

Package CCE Solution：獲取和上傳第三方CA證書的程式

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[程式](#)

[產生並下載CSR](#)

[從CA取得根、中間（如果適用）和應用證書](#)

[將證書上傳到伺服器](#)

[Finesse伺服器](#)

[CUIC伺服器](#)

[證書依賴關係](#)

[將CUIC伺服器根證書上傳到Finesse主伺服器上](#)

[在CUIC主伺服器上上傳Finesse根/中間證書](#)

簡介

本文說明獲取和安裝由第三方供應商生成的證書頒發機構(CA)證書，以便在Finesse和Cisco Unified Intelligence Center(CUIC)伺服器之間建立HTTPS連線所涉及的步驟。

為了使用HTTPS在Finesse和CUIC伺服器之間進行安全通訊，需要設定安全證書。預設情況下，這些伺服器提供使用的自簽名證書，或者客戶可以獲取和安裝CA證書。這些CA證書可以從VeriSign、Thawte、GeoTrust等第三方供應商處獲取，也可以從內部生成。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Package Contact Center Enterprise(PCCE)
- CUIC
- Cisco Finesse
- CA證書

採用元件

文中使用的資訊是根據PCCE解決方案11.0(1)版本。

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。如果您的網路正在作用，請確保您已瞭解任何步驟的潛在影響。

程式



要在Finesse和CUIC伺服器中為HTTPS通訊設定證書，請執行以下步驟：

- 生成和下載證書簽名請求(CSR)
- 使用CSR從CA取得根、中間 (如果適用) 和應用憑證
- 將證書上傳到伺服器


產生並下載CSR

- 1.此處所述的步驟是為了產生和下載CSR。對於Finesse和CUIC伺服器，這些步驟是相同的。
- 2.使用URL開啟Cisco Unified Communications作業系統管理頁，使用在安裝過程中建立的作業系統(OS)管理員帳戶登入。https://hostname of primary server/cmplatform
- 3.生成證書簽名請求。
 - a.導覽至安全>憑證管理>產生CSR。
 - b.從Certificate Purpose*下拉選單中，選擇tomcat。
 - c.選擇Hash Algorithm as SHA256。
 - d.按一下「Generate」，如下圖所示。

Generate Certificate Signing Request

 Generate  Close

Status

 Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose*	tomcat
Distribution*	livedata.ora.com
Common Name	livedata.ora.com
<input checked="" type="checkbox"/> Required Field	
Subject Alternate Names (SANs)	
Parent Domain	ora.com
Key Length*	2048
Hash Algorithm*	SHA256

4. 下載CSR。

a. 導覽至安全>憑證管理>下載CSR。

b. 從Certificate Purpose*下拉選單中，選擇tomcat。

c. 按一下「Download CSR」，如下圖所示。



Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾

Certificate Management

Certificate List



Generate Self-signed



Upload Certificate/Certificate chain



Generate CSR



Download CSR



註：使用輔助伺服器/cmplatform的URL <https://hostname>在輔助伺服器上執行這些步驟，以便獲取CA的CSR。

從CA取得根、中間（如果適用）和應用證書

- 1.將主伺服器和輔助伺服器的CSR資訊提供給第三方CA，如VeriSign、Thawte、GeoTrust等。
- 2.您必須從CA收到主伺服器和輔助伺服器的以下證書鏈：
 - Finesse伺服器：根、中間和應用證書
 - CUIC伺服器：根和應用程式證書

將證書上傳到伺服器

本節介紹如何在Finesse和CUIC伺服器上正確上傳證書鏈。

Finesse伺服器

- 1.上傳主Finesse伺服器根證書：
 - a.在主伺服器的Cisco Unified Communications Operating System Administration頁面上，導航到 Security > Certificate Management > Upload Certificate。

- b. 從「證書用途」下拉選單中，選擇tomcat-trust。
- c. 在「上傳檔案」欄位中，按一下「Browse」，然後瀏覽根憑證檔案。
- d. 按一下「Upload File」。

2. 上傳主Finesse伺服器中間證書：

- a. 從「證書用途」下拉選單中，選擇tomcat-trust。
- b. 在「根證書」欄位中，輸入在上一步中上傳的根證書的名稱。這是在安裝根/公共證書時生成的.pem檔案。

若要檢視此檔案，請導覽至Certificate Management > Find。在憑證清單中，.pem檔案名稱是根據tomcat-trust列出的。

- c. 在「上傳檔案」欄位中，按一下「Browse」，然後瀏覽中間憑證檔案。
- d. 按一下「Upload File」。



註：由於主Finesse伺服器和輔助伺服器之間複製了tomcat-trust儲存，因此不需要將主Finesse伺服器根或中間證書上傳到輔助Finesse伺服器。

3. 上傳主Finesse伺服器應用程式證書：

- a. 從Certificate Purpose下拉選單中，選擇tomcat。
- b. 在Root Certificate欄位中，輸入在上一步中上傳的中間證書的名稱。包括.pem擴展（例如TEST-SSL-CA.pem）。
- c. 在「上傳檔案」欄位中，按一下瀏覽並瀏覽應用程式證書檔案。
- d. 按一下「Upload File」。

4. 上傳輔助Finesse伺服器根和中間證書：

- a. 在輔助伺服器上執行步驟1和2中提到的相同步驟以獲取其證書。



注意：由於是在主伺服器和輔助伺服器之間複製tomcat-trust儲存，因此不需要將輔助Finesse伺服器根或中間證書上傳到主Finesse伺服器。

5. 上傳輔助Finesse伺服器應用程式證書：

- a. 在輔助伺服器上執行步驟3中提到的相同步驟，以獲取自己的證書。


6. 重新啟動伺服器：

- a. 訪問主Finesse伺服器和輔助Finesse伺服器上的CLI，並運行utils system restart命令以重新啟動伺服器。

CUIC伺服器

1.上傳CUIC主伺服器根 (公共) 證書 :

- a.在主伺服器的Cisco Unified Communications Operating System Administration頁面上，導航到 Security > Certificate Management > Upload Certificate。
- b.從「證書用途」下拉選單中，選擇tomcat-trust。
- c.在「上傳檔案」欄位中，按一下「Browse」，然後瀏覽根憑證檔案。
- d.按一下「Upload File」。

 註：由於主CUIC伺服器和輔助伺服器之間複製了Tomcat-trust儲存，因此不需要將主CUIC伺服器根證書上傳到輔助CUIC伺服器。

2.上傳CUIC主伺服器應用程式 (主) 證書 :

- a.從Certificate Purpose下拉選單中，選擇tomcat。
- b.在Root Certificate欄位中，輸入在上一步中上傳的根證書的名稱。


這是安裝根/公共憑證時產生的.pem檔案。要檢視此檔案，請導航到證書管理>查詢。

在憑證清單中，.pem檔案名稱是根據tomcat-trust列出的。包括.pem擴展 (例如，TEST-SSL-CA.pem) 。

- c.在「上傳檔案」欄位中，按一下「Browse」，然後瀏覽應用程式 (主要) 憑證檔案。
- d.按一下「Upload File」。

3.上傳CUIC輔助伺服器根 (公共) 證書 :

- a.在輔助CUIC伺服器上，對其根證書執行步驟1.中提到的相同步驟。

 註：由於是在主伺服器和輔助伺服器之間複製tomcat-trust儲存，因此不需要將輔助CUIC伺服器根證書上傳到主CUIC伺服器。

4.上傳CUIC輔助伺服器應用程式 (主) 證書 :

- a.在輔助伺服器上執行步驟2所述的相同過程以獲取自己的證書。

5.重新啟動伺服器 :

- a.訪問主CUIC伺服器和輔助CUIC伺服器上的CLI，並運行utils system restart命令以重新啟動伺服器。

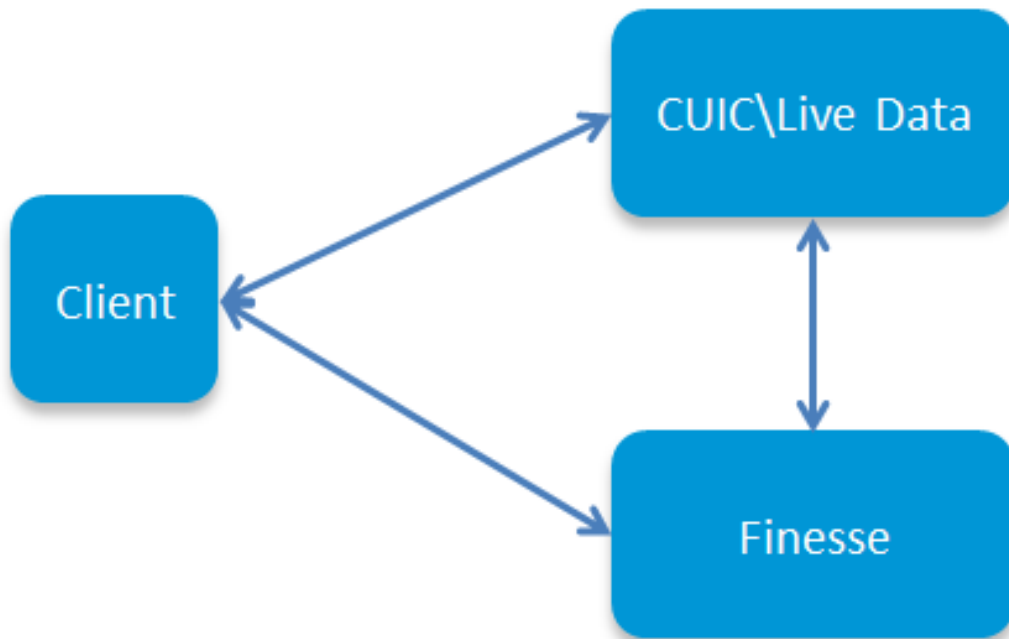
 注意：為了避免證書異常警告，必須使用完全限定域名(FQDN)訪問伺服器。

證書依賴關係

由於Finesse代理和主管使用CUIC小工具進行報告，因此您還必須上傳這些伺服器的根證書，順序如下面所述，以維護這些伺服器之間的HTTPS通訊的證書相關性，如下圖所示。

- 將CUIC伺服器根證書上傳到Finesse主伺服器上
- 在CUIC主伺服器上上傳Finesse根\中間證書

Certificate Dependencies



將CUIC伺服器根證書上傳到Finesse主伺服器上

1. 在主Finesse伺服器上，開啟Cisco Unified Communications Operating System Administration頁面，其中包含URL，然後使用在安裝過程中建立的OS管理員帳戶登入：

主Finesse伺服器/cmplatform的https://hostname

2. 上傳主CUIC根證書。

a. 導覽至Security > Certificate Management > Upload Certificate。


b. 從「證書用途」下拉選單中，選擇tomcat-trust。

c. 在「上傳檔案」欄位中，按一下「Browse」，然後瀏覽根憑證檔案。

d. 按一下「Upload File」。

3. 上傳輔助CUIC根證書。

- a. 導覽至 Security > Certificate Management > Upload Certificate。
- b. 從「證書用途」下拉選單中，選擇 tomcat-trust。
- c. 在「上傳檔案」欄位中，按一下「Browse」，然後瀏覽根憑證檔案。
- d. 按一下「Upload File」。

 註：由於是在主伺服器 and 輔助伺服器之間複製 tomcat-trust 儲存，因此不需要將 CUIC 根證書上載到輔助 Finesse 伺服器。

4. 訪問主 Finesse 伺服器和輔助 Finesse 伺服器上的 CLI，並運行 `utils system restart` 命令以重新啟動伺服器。

在 CUIC 主伺服器上上傳 Finesse 根/中間證書

1. 在主 CUIC 伺服器上，開啟 Cisco Unified Communications Operating System Administration 頁面，其中包含 URL，然後使用在安裝過程中建立的 OS 管理員帳戶登入：

主 CUIC 伺服器/cmplatform的 `https://hostname`


2. 上傳主 Finesse 根證書：

- a. 導覽至 Security > Certificate Management > Upload Certificate。
- b. 從「證書用途」下拉選單中，選擇 tomcat-trust。
- c. 在「上傳檔案」欄位中，按一下「Browse」，然後瀏覽根憑證檔案。
- d. 按一下「Upload File」。

3. 上傳主 Finesse 中間證書：

- a. 從「證書用途」下拉選單中，選擇 tomcat-trust。
- b. 在「根證書」欄位中，輸入在上一步中上載的根證書的名稱。
- c. 在「上傳檔案」欄位中，按一下「Browse」，然後瀏覽中間憑證檔案。
- d. 按一下「Upload File」。

4. 對主即時資料伺服器上的輔助 Finesse `root\Intermediate` 證書執行相同的步驟 2 和步驟 3。

 註：由於是在主伺服器和輔助伺服器之間複製 tomcat-trust 儲存，因此不需要將 Finesse 根/Intermediate 證書上載到輔助 CUIC 伺服器。

5. 訪問主 CUIC 伺服器和輔助 CUIC 伺服器上的 CLI，並運行 `utils system restart` 命令以重新啟動伺服器。

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）。