Collaboration Edge TC−based Endpoints Configuration Example

Document ID: 118696

Contributed by Paul Stojanovski, Cisco TAC Engineer.
Dec 08, 2014

Contents

Introduction

The document describes what is required in order to configure and troubleshoot TelePresence Codec (TC)−based endpoint registration through the Mobile and Remote Access solution.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Mobile and Remote Access Solution
- Video Communication Server (VCS) certificates

- Expressway X8.1.1 or later
- Cisco Unified Communication Manager (CUCM) Release 9.1.2 or later
- TC−based endpoints

Components Used

The information in this document is based on these software and hardware versions:

- VCS X8.1.1 or later
- CUCM Release 9.1(2)SU1 or later and IM & Presence 9.1(1) or later
- TC 7.1 or later firmware ***(TC7.2 recommended)***
- VCS Control & Expressway/Expressway Core & Edge
- CUCM
- TC Endpoint

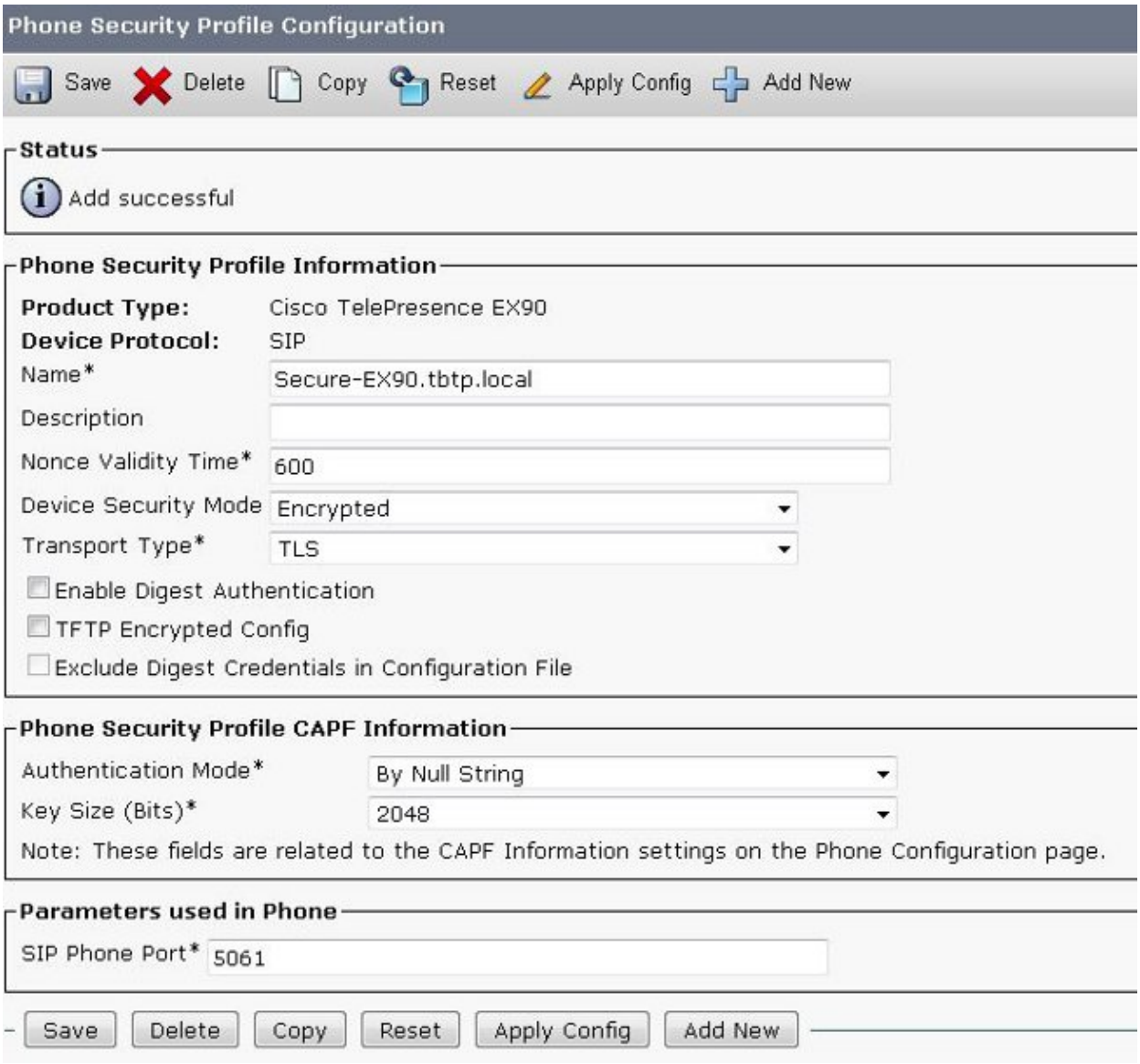
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

These configuration steps assume that the administrator will configure the TC−based endpoint for secure device registration. Secure registration is ***NOT*** a requirement, however the overall Mobile and Remote Access solution guide gives the impression that it is since there are screen shots from the configuration that show secure device profiles on CUCM.

Create a Secure Phone Profile on CUCM in FQDN Format (Optional)

1. In CUCM, select ***System*** > ***Security*** > ***Phone Security Profile***.
2. Click ***Add New***.
3. Select the TC−based endpoint type and configure these parameters:
    a. Name − ***Secure−EX90.tbtp.local (FQDN Format Required)***
    b. Device Security Mode − ***Encrypted***
    c. Transport Type − ***TLS***
    d. SIP Phone Port − ***5061***



Ensure Cluster Security Mode is (1) − Mixed (Optional)

1. In CUCM, select ***System*** > ***Enterprise Parameters***.
2. Scroll down to ***Security Parameters*** > ***Cluster Security Mode*** > ***1***.

If the value is not 1 the CUCM has not been secured. If this is the case, the administrator needs to review one of these two documents in order to secure the CUCM.

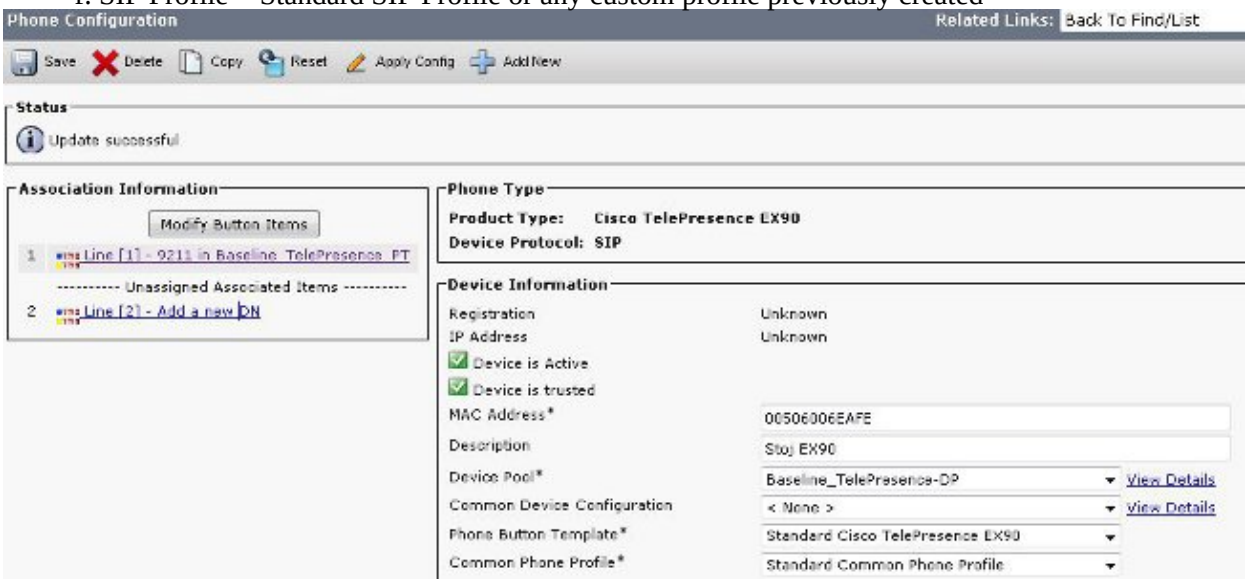
CUCM 9.1(2) Security Guide

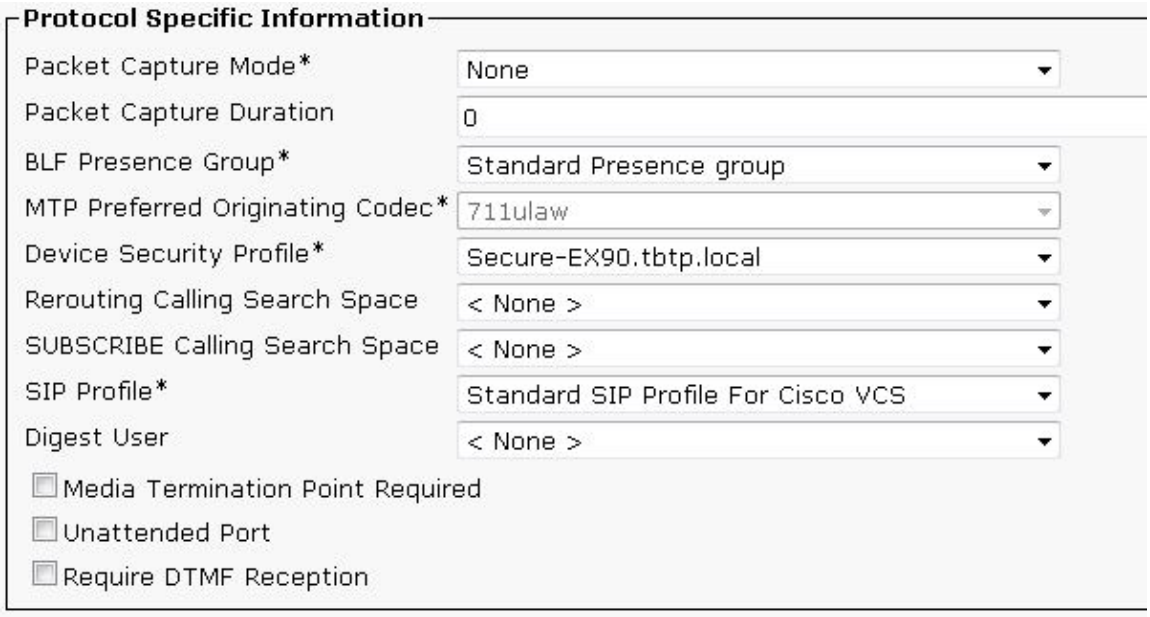
CUCM 10 Security Guide

Create a Profile in CUCM for the TC−based Endpoint

1. In CUCM, select ***Device*** > ***Phone***.
2. Click ***Add New***.

3. Select the TC−based endpoint type and configure these parameters:
    a. MAC Address − MAC Address from the TC−based device
    b. Required starred fields (*)
    c. Owner − User
    d. Owner User ID − Owner associated with device
    e. Device Security Profile − Previously Configured Profile (Secure−EX90.tbtp.local)
    f. SIP Profile − Standard SIP Profile or any custom profile previously created



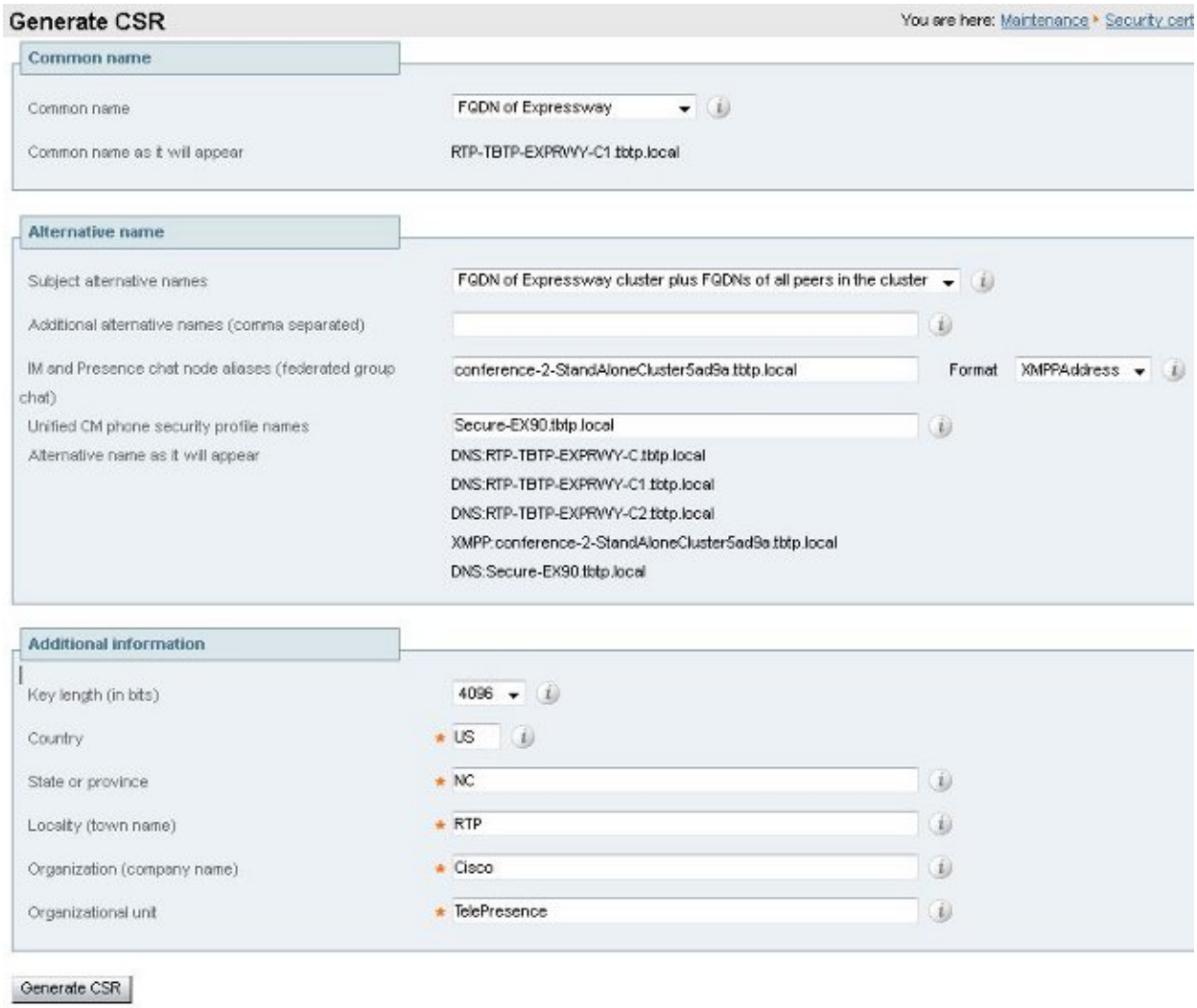


Add the Security Profile Name to the SAN of the Expressway−C/VCS−C Certificate (Optional)

1. In Expressway−C/VCS−C, select ***Maintenance*** > ***Security Certificates*** > ***Server Certificate***.
2. Click ***Generate CSR***.

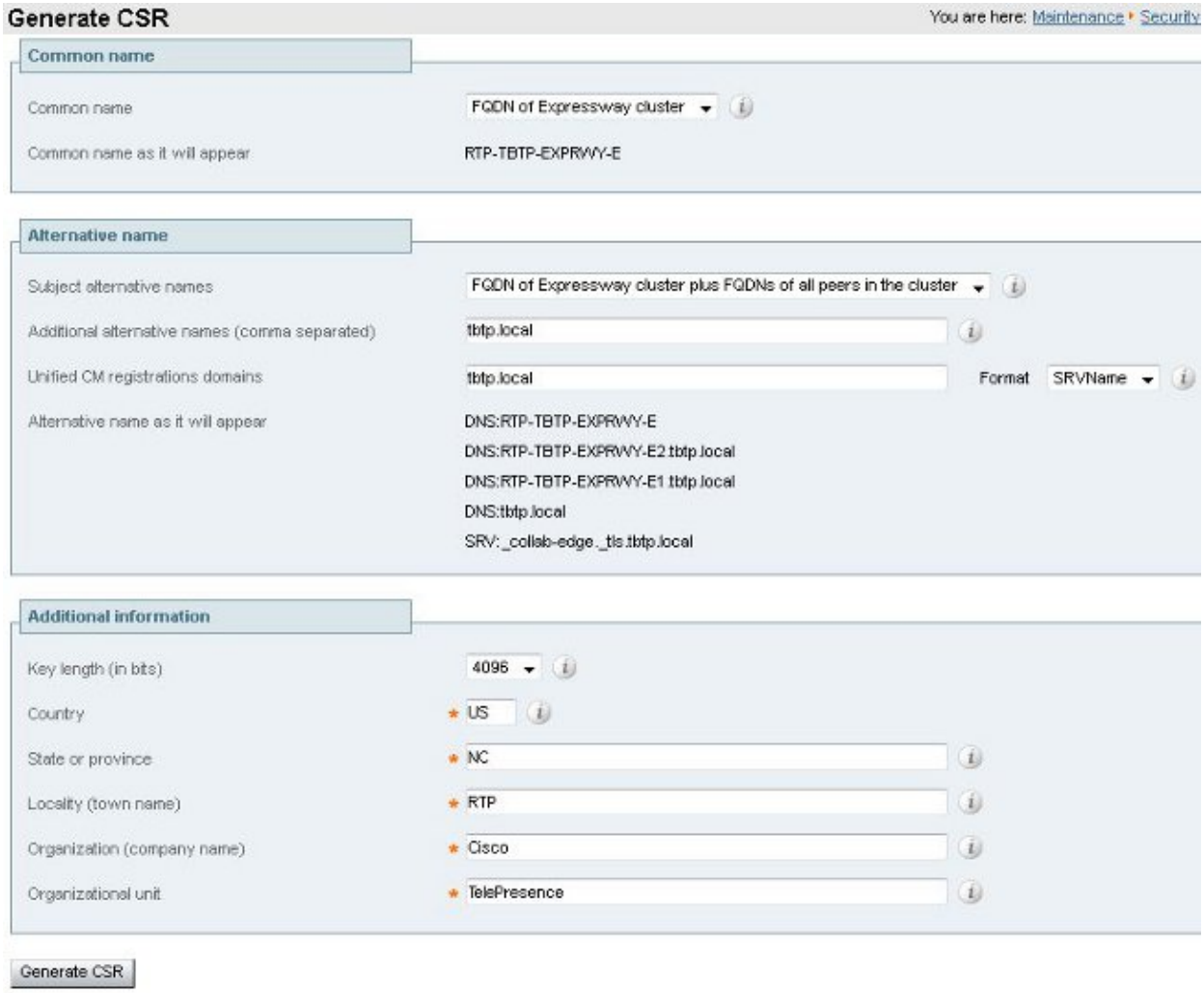
3. Fill out the Certificate Signing Request (CSR) fields and ensure that the "Unified CM phone security profile name" has the exact Phone Security Profile listed in Fully Qualified Domain Name (FQDN) format. For example, Secure−EX90.tbtp.local.

   Note: The Unified CM phone security profile names are listed at the back of the Subject Alternate Name (SAN) field.
4. Send the CSR off to either an Internal or 3rd Party Certificate Authority (CA) to be signed.
5. Select ***Maintenance > Security Certificates > Server Certificate*** in order to upload the certificate to the Expressway−C/VCS−C.



Add the UC Domain to the Expressway−E/VCS−E Certificate

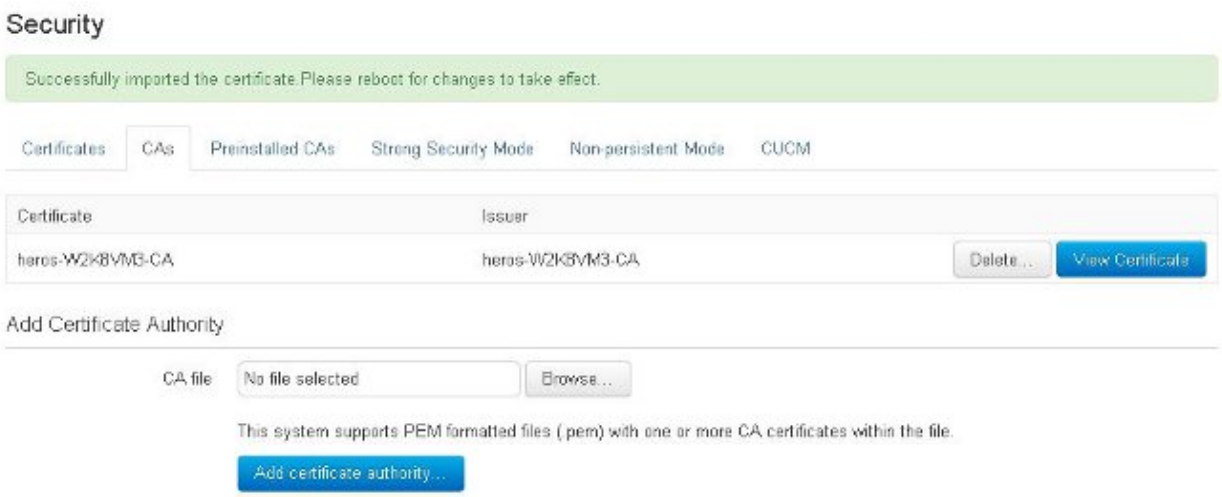
1. In Expressway−E/VCS−E, select ***Maintenance > Security Certificates > Server Certificate***.
2. Click ***Generate CSR***.
3. Fill out the CSR fields and ensure that "Unified CM registrations domains" contain the domain that the TC−based endpoint will make Collaboration Edge (collab−edge) requests to, in either the Domain Name Server (DNS) or Service Name (SRV) formats.
4. Send the CSR off to either an Internal or 3rd Party CA to be signed.
5. Select ***Maintenance > Security Certificates > Server Certificate*** in order to upload the certificate to the Expressway−E/VCS−E.



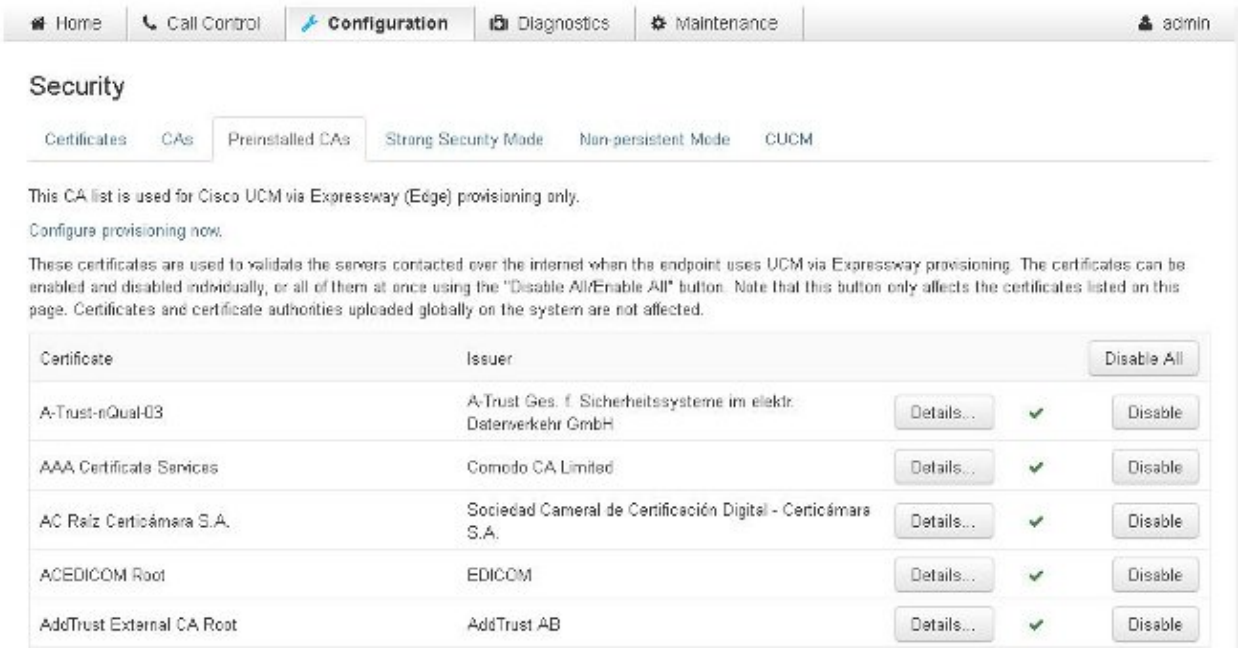
Install the Proper Trusted CA Certificate to the TC−based Endpoint

1. In the TC−based Endpoint, select ***Configuration*** > ***Security***.
2. Select the ***CA*** tab and browse for the CA certificate that signed your Expressway−E/VCS−E certificate.
3. Click ***Add certificate authority***.

Note: Once the certificate is successfully added you will see it listed in the Certificate list.



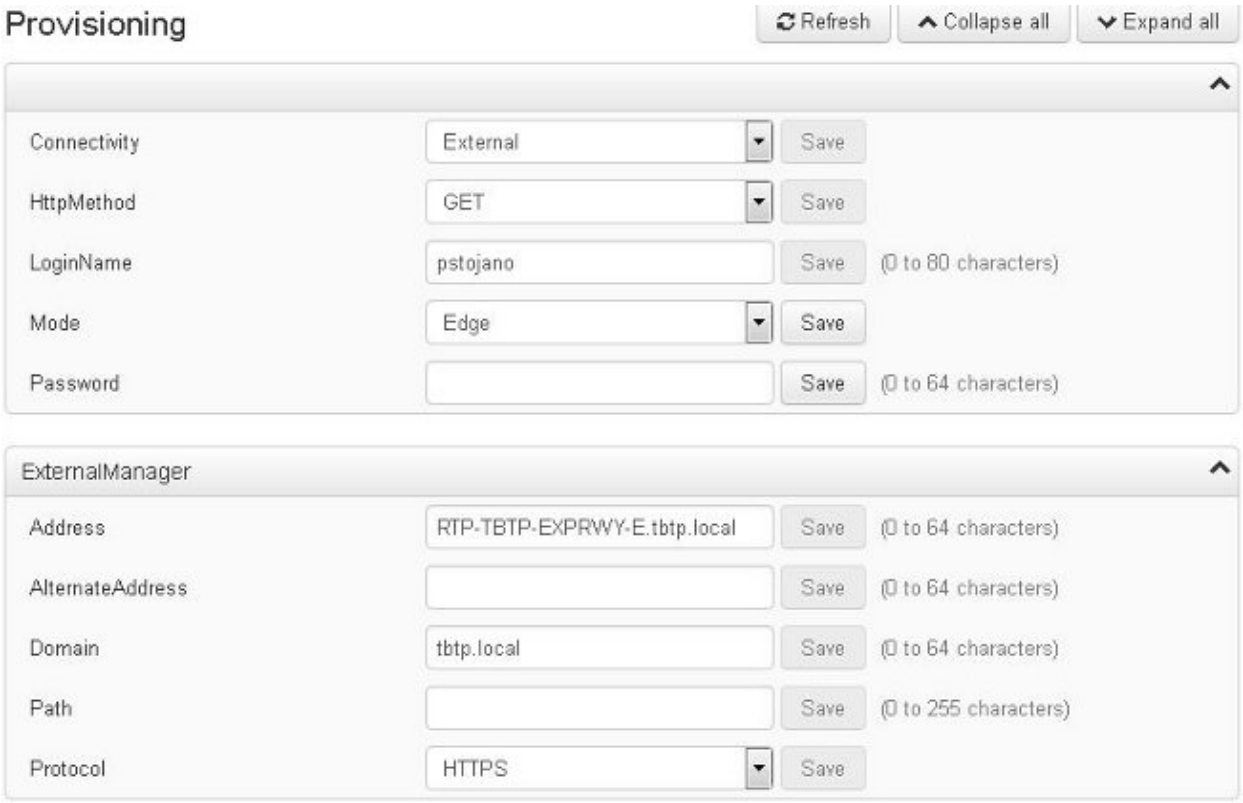
Note: TC 7.2 contains a pre−installed CAs list. If the CA that signed the Expressway−E certificate is contained within this list, the steps listed in this section are not required.



Note: The preinstalled CAs page contains a convenient "Configure provisioning now" button that takes you directly to the required configuration noted in step 2 in the next section.

Set Up a TC−based Endpoint for Edge Provisioning

1. In the TC−based endpoint, select ***Configuration*** > ***Network*** and ensure these fields are properly filled in under the DNS section:
    a. Domain Name
    b. Server Address
2. In the TC−based endpoint, select ***Configuration*** > ***Provisioning*** and ensure these fields are properly filled in:
    a. LoginName − as defined in CUCM
    b. Mode − ***Edge***
    c. Password − as defined in CUCM
    External Manager
    d. Address − Hostname of your Expressway−E/VCS−E
    e. Domain − Domain where your collab−edge record is present



Verify

Use this section to confirm that your configuration works properly.

TC−based Endpoint

1. In the web GUI, navigate to "Home". Look for the 'SIP Proxy 1" section for a "Registered" Status. The Proxy address is your Expressway−E/VCS−E.

2. From the CLI, enter ***xstatus //prov***. If you are registered you should see a Provisioning Status of "Provisioned".

```
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
```

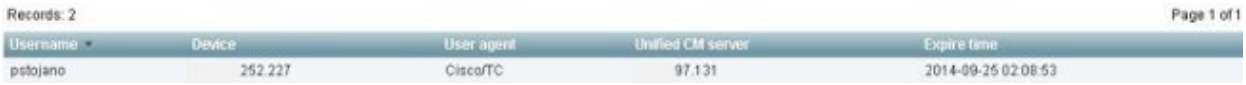
```
*s Provisioning CUCM ExtensionMobility LastLoggedInUserId: ""
*s Provisioning CUCM ExtensionMobility LoggedIn: False
*s Provisioning CUCM ITL State: Installed
*s Provisioning CUCM ProvisionSecurity: Signed
*s Provisioning CUCM TVS Proxy 1 IPv6Address: ""
*s Provisioning CUCM TVS Proxy 1 Port: 2445
*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, select ***Device*** > ***Phone***. Either scroll through the list or filter the list based on your endpoint. You should see a "Registered with %CUCM_IP%" message. The IP address to the right of this should be your Expressway−C/VCS−C which proxies the registration.

Expressway−C

1. In Expressway−C/VCS−C, select ***Status*** > ***Unified Communications*** > ***View Provisioning sessions.***
2. Filter by the IP address of your TC−based endpoint. An example of a Provisioned Session is shown here:



Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Registration issues can be caused by numerous factors which include DNS, certificate issues, configuration, and so on. This section includes a comprehensive list of what you would typically see if you encounter a given problem and how to remediate it. If you run into issues outside of what has already been documented, feel free to include it.

Tools

For starters, be aware of the tools at your disposal.

TC Endpoint

Web GUI

- all.log
- Start extended logging (include a full packet capture)

CLI

These commands are most beneficial in order to troubleshoot in real−time:

- log ctx HttpClient debug 9
- log ctx PROV debug 9
- log output on <−− Shows logging via console

An effective way to recreate the problem is to toggle the Provisioning Mode from "Edge" to "Off" and then back to "Edge" within the web GUI. You can also enter the ***xConfiguration Provisioning Mode:*** command in the CLI.

Expressways

- Diagnostic Logs
- TCPDump

CUCM

- SDI/SDL Traces

Issue 1: Collab−edge Record is Not Visible and/or Hostname is Not Resolvable

As you can see, the get_edge_config fails due to name resolution.

TC Endpoint Logs

```
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/
```

Remediation

1. Verify if the collab−edge record is present and returns the correct hostname.
2. Verify if the DNS server information configured on the client is correct.

Issue 2: CA Is Not Present within the Trusted CA List on the TC−based Endpoint

TC Endpoint Logs

```
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
```

Remediation

1. Verify if a 3rd Party CA is listed under the ***Security*** > ***CAs*** tab on the endpoint.
2. If the CA is listed, verify that it is correct.

Issue 3: Expressway−E Does Not Have the UC Domain Listed within the SAN

TC Endpoint Logs

```
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
```

Remediation

1. Regenerate Expressway−E CSR in order to include the UC Domain(s).
2. It is possible that on the TC endpoint the "ExternalManager Domain" parameter is not set to what the UC Domain is. If this is the case you must match it.

Issue 4: Username and/or Password Supplied in the TC Provisioning Profile Is Incorrect

TC Endpoint Logs

```
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"
```

Remediation

1. Verify that the Username/Password entered under the Provisioning page on the TC endpoint is valid.
2. Verify credentials against the CUCM database.

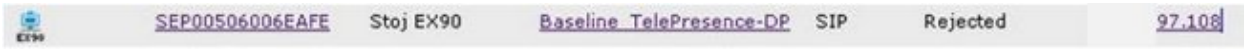
a. Version 10 − use the Self Care Portal
b. Version 9 − use the CM User Options

The URL for both portals is the same: https://%CUCM%/ucmuser/

If presented with an insufficient rights error, ensure these roles are assigned to the user:

- Standard CTI Enabled
- Standard CCM End User

Issue 5: TC−based Endpoint Registration Gets Rejected



CUCM Traces

```
08080021.043 |16:31:15.937 |AppInfo  |SIPStationD(18400) − validTLSConnection:TLS
 InvalidX509NameInCertificate, Rcvd=RTP−TBTP−EXPRWY−C.tbtp.local,
 Expected=SEP00506006EAFE. Will check SAN the next
08080021.044 |16:31:15.937 |AppInfo  |SIPStationD(18400) − validTLSConnection:TLS
 InvalidX509NameInCertificate Error , did not find matching SAN either,
 Rcvd=RTP−TBTP−EXPRWY−C.tbtp.local, Expected=Secure−EX90.tbtp.local
08080021.045 |16:31:15.937 |AppInfo  |ConnectionFailure − Unified CM failed to open
 a TLS connection for the indicated device Device Name:SEP00506006EAFE
 IP Address:xx.xx.97.108 IPV6Address: Device type:584 Reason code:2 App ID:Cisco
 CallManager Cluster ID:StandAloneCluster Node ID:RTP−TBTP−CUCM9  08080021.046
 |16:31:15.938 |AlarmErr |AlarmClass: CallManager, AlarmName: ConnectionFailure,
 AlarmSeverity: Error, AlarmMessage: , AlarmDescription: Unified CM failed to open
 a TLS connection for the indicated device, AlarmParameters:
  DeviceName:SEP00506006EAFE, IPAddress:xx.xx.97.108, IPV6Address:,
 DeviceType:584, Reason:2, AppID:Cisco CallManager, ClusterID:StandAloneCluster,
 NodeID:RTP−TBTP−CUCM9,
```

TC Endpoint

Actual Expressway−C/VCS−C

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

In this specific log example it is clear that the Expressway−C/VCS−C does not contain the Phone Security Profile FQDN in the SAN. (Secure−EX90.tbtp.local). In the Transport Layer Security (TLS) Handshake, the CUCM inspects the Expressway−C/VCS−C's server certificate. Since it does not find it within the SAN it throws the error bolded and reports that it Expected the Phone Security Profile in FQDN format.

Remediation

1. Verify that the Expressway−C/VCS−C contains the Phone Security Profile in FQDN format within the SAN of it's server certificate.
2. Verify that the device uses the correct security profile in CUCM if you use a secure profile in FQDN format.

3. This could also be caused by Cisco bug ID CSCuq86376. If this is the case check the Expressway−C/VCS−C SAN size and the position of the Phone Security Profile within the SAN.

Related Information

- ***Mobile & Remote Access Guide***
- ***VCS Certificate Creation Guide***
- ***EX90/EX60 Getting Started Guide***
- ***CUCM 9.1 Administrator Guide***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Dec 08, 2014 Document ID: 118696