續訂Expressway證書

目錄

簡介

本檔案將說明Expressway/Video Communication Server(VCS)證書續訂流程。

本文檔中的資訊適用於Expressway和VCS。本文檔引用Expressway，但可以與VCS進行互換。

> **附註**：雖然本文旨在幫助您執行證書續訂流程，但最好還要檢查適用於您版本的Cisco Expressway證書建立和使用部署指南。

背景資訊

每當更新證書時，都必須考慮兩個要點，以確保系統在安裝新證書後繼續正常工作：

1.新證書的屬性必須與舊證書的屬性相匹配（主要是主體替代名稱和擴展金鑰用法）

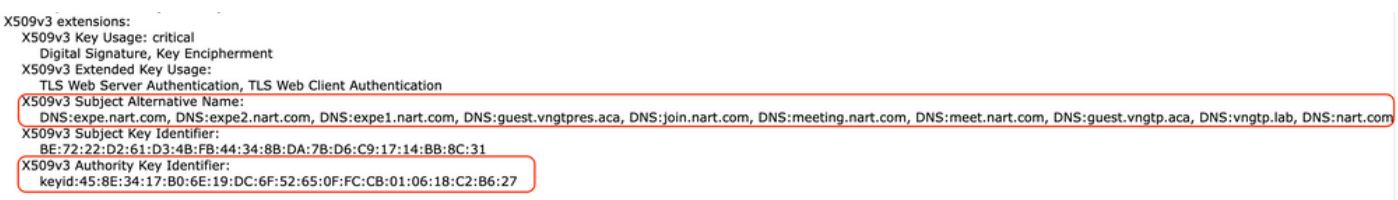
2.用於簽署新證書的CA（證書頒發機構）必須受到與Expressway直接通訊的其他伺服器的信任（例如CUCM、Expressway-C、Expressway-E等）

流程

A)從當前證書獲取資訊

1.開啟Expressway網頁維**護>安全>伺服器證書> Show decoded。**

2.在開啟的新視窗中，將「主體替代名稱」和「授權金鑰識別符號」X509v3副檔名複製到記事本文檔。

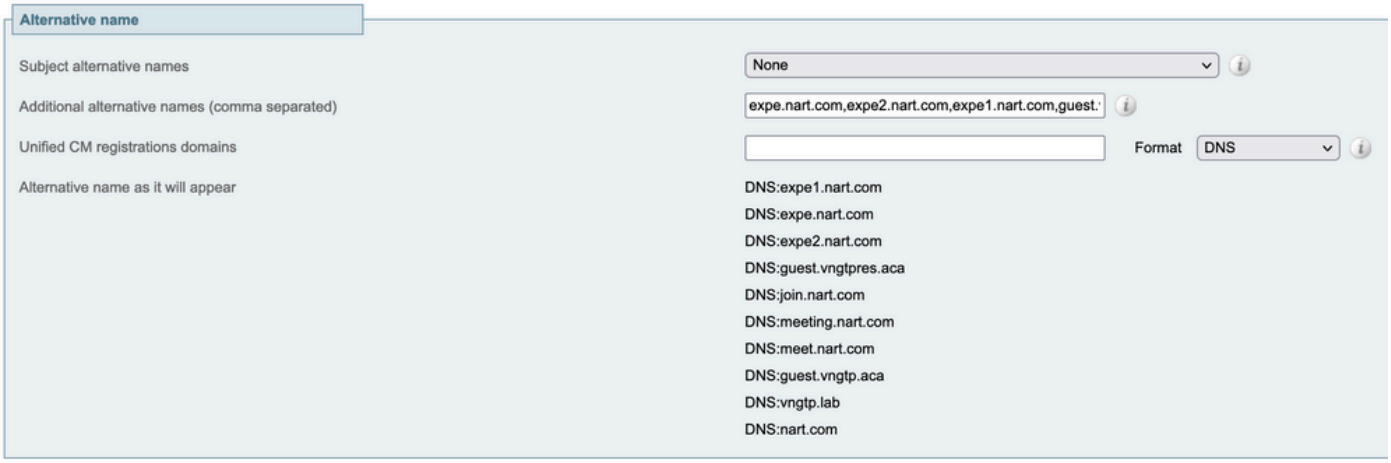


「Show decoded」證書視窗

B)生成CSR（證書簽名請求）並將其傳送到CA（證書頒發機構）進行簽名。

1.從Expressway網頁維**護>安全>伺服器證書>生成CSR。**

2.在「產生CSR」視窗的「其他備用名稱（以逗號分隔）欄位，填寫我們在A部分中儲存的「使用者備用名稱」的所有值，並確保刪除「DNS：」並用逗號分隔清單，請參閱圖（在「備用名稱將顯示」旁邊，您可以看到要在憑證中使用的所有SAN的清單）：



產生CSR SAN專案

3.填寫**Additional Information**部分下的剩餘資訊，如國家/地區、公司、州等，然後按一下**Generate CSR。**

4.產生CSR後，**Maintenance > Security > Server Certificate**頁面會顯示**Discard CSR** 和**Download**選項，您必須選擇**Download**，然後將CSR傳送到CA進行簽名。

> **附註**：確保在安裝新證書之前，未放棄**CSR**，如果已完成**放棄CSR**，然後嘗試安裝使用已放棄的CSR簽名的證書，則證書安裝失敗。

C)檢查新證書中的SAN清單和擴展/增強金鑰使用屬性

在Windows證書管理器中開啟新簽名的證書並檢查：

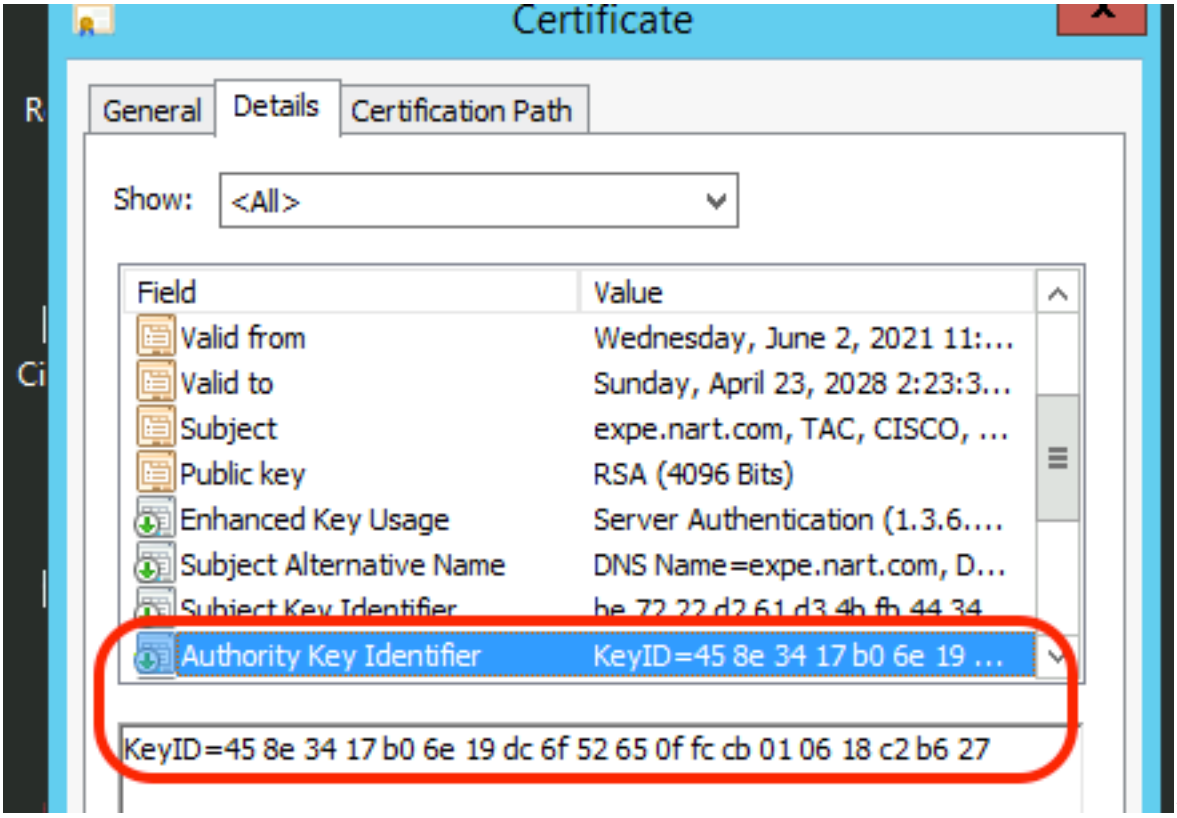
1. SAN清單與我們在生成CSR時使用的A部分中儲存的SAN清單相匹配。

2. 「擴展/增強型金鑰用法」屬性必須包括「客戶端身份驗證」和「伺服器身份驗證」。

> **附註**：如果證書的副檔名為.pem，請將其重新命名為.cer或.crt，以便可以使用Windows證書管理器開啟它。使用Windows證書管理器開啟證書後，您可以轉到**Details**頁籤**> Copy to File**，並將其匯出為Base64編碼檔案，在文本編輯器中開啟時，base64編碼檔案通常頂部有「-----BEGIN CERTIFICATE-----」，底部有「-----END CERTIFICATE-----」

D)檢查簽署新憑證的CA是否與簽署舊憑證的CA相同

在Windows證書管理器中開啟新簽名的證書，複製「授權金鑰識別符號」值，並將其與我們在A部分中儲存的「授權金鑰識別符號」值進行比較。



使用Windows證書管理器開啟的新證書

如果兩個值相同，則意味著使用相同的CA來簽署新證書，而使用相同的CA來簽署舊證書，您可以繼續前往E部分以上傳新證書。

如果這些值不同，則意味著用於簽署新證書的CA不同於用於簽署舊證書的CA，在繼續前往E部分之前，您必須遵循以下步驟：

1.獲取所有中間CA證書（如果有）和根CA證書。

2.轉到**維護>安全>受信任CA證書**，按一下**瀏覽**，然後在電腦上搜尋中間CA證書並上傳。對任何其他中間CA證書和根CA證書執行相同操作。

3.對連線到此伺服器的任何Expressway-E（如果要更新的證書是Expressway-C證書）或連線到此伺服器的任何Expressway-C（如果要更新的證書是Expressway-E證書）執行相同操作。

4.如果要續訂的證書是Expressway-C證書，並且您具有MRA或對CUCM具有安全區域，則必須確保CUCM信任新的根和中間CA，並將根和中間CA證書上傳到CUCM tomcat-trust和callmanager-trust儲存，然後在CUCM上重新啟動相關服務。

E)安裝新證書

在檢查所有先前點後，您現在可以在Expressway上通過**維護>安全>伺服器證書**按一下**瀏覽**從您的電腦中選擇新證書檔案並上傳。

安裝新證書後，必須重新啟動Expressway。

> **附註**：確保從**維護>安全>伺服器證書**上傳到Expressway的證書只包含Expressway伺服器證書，而不包含完整證書鏈，並確保其Base64證書

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）。