

WindTre Nokia A-SBC & Genesys Contact Center using AudioCodes Mediant™ SBC



Table of Contents

Notice.....	v
Security Vulnerabilities	v
WEEE EU Directive	v
Customer Support.....	v
Stay in the Loop with AudioCodes.....	v
Abbreviations and Terminology	v
Document Revision Record	v
Documentation Feedback.....	vi
1 Introduction.....	1
1.1 Intended Audience	1
1.2 About Genesys Contact Center	1
1.3 About AudioCodes SBC Product Series	1
2 Component Information.....	2
2.1 AudioCodes SBC Version	2
2.2 WindTre SIP Trunk Version.....	2
2.3 Genesys Contact Center Version (Optional).....	2
2.4 Interoperability Test Topology	3
2.4.1 Environment Setup.....	4
2.4.2 Known Limitations.....	4
2.4.3 Validation and Certification.....	4
3 Configuring AudioCodes SBC	5
3.1 SBC Configuration Concept	5
3.2 IP Network Interfaces Configuration.....	6
3.2.1 Configure VLANs.....	6
3.2.2 Configure Network Interfaces	7
3.3 Configure Media Realms	7
3.4 Configure SIP Signaling Interfaces	8
3.5 Configure Proxy Sets and Proxy Address.....	9
3.5.1 Configure a Proxy Address	9
3.6 Configure Coders	10
3.7 Configure IP Profiles	11
3.8 Configure SIP Response Codes for Alternative Routing Reasons	13
3.9 Configure IP Groups	14
3.10 Configuring Classification Rules	16
3.11 Configure IP-to-IP Call Routing Rules	17
3.12 Configure Number Manipulation Rules.....	18
3.13 Configure Message Manipulation Rules.....	19
3.14 Miscellaneous Configuration.....	22

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: October-08-2026

Security Vulnerabilities

All security vulnerabilities should be reported to vulnerability@audiocodes.com.

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
12211	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>.

1 Introduction

This Configuration Note describes how to set up the AudioCodes Session Border Controller (hereafter, referred to as *SBC*) for interworking with WindTre's SIP Trunk Nokia A-SBC to interconnect to Genesys Contact Center.

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 AudioCodes or WindTre engineers, who are responsible for installing and configuring WindTre's SIP Trunk.

1.2 About Genesys Contact Center

Genesys Contact Center Solutions allows companies to manage customer requirements effectively by routing customers to appropriate resources and agents through IVR and consolidated cross-channel management of all 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 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.

2 Component Information

2.1 AudioCodes SBC Version

Table 1: AudioCodes SBC Version

SBC Vendor	AudioCodes
Models	■ Mediant 2600 E-SBC ■ Mediant 4000/B SBC ■ Mediant 9000/9030/9080 SBC ■ Mediant Software (VE/CE) SBC
Software Version	7.40A.605.092
Protocol	SIP/UDP
Additional Notes	Cluster configuration

2.2 WindTre SIP Trunk Version

Table 2: WindTre IP-SIP Trunk Version

Vendor/Service Provider	WindTre
SSW Model/Service	Nokia A-SBC
Software Version	
Protocol	SIP/UDP
Additional Notes	None

2.3 Genesys Contact Center Version (Optional)

Table 3: Genesys Contact Center Version

Vendor	Genesys
Model	Genesys Engage - Sip Server Module
Software Version	SIP Server 8.1.102.93
Protocol	SIP/UDP/TCP
Additional Notes	None

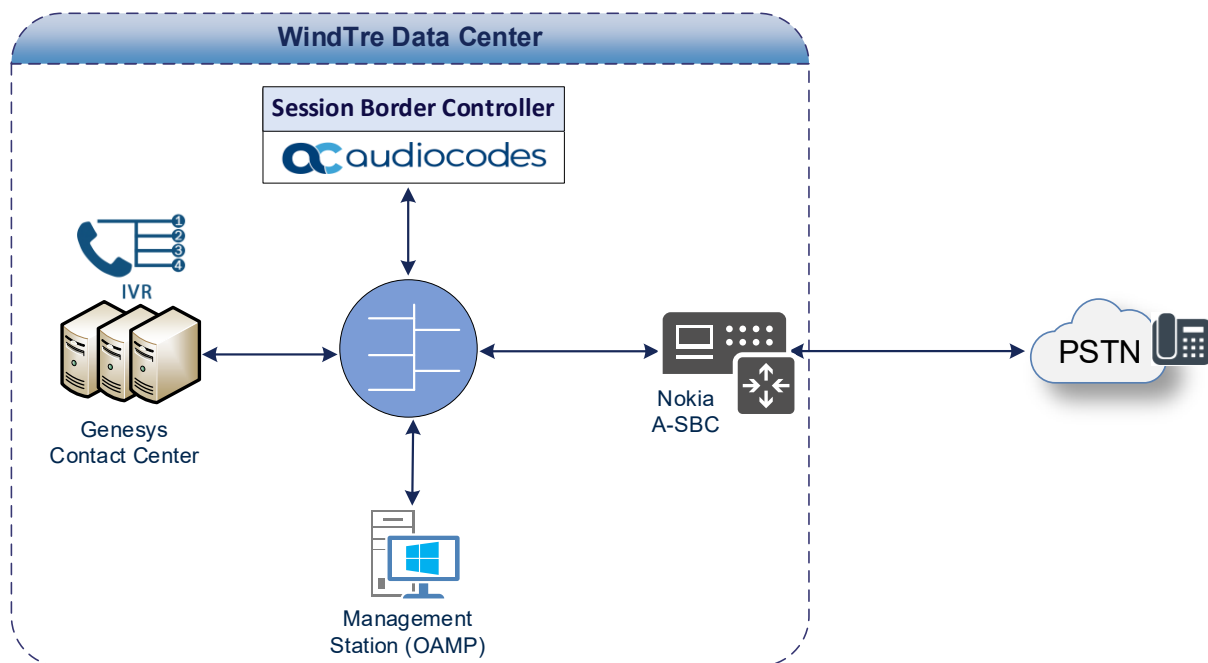
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes SBC and WindTre SIP Trunk's Nokia A-SBC, providing interconnectivity to the Genesys Contact Center was performed using the following topology:

- WindTre aims to provide its customers with enterprise voice capabilities and connectivity to the Contact Center.
- The WindTre Data Center hosts the Genesys Contact Center, which provides advanced contact center functionality and interactive voice response (IVR) capabilities to efficiently connect customers with the appropriate agents and information.
- The AudioCodes SBC provides interconnectivity between the Genesys Contact Center and WindTre SIP Trunk via Nokia A-SBC, as follows:
 - **Connectivity:** The AudioCodes SBC connects to the Genesys Contact Center and the WindTre SIP Trunk via the Nokia A-SBC.
 - **Session:** Real-time voice sessions are established using the IP-based Session Initiation Protocol (SIP)
 - **RTP Traffic:** RTP traffic between the WindTre SIP Trunk (via the Nokia A-SBC) and Genesys Contact Center flows through the AudioCodes SBC.
 - **Network Border:** The AudioCodes SBC provides IP-to-IP network border between the Genesys Contact Center, located in the WindTre's Trusted network, and Nokia A-SBC, located in the Untrusted network.

The figure below illustrates this interoperability test topology:

Figure 1: Layout of an Interoperability Test Environment



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 4: Environment Setup

Area	Setup
Network	Both the Genesys Contact Center and Nokia A-SBC are located in the WindTre Data Center. The Genesys Contact Center is connected to the trusted network, while Nokia A-SBC is connected to the untrusted network.
Signaling Transcoding	■ Genesys Contact Center uses SIP-over-TCP transport type. ■ Nokia A-SBC uses SIP-over-UDP transport type.
Supported Coders	Both systems support G.711 A-law and G.729 coders.
Media Transcoding	Both systems operate with RTP for media transport.



The configuration data used in this document, including IP addresses and FQDNs, is provided for example purposes only. Configure these values 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 with WindTre's Nokia A-SBC.

2.4.3 Validation and Certification

All interoperability tests and integration between WindTre's Nokia A-SBC and Genesys Contact Center using AudioCodes SBC have been fully approved and certified.

3 Configuring AudioCodes SBC

This section provides step-by-step instructions for configuring the AudioCodes SBC to enable interoperability between the Genesys Contact Center and Nokia A-SBC in the WindTre Data Center.

These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 3, and include the following main areas:

- **SBC management interface** – Management Station
- **SBC trusted network interface** – Genesys Contact Center
- **SBC untrusted network interface** – Nokia A-SBC

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

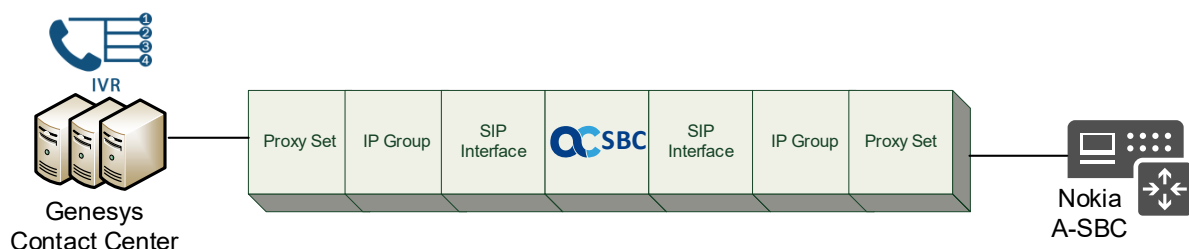


- To implement interconnectivity with WindTre SIP Trunk using the configuration described in this section, the AudioCodes SBC must be installed with a License Key that includes the following software features:
 - **SBC sessions:** Number of sessions based on requirements.
 - **Transcoding sessions:** Required only if media transcoding is needed.
 - **Coders:** Based on requirements.
 For more information about the License Key, contact your AudioCodes sales representative.
- If the 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

3.1 SBC Configuration Concept

The diagram below represents AudioCodes' device configuration concept.

Figure 2: SBC Configuration Concept

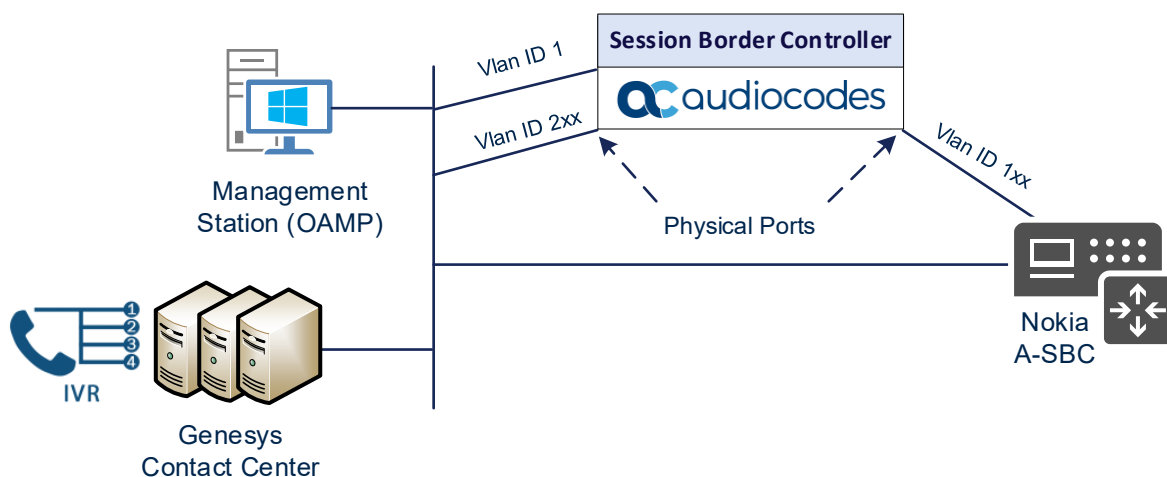


3.2 IP Network Interfaces Configuration

This section describes how to configure SBC's IP network interfaces. Although the SBC supports various deployment methods, the interoperability test topology uses the following configuration:

- **Network connectivity:** The SBC interfaces with the following IP entities:
 - Management Servers, located on the trusted network.
 - Genesys Contact Center Servers, located the trusted network.
 - WindTre SIP Trunk through Nokia A-SBC, located on the untrusted network.
- **Physical connectivity:** The physical connection depends on the network deployment architecture. In the interoperability test topology, the SBC connects to the trusted and untrusted networks using dedicated ethernet ports (i.e., two ports and two network cables).
- **Logical network interfaces:** The SBC also uses following logical network interfaces:
 - Management (VLAN ID 1)
 - VoIP_Lan (VLAN ID 2xx)
 - WAN (VLAN ID 1xx)

Figure 3: Network Interfaces in Interoperability Test Topology



3.2.1 Configure VLANs

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

- Management (assigned the name "Management")
- LAN (assigned the name "VoIP_Lan")
- WAN (assigned the name "WAN")

To configure the VLANs:

1. 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. It will be used for Management interface.
3. Add another VLAN ID 2xx (depending on specific implementation) for the trusted network
4. Add another VLAN ID 1xx (depending on specific implementation) for the untrusted network

3.2.2 Configure Network Interfaces

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

- Management Interface (assigned the name "Management")
- Trusted Network Interface (assigned the name "VoIP_Lan")
- Untrusted Network Interface (assigned the name "WAN")

To configure the IP network interfaces:

1. 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):

Table 5: Configuration Example of the Network Interface Table

Index	Application Types	Interface Mode	IP Address	Prefix Length	Gateway	I/F Name	Ethernet Device
0	OAMP	IPv4 Manual	10.xxx.xxx.xxx	24	10.xxx.0.1	Management	Management
1	Media + Control	IPv4 Manual	172.xxx.xxx.xxx	24	172.xxx.0.1	VoIP	VoIP_Lan
2	Media + Control	IPv4 Manual	192.xxx.xxx.xxx	27	192.xxx.xxx.1	Untrust_Net_1	WAN



Additional Network Interfaces can be configured according to the site specifications.

3.3 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 Teams traffic.

To configure Media Realms:

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

Table 6: Configuration Example Media Realms in Media Realm Table

Index	Name	Topology Location	IPv4 Interface Name	Port Range Start	Number of Media Session Legs
0	Internal_Media (arbitrary name)		VoIP	6000	4000 (media sessions assigned with port range)
1	External_Media (arbitrary name)	Up	Untrust_Net_1	22000	4000 (media sessions assigned with port range)

3.4 Configure SIP Signaling Interfaces

This section describes how to configure SIP Interfaces. For the interoperability test topology, towards the SIP Trunk and towards the Teams Direct Routing 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.

Table 7: Configured SIP Interfaces in SIP Interface Table

Index	Name	Topology Location	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Media Realm
0	SIPInt_internal (arbitrary name)		VoIP	SBC	0	5060	0	Internal_Media
1	SIPInt_Trunk_1 (arbitrary name)	Up	Untrust_Net_1	SBC	5060	0	0	External_Media



Additional SIP Interfaces can be configured according to the site specifications.

3.5 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, Proxy Sets need to be configured for the following entities:

- Genesys Contact Center Servers
- WindTre SIP Trunks through Nokia A-SBC

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 8: Configuration Example Proxy Sets in Proxy Sets Table

Index	Name	SBC IPv4 SIP Interface	Proxy Keep-Alive
1	PRX_SIP-GVP_IV (arbitrary name)	SIPInt_internal	Using Options
2	PRX_SIP-OP_IV (arbitrary name)	SIPInt_internal	Using Options
3	PRX_2nd_DC_SBC (arbitrary name)	SIPInt_internal	Using Options
4	PRX_WindTreTrunk01 (arbitrary name)	SIPInt_Trunk_1	Using Options

3.5.1 Configure a Proxy Address

This section describes how to configure a Proxy Address.

To configure a Proxy Address for Proxy Set:

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

Table 9: Configuration Proxy Address for Proxy Set

Index	Proxy Address	Transport Type
0	<desire IP address>:5060	TCP (for Genesys and second data center) or UDP (for WindTre Trunks)

4. Click **Apply**.
5. Repeat this configuration for each Proxy Set.

3.6 Configure Coders

This section describes how to configure coders using a *Coder Group*. Because Genesys Contact Center and WindTre SIP Trunks may support specific coders, a Coder Group must be configured with required coders for the untrusted network leg.

The Coder Group ID configured in this section is assigned to the 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. Click **New**, and then configure a name for the Coder Group for the WindTre SIP Trunks (e.g., `AudioCodersGroups_Default`).
3. Click **Apply**.
4. Select the new row that you configured, and then click the **Coders Table** link below the table.
The Audio Coders table opens.

Parameter	Value
Coder Name	■ G.729 ■ G.711 A-law

5. 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 voice sent to the WindTre SIP Trunks uses the dedicated coders list whenever possible. Note that this Allowed Coders Group ID will be assigned to the IP Profile belonging to the WindTre SIP Trunks in the next step.

To set a preferred coder for the Genesys:

1. Open the Allowed Audio Coders Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Allowed Audio Coders Groups**).
2. Click **New** and configure a name for the Allowed Audio Coders Group for WindTre SIP Trunks (e.g., `AllowedAudioCoders`).
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 configure an Allowed Coders as follows:

Parameter	Value
Index	0
Coder	G.729
Index	1
Coder	G.711 A-law

6. Open the Media Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Media Settings**).
7. From the '**Extended Coders Behavior**' drop-down list, select **Include Extensions**.
8. Click **Apply**.

3.7 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 entities:

- Trusted Network leg
- Untrusted Network leg

To configure an IP Profile for the Trusted Network

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	0
Name	IP_Prof_Trust_Network (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	Not Secured
SBC Media	
Allowed Audio Coders	AllowedAudioCoders

3. Click **Apply**.

To configure IP Profile for the Untrusted Network:

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

Parameter	Value
General	
Index	1
Name	IP_Prof_Untrust_Network (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	Not Secured
SBC Media	
Extension Coders Group	AudioCodersGroups_Default
Allowed Audio Coders	AllowedAudioCoders
RFC 2833 DTMF Payload Type	96
SBC Signaling	
Remote Delayed Offer Support	Not Supported
SBC Forward and Transfer	
Remote REFER Mode	Handle Locally
Remote 3xx Mode	Handle Locally
SBC Hold	
Remote Hold Format	Send Only

3. Click **Apply**.

3.8 Configure SIP Response Codes for Alternative Routing Reasons

This section describes how to configure SBC to handle SIP error responses received for outgoing SIP dialog-initiating requests, such as INVITE, OPTIONS, and SUBSCRIBE. When a configured SIP error response is received, the SBC attempts to find an alternative route. Alternative routing based on SIP response codes is configured using the following two tables, which have a 'parent-child' relationship:

- **Alternative Reasons Set table ('parent'):** Defines the name of the Alternative Reasons Set
- **Alternative Reasons Rules table ('child'):** Defines the SIP response codes associated with each Alternative Reasons Set

To apply the configured alternative routing rules, assign the Alternative Reasons Set to the destination IP Group in the IP Groups table, using the **SBC Alternative Routing Reasons Set** parameter.

To configure SIP reason codes for alternative IP routing:

1. Open the **Alternative Routing Reasons** table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **Alternative Reasons Set**).
2. Click **New**, and then configure a name for the Alternative Routing Reasons Set (e.g., *Alternative_routing*).
3. Click **Apply**.
4. Select the row of the newly configured Alternative Reasons Set, and then click the **Alternative Reasons Rules** link at the bottom of the page.
The Alternative Reasons Rules table opens.
5. Click **New**, and then select the required **4xx**, **5xx** and **6xx** SIP response codes from the **Release Cause Code** drop-down list.
6. Click **Apply**.

3.9 Configure IP Groups

This section describes how to configure IP Groups. The IP Group represents an IP entity on the network with which 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 entities:

- Genesys Contact Center Servers located on the trusted network
- WindTre second Data Center SBC located on the trusted network
- WindTre SIP Trunks located on the untrusted network

To configure IP Groups:

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

Parameter	Value
Index	0
Name	IPG_Sip-Server-GVP_IV (arbitrary descriptive name)
Type	Server
Proxy Set	PRX_SIP-GVP_IV
IP Profile	IP_Prof_Trust_Network
Media Realm	Internal_Media
Classify By Proxy Set	Disable

2. Configure an IP Group for the Genesys OP Server:

Parameter	Value
Index	1
Name	IPG_Sip-Server-OP_IV (arbitrary descriptive name)
Type	Server
Proxy Set	PRX_SIP-OP_IV
IP Profile	IP_Prof_Trust_Network
Media Realm	Internal_Media
Classify By Proxy Set	Disable

3. Configure an IP Group for the second Data Center SBC:

Parameter	Value
Index	2
Name	IPG_2nd_DC_SBC (arbitrary descriptive name)
Type	Server
Proxy Set	PRX_2nd_DC_SBC
IP Profile	IP_Prof_Trust_Network
Media Realm	Internal_Media
Classify By Proxy Set	Disable

4. Configure an IP Group for the WindTre SIP Trunk:

Parameter	Value
Index	3
Name	IPG_WindTreTrunk01 (arbitrary descriptive name)
Topology Location	Up
Type	Server
Proxy Set	PRX_WindTreTrunk01
IP Profile	IP_Prof_Untrust_Network
Media Realm	External_Media
Classify By Proxy Set	Disable
SBC Alternative Routing Reason Set	Alternative_routing (as configured in previous section)

3.10 Configuring Classification Rules

This section describes how to configure Classification rules. A Classification rule classifies incoming SIP dialog-initiating requests (e.g., INVITE messages) to a 'source' IP Group. The source IP Group is the SIP entity that sent the SIP dialog request. Once classified, the device uses the IP Group to process the call (manipulation and routing).

You can also use the Classification table for employing SIP-level access control for successfully classified calls, by configuring Classification rules with whitelist and blacklist settings. If a Classification rule is configured as a whitelist ("Allow"), the device accepts the SIP dialog and processes the call. If the Classification rule is configured as a blacklist ("Deny"), the device rejects the SIP dialog.

In this interoperability test topology, classification rule must be configured for each IP Group.

WindTre SIP Trunks: Classification is based on the source SIP Interface and transport type (UDP).

Genesys Contact Center servers and the second data center SBC: Classification is based on the source SIP Interface and IP address.

To configure Classification rules for WindTre SIP Trunks:

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

Parameter	Value
Index	0
Name	Class_inbound_WindTre Trunk01 (arbitrary name)
Source SIP Interface	SIPInt_Trunk_1
Source Transport Type	UDP
Action Type	Allow
Source IP Group	IPG_WindTreTrunk01

3. Click **Apply**.
4. Repeat this procedure to configure a classification rule for each WindTre SIP Trunk..

To configure Classification rules for Genesys Servers and second DC SBC:

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

Parameter	Value
Name	Class_inbound_SIP-Server-GVP_IV (arbitrary name)
Source SIP Interface	SIPInt_internal
Source IP Address	<IP address of the Genesys SIP Server>
Action Type	Allow
Source IP Group	IPG_Sip-Server-GVP_IV

3. Click **Apply**.
4. Create similar rules for each Genesys Server and second DC SBC.

3.11 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 Teams Direct Routing and WindTre SIP Trunk:

- Terminate SIP OPTIONS messages on the SBC that are received from any entity.
- Terminate REFER messages to the Genesys SIP Servers.
- Calls from WindTre SIP Trunks to the Genesys SIP Servers.
- Calls from Genesys SIP Servers to WindTre SIP Trunks through Nokia A-SBC.
- If routing to the WindTre SIP Trunks fails, route calls from the Genesys SIP servers to the SBC in the second data center.

To configure IP-to-IP routing rules:

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

Table 10: Configuration Example IP-to-IP Routing Rules

Index	Name	Alternative Route Options	Source IP Group	Request Type	Dest Host	Call Trigger	Dest Type	Dest IP Group	Internal Action
0	Terminate OPTIONS		Any	OPTIONS			Internal		Reply (Response = '200')
1	Refer_to_GVP-IV (arbitrary name)		Any		<Genesys SIP Server IP>	REFER	IP Group	IPG_Sip-Server-GVP_IV	
2	Trunk_to_GVP-IV (arbitrary name)		Any				IP Group	IPG_Sip-Server-GVP_IV	
3	GVP-IV_to_Trunk (arbitrary name)		IPG_Sip-Server-GVP_IV				IP Group	IPG_WindTreTrunk01	
4	GVP-IV_to_2nd_DC_SBC (arbitrary name)	Alternative Route Consider Inputs	IPG_Sip-Server-GVP_IV				IP Group	IPG_2nd_DC_SBC	



The routing configuration may change according to specific deployment topology.

3.12 Configure Number Manipulation Rules

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 3.9 on page 14) to denote the source and destination of the call.



Adapt the manipulation table according to your environment dial plan.

For this interoperability test topology, a number manipulation rule is configured to remove the first three digits from the destination number for calls originating from the Genesys SIP servers

To configure a number manipulation rule:

1. Open the Outbound Manipulations table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Manipulation** > **Outbound Manipulations**).
2. Configure the rules according to your setup.

The table below shows an example of configured IP-to-IP outbound manipulation rules for calls from the Genesys SIP Servers IP Groups:

Rule Index	Description
0	For all SIP Invite messages from Genesys SIP Servers IP Group with any destination number (*), remove 3 digits from the left.

3.13 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 rules:

1. Open the Message Manipulations page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulation Sets**).
2. Click **New** and configure a name for the Message Manipulation Set forWindTre modifying Max-Forwards header value (e.g., *Modify Option Max forward*).
3. Click **Apply**.
4. Select the new row that you added, and then click the **Message Manipulations** link located below the table; the Message Manipulations table opens.
5. Click **New** and configure a manipulation rule that will be assigned to all WindTre SIP Trunks SIP Interfaces. This rule applies to the SIP OPTIONS messages received from Genesys SIP Servers and Nokia A-SBC. They send SIP OPTIONS messages with the Max-Forwards header value '0', which causes error messages in syslog. This rule changes the value of the Max-Forwards header to '70'.

Parameter	Value
Index	0
Name	Change Max-Forwards (arbitrary name)
Message Type	Options.Request
Condition	Header.Max-Forwards=='0'
Action Subject	Header.Max-Forwards
Action Type	Modify
Action Value	'70'

6. Return to the Message Manipulation Sets page.
7. Click **New** and configure a name for the Message Manipulation Set forWindTre outbound traffic towards WindTre SIP Trunks (e.g., *MMS_for_pub_trunk*).
8. Click **Apply**.
9. Select the new row that you added, and then click the **Message Manipulations** link located below the table; the Message Manipulations table opens.

10. Click **New** and configure another manipulation rule. This rule applies to SIP OPTIONS messages sent to the WindTre SIP Trunks IP Groups. This rule replaces the host part of the SIP Request-URI header with the destination IP address.

Parameter	Value
Index	0
Name	Modify Options R-URI Host (arbitrary name)
Message Type	Options
Action Subject	Header.Request-URI.URL.Host
Action Type	Modify
Action Value	Param.Message.Address.Dst.IP

11. Click **New** and configure another manipulation rule. This rule applies to SIP OPTIONS messages sent to the WindTre SIP Trunks IP Groups. This rule replaces the host part of the SIP To header with the destination IP address.

Parameter	Value
Index	1
Name	Modify Options To Host (arbitrary name)
Message Type	Options
Action Subject	Header.To.URL.Host
Action Type	Modify
Action Value	Param.Message.Address.Dst.IP

12. Click **New** and configure another manipulation rule. This rule applies to SIP OPTIONS messages sent to the WindTre SIP Trunks IP Groups. This rule replaces the host part of the SIP From header with the source IP address.

Parameter	Value
Index	2
Name	Modify Options From Host (arbitrary name)
Message Type	Options
Action Subject	Header.From.URL.Host
Action Type	Modify
Action Value	Param.Message.Address.Src.IP

13. Click **New** and configure another manipulation rule. This rule applies to messages sent to the WindTre SIP Trunks IP Groups. This rule removes X-Genesys-Call header.

Parameter	Value
Index	3
Name	Remove X-Genesys-Call header (arbitrary name)
Message Type	Invite
Action Subject	Header.X-Genesys-Call
Action Type	Remove

14. Assign Manipulation Set to the WindTre SIP Trunks SIP Interfaces:
- Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
 - Select the row of the WindTre SIP Trunk SIP Interface, and then click **Edit**.
 - From the 'Pre-Classification Manipulation Set' drop-down list, select **Modify Option Max forward**.
 - Click **Apply**.
 - Repeat this for each WindTre SIP Trunk SIP Interface.
15. Assign Manipulation Set to the WindTre SIP Trunks IP Groups:
- Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
 - Select the row of the WindTre SIP Trunk IP Group, and then click **Edit**.
 - From the 'Outbound Manipulation Set' drop-down list, select **MMS_for_pub_trunk**.
 - Click **Apply**.
 - Repeat this for each WindTre SIP Trunk IP Group.



Depending on your implementation, additional message manipulation rules may be required. For more information, refer to the AudioCodes User Manual, or contact an AudioCodes representative to arrange Professional Services from AudioCodes, and our Professional Services team will help you with your configuration.

3.14 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

Optimizing CPU Cores Usage for a Specific Service (relevant for Mediant 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



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

International Headquarters

Naimi Park
6 Ofra Haza Street
Or Yehuda, 6032303, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.

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

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

©2026 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, 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-12211

