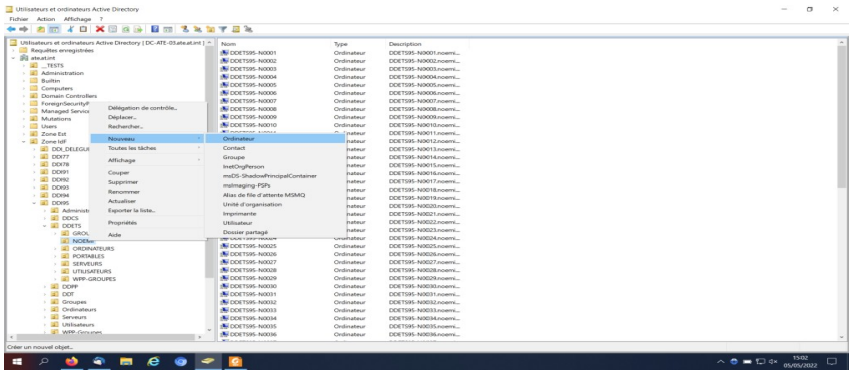




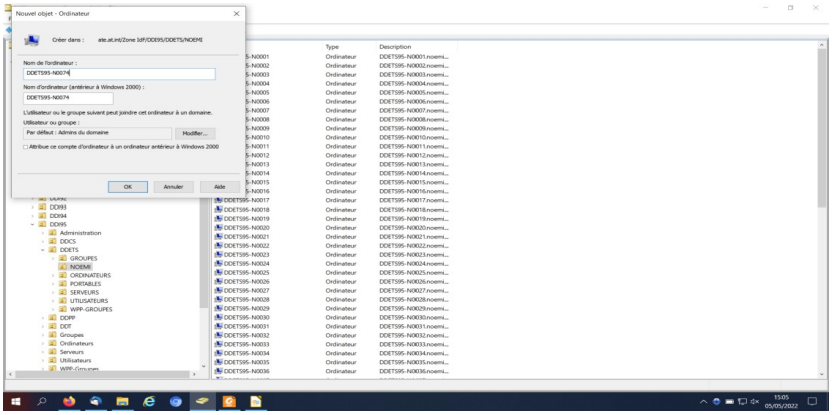
Sur L'AD ATE :

- Création de l'ordinateur DDETS95-Nxxxx, DDPP95-Nxxxx ou DDT95-Nxxx dans la bonne OU
  - ate.at.int\Zone IDF\DDI95\DDPP\NOEMI
  - ate.at.int\Zone IDF\DDI95\DDETS\NOEMI
  - ate.at.int\Zone IDF\DDI95\DDT\NOEMI

Pour créer l'ordinateur : Clic droit → Nouveau → Ordinateur



Nommer l'ordinateur de façon adéquate comme indiqué précédemment (on peut prendre pour modèles les ordinateurs déjà existant).

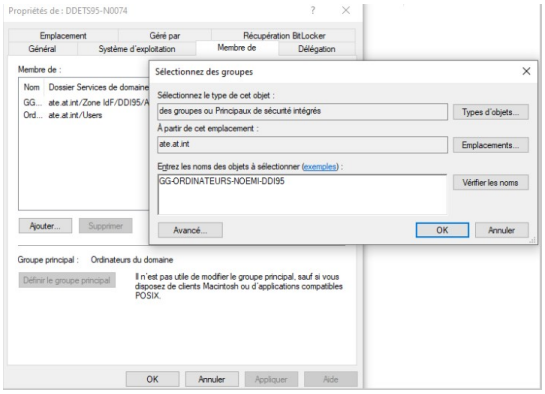


• Ajout du poste dans le groupe GG-ORDINATEURS-NOEMI-DDI95

Clic droit sur l'ordinateur créer→Propriété

1/ Aller dans l'onglet «Membre de»

2/ cliquer sur «ajouter» pour ajouter le groupe

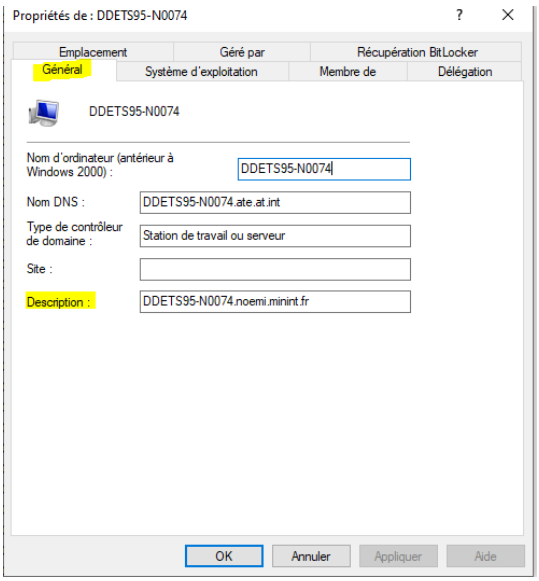


• Description du poste à mettre sous la forme «NOMDUPOSTE.noemi.minint.fr».

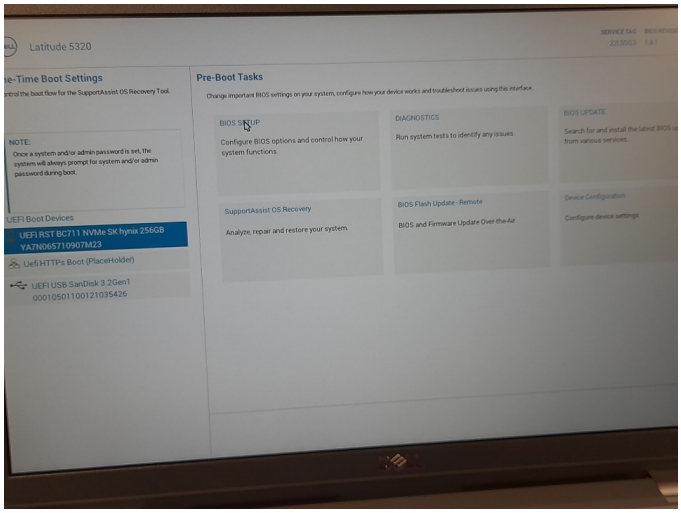
Clic droit sur l'ordinateur créer→Propriété

1/ Aller dans l'onglet «général»

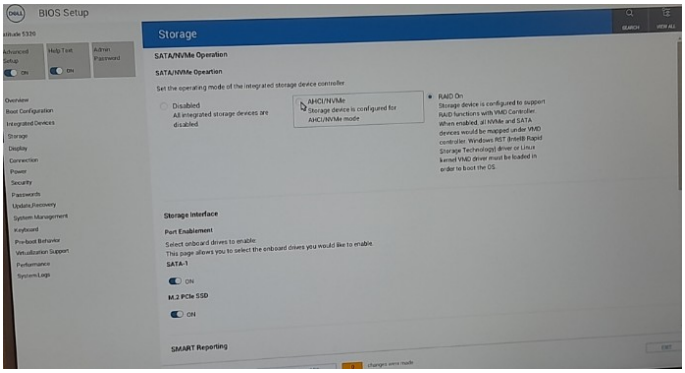
2/ Remplir le champ «description»



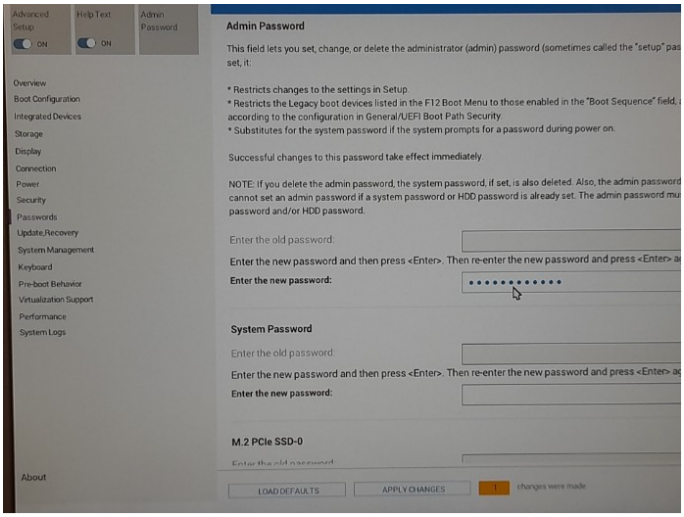
- Dans le BIOS Setup (pour y accéder, spammer la touche F12 au démarrage du poste):



- forcer le mode AHCI (menu Storage / Sata Operation : AHCI)



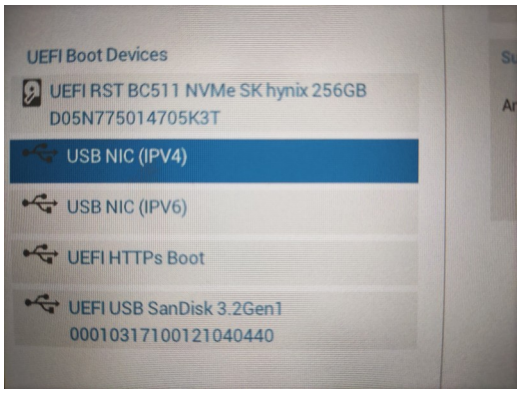
- Mettre en place le mot de passe "AdminPassword" du BIOS (menu Password / AdminPassword)



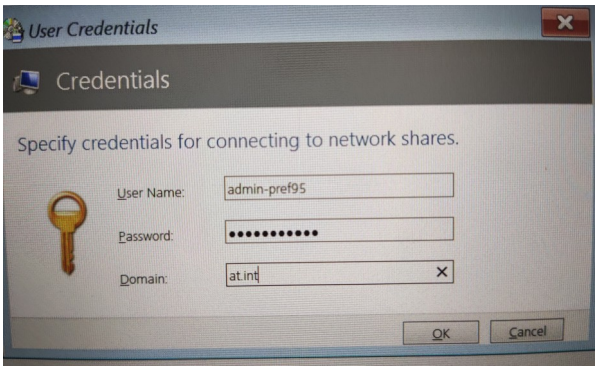
mot de passe à mettre : Ssigroup@p95

- appuyer sur la touche entrée pour confirmer la saisie du mot de passe (il faudra le ressaisir pour confirmer le changement).

● Appliquer les changements, quittez le BIOS Setup (provoque le redémarrage de l'ordinateur), spammer la touche F12 et booter sur « IPV4»



● Après avoir booté sur «IPV4», Patienter jusqu'à l'apparition de cette fenêtre ci-dessous :

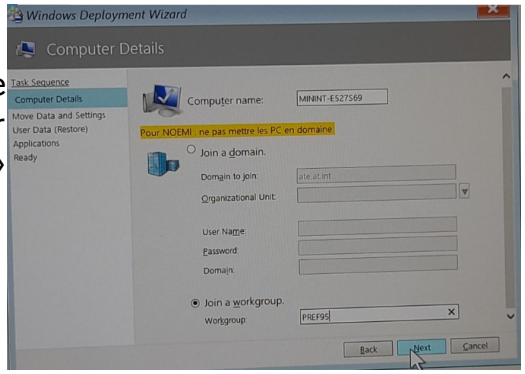


Renseigner :

- User name : admin-pref95
- Password : Ssigroup@08
- Domain : at.int

Ensuite, faire « ok » et suivre les étapes ci-dessous :

1/ **Task séquence :** POSTES → Windows 10 → New computer → choisir le socle W10 20H2, «next»

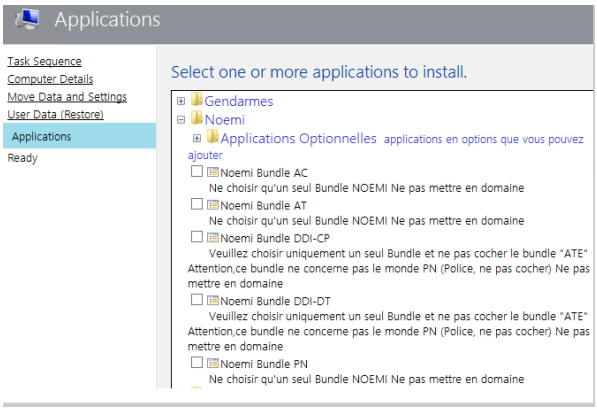


2/ **Computer details :** Ne pas cocher rejoindre de domaine, ne pas renseigner le nom du poste, cocher rejoindre un workgroup, remplir le champ «workgroup» (ex : pref95) puis faire «next»

3/ **Move Data and setting :** ne rien changer, faire «next»

4/ **User Data (Restore) :** ne rien changer, faire «next»

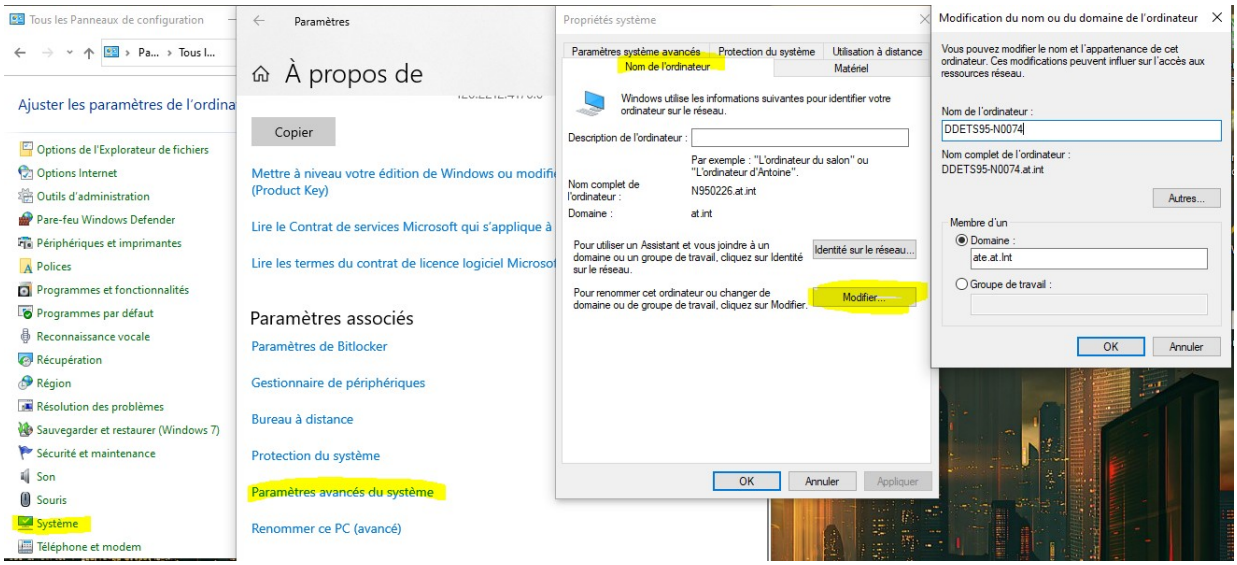
5/ **Applications :** Choisir :
le bundle NOEMI DDI-CP pour la DDPP
le bundle NOEMI DDI-CP pour la DDETS
le bundle NOEMI DDI-DT pour la DDT



6/ Lancer la mastérisation en appuyant sur «begin» (temps estimé : environ une heure)

Sur le nouveau PC, préparation du poste :

- Se connecter en admin-local avec le mdp $3CR3T_@DM1N
- Depuis le panneau de configuration → système → paramètres avancés du système → nom d'ordinateur → modifier :

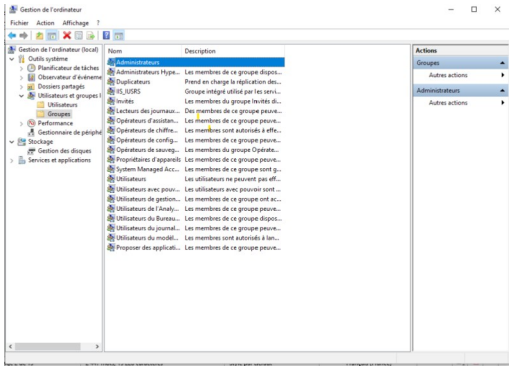


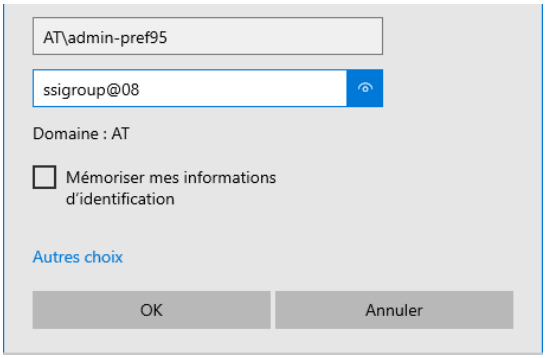
- Renommer le poste comme prévu dans l'AD ATE, DDETS95-Nxxxx, DDPP95-Nxxxx ou DDT95-Nxxx
- Rejoindre le domaine ATE.AT.int avec les identifiants admin-pref95

Les identifiants admin-pref95 sont les suivants :
AT*admin-pref95*
ssigroup@08

/! *Ne pas redémarrer l'ordinateur maintenant* ***/!***

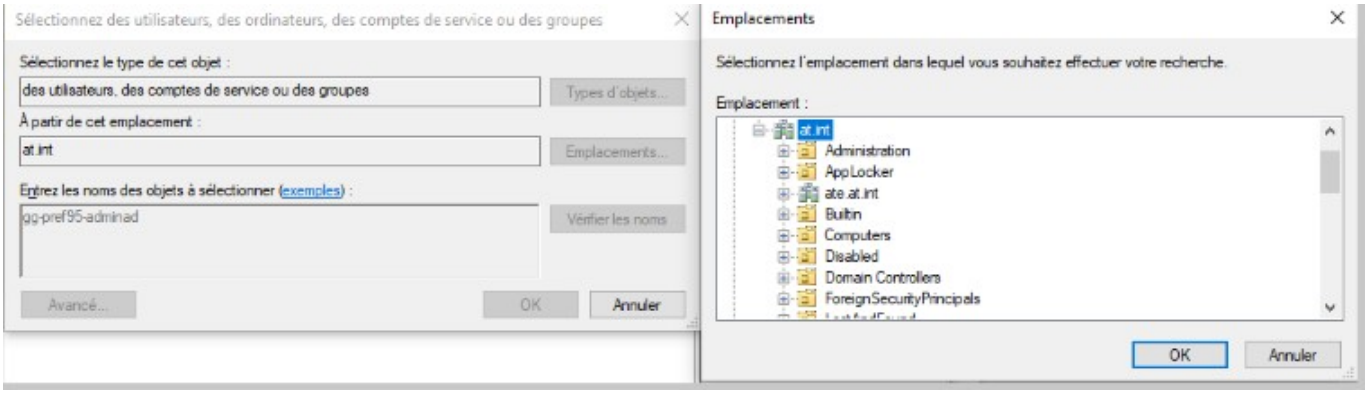
- Depuis le panneau de gestion de l'ordinateur (clic droit sur le logo Windows), dans « Utilisateurs et groupes locaux », « Groupes » et « Administrateurs » : Ajouter…





- identifiants et mdp seront demandés, mettre ceux de admin-pref95 (voir capture d'écran)

● cliquer sur l'onglet « emplacement », choisir AT.int, ajouter « GG-PREF95-ADMINAD »



● Redémarrer l'ordinateur et se connecter sur la session «admin-pref95»

Si l'admin domaine (GG-PREF95-ADMINAD) n'a pas été renseigné avant d'avoir redémarré le poste, vous devrez passer par LAPS pour récupérer le mdp en procédant de la sorte :

Vos identifiants sont ceux de votre session Windows.

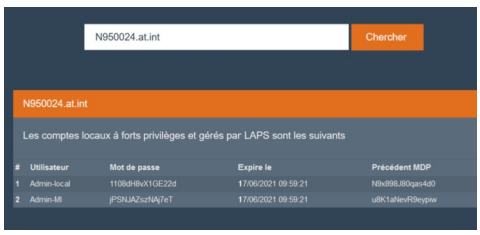
● Sur votre machine admin, utiliser l'outil LAPS accessible à l'adresse : https://laps.pn.int/easylaps

● Dans le champ de recherche, renseigner le nom du poste suivi par « ate.at.int »

● Se connecter en tant que : nomduposte\admin-local avec le mot de passe LAPS récupéré

● Dans la gestion de l'ordinateur, ajouter en administrateur GG-PREF95-ADMINAD

● Se connecter en tant que admin-pref95



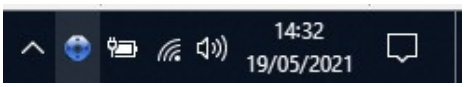
Si le PC vient de rejoindre le domaine, compter jusqu'à une heure pour que le mot de passe soit disponible.

VPN : *Se connecter en tant que admin-pref95*

- Si la licence n'est pas automatiquement remontée et que la fenêtre d'activation apparaît, vérifier que le câble réseau (MI) est bien connecté et cliqué sur « suivant ».

- Si l'activation reste impossible, laisser la page ouverte et procéder aux autres manipulations avant de tester de nouveau.

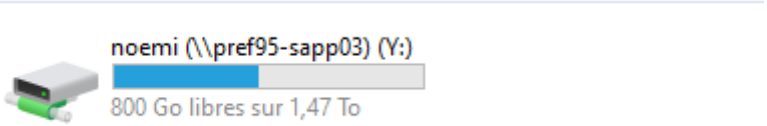
- Si lorsque l'on clique sur l'icône du VPN la fenêtre reste vide, redémarrer le pc.

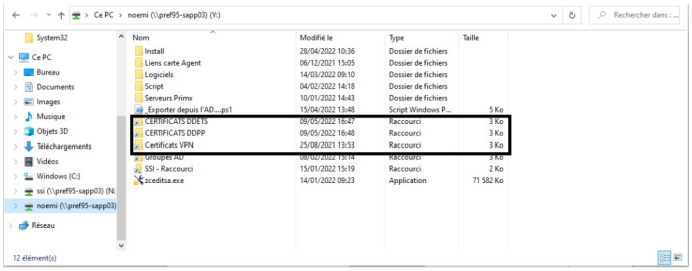


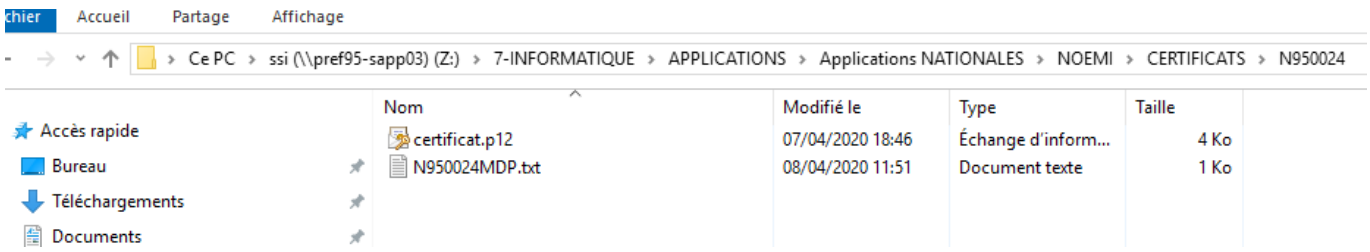
Icône du VPN dans la barre de tâche (cliquer sur la flèche si l'icône n'est pas présente)

● Récupérez le certificat du VPN et son mdp correspondant sur le serveur pref95-sapp03\ssi dans Applications nationales / NOEMI / Certificats DDPP ou DDETS (copier-coller les 2 éléments sur le bureau). Prendre le certificat et mdp présent dans le dossier ayant le même nom que le poste en cours.

En étant connecté sur la session «Admin-pref95» Un lecteur réseau se connecte automatiquement, permettant de naviguer sur le serveur de fichier et récupérer le nécessaire.



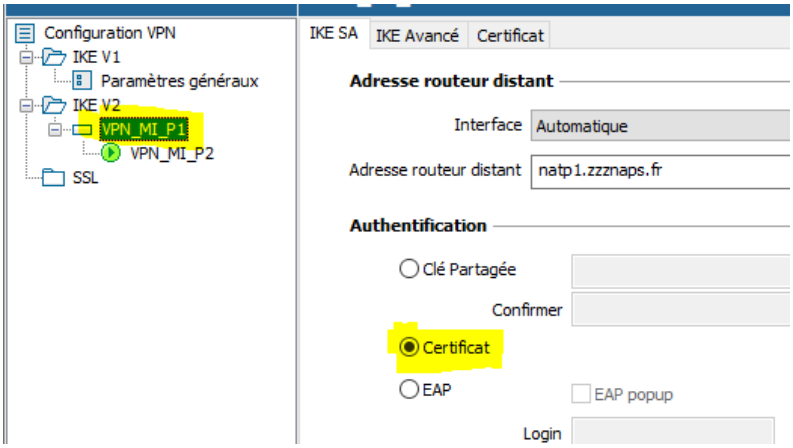




récupérer le certificat + mdp dans le fichier txt

● Ouvrir le panneau de configuration du VPN avec le code : MyP@ssw0rD!

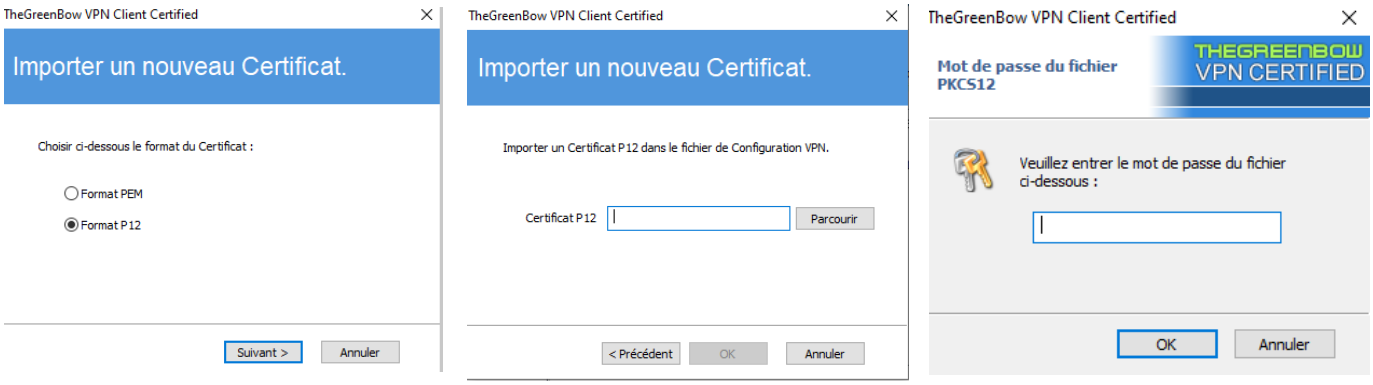
● Dans « VPN_MI_P1 », cliquer sur Certificat.



Panneau de configuration du VPN - Dans « VPN_MI_P1 », cliquer sur Certificat

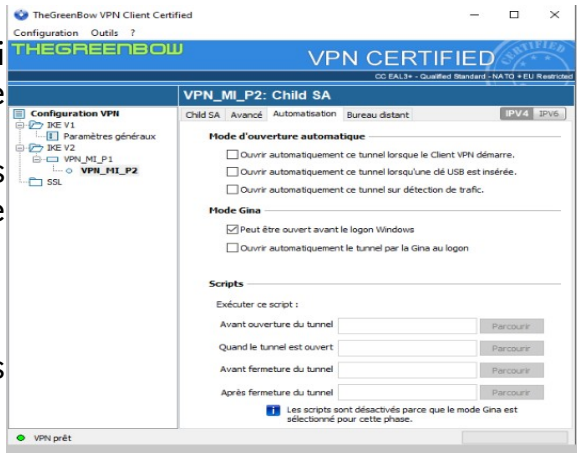
● Cliquer sur «Importer un Certificat...» puis :

- Choisir le format p12 (par défaut)
- Aller chercher le certificat précédemment récupéré et copier sur le bureau (via l'icône parcourir)
- Rentrer le mot de passe contenu dans le .txt, récupéré au préalable.



● Les utilisateurs en DDI passeront d'un VPN qui s'active manuellement à un VPN qui s'active automatiquement par défaut.

Pour éviter de perturber leurs anciennes habitudes, Il faut désactiver l'automatisation de celui-ci (voir capture d'écran).



● Avant de quitter, sauvegarder les modifications (CTRL + S ou configuration > Sauvegarder),

<u>MAJ Windows :</u>

● Lancer les mise à jour Windows via le menu Windows Update en cliquant sur « Rechercher des mises à jour ».

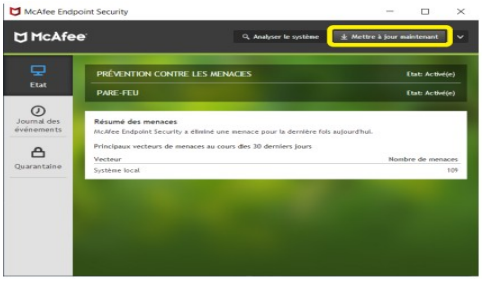
Si une erreur survient et qu'aucune maj n'a été trouvé, le serveur de maj n'est actuellement pas accessible, d'autres machines y accèdent déjà et il vous faudra attendre votre tour. Tant que la session reste ouverte, Windows essaiera de recontacter le serveur de maj.

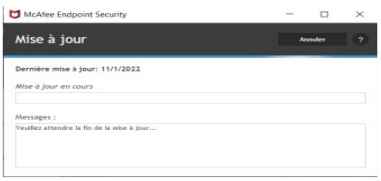
● Redémarrer après les maj et vérifier si de nouvelles sont disponibles a chaque nouveau logiciel / périphérique installé.

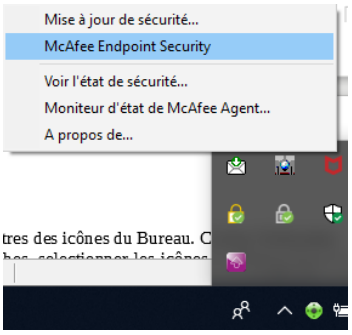
Certaines mises à jour tel que « CRYHOD 2021.1 V2 » peuvent nécessiter plusieurs redémarrages avant d'être totalement installées. Il sera nécessaire de décrypter le poste à chaque fois si il est déjà crypté.

<u>MAJ Anti-virus McAfee :</u>

● Lancer les mise à jour McAfee depuis son interface.







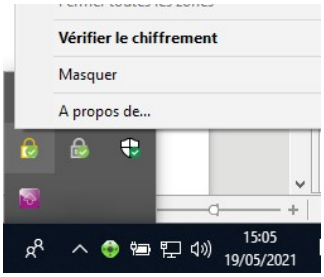
Ouvrir l'interface McAfee

/!\ Ne commencer le cryptage du poste que lorsque toutes les mises à jours seront terminées, Windows ET McAfee.

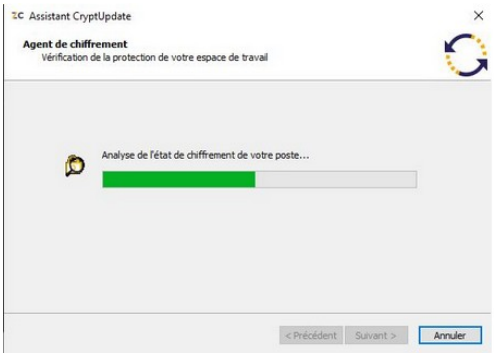
Cryptage :

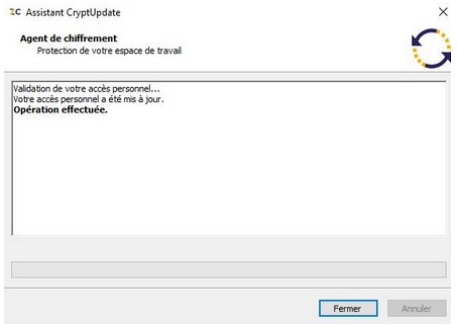
• Ouvrir une session Windows avec une carte agent ayant des droits administrateurs

• Vérifier le chiffrement avec un clic droit sur l'icône ZoneCentral dans la barre de taches.



Icône ZoneCentral dans la barre de tâches

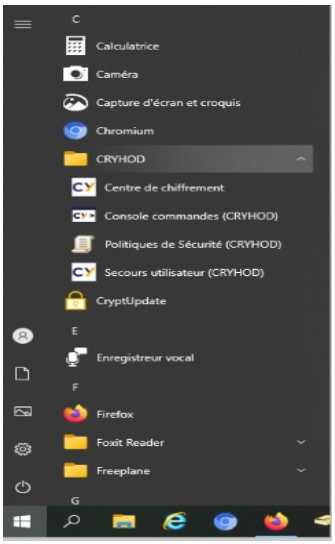




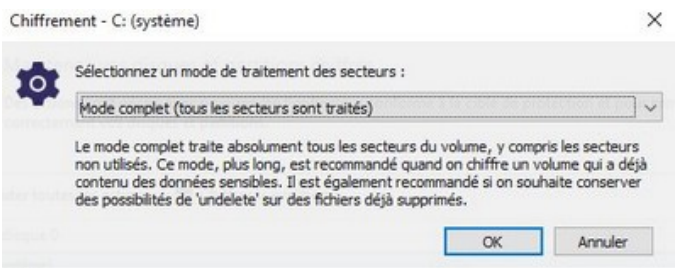
• Lancer le cryptage du poste en :

1/ Se rendant dans l'outil «Centre de Chiffrement» Cryhod (le centre de chiffrement est accessible depuis le menu démarrer).

2/ Cliquer sur «chiffrer la partition»



3/ Choisir le mode de chiffrement complet



4/ redémarrer l'ordinateur lorsque cela est demandé

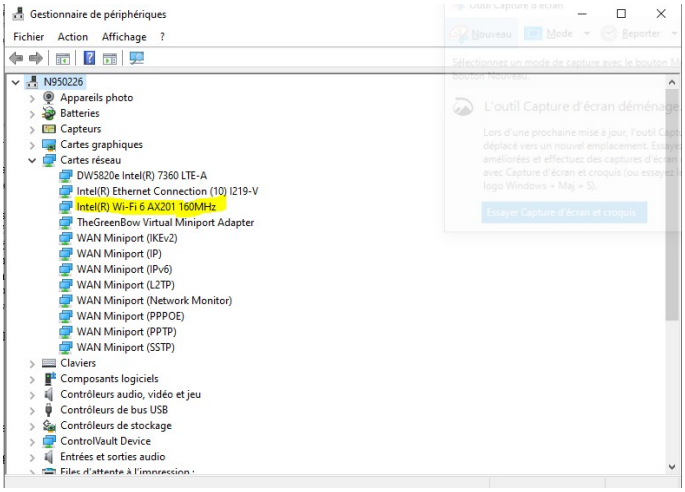
5/ Au redémarrage, si l'interface CRYHOD apparaît, renseigner le code pin de la carte agent administrateur pour déverrouiller CRYHOD :

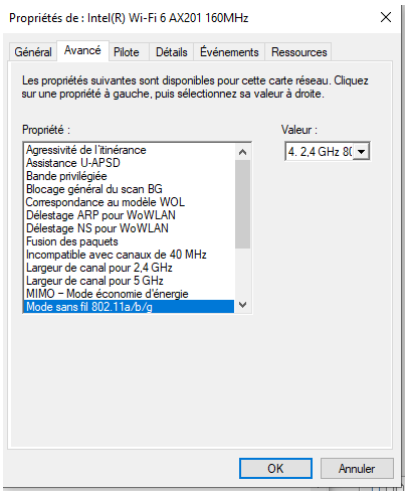
6/ Ouvrir la session Windows avec la carte agent (saisir le code PIN) et laisser le chiffrement se dérouler.

/!\ Avant tout autre manipulation, laisser le cryptage s'effectuer jusqu'à la fin et redémarrer le poste.

Divers : *Depuis une session admin (ex :admin-pref95)*

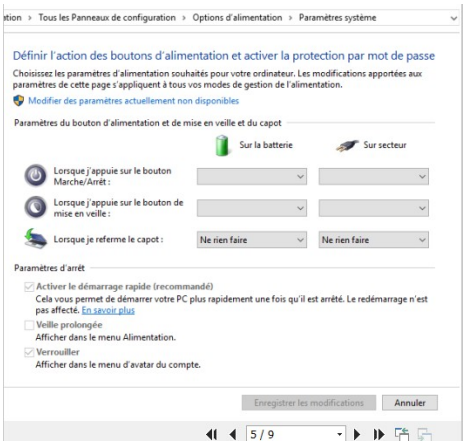
● Modifier la bande de fréquence utilisée par la carte Wi-Fi :
Gestion de périphérique (clic droit sur le logo Windows) > Cartes réseau > choisir la carte wifi

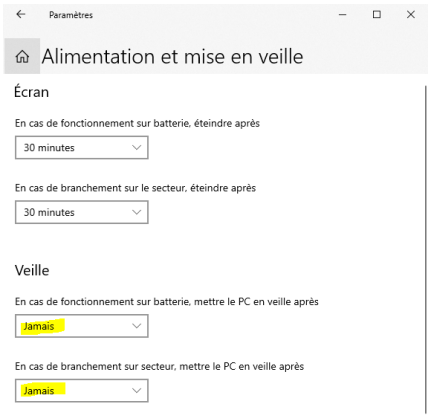




Clic droit sur la carte Wi-Fi > Propriété > Avancé.
Changer la propriété de Mode sans fil 802.11a/b/g en 4. 2,4 GHz 802.11b/g.

● Réglages divers :
- Capot et mise en veille : « Jamais » Pour la mise en veille. Pour le capot choisir « ne rien faire sur batterie et secteur »
Accéder aux paramètres du capot : panneau de configuration → option d'alimentation → choisir l'action qui suit la fermeture du capot
Accéder aux paramètres de mise en veille : tapez « mise en veille » dans la barre de recherche Windows

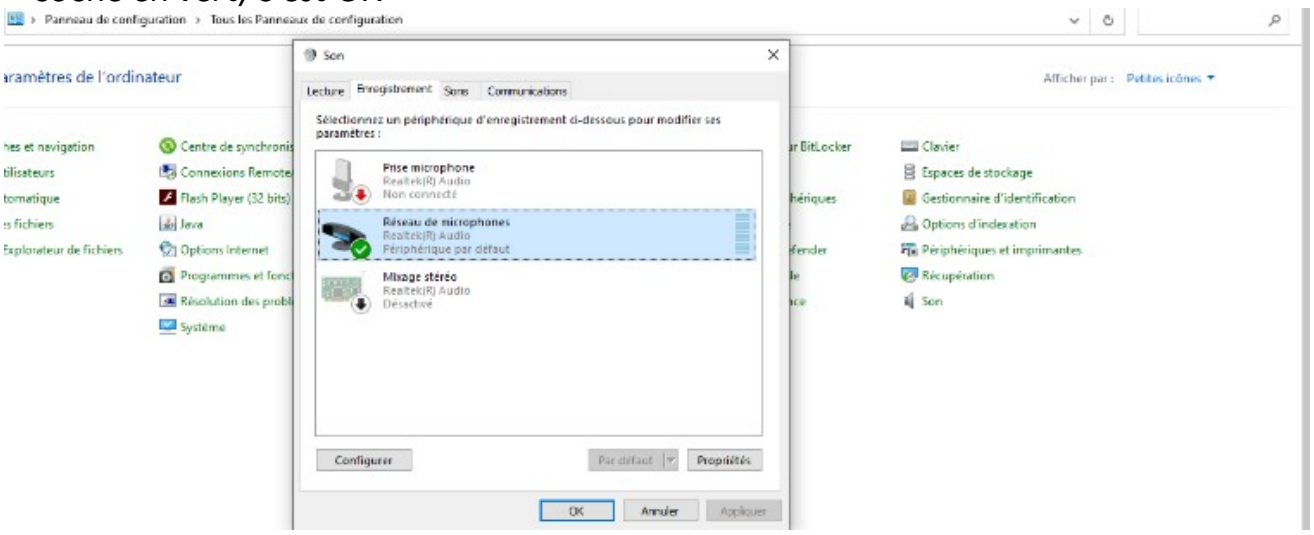




- périphérique audio par défaut ;
    - Lecture : Enceintes

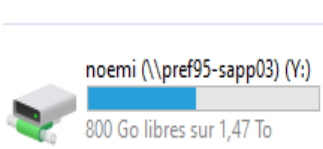
    - Enregistrement : réseau de microphones

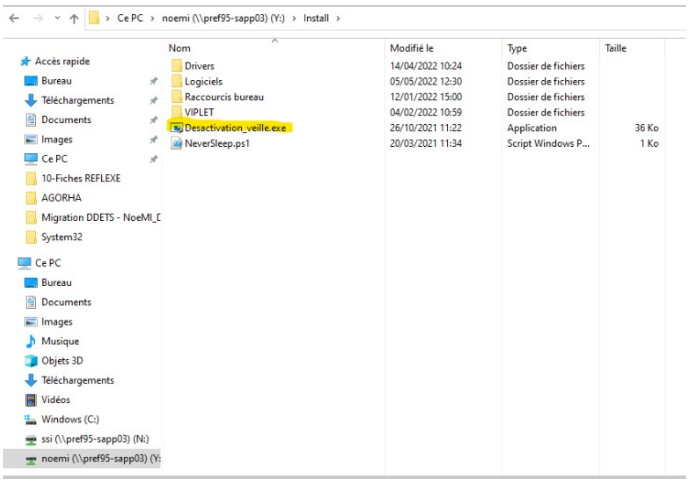
Panneau de configuration → Son →enregistrement → si réseau de microphone coché en vert, c'est OK



- lancer l'exécutable « desactivation_veille.exe »

L'exécutable est à retrouver dans le dossier «install» accessible à partir du lecteur réseau «noemi»



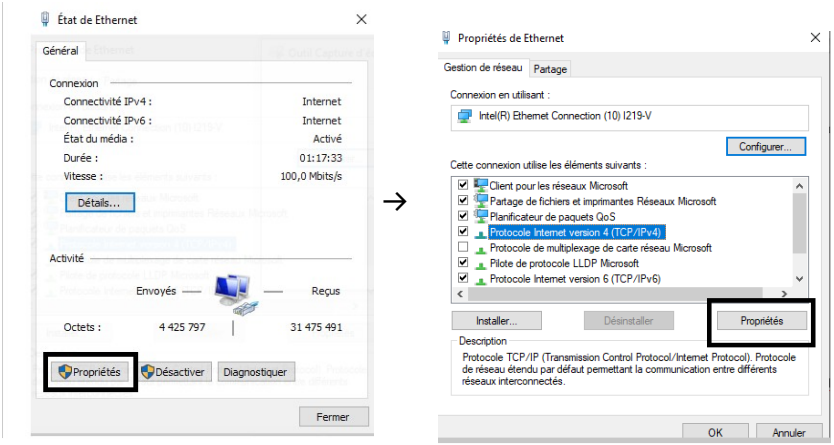


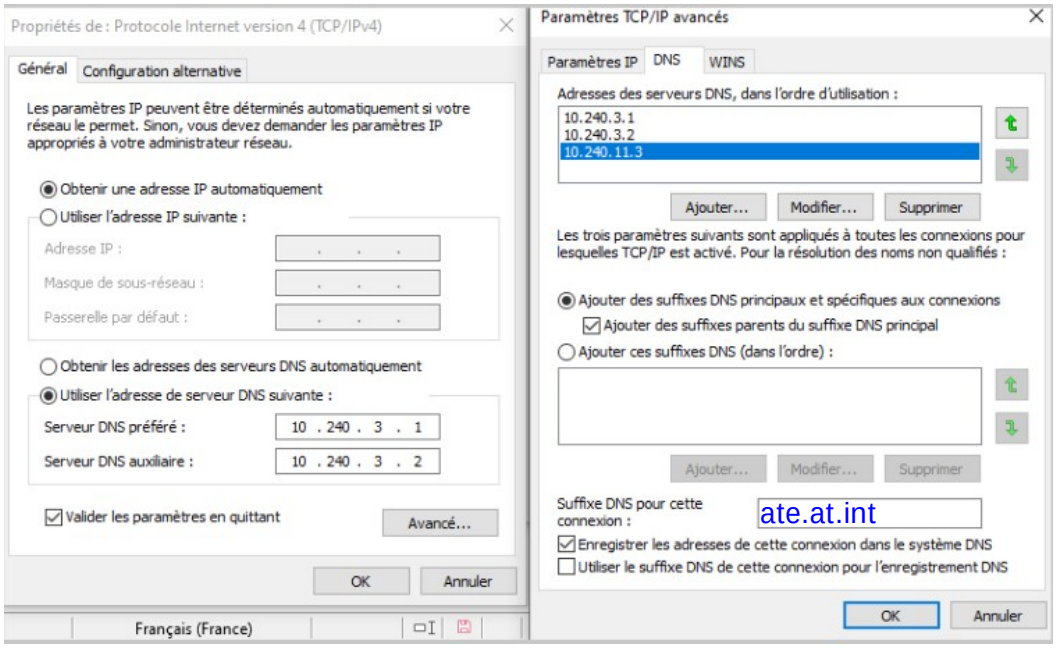
● Renseigner les DNS (**D**omain **N**ame **S**ystem) Nationaux de l'ATE :

10.240.3.1
10.240.3.2
10.240.11.3

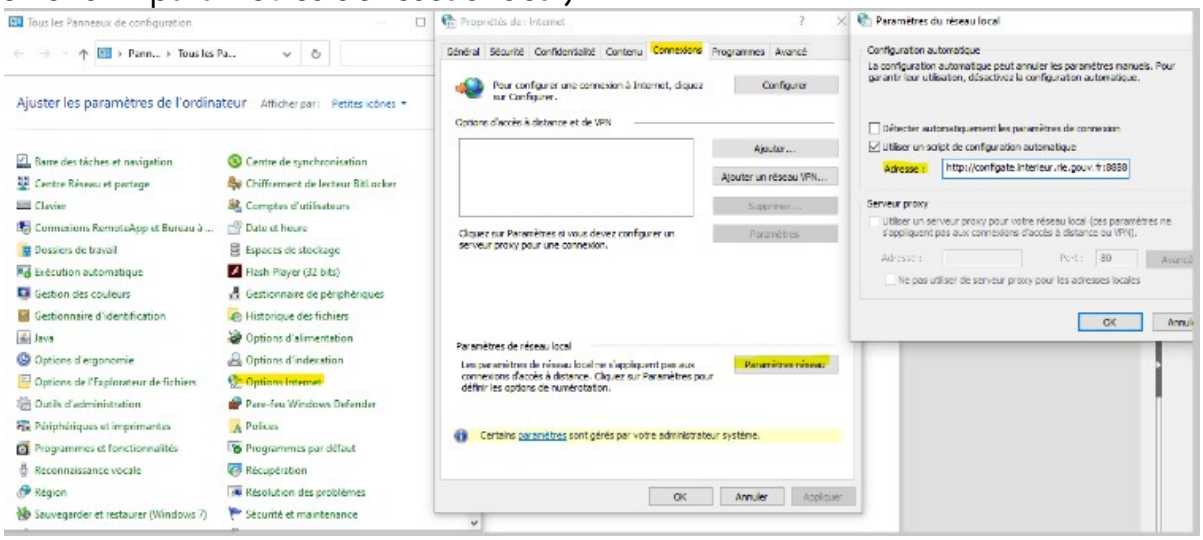
Pour renseigner des DNS :

Panneau de configuration → centre réseau et partage → modifier les paramètres de la carte → Ethernet → propriété → cliquer sur «protocole Internet version 4» puis sur propriété.





• vérifier le paramétrage du proxy (doit se faire automatiquement via GPO) en se rendant dans les options internet (panneau de configuration → Option internet → connexions → paramètres de réseau local)



Le proxy doit être sous la forme suivante :

http://configate.interieur.rie.gouv.fr:8888/configDDCSPP-noemie.pl pour la DDPP et la DDETS

http://configate.interieur.rie.gouv.fr:8888/configDDT.pl pour la DDT