

# Configura proxy CMS WebRTC o Web App su Expressway

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Procedura di configurazione](#)

[Passaggio 1. Integrazione di CMS WB in Expressway-C](#)

[Passaggio 2. Abilitare TURN su Expressway-E e aggiungere le credenziali di autenticazione al database di autenticazione locale](#)

[Passaggio 3. Modificare la porta di amministrazione di Expressway-E](#)

[Passaggio 4. Aggiungere Expressway-E come server TURN per Media NAT Traversal sul server CMS](#)

[Verifica](#)

[Passaggio 1. In Expressway-C, verificare che il Web sia correttamente integrato](#)

[Passaggio 2. Verificare che il server TURN sia stato aggiunto al server CMS](#)

[Passaggio 3. Verifica dell'utilizzo di TURN Relay durante una chiamata in corso](#)

[Risoluzione dei problemi](#)

[Il client WebRTC esterno si connette ma non dispone di supporti \(a causa di un errore ICE\)](#)

[Il client WebRTC esterno non ottiene l'opzione Join Call](#)

[Il client WebRTC esterno è bloccato \(durante il caricamento dei supporti\) durante la connessione a Cospace e viene quindi reindirizzato alla pagina iniziale Web](#)

[Il client WebRTC esterno non è in grado di collegarsi a Cospace e riceve l'avviso \(impossibile connettersi - riprovare più tardi\)](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritta la procedura per configurare Cisco Meeting Server (CMS) WebRTC su Expressway e risolvere i relativi problemi.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Expressway X12.6.1 e versioni successive (x12.6.1 e versioni successive possono funzionare solo con CMS 2.9.2 o versioni successive a causa di modifiche nel


comportamento di Exp TURN)

- CMS Server 2.9.3 e versioni successive
- NAT (Network Address Translation)
- Attraversamento tramite relè (TURN) attorno a NAT
- Session Traversal Utilities (STUN) per NAT
- DNS (Domain Name System)


Prerequisiti di configurazione:

- Le impostazioni relative all'MRA (Basic Mobile and Remote Access) (UC Traversal Zone, tunnel SSH) devono essere già abilitate e configurate in Expressway. [Fare clic qui](#) per le guide all'MRA.
- Per CMS 2.9.x - WebBridge (WB), XMPP e CallBridge configurati e abilitati su CMS, vedere la [guida alla configurazione](#)
- Tasto di opzione TURN installato su Expressway-E.
- La porta TCP 443 è stata aperta sul firewall dall'internet pubblico all'indirizzo IP pubblico di Expressway-E.
- Le porte TCP e UDP 3478 (richieste TURN) sono state aperte sul firewall da Internet pubblica all'indirizzo IP pubblico di Expressway-E.
  - TCP 3478 necessario solo se 'turn servers' nell'API CMS ha tcpPortNumberOverride impostato su 3478.
- La porta UDP 3478 (richieste TURN) è stata aperta sul firewall dal CMS all'indirizzo IP privato di Expressway-E (se si utilizza una scheda NIC doppia su Expressway-E).
  - CMS 2.9.2 e versioni precedenti invia richieste di binding a Exp E, mentre la versione 2.9.3 in avanti invia richieste di allocazione
- Record DNS esterni per l'URL di join per webbridge, risolvibili nell'indirizzo IP pubblico di Expressway-E.
- Record DNS interno per URL di join risolvibile nell'indirizzo IP del server WebBridge.
- Se si esegue X12.5.2 o versioni precedenti, verificare che la riflessione NAT consentita sul firewall esterno per l'indirizzo IP pubblico di Expressway-E, [fare clic qui](#), ad esempio configurazione. A partire dalla versione X12.5.3, questa funzionalità non è più necessaria per un'Expressway autonoma.
- Quando si utilizza la porta 443 per TURN, è necessario aprire la porta UDP 3478 per i supporti sul firewall esterno.


---

 **Attenzione:** quando la porta TCP 443 è abilitata, Expressway non può più rispondere sulla porta TCP 3478.

---

 **Nota:** la coppia Expressway utilizzata per i servizi Jabber Guest non può essere utilizzata per i servizi proxy CMS WebRTC.

---

 **Nota:** se si esegue l'aggiornamento alla versione 3.0 o successive dalle versioni precedenti, consultare la [Guida per un aggiornamento senza problemi da Cisco Meeting Server 2.9 a 3.0 \(e versioni successive\)](#)

---

## Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware, ma è necessario soddisfare i requisiti minimi di versione.

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

Il supporto proxy WebRTC è stato aggiunto a Expressway dalla versione X8.9.2, che consente agli utenti fuori sede di passare a un Cisco Meeting Server Web Bridge.

I client esterni e gli utenti guest possono gestire o unirsi agli spazi senza la necessità di un software diverso da un browser supportato. [Fare clic qui](#) per un elenco dei browser supportati.

Al 5 febbraio 2021, questi sono i browser supportati per CMS 3.1.1:

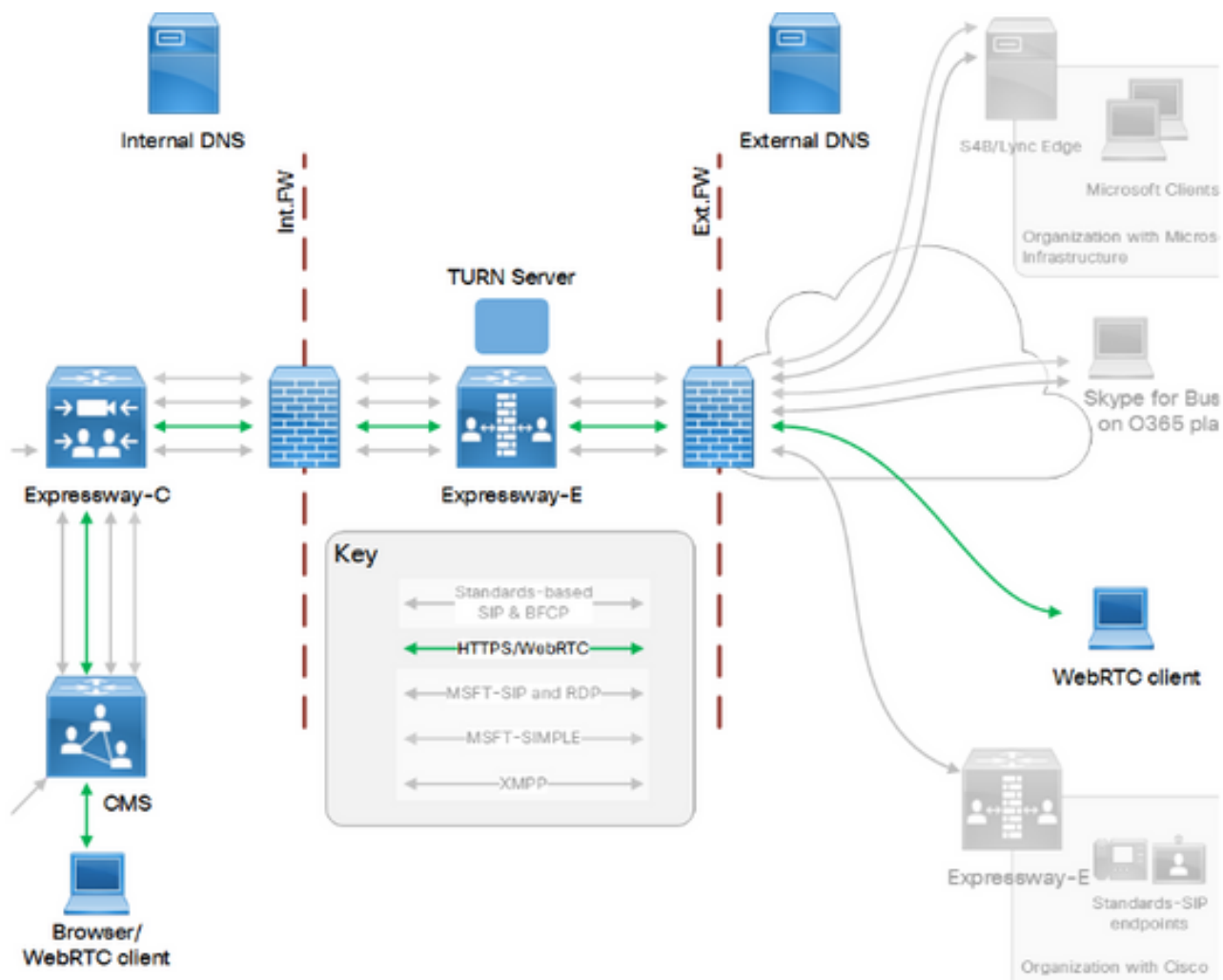
Browsers	Versions
Google Chrome (Windows, macOS and Android)	85
Mozilla Firefox (Windows)	82
Chromium-based Microsoft Edge (Windows)	88
Apple Safari for macOS	13.0 and 14.0
Apple Safari for iOS	iOS versions: 13.0 and 14.0
Yandex (Windows)	20.8 and 20.11

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.

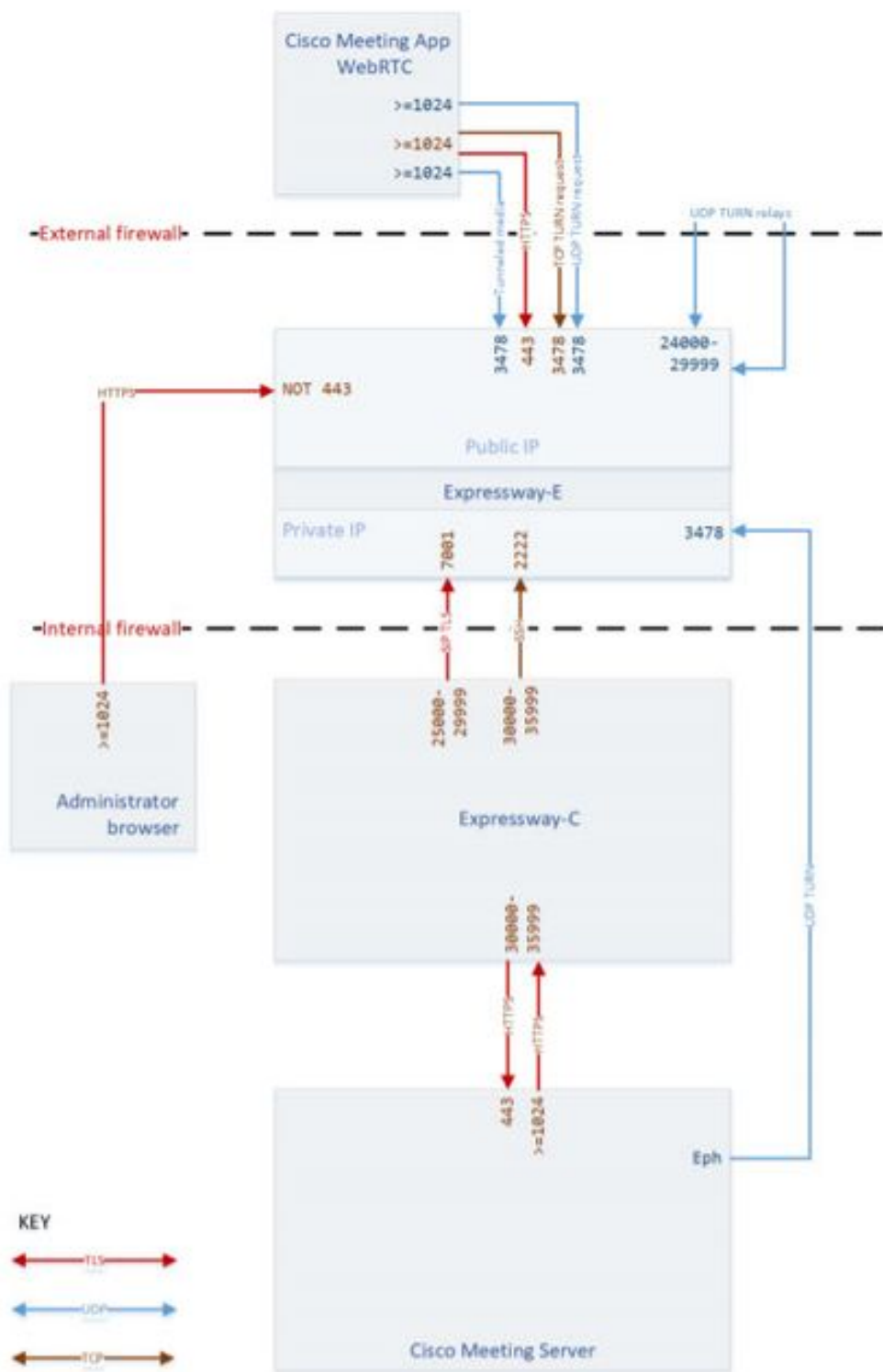
## Configurazione

## Esempio di rete



Questa immagine fornisce un esempio di flusso di connessioni del proxy Web per CMS WebRTC: (dalla [guida alla configurazione dell'utilizzo della porta IP di Exp](#)).

## Web Proxy for Cisco Meeting Server Connections



Nota: quando si esegue X12.5.2 o versione precedente, è necessario configurare il firewall esterno in modo da consentire la riflessione NAT per l'indirizzo IP pubblico Expressway-E (i firewall in genere non considerano attendibili i pacchetti con lo stesso indirizzo IP di origine e di destinazione). A partire dalla versione X12.5.3, questa funzionalità non è più necessaria per un'Expressway autonoma.

## Procedura di configurazione


### Passaggio 1. Integrazione di CMS WB in Expressway-C

- a. Passare a Configurazione > Comunicazione unificata > Cisco Meeting Server.
- b. Attivare il proxy Web di Meeting Server.
- c. Immettere l'URL di join nel campo URI client account Guest.
- d. Fare clic su Salva.
- e. Aggiungere l'URL di aggiunta CMS al certificato del server Expressway-E come nome alternativo del soggetto (SAN). Vedere la [Guida alla creazione e all'utilizzo dei certificati Cisco VCS](#).

The screenshot shows the Cisco Meeting Server configuration page. The 'Configuration' tab is active. In the 'Meeting Server configuration' section, the 'Meeting Server Web Proxy' is set to 'Enable'. The 'Guest account client URI' field is highlighted with a red box and contains the value 'webbridge.alero.aca'. A 'Save' button is located at the bottom left of the configuration area.


### Passaggio 2. Abilitare TURN su Expressway-E e aggiungere le credenziali di autenticazione al database di autenticazione locale

- a. Passare a Configurazione > Attraversamento > TORNITURA.
- b. Abilitare i servizi TURN, da off a on.
- c. Scegliere Configure TURN client credentials on local database e aggiungere le credenziali (nome utente e password).

 Nota: se si dispone di un cluster di Expressway-E che devono essere tutti utilizzati come server TURN, assicurarsi di abilitarlo su tutti i nodi. È necessario configurare due istanze di TurnServer separate tramite API e puntarle a ognuno dei server Expressway-E nel cluster (in base al processo di configurazione mostrato nel Passaggio 4, che mostra il processo per un server Expressway-E; la configurazione del secondo TurnoServer sarebbe simile, utilizzando solo i rispettivi indirizzi IP e le credenziali di Turno per l'altro server Expressway-E).

 Nota: per il traffico TCP/HTTPS è possibile utilizzare un servizio di bilanciamento del carico

---

 di rete davanti alle autostrade, ma il supporto TURN deve comunque passare dal client al server TURN IP pubblico. Il supporto TURN non deve passare attraverso il servizio di bilanciamento del carico di rete


---

### Passaggio 3. Modificare la porta di amministrazione di Expressway-E

Questo passaggio è necessario in quanto le connessioni webrtc sono disponibili su TCP 443, ma Exp 12.7 ha introdotto una nuova DMI (Dedicated Management Interface) che può essere utilizzata per 443.

- a. Passare a Sistema > Amministrazione.
- b. In Configurazione server Web, impostare la porta dell'amministratore Web su 445 dall'elenco a discesa, quindi fare clic su Salva.
- c. Ripetere i punti da 3a a 3b su tutti gli Expressway-E utilizzati per i servizi proxy WebRTC.

---

 Nota: Cisco consiglia di modificare la porta di amministrazione perché i client WebRTC utilizzano 443. Se il browser WebRTC tenta di accedere alla porta 80, Expressway-E reindirizza la connessione a 443.

---

### Passaggio 4. Aggiungere Expressway-E come server TURN per Media NAT Traversal sul server CMS

Da CMS 2.9.x in poi, utilizzare il menu Configuration —>API per aggiungere i server di tornitura:

- serverAddress: (indirizzo IP privato di Expressway)
- clientAddress: (indirizzo IP pubblico di Expressway)
- type: (expressway)
- nome utente: (come configurato nel passaggio 2c)
- password: (come configurata al passaggio 2c)
- tcpPortNumberOverride: 3478

- d. Ripetere il passaggio 4c per ogni server Expressway-E da utilizzare per TURN

In questa immagine viene illustrato un esempio dei passaggi di configurazione:

/api/v1/turnServers/266cb509-71fb-4ecc-b600-b93d07d886ff

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	
useShortTermCredentials	<input type="checkbox"/>	false	- present
sharedSecret	<input type="checkbox"/>		
type	<input checked="" type="checkbox"/>	expressway	- present
numRegistrations	<input type="checkbox"/>	0	- present
tcpPortNumberOverride	<input checked="" type="checkbox"/>	3478	- present
callBridge	<input type="checkbox"/>		Choose
callBridgeGroup	<input type="checkbox"/>		Choose

Modify

## Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Passaggio 1. In Expressway-C, verificare che il Web sia correttamente integrato

a. Passare a Configurazione > Comunicazione unificata > Cisco Meeting Server. È necessario visualizzare l'indirizzo IP del Web:

Status **System** Configuration Applications Users Maintenance

**Cisco Meeting Server** You are here: >

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. Passare a Configurazione > Comunicazione unificata > Elenco indirizzi HTTP consentiti > Regole aggiunte automaticamente. Verificare che sia stato aggiunto alle regole:

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



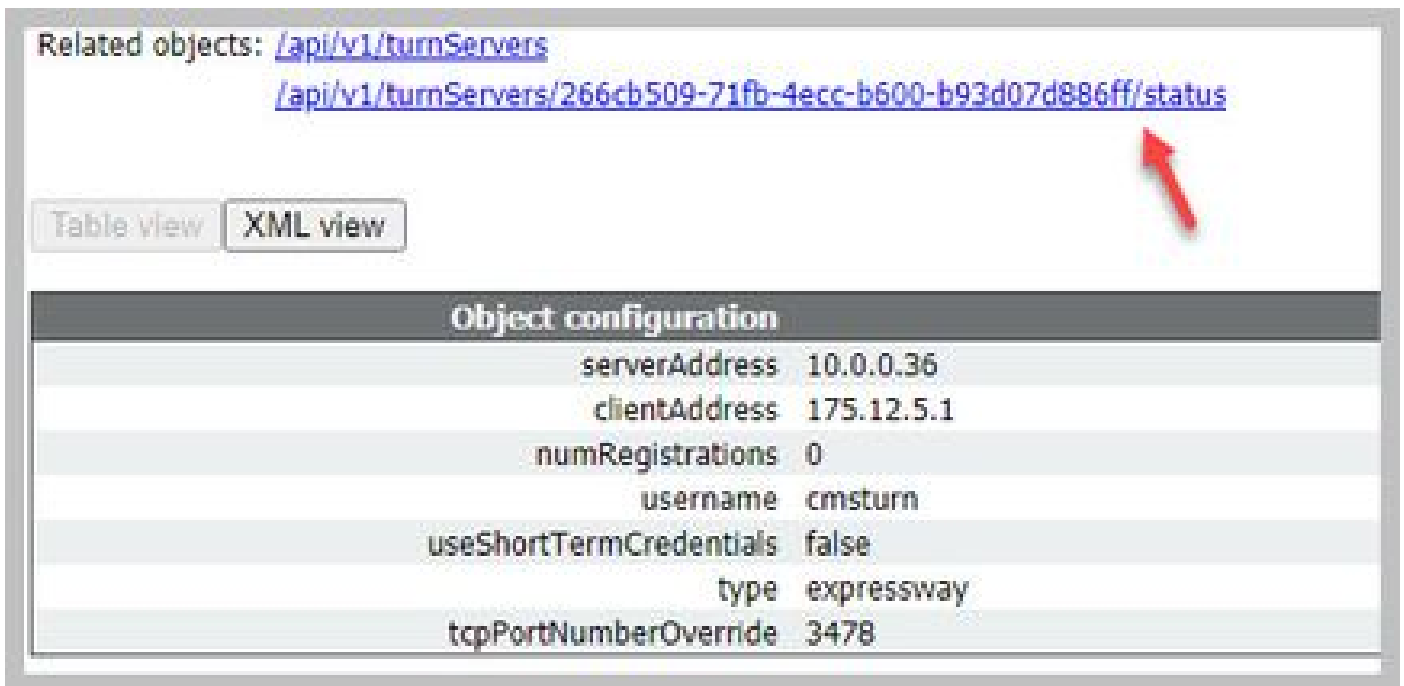
 Nota: non è previsto trovare il Web nei nodi individuati perché le regole consentono semplicemente il proxy del traffico HTTPS al Web e non necessariamente la comunicazione unificata.

c. Verificare che il tunnel Secure Shell (SSH) per il nome di dominio completo (FQDN) Web sia stato compilato da Expressway-C a Expressway-E e che sia attivo. Passare a Stato > Unified Communications > Stato tunnel SSH Unified Communications. È necessario visualizzare l'FQDN del Web e la destinazione deve essere Expressway-E.

Target	Domain	Status	Peer
vcs-e.alero.local	webbridge.alero.aca	Active	10.48.36.247
vcs-e.alero.local	alero.lab	Active	10.48.36.247
vcs-e.alero.local	alero.local	Active	10.48.36.247
vcs-e2.alero.local	alero.lab	Active	10.48.36.247
vcs-e2.alero.local	webbridge.alero.aca	Active	10.48.36.247
vcs-e2.alero.local	alero.local	Active	10.48.36.247

Passaggio 2. Verificare che il server TURN sia stato aggiunto al server CMS

Nel menu API CMS, cercare i server di tornitura e fare clic su ciascuno di essi. All'interno di ogni oggetto, è disponibile un link per controllare lo stato:



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

L'output visualizza informazioni che includono il tempo di andata e ritorno (RTT, Round-trip time) in millisecondi (Ms) associato al server TURN. Queste informazioni sono importanti per la selezione CB del miglior server TURN da utilizzare.

Passaggio 3. Verifica dell'utilizzo di TURN Relay durante una chiamata in corso

Nel momento in cui viene effettuata una chiamata in tempo reale con l'uso del client WebRTC, è possibile visualizzare lo stato di TURN media Relay su Expressway. Passare a Stato > Inoltra uso, quindi scegliere Visualizza.

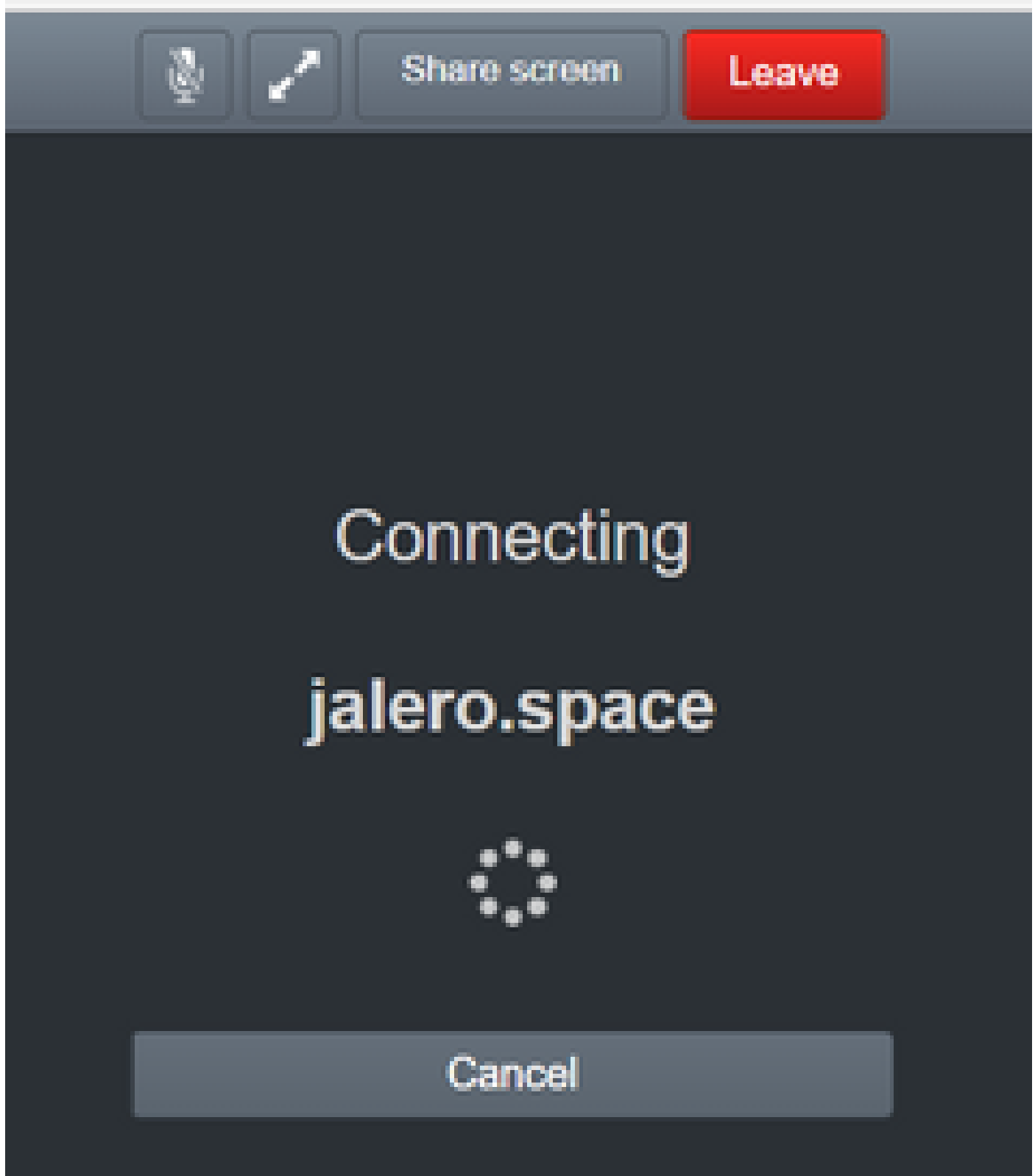
## Risoluzione dei problemi

Strumenti utili:

- File HAR dai browser ([Come generare un file HAR in Chrome o Firefox](#))
- Dump degli internals WebRTC dal browser - chrome://webrtc-internals o edge://webrtc-internals - Crea un dump non appena viene tentato l'accesso.
- Anche i registri della console del browser possono essere utili.
- Wireshark dal client, Exp E, Exp C e CMS.
- Exp E network.http.trafficserver debug per la risoluzione dei problemi dei socket Web.

Il client WebRTC esterno si connette ma non dispone di supporti (a causa di un errore ICE)

In questo scenario, il client RTC è in grado di risolvere l'ID chiamata a jalero.space, ma quando si immette il proprio nome e si seleziona Partecipa alla chiamata, il client visualizza Connessione, come mostrato in questa immagine:



Dopo circa 30 secondi, viene reindirizzato alla pagina Web iniziale.

Per risolvere il problema, procedere come segue:

- Avviare wireshark sul client RTC quando si tenta di effettuare una chiamata e, quando si verifica l'errore, arrestare la cattura.
- Dopo il verificarsi del problema, controllare i registri eventi CMS:

Passare a Registri > Registri eventi su CMS WebAdmin.

- Filtrate le tracce di Wireshark con uno stordimento. Vedere questo esempio:



Nelle tracce di Wireshark, il client invia una richiesta di allocazione con le credenziali configurate al server Expressway-E TURN sulla porta 3478:

```
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
```

Il server risponde con l'errore di allocazione:

```
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
```

o

```
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
```

Nei log del CMS viene visualizzato questo messaggio:

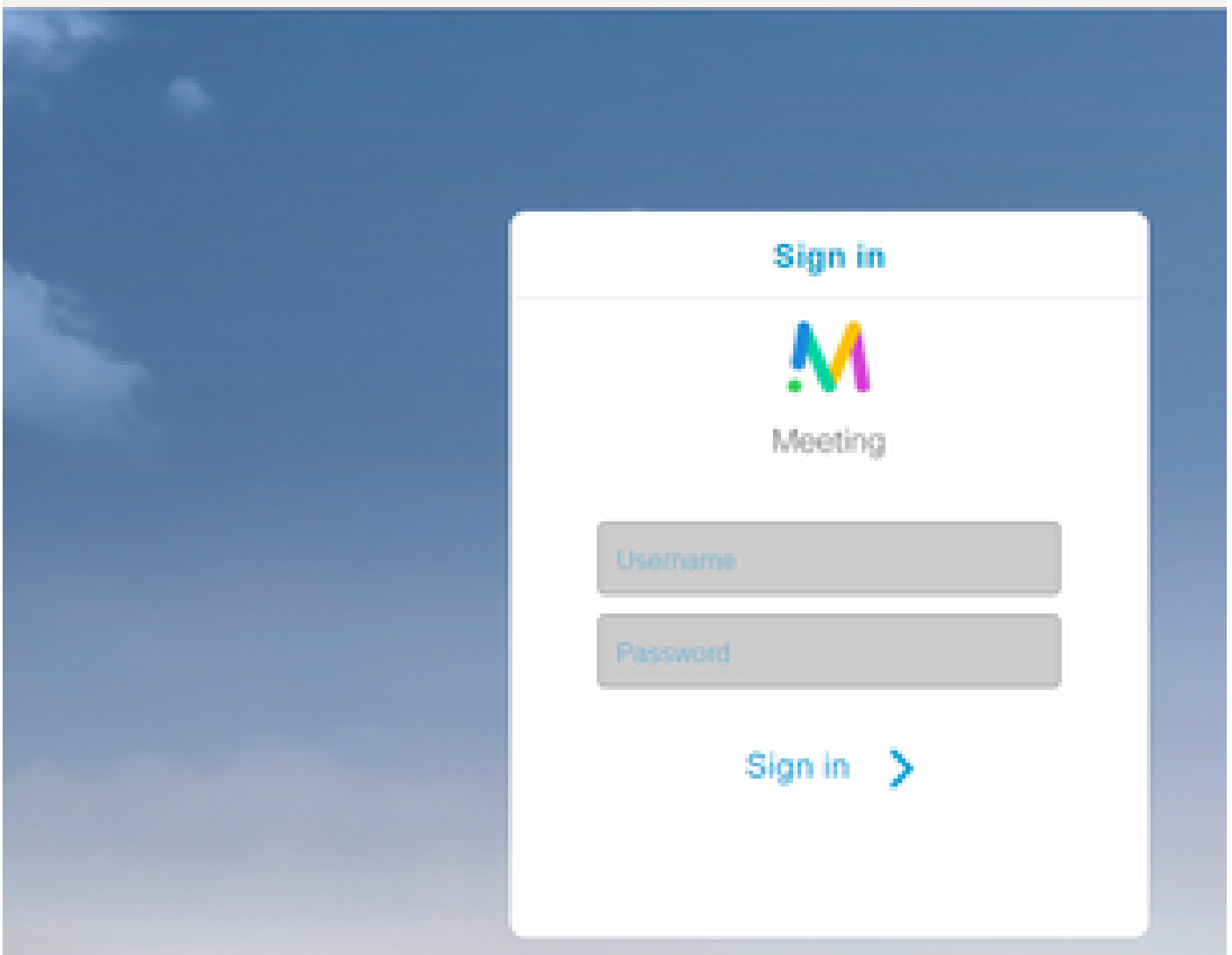
```
2017-04-15    10:34:56.536    Warning    call 7: ICE failure 4 (unauthorized - check credentials)
```

Soluzione:

Controllare le credenziali TURN configurate nel CMS e verificare che corrispondano a quelle configurate nel database di autenticazione locale Expressway-E.

Il client WebRTC esterno non ottiene l'opzione Join Call

⚠ Not secure | <https://webbridge.alero.aca>



Nella pagina Stato ponte di chiamata > Generale viene visualizzato quanto segue:

```
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" f
2017-04-15 11:55:50.835 Info failed to establish connection to web bridge link 2 (unknown erro
```

Soluzione:

- Verificare che il Callbridge sia in grado di risolvere l'URL di join nell'FQDN di webbridge (il Callbridge non deve risolverlo nell'indirizzo IP di Expressway-E).
- Scaricare la cache DNS sul Callbridge, tramite l'interfaccia della riga di comando (CLI), con il comando `dns flush`.
- Verificare che il WebB consideri attendibile il certificato del server Callbridge (non l'autorità emittente).


Il client WebRTC esterno è bloccato (durante il caricamento dei supporti) durante la connessione a Cospace e viene quindi reindirizzato alla pagina iniziale Web

Soluzione:

- Verificare che il CMS sia in grado di risolvere il record SRV \_xmpp-client nella rete interna per il dominio CB e che le connessioni WebRTC funzionino internamente.
- Raccogliere un'acquisizione Wireshark sul client e la registrazione diagnostica, incluso tcpdump su Expressway-E durante il tentativo di connessione con il client esterno:

Passare a Manutenzione > Diagnostica > Registrazione diagnostica e assicurarsi che l'opzione Esegui tcpdump durante la registrazione sia selezionata, come mostrato in questa immagine, prima di selezionare Avvia nuovo registro:

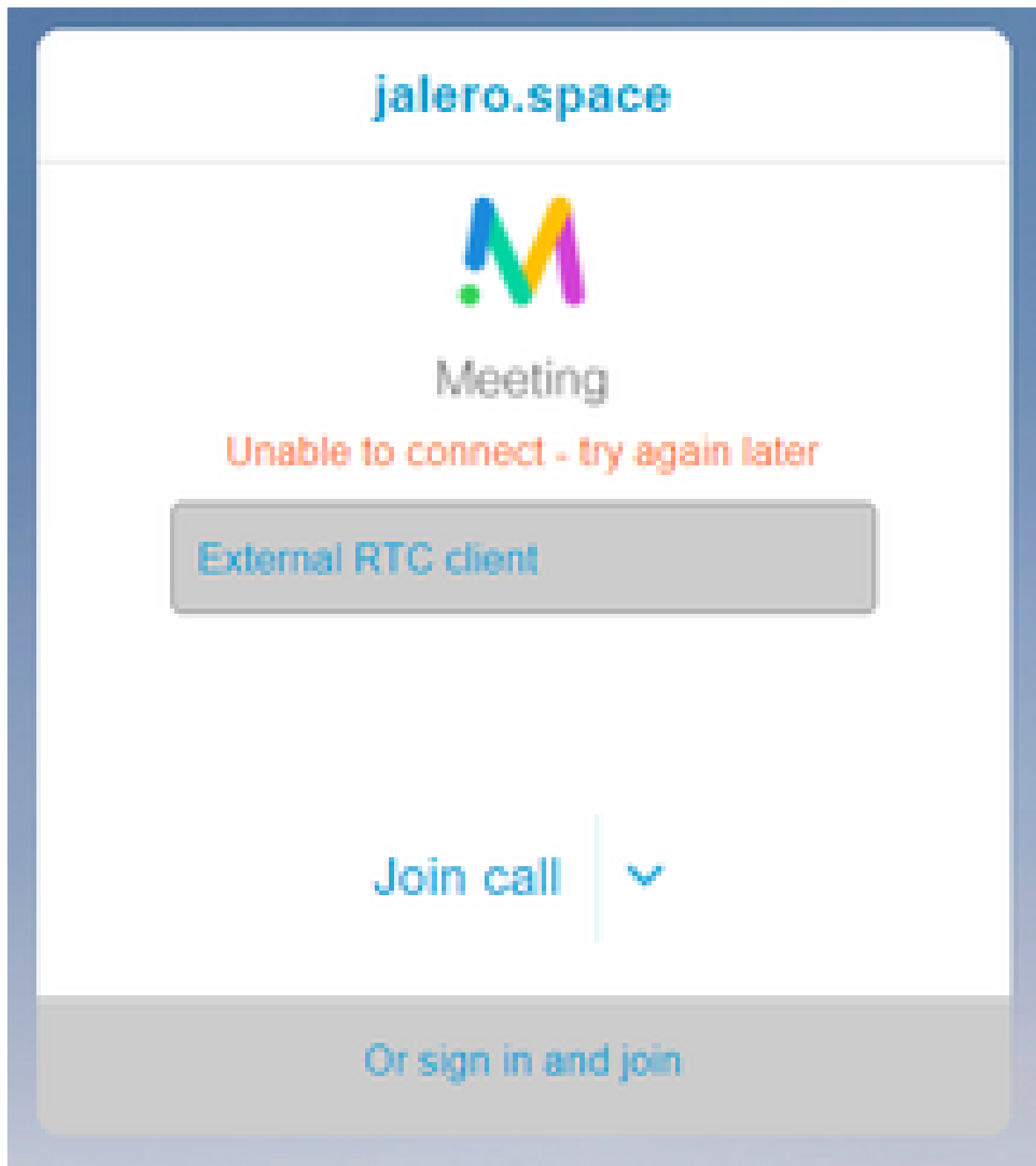


 Nota: assicurarsi che l'acquisizione di Wireshark sul dispositivo del client e la registrazione su Expressway-E siano avviate prima di riprodurre la chiamata che ha generato l'errore. Una volta riprodotta la chiamata non riuscita, interrompere e scaricare la registrazione su Expressway-E e l'acquisizione sul client.

- Estrarre/decomprimere il pacchetto di log scaricato da Expressway-E e aprire il file .pcap acquisito sull'interfaccia pubblica.
- Filtra su entrambe le acquisizioni dei pacchetti con stordimento:
  - Cercare quindi la richiesta di binding dal client esterno all'indirizzo IP pubblico di Expressway-E, fare clic con il pulsante destro del mouse e selezionare Segui > Flusso UDP.
  - Di solito la porta di destinazione della richiesta Binding dal client è compresa nell'intervallo 24000-29999, che è l'intervallo di porte TURN relays su Expressway-E.
- Se non si riceve alcuna risposta alle richieste di binding dal lato del client, verificare l'acquisizione di Expressway-E se le richieste sono in arrivo.
- Se le richieste sono in arrivo e Expressway-E risponde al client, verificare se il firmware esterno consente il traffico UDP in uscita.
- Se le richieste non arrivano, controllare il firmware per verificare che l'intervallo di porte elencato in precedenza non sia bloccato.
- Se Expressway-E è implementato con un controller a doppia interfaccia di rete (DUAL-NIC) con modalità NAT statica abilitata ed è X12.5.2 o precedente, verificare che la riflessione NAT sia supportata e configurata nel firmware esterno. A partire dalla versione X12.5.3, questa funzionalità non è più necessaria per un'Expressway autonoma.

Il client WebRTC esterno non è in grado di collegarsi a Cospace e riceve l'avviso (impossibile connettersi - riprovare più tardi)

In questo scenario, il client RTC è in grado di risolvere l'ID chiamata a jalero.space, ma quando si immette il proprio nome e si seleziona Partecipa alla chiamata, l'avviso Impossibile connettersi - Riprova più tardi viene visualizzato immediatamente:



Soluzione:

Verificare che il CMS, nella rete interna, sia sempre in grado di risolvere il record SRV \_xmpp-client per il dominio CB.

## Informazioni correlate

- [Guida all'utilizzo della porta IP di VCS/Expressway](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)



## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).