协作边缘TC根据终端配置示例

Contents

Introduction
Prerequisites
Requirements
Components Used
Configure
步骤1.创建在CUCM的一个安全的电话配置文件以FQDN格式(可选)。
Step 2.保证簇安全模式是(1) -混合(可选)。
步骤3.创建在CUCM的一个配置文件基于TC的终端的。
步骤4.添加安全配置文件名字到ExpresswayC/VCS C认证的SAN (可选)。
步骤5.添加UC域到ExpresswayE/VCS E认证。
步骤6.安装适当的委托的CA证书对基于TC的终端。
步骤7.设置边缘设置的一个基于TC的终端
Verify
基于TC的终端
CUCM
Expressway-C
Troubleshoot
工具
TC终端
高速公路
CUCM
问题1 ：Collab边缘记录不是可视的并且/或者主机名不是可溶解的
TC终端日志
修正
问题2 ：CA在基于TC的终端的委托的CA列表内不是存在
TC终端日志
修正
问题3 ：ExpresswayE没有在SAN内列出的UC域
TC终端日志
ExpresswayE SAN
修正
问题4 ：在TC和密码供应的用户名设置配置文件是不正确的
TC终端日志
ExpresswayC/VCS C
修正
问题5 ：基于TC的终端注册被拒绝
CUCM跟踪
TC终端
实际ExpresswayC/VCS C
修正

问题6 ：基于TC的终端设置发生故障-没有UDS服务器
Related Information

Introduction

本文描述要求什么配置和排除网真编码(TC)故障-基于终端注册通过移动和远程访问解决方案。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- 移动和远程访问解决方案
- 视频通信服务器(VCS)证书
- Expressway X8.1.1或以上
- Cisco Unified Communications管理器(CUCM)版本9.1.2或以上
- 基于TC的终端
- CE8.x要求Encryption选项键对enable (event) “边缘”作为设置选项

Components Used

本文档中的信息基于以下软件和硬件版本：

- VCS X8.1.1或以上
- CUCM版本9.1(2)SU1或以上和IM &存在9.1(1)或以后
- TC 7.1或以上固件**(建议使用的TC7.2)**
- VCS控制& Expressway/Expressway核心&边缘
- CUCM
- TC终端

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.

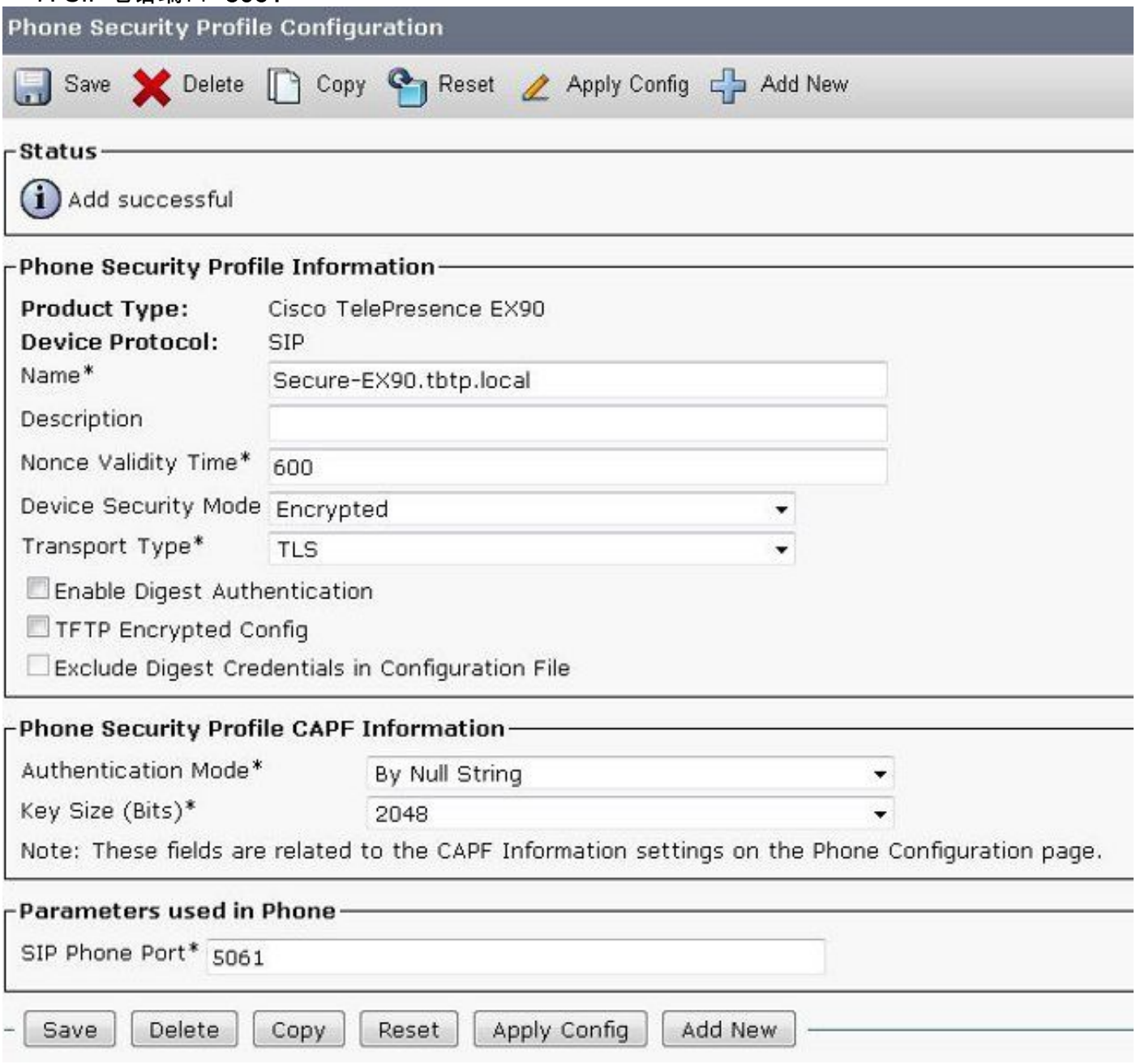
Configure

这些配置步骤假设，管理员将配置安全的设备已注册的基于TC的终端。安全的注册不是需求，然而整体移动和远程访问解决方案指南有印象是，因为有显示获取在CUCM的设备配置文件从配置的屏幕画面。

步骤1.创建在CUCM的安全的电话配置文件以FQDN格式(可选)。

1. 在CUCM，请选择**系统> Security >电话安全配置文件**。
2. 点击**添加新**。
3. 选择基于TC的终端类型并且配置这些参数：
4. 名字- **Secure-EX90.tbtp.local (需要的FQDN格式)**

5. 设备安全模式-**加密**
6. 传输类型- **TLS**
7. SIP电话端口- **5061**



Step 2.保证簇安全模式是(1) -混合(可选)。

1. 在CUCM，请选择**System > Enterprise Parameters**。
2. 移下来到**安全参数>簇安全模式> 1。**

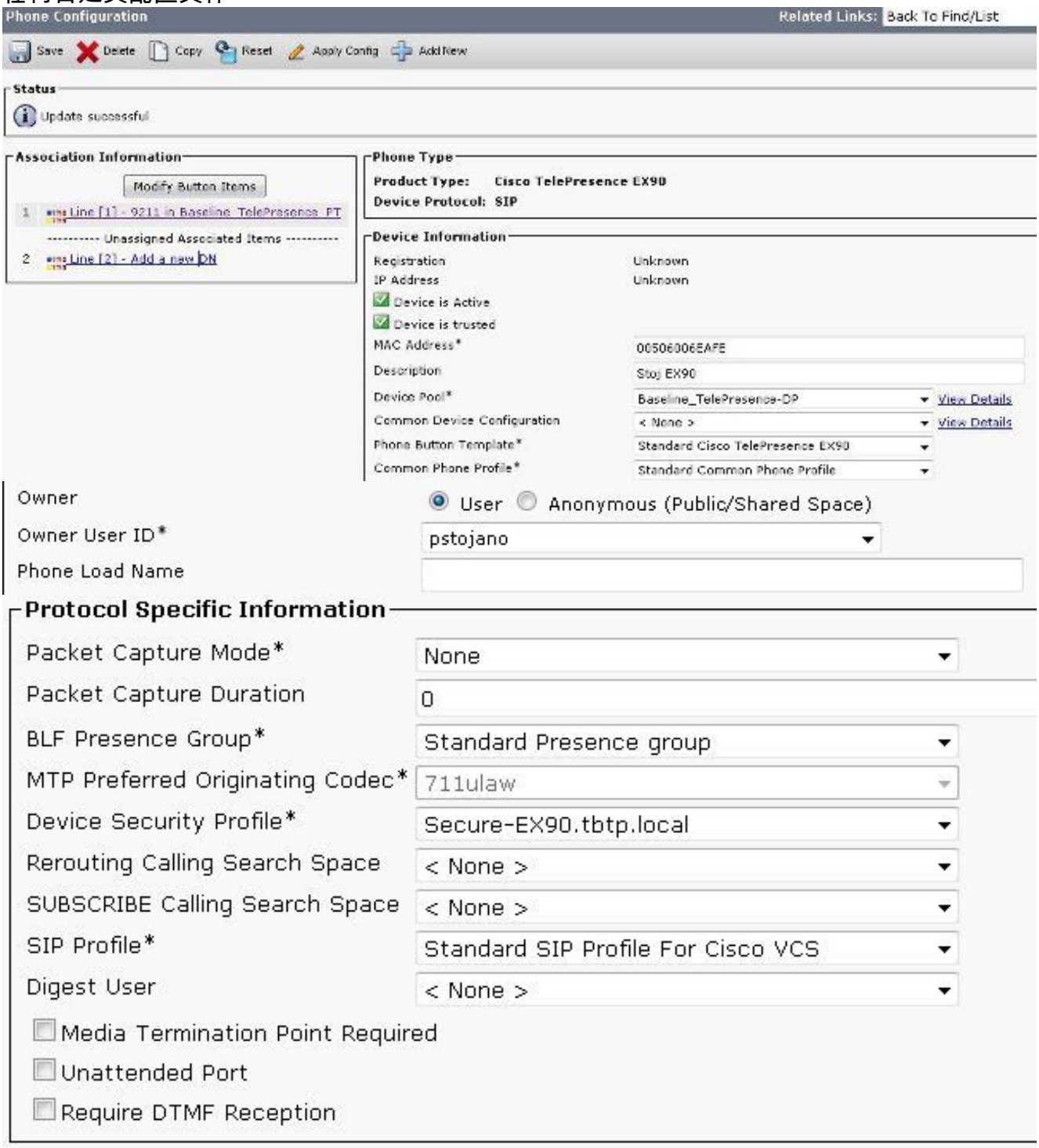
如果值不是1 CUCM未获取。如果这是实际情形，管理员需要查看这两个文件之一为了获取CUCM。

CUCM 9.1(2)安全指南

CUCM 10安全指南

步骤3.创建在CUCM的配置文件基于TC的终端的。

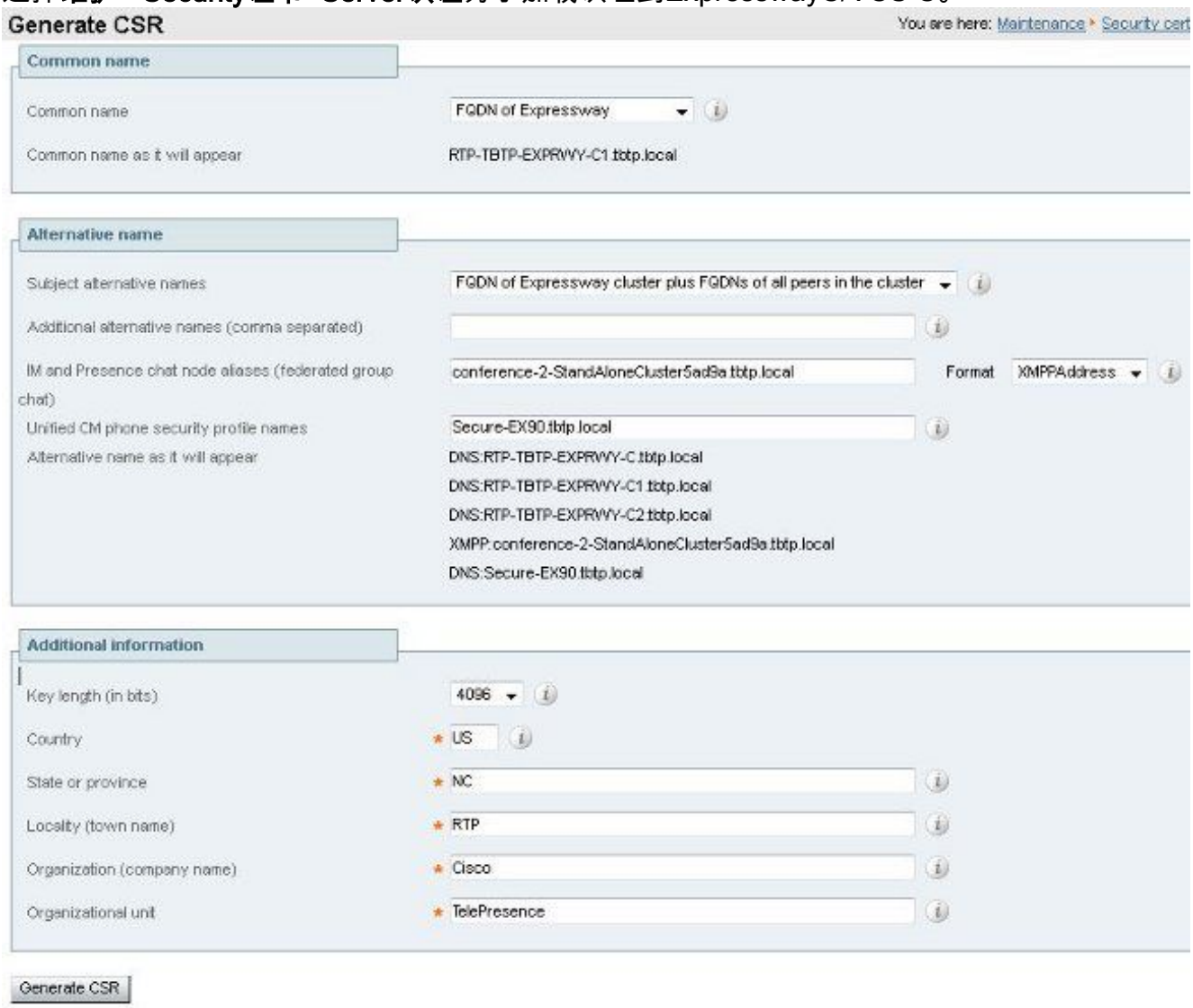
1. 在CUCM，请选择**Device > Phone**。
2. 点击**添加新**。
3. 选择基于TC的终端类型并且配置这些参数： MAC地址-从基于TC的设备的MAC地址必需的担任主角的字段(*)责任人-用户责任人用户ID -与设备产生关联的责任人设备安全配置文件-以前被配置的配置文件(Secure-EX90.tbtp.local)SIP配置文件-标准的SIP配置文件或以前被创建的任何自定义配置文件



步骤4.添加安全配置文件名字到ExpresswayC/VCS C认证的SAN (可选)。

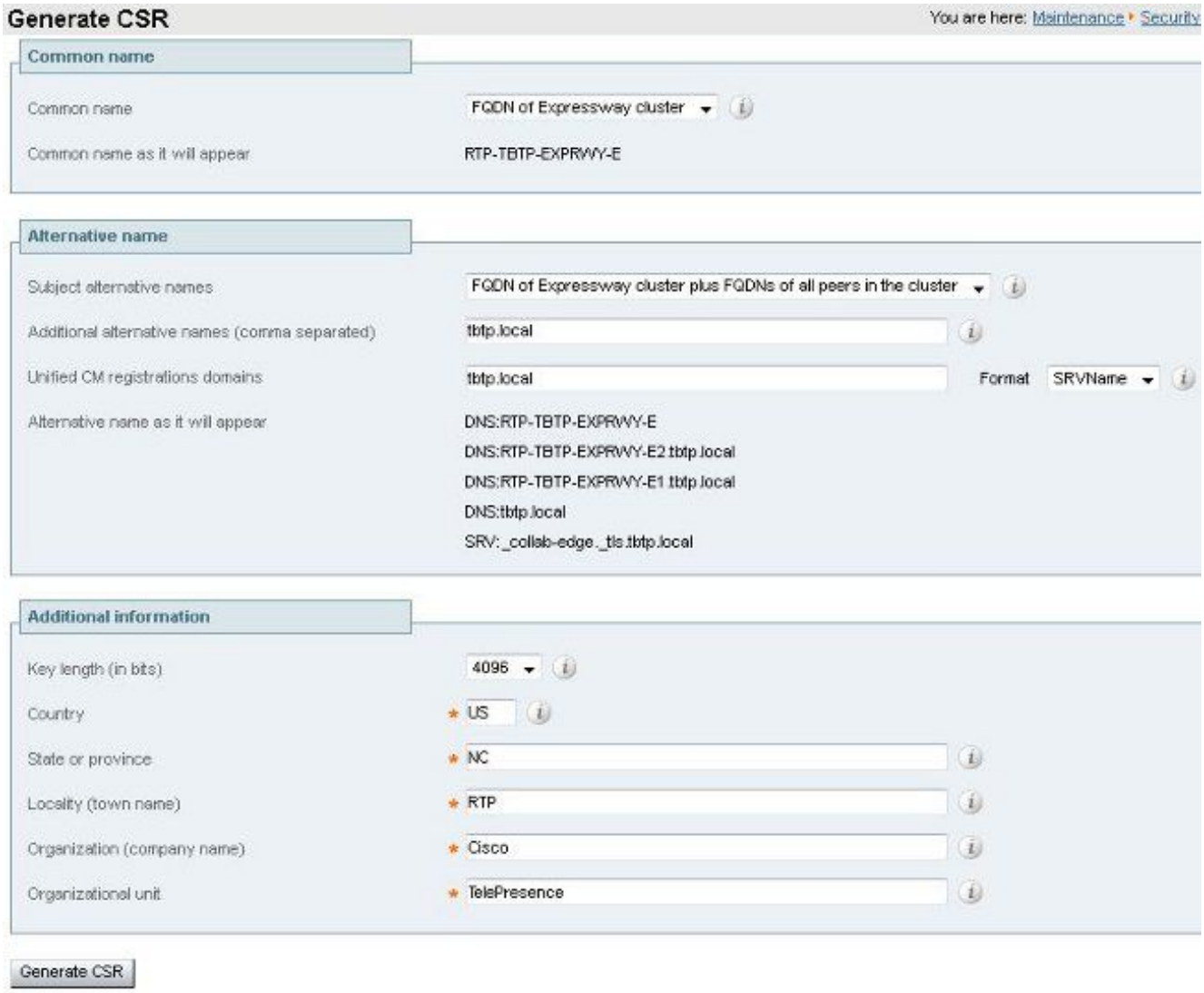
1. 在ExpresswayC/VCS C，请连接对**维护> Security证书>Server认证**。
2. 点击**生成CSR**。

3. 填写认证署名请求(CSR)字段并且保证**统一的CM电话安全配置文件名字**有列出的确切的电话安全配置文件在完全合格的域名(FQDN)格式。例如， **Secure-EX90.tbtp.local**。 **Note**:统一的CM电话安全配置文件名字是列出的在附属的替代名称(SAN)字段的返回。
4. 发送CSR到将签字的一内部或第三方Certificate Authority (CA)。
5. 选择**维护> Security证书>Server认证**为了加载认证到ExpresswayC/VCS C。



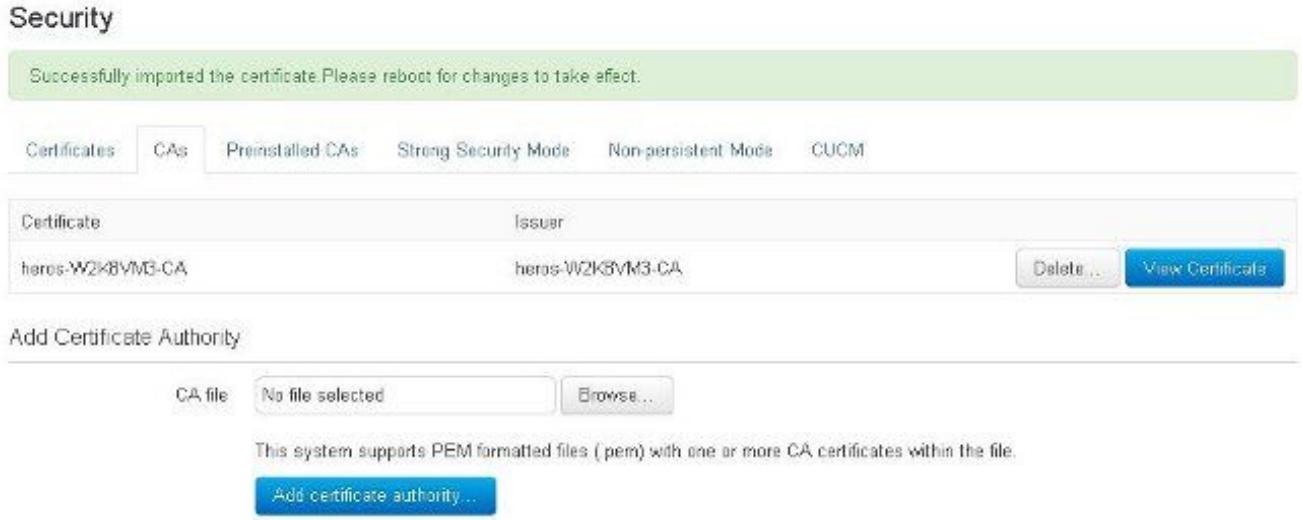
步骤5.添加UC域到ExpresswayE/VCS E认证。

1. 在ExpresswayE/VCS E，请选择**维护> Security证书>Server认证**。
2. 点击**生成CSR**。
3. 填写CSR字段并且保证“统一的CM注册域”包含域基于TC的终端将做协作边缘(collab边缘)请求对，以域名服务器(DNS)或服务名称(SRV)格式。
4. 发送CSR到将签字的内部或第三方CA。
5. 选择**维护> Security证书>Server认证**为了加载认证到ExpresswayE/VCS E。

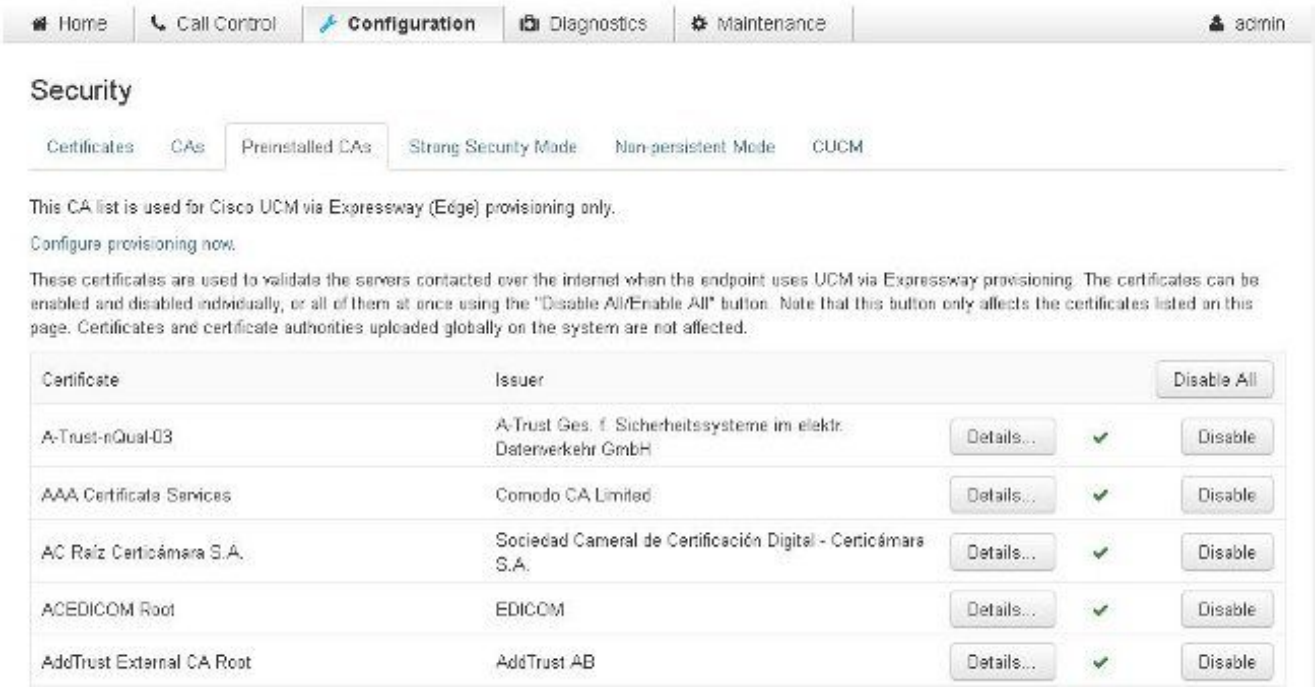


步骤6.安装适当的委托的CA证书对基于TC的终端。

1. 在基于TC的终端，请选择**Configuration>安全**。
2. 选择**CA**选项并且为签署您的ExpresswayE/VCS E认证的CA证书访问。
3. 点击**添加认证机关**。 **Note**:一旦认证成功地添加您看到在认证列表列出了。



Note:TC 7.2包含一张被事先装配的CAs列表。如果签署ExpresswayE认证的CA在此列表内包含，没有需要在此部分列出的步骤。

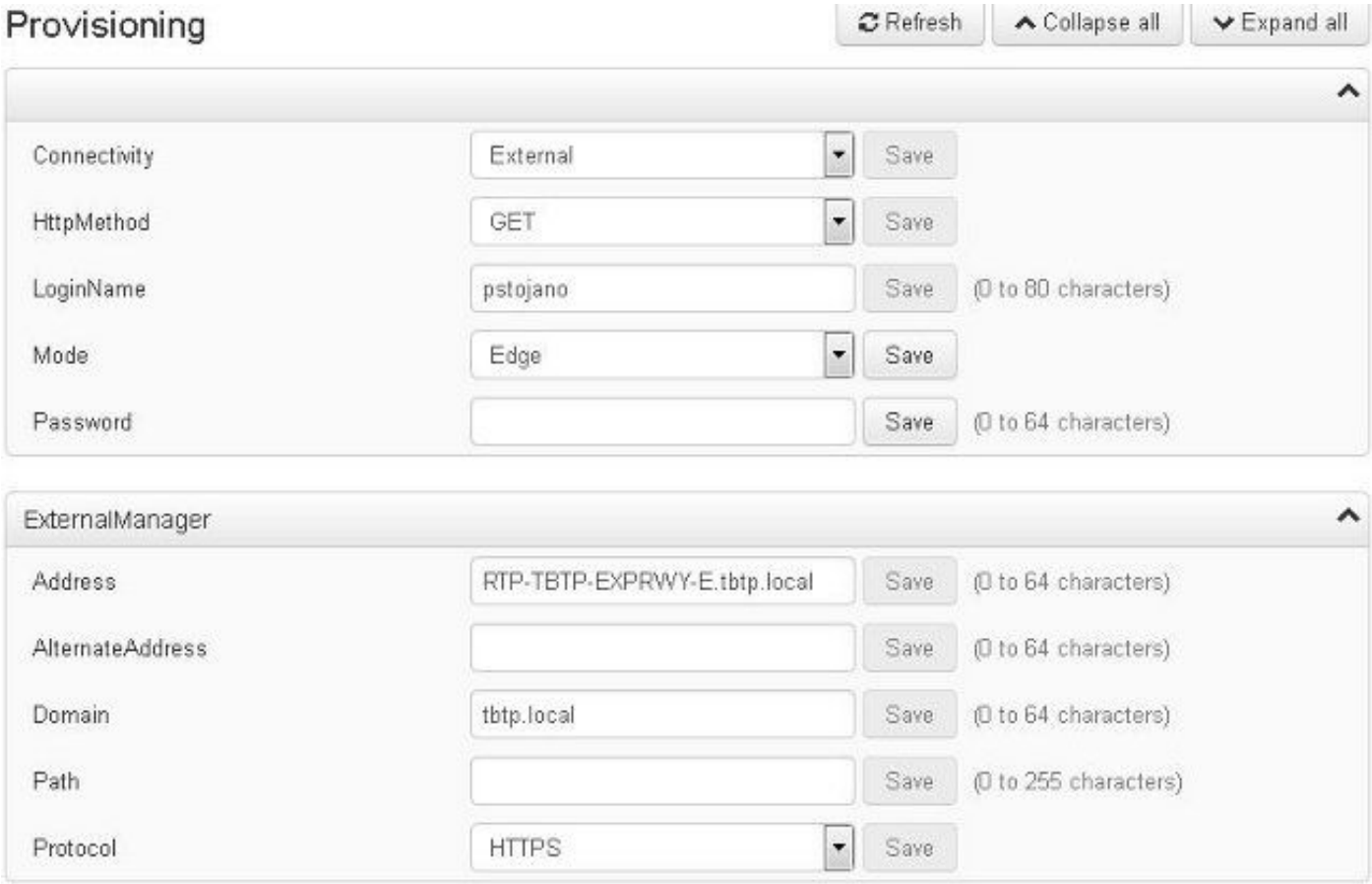


Note:被事先装配的CAs页包含一方便“配置当前设置”把您带直接地对在下个部分的注释的必需的配置第2步的按钮。

步骤7.设置边缘设置的基于TC的终端

- 在基于TC的终端，请选择**Configuration>网络**并且保证这些字段适当地填写在DNS部分下：
  域名
  服务器地址

- 在基于TC的终端，请选择**设置的Configuration>**并且保证这些字段适当地被填装在：
  LoginName -如对CUCM定义
  模式-**边缘**
  密码-如对CUCM定义
  外部管理器
  地址-您的ExpresswayE/VCS E主机名
  域-域您的collab边缘记录存在的地方

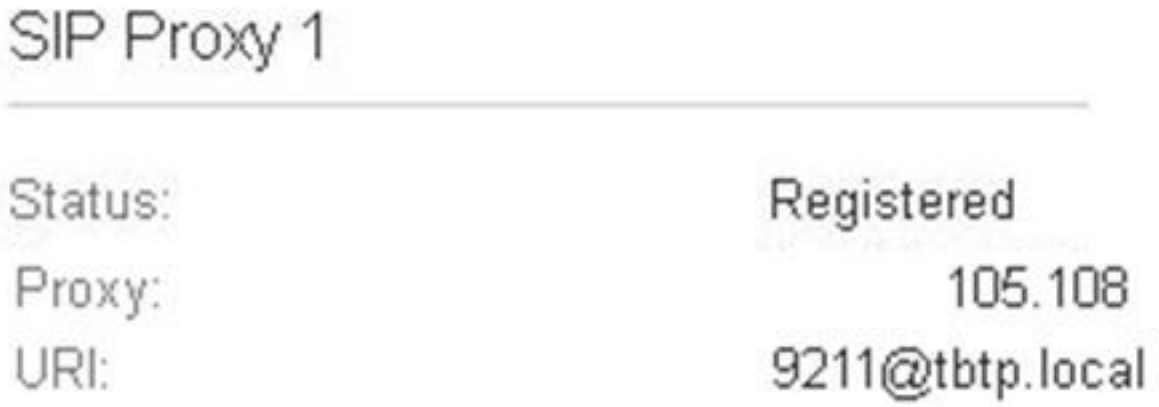


Verify

Use this section to confirm that your configuration works properly.

基于TC的终端

1. 在Web GUI中，请连接对“家”。寻找“注册的”状态的‘SIP代理1"部分。代理地址是您的ExpresswayE/VCS E。



2. 从CLI，请输入**xstatus //prov**。如果注册，您应该看到设置状态的“设置”。

```
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

在CUCM，请选择**Device > Phone**。请通过列表移动或过滤根据您的终端的列表。您应该看到“向%CUCM_IP%”消息登记。在此右边的IP地址应该是代理注册的您的ExpresswayC/VCS C。

Expressway-C

- 在ExpresswayC/VCS C，请选择**状态>统一的通信>视图设置会话。**
- 由您基于TC的终端的IP地址过滤。一次设置的会话的示例在镜像显示：

Troubleshoot

本部分提供的信息可用于对配置进行故障排除。

注册问题可以由包括DNS，认证问题，配置的许多要素导致，等等。此部分包括全面列表什么您典型地会看到，如果如何遇到一个特定问题和对修正它。如果遇到问题的外部的什么已经描述了，请感到自由包括它。

工具

最初，请注意工具在您的处理。

TC终端

Web GUI

- all.log
- 开始延长的记录(请包括一个完整的信息包捕获)

CLI

这些命令是最有利为了排除故障在实时：

- 日志ctx HttpClient调试9
- 日志ctx PROV调试9
- 日志输出在<--通过控制台显示记录

有效方式再现问题将再按乒乓键设置模式从“边缘”对Off然后回到“边缘”在Web GUI内。您能也输入**xConfiguration设置模式：**in命令CLI。

高速公路

- 诊断记录
- Tcpdump

CUCM

- SDI/SDL跟踪

问题1 ：Collab边缘记录不是可视的并且/或者主机名不是可溶解的

正如你看到的get_edge_config发生故障由于名字转换。

TC终端日志

```
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/
```

修正

1. 验证collab边缘记录是否是存在并且返回正确的主机名-。
2. 验证在客户端配置的DNS服务器信息是否是正确的。

问题2 ：CA在基于TC的终端的委托的CA列表内不是存在

TC终端日志

```
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
```

修正

1. 验证第三方CA是否是列出的在终端的**安全> CAs**选项下。
2. 如果CA是列出的，请验证是正确的。

问题3 ：ExpresswayE没有在SAN内列出的UC域

TC终端日志

```
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'
```

ExpresswayE SAN

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

修正

1. 再生ExpresswayE CSR为了包括UC域。
2. 很可能，在TC终端**ExternalManager域**参数没有设置对什么UC域是。如果这是实际情形您必须匹配它。

问题4 ：在TC和密码供应的用户名设置配置文件是不正确的

TC终端日志

```
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/
```

ExpresswayC/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"
```

修正

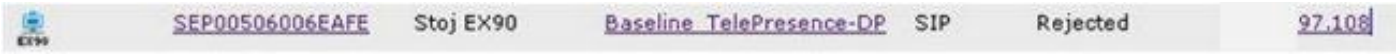
1. 验证用户名/密码被输入在TC终端的设置页下是有效的。
2. 验证证件CUCM数据库。
3. 版本10 -请使用自已关心门户
4. 版本9 -请使用CM用户选项

两个门户的URL是相同的：**https://%CUCM%/ucmuser/**

如果提交与一个不足的权利错误，请保证这些角色分配到用户：

- 被启用的标准的CTI
- 标准的CCM终端用户

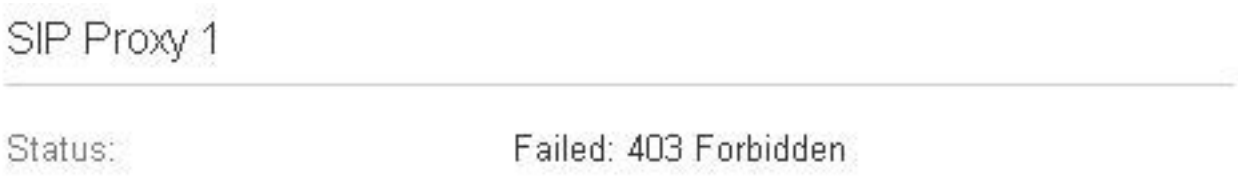
问题5 ：基于TC的终端注册被拒绝



CUCM跟踪

```
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终端



实际ExpresswayC/VCS C

```
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,
```

在此特定日志示例中很清楚ExpresswayC/VCS C在SAN不包含电话安全配置文件FQDN。(Secure-EX90.tbtp.local)。在传输层安全(TLS)握手， CUCM检查Expressway C/VCS C的服务器证明。因为它没在SAN内找到它投掷粗体的错误并且报道期待电话安全配置文件以FQDN格式。

修正

1. 验证ExpresswayC/VCS C在SAN的FQDN格式包含电话安全配置文件它内是服务器证明。
2. 验证设备在CUCM使用正确的安全配置文件，如果在FQDN格式使用一个安全的配置文件。
3. 这能由Cisco Bug ID CSCuq86376也造成。如果这是案件检查ExpresswayC/VCS C SAN大小和电话安全配置文件的位置在SAN内的。

问题6 ：基于TC的终端设置发生故障-没有UDS服务器

此errror一定是存在**诊断下>排除故障**：

```
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终端日志

移动在右边发现在粗体的错误

```
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/><userUdsServer><
server><address></address><tlsPort>8443</tlsPort></server></userUdsServer></edgeConfig></getEdge
ConfigResponse>
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!
```

修正

1. 保证那里是与终端用户帐户产生关联的服务档案和CTI UC服务用于通过MRA服务请求终端设置。

2. 连接对**CUCM admin >用户管理>用户设置> UC服务**并且创建CTI UC服务该点对IP CUCM (即MRA_UC-Service)。

3. 连接对**CUCM admin >用户管理>用户设置>服务档案**并且创建新配置文件(即MRA_ServiceProfile)。

4. 在新的服务档案，请移动到底部和在CTI配置文件部分，选择您创建的新的CTI UC服务(即MRA_UC-Service)，然后点击“Save”。

5. 连接对**CUCM admin >用户管理>终端用户**并且查找用户帐户用于通过MRA服务请求终端设置。

6. 在该用户下**服务设置**，请保证家庭簇是检查和UC服务档案反射您创建的新的服务档案(即MRA_ServiceProfile)，然后点击“Save”。

7. 它可能花费几分钟复制。几分钟后设法禁用在终端的设置模式和启用它在发现终端是否现在注册。

Related Information

- 移动&远程访问指南
- VCS认证创建指南
- EX90/EX60入门指南
- CUCM 9.1管理员指南
- Technical Support & Documentation - Cisco Systems