基于Collaboration Edge TC的终端配置示例

目录

简介

本文档介绍通过移动和远程访问解决方案配置基于网真编解码器(TC)的终端注册并对其进行故障排除所需的内容。

先决条件

要求

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或更高版本
- 思科统一通信管理器(CUCM)9.1.2版或更高版本
- 基于TC的终端
- CE8.x需要加密选项密钥才能启用“边缘”作为调配选项

使用的组件

本文档中的信息基于以下软件和硬件版本：

- VCS X8.1.1或更高版本
- CUCM版本9.1(2)SU1或更高版本以及IM & Presence 9.1(1)或更高版本
- TC 7.1或更高版本固**件（建议使用TC7.2）**
- VCS Control和Expressway/Expressway核心和边缘
- CUCM
- TC终端

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

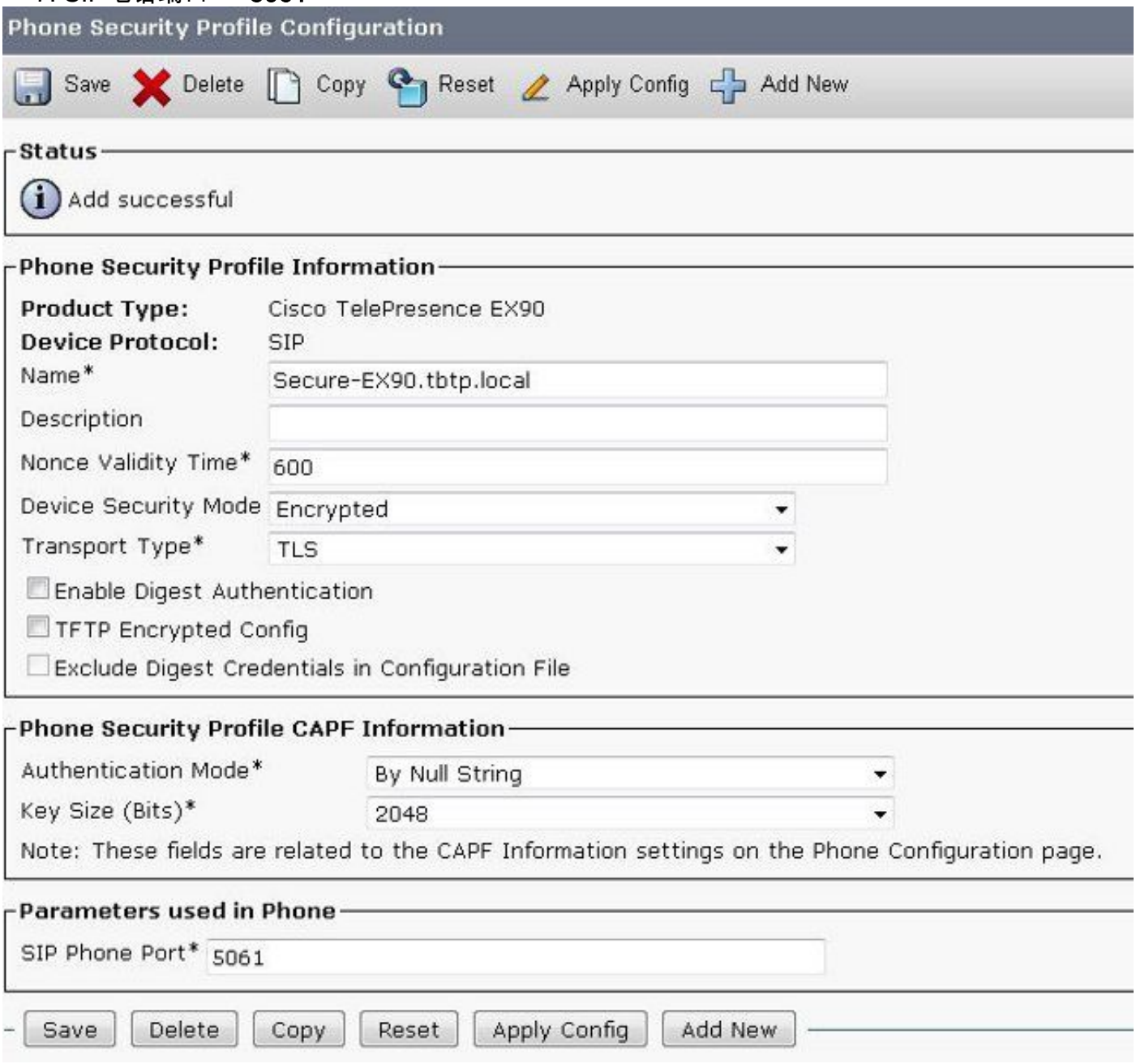
配置

这些配置步骤假设管理员将配置基于TC的终端以进行安全设备注册。安全注**册不**是要求，但整体移动和远程访问解决方案指南给人的印象是，它是因为有来自配置的屏幕截图显示CUCM上的安全设备配置文件。

步骤1.在CUCM上以FQDN格式（可选）创建安全电话配置文件。

1. 在CUCM中，选择**System > Security > Phone Security Profile**。
2. 单击新增。
3. 选择基于TC的终端类型并配置以下参数：
4. 名称 — **Secure-EX90.tbtp.local（需要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



步骤2.确保集群安全模式为(1) — 混合（可选）。

1. 在CUCM中，选择System > Enterprise Parameters。
2. 向下滚动到Security Parameters > Cluster Security Mode > 1。

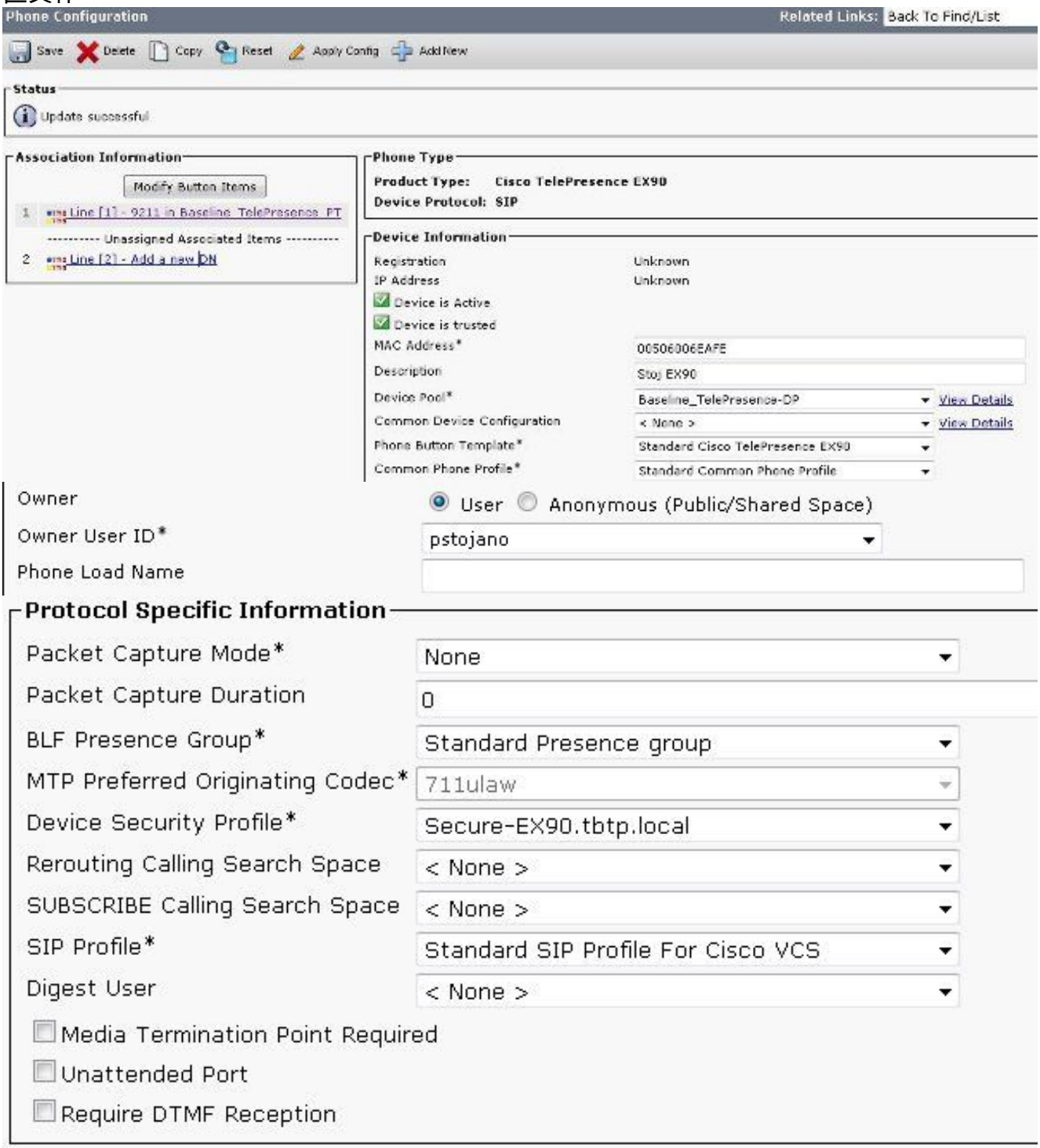
如果值不是1，则CUCM未受保护。如果出现这种情况，管理员需要查看这两个文档之一，以保护CUCM。

CUCM 9.1(2)安全指南

CUCM 10安全指南

步骤3.在CUCM中为基于TC的终端创建配置文件。

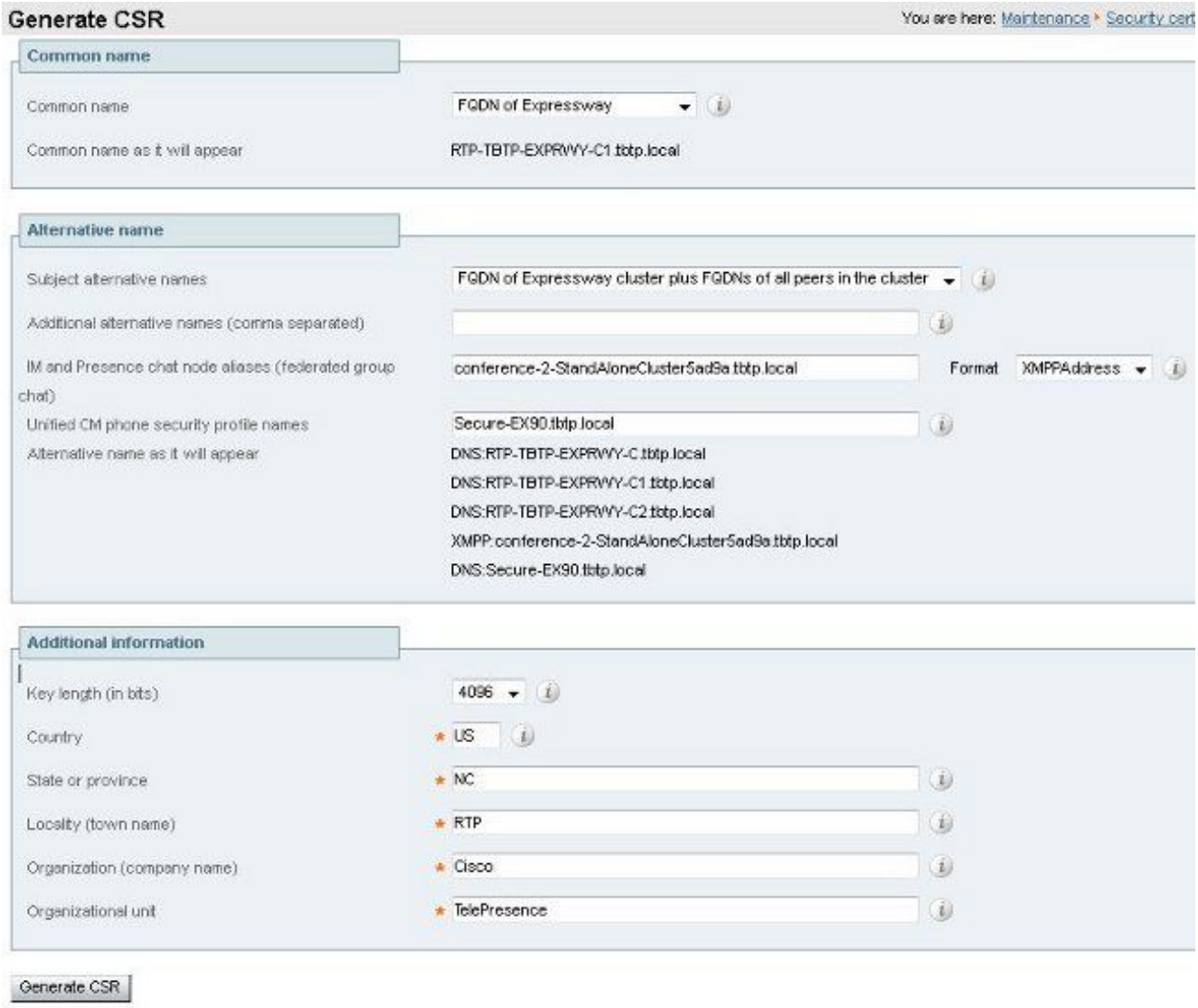
1. 在CUCM中，选择**Device > Phone**。
2. 单击新增。
3. 选择基于TC的终端类型并配置以下参数： MAC地址 — 来自基于TC的设备的MAC地址必填字段(*)所有者 — 用户所有者用户ID — 与设备关联的所有者设备安全配置文件 — 之前配置的配置文件(Secure-EX90.tbtp.local)SIP配置文件 — 标准SIP配置文件或之前创建的任何自定义配置文件



步骤4.将安全配置文件名称添加到Expressway-C/VCS-C证书的SAN（可选）。

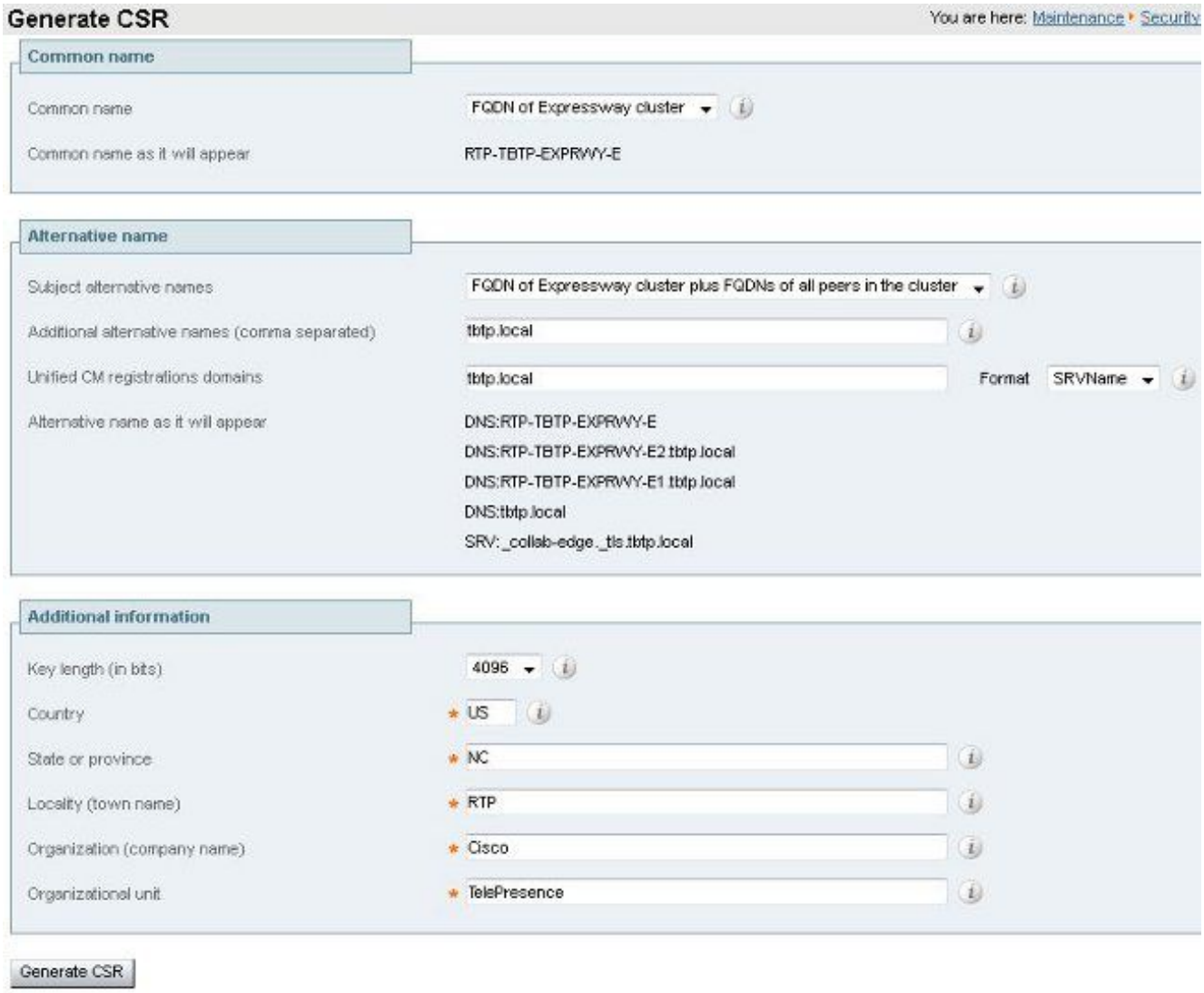
1. 在Expressway-C/VCS-C中，导航至**Maintenance > Security Certificates > Server Certificate**。

2. 点击**生成 CSR**。
3. 填写证书签名请求(CSR)字段，并确保**Unified CM电话安全配置**文件名称具有完全限定域名(FQDN)格式列出的确切电话安全配置文件。例如，**Secure-EX90.tbtp.local**。 **注意**：Unified CM电话安全配置文件名称列在“主题备用名称(SAN)”字段的背面。
4. 将CSR发送到要签名的内部或第三方证书颁发机构(CA)。
5. 选择**Maintenance > Security Certificates > Server Certificate**以将证书上传到Expressway-C/VCS-C。



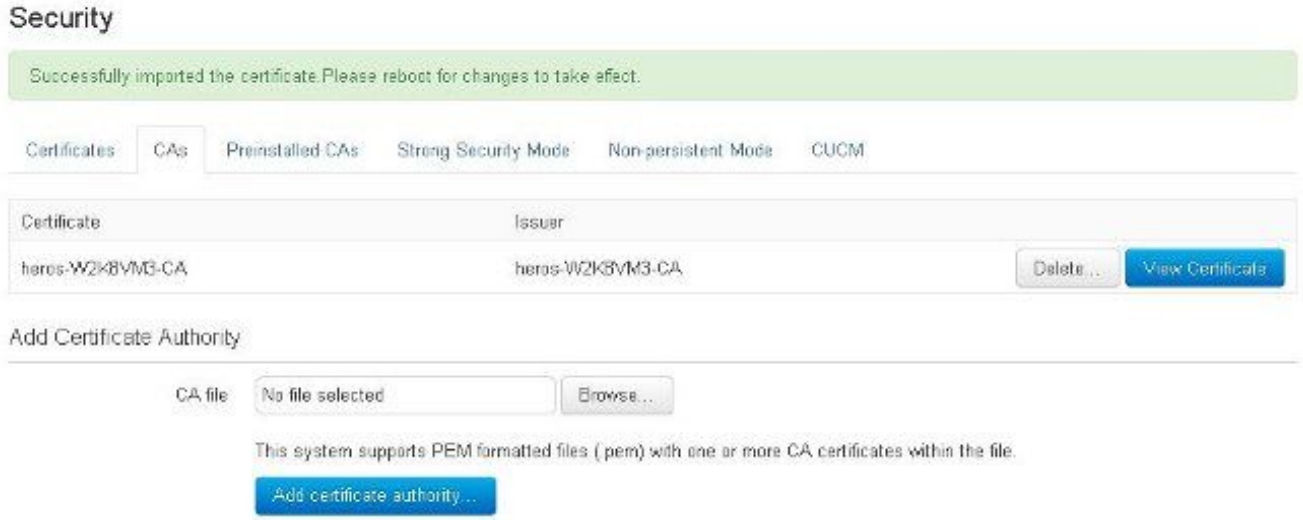
步骤5.将UC域添加到Expressway-E/VCS-E证书。

1. 在Expressway-E/VCS-E中，选择**Maintenance > Security Certificates > Server Certificate**。
2. 点击**生成 CSR**。
3. 填写CSR字段，并确保“Unified CM注册域”包含基于TC的终端以域名服务器(DNS)或服务名(SRV)格式向协作边缘（协作边缘）请求的域。
4. 将CSR发送到要签名的内部或第三方CA。
5. 选择**Maintenance > Security Certificates > Server Certificate**以将证书上传到Expressway-E/VCS-E。

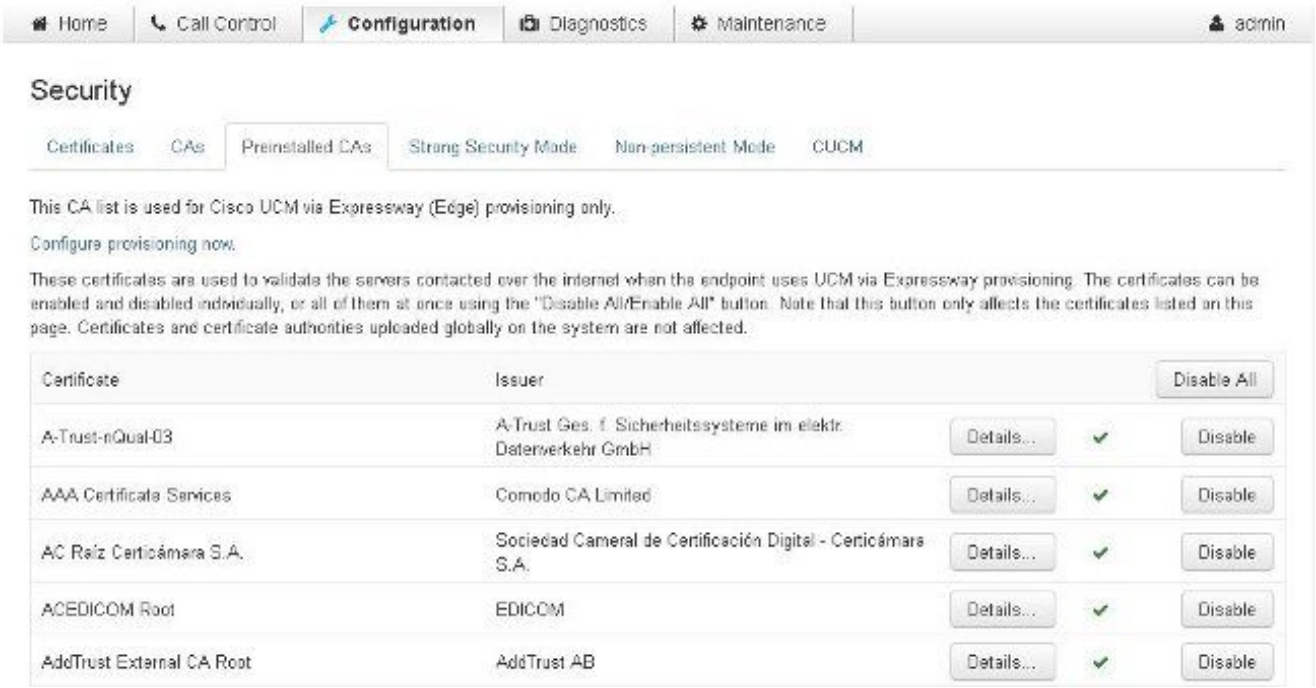


步骤6.将适当的受信任CA证书安装到基于TC的终端。

1. 在基于TC的终端中，选择**Configuration > Security**。
2. 选择**CA**选项卡，并浏览到签署Expressway-E/VCS-E证书的CA证书。
3. 单击“**Add certificate authority(添加证书颁发机**构)”。 **注意：**成功添加证书后，您将看到证书列表中列出该证书。



注意：TC 7.2包含预安装的CA列表。如果签署Expressway E证书的CA包含在此列表中，则不需要此部分列出的步骤。

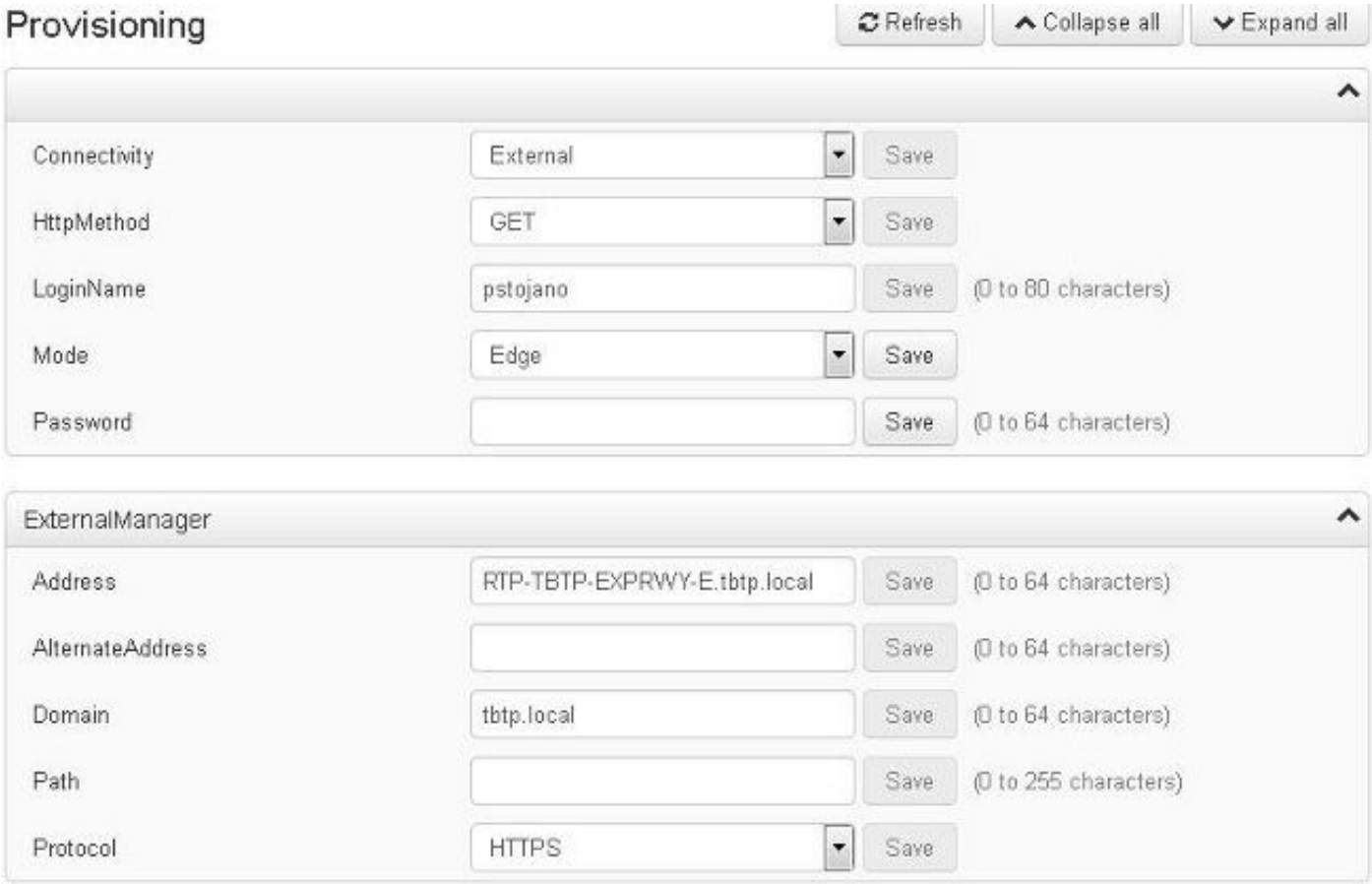


注意：预安装的CA页面包含一个方便的“立即配置调配”按钮，该按钮将您直接转到下一节步骤2中记录的所需配置。

步骤7.为边缘调配设置基于TC的终端

- 在基于TC的终端中，选择**Configuration > Network**并确保在DNS部分下正确填写以下字段：
  域名
  服务器地址

- 在基于TC的终端中，选择**Configuration > Provisioning**，并确保这些字段已正确填写：
  LoginName — 在CUCM中定义
  模式 — **边缘**
  密码 — 在CUCM中定义
  外部管理器
  地址 — Expressway-E/VCS-E的主机名
  域 — 存在协作边缘记录的域



验证

使用本部分可确认配置能否正常运行。

基于TC的终端

1. 在Web GUI中，导航至“主页”。 查找“已注册”状态的“SIP代理1”部分。代理地址是您的Expressway-E/VCS-E。

2. 在CLI中，输入**xstatus //prov**。如果已注册，您应看到“已调配”的调配状态。

```
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中，选择**Device > Phone**。滚动列表或根据终端过滤列表。您应看到“已注册%CUCM_IP%”消息。右侧的IP地址应是代理注册的Expressway-C/VCS-C。

Expressway-C

- 在Expressway-C/VCS-C中，选择**Status > Unified Communications > View Provisioning sessions。**
- 按基于TC的终端的IP地址过滤。已调配会话的示例如图所示：

故障排除

本部分提供的信息可用于对配置进行故障排除。

注册问题可能由许多因素引起，包括DNS、证书问题、配置等。本节包含一个全面的列表，列出在遇到给定问题时通常会看到的情况，以及如何补救。如果您在已记录的内容之外遇到问题，请随时加入。

工具

首先，要了解您可以使用的工具。

TC终端

Web GUI

- all.log
- 开始扩展日志记录（包括完整数据包捕获）

CLI

以下命令对实时故障排除最有益：

- log ctx HttpClient debug 9
- log ctx PROV debug 9
- log on < — 显示通过控制台记录

重新创建问题的有效方法是在Web GUI中将调配模式从“边缘”切换到“关闭”，然后返回“边缘”。您还可以进入**xConfiguration Provisioning Mode:**命令。

Expressways

- 诊断日志
- TCPDump

CUCM

- SDI/SDL跟踪

问题 1:协作边缘记录不可见和/或主机名不可解析

如您所见，get_edge_config由于名称解析而失败。

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/
```

补救

1. 验证协作边缘记录是否存在并返回正确的主机名。
2. 验证客户端上配置的DNS服务器信息是否正确。

问题 2:CA不存在于基于TC的终端上的受信任CA列表中

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
```

补救

1. 验证第三方CA是否列在终端的“安全”>“CA”选项卡下。
2. 如果列出了CA，请验证其是否正确。

问题 3:Expressway-E在SAN中未列出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'
```

Expressway-E SAN

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

补救

1. 重新生成Expressway-E CSR以包括UC域。
2. 在TC终端上，ExternalManager域参**数可**能未设置为UC域。如果是这种情况，您必须匹配。

问题 4:TC调配配置文件中提供的用户名和密码不正确

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/
```

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"
```

补救

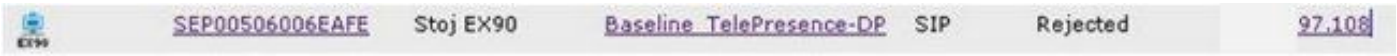
1. 验证在TC终端的Provisioning（调配）页面下输入的Username/Password（用户名/密码）有效。
2. 根据CUCM数据库验证凭证。
3. 版本10 — 使用自助服务门户
4. 版本9 — 使用CM用户选项

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

如果显示权限不足错误，请确保将这些角色分配给用户：

- Standard CTI Enabled
- 标准CCM最终用户

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Expressway-C/VCS-C

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

在此特定日志示例中，很明显Expressway-C/VCS-C在SAN中不包含电话安全配置文件FQDN。

(Secure-EX90.tbtp.local)。 在传输层安全(TLS)握手中，CUCM检查Expressway-C/VCS-C的服务器证书。由于它在SAN中未找到它，因此会抛出错误粗体，并报告它期望使用FQDN格式的电话安全配置文件。

补救

1. 验证Expressway-C/VCS-C是否在其服务器证书的SAN中包含FQDN格式的电话安全配置文件。
2. 如果您使用FQDN格式的安全配置文件，请验证设备在CUCM中使用了正确的安全配置文件。
3. 这也可能是由Cisco Bug ID CSCuq86376引起的。如果是这种情况，请检查Expressway-C/VCS-C SAN大小和电话安全配置文件在SAN中的位置。

问题 6:基于TC的终端调配失败 — 无UDS服务器

在诊断>故障排除**下必**须出**现此错**误：

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

TC终端日志

滚动到右侧以粗体显示错误

```
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/>



        </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!
```

补救

1.确保有与最终用户帐户关联的服务配置文件和CTI UC服务，用于通过MRA服务请求终端调配。

2.导航到**CUCM管理> 用户管理> 用户设置> UC服务**，并创建指向CUCM IP的CTI UC服务（即MRA_UC-Service）。

3.导航至**CUCM admin > User Management > User Settings > Service Profile** 并创建新配置文件

（即MRA_ServiceProfile）。

4.在新服务配置文件中，滚动到底部，在CTI配置文件部分，选择您刚创建的新CTI UC服务（即MRA_UC-Service），然后点击保存。

5.导航至**CUCM管理员> User Management > End User**，并查找用于通过MRA服务请求终端调配的用户帐户。

6.在该用户的**服务设置**下，确保“主集群”已选中，并且UC服务配置文件反映您创建的新服务配置文件（即MRA_ServiceProfile），然后点击保存。

7.复制可能需要几分钟。尝试在终端上禁用调配模式，并在几分钟后将其重新打开，以查看终端现在是否注册。

相关信息

- 移动和远程访问指南
- VCS证书创建指南
- EX90/EX60入门指南
- CUCM 9.1管理员指南
- 技术支持和文档 - Cisco Systems