# Lösung der häufigsten Probleme am Collaboration-Edge

## Inhalt



## Einleitung

In diesem Dokument wird die Fehlerbehebung am Collaboration Edge beschrieben. Dies sind die häufigsten Probleme, mit denen Kunden während der Bereitstellungsphase konfrontiert sind.

# Hintergrundinformationen

Mobile & Remote Access (MRA) ist eine Bereitstellungslösung für Jabber ohne Virtual Private Network (VPN). Mit dieser Lösung können Endbenutzer von einem beliebigen Standort weltweit auf interne Unternehmensressourcen zugreifen. Dieser Leitfaden wurde verfasst, um Technikern, die Probleme mit der Collaboration Edge-Lösung beheben, die Möglichkeit zu geben, die häufigsten Probleme, mit denen Kunden während der Bereitstellung konfrontiert werden, schnell zu identifizieren und zu beheben.

# Voraussetzungen

## Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Unified Communications Manager (CUCM)
- Cisco Expressway Core
- Cisco Expressway-Edge
- Cisco IM und Presence (IM&P)
- Cisco Jabber für Windows
- Cisco Jabber für MAC
- Cisco Jabber für Android
- Cisco Jabber für iOS
- Sicherheitszertifikate
- Domain Name System (DNS)

## Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Expressway-Version X8.1.1 oder spätere Version
- CUCM Version 9.1(2)SU1 oder höher und IM&P Version 9.1(1) oder höher
- Cisco Jabber Version 9.7 oder höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

# Probleme bei der Anmeldung

## Jabber kann sich nicht über MRA anmelden

Dieses Symptom kann durch eine Vielzahl von Problemen verursacht werden, von denen einige

hier erläutert werden.

### 1. Collaboration Edge Service Record (SRV) nicht erstellt und/oder Port 8443 nicht erreichbar

Damit sich ein Jabber-Client erfolgreich mit MRA anmelden kann, muss ein spezifischer SRV-Datensatz für das Collaboration-Edge erstellt werden, auf den extern zugegriffen werden kann. Beim Start eines Jabber-Clients werden DNS SRV-Abfragen ausgeführt:

1. **_cisco-uds**: Dieser SRV-Datensatz wird verwendet, um zu bestimmen, ob ein CUCM-Server verfügbar ist.

2. **_cuplogin**: Dieser SRV-Datensatz wird verwendet, um festzustellen, ob ein IM&P-Server verfügbar ist.

3. **_collab-edge**: Dieser SRV-Datensatz wird verwendet, um festzustellen, ob MRA verfügbar ist.

Wenn der Jabber-Client gestartet wird und keine SRV-Antwort für **_cisco-uds** und **_cuplogin** erhält und **keine** Antwort für **_collab-edge** erhält, verwendet er diese Antwort, um den in der SRV-Antwort aufgeführten Expressway-E zu kontaktieren.

Der SRV-Datensatz **_collab-edge** verweist auf den vollqualifizierten Domänennamen (FQDN) von Expressway-E mit Port **8443**. Wenn die **_collab-edge** SRV nicht erstellt wurde, nicht extern verfügbar ist oder verfügbar ist, Port 8443 jedoch nicht erreichbar ist, meldet sich der Jabber-Client nicht an.

Mit dem SRV Checker im Collaboration Solutions Analyzer (CSA) können Sie überprüfen, ob der SRV-Datensatz von **_collab-edge auflösbar** und der TCP-Port 8443 erreichbar ist.

Wenn Port 8443 nicht erreichbar ist, liegt dies möglicherweise daran, dass ein Sicherheitsgerät (Firewall) den Port blockiert oder das Standard-Gateway (GW) oder die statischen Routen in Exp-E falsch konfiguriert wurden.

### 2. Unzulässiges oder kein verfügbares Zertifikat auf VCS Expressway

Nachdem der Jabber-Client die Antwort für **_collab-edge** erhalten hat, kontaktiert er Expressway mit Transport Layer Security (TLS) über Port 8443, um das Zertifikat von Expressway abzurufen und TLS für die Kommunikation zwischen dem Jabber-Client und Expressway einzurichten.

Wenn Expressway kein gültiges signiertes Zertifikat besitzt, das entweder den FQDN oder die Domäne von Expressway enthält, schlägt dies fehl, und der Jabber-Client meldet sich nicht an.

Wenn dieses Problem auftritt, verwenden Sie das CSR-Tool (Certificate Signing Request) auf Expressway, das automatisch den FQDN von Expressway als Subject Alternative Name (SAN) enthält.

> **Hinweis**: Die MRA erfordert eine sichere Kommunikation zwischen Expressway-C und Expressway-E sowie zwischen Expressway-E und externen Endpunkten.

Die nächste Tabelle mit den Expressway-Zertifikatanforderungen nach Funktion finden Sie im

MRA-Bereitstellungsleitfaden:

**Table 1. CSR Alternative Name Element and Unified Communications Features**

| Add These Items as Subject Alternative Names | When Generating a CSR for These Purposes | | | |
|---|---|---|---|---|
| | Mobile and Remote Sccess | Jabber guest | XMPP Federation | Business to Business Calls |
| Unified CM registrations domains (despite their name, these have more in common with service discovery domains than with Unified CM Unified CM SIP registration domains) | Required on Expressway-E only | – | – | – |
| XMPP federation domains | – | – | Required on Expressway-E only | – |
| IM and Presence Service chat node aliases (federated group chat) | – | – | Required | – |
| Unified CM phone security profile names | Required on Expressway-C only | – | – | – |
| (Clustered systems only) Expressway cluster name | Required on Expressway-C only | Required on Expressway-C only | Required on Expressway-C only | |

### 3. Keine UDS-Server in Edge-Konfiguration gefunden

Nachdem der Jabber-Client erfolgreich eine sichere Verbindung mit Expressway-E hergestellt hat, fragt er nach seiner Edge-Konfiguration (**get_edge_config**). Diese Edge-Konfiguration enthält die SRV-Datensätze für **_cuplogin** und **_cisco-uds**. Wenn die SRV-Einträge **_cisco-uds** nicht in der Edge-Konfiguration zurückgegeben werden, kann der Jabber-Client die Anmeldung nicht fortsetzen.

Um dies zu beheben, stellen Sie sicher, dass **_cisco-uds** SRV-Datensätze intern erstellt und von Expressway-C aufgelöst werden können.

Weitere Informationen zu den DNS SRV-Einträgen finden Sie im MRA-Bereitstellungsleitfaden für X8.11.

Dies ist auch ein häufiges Symptom, wenn Sie sich in einer Dual-Domain. Wenn Sie in einer dualen Domäne ausführen und feststellen, dass der Jabber-Client keinen User Data Service (UDS) zurückgibt, müssen Sie bestätigen, dass die SRV-Einträge _cisco-uds im internen DNS mit der externen Domäne erstellt wurden.

> **Hinweis**: Nach der Expressway-Version X12.5 ist es nicht mehr erforderlich, dem internen DNS einen _cisco-UDS SRV-Eintrag hinzuzufügen. Weitere Informationen zu dieser Erweiterung finden Sie im Mobile and Remote Access Through Cisco Expressway Deployment Guide (X12.5).

### 4. Expressway-C-Protokolle zeigen diesen Fehler an: XCP_JABBERD Detail=Es konnte keine Verbindung mit dem Host "%IP%" hergestellt werden, Port 7400:(111) Verbindung verweigert

Wenn der Expressway-E Network Interface Controller (NIC) falsch konfiguriert ist, kann dies dazu führen, dass der XCP-Server (Extensible Communications Platform) nicht aktualisiert wird. Wenn Expressway-E diese Kriterien erfüllt, liegt wahrscheinlich folgendes Problem vor:

1. Verwendet eine einzelne NIC.
2. Der erweiterte Netzwerkoptionschlüssel ist installiert.
3. Die Option "Dual Network Interfaces verwenden" ist auf **Ja** eingestellt.

Um dieses Problem zu beheben, ändern Sie die Option "Duale Netzwerkschnittstellen verwenden" in "**Nein**".

Der Grund für dieses Problem ist, dass Expressway-E die XCP-Sitzung auf der falschen Netzwerkschnittstelle abhört, was dazu führt, dass die Verbindung ausfällt/ausfällt. Expressway-E hört den TCP-Port 7400 für die XCP-Sitzung ab. Sie können dies überprüfen, wenn Sie das netstatvom VCS als root aus.

### 5. Expressway-E Server-Hostname/Domänenname stimmt nicht mit der Konfiguration in der SRV _collab-edge überein

Wenn der Hostname/die Domäne des Expressway-E-Servers in der DNS-Seitenkonfiguration nicht mit dem übereinstimmt, was in der SRV-Antwort **_collab-edge** empfangen wurde, kann der Jabber-Client nicht mit Expressway-E kommunizieren. Der Jabber-Client verwendet das Element "xmppEdgeServer/Address" in der Antwort "**get_edge_config**", um die XMPP-Verbindung mit Expressway-E herzustellen.

Dies ist ein Beispiel dafür, wie xmppEdgeServer/Address in der Antwort **get_edge_config** von Expressway-E an den Jabber-Client aussieht:

```
<xmppEdgeServer>
<server>
<address>examplelab-vcse1.example URL</address>
<tlsPort>5222</tlsPort>
</server>
</xmppEdgeServer>
```

Um dies zu vermeiden, stellen Sie sicher, dass der SRV-Datensatz **_collab-edge** mit dem Expressway-E-Hostnamen/Domänennamen übereinstimmt. Die Cisco Bug-ID CSCuo83458 wurde dafür abgelegt, und die Cisco Bug-ID CSCuo82526 wurde um einen Teil der Unterstützung ergänzt.

### 6. Anmeldung aufgrund eines aktuellen WebEx Connect-Abonnements nicht möglich

Die Protokolle von Jabber für Windows zeigen Folgendes an:

```
2014-11-22 19:55:39,122 INFO  [0x00002808] [very\WebexCasLookupDirectorImpl.cpp(134)]
[service-discovery] [WebexCasLookupDirectorImpl::makeCasLookupWhenNetworkIs
Available] - makeCasLookupForDomain result is 'Code: IS_WEBEX_CUSTOMER; Server:
http://URL server;
Url: http://example URL server';;;.2014-11-22
19:55:39,122 INFO [0x00002808] [overy\WebexCasLookupDirectorImpl.cpp(67)]
[service-discovery] [WebexCasLookupDirectorImpl::determineIsWebexCustomer] -
Discovered Webex Result from server. Returning server result.2014-11-22 19:55:39,122
DEBUG [0x00002808] [ery\WebexCasLookupUrlConfigImpl.cpp(102)]
[service-discovery] [WebexCasLookupUrlConfigImpl::setLastCasUrl] - setting last_cas_
lookup_url : http://example URL server2014-11-22
19:55:39,123 DEBUG [0x00002808] [pters\config\ConfigStoreManager.cpp(286)]
[ConfigStoreManager] [ConfigStoreManager::storeValue] - key : [last_cas_lookup_url]
value : [http://example URL server/cas/FederatedSSO?org=example URL]2014-11-22
19:55:39,123 DEBUG [0x00002808] [common\processing\TaskDispatcher.cpp(29)]
[TaskDispatcher] [Processing::TaskDispatcher::enqueue] - Enqueue ConfigStore::persist
Values - Queue Size: 02014-11-22 19:55:39,123 DEBUG [0x00002808] [pters\config\ConfigStore
Manager.cpp(140)]
[ConfigStoreManager] [ConfigStoreManager::getValue] - key : [last_cas_lookup_url]
skipLocal : [0] value: [http://website URL/cas/FederatedSSO?org=example URL]
success: [true] configStoreName: [LocalFileConfigStore]
```

Die Anmeldeversuche werden an WebEx Connect weitergeleitet.

Um eine dauerhafte Lösung zu erhalten, müssen Sie sich an WebEx wenden, damit der Standort außer Betrieb genommen werden kann.

### Problemumgehung

Kurzfristig können Sie eine dieser Optionen nutzen, um sie von der Suche auszuschließen.

- Fügen Sie diesen Parameter der Datei jabber-config.xml hinzu. Laden Sie dann die Datei "jabber-config.xml" auf den TFTP-Server auf CUCM hoch. Dazu muss sich der Client zuerst intern anmelden.

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
<Policies>
<ServiceDiscoveryExcludedServices>WEBEX<
/ServiceDiscoveryExcludedServices>
</Policies>
</config>
```

- Führen Sie aus Anwendungsperspektive Folgendes aus:
**msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=CUP EXCLUDED_SERVICES=WEBEX**

  **Hinweis**: Die zweite Option funktioniert nicht für Mobilgeräte.

- Erstellen Sie eine klickbare URL, die den WEBEX-Dienst ausschließt:
**ciscojabber://provision?ServiceDiscoveryExcludedServices=WEBEX**

Weitere Informationen zur UC-Serviceerkennung und zum Ausschluss bestimmter Services finden Sie unter "Bereitstellung am Standort für Cisco Jabber 12.8".

### 7. Der Expressway-C Server zeigt die Fehlermeldung "Konfiguriert, aber mit Fehlern. Bereitstellungsserver: Wartet auf Traversal-Serverinformationen."

Wenn Sie zu Status > Unified Communications navigieren und die Fehlermeldung angezeigt wird, "Configured but with errors. Provisioning server: Waiting for traversal server info." für Unified CM-Registrierungen und IM&P Service verfügen die auf dem Expressway-C konfigurierten internen DNS-Server über zwei DNS A-Einträge für den Expressway-E. Der Grund für mehrere DNS-A-Einträge für den Expressway-E kann sein, dass der betroffene Benutzer von einer einzelnen Netzwerkkarte mit aktivierter statischer NAT auf dem Expressway-E zu einer dualen Netzwerkkarte mit aktivierter statischer NAT oder umgekehrt verschoben und vergessen hat, den entsprechenden DNS-A-Eintrag in den internen DNS-Servern zu löschen. Wenn Sie daher das DNS-Lookup-Utility im Expressway-C verwenden und den FQDN des Expressway-E auflösen, stellen Sie zwei DNS A-Einträge fest.

### Lösung

Wenn die Expressway-E-Netzwerkkarte für eine einzelne Netzwerkkarte mit statischer NAT konfiguriert ist:

1. Löschen Sie den DNS-A-Eintrag für die interne IP-Adresse des Expressway-E in den DNS-Server(n), die in Expressway-C konfiguriert wurden.
2. Löschen Sie den DNS-Cache im Expressway-C und dem Benutzer-PC per CMD (ipconfig /flushdns).
3. Starten Sie den Expressway-C-Server neu.

Wenn die Expressway-E-Netzwerkkarte für eine duale Netzwerkkarte mit aktivierter statischer NAT konfiguriert ist:

1. Löschen Sie den DNS-A-Eintrag für die *externe* IP-Adresse Expressway-E in den DNS-Server(n), die in Expressway-C konfiguriert sind.
2. Löschen Sie den DNS-Cache im Expressway-C und Benutzer-PC per CMD (ipconfig /flushdns).
3. Starten Sie den Expressway-C-Server neu.

### 8. Microsoft DirectAccess installiert

Wenn der Kunde Microsoft DirectAccess auf demselben PC wie den Jabber-Client verwendet und versucht, sich remote anzumelden, kann dies die MRA unterbrechen. DirectAccess erzwingt, dass DNS-Abfragen in das interne Netzwerk getunnelt werden, als ob der PC ein VPN verwendet.

> **Hinweis**: Microsoft DirectAccess wird bei Jabber over MRA nicht unterstützt. Jede Fehlerbehebung ist bestmöglich. Die Konfiguration von DirectAccess unterliegt der Verantwortung des Netzwerkadministrators.

Einige Kunden haben erfolgreich alle DNS-Einträge in der Richtlinientabelle für die Namensauflösung von Microsoft DirectAccess blockiert. Diese Datensätze werden nicht von DirectAccess verarbeitet (Jabber muss in der Lage sein, diese über öffentliche DNS mit MRA aufzulösen):

- SRV-Eintrag für _cisco-uds
- SRV-Datensatz für _cuplogin
- SRV-Eintrag für _collab-edge
- Ein Rekord für alle Expressway Es

### 9. Expressway Reverse DNS-Suche schlägt fehl

Ab Version X8.8 müssen für Expressway/VCS Vorwärts- und Rückwärts-DNS-Einträge für ExpE-, ExpC- und alle CUCM-Knoten erstellt werden.

Die vollständigen Anforderungen finden Sie unter Voraussetzungen und Softwareabhängigkeiten in den x8.8-Versionshinweisen und DNS-Datensätzen für Mobil- und Remote-Zugriff.

Wenn keine internen DNS-Einträge vorhanden sind, kann es in den Expressway-Protokollen zu einem Fehler kommen, der auf reverseDNSLookup verweist:

2016-07-30T13:58:11.102-06:00 hostname XCP_JABBERD[20026]: UTCTime="2016-07-30 19:58:11,102" ThreadID="139882696623872" Module="Jabber" Level="WARN " CodeLocation="cvsservice.cpp:409" Detail="caught exception: exception in reverseDNSLookup: reverse DNS lookup failed for address=x.x.x.x"

Expressway-C erhält nur einen FQDN, wenn der PTR-Datensatz für die Expressway-E IP abgefragt wird. Wenn ein falscher FQDN vom DNS empfangen wird, wird diese Zeile in den Protokollen angezeigt, und es wird ein Fehler ausgegeben:

2020-04-03T17:48:43.685-04:00 hostname XCP_JABBERD[10043]: UTCTime="2020-04-03 21:48:43,685" ThreadID="140028119959296" Module="Jabber" Level="WARN " CodeLocation="cvsservice.cpp:601" Detail="Certificate verification failed for host=xx.xx.xx.xx, additional info: Invalid Hostname"

# Probleme bei der Registrierung

## Softphone kann nicht registriert werden, SIP/2.0 405-Methode nicht zulässig

Ein Diagnoseprotokoll von Expressway-C zeigt ein **SIP/2.0 405 Method Not Allowed** als Antwort auf die vom Jabber-Client gesendete Registrierungsanfrage. Dies ist wahrscheinlich auf einen aktuellen SIP-Trunk (Session Initiation Protocol) zwischen Expressway-C und CUCM mit Port 5060/5061 zurückzuführen.

```
SIP/2.0 405 Method Not Allowed
Via: SIP/2.0/TCP 10.10.40.108:5060;egress-zone=CollabZone;branch=z9hG4bK81e7f5f1c1
ab5450c0b406c91fcbdf181249.81ba6621f0f43eb4f9c0dc0db83fb291;proxy-call-id=da9e25aa-
80de-4523-b9bc-be31ee1328ce;rport,SIP/2.0/TLS 10.10.200.68:7001;egress-zone=Traversal
Zone;branch=z9hG4bK55fc42260aa6a2e3741919177aa84141920.a504aa862a5e99ae796914e85d35
27fe;proxy-call-id=6e43b657-d409-489c-9064-3787fc4919b8;received=10.10.200.68;rport=
7001;ingress-zone=TraversalZone,SIP/2.0/TLS
192.168.1.162:50784;branch=z9hG4bK3a04bdf3;received=172.18.105.10;rport=50784;
ingress-zone=CollaborationEdgeZone
From: <sip:5151@collabzone>;tag=cb5c78b12b4401ec236e1642-1077593a
To: <sip:5151@collabzone>;tag=981335114
Date: Mon, 19 Jan 2015 21:47:08 GMT
Call-ID: cb5c78b1-2b4401d7-26010f99-0fa7194d@192.168.1.162
Server: Cisco-CUCM10.5
CSeq: 1105 REGISTER
Warning: 399 collabzone "SIP trunk disallows REGISTER"
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
Content-Length: 0
```

Um dieses Problem zu beheben, ändern Sie den SIP-Port des SIP-Trunk-Sicherheitsprofils, der auf den aktuellen, im CUCM konfigurierten SIP-Trunk und die CUCM-Expressway-C-Nachbarzone angewendet wird, in einen anderen Port, z. B. 5065. Dies wird in diesem Video weiter erläutert. Nachfolgend finden Sie eine Konfigurationsübersicht:

### CUCM

1. Erstellen Sie ein neues SIP-Trunk-Sicherheitsprofil mit einem Überwachungsport, der nicht 5060 (5065) ist.
2. Erstellen Sie einen SIP-Trunk, der mit dem SIP-Trunk-Sicherheitsprofil verknüpft ist, und legen Sie als Ziel die Expressway-C IP-Adresse, Port 5060, fest.

### Schnellstraße C

1. Erstellen Sie eine Nachbarzone zu CUCM(s) mit einem anderen Zielport als 5060 (5065), um die CUCM-Konfiguration zu übernehmen.
2. Stellen Sie unter Expressway-C **Settings > Protocols > SIP** sicher, dass Expressway-C weiterhin auf 5060 auf SIP wartet.

## Softphone kann sich nicht registrieren, Grund="Unknown domain"

Ein Diagnoseprotokoll von Expressway-C zeigt Event= an.**"Registration Rejected" Reason="Unknown domain"** Service="SIP" Src-ip="XXX.XXX.XXX" Src-port="51601" Protocol="TCP" AOR="sip:XXX.XXX.XXX.XXX".

Um dieses Problem zu beheben, überprüfen Sie folgende Punkte:

- Verwendet der Jabber-Client ein **Secure Device Security-Profil** in CUCM, wenn nicht beabsichtigt ist, ein nicht sicheres Gerätesicherheitsprofil zu verwenden?

- Wenn die Jabber-Clients ein sicheres Gerätesicherheitsprofil verwenden, ist dann der Name des Sicherheitsprofils im FQDN-Format angegeben, und ist dieser FQDN-Name im Expressway-C-Zertifikat als SAN konfiguriert?

- Wenn die Jabber-Clients ein gesichertes Gerätesicherheitsprofil verwenden, navigieren Sie zu **System > Enterprise Parameters > Security Parameters > Cluster Security Mode,** und überprüfen Sie, ob der Cluster Security Mode (Cluster-Sicherheitsmodus) auf 1 gesetzt ist, um sicherzustellen, dass der CUCM-Cluster gesichert wurde. Wenn der Wert **0** ist, muss der Administrator das dokumentierte Verfahren durchlaufen, um den Cluster zu sichern.

## Softphone kann sich nicht registrieren, Grund "Idle countdown expired"

Wenn Sie die Expressway-E-Protokolle während des Zeitraums überprüfen, den der Jabber-Client in einer REGISTER-Nachricht sendet, suchen Sie nach einem **Idle countdown expired** Fehler, wie im Codeausschnitt hier angegeben.

```
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"
Module="network.tcp" Level="DEBUG": Src-ip="JabberPubIP" Src-port="4211"
Dst-ip="VCS-E_IP" Dst-port="5061" Detail="TCP Connecting"
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"
Module="network.tcp" Level="DEBUG": Src-ip="JabberPubIP" Src-port="4211" Dst-ip=
"VCS-E_IP" Dst-port="5061" Detail="TCP Connection Established"2015-02-02T19:46:49+01:00
collabedge tvcs: UTCTime="2015-02-02 18:46:49,606"
Module="network.tcp" Level="DEBUG": Src-port="4211" Dst-ip=
"VCS-E_IP" Dst-port="5061" Detail="TCP Connection Closed" Reason="Idle
countdown expired"
```

Dieser Ausschnitt weist darauf hin, dass die Firewall über einen offenen Port 5061 verfügt. Es wird jedoch kein Datenverkehr auf Anwendungsebene über diesen Port weitergeleitet, sodass die TCP-Verbindung geschlossen wird.

Wenn Sie auf diese Situation stoßen, ist es sehr wahrscheinlich, dass die SIP-Inspection-/Application Layer Gateway (ALG)-Funktion auf der Firewall vor Expressway-E aktiviert ist. Um dieses Problem zu beheben, müssen Sie diese Funktion deaktivieren. Wenn Sie sich nicht sicher sind, wie Sie vorgehen sollen, lesen Sie in der Produktdokumentation Ihres Firewall-Anbieters nach.

Weitere Informationen zu SIP Inspection/ALG finden Sie in Anhang 4 des Cisco Expressway-E und Expressway-C-Basic Configuration Deployment Guide.

## MRA schlägt aufgrund eines in der Firmware konfigurierten Telefonproxys fehl

Ein Diagnoseprotokoll vom Expressway-E zeigt einen TLS-Aushandlungsfehler in Port 5061, jedoch war der SSL-Handshake in Port 8443 erfolgreich.

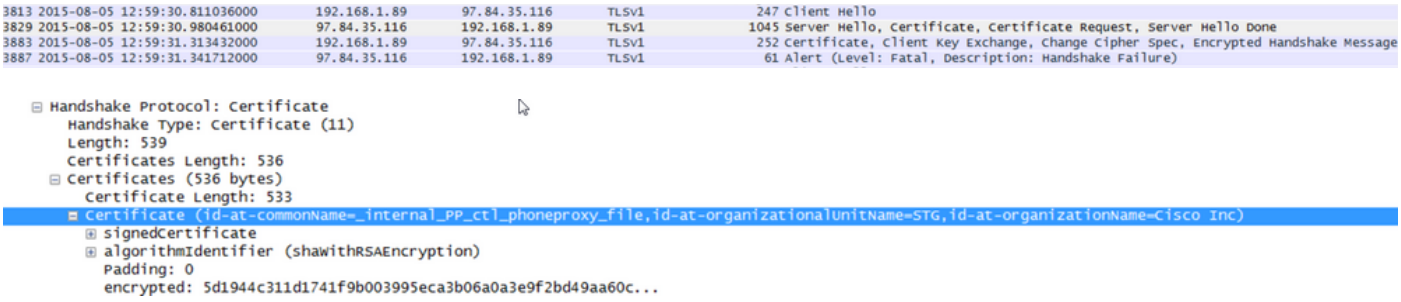
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,533" Module="network.tcp" Level="DEBUG": Src-port="24646" Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connecting"
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,534" Module="network.tcp" Level="DEBUG": Src-port="24646" Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connection Established"
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,535" Module="developer.ssl" Level="ERROR"

CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(67)" Method="::TTSSLErrorOutput" Thread="0x7fae4ddb1700": TTSSL_continueHandshake: Failed to establish SSL connection
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,535" Module="network.tcp" Level="DEBUG": Src-port="24646" Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connection Closed" Reason="Got EOF on socket"
2015-08-04T10:14:23-05:00 expe tvcs: Event="Inbound TLS Negotiation Error" Service="SIP" Src-port="24646" Dst-ip="10.2.0.2" Dst-port="5061" Detail="No SSL error available, probably remote disconnect" Protocol="TLS" Level="1" UTCTime="2015-08-04 15:14:23,535"

Protokolle von Jabber:

-- 2015-08-04 10:48:04.775 ERROR [ad95000] - [csf.cert.][checkIdentifiers] Verification of identity: 'URL address' failed.
-- 2015-08-04 10:48:04.777 INFO [ad95000] - [csf.cert][handlePlatformVerificationResultSynchronously] Verification result : FAILURE reason : [CN_NO_MATCH UNKNOWN]
-- 2015-08-04 10:48:05.284 WARNING [ad95000] - [csf.ecc.handyiron][ssl_state_callback] SSL alert read:fatal:handshake failure
type=eSIP, isRelevant=true, server=URL server name:5061, connectionState=eFailed, isEncrypted=true, failureReason=eTLSFailure, SSLErrorCode=336151568
type=eSIP, isRelevant=true, server=192.168.102.253:5060, connectionState=eFailed, isEncrypted=false, failureReason=eFailedToConnect, serverType=ePrimary, role=eNone
-- 2015-08-04 10:48:05.287 ERROR [ad95000] - [csf.ecc.handyiron][secSSLIsConnected] SSL_do_handshake() returned : SSL_ERROR_SSL.

Die Paketerfassung von Jabber zeigt eine SSL-Verhandlung mit der Expressway E IP; das gesendete Zertifikat stammt jedoch nicht von diesem Server:




Für die Firewall ist Telefon-Proxy konfiguriert.

**Lösung:**

Bestätigen Sie, dass die FW den Telefonproxy ausführt. Um dies zu überprüfen, geben Sie den **show run policy-map** -Befehls und zeigt Ihnen etwas Ähnliches an:

```
class sec_sip
inspect sip phone-proxy ASA-phone-proxy
```

Deaktivieren Sie den Telefonproxy, damit die Telefondienste erfolgreich verbunden werden können.

# Probleme im Zusammenhang mit Anrufen

## Kein Medium bei einem Anruf über MRA

Nachfolgend sind einige der fehlenden und falschen Konfigurationen aufgeführt, die dieses Problem bei Bereitstellungen mit einer oder zwei NICs verursachen können:

- Static NAT ist auf dem Expressway E unter System > Network Interfaces > IP nicht konfiguriert. NAT auf Netzwerkebene muss weiterhin über die Firewall erfolgen, diese

Einstellung übersetzt jedoch die IP auf Anwendungsebene.
- TCP-/UDP-Ports sind in der Firewall nicht geöffnet. Eine Liste der Ports finden Sie im Cisco Expressway IP Port Usage Configuration Guide.

Eine einzelne NIC mit statischen NAT-Bereitstellungen wird nicht empfohlen. Folgende Überlegungen sollten Sie beachten, um Medienprobleme zu vermeiden:

fehlend

- In der UC-Überbrückungszone muss Expressway-C auf die im Expressway-E konfigurierte öffentliche IP-Adresse verweisen.
- Die Medien müssen in der externen Firewall "hairpin" sein oder reflektiert werden. Ein Konfigurationsbeispiel mit einer Cisco ASA-Firewall finden Sie unter Konfigurieren der NAT-Reflektion auf der ASA für die VCS Expressway-TelePresence-Geräte.

Weitere Informationen hierzu finden Sie in Anhang 4 des Cisco Expressway-E und Expressway-C Basic Configuration Deployment Guide.

### Kein Rückruf bei Anruf über MRA an PSTN

Dieses Problem ist auf eine Beschränkung von Expressways vor der Version X8.5 zurückzuführen. Cisco Bug-ID CSCua72781 beschreibt, wie Expressway-C keine Early Media in 183 Session Progress oder 180 Ringing über die Traversal-Zone weiterleitet. Wenn Sie die Versionen X8.1.x oder X8.2.x ausführen, können Sie auf Version X8.5 aktualisieren oder alternativ die hier aufgelistete Problemumgehung durchführen.

Sie können eine Problemumgehung für das Cisco Unified Border Element (CUBE) verwenden, wenn Sie ein SIP-Profil erstellen, das die 183 in eine 180 umwandelt und auf den eingehenden Dial-Peer anwendet. Beispiele:

```
voice class sip-profiles 11
response 183 sip-header SIP-StatusLine modify "SIP/2.0 183 Session Progress"
"SIP/2.0 180 Ringing"
```

Anschließend wurden 180 Early Media entweder auf dem SIP-Profil von **CUCM > CUBE** oder auf dem CUBE selbst im SIP-UA-Konfigurationsmodus deaktiviert.

```
disable-early-media 180
```

## Probleme mit CUCM und IM&P

### ASCII-Fehler, der das Hinzufügen von CUCM verhindert

Wenn Sie CUCM zu Expressway-C hinzufügen, tritt ein ASCII-Fehler auf, der das Hinzufügen von CUCM verhindert.

Wenn Expressway-C CUCM zu seiner Datenbank hinzufügt, durchläuft es eine Reihe von AXL-Abfragen, die sich auf die get- und list-Funktionen beziehen. Beispiele hierfür sind getCallManager, **listCallManager**, **listProcessNode**, **listProcessNodeService** und **getCCMVersion**. Nachdem der **getCallManager-**Prozess ausgeführt wurde, wird ein **ExecuteSQLQuery-**Wert festgelegt, der den Abruf aller CUCM-Vertrauensstellungen für Call Manager oder Tomcat-

Vertrauensstellungen ermöglicht.

Sobald CUCM die Abfrage empfängt und für sie ausführt, meldet er alle seine Zertifikate zurück. Wenn eines der Zertifikate ein Nicht-ASCII-Zeichen enthält, generiert Expressway einen Fehler in der Webschnittstelle, ähnlich wie ascii codec can't decode byte 0xc3 in position 42487: ordinal not in range(128).

Dieses Problem wird mit der Cisco Bug-ID CSCuo5489 verfolgt und in Version X8.2 behoben.

### Ausgehende TLS-Fehler bei 5061 von Expressway-C an CUCM bei sicheren Bereitstellungen

Dieses Problem tritt auf, wenn Sie selbstsignierte Zertifikate für CUCM verwenden und Tomcat.pem/CallManager.pem dasselbe Thema hat. Das Problem wird mit der Cisco Bug-ID CSCun30200 behoben. Die Problemumgehung besteht darin, die Datei tomcat.pem zu löschen und TLS Verify in der CUCM-Konfiguration auf Expressway-C zu deaktivieren.

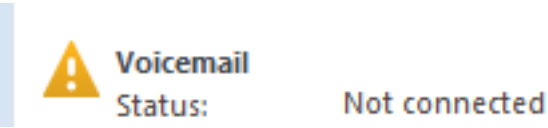
### IM&P-Server nicht hinzugefügt und Fehler aufgetreten

Wenn Sie einen IM&P-Server hinzufügen, meldet Expressway-C "Dieser Server ist kein IM- und Presence-Server" oder "Kommunikation mit dem HTTP-Fehler "HTTPError:500" bei der AXL-Abfrage nicht möglich", sodass der IM&P-Server nicht hinzugefügt wird.

Expressway-C verwendet im Rahmen der Hinzufügung eines IM&P-Servers eine AXL-Abfrage, um die IM&P-Zertifikate in einem expliziten Verzeichnis zu suchen. Aufgrund der Cisco Bug-ID CSCul05131 befinden sich die Zertifikate nicht in diesem Speicher. Daher tritt der Fehler false auf.

## Verschiedene Probleme

### Voicemail-Status auf Jabber-Client zeigt "Nicht verbunden" an




Damit der Jabber-Client-Voicemail-Status erfolgreich verbunden werden kann, müssen Sie die IP-Adresse oder den Hostnamen von Cisco Unity Connection in der HTTP-Zulassungsliste auf Expressway-C konfigurieren.

Führen Sie das entsprechende Verfahren durch, um dies über Expressway-C abzuschließen:

**Vorgehensweise für die Versionen X8.1 und X8.2**

1. Klicken Sie auf **Configuration > Unified Communications > Configuration > Configure HTTP Server allow list**.
2. Klicken Sie auf **Neu > IP/Hostname eingeben > Eintrag erstellen**.
3. Melden Sie sich vom Jabber-Client ab, und melden Sie sich dann wieder an.

**Vorgehensweise für Version X8.5**

1. Klicken Sie auf **Configuration > Unified Communications > Unity Connection Servers**.
2. Klicken Sie auf **Neu > IP/Hostname eingeben, Anmeldeinformationen für Benutzerkonto >**

**Adresse hinzufügen**.
3. Melden Sie sich vom Jabber-Client ab, und melden Sie sich dann wieder an.

## Kontaktfotos werden nicht über Expressways auf Jabber-Clients angezeigt

Die Mobile & Remote Access-Lösung nutzt nur UDS zur Auflösung von Kontaktfotos. Hierfür muss ein Webserver zum Speichern der Fotos verfügbar sein. Die Konfiguration selbst ist zweifach.

1. Die Datei "jabber-config.xml" muss geändert werden, damit die Clients zur Auflösung von Kontaktfotos an den Webserver weitergeleitet werden können. Dies wird durch die hier gezeigte Konfiguration erreicht.

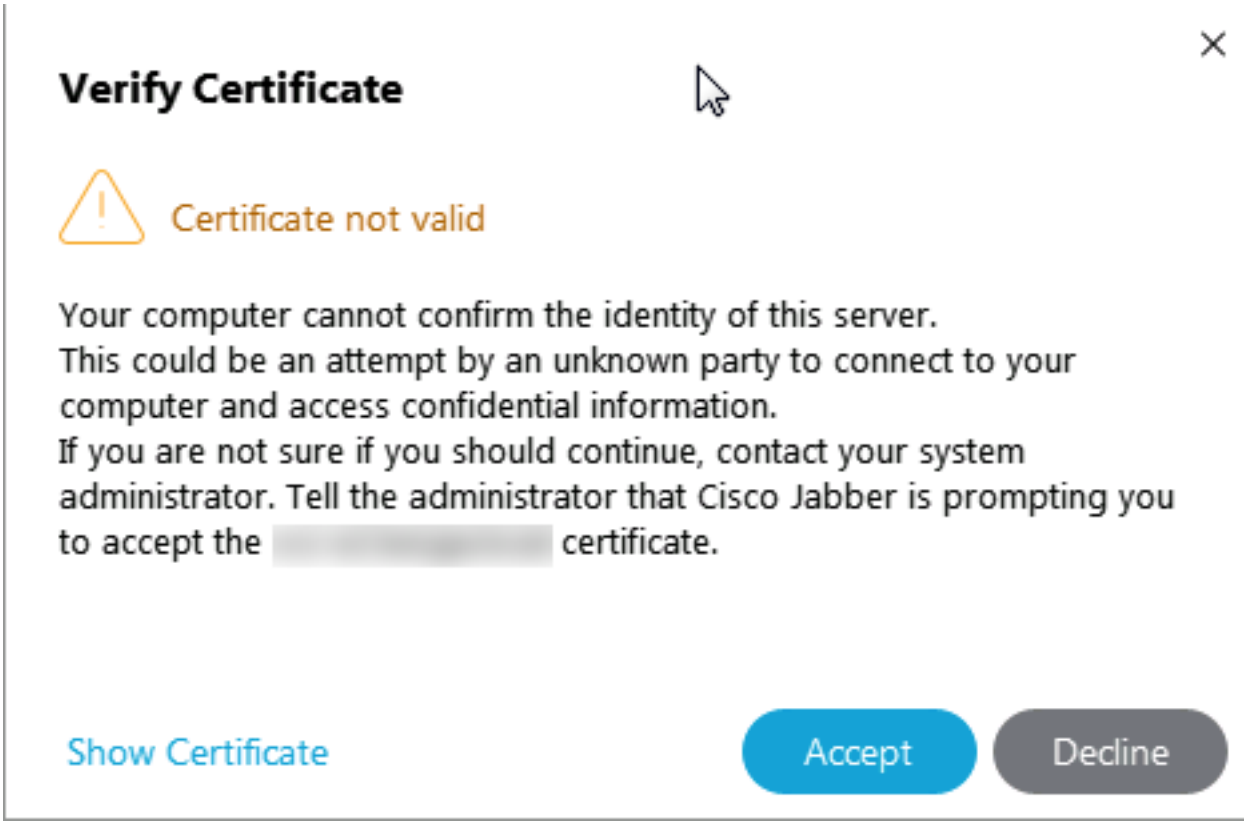
```
<Directory>
<DirectoryServerType>UDS</DirectoryServerType>
<PhotoUriWithToken>http://%IP/Hostname%/photo%%uid%%.jpg<
/PhotoUriWithToken>
<UdsServer>%IP%</UdsServer>
<MinimumCharacterQuery>3</MinimumCharacterQuery>
</Directory>
```

2. Bei Expressway-C muss der Webserver in der Liste der zulässigen HTTP-Server aufgeführt sein.

   Klicken Sie auf **Configuration > Unified Communications > Configuration > Configure HTTP Server allow list**.Klicken Sie auf **Neu > IP/Hostname eingeben > Eintrag erstellen**.Melden Sie sich vom Jabber-Client ab, und melden Sie sich dann wieder an.

   **Hinweis**: Weitere Informationen zur UDS-Kontaktfotoauflösung finden Sie in der Jabber-Kontaktfotodokumentation.

## Jabber-Clients werden aufgefordert, das Expressway-E-Zertifikat bei der Anmeldung zu akzeptieren



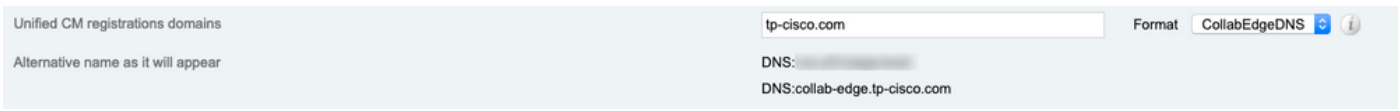

Diese Fehlermeldung kann sich auf das Expressway Edge-Zertifikat beziehen, das nicht von einer öffentlichen Zertifizierungsstelle signiert wurde, die vom Client-Gerät als vertrauenswürdig eingestuft wurde, oder darauf, dass die Domäne im Serverzertifikat nicht als SAN vorhanden ist.

Um den Jabber-Client von der Aufforderung zur Annahme des Expressway-Zertifikats abzuhalten, müssen Sie die beiden unten aufgeführten Kriterien erfüllen:

- Auf dem Gerät/Computer, auf dem der Jabber-Client ausgeführt wird, muss der Signierer des Expressway-E-Zertifikats in seinem Zertifikatvertrauensspeicher aufgeführt sein.

  **Hinweis**: Dies ist einfach zu bewerkstelligen, wenn Sie eine öffentliche Zertifizierungsstelle verwenden, da Mobilgeräte einen großen Zertifikatvertrauensspeicher enthalten.

- Die für den Collab-Edge-Datensatz verwendete Unified CM-Registrierungsdomäne muss im SAN des Expressway-E-Zertifikats vorhanden sein. Das CSR-Tool im Expressway-Server bietet Ihnen die Möglichkeit, die Unified CM-Registrierungsdomäne als SAN hinzuzufügen. Diese wird vorinstalliert, wenn die Domäne für MRA konfiguriert ist. Wenn die Zertifizierungsstelle, die das Zertifikat signiert, eine Domäne nicht als SAN akzeptiert, können Sie auch die Option "CollabEdgeDNS" verwenden, mit der der Domäne das Präfix "collab-edge" hinzugefügt wird:




## Zugehörige Informationen

- [Mobile & Remote Access Anleitung über Expressways]

- Bereitstellungsleitfaden zur Erstellung und Verwendung von Cisco Expressway-Zertifikaten
- Cisco TelePresence Video Communication Server (Cisco VCS) IP-Port-Nutzung für Firewall-Traversal
- Bereitstellungs- und Installationshandbuch für Cisco Jabber
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.