

# Exemplo de Configuração de Endpoints Baseados em TC do Collaboration Edge

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Etapa 1. Crie um perfil de telefone seguro no CUCM no formato FQDN \(opcional\).](#)

[Etapa 2. Verifique se o modo de segurança de cluster está \(1\) - Misto \(opcional\).](#)

[Etapa 3. Crie um perfil no CUCM para o endpoint baseado em TC.](#)

[Etapa 4. Adicione o nome do perfil de segurança à SAN do certificado Expressway-C/VCS-C \(opcional\).](#)

[Etapa 5. Adicione o domínio UC ao certificado Expressway-E/VCS-E.](#)

[Etapa 6. Instale o Certificado CA Confiável Adequado ao Ponto Final baseado em TC.](#)

[Passo 7. Configurar um endpoint baseado em TC para provisionamento de borda](#)

[Verificar](#)

[Ponto de extremidade baseado em TC](#)

[CUCM](#)

[Expressway-C](#)

[Troubleshoot](#)

[Ferramentas](#)

[Ponto de Extremidade TC](#)

[Expressways](#)

[CUCM](#)

[Problema 1: O registro de colab-edge não está visível e/ou o nome do host não pode ser resolvido](#)

[Logs de endpoint TC](#)

[Correção](#)

[Problema 2: CA não está presente na lista de CAs confiáveis no endpoint baseado em TC](#)

[Logs de endpoint TC](#)

[Correção](#)

[Problema 3: O Expressway-E não tem o domínio UC listado na SAN](#)

[Logs de endpoint TC](#)

[SAN Expressway-E](#)

[Correção](#)

[Problema 4: O nome de usuário e/ou a senha fornecidos no perfil de provisionamento do TC estão incorretos](#)

[Logs de endpoint TC](#)

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

[Correção](#)

[Problema 5: O registro de endpoint baseado em TC é rejeitado](#)

[Rastreamentos de CUCM](#)

[Ponto de Extremidade TC](#)

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

[Correção](#)

[Problema 6: Falha no provisionamento de endpoint baseado em TC - sem servidor UDS](#)

[Informações Relacionadas](#)

## Introduction

O documento descreve o que é necessário para configurar e solucionar problemas de registro de endpoint baseado no TelePresence Codec (TC) através da solução Mobile and Remote Access.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Solução de acesso remoto e móvel
- Certificados VCS (Video Communication Server, servidor de comunicação por vídeo)
- Expressway X8.1.1 ou posterior
- Cisco Unified Communication Manager (CUCM) versão 9.1.2 ou posterior
- endpoints com base em TC
- O CE8.x requer a chave de opção de criptografia para ativar a "borda" como uma opção de provisionamento

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- VCS X8.1.1 ou posterior
- CUCM versão 9.1(2)SU1 ou posterior e IM & Presence 9.1(1) ou posterior
- Firmware TC 7.1 ou posterior (**recomendado TC7.2**)
- Controle VCS e Expressway/Expressway Core e Edge
- CUCM
- Ponto de Extremidade TC

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Configurar

Essas etapas de configuração pressupõem que o administrador configurará o ponto de extremidade baseado em TC para o registro seguro de dispositivos. O registro seguro **NÃO** é um requisito, no entanto, o guia geral da solução Mobile and Remote Access dá a impressão de que é, pois há capturas de tela da configuração que mostram perfis de dispositivos seguros no CUCM.

## Etapa 1. Crie um perfil de telefone seguro no CUCM no formato FQDN (opcional).

1. No CUCM, selecione **System > Security > Phone Security Profile**.
2. Clique em **Adicionar novo**.
3. Selecione o tipo de endpoint baseado em TC e configure estes parâmetros:
4. Nome - **Secure-EX90.tbtp.local (Formato FQDN Obrigatório)**
5. Modo de segurança do dispositivo - **Criptografado**
6. Tipo de transporte - **TLS**
7. Porta de telefone SIP - **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\*** Secure-EX90.tbtp.local  
**Description**  
**Nonce Validity Time\*** 600  
**Device Security Mode** Encrypted  
**Transport Type\*** TLS  
 Enable Digest Authentication  
 TFTP Encrypted Config  
 Exclude Digest Credentials in Configuration File

**Phone Security Profile CAPF Information**

**Authentication Mode\*** By Null String  
**Key Size (Bits)\*** 2048  
Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

**Parameters used in Phone**

SIP Phone Port\* 5061

Save Delete Copy Reset Apply Config Add New

## Etapa 2. Verifique se o modo de segurança de cluster está (1) - Misto (opcional).

1. No CUCM, selecione **System > Enterprise Parameters**.
2. Role para baixo até **Security Parameters > Cluster Security Mode > 1**.

### Security Parameters

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

Se o valor não for 1, o CUCM não foi protegido. Se for esse o caso, o administrador precisa revisar um desses dois documentos para proteger o CUCM.

[Guia de segurança do CUCM 9.1\(2\)](#)

[Guia de segurança do CUCM 10](#)

### Etapa 3. Crie um perfil no CUCM para o endpoint baseado em TC.

1. No CUCM, selecione **Dispositivo > Telefone**.
2. Clique em **Adicionar novo**.
3. Selecione o tipo de endpoint baseado em TC e configure estes parâmetros: Endereço MAC - Endereço MAC do dispositivo baseado em TCCampos iniciais obrigatórios (\*)Proprietário - UsuárioID de usuário proprietário - proprietário associado ao dispositivoPerfil de segurança do dispositivo - Perfil configurado anteriormente (Secure-EX90.tbtp.local)Perfil SIP - Perfil SIP padrão ou qualquer perfil personalizado criado anteriormente

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:** Owner User ID\*: pstojano, Phone Load Name: (empty field).
- Owner Type:** Radio buttons for 'User' (selected) and 'Anonymous (Public/Shared Space)'.

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	

#### Etapa 4. Adicione o nome do perfil de segurança à SAN do certificado Expressway-C/VCS-C (opcional).

1. No Expressway-C/VCS-C, navegue para **Manutenção > Certificados de segurança > Certificado do servidor**.
2. Clique em **Gerar CSR**.
3. Preencha os campos Certificate Signing Request (CSR) (Solicitação de Assinatura de Certificado) e verifique se o **nome do perfil de segurança do telefone do Unified CM** tem o perfil exato de segurança do telefone listado no formato Fully Qualified Domain Name (FQDN). Por exemplo, **Secure-EX90.tbtp.local**. **Note:** Os nomes dos perfis de segurança do telefone do Unified CM estão listados na parte traseira do campo Nome alternativo do assunto (SAN).
4. Envie o CSR para uma CA (Autoridade de Certificação) interna ou terceirizada para ser assinada.
5. Selecione **Manutenção > Certificados de Segurança > Certificado do Servidor** para carregar o certificado no Expressway-C/VCS-C.

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

**Common name**

Common name:  ⓘ

Common name as it will appear:

**Alternative name**

Subject alternative names:  ⓘ

Additional alternative names (comma separated):  ⓘ

IM and Presence chat node aliases (federated group chat):  Format:  ⓘ

Unified CM phone security profile names:  ⓘ

Alternative name as it will appear:

**Additional information**

Key length (in bits):  ⓘ

Country:  ⓘ

State or province:  ⓘ

Locality (town name):  ⓘ

Organization (company name):  ⓘ

Organizational unit:  ⓘ

## Etapa 5. Adicione o domínio UC ao certificado Expressway-E/VCS-E.

1. No Expressway-E/VCS-E, selecione **Manutenção > Certificados de Segurança > Certificado de Servidor**.
2. Clique em **Gerar CSR**.
3. Preencha os campos de CSR e certifique-se de que "domínios de registro do Unified CM" contenham o domínio em que o ponto de extremidade baseado em TC fará solicitações de Borda de Colaboração (borda de colab) para, nos formatos Servidor de Nome de Domínio (DNS) ou Nome de Serviço (SRV).
4. Envie o CSR para uma CA interna ou de terceiros para ser assinada.
5. Selecione **Manutenção > Certificados de Segurança > Certificado do Servidor** para carregar o certificado no Expressway-E/VCS-E.

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

**Common name**

Common name:  ⓘ

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

**Alternative name**

Subject alternative names:  ⓘ

Additional alternative names (comma separated):  ⓘ

Unified CM registrations domains:  Format:  ⓘ

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):  ⓘ

Country:  ⓘ

State or province:  ⓘ

Locality (town name):  ⓘ

Organization (company name):  ⓘ

Organizational unit:  ⓘ

## Etapa 6. Instale o Certificado CA Confiável Adequado ao Ponto Final baseado em TC.

1. No Endpoint baseado em TC, selecione **Configuration > Security**.
2. Selecione a guia **CA** e procure o certificado CA que assinou o certificado do Expressway-E/VCS-E.
3. Clique em **Adicionar autoridade de certificado**. **Note:** Quando o certificado for adicionado com êxito, você o verá listado na lista de certificados.

### 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.

**Note:** O TC 7.2 contém uma lista de CAs pré-instaladas. Se a CA que assinou o certificado Expressway-E estiver contida nesta lista, as etapas listadas nesta seção não serão necessárias.

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

**Note:** A página CAs pré-instaladas contém um conveniente botão "Configure o provisionamento agora" que o leva diretamente para a configuração necessária anotada na etapa 2 da próxima seção.

## Passo 7. Configurar um endpoint baseado em TC para provisionamento de borda

- No endpoint baseado em TC, selecione **Configuration > Network** e verifique se esses campos estão preenchidos corretamente na seção DNS:  
Nome de domínio  
Endereço do servidor
- No endpoint baseado em TC, selecione **Configuration > Provisioning (Configuração > Provisionamento)** e verifique se esses campos estão preenchidos corretamente:  
LoginName - conforme definido no CUCM  
Modo- **Borda**  
Senha - conforme definido no CUCM  
Gerenciador externo  
Endereço - Nome de host do seu Expressway-E/VCS-E  
Domínio - Domínio em que seu registro de collab-edge está presente



## 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

## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

### Ponto de extremidade baseado em TC

1. Na GUI da Web, navegue até "Início". Procure a seção 'Proxy SIP 1' para obter um Status "Registrado". O endereço do proxy é seu Expressway-E/VCS-E.

### SIP Proxy 1

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

2. Na CLI, insira `xstatus //prov`. Se estiver registrado, você verá um Status de provisionamento de "Provisionado".

```
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: "pstojano"
*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

No CUCM, selecione **Dispositivo > Telefone**. Role pela lista ou filtre a lista com base no endpoint. Você deve ver uma mensagem "Registrado com %CUCM\_IP%". O endereço IP à direita deve ser o Expressway-C/VCS-C, que faz o proxy do registro.



## Expressway-C

- No Expressway-C/VCS-C, selecione **Status > Unified Communications > Exibir sessões de provisionamento**.
- Filtre pelo endereço IP do endpoint baseado em TC. Um exemplo de uma sessão provisionada é mostrado na imagem:

Records: 2 Page 1 of 1

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

## Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Os problemas de registro podem ser causados por vários fatores, como DNS, problemas de certificado, configuração e assim por diante. Esta seção inclui uma lista abrangente do que você normalmente veria se encontrasse um determinado problema e como corrigi-lo. Se você

encontrar problemas fora do que já foi documentado, sinta-se à vontade para incluí-los.

## Ferramentas

Para começar, conheça as ferramentas à sua disposição.

### Ponto de Extremidade TC

#### GUI da Web

- all.log
- Iniciar registro estendido (incluir uma captura de pacote completa)

#### CLI

Esses comandos são mais benéficos para solucionar problemas em tempo real:

- log ctx HttpClient debug 9
- log ctx PROV debug 9
- log output on <— Mostra o log via console

Uma maneira eficaz de recriar o problema é alternar o modo de provisionamento de "Edge" para "Off" e, em seguida, de volta para "Edge" na GUI da Web. Você também pode entrar no **modo de provisionamento do xConfiguration**: na CLI.

#### Expressways

- [Nos registros de diagnóstico](#)
- TCPCDump

#### CUCM

- Rastreamentos SDI/SDL

## Problema 1: O registro de colab-edge não está visível e/ou o nome do host não pode ser resolvido

Como você pode ver, get\_edge\_config falha devido à resolução de nome.

#### Logs de endpoint TC

```
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/
```

#### Correção

1. Verifique se o registro collab-edge está presente e retorna o nome de host correto.
2. Verifique se as informações do servidor DNS configuradas no cliente estão corretas.

## Problema 2: CA não está presente na lista de CAs confiáveis no endpoint baseado em TC

### Logs de endpoint TC

```
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: rcv: 0
15975.86 HttpClient      Curl_addHandleToPipeline: length: 1
15975.86 HttpClient      - Conn 64 (0x48396560) send_pipe: 0, rcv_pipe: 0
15975.87 HttpClient      - Conn 65 (0x4835a948) send_pipe: 0, rcv_pipe: 0
15975.87 HttpClient      - Conn 67 (0x48390808) send_pipe: 1, rcv_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
```

### Correção

1. Verifique se uma CA de terceiros está listada na guia **Security > CAs** no endpoint.
2. Se a CA estiver listada, verifique se está correta.

## Problema 3: O Expressway-E não tem o domínio UC listado na SAN

### Logs de endpoint TC

```
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'
```

## SAN Expressway-E

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

## Correção

1. Recrie o Expressway-E CSR para incluir os domínios UC.
2. É possível que no endpoint TC o parâmetro **ExternalManager Domain** não esteja definido para o que é o domínio UC. Se esse for o caso, você deve combiná-lo.

## Problema 4: O nome de usuário e/ou a senha fornecidos no perfil de provisionamento do TC estão incorretos

### Logs de endpoint TC

```
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="pstoiano" 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"
```

### Correção


1. Verifique se o nome de usuário/senha inseridos na página Provisionamento no ponto de extremidade TC é válido.
2. Verifique as credenciais no banco de dados do CUCM.
3. Versão 10 - usar o Portal de Cuidados Pessoais
4. Versão 9 - utilizar as Opções do usuário CM

O URL para ambos os portais é o mesmo: <https://%CUCM%/ucmuser/>

Se for apresentado um erro de direitos insuficiente, certifique-se de que estas funções estão atribuídas ao usuário:

- CTI padrão habilitada
- Usuário final CCM padrão

### Problema 5: O registro de endpoint baseado em TC é rejeitado

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

### Rastreamentos de CUCM

```
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,
```

### Ponto de Extremidade TC

Status:

Failed: 403 Forbidden

## Expressway-C/VCS-C real

X509v3 Subject Alternative Name:

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

Neste exemplo de registro específico, está claro que o Expressway-C/VCS-C não contém o FQDN do perfil de segurança do telefone na SAN. (Secure-EX90.tbtp.local). No handshake TLS (Transport Layer Security), o CUCM inspeciona o certificado de servidor do Expressway-C/VCS-C. Como ele não o encontra na SAN, ele descarta o erro em negrito e informa que esperava o perfil de segurança do telefone no formato FQDN.

## Correção

1. Verifique se o Expressway-C/VCS-C contém o perfil de segurança do telefone no formato FQDN na SAN do certificado do servidor.
2. Verifique se o dispositivo usa o perfil de segurança correto no CUCM se você usa um perfil seguro no formato FQDN.
3. Isso também pode ser causado pelo bug da Cisco ID [CSCuq86376](#). Se for esse o caso, verifique o tamanho da SAN Expressway-C/VCS-C e a posição do perfil de segurança do telefone na SAN.

## Problema 6: Falha no provisionamento de endpoint baseado em TC - sem servidor UDS

Este erro deve estar presente em **Diagnostics > Troubleshooting** :

Error: Provisioning Status

Provisioning failed: XML didnt contain UDS server adres

## Logs de endpoint TC

Role para a direita para ver os erros em negrito

```
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</adre
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!
```

## Correção

1. Verifique se há um perfil de serviço e um serviço CTI UC associado à conta do usuário final usado para solicitar o provisionamento de endpoint via serviços MRA.
2. Navegue até **CUCM admin > User Management > User Settings > UC Service** e crie um CTI UC Service que aponte para o IP do CUCM (ou seja, MRA\_UC-Service).
3. Navegue até **CUCM admin > User Management > User Settings > Service Profile** e crie um novo perfil (por exemplo, MRA\_ServiceProfile).
4. No novo Perfil de serviço, role até a parte inferior e, na seção CTI Profile, selecione o novo CTI UC Service que acabou de criar (ou seja, MRA\_UC-Service) e clique em Salvar.
5. Navegue até **CUCM admin > User Management > End User** e localize a conta de usuário usada para solicitar o provisionamento de ponto de extremidade via serviços MRA.
6. Em **Service Settings** desse usuário, verifique se Home Cluster está marcado e se o UC Service Profile reflete o novo Service Profile que você criou (por exemplo, MRA\_ServiceProfile) e clique em Save.
7. Pode levar alguns minutos para replicar. Tente desabilitar o modo de provisionamento no endpoint e ligue-o novamente alguns minutos depois para ver se o endpoint agora se registra.

## Informações Relacionadas

- [Guia de acesso remoto e móvel](#)
- [Guia de criação de certificado VCS](#)
- [Guia de introdução ao EX90/EX60](#)
- [Guia do administrador do CUCM 9.1](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)