Configuration Note

AudioCodes Professional Services – Interoperability Lab

ItalTel SIP Trunk & Genesys Contact Center using AudioCodes Mediant SBC

Version 7.2

Table of Contents

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: June-26-2018

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 Web site at https://www.audiocodes.com/services-support/maintenance-and-support.

Abbreviations and Terminology

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

Document Revision Record

LTRT	Description
12795	Initial document release for Version 7.2.

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 document describes how to configure AudioCodes' Session Border Controller (hereafter referred to as SBC) for interworking between the Italtel ITSP SIP Trunk and Genesys Contact Center.

Note: Throughout this document, the term 'SBC' also refers to AudioCodes' Mediant SBC product series.

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and Genesys Contact Center Partners who are responsible for installing and configuring the Italtel ITSP SIP Trunk and Genesys Contact Center for enabling VoIP calls using AudioCodes' SBC.

1.2 About AudioCodes SBC Product Series

AudioCodes' family of SBC devices enables reliable connectivity and security between the enterprise 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 (MSBR) platforms, or as a software-only solution for deployment with third-party hardware.

1.3 About Genesys Contact Center

Genesys 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 all of a customer’s interactions. Sophisticated profiling, outbound voice and performance management enables companies to provide very personalized customer care and delivery.

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 E-SBC ▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 4000 SBC ▪ Mediant 9000 SBC ▪ Mediant Software SBC (Server Edition and Virtual Edition)
Software Version	SIP_7.20A.158.012
Protocol	▪ SIP/UDP (to the Italtel ITSP SIP Trunk via PostItaliane Lab NetMatch-S SBC) ▪ SIP/UDP (to the Genesys Contact Center system)
Additional Notes	None

2.2 Italtel SIP Trunking Version

Table 2-2: Italtel Version

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

2.3 Genesys Contact Center Version

Table 2-3: Genesys Contact Center Version

Vendor	Genesys
Software Version	Genesys SIP Server v8.1.102.25/Genesys Voice Platform (GVP) v8.5
Protocol	SIP
Additional Notes	None

2.4 Interoperability Test Topology

The Genesys Contact Center SIP Server is connected to the Italtel ITSP SIP Trunk Provider via an SBC in a similar way to an IP-PBX.

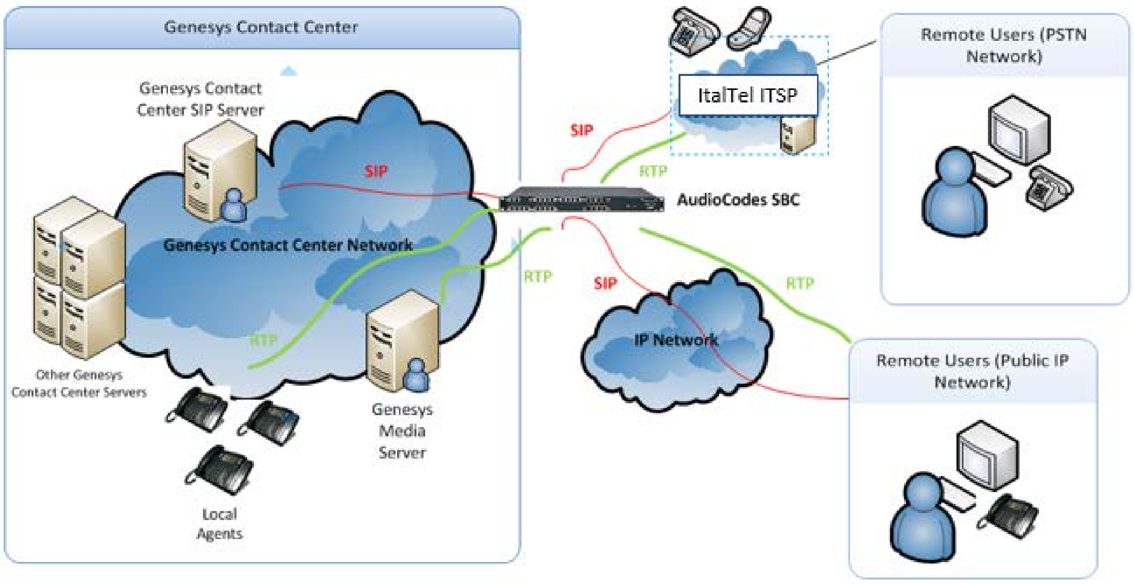
Note: Contact your Genesys Contact Center support channel for more information about topological scenarios.

Interoperability testing between AudioCodes SBC and Italtel ITSP SIP Trunk with Genesys Contact Center 8.1 was performed using the following topology:

- The enterprise was deployed with a Genesys 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 Contact Center with the Public PSTN via the Italtel ITSP SIP Trunk, as an Over the Top (OTT) trunk over the public network. For the IOT, the OTT trunk was through the PostItaliane Lab NetMatch-S SBC which transparently passed SIP messaging to the ItalTel ITSP SIP Trunk
- AudioCodes' SBC was deployed to interconnect between the enterprise's LAN and the SIP trunk.
    - The SBC was connected to the Genesys Contact Center SIP server on the Genesys Contact Center internal network, and to the Italtel ITSP SIP Trunk located on the public network.
    - RTP traffic from/to the Italtel ITSP SIP trunk flowed via an SBC to/from Genesys Contact Center Media Server, or to a local agent phone on the Call Center network, or to a Remote Agent on the PSTN network or public Internet space.

The figure below illustrates the interoperability test topology:

Figure 2-1: Interoperability Test Topology



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	▪ Genesys Contact Center environment as a service is located on the Genesys Contact Center network ▪ Genesys Contact Center agent SIP phones are located on the enterprise's LAN. Remote Agent directory numbers (DNs) exist in the public network ▪ Italtel ITSP SIP Trunk is located on the WAN
Signaling Transcoding	▪ Genesys Contact Center operates with SIP-over-UDP, TCP or TLS transport type ▪ Italtel SIP Trunk operates with SIP-over-UDP transport type. ▪ The interoperability test environment used SIP-over-UDP
Codecs Transcoding	▪ Genesys Contact Center is capable of supporting G.729, G.711A-law, G.711U-law, G.723, G722.2 and G.726 coders ▪ Italtel SIP Trunk supports G.729 (preferred) and G.711 A-law (recommended) coders
Media Transcoding	▪ Genesys Contact Center and Italtel SIP Trunk operate with RTP media Type
DTMF	▪ Genesys Contact Center supports delivering DTMF using SIP INFO message, RFC 2833 Named Telephony events, and in-band per ITU-T Recommendation Q.23 ▪ Italtel supports RFC 2833

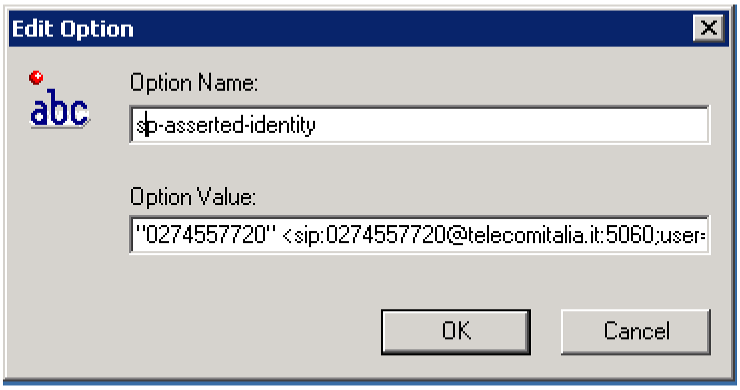
Note: The configuration data used in this document, such as IP addresses and FQDNs are used for example purposes only. This data should be configured according to the site specifications.

2.4.2 Known Limitations/Restrictions/Notes

The following Genesys Call Center functionality is not supported by Italtel SIP Trunk:

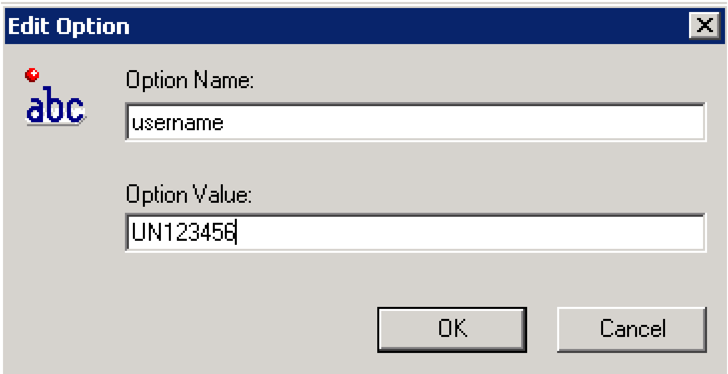
- **SIP 302 Moved Temporarily:** Italtel does not support SIP 302 Moved Temporarily. This should be handled locally by the SBC.
- **SIP REFER:** Italtel does not support SIP REFER operation. This should be handled locally by the SBC.
- **P-Asserted-Identity:** Italtel requires P-Asserted-Identity header to be included in initial SIP INVITE. The SIP URI user part in the PAI must contain the e.164 number of the calling party, which must be one of the (on-net) numbers assigned by Italtel. This can be implemented by Genesys contact center, or it can be handled by the SBC.

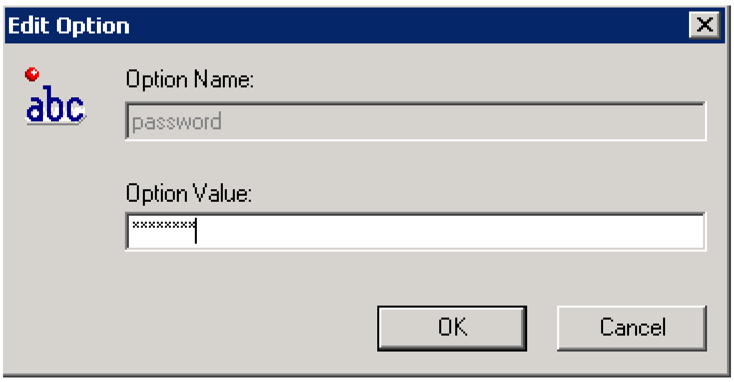
  If considering implementing Genesys contact center implementation, this can be defined in the Genesys DN object (Annex -> TServer section) for each extension, as indicated by the following example using CME.



- **SIP Authentication for Outbound Calls:** Italtel does not support the use of SIP Digest (challenging the SIP User Agent on receiving a SIP Request from the Contact Center). If SIP authentication for outbound calls (from the Contact Center) is required, the SIP authentication challenge can be handled on the SBC as part of the Trunk-Side Equipment (TSE).

  If considering implementation in Genesys contact center, this can be defined in the Options -> AuthClient section of the outgoing trunk, as indicated by the following example using CME. Note if SIP Authentication is not required, then both options would not be defined.





- **SBCMAXFORWARDSLIMIT:** For the interoperability test, this parameter was set to the a setting of 70 (default = 10). Consider configuring this parameter according to deployment requirements. (**Setup** tab > **SBC** folder > **SBC General Settings**)

This page is intentionally left blank.

3 Configuring AudioCodes SBC

This section shows how to configure AudioCodes SBC for interworking between Genesys Contact Center and the Italtel ITSP SIP Trunk. The configuration is based on the interoperability test topology described in Section 2.4 on page 10 and includes the following:

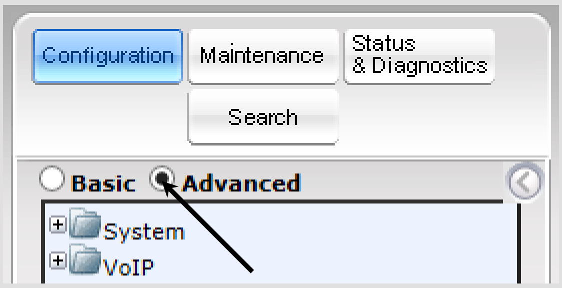
- **SBC WAN interface** - Italtel ITSP SIP Trunking environment
- **SBC LAN interface** - Genesys Contact Center environment

Configuration is performed using the SBC's embedded Web server (referred to as *Web interface* in this document). For detailed information on configuring AudioCodes E-SBCs, refer to the E-SBC User's Manual.

Note:

- To implement the Genesys Contact Center and Italtel ITSP SIP Trunk based on the configuration described in this section, the SBC must be installed with a Software License Key that includes the following software features:
  - √ SBC
  - √ Security
  - √ RTP
  - √ SIP

  For more information about the Software License Key, contact your AudioCodes Sales Representative.
- The scope of this interoperability test and document does not cover all security aspects of connecting the SIP Trunk to the Genesys Contact Center environment. Comprehensive security measures should be implemented per the enterprise's security policies. For security recommendations on AudioCodes' products, refer to the *Recommended Security Guidelines* document.
- The tables in this document were copied from the configured interoperability laboratory system and are listed in the order necessary to route correctly. If the configuration was built with sequential indices, it may be necessary to use the **Up** and **Down** buttons to correctly order the rows. The Genesys2RemoteAgents row has been moved up in the table so the more specific condition is evaluated for routing before the more general conditions.
- Before you begin configuring the SBC, ensure that the SBC's Web interface navigation tree is in **Advanced** display mode, selectable as shown below:



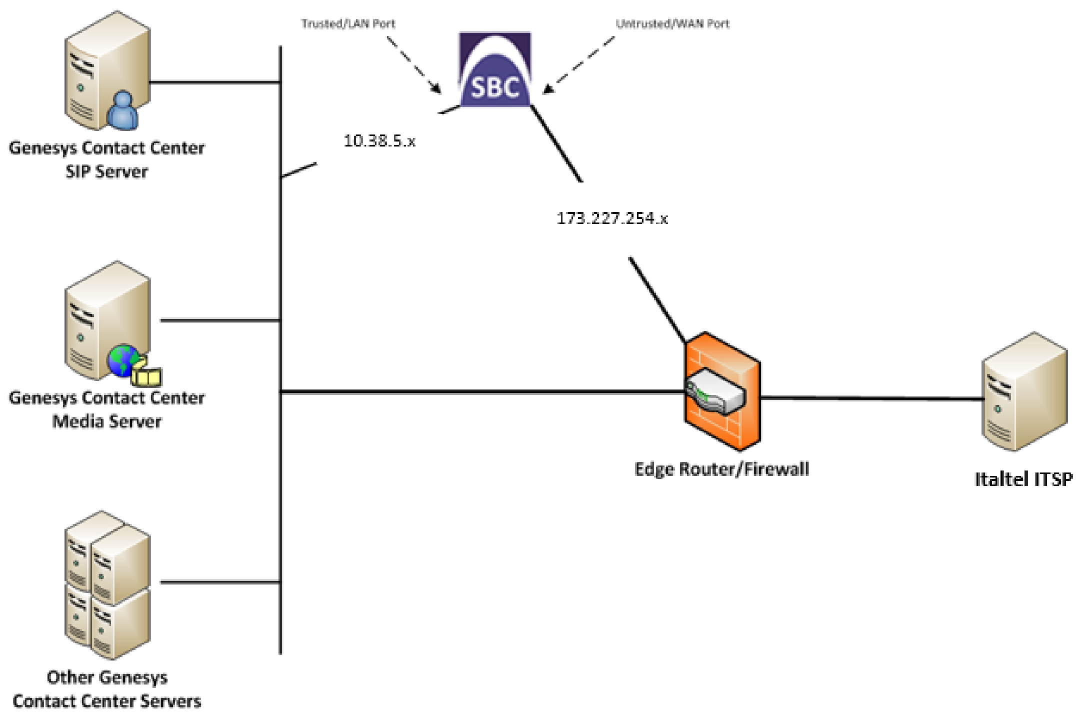
  Note that when the SBC is reset, the navigation tree reverts to **Basic** display mode.

3.1 Step 1: Configure IP Network Interfaces

This step describes how to configure the SBC's IP network interfaces. A number of methods can be used to deploy the SBC; the interoperability test topology uses the following method:

- SBC interfaces with these IP entities:
  - Genesys Contact Center, located on the Genesys Contact Center Service Provider network (LAN)
  - Italtel ITSP SIP Trunk, located on the WAN
- SBC connects to the WAN through a DMZ network.
- Physical connection to the LAN: Type depends on the method used to connect to the Genesys Contact Center Service Provider's network. In the interoperability test topology, the SBC connects to the LAN and WAN using dedicated LAN ports (i.e., using two ports and two network cables).
- SBC uses two logical network interfaces:
  - LAN 10.38.5.x (VLAN ID 1)
  - WAN 173.227.254.x (VLAN ID 2)

Figure 3-1: Network Interfaces in Interoperability Test Topology



3.1.1 Step 1a: Configure Physical Ports

This step describes how to define Physical Ports for each of the following interfaces:

- GE_1: This is a port interfacing the Trusted/LAN network segment. The Genesys SIP Server is access via this interface.
- GE_2: This is a port interfacing the Untrusted/WAN network segment. The ITSP is accessed via this interface.

➢ To configure the physical Ethernet ports:

1. Open the Physical Ports table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Physical Ports**).
2. Confirm configuration of a port and that the port is a member of an Ethernet Group (see next step to make the port a member of an Ethernet Group if needed).

Figure 3-2: Physical Ports-GE1

#0[GE_1]

GENERAL	
Name	GE_1
Description	User Port #0
Mode	Enable
Speed and Duplex	Auto Negotiation

ETHERNET GROUP	
Member of Ethernet Gro...	GROUP_1
Group Status	Active

Figure 3-3: Physical Ports-GE2

#1[GE_2]

GENERAL	
Name	GE_2
Description	User Port #1
Mode	Enable
Speed and Duplex	Auto Negotiation

ETHERNET GROUP	
Member of Ethernet Gro...	GROUP_2
Group Status	Active

3.1.2 Step 1b: Configure Ethernet Port Groups

This step describes how to define members to an Ethernet Port Group for each of the interfaces:

- GROUP_1: This is a redundancy group of ports interfacing the Trusted/LAN network segment. The Genesys SIP Server is access via this interface.
- GROUP_2: This is a redundancy group of ports interfacing the Untrusted/WAN network segment. The ITSP is accessed via this interface

➢ **To configure Ethernet Groups:**

1. Open the Ethernet Groups table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Ethernet Groups**).
2. If the ports defined above are not already a member of different port groups, assign them as such.

Figure 3-4: Ethernet Port Group 1

#0[GROUP_1]

GENERAL	
Name	GROUP_1
Mode	• SINGLE
Member 1	• # [GE_1]
Member 2	• # [--]

Figure 3-5: Ethernet Port Group 2

#1[GROUP_2]

GENERAL	
Name	GROUP_2
Mode	• SINGLE
Member 1	• # [GE_2]
Member 2	• # [--]

3.1.3 Step 1c: Configure Underlying Ethernet Devices

This step describes how to define VLANs for each of the following interfaces:

- LAN VoIP (assigned the name "Trusted")
- WAN VoIP (assigned the name "Untrusted")

➢ **To configure an Ethernet Device:**

1. Open the Ethernet Devices table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Ethernet Devices**).
2. Create an association between the VLAN ID's, underlying interface and the Ethernet Device Name. In this example, VLAN ID 254 is used for the Untrusted interface, but since this is untagged, the value is only noted for future reference to the network VLAN id the traffic passes over.

Figure 3-6: Ethernet Device-Trusted

#0[Trusted]

GENERAL	
Name	Trusted
VLAN ID	1
Underlying Interface	# [GROUP_1]
Tagging	Untagged
MTU	1500

Figure 3-7: Ethernet Device-Untrusted

#1[Untrusted]

GENERAL	
Name	Untrusted
VLAN ID	254
Underlying Interface	# [GROUP_2]
Tagging	Untagged
MTU	1500

3.1.4 Step 1b: Configure Network Interfaces

This step describes how to configure the following interfaces:

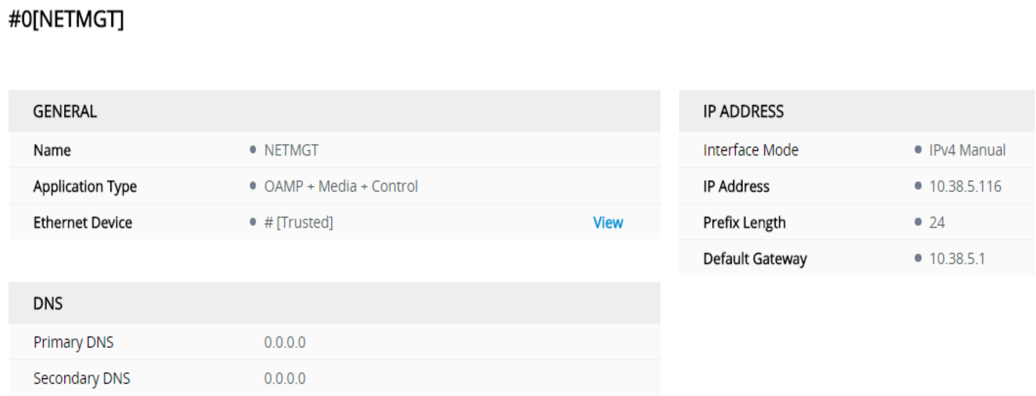
- **LAN VoIP interface** (assigned the name "Trusted")

  and
- **WAN VoIP interface** (assigned the name "Untrusted")

➢ **To configure IP network interfaces:**

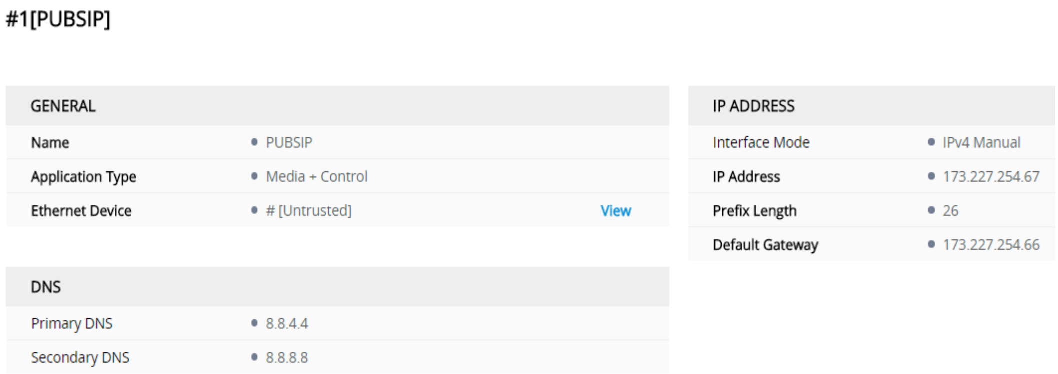
1. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
2. Modify the existing LAN network interface: (per Site Specifications).

Figure 3-8: LAN Network Interface



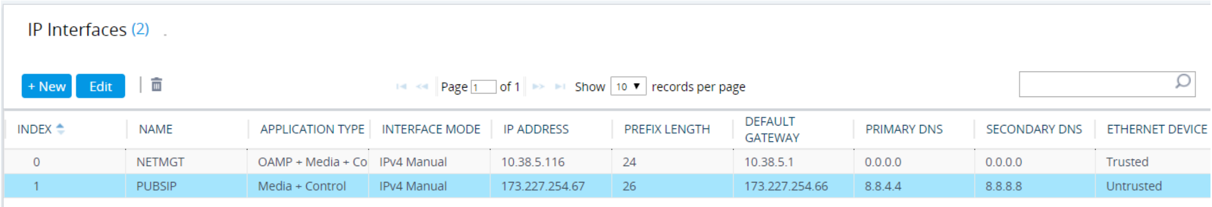
3. Add a network interface for the WAN side: (per Site Specifications).

Figure 3-9: WAN Network Interface



The configured IP network interfaces are shown below:

Figure 3-10: Configured Network Interfaces in IP Interfaces Table



3.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application *if on a hybrid device.*

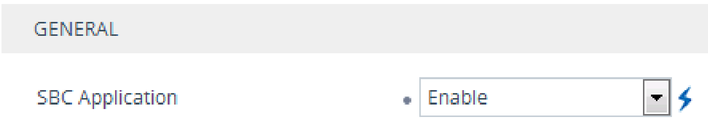
Before you can start configuring the SBC, you must first enable the SBC application. Once enabled, the Web interface displays the menus and parameter fields relevant to the SBC application.

> **Note:** The SBC feature is available only if the device is installed with a License Key that includes this feature.

➢ **To enable the SBC application:**

1. Open the Applications Enabling page (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Applications Enabling**).
2. From the 'SBC Application' drop-down list, select **Enable**:

Figure 3-11: SBC Application



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

3.3 Step 3: Signaling Routing Domains

This step describes Signaling Routing Domains (SRDs). The SRD is a logical representation of an entire SIP-based VoIP network (Layer 5) consisting of groups of SIP users and servers. The SRD is associated with all the configuration entities (e.g., SIP Interfaces and IP Groups) required for routing calls within the network. Typically, only a *single* SRD is required (recommended) for most deployments. Multiple SRDs are only required for multi-tenant deployments, where the physical device is "split" into multiple logical devices. In this case, it is suitable to use the default SRD. The SRD comprises:

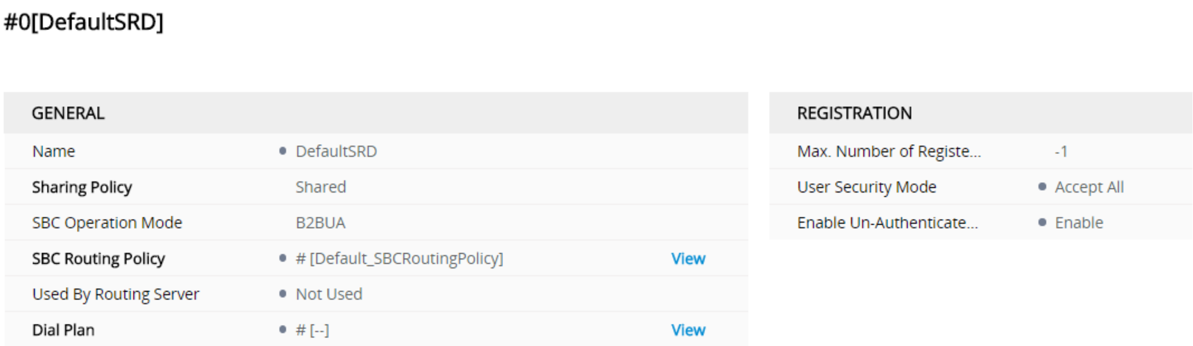
- SIP Interface (mandatory)
- IP Group (mandatory)
- Proxy Set (mandatory)
- Admission Control rule (optional)
- Classification rule (optional)

As each SIP Interface defines a different Layer-3 network on which to route or receive calls and as you can assign multiple SIP Interfaces to the same SRD, for most deployment scenarios (even for multiple Layer-3 network environments), you only need to employ a single SRD to represent your VoIP network (Layer 5). For example, if your VoIP deployment consists of a Genesys SIP Server (LAN), a SIP Trunk (WAN), and far-end users (WAN), you would only need a single SRD. The single SRD would be assigned to three different SIP Interfaces, where each SIP Interface would represent a specific Layer-3 network (IP PBX, SIP Trunk, or far-end users) in your environment.

➢ **To view the default SRD:**

1. Open the SRDs table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).

Figure 3-12: Default SRD



3.3.1 Step 3a: Configure Media Realms

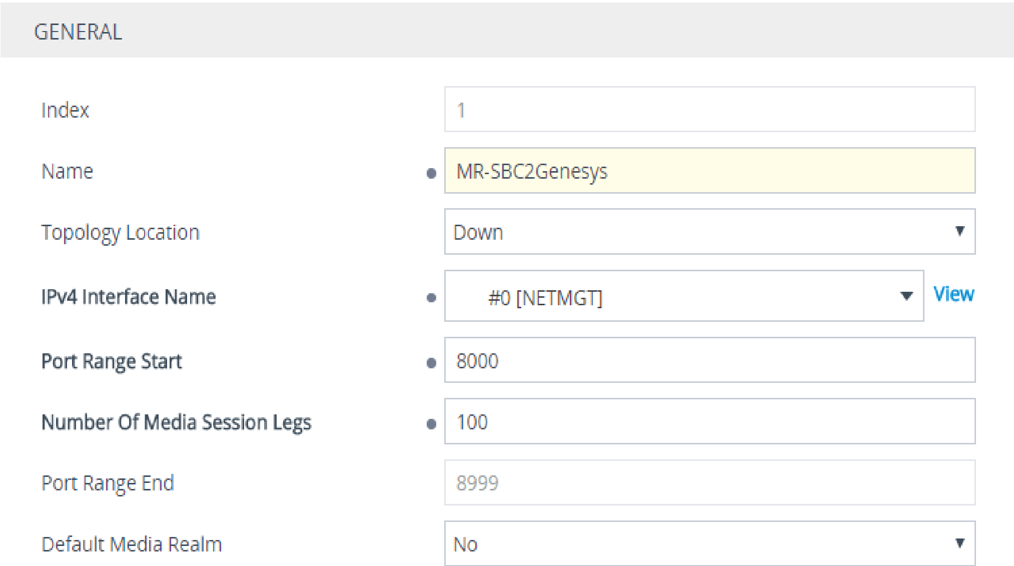
This step describes how to configure Media Realms. The simplest way is to create two Media Realms - one for internal Genesys traffic and one for external ITSP traffic. Remote Agents will also use a Media Realm, but this will be covered later.

➢ **To configure Media Realms:**

1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Modify the existing Media Realm for LAN traffic or create a new MR:

Parameter	Value
Index	**1**
Media Realm Name	**MR-SBC2Genesys** (descriptive name)
IPv4 Interface Name	**NETMGT**
Port Range Start	**8000** (represents lowest UDP port number used for media on LAN).
Number of Media Session Legs	**100** (media sessions assigned with port range)

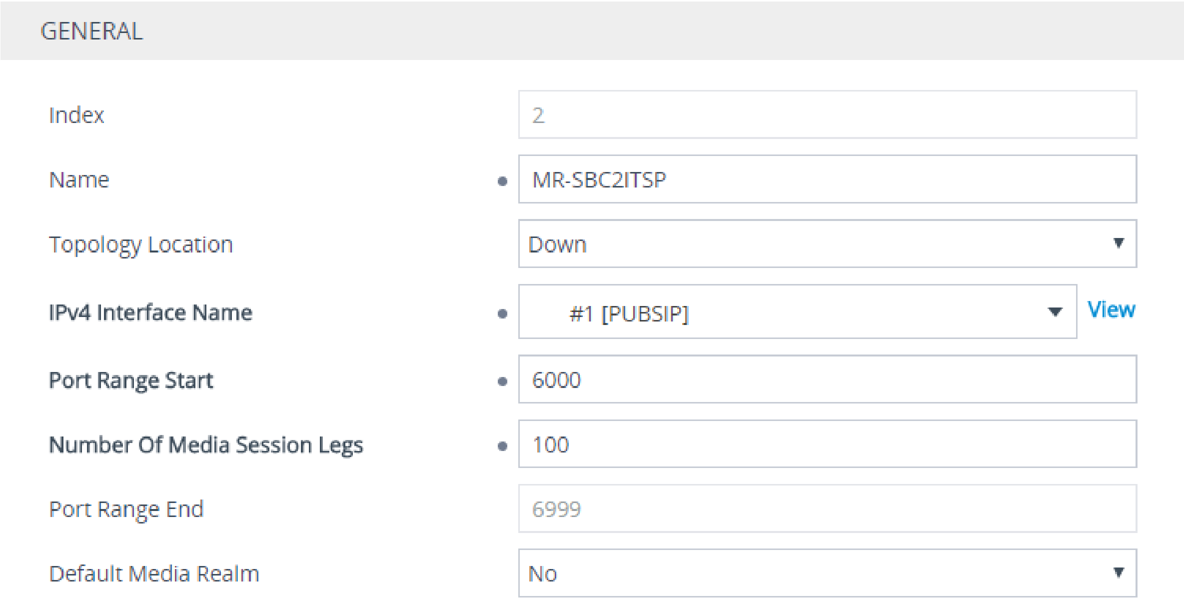
Figure 3-13: Configure Media Realm for LAN



3. Configure a Media Realm for WAN traffic:

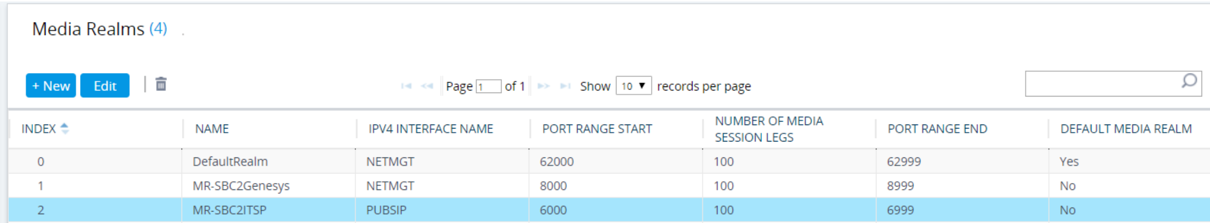
Parameter	Value
Index	**2**
Media Realm Name	**MR-SBC2ITSP** (arbitrary name)
IPv4 Interface Name	**PUBSIP**
Port Range Start	**6000** (represents the lowest UDP port number used for media on WAN).
Number of Media Session Legs	**100** (media sessions assigned with port range).

Figure 3-14: Configure Media Realm for ITSP



The configured Media Realms are shown in the figure below:

Figure 3-15: Configured Media Realms in Media Realm Table



Media Realms (4)

+ New Edit Page 1 of 1 Show 10 records per page

INDEX	NAME	IPV4 INTERFACE NAME	PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	PORT RANGE END	DEFAULT MEDIA REALM
0	DefaultRealm	NETMGT	62000	100	62999	Yes
1	MR-SBC2Genesys	NETMGT	8000	100	8999	No
2	MR-SBC2ITSP	PUBSIP	6000	100	6999	No

3.3.2 Step 3b: Configure SIP Signaling Interfaces

This step describes how to configure SIP Interfaces. For the interoperability test topology, an internal (Genesys) and 2 external SIP Interfaces (one for the ITSP and one for Remote Agents, discussed later) are configured for the SBC.

➢ **To configure a SIP Interface:**

1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
2. Configure a SIP interface for the LAN:

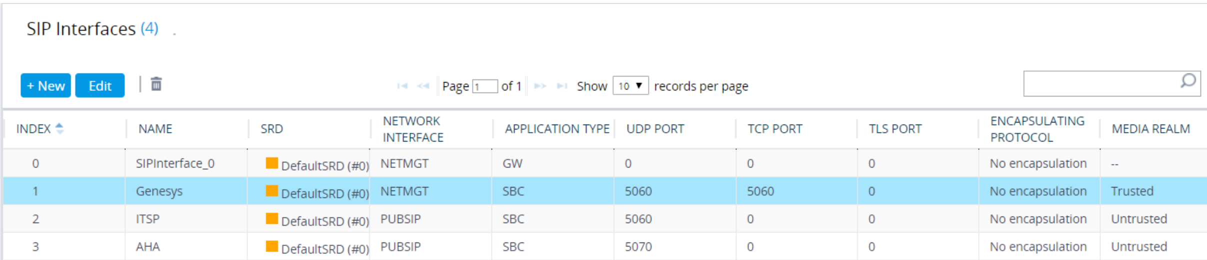
Parameter	Value
Index	**1**
Interface Name	**Genesys** (arbitrary descriptive name)
Network Interface	**NETMGT**
Application Type	**SBC**
UDP	**5060**
SRD	**DefaultSRD**

3. Configure a SIP interface for the WAN:

Parameter	Value
Index	**2**
Interface Name	**ITSP** (arbitrary descriptive name)
Network Interface	**Untrusted**
Application Type	**SBC**
UDP	**5060**
SRD	**DefaultSRD**

The configured SIP Interfaces are shown in the figure below. SIPInterface_0 is a default SIP interface that is not used.

Figure 3-16: Configured SIP Interfaces in SIP Interface Table


SIP Interfaces (4)

+ New Edit Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATING PROTOCOL	MEDIA REALM
0	SIPInterface_0	DefaultSRD (#0)	NETMGT	GW	0	0	0	No encapsulation	--
1	Genesys	DefaultSRD (#0)	NETMGT	SBC	5060	5060	0	No encapsulation	Trusted
2	ITSP	DefaultSRD (#0)	PUBSIP	SBC	5060	0	0	No encapsulation	Untrusted
3	AHA	DefaultSRD (#0)	PUBSIP	SBC	5070	0	0	No encapsulation	Untrusted

3.4 Step 4: Configure Proxy Sets

This step 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 must be configured for the following IP entities:

- Genesys Contact Center SIP Server
- ITSP SIP Trunk

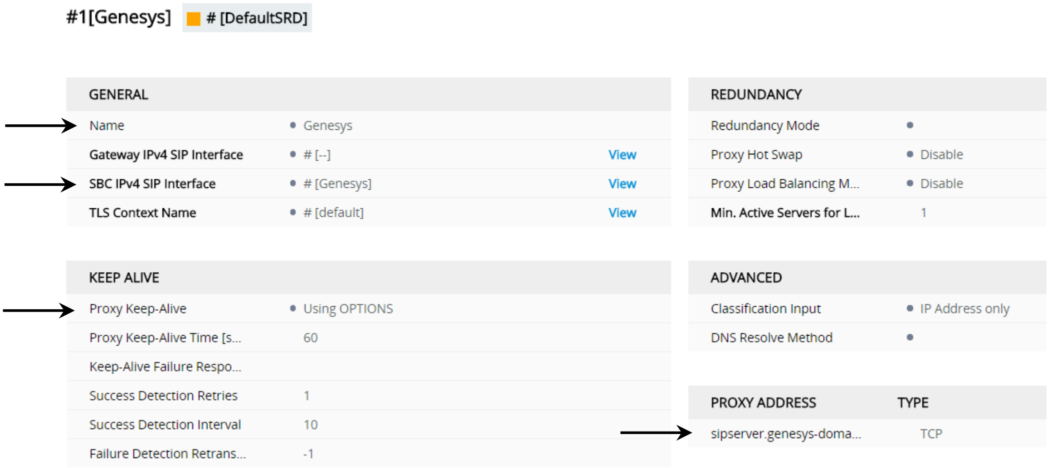
These Proxy Sets will later be associated with IP Groups.

➢ **To configure Proxy Sets:**

1. Open the Proxy Sets Table page (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Configure a Proxy Set for the Genesys Contact Center:

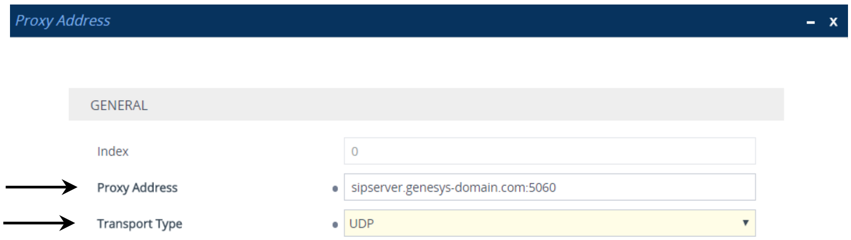
Parameter	Value
Proxy Set ID	**1**
SRD	**DefaultSRD**
Name	**Genesys**
SBC IPv4 SIP Interface	**Genesys**
Proxy Keep Alive	**Using OPTIONs**
Proxy Address	**sipserver.genesys-domain.com:5060** Genesys Contact Center IP address / FQDN and destination port.
Transport Type	**UDP**

Figure 3-17: Configure Proxy Set for Genesys Contact Center SIP Server



3. While positioned on the Proxy Set index, select the Proxy Address Table link at the bottom of the page and configure the address / FQDN for the proxy. Open the Proxy Sets Table page (**Setup** tab > **Signaling&Media** tab > **Core Entities** folder > **Proxy Sets**), position on index, select **Proxy Address** link, and then select **Add**).

Figure 3-18: Proxy Address Table - Add Row



4. Repeat Steps 1-3 for the ITSP Proxy Set.

Parameter	Value
Proxy Set ID	**2**
SRD	**DefaultSRD**
Name	**ITSP (arbitrary)**
SBC IPv4 SIP Interface	**ITSP**
Proxy Keep Alive	**Using OPTIONs**
Proxy Address	**gw0.itsp-iot.com:5060** ITSP IP address / FQDN and destination port.
Transport Type	**UDP**

Figure 3-19: Configure Proxy Set for ITSP SIP Trunk

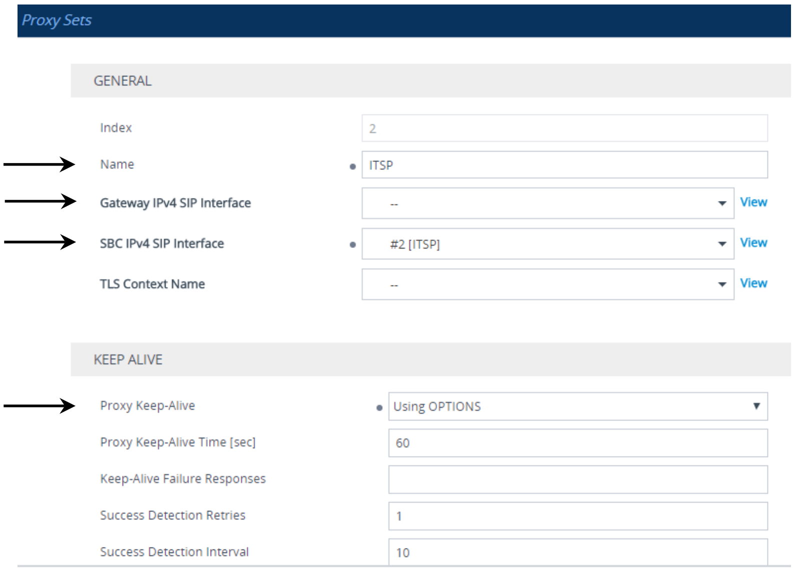
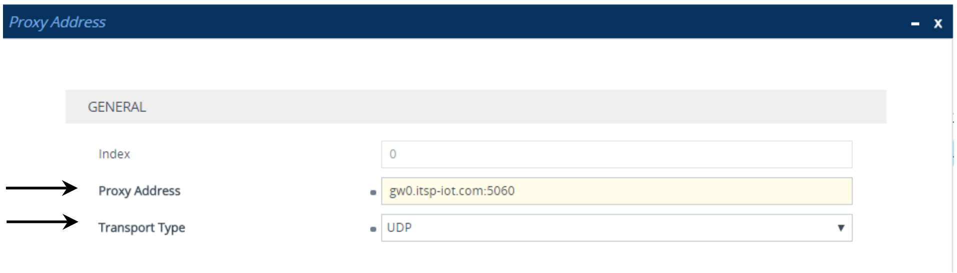


Figure 3-20: Configure Proxy Set for ITSP SIP Trunk – Add Row



3.5 Step 5: Configure IP Groups

This step 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 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. A typical deployment consists of multiple IP Groups associated with the same SRD. For example, you can have a LAN IP PBXs sharing the same SRD, with an ITSP / SIP Trunk and a User group. Once IP Groups are configured, they are used to configure IP-to-IP routing rules for denoting the source and destination of the call.

In the interoperability test topology, IP Groups were configured for the following IP entities:

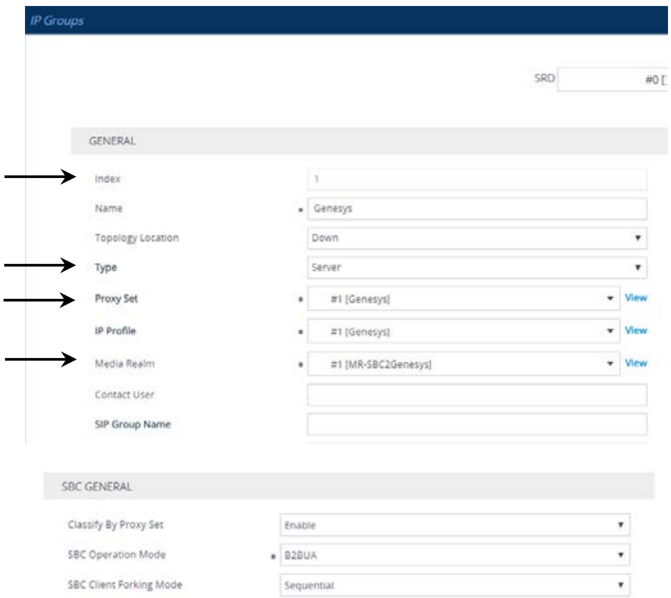
- Genesys Contact Center located on LAN (Server Group)
- ITSP SIP Trunk located on WAN (Server Group)
- Remote User Agents located in the WAN (User Group) (see Section 3.10 on page 39)

➢ **To configure IP Groups:**

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

Parameter	Value
Index	**1**
Type	**Server**
Description	**Genesys** (arbitrary descriptive name)
Proxy Set ID	**Genesys**
SRD	**DefaultSRD**
Media Realm Name	**MR1-SBC2Genesys**
IP Profile ID	**Genesys**

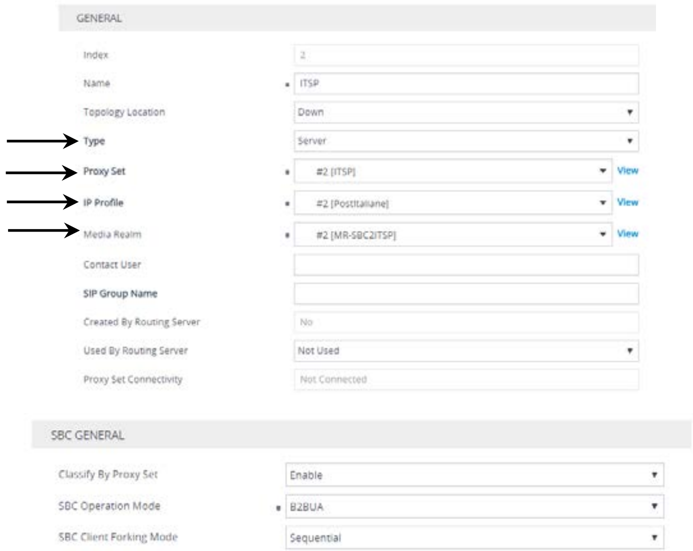
Figure 3-21: Configure an IP Group for the Genesys Call Center



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

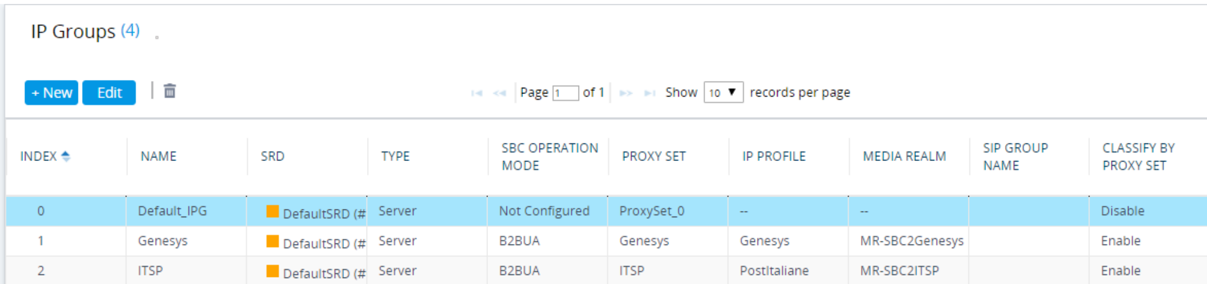
Parameter	Value
Index	**2**
Type	**Server**
Description	**ITSP** (arbitrary descriptive name)
Proxy Set ID	**ITSP**
SRD	**DefaultSRD**
Media Realm Name	**MR2-SBC2ITSP**
IP Profile ID	**ITSP**

Figure 3-22: Configure an IP Group for the ITSP SIP Trunk (Common Tab)



The configured IP Groups are shown in the figure below:

Figure 3-23: Configured IP Groups in IP Group Table


IP Groups (4)

+ New Edit

Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET
0	Default_IPG	DefaultSRD (#	Server	Not Configured	ProxySet_0	--	--		Disable
1	Genesys	DefaultSRD (#	Server	B2BUA	Genesys	Genesys	MR-SBC2Genesys		Enable
2	ITSP	DefaultSRD (#	Server	B2BUA	ITSP	PostItaliane	MR-SBC2ITSP		Enable

3.6 Step 6: Configure IP Profiles

This step describes how to configure IP Profiles. In this interoperability test topology, 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 were configured for the following IP entities:

- Genesys Contact Center
- ITSP SIP trunk

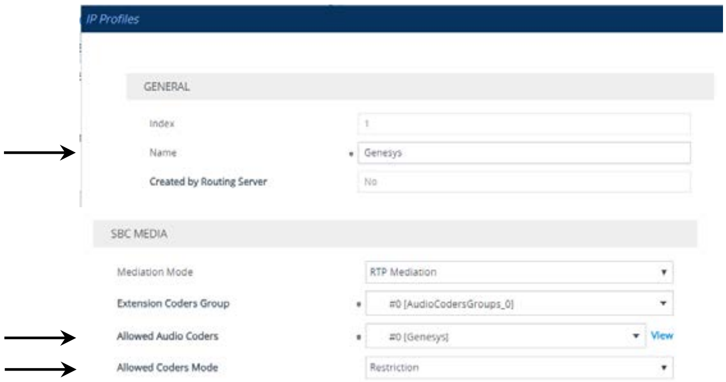
> **Note:** The IP Profile index values were assigned to the IP Groups in the previous step (see Section 3.5 on page 29).

➢ **To configure IP Profiles:**

1. Open the IP Profile Settings page (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles** table).
2. Click **New**.
3. Configure the parameters as follows:

Parameter	Value
Index	**1**
Profile Name	**Genesys SIP Server** (arbitrary descriptive name)
Allowed Coders Group ID	**'Coders Group 1'**
Extension Coders Group	**'AudioCodersGroup_0'**

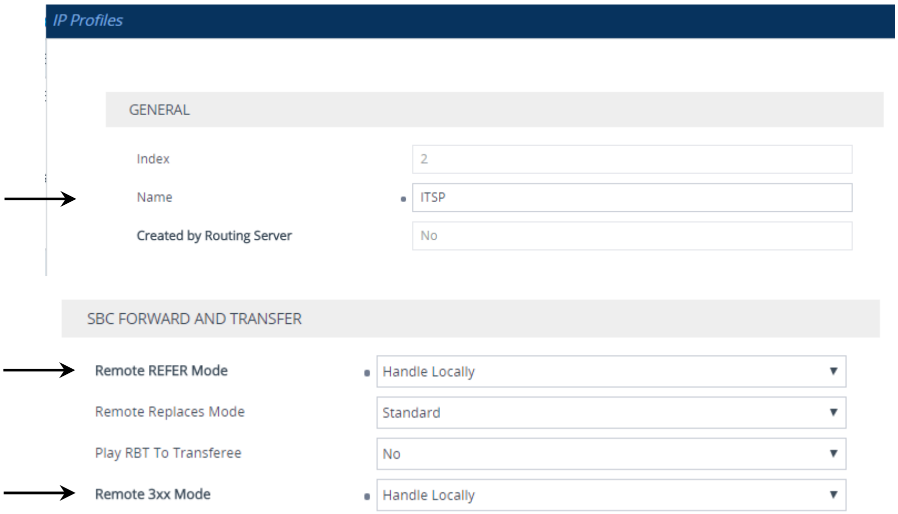
Figure 3-24: Configure IP Profile for Genesys Contact Center



4. Configure an IP Profile for the ITSP SIP Trunk:
   a. Click **New**.
   b. Configure the parameters as follows:

Parameter	Value
Index	**2**
Profile Name	**ITSP** (arbitrary descriptive name)
Remote REFER Behavior	**'Handle Locally'**
Remote Delayed Offer Support	'**Not Supported**': ItalTel does not support receiving INVITE without SDP. In this case, it is necessary to use an extended coders group to provide the SBC a set of coders that can be offered to the ITSP side.
Session Expires Mode (not supported by ItalTel; interoperability was completed with this parameter set to **Transparent**)	**'Transparent':** one of Remote Update Support or Remote Re-INVITE support must be supported to refresh the session (default). **'Not Supported':** If Remote UPDATE/Re-INVITE is '**Not Supported**', Session Expires Mode should also be made 'Not Supported'.
Remote 3xx Mode	**'Handle Locally'**
Extension Coders Group	**'AudioCodersGroup_0'**

Figure 3-25: Configure IP Profile for ITSP SIP Trunk



Note:

- Italtel does not Support SIP 302 Moved Temporarily.
- The SBC may handle the 302 Moved Temporarily locally; the 302 Moved Temporarily response from the SIP server is accepted by the SBC, and then the SBC sends an INVITE to the temporary external number via the ITSP SIP Trunk. Notify messages are passed to the SIP server to provide status on the pending connection. The call is anchored by the SBC.
- The 302 Moved Temporarily handling on the SBC is configured by setting *SBCRemote3xxBehavior* = 'handle locally' in the IP Profile for the ITSP IP Group, and by setting an IP2IP route for calls originating from the ITSP IP Group to trigger on 3xx/REFER and route to ITSP IP Group.

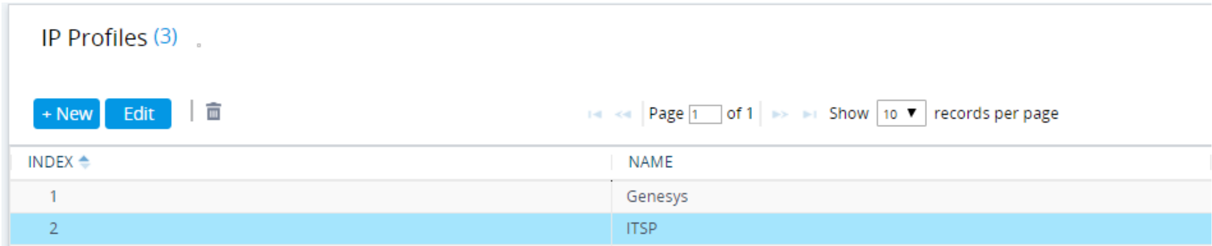
Note:

- The preferred method is that the SBC should be configured to handle the REFER locally. When the SBC receives the REFER, the SBC sends an INVITE to the new destination via the ITSP SIP Trunk or via the Genesys SIP server according to routing rules. Notify messages are passed to the SIP server to provide status on the pending connection. The call is anchored by the SBC.

  The REFER handling on the SBC is configured by setting *SBCRemote3xxBehavior* = 'handle locally' in the IP Profile for the ITSP IP Group, and by setting an IP2IP route for calls originating from the ITSP IP Group to trigger on 3xx/REFER and route to the ITSP IP Group.

The configured IP Groups are shown in the figure below:

Figure 3-26: Configured IP Profiles in IP Profile Table



3.7 Step 7: Configure Coders

This section shows how to configure an Allowed Coders Group to ensure that voice sent to the ITSP SIP Trunk uses the preferred coders only. The Italtel SIP Trunk supports G G.711A-law and G.729 coders. The Genesys Contact Center supports G.729, G.711A-law, G.711U-law, G.723 and GSM coders. Since both entities have common codecs supported, transcoding is not required. However, to ensure transcoding is not used, IP Profiles for both the ITSP and Genesys trunks are configured to use the same Allowed Coders Group ID (configured in previous section).

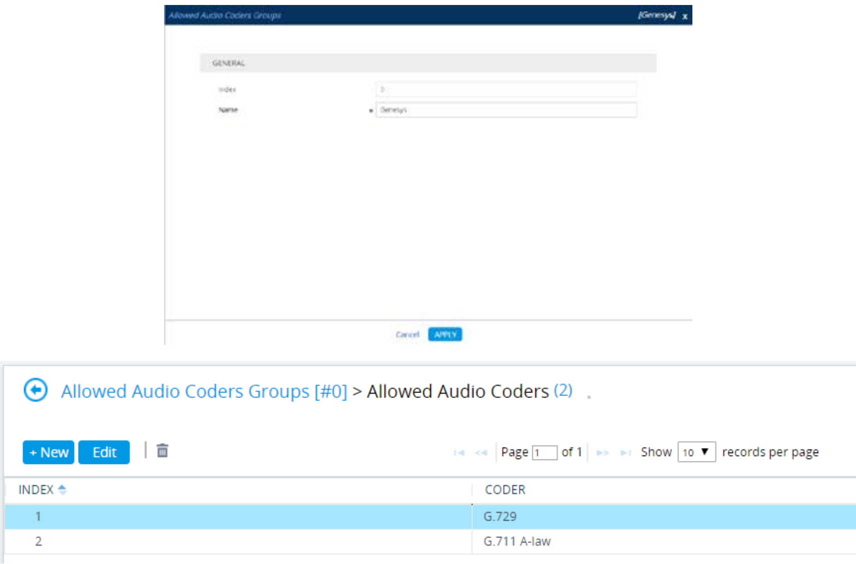
If support for different coders is required in the deployment, an SBC transcoding configuration is required (refer to the *SBC User's Manual*) for Coder Transcoding configuration.

➢ **To set a preferred coder for the ITSP & Genesys Trunk:**

1. Open the Allowed Coders Group page (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Allowed Audio Coders Groups**).
2. Configure an Allowed Coders Group as follows:

Parameter	Value
Allowed Coders Group ID	**1**
Coder Name	**G.729**
Coder Name	**G.711A-Law**

Figure 3-27: Configure an Allowed Coders Group



3. **Submit**
4. Repeat for Allowed Coders Group ID 2 (or set to use the same Allowed Audio Coders Group in the IP Profiles for the ITSP & SIP Server).

3.8 Step 8: Configure IP-to-IP Call Routing Rules

This step 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, it is compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 3.5 on page 29, IP Group 1 represents the Genesys Contact Center, and IP Group 2 represents the ITSP SIP Trunk.

For the interoperability test topology, the following IP-to-IP routing rules are configured to route calls between Genesys Contact Center (LAN) and ITSP SIP Trunk (WAN):

- Terminate SIP OPTIONS messages on the SBC that are received from the LAN/WAN
- Route calls from Genesys Contact Center to the ITSP SIP Trunk
- Calls from ITSP SIP Trunk to Genesys Contact Center
- Trigger rules for handling SIP 3xx/REFER for local agents and external DNs

➢ **To configure IP-to-IP routing rules:**

1. Open the IP-to-IP Routing Table page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. Configure the rules as below or per the required routing plan: (Note: routing associated with Remote Agents will be covered in the next section).

Parameter	Value
Index	**0**
Route Name	**OPTIONS termination** (arbitrary descriptive name)
Request Type	**OPTIONS**
Destination Type	**Dest Address**
Destination Address	**internal**

Parameter	Value
Index	**1**
Route Name	**3xx/Refer Trigger** (arbitrary descriptive name)
Source IP Group ID	**ITSP**
Call Trigger	**3xx or REFER**
ReRoute IP Group	**ITSP**
Destination Username Pattern	**0825* (example)**

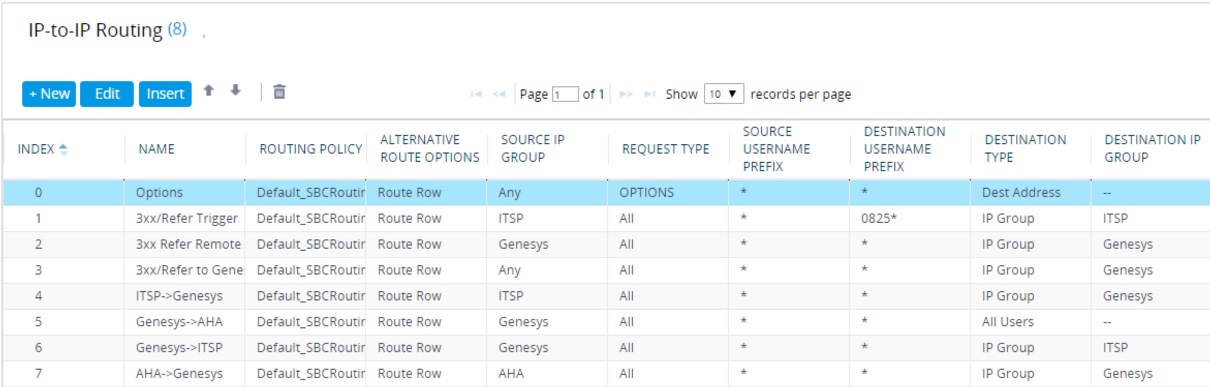
Parameter	Value
Index	**3**
Route Name	**3xx/Refer Trigger** (arbitrary descriptive name)

Source IP Group ID	**Genesys**
Call Trigger	**3xx or REFER**
ReRoute IP Group	**Genesys**

Parameter	Value
Index	**4**
Route Name	**ITSP2Genesys** (arbitrary descriptive name)
Source IP Group ID	**ITSP**
Destination Type	**IP Group**
Destination IP Group ID	**Genesys**

Parameter	Value
Index	**6**
Route Name	**Genesys2ITSP** (arbitrary descriptive name)
Source IP Group ID	**Genesys**
Destination Type	**IP Group**
Destination IP Group ID	**ITSP**

Figure 3-28: Configure IP-to-IP Routing Rules


IP-to-IP Routing (8)

+ New Edit Insert Page 1 of 1 Show 10 records per page

INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PREFIX	DESTINATION USERNAME PREFIX	DESTINATION TYPE	DESTINATION IP GROUP
0	Options	Default_SBCRoutir	Route Row	Any	OPTIONS	*	*	Dest Address	--
1	3xx/Refer Trigger	Default_SBCRoutir	Route Row	ITSP	All	*	0825*	IP Group	ITSP
2	3xx Refer Remote	Default_SBCRoutir	Route Row	Genesys	All	*	*	IP Group	Genesys
3	3xx/Refer to Gene	Default_SBCRoutir	Route Row	Any	All	*	*	IP Group	Genesys
4	ITSP->Genesys	Default_SBCRoutir	Route Row	ITSP	All	*	*	IP Group	Genesys
5	Genesys->AHA	Default_SBCRoutir	Route Row	Genesys	All	*	*	All Users	--
6	Genesys->ITSP	Default_SBCRoutir	Route Row	Genesys	All	*	*	IP Group	ITSP
7	AHA->Genesys	Default_SBCRoutir	Route Row	AHA	All	*	*	IP Group	Genesys

Note: The routing configuration may change according to your specific deployment topology, e.g., the deployment specification may indicate that OPTIONS termination should pass through the SBC to the far end, or, other criteria listed in the table may be used for determining routing.

3.9 Step 9: Configure IP-to-IP Manipulation Rules

This step describes how to configure IP-to-IP manipulation rules. These rules manipulate the source and / or destination number. The device supports SIP URI user part (source and destination) manipulations for inbound and outbound routing. The manipulation rules use the configured IP Groups to denote the source and destination of the call.

> **Note** The following manipulation rules are only examples. Adapt the manipulation table according to your environment dial plan.

Manipulations may be required to strip digits for an access code to the SBC from the Genesys SIP Server or for removing the country code and/or leading prefixes to map ITSP numbers to the DNs used in the Genesys environment.

➢ **To configure a number manipulation rule to remove the trunk access code from messages arriving from Genesys destined for the ITSP:**

1. Open the IP-to-IP Inbound Manipulation page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Manipulation** > **Inbound Manipulations**).
2. Click **Add**.
3. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	**1**
Manipulation Name (optional)	**remove access code**
Source IP Group ID	**Genesys**
Request Type	**All**
Manipulated URI	**Destination**

Figure 3-29: Configure IP-to-IP Inbound Manipulation Rule

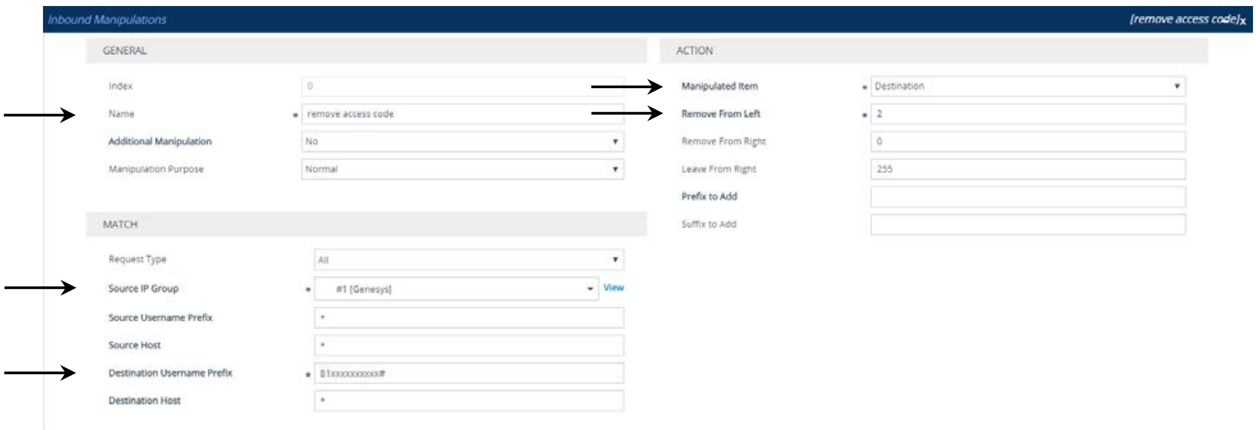
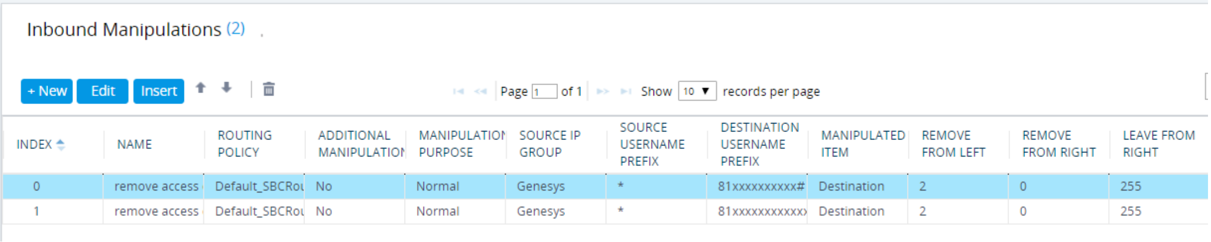


Figure 3-30: Example of Configured IP-to-IP Inbound Manipulation Rules


Inbound Manipulations (2)

+ New | Edit | Insert | Page 1 of 1 | Show 10 records per page

INDEX	NAME	ROUTING POLICY	ADDITIONAL MANIPULATION	MANIPULATION PURPOSE	SOURCE IP GROUP	SOURCE USERNAME PREFIX	DESTINATION USERNAME PREFIX	MANIPULATED ITEM	REMOVE FROM LEFT	REMOVE FROM RIGHT	LEAVE FROM RIGHT
0	remove access	Default_SBCRou	No	Normal	Genesys	*	81xxxxxxxxxx#	Destination	2	0	255
1	remove access	Default_SBCRou	No	Normal	Genesys	*	81xxxxxxxxxxx	Destination	2	0	255

3.10 Step 10: Perform SIP Header Message Manipulations

This step describes the SBC configuration for SIP Message Header Manipulations. A Message Manipulation rule defines a manipulation sequence for SIP messages. SIP message manipulation enables the normalization of SIP messaging fields between communicating network segments. For example, this functionality allows ITSPs to design policies on the SIP messaging fields that must be present before a SIP call enters the ITSP network. Similarly, the enterprise may have policies for the information that can enter or leave its network for policy and security reasons from an ITSP.

Each Message Manipulation rule is configured with a Manipulation Set ID. Sets of manipulation rules are created by assigning each of the relevant Message Manipulation rules to the same Manipulation Set ID. The Manipulation Set ID is used to assign the rules to the specific calls by designating that set ID in the preferred IP Group table. Message rules can be applied pre- (inbound manipulation) or post-classification (outbound manipulation).

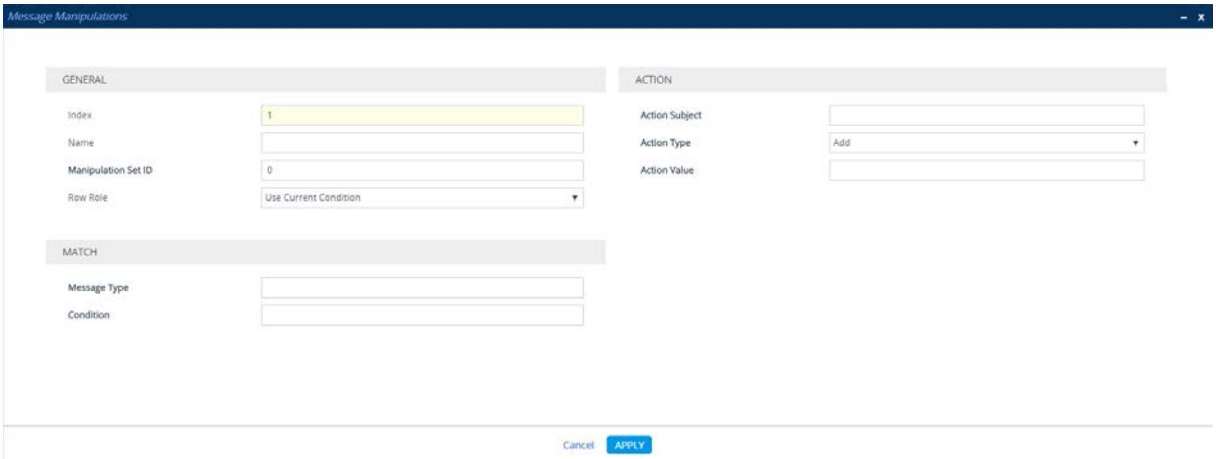
For this interoperability test, message manipulations were applied only to the outbound messages, to the ITSP SIP trunk, for the purposes of modifying existing SIP headers, topology hiding, and adding new SIP headers.

The following procedure generically describes how to configure Message Manipulation rules in the Web interface of the SBC.

➢ **To configure SIP Message Manipulation rules:**

1. Open the IP-to-IP Inbound Manipulation page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).
2. Click **Add**; this screen opens:

Figure 3-38: Configure IP-to-IP Message Manipulation Rule



3. Configure a Message Manipulation rule according to the parameters described in the table below.
4. Click **Submit** and then save (“burn”) your settings to flash memory.

The table below shows the message manipulation used in the interoperability test scenario.

Figure 3-38: Message Manipulation

[MessageManipulations]

Index	Manipulation Name	Man Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
0	modify outbound Request-URI	5	Any		header.request-uri.url.host	2 (Modify)	'posteitaliane.it'	0 (Use Current Condition)
1	Normalize outbound Request-URI	5	Invite		header.request-uri	7 (Normalize)		0 (Use Current Condition)
2	modify from host (so as to keep the tag)	5	Invite		header.from.url.host	2 (Modify)	'telecomitalia.it'	0 (Use Current Condition)
3	modify outbound To host	5	Any		header.to.url.host	2 (Modify)	'telecomitalia.it'	0 (Use Current Condition)
4	modify PAI for REFERs	5	Any		header.p-asserted-identity	2 (Modify)	'<sip:0274557715@telecomitalia.it>'	0 (Use Current Condition)
5		5		header.Referred-By exists	header.contact.url.host	2 (Modify)	header.referred-by.url.host	0 (Use Current Condition)
6	contact host; must be 173.x	5			header.contact.url.host	2 (Modify)	'173.227.254.67'	0 (Use Current Condition)
7	add DH if does not exist	5		header.diversion ! exists	header.diversion	0 (Add)	'<tel: 0274557715@telecomitalia.it>;reason=unknown;counter=1;screen=no;privacy=off'	0 (Use Current Condition)
8	correct hostname on diversion header	5	Any		header.diversion.url.host	2 (Modify)	'telecomitalia.it'	0 (Use Current Condition)

The outbound manipulation rules are not applied for a particular IP Group until the Manipulation Set is assigned as an inbound or outbound manipulation set. In the interoperability test scenario, Manipulation Set 5 was applied to the ITSP IP Group.

3.11 Step 11: Configure Remote Agents

This step describes the SBC configuration for Remote User Agents. Remote Agent DNs are registered on the SBC or through the SBC to the Genesys SIP Server. In the interoperability testing scenario, the Remote Agents are configured on a new Signaling Routing Domain over an existing untrusted interface.

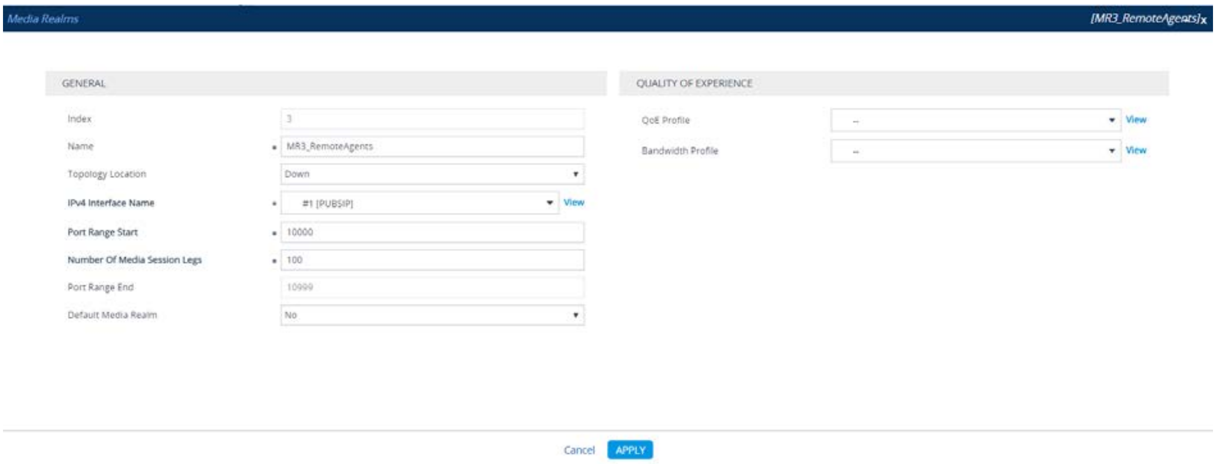
3.11.1 Step 11a: Configure Media Realm for a Remote Agent

This step describes how to configure Media Realms for a Remote Agent. Remote Agents interact with the SBC over the untrusted interface. Use the Media Realm table to designate the media port range that will be associated with the Remote Agents.

➢ **To configure the Media Realm for a Remote Agent:**

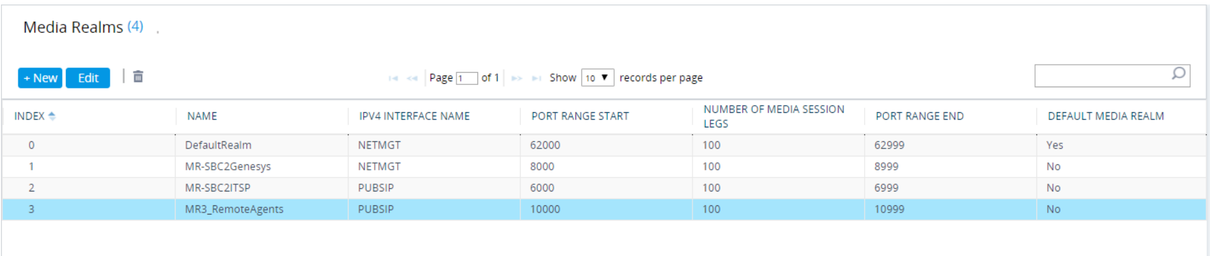
1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).

Figure 3-31: Configure a Remote Agent Media Realm



The figure below shows an example of a configured Media Realm Table including the Media Realm for Remote Agents.

Figure 3-32: Configure a Remote Agent Media Realm



INDEX	NAME	IPV4 INTERFACE NAME	PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	PORT RANGE END	DEFAULT MEDIA REALM
0	DefaultRealm	NETMGT	62000	100	62999	Yes
1	MR-SBC2Genesys	NETMGT	8000	100	8999	No
2	MR-SBC2ITSP	PUBSIP	6000	100	6999	No
3	MR3_RemoteAgents	PUBSIP	10000	100	10999	No

3.11.2 Step 11b: Configure SIP Signaling Interfaces for Remote Agents

This step describes how to create a new SIP Signaling interface on the Untrusted Network Interface for the Remote Agents.

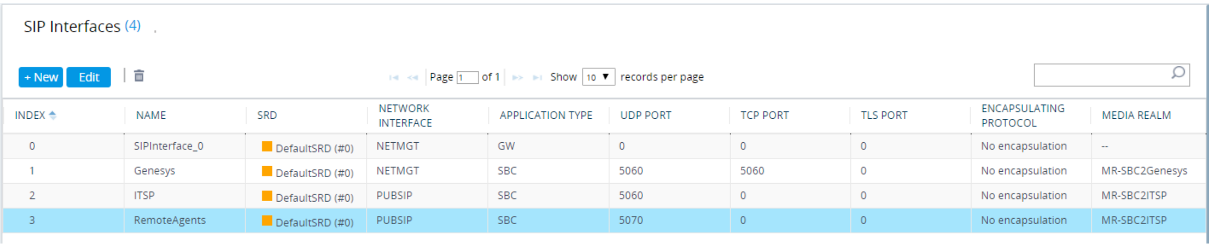
➢ **To configure SIP interfaces for a Remote Agent:**

1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**)
2. Configure a SIP interface for the LAN:

Parameter	Value
Index	**3**
Interface Name	**RemoteAgents** (arbitrary descriptive name)
Network Interface	**PUBSIP**
Application Type	**SBC**
UDP	**5070**
SRD	**DefaultSRD**

The configured SIP Interfaces Table, including the Remote Agents, is shown in the figure below:

Figure 3-33: Configured SIP Interfaces for Remote Agents in SIP Interface Table


SIP Interfaces (4)

+ New Edit

Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATING PROTOCOL	MEDIA REALM
0	SIPInterface_0	DefaultSRD (#0)	NETMGT	GW	0	0	0	No encapsulation	--
1	Genesys	DefaultSRD (#0)	NETMGT	SBC	5060	5060	0	No encapsulation	MR-SBC2Genesys
2	ITSP	DefaultSRD (#0)	PUBSIP	SBC	5060	0	0	No encapsulation	MR-SBC2ITSP
3	RemoteAgents	DefaultSRD (#0)	PUBSIP	SBC	5070	0	0	No encapsulation	MR-SBC2ITSP

3.11.3 Step 11c: Configure Remote (User) Agents IP Group

This step describes how to configure remote (User) agents IP Group. In the interoperability test topology, an IP User Group was configured for Remote (User) Agents registering from the WAN.

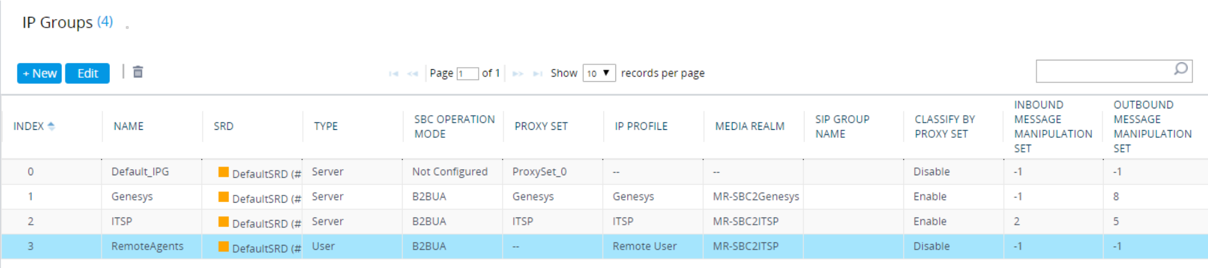
➢ **To configure an IP User Group:**

1. Open the IP Group Table page (**Setup** tab > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Configure an IP Group for the Remote Agents as follows:

Parameter	Value
Index	**3**
Type	**User**
Description	**Remote Agents** (arbitrary descriptive name)
SRD	**DefaultSRD**
Media Realm Name	**MR3-RemoteAgents**
IP Profile ID	**MR3-RemoteAgents**

The configured IP Groups are shown in the figure below:

Figure 3-34: Configured IP Group for Remote Users in IP Group Table



IP Groups (4)

+ New Edit Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATION SET	OUTBOUND MESSAGE MANIPULATION SET
0	Default_IPG	DefaultSRD (#	Server	Not Configured	ProxySet_0	--	--		Disable	-1	-1
1	Genesys	DefaultSRD (#	Server	B2BUA	Genesys	Genesys	MR-SBC2Genesys		Enable	-1	8
2	ITSP	DefaultSRD (#	Server	B2BUA	ITSP	ITSP	MR-SBC2ITSP		Enable	2	5
3	RemoteAgents	DefaultSRD (#	User	B2BUA	--	Remote User	MR-SBC2ITSP		Disable	-1	-1

3.11.4 Step 11d: Configure IP Profiles for Remote Agents

This step describes how to configure IP Profiles for the Remote (User) Agents.

> **Note:** The IP Profile index values were assigned to the IP Groups in the previous step (see Section 3.5 on page 29).

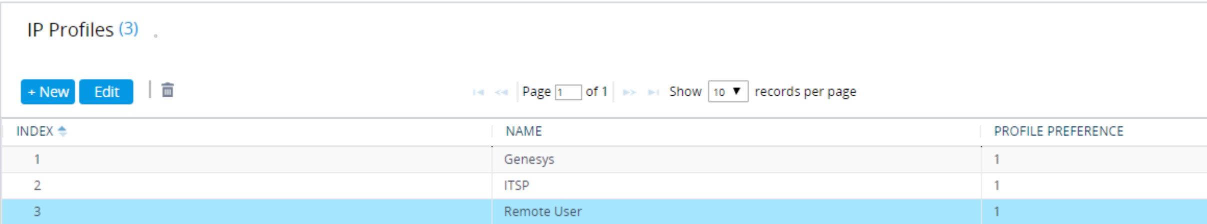
➢ **To configure IP Profile for the Remote (User) Agent:**

1. Open the IP Profile Settings page (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).

> **Note:** Presently, no parameters require configuration on the **SBC** tab for the Remote Agents IP Profile. All parameters are set to their default values. The IP Profile is created for the purpose of future configuration only.

The configured IP Remote Agent Groups are shown in the figure below:

Figure 3-35: Configured IP Profiles in IP Profile Table



3.11.5 Step 11e: Configure Classification Table for Remote Agents

This step describes how to configure the Classification table for Remote Agents. The Classification rules classify incoming SIP dialog-initiating requests to an IP Group from where the SIP dialog request was received. The identified IP Group is then used in the manipulation and routing processes. For Remote Users arriving on an interface with multiple IP Groups, the classification rules will determine the origination IP Group.

➢ **To configure IP Profile for the Remote (User) Agent:**

1. Open the Classification Table page (**Setup** menu **> Signaling & Media** tab **> SBC** folder **> Classification**).
2. Configure the parameters as follows:

Parameter	Value
Index	**1**
Classification Name	**Remote Users** (arbitrary descriptive name)
Source SIP Interface	**RemoteAgents**
Source IP Group ID	**Remote Agents**
Action Type	**Allow**

Figure 3-36: Configure Rule Tab of the Classification Table

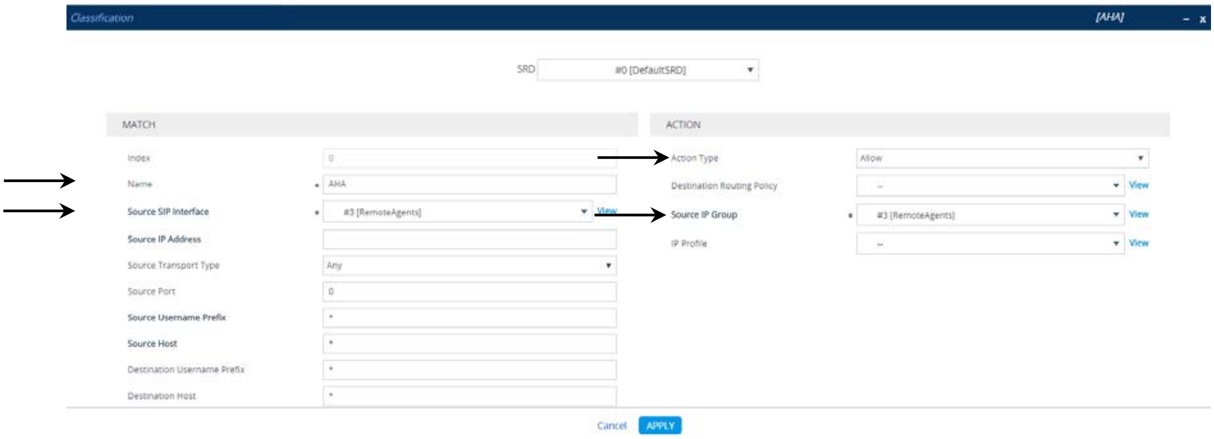
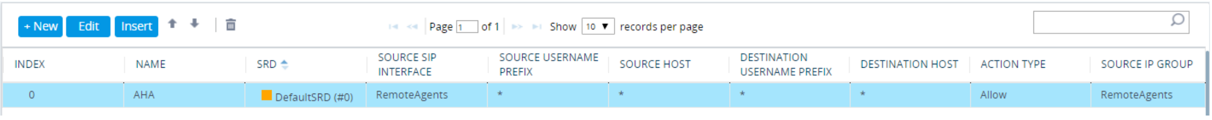


Figure 3-37: Configured Classification Rule for Remote (Users) Agents



INDEX	NAME	SRD	SOURCE SIP INTERFACE	SOURCE USERNAME PREFIX	SOURCE HOST	DESTINATION USERNAME PREFIX	DESTINATION HOST	ACTION TYPE	SOURCE IP GROUP
0	AHA	DefaultSRD (#0)	RemoteAgents	*	*	*	*	Allow	RemoteAgents

3.11.6 Step 11f: Configure IP-to-IP Call Routing Rules for Remote (User) Agent

This step describes how to configure additional IP-to-IP call routing rules that are required for routing calls between the Remote Users (classified to a particular IP Group via the Classification table in Section 3.11.5 on page 44) and the Genesys SIP Server.

The following IP-to-IP call routing rules were configured (see Section 3.8 on page 35):

- Terminate SIP OPTIONS messages on the SBC that are received from the LAN
- Calls from Genesys Contact Center to ITSP SIP Trunk
- Calls from ITSP SIP Trunk to Genesys Contact Center
- Trigger rules for handling SIP 3xx/REFER for local agents and external DNs

For the interoperability test topology, IP-to-IP routing rules were configured to route SIP messages between the Remote (User) Agents and the Genesys SIP Server, and to ensure that the messages are routed back to the correct user group to reach the intended agent.

➢ **To configure IP-to-IP routing rules:**

1. Open the IP-to-IP Routing Table page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. Configure a rule to route between the Remote Agent and the Genesys SIP Server as follows:

Parameter	Value
Index	**10**
Route Name	**Genesys->AHA** (arbitrary descriptive name)
Source IP Group ID	**Genesys**
Destination Type	**All Users**

Parameter	Value
Index	**6**
Route Name	**AHA->Genesys**
Source IP Group ID	**RemoteAgents**
Destination Type	**IP Group**
Destination IP Group ID	**Genesys**

The configured IP-to-IP routing rules including rules for Remote Agents are shown in the figure below.

Figure 3-38: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

IP-to-IP Routing (8)

+ New | Edit | Insert | Page 1 of 1 | Show 10 records per page

INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PREFIX	DESTINATION USERNAME PREFIX	DESTINATION TYPE	DESTINATION IP GROUP
0	Options	Default_SBCRoutir	Route Row	Any	OPTIONS	*	*	Dest Address	--
1	3xx/Refer Trigger	Default_SBCRoutir	Route Row	ITSP	All	*	0825*	IP Group	ITSP
2	3xx Refer Remote	Default_SBCRoutir	Route Row	Genesys	All	*	*	IP Group	Genesys
3	3xx/Refer to Gene	Default_SBCRoutir	Route Row	Any	All	*	*	IP Group	Genesys
4	ITSP->Genesys	Default_SBCRoutir	Route Row	ITSP	All	*	*	IP Group	Genesys
5	Genesys->AHA	Default_SBCRoutir	Route Row	Genesys	All	*	*	All Users	--
6	Genesys->ITSP	Default_SBCRoutir	Alternative Route I	Genesys	All	*	*	IP Group	ITSP
7	AHA->Genesys	Default_SBCRoutir	Route Row	RemoteAgents	All	*	*	IP Group	Genesys

Note: The routing configuration may change according to your specific deployment topology. For example, the deployment specification may indicate a particular set of numbers that should be routed to the User group; however, a particular deployment may handle the routing of Remote Agents over a different trunk from the Genesys SIP Server or may require the use of other criteria/filters in the routing table.

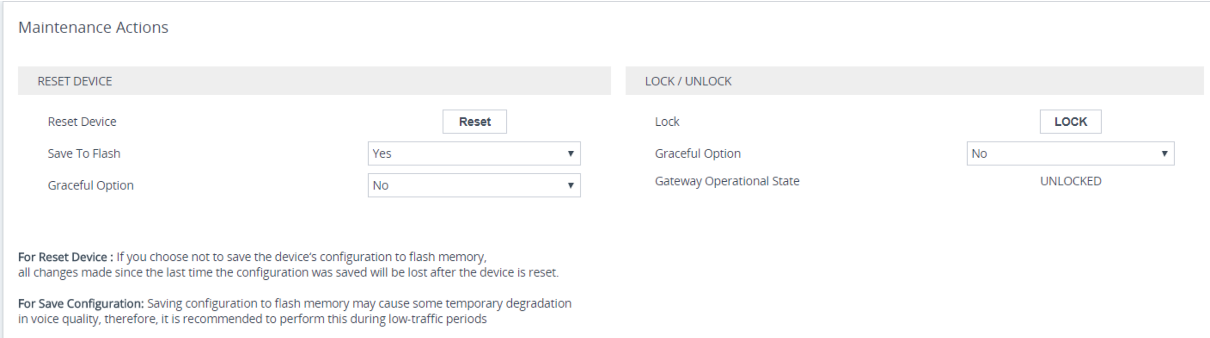
3.12 Step 12: Reset the SBC

After completing the configuration of the SBC, save ("burn") the configuration to the SBC's flash memory with a reset for the settings to take effect.

➢ **To save the configuration to flash memory and reset the device:**

1. Click the Reset button on the top right of the web GUI page.

Figure 3-39: Resetting the SBC



2. Make sure that the Save to FLASH' field is set to **Yes** (default).
3. Click the **Reset** button.

A AudioCodes *ini* File

This appendix shows the *ini* configuration file of the SBC, corresponding to the Web-based configuration described in Section 3 on page 15.

Note: To load and save an *ini* file, use the Configuration File page (**Maintenance** tab > **Software Update** menu > **Configuration File**).

```
;**************
;** Ini File **
;**************

;Board: M500
;HW Board Type: 69 FK Board Type: 76
;Serial Number: 6486615
;Product Key: r6wmr5to25sibANud21Vu6R162MFcNBMb2x3ehcs
;Slot Number: 1
;Software Version: 7.20A.158.012
;DSP Software Version: 5014AE3_R => 721.09
;Board IP Address: 10.38.5.116
;Board Subnet Mask: 255.255.255.0
;Board Default Gateway: 10.38.5.1
;Ram size: 512M Flash size: 64M Core speed: 500Mhz
;Num of DSP Cores: 3 Num DSP Channels: 177
;Num of physical LAN ports: 12
;Profile: NONE
;;;Key features:;Board Type: M500 ;Coders: G723 G729 G728 NETCODER GSM-FR
GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-WB G722 EG711 MS_RTA_NB
MS_RTA_WB SILK_NB SILK_WB SPEEX_NB SPEEX_WB OPUS_NB OPUS_WB ;Channel Type:
DspCh=500 IPMediaDspCh=500 ;IP Media: VoicePromptAnnounc(H248.9) ;DSP Voice
features: IpmDetector RTCP-XR ;QOE features: VoiceQualityMonitoring
MediaEnhancement ;DATA features: ;Security: IPSEC MediaEncryption
StrongEncryption EncryptControlProtocol ;E1Trunks=1 ;T1Trunks=1
;FXSPorts=12 ;FXOPorts=12 ;Control Protocols: CLI TRANSCODING=50 FEU=150
TestCall=30 CODER-TRANSCODING=50 EMS SBC-SIGNALING=150 SBC-MEDIA=150 MGCP
SIP SBC=150 ;Default features:;Coders: G711 G726;

;------ HW components------
;
; Slot # : Module type : # of ports
;----------------------------------------------
; 1 : Empty
; 2 : Empty
; 3 : Empty
;----------------------------------------------


[SYSTEM Params]

SyslogServerIP = 10.38.105.2
EnableSyslog = 1
;NTPServerIP_abs is hidden but has non-default value
NTPServerUTCOffset = -18000
```

```
ENABLEPARAMETERSMONITORING = 1
ActivityListToLog = 'pvc', 'afl', 'dr', 'fb', 'swu', 'naa', 'spc', 'll',
'cli', 'ae'
DebugRecordingDestIP = 10.38.105.2
;VpFileLastUpdateTime is hidden but has non-default value
DayLightSavingTimeStart = '03:SUN/02:02:00'
DayLightSavingTimeEnd = '11:SUN/01:02:00'
DayLightSavingTimeEnable = 1
TR069ACSPASSWORD = '$1$gQ=='
TR069CONNECTIONREQUESTPASSWORD = '$1$gQ=='
NTPServerIP = '10.38.5.73'
;LastConfigChangeTime is hidden but has non-default value
;BarrierFilename is hidden but has non-default value
;PM_gwINVITEDialogs is hidden but has non-default value
;PM_gwSUBSCRIBEDialogs is hidden but has non-default value
;PM_gwSBCRegisteredUsers is hidden but has non-default value
;PM_gwSBCMediaLegs is hidden but has non-default value
;PM_gwSBCTranscodingSessions is hidden but has non-default value

[BSP Params]

PCMLawSelect = 3
UdpPortSpacing = 10
ProductKey = 'r6wmr5to25sibANud21Vu6R162MFcNBMb2x3ehcs'
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[Analog Params]


[ControlProtocols Params]

AdminStateLockControl = 0
QOEServerIp = 10.38.5.73
QOEInterfaceName = 'NETMGT'

[MGCP Params]


[MEGACO Params]


[PSTN Params]


[SS7 Params]


[Voice Engine Params]

BrokenConnectionEventTimeout = 3000
NatMode = 3
PrerecordedTonesFileName = 'prerecordedtones_voiperfect_new.dat'
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

LogoWidth = '145'
;HTTPSPkeyFileName is hidden but has non-default value
;HTTPSCertFileName is hidden but has non-default value
```

```
[SIP Params]

MEDIACHANNELS = 500
GWDEBUGLEVEL = 5
USERINFOFILENAME = 'userinfo.txt'
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value

[IPsec Params]


[SNMP Params]

SNMPManagerIsUsed_0 = 1
SNMPManagerIsUsed_1 = 0
SNMPManagerIsUsed_2 = 0
SNMPManagerIsUsed_3 = 0
SNMPManagerIsUsed_4 = 0
SNMPManagerTableIP_0 = 10.38.5.73
SNMPManagerTableIP_1 = 0.0.0.0
SNMPManagerTableIP_2 = 0.0.0.0
SNMPManagerTableIP_3 = 0.0.0.0
SNMPManagerTableIP_4 = 0.0.0.0

[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_SpeedDuplex,
PhysicalPortsTable_PortDescription, PhysicalPortsTable_GroupMember,
PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_1", 1, 4, "User Port #0", "GROUP_1", "Active";
PhysicalPortsTable 1 = "GE_2", 1, 4, "User Port #1", "GROUP_2", "Active";
PhysicalPortsTable 2 = "GE_4_3", 0, 4, "User Port #2", "None", " ";
PhysicalPortsTable 3 = "GE_4_4", 0, 4, "User Port #3", "None", " ";
PhysicalPortsTable 4 = "FE_5_1", 0, 4, "User Port #4", "None", " ";
PhysicalPortsTable 5 = "FE_5_2", 0, 4, "User Port #5", "None", " ";
PhysicalPortsTable 6 = "FE_5_3", 0, 4, "User Port #6", "None", " ";
PhysicalPortsTable 7 = "FE_5_4", 0, 4, "User Port #7", "None", " ";
PhysicalPortsTable 8 = "FE_5_5", 0, 4, "User Port #8", "None", " ";
PhysicalPortsTable 9 = "FE_5_6", 0, 4, "User Port #9", "None", " ";
PhysicalPortsTable 10 = "FE_5_7", 0, 4, "User Port #10", "None", " ";
PhysicalPortsTable 11 = "FE_5_8", 0, 4, "User Port #11", "None", " ";

[ \PhysicalPortsTable ]


[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group, EtherGroupTable_Mode,
EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 1, "GE_1", "";
EtherGroupTable 1 = "GROUP_2", 1, "GE_2", "";
EtherGroupTable 2 = "GROUP_3", 0, "", "";
EtherGroupTable 3 = "GROUP_4", 0, "", "";
EtherGroupTable 4 = "GROUP_5", 0, "", "";
EtherGroupTable 5 = "GROUP_6", 0, "", "";
```

```
EtherGroupTable 6 = "GROUP_7", 0, "", "";
EtherGroupTable 7 = "GROUP_8", 0, "", "";
EtherGroupTable 8 = "GROUP_9", 0, "", "";
EtherGroupTable 9 = "GROUP_10", 0, "", "";
EtherGroupTable 10 = "GROUP_11", 0, "", "";
EtherGroupTable 11 = "GROUP_12", 0, "", "";

[ \EtherGroupTable ]


[ DeviceTable ]

FORMAT DeviceTable_Index = DeviceTable_VlanID,
DeviceTable_UnderlyingInterface, DeviceTable_DeviceName,
DeviceTable_Tagging, DeviceTable_MTU;
DeviceTable 0 = 1, "GROUP_1", "Trusted", 0, 1500;
DeviceTable 1 = 254, "GROUP_2", "Untrusted", 0, 1500;

[ \DeviceTable ]


[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.38.5.116, 24, 10.38.5.1, "NETMGT", 0.0.0.0,
0.0.0.0, "Trusted";
InterfaceTable 1 = 5, 10, 173.227.254.67, 26, 173.227.254.66, "PUBSIP",
8.8.4.4, 8.8.8.8, "Untrusted";

[ \InterfaceTable ]


[ ACCESSLIST ]

FORMAT ACCESSLIST_Index = ACCESSLIST_Source_IP, ACCESSLIST_Source_Port,
ACCESSLIST_PrefixLen, ACCESSLIST_Start_Port, ACCESSLIST_End_Port,
ACCESSLIST_Protocol, ACCESSLIST_Use_Specific_Interface,
ACCESSLIST_Interface_ID, ACCESSLIST_Packet_Size, ACCESSLIST_Byte_Rate,
ACCESSLIST_Byte_Burst, ACCESSLIST_Allow_type_enum;
ACCESSLIST 0 = "138.132.106.209", 0, 32, 0, 65535, "Any", 1, "PUBSIP", 0,
0, 0, 0;
ACCESSLIST 1 = "71.65.240.156", 0, 32, 0, 65535, "Any", 1, "PUBSIP", 0, 0,
0, 0;
ACCESSLIST 2 = "138.132.106.209", 0, 32, 0, 65535, "icmp", 1, "PUBSIP", 0,
0, 0, 0;
ACCESSLIST 3 = "138.132.106.211", 0, 32, 0, 65535, "Any", 1, "PUBSIP", 0,
0, 0, 0;
ACCESSLIST 4 = "0.0.0.0", 0, 0, 0, 65535, "Any", 1, "PUBSIP", 0, 0, 0, 1;

[ \ACCESSLIST ]


[ WelcomeMessage ]

FORMAT WelcomeMessage_Index = WelcomeMessage_Text;
```

```
WelcomeMessage 1 = "***************************************************";
WelcomeMessage 2 = "** This SBC is being used for Posteitalianie IOT **";
WelcomeMessage 3 = "** Please do not make changes to this device **";
WelcomeMessage 4 = "** Contact: Leo Mallol 919.287.3491 **";
WelcomeMessage 5 = "** **";
WelcomeMessage 6 = "** Version: 7.20A.158.009 **";
WelcomeMessage 7 = "** Public IP Address: 173.227.254.67 **";
WelcomeMessage 8 = "***************************************************";

[ \WelcomeMessage ]


[ WebUsers ]

FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password,
WebUsers_Status, WebUsers_PwAgeInterval, WebUsers_SessionLimit,
WebUsers_CliSessionLimit, WebUsers_SessionTimeout, WebUsers_BlockTime,
WebUsers_UserLevel, WebUsers_PwNonce, WebUsers_SSHPublicKey;
WebUsers 0 = "Admin",
"$1$FCJ0dCYpeC19JXwsfhcRF0ZARkUfERoYEklISB4HBQIEBwEBDlwIXAIFXA1deXdzInd0dCV
5en18enl3fmBjZ2E=", 1, 0, 2, -1, 15, 60, 200,
"4c2f2a78fb659495c1d088af73085f20", "";
WebUsers 1 = "User",
"$1$3Ovk7r6B1tXW0NfTgtmI3dzYjNaJlJSXysSUx5aezJvDmM3HzzA0YzRgMzU1PjloPDo5aGt
1I3R3IXchICAqIyo=", 1, 0, 2, -1, 15, 60, 50,
"c4a93bcd82e88f303f891540d2c9d5e2", "";

[ \WebUsers ]


[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_DTLSVersion, TLSContexts_ServerCipherString,
TLSContexts_ClientCipherString, TLSContexts_RequireStrictCert,
TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary,
TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse, TLSContexts_DHKeySize;
TLSContexts 0 = "default", 0, 0, "RC4:AES128", "DEFAULT", 0, 0, , , 2560,
0, 1024;

[ \TLSContexts ]


[ AudioCodersGroups ]

FORMAT AudioCodersGroups_Index = AudioCodersGroups_Name;
AudioCodersGroups 0 = "AudioCodersGroups_0";

[ \AudioCodersGroups ]


[ AllowedAudioCodersGroups ]

FORMAT AllowedAudioCodersGroups_Index = AllowedAudioCodersGroups_Name;
AllowedAudioCodersGroups 0 = "Genesys";

[ \AllowedAudioCodersGroups ]
```

```
[ IpProfile ]

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupName, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ,
IpProfile_RTPRedundancyDepth, IpProfile_CNGmode,
IpProfile_VxxTransportType, IpProfile_NSEMode, IpProfile_IsDTMFUsed,
IpProfile_PlayRBTone2IP, IpProfile_EnableEarlyMedia,
IpProfile_ProgressIndicator2IP, IpProfile_EnableEchoCanceller,
IpProfile_CopyDest2RedirectNumber, IpProfile_MediaSecurityBehaviour,
IpProfile_CallLimit, IpProfile_DisconnectOnBrokenConnection,
IpProfile_FirstTxDtmfOption, IpProfile_SecondTxDtmfOption,
IpProfile_RxDTMFOption, IpProfile_EnableHold, IpProfile_InputGain,
IpProfile_VoiceVolume, IpProfile_AddIEInSetup,
IpProfile_SBCExtensionCodersGroupName, IpProfile_MediaIPVersionPreference,
IpProfile_TranscodingMode, IpProfile_SBCAllowedMediaTypes,
IpProfile_SBCAllowedAudioCodersGroupName,
IpProfile_SBCAllowedVideoCodersGroupName, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCSendMultipleDTMFMethods,
IpProfile_SBCAssertIdentity, IpProfile_AMDSensitivityParameterSuit,
IpProfile_AMDSensitivityLevel, IpProfile_AMDMaxGreetingTime,
IpProfile_AMDMaxPostSilenceGreetingTime, IpProfile_SBCDiversionMode,
IpProfile_SBCHistoryInfoMode, IpProfile_EnableQSIGTunneling,
IpProfile_SBCFaxCodersGroupName, IpProfile_SBCFaxBehavior,
IpProfile_SBCFaxOfferMode, IpProfile_SBCFaxAnswerMode,
IpProfile_SbcPrackMode, IpProfile_SBCSessionExpiresMode,
IpProfile_SBCRemoteUpdateSupport, IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType,
IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI,
IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey,
IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource,
IpProfile_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone,
IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior,
IpProfile_SBCSDPPtimeAnswer, IpProfile_SBCPreferredPTime,
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,
IpProfile_SBCPlayRBTToTransferee, IpProfile_SBCRTCPMode,
IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection, IpProfile_JitterBufMaxDelay,
IpProfile_SBCUserBehindUdpNATRegistrationTime,
IpProfile_SBCUserBehindTcpNATRegistrationTime,
IpProfile_SBCSDPHandleRTCPAttribute,
IpProfile_SBCRemoveCryptoLifetimeInSDP, IpProfile_SBCIceMode,
IpProfile_SBCRTCPMux, IpProfile_SBCMediaSecurityMethod,
IpProfile_SBCHandleXDetect, IpProfile_SBCRTCPFeedback,
IpProfile_SBCRemoteRepresentationMode, IpProfile_SBCKeepVIAHeaders,
IpProfile_SBCKeepRoutingHeaders, IpProfile_SBCKeepUserAgentHeader,
IpProfile_SBCRemoteMultipleEarlyDialogs,
IpProfile_SBCRemoteMultipleAnswersMode, IpProfile_SBCDirectMediaTag,
IpProfile_SBCAdaptRFC2833BWToVoiceCoderBW,
IpProfile_CreatedByRoutingServer, IpProfile_SBCFaxReroutingMode,
IpProfile_SBCMaxCallDuration, IpProfile_SBCGenerateRTP,
IpProfile_SBCISUPBodyHandling, IpProfile_SBCISUPVariant,
```

```
IpProfile_SBCVoiceQualityEnhancement, IpProfile_SBCMaxOpusBW,
IpProfile_LocalRingbackTone, IpProfile_LocalHeldTone;
IpProfile 1 = "Genesys", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0, 0,
2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "",
"AudioCodersGroups_0", 0, 0, "", "Genesys", "", 0, 0, 0, 0, 0, 0, 0, 8,
300, 400, 0, 0, 0, "", 0, 0, 1, 3, 0, 2, 2, 1, 0, 0, 1, 2, 1, 0, 0, 0, 0,
0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 300, -1, -1,
0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, 1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0, 0, -
1, -1;
IpProfile 2 = "ITSP", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0, 0, 2,
0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "",
"AudioCodersGroups_0", 0, 0, "", "Genesys", "", 0, 0, 0, 0, 0, 0, 0, 8,
300, 400, 1, 0, 0, "", 0, 0, 1, 3, 0, 2, 2, 0, 3, 2, 1, 0, 1, 0, 0, 0, 0,
0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 300, -1, -1,
0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0, 0,
-1, -1;
IpProfile 3 = "Remote User", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24,
0, 0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", "", 0, 0,
"", "", "", 0, 0, 0, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, "", 0, 0, 1, 3, 0,
2, 2, 1, 3, 2, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -
1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, -1;

[ \IpProfile ]


[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile,
CpMediaRealm_TopologyLocation;
CpMediaRealm 0 = "DefaultRealm", "NETMGT", "", 62000, 100, 62999, 1, "",
"", 0;
CpMediaRealm 1 = "MR-SBC2Genesys", "NETMGT", "", 8000, 100, 8999, 0, "",
"", 0;
CpMediaRealm 2 = "MR-SBC2ITSP", "PUBSIP", "", 6000, 100, 6999, 0, "", "",
0;
CpMediaRealm 3 = "MR3_RemoteAgents", "PUBSIP", "", 10000, 100, 10999, 0,
"", "", 0;

[ \CpMediaRealm ]


[ SBCRoutingPolicy ]

FORMAT SBCRoutingPolicy_Index = SBCRoutingPolicy_Name,
SBCRoutingPolicy_LCREnable, SBCRoutingPolicy_LCRAverageCallLength,
SBCRoutingPolicy_LCRDefaultCost, SBCRoutingPolicy_LdapServerGroupName;
SBCRoutingPolicy 0 = "Default_SBCRoutingPolicy", 0, 1, 0, "";

[ \SBCRoutingPolicy ]


[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers,
SRD_EnableUnAuthenticatedRegistrations, SRD_SharingPolicy,
```

```
SRD_UsedByRoutingServer, SRD_SBCOperationMode, SRD_SBCRoutingPolicyName,
SRD_SBCDialPlanName;
SRD 0 = "DefaultSRD", 0, -1, 1, 0, 0, 0, "Default_SBCRoutingPolicy", "";

[ \SRD ]


[ MessagePolicy ]

FORMAT MessagePolicy_Index = MessagePolicy_Name,
MessagePolicy_MaxMessageLength, MessagePolicy_MaxHeaderLength,
MessagePolicy_MaxBodyLength, MessagePolicy_MaxNumHeaders,
MessagePolicy_MaxNumBodies, MessagePolicy_SendRejection,
MessagePolicy_MethodList, MessagePolicy_MethodListType,
MessagePolicy_BodyList, MessagePolicy_BodyListType,
MessagePolicy_UseMaliciousSignatureDB;
MessagePolicy 0 = "Malicious Signature DB Protection", -1, -1, -1, -1, -1,
1, "", 0, "", 0, 1;

[ \MessagePolicy ]


[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
SIPInterface_AdditionalUDPPorts, SIPInterface_SRDName,
SIPInterface_MessagePolicyName, SIPInterface_TLSContext,
SIPInterface_TLSMutualAuthentication, SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,
SIPInterface_PreClassificationManSet, SIPInterface_EncapsulatingProtocol,
SIPInterface_MediaRealm, SIPInterface_SBCDirectMedia,
SIPInterface_BlockUnRegUsers, SIPInterface_MaxNumOfRegUsers,
SIPInterface_EnableUnAuthenticatedRegistrations,
SIPInterface_UsedByRoutingServer, SIPInterface_TopologyLocation,
SIPInterface_PreParsingManSetName;
SIPInterface 0 = "SIPInterface_0", "NETMGT", 0, 0, 0, 0, "", "DefaultSRD",
"", "default", -1, 0, 500, -1, 0, "", 0, -1, -1, -1, 0, 0, "";
SIPInterface 1 = "Genesys", "NETMGT", 2, 5060, 5060, 0, "", "DefaultSRD",
"", "default", -1, 0, 500, -1, 0, "MR-SBC2Genesys", 0, -1, -1, -1, 0, 0,
"";
SIPInterface 2 = "ITSP", "PUBSIP", 2, 5060, 0, 0, "", "DefaultSRD", "",
"default", -1, 0, 500, -1, 0, "MR-SBC2ITSP", 0, -1, -1, -1, 0, 0, "";
SIPInterface 3 = "RemoteAgents", "PUBSIP", 2, 5070, 0, 0, "", "DefaultSRD",
"", "default", -1, 0, 500, -1, 0, "MR-SBC2ITSP", 0, -1, -1, -1, 0, 0, "";

[ \SIPInterface ]


[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_ProxyName, ProxySet_EnableProxyKeepAlive,
ProxySet_ProxyKeepAliveTime, ProxySet_ProxyLoadBalancingMethod,
ProxySet_IsProxyHotSwap, ProxySet_SRDName, ProxySet_ClassificationInput,
ProxySet_TLSContextName, ProxySet_ProxyRedundancyMode,
ProxySet_DNSResolveMethod, ProxySet_KeepAliveFailureResp,
ProxySet_GWIPv4SIPInterfaceName, ProxySet_SBCIPv4SIPInterfaceName,
ProxySet_GWIPv6SIPInterfaceName, ProxySet_SBCIPv6SIPInterfaceName,
ProxySet_MinActiveServersLB, ProxySet_SuccessDetectionRetries,
```

```
ProxySet_SuccessDetectionInterval,
ProxySet_FailureDetectionRetransmissions;
ProxySet 0 = "ProxySet_0", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "",
"SIPInterface_0", "", "", "", 1, 1, 10, -1;
ProxySet 1 = "Genesys", 1, 60, 0, 0, "DefaultSRD", 0, "default", -1, -1,
"", "", "Genesys", "", "", 1, 1, 10, -1;
ProxySet 2 = "ITSP", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "",
"ITSP", "", "", 1, 1, 10, -1;

[ \ProxySet ]


[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Name, IPGroup_ProxySetName,
IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_SipReRoutingMode,
IPGroup_AlwaysUseRouteTable, IPGroup_SRDName, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileName, IPGroup_MaxNumOfRegUsers,
IPGroup_InboundManSet, IPGroup_OutboundManSet, IPGroup_RegistrationMode,
IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile, IPGroup_BWProfile,
IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IPGroup_SIPConnect, IPGroup_SBCPSAPMode,
IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer,
IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup_SBCRouteUsingRequestURIPort, IPGroup_SBCKeepOriginalCallID,
IPGroup_TopologyLocation, IPGroup_SBCDialPlanName,
IPGroup_CallSetupRulesSetId, IPGroup_Tags, IPGroup_SBCUserStickiness,
IPGroup_UserUDPPortAssignment;
IPGroup 0 = 0, "Default_IPG", "ProxySet_0", "", "", -1, 0, "DefaultSRD",
"", 0, "", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "",
0, "", "", 0, 0, "default", 0, 0, -1, 0, 0, 0, "", -1, "", 0, 0;
IPGroup 1 = 0, "Genesys", "Genesys", "", "", -1, 0, "DefaultSRD", "MR-
SBC2Genesys", 1, "Genesys", -1, -1, 8, 0, 1, "", 0, -1, -1, "", "",
"$1$gQ==", 0, "", "", 0, "", "", 0, 0, "default", 0, 0, 0, 0, 0, 0, "", -1,
"", 0, 0;
IPGroup 2 = 0, "ITSP", "ITSP", "", "", -1, 0, "DefaultSRD", "MR-SBC2ITSP",
1, "ITSP", -1, 2, 5, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "", 0,
"", "", 0, 0, "default", 0, 0, 0, 0, 0, 0, "", -1, "", 0, 0;
IPGroup 3 = 1, "RemoteAgents", "", "", "", -1, 0, "DefaultSRD", "MR-
SBC2ITSP", 0, "Remote User", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "",
"$1$gQ==", 0, "", "", 0, "", "", 0, 0, "default", 0, 0, 0, 0, 0, 0, "", -1,
"", 0, 0;

[ \IPGroup ]


[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex,
ProxyIp_IpAddress, ProxyIp_TransportType;
ProxyIp 0 = "1", 0, "sipserver.genesys-domain.com:5060", 0;
ProxyIp 2 = "2", 0, "gw0.itsp-iot.com:5060", 0;

[ \ProxyIp ]


[ Account ]
```

```
FORMAT Account_Index = Account_ServedTrunkGroup, Account_ServedIPGroupName,
Account_ServingIPGroupName, Account_Username, Account_Password,
Account_HostName, Account_ContactUser, Account_Register,
Account_RegistrarStickiness, Account_RegistrarSearchMode,
Account_RegEventPackageSubscription, Account_ApplicationType,
Account_RegByServedIPG, Account_UDPPortAssignment;
Account 0 = -1, "ITSP", "Genesys", "genesys", "$1$tIWHhYONjw==", "", "", 0,
0, 0, 0, 2, 0, 0;

[ \Account ]


[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_RoutingPolicyName, IP2IPRouting_SrcIPGroupName,
IP2IPRouting_SrcUsernamePattern, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePattern, IP2IPRouting_DestHost,
IP2IPRouting_RequestType, IP2IPRouting_MessageConditionName,
IP2IPRouting_ReRouteIPGroupName, IP2IPRouting_Trigger,
IP2IPRouting_CallSetupRulesSetId, IP2IPRouting_DestType,
IP2IPRouting_DestIPGroupName, IP2IPRouting_DestSIPInterfaceName,
IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup, IP2IPRouting_DestTags,
IP2IPRouting_SrcTags, IP2IPRouting_IPGroupSetName,
IP2IPRouting_RoutingTagName, IP2IPRouting_InternalAction;
IP2IPRouting 0 = "Options", "Default_SBCRoutingPolicy", "Any", "*", "*",
"*", "*", 6, "", "Any", 0, -1, 1, "", "", "internal", 0, -1, 0, 0, "", "",
"", "", "default", "";
IP2IPRouting 1 = "3xx/Refer Trigger", "Default_SBCRoutingPolicy", "ITSP",
"*", "*", "0825*", "*", 0, "", "Genesys", 3, -1, 0, "ITSP", "", "", 0, -1,
0, 0, "", "", "", "", "default", "";
IP2IPRouting 2 = "3xx Refer Remote Agents", "Default_SBCRoutingPolicy",
"Genesys", "*", "*", "*", "*", 0, "", "RemoteAgents", 3, -1, 0, "Genesys",
"", "", 0, -1, 0, 0, "", "", "", "", "default", "";
IP2IPRouting 3 = "3xx/Refer to Genesys", "Default_SBCRoutingPolicy", "Any",
"*", "*", "*", "*", 0, "", "Genesys", 3, -1, 0, "Genesys", "", "", 0, -1,
0, 0, "", "", "", "", "default", "";
IP2IPRouting 4 = "ITSP->Genesys", "Default_SBCRoutingPolicy", "ITSP", "*",
"*", "*", "*", 0, "", "Any", 0, -1, 0, "Genesys", "", "", 0, -1, 0, 0, "",
"", "", "", "default", "";
IP2IPRouting 5 = "Genesys->AHA", "Default_SBCRoutingPolicy", "Genesys",
"*", "*", "*", "*", 0, "", "Any", 0, -1, 10, "", "", "", 0, -1, 0, 0, "",
"", "", "", "default", "";
IP2IPRouting 6 = "Genesys->ITSP", "Default_SBCRoutingPolicy", "Genesys",
"*", "*", "*", "*", 0, "", "Any", 0, -1, 0, "ITSP", "", "", 0, -1, 1, 0,
"", "", "", "", "default", "";
IP2IPRouting 7 = "AHA->Genesys", "Default_SBCRoutingPolicy",
"RemoteAgents", "*", "*", "*", "*", 0, "", "Any", 0, -1, 0, "Genesys", "",
"", 0, -1, 0, 0, "", "", "", "", "default", "";

[ \IP2IPRouting ]


[ Classification ]

FORMAT Classification_Index = Classification_ClassificationName,
Classification_MessageConditionName, Classification_SRDName,
```

```
Classification_SrcSIPInterfaceName, Classification_SrcAddress,
Classification_SrcPort, Classification_SrcTransportType,
Classification_SrcUsernamePattern, Classification_SrcHost,
Classification_DestUsernamePattern, Classification_DestHost,
Classification_ActionType, Classification_SrcIPGroupName,
Classification_DestRoutingPolicy, Classification_IpProfileName;
Classification 0 = "AHA", "", "DefaultSRD", "RemoteAgents", "", 0, -1, "*",
"*", "*", "*", 1, "RemoteAgents", "", "";

[ \Classification ]


[ IPInboundManipulation ]

FORMAT IPInboundManipulation_Index =
IPInboundManipulation_ManipulationName,
IPInboundManipulation_RoutingPolicyName,
IPInboundManipulation_IsAdditionalManipulation,
IPInboundManipulation_ManipulationPurpose,
IPInboundManipulation_SrcIPGroupName,
IPInboundManipulation_SrcUsernamePattern, IPInboundManipulation_SrcHost,
IPInboundManipulation_DestUsernamePattern, IPInboundManipulation_DestHost,
IPInboundManipulation_RequestType, IPInboundManipulation_ManipulatedURI,
IPInboundManipulation_RemoveFromLeft,
IPInboundManipulation_RemoveFromRight,
IPInboundManipulation_LeaveFromRight, IPInboundManipulation_Prefix2Add,
IPInboundManipulation_Suffix2Add;
IPInboundManipulation 0 = "remove access code", "Default_SBCRoutingPolicy",
0, 0, "Genesys", "*", "*", "81xxxxxxxxxx#", "*", 0, 1, 2, 0, 255, "", "";
IPInboundManipulation 1 = "remove access code (for calls out the PS",
"Default_SBCRoutingPolicy", 0, 0, "Genesys", "*", "*", "81xxxxxxxxxxxxx#",
"*", 0, 1, 2, 0, 255, "", "";

[ \IPInboundManipulation ]


[ MessageManipulations ]

FORMAT MessageManipulations_Index = MessageManipulations_ManipulationName,
MessageManipulations_ManSetID, MessageManipulations_MessageType,
MessageManipulations_Condition, MessageManipulations_ActionSubject,
MessageManipulations_ActionType, MessageManipulations_ActionValue,
MessageManipulations_RowRole;
MessageManipulations 0 = "modify outbound Request-URI", 5, "Any", "",
"header.request-uri.url.host", 2, "'posteitaliane.it'", 0;
MessageManipulations 1 = "Normalize outbound Request-URI", 5, "Invite", "",
"header.request-uri", 7, "", 0;
MessageManipulations 2 = "modify from host (so as to keep the tag)", 5,
"Invite", "", "header.from.url.host", 2, "'telecomitalia.it'", 0;
MessageManipulations 3 = "modify outbound To host", 5, "Any", "",
"header.to.url.host", 2, "'telecomitalia.it'", 0;
MessageManipulations 4 = "modify PAI for REFERs", 5, "Any", "", "header.p-
asserted-identity", 2, "'<sip:0274557715@telecomitalia.it>'", 0;
MessageManipulations 5 = "", 5, "", "header.Referred-By exists",
"header.contact.url.host", 2, "header.referred-by.url.host", 0;
MessageManipulations 6 = "contact host; must be 173.x", 5, "", "",
"header.contact.url.host", 2, "'173.227.254.67'", 0;
MessageManipulations 7 = "add DH if does not exist", 5, "",
"header.diversion !exists", "header.diversion", 0,
```

```
"'<tel:0274557715@telecomitalia.it>;reason=unknown;counter=1;screen=no;priv
acy=off'", 0;
MessageManipulations 8 = "correct hostname on diversion header", 5, "Any",
"", "header.diversion.url.host", 2, "'telecomitalia.it'", 0;
[ \MessageManipulations ]


[ GwRoutingPolicy ]

FORMAT GwRoutingPolicy_Index = GwRoutingPolicy_Name,
GwRoutingPolicy_LCREnable, GwRoutingPolicy_LCRAverageCallLength,
GwRoutingPolicy_LCRDefaultCost, GwRoutingPolicy_LdapServerGroupName;
GwRoutingPolicy 0 = "GwRoutingPolicy", 0, 1, 0, "";

[ \GwRoutingPolicy ]


[ LoggingFilters ]

FORMAT LoggingFilters_Index = LoggingFilters_FilterType,
LoggingFilters_Value, LoggingFilters_LogDestination,
LoggingFilters_CaptureType, LoggingFilters_Mode;
LoggingFilters 1 = 1, "", 1, 2, 1;

[ \LoggingFilters ]


[ ResourcePriorityNetworkDomains ]

FORMAT ResourcePriorityNetworkDomains_Index =
ResourcePriorityNetworkDomains_Name,
ResourcePriorityNetworkDomains_Ip2TelInterworking;
ResourcePriorityNetworkDomains 1 = "dsn", 1;
ResourcePriorityNetworkDomains 2 = "dod", 1;
ResourcePriorityNetworkDomains 3 = "drsn", 1;
ResourcePriorityNetworkDomains 5 = "uc", 1;
ResourcePriorityNetworkDomains 7 = "cuc", 1;

[ \ResourcePriorityNetworkDomains ]


[ SBCUserInfoTable ]

;
; *** TABLE SBCUserInfoTable ***
; This table contains hidden elements and will not be exposed.
; This table exists on board and will be saved during restarts.
;

[ \SBCUserInfoTable ]


[ MaliciousSignatureDB ]

FORMAT MaliciousSignatureDB_Index = MaliciousSignatureDB_Name,
MaliciousSignatureDB_Pattern;
MaliciousSignatureDB 0 = "SIPVicious", "Header.User-Agent.content prefix
'friendly-scanner'";
MaliciousSignatureDB 1 = "SIPScan", "Header.User-Agent.content prefix 'sip-
scan'";
```

```
MaliciousSignatureDB 2 = "Smap", "Header.User-Agent.content prefix 'smap'";
MaliciousSignatureDB 3 = "Sipsak", "Header.User-Agent.content prefix
'sipsak'";
MaliciousSignatureDB 4 = "Sipcli", "Header.User-Agent.content prefix
'sipcli'";
MaliciousSignatureDB 5 = "Sivus", "Header.User-Agent.content prefix
'SIVuS'";
MaliciousSignatureDB 6 = "Gulp", "Header.User-Agent.content prefix 'Gulp'";
MaliciousSignatureDB 7 = "Sipv", "Header.User-Agent.content prefix 'sipv'";
MaliciousSignatureDB 8 = "Sundayddr Worm", "Header.User-Agent.content
prefix 'sundayddr'";
MaliciousSignatureDB 9 = "VaxIPUserAgent", "Header.User-Agent.content
prefix 'VaxIPUserAgent'";
MaliciousSignatureDB 10 = "VaxSIPUserAgent", "Header.User-Agent.content
prefix 'VaxSIPUserAgent'";
MaliciousSignatureDB 11 = "SipArmyKnife", "Header.User-Agent.content prefix
'siparmyknife'";

[ \MaliciousSignatureDB ]


[ AllowedAudioCoders ]

FORMAT AllowedAudioCoders_Index =
AllowedAudioCoders_AllowedAudioCodersGroupName,
AllowedAudioCoders_AllowedAudioCodersIndex, AllowedAudioCoders_CoderID,
AllowedAudioCoders_UserDefineCoder;
AllowedAudioCoders 0 = "Genesys", 2, 1, "";
AllowedAudioCoders 1 = "Genesys", 1, 3, "";

[ \AllowedAudioCoders ]


[ AudioCoders ]

FORMAT AudioCoders_Index = AudioCoders_AudioCodersGroupId,
AudioCoders_AudioCodersIndex, AudioCoders_Name, AudioCoders_pTime,
AudioCoders_rate, AudioCoders_PayloadType, AudioCoders_Sce,
AudioCoders_CoderSpecific;
AudioCoders 0 = "AudioCodersGroups_0", 0, 3, 2, 19, -1, 0, "";
AudioCoders 1 = "AudioCodersGroups_0", 1, 1, 2, 90, -1, 0, "";

[ \AudioCoders ]
```

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

AudioCodes Inc.
27 World's Fair Drive,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

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

Document #: LTRT-12795