

# 配置Finesse和CTI伺服器之間的安全通訊

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[CCE CTI伺服器安全](#)

[Finesse安全配置](#)

[生成代理PG證書 \(CTI伺服器\)](#)

[獲取CA簽名的CSR證書](#)

[匯入CCE PG的CA簽名證書](#)

[生成Finesse證書](#)

[由CA簽署Finesse證書](#)

[匯入Finesse應用程式和根簽名的證書](#)

[驗證](#)

[疑難排解](#)

## 簡介

本檔案介紹如何在Cisco Contact Center Enterprise(CCE)解決方案中的Cisco Finesse和Computer Telephony Integration(CTI)伺服器之間實作憑證授權單位(CA)簽署的憑證。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- CCE版本12.0(1)
- Finesse版本12.0(1)
- CTI伺服器

### 採用元件

本檔案中的資訊是根據以下軟體版本：

- 套裝CCE(PCCE)12.0(1)
- Finesse 12.0(1)

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

在CCE版本11.5中，思科開始支援傳輸層安全(TLS)版本1.2，該版本允許通過TLS 1.2安全地傳輸會話初始協定(SIP)和即時傳輸協定(RTP)消息。從CCE 12.0開始，作為保護移動資料的一部分，思科開始在大部分聯絡中心呼叫流上支援TLS 1.2:入站和出站語音、多通道和外部資料庫。本文的重點是入站語音，特別是Finesse和CTI伺服器之間的通訊。

CTI伺服器支援以下連線模式：

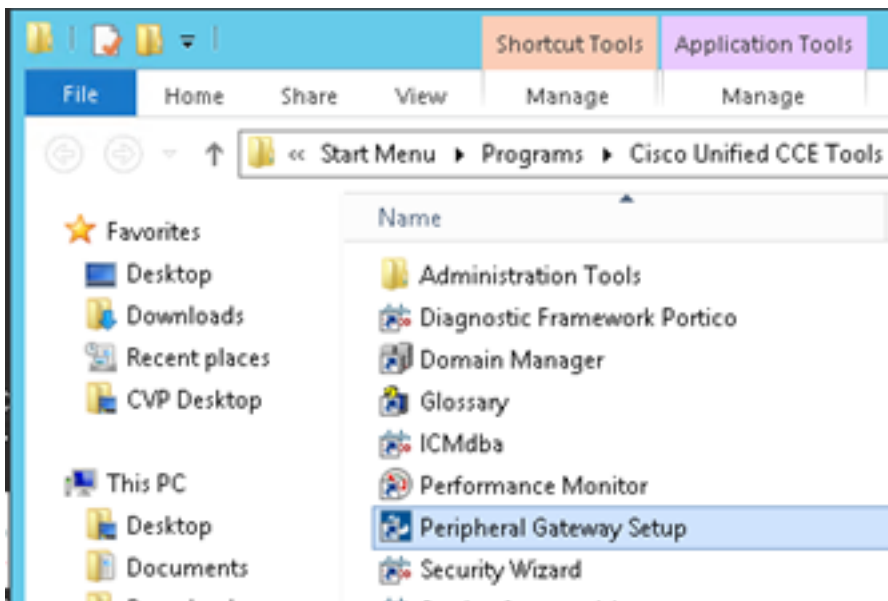
- **僅安全連線**:允許在CTI伺服器和CTI客戶端 ( Finesse、撥號器、CTIOS和ctitest ) 之間進行安全連線。
- **安全連線和非安全連線 ( 混合模式 )**：允許在CTI伺服器和CTI客戶端之間進行安全連線和非安全連線。這是預設連線模式。將先前版本升級到CCE 12.0(1)時將配置此模式。

附註：不支援僅非安全模式。

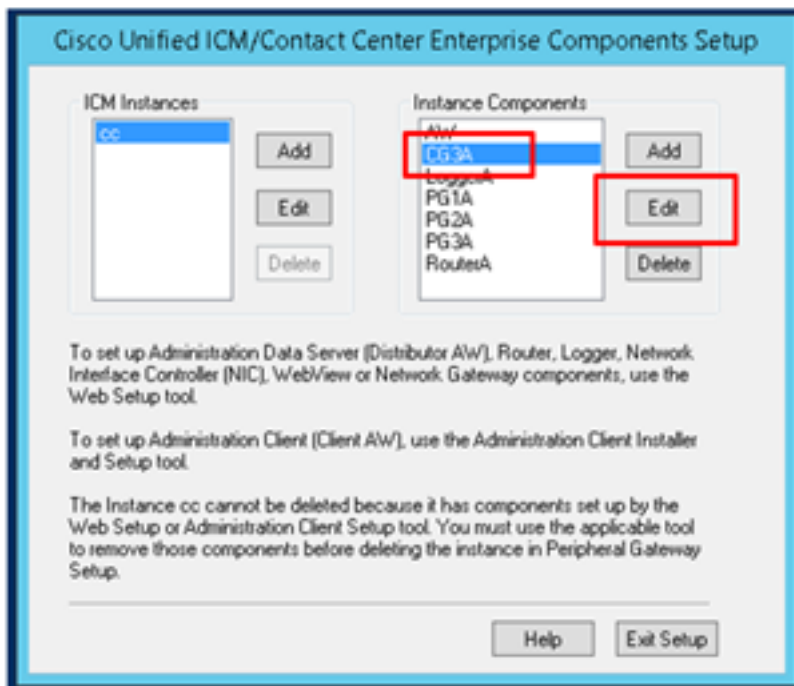
## 設定

### CCE CTI伺服器安全

步驟1.在PCCE管理工作站(AW)上，開啟Unified CCE Tools資料夾，然後按兩下Peripheral Gateway Setup。

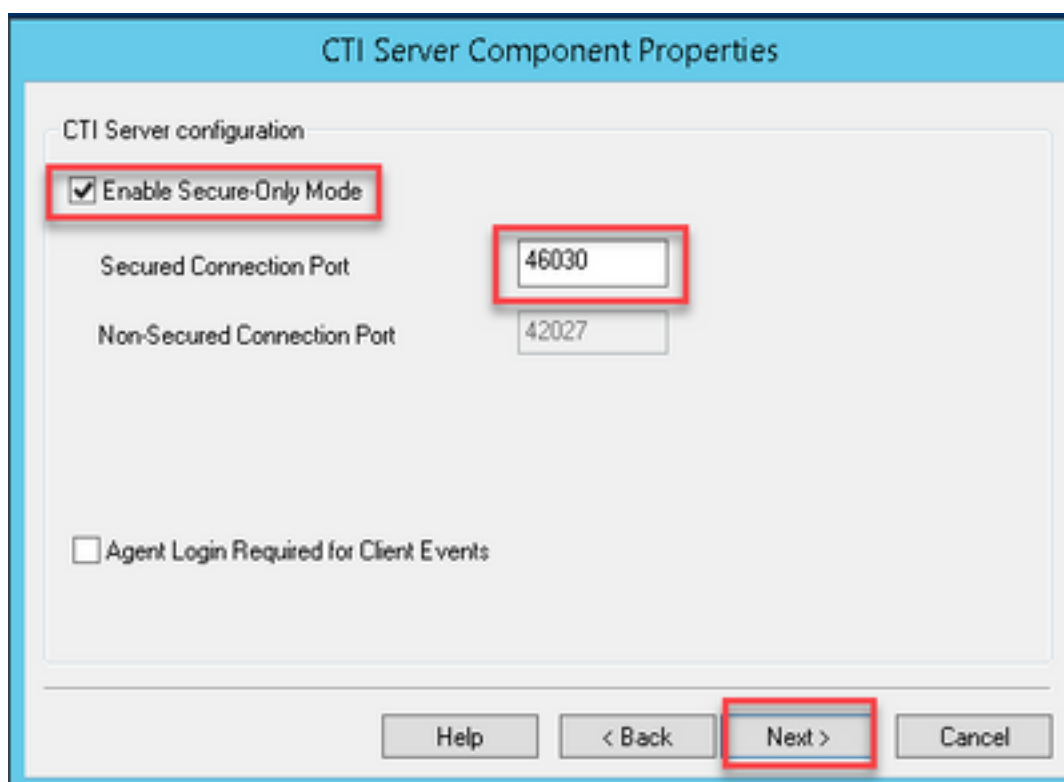


步驟2.選擇CG3A，然後按一下Edit。



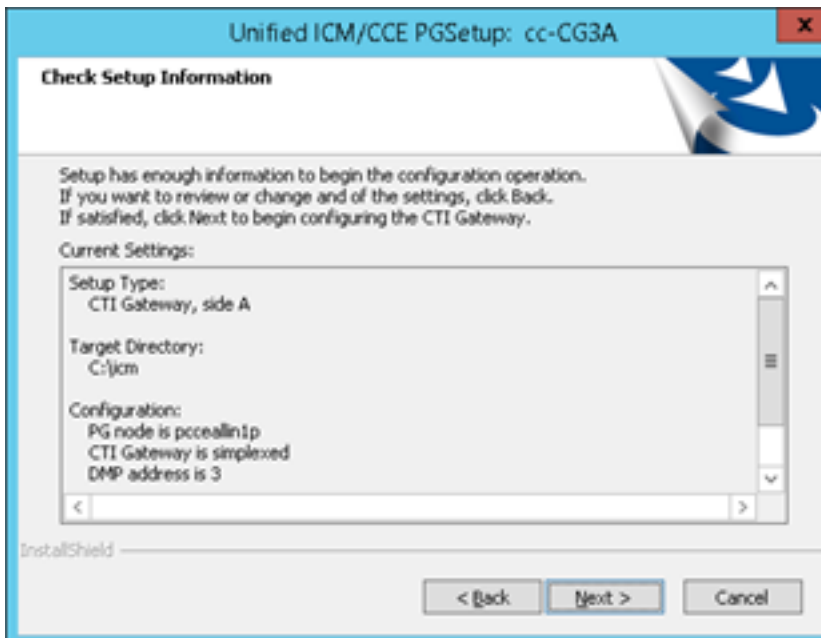
步驟3.在CTI伺服器屬性上，按一下下一步。有關設定停止CG3A服務的問題，請選擇Yes。

步驟4.在CTI伺服器元件屬性上，選擇啟用僅安全模式。請注意安全連線埠(46030)，因為在下一個練習中，您必須在Finesse中配置相同的埠。按「Next」（下一步）。

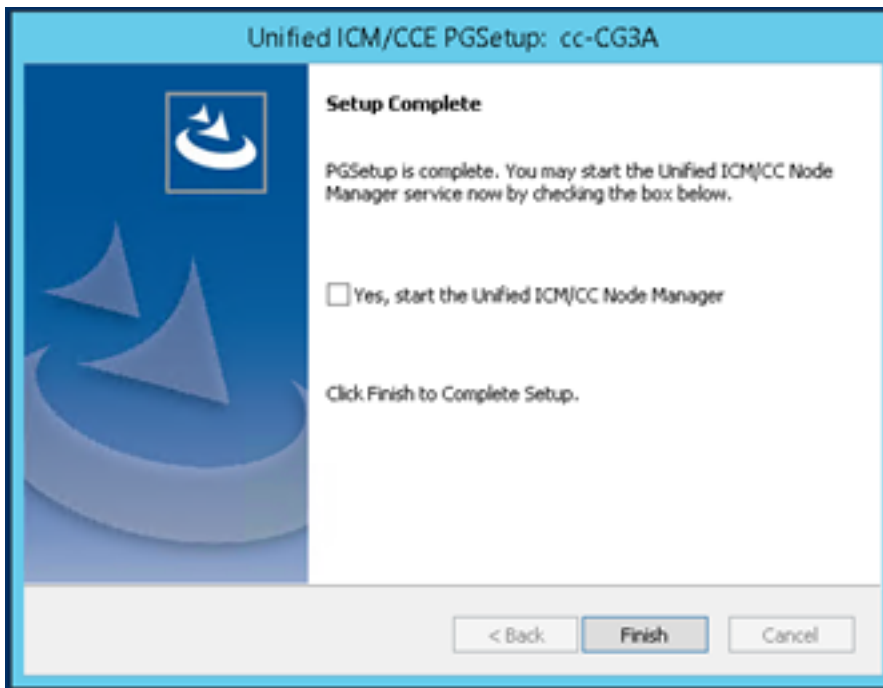


附註：預設安全通訊為42030，但本文檔使用的實驗為40630。埠號是包括ICM系統ID的公式的一部分。當系統id為1(CG1a)時，預設埠號通常為42030。由於實驗中的系統id為3(CG3a)，因此預設埠號為46030。

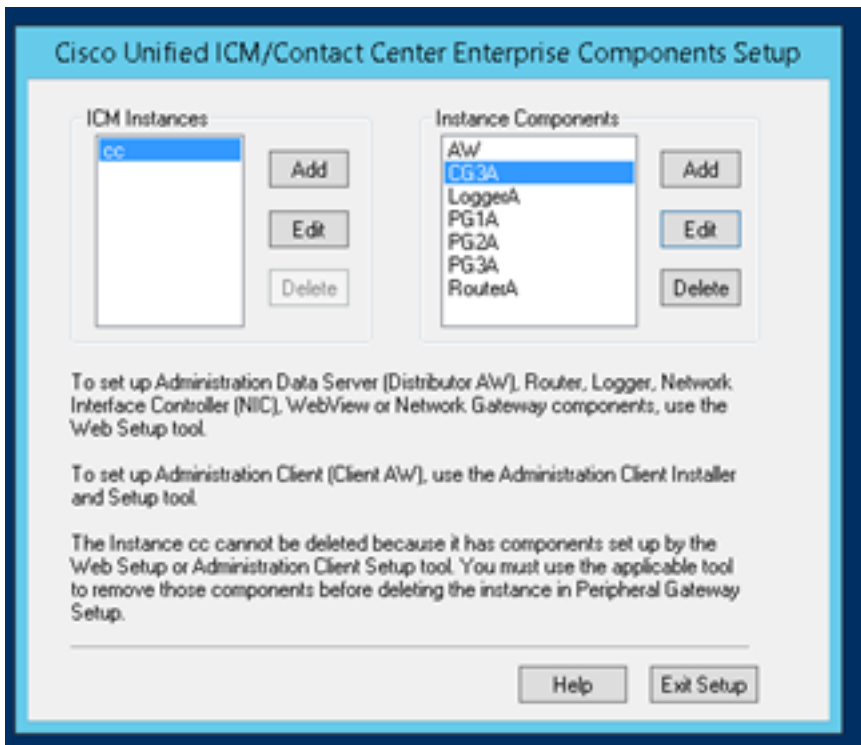
步驟5.在CTI Network Interface Properties上，按一下「Next」。檢查Setup Information，然後按一下Next。



步驟6.按一下Finish，如下圖所示。



步驟7.按一下Exit Setup，並等待設定視窗關閉為止，如下圖所示。



步驟8.在PCCEAIn1案頭上，按兩下**Unified CCE service Control**。

步驟9.選擇Cisco ICM cc CG3A，然後按一下**Start**。

## Finesse安全配置

步驟1.開啟Web瀏覽器並導航至**Finesse Administration**。

步驟2.向下滾動至**Contact Center Enterprise CTI Server Settings**部分，如下圖所示。

步驟3.更改在上一個練習中在CG3A上配置的安全通訊埠的A側埠：46030。選中**Enable SSL encryption**，然後點選**Save**。

Contact Center Enterprise CTI Server Settings

Note: Any changes made to the settings on this gadget require a restart of Cisco Finesse Tomcat to take effect.

Contact Center Enterprise CTI Server Settings

A Side Host/IP Address*	<input type="text" value="10.10.10.10"/>	B Side Host/IP Address	<input type="text"/>
A Side Port*	<input type="text" value="46030"/>	B Side Port	<input type="text"/>
Peripheral ID*	<input type="text" value="5000"/>		

Enable SSL encryption

附註：為了測試連線，您需要先重新啟動Finesse Tomcat服務或重新啟動Finesse伺服器。

步驟4.從Finesse管理頁面註銷。

步驟5.使用Finesse開啟SSH會話。

步驟6.在FINESSEA SSH會話上，執行命令：

### utils系統重新啟動

當系統詢問您是否要重新啟動系統時，輸入yes。

```
Using username "administrator".
Command Line Interface is starting up, please wait ...

Welcome to the Platform Command Line Interface

VMware Installation:
 2 vCPU: Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz
 Disk 1: 146GB, Partitions aligned
 8192 Mbytes RAM

admin:utils system restart

Do you really want to restart ?

Enter (yes/no)? yes

Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...
```

### 生成代理PG證書 ( CTI伺服器 )

CiscoCertUtils是在CCE版本12上發佈的新工具。您可以使用此工具管理入站語音的所有CCE證書。在本文中，您使用這些CiscoCertUtils來產生外圍閘道(PG)憑證簽署請求(CSR)。

步驟1. 執行此命令以產生CSR憑證：`CiscocertUtil /generateCSR`

```
C:\Users\Administrator.CC>
C:\Users\Administrator.CC>CiscocertUtil /generateCSR

Key already exists at C:\nicm\ssl\keys\host.key. It will be used to generate the
CSR.

SSL config path = C:\nicm\ssl\cfg\openssl.cfg
SYSTEM command is C:\nicm\ssl\bin\openssl.exe req -new -key C:\nicm\ssl\keys\host.
key -out C:\nicm\ssl\certs\host.csr
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.
```

提供所需的資訊，例如：

國家/地區名稱：美國

省或州名稱：MA

地區名稱：BXB

組織名稱：思科

組織單位：CX

公用名：PCCEAllin1.cc.lab

電子郵件：[jdoe@cc.lab](mailto:jdoe@cc.lab)

質詢密碼：火車1ng!

可選的公司名稱：思科

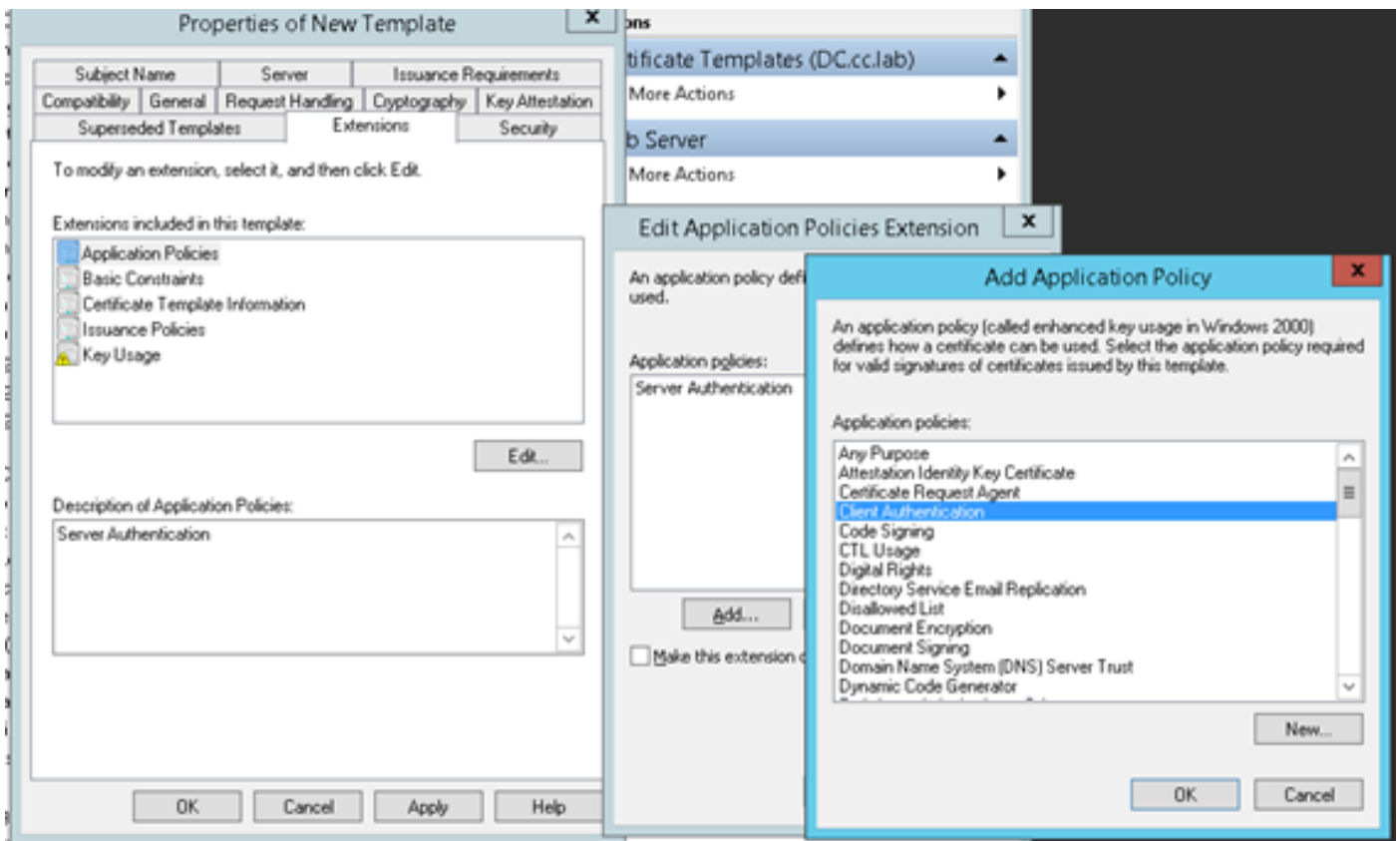
主機證書和金鑰儲存在C:\nicm\ssl\certs和C:\nicm\ssl\keys中。

步驟2. 導覽至C:\nicm\ssl\certs資料夾，並確保已產生host.csr檔案。

## 獲取CSR證書 由CA簽署

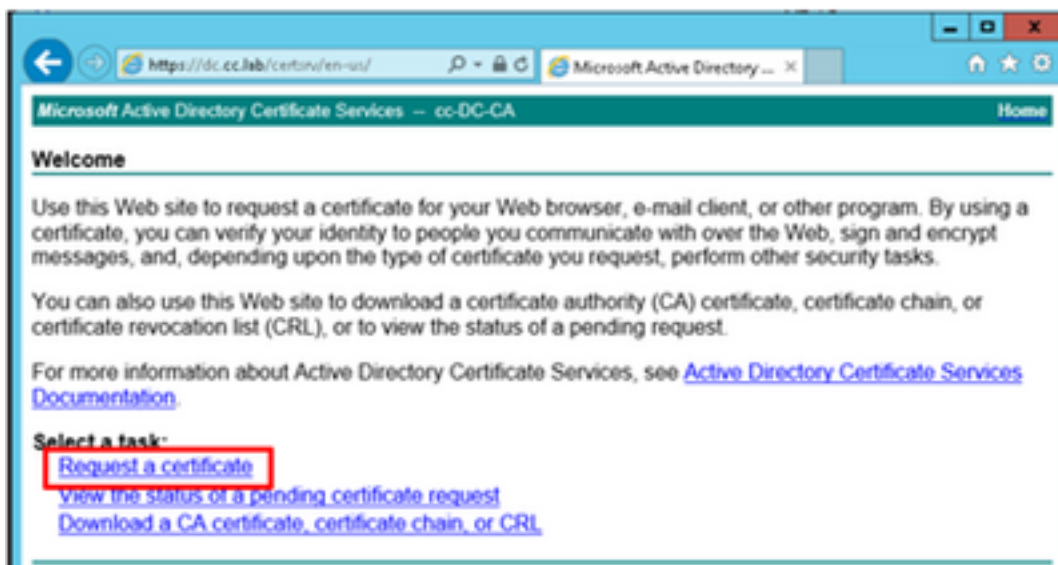
產生CSR憑證後，需要由第三方CA簽署。在本練習中，安裝在域控制器中的Microsoft CA用作第三方CA。

使用Microsoft CA時，請確保CA使用的證書模板包括客戶端和伺服器身份驗證，如圖所示。



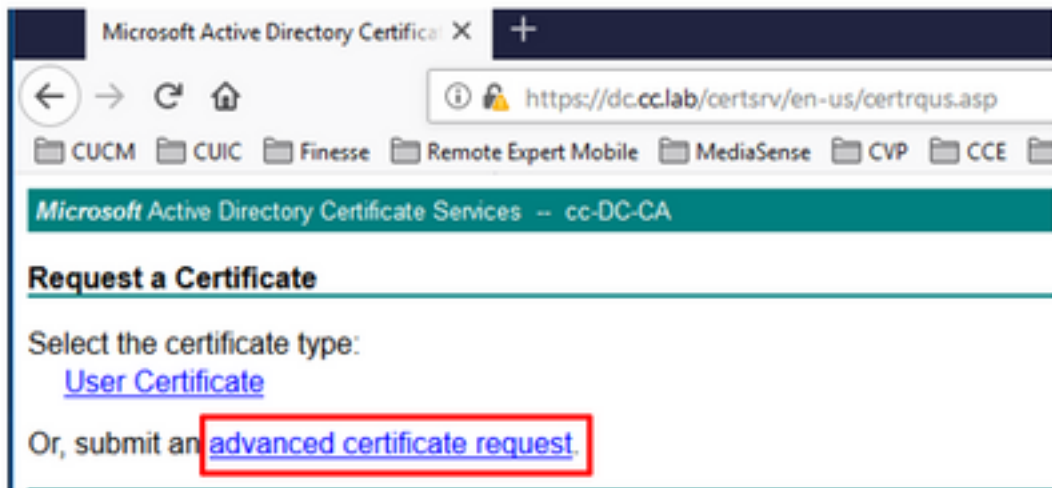
步驟1.開啟Web瀏覽器並導航至CA。

步驟2.在Microsoft Active Directory證書服務上，選擇請求證書。



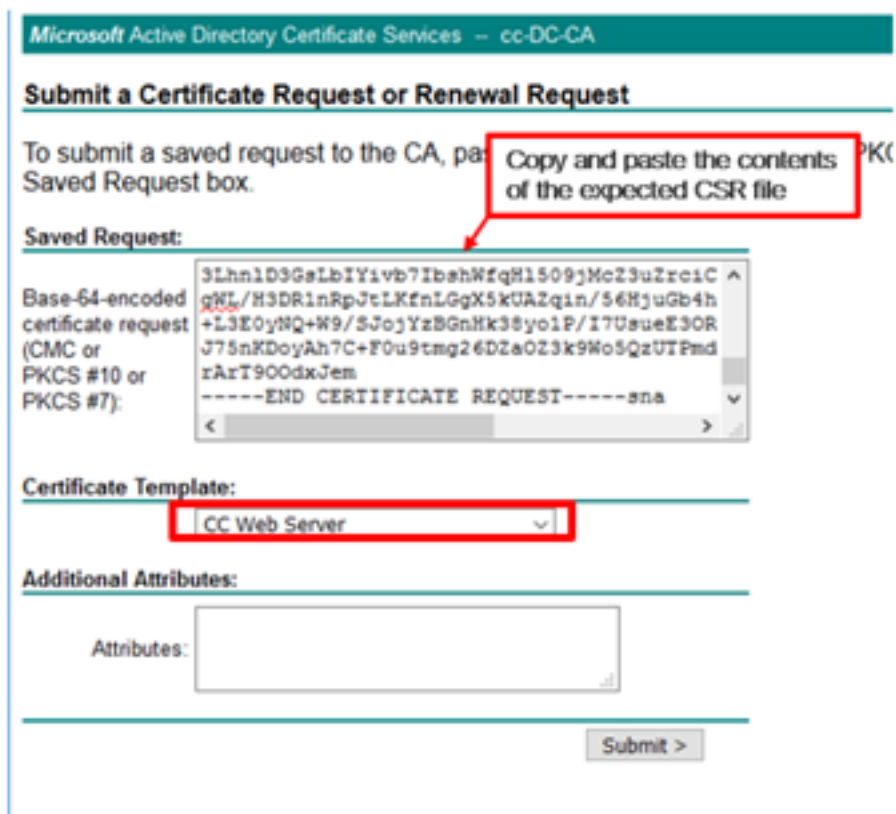
步驟3.選擇advanced certificate request選項。





步驟4.在「advanced certificate request」上，複製並貼上「Saved Request」框中的PG代理CSR證書的內容。

步驟5.選擇具有客戶端和服務器身份驗證的Web Server模板。在實驗中，CC Web Server模板是使用客戶端和伺服器身份驗證建立的。



步驟6.按一下Submit。

步驟7.選擇Base 64 encoded，然後按一下Download Certificate，如下圖所示。

## Certificate Issued

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded



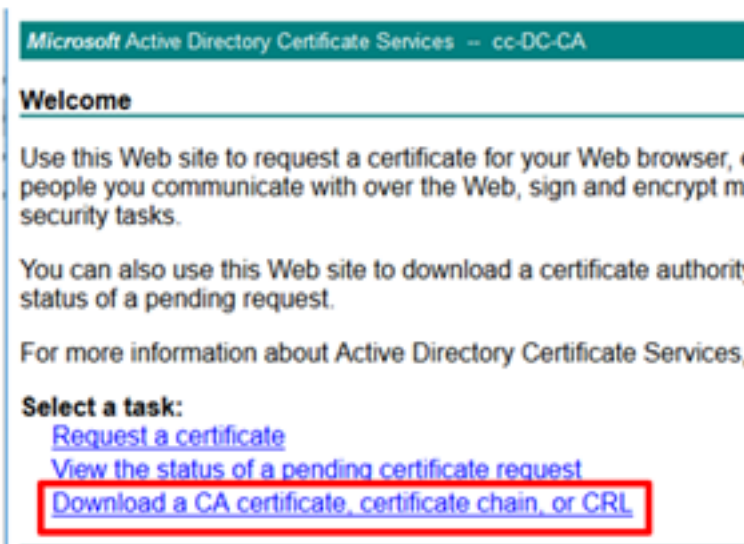
[Download certificate](#)

[Download certificate chain](#)

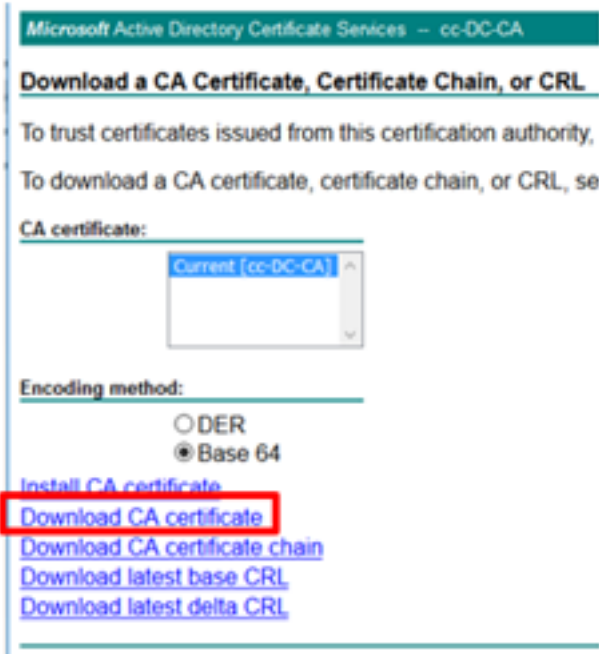
步驟8. 儲存檔案，然後按一下OK。檔案儲存在Downloads資料夾中。

步驟9. 將檔案重新命名為host.cer ( 可選 )。

步驟10. 您還需要生成根證書。返回CA證書頁面，然後選擇下載CA證書、證書鏈或CRL。您只需執行一次此步驟，因為所有伺服器 ( PG代理和Finesse ) 的根證書都相同。

A screenshot of the Microsoft Active Directory Certificate Services website. The page title is "Microsoft Active Directory Certificate Services -- cc-DC-CA". Below the title is a "Welcome" section. The main content area contains the following text: "Use this Web site to request a certificate for your Web browser, e people you communicate with over the Web, sign and encrypt m security tasks." "You can also use this Web site to download a certificate authority status of a pending request." "For more information about Active Directory Certificate Services,". Under the heading "Select a task:", there are three links: "Request a certificate", "View the status of a pending certificate request", and "Download a CA certificate, certificate chain, or CRL". The last link is highlighted with a red rectangular box.

步驟11. 按一下Base 64，然後選擇Download CA certificate。



步驟12.按一下Save File，然後選擇OK。檔案將儲存在預設位置Downloads。

## 匯入CCE PG的CA簽名證書

步驟1. 在PG Agent上，導航至C:\icm\ssl\certs，然後在此處貼上根和PG Agent簽名的檔案。

步驟2.將c:\icm\ssl\certs上的host.pem證書重新命名為selfhost.pem。

步驟3.將c:\icm\ssl\certs資料夾上的host.cer重新命名為host.pem。

步驟4.安裝根證書。在命令提示符下，發出以下命令：**CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer**

```
C:\Users\Administrator.CC>CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer
Install String is certutil -enterprise -addstore -f Root C:\icm\ssl\certs\rootAll.cerRoot "Trusted Root Certification Authorities"
Signature matches Public Key
Related Certificates:
Exact match:
Element 0:
Serial Number: 480a0f1b836a50b54c66a65f5298fae
Issuer: CN=cc-DC-CA, DC=cc, DC=lab
NotBefore: 2/8/2017 3:43 PM
NotAfter: 2/8/2028 3:53 PM
Subject: CN=cc-DC-CA, DC=cc, DC=lab
CA Version: 00.0
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): ec 49 6e f7 cb 9a c0 3a f5 46 2b ae 4f 1f 1b 15 fd 38 81 5f

Certificate "cc-DC-CA" already in store.
CertUtil: -addstore command completed successfully.
C:\Users\Administrator.CC>
```

步驟5. 安裝運行相同命令的應用程式簽名證書：**CiscoCertUtil /install C:\icm\ssl\certs\host.pem**

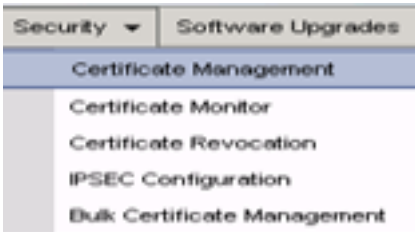
```
C:\Users\Administrator.CC>CiscoCertUtil /install C:\icm\ssl\certs\host.pem
Install String is certutil -enterprise -addstore -f Root C:\icm\ssl\certs\host.p
enRoot "Trusted Root Certification Authorities"
Certificate "PCCALLin1.cc.lab" added to store.
CertUtil: -addstore command completed successfully.
C:\Users\Administrator.CC>
```

步驟6.循環PG。開啟Unified CCE Service Control，然後循環Cisco ICM Agent PG。

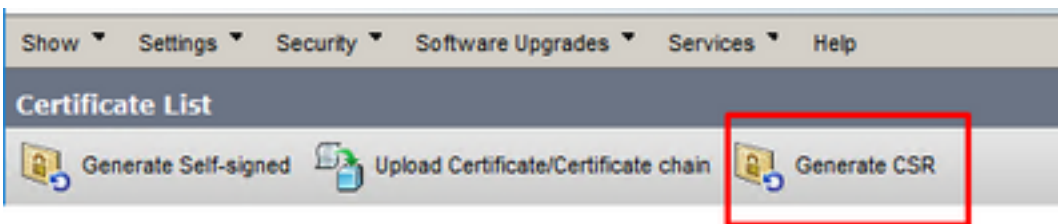
## 生成Finesse證書

步驟1.開啟Web瀏覽器並導航至Finesse OS Admin。

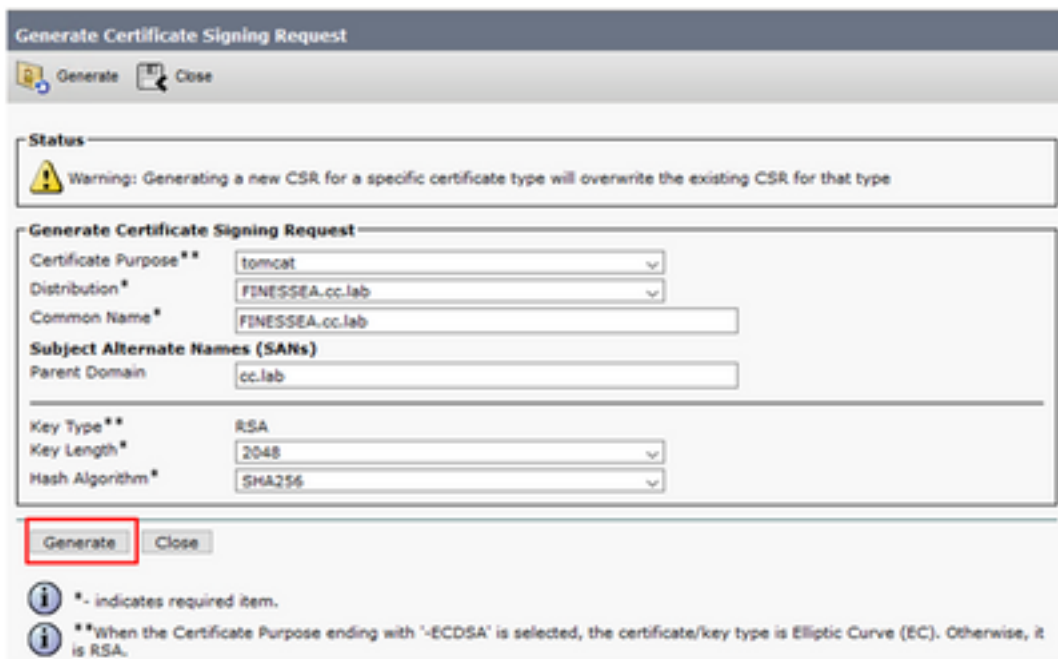
步驟2.使用作業系統管理員憑證登入，然後導覽至Security > Certificate Management，如下圖所示。



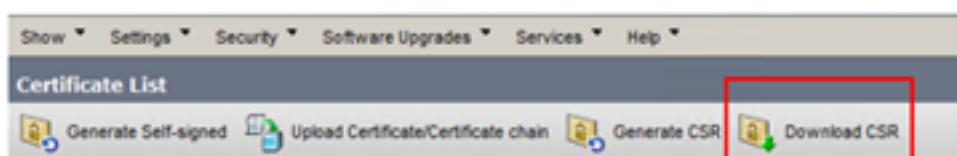
步驟3.按一下Generate CSR，如下圖所示。



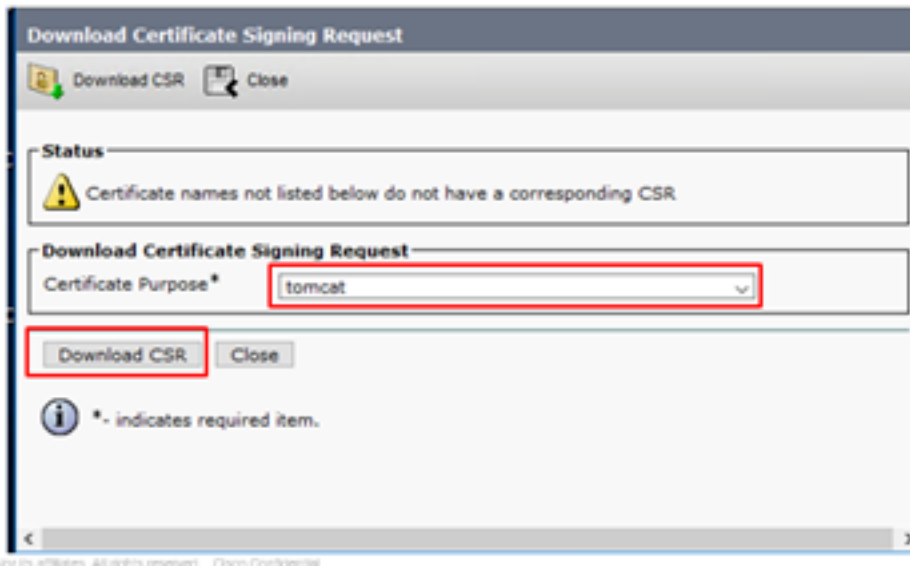
步驟4.在Generate Certificate Signing Request上，使用預設值，然後點選Generate。



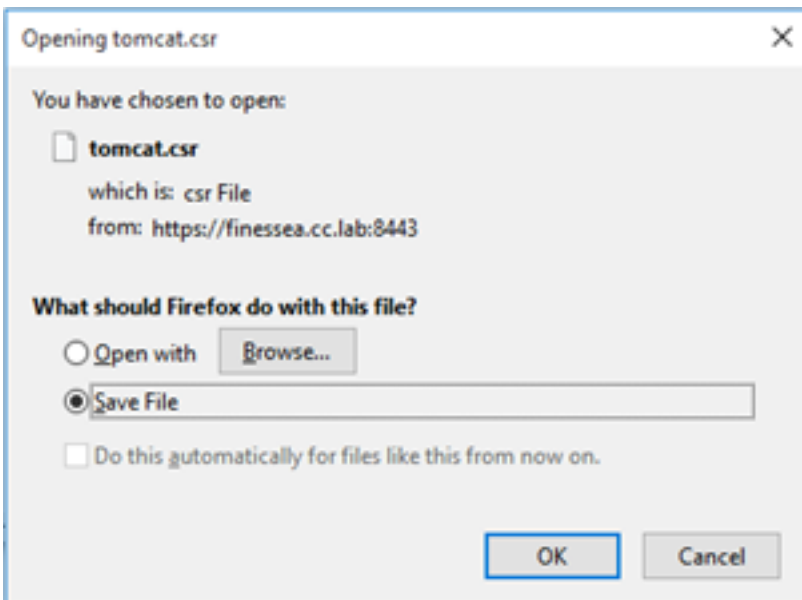
步驟5.關閉Generate Certificate Signing Request視窗並選擇Download CSR。



步驟6.在「憑證用途」上，選擇tomcat，然後按一下Download CSR。



步驟7.選擇Save File，然後按一下OK，如下圖所示。



步驟8.關閉Download Certificate Signing Request視窗。證書儲存在預設位置（此電腦>下載）。

步驟9.開啟Windows資源管理器並導航到該資料夾。按一下右鍵此證書並將其重新命名：  
：finessetomcat.csr

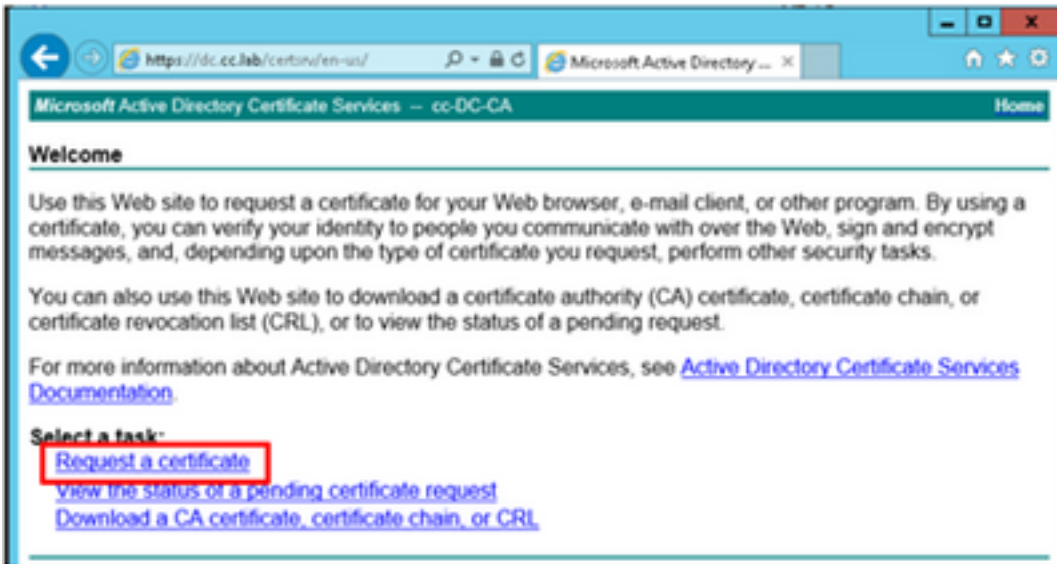
## 由CA簽署Finesse證書

在本節中，使用上一步中使用的Microsoft CA作為第三方CA。

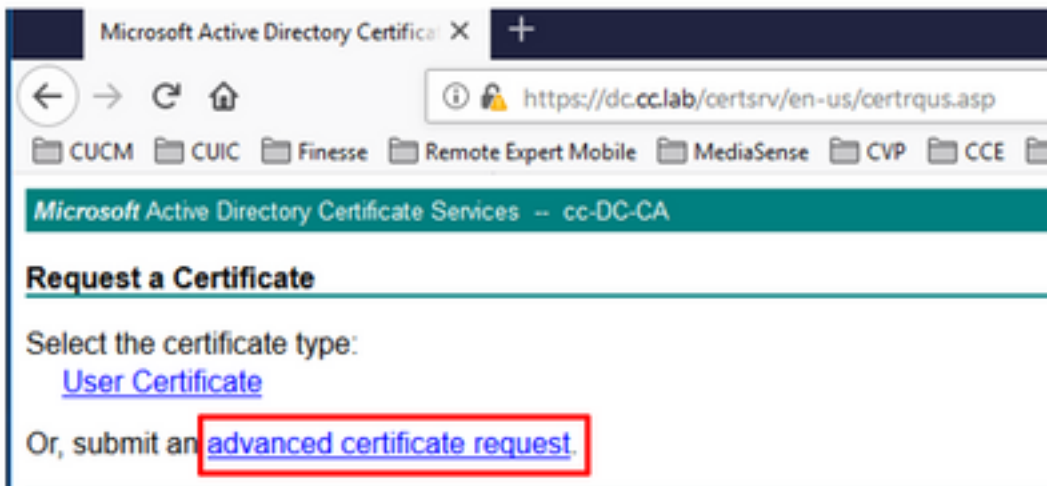
**附註：** 確保CA使用的證書模板包括客戶端和伺服器身份驗證。

步驟1.開啟Web瀏覽器並導航至CA。

步驟2.在Microsoft Active Directory證書服務上，選擇請求證書。



步驟3.選擇advanced certificate request選項，如下圖所示。



步驟4.在進階憑證請求上，複製並貼上Saved Request方塊中Finesse CSR憑證的內容。

步驟5.選擇具有客戶端和伺服器身份驗證的Web伺服器模板。在本實驗中，CC Web Server模板是使用客戶端和伺服器身份驗證建立的。



Microsoft Active Directory Certificate Services -- cc-DC-CA

### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste the contents of the Saved Request box. Copy and paste the contents of the expected CSR file

Saved Request:

```
3Lhn1D3GcLbIY1vb7IbshWfqH1509jMcZ3uZrciC
gKtL/H3DR1nRpJcLKfnLGgX5kUA2qin/56HjuGb4h
+L3E0yNQ+W9/SJoYzBGnHk38yo1P/I7UsueE3OR
J75SnKDoyAh7C+F0u9tmq26DZaOZ3k9No5QzUTPmd
rArT900dxJem
-----END CERTIFICATE REQUEST-----sna
```

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

Certificate Template:  
CC Web Server

Additional Attributes:

Attributes:

步驟6.按一下Submit。


步驟7.選擇Base 64 encoded，然後按一下Download certificate，如下圖所示。

Microsoft Active Directory Certificate Services -- cc-DC-CA

### Certificate Issued

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded

 [Download certificate](#)  
[Download certificate chain](#)

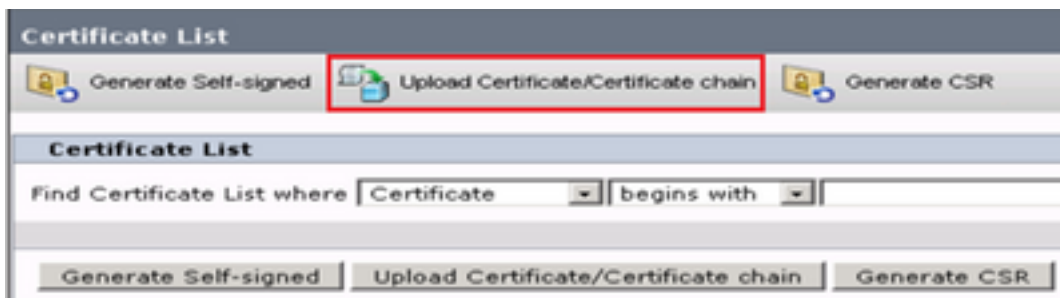
步驟8.儲存檔案，然後按一下OK。檔案儲存在Downloads資料夾中。

步驟9.將檔案重新命名為finesse.cer。

### 匯入Finesse應用程式和根簽名的證書

步驟1. 在Web程式上，開啟Finesse OS Admin頁面並導航至Security> Certificate Management。

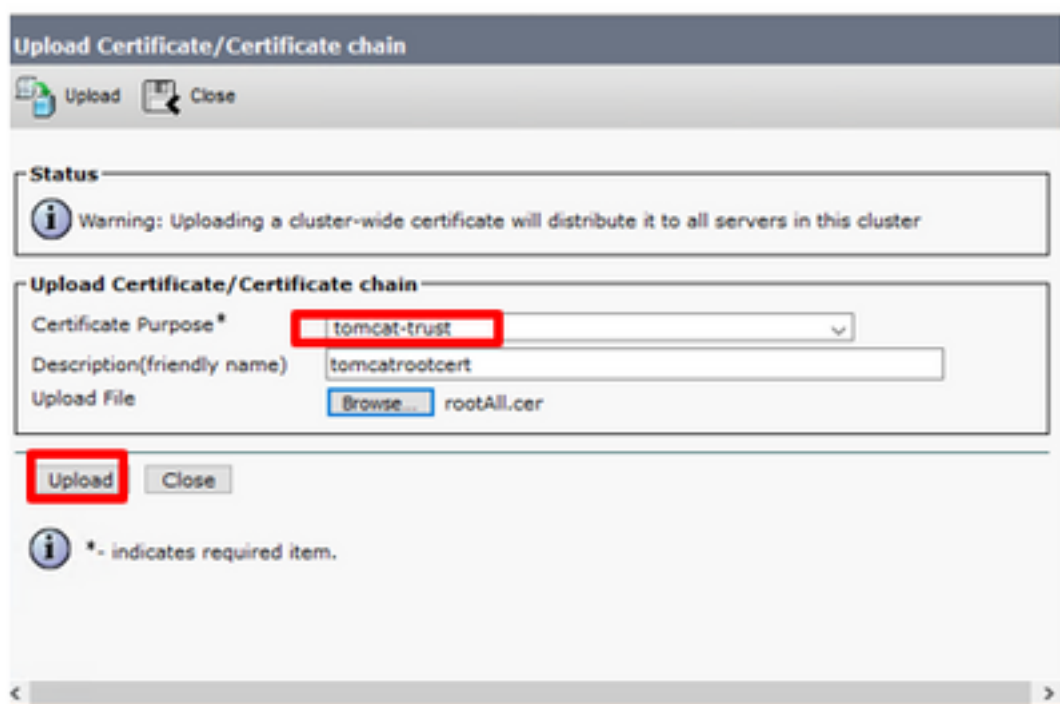
步驟2.按一下Upload Certificate/Certificate chain按鈕，如下圖所示。



步驟3.在快顯視窗中選擇tomcat-trust for **Certificate Purpose**。

步驟4.按一下**Browse...**按鈕，選擇要匯入的根證書檔案。然後按一下**Open**按鈕。

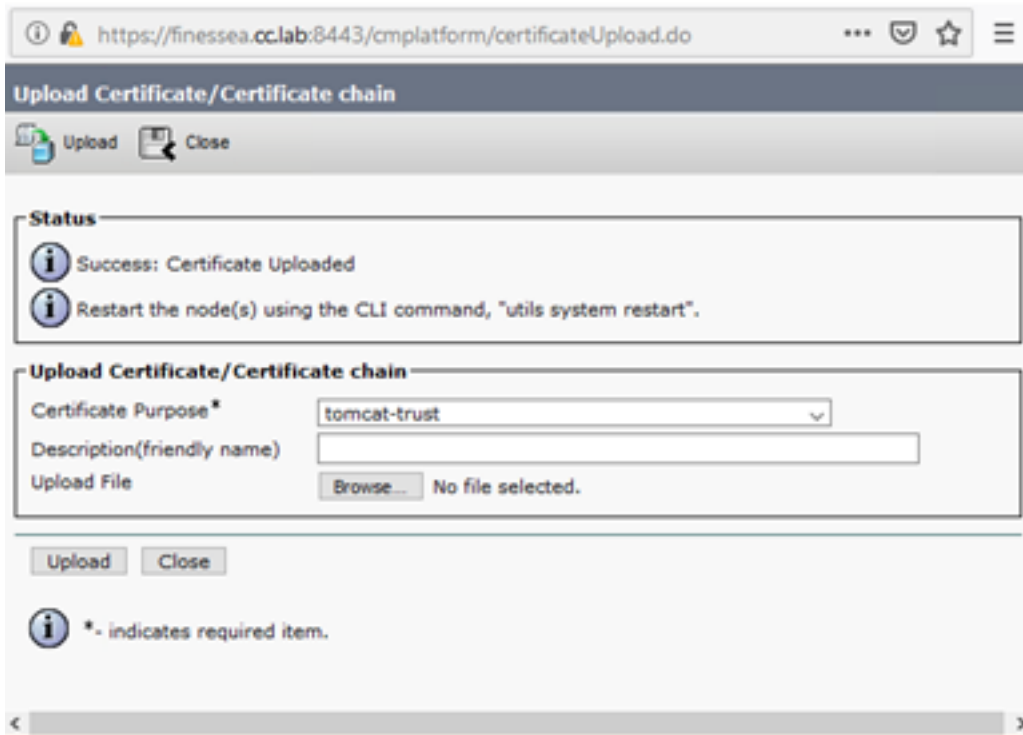
步驟5.在說明中寫入類似tomcatrootcert的內容，然後按一下**Upload**按鈕，如下圖所示。



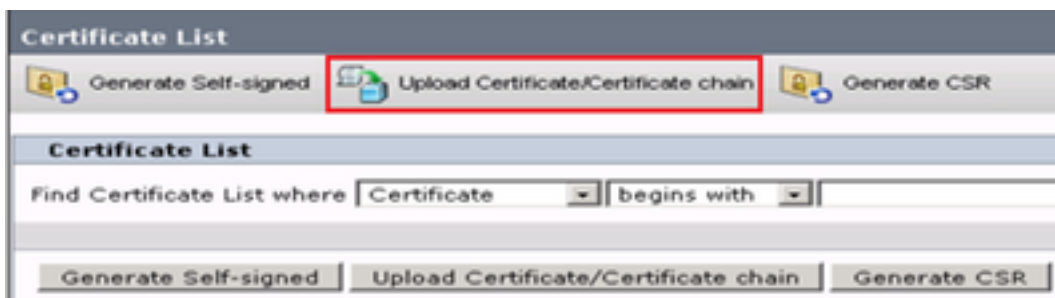
步驟6.等到您看到**Success:Certificate Uploaded**消息以關閉視窗。

系統將要求您重新啟動系統，但首先繼續上傳Finesse應用程式簽名的證書，然後您可以重新啟動系統。





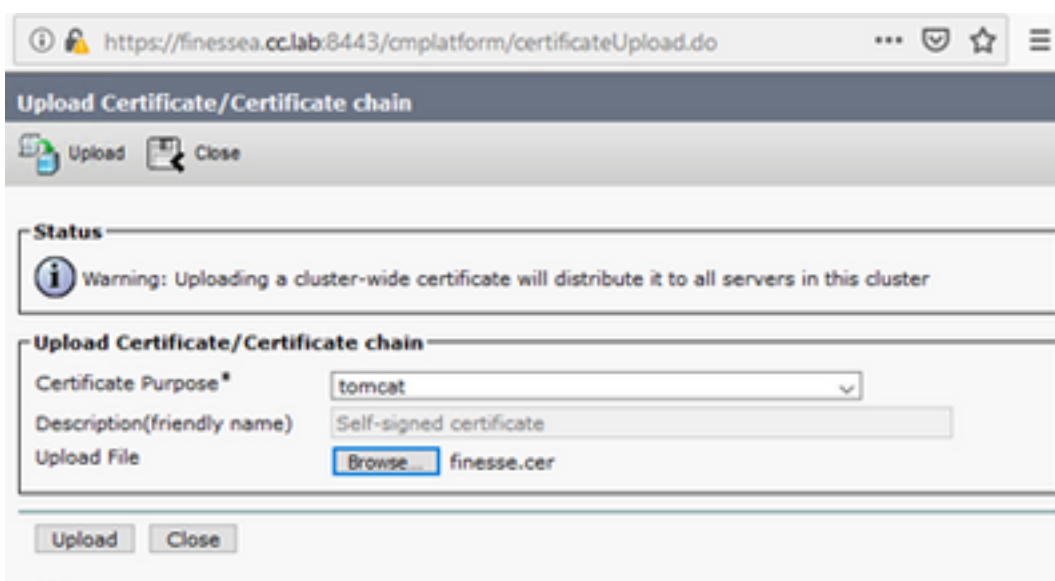
步驟7.按一下Upload Certificate/Certificate chain按鈕上的更多時間以匯入Finesse應用程式證書。



步驟8.在快顯視窗中選擇tomcat for Certificate Purpose。

步驟9.按一下Browse...按鈕，然後選擇Finesse CA簽名檔案finesse.cer。然後按一下Open按鈕。

步驟10.按一下Upload按鈕。



步驟11.等到您看到Success:證書上傳消息。

再次請求重新啟動系統。關閉視窗並繼續重新啟動系統。

## **驗證**

目前沒有適用於此組態的驗證程序。

## **疑難排解**

目前尚無適用於此組態的具體疑難排解資訊。