

Privésleutelverificatie configureren met ISE

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Maak de private en publieke sleutels in Windows](#)

[Maak de private en publieke sleutels via in MacOS](#)

[Configureer het certificaat om in ISE in te loggen](#)

[Verifiëren](#)

[Aanmelden bij Windows](#)

[Aanmelden bij MacOS](#)

[Inloggen in Putty](#)

[Problemen oplossen](#)

[Fout bij importeren openbare sleutel](#)

Inleiding

In dit document wordt beschreven hoe u een private secure shell (SSH)-sleutel kunt maken voor verificatie van de CLI op de Identity Secure Engine (ISE).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Opslagplaats in ISE.
- Certificaatverificatie.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ISE 3.3 patch 3
- Windows 10
- MacOS X
- SSH client Putty

De informatie in dit document is gebaseerd op de apparaten in een specifieke

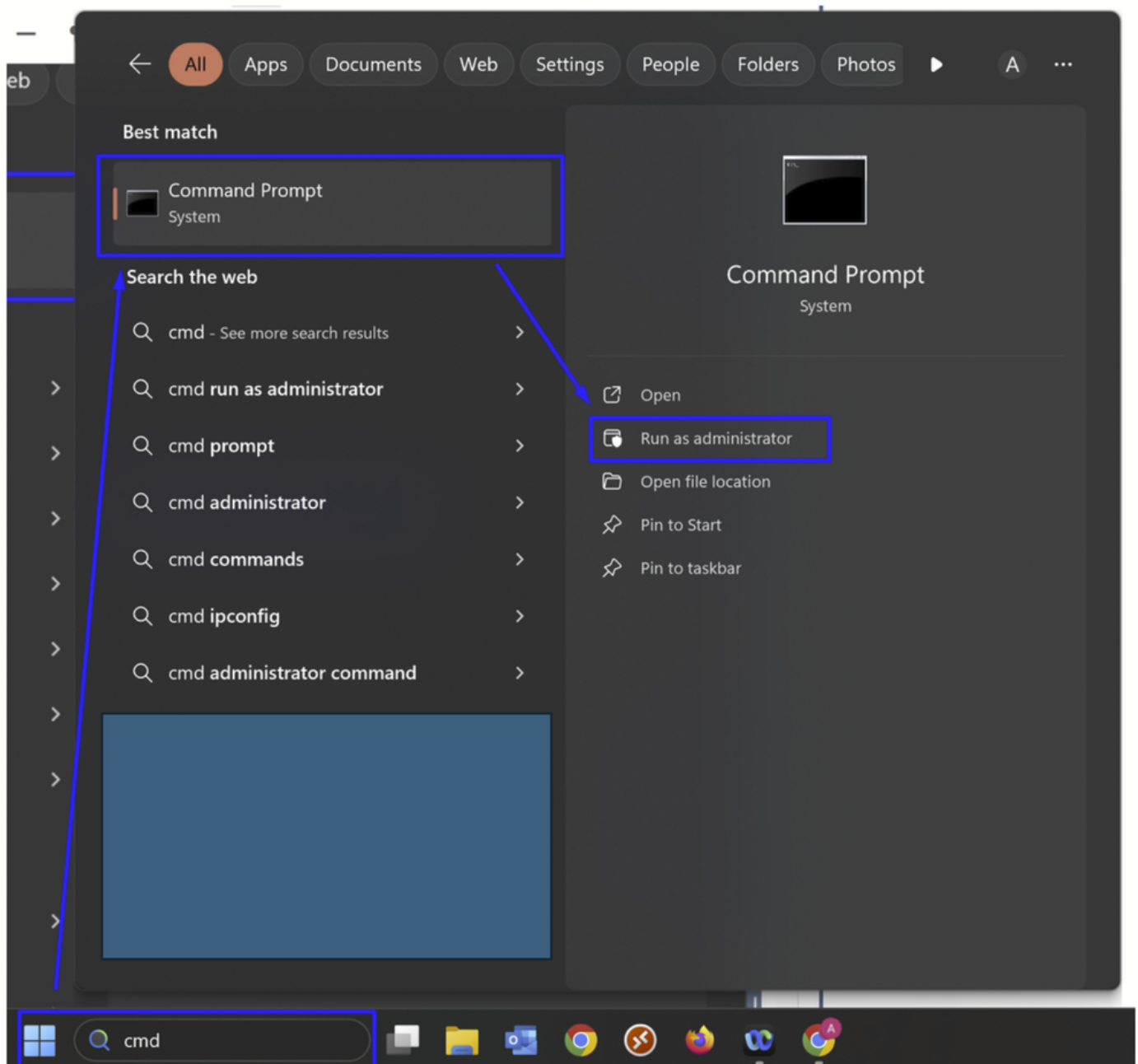
laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Maak de private en publieke sleutels in Windows

Klik op het pictogram Zoeken op de taakbalk:

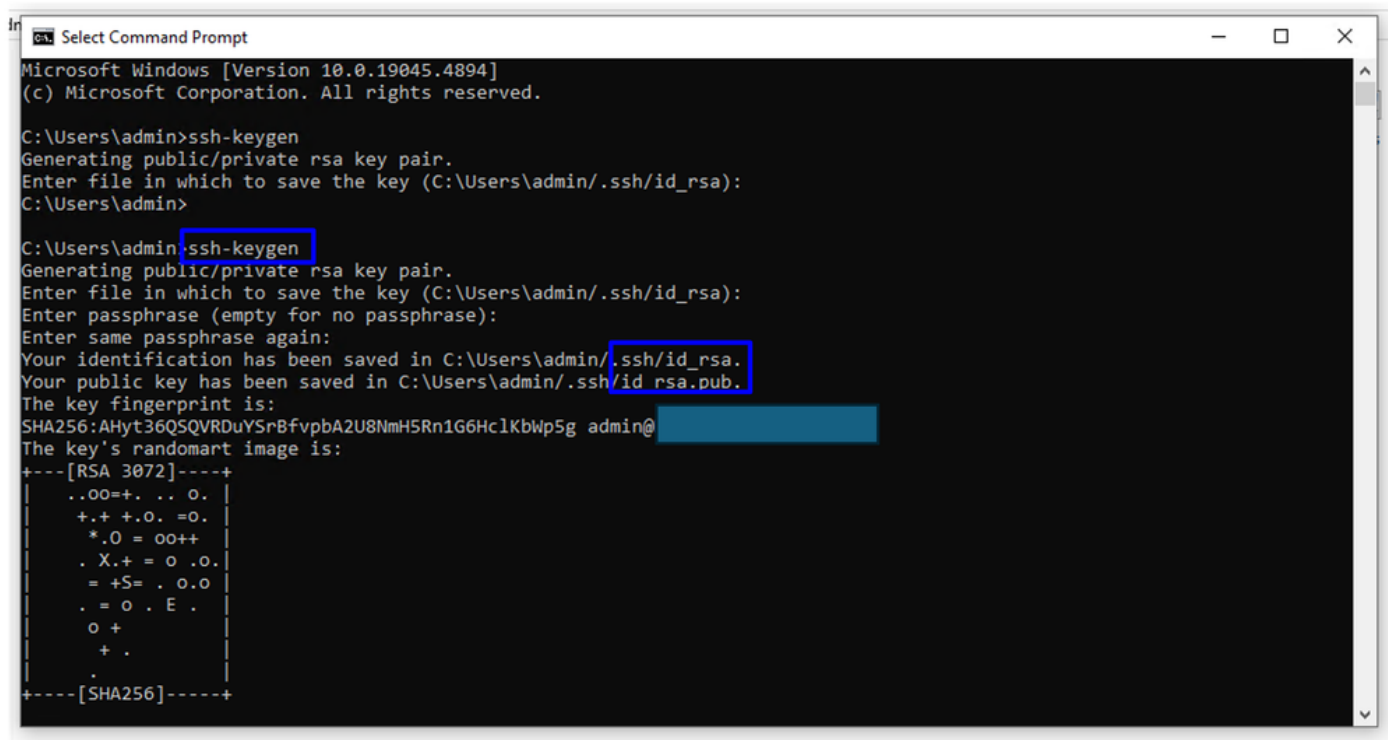
- Typ cmd in de zoekbalk
- Klik in de zoekresultaten met de rechtermuisknop op Opdrachtprompt en selecteer Uitvoeren als beheerder. Dit zorgt ervoor dat u over de nodige machtigingen beschikt om opdrachten uit te voeren



- Voer de volgende opdracht uit:

ssh-keygen

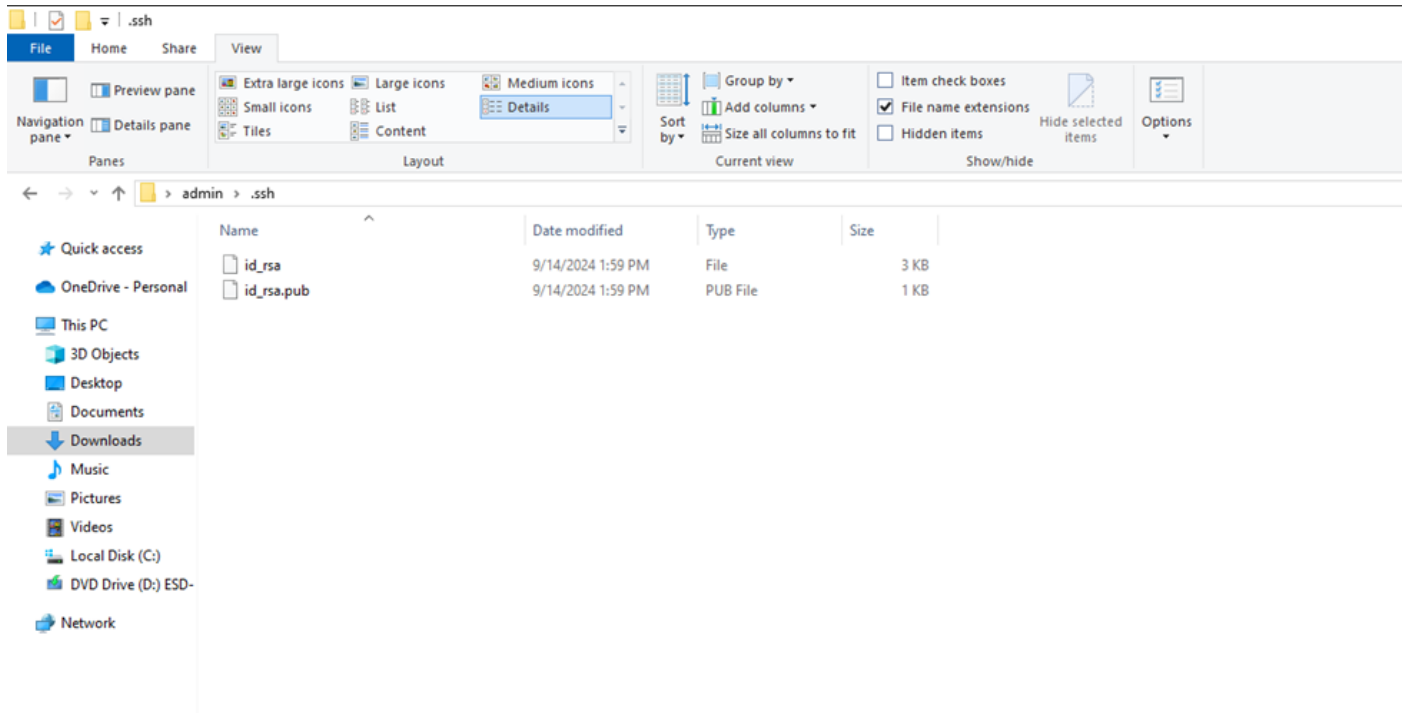
- Dit vraagt u om de encryptiesleutel twee keer in te voeren. Sla het op, want dit is voor authenticatie tegen de ISE als het nieuwe wachtwoord. Daarna resulteert dit in het maken van twee bestanden, de private (id_rsa) en de public (id_rsa.pub) sleutels, dan. Sla de bestanden op in één directory. De standaardversie is bijvoorbeeld gebruikt



```
Microsoft Windows [Version 10.0.19045.4894]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\admin\.ssh/id_rsa):
C:\Users\admin>
C:\Users\admin>ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\admin\.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\admin\.ssh/id_rsa.
Your public key has been saved in C:\Users\admin\.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:AHyt36Q5QVRDuYSr8fvpbA2U8NmH5Rn1G6HclKbWp5g admin@
The key's randomart image is:
+---[RSA 3072]-----+
| ..00=+. . . 0. |
| +. +.0. =0. |
| *.0 = 00++ |
| . X.+ = 0 .0. |
| = +S= . 0.0 |
| . = 0 . E . |
| 0 + |
| + . |
| . |
+----[SHA256]-----+
```

- Controleer waar de bestanden zijn opgeslagen



Breng de publieke sleutel over (`id_rsa.pub`) in de map met de bestandsopslagplaats die is geconfigureerd op ISE.

Maak de private en publieke sleutels via in MacOS

Klik op het Finder pictogram in het Dock

- Navigeer naar de Applications folder
- In de map Applications folder Hulpprogramma's zoeken en openen
- In de lijst met hulpprogramma's vindt u Terminal
- Dubbelklik op om Terminal het te openen
- Typ in het Terminal venster "ssh-keygen -t rsa" en druk op de enter-toets om het uit te voeren
- Schrijf de encryptiesleutel twee keer en save it
- Ga naar de locatie van de bestanden

Breng de publieke sleutel over (`id_rsa.pub`) in de map met de bestandsopslagplaats die is geconfigureerd op 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 .                     |
+-----+

```

Configureer het certificaat om in te loggen in ISE

Bevestig of het openbare bestand zich onder de repository bevindt met behulp van de volgende opdracht:

```
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

```

- Importeer het bestand met de openbare sleutel (id_rsa.pub) met de opdracht in de voorkeursmodus:

crypto key import

repository

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

- Ga naar de globale configuratiemodus en gebruik de opdracht:

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>
```

Gebruik de opdracht om te controleren of u geen fouten krijgt terwijl u de openbare sleutel importeert. Het wordt aanbevolen om hiermee door te gaan via de consolepoort om te voorkomen dat de toegang tot de ISE verloren gaat.

Verifiëren

Aanmelden bij Windows

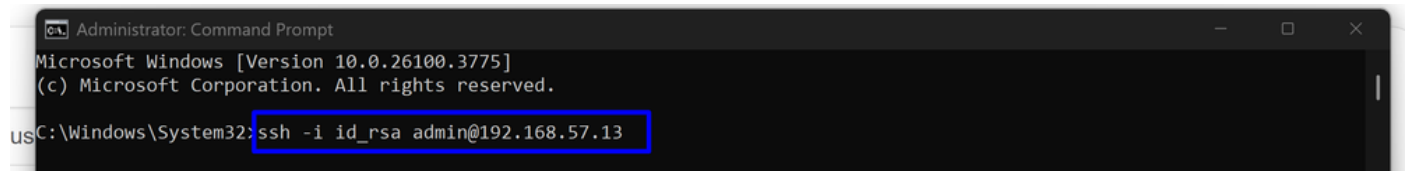
Probeer toegang te krijgen tot de ISE via `cmd` het commando:

ssh -i

@

EXAMPLE:

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



Gebruik de encryptiesleutel die is geconfigureerd in de stap [Maak de private en public keys in Windows](#) om te verifiëren.

Aanmelden bij MacOS

Voer deze opdracht in de terminal in:

```
ssh -i
```

@

EXAMPLE:

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

of

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

@

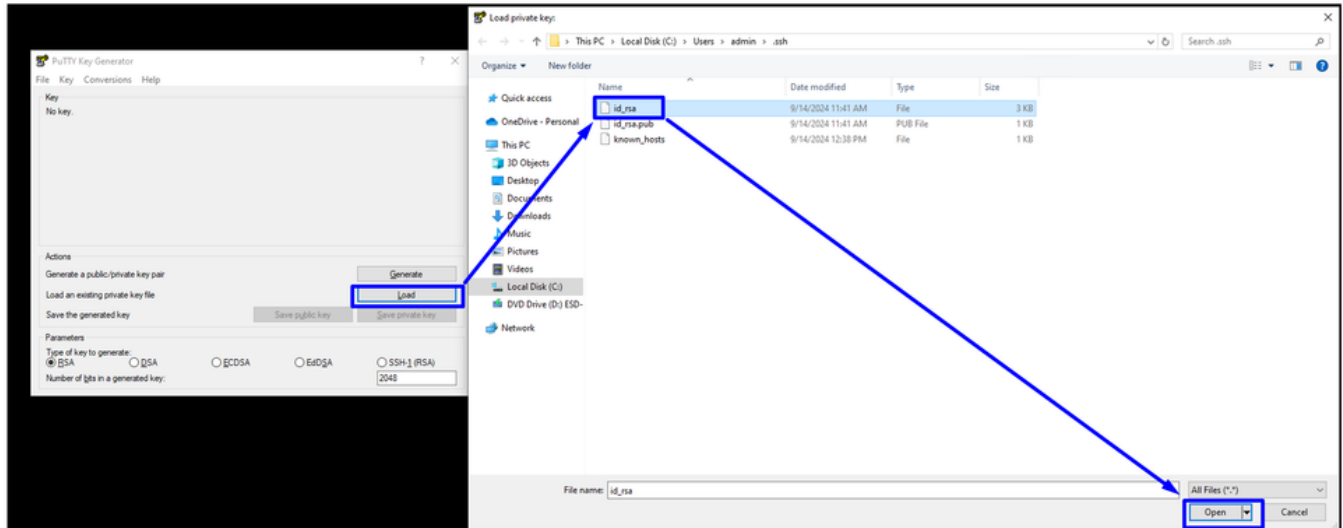
EXAMPLE:

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

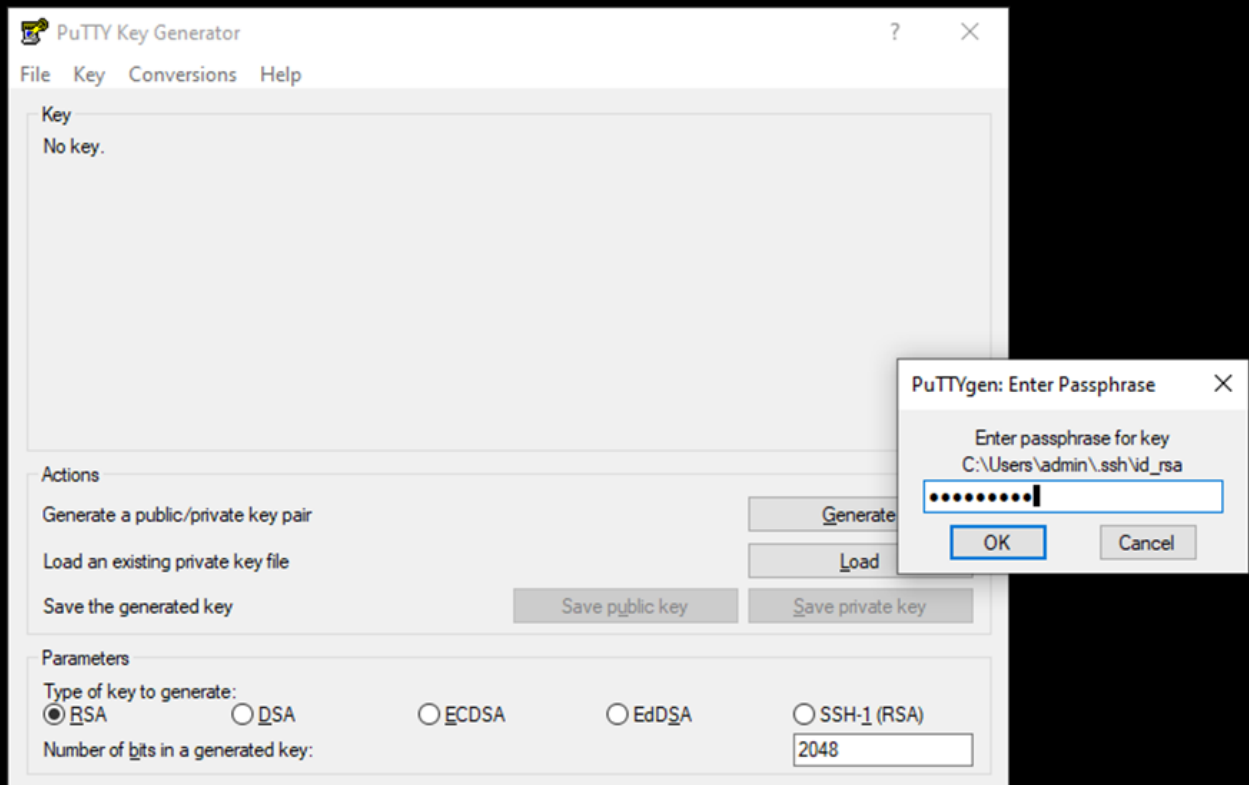
Gebruik de encryptiesleutel die is geconfigureerd in de stap [Maak de private en publieke sleutels via in MacOS](#) om te verifiëren.

Inloggen in Putty

Open PuTTY key generator (zoeken op PuttyGen in de startzoekbalk), klik op Load, selecteer alle bestanden en open de privésleutel die is gegenereerd vanuit cmd (Windows) of terminal (MacOS):

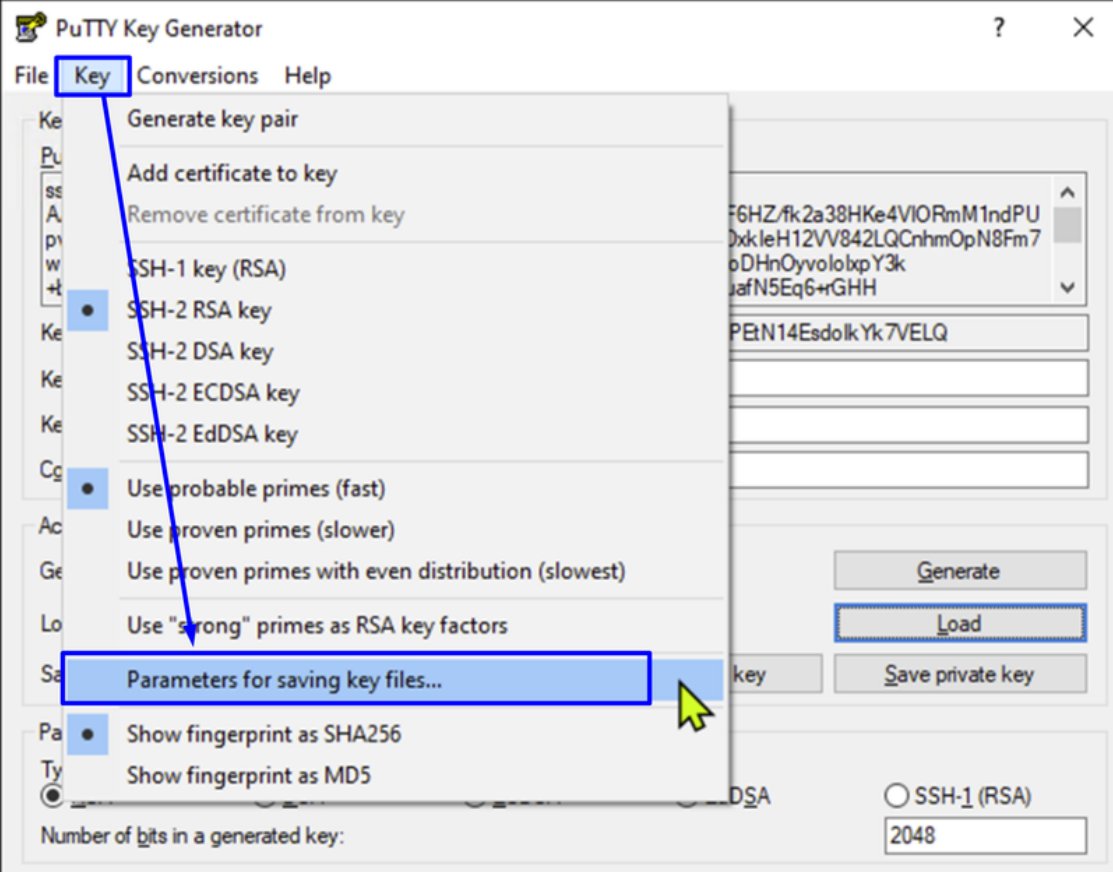


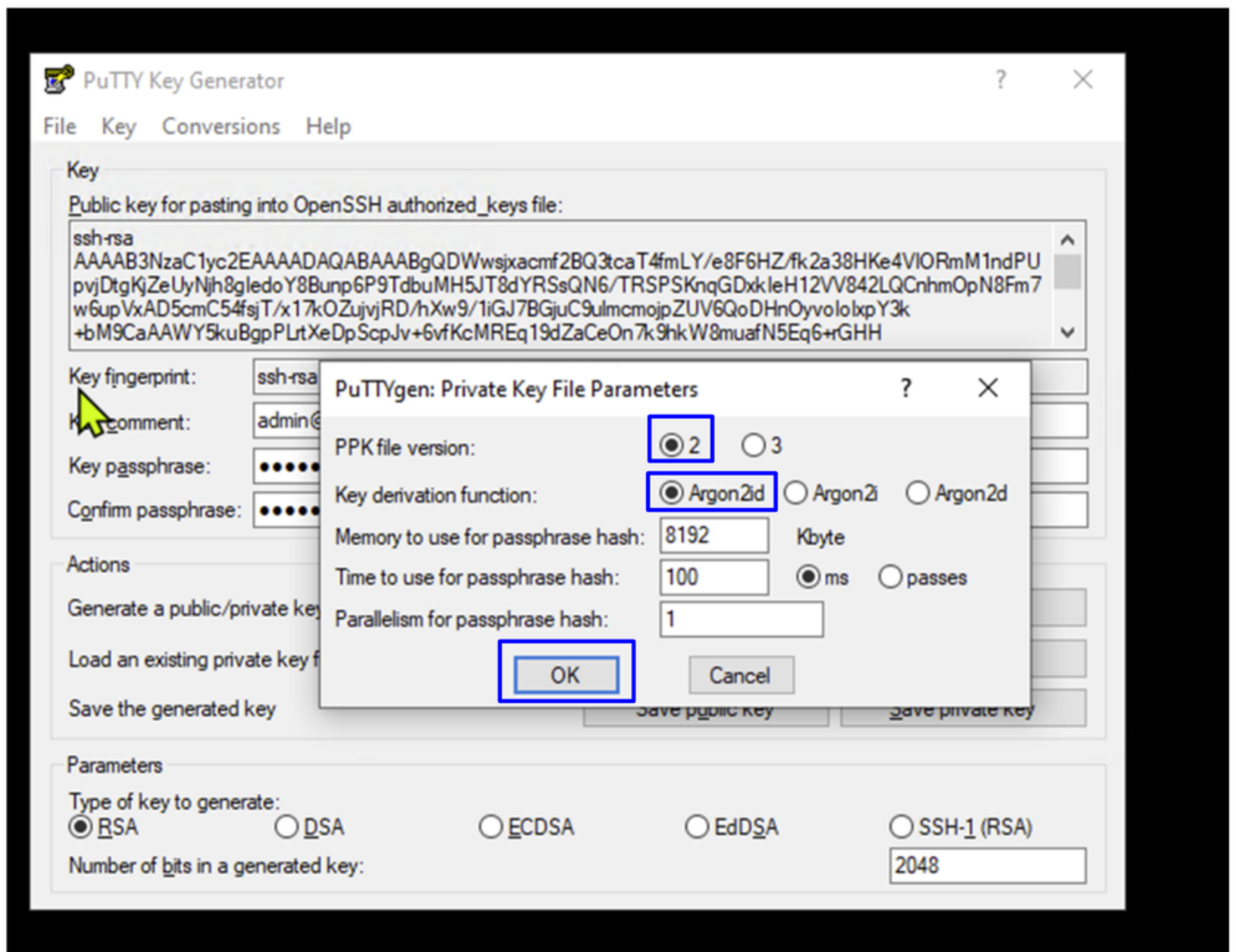
- Schrijf de eerder gebruikte coderingssleutel in de cmd of terminal



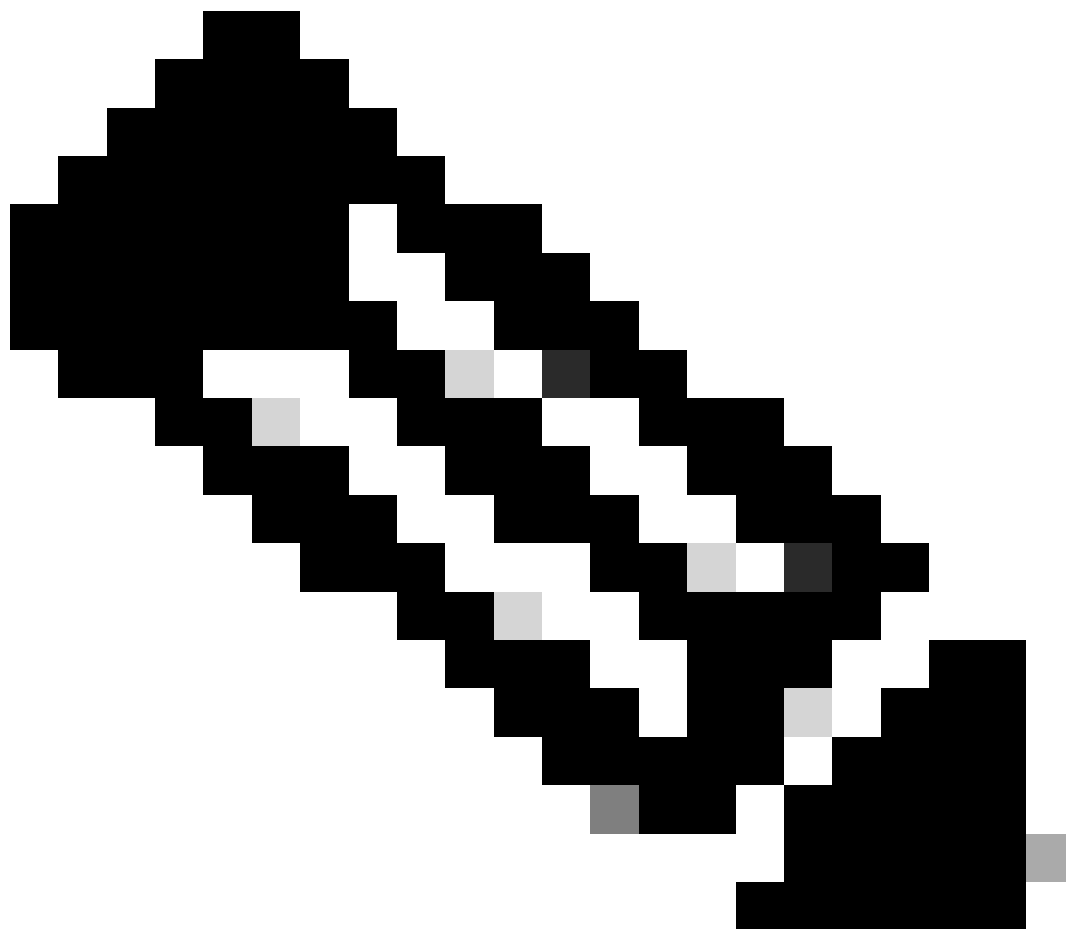
Converteer dit bestand naar een Putty-versie die compatibel is door de volgende stappen uit te voeren:

- Klik op Sleutel > Parameters voor het opslaan van belangrijke bestanden



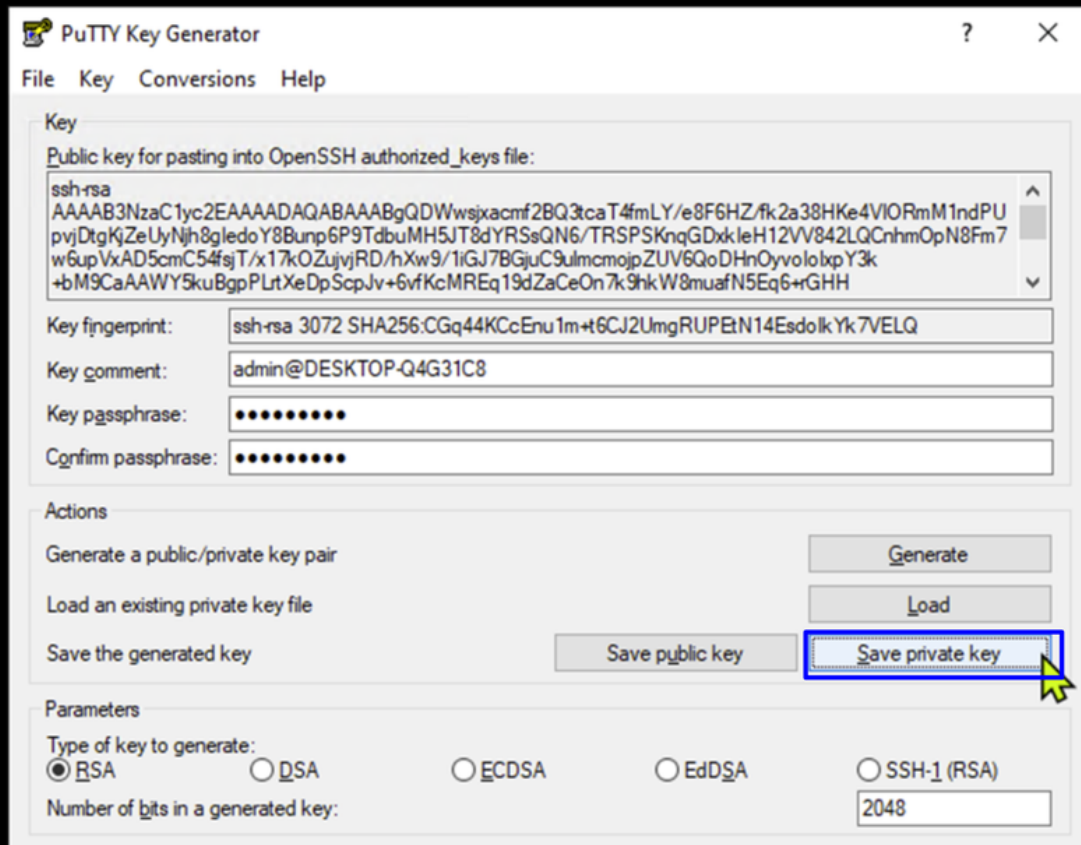


- PPK file version Kies: 2
- Key derivation function Kies: Argon2id



Opmerking: voor de rest van de parameters gebruikt u de standaardwaarden.

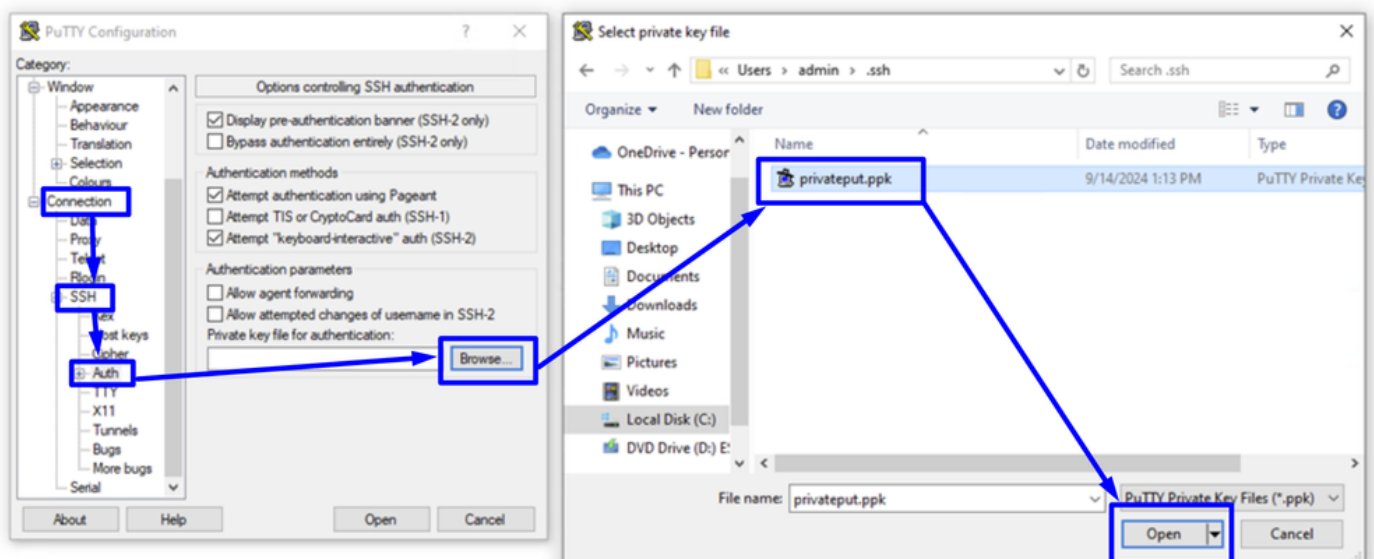
-
- Klik op de knop `Ok`



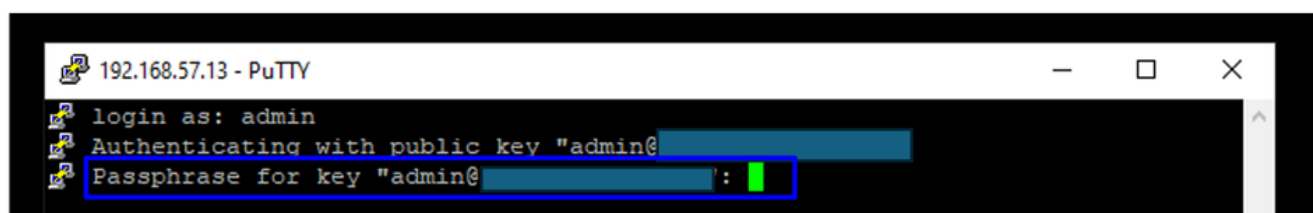
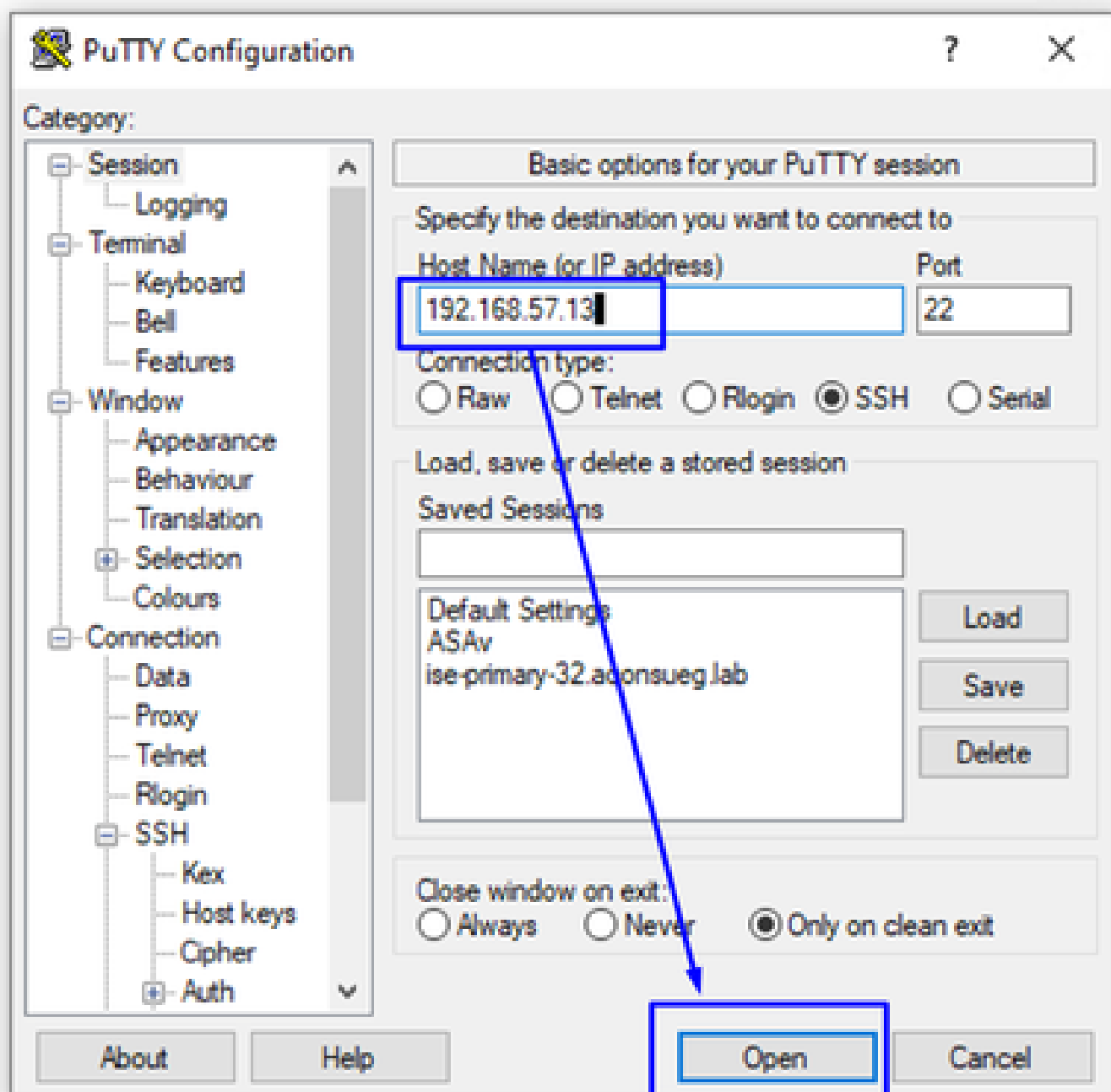
- Klik op Save private Key

Nadat u de sleutel op uw computer hebt opgeslagen, bent u klaar om deze te gebruiken door naar de volgende voorbeelden te verwijzen:

- open stopverf
- Klik op **Connection > SSH > Auth > Browse**
- Selecteer uw persoonlijke sleutel en klik op **Open**



- Ga terug naar sessie, stel het IP-adres of de hostnaam (FQDN) van de ISE in
- Klik op Openen



Gebruik de encryptiesleutel die is geconfigureerd in de stap [Maak de private en public keys via in MacOS](#) of [Maak de private en public keys in Windows](#) om te verifiëren.

Problemen oplossen

Bekijk foutmeldingen van de eindpuntsite en voeg in de ssh-verbinding de flag -v toe

Example for Windows:

```
ssh -v -i id_rsa admin@192.168.57.13
```

Example for MacOS:

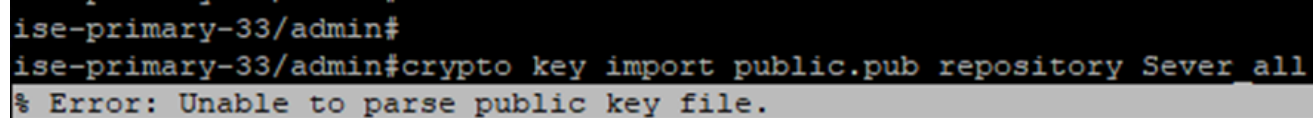
```
ssh -v -i id_rsa admin@192.168.57.13
```

of

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

Fout bij importeren openbare sleutel

% fout: bestand met openbare sleutel kan niet worden ontleed.



```
ise-primary-33/admin#  
ise-primary-33/admin#crypto key import public.pub repository Sever all  
% Error: Unable to parse public key file.
```

Als u problemen ondervindt bij het importeren van meer dan één openbare sleutel, neemt u contact op met Cisco-ondersteuning.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.