

# 調整Cisco IOS XE SD-WAN邊緣上的預設SSH RSA金鑰的大小

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[組態](#)

[驗證](#)

---

## 簡介

本文檔介紹如何在Cisco IOS® XE SD-WAN邊緣上將用於安全協定的預設SSH RSA金鑰增加到更長的長度。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- Cisco Catalyst軟體定義廣域網路(SD-WAN)
- SSH金鑰和證書基本操作
- RSA演算法

### 採用元件

- Cisco IOS® XE Catalyst SD-WAN邊緣17.9.4a

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

安全殼層(SSH)是一種網路協定，允許使用者建立到裝置的遠端連線，即使是在未受保護的網路上。該協定使用基於客戶端 — 伺服器架構的標準加密機制來保護會話。

RSA是Rivest、Shamir、Adleman :使用兩個金鑰的加密演算法 ( 公鑰加密系統 ) : 公鑰和私鑰，也稱為金鑰對。公有RSA金鑰是加密金鑰，私有RSA金鑰是解密金鑰。

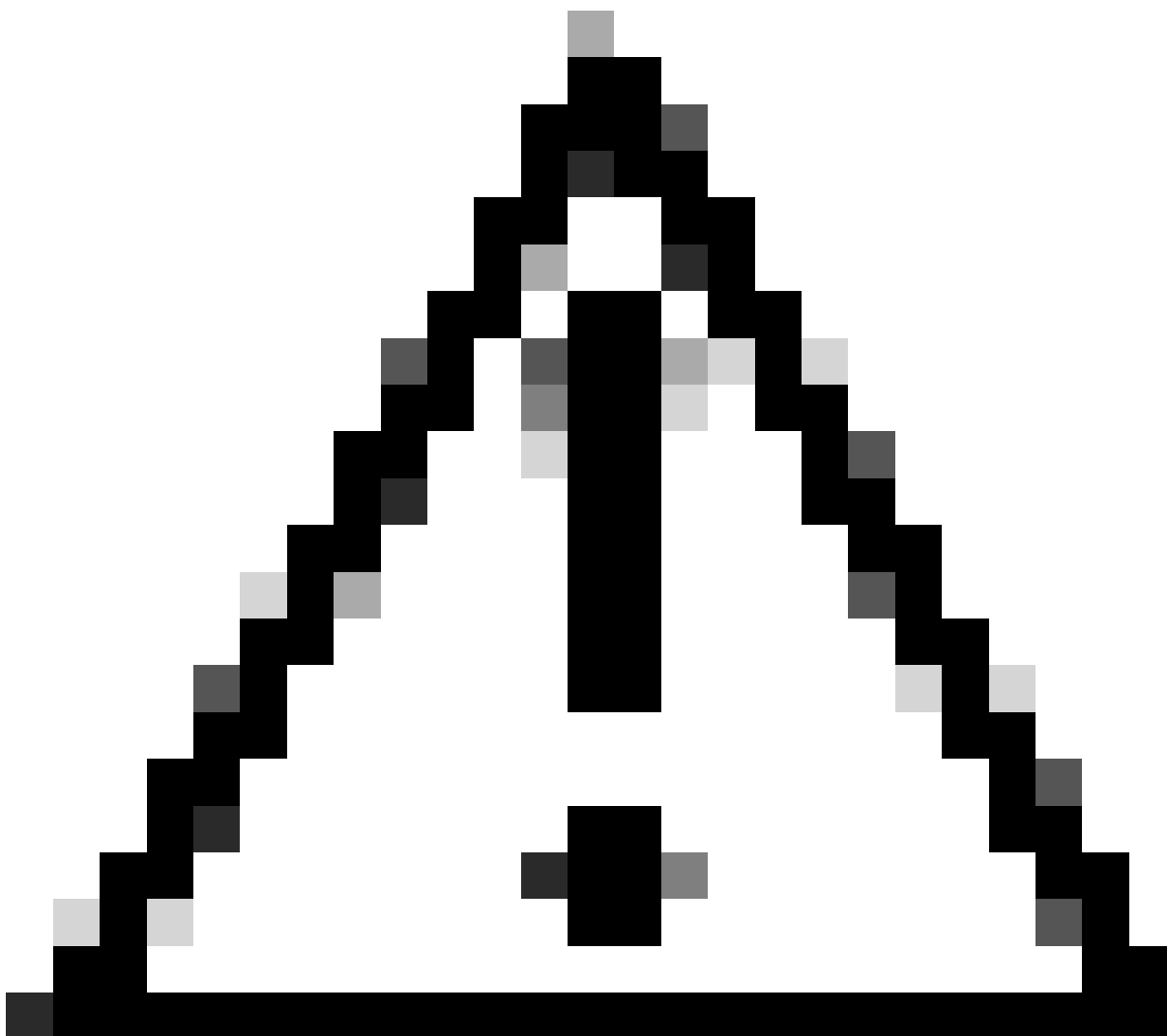
RSA金鑰具有定義的模數長度 ( 以位為單位 )。當一個RSA金鑰的長度為2048位時，它實際上意味著模數值介於22047和22048之間。由於給定對的公用金鑰和專用金鑰共用相同的模數，因此根據定義，它們也具有相同的長度。

信任點證書是自簽名的證書，因此命名信任點，因為它不依賴於任何其他方或其他方的信任。

Cisco IOS公開金鑰基礎架構(PKI)提供憑證管理，以支援IP安全(IPSec)、安全殼層(SSH)和安全通訊端層(SSL)等安全通訊協定。

SSH RSA金鑰在Cisco Catalyst SD-WAN上非常重要，因為SSH協定使用SSH金鑰在SD-WAN Manager和SD-WAN邊緣裝置之間建立通訊，因為SD-WAN Manager使用Netconf協定，通過SSH來管理、配置和監控裝置。

因此，必須始終同步和更新金鑰。如果通過合規性和稽核，需要修改金鑰長度以確保安全，則有必要完成本文檔中介紹的過程，以調整金鑰大小並在證書上正確同步金鑰，從而避免SD-WAN Manager和SD-WAN Edge裝置之間斷開連線。

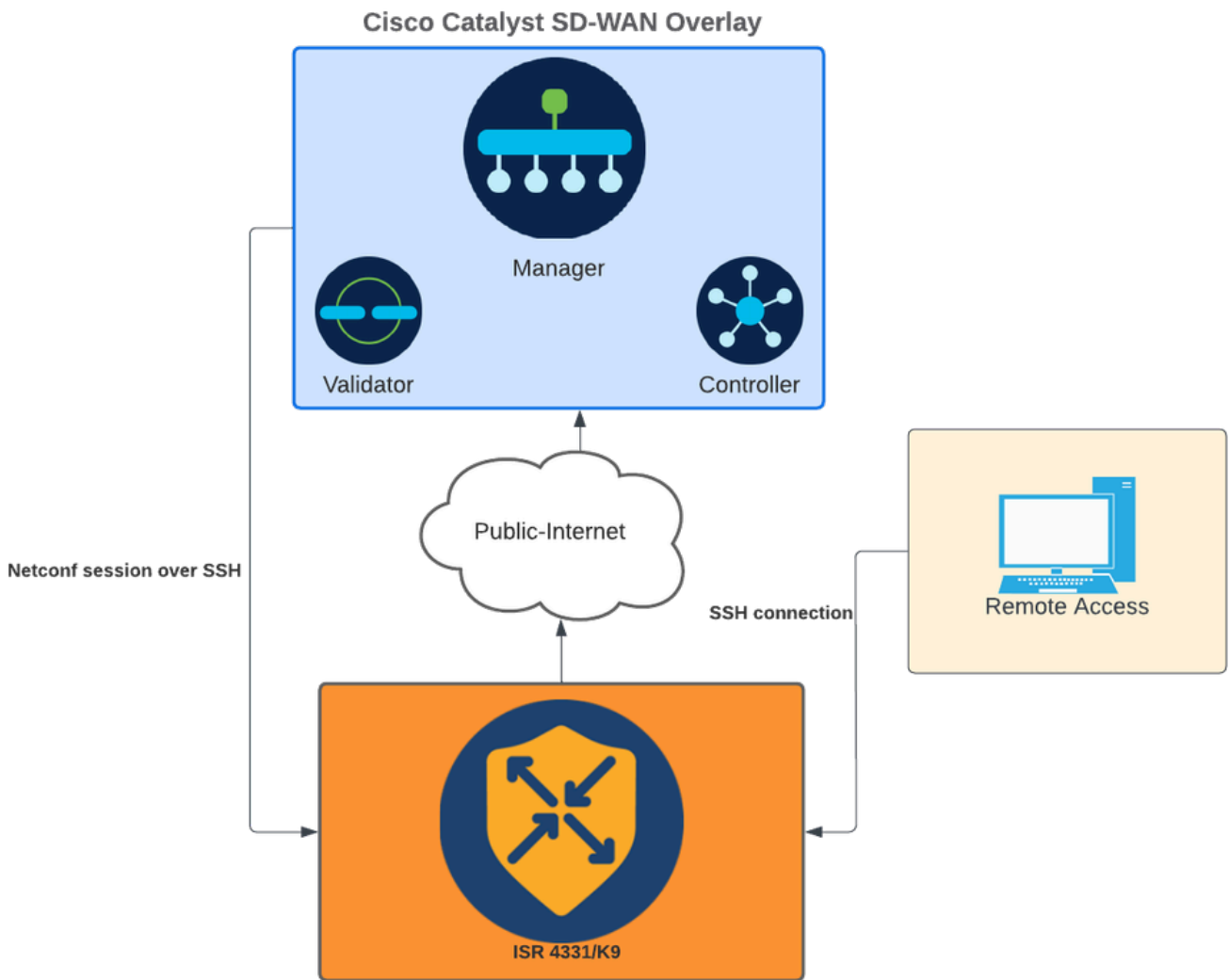


注意：請完成該過程中的所有步驟，以避免丟失對裝置的訪問許可權。如果裝置處於生產狀態，建議在維護視窗中執行，並讓控制檯訪問裝置。

---

## 設定

### 網路圖表



網路圖表

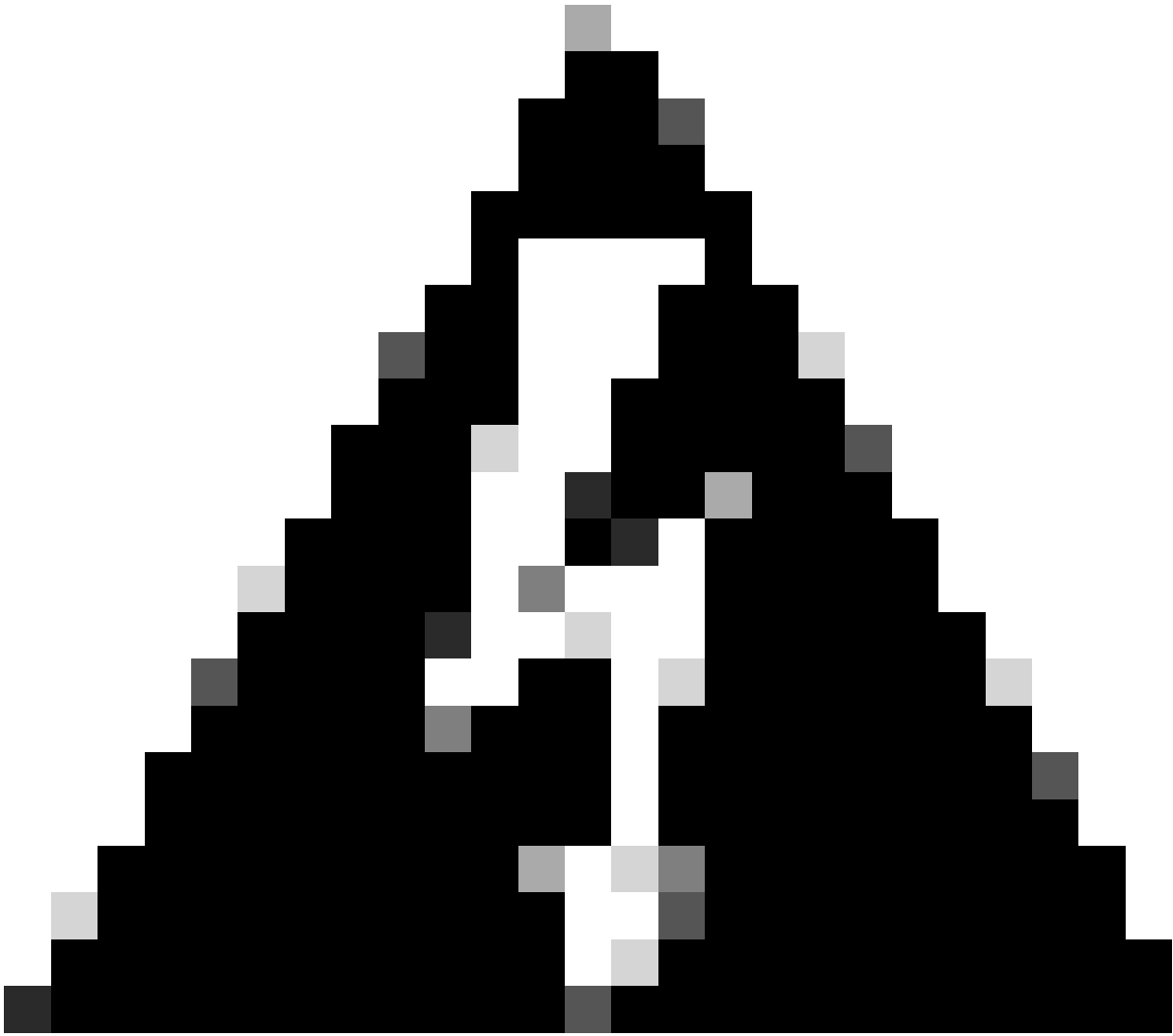
## 組態

WAN邊緣裝置中的RSA金鑰只能使用命令列介面(CLI)進行修改；不能使用CLI附加功能模板來更新金鑰。



警告：建議使用控制檯完成此過程，因為SD-WAN Manager SSH工具在該過程完成之前不可用。

---



警告：此過程需要重新啟動裝置。如果裝置處於生產狀態，建議在維護視窗中執行，並讓控制檯訪問裝置。如果沒有控制檯訪問，將另一個遠端訪問協定臨時配置為telnet。

---

此配置示例說明如何刪除RSA 2048和使用RSA 4096金鑰。

1 — 獲取當前的SSH金鑰名稱。

```
<#root>
```

```
Device#
```

```
show ip ssh
```

```
SSH Enabled - version 2.0
```

```
Authentication methods:publickey,keyboard-interactive,password
```

```
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecds
```

```
Hostkey Algorithms:x509v3-ssh-rsa,rsa-sha2-512,rsa-sha2-256,ssh-rsa
```

```
Encryption Algorithms:aes128-gcm,aes256-gcm,aes128-ctr,aes192-ctr,aes256-ctr
```

```
MAC Algorithms:hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512,
```

KEX Algorithms:ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha1  
Authentication timeout: 120 secs; Authentication retries: 3  
Minimum expected Diffie Hellman key size : 2048 bits  
IOS Keys in SECSH format(ssh-rsa, base64 encoded):

TP-self-signed-1072201169 <<<< RSA Key Name

Modulus Size : 2048 bits

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAZ5urq7f/X+AZJjUnM0dF9pLX+V0jPR8arK6bLSU7d
iGeSDDwW2MPNck/U5HBry9P/L4nKyZ1oEvAhfy7cJVvmoHD41NQW9wb/hLtimuujnRRYkKuIWLmoI7AH
y6YQoetew8XVg1VIjva+JzQ5ZX1JGm8AzN6a95RbRNhGRzgz9cTFmD7m6ArIKZPMYQabXfrY+m/HuQ2
aytbHtJMgm0Qk2fLPak03PnQNYXpiDP3Cm0Eh3LJg82FZQ1eohmhm+mAIwU4m1LHUouigyBuq1KEBVe
z3vxjB9X8rGF3qzUcx21pHmhXaNpXWen2QQbyfAIDo8WXVoff24uLY1wCVkv
```

## 2 — 獲取當前信任點自簽名證書。

<#root>

Device#

```
show crypto pki trustpoint
```

Trustpoint TP-self-signed-1072201169: <<<< Self-signed Trustpoint name

Subject Name:

cn=IOS-Self-Signed-Certificate-1072201169

Serial Number (hex): 01

Persistent self-signed certificate trust point

Using key label

TP-self-signed-1072201169

兩個value-name必須匹配。

## 3 — 刪除當前金鑰。

<#root>

Device#

```
crypto key zeroize rsa
```

#### 4 — 驗證舊金鑰是否已成功刪除。

```
<#root>  
Device#  
show ip ssh
```

#### 5 — 生成新金鑰。

```
<#root>  
Device#  
crypto key generate rsa modulus 4096 label
```

```
The name for the keys will be: TP-self-signed-1072201169  
% The key modulus size is 4096 bits  
% Generating crypto RSA keys in background ...  
*Jun 25 21:35:18.919: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-1072201169 has been generated  
*Jun 25 21:35:18.924: %SSH-5-ENABLED: SSH 2.0 has been enabled  
*Jun 25 21:35:23.205: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-1072201169 has been generated  
*Jun 25 21:35:29.674: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private config file
```

完成此過程可能需要2到5分鐘。

#### 6 — 驗證生成的新金鑰。

```
<#root>  
Device#  
show ip ssh
```

```
SSH Enabled - version 2.0  
Authentication methods:publickey,keyboard-interactive,password  
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521  
Hostkey Algorithms:x509v3-ssh-rsa,rsa-sha2-512,rsa-sha2-256,ssh-rsa  
Encryption Algorithms:aes128-gcm,aes256-gcm,aes128-ctr,aes192-ctr,aes256-ctr  
MAC Algorithms:hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha2-512-etm@openssh.com  
KEX Algorithms:ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha1  
Authentication timeout: 120 secs; Authentication retries: 3  
Minimum expected Diffie Hellman key size : 2048 bits  
  
IOS Keys in SECSH format(ssh-rsa, base64 encoded): TP-self-signed-1072201169
```



Modulus Size : 4096 bits <<<< Key Size

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQDE0t/SX3oQKN6z0Wv0aFAkMcaZNzQ6JgP+7xjuX143
YS7YGmOPwIPgs8N2LWvmdLXQ/PqsQOGGsdxo2+2Y/idAFm808mb6bcWfU+t3b/Pf6GBzUv8SPnR4i4nN
5GYhZE9HX3REWYp7d+7l1YawrDzpJ6d8RgUWLOtgHSzQ7P796c0B1YLtK3eF00H1AFmFy5ec8Own7ik0
JjKtwEozImFMjHZfUEUjFuhPJELB06yYEipPMMRaZYFfTRbNjM8/7S0JG1FkgFVW5nITTIgISoMV8EJv
bLl8cVgATDb10ckeDb7uU6PDXm3zonmZC0yqHtF10A0JxUpUa6Iry1XwMzzZqDdu32F5If4/SSCmbHV2
46P8AjCdu/2TKK5et0049UH0y0bMgPuWrJpwtk1iYA3+t6N/Qd1C5VSoua+TsMfp7Dh3k6qUTFUSy2h3
Kiibov1HKYvkcqXi6nDfAKb8o+Z8/43xbvWlDIKAuj1rbdyqPAJB411TZJk0Hk8zRP5gZ8u4jtjNKQHb
vNa3ieg4RLED0x41qCk+iSRzdddMq2te1xSWFPh67i4BnJHvhVnR6LF5Gu+uF5TWwcpy2MMOu14YDJYr
D+jnyoZr4PnfwAgk4M9U89deWS1IRPMIXYd35YmLvD60eQ5EQALNiNPUEkpdPKs4orYysEV0pRoY+HQ
```

現在，將生成新金鑰。但是，在刪除舊金鑰時，Netconf會話正在使用的自簽名證書也會從信任點刪除。

```
<#root>
```

```
Device#
```

```
sh crypto pki trustpoint status
```


```
Trustpoint TP-self-signed-1072201169:
Issuing CA certificate configured::
Issuing CA certificate configured:
Subject Name:
cn=Cisco Licensing Root CA,o=Cisco
Fingerprint MD5: 1468DC18 250BDFCF 769C29DF E1F7E5A8
Fingerprint SHA1: 5CA95FB6 E2980EC1 5AFB681B BB7E62B5 AD3FA8B8
State:
```

```
Keys generated ..... No <<<< Depending on the version, it can erase the key or even that, delete
```

```
Issuing CA authenticated ..... Yes
Certificate request(s) ..... None
```

一旦生成新的4096金鑰，將不會在自簽名證書上自動更新金鑰，並且必須完成額外的步驟才能更新金鑰。

---

 附註：如果僅生成金鑰但未在證書中更新，則SD-WAN Manager會丟失Netconf會話，這可能會中斷裝置的所有管理活動（模板、配置等）。

---

產生憑證/分配金鑰的方式有兩種：

1 — 重新載入裝置。

```
<#root>
```

```
Device#
```

```
reload
```

2 — 重新啟動HTTP secure-server。僅當裝置處於CLI模式時，此選項才可用。

```
<#root>
```

```
Device (config)#
```

```
no ip http secure-server
```

```
Device (config)#
```

```
commit
```

```
Device (config)#
```

```
ip http secure-server
```

```
Device (config)#
```

```
commit
```

## 驗證

重新載入後，驗證是否已產生新金鑰，以及憑證是否位於具有相同名稱的信任點下。

```
<#root>
```

```
Device#
```

```
show ip ssh
```

```
SSH Enabled - version 2.0
```

```
Authentication methods:publickey,keyboard-interactive,password
```

```
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecds
```

```
Hostkey Algorithms:x509v3-ssh-rsa,rsa-sha2-512,rsa-sha2-256,ssh-rsa
```

```
Encryption Algorithms:aes128-gcm,aes256-gcm,aes128-ctr,aes192-ctr,aes256-ctr
```

```
MAC Algorithms:hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512,
```

```
KEX Algorithms:ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha1
```

```
Authentication timeout: 120 secs; Authentication retries: 3
```

```
Minimum expected Diffie Hellman key size : 2048 bits
```

```
IOS Keys in SECSH format(ssh-rsa, base64 encoded): TP-self-signed-1072201169
```

```
Modulus Size : 4096 bits
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQDE0t/SX3oQKN6z0Wv0aFAkMcaZNzQ6JgP+7xjuX143  
YS7YGmOPwIPgs8N2LWvmdLXQ/PqsQOGGsdxo2+2Y/idAFm808mb6bcWFU+t3b/Pf6GBzUv8SPnR4i4nN  
5GYhZE9HX3REWYp7d+711YawrDzpJ6d8RgUWL0tgHSzQ7P796c0B1YLtK3eF00H1AFmFy5ec80wn7ik0
```

JjKtwEozImFMjHZfUEUjFuhPJELB06yYEipPWMRaZYFfTRbNJm8/7S0JG1FkgFW5nITTIgISoMV8EJv  
bL18cVgATDb10ckeDb7uU6PDXm3zonmZC0yqHtF10A0JxUpUa6Iry1XwMzzZqDdu32F5If4/SSCmbHV2  
46P8AjCdu/2TKK5et0049UH0y0bMgPuWrJpwtk1iYA3+t6N/Qd1C5VSoua+Tsmfp7Dh3k6qUTFUSy2h3  
Kiibov1HKyvkcqXi6nDfAKb8o+Z8/43xbvW1DIKAuj1rbdyqPAJB411TZJk0Hk8zRP5gZ8u4jtjNKQHb  
vNa3ieg4RLED0x41qCk+iSRzdddMq2te1xSWFPh67i4BnJHvhVnR6LF5Gu+uF5TWwcpy2MMOu14YDJYr  
D+jnyoZr4PnfwAgk4M9U89deWS1IRPMIXYd35YmLvD60eQ5EQALNiNPUEkpdPKs4orYysEV0pRoY+HQ

<#root>

Device#

```
show crypto pki trustpoint
```

```
Trustpoint TP-self-signed-1072201169: <<<< Trustpoint name
```

Subject Name:

cn=IOS-Self-Signed-Certificate-1072201169

Serial Number (hex): 01

Persistent self-signed certificate trust point

Using key label TP-self-signed-107220116

<#root>

Device#

```
show crypto pki certificates
```

Router Self-Signed Certificate

Status: Available

Certificate Serial Number (hex): 01

Certificate Usage: General Purpose

Issuer:

cn=IOS-Self-Signed-Certificate-1072201169

Subject:

Name: IOS-Self-Signed-Certificate-1072201169

cn=IOS-Self-Signed-Certificate-1072201169

Validity Date:

start date: 21:07:33 UTC Dec 27 2023

end date: 21:07:33 UTC Dec 26 2033

Associated Trustpoints: TP-self-signed-1072201169

Storage: nvram:IOS-Self-Sig#4.cer

確認SD-WAN Manager可以將配置更改應用到裝置路由器。

## 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）。