

Collaboration Edge の TC ベース エンドポイントの設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ステップ 1 : CUCM で FQDN 形式による安全な電話プロファイルを作成します \(オプション \) 。](#)

[ステップ 2 : クラスタセキュリティモードが \(1\) – 混合 \(オプション \) であることを確認します。](#)

[ステップ 3 : CUCM で TC ベースのエンドポイント用プロファイルを作成します。](#)

[ステップ 4 : Expressway-C/VCS-C 証明書の SAN にセキュリティプロファイル名を追加します \(オプション \) 。](#)

[ステップ 5 : Expressway-E/VCS-E 証明書に UC ドメインを追加します。](#)

[ステップ 6 : TC ベースのエンドポイントに、適切な信頼された CA 証明書をインストールします。](#)

[ステップ 7 : エッジプロビジョニング用に TC ベースのエンドポイントをセットアップします](#)

[確認](#)

[TC ベースのエンドポイント](#)

[CUCM](#)

[Expressway-C](#)

[トラブルシューティング](#)

[ツール](#)

[TC エンドポイント](#)

[Expressway](#)

[CUCM](#)

[問題 1 : collab-edge レコードが表示されない/ホスト名を解決できない](#)

[TC エンドポイントのログ](#)

[修復](#)

[問題 2 : TC ベースのエンドポイント上の信頼された CA リストに CA が含まれていない](#)

[TC エンドポイントのログ](#)

[修復](#)

[問題 3 : Expressway-E の UC ドメインが SAN にリストされていない](#)

[TC エンドポイントのログ](#)

[Expressway-E SAN](#)

[修復](#)

[問題 4 : TC プロビジョニングプロファイルで指定されているユーザ名またはパスワード、あるいはその両方が誤っている](#)

[TC エンドポイントのログ](#)

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

[修復](#)

[問題 5 : TC ベースのエンドポイントの登録が拒否される](#)

[CUCM トレース](#)

[TC エンドポイント](#)

[実際の Expressway-C/VCS-C](#)

[修復](#)

[問題 6 : TC ベースのエンドポイント プロビジョニングが失敗する - UDS サーバがない](#)

[関連情報](#)

概要

このドキュメントでは、モバイルおよびリモート アクセス ソリューションを介して TelePresence Codec (TC) ベースのエンドポイントの登録を設定またはトラブルシューティングするのに必要な手順を説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- モバイルおよびリモート アクセス ソリューション
- Video Communication Server (VCS) 証明書
- Expressway X8.1.1 以降
- Cisco Unified Communications Manager (CUCM) リリース 9.1.2 以降
- TC ベースのエンドポイント
- CE8.x では、暗号化オプション キーを使用して、プロビジョニング オプションとして [Edge] を有効にする必要があります

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- VCS X8.1.1 以降
- CUCM リリース 9.1(2)SU1 以降および IM & Presence 9.1(1) 以降
- TC 7.1 以降のファームウェア (TC 7.2 を推奨)
- VCS Control と VCS Expressway/Expressway Core と Expressway Edge
- CUCM
- TC エンドポイント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

この設定手順では、安全なデバイス登録用に管理者が TC ベースのエンドポイントを設定することを前提とします。モバイルおよびリモート アクセス ソリューション ガイドに掲載されている設定のスクリーンショットは CUCM 上のセキュア デバイス プロファイルを示しているため、安

全な登録が必須であるような印象を与えますが、安全な登録は必須ではありません。

ステップ 1 : CUCM で FQDN 形式による安全な電話プロファイルを作成します (オプション) 。

1. CUCM で、[System] > [Security] > [Phone Security Profile] を選択します。
2. [Add New] をクリックします。
3. TC ベースのエンドポイントのタイプを選択して、次のパラメータを設定します。
4. [Name] : **Secure-EX90.tbtp.local** (FQDN 形式であることが必須です)
5. [Device Security Mode] : [Encrypted]
6. [Transport Type] : [TLS]
7. [SIP Phone Port] : [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* 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

ステップ2 : クラスタセキュリティモードが(1) – 混合 (オプション) であることを確認します。

1. CUCM で、[System] > [Enterprise Parameters] を選択します。

2. [Security Parameters] > [Cluster Security Mode] > [1] までスクロール ダウンします。



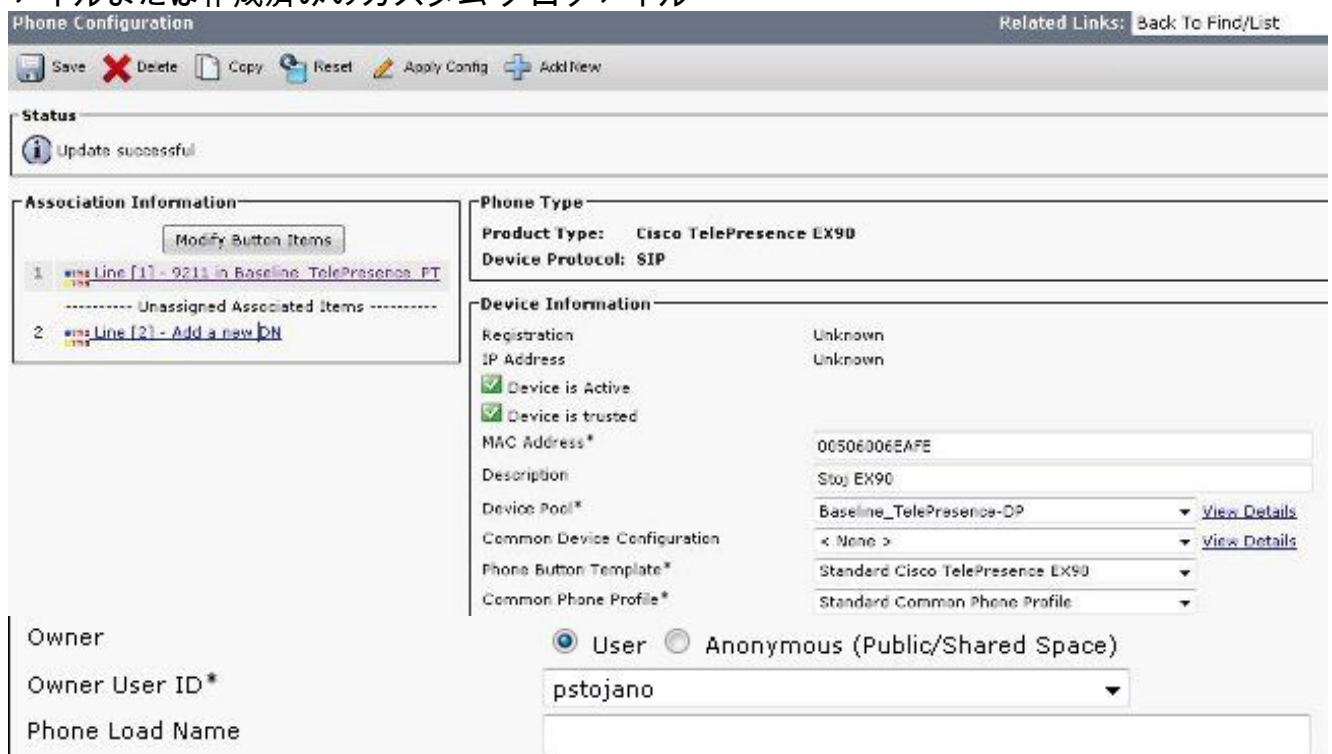
値が 1 でない場合、CUCM はセキュリティで保護されていません。その場合、管理者は次の 2 つのドキュメントのいずれかを確認して CUCM をセキュリティで保護する必要があります。

[CUCM 9.1\(2\) セキュリティ ガイド](#)

[CUCM 10 セキュリティ ガイド](#)

ステップ 3 : CUCM で TC ベースのエンドポイント用プロファイルを作成します。

1. CUCM で、[Device] > [Phone] を選択します。
2. [Add New] をクリックします。
3. TC ベースのエンドポイントのタイプを選択して、次のパラメータを設定します。 [MAC Address] : TC ベースのデバイスの MAC アドレスアスタリスク (*) が付いた必須フィールド [Owner] : [User][Owner User ID] : デバイスに関連付けられている所有者 [Device Security Profile] : 設定済みのプロファイル (Secure-EX90.tbtp.local) [SIP Profile] : 標準 SIP プロファイルまたは作成済みのカスタム プロファイル

A screenshot of the 'Phone Configuration' page in a web interface. The page title is 'Phone Configuration' and there is a 'Related Links: Back To Find/List' link. Below the title is a toolbar with icons for Save, Delete, Copy, Reset, Apply Config, and Add New. A status message says 'Update successful'. The main content is divided into several sections: 'Association Information' with a table of lines, 'Phone Type' with 'Product Type: Cisco TelePresence EX90' and 'Device Protocol: SIP', 'Device Information' with fields for Registration, IP Address, Device is Active, Device is trusted, MAC Address*, Description, Device Pool*, Common Device Configuration, Phone Button Template*, and Common Phone Profile*. At the bottom, there are radio buttons for 'User' (selected) and 'Anonymous (Public/Shared Space)', and a dropdown menu for 'Owner User ID*' with the value 'pstoiano'.

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	

ステップ 4 : Expressway-C/VCS-C 証明書の SAN にセキュリティ プロファイル名を追加します (オプション) 。

1. Expressway-C/VCS-C で、[Maintenance] > [Security Certificates] > [Server Certificate] に移動します。
2. [Generate CSR] をクリックします。
3. 証明書署名要求 (CSR) 関連のフィールドに入力し、[Unified CM phone security profile names] に、完全修飾ドメイン名 (FQDN) 形式の正確な電話セキュリティ プロファイルがリストされていることを確認します。たとえば、Secure-EX90.tbtp.local です。注 : Unified CM 電話セキュリティ プロファイル名が、[Subject alternate name] (SAN) フィールドの下方にリストされます。
4. CSR を内部認証局 (CA) またはサードパーティ CA に送信して署名を受けます。
5. 証明書を Expressway-C/VCS-C にアップロードするために、[Maintenance] > [Security Certificates] > [Server Certificate] を選択します。

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

Common name

Common name: ⓘ

Common name as it will appear: RTP-TBTP-EXPRWY-C1.tftp.local

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: DNS:RTP-TBTP-EXPRWY-C.tftp.local
DNS:RTP-TBTP-EXPRWY-C1.tftp.local
DNS:RTP-TBTP-EXPRWY-C2.tftp.local
XMPP:conference-2-StandAloneCluster5ad9a.tftp.local
DNS:Secure-EX90.tftp.local

Additional information

Key length (in bits): ⓘ

Country: ⓘ

State or province: ⓘ

Locality (town name): ⓘ

Organization (company name): ⓘ

Organizational unit: ⓘ

ステップ 5 : Expressway-E/VCS-E 証明書に UC ドメインを追加します。

- Expressway-E/VCS-E で、[Maintenance] > [Security Certificates] > [Server Certificate] を選択します。
- [Generate CSR] をクリックします。
- CSR 関連のフィールドに入力します。[Unified CM registrations domains] では、TC ベースのエンドポイントからのコラボレーション エッジ (collab-edge) 要求の送信先であるドメインが、ドメイン ネーム サーバ (DNS) 形式またはサービス名 (SRV) 形式のいずれかで指定されていることを確認します。
- CSR を内部 CA またはサードパーティ CA に送信して署名を受けます。
- 証明書を Expressway-E/VCS-E にアップロードするために、[Maintenance] > [Security Certificates] > [Server Certificate] を選択します。

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.tbtcp.local
DNS:RTP-TBTP-EXPRWY-E1.tbtcp.local
DNS:tbtcp.local
SRV:_collab-edge._tls.tbtcp.local
```

Additional information

Key length (in bits): ⓘ

Country: ⓘ

State or province: ⓘ

Locality (town name): ⓘ

Organization (company name): ⓘ

Organizational unit: ⓘ

ステップ 6 : TC ベースのエンドポイントに、適切な信頼された CA 証明書をインストールします。

1. TC ベースのエンドポイントで、[Configuration] > [Security] を選択します。
2. [CA] タブを選択し、Expressway-E/VCS-E 証明書に署名した CA の CA 証明書を参照します。
3. [Add certificate authority] をクリックします。注：証明書が正常に追加されると、[Certificate] リストにその証明書が表示されます。

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.

注：TC 7.2 には、事前インストール済み CA のリストが含まれています。Expressway-E 証

明書に署名した CA がこのリストに含まれている場合は、このセクションに記載する手順を実行する必要はありません。

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

注：[Preinstalled CAs] ページには使いやすい [Configure provisioning now] ボタンがあり、それをクリックすると、次のセクションのステップ 2 で説明する必須の設定に直接移動できます。

ステップ 7：エッジプロビジョニング用に TC ベースのエンドポイントをセットアップします

- TC ベースのエンドポイントで、[Configuration] > [Network] を選択し、[DNS] セクションの次のフィールドに適切な値が入力されていることを確認します。
ドメイン名
Server address
- TC ベースのエンドポイントで、[Configuration] > [Provisioning] を選択し、次のフィールドに適切な値が入力されていることを確認します。
[LoginName]：CUCM で定義されているログイン名
Mode- エッジ
[Password]：CUCM で定義されているパスワード
External Manager
[Address]：Expressway-E/VCS-E のホスト名
[Domain]：collab-edge レコードが存在するドメイン

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

確認

ここでは、設定が正常に機能しているかどうかを確認します。

TC ベースのエンドポイント

1. Web GUI で、[Home] に移動します。[SIP Proxy 1] セクションを調べて、ステータスが [Registered] になっていることを確認します。プロキシ アドレスが Expressway-E/VCS-E に設定されていることを確認します。

SIP Proxy 1

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

2. CLI から、「`xstatus //prov`」と入力します。登録されている場合は、[Provisioning Status] に [Provisioned] と表示されます。

```
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
```

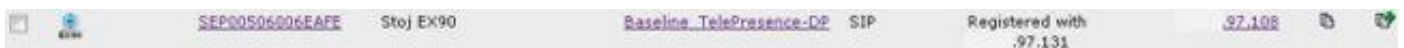
```

*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

CUCM で、[Device] > [Phone] を選択します。リスト全体をスクロールするか、エンドポイントに基づいてリストをフィルタリングして、「Registered with %CUCM_IP%」というメッセージを見つけます。その右側に表示されている IP アドレスが、登録をプロキシする Expressway-C/VCS-C です。



Expressway-C

- Expressway-C/VCS-C で、[Status] > [Unified Communications] > [View Provisioning sessions] を選択します。
- TC ベースのエンドポイントの IP アドレスでフィルタリングします。プロビジョニングされたセッションの例を下の図に示します。

Records: 2 Page 1 of 1

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

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

DNS、証明書の問題、設定などのさまざまな要因によって、登録の問題が発生する可能性があります。このセクションでは、特定の問題が発生した場合によく表示される情報を包括的にリスト

し、その問題を修復する方法を説明します。まだ文書化されていない問題が発生した場合は、その問題をリストに自由に追加してください。

ツール

まずは、使用できるツールを確認してください。

TC エンドポイント

Web GUI

- all.log
- 拡張ロギングの開始 (完全なパケット キャプチャを含む)

CLI

リアルタイムでトラブルシューティングを行うには、次のコマンドが特に役立ちます。

- log ctx HttpClient debug 9
- log ctx PROV debug 9
- log output on <- コンソール経由のロギングを表示

問題を再現するのに効果的な方法は、Web GUI でプロビジョニング モードを [Edge] から [Off] に切り替えた後、[Edge] に戻すことです。また、CLI で `xConfiguration Provisioning Mode:コマンド` を入力することもできます。

Expressway

- [診断ログ](#)
- TCPDump

CUCM

- SDI/SDL トレース

問題 1 : collab-edge レコードが表示されない/ホスト名を解決できない

ログを見るとわかるように、名前解決が原因で `get_edge_config` が失敗しています。

TC エンドポイントのログ

```
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/
```

修復

1. collab-edge レコードが存在すること、正しいホスト名を返すことを確認します。
2. クライアント上に設定されている DNS サーバ情報が正しいことを確認します。

問題 2 : TC ベースのエンドポイント上の信頼された CA リストに CA が含まれていない

TC エンドポイントのログ

```
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
```

修復

1. エンドポイントで [Security] > [CAs] タブに移動し、サードパーティ CA がリストされているかどうかを確認します。
2. CA がリストされている場合は、正しい CA であることを確認します。

問題 3 : Expressway-E の UC ドメインが SAN にリストされていない

TC エンドポイントのログ

```
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
```

修復

1. UC ドメインを含めるために、Expressway-E CSR を再生成します。
2. TC エンドポイントで、[ExternalManager Domain] パラメータが、該当する UC ドメインに設定されていない可能性があります。その場合は、パラメータを該当する UC ドメインと一致させる必要があります。

問題 4 : TC プロビジョニング プロファイルで指定されているユーザ名またはパスワード、あるいはその両方が誤っている

TC エンドポイントのログ

```
83716.67 HttpClient      Server auth using Basic with user 'pstoiano'
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="pstojano"
Server="('https', 'xx.xx.97.131', 8443)" Reason="<twisted.python.failure.Failure
<type 'exceptions.Exception'>>" UTCTime="2014-09-25 17:46:20,92"
```

修復


1. TC エンドポイント上の [Provisioning] ページで入力されたユーザ名/パスワードが有効であることを確認します。
2. クレデンシャルを CUCM データベースと照合します。
3. バージョン 10 : セルフケアポータルを使用
4. バージョン 9 : CM ユーザオプションを使用

ポータルの URL は両方とも同じで、次のとおりです。 <https://%CUCM%/ucmuser/>

十分な権限がないというエラーが表示されたら、次の役割がユーザに割り当てられるようにします。

- Standard CTI Enabled
- Standard CCM End User

問題 5 : TC ベースのエンドポイントの登録が拒否される

	SEP00506006EAFE	Stoj EX90	Baseline TelePresence-DP	SIP	Rejected	97.108
---	-----------------	-----------	--------------------------	-----	----------	--------

CUCM トレース

```
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 エンドポイント

SIP Proxy 1

Status:

Failed: 403 Forbidden

実際の Expressway-C/VCS-C

X509v3 Subject Alternative Name:

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

この特定のログ例では、Expressway-C/VCS-CにSAN内の電話セキュリティプロファイル FQDN(Secure-EX90.tbtp.local)が含まれていないことが明らかです。Transport Layer Security (TLS) ハンドシェイクで、CUCM は Expressway-C/VCS-C のサーバ証明書を検査します。このサーバ証明書が SAN 内に見つからないため、CUCM は上記の太字で示されたエラーをスローし、FQDN 形式の電話セキュリティプロファイルが想定されていたことを報告します。

修復

1. Expressway-C/VCS-C のサーバ証明書の SAN に、FQDN 形式の電話セキュリティプロファイルが含まれていることを確認します。
2. FQDN 形式のセキュリティプロファイルを使用している場合は、デバイスが CUCM で正しいセキュリティプロファイルを使用していることを確認します。
3. これは、Cisco Bug ID [CSCuq86376](#)が原因である可能性もあります。この場合は、Expressway-C/VCS-C SANのサイズと、SAN内の電話セキュリティプロファイルの位置を確認してください。

問題 6 : TC ベースのエンドポイント プロビジョニングが失敗する - UDS サーバがない

[Diagnostics] > [Troubleshooting] の下にこのエラーが表示されるはずです。

Error: Provisioning Status

Provisioning failed: XML didnt contain UDS server address

TC エンドポイントのログ

右にスクロールすると、太字のエラーが表示されます。

```
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!
```

修復

1. MRAサービス経由でエンドポイントプロビジョニングを要求するために使用されるエンドユーザアカウントに、サービスプロファイルとCTI UCサービスが関連付けられていることを確認します。
2. [CUCM admin] > [User Management] > [User Settings] > [UC Service]に移動し、CUCMのIP(MRA_UC-Service)をポイントするCTI UCサービスを作成します。
3. [CUCM admin] > [User Management] > [User Settings] > [Service Profile] に移動し、新しいプロファイル(MRA_ServiceProfile)を作成します。
4. 新しいサービスプロファイルで、下にスクロールし、[CTI Profile]セクションで、作成したばかりの新しいCTI UCサービス(MRA_UC-Service)を選択し、[Save]をクリックします。
5. [CUCM admin] > [User Management] > [End User]に移動し、MRAサービス経由でエンドポイントプロビジョニングを要求するために使用するユーザアカウントを見つけます。
6. そのユーザの[Service Settings] で、[Home Cluster]がオンになっており、作成した新しいサービスプロファイル(MRA_ServiceProfile)がUCサービスプロファイルに反映されていることを確認し、[Save]をクリックします。
7. 複製には数分かかることがあります。エンドポイント上でプロビジョニング モードを無効にして、数分後に元に戻し、エンドポイントが登録されたかどうかを確認します。

関連情報

- [モバイルおよびリモート アクセス ガイド](#)
- [VCS 証明書作成ガイド](#)
- [EX90/EX60 入門ガイド](#)
- [CUCM 9.1 管理者ガイド](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)