Esempio di configurazione degli endpoint basati su TC di Collaboration Edge

Sommario

Introduzione

Il documento descrive i requisiti per configurare e risolvere i problemi relativi alla registrazione degli endpoint basata su TelePresence Codec (TC) tramite la soluzione Mobile and Remote Access.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Soluzione Mobile and Remote Access
- Certificati di Video Communication Server (VCS)
- Expressway X8.1.1 o versioni successive
- Cisco Unified Communications Manager (CUCM) versione 9.1.2 o successive
- Endpoint basati su TC
- CE8.x richiede la chiave dell'opzione di crittografia per abilitare "Edge" come opzione di provisioning

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- VCS X8.1.1 o versione successiva
- CUCM release 9.1(2)SU1 o successive e IM & Presence 9.1(1) o successive
- Firmware TC 7.1 o successivo **(TC7.2 consigliato)**
- Controllo VCS e Expressway/Expressway Core & Edge
- CUCM
- Endpoint TC

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

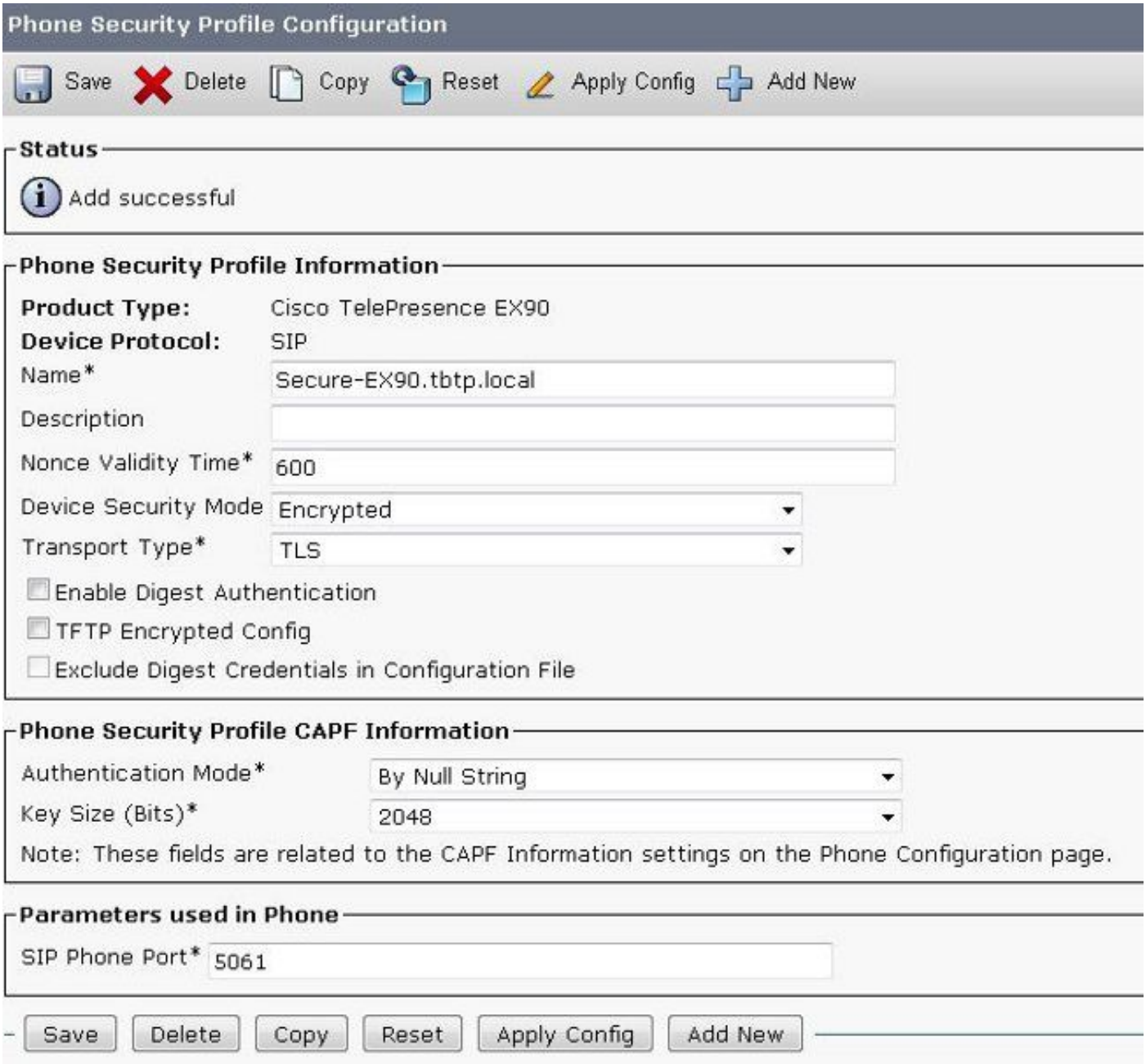
Configurazione

In questa procedura di configurazione si presuppone che l'amministratore configuri l'endpoint basato su TC per una registrazione sicura del dispositivo. La registrazione sicura **NON** è un requisito, tuttavia la guida generale alla soluzione di accesso remoto e mobile dà l'impressione che sia proprio perché ci sono schermate della configurazione che mostrano profili di dispositivi

sicuri su CUCM.

Passaggio 1. Creare un profilo per telefono protetto in CUCM in formato FQDN (facoltativo).

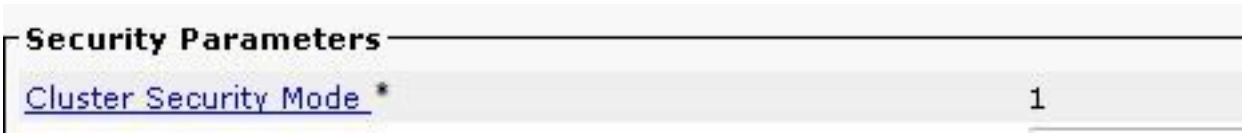
1. In CUCM, selezionare **Sistema > Sicurezza > Profilo sicurezza telefono**.
2. Fare clic su **Aggiungi nuovo**.
3. Selezionare il tipo di endpoint basato su TC e configurare i seguenti parametri:
4. Nome - **Secure-EX90.tbtp.local (formato FQDN richiesto)**
5. Modalità di protezione dispositivo - **Crittografia**
6. Tipo di trasporto - **TLS**
7. SIP Phone Port - **5061**



Passaggio 2. Verificare che la modalità di sicurezza del cluster sia (1) - Mista (facoltativo).

1. In CUCM, selezionare **Sistema > Parametri Enterprise**.

2. Scorrere verso il basso fino a **Parametri di sicurezza > Modalità di sicurezza cluster > 1**.



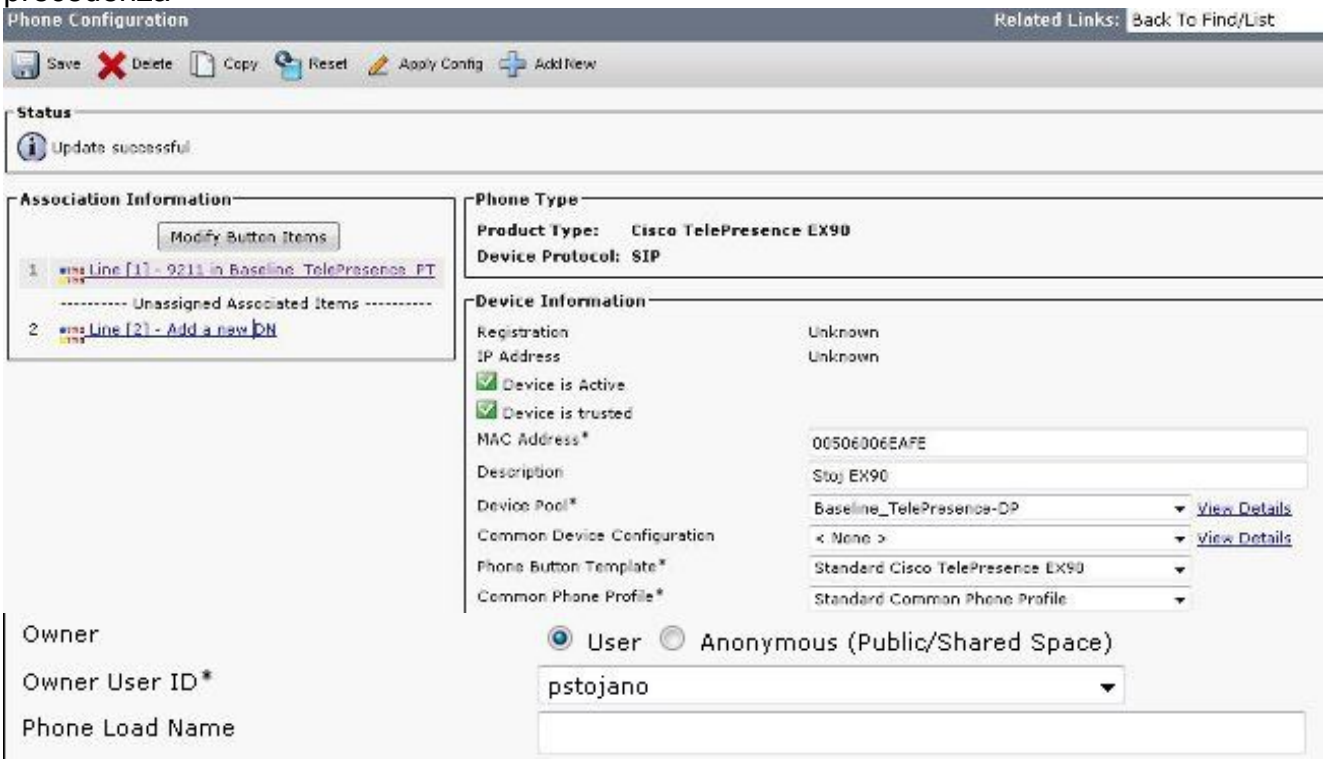
Se il valore non è 1, CUCM non è stato protetto. In questo caso, l'amministratore deve esaminare uno di questi due documenti per proteggere CUCM.

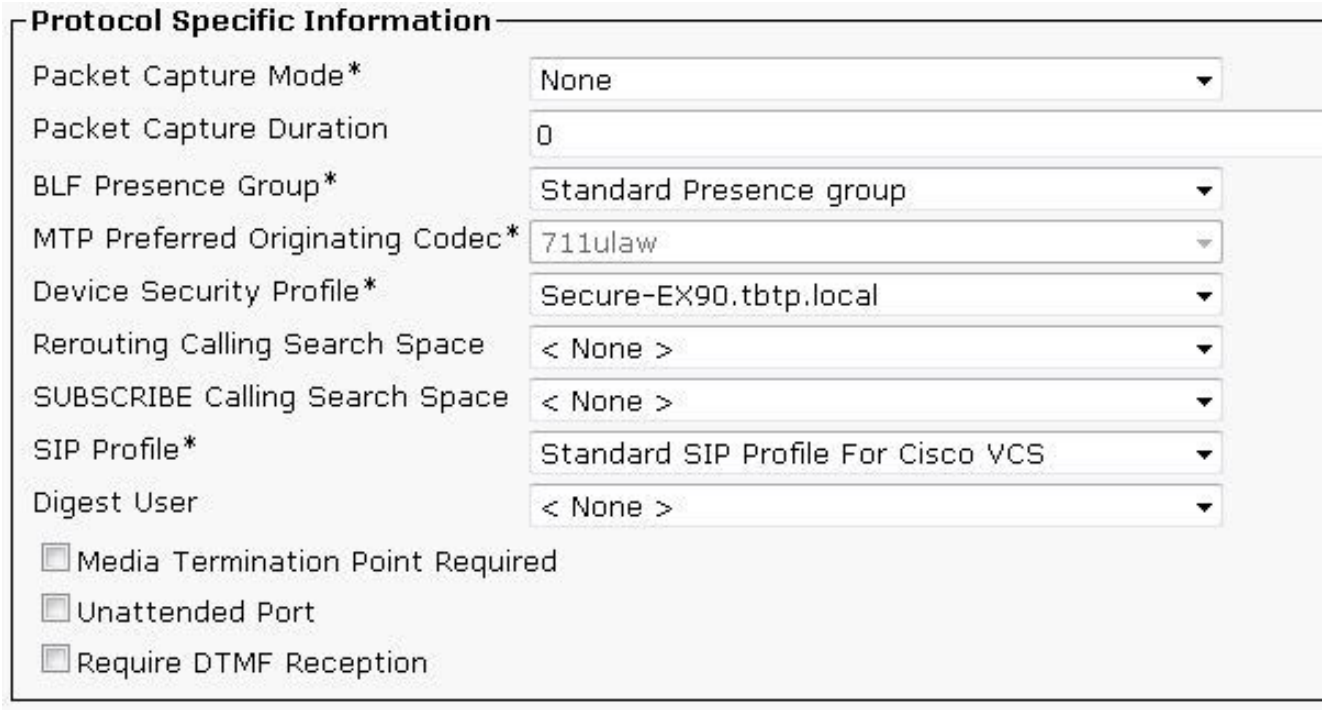
Guida alla sicurezza di CUCM 9.1(2)

Guida alla sicurezza di CUCM 10

Passaggio 3. Creare un profilo in CUCM per l'endpoint basato su TC.

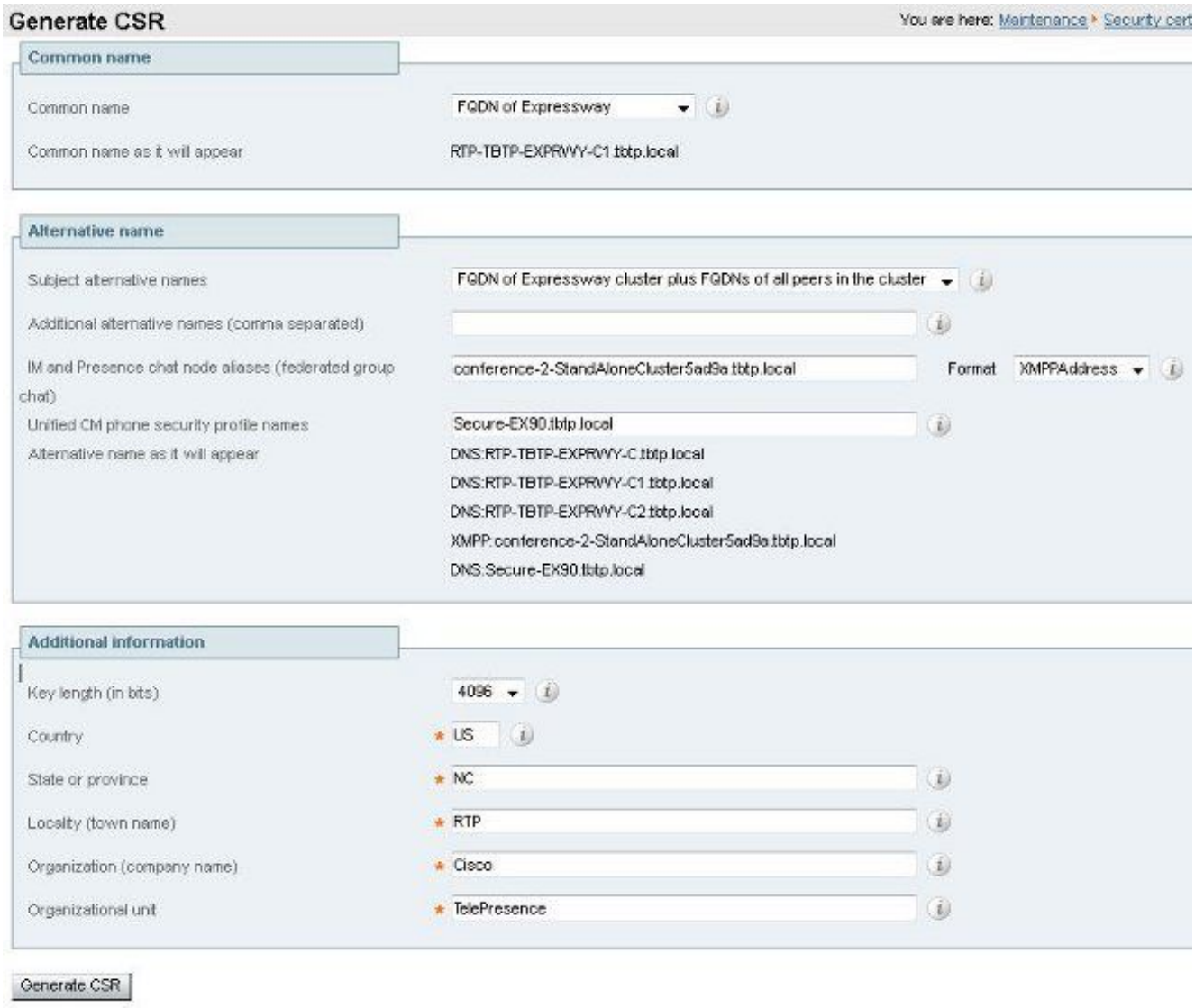
1. In CUCM, selezionare **Periferica > Telefono**.
2. Fare clic su **Aggiungi nuovo**.
3. Selezionare il tipo di endpoint basato su TC e configurare i seguenti parametri: Indirizzo MAC - Indirizzo MAC dal dispositivo basato su TCCampi contrassegnati con asterisco (*)Proprietario - UtenteID utente proprietario - Proprietario associato al dispositivoProfilo di sicurezza del dispositivo - Profilo configurato in precedenza (Secure-EX90.tbtp.local)Profilo SIP - Profilo SIP standard o qualsiasi profilo personalizzato creato in precedenza





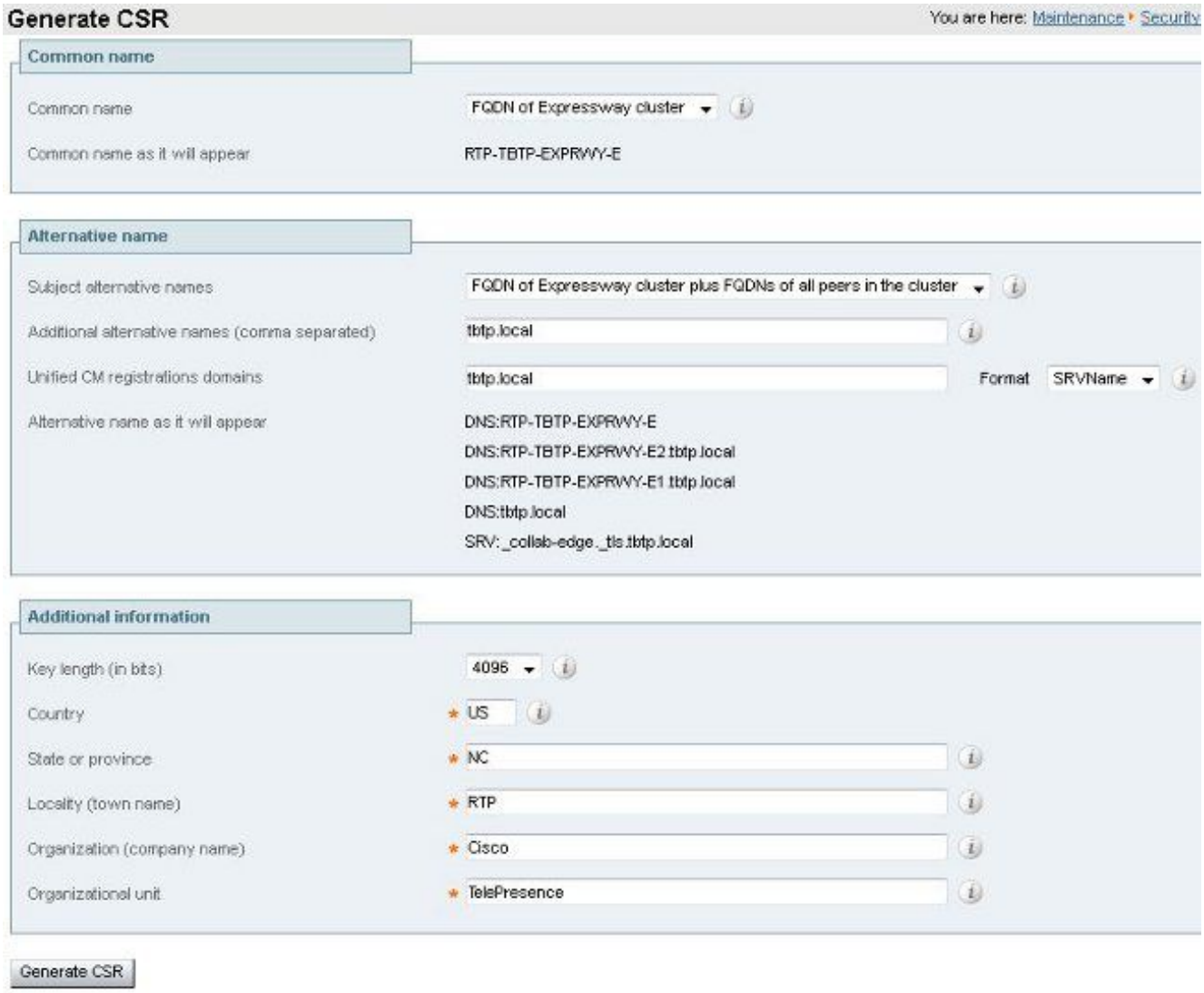
Passaggio 4. Aggiungere il nome del profilo di sicurezza alla SAN del certificato Expressway-C/VCS-C (facoltativo).

1. In Expressway-C/VCS-C, selezionare **Manutenzione > Certificati di sicurezza > Certificato server**.
2. Fare clic su **Genera CSR**.
3. Compilare i campi CSR (Certificate Signing Request) e verificare che il **nome del profilo di sicurezza telefonica di CM unificato** disponga del profilo di sicurezza telefonica esatto elencato nel formato FQDN (Fully Qualified Domain Name). Ad esempio, **Secure-EX90.tbtp.local**. **Nota:** I nomi dei profili di sicurezza telefonica di Unified CM sono elencati sul retro del campo Nome soggetto alternativo (SAN).
4. Inviare il CSR a un'Autorità di certificazione (CA) interna o di terze parti da firmare.
5. Selezionare **Manutenzione > Certificati di sicurezza > Certificato server** per caricare il certificato in Expressway-C/VCS-C.



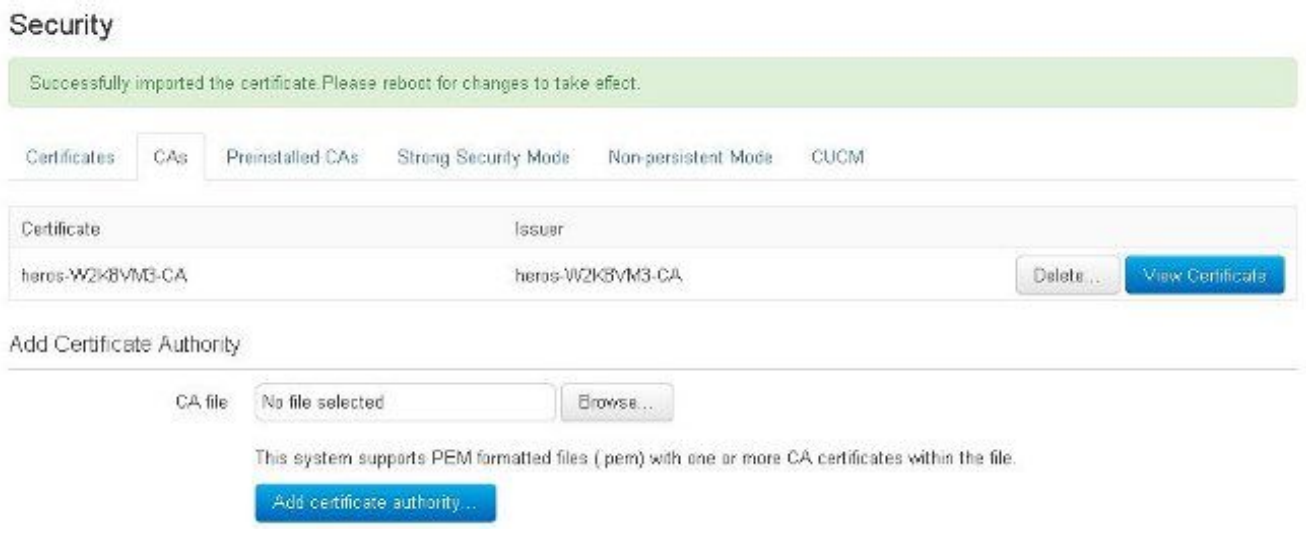
Passaggio 5. Aggiungere il dominio UC al certificato Expressway-E/VCS-E.

1. In Expressway-E/VCS-E selezionare **Manutenzione > Certificati di sicurezza > Certificato server**.
2. Fare clic su **Genera CSR**.
3. Compilare i campi CSR e verificare che i "domini di registrazione CM unificati" contengano il dominio a cui l'endpoint basato su TC invierà richieste Collaboration Edge (collab-edge) in formato DNS (Domain Name Server) o SRV (Service Name Server).
4. Inviare il CSR a una CA interna o di terze parti da firmare.
5. Selezionare **Manutenzione > Certificati di sicurezza > Certificato server** per caricare il certificato in Expressway-E/VCS-E.

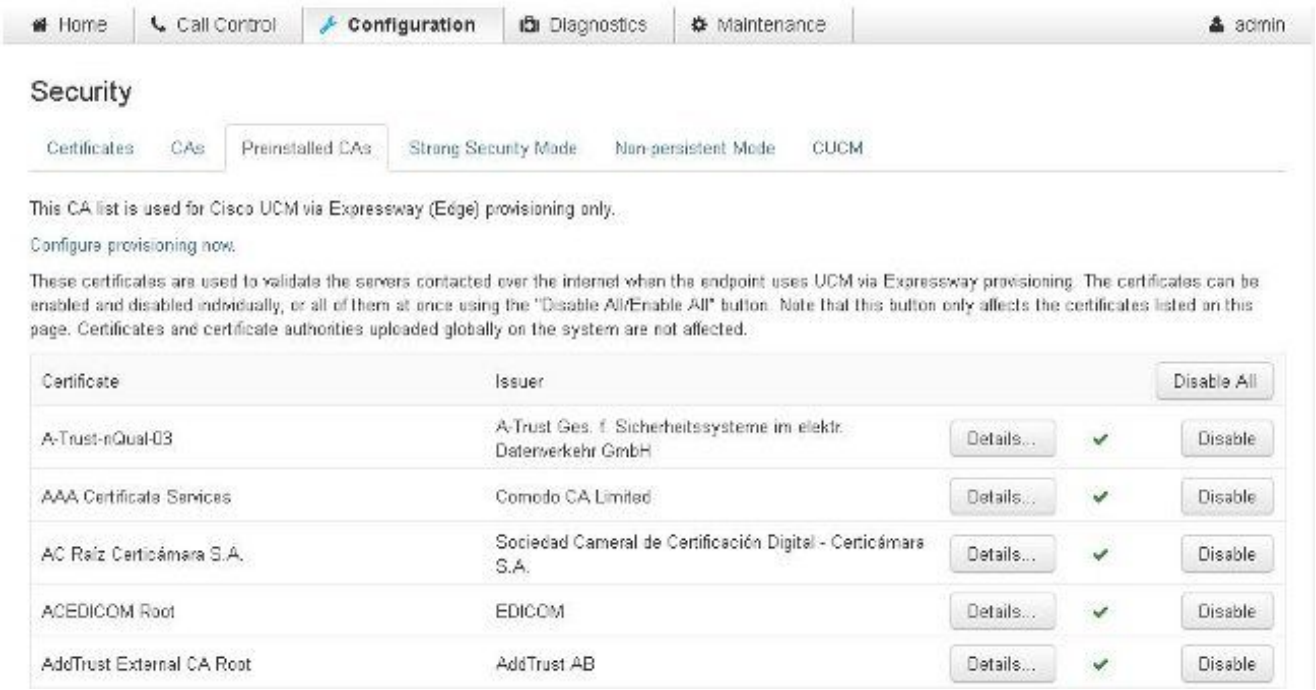


Passaggio 6. Installare il certificato CA attendibile appropriato nell'endpoint basato su TC.

1. Nell'endpoint basato su TC, selezionare **Configurazione > Sicurezza**.
2. Selezionare la scheda **CA** e cercare il certificato CA che ha firmato il certificato Expressway-E/VCS-E.
3. Fare clic su **Aggiungi autorità di certificazione**. **Nota:** Una volta aggiunto il certificato, questo verrà visualizzato nell'elenco dei
certificati.



Nota: TC 7.2 contiene un elenco di CA preinstallate. Se la CA che ha firmato il certificato Expressway-E è inclusa in questo elenco, i passaggi elencati in questa sezione non sono necessari.

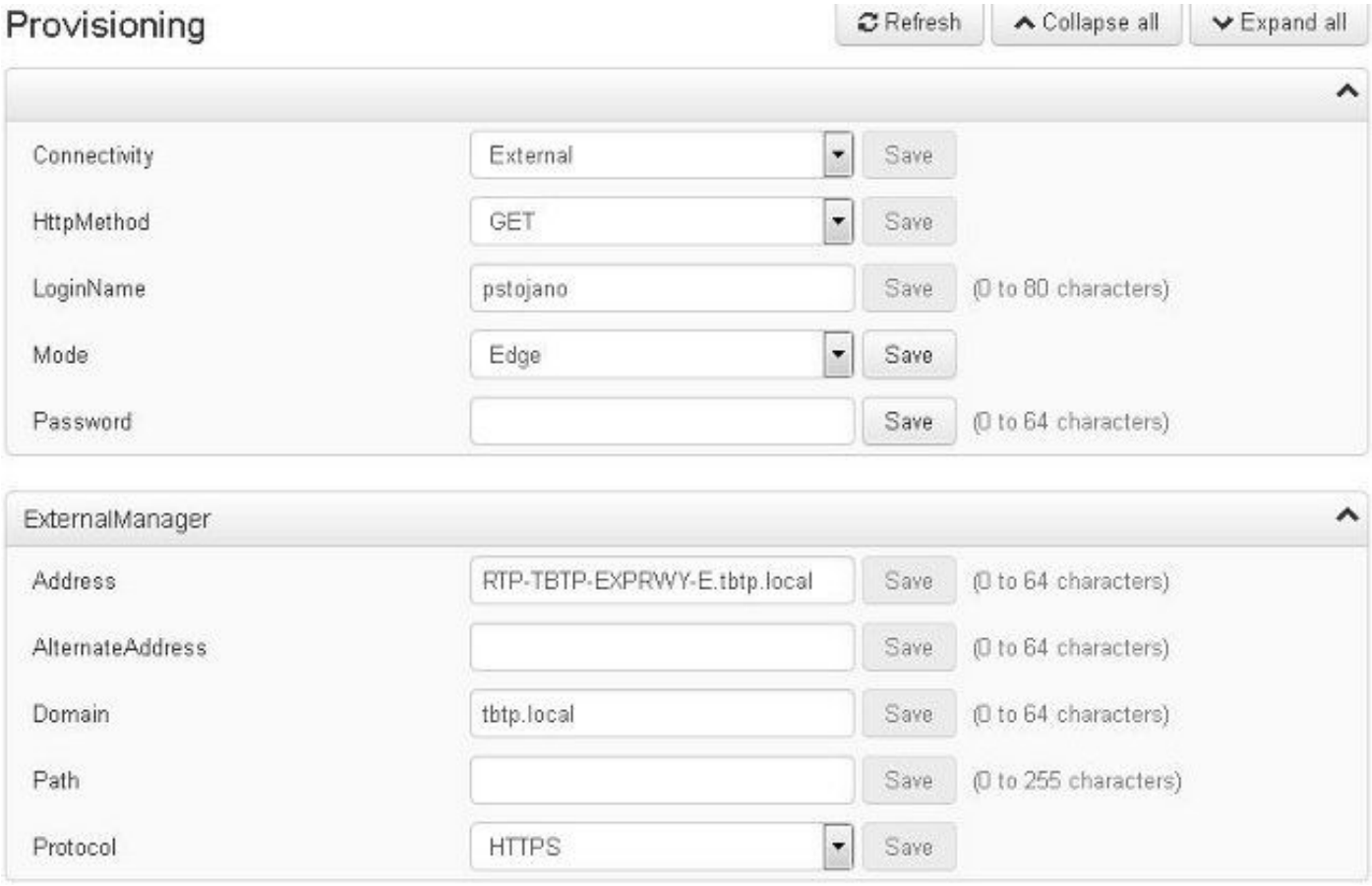


Nota: La pagina CA preinstallate contiene un pratico pulsante "Configura provisioning immediato" che consente di passare direttamente alla configurazione richiesta indicata al passaggio 2 della sezione successiva.

Passaggio 7. Configurazione di un endpoint basato su TC per il provisioning di Edge

- Nell'endpoint basato su TC, selezionare **Configurazione > Rete** e verificare che i campi siano compilati correttamente nella sezione DNS:
  Nome dominio
  Indirizzo server

- Nell'endpoint basato su TC, selezionare **Configurazione > Provisioning** e verificare che i campi siano compilati correttamente:
  LoginName - come definito in CUCM
  Modalità - **Bordo**
  Password - come definita in CUCM
  Responsabile esterno
  Indirizzo: nome host di Expressway-E/VCS-E
  Dominio - Dominio in cui è presente il record del margine del laboratorio



Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Endpoint basato su TC

1. Nell'interfaccia utente del Web, selezionare "Home". Cercare la sezione 'SIP Proxy 1' per uno stato "Registrato". L'indirizzo proxy è Expressway-E/VCS-E.

2. Dalla CLI, immettere **xstatus //prov**. Se si è registrati, lo stato di provisioning dovrebbe essere "Provisioning eseguito".

```
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

In CUCM, selezionare **Periferica > Telefono**. Scorrere l'elenco o filtrarlo in base all'endpoint. Verrà visualizzato il messaggio "Registrato con %CUCM_IP%". L'indirizzo IP a destra di questo deve essere Expressway-C/VCS-C che fornisce il proxy della registrazione.

Expressway-C

- In Expressway-C/VCS-C, selezionare **Status > Unified Communications > View Provisioning session.**
- Filtrare in base all'indirizzo IP dell'endpoint basato su TCP. Nell'immagine è mostrato un esempio di sessione di provisioning:

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

I problemi di registrazione possono essere causati da numerosi fattori, tra cui DNS, problemi di certificato, configurazione e così via. In questa sezione viene fornito un elenco completo di ciò che si verifica in genere quando si verifica un determinato problema e di come risolverlo. Se incontra

problemi che esulano da quanto è già stato documentato, non esitare a includerli.

Strumenti

Per iniziare, è importante conoscere gli strumenti a disposizione.

Endpoint TC

GUI Web

- tutto.log
- Avvia registrazione estesa (include l'acquisizione di un pacchetto completo)

CLI

Questi comandi sono particolarmente utili per risolvere i problemi in tempo reale:

- log ctx HttpClient debug 9
- log ctx PROV debug 9
- log output su <— Visualizza la registrazione tramite console

Un modo efficace per ricreare il problema consiste nel commutare la modalità di provisioning da "Edge" a "Off" e quindi tornare a "Edge" nell'interfaccia grafica Web. È inoltre possibile accedere alla **modalità di provisioning di xConfiguration:** nella CLI.

Expressways

- Registri diagnostici
- TCPDump

CUCM

- Tracce SDI/SDL

Numero 1: Il record del bordo della collab non è visibile e/o il nome host non è risolvibile

Come si può vedere, get_edge_config non riesce a causa della risoluzione dei nomi.

Registri 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/
```

Correzione

1. Verificare se il record collab-edge è presente e restituire il nome host corretto.
2. Verificare che le informazioni sul server DNS configurate nel client siano corrette.

Numero 2: CA non presente nell'elenco di CA attendibili nell'endpoint basato su TC

Registri 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: 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
```

Correzione

1. Verificare se nella scheda **Sicurezza > CA** dell'endpoint è elencata una CA di terze parti.
2. Se la CA è elencata, verificare che sia corretta.

Numero 3: Expressway-E non dispone del dominio UC elencato nella SAN

Registri 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'
```

Expressway-E SAN

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

Correzione

1. Rigenerare CSR Expressway-E per includere i domini UC.
2. Èpossibile che nell'endpoint TC il parametro **ExternalManager Domain** non sia impostato sul dominio UC. In questo caso, è necessario trovare una corrispondenza.

Numero 4: Il nome utente e/o la password forniti nel profilo di provisioning del TC non sono corretti

Registri endpoint TC

```
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"
```

Correzione

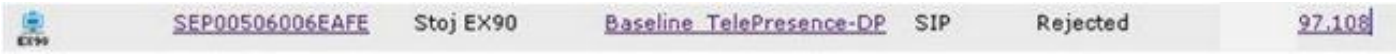
1. Verificare che il nome utente e la password immessi nella pagina Provisioning sull'endpoint TC siano validi.
2. Verificare le credenziali rispetto al database CUCM.
3. Versione 10 - utilizzo del portale Self Care
4. Versione 9 - utilizzare le opzioni utente di CM

L'URL di entrambi i portali è lo stesso: **https://%CUCM%/ucmuser/**

Se viene visualizzato un errore relativo ai diritti insufficienti, assicurarsi che all'utente vengano assegnati i ruoli seguenti:

- CTI standard abilitata
- Utente finale CCM standard

Numero 5: La registrazione dell'endpoint basata su TC viene rifiutata



Tracce 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,
```

Endpoint TC

Expressway-C/VCS-C effettivo

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

In questo esempio di registro specifico è chiaro che Expressway-C/VCS-C non contiene il nome di dominio completo (FQDN) del profilo di sicurezza telefono nella rete SAN (Secure-EX90.tbtp.local). Nell'handshake TLS (Transport Layer Security), CUCM controlla il certificato del server di Expressway-C/VCS-C. Poiché non viene individuato all'interno della SAN, genera l'errore in grassetto e segnala che Previsto il profilo di sicurezza del telefono in formato FQDN.

Correzione

1. Verificare che Expressway-C/VCS-C contenga il profilo di sicurezza del telefono in formato FQDN all'interno della SAN del relativo certificato server.
2. Verificare che il dispositivo utilizzi il profilo di sicurezza corretto in CUCM se si utilizza un profilo sicuro in formato FQDN.
3. La causa potrebbe essere anche l'ID bug Cisco CSCuq86376. In questo caso, verificare le dimensioni della SAN Expressway-C/VCS-C e la posizione del profilo di sicurezza telefonica all'interno della SAN.

Numero 6: Provisioning degli endpoint basato su TC non riuscito - nessun server UDS

Questo errore deve essere presente in **Diagnostica > Risoluzione dei problemi** :

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

Registri endpoint TC

Scorrere verso destra per visualizzare gli errori in grassetto

```
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!
```

Correzione

1. Verificare che all'account utente finale utilizzato per richiedere il provisioning dell'endpoint tramite i servizi MRA siano associati un profilo di servizio e un servizio UC CTI.

2. Passare a **CUCM admin > Gestione utente > Impostazioni utente > Servizio UC** e creare un servizio UC CTI che punti all'IP di CUCM (ad esempio MRA_UC-Service).

3. Passare a **CUCM admin > User Management > User Settings > Service Profile** e creare un nuovo profilo (ad esempio MRA_ServiceProfile).

4. Nel nuovo profilo di servizio, scorrere verso il basso e nella sezione Profilo CTI, selezionare il nuovo servizio CTI UC appena creato (ad esempio MRA_UC-Service), quindi fare clic su Salva.

5. Passare a **CUCM admin > User Management > End User** (Gestione utenti > Utente **finale)** e individuare l'account utente utilizzato per richiedere il provisioning dell'endpoint tramite i servizi MRA.

6. In **Impostazioni servizio** dell'utente, verificare che il cluster home sia selezionato e che il profilo di servizio UC rifletta il nuovo profilo di servizio creato (ad esempio MRA_ServiceProfile), quindi fare clic su Salva.

7. La replica potrebbe richiedere alcuni minuti. Provare a disabilitare la modalità di provisioning sull'endpoint e riattivarla alcuni minuti dopo per verificare se l'endpoint è registrato.

Informazioni correlate

- Guida all'accesso remoto e mobile
- Guida alla creazione di certificati VCS
- Guida introduttiva per EX90/EX60
- Guida per l'amministratore di CUCM 9.1
- Documentazione e supporto tecnico – Cisco Systems