

將Expressway核心的根/中間證書上傳到CUCM

目錄

[簡介](#)

[背景資訊](#)

[組態](#)

[步驟 1. 獲取簽署Expressway C伺服器證書的根證書和中間證書](#)

[步驟 2. 上傳CUCM上的根證書和中間證書 \(如果適用\)](#)

[步驟 3. 在CUCM上重新啟動必要的服務](#)

[相關資訊](#)

簡介

本文檔介紹如何將已簽名Expressway-C證書的CA的根證書和中間證書上傳到CUCM發佈伺服器。

背景資訊

由於X14.0.2中Expressway上的流量伺服器服務的改進，即使伺服器(CUCM)處於非安全模式，只要伺服器(CUCM)請求在8443以外的埠 (例如，6971,6972) 上運行的服務，Expressway-C就會傳送其客戶端證書。由於進行了此更改，因此需要將Expressway-C證書簽名證書頒發機構(CA)同時作為tomcat-trust和callmanager-trust增加到CUCM中。

在Expressway升級到X14.0.2或更高版本後，無法上傳CUCM上的Expressway-C簽名CA導致MRA登入失敗。

要使CUCM信任Expressway-C傳送的證書，tomcat-trust和callmanager-trust必須包含根CA以及參與簽署Expressway-C證書的任何中間CA。

組態

步驟 1. 獲取簽署Expressway C伺服器證書的根證書和中間證書

當您最初從簽署該伺服器證書的CA收到伺服器證書時，您還擁有該伺服器證書的根證書和中間證書，並將它們儲存在安全位置。如果您仍然擁有這些檔案或可以從您的CA再次下載這些檔案，則可以轉到第2步，在該步中可以找到有關如何將它們上傳到CUCM的說明。

如果不再擁有這些檔案，您可以從Expressway-C Web介面下載它們。這有點複雜，因此強烈建議您聯絡您的CA，儘可能從他們下載信任庫。

在Expressway-C上，導航到維護>安全>伺服器證書，然後按一下「伺服器證書」旁邊的顯示 (解碼) 按鈕。這將打開一個包含Expressway-C伺服器證書內容的新窗口/頁籤。您可以在此處查詢「頒發者」欄位：

<#root>

Certificate:

Data:
Version: 3 (0x2)
Serial Number:
55:00:00:02:21:bb:2d:41:60:55:d7:b2:27:00:01:00:00:02:21
Signature Algorithm: sha256WithRSAEncryption

Issuer: O=DigiCert Inc, CN=DigiCert Global CA-1

Validity

Not Before: Dec 8 10:36:57 2021 GMT

Not After : Dec 8 10:36:57 2023 GMT

Subject: C=BE, ST=Flamish-Brabant, L=Diegem, O=Cisco, OU=TAC, CN=vcs-c1.vngtp.lab

Subject Public Key Info:

...

在本示例中，Expressway-C伺服器證書由DigiCert Inc.組織頒發，其通用名稱為DigiCert Global CA-1。

現在，導航到維護>安全>受信任CA證書，在清單中檢視您是否有證書在「主題」欄位中具有完全相同的值。在本示例中，這是Subject欄位中的O=DigiCert Inc，CN=DigiCert Global CA-1。如果找到匹配項，則表示這是中繼CA。您需要此檔案，並且需要繼續查詢，直到找到根CA。

如果您找不到相符專案，請在「簽發者」欄位中搜尋具有此值的憑證，且其主旨與簽發者相符。如果您找到相符專案，則表示這是根CA檔案，是我們唯一需要的檔案。

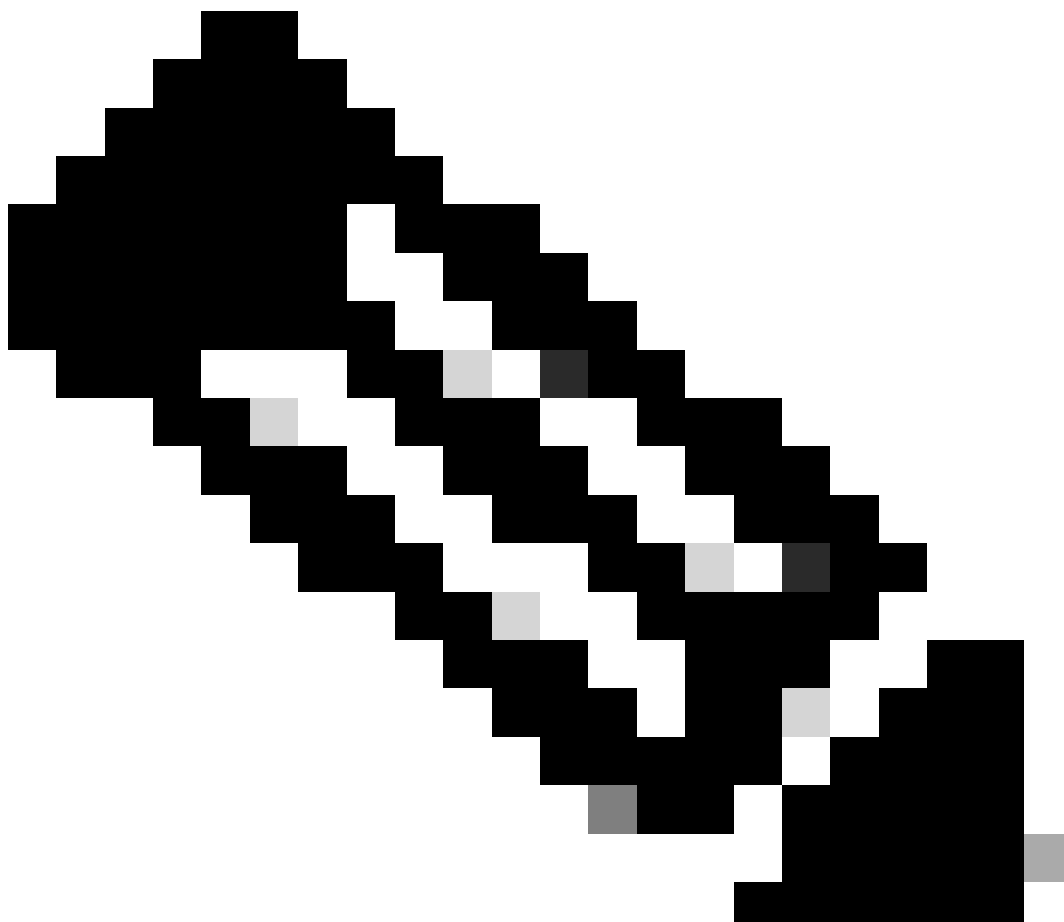
Type	Issuer	Subject
<input type="checkbox"/> Certificate	CN=vngtp-ACTIVE-DIR-CA	Matches Issuer
<input type="checkbox"/> Certificate	O=IdenTrust, CN=IdenTrust Commercial Root CA 1	Matches Issuer
<input type="checkbox"/> Certificate	O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root	Matches Issuer
<input type="checkbox"/> Certificate	O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA	Matches Issuer
<input type="checkbox"/> Certificate	O=The Go Daddy Group, Inc., OU=Go Daddy Class 2 Certification Authority	Matches Issuer
<input type="checkbox"/> Certificate	O=GoDaddy.com, Inc., CN=Go Daddy Root Certificate Authority - G2	Matches Issuer
<input type="checkbox"/> Certificate	O=QuoVadis Limited, CN=QuoVadis Root CA 2	Matches Issuer
<input type="checkbox"/> Certificate	O=thawte, Inc., OU=Certification Services Division, OU=(c) 2006 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA	Matches Issuer
<input type="checkbox"/> Certificate	O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G5	Matches Issuer
<input type="checkbox"/> Certificate	O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA	O=DigiCert Inc, CN=DigiCert Global CA-1

Show all (decoded) Show all (PEM file) Delete Select all Unselect all

Expressway信任儲存

在本例中，在找到證書後，您注意到Subject欄位與Issuer欄位不匹配。這表示這是中繼CA憑證。除了根憑證之外，您還需要此憑證。如果主題表明與頒發者匹配，則您會知道這是根證書頒發機構，也是您需要信任的唯一證書。

如果您有中間憑證，您必須繼續執行，直到我們找到根憑證為止。為此，請檢視您的中間證書的Issuer欄位。然後在Subject欄位中查詢具有相同值的證書。在我們的示例中，這是O=DigiCert



注意：底部必須有一個空行。


步驟 2.上傳CUCM上的根證書和中間證書 (如果適用)

- 登入您的CUCM發佈伺服器的Cisco Unified OS Administration頁面。
- 導航到安全>證書管理。
- 按一下Upload Certificate/Certificate chain按鈕。
- 在新視窗中，開始從步驟1上傳根憑證。上傳至tomcat-trust。

Upload Certificate/Certificate chain

Upload Close


Status

 Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose*	tomcat-trust
Description(friendly name)	DigiCert root CA Certificate
Upload File	Browse... root.pem

Upload Close

 *- indicates required item.

- 按一下Upload按鈕，然後必須看到Success：Certificate Uploaded。忽略要求您立即重新啟動Tomcat的消息。
- 現在使用CallManager-trust上傳相同的根檔案以用於證書目的。
- 對Expressway-C上使用的所有中間證書重複上述步驟（上傳到tomcat-trust和CallManager-trust）。

步驟 3.在CUCM上重新啟動必要的服務

需要在CUCM集群中的每個CUCM節點上重新啟動這些服務：

- Cisco CallManager
- Cisco TFTP
- Cisco Tomcat

可以從CUCM的Cisco Unified Serviceability頁面重新啟動Cisco CallManager和Cisco TFTP：

- 登入到CUCM發佈伺服器的Cisco Unified Serviceability頁面。
- 導航到工具>控制中心-功能服務。
- 選擇您的Publisher作為伺服器。
- 選擇Cisco CallManager服務，然後按一下Restart按鈕。
- 重新啟動Cisco CallManager服務後，選擇Cisco TFTP service，然後按一下Restart按鈕。

Cisco Tomcat只能從CLI重新啟動：

- 打開與CUCM發佈伺服器的命令列連線。
- 使用命令utils service restart Cisco Tomcat。

相關資訊

[技術支援與檔案- Cisco Systems](#)

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）。