

# 將UCS伺服器證書配置為CIMC

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[產生CSR](#)

[建立自簽名證書](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

---

## 簡介

本文說明如何產生憑證簽署請求(CSR)以取得新憑證。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 您必須以具有管理員許可權的使用者身份登入才能配置證書。
- 確保CIMC時間設定為當前時間。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- CIMC 1.0或更高版本
- Openssl

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

可將證書上傳到思科整合管理控制器(CIMC)以替換當前伺服器證書。伺服器憑證可以由公用憑證授權單位(CA)（例如Verisign）簽署，或由您自己的憑證授權單位簽署。產生的憑證金鑰長度為

2048位元。

## 設定

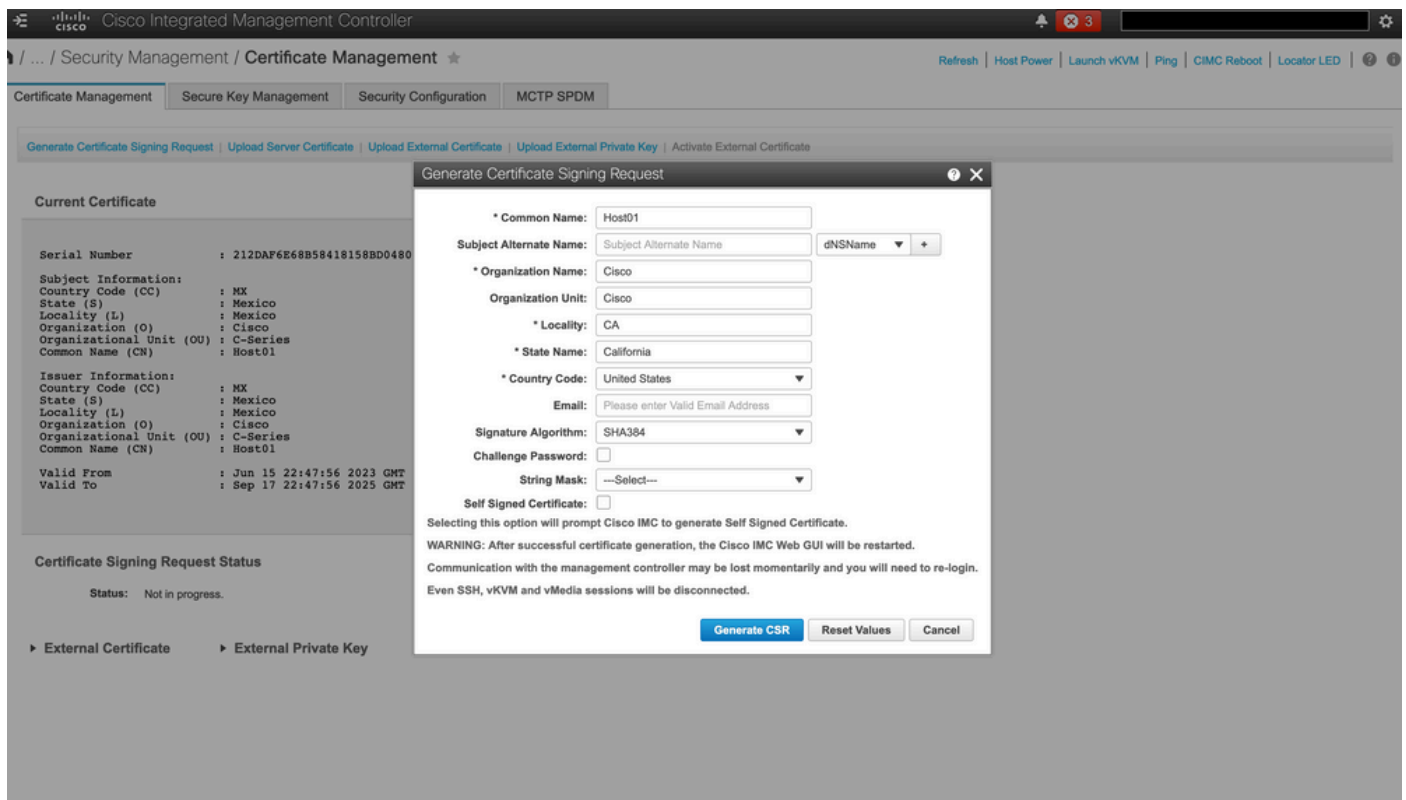
步驟 1.	從CIMC生成CSR。
步驟 2.	將CSR檔案提交給CA以簽署證書。如果您的組織生成自己的自簽名證書，則可以使用CSR檔案生成自簽名證書。
步驟 3.	將新證書上傳到CIMC。

 注意：上傳的證書必須從CIMC生成的CSR中建立。請勿上傳不是由此方法建立的憑證。

## 產生CSR

導航到管理頁籤 > 安全管理 > 證書管理 > 生成證書簽名請求 (CSR)，然後填寫以\*標籤的詳細資訊。


此外，請參閱[生成證書簽名請求指南](#)。



The screenshot shows the Cisco Integrated Management Controller (CIMC) web interface. The main page is titled 'Certificate Management' and includes tabs for 'Secure Key Management', 'Security Configuration', and 'MCTP SPDM'. A modal dialog box titled 'Generate Certificate Signing Request' is open, displaying the following fields and options:

- \* Common Name: Host01
- Subject Alternate Name: Subject Alternate Name (with a dropdown for dNSName)
- \* Organization Name: Cisco
- Organization Unit: Cisco
- \* Locality: CA
- \* State Name: California
- \* Country Code: United States (dropdown)
- Email: Please enter Valid Email Address
- Signature Algorithm: SHA384 (dropdown)
- Challenge Password: (empty field)
- String Mask: ---Select---
- Self Signed Certificate:

Below the form, a warning message is displayed: "WARNING: After successful certificate generation, the Cisco IMC Web GUI will be restarted. Communication with the management controller may be lost momentarily and you will need to re-login. Even SSH, vKVM and vMedia sessions will be disconnected." At the bottom of the dialog are buttons for 'Generate CSR', 'Reset Values', and 'Cancel'.


 注意：請使用主體替代名稱指定此伺服器的其他主機名稱。未配置dNSName或將其從上傳的證書中排除，可能會導致瀏覽器阻止對Cisco IMC介面的訪問。

下一步要做什麼？

執行下列工作：

- 如果您不想從公共證書頒發機構獲取證書，並且您的組織不運行自己的證書頒發機構，則可以允許CIMC從CSR內部生成自簽名證書並立即將其上傳到伺服器。選中 Self Signed Certificate框以執行此任務。
- 如果您的組織操作自己的自簽名證書，請複製-----BEGIN ...to END CERTIFICATE REQUEST-----的命令輸出並貼上到名為csr.txt的檔案。將CSR檔案輸入到證書伺服器以生成自簽名證書。
- 如果您從公共證書頒發機構獲取證書，請將-----BEGIN ... to END CERTIFICATE REQUEST-----的命令輸出複製到名為csr.txt的檔案中。將CSR檔案提交到證書頒發機構以獲取簽名證書。確保證書屬於伺服器型別。

---

 注意：成功生成證書後，Cisco IMC Web GUI將重新啟動。與管理控制器的通訊可能會暫時遺失，需要重新登入。

---

如果您沒有使用第一個選項(其中CIMC在內部生成並上傳自簽名證書)，則必須建立新的自簽名證書並將其上傳到CIMC。

## 建立自簽名證書

作為公共CA和簽署伺服器證書的替代方案，請運行您自己的CA並簽署您自己的證書。本節介紹用於建立CA和使用OpenSSL伺服器證書生成伺服器證書的命令。有關OpenSSL的詳細資訊，請參閱[OpenSSL](#)。

步驟 1.生成RSA私鑰，如圖所示。

```
<#root>
[root@redhat ~]#
openssl genrsa -out ca.key 1024
```

步驟 2.如圖所示，生成新的自簽名證書。

```
<#root>
[root@redhat ~]#
openssl req -new -x509 -days 1095 -key ca.key -out ca.crt
```

You are about to be asked to enter information that will be incorporated into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [XX]:

US

State or Province Name (full name) []:

California

Locality Name (eg, city) [Default City]:

California

Organization Name (eg, company) [Default Company Ltd]:

Cisco

Organizational Unit Name (eg, section) []:

Cisco

Common Name (eg, your name or your server's hostname) []:

Host01

Email Address []:

[root@redhat ~]#

步驟 3. 確保證書型別為「server」，如圖所示。

```
<#root>
```

```
[root@redhat ~]#
```

```
echo "nsCertType = server" > openssl.conf
```

步驟 4. 指示CA使用您的CSR檔案生成伺服器證書，如圖所示。

```
<#root>
```

```
[root@redhat ~]#
```

```
openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 01 -CAkey ca.key -out server.crt -extfile
```

步驟 5. 驗證產生的憑證的型別是否為Server，如下圖所示。

<#root>

[root@redhat ~]#

openssl x509 -in server.crt -purpose

Certificate purposes:

SSL client : No

SSL client CA : No

SSL server :

Yes

SSL server CA : No

Netscape SSL server : Yes

Netscape SSL server CA : No

S/MIME signing : No

S/MIME signing CA : No

S/MIME encryption : No

S/MIME encryption CA : No

CRL signing : Yes

CRL signing CA : No

Any Purpose : Yes

Any Purpose CA : Yes

OCSP helper : Yes

OCSP helper CA : No

Time Stamp signing : No

Time Stamp signing CA : No

-----BEGIN CERTIFICATE-----

```
MIIDFzCCAoCgAwIBAgIBATANBgkqhkiG9w0BAQsFADBoMQswCQYDVQQGEwJVUzET
MBEGA1UECAwKQ2FsaWZvcn5pYTETMBEGA1UEBwwKQ2FsaWZvcn5pYTEOMAwGA1UE
CgwFQ2IzY28xDjAMBGNVBA5MBUNpc2NvMQ8wDQYDVQQDDAIZb3NOMDEwHhcNMjMw
NjI3MjI0NDU1WjBGMQswCQYDVQQGEwJVUzETMBEGA1UE
CAwKQ2FsaWZvcn5pYTELMakGA1UEBwwCQ0ExDjAMBGNVBAoMBUNpc2NvMQ4wDAYD
VQQLDAVDaXNjbzEPMAOGA1UEAwwGSG9zdDAxMIIBIjANBgkqhkiG9w0BAQEFAAOCC
AQ8AMIIBCgKCAQEAuhJ50V004MZNv3dgQw0Mns9sgzZwjJS8Lv0tHt+GA4uzNf1Z
WKNyZbzD/yLoXiV8ZFgawJbqEe2yijVzEcguZQTGFRkAWmDeckM9Fieob03B5Fnt
pC8M9Dfb3YmkIx29abrZKFEIrybabbG4gQyFzG0B6D9CK1WuoEzsE7zH0oJX4Bcy
ISE0RsOd9bsXvxyLk2cauS/zvI9hvrwW9P/Og8nF3Y+PGtm/bnfodEnNFWPLtvF
dGuG5/wBmmMbEb/GbrH9uVcy0z+3HReDcQ+kJde7PoFK3d6Z0dkh7Mmtjpvk5ucQ
NgzaeoCDL0Bn+Zl0800/eciScsGIJKxYD/FYlQIDAQABo1UwUzARBglghkgBhvhC
AQEEBAMCBkAwHQYDVRO0BBYEFJ20TeuP27jyCJRiAKKfflNc0hbMB8GA1UdIwQY
MBaAFA4QR965FinE4GrhkiwRV62ziPj/MA0GCSqGSIb3DQEBwUAA4GBAJuL/Bej
DxenfCt6pBA709GtktwUS/rEtpQX190hdlahjwbFG/67MYIpIEbidL1BCw55dal
LI7sgu1dnItnIGsJI1L7h6IEFBu/coCvBtopOYUanaBJ1BgxBWhT2FAnmB9wIvYJ
5rMx95vWZxt3KGE8Q1P+eGkMAHWA8M0yhwHa
```

-----END CERTIFICATE-----

[root@redhat ~]#

步驟 6.上傳伺服器憑證，如圖所示。

Cisco Integrated Management Controller

External Certificate uploaded successfully

admin@

Refresh | Host Power | Launch vKVM | Ping | CIMC Reboot | Locator LED

Certificate Management | Secure Key Management | Security Configuration

Generate Certificate Signing Request | Upload Server Certificate | Upload External Certificate | Upload External Private Key | Activate External Certificate

**Current Certificate**

```
Serial Number      : 212DAF6E68B58418158BD04804D64B2C5EE08B6B
Subject Information:
Country Code (CC)  : MX
State (S)          : Mexico
Locality (L)       : Mexico
Organization (O)   : Cisco
Organizational Unit (OU) : C-Series
Common Name (CN)   : Host01
Issuer Information:
Country Code (CC)  : MX
State (S)          : Mexico
Locality (L)       : Mexico
Organization (O)   : Cisco
Organizational Unit (OU) : C-Series
Common Name (CN)   : Host01
Valid From         : Jun 15 22:47:56 2023 GMT
Valid To           : Sep 17 22:47:56 2025 GMT
```

**Certificate Signing Request Status**

Status: Not in progress.

External Certificate | External Private Key

## 驗證

使用本節內容，確認您的組態是否正常運作。

導航到管理>證書管理，驗證當前證書，如圖所示。

Cisco Integrated Management Controller

admin@

Refresh | Host Power | Launch vKVM | Ping | CIMC Reboot | Locator LED

Certificate Management | Secure Key Management | Security Configuration | MCTP SPDM

Generate Certificate Signing Request | Upload Server Certificate | Upload External Certificate | Upload External Private Key | Activate External Certificate

**Current Certificate**

```
Serial Number      : 01
Subject Information:
Country Code (CC)  : US
State (S)          : California
Locality (L)       : CA
Organization (O)   : Cisco
Organizational Unit (OU) : Cisco
Common Name (CN)   : Host01
Issuer Information:
Country Code (CC)  : US
State (S)          : California
Locality (L)       : California
Organization (O)   : Cisco
Organizational Unit (OU) : Cisco
Common Name (CN)   : Host01
Valid From         : Jun 27 22:44:15 2023 GMT
Valid To           : Jun 26 22:44:15 2024 GMT
```

**Certificate Signing Request Status**

Status: Not in progress.

External Certificate | External Private Key

## 疑難排解

目前沒有特定資訊可用於對此組態進行疑難排解。

## 相關資訊

- [思科漏洞ID CSCup26248](#) -無法將第三方CA SSL憑證上傳到CIMC 2.0。(1a)
- [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）。