Dépannage de CUBE via Collaboration Solutions Analyzer

Table des matières

Introduction

Ce document décrit les outils Log Analyser et SIP Profile Tester pour dépanner CUBE à l'aide du portail Collaboration Solutions Analyzer.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Border Element (CUBE) Enterprise.
- Protocole SIP (Session Initiation Protocol).
- Collection de journaux CUBE (débogage).

Pour commencer

Collaboration Solutions Analyzer (CSA) est une suite d'outils conçue pour prendre en charge votre solution de collaboration tout au long de son cycle de vie. Elle permet d'identifier les problèmes et fournit des plans d'action correctifs en cas de besoin, facilitant ainsi chaque phase de la solution de collaboration.

Accédez à Collaboration Solution Analyzer à l'adresse https://cway.cisco.com/csa-new/#/home

Remarque : L'utilisation du navigateur Chrome garantit le fonctionnement optimal de l'outil.

Considérations

Les outils sont conçus pour un périphérique CUBE qui gère les appels SIP à SIP. Tout autre protocole vocal n'est pas pris en charge par les outils.

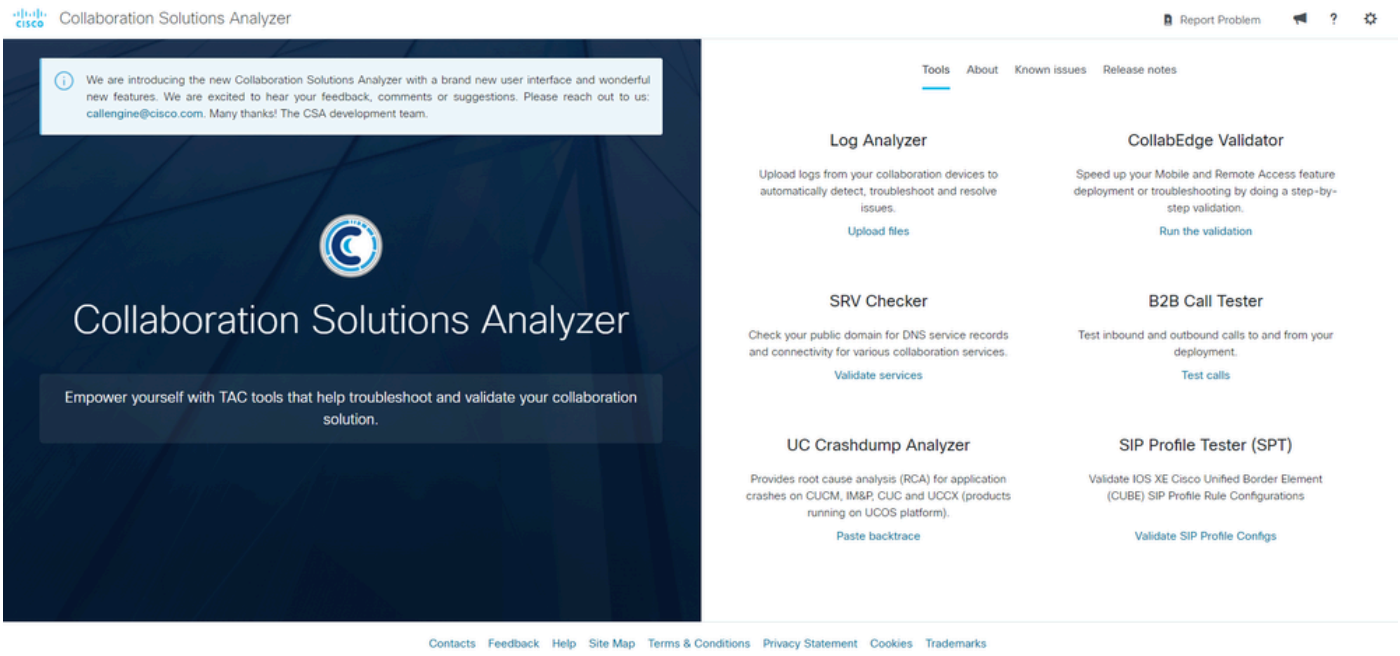
Log Analyzer utilise les journaux CUBE (basés sur le débogage des messages SIP) pour l'analyse.

Si vous avez besoin d'aide avec un autre protocole vocal, utilisez Cisco Support Assistant pour les engagements du TAC à l'adresse https://supportassistant.cisco.com

Description de plateforme

La plate-forme CSA fournit les outils CUBE suivants :

- Log Analyzer : télécharge les journaux depuis CUBE et d'autres périphériques de collaboration pour détecter, dépanner et résoudre automatiquement les problèmes.
- Testeur de profil SIP - Validez la configuration du profil SIP.



Accueil CSA

Analyseur De Journaux

L'outil Log Analyser permet aux administrateurs d'examiner la signalisation d'appel traitée par le périphérique CUBE. Il offre une analyse complète des fichiers journaux, notamment :

- Informations sur le segment
- Diagramme En Échelle

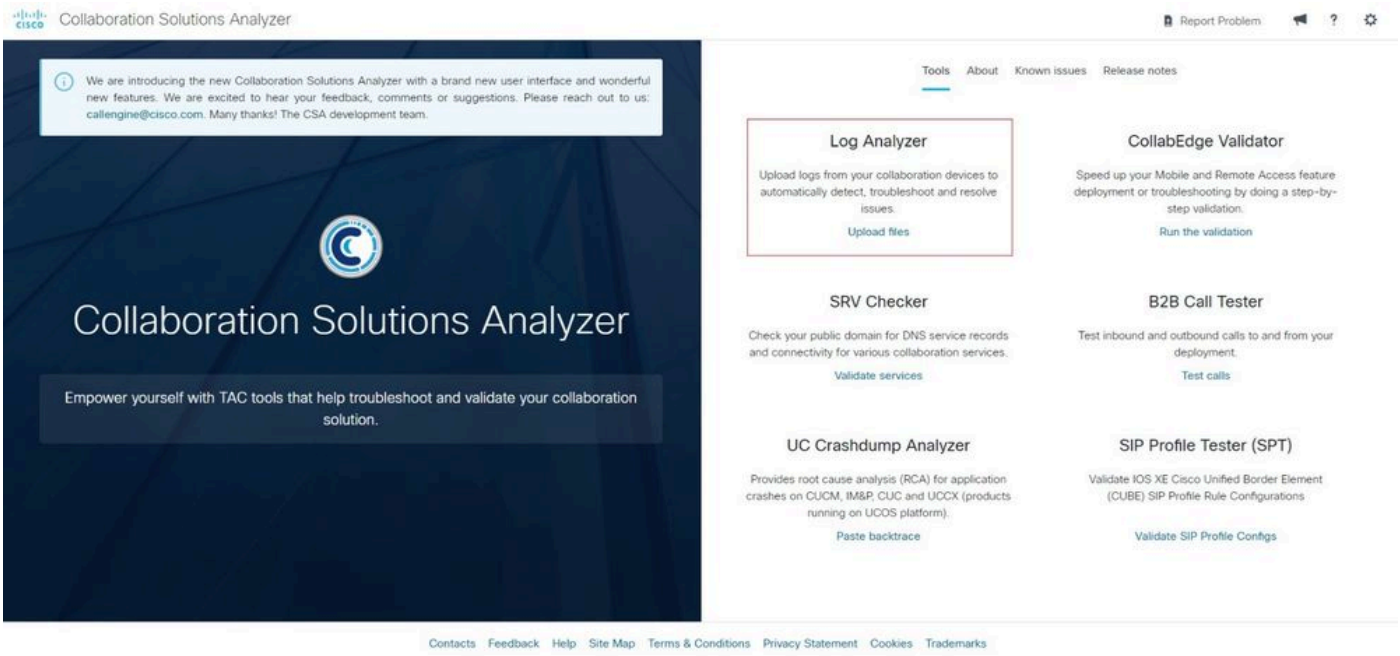
- Signalisation

Remarque : le débogage CUBE (messages debug ccsip) d'un appel qui a été traité par le CUBE doit d'abord être collecté et stocké dans un fichier texte. Seul le débogage SIP et aucune autre sortie, telle que les commandes show, doivent être inclus dans ce fichier texte.

Télécharger les fichiers journaux CUBE

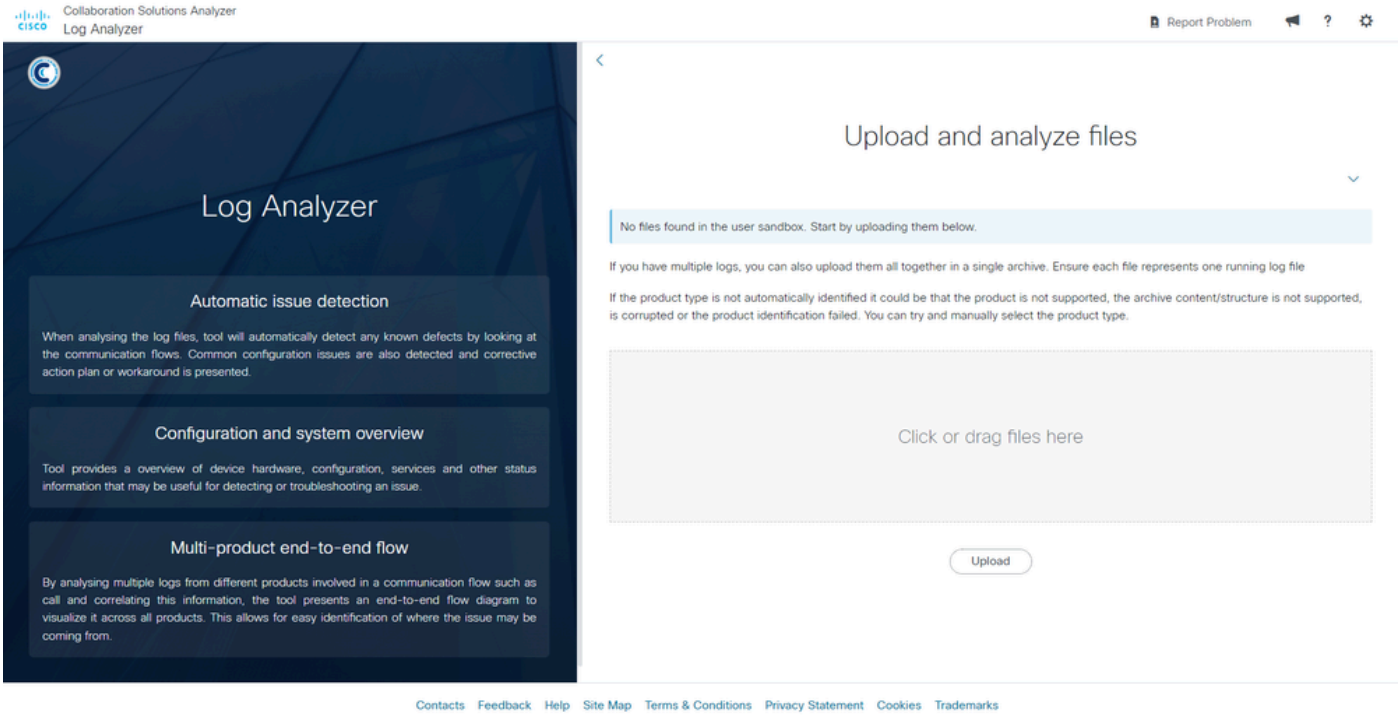
Accédez à Collaboration Solution Analyzer à l'adresse https://cway.cisco.com/csa-new/#/home

Sélectionnez ensuite l'outil en cliquant sur Upload files dans la section Log Analyser.



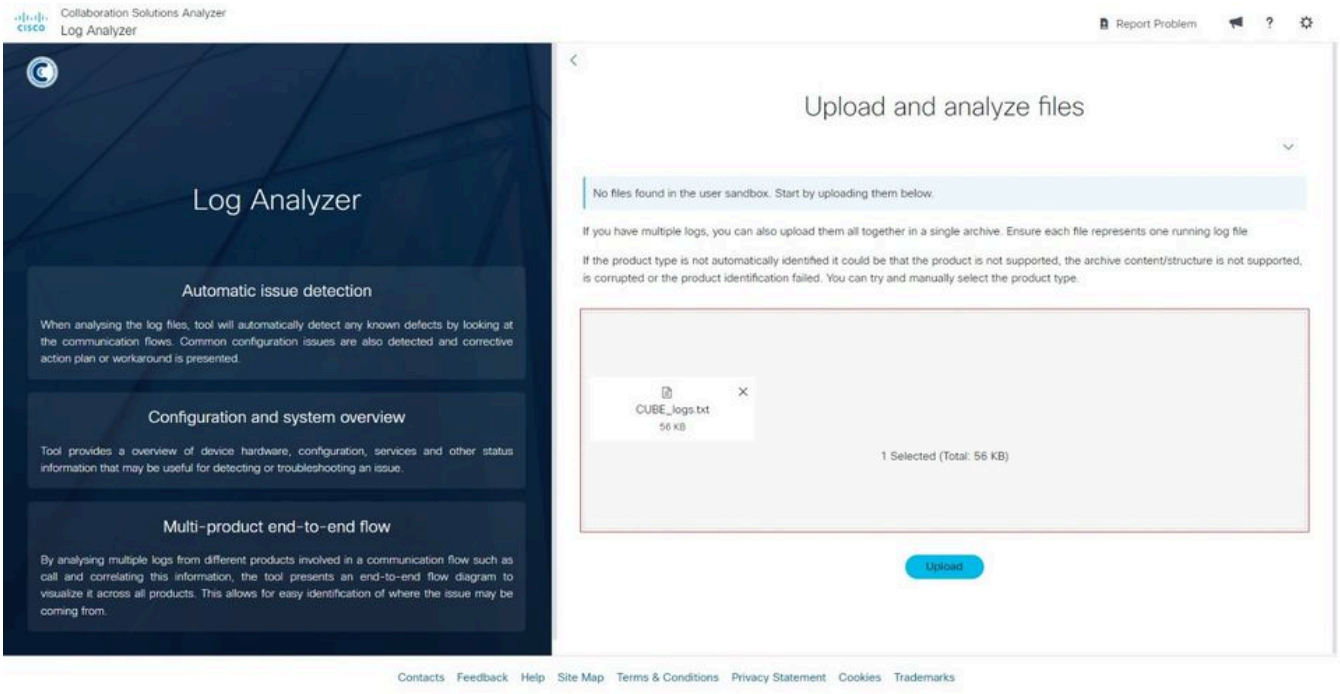
Accueil de Log Analyser

La plate-forme affiche l'écran de l'outil dans lequel un fichier peut être sélectionné ou déplacé.



Chargement de Log Analyser

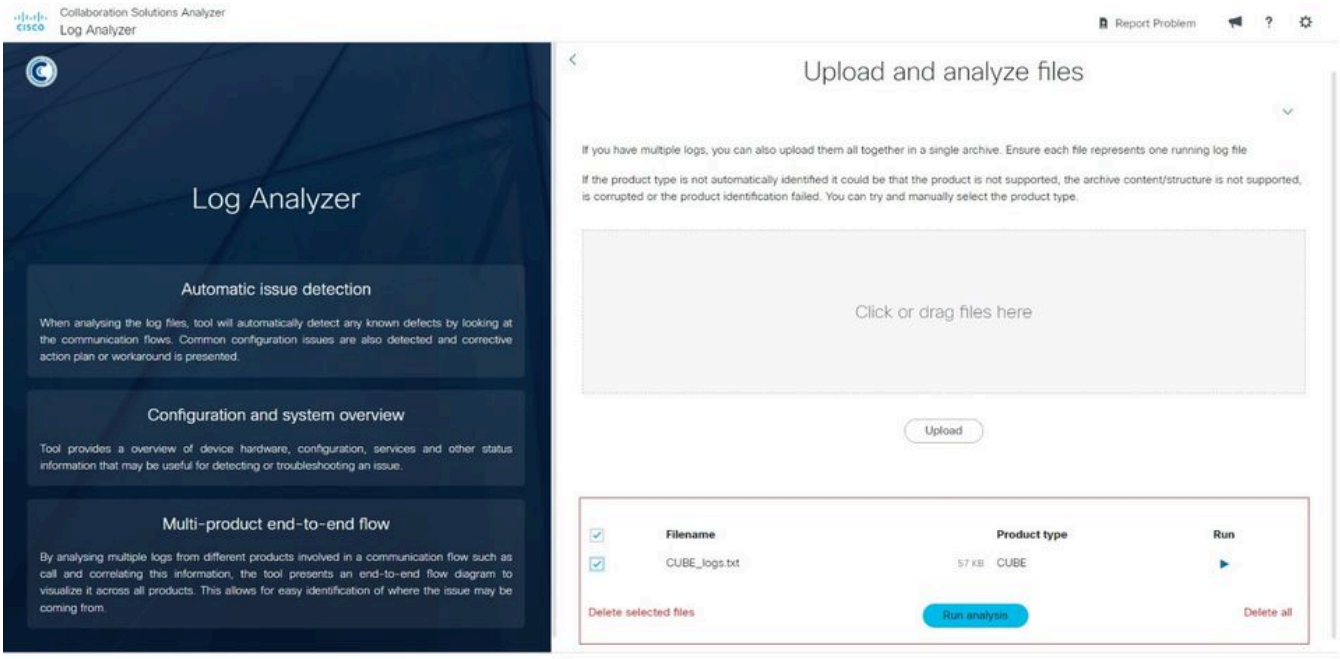
Pour terminer le processus de téléchargement du fichier pour l'outil à analyser, cliquez sur le bouton Upload.



Fichier de téléchargement Log Analyser

Après avoir téléchargé le fichier dans l'outil, sélectionnez le(s) fichier(s) que vous souhaitez analyser en cochant la case correspondante, puis cliquez sur le bouton Exécuter l'analyse.

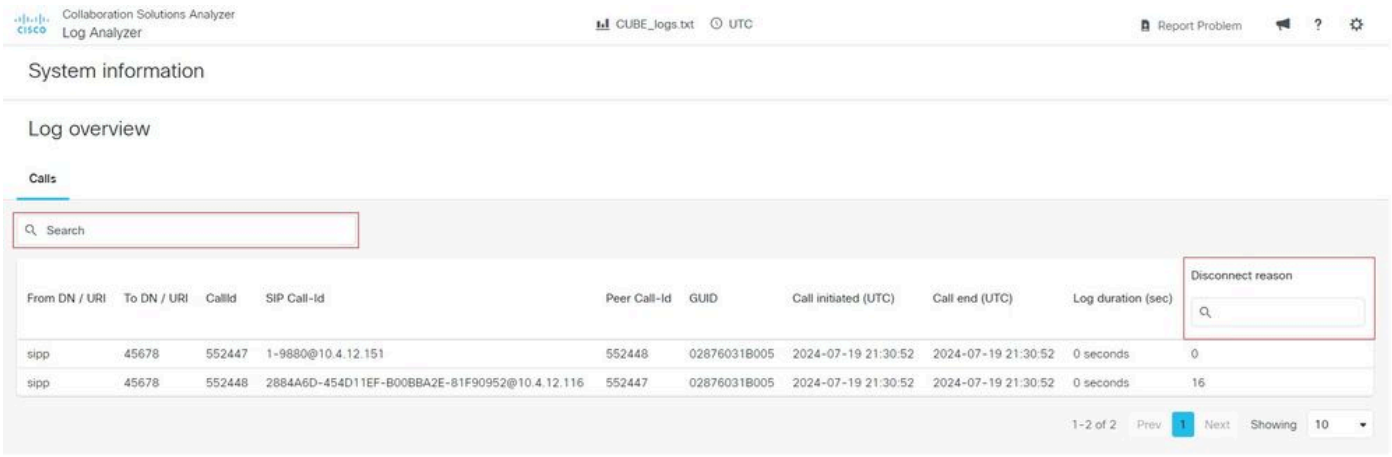
- Le système définit le type de produit sur CUBE.
- Plusieurs fichiers peuvent être analysés dans la même session.



Type de produit Log Analyser

L'outil analyse tous les appels de signalisation capturés dans le fichier texte et affiche un résumé des tronçons d'appel identifiés. Vous pouvez ensuite appliquer deux filtres :

- Rechercher : filtre les sessions d'appel en fonction de données spécifiques, telles que les numéros composés.
- Rechercher par motif de déconnexion : filtre les sessions d'appel en fonction du motif de déconnexion.

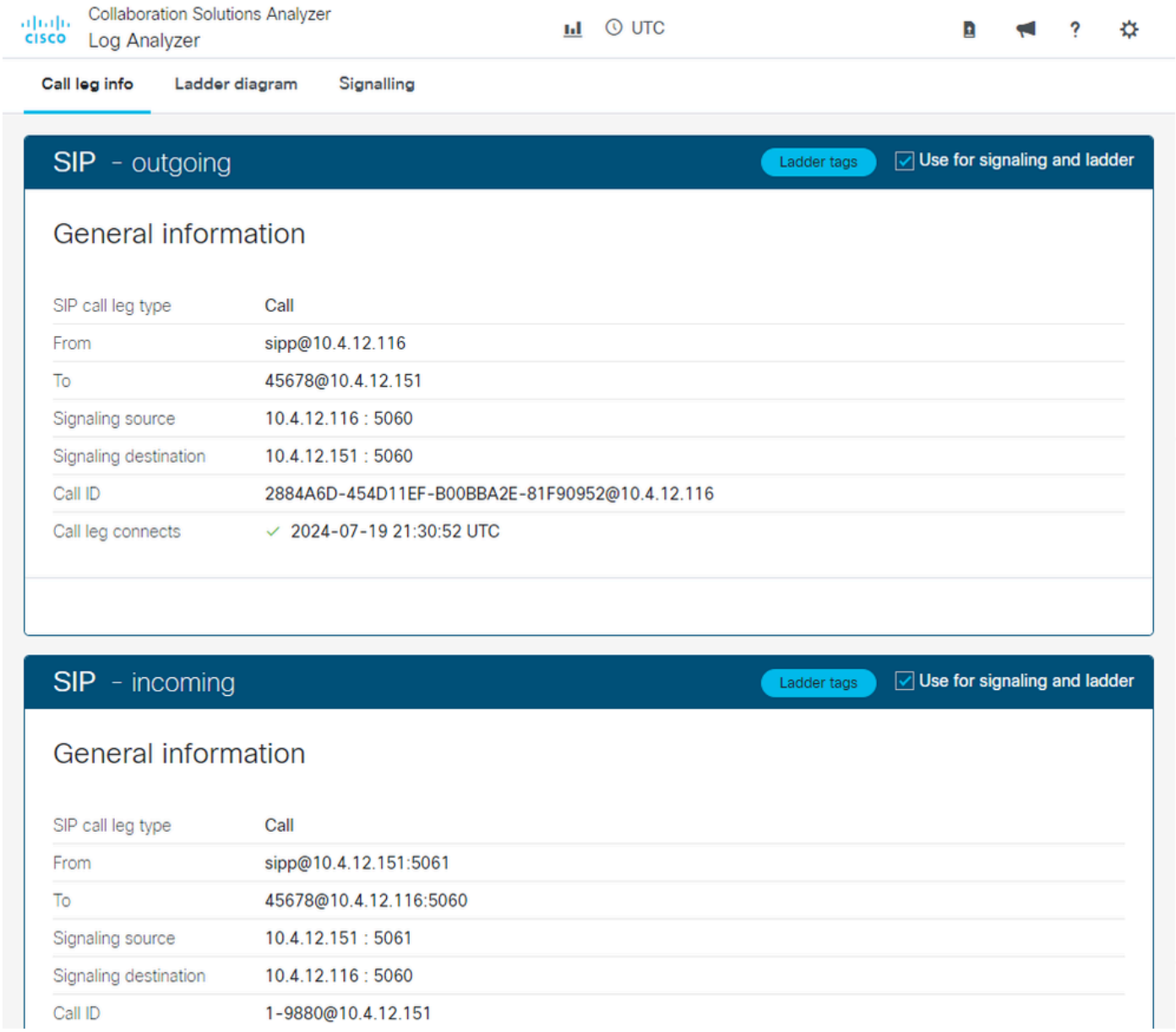


Pour poursuivre l'analyse détaillée, sélectionnez la ligne de session d'appel sur laquelle vous souhaitez vous concentrer et l'outil affiche l'analyse complète avec les informations sur le segment d'appel, le schéma en échelle et la signalisation.

Informations sur le segment d'appel

La première étape présente les informations de segment d'appel, qui affichent la vue d'ensemble de l'appel :

- Type de branche d'appel SIP
- From - Provient de l'en-tête FROM SIP du message INVITE.
- To : obtenu à partir de l'en-tête TO SIP du message INVITE.
- Source de signalisation : adresse IP et port du périphérique source. Provient de l'en-tête VIA SIP du message INVITE.
- Signaling Destination : adresse IP et port du périphérique de destination. Provient de l'en-tête SIP URI du message INVITE.
- ID d'appel : obtenu à partir de l'en-tête SIP CALL-ID du message INVITE.
- Connexion du tronçon d'appel - Horodatage de session d'appel.

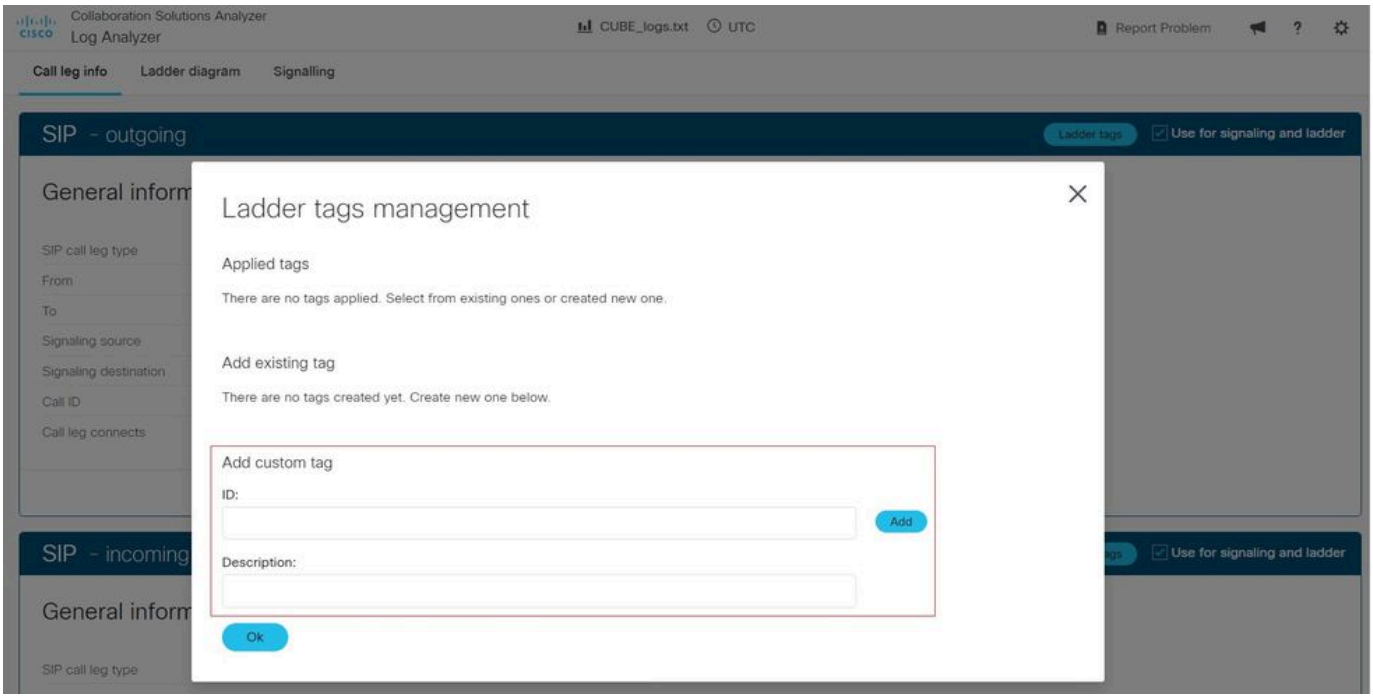


Informations de segment d'appel Log Analyser

Dans cette section, les balises d'échelle peuvent être activées pour mettre en surbrillance les messages dans le schéma d'échelle. L'application comporte 2 champs :

- ID - Saisissez le paramètre spécifique que vous souhaitez mettre en surbrillance.
- Description - Ajoute une description du paramètre.

Cliquez sur le bouton Add pour terminer le processus.



Étiquettes d'échelle Log Analyser

Diagramme En Échelle

Dans la deuxième étape, un schéma en échelle est présenté, représentant visuellement les messages SIP échangés pendant l'appel. Les messages sont codés en couleur pour une identification facile :

- Couleur bleue - messages SIP INVITE.
- Couleur verte : messages SIP 200 OK et ACK.
- Couleur rouge : messages SIP BYE.

Pour télécharger une copie du schéma, cliquez sur le bouton Download Ladder. Le diagramme est téléchargé et enregistré en tant que fichier image PNG. Veuillez noter que cette option n'est disponible que si vous utilisez le navigateur Google Chrome.

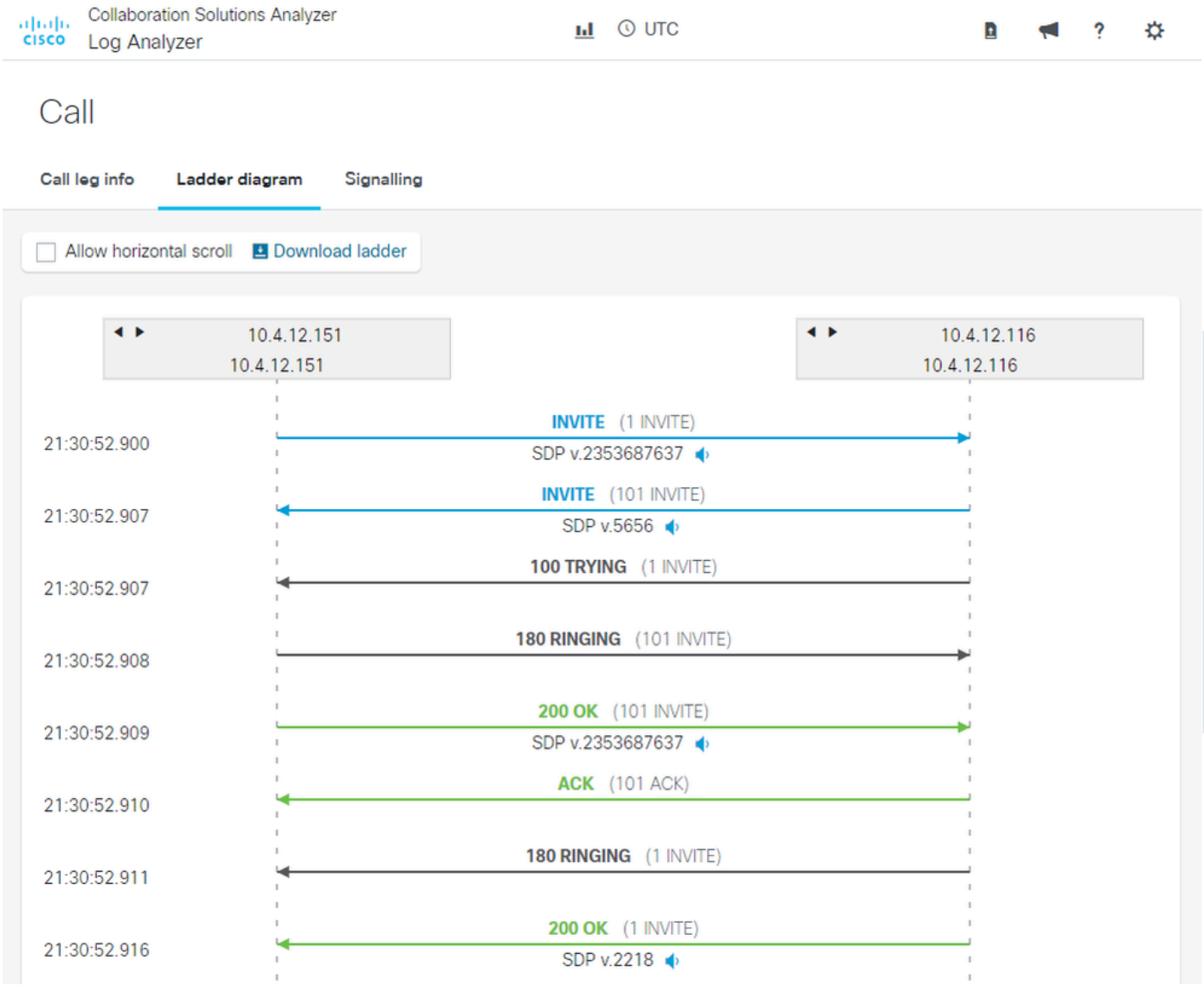
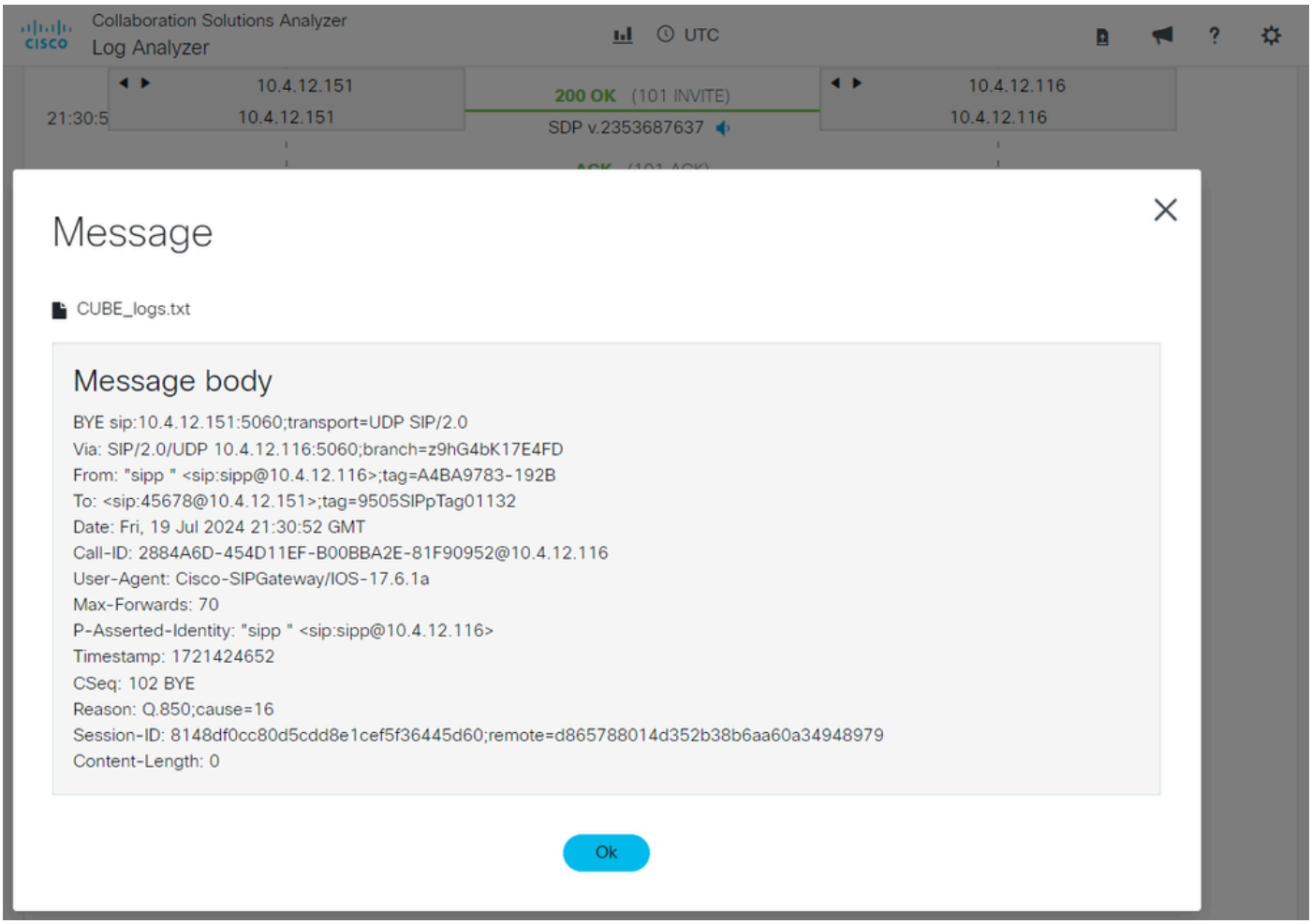


Diagramme De L'Échelle Log Analyser

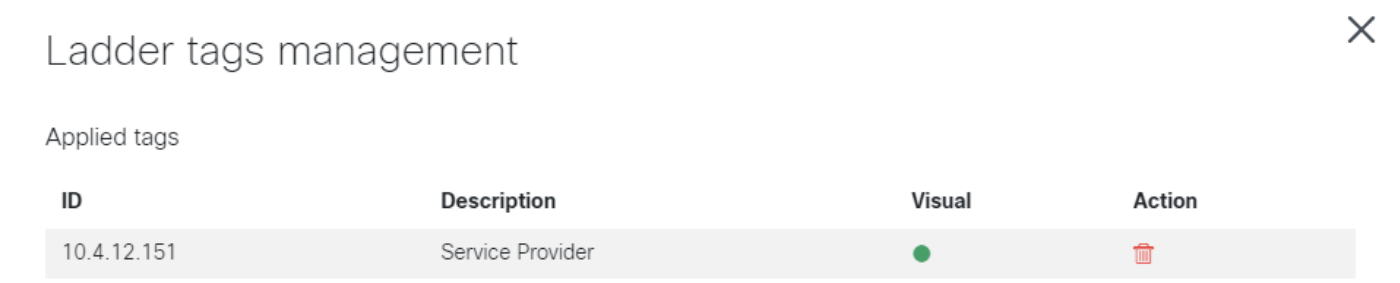
Cet outil permet à l'administrateur d'ouvrir des messages SIP et d'afficher leur contenu. Cliquez sur un message pour l'ouvrir.



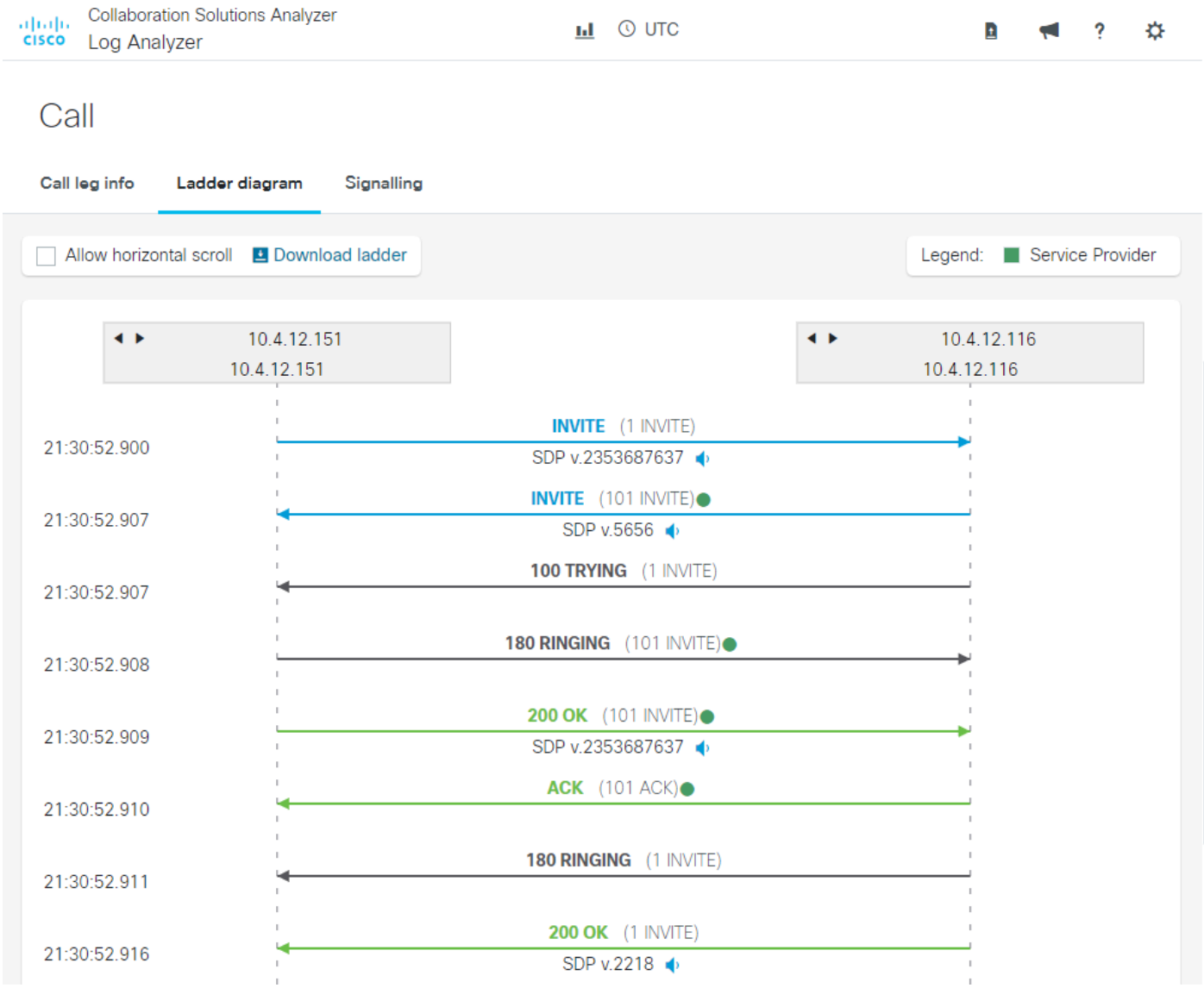
Message Diagramme d'échelle Log Analyser

L'administrateur peut ajouter des balises d'échelle pour visualiser les messages SIP avec un point distinctif dans la section Informations sur le segment d'appel. Tout paramètre inclus dans le message SIP peut être utilisé pour la balise.

Dans cet exemple, une adresse IP est utilisée pour le paramètre ID et une description est ajoutée. Les messages SIP contenant l'adresse IP sont mis en surbrillance avec un point pour les distinguer des autres messages.

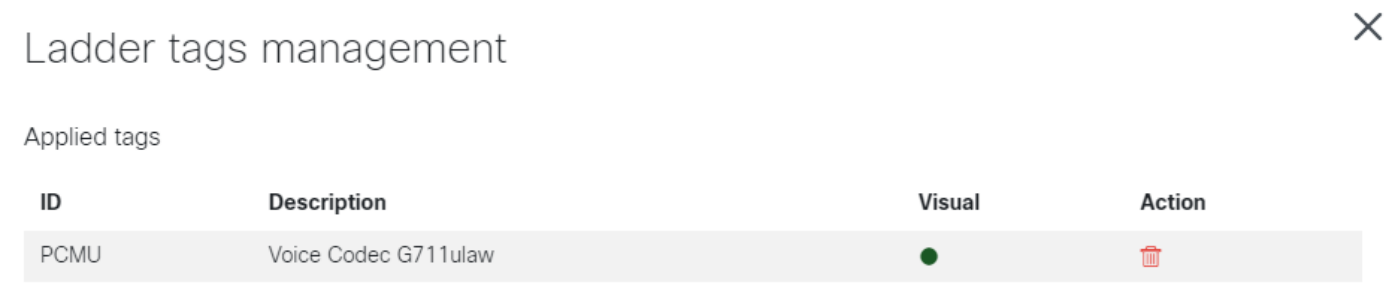


Étiquettes d'échelle Log Analyser 1

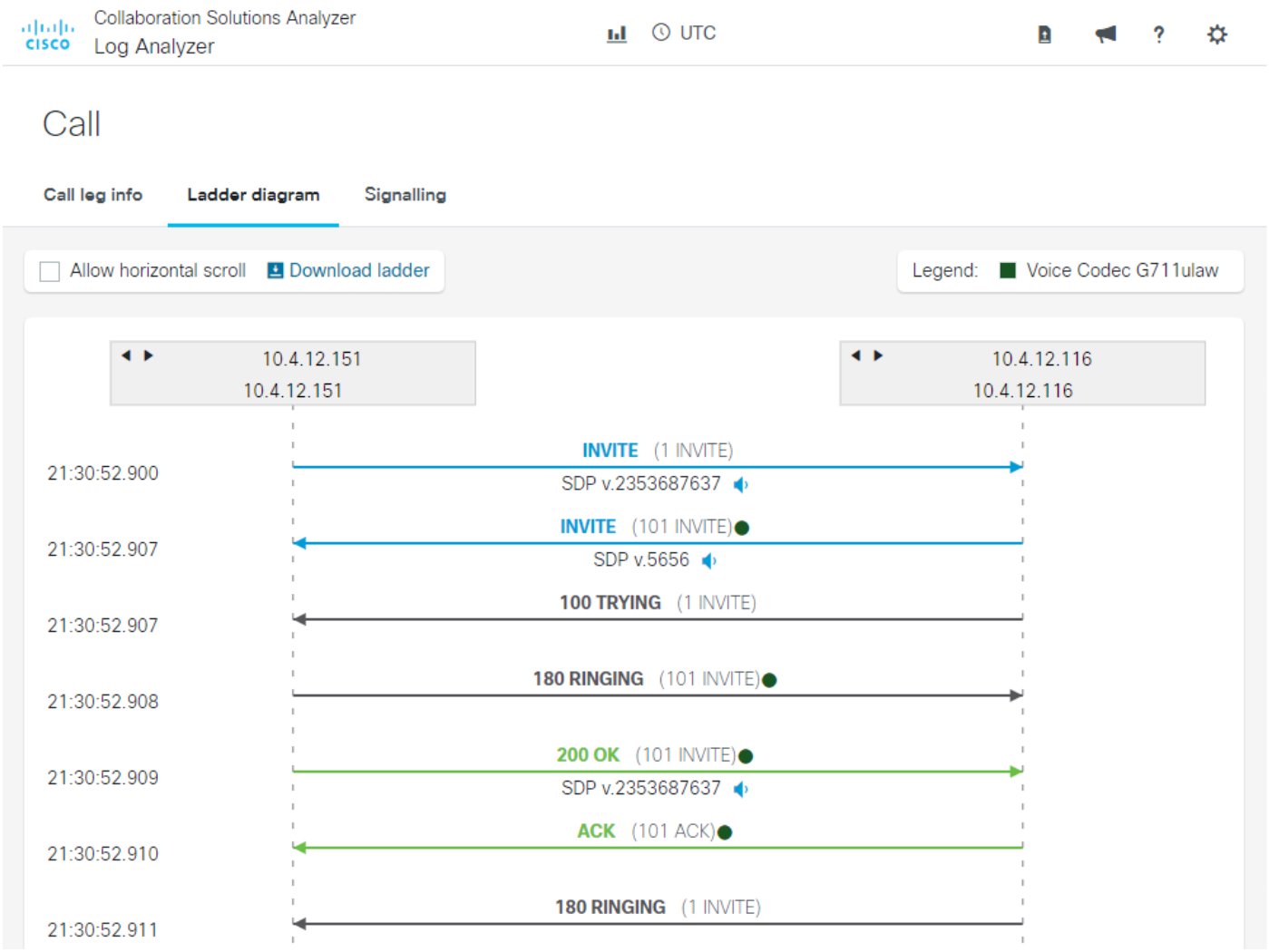


Étiquettes d'échelle Log Analyser 2

Un autre filtre qui peut être utilisé pour distinguer les messages SIP des autres messages est un codec vocal.



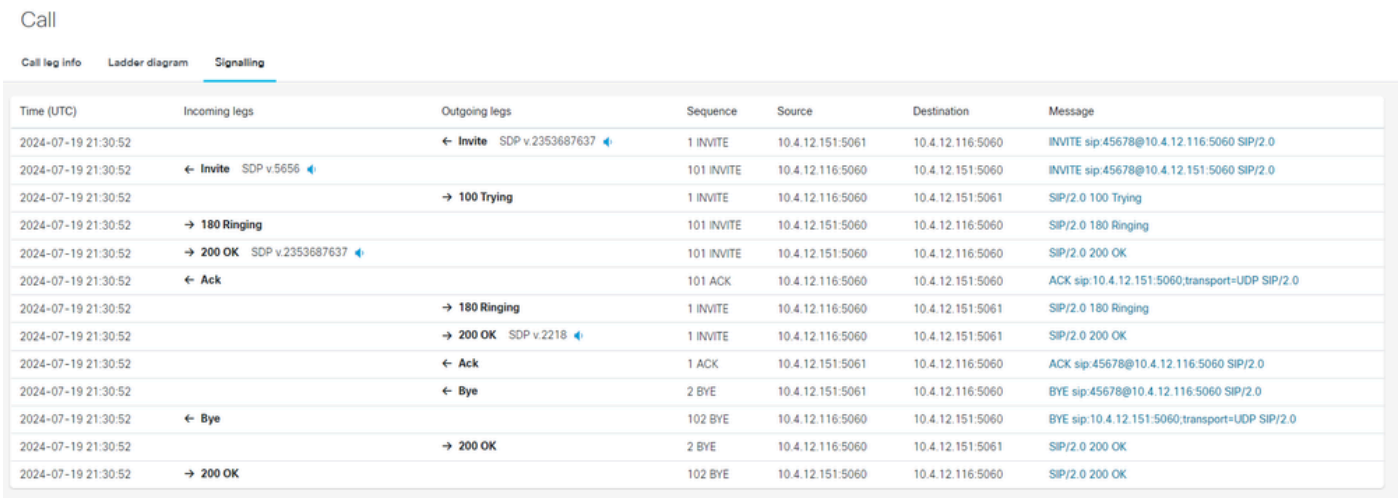
Étiquettes d'échelle Log Analyser 3



Étiquettes d'échelle Log Analyser 4

Signalisation

La dernière étape est la signalisation, qui affiche les messages SIP pour les deux branches CUBE (entrantes et sortantes). Il contient les adresses IP source et de destination. Cliquez pour afficher le message.



Signalisation Log Analyser

Message de signalisation Log Analyser

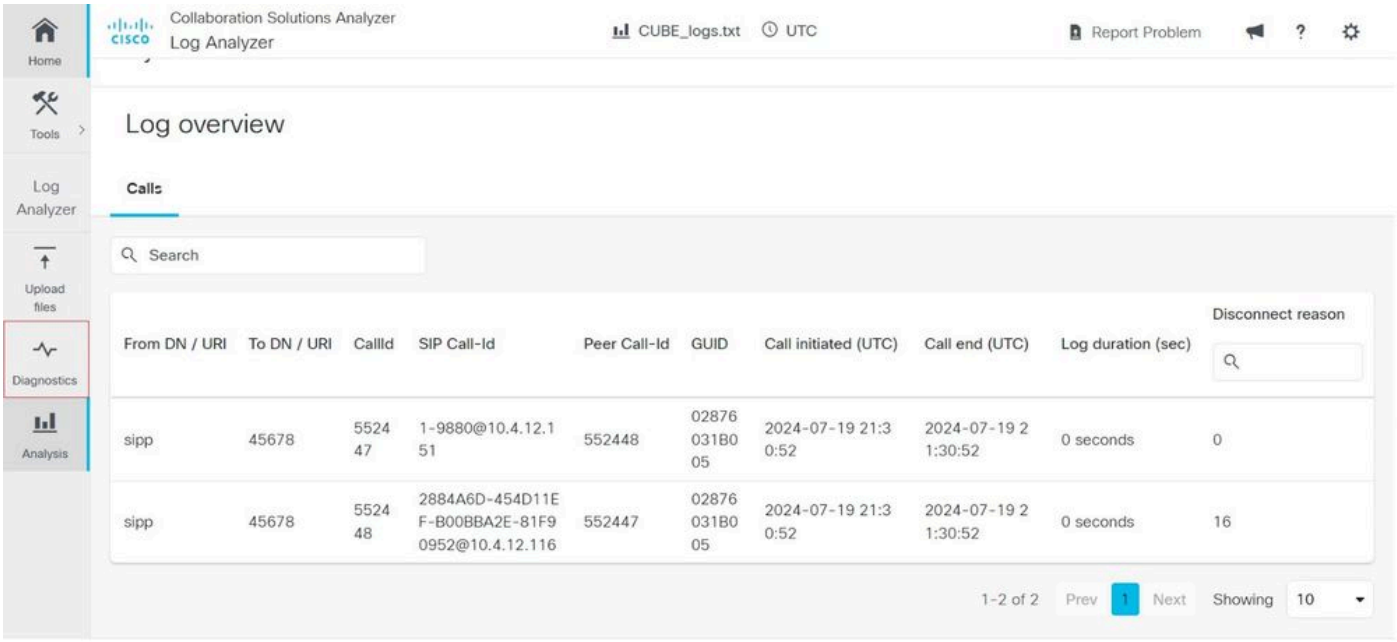
Diagnostics

Toutes les données analysées à partir des journaux sont exécutées sur des signatures de diagnostic qui identifient les défauts connus, les problèmes courants ou les erreurs de configuration et fournissent un plan d'action corrective.

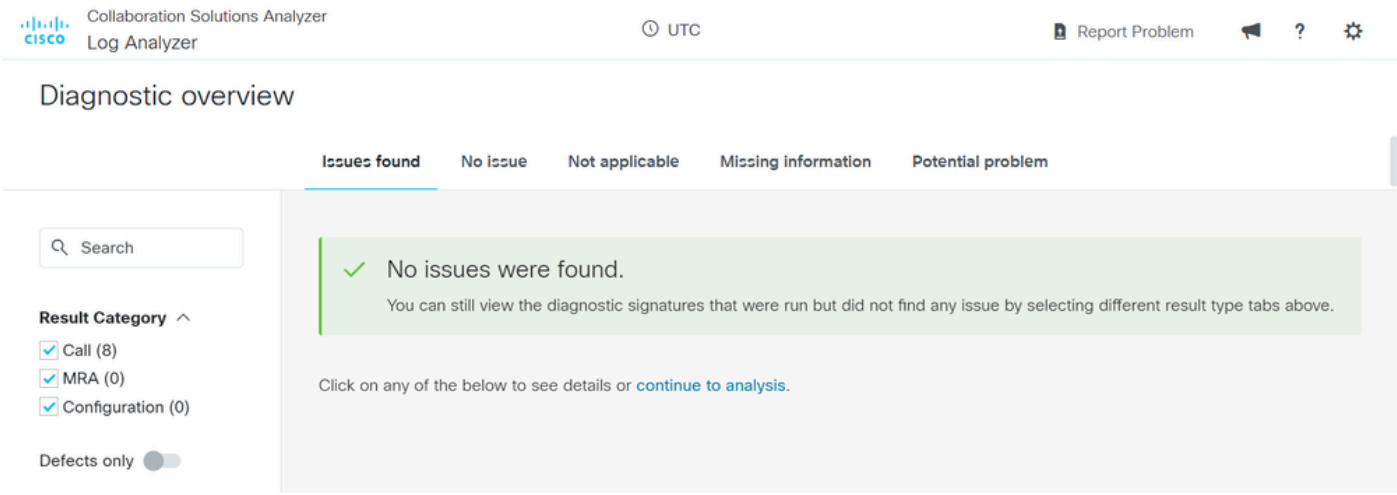
Une fois qu'un appel capturé dans les journaux a été sélectionné pour afficher l'analyse de résumé d'appel, la plate-forme CSA doit afficher la section Diagnostics, qui contient ces informations :

- Problèmes détectés
- Informations manquantes
- Problème potentiel

Un bouton bascule peut être activé pour filtrer et afficher uniquement les défauts.



Accueil de Log Analyser Diagnostics



Présentation des diagnostics Log Analyser

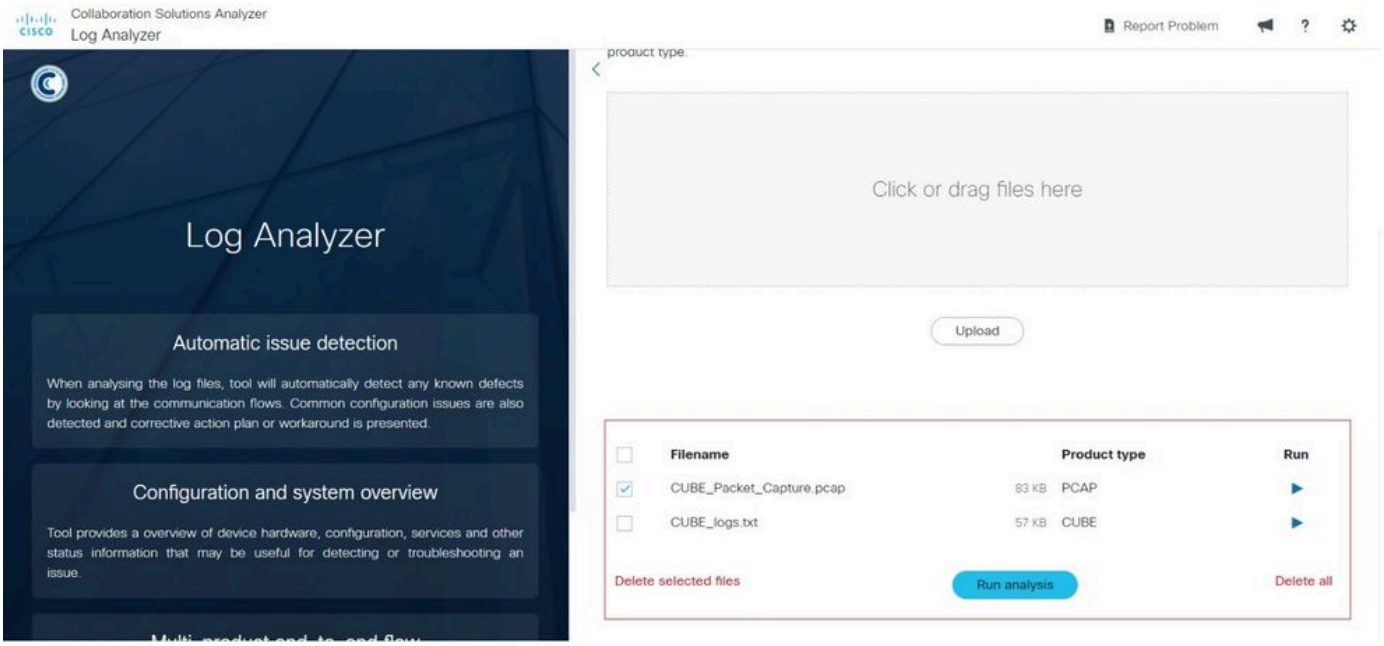
Capture de paquets CUBE

La capture de paquets est un tampon de fichiers créé pour collecter une copie des paquets réels au niveau d'une interface réseau CUBE ou de tout périphérique réseau vocal. Ce fichier peut être ouvert et analysé par un logiciel d'analyse de réseau, tel que Wireshark.

L'outil Log Analyzer a été amélioré avec un analyseur de capture de paquets qui peut traiter les extensions de format de fichier pcap ou pcapng, fournissant un résumé des statistiques de session et de réseau collectées à partir des appels.

Le fichier de capture de paquets doit être téléchargé vers l'outil Log Analyzer de la même manière

que le fichier journal CUBE. Le système détermine le type de produit comme PCAP.



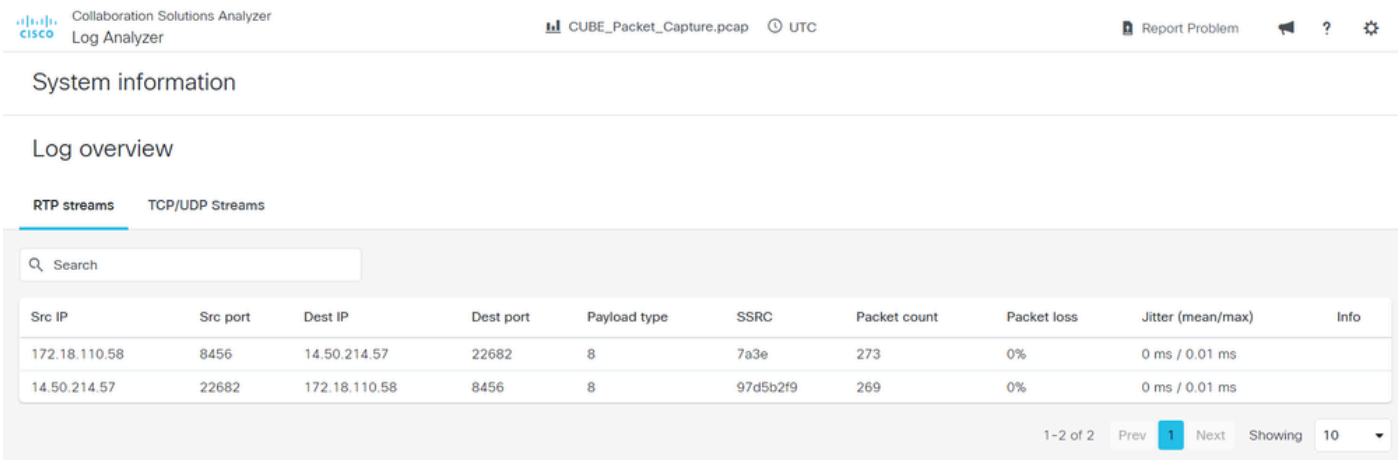
Fichier de capture de paquets Log Analyzer

Une fois que le bouton Exécuter l'analyse est activé, l'outil Analyseur de journal analyse les informations et fournit un résumé des sessions capturées dans deux colonnes :

- Flux RTP
- Flux TCP/UDP

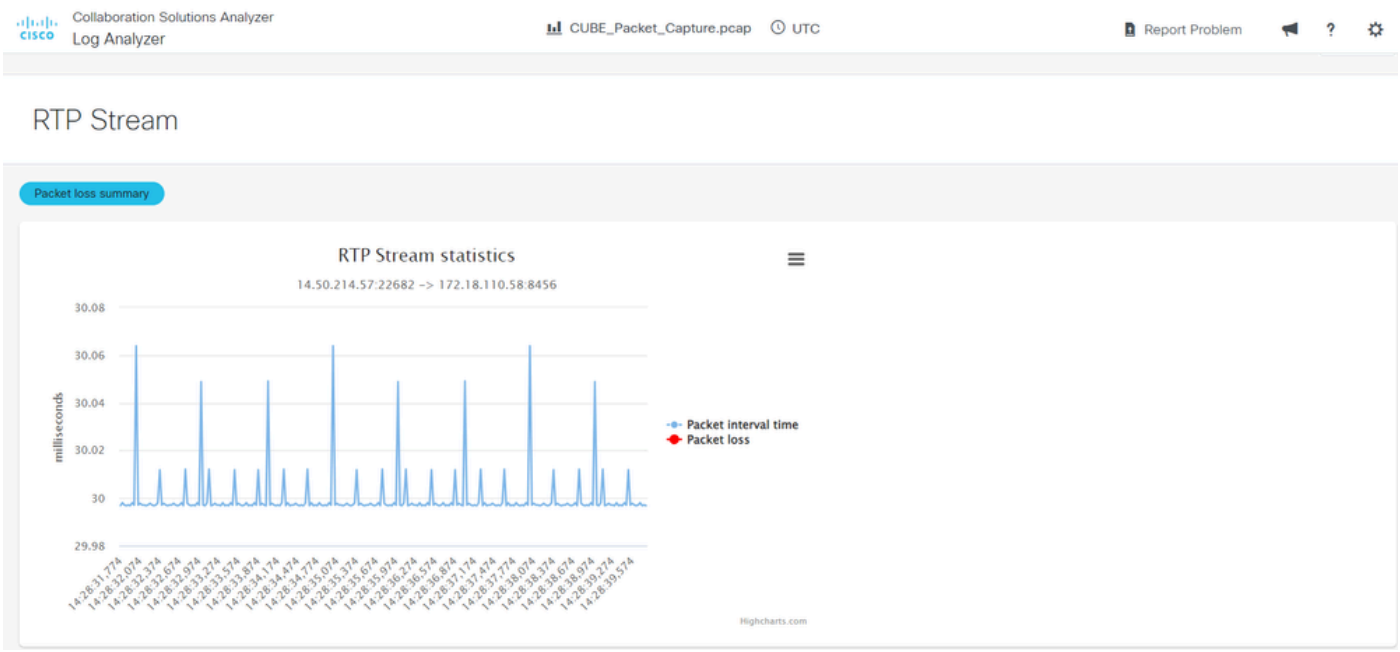
Remarque : si la capture de paquets inclut des flux SRTP, elle est affichée dans la colonne « RTP flows » et une analyse du réseau est effectuée. La partie audio d'un flux SRTP n'est pas décodée.

Sélectionnez une session dans la colonne Flux RTP et l'outil affiche les statistiques du flux RTP pour cette connexion. Si le flux est affecté par les conditions du réseau, le paramètre Packet Loss (Perte de paquets) est marqué par des points rouges.



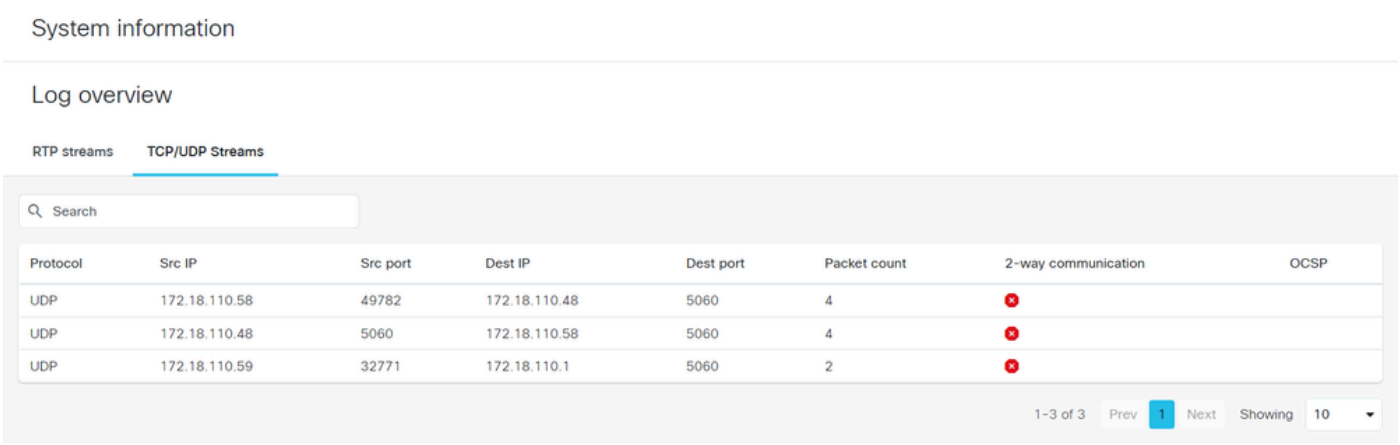
Analyse PCAP Log Analyser

Les statistiques de flux RTP peuvent être téléchargées dans un format de fichier texte qui contient un résumé de la perte de paquets. Cliquez sur le bouton Packet Loss Summary pour télécharger le fichier.



Flux RTP Log Analyzer PCAP

Pour les flux TCP/UDP, le système affiche le résumé des sessions capturées.



Flux TCP UDP PCAP de Log Analyzer

Testeur de profil SIP (SPT)

Les profils SIP (Session Initiation Protocol) sont utilisés pour modifier les messages SIP entrants ou sortants afin de garantir la compatibilité entre les différents périphériques. L'outil « SIP Profile Tester » vous permet de valider votre configuration avant de la déployer dans un environnement actif.

L'outil Profil SIP se compose de 3 sections :

- SIP Profile Rules - Fenêtre permettant d'insérer les règles SIP PROFILE à tester.

- SIP Message to Apply Rules - Fenêtre permettant de coller le message SIP à l'endroit où les règles doivent être appliquées.
- Message SIP à copier à partir de - (Facultatif) Fenêtre permettant de coller un message SIP au cas où une configuration de liste de copie serait testée. Une configuration de liste de copie copie copie le contenu d'un en-tête entrant reçu par un périphérique vers un en-tête sortant.

L'outil contient 2 boutons pour gérer les tests :

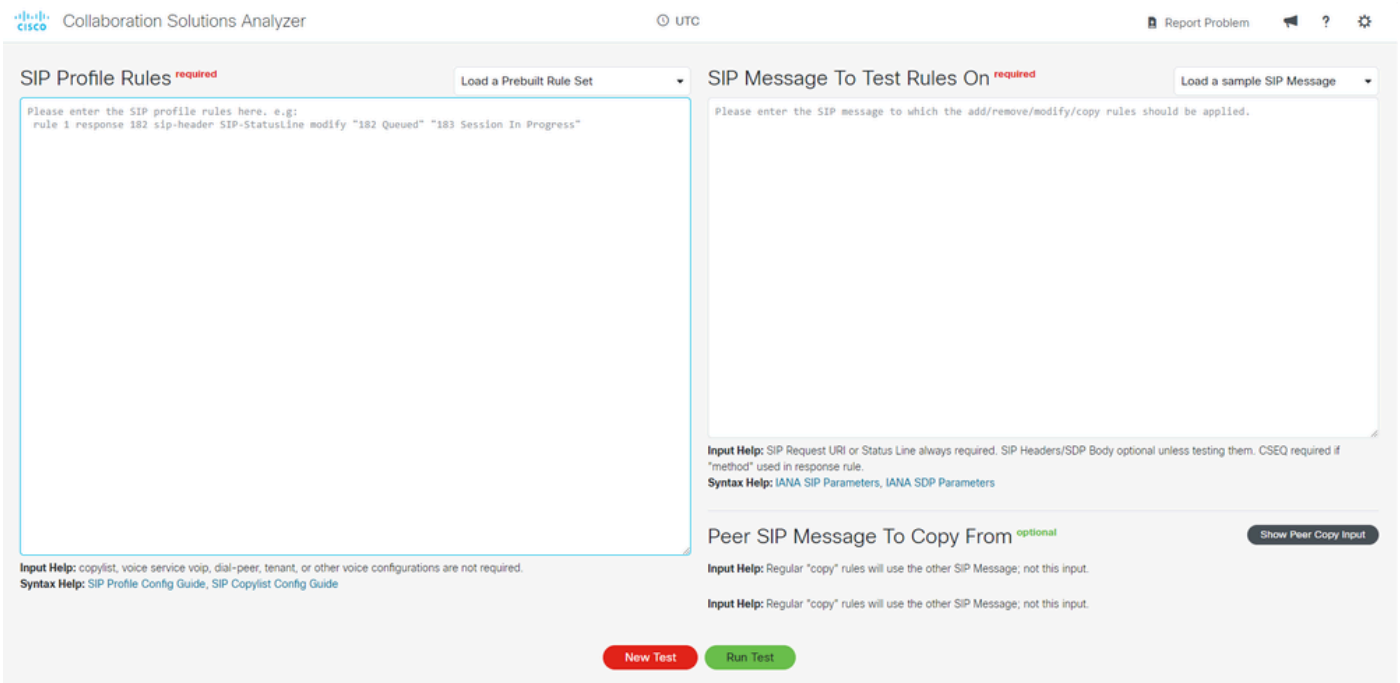
- Bouton vert - Pour exécuter un test.
- Bouton rouge - Pour réinitialiser et effacer les paramètres.

Après avoir sélectionné le bouton vert pour exécuter le test, l'outil affiche ces options :

- Bouton rouge - Nouveau test
- Bouton bleu - Afficher les entrées

Mise en surbrillance des résultats du message SIP original/modifié :

- Couleur bleue - Les en-têtes SIP modifiés ou le corps SDP sont mis en surbrillance bleue dans les deux zones de message.
- Couleur verte - Les en-têtes SIP ou le corps SDP ajoutés sont mis en surbrillance verte dans le résultat du message SIP modifié uniquement.
- Couleur rouge - Les en-têtes SIP ou le corps SDP supprimés sont mis en surbrillance rouge dans le résultat du message SIP d'origine uniquement.



SIP PROFILE - Accueil

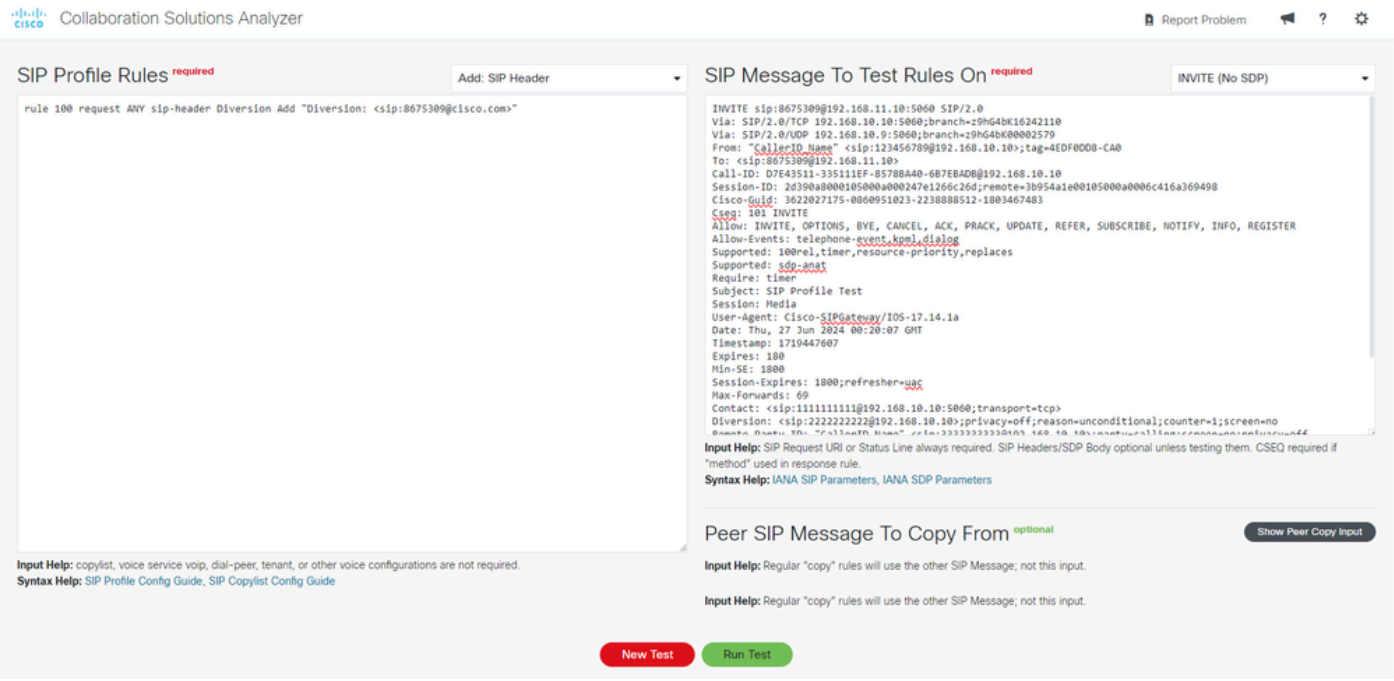
Exemple de profil SIP prédéfini

Cet outil fournit des exemples prédéfinis pour simplifier les tests. En haut de chaque fenêtre, une

boîte d'application permet de sélectionner ces exemples.

Voici comment utiliser une configuration prédéfinie :

1. Cliquez sur Load a Prebuilt Rule Set et sélectionnez Add : SIP Header.
2. Cliquez sur Load a Sample SIP Message et sélectionnez INVITE (No SDP).
3. Cliquez sur le bouton vert Run Test pour exécuter le test.

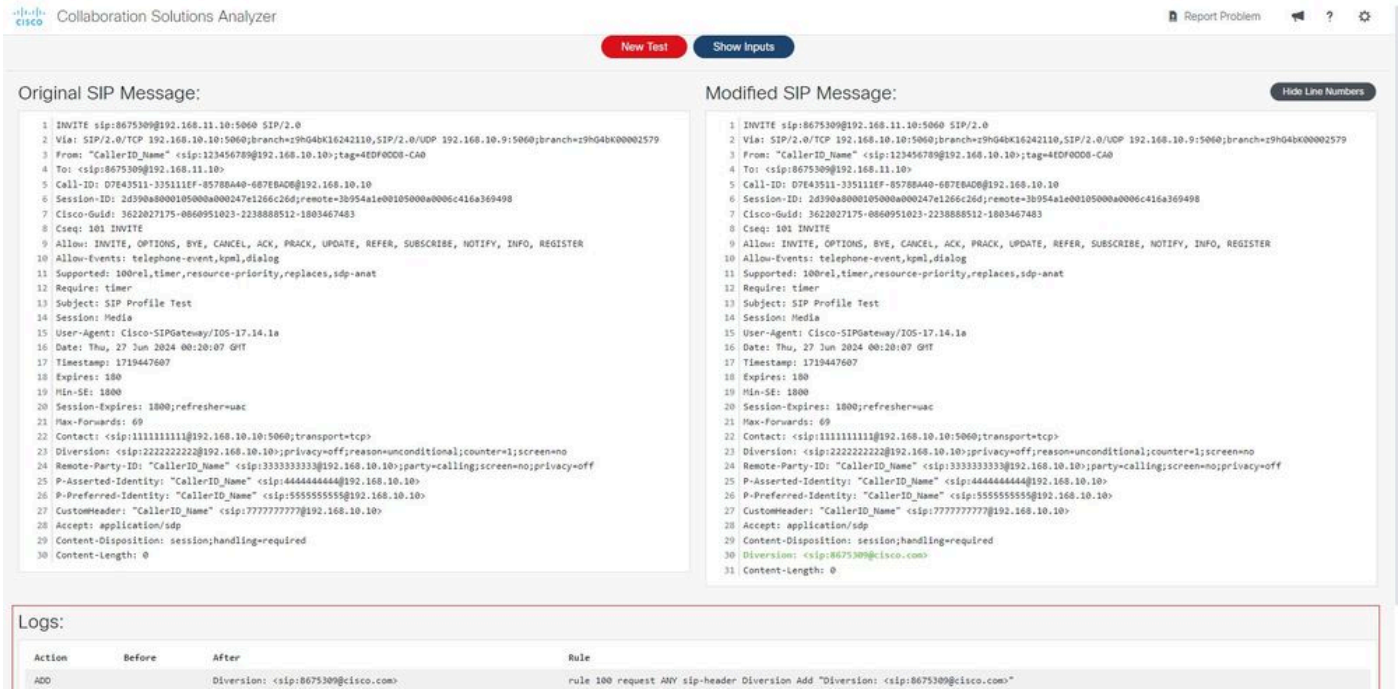


PROFIL SIP préconfiguré

L'outil affiche un nouvel écran avec les résultats du test :

Message SIP modifié

```
ADDED (GREEN) - Diversion: <sip:8675309@cisco.com
```



Exemple d'ajout préconfiguré de PROFIL SIP

Voici un exemple de mise en surbrillance de modification/ajout/suppression :

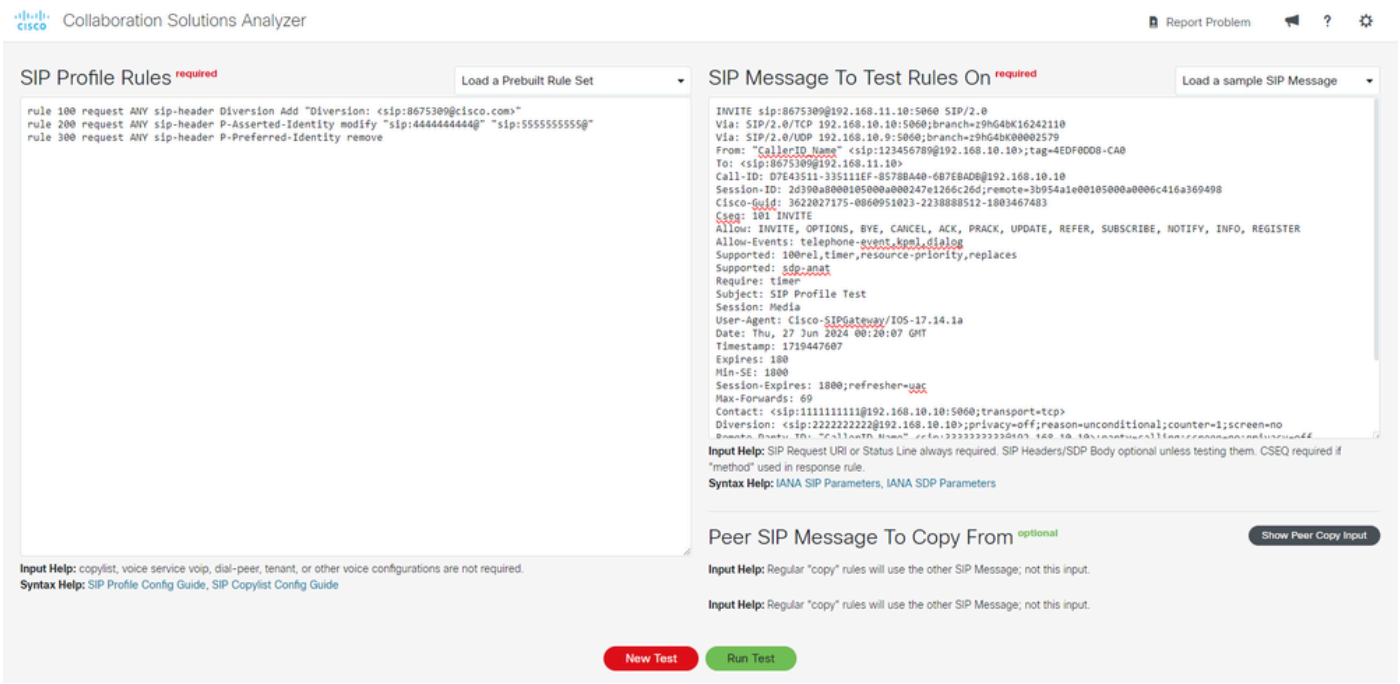
Règles de profil SIP

```
rule 100 request ANY sip-header Diversion Add "Diversion: <sip:8675309@cisco.com>"
rule 200 request ANY sip-header P-Asserted-Identity modify "sip:4444444444@" "sip:5555555555@"
rule 300 request ANY sip-header P-Preferred-Identity remove
```

Message Sip Sur Lequel Tester Les Règles

```
INVITE sip:8675309@192.168.11.10:5060 SIP/2.0
Via: SIP/2.0/TCP 192.168.10.10:5060;branch=z9hG4bK16242110
Via: SIP/2.0/UDP 192.168.10.9:5060;branch=z9hG4bK00002579
From: "CallerID_Name" <sip:123456789@192.168.10.10>;tag=4EDF0DD8-CA0
To: <sip:8675309@192.168.11.10>
Call-ID: D7E43511-335111EF-8578BA40-6B7EBADB@192.168.10.10
Session-ID: 2d390a8000105000a000247e1266c26d;remote=3b954a1e00105000a0006c416a369498
Cisco-Guid: 3622027175-0860951023-2238888512-1803467483
Cseq: 101 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
Allow-Events: telephone-event,kpml,dialog
Supported: 100rel,timer,resource-priority,replaces
Supported: sdp-anat
Require: timer
Subject: SIP Profile Test
Session: Media
User-Agent: Cisco-SIPGateway/IOS-17.14.1a
Date: Thu, 27 Jun 2024 00:20:07 GMT
Timestamp: 1719447607
Expires: 180
```

```
Min-SE: 1800
Session-Expires: 1800;refresher=uac
Max-Forwards: 69
Contact: <sip:1111111111@192.168.10.10:5060;transport=tcp>
Diversion: <sip:2222222222@192.168.10.10>;privacy=off;reason=unconditional;counter=1;screen=no
Remote-Party-ID: "CallerID_Name" <sip:3333333333@192.168.10.10>;party=calling;screen=no;privacy=off
P-Asserted-Identity: "CallerID_Name" <sip:4444444444@192.168.10.10>
P-Preferred-Identity: "CallerID_Name" <sip:5555555555@192.168.10.10>
CustomHeader: "CallerID_Name" <sip:7777777777@192.168.10.10>
Accept: application/sdp
Content-Disposition: session;handling=required
Content-Length: 0
```



Exemple de suppression de modification de profil SIP

Pour afficher le résultat, cliquez sur Exécuter le test.

Message SIP d'origine

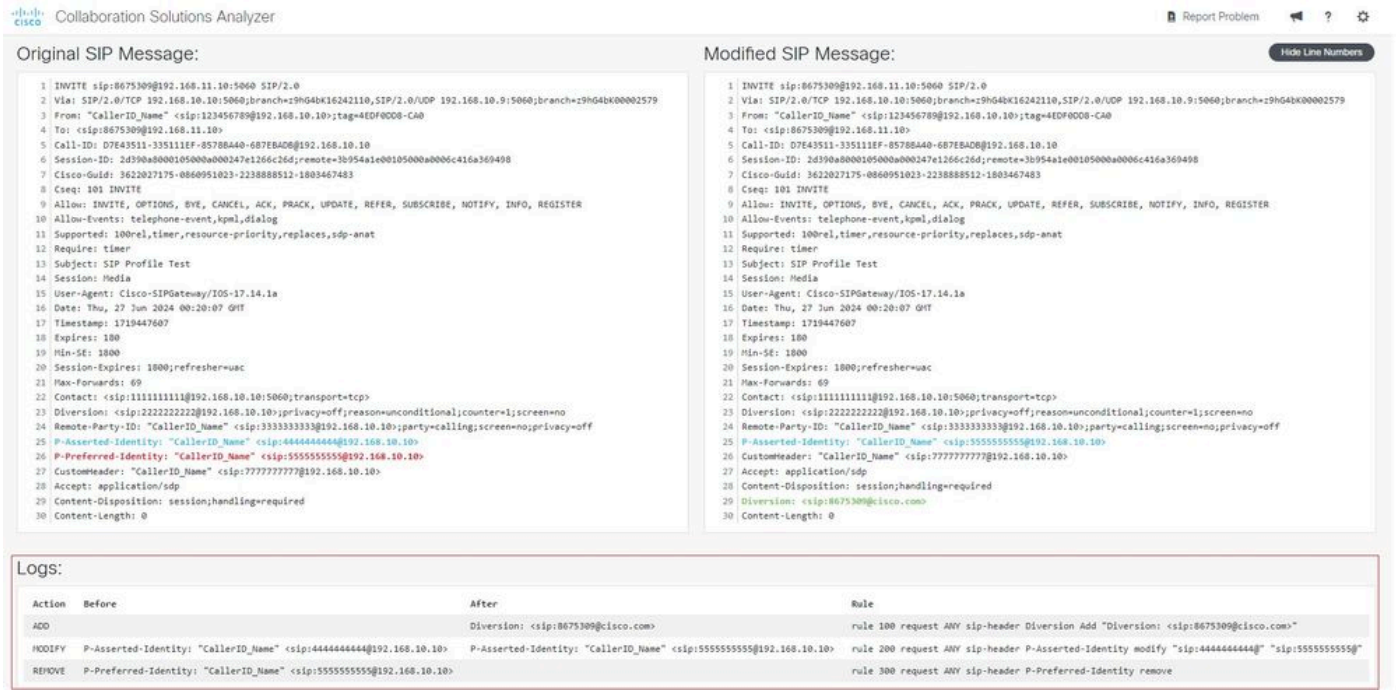
```
MODIFIED (BLUE) - P-Asserted-Identity: "CallerID_Name"

        4444444444@192.168.10.10>

REMOVED (RED) - P-Preferred-Identity: "CallerID_Name" <sip:5555555555@192.168.10.10>
```

Message SIP modifié

```
MODIFIED (BLUE) - P-Asserted-Identity: "CallerID_Name" <sip:5555555555@192.168.10.10>
ADDED (GREEN) - Diversion: <sip:8675309@cisco.com>
```



PROFIL SIP Modifier Ajouter Supprimer Exemple 2

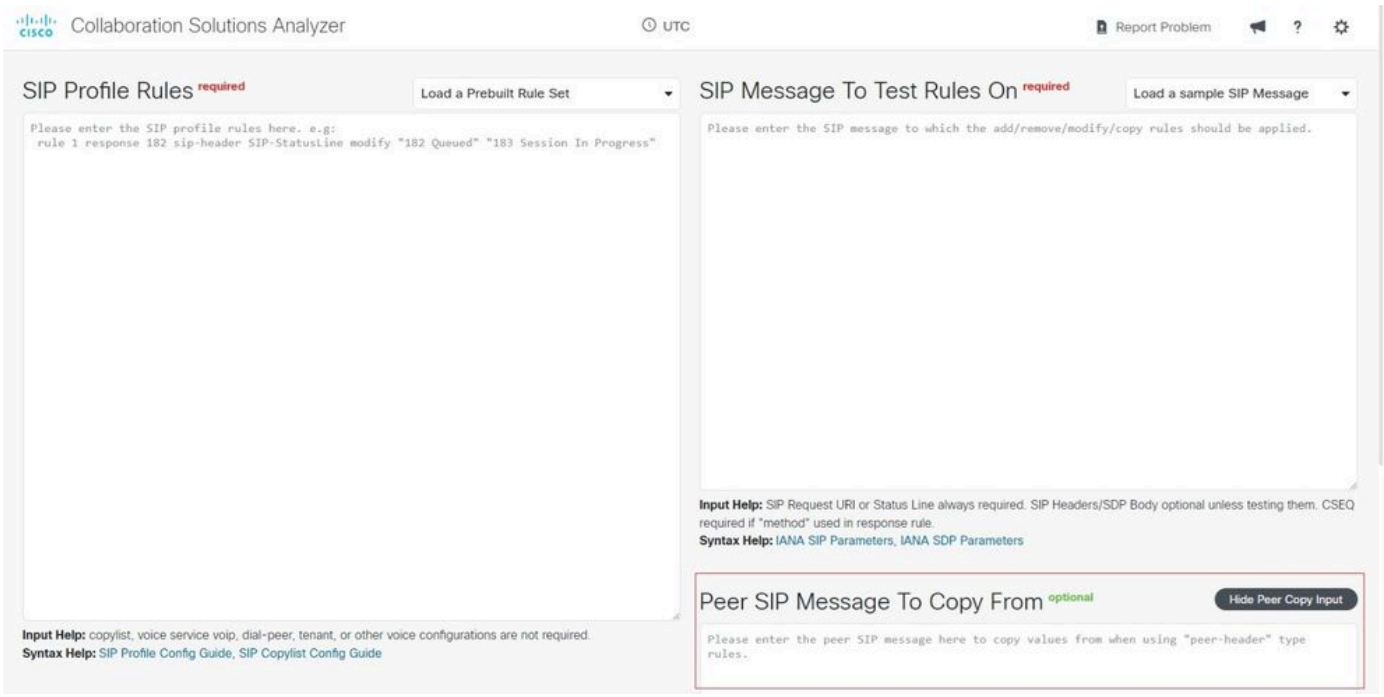
Copylist SIP Profile

Pour copier le contenu d'un en-tête entrant qu'un périphérique reçoit vers un en-tête sortant (liste de copie SIP), ces entrées d'outil peuvent être utilisées :

- Organigramme : Message SIP entrant — > CUBE — > Message SIP modifié

- Message SIP homologue à copier - Message SIP à copier.
- Message SIP pour tester les règles - Message SIP pour appliquer les règles.

Pour activer la section Message SIP homologue à copier depuis, l'option Show Peer Copy Input doit être activée. Vous pouvez cliquer sur Hide Peer Copy Input pour masquer cette section.



SIP PROFILE Copylist Accueil

Voici un exemple de règles SIP, de messages SIP entrants et modifiés :

Règles de profil SIP.

```
request INVITE peer-header sip To copy “sip:(.*)@” u01
request INVITE sip-header SIP-Req-URI modify “sip:(.*)@” sip:\u01@
```

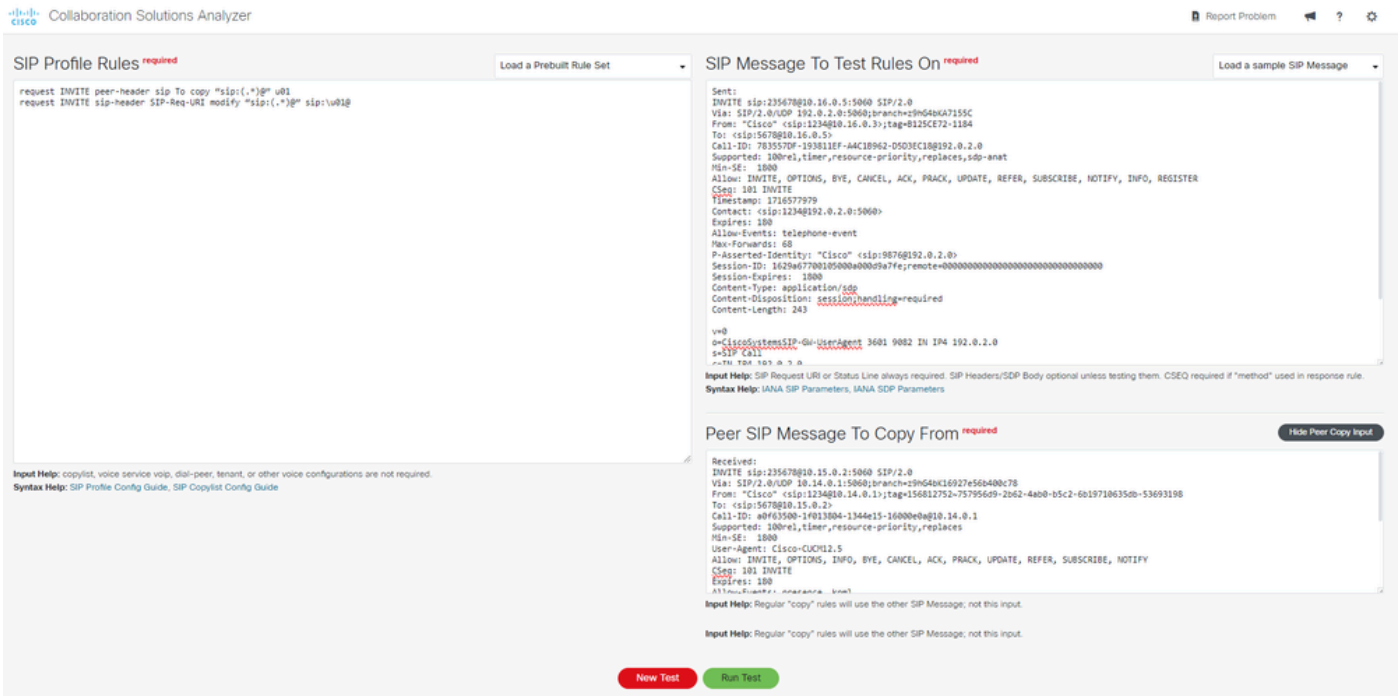
Message SIP pour appliquer les règles.

```
Sent:
INVITE sip:235678@10.16.0.5:5060 SIP/2.0
Via: SIP/2.0/UDP 192.0.2.0:5060;branch=z9hG4bKA7155C
From: "Cisco" <sip:1234@10.16.0.3>;tag=B125CE72-1184
To: <sip:5678@10.16.0.5>
Call-ID: 783557DF-193811EF-A4C1B962-D5D3EC18@192.0.2.0
Supported: 100rel,timer,resource-priority,replaces,sdp-anat
Min-SE:  1800
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
CSeq: 101 INVITE
Timestamp: 1716577979
Contact: <sip:1234@192.0.2.0:5060>
Expires: 180
Allow-Events: telephone-event
Max-Forwards: 68
P-Asserted-Identity: "Cisco" <sip:9876@192.0.2.0>
Session-ID: 1629a67700105000a000d9a7fe;remote=00000000000000000000000000000000
Session-Expires:  1800
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 243
```

```
v=0
o=CiscoSystemsSIP-GW-UserAgent 3601 9082 IN IP4 192.0.2.0
s=SIP Call
c=IN IP4 192.0.2.0
t=0 0
m=audio 8402 RTP/AVP 0 101
c=IN IP4 192.0.2.0
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
```

Message SIP à copier.

```
Received:
INVITE sip:235678@10.15.0.2:5060 SIP/2.0
Via: SIP/2.0/UDP 10.14.0.1:5060;branch=z9hG4bK16927e56b400c78
From: "Cisco" <sip:1234@10.14.0.1>;tag=156812752~757956d9-2b62-4ab0-b5c2-6b19710635db-53693198
To: <sip:5678@10.15.0.2>
Call-ID: a0f63500-1f013804-1344e15-16000e0a@10.14.0.1
Supported: 100rel,timer,resource-priority,replaces
Min-SE:  1800
User-Agent: Cisco-CUCM12.5
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
CSeq: 101 INVITE
Expires: 180
Allow-Events: presence, kpml
Supported: X-cisco-srtp-fallback,X-cisco-original-called
Call-Info: <sip:10.14.0.1:5060>;method="NOTIFY;Event=telephone-event;Duration=500"
Call-Info: <urn:x-cisco-remotecc:callinfo>;x-cisco-video-traffic-class=DESKTOP
Session-ID: 1629a67700105000885a92d9a7fe;remote=00000000000000000000000000000000
Cisco-Guid: 2700489984-0000065536-0000126777-1234102346
Session-Expires:  1800
P-Asserted-Identity: "Cisco" <sip:1234@10.14.0.1>
Remote-Party-ID: "Cisco" <sip:1234@10.14.0.1>;party=calling;screen=yes;privacy=off
Contact: <sip:1234@10.14.0.1:5060>;+u.sip!devicename.ccm.cisco.com="SEP885A92D9A7FE"
Max-Forwards: 69
Content-Length: 0
```



Exemple de liste de copie de PROFIL SIP

Continuez en cliquant sur le bouton Run Test pour lancer l'outil.

Registre De Copie

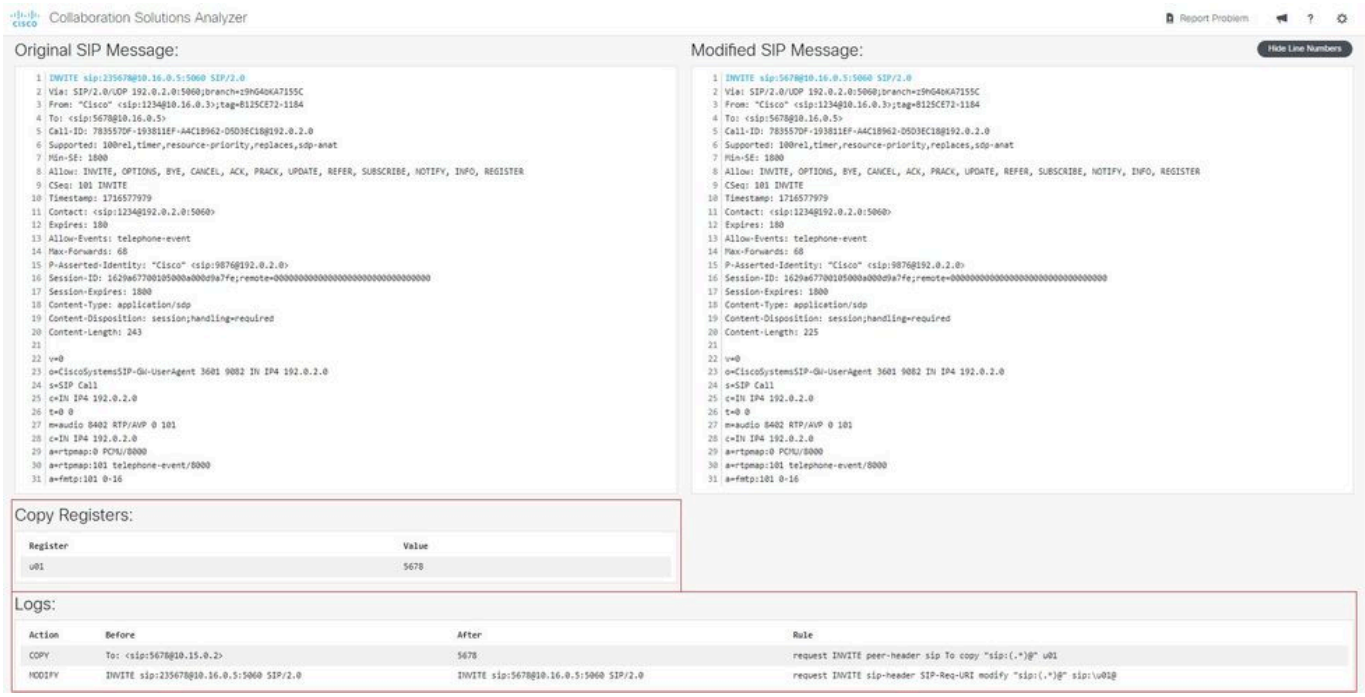
```
Register: u01
Value: 5678
```

Message SIP d'origine

```
MODIFIED (BLUE) - INVITE sip:235678@10.16.0.5:5060 SIP/2.0
```

Message SIP modifié

```
MODIFIED (BLUE) - INVITE sip:5678@10.16.0.5:5060 SIP/2.0
```

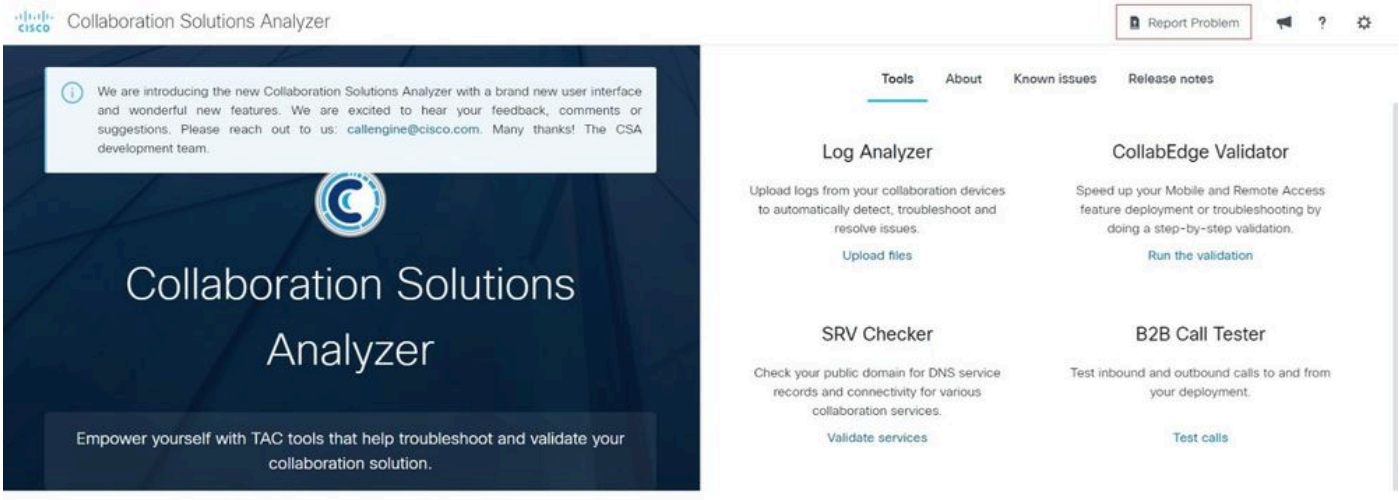


Copylist du PROFIL SIP - Exemple 2

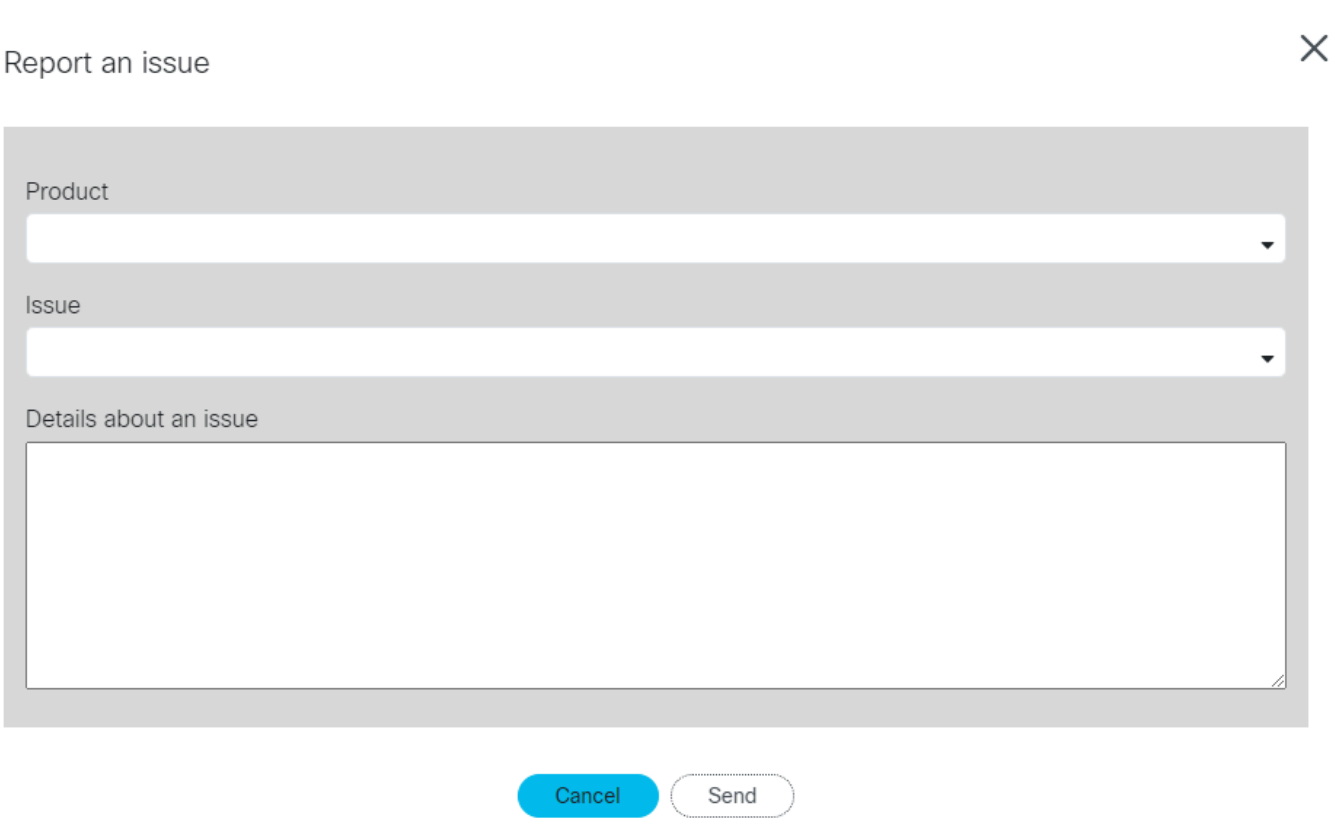
Signaler Un Problème

En haut de la plate-forme CSA, la section Signaler un problème vous permet de partager tout problème détecté dans les outils.

De plus, l'administrateur peut fournir des commentaires, des suggestions ou des commentaires en envoyant un courriel à l'adresse où l'équipe de développement de l'ASC traite l'information.

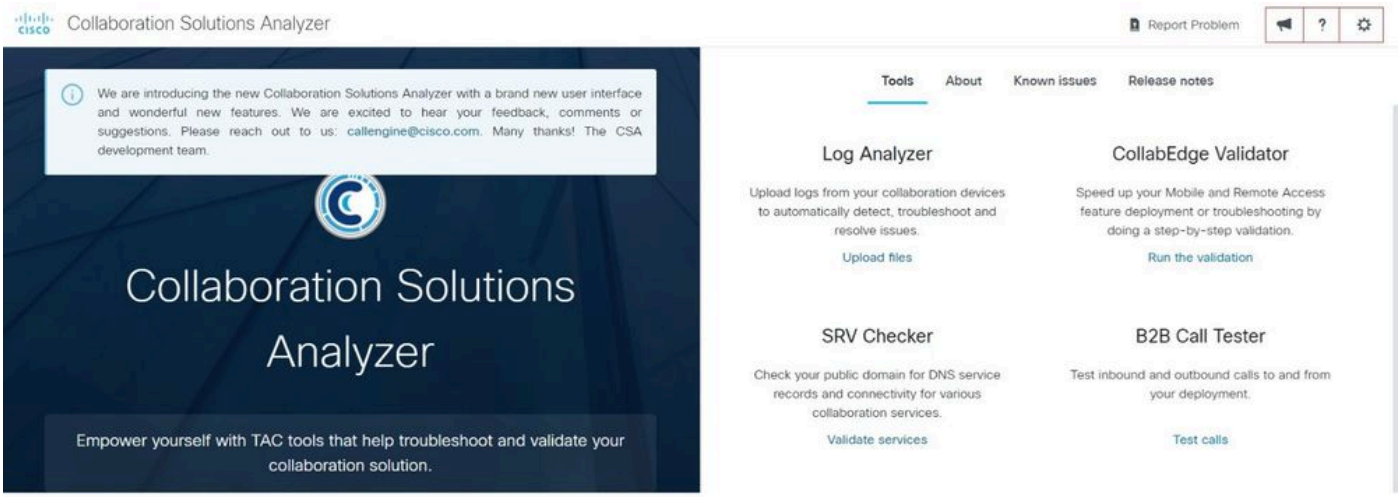


Signaler un problème Accueil



Problème de rapport

Trois icônes ont été activées pour permettre à l'utilisateur de fournir des commentaires (icône de mégaphone), de consulter la documentation utilisateur (icône de point d'interrogation) et d'ouvrir les paramètres utilisateur (icône de roue dentée).



Icônes

Informations relatives au support

[Configurer la collecte de débogage pour les passerelles CUBE et TDM]

[Guide de configuration de Cisco Unified Border Element via Cisco IOS XE 17.5]

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.