Configuration Note

AudioCodes Professional Services – Interoperability Lab

Pindrop Fraud Detection and Authentication Solution with GenesysCloud Contact Center using AudioCodes Mediant™ SBC

Version 7.4

Table of Contents

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: January-11-2023

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at https://www.audiocodes.com/services-support/maintenance-and-support.

Stay in the Loop with AudioCodes

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

General Notes, Warnings, and Safety Information

OPEN SOURCE SOFTWARE. Portions of the software may be open source software and may be governed by and distributed under open source licenses, such as the terms of the GNU General Public License (GPL), the terms of the Lesser General Public License (LGPL), BSD and LDAP. If any open source software is provided in object code, and its accompanying license requires that it be provided in source code as well, the Buyer may receive such source code by contacting AudioCodes.

Document Revision Record

LTRT	Description
39465	Initial document release
39466	Update of Pindrop Solution Name
39467	Updates according to latest Pindrop implementation
39468	Update about Account ID according to Pindrop request

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at https://online.audiocodes.com/documentation-feedback.

1 Introduction

This *Configuration Note* describes an example implementation of AudioCodes Session Border Controller (referred to in this document as *SBC*) for interworking between AudioCodes Contact Center and Pindrop Fraud Detection and Authentication Solution.

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and AudioCodes Partners who are responsible for installing and configuring AudioCodes Contact Center and AudioCodes SBC for enabling recording VoIP calls using Pindrop Fraud Detection and Authentication Solution.

1.2 About AudioCodes SBC Product Series

AudioCodes' family of SBC devices enables reliable connectivity and security between the Enterprise's and the service provider's VoIP networks.

The SBC provides perimeter defense as a way of protecting Enterprises from malicious VoIP attacks; mediation for allowing the connection of any PBX and/or IP-PBX to any service provider; and Service Assurance for service quality and manageability.

Designed as a cost-effective appliance, the SBC is based on field-proven VoIP and network services with a native host processor, allowing the creation of purpose-built multiservice appliances, providing smooth connectivity to cloud services, with integrated quality of service, SLA monitoring, security and manageability. The native implementation of SBC provides a host of additional capabilities that are not possible with standalone SBC appliances such as VoIP mediation, PSTN access survivability, and third-party value-added services applications. This enables Enterprises to utilize the advantages of converged networks and eliminate the need for standalone appliances.

AudioCodes SBC is available as an integrated solution running on top of its field-proven Mediant Media Gateway and Multi-Service Business Router platforms, or as a software-only solution for deployment with third-party hardware.

1.2.1 Known Limitations

There were no limitations observed in the homologation tests run between the Pindrop Fraud Detection and Authentication Solution and AudioCodes Contact Center through AudioCodes' SBC.

2 Configuring Pindrop Fraud Detection and Authentication Solution

The Pindrop Fraud Detection and Authentication Solution is a managed service, Pindrop is responsible for the configuration of the managed service.

3 Configuring a Trunk on GenesysCloud

This section shows an example of the GenesysCloud Contact Center settings for integrating with Pindrop Fraud Detection and Authentication Solution and AudioCodes' SBC.

Figure 3-1: Configured External Trunk to AudioCodes SBC

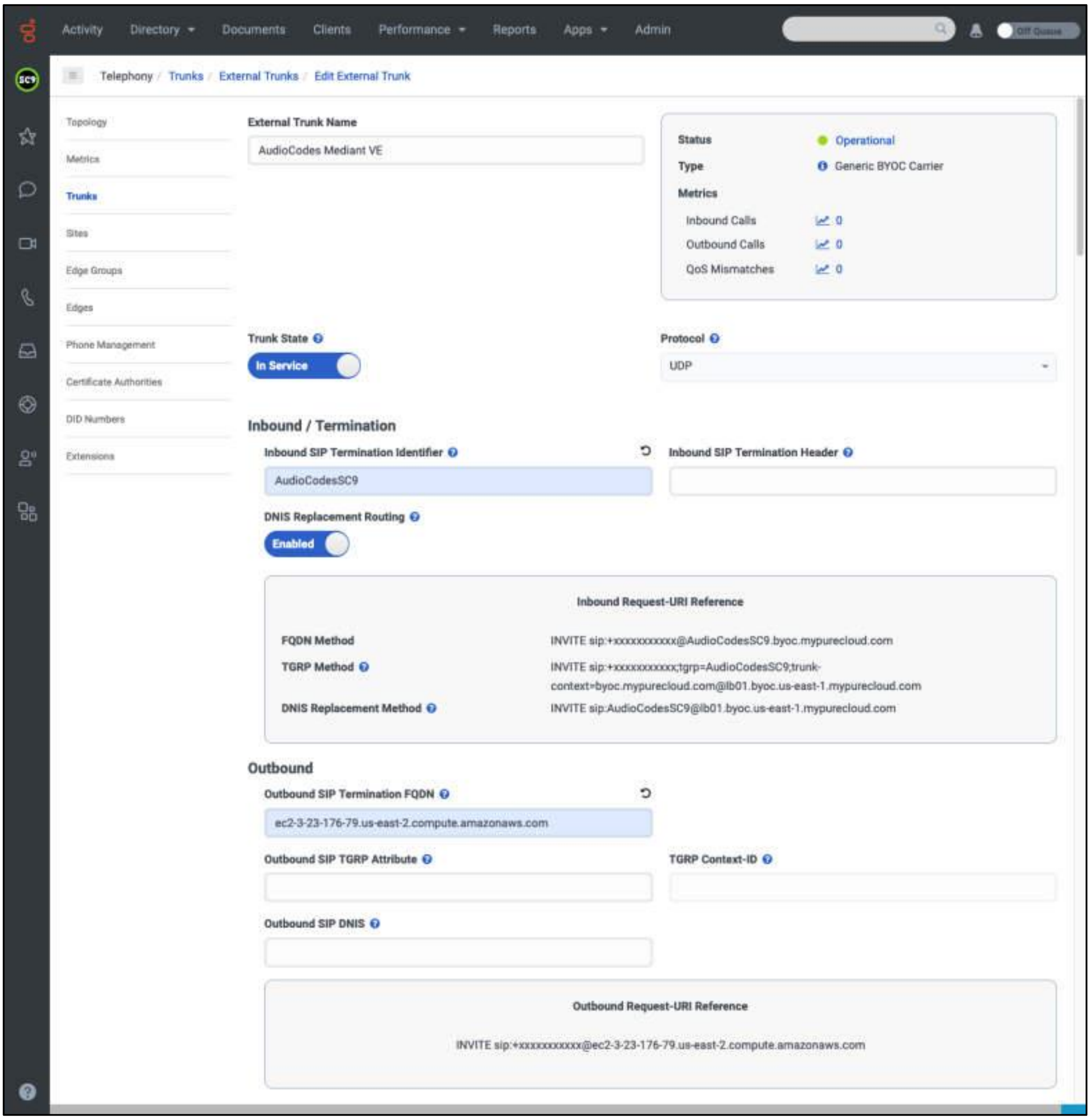


Figure 3-2: Configured SIP Access Control

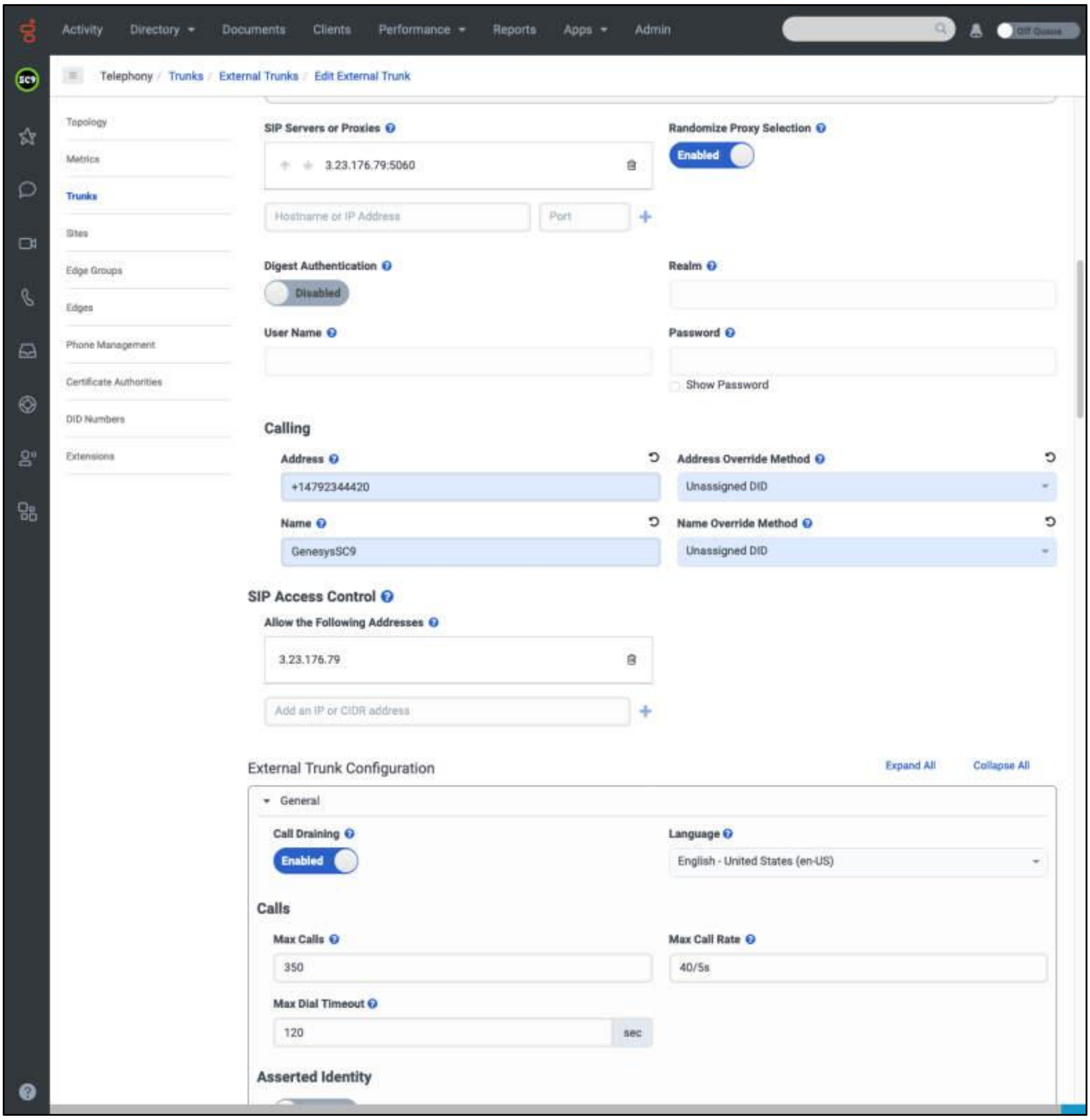


Figure 3-3: Configured Inbound/Outbound Rules

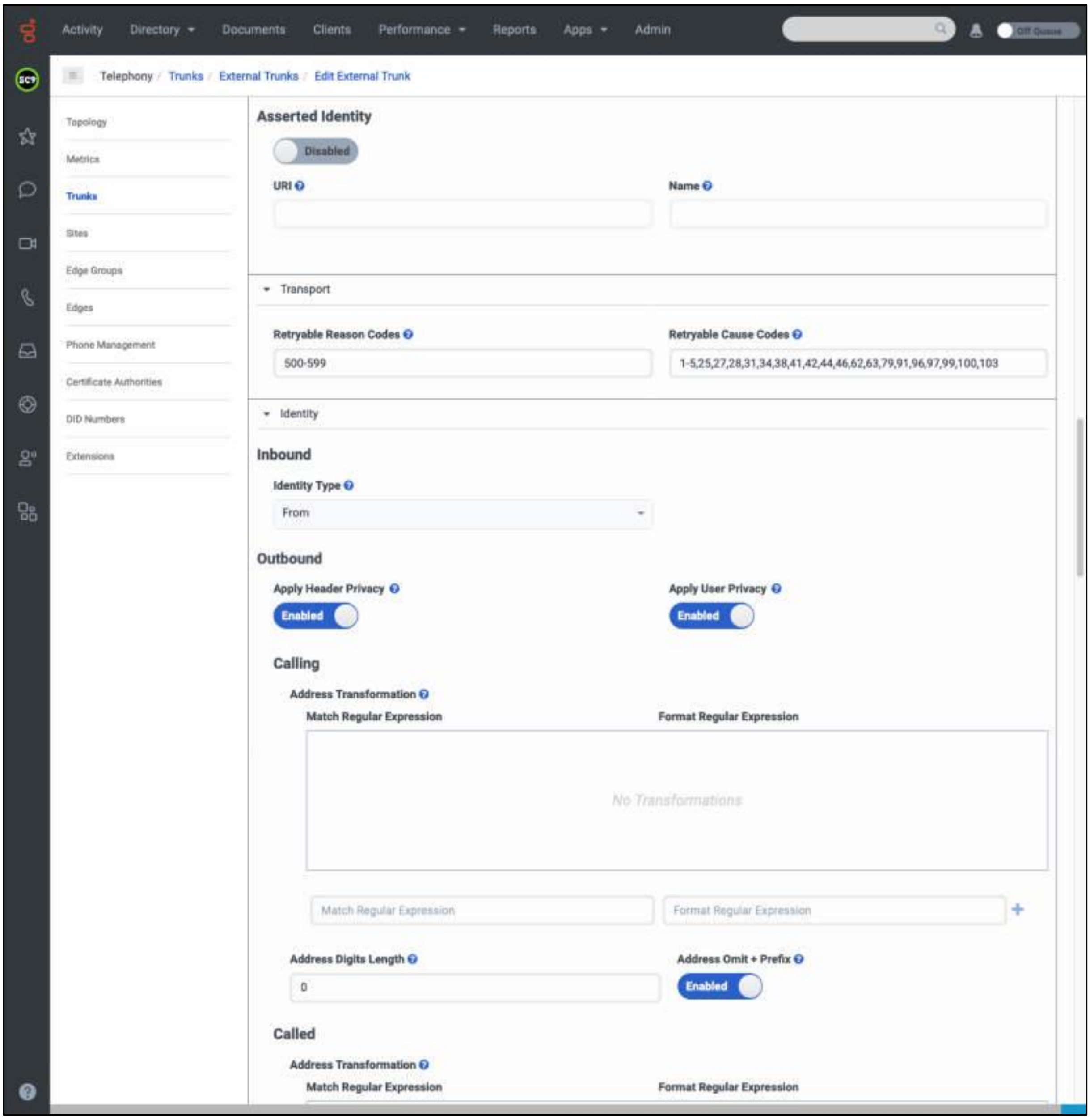


Figure 3-4: Configured Media Behavior

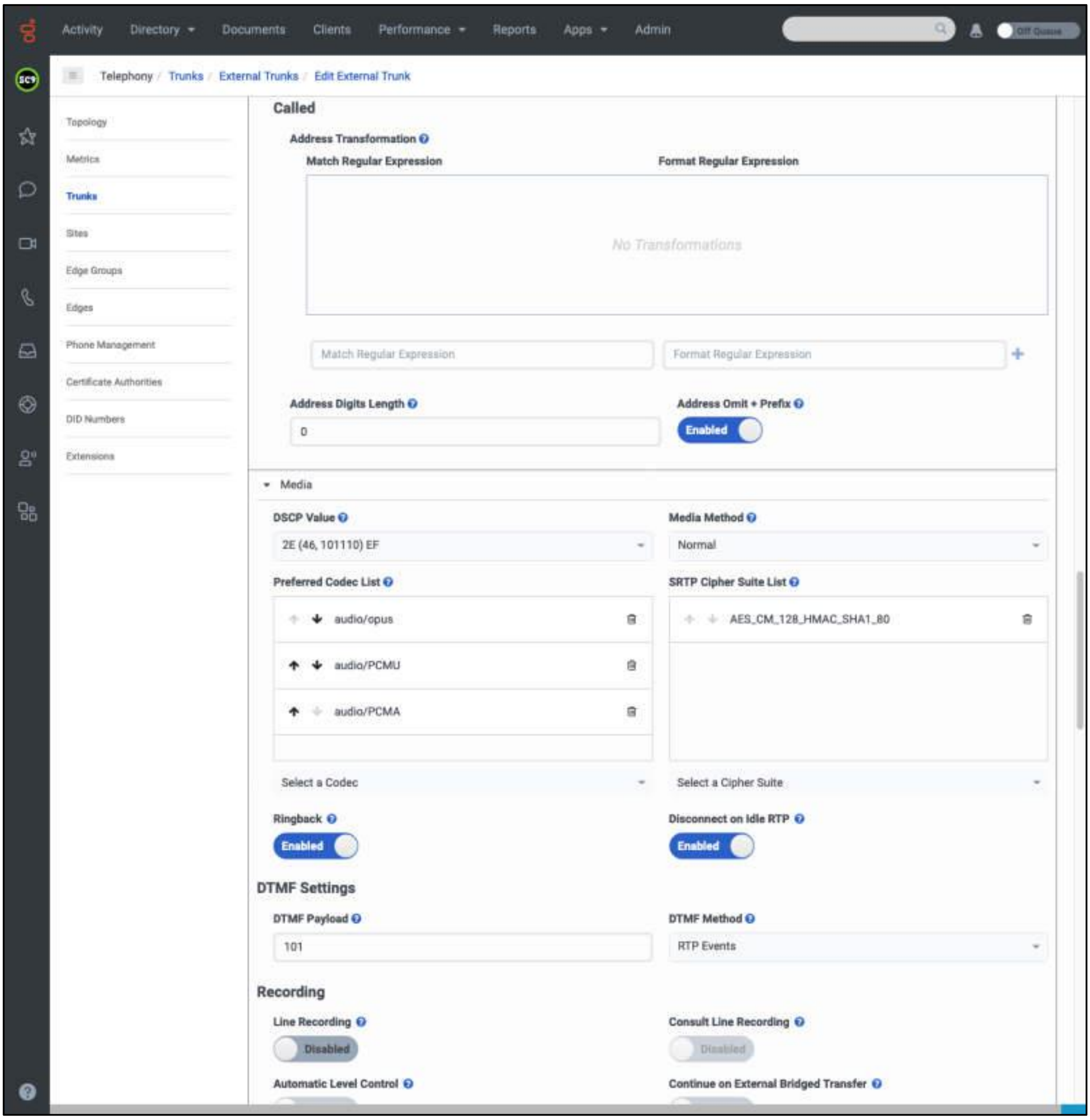


Figure 3-5: Configured User to User Information (UUI)

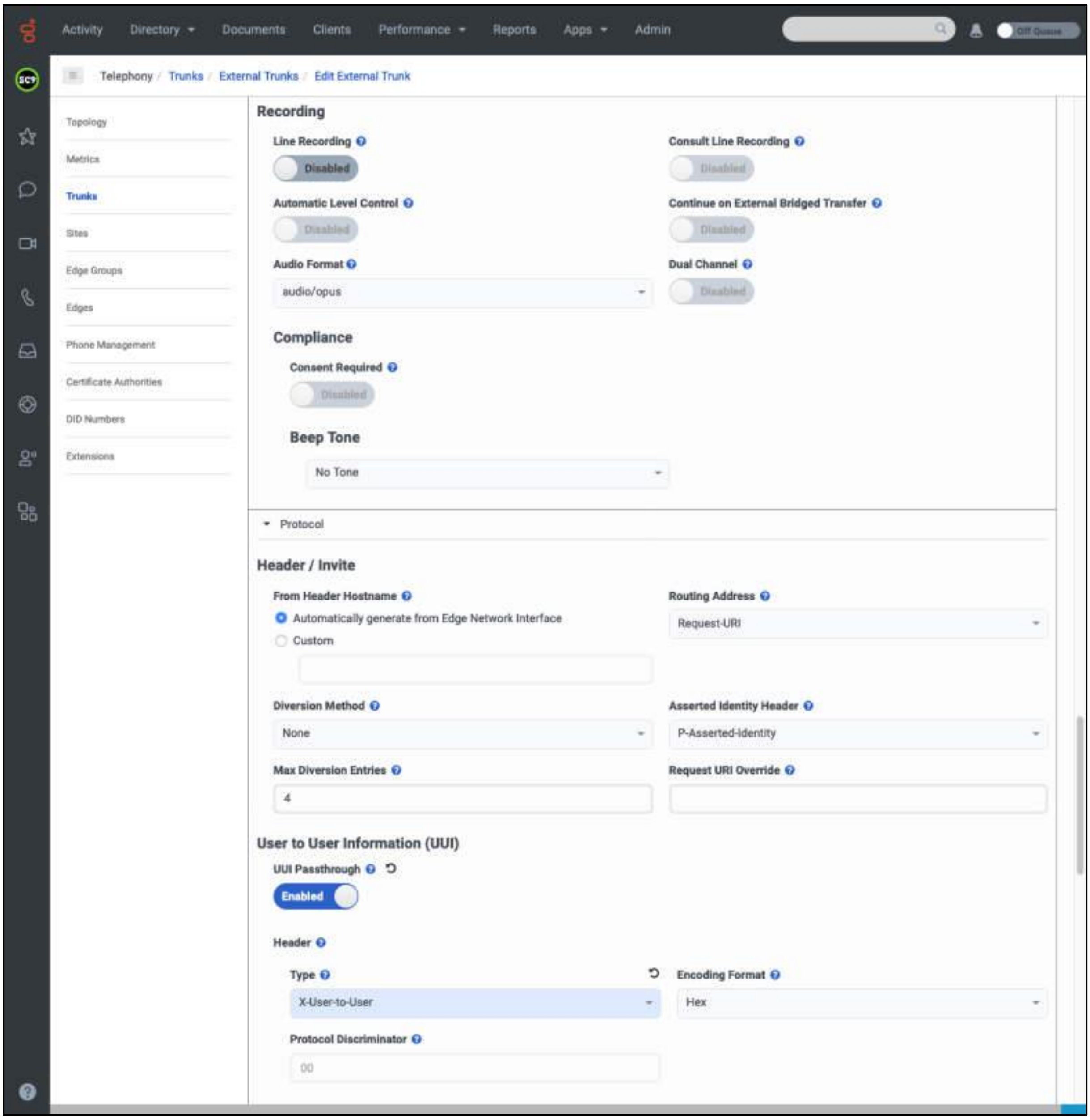


Figure 3-6: Configured User Data

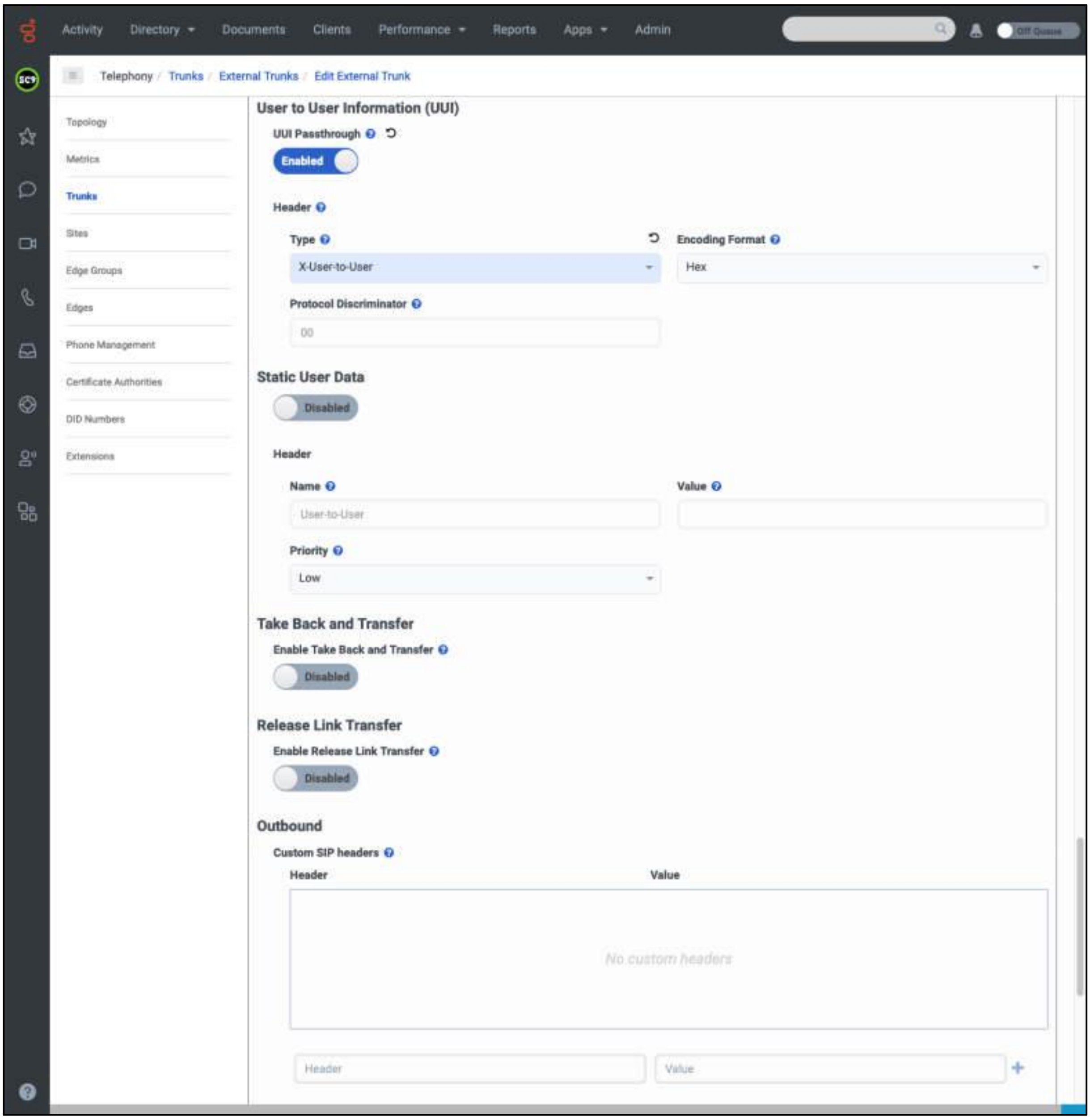
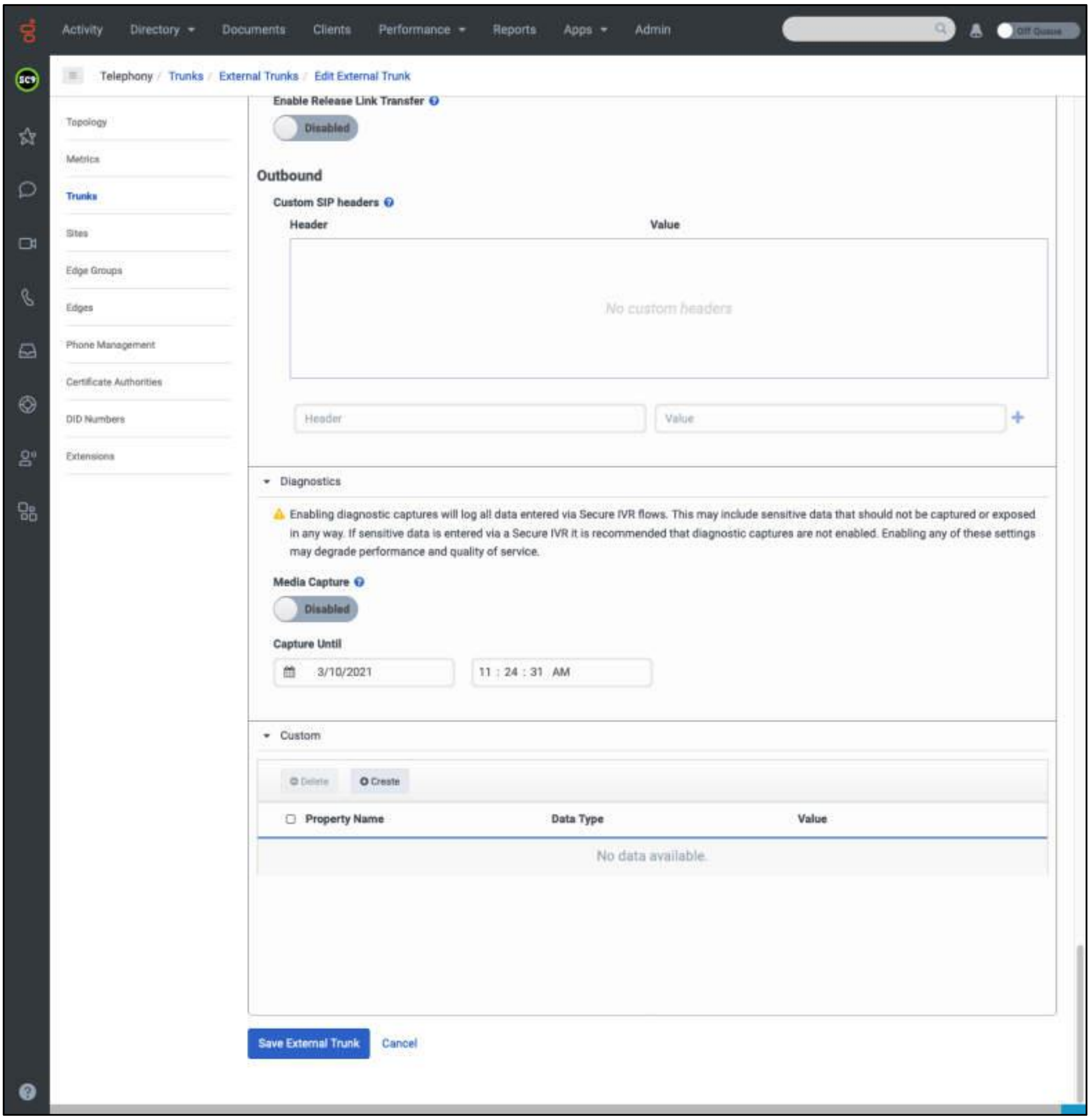


Figure 3-7: Save Trunk Configuration



4 Configuring AudioCodes SBC

This section shows how to configure AudioCodes' SBC for interworking between Pindrop Fraud Detection and Authentication Solution and the AudioCodes Contact Center.

The configuration is performed using the SBC's embedded Web server (referred to in this document as *Web interface*).

- For implementing Pindrop Fraud Detection and Authentication Solution and AudioCodes Contact Center based on the configuration described in this section, AudioCodes' SBC must be installed with a License Key that includes the following software features:
  - SBC Sessions
  - Security
  - SIPRec Sessions

  For more information about the License Key, contact your AudioCodes sales representative.
- The scope of this document does **not** cover all security aspects for configuring this topology. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products, refer to the *Recommended Security Guidelines* document, which can be found on AudioCodes' website.

4.1 IP Network Interface Configuration

This section describes how to configure the SBC's IP network interface. There are several ways to deploy the SBC; however, **this** test topology employs the following deployment method:

- SBC implemented in the Amazon with 3 IP interfaces, used for the following purposes:
  - AudioCodes Contact Center and Management (OAMP)
  - Vonage SIP Trunk
  - Pindrop Fraud Detection and Authentication Solution

4.1.1 Configure Network Interface

The Network Interface is configured automatically in the Amazon implementation. Refer to the *Mediant Virtual Edition SBC for Amazon AWS Installation Manual* or the *Mediant Cloud Edition SBC Installation Manual* to configure the Amazon image (AMI).

4.1.2 Configure NAT Translation

The SBC, located in the Amazon Cloud, implements private IP addresses. The NAT Translation table lets you configure network address translation (NAT) rules for translating source IP addresses into NAT IP addresses (*global* - *public*) used in front of the Amazon firewall facing the AudioCodes, Vonage SIP Trunk and Pindrop Fraud Detection and Authentication Solution.

To configure the NAT translation rules:

1. Open the NAT Translation table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **NAT Translation**).
2. Click **New**; use the following table as reference when configuring a NAT translation rule:

Parameter	Value
Index	**0**
Source Interface	**eth0** (IP Network Interface, configured in the previous section)
Source Start Port	**1**
Source End Port	**65535**
Target IP Mode	**Automatic** (this mode is required if your AWS environment has been configured with an Elastic IP address and you want the device to automatically associate it with the selected source interface as the global (public) IP address).
Target IP Address	Configured only if the previous parameter is configured with 'Manual' value.
Automatic Target IP Address	Read-only-field

3. Click **Apply**.

Configure additional rules for each IP Interface.

4.2 Configure Media Realms

This section describes how to configure Media Realms. In this test topology Media Realm was created for each entity.

To configure Media Realms:

1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Configure Media Realms as follows (you can use the default Media Realm (Index 0), but modify it):

Table 4-1: Configuration Example Media Realms in Media Realm Table

Index	Name	Topology Location	IPv4 Interface Name	Port Range Start	Number of Media Session Legs
0	GenesysCloud (arbitrary name)		eth0	6000	100 (media sessions assigned with port range)
1	Vonage (arbitrary name)	Up	eth1	6000	100 (media sessions assigned with port range)
2	Pindrop (arbitrary name)		eth2	6000	100 (media sessions assigned with port range)

4.3 Configure SIP Signaling Interfaces

This section describes how to configure SIP Interfaces. As Media Realms, for the homologation test topology, three SIP Interfaces must be configured – one for each destination.

To configure SIP Interfaces:

1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
2. Configure SIP Interfaces. You can use the default SIP Interface (Index 0), but modify it as shown in the table below. The table below shows an example of the configuration. You can change some parameters according to your requirements.

Table 4-2: Configured SIP Interfaces in SIP Interface Table

Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Classification Failure Response Type	Media Realm
0	GenesysCloud (arbitrary name)	eth0	SBC	5060	5060	5061	0 (Recommended to prevent DoS attacks)	GenesysCloud
1	Vonage (arbitrary name)	eth1	SBC	5060	0	0	0 (Recommended to prevent DoS attacks)	Vonage
2	Pindrop (arbitrary name)	eth2	SBC	5060	5060	5061	0 (Recommended to prevent DoS attacks)	Pindrop

4.4 Configure Proxy Sets and Proxy Address

This section describes how to configure Proxy Sets. The Proxy Set defines the destination address (IP address or FQDN) of the IP entity server. Proxy Sets can also be used to configure load balancing between multiple servers.

For the homologation test topology, three Proxy Sets need to be configured for the following IP entities:

- AudioCodes Contact Center
- Vonage SIP Trunk
- Pindrop Fraud Detection and Authentication Solution

The Proxy Sets will be later applied to the VoIP network by assigning them to IP Groups.

To configure Proxy Sets:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder >**Proxy Sets**).
2. Configure Proxy Sets as shown in the table below:

Table 4-3: Configuration Example Proxy Sets in Proxy Sets Table

Index	Name	SBC IPv4 SIP Interface	Proxy Keep-Alive	DNS Resolve Method
1	ProxySet_GenesysCloud (arbitrary name)	GenesysCloud	Using Options	-
2	ProxySet_Vonage (arbitrary name)	Vonage	Using Options	SRV
3	Pindrop (arbitrary name)	Pindrop	Using Options	-

4.4.1 Configure a Proxy Address

This section shows how to configure a Proxy Address.

To configure a Proxy Address for ProxySet_GenesysCloud:

1. Open the Proxy Sets table (Setup menu > Signaling & Media tab > Core Entities folder > Proxy Sets) and then click the Proxy Set **ProxySet_GenesysCloud**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
2. Click **+New**; and configure the address of the Proxy Set according to the parameters described in the table below:

Table 4-4: Configuration Example of Proxy Address for ProxySet_GenesysCloud

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	123.123.123.123:5060 (IP address and port of GenesysCloud Server 1)	UDP	0	0
1	124.124.124.124:5060 (IP address and port of GenesysCloud Server 2)	UDP	0	0
2	125.125.125.125:5060 (IP address and port of GenesysCloud Server 3)	UDP	0	0

3. Click **Apply**.

To configure a Proxy Address for ProxySet_Vonage:

1. Open the Proxy Sets table (Setup menu > Signaling & Media tab > Core Entities folder > Proxy Sets) and then click the Proxy Set **ProxySet_Vonage**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
2. Click **+New**; and configure the address of the Proxy Set according to the parameters described in the table below:

Table 4-5: Configuration Example of Proxy Address for ProxySet_Vonage

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	sip-us-2-1.nexmo.com (FQDN of the Vonage SIP Trunk)	UDP	0	0
1	321.321.321.321 (IP address of Vonage SIP Trunk Server 1)	UDP	0	0
2	322.322.322.322 (IP address of Vonage SIP Trunk Server 2)	UDP	0	0
3	323.323.323.323 (IP address of Vonage SIP Trunk Server 3)	UDP	0	0

3. Click **Apply**.

To configure a Proxy Address for Pindrop:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**) and then click the Proxy Set **Pindrop**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
2. Click **+New**; and configure the address of the Proxy Set according to the parameters described in the table below:

Table 4-6: Configuration Example of Proxy Address for Pindrop

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	456.456.456.456:5060 (IP address and port of Pindrop Recording Server)	UDP	0	0

3. Click Appl**y**.

4.5 Configure Coders

This section describes how to configure coders (termed *Coder Group*).

To configure coders:

1. Open the Coder Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Coder Groups**).
2. Modify default Coder Group:

Parameter	Value
Coder Group Name	AudioCodersGroups_0
Coder Name	▪ G.711 U-law ▪ G.711 A-law ▪ G.729

4.6 Configure IP Profiles

This section describes how to configure IP Profiles. The IP Profile defines a set of call capabilities relating to signaling (e.g., SIP message terminations such as REFER) and media (e.g., coder and transcoding method).

In this homologation test topology, IP Profiles need to be configured for the following IP entities:

- AudioCodes Contact Center and Vonage SIP Trunk

To configure an IP Profile for the AudioCodes Contact Center:

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Click **New**, and then configure the parameters as follows:

Parameter	Value
General	
Index	1
Name	GenesysCloud
SBC Media	
Extension Coders Group	AudioCodersGroups_0

3. Click **Apply**.

To configure IP Profile for the Vonage SIP Trunk:

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Click **New**, and then configure the parameters as follows:

Parameter	Value
General	
Index	2
Name	Vonage (arbitrary descriptive name)
SBC Media	
Extension Coders Group	AudioCodersGroups_0

3. Click **Apply**.

IP Profiles configuration may change according to your specific deployment topology.

4.7 Configure IP Groups

This section describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the SBC communicates. This can be a server (e.g., IP PBX or ITSP) or it can be a group of users (e.g., LAN IP phones). For servers, the IP Group is typically used to define the server's IP address by associating it with a Proxy Set. Once IP Groups are configured, they are used to configure IP-to-IP routing rules for denoting source and destination of the call.

In this homologation test topology, IP Groups must be configured for the following IP entities:

- AudioCodes Contact Center
- Vonage SIP Trunk
- Pindrop Fraud Detection and Authentication Solution

To configure IP Groups:

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Configure an IP Group for the AudioCodes Contact Center:

Parameter	Value
Index	0
Name	GenesysCloud
Type	Server
Proxy Set	ProxySet_GenesysCloud
IP Profile	GenesysCloud
Media Realm	GenesysCloud
SIP Group Name	(According to requirement)

3. Configure an IP Group for the Vonage SIP Trunk:

Parameter	Value
Index	1
Name	Vonage
Type	Server
Proxy Set	ProxySet_Vonage
IP Profile	Vonage
Media Realm	Vonage
SIP Group Name	(According to requirement)
Call Setup Rules Set ID	0

4. Configure an IP Group for the Pindrop recording system:

Parameter	Value
Index	2
Name	Pindrop
Type	Server
Proxy Set	Pindrop
Media Realm	Pindrop

4.8 Configure IP-to-IP Call Routing Rules

This section describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected.

For the homologation test topology, the following IP-to-IP routing rules need to be configured to route calls between the Vonage SIP Trunk, AudioCodes Contact Center and Pindrop Fraud Detection and Authentication Solution.

To configure IP-to-IP routing rules:

1. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. Configure rules as follows:

Index	Name	Source IP Group	Request Type	Destinati on Type	Destination IP Group	Destination Address
0	Handle Options (arbitrary name)	Any	OPTIONS	Dest Address		internal
1	Vonage to Genesys (arbitrary name)	Vonage	All	IP Group	GenesysCloud	
2	Genesys to Vonage (arbitrary name)	GenesysCloud	All	IP Group	Vonage	

The routing configuration may change according to your specific deployment topology.

4.9 Configure Registration Accounts (Optional)

This section describes how to configure SIP registration accounts. This is required so that the SBC can register with the Vonage SIP Trunk on behalf of GenesysCloud. Vonage SIP Trunk requires registration and authentication to provide service.

In the homologation test topology, the Served IP Group is GenesysCloud IP Group and the Serving IP Group is Vonage SIP Trunk IP Group.

To configure a registration account:

1. Open the Accounts table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Accounts**).
2. Click **New**.
3. Configure the account according to the provided information from Vonage, for GenesysCloud, serving by Vonage SIP Trunk:

Parameter	Value
Served IP Group	GenesysCloud
Application Type	SBC
Serving IP Group	Vonage
Register	Regular
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

4. Click **Apply**.

4.10 Configure Call Setup Rules

This section describes how to configure Call Setup Rules. Call Setup rules define various sequences that are run upon receipt of an incoming call (dialog) at call setup before the device routes the call to its destination.

Configured Call Setup Rule need be assigned to Vonage IP Group.

To configure a Call Setup Rules:

1. Open the Call Setup Rules table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Call Setup Rules**).
2. Click **New** and configure Call Setup rules according to the parameters described in the table below.

Table 4-7: Call Setup Rules Table

Index	Rules Set ID	Name	Condition	Action Subject	Action Type	Action Value
0	0	PSTN Call-ID	Header.Call-ID regex (.*)(@)(.*)	Var.Session.PSTN_Call-ID	Modify	$1
1	0	PSTN isup-oli	Header.From.URL.Param.isup-oli exists	Var.Session.PSTN_isup-oli	Modify	Header.From.URL.Param.isup-oli
2	0	PSTN To User	Header.Request-Uri.MethodType == '5'	Var.Session.PSTN_To_User	Modify	Header.To.URL.User
3	0	PSTN From User	Header.Request-Uri.MethodType == '5'	Var.Session.PSTN_From_User	Modify	Header.From.URL.User
4	0	PSTN_PAI	Header.P-Asserted-Identity exists	Var.Session.PSTN_PAI	Modify	Header.P-Asserted-Identity

3. Click **Apply** and then save your settings to flash memory.

Rule Index	Description
0	For messages received from Vonage SIP Trunk, the value of the Call-ID header is assigned to the 'Call-ID' session variable, which will be added to the outgoing messages towards the GenesysCloud (in x-user-to-user header) and Pindrop (in x-customer-ixn header).
1	For messages received from Vonage SIP Trunk, if the 'isup-oli' parameter exists in the SIP From header, the value of this parameter is stored in the session variable for further usage.
2	For all Invite messages received from Vonage SIP Trunk, the value of the user part of the SIP To header is stored in the session variable for further usage.
3	For all Invite messages received from Vonage SIP Trunk, the value of the user part of the SIP From header is stored in the session variable for further usage.
4	For messages received from Vonage SIP Trunk, the value of the SIP P-Asserted-Identity header is stored in the session variable for further usage.

4.11 Configuring SIP Recording

This section describes the SBC's SIP Recording configuration for recording all calls from Genesys Contact Center by the Pindrop Fraud Detection and Authentication Solution.

To configure SIP Recording settings:

1. Open the SIP Recording Settings page (**Setup** menu > **Signaling & Media** tab > **SIP Recording** folder > **SIP Recording Settings**).
2. From the 'SIP Recording Time Stamp Format' drop-down list, select **UTC**.
3. From the 'SIP Recording Metadata Format' drop-down list, select **RFC 7865**.

4.11.1 Configuring SIP Recording Rules

This section describes how to configure SIP Recording rules through the Web interface. The SIP Recording Rules table lets you configure up to 30 SIP-based media recording rules. A SIP Recording rule defines call routes that you want to record.

To configure a SIP Recording Routing rule:

1. Open the SIP Recording Rules table (**Setup** menu > **Signaling & Media** tab > **SIP Recording** folder > **SIP Recording Rules**).
2. Click **New** and configure a SIP recording rule according to the table below:

Index	Recorded IP Group	Peer IP Group	Caller	Recording Server (SRS) IP Group
0	GenesysCloud	Any	Both	Pindrop

4.12 Configure Message Manipulation Rules

This section describes how to configure SIP message manipulation rules. SIP message manipulation rules can include insertion, removal, and/or modification of SIP headers. Manipulation rules are grouped into Manipulation Sets, enabling you to apply multiple rules to the same SIP message (IP entity).

Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

To configure SIP message manipulation rule:

1. Open the Message Manipulations page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).
2. Click **New** and configure Call Setup rules according to the parameters described in the table below.

Table 4-8: Message Manipulations Rules Table

Index	Manipulation Name	Man Set ID	Message Type	Condition	Action Subject	Action Type	Action Value
0	Pindrop_X-Account-ID	0	Invite.Request		Header.X-Account-ID	Add	See footnote [1]
1	Pindrop_X-Pindrop_ID	0	Invite.Request	Var.Session.PSTN_Call-ID exists	Header.X-Customer-IXN	Add	Var.Session.PSTN_Call-ID
2	Pindrop_isup-oli	0	Invite.Request	Var.Session.PSTN_isup-oli exists	Header.From.URL.Param.isup-oli	Add	Var.Session.PSTN_isup-oli
3	Pindrop_To_User	0	Invite.Request	Var.Session.PSTN_To_User exists	Header.To.URL.User	Modify	Var.Session.PSTN_To_User
4	Pindrop_From_User	0	Invite.Request	Var.Session.PSTN_From_User exists	Header.From.URL.User	Modify	Var.Session.PSTN_From_User
5	Prindrop_PAI	0	Invite.Request	Var.Session.PSTN_PAI exists	Header.P-Asserted-Identity	Add	Var.Session.PSTN_PAI
6	Genesys_X-User-To-User	1	Invite.Request	Var.Session.PSTN_Call-ID exists	Header.X-User-To-User	Add	Var.Session.PSTN_Call-ID

3. Click **Apply** and save your settings to flash memory.
4. Assign Manipulation Set ID 1 to the GenesysCloud IP Group:
   a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
   b. Select the row of the Pindrop IP Group, and then click **Edit**.
   c. Set the 'Outbound Message Manipulation Set' field to **0**.
   d. Click **Apply**.
5. Assign Manipulation Set ID 0 to the Pindrop IP Group:
   a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
   b. Select the row of the GenesysCloud IP Group, and then click **Edit**.
   c. Set the 'Outbound Message Manipulation Set' field to **1**.
   d. Click **Apply**.

[1] Please contact Pindrop Account Team to receive appropriated Account ID used for routing, which is added as "X-Account-ID" header.

4.13 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

4.13.1 Optimizing CPU Cores Usage for a Specific Service (relevant for Mediant 9000 and Software SBC only)

This section describes how to optimize the SBC's CPU cores usage for a specified profile to achieve maximum capacity for that profile. The supported profiles include:

- SIP profile – improves SIP signaling performance, for example, SIP calls per second (CPS)
- SRTP profile – improves maximum number of SRTP sessions
- Transcoding profile – enables all DSP-required features, for example, transcoding and voice in-band detectors

To optimize core allocation for a profile:

1. Open the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC General Settings**).
2. From the 'SBC Performance Profile' drop-down list, select the required profile:

3. Click **Apply**, and then reset the device with a burn-to-flash for your settings to take effect.

International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide
Website: https://www.audiocodes.com

Document #: LTRT-39468