Configuration de l'authentification par clé privée avec ISE

Table des matières

Introduction

Ce document décrit comment créer une clé SSH (Private Secure Shell) pour l'authentification à l'interface de ligne de commande sur Identity Secure Engine (ISE).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Référentiel dans ISE.
- Authentification par certificat.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Correctif 3 ISE 3.3
- Windows 10
- MacOS X

- Putty client SSH

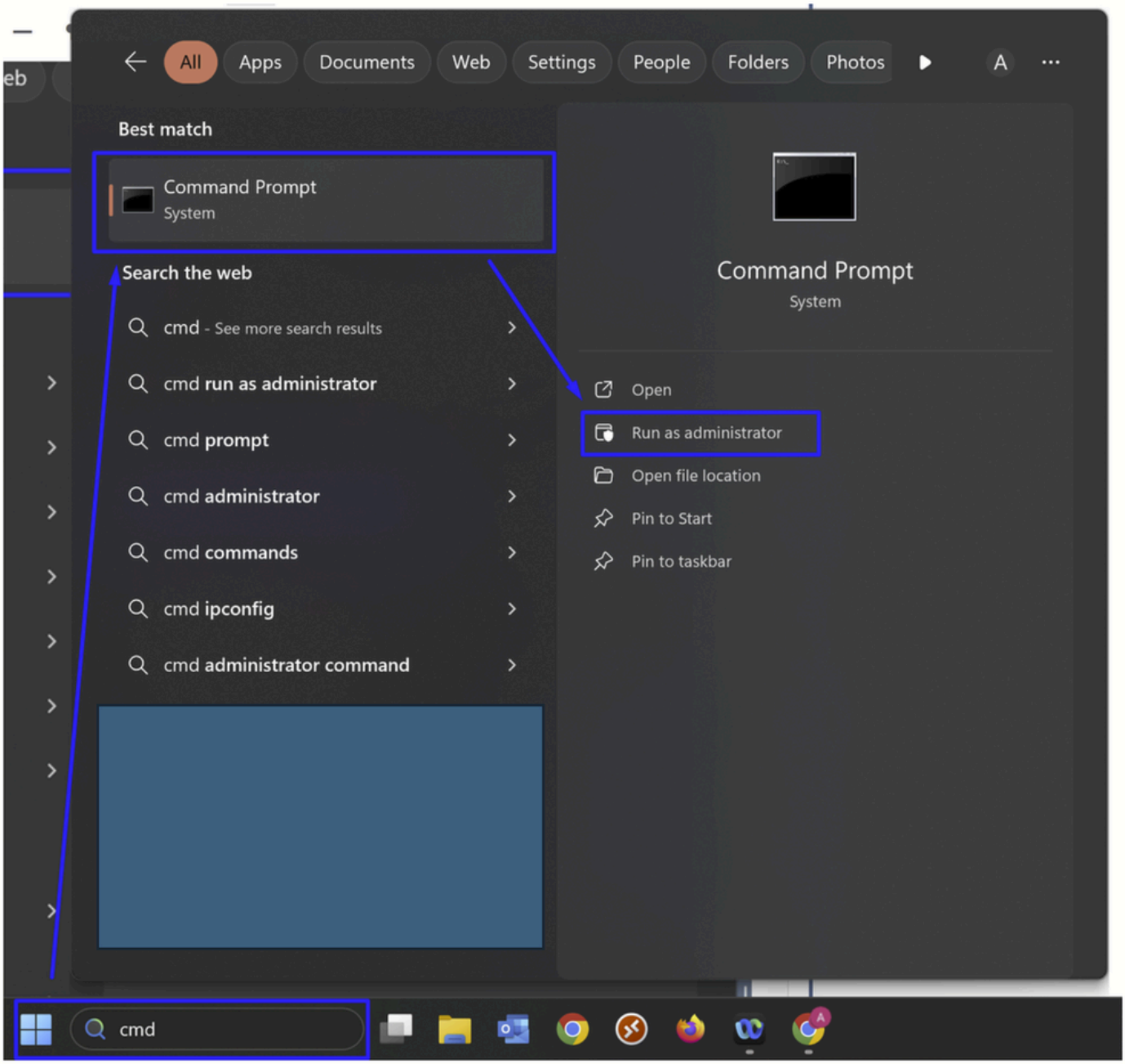
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configurer

Créer les clés privée et publique dans Windows

Cliquez sur l'icône Rechercher située dans la barre des tâches :

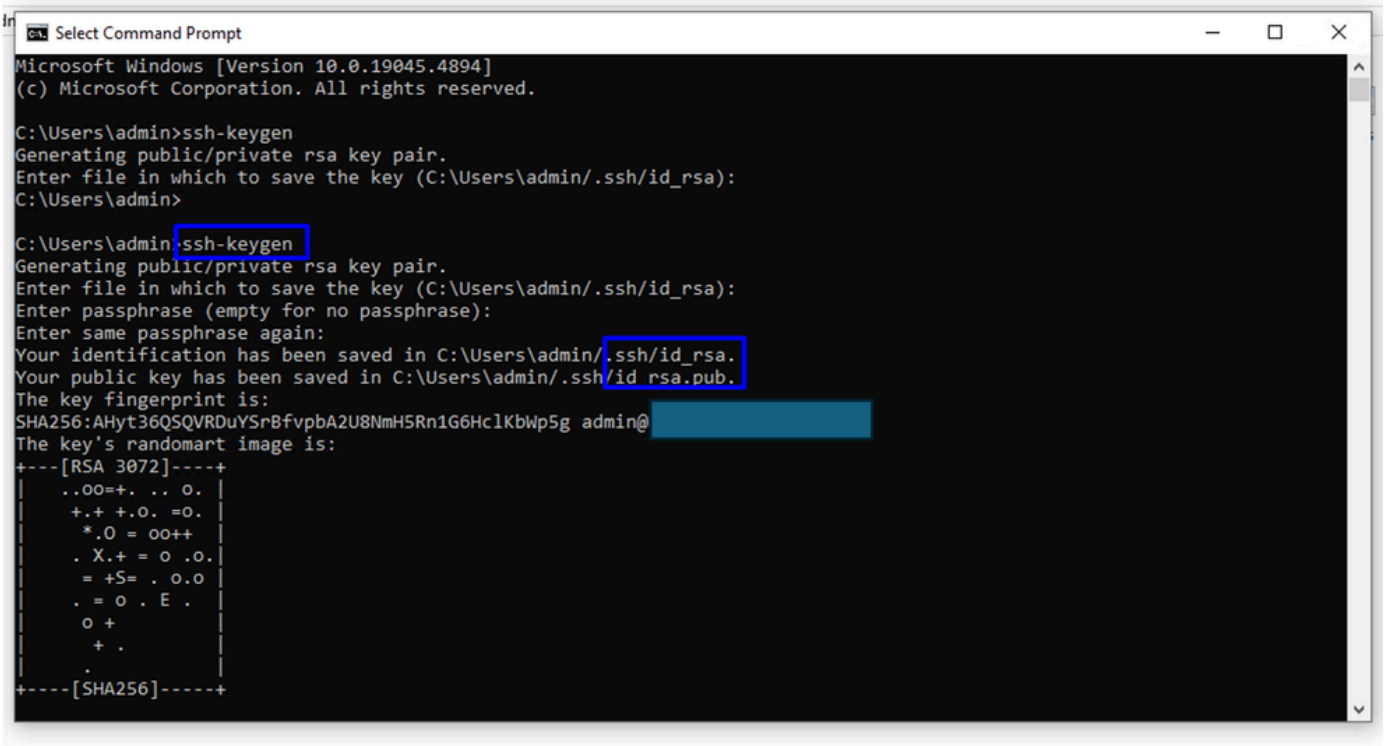
· Tapez cmd dans la barre de recherche
· Dans les résultats de la recherche, cliquez avec le bouton droit sur Invite de commandes et sélectionnez Exécuter en tant qu'administrateur. Vous disposez ainsi des autorisations nécessaires pour exécuter des commandes



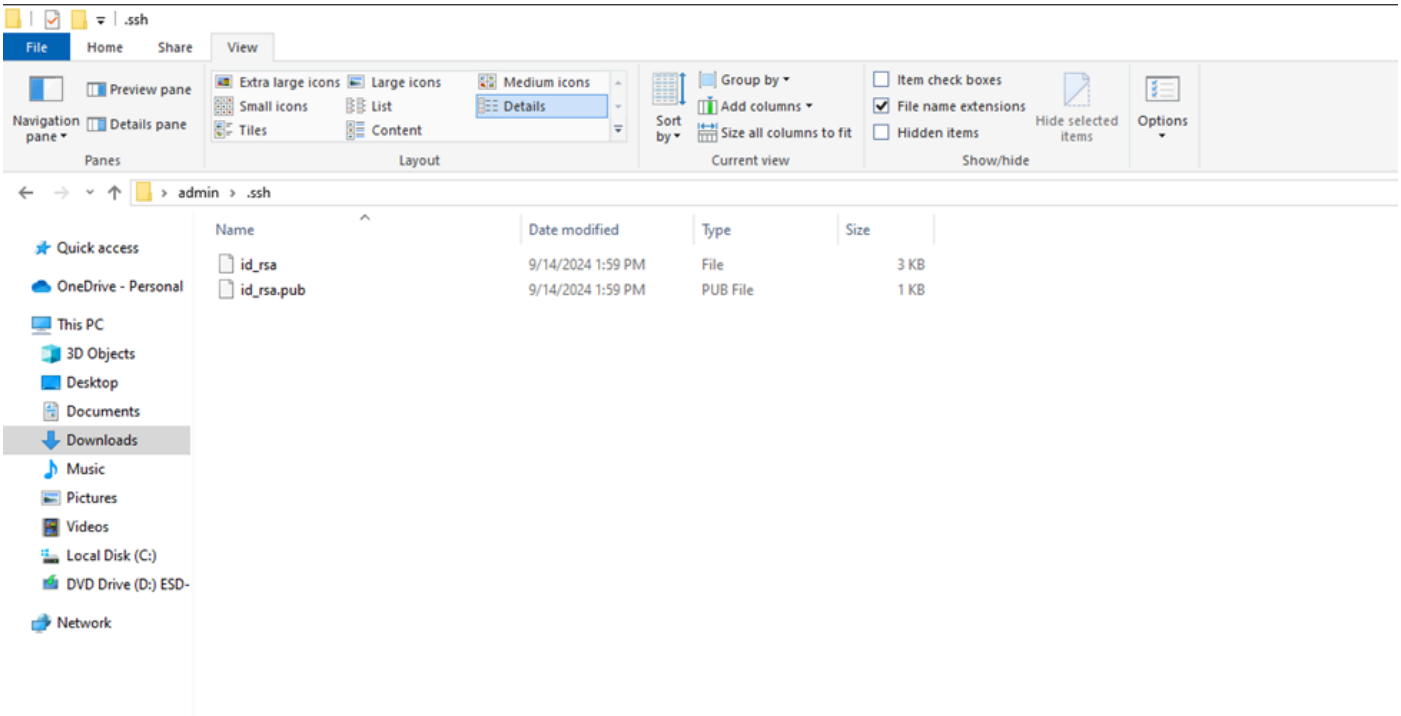
· Exécutez la commande suivante :

```
ssh-keygen
```

- Vous êtes alors invité à saisir deux fois la clé de cryptage. Veuillez l'enregistrer, car il s'agit d'une authentification par rapport à ISE en tant que nouveau mot de passe. Ensuite, il en résulte la création de deux fichiers, les clés privée (id_rsa) et publique (id_rsa.pub), puis. Enregistrez les fichiers dans un répertoire. Par exemple, la valeur par défaut a été utilisée



- Vérifier l'emplacement de stockage des fichiers



Transférez la clé publique **(id_rsa.pub)** dans le dossier du référentiel de fichiers configuré sur ISE.

Créez les clés privée et publique via dans MacOS

Cliquez sur l'**Finder**icône située dans le Dock
· Accédez à la page **Applications folder**

· Dans le **Applications folder**, localisez et ouvrez le dossier Utilities
· Dans la liste Utilitaires, recherchez **Terminal**
· Double-cliquez sur **Terminal** pour l'ouvrir
· Dans la **Terminal** fenêtre, tapez « ssh-keygen -t rsa« et appuyez sur la touche Entrée pour l'exécuter
· Écrivez la clé de chiffrement deux fois et **save it**
· Accéder à l'emplacement des fichiers
Transférez la clé publique **(id_rsa.pub)** dans le dossier du référentiel de fichiers configuré sur ISE.

```
Your identification has been saved in /Users/myname/.ssh/id_rsa.
Your public key has been saved in /Users/myname/.ssh/id_rsa.pub.
The key fingerprint is:
ae:89:72:0b:85:da:5a:f4:7c:1f:c2:43:fd:c6:44:38 myname@mymac.local
The key's randomart image is:
+--[ RSA 2048]----+
|                 |
|          .      |
|         E .     |
|    .    . o     |
|  o . . S .      |
| + + o . +       |
|. + o = o +      |
| o...o * o       |
|.  oo.o .        |
+-----------------+
```

Configurer le certificat pour la connexion à ISE

Corroborez si le fichier public se trouve sous le référentiel à l'aide de la commande suivante :

```
show repository
```

```
ise-primary-33/admin#
ise-primary-33/admin#show repository Sever_all
Backup-Cisco-CFG10-240222-0915.tar.gpg
cisco-secure-client-win-5.0.05040-core-vpn-webdeploy-k9.msi
cisco-secure-client-win-5.0.05040-webdeploy-k9.pkg
Ethernet1.xml
FullReport_29-Mar-2024.csv
grise04conf-CFG10-240213-2200.tar.gpg
id_rsa.pub
```

- Importez le fichier de clé publique à l'**(id_rsa.pub)**aide de la commande en mode privilégié :

```
crypto key import

        repository
```

```
ise-primary-33/admin#crypto key import public.pub repository Sever all
```

- Passez en mode de configuration globale et utilisez la commande suivante :

```
service sshd PubkeyAuthentication
```

```
ise-primary-33/admin(config)#service sshd PubkeyAuthentication
  Enabling key pair authentication automatically disables password-based
authentication.
%
% To enable key pair authentication in this Cisco ISE node,
% add at least one public key to the node. You must add
% a public key even if you want to configure private key usage in a later
step.
% If you don't already have a public key file in your system,
% add one to a repository now. Then, import the key file with the following
command:
% crypto key import <public key filename> repository <repository name>
```

Veuillez utiliser la commande afin de vérifier que vous n'obtenez aucune erreur pendant l'importation de la clé publique. Il est conseillé de poursuivre cette opération via le port de console pour éviter de perdre l'accès à l'ISE.

Vérifier

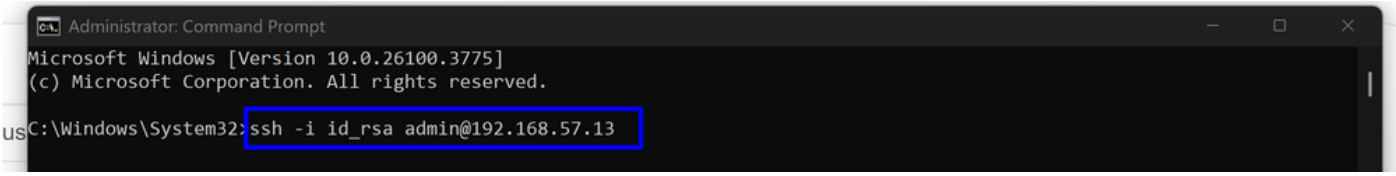
Connexion à Windows

Essayez d'accéder à l'ISE via **cmd** en utilisant la commande suivante :

```
ssh -i

        @


EXAMPLE:
ssh -i id_rsa admin@192.168.57.13
```



Utilisez la clé de chiffrement configurée à l'étape Créer les clés privée et publique sous Windows afin de vous authentifier.

Connexion à MacOS

Entrez la commande suivante dans le terminal :

```
ssh -i

        @


EXAMPLE:
ssh -i id_rsa admin@192.168.57.13
```

ou

```
ssh -i ~/.ssh/
```

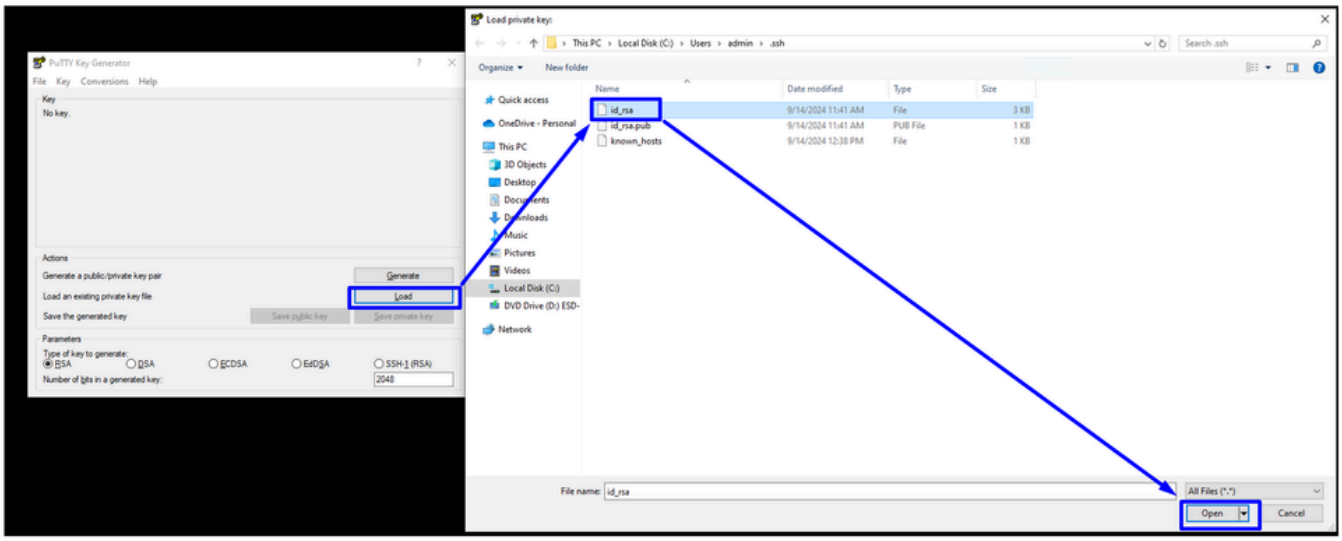
```
        @
```

```
EXAMPLE:
ssh -i ~/.ssh/id_rsa admin@192.168.57.13
```

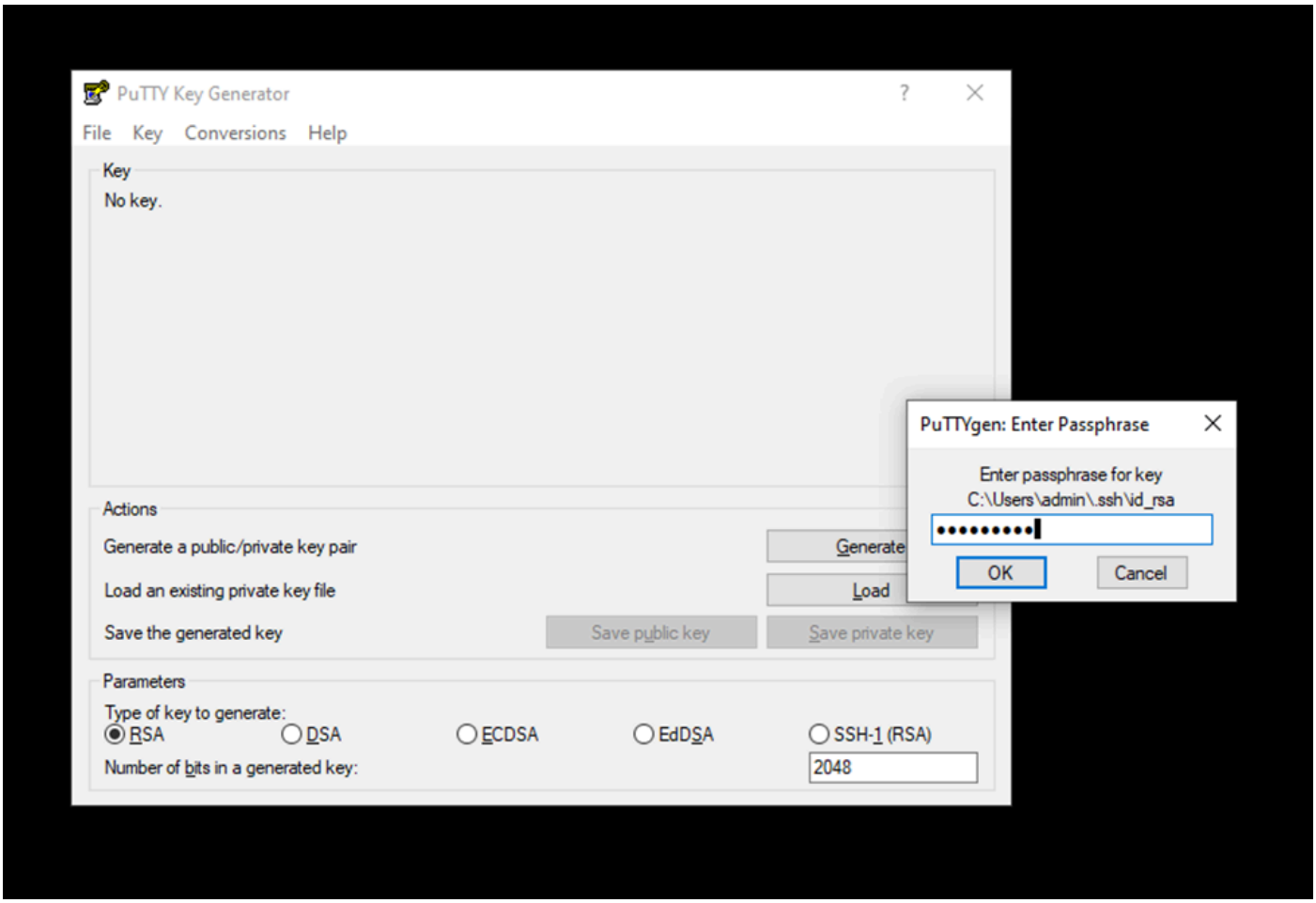
Utilisez la clé de chiffrement configurée à l'étape Créer les clés privée et publique via dans MacOS afin de vous authentifier.

Se connecter à Putty

Ouvrez PuTTy key generator (recherchez par PuttyGen dans la barre de recherche de démarrage), cliquez sur Charger, sélectionnez tous les fichiers, et ouvrez la clé privée générée à partir de cmd (Windows) ou terminal (MacOS) :

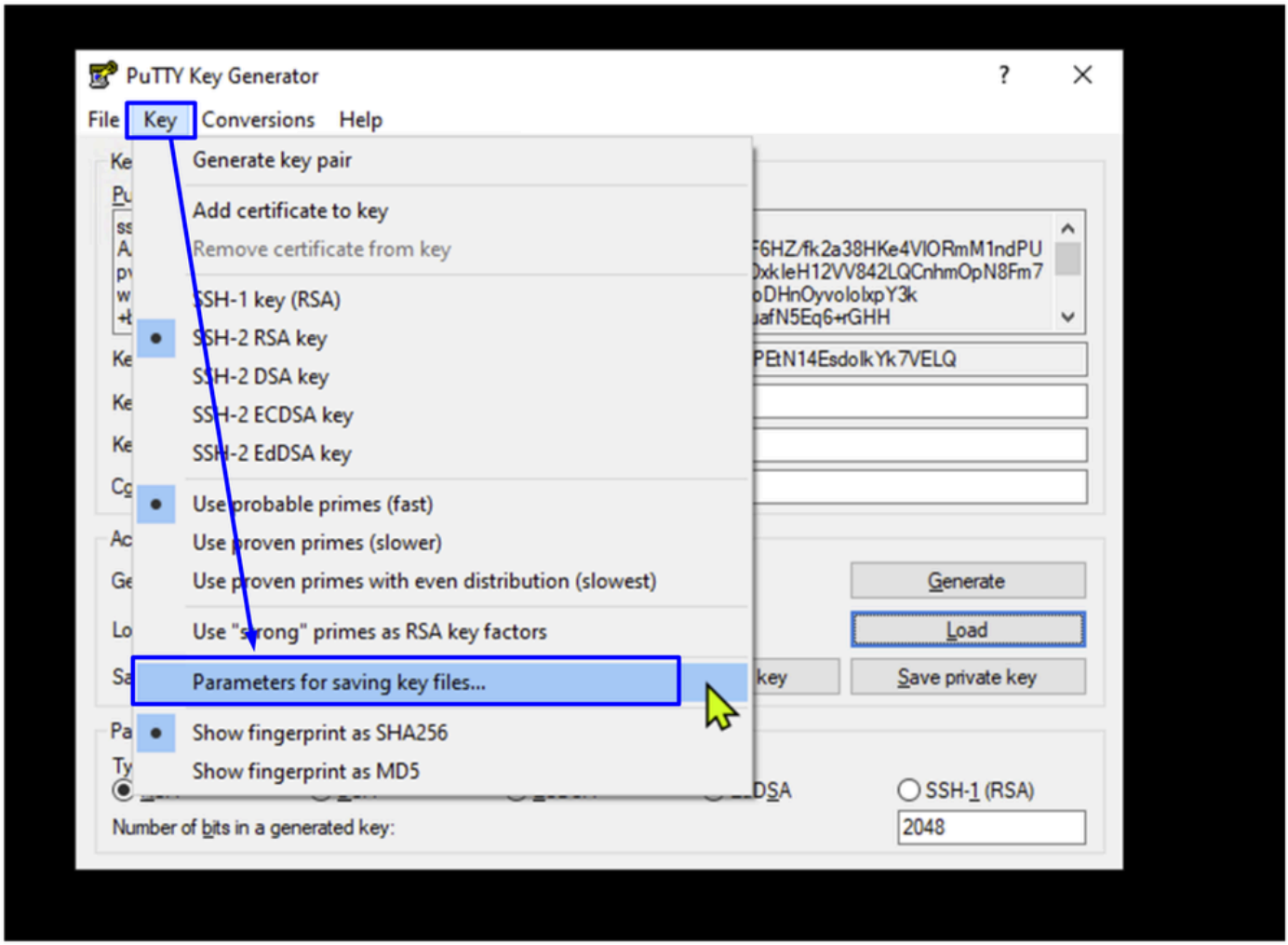


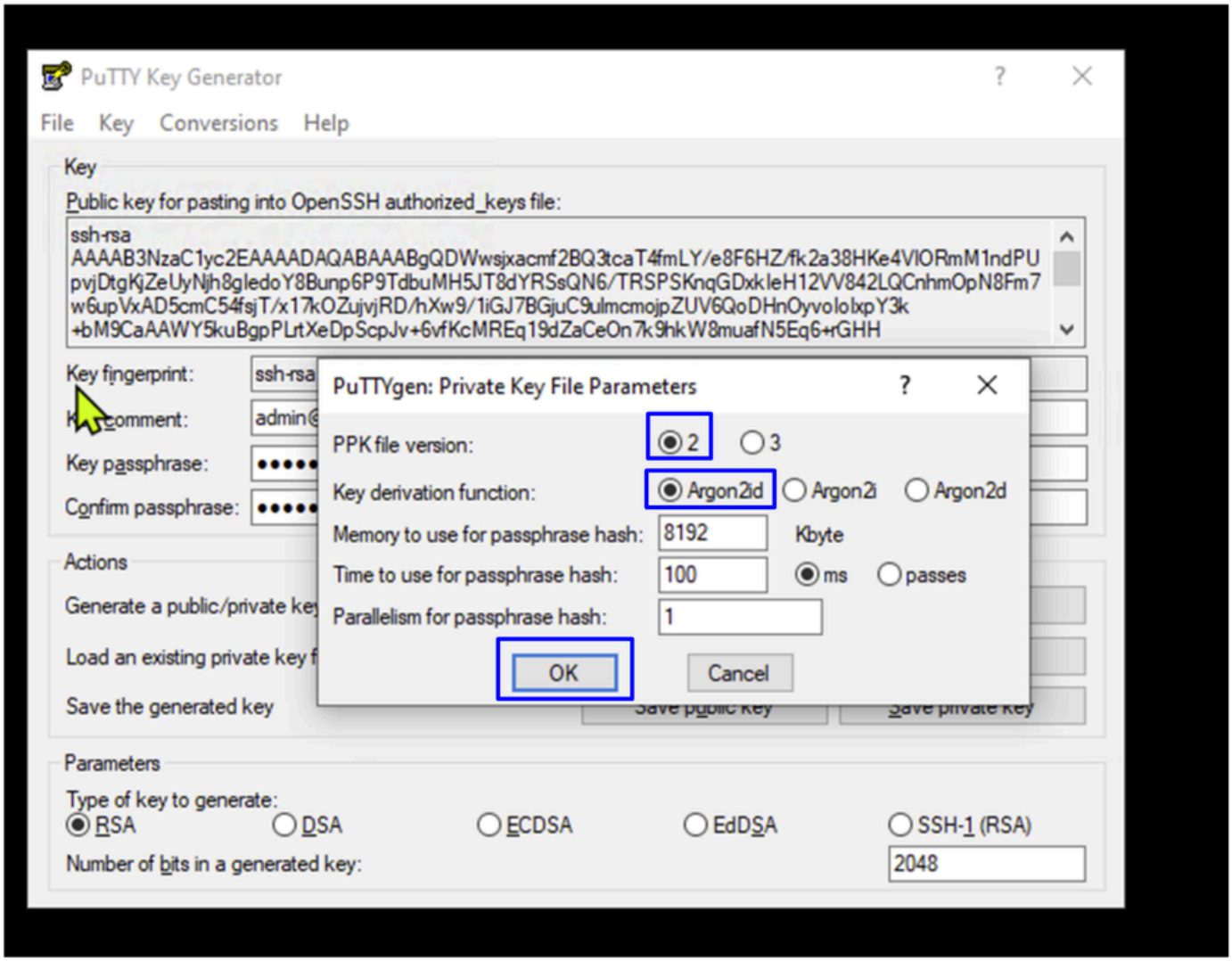
- Écrivez la clé de chiffrement précédemment utilisée dans la cmd ou le terminal



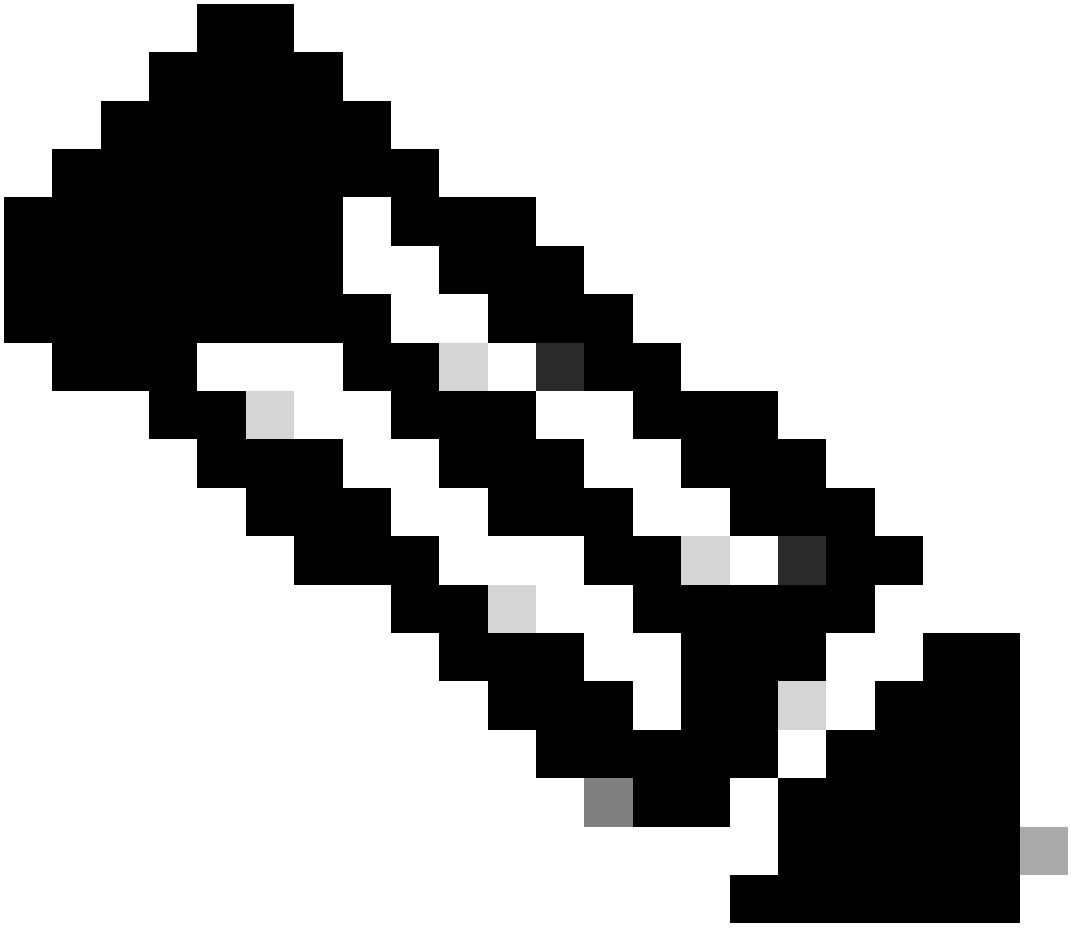
Convertissez ce fichier en une version compatible Putty en exécutant les étapes suivantes :

- Cliquez sur Key > Parameters pour enregistrer les fichiers de clés


PuTTY Key Generator
File
Key
Conversions
Help
Generate key pair
Add certificate to key
Remove certificate from key
SSH-1 key (RSA)
SSH-2 RSA key
SSH-2 DSA key
SSH-2 ECDSA key
SSH-2 EdDSA key
Use probable primes (fast)
Use proven primes (slower)
Use proven primes with even distribution (slowest)
Use "strong" primes as RSA key factors
Parameters for saving key files...
Show fingerprint as SHA256
Show fingerprint as MD5
Generate
Load
Save private key
SSH-1 (RSA)
Number of bits in a generated key:
2048

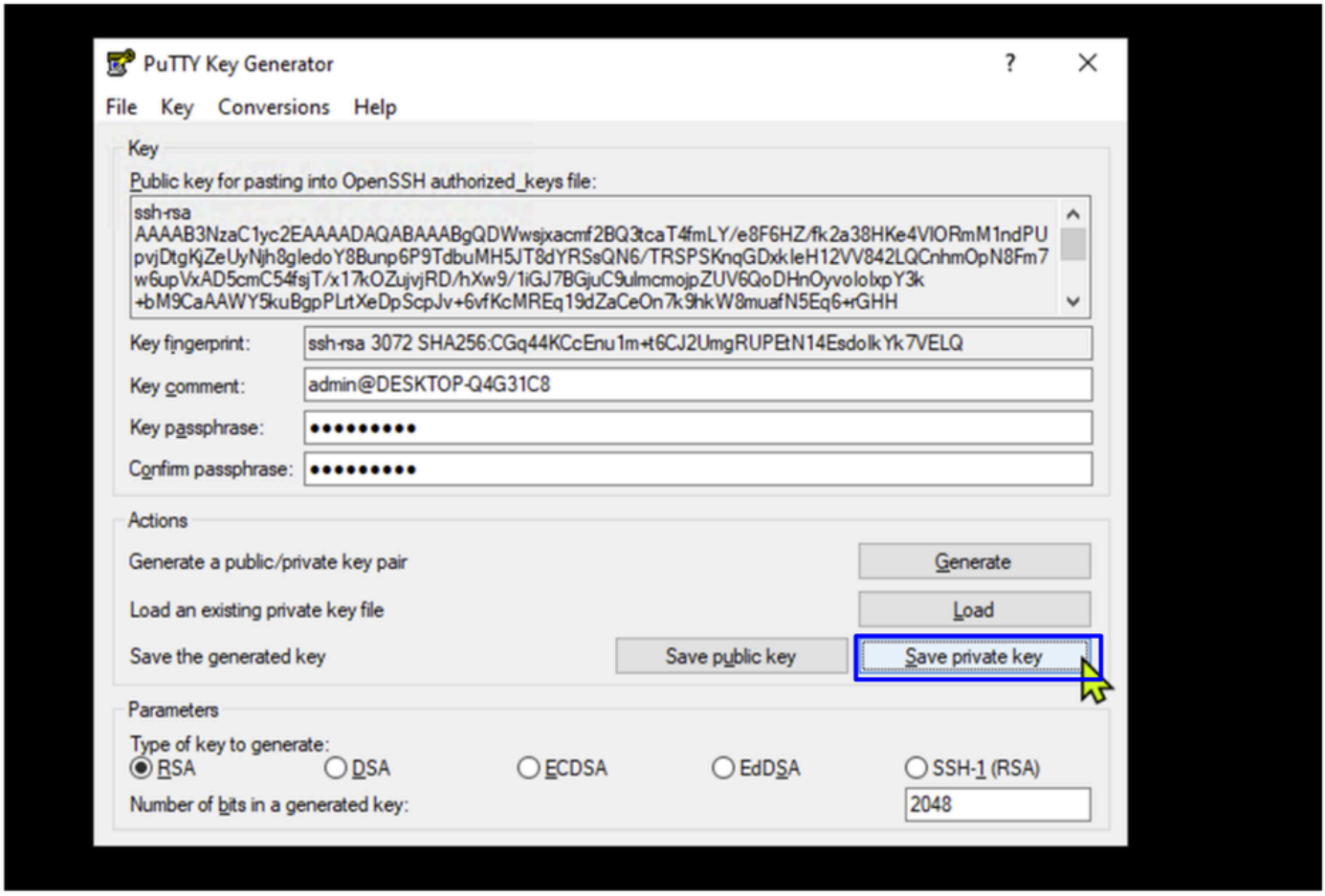


- PPK file version : Choisissez 2
- **Key derivation function**: Choisir Argon2id



Remarque : Pour le reste des paramètres, utilisez les valeurs par défaut.

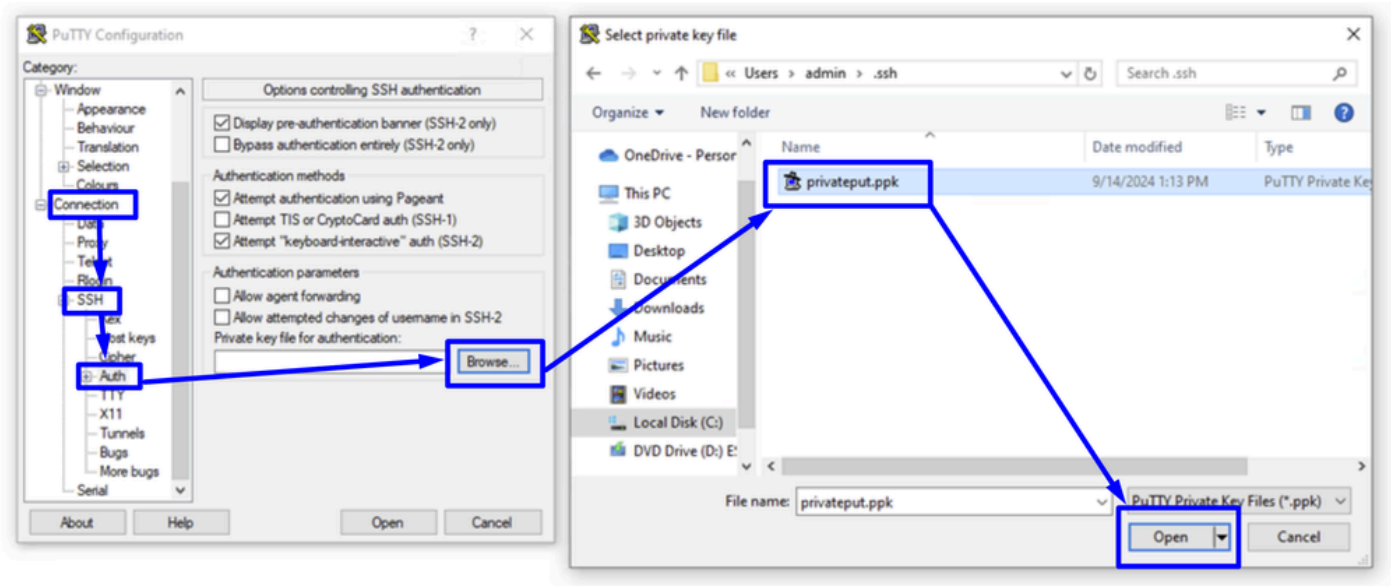
- Cliquer Ok



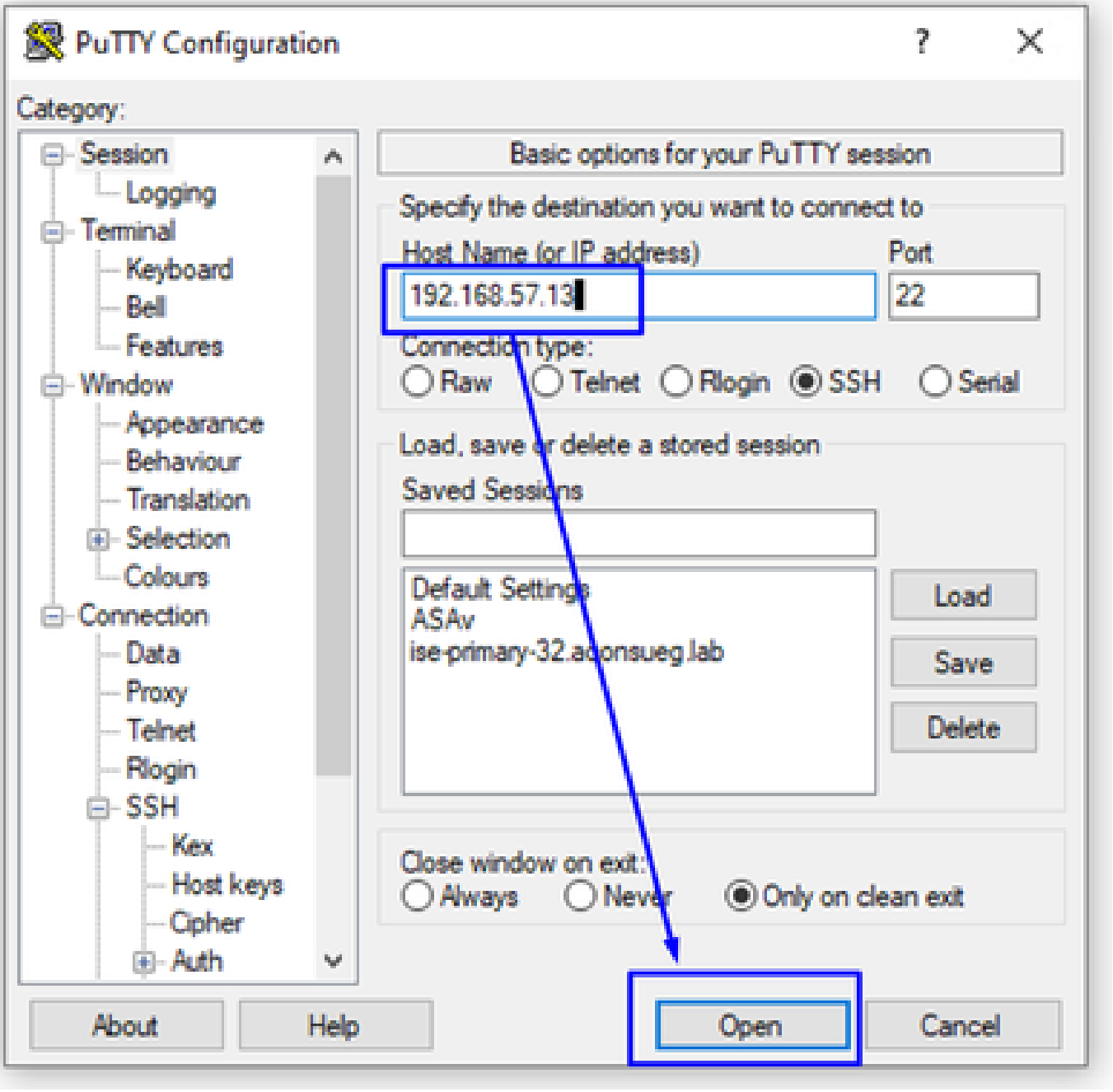
- Cliquez sur Save private Key

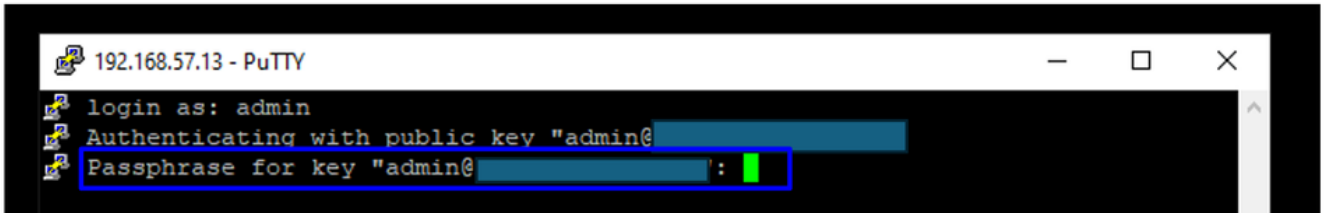
Après avoir enregistré la clé sur votre ordinateur, vous êtes prêt à l'utiliser en vous reportant aux exemples suivants :

- Putty Ouvert
- Cliquez sur **Connection > SSH > Auth > Browse**
- Sélectionnez votre clé privée et cliquez sur Open



- Revenez à Session, définissez l'adresse IP ou le nom d'hôte (FQDN) de l'ISE
- Cliquez sur Ouvrir





Utilisez la clé de cryptage configurée à l'étape Create the private and public keys via dans MacOS ou Create the private and public keys in Windows afin de vous authentifier.

Dépannage

Extraire les messages d'erreur du site de point d'extrémité en ajoutant l'indicateur -v à la connexion ssh

```
Example for Windows:
ssh -v -i id_rsa admin@192.168.57.13
```

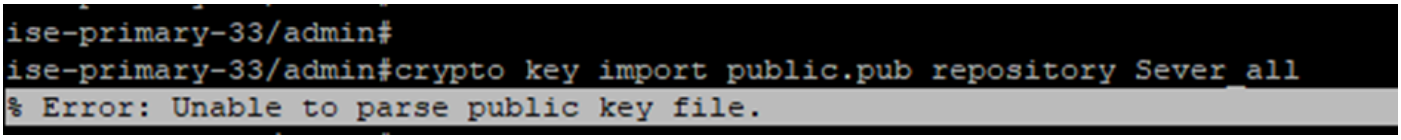
```
Example for MacOS:
ssh -v -i id_rsa admin@192.168.57.13
```

ou

```
ssh -v -i ~/.ssh/id_rsa admin@192.168.57.13
```

Erreur d'importation de la clé publique

%ERROR: Impossible d'analyser le fichier de clé publique.



Si vous rencontrez des difficultés lors de l'importation de plusieurs clés publiques, veuillez contacter le support technique de Cisco.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.