

Par Erwan COPOL et Erwan CLOUX

Créé le 13 mars 2022

Version 1.0

# LA MISE EN PLACE DU TELETRAVAIL

Dossier interne  
ASSURMER

Validé par Claire EDOUARD le 15  
mars 2022

A destination des collaborateurs  
d'AssurMer et remis en main propre

Nombre de pages : 13

# Table des matières

<b>I. Les outils de déploiements.....</b>	<b>3</b>
<b>a. Présentation de Serva .....</b>	<b>3</b>
<b>b. Présentation de WDS .....</b>	<b>4</b>
<b>c. Comparaison des outils .....</b>	<b>4</b>
<b>II. La double authentification .....</b>	<b>4</b>
<b>III. Notre déploiement .....</b>	<b>5</b>
<b>Pré-requis .....</b>	<b>5</b>
<b>Lexique .....</b>	<b>5</b>
<b>a. Préparation de Serva (Serveur) .....</b>	<b>5</b>
<b>b. Préparation de Protectimus (Master) .....</b>	<b>8</b>
<b>c. Préparation de l'image (Serveur) .....</b>	<b>10</b>
<b>d. Démarrage en PXE (Client) .....</b>	<b>10</b>
<b>IV. Documents annexe .....</b>	<b>13</b>
<b>a. Documents utilisateur .....</b>	<b>13</b>
<b>b. Documents d'administration .....</b>	<b>13</b>

# I. Les outils de déploiements

Pour utiliser un ordinateur, celui-ci a besoin d'un système d'exploitation.

Pour installer un système d'exploitation la méthode la plus commune est d'utilisé un lecteur physique (CD, clé USB, etc.) cependant, lorsque l'on a besoin d'installé un système d'exploitation sur beaucoup de postes, cette méthode devient très vite longue. C'est pour répondre à ce problème que le PXE a été créé.

Le PXE pour Pre-boot eXecution Environment est une technologie qui permet à du matériel compatible de démarrer sur une image via un protocole réseau (par exemple TFTP). L'image récupérée peut être celle du système d'exploitation, un outil ou encore une image personnalisée contenant des applications, pilotes...

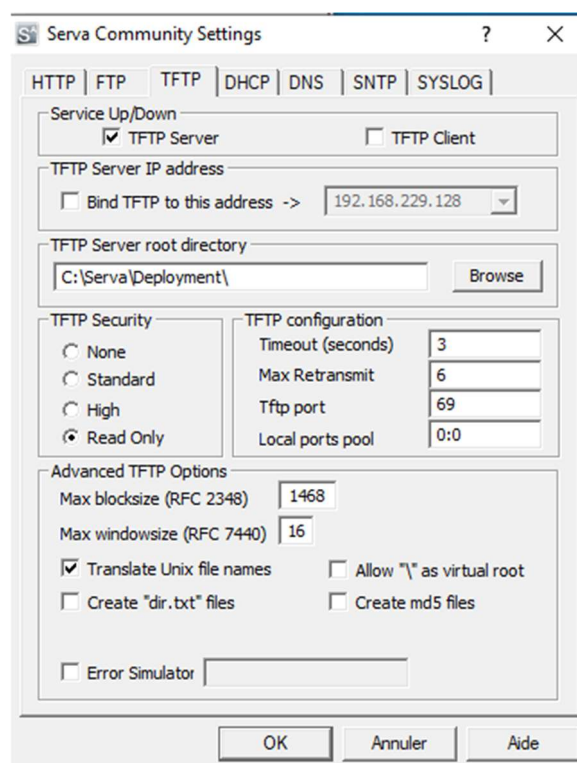
Le PXE repose sur une relation entre un serveur PXE et une ou plusieurs machines clientes. Le serveur PXE peut être initialisé de différentes manières, et nous avons choisi d'en présenter deux : Serva et WDS.

Une machine cliente doit seulement avoir une carte mère compatible PXE pour pouvoir être utilisée.

## a. Présentation de Serva

Serva est un logiciel qui permet de mettre en place un serveur PXE sur une machine Windows traditionnel. Cela est particulièrement intéressant car cette méthode ne nécessite pas l'utilisation d'un Windows Server qui implique un certain coût. Serva, par rapport à d'autres outils propose une multitude de possibilité de configurations.

Serva est un logiciel portable et est « freemium » c'est-à-dire qu'il est utilisable gratuitement mais vas nous limiter dans ses fonctions. Dans sa version gratuite, le logiciel nous permet seulement d'installer 9 machines par 9 machines et le serveur peut être allumée en continue seulement 20 minutes. Pour 67.50€/an, Serva permet de débloquent ces fonctionnalités en illimité.



## b. Présentation de WDS

WDS est un rôle intégré au système d'exploitation Windows Server qui permet de mettre en place un serveur TFTP pour installer un système d'exploitation en PXE. Bien que gratuit, il implique donc obligatoirement la mise en place d'un Windows Server qui est assez coûteuse.

WDS est aussi très restreint en fonctionnalité et en flexibilité, et va par défaut seulement permettre de déployer Windows. De plus, WDS nécessite beaucoup de prérequis pour être fonctionnel tel qu'un contrôleur de domaine (Active Directory) et un rôle DHCP.

## c. Comparaison des outils

Serva	WDS
Pas de prérequis à part une machine Windows ou un serveur Windows	Nécessite de passer par un Windows Server avec plusieurs rôles configurés
Entièrement personnalisable et paramétrable	Utilisé d'obligé le protocole TFTP sans configuration possible
Permet des déploiements d'OS multiples, ne se limite pas à Windows	Par défaut, se limite à Windows
67.50€/an dans le cadre de notre utilisation avec 111 postes	Gratuit (intégré à Windows Serveur)

Nous avons choisi de travailler avec Serva pour sa flexibilité, sa personnalisation possible et son aspect clé en main qui ne nécessite pas de prérequis.

## II. La double authentification

Afin de proposer une double authentification au démarrage du poste, nous avons proposé 3 méthodes possible à l'utilisateur préalablement à la livraison des postes :

- Le SMS (2€/SMS) : Méthode TOTP de code renouvelée toute les 5 min
- L'e-mail (gratuit) : Méthode TOTP de code renouvelée toute les 5 min
- Le Protectimus Two (12€/utilisateur) : boîtier physique générant des codes TOTP toute les 5 min

Le TOTP pour Time-based One-Time Password est un moyen d'authentification OTP (One-Time Password) qui se base sur un changement de code à un intervalle régulier (ici 5 minutes).

Afin de vérifier les codes, le poste sera fonctionnel uniquement lorsqu'il sera connecté à Internet.

## III. Notre déploiement

### Pré-requis

- Une machine « Master » qui sera le modèle
- Une ou plusieurs machines « clientes » qui recevront l'image du Master
- Une machine « serveur » qui permettra de déployer notre image

### Lexique

**DHCP** : Attribution automatique d'IP à un réseau

**ProxyDHCP** : Fonctionne sur le même principe que le DHCP mais ne fournit pas réellement d'IP, il permet seulement le fonctionnement du PXE

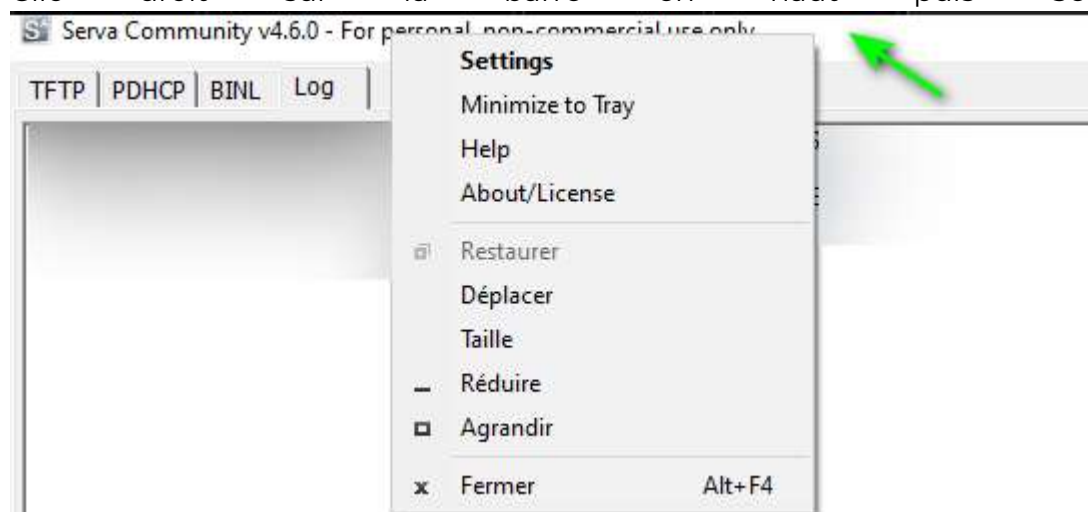
**TFTP** : Protocole réseau de transfert de fichier fonctionnant sur le port UDP 69. Il permet le transfert des images systèmes.

**Master** : Machine destinée à être clonée

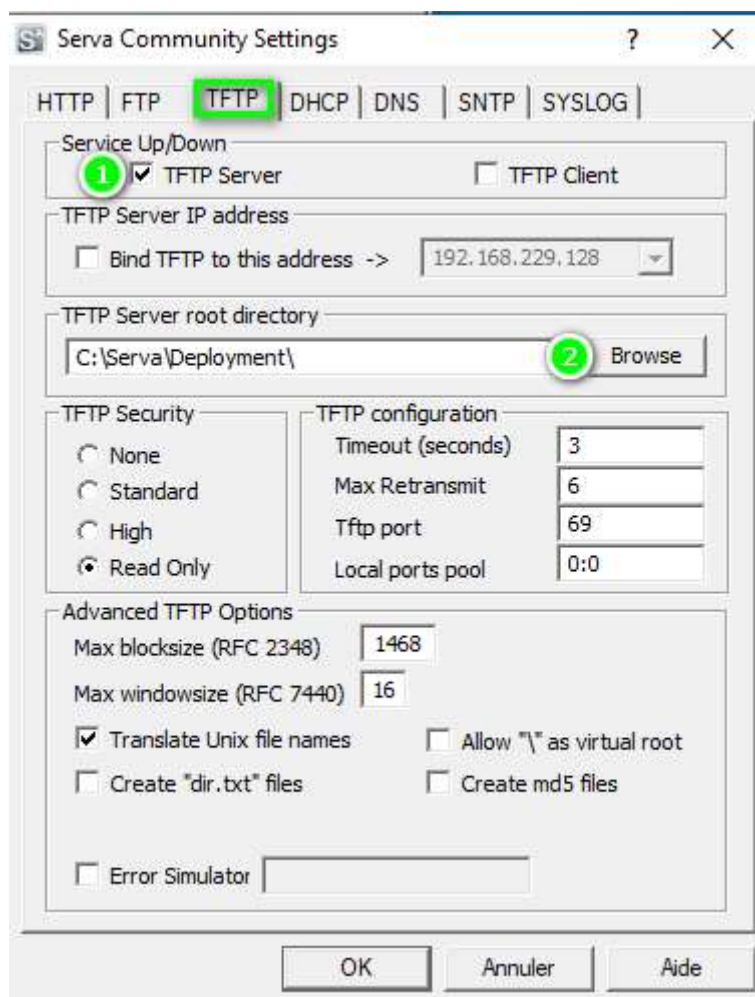
**Client** : Machines recevant le Master

### a. Préparation de Serva (Serveur)

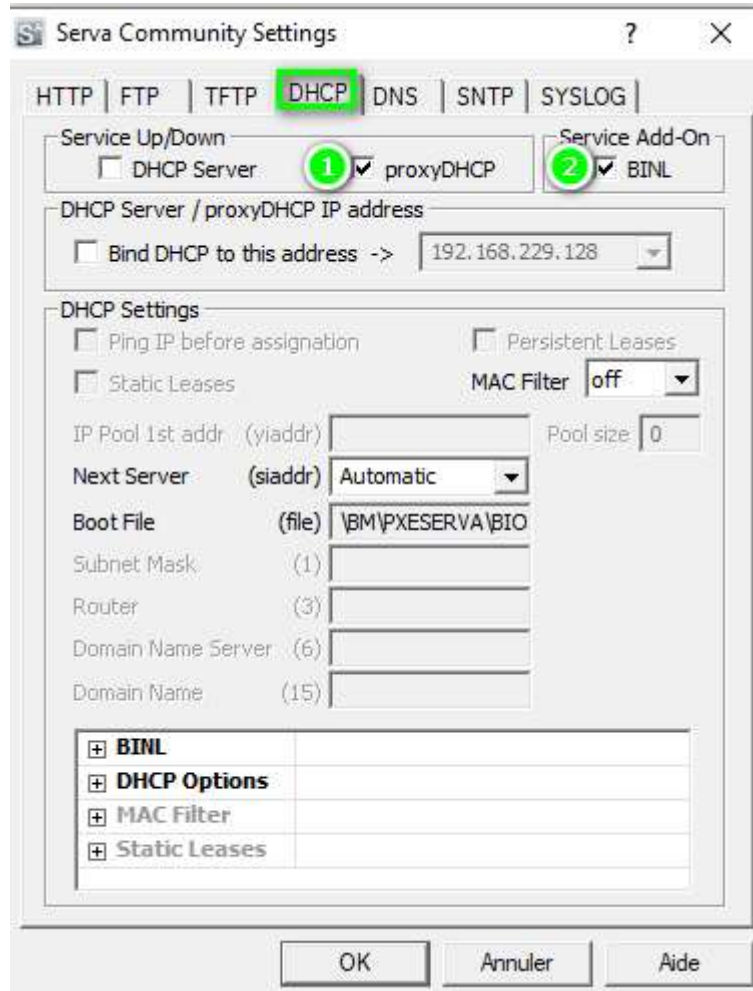
1. Extraire l'archive Serva dans un dossier à la racine du disque dur
2. Lancer Serva64 et autoriser l'accès au réseau
3. Clic droit sur la barre en haut puis Settings



4. Aller dans l'onglet TFTP, cocher TFTP Server, puis Browse pour localiser le répertoire du serveur que l'on va placer dans un dossier situé dans le dossier Serva.



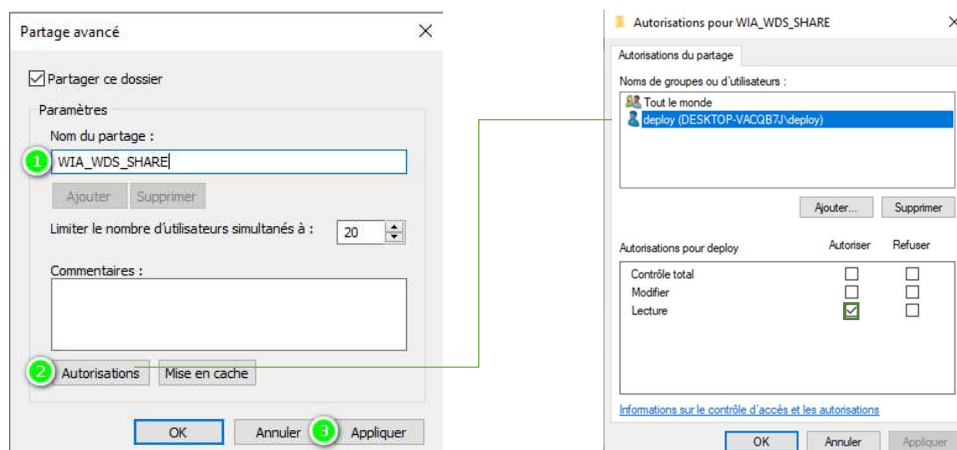
5. Aller dans l'onglet DHCP, et cocher les cases proxyDHCP ainsi que BINL



6. Cliquer sur Ok pour valider et relancer le logiciel
7. Ouvrir CMD et créer un utilisateur avec les identifiants suivant : deploy/deploy. La commande utilisée est la suivante :

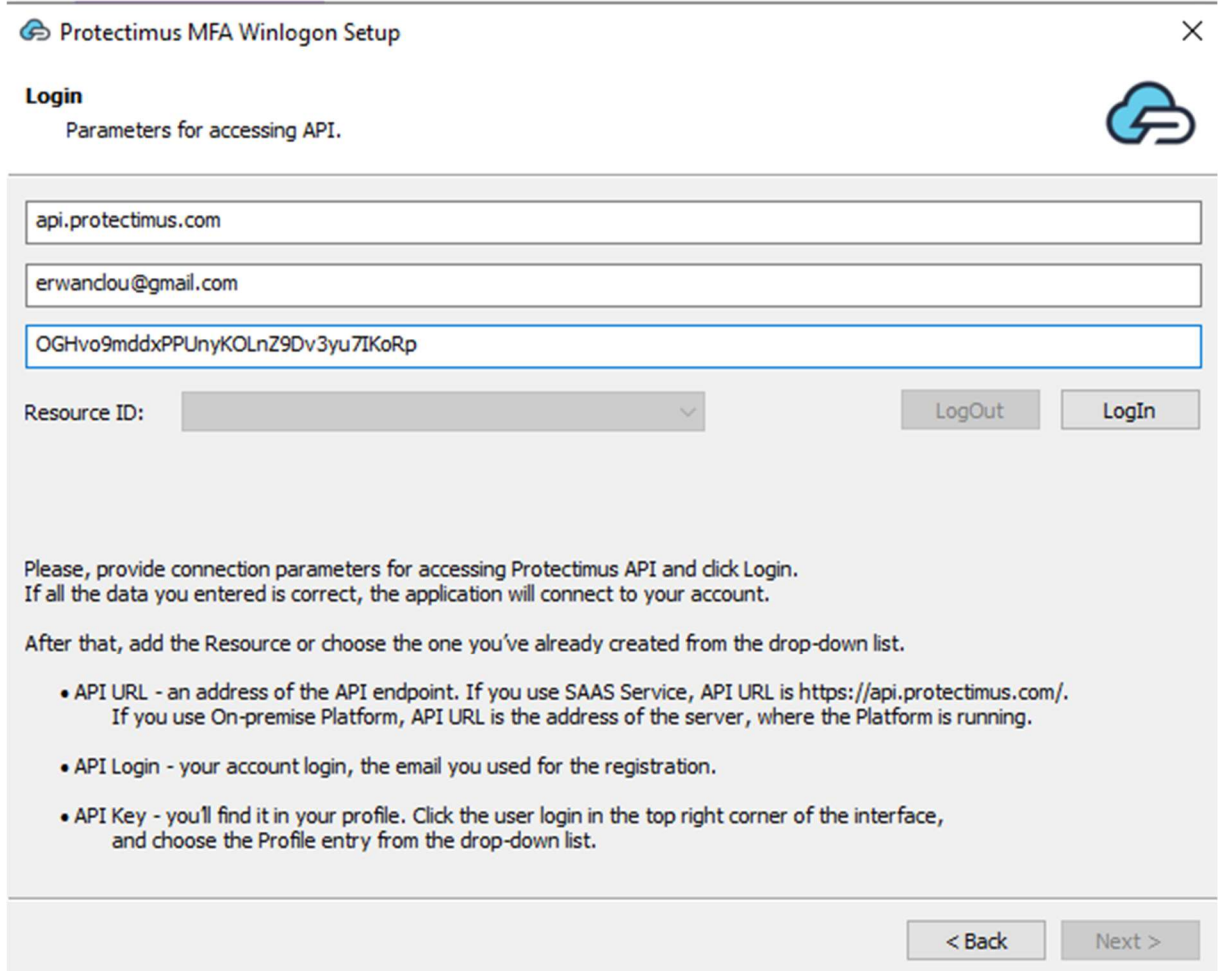
```
net user "deploy" "deploy" /add
```

8. Aller dans dossier du serveur puis trouver WIA\_WDS, puis, faire clic droit Propriété puis Partage et Partage Avancé. Renommer le partage en WIA\_WDS\_SHARE et cliquer sur Autorisations pour ajouter l'utilisateur deploy avec seulement droit de lecture



## b. Préparation de Protectimus (Master)

1. Se connecter à <https://service.protectimus.com/en/>
2. Cliquer sur profile et copier l'API key
3. Installer ProtectimusWinlogon et remplir les informations suivantes :



The screenshot shows the 'Protectimus MFA Winlogon Setup' window. The title bar includes the Protectimus logo and a close button. The window has a 'Login' section with the subtitle 'Parameters for accessing API.' and a Protectimus logo in the top right corner. Below the subtitle are three input fields: the first contains 'api.protectimus.com', the second contains 'erwandou@gmail.com', and the third contains 'OGHvo9mddxPPUnyKOLnZ9Dv3yu7IKoRp'. Below these fields is a 'Resource ID:' label followed by a dropdown menu. To the right of the dropdown are 'LogOut' and 'LogIn' buttons. Below the input fields, there is a paragraph of instructions: 'Please, provide connection parameters for accessing Protectimus API and click Login. If all the data you entered is correct, the application will connect to your account.' followed by another paragraph: 'After that, add the Resource or choose the one you've already created from the drop-down list.' Below these paragraphs is a bulleted list of instructions: '• API URL - an address of the API endpoint. If you use SAAS Service, API URL is https://api.protectimus.com/. If you use On-premise Platform, API URL is the address of the server, where the Platform is running.', '• API Login - your account login, the email you used for the registration.', and '• API Key - you'll find it in your profile. Click the user login in the top right corner of the interface, and choose the Profile entry from the drop-down list.' At the bottom right of the window are '< Back' and 'Next >' buttons.

Protectimus MFA Winlogon Setup

**Login**  
Parameters for accessing API.

api.protectimus.com

erwandou@gmail.com

OGHvo9mddxPPUnyKOLnZ9Dv3yu7IKoRp

Resource ID: ▼ LogOut LogIn

Please, provide connection parameters for accessing Protectimus API and click Login.  
If all the data you entered is correct, the application will connect to your account.

After that, add the Resource or choose the one you've already created from the drop-down list.

- API URL - an address of the API endpoint. If you use SAAS Service, API URL is <https://api.protectimus.com/>.  
If you use On-premise Platform, API URL is the address of the server, where the Platform is running.
- API Login - your account login, the email you used for the registration.
- API Key - you'll find it in your profile. Click the user login in the top right corner of the interface,  
and choose the Profile entry from the drop-down list.

< Back Next >



4. Cliquer sur Login et entrer MACHINES puis Add Resource

Protectimus MFA Winlogon Setup

**Login**  
Parameters for accessing API.

api.protectimus.com

erwandou@gmail.com

OGHvo9mddxPPUnyKOLnZ9Dv3yu7IKoRp

Resource ID: 1693 MACHINES

LogOut Login

Add Resource MACHINES

Balance: 25.00

Please, provide connection parameters for accessing Protectimus API and click Login.  
If all the data you entered is correct, the application will connect to your account.

After that, add the Resource or choose the one you've already created from the drop-down list.

- API URL - an address of the API endpoint. If you use SAAS Service, API URL is <https://api.protectimus.com/>. If you use On-premise Platform, API URL is the address of the server, where the Platform is running.
- API Login - your account login, the email you used for the registration.
- API Key - you'll find it in your profile. Click the user login in the top right corner of the interface, and choose the Profile entry from the drop-down list.

< Back Next >

5. Retourner sur <https://service.protectimus.com/en/>, onglet ressource et cliquer sur la ressource machine créée
6. Cliquer sur Winlogon et remplir de la manière suivante afin de créer automatiquement chaque utilisateur

Winlogon	RDP	Description
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	① If the parameter is deactivated, access to the computer will be completely closed
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	① If the parameter is deactivated, the second factor will not be requested for local or RDP authentication
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	① Provides access to users not registered in the Protectimus service
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	① Provides access without tokens to users, assigned to the resource
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	① Allows unregistered users to get registered and assigned to the current resource at first login
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	① Allows the user to register the token on their own at the first login
Protectimus MAIL		① This type of token will be registered by the user
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	① If the parameter is activated, the second factor will not be requested for RDP access with defined IP addresses
Add IP		

7. Aller dans l'onglet User et Add User pour créer l'utilisateur. Remplir le champ Login, email, First name et Last Name. On peut aussi faire un csv et l'import avec Import User

- 8.a Cliquer sur l'onglet Tokens et Add Token. Dans Software Tokens sélectionner Protectimus MAIL et remplir les informations demandées puis Save
- 8.b Cliquer sur l'onglet Tokens et Add Token. Dans Software Tokens sélectionner Protectimus SMS et remplir les informations demandées puis Save
- 8.c Cliquer sur l'onglet Tokens et Add Token. Dans Hardware Tokens sélectionner Protectimus Two et remplir les informations demandées puis Save
9. Aller dans l'onglet Ressources cliquer sur Assign puis Token et sélectionner les tokens précédemment créé
10. Aller dans l'onglet Ressources cliquer sur Assign puis Users et sélectionner les utilisateurs précédemment créés
11. Renommer l'utilisateur actuel en AssurmerAdmin qui sera le compte administrateur et créer un utilisateur AssurmerUser **SANS SE CONNECTER** avec un mot de passe par défaut : azerty.
12. Redémarrer en Démarrage avancé via les paramètres puis Dépannage, options avancées, invite de commande.
13. Cliquer sur AssurmerAdmin et entrer le mot de passe.
14. Entrer la commande suivante :

```
dism /Capture-Image /CaptureDir:C:\ /ImageFile:C:\install.wim
/Name:windows10 /description:2022-03-28
```

15. Transférer le fichier install.wim généré à la racine du disque sur notre machine serveur

## c. Préparation de l'image (Serveur)

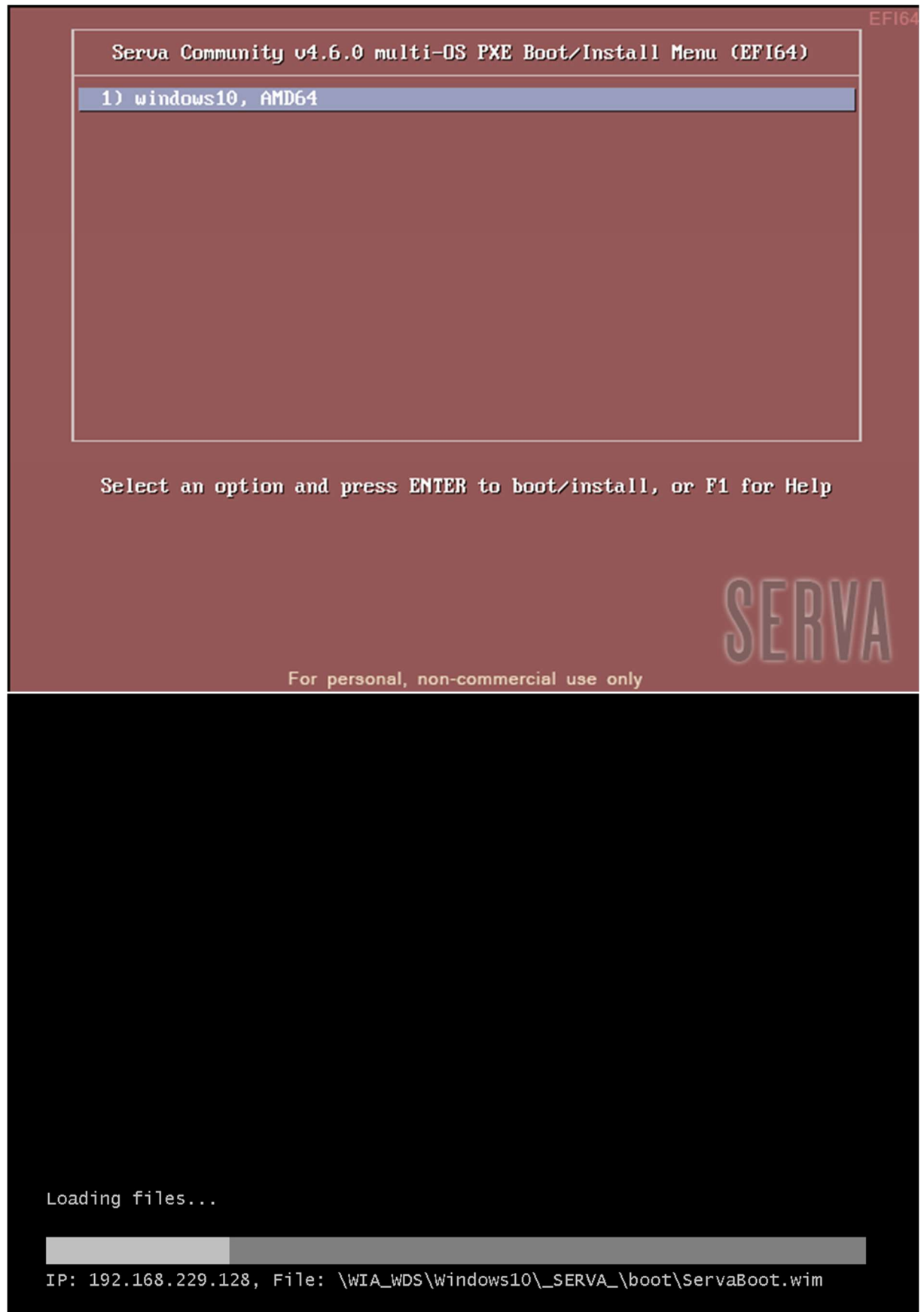
1. Créer un dossier Windows10 dans le dossier WDA\_WDS
2. Déposer install.wim à la racine du disque dur
3. Ouvrir CMD en Administrateur et rentrer la commande suivante
 

```
dism /Export-Image /SourceImageFile:C:\install.wim /SourceIndex:1
/DestinationImageFile:C:\install.esd /Compress:Max /CheckIntegrity
```
4. Extraire un ISO Windows10 dans le dossier C:\Sera\Deployment\WIA\_WDS\Windows10
5. Remplacer le fichier install.esd qui est situé à C:\Sera\Deployment\WIA\_WDS\Windows10\sources par install.esd qui est à la racine du disque
6. Lancer Serva

## d. Démarrage en PXE (Client)

1. Démarrer la machine en PXE (la machine devrait démarrer d'elle même dans ce mode si aucun OS est installé et qu'aucun périphérique n'est branché)

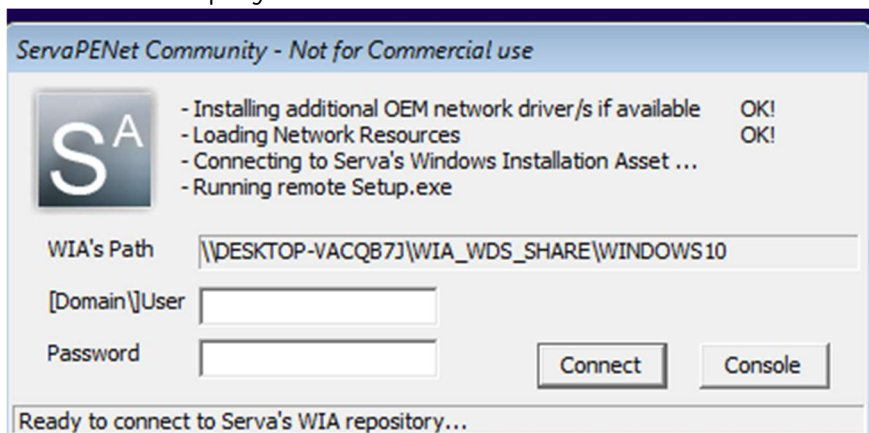
2. Sélectionner Windows10 et faire Entrer



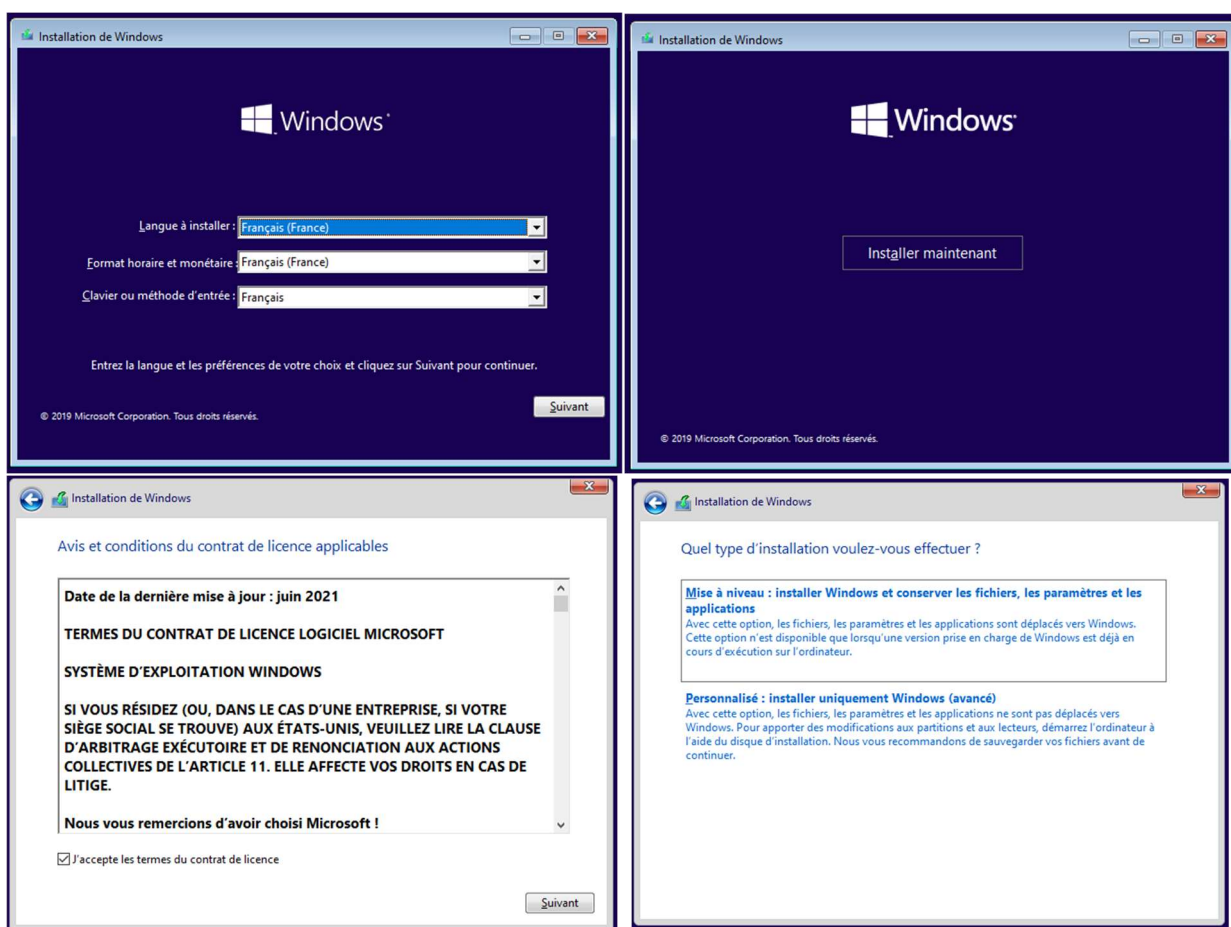
3. Se connecter avec les identifiants suivants :

User : deploy

Password : deploy



4. Attendre que la connexion s'effectue puis effectuer une installation Windows classique en sélectionnant Windows 10 Professionnel et Installer uniquement Windows



La machine cliente est prête à être livrée.

## **IV. Documents annexe**

### **a. Documents utilisateur**

Un document Excel contenant un calendrier est joint à ce dossier afin de pouvoir organiser la remise des postes. Un créneau en cas de problème a été mis en place

Le poste sera livré avec une souris, une sacoche et un manuel utilisateur qui lui permettra de comprendre son appareil ainsi que de le configurer pour la première fois.

Enfin, deux mails ont été envoyés aux utilisateurs, un leur demandant leur choix de méthode d'authentification et un les informant de la future livraison.

### **b. Documents d'administration**

Ce dossier est joint d'un fichier protégé par un mot de passe contenant les données relatives aux utilisateurs (Noms, prénoms, et éventuellement téléphone selon l'authentification choisie).

Afin de garder une trace de l'utilisation de ces données et de les encadrés, nous avons joints un registre de traitement.