

Dépannage de CUBE via Collaboration Solutions Analyzer

Table des matières

[Introduction](#)

[Exigences](#)

[Pour commencer](#)

[Considérations](#)

[Description de plateforme](#)

[Analyseur De Journaux](#)

[Télécharger les fichiers journaux CUBE](#)

[Informations sur le segment d'appel](#)

[Diagramme En Échelle](#)

[Signalisation](#)

[Diagnostics](#)

[Capture de paquets CUBE](#)

[Testeur de profil SIP \(SPT\)](#)

[Exemple de profil SIP prédéfini](#)

[Copylist SIP Profile](#)

[Signaler Un Problème](#)

[Informations relatives au support](#)

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.

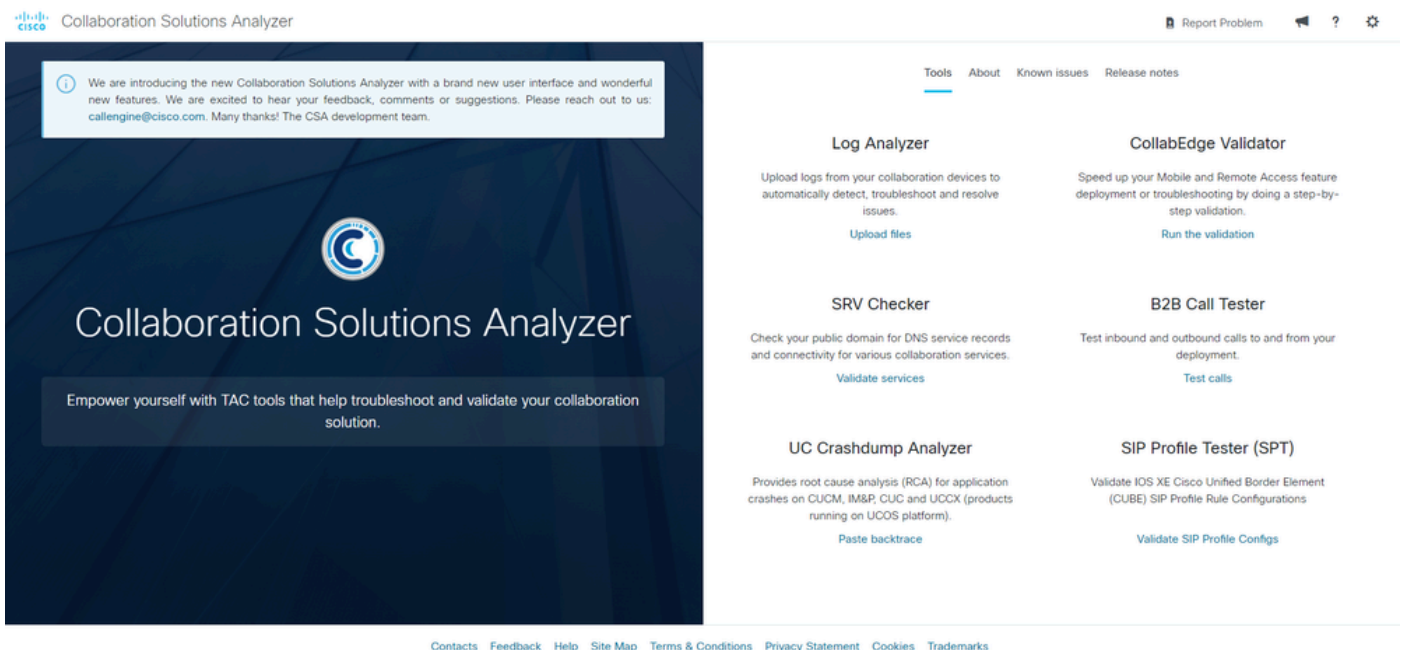
Log Analyzer utilise les journaux CUBE (basés sur le débogage des messages SIP) pour l'analyse.

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.



The screenshot shows the main interface of the Collaboration Solutions Analyzer (CSA) website. On the left, there is a large dark blue banner with the Cisco logo and the text "Collaboration Solutions Analyzer" and "Empower yourself with TAC tools that help troubleshoot and validate your collaboration solution." A notification box at the top left of the banner says: "We are introducing the new Collaboration Solutions Analyzer with a brand new user interface and wonderful new features. We are excited to hear your feedback, comments or suggestions. Please reach out to us: callengine@cisco.com. Many thanks! The CSA development team." On the right, there is a navigation menu with "Tools" selected, and "About", "Known issues", and "Release notes". Below the menu, there are six tool cards arranged in a 3x2 grid:

- Log Analyzer**: Upload logs from your collaboration devices to automatically detect, troubleshoot and resolve issues. [Upload files](#)
- CollabEdge Validator**: Speed up your Mobile and Remote Access feature deployment or troubleshooting by doing a step-by-step validation. [Run the validation](#)
- SRV Checker**: Check your public domain for DNS service records and connectivity for various collaboration services. [Validate services](#)
- B2B Call Tester**: Test inbound and outbound calls to and from your deployment. [Test calls](#)
- UC Crashdump Analyzer**: Provides root cause analysis (RCA) for application crashes on CUCM, IM&P, CUC and UCCX (products running on UCOS platform). [Paste backtrace](#)
- SIP Profile Tester (SPT)**: Validate IOS XE Cisco Unified Border Element (CUBE) SIP Profile Rule Configurations. [Validate SIP Profile Configs](#)

At the bottom of the page, there is a footer with links: [Contacts](#), [Feedback](#), [Help](#), [Site Map](#), [Terms & Conditions](#), [Privacy Statement](#), [Cookies](#), [Trademarks](#)


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

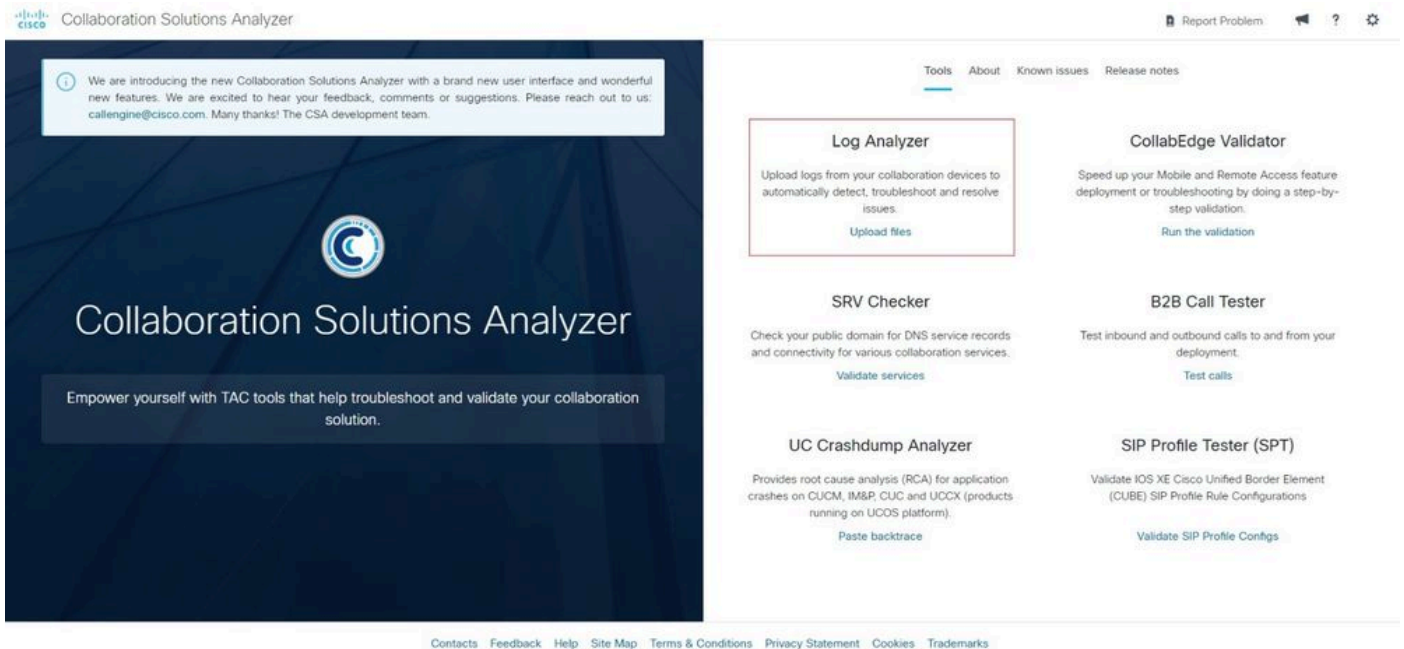
- Signalisation

 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 Analyzer.



Collaboration Solutions Analyzer

We are introducing the new Collaboration Solutions Analyzer with a brand new user interface and wonderful new features. We are excited to hear your feedback, comments or suggestions. Please reach out to us: callengine@cisco.com. Many thanks! The CSA development team.

Collaboration Solutions Analyzer

Empower yourself with TAC tools that help troubleshoot and validate your collaboration solution.

Tools About Known issues Release notes

Log Analyzer
Upload logs from your collaboration devices to automatically detect, troubleshoot and resolve issues.
Upload files

CollabEdge Validator
Speed up your Mobile and Remote Access feature deployment or troubleshooting by doing a step-by-step validation.
Run the validation

SRV Checker
Check your public domain for DNS service records and connectivity for various collaboration services.
Validate services

B2B Call Tester
Test inbound and outbound calls to and from your deployment.
Test calls

UC Crashdump Analyzer
Provides root cause analysis (RCA) for application crashes on CUCM, IM&P, CUC and UCCX (products running on UCOS platform).
Paste backtrace

SIP Profile Tester (SPT)
Validate IOS XE Cisco Unified Border Element (CUBE) SIP Profile Rule Configurations.
Validate SIP Profile Configs

Contacts Feedback Help Site Map Terms & Conditions Privacy Statement Cookies Trademarks

Accueil de Log Analyser

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

Log Analyzer

Automatic issue detection

When analysing the log files, tool will automatically detect any known defects by looking at the communication flows. Common configuration issues are also detected and corrective action plan or workaround is presented.

Configuration and system overview

Tool provides a overview of device hardware, configuration, services and other status information that may be useful for detecting or troubleshooting an issue.

Multi-product end-to-end flow

By analysing multiple logs from different products involved in a communication flow such as call and correlating this information, the tool presents an end-to-end flow diagram to visualize it across all products. This allows for easy identification of where the issue may be coming from.

Upload and analyze files

No files found in the user sandbox. Start by uploading them below.

If you have multiple logs, you can also upload them all together in a single archive. Ensure each file represents one running log file

If the product type is not automatically identified it could be that the product is not supported, the archive content/structure is not supported, is corrupted or the product identification failed. You can try and manually select the product type.

Click or drag files here

Upload

Chargement de Log Analyzer

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

Log Analyzer

Automatic issue detection

When analysing the log files, tool will automatically detect any known defects by looking at the communication flows. Common configuration issues are also detected and corrective action plan or workaround is presented.

Configuration and system overview

Tool provides a overview of device hardware, configuration, services and other status information that may be useful for detecting or troubleshooting an issue.

Multi-product end-to-end flow

By analysing multiple logs from different products involved in a communication flow such as call and correlating this information, the tool presents an end-to-end flow diagram to visualize it across all products. This allows for easy identification of where the issue may be coming from.

Upload and analyze files

No files found in the user sandbox. Start by uploading them below.

If you have multiple logs, you can also upload them all together in a single archive. Ensure each file represents one running log file

If the product type is not automatically identified it could be that the product is not supported, the archive content/structure is not supported, is corrupted or the product identification failed. You can try and manually select the product type.

CUBE_logs.txt
56 KB

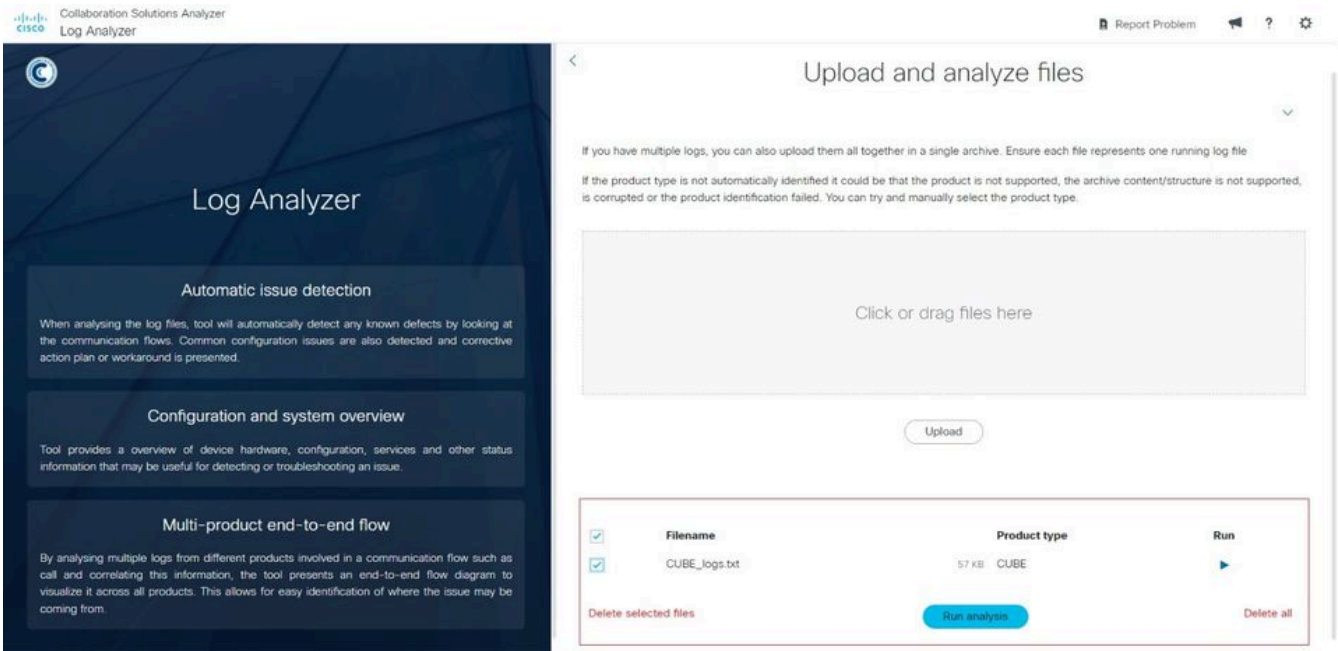
1 Selected (Total: 56 KB)

Upload

Fichier de téléchargement Log Analyzer

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.

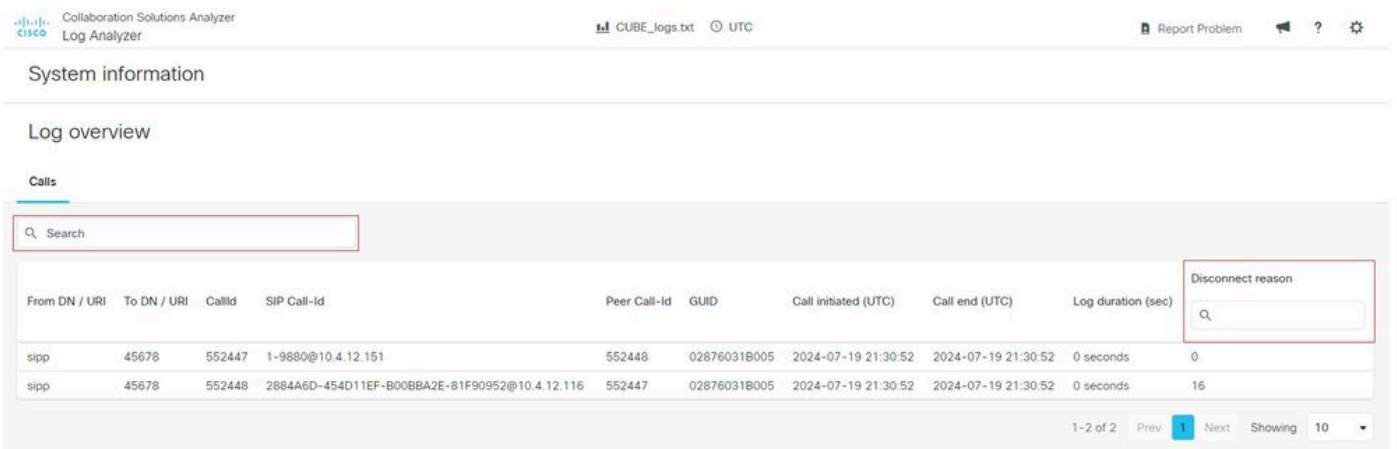
- Le système définit le type de produit sur CUBE.
- Plusieurs fichiers peuvent être analysés dans la même session.



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.

SIP - outgoing

Ladder tags

Use for signaling and ladder

General information

SIP call leg type	Call
From	sipp@10.4.12.116
To	45678@10.4.12.151
Signaling source	10.4.12.116 : 5060
Signaling destination	10.4.12.151 : 5060
Call ID	2884A6D-454D11EF-B00BBA2E-81F90952@10.4.12.116
Call leg connects	✓ 2024-07-19 21:30:52 UTC

SIP - incoming

Ladder tags

Use for signaling and ladder

General information

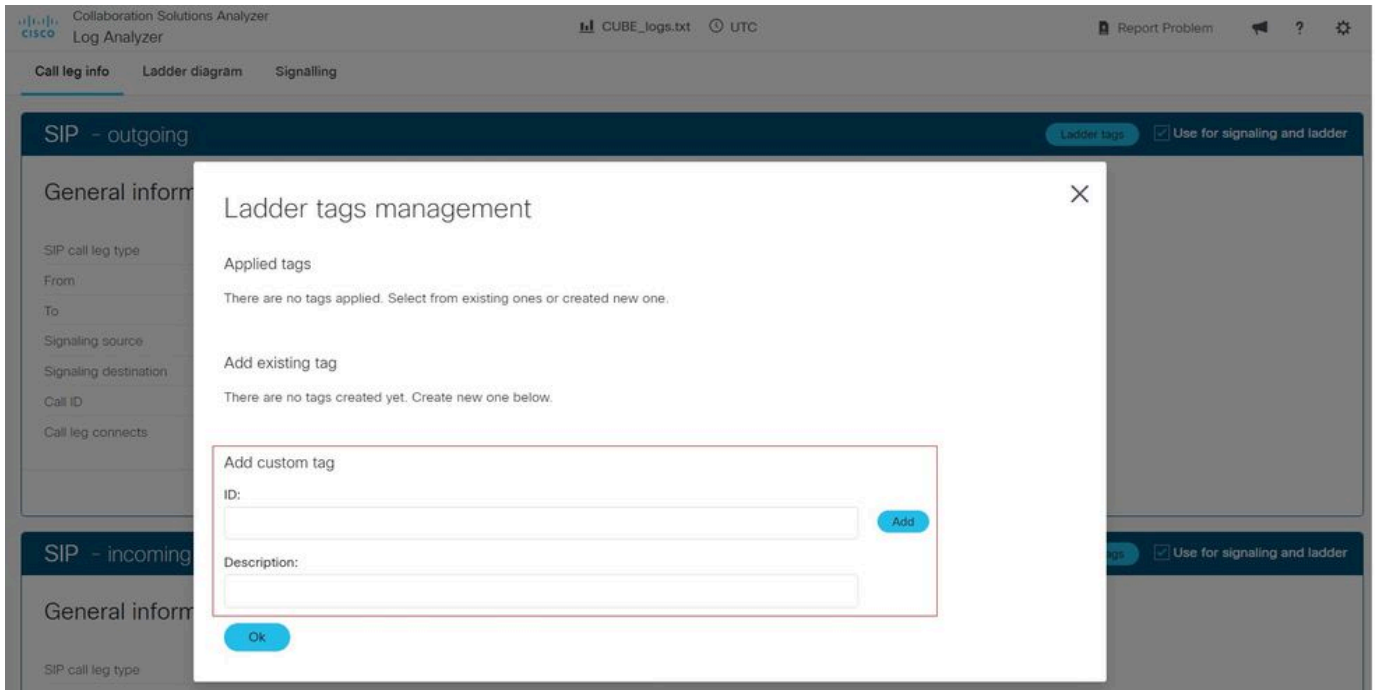
SIP call leg type	Call
From	sipp@10.4.12.151:5061
To	45678@10.4.12.116:5060
Signaling source	10.4.12.151 : 5061
Signaling destination	10.4.12.116 : 5060
Call ID	1-9880@10.4.12.151

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.

Call

Call leg info **Ladder diagram** Signalling

Allow horizontal scroll [Download ladder](#)

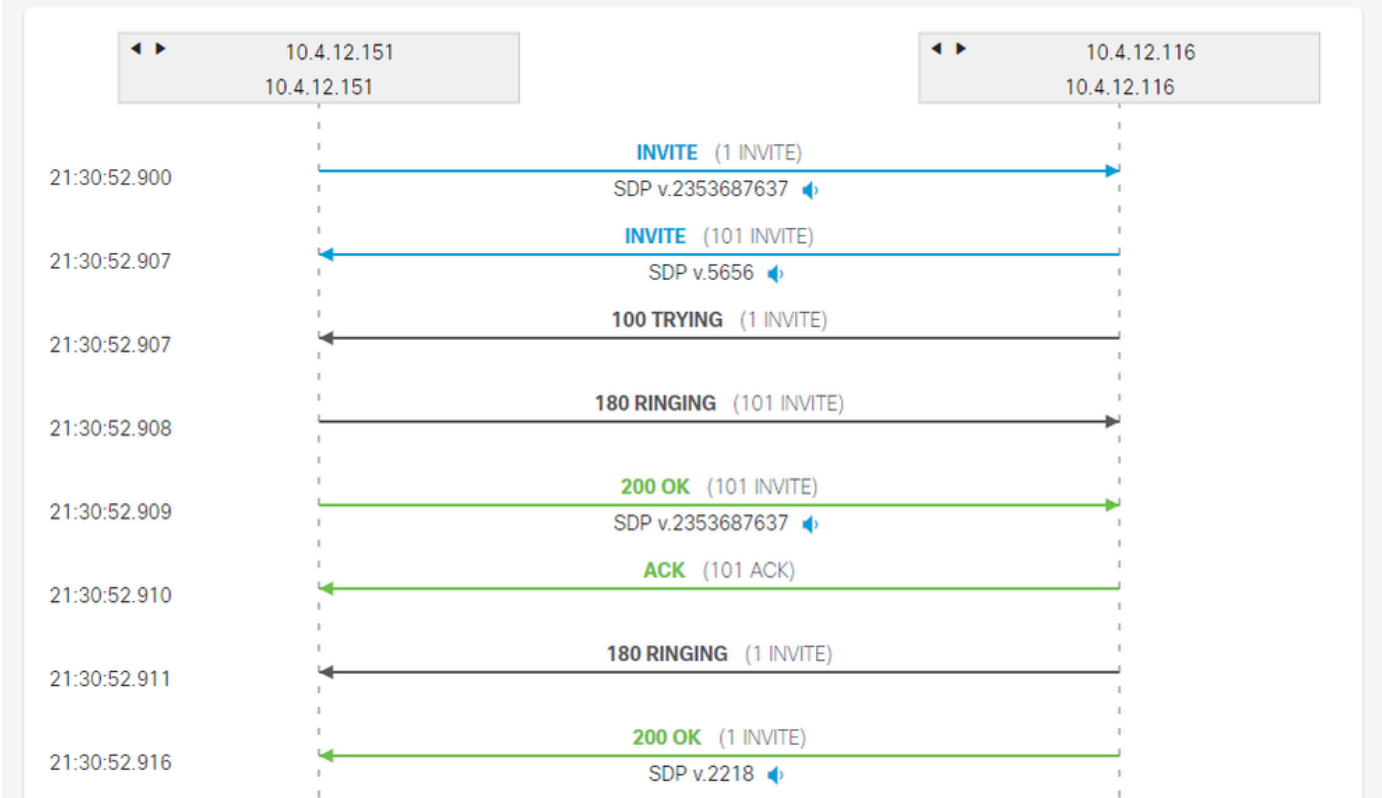


Diagramme De L'Échelle Log Analyser

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

Collaboration Solutions Analyzer
Log Analyzer

UTC

21:30:5 10.4.12.151 10.4.12.116

200 OK (101 INVITE)

SDP v.2353687637

Message

CUBE_logs.txt

Message body

```

BYE sip:10.4.12.151:5060;transport=UDP SIP/2.0
Via: SIP/2.0/UDP 10.4.12.116:5060;branch=z9hG4bK17E4FD
From: "sipp" <sip:sipp@10.4.12.116>;tag=A4BA9783-192B
To: <sip:45678@10.4.12.151>;tag=9505SIPpTag01132
Date: Fri, 19 Jul 2024 21:30:52 GMT
Call-ID: 2884A6D-454D11EF-B00BBA2E-81F90952@10.4.12.116
User-Agent: Cisco-SIPGateway/IOS-17.6.1a
Max-Forwards: 70
P-Asserted-Identity: "sipp" <sip:sipp@10.4.12.116>
Timestamp: 1721424652
CSeq: 102 BYE
Reason: Q.850;cause=16
Session-ID: 8148df0cc80d5cdd8e1cef5f36445d60;remote=d865788014d352b38b6aa60a34948979
Content-Length: 0

```

Ok

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.

Ladder tags management

Applied tags

ID	Description	Visual	Action
10.4.12.151	Service Provider	●	🗑️

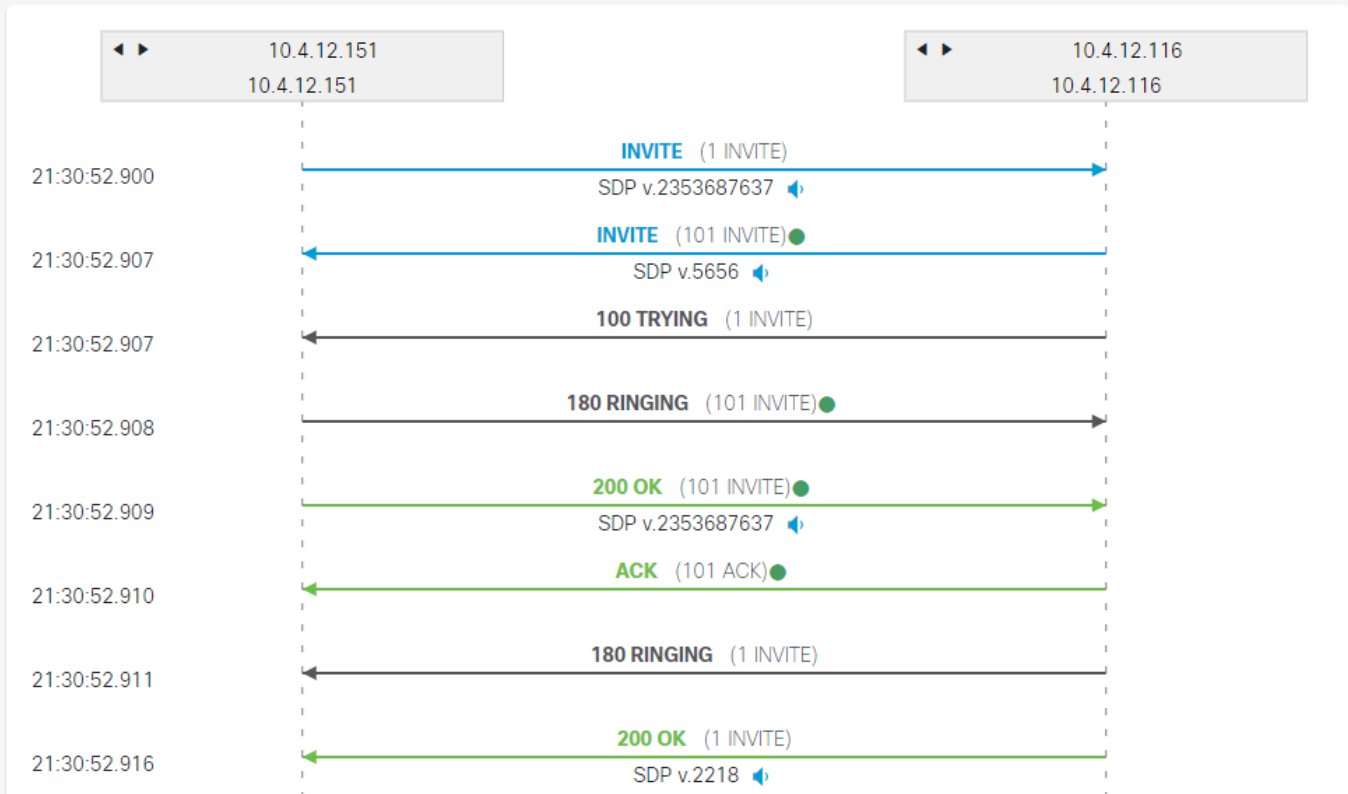
Étiquettes d'échelle Log Analyser 1

Call

Call leg info **Ladder diagram** Signalling

Allow horizontal scroll

Legend: ■ Service Provider



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.

Ladder tags management



Applied tags

ID	Description	Visual	Action
PCMU	Voice Codec G711ulaw	●	🗑️

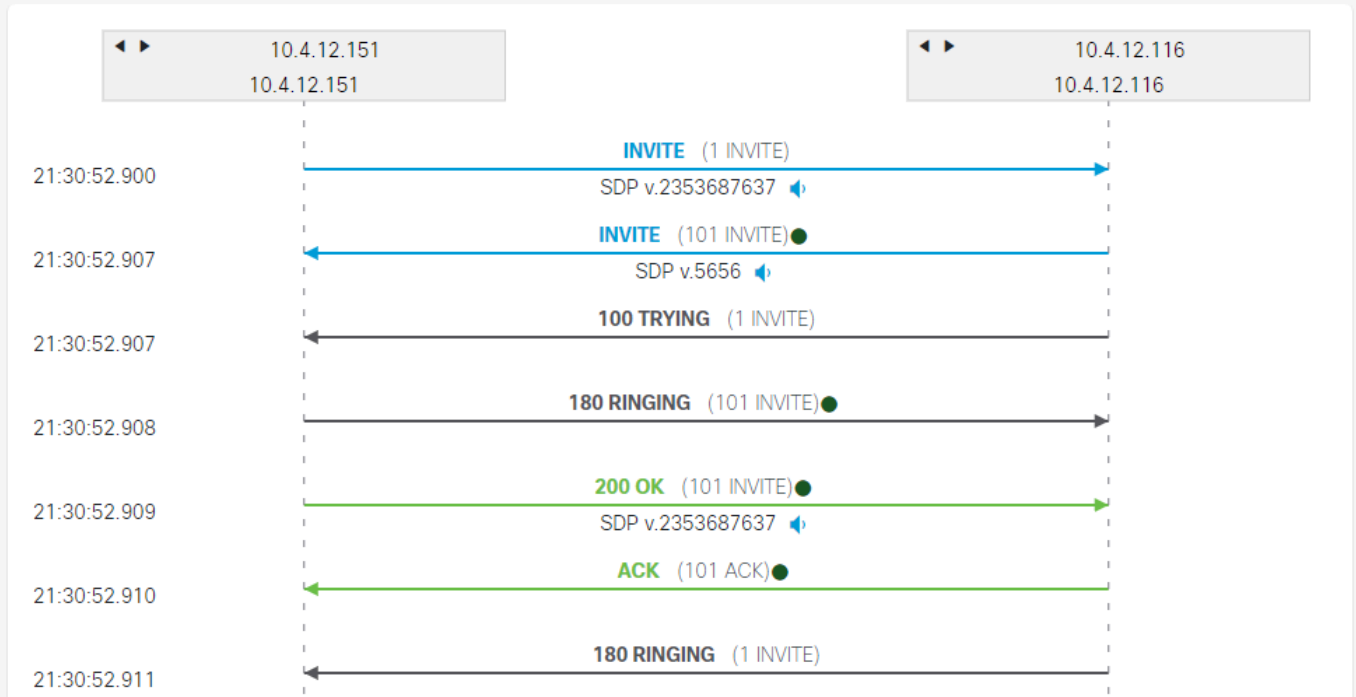
Étiquettes d'échelle Log Analyser 3

Call

Call leg info **Ladder diagram** Signalling

Allow horizontal scroll

Legend: ■ Voice Codec G711ulaw



Étiquettes d'échelle Log Analyser 4

Signalisation

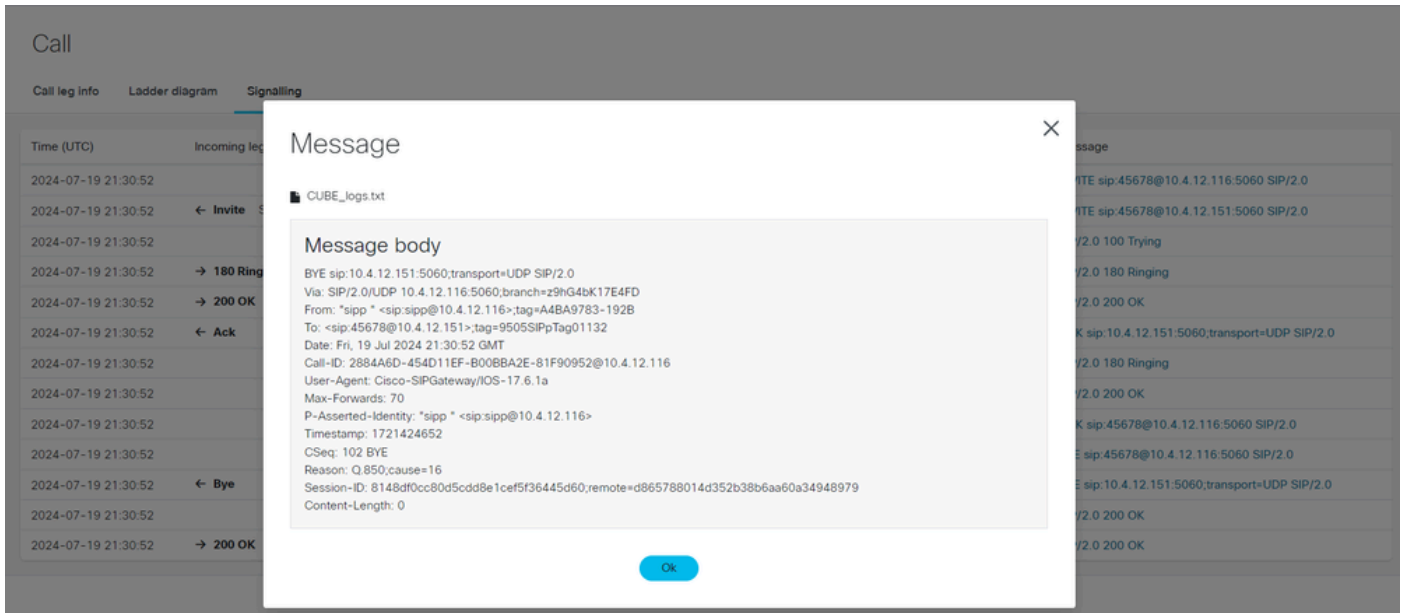
La dernière étape est la signalisation, qui affiche les messages SIP pour les deux branches CUBE (entrantes et sortantes). Il contient les adresses IP source et de destination. Cliquez pour afficher le message.

Call

Call leg info **Ladder diagram** **Signalling**

Time (UTC)	Incoming legs	Outgoing legs	Sequence	Source	Destination	Message
2024-07-19 21:30:52		← Invite SDP v.2353687637	1 INVITE	10.4.12.151:5061	10.4.12.116:5060	INVITE sip:45678@10.4.12.116:5060 SIP/2.0
2024-07-19 21:30:52	← Invite SDP v.5656		101 INVITE	10.4.12.116:5060	10.4.12.151:5060	INVITE sip:45678@10.4.12.151:5060 SIP/2.0
2024-07-19 21:30:52		→ 100 Trying	1 INVITE	10.4.12.116:5060	10.4.12.151:5061	SIP/2.0 100 Trying
2024-07-19 21:30:52	→ 180 Ringing		101 INVITE	10.4.12.151:5060	10.4.12.116:5060	SIP/2.0 180 Ringing
2024-07-19 21:30:52	→ 200 OK SDP v.2353687637		101 INVITE	10.4.12.151:5060	10.4.12.116:5060	SIP/2.0 200 OK
2024-07-19 21:30:52	← Ack		101 ACK	10.4.12.116:5060	10.4.12.151:5060	ACK sip:10.4.12.151:5060;transport=UDP SIP/2.0
2024-07-19 21:30:52		→ 180 Ringing	1 INVITE	10.4.12.116:5060	10.4.12.151:5061	SIP/2.0 180 Ringing
2024-07-19 21:30:52		→ 200 OK SDP v.2218	1 INVITE	10.4.12.116:5060	10.4.12.151:5061	SIP/2.0 200 OK
2024-07-19 21:30:52		← Ack	1 ACK	10.4.12.151:5061	10.4.12.116:5060	ACK sip:45678@10.4.12.116:5060 SIP/2.0
2024-07-19 21:30:52		← Bye	2 BYE	10.4.12.151:5061	10.4.12.116:5060	BYE sip:45678@10.4.12.116:5060 SIP/2.0
2024-07-19 21:30:52	← Bye		102 BYE	10.4.12.116:5060	10.4.12.151:5060	BYE sip:10.4.12.151:5060;transport=UDP SIP/2.0
2024-07-19 21:30:52		→ 200 OK	2 BYE	10.4.12.116:5060	10.4.12.151:5061	SIP/2.0 200 OK
2024-07-19 21:30:52	→ 200 OK		102 BYE	10.4.12.151:5060	10.4.12.116:5060	SIP/2.0 200 OK

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.

Collaboration Solutions Analyzer
Log Analyzer

CUBE_logs.txt UTC

Report Problem ?

Log overview

Calls

Search

From DN / URI	To DN / URI	CallId	SIP Call-Id	Peer Call-Id	GUID	Call initiated (UTC)	Call end (UTC)	Log duration (sec)	Disconnect reason
sipp	45678	5524 47	1-9880@10.4.12.1 51	552448	02876 031B0 05	2024-07-19 21:3 0:52	2024-07-19 2 1:30:52	0 seconds	0
sipp	45678	5524 48	2884A6D-454D11E F-B00BBA2E-81F9 0952@10.4.12.116	552447	02876 031B0 05	2024-07-19 21:3 0:52	2024-07-19 2 1:30:52	0 seconds	16

1-2 of 2 Prev 1 Next Showing 10

Accueil de Log Analyser Diagnostics

Collaboration Solutions Analyzer
Log Analyzer

UTC

Report Problem ?

Diagnostic overview

Issues found No issue Not applicable Missing information Potential problem

Search

Result Category ^

- Call (8)
- MRA (0)
- Configuration (0)

Defects only

✓ No issues were found.

You can still view the diagnostic signatures that were run but did not find any issue by selecting different result type tabs above.

Click on any of the below to see details or [continue to analysis](#).

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.

The screenshot shows the Cisco Log Analyzer interface. On the left is a dark sidebar with the title 'Log Analyzer' and sections for 'Automatic issue detection' and 'Configuration and system overview'. The main area is titled 'product type.' and contains a large grey box with the text 'Click or drag files here' and an 'Upload' button. Below this is a table with columns 'Filename', 'Product type', and 'Run'. The table contains two rows: 'CUBE_Packet_Capture.pcap' (83 KB, PCAP) and 'CUBE_logs.txt' (57 KB, CUBE). There are checkboxes for each row, a 'Run analysis' button, and a 'Delete selected files' button.

Filename	Product type	Run
<input checked="" type="checkbox"/> CUBE_Packet_Capture.pcap	83 KB PCAP	
<input type="checkbox"/> CUBE_logs.txt	57 KB CUBE	

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.

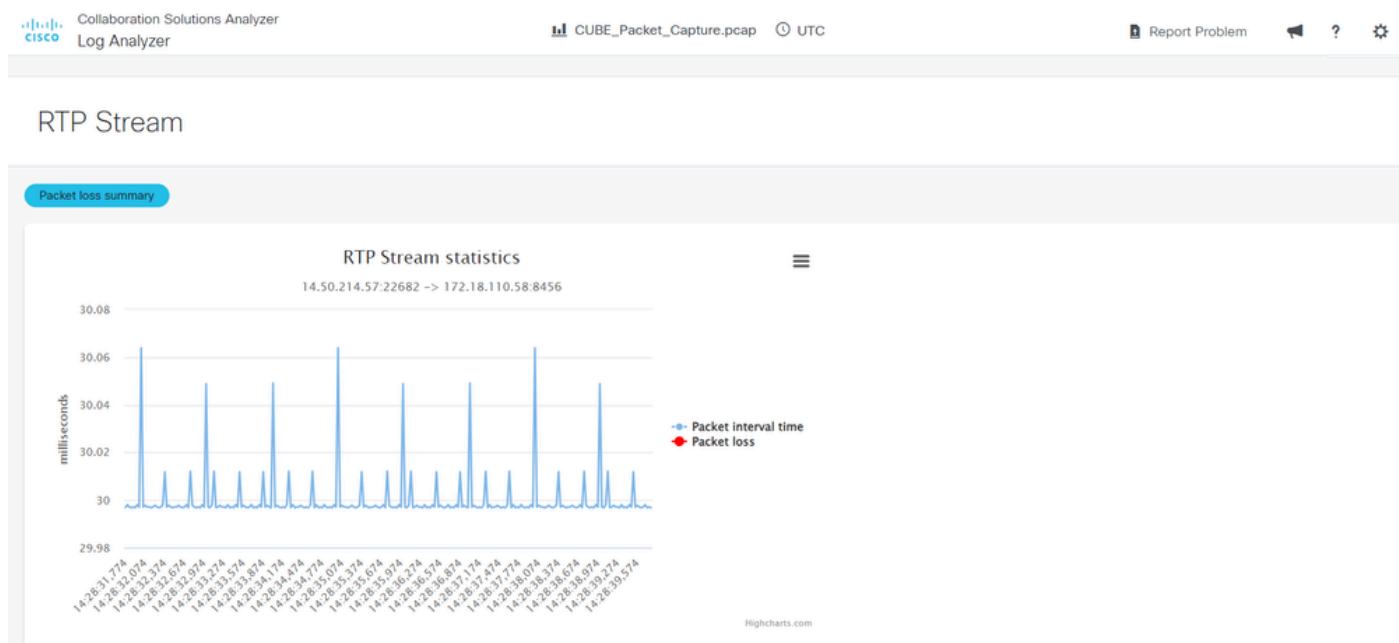
Sélectionnez une session dans la colonne Flux RTP et l'outil affiche les statistiques du flux RTP pour cette connexion. Si le flux est affecté par les conditions du réseau, le paramètre Packet Loss (Perte de paquets) est marqué par des points rouges.

The screenshot shows the Cisco Log Analyzer interface with the 'RTP streams' tab selected. The 'Log overview' section displays a table with columns: Src IP, Src port, Dest IP, Dest port, Payload type, SSRC, Packet count, Packet loss, Jitter (mean/max), and Info. The table contains two rows of data. Below the table is a pagination control showing '1-2 of 2' and 'Showing 10'.

Src IP	Src port	Dest IP	Dest port	Payload type	SSRC	Packet count	Packet loss	Jitter (mean/max)	Info
172.18.110.58	8456	14.50.214.57	22682	8	7a3e	273	0%	0 ms / 0.01 ms	
14.50.214.57	22682	172.18.110.58	8456	8	97d5b2f9	269	0%	0 ms / 0.01 ms	

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.

System information

Log overview

RTP streams TCP/UDP Streams

Search

Protocol	Src IP	Src port	Dest IP	Dest port	Packet count	2-way communication	OCSP
UDP	172.18.110.58	49782	172.18.110.48	5060	4	✖	
UDP	172.18.110.48	5060	172.18.110.58	5060	4	✖	
UDP	172.18.110.59	32771	172.18.110.1	5060	2	✖	

1-3 of 3 Prev 1 Next Showing 10

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 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.

The screenshot shows the Cisco Collaboration Solutions Analyzer interface. At the top, it displays the Cisco logo, the text "Collaboration Solutions Analyzer", and "UTC". On the right, there are links for "Report Problem", a help icon, and a settings icon. The main interface is divided into two primary sections: "SIP Profile Rules" and "SIP Message To Test Rules On".

The "SIP Profile Rules" section has a "required" status and a "Load a Prebuilt Rule Set" dropdown. Below it is a text area containing the example rule: "rule 1 response 182 sip-header SIP-Statusline modify \"182 Queued\" \"183 Session In Progress\"". Below the text area, there is an "Input Help" section stating that copylist, voice service voip, dial-peer, tenant, or other voice configurations are not required, and a "Syntax Help" link to the SIP Profile Config Guide and SIP Copylist Config Guide.

The "SIP Message To Test Rules On" section also has a "required" status and a "Load a sample SIP Message" dropdown. Below it is a large text area for entering the SIP message. Below this text area, there is an "Input Help" section stating that SIP Request URI or Status Line is always required, and SIP Headers/SDP Body is optional unless testing them. Below that is a "Syntax Help" link to IANA SIP Parameters and IANA SDP Parameters.

Below these two sections is a "Peer SIP Message To Copy From" section with an "optional" status and a "Show Peer Copy Input" button. Below this, there is an "Input Help" section stating that regular "copy" rules will use the other SIP Message, not this input.

At the bottom of the interface, there are two buttons: a red "New Test" button and a green "Run Test" button.

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.

The screenshot shows the Cisco Collaboration Solutions Analyzer interface. On the left, under 'SIP Profile Rules', a rule is configured with the header 'Add: SIP Header' and the content 'rule 100 request ANY sip-header Diversion Add "Diversion: < sip:8675309@cisco.com>"'. On the right, under 'SIP Message To Test Rules On', a sample INVITE message is shown with various headers like 'Via: SIP/2.0/TCP', 'From: "CallerID Name"', 'Call-ID', 'Session-ID', 'Cisco-Guid', 'Cseq: 101 INVITE', 'Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER', 'Supported: 100rel, timer, resource-priority, replaces', 'Require: sip-addr', 'Subject: SIP Profile Test', 'User-Agent: Cisco-SIPGateway/IOS-17.14.1a', 'Date: Thu, 27 Jun 2024 00:28:07 GMT', 'Timestamp: 1710447607', 'Expires: 180', 'Min-SE: 1800', 'Session-Expires: 1800;refresher-uac', 'Max-Forwards: 69', 'Contact: < sip:111111111@192.168.10.10:5060;transport=tcp>', and 'Diversion: < sip:222222222@192.168.10.10;privacy=off;reason=unconditional;counter=1;screen=no >'. Below the message, there are 'Input Help' and 'Syntax Help' sections. At the bottom, there are 'New Test' and 'Run Test' buttons.

PROFIL SIP préconfiguré

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

Message SIP modifié

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

New Test

Show Inputs

Original SIP Message:

```

1 INVITE sip:8675309@192.168.11.10:5060 SIP/2.0
2 Via: SIP/2.0/TCP 192.168.10.10:5060;branch=z9hG4bK16242110,SIP/2.0/UDP 192.168.10.9:5060;branch=z9hG4bK00002579
3 From: "CallerID_Name" <sip:123456789@192.168.10.10>;tag=4EDF0DD8-CA0
4 To: <sip:8675309@192.168.11.10>
5 Call-ID: D7E43511-335111EF-8578BA40-6B7EBADB@192.168.10.10
6 Session-ID: 2d390a8000105000a000247e1266c26d;remote=3b954a1e00105000a0006c416a369498
7 Cisco-Guid: 3622027175-0860951023-2238888512-1803467483
8 Cseq: 101 INVITE
9 Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
10 Allow-Events: telephone-event, kpml, dialog
11 Supported: 100rel, timer, resource-priority, replaces, sdp-anat
12 Requires: timer
13 Subject: SIP Profile Test
14 Session: Media
15 User-Agent: Cisco-SIPGateway/IOS-17.14.1a
16 Date: Thu, 27 Jun 2024 00:20:07 GMT
17 Timestamp: 1719447607
18 Expires: 180
19 Min-SE: 1800
20 Session-Expires: 1800;refresher=uac
21 Max-Forwards: 69
22 Contact: <sip:111111111@192.168.10.10:5060;transport=tcp>
23 Diversion: <sip:222222222@192.168.10.10>;privacy=off;reason=unconditional;counter=1;screen=no
24 Remote-Party-ID: "CallerID_Name" <sip:333333333@192.168.10.10>;party=calling;screen=no;privacy=off
25 P-Asserted-Identity: "CallerID_Name" <sip:444444444@192.168.10.10>
26 P-Preferred-Identity: "CallerID_Name" <sip:555555555@192.168.10.10>
27 CustomHeader: "CallerID_Name" <sip:777777777@192.168.10.10>
28 Accept: application/sdp
29 Content-Disposition: session;handling=required
30 Content-Length: 0

```

Modified SIP Message:

Hide Line Numbers

```

1 INVITE sip:8675309@192.168.11.10:5060 SIP/2.0
2 Via: SIP/2.0/TCP 192.168.10.10:5060;branch=z9hG4bK16242110,SIP/2.0/UDP 192.168.10.9:5060;branch=z9hG4bK00002579
3 From: "CallerID_Name" <sip:123456789@192.168.10.10>;tag=4EDF0DD8-CA0
4 To: <sip:8675309@192.168.11.10>
5 Call-ID: D7E43511-335111EF-8578BA40-6B7EBADB@192.168.10.10
6 Session-ID: 2d390a8000105000a000247e1266c26d;remote=3b954a1e00105000a0006c416a369498
7 Cisco-Guid: 3622027175-0860951023-2238888512-1803467483
8 Cseq: 101 INVITE
9 Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
10 Allow-Events: telephone-event, kpml, dialog
11 Supported: 100rel, timer, resource-priority, replaces, sdp-anat
12 Requires: timer
13 Subject: SIP Profile Test
14 Session: Media
15 User-Agent: Cisco-SIPGateway/IOS-17.14.1a
16 Date: Thu, 27 Jun 2024 00:20:07 GMT
17 Timestamp: 1719447607
18 Expires: 180
19 Min-SE: 1800
20 Session-Expires: 1800;refresher=uac
21 Max-Forwards: 69
22 Contact: <sip:111111111@192.168.10.10:5060;transport=tcp>
23 Diversion: <sip:222222222@192.168.10.10>;privacy=off;reason=unconditional;counter=1;screen=no
24 Remote-Party-ID: "CallerID_Name" <sip:333333333@192.168.10.10>;party=calling;screen=no;privacy=off
25 P-Asserted-Identity: "CallerID_Name" <sip:444444444@192.168.10.10>
26 P-Preferred-Identity: "CallerID_Name" <sip:555555555@192.168.10.10>
27 CustomHeader: "CallerID_Name" <sip:777777777@192.168.10.10>
28 Accept: application/sdp
29 Content-Disposition: session;handling=required
30 Diversion: <sip:8675309@cisco.com>
31 Content-Length: 0

```

Logs:

Action	Before	After	Rule
ADD		Diversion: <sip:8675309@cisco.com>	rule 100 request ANY sip-header Diversion Add "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:444444444@" "sip:555555555@"
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:111111111@192.168.10.10:5060;transport=tcp>
 Diversion: <sip:222222222@192.168.10.10>;privacy=off;reason=unconditional;counter=1;screen=no
 Remote-Party-ID: "CallerID_Name" <sip:333333333@192.168.10.10>;party=calling;screen=no;privacy=off
 P-Asserted-Identity: "CallerID_Name" <sip:444444444@192.168.10.10>
 P-Preferred-Identity: "CallerID_Name" <sip:555555555@192.168.10.10>
 CustomHeader: "CallerID_Name" <sip:777777777@192.168.10.10>
 Accept: application/sdp
 Content-Disposition: session;handling=required
 Content-Length: 0

The screenshot shows the Cisco Collaboration Solutions Analyzer interface. On the left, under 'SIP Profile Rules', there are three rules: rule 100 (Add Diversion), rule 200 (Modify P-Asserted-Identity), and rule 300 (Remove P-Preferred-Identity). On the right, under 'SIP Message To Test Rules On', a sample INVITE message is displayed with various headers and body text. At the bottom, there are 'New Test' and 'Run Test' buttons.

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:555555555@192.168.10.10>

Message SIP modifié

MODIFIED (BLUE) - P-Asserted-Identity: "CallerID_Name" <sip:555555555@192.168.10.10>
ADDED (GREEN) - Diversion: <sip:8675309@cisco.com>

The screenshot displays the Cisco Collaboration Solutions Analyzer interface. At the top, it shows the original and modified SIP messages side-by-side. The original message (left) includes headers like 'Via: SIP/2.0/TCP 192.168.10.10:5060', 'From: "CallerID_Name" <sip:123456789@192.168.10.10>', and 'P-Preferred-Identity: "CallerID_Name" <sip:555555555@192.168.10.10>'. The modified message (right) shows the same headers but with changes: 'P-Asserted-Identity: "CallerID_Name" <sip:555555555@192.168.10.10>' and 'Diversion: <sip:8675309@cisco.com>'. Below the messages is a 'Logs' section with a table showing actions performed on the message.

Action	Before	After	Rule
ADD		Diversion: <sip:8675309@cisco.com>	rule 100 request ANY sip-header Diversion Add "Diversion: <sip:8675309@cisco.com>"
MODIFY	P-Asserted-Identity: "CallerID_Name" <sip:444444444@192.168.10.10>	P-Asserted-Identity: "CallerID_Name" <sip:555555555@192.168.10.10>	rule 200 request ANY sip-header P-Asserted-Identity modify "sip:444444444@" "sip:555555555@"
REMOVE	P-Preferred-Identity: "CallerID_Name" <sip:555555555@192.168.10.10>		rule 300 request ANY sip-header P-Preferred-Identity remove

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 Rules required

Load a Prebuilt Rule Set

Please enter the SIP profile rules here. e.g:
rule 1 response 182 sip-header SIP-Statusline modify "182 Queued" "183 Session In Progress"

Input Help: copylist, voice service voip, dial-peer, tenant, or other voice configurations are not required.
Syntax Help: SIP Profile Config Guide, SIP Copylist Config Guide

SIP Message To Test Rules On required

Load a sample SIP Message

Please enter the SIP message to which the add/remove/modify/copy rules should be applied.

Input Help: SIP Request URI or Status Line always required. SIP Headers/SDP Body optional unless testing them. CSEQ required if "method" used in response rule.
Syntax Help: IANA SIP Parameters, IANA SDP Parameters

Peer SIP Message To Copy From optional

Hide Peer Copy Input

Please enter the peer SIP message here to copy values from when using "peer-header" type rules.

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, kpm1
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

SIP Profile Rules required

Load a Prebuilt Rule Set

```
request INVITE peer-header sip to copy "sip:(.*)@u01
request INVITE sip-header SIP-Req-URI modify "sip:(.*)@u01
```

Input Help: copylist, voice service voip, dial-peer, tenant, or other voice configurations are not required.
Syntax Help: SIP Profile Config Guide, SIP Copylist Config Guide

SIP Message To Test Rules On required

Load a sample SIP Message

```
Sent:
INVITE sip:235678@10.16.0.5:5060 SIP/2.0
Via: SIP/2.0/UDP 192.0.2.0:5060;branch=2964647155C
From: "Cisco" <sip:1234@10.16.0.3>;tag=8125CE72-1184
To: <sip:5678@10.16.0.5>
Call-ID: 7835570P-193611EF-AC18962-0503EC10@192.0.2.0
Supported: 100rel,timer,resource-priority,replaces,sdp-annot
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: 1629a6770010500a00009a7fe;remote=00000000000000000000000000000000
Session-Expires: 1800
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 243
```

Input Help: SIP Request URI or Status Line always required. SIP Headers/SDP Body optional unless testing them. CSEQ required if "method" used in response rule.
Syntax Help: IANA SIP Parameters, IANA SDP Parameters

Peer SIP Message To Copy From required

Hide Peer Copy Input

```
Received:
INVITE sip:235678@10.15.0.2:5060 SIP/2.0
Via: SIP/2.0/UDP 10.14.0.1:5060;branch=29646416927456440b-78
From: "Cisco" <sip:1234@10.14.0.1>;tag=456812752-75795649-2062-4ab0-b5c2-6b19710635db-53693198
To: <sip:5678@10.15.0.2>
Call-ID: a9f63508-1f013004-1344e15-1600be@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
Expires: 180
```

Input Help: Regular "copy" rules will use the other SIP Message; not this input.
Input Help: Regular "copy" rules will use the other SIP Message; not this input.

New Test
Run Test

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

Report an issue



Product

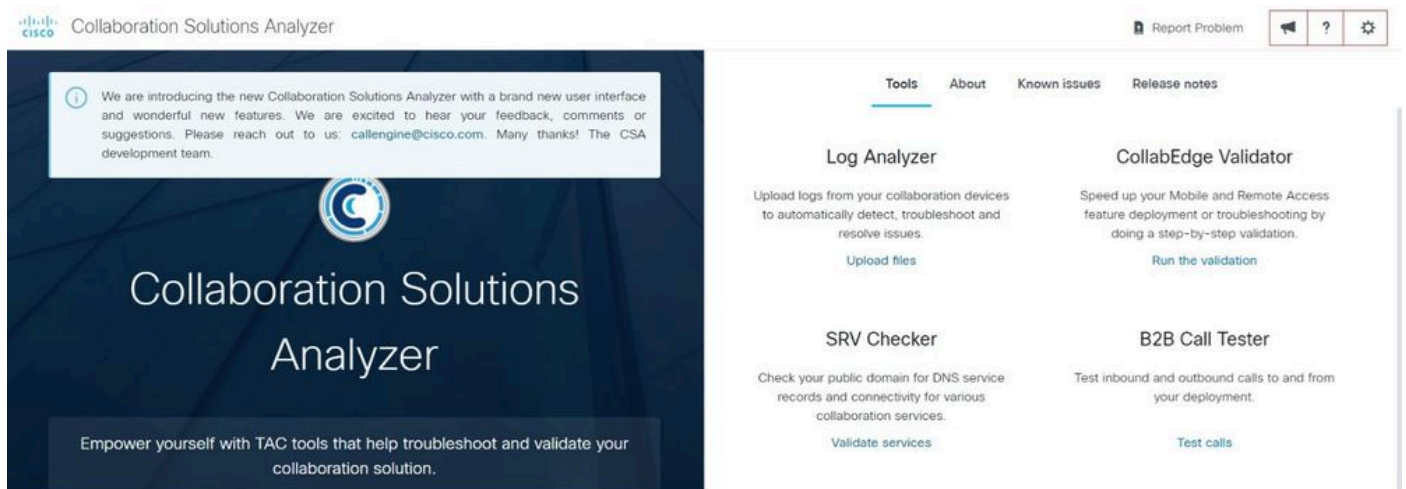
Issue

Details about an issue

Cancel Send

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](#)

Chapitre 1 : Profils SIP

Utilisation des profils SIP sur les exemples d'utilisation CUBE Enterprise

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.