

Ejemplo de Configuración de Terminales Basados en TC de Collaboration Edge

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Paso 1. Cree un perfil de teléfono seguro en CUCM en formato FQDN \(opcional\).](#)

[Paso 2. Asegúrese de que Cluster Security Mode \(Modo de seguridad del clúster\) sea \(1\) - Mixed \(Mixto\) \(Opcional\).](#)

[Paso 3. Cree un perfil en CUCM para el terminal basado en TC.](#)

[Paso 4. Agregue el nombre del perfil de seguridad a la SAN del certificado de Expressway-C/VCS-C \(opcional\).](#)

[Paso 5. Agregue el dominio de UC al certificado de Expressway-E/VCS-E.](#)

[Paso 6. Instale el certificado de CA de confianza adecuado en el terminal basado en TC.](#)

[Paso 7. Configuración de un terminal basado en TC para el aprovisionamiento perimetral](#)

[Verificación](#)

[Terminal basado en TC](#)

[CUCM](#)

[Expressway-C](#)

[Troubleshoot](#)

[Herramientas](#)

[terminal TC](#)

[Expressway](#)

[CUCM](#)

[Problema 1: El registro de la frontera de colaboración no está visible y/o el nombre de host no se puede resolver](#)

[Registros de terminales TC](#)

[Remediación](#)

[Problema 2: CA no está presente en la lista de CA de confianza en el terminal basado en TC](#)

[Registros de terminales TC](#)

[Remediación](#)

[Problema 3: Expressway-E no tiene el dominio de UC incluido en la SAN](#)

[Registros de terminales TC](#)

[SAN de Expressway-E](#)

[Remediación](#)

[Problema 4: El nombre de usuario o la contraseña proporcionados en el perfil de aprovisionamiento de TC son incorrectos](#)

[Registros de terminales TC](#)

[Expressway-C/VCS-C](#)

[Remediación](#)

[Problema 5: Se rechaza el registro de terminales basado en TC](#)

[Rastros de CUCM](#)

[terminal TC](#)

[Expressway-C/VCS-C real](#)

[Remediación](#)

[Problema 6: Falla el aprovisionamiento de terminales basado en TC - No hay servidor UDS](#)

[Información Relacionada](#)

Introducción

El documento describe lo que se necesita para configurar y resolver problemas de registro de terminales basado en el códec de TelePresence (TC) a través de la solución de acceso remoto y móvil.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Solución de acceso remoto y móvil
- Certificados de Video Communication Server (VCS)
- Expressway X8.1.1 o posterior
- Cisco Unified Communication Manager (CUCM) versión 9.1.2 o posterior
- terminales basados en TC
- CE8.x requiere la clave de opción de cifrado para habilitar "Edge" como opción de aprovisionamiento

Componentes Utilizados

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

- VCS X8.1.1 o posterior
- CUCM versión 9.1(2)SU1 o posterior y IM & Presence 9.1(1) o posterior
- Firmware TC 7.1 o posterior (**se recomienda TC7.2**)
- VCS Control y Expressway/Expressway Core y Edge
- CUCM
- terminal TC

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.

Configurar

Estos pasos de configuración suponen que el administrador configurará el terminal basado en TC

para el registro seguro del dispositivo. El registro seguro **NO** es un requisito; sin embargo, la guía general de la solución de acceso remoto y móvil da la impresión de que es porque hay capturas de pantalla de la configuración que muestran perfiles de dispositivo seguros en CUCM.

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

1. En CUCM, seleccione **System > Security > Phone Security Profile**.
2. Haga clic en **Agregar nuevo**.
3. Seleccione el tipo de terminal basado en TC y configure estos parámetros:
4. Nombre - **Secure-EX90.tbtp.local** (se requiere formato FQDN)
5. Modo de seguridad del dispositivo - **Cifrado**
6. Tipo de transporte - **TLS**
7. Puerto telefónico SIP - **5061**

Phone Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

Status

i Add successful

Phone Security Profile Information

Product Type: Cisco TelePresence EX90

Device Protocol: SIP

Name* Secure-EX90.tbtp.local

Description

Nonce Validity Time* 600

Device Security Mode Encrypted

Transport Type* TLS

Enable Digest Authentication

TFTP Encrypted Config

Exclude Digest Credentials in Configuration File

Phone Security Profile CAPF Information

Authentication Mode* By Null String

Key Size (Bits)* 2048

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Parameters used in Phone

SIP Phone Port* 5061

Save Delete Copy Reset Apply Config Add New

Paso 2. Asegúrese de que Cluster Security Mode (Modo de seguridad del clúster) sea (1) - Mixed (Mixto) (Opcional).

1. En CUCM, seleccione **System > Enterprise Parameters**.
2. Desplácese hacia abajo hasta **Parámetros de seguridad > Modo de seguridad de clúster > 1**.



Si el valor no es 1, CUCM no se ha protegido. Si este es el caso, el administrador necesita revisar uno de estos dos documentos para proteger la CUCM.

[Guía de seguridad de CUCM 9.1\(2\)](#)

[Guía de seguridad de CUCM 10](#)

Paso 3. Cree un perfil en CUCM para el terminal basado en TC.

1. En CUCM, seleccione **Device > Phone**.
2. Haga clic en **Agregar nuevo**.
3. Seleccione el tipo de terminal basado en TC y configure estos parámetros: Dirección MAC: dirección MAC del dispositivo basado en TCCampos marcados obligatorios (*)Propietario - UsuarioID de usuario propietario: propietario asociado al dispositivoPerfil de seguridad del dispositivo: perfil configurado anteriormente (Secure-EX90.tbtp.local)Perfil SIP: perfil SIP estándar o cualquier perfil personalizado creado previamente

The screenshot shows the 'Phone Configuration' page in CUCM. The page title is 'Phone Configuration' and the 'Related Links' are 'Back To Find/List'. The 'Status' section shows 'Update successful'. The 'Association Information' section shows a list of lines: 'Line [1] - 9211 in Baseline_TelePresence_PT' and 'Line [2] - Add a new DN'. The 'Phone Type' section shows 'Product Type: Cisco TelePresence EX90' and 'Device Protocol: SIP'. The 'Device Information' section is expanded, showing fields for Registration, IP Address, Device is Active, Device is trusted, MAC Address, Description, Device Pool, Common Device Configuration, Phone Button Template, and Common Phone Profile. The 'Owner' section is also visible, showing 'Owner User ID' set to 'pstojano'.

Protocol Specific Information	
Packet Capture Mode*	None
Packet Capture Duration	0
BLF Presence Group*	Standard Presence group
MTP Preferred Originating Codec*	711ulaw
Device Security Profile*	Secure-EX90.tbtp.local
Rerouting Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile For Cisco VCS
Digest User	< None >
<input type="checkbox"/> Media Termination Point Required	
<input type="checkbox"/> Unattended Port	
<input type="checkbox"/> Require DTMF Reception	

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

1. En Expressway-C/VCS-C, vaya a **Mantenimiento > Certificados de seguridad > Certificado de servidor**.
2. Haga clic en **Generar CSR**.
3. Rellene los campos Solicitud de firma de certificado (CSR) y asegúrese de que el **nombre del perfil de seguridad del teléfono de Unified CM** tenga el perfil de seguridad del teléfono exacto que aparece en el formato de nombre de dominio completo (FQDN). Por ejemplo, **Secure-EX90.tbtp.local**. **Nota:** Los nombres del perfil de seguridad del teléfono de Unified CM se muestran en la parte posterior del campo Nombre alternativo del sujeto (SAN).
4. Envíe el CSR a una Autoridad de Certificación Interna o a una Autoridad de Certificación de Terceros (CA) que se firmará.
5. Seleccione **Mantenimiento > Certificados de seguridad > Certificado de servidor** para cargar el certificado en Expressway-C/VCS-C.

Generate CSR You are here: [Maintenance](#) > [Security cert](#)

Common name

Common name: ⓘ

Common name as it will appear:

Alternative name

Subject alternative names: ⓘ

Additional alternative names (comma separated): ⓘ

IM and Presence chat node aliases (federated group chat): Format: ⓘ

Unified CM phone security profile names: ⓘ

Alternative name as it will appear:
 DNS:RTP-TBTP-EXPRWY-C.tftp.local
 DNS:RTP-TBTP-EXPRWY-C1.tftp.local
 DNS:RTP-TBTP-EXPRWY-C2.tftp.local
 XMPP:conference-2-StandAloneCluster5ad9a.tftp.local
 DNS:Secure-EX90.tftp.local

Additional information

Key length (in bits): ⓘ

Country: ⓘ

State or province: ⓘ

Locality (town name): ⓘ

Organization (company name): ⓘ

Organizational unit: ⓘ

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

1. En Expressway-E/VCS-E, seleccione **Mantenimiento > Certificados de seguridad > Certificado de servidor**.
2. Haga clic en **Generar CSR**.
3. Rellene los campos CSR y asegúrese de que los "dominios de registro de Unified CM" contienen el dominio al que el terminal basado en TC realizará solicitudes de Collaboration Edge (en el perímetro de la colaboración) en los formatos Domain Name Server (DNS) o Service Name (SRV).
4. Envíe la CSR a una CA interna o de terceros para que la firme.
5. Seleccione **Mantenimiento > Certificados de seguridad > Certificado de servidor** para cargar el certificado en Expressway-E/VCS-E.

Generate CSR You are here: [Maintenance](#) > [Security](#)

Common name

Common name: ⓘ

Common name as it will appear: RTP-TBTP-EXPRWY-E

Alternative name

Subject alternative names: ⓘ

Additional alternative names (comma separated): ⓘ

Unified CM registrations domains: Format: ⓘ

Alternative name as it will appear:

DNS:RTP-TBTP-EXPRWY-E
 DNS:RTP-TBTP-EXPRWY-E2.tbtcp.local
 DNS:RTP-TBTP-EXPRWY-E1.tbtcp.local
 DNS:tbtcp.local
 SRV:_collab-edge._tls.tbtcp.local

Additional information

Key length (in bits): ⓘ

Country: ⓘ

State or province: ⓘ

Locality (town name): ⓘ

Organization (company name): ⓘ

Organizational unit: ⓘ

Paso 6. Instale el certificado de CA de confianza adecuado en el terminal basado en TC.

1. En el terminal basado en TC, seleccione **Configuration > Security**.
2. Seleccione la ficha **CA** y busque el certificado de CA que firmó el certificado de Expressway-E/VCS-E.
3. Haga clic en **Agregar autoridad de certificado**. **Nota:** Una vez que el certificado se haya agregado correctamente, lo verá en la lista de certificados.

Security

Successfully imported the certificate. Please reboot for changes to take effect.

Certificates **CA**s Preinstalled CA's Strong Security Mode Non-persistent Mode CUCM

Certificate	Issuer	
heros-W2K8VM3-CA	heros-W2K8VM3-CA	<input type="button" value="Delete..."/> <input type="button" value="View Certificate"/>

Add Certificate Authority

CA file:

This system supports PEM formatted files (.pem) with one or more CA certificates within the file.

Nota: TC 7.2 contiene una lista de CA preinstalada. Si la CA que firmó el certificado de Expressway-E está incluida en esta lista, no se requieren los pasos enumerados en esta sección.

The screenshot shows the Cisco UCM Administration interface. The top navigation bar includes Home, Call Control, Configuration (selected), Diagnostics, and Maintenance. The user is logged in as 'admin'. The main heading is 'Security', with sub-tabs for Certificates, CAs, Preinstalled CAs (selected), Strong Security Mode, Non-persistent Mode, and CUCM. Below the tabs, there is a note: 'This CA list is used for Cisco UCM via Expressway (Edge) provisioning only. Configure provisioning now.' A paragraph explains that these certificates are used to validate servers contacted over the internet and can be enabled or disabled individually or all at once. Below this is a table of preinstalled CAs with columns for Certificate, Issuer, and a 'Disable All' button. Each row also has 'Details...' and 'Disable' buttons. A green checkmark is visible in the middle of each row, indicating they are enabled.

Certificate	Issuer	Disable All
A-Trust-nQual-03	A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	Details... ✓ Disable
AAA Certificate Services	Comodo CA Limited	Details... ✓ Disable
AC Raíz Certificámara S.A.	Sociedad Cameral de Certificación Digital - Certificámara S.A.	Details... ✓ Disable
ACEDICOM Root	EDICOM	Details... ✓ Disable
AddTrust External CA Root	AddTrust AB	Details... ✓ Disable

Nota: La página de CA preinstaladas contiene un cómodo botón "Configurar aprovisionamiento ahora" que le lleva directamente a la configuración requerida indicada en el paso 2 de la siguiente sección.

Paso 7. Configuración de un terminal basado en TC para el aprovisionamiento perimetral

- En el extremo basado en TC, seleccione **Configuration > Network** y asegúrese de que estos campos se rellenen correctamente en la sección DNS:
Nombre de dominio
Dirección del servidor
- En el terminal basado en TC, seleccione **Configuration > Provisioning** y asegúrese de que estos campos estén correctamente rellenos:
Nombre de inicio de sesión: tal y como se define en CUCM
Modo- **Perímetro**
Contraseña: tal como se define en CUCM
Administrador externo
Dirección: nombre de host de Expressway-E/VCS-E
Dominio: dominio en el que está presente el registro de la frontera de colaboración

Provisioning

[Refresh](#)[Collapse all](#)[Expand all](#)

Connectivity	External	Save
HttpMethod	GET	Save
LoginName	pstojano	Save (0 to 80 characters)
Mode	Edge	Save
Password		Save (0 to 64 characters)

ExternalManager		
Address	RTP-TBTP-EXPRWY-E.tbtp.local	Save (0 to 64 characters)
AlternateAddress		Save (0 to 64 characters)
Domain	tbtp.local	Save (0 to 64 characters)
Path		Save (0 to 255 characters)
Protocol	HTTPS	Save

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Terminal basado en TC

1. En la interfaz gráfica de usuario web, vaya a "Inicio". Busque la sección "Proxy SIP 1" para ver el estado "Registrado". La dirección de proxy es Expressway-E/VCS-E.

SIP Proxy 1

Status:	Registered
Proxy:	105.108
URI:	9211@tbtp.local

2. Desde la CLI, ingrese `xstatus //prov`. Si está registrado, debe ver el estado de aprovisionamiento de "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
```

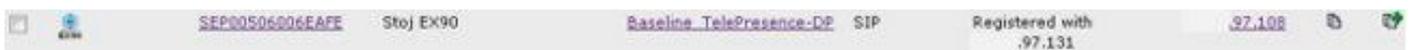
```

*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 **Device > Phone**. Desplácese por la lista o filtre la lista en función del terminal. Debería ver un mensaje "Registrado con %CUCM_IP%". La dirección IP a la derecha de esto debe ser su Expressway-C/VCS-C que envía el registro.



Expressway-C

- En Expressway-C/VCS-C, seleccione **Estado > Unified Communications > Ver sesiones de aprovisionamiento**.
- Filtre por la dirección IP de su terminal basado en TC. En la imagen se muestra un ejemplo de una sesión aprovisionada:

Records: 2 Page 1 of 1

Username	Device	User agent	Unified CM server	Expire time
pstojano	252.227	CiscoTC	97.131	2014-09-25 02:08:53

Troubleshoot

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

Los problemas de registro pueden ser causados por numerosos factores que incluyen DNS, problemas de certificados, configuración, etc. Esta sección incluye una lista completa de lo que normalmente vería si se encontrara con un problema determinado y cómo solucionarlo. Si

encuentra problemas fuera de lo que ya se ha documentado, no dude en incluirlos.

Herramientas

Para empezar, tenga en cuenta las herramientas a su disposición.

terminal TC

GUI web

- all.log
- Iniciar registro extendido (incluye una captura de paquetes completa)

CLI

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

- log ctx HttpClient debug 9
- log ctx PROV debug 9
- salida de registro en <— Muestra el registro a través de la consola

Una forma eficaz de recrear el problema es cambiar el modo de aprovisionamiento de "Edge" a "Off" y volver a "Edge" dentro de la GUI web. También puede ingresar al **Modo de Aprovisionamiento xConfiguration**: en la CLI.

Expressway

- [Registros de diagnóstico](#)
- TCPDump

CUCM

- Rastreo SDI/SDL

Problema 1: El registro de la frontera de colaboración no está visible y/o el nombre de host no se puede resolver

Como puede ver, get_edge_config falla debido a la resolución del nombre.

Registros de terminales 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/
```

Remediación

1. Verifique si el registro del borde de la colecta está presente y devuelve el nombre de host correcto.
2. Verifique si la información del servidor DNS configurada en el cliente es correcta.

Problema 2: CA no está presente en la lista de CA de confianza en el terminal basado en TC

Registros de terminales 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

```

Remediación

1. Verifique si una CA de terceros aparece en la ficha **Security > CAs** en el terminal.
2. Si se muestra la CA, verifique que sea correcta.

Problema 3: Expressway-E no tiene el dominio de UC incluido en la SAN

Registros de terminales 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'
```

SAN de Expressway-E

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

Remediación

1. Regenerar Expressway-E CSR para incluir los dominios de UC.
2. Es posible que en el extremo TC el parámetro **ExternalManager Domain** no esté configurado en lo que es UC Domain. Si este es el caso, debe coincidir con él.

Problema 4: El nombre de usuario o la contraseña proporcionados en el perfil de aprovisionamiento de TC son incorrectos

Registros de terminales TC

```
83716.67 HttpClient Server auth using Basic with user 'pstoiano'
83716.67 HttpClient GET /dGJ0cC5jb20/get_edge_config/ HTTP/1.1
Authorization: xxxxxxx
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/pstoiano/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="pstoiano" 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="pstoiano"**

Server="('https', 'xx.xx.97.131', 8443)" Reason="<twisted.python.failure.Failure

<type 'exceptions.Exception'>>" UTCTime="2014-09-25 17:46:20,92"

Remediación

1. Verifique que el nombre de usuario/contraseña ingresado en la página Provisioning en el extremo TC sea válido.
2. Verifique las credenciales con la base de datos de CUCM.
3. Versión 10: utilice el portal de autoayuda
4. Versión 9: utilice las opciones de usuario de CM

La URL de ambos portales es la misma: <https://%CUCM%/ucmuser/>

Si se presenta un error de derechos insuficiente, asegúrese de que estas funciones se asignan al usuario:

- Standard CTI Enabled
- Usuario final de CCM estándar

Problema 5: Se rechaza el registro de terminales basado en TC

	SEP00506006EAFE	Stoj EX90	Baseline TelePresence-DP	SIP	Rejected	97.108
---	---------------------------------	-----------	--	-----	----------	------------------------

Rastros de 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,
```

terminal TC

SIP Proxy 1

Status:

Failed: 403 Forbidden

Expressway-C/VCS-C real

X509v3 Subject Alternative Name:

DNS:RTP-TBTP-EXPRWY-C.tbtp.local, XMPP:conference-2-StandAloneCluster5ad9a.tbtp.local

En este ejemplo de registro específico, está claro que Expressway-C/VCS-C no contiene el FQDN del perfil de seguridad del teléfono en la SAN. (Secure-EX90.tbtp.local). En el intercambio de señales de seguridad de la capa de transporte (TLS), CUCM inspecciona el certificado de servidor de Expressway-C/VCS-C. Como no lo encuentra dentro de la SAN, produce el error en negrita e informa que esperaba el perfil de seguridad del teléfono en formato FQDN.

Remediación

1. Verifique que Expressway-C/VCS-C contenga el perfil de seguridad del teléfono en formato FQDN dentro de la SAN de su certificado de servidor.
2. Verifique que el dispositivo utilice el perfil de seguridad correcto en CUCM si utiliza un perfil seguro en formato FQDN.
3. Esto también podría ser causado por el ID de bug de Cisco [CSCuq86376](#). Si este es el caso, verifique el tamaño de la SAN de Expressway-C/VCS-C y la posición del perfil de seguridad del teléfono dentro de la SAN.

Problema 6: Falla el aprovisionamiento de terminales basado en TC - No hay servidor UDS

Este error debe estar presente en **Diagnostics > Troubleshooting** :

Error: Provisioning Status

Provisioning failed: XML didnt contain UDS server address

Registros de terminales TC

Desplácese a la derecha para ver los errores en negrita

```
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;&lt;/route></sipRequest><xmppEdgeServer><server><address>expe.domain.com</adre
```

```
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!
```

Remediación

1. Asegúrese de que haya un perfil de servicio y un servicio CTI UC asociados a la cuenta de usuario final que se utiliza para solicitar el aprovisionamiento de terminales a través de los servicios MRA.
2. Navegue hasta **CUCM admin > User Management > User Settings > UC Service** y cree un CTI UC Service que apunte a la IP de CUCM (es decir, MRA_UC-Service).
3. Navegue hasta **CUCM admin > User Management > User Settings > Service Profile** y cree un nuevo perfil (es decir, MRA_ServiceProfile).
4. En el nuevo perfil de servicio, desplácese hasta la parte inferior y, en la sección Perfil CTI, seleccione el nuevo servicio CTI UC que acaba de crear (es decir, MRA_UC-Service) y, a continuación, haga clic en Guardar.
5. Navegue hasta **CUCM admin > User Management > End User** y busque la cuenta de usuario utilizada para solicitar el aprovisionamiento de terminales a través de los servicios MRA.
6. En **Configuración de servicio** de ese usuario, asegúrese de que el clúster de inicio esté activado y que el perfil de servicio de UC refleje el nuevo perfil de servicio que creó (es decir, MRA_ServiceProfile) y, a continuación, haga clic en Guardar.
7. Puede tardar unos minutos en replicarse. Intente inhabilitar el modo de aprovisionamiento en el terminal y vuelva a activarlo unos minutos después para ver si el terminal se registra ahora.

Información Relacionada

- [Guía de acceso móvil y remoto](#)
- [Guía de creación de certificados de VCS](#)
- [Guía de inicio de EX90/EX60](#)
- [Guía del administrador de CUCM 9.1](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)