ISEを使用した秘密キー認証の設定

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

設定

- Windowsで秘密キーと公開キーを作成する
- MacOSで秘密キーと公開キーを作成する
- ISEにログインするための証明書の設定

確認

- Windowsでのログイン
- MacOSでのログイン
- Puttyにログインします。

トラブルシュート

- 公開キーのインポート中にエラーが発生しました

はじめに

このドキュメントでは、Identity Secure Engine(ISE)のCLIに対する認証用のプライベートセキュアシェル(SSH)キーを作成する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ISEのリポジトリ。
- 証明書認証。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ISE 3.3 パッチ 3
- Windows 10
- MacOS X
- SSHクライアントPutty

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

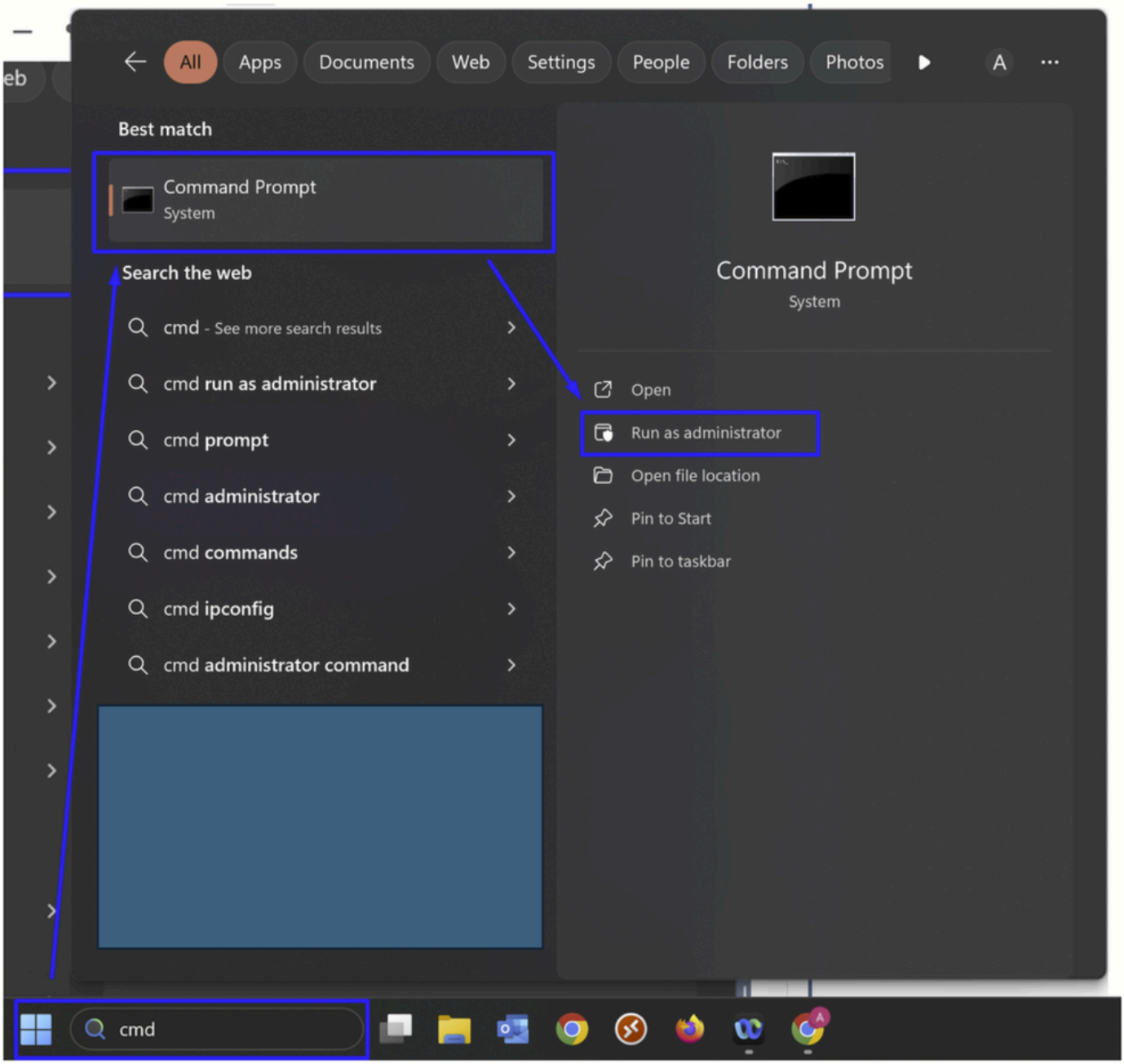
キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

Windowsで秘密キーと公開キーを作成する

タスクバーにある検索アイコンをクリックします。

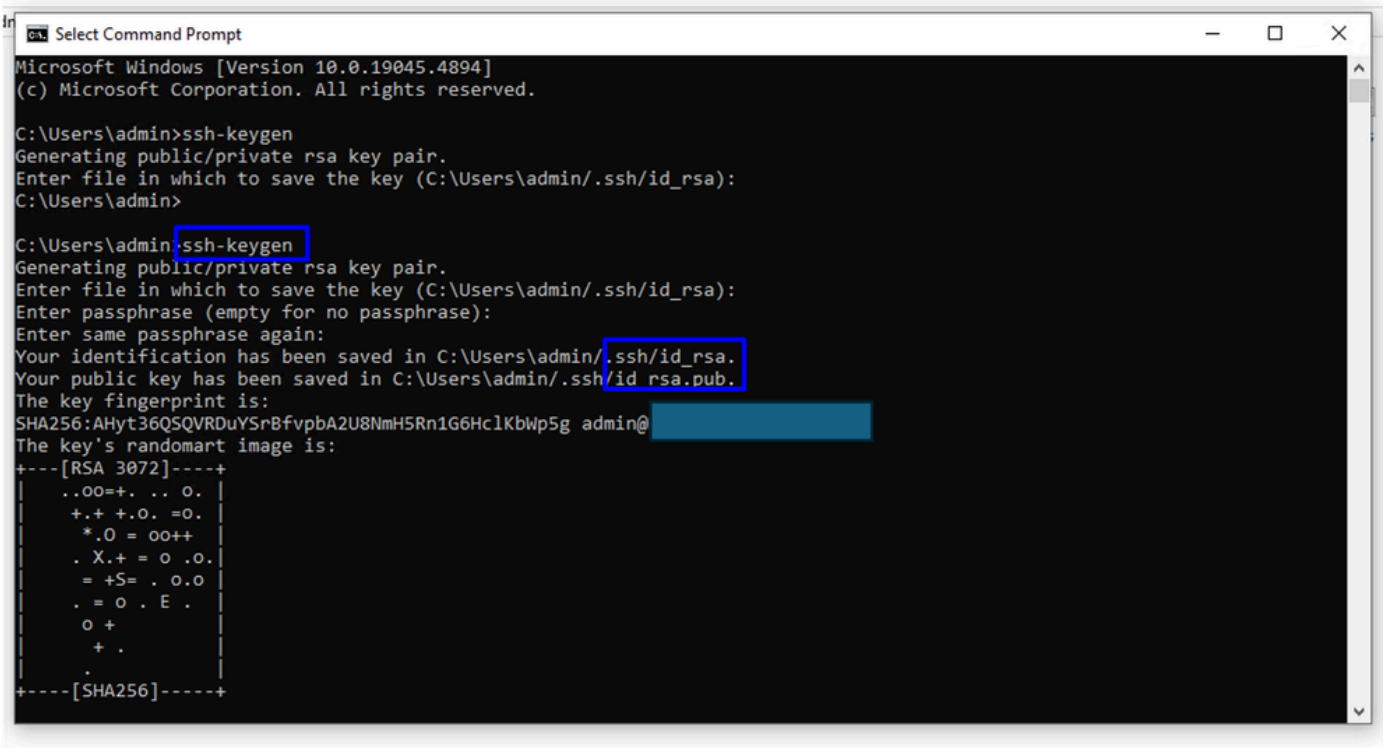
・ 検索バーにcmdと入力します。
・ 検索結果で、[コマンドプロンプト]を右クリックし、[管理者として実行]を選択します。これにより、コマンドを実行するために必要な権限が得られます



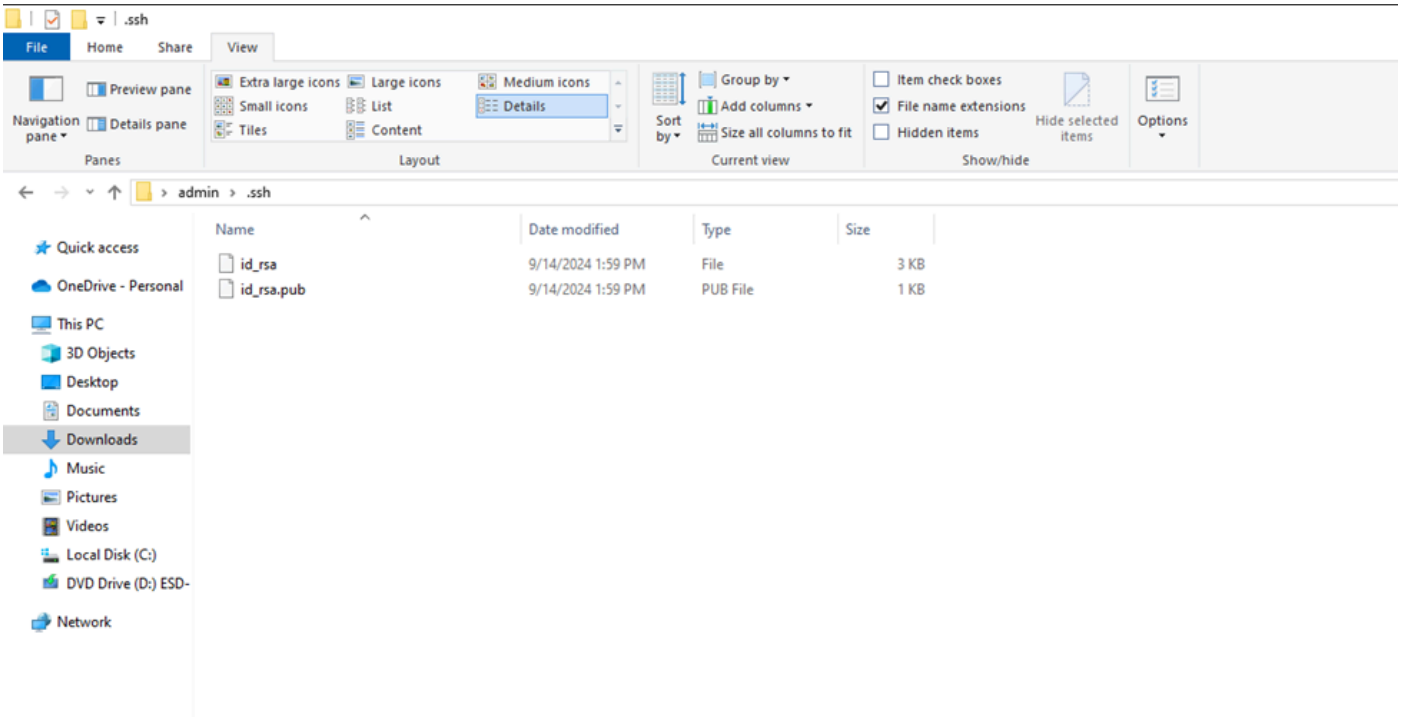
・ 次のコマンドを実行します：

```
ssh-keygen
```

- これにより、暗号化キーを2回入力するように求められます。これは、新しいパスワードとしてISEに対して認証されるためなので、保存してください。その後、プライベートキー(id_rsa)とパブリックキー(id_rsa.pub)の2つのファイルが作成されます。ファイルを1つのディレクトリに保存します。たとえば、デフォルトが使用されました



- ファイルの格納場所を確認する



ISEで設定されているファイルリポジトリフォルダ内の公開キー「(id_rsa.pub)」を転送します。

MacOSで秘密キーと公開キーを作成する

ドックにある「Finder」アイコンをクリックします
- に移動します。 Applications folder
- Applications folder内でUtilitiesフォルダを見つけて開きます
- [ユーティリティ]リストで、次の項目を検索します： Terminal
- 「Terminal」をダブルクリックして開きます。
- 「Terminal」ウィンドウで「ssh-keygen -t rsa」と入力し、Enterキーを押して実行します
- 暗号鍵を2回書き込み、 save it
- ファイルの場所に移動

ISEで設定されているファイルリポジトリフォルダ内の公開キー「(id_rsa.pub)」を転送します。

```
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:89:72:6b: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 .       |
+-----------------+
```

ISEにログインするための証明書の設定

次のコマンドを使用して、パブリックファイルがリポジトリの下にあるかどうかを確認します。

```
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
```

- 特権モードで次のコマンドを使用して、公開キーファイル(id_rsa.pub)をインポートします。

```
crypto key import
```

repository

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

- グローバルコンフィギュレーションモードにを入力し、コマンドを使用します。

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>
```

公開キーのインポート中にエラーが発生しないことを確認するには、コマンドを使用してください。ISEへのアクセスが失われないように、コンソールポート経由で続行することを推奨します。

確認

Windowsでのログイン

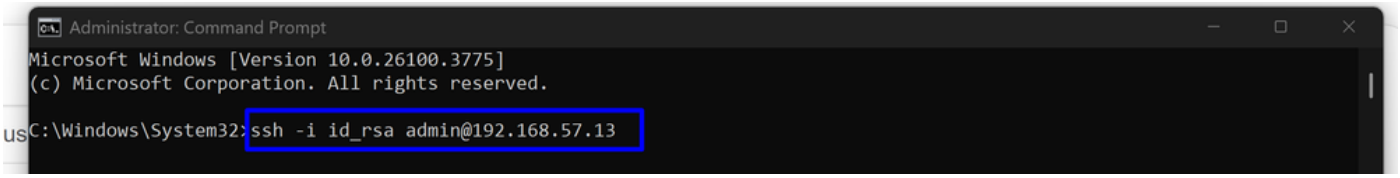
次のコマンドを使用して、cmd経由でのISEへのアクセスを試みます。

ssh -i

@

EXAMPLE:

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



「Windowsで秘密キーと公開キーを作成する」の手順で設定した暗号化キーを使用して認証します。

MacOSでのログイン

端末で次のコマンドを入力します。

```
ssh -i

        @


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

または

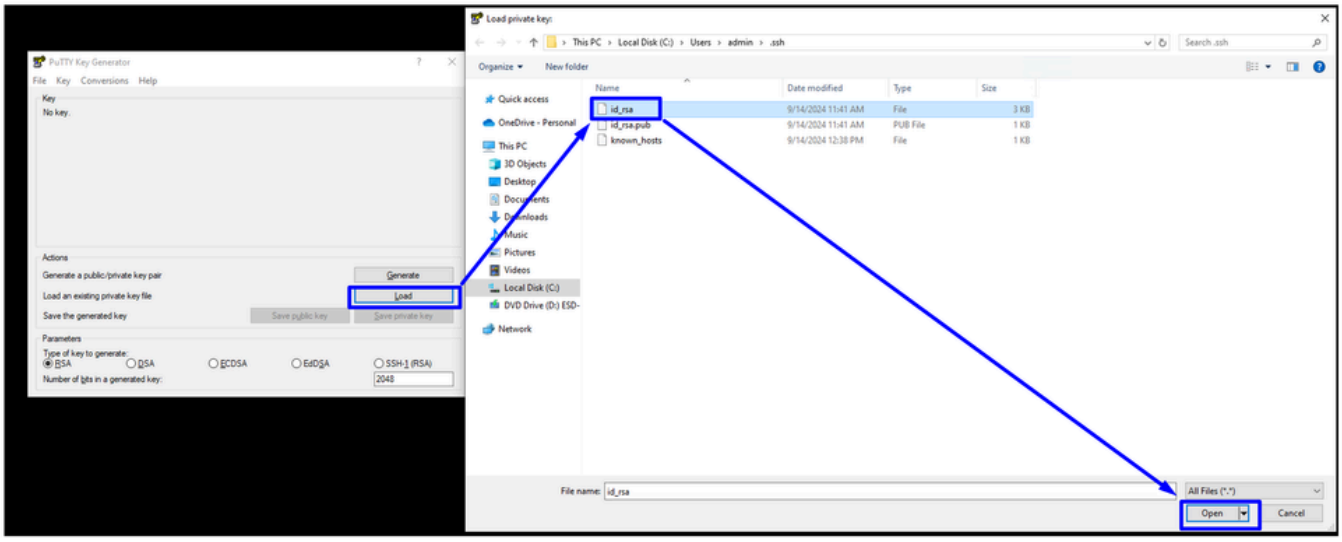
```
ssh -i ~/.ssh/

        @
```

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

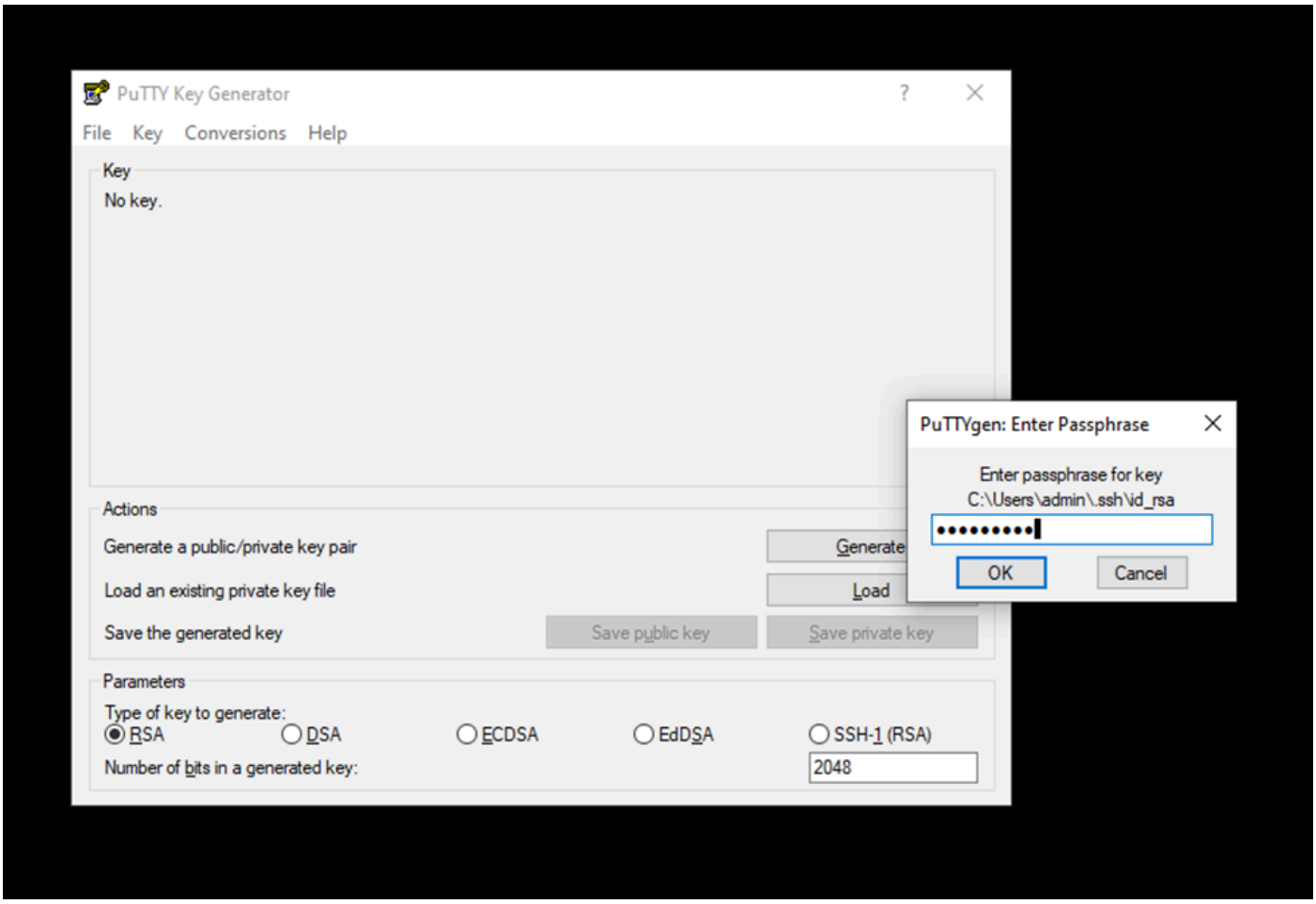
認証するには、「MacOSでの秘密鍵と公開鍵の作成にを使用する」の手順で設定した暗号キーを使用します。

Puttyにログインします。

PuTTy key generatorを開き（スタート検索バーでPuttyGenで検索）、Loadをクリックし、すべてのファイルを選択し、cmd(Windows)またはterminal(MacOS)から生成された秘密キーを開きます。

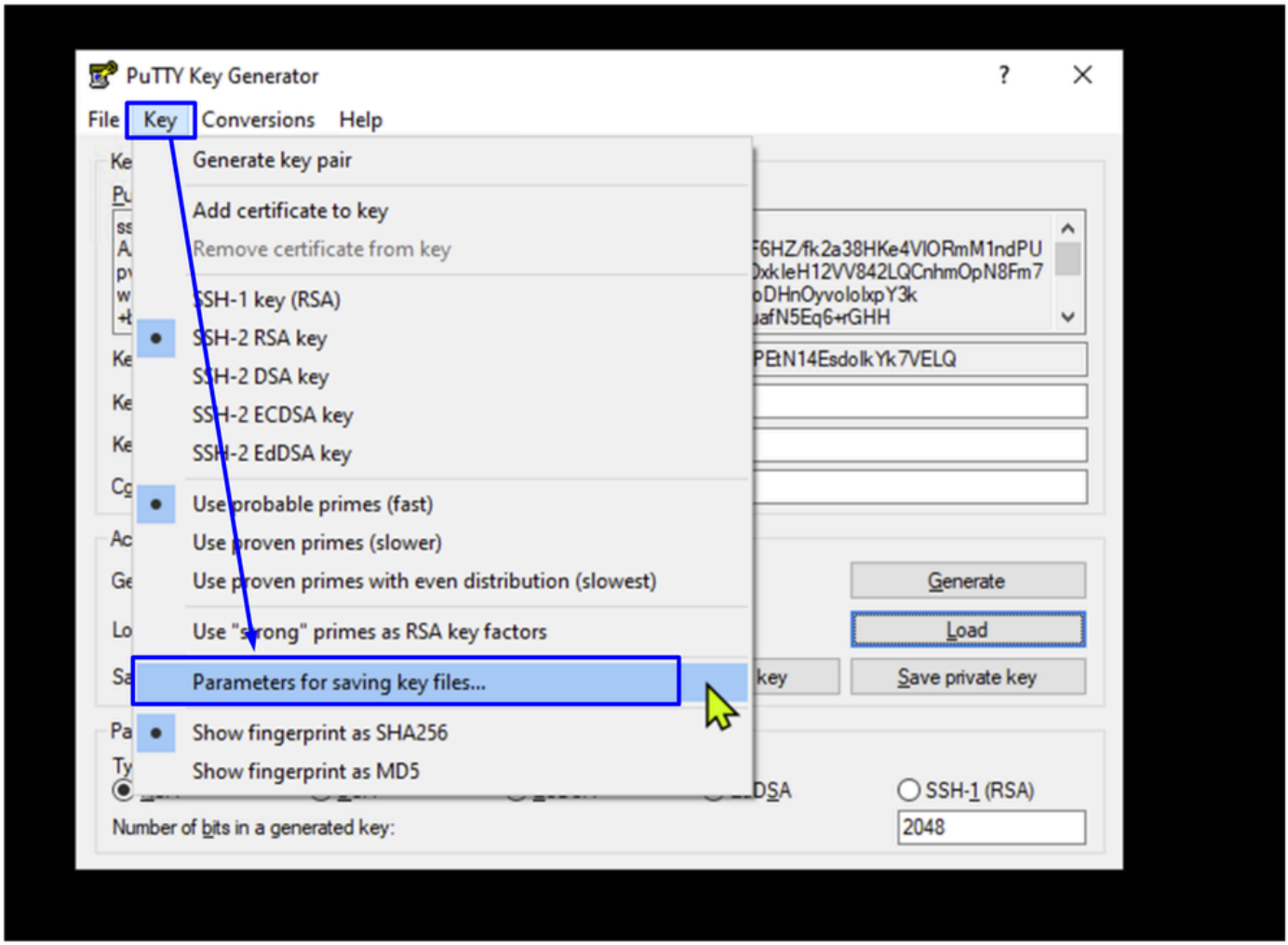


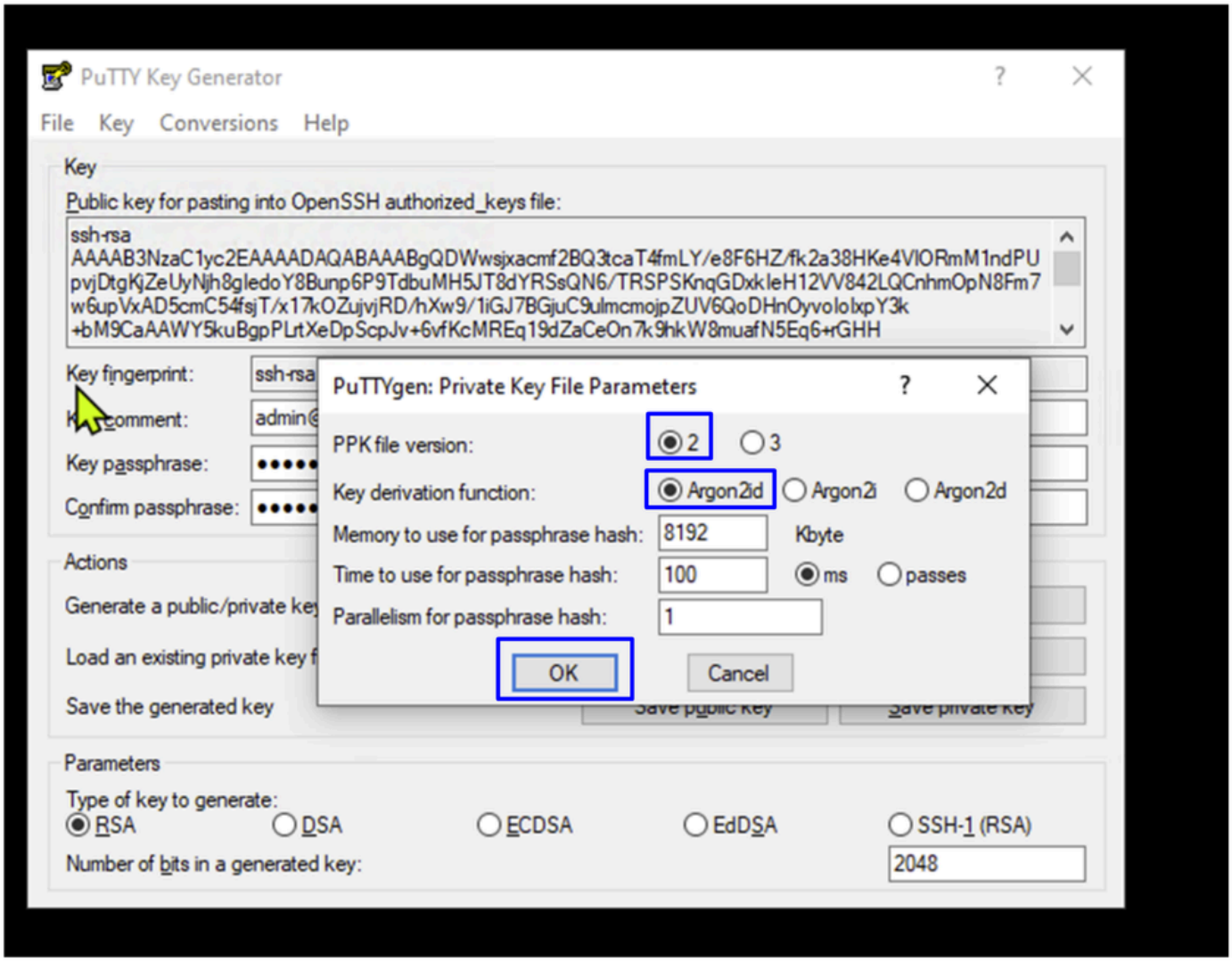
- cmdまたはterminalで以前使用した暗号キーを書き込みます



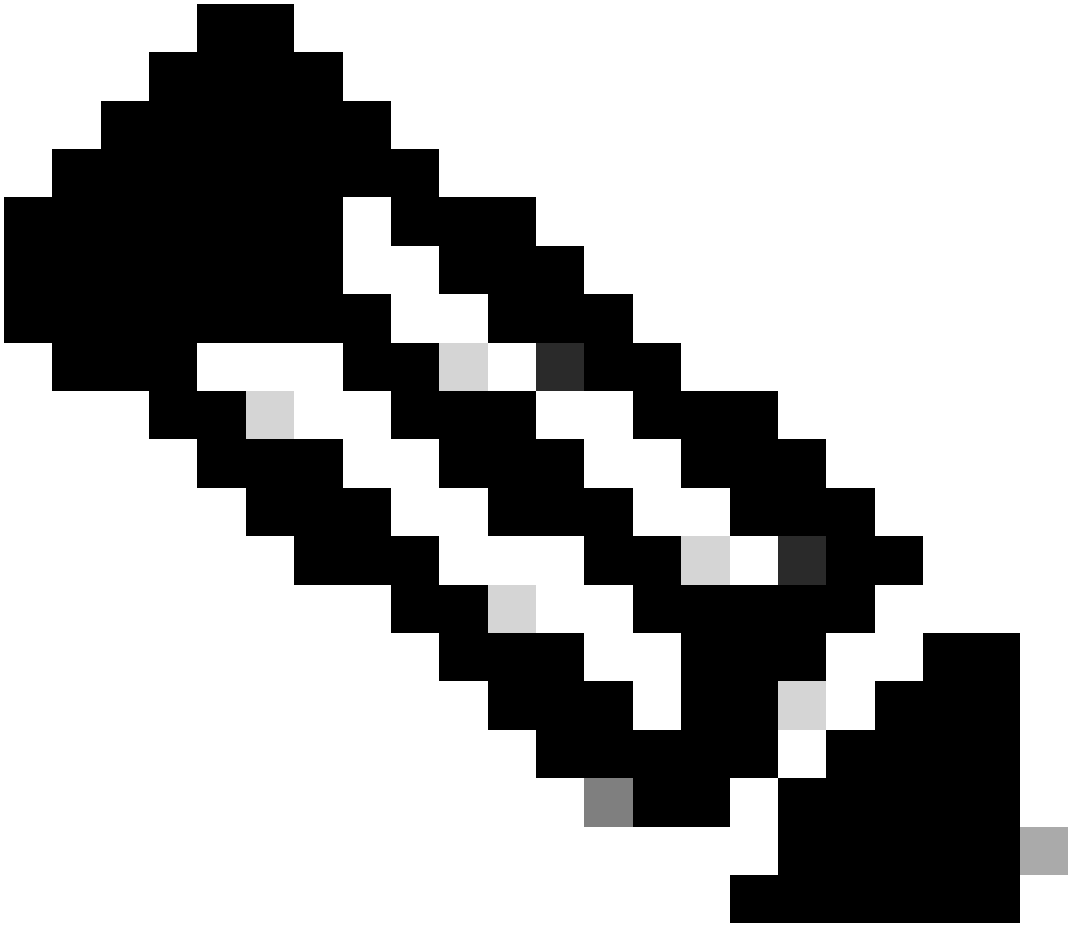
次の手順を実行して、このファイルを互換性のあるPuttyバージョンに変換します。

- Key > Parameters for saving key filesをクリックします。


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

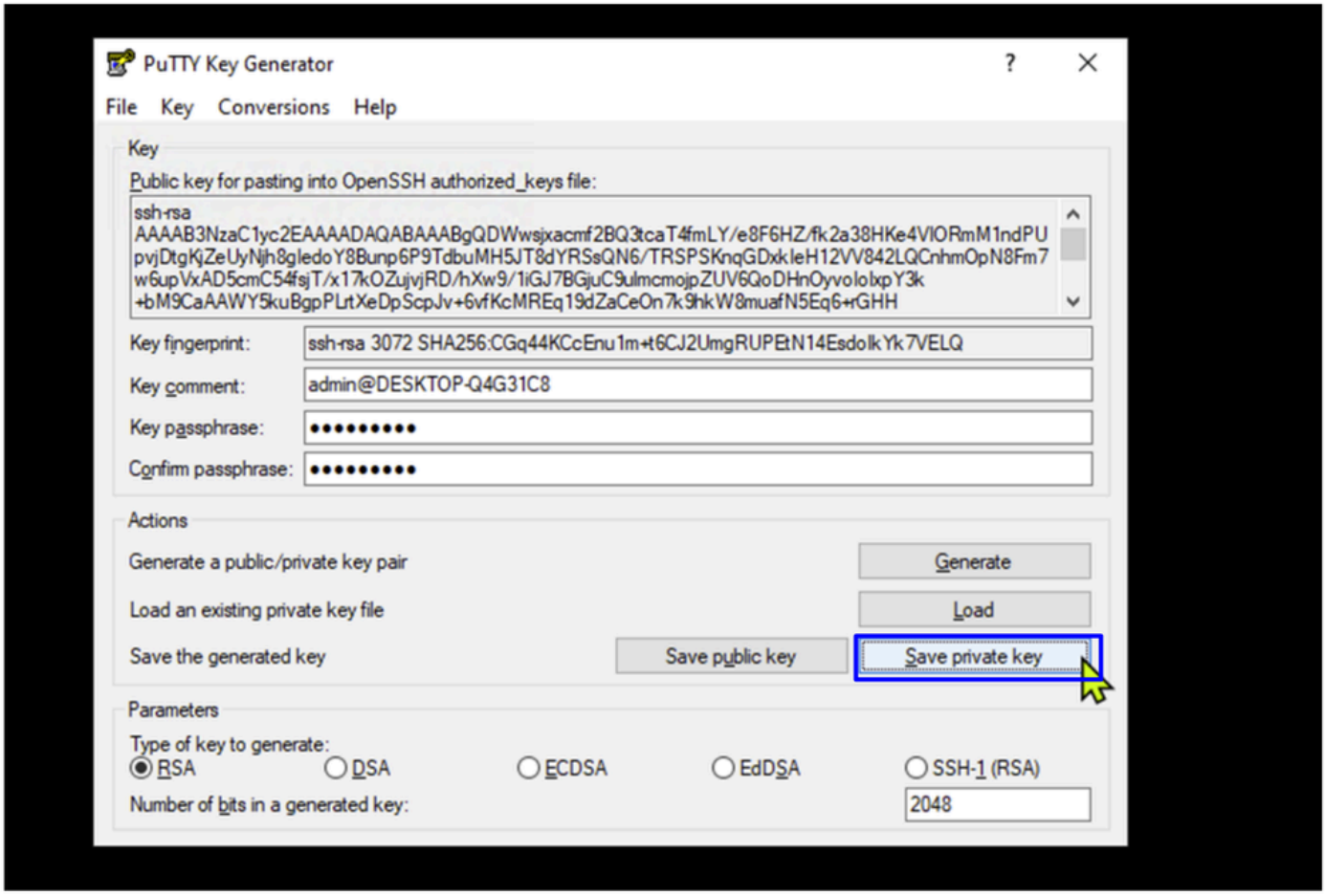


- PPK file version：2を選択
- **Key derivation function**: Argon2idを選択



注：残りのパラメータにはデフォルト値を使用します。

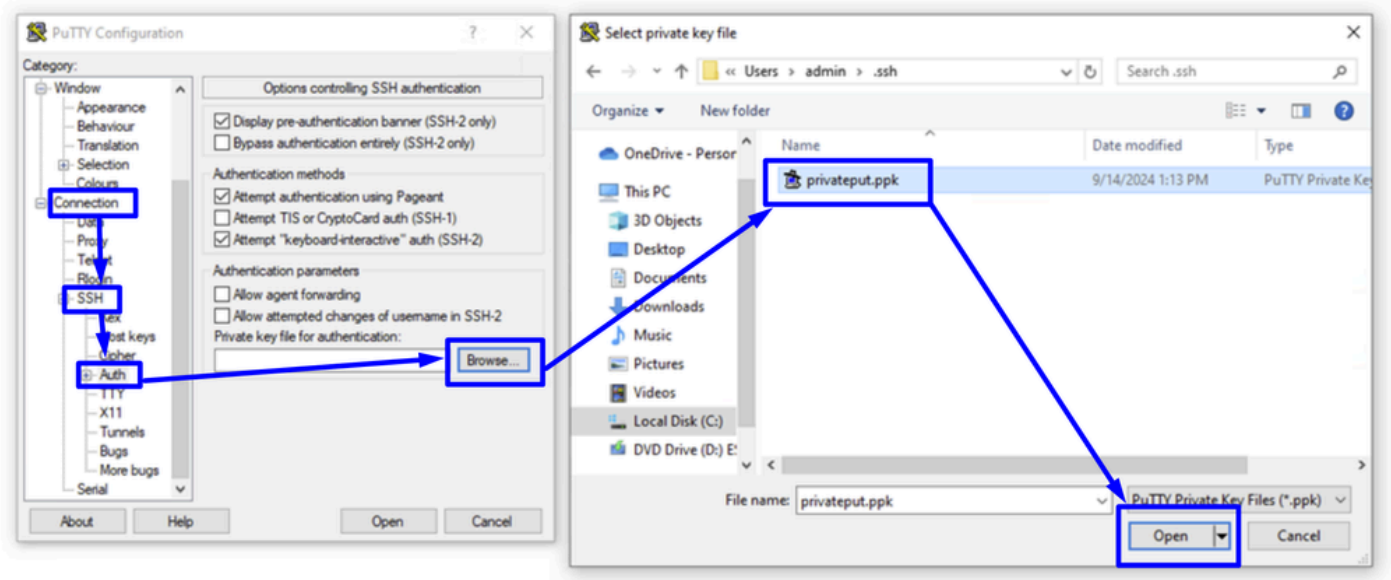
- [保存（ Ok



- クリック Save private Key

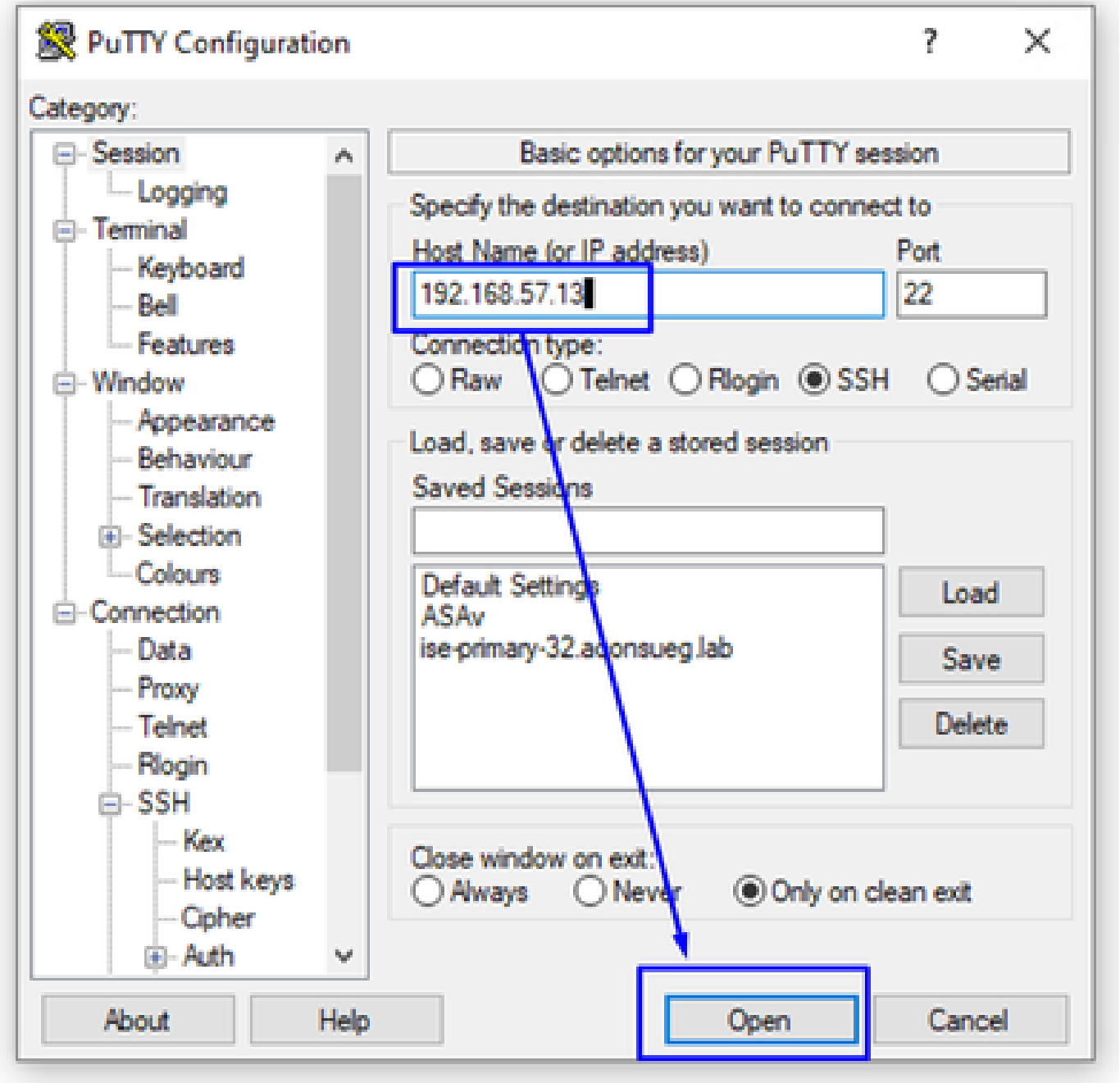
コンピュータにキーを保存したら、次の例を参照してキーを使用できます。

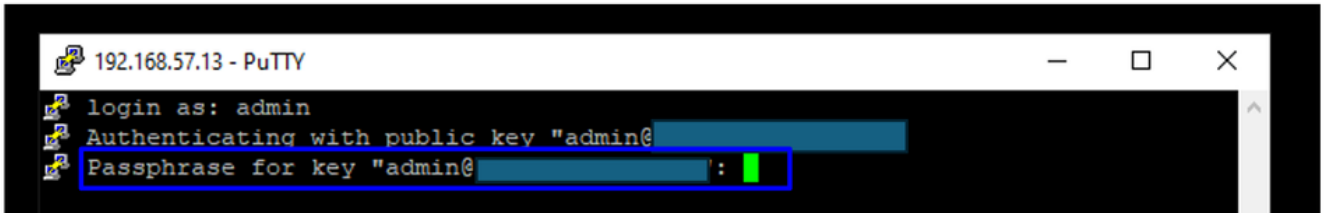
- Puttyを開く
- **Connection** > **SSH** > **Auth** >をクリックします **Browse**
- 秘密キーを選択し、 Open



- セッションに戻り、ISEのIPアドレスまたはホスト名(FQDN)を設定します

- Openをクリックします





MacOSでの秘密キーと公開キーの作成手順またはWindowsでの秘密キーと公開キーの作成手順で設定した暗号化キーを使用して、認証を行います。

トラブルシュート

エンドポイントサイトからのエラーメッセージを確認し、ssh接続にフラグ-vを追加します。

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

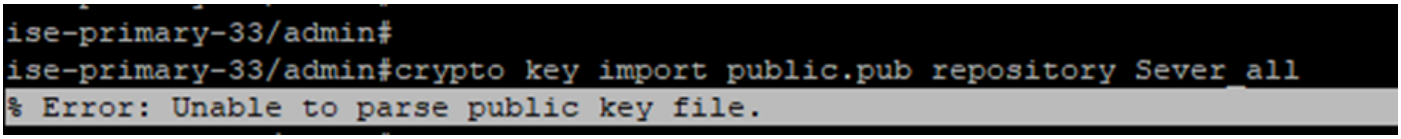
```
Example for MacOS:
ssh -v -i id_rsa admin@192.168.57.13
```

または

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

公開キーのインポート中にエラーが発生しました

%エラー：公開キーファイルを解析できません。



複数の公開キーをインポートする際に不便が生じる場合は、Ciscoサポートにお問い合わせください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。