A borda da Colaboração TC-baseou o exemplo de configuração dos valores-limite

Índice

Introdução

O documento descreve o que é exigido configurar e pesquisar defeitos o codec do TelePresence (TC) - registro de ponto final baseado com o móbil e a solução de acesso remoto.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Móbil e solução de acesso remoto
- Certificados do server de comunicação de vídeo (VC)
- Via expressa X8.1.1 ou mais tarde
- Cisco unificou a liberação 9.1.2 do gerente de uma comunicação (CUCM) ou mais atrasado
- valores-limite TC-baseados
- CE8.x exige a chave da opção de criptografia permitir a “borda” como uma opção do abastecimento

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- VC X8.1.1 ou mais tarde
- Liberação CUCM 9.1(2)SU1 ou mais tarde e IM & presença 9.1(1) ou mais atrasado
- TC 7.1 ou firmware mais atrasado **(TC7.2 recomendado)**
- Os VC controlam & via expressa/núcleo da via expressa & afiam
- CUCM
- Valor-limite TC

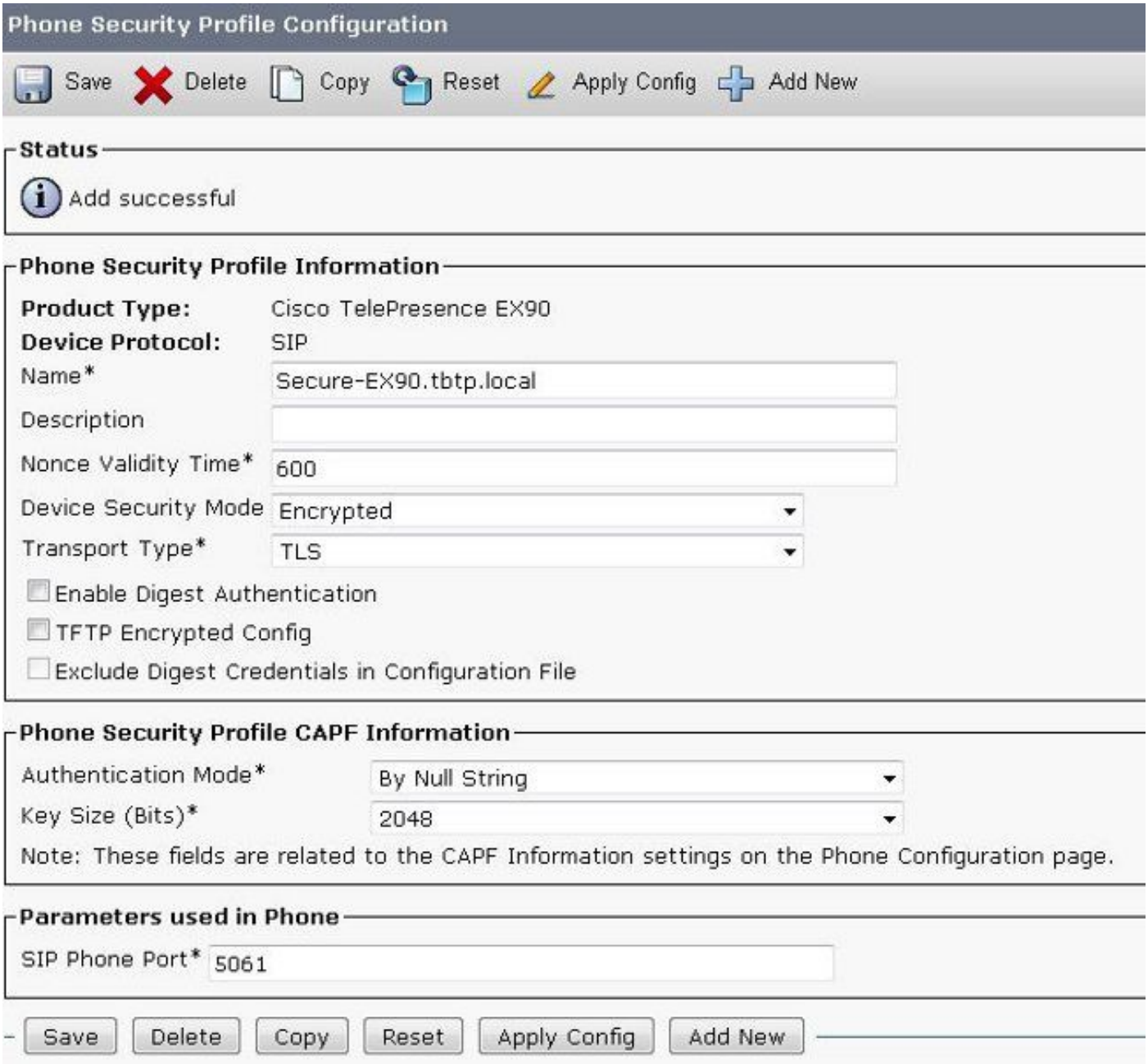
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Estas etapas de configuração supõem que o administrador configurará o valor-limite TC-baseado para fixa o registro do dispositivo. O registro seguro não é uma exigência, porém o guia total do móbil e da solução de acesso remoto dá a impressão que é desde que há os screen shots da configuração que mostram perfis de dispositivo seguros em CUCM.

Etapa 1. Crie um perfil seguro do telefone em CUCM no formato FQDN (opcional).

1. Em CUCM, selecione o **> segurança do sistema > o perfil de segurança do telefone**.
2. O clique **adiciona novo**.
3. Selecione o tipo TC-baseado do valor-limite e configurar estes parâmetros:
4. Nome - **Secure-EX90.tbtp.local (formato FQDN exigido)**
5. Modo da segurança do dispositivo - **Cifrado**
6. Tipo do transporte - **TLS**
7. Porta de telefone do SORVO - **5061**



Etapa 2. Assegure-se de que modo de segurança do conjunto seja (1) - Misturado (opcional).

1. Em CUCM, selecione o **sistema > parâmetros de empreendimento**.
2. Enrole para baixo **parâmetros de segurança > modo de segurança do conjunto > 1.**

Se o valor não é 1 o CUCM não esteve fixado. Se este é o caso, o administrador precisa de rever

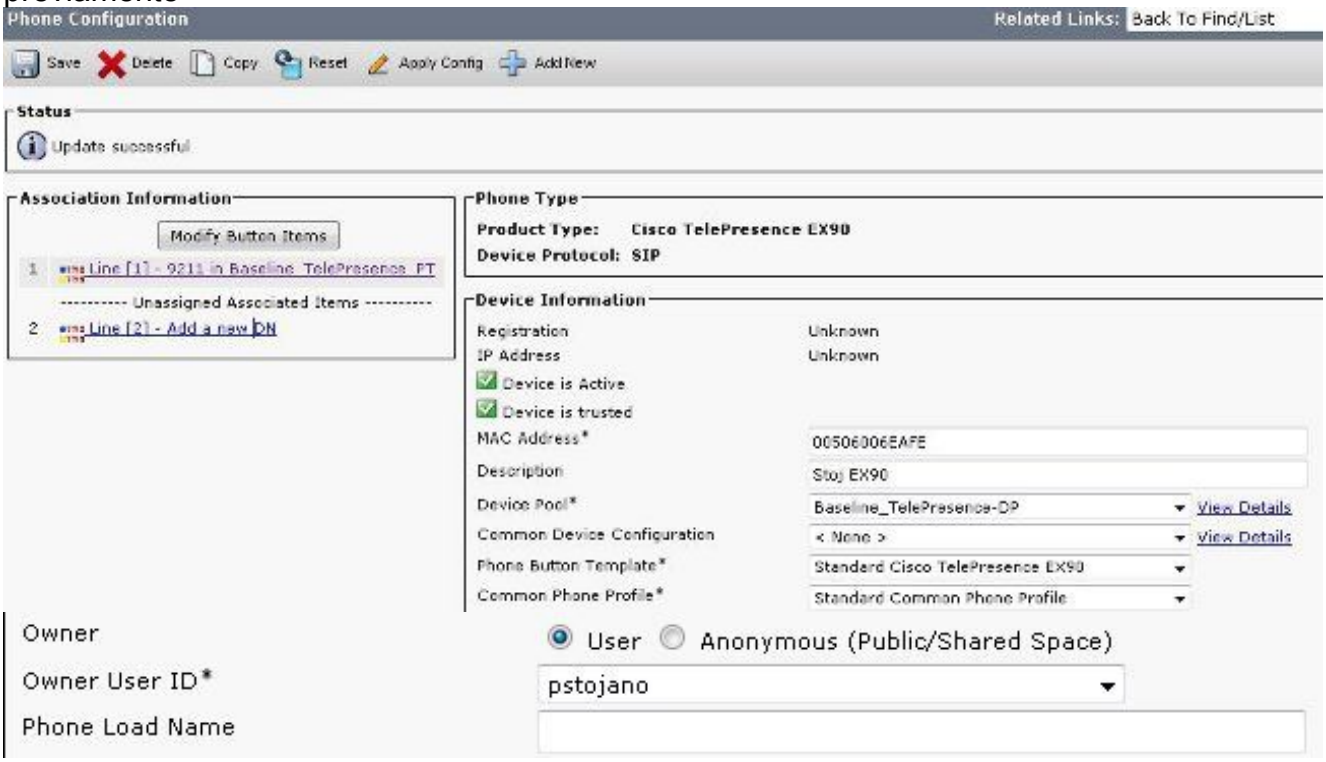
um destes dois documentos a fim fixar o CUCM.

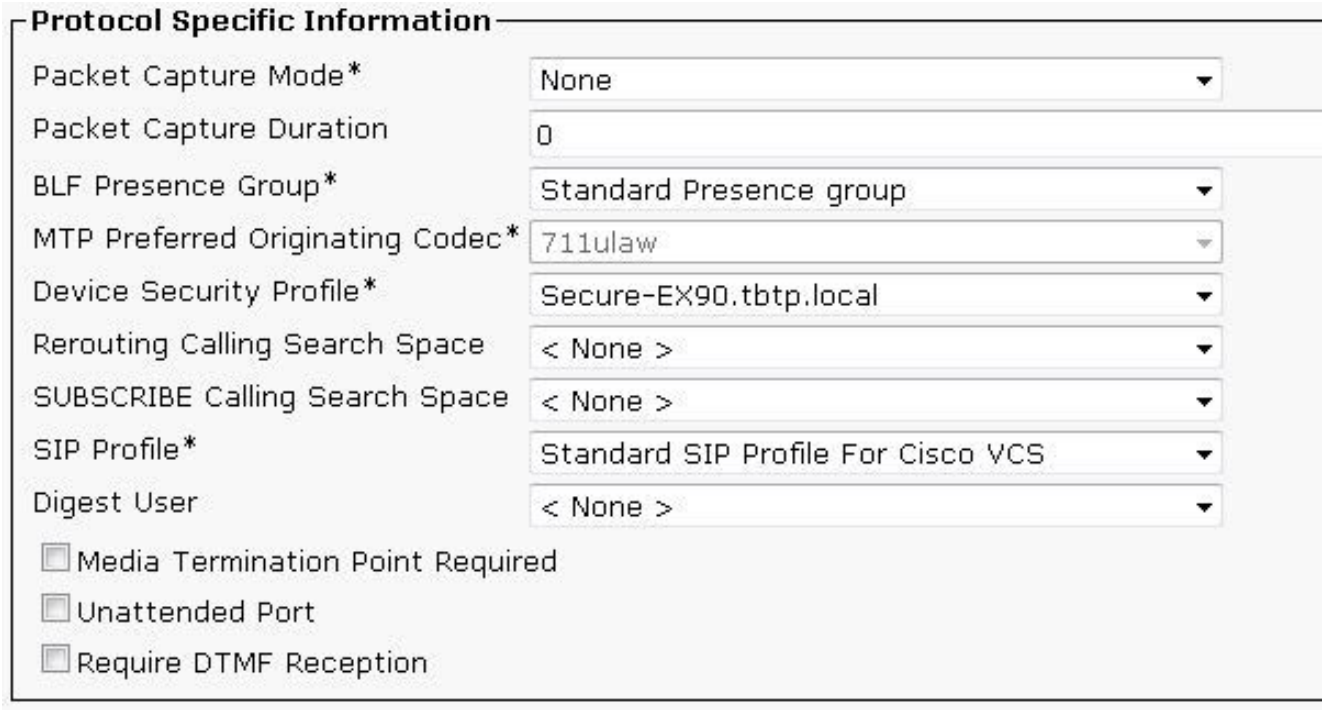
Guia da Segurança CUCM 9.1(2)

Guia da Segurança CUCM 10

Etapa 3. Crie um perfil em CUCM para o valor-limite TC-baseado.

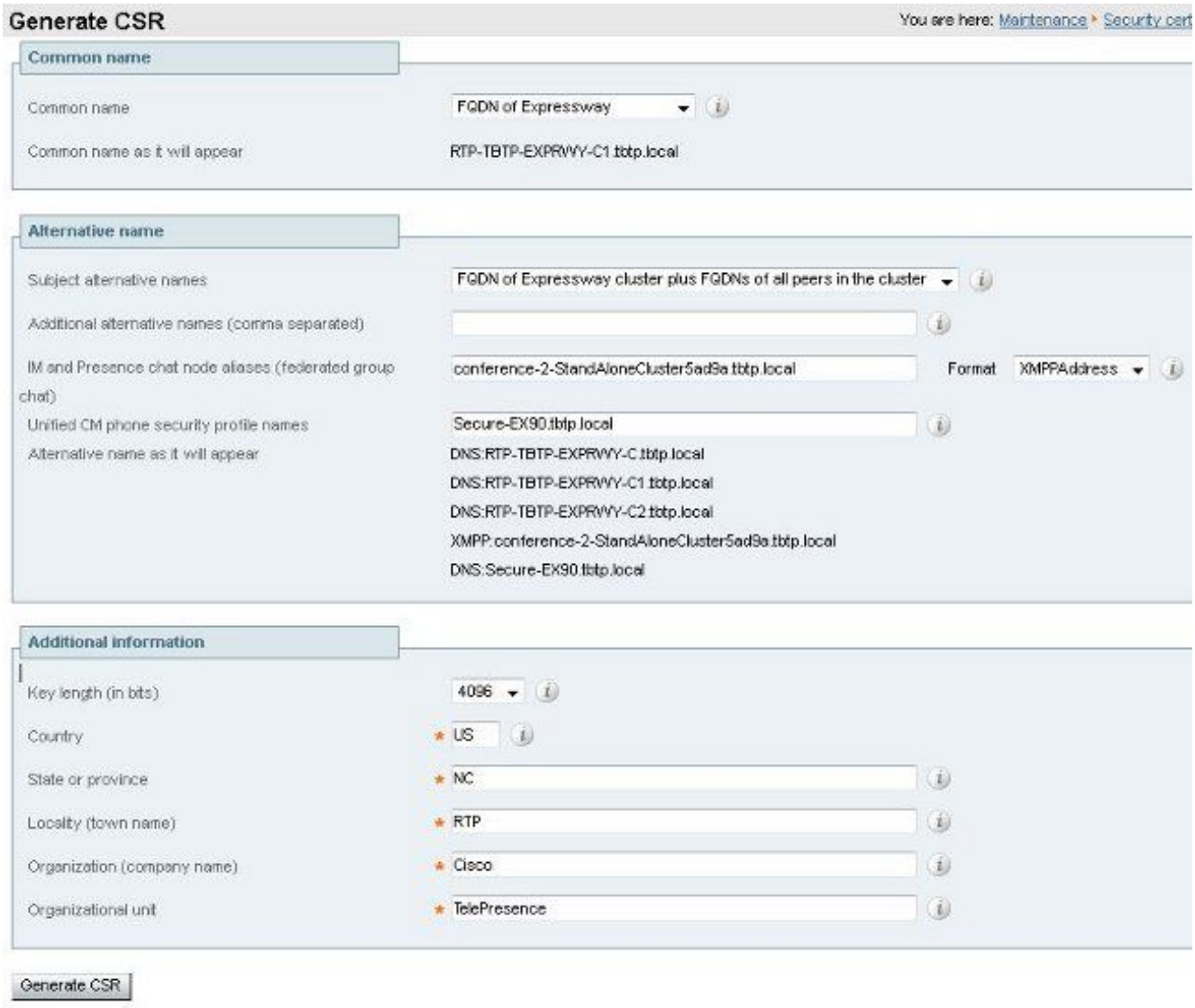
1. Em CUCM, selecione o **dispositivo > o telefone**.
2. O clique **adiciona novo**.
3. Selecione o tipo TC-baseado do valor-limite e configurar estes parâmetros: MAC address - MAC address do dispositivo TC-baseadoCampos starred exigidos (*)Proprietário - UsuárioUsuário do proprietário - identificação - proprietário associado com o dispositivoPerfil de segurança do dispositivo - Perfil previamente configurado (Secure-EX90.tbtp.local)Perfil do SORVO - Perfil padrão do SORVO ou algum perfil feito sob encomenda criado previamente





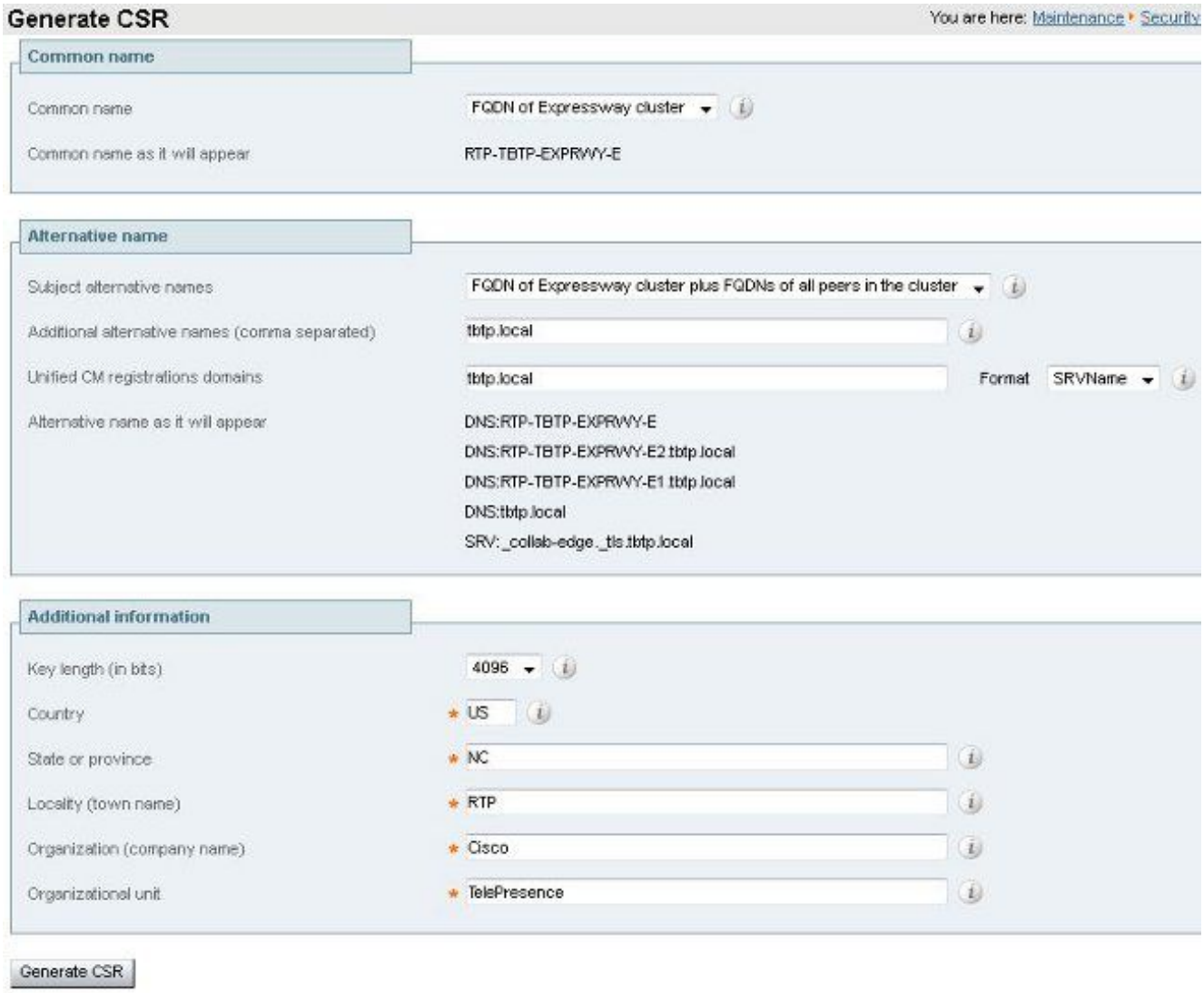
Etapa 4. Adicionar o nome do perfil de segurança ao SAN do certificado Expressway-C/VCS-C (opcional).

1. Em Expressway-C/VCS-C, navegue aos **Certificados > ao certificado de servidor do > segurança da manutenção**.
2. O clique **gerencie o CSR**.
3. Complete os campos da solicitação de assinatura de certificado (CSR) e assegure-se de que o **nome unificado do perfil de segurança do telefone CM** tenha o perfil de segurança exato do telefone alistado no formato do nome de domínio totalmente qualificado (FQDN). Por exemplo, **Secure-EX90.tbtp.local**. Nota: Os nomes unificados do perfil de segurança do telefone CM estão listados na parte traseira do campo sujeito do nome alternativo (SAN).
4. Envie o CSR fora a um Certificate Authority (CA) interno ou da 3ª parte a ser assinado.
5. Selecione **Certificados > certificado de servidor do > segurança da manutenção** a fim transferir arquivos pela rede o certificado ao Expressway-C/VCS-C.



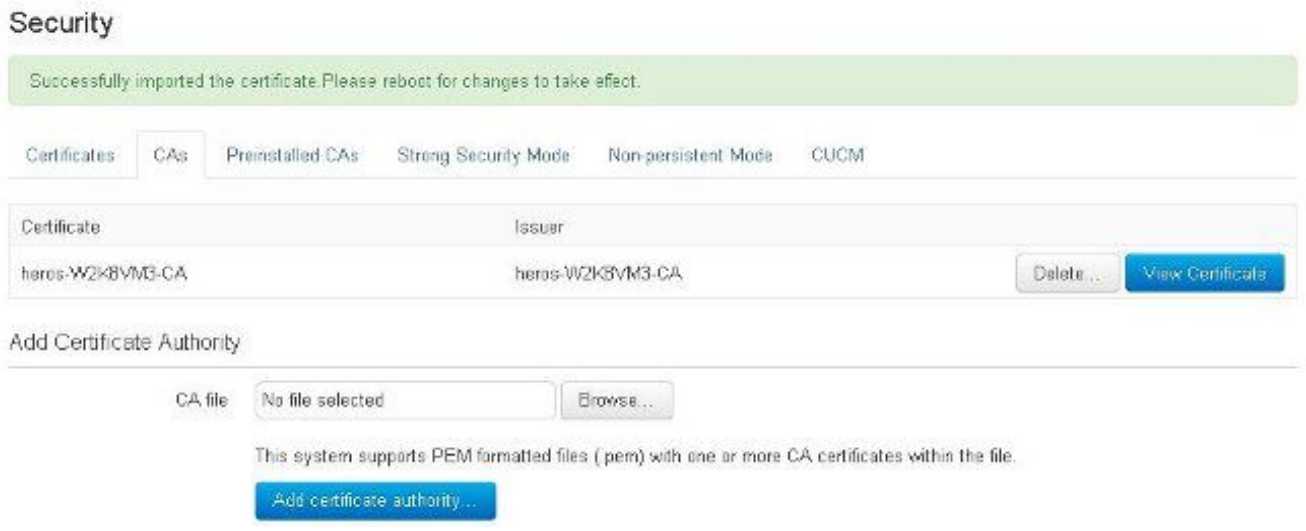
Etapa 5. Adicionar o domínio UC ao certificado Expressway-E/VCS-E.

1. Em Expressway-E/VCS-E, selecione **Certificados > certificado de servidor do > segurança da manutenção**.
2. O clique **gerencie o CSR**.
3. Complete os campos CSR e assegure-se de que “os domínios unificados dos registros CM” contenham o domínio que o valor-limite TC-baseado fará pedidos da borda da Colaboração (collab-borda) a, no Domain Name Server (DNS) ou em formatos do nome do serviço (SRV).
4. Envie o CSR fora a um interno ou à 3ª parte CA a ser assinado.
5. Selecione **Certificados > certificado de servidor do > segurança da manutenção** a fim transferir arquivos pela rede o certificado ao Expressway-E/VCS-E.

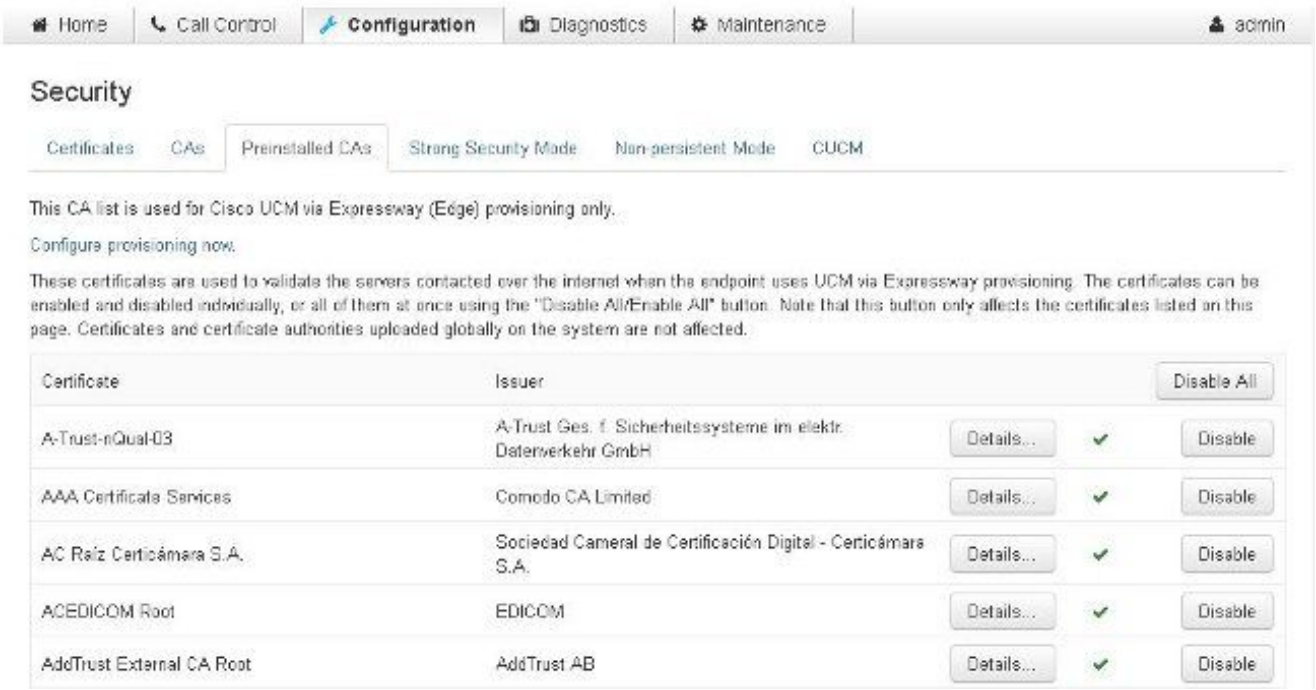


Etapa 6. Instale o certificado de CA confiado apropriado ao valor-limite TC-baseado.

1. No valor-limite TC-baseado, selecione o **> segurança da configuração**.
2. Selecione a aba de **CA** e consulte para o certificado de CA que assinou seu certificado Expressway-E/VCS-E.
3. O clique **adiciona o Certificate Authority**. Nota: Uma vez que o certificado é adicionado com sucesso você verá que alistou na lista do certificado.



Nota: O TC 7.2 contém uma lista instalada CA. Se CA que assinou o certificado da via expressa-e é contido dentro desta lista, as etapas alistadas nesta seção não estão exigidas.

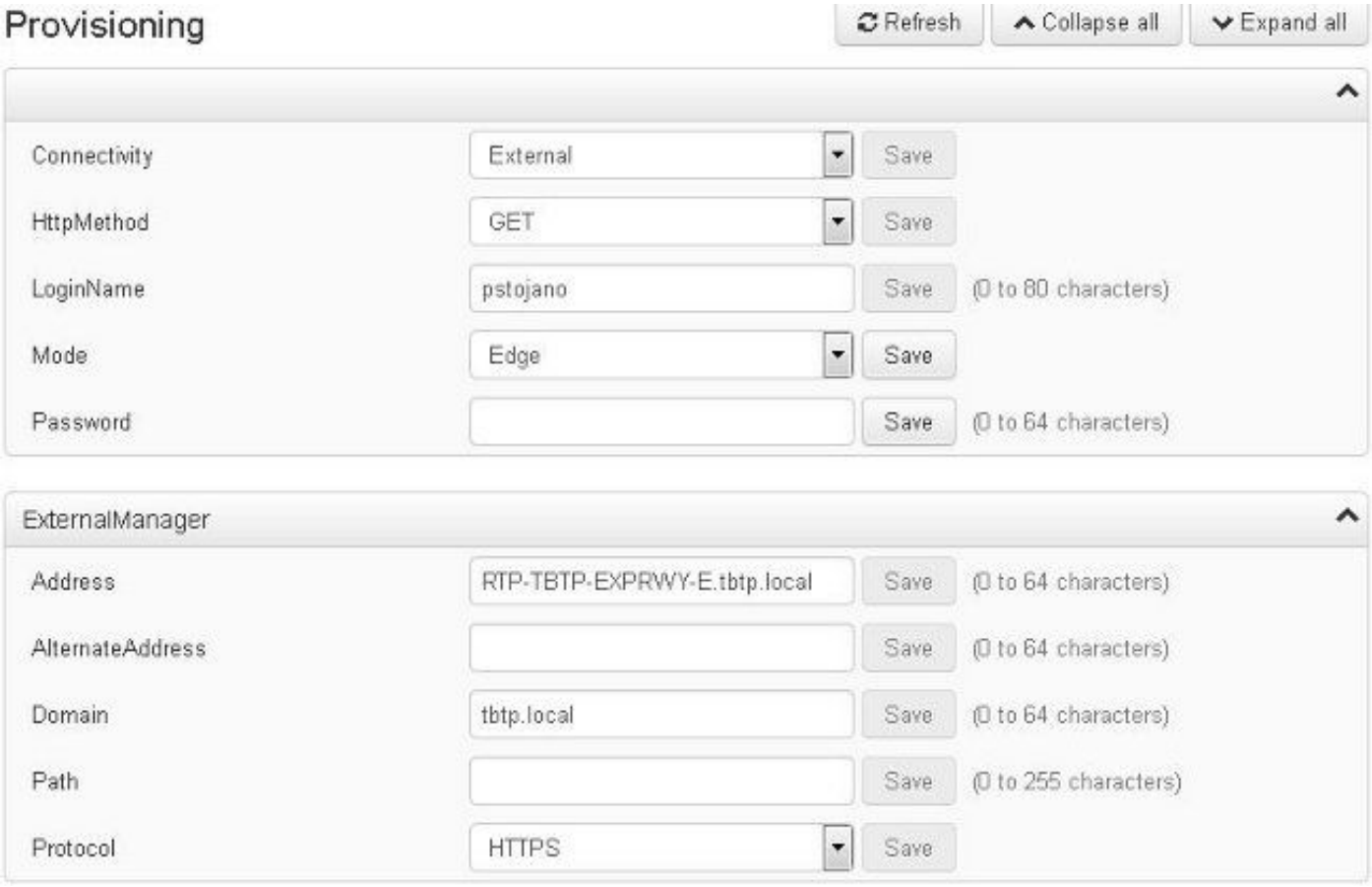


Nota: A página instalada CA contém um conveniente “configura o abastecimento agora” abotoa-se que o toma diretamente à configuração requerida notável em etapa 2 na próxima seção.

Etapa 7. Estabelecer um valor-limite TC-baseado para o abastecimento da borda

- No valor-limite TC-baseado, a **configuração > a rede** seletas e asseguram-se de que estes campos estejam preenchidos corretamente sob a seção DNS:
  Nome de domínio
  Endereço do servidor

- No valor-limite TC-baseado, a **configuração > o abastecimento** seletos e asseguram-se de que estes campos estejam enchidos corretamente em:
  LoginName - como definido em CUCM
  Modo - **Borda**
  Senha - como definido em CUCM
  Gerenciador externo
  Endereço - Hostname de seu Expressway-E/VCS-E
  Domínio - Domínio onde seu registro da collab-borda esta presente



Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

valor-limite TC-baseado

1. Na Web GUI, navegue “home”. Procure 'a seção do proxy 1" do SORVO para um estado “registrado”. O endereço de proxy é seu Expressway-E/VCS-E.

2. Do CLI, entre no **xstatus //prov**. Se você é registrado, você deve ver um estado do abastecimento de “fornecida”. **`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

Em CUCM, selecione o **dispositivo > o telefone**. Ou o rolo através da lista ou filtra a lista baseada em seu valor-limite. Você deve ver “registrado com uma mensagem de %CUCM_IP%”. O endereço IP de Um ou Mais Servidores Cisco ICM NT à direita deste deve ser seu Expressway-C/VCS-C que proxys o registro.

Via expressa-C

- Em Expressway-C/VCS-C, selecione o **estado > as comunicações unificadas > as sessões do abastecimento da vista.**
- Filtre pelo endereço IP de Um ou Mais Servidores Cisco ICM NT de seu valor-limite TC-baseado. Um exemplo de uma sessão fornecida é mostrado na imagem:

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

As edições do registro podem ser causadas pelos fatores numerosos que incluem o DNS, edições do certificado, configuração, e assim por diante. Esta seção inclui uma lista abrangente do que você veria tipicamente se você encontra um problema dado e de como ao remediate ele. Se você

é executado em edições fora do que tem sido documentado já, sinta livre inclui-lo.

Ferramentas

Para começar, esteja ciente das ferramentas em sua eliminação.

Valor-limite TC

Web GUI

- all.log
- Comece registro prolongado (inclua uma captação do pacote completo)

CLI

Estes comandos são os mais benéficos a fim pesquisar defeitos no tempo real:

- o ctx HttpClient do log debuga 9
- o ctx PROV do log debuga 9
- registro de saída em <-- Mostras que registram através do console

Uma maneira eficaz recrear o problema é firmar o modo do abastecimento da “borda” a "OFF" e então de volta à “borda” dentro da Web GUI. Você pode igualmente entrar no **modo do abastecimento do xConfiguration:** comando no CLI.

Vias expressas

- Log de diagnóstico
- Tcpdump

CUCM

- Traços SDI/SDL

Edição 1: o registro da Collab-borda não é visível e/ou o hostname não é solucionável

Como você pode ver, o get_edge_config falha devido à resolução de nome.

Logs do valor-limite 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/
```

Remediação

1. Verifique se o registro da collab-borda esta presente e retorna o hostname correto.

2. Verifique se a informação de servidor de DNS configurada no cliente está correta.

Edição 2: CA não está atual dentro da lista confiada de CA no valor-limite TC-baseado

Logs do valor-limite 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
```

Remediação

1. Verifique se uma 3ª parte CA está listada sob a aba da **Segurança > CA no** valor-limite.
2. Se CA está listado, verifique que está correto.

Edição 3: A via expressa-e não tem o domínio UC alistado dentro do SAN

Logs do valor-limite 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'
```

Via expressa-e SAN

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

Remediação

1. Via expressa-e regenerada CSR a fim incluir os domínios UC.
2. Épossível que no valor-limite TC o parâmetro do **domínio de ExternalManager** não está ajustado a qual o domínio UC é. Se este é o caso você deve combiná-lo.

Edição 4: O username e/ou a senha fornecidos no perfil do abastecimento TC estão incorretos

Logs do valor-limite 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"
```

Remediação

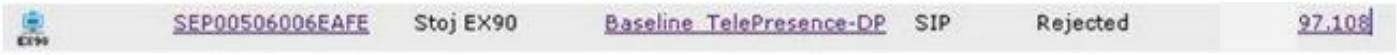
1. Verifique que o username/senha incorporada sob a página de abastecimento no valor-limite TC é válidos.
2. Verifique credenciais contra o base de dados CUCM.
3. Versão 10 - use o portal do cuidado do auto
4. Versão 9 - use as opções de usuário CM

A URL para ambos os portais é a mesma: **https://%CUCM%/ucmuser/**

Se apresentado com um insuficiente erro dos direitos, assegure-se de que estes papéis estejam atribuídos ao usuário:

- Padrão CTI permitido
- Utilizador final padrão CCM

Edição 5: O registro de ponto final TC-baseado obtém rejeitado



Traços 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,
```

Valor-limite TC

Expressway-C/VCS-C real

```
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,
```

Neste exemplo de registro específico é claro que o Expressway-C/VCS-C não contém o FQDN do perfil de segurança do telefone no SAN. (Secure-EX90.tbtp.local). No aperto de mão do Transport Layer Security (TLS), o CUCM inspeciona o certificado de servidor Expressway-C/VCS-C. Desde que não o encontra dentro do SAN joga o erro negrito e relata que esperou o perfil de segurança do telefone no formato FQDN.

Remediação

1. Verifique que o Expressway-C/VCS-C contém o perfil de segurança do telefone no formato FQDN dentro do SAN dele é certificado de servidor.
2. Verifique que o dispositivo usa o perfil de segurança correto em CUCM se você usa um perfil seguro no formato FQDN.
3. Isto podia igualmente ser causado pela identificação de bug Cisco CSCuq86376. Se esta é a verificação do caso o tamanho Expressway-C/VCS-C SAN e a posição do perfil de segurança do telefone dentro do SAN.

Edição 6: o abastecimento TC-baseado do valor-limite falha - Nenhum server UD

Esta obrigação do errror esta presente sob **diagnósticos > Troubleshooting**:

```
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,
```

Logs do valor-limite TC

Rolo à direita ver os erros em corajoso

```
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!
```

Remediação

1. Assegure-se de que haja um serviço do perfil e CTI UC do serviço associado com a conta do utilizador final usada para pedir o abastecimento do valor-limite através dos serviços MRA.

2. Navegue a **CUCM admin > gerenciamento de usuário > configurações de usuário > serviço UC** e crie um serviço CTI UC esses pontos ao IP de CUCM (isto é MRA_UC-Service).

3. Navegue a **CUCM admin > gerenciamento de usuário > configurações de usuário > perfil do serviço** e crie um perfil novo (isto é MRA_ServiceProfile).

4. No perfil novo do serviço, enrole a parte inferior e na seção do perfil CTI, selecionam o serviço que novo CTI UC você apenas criou (isto é MRA_UC-Service), a seguir clicam a salvaguarda.

5. Navegue a **CUCM admin > gerenciamento de usuário > utilizador final** e encontre a conta de usuário usada para pedir o abastecimento do valor-limite através dos serviços MRA.

6. Sob **ajustes do serviço d**esse usuário, assegure-se de que o conjunto home seja verificação e esse perfil do serviço UC reflita o perfil que novo do serviço você criou (isto é MRA_ServiceProfile), a seguir clique a salvaguarda.

7. Pode tomar alguns minutos para replicate. Tente desabilitar o modo do abastecimento no valor-limite e girá-lo para trás no poucos minutos depois para ver se o valor-limite se registra agora.

Informações Relacionadas

- Móbil & guia do Acesso remoto
- Guia da criação do certificado VC
- EX90/EX60 que obtém o guia começado
- Guia do administrador CUCM 9.1
- Suporte Técnico e Documentação - Cisco Systems