AudioCodes Professional Services – Interoperability Lab

Genesys Cloud Contact Center and Generic SIP Trunk using AudioCodes Mediant[™] SBC

Version 7.4





Table of Contents

1	Intro	oduction	7
	1.1	Intended Audience	7
	1.2	About Genesys Cloud Contact Center	7
	1.3	About AudioCodes SBC Product Series	7
2	Com	ponent Information	9
	2.1	AudioCodes SBC Version	9
	2.2	Generic SIP Trunking Version	9
	2.3	Genesys Cloud Contact Center Version	9
	2.4	Interoperability Test Topology	.10
		2.4.1 Environment Setup	.11
		2.4.2 Known Limitations	.11
3	Con	figuring Genesys Cloud	13
	3.1	Prerequisites	.13
	3.2	Adding a New BYOC Cloud Trunk	.14
	3.3	Adding a New Outbound Route on Site	.21
4	Con	figuring AudioCodes SBC	23
	4.1	IP Network Interfaces Configuration	.24
		4.1.1 Configure VLANs	.24
	4.0	4.1.2 Configure Network Interfaces	.25
	4.2	SIP ILS Connection Configuration (Optional)	.26
		4.2.1 Configure the NTP Server Address	.20
		4.2.3 Configure a Certificate	.28
	4.3	Configure Media Realms	.28
	4.4	Configure SIP Signaling Interfaces	.29
	4.5	Configure Proxy Sets and Proxy Address	.30
		4.5.1 Configure a Proxy Address	.31
	4.6	Configure Coders	.33
	4.7	Configure IP Profiles	.36
	4.8	Configure IP Groups	.38
	4.9	Configure SRTP	.39
	4.10	Configure IP-to-IP Call Routing Rules	.40
	4.11	Contigure Number Manipulation Rules (Optional)	.41
	4.12	Miscellaneous Configuration.	.42
		4.12.1 Optimizing CPU Cores Usage for a Specific Service (Relevant for Mediant 9000 and Software SBC only)	.42



This page is intentionally left blank.

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: November-15-2021

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.

Document Revision Record

LTRT	Description
39478	Initial document release.

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 Web site at https://online.audiocodes.com/documentation-feedback.



This page is intentionally left blank.

1 Introduction

This Configuration Note describes how to set up the AudioCodes Enterprise Session Border Controller (hereafter, referred to as *SBC*) for interworking between Generic SIP Trunk and the Genesys Cloud Contact Center environment.

You can also use AudioCodes' SBC Wizard tool to automatically configure the SBC based on this interoperability setup. However, it is recommended to read through this document to better understand the various configuration options. For more information on AudioCodes' SBC Wizard including the download option, visit AudioCodes Web site at https://www.audiocodes.com/partners/sbc-interoperability-list.

1.1 Intended Audience

This document is intended for engineers, or AudioCodes and Generic partners who are responsible for installing and configuring Generic SIP Trunk and Genesys Cloud Contact Center for enabling VoIP calls using AudioCodes SBC.

1.2 About Genesys Cloud Contact Center

Genesys Cloud Contact Center Solutions allow companies to manage customer requirements effectively by routing customers to appropriate resources and agents through IVR and consolidated cross-channel management of a customer's interactions. Sophisticated profiling, outbound voice and performance management enables companies to provide very personalized customer care and delivery.

1.3 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. The SBC can be offered as a Virtualized SBC, supporting the following platforms: Hyper-V, AWS, AZURE, AWP, KVM and VMWare.



This page is intentionally left blank.

2 Component Information

2.1 AudioCodes SBC Version

Table 2-1: AudioCodes SBC Version

SBC Vendor	AudioCodes		
Models	 Mediant 500/L Gateway & E-SBC Mediant 800B/C Gateway & E-SBC Mediant 1000B Gateway & E-SBC Mediant 2600 E-SBC Mediant 4000/B SBC Mediant 9000/9030/9080 SBC Mediant Software SBC (VE/SE/CE) 		
Software Version	7.40A.100.238 or later		
Protocol	SBC can be configured to work SIP/UDP, SIP/TCP or SIP/TLS towards Generic SIP Trunk and / or Genesys Cloud Contact Center, depending on customer requirements.		
Additional Notes	None		

2.2 Generic SIP Trunking Version

Table 2-2: Generic Version

Vendor/Service Provider	Generic
SSW Model/Service	
Software Version	
Protocol	SIP
Additional Notes	None

2.3 Genesys Cloud Contact Center Version

Table 2-3: Genesys Cloud Contact Center Version

Vendor	Genesys
Model	Contact Center
Software Version	November 3, 2021
Protocol	SIP
Additional Notes	None

2.4 Interoperability Test Topology

The Genesys Cloud Contact Center is connected to the Generic SIP Trunk via an SBC.



Note: Contact your Genesys Contact Center support channel for more information about topological scenarios.

The interoperability testing between AudioCodes SBC and Generic SIP Trunk with Genesys Cloud Contact Center was done using the following topology setup:

- The Enterprise was deployed with a Genesys Cloud Contact Center as a service using robust Contact Center functionality and interactive voice response (IVR) to efficiently connect customers with the right agents and information at the right time.
- The Enterprise SBC connected the Genesys Cloud Contact Center with the Public PSTN via the Generic SIP Trunk, as an External Trunk over the public network.
- AudioCodes SBC is implemented to interconnect between the SIP Trunk and Genesys Cloud Contact Center
 - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
 - **Border:** IP-to-IP network border both Generic SIP Trunk and the Genesys Cloud Contact Center are located in the public network.

The figure below illustrates this interoperability test topology:

Figure 2-1: Interoperability Test Topology between SBC and Genesys Cloud Contact Center with Generic SIP Trunk



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	Both, Generic SIP Trunk and Genesys Cloud Contact Center are located on the Enterprise's (or Service Provider's) WAN
Signaling Transcoding	 Genesys Cloud Contact Center operates with SIP-over-UDP, TCP or SIP-over-TLS transport type Generic SIP Trunk transport type depends on customer requirements The interoperability test environment used SIP-over-UDP
Codecs Transcoding	 Genesys Cloud Contact Center supports OPUS, G.711U-law and G.711A-law coders Generic SIP Trunk supports G.711U-law, G.711A-law, and G.729 coders
Media Transcoding	Connection to both, Generic SIP Trunk and Genesys Cloud Contact Center can operate with RTP or SRTP media types, depending on the signaling transport type.



Note: The configuration data used in this document, such as IP addresses and FQDNs are used for example purposes only. This data should be configured according to the site specifications.

2.4.2 Known Limitations

There were no limitations observed in the interoperability tests done for the AudioCodes SBC interworking between Genesys Cloud Contact Center and Generic SIP Trunk.



This page is intentionally left blank.

3 Configuring Genesys Cloud

This section describes how to configure new SIP Trunk (BYOC Cloud) on Genesys Cloud Contact Center to operate with Generic SIP Trunk through AudioCodes SBC.

3.1 **Prerequisites**

Before you begin configuration, make sure that the BYOC Cloud add-on is available and active in your Genesys Cloud organization:

- 1. From Genesys Desktop, in Admin, select Genesys Add-Ons in Account Settings.
- 2. If the BYOC Cloud option is available in your org, you should see a **BYOC Cloud** tile. Otherwise, please reach out to your Genesys contact to ask for it.
- 3. Make sure to **Activate** this add-on (it will then appear as **Active**).

Apps 👻 Directory -Documents Genesys Add Ons Genesys Cloud Genesys Cloud Genesys Cloud Genesys Cloud Genesys Cloud BYOC Cloud Genesys Cloud Genesys Cloud Static Genesys Predictive Genesys Cloud Voice WebRTC TURN Wallboards Engagement Genesys Cloud Voice is a The BYOC Cloud solution voice over IP telephony provides flexibility and Gives telephony admins the Predictive Engagement is a Leveraging the Genesys service that you can activate nteroperability to the Cloud Performance > ability to force the use of real-time journey analytics for use with your Genesys platform that observes and Genesys Cloud suite of Dashboard functionality, this TURN for every call for a Cloud organization. voice services by allowing Genesys Add On allows you given WebRTC station This analyzes visitors on to project the Dashboard. lets them bounce media. Genesys Cloud customer Active Detai Details Details Activate Details Active Active Active Details Genesys Cloud Genesys Cloud Genesys Dialog Engine Genesys Predictive Routing Bot Flows Genesys Dialog Engine Bot Genesys Predictive Routing Flows is an intuitive bot uses customer, agent and authoring platform. interaction data to predict combining natural language agent best suited to improve with Genesys Architect's a business metrics for an. Activate Details Activate Details

Figure 3-1: Activate Genesys BYOC Cloud Add-Ons

A Genesys Cloud is deployed in a single AWS region. See <u>AWS regions for Genesys Cloud</u> <u>deployment</u> for a list of supported regions, or to determine in which region your Genesys Cloud organization is deployed.

If you have a mechanism to control the IP Addresses, allow it to access to your device (SIP Access Control List):

For SIP, you can find the list of the BYOC Cloud public SIP IP addresses, for each AWS/Genesys Cloud region, <u>here</u>.

If you also need to define a list for the media traffic (Genesys Cloud Media), see <u>IP addresses</u> for the firewall allowlist.

3.2 Adding a New BYOC Cloud Trunk

The procedure below describes how add external trunk as Genesys Cloud Bring Your Own Carrier (BYOC) Cloud Trunk.

- > To add a new BYOC Cloud Trunk:
- 1. From the Genesys Desktop, in Admin, select **Trunks** in **Telephony**.
- 2. Click on the **Create New** button (**External Trunks** tab).
- **3.** In the 'External Trunk Name' field, enter a name for your External Trunk (e.g., *AudioCodes Trunk*).
- 4. From the 'Type' drop-down list, select **BYOC Carrier**.
- 5. From the 'sub-type' drop-down list, select Generic BYOC Carrier.
- 6. From the 'Protocol' drop-down list, select the Transport Protocol used for SIP: UDP/TCP/TLS (e.g., TLS).
- 7. Under the **Inbound / Termination** group, in the 'Inbound SIP Termination Identifier' field, enter a value (e.g., *audiocodestrk*).

This is the unique identifier of your trunk. It is used for inbound calls to Genesys Cloud, to uniquely identify a customer (Genesys Cloud org.) and a trunk, in a specific region (e.g., *sip:+xxxxxxxx@audiocodestrk.byoc.usw2.pure.cloud*).

Activity Directory - Do	cuments Performance v Reports Apps v	Admin Q Off Gu
■ Telephony / Trunks / Exte	ernal Trunks / Create External Trunk	
Topology	External Trunk Name	
Metrics 3	AudioCodes Trunk	Status New Type Ø Generic BYOC Carrier
Trunks	Туре	
Sites	BYOC Carrier	
51.0	Generic BYOC Carrier	Ŧ
Edge Groups	Managed By 🕢	
Edges	Everyone Provider Only	
Phone Management	Trunk State 😧	C S Isotora
Certificate Authorities	In Service	5 TLS ~
DID Numbers	Inbound / Termination	
Extensions	Inbound SIP Termination Identifier 😧	D Inbound SIP Termination Header @
	audiocodestrk	
	DNIS Replacement Routing 😧	
	Disabled	
		Inbound Request-URI Reference
	FQDN Method	INVITE sip:+xxxxxxxx@audiocodestrk.byoc.usw2.pure.cloud

Figure 3-2: Adding the new BYOC Cloud Trunk

- 8. Under the SIP Servers or Proxies group, under Outbound, set the IP Address(es) or FDQN(s) and Port for SIP (to reach AudioCodes SBC).
- 9. If you have decided to leverage Digest Authentication, under **Outbound**, enable **Digest Authentication** and set the values for **Realm**, **User Name** and **Password**.
- **10.** Under **Outbound**, in **Calling**, from the 'Address Override Method' drop-down list, select **Unassigned DID**.

This is to preserve the CLI of the caller when the call is transferred from Genesys Cloud to your device (from the header).

You will also need to define a **Caller ID** value (e.g., an E.164 number +34910603165) which is used as a default value if the CLI of the caller can't be propagated to your system (e.g., a Genesys Cloud Contact Center Agent, with no assigned number, makes a call to your trunk).

Activity Directory - Docum	nents Performance v Reports Apps v Admin			٩	Off Queue
■ Telephony / Trunks / Externa	Il Trunks / Edit External Trunk				
Topology	SIP Servers or Proxies 😧				
Metrics		÷			
Trunks 💙	★ ↓ 52.137.104.101:5060	ŵ			
Sites	★ ↓ 40.68.84.177:5050	ŵ			
Edge Groups					
Edges	Hostname or IP Address Port	_+			_
Phone Management	Digest Authentication 📀		Realm 🕑		ъ
Certificate Authorities	Enabled		sip.audiocodes.com		
DID Numbers	User Name 🕢	ຽ	Password 🕑		
Extensions	username				
	Calling				
	Address Override Method 🚱	5	Caller ID 😧		э
	Unassigned DID	-	+34910603165		
	Name Override Method 😧	5	Caller Name 🥹		ວ
	Unassigned DID	Ť	AudioCodes		

Figure 3-3: Definitions of the New BYOC Cloud Trunk

11. Under the **SIP Access Control** group, define the list of IP addresses that your device uses for SIP (e.g., 52.137.104.101). This list is to control access on the Genesys Cloud side.



Figure 3-4: SIP Access Control List

	ocuments Performance - Reports Apps - Admin		
	ernal Trunks / Edit External Trunk		
Topology	SIP Access Control 🕢		
Metrics	Allow the Following Addresses 🥹		
Trunks	52.137.104.101 會		
Sites	40.68.84.177 會		
Edge Groups	5.29.55.180		
Edges			
Phone Management	Add an IP or CIDR address		
Certificate Authorities	External Trunk Configuration	Expand All	Collapse All

12. Under the **Identity** group, for **Calling** and **Called**, disable **Address Omit + Prefix**. If disabled, when a call comes to the Genesys Cloud and is transferred to your trunk (via the configured BYOC Cloud trunk), the + prefix will be preserved in From and To header. If enabled, the + prefix will be removed (if it is present in the From/To numbers).

Figure 3-5: Omit + Prefix in Calling Number

Activity Directory - Doc	uments Performance 🕶 Reports App	Admin	
■ Telephony / Trunks / Exte	rnal Trunks / Edit External Trunk		
Topology	▼ Identity		
Metrics	Inbound		
Trunks	Identity Type 😧		
Sites			
Edge Groups	Apply Header Privacy 😧	Apply User Privacy 🕢	
Edges	Enabled	Enabled	
Phone Management	Calling		
Certificate Authorities	Address Transformation 😮		
DID Numbers	Match Regular Expression	Format Regular Expression	
Extensions			
		No Transformations	
	Match Regular Expression	Format Regular Expression	+
	Address Digits Length 📀	Address Omit + Prefix 😡 🕤	
	0	1 Disabled	

Activity Directory – Do	cuments Performance v Reports	Apps 🔻 Admin	
	ernal Trunks / Edit External Trunk		
Topology	Called		
Metrics	Address Transformation 🚱 Match Regular Expression	Format Regular Expression	
Trunks			
Sites		No Transformations	
Edge Groups		No Hanstonnations	
Edges			
Phone Management	Match Regular Expression	Format Degular Expression	+
Certificate Authorities	Water Regular Expression	Poind Regular Expression	
DID Numbers	Address Digits Length 🕢	Address Omit + Prefix @ ">	
Extensions	U	Disduced	

Figure 3-6: Omit + Prefix in Called Number

13. Under the **Media** group, define your **Preferred Codec List**, based on the audio codecs your trunk supports (e.g., audio/opus, audio/PCMU, audio/PCMA). If SRTP is used, you can define the list of specific ciphers.

Activity Directory - Doc	uments Performance 🕶 Reports Apps	✓ Admin	
■ Telephony / Trunks / Exter	nal Trunks / Edit External Trunk		
Topology	External Trunk Configuration		Expand All Collapse All
Metrics	▶ General		
Trunks	Transport		
Sites	Identity		
	✓ Media		
Eage Groups	DSCP Value 😧	Media Method 🥑	
Edges	2E (46, 101110) EF	- Normal	·
Phone Management	Preferred Codec List 😧	SRTP Cipher Suite List 🕑	
Certificate Authorities	↑ ↓ audio/opus		IA1_80
DID Numbers	2 🛧 🗸 audio/PCMU	ê	
Extensions	↑ ↓ audio/PCMA	ê	
	Select a Codec	✓ Select a Cipher Suite	-
	Ringback 😧	Disconnect on Idle RTP 😧	
	Enabled	Enabled	
	DTMF Settings		
	DTMF Payload 😧	DTMF Method 🕢	
	101	RTP Events	-

Figure 3-7: Codec List

- 14. Under the **Protocol** group, enable the **Conversation Headers** toggle. By enabling this feature, Genesys Cloud automatically attaches the ConversationId, as a custom SIP header, in the outgoing SIP messages:
 - **a.** For outbound calls (Genesys Cloud to External SIP Trunk), Genesys Cloud adds a **x-inin-cnv** header containing the ConversationId on SIP INVITE.
 - b. For inbound calls (External SIP Trunk to Genesys Cloud), Genesys Cloud adds a x-inin-cnv header containing the ConversationId in the 200 OK (following the received SIP INVITE).

Activity Directory - Doc	uments Performance 🕶 Reports Apps 🕶 Admin	
Telephony / Trunks / Exter	nal Trunks / Edit External Trunk	
Topology	✓ Protocol	
Metrics	Header / Invite	
Trunks 13	Conversation Headers I S	From Header Hostname 😧
Sites		O Custom
Edge Groups	Routing Address 😧	Diversion Method 😧
Edges	Request-URI	▼ None ▼
Phone Management	Asserted Identity Header 😧	Max Diversion Entries 📀
Certificate Authorities	P-Asserted-Identity	• 4
DID Numbers	Request URI Override 🥹	
Extensions		

15. Under the **Protocol** group, enable **Take Back and Transfer**. This enables support of REFER on Genesys Cloud.

Activity Directory - Doct	uments Performance - Reports Apps - Admin
■ Telephony / Trunks / Exter	nal Trunks / Edit External Trunk
Topology Metrics	Take Back and Transfer Enable Take Back and Transfer Enabled
Trunks Sites	Release Link Transfer Enable Release Link Transfer 📀
Edge Groups Edges	Disabled Outbound
Phone Management	Custom SIP headers 😧 Header Value
DID Numbers	
Extensions	No custom headers
	Header Value
	Diagnostics
	Custom Save External Trunk Cancel

Figure 3-9: Enable REFER

16. To pass any additional data from Genesys Cloud to the external device through the SIP Trunk, enable User to User Information (UUI) Data on the BYOC Cloud trunk. Under the **Protocol** group, in **User to User Information (UUI)**, enable the **UUI Passthrough** toggle and select the **Header Type** (User-to-User) and **Encoding Format** (hex, ascii) you want to use.

Activity Directory - Doc	uments Performance - Reports App	os 👻 Admin		
	nal Trunks / Edit External Trunk			
Topology	Asserted Identity Header 😧	Max Di	Diversion Entries 🕢	
Metrics	Request URI Override 🚱	4		
Trunks				
Sites	User to User Information (UUI)			
Edges	UUI Passthrough @ D			
Phone Management	Header 😧			
Certificate Authorities	Туре 🕢	Enco	oding Format 😧	c
DID Numbers	User-to-User	- Asc	cii	-
Extensions	Protocol Discriminator 😧			

Figure 3-10: Enabling UUI Header

3.3 Adding a New Outbound Route on Site

The procedure below describes how to add an external trunk, created in the previous section, as an outbound route for a specific site. We need to make sure that this trunk will be selected.

> To add a new Outbound Route on Site:

1. From the Genesys Desktop, in Admin, navigate to **Sites** in **Telephony**, and then select the site where you want to add your BYOC Cloud trunk (or create a new one):

Figure 3-11: Site Selection

Toplogy Toplogy General Number Plans Outbound Routes Site Trunks Cotol Site Decription Edge Groups Edge Groups Edge Groups <th></th> <th>ocuments Performance -</th> <th>Reports Apps 🕶 Admin</th> <th></th> <th></th> <th>Q Off Que</th>		ocuments Performance -	Reports Apps 🕶 Admin			Q Off Que
Topology General Number Plans Outbound Routes Simulate Call Metrics Turks Cobl Site Base Description Edge Groups Caction Pone Management Cibl Cobl Gutlevsky Dibaber Media @ General Disaber Media @ Automatic Updates @ Ture Dialy Ture Oath State Dialy State State Condition Dialy State State Condition State Construction Construction C	■ Telephony / Sites / Edit	Site				
Metrics Trusks Cobl Site Bescription Edges Location Phone Management Cetificate Authorities DID Numbers Beco-Lookup TURN • Extensions Media • Catlog Neeurence Type Time Cally Time Call day Stat Time End Site Stat Time End Time Stat Time End Time Stat Time End Time	Topology	General Number Plans	Outbound Routes Simulate Call			
Tunks Cobi Site Sites Description Edge Groups	Metrics	Site Name				
Sites Description Edge Groups	Trunks	Cobi Site			Default Site	This is the default site
Edge Groups	Sites	Description			Type Media Model	Branch Site Cloud
Edges Location Phone Management Certificate Authorities DID Numbers Geo-Lookup TURN © Disabled Automatic Updates © Recurrence Type Dialy Time Daily Time Oal day © Range Start Time End Time 2 : 00 AM	Edge Groups				Phones	5
Phone Management Certificate Authorities DID Numbers Beco-Lookup TURN • Disabled Automatic Updates • Recurrence Type Daily Time Daily Start Time End Time 2 : 00 AM	Edges	Location			Edge Group	PureCloud Voice - AWS @
Certificate Authorities DID Numbers Media Geo-Lookup TURN Geo-Lookup TURN Disabled Automatic Updates Automatic Updates Recurrence Type Time Daily Time Ali day Range Start Time End Time 2 : 00 AM S : 00 AM	Phone Management	Cobi Gurievsky		-	Topology Diagram	A Show Topology
DID Numbers Media ? Extensions Geo-Lookup TURN ? Disabled Disabled Automatic Updates ? Recurrence Type Time Zone Daily Asia/Jerusalem (+02:00) Time All day ? Range Start Time End Time 2 : 00 AM 5 : 00 AM	Certificate Authorities					
Extensions	DID Numbers	Media 😮				
Disabled Automatic Updates Recurrence Type Daily Time All day Range Start Time Star	Extensions	Geo-Lookup TURN @				
Automatic Updates Recurrence Type Daily Time All day Range Start Time 2 : 00 AM S : 00 AM Time S : 00 AM Time S : 00 AM Time		Disabled				
Recurrence Type Time Zone Daily Asia/Jerusalem (+02:00) Time All day Range Start Time 2:00 AM 5:00 AM		Automatic Updates 😯				
Daily Asia/Jerusalem (+02:00) Time All day Range Start Time End Time 2 : 00 AM 5 : 00 AM		Recurrence Type			Time Zone	
Time All day Range Start Time 2 : 00 AM 5 : 00 AM		Daily		~	Asia/Jerusalem (+02:00)	Ŧ
Ani vay Range Start Time 2 : 00 AM 5 : 00 AM		Time				
Start Time End Time 2 : 00 AM 5 : 00 AM		An day Range				
2 : 00 AM 5 : 00 AM		Start Time	End Time			
		2 :00 AM	5 : 00 AM			

2. Navigate to the **Outbound Routes** tab, and then add an external trunk, created in the previous section (e.g., *AudioCodes Trunk*) for Default Outbound Route:

Activity Directory - Do	cuments Performance -	Reports Apps v Admin	Q Off Queue
Telephony / Sites / Edit S	Site		
Topology	General Number Plans	Outbound Routes Simulate Call	
Metrics	+ New Outbound Route		🗑 Delete Outbound Route
Trunks	Default Outbound Route	Outbound Route Name	Distribution Pattern
Sites		Default Outbound Route	Sequential Random
Edge Groups		Description	
Edges			
Phone Management		State	
Certificate Authorities		Enabled	
DID Numbers		Classifications	Select External Hunks +
Extensions		Network x	
	Save Outbound Routes	Cancel	

Figure 3-12: Outbound Routes

Optionally, you can add a dedicated Number Plan (under *Number Plans* tab), to match specific DID numbers.

For a more deeper description, refer to the BYOC Cloud quick start guide.

4 Configuring AudioCodes SBC

This section provides step-by-step procedures on how to configure AudioCodes SBC for interworking between Genesys Cloud Contact Center and the Generic SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 10, and includes the following main areas:

- SBC LAN interface Management Station
- SBC WAN interface Generic SIP Trunking and Genesys Cloud environment

This configuration is done using the SBC's embedded Web server (hereafter, referred to as *Web interface*).

Notes:

- For implementing Genesys Cloud and Generic SIP Trunk based on the configuration described in this section, AudioCodes SBC must be installed with a License Key that includes the following software features:
 - Number of SBC sessions (based on requirements)
 - Transcoding sessions (only if media transcoding is needed)
 - Coders (based on requirements)

For more information about the License Key, contact your AudioCodes sales representative.

- If your SBC is deployed in a virtual environment and transcoding is required, your virtual machine must have a minimum of two vCPUs. For more information, please refer to the appropriate *Installation Manual*, which can be found on AudioCodes website.
- 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 at AudioCodes web site



4.1 **IP Network Interfaces Configuration**

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

- SBC interfaces with the following IP entities:
 - Management Servers, located on the LAN
 - Genesys Cloud Contact Center and Generic SIP Trunk, located on the WAN
- SBC connects to the WAN through a DMZ network
- Physical connection: The type of physical connection depends on the method used to connect to the Enterprise's network. In the interoperability test topology, SBC connects to the LAN and DMZ using dedicated ethernet ports (i.e., two ports and two network cables are used).
- SBC also uses two logical network interfaces:
 - LAN (VLAN ID 1)
 - DMZ (VLAN ID 2)

Figure 4-1: Network Interfaces in Interoperability Test Topology



4.1.1 Configure VLANs

This section describes how to configure VLANs for each of the following interfaces:

- LAN (assigned the name "LAN_IF")
- WAN (assigned the name "WAN_IF")
- To configure the VLANs:
- Open the Ethernet Device table (Setup menu > IP Network tab > Core Entities folder > Ethernet Devices).
- 2. There will be one existing row for VLAN ID 1 and underlying interface GROUP_1.
- 3. Add another VLAN ID 2 for the WAN side.

4.1.2 Configure Network Interfaces

This section describes how to configure the IP network interfaces for each of the following interfaces:

- LAN Interface (assigned the name "LAN_IF")
- WAN Interface (assigned the name "WAN_IF")

> To configure the IP network interfaces:

- Open the IP Interfaces table (Setup menu > IP Network tab > Core Entities folder > IP Interfaces).
- 2. Configure the IP interfaces as follows (your network parameters might be different):

Index	Application Types	Interface Mode	IP Address	Prefix Length	Gateway	DNS	I/F Name	Ethernet Device
0	OAMP+ Media + Control	IPv4 Manual	10.15.77.77	16	10.15.0.1	10.15.27.1	LAN_IF	vlan 1
1	Media + Control (as this interface points to the internet, enabling OAMP is not recommended)	IPv4 Manual	195.189.192.157 (DMZ IP address of SBC)	25	195.189.192.129 (router's IP address)	According to your Internet provider's instructions	WAN_IF	vlan 2

Table 4-1: Configuration Example of the Network Interface Table

The configured IP network interfaces are shown below:

Figure 4-2: Configured Network Interfaces in IP Interfaces Table

t 🗌 🗇		IN IN Page 1	of1 ►> ► 5	Show 10 ▼ recor	ds per page			Q
NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
LAN_IF	OAMP + Media +	IPv4 Manual	10.15.17.77	16	10.15.0.1	10.15.27.1	0.0.0.0	vlan 1
WAN_IF	Media + Control	IPv4 Manual	195.189.192.157	25	195.189.192.129	80.179.52.100	80.179.55.100	vlan 2
	NAME	Image: Constraint of the second se	Image: Constraint of the second se	Image: Type INTERFACE IP ADDRESS NAME APPLICATION TYPE INTERFACE MODE IP ADDRESS LAN_IF OAMP + Media + IPv4 Manual 10.15.17.77 WAN_IF Media + Control IPv4 Manual 195.189.192.157	Image: Type APPLICATION INTERFACE IP ADDRESS PREFIX LENGTH NAME APPLICATION INTERFACE IP ADDRESS PREFIX LENGTH LAN_IF OAMP + Media + IPV4 Manual 10.15.17.77 16 WAN_IF Media + Control IPv4 Manual 195.189.192.157 25	Image APPLICATION TYPE INTERFACE MODE IP ADDRESS PREFIX LENGTH DEFAULT GATEWAY LAN_IF OAMP + Media + IPv4 Manual 10.15.17.77 16 10.15.0.1 WAN_IF Media + Control IPv4 Manual 195.189.192.157 25 195.189.192.129	Image: Type APPLICATION Type INTERFACE MODE IP ADDRESS PREFIX LENGTH DEFAULT GATEWAY PRIMARY DNS LAN_IF OAMP + Media + IPv4 Manual 10.15.17.77 16 10.15.0.1 10.15.27.1 WAN_IF Media + Control IPv4 Manual 195.189.192.157 25 195.189.192.129 80.179.52.100	Image:

4.2 SIP TLS Connection Configuration (Optional)

This section describes how to configure the SBC for using a TLS connection with the Genesys Cloud.



Note: This configuration is essential for a secure SIP TLS connection <u>only</u> and that's why if your connection to Genesys Cloud is over TCP or UDP, <u>skip this section</u>.

4.2.1 Configure the NTP Server Address

This section describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (Microsoft NTP server or another global server) to ensure that the SBC receives the current date and time. This is necessary for validating certificates of remote parties. It is important, that NTP Server will locate on the OAMP IP Interface (LAN_IF in our case) or will be accessible through it.

> To configure the NTP server address:

- 1. Open the Time & Date page (Setup menu > Administration tab > Time & Date).
- 2. In the 'Primary NTP Server Address' field, enter the IP address of the NTP server (e.g., **10.15.27.1**).

NTP SERVER	
Enable NTP	Enable 🗸
Primary NTP Server Address (IP or FQDN)	• 10.15.27.1
Secondary NTP Server Address (IP or FQDN)	
NTP Update Interval	Hours: 24 Minutes: 0
NTP Authentication Key Identifier	0
NTP Authentication Secret Key	

Figure 4-3: Configuring NTP Server Address

3. Click Apply.

4.2.2 Create a TLS Context for Genesys Cloud

This section describes how to configure TLS Context in the SBC.

- To configure the TLS version:
- Open the TLS Contexts table (Setup menu > IP Network tab > Security folder > TLS Contexts).
- 2. Create a new TLS Context by clicking **New** at the top of the interface, and then configure the parameters using the table below as reference.



Note: You can use the existing (default) TLS Context, but we recommend creating an additional one, dedicated to our setup.

Table 4-2: New TLS Context

Index	Name	TLS Version			
1	Genesys (arbitrary descriptive name)	TLSv1.2			
All other parameters can be left unchanged with their default values.					

Figure 4-4: Configuring TLS Context for Genesys Cloud

mexts [Genesys]					
GENERAL			OCSP		
Index	1		OCSP Server	Disable	~
Name	Genesys		Primary OCSP Server	0.0.0.0	
TLS Version •	TLSv1.2	~	Secondary OCSP Server	0.0.0.0	
DTLS Version	DTLSv1.0 and DTLSv1.2	~	OCSP Port	2560	
Cipher Server	DEFAULT		OCSP Default Response	Reject	~
Cipher Client	DEFAULT				
Cipher Server TLS1.3	TLS_AES_256_GCM_SHA384:TLS_CHAC	HA20			
Cipher Client TLS1.3	TLS_AES_256_GCM_SHA384:TLS_CHAC	HA20			
Key Exchange Groups	X25519:P-256:P-384:X448				
Strict Certificate Extension Validation	Disable	~			
DH key Size	2048	~			
TLS Renegotiation	Enable	~			

3. Click Apply.

4.2.3 Configure a Certificate

This section describes how to deploy Genesys Trusted Root Certificates on the SBC.

- To load trusted root certificates:
- Open the TLS Contexts page (Setup menu > IP Network tab > Security folder > TLS Contexts).
- 2. In the TLS Contexts page, select the required TLS Context index row, and then click the Trusted Root Certificates link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
- 3. Click the **Import** button, and then select all Root Certificates obtained from Genesys or from your Certification Authority to load.
- 4. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.

4.3 Configure Media Realms

This section describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for the SIP Trunk traffic and one for the Genesys traffic.

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	MR-SIPTrunk (arbitrary name)		WAN_IF	6000	100 (media sessions assigned with port range)
1	MR-Genesys (arbitrary name)	Up	WAN_IF	7000	100 (media sessions assigned with port range)

Table 4-3: Configuration Example Media Realms in Media Realm Table

The configured Media Realms are shown in the figure below:

Figure 4-5: Configured Media Realms in Media Realm Table

Media Realms (2)								
+ New Edit	â	ra 🤜 Page 1	of 1 🏎 🖬 Show 10 🗙	 records per page 		Q		
INDEX	NAME	IPV4 INTERFACE NAME	UDP PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	UDP PORT RANGE END	DEFAULT MEDIA REALM		
0	MR-SIPTrunk	WAN_IF	6000	100	6999	No		
1	MR-Genesys	WAN_IF	7000	100	7999	No		

4.4 Configure SIP Signaling Interfaces

This section describes how to configure SIP Interfaces. For the interoperability test topology, towards the SIP Trunk and towards the Genesys Cloud SIP Interfaces must be configured for the SBC.

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.



Note: The following example used TLS connectivity between the SBC and Genesys Cloud.

Table 4-4: 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	SI- SIPTrunk (arbitrary name)	WAN_IF	SBC	5060 (according to Service Provider requirement)	0	0	0 (Recommended to prevent DoS attacks)	MR-SIPTrunk
1	SI- Genesys (arbitrary name)	WAN_IF	SBC	0	0	5061 (as configured on Genesys site)	0 (Recommended to prevent DoS attacks)	MR-Genesys

The configured SIP Interfaces are shown in the figure below:

Figure 4-6: Configured SIP Interfaces in SIP Interface Table

SIP Inter	faces (2)								
+ New [Edit 🛛 🗍 面		ra <a page<="" th=""><th>1 of 1 •• •</th><th>Show 10 ∨ rec</th><th>ords per page</th><th></th><th></th><th>Q</th>	1 of 1 •• •	Show 10 ∨ rec	ords per page			Q
INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATING PROTOCOL	MEDIA REALM
0	SI-SIPTrunk	DefaultSRD (#	WAN_IF	SBC	5060	0	0	No encapsulatio	MR-SIPTrunk
1	SI-Genesys	DefaultSRD (#	WAN_IF	SBC	0	0	5061	No encapsulatio	MR-Genesys

4.5 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 interoperability test topology, two Proxy Sets need to be configured for the following IP entities:

- Generic SIP Trunk
- Genesys Cloud

The Proxy Sets will later be 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 4-5: Configuration Example Proxy Sets in Proxy Sets Table

Index	Name	SBC IPv4 SIP Interface	TLS Context Name	Proxy Keep- Alive	Proxy Hot Swap	Proxy Load Balancing Method	DNS Resolve Method
1	PS- SIPTrunk (arbitrary name)	SI-SIPTrunk	Default	Using Options	-	-	-
2	PS- Genesys (arbitrary name)	SI-Genesys	Genesys	Using Options	Enable	Round Robin	SRV

The configured Proxy Sets are shown in the figure below:

Figure 4-7: Configured Proxy Sets in Proxy Sets Table

Proxy Sets (3).						
+ New Edit		14 44	Page 1 of 1 🍉 🕨	Show 10 🗸 record	s per page		Q
INDEX	NAME	SRD	GATEWAY IPV4 SIP INTERFACE	SBC IPV4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	ProxySet_0	DefaultSRD (#0)		SI-SIPTrunk	60		Disable
1	PS-SIPTrunk	DefaultSRD (#0)		SI-SIPTrunk	60		Disable
2	PS-Genesys	DefaultSRD (#0)		SI-Genesys	60		Enable

4.5.1 Configure a Proxy Address

This section shows how to configure a Proxy Address.

- > To configure a Proxy Address for SIP Trunk:
- Open the Proxy Sets table (Setup menu > Signaling & Media tab > Core Entities folder > Proxy Sets), click the Proxy Set PS-SIPTrunk, and then click the Proxy Address link located below the table; the Proxy Address table opens.
- 2. Click **+New**; the following dialog box appears:

Figure 4-8: Configuring Proxy Address for SIP Trunk

Proxy Add	dress			-	x
	GENERAL				
	Index		0		
	Proxy Address	•	SIPTrunk.com:5060		
	Transport Type	•	UDP T		

3. Configure the address of the Proxy Set according to the parameters described in the table below:

Table 4-6: Configuration Proxy Address for SIP Trunk

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	SIPTrunk.com:5060 (SIP Trunk IP / FQDN and port)	UDP	0	0

4. Click Apply.

- > To configure a Proxy Address for Genesys Cloud:
- Open the Proxy Sets table (Setup menu > Signaling & Media tab > Core Entities folder > Proxy Sets) and then click the Proxy Set PS-Genesys, and then click the Proxy Address link located below the table; the Proxy Address table opens.
- 2. Click **+New**; the following dialog box appears:

Figure 4-9: Configuring Proxy Address for Genesys Cloud

Proxy A	Address		- x
	GENERAL		
	Index	0	
	Proxy Address	• byoc.usw2.pure.cloud	
	Transport Type	• TLS 🗸	
	Proxy Priority	0	
	Proxy Random Weight	0	

3. 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	byoc.usw2.pure.cloud (FQDN of the appropriated Genesys BYOC Cloud region)	TLS	0	0

Table 4-7: Configuration Proxy Address for Genesys Cloud

4. Click Apply.

4.6 Configure Coders

This section describes how to configure coders (termed *Coder Group*). As Genesys Cloud supports the OPUS coder while the network connection to Generic SIP Trunk may restrict operation with a dedicated coders list, you need to add a Coder Group with the supported coders for each leg, the Genesys Cloud and the Generic SIP Trunk.

Note that the Coder Group ID for this entity will be assigned to its corresponding IP Profile in the next step.

- > To configure coders:
- 1. Open the Coder Groups table (Setup menu > Signaling & Media tab > Coders & Profiles folder > Coder Groups).
- 2. Configure a Coder Group for Genesys Cloud:

Parameter	Value
Coder Group Name	AudioCodersGroups_1
Coder Name	 Opus G.711 U-law G.711 A-law

Figure 4-10: Configuring Coder Group for Genesys Cloud

(Coder Groups											
		Cod	er Group N	ame 1:7	udioCod	ersGroup	os_1 ✔ Delete G	roup				
1	Coder Name		Packetiza	tion Time	Ra	ite	Payload Type	Silence Supp	ression	_	Coder Specific	
ľ	Opus	~	20	~	N/A	~	111	N/A	\sim			
ľ	G.711U-law	~	20	~	64	~	0	Disabled	~			
	G.711A-law	~	20	~	64	~	8	Disabled	~			
		~		~		~			~			

3. Click **Apply**, and then confirm the configuration change in the prompt that pops up.

The procedure below describes how to configure an Allowed Coders Group to ensure that the voice sent to the Genesys Cloud, uses the dedicated coders list whenever possible. Note that this Allowed Coders Group ID will be assigned to the IP Profile belonging to the Genesys Cloud in the next step.

- > To set a preferred coder for the Genesys Cloud:
- Open the Allowed Audio Coders Groups table (Setup menu > Signaling & Media tab > Coders & Profiles folder > Allowed Audio Coders Groups).
- 2. Click **New**, and then configure a name for the Allowed Audio Coders Group for the Genesys Cloud.

Figure 4-11: Configuring Allowed Coders Group for the Genesys Cloud

Allowed	d Audio Coders Groups [Genesy	s Allowed Coders]	– x
	GENERAL		
	Index	0	
	Name	Genesys Allowed Coders	
		,	

- 3. Click Apply.
- 4. Select the new row that you configured, and then click the **Allowed Audio Coders** link located below the table; the Allowed Audio Coders table opens.
- 5. Click **New**, and then configure an Allowed Coders as follows:

Index	Coder
0	Opus
1	G.711 U-law
2	G.711 A-law

Figure 4-12: Configuring Allowed Coders for the Genesys Cloud

Allowed Audio Coders Groups [#0] > Allowed Audio Coders (3)							
+ New Edit 🔟	I ← ← Page 1 of 1 ► ► Show 10 records per pa	Q					
INDEX	CODER	USER-DEFINED CODER					
0	Opus						
1	G.711 U-law						
2	G.711 A-law						

Open the Media Settings page (Setup menu > Signaling & Media tab > Media folder > Media Settings).

Media Settings		
GENERAL		
NAT Traversal	Disable NAT	~
Enable Continuity Tones	Disable	~ 5
Number of Media Channels	-1	
Enforce Media Order	Disable	~
SDP Session Owner	AudiocodesGW	
Media IP Version Preference	Only IPv4	~
SBC SETTINGS		
Preferences Mode	Include Extensions	~
Enforce Media Order	Disable	~
Reserve DSP on SDP Offer	Enable	~

Figure 4-13: SBC Preferences Mode

- 7. From the 'Preferences Mode' drop-down list, select Include Extensions.
- 8. Click Apply.

4.7 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 interoperability test topology, IP Profiles need to be configured for the following IP entities:

- Generic SIP trunk to operate in non-secure mode using RTP and SIP over UDP
- Genesys Cloud to operate in secure mode using SRTP and SIP over TLS
- > To configure an IP Profile for the Generic 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	1
Name	SIPTrunk
Media Security	
SBC Media Security Mode	Not Secured
SBC Signaling	
P-Asserted-Identity Header Mode	Add (required for anonymous calls)

Figure 4-14: Configuring IP Profile for Generic SIP Trunk

ofiles [SIPTrunk]						
GENERAL				SBC SIGNALING		
Index	1			PRACK Mode	Transparent	•
Name	• SIPT	runk		P-Asserted-Identity Header Mode	• Add	•
Created by Routing Server	No			Diversion Header Mode	As Is	•
				History-Info Header Mode	As Is	•
MEDIA SECURITY				Session Expires Mode	Transparent	•
SBC Media Security Mode		Not Secured	•	SIP UPDATE Support	Supported	•
Gateway Media Security Mode		Preferable		Remote re-INVITE	Supported	•
Symmetric MKI		Disable	•	Remote Delayed Offer Support	Supported	•
MKI Size		0		MSRP re-INVITE/UPDATE	Supported	•
SBC Enforce MKI Size		Don't enforce	*	MSRP Offer Setup Role	ActPass	•
SBC Media Security Method		SDES	*	MSRP Empty Message Format	Default	•
Reset SRTP Upon Re-key		Disable	•	Remote Representation Mode	According to Operation Mode	٣
			Cancel	APPLY		

3. Click Apply.

> To configure IP Profile for the Genesys Cloud:

- 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	Genesys (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	Secured (if TLS/SRTP implemented)
SBC Media	
Extension Coders Group	AudioCodersGroups_1
Allowed Audio Coders	Genesys Allowed Coders
Allowed Coders Mode	Restriction and Preference
RFC 2833 Mode	Extend
RFC 2833 DTMF Payload Type	101

Figure 4-15: Configuring IP Profile for Genesys Cloud

GENERAL			SBC SIGNALING		
Index 2			PRACK Mode	Transparent	~
Name Ge	nesys		P-Asserted-Identity Header Mode	As Is	~
Created by Routing Server			Diversion Header Mode	As Is	~
Used By Routing Server No	t Used	~	History-Info Header Mode	As Is	~
			Session Expires Mode	Transparent	~
MEDIA SECURITY			SIP UPDATE Support	Supported	~
SBC Media Security Mode	Secured	~	Remote re-INVITE	Supported	*
Gateway Media Security Mode	Preferable	~	Remote Delayed Offer Support	Supported	*
Symmetric MKI	Disable	~	MSRP re-INVITE/UPDATE	Supported	~
MKI Size	0		MSRP Offer Setup Role	ActPass	~
SBC Enforce MKI Size	Don't enforce	*	MSRP Empty Message Format	Default	~
SBC Media Security Method	SDES	~	Remote Representation Mode	According to Operation Mode	~

3. Click Apply.



Note: The configuration may change according to specific SIP Trunk requirements.

4.8 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 interoperability test topology, IP Groups must be configured for the following IP entities:

- Generic SIP Trunk
- Genesys Cloud Contact Center
- > 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 Generic SIP Trunk:

Parameter	Value
Index	1
Name	SIPTrunk
Туре	Server
Proxy Set	PS-SIPTrunk
IP Profile	SIPTrunk
Media Realm	MR-SIPTrunk
SIP Group Name	audiocodestrk.byoc.usw2.pure.cloud (according to requirement)

3. Configure an IP Group for the Genesys Cloud:

Parameter	Value
Index	2
Name	Genesys
Topology Location	Up
Туре	Server
Proxy Set	PS-Genesys
IP Profile	Genesys
Media Realm	MR-Genesys
SIP Group Name	audiocodestrk.byoc.usw2.pure.cloud (according to requirement)

The configured IP Groups are shown in the figure below:

IP Grou	IP Groups (3)										
+ New	Edit			🛯 🔜 Page 1	of 1 🕨	Show 10 🗸	records per pag	;e			Q
INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATI(SET	OUTBOUND MESSAGE MANIPULATI SET
0	Default_IPG	DefaultSRI	Server	Not Configure	ProxySet_0				Disable	-1	-1
1	SIPTrunk	DefaultSRI	Server	Not Configure	PS-SIPTrunk	SIPTrunk	MR-SIPTrunk	audcinterop.k	Enable	-1	-1
2	Genesys	DefaultSR	Server	Not Configure	PS-Genesys	Genesys	MR-Genesys	audcinterop.t	Enable	0	1

4.9 Configure SRTP

This section describes how to configure media security. If connectivity between AudioCodes SBC and Genesys Cloud was implemented in secure mode (TLS/SRTP), configure the SBC to operate in the same manner.

- > To configure media security:
- Open the Media Security page (Setup menu > Signaling & Media tab > Media folder > Media Security).
- 2. From the 'Media Security' drop-down list, select **Enable** to enable SRTP.

Media Security		
GENERAL		
Media Security	• Enable	•
Media Security Behavior	Preferable	•
Offered SRTP Cipher Suites	All	•
Aria Protocol Support	Disable	•
MASTER KEY IDENTIFIER		
Master Key Identifier (MKI) Size	0	
Symmetric MKI	Disable	•

Figure 4-17: Configuring SRTP

3. Click Apply.

4.10 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 interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between Genesys Cloud Contact Center and Generic SIP Trunk:

- Terminate SIP OPTIONS messages on the SBC that are received from any entity
- Calls from Genesys Cloud to Generic SIP Trunk
- Calls from Generic SIP Trunk to Genesys Cloud
- > 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).
- 2. Configure routing rules as shown in the table below:

Table 4-8: Configuration IP-to-IP Routing Rules

Index	Name	Source IP Group	Request Type	Call Triger	ReRoute IP Group	Dest Type	Dest IP Group	Internal Action
0	Terminate OPTIONS	Any	OPTIONS			Internal		Reply (Response ='200')
1	Genesys to SIP Trunk (arbitrary name)	Genesys				IP Group	SIPTrunk	
2	SIP Trunk to Genesys (arbitrary name)	SIPTrunk				IP Group	Genesys	

The configured routing rules are shown in the figure below:

Figure 4-18: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

IP-to-IP Routing (3)											
+ New	Edit Insert	↑ ↓ 🖻	14	- Page 1	of 1 🕨 🖬	Show 10 🗸	records per page				Q
INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PATTERN	DESTINATION USERNAME PATTERN	DESTINATION TYPE	DESTINATION	DESTINATION SIP INTERFACE	DESTINATIO ADDRESS
0	Options termi	Default_SBCR	Route Row	Any	OPTIONS	*	*	Internal			
1	SIP Trunk to G	Default_SBCR	Route Row	SIPTrunk	All	*	*	IP Group	Genesys		
2	Genesys to SII	Default_SBCR	Route Row	Genesys	All	*	*	IP Group	SIPTrunk		



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

4.11 Configure Number Manipulation Rules (Optional)

This section describes how to configure IP-to-IP manipulation rules. These rules manipulate the SIP Request-URI user part (source or destination number). The manipulation rules use the configured IP Groups (as configured in Section 4.8 on page 32) to denote the source and destination of the call.



Note: Adapt the manipulation table according to your environment dial plan.

For example, for this interoperability test topology, a manipulation is configured to add the "+" (plus sign) to the destination number (if it not exists) for calls from the Generic SIP Trunk to the Genesys Cloud for any destination username pattern.

- > To configure a number manipulation rule:
- Open the Outbound Manipulations table (Setup menu > Signaling & Media tab > SBC folder > Manipulation > Outbound Manipulations).
- 2. Configure the rules according to your setup.

The figure below shows an example of configured IP-to-IP outbound manipulation rules for calls between Genesys Cloud IP Group and Generic SIP Trunk IP Group:

Figure 4-19: Example of Configured IP-to-IP Outbound Manipulation Rules

Outbound Manipulations (1)													
+ New	Edit	Insert 🛊 🖡	亩	14 - 44	Page 1	of 1 🕨 🕨	Show 10 🗸	records per	page				Q
INDEX	NAME	ROUTING POLICY	ADDITION/ MANIPULA	SOURCE IP GROUP	DESTINATION IP GROUP	SOURCE USERNAME PATTERN	DESTINATI USERNAME PATTERN	MANIPULA ITEM	REMOVE FROM LEFT	REMOVE FROM RIGHT	LEAVE FROM RIGHT	PREFIX TO ADD	SUFFIX TO ADD
0	Add +	Default_SB(No	SIPTrunk	Genesys	*	[1-9]	Destination	0	0	255	+	

Rule Index	Description
0	Calls from SIP Trunk IP Group to Genesys Cloud IP Group with the prefix destination. Can be any number with digits 1 to 9. Add "+" to the prefix of the destination number.

4.12 Miscellaneous Configuration

This section describes a miscellaneous SBC configuration.

4.12.1 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:

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.

his page is intentionally left blank.

International Headquarters

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

AudioCodes Inc.

200 Cottontail Lane Suite A101E Somerset NJ 08873 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>

©2021 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 and CloudBond 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-39478

