Fehlerbehebung bei CUBE über Collaboration Solutions Analyzer

Inhalt

Einleitung

In diesem Dokument werden die Tools Log Analyzer und SIP Profile Tester zur Fehlerbehebung bei CUBE im Collaboration Solutions Analyzer-Portal beschrieben.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Unified Border Element (CUBE) Enterprise
- Session Initiation Protocol (SIP)
- CUBE-Protokollsammlung (Debugging)

Erste Schritte

Collaboration Solutions Analyzer (CSA) ist eine Suite von Tools, die Ihre Collaboration-Lösung während ihres gesamten Lebenszyklus unterstützen. Es hilft bei der Identifizierung von Problemen und stellt bei Bedarf Pläne für Korrekturmaßnahmen bereit, die in jeder Phase der Collaboration-Lösung hilfreich sind.

Navigieren Sie zum Collaboration Solution Analyzer unter https://cway.cisco.com/csa-new/#/home

Hinweis: Die Verwendung des Chrome-Browsers stellt sicher, dass das Tool optimal funktioniert.

Überlegungen

Die Tools sind für ein CUBE-Gerät konzipiert, das SIP-zu-SIP-Anrufe verarbeitet. Die Tools unterstützen kein anderes Sprachprotokoll.

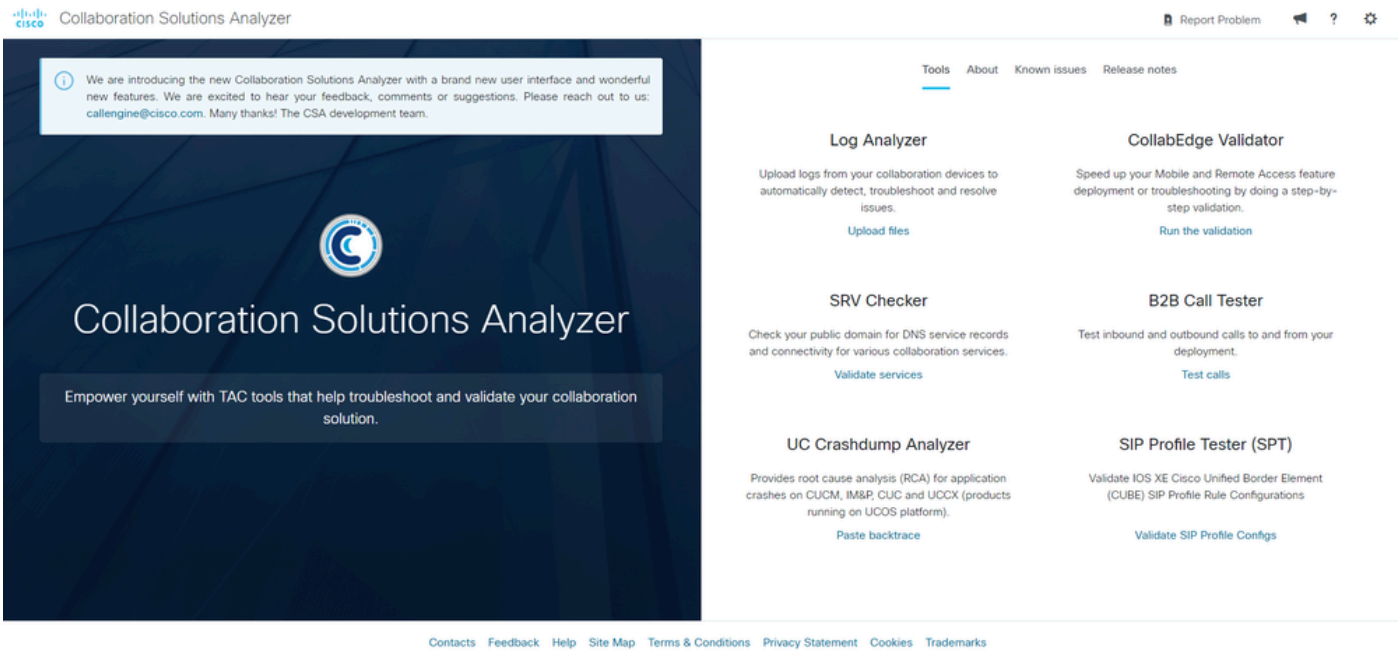
Log Analyzer verwendet CUBE-Protokolle (basierend auf dem Debugging von SIP-Nachrichten) für die Analyse.

Wenn Sie Hilfe zu einem anderen Sprachprotokoll benötigen, verwenden Sie den Cisco Support Assistant für TAC-Verträge unter https://supportassistant.cisco.com

Plattformbeschreibung

Die CSA-Plattform bietet die folgenden CUBE-Tools:

- Log Analyzer - Lädt Protokolle von CUBE und anderen Collaboration-Geräten hoch, um Probleme automatisch zu erkennen, zu beheben und zu beheben.
- SIP-Profiltester - Validierung der SIP-Profilkonfiguration



CSA-Startseite

Log Analyzer

Mit dem Log Analyzer-Tool können Administratoren die vom CUBE-Gerät verarbeitete Anrufsignalisierung untersuchen. Es bietet eine umfassende Analyse von Protokolldateien, einschließlich:

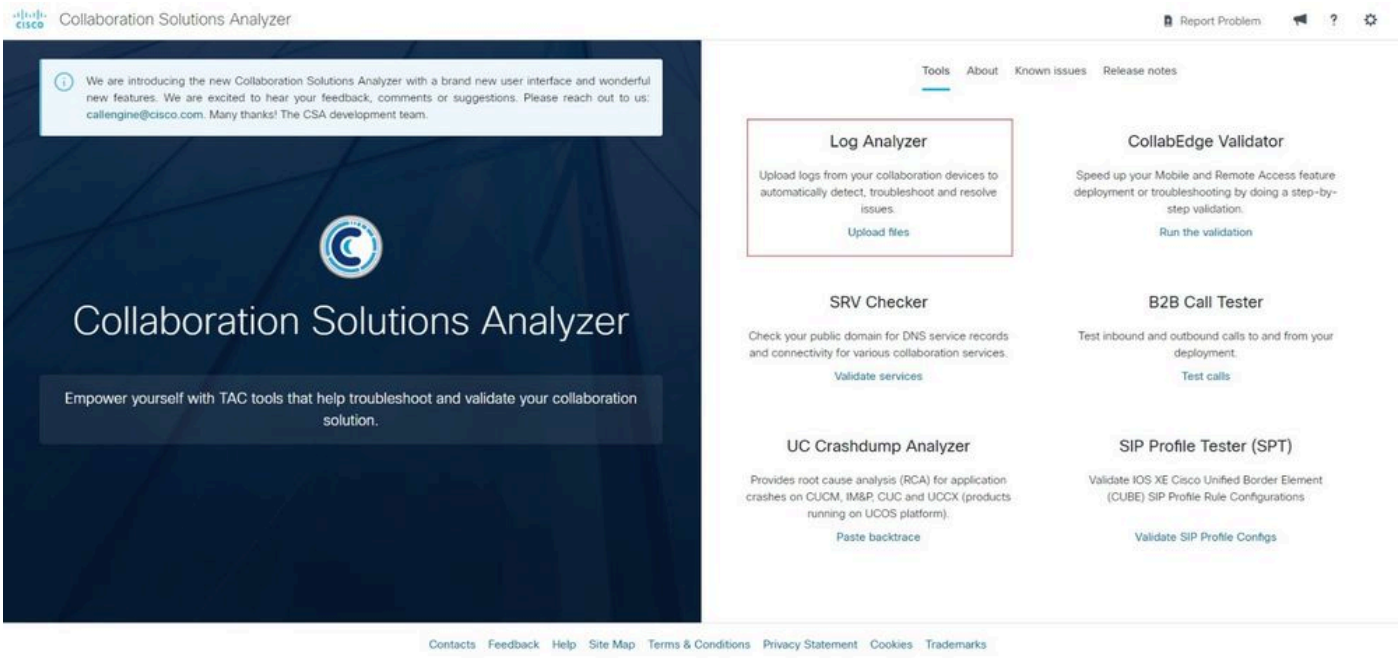
- Informationen zum Anrufabschnitt
- Leiterdiagramm
- Signalisierung

Hinweis: CUBE-Debugging (debug ccsip messages) von einem Aufruf, der vom CUBE verarbeitet wurde, muss zunächst gesammelt und in einer Textdatei gespeichert werden. In dieser Textdatei dürfen nur SIP-Debugging und keine andere Ausgabe, wie Befehle zum Anzeigen, enthalten sein.

CUBE-Protokolldateien hochladen

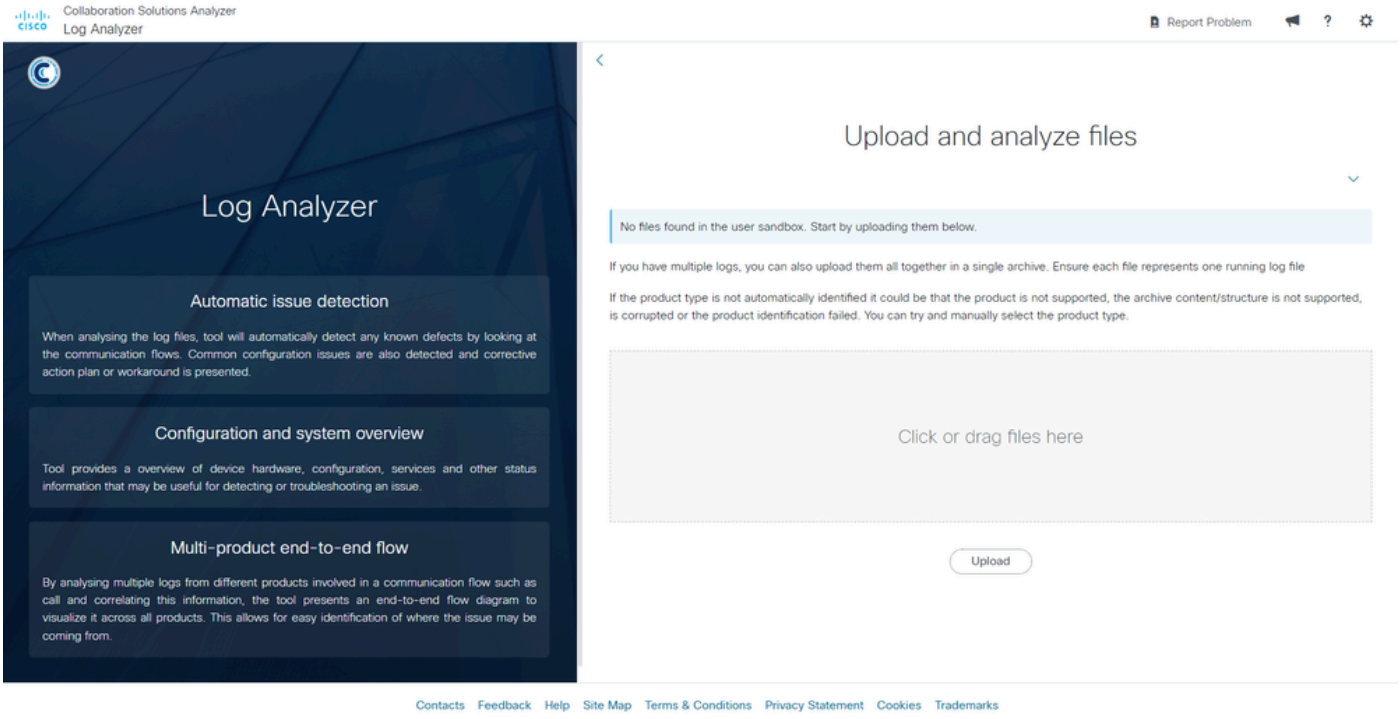
Navigieren Sie zum Collaboration Solution Analyzer unter https://cway.cisco.com/csa-new/#/home

Wählen Sie dann das Tool aus, indem Sie im Abschnitt Log Analyzer auf Dateien hochladen klicken.



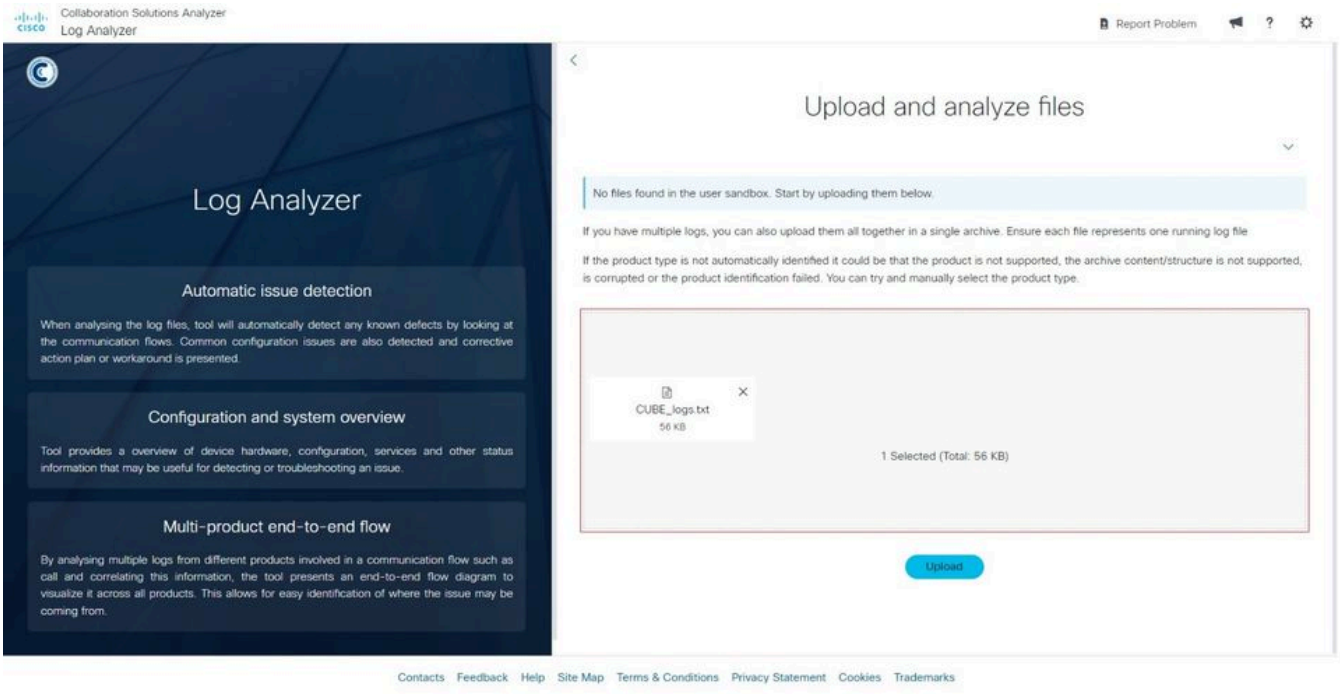
Log Analyzer - Startseite

Die Plattform zeigt den Werkzeugbildschirm an, auf dem eine Datei ausgewählt oder gezogen werden kann.



Hochladen der Protokollanalyse

Klicken Sie auf die Schaltfläche Upload, um das Hochladen der Datei für das zu analysierende Tool abzuschließen.

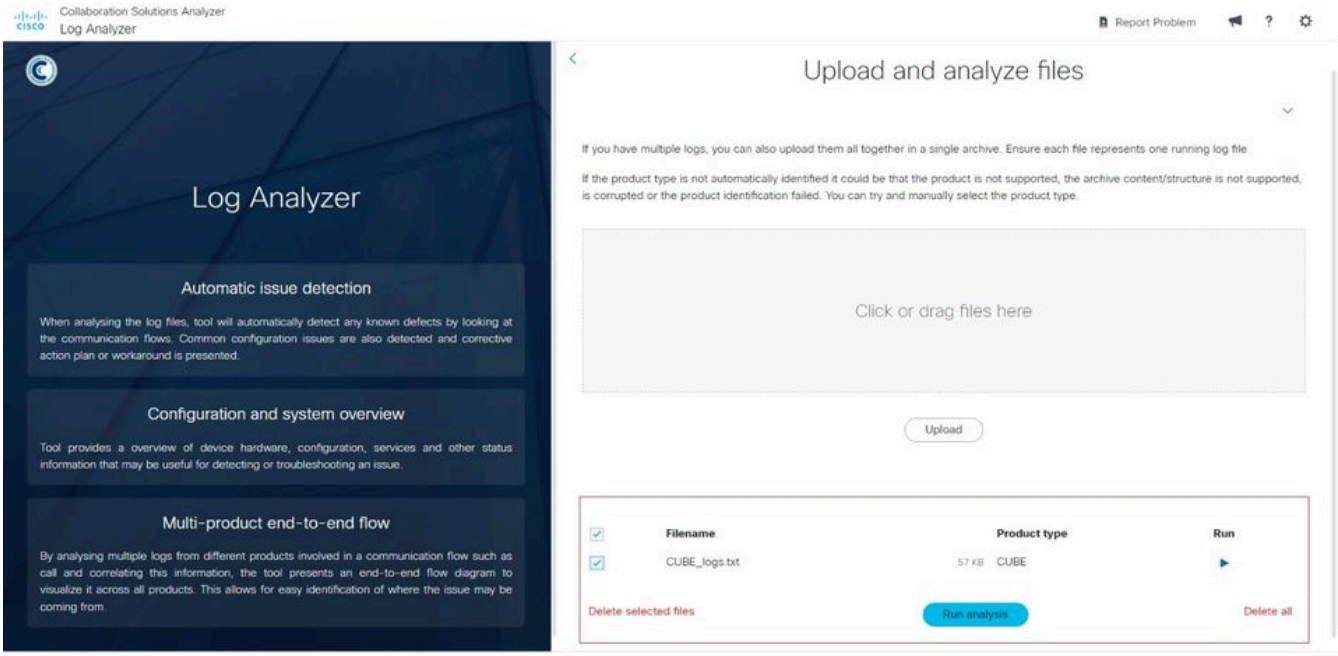


Upload-Datei von Log Analyzer

Nachdem Sie die Datei in das Tool hochgeladen haben, wählen Sie die zu analysierende(n) Datei(en) aus, indem Sie das entsprechende Kästchen markieren und dann auf die Schaltfläche

Analyse ausführen klicken.

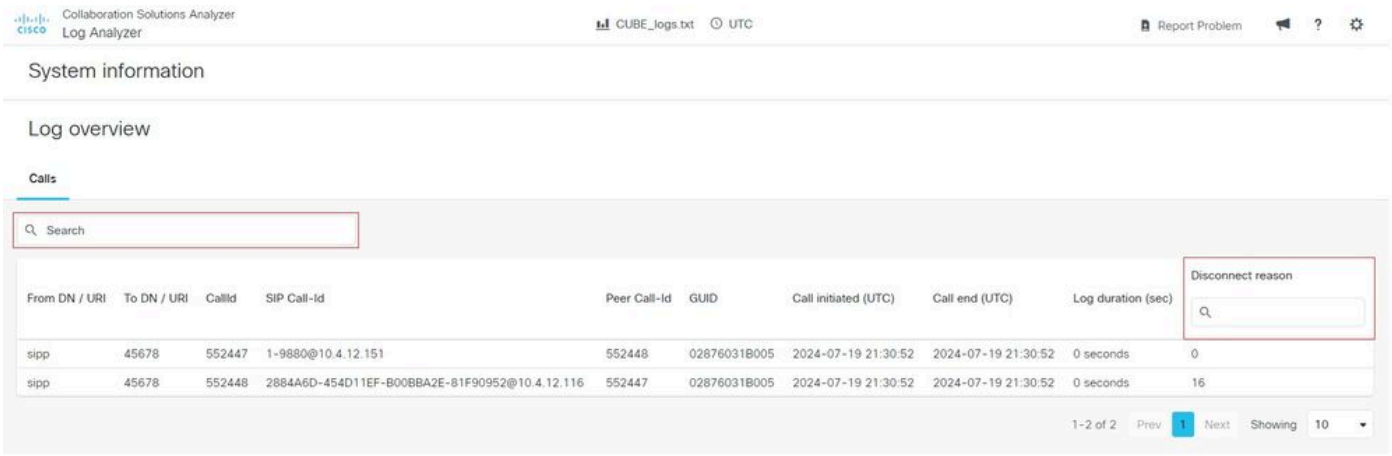
- Das System setzt den Produkttyp auf CUBE.
- In derselben Sitzung können mehrere Dateien analysiert werden.



Log Analyzer-Produkttyp

Das Tool analysiert alle in der Textdatei erfassten Signalisierungsaufrufe und zeigt eine Zusammenfassung der identifizierten Anrufabschnitte an. Sie können dann zwei Filter anwenden:

- Suche: Filtert Anrufsitzungen nach bestimmten Daten, z. B. gewählten Nummern.
- Suchen Sie nach "Grund für Verbindungstrennung", um Anrufsitzungen nach dem Grund für die Verbindungstrennung zu filtern.

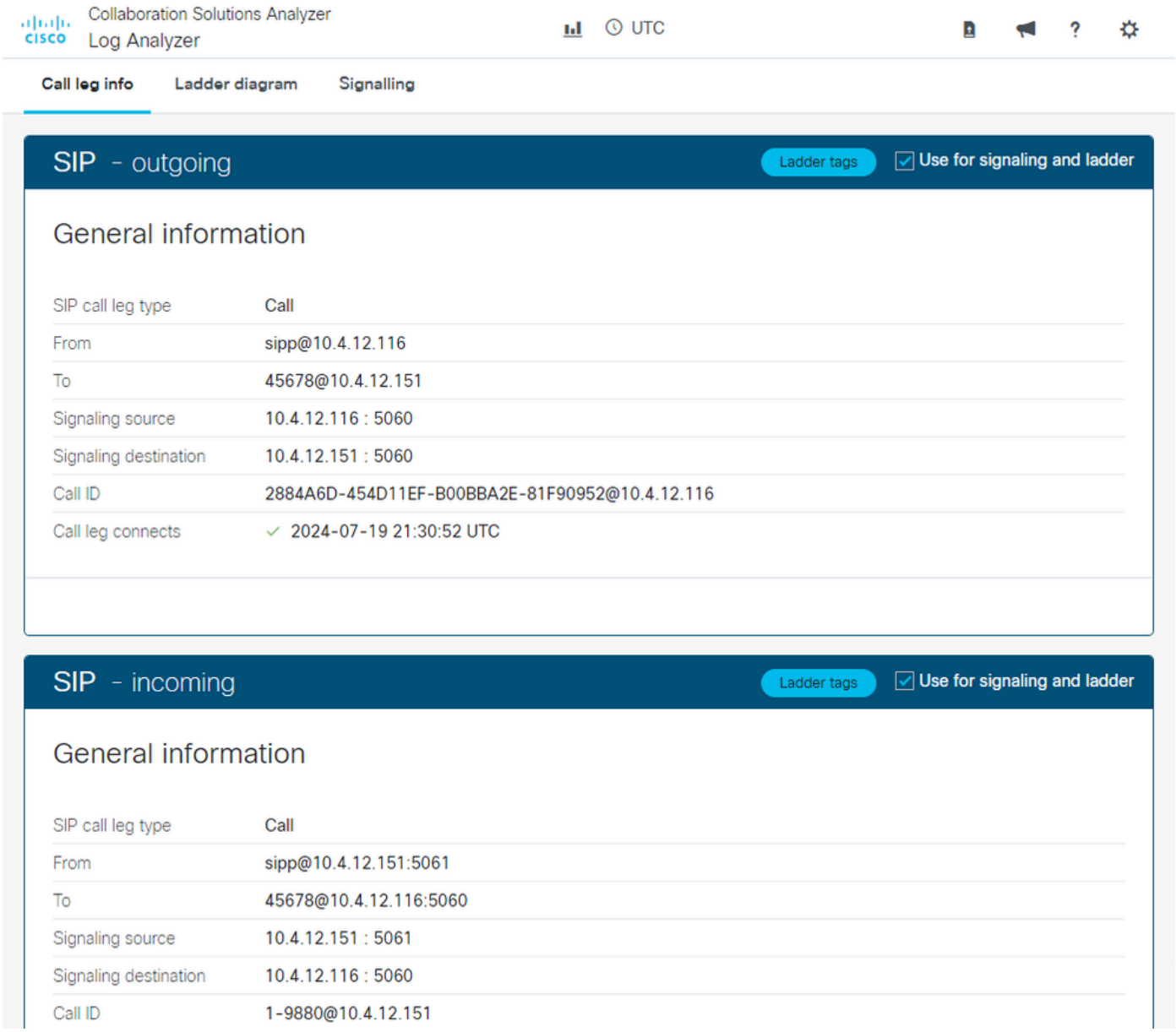


Um mit der detaillierten Analyse fortzufahren, wählen Sie die Gesprächsleitung aus, auf die Sie sich konzentrieren möchten, und das Tool zeigt die vollständige Analyse mit den Informationen zum Anrufabschnitt, dem Leiterdiagramm und der Signalisierung an.

Informationen zum Anrufabschnitt

In der ersten Phase werden die Anrufleitungsinformationen mit der Übersicht des Anrufs präsentiert:

- Typ der SIP-Anrufstrecke
- From (Von): Wird vom FROM-SIP-Header der INVITE-Nachricht abgerufen.
- An - Wird vom TO-SIP-Header der INVITE-Nachricht abgerufen.
- Signalisierungsquelle - IP-Adresse und Port des Quellgeräts. Abgerufen aus dem VIA-SIP-Header der INVITE-Nachricht.
- Signalisierungsziel - IP-Adresse und Port des Zielgeräts. Wird vom URI-SIP-Header der INVITE-Nachricht abgerufen.
- Anruf-ID: vom SIP-CALL-ID-Header der INVITE-Nachricht bezogen.
- Verbindung des Anrufzweigs - Zeitstempel der Anrufsitzung.

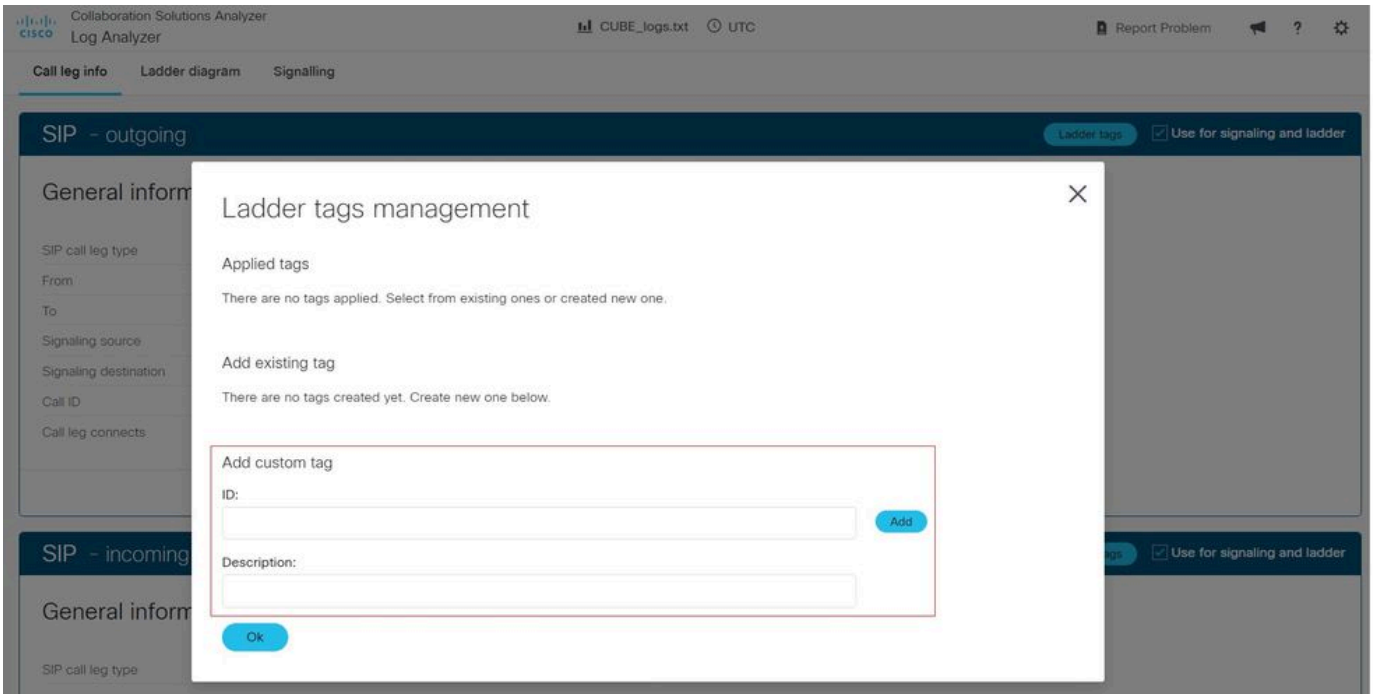


Log Analyzer-Anrufübertragungsinformationen

In diesem Abschnitt können Leitertags aktiviert werden, um Nachrichten im Leiterdiagramm hervorzuheben. Die Anwendung umfasst zwei Felder:

- ID: Geben Sie den gewünschten Parameter ein.
- Beschreibung: Fügen Sie eine Beschreibung des Parameters hinzu.

Klicken Sie auf die Schaltfläche Hinzufügen, um den Vorgang abzuschließen.



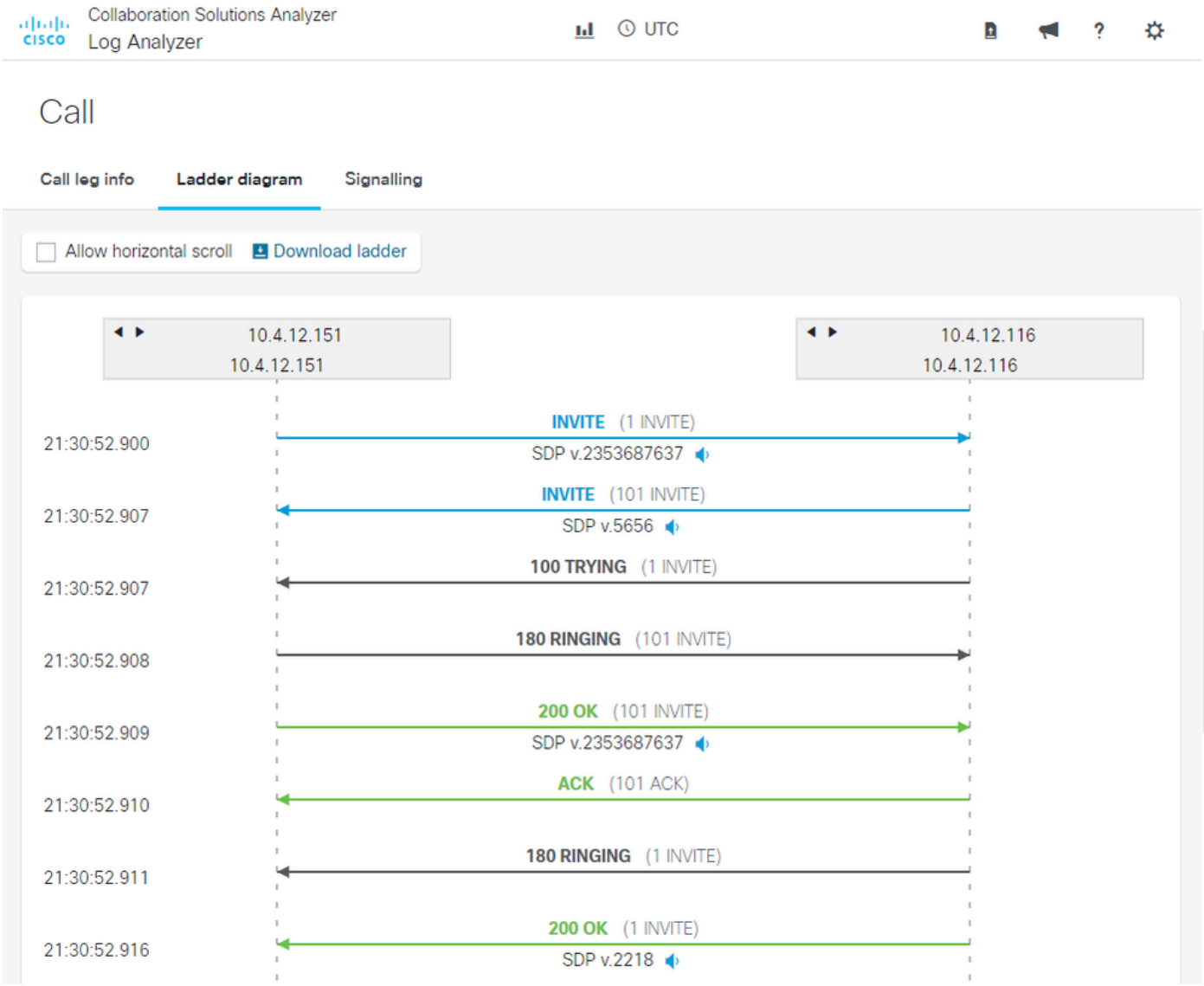
Leitermarkierungen für Protokollanalyse

Leiterdiagramm

In der zweiten Stufe wird ein Leiterdiagramm dargestellt, das die während des Gesprächs ausgetauschten SIP-Nachrichten visuell darstellt. Die Meldungen sind farblich gekennzeichnet, um eine einfache Identifizierung zu ermöglichen:

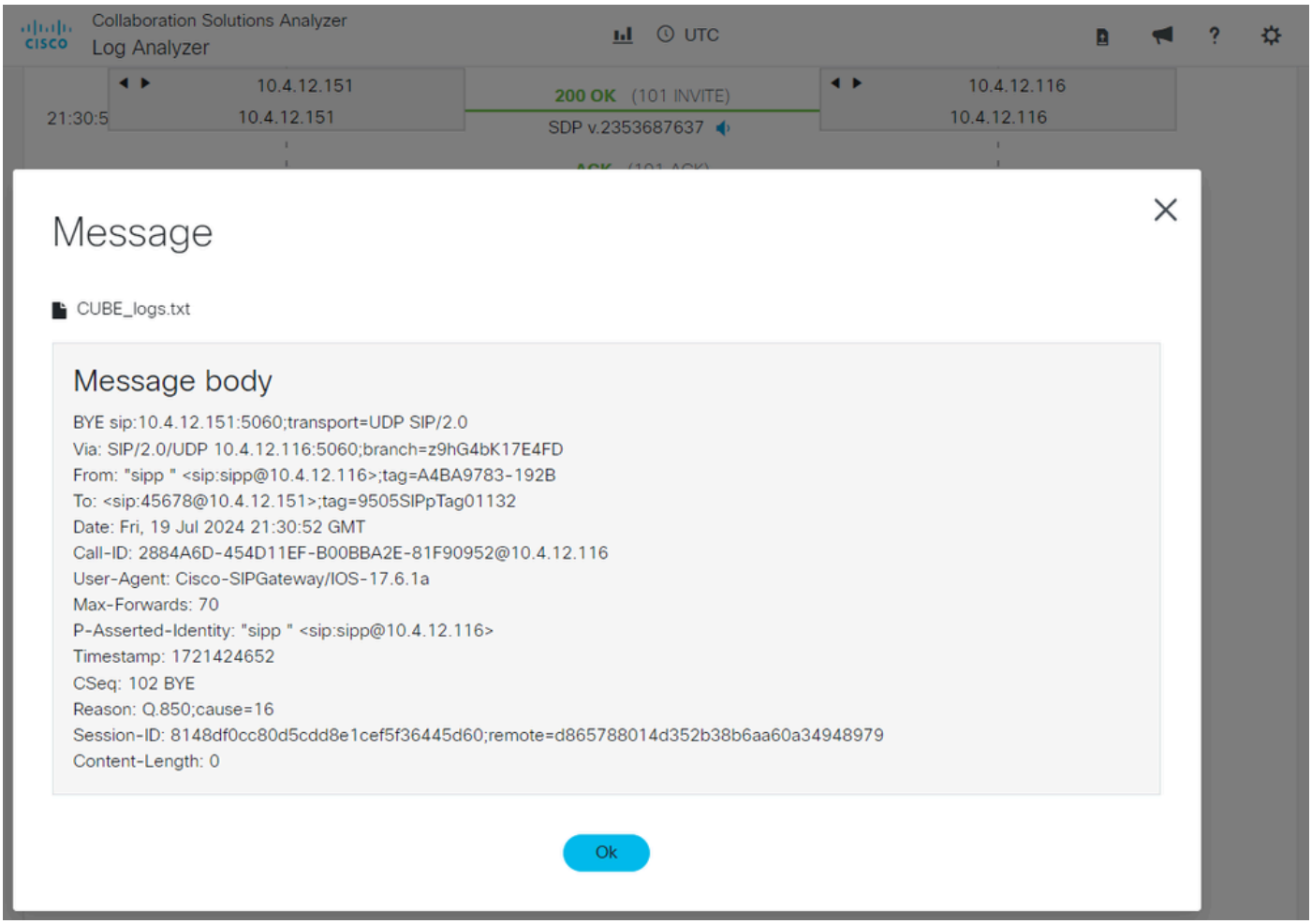
- Blaue Farbe - SIP-INVITE-Nachrichten
- Grüne Farbe - SIP 200 OK und ACK Nachrichten.
- Rote Farbe - SIP BYE-Nachrichten

Um eine Kopie des Diagramms herunterzuladen, klicken Sie auf die Schaltfläche Leiter herunterladen. Das Diagramm wird heruntergeladen und als PNG-Bilddatei gespeichert. Beachten Sie, dass diese Option nur verfügbar ist, wenn Sie den Google Chrome-Browser verwenden.



Leiterdiagramm der Protokollanalyse

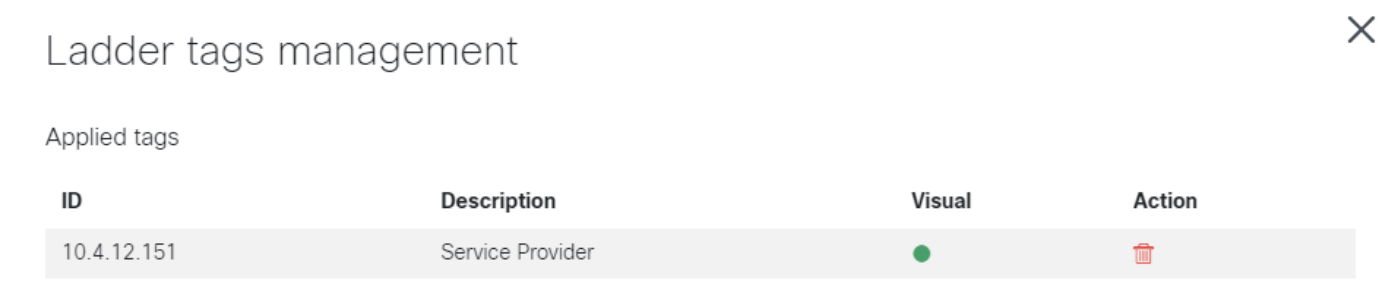
Mit diesem Tool kann der Administrator SIP-Nachrichten öffnen und deren Inhalt anzeigen. Klicke auf eine Nachricht, um sie zu öffnen.



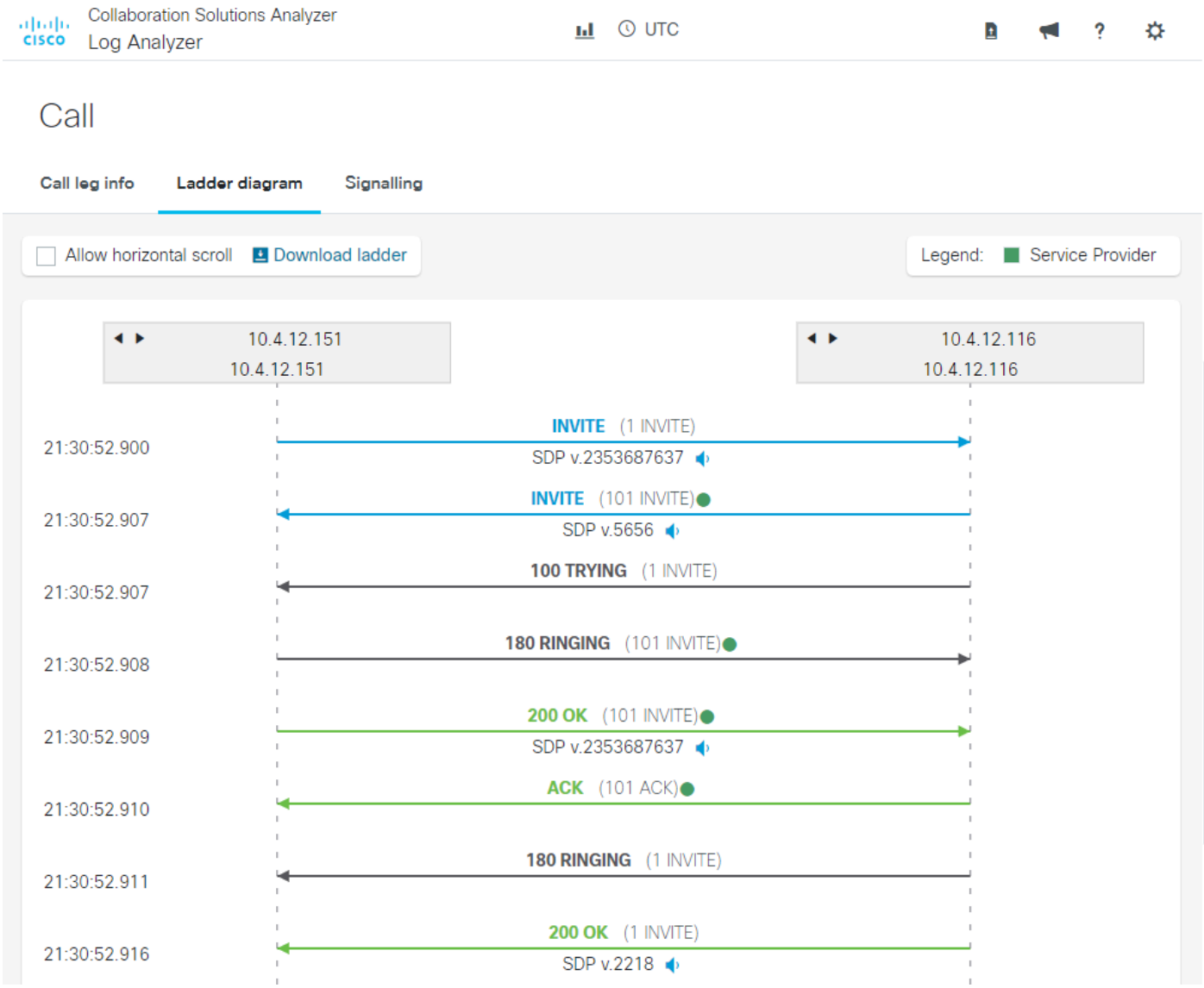
Leiterdiagrammmeldung der Protokollanalyse

Der Administrator kann Leitermarkierungen hinzufügen, um SIP-Nachrichten mit einem speziellen Punkt im Abschnitt "Anrufweiterleitungsinformationen" anzuzeigen. Für den Tag kann jeder Parameter verwendet werden, der in der SIP-Nachricht enthalten ist.

In diesem Beispiel wird eine IP-Adresse für den ID-Parameter verwendet, und es wird eine Beschreibung hinzugefügt. SIP-Nachrichten, die die IP-Adresse enthalten, werden mit einem Punkt markiert, um sie von anderen Nachrichten zu unterscheiden.

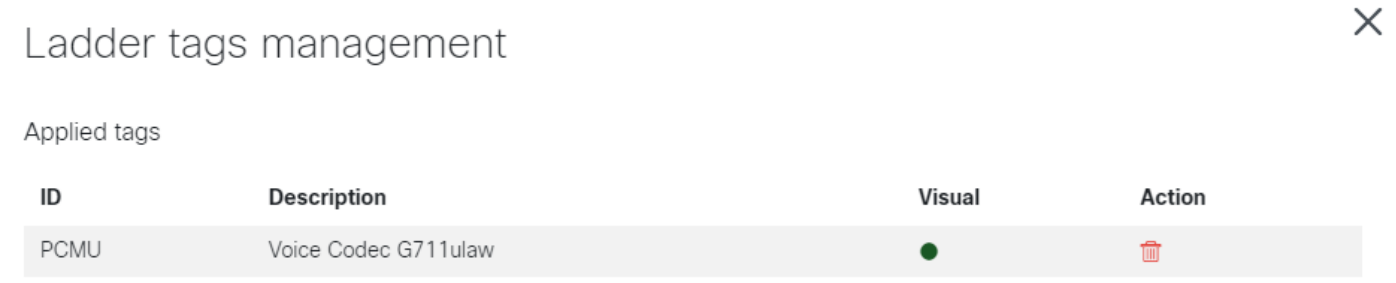


Leitermarkierungen 1 für Protokollanalyse

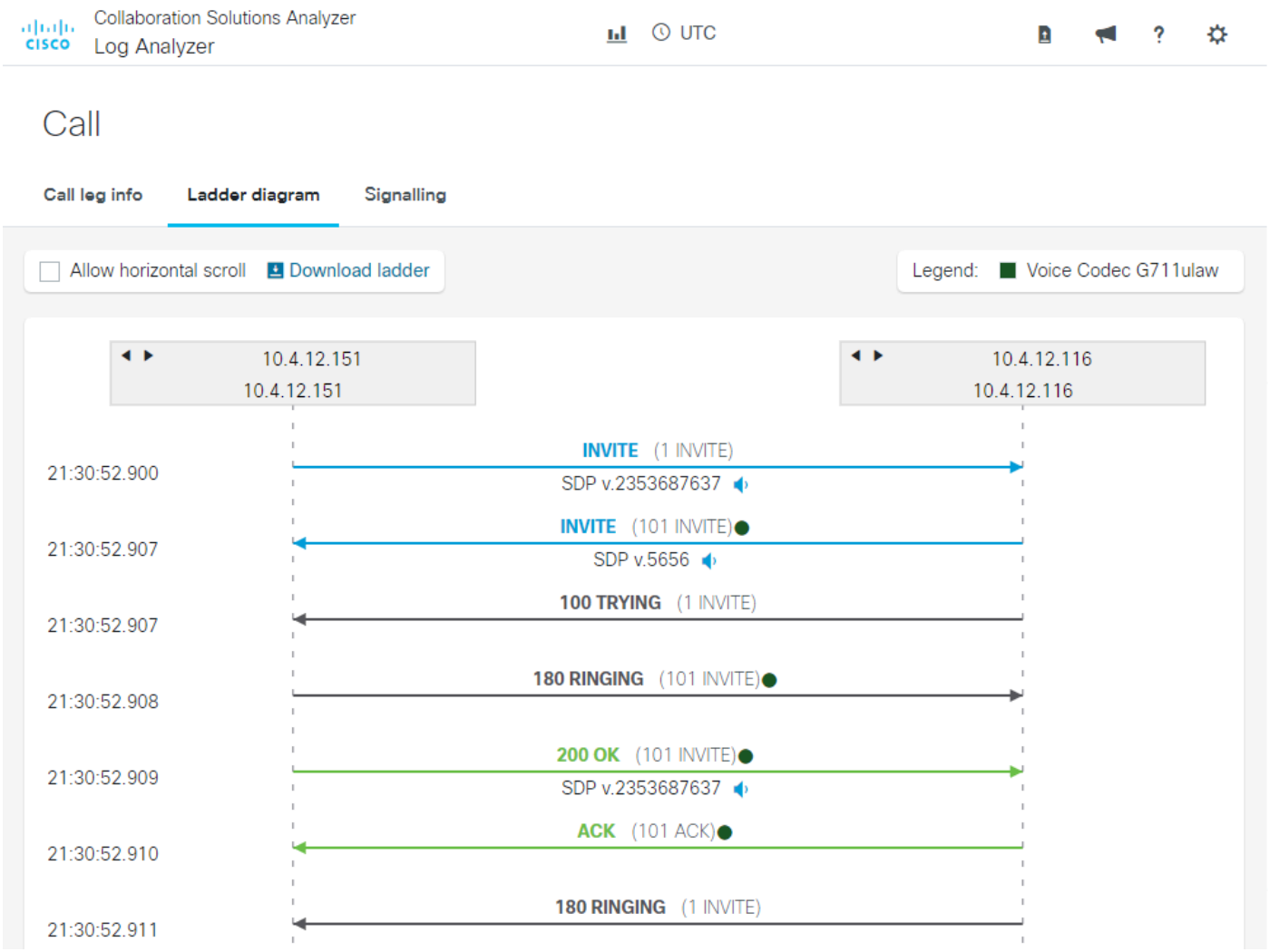


Protokoll-Analyzer-Leitermarkierungen 2

Ein weiterer Filter, mit dem SIP-Nachrichten von anderen Nachrichten unterschieden werden können, ist ein Sprach-Codec.



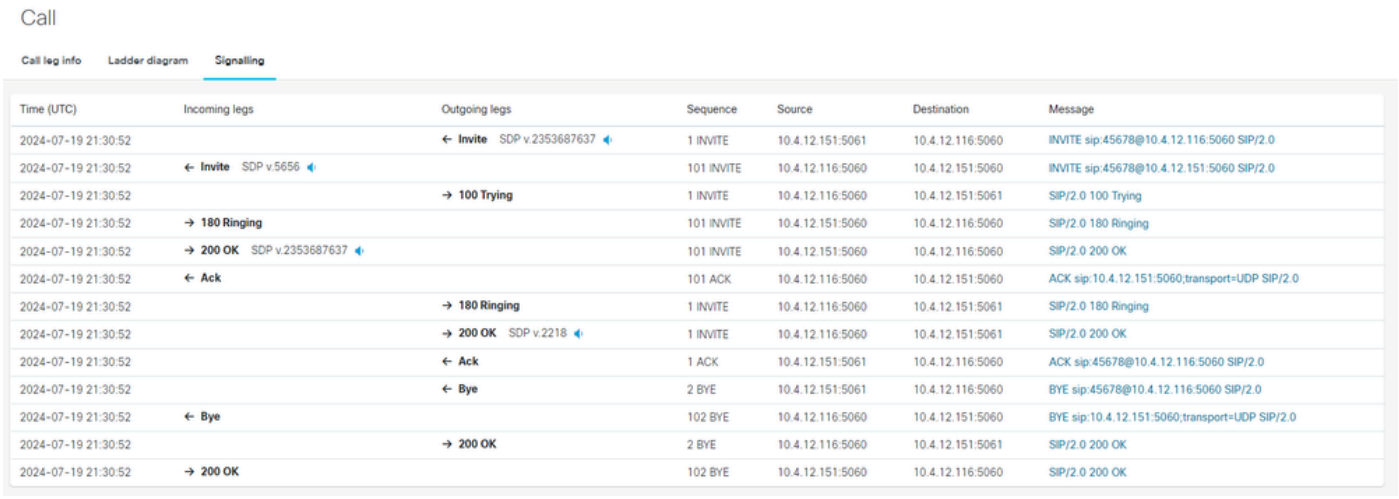
Leitermarkierungen der Protokollanalyse 3



Leitermarkierungen für Protokollanalyse 4

Signalisierung

Die letzte Stufe ist die Signalisierung, die die SIP-Nachrichten für beide CUBE-Abschnitte (ein- und ausgehend) anzeigt. Sie enthält die Quell- und Ziel-IP-Adressen. Klicken Sie auf, um die Nachricht anzuzeigen.



Protokoll-Analyzer-Signalisierung

Signalisierungsmeldung des Log Analyzer

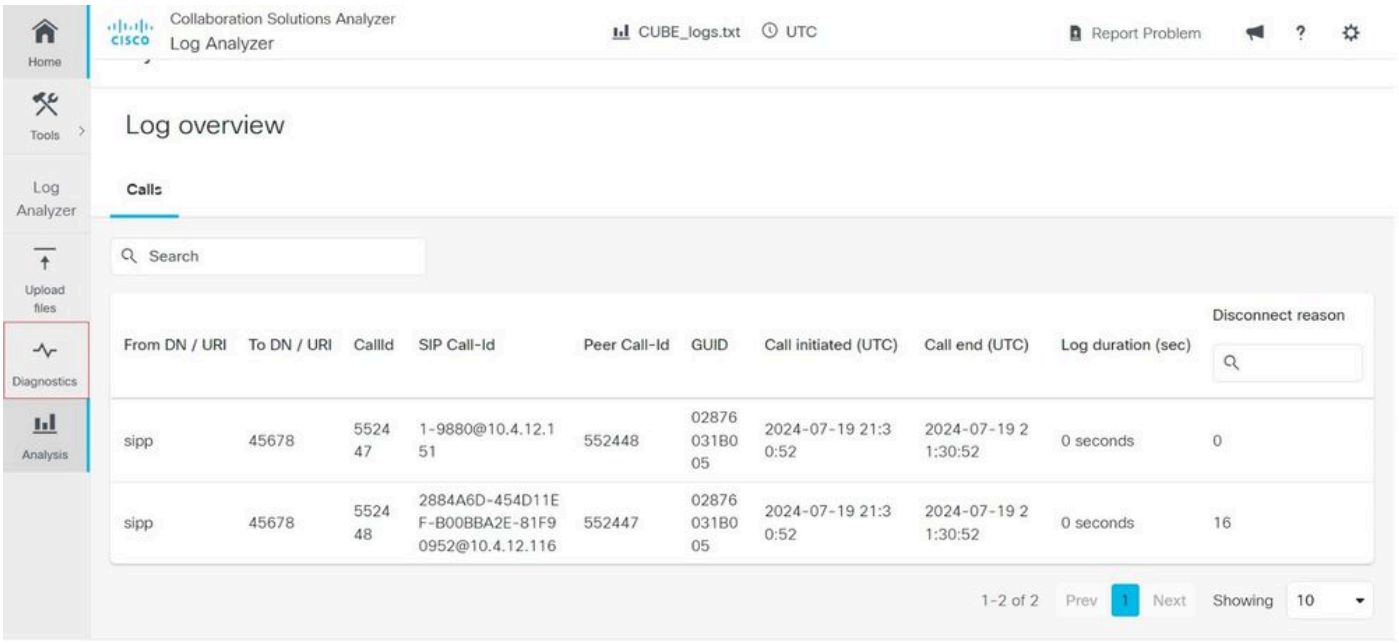
Diagnose

Alle Daten, die aus Protokollen analysiert werden, werden mit Diagnosesignaturen abgeglichen, die bekannte Fehler, häufig auftretende Probleme oder Fehlkonfigurationen erkennen und einen Korrekturmaßnahmenplan bereitstellen.

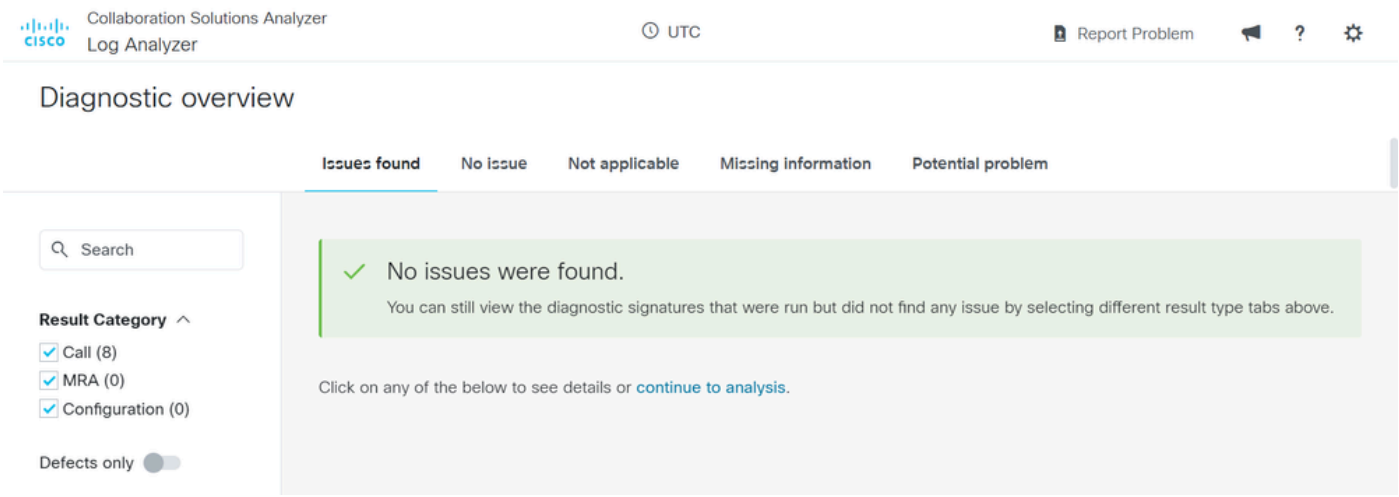
Nachdem ein in den Protokollen erfasster Anruf ausgewählt wurde, um die Anrufsübersichtsanalyse anzuzeigen, zeigt die CSA-Plattform den Abschnitt Diagnostics (Diagnose) an, der folgende Informationen enthält:

- Gefundene Probleme
- Fehlende Informationen
- Potenzielles Problem

Eine Umschalttaste kann aktiviert werden, um nur Defekte zu filtern und anzuzeigen.



Diagnose-Startseite für Protokollanalyse



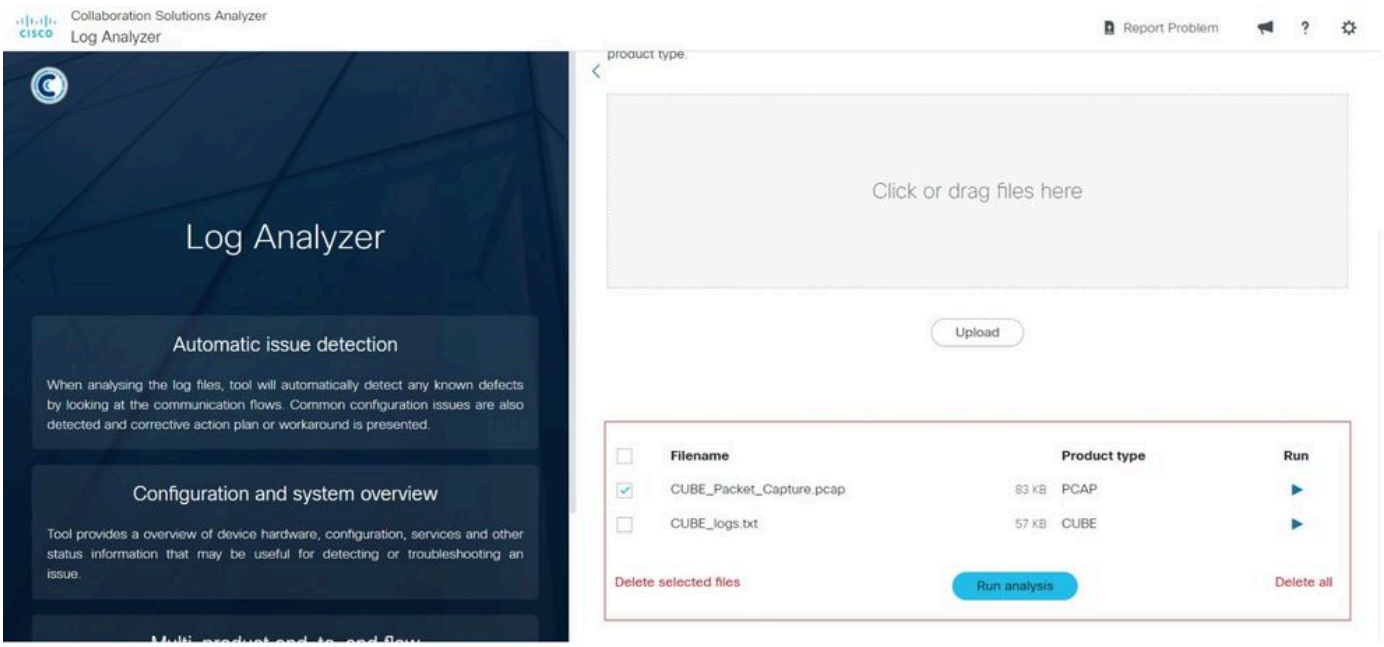
Übersicht: Log Analyzer-Diagnose

CUBE-Paketerfassung

Die Paketerfassung ist ein Dateipuffer, der erstellt wird, um eine Kopie der tatsächlichen Pakete an einer CUBE-Netzwerkschnittstelle oder einem beliebigen Sprachnetzwerkgerät zu sammeln. Diese Datei kann mit einer Netzwerkanalysesoftware wie Wireshark geöffnet und analysiert werden.

Das Log Analyzer Tool wurde um einen Packet Capture Analyzer erweitert, der pcap- oder pcapng-Dateiformate verarbeiten kann und eine Zusammenfassung der Sitzungs- und Netzwerkstatistiken bietet, die aus Anrufen erfasst werden.

Die Paketerfassungsdatei muss wie die CUBE-Protokolldatei in das Log Analyzer-Tool hochgeladen werden. Das System bestimmt den Produkttyp als PCAP.



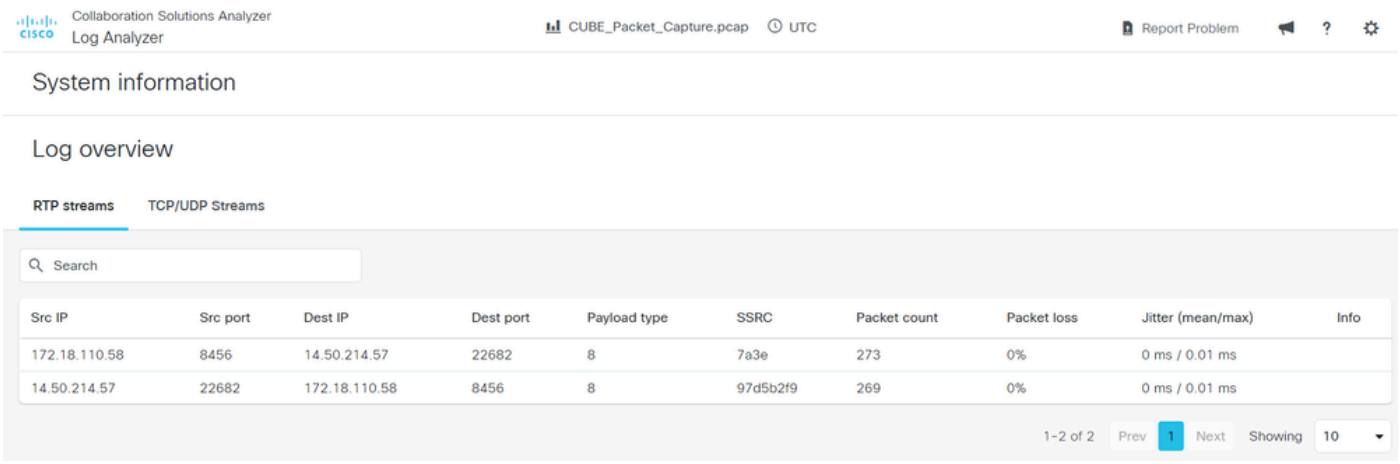
Protokolldatei zur Paketerfassung

Sobald die Schaltfläche Analyse ausführen aktiviert ist, analysiert das Log Analyzer-Tool die Informationen und bietet eine Zusammenfassung der erfassten Sitzungen in zwei Spalten:

- RTP-Streams
- TCP-/UDP-Streams

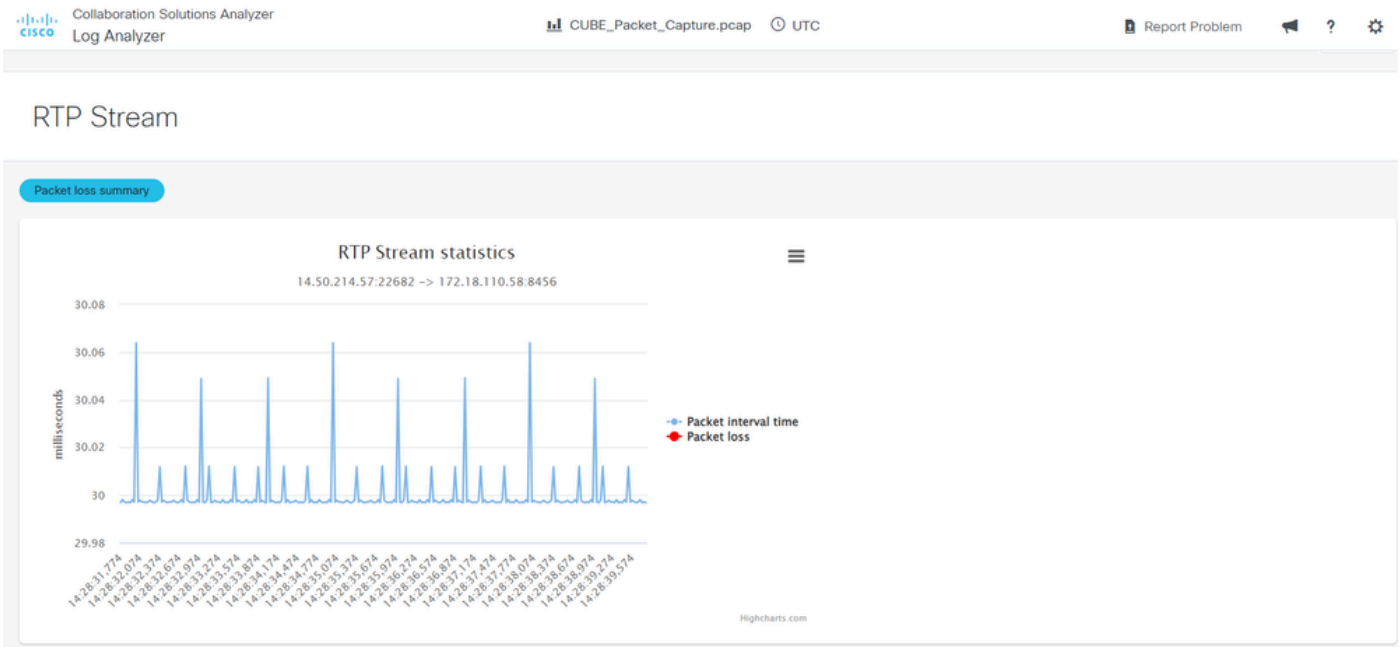
Hinweis: Wenn die Paketerfassung SRTP-Streams enthält, wird dies in der Spalte "RTP-Streams" angezeigt, und es wird eine Netzwerkanalyse durchgeführt. Der Audioteil eines SRTP-Streams wird nicht decodiert.

Wählen Sie eine Sitzung aus der Spalte "RTP-Streams" aus, und das Tool zeigt die RTP-Stream-Statistiken für diese Verbindung an. Wenn der Stream von den Netzwerkbedingungen beeinflusst wird, muss der Parameter "Packet Loss" (Paketverlust) mit roten Punkten gekennzeichnet werden.



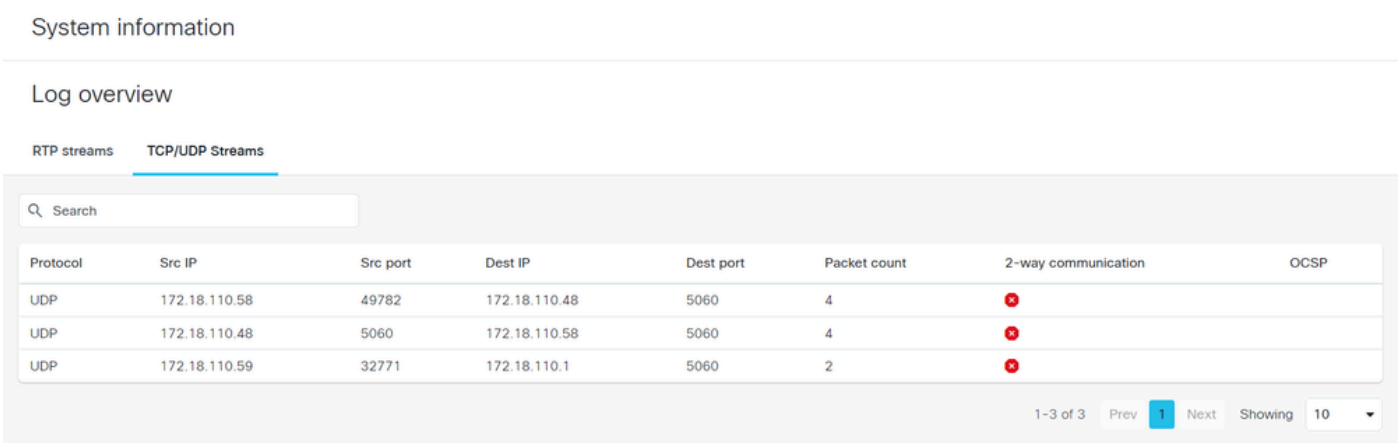
Log Analyzer - PCAP-Analyse

Die RTP-Flussstatistik kann in einem Textdateiformat heruntergeladen werden, das eine Zusammenfassung des Paketverlusts enthält. Klicken Sie auf die Schaltfläche Packet Loss Summary (Paketverlustübersicht), um die Datei herunterzuladen.



Log Analyzer - PCAP-RTP-Stream

Bei TCP-/UDP-Streams zeigt das System die Zusammenfassung der aufgezeichneten Sitzungen an.



Log Analyzer PCAP TCP UDP-Streams

SIP-Profiltester (SPT)

SIP-Profile (Session Initiation Protocol) dienen dazu, eingehende und ausgehende SIP-Nachrichten zu ändern, um die Kompatibilität zwischen verschiedenen Geräten sicherzustellen. Mit dem Tool "SIP Profile Tester" können Sie Ihre Konfiguration validieren, bevor Sie sie in einer Live-Umgebung bereitstellen.

Das SIP-Profil-Tool besteht aus drei Abschnitten:

- SIP Profile Rules (SIP-Profilregeln): Fenster zum Einfügen der zu testenden SIP PROFILE-Regeln
- SIP-Nachricht zum Anwenden von Regeln - Fenster zum Einfügen der SIP-Nachricht, in die die Regeln angewendet werden sollen.
- SIP-Nachricht zum Kopieren von - (optional) Fenster zum Einfügen einer SIP-Nachricht, falls die Konfiguration einer Kopierliste getestet wurde. Bei einer Konfiguration der Kopierliste wird der Inhalt eines von einem Gerät empfangenen eingehenden Headers in einen ausgehenden Header kopiert.

Das Tool enthält 2 Schaltflächen zum Verwalten der Tests:

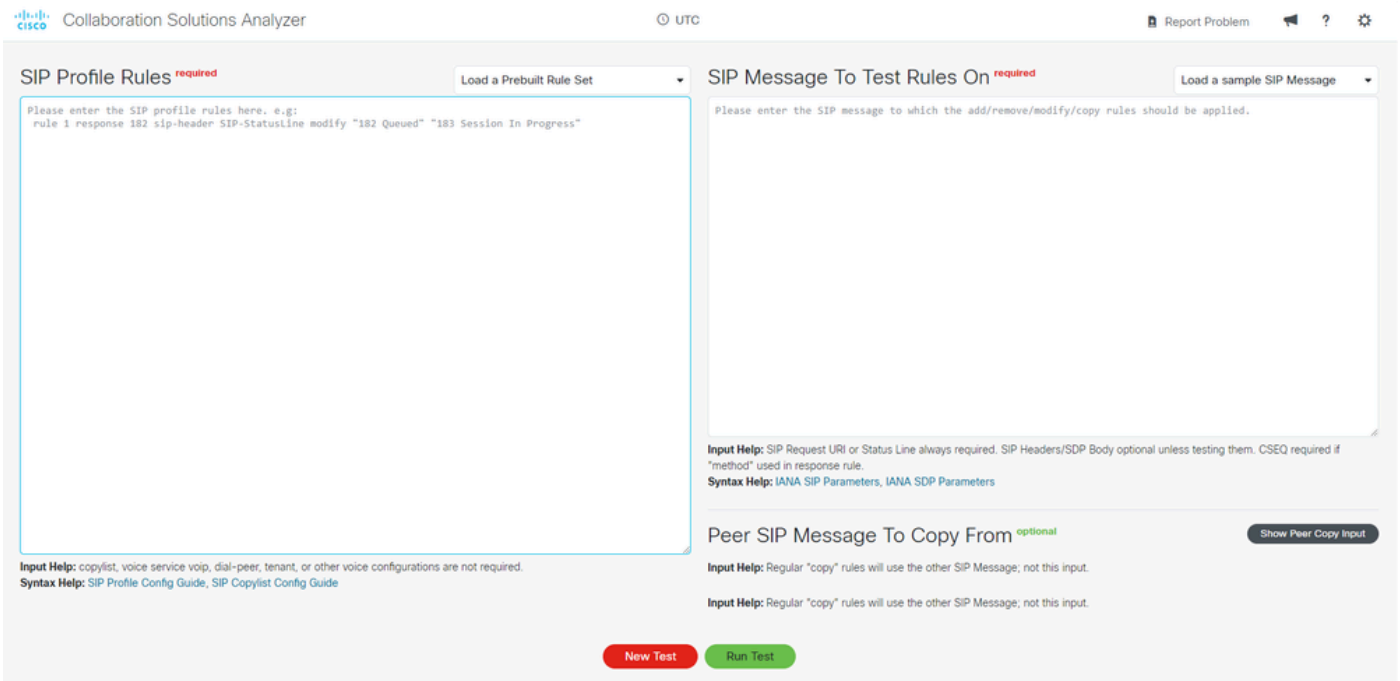
- Grüne Schaltfläche - So führen Sie einen Test aus.
- Rote Schaltfläche - Zum Zurücksetzen und Löschen von Einstellungen.

Nachdem Sie die grüne Schaltfläche zum Ausführen des Tests ausgewählt haben, zeigt das Tool folgende Optionen an:

- Roter Knopf - Neuer Test
- Blaue Schaltfläche - Eingaben anzeigen

Hervorhebung der Ergebnisse der ursprünglichen/geänderten SIP-Nachricht:

- Blaue Farbe: Geänderte SIP-Header oder SDP-Haupttext werden in beiden Nachrichtenbereichen blau hervorgehoben.
- Grüne Farbe: Hinzugefügte SIP-Header oder SDP-Body werden nur im Ergebnis der geänderten SIP-Nachricht grün hervorgehoben.
- Rote Farbe: Entfernte SIP-Header oder SDP-Body werden nur im ursprünglichen SIP-Nachrichtenergebnis rot hervorgehoben.



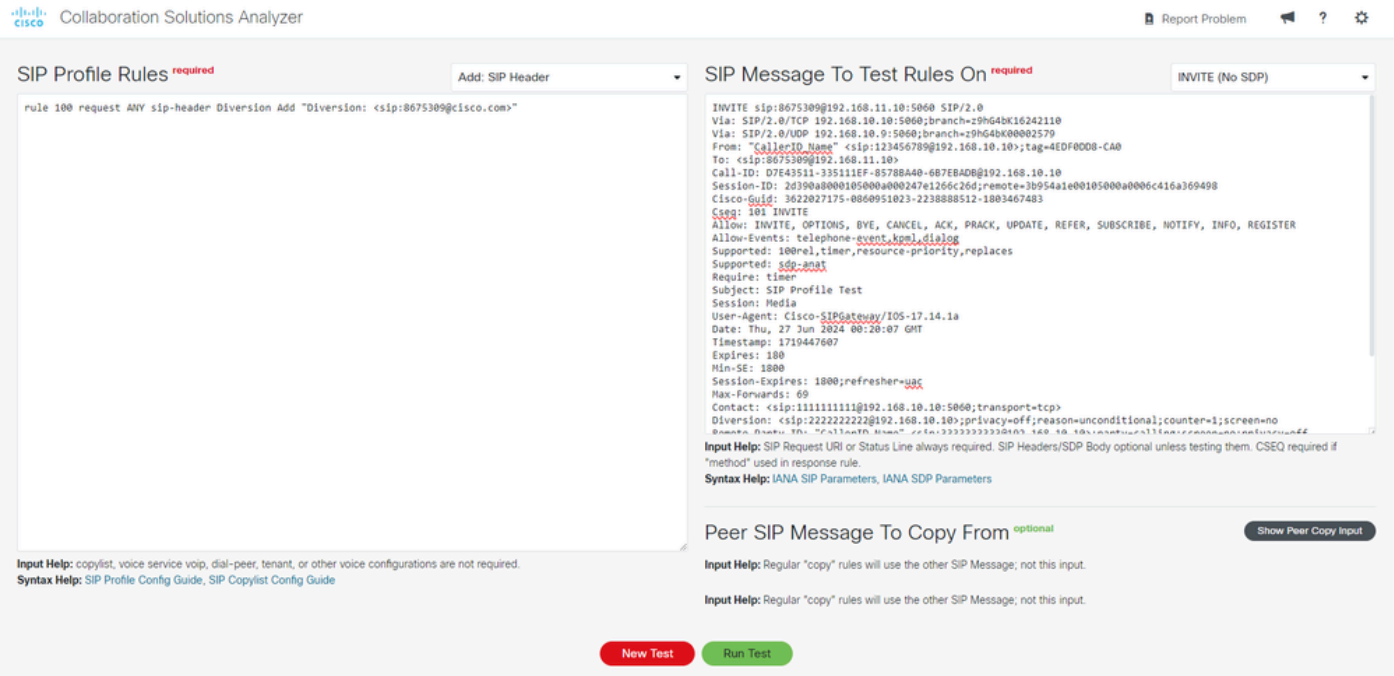
SIP-PROFIL - Startseite

Beispiel eines vordefinierten SIP-Profils

Das Tool enthält vordefinierte Beispiele zur Vereinfachung von Tests. Oben in jedem Fenster befindet sich ein Anwendungsfeld zur Auswahl dieser Beispiele.

Verwenden einer vordefinierten Konfiguration:

1. Klicken Sie auf Vordefinierten Regelsatz laden, und wählen Sie Hinzufügen: SIP-Header aus.
2. Klicken Sie auf Load a Sample SIP Message, und wählen Sie INVITE (No SDP) aus.
3. Wählen Sie die grüne Schaltfläche Test ausführen, um den Test auszuführen.

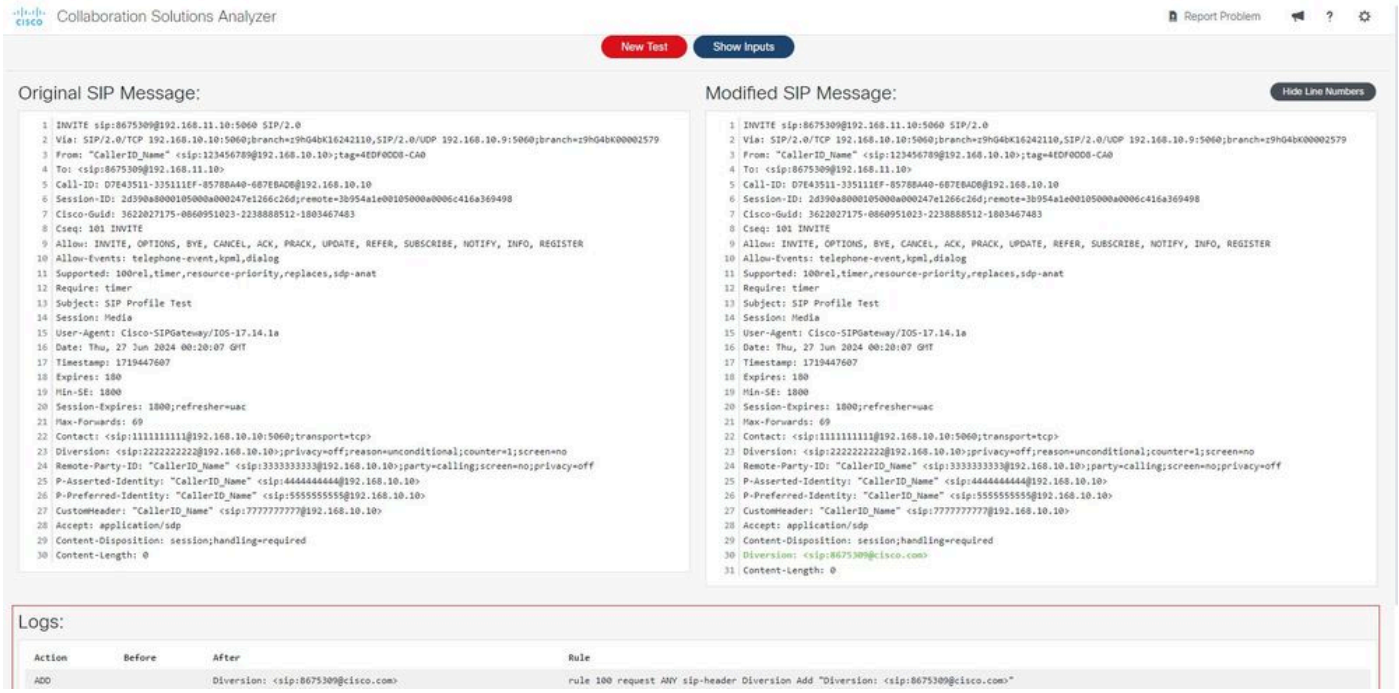


SIP-PROFIL vorinstalliert

Das Tool zeigt einen neuen Bildschirm mit den Testergebnissen an:

Geänderte SIP-Nachricht

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



SIP-PROFIL - Vorerstelltes Add-Beispiel

Dies ist ein Beispiel für das Ändern/Hinzufügen/Entfernen der Hervorhebung:

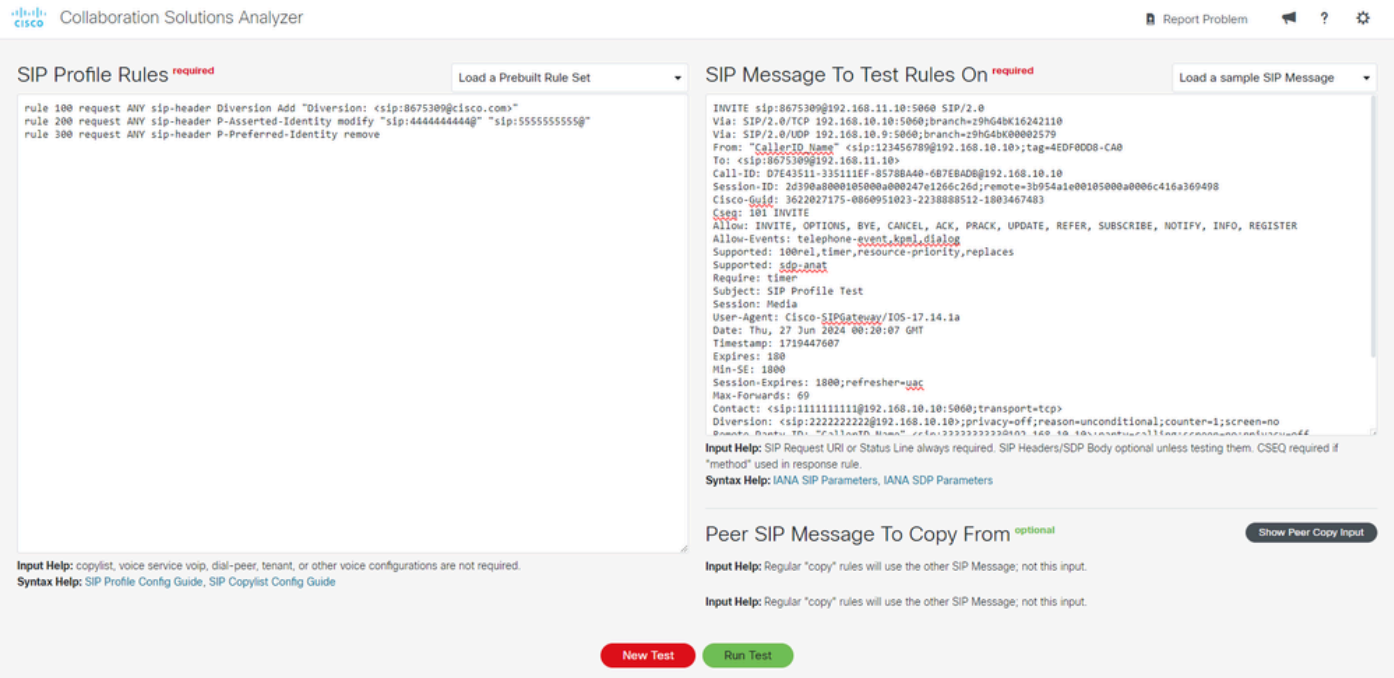
SIP-Profilregeln

```
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-Nachricht an Testregeln auf

```
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-PROFIL Ändern Hinzufügen Beispiel entfernen

Um das Ergebnis anzuzeigen, klicken Sie auf Test ausführen.

Ursprüngliche SIP-Nachricht

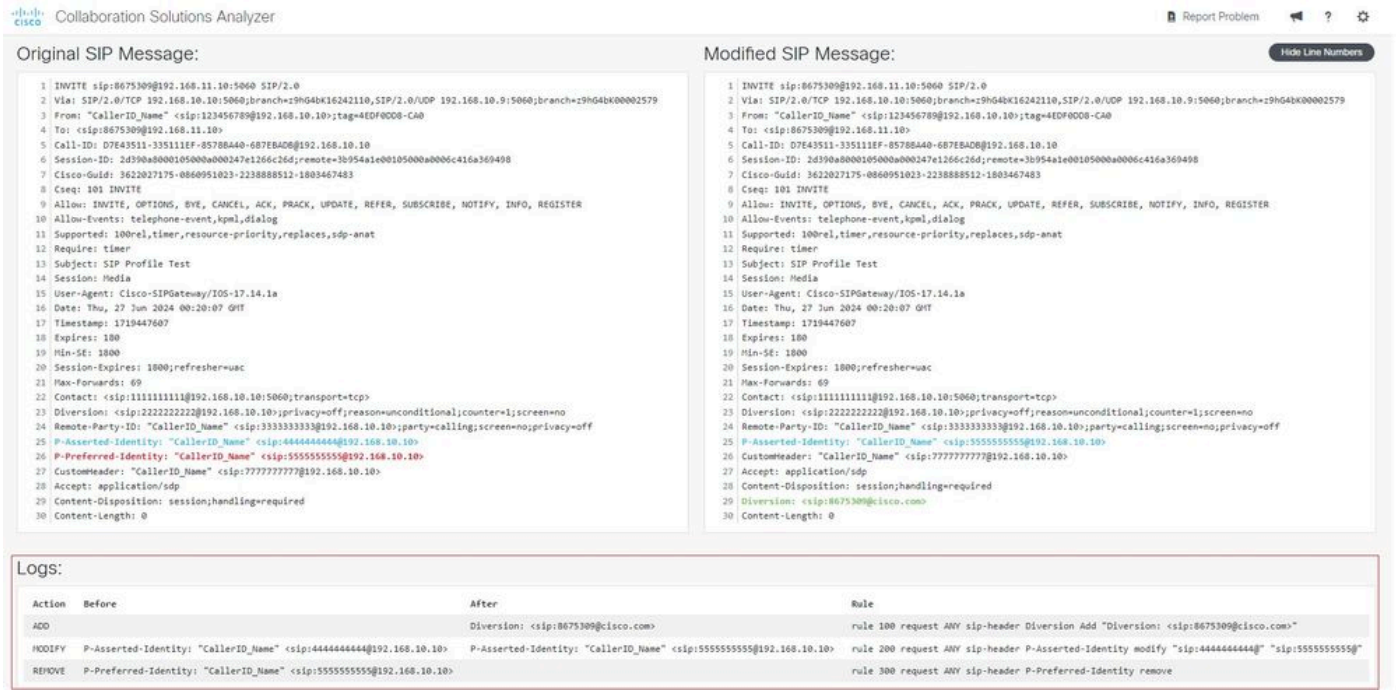
```
MODIFIED (BLUE) - P-Asserted-Identity: "CallerID_Name"

        4444444444@192.168.10.10>

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

Geänderte SIP-Nachricht

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



SIP-PROFIL Ändern Hinzufügen Entfernen Beispiel 2

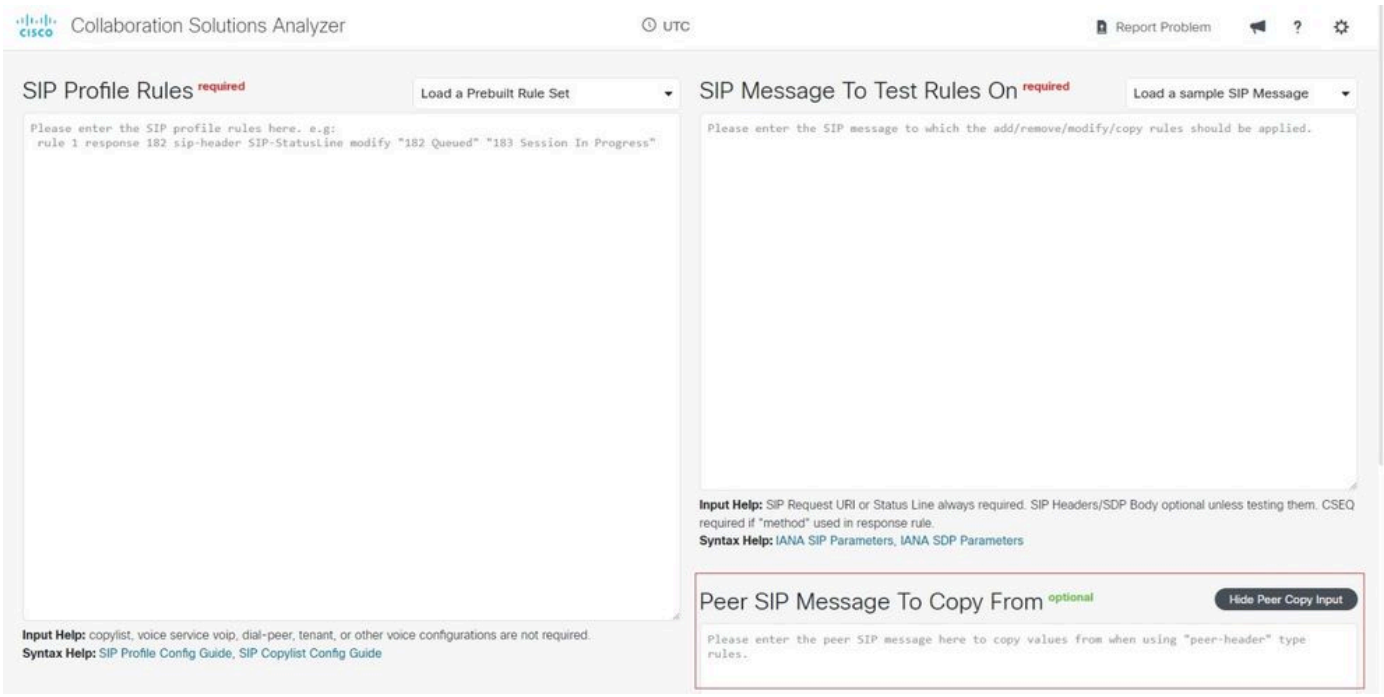
Copylist SIP-Profil

Zum Kopieren von Inhalten aus einem eingehenden Header, die ein Gerät empfängt, in einen ausgehenden Header (SIP-Copylist) können die folgenden Tool-Eingaben verwendet werden:

- Flussdiagramm: Eingehende SIP-Nachricht — > CUBE — > Geänderte SIP-Nachricht

- Zu kopierende SIP-Nachricht - SIP-Nachricht, von der kopiert werden soll.
- SIP-Nachricht an Testregeln an - SIP-Nachricht zum Anwenden von Regeln.

Um den Abschnitt Von Peer-SIP-Nachricht kopieren zu aktivieren, muss die Option Peer-Copy-Eingabe anzeigen aktiviert sein. Klicken Sie auf "Peerkopie-Eingabe ausblenden", um diesen Abschnitt auszublenden.



SIP-PROFILE - Copyright

Dies ist ein Beispiel für SIP-Regeln, eingehende und geänderte SIP-Nachrichten:

SIP-Profilregeln

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

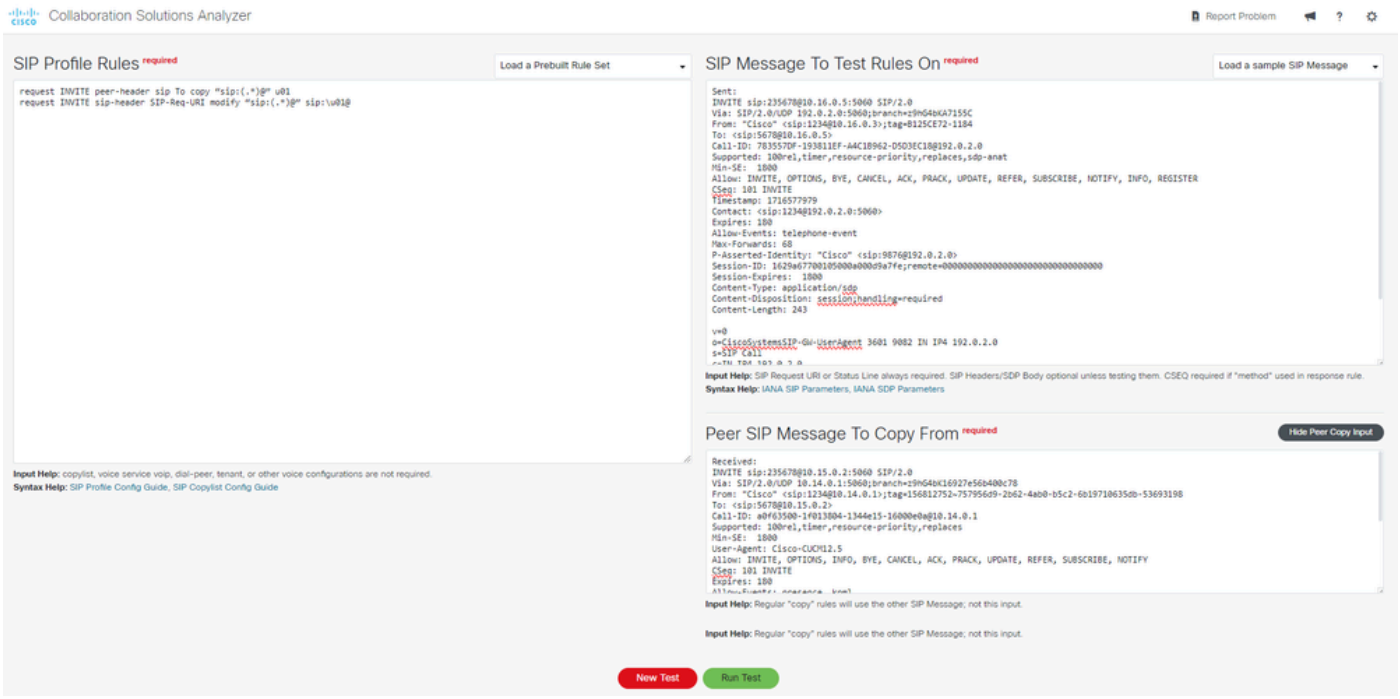
SIP-Nachricht zum Anwenden von Regeln

```
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-Nachricht zum Kopieren.

```
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 - Beispiel einer Copylist

Klicken Sie auf die Schaltfläche Test ausführen, um das Tool zu starten.

Registrieren kopieren

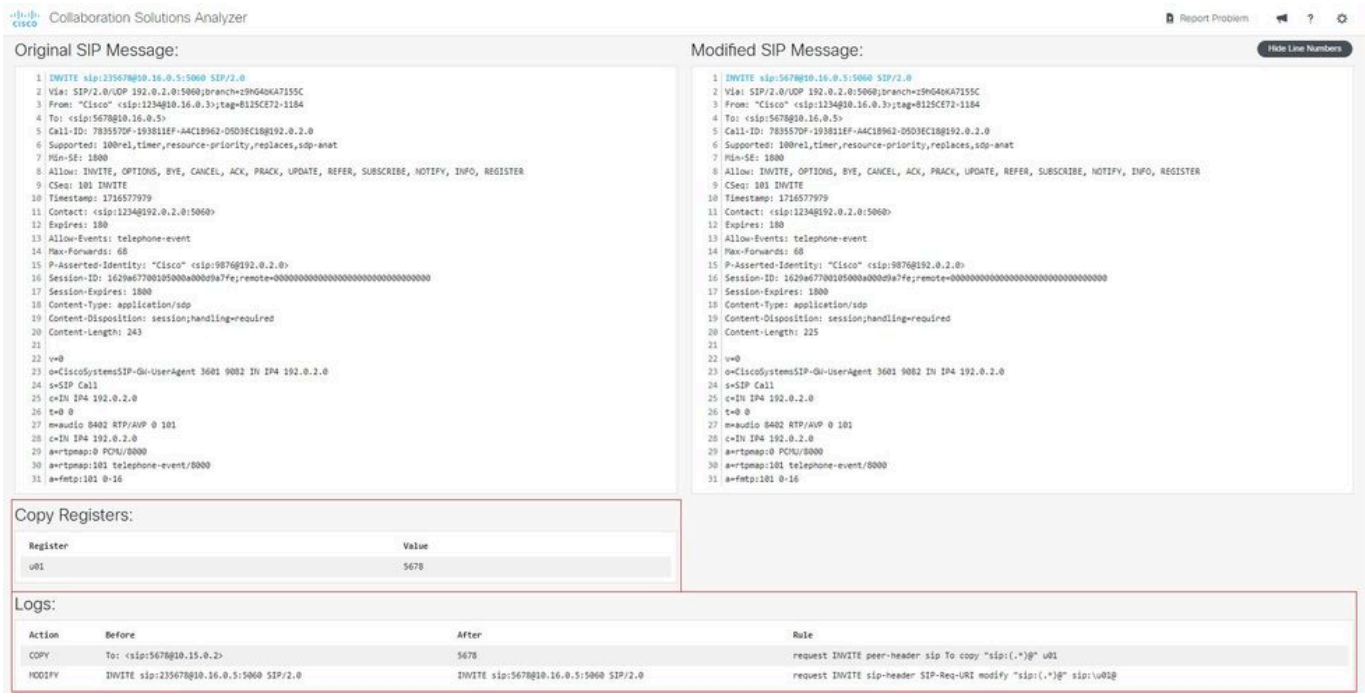
```
Register: u01
Value: 5678
```

Ursprüngliche SIP-Nachricht

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

Geänderte SIP-Nachricht

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

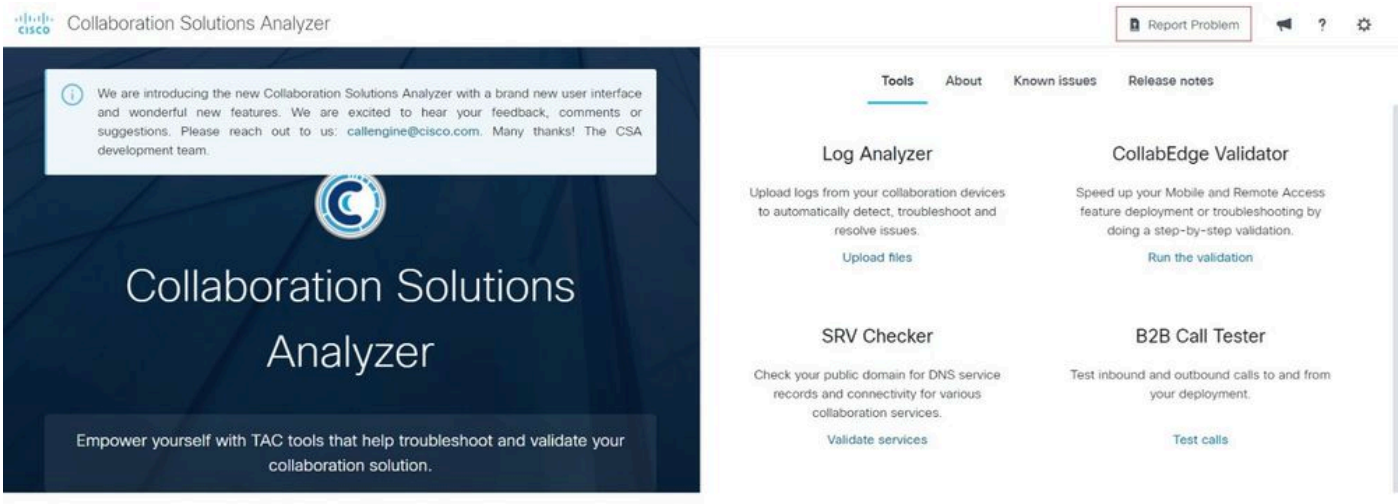


SIP-PROFIL-Copylist - Beispiel 2

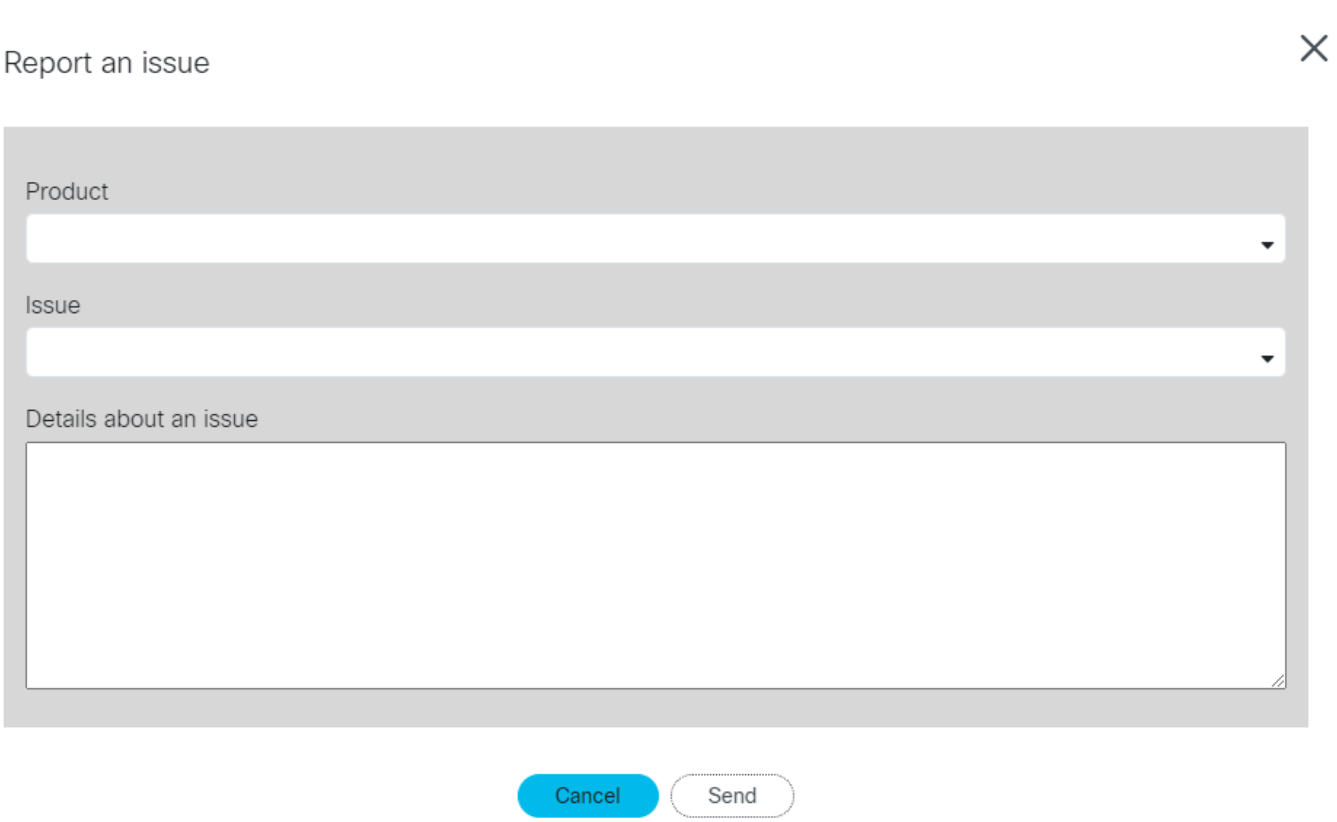
Problem melden

Oben auf der CSA-Plattform können Sie im Abschnitt Problem melden alle in den Tools festgestellten Probleme melden.

Darüber hinaus kann der Administrator Feedback, Kommentare oder Vorschläge abgeben, indem er eine E-Mail an die Stelle sendet, an der das CSA-Entwicklungsteam die Informationen verarbeitet.

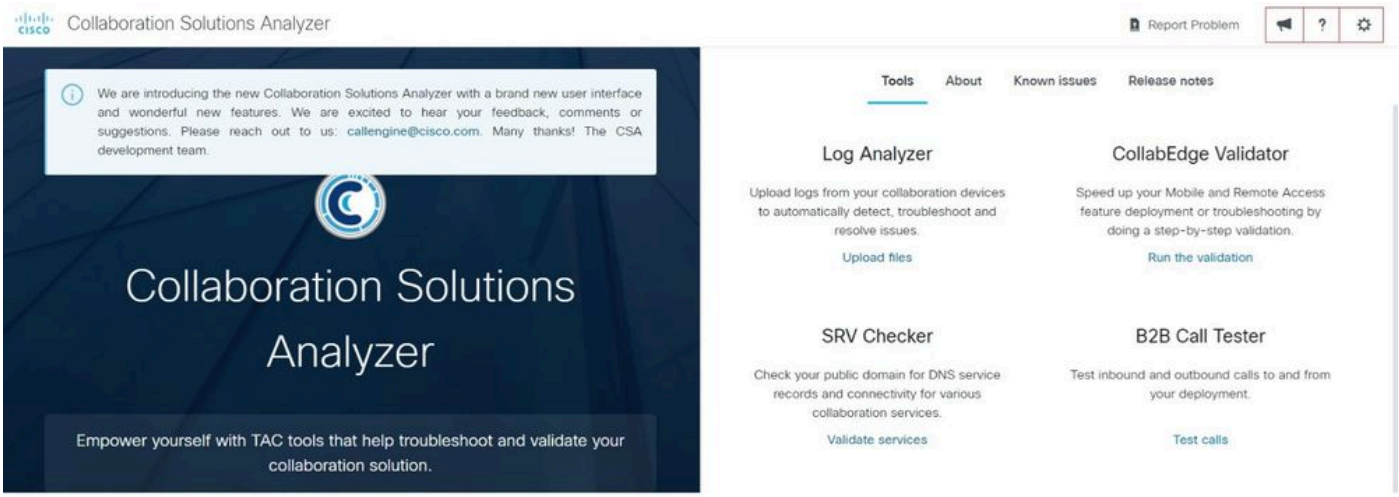


Problem melden - Startseite



Problem melden

Es wurden drei Symbole aktiviert, über die der Benutzer Feedback geben (Megaphon-Symbol), die Benutzerdokumentation überprüfen (Fragezeichen-Symbol) und die Benutzereinstellungen öffnen kann (Zahnrad-Symbol).



Symbole

Support-bezogene Informationen

[Debug-Sammlung für CUBE- und TDM-Gateways konfigurieren]

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

Kapitel: SIP-Profile

Verwendung von SIP-Profilen für CUBE Enterprise - allgemeine Anwendungsfälle

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.