

在Google雲平台上部署CSR1000v/C8000v

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[專案設定](#)

[步驟 1. 確定帳戶的有效專案。](#)

[步驟 2. 建立新的VPC和子網。](#)

[步驟 3. 虛擬例項部署。](#)

[驗證部署](#)

[從遠端連線至新執行處理](#)

[使用Bash終端登入到CSR1000v/C8000v](#)

[使用PuTTY登入到CSR1000v/C8000v](#)

[使用SecureCRT登入到CSR1000v/C8000v](#)

[其他VM登入方法](#)

[授權其他使用者登入GCP中的CSR1000v/C8000v](#)

[設定新的使用者名稱/密碼](#)

[使用SSH金鑰配置新使用者](#)

[驗證登入至CSR1000v/C8000v的已配置使用者](#)

[疑難排解](#)

[如果顯示「作業逾時」錯誤訊息。](#)

[如果需要密碼](#)

[相關資訊](#)

簡介

本檔案介紹在Google Cloud Platform (GCP)上部署和設定Cisco CSR1000v和Catalyst 8000v (C800v)的程式。

必要條件

需求

思科建議您瞭解以下主題：

- [虛擬化技術/虛擬機器器\(VM\)](#)
- [雲端平台](#)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 對Google Cloud Platform的活動訂閱，已建立專案
- GCP主控台
- GCP市場
- Bash終端、Putty或SecureCRT
- 公用和專用安全殼層(SSH)金鑰

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊


從17.4.1開始，CSR1000v變為C8000v，具有相同的功能，但增加了新功能，如SD-WAN和Cisco DNA許可。如需進一步參考，請驗證官方產品資料表：

[Cisco Cloud Services Router 1000v資料表](#)

[Cisco Catalyst 8000V Edge軟體資料表](#)

因此，本指南適用於CSR1000v和C8000v路由器的安裝。

專案設定


 注意：在撰寫本文檔時，新使用者有300美元的免費積分，可將GCP作為免費套餐全面探索一年。這由Google定義，不受思科控制。

 注意：本文檔要求建立公用SSH金鑰和專用SSH金鑰。有關其他資訊，請參閱[生成例項SSH金鑰以便在Google雲平台中部署CSR1000v](#)

步驟 1. 確定帳戶的有效專案。

確保您的帳戶具有有效且活動的專案，這些專案必須與具有Compute Engine許可權的組關聯。

對於此示例部署，使用GCP中建立的專案。

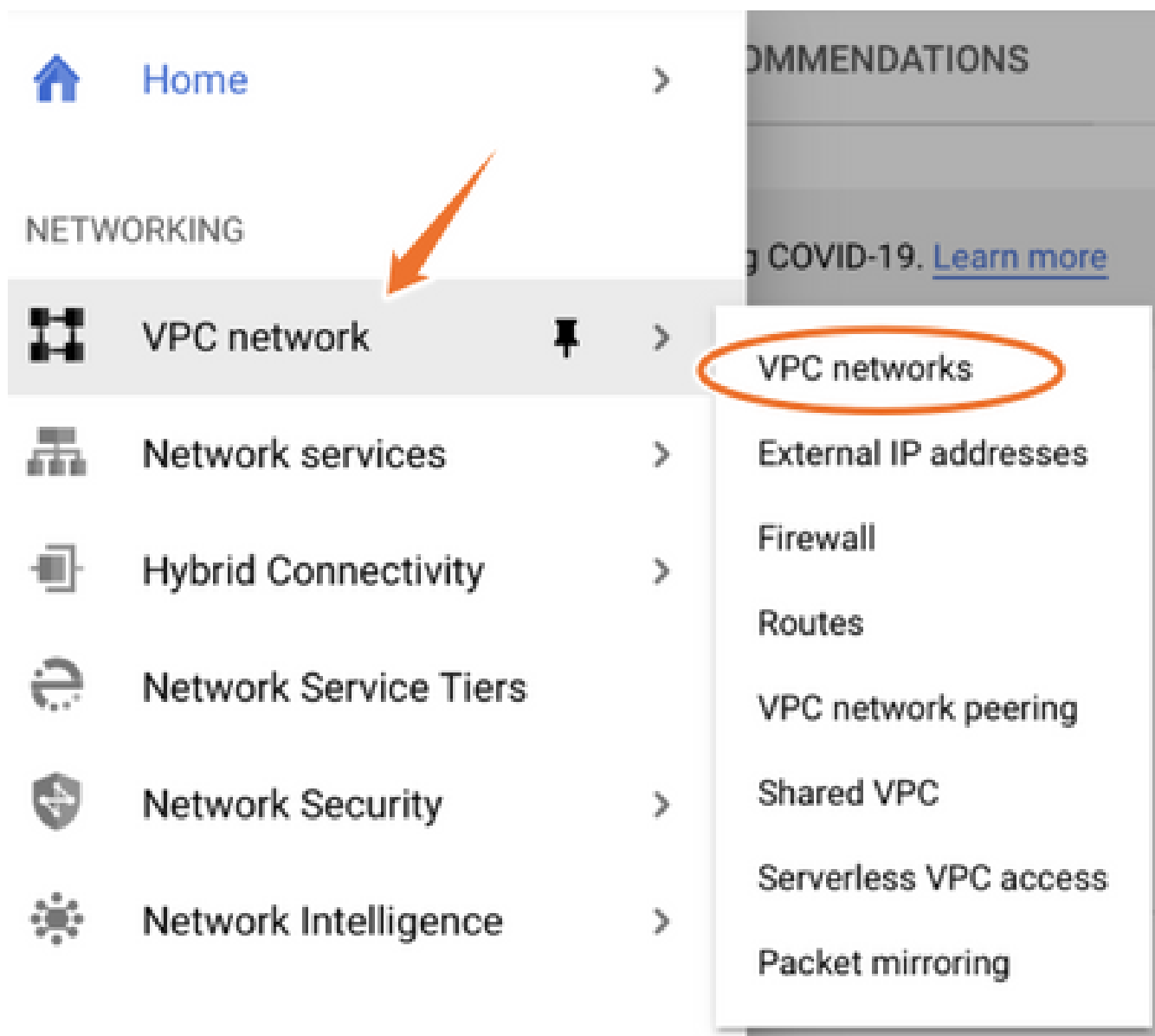
 附註：若要建立新專案，請參閱[建立和管理專案](#)。

步驟 2. 建立新的VPC和子網。

建立新的虛擬私有雲(VPC)和必須與CSR1000v例項關聯的子網。

可以使用預設VPC或以前建立的VPC和子網。

在控制檯控制台中，選擇VPC網路> VPC網路 (如圖所示)。



選擇Create VPC Network (如圖所示)。

Name ↑	Region	Subnets	MTU ⓘ	Mode	IP address ranges	Gateways	Firewall Rules
▼ default		24	1460	Auto ▼			22
	us-central1	default			10.128.0.0/20	10.128.0.1	
	europa-west1	default			10.132.0.0/20	10.132.0.1	
	us-west1	default			10.138.0.0/20	10.138.0.1	
	asia-east1	default			10.140.0.0/20	10.140.0.1	
	us-east1	default			10.142.0.0/20	10.142.0.1	
	asia-northeast1	default			10.146.0.0/20	10.146.0.1	
	asia-southeast1	default			10.148.0.0/20	10.148.0.1	
	us-east4	default			10.150.0.0/20	10.150.0.1	
	australia-southeast1	default			10.152.0.0/20	10.152.0.1	

註：目前，CSR1000v僅部署在GCP上的美國中部地區。

如圖所示配置VPC名稱。

← Create a VPC network

Name *
csr-vpc

Lowercase letters, numbers, hyphens allowed

Description

配置與VPC關聯的子網名稱並選擇區域us-central1。

在us-central1 CIDR 10.128.0.0/20內分配有效的IP地址範圍，如圖所示。

保留其他設定作為預設值並選擇建立按鈕：

Subnets

Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets. [Learn more](#)

Subnet creation mode

- Custom
 Automatic

New subnet

Name *
csr-subnet

Lowercase letters, numbers, hyphens allowed

[Add a description](#)

Region *
us-central1

IP address range *
10.10.1.0/24

 備註：如果選取「自動」，GCP會指定區域CIDR內的自動有效範圍。

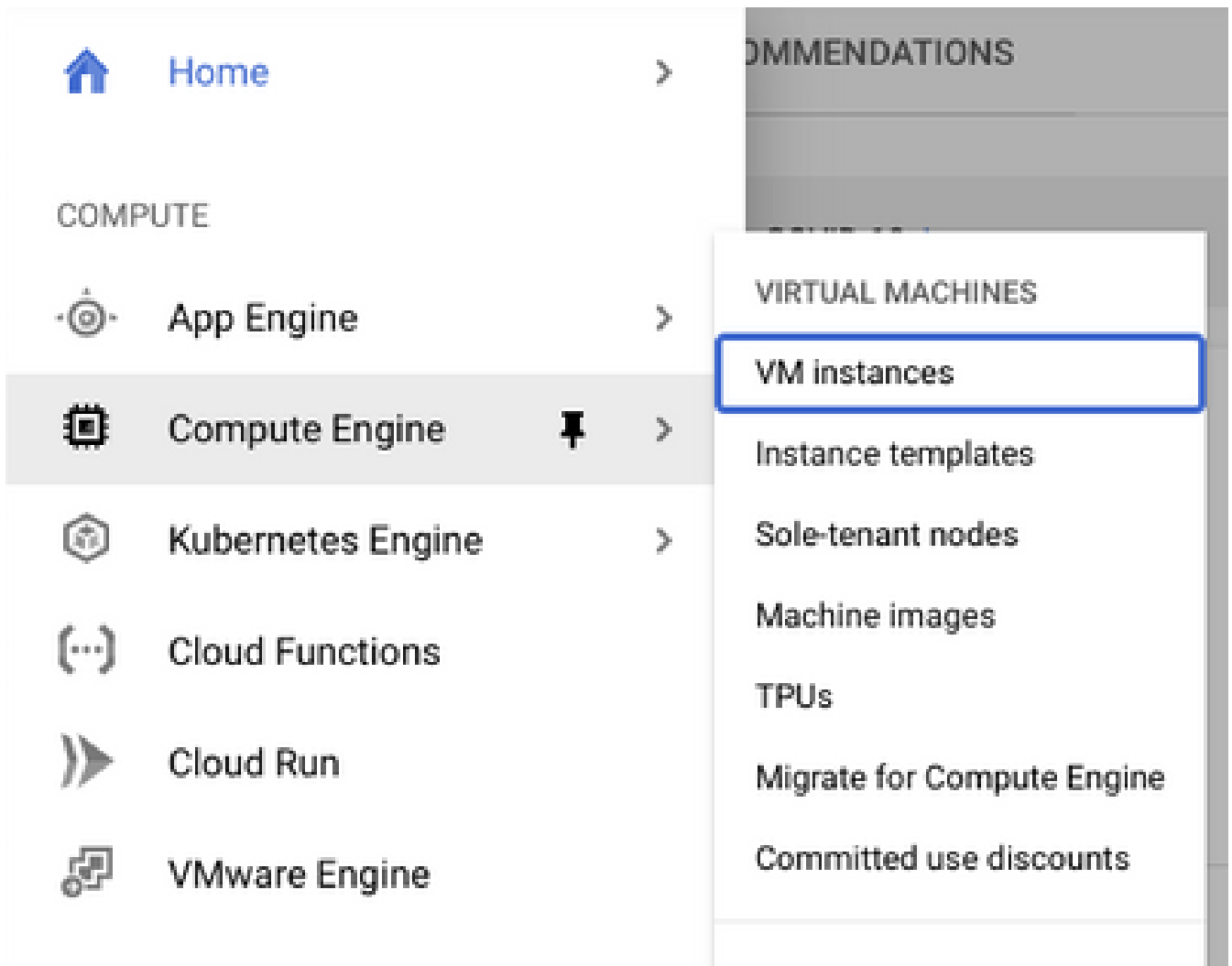
建立過程完成後，新VPC將顯示在VPC網路部分，如圖所示。

VPC networks [+ CREATE VPC NETWORK](#) [REFRESH](#)

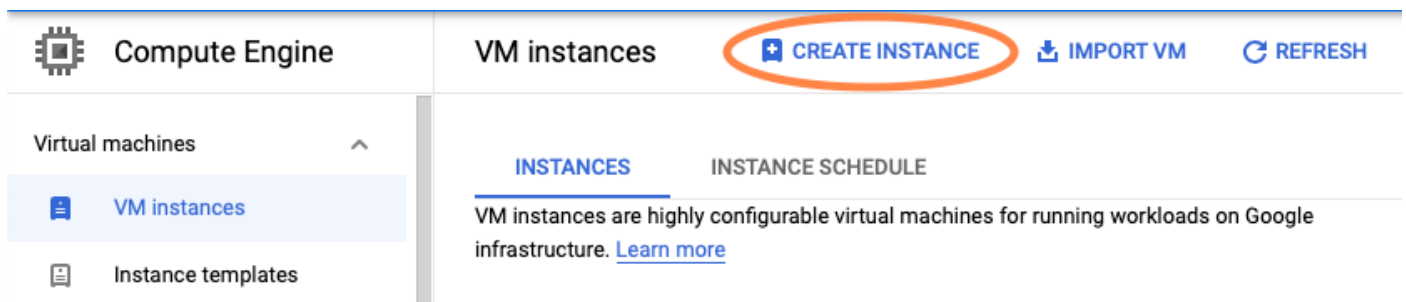
Name ↑	Region	Subnets	MTU ?	Mode	IP address ranges	Gateways
▼ csr-vpc		1	1460	Custom		
	us-central1	csr-subnet			<u>10.10.1.0/24</u>	<u>10.10.1.1</u>

步驟 3. 虛擬例項部署。

在計算引擎部分，選擇計算引擎 > VM例項，如下圖所示。



在VM控制台中，選擇建立例項頁籤，如圖所示。



請使用圖中所示的GCP marketplace顯示思科產品。



Create an instance

To create a VM instance, select one of the options:



New VM instance

Create a single VM instance from scratch



New VM instance from template

Create a single VM instance from an existing template



New VM instance from machine image

Create a single VM instance from an existing machine image



Marketplace

Deploy a ready-to-go solution onto a VM instance

在搜尋欄中，鍵入Cisco CSR 或Catalyst C8000v，選擇符合您要求的型號和版本，然後選擇Launch。

對於此示例部署，選擇了第一個選項，如圖所示。

Filter Type to filter

Category

Compute

(4)

Networking

(7)

Type

Virtual machines

X

Virtual machines

7 results

**Cisco Cloud Services Router 1000V (CSR 1000V)**

Cisco Systems

The Bring Your Own License (BYOL) of Cisco Cloud Services Router (CSR1000V) delivers enterprise-class networking services in the cloud through Google Compute Platform. This software supports all the four CSR Technology packages. This enables enterprise IT to deploy the same enterprise-class networking services in the cloud through Google Compute Platform.

**Cisco Cloud Services Router 1000V - 16.12 - BYOL**

Cisco Systems

The Bring Your Own License (BYOL) of Cisco Cloud Services Router (CSR1000V) delivers enterprise-class networking services in the cloud through Google Compute Platform. This software supports all the four CSR Technology packages. This enables enterprise IT to deploy the same enterprise-class networking services in the cloud through Google Compute Platform.

**Cisco Cloud Services Router 1000V - 17.2.1r - BYOL**

Cisco Systems

The Bring Your Own License (BYOL) of Cisco Cloud Services Router (CSR1000V) delivers enterprise-class networking services in the cloud through Google Compute Platform. This software supports all the four CSR Technology packages. This enables enterprise IT to deploy the same enterprise-class networking services in the cloud through Google Compute Platform.

**Cisco Cloud Services Router 1000V - 17.3 - BYOL**

Cisco Systems

The Bring Your Own License (BYOL) of Cisco Cloud Services Router (CSR1000V) delivers enterprise-class networking services in the cloud through Google Compute Platform. This software supports all the four CSR Technology packages. This enables enterprise IT to deploy the same enterprise-class networking services in the cloud through Google Compute Platform.

Marketplace > "catalyst 8000v edge software - byol" > Virtual machines

Filter Type to filter

Virtual machines

Category



1 result

Compute

(1)

Networking

(1)

Type

Virtual machines



Catalyst 8000V Edge Software - BYOL

Cisco Systems

As part of Cisco's Cloud connect portfolio, the Bring Your Own License (BYOL) version of C 8000V) delivers the maximum performance for virtual enterprise-class networking service the Catalyst 8000V (C8000V) DNA packages and supports the high-performance versions

注意：BYOL代表「自帶許可證」。

備註：目前，GCP不支援「現收現付」(PAYG)模式。

GCP需要輸入必須與VM關聯的配置值，如圖所示：

在GCP中部署CSR1000v/C8000v需要使用者名稱和SSH公鑰，如圖所示。如果尚未建立SSH金鑰，請參閱[生成例項SSH金鑰以便在Google雲平台中部署CSR1000v](#)。

← New Cisco Cloud Services Router 1000V (CSR 1000V)

Deployment name

Instance name

Username

Instance SSH Key

Zone ?

Machine type ?

15 GB memory

[Customize](#)

Boot Disk

Boot disk type ?

Boot disk size in GB ?

選擇之前建立的VPC和子網，並在外部IP中選擇Evermeral，以便讓公共IP與例項關聯，如圖所示。

配置此配置後。選取啟動按鈕。

Networking

Network ?

csr-vpc

Subnetwork ?

csr-subnet (10.10.1.0/24)

External IP ?

Ephemeral


Firewall ?

Add tags and firewall rules to allow specific network traffic from the Internet

- Allow TCP port 22 traffic
- Allow HTTP traffic
- Allow TCP port 21 traffic

 注意：透過SSH連線到CSR例項需要埠22。HTTP埠是可選的。

部署完成後，選擇Compute Engine > VM instances 以驗證已成功部署新的CSR1000v，如圖所示。

Name	Zone	Recommendation	In use by	Internal IP	External IP	Connect
<input checked="" type="checkbox"/> csr-cisco	us-central1-f			10.10.1.2 (nic0)		SSH

驗證部署

從遠端連線至新執行處理

在GCP中登入到CSR1000v/C8000V的最常用方法是Bash終端中的命令列Putty和SecureCRT。在本節中，是連線上述方法所需的配置。

使用Bash終端登入到CSR1000v/C8000v

遠端連線到新CSR所需的語法為：

<#root>

```
ssh -i private-key-path username@publicIPAddress
```

範例：

```
<#root>
```

```
$  
ssh -i CSR-sshkey <snip>@X.X.X.X  
  
The authenticity of host 'X.X.X.X (X.X.X.X)' can't be established.  
RSA key fingerprint is SHA256:c3JsVDEt68CeUFGhp91rYz7tU07htbsPhAwanh3feC4.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'X.X.X.X' (RSA) to the list of known hosts.
```

如果連線成功，則顯示CSR1000v提示

```
<#root>
```

```
$  
ssh -i CSR-sshkey <snip>@X.X.X.X
```

```
csr-cisco# show version  
Cisco IOS XE Software, Version 16.09.01  
Cisco IOS Software [Fuji], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.9.1, RELEASED  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2018 by Cisco Systems, Inc.  
Compiled Tue 17-Jul-18 16:57 by mcpre
```

使用PuTTY登入到CSR1000v/C8000v

要連線Putty，請使用PuTTYgen應用程式將私鑰從PEM轉換為PPK格式。

有關其他資訊，請參閱[使用PuTTYgen將Pem轉換為Ppk檔案](#)。

以正確格式生成私鑰後，您必須在Putty中指定路徑。

在SSH連線選單的auth選項中選擇用於身份驗證的私鑰檔案部分。

瀏覽至儲存金鑰的資料夾，然後選取建立的金鑰。在本示例中，影象顯示Putty選單的圖形檢視和所需的狀態：



Category:

- ... Keyboard
- ... Bell
- ... Features
- [-] Window
 - ... Appearance
 - ... Behaviour
 - ... Translation
 - [+] Selection
 - ... Colours
- [-] **Connection**
 - ... Data
 - ... Proxy
 - ... Telnet
 - ... Rlogin
 - [-] **SSH**
 - ... Kex
 - ... Host keys
 - ... Cipher
 - [+] **Auth**
 - ... TTY
 - ... X11
 - ... Tunnels

Options controlling SSH authentication

- Display pre-authentication banner (SSH-2 only)
- Bypass authentication entirely (SSH-2 only)

Authentication methods

- Attempt authentication using Pageant
- Attempt TIS or CryptoCard auth (SSH-1)
- Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

- Allow agent forwarding
- Allow attempted changes of username in SSH-2

Private key file for authentication:

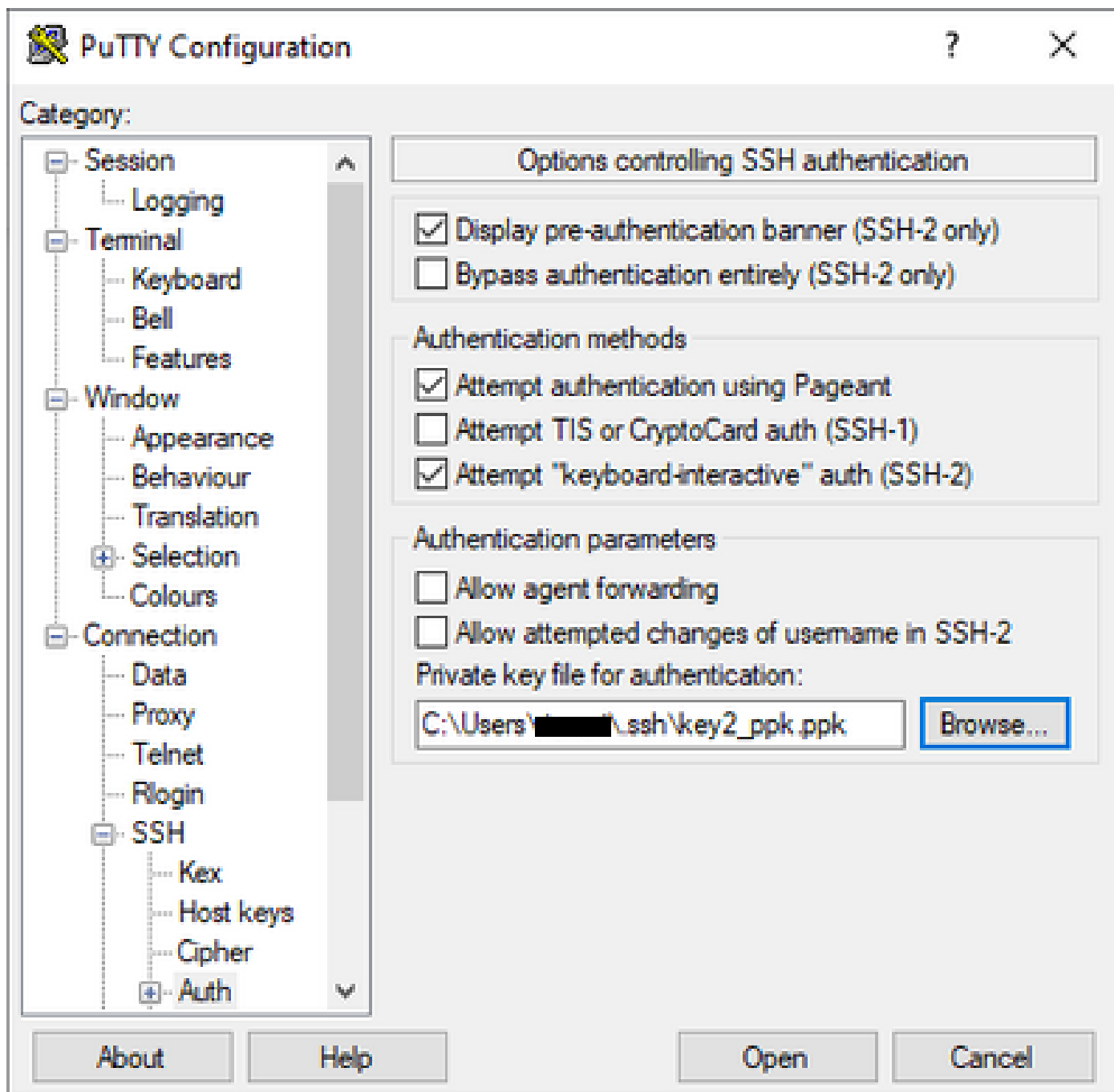
Browse...

About

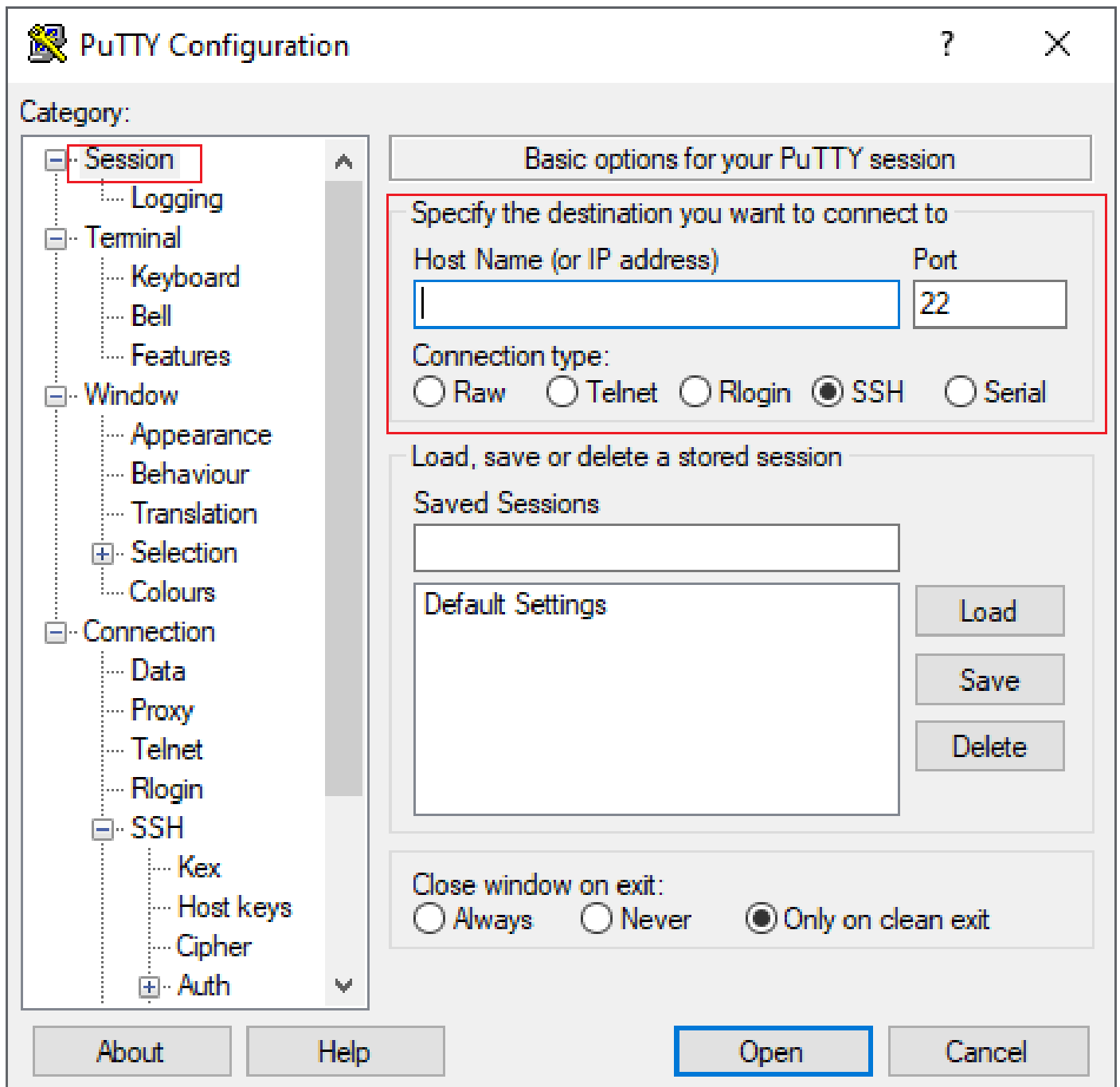
Help

Open

Cancel



選擇正確的金鑰後，返回主選單並使用CSR1000v例項的外部IP地址透過SSH進行連線，如圖所示。



 注意：系統將請求在生成的SSH金鑰中定義的使用者名稱/口令登入。

```
log in as: cisco
Authenticating with public key "imported-openssh-key"
Passphrase for key "imported-openssh-key":
```

```
csr-cisco#
```

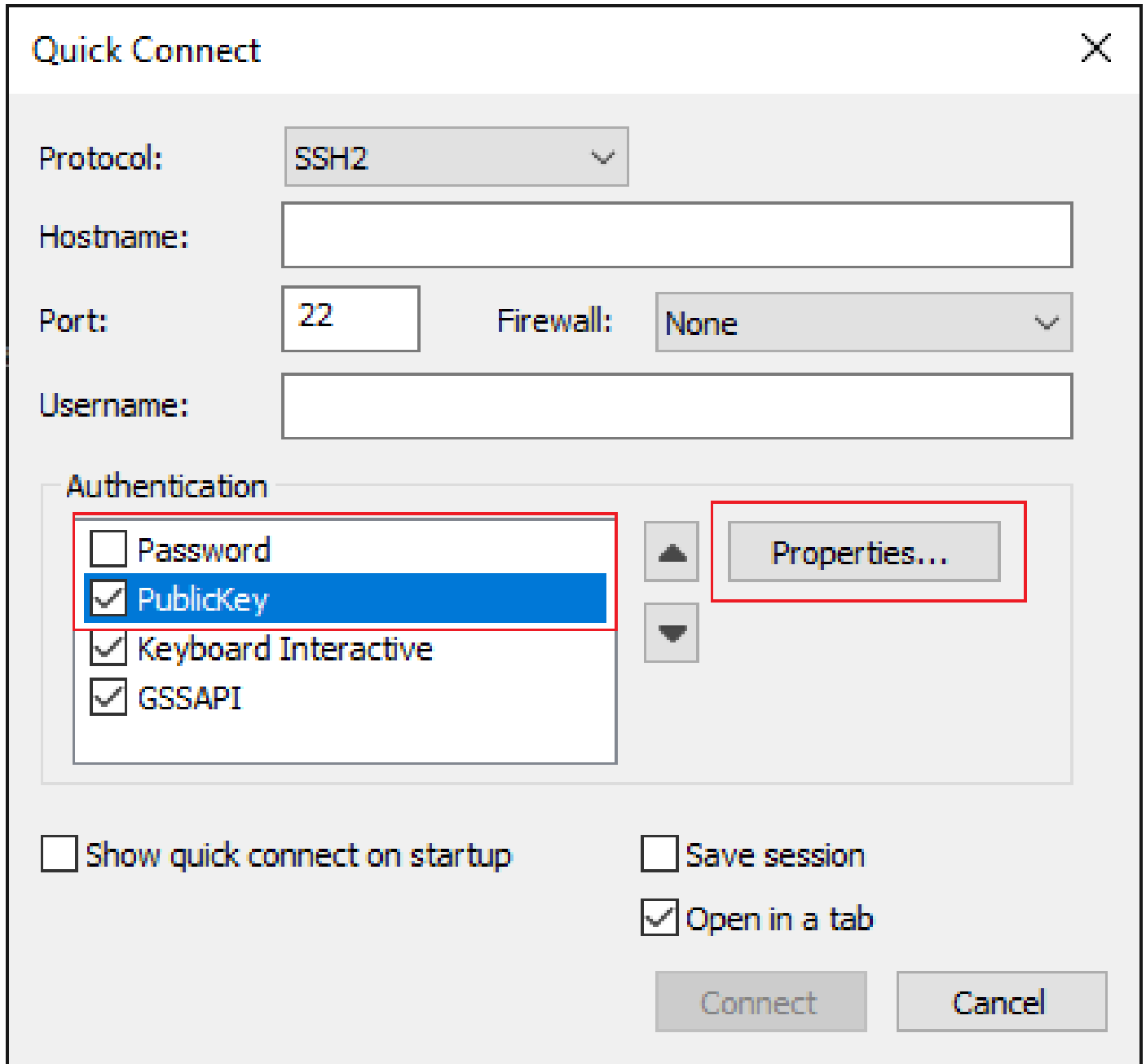
使用SecureCRT登入到CSR1000v/C8000V

SecureCRT需要PEM格式的私鑰，這是私鑰的預設格式。

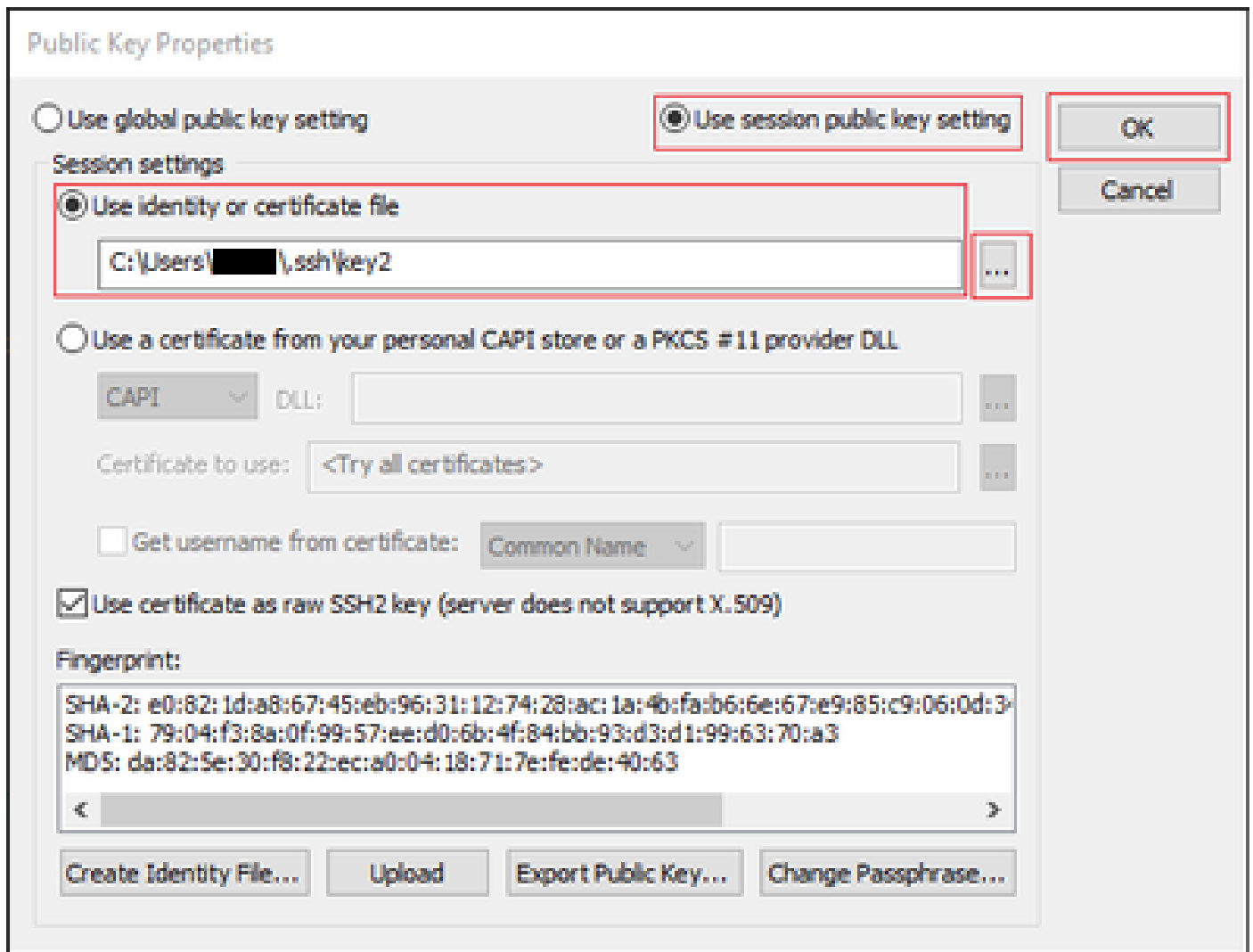
在SecureCRT中，指定功能表中私密金鑰的路徑：

「檔案」>「快速連線」>「身份驗證」>「取消選中密碼」>「公鑰」>「屬性」。

此影像顯示了預期的視窗：



選擇Use session public key string > Select Use identity or certificate file > Select ...按鈕>導航到目錄並選擇所需的金鑰>選擇OK (如圖所示)。



最後，透過SSH連線到例項地址的外部IP，如圖所示。

Quick Connect

Protocol: SSH2

Hostname: |

Port: 22 Firewall: None

Username:

Authentication

- PublicKey
- Keyboard Interactive
- GSSAPI
- Password

Show quick connect on startup Save session Open in a tab

Connect Cancel

 注意：系統將請求在生成的SSH金鑰中定義的使用者名稱/口令登入。

```
<#root>
```

```
csr-cisco#
```

```
show logging
```

```
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited, 0 flushes, 0 overruns, xml disabled)
```

```
No Active Message Discriminator.
```

```
<snip>
```

```
*Jan 7 23:16:13.315: %SEC_log in-5-log in_SUCCESS: log in Success [user: cisco] [Source: X.X.X.X] [local interface: GigabitEthernet0/0/0]  
csr-cisco#
```

其他VM登入方法

 註：請參閱[使用高級方法連線到Linux VM](#)文檔。

授權其他使用者登入GCP中的CSR1000v/C8000v

成功登入到CSR1000v例項後，可以使用以下方法配置其他使用者：

設定新的使用者名稱/密碼

使用以下命令配置新使用者和密碼：

```
<#root>
enable

configure terminal

username <username> privilege <privilege level> secret <password>

end
```

範例：

```
<#root>
csr-cisco#
configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
csr-cisco(config)#
csr-cisco(config)#
username cisco privilege 15 secret cisco

csr-cisco(config)#
end

csr-cisco#
```

新使用者現在能夠登入到CSR1000v/C8000v例項。

使用SSH金鑰配置新使用者

要訪問CSR1000v例項，請配置公鑰。例項後設資料中的SSH金鑰不提供對CSR1000v的訪問。

使用以下命令使用SSH金鑰配置新使用者：

```
<#root>
configure terminal

ip ssh pubkey-chain


username <username>

key-string

<public ssh key>

exit

end
```

 注意：Cisco CLI的最大行長度為254個字元，因此金鑰字串無法滿足此限制，因此可以方便地將金鑰字串換行以適合終端行。有關如何克服此限制的詳細資訊，請參閱[生成例項SSH金鑰以便在Google雲平台中部署CSR1000v](#)

```
<#root>
$
fold -b -w 72 /mnt/c/Users/ricneri/.ssh/key2.pub

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAD1dzZ/iJi3VeHs4qDoxOP67jebaGwC6vkC
n29bwSQ4CPJGVRLcVSNPcPPqVydiXVEOG8e9gFszkpk6c2me0+TRsSLiwhIgy28lyw5xhn1U
ck/AYpy9E6TyEEu9w6Fz0xTG2Qhe1n9b5Les6K9PFP/mR6WUMbfmaFredV/sADnODPO+OfTK
/OZPg34DNfcFhg1ja5GzudRb3S4nBBhDzuVrVC9RbA4PHVMXrLbIfq1ks3PCVG0tW1HxxTU4
FckmEAg4NEqMVLsm26nLvrNK6z71RMcIKZZcST+SL61Qv33gkUKIoGB9qx/+D1RvurVXFcdq
3Cmxm2swHmb6M1rEtqIv cisco
$

csr-cisco#
```

```
configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
csr-cisco(config)#
```

```
csr-cisco(config)#
```

```
ip ssh pubkey-chain
```

```
csr-cisco(conf-ssh-pubkey)#
```

```
username cisco
```

```
csr-cisco(conf-ssh-pubkey-user)#
```

```
key-string
```

```
csr-cisco(conf-ssh-pubkey-data)#
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDldzZ/iJi3VeHs4qDoxOP67jebaGwC
```

```
csr-cisco(conf-ssh-pubkey-data)#
```

```
6vkCn29bwsQ4CPJGVRLcVSNPcPPqVydiXVEOG8e9gFszkpk6c2meO+TRsSLiwHigv28l
```

```
csr-cisco(conf-ssh-pubkey-data)#
```

```
yw5xhn1Uck/AYpy9E6TyEEu9w6Fz0xTG2Qhe1n9b5Les6K9PFP/mR6WUMbfmaFredV/s
```

```
csr-cisco(conf-ssh-pubkey-data)#
```

```
ADnODPO+OfTK/OZPg34DNfcFhglja5GzudRb3S4nBBhDzuVrVC9RbA4PHVMXrLbIfqlk
```

```
csr-cisco(conf-ssh-pubkey-data)#
```

```
s3PCVG0tW1HxxTU4FckmEAg4NEqMVLsm26nLvrNK6z7lRMcIKZZcST+SL6lQv33gkUKI
```

```
csr-cisco(conf-ssh-pubkey-data)#
```

```
oGB9qx/+DlRvurVXfCdq3Cmxm2swHmb6MlrEtqIv cisco
```

```
csr-cisco(conf-ssh-pubkey-data)#
```

```
exit
```

```
csr-cisco(conf-ssh-pubkey-user)#
```

```
end
```

```
csr-cisco#
```

驗證登入至CSR1000v/C8000v的已配置使用者

為了確認配置設定正確，請使用建立的憑據或具有其他憑據的公鑰的私鑰對登入。

從路由器端，檢視包含終端IP地址的成功登入日誌。

```
<#root>
```

```
csr-cisco#
```

```
show clock
```

```
*00:21:56.975 UTC Fri Jan 8 2021
```

```
csr-cisco#
```

```
csr-cisco#
```

```
show logging
```

```
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited, 0 flushes, 0 overruns, xml disabled)
```

```
<snip>
```

```
*Jan 8 00:22:24.907: %SEC_log in-5-log in_SUCCESS: log in Success [user: <snip>] [Source: <snip>] [local interface: <snip>]  
csr-cisco#
```

疑難排解

如果顯示「作業逾時」錯誤訊息。

```
<#root>
```

```
$
```

```
ssh -i CSR-sshkey <snip>@X.X.X.X
```

```
ssh: connect to host <snip> port 22: Operation timed out
```

可能原因:

- 執行處理尚未完成部署。
- 公有地址不是分配給VM中nic0的地址。

解決方案：

等待虛擬機器部署完成。通常，CSR1000v部署最多需要5分鐘才能完成。

如果需要密碼

如果需要密碼：

```
<#root>
```

```
$
```

```
ssh -i CSR-sshkey <snip>@X.X.X.X
```

```
Password:
```

```
Password:
```

可能起因：

- 使用者名稱或私密金鑰不正確。
- 在MacOS或Linux等較新版本的Operating System上，OpenSSH實用程式預設情況下不啟用RSA。

解決方案：

- 確保使用者名稱與部署CSR1000v/C8000v時指定的使用者名稱相同。
- 確保私鑰與部署時包含金鑰相同。
- 在ssh命令中指定接受的金鑰型別：

```
<#root>
```

```
ssh -o PubkeyAcceptedKeyTypes=ssh-rsa -i <private_key> <user>@<host_ip>
```

相關資訊

- [Cisco Cloud Services Router 1000v資料表](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。