Session Border Controllers (SBC)

AudioCodes Mediant™ Series

Interoperability Lab

Configuration Note

Windstream SIP Trunk & Genesys Contact Center using AudioCodes Mediant SBC

windstream.

Genesys

SBC

AudioCodes

Version 7.0

December 2015

Document # LTRT-39430

Table of Contents

Table of Figures

List of Tables

This page is intentionally left blank

Notice

This document describes how to connect the Windstream ITSP SIP Trunk and Genesys Contact Center using AudioCodes Mediant SBC product series.

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 and other documents as well as software files can be viewed by registered customers at http://www.audiocodes.com/downloads.

Date Published: Dec-15-2015

Trademarks

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 www.audiocodes.com/support.

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 http://www.audiocodes.com/downloads.

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 Windstream ITSP SIP Trunk and Genesys Contact Center.

> **Note:** Throughout this document, the term 'SBC' also refers to AudioCodes' Mediant E-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 Windstream 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_7.00.035.012
Protocol	§ SIP/UDP (to the Windstream ITSP SIP Trunk) § SIP/UDP (to the Genesys Contact Center system)
Additional Notes	None

2.2 Windstream SIP Trunking Version

Table 2-2: Windstream Version

Vendor/Service Provider	Windstream
SSW Model/Service	BroadSoft
Software Version	R17SP4
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 v8.1.101.57/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 Windstream ITSP SIP Trunk Provider via an SBC in a similar way to an IP-PBX.

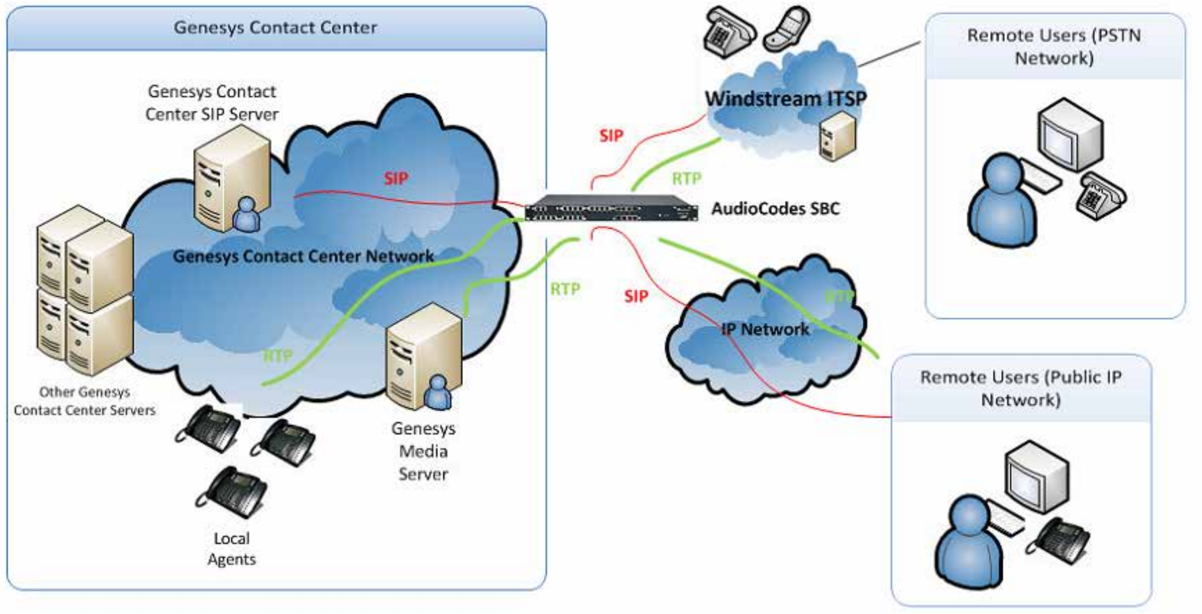
Note: Contact your Genesys Contact Center support channel for more information about topological scenarios.

Interoperability testing between AudioCodes SBC and Windstream 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 Windstream ITSP SIP Trunk, as an Over the Top (OTT) trunk over the public network.
- 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 Windstream ITSP SIP Trunk located on the public network.
    - RTP traffic from/to the Windstream 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 § Windstream ITSP SIP Trunk is located on the WAN
Signaling Transcoding	§ Genesys Contact Center operates with SIP-over-UDP, TCP or TLS transport type § Windstream SIP Trunk operates with SIP-over-UDP transport type. § The interoperability test environment used SIP-over-UDP
Codecs Transcoding	§ Genesys Contact Center supports G.729, G.711A-law, G.711U-law, G.723, G722.2 and G.726 coders § Windstream SIP Trunk supports G.711A-law (mandatory) and G.711U-law (recommended) coders
Media Transcoding	§ Genesys Contact Center and Windstream 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 § Windstream 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 Windstream SIP Trunk:

- **SIP 302 Moved Temporarily**. Windstream does not support 302 Moved Temporarily. This should be handled locally by the SBC.
- **SIP REFER**. The Windstream SIP specification indicates support of the network REFER; however, in the Request Single Step Call Transfer scenario, when the SIP server sends the REFER out to the network and waits for the incoming INVITE to match the REFER, the INVITE from the Windstream network is without matching information, thereby resulting in a new call. The SIP server continues to wait for the INVITE to match the REFER and the leg to the first agent is not released until a new 'matching' leg is created. This is when the SIP server reports that the Request Single Step Transfer succeeded; however, in this case, the two legs are not matched and therefore the transfer inside the SIP server does not succeed.

  This scenario can be mitigated by handling the SIP REFER locally on the SBC. The SBC will reply with a SIP 202 Accepted and additional NOTIFYs reflecting the state of the new INVITE. For internal agents, the SBC routing directs a new INVITE to the

Genesys SIP server, with the Request-URI set to the value of the contact in the REFER.

For REFERs to external destinations, the SBC routing directs a new INVITE to the ITSP with a Diversion Header containing the original destination number and with the Request-URI set to the new external destination number.

- **SIP Authentication for Outbound Calls**. Windstream 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).
- **SIP Authentication for Inbound Calls**. Windstream does not support challenge/authentication for outbound calls from Windstream (inbound to the Contact Center). If required, a SIP authentication response can be handled on the SBC as part of the Trunk-Side Equipment (TSE).
- **SBCMAXFORWARDSLIMIT** for the interoperability test was at the SBC default setting of 10. Consider adjusting this corresponding to deployment requirements. (**Configuration** > **VoiP** > **SBC** > **SBC General Settings**)
- **BrokenConnectionEventTimeout**. For a call scenario in which a call is opened from the Call Center with an INVITE and no SDP, the call drops due to no RTP. This issue was resolved by configuring BrokenConnectionEventTimout (global parameter) to 1000 (over the default 100). Setting it to 1000 is the equivalent of 100 seconds. This is preferred over disabling Broken Connection Event detection, unless it is determined to be necessary.
- **Diversion Header**. When inbound calls to the Call Center are re-routed outbound by the SIP server using an INVITE without SDP, it is necessary to include a Diversion Header in the outbound INVITE if the SIP server is not configured to send a P-Asserted-Identity (PAI) header on the outbound trunk to the SBC. If the PAI header is passed or inserted by the SBC, the ITSP will route the call without the Diversion header being added. In the interoperability test scenario, this was tested both ways. Refer to the manipulations of set 19 in the Appendix that'll be part of manipulation set 1 if the SBC inserts the Diversion header. In this case, manipulations were used to take the redirected number from the To: header and map that number to the Diversion header. In the Diversion header, an on-network number should be chosen. For the interoperability test scenario, the Routing Pointing was specified as the on-network number.
- **Early Media**. The Windstream ITSP does not support Early Media. In standard deployments, Windstream will not send 100REL in the Supported line of a SIP INVITE. During testing, if Early Media was invoked, the call resulted in no speech path. The issue was determined to be in Windstream’s PSTN network, but no resolution was found during testing.

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 Windstream ITSP SIP Trunk. The configuration is based on the interoperability test topology described in Section 2.4 on page 12 and includes the following:

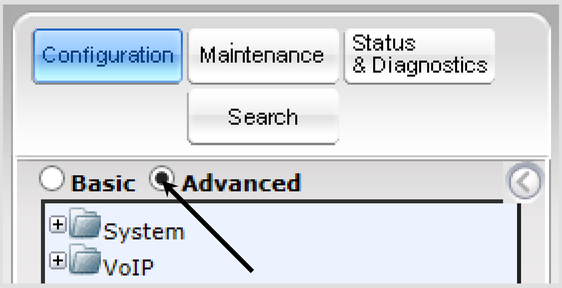
- **SBC WAN interface** - Windstream ITSP SIP Trunking environment
- **SBC LAN interface** - Genesys Contact Center environment

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

Notes:

- To implement the Genesys Contact Center and Windstream 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.
- Before you begin configuring the SBC, ensure that the SBC's Web interface navigation tree is in **Advanced** display mode, selectable as shown below:



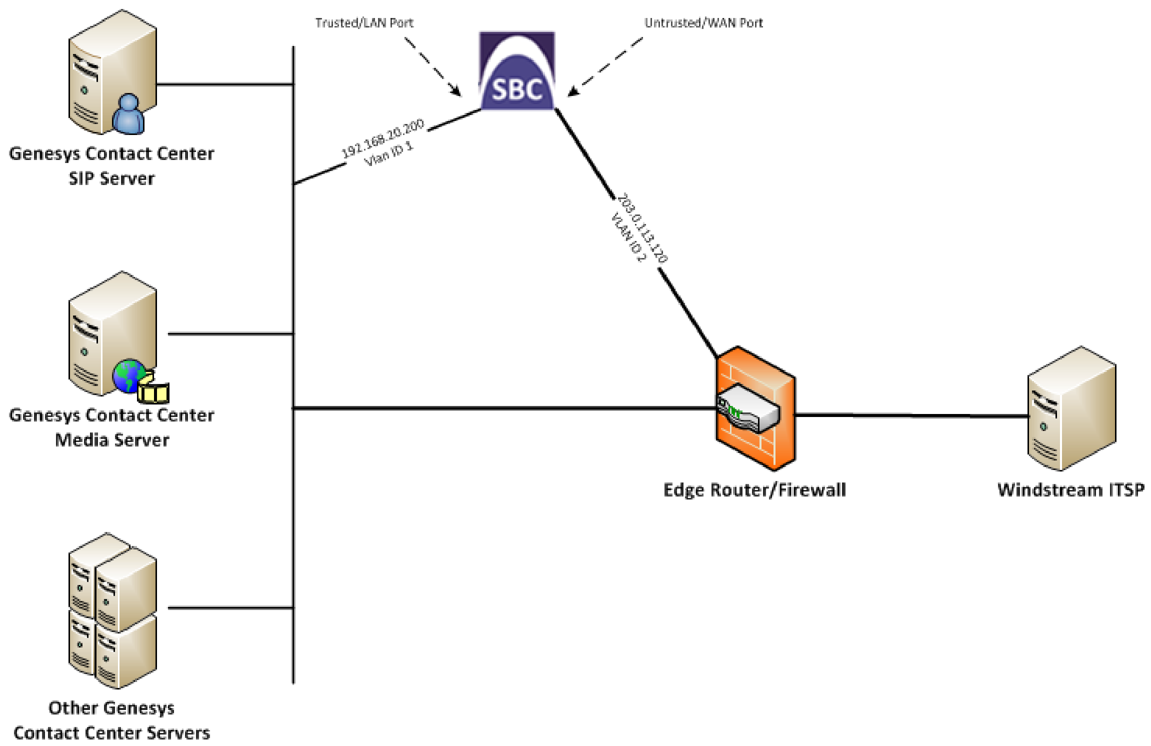
  Note that when the SBC is reset, the navigation tree reverts to **Basic** display mode.

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)
  - Windstream 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 also uses two logical network interfaces:
  - LAN (VLAN ID 1)
  - WAN (VLAN ID 2)

Figure 3-1: Network Interfaces in Interoperability Test Topology



3.1.1 Step 1a: Configure VLANs

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

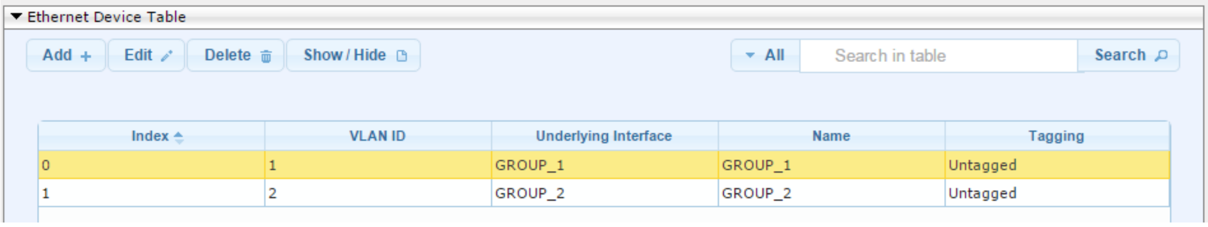
- LAN VoIP (assigned the name "Call Center")
- WAN VoIP (assigned the name "Provider")

Ø To configure the VLANs:

1. Open the Ethernet Device Table page (**Configuration** tab > **VoIP** menu > **Network** > **Ethernet Device Table**); in the table you'll see an existing row for VLAN ID 1 and underlying interface GROUP_1.
2. Add another VLAN ID 2 for the WAN side as follows:

Parameter	Value
Index	**1**
VLAN ID	**2**
Underlying Interface	**GROUP_2** (Ethernet port group)
Name	**GROUP_2**
Tagging	**Untagged**

Figure 3-2: Configured VLAN IDs in Ethernet Device Table



Index	VLAN ID	Underlying Interface	Name	Tagging
0	1	GROUP_1	GROUP_1	Untagged
1	2	GROUP_2	GROUP_2	Untagged

3.1.2 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")

Ø To configure these IP network interfaces:

1. Open the IP Interfaces Table page (**Configuration** tab > **VoIP** menu > **Network** > **IP Interfaces Table**).

2. Modify the existing LAN network interface:
   a. Select the **Index** option of the **OAMP + Media + Control** table row, and then click **Edit**.
   b. Configure the interface as follows:

Parameter	Value
IP Address	**192.168.20.200** (IP address of SBC)
Prefix Length	**24** (subnet mask in bits for 255.255.255.0)
Gateway	**192.168.20.1**
Interface Name	**NETMGT** (arbitrary descriptive name)
Primary DNS Server IP Address	Add DNS Server IP address in this network
Underlying Device	**GROUP_1**

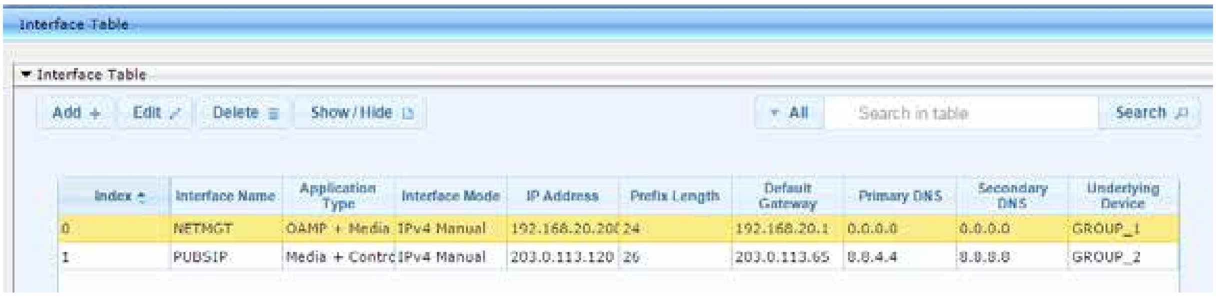
3. Add a network interface for the WAN side:
   a. Enter **1**, and then click **Add Index**.
   a. Configure the interface as follows:

Parameter	Value
Application Type	**Media + Control**
IP Address	**203.0.113.120** (WAN IP address)
Prefix Length	**26** (for 255.255.255.128)
Gateway	**203.0.113.65** (router's IP address)
Interface Name	**PUBSIP** (arbitrary descriptive name)
Primary DNS Server IP Address	**8.8.4.4** (as specified by ISP)
Secondary DNS Server IP Address	**8.8.8.8** (as specified by ISP)
Underlying Device	**GROUP_2**

4. Click **Apply**, and then **Done**.

The configured IP network interfaces are shown below:

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


Interface Table

Interface Table

Add + | Edit | Delete | Show / Hide | All | Search in table | Search

Index	Interface Name	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Primary DNS	Secondary DNS	Underlying Device
0	NETMGT	OAMP + Media	IPv4 Manual	192.168.20.20(	24	192.168.20.1	0.0.0.0	0.0.0.0	GROUP_1
1	PUBSIP	Media + Contrc	IPv4 Manual	203.0.113.120	26	203.0.113.65	8.8.4.4	8.8.8.8	GROUP_2

3.2 Step 2: Enable the SBC Application

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

Ø **To enable the SBC application:**

1. Open the Applications Enabling page (**Configuration** tab > **VoIP** menu > **Applications Enabling** > **Applications Enabling**).

Figure 3-4: Enabling SBC Application

2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Submit**.
4. Reset the SBC with a burn to flash for the setting to take effect (see Section 3.12 on page 68).

3.3 Step 3: Configure Signaling Routing Domains

This step describes how to configure 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:

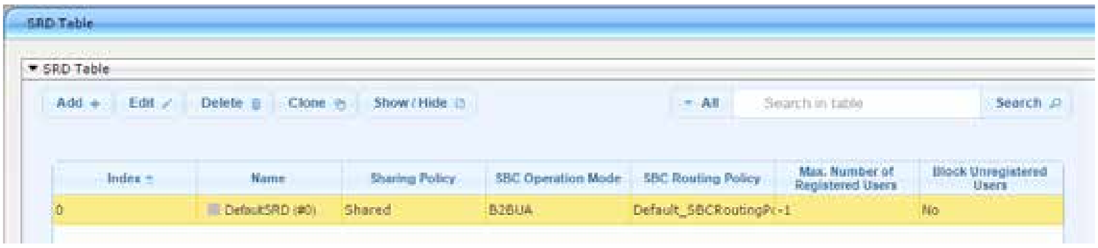
- SIP Interface (mandatory)
- IP Group (mandatory)
- Proxy Set (mandatory)
- Admission Control rule (optional)
- Classification rule (optional)

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 an 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.

Ø To view the default SRD:

- Access the SRD Table (**Configuration** > **VoIP** > **VoIP Network** > **SRD Table**).

Figure 3-5: SRD Table



3.3.1 Step 3a: Configure Media Realms

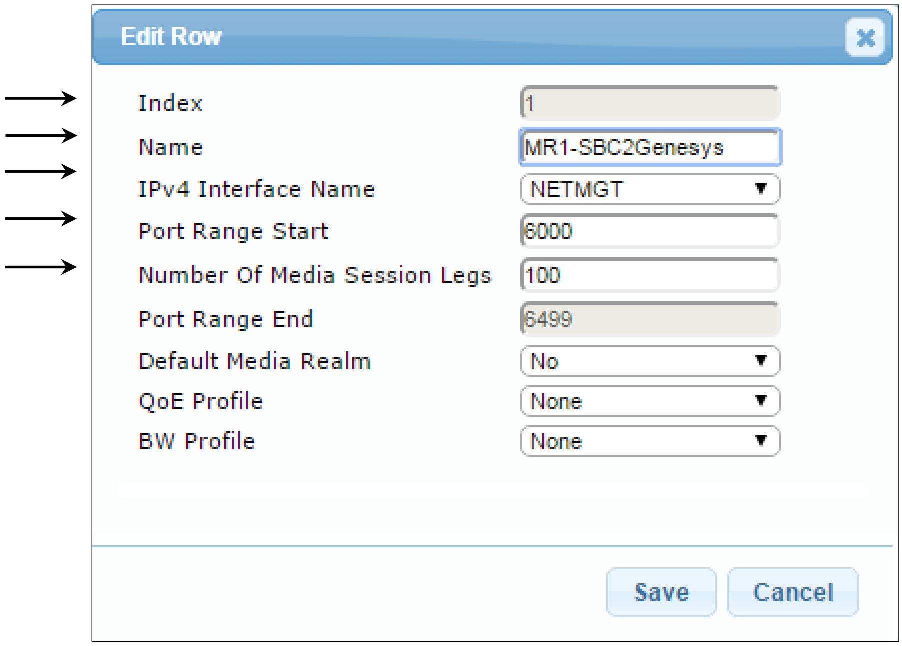
This step describes how to configure Media Realms. The simplest way is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

Ø To configure Media Realms:

1. Open the Media Realm Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Media Realm Table**).
2. Modify the existing Media Realm for LAN traffic:

Parameter	Value
Index	**1**
Media Realm Name	**MR-SBC2Genesys** (descriptive name)
IPv4 Interface Name	**NETMGT**
Port Range Start	**6000** (represents lowest UDP port number used for media on LAN).
Number of Media Session Legs	**100** (media sessions assigned with port range)

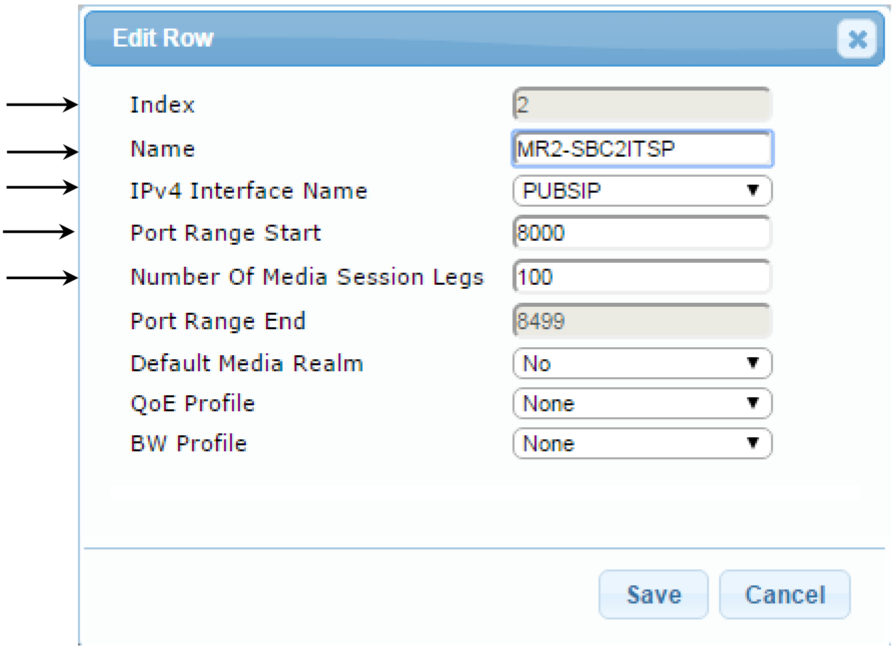
Figure 3-6: Configure Media Realm for LAN



3. Configure a Media Realm for WAN traffic:

Parameter	Value
Index	**2**
Media Realm Name	**MR2-SBC2ITSP** (arbitrary name)
IPv4 Interface Name	**PUBSIP**
Port Range Start	**8000** (represents the lowest UDP port number used for media on WAN).
Number of Media Session Legs	**100** (media sessions assigned with port range).

Figure 3-7: Configure Media Realm for WAN



The configured Media Realms are shown in the figure below:

Figure 3-8: Configured Media Realms in Media Realm Table

Media Realm Table

Index	Name	IPv4 Interface Name	Port Range Start	Number Of Media Session Legs	Port Range End	Default Media Realm
1	MR1-SBC2Genesys	NETMGT	6000	100	6499	No
2	MR2-SBC2ITSP	PUBSIP	8000	100	8499	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 and external SIP Interface is configured for the SBC.

Ø To configure SIP Interfaces:

1. Open the SIP Interface Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SIP Interface Table**).
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:

Figure 3-9: Configured SIP Interfaces in SIP Interface Table

SIP Interface Table

Index	Name	SRD	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Encapsulating Protocol	Media Realm
1	Genesys	DefaultSRD (	NETMGT	SBC	5060	0	0	No encapsulati	MR1-SBC2Gen
2	ITSP	DefaultSRD (	PUBSIP	SBC	5060	0	0	No encapsulati	MR2-SBC2ITSF

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
- Windstream ITSP SIP Trunk

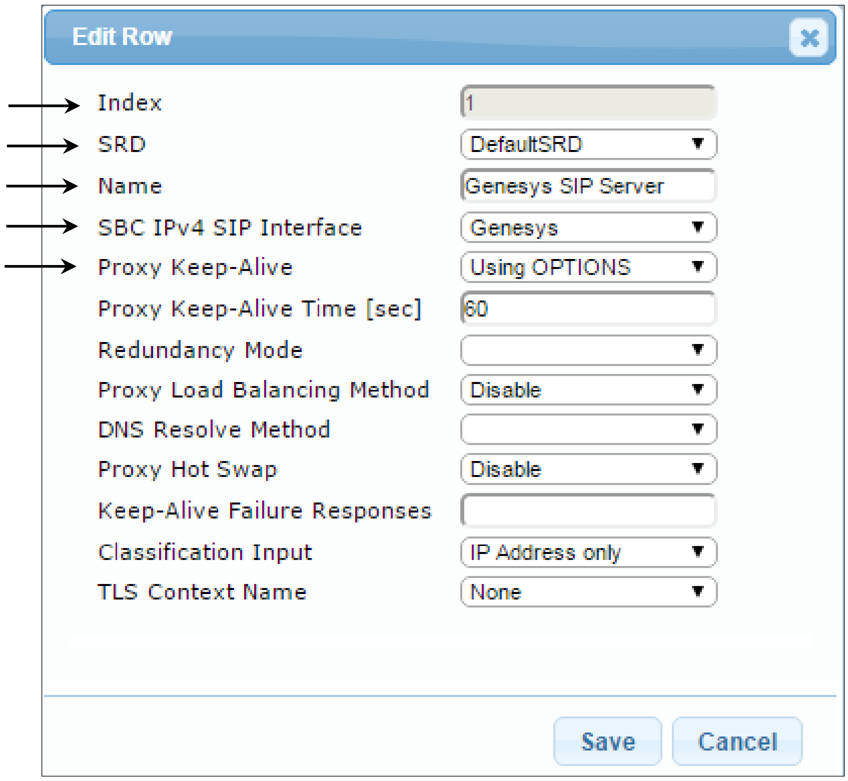
These Proxy Sets will later be associated with IP Groups.

Ø To configure Proxy Sets:

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table**).
2. Configure a Proxy Set for the Genesys Contact Center:

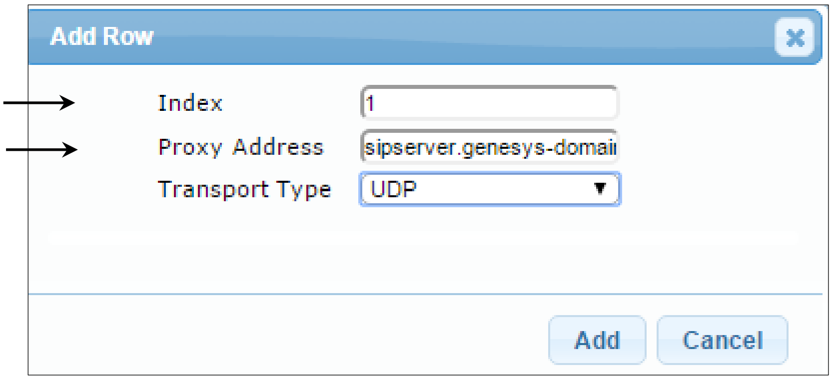
Parameter	Value
Proxy Set ID	**1**
SRD	**DefaultSRD**
Name	**Genesys SIP Server**
SBC IPv4 SIP Interface	**Genesys**
Proxy Keep Alive	**Using OPTIONs**
Proxy Address	**sipserver.genesys-domain.com:5060** Genesys Contact Center IP address / FQDN and destination port.
Transport Type	**UDP**

Figure 3-10: 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 (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table**), position on index, select **Proxy Address Table**, and then select **Add**).

Figure 3-11: Proxy Address Table - Add Row



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

Parameter	Value
Proxy Set ID	**1**
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 3-12: Configure Proxy Set for ITSP SIP Trunk

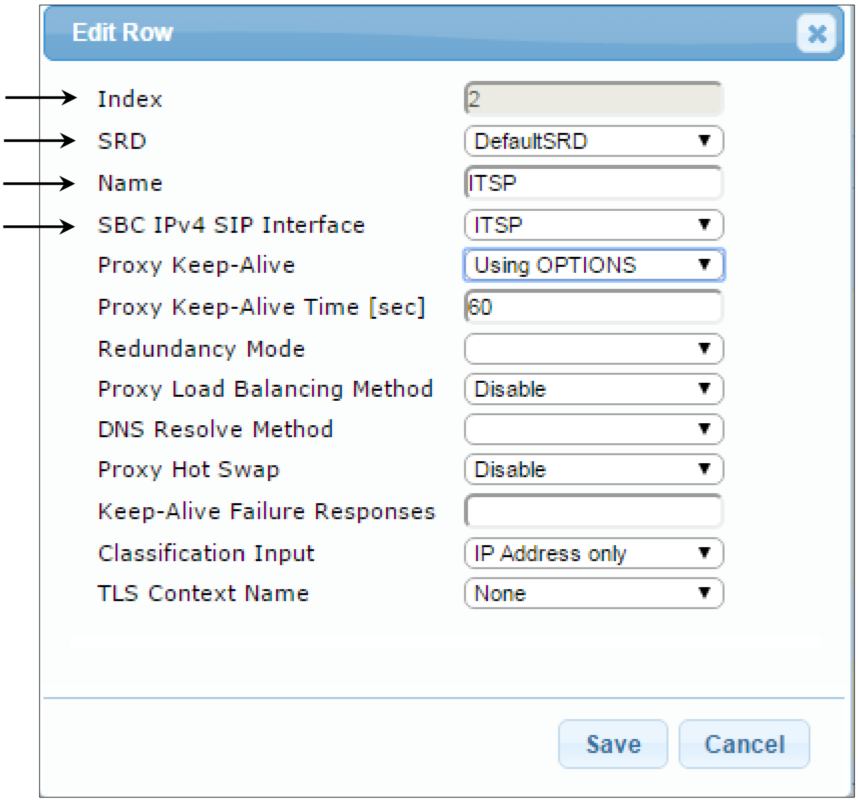
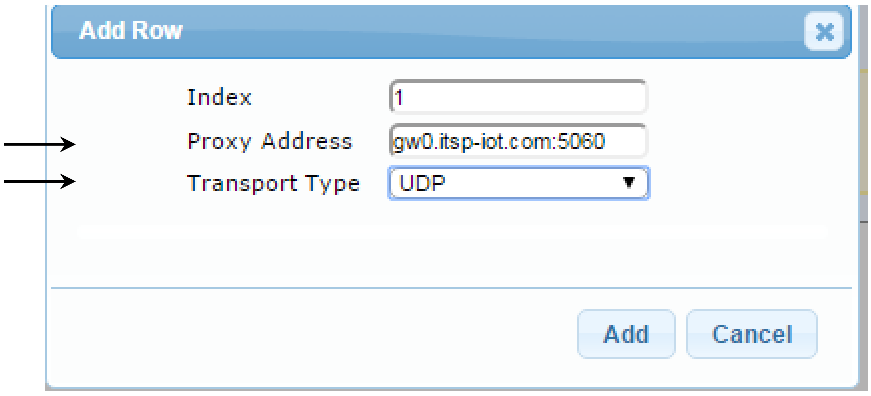


Figure 3-13: Configure Proxy Set for ITSP SIP Trunk – Add Row



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 52)

Ø To configure IP Groups:

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group 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 3-14: Configure an IP Group for the Genesys Call Center (Common Tab)

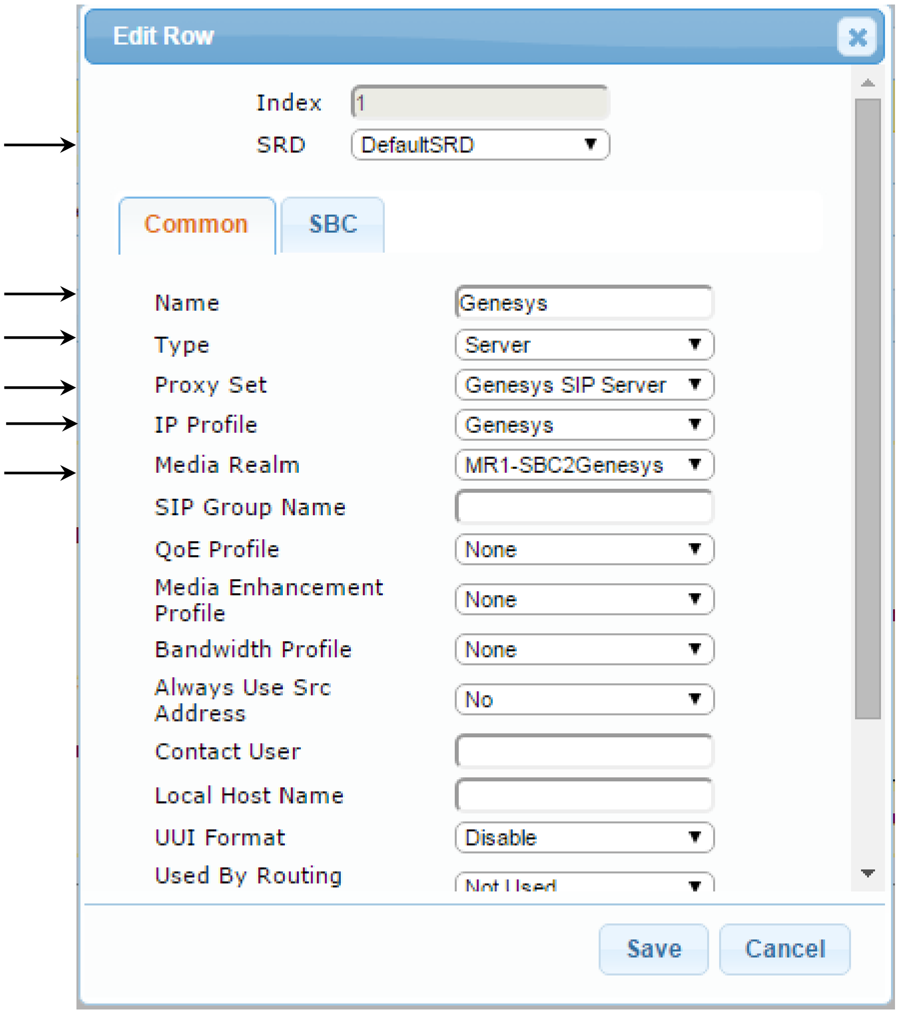
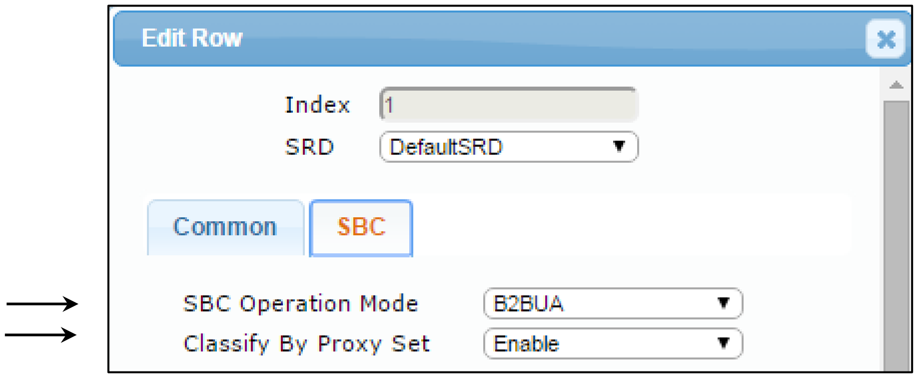


Figure 3-15: Configure an IP Group for the Genesys Call Center (SBC Tab)



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 3-16: Configure an IP Group for the ITSP SIP Trunk (Common Tab)

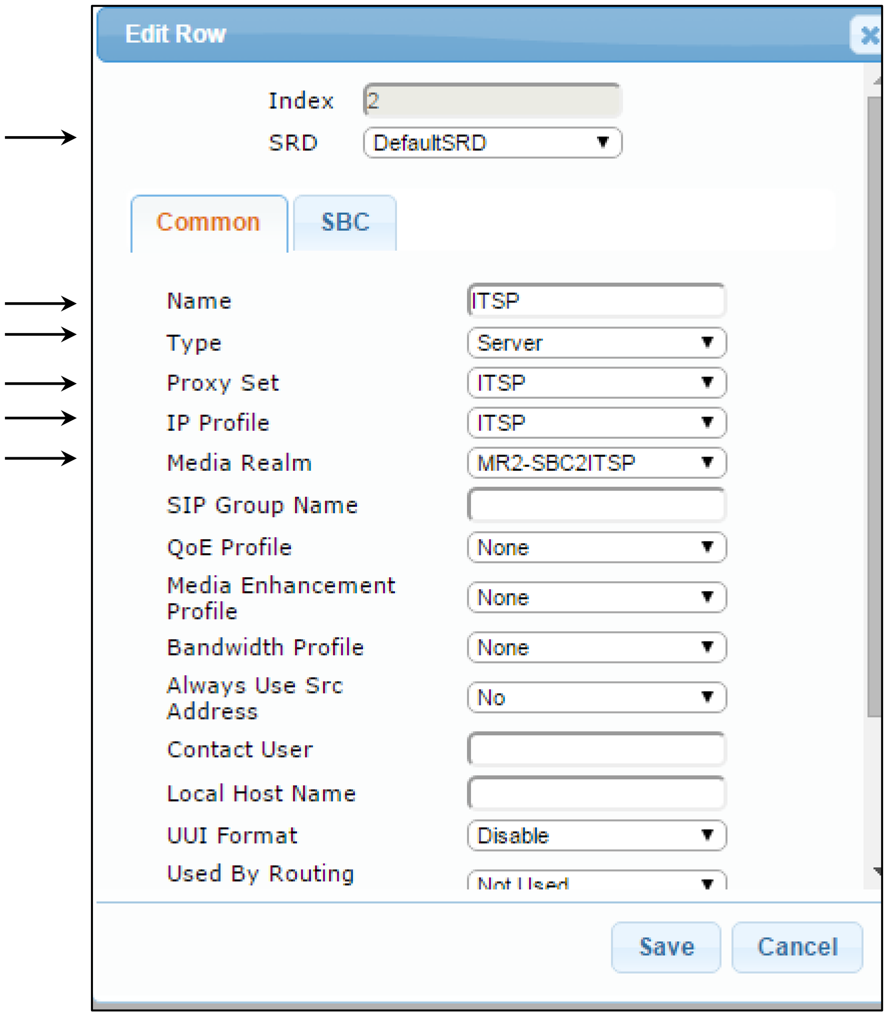
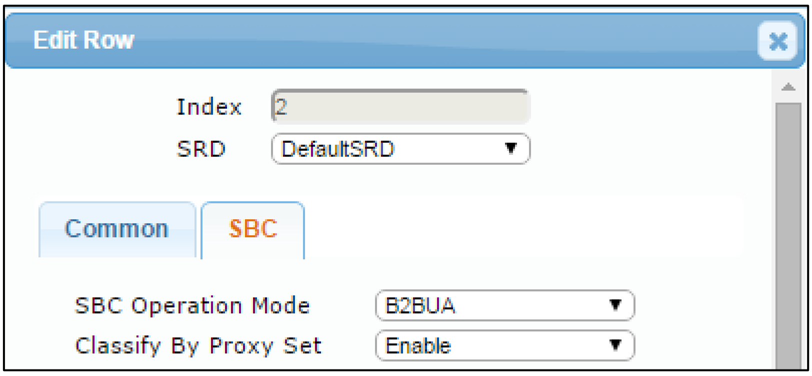


Figure 3-17: Configure an IP Group for the ITSP SIP Trunk (SBC Tab)



The configured IP Groups are shown in the figure below:

Figure 3-18: Configured IP Groups in IP Group Table

IP Group Table

Add + | Edit | Delete | Show / Hide | All | Search in table | Search

Index	Name	SRD	Type	SBC Operation Mode	Proxy Set	IP Profile	Media Realm	SIP Group Name	Classify By Proxy Set	Inbound Message Manipulatior Set	Outbound Message Manipulatior Set
1	Genesys	DefaultSR	Server	B2BUA	Genesys SIF	Genesys	MR1-SBC2G		Enable	3	12
2	ITSP	DefaultSR	Server	B2BUA	ITSP	ITSP	MR2-SBC2IT		Enable	-1	1

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
- Windstream ITSP SIP trunk

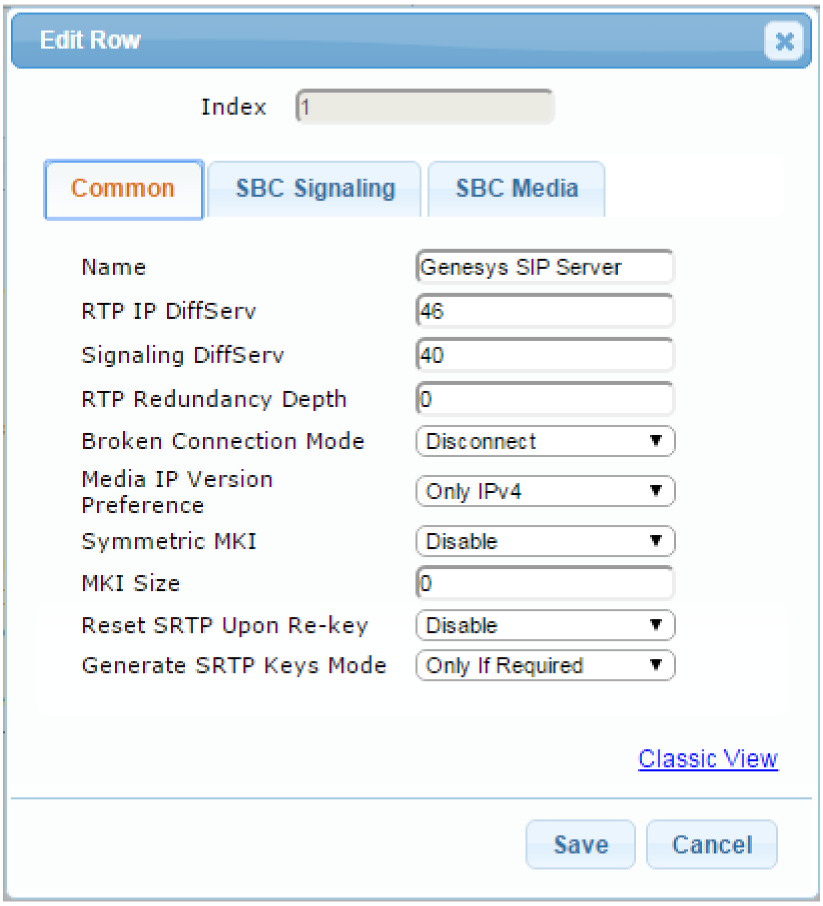
Note: The IP Profile index values were assigned to the IP Groups in the previous step (see Section 3.5 on page 28).

To configure IP Profiles:

1. Open the IP Profile Settings page (**Configuration** tab > **VoIP** > **Coders and Profiles** > **IP Profile Settings**).
2. Click **Add**.
3. Click the **Common** tab, and then configure the parameters as follows:

Parameter	Value
Index	**1**
Profile Name	**Genesys SIP Server** (arbitrary descriptive name)

Figure 3-19: Configure IP Profile for Genesys Contact Center (Common Tab)



4. Click the **SBC** tab, and then configure the parameters as follows:

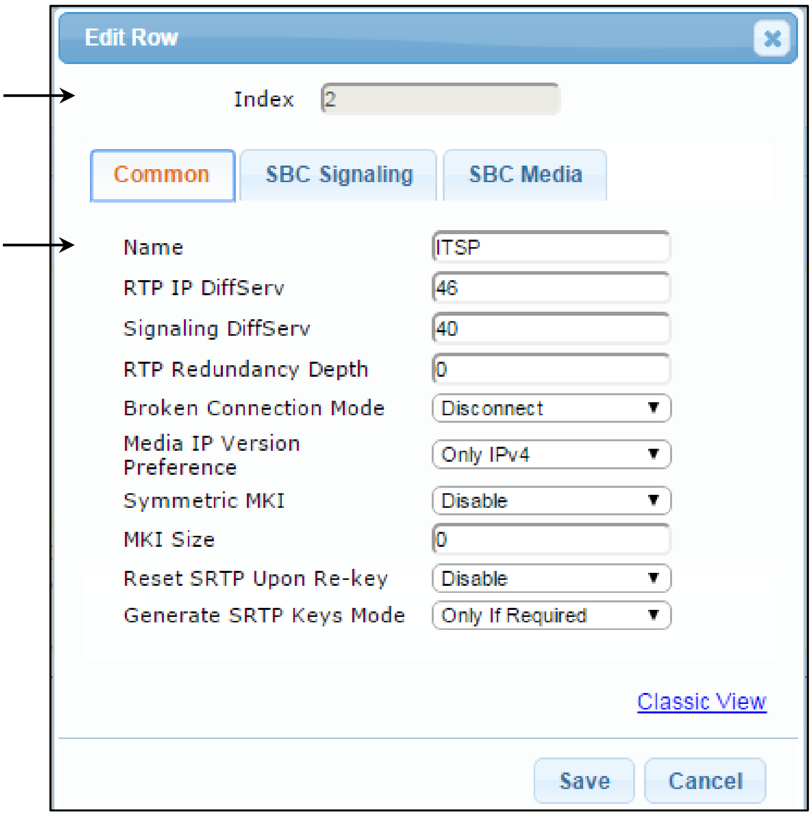
Parameter	Value
Allowed Coders Group ID	'**Coders Group 1**'

Figure 3-20: Configure IP Profile for Genesys Contact Center (SBC Tab)

5. Configure an IP Profile for the Windstream ITSP SIP Trunk:
   a. Click **Add**.
   b. Click the **Common** tab, and then configure the parameters as follows:

Parameter	Value
Index	**2**
Profile Name	**ITSP** (arbitrary descriptive name)

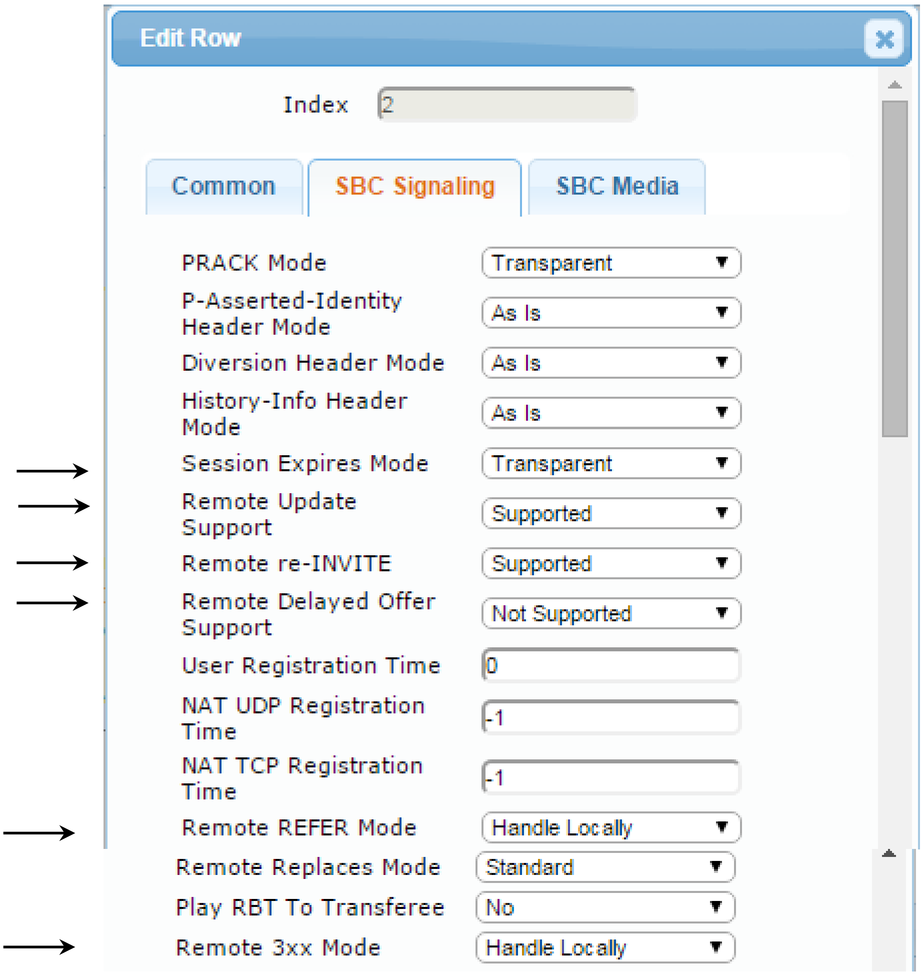
Figure 3-21: Configure IP Profile for ITSP SIP Trunk (Common Tab)



   c. Click the **SBC Signaling** tab and then configure the parameters as follows:

Parameter	Value
Remote REFER Behavior	**'Handle Locally'**
Remote Delayed Offer Support	'**Not Supported**': Windstream 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 Windstream; 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 Update Support (Optional)	**'Supported'/'Not Supported'**
Remote Re-INVITE Support (Optional)	**'Supported'/'Not Supported'**

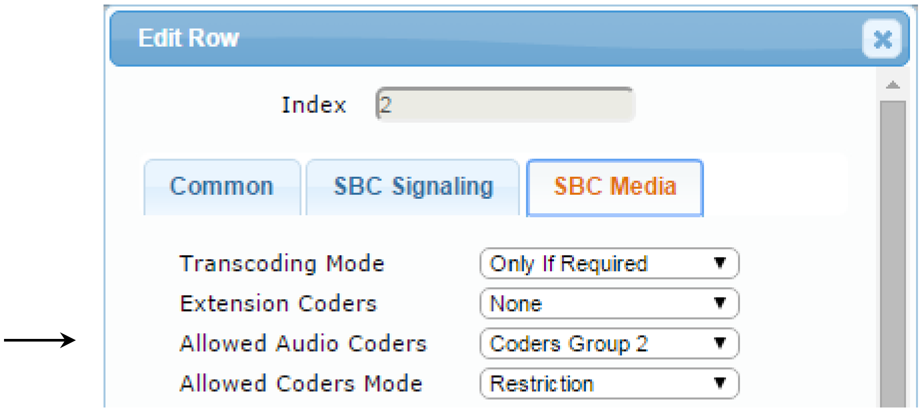
Figure 3-22: Configure IP Profile for ITSP SIP Trunk – SBC Tab



d. Click the **SBC Media** tab, and then configure the parameters as follows:

Parameter	Value
Allowed Coders Group ID	**‘Coders Group 2’**

Figure 3-23: Configure IP Profile for ITSP SIP Trunk – SBC Tab



Notes:

- Windstream 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.

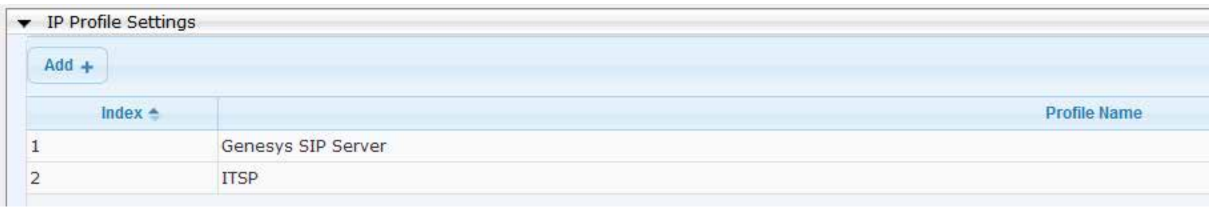
Notes:

- 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 3-24: Configured IP Profiles in IP Profile Table



IP Profile Settings

Add +

Index	Profile Name
1	Genesys SIP Server
2	ITSP

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 Windstream SIP Trunk supports G G.711U-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).

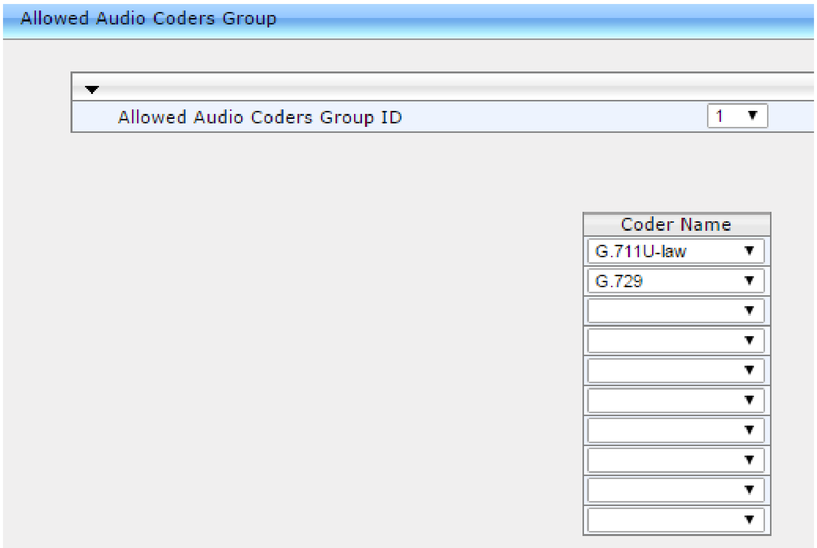
If support for different coders is required in the deployment, an SBC transcoding configuration is required (refer to the *SBC User's Manual*) for Coder Transcoding configuration.

Ø To set a preferred coder for the Windstream SIP & Genesys Trunk:

1. Open the Allowed Coders Group page (**Configuration** tab > **VoIP** > **SBC** > **Allowed Coders Group**).
2. Configure an Allowed Coders Group as follows:

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

Figure 3-25: 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 28, 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):

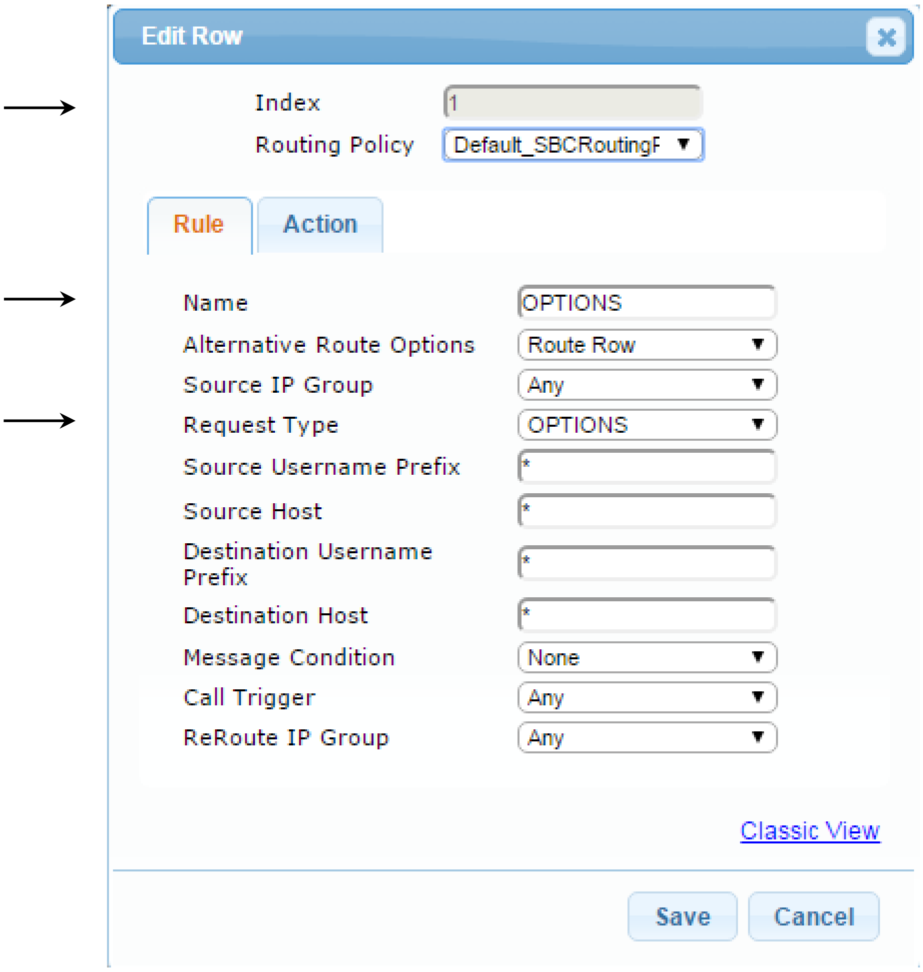
- Terminate SIP OPTIONS messages on the SBC that are received from the LAN/WAN
- Route calls from Genesys Contact Center to the Windstream ITSP SIP Trunk
- Calls from Windstream ITSP SIP Trunk to Genesys Contact Center
- Trigger rules for handling SIP 3xx/REFER for local agents and external DNs

Ø To configure IP-to-IP routing rules:

1. Open the IP-to-IP Routing Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. Configure a rule to terminate SIP OPTIONS messages received from the LAN:
   a. Click **Add**.
   d. Click the **Rule** tab, and then configure the parameters as follows:

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

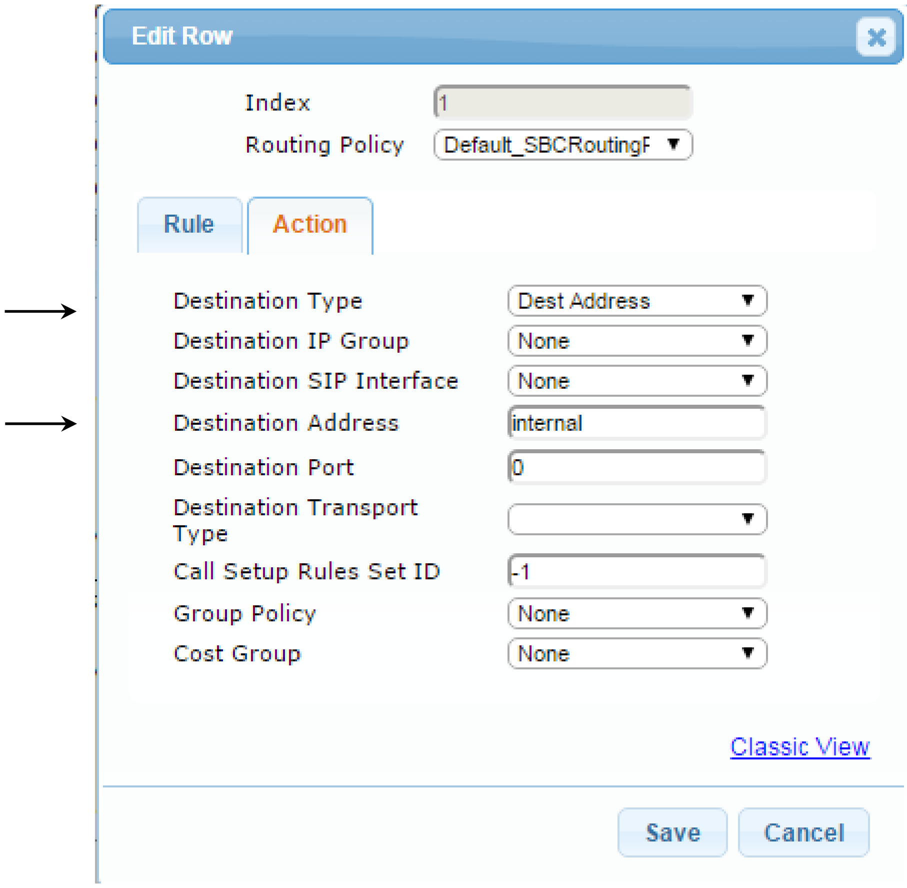
Figure 3-26: Configure IP-to-IP Routing Rule for Terminating SIP OPTIONS - Rule Tab



3. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Destination Type	**Dest Address**
Destination Address	**internal**

Figure 3-27: Configure IP-to-IP Routing Rule for Terminating SIP OPTIONS - Action Tab



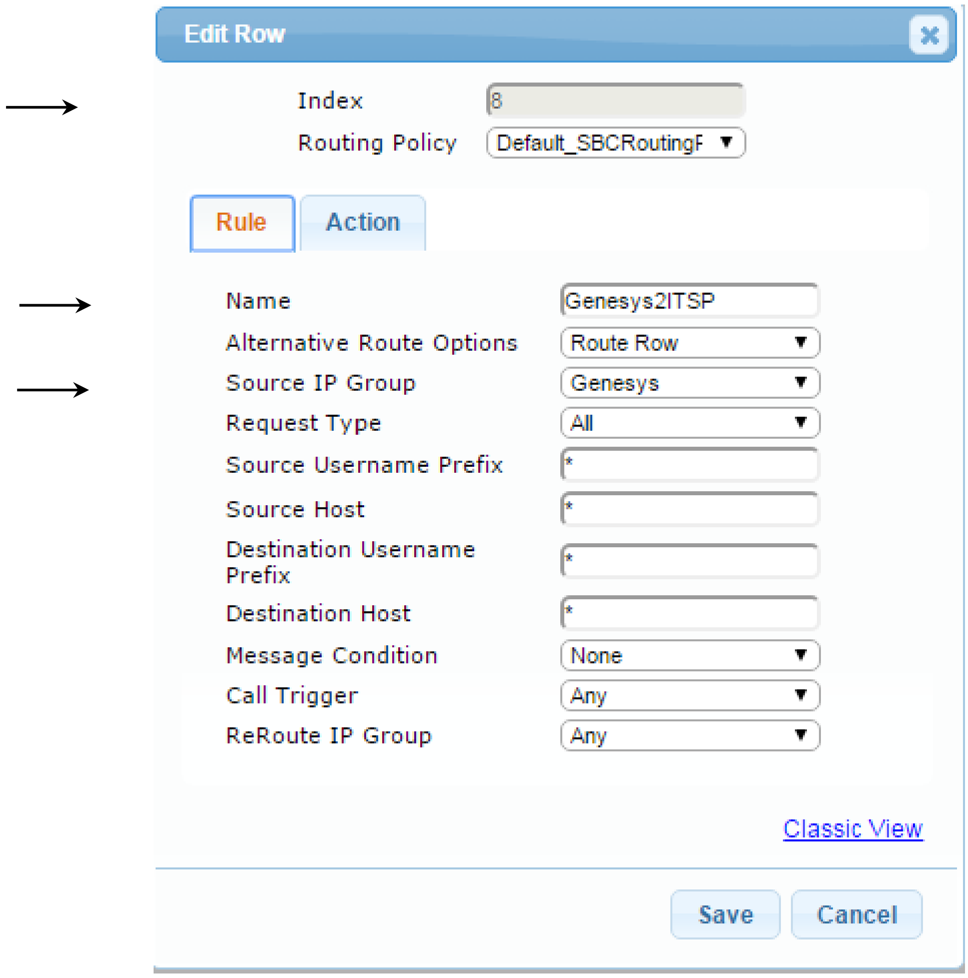
4. Configure a rule to route calls from Genesys Contact Center to Windstream SIP Trunk:

   a. Click **Add**.

   b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	**8**
Route Name	**Genesys2ITSP** (arbitrary descriptive name)
Source IP Group ID	**Genesys**

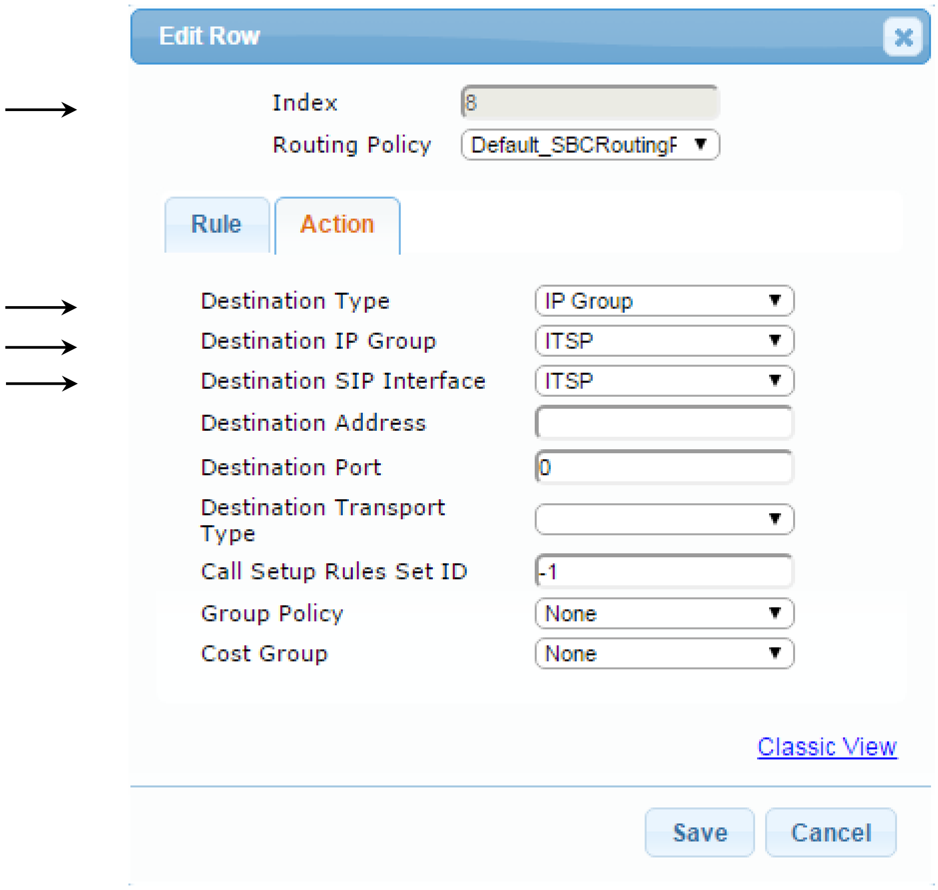
Figure 3-28: Configure IP-to-IP Routing Rule for Genesys to ITSP – Rule tab



5. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Destination Type	**IP Group**
Destination IP Group ID	**2**
Destination SIP Interface	**2**

Figure 3-29: Configure IP-to-IP Routing Rule for Genesys to ITSP – Action tab



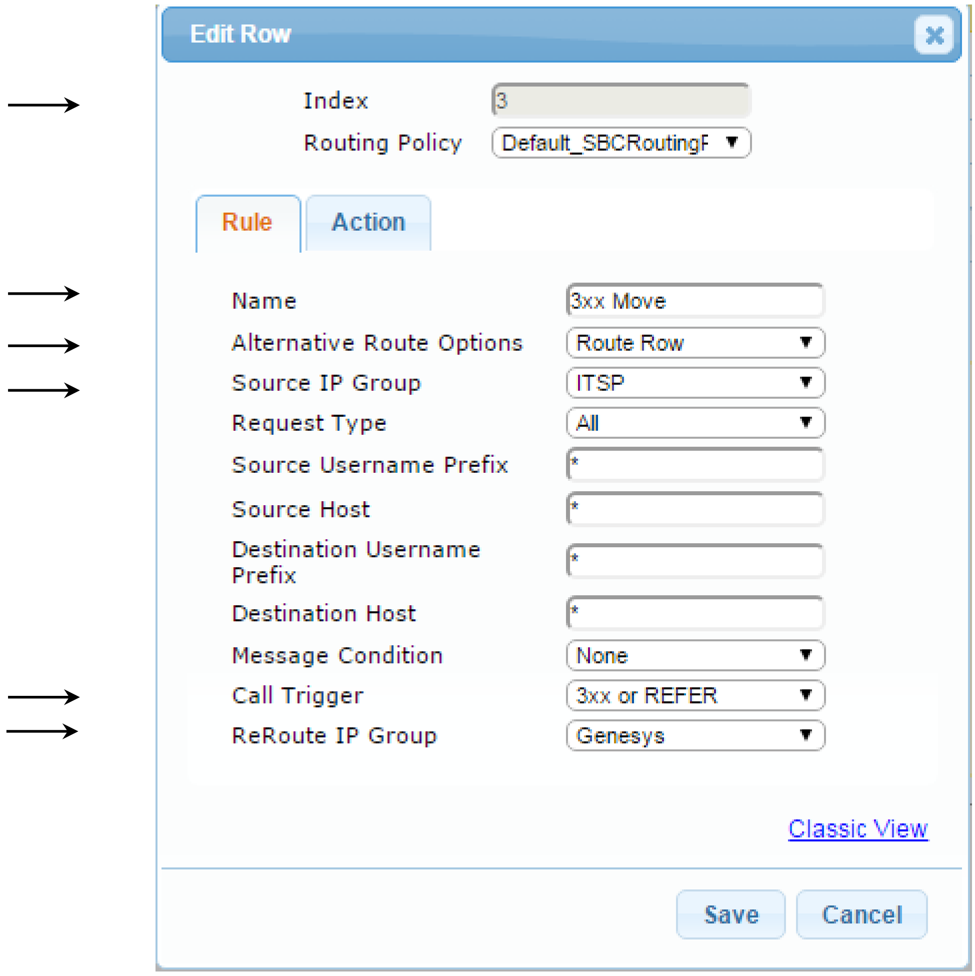
6. Configure a trigger rule to route local Agent REFERS to the network from to the Genesys Contact Center back to Genesys SIP Server:

   a. Click **Add**.

   b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	**3**
Route Name	**3xx/Refer local** (arbitrary descriptive name)
Source IP Group ID	**ITSP**
Call Trigger	**3xx or REFER**
ReRoute IP Group	**Genesys**

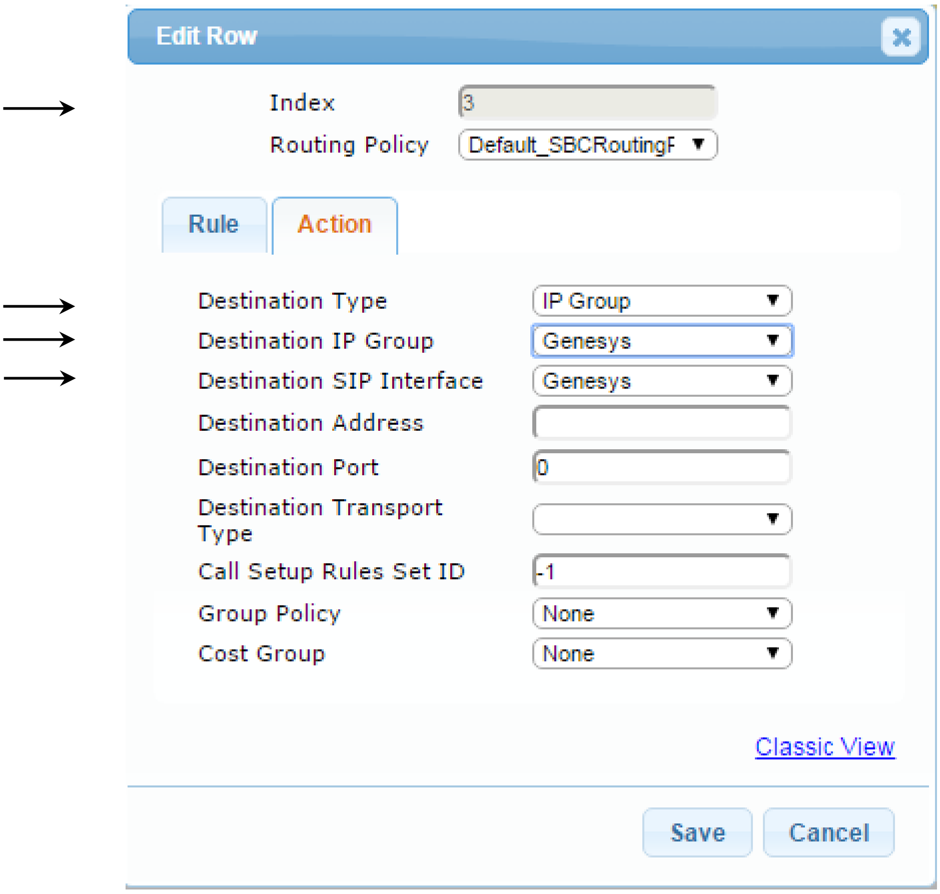
Figure 3-30: Configure IP-to-IP Routing Trigger Rule for 3xx/REFER to local agents – Rule tab



7. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Destination Type	**IP Group**
Destination IP Group ID	**Genesys**
Destination SRD ID	**Genesys**

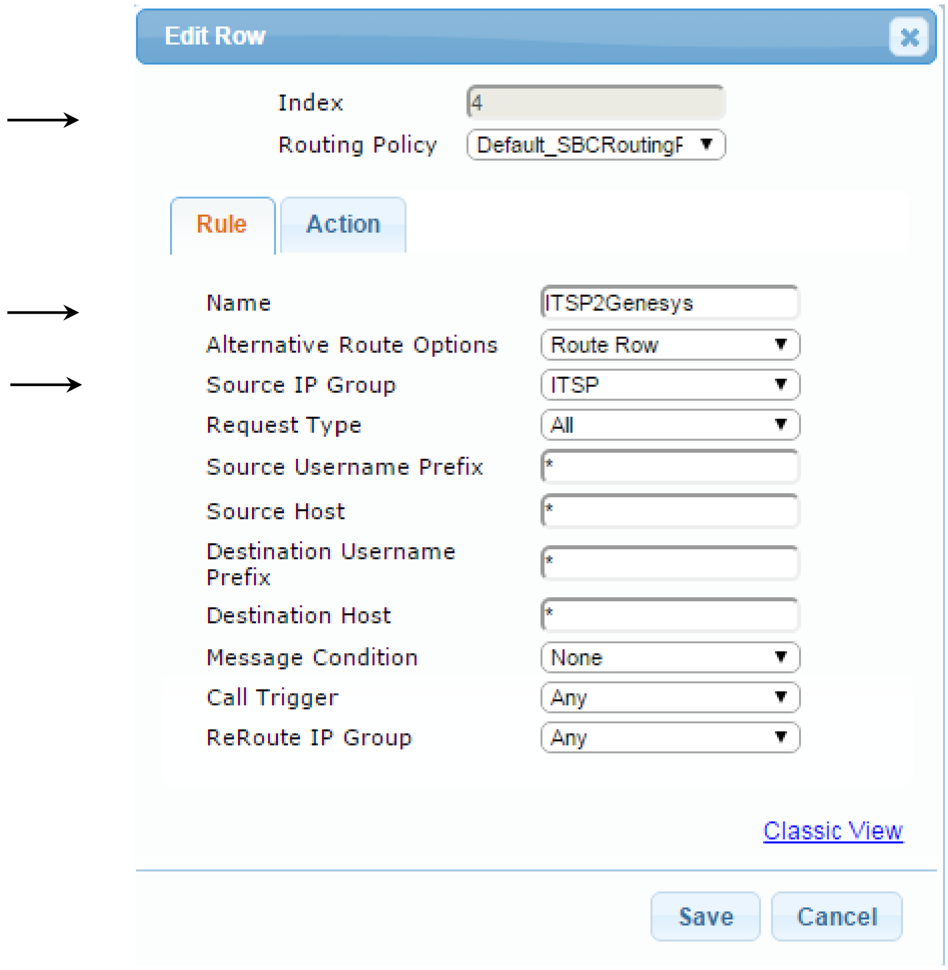
Figure 3-31: Configure IP-to-IP Routing Rule for Trigger Rule for 3xx/REFER to local agents – Action Tab



8. Configure a rule to route calls from ITSP SIP Trunk to the Genesys Contact Center:
   a. Click **Add**.
   b. Click the **Rule** tab, and then configure the parameters as follows:

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

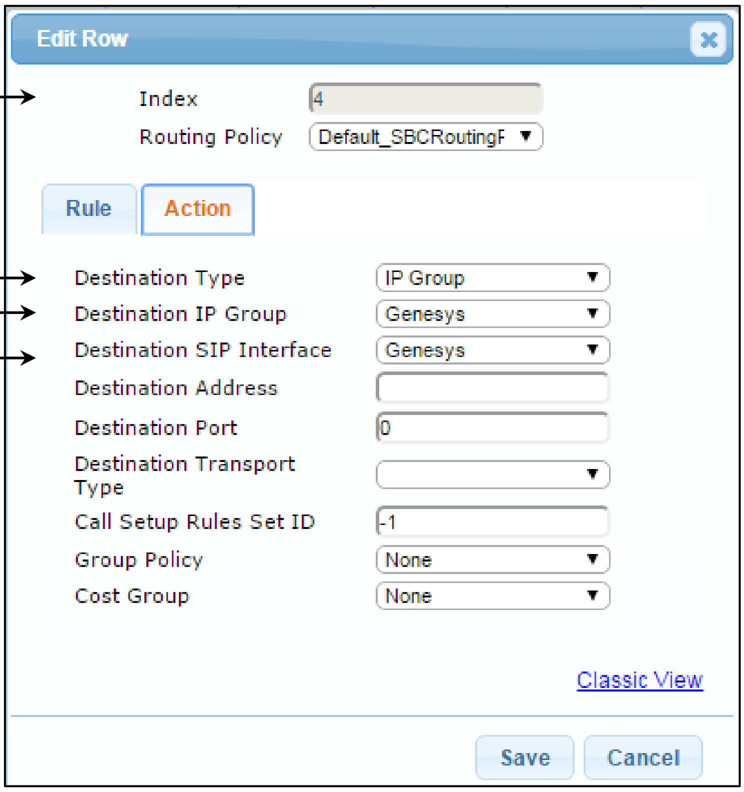
Figure 3-32: Configure IP-to-IP Routing Rule for ITSP to Genesys – Rule tab



9. Click the **Action** tab, and then configure the parameters as follows:

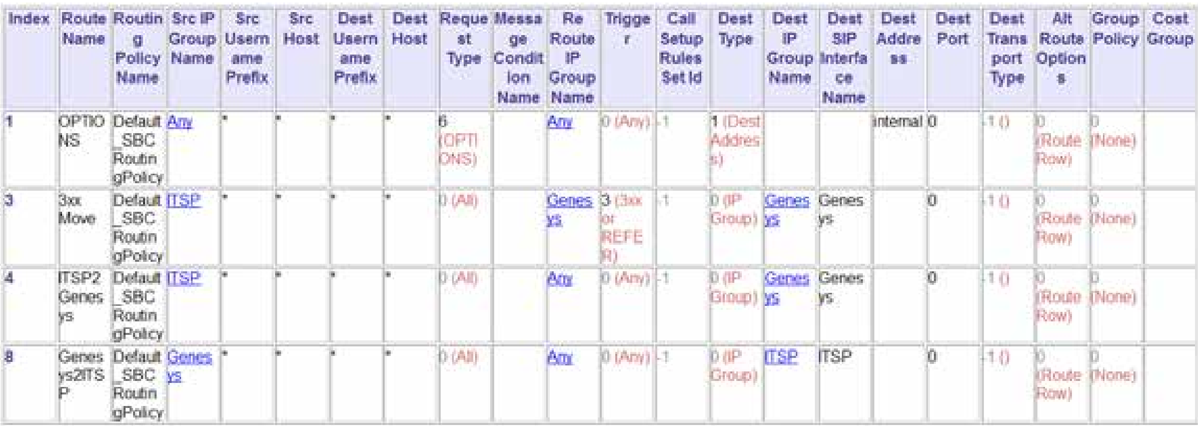
Parameter	Value
Destination Type	**IP Group**
Destination IP Group ID	**1**
Destination SRD ID	**1**

Figure 3-33: Configure IP-to-IP Routing Rule for ITSP to Genesys – Action tab



The configured routing rules are shown in the figure below:

Figure 3-34: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table



Index	Route Name	Routing Policy Name	Src IP Group Name	Src Username Prefix	Src Host	Dest Username Prefix	Dest Host	Request Type	Message Condition Name	ReRoute IP Group Name	Trigger	Call Setup Rules Set Id	Dest Type	Dest IP Group Name	Dest SIP Interface Name	Dest Address	Dest Port	Dest Transport Type	Alt Route Options	Group Policy	Cost Group
1	OPTIONS	Default_SBCRoutingPolicy	Any	*	*	*	*	6 (OPTIONS)		Any	0 (Any)	-1	1 (Dest Address)			internal	0	-1 ()	0 (Route Row)	0 (None)	
3	3xx Move	Default_SBCRoutingPolicy	ITSP	*	*	*	*	0 (All)		Genesys	3 (3xx or REFER)	-1	0 (IP Group)	Genesys	Genesys		0	-1 ()	0 (Route Row)	0 (None)	
4	ITSP2Genesys	Default_SBCRoutingPolicy	ITSP	*	*	*	*	0 (All)		Any	0 (Any)	-1	0 (IP Group)	Genesys	Genesys		0	-1 ()	0 (Route Row)	0 (None)	
8	Genesys2ITSP	Default_SBCRoutingPolicy	Genesys	*	*	*	*	0 (All)		Any	0 (Any)	-1	0 (IP Group)	ITSP	ITSP		0	-1 ()	0 (Route Row)	0 (None)	

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.

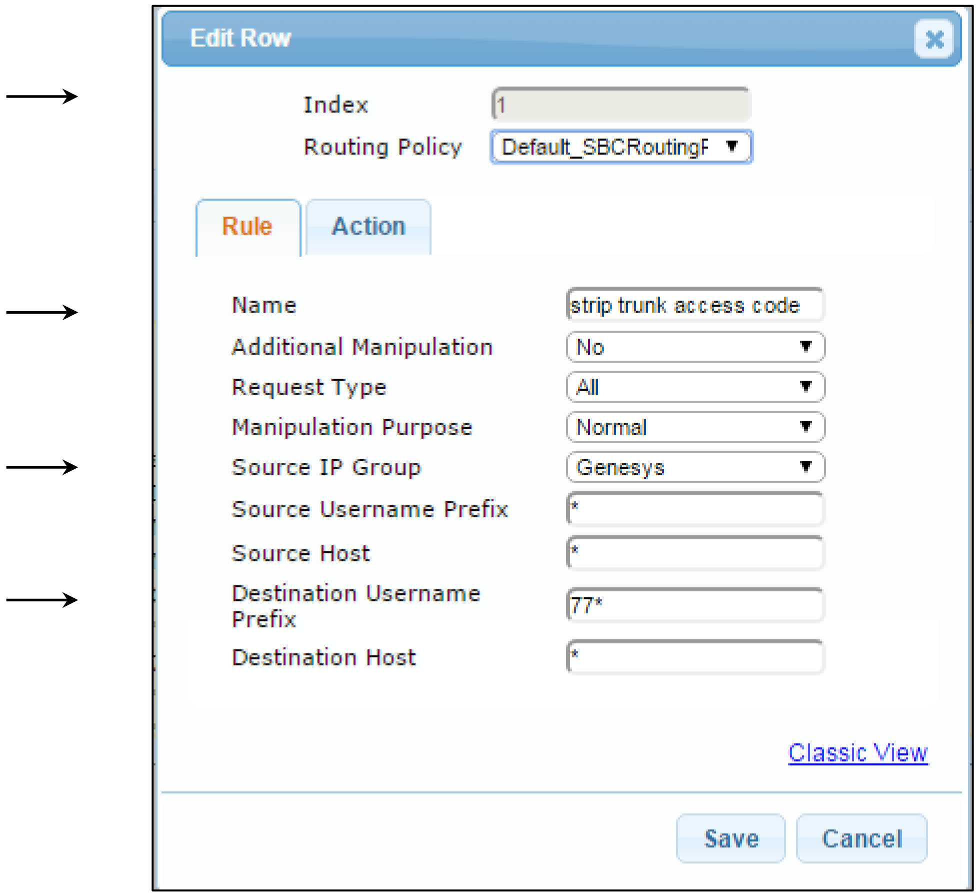
Manipulations may be required to strip digits for an access code to the SBC from the Genesys SIP Server or for removing the country code and/or leading prefixes to map ITSP numbers to the DNs used in the Genesys environment.

Ø **To configure a number manipulation rule to remove the Country Code from messages arriving from the ITSP destined for the Genesys SIP Server:**

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

Parameter	Value
Index	**1**
Manipulation Name (optional)	**Strip trunk access code**
Source IP Group ID	**Genesys**
Request Type	**INVITE and REGISTER**
Manipulated URI	**Destination**

Figure 3-35: Configure IP-to-IP Inbound Manipulation Rule – Rule Tab

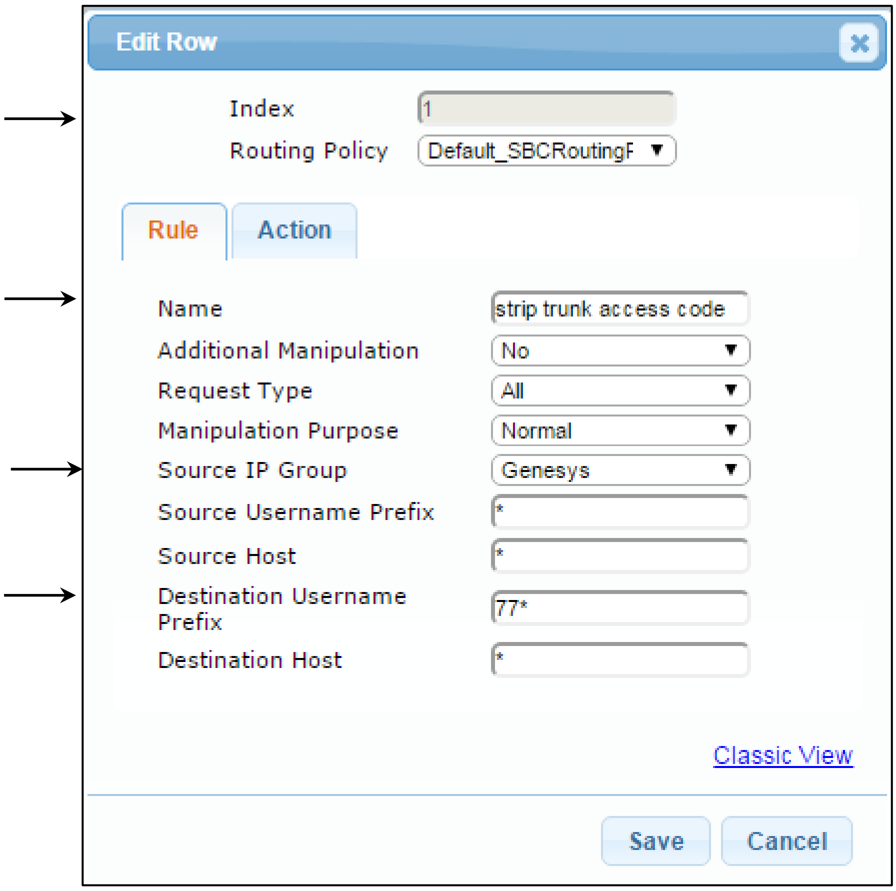


Ø **To configure a number manipulation rule to remove the trunk access code from messages arriving from Genesys destined for the ITSP:**

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

Parameter	Value
Index	**1**
Manipulation Name (optional)	**rm SBC access code**
Source IP Group ID	**Genesys**
Destination Username Prefix	**77**

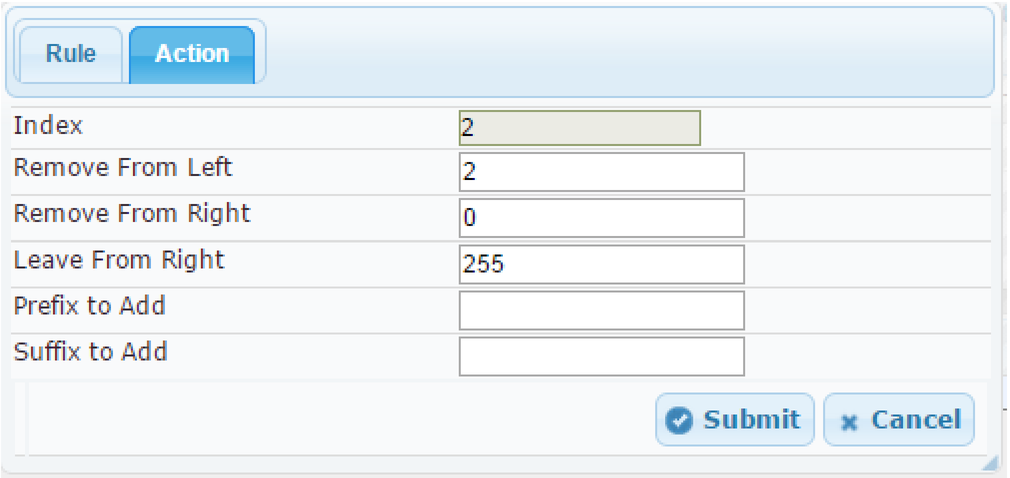
Figure 3-36: Configure IP-to-IP Inbound Manipulation Rule – Rule Tab



4. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Manipulated URI	**Destination**
Remove from Left	**2**

Figure 3-37: Configure IP-to-IP Inbound Manipulation Rule - Action Tab



5. Click **Submit**.

The figure below shows an example of configured IP-to-IP inbound manipulation rule for calls between IP Group 2 (i.e., Genesys Contact Center) and IP Group 1 (i.e., ITSP SIP Trunk):

Figure 3-38: Example of Configured IP-to-IP Inbound Manipulation Rules

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).

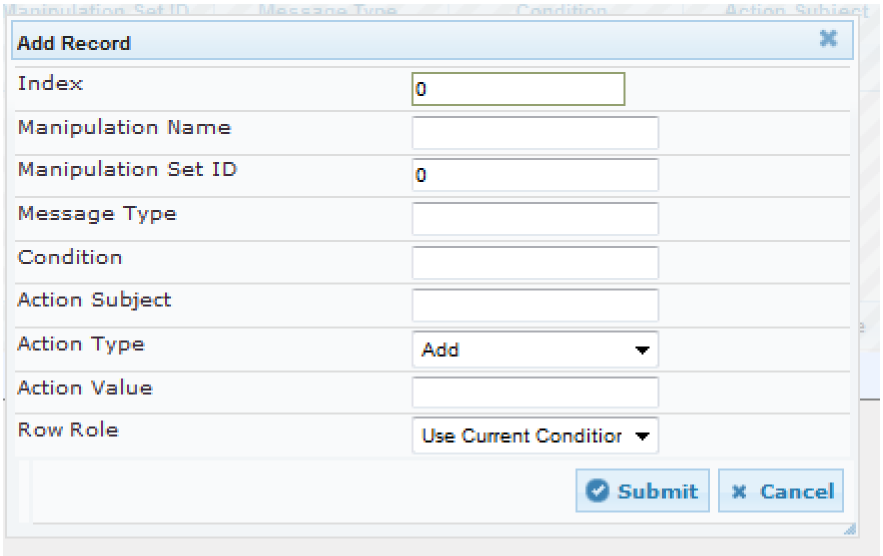
For this interoperability test, message manipulations were applied only to the outbound messages, to the ITSP SIP trunk, for the purposes of modifying existing SIP headers, topology hiding, and adding new SIP headers.

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

Ø To configure SIP Message Manipulation rules:

1. Open the IP-to-IP Inbound Manipulation page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Click **Add**; this screen opens:

Figure 3-38: Configure IP-to-IP Inbound Manipulation Rule - Action Tab



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.

[MessageManipulations]

Index	Manipulation Name	Man Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
7	URI host	1	Any	header.REQUEST-URI.url.host == '10.38.5.116'	header.REQUEST-URI.url.host	2 (Modify)	'gw0.itsp-iot.com'	0 (Use Current Condition)
8	To	1	Any	header.to.url.host == '10.38.5.116'	header.to.url.host	2 (Modify)	'gw0.itsp-iot.com'	1 (Use Previous Condition)
9	From Host	1	Any	Header.From.Url.Host contains '10.38.5.116'	Header.From.Url.Host	2 (Modify)	'203.0.113.120'	0 (Use Current Condition)
12	Call Transfer	1	Any	header.referred-by exists	header.referred-by.url.host	2 (Modify)	header.from.url.host	0 (Use Current Condition)
13	Call Transfer	1	Any	header.referred-by exists	header.from.url.user	2 (Modify)	header.referred-by.url.user	0 (Use Current Condition)
15	Refer to	1			header.refer-to.url.host	2 (Modify)	'gw0.itsp-iot.com'	0 (Use Current Condition)
16	Referred-by	1		header.referred-by exists	header.referred-by.url.host	2 (Modify)	'203.0.113.120'	0 (Use Current Condition)
19	PAI host	1	Any	header.P-Asserted-Identity exists	header.P-Asserted-Identity.url.host	2 (Modify)	'203.0.113.120'	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 1 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.

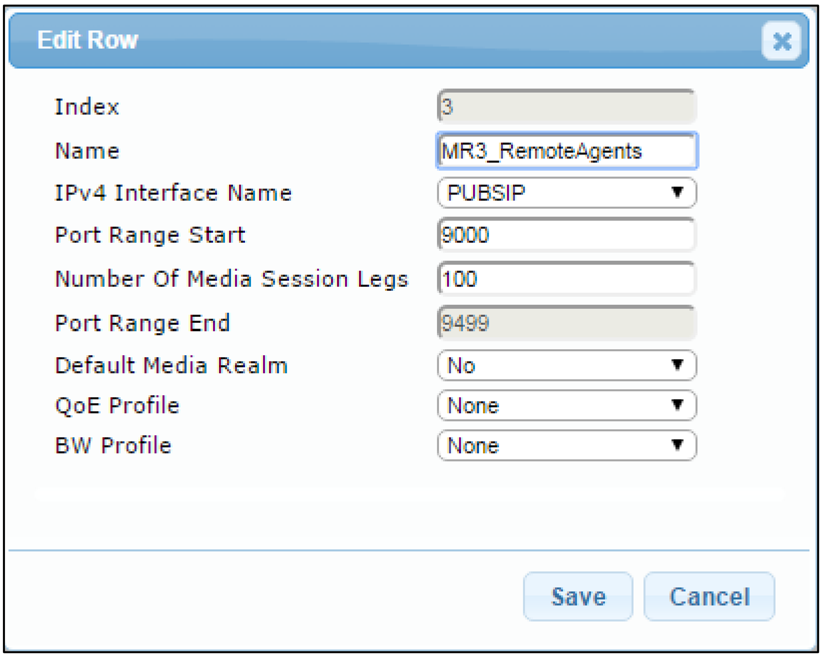
3.11.1 Step 11a: Configure Media Realm for a Remote Agent

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.

Ø To configure the Media Realm for a Remote Agent:

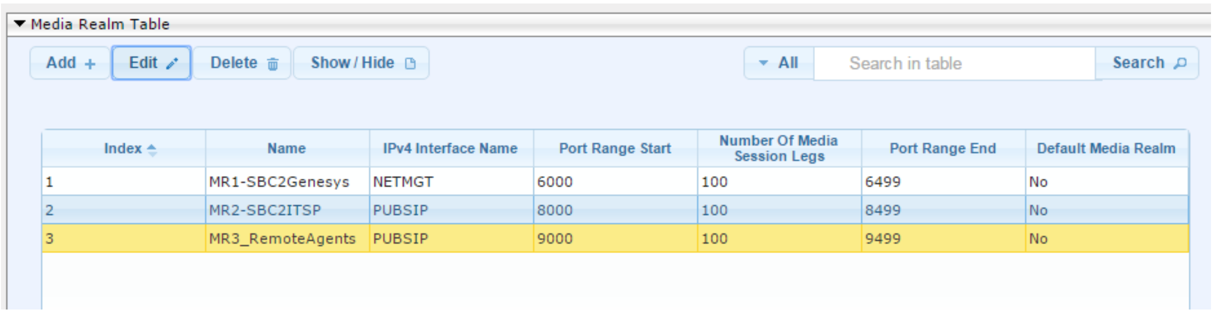
1. Open the **Advanced Parameters** page (**Configuration** tab > **VoIP** menu > **Media Realm Table**).

Figure 3-39: 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 3-40: 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
1	MR1-SBC2Genesys	NETMGT	6000	100	6499	No
2	MR2-SBC2ITSP	PUBSIP	8000	100	8499	No
3	MR3_RemoteAgents	PUBSIP	9000	100	9499	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.

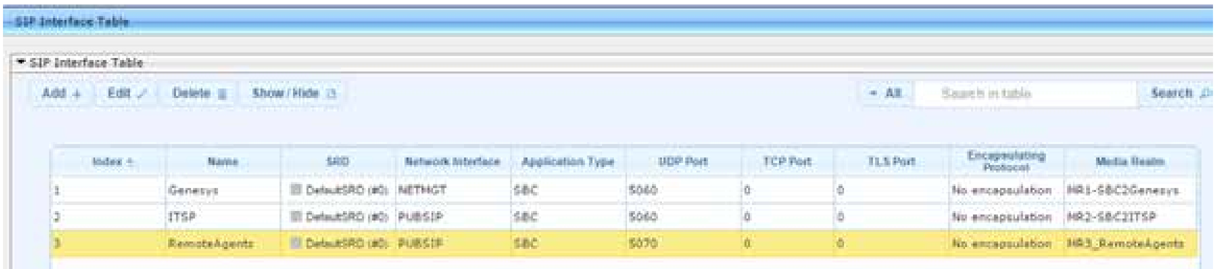
Ø **To configure SIP interfaces for a Remote Agent:**

1. Open the SIP Interface Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SIP Interface Table**).
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 3-41: Configured SIP Interfaces for Remote Agents in SIP Interface Table



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.

Ø To configure an IP User Group:

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
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**

Figure 3-42: Configure an IP Group for the Remote (User) Agents (Common Tab)

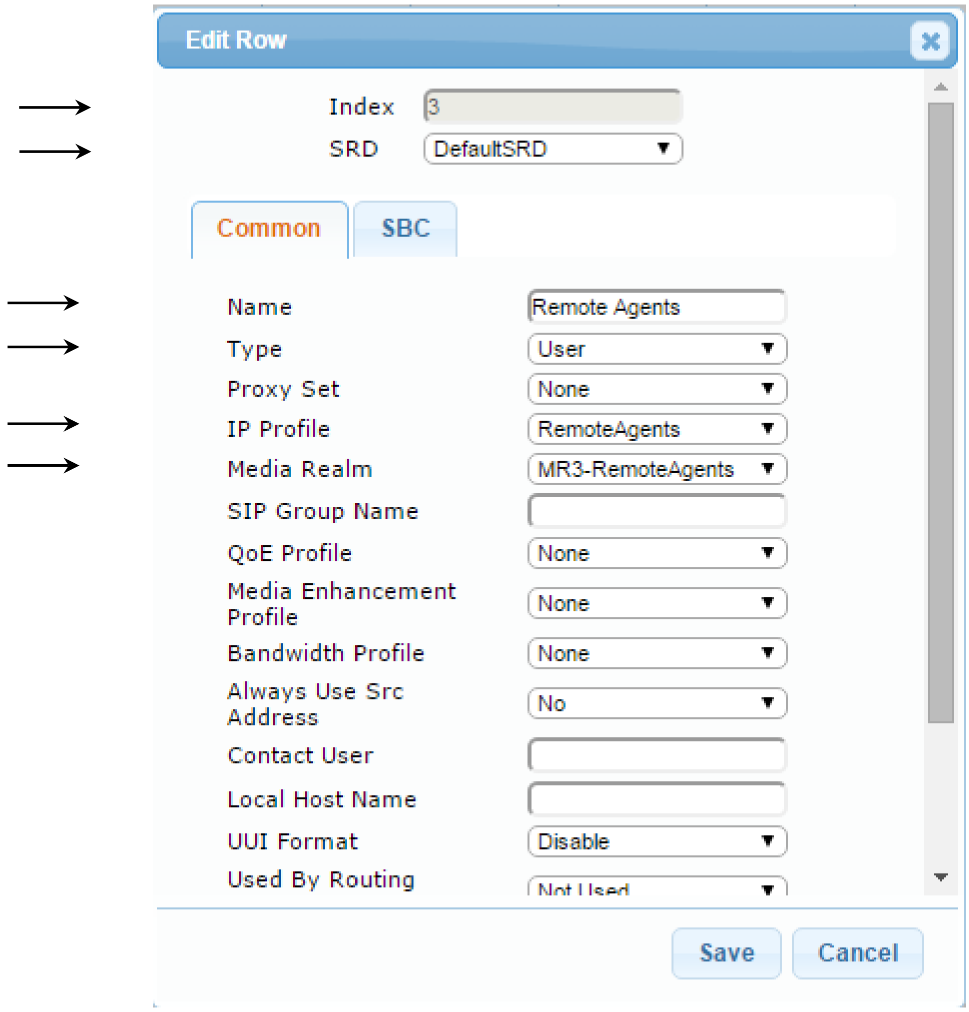
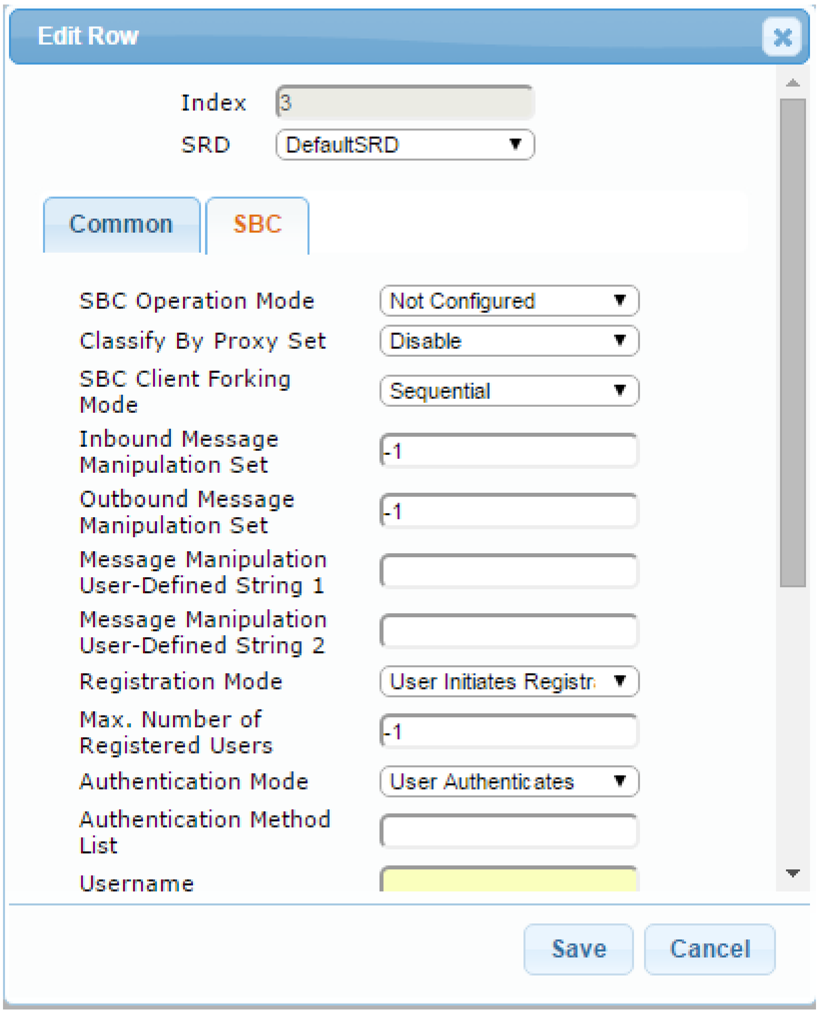
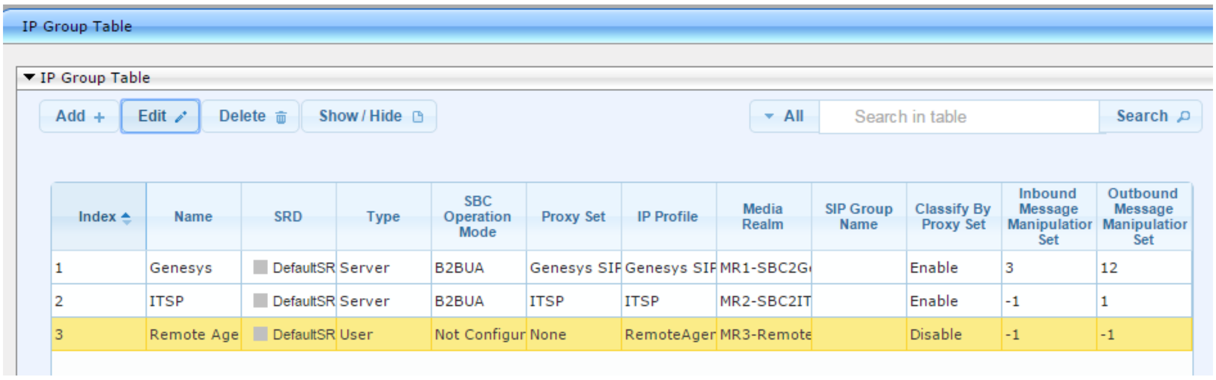


Figure 3-43: Configure an IP Group for Remote User Agents (SBC Tab)



The configured IP Groups are shown in the figure below:

Figure 3-44: Configured IP Group for Remote Users in IP Group Table



IP Group Table

IP Group Table

Add + Edit Delete Show / Hide All Search in table Search

Index	Name	SRD	Type	SBC Operation Mode	Proxy Set	IP Profile	Media Realm	SIP Group Name	Classify By Proxy Set	Inbound Message Manipulatior Set	Outbound Message Manipulatior Set
1	Genesys	DefaultSR	Server	B2BUA	Genesys SIF	Genesys SIF	MR1-SBC2G		Enable	3	12
2	ITSP	DefaultSR	Server	B2BUA	ITSP	ITSP	MR2-SBC2IT		Enable	-1	1
3	Remote Age	DefaultSR	User	Not Configur	None	RemoteAger	MR3-Remote		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.

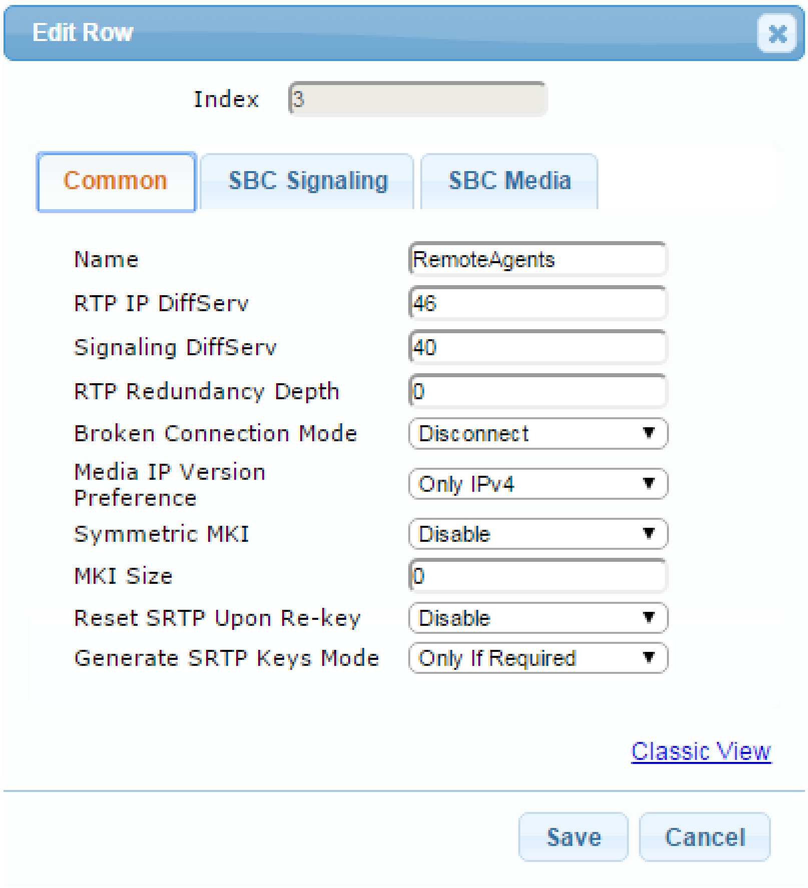
Note: The IP Profile index values were assigned to the IP Groups in the previous step (see Section 3.5 on page 28).

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

1. Open the IP Profile Settings page (**Configuration** tab > **VoIP** > **Coders and Profiles** > **IP Profile Settings**).
2. Click **Add**.
3. Click the **Common** tab, and then configure the parameters as follows:

Parameter	Value
Index	**3**
Profile Name	**Remote Users** (arbitrary descriptive name)

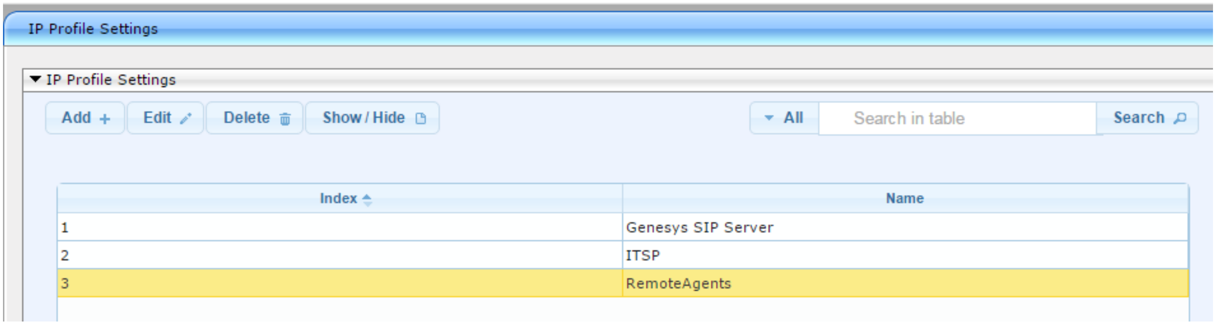
Figure 3-45: Configure IP Profile for Remote Users (Common Tab)



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 3-46: Configured IP Profiles in IP Profile Table



3.11.5 Step 11e: Configure Classification Table for Remote Agents

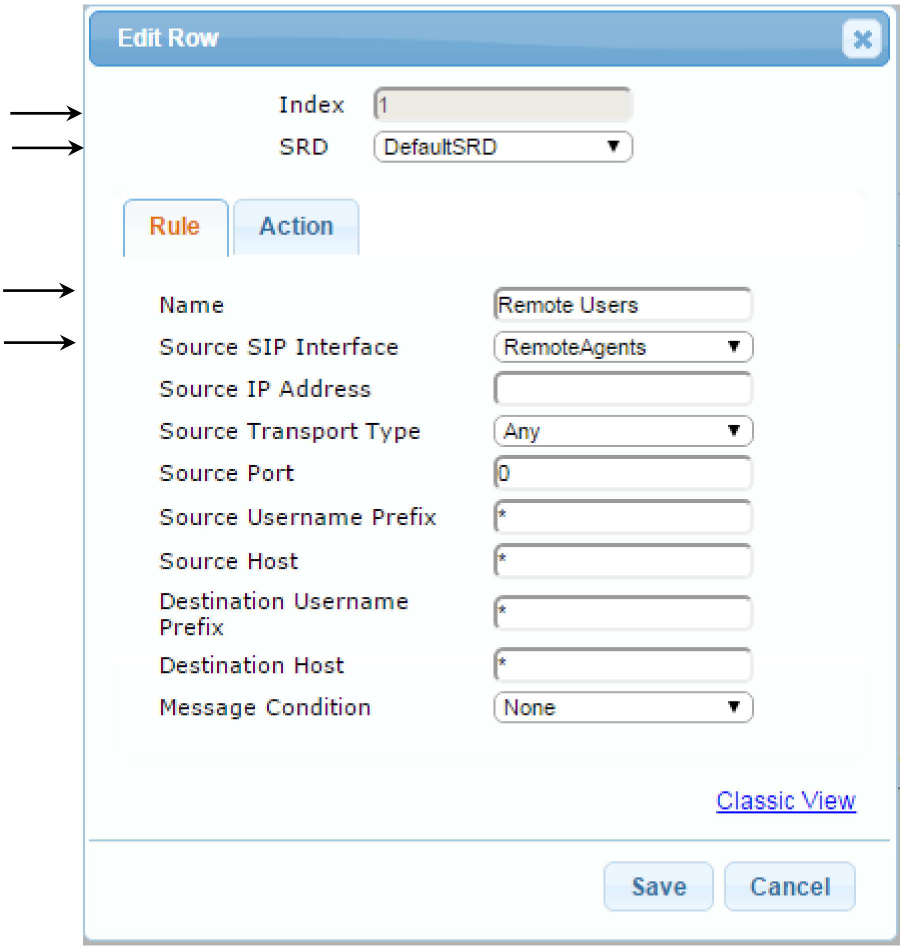
This step describes how to configure the Classification table for Remote Agents. The Classification rules classify incoming SIP dialog-initiating requests to an IP Group from where the SIP dialog request was received. The identified IP Group is then used in the manipulation and routing processes. For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

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

1. Open the Classification Table page (**Configuration** tab > **VoIP** > **SBC** > **Routing SBC > Classification Table**).
2. Click **Add**.
3. On the **Rule** tab, configure the parameters as follows:

Parameter	Value
Index	**1**
Classification Name	**Remote Users** (arbitrary descriptive name)
Source SIP Interface	**RemoteAgents**

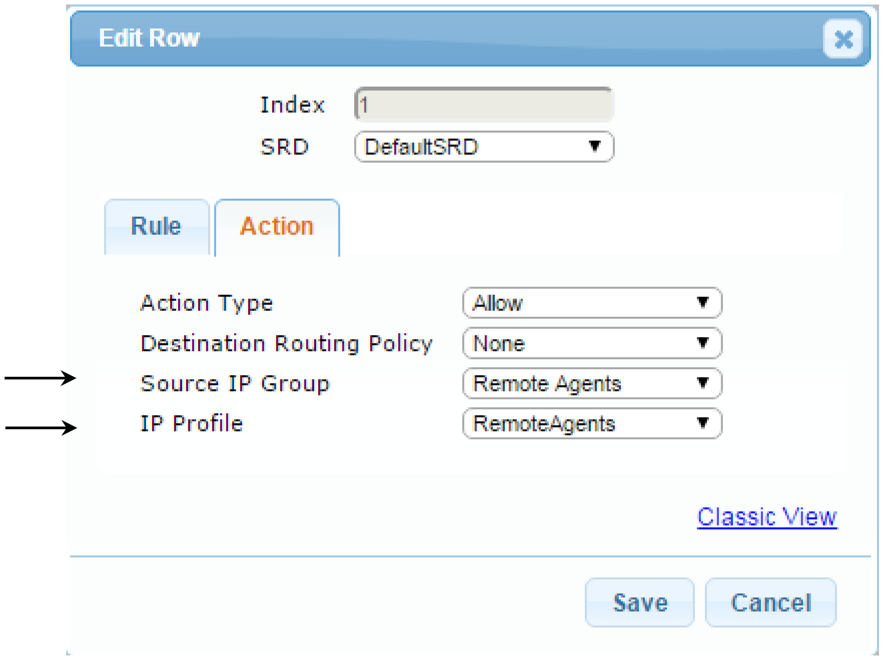
Figure 3-47: Configure Rule Tab of the Classification Table



4. On the **Action** tab, configure the parameters as follows:

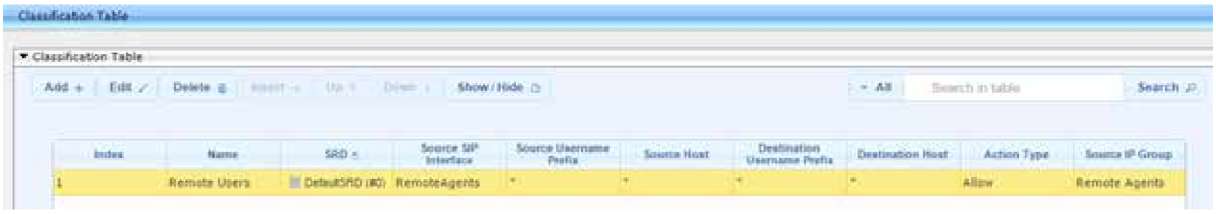
Parameter	Value
Source IP Group ID	**Remote Agents**
IP Profile	**RemoteAgents**

Figure 3-48: Configured IP Profiles in IP Profile Table



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

Figure 3-49: Configured Classification Rule for Remote (Users) Agents



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 59) and the Genesys SIP Server.

The following IP-to-IP call routing rules were configured (see Section 3.8 on page 39):

- 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

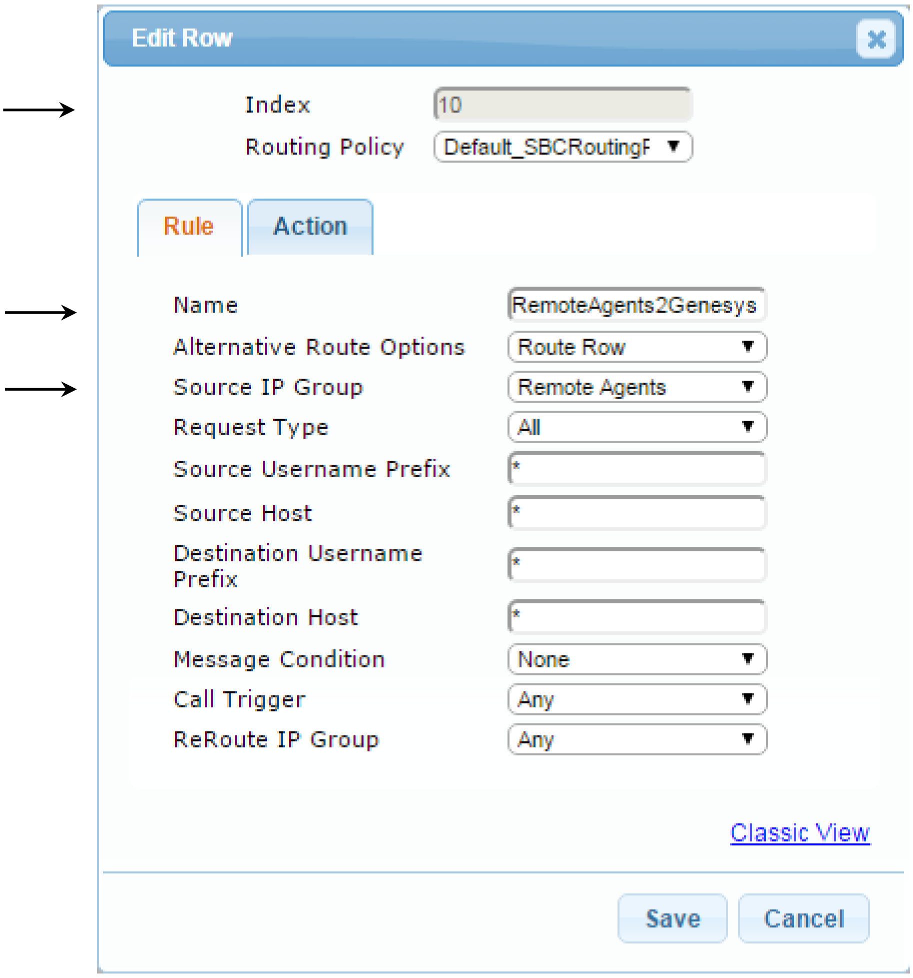
For the interoperability test topology, IP-to-IP routing rules were configured to route SIP messages between the Remote (User) Agents and the Genesys SIP Server, and to ensure that the messages are routed back to the correct user group to reach the intended agent.

Ø To configure IP-to-IP routing rules:

1. Open the IP-to-IP Routing Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. Configure a rule to route between the Remote Agent and the Genesys SIP Server:
   a. Click **Add**.
   b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	**10**
Route Name	**RemoteAgents2Genesys** (arbitrary descriptive name)
Source IP Group ID	**Remote Agents**

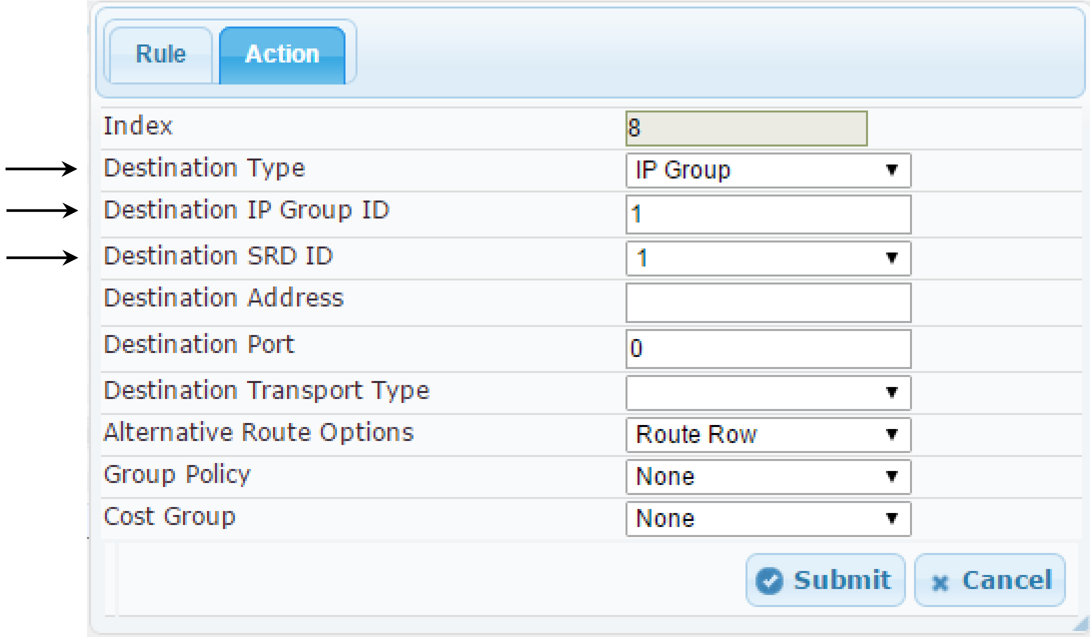
Figure 3-50: Configure IP-to-IP Routing Rule for Terminating RemoteAgents2Genesys – Rule Tab



3. Click the **Action** tab, configure the parameters as follows, and then click **Submit**.

Parameter	Value
Destination Type	**IP Group**
Destination IP Group ID	**Genesys**
Destination SIP Interface	**Genesys**

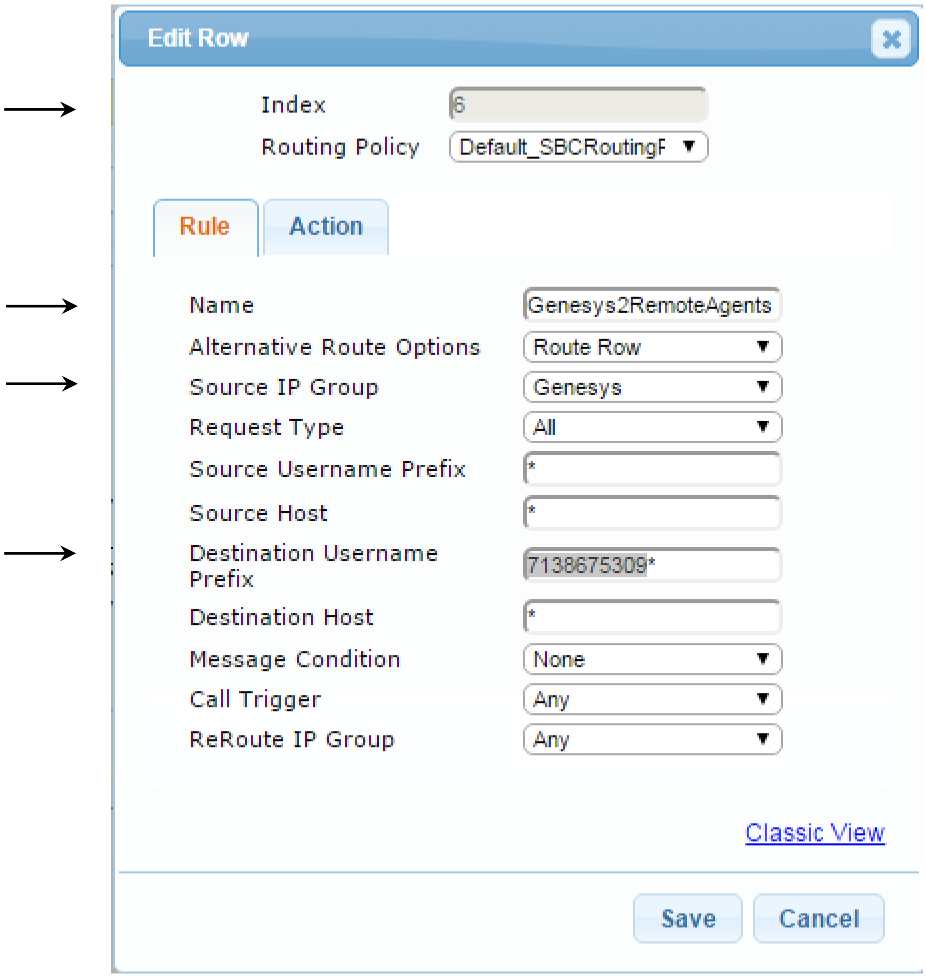
Figure 3-51: Configure IP-to-IP Routing Rule for Terminating RemoteAgents2Genesys – Action Tab



4. Configure a rule to route calls from the Genesys Contact Center to the Remote User Agent Group. Note that in this case the rule is inserted in the IP-to-IP Routing table above the routing rule that already exists for calls from IP Group 1 (Genesys) toward the ITSP IP Group 2. For the Genesys to Remote Agent routing rule, the destination number is used to differentiate these calls from those calls that will be routed to the ITSP. For calls in the Remote Agent group, the SBC will determine the next destination from the Address of Record (AOR) table.
   a. Select Index 1 (Genesys2ITSP route), and then click **Insert +**.
   b. Click the **Rule** tab, configure the parameters as follows, and then click **Submit**.

Parameter	Value
Index	**6**
Route Name	**Genesys2RemoteAgents** (arbitrary descriptive name)
Source IP Group ID	**Genesys**
Destination Username Prefix	**7138675309***

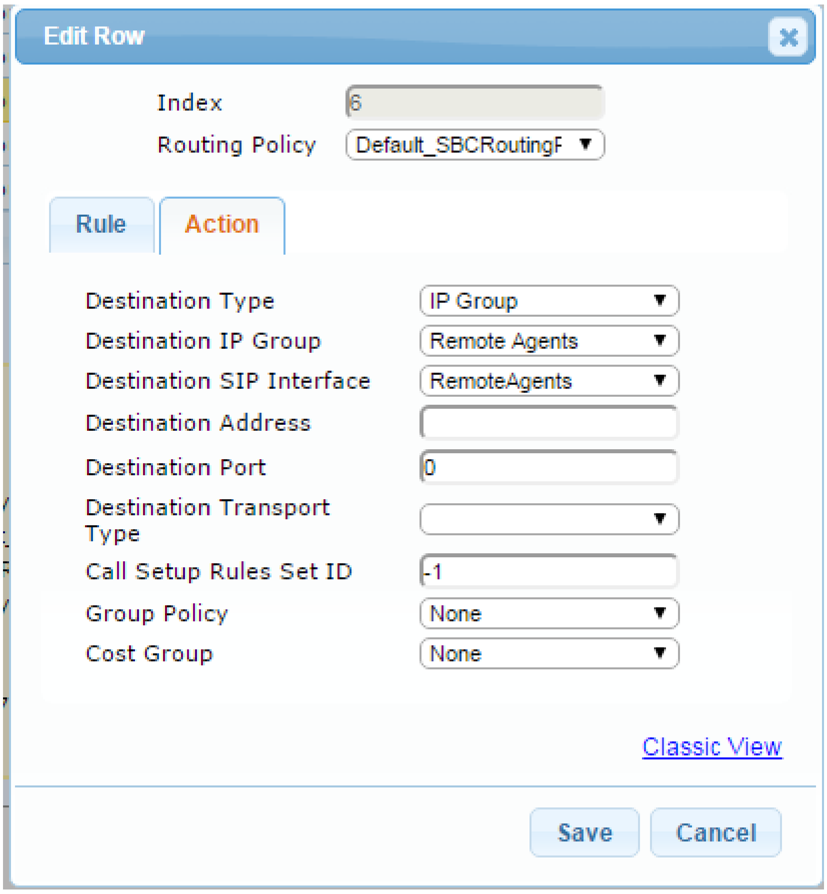
Figure 3-52: Configure IP-to-IP Routing Rule for Genesys to Remote Agent Group – Rule tab



5. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Destination Type	**IP Group**
Destination IP Group ID	**Remote Agents**
Destination SRD ID	**RemoteAgents**

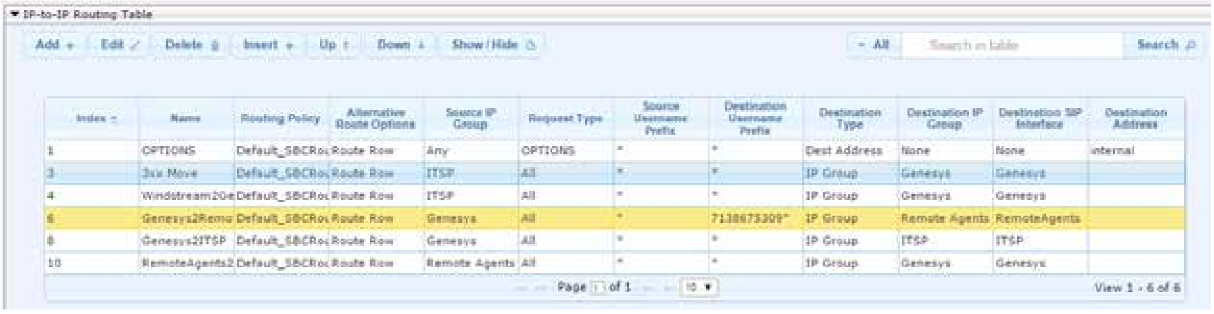
Figure 3-53: Configure IP-to-IP Routing Rule for Genesys to SIP Trunk – Action tab



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

Note: 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.

Figure 3-54: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table


IP-to-IP Routing Table

Add Edit Delete Insert Up Down Show / Hide — All — Search in table — Search

Index	Name	Routing Policy	Alternative Route Options	Source IP Group	Request Type	Source Username Prefix	Destination Username Prefix	Destination Type	Destination IP Group	Destination SIP Interface	Destination Address
1	OPTIONS	Default_SBCRo	Route Row	Any	OPTIONS	*	*	Dest Address	None	None	internal
3	3xx Move	Default_SBCRo	Route Row	ITSP	All	*	*	IP Group	Genesys	Genesys	
4	Windstream2Ge	Default_SBCRo	Route Row	ITSP	All	*	*	IP Group	Genesys	Genesys	
6	Genesys2Remo	Default_SBCRo	Route Row	Genesys	All	*	7138675309*	IP Group	Remote Agents	RemoteAgents	
8	Genesys2ITSP	Default_SBCRo	Route Row	Genesys	All	*	*	IP Group	ITSP	ITSP	
10	RemoteAgents2	Default_SBCRo	Route Row	Remote Agents	All	*	*	IP Group	Genesys	Genesys	

Page 1 of 1 — 10 — View 1 - 6 of 6

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.

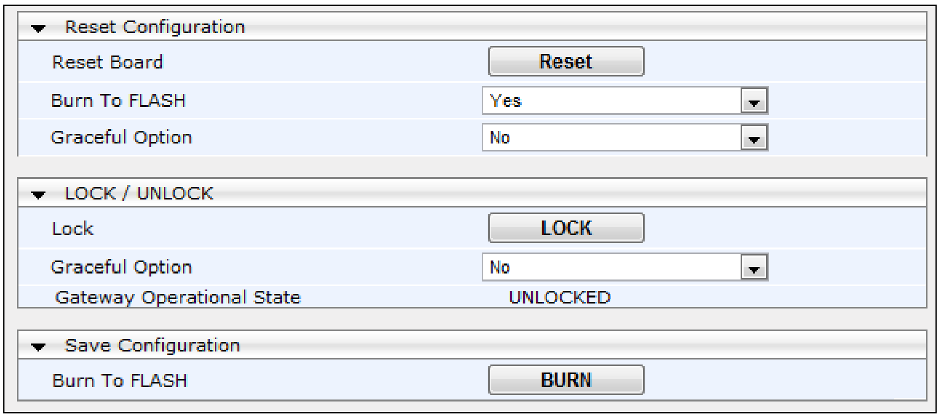
3.12 Step 12: Reset the SBC

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.

Ø To save the configuration to flash memory:

1. Open the Maintenance Actions page (**Maintenance** tab > **Maintenance** menu > **Maintenance Actions**).

Figure 3-55: Resetting the SBC



2. Make sure that the 'Burn 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 17.

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

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

;Board: Mediant SW
;Board Type: 73
;Serial Number: 115991455101440
;Product Key:
;Slot Number: 1
;Software Version: 7.00A.040.004
;DSP Software Version: SOFTDSP => 700.40
;Board IP Address: 192.168.20.200
;Board Subnet Mask: 255.255.255.0
;Board Default Gateway: 192.168.20.1
;Ram size: 7700M Flash size: 0M
;Num of DSP Cores: 0 Num DSP Channels: 0
;Profile: NONE
;;;Key features:;Board Type: Mediant SW ;Max SW Ver: 9.80;DSP Voice features: ;DATA
features: ;Security: IPSEC MediaEncryption StrongEncryption EncryptControlProtocol
;Channel Type: DspCh=0 ;HA ;Control Protocols: MGCP SIP SBC=2000 MSFT CLI
TestCall=2000 EMS ;Default features:;Coders: G711 G726;


;MAC Addresses in use:
;---------------------------
;GROUP_1 - 6c:3b:e5:51:49:68
;GROUP_2 - 6c:3b:e5:51:49:69
;GROUP_3 - e4:11:5b:97:52:06
;GROUP_4 - e4:11:5b:97:52:07
;----------------------------------------------


[SYSTEM Params]

SyslogServerIP = 10.38.5.76
EnableSyslog = 1
DebugRecordingDestIP = 10.38.5.76
;VpFileLastUpdateTime is hidden but has non-default value
NTPServerIP = '0.0.0.0'
;LastConfigChangeTime is hidden but has non-default value
;PM_gwINVITEDialogs is hidden but has non-default value
;PM_gwSBCMediaLegs is hidden but has non-default value

[BSP Params]

PCMLawSelect = 3
AuthorizedTPNCPServers_0 = 0.0.0.0
AuthorizedTPNCPServers_1 = 0.0.0.0
AuthorizedTPNCPServers_2 = 0.0.0.0
AuthorizedTPNCPServers_3 = 78.75.78.85
RoutingTableHopsCountColumn = 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
```

```
1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
UdpPortSpacing = 5
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[ControlProtocols Params]

AdminStateLockControl = 0


[Voice Engine Params]

BrokenConnectionEventTimeout = 1000

[WEB Params]

LogoWidth = '145'
HTTPSCipherString = 'RC4:EXP'

[SIP Params]

GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
ENABLEEARLYMEDIA = 1
ENABLEPASSOCIATEDURIHEADER = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
ENERGYDETECTORCMD = 104
ANSWERDETECTORCMD = 12582952
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value

[IPsec Params]


[SNMP Params]

;ContextEngineID is hidden but has non-default value

[ 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_3", 1, 4, "User Port #2", "GROUP_3", "Active";
PhysicalPortsTable 3 = "GE_4", 1, 4, "User Port #3", "GROUP_4", "Active";

[ \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", 1, "GE_3", "";
EtherGroupTable 3 = "GROUP_4", 1, "GE_4", "";

[ \EtherGroupTable ]


[ DeviceTable ]
```

```
FORMAT DeviceTable_Index = DeviceTable_VlanID, DeviceTable_UnderlyingInterface,
DeviceTable_DeviceName, DeviceTable_Tagging;
DeviceTable 0 = 1, "GROUP_1", "GROUP_1", 0;
DeviceTable 1 = 2, "GROUP_2", "GROUP_2", 0;

[ \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, 192.168.20.200, 24, 192.168.20.1, "NETMGT", 0.0.0.0,
0.0.0.0, "GROUP_1";
InterfaceTable 1 = 5, 10, 203.0.113.120, 26, 203.0.113.65, "PUBSIP", 8.8.4.4,
8.8.8.8, "GROUP_2";

[ \InterfaceTable ]



[ DspTemplates ]

FORMAT DspTemplates_Index = DspTemplates_DspTemplateNumber,
DspTemplates_DspResourcesPercentage;
DspTemplates 0 = 0, 100;

[ \DspTemplates ]


[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_ServerCipherString, TLSContexts_ClientCipherString,
TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary,
TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse;
TLSContexts 0 = "default", 0, "RC4:EXP", "ALL:!ADH", 0, , , 2560, 0;

[ \TLSContexts ]


[ IpProfile ]

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupID, IpProfile_IsFaxUsed, IpProfile_JitterBufMinDelay,
IpProfile_JitterBufOptFactor, IpProfile_IPDiffServ, IpProfile_SigIPDiffServ,
IpProfile_SCE, IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,
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_SBCExtensionCodersGroupID,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedCodersGroupID,
IpProfile_SBCAllowedVideoCodersGroupID, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,
IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel,
IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime,
IpProfile_SBCDiversionMode, IpProfile_SBCHistoryInfoMode,
```

```
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,
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 1 = "Genesys SIP Server", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0,
0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", 1, -1, 0, 0, 0, 0,
0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 0, 0, 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;
IpProfile 2 = "ITSP", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0, -1, 1, 0,
0, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", 2, -1, 0, 0, 0, 0, 0, 0, 8, 300,
400, 0, 0, 0, -1, 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;
IpProfile 3 = "RemoteAgents", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0, -
1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", 2, -1, 1, 0, 0, 0, 0, 0, 8,
300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 0, 0, 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;

[ \IpProfile ]


[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName, CpMediaRealm_IPv4IF,
CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart, CpMediaRealm_MediaSessionLeg,
CpMediaRealm_PortRangeEnd, CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile,
CpMediaRealm_BWProfile;
CpMediaRealm 1 = "MR1-SBC2Genesys", "NETMGT", "", 6000, 100, 6499, 0, "", "";
CpMediaRealm 2 = "MR2-SBC2ITSP", "PUBSIP", "", 8000, 100, 8499, 0, "", "";
CpMediaRealm 3 = "MR3-RemoteAgents", "PUBSIP", "", 9000, 100, 9499, 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 0 = "DefaultSRD", 0, -1, 1, 0, 0, 0, "Default_SBCRoutingPolicy";

[ \SRD ]


[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType, SIPInterface_UDPPort,
SIPInterface_TCPPort, SIPInterface_TLSPort, 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 1 = "Genesys", "NETMGT", 2, 5060, 0, 0, "DefaultSRD", "", "default", -
1, 0, 500, 17, 0, "MR1-SBC2Genesys", 0, -1, -1, -1, 0;
SIPInterface 2 = "ITSP", "PUBSIP", 2, 5060, 0, 0, "DefaultSRD", "", "default", -1,
0, 500, -1, 0, "MR2-SBC2ITSP", 0, -1, -1, -1, 0;
SIPInterface 3 = "RemoteAgents", "PUBSIP", 2, 5070, 0, 0, "DefaultSRD", "",
"default", -1, 0, 500, -1, 0, "MR3-RemoteAgents", 0, -1, -1, -1, 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_SASIPv4SIPInterfaceName,
ProxySet_GWIPv6SIPInterfaceName, ProxySet_SBCIPv6SIPInterfaceName,
ProxySet_SASIPv6SIPInterfaceName;
ProxySet 1 = "Genesys SIP Server", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "",
"", "Genesys", "", "", "", "";
ProxySet 2 = "ITSP", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "", "ITSP", "",
"", "", "";

[ \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_MediaEnhancementProfile, IPGroup_AlwaysUseSourceAddr,
IPGroup_MsgManUserDef1, IPGroup_MsgManUserDef2, IPGroup_SIPConnect,
IPGroup_SBCPSAPMode, IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer,
```

```
IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup_SBCRouteUsingRequestURIPort, IPGroup_SBCKeepOriginalCallID;
IPGroup 1 = 0, "Genesys", "Genesys SIP Server", "", "", -1, 0, "DefaultSRD", "MR1-
SBC2Genesys", 1, "Genesys SIP Server", -1, 3, 12, 0, 0, "", 0, -1, -1, "", "",
"$1$gQ==", 0, "", "", "", 0, "", "", 0, 0, "", 0, 0, 0, 0, 0;
IPGroup 2 = 0, "ITSP", "ITSP", "", "", -1, 0, "DefaultSRD", "MR2-SBC2ITSP", 1,
"ITSP", -1, -1, 1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "", "", 0, "",
"", 0, 0, "", 0, 0, 0, 0, 0;
IPGroup 3 = 1, "Remote Agents", "", "", "", -1, 0, "DefaultSRD", "MR3-
RemoteAgents", 0, "RemoteAgents", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "",
"$1$gQ==", 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", 1, "sipserver.genesys-domain.com:5060", 0;
ProxyIp 2 = "2", 1, "gw0.itsp-iot.com:5060", 0;

[ \ProxyIp ]


[ Account ]

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

[ \Account ]


[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName, IP2IPRouting_RoutingPolicyName,
IP2IPRouting_SrcIPGroupName, IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, 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 1 = "OPTIONS", "Default_SBCRoutingPolicy", "Any", "*", "*", "*", "*",
6, "", "Any", 0, -1, 1, "", "", "internal", 0, -1, 0, 0, "";
IP2IPRouting 3 = "3xx Move", "Default_SBCRoutingPolicy", "ITSP", "*", "*", "*",
"*", 0, "", "Genesys", 3, -1, 0, "Genesys", "Genesys", "", 0, -1, 0, 0, "";
IP2IPRouting 4 = "Windstream2Genesys", "Default_SBCRoutingPolicy", "ITSP", "*",
"*", "*", "*", 0, "", "Any", 0, -1, 0, "Genesys", "Genesys", "", 0, -1, 0, 0, "";
IP2IPRouting 6 = "Genesys2RemoteAgents", "Default_SBCRoutingPolicy", "Genesys",
"*", "*", "7138675309*", "*", 0, "", "Any", 0, -1, 0, "Remote Agents",
"RemoteAgents", "", 0, -1, 0, 0, "";
IP2IPRouting 8 = "Genesys2ITSP", "Default_SBCRoutingPolicy", "Genesys", "*", "*",
"*", "*", 0, "", "Any", 0, -1, 0, "ITSP", "ITSP", "", 0, -1, 0, 0, "";
IP2IPRouting 10 = "RemoteAgents2Genesys", "Default_SBCRoutingPolicy", "Remote
Agents", "*", "*", "*", "*", 0, "", "Any", 0, -1, 0, "Genesys", "Genesys", "", 0, -
1, 0, 0, "";

[ \IP2IPRouting ]


[ Classification ]

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

```
Classification_SrcSIPInterfaceName, Classification_SrcAddress,
Classification_SrcPort, Classification_SrcTransportType,
Classification_SrcUsernamePrefix, Classification_SrcHost,
Classification_DestUsernamePrefix, Classification_DestHost,
Classification_ActionType, Classification_SrcIPGroupName,
Classification_DestRoutingPolicy, Classification_IpProfileName;
Classification 1 = "Remote Users", "", "DefaultSRD", "RemoteAgents", "", 0, -1,
"*", "*", "*", "*", 1, "Remote Agents", "", "RemoteAgents";

[ \Classification ]


[ IPInboundManipulation ]

FORMAT IPInboundManipulation_Index = IPInboundManipulation_ManipulationName,
IPInboundManipulation_RoutingPolicyName,
IPInboundManipulation_IsAdditionalManipulation,
IPInboundManipulation_ManipulationPurpose, IPInboundManipulation_SrcIPGroupName,
IPInboundManipulation_SrcUsernamePrefix, IPInboundManipulation_SrcHost,
IPInboundManipulation_DestUsernamePrefix, IPInboundManipulation_DestHost,
IPInboundManipulation_RequestType, IPInboundManipulation_ManipulatedURI,
IPInboundManipulation_RemoveFromLeft, IPInboundManipulation_RemoveFromRight,
IPInboundManipulation_LeaveFromRight, IPInboundManipulation_Prefix2Add,
IPInboundManipulation_Suffix2Add;
IPInboundManipulation 1 = "strip trunk access code", "Default_SBCRoutingPolicy", 0,
0, "Genesys", "*", "*", "77*", "*", 0, 1, 2, 0, 255, "", "";

[ \IPInboundManipulation ]


[ CodersGroup0 ]

FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce,
CodersGroup0_CoderSpecific;
CodersGroup0 0 = "g711Ulaw64k", 20, 0, -1, 0, "";
CodersGroup0 1 = "g729", 20, 0, -1, 0, "";

[ \CodersGroup0 ]


[ CodersGroup1 ]

FORMAT CodersGroup1_Index = CodersGroup1_Name, CodersGroup1_pTime,
CodersGroup1_rate, CodersGroup1_PayloadType, CodersGroup1_Sce,
CodersGroup1_CoderSpecific;
CodersGroup1 0 = "g711Ulaw64k", 20, 0, -1, 0, "";
CodersGroup1 1 = "g729", 20, 0, -1, 0, "";

[ \CodersGroup1 ]


[ CodersGroup2 ]

FORMAT CodersGroup2_Index = CodersGroup2_Name, CodersGroup2_pTime,
CodersGroup2_rate, CodersGroup2_PayloadType, CodersGroup2_Sce,
CodersGroup2_CoderSpecific;
CodersGroup2 0 = "g711Ulaw64k", 20, 0, -1, 0, "";
CodersGroup2 1 = "g729", 20, 0, -1, 0, "";

[ \CodersGroup2 ]


[ AllowedCodersGroup1 ]

FORMAT AllowedCodersGroup1_Index = AllowedCodersGroup1_Name;
AllowedCodersGroup1 0 = "g711Ulaw64k";
```

```
AllowedCodersGroup1 1 = "g729";

[ \AllowedCodersGroup1 ]


[ AllowedCodersGroup2 ]

FORMAT AllowedCodersGroup2_Index = AllowedCodersGroup2_Name;
AllowedCodersGroup2 0 = "g711Ulaw64k";
AllowedCodersGroup2 1 = "g729";

[ \AllowedCodersGroup2 ]


[ MessageManipulations ]

FORMAT MessageManipulations_Index = MessageManipulations_ManipulationName,
MessageManipulations_ManSetID, MessageManipulations_MessageType,
MessageManipulations_Condition, MessageManipulations_ActionSubject,
MessageManipulations_ActionType, MessageManipulations_ActionValue,
MessageManipulations_RowRole;
MessageManipulations 0 = "diversion", 19, "invite.request", "header.request-
uri.url.user != header.to.url.user", "header.diversion", 0, "header.to.url.user +
'<sip:' + header.to.url.user + '@173.227.254.67>'+ ';user=phone>;userid=", 0;
MessageManipulations 1 = "diversion", 19, "invite.Request", "", "header.diversion",
0, "'7138675309' + '<sip:' + '7138675310' + '@173.227.254.67>'+
';user=phone>;userid=", 0;
MessageManipulations 7 = "URI host", 1, "Any", "header.REQUEST-URI.url.host ==
'10.38.5.116'", "header.REQUEST-URI.url.host", 2, "'gw0.itsp-iot.com'", 0;
MessageManipulations 8 = "To", 1, "Any", "header.to.url.host == '10.38.5.116'",
"header.to.url.host", 2, "'gw0.itsp-iot.com'", 1;
MessageManipulations 9 = "From Host", 1, "Any", "Header.From.Url.Host contains
'10.38.5.116'", "Header.From.Url.Host", 2, "'203.0.113.120'", 0;
MessageManipulations 12 = "Call Transfer", 1, "Any", "header.referred-by exists",
"header.referred-by.url.host", 2, "header.from.url.host", 0;
MessageManipulations 13 = "Call Transfer", 1, "Any", "header.referred-by exists",
"header.from.url.user", 2, "header.referred-by.url.user", 0;
MessageManipulations 15 = "Refer to:", 1, "", "", "header.refer-to.url.host", 2,
"'gw0.itsp-iot.com'", 0;
MessageManipulations 16 = "Referred-by", 1, "", "header.referred-by exists",
"header.referred-by.url.host", 2, "'203.0.113.120'", 0;
MessageManipulations 19 = "PAI host", 1, "Any", "header.P-Asserted-Identity
exists", "header.P-Asserted-Identity.url.host", 2, "'203.0.113.120'", 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 0 = 1, "", 1, 3, 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 ]


[ StaticRouteTable ]

FORMAT StaticRouteTable_Index = StaticRouteTable_DeviceName,
StaticRouteTable_Destination, StaticRouteTable_PrefixLength,
StaticRouteTable_Gateway, StaticRouteTable_Description;
StaticRouteTable 0 = "Unknown", 192.168.20.71, 24, 192.168.20.1, "";

[ \StaticRouteTable ]
```

Configuration Note

www.audiocodes.com