

設定協同合作邊緣(MRA)憑證並疑難排解

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[Public vs. Private Certificate Authority\(CA\)](#)

[憑證運作方式](#)

[SSL交換摘要](#)

[設定](#)

[Expressway-C和Expressway-E遍歷區域/信任](#)

[生成並簽名CSR](#)

[將Expressway-C和Expressway-E配置為相互信任](#)

[Cisco Unified Communications Manager\(CUCM\)與Expressway-C之間的安全通訊](#)

[概觀](#)

[配置CUCM和Expressway-C之間的信任](#)

[具有自簽名證書的CUCM伺服器](#)

[Expressway-C和Expressway-E集群注意事項](#)

[群集證書](#)

[受信任的CA清單](#)

[驗證](#)

[檢查當前證書資訊](#)

[在Wireshark中讀取/匯出證書](#)

[疑難排解](#)

[測試以瞭解Expressway上的證書是否受信任](#)

[Synergy Light終端 \(7800/8800系列電話 \)](#)

[影片資源](#)

[為MRA或群集Expressway生成CSR](#)

[將Server證書安裝到Expressway](#)

[如何在Expressway之間配置證書信任](#)

簡介

本檔案介紹有關行動遠端存取(MRA)部署的憑證。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

公共證書頒發機構與專用證書頒發機構(CA)

在Expressway-C和E伺服器上有多種對證書進行簽名的選項。您可以選擇由公用CA(例如GoDaddy、Verisign或其他)簽署憑證簽署請求(CSR)，或者如果您使用自己的憑證授權單位(可以使用OpenSSL或內部企業CA(例如Microsoft Windows伺服器)進行自簽署)，則可以在內部簽署該請求。有關如何建立和簽署上述任何方法所使用的CSR的更多資訊，請參閱《[Video Communication Server\(VCS\)Certificate Creation Guide](#)》。

唯一真正需要由公共CA簽名的伺服器是Expressway-E。這是客戶端通過MRA登入時唯一看到證書的伺服器，因此，使用公共CA以確保使用者不必手動接受證書。Expressway-E可以使用內部CA簽名的證書，但首次使用使用者將被提示接受不受信任的證書。7800和8800系列電話的MRA註冊不適用於內部證書，因為無法修改其證書信任清單。為簡單起見，建議您的Expressway-C和Expressway-E證書都由同一個CA簽名；但是，只要您在這兩個伺服器上正確配置了受信任CA清單，就不要要求這樣做。

憑證鏈運作方式

證書在兩個或多個證書的鏈中連結在一起，用於驗證對伺服器證書簽名的源。鏈結中有三種型別的憑證：使用者端/伺服器憑證、中間憑證（在某些情況下）和根憑證（也稱為根CA，因為這是簽署憑證的最高層授權）。

證書包含構建鏈的兩個主要欄位：subject和issuer。

使用者是此憑證代表的伺服器或授權單位的名稱。在Expressway-C或Expressway-E(或其他統一通訊(UC)裝置)的情況下，它是從完全限定域名(FQDN)構建的。

頒發者是驗證該特定證書的機構。由於任何人都可以對證書進行簽名（包括建立證書的伺服器，首先也稱為自簽名證書），因此伺服器和客戶端具有其信任為可信的發行者或CA的清單。

憑證鏈結一律以自簽名的頂層憑證或根憑證結尾。當您在證書層次結構中移動時，每個證書相對於主題具有不同的頒發者。最後，您會遇到主題和頒發者匹配的根CA。這表示它是頂級證書，因此是需要由客戶端或伺服器的受信任CA清單信任的證書。

SSL交握摘要

在遍歷區域的情況下，Expressway-C始終充當客戶端，而Expressway-E始終充當伺服器。簡化的Exchange的工作方式如下：

Expressway-C高速公路 — E

```
-----Client Hello----->  
<-----Server Hello-----  
<----Server Certificate-----  
<----Certificate Request—  
-----Client Certificate----->
```

此處的金鑰在交換中，因為Expressway-C總是發起連線，因此始終是客戶端。Expressway-E是第一個傳送其證書的。如果Expressway-C無法驗證此證書，它將斷開握手，並且無法向Expressway-E傳送自己的證書。

另一個需要注意的重要事項是傳輸層安全(TLS)Web客戶端身份驗證和證書上的TLS Web伺服器身份驗證屬性。這些屬性是在簽署CSR的CA上確定的（如果使用Windows CA，則由選定的模板確定），並指示憑證在使用者端或伺服器的角色中是否有效（或兩者均有）。因為對於VCS或Expressway，它可以基於具體情況（遍歷區域始終相同），並且證書必須具有客戶端和伺服器身份驗證屬性。

Expressway-C和Expressway-E在上傳到新伺服器證書時出錯（如果兩者均未應用）。

如果您不確定證書是否具有這些屬性，則可以在瀏覽器或作業系統中開啟證書詳細資訊，並檢查「擴展金鑰用法」部分（請參見映像）。格式可能不同，並取決於您如何檢視憑證。

範例：

Certificate Hierarchy

ACTIVE DIRECTORY-CA

Certificate Fields

- Extended Key Usage
- Certificate Subject Alt Name
- Certificate Subject Key ID
- Certificate Authority Key Identifier
- CRL Distribution Points
- Authority Information Access
- Object Identifier (1.3.6.1.4.1.311.21.7)
- Object Identifier (1.3.6.1.4.1.311.21.10)

Field Value

Not Critical
TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)
TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)


Export...

設定

Expressway-C和Expressway-E遍歷區域/信任

生成並簽署CSR

如前所述，Expressway-C和Expressway-E證書必須由內部或外部CA或OpenSSL簽名才能進行自簽名。

 註：不能使用Expressway伺服器上的臨時證書，因為它不受支援。如果您使用帶有CA簽名證書且未明確定義主題行的萬用字元證書，則不支援該萬用字元證書。


第一步是產生CSR，並讓其使用首選CA型別簽署。《證書建立指南》中具體介紹了此[操作的過程](#)。建立CSR時，請務必記住憑證中必須包括的必要使用者替代名稱(SAN)。證書指南和移動遠端訪問部署指南中也列出此資訊。檢視該指南的最新版本，因為新功能到達時可以新增更多內容。根據使用的功能，需要包括的常見SAN的清單：

Expressway-C

- 新增到域清單中的任何域（內部或外部）。
- 如果使用XMPP聯合，則可以使用任何持久聊天節點別名。
- 如果使用安全裝置配置檔案，則在CUCM上使用安全裝置配置檔名稱。

Expressway-E

- 在Expressway-C上配置的任何域。
- 如果使用XMPP聯合，則可以使用任何持久聊天節點別名。
- 為XMPP聯盟通告的所有域。

 注意：如果用於外部服務記錄(SRV)查詢的基礎域未作為SAN包含在Expressway-E證書(xxx.com或collab-edge.xxx.com)中，則Jabber客戶端仍要求終端使用者在第一個連線上接受證書，並且TC終端將完全無法連線。

將Expressway-C和Expressway-E配置為相互信任

為了讓統一通訊穿越區域建立連線，Expressway-C和Expressway-E必須信任彼此的證書。在本示例中，假設Expressway-E證書由使用此層次結構的公共CA簽名。

證書3

頒發者：GoDaddy根CA

主題：GoDaddy根CA

證書2

頒發者：GoDaddy根CA

主題：GoDaddy中間機構

證書1

發行商：GoDaddy中間機構

主題：Expressway-E.lab

Expressway-C需要配置信任證書1。在大多數情況下，根據應用到伺服器的受信任證書，它只傳送其最低級別的伺服器證書。這意味著，要使Expressway-C信任證書1，您必須將證書2和3上傳到Expressway-C的受信任CA清單(Maintenance > Security > Trusted CA List)。如果Expressway-C收到Expressway-E證書時省略中間證書2，它將無法將其與受信任的GoDaddy根CA關聯，因此將拒絕該證書。

證書3

頒發者：GoDaddy根CA

主題：GoDaddy根CA

證書1

頒發者：GoDaddy中間機構 — 不受信任！

主題：Expressway-E.lab

此外，如果只將沒有根的中間憑證上傳到Expressway-C的受信任CA清單，會發現GoDaddy中間授權機構受信任，但它由更高的授權機構簽署，在本案例中，GoDaddy根CA不受信任，因此它會失敗。

證書2

頒發者：GoDaddy根CA — 不受信任！

主題：GoDaddy中間機構

證書1

發行商：GoDaddy中間機構

主題：Expressway-E.lab

將所有中介軟體和根新增到受信任CA清單後，可以驗證證書……

證書3

頒發者：GoDaddy根CA — 自簽名的頂級證書受信任且鏈結完成！

主題：GoDaddy根CA

證書2

頒發者：GoDaddy根CA

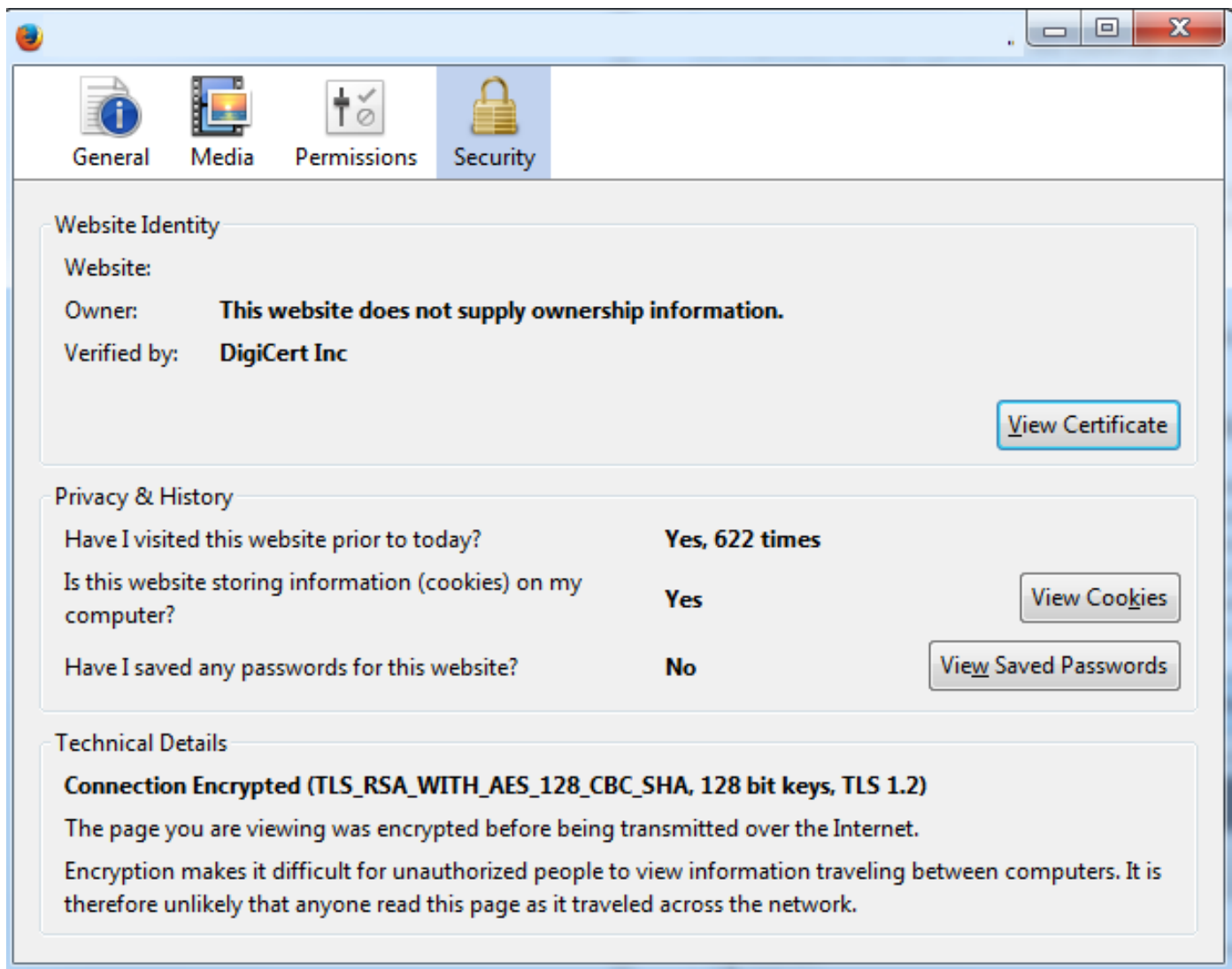
主題：GoDaddy中間機構

證書1

發行商：GoDaddy中間機構

主題：Expressway-E.lab

如果您不確定證書鏈是什麼，可以在登入到特定Expressway的Web介面時檢查瀏覽器。該過程因瀏覽器而異，但是在Firefox中，您可以按一下位址列最左側的鎖定圖示。然後在彈出視窗中，按一下更多資訊>檢視證書>詳細資訊。如果瀏覽器能將整個鏈條拼湊在一起，您就可以從上到下看到鏈條。如果頂級證書沒有匹配的主題和頒發者，則表示鏈結未完成。如果點選export並突出顯示所需的證書，則您也可以自行匯出鏈中的每個證書。如果您不完全確定您已向CA信任清單上傳了正確的證書，這將非常有用。



General Details

This certificate has been verified for the following uses:

SSL Client Certificate

SSL Server Certificate

Issued To

Common Name (CN)

Organization (O)

Organizational Unit (OU)

Serial Number

Issued By

Common Name (CN) DigiCert SHA2 High Assurance Server CA

Organization (O) DigiCert Inc

Organizational Unit (OU)

Period of Validity

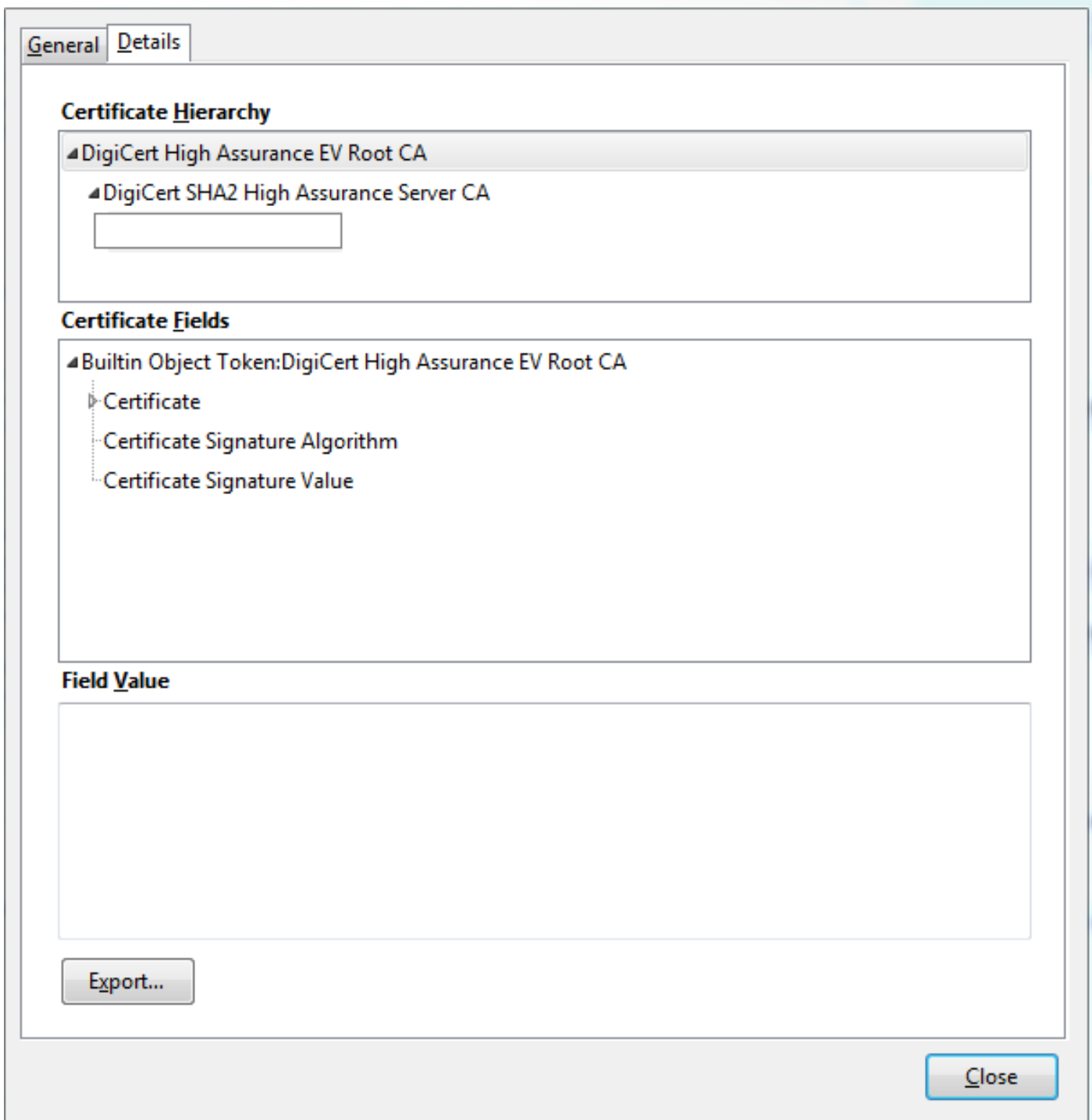
Begins On 3/25/2015

Expires On 4/12/2017

FingerprintsSHA-256 Fingerprint 3B:37:23:04:BE:92:0C:FF:2D:48:0B:52:07:5C:D5:08:
F3:75:F6:0D:43:98:8B:73:22:A4:ED:A8:E6:D7:2A:23

SHA1 Fingerprint CE:7B:79:41:94:9E:07:48:F3:A4:B4:07:03:76:D3:52:12:5D:A9:42

Close



現在Expressway-C信任來自Expressway-E的證書，請確保證書在相反方向工作。如果Expressway-C證書由簽署Expressway-E的相同CA簽署，則過程非常簡單。將已上傳到C的相同證書上傳到Expressway-E上的受信任CA清單。如果C由不同的CA簽名，則需要使用與圖中所示相同的過程，但改用已簽名的Expressway-C證書的鍵。

思科統一通信管理器(CUCM)和Expressway-C之間的安全通訊

概觀

與Expressway-C和Expressway-E之間的遍歷區域不同，Expressway-C和CUCM之間不需要安全信

令。除非內部安全策略不允許安全信令，否則必須始終將MRA配置為首先在CUCM上使用非安全裝置配置檔案，以確認其餘部署是正確的，然後再繼續此步驟。

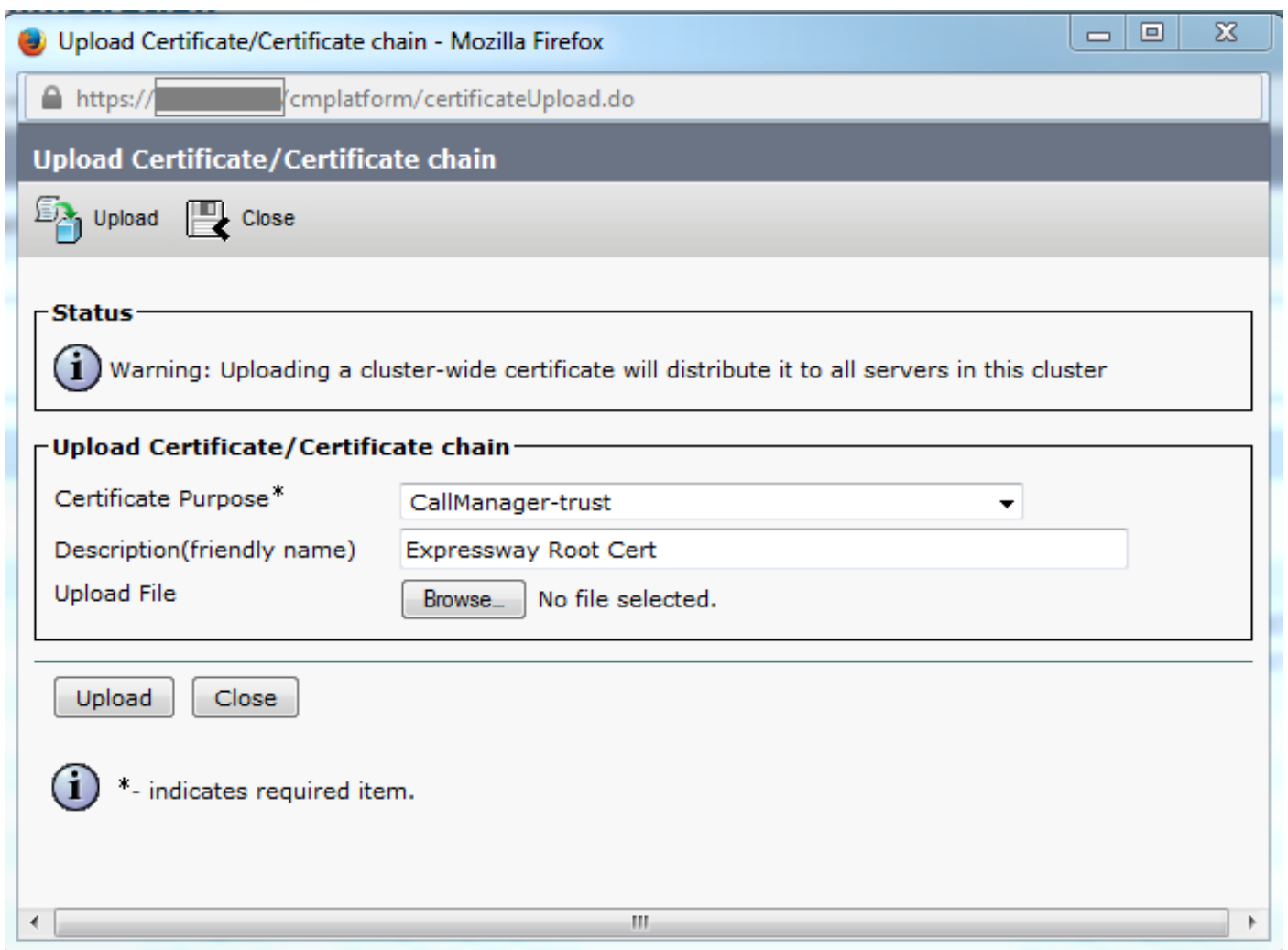
在CUCM和Expressway-C之間可以啟用兩個主要安全功能：TLS驗證和安全裝置註冊。這兩者之間有一個重要的區別，因為它們在SSL交握中使用來自CUCM端的兩個不同證書。

TLS驗證 — tomcat證書

安全SIP註冊 — CallManager證書


配置CUCM和Expressway-C之間的信任

本例中的概念與Expressway-C和Expressway-E之間的概念完全相同。CUCM必須首先信任Expressway-C的伺服器證書。這意味著，在CUCM上，需要將Expressway-C的中介和根證書上傳為TLS驗證功能的tomcat-trust證書和用於安全裝置註冊的CallManager-trust。為此，請導航至CUCM Web GUI右上角的Cisco Unified OS Administration，然後導航至Security> Certificate Management。您可以在此處按一下Upload Certificate/Certificate Chain，然後選擇正確的信任格式，或按一下Find檢視當前上傳的證書清單。



您需要確保Expressway-C信任簽署CUCM證書的CA。如果將其新增到受信任CA清單，就可以達成此目的。在幾乎所有情況下，如果您使用CA對CUCM證書進行簽名，則tomcat和CallManager證書必須由同一CA進行簽名。如果它們不同，則在使用TLS驗證和安全註冊時，您需要信任它們。

對於安全SIP註冊，還必須確保應用於裝置的CUCM上的安全裝置配置檔名稱在Expressway-C證書中列為SAN。如果其中不包含安全註冊消息，它將失敗，CUCM的403，表示TLS失敗。

 注意：當在CUCM和Expressway-C之間進行SSL握手以進行安全SIP註冊時，將發生兩次握手。首先，Expressway-C充當客戶端，並啟動與CUCM的連線。成功完成後，CUCM會啟動另一個握手，作為客戶端進行回覆。這意味著與Expressway-C一樣，CUCM上的CallManager證書必須同時應用TLS Web客戶端和TLS Web伺服器身份驗證屬性。不同之處在於，CUCM允許上傳這些證書而不使用這兩者，並且如果CUCM僅具有伺服器身份驗證屬性，則內部安全註冊可以正常工作。如果您在清單上查詢CallManager證書並選擇該證書，則可以在CUCM上確認這一點。在此，您可以檢視「擴展」部分下的用法oid。客戶端身份驗證中顯示1.3.6.1.5.5.7.3.2，伺服器身份驗證中顯示1.3.6.1.5.5.7.3.1。您還可以從此視窗下載證書。

Certificate Details(CA-signed) - Mozilla Firefox

https://[redacted]/cmplatform/certificateEdit.do?cert=/usr/local/cm/.security/CallManager/certs/CallManager.per

Certificate Details for cucm10-lab-pub.tkratzke.local, CallManager

Regenerate Generate CSR Download .PEM File Download .DER File

Status

Status: Ready


Certificate Settings


Locally Uploaded	01/04/15
File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Certificate Signed by tkratzke-ACTIVEDIRECTORY-CA

Certificate File Data

```
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100c3f0061dafbffa97cd781c9627134664cae9f55d5d92871b60ce17ddf78972963a4
1db705c43c97046df73897748e2a2459c96f7cd3cc849c71055b27ffd30dc6d4ebc727beb7a96e98ab78
01d25eb0e354086e318df242d4039004f2c569308c875697ecdf2b9040d4aa22da5b7a82f667abbd2342
0fe820dd157a648ee4c611ca8612cef49f35dd8e01677b18edca260c6aa3920da979e4adadb7ed4c776e
e1c9a28d9eaf90648cafaf757a7050ec0fc383eccbb227d0947e3265737f640e7db4d280e477689ba395
60a6a39db010fadb4e2da05beea5c8f47357726d90e56c1415c499e8d09ab36357c1223f1bae52baa82
32ba70485bd745407b354bd09d0203010001
Extensions: 9 present
[
  Extension: ExtKeyUsageSyntax (OID.2.5.29.37)
  Critical: false
  Usage oids: 1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.1,
]
```

Regenerate Generate CSR Download .PEM File Download .DER File

 注意：應用於集群中發佈者的信任證書必須複製到訂閱伺服器。最好通過在新配置上分別登入進行確認。

 註：為了使Expressway-C正確驗證來自CUCM的證書，必須在Expressway-C中新增具有FQDN而不是IP地址的CUCM伺服器。IP地址的唯一工作方式是在證書中將每個CUCM節點的IP新增為SAN，這幾乎是永遠無法完成的。

具有自簽名證書的CUCM伺服器

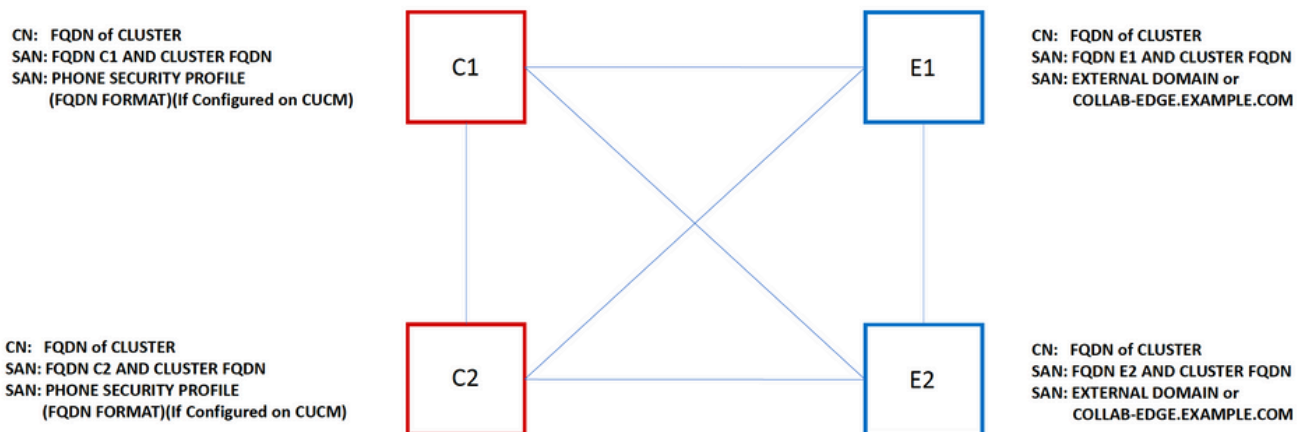
預設情況下，CUCM伺服器附帶自簽名證書。如果這些設定均已就緒，則無法同時使用TLS驗證和安全裝置註冊。任何一個功能都可以單獨使用，但由於證書是自簽名的，這意味著自簽名的Tomcat和自簽名的CallManager證書都需要上傳到Expressway-C上的受信任CA清單。當Expressway-C搜尋其信任清單以驗證證書時，它會在其找到具有匹配主題的證書時停止。因此，無論信任清單中的哪個較高者（即tomcat或CallManager），該功能都會起作用。下層會失敗，就像它不存在一樣。解決此問題的方法是使用CA（公共或私有）簽署CUCM證書，並單獨信任該CA。

Expressway-C和Expressway-E集群注意事項

群集證書

如果具有用於冗餘的Expressway-C或Expressway-E伺服器群集，則強烈建議您為每個伺服器生成單獨的CSR，並由CA對其進行簽名。在上一個場景中，每個對等體證書的公用名(CN)將是相同的群集完全限定域名(FQDN)，而SAN將是群集FQDN和相應的對等體FQDN，如下圖所示：

Expressway Cluster Certificates MRA

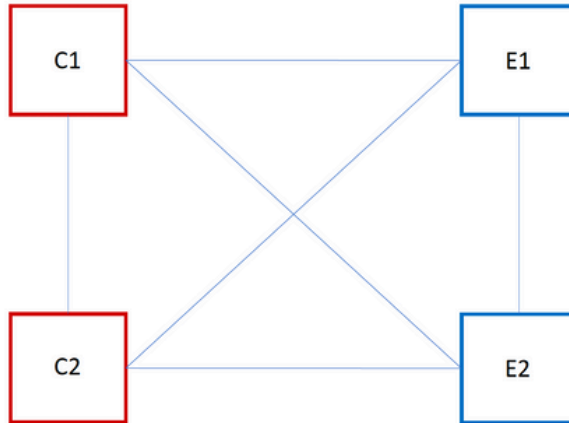


可以將群集FQDN用作CN，SAN中的每個對等體FQDN和群集FQDN對群集中的所有節點使用相同的證書，因此，可避免由公共CA簽署的多個證書的成本。

Expressway Cluster Certificates

MRA


CN: FQDN of CLUSTER
SAN: FQDN C1, FQDN C2 AND CLUSTER FQDN
SAN: PHONE SECURITY PROFILE
(FQDN FORMAT)(If Configured on CUCM)



CN: FQDN of CLUSTER
SAN: FQDN E1, FQDN E2 AND CLUSTER FQDN
SAN: EXTERNAL DOMAIN or
COLLAB-EDGE.EXAMPLE.COM

CN: FQDN of CLUSTER
SAN: FQDN C2, FQDN C1 AND CLUSTER FQDN
SAN: PHONE SECURITY PROFILE
(FQDN FORMAT)(If Configured on CUCM)

CN: FQDN of CLUSTER
SAN: FQDN E2, FQDN E1 AND CLUSTER FQDN
SAN: EXTERNAL DOMAIN or
COLLAB-EDGE.EXAMPLE.COM

 注意：只有在UCM上使用Secure Phone Security Profiles時，才需要Cs證書上的電話安全配置檔名稱。外部域或collab-edge.example.com(其中example.com是您的域)僅是通過MRA註冊IP電話和TC終端的要求。這是通過MRA註冊Jabber的可選功能。如果不存在，則jabber會在jabber通過MRA登入時提示接受證書。

如果絕對必要，這可以通過下一個過程完成，或者您可以使用OpenSSL手動產生私鑰和CSR：

步驟1.在群集的主節點上生成CSR，並將其配置為將群集別名列為CN。新增群集中的所有對等體作為備用名稱，以及所有其他必需的SAN。

步驟2.簽署此CSR並將其上傳到主要對等體。

步驟3.以root使用者身份登入到主節點，並下載位於/Tandberg/persistent/certs中的私鑰。

步驟4.將簽名證書和匹配的私鑰上傳到集群中的其他對等方。

 註：出於以下原因，不建議這樣做：

- 1.由於所有對等體使用相同的私鑰，因此存在安全風險。如果某個伺服器受到某種危害，攻擊者可以解密來自任何伺服器的流量。
- 2.如果需要變更憑證，必須再次執行整個程式，而不是簡單的產生CSR和簽署程式。

受信任的CA清單

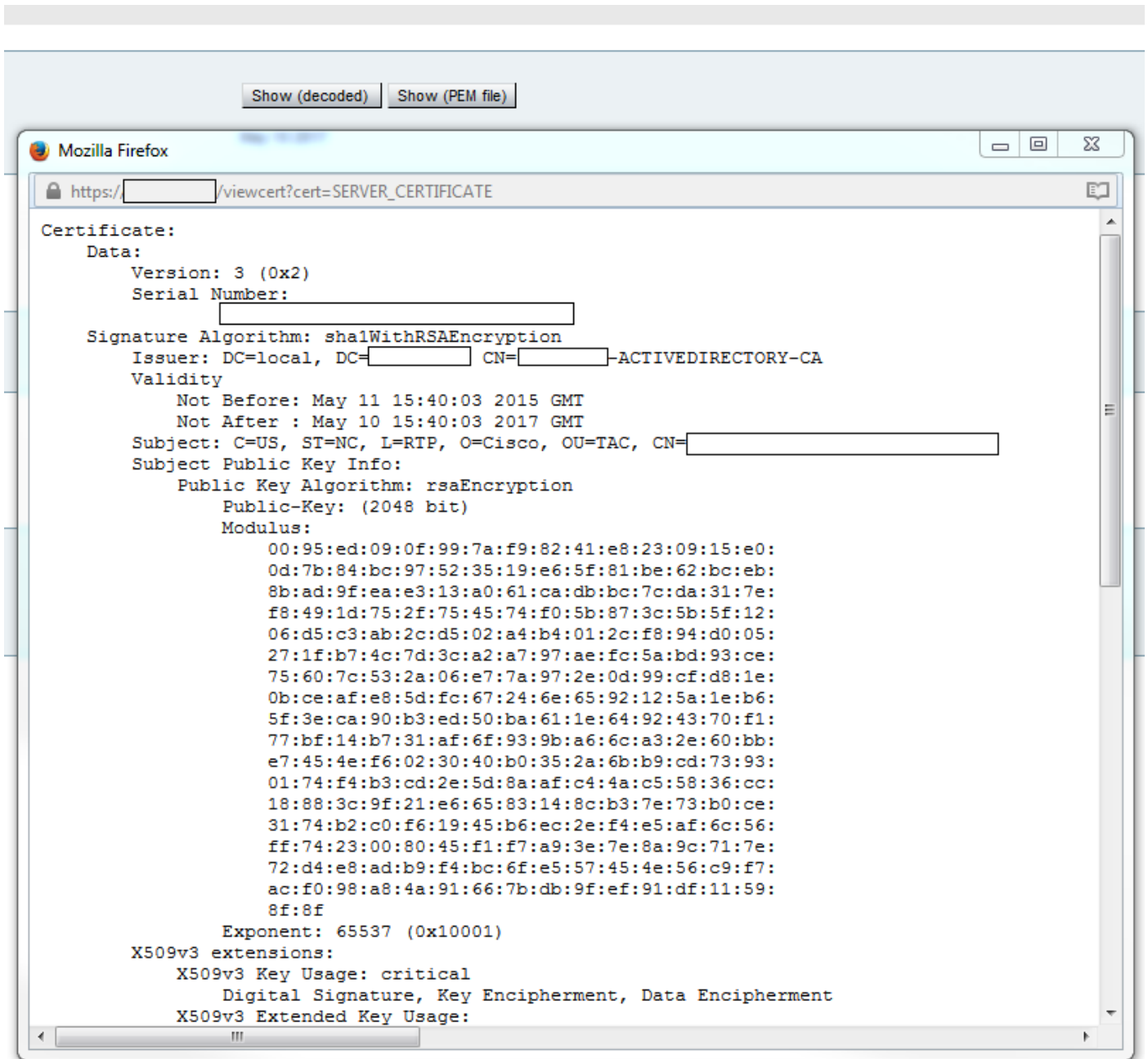
與群集中的CUCM使用者不同，在Expressway或VCS群集中，受信任的CA清單不會從一個對等體複製到另一個對等體。這表示如果您有叢集，則需要手動將受信任憑證上傳到每個對等點上的CA清單。

驗證

使用本節內容，確認您的組態是否正常運作。

檢查當前證書資訊

有多種方法可以檢查現有證書上的資訊。第一個選項是通過Web瀏覽器。使用上一節中描述的方法，該方法也可用於匯出鏈中的特定證書。如果需要驗證SAN或新增到Expressway伺服器證書的其他屬性，可以直接通過Web圖形使用者介面(GUI)執行此操作，導航到Maintenance > Security Certificates > Server Certificate，然後按一下Show Decoded。



此處您可以看到憑證的所有特定詳細資訊，而無需下載該憑證。如果尚未上傳關聯的簽名證書，則您也可以對活動CSR執行相同操作。

在Wireshark中讀取/匯出證書

如果您的SSL握手的Wireshark捕獲包括證書交換，則Wireshark實際上可以為您解碼證書，並且您

實際上可以從內部匯出鏈中的任何證書（如果交換了整個鏈）。針對證書交換的特定埠過濾資料包捕獲（在遍歷區域的情況下通常為7001）。接下來，如果您沒有看到客戶端和伺服器hello資料包以及SSL握手，請按一下右鍵TCP流中的一個資料包，然後選擇decode as。此處，選擇「SSL」，然後按一下「apply」。現在，如果您已擷取正確的流量，則必須看到憑證交換。從負載中包含證書的正確伺服器查詢資料包。展開下方窗格中的SSL區段，直到看到憑證清單，如下圖所示：

No.	Time	Source	Destination	Protocol	Length	Info
1803	2015-06-03 18:01:07.522714			TCP	74	25018→7001 [SYN] S
1806	2015-06-03 18:01:07.522835			TCP	74	7001→25018 [SYN, A
1807	2015-06-03 18:01:07.522855			TCP	66	25018→7001 [ACK] S
1808	2015-06-03 18:01:07.523594			TLSv1.2	266	Client Hello
1809	2015-06-03 18:01:07.523846			TCP	66	7001→25018 [ACK] S
1811	2015-06-03 18:01:07.538935			TLSv1.2	1514	Server Hello
1812	2015-06-03 18:01:07.538970			TCP	66	25018→7001 [ACK] S
1813	2015-06-03 18:01:07.539008			TLSv1.2	1514	Certificate

Frame 1813: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
 Ethernet II, Src: Vmware_al:14:46 (), Dst: Vmware_al:1e:e1 ()
 Internet Protocol Version 4, Src:
 Transmission Control Protocol, Src Port: 7001 (7001),
 [2 Reassembled TCP Segments (2541 bytes): #1811(1390), #1813(1151)]
 Secure Sockets Layer
 TLSv1.2 Record Layer: Handshake Protocol: Certificate
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 2536
 Handshake Protocol: Certificate
 Handshake Type: Certificate (11)
 Length: 2532
 Certificates Length: 2529
 Certificates (2529 bytes)
 Certificate Length: 1612
 Certificate (id-at-commonName= , id-at-organizationalUnitName= , id-at-organizationNA
 Certificate Length: 911
 Certificate (id-at-commonName= -ACTIVEDIRECTORY-CA, dc= , dc=)

您可以在此處展開任何憑證以檢視所有詳細資訊。如果要匯出證書，請按一下右鍵鏈中所需的證書（如果有多個證書），然後選擇Export Selected Packet Bytes。輸入證書名稱，然後按一下Save。現在，您必須能夠在Windows證書檢視器中開啟證書（如果為其提供.cer副檔名），或者將其上傳到任何其他工具進行分析。

疑難排解

本節提供的資訊用於對組態進行疑難排解。

測試以瞭解Expressway上的證書是否受信任

雖然最佳方法是手動檢查證書鏈並確保所有成員都包含在Expressway信任CA清單中，但您可以快速檢查，以確保Expressway在Web GUI中維護>安全證書下的客戶端證書測試幫助信任特定客戶端的證書。保持所有預設設定相同。從下拉選單中選擇Upload Test File(pem format)，然後選擇要驗證的客戶端證書。如果憑證不受信任，您會收到錯誤（如圖所示），說明遭拒絕的原因。您看到的錯誤是上傳憑證的解碼資訊以供參考。

Client certificate testing

Client certificate

Certificate source: Uploaded test file (PEM format) ⓘ

Select the file you want to test: Browse... No file selected. ⓘ

Currently uploaded test file: pm-vcsc01.cer

This tests whether a client certificate is valid when checked against the Expressway certificate authority.

Certificate-based authentication pattern

Regex to match against certificate: /Subject:.*CN=(?<captureCommonName>{[^\,\\]}(\,))*/m

Username format: #captureCommonName#

Make these settings permanent

This section applies only if your certificate contains authentication credential username format combinations to the nominated certificate to see if the certificate matches the nominated certificate.

Check certificate

Certificate test results

Valid certificate: Invalid: The client certificate is not signed by a CA in the trusted CA list.

如果您收到錯誤，聲稱Expressway無法獲取證書CRL，但Expressway未使用CRL檢查，則這意味著證書將受信任並已通過所有其他驗證檢查。

Client certificate testing

Client certificate

Certificate source: Uploaded test file (PEM format) ⓘ

Select the file you want to test: Browse... No file selected. ⓘ

Currently uploaded test file: vcs.cer

This tests whether a client certificate is valid when checked against the Expressway certificate authority.

Certificate-based authentication pattern

Regex to match against certificate: /Subject:.*CN=(?<captureCommonName>{[^\,\\]}(\,))*/m

Username format: #captureCommonName#

Make these settings permanent

This section applies only if your certificate contains authentication credential username format combinations to the nominated certificate to see if the certificate matches the nominated certificate.


Check certificate


Certificate test results


Valid certificate: Invalid: unable to get certificate CRL, please ensure that you have uploaded a CRL for the CA that signed this client certificate


Synergy Light終端 (7800/8800系列電話)

這些新裝置隨附預填充的證書信任清單，其中包括大量眾所周知的公共CA。無法修改此信任清單，這意味著您的Expressway-E證書必須由其中一個匹配的公共CA簽名才能使用這些裝置。如果是由內部CA或其他公共CA簽署，則連線將失敗。使用者沒有選項可手動接受與Jabber客戶端相同的證書。

 註：對於某些部署，使用具有7800/8800系列電話上所包括清單中的CA的Citrix NetScaler等裝置可以通過MRA註冊，即使Expressway-E使用內部CA也是如此。需要將NetScalers根CA上傳到Expressway-E，並且需要將內部根CA上傳到Netscaler以使SSL身份驗證生效。事實證明，這一策略行之有效，是盡最大努力的支援。

 註：如果受信任的CA清單似乎包含所有正確的證書，但仍被拒絕，請確保清單中沒有具有相同主題的另一個證書可能與正確的證書衝突。當所有其它方法都失敗時，您始終可以從瀏覽器或Wireshark直接匯出鍵，並將所有證書上傳到對方的伺服器CA清單。這將保證它是受信任的證書。

 注意：排除遍歷區域故障時，有時問題可能看起來與證書有關，但實際上問題出在軟體方面。確保用於遍歷的帳戶使用者名稱和密碼正確。

 註：VCS或Expressway在證書的SAN欄位中不支援超過999個字元。任何超過此限制的SAN (需要許多備用名稱) 將被忽略，就像它們不存在一樣。

影片資源

本節提供的影片資訊可以指導您完成所有證書配置過程。

[為MRA或群集Expressway生成CSR](#)

[將伺服器證書安裝到Expressway](#)

[如何在Expressway之間配置證書信任](#)

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）。