

Konfigurieren von CMS WebRTC oder Web App Proxy über Expressway

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationsschritte](#)

[Schritt 1: Integration von CMS WB auf Expressway-C](#)

[Schritt 2: Aktivieren Sie "TURN" auf dem Expressway-E, und fügen Sie der lokalen Authentifizierungsdatenbank die Authentifizierungsinformationen hinzu.](#)

[Schritt 3: Ändern des Administrationsports des Expressway-E](#)

[Schritt 4: Fügen Sie den Expressway-E als TURN-Server für Media NAT Traversal zum CMS-Server hinzu.](#)

[Überprüfung](#)

[Schritt 1: Überprüfen Sie auf Expressway-C, ob das WB korrekt integriert ist.](#)

[Schritt 2: Überprüfen Sie, ob der TURN-Server zum CMS-Server hinzugefügt wurde.](#)

[Schritt 3: Überprüfen der TURN-Relayverwendung während eines laufenden Anrufs](#)

[Fehlerbehebung](#)

[Externer WebRTC-Client verbindet sich, aber keine Medien \(wegen ICE-Fehler\)](#)

[Externer WebRTC-Client erhält keine Option zur Teilnahme](#)

[Externer WebRTC-Client blockiert \(beim Laden von Medien\), wenn eine Verbindung mit Cospace hergestellt wird, und wird dann auf die WB-Startseite umgeleitet](#)

[Externer WebRTC-Client kann Cospace nicht beitreten und erhält Warnung \(Verbindung kann nicht hergestellt werden - Versuchen Sie es später erneut\)](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die Schritte zur Konfiguration und Fehlerbehebung von Cisco Meeting Server (CMS) WebRTC über Expressway beschrieben.

Voraussetzungen

Anforderungen

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

- Expressway X12.6.1 und höher (x12.6.1 und höher können aufgrund von Änderungen im EXP TURN-Verhalten nur mit CMS 2.9.2 oder höher arbeiten)
- CMS Server 2.9.3 und höher
- Network Address Translation (NAT)
- Traversal mithilfe von Relays (TURN) um NAT
- Session Traversal Utilities (STUN) für NAT
- Domain Name System (DNS)

Konfigurationsvoraussetzungen:

- Grundlegende MRA-bezogene Einstellungen (Mobile and Remote Access) (UC Traversal zone, SSH Tunnels) müssen bereits auf dem Expressway aktiviert und konfiguriert sein. [Klicken Sie hier](#), um MRA-Leitfäden anzuzeigen.
- Informationen zur Konfiguration und Aktivierung von CMS 2.9.x - WebBridge (WB), XMPP und CallBridge auf CMS finden Sie im [Konfigurationsleitfaden](#).
- Auf dem Expressway-E installierte Taste DREHEN.
- TCP-Port 443 wurde auf der Firewall vom öffentlichen Internet zur öffentlichen IP-Adresse des Expressway-E geöffnet.
- TCP- und UDP-Port 3478 (TURN-Anfragen) wurden auf der Firewall vom öffentlichen Internet zur öffentlichen IP-Adresse des Expressway-E geöffnet.
 - TCP 3478 wird nur benötigt, wenn 'turnservers' in der CMS-API tcpPortNumberOverride auf 3478 festgelegt hat.
- Der UDP Port 3478 (TURN-Anfragen) wurde auf der Firewall vom CMS zur privaten IP-Adresse des Expressway-E geöffnet (wenn Sie Dual-NIC auf dem Expressway-E verwenden).
 - CMS 2.9.2 und frühere Versionen senden Bindungsanforderungen an Exp E, während 2.9.3 Weiterleitungen Allocate-Anforderungen sendet.
- Externe DNS-Einträge für die Join-URL für Webbridge, auflösbar in die öffentliche IP-Adresse des Expressway-E.
- Interner DNS-Eintrag für Join-URL, auflösbar in die IP-Adresse des Webbridge-Servers.
- Wenn Sie X12.5.2 oder frühere Versionen ausführen, stellen Sie sicher, dass die NAT-Reflektion für die öffentliche IP-Adresse von Expressway-E auf der externen Firewall zulässig ist. [Klicken Sie beispielsweise hier](#) für die Konfiguration. Ab X12.5.3 ist dies für einen Standalone-Expressway nicht mehr erforderlich.
- Wenn Sie Port 443 für TURN verwenden, müssen Sie UDP Port 3478 für Medien auf der externen Firewall öffnen.

Achtung: Wenn TCP-Port 443 aktiviert ist, kann der Expressway nicht mehr auf TCP-Port 3478 reagieren.

Hinweis: Expressway-Paare für Jabber Guest-Services können nicht für CMS WebRTC Proxy-Services verwendet werden.

Hinweis: Informationen zum Upgrade von früheren Versionen auf Version 3.0 oder höher finden Sie unter [Anleitung für ein reibungsloses Upgrade von Cisco Meeting Server 2.9 auf 3.0 \(und höher\)](#).

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt. Die Mindestanforderungen für Softwareversionen müssen jedoch erfüllt werden.

- CMS-API (Application Program Interface)
- Schnellstraße
- CMS-Server

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 kennen.

Hintergrundinformationen

Seit Version X8.9.2 wurde Expressway um die WebRTC Proxy-Unterstützung erweitert. So können externe Benutzer auf eine Cisco Meeting Server Web Bridge zugreifen.

Externe Clients und Gäste können Bereiche verwalten oder beitreten, ohne dass eine andere Software als ein unterstützter Browser erforderlich ist. [Klicken Sie hier](#), um eine Liste der unterstützten Browser anzuzeigen.

Ab dem 5. Februar 2021 werden die folgenden Browser für CMS 3.1.1 unterstützt:

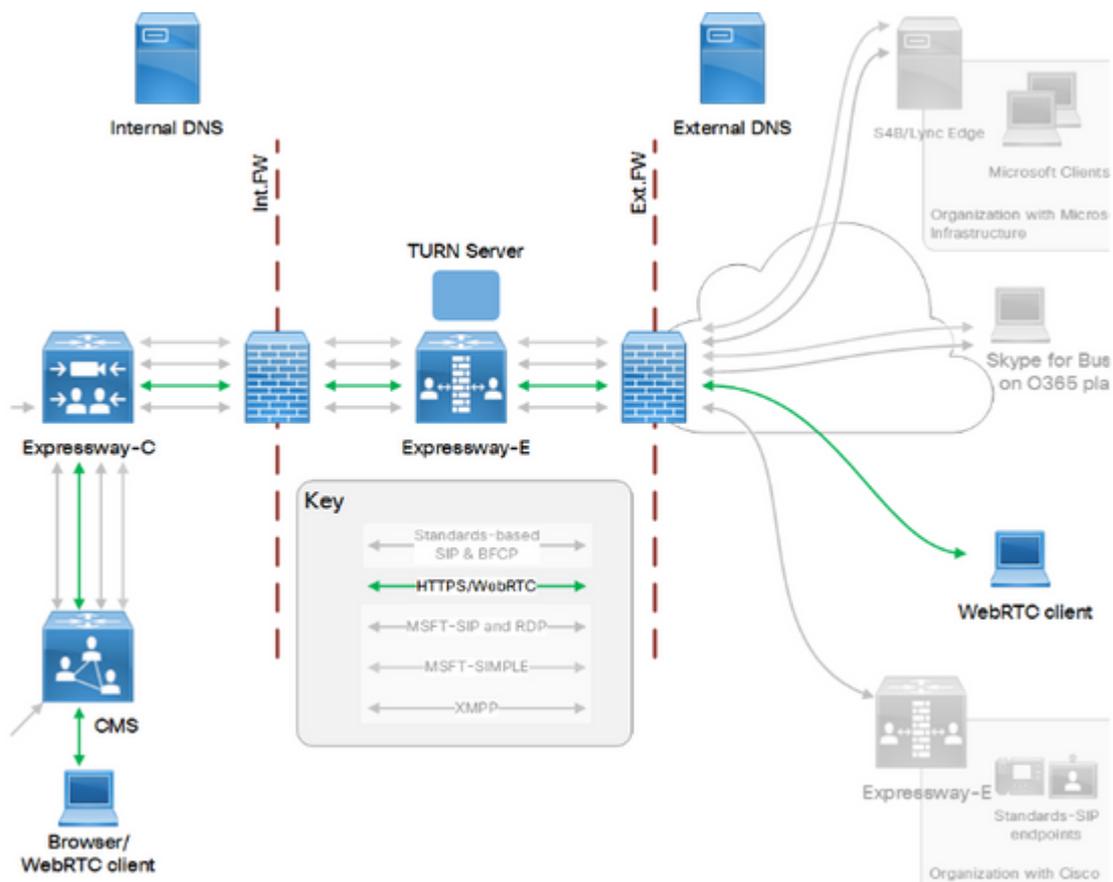
| Browsers | Versions |
|--|-----------------------------|
| Google Chrome (Windows, macOS and Android) | 85 |
| Mozilla Firefox (Windows) | 82 |
| Chromium-based Microsoft Edge (Windows) | 85 |
| Apple Safari for macOS | 13.x and 14.0 |
| Apple Safari for iOS | iOS versions: 13.x and 14.0 |
| Yandex (Windows) | 20.8 and 20.11 |

Note: Web app is not supported on the legacy Microsoft Edge.

Note: Web app is not supported on virtual machines (VMs) running these supported browsers.

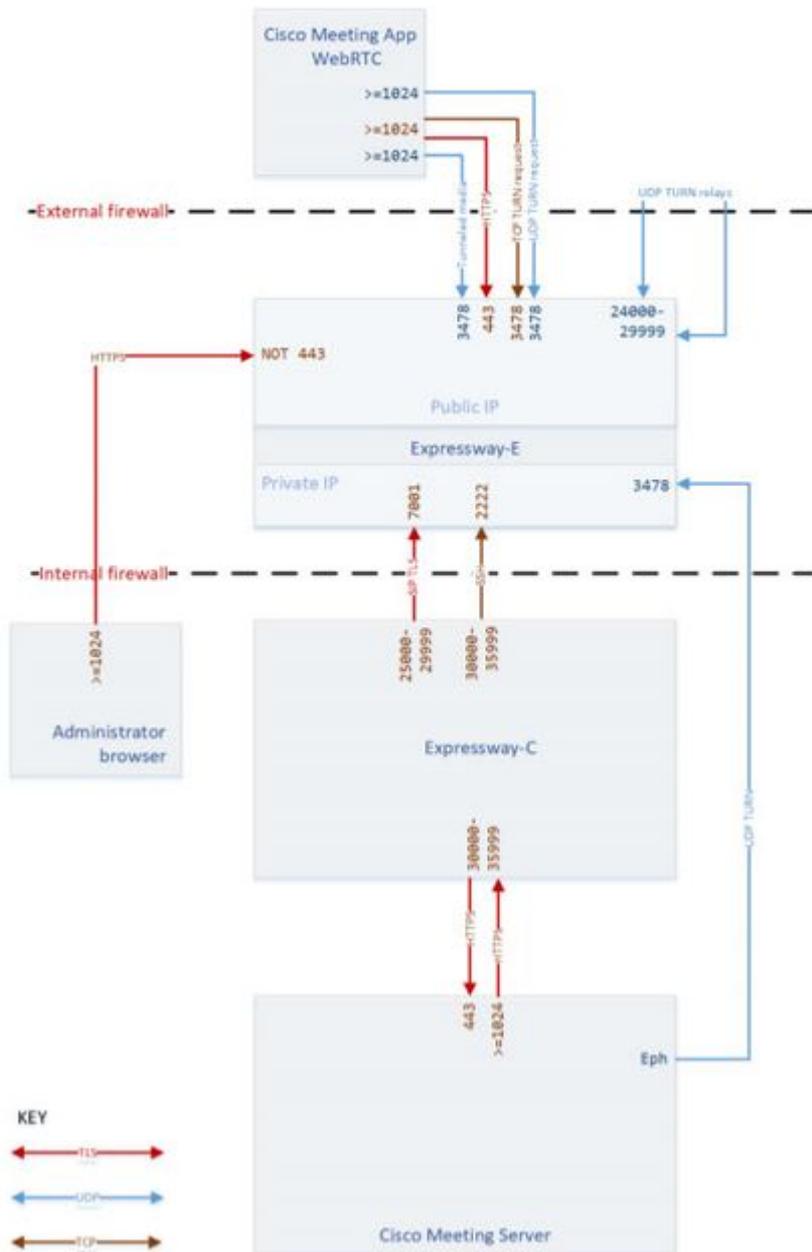
Konfigurieren

Netzwerkdiagramm



Dieses Bild zeigt ein Beispiel für den Verbindungsfluss des Webproxys für CMS WebRTC: (aus dem [Konfigurationsleitfaden](#) für die Verwendung des Exp-IP-Ports).

Web Proxy for Cisco Meeting Server Connections



Hinweis: Wenn Sie X12.5.2 oder früher ausführen, müssen Sie Ihre externe Firewall so konfigurieren, dass NAT-Reflektion für die öffentliche Expressway-E & IP-Adresse möglich ist (Firewalls misstrauen in der Regel Paketen, die dieselbe Quell- und Ziel-IP-Adresse haben). Ab X12.5.3 ist dies für einen Standalone-Expressway nicht mehr erforderlich.

Konfigurationsschritte

Schritt 1: Integration von CMS WB auf Expressway-C

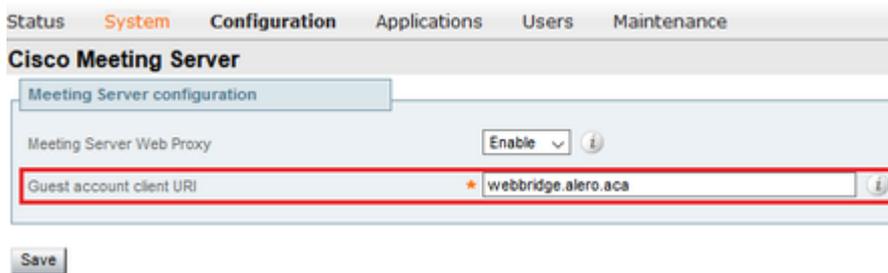
antwort: Navigieren Sie zu **Konfiguration > Unified Communication > Cisco Meeting Server**.

b. Aktivieren Sie **den Webproxy des Meeting-Servers**.

c. Geben Sie die Join-URL in das Feld **Guest Account Client URI** ein.

d. Klicken Sie auf **Speichern**.

e. Fügen Sie die CMS-Join-URL dem Expressway-E-Serverzertifikat als Subject Alternative Name (SAN) hinzu. Siehe [Cisco VCS Certificate Creation and Use Deployment Guide](#).



Schritt 2: Aktivieren Sie "TURN" auf dem Expressway-E, und fügen Sie der lokalen Authentifizierungsdatenbank die Authentifizierungsinformationen hinzu.

antwort: Navigieren Sie zu **Konfiguration > Traversal > TURN**.

b. Aktivieren Sie **die Dienste "SCHALTEN"**, von **Aus** bis **Ein**.

c. Wählen Sie **Anmeldeinformationen für den TURN-Client in der lokalen Datenbank konfigurieren**, und fügen Sie die Anmeldeinformationen (Benutzername und Kennwort) hinzu.

Hinweis: Wenn Sie einen Cluster von Expressway-Es haben und diese alle als TURN-Server verwendet werden sollen, dann stellen Sie sicher, dass Sie ihn auf allen Knoten aktivieren. Sie müssen zwei separate turnServer-Instanzen über API konfigurieren und sie auf jeden der Expressway-E-Server im Cluster verweisen (gemäß dem in Schritt 4 gezeigten Konfigurationsprozess, der den Prozess für einen Expressway-E-Server zeigt; die Konfiguration des zweiten turnServers wäre ähnlich, nur unter Verwendung der jeweiligen IP-Adressen und Anmeldeinformationen für den anderen Expressway-E-Server).

Hinweis: Sie können einen Netzwerk-Load Balancer vor Ihren Schnellstraßen für TCP/HTTPS-Datenverkehr verwenden, aber TURN-Medien müssen weiterhin von Client zu TURN-Servern für die öffentliche IP übertragen werden. TURN-Medien dürfen den Netzwerk-Load Balancer nicht passieren.

Schritt 3: Ändern des Administrationsports des Expressway-E

Dieser Schritt ist erforderlich, da WebRTC-Verbindungen über TCP 443 bereitgestellt werden. Mit Exp 12.7 wurde jedoch eine neue dedizierte Verwaltungsschnittstelle (Dedicated Management Interface, DMI) eingeführt, die für 443 verwendet werden kann.

antwort: Navigieren Sie zu **System > Administration (System > Verwaltung)**.

b. Ändern Sie unter **Webserverkonfiguration** den **Webadministratorport** aus den Dropdown-Optionen auf **445**, und klicken Sie dann auf **Speichern**.

c. Wiederholen Sie die Schritte 3a bis 3b auf allen Expressway-ES, die für WebRTC-Proxydienste verwendet werden.

Hinweis: Cisco empfiehlt, den Administrations-Port zu ändern, da WebRTC-Clients 443 verwenden. Wenn der WebRTC-Browser versucht, auf Port 80 zuzugreifen, leitet der Expressway-E die Verbindung zu 443 um.

Schritt 4: Fügen Sie den Expressway-E als TURN-Server für Media NAT Traversal zum CMS-Server hinzu.

In CMS 2.9.x können Sie über das Menü **Konfiguration** > **API Server** hinzufügen:

- serverAddress: (Private IP-Adresse von Expressway)
- clientAddress: (Öffentliche IP-Adresse von Expressway)
- Typ: (Schnellstraße)
- Benutzername: (wie in Schritt 2c konfiguriert)
- Kennwort: (gemäß Konfiguration in Schritt 2c)
- tcpPortNumberOverride: 3478

d. Wiederholen Sie Schritt 4c für jeden für TURN zu verwendenden Expressway-E-Server.

Dieses Bild zeigt ein Beispiel der Konfigurationsschritte:

| Field | Value | Status |
|-------------------------|--|-----------|
| serverAddress | <input checked="" type="checkbox"/> Address CB reaches out to using 3478 UDP | - present |
| clientAddress | <input checked="" type="checkbox"/> Address Client (web app or WebRTC) uses for TURN | - present |
| username | <input checked="" type="checkbox"/> username that was configured in step 2c | - present |
| password | <input checked="" type="checkbox"/> password that was configured in step 2c | - present |
| useShortTermCredentials | <input type="checkbox"/> false | - present |
| sharedSecret | <input type="text"/> | |
| type | <input checked="" type="checkbox"/> expressway | - present |
| numRegistrations | <input type="text"/> 0 | - present |
| tcpPortNumberOverride | <input checked="" type="checkbox"/> 3478 | - present |
| callBridge | <input type="text"/> Choose | |
| callBridgeGroup | <input type="text"/> Choose | |

Modify

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Schritt 1: Überprüfen Sie auf Expressway-C, ob das WB korrekt integriert ist.

antwort: Navigieren Sie zu **Konfiguration** > **Unified Communication** > **Cisco Meeting Server**. Sie müssen die IP-Adresse des WB sehen:

Cisco Meeting Server

You are here: [C](#)

Meeting Server configuration

Meeting Server Web Proxy

Guest account client URI

| Guest account client URI resolved to the following targets | |
|--|------------|
| Name | Address |
| webbridge.alero.aca | 10.48.36.5 |

b. Navigieren Sie zu **Konfiguration > Unified Communication > HTTP-Zulassungsliste > Automatisch hinzugefügte Regeln**. Überprüfen Sie, ob dies den Regeln hinzugefügt wurde:

| | | | | | |
|----------------------------|-------|-----|--------|---|------------------------------|
| Meeting Server web bridges | https | 443 | Prefix | / | GET, POST, PUT, HEAD, DELETE |
| Meeting Server web bridges | wss | 443 | Prefix | / | GET, POST, PUT, HEAD, DELETE |

Hinweis: Es wird nicht erwartet, dass der WB in den erkannten Knoten zu finden, da die Regeln lediglich den Proxy für HTTPS-Verkehr zum WB und nicht unbedingt für Unified Communications zulassen.

c. Überprüfen Sie, ob der Secure Shell (SSH)-Tunnel für den WB FQDN auf dem Expressway-C zum Expressway-E gebaut wurde und aktiv ist. Navigieren Sie zu **Status > Unified Communications > Unified Communications SSH tunnels status**. Sie müssen den FQDN der WB sehen und das Ziel muss der Expressway-E sein.

Unified Communications SSH tunnels status

You are here: [Status](#) > [Unified Communications](#)

| Target | Domain | Status |
|--------------------|---------------------|--------|
| vcs-e.alero.local | webbridge.alero.aca | Active |
| vcs-e.alero.local | alero.lab | Active |
| vcs-e.alero.local | alero.local | Active |
| vcs-e2.alero.local | alero.lab | Active |
| vcs-e2.alero.local | webbridge.alero.aca | Active |
| vcs-e2.alero.local | alero.local | Active |

Schritt 2: Überprüfen Sie, ob der TURN-Server zum CMS-Server hinzugefügt wurde.

Suchen Sie im CMS API-Menü die Turn-Server, und klicken Sie auf die einzelnen Server. In jedem Objekt gibt es einen Link, um den Status zu überprüfen:

Related objects: </api/v1/turnServers>
</api/v1/turnServers/266cb509-71fb-4ecc-b600-b93d07d886ff/status>

Table view XML view

| Object configuration | |
|-------------------------|------------|
| serverAddress | 10.0.0.36 |
| clientAddress | 175.12.5.1 |
| numRegistrations | 0 |
| username | cmsturn |
| useShortTermCredentials | false |
| type | expressway |
| tcpPortNumberOverride | 3478 |

Die Ausgabe zeigt Informationen an, die die Round-Trip Time (RTT) in Millisekunden (Ms) enthalten, die dem TURN-Server zugeordnet sind. Diese Informationen sind wichtig für die CB-Auswahl des besten zu verwendenden TURN-Servers.

Schritt 3: Überprüfen der TURN-Relayverwendung während eines laufenden Anrufs

Bei einem Live-Anruf, der über den WebRTC-Client geführt wird, können Sie den Status des TURN-Medien-Relays auf dem Expressway anzeigen. Navigieren Sie zu **Status > TURN relay usage**, und wählen Sie **view (Ansicht)**.

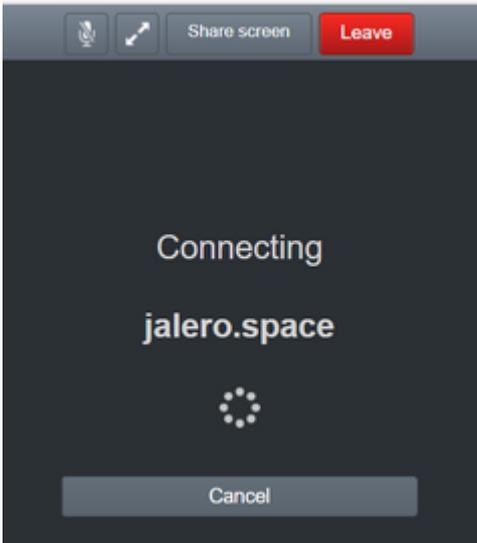
Fehlerbehebung

Nützliche Tools:

- HAR-Datei von Browsern ([Wie man eine HAR-Datei in Chrome oder Firefox zu generieren](#))
- WebRTC internals dump from browser - chrome://webrtc-internals or edge://webrtc-internals - Erstellen Sie dump, sobald der Join-Versuch unternommen wird.
- Browserkonsolenprotokolle können ebenfalls hilfreich sein.
- Wireshark-Erfassung vom Client, Exp E, Exp C und CMS.
- Exp E network.http.trafficserver debuggt Hilfe bei der Fehlerbehebung für Websocket.

Externer WebRTC-Client verbindet sich, aber keine Medien (wegen ICE-Fehler)

In diesem Szenario ist der RTC-Client in der Lage, die Anruf-ID in jalero.space aufzulösen. Wenn Sie jedoch Ihren Namen eingeben und **Anruf beitreten** auswählen, zeigt der Client **Verbindung** an, wie in der folgenden Abbildung dargestellt:



Nach ca. 30 Sekunden wird sie auf die erste WB-Seite umgeleitet.

Führen Sie zur Fehlerbehebung die folgenden Schritte aus:

- Starten Sie Wireshark auf dem RTC-Client, wenn Sie einen Anruf tätigen, und stoppen Sie die Erfassung, wenn der Fehler auftritt.
- Überprüfen Sie nach Auftreten des Problems die CMS-Ereignisprotokolle:

Navigieren Sie im CMS-Webadministrator zu **Protokolle** > Ereignisprotokolle.

- Filtern Sie die Wireshark-Spuren mit Betäubung. Siehe folgendes Beispiel:



In den Wireshark-Ablaufverfolgungen sehen Sie, dass der Client eine **Zuweisungsanforderung** mit konfigurierten Anmeldeinformationen an den Expressway-E TURN-Server an Port 3478 sendet:

```
1329    2017-04-15 10:26:42.108282    10.55.157.229    10.48.36.248    STUN    186
Allocate Request UDP user: expturncreds realm: TANDBERG with nonce
```

Der Server antwortet mit dem **Fehler "Zuordnen"**:

```
1363    2017-04-15 10:26:42.214119    10.48.36.248    10.55.157.229    STUN    254
Allocate Error Response user: expturncreds with nonce realm: TANDBERG UDP error-code: 431
(*Unknown error code*) Integrity Check Failure
```

Oder

```
3965    2017-04-15 10:34:54.277477    10.48.36.248    10.55.157.229    STUN    218
Allocate Error Response user: expturncreds with nonce realm: TANDBERG UDP error-code: 401
(Unauthorized) Unauthorized
```

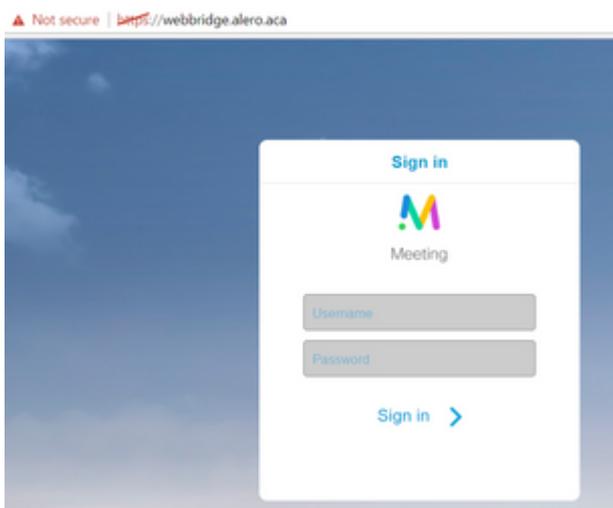
In den CMS-Protokollen wird diese Protokollmeldung angezeigt:

```
2017-04-15 10:34:56.536 Warning call 7: ICE failure 4 (unauthorized - check credentials)
```

Lösung:

Überprüfen Sie die im CMS konfigurierten TURN-Anmeldeinformationen, und stellen Sie sicher, dass sie mit den in der lokalen Expressway-E-Authentifizierungsdatenbank konfigurierten Anmeldeinformationen übereinstimmen.

Externer WebRTC-Client erhält keine Option zur Teilnahme



Auf der Seite "Callbridge **Status > General**" (Rufbrückenstatus > Allgemein) wird Folgendes angezeigt:

```
2017-04-15 12:09:06.647 Web bridge connection to "webbridge.alero.aca" failed (DNS failure)
2017-04-15 12:10:11.634 Warning web bridge link 2: name resolution for "webbridge.alero.aca" fa
2017-04-15 11:55:50.835 Info failed to establish connection to web bridge link 2 (unknown error
```

Lösung:

- Stellen Sie sicher, dass die Callbridge die Join-URL in den Webbridge-FQDN auflösen kann (die Callbridge darf dies nicht in die IP-Adresse des Expressway-E auflösen).
- Leeren Sie den DNS-Cache auf der Callbridge über die Befehlszeilenschnittstelle (CLI) mit dem Befehl **dns flush**.
- Stellen Sie sicher, dass die WB dem Callbridge-Serverzertifikat vertraut (nicht dem Aussteller).

Externer WebRTC-Client blockiert (beim Laden von Medien), wenn eine Verbindung mit Cospace hergestellt wird, und wird dann auf die WB-Startseite umgeleitet

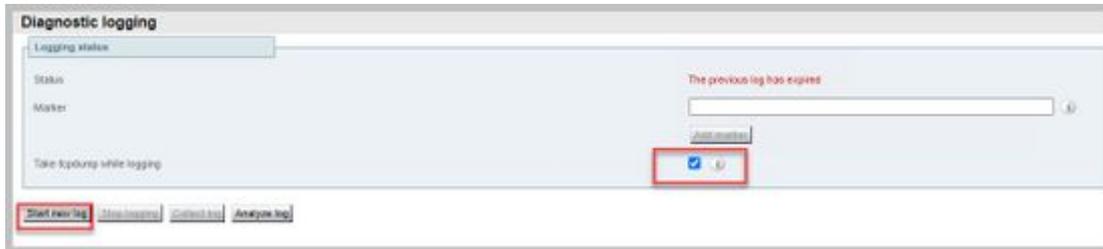
Lösung:

- Stellen Sie sicher, dass CMS den SRV-Datensatz `_xmpp-client` im internen Netzwerk für die CB-

Domäne auflösen kann, und stellen Sie sicher, dass WebRTC-Verbindungen intern funktionieren.

- Erfassen Sie eine Wireshark-Aufzeichnung auf dem Client und die Diagnoseprotokollierung einschließlich tcpdump auf dem Expressway-E, während Sie versuchen, eine Verbindung mit dem externen Client herzustellen:

Navigieren Sie zu **Maintenance > Diagnostics > Diagnostic logging**, und stellen Sie sicher, dass **Take tcpdump while logging** markiert ist (wie in diesem Bild gezeigt), bevor Sie **Start new log** auswählen:

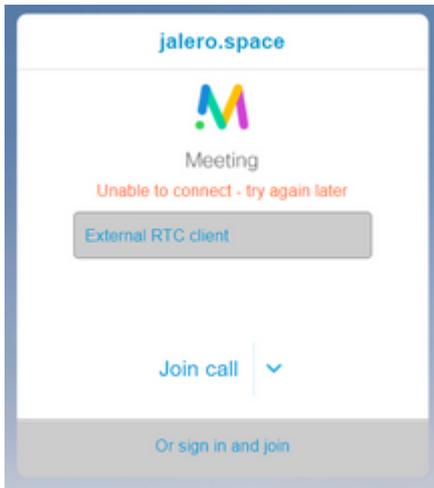


Hinweis: Stellen Sie sicher, dass die Wireshark-Erfassung auf dem Client-Gerät und die Protokollierung auf dem Expressway-E gestartet werden, bevor Sie den fehlerhaften Anruf reproduzieren. Wenn der fehlerhafte Anruf reproduziert wurde, stoppen Sie die Protokollierung auf dem Expressway-E und laden Sie die Aufzeichnung auf den Client herunter.

- Extrahieren/entpacken Sie das von Expressway-E heruntergeladene Protokollpaket und öffnen Sie die .pcap-Datei, die auf der Schnittstelle zur öffentlichen Ansicht gespeichert ist.
- Filtern Sie nach beiden Paketerfassungen mit Betäubung:
 - Suchen Sie dann nach der Bindungsanforderung vom externen Client an die öffentliche Expressway-E-IP-Adresse, klicken Sie mit der rechten Maustaste, und wählen Sie **Follow > UDP Stream aus**.
 - Normalerweise liegt der Zielport der Binding-Anforderung vom Client im Bereich von 24000-29999, d. h. der TURN-Relay-Port-Bereich auf dem Expressway-E.
- Wenn auf der Clientseite keine Antwort auf die Binding-Anforderungen empfangen wird, überprüfen Sie, ob die Anforderungen eintreffen, in der Erfassung von Expressway-E.
- Wenn die Anfragen eingehen und der Expressway-E dem Client antwortet, überprüfen Sie, ob die externe FW den ausgehenden UDP-Datenverkehr zulässt.
- Wenn die Anfragen nicht eingehen, überprüfen Sie die FW, um sicherzustellen, dass der zuvor aufgeführte Port-Bereich nicht blockiert wird.
- Wenn der Expressway-E mit einem Dual Network Interface Controller (DUAL-NIC) mit aktiviertem statischen NAT-Modus und X12.5.2 oder früher bereitgestellt wird, stellen Sie sicher, dass NAT-Reflektion auf der externen FW unterstützt und konfiguriert wird. Ab X12.5.3 ist dies für einen Standalone-Expressway nicht mehr erforderlich.

Externer WebRTC-Client kann Cospace nicht beitreten und erhält Warnung (Verbindung kann nicht hergestellt werden - Versuchen Sie es später erneut)

In diesem Szenario ist der RTC-Client in der Lage, die Anruf-ID in jalero.space aufzulösen. Wenn Sie jedoch Ihren Namen eingeben und **Anruf beitreten** auswählen, wird sofort die Warnung **Verbindung nicht möglich - später erneut versuchen** angezeigt:



Lösung:

Überprüfen Sie, ob CMS im internen Netzwerk in der Lage ist, den SRV-Datensatz _xmpp-client für die CB-Domäne immer aufzulösen.

Zugehörige Informationen

- [VCS/Expressway-IP-Port-Nutzungsleitfaden](#)
- [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.