El borde de la Colaboración TC-basó el ejemplo de configuración de los puntos finales

Contenido

Introducción

El documento describe qué se requiere configurar y resolver problemas el codificador-decodificador del TelePresence (TC) - registro del punto final basado a través del móvil y de la solución de acceso remoto.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Móvil y solución de acceso remoto
- Certificados del servidor del comunicación mediante video (VCS)
- Autopista X8.1.1 o más adelante
- Cisco unificó la versión 9.1.2 del administrador de la comunicación (CUCM) o más adelante
- puntos finales TC-basados
- CE8.x requiere la clave de la opción de encripción habilitar el “borde” como opción del aprovisionamiento

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- VCS X8.1.1 o más adelante
- Versión CUCM 9.1(2)SU1 o más adelante e IM y presencia 9.1(1) o más adelante
- TC 7.1 o firmware posterior **(TC7.2 recomendado)**
- Control VCS y autopista/base y borde de la autopista
- CUCM
- Punto final TC

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

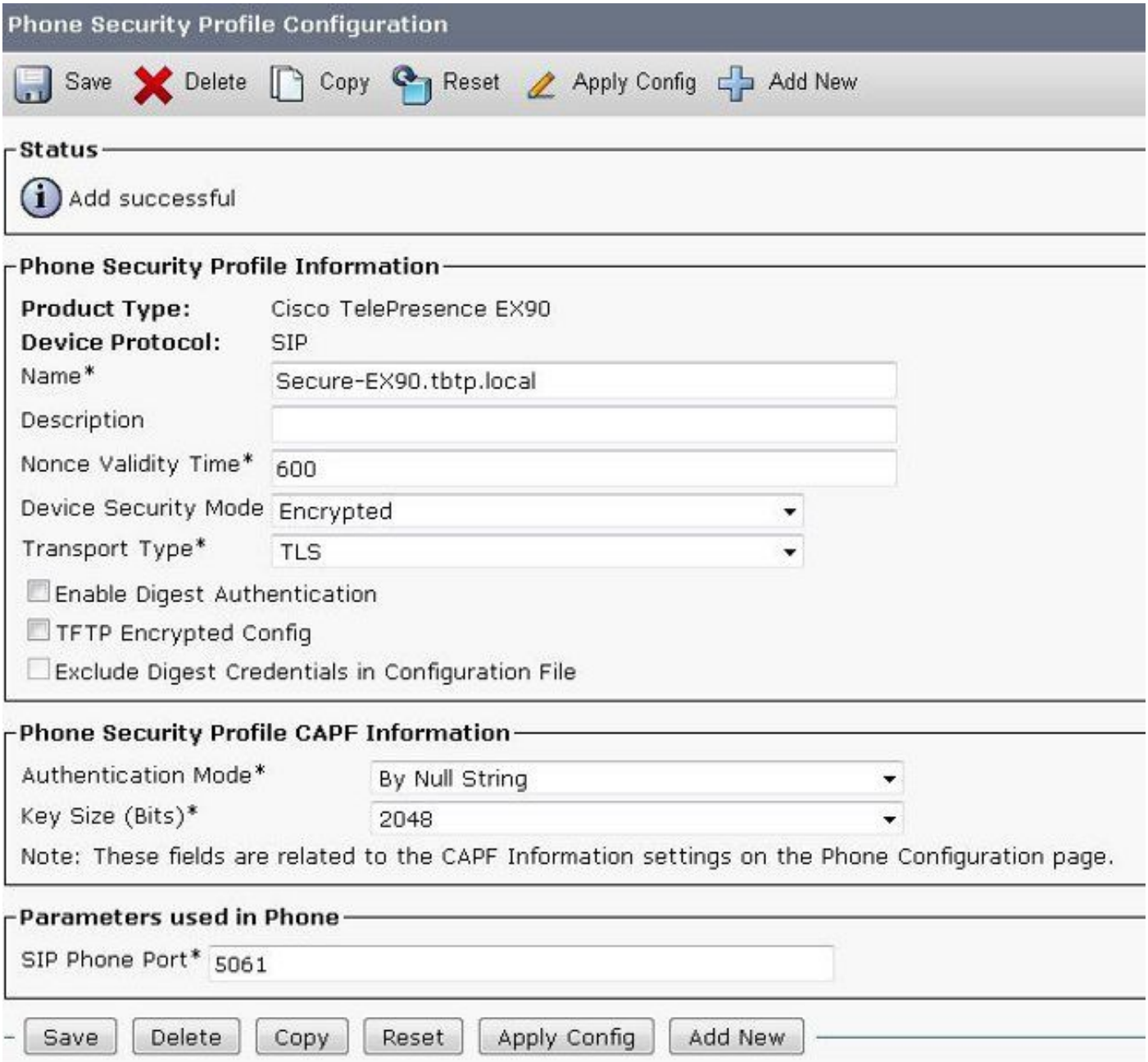
Configurar

Estos pasos para la configuración asumen que el administrador configurará el punto final TC-basado para asegura el registro del dispositivo. El registro seguro no es un requisito, no obstante

la guía total del móvil y de la solución de acceso remoto da la impresión que es puesto que hay las capturas de pantalla de la configuración que muestran los perfiles del dispositivo seguros en CUCM.

Paso 1. Cree un perfil seguro del teléfono en CUCM en el formato FQDN (opcional).

1. En CUCM, seleccione el **> Security (Seguridad) del sistema > el perfil de seguridad del teléfono**.
2. El tecleo **agrega nuevo**.
3. Seleccione el tipo TC-basado del punto final y configure estos parámetros:
4. Nombre - **Secure-EX90.tbtp.local (formato FQDN requerido)**
5. Modo de la seguridad del dispositivo - **Cifrado**
6. Tipo del transporte - **TLS**
7. Puerto telefónico del SORBO - **5061**



Paso 2. Asegúrese que modo seguro del cluster sea (1) - Mezclado (opcional).

1. En CUCM, seleccione el **System (Sistema) > Enterprise Parameters (Parámetros Enterprise)**.
2. Navegue hacia abajo a los **parámetros de seguridad > al modo seguro del cluster > 1.**

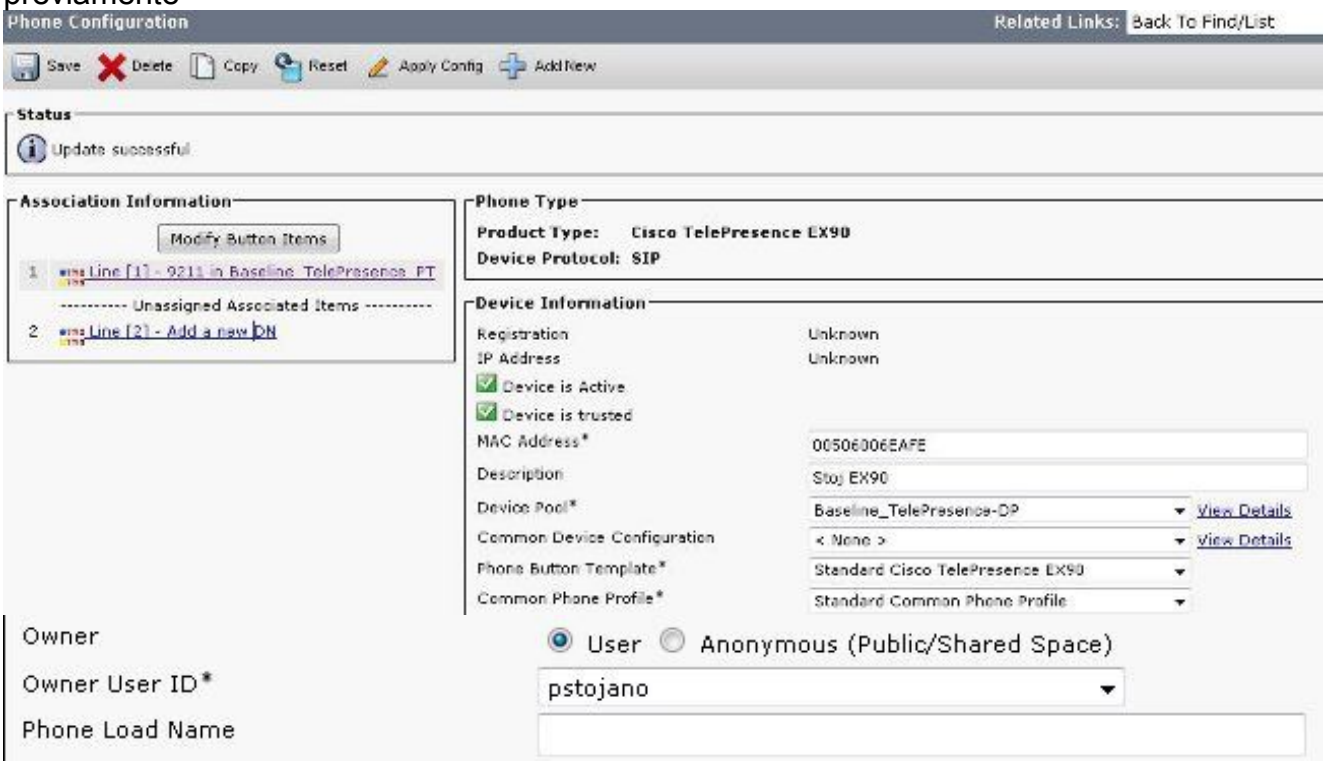
Si el valor no es 1 el CUCM no se ha asegurado. Si éste es el caso, el administrador necesita revisar uno de estos dos documentos para asegurar el CUCM.

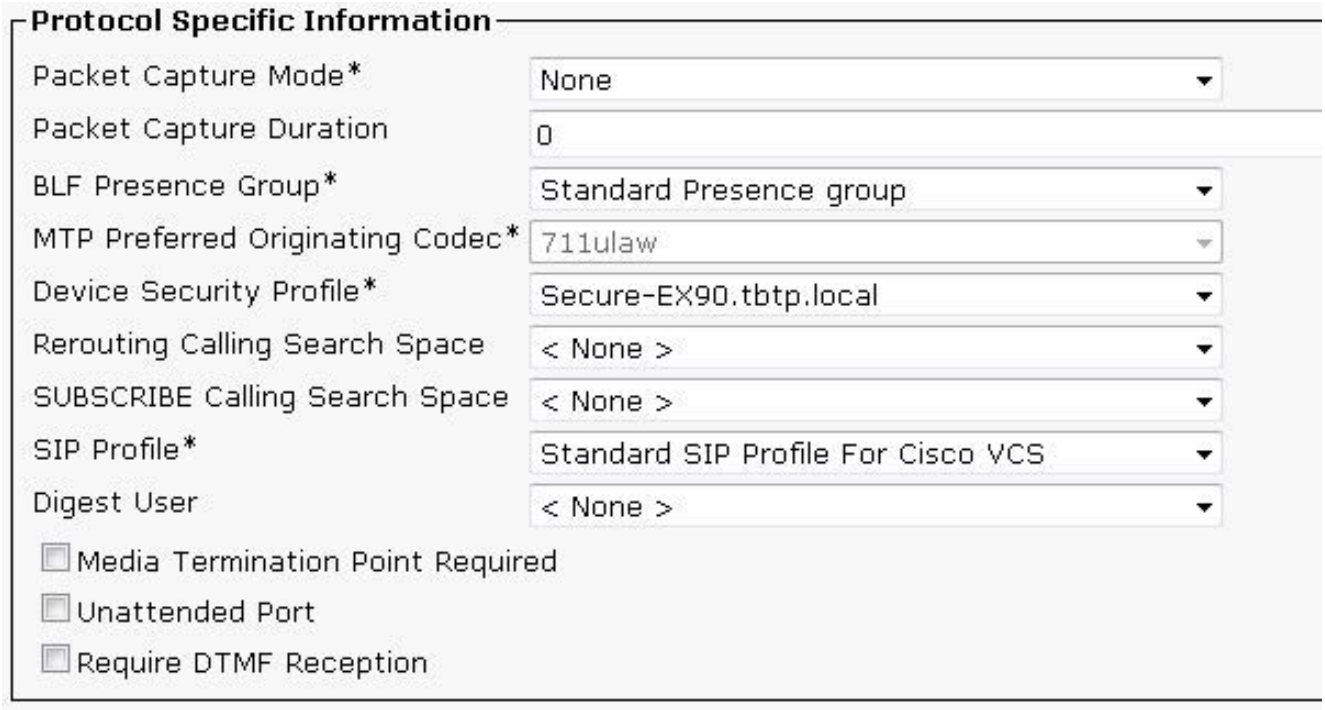
Guía de la Seguridad CUCM 9.1(2)

Guía de la Seguridad CUCM 10

Paso 3. Cree un perfil en CUCM para el punto final TC-basado.

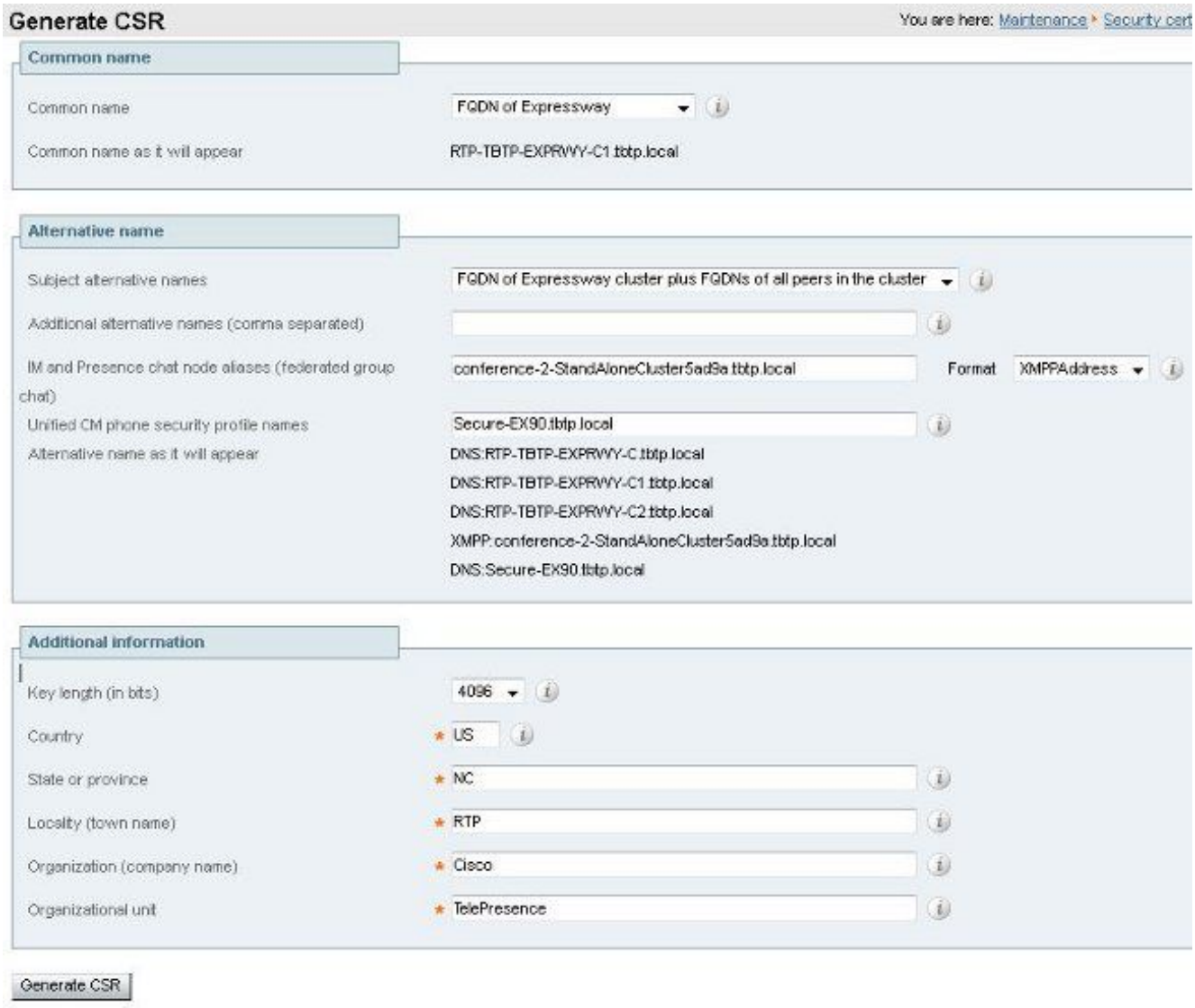
1. En CUCM, seleccione el **Device (Dispositivo) > Phone (Teléfono)**.
2. El tecleo **agrega nuevo**.
3. Seleccione el tipo TC-basado del punto final y configure estos parámetros: Dirección MAC - Dirección MAC del dispositivo TC-basadoCampos protagonizados requeridos (*)Propietario - UsuarioIdentificación del usuario del propietario - Propietario asociado al dispositivoPerfil de seguridad del dispositivo - Perfil previamente configurado (Secure-EX90.tbtp.local)Perfil del SORBO - Perfil estándar del SORBO o cualquier perfil de encargo creado previamente





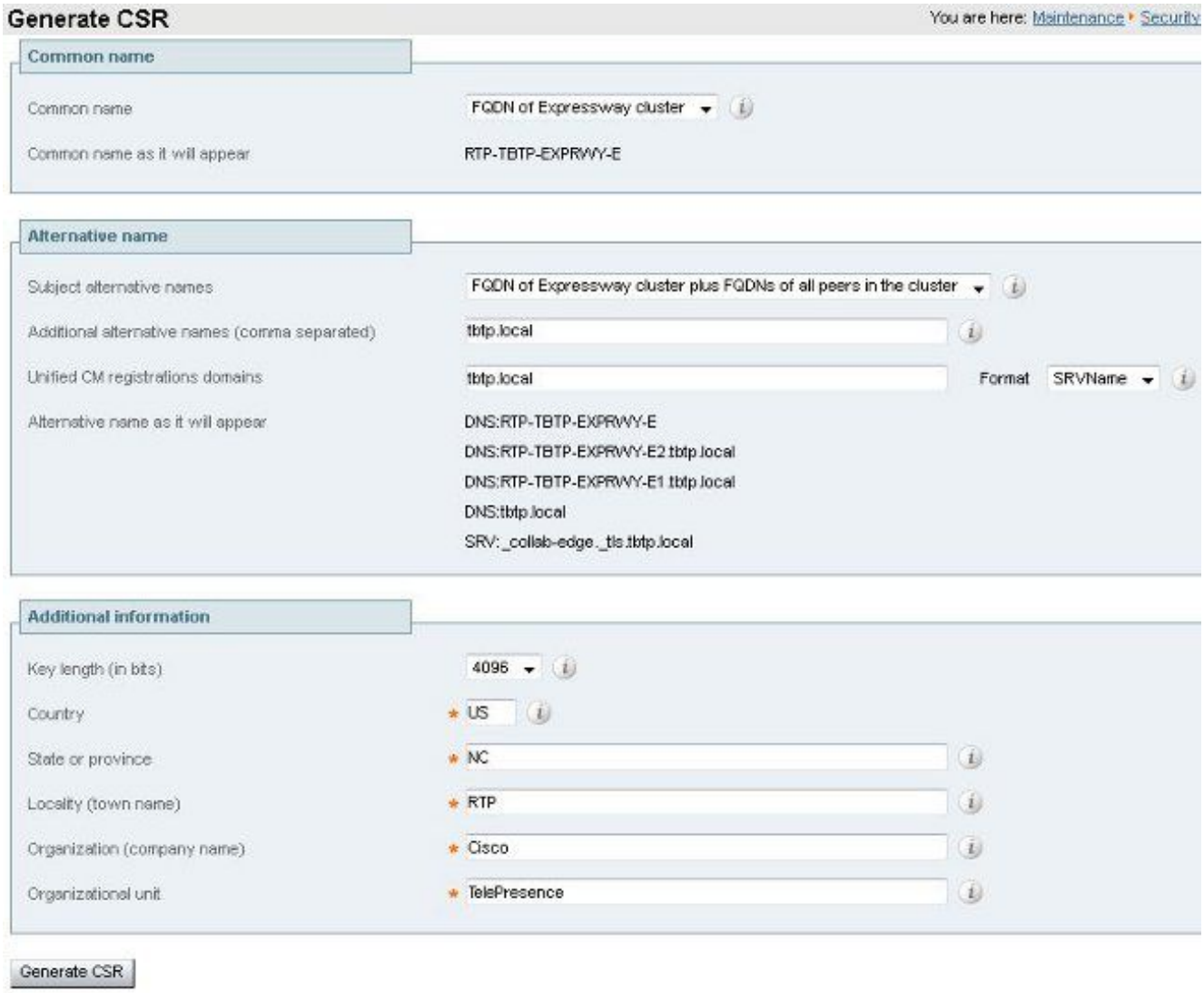
Paso 4. Agregue el nombre del perfil de seguridad al SAN del certificado Expressway-C/VCS-C (opcional).

1. En Expressway-C/VCS-C, navegue a los **Certificados > al certificado de servidor del > Security (Seguridad) del mantenimiento**.
2. El tecleo **genera el CSR**.
3. Complete los campos del pedido de firma de certificado (CSR) y asegúrese de que el **nombre unificado del perfil de seguridad del teléfono CM** tiene el perfil de seguridad exacto del teléfono enumerado en el formato del nombre de dominio completo (FQDN). Por ejemplo, **Secure-EX90.tbtp.local**. Nota: Los nombres unificados del perfil de seguridad del teléfono CM son mencionados en la parte posterior del campo sujeto del nombre alterno (SAN).
4. Envíe el CSR a un Certificate Authority (CA) interno o de las de otras compañías que se firmará.
5. Seleccione los **Certificados > el certificado de servidor del > Security (Seguridad) del mantenimiento** para cargar el certificado al Expressway-C/VCS-C.



Paso 5. Agregue el dominio UC al certificado Expressway-E/VCS-E.

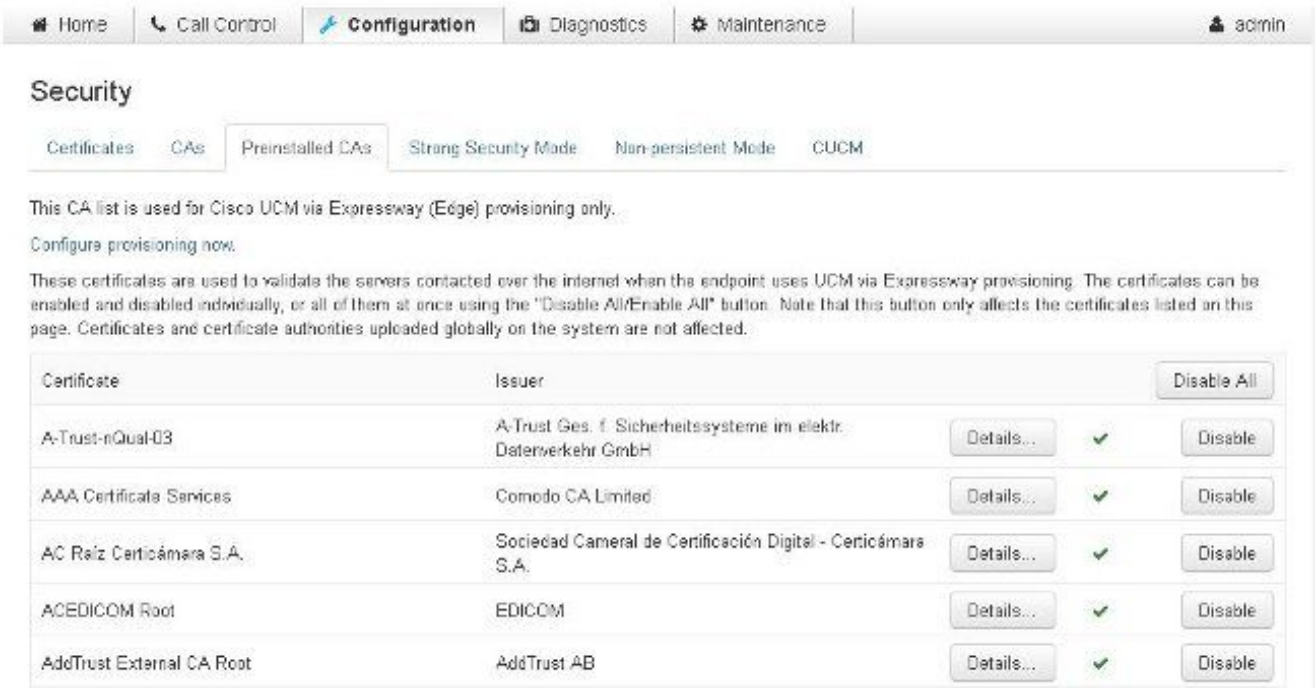
1. En Expressway-E/VCS-E, seleccione los **Certificados > el certificado de servidor del > Security (Seguridad) del mantenimiento**.
2. El tecleo **genera el CSR**.
3. Complete los campos CSR y asegúrese de que los “dominios unificados de los registros de CM” contienen el dominio que el punto final TC-basado hará las peticiones del borde de la Colaboración (collab-borde) a, en el Domain Name Server (DNS) o los formatos del nombre del servicio (SRV).
4. Envíe el CSR a un interno o a las de otras compañías CA que se firmará.
5. Seleccione los **Certificados > el certificado de servidor del > Security (Seguridad) del mantenimiento** para cargar el certificado al Expressway-E/VCS-E.



Paso 6. Instale el certificado de CA de confianza apropiado al punto final TC-basado.

1. En el punto final TC-basado, seleccione el **> Security (Seguridad) de la configuración**.
2. Seleccione la lengueta de **CA** y hojee para el certificado de CA que firmó su certificado Expressway-E/VCS-E.
3. El tecleo **agrega el Certificate Authority**. Nota: Una vez que el certificado se agrega con éxito usted verá que enumeró en la lista del
certificado.

Nota: El TC 7.2 contiene una lista instalada previamente CA. Si CA que firmó el certificado de la autopista-e se contiene dentro de esta lista, los pasos enumerados en esta sección no se
requieren.

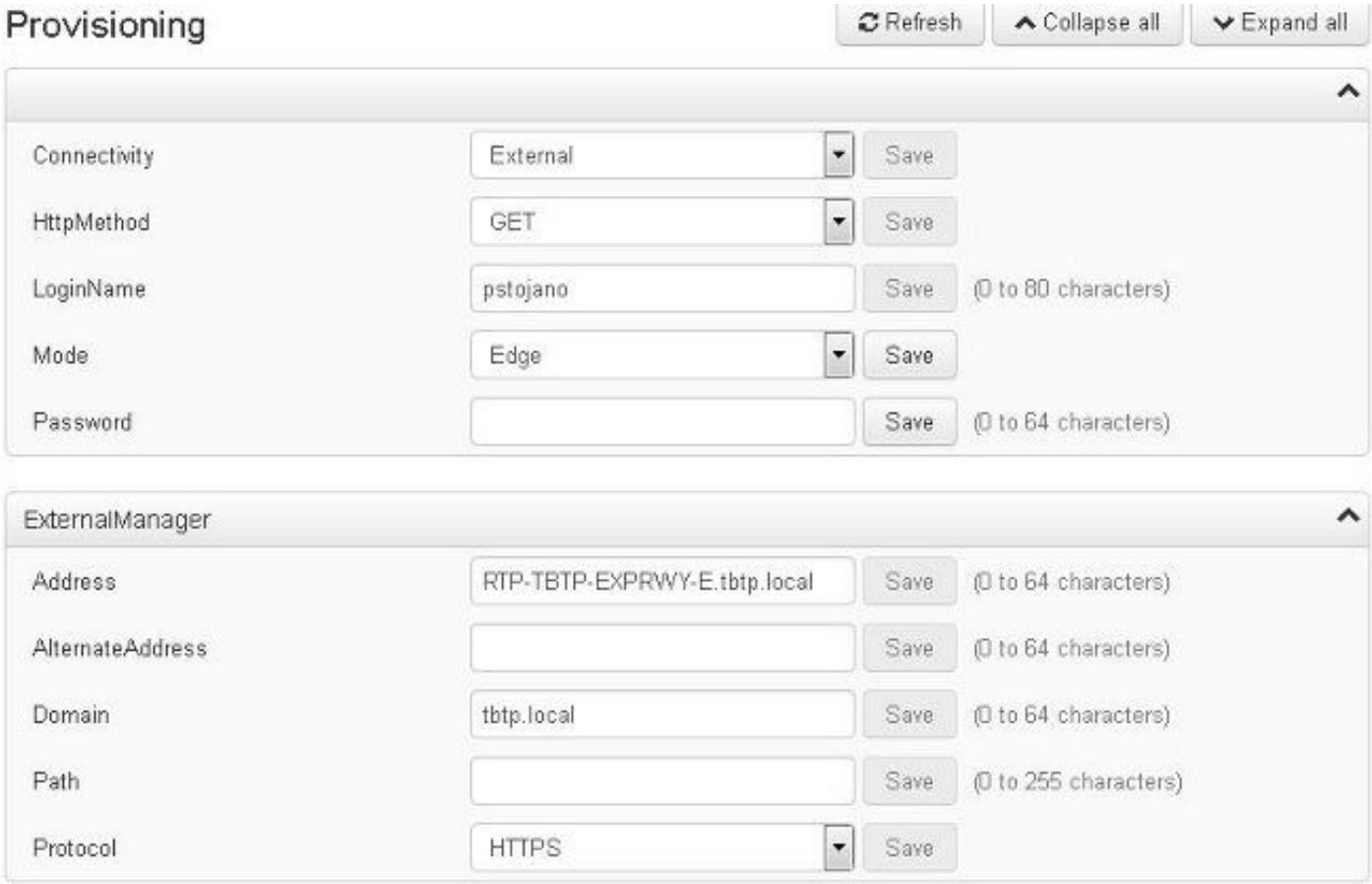


Nota: La página instalada previamente CA contiene una “configuración conveniente ahora provisioning” el botón que le lleva directamente a la configuración necesaria conocida en el paso 2 en la siguiente sección.

Paso 7. Configure un punto final TC-basado para el aprovisionamiento del borde

- En el punto final TC-basado, la **configuración > la red** selectas y se aseguran que estos campos están completados correctamente bajo sección DNS:
  Nombre de dominio
  Dirección del servidor

- En el punto final TC-basado, la **configuración > el aprovisionamiento** selectos y se aseguran que estos campos están completados correctamente:
  LoginName - según lo definido en CUCM
  Modo - **Borde**
  Contraseña - según lo definido en CUCM
  Administrador externo
  Direccionamiento - Nombre de host de su Expressway-E/VCS-E
  Dominio - Dominio donde está presente su expediente del collab-borde

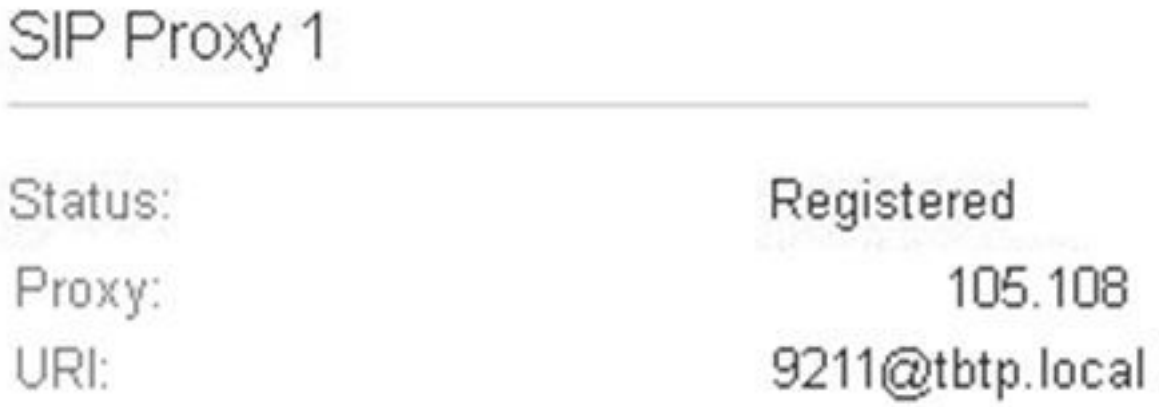


Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

punto final TC-basado

1. En la red GUI, navegue “casero”. Busque 'la sección del proxy el 1" del SORBO para un estatus “registrado”. La dirección del proxy es su Expressway-E/VCS-E.



2. Del CLI, ingrese el **xstatus //prov**. Si le registran, usted debe ver un estatus del aprovisionamiento del “aprovisionado”. **`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

En CUCM, seleccione el **Device (Dispositivo) > Phone (Teléfono)**. Navegue a través de la lista o filtre la lista basada en su punto final. Usted debe ver “registrado con un mensaje del %CUCM_IP%”. La dirección IP a la derecha de esto debe ser su Expressway-C/VCS-C que los proxys el registro.

Autopista-C

- En Expressway-C/VCS-C, **estatus > Comunicaciones unificadas > sesiones** selectos del **aprovisionamiento de la visión.**
- Filtre por la dirección IP de su punto final TC-basado. Un ejemplo de una sesión del aprovisionado se muestra en la imagen:

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Los problemas del registro se pueden causar por los factores numerosos que incluyen el DNS, los problemas del certificado, configuración, y así sucesivamente. Esta sección incluye una lista amplia de lo que usted típicamente vería si usted encuentra un problema dado y de cómo al

remediate él. Si usted se ejecuta en los problemas fuera de qué se ha documentado ya, no dude en incluirlo.

Herramientas

Para empezar, sea consciente de las herramientas en su disposición.

Punto final TC

Red GUI

- all.log
- Comience el registro extendido (incluya una captura del paquete completo)

CLI

Estos comandos son los más beneficiosos para resolver problemas en el tiempo real:

- debug 9 de HttpClient del ctx del registro
- del registro del ctx debug 9 PROV
- salida del registro en <-- Demostraciones que registran vía la consola

Una manera eficaz de reconstruir el problema es conectar el modo del aprovisionamiento del “borde” a "OFF" y entonces de nuevo al “borde” dentro de la red GUI. Usted puede también ingresar el **modo del aprovisionamiento del xConfiguration:** comando en el CLI.

Autopistas

- Registros de diagnóstico
- Tcpdump

CUCM

- Trazas SDI/SDL

Problema 1: el expediente del Collab-borde no es visible y/o el nombre de host no es resolvable

Como usted puede ver, el get_edge_config falla debido a la resolución de nombre.

Registros del punto final 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/
```

Corrección

1. Verifique si el expediente del collab-borde está presente y vuelve el nombre de host correcto.
2. Verifique si la información del servidor DNS configurada en el cliente está correcta.

Problema 2: CA no está presente dentro de la lista de confianza de CA en el punto final TC-basado

Registros del punto final 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
```

Corrección

1. Verifique si las de otras compañías CA son mencionadas bajo lengueta de la **Seguridad > CA** en el punto final.
2. Si CA es mencionado, verifique que esté correcto.

Problema 3: La autopista-e no tiene el dominio UC enumerado dentro del SAN

Registros del punto final 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'
```

Autopista-e SAN

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

Corrección

1. Autopista-e regenerada CSR para incluir los dominios UC.
2. Es posible que en el punto final TC el parámetro del **dominio de ExternalManager** no está fijado a cuál es el dominio UC. Si éste es el caso usted debe hacerlo juego.

Problema 4: El nombre de usuario y/o la contraseña suministrados en el perfil del aprovisionamiento TC es incorrectos

Registros del punto final 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"
```

Corrección

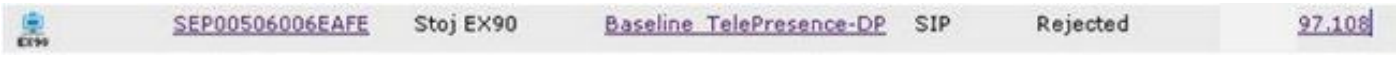
1. Verifique que el nombre de usuario/la contraseña ingresada bajo la página de aprovisionamiento en el punto final TC sea válidos.
2. Verifique las credenciales contra la base de datos CUCM.
3. Versión 10 - utilice el portal del cuidado del uno mismo
4. Versión 9 - utilice las Opciones del usuario CM

El URL para ambos portales es lo mismo: **https://%CUCM%/ucmuser/**

Si está presentado con un error escaso de las derechas, asegúrese que estos papeles están asignados al usuario:

- Standard CTI Enabled
- Usuario final estándar de CCM

Problema 5: El registro del punto final TC-basado consigue rechazado



Trazas 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,
```

Punto final 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,
```

En este ejemplo de registro específico está claro que el Expressway-C/VCS-C no contiene el perfil de seguridad FQDN del teléfono en el SAN. (Secure-EX90.tbtp.local). En el apretón de manos de Transport Layer Security (TLS), el CUCM examina el certificado de servidor Expressway-C/VCS-C. Puesto que no lo encuentra dentro del SAN lanza el error en negrita y señala que contaba con el perfil de seguridad del teléfono en el formato FQDN.

Corrección

1. Verifique que el Expressway-C/VCS-C contenga el perfil de seguridad del teléfono en el formato FQDN dentro del SAN de él sea certificado de servidor.
2. Verifique que el dispositivo utilice el perfil de seguridad correcto en CUCM si usted utiliza un perfil seguro en el formato FQDN.
3. Esto se podía también causar por el Id. de bug Cisco CSCuq86376. Si éste es el control del caso el tamaño Expressway-C/VCS-C SAN y la posición del perfil de seguridad del teléfono dentro del SAN.

Problema 6: el aprovisionamiento TC-basado del punto final falla - Ningún servidor UD

Este errror debe estar presente bajo los **diagnósticos** > el **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,
```

Registros del punto final TC

Navegue a la derecha de ver los errores en intrépido

```
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!
```

Corrección

1. Asegúrese que haya un servicio del perfil y CTI UC del servicio asociado a la cuenta del usuario final usada para pedir el aprovisionamiento del punto final vía los servicios MRA.

2. Navegue a **CUCM admin > User Management (Administración de usuario) > los ajustes de usuario > servicio UC** y cree un servicio CTI UC esas puntas al IP de CUCM (es decir MRA_UC-Service).

3. Navegue a **CUCM admin > User Management (Administración de usuario) > los ajustes de usuario > perfil del servicio** y cree un nuevo perfil (es decir MRA_ServiceProfile).

4. En el nuevo perfil del servicio, navegue a la parte inferior y en la sección del perfil CTI, seleccionan el nuevo servicio CTI UC que usted acaba de crear (es decir MRA_UC-Service), después hacen clic la salvaguardia.

5. Navegue a **CUCM admin > User Management (Administración de usuario) > usuario final** y encuentre la cuenta de usuario utilizada para pedir el aprovisionamiento del punto final vía los servicios MRA.

6. Bajo **configuraciones del servicio de** ese usuario, asegúrese que a casa el cluster sea control y ese perfil del servicio UC refleja el nuevo perfil del servicio que usted creó (es decir MRA_ServiceProfile), después hace clic la salvaguardia.

7. Puede tardar algunos minutos para replicar. Intente inhabilitar el modo del aprovisionamiento en el punto final y darle vuelta detrás en unos minutos más tarde para ver si el punto final ahora se registra.

Información Relacionada

- Móvil y guía del Acceso Remoto
- Guía de la creación del certificado VCS
- Guía de introducción EX90/EX60
- Guía del administrador CUCM 9.1
- Soporte Técnico y Documentación - Cisco Systems