Troubleshoot CUBE via Collaboration Solutions Analyzer

Contents

Introduction

This document describes **Log Analyzer** and **SIP Profile Tester** tools for troubleshooting CUBE using the Collaboration Solutions Analyzer portal.

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Border Element (CUBE) Enterprise.
- Session Initiation Protocol (SIP).
- CUBE log collection (debugging).

Getting started

Collaboration Solutions Analyzer (CSA) is a suite of tools designed to support your collaboration solution throughout its lifecycle. It helps identify issues and provides corrective action plans when needed, assisting in every phase of the collaboration solution.

Navigate to the **Collaboration Solution Analyzer** at https://cway.cisco.com/csa-new/#/home

---

Note: Using the **Chrome browser** ensures that the tool functions optimally.

Considerations

The tools are designed for a CUBE device that handles SIP-to-SIP calls. Any other voice protocol is not supported by the tools.

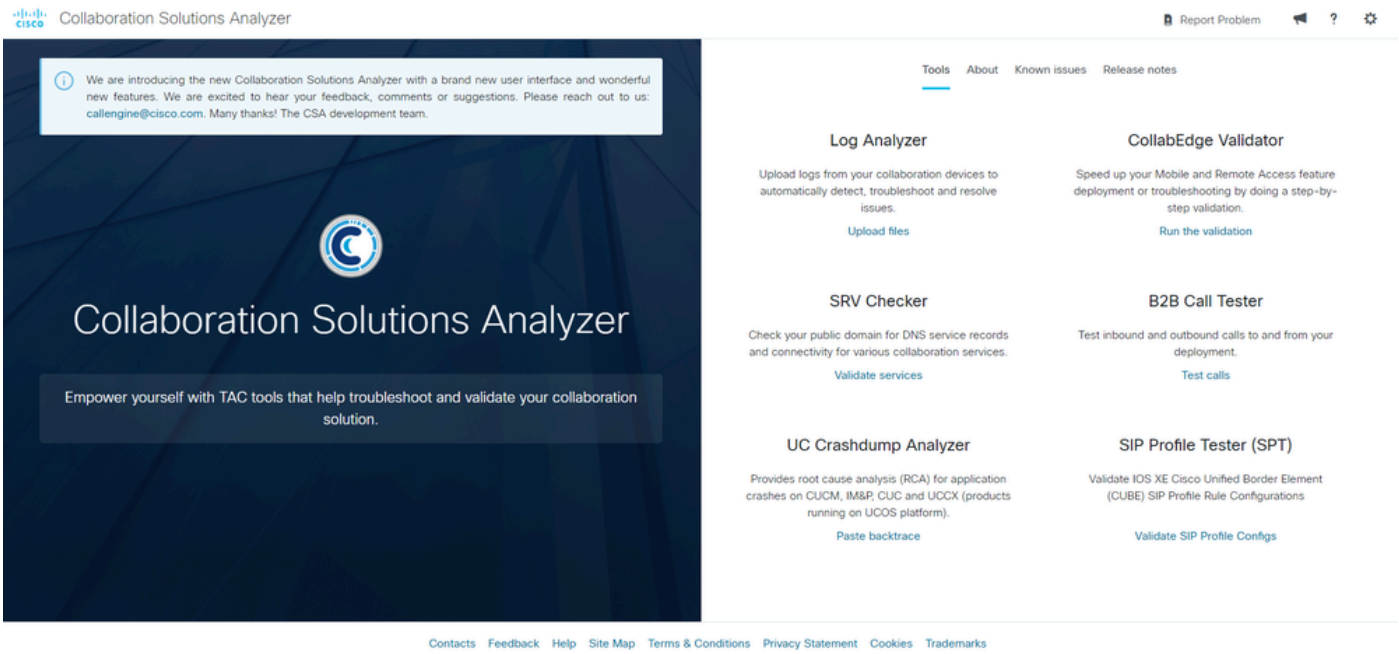
Log Analyzer uses CUBE logs (based on SIP message debugging) for parsing.

If you need help with another voice protocol, please utilize **Cisco Support Assistant** for TAC engagements at https://supportassistant.cisco.com

Platform Description

The **CSA** platform provides these CUBE tools:

- **Log Analyzer** - Upload logs from CUBE and other collaboration devices to automatically detect, troubleshoot and resolve issues.
- **SIP Profile Tester** - Validate SIP Profile Configuration.



CSA Home

Log Analyzer

The **Log Analyzer** tool enables administrators to examine the call signaling handled by the CUBE device. It offers a comprehensive analysis of log files, including:

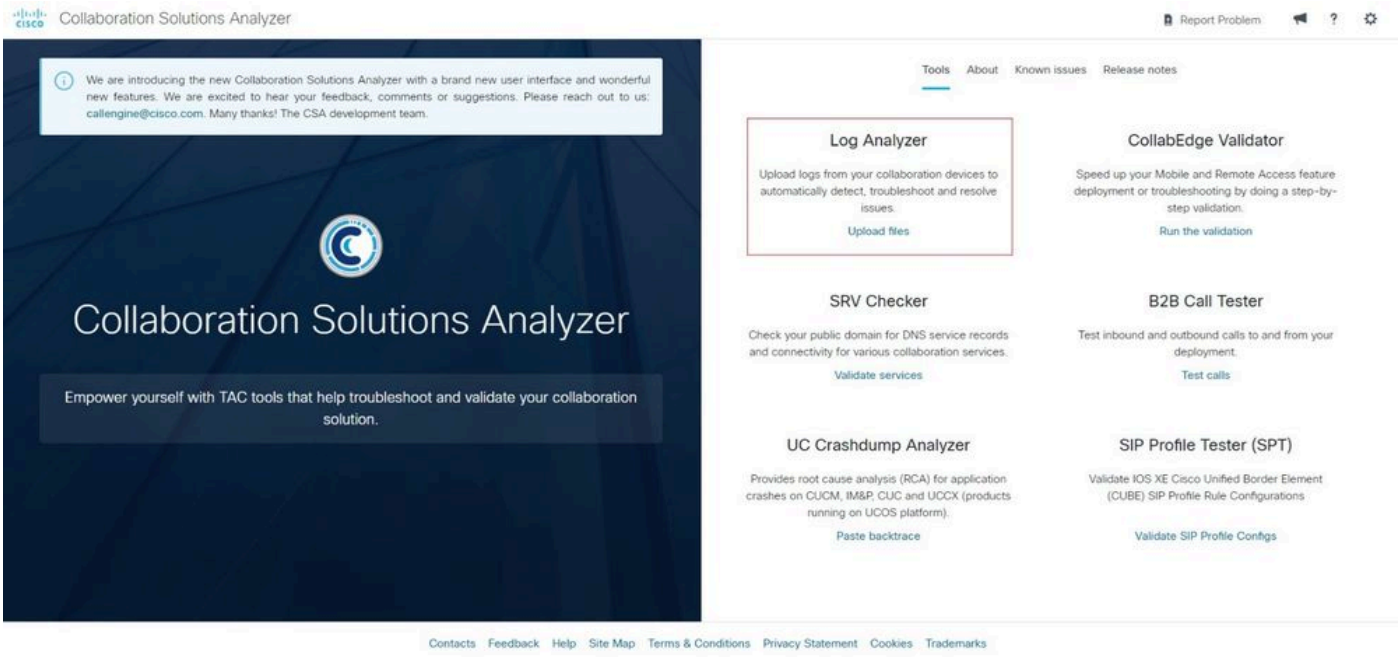
- **Call leg info**
- **Ladder Diagram**
- **Signaling**

Note: CUBE debugging (**debug ccsip messages**) from a call that has been processed by the CUBE must first be collected and stored in a text file. Only SIP debug and no other output, such as show commands, must be included in this text file.

Upload CUBE log files

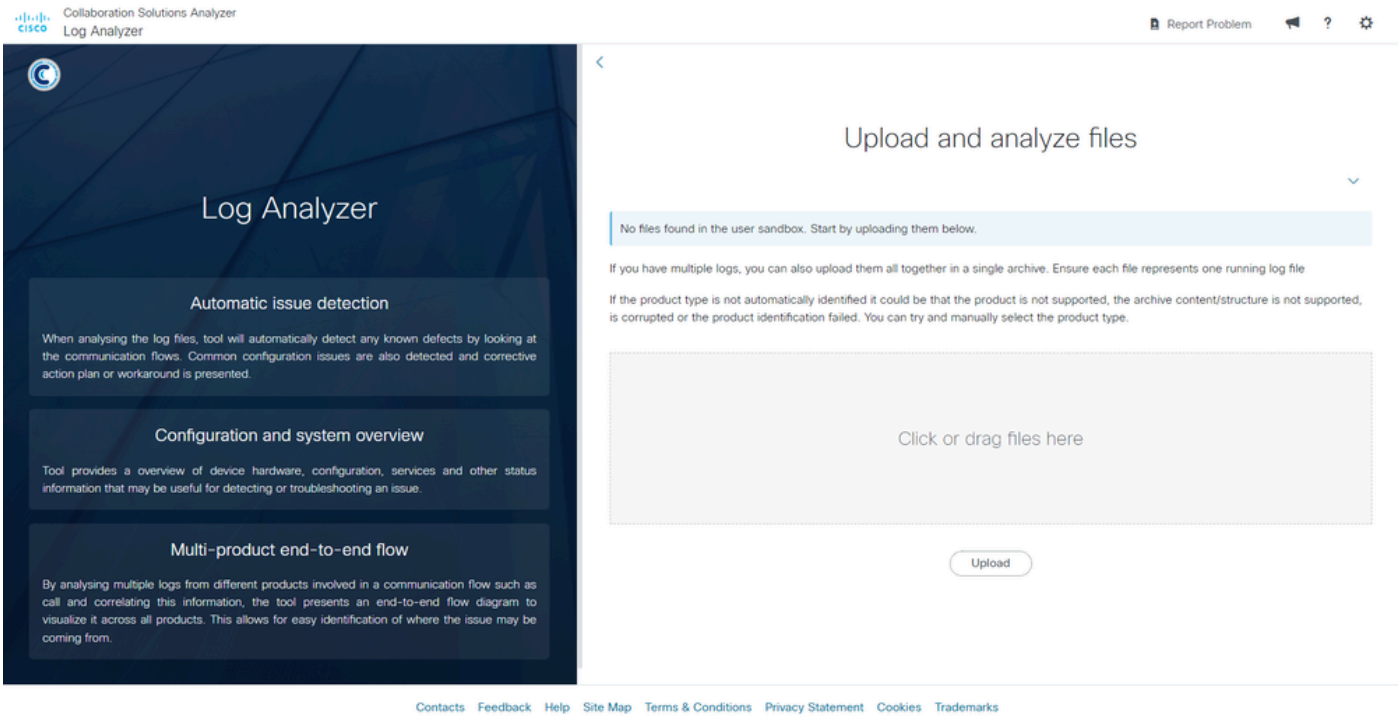
Navigate to the **Collaboration Solution Analyzer** at https://cway.cisco.com/csa-new/#/home

Then select the tool by clicking on **Upload files** in the **Log Analyzer** section.



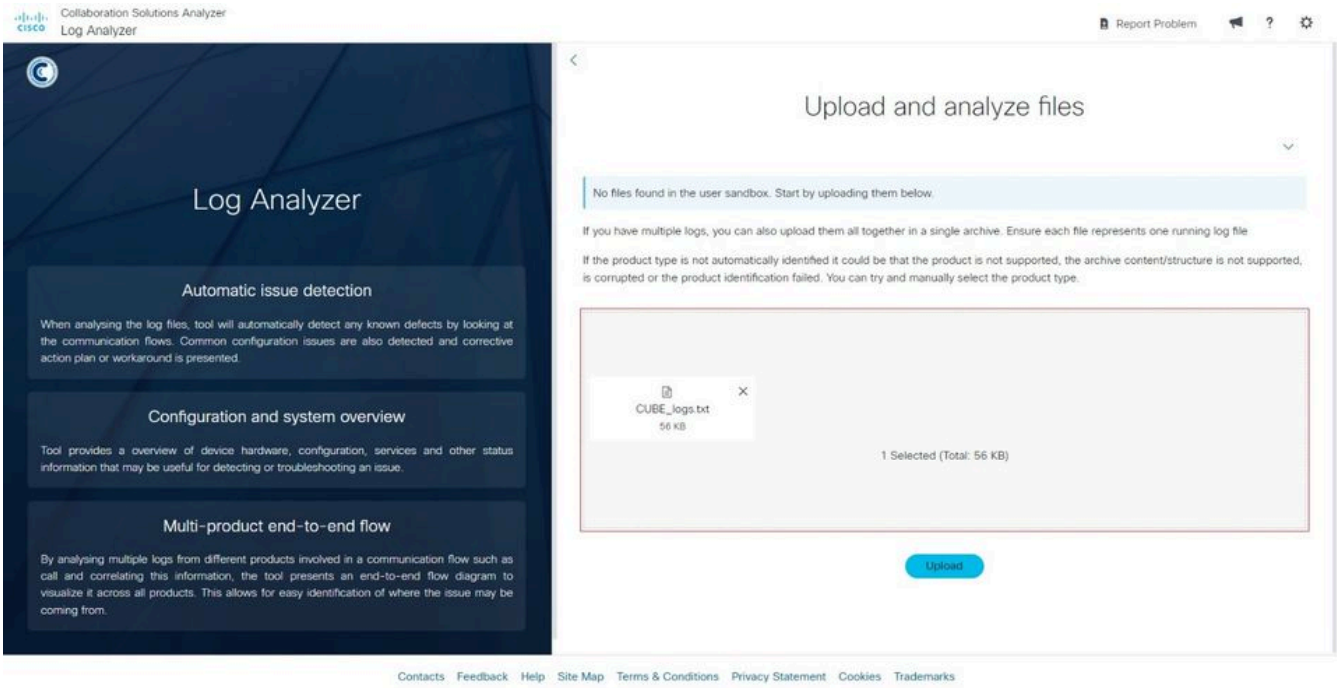
Log Analyzer Home

The platform displays the tool screen where a file can be selected or dragged.



Log Analyzer Upload

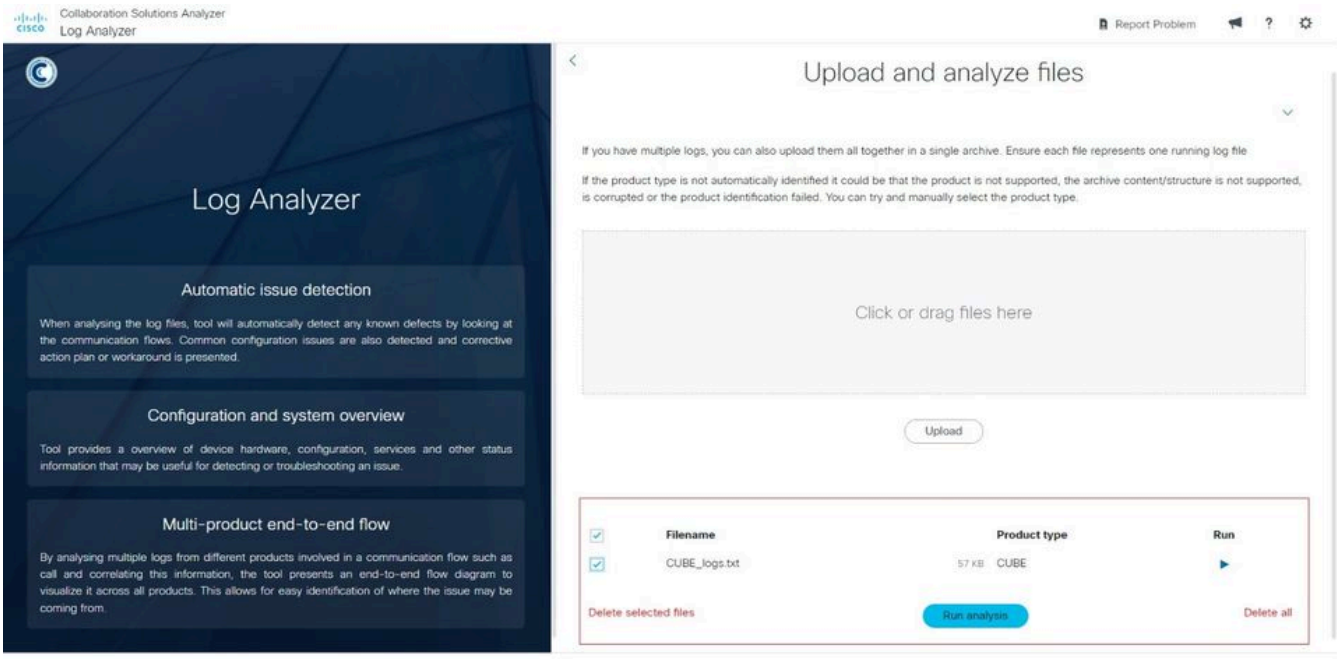
To complete the process of uploading the file for the tool to analyze, click on the **Upload** button.



Log Analyzer Upload File

After uploading the file to the tool, select the file(s) you want to analyze by checking the corresponding box, then click on the **Run Analysis** button.

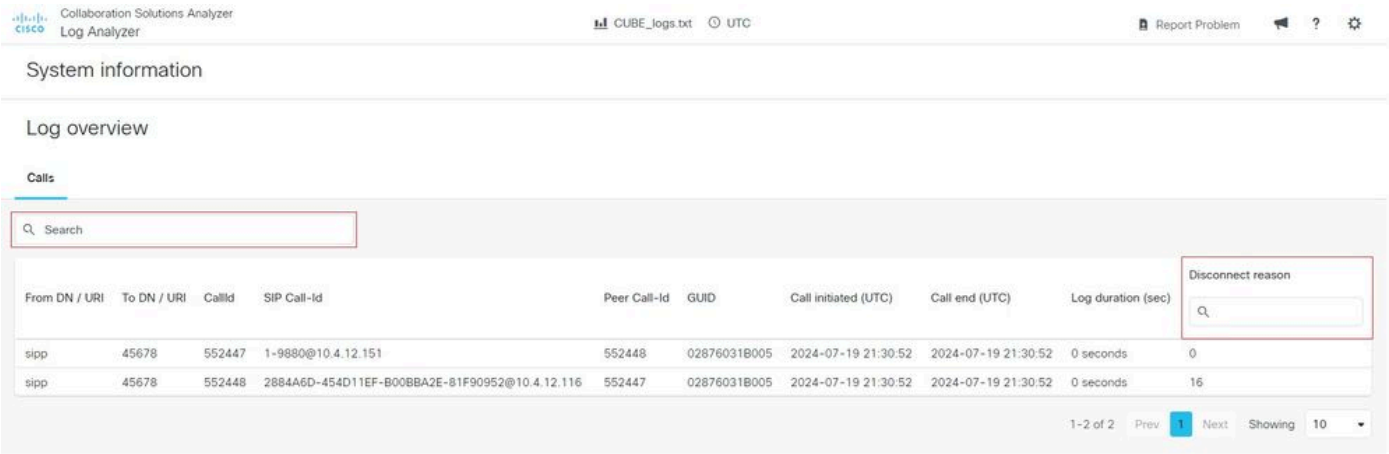
- The system sets the **Product Type** to CUBE.
- More than one file can be analyzed in the same session.



Log Analyzer Product Type

The tool analyzes all the signaling calls captured in the text file and display a summary of the identified call legs. You can then apply two filters:

- **Search** - Filter call sessions by specific data, such as dialed numbers.
- **Search by 'Disconnect Reason** - Filter call sessions based on the reason for call disconnection.



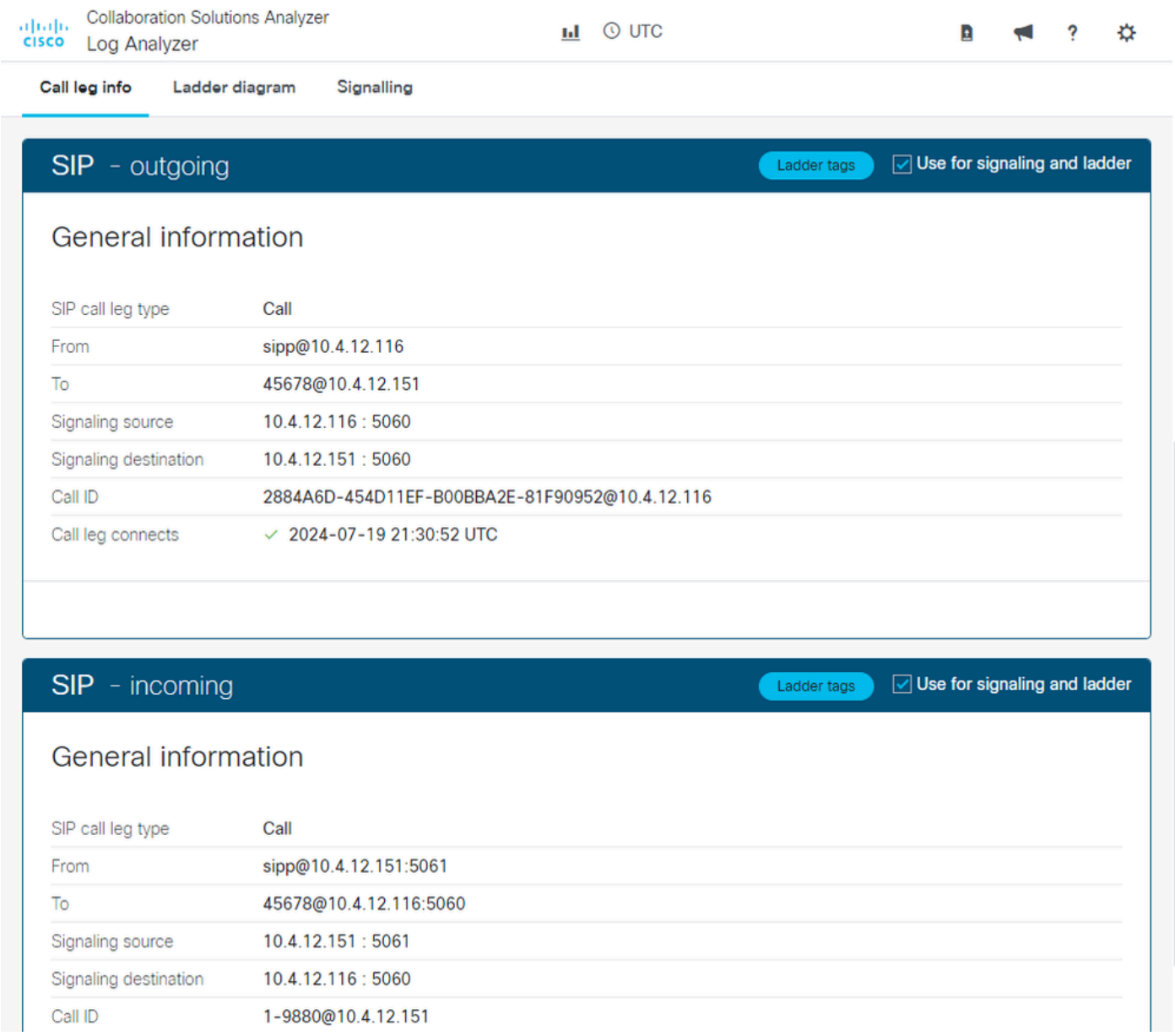
Log Analyzer Call Filter

To continue with the detailed analysis, select the call session line you want to focus on, and the tool displays the full analysis showing the **Call Leg Information**, **Ladder Diagram** and **Signaling**.

Call Leg Information

The first stage presents the **Call Leg Information**, which displays the overview of the call:

- **SIP call leg type**
- **From** – Obtained from the FROM SIP header of the INVITE message.
- **To** – Obtained from the TO SIP header of the INVITE message.
- **Signaling source** – IP address and port of the source device. Obtained from the VIA SIP header of the INVITE message.
- **Signaling Destination** – IP address and port of destination device. Obtained from the URI SIP header of the INVITE message.
- **Call ID** - Obtained from the SIP CALL-ID header of the INVITE message.
- **Call leg connects** – Call session timestamp.

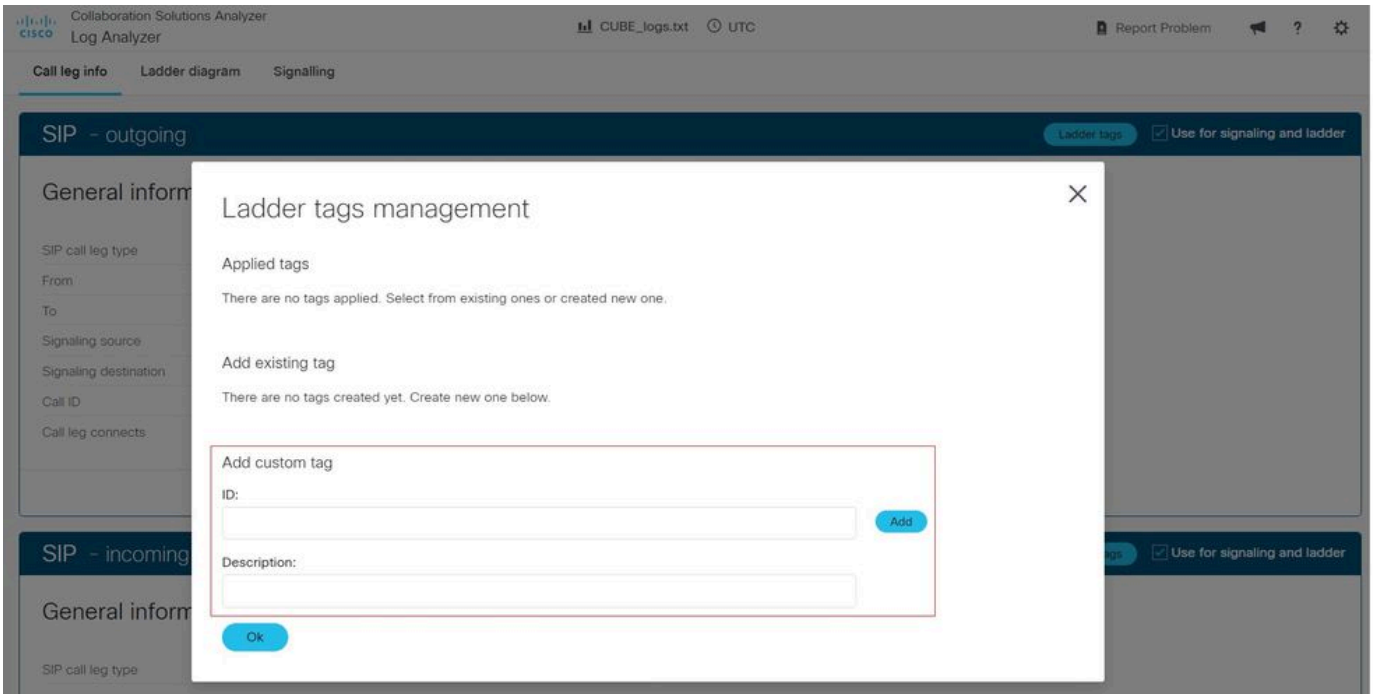


Log Analyzer Call Leg Info

In this section, Ladder tags can be enabled to highlight messages in the **Ladder Diagram**. The application has 2 fields:

- **ID** - Enter the specific parameter you wish to highlight.
- **Description** - Add a description of the parameter.

Click on the **Add** button to complete the process.



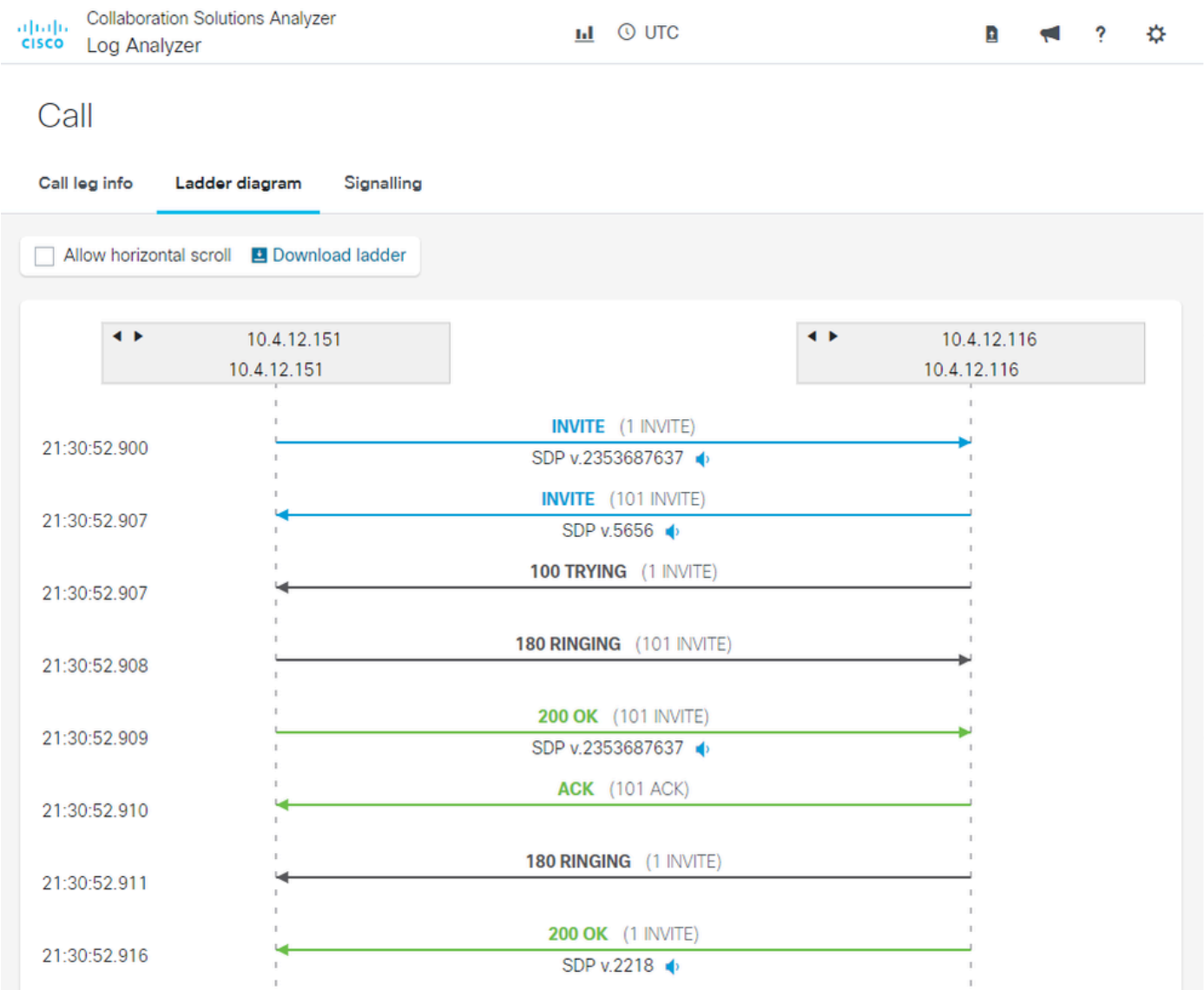
Log Analyzer Ladder Tags

Ladder Diagram

In the second stage, a **Ladder Diagram** is presented, visually depicting the SIP messages exchanged during the call. The messages are **color-coded** for easy identification:

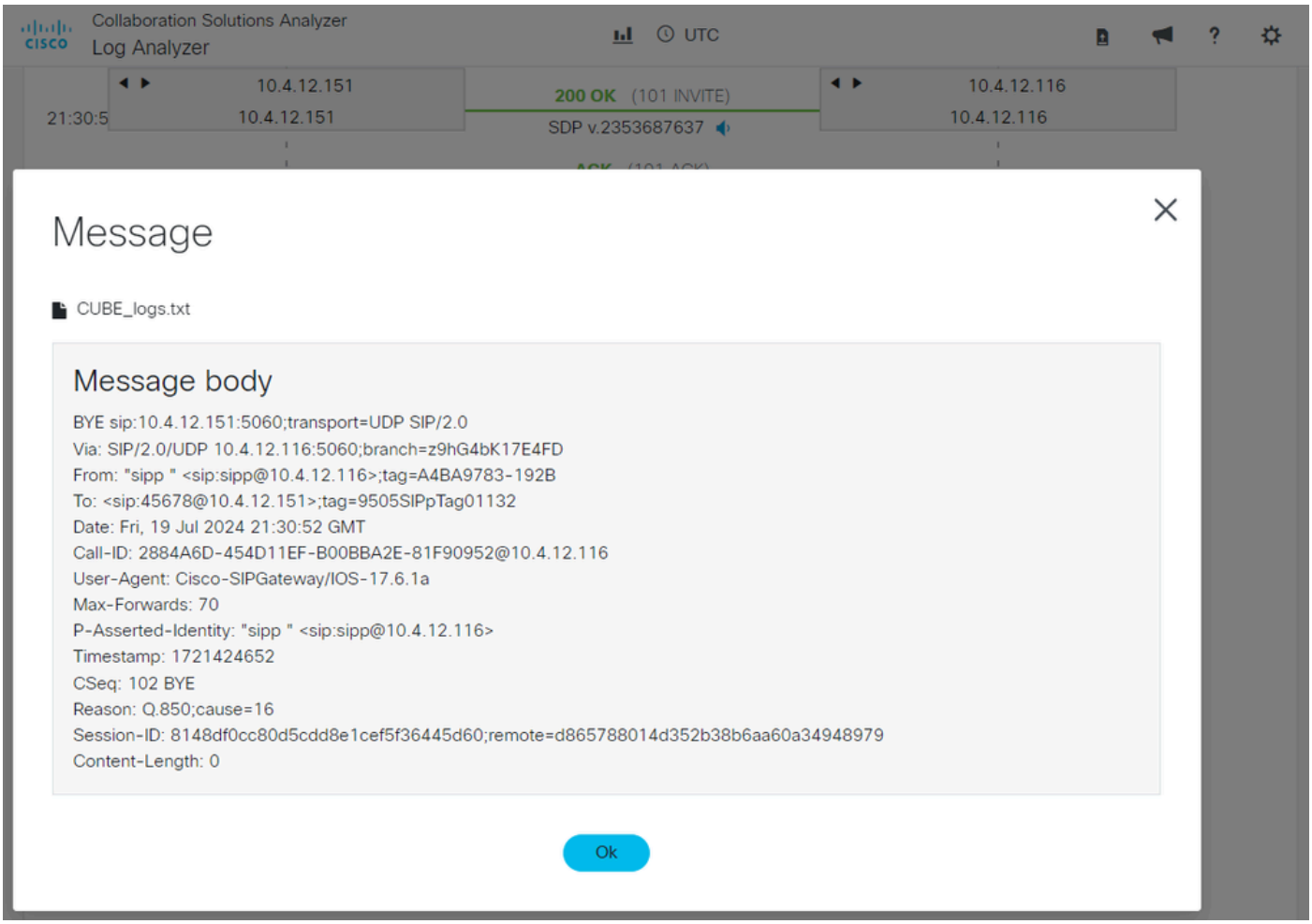
- **Blue color** – SIP INVITE messages.
- **Green color** – SIP 200 OK and ACK messages.
- **Red color** – SIP BYE messages.

To download a copy of the diagram, click on the **Download Ladde**r button. The diagram is downloaded and saved as a **PNG image file**. Please note that this option is only available when using the **Google Chrome browser.**



Log Analyzer Ladder Diagram

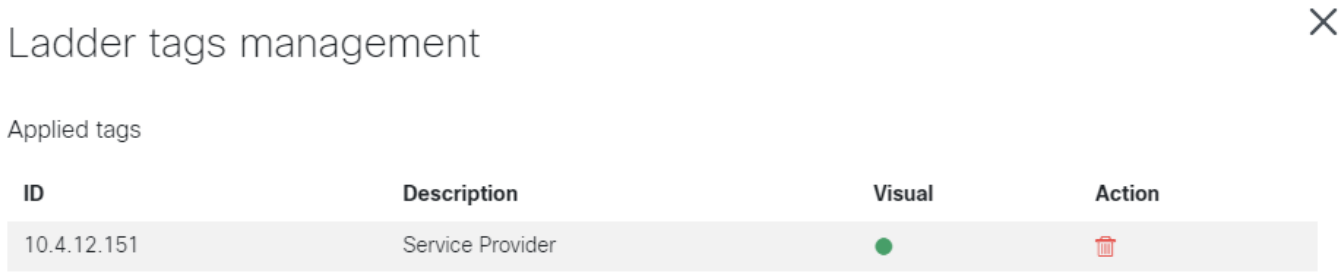
This tool allows the administrator to open SIP messages and view their content. Click on a message to open it.



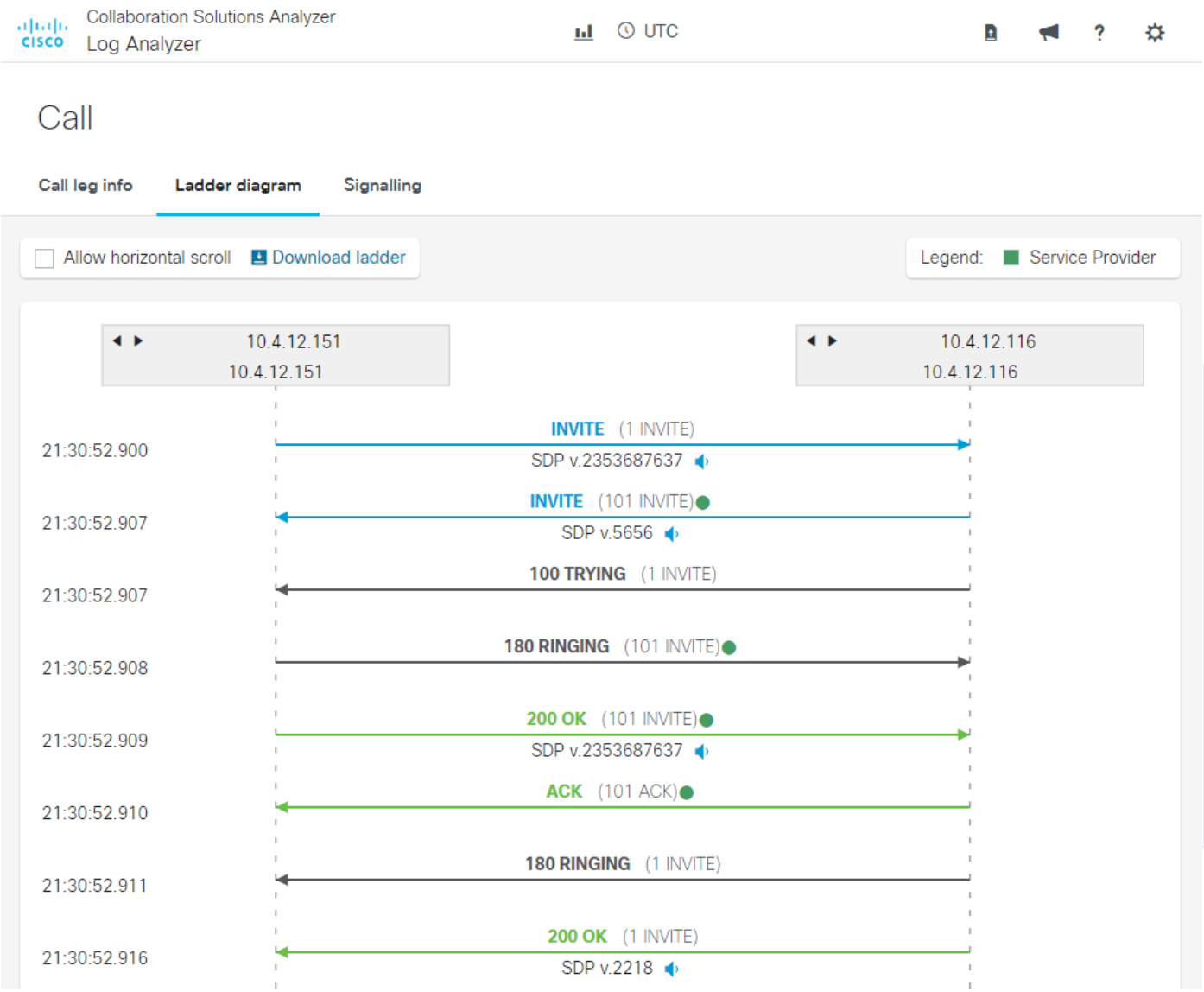
Log Analyzer Ladder Diagram Message

The administrator can add **Ladder Tags** to visualize SIP messages with a distinctive dot mark in the **Call Leg Information** section. Any parameter included in the SIP message can be used for the tag.

In this example an IP address is used for the ID parameter and a description is added. SIP messages containing the IP address are highlighted with a dot mark to distinguish them from other messages.

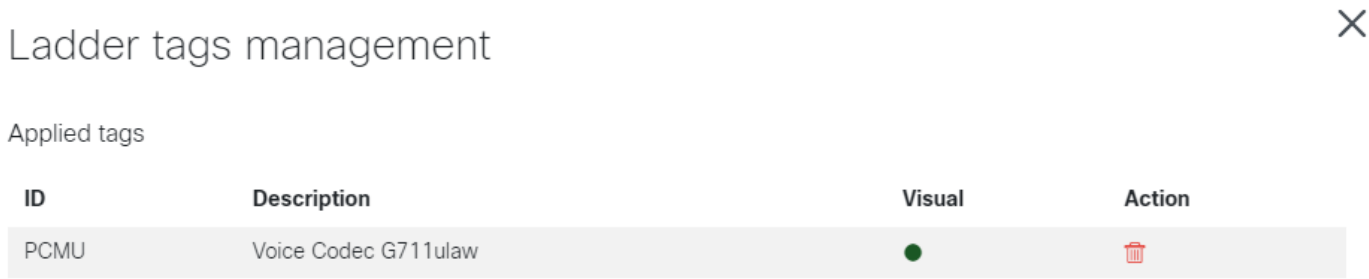


Log Analyzer Ladder Tags 1

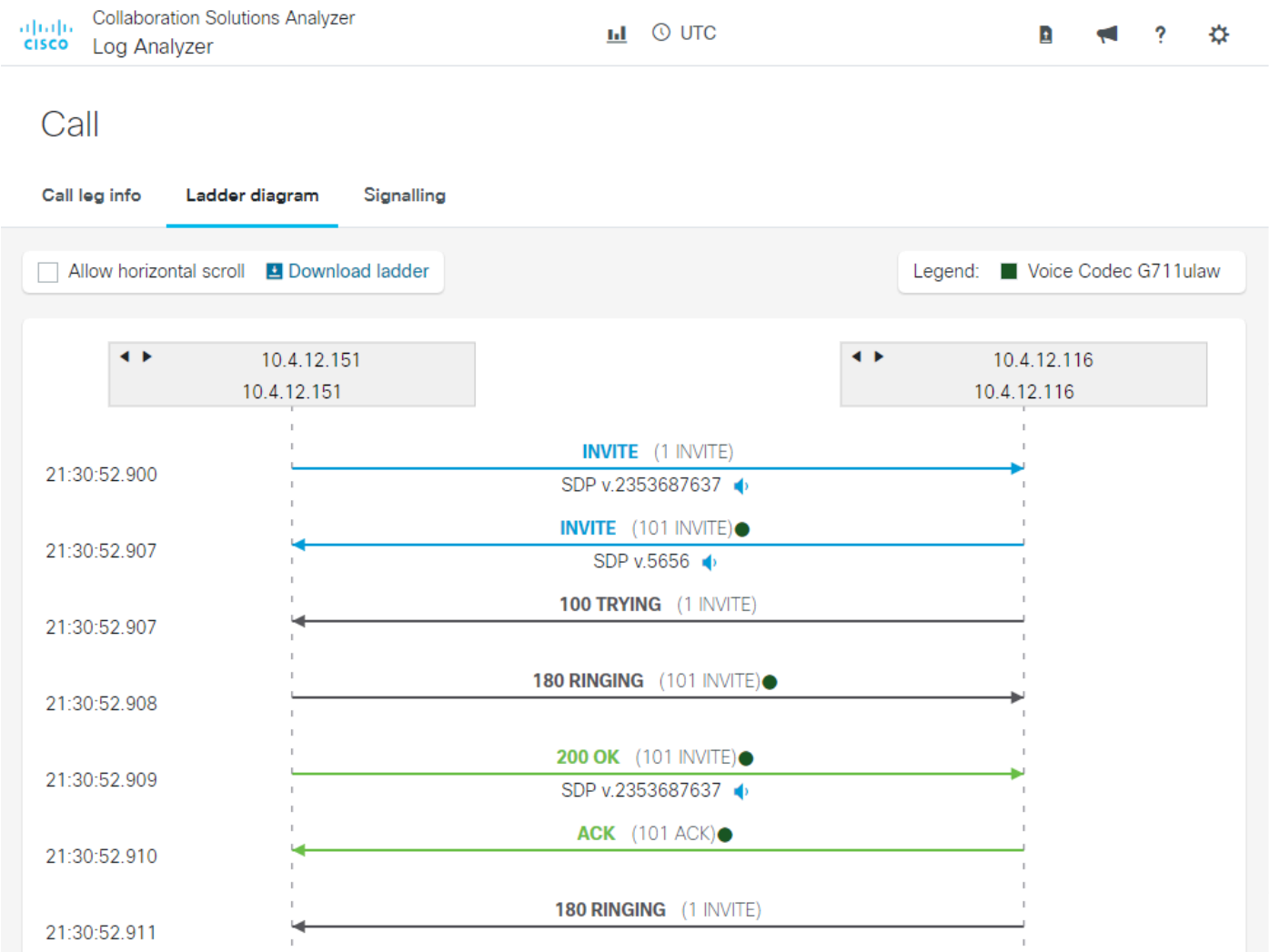


Log Analyzer Ladder Tags 2

Another filter that can be used to distinguish SIP messages from other messages is a voice codec.



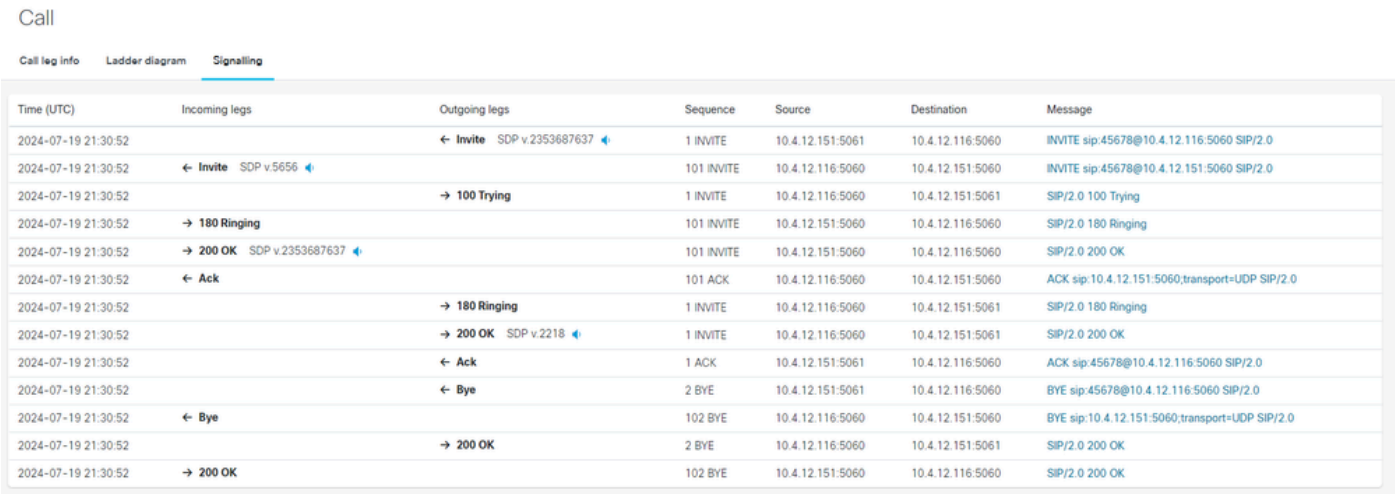
Log Analyzer Ladder Tags 3



Log Analyzer Ladder Tags 4

Signaling

The last stage is the **Signaling**, which displays the SIP messages for both CUBE legs (incoming and outgoing). It contains the source and destination IP addresses. Click to view the 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

Log Analyzer Signaling

Log Analyzer Signaling Message

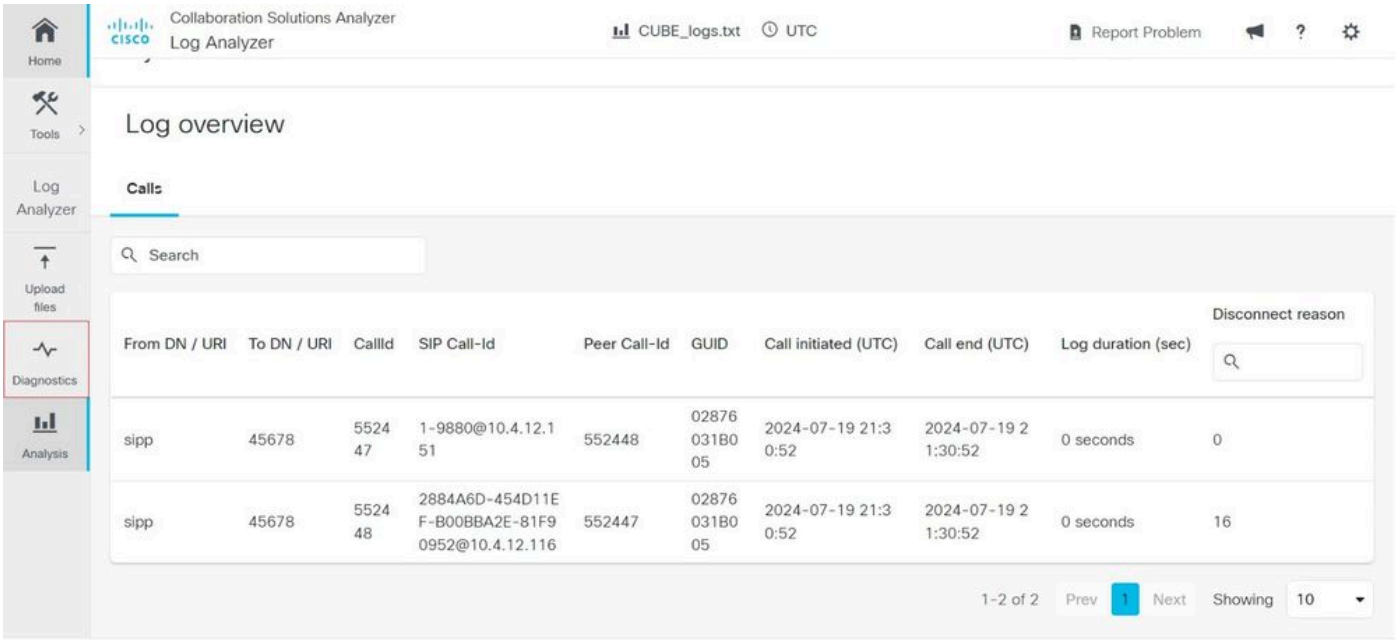
Diagnostics

All data that is parsed from logs is run against **Diagnostic Signatures** that identify known defects, commonly seen issues or misconfigurations and provide a corrective action plan.

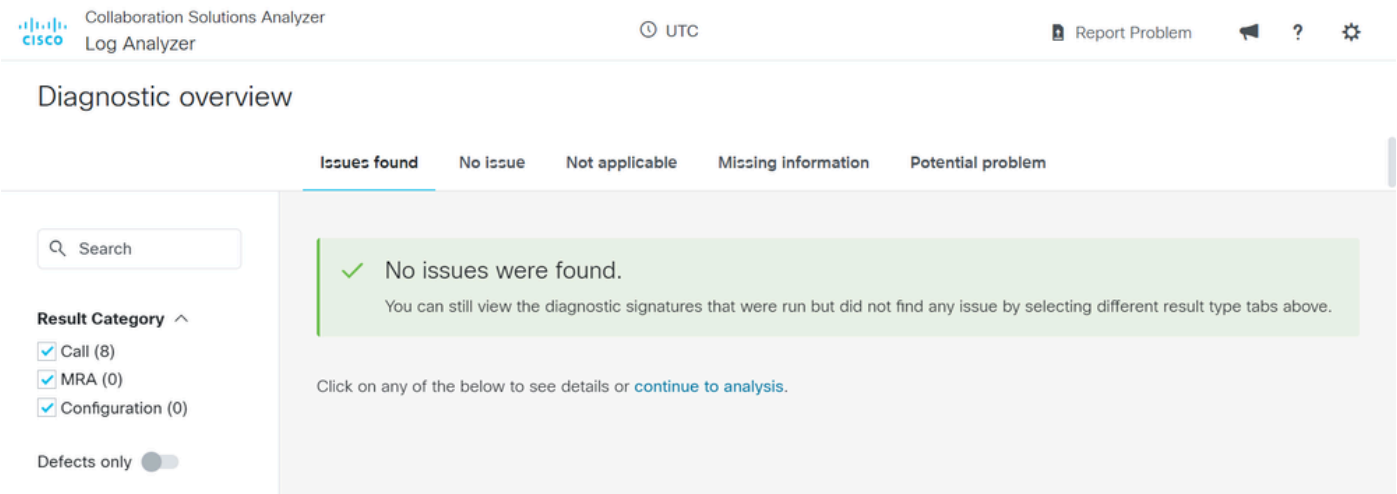
Once a call captured in the logs has been selected to display the call summary analysis, the CSA platform shall display the **Diagnostics** section, which contains this information:

- Issues Found
- Missing Information
- Potential Problem

A toggle button can be activated to filter and display only defects.



Log Analyzer Diagnostics Home



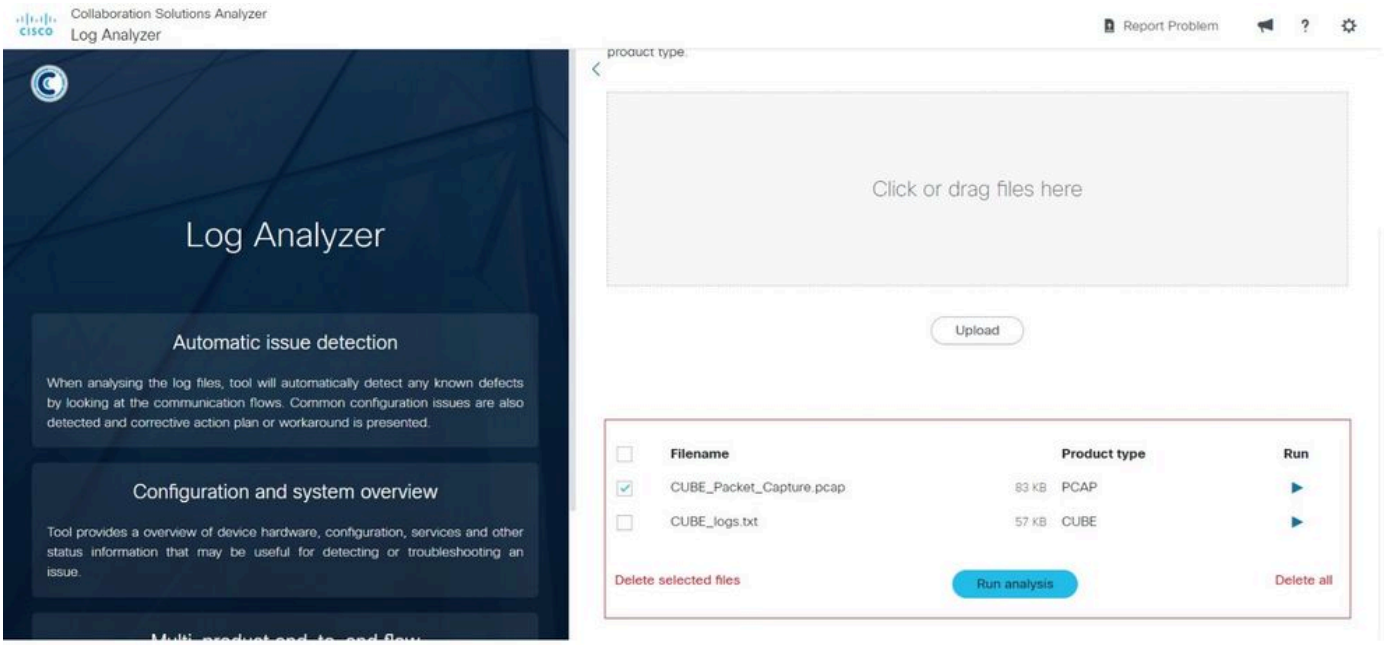
Log Analyzer Diagnostics overview

CUBE Packet Capture

Packet capture is a file buffer created to gather a copy of the actual packets at a CUBE network interface or any voice network device. This file can be open and analyzed by network analyzer software, such as **Wireshark**.

The **Log Analyzer tool** has been enhanced with a Packet Capture analyzer that can process pcap or pcapng file format extensions, providing a summary of session and network statistics collected from calls.

The Packet Capture file must be uploaded to the **Log Analyzer tool** in the same way as the CUBE log file. The system determines the product type as **PCAP**.



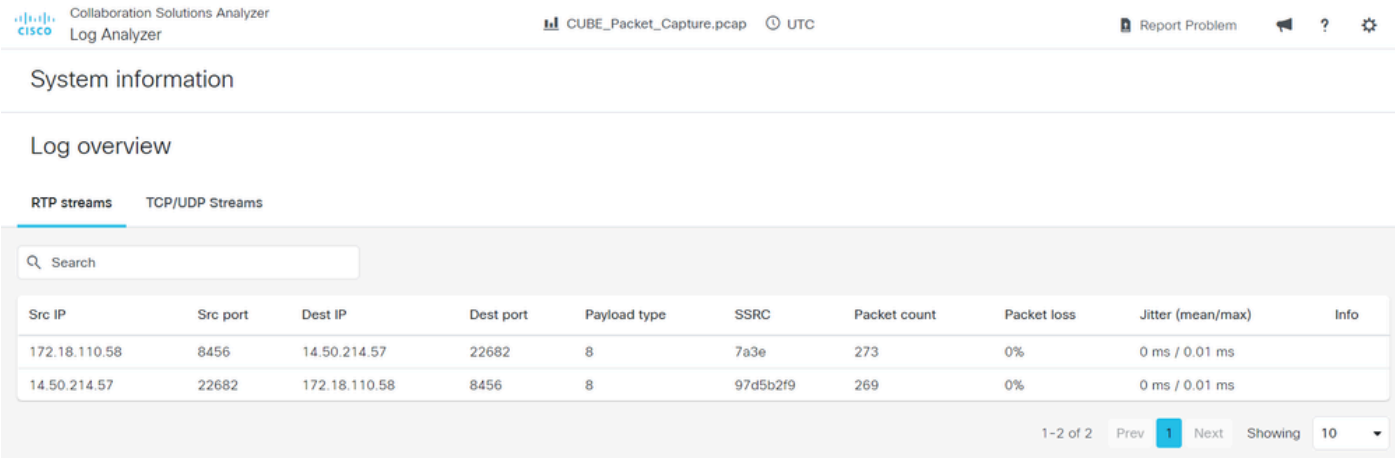
Log Analzyer Packet Capture File

Once the **Run analysis** button is activated, the **Log Analyzer** tool analyzes the information and provides a summary of the captured sessions in two columns:

- RTP streams
- TCP/UDP Streams

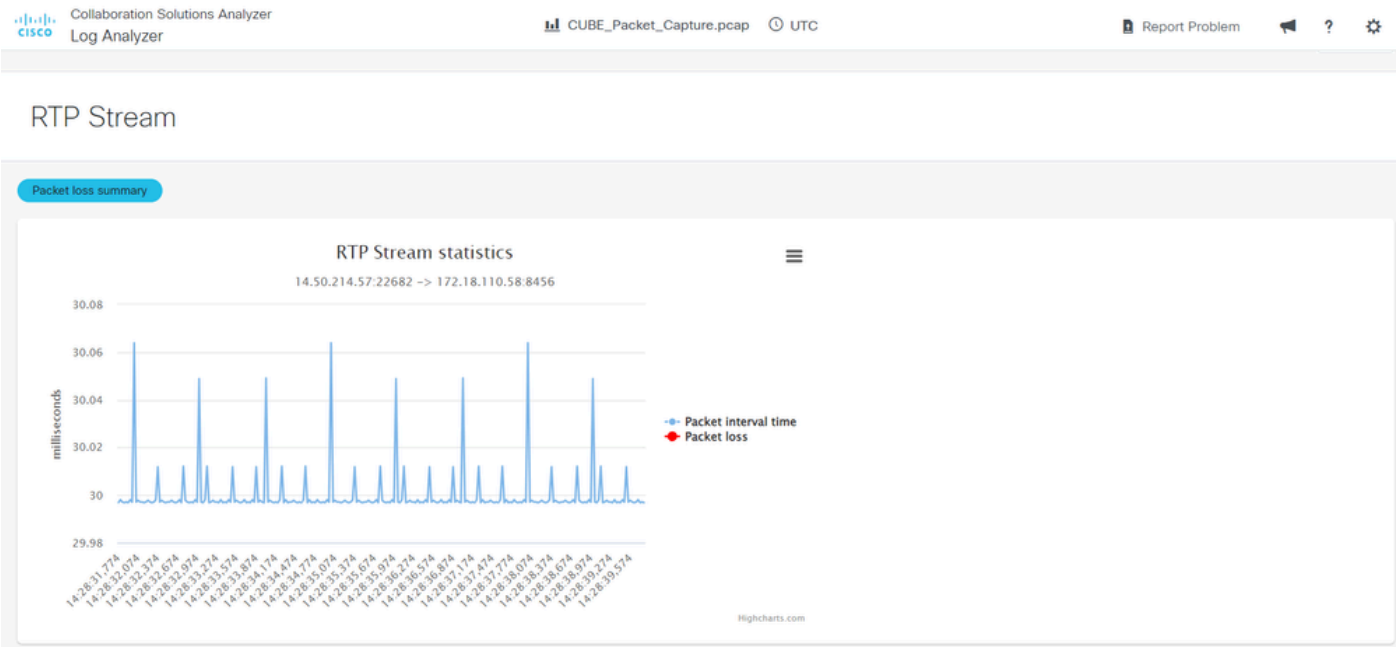
Note: If the packet capture includes SRTP streams, it is shown in the 'RTP streams' column and a network analysis is performed. The audio part of an SRTP stream is not decoded.

Select a session from the RTP streams column and the tool display the RTP stream stats for that connection. If the stream is being affected by the network conditions, the Packet Loss parameter shall be marked with red dots.



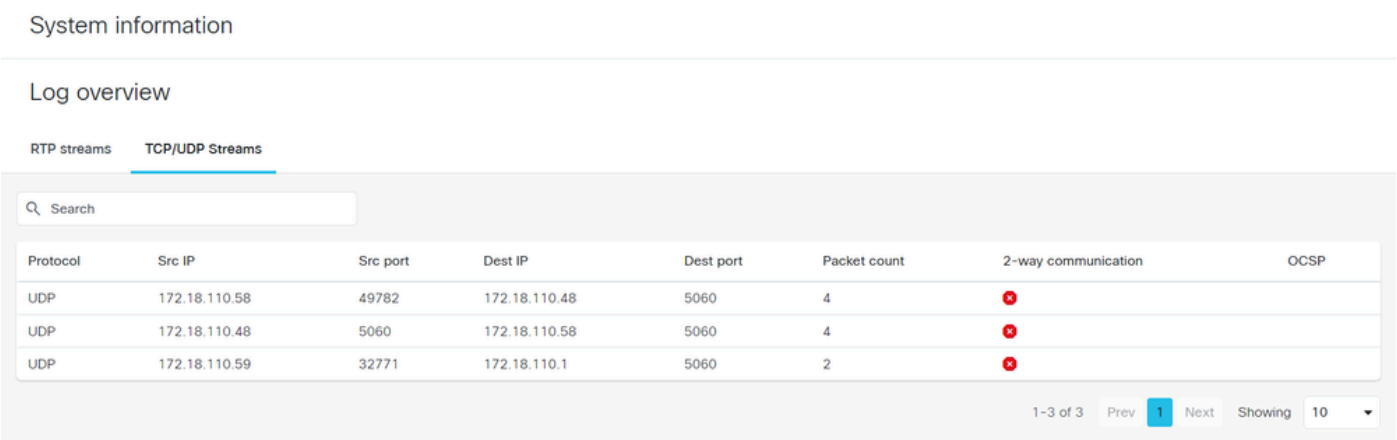
Log Analyzer PCAP analysis

The **RTP Flow Statistics** can be downloaded in a text file format which contains a summary of packet loss. Click on the **Packet Loss Summary** button to download the file.



Log Analyzer PCAP RTP Stream

For TCP/UDP Streams, the system displays the summary of captured sessions.



Log Analyzer PCAP TCP UDP Streams

SIP Profile Tester (SPT)

Session Initiation Protocol (SIP) profiles are used to modify incoming or outgoing SIP messages to ensure compatibility between different devices. The 'SIP Profile Tester' tool allows you to validate your configuration before deploying it in a live environment.

The SIP Profile tool consists of 3 sections:

- **SIP Profile Rules** - Window to insert the SIP PROFILE rules to be tested.
- **SIP Message to Apply Rules** - Window to paste the SIP Message where the rules are to be applied.
- **SIP message to copy from** - (Optional) Window to paste a SIP message in case a copy list configuration is tested. A copy list configuration copies the content of an inbound header received by a device to an outbound header.

The tool contains 2 buttons to manage the tests:

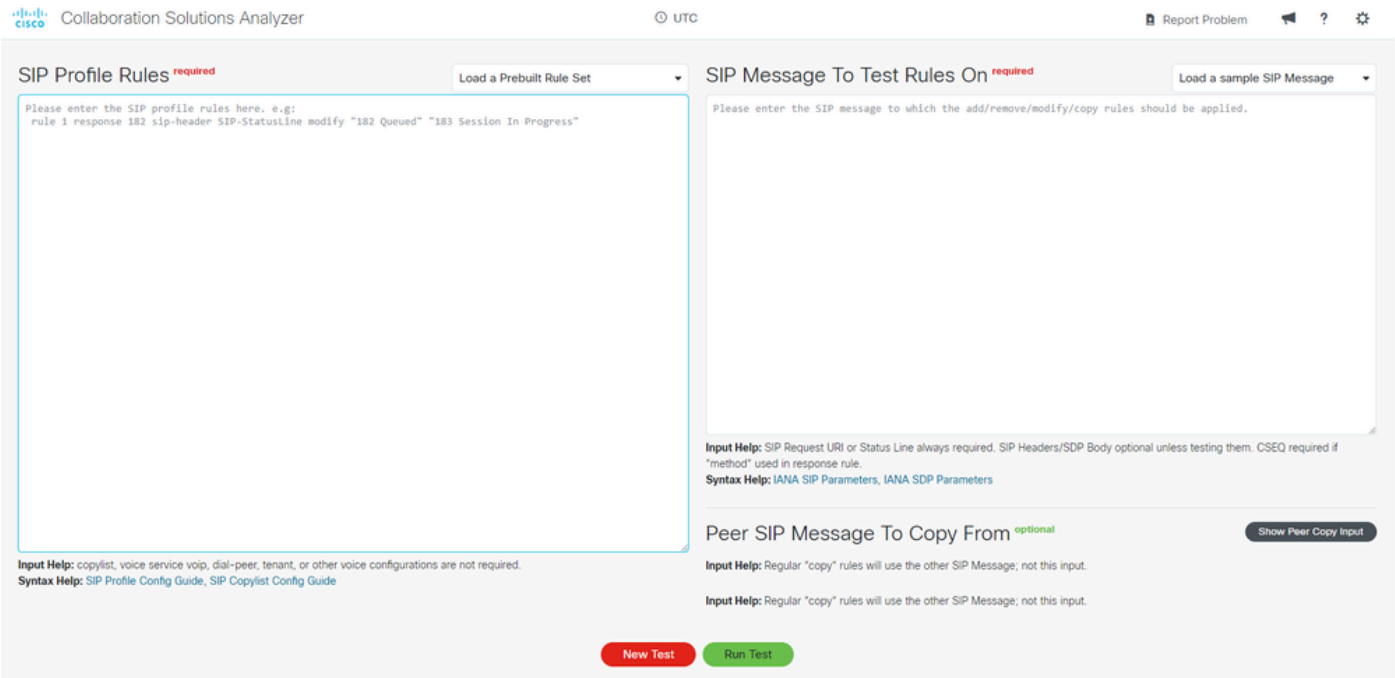
- **Green Button** – To run a test.
- **Red Button** – To reset and clear settings.

After selecting the **Green Button** to run the test, the tool displays these options:

- **Red Button** - New Test
- **Blue Button** - Show Inputs

Highlighting of the Original/Modified SIP Message results:

- **Blue Color** - Modified SIP Headers or SDP Body are highlighted blue in both message areas.
- **Green Color** - Added SIP Headers or SDP Body are highlighted green in the Modified SIP message result only.
- **Red Color** - Removed SIP Headers or SDP Body are highlighted red in the original SIP message result only.



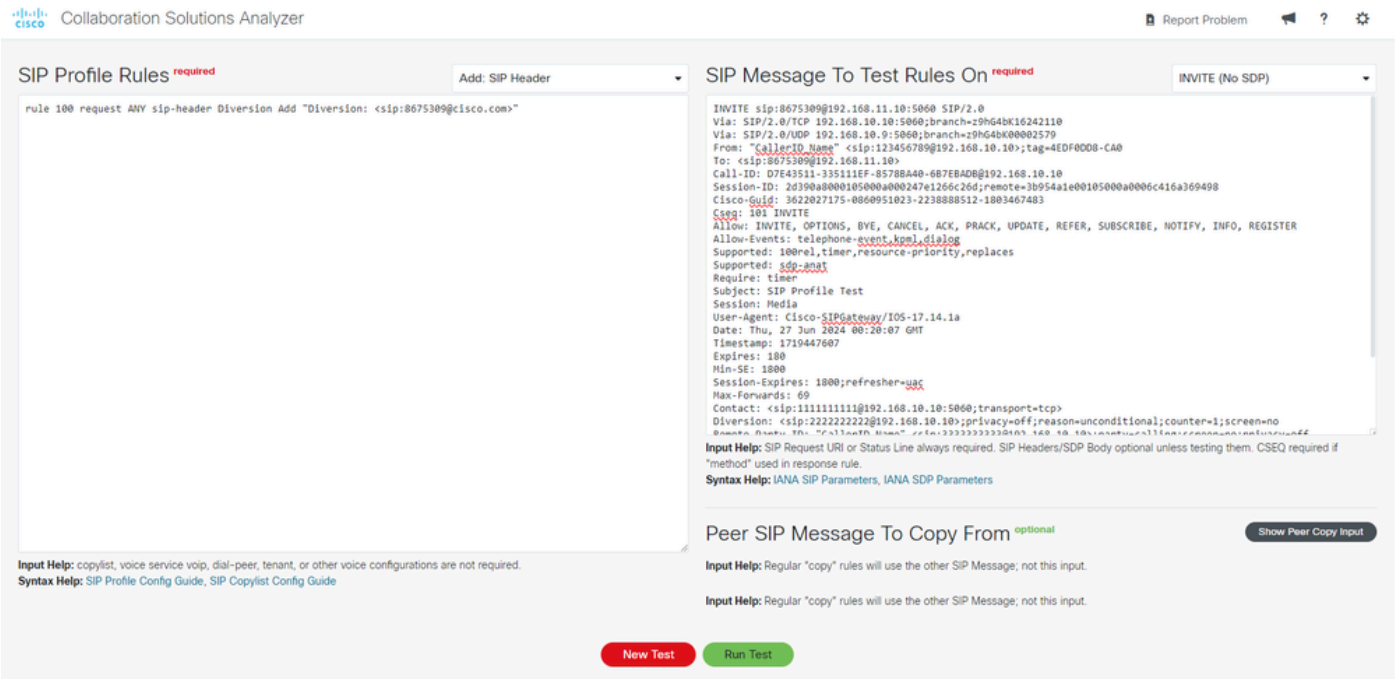
SIP PROFILE Home

Prebuilt SIP Profile Example

The tool provides pre-built examples to simplify testing. At the top of each window, there is an application box for selecting these examples.

Here is how to use a predefined configuration:

1. Click on **Load a Prebuilt Rule Set** and select **Add: SIP Header.**
2. Click on **Load a Sample SIP Message** and select **INVITE (No SDP).**
3. Select the green **Run Test** button to execute the test.

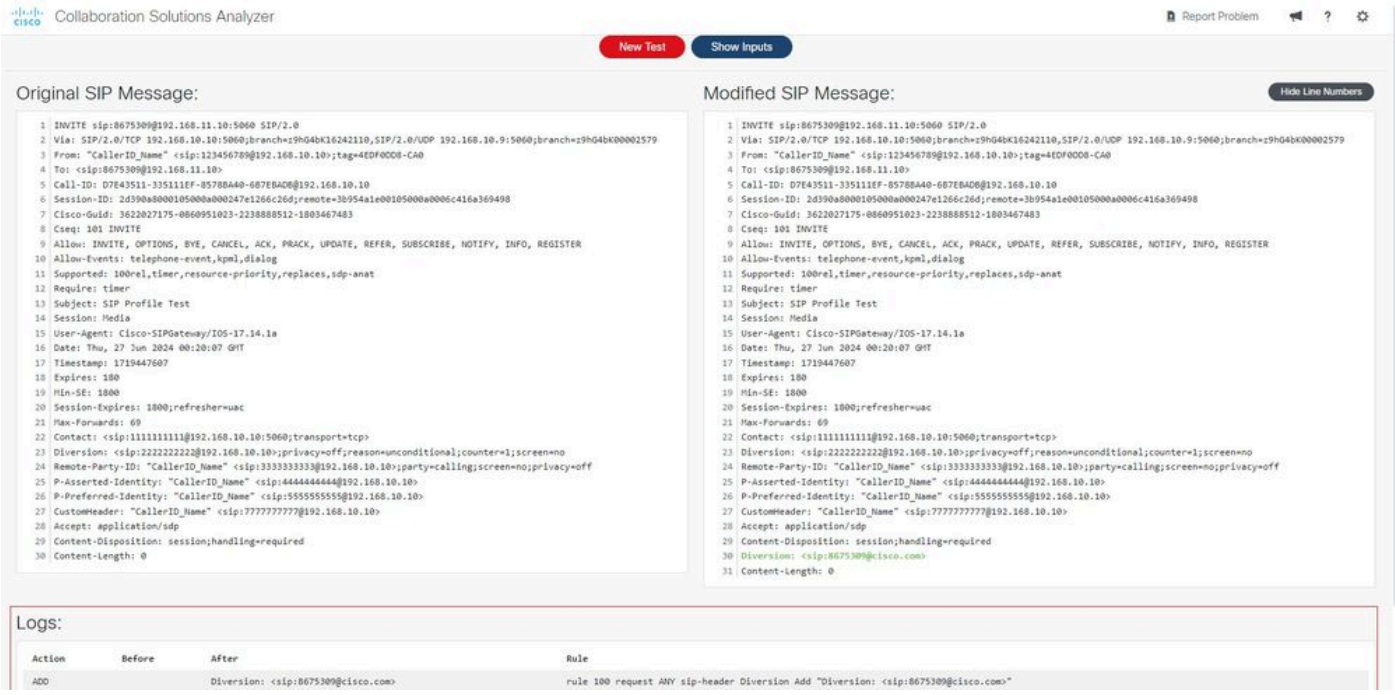


SIP PROFILE Prebuilt

The tool displays a new screen with the results of the test:

Modified SIP message

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



SIP PROFILE Prebuilt Add Example

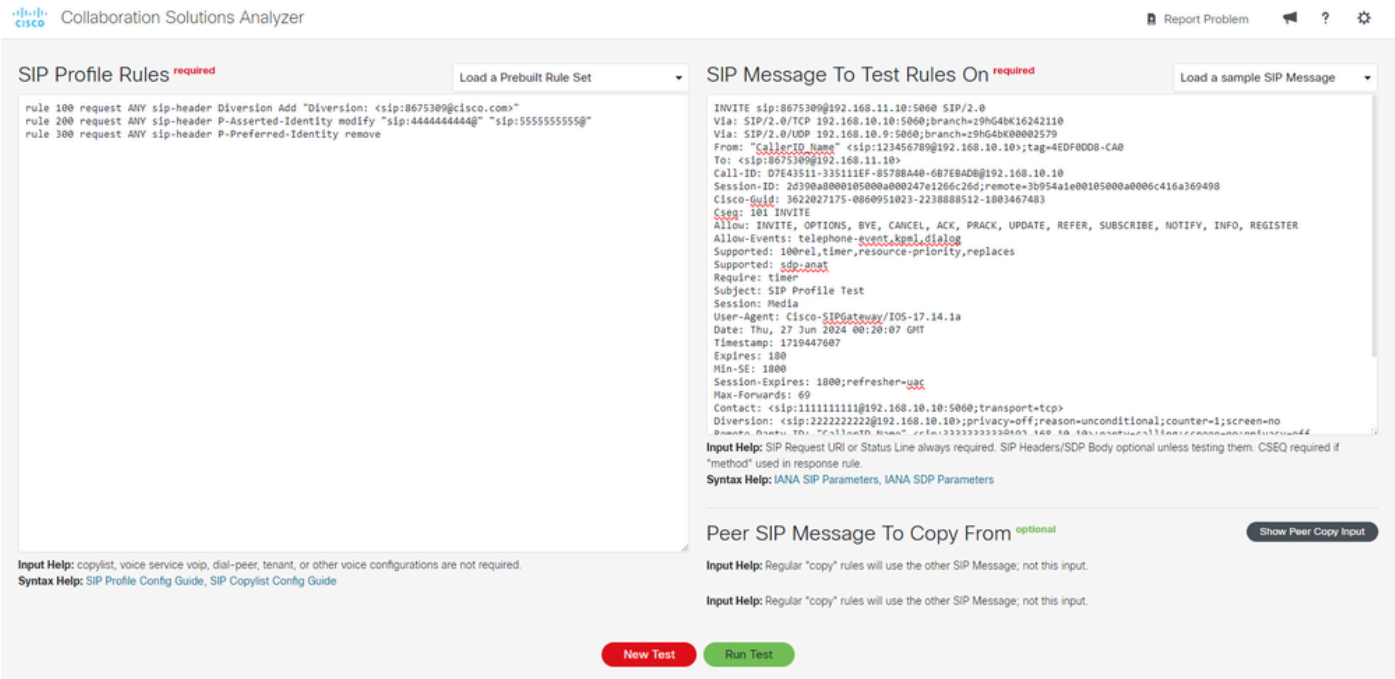
This is an example of the modify/add/remove highlighting:

SIP Profile Rules

```
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
```

Sip Message To Test Rules On

```
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
```



SIP PROFILE Modify Add Remove Example

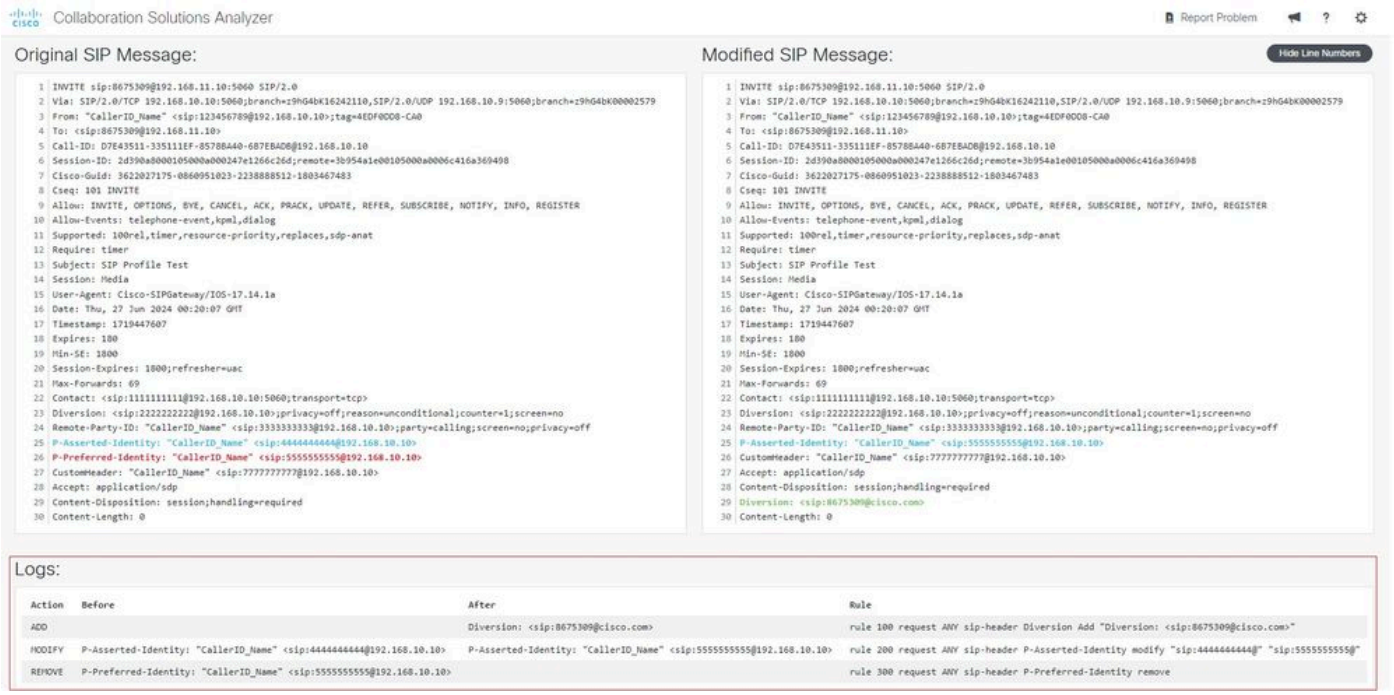
To view the result, click on **Run Test.**

Original SIP message

```
MODIFIED (BLUE) - P-Asserted-Identity: "CallerID_Name" <sip:4444444444@192.168.10.10>
REMOVED (RED) - P-Preferred-Identity: "CallerID_Name" <sip:5555555555@192.168.10.10>
```

Modified SIP message

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



SIP PROFILE Modify Add Remove Example 2

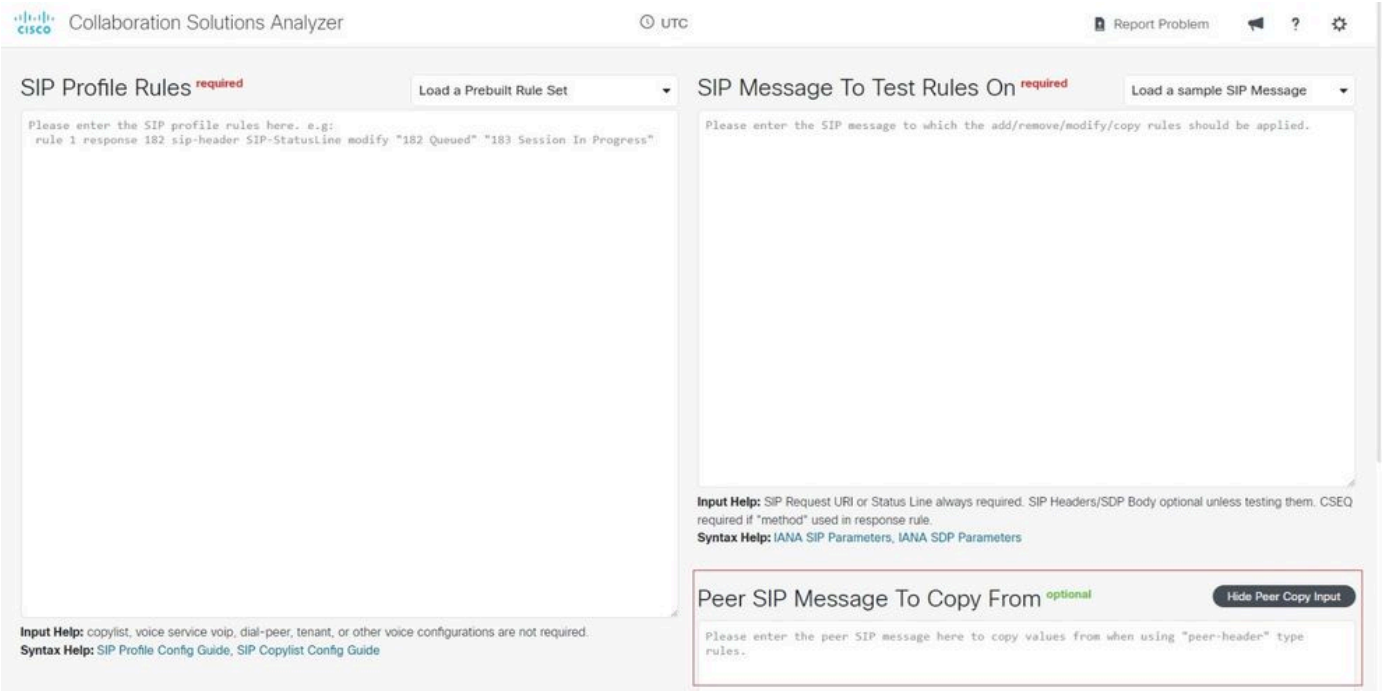
Copylist SIP Profile

For copying content from an incoming header that a device receives to an outgoing header (SIP copylist), these tool inputs can be used:

- Flow Chart: Incoming SIP Message -- > CUBE -- > Modified SIP Message

- Peer SIP Message To Copy From – SIP message to copy from.
- Sip Message To Test Rules On – SIP message to apply rules.

To enable the **Peer SIP Message To Copy From** section, the **Show Peer Copy Input** option must be enabled. You can click on **Hide Peer Copy Input** to hide this section.



This is an example of SIP Rules, Incoming and Modified SIP Messages:

SIP profile rules.

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

SIP message to apply rules.

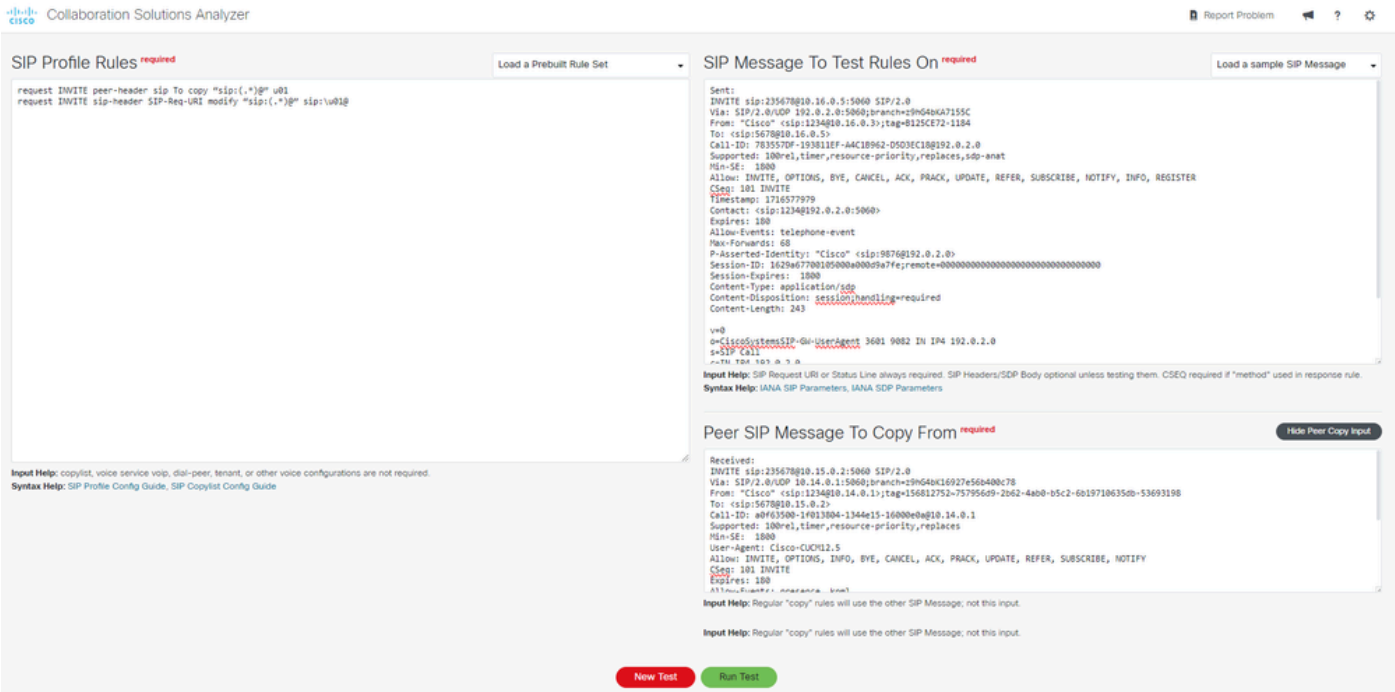
```
Sent:
INVITE sip:235678@10.16.0.5:5060 SIP/2.0
Via: SIP/2.0/UDP 192.0.2.0:5060;branch=z9hG4bKA7155C
From: "Cisco" <sip:1234@10.16.0.3>;tag=B125CE72-1184
To: <sip:5678@10.16.0.5>
Call-ID: 783557DF-193811EF-A4C1B962-D5D3EC18@192.0.2.0
Supported: 100rel,timer,resource-priority,replaces,sdp-anat
Min-SE:  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
```

SIP message to copy from.

```
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
```



SIP PROFILE Copylist Example

Continue by clicking on the **Run Test** button to launch the tool.

Copy Register

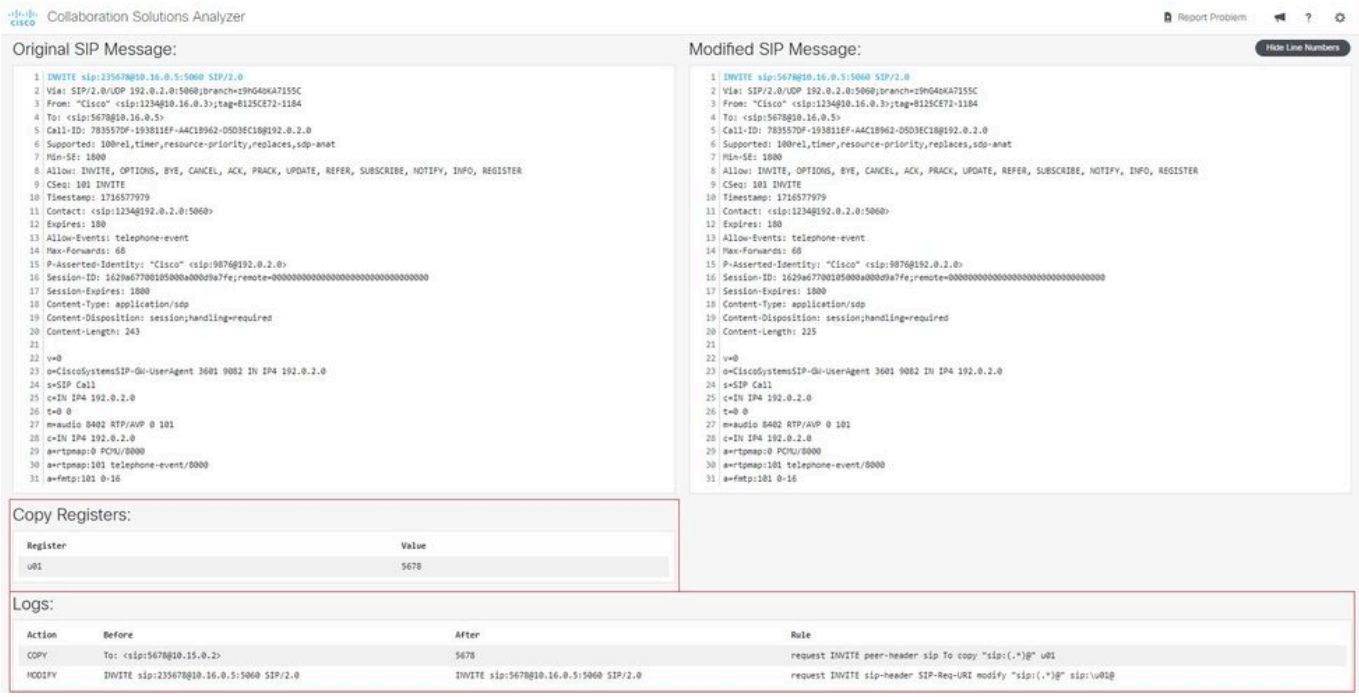
```
Register: u01
Value: 5678
```

Original SIP message

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

Modified SIP message

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

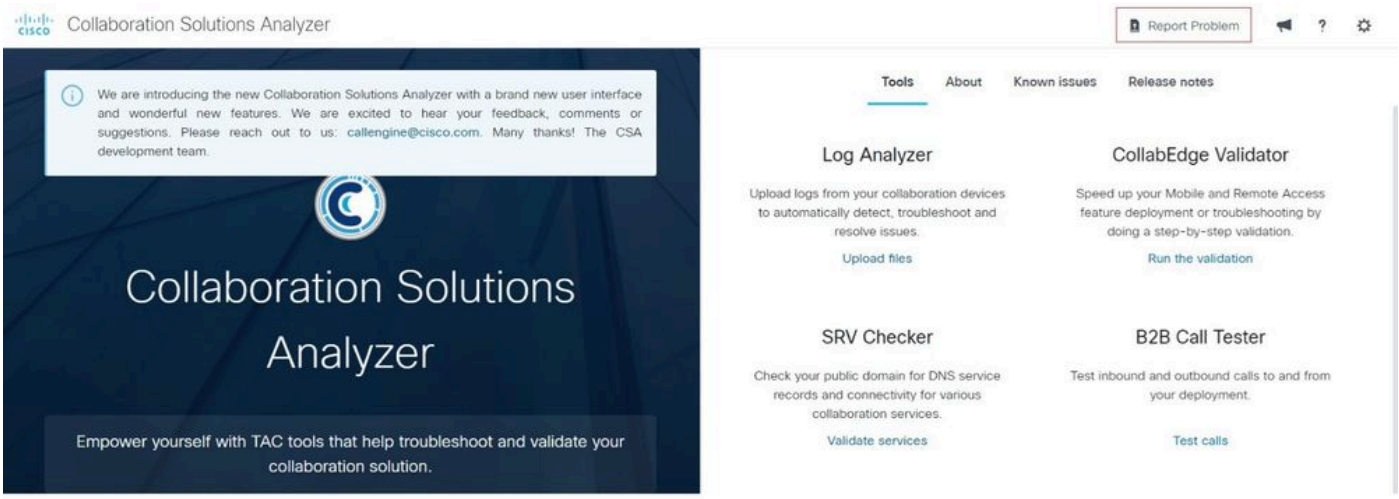


SIP PROFILE Copylist Example 2

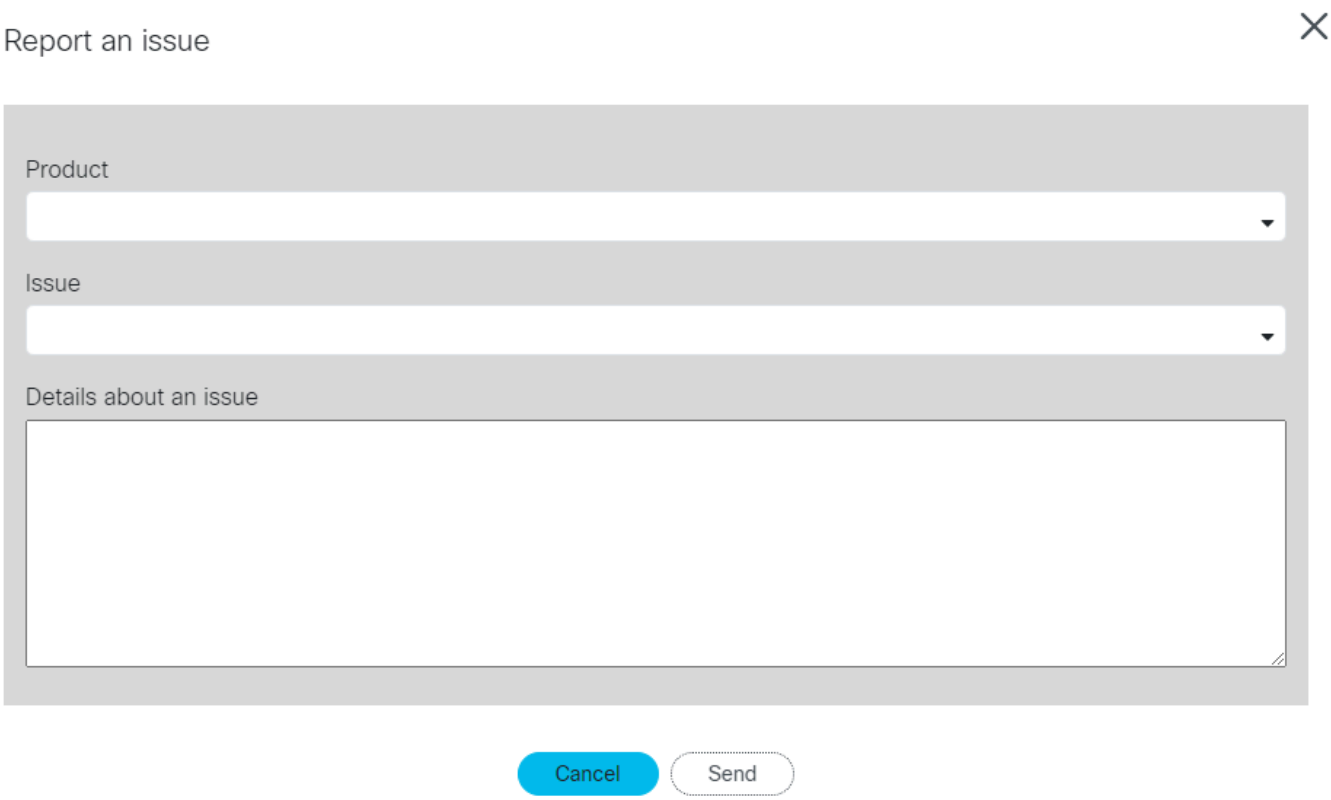
Report A Problem

At the top of the CSA Platform, the **Report A Problem** section allows you to share any issue detected in the tools.

In addition, the administrator can provide feedback, comments or suggestions by sending an email to where the CSA development team processes the information.

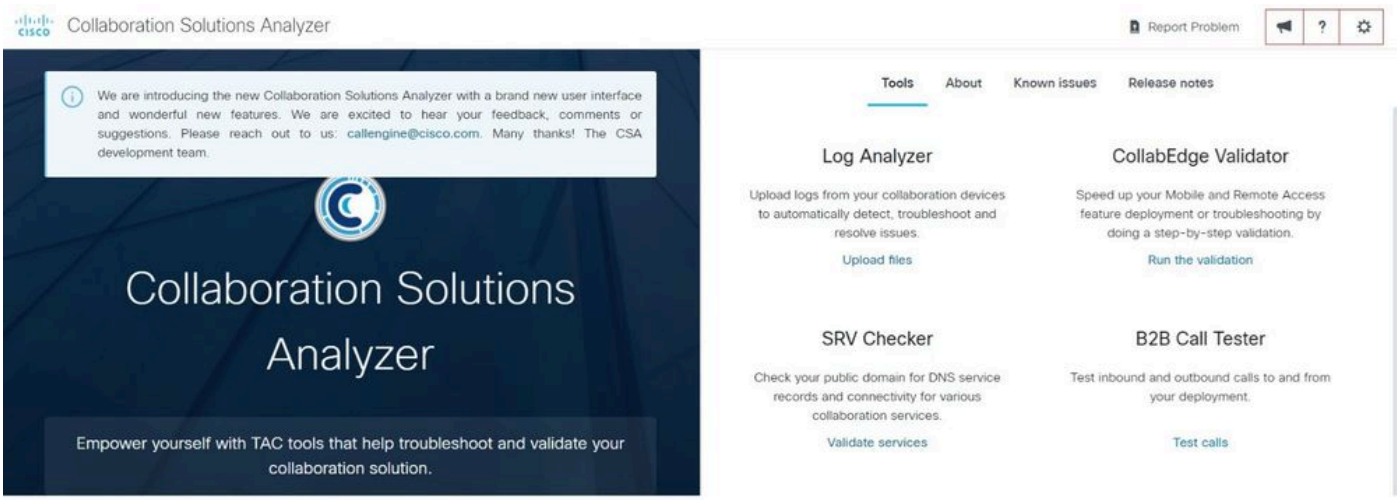


Report Problem Home



Report Issue

Three icons have been enabled to allow the user to Provide Feedback (megaphone icon), review the user documentation (question mark icon) and open user settings (cogwheel icon).



Icons

Support Related Information

[Configure Debug Collection for CUBE and TDM Gateways]

[Cisco Unified Border Element Configuration Guide Through Cisco IOS XE 17.5]

[Chapter: SIP Profiles]

Use SIP Profiles on CUBE Enterprise Common Use Cases