

產生第三方憑證的 CSR，並將鏈結的憑證下載到 WLC

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[鏈結憑證](#)

[支援鏈結憑證](#)

[憑證級別](#)

[步驟 1.產生CSR](#)

[選項 A：具有 OpenSSL 的 CSR](#)

[選項 B：WLC 產生的 CSR](#)

[步驟 2.簽署憑證](#)

[選項A：從您的企業CA取得Final.pem檔案](#)

[選項B：從第三方CA取得Final.pem檔案](#)

[步驟 3：CLI。使用 CLI 將第三方憑證下載到 WLC](#)

[步驟 3：GUI。使用 GUI 將第三方憑證下載到 WLC](#)

[疑難排解](#)

[高可用性 \(HA SSO\) 注意事項](#)

[相關資訊](#)

簡介

本檔案介紹如何在AireOS WLC上產生和匯入憑證。

必要條件

需求

思科建議您瞭解以下主題：

- [如何設定 WLC、輕型存取點 \(LAP\) 和無線用戶端卡以達成基本操作.](#)
- [如何使用 OpenSSL 應用程式.](#)
- [公開金鑰基礎架構和數位憑證](#)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 5508 WLC (執行韌體版本 8.3.102)
- 適用於 Microsoft Windows 的 OpenSSL 應用程式
- 第三方憑證授權單位 (CA) 特定的註冊工具

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。

鏈結憑證

憑證鏈結是一系列憑證，鏈結中的每個憑證皆由後續的憑證簽署。

憑證鏈結旨在建立一條從對等憑證到受信任 CA 憑證的信任鏈。CA在簽署對等憑證時擔保其身分。

如果CA是您信任的CA (若您的根憑證目錄中存在CA憑證的副本，即可得知)，這代表您也可以信任簽署的對等憑證。

通常，用戶端並不接受憑證，因為這些憑證不是是由已知的 CA 建立的。用戶端通常會指出無法驗證憑證的有效性。

如果憑證是由中間 CA 簽署，而中間 CA 並不為用戶端瀏覽器所知，就會發生這種情況。在這種情況下，必須使用鏈結的 SSL 憑證或憑證群組。

支援鏈結憑證

控制器允許將設備憑證以鏈結憑證方式下載，以用於 Web 驗證。

憑證級別

- 第 0 級：僅使用 WLC 上的伺服器憑證
- 第 1 級：使用 WLC 上的伺服器憑證和 CA 根憑證
- 第 2 級：使用 WLC 上的伺服器憑證、一組單一 CA 中間憑證和 CA 根憑證
- 第 3 級：使用 WLC 上的伺服器憑證、兩組單一 CA 中間憑證和 CA 根憑證

WLC 不支援 WLC 上大小超過 10KB 的鏈結憑證。但是，WLC 版本 7.0.230.0 和更新版本已移除此限制。




注意：現已支援鏈結憑證，且Web驗證和Web管理實際上需要使用鏈結憑證。



注意：本地EAP、管理或Web驗證完全支援萬用字元憑證

Web 驗證憑證可以是以下任一形式：

- 鏈接
- 未鏈結
- 自動產生

 註：在WLC版本7.6和更新版本中，僅支援鏈結憑證（因此必須使用）


若要出於管理目的，產生未鏈結的憑證，本檔案將忽略憑證與CA憑證合併的相關部分。

本文探討如何正確地將鏈結的安全通訊端層 (SSL) 憑證安裝到 WLC。

步驟 1. 產生CSR

產生 CSR 的方式有兩種：手動使用OpenSSL（8.3版之前的WLC軟體中唯一可行的方式）或前往WLC本身產生CSR（8.3.102後可用）。


選項 A：具有 OpenSSL 的 CSR

 注意:Chrome版本58和更新版本不單獨信任證書的公用名，並且要求同時存在使用者替代名稱。下一節說明如何將SAN欄位新增到OpenSSL CSR（此瀏覽器的一項新要求）。

完成以下步驟，以便使用 OpenSSL 產生 CSR：

1. 安裝並開啟 [OpenSSL](#)。 

在Microsoft Windows中，openssl.exe預設位於 C:\> openssl > bin.

 注意：OpenSSL版本0.9.8是建議舊版WLC使用的版本；但是，自版本7.5起，還新增對於OpenSSL版本1.0的支援(請參閱思科錯誤ID [CSCti65315](#) — 需要對於使用OpenSSL v1.0產生的憑證的支援)，而且是建議使用的版本。OpenSSL 1.1有關作業也經過測試，在WLC 8.x和更新版本中有效。

2. 找到您的 OpenSSL 設定檔並複製，以便針對此 CSR 編輯該檔案。編輯副本以新增以下部分：

- 3.

```
<#root>
```

```
[req]
```

```
req_extensions = v3_req
```

```
[ v3_req ]
```

```
# Extensions to add to a certificate request
```

```
basicConstraints = CA:FALSE
```

```
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
```

```
subjectAltName = @alt_names
```

```
[alt_names]
```

```
DNS.1 = server1.example.com
```

```
DNS.2 = mail.example.com
DNS.3 = www.example.com
DNS.4 = www.sub.example.com
DNS.5 = mx.example.com
DNS.6 = support.example.com
```


以「DNS. 1」、「DNS. 2」(依此類推)開頭的行必須包含您憑證的所有替代名稱。然後寫入用於WLC的任何可能的URL。上例中粗體行不存在，或者在我們的實驗室openSSL版本中進行了註釋。視作業系統和openssl版本而定。我們將修改後的配置版本儲存為 `openssl-san.cnf` 例如。

4. 輸入以下命令可產生新的CSR:

```
<#root>
OpenSSL>
req -new -newkey rsa:3072 -nodes -keyout mykey.pem -out myreq.pem -config openssl-san.cnf
```

 註：自8.5軟體版本起，WLC支援的最大金鑰大小為4096位元

5. 系統會提示您輸入一些資訊：國家/地區名稱、州/省、城市等。請提供必要資訊。

 注意：必須提供正確的通用名稱。確定用來建立憑證的主機名稱(一般名稱)與WLC上虛擬介面IP位址的網域名稱系統(DNS)主機名稱項目相符，且此名稱也存在DNS中。此外，在對虛擬IP(VIP)介面做出變更後，您必須重新啟動系統，才能使變更內容生效。

以下是範例：

```
<#root>
OpenSSL>
req -new -newkey rsa:3072 -nodes -keyout mykey.pem -out myreq.pem -config openssl-san.cnf

Loading 'screen' into random state - done
Generate a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'mykey.pem'
-----
You are about to be asked to enter information that is 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 is a default value,
```

If you enter '.', the field is left blank.

Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ABC
Organizational Unit Name (eg, section) []:CDE
Common Name (eg, YOUR name) []:XYZ.ABC
Email Address []:(email address)

Please enter the following 'extra' attributes
to be sent with your certificate request

A challenge password []:Test123
An optional company name []:OpenSSL>

6. 您可以使用GUI驗證CSR (特別是用於驗證SAN屬性存在與否) `openssl req -text -noout -in csrfilename`

7. 提供所有必要的詳細資訊後，系統會產生兩個檔案：


- 包含名稱 mykey.pem 的新私密金鑰
- 包含名稱 myreq.pem 的 CSR

選項 B : WLC 產生的 CSR

如果您的WLC執行的軟體版本是8.3.102或更新版本，則更安全的選項是使用WLC產生CSR。好處在於，金鑰是在WLC上產生的，永遠不會離開WLC；因此，絕不會暴露到外界。

目前，此方法不允許在CSR中設定SAN，已知這會導致某些瀏覽器出現問題（這些瀏覽器會要求需有SAN屬性）。某些CA允許在簽署時插入SAN欄位，因此最好向您的CA確認。

WLC本身產生的CSR使用2048位元的金鑰大小，而ecdsa金鑰大小為256位元。

 註：如果您執行CSR產生命令，且尚未安裝後續憑證，則下次重新啟動時，HTTPS將完全無法存取WLC，因為WLC會在重新啟動後使用新產生的CSR金鑰，但沒有搭配該金鑰的憑證。


若要產生用於 Web 驗證的 CSR，請輸入以下命令：


```
(WLC)>config certificate generate csr-webauth BE BR Brussels Cisco TAC mywebauthportal.wireless.com tac@cisco.com  
-----BEGIN CERTIFICATE REQUEST-----  
MIICqjCCAZICAQAwwZTELMAkGA1UECAwCQlIxETAPBgNVBACMCEJydXNzZWxzMQ4w  
DAYDVQQKDAVDaXNjbzEMMAoGA1UECwwDVEFDMSUwIwYDVQQDDDBxteXdlYmF1dGhw  
b3J0YWwud2lyZWxlc3MuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC  
AQEAnssc0BxlJ2ULa3xgJH5IAUtbD9CuQVqqf2nflh+V1tu82rzTvz38bjF3g+MX  
JiaBbKMA27VJH1J2K2ycDMIhJyYpH9N59T4fXvZr3JNGVfmHIRuYDnCSdii0ookK  
FU4sDwXyOxR6gfB6m+Uv5SCOuzfBsTz5bfQ1NIZqg1hNemnhqVgbXEd90sgJmaF2  
0tsL0jUhbLosdwMLUbZ5LUa34mvufol3VAKA0cmWZh2WzMJial2JpbO0afRO3kSg  
x3XDkZiR7Z9a8rK6Xd8rwDlx0TcMFWdWVcKMDgh7Tw+Ba1cUjjiMzKT6OOjFGOGu  
yNkgYefrBN+WkDdc6c55bxErwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAB0K  
ZvEpAafoovphlcXIEIL2DSwVzjlbD9u7T5JRGgqri1l9/0wzxFjTymQofga427mj  
5dNqlCWxRFmKhAmO0fGQkUoP1YhJRxidU+0T8O46s/stbhj9nuInmoTgPaA0s3YH
```

```
tDdWgjmV2ASnroUV9oBNu3wR6RQtKDX/CnTSRG5YufTWOVf9IRnL9LkU6pzA69Xd
YHPLnD2ygR1Q+3ls4+5Jw6ZQAaqIPWyVQccvGyFacscA7L+nZK3SSITzGt9B2HAa
PQ8DQOaCwnqt2efYmaezGiHOR8XHOaWcNoJQCFOnb4KK6/1aF/7eOS4LMA+jSzt4
Wkc/wH4DyYdH7x5jzHc=
-----END CERTIFICATE REQUEST-----
```

若要產生用於Web管理的CSR，命令變更為：

```
(WLC)>config certificate generate csr-webadmin BE BR Brussels Cisco TAC mywebauthportal.wireless.com tac@cisco.com
```

 註：輸入命令後，CSR會列印在終端機上。沒有其他方法可以擷取，無法從WLC上傳，也無法儲存。輸入命令後，必須將其複製貼上到您電腦上的檔案中。產生的金鑰會保留在 WLC 上，直到產生下一個 CSR（金鑰因次被覆寫）。如果您之後需要變更WLC硬體(RMA)，您將無法重新安裝與新金鑰相同的憑證，新WLC上會產生CSR。

 成長至

然後，您必須將此 CSR 交給您的第三方簽署機構或您的企業公開金鑰基礎架構 (PKI)。

步驟 2. 簽署憑證

選項A：從您的企業CA取得Final.pem檔案

此範例僅示範目前的企業CA（在本範例中為Windows Server 2012），並不涵蓋從頭開始設定Windows Server CA的步驟。

1. 在瀏覽器中，前往您的企業CA頁面(通常為https://<CA-ip>/certsrv)，然後按一下 **Request a certificate**.

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

2. 按一下 **advanced certificate request**.

Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#).

3. 輸入您從 WLC 或 OpenSSL 取得的 CSR。在「Certificate Template」下拉清單中，選擇「Web Server」。

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request into the Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
5dNq1CWxRFmKham00fGQkUoP1YhJRxiDu+0T8O46
tDdWgjmV2ASnroUV9oBnu3wR6RQtKDX/CnTSRG5Y
YHPLnD2ygR1Q+3Is4+5Jw6ZQAaqlPWYVQccvGyFa
PQ8DQOaCwnqt2efYmaezGiHOR8XHOaWcNoJQCFOn
Wkc/wH4DyYdh7x5jzHc=
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server 

Additional Attributes:

Attributes:

Submit >

4. 按一下 Base 64 encoded 單選按鈕。

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

5. 如果下載的憑證的型別為PKCS7(.p7b)，請將其轉換為PEM（在下一個範例中，憑證鏈結已下載為檔案名稱「All-certs.p7b」）：

```
openssl pkcs7 -print_certs -in All-certs.p7b -out All-certs.pem
```

6. 如果您使用選項A（OpenSSL來產生CSR），請將憑證鏈結（在本範例中命名為「All-certs.pem」）憑證與連同CSR一起產生的私密金鑰（裝置憑證的私密金鑰，在本範例中為mykey.pem）合併，然後將檔案另存為final.pem。如果您直接從WLC（選項B）產生CSR，請跳過此步驟。

在OpenSSL應用程式中輸入以下命令，以便建立All-certs.pem和final.pem檔案：


```
<#root>
```

```
openssl>
```

```
pkcs12 -export -in All-certs.pem -inkey mykey.pem  
-out All-certs.p12 -clcerts -passin pass:check123  
-passout pass:check123
```


```
openssl>
```

```
pkcs12 -in All-certs.p12 -out final.pem  
-passin pass:check123 -passout pass:check123
```

 註：在此命令中，必須輸入引數 — passin 和-passout。針對 -passout 參數所設定的密碼必須與 WLC 上所設定的 certpassword 參數相符。在本範例中，針對 -passin 和 -passout 參數所設定的密碼為 check123。

若您按照「選項A：使用OpenSSL來產生CSR」操作，final.pem是下載到WLC的檔案。

如果您按照「選項B：由WLC本身產生的CSR」，則All-certs.pem是下載到WLC的檔案。下一步是將此檔案下載到 WLC。


 註：如果將憑證上傳到WLC失敗，請確認pem檔案中是否存在整個鏈結。請參閱選項B的步驟2（從第三方CA取得final.pem），看看必須出現的結果。如果您在檔案中只看到一個憑證，則需要手動下載所有中間 CA 和根 CA 憑證檔案，並將其附加（透過簡單的複製貼上）到該檔案以建立鏈結。

選項B：從第三方CA取得Final.pem檔案

1. 將 CSR 資訊複製貼上到任一 CA 註冊工具中。

將 CSR 提交給第三方 CA 後，第三方 CA 會以數位方式簽署憑證，並透過電子郵件傳回簽署的憑證鏈結。在鏈結憑證的情況下，您會收到來自 CA 的整個憑證鏈結。如果您只有一個中間憑證，如本例所示，您將收到來自 CA 的這三個憑證：

- Root certificate.pem
- Intermediate certificate.pem
- Device certificate.pem

 注意：請確保憑證與Apache的安全雜湊演演算法1(SHA1)加密相容。

2. 收到所有三個憑證後，按以下順序將每個 pem 檔案的內容複製貼上到另一個檔案中：

```
-----BEGIN CERTIFICATE-----
*Device cert*
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
*Intermediate CA cert *
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
*Root CA cert *
-----END CERTIFICATE-----
```

3. 將檔案另存為 All-certs.pem。
4. 如果您使用選項A（OpenSSL來產生CSR），請將All-certs.pem憑證與連同CSR一起產生的私密金鑰（裝置憑證的私密金鑰，在本範例中為mykey.pem）合併，然後將檔案另存為final.pem。如果您直接從WLC（選項B）產生CSR，請跳過此步驟。

在OpenSSL應用程式中輸入以下命令，以便建立All-certs.pem和final.pem檔案：


```
<#root>

openssl>

pkcs12 -export -in All-certs.pem -inkey mykey.pem
        -out All-certs.p12 -clcerts -passin pass:check123
        -passout pass:check123

openssl>

pkcs12 -in All-certs.p12 -out final.pem
        -passin pass:check123 -passout pass:check123
```

 註：在此命令中，必須輸入引數 — passin 和-passout。針對 -passout 參數所設定的密碼必須與 WLC 上所設定的 certpassword 參數相符。在本範例中，針對 -passin 和 -passout 參數所設定的密碼為 check123。

若您按照「選項A：使用OpenSSL來產生CSR」操作，final.pem是下載到WLC的檔案。如果您按照「選項B：由WLC本身產生的CSR」，則All-certs.pem是您必須下載到WLC的檔案。下一步是將此檔案下載到WLC。

 註：也支援SHA2。思科漏洞 ID [CSCuf20725](#) 是請求對於 SHA512 支援。

步驟 3：CLI。使用 CLI 將第三方憑證下載到 WLC

完成以下步驟，使用CLI將鏈結憑證下載到WLC:

1. 將 final.pem file 移動到 TFTP 伺服器上的預設目錄中。
2. 在CLI中，輸入以下命令以變更下載設定：


```
<#root>
>
transfer download mode tftp
>
transfer download datatype webauthcert
>
transfer download serverip
```

```
>  
transfer download path
```

```
>  
transfer download filename final.pem
```

3. 輸入 .pem 檔案的密碼，以便作業系統解密 SSL 金鑰和憑證。

```
<#root>  
>  
transfer download certpassword password
```

 註：請確定 certpassword 的值與在「[產生CSR](#)」一節的步驟4 (或5) 中設定的-passout引數密碼相同。在本例中，certpassword 必須是 check123。如果您選擇了選項 B (也就是使用WLC本身產生CSR)，請將certpassword欄位留空。

4. 輸入 transfer download start 命令可檢視更新的設定。然後在出現提示時輸入 y，以確認目前的下載設定並開始下載憑證和金鑰。以下是範例：

```
<#root>  
(Cisco Controller) >  
transfer download start  
  
Mode..... TFTP  
Data Type..... Site Cert  
TFTP Server IP..... 10.77.244.196  
TFTP Packet Timeout..... 6  
TFTP Max Retries..... 10  
TFTP Path...../  
TFTP Filename..... final.pem
```

This might take some time.
Are you sure you want to start? (y/N)

y

TFTP EAP Dev cert transfer start.

Certificate installed.

Reboot the switch to use new certificate.

5. 重新啟動 WLC 以使變生效。

步驟 3：GUI。使用 GUI 將第三方憑證下載到 WLC

完成以下步驟，以便使用 GUI 將鏈結憑證下載到 WLC：

1. 將裝置憑證 final.pem 複製到 TFTP 伺服器上的預設目錄。
2. 選擇 Security > Web Auth > Cert 以開啟「Web Authentication Certificate」頁面。
3. 請檢視 Download SSL Certificate 釐取方塊，以便檢視 Download SSL Certificate From TFTP Server 引數。
4. 在「IP Address」欄位中，輸入 TFTP 伺服器的 IP 位址。

The screenshot displays the Cisco WLC GUI interface for configuring a Web Authentication Certificate. The 'SECURITY' tab is selected, and the 'Web Authentication Certificate' page is open. The 'Current Certificate' section shows details for 'bn39WebAuthCer', including its type, serial number, validity period, and issuer information. Below this, the 'Download SSL Certificate' section is expanded, revealing the 'Download SSL Certificate From TFTP Server' configuration area. This area contains several input fields: 'Server IP Address' (172.204.196), 'Maximum retries' (17), 'Timeout (seconds)' (6), 'Certificate File Path' (/), 'Certificate File Name' (final.pem), and 'Certificate Password' (*****). A red box highlights the 'Download SSL Certificate From TFTP Server' section and its fields.

5. 在「File Path」欄位中，輸入憑證的目錄路徑。
6. 在「File Name」欄位中，輸入憑證的名稱。
7. 在「Certificate Password」欄位中，輸入用來保護憑證的密碼。
8. 按一下 **Apply**.
9. 下載完成後，選擇 **Commands > Reboot > Reboot**.
10. 如果系統提示儲存更改，請按一下 **Save and Reboot**.
11. 按一下「OK」以確認重新啟動控制器的決定。

疑難排解

若要疑難排解WLC上憑證的安裝，請在WLC上開啟命令列，並輸入 `debug transfer all enable` 和 `debug pm pki enable` 然後完成下載憑證程式。

In some cases, the logs only say that the certificate installation failed:

```
*TransferTask: Sep 09 08:37:17.415: RESULT_STRING: TFTP receive complete... Installing Certificate.
```

```
*TransferTask: Sep 09 08:37:17.415: RESULT_CODE:13
```

```
TFTP receive complete... Installing Certificate.
```

```
*TransferTask: Sep 09 08:37:21.418: Adding cert (1935 bytes) with certificate key password.
```

```
*TransferTask: Sep 09 08:37:21.421: RESULT_STRING: Error installing certificate.
```

驗證憑證格式和鏈結。請記住，低於版本7.6的WLC須具備整個鏈結，因此您只能上傳WLC憑證。檔案中必須存在通到根 CA 的鏈結。

以下是中間 CA 不正確時的偵錯範例：

```
*TransferTask: Jan 04 19:08:13.338: Add WebAuth Cert: Adding certificate & private key using password c
*TransferTask: Jan 04 19:08:13.338: Add ID Cert: Adding certificate & private key using password check1
*TransferTask: Jan 04 19:08:13.338: Add Cert to ID Table: Adding certificate (name: bsnSslWebauthCert)
*TransferTask: Jan 04 19:08:13.338: Add Cert to ID Table: Decoding PEM-encoded Certificate (verify: YES
*TransferTask: Jan 04 19:08:13.338: Decode & Verify PEM Cert: Cert/Key Length was 0, so taking string l
*TransferTask: Jan 04 19:08:13.338: Decode & Verify PEM Cert: Cert/Key Length 7148 & VERIFY
*TransferTask: Jan 04 19:08:13.342: Decode & Verify PEM Cert: X509 Cert Verification return code: 0
*TransferTask: Jan 04 19:08:13.342: Decode & Verify PEM Cert: X509 Cert Verification result text: unabl
*TransferTask: Jan 04 19:08:13.342: Decode & Verify PEM Cert: Error in X509 Cert Verification at 0 dept
```

*TransferTask: Jan 04 19:08:13.343: Add Cert to ID Table: Error decoding (verify: YES) PEM certificate
*TransferTask: Jan 04 19:08:13.343: Add ID Cert: Error decoding / adding cert to ID cert table (verifyC
*TransferTask: Jan 04 19:08:13.343: Add WebAuth Cert: Error adding ID cert

高可用性 (HA SSO) 注意事項

如 WLC HA SSO 部署指南所述，在 HA SSO 的情況中，憑證不會從主控制器複製到輔助控制器。

這表示您必須先將所有憑證匯入輔助控制器，再建立HA配對。

另一個警告是，如果您在主WLC上產生CSR（並因此在本地建立金鑰），則無法匯出該金鑰。

唯一的方法是使用 OpenSSL 產生主 WLC 的 CSR（因此具有連結到憑證的金鑰），並在兩個 WLC 上匯入該憑證/金鑰組合。

相關資訊

- [產生第三方憑證的 CSR，並將未鏈結的憑證下載到 WLC](#)
- [產生 Wireless Control System \(WCS\) 上第三方憑證的憑證簽署請求 \(CSR\)](#)
- [在 Linux 伺服器設定上安裝 Wireless Control System \(WCS\) 憑證簽署請求 \(CSR\) 的範例](#)
- [技術支援與文件 - Cisco Systems](#)
- [WLC HA SSO 指南](#)

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）。