

# 解決合作邊緣最常見的問題

## 目錄

[簡介](#)

[背景資訊](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[登入問題](#)

[Jabber無法通過MRA登入](#)

[1.未建立合作邊緣服務記錄\(SRV\)和/或無法連線埠8443](#)

[2. VCS Expressway上的證書不可接受或不可用](#)

[3.在邊緣配置中找不到UDS伺服器](#)

[4. Expressway-C日誌顯示以下錯誤： XCP\\_JABBERD Detail=無法連線到主機「%IP%」，埠7400:\(111\)連線被拒絕](#)

[5. Expressway-E伺服器主機名/域名與 collab-edge SRV中的配置不匹配](#)

[6.由於當前的WebEx Connect訂閱，無法登入](#)

[7. Expressway-C伺服器顯示錯誤消息：「已配置但出現錯誤。正在設定伺服器：正在等待穿越伺服器資訊。」](#)

[8.已安裝Microsoft DirectAccess](#)

[9. Expressway反向DNS查詢失敗](#)

[註冊問題](#)

[軟電話無法註冊，不允許SIP/2.0 405方法](#)

[Softphone無法註冊，原因="未知域"](#)

[軟電話無法註冊，原因是「空閒倒計時已過期」](#)

[由於韌體中配置了電話代理，MRA失敗](#)

[呼叫 — 相關問題](#)

[通過MRA呼叫時無介質](#)

[通過MRA呼叫到PSTN時無回鈴](#)

[CUCM和IM&P問題](#)

[阻止新增CUCM的ASCII錯誤](#)

[5061上從Expressway-C到CUCM的安全部署中的出站TLS故障](#)

[未新增IM&P伺服器且遇到錯誤](#)

[其他問題](#)

[Jabber客戶端上的語音郵件狀態顯示「未連線」](#)

[聯絡人照片不會通過Expressway顯示在Jabber客戶端上](#)

[Jabber客戶端在登入期間提示接受Expressway-E證書](#)

[相關資訊](#)

## 簡介

本文檔介紹如何解決客戶在部署階段面臨的最常見合作邊緣問題。

## 背景資訊

移動和遠端訪問(MRA)是用於虛擬專用無網路(VPN)Jabber功能的部署解決方案。此解決方案允許終端使用者從全球任何地方連線到內部企業資源。編寫本指南是為了使對Collaboration Edge解決方案進行故障排除的工程師能夠快速確定並解決客戶在部署階段面臨的最常見問題。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 思科整合通訊管理員(CUCM)
- Cisco Expressway核心
- Cisco Expressway邊緣
- Cisco IM和狀態(IM&P)
- Windows版Cisco Jabber
- Mac版Cisco Jabber
- Cisco Jabber for Android
- Cisco iOS版Jabber
- 安全憑證
- 網域名稱系統(DNS)

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Expressway版本X8.1.1或更高版本
- CUCM 9.1(2)SU1或更高版本和IM&P 9.1(1)或更高版本
- Cisco Jabber 9.7或更高版本

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。

## 登入問題

### Jabber無法通過MRA登入

此症狀可能由一系列問題引起，其中某些問題將在此處概述。

#### 1.未建立合作邊緣服務記錄(SRV)和/或無法連線埠8443

要使Jabber客戶端能夠成功使用MRA登入，必須建立特定的合作邊緣SRV記錄並且可從外部訪問。當Jabber客戶端最初啟動時，它將進行DNS SRV查詢：

1. **\_cisco-uds**:此SRV記錄用於確定CUCM伺服器是否可用。
2. **\_cuplogin**：此SRV記錄用於確定是否有IM&P伺服器。
3. **\_collab-edge**:此SRV記錄用於確定MRA是否可用。

如果已啟動Jabber使用者端，但未收到\_cisco-uds和\_cuplogin的SRV回應，且未收到\_collab-edge的回應，則它會使用此回應嘗試連線在SRV回應中列出的Expressway-E。

\_collab-edge SRV記錄指向埠8443的Expressway-E的完全限定域名(FQDN)。如果\_collab-edge SRV未建立，或不在外部可用，或如果它可用，但無法訪問埠8443，則Jabber客戶端無法登入。

您可以確認\_collab-edge SRV記錄是否可解析，以及使用[Collaboration Solutions Analyzer\(CSA\)中的SRV檢查器是否可以訪問TCP埠8443](#)。

如果連線埠8443無法連線，則可能是由於安全裝置(防火牆)封鎖連線埠，或因為Exp-E中的預設閘道(GW)或靜態路由組態錯誤。

## 2. VCS Expressway上的證書不可接受或不可用

在Jabber客戶端收到\_collab-edge的答案後，它會通過埠8443與具有傳輸層安全(TLS)的Expressway聯絡，嘗試從Expressway檢索證書，以設定TLS來進行Jabber客戶端和Expressway之間的通訊。

如果Expressway沒有包含Expressway FQDN或域的有效簽名證書，則此操作會失敗，並且Jabber客戶端無法登入。

如果發生此問題，請在Expressway上使用證書簽名請求(CSR)工具，該工具會自動將Expressway的FQDN作為使用者替代名稱(SAN)包括在內。

**注意:**MRA要求在Expressway-C和Expressway-E之間以及Expressway-E和外部終端之間進行安全通訊。

在[MRA部署指南](#)中可找到具有Expressway證書要求功能的下一個表：

Table 1. CSR Alternative Name Element and Unified Communications Features

Add These Items as Subject Alternative Names	When Generating a CSR for These Purposes			
	Mobile and Remote Sccess	Jabber guest	XMPP Federation	Business to Business Calls
Unified CM registrations domains (despite their name, these have more in common with service discovery domains than with Unified CM Unified CM SIP registration domains)	Required on Expressway-E only	–	–	–
XMPP federation domains	–	–	Required on Expressway-E only	–
IM and Presence Service chat node aliases (federated group chat)	–	–	Required	–
Unified CM phone security profile names	Required on Expressway-C only	–	–	–
(Clustered systems only) Expressway cluster name	Required on Expressway-C only	Required on Expressway-C only	Required on Expressway-C only	–

## 3.在邊緣配置中找不到UDS伺服器

Jabber使用者端成功建立與Expressway-E的安全連線後，會要求進行邊緣組態(get\_edge\_config)。此邊緣配置包含\_cuplogin和\_cisco-uds的SRV記錄。如果在邊緣配置中未返回\_cisco-uds SRV記錄，則Jabber客戶端無法繼續登入。

若要解決此問題，請確保\_cisco-uds SRV記錄已在內部建立，並且可由Expressway-C解析。

有關DNS SRV記錄的詳細資訊，請參閱[X8.11的MRA部署指南](#)。

如果您位於雙域中，這也是一個常見症狀。如果您在雙域中運行，並且發現Jabber客戶端未返回任何使用者資料服務(UDS)，則必須確認在內部DNS中與外部域一起建立了\_cisco-uds SRV記錄。

註：在Expressway版本X12.5之後，不再需要將\_cisco-UDS SRV記錄新增到內部DNS。有關此增強功能的詳細資訊，請參閱[通過Cisco Expressway的移動和遠端訪問部署指南\(X12.5\)](#)。

#### 4. Expressway-C日誌顯示以下錯誤：XCP\_JABBERD Detail=無法連線到主機「%IP%」，埠7400:(111)連線被拒絕

如果Expressway-E網路介面控制器(NIC)配置不正確，可能會導致無法更新可擴展通訊平台(XCP)伺服器。如果Expressway-E符合以下標準，則可能會遇到此問題：

1. 使用單個NIC。
2. 高級網路選項金鑰已安裝。
3. Use Dual Network Interfaces選項設定為**Yes**。

要解決此問題，請將Use Dual Network Interfaces選項更改為**No**。

出現此問題的原因是Expressway-E在錯誤的網路介面上偵聽XCP會話，從而導致連線失敗/超時。Expressway-E在TCP埠7400上監聽XCP會話。如果您使用 netstat命令。

#### 5. Expressway-E伺服器主機名/域名與\_collab-edge SRV中的配置不匹配

如果DNS頁面配置中的Expressway-E伺服器主機名/域與\_collab-edge SRV應答中收到的不匹配，則Jabber客戶端無法與Expressway-E通訊。Jabber客戶端使用get\_edge\_config響應中的xmppEdgeServer/Address元素建立到Expressway-E的XMPP連線。

以下是從Expressway-E到Jabber客戶端的get\_edge\_config響應中xmppEdgeServer/Address的示例：

```
<xmppEdgeServer>
<server>
<address>examplelab-vcse1.example URL</address>
<tlsPort>5222</tlsPort>
</server>
</xmppEdgeServer>
```

為了避免這種情況，請確保\_collab-edge SRV記錄與Expressway-E主機名/域名匹配。已為此錯誤歸檔思科錯誤ID [CSCuo83458](#)，並且已在思科錯誤ID [CSCuo82526](#)上新增部分支援。

#### 6. 由於當前的WebEx Connect訂用，無法登入

Windows版Jabber日誌顯示以下內容：

```
2014-11-22 19:55:39,122 INFO [0x00002808] [very\WebexCasLookupDirectorImpl.cpp(134)]
[service-discovery] [WebexCasLookupDirectorImpl::makeCasLookupWhenNetworkIs
Available] - makeCasLookupForDomain result is 'Code: IS_WEBEX_CUSTOMER; Server:
http://URL server;
Url: http://example URL server';;.2014-11-22
19:55:39,122 INFO [0x00002808] [overly\WebexCasLookupDirectorImpl.cpp(67)]
```

```
[service-discovery] [WebexCasLookupDirectorImpl::determineIsWebexCustomer] -
Discovered Webex Result from server. Returning server result.2014-11-22 19:55:39,122
DEBUG [0x00002808] [ery\WebexCasLookupUrlConfigImpl.cpp(102)]
[service-discovery] [WebexCasLookupUrlConfigImpl::setLastCasUrl] - setting last_cas_
lookup_url : http://example URL server2014-11-22
19:55:39,123 DEBUG [0x00002808] [pters\config\ConfigStoreManager.cpp(286)]
[ConfigStoreManager] [ConfigStoreManager::storeValue] - key : [last_cas_lookup_url]
value : [http://example URL server/cas/FederatedSSO?org=example URL]2014-11-22
19:55:39,123 DEBUG [0x00002808] [common\processing\TaskDispatcher.cpp(29)]
[TaskDispatcher] [Processing::TaskDispatcher::enqueue] - Enqueue ConfigStore::persist
Values - Queue Size: 02014-11-22 19:55:39,123 DEBUG [0x00002808] [pters\config\ConfigStore
Manager.cpp(140)]
[ConfigStoreManager] [ConfigStoreManager::getValue] - key : [last_cas_lookup_url]
skipLocal : [0] value: [http://website URL/cas/FederatedSSO?org=example URL]
success: [true] configStoreName: [LocalFileConfigStore]
```

登入嘗試定向到WebEx Connect。

若要獲得永久解決方案，必須聯絡[WebEx](#)才能停用該網站。

## 因應措施

在短期內，您可以使用這些選項之一將其從查詢中排除。

- 將此引數新增到jabber-config.xml中。然後將jabber-config.xml檔案上傳到CUCM上的TFTP伺服器。它要求客戶端首先在內部登入。

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
<Policies>
<ServiceDiscoveryExcludedServices>WEBEX<
/ServiceDiscoveryExcludedServices>
</Policies>
</config>
```

- 從應用程式的角度來看，請運行以下命令：  
`msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=CUP EXCLUDED_SERVICES=WEBEX`

註：第二個選項不適用於流動裝置。

- 建立一個可點選的URL，其中排除WEBEX服務：  
`ciscojabber://provision?ServiceDiscoveryExcludedServices=WEBEX`

有關UC服務發現以及如何在[Cisco Jabber 12.8本地部署中排除某些服務的詳細資訊](#)，請參閱。

## 7. Expressway-C伺服器顯示錯誤消息：「已配置但出現錯誤。正在設定伺服器：正在等待穿越伺服器資訊。」

如果導航到Status > Unified Communications並看到錯誤消息，"Configured but with errors. Provisioning server: Waiting for traversal server info." 對於Unified CM註冊和IM&P服務，在Expressway-C上配置的內部DNS伺服器具有兩個Expressway-E的DNS A記錄。Expressway-E的多個DNS A記錄背後的原因可能是受影響的使用者從在Expressway-E上啟用了靜態NAT的單個NIC移動到啟用了靜態NAT的雙個NIC，反之亦然，並且忘記刪除內部DNS伺服器中適當的DNS A記錄。因此，當您在Expressway-C中使用DNS查詢實用程式並解析Expressway-E FQDN時，您會注意到兩個DNS A記錄。

## 解決方案

如果為Expressway-E NIC配置了靜態NAT:

1. 刪除Expressway-C中配置的DNS伺服器中Expressway-E內部IP地址的DNS A記錄。
2. 通過CMD刷新Expressway-C中的DNS快取和使用者PC(ipconfig /flushdns)。
3. 重新啟動Expressway-C伺服器。

如果Expressway-E NIC配置為啟用靜態NAT的雙NIC:

1. 刪除Expressway-C中配置的DNS伺服器中Expressway-E 外部IP地址的DNS A記錄。
2. 通過CMD刷新Expressway C和使用者PC中的DNS快取(ipconfig /flushdns)。
3. 重新啟動Expressway-C伺服器。

## 8. 已安裝Microsoft DirectAccess

如果客戶在與Jabber客戶端相同的PC上使用Microsoft DirectAccess，則當您嘗試遠端登入時，可能會中斷MRA。DirectAccess強制將DNS查詢通過隧道傳送到內部網路，就像PC使用VPN一樣。

**註:**Microsoft DirectAccess不受Jabber over MRA支援。任何故障排除都是盡力而為。DirectAccess的配置由網路管理員負責。

有些客戶成功阻止了Microsoft DirectAccess名稱解析策略表中的所有DNS記錄。DirectAccess不會處理這些記錄（Jabber需要能夠通過MRA的公共DNS解析這些記錄）：

- \_cisco-uds的SRV記錄
- CUPLOGIN的SRV記錄(\_C)
- \_collab-edge的SRV記錄
- 所有Expressway Es的記錄

## 9. Expressway反向DNS查詢失敗

從X8.8版本開始，Expressway/VCS要求為ExpE、ExpC和所有CUCM節點建立正向和反向DNS條目。

有關完整要求，請參閱[移動和遠端訪問的x8.8發行說明](#)和DNS記錄中的[前提條件和軟體相關性](#)。

如果內部DNS記錄不存在，Expressway日誌中可能會出現引用reverseDNSLookup的錯誤：

```
2016-07-30T13:58:11.102-06:00 hostname XCP_JABBERD[20026]: UTCTime="2016-07-30 19:58:11,102"  
ThreadID="139882696623872" Module="Jabber" Level="WARN " CodeLocation="cvsservice.cpp:409" Detail="caught exception:  
exception in reverseDNSLookup: reverse DNS lookup failed for address=x.x.x.x"
```

查詢Expressway-E IP的PTR記錄時，Expressway-C僅收到一個FQDN。如果從DNS收到錯誤的FQDN，則會在日誌中顯示此行並失敗：

```
2020-04-03T17:48:43.685-04:00 hostname XCP_JABBERD[10043]: UTCTime="2020-04-03 21:48:43,685"  
ThreadID="140028119959296" Module="Jabber" Level="WARN " CodeLocation="cvsservice.cpp:601" Detail="Certificate  
verification failed for host=xx.xx.xx.xx, additional info: Invalid Hostname"
```

## 註冊問題

軟電話無法註冊，不允許SIP/2.0 405方法

來自Expressway-C的診斷日誌顯示 SIP/2.0 405 Method Not Allowed 消息響應Jabber客戶端傳送的註冊請求。這可能是因為連線埠5060/5061的Expressway-C和CUCM之間的目前作業階段啟始通訊協定(SIP)主幹所造成。

#### SIP/2.0 405 Method Not Allowed

```
Via: SIP/2.0/TCP 10.10.40.108:5060;egress-zone=CollabZone;branch=z9hG4bK81e7f5f1c1ab5450c0b406c91fcbdf181249.81ba6621f0f43eb4f9c0dc0db83fb291;proxy-call-id=da9e25aa-80de-4523-b9bc-be31ee1328ce;rport,SIP/2.0/TLS 10.10.200.68:7001;egress-zone=TraversalZone;branch=z9hG4bK55fc42260aa6a2e3741919177aa84141920.a504aa862a5e99ae796914e85d3527fe;proxy-call-id=6e43b657-d409-489c-9064-3787fc4919b8;received=10.10.200.68;rport=7001;ingress-zone=TraversalZone,SIP/2.0/TLS 192.168.1.162:50784;branch=z9hG4bK3a04bdf3;received=172.18.105.10;rport=50784;ingress-zone=CollaborationEdgeZone
From: <sip:5151@collabzone>;tag=cb5c78b12b4401ec236e1642-1077593a
To: <sip:5151@collabzone>;tag=981335114
Date: Mon, 19 Jan 2015 21:47:08 GMT
Call-ID: cb5c78b1-2b4401d7-26010f99-0fa7194d@192.168.1.162
Server: Cisco-CUCM10.5
CSeq: 1105 REGISTER
```

**Warning: 399 collabzone "SIP trunk disallows REGISTER"**

Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY  
Content-Length: 0

若要更正此問題，請將應用於在CUCM中配置的當前SIP中繼的SIP中繼安全配置檔案上的SIP埠和CUCM的Expressway-C鄰居區域更改為其他埠，例如5065。本影片將對此作進一步說明。以下是組態摘要：

## CUCM

1. 建立一個新的SIP中繼安全配置檔案，該配置檔案具有非5060(5065)的偵聽埠。
2. 建立與SIP中繼安全配置檔案相關聯的SIP中繼，並將目的地設定為Expressway-C IP地址，埠5060。

## Expressway-C

1. 建立與CUCM的鄰居區域，且目標埠不是5060(5065)，以匹配CUCM配置。
2. 在Expressway-C Settings > Protocols > SIP中，確保Expressway-C仍然在5060上偵聽SIP。

## 軟體電話無法註冊，原因="Unknown domain"

來自Expressway-C的診斷日誌顯示事件="Registration Rejected" Reason="Unknown domain" Service="SIP" Src-ip="XXX.XXX.XXX" Src-port="51601" Protocol="TCP" AOR="sip:XXX.XXX.XXX.XXX"。

若要更正此問題，請檢查以下幾點：

- 當目的不是使用非安全裝置安全配置檔案時，Jabber客戶端是否在CUCM中使用安全裝置安全配置檔案？
- 如果Jabber客戶端使用安全的裝置安全配置檔案，則安全配置檔案的名稱是否為FQDN格式，以及該FQDN名稱是否在Expressway-C證書上配置為SAN？
- 如果Jabber客戶端使用安全的裝置安全配置檔案，請導航到System > Enterprise Parameters > Security Parameters > Cluster Security Mode，並檢查群集安全模式是否設定為1，以驗證CUCM群集是否已受到保護。如果值為0，則管理員必須完成所記錄的過程以保護群集。

## 軟體電話無法註冊，原因 "Idle countdown expired"

在Jabber客戶端傳送註冊消息的時間範圍內檢視Expressway-E日誌時，請查詢 `Idle countdown expired` 錯誤，如這裡的代碼片斷所示。

```
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"  
Module="network.tcp" Level="DEBUG": Src-ip="JabberPubIP" Src-port="4211"  
Dst-ip="VCS-E_IP" Dst-port="5061" Detail="TCP Connecting"  
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"  
Module="network.tcp" Level="DEBUG": Src-ip="JabberPubIP" Src-port="4211" Dst-ip=  
"VCS-E_IP" Dst-port="5061" Detail="TCP Connection Established" 2015-02-02T19:46:49+01:00  
collabedge tvcs: UTCTime="2015-02-02 18:46:49,606"  
Module="network.tcp" Level="DEBUG": Src-port="4211" Dst-ip=  
"VCS-E_IP" Dst-port="5061" Detail="TCP Connection Closed" Reason="Idle  
countdown expired"
```

此代碼片斷表示防火牆確實開啟了埠5061；但是，在足夠長的時間內沒有傳遞的應用層流量，因此TCP連線關閉。

如果您遇到這種情況，Expressway-E前面的防火牆很有可能開啟SIP檢測/應用層網關(ALG)功能。若要修正此問題，您必須停用此功能。如果您不確定如何執行此操作，請參閱防火牆供應商產品文檔。

有關SIP檢測/ALG的詳細資訊，請參閱[Cisco Expressway-E和Expressway-C基本配置部署指南](#)的附錄4。

## 由於韌體中配置了電話代理，MRA失敗

來自Expressway-E的診斷日誌在埠5061中顯示TLS協商失敗，但在埠8443中成功進行SSL握手。

```
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,533" Module="network.tcp" Level="DEBUG": Src-  
port="24646" Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connecting"  
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,534" Module="network.tcp" Level="DEBUG": Src-  
port="24646" Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connection Established"  
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,535" Module="developer.ssl" Level="ERROR"  
CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(67)" Method="::TTSSLerOutput" Thread="0x7fae4ddb1700":  
TTSSL_continueHandshake: Failed to establish SSL connection  
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,535" Module="network.tcp" Level="DEBUG": Src-  
port="24646" Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connection Closed" Reason="Got EOF on socket"  
2015-08-04T10:14:23-05:00 expe tvcs: Event="Inbound TLS Negotiation Error" Service="SIP" Src-port="24646" Dst-ip="10.2.0.2"  
Dst-port="5061" Detail="No SSL error available, probably remote disconnect" Protocol="TLS" Level="1" UTCTime="2015-08-04  
15:14:23,535"
```

Jabber日誌：

```
-- 2015-08-04 10:48:04.775 ERROR [ad95000] - [csf.cert.][checkIdentifiers] Verification of identity: 'URL address' failed.  
-- 2015-08-04 10:48:04.777 INFO [ad95000] - [csf.cert.][handlePlatformVerificationResultSynchronously] Verification result :  
FAILURE reason : [CN_NO_MATCH UNKNOWN]  
-- 2015-08-04 10:48:05.284 WARNING [ad95000] - [csf.ecc.handymiron][ssl_state_callback] SSL alert read:fatal:handshake failure  
type=eSIP, isRelevant=true, server=URL server name:5061, connectionState=eFailed, isEncrypted=true,  
failureReason=eTLSError, SSLErrorCode=336151568  
type=eSIP, isRelevant=true, server=192.168.102.253:5060, connectionState=eFailed, isEncrypted=false,  
failureReason=eFailedToConnect, serverType=ePrimary, role=eNone  
-- 2015-08-04 10:48:05.287 ERROR [ad95000] - [csf.ecc.handymiron][secSSLIsConnected] SSL_do_handshake() returned :  
SSL_ERROR_SSL.
```

來自Jabber的封包擷取顯示與Expressway E IP的SSL交涉；但傳送的憑證並非來自此伺服器：



3813	2015-08-05 12:59:30.811036000	192.168.1.89	97.84.35.116	TLSv1	247 Client Hello
3829	2015-08-05 12:59:30.980461000	97.84.35.116	192.168.1.89	TLSv1	1045 Server Hello, Certificate, Certificate Request, Server Hello Done
3883	2015-08-05 12:59:31.313432000	192.168.1.89	97.84.35.116	TLSv1	252 Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
3887	2015-08-05 12:59:31.341712000	97.84.35.116	192.168.1.89	TLSv1	61 Alert (Level: Fatal, Description: Handshake Failure)

```

Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 539
Certificates Length: 536
Certificates (536 bytes)
Certificate Length: 533
Certificate (id-at-commonName=_internal_PP_ct_phoneproxy_file,id-at-organizationalUnitName=STG,id-at-organizationName=Cisco Inc)
  signedCertificate
  algorithmIdentifier (shaWithRSAEncryption)
    Padding: 0
    encrypted: 5d1944c311d1741f9b003995eca3b06a0a3e9f2bd49aa60c...

```

FW已配置電話代理。

## 解決方案：

確認FW運行電話代理。若要檢查這一點，請輸入 `show run policy-map` 命令時，會顯示類似以下內容：

```

class sec_sip
inspect sip phone-proxy ASA-phone-proxy

```

禁用電話代理，以便電話服務成功連線。

## 呼叫 — 相關問題

### 通過MRA呼叫時無介質

以下是一些缺少和不正確的配置，這些配置可能會導致單NIC和雙NIC部署中出現此問題：

- Expressway-E中的System > Network Interfaces > IP下未配置靜態NAT。網路層的NAT仍然需要在防火牆中完成，但是此設定會轉換應用層的IP。
- 防火牆中的TCP/UDP埠未開啟。有關埠清單，請參閱[Cisco Expressway IP埠使用配置指南](#)

建議不要使用具有靜態NAT部署的單個NIC。以下是防止介質問題的注意事項：

issing

- 在UC遍歷區域中，Expressway-C需要指向Expressway-E中配置的公共IP地址。
- 介質必須「發卡」或在外部防火牆中反射。在[為VCS Expressway TelePresence裝置在ASA上配置NAT反射](#)中，可以找到思科ASA防火牆的配置示例。

有關此問題的詳細資訊，請參閱[Cisco Expressway-E和Expressway-C基本配置部署指南的附錄4](#)。

### 通過MRA呼叫到PSTN時無回鈴

此問題是由於X8.5之前的版本對Expressway的限制。思科錯誤ID [CSCua72781](#)描述了Expressway-C如何在183會話進度或180在遍歷區域中振鈴時轉發早期媒體。如果運行版本X8.1.x或X8.2.x，可以升級到版本X8.5，也可以執行此處列出的解決方法。

如果您的SIP配置檔案將183轉換為180並將其應用於傳入撥號對等體，則可以在思科統一邊界元素(CUBE)上使用解決方法。例如：

```
voice class sip-profiles 11
```

```
response 183 sip-header SIP-StatusLine modify "SIP/2.0 183 Session Progress"  
"SIP/2.0 180 Ringing"
```

然後，他們將在CUCM > CUBE的SIP配置檔案或CUBE本身的sip-ua配置模式下禁用180 Early Media。

```
disable-early-media 180
```

## CUCM和IM&P問題

### 阻止新增CUCM的ASCII錯誤

將CUCM新增到Expressway-C時，會遇到阻止新增CUCM的ASCII錯誤。

當Expressway-C將CUCM新增到其資料庫時，它會運行一系列與get和list函式相關的AXL查詢。這些示例包括getCallManager、listCallManager、listProcessNode、listProcessNodeService和getCCMVersion。運行getCallManager進程後，ExecuteSQLQuery設定將成功檢索所有CUCM Call Manager-trust或tomcat-trust。

一旦CUCM收到查詢並在查詢上執行，CUCM就會報告回其所有證書。如果其中一個證書包含非ASCII字元，則Expressway會在Web介面中生成錯誤，類似於 `ascii codec can't decode byte 0xc3 in position 42487: ordinal not in range(128)`。

此問題已使用思科錯誤ID [CSCuo5489](#)跟蹤，並在X8.2版中解決。

### 5061上從Expressway-C到CUCM的安全部署中的出站TLS故障

當您在CUCM和Tomcat.pem/CallManager.pem上使用自簽名證書時，會出現此問題。此問題已透過思科錯誤ID [CSCun30200](#)解決。糾正此問題的解決方法是刪除tomcat.pem並從Expressway-C上的CUCM配置中禁用「TLS驗證」。

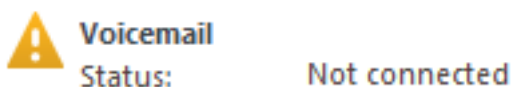
### 未新增IM&P伺服器且遇到錯誤

新增IM&P伺服器時，Expressway-C會報告「此伺服器不是IM and Presence Server」或「無法與.AXL查詢HTTP錯誤「HTTPError:500」，從而導致無法新增IM&P伺服器。

作為新增IM&P伺服器的一部分，Expressway-C使用AXL查詢在顯式目錄中查詢IM&P證書。由於思科錯誤ID [CSCul05131](#)，證書不在該儲存區中；因此您會遇到錯誤資訊。

## 其他問題

### Jabber客戶端上的語音郵件狀態顯示「未連線」



為了使Jabber客戶端語音郵件狀態成功連線，必須在Expressway-C上的HTTP允許清單中配置Cisco Unity Connection IP地址或主機名。

要從Expressway-C完成此操作，請執行相關步驟：

## X8.1和X8.2版的程式

1. 按一下**Configuration > Unified Communications > Configuration > Configure HTTP server allow list**。
2. 按一下**New > Enter IP/Hostname > Create entry**。
3. 註銷Jabber客戶端，然後重新登入。

## X8.5版的過程

1. 按一下**Configuration > Unified Communications > Unity Connection Servers**。
2. 按一下**New > Enter IP/Hostname, User account credentials > Add Address**。
3. 註銷Jabber客戶端，然後重新登入。

## 聯絡人照片不會通過Expressway顯示在Jabber客戶端上

移動和遠端訪問解決方案僅利用UDS來解析聯絡人照片。這要求您有一台可用於儲存照片的Web伺服器。該配置本身是雙重的。

1. 必須修改jabber-config.xml檔案，才能將客戶端定向到Web伺服器以解析聯絡人照片。此處的配置實現了這一點。

```
<Directory>
<DirectoryServerType>UDS</DirectoryServerType>
<PhotoUriWithToken>http://%IP/Hostname%/photo%uid%.jpg<
/PhotoUriWithToken>
<UdsServer>%IP%</UdsServer>
<MinimumCharacterQuery>3</MinimumCharacterQuery>
</Directory>
```

2. Expressway-C必須在HTTP伺服器允許清單中列出Web伺服器。

按一下**Configuration > Unified Communications > Configuration > Configure HTTP server allow list**。按一下**New > Enter IP/Hostname > Create entry**。註銷Jabber客戶端，然後重新登入。

**注意：**有關UDS聯絡人照片解析的詳細資訊，請參閱[Jabber聯絡人照片文檔](#)。

## Jabber客戶端在登入期間提示接受Expressway-E證書

## Verify Certificate



Certificate not valid

Your computer cannot confirm the identity of this server.  
This could be an attempt by an unknown party to connect to your computer and access confidential information.  
If you are not sure if you should continue, contact your system administrator. Tell the administrator that Cisco Jabber is prompting you to accept the [redacted] certificate.

Show Certificate

Accept

Decline

此錯誤消息可能與未由客戶端裝置信任的公共CA簽名的Expressway邊緣證書，或者該域在伺服器證書中缺少作為SAN的CA有關。

要從Expressway證書接受提示中停止Jabber客戶端，必須滿足下面列出的兩個條件：

- 運行Jabber客戶端的裝置/電腦必須在其證書信任儲存中列出Expressway-E證書的簽名者。

**注意：**如果您使用公共證書頒發機構，則很容易完成此操作，因為流動裝置包含大型證書信任儲存。

- 用於collab-edge記錄的Unified CM註冊域必須存在於Expressway-E證書的SAN中。Expressway伺服器中的CSR工具為您提供將Unified CM註冊域新增為SAN的選項，如果該域配置為MRA，則預載入該工具。如果簽署憑證的CA不接受網域作為SAN，您還可以使用「CollabEdgeDNS」選項，該選項會將字首「collab-edge」新增到網域中：

Unified CM registrations domains	<input type="text" value="tp-cisco.com"/>	Format	CollabEdgeDNS
Alternative name as it will appear	DNS: [redacted]		
	DNS:collab-edge.tp-cisco.com		

## 相關資訊

- [Expressway上的移動和遠端訪問指南](#)
- [Cisco Expressway證書建立和使用部署指南](#)
- [Cisco TelePresence Video Communication Server\(Cisco VCS\)IP埠的使用用於防火牆穿越](#)
- [Cisco Jabber部署和安裝指南](#)
- [技術支援與文件 - 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）。