

Unified CCE解決方案：獲取和上傳第三方CA證書的程式 (版本11.x)

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[步驟 1.生成並下載證書簽名請求\(CSR\)。](#)

[步驟 2.從證書頒發機構獲取根、中間 \(如果適用 \) 步驟5和應用程式證書。](#)

[步驟 3.將證書上傳到伺服器。](#)

[Finesse伺服器](#)

[CUIC伺服器 \(假設證書鏈中不存在中間證書 \)](#)

[即時資料伺服器](#)

[即時資料伺服器證書依賴關係](#)

[驗證](#)

[疑難排解](#)

簡介

本文檔旨在詳細解釋獲取和安裝證書頒發機構(CA)證書所涉及的步驟，該證書由第三方供應商生成，用於在Finesse、思科統一情報中心(CUIC)和即時資料(LD)伺服器之間建立HTTPS連線。

必要條件

需求

思科建議您瞭解以下主題：

- 思科整合客服中心企業版(UCCE)
- Cisco Live Data(LD)
- Cisco Unified Intelligence Center(CUIC)
- Cisco Finesse
- CA認證

採用元件

本文檔中使用的資訊基於UCCE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。

背景資訊

為了使用HTTPS在Finesse、CUIC和即時資料伺服器之間進行安全通訊，需要設定安全證書。預設情況下，這些伺服器會提供所使用的自簽名的憑證，或是客戶可以取得和安裝憑證授權單位(CA)簽名的憑證。這些CA證書可以從第三方供應商 (如VeriSign、Thawte、GeoTrust) 獲得，也可以從內部生產。

設定

在Finesse、CUIC和Live Data伺服器中設定HTTPS通訊的證書需要以下步驟：

1. 生成並下載證書簽名請求(CSR)。
2. 使用CSR從證書頒發機構獲取根、中間 (如果適用) 和應用程式證書。
3. 將證書上傳到伺服器。

步驟 1.生成並下載證書簽名請求(CSR)。

1. 這裡所述的生成和下載CSR的步驟對於Finesse、CUIC和Live資料伺服器是相同的。
2. 使用指定的URL開啟Cisco Unified Communications Operating System Administration頁面，然後使用在安裝過程中建立的OS管理員帳戶登入
`https://FQDN:8443/cmplatform`
3. 產生憑證簽署請求(CSR)，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

Required Field

Subject Alternate Names (SANs)

Parent Domain ora.com

Key Length* 2048

Hash Algorithm* SHA256

Generate Close

步驟 1.導覽至Security > Certificate Management > Generate CSR。

步驟 2.從證書用途名稱下拉選單中，選擇tomcat。

步驟 3.根據業務需求選擇雜湊演算法和金鑰長度。

— 金鑰長度：2048 \雜湊演算法：建議使用SHA256

步驟 4.按一下「Generate CSR」。

註：如果企業要求使用域名填寫「主體替代名稱(SAN)」父域欄位，請注意文檔「[Finesse中第三方簽名證書的SAN問題](#)」中的問題地址。

4. 下載憑證簽署請求(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



步驟 1. 導覽至 Security > Certificate Management > Download CSR。

步驟 2. 從 Certificate Name (證書名稱) 下拉選單中，選擇 tomcat。

步驟 3. 按一下「Download CSR」。

附註：

註：使用 <https://FQDN:8443/cmplatform> 在輔助伺服器上執行上述步驟，以獲取證書頒發機構的 CSR

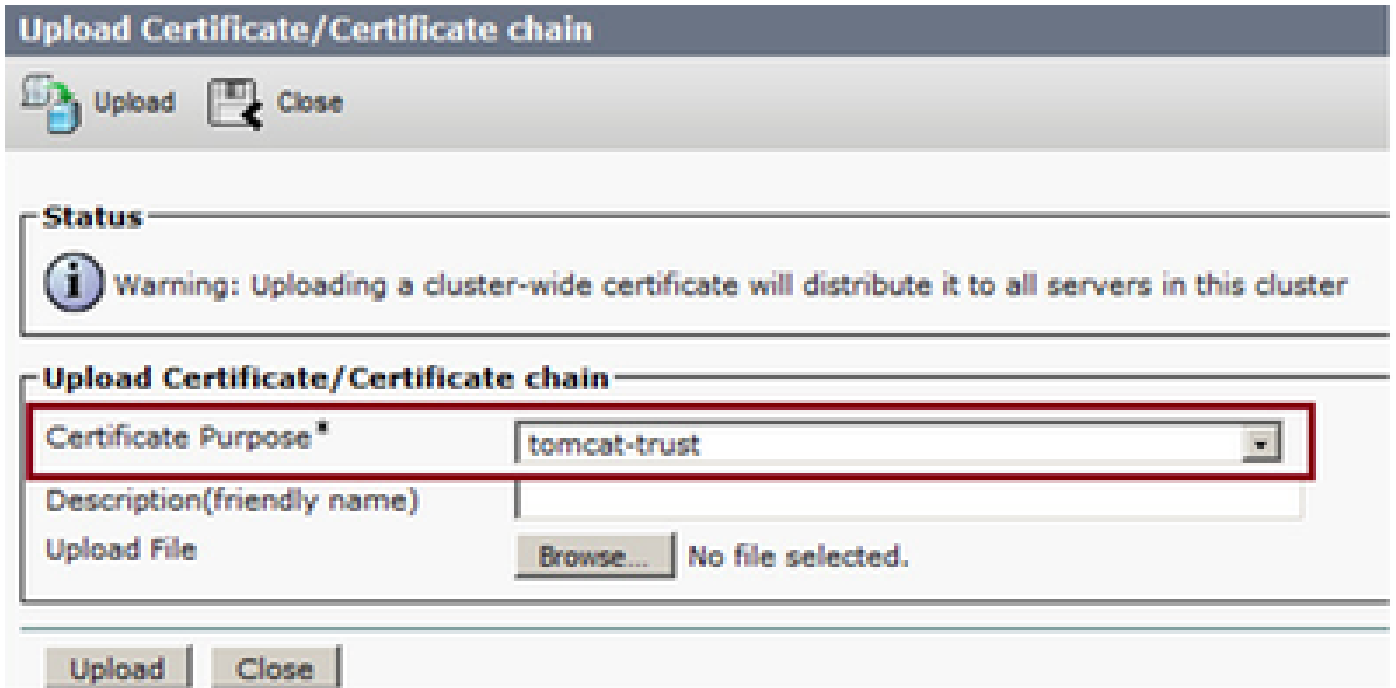
步驟 2. 從證書頒發機構獲取根、中間 (如果適用) 步驟5和應用程式證書。

1. 向第三方證書頒發機構 (如 VeriSign、Thawte、GeoTrust 等) 提供主伺服器和輔助伺服器的證書簽名請求 (CSR) 資訊。
2. 從證書頒發機構中，應該接收主伺服器和輔助伺服器的以下證書鏈。
 - Finesse 伺服器：根、中間 (可選) 和應用程式證書
 - CUIC 伺服器：根、中間 (可選) 和應用程式證書
 - 即時資料服務：根、中間 (可選) 和應用程式證書

步驟 3. 將證書上傳到伺服器。

本節介紹如何在Finesse、CUIC和Live資料伺服器上正確上傳證書鏈。

Finesse伺服器



1. 藉助以下步驟，將根證書上傳到主Finesse伺服器上：

- 步驟 1.在主伺服器Cisco Unified Communications Operating System Administration頁面上，導航至 安全(Security)>證書管理(Certificate Management)>上傳證書(Upload Certificate)。
- 步驟 2.從Certificate Name (證書名稱) 下拉選單中，選擇tomcat-trust。
- 步驟 3.在「Upload File」欄位中，按一下browse並瀏覽到根憑證檔案。
- 步驟 4.按一下「Upload File」。

2. 藉助以下步驟，將中間證書上傳到主Finesse伺服器上：

- 步驟 1.上傳中間證書的步驟與根證書的步驟相同，如步驟1所示。
- 步驟 2.在主伺服器Cisco Unified Communications Operating System Administration頁面上，導航到Security > Certificate Management > Upload Certificate。
- 步驟 3.從Certificate Name (證書名稱) 下拉選單中，選擇tomcat-trust。
- 步驟 4.在Upload File欄位中，按一下browse並瀏覽到Intermediate certificate file。
- 步驟 5.按一下「Upload」。

注意：由於在主伺服器和輔助伺服器之間複製Tomcat-trust儲存，因此不需要將根證書或中間證書上載到輔助finesse伺服器。

3. 上傳主Finesse伺服器應用程式證書，如下圖所示：

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[®] tomcat

Description(friendly name) Self-signed certificate

Upload File Browse... No file selected.

Upload Close

步驟 1. 從Certificate Name (證書名稱) 下拉選單中，選擇tomcat。

步驟 2. 在「Upload File」欄位中，按一下Browse，然後瀏覽至應用程式憑證檔案。

步驟 3. 按一下Upload以上傳檔案。

4. 上傳輔助財務伺服器應用程式證書。

在此步驟中在輔助伺服器上執行步驟3中提到的相同過程以獲取其自己的應用程式證書。

5. 現在，您可以重新啟動伺服器。

訪問主Finesse伺服器和輔助Finesse伺服器上的CLI，並輸入命令utils system restart以重新啟動伺服器。

CUIC伺服器 (假設證書鏈中不存在中間證書)

1. 在主CUIC伺服器上上傳根證書。

步驟 1. 在主伺服器Cisco Unified Communications Operating System Administration頁面上，導航到Security > Certificate Management > Upload Certificate/Certificate chain。

步驟 2. 從Certificate Name (證書名稱) 下拉選單中，選擇tomcat-trust。

步驟 3. 在「Upload File」欄位中，按一下browse並瀏覽到根憑證檔案。

步驟 4. 按一下「Upload File」。

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

2. 上傳主CUIC伺服器應用程式證書。

- 步驟 1. 從Certificate Name (證書名稱) 下拉選單中，選擇tomcat。
- 步驟 2. 在上傳檔案欄位中，點選瀏覽並瀏覽到應用程式證書檔案。
- 步驟 3. 按一下「Upload File」。

3. 上載輔助CUIC伺服器應用程式證書。

在輔助伺服器上執行步驟(2)中所述的相同過程以獲取自己的應用程式證書

4. 重新啟動伺服器

訪問主CUIC伺服器和輔助CUIC伺服器上的CLI，並輸入命令utils system restart以重新啟動伺服器。

註：如果CA機構提供包含中間證書的證書鏈，則Finesse伺服器部分中提到的步驟也適用於CUIC服務。

即時資料伺服器

1. Live-Data伺服器上上傳證書所涉及的步驟與Finesse或CUIC伺服器相同，具體取決於證書鏈。

2. 在主即時資料伺服器上上傳根證書。

- 步驟 1. 在主伺服器Cisco Unified Communications Operating System Administration頁面上，導航到Security > Certificate Management > Upload Certificate。
- 步驟 2. 從Certificate Name (證書名稱) 下拉選單中，選擇tomcat-trust。
- 步驟 3. 在「Upload File」欄位中，按一下browse，然後瀏覽到根憑證檔案。
- 步驟 4. 按一下「Upload」。

3. 在主即時資料伺服器上上傳中間證書。

- 步驟 1. 上傳中間證書的步驟與根證書的步驟相同，如步驟1所示。
- 步驟 2. 在主伺服器Cisco Unified Communications Operating System Administration頁面上，導航到Security > Certificate Management > Upload Certificate。
- 步驟 3. 從Certificate Name (證書名稱) 下拉選單中，選擇tomcat-trust。
- 步驟 4. 在「Upload File」欄位中，按一下browse，然後瀏覽到Intermediate certificate file。
- 步驟 5. 按一下「Upload」。

注意：由於在主伺服器和輔助伺服器之間複製Tomcat-trust儲存，因此不需要將根證書或中間證書上傳到輔助即時資料伺服器。

4. 上傳主即時資料伺服器應用程式證書。

- 步驟 1. 從Certificate Name (證書名稱) 下拉選單中，選擇tomcat。

步驟 2.在「Upload File」欄位中，按一下Browse，然後瀏覽至應用程式憑證檔案。
步驟 3.按一下「Upload」。

5. 上傳輔助即時資料伺服器應用程式證書。

在輔助伺服器上執行上述步驟(4)，以獲取自己的應用程式證書。

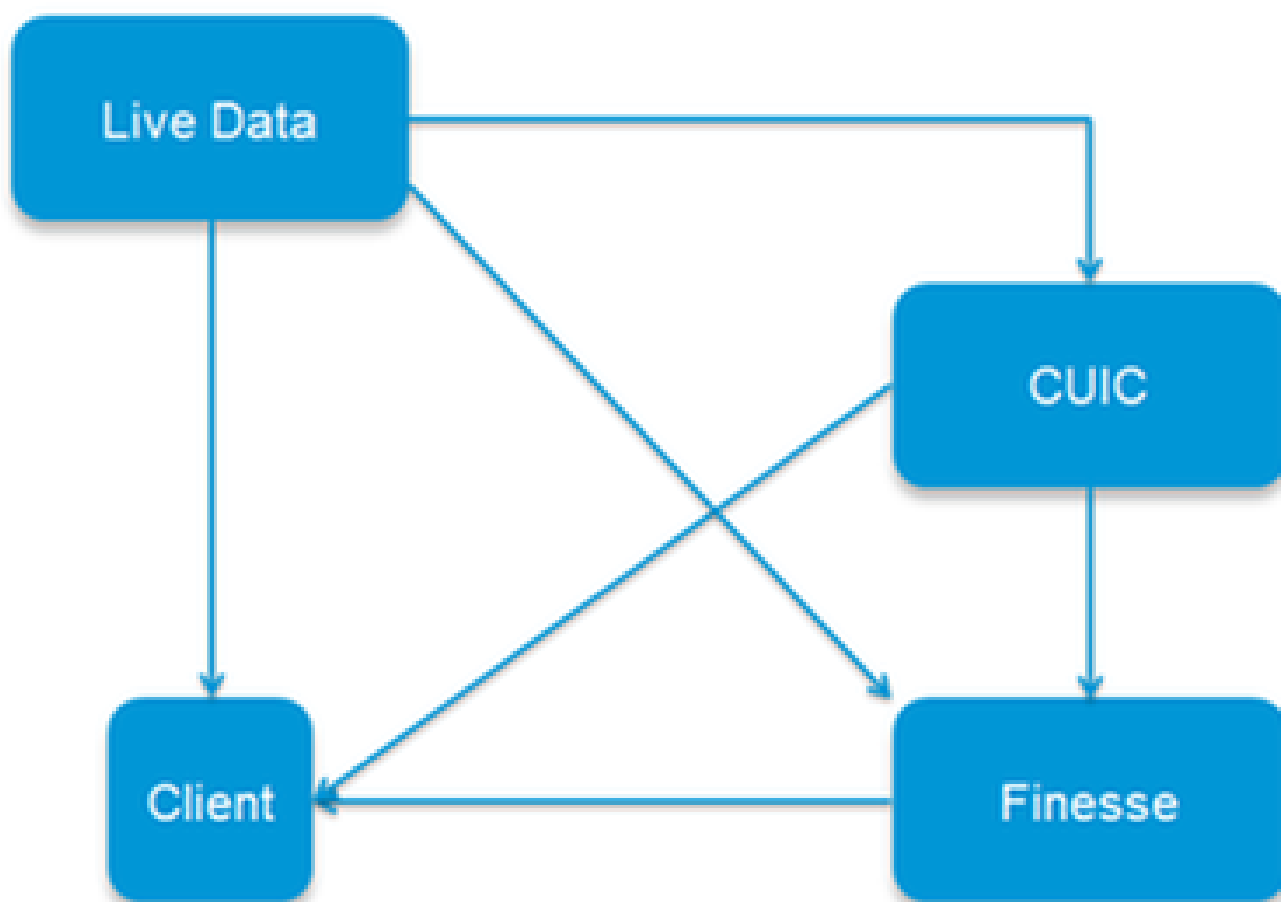
6. 重新啟動伺服器

訪問主Finesse伺服器和輔助Finesse伺服器上的CLI，並輸入命令「utils system restart」以重新啟動伺服器。

即時資料伺服器證書依賴關係

隨著即時資料伺服器與CUIC和Finesse伺服器互動，這些伺服器之間存在證書依賴關係，如下圖所示：

Certificate Dependencies



對於第三方CA證書鏈，組織中所有伺服器的根證書和中間證書是相同的。因此，為使Live資料伺服

器正常工作，您必須確保Finesse和CUIC伺服器將根證書和中間證書正確載入到Tomcat-Trust容器。

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。

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）。