

Konfigurationsbeispiel für Endgeräte auf Basis des Collaboration Edge

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Schritt 1: Erstellen Sie ein sicheres Telefonprofil auf dem CUCM im FQDN-Format \(optional\).](#)

[Schritt 2: Stellen Sie sicher, dass der Cluster-Sicherheitsmodus \(1\) - Gemischt \(optional\) ist.](#)

[Schritt 3: Erstellen Sie ein Profil im CUCM für den TC-basierten Endpunkt.](#)

[Schritt 4: Fügen Sie dem SAN des Expressway-C/VCS-C-Zertifikats den Sicherheitsprofilnamen hinzu \(optional\).](#)

[Schritt 5: Fügen Sie die UC-Domäne dem Expressway-E/VCS-E-Zertifikat hinzu.](#)

[Schritt 6: Installieren Sie das entsprechende Zertifikat der vertrauenswürdigen Zertifizierungsstelle auf dem TC-basierten Endpunkt.](#)

[Schritt 7: Einrichtung eines TC-basierten Endpunkts für die Edge-Bereitstellung](#)

[Überprüfen](#)

[TC-basierte Endgeräte](#)

[CUCM](#)

[Expressway-C](#)

[Fehlerbehebung](#)

[Tools](#)

[TC-Endpunkt](#)

[Expressdienste](#)

[CUCM](#)

[Ausgabe 1: Der Collab-Edge-Datensatz ist nicht sichtbar und/oder der Hostname ist nicht auflösbar.](#)

[TC-Endpunktprotokolle](#)

[Problembehebung](#)

[Ausgabe 2: CA ist nicht in der Liste der vertrauenswürdigen Zertifizierungsstellen auf dem TC-basierten Endpunkt vorhanden.](#)

[TC-Endpunktprotokolle](#)

[Problembehebung](#)

[Ausgabe 3: Expressway-E hat die im SAN aufgeführte UC-Domäne nicht.](#)

[TC-Endpunktprotokolle](#)

[Expressway-E SAN](#)

[Problembehebung](#)

[Ausgabe 4: Benutzername und/oder Kennwort im TC-Bereitstellungsprofil sind falsch](#)

[TC-Endpunktprotokolle](#)

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

[Problembehebung](#)

[Ausgabe 5: TC-basierte Endpunktregistrierung wird abgelehnt](#)

[CUCM-Ablaufverfolgungen](#)

[TC-Endpunkt](#)

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

[Problembeseitigung](#)

[Ausgabe 6: TC-basierte Endpunkt-Bereitstellung schlägt fehl - kein UDS-Server](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie die TelePresence Codec (TC)-basierte Endgerätregistrierung über die Mobile- und Remote-Zugriffslösung konfiguriert und Fehler bei diesen behoben werden können.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Mobile und Remote Access-Lösung
- Video Communication Server (VCS)-Zertifikate
- Expressway X8.1.1 oder spätere Version
- Cisco Unified Communication Manager (CUCM) Version 9.1.2 oder höher
- TC-basierte Endgeräte
- Für CE8.x ist der Verschlüsselungsoptionen-Schlüssel erforderlich, um "Edge" als Bereitstellungsoption zu aktivieren.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- VCS X8.1.1 oder spätere Version
- CUCM-Version 9.1(2)SU1 oder höher und IM & Presence 9.1(1) oder höher
- TC 7.1 oder höher Firmware (**TC7.2 empfohlen**)
- VCS Control & Expressway/Expressway Core & Edge
- CUCM
- TC-Endpunkt

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Bei diesen Konfigurationsschritten wird davon ausgegangen, dass der Administrator den TC-basierten Endpunkt für die sichere Geräteregistrierung konfiguriert. Eine sichere Registrierung ist **NICHT** erforderlich. Der allgemeine Lösungsleitfaden für Mobil- und Remote-Zugriff vermittelt jedoch den Eindruck, dass es Screenshots aus der Konfiguration gibt, die sichere Geräteprofile auf dem CUCM anzeigen.

Schritt 1: Erstellen Sie ein sicheres Telefonprofil auf dem CUCM im FQDN-Format (optional).

1. Wählen Sie in CUCM **System > Security > Phone Security Profile (System > Sicherheit > Telefonsicherheitsprofil)**.
2. Klicken Sie auf **Neu hinzufügen**.
3. Wählen Sie den TC-basierten Endgerätetyp aus, und konfigurieren Sie folgende Parameter:
4. Name - **Secure-EX90.tbtp.local (FQDN-Format erforderlich)**
5. Gerätesicherheitsmodus - **verschlüsselt**
6. Transporttyp - **TLS**
7. SIP-Telefonanschluss - **5061**

Phone Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

Status

Add successful

Phone Security Profile Information

Product Type: Cisco TelePresence EX90
Device Protocol: SIP

Name*
Description
Nonce Validity Time*
Device Security Mode
Transport Type*

Enable Digest Authentication
 TFTP Encrypted Config
 Exclude Digest Credentials in Configuration File

Phone Security Profile CAPF Information

Authentication Mode*
Key Size (Bits)*

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

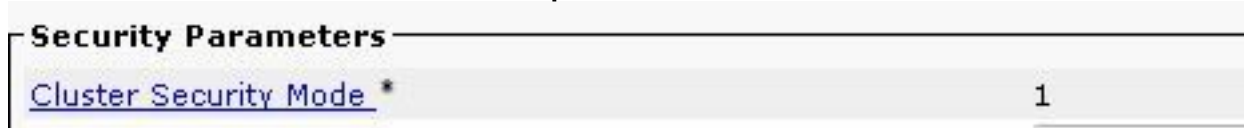
Parameters used in Phone

SIP Phone Port*

Save Delete Copy Reset Apply Config Add New

Schritt 2: Stellen Sie sicher, dass der Cluster-Sicherheitsmodus (1) - Gemischt (optional) ist.

1. Wählen Sie in CUCM System > Enterprise Parameters aus.
2. Blättern Sie nach unten zu Sicherheitsparameter > Clustersicherheitsmodus > 1.



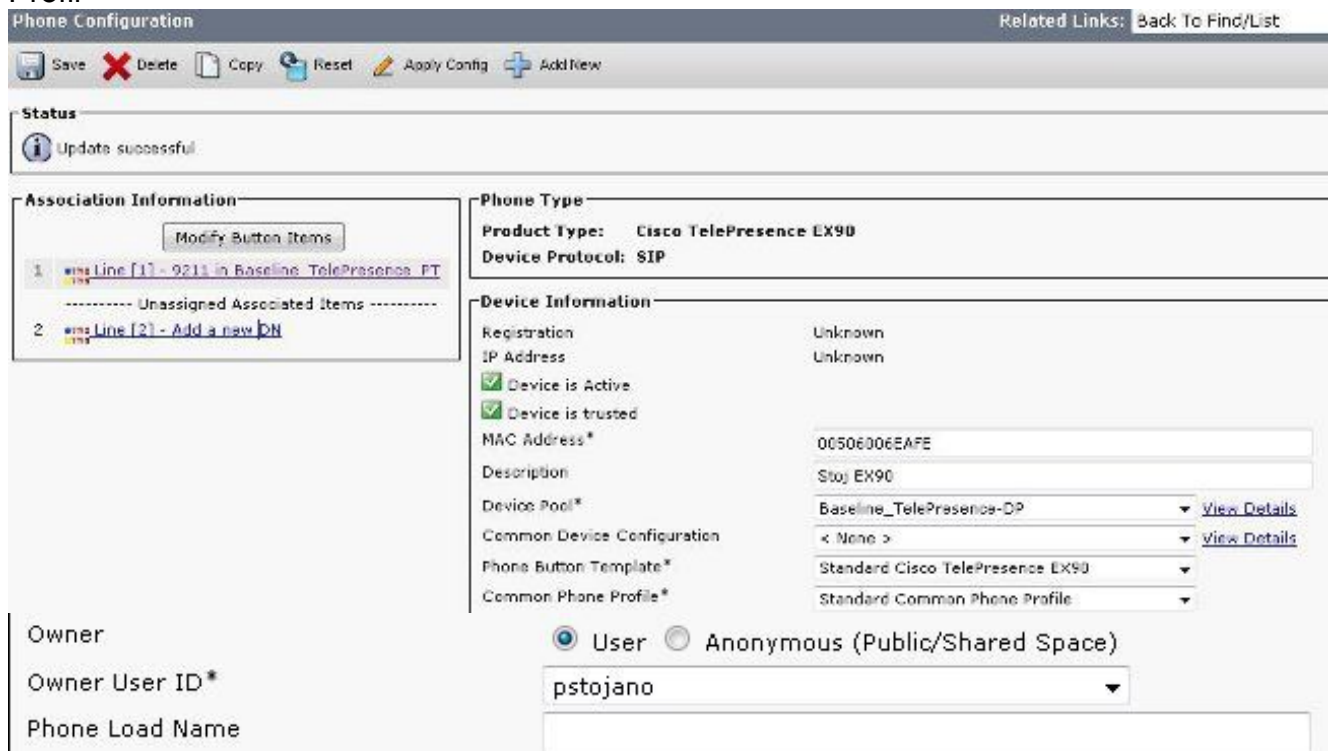
Wenn der Wert nicht 1 ist, wurde der CUCM nicht gesichert. In diesem Fall muss der Administrator eines dieser beiden Dokumente überprüfen, um den CUCM zu sichern.

[CUCM 9.1\(2\)-Sicherheitsleitfaden](#)

[CUCM 10-Sicherheitsleitfaden](#)

Schritt 3: Erstellen Sie ein Profil im CUCM für den TC-basierten Endpunkt.

1. Wählen Sie in CUCM Gerät > Telefon aus.
2. Klicken Sie auf Neu hinzufügen.
3. Wählen Sie den TC-basierten Endgerätetyp aus, und konfigurieren Sie folgende Parameter:
MAC-Adresse - MAC-Adresse des TC-basierten Geräts Pflichtfelder mit Sternchen
(*Eigentümer - BenutzerEigentümer-Benutzer-ID - Dem Gerät zugeordneter
EigentümerGerätesicherheitsprofil - Zuvor konfiguriertes Profil (Secure-EX90.tbtp.local)SIP-
Profil: Standard-SIP-Profil oder jedes zuvor erstellte benutzerdefinierte
Profil



The screenshot shows the 'Phone Configuration' page for a Cisco TelePresence EX90 device. The 'Device Information' section is expanded, showing the following configuration:

- Registration: Unknown
- IP Address: Unknown
- Device is Active:
- Device is trusted:
- MAC Address*: 00506006EAFE
- Description: Stoj EX90
- Device Pool*: Baseline_TelePresence-DP [View Details](#)
- Common Device Configuration: < None > [View Details](#)
- Phone Button Template*: Standard Cisco TelePresence EX90
- Common Phone Profile*: Standard Common Phone Profile

The 'Owner' is set to 'User' and the 'Owner User ID' is '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	

Schritt 4: Fügen Sie dem SAN des Expressway-C/VCS-C-Zertifikats den Sicherheitsprofilnamen hinzu (optional).

1. Navigieren Sie in Expressway-C/VCS-C zu **Maintenance > Security Certificates > Server Certificate**.
2. Klicken Sie auf **CSR erstellen**.
3. Füllen Sie die Felder für die Zertifikatsanforderung (Certificate Signing Request, CSR) aus, und stellen Sie sicher, dass der **Sicherheitsprofilname des Unified CM-Telefons** das genaue im Fully Qualified Domain Name (FQDN)-Format aufgelistete Telefonsicherheitsprofil aufweist. Beispielsweise **Secure-EX90.tbtp.local**. **Hinweis:** Die Sicherheitsprofilnamen für Unified CM-Telefone werden unten im Feld "Subject Alternate Name (SAN)" (Alternativer Name (SAN) für Betreff) aufgeführt.
4. Senden Sie die CSR-Anfrage an eine Zertifizierungsstelle (Internal Certificate Authority, CA) eines internen oder Drittanbieters, die unterzeichnet werden soll.
5. Wählen Sie **Maintenance > Security Certificates > Server Certificate** aus, um das Zertifikat auf Expressway-C/VCS-C hochzuladen.

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

Common name

Common name: ⓘ

Common name as it will appear: RTP-TBTP-EXPRWY-C1.tbtp.local

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.tbtp.local
 DNS:RTP-TBTP-EXPRWY-C1.tbtp.local
 DNS:RTP-TBTP-EXPRWY-C2.tbtp.local
 XMPP:conference-2-StandAloneCluster5ad9a.tbtp.local
 DNS:Secure-EX90.tbtp.local

Additional information

Key length (in bits): ⓘ

Country: ⓘ

State or province: ⓘ

Locality (town name): ⓘ

Organization (company name): ⓘ

Organizational unit: ⓘ

Schritt 5: Fügen Sie die UC-Domäne dem Expressway-E/VCS-E-Zertifikat hinzu.

1. Wählen Sie in Expressway-E/VCS-E **Maintenance > Security Certificates > Server Certificate**.
2. Klicken Sie auf **CSR erstellen**.
3. Füllen Sie die CSR-Felder aus, und stellen Sie sicher, dass die "Unified CM-Registrierungsdomänen" die Domäne enthalten, die der TC-basierte Endpunkt Collaboration Edge (Collab-Edge)-Anfragen im Format Domain Name Server (DNS) oder Service Name (SRV) stellt.
4. Senden Sie die CSR-Anfrage an eine interne CA oder eine Zertifizierungsstelle eines Drittanbieters, die unterzeichnet werden soll.
5. Wählen Sie **Maintenance > Security Certificates > Server Certificate** aus, um das Zertifikat auf Expressway-E/VCS-E hochzuladen.

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.tbtpt.local
 DNS:RTP-TBTP-EXPRWY-E1.tbtpt.local
 DNS:tbtpt.local
 SRV:_collab-edge._tls.tbtpt.local

Additional information

Key length (in bits): ⓘ

Country: ⓘ

State or province: ⓘ

Locality (town name): ⓘ

Organization (company name): ⓘ

Organizational unit: ⓘ

Schritt 6: Installieren Sie das entsprechende Zertifikat der vertrauenswürdigen Zertifizierungsstelle auf dem TC-basierten Endpunkt.

1. Wählen Sie im TC-basierten Endpunkt **Konfiguration > Sicherheit aus**.
2. Wählen Sie die Registerkarte **CA** aus, und suchen Sie nach dem Zertifizierungsstellenzertifikat, das Ihr Expressway-E/VCS-E-Zertifikat signiert hat.
3. Klicken Sie auf **Zertifizierungsstelle hinzufügen**. **Hinweis:** Sobald das Zertifikat erfolgreich hinzugefügt wurde, wird es in der Zertifikatsliste aufgeführt.

Security

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

Certificates **CA**s Preinstalled CAs 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.

Hinweis: TC 7.2 enthält eine vorinstallierte CA-Liste. Wenn die Zertifizierungsstelle, die das Expressway-E-Zertifikat signiert hat, in dieser Liste enthalten ist, sind die in diesem Abschnitt aufgeführten Schritte nicht erforderlich.

The screenshot shows the Cisco UCM Administration interface. The top navigation bar includes 'Home', 'Call Control', 'Configuration', 'Diagnostics', and 'Maintenance'. The user is logged in as 'admin'. The 'Security' section is active, with sub-tabs for 'Certificates', 'CAs', 'Preinstalled CAs', 'Strong Security Mode', 'Non-persistent Mode', and 'CUCM'. The 'Preinstalled CAs' tab is selected. Below the tabs, there is a note: 'This CA list is used for Cisco UCM via Expressway (Edge) provisioning only. Configure provisioning now.' Below this, a paragraph explains that these certificates are used to validate servers contacted over the internet. A table lists the pre-installed CAs:

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

Hinweis: Die Seite für vorinstallierte CAs enthält eine praktische Schaltfläche "Configure Provisioning now" (Jetzt bereitstellen konfigurieren), mit der Sie direkt zur erforderlichen Konfiguration gelangen, die in Schritt 2 im nächsten Abschnitt beschrieben wird.

Schritt 7: Einrichtung eines TC-basierten Endpunkts für die Edge-Bereitstellung

- Wählen Sie auf dem TC-basierten Endpunkt **Configuration > Network** (Konfiguration > Netzwerk) aus, und stellen Sie sicher, dass diese Felder unter dem DNS-Abschnitt korrekt ausgefüllt sind:
Domänenname
Serveradresse
- Wählen Sie im TC-basierten Endpunkt **Konfiguration > Bereitstellung** aus, und stellen Sie sicher, dass diese Felder korrekt ausgefüllt sind:
LoginName - wie in CUCM definiert
Modus - **Edge**
Kennwort - wie im CUCM definiert
Externer Manager
Adresse - Hostname des Expressway-E/VCS-E
Domäne: Domäne, in der Ihr Kollab-Edge-Datensatz vorhanden ist

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

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

TC-basierte Endgeräte

1. Navigieren Sie in der Web-Benutzeroberfläche zu "Startseite". Suchen Sie im Abschnitt "SIP Proxy 1" nach dem Status "Registriert". Die Proxy-Adresse ist Ihre Expressway-E/VCS-E.

SIP Proxy 1

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

2. Geben Sie in der CLI `xstatus //prov` ein. Wenn Sie registriert sind, sollte der Bereitstellungsstatus "Provisioned" (Bereitgestellt) angezeigt werden.

```
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
```

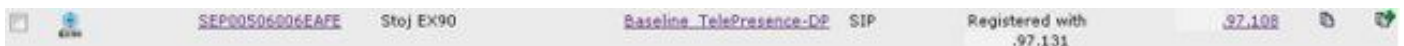
```

*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

Wählen Sie in CUCM **Gerät > Telefon aus**. Blättern Sie entweder durch die Liste, oder filtern Sie die Liste basierend auf Ihrem Endpunkt. Sie sollten die Meldung "Registriert mit %CUCM_IP%" erhalten. Die IP-Adresse rechts davon sollte Ihr Expressway-C/VCS-C sein, der die Registrierung vornimmt.



Expressway-C

- Wählen Sie in Expressway-C/VCS-C die Optionen **Status > Unified Communications > Bereitstellungssitzungen anzeigen aus**.
- Filtern Sie nach der IP-Adresse Ihres TC-basierten Endpunkts. Ein Beispiel für eine bereitgestellte Sitzung wird im Bild angezeigt:

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

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Registrierungsprobleme können durch zahlreiche Faktoren verursacht werden, z. B. DNS, Probleme mit Zertifikaten, Konfiguration usw. Dieser Abschnitt enthält eine umfassende Liste der typischen Auswirkungen eines Problems und der Möglichkeiten, dieses zu beheben. Wenn Sie auf

Probleme stoßen, die nicht mit bereits dokumentierten Inhalten verbunden sind, können Sie diese gerne einschließen.

Tools

Zunächst sollten Sie sich der Ihnen zur Verfügung stehenden Tools bewusst sein.

TC-Endpunkt

Web-Benutzeroberfläche

- all.log
- Start der erweiterten Protokollierung (einschließlich umfassender Paketerfassung)

CLI

Diese Befehle sind besonders hilfreich, um in Echtzeit eine Fehlerbehebung durchzuführen:

- log ctx HttpClient debug 9
- log ctx PROV debug 9
- Protokollausgabe bei <— Zeigt die Protokollierung über die Konsole an

Eine effektive Möglichkeit zur Wiederherstellung des Problems besteht darin, den Provisioning-Modus von "Edge" auf "Off" (Aus) und dann wieder zurück auf "Edge" (Edge) in der Web-GUI umzuschalten. Sie können auch den **xConfiguration Provisioning Mode** eingeben: in der CLI.

Expressdienste

- [Diagnoseprotokolle](#)
- TCPCDump

CUCM

- SDI/SDL Traces

Ausgabe 1: Der Collab-Edge-Datensatz ist nicht sichtbar und/oder der Hostname ist nicht auflösbar.

Wie Sie sehen können, schlägt get_edge_config aufgrund der Namensauflösung fehl.

TC-Endpunktprotokolle

```
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/
```

Problembhebung

1. Überprüfen Sie, ob der Collab-Edge-Datensatz vorhanden ist, und geben Sie den richtigen Hostnamen zurück.
2. Überprüfen Sie, ob die auf dem Client konfigurierten DNS-Serverinformationen korrekt sind.

Ausgabe 2: CA ist nicht in der Liste der vertrauenswürdigen Zertifizierungsstellen auf dem TC-basierten Endpunkt vorhanden.

TC-Endpunktprotokolle

```
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
```

Problembhebung

1. Überprüfen Sie, ob eine Drittanbieter-CA auf dem Endgerät auf der Registerkarte **Security > CAs** aufgeführt ist.
2. Wenn die CA aufgeführt ist, stellen Sie sicher, dass sie korrekt ist.

Ausgabe 3: Expressway-E hat die im SAN aufgeführte UC-Domäne nicht.

TC-Endpunktprotokolle

```
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
```

Problembhebung

1. Regeneriert Expressway-E CSR, um die UC-Domäne(n) einzuschließen.
2. Es ist möglich, dass der **ExternalManager Domain**-Parameter auf dem TC-Endpunkt nicht auf die UC-Domäne festgelegt ist. Wenn dies der Fall ist, müssen Sie es abgleichen.

Ausgabe 4: Benutzername und/oder Kennwort im TC-Bereitstellungsprofil sind falsch

TC-Endpunktprotokolle

```
83716.67 HttpClient      Server auth using Basic with user 'pstojano'
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/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"

Problembehebung

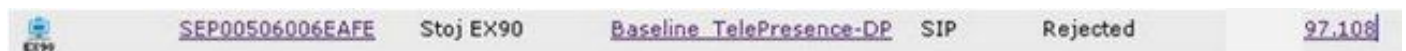
1. Überprüfen Sie, ob der Benutzername/das Kennwort, das auf der Bereitstellungsseite des TC-Endpunkts eingegeben wurde, gültig ist.
2. Überprüfen Sie die Anmeldeinformationen für die CUCM-Datenbank.
3. Version 10 - Verwenden des Self Care Portals
4. Version 9 - Verwenden der CM-Benutzeroptionen

Die URL für beide Portale ist identisch: <https://%CUCM%/ucmuser/>

Wenn ein nicht ausreichender Fehler bei den Rechten angezeigt wird, stellen Sie sicher, dass diese Rollen dem Benutzer zugewiesen sind:

- Standard-CTI aktiviert
- Standard-CCM-Endbenutzer

Ausgabe 5: TC-basierte Endpunktregistrierung wird abgelehnt



CUCM-Ablaufverfolgungen

```
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,
```

TC-Endpoint

SIP Proxy 1

Status:

Failed: 403 Forbidden

Expressway-C/VCS-C

X509v3 Subject Alternative Name:

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

In diesem spezifischen Protokollbeispiel wird deutlich, dass der Expressway-C/VCS-C das Telefon-Sicherheitsprofil FQDN im SAN nicht enthält. (Secure-EX90.tbtp.local). Im Transport Layer Security (TLS) Handshake prüft der CUCM das Serverzertifikat von Expressway-C/VCS-C. Da das Gerät im SAN nicht gefunden wird, wird der Fehler ausgeblendet und es wird berichtet, dass es das Telefon-Sicherheitsprofil im FQDN-Format erwartet hat.

Problembhebung

1. Überprüfen Sie, ob der Expressway-C/VCS-C das Telefon-Sicherheitsprofil im FQDN-Format im SAN des Serverzertifikats enthält.
2. Überprüfen Sie, ob das Gerät das richtige Sicherheitsprofil in CUCM verwendet, wenn Sie ein sicheres Profil im FQDN-Format verwenden.
3. Dies kann auch durch die Cisco Bug-ID [CSCuq86376](#) verursacht werden. In diesem Fall überprüfen Sie die SAN-Größe von Expressway-C/VCS-C und die Position des Telefon-Sicherheitsprofils im SAN.

Ausgabe 6: TC-basierte Endpunkt-Bereitstellung schlägt fehl - kein UDS-Server

Dieser Fehler muss unter **Diagnose > Fehlerbehebung** vorhanden sein:

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

TC-Endpointprotokolle

Blättern Sie nach rechts, um die fett formatierten Fehler anzuzeigen.

```
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</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!
```

Problembhebung

1. Stellen Sie sicher, dass dem Endbenutzerkonto ein Serviceprofil und ein CTI UC-Service zugeordnet sind, um die Bereitstellung von Endgeräten über MRA-Services anzufordern.
2. Navigieren Sie zu **CUCM admin> User Management> User Settings > UC Service**, und erstellen Sie einen CTI UC Service, der auf die IP-Adresse des CUCM zeigt (d. h. MRA_UC-Service).
3. Navigieren Sie zu **CUCM Admin> User Management> User Settings > Service Profile**, und erstellen Sie ein neues Profil (z. B. MRA_ServiceProfile).
4. Blättern Sie im neuen Serviceprofil zum Ende, und wählen Sie im Bereich CTI-Profil den neuen CTI UC-Service aus, den Sie gerade erstellt haben (d. h. MRA_UC-Service), und klicken Sie dann auf Speichern.
5. Navigieren Sie zu **CUCM admin> User Management > Endbenutzer**, und suchen Sie das Benutzerkonto, das zum Anfordern der Endpunktbereitstellung über MRA-Dienste verwendet wird.
6. Stellen Sie unter **Diensteinstellungen** dieses Benutzers sicher, dass der Home-Cluster aktiviert ist und dass das UC-Serviceprofil das von Ihnen erstellte neue Serviceprofil widerspiegelt (d. h. MRA_ServiceProfile), und klicken Sie dann auf Speichern.
7. Die Replikation kann einige Minuten in Anspruch nehmen. Versuchen Sie, den Bereitstellungsmodus am Endpunkt zu deaktivieren und ihn einige Minuten später wieder einzustellen, um festzustellen, ob der Endpunkt jetzt registriert wird.

Zugehörige Informationen

- [Leitfaden für Mobil- und Remote-Zugriff](#)
- [Leitfaden zur Erstellung von VCS-Zertifikaten](#)
- [EX90/EX60: Erste Schritte](#)
- [Administratoranleitung für CUCM 9.1](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)