

# Expressway를 통해 CMS WebRTC 또는 Web App 프록시 구성

## 목차

---

### [소개](#)

### [사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

### [배경 정보](#)

### [구성](#)

[네트워크 다이어그램](#)

[컨피그레이션 단계](#)

[1단계. Expressway-C에 CMS WB 통합](#)

[2단계. Expressway-E에서 TURN을 활성화하고 로컬 인증 데이터베이스에 인증 자격 증명을 추가합니다.](#)

[3단계. Expressway-E의 관리 포트 변경](#)

[4단계. CMS 서버에 미디어 NAT 통과를 위한 TURN 서버로 Expressway-E를 추가합니다](#)

[다음을 확인합니다.](#)

[1단계. Expressway-C에서 WB가 올바르게 통합되었는지 확인합니다.](#)

[2단계. TURN 서버가 CMS 서버에 추가되었는지 확인합니다.](#)

[3단계. 진행 중인 통화 중 TURN 릴레이 사용 확인](#)

### [문제 해결](#)

[외부 WebRTC 클라이언트가 연결되지만 미디어가 없음\(ICE 오류로 인해\)](#)

[외부 WebRTC 클라이언트가 참가 통화 옵션을 가져오지 않음](#)

[Cospace에 연결할 때 외부 WebRTC 클라이언트가 \(미디어를 로드하는 동안\) 멈춘 다음 WB 초기 페이지로 리디렉션됩니다.](#)

[외부 WebRTC 클라이언트가 Cospace에 참가할 수 없으며 경고가 표시됩니다\(연결할 수 없음 - 나중에 다시 시도\).](#)

### [관련 정보](#)

---

## 소개

이 문서에서는 Expressway를 통한 CMS(Cisco Meeting Server) WebRTC 구성 및 문제 해결 단계에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.


- Expressway X12.6.1 이상(x12.6.1 이상은 Exp TURN 동작의 변경으로 인해 CMS 2.9.2 이상에서만 작동할 수 있음)
- CMS 서버 2.9.3 이상

- NAT(Network Address Translation)
- NAT 주변의 릴레이(TURN)를 사용한 통과
- NAT용 STUN(Session Traversal Utility)
- DNS(Domain Name System)

#### 구성 사전 요구 사항:

- 기본 모바일 및 원격 액세스(MRA) 관련 설정(UC Traversal zone, SSH 터널)이 Expressway에서 이미 활성화되어 구성되어 있어야 합니다. MRA 가이드는 [여기](#)를 클릭하십시오.
- CMS 2.9.x - CMS에서 구성 및 활성화된 WebBridge(WB), XMPP 및 CallBridge의 경우 컨피그레이션 [가이드를 참조하십시오](#)
- Expressway-E에 설치된 TURN 옵션 키
- 공용 인터넷에서 Expressway-E의 공용 IP 주소로 연결되는 방화벽에서 열린 TCP 포트 443
- 공용 인터넷에서 Expressway-E의 공용 IP 주소로 연결되는 방화벽에서 열린 TCP 및 UDP 포트 3478(TURN 요청)
  - CMS API의 'turnservers'에 tcpPortNumberOverride가 3478로 설정된 경우에만 TCP 3478이 필요합니다.
- CMS에서 Expressway-E의 프라이빗 IP 주소로 향하는 방화벽에서 열리는 UDP 포트 3478(TURN 요청)입니다(Expressway-E에서 Dual-NIC를 사용하는 경우).
  - CMS 2.9.2 및 이전 버전에서는 Exp E에 바인딩 요청을 보내고, 2.9.3 이후 버전에서는 할당 요청을 보냅니다
- Expressway-E의 공용 IP 주소로 확인 가능한 webbridge용 가입 URL에 대한 외부 DNS 레코드
- Webbridge 서버의 IP 주소로 확인 가능한 조인 URL에 대한 내부 DNS 레코드입니다.
- X12.5.2 이하를 실행하는 경우 Expressway-E의 공용 IP 주소에 대해 외부 방화벽에서 NAT 반사가 허용되는지 확인하고 컨피그레이션과 같이 [여기를 클릭합니다](#). X12.5.3부터 독립형 Expressway에서는 이 기능이 더 이상 필요하지 않습니다.
- TURN에 포트 443을 사용하는 경우에도 외부 방화벽의 미디어에 대해 UDP 포트 3478을 열어야 합니다.


---

 주의: TCP 포트 443이 활성화된 경우 Expressway는 더 이상 TCP 포트 3478에서 응답할 수 없습니다.

---

 참고: Jabber 게스트 서비스에 사용되는 Expressway 쌍은 CMS WebRTC 프록시 서비스에 사용할 수 없습니다.

---

 참고: 이전 버전에서 3.0 이상으로 업그레이드할 경우 [Cisco Meeting Server 2.9에서 3.0\(및 이후\)으로 원활하게 업그레이드하기 위한 지침](#)을 참조하십시오

---

#### 사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 제한되지 않지만 최소 소프트웨어 버전 요구 사항을 충족해야 합니다.

- CMS API(Application Program Interface)
- 고속도로
- CMS 서버

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

WebRTC 프록시 지원이 버전 X8.9.2에서 Expressway에 추가되어 오프프레미스 사용자가 Cisco Meeting Server Web Bridge로 이동할 수 있습니다.

외부 클라이언트 및 게스트는 지원되는 브라우저 이외의 소프트웨어 없이도 스페이스를 관리하거나 참가할 수 있습니다. [지원되는](#) 브라우저 목록을 보려면 여기를 클릭하십시오.

2021년 2월 5일자로 CMS 3.1.1에서 지원되는 브라우저는 다음과 같습니다.

Table 2: Cisco Meeting Server web app tested on browsers and versions

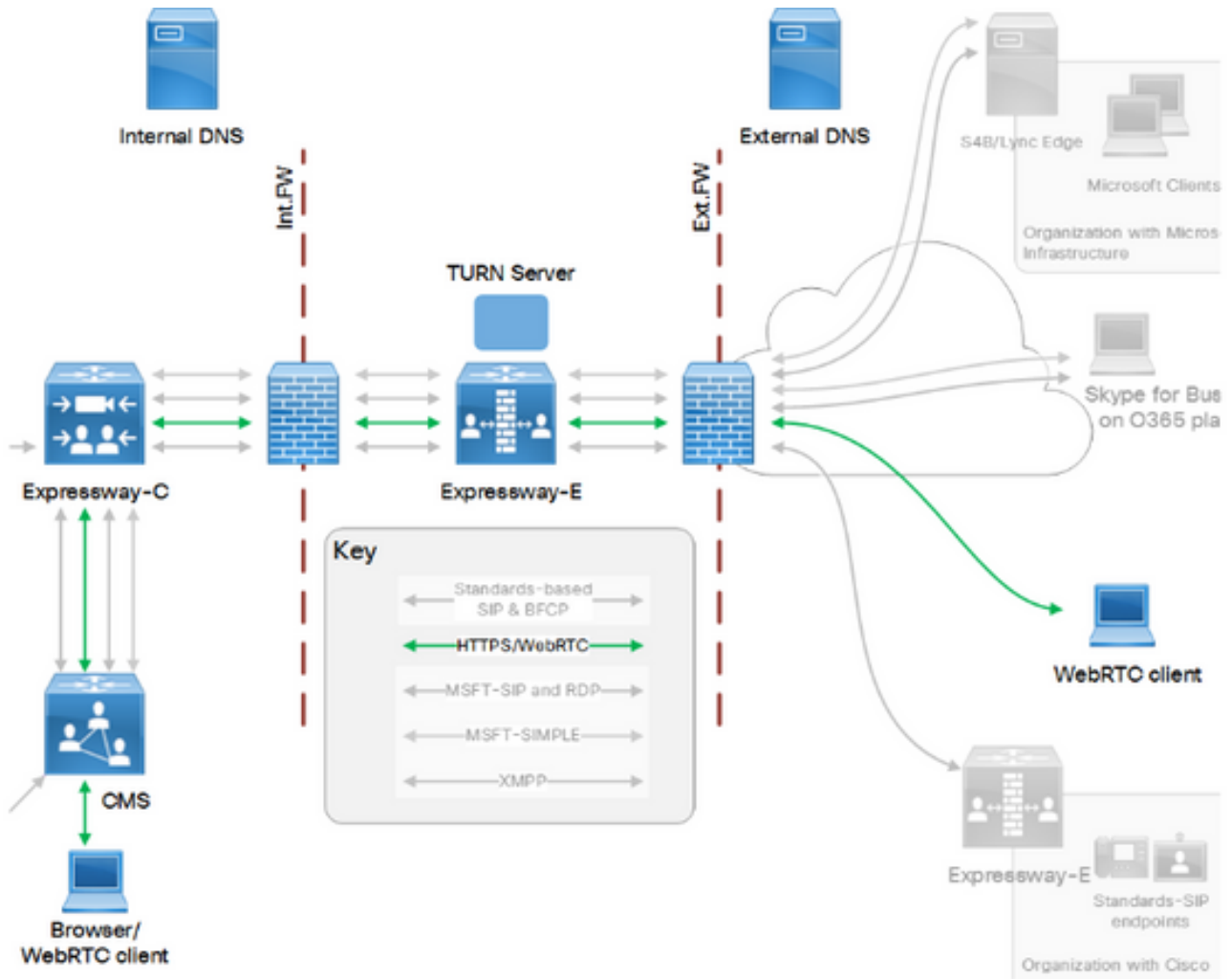
Browsers	Versions
Google Chrome (Windows, macOS and Android)	85
Mozilla Firefox (Windows)	82
Chromium-based Microsoft Edge (Windows)	88
Apple Safari for macOS	13.x and 14.0
Apple Safari for iOS	iOS versions: 13.x and 14.0
Yandex (Windows)	20.8 and 20.11

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.

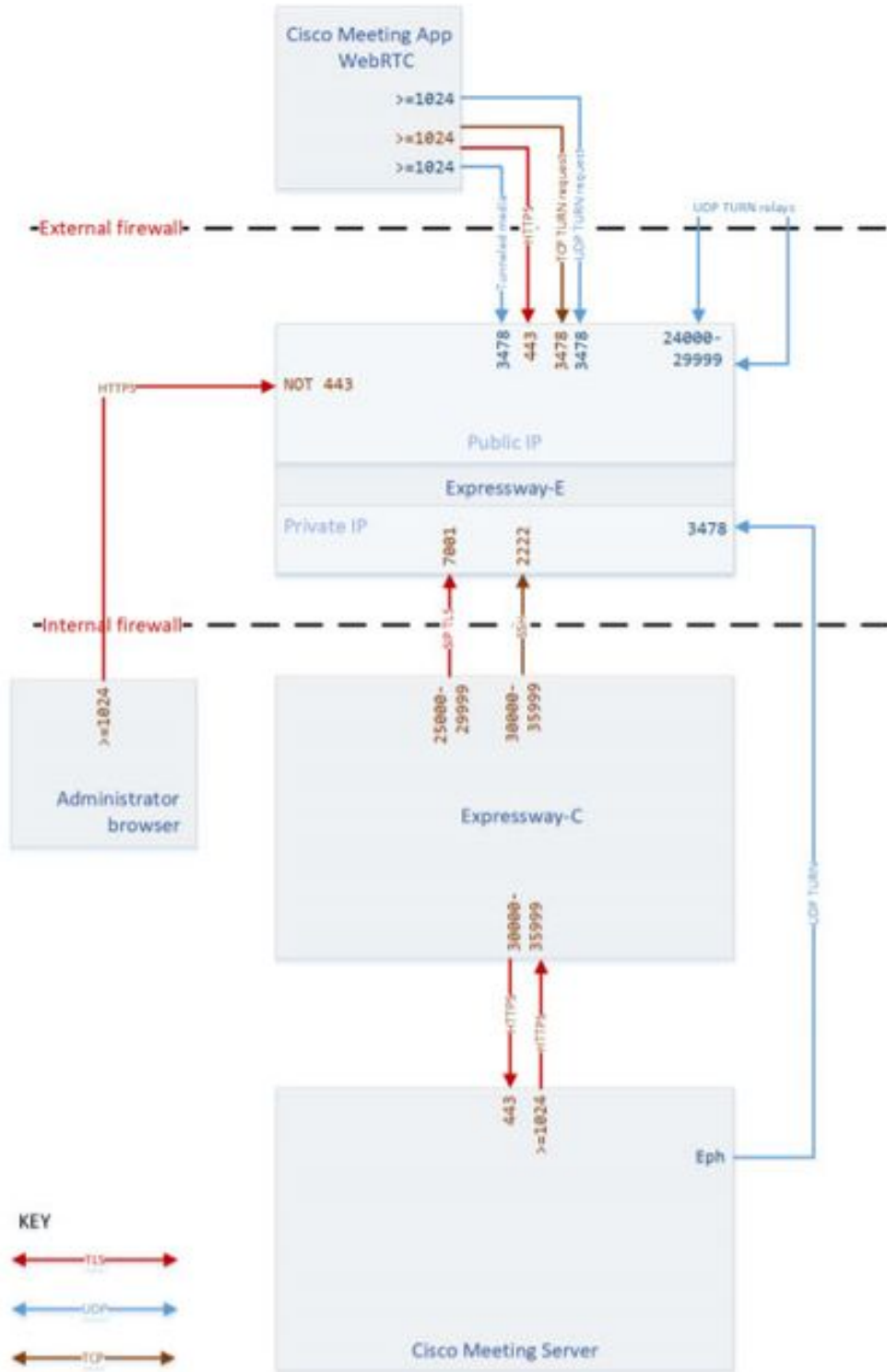
## 구성

### 네트워크 다이어그램



이 이미지는 CMS WebRTC용 웹 프록시의 연결 흐름(Exp IP 포트 사용 컨피그레이션 가이드에서)의 [예를](#) 제공합니다.

# Web Proxy for Cisco Meeting Server Connections



참고: X12.5.2 이하를 실행하는 경우 Expressway-E 및 공용 IP 주소에 대한 NAT 반사를 허용하도록 외부 방화벽을 구성해야 합니다(일반적으로 방화벽은 소스 및 대상 IP 주소가 동일한 패킷을 불신함). X12.5.3부터 독립형 Expressway에서는 이 기능이 더 이상 필요하지 않습니다.

## 컨피그레이션 단계


1단계. Expressway-C에 CMS WB 통합

- Configuration(컨피그레이션) > Unified Communication(Unified Communication) > Cisco Meeting Server(Cisco Meeting Server)로 이동합니다.
- Meeting Server 웹 프록시를 사용하도록 설정합니다.
- Guest account client URI(게스트 어카운트 클라이언트 URI) 필드에 Join URL(조인 URL)을 입력합니다.
- 저장을 클릭합니다.
- CMS 조인 URL을 Expressway-E 서버 인증서에 주체 대체 이름(SAN)으로 추가합니다. [Cisco VCS Certificate Creation and Use Deployment Guide](#)를 참조하십시오.


The screenshot shows the Cisco Meeting Server configuration interface. At the top, there are navigation tabs: Status, System, Configuration, Applications, Users, and Maintenance. Below these is the 'Cisco Meeting Server' header. Underneath, there's a 'Meeting Server configuration' section. It includes a 'Meeting Server Web Proxy' dropdown menu set to 'Enable'. Below that, the 'Guest account client URI' field is highlighted with a red border and contains the text 'webbridge.alero.aca'. At the bottom left of the configuration area, there is a 'Save' button.

2단계. Expressway-E에서 TURN을 활성화하고 로컬 인증 데이터베이스에 인증 자격 증명을 추가합니다.

- Configuration(컨피그레이션) > Traversal(접근) > TURN(회전)로 이동합니다.
- TURN SERVICES를 OFF에서 ON으로 활성화합니다.
- Configure TURN client credentials on local database(로컬 데이터베이스에서 TURN 클라이언트 자격 증명 구성)를 선택하고 자격 증명(사용자 이름 및 비밀번호)을 추가합니다.

 참고: Expressway-E 클러스터가 있고 모두 TURN 서버로 사용될 경우 모든 노드에서 해당 클러스터를 활성화해야 합니다. API를 통해 두 개의 개별 turnServer 인스턴스를 구성하고 이를 클러스터의 각 Expressway-E 서버로 전달해야 합니다(한 Expressway-E 서버에 대한 프로세스를 표시하는 4단계의 컨피그레이션 프로세스에 따라). 두 번째 turnServer의 컨피그레이션은 다른 Expressway-E 서버에 대한 각 IP 주소와 턴 자격 증명을 사용하는 경우에만 유사합니다.

 참고: TCP/HTTPS 트래픽의 경우 고속 도로 앞에 네트워크 로드 밸런서를 사용할 수 있지만

 TURN 미디어는 클라이언트에서 TURN 서버의 공용 IP로 계속 이동해야 합니다. TURN 미디어는 네트워크 로드 밸런서를 통과하지 않아야 합니다


### 3단계. Expressway-E의 관리 포트 변경

이 단계는 webrtc 연결이 TCP 443에서 제공되므로 필요합니다. 그러나 Exp 12.7에는 443에 사용할 수 있는 새로운 DMI(Dedicated Management Interface)가 도입되었습니다.

a. 시스템 > 관리로 이동합니다.

b. Web server configuration(웹 서버 컨피그레이션)의 드롭다운 옵션에서 웹 관리자 포트를 445로 변경한 다음 Save(저장)를 클릭합니다.

c. WebRTC 프록시 서비스에 사용되는 모든 Expressway-E에서 3a-3b 단계를 반복합니다.

 참고: WebRTC 클라이언트는 443을 사용하므로 관리 포트를 변경하는 것이 좋습니다. WebRTC 브라우저에서 포트 80에 액세스하려고 하면 Expressway-E가 연결을 443으로 리디렉션합니다.

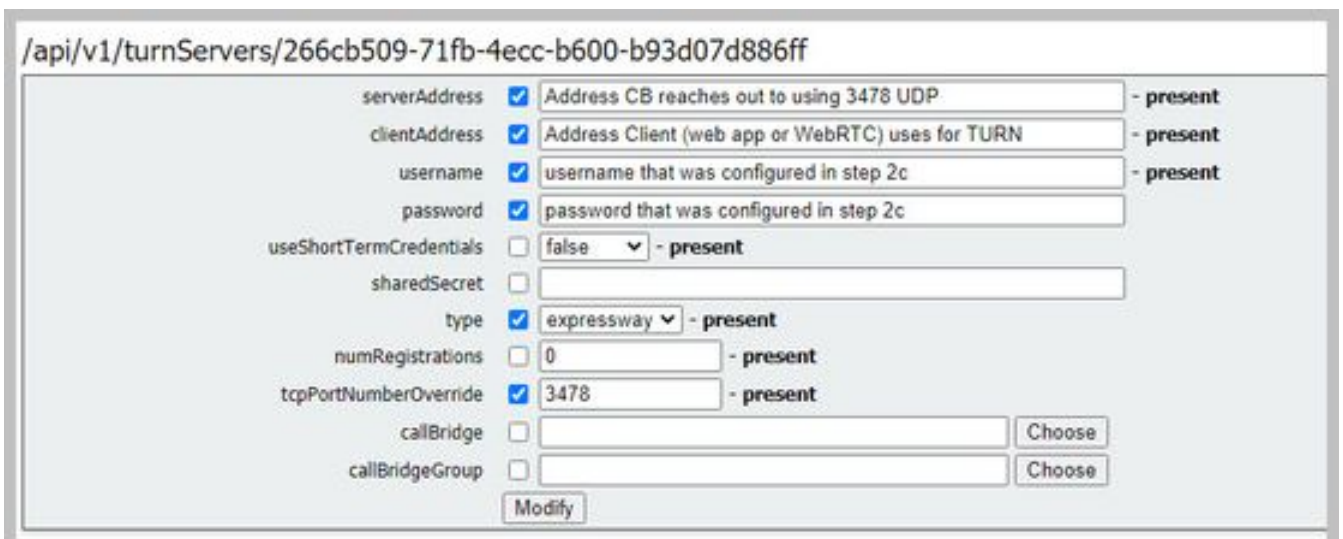
### 4단계. CMS 서버에 미디어 NAT 통과를 위한 TURN 서버로 Expressway-E를 추가합니다

CMS 2.9.x에서 Configuration(컨피그레이션) → API(API) 메뉴를 사용하여 턴 서버를 추가합니다.

- serverAddress: (Expressway의 전용 IP 주소)
- clientAddress: (Expressway의 공용 IP 주소)
- 유형: (expressway)
- username(사용자 이름): (2c단계에서 구성)
- 비밀번호: (2c단계에서 구성된 대로)
- tcpPortNumberOverride: 3478

d. TURN에 사용할 모든 Expressway-E 서버에 대해 4c단계를 반복합니다.

이 이미지는 컨피그레이션 단계의 예를 제공합니다.



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	

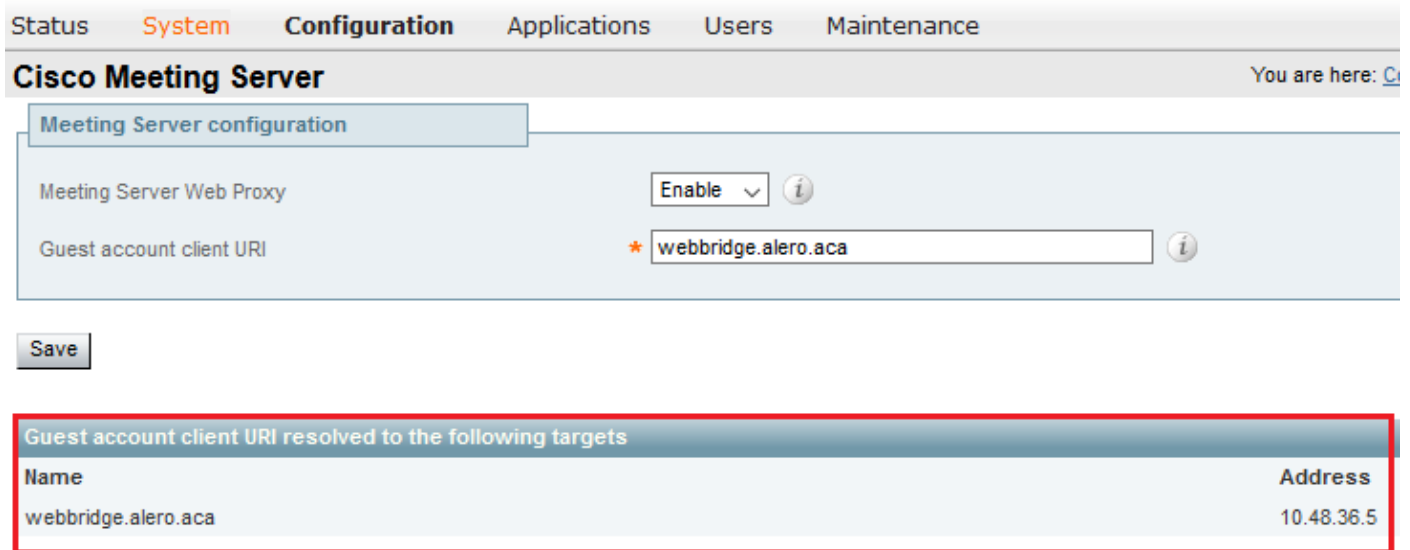
Modify

## 다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

1단계. Expressway-C에서 WB가 올바르게 통합되었는지 확인합니다.

a. Configuration(컨피그레이션) > Unified Communication(Unified Communication) > Cisco Meeting Server(Cisco Meeting Server)로 이동합니다. WB의 IP 주소가 표시되어야 합니다.




The screenshot shows the Cisco Meeting Server configuration interface. The 'Meeting Server Web Proxy' is set to 'Enable' and the 'Guest account client URI' is 'webbridge.alero.aca'. Below the configuration, a table shows the resolved target for the URI.

Name	Address
webbridge.alero.aca	10.48.36.5

b. Configuration(컨피그레이션) > Unified Communication(유니파이드 커뮤니케이션) > HTTP allow list(HTTP 허용 목록) > Automatically added rules(자동으로 추가된 규칙)로 이동합니다. 규칙에 추가되었는지 확인합니다.

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

 참고: 규칙은 단순히 WB에 대한 HTTPS 트래픽의 프록시를 허용하기 위한 것이며, 반드시 통합 커뮤니케이션을 위한 것은 아니기 때문에 검색된 노드에서 WB를 찾을 것으로 예상되지 않습니다.

c. WB FQDN에 대한 SSH(Secure Shell) 터널이 Expressway-C에서 Expressway-E로 구축되었으며 활성 상태인지 확인합니다. Status(상태) > Unified Communications > Unified Communications SSH tunnels status(Unified Communications SSH 터널 상태)로 이동합니다. WB의 FQDN을 확인해야 하며 대상은 Expressway-E여야 합니다.



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

2단계. TURN 서버가 CMS 서버에 추가되었는지 확인합니다.

CMS API 메뉴에서 turn servers(서버 전환)를 조회하고 각 서버를 클릭합니다. 각 객체 내에는 상태를 확인할 수 있는 링크가 있습니다.

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

TURN 서버와 연결된 RTT(왕복 시간)를 포함하는 정보가 출력에 표시됩니다(밀리초). 이 정보는 사용할 최상의 TURN 서버의 CB 선택에 중요합니다.

3단계. 진행 중인 통화 중 TURN 릴레이 사용 확인

WebRTC 클라이언트를 사용하여 라이브 통화를 할 때 Expressway에서 TURN 미디어 릴레이 상태를 볼 수 있습니다. Status(상태) > TURN relay usage(릴레이 사용 회전)로 이동한 다음 view(보기)를 선택합니다.

## 문제 해결

유용한 툴:

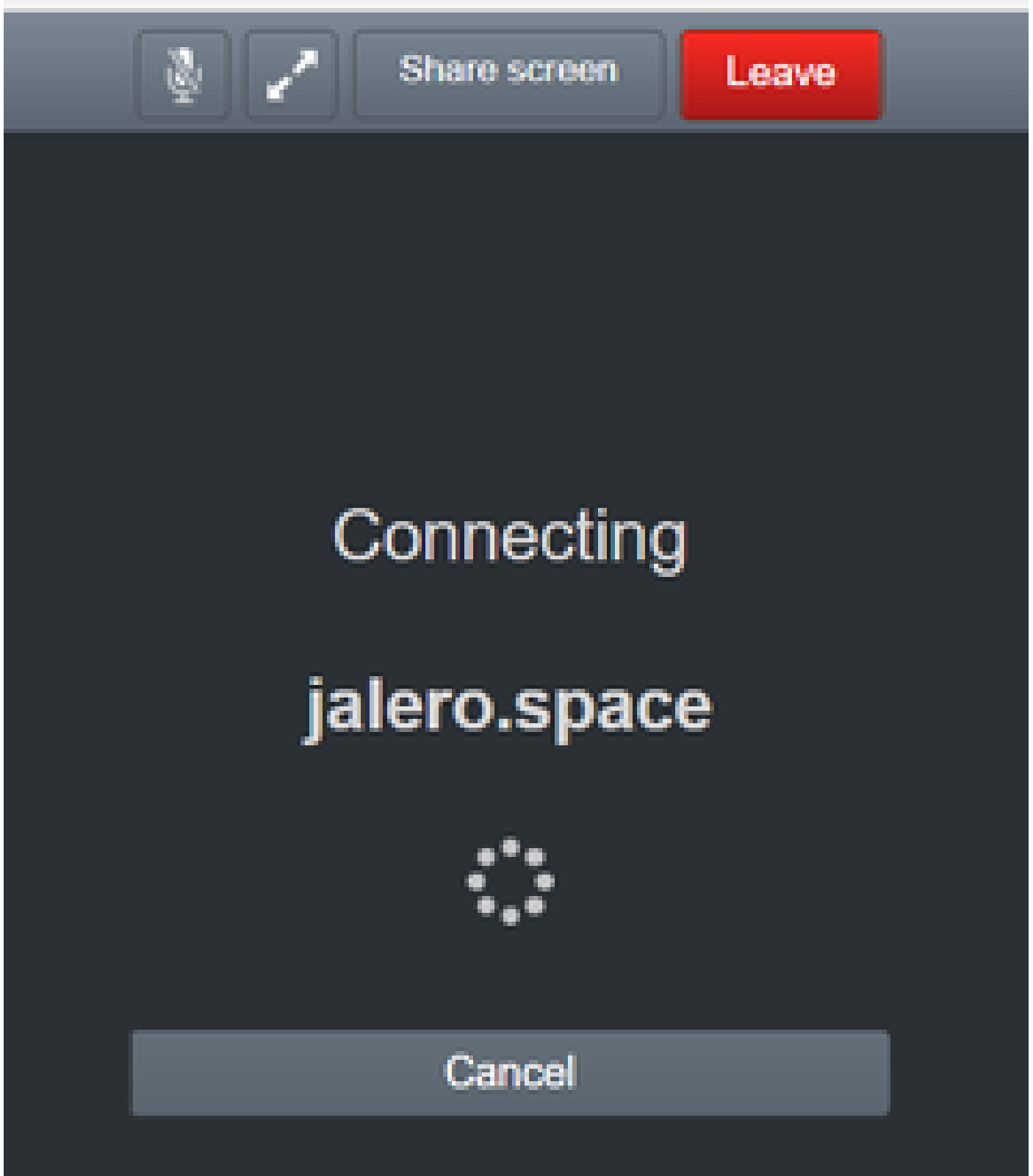
- 브라우저에서 HAR 파일([Chrome 또는 Firefox에서 HAR 파일을 생성하는 방법](#))
- 브라우저에서 WebRTC 내부 덤프(chrome://webrtc-internals 또는 edge://webrtc-internals) -

참가를 시도하는 즉시 덤프를 만듭니다.

- 브라우저 콘솔 로그도 유용합니다.
- 클라이언트, Exp E, Exp C 및 CMS에서 Wireshark 캡처
- Exp E network.http.trafficserver 디버깅은 websocket 문제 해결에 도움이 됩니다.

외부 WebRTC 클라이언트가 연결되지만 미디어가 없음(ICE 오류로 인해)

이 시나리오에서 RTC 클라이언트는 통화 ID를 jalero.space로 확인할 수 있지만 이름을 입력하고 통화 참가를 선택하면 다음 이미지와 같이 클라이언트에 연결이 표시됩니다.



약 30초 후에, 그것은 초기 WB 페이지로 리디렉션된다.

문제를 해결하려면 다음 단계를 완료하십시오.

- 통화를 시도할 때 RTC 클라이언트에서 wireshark를 시작하고 오류가 발생하면 캡처를 중지합니다.
- 문제가 발생한 후 CMS 이벤트 로그를 확인합니다.

CMS WebAdmin에서 Logs(로그) > Event logs(이벤트 로그)로 이동합니다.

- Wireshark 추적을 스톤으로 필터링합니다. 다음 예를 참조하십시오.



Wireshark 추적에서는 클라이언트가 자격 증명에 구성된 Allocate Request를 포트 3478의 Expressway-E TURN 서버로 전송하는 것을 볼 수 있습니다.

```
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
```

서버가 할당 오류로 응답합니다.

```
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
```

또는

```
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
```

CMS 로그에는 다음 로그 메시지가 표시됩니다.

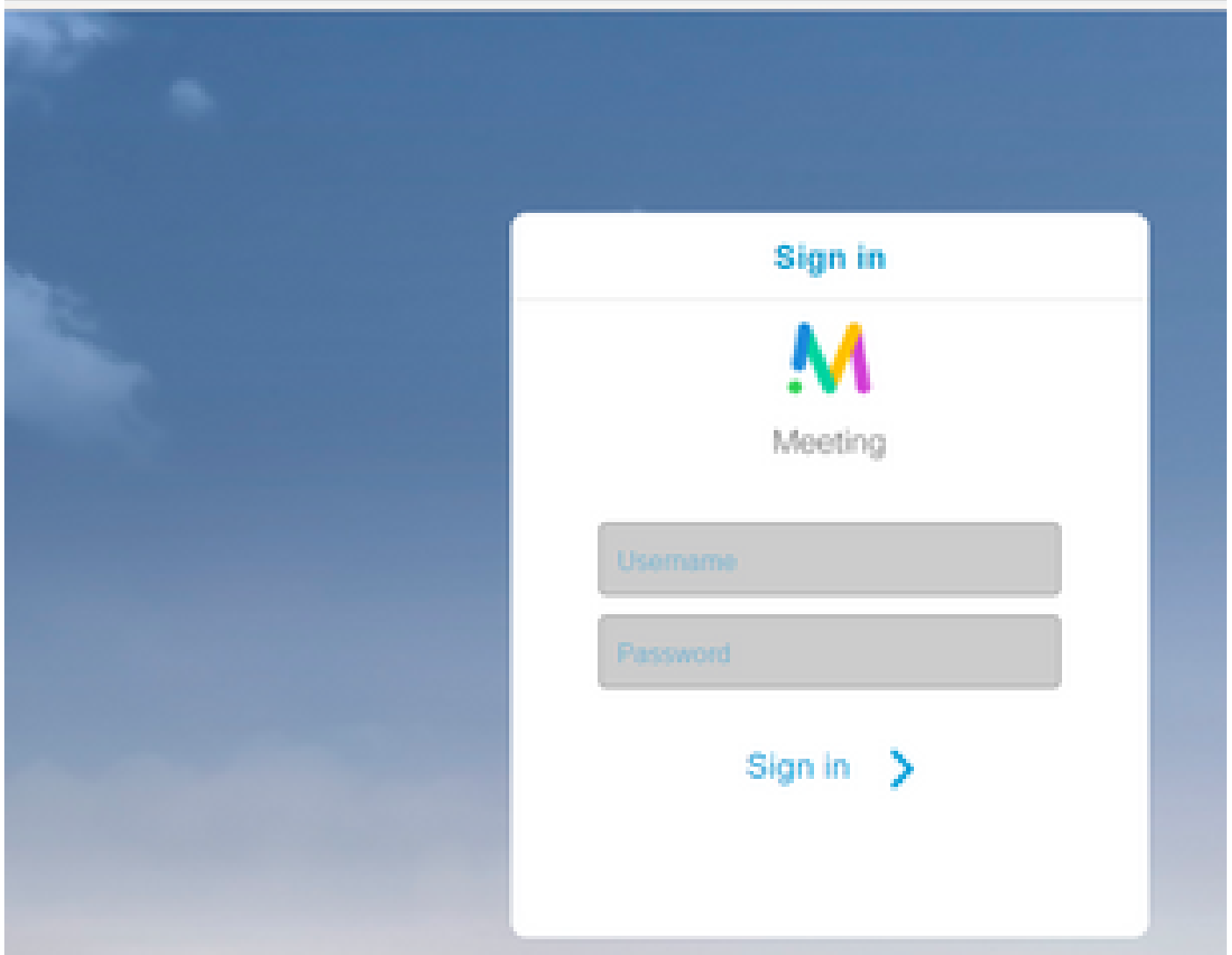
```
2017-04-15    10:34:56.536    Warning    call 7: ICE failure 4 (unauthorized - check credentials)
```

해결책:

CMS에 구성된 TURN 자격 증명을 확인하고 Expressway-E 로컬 인증 데이터베이스에 구성된 자격 증명과 일치하는지 확인합니다.

외부 WebRTC 클라이언트가 참가 통화 옵션을 가져오지 않음

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



Callbridge Status(Callbridge 상태) > General(일반) 페이지에 다음과 같이 표시됩니다.

```
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
```

해결책:

- Callbridge가 Join URL을 webbridge FQDN으로 확인할 수 있는지 확인합니다. Callbridge는 Expressway-E의 IP 주소로 확인하지 않아야 합니다.
- CLI(Command Line Interface)를 통해 Callbridge의 DNS 캐시를 dns flush 명령으로 플러시합니다.
- WB가 Callbridge 서버 인증서(발급자 아님)를 신뢰하는지 확인합니다.


Cospace에 연결할 때 외부 WebRTC 클라이언트가 (미디어를 로드하는 동안) 멈춘 다음 WB 초기 페이지로 리디렉션됩니다.

해결책:

- CMS가 CB 도메인에 대한 내부 네트워크의 \_xmpp-client SRV 레코드를 확인할 수 있는지 확인하고 WebRTC 연결이 내부적으로 작동하는지 확인합니다.
- 외부 클라이언트에 연결을 시도하는 동안 클라이언트에서 Wireshark 캡처 및 Expressway-E에서 tcpdump를 비롯한 진단 로깅을 수집합니다.

Maintenance(유지 관리) > Diagnostics(진단) > Diagnostic logging(진단 로깅)으로 이동하고 Start new log(새 로그 시작)를 선택하기 전에 이 이미지에 표시된 대로 Take tcpdump while logging(기록 중 tcpdump 가져오기)이 선택되어 있는지 확인합니다.



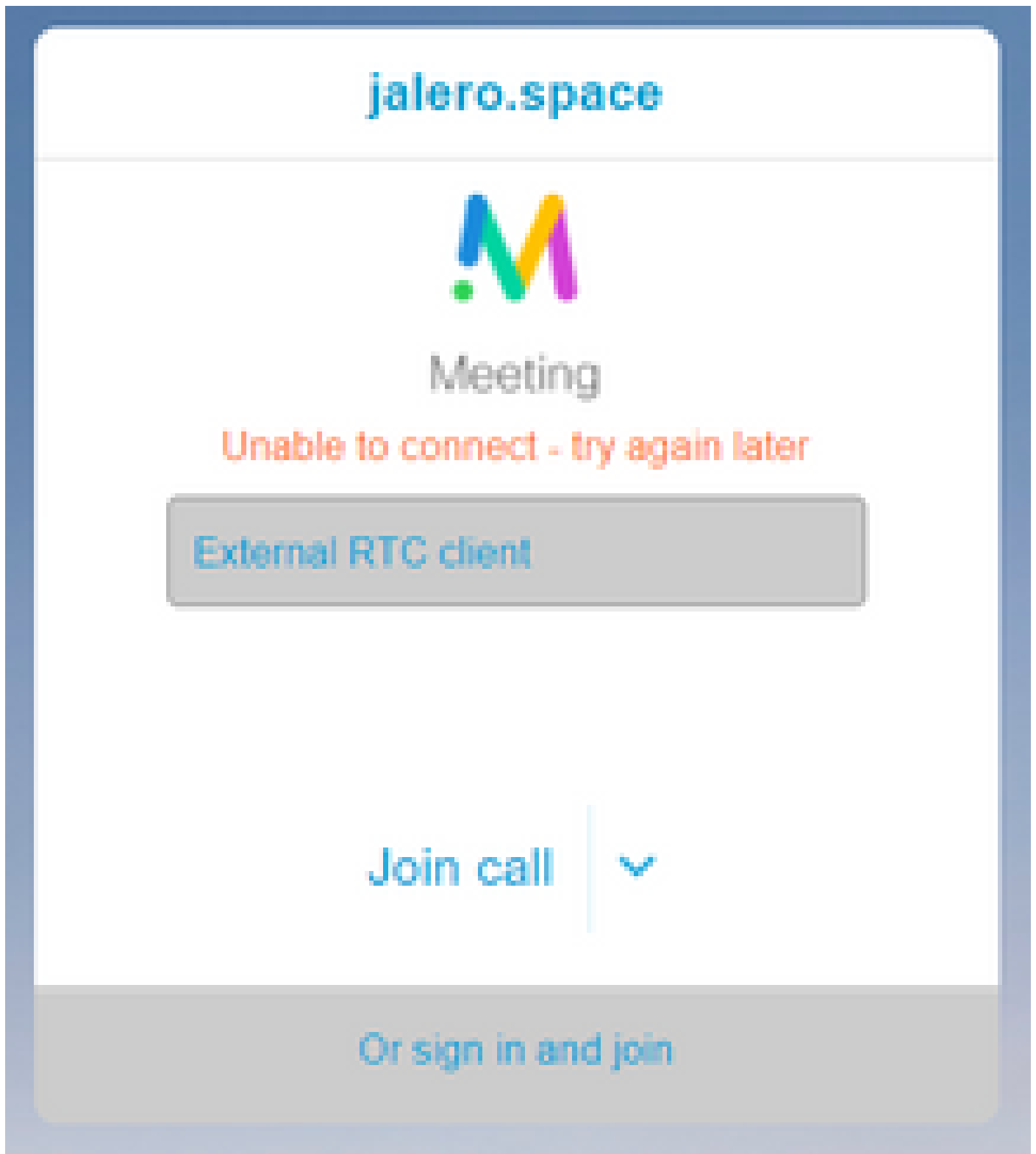
 참고: 실패한 통화를 재생하기 전에 클라이언트 디바이스의 Wireshark 캡처 및 Expressway-E의 로깅이 시작되었는지 확인하십시오. 오류가 발생한 통화가 재현되면 Expressway-E에서 로깅을 중지하고 클라이언트에서 캡처를 다운로드합니다.

- Expressway-E에서 다운로드한 로그 번들의 압축을 풀거나 압축을 풀고 공용 인터페이스에서 가져온 .pcap 파일을 엽니다.
- Stun을 사용하여 두 패킷 캡처를 모두 필터링합니다.
  - 그런 다음 외부 클라이언트에서 Expressway-E 공용 IP 주소에 대한 바인딩 요청을 찾고 마우스 오른쪽 버튼을 클릭한 다음 Follow(팔로우) > UDP Stream(UDP 스트림)을 선택합니다.
  - 일반적으로 클라이언트의 바인딩 요청의 대상 포트는 Expressway-E의 TURN 릴레이 포트 범위인 24000-29999 범위에 있습니다.
- 클라이언트 측에서 Binding 요청에 대한 응답이 수신되지 않으면 Expressway-E의 캡처에서 요청이 도착하는지 확인합니다.
- 요청이 도착하고 Expressway-E가 클라이언트에 응답하는 경우 외부 FW에서 아웃바운드 UDP 트래픽을 허용하는지 확인합니다.
- 요청이 도착하지 않을 경우 FW를 확인하여 이전에 나열된 포트 범위가 차단되지 않았는지 확인합니다.
- Expressway-E가 고정 NAT 모드가 활성화된 듀얼 네트워크 인터페이스 컨트롤러(DUAL-NIC)와 함께 구축되고 X12.5.2 이전 버전인 경우 외부 FW에서 NAT 반영이 지원 및 구성되는지 확인합니다. X12.5.3부터 독립형 Expressway에서는 이 기능이 더 이상 필요하지 않습니다.

외부 WebRTC 클라이언트가 Cospace에 참가할 수 없으며 경고가 표시됩니다(연결할 수 없음 - 나

중에 다시 시도).

이 시나리오에서는 RTC 클라이언트가 통화 ID를 jalero.space로 확인할 수 있지만 이름을 입력하고 통화참가를 선택하면 연결할 수 없음 - 나중에 다시 시도를 선택하라는 경고가 즉시 표시됩니다.



해결책:

내부 네트워크의 CMS에서 CB 도메인에 대한 \_xmpp-client SRV 레코드를 항상 확인할 수 있는지

확인합니다.

## 관련 정보

- [VCS/Expressway IP 포트 사용 설명서](#)
- [기술 지원 및 문서 - Cisco Systems](#)



이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.