

# Collaboration Edge TC-gebaseerde configuratievoorbeeld voor endpoints

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Stap 1. Maak een beveiligd telefoonprofiel op CUCM in FQD-indeling \(optioneel\).](#)

[Stap 2. Zorg ervoor dat de Cluster Security Mode is \(1\) - Gemengde \(optioneel\).](#)

[Stap 3. Maak een profiel in CUCM voor het op TC gebaseerde endpoint.](#)

[Stap 4. Voeg de Security Profile Name toe aan de SAN van het Expressway-C/VCS-C Certificate \(optioneel\).](#)

[Stap 5. Voeg het UC-domein toe aan het Expressway-E/VCS-E-certificaat.](#)

[Stap 6. Installeer het juiste Trusted CA-certificaat aan de hand van het TC-endpoint.](#)

[Stap 7. Stel een TC-gebaseerd endpoint in voor Edge-provisioning](#)

[Verifiëren](#)

[op TC-gebaseerde endpoint](#)

[CUCM](#)

[snelweg-C](#)

[Problemen oplossen](#)

[Tools](#)

[TC-endpoint](#)

[snelwegen](#)

[CUCM](#)

[Vraag 1: Het Collaboration-edge record is niet zichtbaar en/of Hostname is niet oplosbaar](#)

[TC-endpoints](#)

[verbetering](#)

[Onderdeel 2: CA is niet aanwezig in de Trusted CA-lijst op het TC-gebaseerde endpoint](#)

[TC-endpoints](#)

[verbetering](#)

[Vraag 3: Expressway-E heeft niet het UC-domein dat in de SAN is vermeld](#)

[TC-endpoints](#)

[Expressway-E SAN](#)

[verbetering](#)

[Vraag 4: Gebruikersnaam en/of wachtwoord die in het TC-provisioningprofiel zijn geleverd, is niet juist](#)

[TC-endpoints](#)

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

[verbetering](#)

[Vraag 5: Op TC gebaseerde endpointregistratie wordt afgekeurd](#)

[CUCM-sporen](#)

[TC-endpoint](#)

[Feitelijke snelweg-C/VCS-C](#)

[verbetering](#)

[Vraag 6: TC-gebaseerde Endpoint Provisioning faalt - geen UDS-server](#)

[Gerelateerde informatie](#)

## Inleiding

Het document beschrijft wat er vereist is om TelePresence-codec (TC) te configureren en problemen op te lossen door middel van de mobiele en afstandsbediening.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Mobiele en externe toegangsooplossing
- VCS-certificaten (Video Communication Server)
- snelweg X8.1.1 of hoger
- Cisco Unified Communications Manager (CUCM) release 9.1.2 of hoger
- Op TC gebaseerde endpoints
- CE8.x vereist dat de coderingsoptie wordt ingesteld om "Edge" als een provisioningoptie in te schakelen

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- VCS X8.1.1 of hoger
- CUCM release 9.1(2)SU1 of later en IM & Presence 9.1(1) of hoger
- TC 7.1 of hoger firmware (**TC7.2 aanbevolen**)
- Core en edge voor VCS Control en snelwegen/snelwegen
- CUCM
- TC-endpoint

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Configureren

Deze configuratiestappen zijn gebaseerd op het feit dat de beheerder het op TC gebaseerde eindpunt voor beveiligde apparaatregistratie zal configureren. Beveiligde registratie is **NIET** een vereiste, maar de algemene gids voor de oplossing voor mobiele en externe toegang wekt de indruk dat dit is omdat er screenshots zijn van de configuratie die beveiligde apparaatprofielen op CUCM weergeven.

## Stap 1. Maak een beveiligd telefoonprofiel op CUCM in FQD-indeling (optioneel).

1. Selecteer in CUCM **System > Security > Phone security profiel**.
2. Klik op **Nieuw toevoegen**.
3. Selecteer het op TC gebaseerde type eindpunt en stel deze parameters in:
4. Naam - **Secure-EX90.tbp.local** (FQD-formaat vereist)
5. Apparaatbeveiligingsmodus - **Versleuteld**
6. Type transport - **TLS**
7. SIP-telefoon - **5061**

### Phone Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

---

**Status**

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

## Stap 2. Zorg ervoor dat de Cluster Security Mode is (1) - Gemengde (optioneel).

1. Selecteer in CUCM **System > Enterprise parameters**.
2. Scrollt naar **security parameters > Cluster security modus > 1**.

### Security Parameters

<u>Cluster Security Mode</u> *	1
--------------------------------	---

Als de waarde niet 1 is, is de CUCM niet beveiligd. Als dit zich voordoet, moet de beheerder een van deze twee documenten bekijken om het CUCM te beveiligen.

[UCM 9.1\(2\) security gids](#)

[UCM M100 security handleiding](#)

### Stap 3. Maak een profiel in CUCM voor het op TC gebaseerde endpoint.

1. Selecteer in CUCM **Apparaat > Telefoon**.
2. Klik op **Nieuw toevoegen**.
3. Selecteer het op TC gebaseerde type eindpunt en stel deze parameters in: MAC-adres - MAC-adres van het op TC gebaseerde apparaat Vereiste starrelvelden (\*) Eigenaar - gebruiker Gebruikersnaam - Eigenaar bij apparaat Apparaatbeveiligingsprofiel - eerder ingesteld profiel (Secure-EX90.tbp.local) SIP-profiel - standaard SIP-profiel of een aangepast profiel dat eerder is gemaakt

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' section indicates 'Update successful'. The main configuration area is divided into several sections:

- Association Information:** Shows two lines. Line 1 is 'Line [1] - 9211 in Baseline\_TelePresence\_PT'. Line 2 is 'Line [2] - Add a new DN'. There is a 'Modify Button Items' button above the lines.
- 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:** Radio buttons for 'User' (selected) and 'Anonymous (Public/Shared Space)'. Owner User ID\*: pstojano. Phone Load Name: (empty field).

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 > ▼
<input type="checkbox"/> Media Termination Point Required	
<input type="checkbox"/> Unattended Port	
<input type="checkbox"/> Require DTMF Reception	

#### Stap 4. Voeg de Security Profile Name toe aan de SAN van het Expressway-C/VCS-C Certificate (optioneel).

1. Schuif in Express-C/VCS-C naar **Onderhoud > Security Certificaten > Server-certificaat**.
2. Klik op **Generate CSR**.
3. Vul de velden certificaataanvraag (CSR) in en zorg ervoor dat de **Unified CM**-naam van het **beveiligingsprofiel** van de telefoon het exacte telefoonbeveiligingsprofiel heeft dat in het FQDN-formaat (Full Qualified Domain Name) is opgenomen. Bijvoorbeeld, **Secure-EX90.tbtp.local**. Opmerking: De Unified CM telefoon security profielnamen zijn vermeld op de achterzijde van het veld Onderwerp Alternate Name (SAN).
4. Verzend de CSR naar een interne of derde partij certificaatinstantie (CA) die wordt ondertekend.
5. Selecteer **Onderhoud > Beveiligingscertificaten > servercertificaat** om het certificaat te uploaden naar de sneltoets-C/VCS-C.

## Generate CSR

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

<b>Common name</b>	
Common name	FGDN of Expressway <input type="button" value="i"/>
Common name as it will appear	RTP-TBTP-EXPRWY-C1.tbtp.local
<b>Alternative name</b>	
Subject alternative names	FGDN of Expressway cluster plus FGDNs of all peers in the cluster <input type="button" value="i"/>
Additional alternative names (comma separated)	<input type="text"/> <input type="button" value="i"/>
IM and Presence chat node aliases (federated group chat)	conference-2-StandAloneCluster5ad9a.tbtp.local <input type="button" value="i"/> Format <input type="text" value="XMPPAddress"/> <input type="button" value="i"/>
Unified CM phone security profile names	Secure-EX90.tbtp.local <input type="button" value="i"/>
Alternative name as it will appear	DNS:RTP-TBTP-EXPRWY-C.tbtp.local DNS:RTP-TBTP-EXPRWY-C1.tbtp.local DNS:RTP-TBTP-EXPRWY-C2.tbtp.local XMPP:conference-2-StandAloneCluster5ad9a.tbtp.local DNS:Secure-EX90.tbtp.local
<b>Additional information</b>	
Key length (in bits)	4096 <input type="button" value="i"/>
Country	* US <input type="button" value="i"/>
State or province	* NC <input type="button" value="i"/>
Locality (town name)	* RTP <input type="button" value="i"/>
Organization (company name)	* Cisco <input type="button" value="i"/>
Organizational unit	* TelePresence <input type="button" value="i"/>
<input type="button" value="Generate CSR"/>	

### Stap 5. Voeg het UC-domein toe aan het Expressway-E/VCS-E-certificaat.

1. Selecteer **Onderhoud > Security Certificaten > Server Certificate** in **Express-E/VCS-E**.
2. Klik op **Generate CSR**.
3. Vul de CSR-velden in en zorg ervoor dat "Unified CM registrations domeinen" het domein bevatten dat het op TC gebaseerde eindpunt aan de Collaboration Edge (Collab-edge) verzoeken zal doen, in ofwel de Domain Name Server (DNS) of de Service Name (SRV)-formaten.
4. Verzend de CSR naar een interne of derde partij CA om te worden ondertekend.
5. Selecteer **Onderhoud > Security Certificaten > Server Certificate** om het certificaat te uploaden naar de 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 ⓘ

## Stap 6. Installeer het juiste Trusted CA-certificaat aan de hand van het TC-endpoint.

1. Selecteer in het op TC gebaseerde eindpunt de optie **Configuration > Security**.
2. Selecteer het tabblad **CA** en blader voor het CA-certificaat dat uw sneltoets-E/VCS-E-certificaat heeft ondertekend.
3. Klik op **Certificaat toevoegen**. Opmerking: Zodra het certificaat is toegevoegd, ziet u het in de certificaatlijst staan.

### Security

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

Certificates **CA's** Preinstalled CA's Strong Security Mode Non-persistent Mode CUCM

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

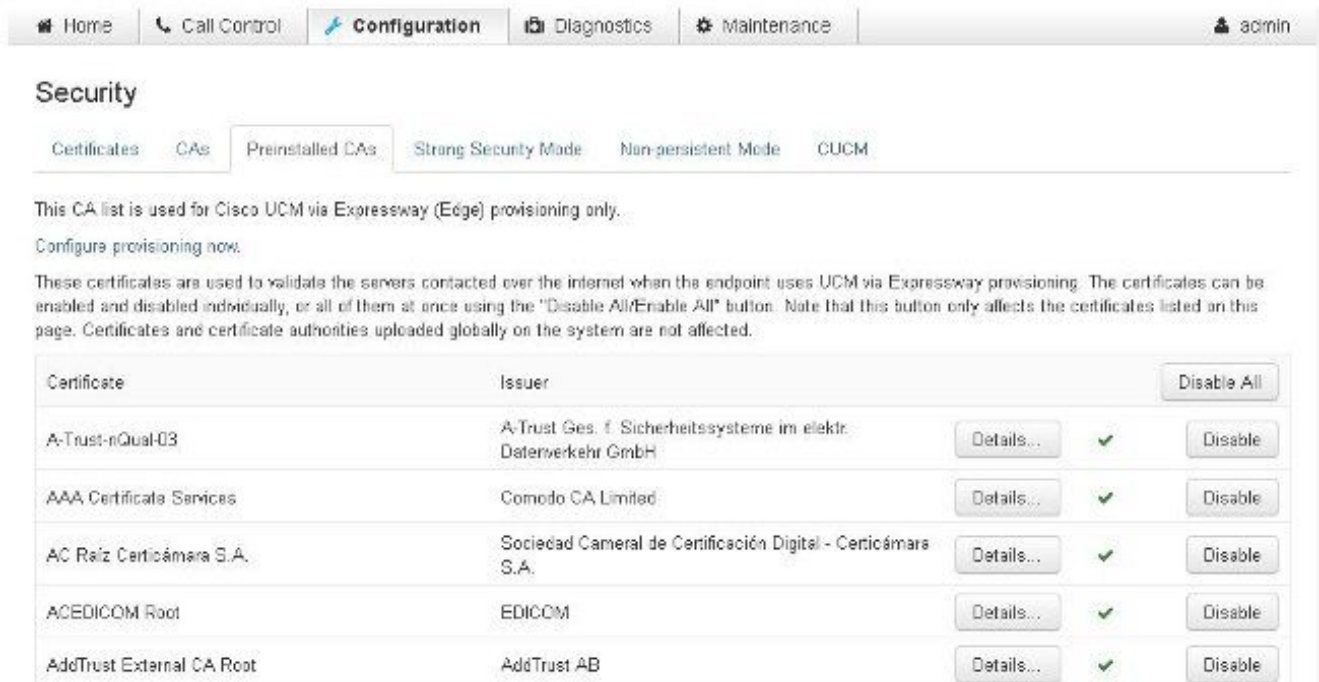
Add Certificate Authority

CA file:

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

Opmerking: TC 7.2 bevat een vooraf geïnstalleerde CA's lijst. Als de CA die het certificaat

expressway-E heeft ondertekend in deze lijst staat, zijn de in deze sectie vermelde stappen niet vereist.



The screenshot shows the Cisco UCM configuration interface. The top navigation bar includes Home, Call Control, Configuration (selected), Diagnostics, and Maintenance. The user is logged in as 'admin'. The main section is titled 'Security' and has tabs for Certificates, CAs, Preinstalled CAs (selected), Strong Security Mode, Non-persistent Mode, and CUCM. Below the tabs, there is a note: 'This CA list is used for Cisco UCM via Expressway (Edge) provisioning only. Configure provisioning now.' A paragraph explains that these certificates are used to validate servers contacted over the internet and can be enabled or disabled individually or all at once. Below this is a table of pre-installed certificates.

Certificate	Issuer	Details...	Status	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

Opmerking: De voorgeïnstalleerde CA's pagina bevat een handige "Voorstelling nu configureren" knop die u rechtstreeks naar de gewenste configuratie voert zoals aangegeven in stap 2 in de volgende sectie.

## Stap 7. Stel een TC-gebaseerd endpoint in voor Edge-provisioning

- Selecteer in het TC-gebaseerde eindpunt **Configuration > Network** en zorg ervoor dat deze velden correct ingevuld zijn onder de DNS-sectie:  
Domain Name  
Serveradres
- Selecteer in het op TC gebaseerde eindpunt de optie **Configuration > Provisioning** en zorg ervoor dat deze velden correct ingevuld zijn:  
LoginName - zoals gedefinieerd in CUCM  
Modus - **Rand**  
Wachtwoord - zoals gedefinieerd in CUCM  
Externe Manager  
Adres - achternaam van uw snelweg-E/VCS-E  
Domain - Domain waar uw collab-edge record aanwezig is



## 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

## Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

### op TC-gebaseerde endpoint

1. In de web GUI, navigeer naar "Begin". Bekijk het gedeelte 'SIP proxy 1' voor een "Geregistreerde" status. Het proxy-adres is uw Expressway-E/VCS-E.

### SIP Proxy 1

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

2. Voer vanuit de CLI `xstatus //prov in`. Als u geregistreerd bent, ziet u een provisioningstatus van "Provisioning".

```
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: "pstojsano"
*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

Selecteer in CUCM **Apparaat > Telefoon**. ofwel door de lijst te bladeren of door de lijst te filteren op basis van uw eindpunt. U dient een bericht "Geregistreerd met %CUCM\_IP%" te zien. Het IP-adres rechts van dit adres moet uw Expressway-C/VCS-C zijn, die de registratie aanvult.



## snelweg-C

- Selecteer in snelweg-C/VCS-C de optie **Status > Unified Communications > Provisioning-sessies**.
- Filter door het IP adres van uw op TC gebaseerd eindpunt. Een voorbeeld van een geplande sessie wordt in de afbeelding weergegeven:

Records: 2 Page 1 of 1

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

## Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Vraagstukken op het gebied van registratie kunnen worden veroorzaakt door talrijke factoren zoals DNS, certificaatproblemen, configuratie en dergelijke. Deze sectie omvat een uitgebreide lijst van wat u typisch zou zien als u een bepaald probleem zou ontmoeten en hoe het te verhelpen. Als je problemen tegenkomt buiten wat al is gedocumenteerd, kun je het gratis toevoegen.

## Tools

Om te beginnen, let op de gereedschappen die je tot je beschikking hebt.

### TC-endpoint

#### Web GUI

- all.log
- Uitgebreide loggen starten (inclusief een volledige pakketvastlegging)

#### CLI

Deze opdrachten zijn vooral geschikt voor probleemoplossing in real-time:

- HTTP-client debug 9
- log ctx PROV debug 9
- loguitvoer op ← Geeft loggen via console weer

Een effectieve manier om het probleem te herscheppen, is om de Provisioning Mode van "Edge" in te schakelen op "Off" en dan terug naar "Edge" in de web GUI. U kunt ook de **xConfiguration Provisioning Mode** invoeren: commando in de CLI.

#### snelwegen

- [Diagnostische logboek](#)
- CPDump

#### CUCM

- SDI/SDL-sporen

## Vraag 1: Het Collaboration-edge record is niet zichtbaar en/of Hostname is niet oplosbaar

Zoals u kunt zien, zal get\_edge\_fig mislukken door de naam resolutie te noemen.

### TC-endpoints

```
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/
```

#### verbetering

1. Controleer of het Collab-edge record aanwezig is en retourneert de juiste hostname.
2. Controleer of de DNS server-informatie die op de client is ingesteld, juist is.

## Onderdeel 2: CA is niet aanwezig in de Trusted CA-lijst op het TC-gebaseerde endpoint

### TC-endpoints

```
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
```

### verbetering

1. Controleer of een CA van de derde partij in de lijst staat onder het tabblad **Security > CA's** op het eindpunt.
2. Als de CA is vermeld, controleer dan of zij juist is.

## Vraag 3: Expressway-E heeft niet het UC-domein dat in de SAN is vermeld

### TC-endpoints

```
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

### verbetering

1. Regeer Expressway-E CSR om het UC-domein(en) te omvatten.
2. Het is mogelijk dat op het TC-eindpunt de **ExternManager Domain** parameter niet is ingesteld op wat het UC-domein is. Als dit zich voordoet, moet u het evenaren.

## Vraag 4: Gebruikersnaam en/of wachtwoord die in het TC-provisioningprofiel zijn geleverd, is niet juist

### TC-endpoints

```
83716.67 HttpClient      Server auth using Basic with user 'pstojano'
83716.67 HttpClient GET /dGJ0cC5jb20/get_edge_config/ HTTP/1.1
Authorization: xxxxxx
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/
```

### Snelweg-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="pstojano"  
Server="('https', 'xx.xx.97.131', 8443)" Reason="<twisted.python.failure.Failure  
<type 'exceptions.Exception'>>" UTCTime="2014-09-25 17:46:20,92"
```

## verbetering


1. Controleer dat de gebruikersnaam/het wachtwoord dat onder de Provisioning-pagina op het TC-eindpunt is ingevoerd, geldig is.
2. Controleer geloofsbrieven aan de gegevensbank van CUCM.
3. Versie 10 - gebruik het selfservice portal
4. Versie 9 - gebruik de CM-gebruikersopties

De URL voor beide poorten is hetzelfde: <https://%CUCM%/ucmuser/>

Indien ingediend met een ontoereikende rechtenfout, zorg er dan voor dat deze rollen zijn toegewezen aan de gebruiker:

- Standaard CTI-enabled
- Standaard CCM-eindgebruiker

## Vraag 5: Op TC gebaseerde endpointregistratie wordt afgekeurd

	<a href="#">SEP00506006EAFE</a>	Stoj EX90	<a href="#">Baseline TelePresence-DP</a>	SIP	Rejected	<a href="#">97.108</a>
---	---------------------------------	-----------	--	-----	----------	------------------------

## CUCM-sporen

```
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-endpoint

Status:

Failed: 403 Forbidden

## Feitelijke snelweg-C/VCS-C

X509v3 Subject Alternative Name:

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

In dit specifieke logvoorbeeld is duidelijk dat de Expressway-C/VCS-C niet de FQDN-beveiligingsprofiel van de telefoon bevat in de SAN. (Secure-EX90.tbtp.local). In de TLS-handdruk (Transport Layer Security) inspecteert het CUCM het servercertificaat van de expressway-C/VCS-C. Aangezien dit niet in SAN is gevonden, werpt het de bolde fout en meldt het dat het het profiel van de Veiligheid van de telefoon in FQDN-formaat verwachtte.

## verbetering

1. Controleer dat Expressway-C/VCS-C het telefoonbeveiligingsprofiel in FQDN-indeling bevat binnen de SAN van het servercertificaat.
2. Controleer dat het apparaat het juiste veiligheidsprofiel in CUCM gebruikt als u een veilig profiel in FQDN-formaat gebruikt.
3. Dit kan ook veroorzaakt zijn door Cisco bug-ID [CSCuq86376](#). Als dit probleem zich voordoet, controleert u de grootte van de snelweg-C/VCS-C SAN en de positie van het telefoonbeveiligingsprofiel in de SAN.

## Vraag 6: TC-gebaseerde Endpoint Provisioning faalt - geen UDS-server

Deze fout moet aanwezig zijn onder **Diagnostiek > Problemen oplossen** :

Error: Provisioning Status

Provisioning failed: XML didnt contain UDS server adres

## TC-endpoints

Scrollt naar rechts om de fouten in vet te zien

```
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/ZXUuY2hlZ2cuY29t/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!
```

## verbetering

1. Zorg ervoor dat er een serviceprofiel en CTRI UC-service is gekoppeld aan de eindgebruikersaccount die wordt gebruikt om via MRA-services een voorziening voor endpoints aan te vragen.
2. Navigeer naar **CUCM admin >User Management>User Settings > UC Service** en maak een **CTI UC-service** die op de IP van CUCM wijst (d.w.z. MRA\_UC-Service).
3. Navigeer naar **CUCM-beheerder>Gebruikersbeheer >gebruikersinstellingen > Serviceprofiel** en om een nieuw profiel te maken (bv. MRA\_ServiceProfile).
4. In het nieuwe serviceprofiel klikt u onder in het vak CTI Profile en vervolgens selecteert u de nieuwe CTI UC Service die u zojuist hebt gemaakt (bv. MRA\_UC-Service) en vervolgens klikt u op Save.
5. Navigeer naar **CUCM-beheerder >Gebruikersbeheer >Eindgebruiker** en vind de gebruikersaccount die wordt gebruikt om via MRA-services een voorziening voor endpoints aan te vragen.
6. Controleer onder **Service-instellingen** van die gebruiker of de Home Cluster wordt gecontroleerd en of het UC-serviceprofiel het nieuwe serviceprofiel weergeeft dat u hebt gemaakt (bv. MRA\_ServiceProfile), en klik vervolgens op Opslaan.
7. Het kan een paar minuten duren om dit na te bootsen. Probeer de provisioningmodus op het eindpunt uit te schakelen en draai deze een paar minuten later terug om te zien of het eindpunt nu registreert.

## Gerelateerde informatie

- [Mobiele en externe toegangsgids](#)
- [Creatie van VCS-certificaten](#)
- [EX90/EX60 Introductiegids](#)
- [CUCM 9.1 Administrator-gids](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)