

更新Expressway證書

目錄

[簡介](#)

[背景資訊](#)

[程序](#)

- [A\)從當前證書獲取資訊](#)
- [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。](#)
- [C\)檢查新證書中的SAN清單和擴展/增強金鑰使用屬性](#)
- [D\)檢查簽署新憑證的CA與簽署舊憑證的CA是否相同](#)
- [E\)安裝新憑證](#)

簡介

本文檔介紹Expressway/影片通訊伺服器(VCS)證書續訂流程。

背景資訊

本文檔中的資訊適用於Expressway和VCS。文檔引用了Expressway，但是它可以與VCS互換。



注意：雖然本文檔旨在幫助您進行證書續訂流程，但最好還要閱讀您的版本的[思科Expressway證書建立和使用部署指南](#)。

每當要更新證書時，必須考慮兩個要點，以驗證系統在安裝新證書後是否繼續正常工作：

1. 新憑證的屬性必須與舊憑證的屬性相符（主要是主體替代名稱和擴充金鑰用途）。
2. 簽署新證書的CA（證書頒發機構）必須由與Expressway直接通訊的其他伺服器（例如CUCM、Expressway-C、Expressway-E...）信任。

程序

A)從當前證書獲取資訊

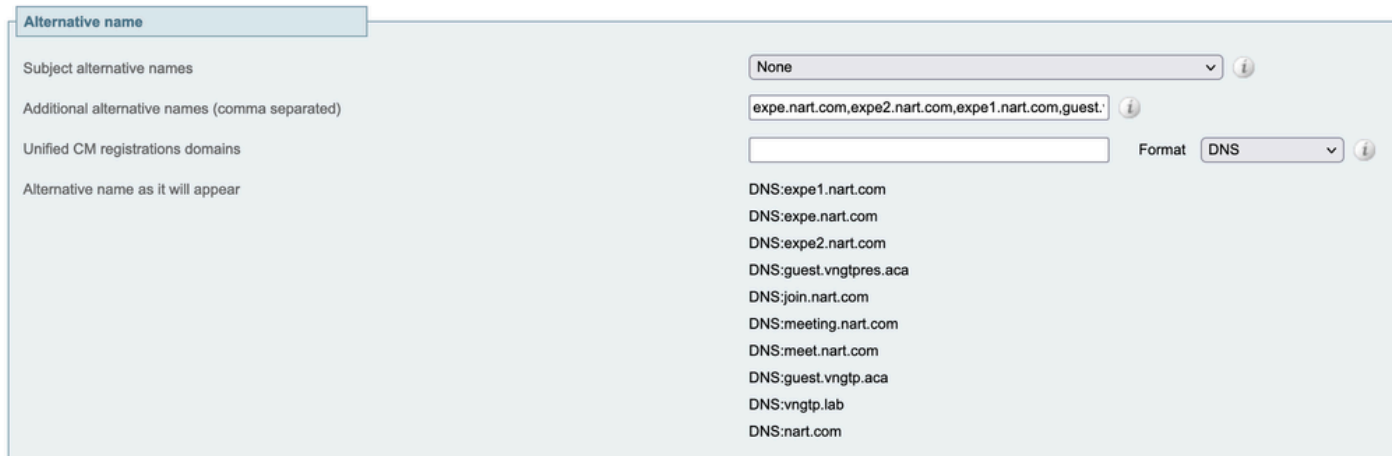
1. 打開Expressway網頁維護>安全>伺服器證書>顯示解碼。
2. 在開啟的新視窗中，將主體替代名稱和授權金鑰辨識碼X509v3副檔名複製到記事本檔案。

```
X509v3 extensions:
X509v3 Key Usage: critical
  Digital Signature, Key Encipherment
X509v3 Extended Key Usage:
  TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Subject Alternative Name:
  DNS:expe.nart.com, DNS:expe2.nart.com, DNS:expe1.nart.com, DNS:guest.vngtpres.aca, DNS:join.nart.com, DNS:meeting.nart.com, DNS:meet.nart.com, DNS:guest.vngtp.aca, DNS:vngtp.lab, DNS:nart.com
X509v3 Subject Key Identifier:
  BE:72:22:D2:61:D3:4B:FB:44:34:8B:DA:7B:D6:C9:17:14:BB:8C:31
X509v3 Authority Key Identifier:
  keyid:45:8E:34:17:B0:6E:19:DC:6F:52:65:0F:FC:CB:01:06:18:C2:B6:27
```

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「其他替代名稱 (以逗號分隔) 」欄位中，輸入主體替代名稱在區段A中儲存的所有值，然後移除DNS：並以逗號分隔清單。

在此圖中，在顯示的備用名稱旁，有一個列出要在證書中使用的所有SAN的清單)：



產生CSR SAN專案


3. 輸入其他資訊部分下的其餘資訊 (如國家/地區、公司、州/省.....) ，然後按一下生成CSR。
4. 產生CSR後，頁面維護>安全>伺服器憑證顯示捨棄CSR 和下載的選項。選擇下載並將CSR傳送給CA進行簽名。

 注意：請在安裝新證書之前勿丟棄CSR。如果完成丟棄CSR，然後嘗試安裝與被丟棄的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

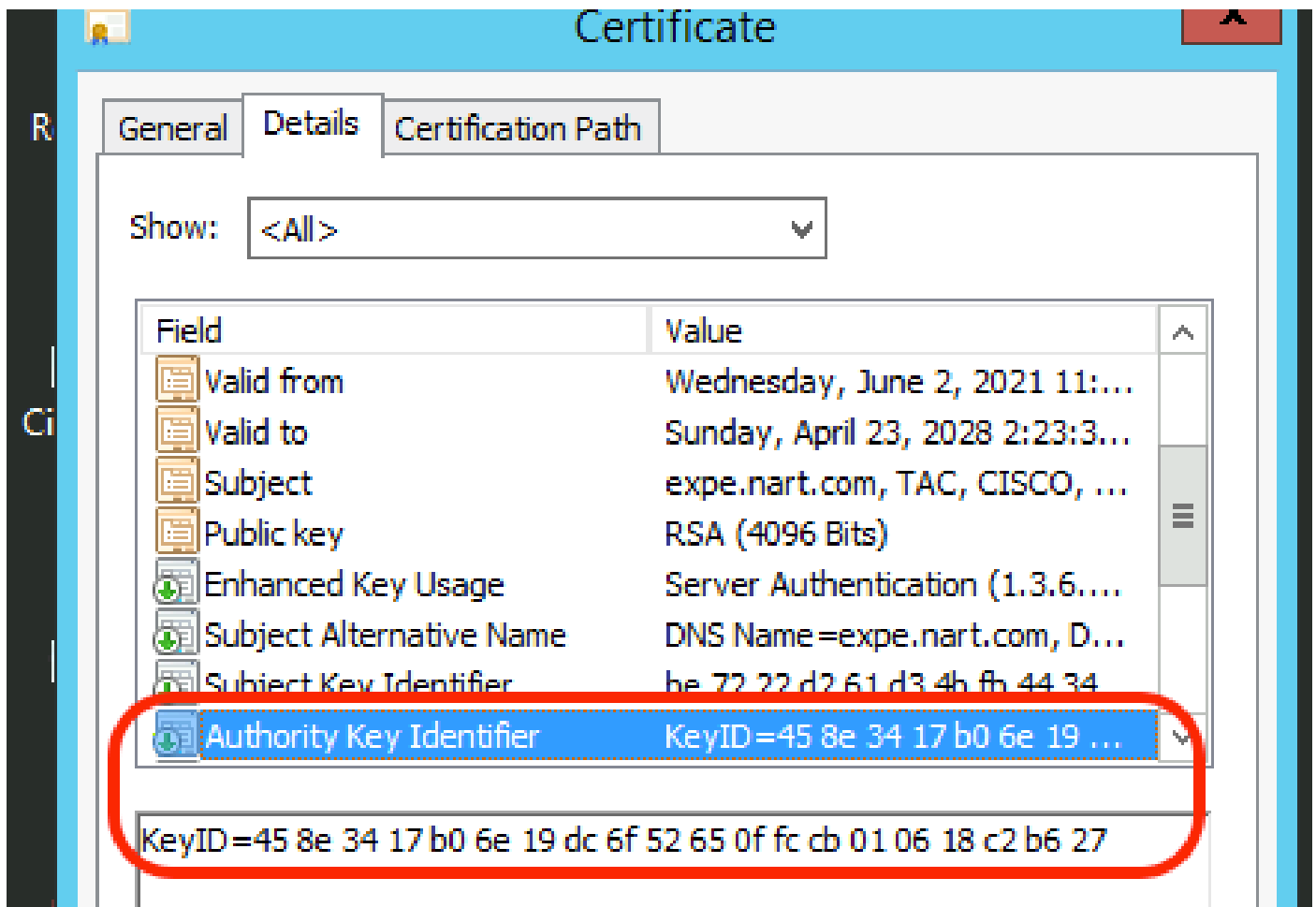
在Windows證書管理器中打開新簽名的證書並驗證：

1. SAN清單與我們在生成CSR時使用的A部分中儲存的SAN清單匹配。
2. 「擴展/增強型金鑰使用」屬性必須包括客戶端身份驗證和伺服器身份驗證。

 注意：如果證書的副檔名為.pem，請將其重新命名為.cer或.crt，以便使用Windows證書管理器打開它。使用Windows證書管理器打開證書後，您可以轉到詳細資訊頁籤> 複製到檔案，然後將其導出為Base64編碼檔案，在文本編輯器中打開時，base64編碼檔案的頂部通常顯示「-----BEGIN CERTIFICATE-----」，底部通常顯示「-----END CERTIFICATE-----」

D) 檢查簽署新憑證的CA與簽署舊憑證的CA是否相同

在Windows證書管理器中打開新簽名的證書，然後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證書管理器打開的新證書

如果兩個值相同，則意味著使用與用於簽署舊證書的CA相同的CA來簽署新證書，您可以繼續參閱第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，在繼續執行E部分之前應採取的步驟如下：

1. 獲取所有中間CA證書（如果有）和根CA證書。
2. 轉至維護>安全>受信任CA證書(CA證書)，按一下瀏覽，然後在您的電腦上搜尋中間CA證書並上傳。請為任何其他中間CA憑證和根CA憑證執行相同的動作。
3. 在連線到此伺服器的任何Expressway E（如果要續訂的證書為Expressway C證書）或連線到此伺服器的任何Expressway C（如果要續訂的證書為Expressway E證書）上執行相同操作。
4. 如果要續訂的證書是Expressway-C證書，並且您具有MRA或CUCM的安全區域
 - 驗證CUCM信任新的根和中間CA。
 - 將根和中間CA證書上傳到CUCM tomcat-trust和callmanager-trust儲存區。


- 重新啟動CUCM上的相關服務。

E)安裝新憑證

如果之前檢查了所有要點，可以透過維護>安全>伺服器證書在Expressway上安裝新證書。

按一下Browse 並從您的電腦中選擇新的證書檔案並上傳它。

安裝新證書後，必須重新啟動Expressway。

 注意：驗證要從維護>安全>伺服器證書上傳到Expressway的證書是否只包含Expressway伺服器證書，而非完整證書鏈，並驗證它是Base64證書。

將單一憑證新增至多個Expressway：

- 為整個expressway e集群建立單個證書。
- 建立包含所有FQDN以及您在Expressway上使用的額外功能的CSR (如果是CMS WebConnect、加入URL和域、如果是MRA、您的註冊/登入域)

範例：

Exwycluster.domain

Exwy1.domain

Exwy2.domain

Exwy3.domain

Exwy4.domain

額外功能 (網域或CMS URL)

- 完成CSR後，您可以使用SFTP程式擷取此CSR的私密金鑰 (建議使用WinSCP，我們會大量使用)
- 打開WinSCP並連線到建立CSR的expressway e
- 導覽至tandberg/persistent/certs/ CSR或憑證簽署請求 (可能顯示以及擱置中)
- 將私鑰從expressway e複製到您的案頭上，
- 完成此操作後，我們就可以對所有4個節點使用相同的證書。

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）。