

Fehlerbehebung bei CUBE über Collaboration Solutions Analyzer

Inhalt

[Einleitung](#)

[Anforderungen](#)

[Erste Schritte](#)

[Überlegungen](#)

[Plattformbeschreibung](#)

[Log Analyzer](#)

[CUBE-Protokolldateien hochladen](#)

[Informationen zum Anrufabschnitt](#)

[Leiterdiagramm](#)

[Signalisierung](#)

[Diagnose](#)

[CUBE-Paketerfassung](#)

[SIP-Profiltester \(SPT\)](#)

[Beispiel eines vordefinierten SIP-Profiles](#)

[Copylist SIP-Profil](#)

[Problem melden](#)

[Support-bezogene Informationen](#)

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.

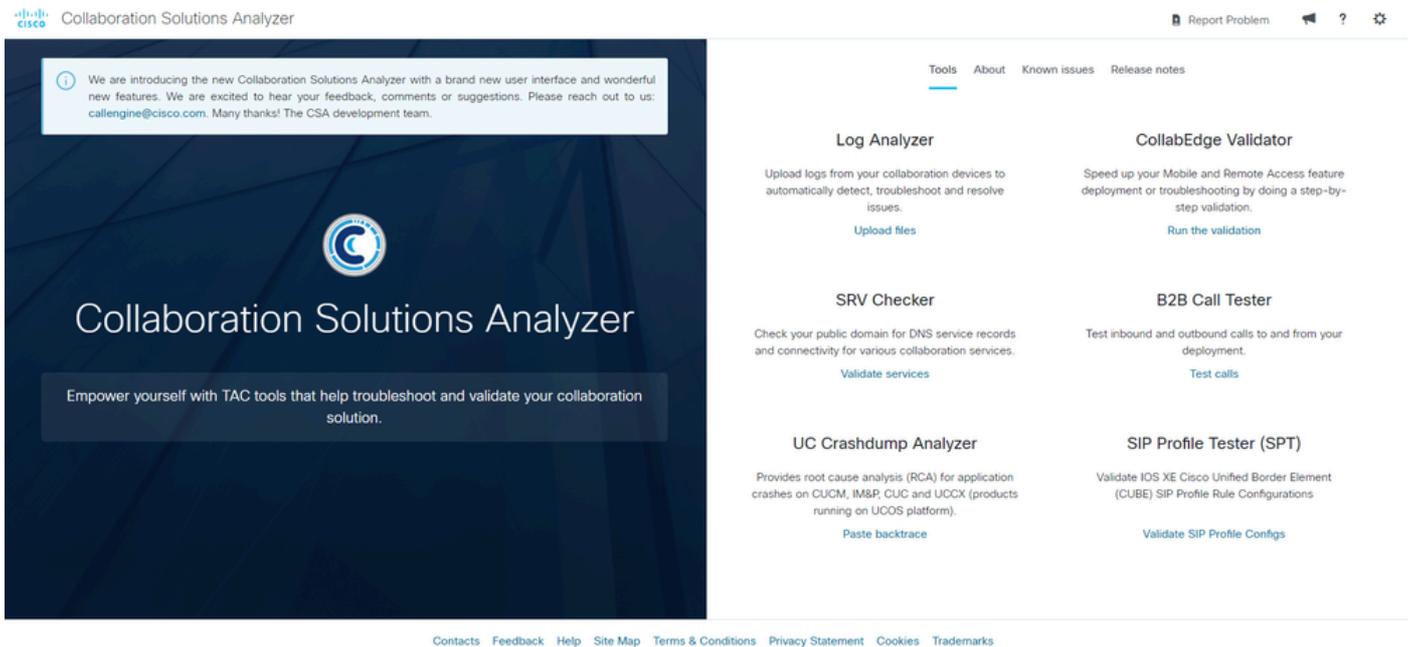
Log Analyzer verwendet CUBE-Protokolle (basierend auf dem Debugging von SIP-Nachrichten) für die Analyse.

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



Collaboration Solutions Analyzer

Report Problem

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](#)

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

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

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:

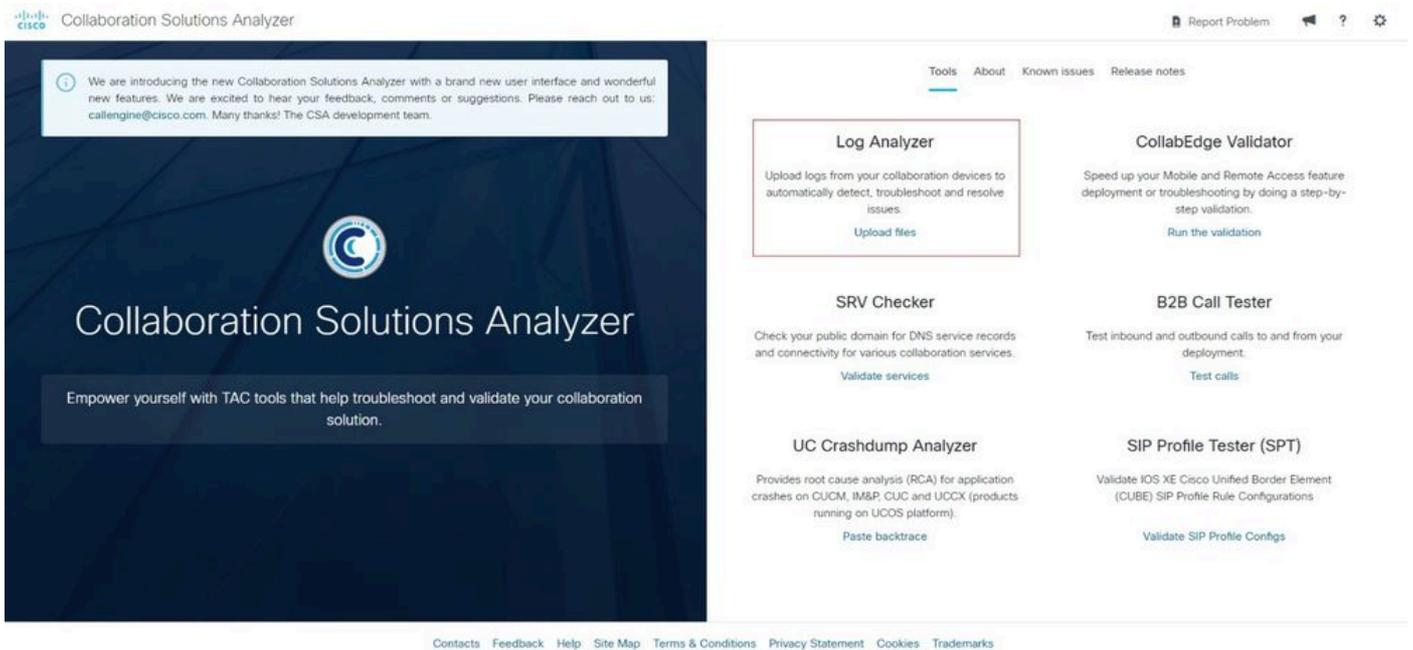
- Informationen zum Anrufabschnitt
- Leiterdiagramm
- Signalisierung

 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.



The screenshot shows the Collaboration Solutions Analyzer (CSA) web interface. The page has a dark blue header with the Cisco logo and the text "Collaboration Solutions Analyzer". Below the header, there is a navigation bar with links for "Tools", "About", "Known issues", and "Release notes". The main content area is divided into several tool cards, each with a title, a brief description, and a primary action button. The "Log Analyzer" card is highlighted with a red border. The other cards include "CollabEdge Validator", "SRV Checker", "B2B Call Tester", "UC Crashdump Analyzer", and "SIP Profile Tester (SPT)". At the bottom of the page, there is a footer with links for "Contacts", "Feedback", "Help", "Site Map", "Terms & Conditions", "Privacy Statement", "Cookies", and "Trademarks".

Log Analyzer - Startseite

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

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

Hochladen der Protokollanalyse

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

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)

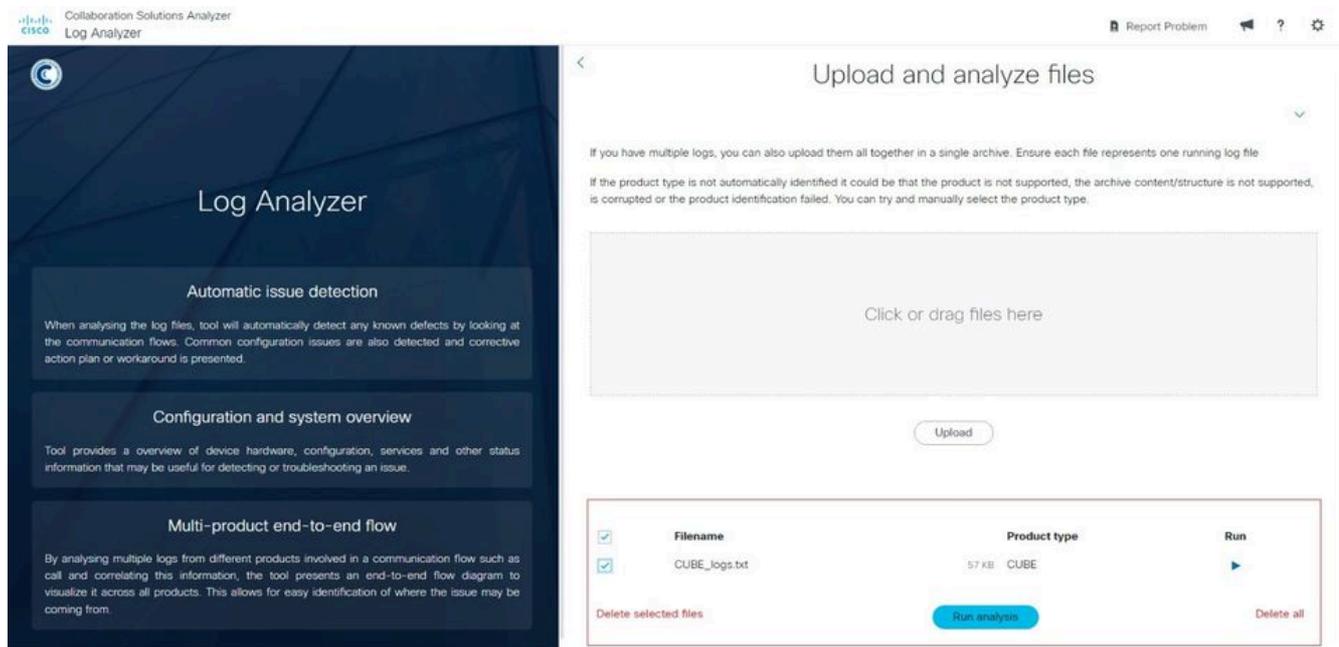
Upload

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.

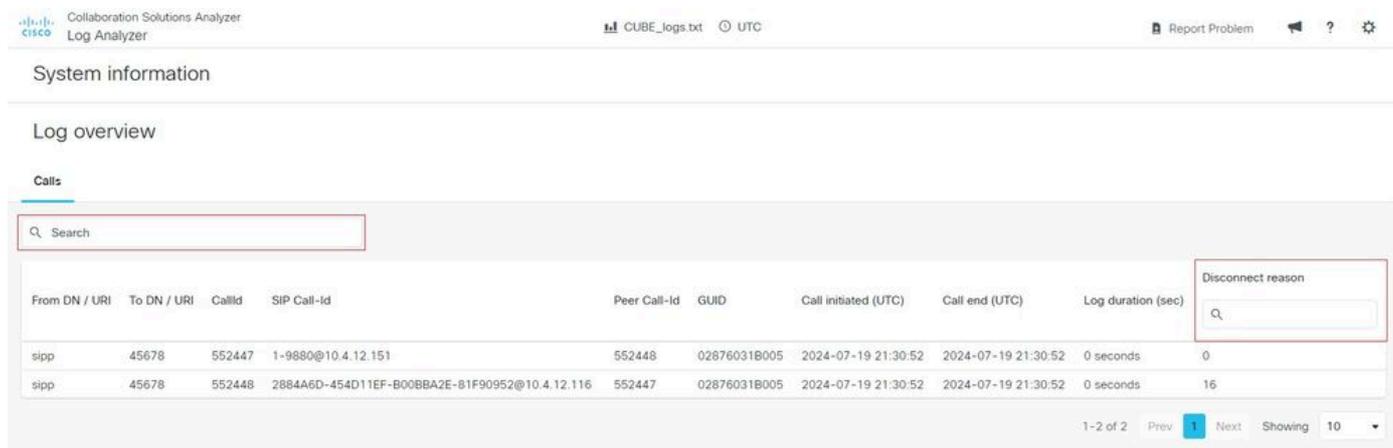
- Das System setzt den Produkttyp auf CUBE.
- In derselben Sitzung können mehrere Dateien analysiert werden.



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 Anruffsitzungen nach bestimmten Daten, z. B. gewählten Nummern.
- Suchen Sie nach "Grund für Verbindungstrennung", um Anruffsitzungen 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 Anruffsitzung.

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

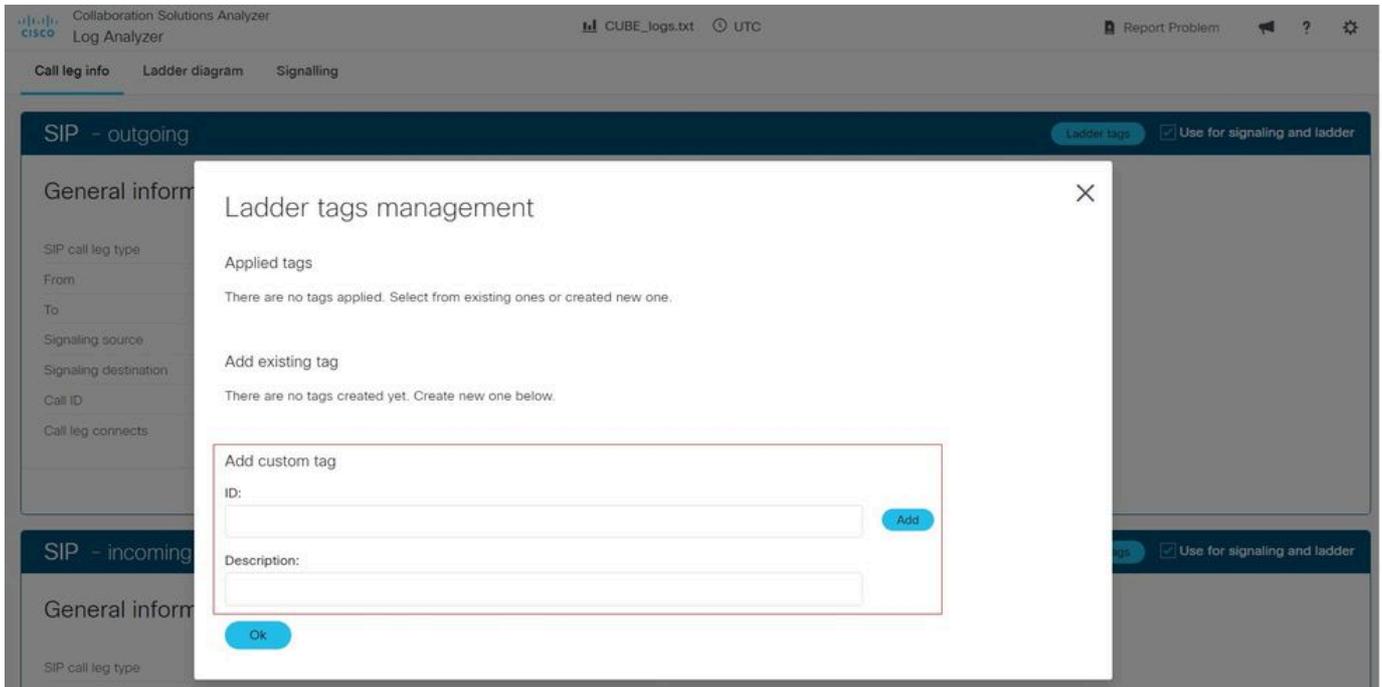
| | |
|-----------------------|------------------------|
| SIP call leg type | Call |
| From | sipp@10.4.12.151:5061 |
| To | 45678@10.4.12.116:5060 |
| Signaling source | 10.4.12.151 : 5061 |
| Signaling destination | 10.4.12.116 : 5060 |
| Call ID | 1-9880@10.4.12.151 |

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:

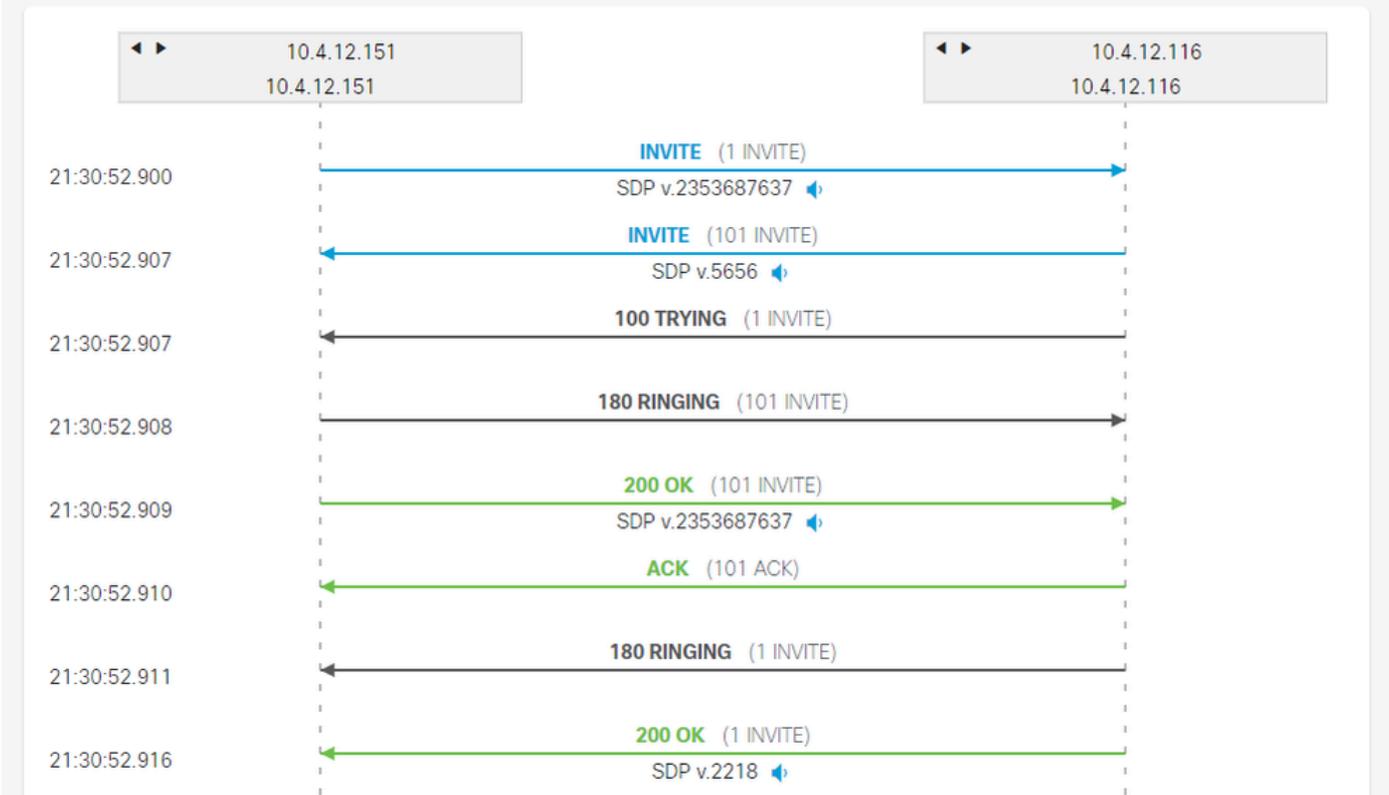
- Blaue Farbe - SIP-INVITE-Nachrichten
- Grüne Farbe - SIP 200 OK und ACK Nachrichten.
- Rote Farbe - SIP BYE-Nachrichten

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.

Call

Call leg info **Ladder diagram** Signalling

Allow horizontal scroll [Download ladder](#)



Leiterdiagramm der Protokollanalyse

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

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

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.

Ladder tags management

Applied tags

| ID | Description | Visual | Action |
|-------------|------------------|--------|--------|
| 10.4.12.151 | Service Provider | ● | 🗑️ |

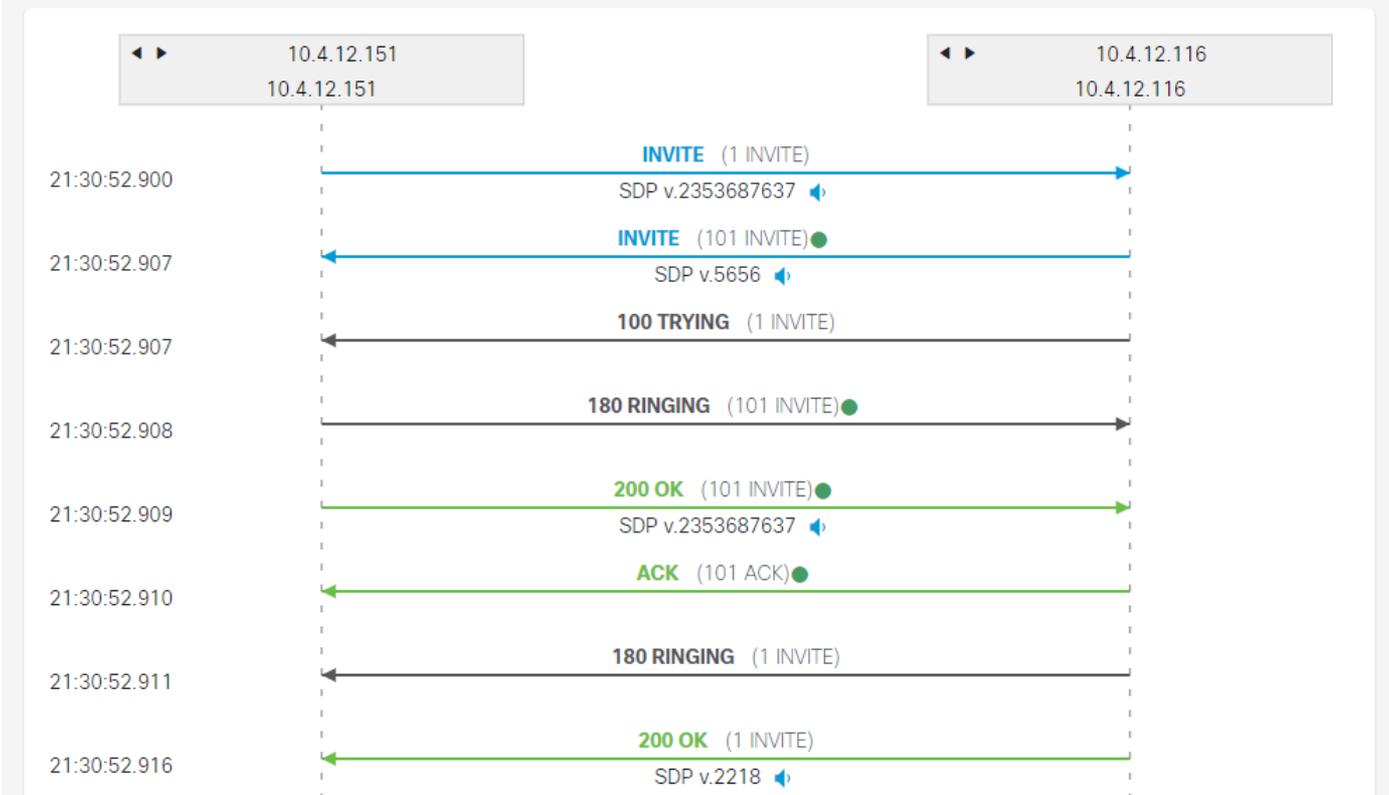
Leitermarkierungen 1 für Protokollanalyse

Call

Call leg info **Ladder diagram** Signalling

Allow horizontal scroll

Legend: ■ Service Provider



Protokoll-Analyzer-Leitermarkierungen 2

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

Ladder tags management



Applied tags

| ID | Description | Visual | Action |
|------|----------------------|--------|--------|
| PCMU | Voice Codec G711ulaw | ● | 🗑️ |

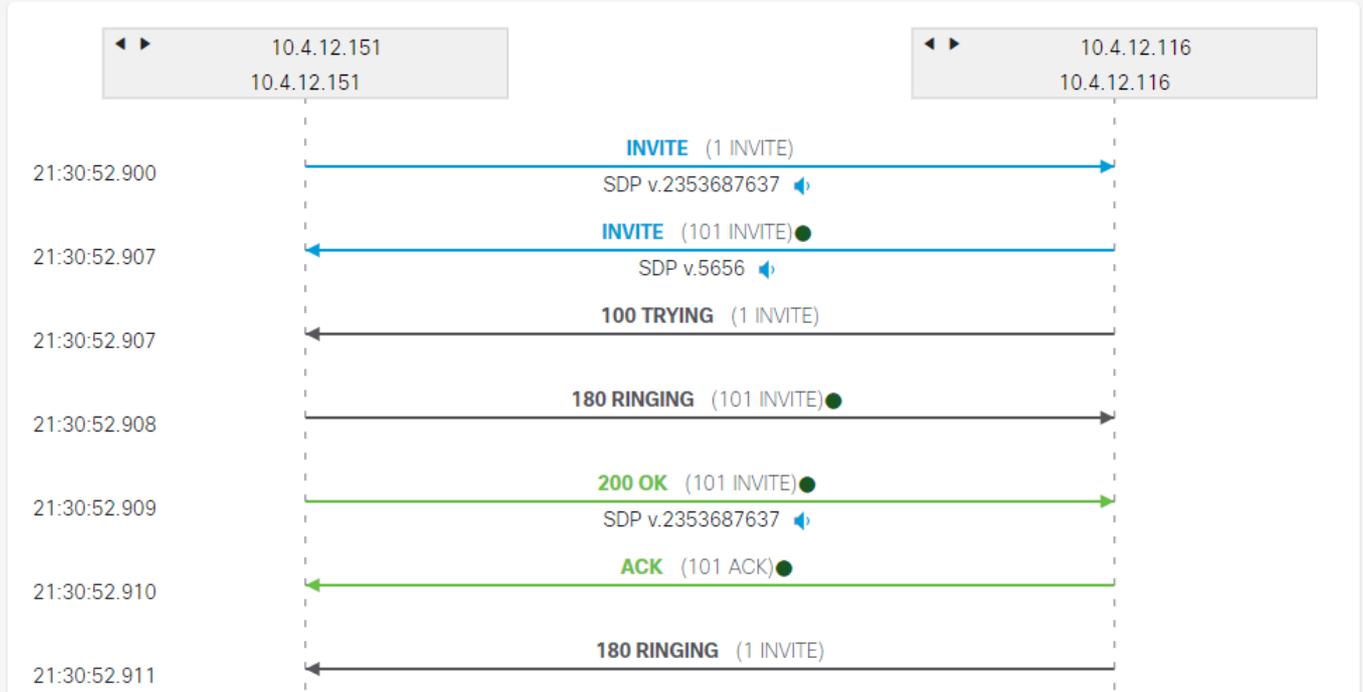
Leitermarkierungen der Protokollanalyse 3

Call

Call leg info **Ladder diagram** Signalling

Allow horizontal scroll Download ladder

Legend: ■ Voice Codec G711ulaw



Leitermarkierungen für Protokollanalyse 4

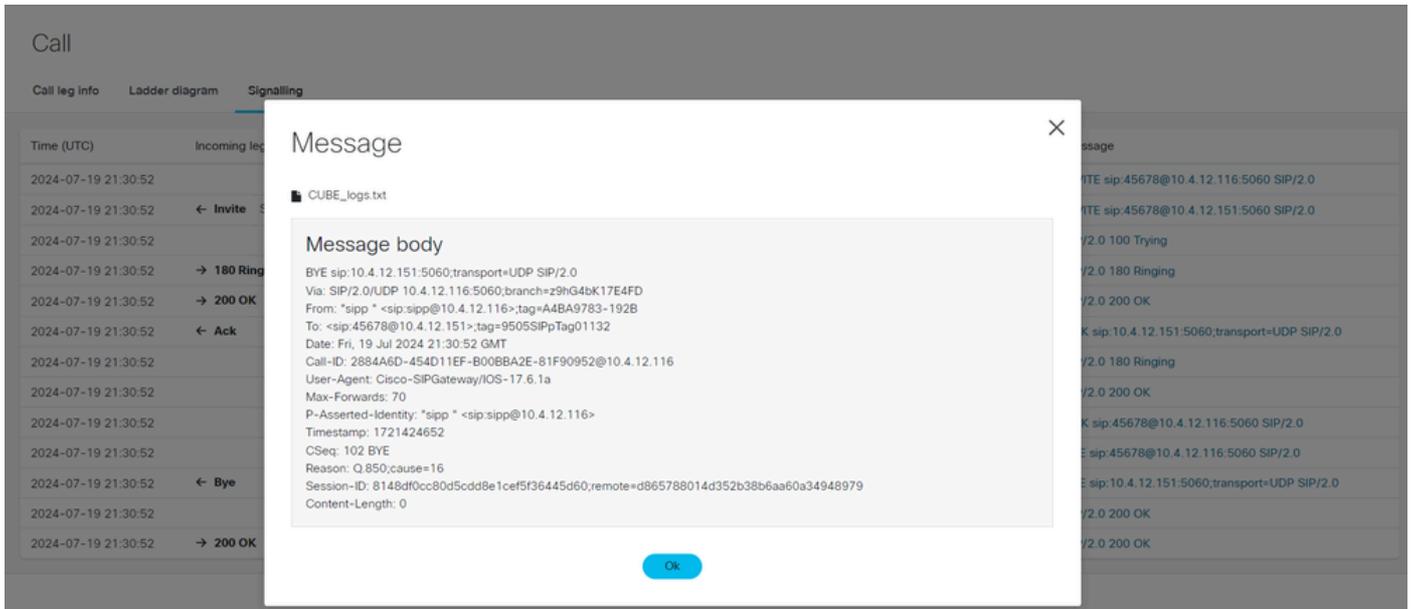
Signalisierung

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.

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 |



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.

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

Diagnose-Startseite für Protokollanalyse

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](#).

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.

The screenshot shows the Cisco Log Analyzer interface. On the left, there is a sidebar with 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 for 'Filename', 'Product type', and 'Run'. The table lists two files: 'CUBE_Packet_Capture.pcap' (83 KB, PCAP) and 'CUBE_logs.txt' (57 KB, CUBE). The first file is selected with a checkmark. There are buttons for 'Delete selected files', 'Run analysis', and 'Delete all'.

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.

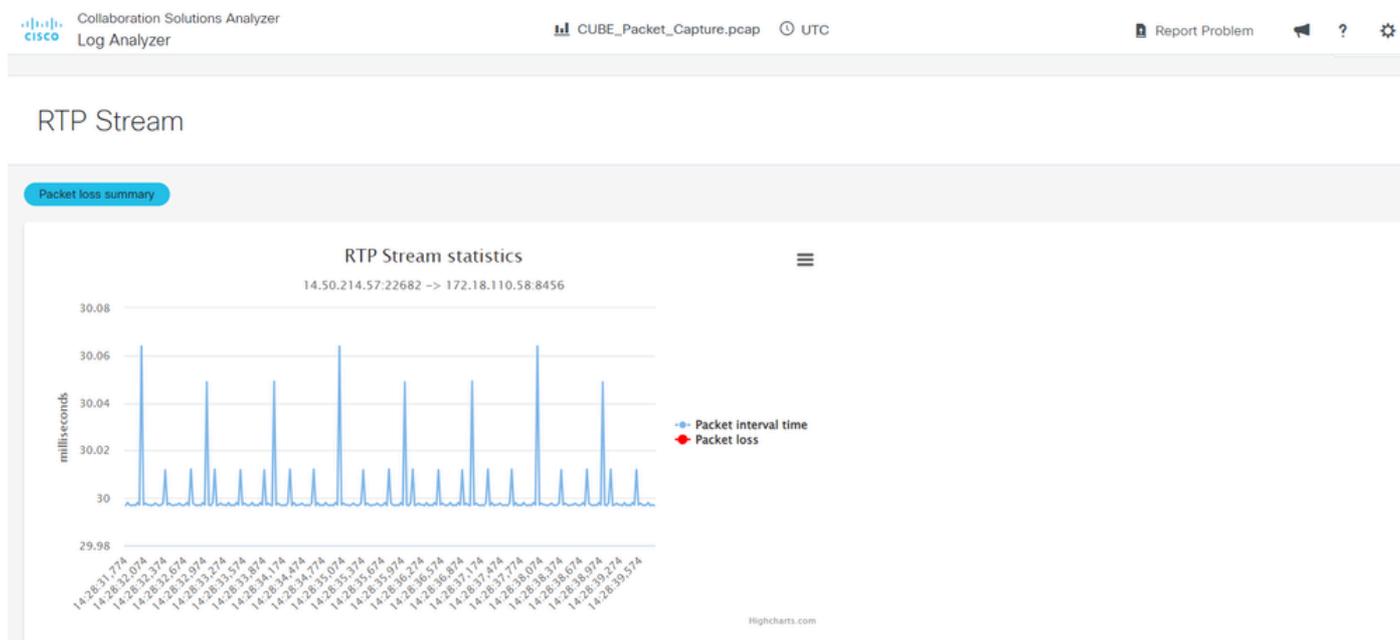
The screenshot shows the Cisco Log Analyzer interface with the 'RTP streams' tab selected. The 'Log overview' section displays a table with the following data:

| 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 | |

At the bottom right, there is a pagination control showing '1-2 of 2' items, with '1' selected, and a 'Showing 10' dropdown menu.

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.

System information

Log overview

RTP streams **TCP/UDP Streams**

Q Search

| Protocol | Src IP | Src port | Dest IP | Dest port | Packet count | 2-way communication | OCSF |
|----------|---------------|----------|---------------|-----------|--------------|---------------------|------|
| 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

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.

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** (required): This section has a dropdown menu 'Load a Prebuilt Rule Set'. 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 'Input Help' (copylist, voice service voip, dial-peers, tenant, or other voice configurations are not required) and 'Syntax Help' (SIP Profile Config Guide, SIP Copylist Config Guide).
- SIP Message To Test Rules On** (required): This section has a dropdown menu 'Load a sample SIP Message'. Below it is a large empty text area. Below this area, there is '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.) and 'Syntax Help' (IANA SIP Parameters, IANA SDP Parameters).

Below these sections, there is a section for **Peer SIP Message To Copy From** (optional) with a 'Show Peer Copy Input' button. It includes 'Input Help' (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.

Beispiel eines vordefinierten SIP-Profiles

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.

The screenshot displays the Cisco Collaboration Solutions Analyzer interface. The top navigation bar includes the Cisco logo, the text 'Collaboration Solutions Analyzer', and utility icons for 'Report Problem', a search icon, a help icon, and a settings icon. The main content area is divided into two panels. The left panel, titled 'SIP Profile Rules' with a 'required' status, contains a configuration rule: 'rule 100 request ANY sip-header Diversion Add "Diversion: <sip:8675309@cisco.com>"'. Below this rule, there is an 'Input Help' section stating 'copylist, voice service voip, dial-peer, tenant, or other voice configurations are not required.' and a 'Syntax Help' section pointing to 'SIP Profile Config Guide, SIP Copylist Config Guide'. The right panel, titled 'SIP Message To Test Rules On' with a 'required' status, shows a dropdown menu set to 'INVITE (No SDP)'. The main area of this panel displays a detailed SIP INVITE message with various headers and body text, including 'Via: SIP/2.0/TCP 192.168.10.10:5060;branch=z9hG4bK16242110', 'From: "Callisto Home" <sip:123456789@192.168.10.10>;tag=4EDF0000-CA0', 'Call-ID: 07E43511-335111EF-85788A40-687EBAD8@192.168.10.10', 'Session-ID: 2d390a8000105000a000247e126c26d;remote=3b954a1e00105000a0006c416a369498', 'Cisco-Guid: 3622027175-8860951023-2238888512-1803467483', 'Cseq: 101 INVITE', 'Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER', 'Supported: 100rel,timer,resource-priority,replaces', 'Subject: SIP Profile Test', 'User-Agent: Cisco-SIPGateway/IOS-17.14.1a', 'Date: Thu, 27 Jun 2024 00:20:07 GMT', 'Timestamp: 1719447607', 'Expires: 180', 'Session-Expires: 1800;refresher-uac', 'Max-Forwards: 69', and 'Contact: <sip:111111111@192.168.10.10:5060;transport=tcp>'. Below the message, there is an 'Input Help' section stating 'SIP Request URI or Status Line always required. SIP Headers/SDP Body optional unless testing them. CSEQ required if "method" used in response rule.' and a 'Syntax Help' section pointing to 'IANA SIP Parameters, IANA SDP Parameters'. At the bottom of the right panel, there is a section 'Peer SIP Message To Copy From' with an 'optional' status and a 'Show Peer Copy Input' button. Below this, there is another 'Input Help' section stating 'Regular "copy" rules will use the other SIP Message; not this input.' At the very bottom of the interface, there are two buttons: 'New Test' (red) and 'Run Test' (green).

SIP-PROFIL vorinstalliert

Das Tool zeigt einen neuen Bildschirm mit den Testergebnissen an:

Geänderte SIP-Nachricht

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>" |

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:444444444@" "sip:555555555@"
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: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 SIP INVITE message is displayed with various headers like Via, From, To, Call-ID, Session-ID, etc. Below the message, there are sections for 'Peer SIP Message To Copy From' and 'Run Test' buttons.

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"

444444444@192.168.10.10>

REMOVED (RED) - P-Preferred-Identity: "CallerID_Name" <sip:555555555@192.168.10.10>

Geänderte SIP-Nachricht

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. It is divided into three main sections: 'Original SIP Message', 'Modified SIP Message', and 'Logs'.

Original SIP Message: Shows a standard SIP INVITE message with headers such as 'Via: SIP/2.0/TCP 192.168.10.10:5060', 'From: "CallerID_Name" <sip:123456789@192.168.10.10>', 'To: <sip:8675309@192.168.10.10>', and 'P-Preferred-Identity: "CallerID_Name" <sip:555555555@192.168.10.10>'.

Modified SIP Message: Shows the same SIP INVITE message but with modifications. The 'P-Preferred-Identity' header is now 'P-Preferred-Identity: "CallerID_Name" <sip:555555555@192.168.10.10>' (highlighted in blue), and a new 'Diversion: <sip:8675309@cisco.com>' header has been added (highlighted in green).

Logs: A table summarizing the changes:

| 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-Preferred-Identity: "CallerID_Name" <sip:444444444@192.168.10.10> | P-Preferred-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 |

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 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 - 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, 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

Report an issue



Product

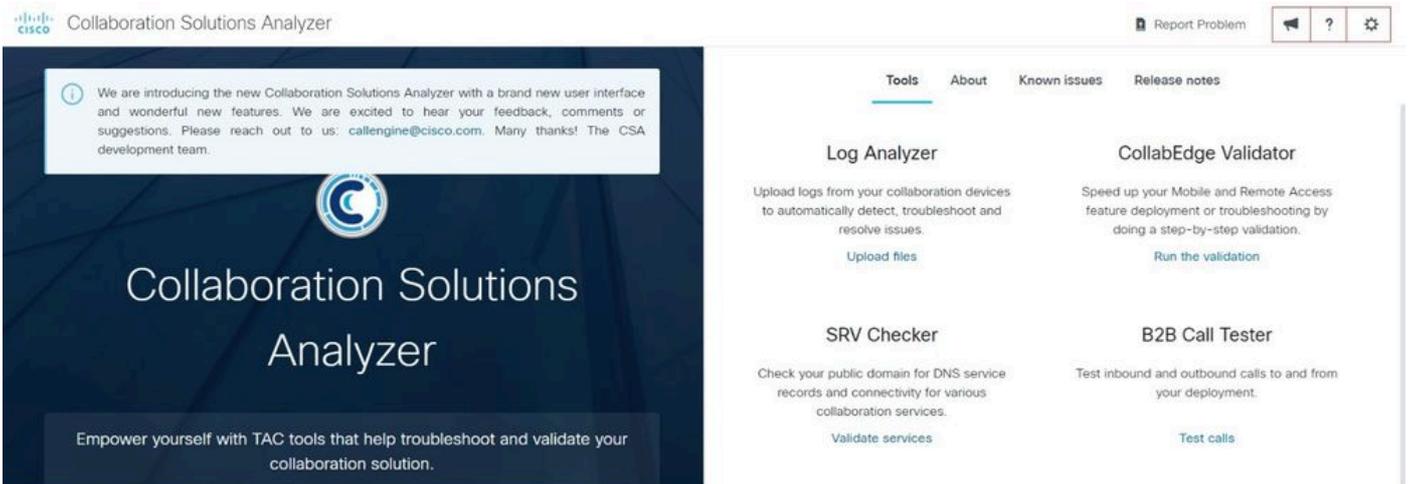
Issue

Details about an issue

Cancel Send

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.