

Solucionar problemas do CUBE por meio do Collaboration Solutions Analyzer

Contents

[Introdução](#)

[Requisitos](#)

[Introdução](#)

[Considerações](#)

[Descrição da plataforma](#)

[Analisador de log](#)

[Carregar arquivos de log do CUBE](#)

[Informações sobre o Leg da chamada](#)

[Diagrama de Escada](#)

[Sinalização](#)

[Diagnósticos](#)

[Captura de pacotes do CUBE](#)

[Testador de perfil SIP \(SPT\)](#)

[Exemplo de perfil SIP pré-criado](#)

[Perfil SIP da Lista de Cópias](#)

[Relatar Um Problema](#)

[Informações relacionadas ao suporte](#)

Introdução

Este documento descreve as ferramentas Log Analyzer e SIP Profile Tester para solucionar problemas do CUBE usando o portal Collaboration Solutions Analyzer.

Requisitos


A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Border Element (CUBE) Enterprise
- Session Initiation Protocol (SIP) (Protocolo de Iniciação da Sessão (SIP)).
- Coleção de logs do CUBE (depuração).

Introdução

O Collaboration Solutions Analyzer (CSA) é um conjunto de ferramentas criado para oferecer suporte à sua solução de colaboração durante todo o seu ciclo de vida. Ele ajuda a identificar problemas e fornece planos de ação corretivos quando necessário, auxiliando em todas as fases da solução de colaboração.

Navegue até o Collaboration Solution Analyzer em <https://cway.cisco.com/csa-new/#/home>

 Observação: usar o navegador Chrome garante que a ferramenta funcione de forma ideal.

Considerações

As ferramentas foram projetadas para um dispositivo CUBE que lida com chamadas SIP para SIP. Nenhum outro protocolo de voz é suportado pelas ferramentas.

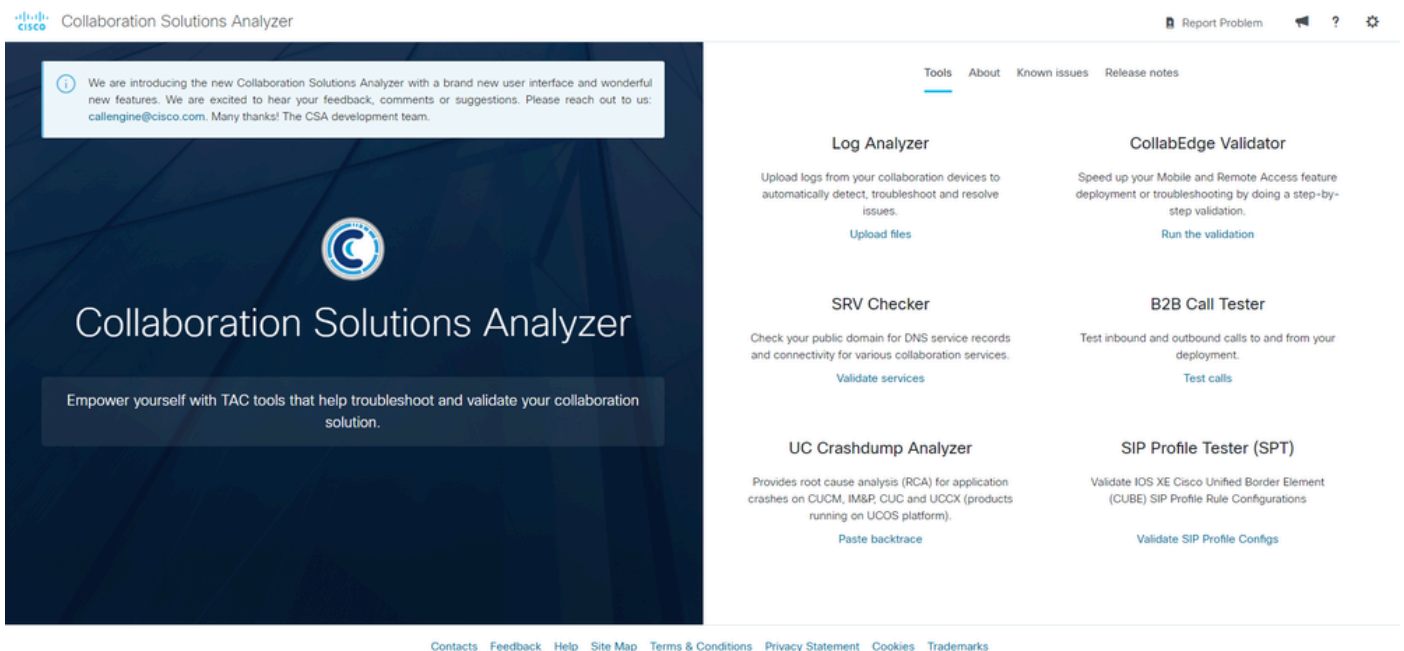
O Log Analyzer usa logs do CUBE (com base na depuração de mensagens do SIP) para análise.

Se precisar de ajuda com outro protocolo de voz, utilize o Cisco Support Assistant para obter compromissos com o TAC em <https://supportassistant.cisco.com>

Descrição da plataforma

A plataforma CSA oferece estas ferramentas CUBE:

- Log Analyzer - Carregue registros do CUBE e de outros dispositivos de colaboração para detectar, solucionar e resolver problemas automaticamente.
- Testador de Perfil SIP - Valide a Configuração do Perfil SIP.




Página inicial do CSA

Analisador de log

A ferramenta Log Analyzer permite que os administradores examinem a sinalização de chamadas tratada pelo dispositivo CUBE. Ele oferece uma análise abrangente dos arquivos de registro, incluindo:

- Informações do leg da chamada
- Diagrama de Escada

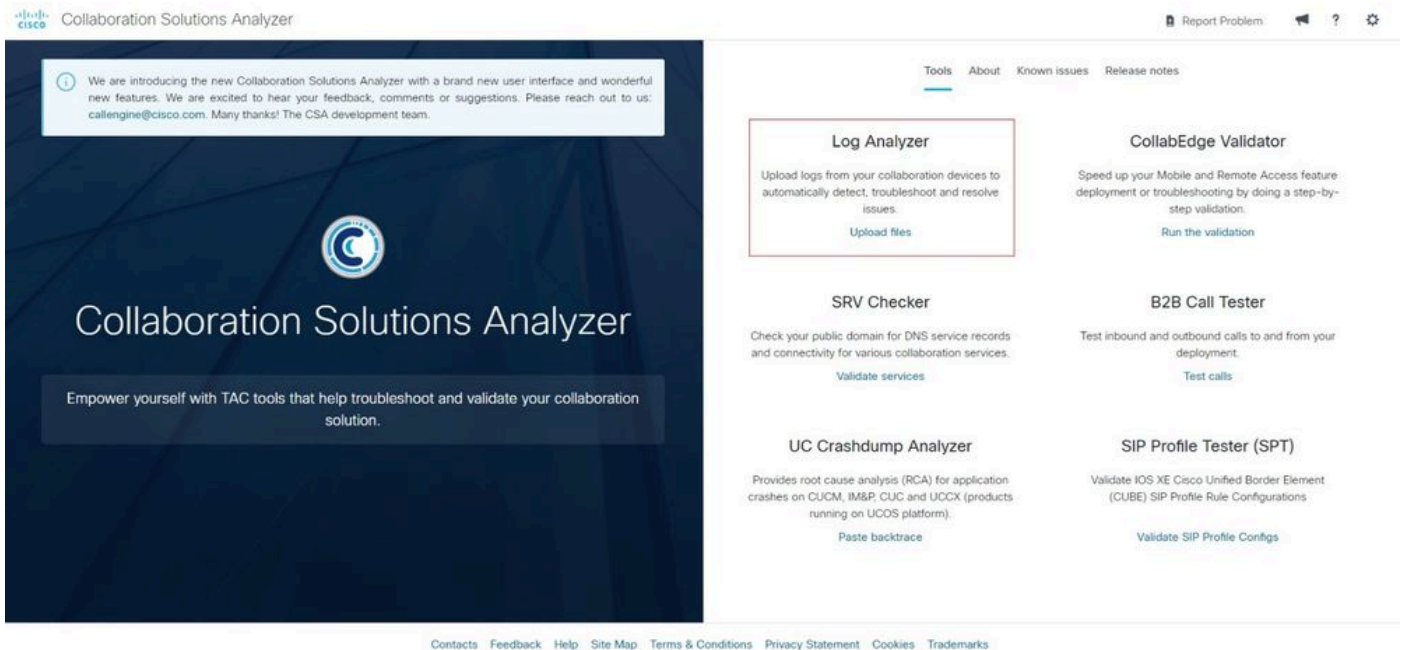
- Sinalização

 Observação: a depuração do CUBE (depurar mensagens ccsip) de uma chamada processada pelo CUBE deve primeiro ser coletada e armazenada em um arquivo de texto. Somente a depuração SIP e nenhuma outra saída, como comandos show, devem ser incluídos nesse arquivo de texto.

Carregar arquivos de log do CUBE

Navegue até o Collaboration Solution Analyzer em <https://cway.cisco.com/csa-new/#/home>

Em seguida, selecione a ferramenta clicando em Upload files na seção Log Analyzer.



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 menu with links for "Tools", "About", "Known issues", and "Release notes". The main content area displays several tool cards, each with a title, a brief description, and a primary action button. The "Log Analyzer" card is highlighted with a red box. The other cards include "CollabEdge Validator", "SRV Checker", "B2B Call Tester", "UC Crashdump Analyzer", and "SIP Profile Tester (SPT)". A footer at the bottom contains links for "Contacts", "Feedback", "Help", "Site Map", "Terms & Conditions", "Privacy Statement", "Cookies", and "Trademarks".

Página inicial do Log Analyzer

A plataforma exibe a tela da ferramenta onde um arquivo pode ser selecionado ou arrastado.

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

Carregar analisador de log

Para concluir o processo de upload do arquivo para a ferramenta analisar, clique no botão Upload.

Log Analyzer

Automatic issue detection

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

Configuration and system overview

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

Multi-product end-to-end flow

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

Upload and analyze files

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

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

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

CUBE_logs.txt
56 KB

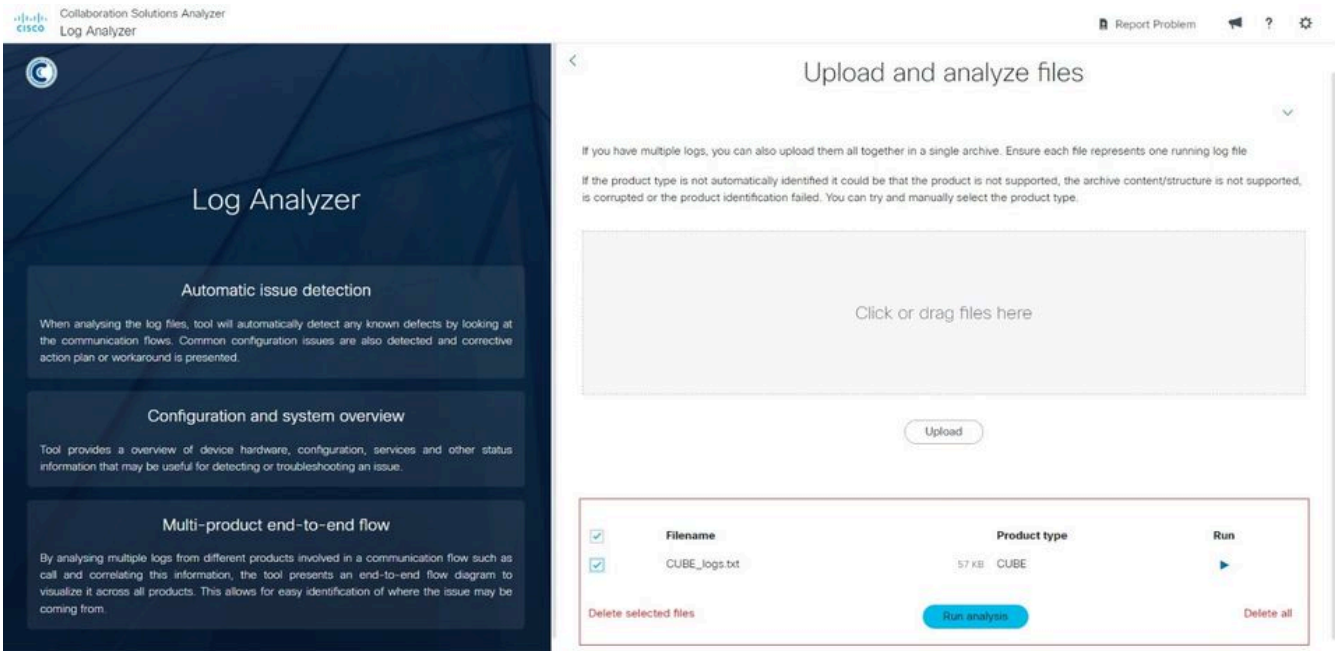
1 Selected (Total: 56 KB)

Upload

Arquivo de upload do Log Analyzer

Depois de carregar o arquivo na ferramenta, selecione o(s) arquivo(s) que deseja analisar marcando a caixa correspondente e clique no botão Executar análise.

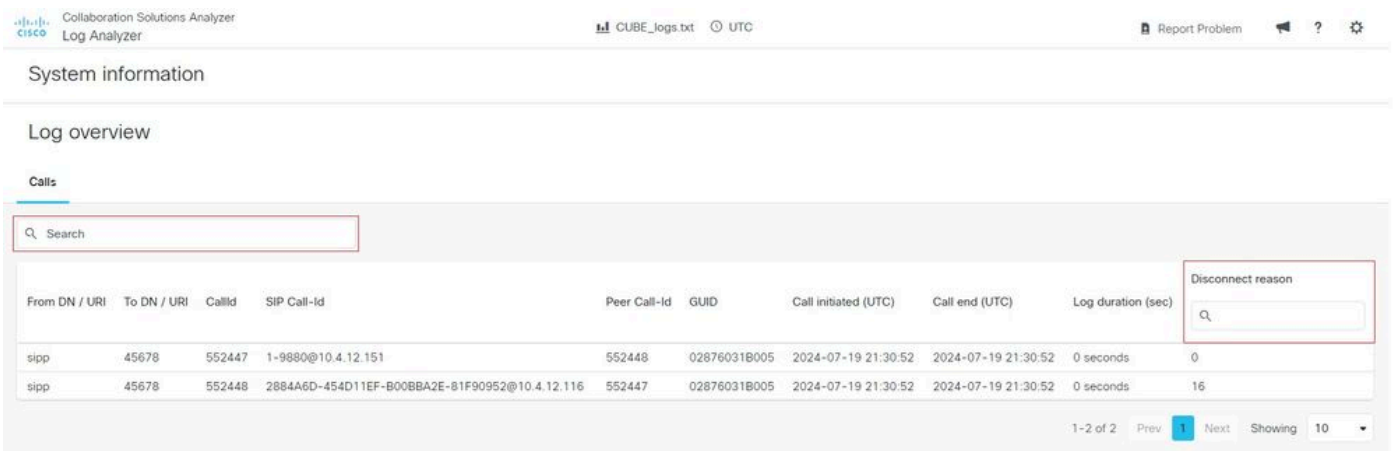
- O sistema define o Tipo de Produto como CUBE.
- Mais de um arquivo pode ser analisado na mesma sessão.



Tipo de Produto do Analisador de Log

A ferramenta analisa todas as chamadas de sinalização capturadas no arquivo de texto e exibe um resumo dos segmentos de chamada identificados. Em seguida, você pode aplicar dois filtros:

- Pesquisar - Filtre as sessões de chamada por dados específicos, como números discados.
- Pesquisar por 'Motivo da desconexão — filtre as sessões de chamada com base no motivo da desconexão da chamada.



Filtro de Chamada do Analisador de Log

Para continuar com a análise detalhada, selecione a linha da sessão de chamada na qual deseja focalizar e a ferramenta exibirá a análise completa mostrando as Informações do segmento de chamada, o Diagrama da escada e a Sinalização.

Informações sobre o Leg da chamada

O primeiro estágio apresenta as Informações do Leg da Chamada, que exibem a visão geral da chamada:

- Tipo de leg da chamada SIP
- De - Obtido do cabeçalho SIP DE da mensagem INVITE.
- Para - Obtido do cabeçalho SIP TO da mensagem INVITE.
- Origem da sinalização - endereço IP e porta do dispositivo de origem. Obtido do cabeçalho SIP VIA da mensagem INVITE.
- Signaling Destination - IP address and port of destination device (Destino da sinalização - Endereço IP e porta do dispositivo de destino). Obtido do cabeçalho SIP URI da mensagem INVITE.
- ID da chamada - Obtido do cabeçalho SIP CALL-ID da mensagem INVITE.
- O segmento de chamada se conecta - Carimbo de data/hora da sessão de chamada.



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

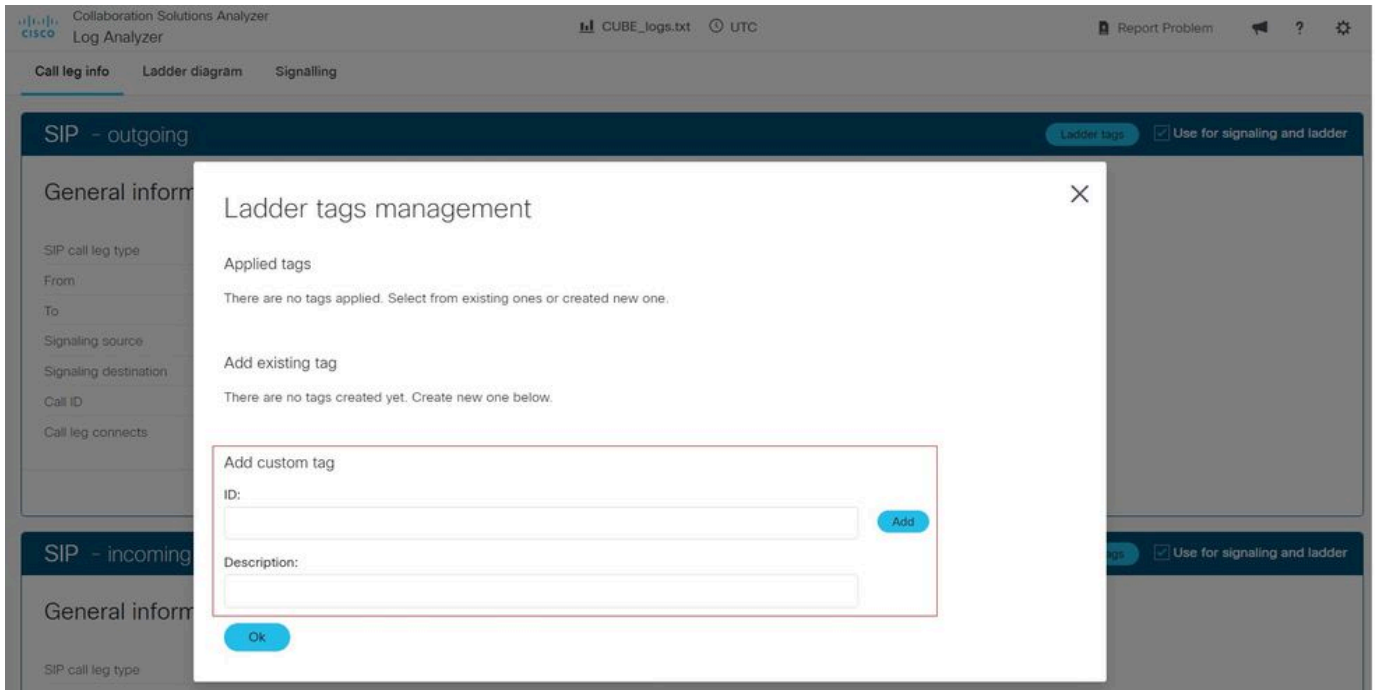
SIP call leg type	Call
From	sipp@10.4.12.151:5061
To	45678@10.4.12.116:5060
Signaling source	10.4.12.151 : 5061
Signaling destination	10.4.12.116 : 5060
Call ID	1-9880@10.4.12.151

Log Analyzer - Informações do Leg de Chamada

Nesta seção, as tags de Escada podem ser ativadas para destacar mensagens no Diagrama de Escada. O aplicativo tem 2 campos:

- ID - Insira o parâmetro específico que deseja realçar.
- Descrição - Adicione uma descrição do parâmetro.

Clique no botão Add para concluir o processo.



Marcas de Escada do Analisador de Log

Diagrama de Escada

No segundo estágio, um Diagrama de Escada é apresentado, representando visualmente as mensagens SIP trocadas durante a chamada. As mensagens são codificadas por cores para facilitar a identificação:

- Cor azul - mensagens CONVITE SIP.
- Cor verde - mensagens SIP 200 OK e ACK.
- Cor vermelha - Mensagens SIP BYE.

Para fazer o download de uma cópia do diagrama, clique no botão Download Ladder. O diagrama é baixado e salvo como um arquivo de imagem PNG. Observe que essa opção só está disponível ao usar o navegador Google Chrome.

Call

Call leg info **Ladder diagram** Signalling

Allow horizontal scroll [Download ladder](#)

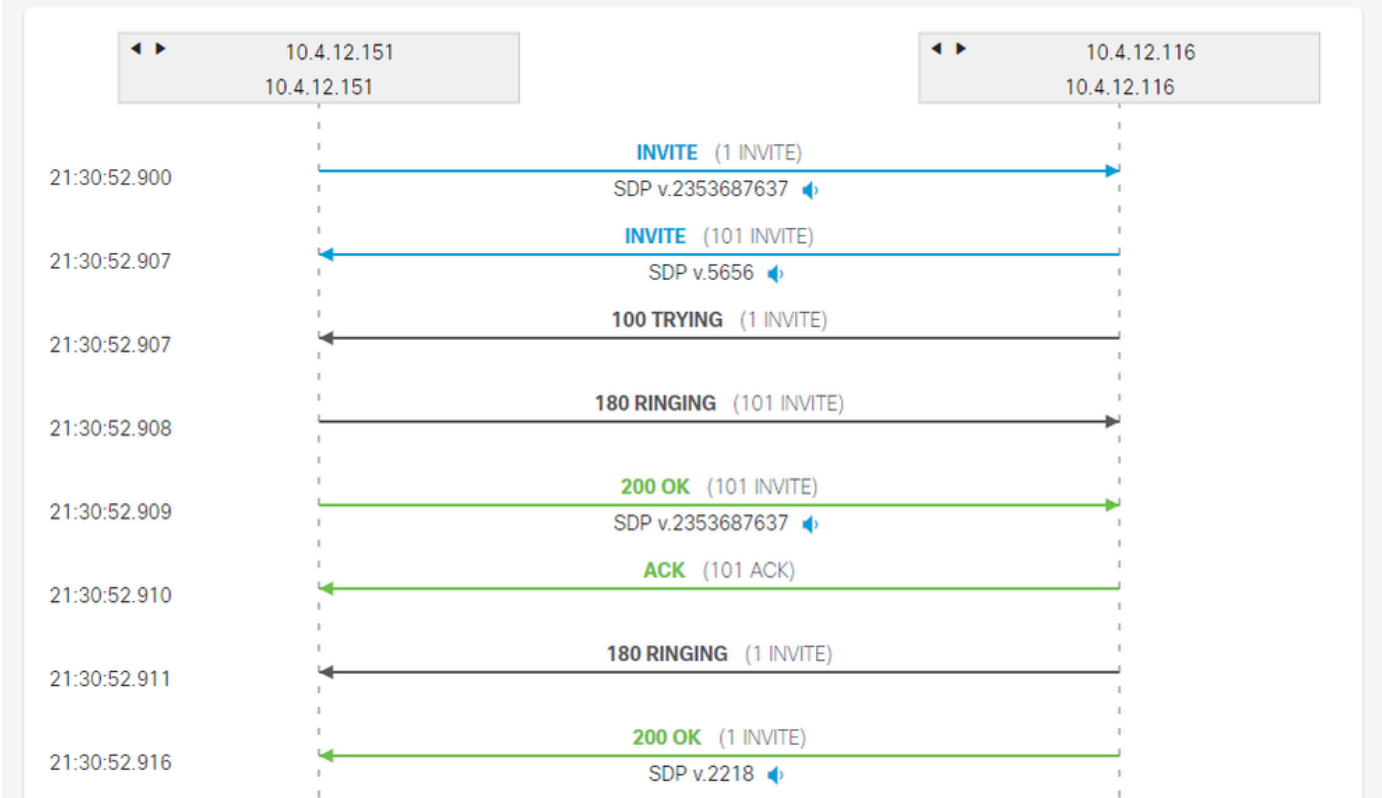
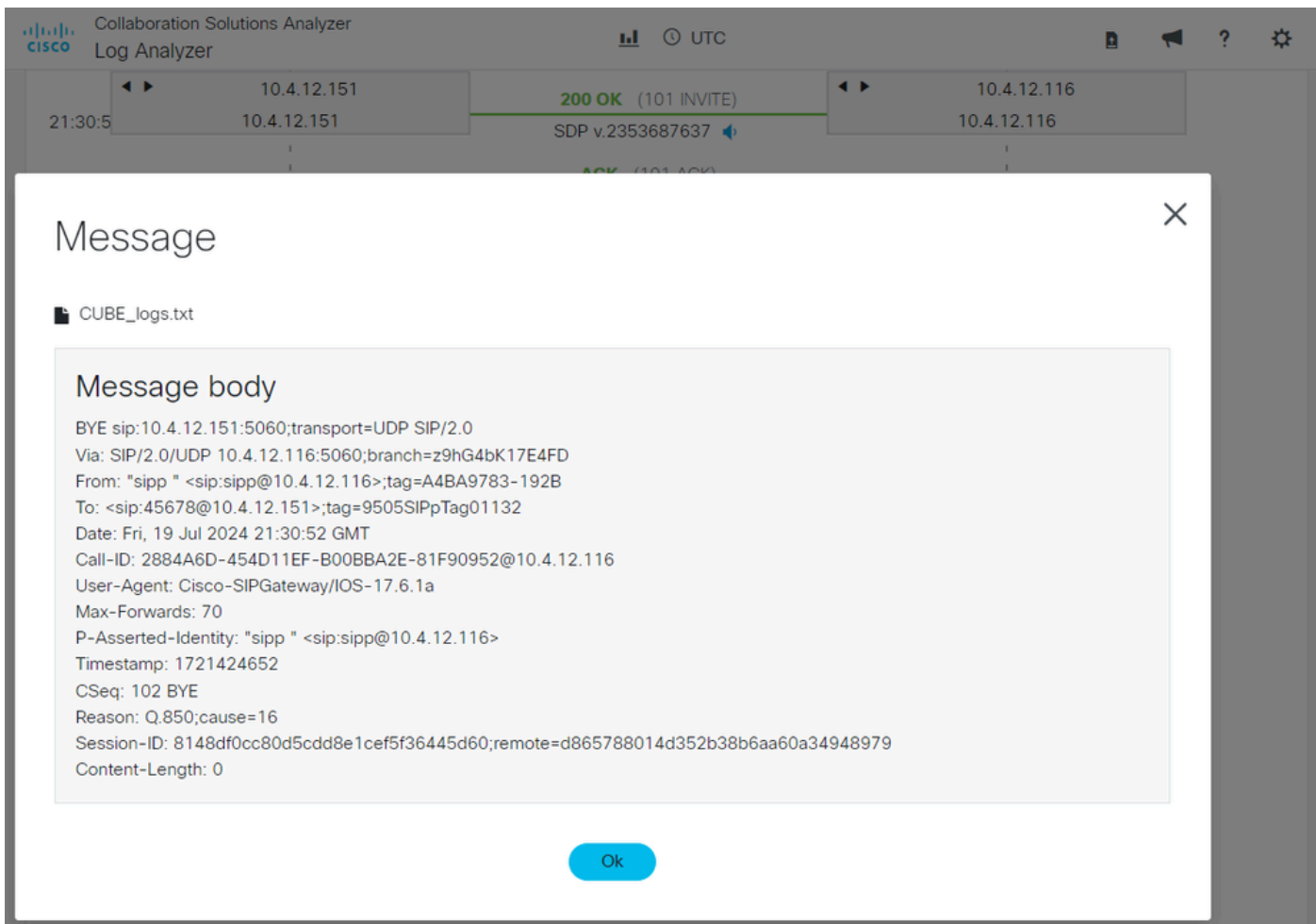


Diagrama da Escada do Analisador de Log

Essa ferramenta permite que o administrador abra mensagens SIP e exiba seu conteúdo. Clique em uma mensagem para abri-la.



Mensagem de Diagrama de Escada do Analisador de Log

O administrador pode adicionar Ladder Tags para visualizar mensagens SIP com uma marca de ponto distinta na seção Call Leg Information. Qualquer parâmetro incluído na mensagem SIP pode ser usado para a marca.

Neste exemplo, um endereço IP é usado para o parâmetro ID e uma descrição é adicionada. As mensagens SIP que contêm o endereço IP são realçadas com uma marca de ponto para distingui-las de outras mensagens.

Ladder tags management

Applied tags

ID	Description	Visual	Action
10.4.12.151	Service Provider	●	🗑️

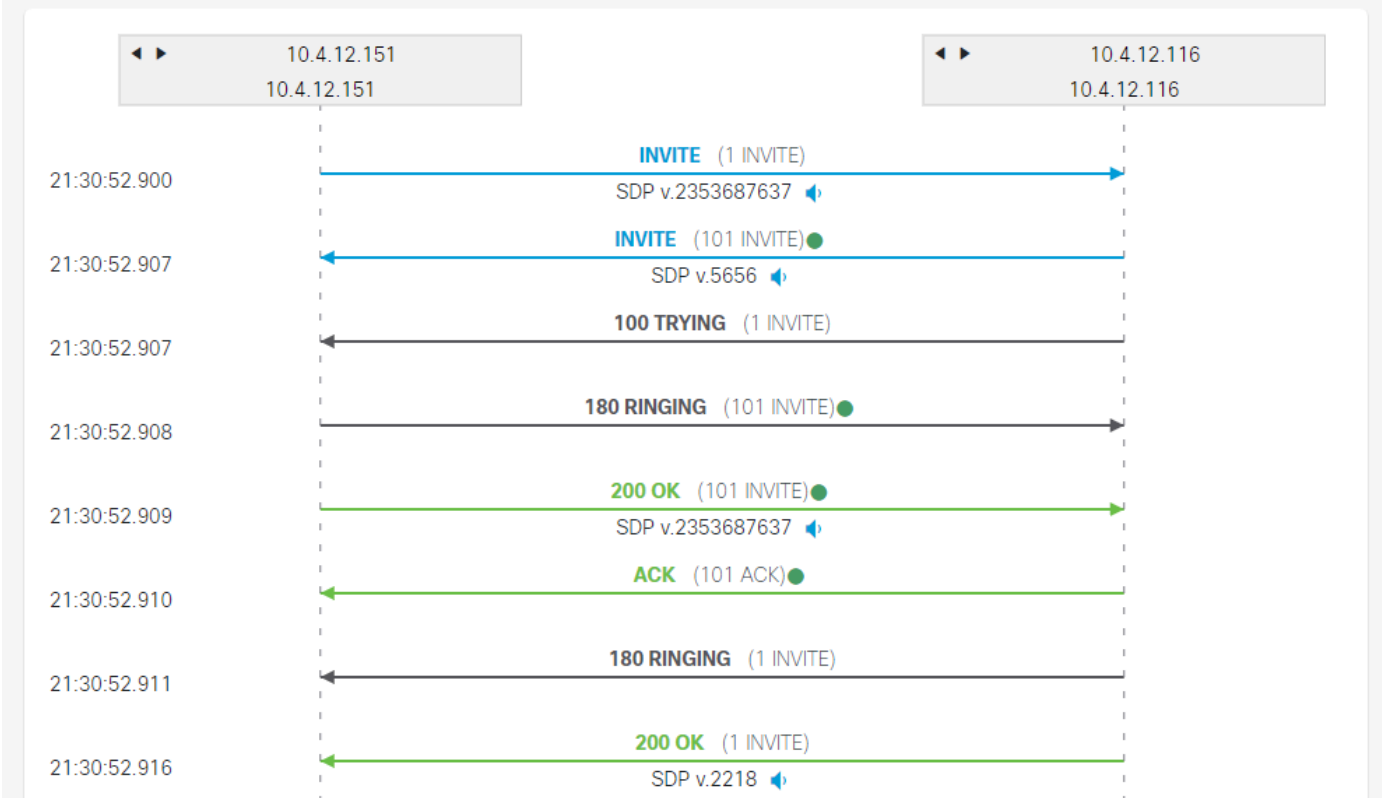
Etiquetas de escada do analisador de log 1

Call

Call leg info **Ladder diagram** Signalling

Allow horizontal scroll

Legend: ■ Service Provider



Etiquetas de escada do analisador de log 2

Outro filtro que pode ser usado para distinguir mensagens SIP de outras mensagens é um codec de voz.

Ladder tags management



Applied tags

ID	Description	Visual	Action
PCMU	Voice Codec G711ulaw	●	🗑️

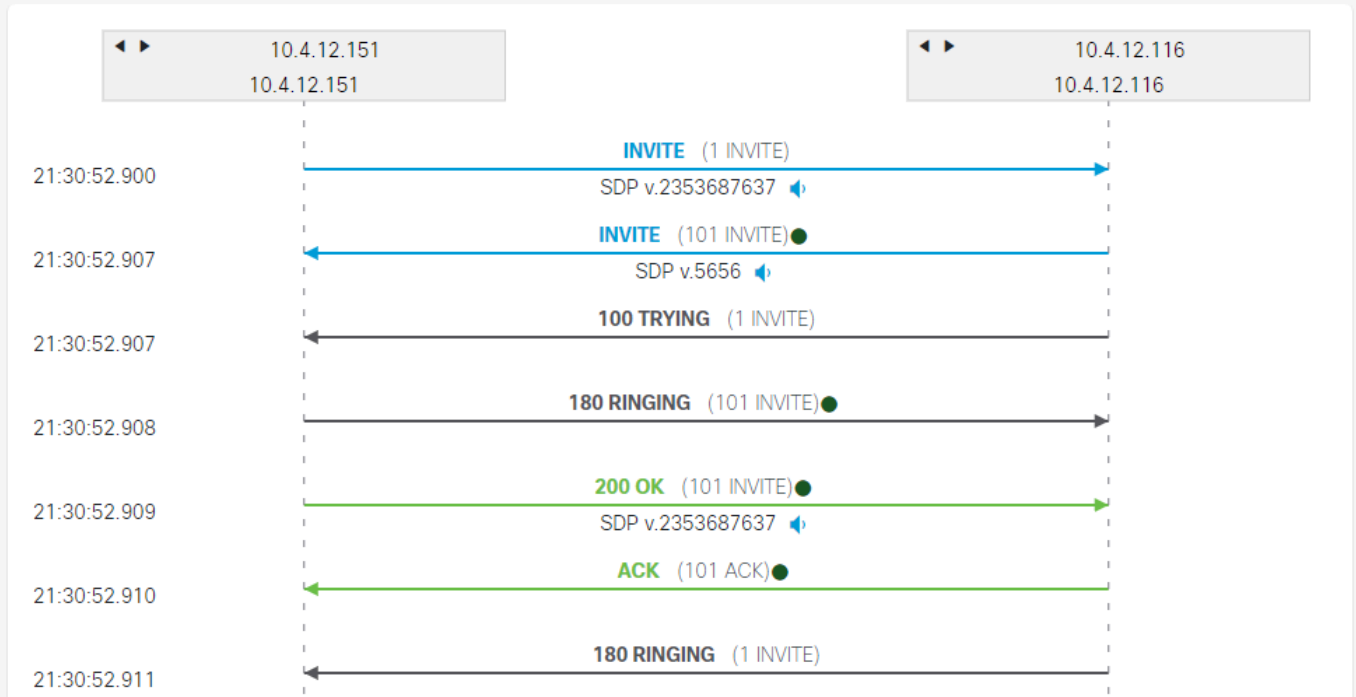
Etiquetas de escada do analisador de log 3

Call

Call leg info **Ladder diagram** Signalling

Allow horizontal scroll

Legend: ■ Voice Codec G711ulaw



Etiquetas de escada do analisador de log 4

Sinalização

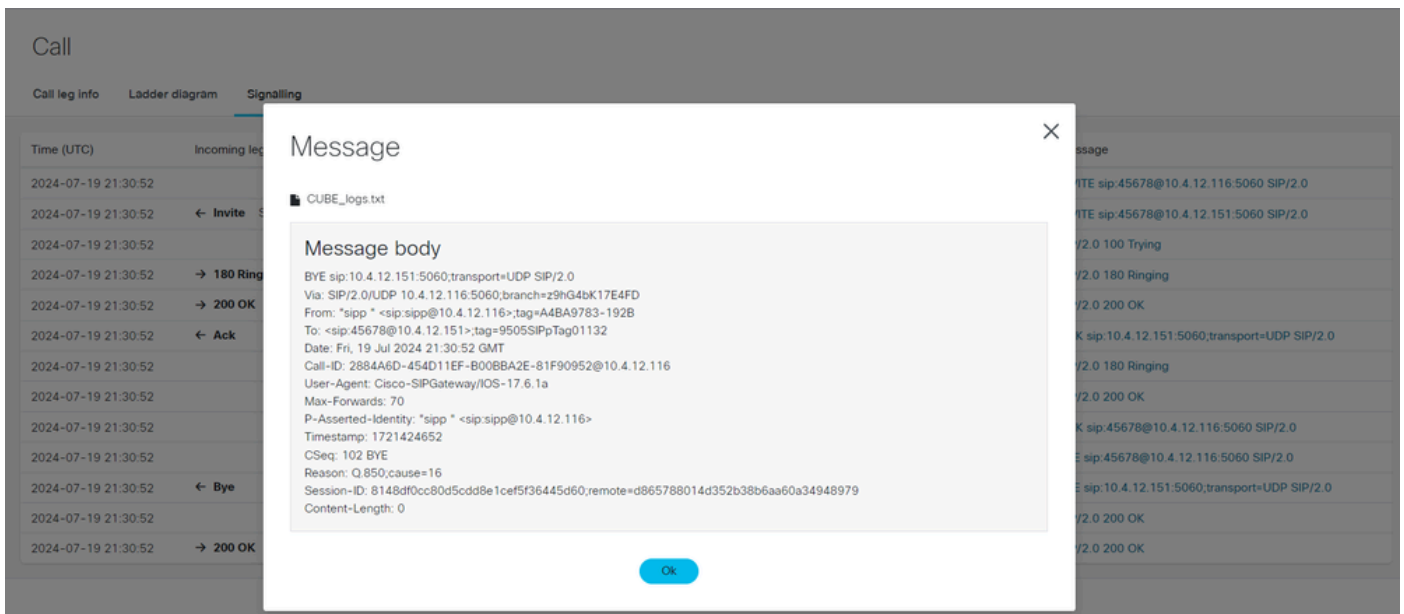
O último estágio é a Sinalização, que exibe as mensagens SIP para os dois trechos do CUBE (entrada e saída). Ele contém os endereços IP origem e destino. Clique para exibir a mensagem.

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

Sinalização do analisador de log



Mensagem de Sinalização do Analisador de Log

Diagnósticos

Todos os dados analisados nos registros são executados em Assinaturas de Diagnóstico que identificam defeitos conhecidos, problemas comumente observados ou configurações incorretas e fornecem um plano de ação corretivo.

Depois que uma chamada capturada nos registros tiver sido selecionada para exibir a análise resumida da chamada, a plataforma CSA exibirá a seção Diagnóstico, que contém as seguintes informações:

- Problemas encontrados
- Informações Ausentes
- Problema potencial

Um botão de alternância pode ser ativado para filtrar e exibir somente defeitos.

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	552447	1-9880@10.4.12.151	552448	02876031B005	2024-07-19 21:30:52	2024-07-19 21:30:52	0 seconds	0
sipp	45678	552448	2884A6D-454D11E-F-B00BBA2E-81F90952@10.4.12.116	552447	02876031B005	2024-07-19 21:30:52	2024-07-19 21:30:52	0 seconds	16

1-2 of 2 Prev 1 Next Showing 10

Home de Diagnósticos do Analisador de Log

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](#).

Visão geral do Log Analyzer Diagnostics

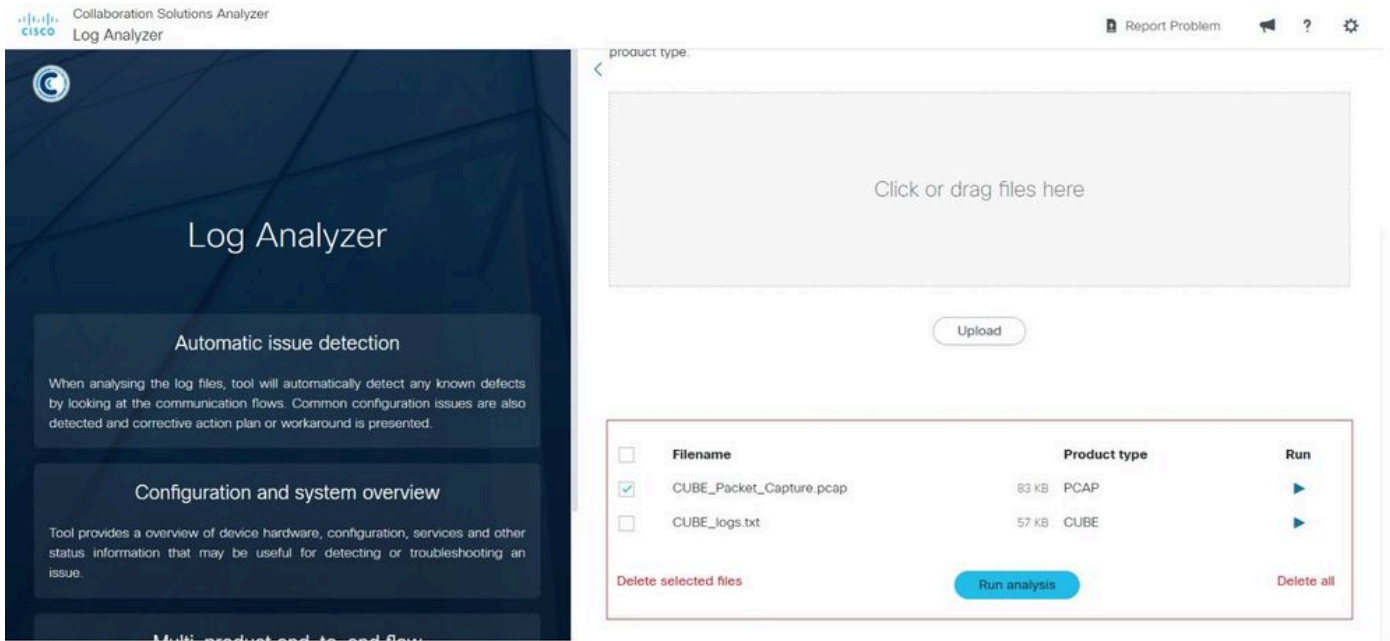
Captura de pacotes do CUBE

A captura de pacotes é um buffer de arquivos criado para reunir uma cópia dos pacotes reais em uma interface de rede do CUBE ou em qualquer dispositivo de rede de voz. Esse arquivo pode ser aberto e analisado por um software analisador de rede, como o Wireshark.

A ferramenta Log Analyzer foi aprimorada com um analisador de Captura de Pacotes que pode processar extensões de formato de arquivo pcap ou pcapng, fornecendo um resumo de estatísticas de sessão e rede coletadas de chamadas.

O arquivo de Captura de Pacotes deve ser carregado na ferramenta Log Analyzer da mesma


forma que o arquivo de log do CUBE. O sistema determina o tipo de produto como PCAP.



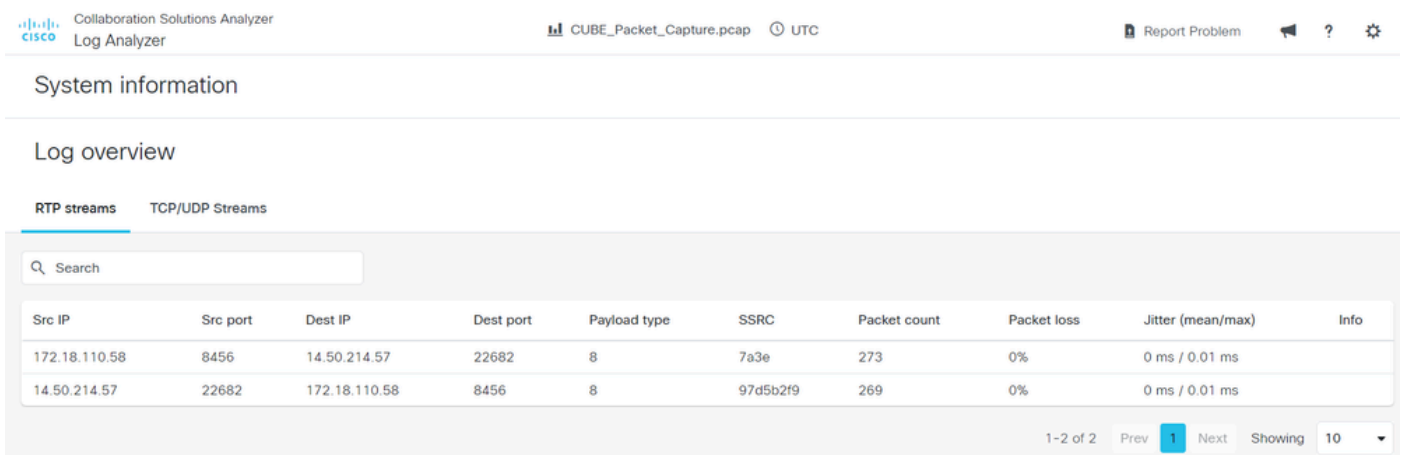
Arquivo de Captura de Pacotes do Analisador de Log

Quando o botão Executar análise é ativado, a ferramenta Analisador de log analisa as informações e fornece um resumo das sessões capturadas em duas colunas:

- Fluxos de RTP
- Fluxos TCP/UDP

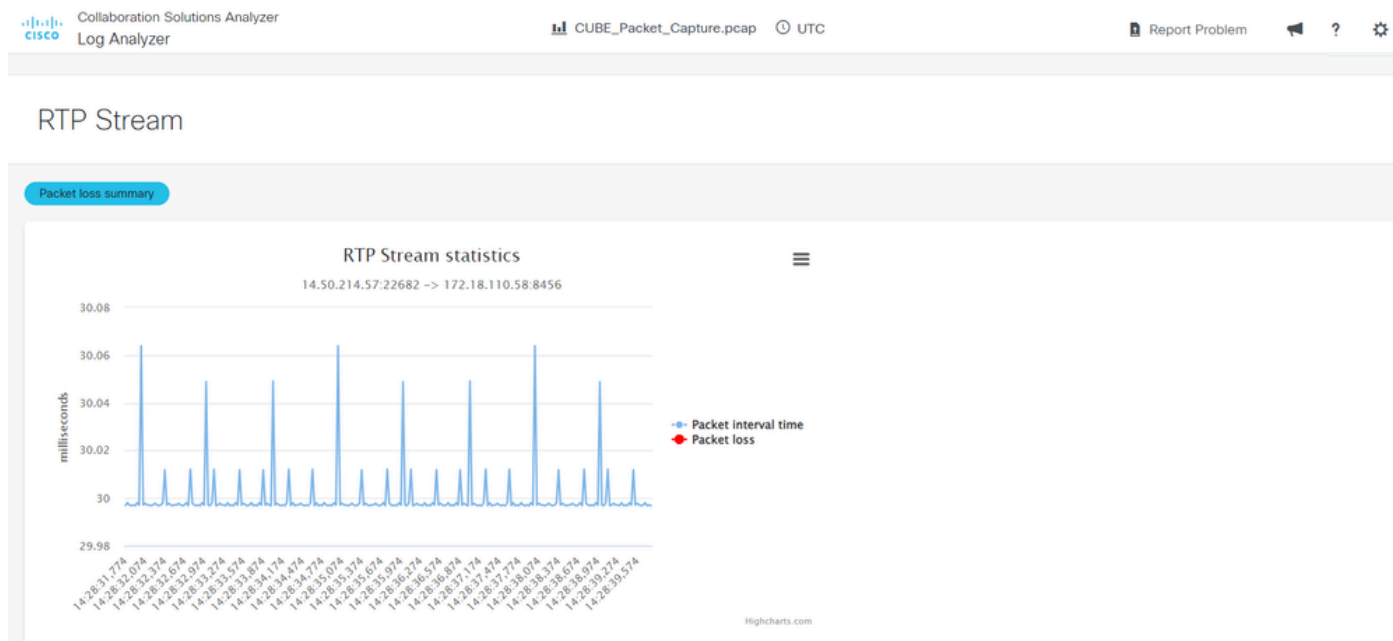
 **Observação:** se a captura de pacotes incluir fluxos SRTP, ela será mostrada na coluna 'Fluxos RTP' e uma análise de rede será executada. A parte de áudio de um fluxo SRTP não é decodificada.

Selecione uma sessão na coluna Fluxos de RTP e a ferramenta exibirá o status do fluxo de RTP para essa conexão. Se o fluxo estiver a ser afetado pelas condições da rede, o parâmetro "Perda de pacotes" deve ser marcado com pontos vermelhos.



Análise PCAP do Log Analyzer

O download das estatísticas de fluxo RTP pode ser feito em um formato de arquivo de texto que contém um resumo da perda de pacotes. Clique no botão Packet Loss Summary para fazer o download do arquivo.



Fluxo PCAP RTP do Analisador de Log

Para fluxos TCP/UDP, o sistema exibe o resumo das sessões capturadas.

System information

Log overview

RTP streams TCP/UDP Streams

Search

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

1-3 of 3 Prev 1 Next Showing 10

Fluxos UDP TCP PCAP do Analisador de Log

Testador de perfil SIP (SPT)

Os perfis SIP (Session Initiation Protocol) são usados para modificar mensagens SIP de entrada ou saída para garantir a compatibilidade entre dispositivos diferentes. A ferramenta "Testador de perfil SIP" permite validar sua configuração antes de implantá-la em um ambiente ativo.

A ferramenta Perfil SIP consiste em 3 seções:

- Regras de perfil SIP - Janela para inserir as regras de PERFIL SIP a serem testadas.
- Mensagem SIP para aplicar regras - Janela para colar a mensagem SIP onde as regras

devem ser aplicadas.

- Mensagem SIP para copiar de - (Opcional) Janela para colar uma mensagem SIP caso uma configuração de lista de cópia seja testada. Uma configuração de lista de cópia copia o conteúdo de um cabeçalho de entrada recebido por um dispositivo para um cabeçalho de saída.

A ferramenta contém 2 botões para gerenciar os testes:

- Botão verde - Para executar um teste.
- Botão vermelho - Para redefinir e limpar as configurações.

Depois de selecionar o botão verde para executar o teste, a ferramenta exhibe estas opções:

- Botão vermelho - Novo teste
- Botão azul - Mostrar entradas

Destaque dos resultados da mensagem SIP original/modificada:

- Blue Color - (Cor azul) Os cabeçalhos SIP modificados ou o corpo SDP estão destacados em azul nas duas áreas de mensagem.
- Cor verde - Cabeçalhos SIP ou Corpo SDP adicionados são realçados em verde somente no resultado da mensagem SIP modificado.
- Cor vermelha - Os cabeçalhos SIP ou o corpo SDP removidos são realçados em vermelho somente no resultado da mensagem SIP original.

The screenshot shows the Cisco Collaboration Solutions Analyzer interface. At the top, it displays the Cisco logo and the text 'Collaboration Solutions Analyzer'. On the right side, there are icons for 'UTC', 'Report Problem', a help icon, and a settings icon. The main interface is divided into two primary sections: 'SIP Profile Rules' and 'SIP Message To Test Rules On'. Both sections have a 'required' status indicator and a 'Load' button. The 'SIP Profile Rules' section contains a text area with a sample rule: 'rule 1 response 182 sip-header SIP-StatusLine modify "182 Queued" "183 Session In Progress"'. Below this text area, there is an 'Input Help' section stating that copylist, voice service voip, dial-peer, tenant, or other voice configurations are not required, and a 'Syntax Help' link to SIP Profile Config Guide and SIP Copylist Config Guide. The 'SIP Message To Test Rules On' section has a text area for entering the SIP message. Below it, there is an 'Input Help' section stating that SIP Request URI or Status Line is always required, and SIP Headers/SDP Body is optional unless testing them. There is also a 'Syntax Help' link to IANA SIP Parameters and IANA SDP Parameters. Below these sections, there is a 'Peer SIP Message To Copy From' section with an 'optional' status and a 'Show Peer Copy Input' button. At the bottom of the interface, there are two buttons: 'New Test' (red) and 'Run Test' (green).

Início do PERFIL SIP

Exemplo de perfil SIP pré-criado

A ferramenta fornece exemplos pré-desenvolvidos para simplificar os testes. Na parte superior de cada janela, há uma caixa de aplicativo para selecionar esses exemplos.

Veja como usar uma configuração predefinida:

1. Clique em Load a Prebuilt Rule Set e selecione Add: SIP Header.
2. Clique em Carregar uma Mensagem SIP de Amostra e selecione CONVITE (Sem SDP).
3. Selecione o botão verde Run Test para executar o teste.

The screenshot displays the Cisco Collaboration Solutions Analyzer interface. On the left, under 'SIP Profile Rules', a rule is defined: 'rule 100 request ANY sip-header Diversion Add "Diversion: < sip:8675309@cisco.com>"'. Below this, there are 'Input Help' and 'Syntax Help' sections. On the right, under 'SIP Message To Test Rules On', a prebuilt rule is selected: 'INVITE (No SDP)'. The main area shows a detailed SIP INVITE message with various headers and body text. At the bottom, there are 'New Test' and 'Run Test' buttons.

PERFIL SIP Pré-construído

A ferramenta exibe uma nova tela com os resultados do teste:

Mensagem SIP modificada

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 Require: 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 Require: 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>"

Exemplo de Adição Pré-construída de SIP PROFILE

Este é um exemplo do realce de modificação/adição/remoção:

Regras de perfil SIP

```

rule 100 request ANY sip-header Diversion Add "Diversion: <sip:8675309@cisco.com>"
rule 200 request ANY sip-header P-Asserted-Identity modify "sip:444444444@" "sip:555555555@"
rule 300 request ANY sip-header P-Preferred-Identity remove

```

Mensagem Sip Para Testar Regras Em

```

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 adds a Diversion header, rule 200 modifies the P-Asserted-Identity header, and rule 300 removes the P-Preferred-Identity header. On the right, under 'SIP Message To Test Rules On', a sample INVITE message is displayed with various headers and body content. The interface includes buttons for 'New Test' and 'Run Test' at the bottom.

SIP PROFILE Modificar Adicionar Remover Exemplo

Para ver o resultado, clique em Run Test (Executar teste).

Mensagem SIP original

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

4444444444@192.168.10.10>

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

Mensagem SIP modificada

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>', and 'To: <sip:8675309@192.168.10.10>'. It includes session details like 'Session-ID: 2d390a8000105000a000247e1266c26d' and 'Cisco-Guid: 3622027175-0860951023-223888512-1803467483'.

Modified SIP Message: Shows the same SIP message but with modifications. Key changes include the 'P-Asserted-Identity' header being set to 'CallerID_Name' <sip:555555555@192.168.10.10> and a 'Diversion' header added: 'Diversion: <sip:8675309@cisco.com>'. The 'Remote-Party-ID' is also updated to 'CallerID_Name' <sip:333333333@192.168.10.10>.

Logs: A table showing the actions performed on the message:

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

Exemplo 2 de Modificação de PERFIL SIP Adicionar/Remover

Perfil SIP da Lista de Cópias

Para copiar conteúdo de um cabeçalho de entrada que um dispositivo recebe para um cabeçalho de saída (lista de cópia SIP), estas entradas de ferramenta podem ser usadas:

- Fluxograma: Mensagem SIP de Entrada —> CUBE —> Mensagem SIP Modificada
- Mensagem SIP de Par para Copiar de - Mensagem SIP para copiar.
- Mensagem Sip para testar regras em - Mensagem SIP para aplicar regras.

Para habilitar a seção Mensagem SIP do Par para Copiar de, a opção Mostrar Entrada de Cópia do Par deve ser habilitada. Você pode clicar em Hide Peer Copy Input para ocultar esta seção.

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.

Página Inicial da Lista de Cópias do PERFIL SIP

Este é um exemplo de Regras SIP, Mensagens SIP de Entrada e Modificadas:

Regras de perfil SIP.

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

Mensagem SIP para aplicar regras.

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

Mensagem SIP da qual copiar.

Received:

INVITE sip:235678@10.15.0.2:5060 SIP/2.0
Via: SIP/2.0/UDP 10.14.0.1:5060;branch=z9hG4bK16927e56b400c78
From: "Cisco" <sip:1234@10.14.0.1>;tag=156812752~757956d9-2b62-4ab0-b5c2-6b19710635db-53693198
To: <sip:5678@10.15.0.2>
Call-ID: a0f63500-1f013804-1344e15-16000e0a@10.14.0.1
Supported: 100rel,timer,resource-priority,replaces
Min-SE: 1800
User-Agent: Cisco-CUCM12.5
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
CSeq: 101 INVITE
Expires: 180
Allow-Events: presence, kpm1
Supported: X-cisco-srtp-fallback,X-cisco-original-called
Call-Info: <sip:10.14.0.1:5060>;method="NOTIFY;Event=telephone-event;Duration=500"
Call-Info: <urn:x-cisco-remotecc:callinfo>;x-cisco-video-traffic-class=DESKTOP
Session-ID: 1629a67700105000885a92d9a7fe;remote=00000000000000000000000000000000
Cisco-Guid: 2700489984-0000065536-0000126777-1234102346
Session-Expires: 1800
P-Asserted-Identity: "Cisco" <sip:1234@10.14.0.1>
Remote-Party-ID: "Cisco" <sip:1234@10.14.0.1>;party=calling;screen=yes;privacy=off
Contact: <sip:1234@10.14.0.1:5060>;+u.sip!devicename.ccm.cisco.com="SEP885A92D9A7FE"
Max-Forwards: 69
Content-Length: 0

SIP Profile Rules required

Load a Prebuilt Rule Set

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

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

SIP Message To Test Rules On required

Load a sample SIP Message

```
Sent:
INVITE sip:235678@10.16.0.5:5060 SIP/2.0
Via: SIP/2.0/UDP 192.0.2.0:5060;branch=2964647155C
From: "Cisco" <sip:1234@10.16.0.3>;tag=8125CE72-1184
To: <sip:5678@10.16.0.5>
Call-ID: 7835570P-193611EF-AC18962-D5D3EC10@192.0.2.0
Supported: 100rel,timer,resource-priority,replaces,sdp-annot
Min-SE: 1800
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
CSeq: 101 INVITE
Timestamp: 1716577979
Contact: <sip:1234@192.0.2.0:5060>
Expires: 180
Allow-Events: telephone-event
Max-Forwards: 68
P-Asserted-Identity: "Cisco" <sip:9876@192.0.2.0>
Session-ID: 1629a6770010500a00009a7fe;remote=00000000000000000000000000000000
Session-Expires: 1800
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 243
```

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

Peer SIP Message To Copy From required

Hide Peer Copy Input

```
Received:
INVITE sip:235678@10.15.0.2:5060 SIP/2.0
Via: SIP/2.0/UDP 10.14.0.1:5060;branch=29646416927456440b-78
From: "Cisco" <sip:1234@10.14.0.3>;tag=156812752-75795649-2062-4ab0-b5c2-6b19710635db-53693198
To: <sip:5678@10.15.0.2>
Call-ID: a9f63508-1f013004-1344e15-1600be@10.14.0.1
Supported: 100rel,timer,resource-priority,replaces
Min-SE: 1800
User-Agent: Cisco-CUCM12.5
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
Expires: 180
```

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

New Test
Run Test

Exemplo de Copylist de SIP PROFILE

Continue clicando no botão Run Test para iniciar a ferramenta.

Copiar Registro

Register: u01
Value: 5678

Mensagem SIP original

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

Mensagem SIP modificada

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

Report an issue



Product

Issue

Details about an issue

Cancel

Send

Relatar Problema

Três ícones foram ativados para permitir que o usuário forneça feedback (ícone do megafone), revise a documentação do usuário (ícone do ponto de interrogação) e abra as configurações do usuário (ícone do cogwheel).

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

Ícones

Informações relacionadas ao suporte

[Configurar a coleta de depuração para gateways CUBE e TDM](#)

[Guia de configuração do Cisco Unified Border Element através do Cisco IOS XE 17.5](#)

[Capítulo: Perfis SIP](#)

[Usar perfis SIP em casos de uso comuns do CUBE Enterprise](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.