

## Safe automatically Domain Join computer – SCCM / MDT OS Deployment without privilege

When the company want to join installed computer to Active Directory domain during OSD process with MDT/SCCM or other solution, there is a huge security breach to use a specific account that have permission to create object.

Because the join domain account is often visible in deployment file (unattend.xml, customsettings,...) during the WinPE phase or OSD.

When I ask why you do this, the answer is normally “the account cannot open the session, the account is audited ...)”

But this practice does not respect the JEA by allowing users limited permission

To solve and secure this operation I developed a free tool “SJDOMAIN” for Offline automatically Domain Join during OSD based on "François-Xavier Cat" [Script](#).

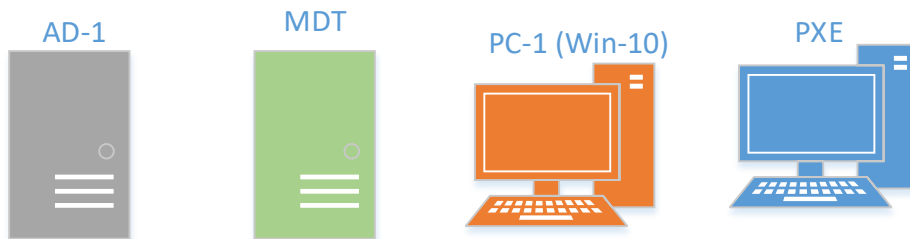
The solution consists of one files function and a special Task Sequence step. So in a nutshell, the sjdomain tool creates both an Offline Domain Join blob and add applied automatically the file.

### Step:

- Create a provision files
- Create application package for automatically deploy
- Add applications in task
- Test result

# 1-Create a provision files

My lab :

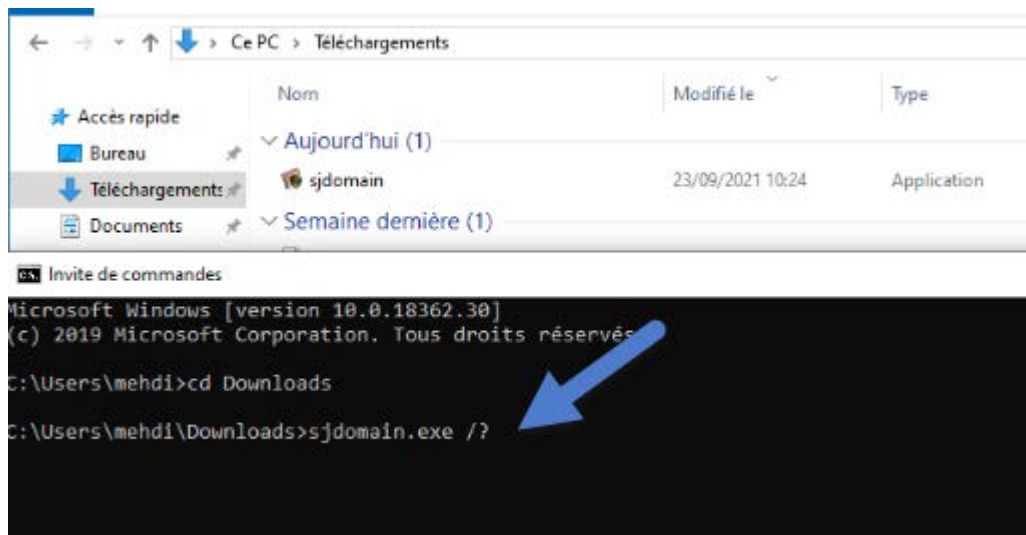


This solutions workon SCCM as MDT, my SCCM is broken I will test it on MDT.

-From any computer on the domain you can also use the server if you want, open “CMD” terminal with account that have the right to create an object on AD, in my case a specific account that only admin can use it, no technical teams. (the CMD don’t need administrator right)

-Download the tool from github on this [link](#)

-Open the cmd and navigate to the folder, you can also drop the exe on cmd



-Now there is many way to add computer, the comond “/?” give more details

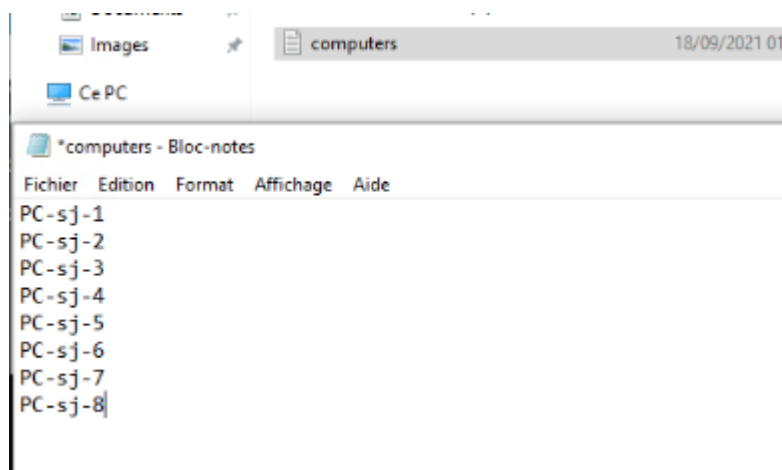
If we have on computer we can enter the command :

Sjdomain.exe “Computer-name”

If we have more, we can use “,” :

```
Sjdomain.exe "computer-1,computer-2computer-3"
```

We can also use a file .txt if we have many computer, we will show this method in our example



-Now we can add computer on AD from this file, with this command

Sjdomain “file-path”, in our example the file is in the same path that exe, if it isent we can add the path like :

```
Sjdomain “:c\path\file.txt”
```

PS : We can also add “-Reuse” if we want that computer will be increased if already exist in the domain, this method is used if not first deploy

We can also add a specific OU if we want with command “-OU”, by default computer is created on “Computer OU”

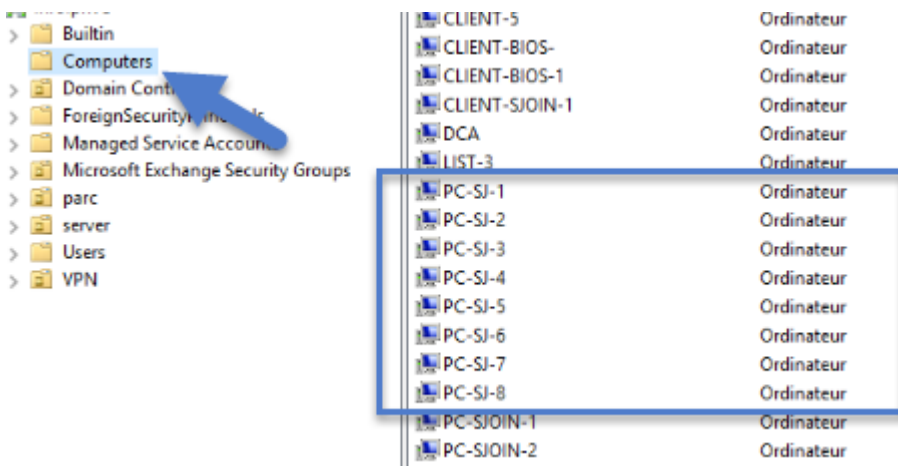
A folder will be created on default location contains the file

```
C:\Users\mehdi\Downloads>sjdomain.exe "./computers.txt"

Répertoire : C:\Users\mehdi\Downloads

Mode                LastWriteTime         Length Name
----                -
d-----          23/09/2021   10:40         PC-sj-1
added
PC-sj-2
added
```

The Computer Accounts will be created on our AD



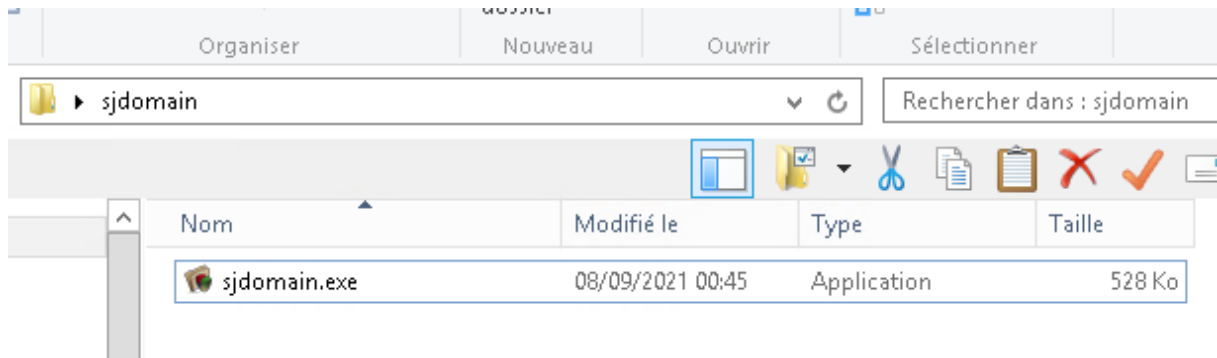
On our machine, files is created on same directory tool

PC > Téléchargements **approv** Rechercher di

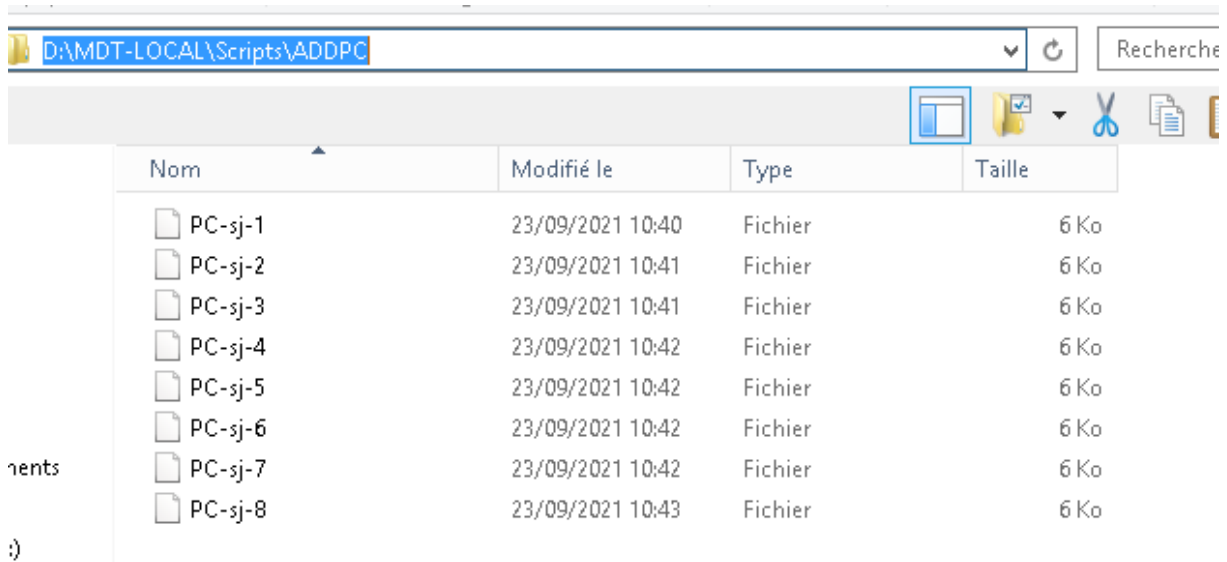
Nom	Modifié le	Type	Taille
PC-sj-1	23/09/2021 10:40	Fichier	6 Ko
PC-sj-2	23/09/2021 10:41	Fichier	6 Ko
PC-sj-3	23/09/2021 10:41	Fichier	6 Ko
PC-sj-4	23/09/2021 10:42	Fichier	6 Ko
PC-sj-5	23/09/2021 10:42	Fichier	6 Ko
PC-sj-6	23/09/2021 10:42	Fichier	6 Ko
PC-sj-7	23/09/2021 10:42	Fichier	6 Ko
PC-sj-8	23/09/2021 10:43	Fichier	6 Ko

## 2 Create application package for automatically deploy

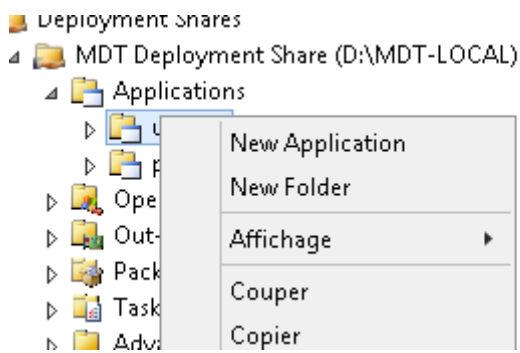
In your MDT server, add the tool “sjdomain.exe” into a folder



We need to create a folder contains the files generated on last step, you can use the network sharing or add it to a MDT folder, in our example a was created a folder “ADDPC” on scripts path on default MDT deployment share directory.



Now we will create a new application from MDT :



Click next

Chose applications with source files



### Application Type

<p>Application Type</p> <p>Details</p> <p>Source</p> <p>Destination</p> <p>Command Details</p> <p>Summary</p> <p>Progress</p> <p>Confirmation</p>	<p>Specify the type of application to add.</p> <ul style="list-style-type: none"><li><input checked="" type="radio"/> Application with source files Copy the source files for this application to the deployment share, which will be used for installing the application.</li><li><input type="radio"/> Application without source files or elsewhere on the network. Either no source files are required for this application, or the application exists at a separate UNC path (e.g. a DFS share).</li><li><input type="radio"/> Application bundle. Create a new application bundle. There is no installation command associated with this application. Instead, only the dependencies of this application will be installed. These dependencies can be configured after the item has been added.</li></ul>
---	---

## Enter information

Application Type	Specify the details for this application.
Details	Publisher: (Optional) <input type="text"/>
Source	Application Name: <input type="text" value="sjdomain"/>
Destination	Version: (Optional) <input type="text"/>
Command Details	Language: (Optional) <input type="text" value="en"/>
Summary	
Progress	
Confirmation	

Choose your folder contains the applications “sjdomain.exe” in our case

Application Type	In order to add this application, all the files need to be copied to the deployment share. Specify the location of these files.
Details	Source directory: <input type="text" value="C:\Users\mehdi\Desktop\sjdomain"/> <input type="button" value="Browse..."/>
Source	<input type="checkbox"/> Move the files to the deployment share instead of copying them.
Destination	
Command Details	
Summary	
Progress	
Confirmation	

Enter these command line :

```
sjdomain.exe addcomp "%scriptroot%\ADDPC"
```

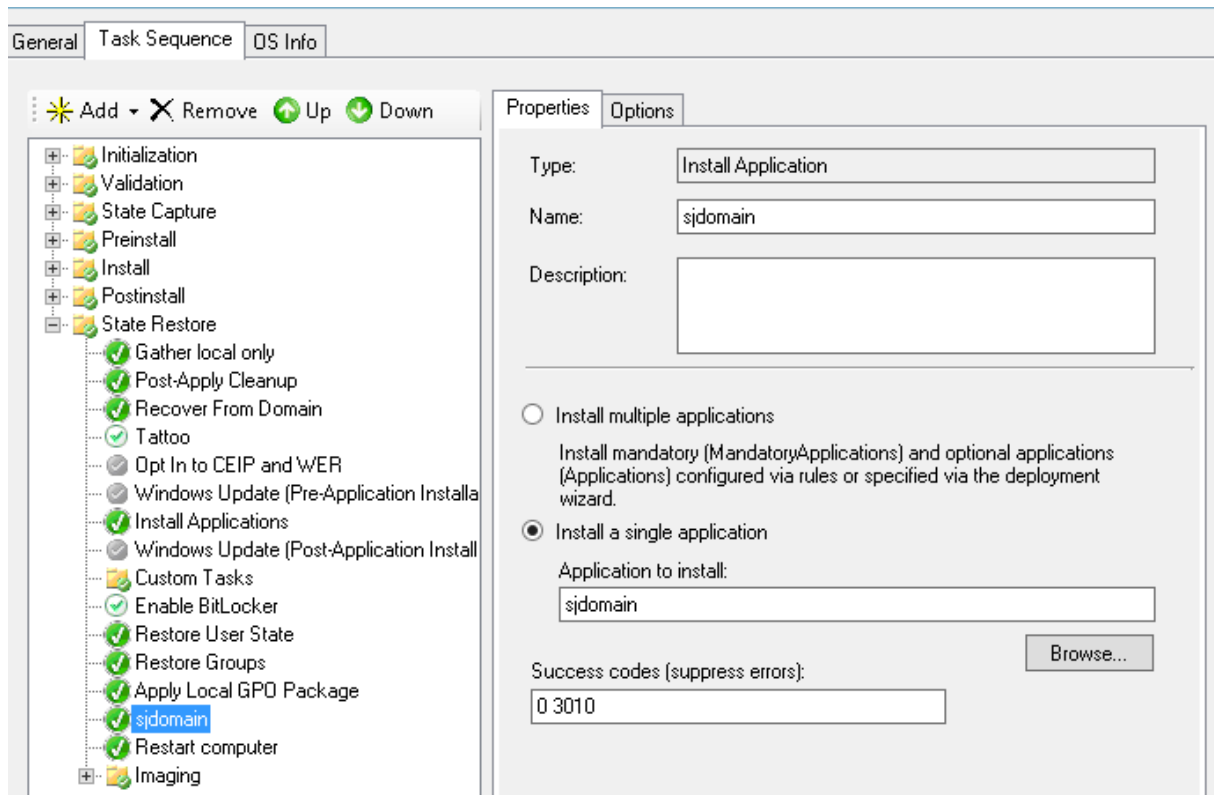
PS : for our example, I copied the files to the folder “ADDPC” into scripts on local mdt path, if you use another sharing folder you must change the path like these :

```
Sjdomain.exe addcomp “your-UNC-folders”
```



### 3-Add application in the Task

Add the applications and a restart action to your deploy task sequence in last step like the pictures:

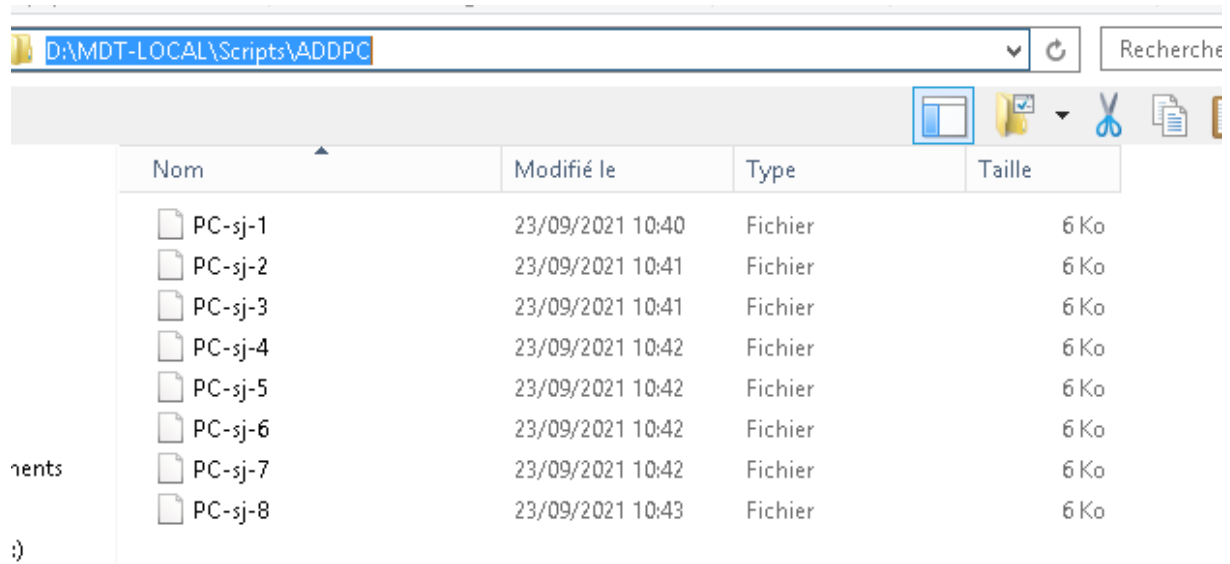


No click ok.

## 4-Test result

Now launch your computer, select task, and don't forget to rename computer with same name that exist in the folder and already generated

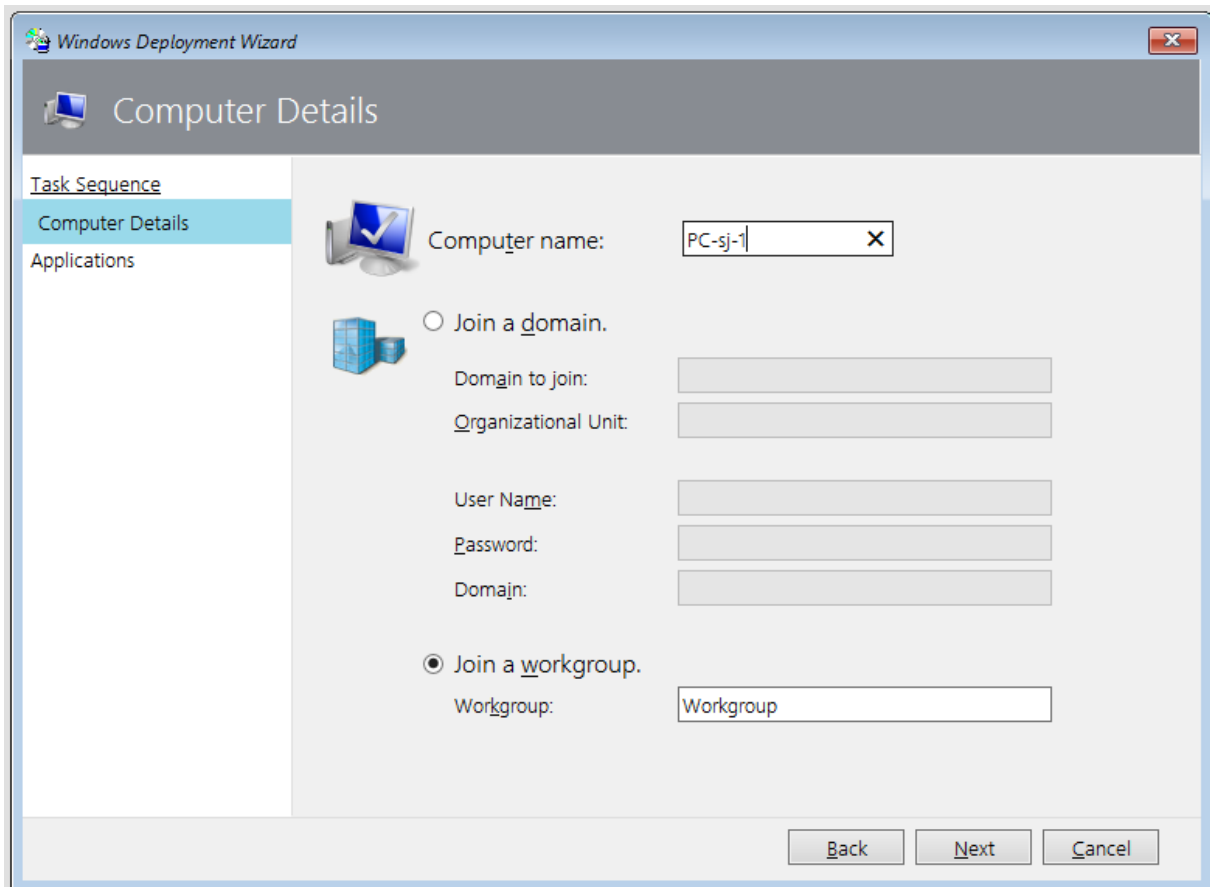
This is an example :



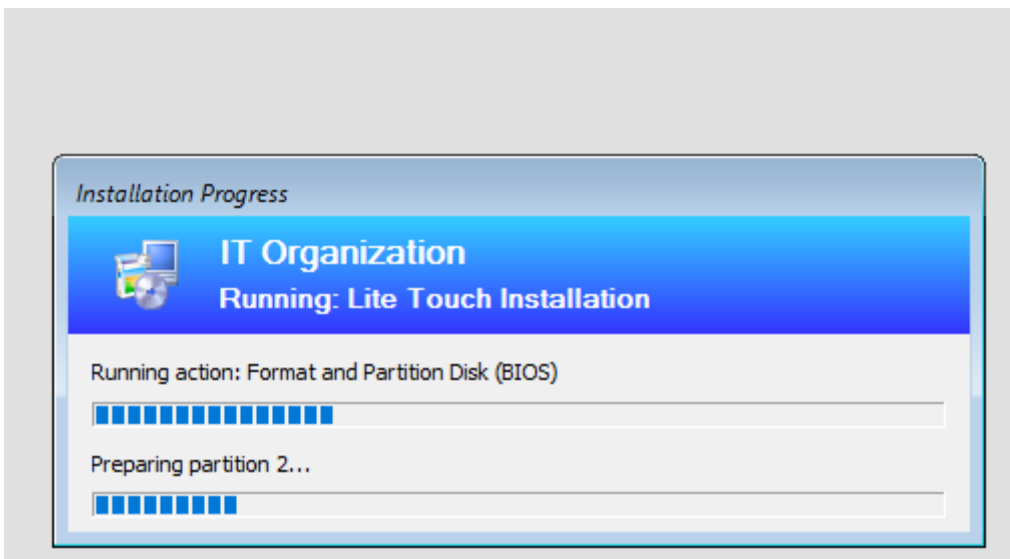
Nom	Modifié le	Type	Taille
PC-sj-1	23/09/2021 10:40	Fichier	6 Ko
PC-sj-2	23/09/2021 10:41	Fichier	6 Ko
PC-sj-3	23/09/2021 10:41	Fichier	6 Ko
PC-sj-4	23/09/2021 10:42	Fichier	6 Ko
PC-sj-5	23/09/2021 10:42	Fichier	6 Ko
PC-sj-6	23/09/2021 10:42	Fichier	6 Ko
PC-sj-7	23/09/2021 10:42	Fichier	6 Ko
PC-sj-8	23/09/2021 10:43	Fichier	6 Ko

I will chose as name of computer one of this list, I'm choosing "PC-sj-1"

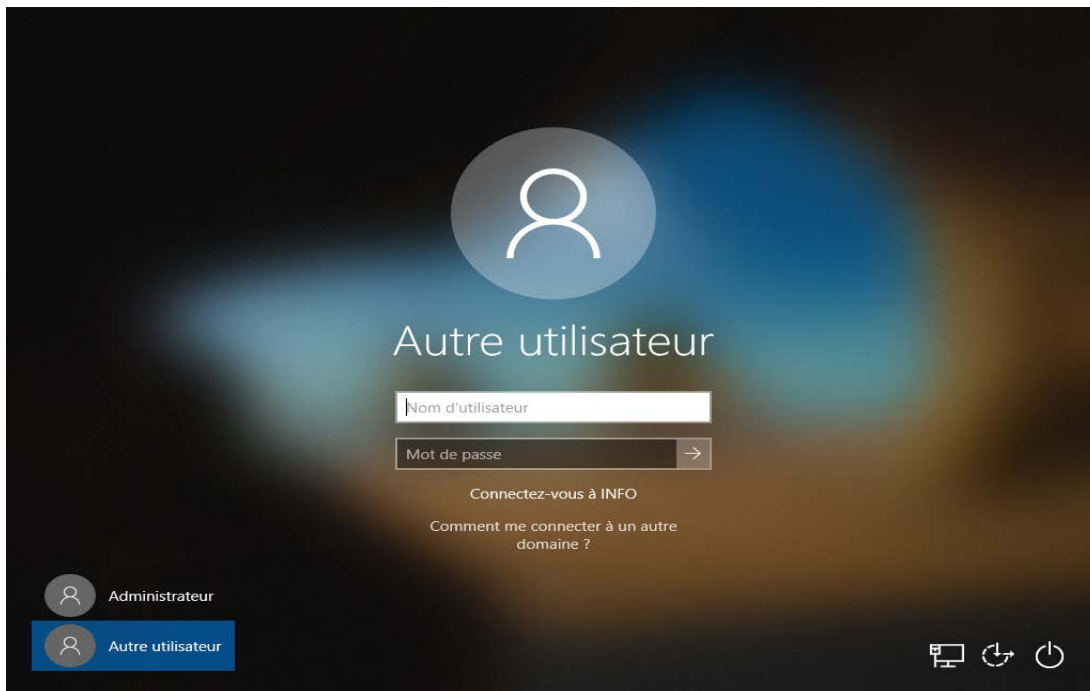
PS: don't forget to respect the case sensitive



You can launch the deployment



When finished the computer will be renamed automatically, and joined in the domain, without any password or permission, in the future if you want to add more computer you need also copying the files generated like step 1 on your sharing file, in our example "Scripts\ADDPC"



After the finish deployment the computer is in the domain, we can use this with external media from iso without connection in the domain

#### Édition Windows

Windows 10 Professionnel  
Éducation  
© 2019 Microsoft Corporation.  
Tous droits réservés.



#### Système

Processeur :	Intel(R) Core(TM) i7-2600 CPU @ 3.40GHz 3.39 GHz
Mémoire installée (RAM) :	1,41 Go
Type du système :	Système d'exploitation 64 bits, processeur x64
Stylet et fonction tactile :	La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponible sur cet écran.

#### Paramètres de nom d'ordinateur, de domaine et de groupe de travail

Nom de l'ordinateur :	PC-sj-1
Nom complet :	PC-sj-1.info.prive
Description de l'ordinateur :	
Domaine :	info.prive

 [Modifier les paramètres](#)