通过Collaboration Solutions Analyzer排除CUBE故障

目录

简介

本文档介绍用于使用协作解决方案分析器门户对CUBE进行故障排除的日志分析器和SIP配置文件测试器工具。

要求

Cisco 建议您了解以下主题：

- 思科统一边界元素(CUBE)企业版。
- 会话初始协议(SIP)。
- CUBE日志收集（调试）。

快速入门

Collaboration Solutions Analyzer (CSA)是一套工具，用于在协作解决方案的整个生命周期内为其提供支持。它有助于确定问题并在需要时提供纠正性行动计划，在协作解决方案的每个阶段提供帮助。

导航至协作解决方案分析器(https://cway.cisco.com/csa-new/#/home

注意：使用Chrome浏览器可确保工具以最佳状态运行。

考虑事项

这些工具专为处理SIP到SIP呼叫的CUBE设备设计。这些工具不支持任何其他语音协议。

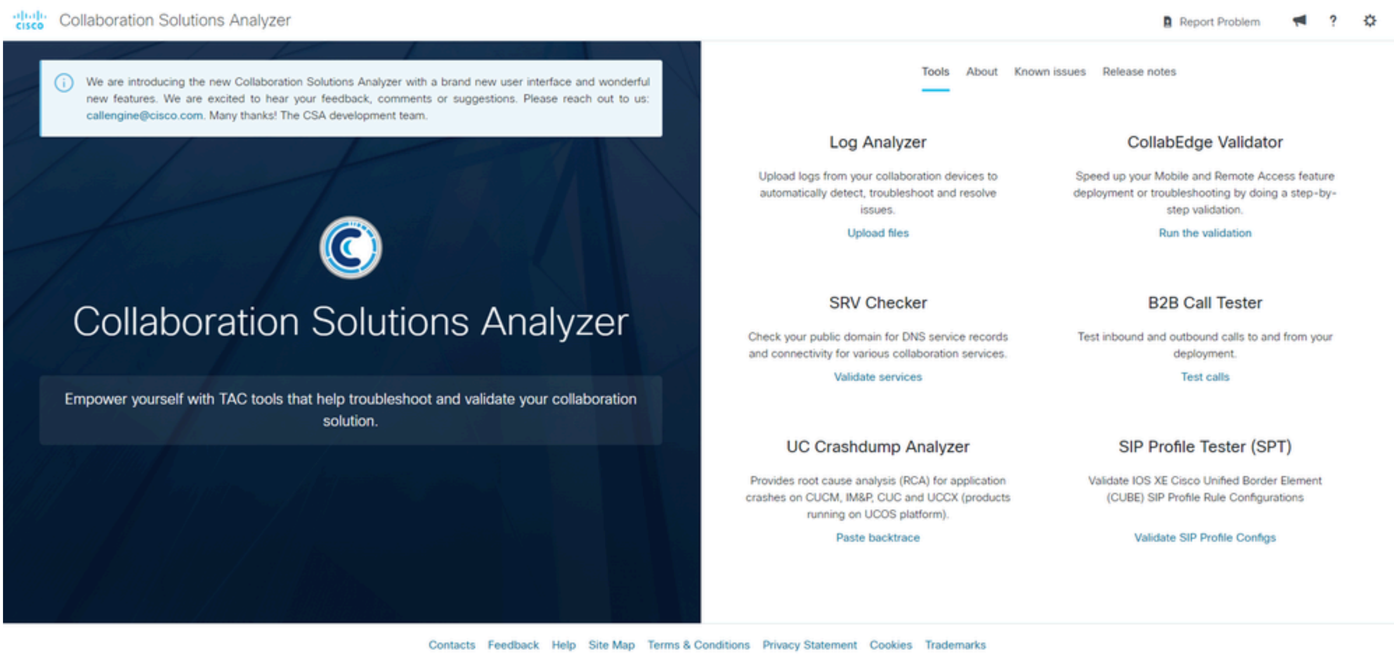
日志分析器使用CUBE日志（基于SIP消息调试）进行分析。

如需其他语音协议方面的帮助，请使用https://supportassistant.cisco.com上的思科支持助理进行TAC活动

平台说明

CSA平台提供以下CUBE工具：

- 日志分析器 -从CUBE和其他协作设备上传日志，以自动检测、故障排除和解决问题。
- SIP配置文件测试器 -验证SIP配置文件配置。



CSA主页

日志分析器

管理员可以通过日志分析器工具检查CUBE设备处理的呼叫信令。它提供日志文件的全面分析，包括：

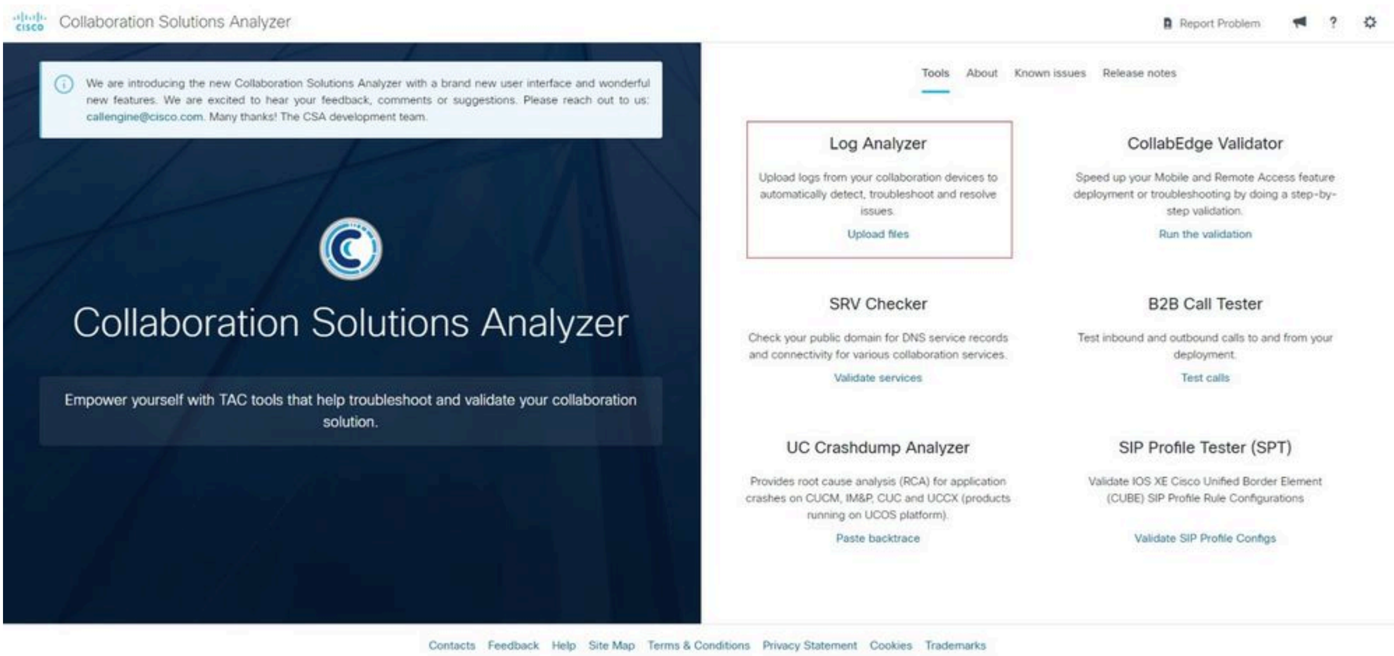
- 呼叫段信息
- 梯形图
- 信令

注意：必须先收集由CUBE处理的呼叫中的CUBE调试(debug ccsip messages)，并将其存储在文本文件中。此文本文件中必须包括SIP调试以及任何其他输出（例如show命令）。

上传CUBE日志文件

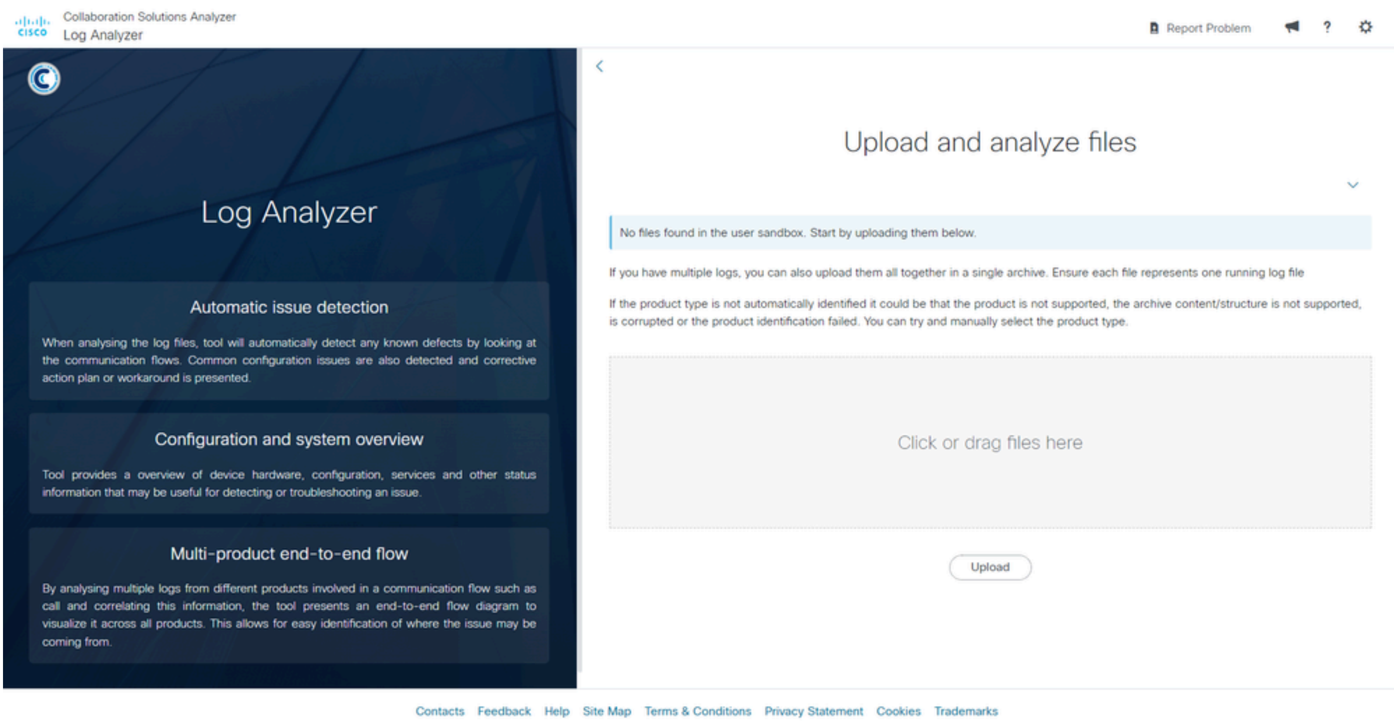
导航至协作解决方案分析器(https://cway.cisco.com/csa-new/#/home

然后单击日志分析器部分中的上传文件以选择工具。



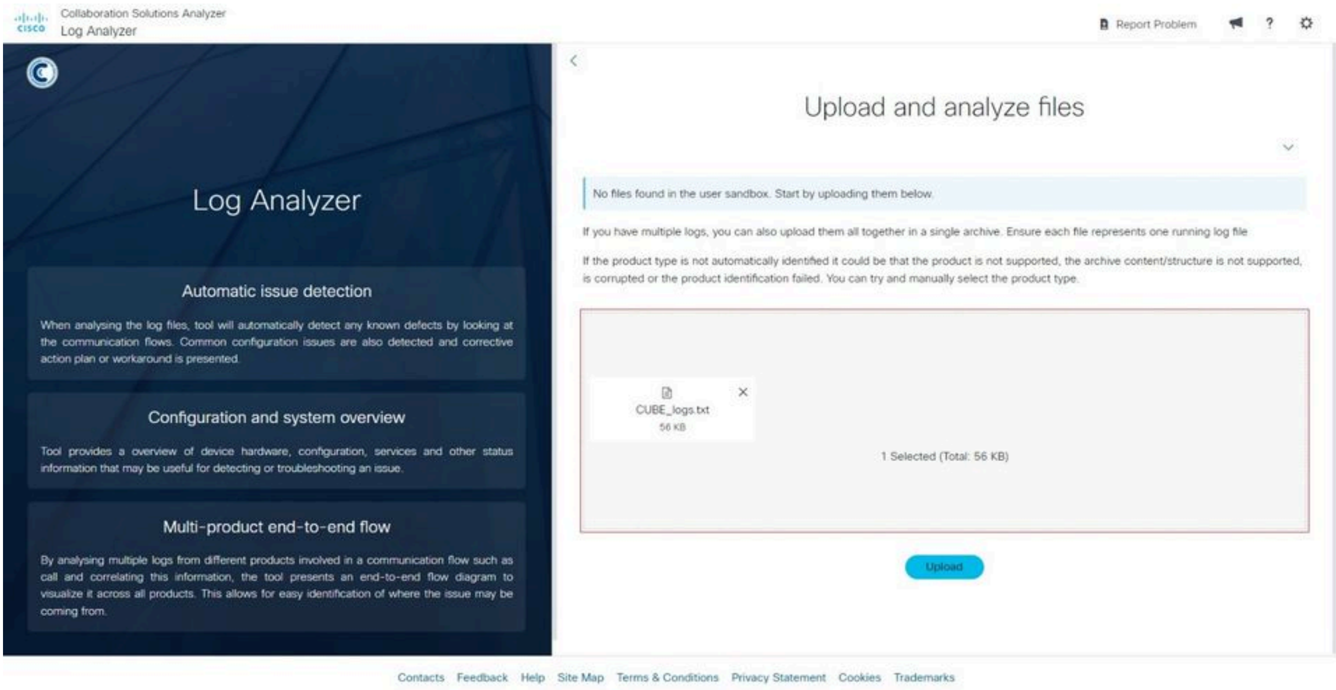
日志分析器主页

平台显示工具屏幕，可在其中选择或拖动文件。



日志分析器上传

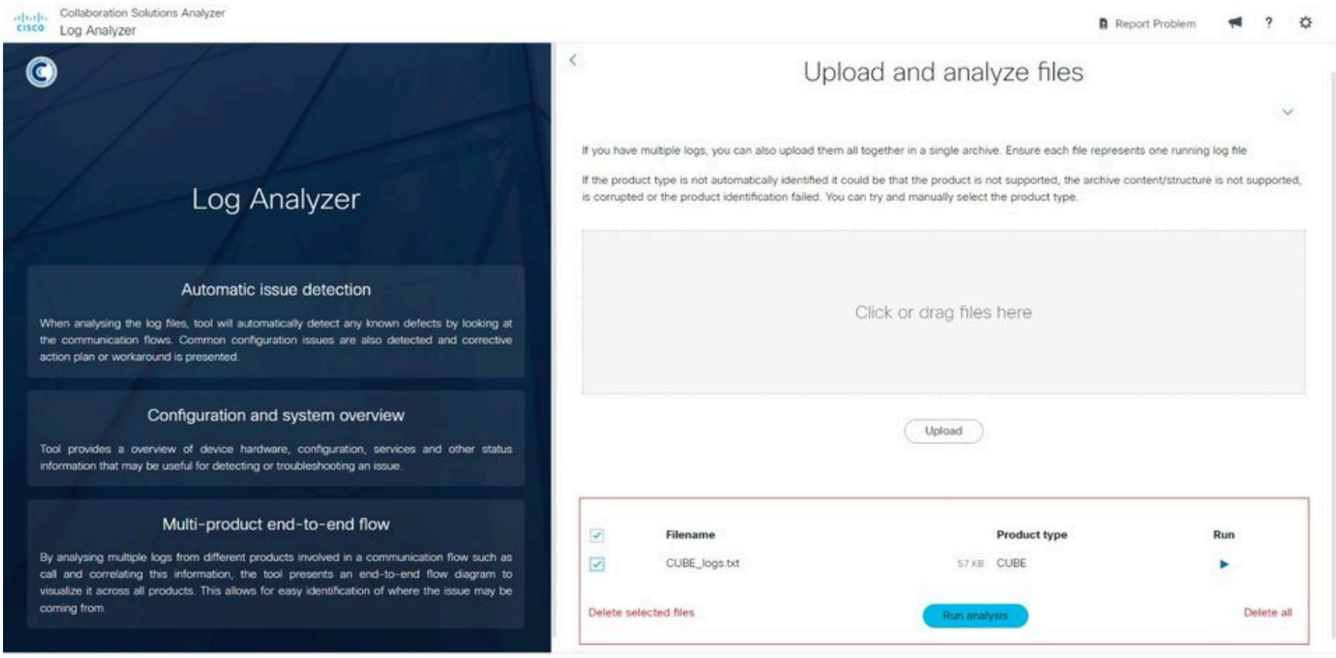
要完成上传文件以供工具分析的过程，请点击上传按钮。



日志分析器上传文件

将文件上传到工具后，通过选中相应的框来选择要分析的文件，然后单击Run Analysis按钮。

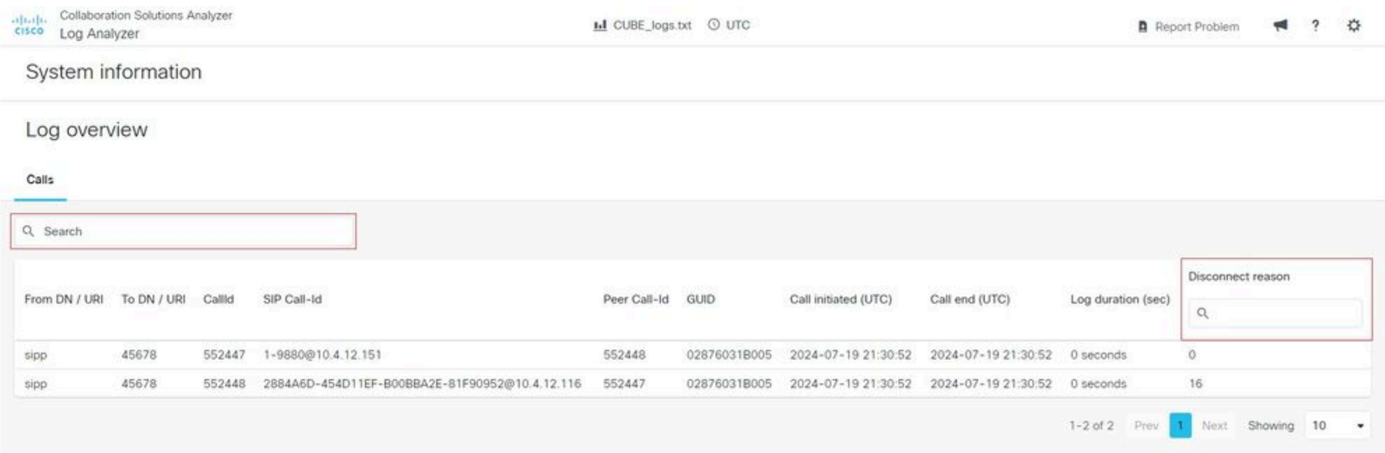
- 系统将产品类型设置为CUBE。
- 可以在同一会话中分析多个文件。



日志分析器产品类型

该工具分析在文本文件中捕获的所有信令呼叫，并显示所识别呼叫段的摘要。然后，可以应用两个过滤器：

- 搜索- 按特定数据（如拨叫号码）过滤呼叫会话。
- 按“断开原因”搜索- 根据呼叫断开原因过滤呼叫会话。



日志分析器调用过滤器

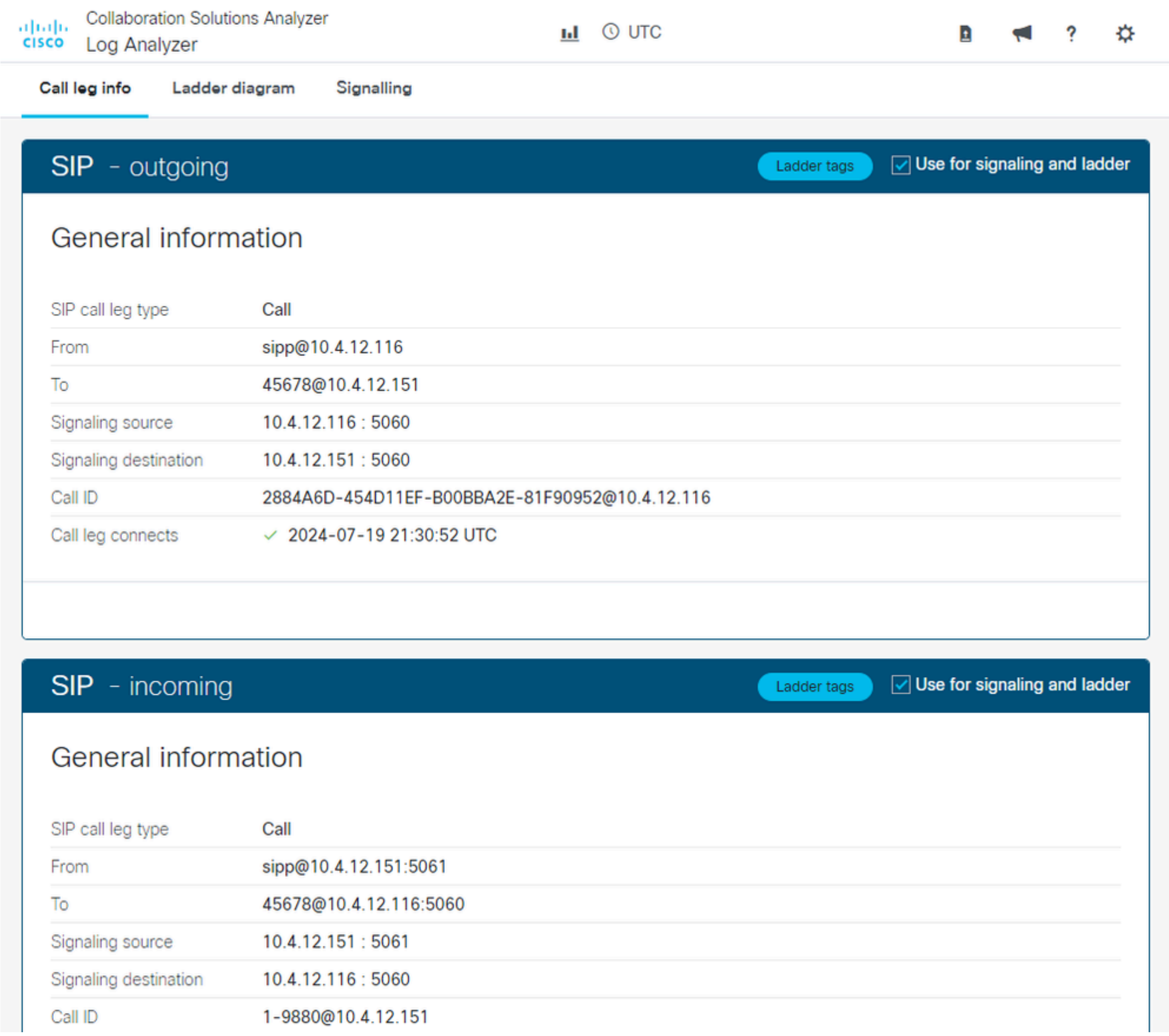
要继续详细分析，请选择您要关注的呼叫会话线路，该工具将显示展示呼叫分支信息、梯形图和信

令的完整分析。

呼叫段信息

第一阶段显示呼叫段信息，其中显示呼叫的概述：

- SIP呼叫段类型
- 发件人 -从INVITE消息的SIP报头获取。
- To -从INVITE消息的“TO SIP”报头获取。
- 信令源 -源设备的IP地址和端口。从INVITE消息的VIA SIP报头获取。
- 信令目标 -目标设备的IP地址和端口。从INVITE消息的URI SIP报头获取。
- 呼叫ID -从INVITE消息的SIP呼叫ID报头获取。
- 呼叫段连接- 呼叫会话时间戳。

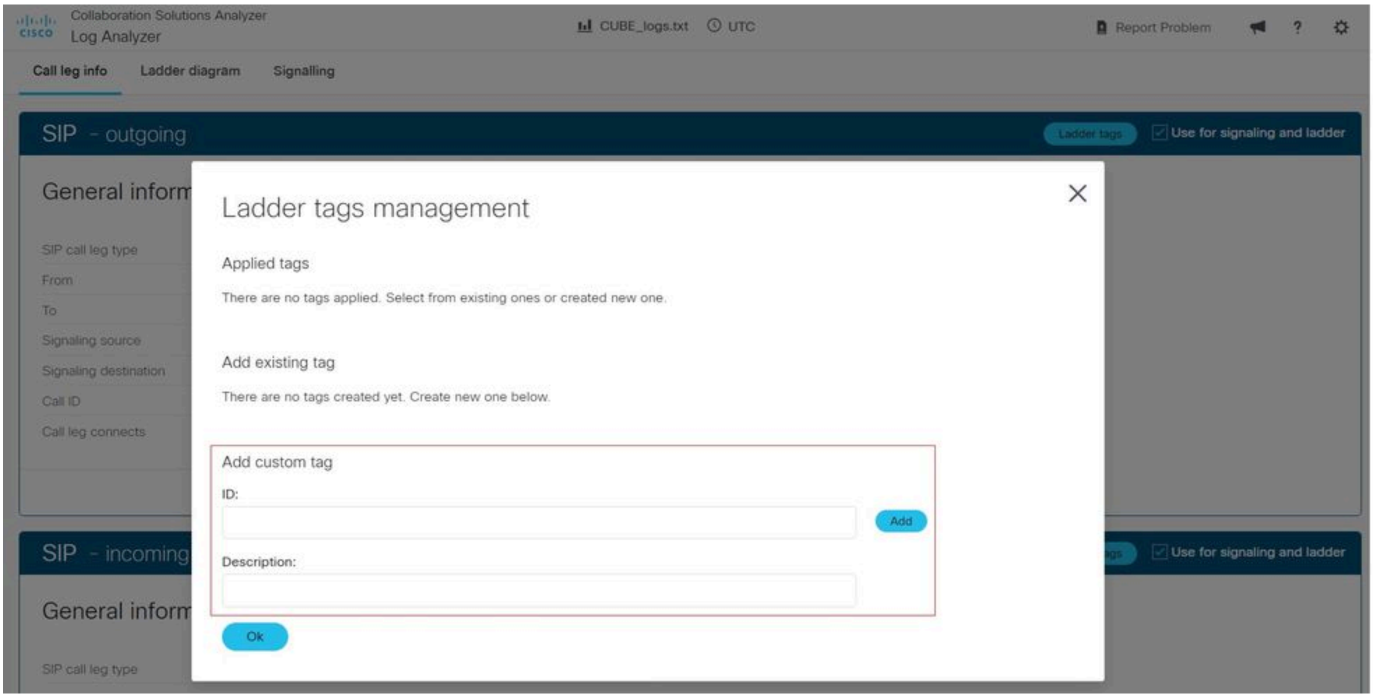


日志分析器呼叫段信息

在此部分，可以启用梯形标记以突出显示梯形图中的消息。该应用程序有2个字段：

- ID -输入要突出显示的特定参数。
- Description -添加参数的说明。

单击Add按钮完成此过程。



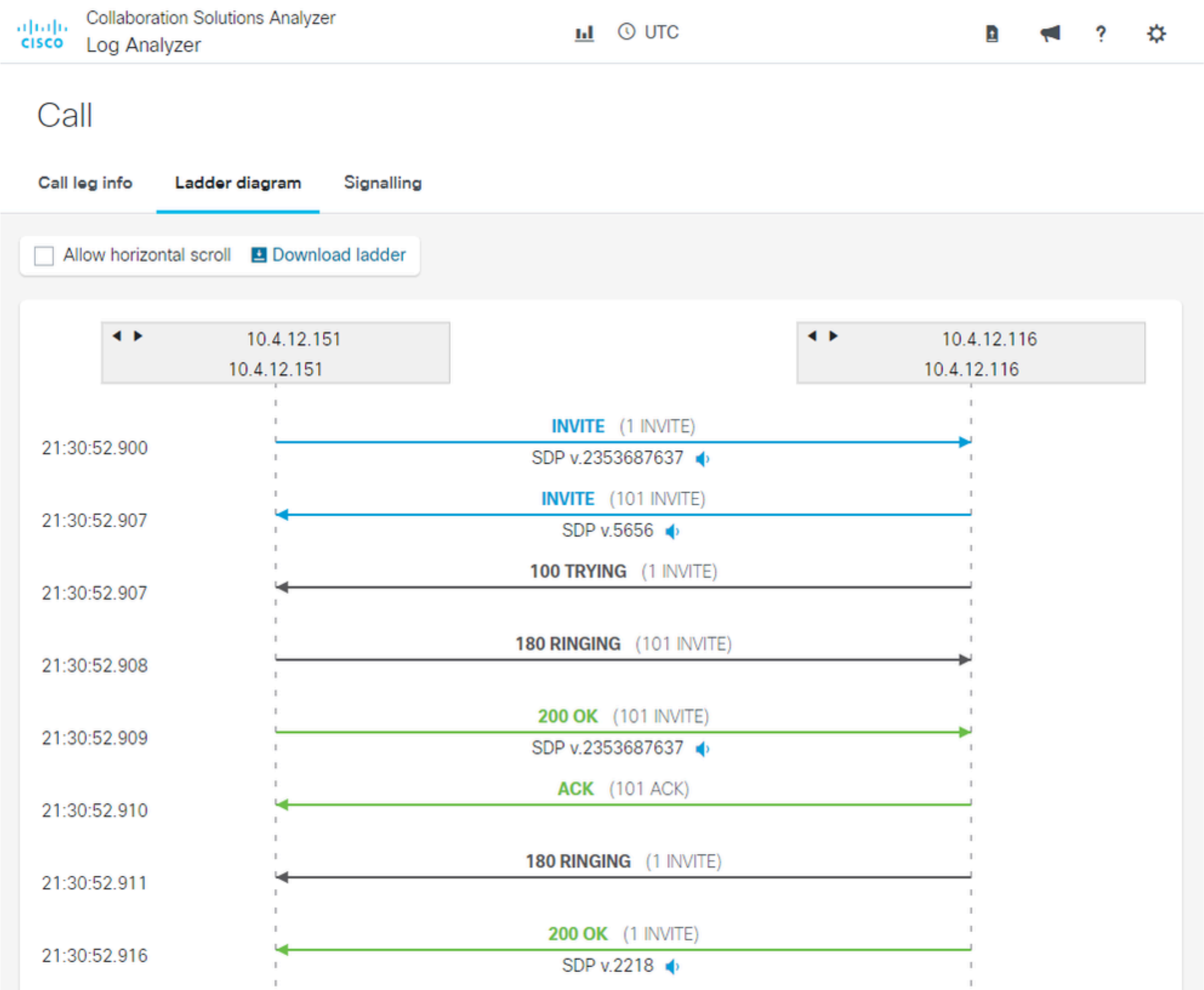
日志分析器梯形标签

梯形图

在第二阶段，显示梯形图，直观地描述呼叫过程中交换的SIP消息。这些消息采用颜色编码，以方便识别：

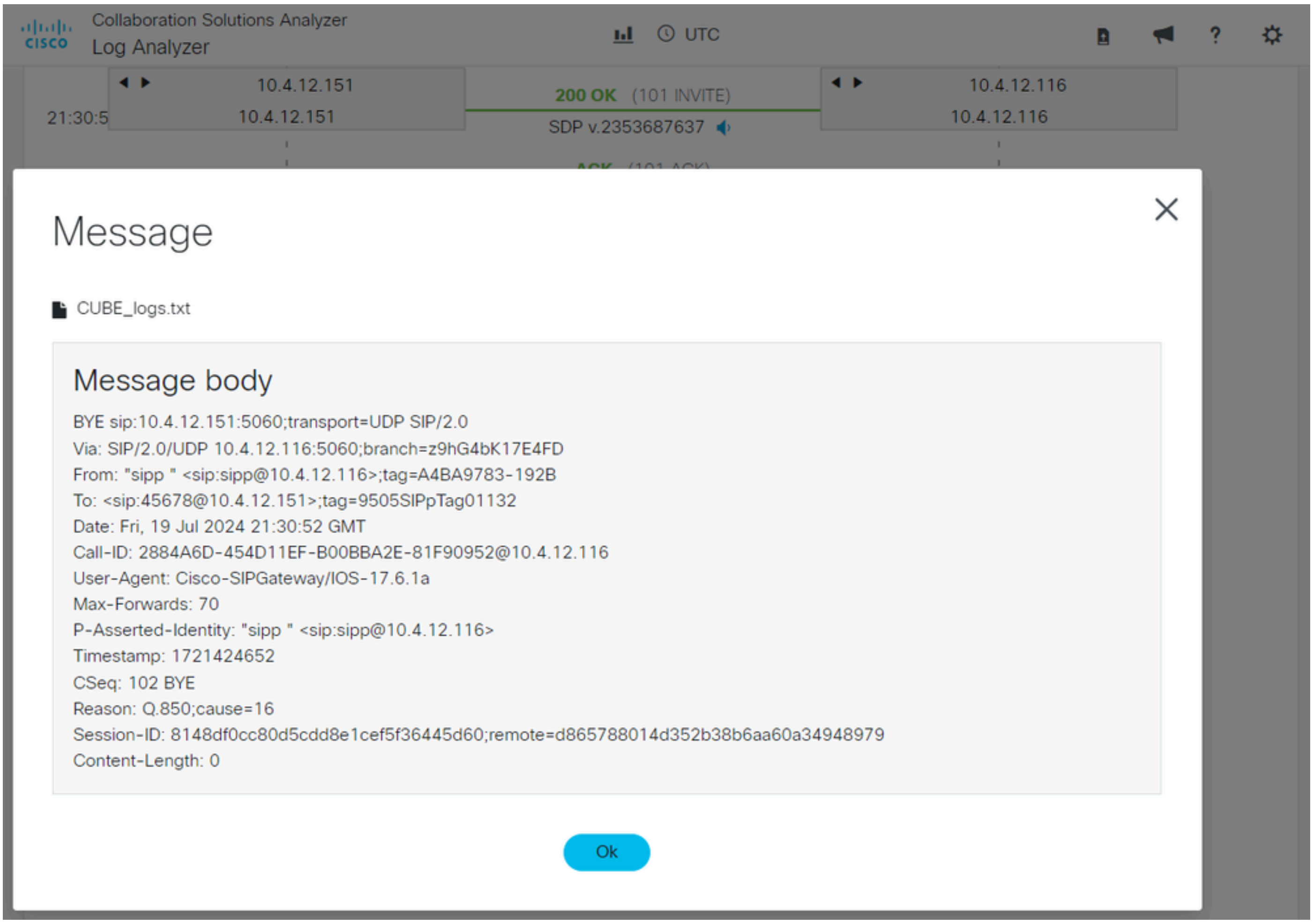
- 蓝色- SIP INVITE消息。
- 绿色 - SIP 200 OK和ACK消息。
- 红色- SIP BYE消息。

要下载图的副本，请单击Download Ladder按钮。系统随即会下载该图并将其保存为PNG图像文件。请注意，此选项仅在使用Google Chrome浏览器时可用。



日志分析器梯形图

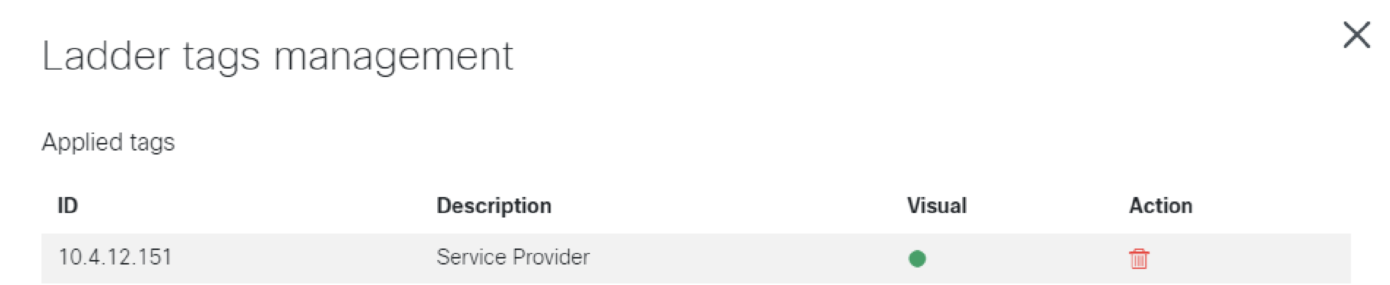
此工具允许管理员打开SIP消息并查看其内容。单击一条消息将其打开。



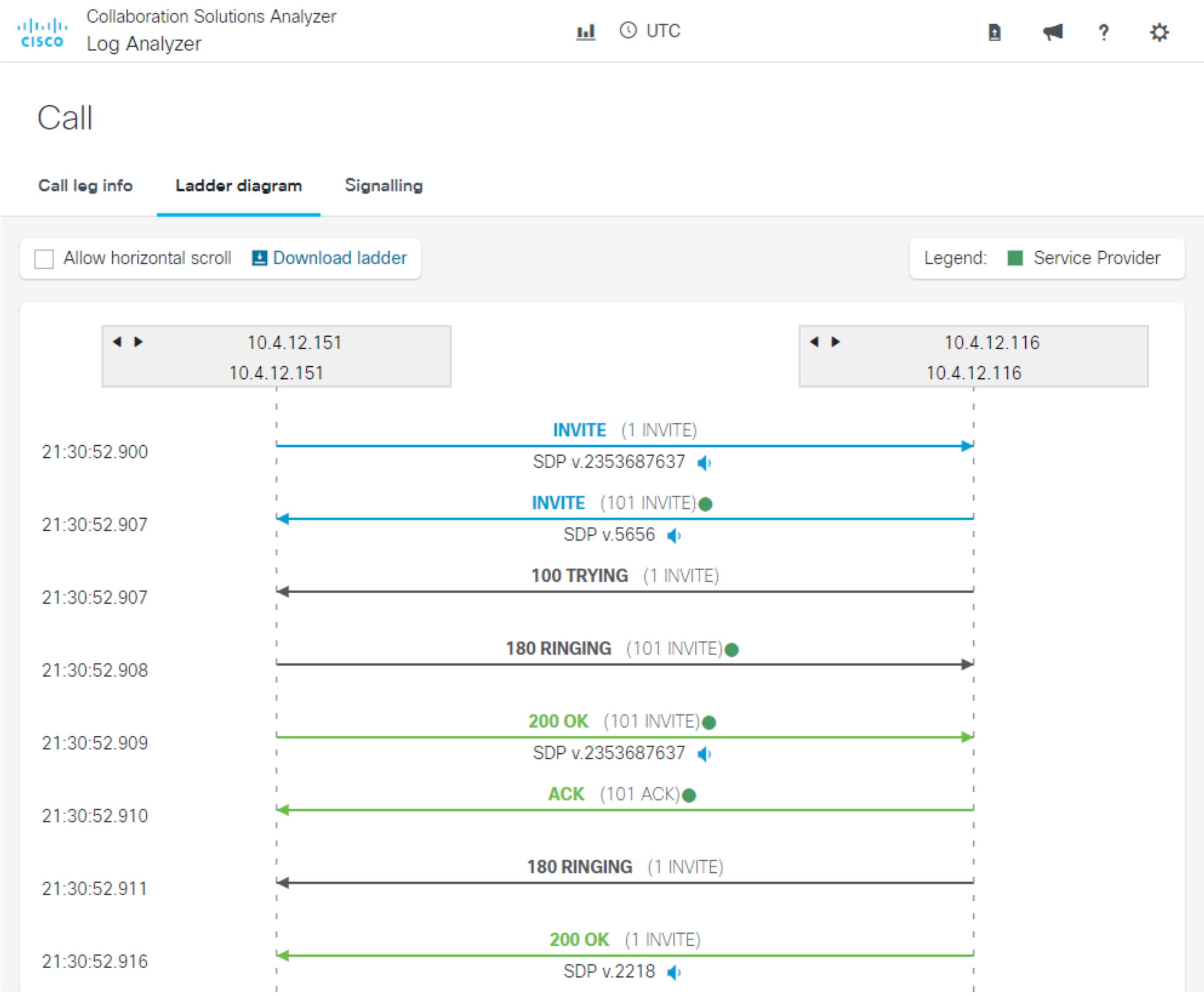
日志分析器梯形图消息

管理员可以在呼叫分支信息部分添加阶梯标记以使SIP消息具有明显的点标记。SIP消息中包含的任何参数都可用于标记。

在本例中，ID参数使用IP地址，并且添加了说明。包含IP地址的SIP消息以圆点标记突出显示，以便与其他消息区分。



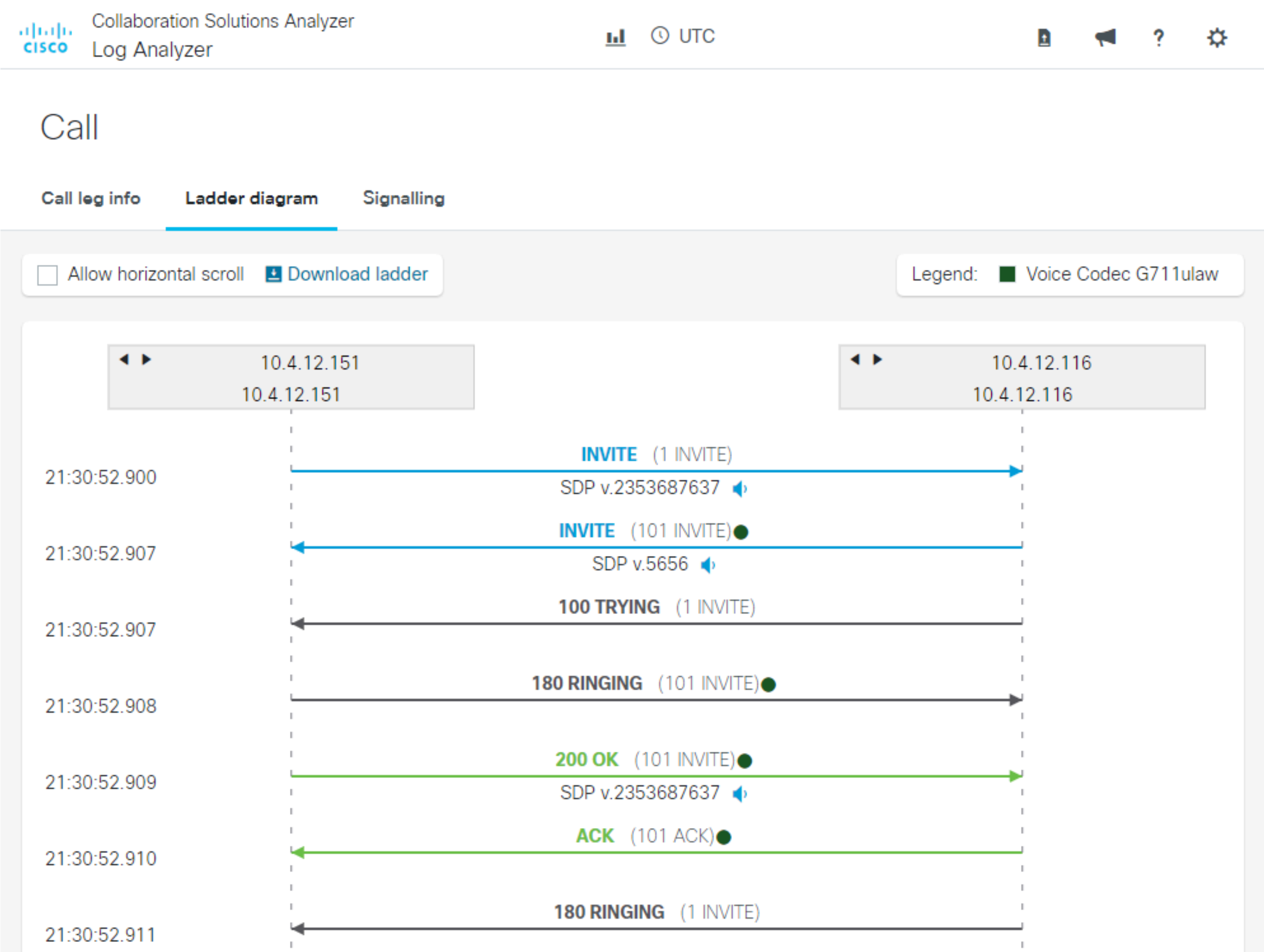
日志分析器梯形标签1



日志分析器梯形标签2

可用于区分SIP消息与其他消息的另一个过滤器是语音编解码器。

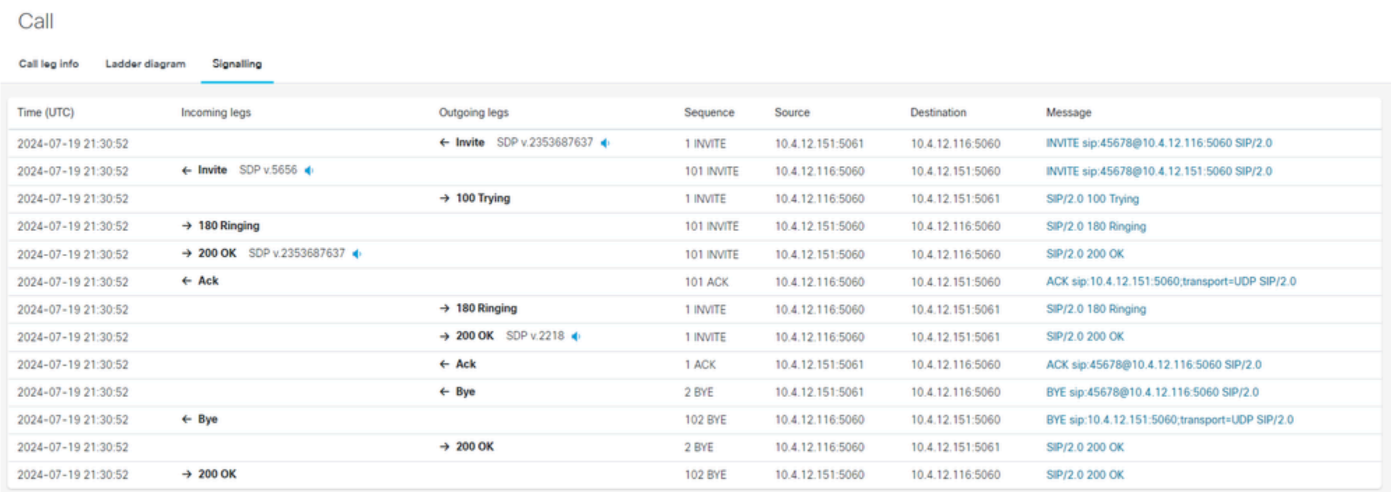
日志分析器梯形标签3



日志分析器梯形标签4

信令

最后阶段是信令，它显示CUBE段（传入和传出）的SIP消息。它包含源IP地址和目的IP地址。单击以查看消息。



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

日志分析器信令

日志分析器信令消息

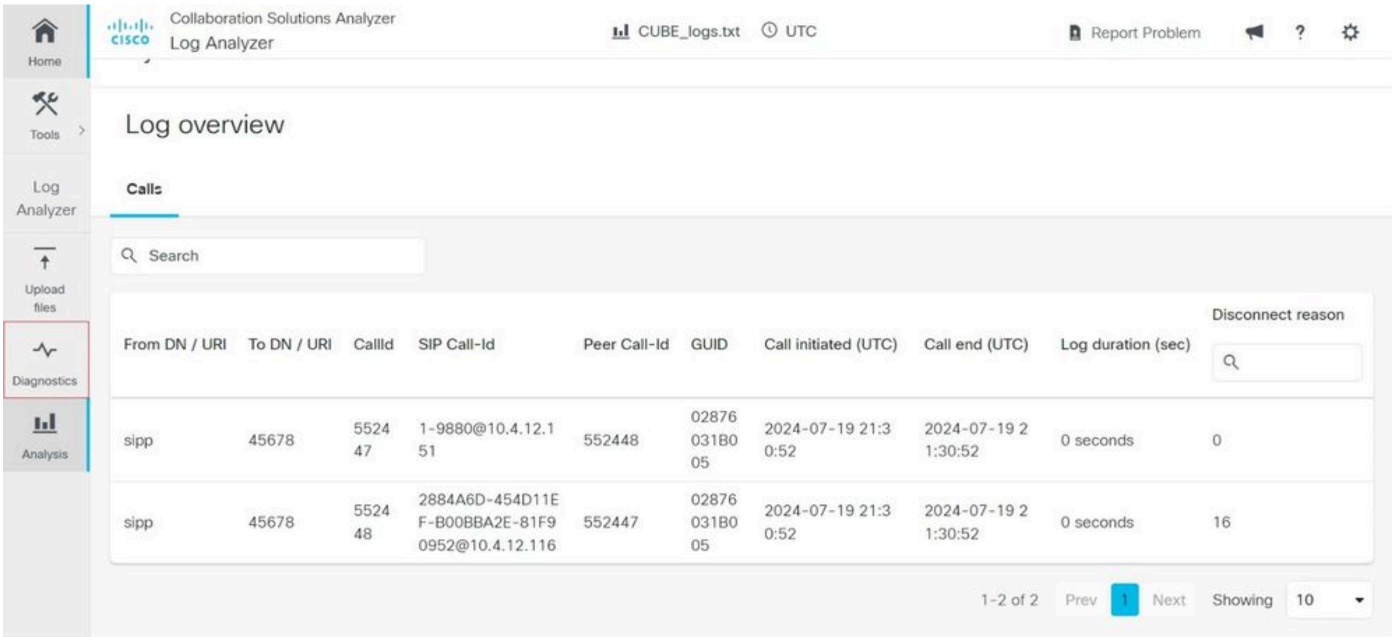
诊断

从日志分析的所有数据都将根据诊断签名运行，这些签名可识别已知缺陷、常见问题或错误配置，并提供纠正措施计划。

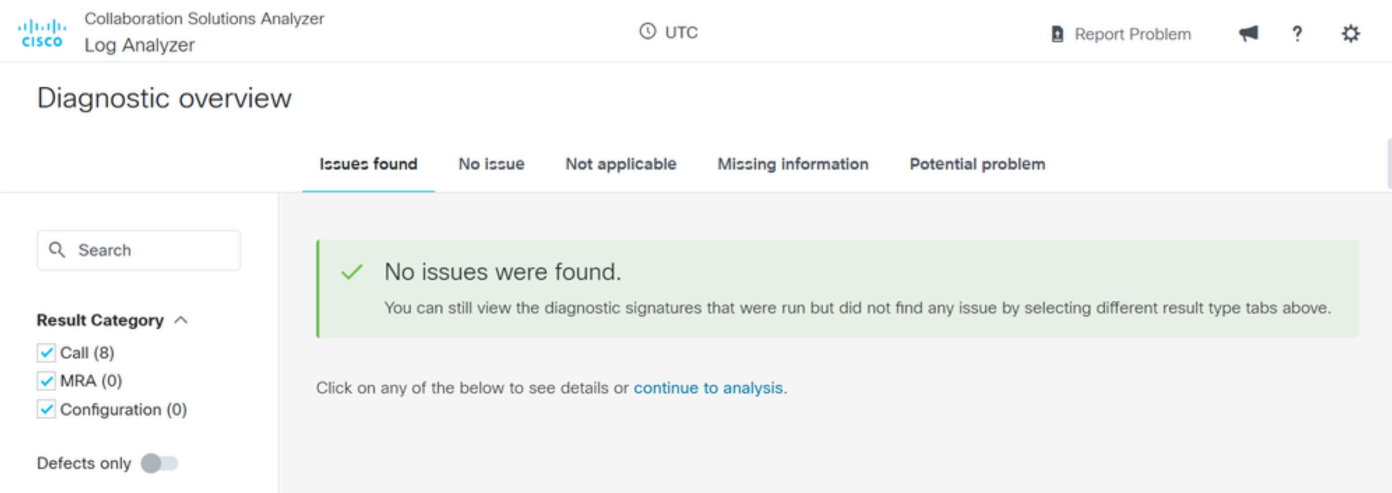
选择在日志中捕获的呼叫显示呼叫摘要分析后，CSA平台应显示诊断部分，其中包含以下信息：

- 发现的问题
- 缺少信息
- 潜在问题

可激活切换按钮以仅过滤和显示缺陷。



日志分析器诊断程序主页



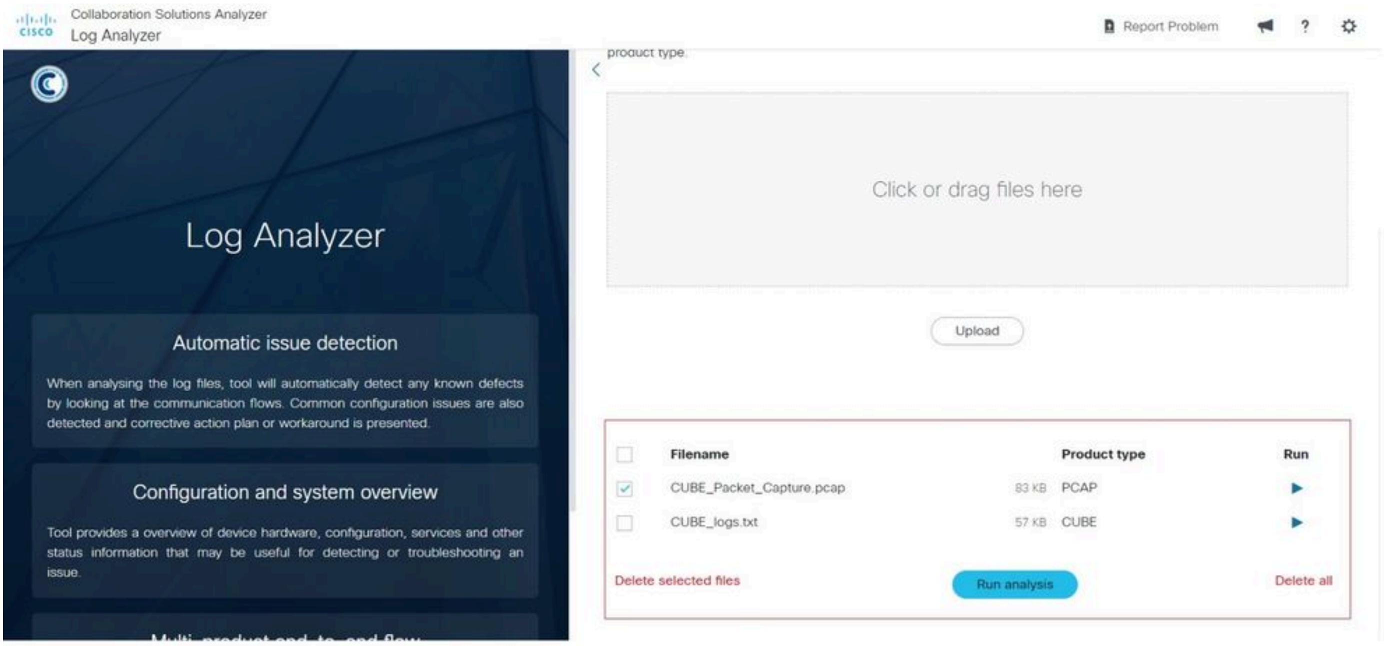
日志分析器诊断概述

CUBE数据包捕获

数据包捕获是一种文件缓冲区，创建它的目的是在CUBE网络接口或任何语音网络设备上收集实际数据包的副本。此文件可以通过网络分析器软件(如Wireshark)打开和分析。

日志分析工具已通过数据包捕获分析工具进行增强，该工具可以处理pcap或pcpng文件格式扩展，提供从呼叫中收集的会话和网络统计信息的摘要。

数据包捕获文件必须以CUBE日志文件相同的方式上传到日志分析器工具。系统将产品类型确定为PCAP。



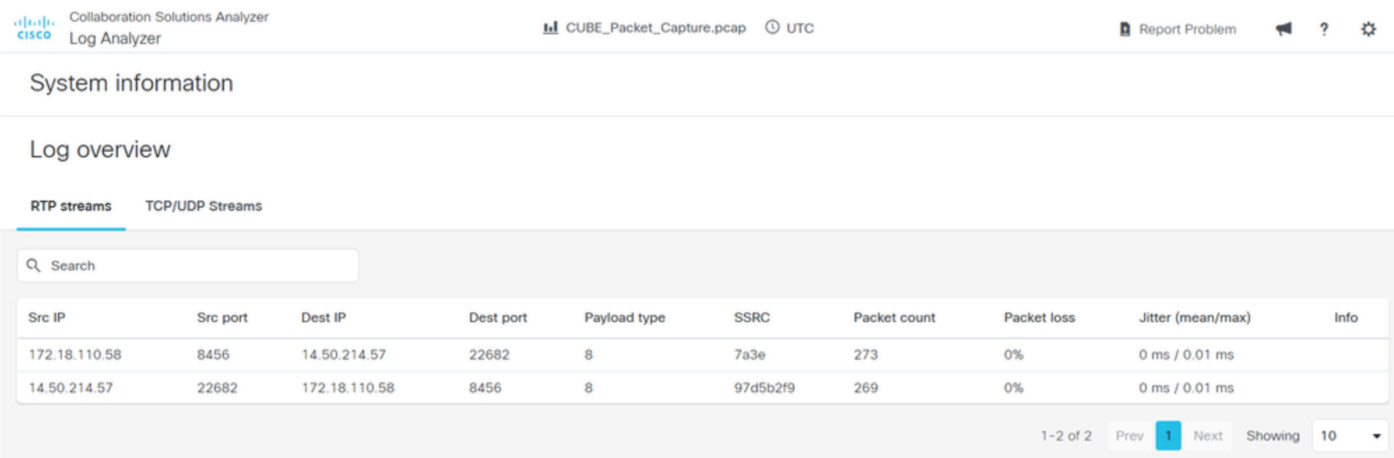
日志分析器数据包捕获文件

激活运行分析按钮后，日志分析器工具将分析信息并在两列中提供所捕获会话的摘要：

- RTP流
- TCP/UDP数据流

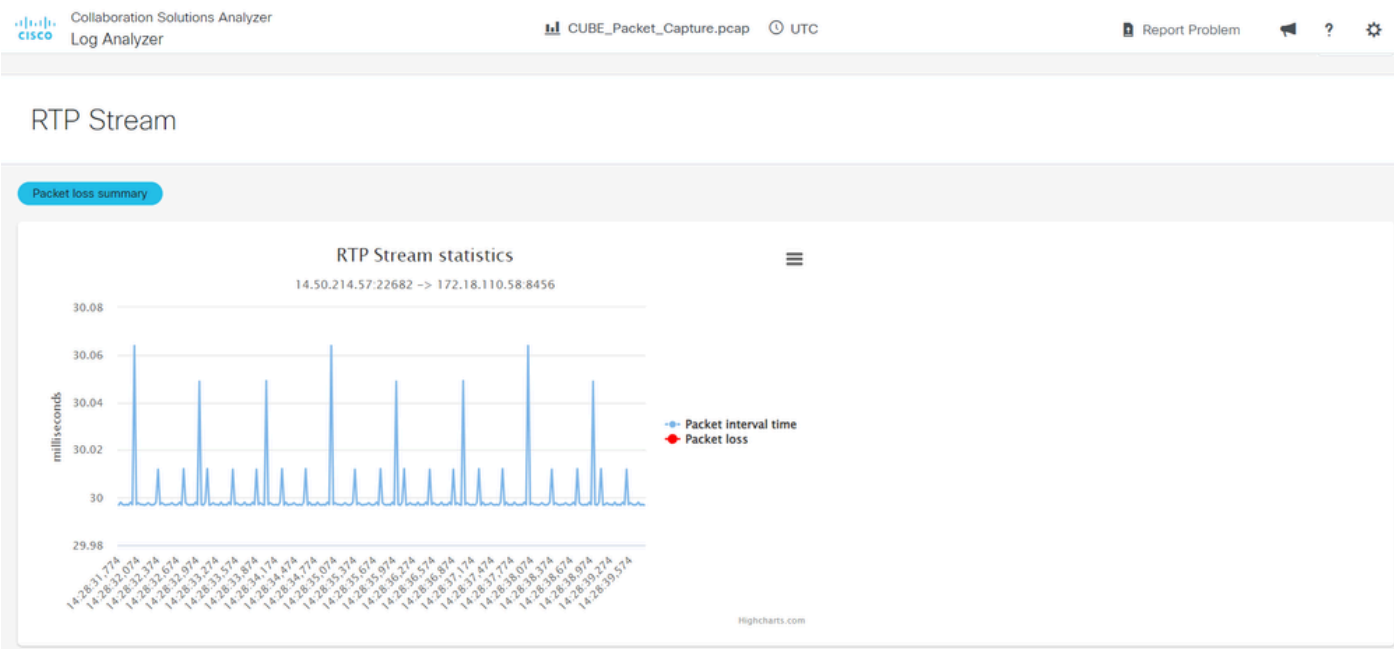
注意：如果数据包捕获包含SRTP流，则它将显示在“RTP流”列中，并执行网络分析。SRTP流的音频部分未解码。

从RTP流列中选择一个会话，工具将显示该连接的RTP流统计信息。如果数据流受到网络条件的影响，则丢包参数应标有红点。



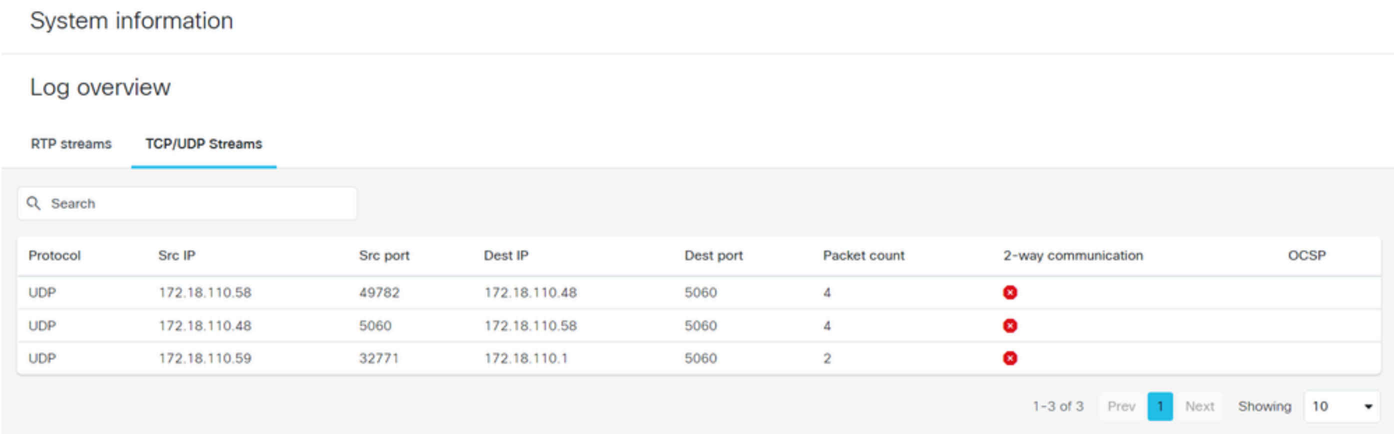
日志分析器PCAP分析

RTP流统计信息可以以包含数据包丢失摘要的文本文件格式下载。单击Packet Loss Summary按钮以下载文件。



日志分析器PCAP RTP流

对于TCP/UDP流，系统显示捕获的会话的摘要。



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	✖	

日志分析器PCAP TCP UDP数据流

SIP配置文件测试器(SPT)

会话发起协议(SIP)配置文件用于修改传入或传出SIP消息，以确保不同设备之间的兼容性。“SIP配置文件测试器”工具允许您在实时环境中部署配置之前验证配置。

SIP配置文件工具包含3个部分：

- SIP配置文件规则 -用于插入要测试的SIP配置文件规则的窗口。
- SIP Message to Apply Rules -用于将SIP消息粘贴到要应用规则的位置的窗口。
- SIP message to copy from -（可选）用于粘贴SIP消息以备测试复制列表配置时使用。复制列表配置将设备接收的入站报头内容复制到出站报头。

该工具包含2个用于管理测试的按钮：

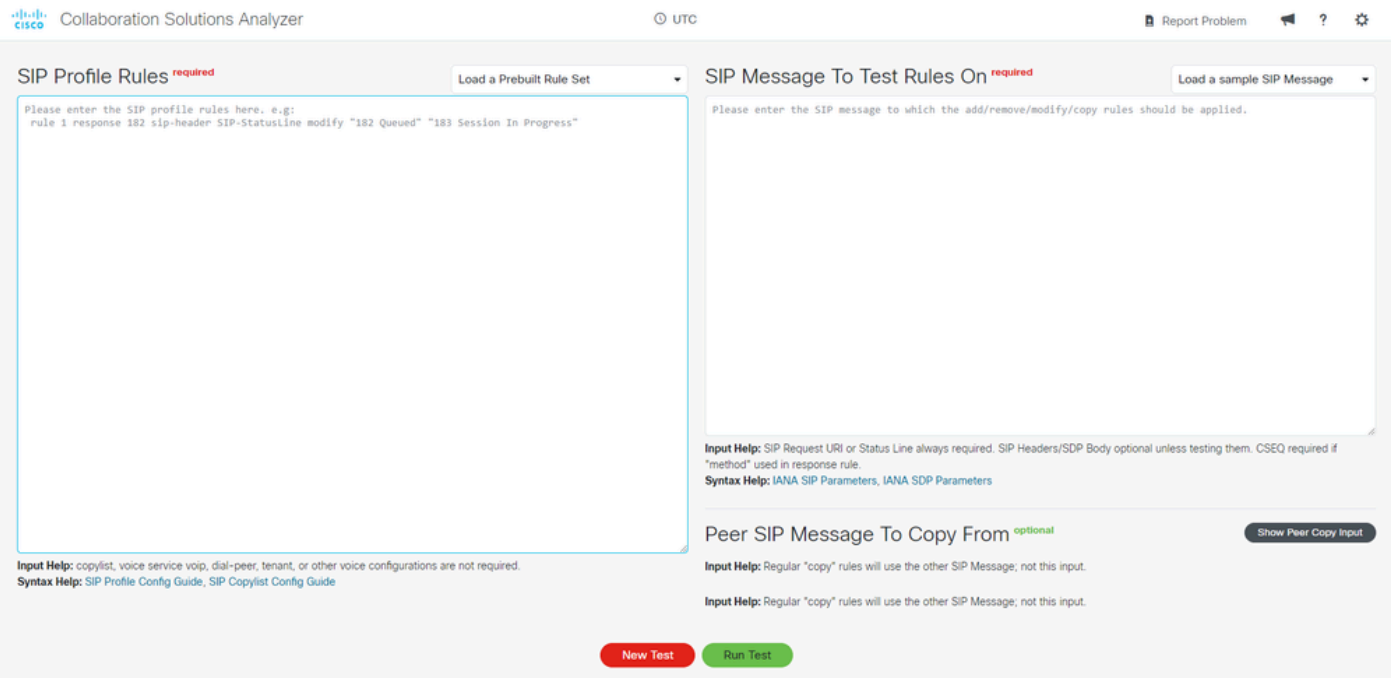
- 绿色按钮- 运行测试。
- 红色按钮- 用于重置和清除设置。

选择绿色按钮运行测试后，该工具将显示以下选项：

- 红色按钮- 新测试
- 蓝色按钮- 显示输入

突出显示原始/修改的SIP消息结果：

- 蓝色- 修改的SIP报头或SDP正文在两个消息区域中均以蓝色突出显示。
- 绿色- 添加的SIP报头或SDP正文仅在修改的SIP消息结果中突出显示为绿色。
- 红色- 删除的SIP报头或SDP正文仅在原始SIP消息结果中突出显示为红色。



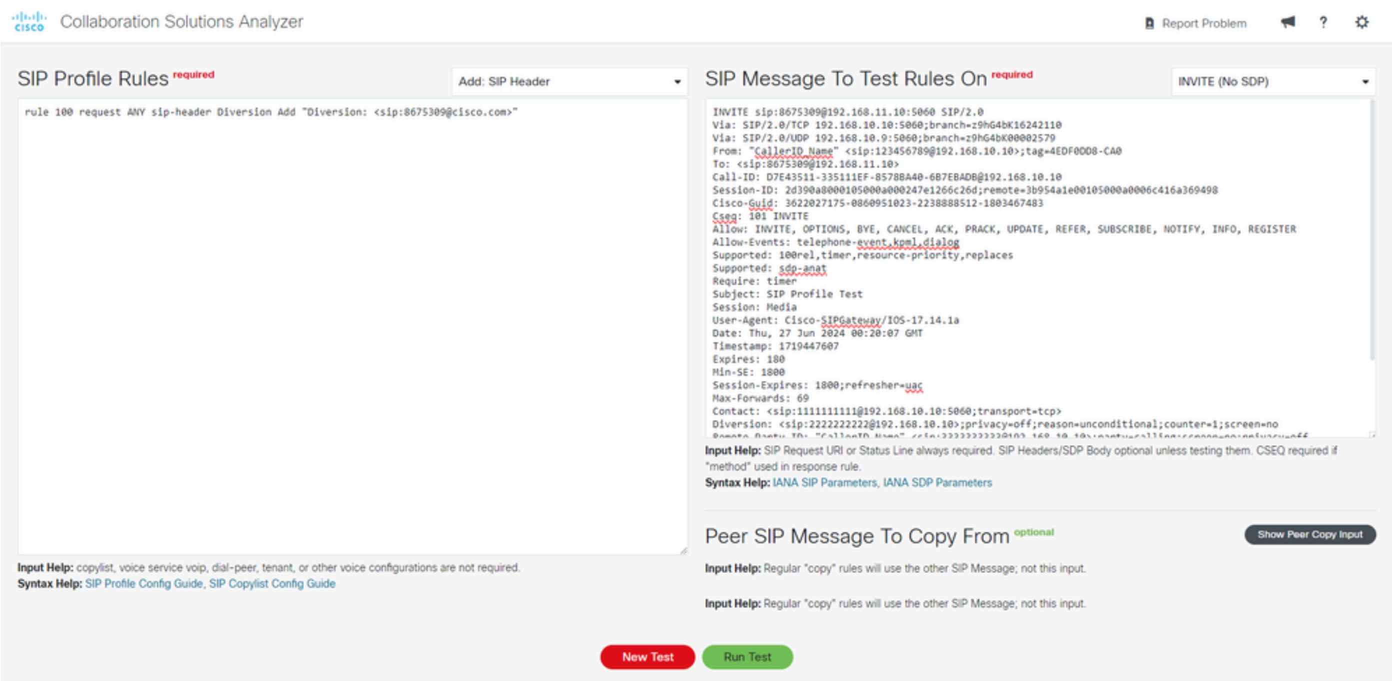
SIP配置文件主页

预构建SIP配置文件示例

该工具提供预建示例来简化测试。在每个窗口的顶部，都有一个用于选择这些示例的应用程序框。

以下是如何使用预定义的配置：

1. 点击加载预构建规则集并选择添加：SIP报头。
2. 点击加载示例SIP消息并选择邀请（无SDP）。
3. 选择绿色的Run Test 按钮以执行测试。

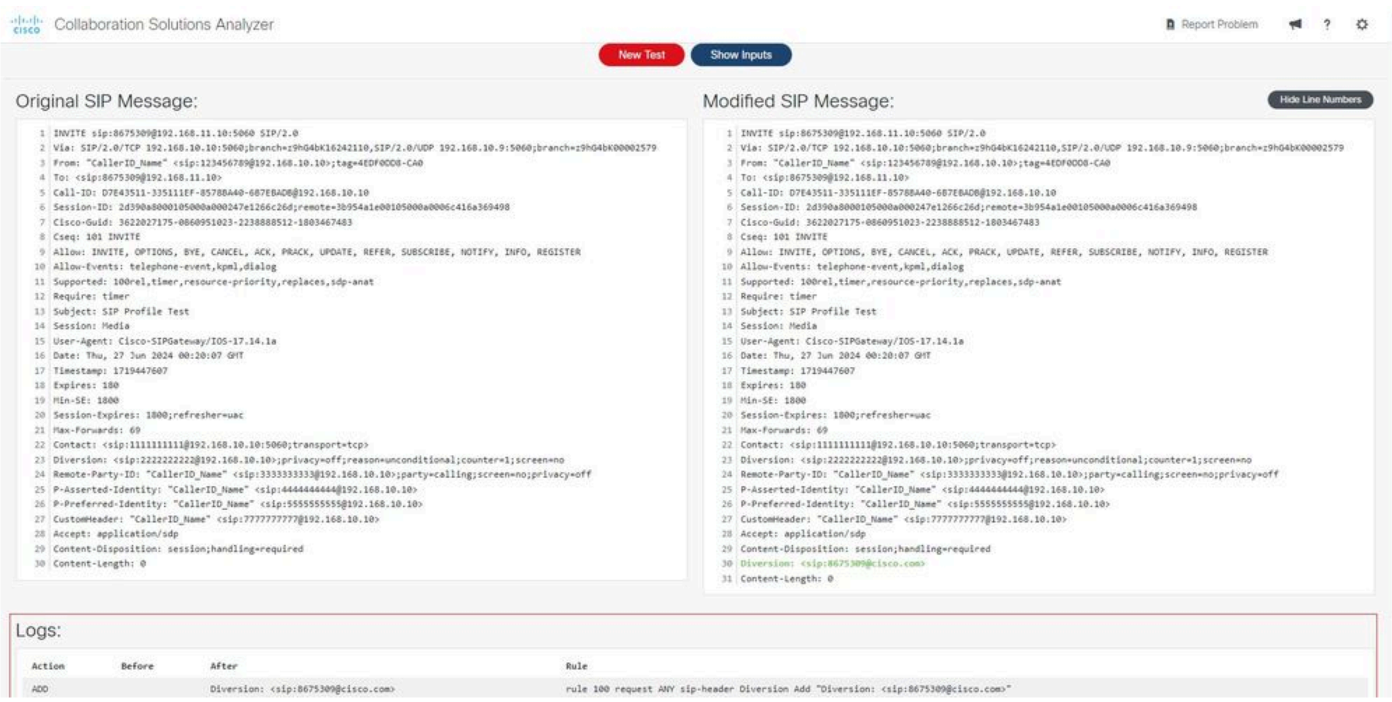


预置SIP配置文件

该工具将显示一个新屏幕，显示测试结果：

修改的SIP消息

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



SIP配置文件预构建添加示例

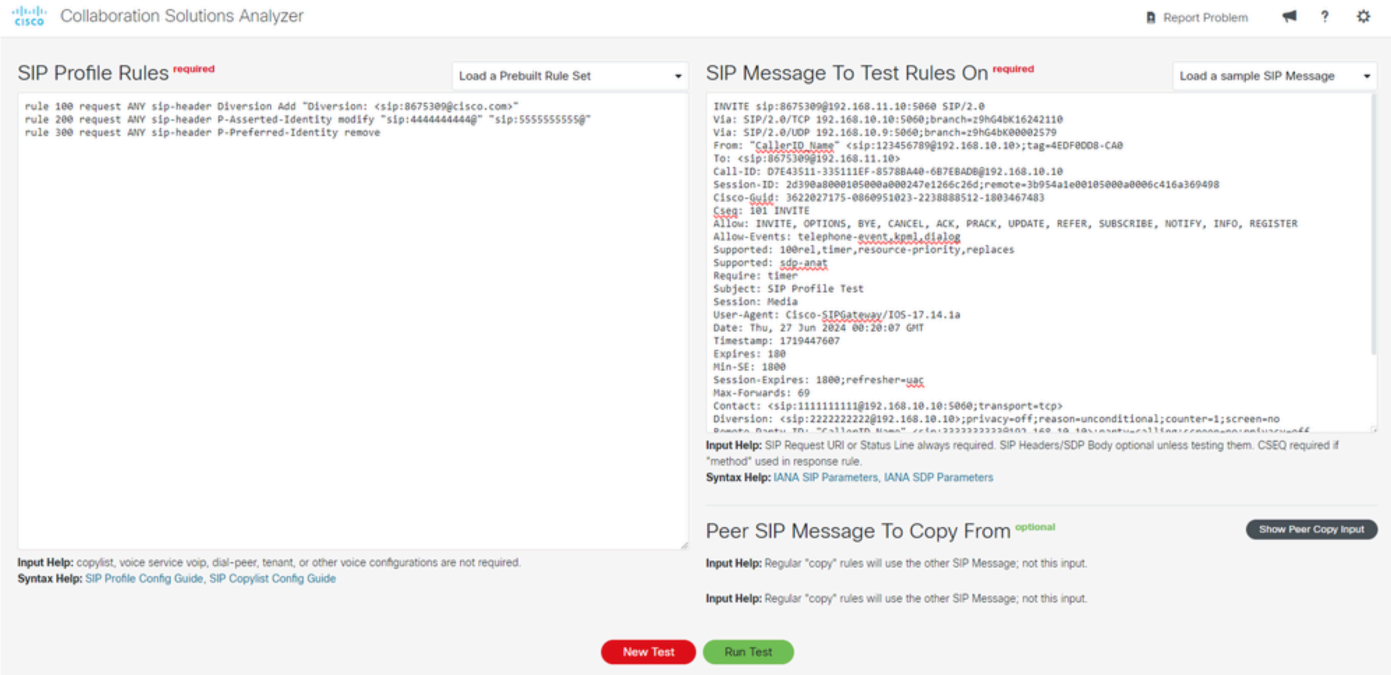
下面是修改/添加/删除突出显示的示例：

SIP配置文件规则

```
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
```

测试规则的Sip消息

```
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配置文件修改添加删除示例

要查看结果，请单击Run Test。

原始SIP消息

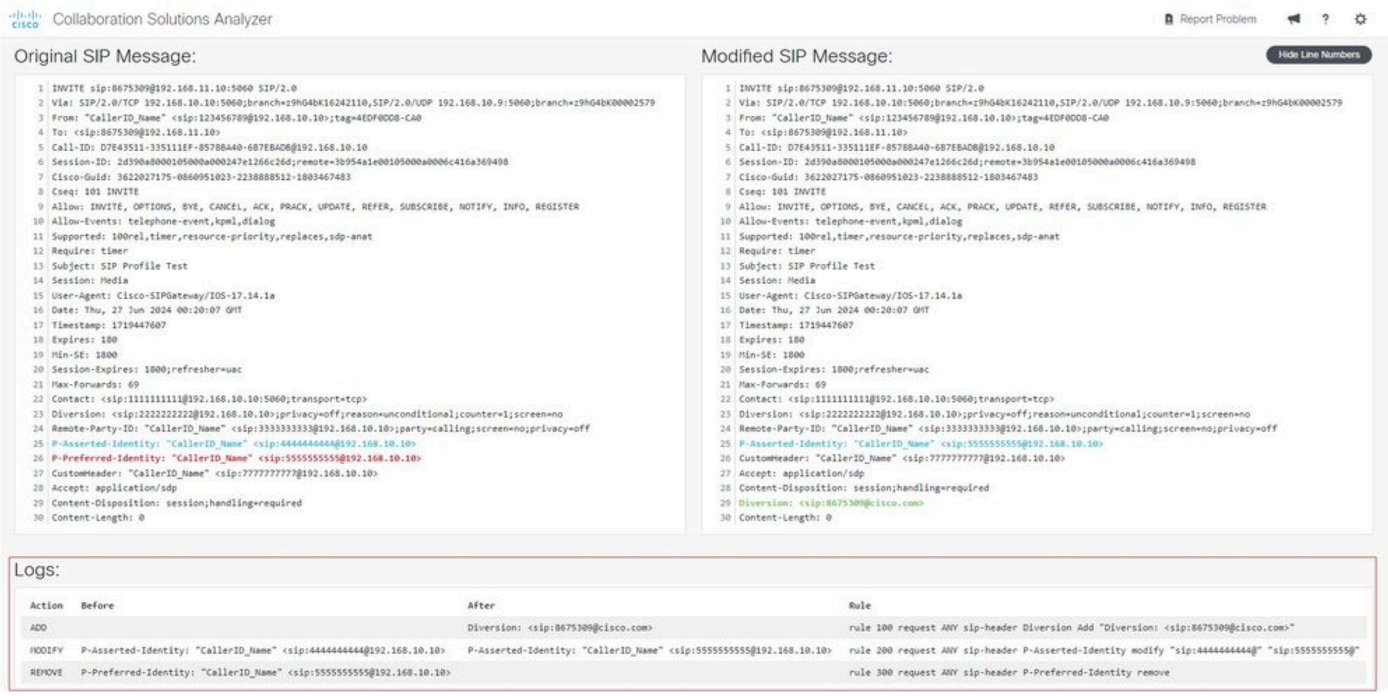
```
MODIFIED (BLUE) - P-Asserted-Identity: "CallerID_Name"
```

```
       4444444444@192.168.10.10>
```

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

修改的SIP消息

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



SIP配置文件修改添加删除示例2

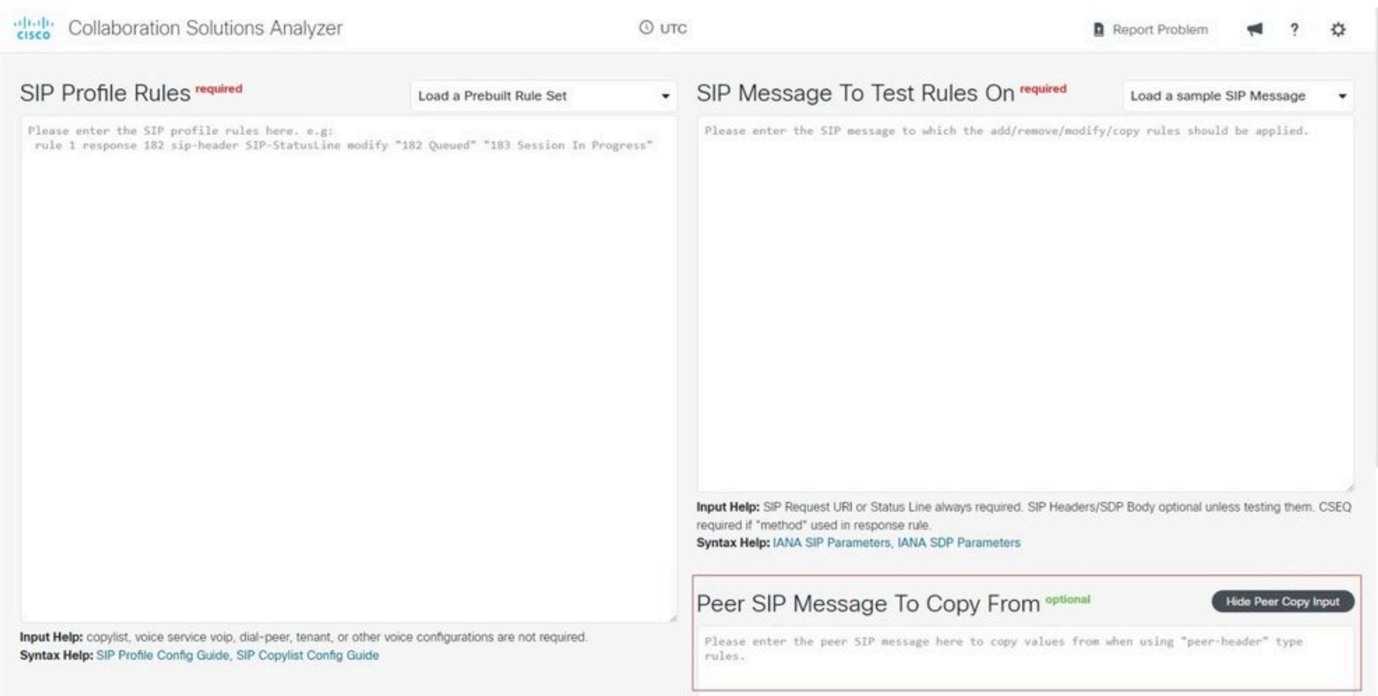
Copylist SIP配置文件

要将设备收到的传入报头中的内容复制到传出报头（SIP复制列表），可以使用以下工具输入：

- 流程图：传入SIP消息— > CUBE — >修改的SIP消息

- Peer SIP Message To Copy From -要从中复制的SIP消息。
- Sip Message To Test Rules On -用于应用规则的SIP消息。

要启用要从中复制的对等SIP消息部分，必须启用Show Peer Copy Input选项。您可以单击Hide Peer Copy Input隐藏此部分。



以下是SIP规则、传入和修改的SIP消息的示例：

SIP配置文件规则。

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

要应用规则的SIP消息。

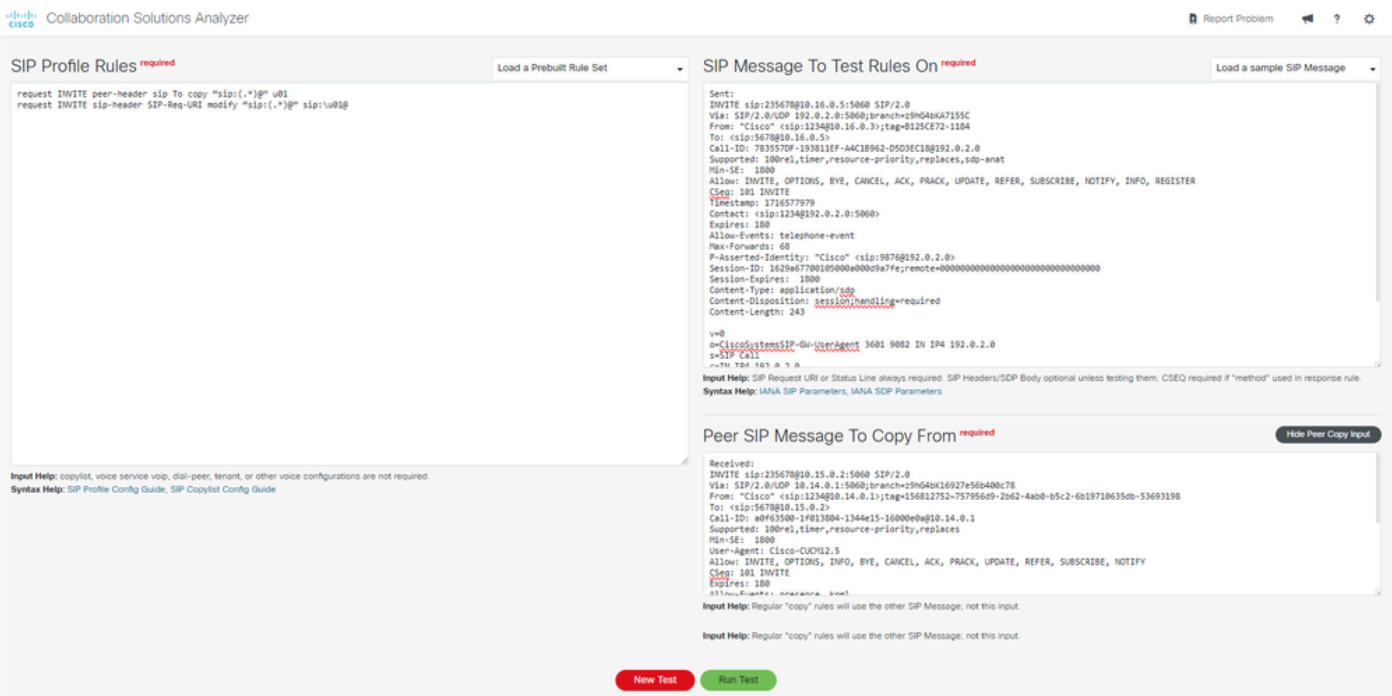
```
Sent:
INVITE sip:235678@10.16.0.5:5060 SIP/2.0
Via: SIP/2.0/UDP 192.0.2.0:5060;branch=z9hG4bKA7155C
From: "Cisco" <sip:1234@10.16.0.3>;tag=B125CE72-1184
To: <sip:5678@10.16.0.5>
Call-ID: 783557DF-193811EF-A4C1B962-D5D3EC18@192.0.2.0
Supported: 100rel,timer,resource-priority,replaces,sdp-anat
Min-SE: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

要从中复制的SIP消息。

```
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配置文件复制列表示例

单击Run Test 按钮继续以启动工具。

复制寄存器

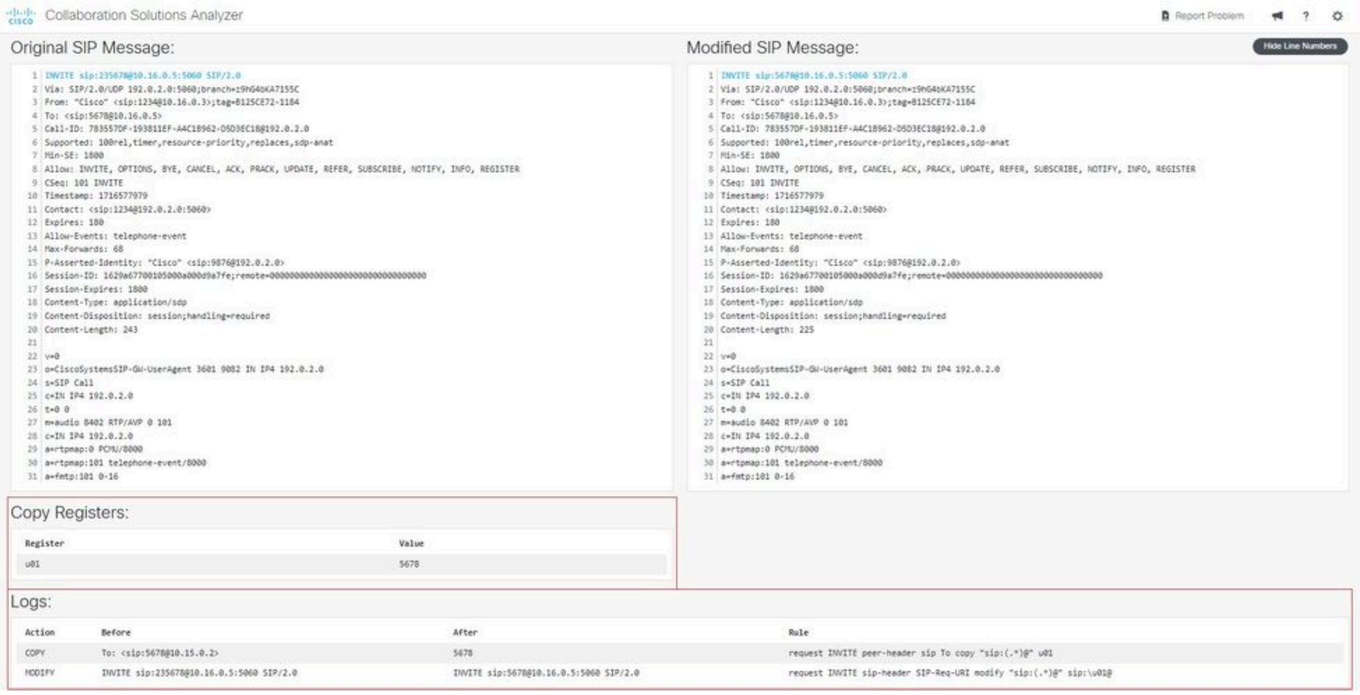
```
Register: u01
Value: 5678
```

原始SIP消息

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

修改的SIP消息

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

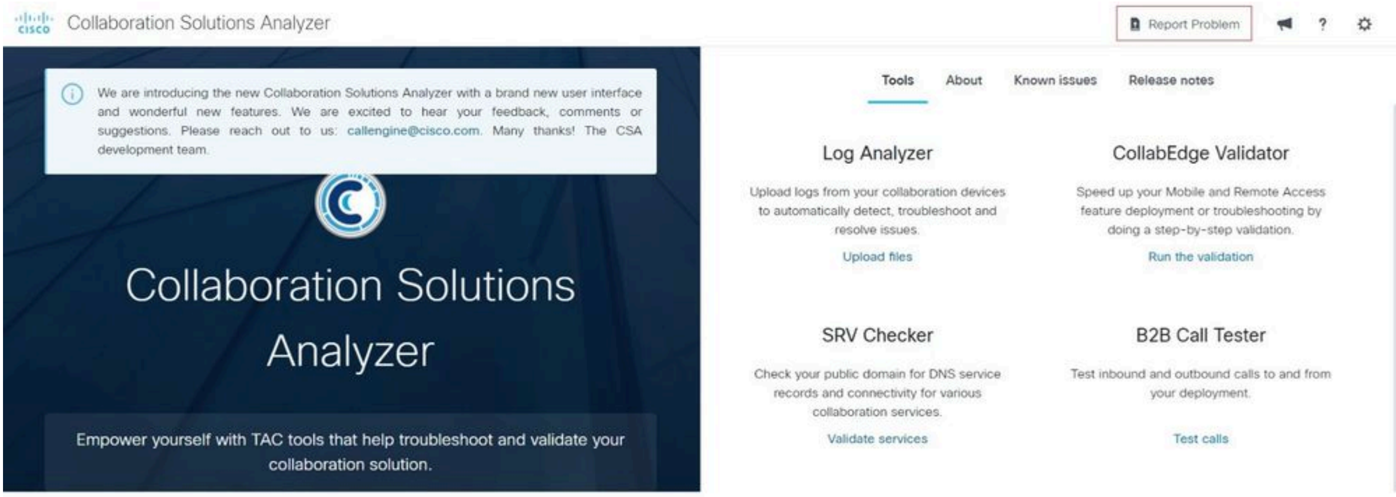


SIP配置文件复制列表示例2

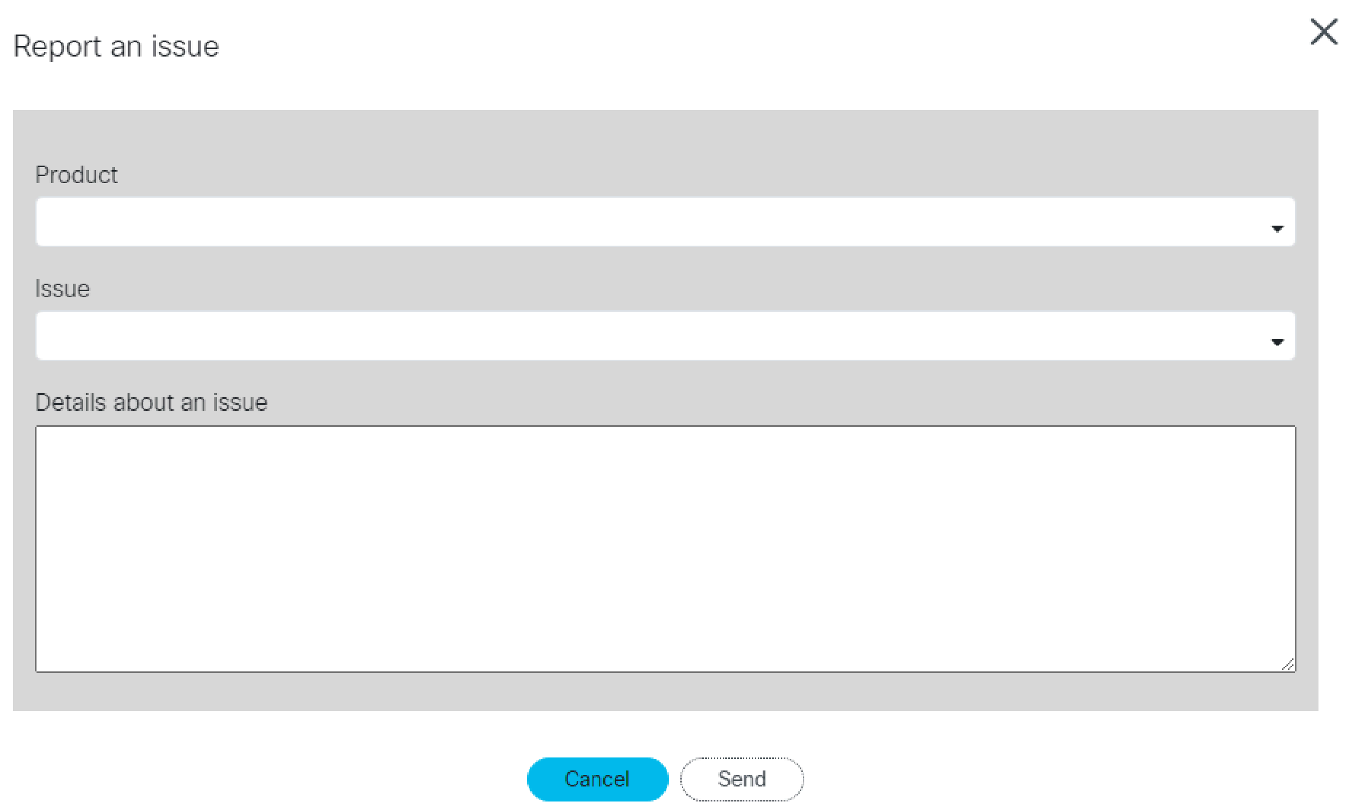
报告问题

在CSA平台顶部，Report A Problem部分允许您共享工具中检测到的任何问题。

此外，管理员还可以通过向CSA开发团队处理信息的位置发送邮件来提供反馈、意见或建议。

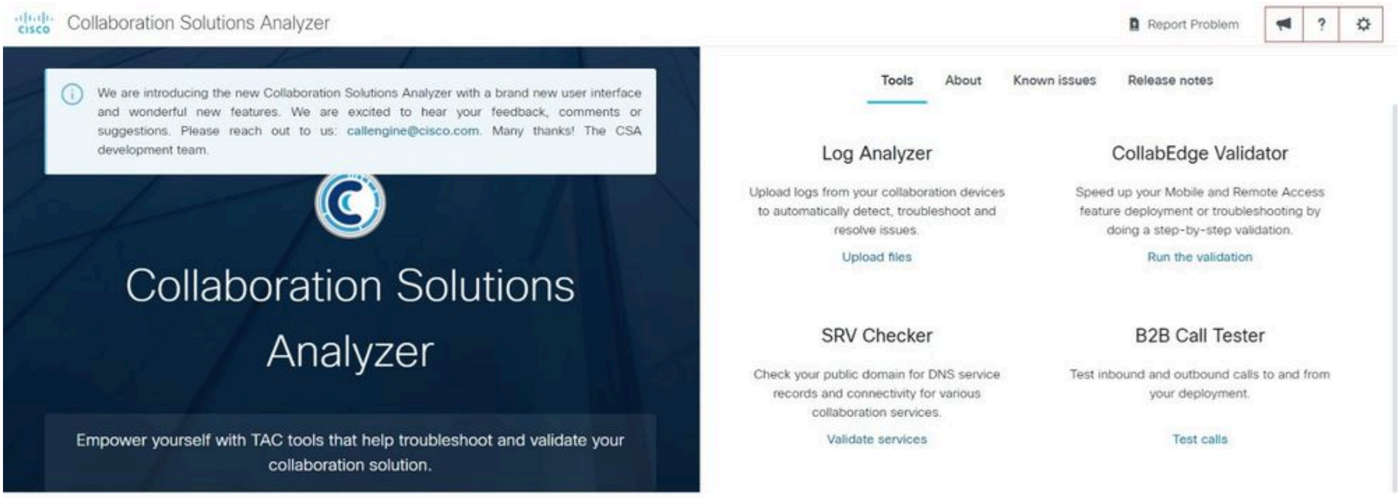


报告问题主页



报告问题

已启用三个图标，以允许用户提供反馈（麦克风图标）、查看用户文档（问号图标）和打开用户设置（齿轮图标）。



图标

支持相关信息

[配置CUBE和TDM网关的调试集合]

[贯穿思科IOS XE 17.5的思科统一边界元素配置指南]

[章节：SIP配置文件]

[在CUBE企业常见使用案例上使用SIP配置文件]