

Configurer les appels audio et vidéo interentreprises (business-to-business) au moyen d'Expressway intégré à CUCM

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Étape 1. Liaison SIP entre CUCM et Expressway-C](#)

[a. Ajouter un nouveau profil de sécurité de la ligne principale SIP](#)

[b. Configurez la ligne principale SIP sur CUCM.](#)

[c. Configurer une zone voisine sur Expressway-C](#)

[d. Vérifier les certificats](#)

[Étape 2. Configurer une zone de traverse entre Expressway-C et Expressway-E](#)

[a. Configuration d'une zone de traverse pour le trafic B2B sur Expressway-C](#)

[b. Configuration d'une zone de traverse pour le trafic B2B sur Expressway-E](#)

[Étape 3. Configurer la zone DNS sur Expressway-E](#)

[Étape 4. Configurer le plan de numérotation](#)

[a. Transforme et/ou recherche de règles sur Expressway-C et E](#)

[b. Schéma\(s\) de routage SIP dans CUCM](#)

[c. Pour le routage d'appels SIP, les enregistrements SRV doivent être créés sur les serveurs DNS publics.](#)

[d. Configurer le nom complet du domaine du groupe \(cluster\) dans CUCM.](#)

[e. Créer une transformation sur Expressway-C qui permet de supprimer le port de l'URI reçu dans l'invitation de CUCM.](#)

[Étape 5. Télécharger des licences multimédia sur Expressway](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment intégrer et configurer le déploiement interentreprises (B2B) des appels audio et vidéo par l'entremise d'Expressway et intégré au Cisco Unified Call Manager (CUCM).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Expressway-C (Exp-C)
- Expressway-E (Exp-E)
- Cisco Unified Call Manager (CUCM)
- Cisco Unity Connection (CUC)
- Téléprésence par Video Communication Server-C (VCS-C)
- Téléphone Jabber
- Cisco Telepresence System (CTS)
- Téléphone EX
- Session Initiation Protocol (SIP)
- Hypertext Transfer Protocol (HTTP)
- eXtensible Messaging and Presence Protocol (XMPP)
- Cisco Unified IM and Presence (IM&P)
- Certificats

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Expressway C et E X8.1.1 ou ultérieur
- Unified Communications Manager (CUCM) 10.0 ou ultérieur.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Les étapes suivantes décrivent de manière détaillée comment intégrer et configurer le déploiement interentreprises (B2B) des appels audio et vidéo par l'entremise d'Expressway intégré au CUCM dans le but de faire et de recevoir des appels d'autres entreprises (domaines).

Expressway avec la fonction d'accès distant mobile (MRA) permet l'enregistrement transparent des terminaux Jabber et TC situés en dehors du réseau de l'entreprise, comme le montre le schéma de réseau.

La même architecture assure également une intégration/des appels fluides entre différentes entreprises (intégration d'entreprise à entreprise, par exemple pour les applications audio, vidéo et IM&P). (B2B)

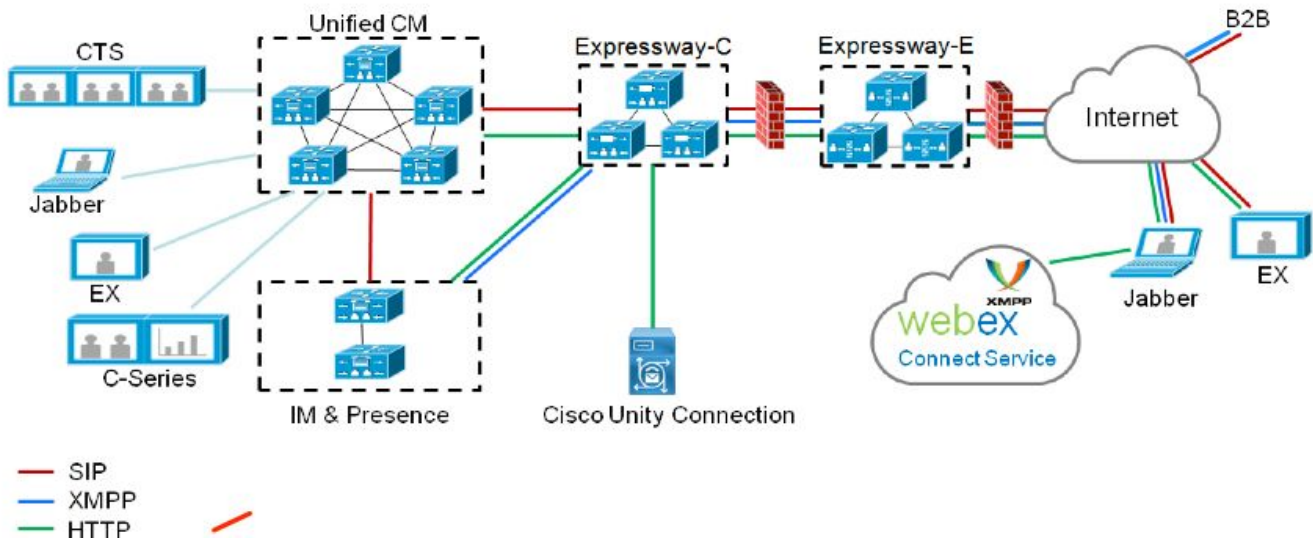
Ce document ne couvre pas la partie IM&P, ni l'intégration H.323.

Avant de continuer, vous devez vous assurer que le service DNS (SRV) approprié a été créé pour votre domaine. Ces enregistrements sont utilisés par d'autres sociétés pour trouver l'emplacement de votre Expressway.

Configuration

Diagramme du réseau

Cette illustration donne un exemple de diagramme de réseau



Étape 1. Liaison SIP entre CUCM et Expressway-C

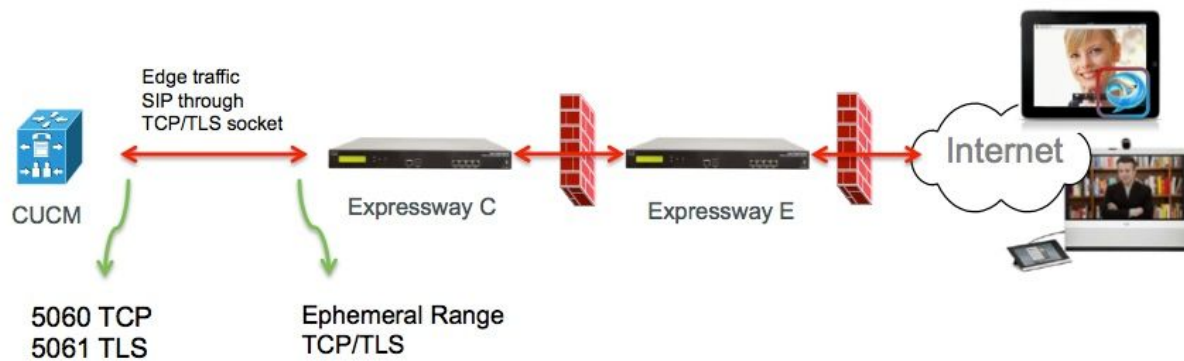
Une fois la détection CUCM effectuée par Expressway-C, les zones voisines sont automatiquement configurées pour chaque noeud et le protocole de transport est découvert.

Lorsque le cluster CUCM est configuré en mode mixte, il existe une zone pour le protocole TCP (Transmission Control Protocol) pour le trafic non sécurisé avec le port de destination 5060 et une zone pour TLS (Transport Layer Security) pour le trafic sécurisé avec le port de destination 5061. Ces ports ne peuvent pas être modifiés.

Les deux zones sont utilisées pour tous les appels de périphérie vers et depuis les points d'extrémité de périphérie.

Les appels entrants provenant des points d'extrémité Edge prennent la route de ces zones ajoutées automatiquement et ciblent conséquemment les ports TCP 5060 ou TLS 5061 du CUCM.

Les points d'extrémités Edge enregistrent et font ou reçoivent des appels par les interfaces de connexion établies.



Pour les appels B2B, configurez une liaison SIP dans CUCM qui pointe vers Expressway-C où CUCM écoute généralement le trafic entrant de cette passerelle sur le port 5060 ou 5061.

Puisque le trafic Edge vient de la même source IP sur les ports 5060/5061, vous devez utiliser un autre port de réception pour cette ligne principale dans CUCM. Sinon, le trafic de périphérie est acheminé vers le périphérique de liaison SIP dans CUCM et non vers le périphérique de point d'extrémité (CSF ou EX).

Du côté de Expressway-C, utilisez les ports 5060 et 5061 pour le SIP (Session Initiation Protocol) TCP/TLS.

Cette illustration décrit un cas où CUCM reçoit le trafic entrant sur les ports 6060/6061 sur cette ligne principale.



Voici les étapes de configuration pour ce déploiement. Convient aux déploiements sécurisés et non sécurisés.

a. Ajouter un nouveau profil de sécurité de la ligne principale SIP

Dans le page d'administration de CUCM, naviguez jusqu'à > Device > Trunk.

Configurez un port entrant différent de 5060/5061, ici utilisez 6060 pour TCP et 6061 pour TLS

Profil de ligne principale SIP non sécurisée

- SIP Trunk Security Profile Information

Name*	B2B SIP TRUNK EXPRESSWAY None Secure
Description	Non Secure SIP Trunk Profile for B2B Expressway
Device Security Mode	Non Secure
Incoming Transport Type*	TCP+UDP
Outgoing Transport Type	TCP
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	
Incoming Port*	6060
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input type="checkbox"/> Accept out-of-dialog refer**	
<input checked="" type="checkbox"/> Accept unsolicited notification	
<input checked="" type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

Profil de la ligne principale SIP sécurisée

Pour TLS, vous devez aussi configurer le Subject name X.509 qui correspond au CN du certificat présenté à Expressway-C. En outre, téléchargez également l'Expressway-C ou le certificat CA (qui a délivré le certificat Expressway-C) dans le magasin de confiance de certificat CUCM.

- SIP Trunk Security Profile Information

Name*	B2B SIP TRUNK EXPRESSWAY SECURE
Description	Secure SIP Trunk Profile for B2B Expressway
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	expresswayc.cisco.com
Incoming Port*	6061
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input type="checkbox"/> Accept out-of-dialog refer**	
<input type="checkbox"/> Accept unsolicited notification	
<input type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

b. Configurez la ligne principale SIP sur CUCM.

Par cette liaison, tous les appels B2B circulent à destination et en provenance de CUCM.

Les paramètres de configuration de ligne principale SIP sont standard pour CUCM avec les déploiements VCS.

Assurez-vous d'associer le profil de sécurité créé à l'étape 1.

c. Configurer une zone voisine sur Expressway-C

Une zone voisine doit être configurée sur Expressway-C pour cibler CUCM.

Cette zone est utilisée pour acheminer le trafic B2B entrant au CUCM.

La configuration est standard, sauf que vous devez vous assurer de configurer le port de destination pour qu'il corresponde au port d'entrée configuré dans le profil de sécurité de la ligne

principale SIP affecté à la ligne principale SIP sur CUCM.

Dans cet exemple, le port de destination utilisé est 6060 pour SIP/TCP et 6061 pour SIP/TLS.
(reportez-vous à l'étape 1), comme indiqué dans l'illustration

À partir de la page Expressway Administration, accédez à **Configuration > Dial Plan > Transforms
y Configuration**

Zone voisine pour TCP SIP :

Configuration

Name ⓘ

Type Neighbor

Hop count ⓘ

H.323

Mode ⓘ

SIP

Mode ⓘ

Port ⓘ

Transport ⓘ

Accept proxied registrations ⓘ

Media encryption mode ⓘ

ICE support ⓘ

Authentication

Authentication policy ⓘ

SIP authentication trust mode ⓘ

Location

Peer 1 address ⓘ SIP: Reachable: 10.48.79.105:6050

Peer 2 address ⓘ

Peer 3 address ⓘ

Peer 4 address ⓘ

Peer 5 address ⓘ

Peer 6 address ⓘ

Advanced

Zone profile ⓘ

Zone voisine pour TLS SIP - avec le mode de vérification TLS activé

Lorsque le mode de vérification TLS est activé, vous devez vous assurer l'**adresse homologue correspond au CN ou au SAN du certificat présenté par CUCM**. En règle générale, avec le mode de vérification TLS, vous configurez le nom de domaine complet (FQDN) du noeud CUCM pour l'adresse homologue.

À partir de la page Expressway Administration, accédez à **Configuration > Dial Plan > Transforms**

y Configuration.

Configuration	
Name	CUCMZONE ⓘ
Type	Neighbor
Hop count	20 ⓘ
H.323	
Mode	Off ⓘ
SIP	
Mode	On ⓘ
Port	6061 ⓘ
Transport	TLS ⓘ
TLS verify mode	On ⓘ
Accept proxied registrations	Deny ⓘ
Media encryption mode	Auto ⓘ
ICE support	Off ⓘ
Authentication	
Authentication policy	Do not check credentials ⓘ
SIP authentication trust mode	Off ⓘ
Location	
Peer 1 address	cucm.cisco.com ⓘ SIP: Reachable: 10.48.79.105:6060
Peer 2 address	ⓘ
Peer 3 address	ⓘ
Peer 4 address	ⓘ
Peer 5 address	ⓘ
Peer 6 address	ⓘ
Advanced	
Zone profile	Cisco Unified Communications Manager (8.6.1 or later) ⓘ

Zone voisine pour TLS SIP, avec le mode de vérification TLS désactivé

Lorsque le mode de vérification TLS est désactivé, l'adresse homologue peut être l'adresse IP, le nom d'hôte ou le nom de domaine complet du noeud CUCM.

À partir de la page Expressway Administration, accédez à **Configuration > Dial Plan > Transforms y Configuration**

Configuration

Name ⓘ

Type Neighbor

Hop count ⓘ

H.323

Mode ⓘ

SIP

Mode ⓘ

Port ⓘ

Transport ⓘ

TLS verify mode ⓘ

Accept proxied registrations ⓘ

Media encryption mode ⓘ

ICE support ⓘ

Authentication

Authentication policy ⓘ

SIP authentication trust mode ⓘ

Location

Peer 1 address ⓘ SIP: Reachable 10.48.79.105:6050

Peer 2 address ⓘ

Peer 3 address ⓘ

Peer 4 address ⓘ

Peer 5 address ⓘ

Peer 6 address ⓘ

Advanced

Zone profile ⓘ

d. Vérifier les certificats

Pour le TLS, assurez-vous que :

- Le certificat du serveur Expressway-C ou la racine du CA (utilisée pour signer le certificat) est téléversé dans le dépôt CUCM sur tous les serveurs du groupe.

- Le certificat CallManager ou la racine du CA (utilisée pour signer le certificat) est téléversé dans liste de certificats du CA du Trusted CA sur le serveur Expressway-C.

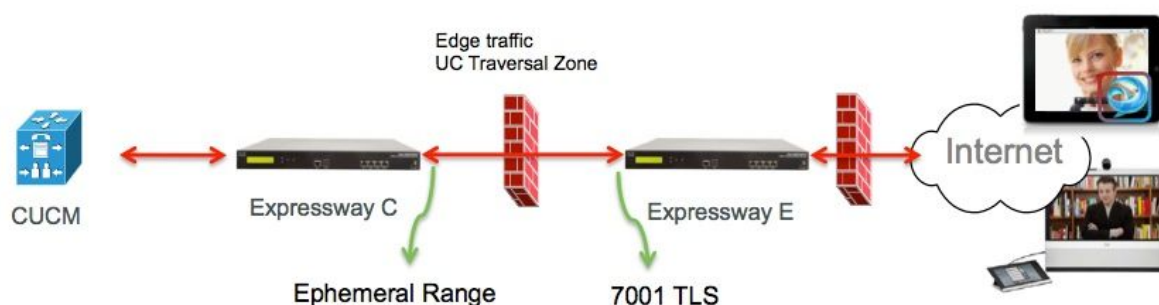
Étape 2. Configurer une zone de traverse entre Expressway-C et Expressway-E

Un horaire que la traversée distincts doit être configuré pour le trafic de route le B2B entre Expressway-C et Expressway E.

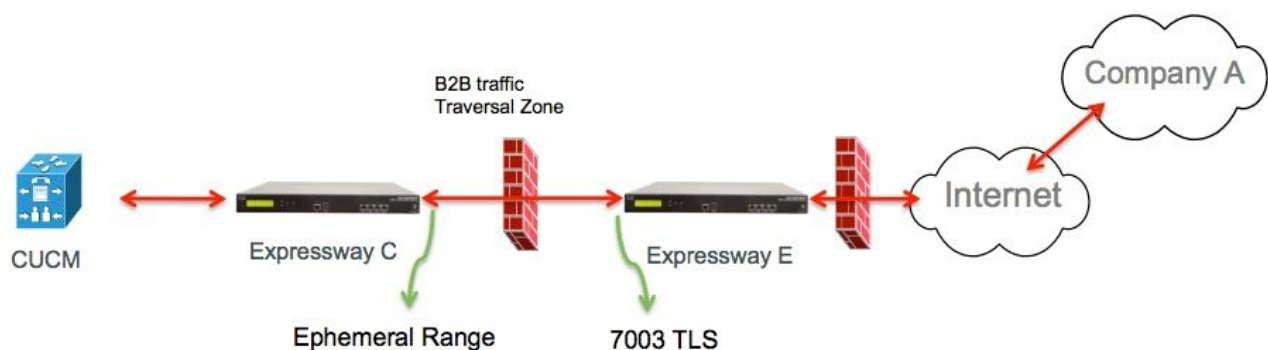
Il s'agit d'une configuration standard de zone de traverse, mais pour la ligne principale SIP du CUCM, un port différent du port utilisé par la zone de traverse UC pour le trafic Edge doit être configuré.

Le port standard pour la zone de traverse UC est 7001. Pour la zone de traversée B2B, vous pouvez par exemple configurer 7003.

La zone de traverse UC pour le trafic Edge est décrite dans l'illustration suivante



La zone de traverse pour le trafic B2B est décrite dans l'illustration suivante



a. Configuration d'une zone de traverse pour le trafic B2B sur Expressway-C

Expressway-C est le client de zone de traversée, dans cet exemple, le port de destination est

Avec le mode de vérification TLS activé, assurez-vous que l'adresse homologue configurée corresponde au CN ou au SAN du certificat présenté par Expressway-E

À partir de la page Expressway Administration, accédez à **Configuration > Dial Plan > Transforms y Configuration**.

Configuration

Name: B2B-Traversal

Type: Traversal client

Hop count: 15

Connection credentials

Username: eft

Password: *****

H.323

Mode: Off

Protocol: Assent

SIP

Mode: On

Port: 7003

Transport: TLS

TLS verify mode: On

Accept proxied registrations: Allow

Media encryption mode: Auto

ICE support: Off

SIP poison mode: Off

Authentication

Authentication policy: Do not check credentials

Client settings

Retry interval: 120

Location

Peer 1 address: eft-xwye.coluc.com

Peer 2 address:

Peer 3 address:

b. Configuration d'une zone de traverse pour le trafic B2B sur Expressway-E

Expressway-E est le serveur de zone de traversée, dans cet exemple, le port d'écoute est 7003.

Avec le mode de vérification TLS activé, assurez-vous que le **TLS verify subject name** configuré correspond au **CN** ou au **SAN** du certificat présenté par Expressway-C

À partir de la page Expressway Administration, accédez à **Configuration > Dial Plan > Transforms y Configuration**.

Configuration

Name * ⓘ

Type Traversal server

Hop count * ⓘ

Connection credentials

Username * ⓘ

Password [Add/Edit local authentication database](#)

H.323

Mode ⓘ

Protocol ⓘ

H.460.19 demultiplexing mode ⓘ

SIP

Mode ⓘ

Port * ⓘ

Transport ⓘ

TLS verify mode ⓘ

TLS verify subject name * ⓘ

Accept proxied registrations ⓘ

Media encryption mode ⓘ

ICE support ⓘ

SIP poison mode ⓘ

Authentication

Authentication policy ⓘ

Étape 3. Configurer la zone DNS sur Expressway-E

Pour router le trafic B2B, configurez une zone DNS sur Expressway-E.

Expressway-E, pour le trafic destiné à cette zone, effectue une recherche DNS SRV pour les protocoles ther _sip ou _sips et ceci pour le domaine dérivé de la partie domaine de l'URI SIP.

La cible SRV retournée par le serveur DNS utilisée pour acheminer l'appel SIP.

La configuration est une configuration standard de zone DNS.

À partir de la page Expressway Administration, accédez à **Configuration > Zones**.

Create zone You are here: [Configuration](#) > [Zones](#) > [Zones](#) > [Create zone](#)

Configuration

Name	<input type="text" value="DNSZone"/>
Type	<input type="text" value="DNS"/>
Hop count	<input type="text" value="15"/>

H.323

Mode	<input type="text" value="On"/>
------	---------------------------------

SIP

Mode	<input type="text" value="On"/>
TLS verify mode	<input type="text" value="Off"/>
Fallback transport protocol	<input type="text" value="TCP"/>
Media encryption mode	<input type="text" value="Auto"/>
ICE support	<input type="text" value="Off"/>

Advanced

Include address record	<input type="text" value="Off"/>
Zone profile	<input type="text" value="Default"/>

Étape 4. Configurer le plan de numérotation

a. Transforme et/ou recherche de règles sur Expressway-C et E

À partir de la page Administration d'Expressway, accédez à **Configuration > Dial Plan > Transforms y Configuration > Dial Plan > Transform or Search Rules**

Pour plus d'informations, consultez les [guides de déploiement VCS](#) (Control with Expressway), le chapitre sur la configuration du routage :

b. Schéma(s) de routage SIP dans CUCM

Pour de plus amples renseignements, veuillez consulter le guide d'administration du système CUCM (Dialplan Deployment)

c. Pour le routage d'appels SIP, les enregistrements SRV doivent être créés sur les serveurs DNS publics.

Comme l'illustre l'image, il répertorie les enregistrements SRV requis, ainsi que les appels H323 B2B qui n'ont pas été traités dans ce document. Notez également que le UDP SIP est désactivé par défaut sur Expressway

DNS SRV records

Name	Service	Protocol	Priority	Weight	Port	Target host
example.com.	h323cs	tcp	10	10	1720	expe.example.com.
example.com.	h323ls	udp	10	10	1719	expe.example.com.
example.com.	sip	tcp	10	10	5060	expe.example.com.
example.com.	sip	udp *	10	10	5060	expe.example.com.
example.com.	sips	tcp	10	10	5061	expe.example.com.

d. Configurer le nom complet du domaine du groupe (cluster) dans CUCM.

Vous pouvez saisir plusieurs entrées séparées par une virgule.



Clusterwide Domain Configuration

Organization Top Level Domain

Cluster Fully Qualified Domain Name

e. Créer une transformation sur Expressway-C qui permet de supprimer le port de l'URI reçu dans l'invitation de CUCM.

Pour plus d'informations, recherchez ce document [Appels de CUCM vers la zone DNS sur VCS Expressway envoyés à une adresse IP incorrecte](#)

À partir de la page d'administration d'Expressway, naviguez jusqu'à Configuration > Dial Plan > Transforms y Configuration > Dial Plan > Transform

Configuration

Priority: 5

Description: Remove port from URI for outbound calls to vngtp.lab

Pattern type: Regex

Pattern string: (.*)@vngtp.lab(:.*)?

Pattern behavior: Replace

Replace string: 11@vngtp.lab

State: Enabled

Le SRND contient également un chapitre complet au sujet de Dialplan

Étape 5. Télécharger des licences multimédia sur Expressway

Les licences multimédias (alias Traversal Zone licences) doivent être téléversées sur chaque serveur Expressway.

En cas d'absence ou de configuration incorrecte, les appels sont libérés avec ce message d'erreur : « Limite de licence d'appel atteinte : You have reached your license limit of concurrent traversal call licenses »

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Pour plus d'informations sur le dépannage B2B, reportez-vous à ce document [Dépannage des problèmes les plus courants pour les appels entre entreprises via Expressway](#)

Informations connexes

- [Serveur de communication vidéo \(VCS\) Cisco TelePresence](#)
- [Support et documentation techniques - Cisco Systems](#)