AudioCodes Professional Services – Interoperability Lab

# Pindrop Fraud Detection and Authentication Solution with GenesysCloud Contact Center using AudioCodes Mediant<sup>™</sup> SBC

Version 7.4



**GENESYS**<sup>®</sup>



# **Table of Contents**

Not	ice			iii					
	WEEE	EU Dire	ective	iii					
	Custo	mer Suj	oport	iii					
	Stay	in the L	_oop with AudioCodes	iii					
	Abbreviations and Terminologyii								
	Gene	ral Note	s, Warnings, and Safety Information	iii					
	Docui	evision Record	iv						
	Docu	mentati	on Feedback	iv					
1	Intro	ductio	۱	1					
	1.1	Intend	ed Audience	1					
	1.2	About	AudioCodes SBC Product Series	1					
		1.2.1	Known Limitations	1					
2	Confi	iguring	Pindrop Fraud Detection and Authentication Solution	2					
3	Confi	guring	a Trunk on GenesysCloud	3					
4	Confi	Configuring AudioCodes SBC10							
	4.1	IP Netv	work Interface Configuration	10					
		4.1.1	Configure Network Interface	10					
		4.1.2	Configure NAT Translation	11					
	4.2	Config	ure Media Realms	12					
	4.3	Config	ure SIP Signaling Interfaces	12					
	4.4	Config	ure Proxy Sets and Proxy Address	13					
		4.4.1	Configure a Proxy Address	13					
	4.5	Config	ure Coders	15					
	4.6	Config	ure IP Profiles	16					
	4.7	Config	ure IP Groups	17					
	4.8	Config	ure IP-to-IP Call Routing Rules	18					
	4.9	Config	ure Registration Accounts (Optional)	19					
	4.10	Config	ure Call Setup Rules	20					
	4.11	Config	uring SIP Recording	21					
		4.11.1	Configuring SIP Recording Rules	21					
	4.12	Config	ure Message Manipulation Rules	22					
	4.13	Miscel	laneous Configuration	23					
		4.13.1 Softwar	Optimizing CPU Cores Usage for a Specific Service (relevant for Mediant 9000 and re SBC only)	23					

### 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 <a href="https://www.audiocodes.com/library/technical-documents">https://www.audiocodes.com/library/technical-documents</a>.

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 <a href="https://www.audiocodes.com/services-support/maintenance-and-support">https://www.audiocodes.com/services-support/maintenance-and-support</a>.

### 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 <a href="https://online.audiocodes.com/documentation-feedback">https://online.audiocodes.com/documentation-feedback</a>.

# **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

inforo@à	External Trunk Name			
Metrica	AudioCodes Mediant VE		Status	Operational
			Type	Generic BYOC Carrier
Trunks			Inbound Callis	w. 0
Sites			Outbound Calls	1 0
Edge Groups			QoS Mismatches	₩ 0
Edges				
Phone Management	Trunk State 💿		Protocol O	
Certificate Authorities			UDP	
DID Numbers	Inbound / Termination			
Extensiona	Inbound SIP Termination Identifier 😧	c	Inbound SIP Terminatio	n Header 🧿
	AudioCodesSC9			
	DNIE Peolecement Pouring			
	Enabled			
		Inbound Reque	st-URI Reference	
	FQDN Method TGRP Method O	Inbound Reque INVITE sip:+xxxxxxxx INVITE sip:+xxxxxxxxx context=byxc.mypur	st-URI Reference coxx@AudioCodesSC9.byo cocx;tgrp=AudioCodesSC9; ecloud.com@lb01.byoc.us	c.mypurecloud.com trunk- east-1.mypurecloud.com
	FQDN Method TGRP Method 😧 DNIS Replacement Method 😧	Inbound Reque INVITE sip:+xxxxxxxx INVITE sip:+xxxxxxxx context=bycc.mypur INVITE sip:AudioCod	st-URI Reference coxx@AudioCodesSC9.byo coxx,tgrp=AudioCodesSC9; ecloud.com@lb01.byoc.us esSC9@lb01.byoc.us-east	c.mypurecloud.com trunk- east-1.mypurecloud.com -1.mypurecloud.com
	FQDN Method TGRP Method © DNIS Replacement Method ©	Inbound Reque INVITE sip+sococoo INVITE sip+sococoo context=byoc.mypur INVITE sip-AudioCod	st-URI Reference coox@AudioCodesSC9.byo coox;tgrp=AudioCodesSC9; ecloud.com@lb01.byoc.us esSC9@lb01.byoc.us-east	c.mypurecloud.com trunk- east-1.mypurecloud.com -1.mypurecloud.com
	FQDN Method TGRP Method O DNIS Replacement Method O Outbound Outbound SIP Termination FQDN O	Inbound Reque INVITE sip:+xxxxxxxxx INVITE sip:+xxxxxxxx INVITE sip:AudioCod	st-URI Reference cxx:@AudioCodesSC9.byo cxx:grp=AudioCodesSC9; ecloud.com@lb01.byoc.us esSC9@lb01.byoc.us-east	c.mypurecloud.com trunk- east-1.mypurecloud.com -1.mypurecloud.com
	FQDN Method TGRP Method • DNIS Replacement Method • Outbound Outbound SIP Termination FQDN • ec2-3-23-176-79.us-east-2.compute.amazonaws	Inbound Reque INVITE sip:+sococoo context=byoc.mypur INVITE sip:AudioCod	st-URI Reference coox@AudioCodesSC9.byo coox;tgrp=AudioCodesSC9; ecloud.com@lb01.byoc.us esSC9@lb01.byoc.us-east	c.mypurecloud.com trunk- east-1.mypurecloud.com -1.mypurecloud.com
	FQDN Method TGRP Method © DNIS Replacement Method © Outbound Outbound SIP Termination FQDN © ec2-3-23-176-79.us-east-2.compute.amazonaws. Outbound SIP TGRP Attribute ©	Inbound Reque INVITE sip+sococo ontext=byoc.mypur INVITE sip-sudioCod	st-URI Reference cocx@AudioCodesSC9.byo cocxtgrp=AudioCodesSC9; ecloud.com@lb01.byoc.us esSC9@lb01.byoc.us-east TGRP Context-ID ©	c.mypurecloud.com trunk- east-1.mypurecloud.com -1.mypurecloud.com
	FQDN Method TGRP Method © DNIS Replacement Method © Outbound Outbound SIP Termination FQDN © ec2-3-23-176-79.us-east-2.compute.amazonawa Outbound SIP TGRP Attribute ©	Inbound Reque INVITE sip:+xxxxxxxx INVITE sip:+xxxxxxxx INVITE sip:AudioCod	st-URI Reference cocx@AudioCodesSC9.byo cocxtgrp=AudioCodesSC9; ecloud.com@lb01.byoc.us esSC9@lb01.byoc.us esSC9@lb01.byoc.us TGRP Context-ID	c.mypurecloud.com trunk- -aast-1.mypurecloud.com -1.mypurecloud.com
	FQDN Method TGRP Method © DNIS Replacement Method © Outbound Outbound SIP Termination FQDN © ec2-3-23-176-79.us-east-2.compute.amazonaws Outbound SIP TGRP Attribute © Outbound SIP DNIS ©	Inbound Reque	st-URI Reference cocx@AudioCodesSC9.byo cocx;tgrp=AudioCodesSC9; ecloud.com@ib01.byoc.us esSC9@ib01.byoc.us-east TGRP Contaxt-ID •	c.mypurecloud.com trunk- east-1.mypurecloud.com -1.mypurecloud.com

Topology	SIP Servers or Proxies O		Randomize Proxy Selection 😧	
Metrica	3.23.176.79:5060	8	Enabled	
Trunks		1.00		
Sites	Hostname of IP Address Port	+		
Edge Groups	Digest Authentication 😧		Realm 😜	
Edges	Disabled			
Phone Management	User Name 😧		Password 😧	
Constitution & advantation				
Centrate Autorities			Show Password	
DID Numbers	Calling			
Extensiona	Address O	5	Address Override Method 😧	
	+14792344420		Unassigned DID	
	Name O	5	Name Override Method O	
	Genesysocy		unasagneu uru	
	SIP Access Control 😧			
	Allow the Following Addresses O			
	3.23.176.79	8		
	Add an IP or CIDR address	+		
	External Trunk Configuration		Expand All	Collapse All
	• General			1.254 New York
	Call Draining 📀		Language 😡	
	Enabled		English - United States (en-US)	
	Calls			
	Max Calls 😡		Max Cali Rate 😡	
	350		40/5s	
	Max Dial Timeout 😡			
	120	sec		

#### Figure 3-2: Configured SIP Access Control

Topology	Asserted Identity	
Metrica	Disabled	
Trunka	URI O	Name 🖸
Stes		
Edge Groups		
Edges	Transport	
Phone Management	Retryable Reason Codes 🕗	Retryable Cause Codes 😧
Certificate Authorities	500-599	1-5,25,27,28,31,34,38,41,42,44,46,62,63,79,91,96,97,99,100,103
DID Numbers	- identity	
Extensiona	Inbound	
	identity Type 🧿	
	From	<b>a</b>
	LARSON .	
	Outbound	
	Apply Header Privacy 😜	Apply User Privacy 💿
	Enabled	Enabled
	Calling	
	Address Transformation 😡	
	Match Regular Expression	Format Regular Expression
		No Transformations
	These Results Consults	County Description
	March wathings Exploration	1 - curner regular expression
	Address Digits Length 😧	Address Omit + Prefix 😡

Figure 3-3: Configured Inbound/Outbound Rules

Trunks  Eldge Groups  Edges  Phone Management  Certificate Authonties  DID Numbers  Extensions	No T Match Regular Expression Address Digits Length ©	Format Regular Expression	]+
Sites Edge Groups Edges Phone Management Certificate Authorities DID Numbers Extensions	Mo T Match Regular Expression Address Digits Length ©	Formations	+
Edge Groups Edges Phone Management Certificate Authonities DID Numbers Extensions	Match Regular Expression Address Digits Length  0	Format Regular Expression Address Omit + Prefix  Enabled	]+
Edges Phone Management Certificate Authorities DID Numbers Extensions	Match Regular Expression Address Digits Length  0 0	Format Regular Expression Address Omit + Prefix  Enabled	]+
Phone Management Certificate Authorities DID Numbers Extensions	Match Regular Expression Address Digits Length  0	Format Regular Expression Address Omit + Prefix  Enabled	]+
Certificate Authonities DID Numbers Extensions	Address Digits Length	Address Omit + Prefix 0	
DID Numbers Extensions	Address Digits Length O	Address Omit + Prefix 0	
Extensiona	0	Enabled (	
Condition of the second			
	- Media		
	DSCP Value 0	Media Method 😡	
	2E (46, 101110) EF -	Normal	
	Preferred Codec List 😡	SRTP Cipher Suite List 😡	
	+ 🗣 audio/opus	+ + AES_CM_128_HMAC_SHA1_80	1
	★ ↓ audio/PCMU		
	◆ audio/PCMA		
	Select a Codec -	Select a Cipher Suite	
	Ringback O Enabled	Disconnect on Idle RTP Q	
	DTMF Settings		
	DTMF Payload O	DTMF Method O	
	101	RTP Events	
	Recording		
	Line Recording 💿	Consult Line Recording 😧	
	Disabled	Dimuliled	

Figure 3-4: Configured Media Behavior

relephony / runks				
Topology	Recording			
Metrica			Consult Line Recording O	
	Disabled		Disabled	
Trunks	Automatic Level Control 😧		Continue on External Bridged Transfer 😧	
Sites	Disabled		Dimmined	
Edge Groups	Audio Format O		Dual Channel 📀	
per escara	audio/opus		Disabled	
Edges	A CONTRACTORY			
Phone Management	Compliance			
Certificate Authorities	Consent Required O			
	Disabled			
DID Hambers	Beep Tone			
Extensiona	No Tone			
	100 1010			
	* Protocol			
	Header / Invite			
	From Header Hostname 📀		Routing Address 📀	
	Automatically generate from Edge Network Interface     Qustom		Request-URI	
	an brancha			
	Diversion Method 😜		Asserted Identity Header O	
	None		P-Asserted-identity	
	Max Diversion Entries 😯		Request URI Override 😧	
	4			
	there is there information (1910)			
	Ull Pasethrough Q. D			
	Enabled			
	Header O			
	Туре 🕖	0	Encoding Format 0	
	X-User-to-User	<b>T</b> :	Hex	
	Destanal Discriminator O			
	Linnen Maciminan A			

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

90 OG	Activity Directory - Do	cuments Clients Performance <del>-</del> Repo emal Trunks <u>Edit External Trunk</u>	rts Apps <del>-</del> Admi	in 🧲	
S ≤ C B ≤ B ≤ B	Telephony / Trunks / Ext Topology Metrics Trunks Extensions Edges Phone Management Certificate Authorities DID Numbers Extensions	rmal Trunks - Edit External Trunk	د - -	Encoding Format  Hex	
Ø		Enable Take Back and Transfer  Disabled  Release Link Transfer Enable Release Link Transfer Disabled  Outbound Custom SIP headers  Header  Header	No.custo	lue m headors Value -	+

Figure 3-6: Configured User Data

	Enable Release Link Transfer 🥹	
Topology	Disabled	
Metrica	Outbound	
Trunks	Custom SIP headers 😧	
Stes	Header Value	
Edge Groups		
Edges	No custom hea	ders
Phone Management	-	
Certificate Authorities		
DID Numbers	Header Value	+
Extensiona		
	1	
	Diagnostics     Enabling diagnostic captures will log all data entered via Secure IVR flows. This m     in any way. If sensitive data is entered via a Secure IVR it is recommended that dia     may degrade performance and quality of service.  Media Capture	ay include sensitive data that should not be captured or expo- agnostic captures are not enabled. Enabling any of these settin
	<ul> <li>Diagnostics</li> <li>Enabling diagnostic captures will log all data entered via Secure IVR flows. This m in any way. If sensitive data is entered via a Secure IVR it is recommended that dia may degrade performance and quality of service.</li> <li>Media Capture O</li> <li>Disabled</li> <li>Capture Until</li> </ul>	ay include sensitive data that should not be captured or expos agnostic captures are not enabled. Enabling any of these settir
	<ul> <li>Diagnostics</li> <li>Enabling diagnostic captures will log all data entered via Secure IVR flows. This m in any way. If sensitive data is entered via a Secure IVR it is recommended that dia may degrade performance and quality of service.</li> <li>Media Capture ()</li> <li>Disabled</li> <li>Capture Until</li> <li>3/10/2021</li> <li>11 : 24 : 31 AM</li> </ul>	ay include sensitive data that should not be captured or expos agnostic captures are not enabled. Enabling any of these settin
	<ul> <li>Diagnostics</li> <li>Enabling diagnostic captures will log all data entered via Secure IVR flows. This m in any way. If sensitive data is entered via a Secure IVR it is recommended that dia may degrade performance and quality of service.</li> <li>Media Capture </li> <li>Disabled</li> <li>Capture Until</li> <li>3/10/2021</li> <li>11 : 24 : 31 AM</li> <li>Custom</li> </ul>	ay include sensitive data that should not be captured or expos
	<ul> <li>Diagnostics</li> <li>Enabling diagnostic captures will log all data entered via Secure IVR flows. This m in any way. If sensitive data is entered via a Secure IVR it is recommended that dia may degrade performance and quality of service.</li> <li>Media Capture Disabled</li> <li>Capture Until</li> <li>3/10/2021</li> <li>11 : 24 : 31 AM</li> <li>Custom</li> </ul>	ay include sensitive data that should not be captured or expos
	Diagnostics     Enabling diagnostic captures will log all data entered via Secure IVR flows. This m in any way. If sensitive data is entered via a Secure IVR it is recommended that dia may degrade performance and quality of service.      Media Capture      Disabled     Capture Until	ay include sensitive data that should not be captured or expos agnostic captures are not enabled. Enabling any of these settin
	Diagnostics     Enabling diagnostic captures will log all data entered via Secure IVR flows. This m in any way. If sensitive data is entered via a Secure IVR it is recommended that dia may degrade performance and quality of service.      Media Capture      Disabled     Capture Until	ay include sensitive data that should not be captured or expos agnostic captures are not enabled. Enabling any of these settin Value
	Diagnostics     Enabling diagnostic captures will log all data entered via Secure IVR flows. This m in any way. If sensitive data is entered via a Secure IVR it is recommended that dia may degrade performance and quality of service.      Media Capture      Disabled     Capture Until	ay include sensitive data that should not be captured or expos agnostic captures are not enabled. Enabling any of these settin Value
	<ul> <li>Diagnostics</li> <li>Enabling diagnostic captures will log all data entered via Secure IVR flows. This m in any way. If sensitive data is entered via a Secure IVR it is recommended that dia may degrade performance and quality of service.</li> <li>Media Capture          <ul> <li>Disabled</li> <li>Capture Until</li> <li>3/10/2021</li> <li>11: 24: 31 AM</li> </ul> </li> <li>Custom         <ul> <li>Oreste</li> <li>Property Name</li> <li>Data Type</li> <li>No data available</li> </ul> </li> </ul>	ay include sensitive data that should not be captured or expos agnostic captures are not enabled. Enabling any of these settin Value
	Diagnostics     Enabling diagnostic captures will log all data entered via Secure IVR flows. This m in any way. If sensitive data is entered via a Secure IVR it is recommended that dia may degrade performance and quality of service.      Media Capture      Disabled     Capture Until	ay include sensitive data that should not be captured or expos agnostic captures are not enabled. Enabling any of these settin Value

#### 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 <u>Mediant Virtual Edition SBC for Amazon AWS Installation Manual</u> or the <u>Mediant Cloud Edition SBC</u> <u>Installation Manual</u> 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:

- 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	<b>eth0</b> (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:** 

- 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):

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)

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

# 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:

- 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.

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

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

# 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:** 

- 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:

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

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

### 4.4.1 Configure a Proxy Address

This section shows how to configure a Proxy Address.

(arbitrary name)

#### To configure a Proxy Address for ProxySet\_GenesysCloud:

 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.

Options

2. Click +New; and configure the address of the Proxy Set according to the parameters described in the table below:

Table 4-4: Configuration Ex	ample of Proxy Address f	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:

- 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:

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

#### Table 4-5: Configuration Example of Proxy Address for ProxySet\_Vonage

#### 3. Click Apply.

#### To configure a Proxy Address for Pindrop:

- 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 Apply.

# 4.5 Configure Coders

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

To configure coders:

- 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	<ul> <li>G.711 U-law</li> <li>G.711 A-law</li> <li>G.729</li> </ul>

### 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:

- 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:

- 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:**

- 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
Туре	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
Туре	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
Туре	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:

 Open the IP-to-IP Routing table (Setup menu > Signaling & Media tab > SBC folder > Routing > IP-to-IP Routing).

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	

2. Configure rules as follows:



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:

- 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:

- 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.

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

#### Table 4-7: Call Setup Rules Table

3.	Click Apply and then save your settings to flash	memory.
3.	Click <b>Apply</b> and then save your settings to hash	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:

- 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:

- 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:

- 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.

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 <sup>1</sup>
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

Table 4-8: Message Manipulations Rules Table

- 3. Click **Apply** and save your settings to flash memory.
- 4. Assign Manipulation Set ID 1 to the GenesysCloud IP Group:
  - 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:
  - 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.

<sup>&</sup>lt;sup>1</sup> 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:

- 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:

SBC Performance Profile

Optimized for transcoding

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: <u>https://www.audiocodes.com/corporate/offices-worldwide</u> Website: <u>https://www.audiocodes.com</u>

©2023 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, and AudioCodes Room Experience are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-39468

