

# 在CCE解決方案中實施CA簽名的證書

## 目錄

---

### [簡介](#)

### [必要條件](#)

#### [需求](#)

#### [採用元件](#)

### [背景](#)

### [程式](#)

#### [基於CCE Windows的伺服器](#)

##### [1.生成CSR](#)

##### [2.獲取CA簽名的證書](#)

##### [3.上傳CA簽名的證書](#)

##### [4.將CA簽名的證書繫結到IIS](#)

##### [5.將CA簽名的證書繫結到診斷入口網站](#)

##### [6.將根證書和中間證書匯入Java金鑰庫](#)

#### [CVP解決方案](#)

##### [1.使用FQDN生成證書](#)

##### [2.產生CSR](#)

##### [3.獲取CA簽名的證書](#)

##### [4.匯入CA簽名證書](#)

#### [VOS伺服器](#)

##### [1.生成CSR證書](#)

##### [2.獲取CA簽名的證書](#)

##### [3.上傳應用程式和根證書](#)

### [驗證](#)

### [疑難排解](#)

### [相關資訊](#)

---

## 簡介

本檔案介紹如何在思科客服中心企業版(CCE)解決方案中實作憑證授權單位(CA)簽署憑證。

作者：Anuj Bhatia、Robert Rogier和Ramiro Amaya，思科TAC工程師。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- [整合客服中心企業版\(UCCE\)版本12.5\(1\)](#)
- [套裝客服中心企業版本12.5\(1\)](#)
- [客戶語音入口網站\(CVP\)版本12.5\(1\)](#)

- Cisco Virtualized Voice Browser(VVB)
- Cisco CVP營運和管理主控台(OAMP)
- Cisco Unified Intelligence Center(CUIC)
- 思科整合通訊管理員(CUCM)

## 採用元件

本檔案中的資訊是根據以下軟體版本：

- PCCE 12.5(1)
- CVP 12.5(1)
- Cisco VVB 12.5
- Finess 12.5
- CUIC 12.5
- Windows 2016

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

證書用於確保客戶端和伺服器之間的身份驗證通訊是安全的。

使用者可以從CA購買證書，也可以使用自簽名證書。

自簽名證書（顧名思義）由身份得到認證的同一實體簽署，而不是由證書頒發機構簽署。自簽名證書不被認為與CA證書一樣安全，但在許多應用程式中預設使用自簽名證書。

在Package Contact Center Enterprise(PCCE)解決方案版本12.x中，該解決方案的所有元件均由單一平台(SPOG)控制，該平台託管在主管理工作站(AW)伺服器中。

由於PCCE 12.5(1)版本中的安全管理合規性(SRC),SPOG和解決方案中的其他元件之間的所有通訊都通過安全的HTTP協定完成。在UCCE 12.5中，元件之間的通訊也通過安全HTTP協定完成。

本文檔詳細介紹在CCE解決方案中實施CA簽名的證書以實現安全HTTP通訊所需的步驟。有關任何其他UCCE安全注意事項，請參閱[UCCE安全指南](#)。有關不同於安全HTTP的任何其他CVP安全通訊，請參閱CVP配置指南：[CVP安全指南中的安全指南](#)。

## 程式

### 基於CCE Windows的伺服器

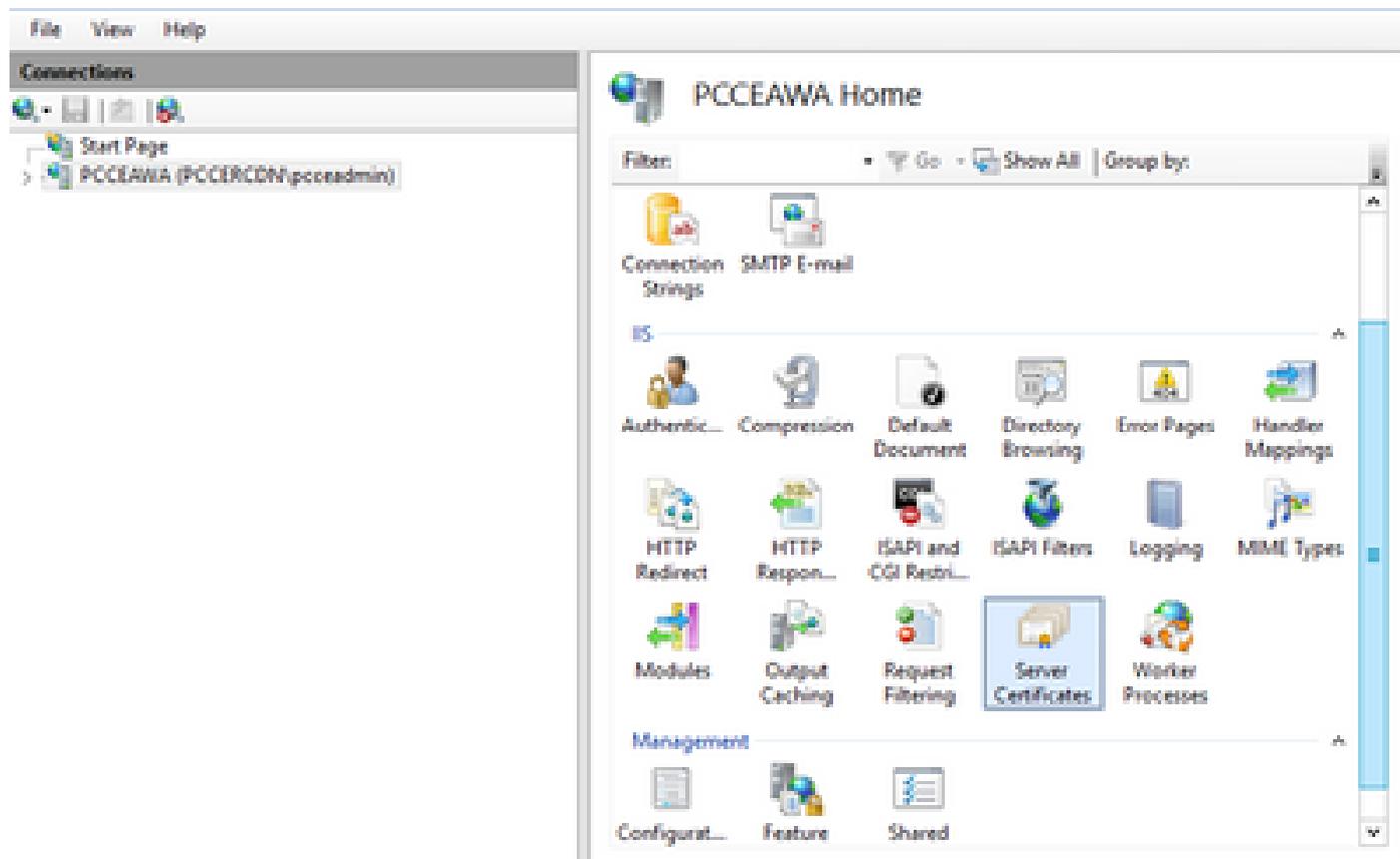
#### 1.生成CSR

此程式說明如何從Internet Information Services(IIS)管理器生成證書簽名請求(CSR)。

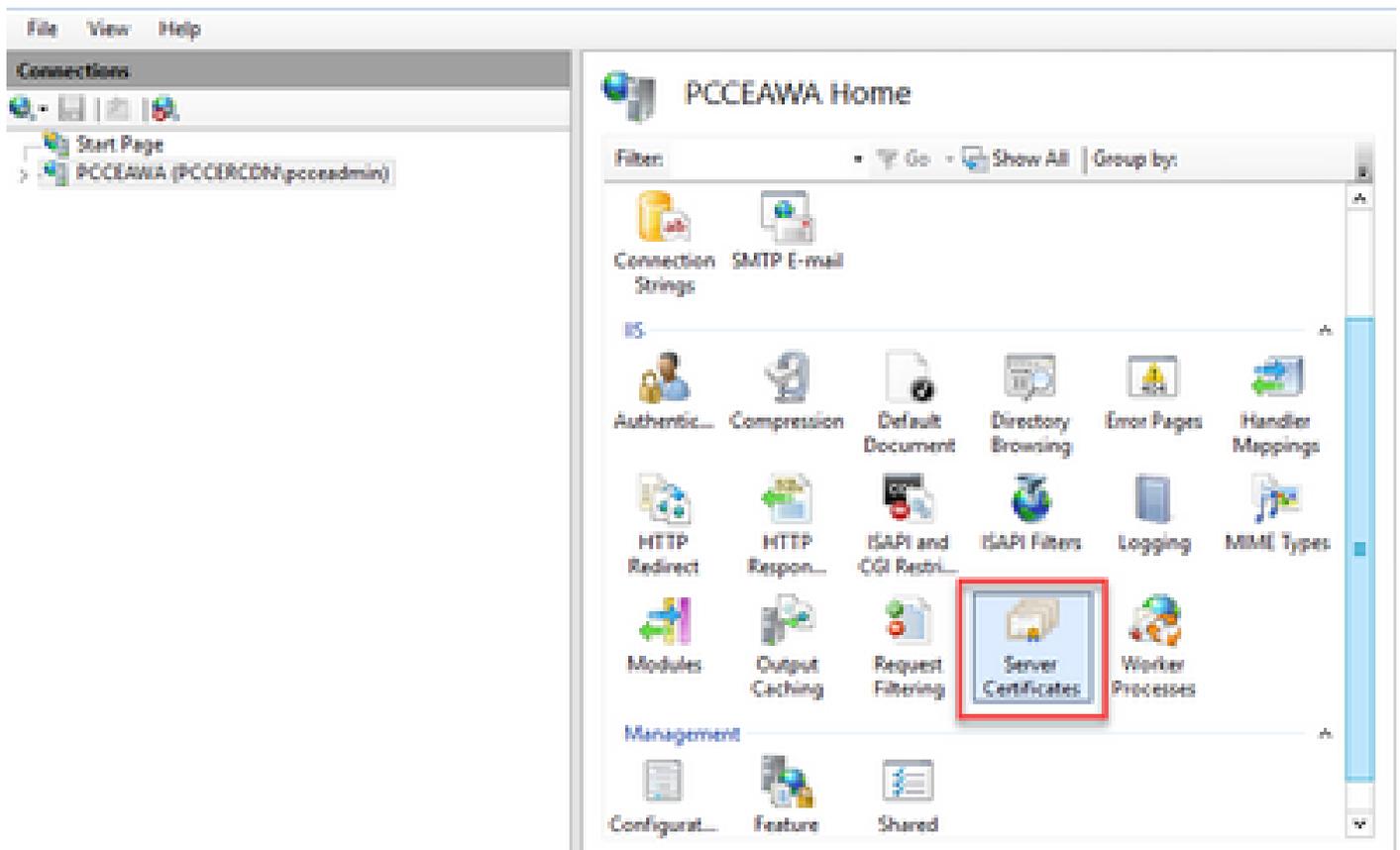
步驟 1. 登入到Windows，然後選擇「控制面板」>「管理工具」>「Internet資訊服務(IIS)管理器」。

。

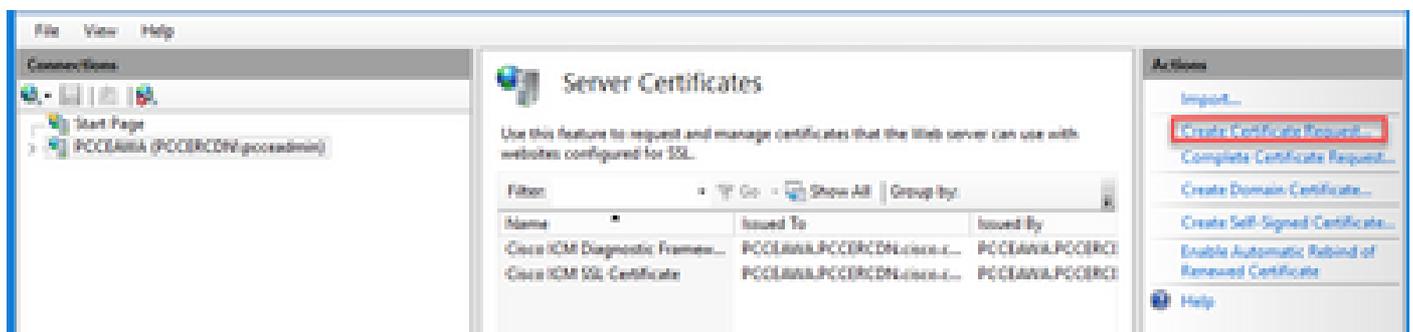
步驟 2. 在「連線」窗格中，按一下伺服器名稱。將顯示伺服器Home窗格。



步驟 3. 在IIS區域中，按兩下Server Certificates。



步驟 4.在「操作」窗格中，按一下建立證書請求。



步驟 5.在「請求證書」對話方塊中，執行以下操作：

在顯示的欄位中指定所需資訊，然後按一下下一步。

Request Certificate

Distinguished Name Properties

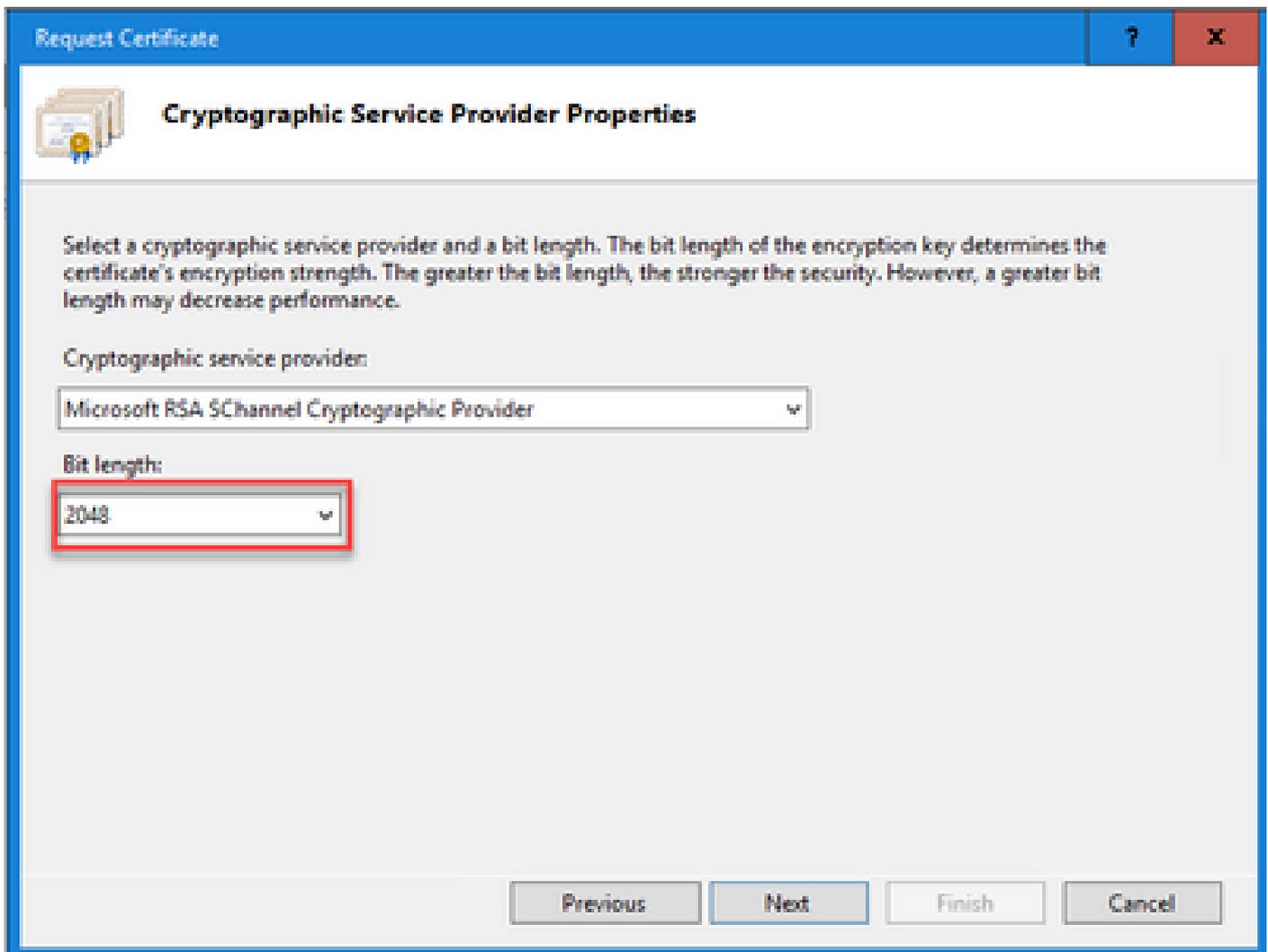
Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	<input type="text" value="pccerwa.pccercdn.cisco.com"/>
Organization:	<input type="text" value="Cisco"/>
Organizational unit:	<input type="text" value="CX"/>
City/locality:	<input type="text" value="RCDN"/>
State/province:	<input type="text" value="TX"/>
Country/region:	<input type="text" value="US"/>

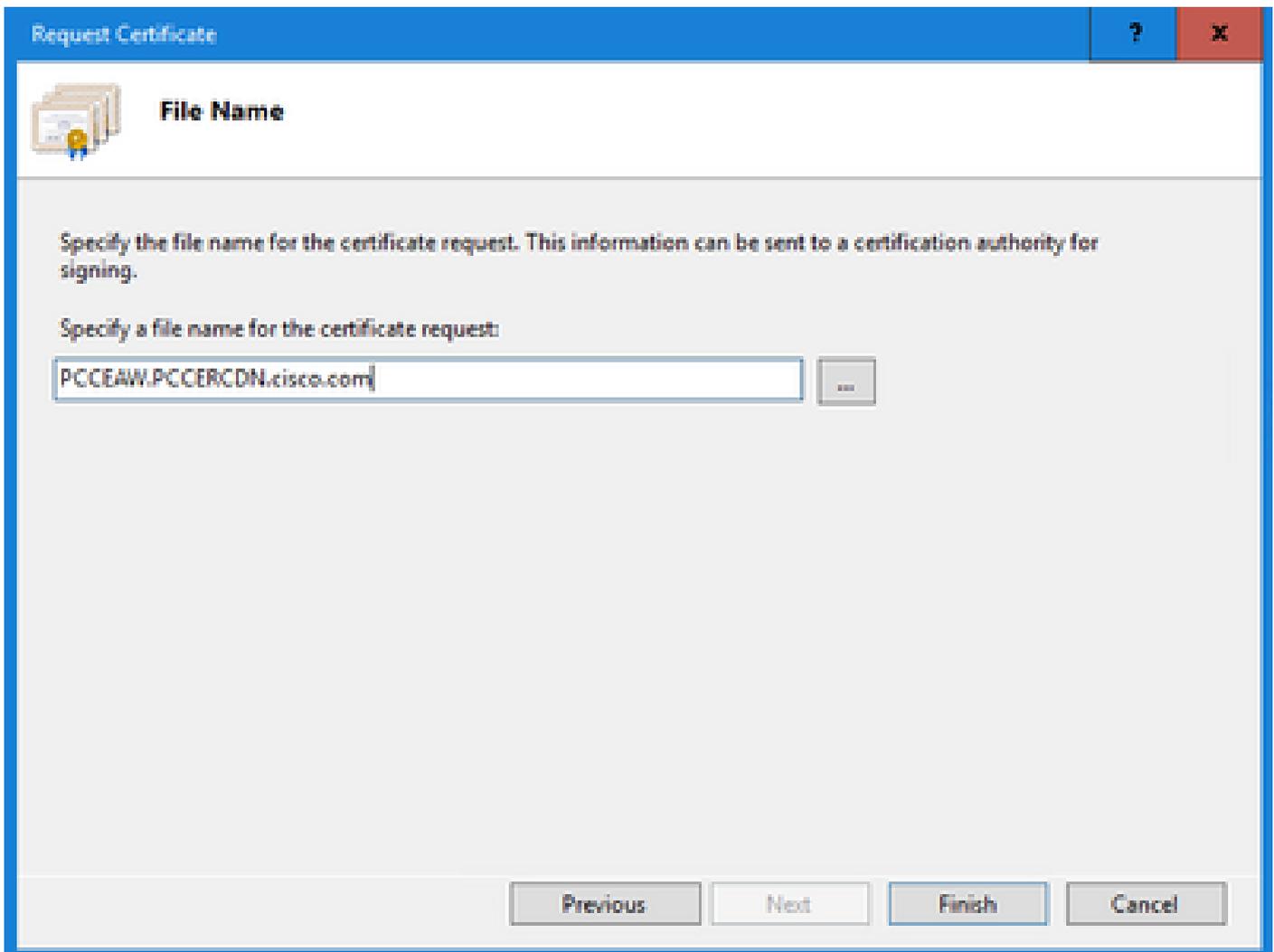
Previous Next Finish Cancel

在Cryptographic service provider下拉選單中，保留預設設定。

從「位長度」(Bit length)下拉選單中，選擇2048。



步驟 6. 為證書請求指定檔名，然後按一下Finish。



## 2. 獲取CA簽名的證書

步驟 1. 在CA上簽署憑證。

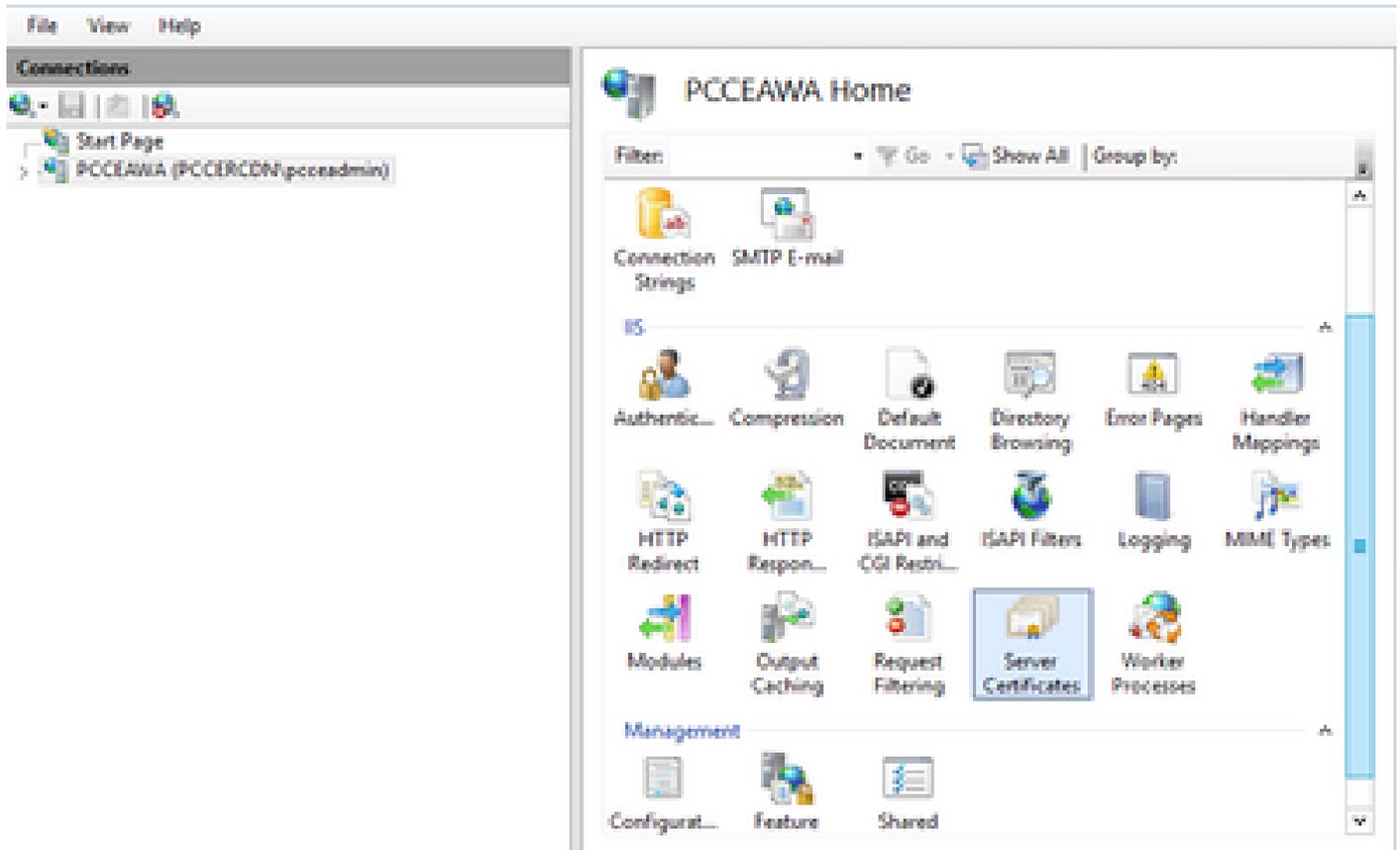
 注意：確保CA使用的證書模板包含客戶端和伺服器身份驗證。

步驟 2. 從您的憑證授權單位取得CA簽署的憑證(Root、Application和Intermediate (如果有))。

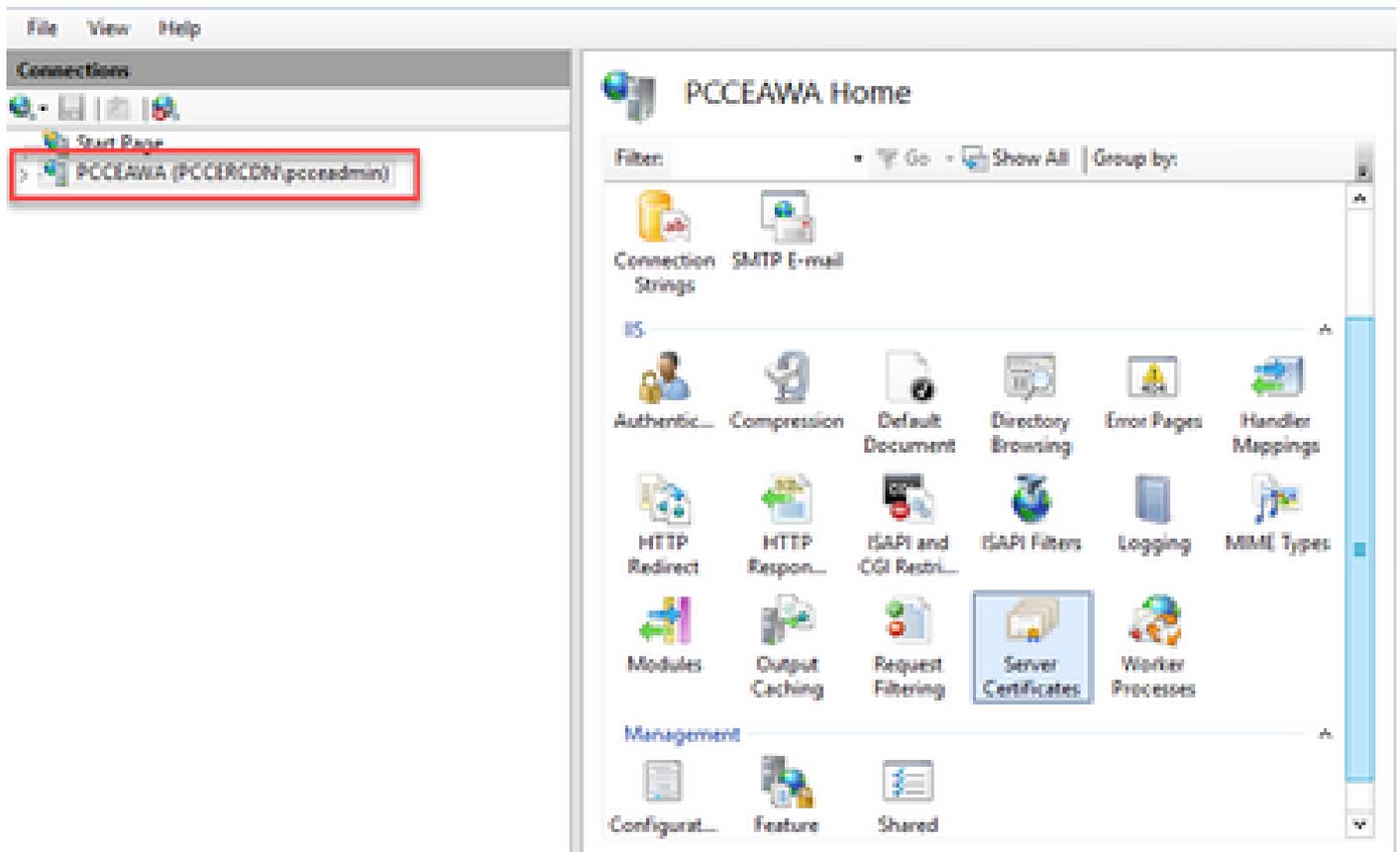
## 3. 上傳CA簽名的證書

步驟 1. 登入到Windows，然後選擇「控制面板」>「管理工具」>「Internet資訊服務(IIS)管理器」。

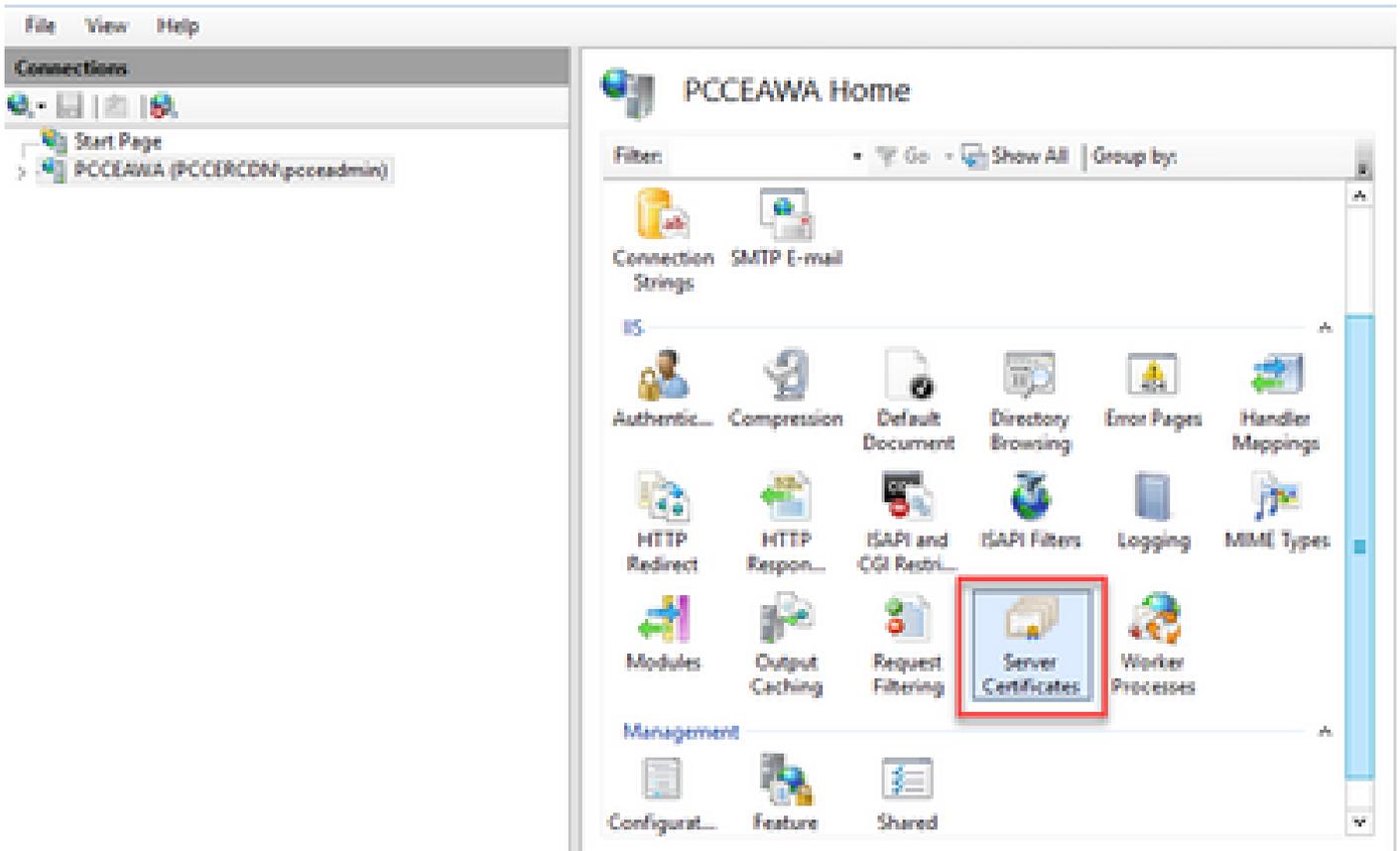
。



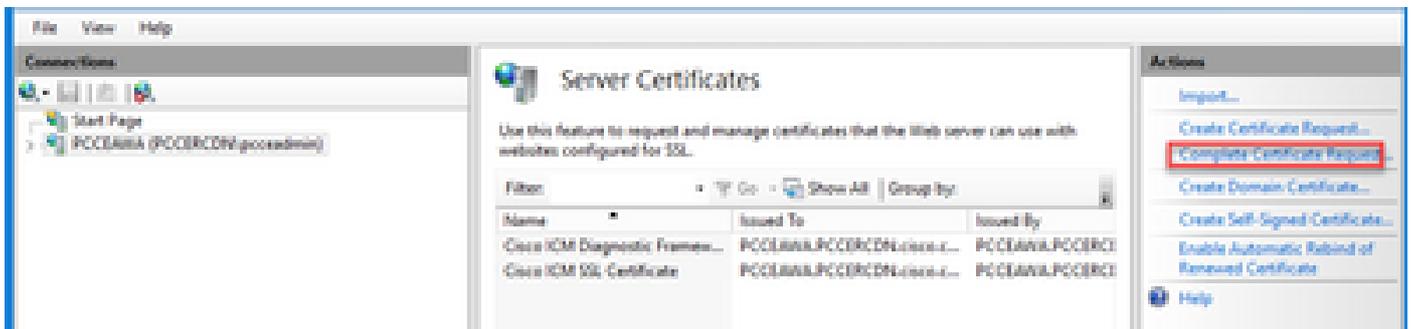
步驟 2. 在「連線」窗格中，按一下伺服器名稱。



步驟 3. 在 IIS 區域中，按兩下伺服器證書。



步驟 4. 在「操作」窗格中，按一下完成證書請求。



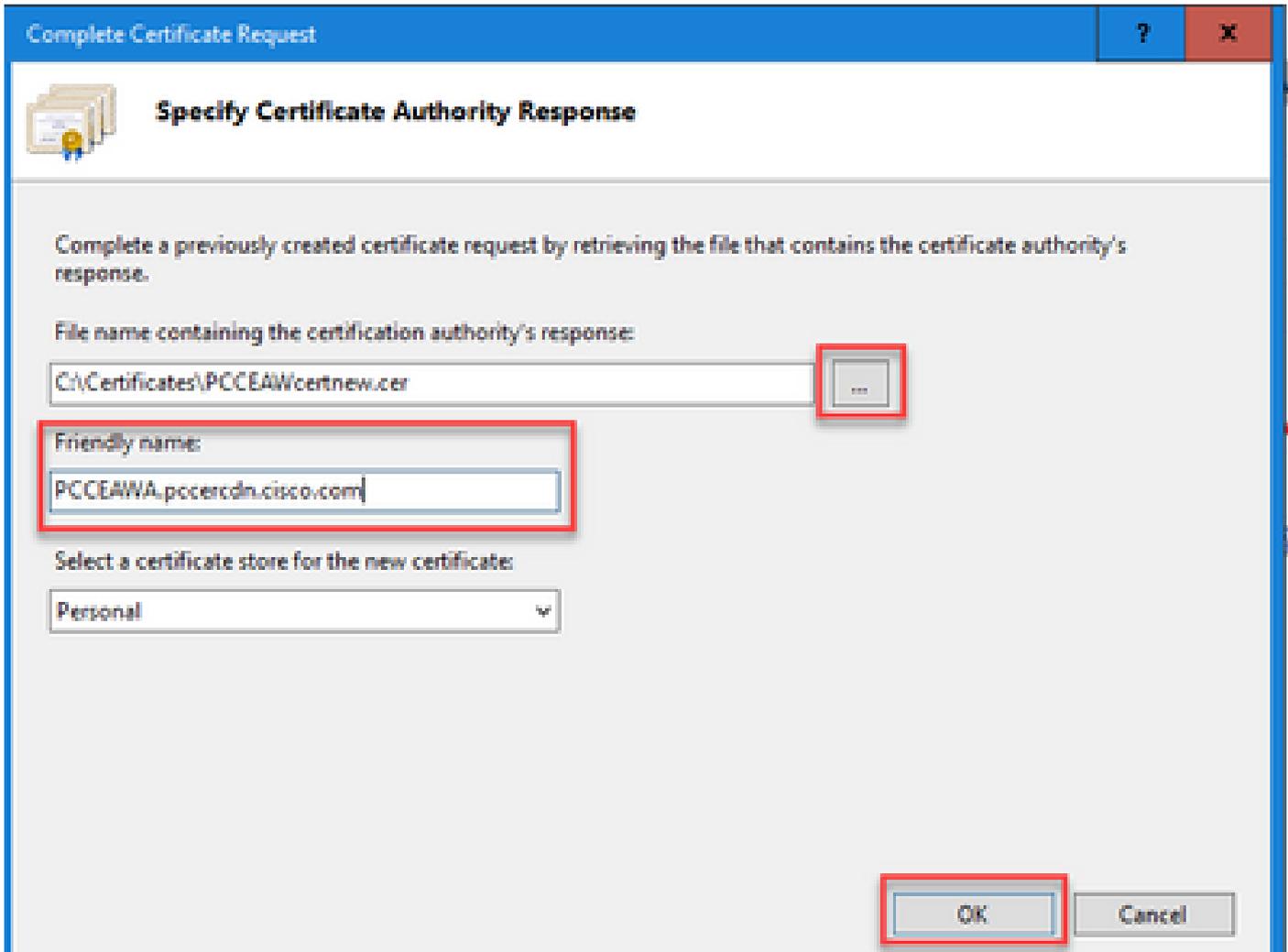
步驟 5. 在 Complete Certificate Request 對話方塊中，填寫以下欄位：

在包含證書頒發機構響應欄位的檔名中，按一下.....按鈕。

瀏覽到已簽名的應用程式證書的儲存位置，然後按一下「開啟」。

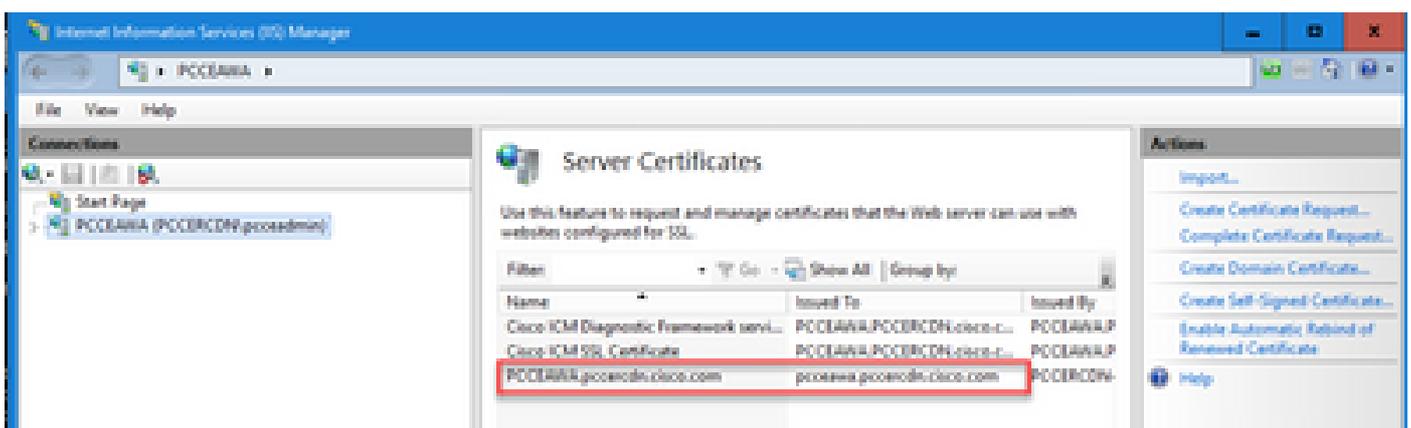
 注意：如果這是二層CA實施，並且根證書尚未在伺服器證書儲存中，則需要在匯入簽名證書之前將根證書上傳到Windows儲存中。如果需要將根CA上傳到Windows應用商店 <https://docs.microsoft.com/en-us/skype-sdk/sdn/articles/installing-the-trusted-root-certificate>，請參閱此文檔。

在「友好名稱」欄位中，輸入伺服器的完全限定域名(FQDN)或任何重要的名稱。確保「Select a certificate store for the new certificate」下拉選單保留為「Personal」。



步驟 6. 按一下OK以上傳憑證。

如果證書上傳成功，證書將顯示在「伺服器證書」窗格中。

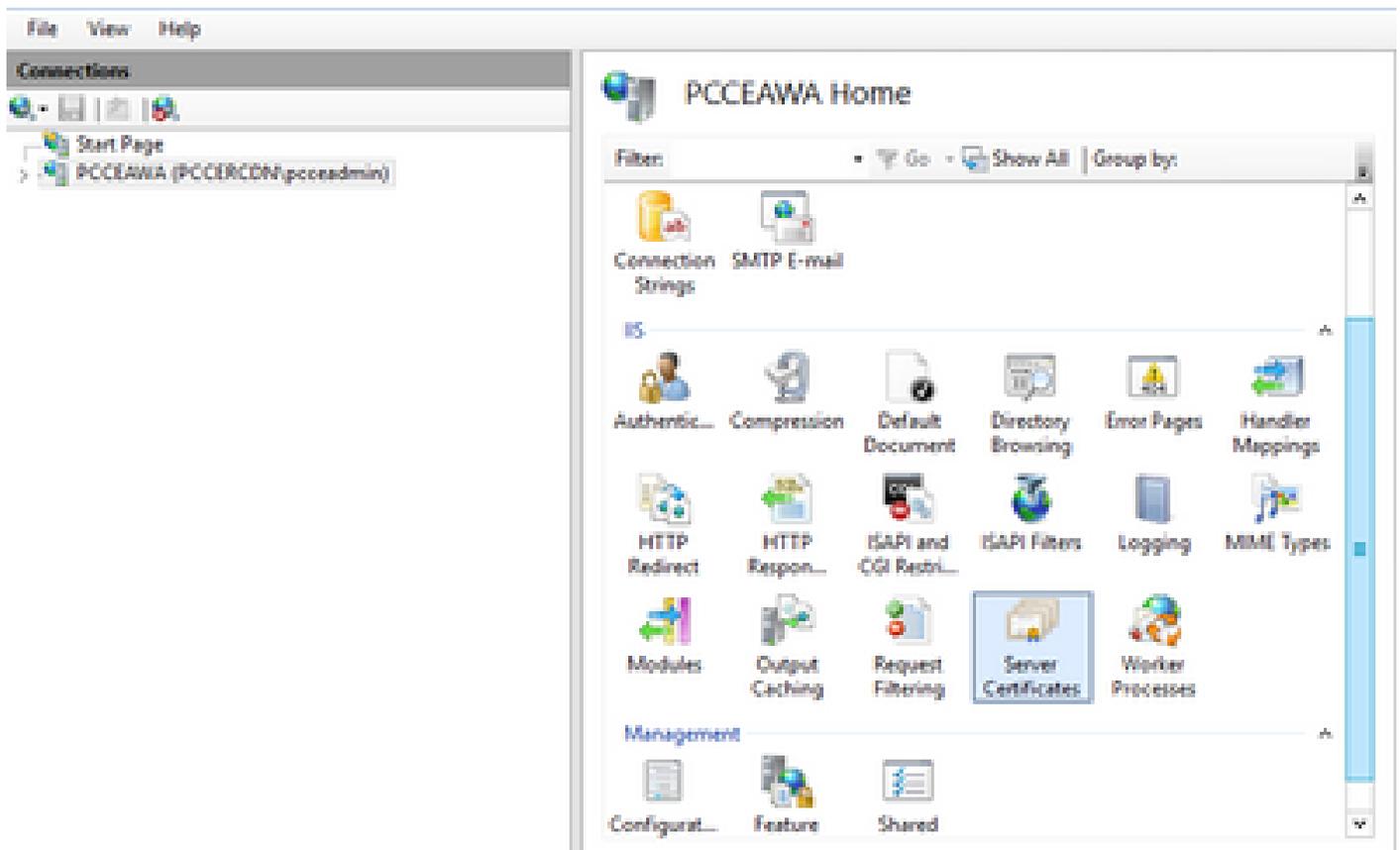


#### 4. 將CA簽名的證書繫結到IIS

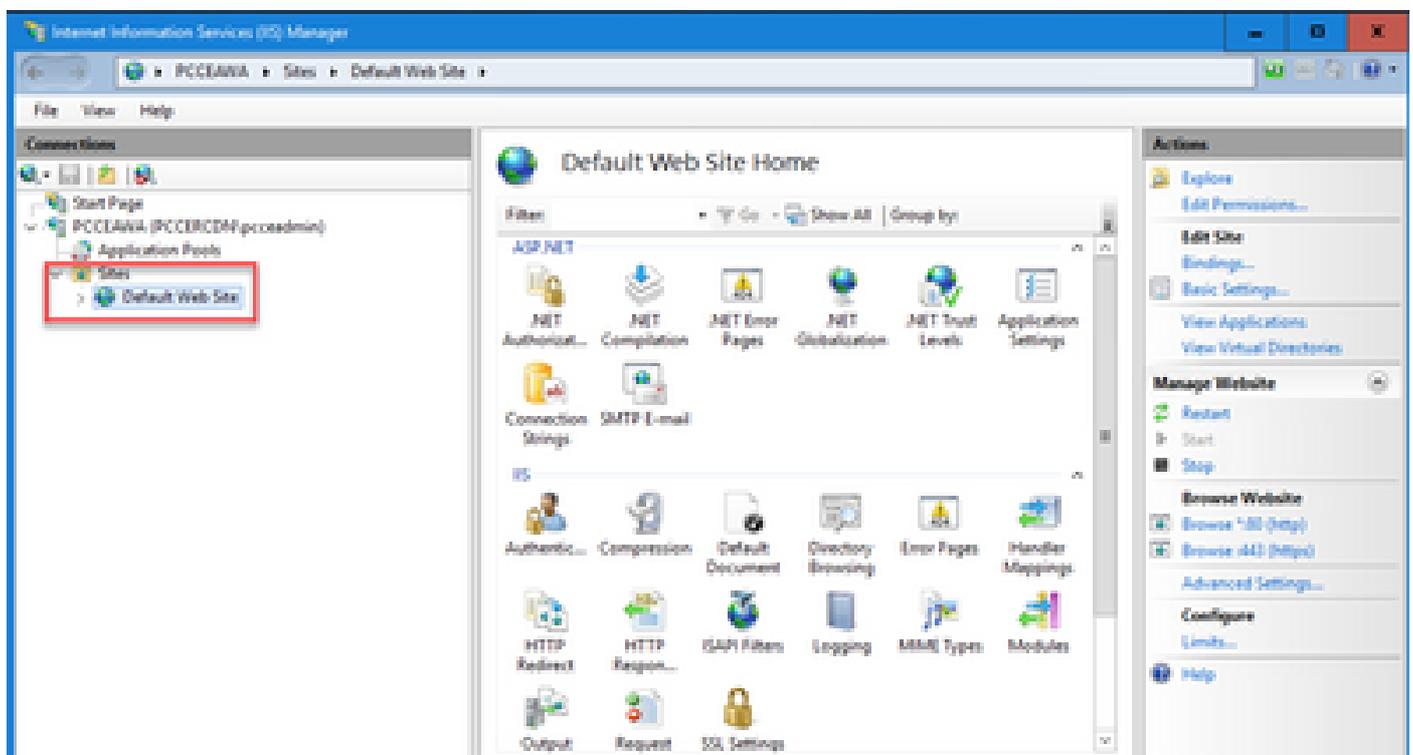
以下步驟說明如何在IIS管理器中繫結CA簽名證書。

步驟 1. 登入到Windows，然後選擇「控制面板」>「管理工具」>「Internet資訊服務(IIS)管理器」。

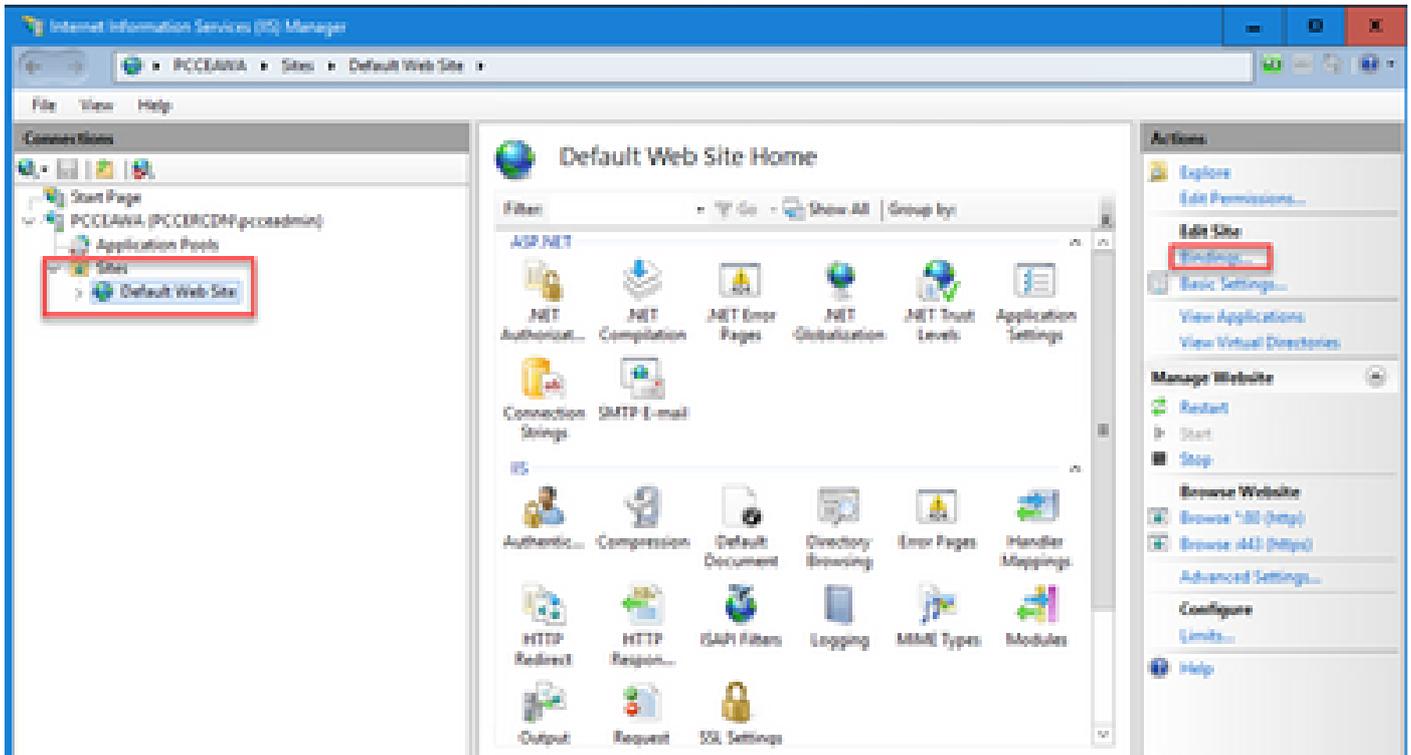
。



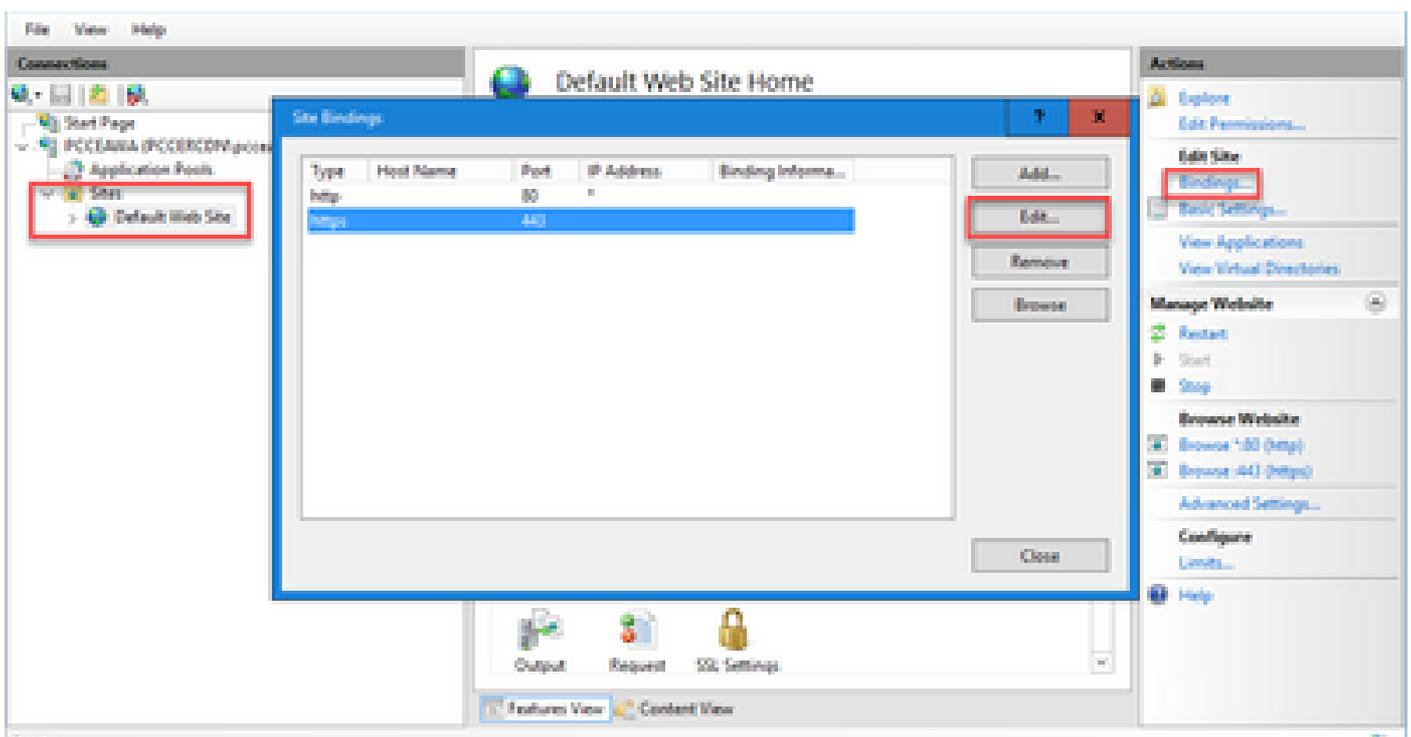
步驟 2.在「連線」窗格中，選擇<server\_name> > Sites > Default Web Site。



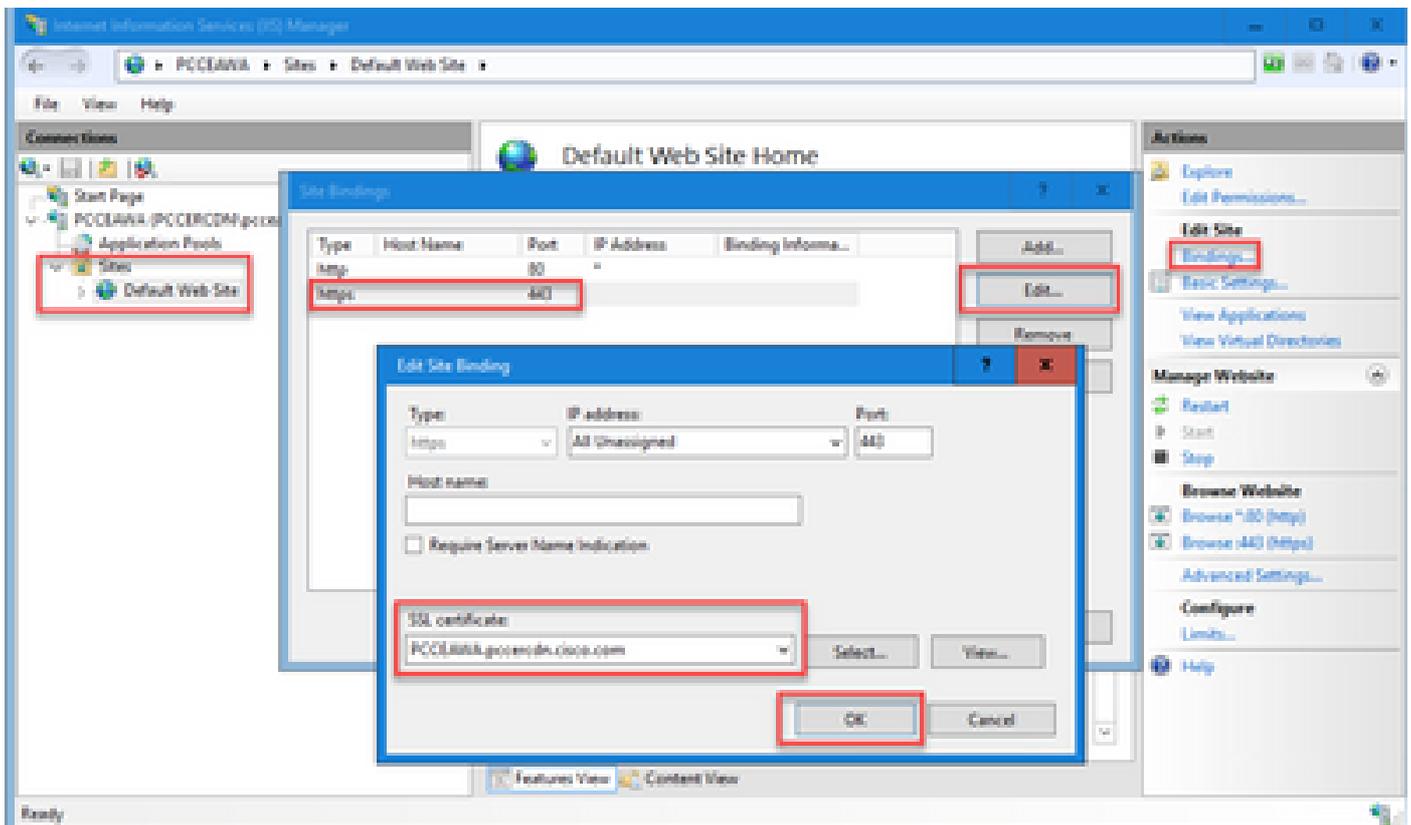
步驟 3.在「操作」窗格中，單擊「繫結.....」



步驟 4. 按一下「https with port 443」，然後按一下「Edit...」。

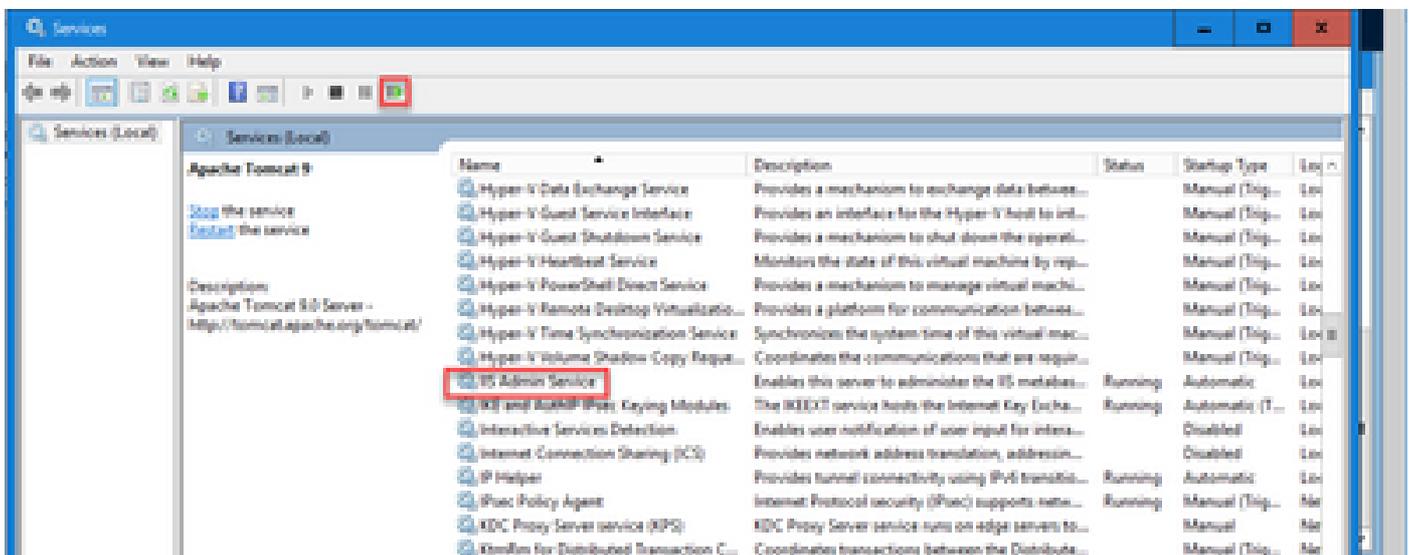


步驟 5. 從SSL證書(SSL certificate)下拉選單中，選擇與上一步中提供的友好名稱相同的證書。



步驟 6.按一下「OK」(確定)。

步驟 7.導航到開始>運行> services.msc，然後重新啟動IIS管理服務。



如果IIS重新啟動成功，則啟動應用程式時不會出現證書錯誤警告。

## 5.將CA簽名的證書繫結到診斷入口網站

以下步驟說明如何在Diagnostic Portico中繫結CA簽名證書。

步驟 1.開啟命令提示符(以管理員身份運行)。

步驟 2. 導航到Diagnostic Portico主資料夾。運行此命令：

```
cd c:\icm\serviceability\diagnostics\bin
```

步驟 3. 刪除當前繫結到診斷門戶的證書。運行此命令：

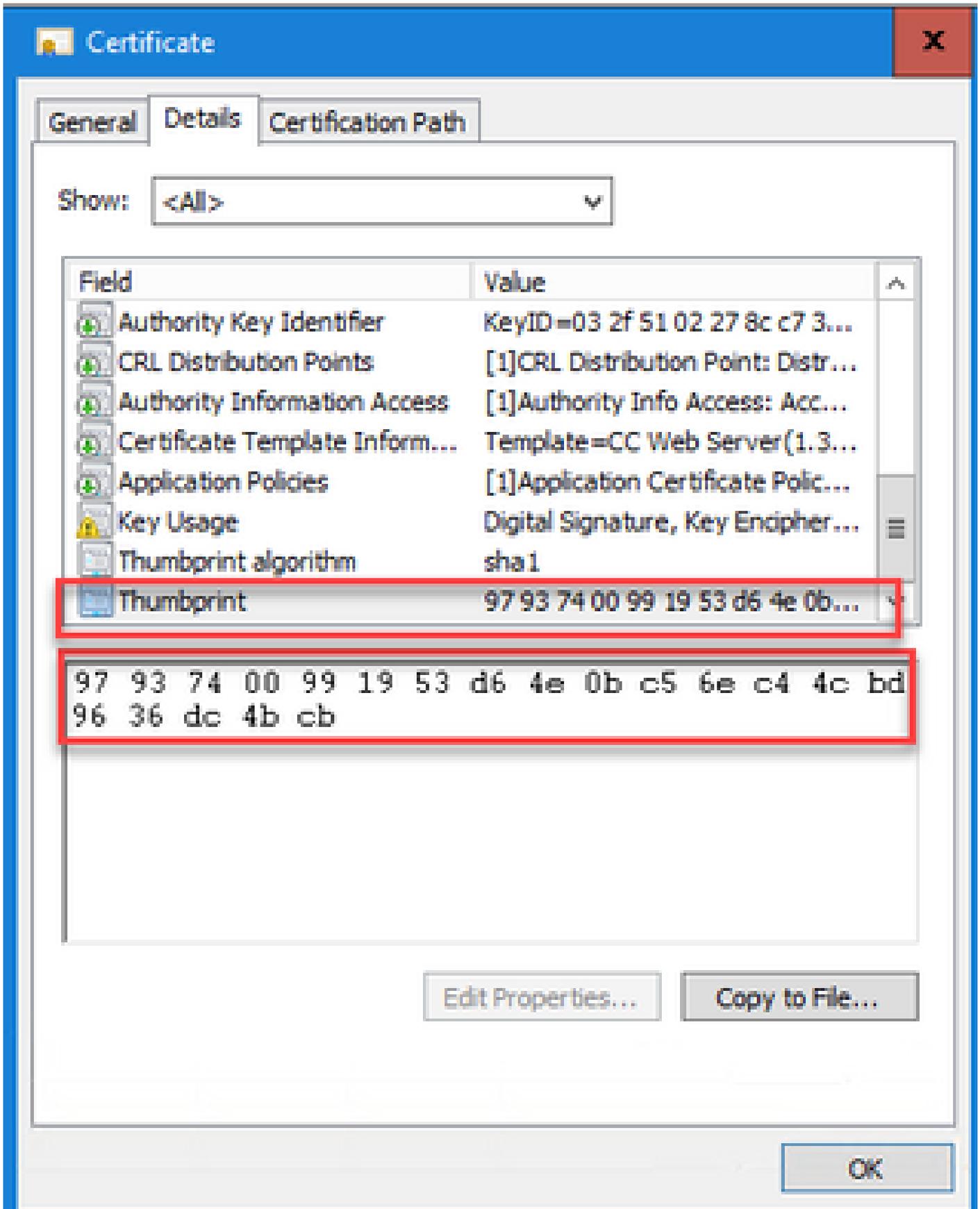
```
DiagFwCertMgr /task:UnbindCert
```

```
c:\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:UnbindCert
*****
Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager
*****

Executing Task: 'UnbindCert'
Read port number from service configuration file: '7890'
ATTEMPTING TO UNBIND CERTIFICATE FROM WINDOWS HTTP SERVICE
Binding IP Address: '0.0.0.0:7890'
Attempting to delete the existing binding on 0.0.0.0:7890
Deleted existing binding successfully
Deleted entry from the service registry
ALL TASKS FOR UNBINDING THE CERTIFICATE FROM HTTP SERVICE COMPLETED SUCCESSFULLY

c:\icm\serviceability\diagnostics\bin>
```

步驟 4. 開啟簽名證書並複製指紋欄位的雜湊內容（不含空格）。



步驟 5. 運行此命令並貼上雜湊內容。

```
DiagFwCertMgr /task:BindCertFromStore /certhash:<hash_value>
```

```
c:\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:BindCertFromStore /certhash:97937400991953d64e08c56ec44cb09636dc48cb
9c48cb

Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager
*****

Executing Task: 'BindCertFromStore'
Read port number from service configuration file: '7890'
Certhash Argument Passed: '97937400991953d64e08c56ec44cb09636dc48cb'
ATTEMPTING TO BIND CERTIFICATE WITH WINDOWS HTTP SERVICE
Binding IP Address: '0.0.0.0:7890'
Trying to look up certificate: 97937400991953d64e08c56ec44cb09636dc48cb
Local Computer Personal certificate store was opened successfully
Certificate requested found in store
Certificate store was closed successfully
Certificate bind with HTTP service on 0.0.0.0:7890 completed successfully
Found existing registry key for the service
Hash of certificate used saved in the service registry
ALL TASKS FOR BINDING THE CERTIFICATE WITH HTTP SERVICE COMPLETED SUCCESSFULLY

c:\icm\serviceability\diagnostics\bin>
```

如果證書繫結成功，則顯示證書繫結為VALID消息。

步驟 6. 驗證證書繫結是否成功。運行此命令：

DiagFwCertMgr /task:ValidateCertBinding

```
c:\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:ValidateCertBinding

Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager
*****

Executing Task: 'ValidateCertBinding'
Read port number from service configuration file: '7890'
ATTEMPTING TO VALIDATE CERTIFICATE BINDING WITH WINDOWS HTTP SERVICE
Binding IP Address: '0.0.0.0:7890'
Attempting to query HTTP service for SSL certificate binding
Found a certificate binding on 0.0.0.0:7890
Attempting to locate this certificate in the Local Computer certificate store
Trying to look up certificate: 97937400991953d64e08c56ec44cb09636dc48cb
Local Computer Personal certificate store was opened successfully
Certificate requested found in store
Certificate store was closed successfully
The certificate binding is VALID
Certificate hash stored in service registry matches certificate used by service
ALL TASKS FOR VALIDATING CERTIFICATE BINDING COMPLETED SUCCESSFULLY

c:\icm\serviceability\diagnostics\bin>
```

 注意：預設情況下，DiagFwCertMgr使用埠7890。

如果證書繫結成功，則顯示證書繫結為VALID消息。

步驟 7.重新啟動診斷框架服務。運行以下命令：

```
net stop DiagFwSvc  
net start DiagFwSvc
```

如果診斷框架成功重新啟動，則啟動應用程式時不會出現證書錯誤警告。

## 6.將根證書和中間證書匯入Java金鑰庫

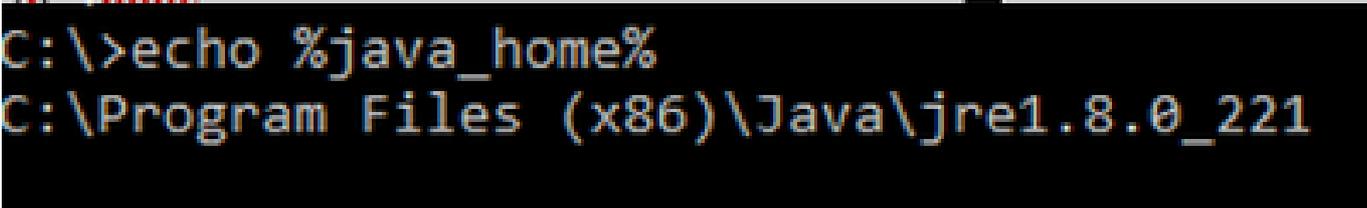
---

 注意：開始之前，您必須以管理員身份備份金鑰庫並從Java主目錄運行命令。

---

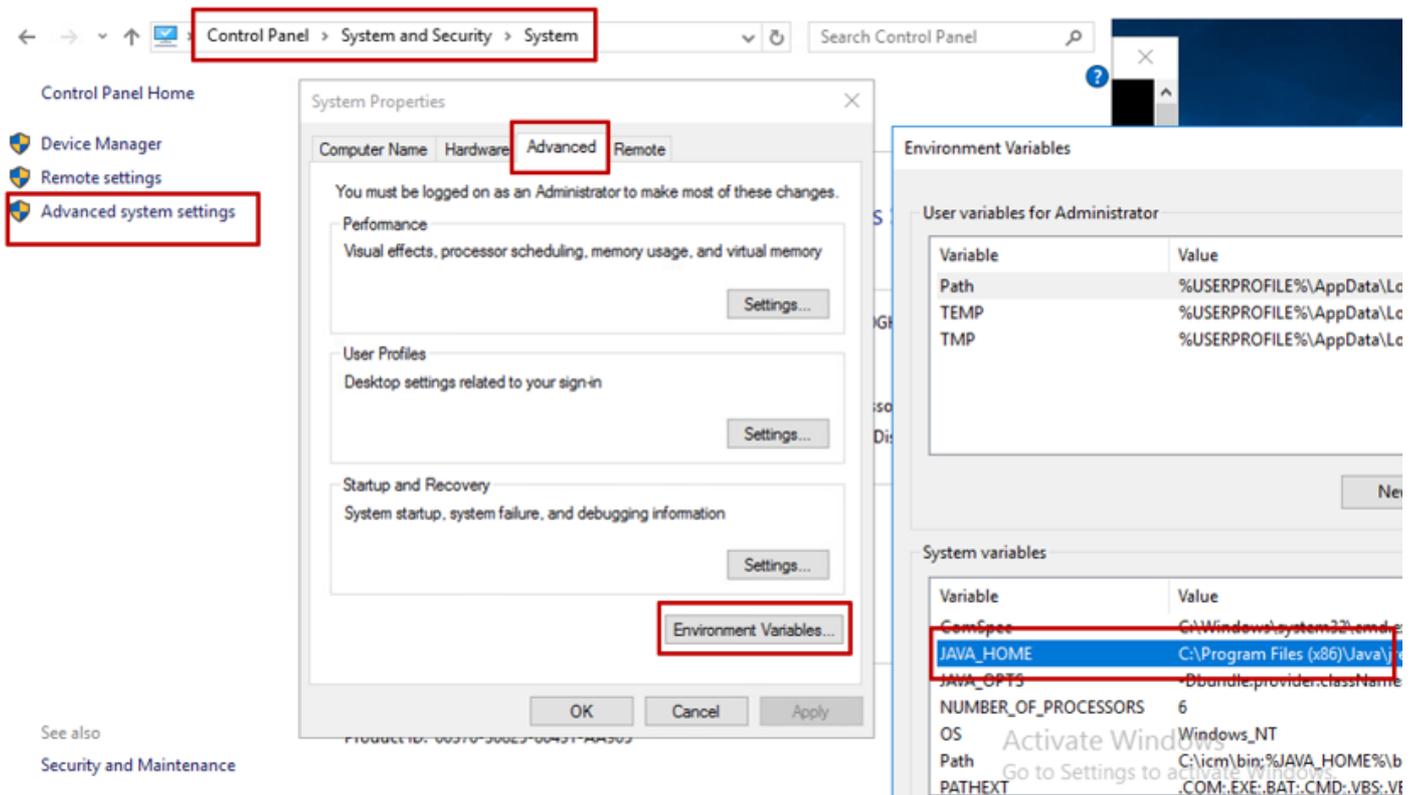
步驟1.瞭解Java主目錄路徑，以確保Java金鑰工具位於何處。您可以通過幾種方法查詢java home路徑。

選項1: CLI命令:echo %JAVA\_HOME%



```
C:\>echo %java_home%  
C:\Program Files (x86)\Java\jre1.8.0_221
```

選項2：通過高級系統設定手動操作，如下圖所示



註：在UCCE 12.5上，預設路徑為C:\Program Files(x86)\Java\jre1.8.0\_221\bin。但是，如果您已使用12.5(1a)安裝程式或安裝了12.5 ES55（必需OpenJDK ES），則使用CCE\_JAVA\_HOME而不是JAVA\_HOME，因為資料儲存路徑已使用OpenJDK進行了更改。有關在CCE和CVP中進行OpenJDK遷移的詳細資訊，請參閱以下文檔：[在CCE 2.5\(1\)中安裝和遷移到OpenJDK](#)和[在CVP 12.5\(1\)中安裝和遷移到OpenJDK](#)。

步驟 2. 從C:\Program Files(x86)\Java\jre1.8.0\_221\lib\security資料夾備份cacerts檔案。您可以將其複製到其他位置。

步驟 3. 以管理員身份開啟命令視窗以運行命令：

```
keytool.exe -keystore ./cacerts -import -file <path where the Root, or Intermediate certificate are stored>
```

註：所需的特定憑證取決於您用於簽署憑證的CA。在雙層CA中（這是公共CA的典型例子，且比內部CA更安全），則需要匯入根憑證和中間憑證。在沒有中間體的獨立CA中（通常在實驗室或更簡單的內部CA中看到），只需要匯入根證書。

## CVP解決方案

### 1. 使用FQDN生成證書

以下過程介紹了如何使用FQDN為Web服務管理器(WSM)、語音XML(VXML)、呼叫伺服器和管理(OAMP)服務生成證書。

---

 注意：安裝CVP時，證書名稱僅包括伺服器名稱，而不包括FQDN，因此，需要重新生成證書。

---

 注意：開始之前，必須執行以下操作：

1. 獲取金鑰庫密碼。運行命令：其他%`CVP_HOME%`\conf\security.properties。運行keytool命令時需要此密碼。
  2. 將%`CVP_HOME%`\conf\security資料夾複製到另一個資料夾。
  3. 以管理員身份開啟命令視窗以運行命令。
- 

## CVP伺服器

步驟 1. 要刪除CVP伺服器證書，請運行以下命令：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a  
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a  
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
```

出現提示時輸入金鑰庫密碼。

步驟 2. 要生成WSM證書，請運行以下命令：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair
```

出現提示時輸入金鑰庫密碼。

---

 註：預設情況下，生成的證書為兩年。使用 `— validity XXXX` 設定重新生成證書時的到期日期，否則證書的有效期為90天，並且需要在此時間之前由CA簽名。對於大多數此類證書，3-5年必須是合理的驗證時間。

---

以下是一些標準有效性輸入：

一年	365
兩年	730
三年	1095

四年	1460
五年	1895
十年	3650

 注意：在12.5證書中必須是SHA 256、金鑰大小2048和加密演算法RSA，請使用以下引數設定這些值：-keyalg RSA和 — keysize 2048。CVP金鑰庫命令必須包括 — storetype JCEKS引數。如果不這樣做，則證書、金鑰或更糟的金鑰庫可能會損壞。

指定伺服器的FQDN，在問題中您的名字和姓是什麼？

```
C:\Cisco\CVP\jre\bin>keytool.exe -genkeypair -v -storetype JCEKS -keystore c:\Cisco\CVP\conf\security\keystore -alias w
in_certificate1 -keysize 2048 -keyalg RSA
Enter keystore password:
What is your first and last name?
 [unknown]: cvp.bona.com
What is the name of your organizational unit?
 [unknown]:
```

請完成以下其他問題：

您的組織單位名稱是什麼？

[未知]: <指定OU>

貴公司的名稱是什麼？

[未知]: <指定組織的名稱>

您的城市或地區名稱是什麼？

[未知]: <指定城市/地區名稱>

您所在州或省份的名稱是什麼？

[未知]: <指定省/市/自治區名稱>

此裝置的國碼（兩個字母）是什麼？

[未知]: <指定雙字母國家/地區代碼>

為接下來的兩個輸入指定yes。

步驟 3.對vxml\_certificate和callserver\_certificate執行相同的步驟：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -genkeypai
```

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -genkeypai
```

## CVP報告伺服器

步驟 1.要刪除WSM和報告伺服器證書，請運行以下命令：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -delete -a  
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -delete -a
```

出現提示時輸入金鑰庫密碼。

步驟 2.要生成WSM證書，請運行以下命令：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -genkeypair
```

出現提示時輸入金鑰庫密碼。

為查詢指定伺服器的FQDN(您的名字和姓氏是什麼)，然後繼續執行與CVP伺服器相同的步驟。

步驟 3.對callserver\_certificate執行相同步驟：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -genkeypair
```

## CVP OAMP ( UCCE部署 )

由於在PCCE解決方案版本12.x中，該解決方案的所有元件都由SPOG控制，並且未安裝OAMP，因此僅對於UCCE部署解決方案需要執行這些步驟。

步驟 1.要刪除WSM和OAMP伺服器證書，請運行以下命令：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -delete -a  
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -delete -a
```

出現提示時輸入金鑰庫密碼。

步驟 2.要生成WSM證書，請運行以下命令：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair
```

出現提示時輸入金鑰庫密碼。

為查詢指定伺服器的FQDN(您的名字和姓氏是什麼)，然後繼續執行與CVP伺服器相同的步驟。

步驟 3.對oamp\_certificate執行相同步驟：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair
```

出現提示時輸入金鑰庫密碼。

## 2.產生CSR

---

 注意：與RFC5280相容的瀏覽器要求每個證書中都包含主體替代名稱(SAN)。在產生CSR時，可以使用SAN的 `-ext` 引數完成此操作。

---

### 主題替代名稱

`-ext` 引數允許使用者使用特定的擴展。顯示的示例將新增一個主題替代名稱(SAN)，該名稱帶有伺服器的完全限定域名(FQDN)以及localhost。其他SAN欄位可以新增為逗號分隔值。

有效的SAN型別包括：

```
ip:192.168.0.1  
dns:myserver.mydomain.com  
email:name@mydomain.com
```

例如：`-ext san=dns:mycwp.mydomain.com,dns:localhost`

### CVP伺服器

步驟 1.生成別名的證書請求。運行此命令並將其儲存到檔案(例如wsm\_certificate)：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -
```

出現提示時輸入金鑰庫密碼。

步驟 2.對vxml\_certificate和callserver\_certificate執行相同的步驟：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -certreq -
```

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -certreq -
```

出現提示時輸入金鑰庫密碼。

## CVP報告伺服器

步驟 1.生成別名的證書請求。運行此命令並將其儲存到檔案（例如wsmreport\_certificate）：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -certreq -
```

出現提示時輸入金鑰庫密碼。

步驟 2.對callserver\_certificate執行相同步驟：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -certreq -
```

出現提示時輸入金鑰庫密碼。

## CVP OAMP ( UCCE部署 )

步驟 1.生成別名的證書請求。運行此命令並將其儲存到檔案（例如oamp\_certificate）：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -certreq -
```

Ensure to replace "mycvp.mydomain.com" with your OAMP FQDN.

Enter the keystore password when prompted.

步驟 2.對oamp\_certificate執行相同步驟：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -certreq -
```

出現提示時輸入金鑰庫密碼。

### 3. 獲取CA簽名的證書

步驟 1. 在CA上簽署證書 ( CVP伺服器的WSM、Callserver和VXML伺服器；CVP OAMP伺服器的WSM和OAMP，以及報告伺服器的WSM和Callserver )。

步驟 2. 從CA頒發機構下載應用程式證書和根證書。

步驟 3. 將根證書和CA簽名的證書複製到每台伺服器的%CVP\_HOME%\conf\security\資料夾中。

### 4. 匯入CA簽名證書

將這些步驟應用於CVP解決方案的所有伺服器。 僅需要匯入該伺服器上元件的證書的CA簽名證書。

步驟 1. 匯入根證書。運行此命令：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v
```

出現提示時輸入金鑰庫密碼。在Trust this certificate提示符下，鍵入Yes。

如果有中間證書，請運行以下命令：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias intermediate_ca -file
```

出現提示時輸入金鑰庫密碼。在Trust this certificate提示符下，鍵入Yes。

步驟 2. 為該伺服器證書 ( CVP、Reporting和OAMP ) 匯入CA簽名的WSM。運行此命令：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v
```

出現提示時輸入金鑰庫密碼。在Trust this certificate提示符下，鍵入Yes。

步驟 3. 在CVP伺服器和報告伺服器中，匯入Callserver CA簽名證書。運行此命令：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v
```

出現提示時輸入金鑰庫密碼。在Trust this certificate提示符下，鍵入Yes。

步驟 4.在CVP伺服器中匯入VXML伺服器CA簽名證書。運行此命令：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v
```

步驟 5.在CVP OAMP伺服器 ( 僅適用於UCCE ) 中匯入OAMP伺服器CA簽名證書。運行此命令：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v
```

步驟 6.重新啟動伺服器。

 注意：在UCCE部署中，確保使用生成CSR時提供的FQDN在CVP OAMP中新增伺服器 ( 報告、CVP伺服器等 )。

## VOS伺服器

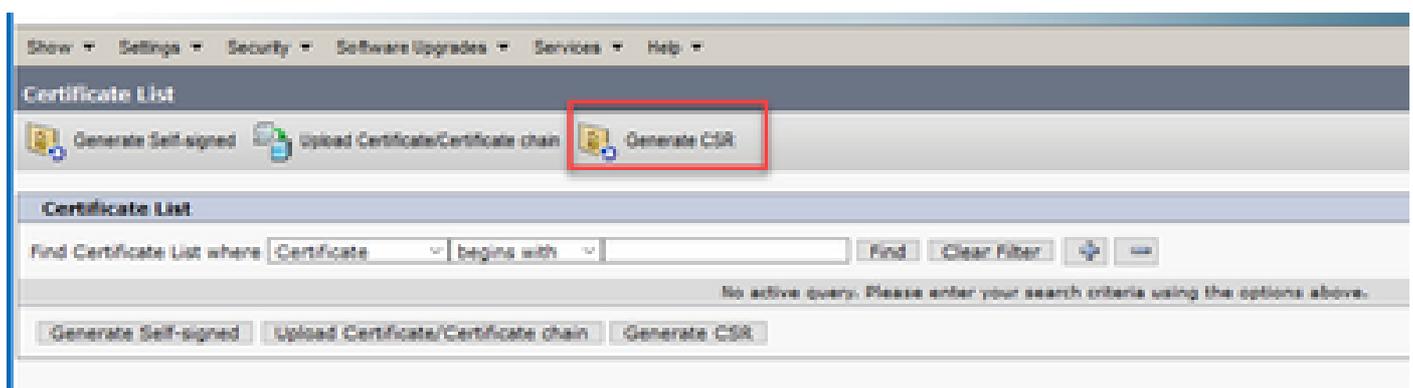
### 1.生成CSR證書

此程式說明如何從基於思科語音作業系統(VOS)的平台產生Tomcat CSR憑證。此過程適用於所有基於VOS的應用程式，例如：

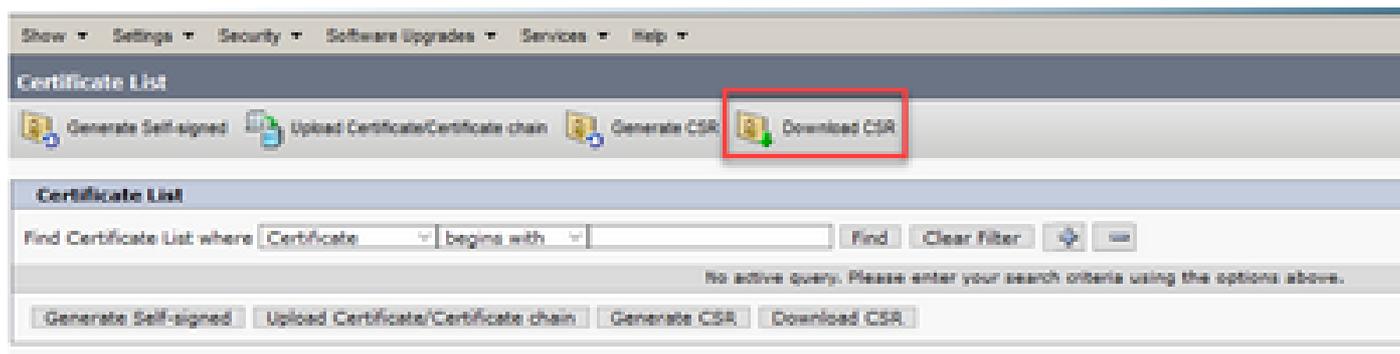
- CUCM
- Finesse
- CUIC \即時資料(LD)\身份伺服器(IDS)
- 雲端連線
- Cisco VVB

步驟 1.導航至Cisco Unified Communications Operating System Administration頁面：<https://FQDN:<8443或443>/cmplatform>。

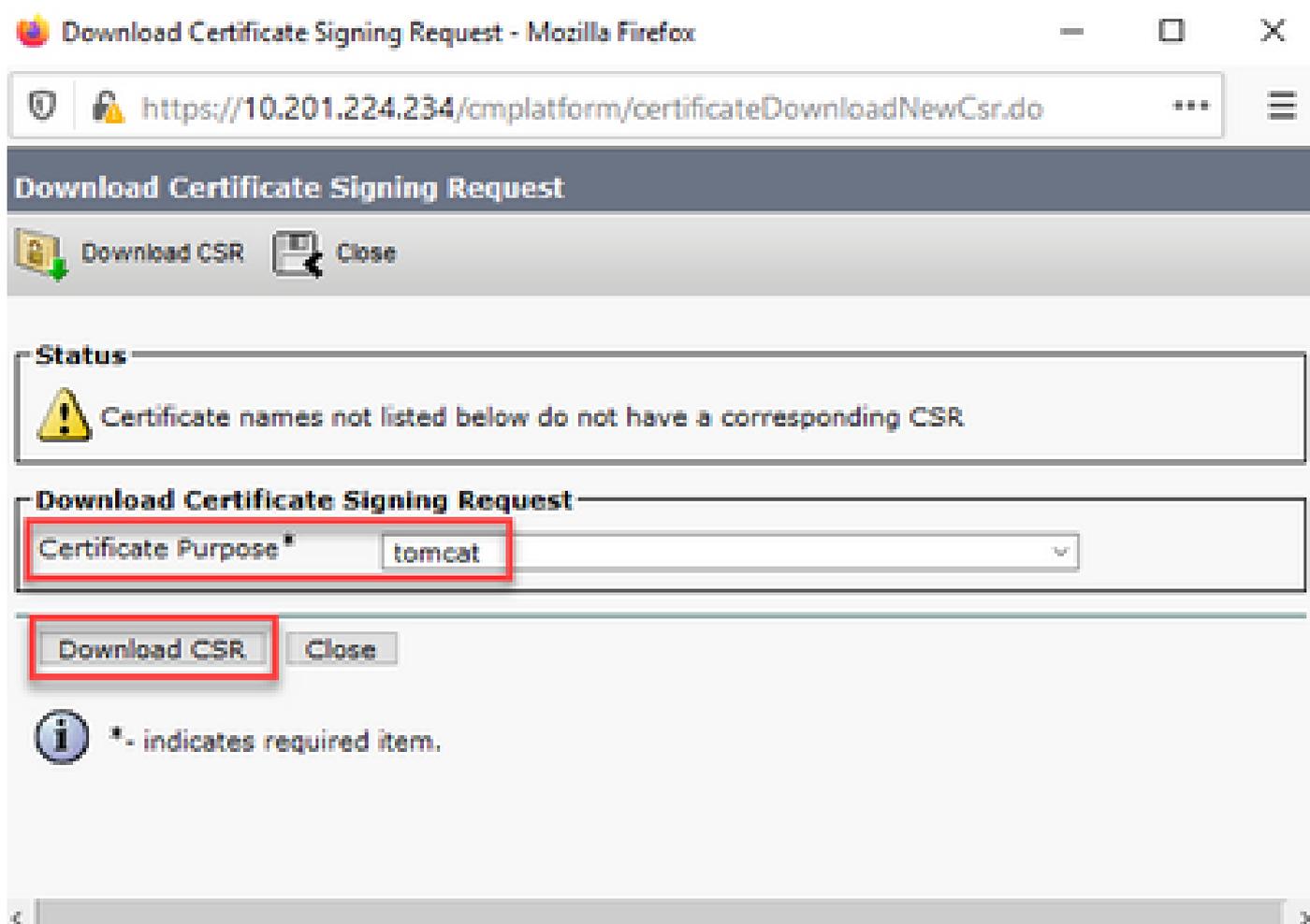
步驟 2.導覽至Security > Certificate Management，然後選擇Generate CSR。



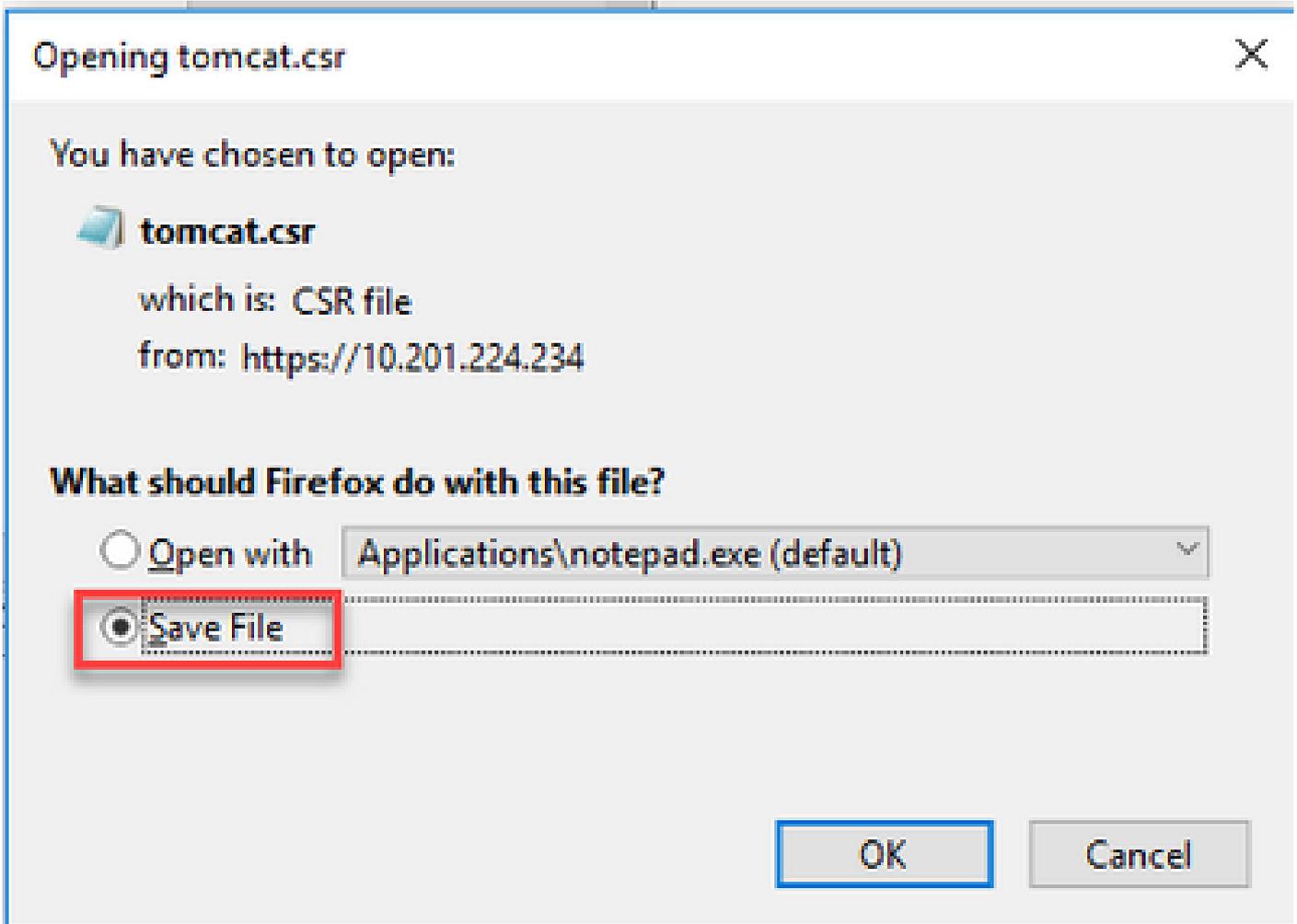
步驟 3.產生CSR憑證後，關閉視窗並選擇下載CSR。



步驟 4.確保證書用途為tomcat，然後按一下Download CSR。



步驟 5.按一下「Save File」。檔案儲存在Download資料夾中。



## 2. 獲取CA簽名的證書

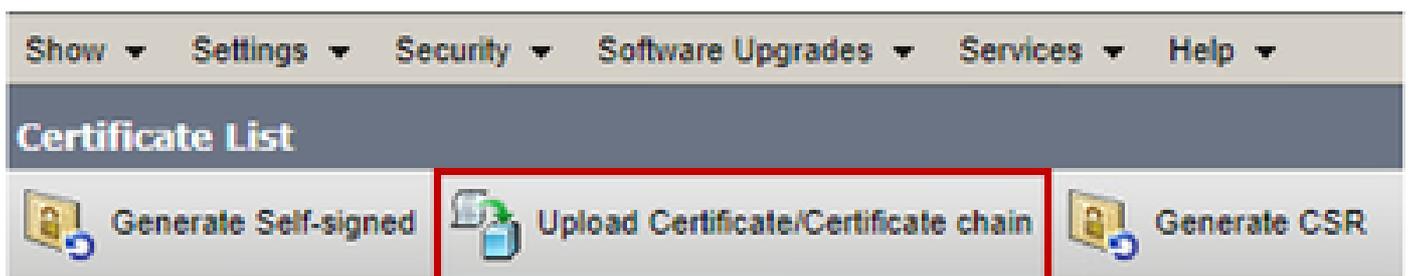
步驟 1. 在CA上匯出的tomcat證書上簽名。

步驟 2. 從CA機構下載應用程式和根證書。

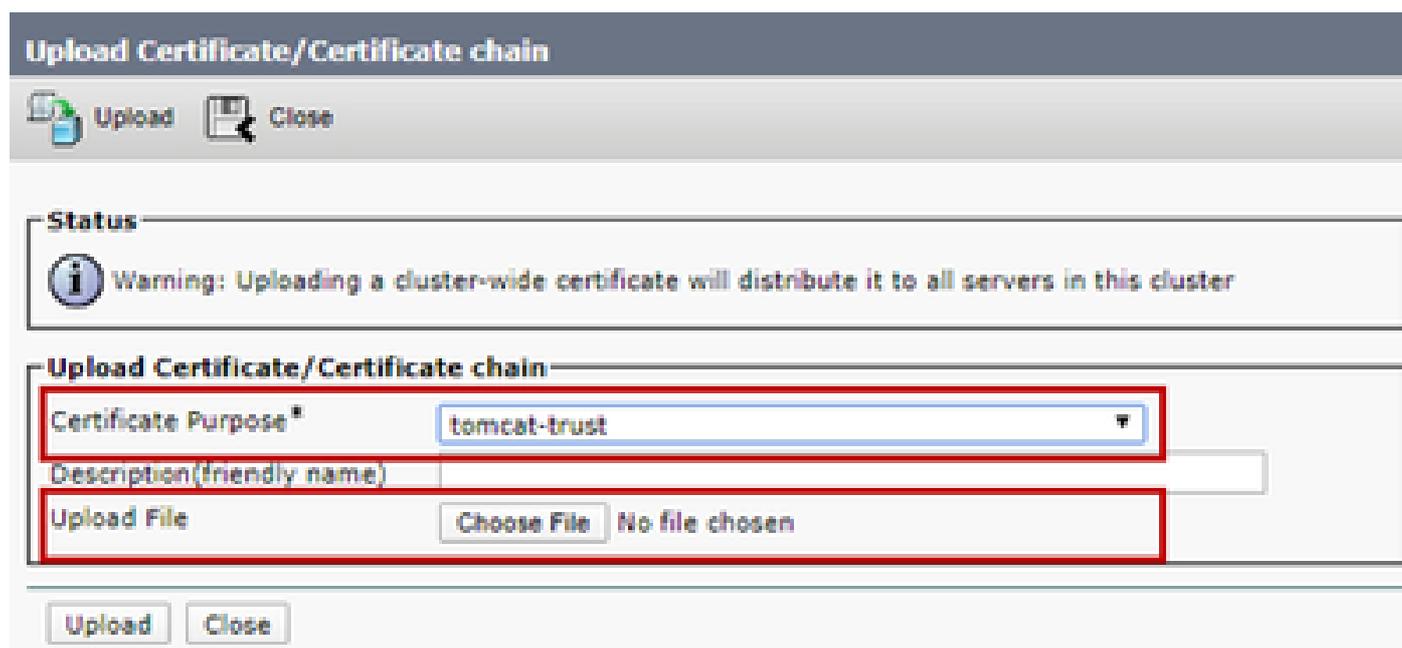
## 3. 上傳應用程式和根證書

步驟 1. 導航至Cisco Unified Communications Operating System Administration頁面：  
：<https://FQDN:<8443或443>/cmplatform>。

步驟 2. 導覽至Security > Certificate Management，然後選擇Upload Certificate/Certificate chain。



步驟 3.在「Upload certificate/Certificate chain」視窗上，在「certificate purpose」欄位中選擇 tomcat-trust，然後上傳根憑證。



**Upload Certificate/Certificate chain**

Upload Close

**Status**

**i** Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

**Upload Certificate/Certificate chain**

Certificate Purpose<sup>®</sup> tomcat-trust

Description(friendly name)

Upload File Choose File No file chosen

Upload Close

步驟 4.將中間證書（如果有）上傳為tomcat-trust。

步驟 5.在「Upload certificate/Certificate chain」視窗上，在「Certificate Purpose」欄位中選擇 now tomcat，並上傳應用CA簽名的憑證。

**Upload Certificate/Certificate chain**

Upload Close

**Status**

**i** Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

**Upload Certificate/Certificate chain**

Certificate Purpose <sup>*</sup>	tomcat
Description(friendly name)	Self-signed certificate
Upload File	Browse... No file selected.

Upload Close

**i** <sup>\*</sup> - indicates required item.

步驟 6.重新啟動伺服器。

## 驗證

重新啟動伺服器後，執行以下步驟以驗證CA簽名的實現：

步驟 1.開啟Web瀏覽器並清除快取。

步驟 2.關閉並再次開啟瀏覽器。

現在，您必須看到證書開關以開始CA簽名的證書，並且瀏覽器視窗中指示證書是自簽名的，因此不受信任，必須離開。

## 疑難排解

本指南中沒有用於排除CA簽名證書實施故障的步驟。

## 相關資訊

- CVP配置指南：[CVP配置指南 — 安全](#)
- UCCE配置指南：[UCCE配置指南 — 安全](#)
- PCCE管理指南：[PCE管理指南 — 安全](#)
- UCCE自簽名證書：[Exchange UCCE自簽名證書](#)

- PCCE自簽名證書：[Exchange PCCE自簽名證書](#)
- 在CCE 12.5(1)中安裝和遷移到OpenJDK:[CCE OpenJDK遷移](#)
- 在CVP 12.5(1)中安裝和遷移到OpenJDK:[CVP OpenJDK遷移](#)

[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）。