Expressway證書故障排除

目錄

簡介

本文檔介紹證書的工作方式以及Expressway伺服器中證書的最常見問題和提示。

必要條件

需求

思科建議您瞭解以下主題：

- Expressway和視訊通訊伺服器(VCS)伺服器
- 安全套接字層(SSL)
- 憑證
- Telepresence裝置
- 移動和遠端訪問
- 合作部署

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Expressway x14

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

SSL和憑證是一種標準，在其他裝置和品牌間使用的方法相同。本文檔重點介紹Expressway中的證書用途。

定義

證書用於在兩台裝置之間建立安全連線。它們是驗證伺服器或裝置身份的數位簽章。某些協定(例如超文本傳輸協定安全(HTTPS)或會話初始協定(SIP)傳輸層安全(TLS))需要使用證書才能正常工作。

談論憑證時使用的不同術語：

- 證書簽名請求(CSR)：使用標識裝置的名稱建立的模板，以便以後簽名並轉換為客戶端或伺服器證書
- 證書：已簽名的CSR。這些是身份型別，安裝在裝置上用於SSL協商。它們可以由自己或證書頒發機構簽名。
- 證書簽名：驗證相關證書合法性的標識；這些標識以其他證書的形式顯示。
- 自簽名證書：由自己簽名的客戶端或伺服器證書
- 證書頒發機構(CA)：簽署證書的實體
    - Intermediate Certificate（中間證書）：CA證書不是由自身簽名而是由另一個CA證書簽名，通常由根證書簽名，但也可以由另一個中間證書簽名
    - 根證書：由自身簽名的CA證書

基本原則

當客戶端與伺服器對話並開始SSL對話時，它們會交換證書，稍後將證書用於加密裝置之間的流量。作為交換的一部分，裝置還確定證書是否受信任。要確定證書是否受信任，必須滿足多個條件，有些條件是：

- 最初用於聯絡伺服器的完全限定域名(FQDN)與伺服器提供的證書內的名稱相匹配。
    - 例如，當您在瀏覽器上開啟網頁時，cisco.com會解析提供證書的伺服器的IP，該伺服器必須包含cisco.com作為名稱才能受到信任。

- 對伺服器提供的伺服器證書（或自簽名時相同的伺服器證書）進行簽名的CA證書存在於裝置的CA受信任證書清單中。
    - 裝置具有受信任的CA證書清單，電腦通常包含具有公認公共證書頒發機構的預置清單。

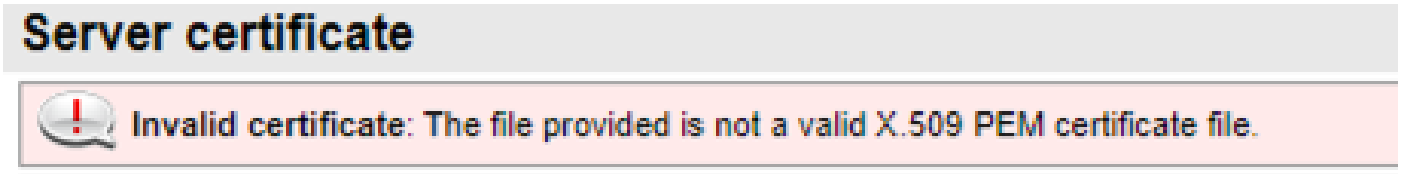
- 當前日期和時間在證書的有效期限內。
    - 憑證授權單位僅在一定的時間內簽署CSR，這由CA決定。

- 證書未吊銷。
    - 公共證書頒發機構通常在證書中包含證書撤銷清單URL。這樣接收證書的參與方可以確認證書未被CA吊銷。

常見問題

Expressway證書上傳失敗

有幾個原因會導致此情況。它們會導致不同的描述性錯誤。



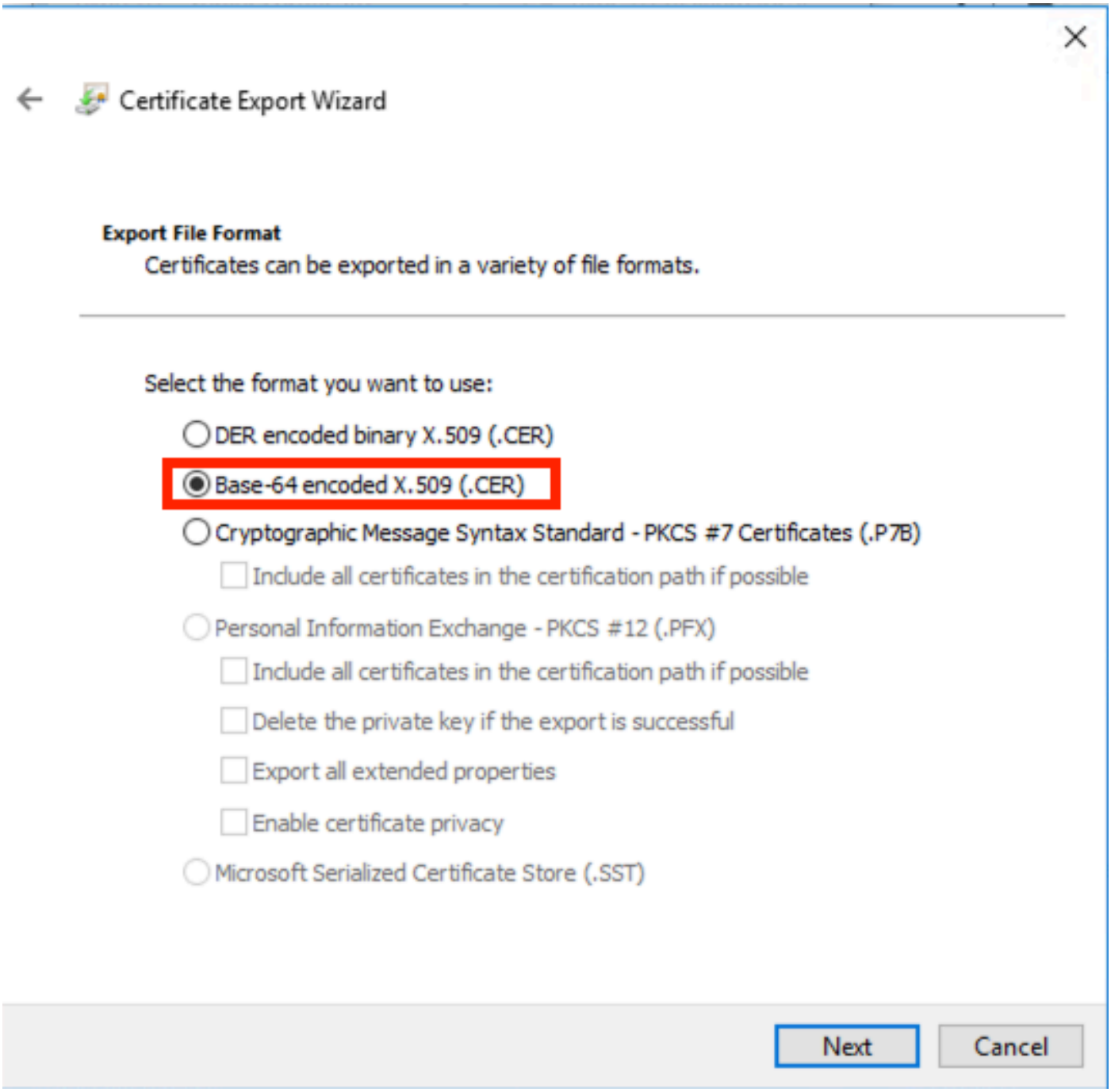
證書格式無效

當證書的格式無效時，會發生第一個錯誤。副檔名並不重要。

如果憑證未開啟，可以從CA以正確的格式要求新憑證

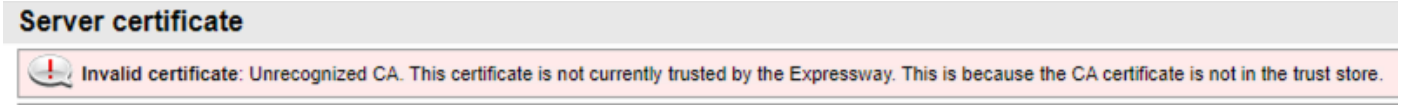
如果證書開啟，請執行以下步驟：

步驟 1.開啟證書並導航到Details頁籤。
步驟 2.選擇Copy to File。
步驟 3.按照嚮導操作，確保已選擇Base-64 encoded。



證書格式選擇

步驟 4.儲存後，將新檔案上傳到Expressway上。



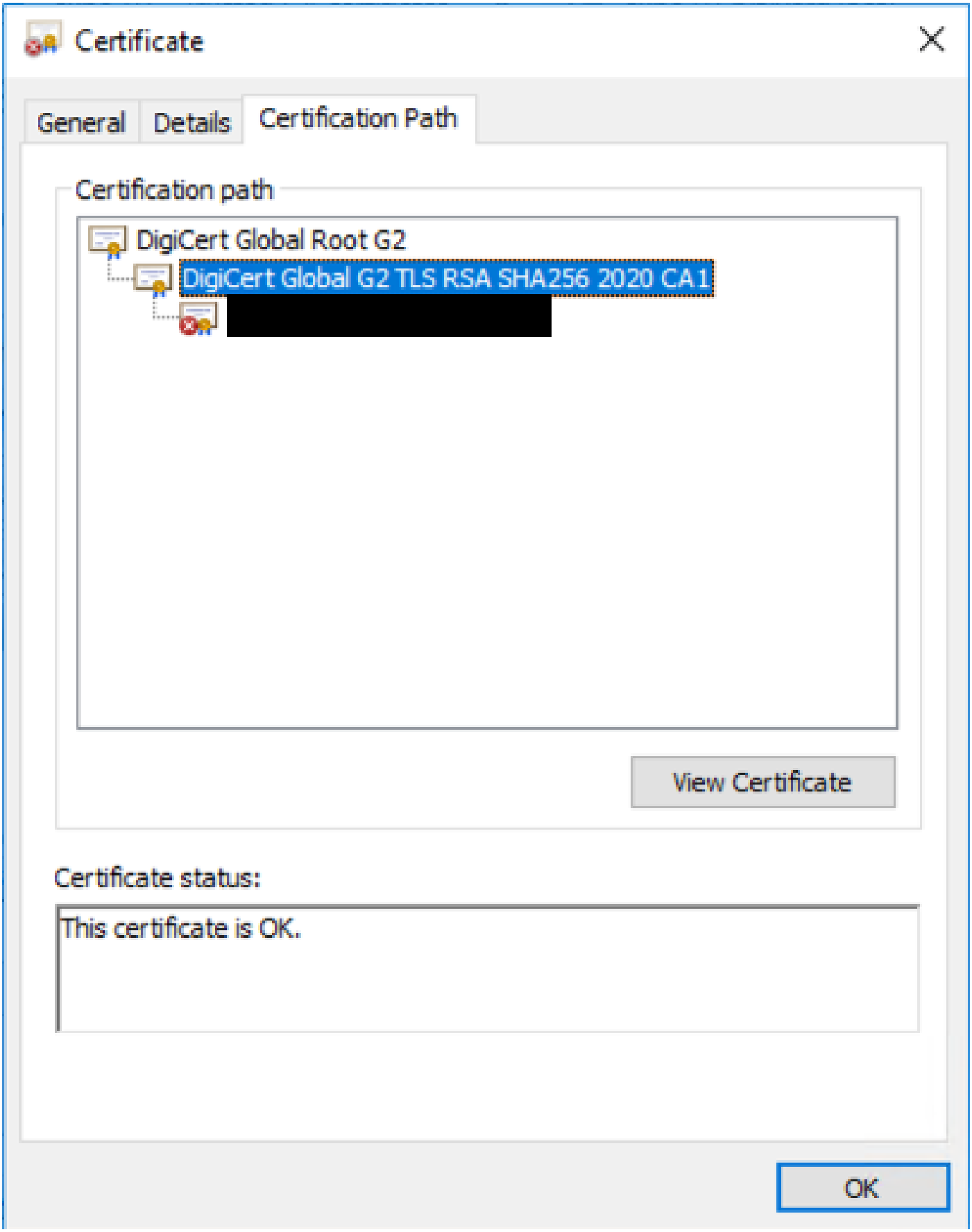
不受信任的CA證書鏈

當簽署伺服器證書的CA證書不受信任時會發生此錯誤。上傳伺服器憑證之前，伺服器必須信任鏈結中的所有CA憑證。

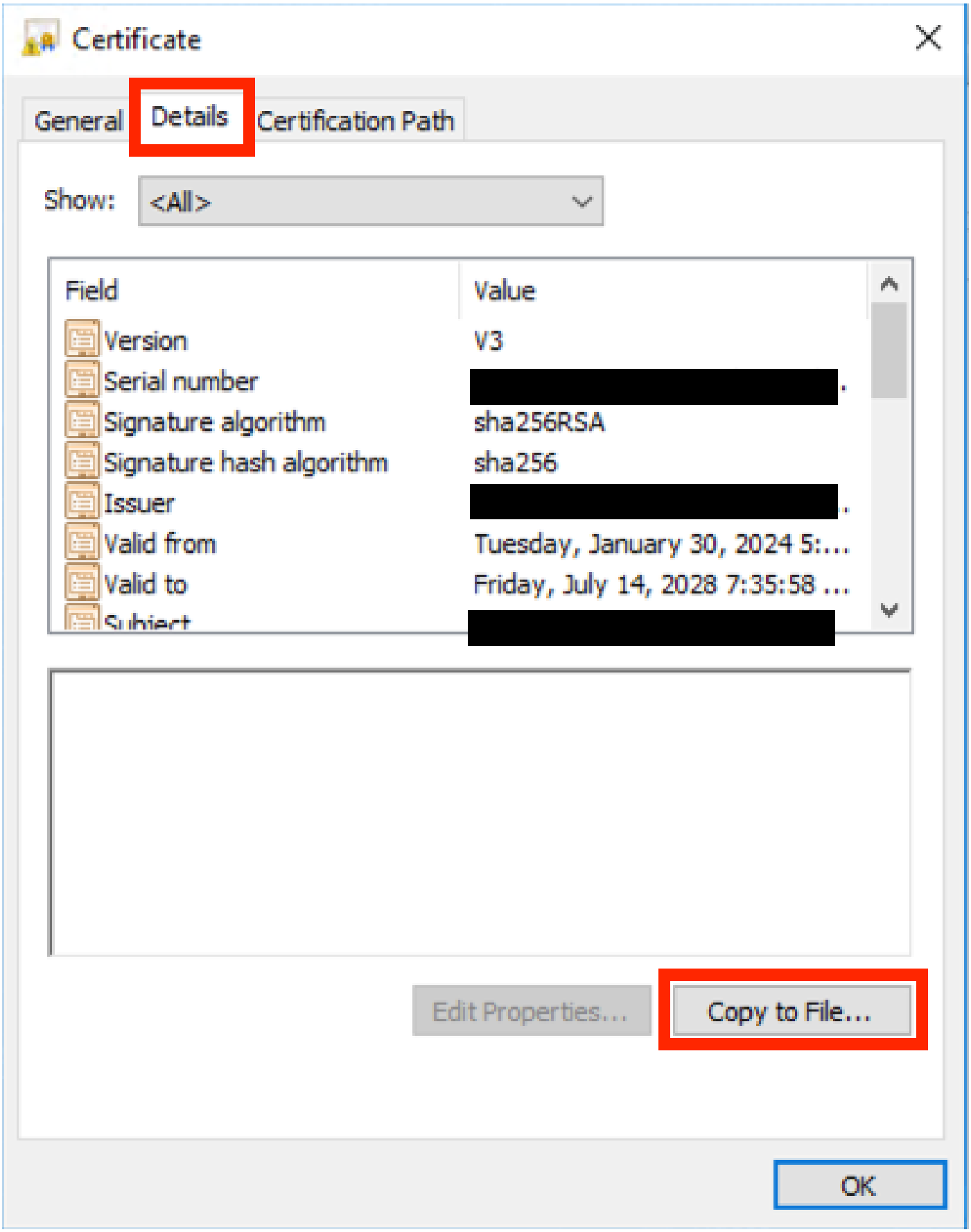
通常CA會提供CA憑證以及已簽名的伺服器憑證。如果可用，請跳至下面的步驟6。

如果CA證書不可用，可從伺服器證書獲取這些證書。請遵循以下步驟：

步驟 1.開啟服務器證書。
步驟 2.導航到Certification Path選項卡。排名靠前的證書被視為根CA證書。底部是伺服器憑證，介於兩者之間的都視為中間CA憑證。
步驟 3.選擇CA證書並選擇View Certificate。



步驟 4.導覽至Details索引標籤，然後按照之前的步驟操作，以便將憑證儲存到另一個檔案中。
步驟 5.對存在的所有CA證書重複這些步驟。



Certificate Details頁籤

所有CA證書可用後，將其上傳到Expressway受信任CA證書清單：

步驟 6.在Expressway伺服器上導航到維護>安全>受信任CA證書。

步驟 7.選擇Choose File並上傳。
步驟 8.對每個CA憑證重複步驟7。
步驟 9.所有CA證書上傳到信任清單後，將伺服器證書上傳到伺服器。

遍歷區域關閉，出現錯誤TLS協商錯誤

當Expressway-C和Expressway-E之間的SSL交換未成功完成時，會發生此錯誤。可能導致此問題的幾個示例：

- 主機名與提供的證書中的名稱不匹配。
  - 確保Expressway-C遍歷區域上配置的對等地址與Expressway-E伺服器證書上的至少一個名稱相匹配
- TLS驗證名稱與提供的證書中的名稱不匹配。
  - 確保Expressway-E遍歷區域上配置的TLS驗證名稱與Expressway-C伺服器證書上的名稱之一匹配。如果是群集配置，建議將Expressway-C群集FQDN配置為TLS。驗證該名稱，因為此名稱必須存在於群集的所有節點上。
- 伺服器不信任CA證書
  - 正如每個伺服器在上傳伺服器憑證前必須信任其自己的CA憑證，其他伺服器也必須信任這些CA憑證才能信任伺服器憑證。為此，請確保來自兩個Expressway伺服器的證書路徑的所有CA證書都存在於所有相關伺服器的受信任CA清單中。CA憑證可以按照本文前面提供的步驟擷取。

證書續訂後，遍歷區域已啟動，但SSH隧道已關閉

SSH通道故障

當一個或多個中間CA證書不可信，根CA證書信任啟用穿越區域連線，但SSH隧道是更詳細的連線，當整個鏈不受信任時可能會失敗，中間CA證書經常被證書頒發機構更改，因此證書的更新可能觸發此問題。確保所有中間CA證書都上載到所有Expressway信任清單上。

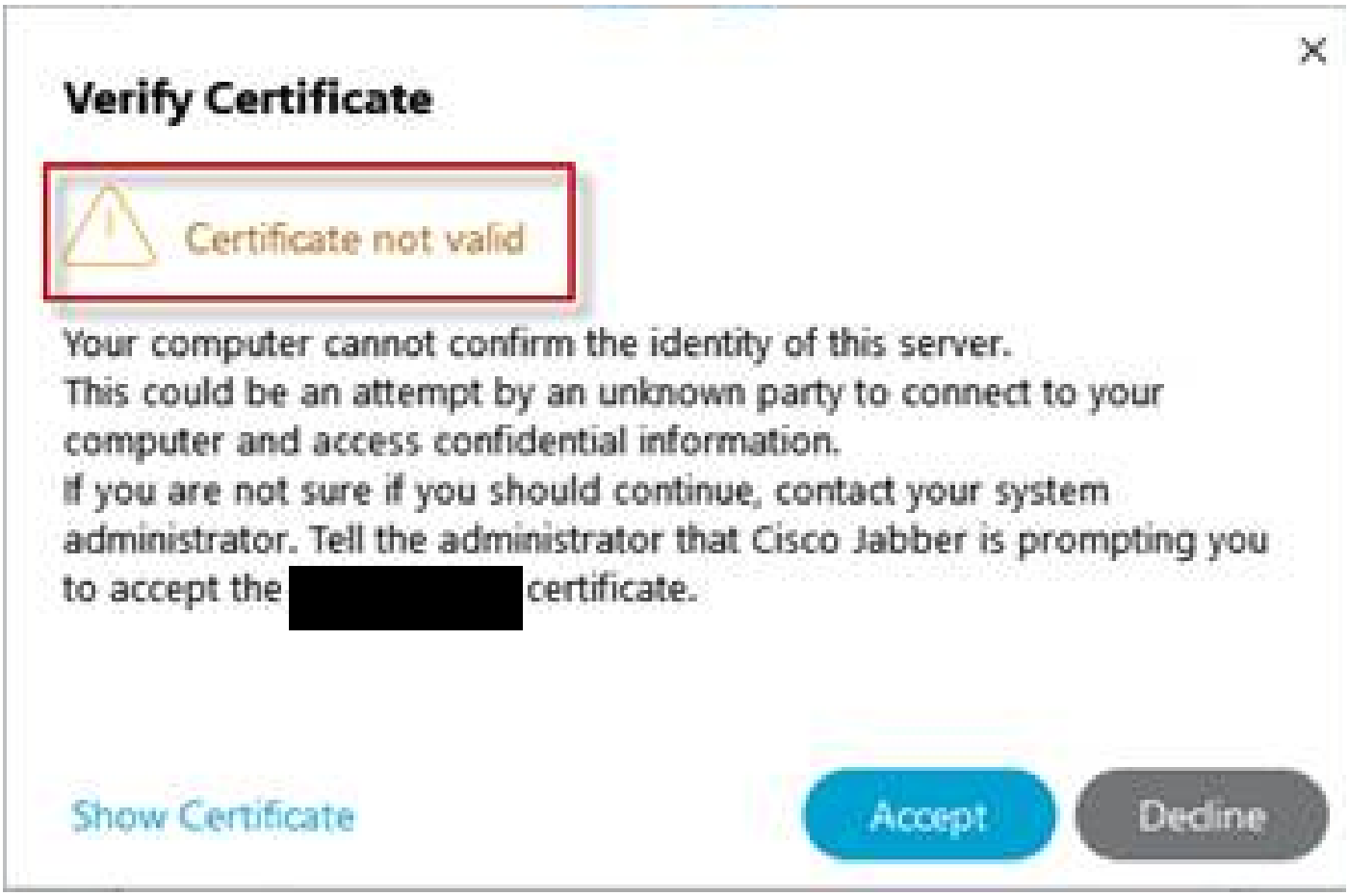
升級或證書續訂後，移動和遠端訪問登入失敗

登入可能會因證書原因而失敗，但是在較新版本的Expressway軟體上，由於安全原因，已實施了一些軟體更改，強制在以前未執行的位置進行證書驗證。

此處對此有更詳細的說明：Traffic Server Enforces Certificate Verification

解決方法中規定，確保Expressway-C CA證書作為tomcat-trust和callmanager-trust上傳到Cisco Unified Communications Manager，然後重新啟動所需的服務。

移動和遠端訪問登入時Jabber上的證書警報



Jabber不受信任的證書警告

當應用程式上使用的域與Expressway-E伺服器證書上的使用者替代名稱不匹配時，會發生此行為。請確保example .com或備用collab-edge.example .com是證書上存在的主題替代名稱之一。

相關資訊

思科技術支援與下載

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）。