Collaboration Edge TC 기반 엔드포인트 컨피그레이션 예

목차

소개
사전 요구 사항
요구 사항
사용되는 구성 요소
구성
1단계. FQDN 형식으로 CUCM에 Secure Phone Profile(보안 전화기 프로파일)을 생성합니다(선택 사항).
2단계. 클러스터 보안 모드가 (1) - 혼합(선택 사항)인지 확인합니다.
3단계. TC 기반 엔드포인트의 CUCM에서 프로파일을 생성합니다.
4단계. Expressway-C/VCS-C 인증서의 SAN에 보안 프로파일 이름을 추가합니다(선택 사항).
5단계. Expressway-E/VCS-E 인증서에 UC 도메인을 추가합니다.
6단계. TC 기반 엔드포인트에 올바른 신뢰할 수 있는 CA 인증서를 설치합니다.
7단계. 에지 프로비저닝을 위한 TC 기반 엔드포인트 설정
다음을 확인합니다.
TC 기반 엔드포인트
CUCM
Expressway-C
문제 해결
툴
TC 엔드포인트
고속도로
CUCM
문제 1:Collab-edge 레코드가 보이지 않거나 호스트 이름을 확인할 수 없습니다.
TC 엔드포인트 로그
교정
문제 2:CA가 TC 기반 엔드포인트의 신뢰할 수 있는 CA 목록에 없음
TC 엔드포인트 로그
교정
문제 3:Expressway-E는 SAN 내에 UC 도메인이 나열되지 않음
TC 엔드포인트 로그
Expressway-E SAN
교정
문제 4:TC 프로비저닝 프로파일에 제공된 사용자 이름 및/또는 암호가 잘못되었습니다.
TC 엔드포인트 로그
Expressway-C/VCS-C
교정
문제 5:TC 기반 엔드포인트 등록이 거부됨
CUCM 추적
TC 엔드포인트

실제 Expressway-C/VCS-C
교정
문제 6:TC 기반 엔드포인트 프로비저닝 실패 - UDS 서버 없음
관련 정보

소개

이 문서에서는 모바일 및 원격 액세스 솔루션을 통해 TC(TelePresence Codec) 기반 엔드포인트 등록을 구성하고 문제를 해결하는 데 필요한 사항을 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 모바일 및 원격 액세스 솔루션
- VCS(Video Communication Server) 인증서
- Expressway X8.1.1 이상
- Cisco CUCM(Unified Communication Manager) 릴리스 9.1.2 이상
- TC 기반 엔드포인트
- CE8.x에는 프로비저닝 옵션으로 "Edge"를 활성화하려면 암호화 옵션 키가 필요합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- VCS X8.1.1 이상
- CUCM 릴리스 9.1(2)SU1 이상 및 IM & Presence 9.1(1) 이상
- TC 7.1 이상 펌웨어**(TC7.2 권장)**
- VCS 제어 및 Expressway/Expressway 코어 및 에지
- CUCM
- TC 엔드포인트

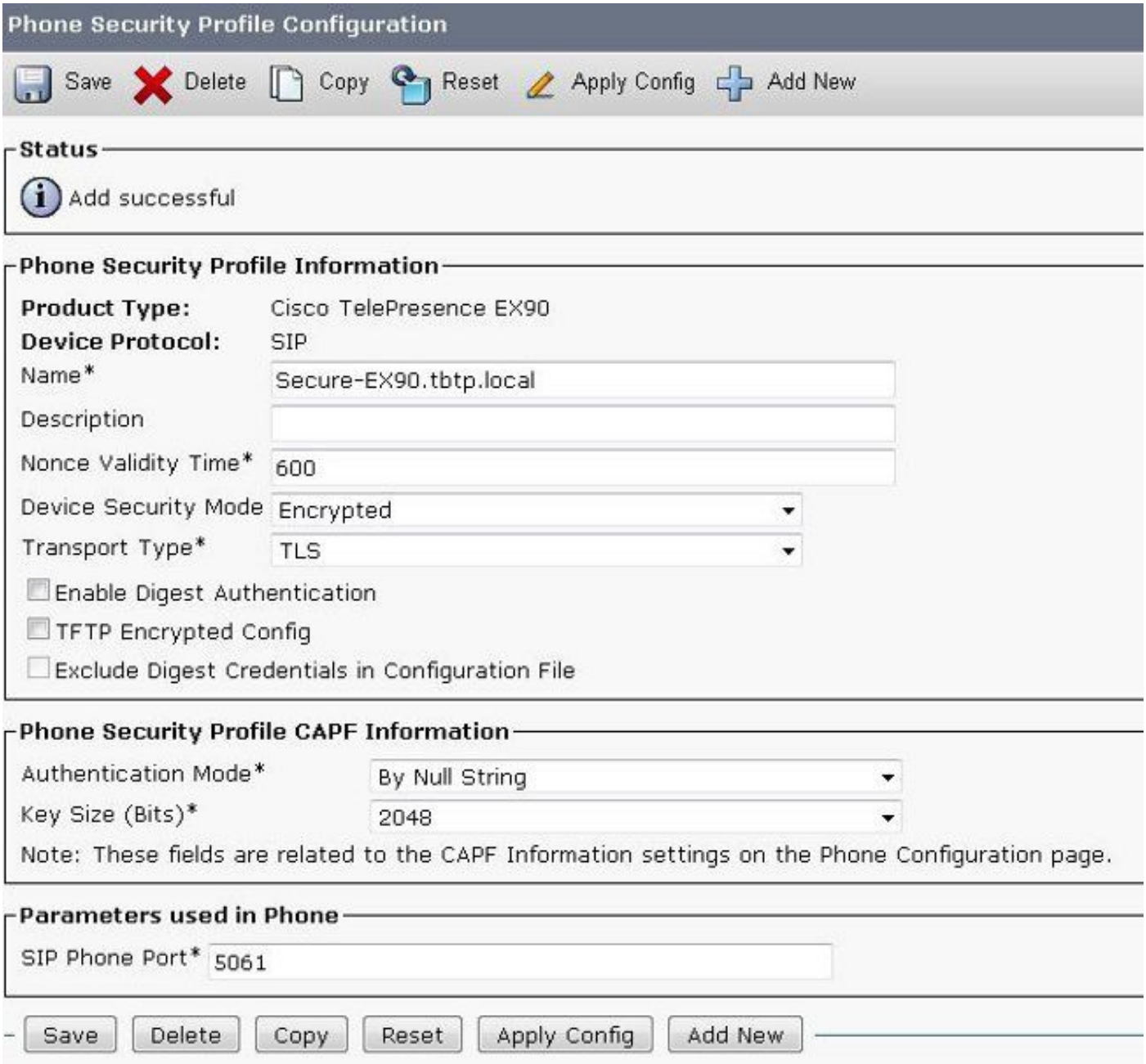
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

이러한 컨피그레이션 단계에서는 관리자가 보안 디바이스 등록을 위해 TC 기반 엔드포인트를 구성한다고 가정합니다.보안 등록은 **필요하지** 않지만, 전반적인 모바일 및 원격 액세스 솔루션 가이드는 CUCM의 보안 디바이스 프로파일을 보여주는 컨피그레이션의 스크린샷이 있기 때문에 보안 등록은 필요한 것으로 인식합니다.

1단계. FQDN 형식으로 CUCM에 Secure Phone Profile(보안 전화기 프로파일)을 생성합니다(선택 사항).

1. CUCM에서 **System > Security > Phone Security Profile을** 선택합니다.
2. Add **New를 클릭합니다**.
3. TC 기반 엔드포인트 유형을 선택하고 다음 매개변수를 구성합니다.
4. 이름 - **Secure-EX90.tbtp.local(FQDN 형식 필요)**
5. 디바이스 보안 모드 - **암호화됨**
6. 전송 유형 - **TLS**
7. SIP Phone Port - **5061**



2단계. 클러스터 보안 모드가 (1) - 혼합(선택 사항)인지 확인합니다.

1. CUCM에서 System **> Enterprise Parameters를** 선택합니다.
2. 아래로 스크롤하여 **Security Parameters(보안 매개변수) > Cluster Security Mode(클러스터 보안 모드) > 1로 이동합니다**.

값이 1이 아니면 CUCM이 보호되지 않은 것입니다.이 경우 관리자는 CUCM을 보호하기 위해 이 두

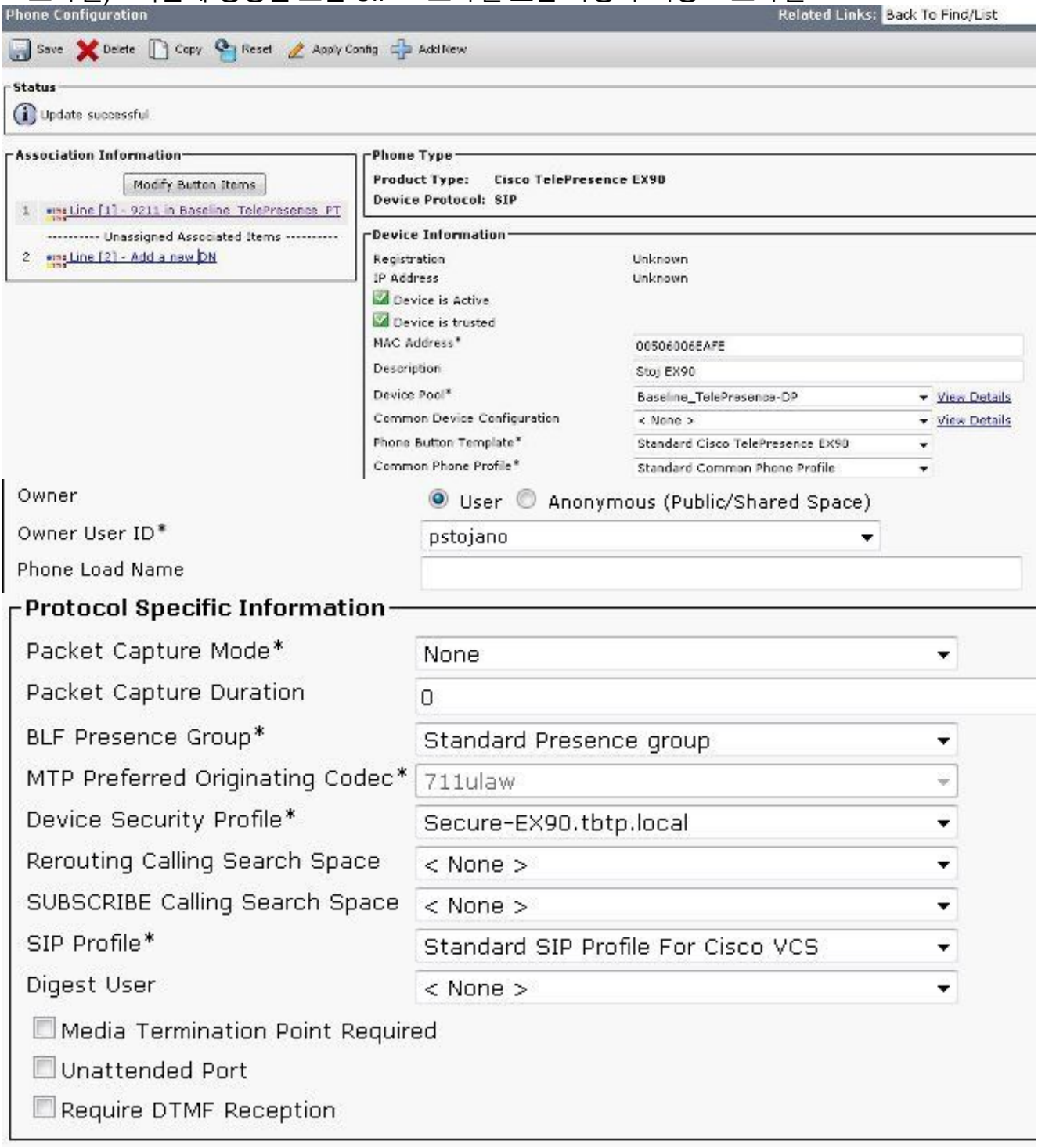
문서 중 하나를 검토해야 합니다.

CUCM 9.1(2) 보안 가이드

CUCM 10 보안 가이드

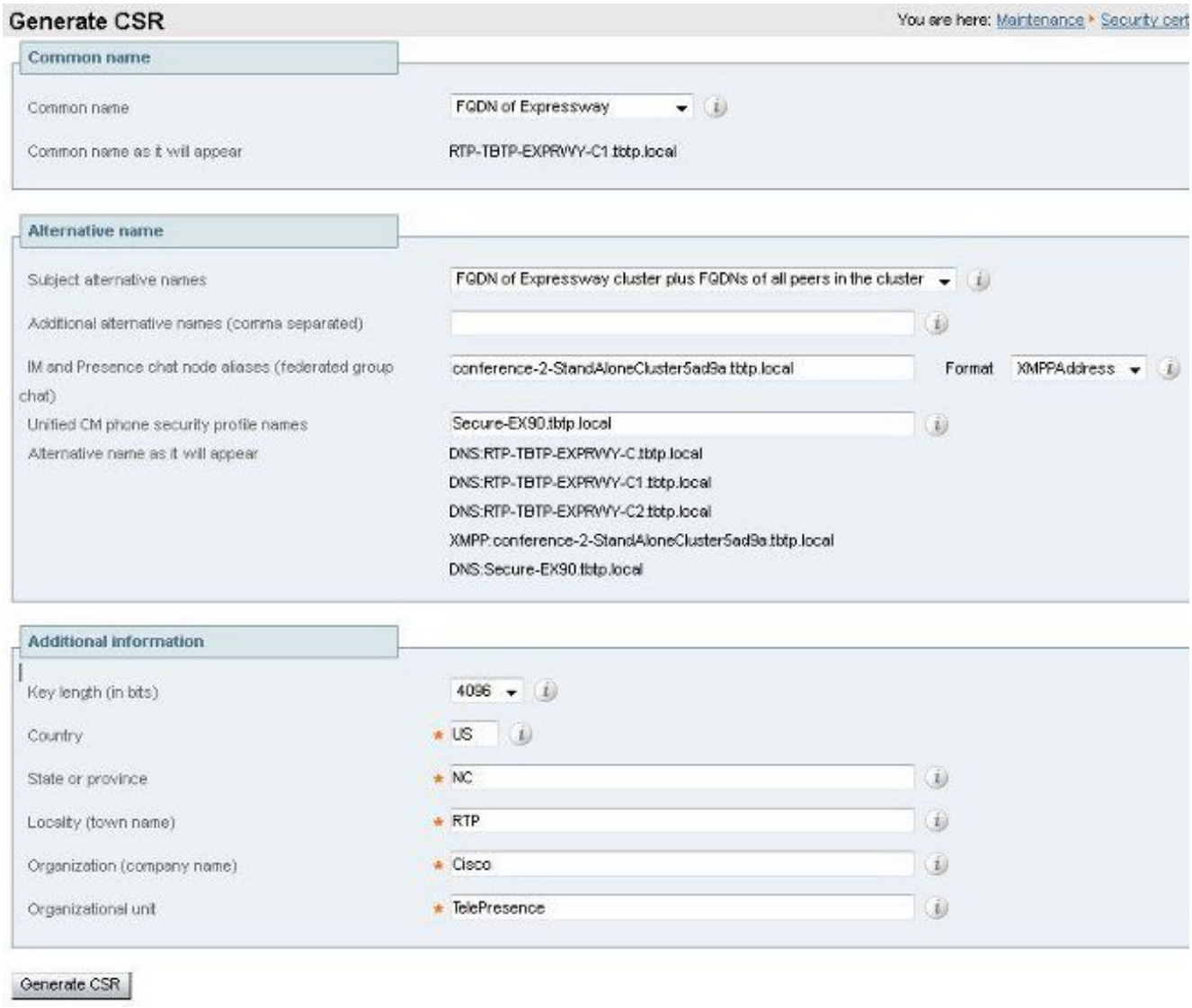
3단계. TC 기반 엔드포인트의 CUCM에서 프로파일을 생성합니다.

1. CUCM에서 Device **> Phone을** 선택합니다.
2. Add **New를 클릭합니다**.
3. TC 기반 엔드포인트 유형을 선택하고 다음 매개변수를 구성합니다. MAC 주소 - TC 기반 디바이스의 MAC 주소필수 주문자 필드(*)소유자 - 사용자소유자 사용자 ID - 장치와 연결된 소유자디바이스 보안 프로파일 - 이전에 구성된 프로파일(Secure-EX90.tbtp.local)SIP Profile(SIP 프로파일) - 이전에 생성된 표준 SIP 프로파일 또는 사용자 지정 프로파일



4단계. Expressway-C/VCS-C 인증서의 SAN에 보안 프로파일 이름을 추가합니다(선택 사항).

1. Expressway-C/VCS-C에서 **Maintenance > Security Certificates > Server Certificate로 이동합니다**.
2. Generate CSR(**CSR 생성)을 클릭합니다**.
3. CSR(Certificate Signing Request) 필드를 입력하고 **Unified CM 전화 보안 프로파일 이름**에 FQDN(Fully Qualified Domain Name) 형식으로 나열된 정확한 전화 보안 프로파일이 있는지 확인합니다.예: **Secure-EX90.tbtp.local**. **참고:**Unified CM 전화 보안 프로파일 이름은 SAN(Subject Alternate Name) 필드 뒷면에 나열됩니다.
4. 서명할 내부 또는 타사 CA(Certificate Authority)에 CSR을 보냅니다.
5. Expressway-C/VCS-C에 인증서를 업로드하려면 **Maintenance > Security Certificates > Server Certificate**를 선택합니다.

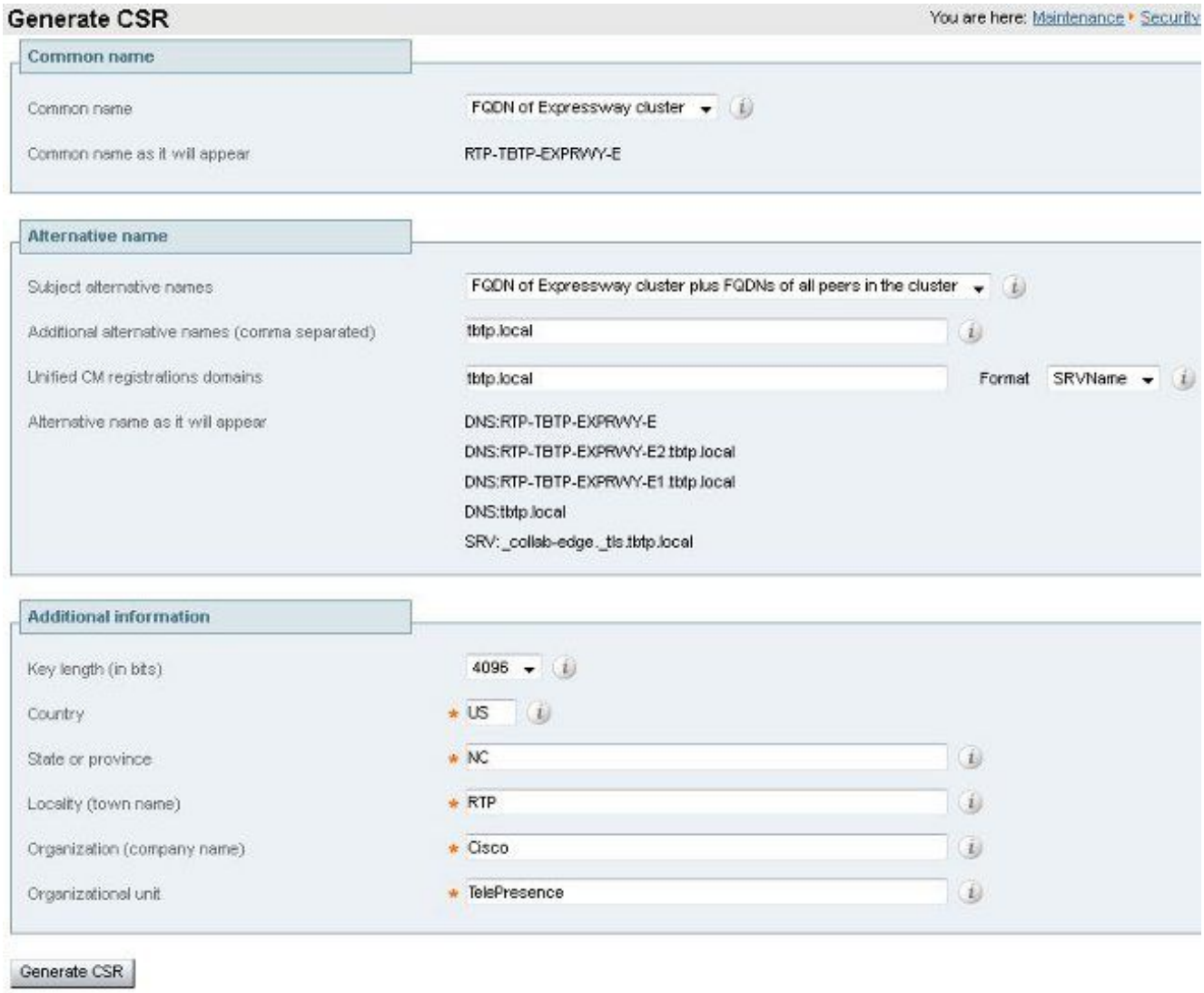


5단계. Expressway-E/VCS-E 인증서에 UC 도메인을 추가합니다.

1. Expressway-E/VCS-E에서 **Maintenance > Security Certificates > Server Certificate**를 선택합니다.
2. Generate CSR(**CSR 생성)을 클릭합니다**.
3. CSR 필드를 입력하고 "Unified CM 등록 도메인"에 TC 기반 엔드포인트가 DNS(Domain Name Server) 또는 SRV(Service Name) 형식으로 Collaboration Edge(collab-edge) 요청을 할

도메인이 포함되어 있는지 확인합니다.

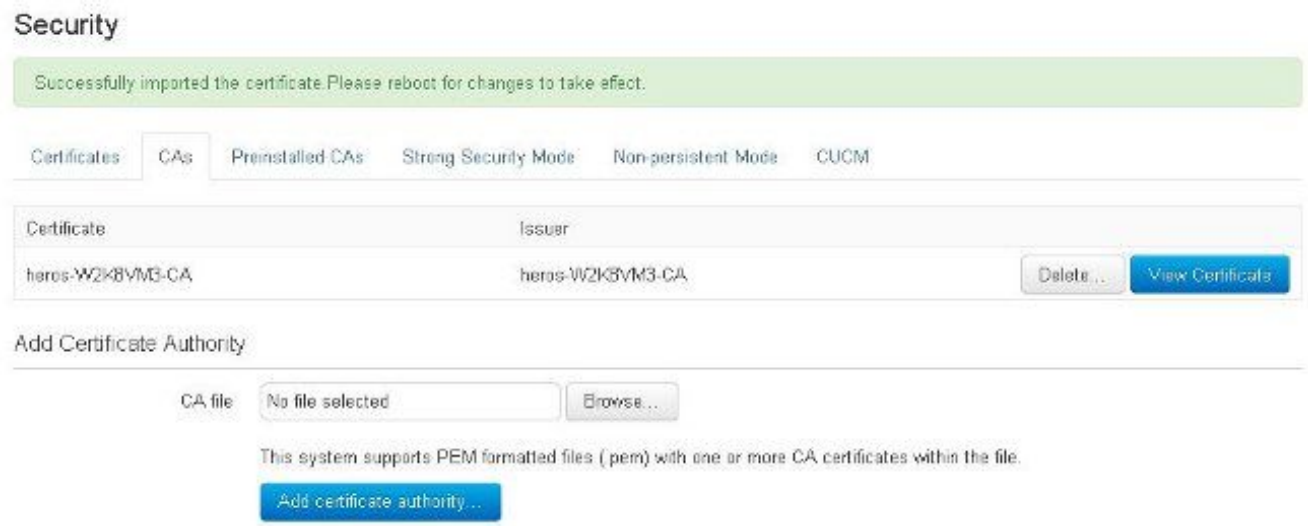
4. 서명할 내부 또는 서드파티 CA에 CSR을 보냅니다.
5. Expressway-E/VCS-E에 인증서를 업로드하려면 **Maintenance > Security Certificates > Server Certificate**를 선택합니다.



6단계. TC 기반 엔드포인트에 올바른 신뢰할 수 있는 CA 인증서를 설치합니다.

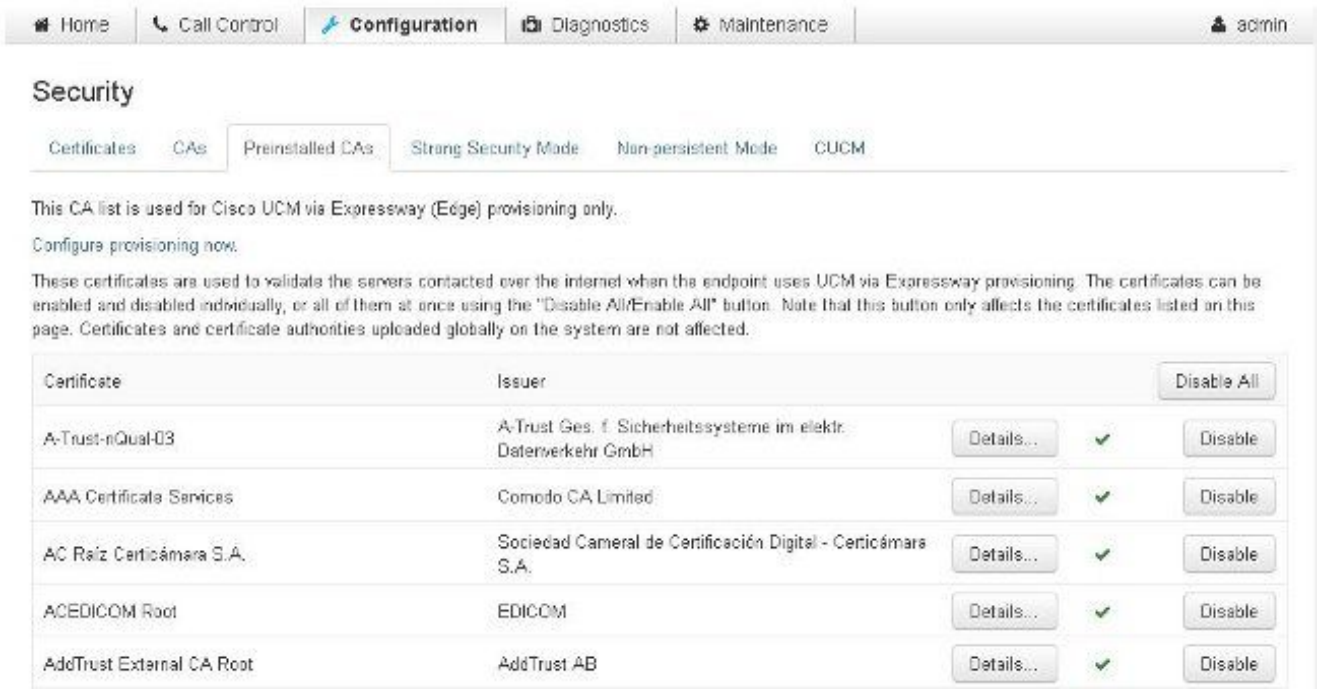
1. TC 기반 엔드포인트에서 Configuration(컨피그레이션) **> Security(보안)를** 선택합니다.
2. **CA** 탭을 선택하고 Expressway-E/VCS-E 인증서에 서명한 CA 인증서를 찾습니다.
3. Add **certificate authority를 클릭합니다**. **참고:**인증서가 성공적으로 추가되면 Certificate(인증서) 목록에 나열된 인증서가 표시됩니다

.



참고:TC 7.2에는 사전 설치된 CA 목록이 포함되어 있습니다.Expressway-E 인증서에 서명한 CA가 이 목록에 포함되어 있으면 이 섹션에 나열된 단계가 필요하지 않습니다

.



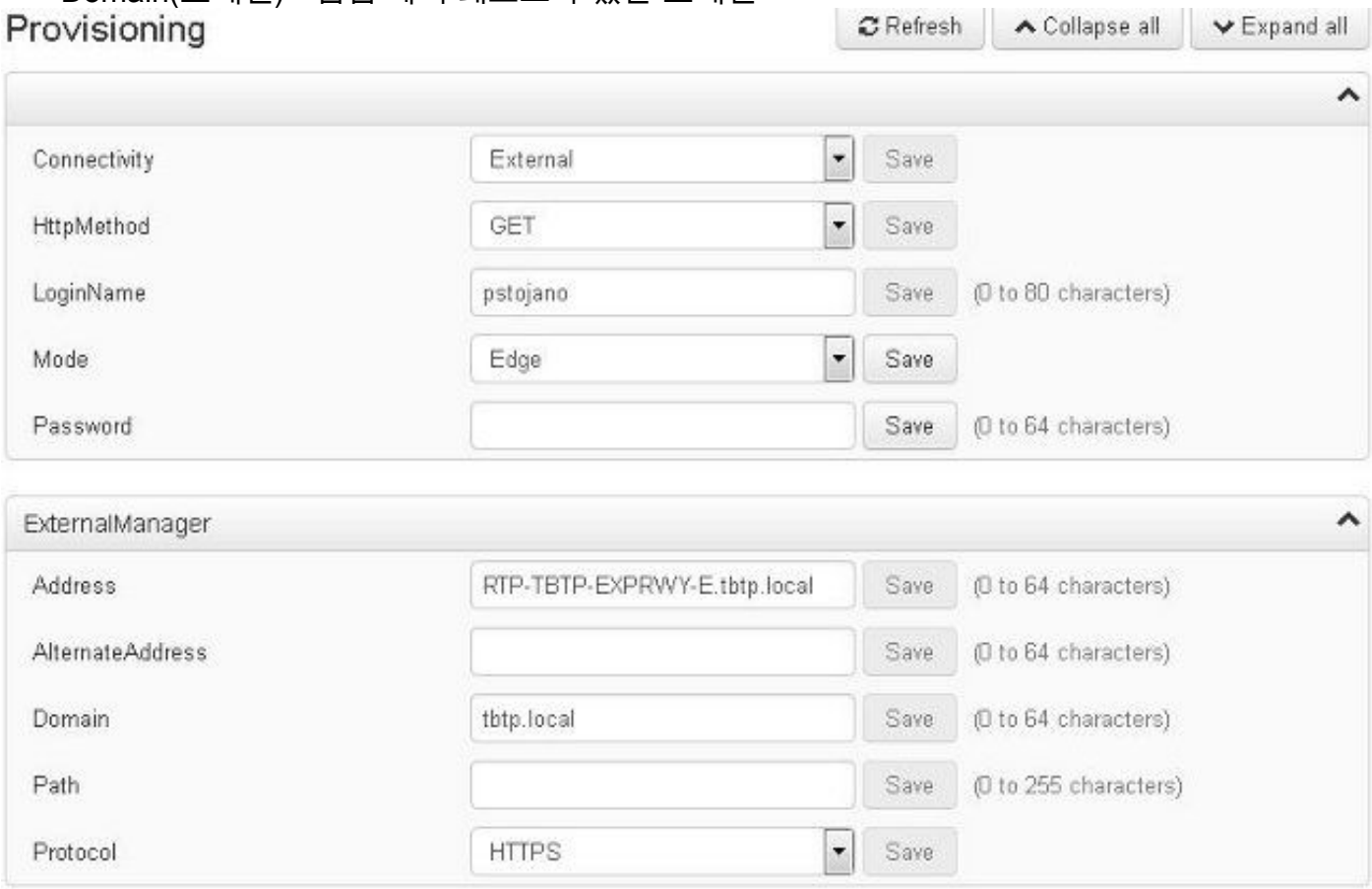
참고:사전 설치된 CAs 페이지에는 다음 섹션의 2단계에서 설명한 필수 컨피그레이션으로 바로 연결되는 편리한 "지금 프로비저닝 구성" 버튼이 있습니다.

7단계. 에지 프로비저닝을 위한 TC 기반 엔드포인트 설정

- TC 기반 엔드포인트에서 Configuration(컨피그레이션) > **Network(네트워크)**를 선택하고 DNS 섹션 아래에서 이 필드가 올바르게 채워졌는지 확인합니다.
  도메인 이름
  서버 주소

- TC 기반 엔드포인트에서 Configuration(컨피그레이션) > **Provisioning(프로비저닝)**을 선택하고 다음 필드가 올바르게 입력되었는지 확인합니다.
  LoginName - CUCM에 정의된 대로
  모드 - **에지**

비밀번호 - CUCM에 정의된 대로
외부 관리자
Address(주소) - Expressway-E/VCS-E의 호스트 이름
Domain(도메인) - 협업 에지 레코드가 있는 도메인

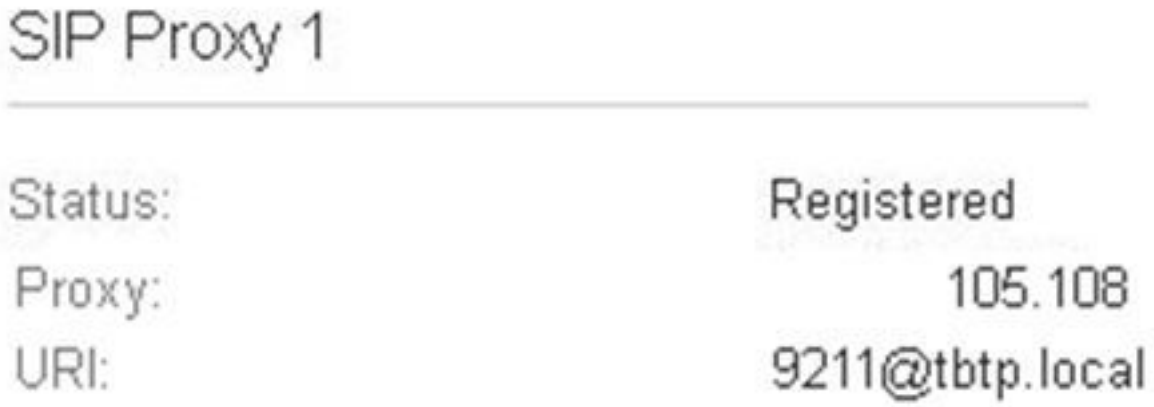


다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

TC 기반 엔드포인트

1. 웹 GUI에서 "Home(홈)"으로 이동합니다. 'SIP Proxy 1' 섹션에서 "Registered(등록됨)" 상태를 확인합니다.프록시 주소는 Expressway-E/VCS-E입니다.



2. CLI에서 xstatus **//prov를 입력합니다**.등록된 경우 프로비저닝 상태가 "Provisioned(프로비저닝됨)"로 표시됩니다.

```
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

CUCM에서 Device **> Phone을** 선택합니다.목록을 스크롤하거나 엔드포인트를 기준으로 목록을 필터링합니다."Registered with %CUCM_IP%" 메시지가 표시됩니다.이 오른쪽의 IP 주소는 등록을 프록시하는 Expressway-C/VCS-C여야 합니다.

Expressway-C

- Expressway-C/VCS-C에서 **Status > Unified Communications > View Provisioning sessions를** 선택합니다.
- TC 기반 엔드포인트의 IP 주소로 필터링합니다.프로비저닝된 세션의 예는 다음과 같습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

등록 문제는 DNS, 인증서 문제, 컨피그레이션 등을 포함한 여러 요인으로 인해 발생할 수 있습니다 .이 섹션에는 특정 문제가 발생할 경우 일반적으로 어떤 내용을 확인하고 이를 해결하는 방법에 대한 포괄적인 목록이 포함되어 있습니다.이미 문서화된 문제 이외의 문제가 발생할 경우 언제든지 포함하십시오.

툴

우선, 여러분이 활용할 수 있는 툴을 숙지하십시오.

TC 엔드포인트

웹 GUI

- all.log
- 확장 로깅 시작(전체 패킷 캡처 포함)

CLI

이러한 명령은 실시간 문제 해결을 위해 가장 유용합니다.

- 로그 ctx HttpClient 디버그 9
- 로그 ctx PROV 디버그 9
- log output on <— 콘솔을 통한 로깅을 표시합니다.

이 문제를 재생성하는 효과적인 방법은 프로비저닝 모드를 "Edge"에서 "Off"로 전환한 다음 웹 GUI에서 "Edge"로 전환하는 것입니다.xConfiguration Provisioning **Mode**를 입력할 수도 있습니다 .명령을 실행합니다.

고속도로

- 진단 로그
- TCPDump

CUCM

- SDI/SDL 추적

문제 1:Collab-edge 레코드가 보이지 않거나 호스트 이름을 확인할 수 없습니다.

보시다시피 이름 확인 때문에 get_edge_config가 실패합니다.

TC 엔드포인트 로그

```
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/
```

교정

1. collab-edge 레코드가 있는지 확인하고 올바른 호스트 이름을 반환합니다.
2. 클라이언트에 구성된 DNS 서버 정보가 올바른지 확인합니다.

문제 2:CA가 TC 기반 엔드포인트의 신뢰할 수 있는 CA 목록에 없음

TC 엔드포인트 로그

```
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
```

교정

1. 엔드포인트의 Security(**보안**) > CAs(**CA**) 탭 아래에 타사 CA가 나열되는지 확인합니다.
2. CA가 나열되면 CA가 올바른지 확인합니다.

문제 3:Expressway-E는 SAN 내에 UC 도메인이 나열되지 않음

TC 엔드포인트 로그

```
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.tbtppppp.local**

교정

1. UC 도메인을 포함하도록 Expressway-E CSR을 재생성합니다.
2. TC 엔드포인트에서 ExternalManager **Domain** 매개 변수가 UC 도메인과 다르게 설정될 수 있습니다.이 경우 반드시 일치해야 합니다.

문제 4:TC 프로비저닝 프로파일에 제공된 사용자 이름 및/또는 암호가 잘못되었습니다.

TC 엔드포인트 로그

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/

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"
```

교정

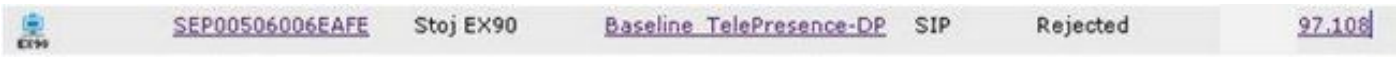
1. TC 엔드포인트의 Provisioning(프로비저닝) 페이지에 입력한 Username/Password(사용자 이름/비밀번호)가 유효한지 확인합니다.
2. CUCM 데이터베이스에 대한 자격 증명을 확인합니다.
3. 버전 10 - 셀프 케어 포털 사용
4. 버전 9 - CM 사용자 옵션 사용

두 포털의 URL이 동일합니다.**https://%CUCM%/ucmuser/**

권한 부족 오류가 표시된 경우 다음 역할이 사용자에게 할당되었는지 확인합니다.

- 표준 CTI 사용
- 표준 CCM 최종 사용자

문제 5:TC 기반 엔드포인트 등록이 거부됨



CUCM 추적

```
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 엔드포인트

실제 Expressway-C/VCS-C

```
X509v3 Subject Alternative Name:
DNS:RTP-TBTP-EXPRWY-C.tbtp.local, XMPP:conference-2-StandAloneCluster5ad9a.tbtp.local
```

이 특정 로그 예에서는 Expressway-C/VCS-C가 SAN에 Phone Security Profile FQDN을 포함하지 않습니다(Secure-EX90.tbtp.local). TLS(Transport Layer Security) 핸드셰이크에서 CUCM은 Expressway-C/VCS-C의 서버 인증서를 검사합니다.SAN에서 찾을 수 없으므로 굵은 오류를 던지고 FQDN 형식으로 전화기 보안 프로파일을 예상했음을 보고합니다.

교정

1. Expressway-C/VCS-C에 해당 서버 인증서의 SAN 내의 FQDN 형식의 전화 보안 프로파일이 포함되어 있는지 확인합니다.
2. FQDN 형식으로 보안 프로필을 사용하는 경우 디바이스에서 CUCM에서 올바른 보안 프로필을 사용하는지 확인합니다.
3. 이는 Cisco 버그 ID CSCuq86376 때문일 수도 있습니다. 이 경우 Expressway-C/VCS-C SAN 크기와 SAN 내에서 전화기 보안 프로필의 위치를 확인하십시오.

문제 6:TC 기반 엔드포인트 프로비저닝 실패 - UDS 서버 없음

이 오류는 Diagnostics(진단) > **Troubleshooting(문제 해결)** 아래에 있어야 합니다.

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

TC 엔드포인트 로그

오른쪽으로 스크롤하여 오류를 굵게 표시

```
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!
```

교정

1. MRA 서비스를 통해 엔드포인트 프로비저닝을 요청하는 데 사용되는 최종 사용자 계정과 연결된 서비스 프로필 및 CTI UC 서비스가 있는지 확인합니다.

2. CUCM **admin(CUCM 관리)> User Management(**사용자 관리)**>** User Settings(**사용자 설정) > UC Service(UC 서비스)로 이동하고 CUCM의 IP(예: MRA_UC-Service)를 가리키는 CTI UC 서비스를 생성합니다.**

3. CUCM **admin(CUCM 관리)> User Management(사용자 관리)>** User Settings(**사용자 설정) > Service Profile(서비스 프로파일)으로 이동하여 새 프로파일(예: MRA_ServiceProfile)을 생성합니다.**

4. 새 서비스 프로필의 맨 아래로 스크롤하여 CTI 프로필 섹션에서 방금 생성한 새 CTI UC 서비스(예: MRA_UC-Service)를 선택한 다음 저장을 클릭합니다.

5. CUCM **admin(CUCM 관리)>** User Management(**사용자 관리) >**End User(최종 사용자)로 이동하여 MRA 서비스를 통해 엔드포인트 프로비저닝을 요청하는 데 사용되는 사용자 계정을 찾습니다.

6. 해당 사용자의 **서비스 설정** 아래에서 홈 클러스터가 확인되고 UC 서비스 프로파일이 사용자가 생성한 새 서비스 프로파일(예: MRA_ServiceProfile)을 반영하는지 확인한 다음 저장을 클릭합니다.

7. 복제하는 데 몇 분 정도 걸릴 수 있습니다.엔드포인트에서 프로비저닝 모드를 비활성화하고 몇 분 후에 다시 켜서 엔드포인트가 지금 등록되는지 확인합니다.

관련 정보

- 모바일 및 원격 액세스 가이드
- VCS 인증서 생성 가이드
- EX90/EX60 시작 가이드
- CUCM 9.1 관리자 가이드
- 기술 지원 및 문서 – Cisco Systems