



PREREQUIS	2
Création du compte AD de l'occupant	2
Création du poste dans l'active directory	4
Masterisation « MDT »	5
Paramètres et Chiffrement	10
VPN GREENBOW	13
CHIFFREMENT ET .ZAF	15
Création .zaf	17

Auteur	Titre	Nombre de page	Validateur	Date de validation	Organisation	Date
BELAHA SIDAHMED	Procédure de création d'un NOEMI		LAMINE Rikia		Préfecture des Hauts-de-Seine	29/03/2024



PREREQUIS

Création du compte AD de l'occupant

Tout d'abord identifié le besoin grâce à la fiche d'intervention envoyé par le demandeur : ici crée un poste NOEMI.

NOM* : CÉMOI	Prénom* : DUPONT
Date arrivée* : 01/03/2024	Date départ : 31/07/2024

Nouvel Arrivant

Direction/Service : MVCS

N° RIO* :

Fonction : Stagiaire

Étape-Bureau* : 10^{ème}

Déménagement

N° de bureau de départ :

N° de bureau d'arrivée :

N° de téléphone de départ :

N° de téléphone d'arrivée* :

Besoin matériel

Ordinateur ☐

NOEMI ☒

Imprimante* :

Retrait d'un ordinateur fixe ☐

Nom de l'ordinateur en place :

Imprimante de bureau en place ☐

Imprimante titre (AGDREF-SNPC) ☐

Accès aux ressources réseau

Droits serveurs identique à * EXEMPLE BIENSUR

Accès ORION* : Oui ☒ Non ☐

Cadre A ☒

Par conséquent, nous allons créer dans l'AD (active directory) **Monsieur DUPONT** .

Mais nous devons copier ces droits sur **EXEMPLE BIENSUR**.

CEMOI DUPONT	Utilisateur	PREF92/DMI/ELOIGNEMENT
--------------	-------------	------------------------



Nous allons faire un clic droit sur ce profil, et cliquer sur copier...

Copier l'objet - Utilisateur

Créer dans : at.int/Zone IdF/PREF92/PREF-NANTERRE/Utilisateurs

Prénom : DUPONT Initiales :

Nom : CEMOI

Nom complet : CEMOIDUPONT

Nom d'ouverture de session de l'utilisateur :

CEMOIDU @minint.fr

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

AT\

< Précédent Suivant > Annuler

La règle à respecter est très simple :

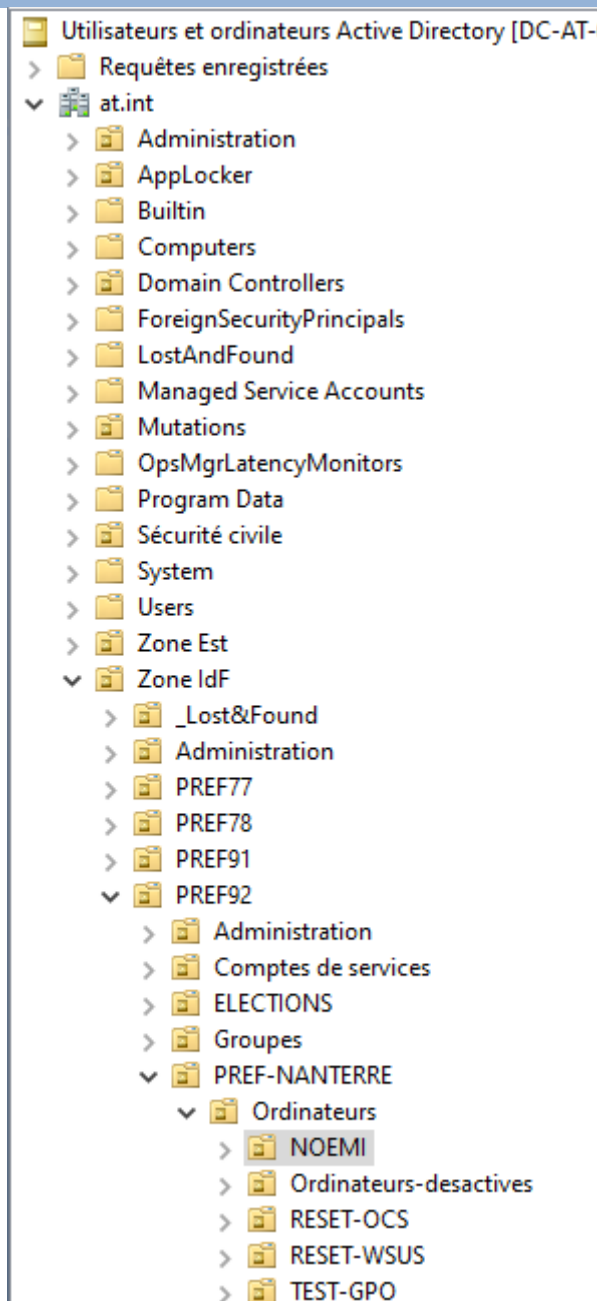
- Nom d'ouverture de session doit être le nom de l'utilisateur et les deux premières lettres de son prénom, les deux éléments doivent se suivre et être en MAJUSCULE !
- S'il s'agit d'un nom composé, on ne met jamais d'espace, à la place on insère ce tiret « - »

Il faut créer le compte dans l'AD sans oublier de l'ajouter au membre du groupe **NOEMI**

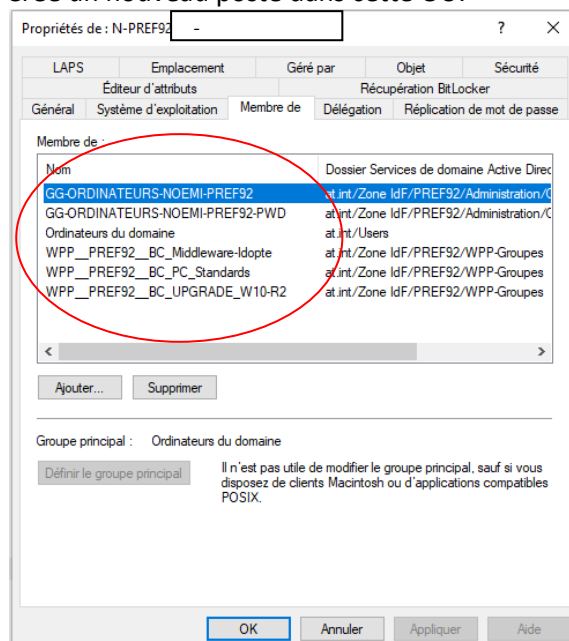
Création du poste dans l'active directory



ACTIVE DIRECTORY > at.int > Zone IdF > PREF92 > PREF-NANTERRE > Ordinateurs > NOEMI



Crée un nouveau poste dans cette OU.



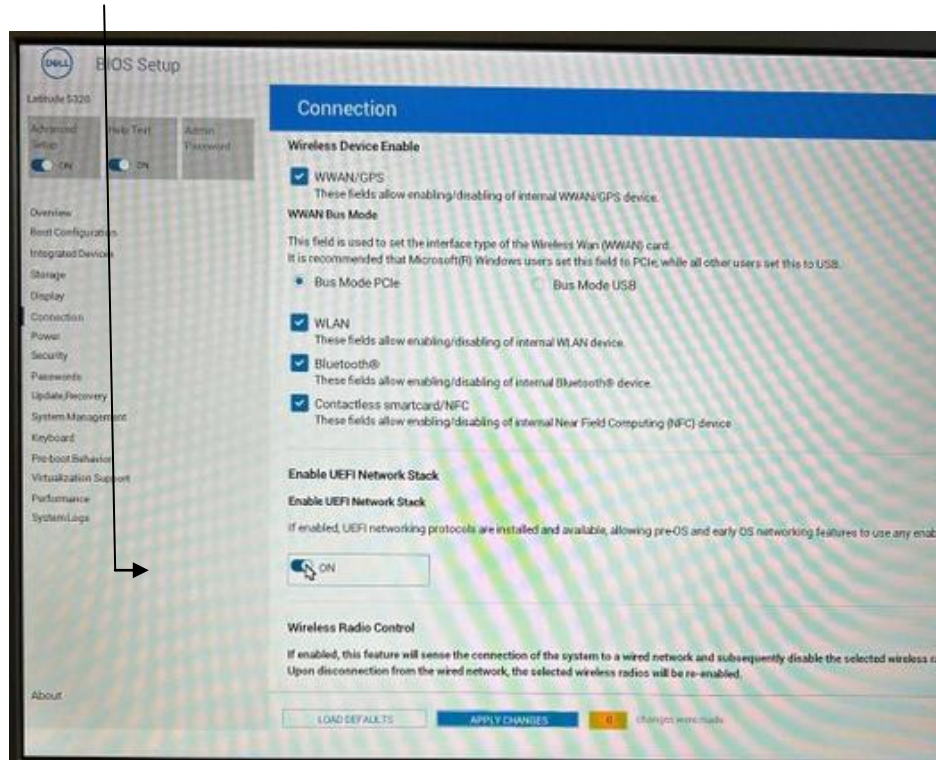
Ajouter le NOEMI précédemment crée dans les groupes ci-dessus

Nous pouvons passer à l'étape de Masterisation.

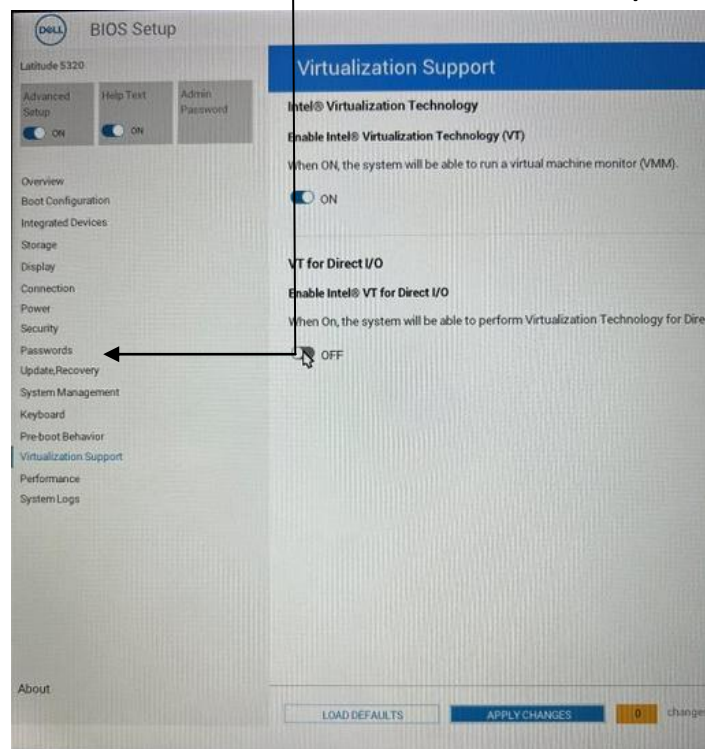


Masterisation « MDT »

Avant d'entamer le MDT nous allons ajuster certain paramètres. Nous allons activer ce paramètre ci-dessous. « **UEFI Network Stack** » cela va nous permettre de **masteriser le poste** sur le réseau RIE.

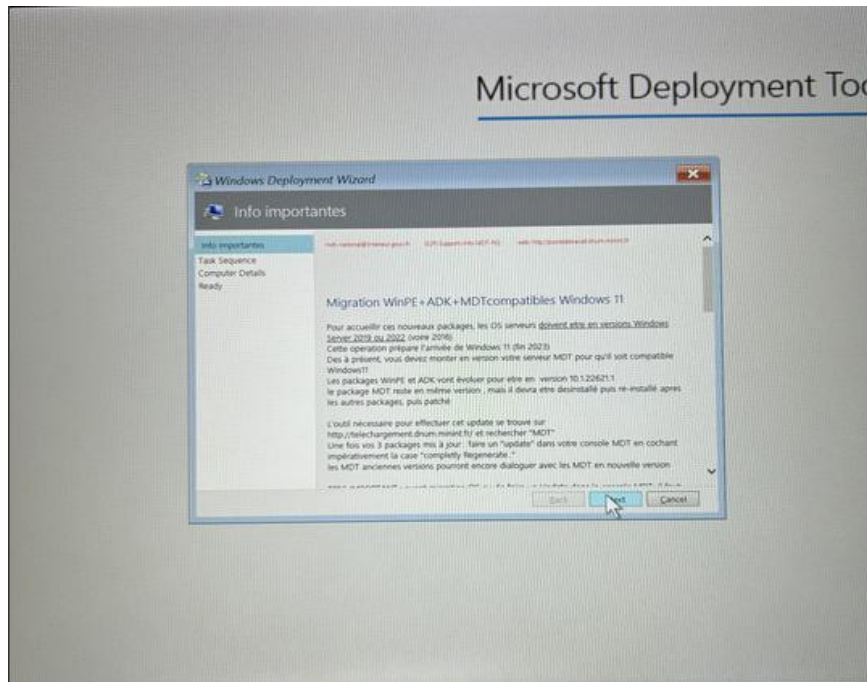


Nous allons ensuite désactiver le « **VT for Direct I/O** »



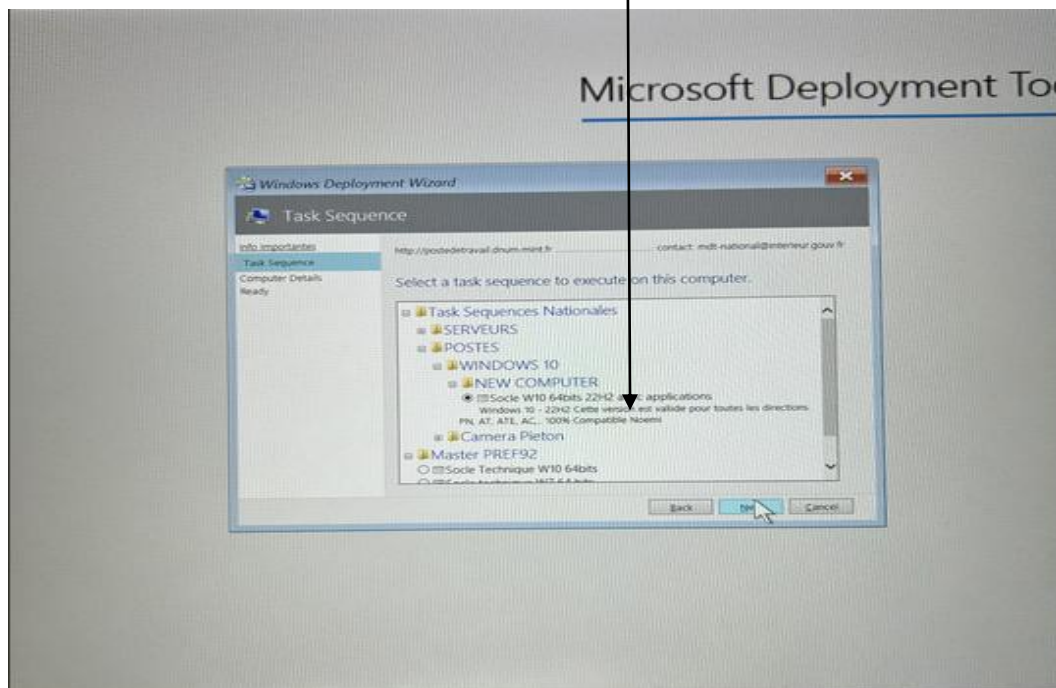


Nous pourrons ensuite Cliquer sur EXIT et sauvegarder les paramètres. Au redémarrage nous appuyons F12 pour accéder Menu « Boot » et enfin nous sélectionnons **NIC IPV4** ou **USB IPV4** afin d'accéder au MDT « Microsoft Deployment Toolkit » . On continue vers l'étape suivante en cliquant Next.



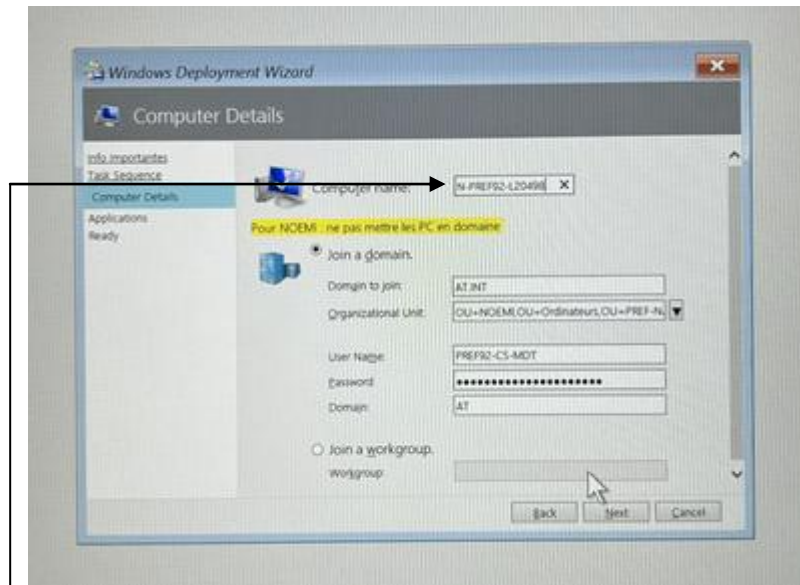
Etape suivant nous arrivons vers une interface ou nous pouvons sélectionner **les différentes versions** dans notre cas cela sera constamment :

POSTES > WINDOWS 10 > NEW COMPUTER > **Socle W10 64 bits 22H2**





Une fois ceci sélectionné nous pouvons accéder à l'étape suivante.

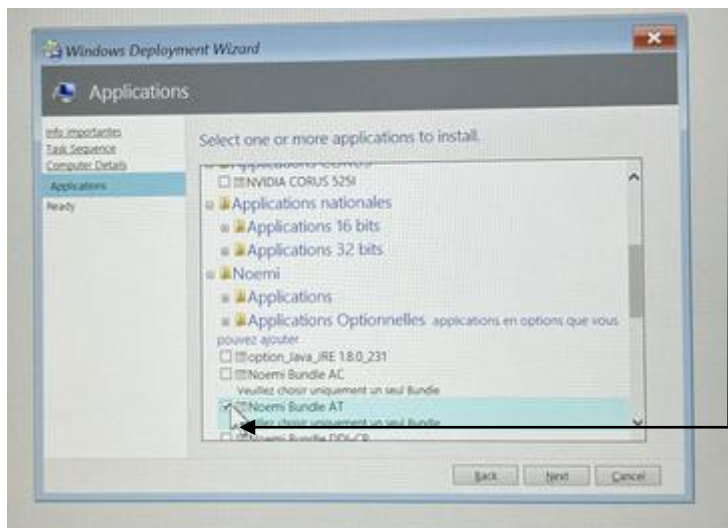
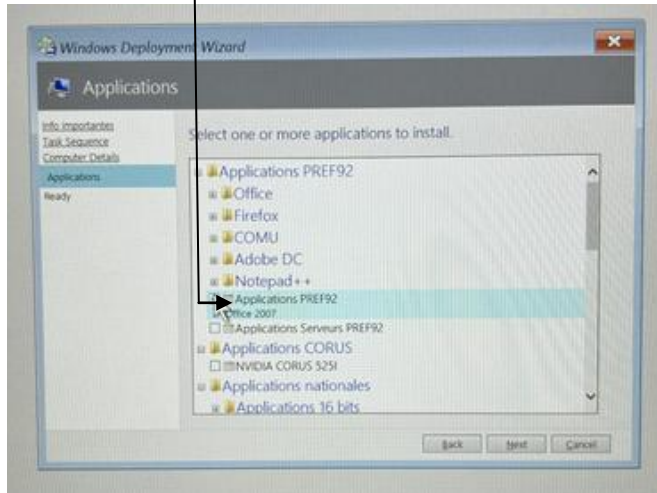


Nous arrivons au **nommage du PC**, il faut changer le nom attribué par défaut.

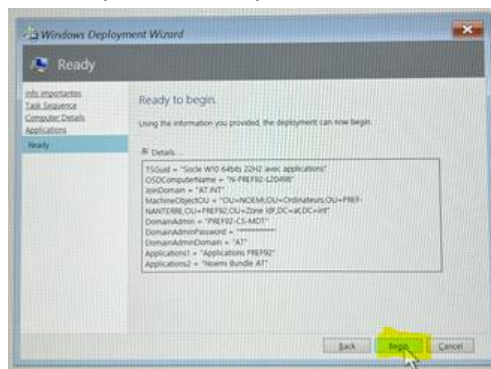
> **N-PREF92-L20XXX**

Une fois ceci effectué nous allons sélectionner **les applications celons notre besoin**

« **Applications PREF92** » ainsi que le bundle le notre « **Bunddle AT** ».



Pour finir nous avons le résumé de nos paramètres, pour **lancer le MDT** il nous suffit juste de



cliquer sur le bouton « Begin ».





Paramètres et Chiffrement

Lors du premier démarrage nous devons obligatoirement nous connecter avec le compte

admin-local (KEYPASS)

Si vous n'arrivez pas à vous connecter avec un autre utilisateur cela veut dire que vous êtes en workgroup (bug du MDT)

Pour cela nous allons dans PARAMETRES > SYSTEME > Renommer ce PC (avancé)

Une page va apparaître cliquer sur :

Renommer ce PC (avancé)

À propos de

Votre ordinateur est surveillé et protégé.

[Voir les détails dans la sécurité Windows](#)

Spécifications de l'appareil

Nom de l'appareil	N-PREF92-L20498
Processeur	11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz 1.38 GHz
Mémoire RAM installée	16 Go (15,7 Go utilisable)

Paramètres associés

[Paramètres de Bitlocker](#)

[Gestionnaire de périphériques](#)

[Bureau à distance](#)

[Protection du système](#)

[Paramètres avancés du système](#)

[Renommer ce PC \(avancé\)](#)



Renommé ce PC (avancé) > Modifier... > Domaine : at.int> OK

> **S'authentifier avec un utilisateur possédant les droits administrateur**

Propriétés système

Paramètres système avancés Protection du système Utilisation à distance

Nom de l'ordinateur Matériel

Windows utilise les informations suivantes pour identifier votre ordinateur sur le réseau.

Description de l'ordinateur :

Par exemple : "L'ordinateur du salon" ou "L'ordinateur d'Antoine".

Nom complet de l'ordinateur : N-PREF92-L20498

Groupe de travail : WORKGROUP

Pour utiliser un Assistant et vous joindre à un domaine ou un groupe de travail, cliquez sur Identité sur le réseau.

Identité sur le réseau...

Pour renommer cet ordinateur ou changer de domaine ou de groupe de travail, cliquez sur Modifier.

Modifier...

OK Annuler Appliquer

Modification du nom ou du domaine de l'ordinateur

Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influencer sur l'accès aux ressources réseau.

Nom de l'ordinateur : N-PREF92-L20498

Nom complet de l'ordinateur : N-PREF92-L20498

Autres...

Membre d'un

☒ Domaine : at.int

☐ Groupe de travail : WORKGROUP

OK Annuler

La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponible sur cet écran



Le poste va redémarrer, désormais il sera nécessaire de basculer sur le compte.

MDT NOEMI :

ID : NOEMI

MDP : KEYPASS

Vérifier les mises à jour et attendre qu'elles soient bien toutes opérationnelles.

Faire plusieurs recherches de mises à jour avant de se déconnecter de cette session.

Windows Update

*Votre organisation gère certains paramètres
[Afficher les stratégies de mise à jour configurées](#)



Recherche des mises à jour en cours...

- Recevez les dernières mises à jour dès qu'elles sont disponibles
Ce paramètre n'est pas disponible en raison de la stratégie de votre organisation ☐ Désactivé
- Suspendre les mises à jour pendant 7 jours
La mise en pause n'est pas disponible conformément à la stratégie de votre organisation
- Afficher l'historique des mises à jour
Voir les mises à jour installées sur votre appareil
- Options avancées
Paramètres et contrôles de mise à jour supplémentaires

Windows Update

*Votre organisation gère certains paramètres
[Afficher les stratégies de mise à jour configurées](#)



Vous êtes à jour

Dernière vérification : aujourd'hui, 09:37

Rechercher des mises à jour

- Recevez les dernières mises à jour dès qu'elles sont disponibles
Ce paramètre n'est pas disponible en raison de la stratégie de votre organisation ☐ Désactivé
- Suspendre les mises à jour pendant 7 jours
La mise en pause n'est pas disponible conformément à la stratégie de votre organisation
- Afficher l'historique des mises à jour
Voir les mises à jour installées sur votre appareil
- Options avancées
Paramètres et contrôles de mise à jour supplémentaires



VPN GREENBOW

IMPORT CERTIFICAT

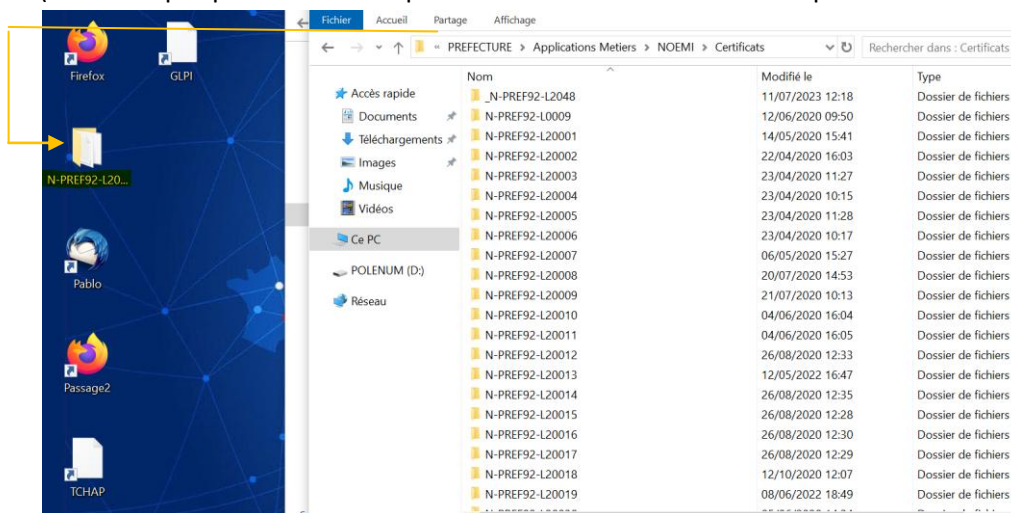
Se connecté sur une session administrateur et respecter les étapes décrite ci-dessous.

Récupérer le certificat concernant le poste NOEMI dans le chemin relatif ci-dessous.

Le chemin relatif : M:\PREFECTURE\Applications Metiers\NOEMI\Certificats (faire un copier/coller)

Ensuite aller récupérer le certificat dans le dossier ci-dessous et l'extraire*.

(*Ce n'est pas possible de récupérer le certificat sur le réseau depuis l'interface d'interaction)



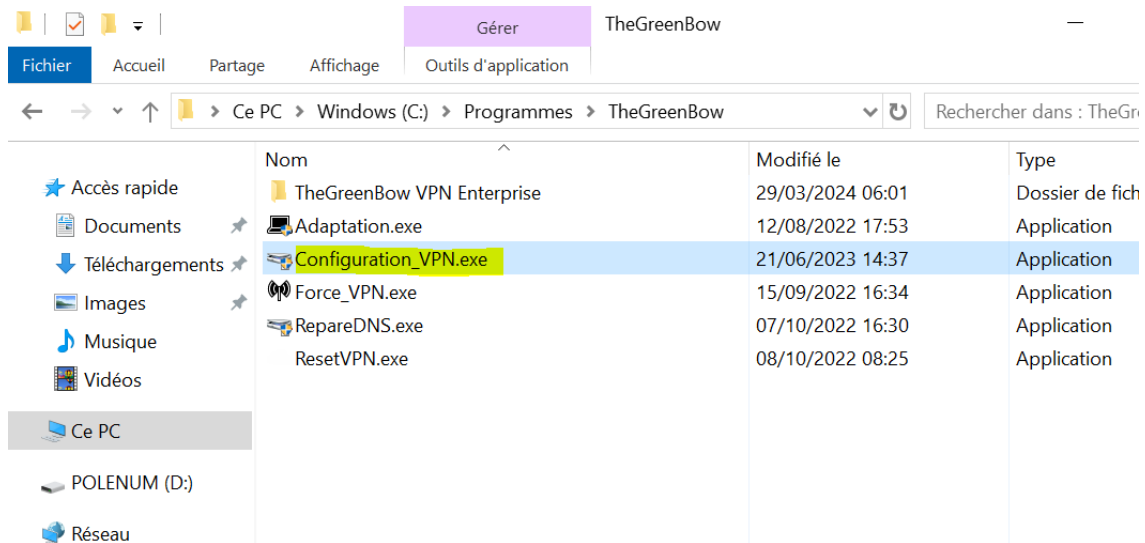


Le VPN va apparaître ensuite nous nous dirigerons vers l'emplacement du dossier de celui-ci.

Un dossier comme ceci devrait apparaître.

Chemin relatif : C:\Program Files\TheGreenBow

Pour installer le certificat. Ouvrir l'exécutable de configuration VPN.



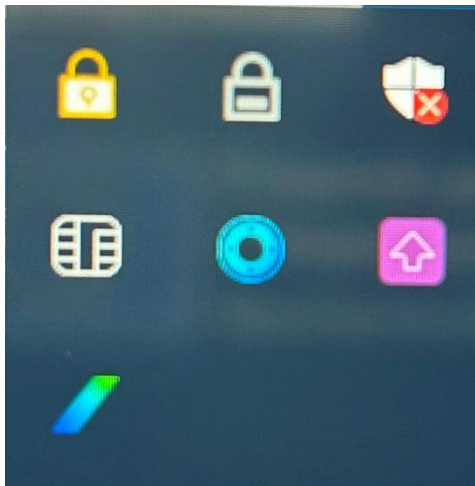


CHIFFREMENT ET .ZAF

Dans un premier temps se connecter avec une session du administrateur carte agent ministérielle
« **IMPORTANT** » sans cela le chiffrement ne pourras pas ce lancer.

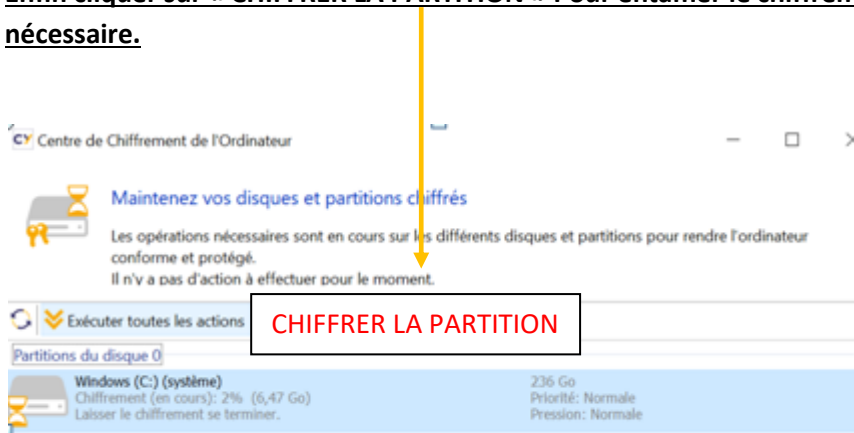
Insérer la carte et renseigner le code PIN.

Se diriger vers l'interface ci-dessous en cliquant sur la petite flèche.



Puis le cadenas gris afin d'accéder a l'interface ci-dessous.

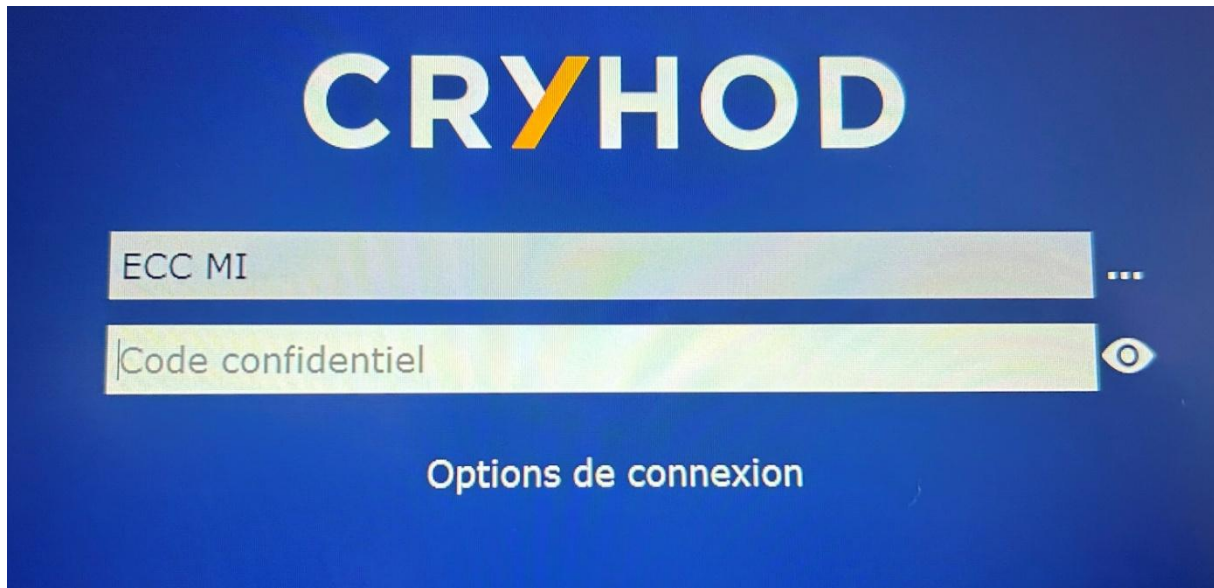
Enfin cliquer sur « CHIFFRER LA PARTITION » Pour entamer le chiffrement un redémarrage est nécessaire.



L'interface CRYHOD s'ouvre et demande le code de la carte agent.

Une fois l'interface CRYHOD passé

Se connecter ensuite avec une session Windows admin.



Attendre la fin du chiffrement.



Création .zaf

Pas de .zaf mais carte CAM

- Donner RDV a l'agent
- Se connecter à la session agent
- Insérer la carte agent
- Renseigner le code PIN dans l'interface (CRYHOD)
- Si nous arrivons à passer l'interface CRYHOD avec le code de la CAM alors : REUSSITE
- Si vous rencontrer un problème avec l'étape précédente utilisé la carte d'un agent « SIDSIC »

Vérifier dans l'AD : prenom.nom.rio

Général Adresse Compte Profil

Nom d'ouverture de session de l'utilisateur :

gil [] 0545

Propriété []

? X

Général	Adresse	Compte	Profil	Téléphones	Organisation	Certificats publiés
Membre de	Réplication de mot de passe	Objet	Sécurité	Environnement	Sessions	
Contrôle à distance	Profil des services Bureau à distance	COM+	Éditeur d'attributs			

Attributs :

Attribut	Valeur
displayNamePrintable	<non défini>
distinguishedName	[] J=Utilisateurs,OU:
division	<non défini>
dSASignature	<non défini>
dSCorePropagationD...	13/03/2024 19:13:58 Paris, Madrid; 11/12/2
dynamicLDAPServer	<non défini>
employeeID	165 []

Vérifier l'employeeID

Vérifier les certificats

[]



Propriétés de : CAMPMAS GILLES

?

✕

Membre de	Réplication de mot de passe	Objet	Sécurité	Environnement	Sessions
Contrôle à distance	Profil des services	Bureau à distance	COM+	Éditeur d'attributs	
Général	Adresse	Compte	Profil	Téléphones	Organisation
Certificats publiés					

Liste des certificats X509 publiés pour le compte d'utilisateur

Délivré à	Délivré par	Rôles prévus	Date d'expira
GIL [redacted] 505...	AC PERSON...		19/10/2026
GIL [redacted] 505...	AC PERSON...	Authentification du cli...	19/10/2026
GIL [redacted] 505...	AC PERSON...		19/10/2026

Ouvrir la session de l'utilisateur.

Cliquer sur suivant. Pour les nouveaux arrivants la configuration se fera en mot de passe.

Une directive précise est a respecté pour les mots de passe (voir avec le service support)

Cliquer sur suivant puis TERMINER la (.zaf) va se créer.

Se rendre dans l'interface ci-dessous



➤ Clic droit sur le cadenas



SI Problème rencontrer respecter cette procédure

La 1 ère étape est d'aller vérifier les certificats comme montrer précédemment.

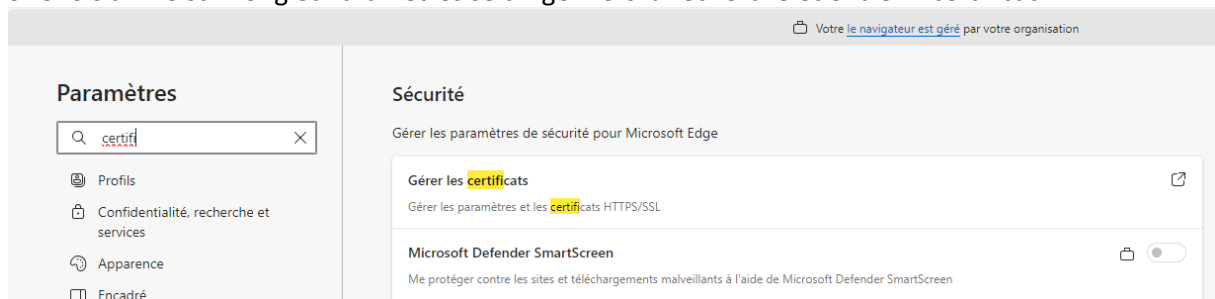
SI non

Insérer la carte dans un lecteur ou dans le lecteur du poste.

Lancer un navigateur (préférence : edge) Se diriger vers ce symbole puis cliquer sur « paramètre »

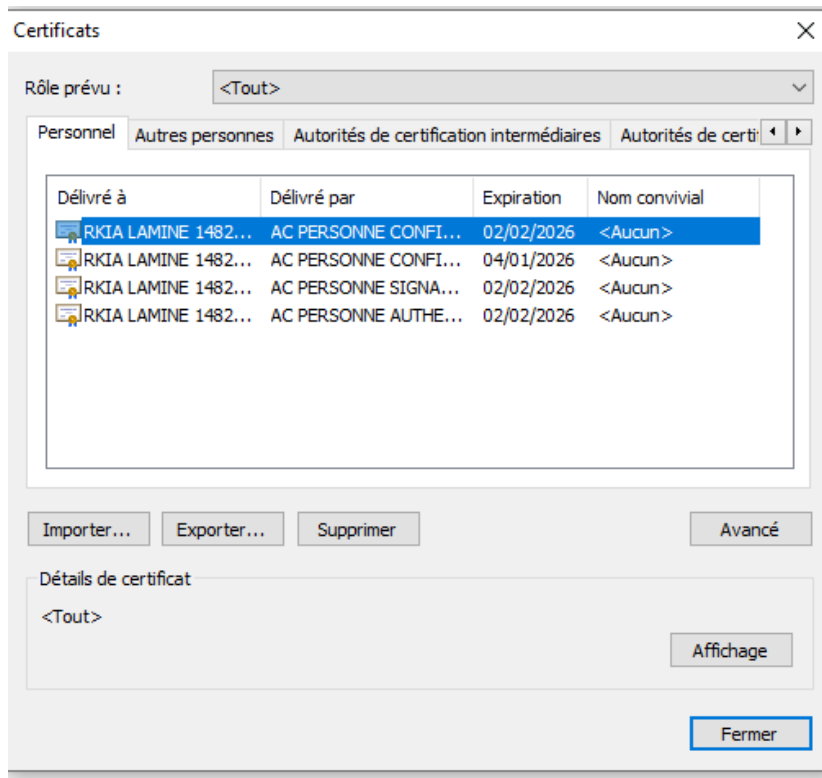


Une fois arrivé sur l'onglet Paramètres se diriger vers la recherche et entrer « certificat »





Cliquer sur « Gérer les certificats »



Une page comme celle ci devrait apparaitre.

Nous allons donc transférer les certificats et les insérer manuellement dans l' AD

Afin de continuer vers cette voie cliquer sur exporter et transférer chaque certif vers un dossier sur votre bureau (il faudra le supprimer après opération).

Sélectionner un certificat et cliquer sur exporter puis continuer de cliquer sur suivant sans modifier jusqu'à l'interface ou nous pourrons sélectionner le chemin vers le quelle le certificat sera exporter.



← Assistant Exportation du certificat

Bienvenue dans l'Assistant Exportation du certificat

Cet Assistant vous aide à copier des certificats, des listes de certificats de confiance et des listes de révocation des certificats d'un magasin de certificats vers votre disque.

Un certificat, émis par une autorité de certification, confirme votre identité et contient des informations permettant de protéger des données ou d'établir des connexions réseau sécurisées. Le magasin de certificats est la zone système où les certificats sont conservés.

Pour continuer, cliquez sur Suivant.

Suivant

Annuler



← Assistant Exportation du certificat

Exporter la clé privée

Vous pouvez choisir d'exporter la clé privée avec le certificat.

Les clés privées sont protégées par mot de passe. Si vous voulez exporter la clé privée avec le certificat, vous devez taper un mot de passe dans une prochaine page.

Voulez-vous exporter la clé privée avec le certificat ?

☐ Oui, exporter la clé privée

☒ Non, ne pas exporter la clé privée

Remarque : la clé privée associée est marquée comme ne pouvant pas être exportée. Seul le certificat peut être exporté.

Suivant

Annuler



← Assistant Exportation du certificat

Format du fichier d'exportation

Les certificats peuvent être exportés dans divers formats de fichiers.

Sélectionnez le format à utiliser :

- ☒ X.509 binaire encodé DER (*.cer)
- ☐ X.509 encodé en base 64 (*.cer)
- ☐ Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.P7B)
 - ☐ Inclure tous les certificats dans le chemin d'accès de certification, si possible
- ☐ Échange d'informations personnelles - PKCS #12 (.PFX)
 - ☐ Inclure tous les certificats dans le chemin d'accès de certification, si possible
 - ☐ Supprimer la clé privée si l'exportation réussit
 - ☐ Exporter toutes les propriétés étendues
 - ☐ Activer la confidentialité de certificat
- ☐ Magasin de certificats sérialisés Microsoft (.SST)

Suivant

Annuler



← Assistant Exportation du certificat

Fichier à exporter

Spécifiez le nom du fichier à exporter

Nom du fichier :

Parcourir...

Suivant

Annuler

Numéroter les fichiers en fonction du nombre de certif présent sur la carte.(créer un dossier pour)



← Assistant Exportation du certificat

Fin de l'Assistant Exportation du certificat

Vous avez terminé l'Assistant Exportation du certificat.

Vous avez spécifié les paramètres suivants :

Nom du fichier	C:\Users\BELAHASI
Exporter les clés	Non
Indure tous les certificats dans le chemin d'accès de certification	Non
Format de fichier	X.509 binaire encod

Terminer

Annuler

Enfin cliquer sur terminer.



Propriétés de : LAMINE Rikia

Membre de	Réplication de mot de passe	Objet	Sécurité	Environnement		
Sessions	Contrôle à distance	Profil des services	Bureau à distance	COM+		
Général	Adresse	Compte	Profil	Téléphones	Organisation	Certificats publiés

Nom d'ouverture de session de l'utilisateur :

@minint.fr

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

☐ Déverrouiller le compte

Options de compte :

- ☐ L'utilisateur devra changer le mot de passe
- ☐ L'utilisateur ne peut pas changer de mot de passe
- ☐ Le mot de passe n'expire jamais
- ☐ Enregistrer le mot de passe en utilisant un chiffrement réversible

Date d'expiration du compte

☒ Jamais

☐ Fin de :