

合作邊緣TC型終端配置示例

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[步驟1.在CUCM上以FQDN格式建立安全電話配置檔案 \(可選\)。](#)

[步驟2.確保集群安全模式為\(1\) — 混合 \(可選\)。](#)

[步驟3.在CUCM中為基於TC的終端建立配置檔案。](#)

[步驟4.將安全配置檔名稱新增到Expressway-C/VCS-C證書的SAN中 \(可選\)。](#)

[步驟5.將UC域新增到Expressway-E/VCS-E證書。](#)

[步驟6.將適當的受信任CA證書安裝到基於TC的終端。](#)

[步驟7.為邊緣調配設定基於TC的終端](#)

[驗證](#)

[基於TC的終端](#)

[CUCM](#)

[Expressway-C](#)

[疑難排解](#)

[工具](#)

[TC端點](#)

[高速公路](#)

[CUCM](#)

[問題1:Collab-edge記錄不可見和/或主機名不可解析](#)

[TC終端日誌](#)

[補救](#)

[問題2:CA不在基於TC的終端上的受信任CA清單中](#)

[TC終端日誌](#)

[補救](#)

[問題3:Expressway-E沒有在SAN中列出UC域](#)

[TC終端日誌](#)

[Expressway-E SAN](#)

[補救](#)

[問題4:TC設定配置檔案中提供的使用者名稱和/或密碼不正確](#)

[TC終端日誌](#)

[Expressway-C/VCS-C](#)

[補救](#)

[第五期：基於TC的終端註冊被拒絕](#)

[CUCM跟蹤](#)

[TC端點](#)

[實際Expressway-C/VCS-C](#)

[補救](#)

簡介

本文檔介紹通過移動和遠端訪問解決方案配置基於網真編解碼器(TC)的終端註冊並對其進行故障排除所需的內容。

必要條件

需求

思科建議您瞭解以下主題：

- 移動和遠端訪問解決方案
- 視訊通訊伺服器(VCS)憑證
- Expressway X8.1.1或更高版本
- Cisco Unified Communication Manager(CUCM)版本9.1.2或更高版本
- 基於TC的終端
- CE8.x需要加密選項金鑰以啟用「邊緣」作為調配選項

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- VCS X8.1.1或更高版本
- CUCM 9.1(2)SU1或更高版本以及IM & Presence 9.1(1)或更高版本
- TC 7.1或更高版本的韌體 (**建議使用TC7.2**)
- VCS控制與Expressway/Expressway核心與邊緣
- CUCM
- TC端點

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

這些配置步驟假定管理員將配置基於TC的終端以進行安全裝置註冊。安全註冊不是要求的，但整體移動和遠端訪問解決方案指南給人的印象是，因為配置中有螢幕截圖顯示CUCM上的安全裝置配置檔案。

步驟1.在CUCM上以FQDN格式建立安全電話配置檔案 (可選) 。

1. 在CUCM中，選擇System > Security > Phone Security Profile。
2. 按一下「Add New」。
3. 選擇基於TC的終端型別並配置以下引數：
4. 名稱 — Secure-EX90.tbtp.local (需要FQDN格式)

5. 裝置安全模式 — 已加密
6. 傳輸型別 — TLS
7. SIP電話埠 — 5061

Phone Security Profile Configuration

Save ✖ Delete Copy Reset Apply Config + Add New

Status

i Add successful

Phone Security Profile Information

Product Type: Cisco TelePresence EX90

Device Protocol: SIP

Name*

Description

Nonce Validity Time*

Device Security Mode

Transport Type*

Enable Digest Authentication

TFTP Encrypted Config

Exclude Digest Credentials in Configuration File

Phone Security Profile CAPF Information

Authentication Mode*

Key Size (Bits)*

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Parameters used in Phone

SIP Phone Port*

Save Delete Copy Reset Apply Config Add New

步驟2.確保集群安全模式為(1) — 混合 (可選)。

1. 在CUCM中，選擇System > Enterprise Parameters。
2. 向下滾動至Security Parameters > Cluster Security Mode > 1。

Security Parameters

Cluster Security Mode *	1
---	---

如果該值不是1，則未保護CUCM。如果是這種情況，管理員需要檢視這兩個文檔之一以保護CUCM。

[CUCM 9.1\(2\)安全指南](#)

[CUCM 10安全指南](#)

步驟3.在CUCM中為基於TC的終端建立配置檔案。

1. 在CUCM中，選擇**Device > Phone**。
2. 按一下「**Add New**」。
3. 選擇基於TC的終端型別並配置以下引數：
MAC地址 — 基於TC的裝置的MAC地址必填星型欄位(*)
所有者 — 使用者所有者
使用者ID — 與裝置關聯的所有者裝置安全配置檔案 — 先前配置的配置檔案(Secure-EX90.tbtp.local)
SIP配置檔案 — 標準SIP配置檔案或以前建立的任何自定義配置檔案

The screenshot shows the 'Phone Configuration' page in CUCM. At the top, there are navigation buttons: Save, Delete, Copy, Reset, Apply Config, and Add New. A 'Status' bar indicates 'Update successful'. The main configuration area is divided into several sections:

- Association Information:** Shows two lines: 'Line 1 [1] - 9211 in Baseline_TelePresence_PT' and 'Line 2 [2] - Add a new DN'. A 'Modify Button Items' button is present.
- Phone Type:** Product Type: Cisco TelePresence EX90, Device Protocol: SIP.
- Device Information:** Registration: Unknown, IP Address: Unknown, Device is Active (checked), Device is trusted (checked), MAC Address*: 00506006EAFE, Description: Stoj EX90, Device Pool*: Baseline_TelePresence-DP, Common Device Configuration: < None >, Phone Button Template*: Standard Cisco TelePresence EX90, Common Phone Profile*: Standard Common Phone Profile.
- Owner:** Owner User ID*: pstoiano, Phone Load Name: (empty).
- Protocol Specific Information:** Packet Capture Mode*: None, Packet Capture Duration: 0, BLF Presence Group*: Standard Presence group, MTP Preferred Originating Codec*: 711ulaw, Device Security Profile*: Secure-EX90.tbtp.local, Rerouting Calling Search Space: < None >, SUBSCRIBE Calling Search Space: < None >, SIP Profile*: Standard SIP Profile For Cisco VCS, Digest User: < None >. There are also checkboxes for 'Media Termination Point Required', 'Unattended Port', and 'Require DTMF Reception', all of which are currently unchecked.

步驟4.將安全配置檔名稱新增到Expressway-C/VCS-C證書的SAN中 (可選) 。

1. 在Expressway-C/VCS-C中，導航到**維護>安全證書>伺服器證書**。
2. 按一下「**Generate CSR**」。

- 填寫「證書簽名請求(CSR)」欄位，並確保Unified CM電話安全配置檔名稱具有完全限定域名(FQDN)格式中列出的準確電話安全配置檔案。例如Secure-EX90.tbtp.local。附註：Unified CM電話安全配置檔名稱列在Subject Alternate Name(SAN)欄位的後面。
- 將CSR寄送到內部或第三方憑證授權單位(CA)以簽署。
- 選擇**Maintenance > Security Certificates > Server Certificate**，將證書上傳到Expressway-C/VCS-C。

Generate CSR You are here: [Maintenance](#) > [Security cert](#)

Common name

Common name: FQDN of Expressway ⓘ

Common name as it will appear: RTP-TBTP-EXPRVY-C1.tbtp.local

Alternative name

Subject alternative names: FQDN of Expressway cluster plus FQDNs of all peers in the cluster ⓘ

Additional alternative names (comma separated): ⓘ

IM and Presence chat node aliases (federated group chat): conference-2-StandAloneCluster5ad9a.tbtp.local Format: XMPPAddress ⓘ

Unified CM phone security profile names: Secure-EX90.tbtp.local ⓘ

Alternative name as it will appear: DNS:RTP-TBTP-EXPRVY-C.tbtp.local
DNS:RTP-TBTP-EXPRVY-C1.tbtp.local
DNS:RTP-TBTP-EXPRVY-C2.tbtp.local
XMPP:conference-2-StandAloneCluster5ad9a.tbtp.local
DNS:Secure-EX90.tbtp.local

Additional information

Key length (in bits): 4096 ⓘ

Country: * US ⓘ

State or province: * NC ⓘ

Locality (town name): * RTP ⓘ

Organization (company name): * Cisco ⓘ

Organizational unit: * TelePresence ⓘ

步驟5.將UC域新增到Expressway-E/VCS-E證書。

- 在Expressway-E/VCS-E中，選擇**Maintenance > Security Certificates > Server Certificate**。
- 按一下「**Generate CSR**」。
- 填寫CSR欄位並確保「Unified CM註冊域」包含基於TC的終端將以域名伺服器(DNS)或服務名稱(SRV)格式向其發出合作邊緣(collab-edge)請求的域。
- 將CSR傳送給要簽署的內部或第三方CA。
- 選擇**Maintenance > Security Certificates > Server Certificate**，將證書上傳到Expressway-E/VCS-E。

Generate CSR You are here: [Maintenance](#) > [Security](#)

Common name

Common name: FQDN of Expressway cluster ⓘ

Common name as it will appear: RTP-TBTP-EXPRWY-E

Alternative name

Subject alternative names: FQDN of Expressway cluster plus FQDNs of all peers in the cluster ⓘ

Additional alternative names (comma separated): tbtpt.local ⓘ

Unified CM registrations domains: tbtpt.local Format: SRVName ⓘ

Alternative name as it will appear:

```
DNS:RTP-TBTP-EXPRWY-E
DNS:RTP-TBTP-EXPRWY-E2.tbtpt.local
DNS:RTP-TBTP-EXPRWY-E1.tbtpt.local
DNS:tbtpt.local
SRV:_collab-edge._tls.tbtpt.local
```

Additional information

Key length (in bits): 4096 ⓘ

Country: * US ⓘ

State or province: * NC ⓘ

Locality (town name): * RTP ⓘ

Organization (company name): * Cisco ⓘ

Organizational unit: * TelePresence ⓘ

步驟6.將適當的受信任CA證書安裝到基於TC的終端。

1. 在基於TC的終端中，選擇 **Configuration > Security**。
2. 選擇 **CA** 頁籤，並瀏覽到簽署 Expressway-E/VCS-E 證書的 CA 證書。
3. 按一下 **Add certificate authority**。附註：成功新增證書後，您將看到該證書在「證書」清單中列出。

Security

Successfully imported the certificate. Please reboot for changes to take effect.

Certificates **CAs** Preinstalled CAs Strong Security Mode Non-persistent Mode CUCM

Certificate	Issuer	
heras-W2K8VM3-CA	heras-W2K8VM3-CA	Delete... <input type="button" value="View Certificate"/>

Add Certificate Authority

CA file:

This system supports PEM formatted files (.pem) with one or more CA certificates within the file.

附註：TC 7.2 包含預安裝 CA 清單。如果簽署 Expressway E 證書的 CA 包含在此清單中，則無需執行本節列出的步驟。

Home Call Control **Configuration** Diagnostics Maintenance admin

Security

Certificates CAs **Preinstalled CAs** Strong Security Mode Non-persistent Mode CUCM

This CA list is used for Cisco UCM via Expressway (Edge) provisioning only.
Configure provisioning now.

These certificates are used to validate the servers contacted over the internet when the endpoint uses UCM via Expressway provisioning. The certificates can be enabled and disabled individually, or all of them at once using the "Disable All/Enable All" button. Note that this button only affects the certificates listed on this page. Certificates and certificate authorities uploaded globally on the system are not affected.

Certificate	Issuer			Disable All
A-Trust-nQual-03	A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	Details...	✓	Disable
AAA Certificate Services	Comodo CA Limited	Details...	✓	Disable
AC Raíz Certicámara S.A.	Sociedad Cameral de Certificación Digital - Certicámara S.A.	Details...	✓	Disable
ACEDICOM Root	EDICOM	Details...	✓	Disable
AddTrust External CA Root	AddTrust AB	Details...	✓	Disable

附註：預安裝CA頁面包含一個方便的「立即配置調配」按鈕，該按鈕可讓您直接進入下一節的步驟2中所述的所需配置。

步驟7.為邊緣調配設定基於TC的終端

- 在基於TC的終端中，選擇**Configuration > Network**，並確保在DNS部分下正確填寫這些欄位：
 域名
 伺服器位址
- 在基於TC的終端中，選擇**Configuration > Provisioning**，並確保正確填寫以下欄位：
 LoginName — 在CUCM中定義
 模式 — **邊緣**
 密碼 — 在CUCM中定義
 外部管理員
 Address - Expressway-E/VCS-E的主機名
 域 — 存在合作邊緣記錄的域

Provisioning

[Refresh](#)[Collapse all](#)[Expand all](#)

Connectivity	External	Save
HttpMethod	GET	Save
LoginName	pstojano	Save (0 to 80 characters)
Mode	Edge	Save
Password		Save (0 to 64 characters)

ExternalManager		
Address	RTP-TBTP-EXPRWY-E.tbtp.local	Save (0 to 64 characters)
AlternateAddress		Save (0 to 64 characters)
Domain	tbtp.local	Save (0 to 64 characters)
Path		Save (0 to 255 characters)
Protocol	HTTPS	Save

驗證

使用本節內容，確認您的組態是否正常運作。

基於TC的終端

1. 在Web GUI中，導航到「Home」。查詢「SIP Proxy 1」部分以獲取「已註冊」狀態。代理地址是您的Expressway-E/VCS-E。

SIP Proxy 1

Status:	Registered
Proxy:	105.108
URI:	9211@tbtp.local

2. 在CLI中輸入`xstatus //prov`。如果您已註冊，您應該會看到「已布建」的布建狀態。

```
xstatus //prov
*s Network 1 IPv4 DHCP ProvisioningDomain: ""
*s Network 1 IPv4 DHCP ProvisioningServer: ""
*s Provisioning CUCM CAPF LSC: Installed
*s Provisioning CUCM CAPF Mode: IgnoreAuth
*s Provisioning CUCM CAPF OperationResult: NotSet
*s Provisioning CUCM CAPF OperationState: NonPending
*s Provisioning CUCM CAPF ServerName: ""
```



```

*s Provisioning CUCM CAPF ServerPort: 0
*s Provisioning CUCM CTL State: Installed
*s Provisioning CUCM ExtensionMobility Enabled: False
*s Provisioning CUCM ExtensionMobility LastLoggedInUserId: ""
*s Provisioning CUCM ExtensionMobility LoggedIn: False
*s Provisioning CUCM ITL State: Installed
*s Provisioning CUCM ProvisionSecurity: Signed
*s Provisioning CUCM TVS Proxy 1 IPv6Address: ""
*s Provisioning CUCM TVS Proxy 1 Port: 2445
*s Provisioning CUCM TVS Proxy 1 Priority: 0
*s Provisioning CUCM TVS Proxy 1 Server: "xx.xx.97.131"
*s Provisioning CUCM UserId: "pstoiano"
*s Provisioning NextRetry: ""
*s Provisioning Reason: ""
*s Provisioning Server: "xx.xx.97.131"
*s Provisioning Software Current CompletedAt: ""
*s Provisioning Software Current URL: ""
*s Provisioning Software Current VersionId: ""
*s Provisioning Software UpgradeStatus LastChange: "2014-06-30T19:08:40Z"
*s Provisioning Software UpgradeStatus Message: ""
*s Provisioning Software UpgradeStatus Phase: None
*s Provisioning Software UpgradeStatus SecondsUntilUpgrade: 0
*s Provisioning Software UpgradeStatus SessionId: ""
*s Provisioning Software UpgradeStatus Status: None
*s Provisioning Software UpgradeStatus URL: ""
*s Provisioning Software UpgradeStatus VersionId: ""
*s Provisioning Status: Provisioned
** end

```

CUCM

在CUCM中，選擇**Device > Phone**。滾動清單或根據您的終端過濾清單。您應該會看到「已向 %CUCM_IP%註冊」消息。此右邊的IP地址應該是代理註冊的Expressway-C/VCS-C。



Expressway-C

- 在Expressway-C/VCS-C中，選擇**Status > Unified Communications > View Provisioning sessions**。
- 根據基於TC的終端的IP地址進行過濾。圖中所示為已布建的作業階段的範例：

Records: 2 Page 1 of 1

Username	Device	User agent	Unified CM server	Expire time
pstoiano	252.227	Cisco/TC	97.131	2014-09-25 02:08:53

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

註冊問題可能是由多種因素造成的，包括DNS、證書問題、配置等。此部分包含一個完整清單，列出遇到給定問題時通常看到的內容以及如何補救。如果您遇到已記錄內容以外的問題，請隨時將其包括在內。

工具

首先，請注意可供您使用的工具。

TC端點

Web GUI

- all.log
- 開始擴展日誌記錄 (包括完整資料包捕獲)

CLI

以下命令對於即時故障排除最為有用：

- log ctx HttpClient debug 9
- log ctx PROV調試9
- log output on < — 顯示通過控制檯日誌記錄

重新建立問題的有效方法是在Web GUI中將布建模式從「Edge」切換到「Off」，然後返回「Edge」。您還可以進入xConfiguration Provisioning Mode:命令。

高速公路

- [診斷日誌](#)
- tcpdump

CUCM

- SDI/SDL跟蹤

問題1:Collab-edge記錄不可見和/或主機名不可解析

您可以看到，由於名稱解析，get_edge_config失敗。

TC終端日誌

```
15716.23 HttpClient HTTPClientCurl error
(https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/):
'Couldn't resolve host name'
```

```
15716.23 PROV ProvisionRequest failed: 4 (Couldn't resolve host name)
15716.23 PROV I: notify_http_done: Received 0 (Couldn't resolve host name) on request
https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/
```

補救

1. 驗證是否存在合作邊緣記錄並返回正確的主機名。
2. 驗證客戶端上配置的DNS伺服器資訊是否正確。

問題2:CA不在基於TC的終端上的受信任CA清單中

TC終端日誌

```
15975.85 HttpClient      Trying xx.xx.105.108...
15975.85 HttpClient Adding handle: conn: 0x48390808
15975.85 HttpClient Adding handle: send: 0
15975.86 HttpClient Adding handle: recv: 0
15975.86 HttpClient Curl_addHandleToPipeline: length: 1
15975.86 HttpClient - Conn 64 (0x48396560) send_pipe: 0, recv_pipe: 0
15975.87 HttpClient - Conn 65 (0x4835a948) send_pipe: 0, recv_pipe: 0
15975.87 HttpClient - Conn 67 (0x48390808) send_pipe: 1, recv_pipe: 0
15975.87 HttpClient Connected to RTP-TBTP-EXPRWY-E.tbtp.local (xx.xx.105.108)
port 8443 (#67)
15975.87 HttpClient successfully set certificate verify locations:
15975.87 HttpClient CAfile: none
CApath: /config/certs/edge_ca_list
15975.88 HttpClient Configuring ssl context with special Edge certificate verifier
15975.88 HttpClient SSLv3, TLS handshake, Client hello (1):
15975.88 HttpClient SSLv3, TLS handshake, Server hello (2):
15975.89 HttpClient SSLv3, TLS handshake, CERT (11):
15975.89 HttpClient SSLv3, TLS alert, Server hello (2):
15975.89 HttpClient SSL certificate problem: self signed certificate in
certificate chain
15975.89 HttpClient Closing connection 67
15975.90 HttpClient HTTPClientCurl error
(https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/):
'Peer certificate cannot be authenticated with given CA certificates'

15975.90 PROV ProvisionRequest failed: 4 (Peer certificate cannot be
authenticated with given CA certificates)
15975.90 PROV I: notify_http_done: Received 0 (Peer certificate cannot be
authenticated with given CA certificates) on request
https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/
15975.90 PROV EDGEProvisionUser: start retry timer for 15 seconds
```

補救

1. 驗證終端上的**Security > CAs**頁籤下是否列出了第三方CA。
2. 如果列出了CA，請驗證它是否正確。

問題3:Expressway-E沒有在SAN中列出UC域

TC終端日誌

```
82850.02 CertificateVerification ERROR: [verify_edge_domain_in_san]: Edge TLS
verification failed: Edge domain 'tbtp.local' and corresponding SRVName
'_collab-edge.tls.tbtp.local' not found in certificate SAN list
82850.02 HttpClient SSLv3, TLS alert, Server hello (2):
82850.02 HttpClient SSL certificate problem: application verification failure
82850.02 HttpClient Closing connection 113
82850.02 HttpClient HTTPClientCurl error
(https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/):
'Peer certificate cannot be authenticated with given CA certificates'
```

Expressway-E SAN

```
X509v3 Subject Alternative Name:
DNS:RTP-TBTP-EXPRWY-E.tbtp.local, SRV:_collab-edge.tls.tbtp.local
```

補救

1. 重新生成Expressway-E CSR以包括UC域。
2. 在TC終結點上，ExternalManager Domain引數可能未設定為UC Domain的值。如果是這種情況，您必須匹配它。

問題4:TC設定配置檔案中提供的使用者名稱和/或密碼不正確

TC終端日誌

```
83716.67 HttpClient      Server auth using Basic with user 'pstojano'
83716.67 HttpClient GET /dGJ0cC5jb20/get_edge_config/ HTTP/1.1
Authorization: xxxxxxx
Host: RTP-TBTP-EXPRWY-E.tbtp.local:8443
Cookie: JSESSIONIDSSO=34AFA4A6DEE1DDCE8B1D2694082A6D0A
Content-Type: application/x-www-form-urlencoded
Accept: text/xml
User-Agent: Cisco/TC
Accept-Charset: ISO-8859-1,utf-8
83716.89 HttpClient HTTP/1.1 401 Unauthorized
83716.89 HttpClient Authentication problem. Ignoring this.
83716.90 HttpClient WWW-Authenticate: Basic realm="Cisco-Edge"
83716.90 HttpClient Server CE_C ECS is not blacklisted
83716.90 HttpClient Server: CE_C ECS
83716.90 HttpClient Date: Thu, 25 Sep 2014 17:42:51 GMT
83716.90 HttpClient Age: 0
83716.90 HttpClient Transfer-Encoding: chunked
83716.91 HttpClient Connection: keep-alive
83716.91 HttpClient
83716.91 HttpClient 0
83716.91 HttpClient Connection #116 to host RTP-TBTP-EXPRWY-E.tbtp.local
left intact
83716.91 HttpClient HTTPClientCurl received HTTP error 401

83716.91 PROV ProvisionRequest failed: 5 (HTTP code=401)
83716.91 PROV I: notify_http_done: Received 401 (HTTP code=401) on request
https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/
```

Expressway-C/VCS-C

```
2014-09-25T13:46:20-04:00 RTP-TBTP-EXPRWY-C edgeconfigprovisioning
UTCTime="2014-09-25 17:46:20,92" Module="network.http.edgeconfigprovisioning"
Level="DEBUG" Action="Received"
Request-url="https://xx.xx.97.131:8443/cucm-uds/user/pstojano/devices"
HTTPMSG:
|HTTP/1.1 401 Unauthorized
Expires: Wed, 31 Dec 1969 19:00:00 EST
Server:
Cache-Control: private
Date: Thu, 25 Sep 2014 17:46:20 GMT
Content-Type: text/html;charset=utf-8
WWW-Authenticate: Basic realm="Cisco Web Services Realm"

2014-09-25T13:46:20-04:00 RTP-TBTP-EXPRWY-C UTCTime="2014-09-25 17:46:20,92"
Module="developer.edgeconfigprovisioning.server" Level="DEBUG"
CodeLocation="edgeprotocol(1018)" Detail="Failed to authenticate user against server"
Username="pstojano" Server="('https', 'xx.xx.97.131', 8443)"
Reason="<twisted.python.failure.Failure <type 'exceptions.Exception'>>"
"2014-09-25T13:46:20-04:00 RTP-TBTP-EXPRWY-C edgeconfigprovisioning:"
```

```
Level="INFO" Detail="Failed to authenticate user against server" Username="pstoiano"
Server="('https', 'xx.xx.97.131', 8443)" Reason="<twisted.python.failure.Failure
<type 'exceptions.Exception'>>" UTCTime="2014-09-25 17:46:20,92"
```

補救

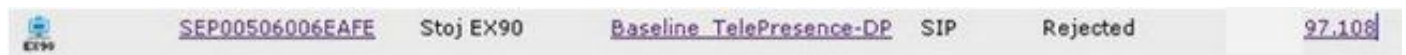
1. 驗證在TC終端上的Provisioning頁面下輸入的使用者名稱/密碼是否有效。
2. 針對CUCM資料庫驗證憑據。
3. 版本10 — 使用自助服務門戶
4. 版本9 — 使用CM使用者選項

兩個入口的URL相同：<https://%CUCM%/ucmuser/>

如果出現許可權不足錯誤，請確保將這些角色分配給使用者：

- 已啟用標準CTI
- 標準CCM終端使用者

第五期：基於TC的終端註冊被拒絕



CUCM跟蹤

```
08080021.043 |16:31:15.937 |AppInfo |SIPStationD(18400) - validTLSConnection:TLS
InvalidX509NameInCertificate, Rcvd=RTP-TBTP-EXPRWY-C.tbtp.local,
Expected=SEP00506006EAFE. Will check SAN the next
08080021.044 |16:31:15.937 |AppInfo |SIPStationD(18400) - validTLSConnection:TLS
InvalidX509NameInCertificate Error , did not find matching SAN either,
Rcvd=RTP-TBTP-EXPRWY-C.tbtp.local, Expected=Secure-EX90.tbtp.local
08080021.045 |16:31:15.937 |AppInfo |ConnectionFailure - Unified CM failed to open
a TLS connection for the indicated device Device Name:SEP00506006EAFE
IP Address:xx.xx.97.108 IPV6Address: Device type:584 Reason code:2 App ID:Cisco
CallManager Cluster ID:StandAloneCluster Node ID:RTP-TBTP-CUCM9 08080021.046
|16:31:15.938 |AlarmErr |AlarmClass: CallManager, AlarmName: ConnectionFailure,
AlarmSeverity: Error, AlarmMessage: , AlarmDescription: Unified CM failed to open
a TLS connection for the indicated device, AlarmParameters:
DeviceName:SEP00506006EAFE, IPAddress:xx.xx.97.108, IPV6Address:,
DeviceType:584, Reason:2, AppID:Cisco CallManager, ClusterID:StandAloneCluster,
NodeID:RTP-TBTP-CUCM9,
```

TC端點

SIP Proxy 1

Status:

Failed: 403 Forbidden

實際Expressway-C/VCS-C

X509v3 Subject Alternative Name:

DNS:RTP-TBTP-EXPRWY-C.tbtp.local, XMPP:conference-2-StandAloneCluster5ad9a.tbtp.local

在此特定日誌示例中，Expressway-C/VCS-C在SAN中顯然不包含電話安全配置檔案FQDN。

(Secure-EX90.tbtp.local)。在傳輸層安全(TLS)握手中，CUCM檢查Expressway-C/VCS-C的伺服器

證書。由於在SAN中找不到該配置檔案，因此它會拋出粗體錯誤，並報告其預期使用FQDN格式的電話安全配置檔案。

補救

1. 驗證Expressway-C/VCS-C在其伺服器證書的SAN中包含FQDN格式的電話安全配置檔案。
2. 如果您使用FQDN格式的安全配置檔案，請確認裝置在CUCM中使用正確的安全配置檔案。
3. 這也可能由Cisco錯誤ID [CSCuq86376](#)引起。如果是這種情況，請檢查Expressway-C/VCS-C SAN大小和電話安全配置檔案在SAN中的位置。

第六期：基於TC的終端調配失敗 — 無UDS伺服器

此錯誤必須在Diagnostics > Troubleshooting下出現

```
Error: Provisioning Status
Provisioning failed: XML didnt contain UDS server address
```

TC終端日誌

向右滾動檢視粗體錯誤

```
9685.56 PROV      REQUEST_EDGE_CONFIG:
9685.56 PROV      <?xml version='1.0' encoding='UTF-8'?>
9685.56 PROV      <getEdgeConfigResponse version="1.0"><serviceConfig><service><name>_cisco-phone-
tftp</name><error>NameError</error></service><service><name>_cuplogin</name><error>NameError</er
ror></service><service><name>_cisco-
uds</name><server><priority>1</priority><weight>1</weight><port>8443</port><address>cucm.domain.
int</address></server></service><service><name>tftpServer</name><address></address><address></ad
dress></service></serviceConfig><edgeConfig><sipEdgeServer><server><address>expe.domain.com</add
ress><tlsPort>5061</tlsPort></server></sipEdgeServer><sipRequest><route>&lt; sip:192.168.2.100:50
61;transport=tls;zone-
id=3;directed;lr&gt;</route></sipRequest><xmppEdgeServer><server><address>expe.domain.com</addre
ss><tlsPort>5222</tlsPort></server></xmppEdgeServer><httpEdgeServer><server><address>expe.domain
.com</address><tlsPort>8443</tlsPort></server></httpEdgeServer><turnEdgeServer/>

      </edgeConfig></getEdgeConfigResponse>
9685.57 PROV ERROR: Edge provisioning failed!
url='https://expe.domain.com:8443/ZXuY2hlZ2cuY29t/get_edge_config/', message='XML didn't
contain UDS server address'
9685.57 PROV      EDGEProvisionUser: start retry timer for 15 seconds
9700.57 PROV I: [statusCheck] No active VcsE, reprovisioning!
```

補救

1. 確保有一個服務配置檔案和CTI UC服務與終端使用者帳戶相關聯，該帳戶用於通過MRA服務請求終端調配。
2. 導航到CUCM admin > User Management > User Settings > UC Service，然後建立指向CUCM的IP的CTI UC服務（即MRA_UC服務）。
3. 導航到CUCM admin > User Management > User Settings > Service Profile，然後建立新的配置檔案（即MRA_ServiceProfile）。

4. 在新服務配置檔案中，滾動到底部，然後在「CTI配置檔案」部分，選擇您剛剛建立的新CTI統一通訊服務（即MRA_UC服務），然後按一下「儲存」。
5. 導航至CUCM admin > User Management > End User，然後查詢用於通過MRA服務請求終端調配的使用者帳戶。
6. 在該使用者的**服務設定**下，確保選中「主集群」並且「統一通訊服務配置檔案」反映您建立的新服務配置檔案（即MRA_ServiceProfile），然後按一下「儲存」。
7. 複製可能需要幾分鐘時間。嘗試禁用終端上的調配模式，並在幾分鐘後重新開啟，以檢視終端現在是否註冊。

相關資訊

- [移動和遠端訪問指南](#)
- [VCS證書建立指南](#)
- [EX90/EX60入門指南](#)
- [CUCM 9.1管理員指南](#)
- [技術支援與文件 - Cisco Systems](#)