

Session Border Controllers (SBC)

AudioCodes Mediant™ Series

Interoperability Lab

Configuration Note

Telenor SIP Trunk & Genesys Contact Center using AudioCodes Mediant SBC



Version 6.8

June 2015

Document # LTRT-12355



Table of Contents

1	Introduction	9
1.1	Intended Audience	9
1.2	About AudioCodes SBC Product Series	9
1.3	About Genesys Contact Center	9
2	Component Information.....	11
2.1	AudioCodes SBC Version.....	11
2.2	Telenor SIP Trunking Version.....	11
2.3	Genesys Contact Center Version	11
2.4	Interoperability Test Topology	12
2.4.1	Environment Setup	14
2.4.2	Known Limitations/Restrictions.....	14
3	Configuring AudioCodes SBC	17
3.1	Step 1: Configure IP Network Interfaces.....	18
3.1.1	Step 1a: Configure VLANs.....	19
3.1.2	Step 1b: Configure Network Interfaces.....	19
3.1.3	Step 1c: Configure the Native VLAN ID.....	21
3.2	Step 2: Enable the SBC Application	22
3.3	Step 3: Configure Signaling Routing Domains	23
3.3.1	Step 3a: Configure Media Realms.....	23
3.3.2	Step 3b: Configure SRDs	25
3.3.3	Step 3c: Configure SIP Signaling Interfaces	27
3.4	Step 4: Configure Proxy Sets	28
3.5	Step 5: Configure IP Groups.....	31
3.6	Step 6: Configure IP Profiles	36
3.7	Step 7: Configure Coders	41
3.8	Step 8: Configure IP-to-IP Call Routing Rules	42
3.9	Step 9: Configure IP-to-IP Manipulation Rules.....	52
3.10	Step 10: SIP Header Message Manipulations.....	57
3.11	Step 10: Remote Agents	59
3.11.1	Step 10a: Configure Media Realm for a Remote Agent.....	59
3.11.2	Step 10b: Configure SRD for Remote Agent.....	60
3.11.3	Step 10c: Configure SIP Signaling Interfaces for Remote Agent.....	61
3.11.4	Step 10d: Configure Remote (User) Agents IP Group	62
3.11.5	Step 10e: Configure IP Profiles for Remote Agents	64
3.11.6	Step 10f: Configure Classification Table for Remote Agents	66
3.11.7	Step 10g: Configure IP-to-IP Call Routing Rules for Remote (User) Agent.....	68
3.12	Step 11: Reset the SBC	73
A	AudioCodes <i>ini</i> File.....	75

Table of Figures

Figure 2-1: Interoperability Test Topology.....	13
Figure 3-1: Network Interfaces in Interoperability Test Topology.....	18
Figure 3-2: Configured VLAN IDs in Ethernet Device Table.....	19
Figure 3-3: Configured Network Interfaces in IP Interfaces Table	20
Figure 3-4: Configured Port Native VLAN	21
Figure 3-5: Enabling SBC Application	22
Figure 3-6: Configuring Media Realm for LAN	23
Figure 3-7: Configuring Media Realm for WAN.....	24
Figure 3-8: Configured Media Realms in Media Realm Table	24
Figure 3-9: Configuring LAN SRD	25
Figure 3-10: Configuring WAN SRD.....	26
Figure 3-11: Configured SIP Interfaces in SIP Interface Table	27
Figure 3-12: Configuring Proxy Set for Genesys Contact Center SIP Server.....	29
Figure 3-13: Configuring Proxy Set for ITSP SIP Trunk.....	30
Figure 3-14: Configuring an IP Group for the Genesys Call Center (Common Tab)	32
Figure 3-15: Configuring an IP Group for the Genesys Call Center (SBC Tab)	33
Figure 3-16: Configuring an IP Group for the ITSP SIP Trunk (Common Tab)	34
Figure 3-17: Configuring an IP Group for the ITSP SIP Trunk (SBC Tab).....	35
Figure 3-18: Configured IP Groups in IP Group Table	35
Figure 3-19: Configuring IP Profile for Genesys Contact Center (Common Tab).....	36
Figure 3-20: Configuring IP Profile for Genesys Contact Center (SBC Tab)	37
Figure 3-21: Configuring IP Profile for ITSP SIP Trunk (Common Tab)	38
Figure 3-22: Configuring IP Profile for ITSP SIP Trunk – SBC Tab.....	39
Figure 3-23: Configured IP Profiles in IP Profile Table	40
Figure 3-24: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS - Rule Tab	43
Figure 3-25: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS - Action Tab	43
Figure 3-26: Configuring IP-to-IP Routing Rule for Genesys to ITSP – Rule tab	44
Figure 3-27: Configuring IP-to-IP Routing Rule for Genesys to ITSP – Action tab.....	45
Figure 3-28: Configuring IP-to-IP Routing Trigger Rule for 3xx/REFER to local agents – Rule tab	46
Figure 3-29: Configuring IP-to-IP Routing Rule for Trigger Rule for 3xx/REFER to local agents – Action Tab.....	47
Figure 3-30: Configuring IP-to-IP Routing Rule for ITSP to Genesys – Rule tab	48
Figure 3-31: Configuring IP-to-IP Routing Rule for Telenor ITSP to Genesys – Action tab	49
Figure 3-32: Configuring IP-to-IP Routing Rule for ITSP to Genesys – Rule tab	50
Figure 3-33: Configuring IP-to-IP Routing Rule for ITSP to Genesys – Action tab.....	51
Figure 3-34: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table	51
Figure 3-35: Configuring IP-to-IP Inbound Manipulation Rule – Rule Tab.....	53
Figure 3-36: Configuring IP-to-IP Inbound Manipulation Rule - Action Tab.....	54
Figure 3-37: Configuring IP-to-IP Inbound Manipulation Rule – Rule Tab.....	55
Figure 3-38: Configuring IP-to-IP Inbound Manipulation Rule - Action Tab.....	56
Figure 3-39: Example of Configured IP-to-IP Inbound Manipulation Rules	56
Figure 3-40: Configuring Remote Agent Media Realm	59
Figure 3-41: Configuring Remote Agent Media Realm	59
Figure 3-42: Configuring SRD for Remote Agents.....	60
Figure 3-43: Configuring Remote Agent Media Realm	60
Figure 3-44: Configured SIP Interfaces for Remote Agents in SIP Interface Table.....	61
Figure 3-45: Configuring an IP Group for the Remote (User) Agents (Common Tab)	62
Figure 3-46: Configuring an IP Group for Remote User Agents (SBC Tab)	63
Figure 3-47: Configured IP Group for Remote Users in IP Group Table	63
Figure 3-48: Configuring IP Profile for Remote Users (Common Tab)	64
Figure 3-49: Configuring IP Profile for Remote (User) Agents (SBC Tab).....	65
Figure 3-50: Configured IP Profiles in IP Profile Table	66
Figure 3-51: Configuring Rule Tab of the Classification Table.....	67
Figure 3-52: Configured IP Profiles in IP Profile Table	67
Figure 3-53: Configured Classification Rule for Remote (Users) Agents.....	67
Figure 3-54: Configuring IP-to-IP Routing Rule for Terminating RemoteAgents2Genesys – Rule Tab.....	69

Figure 3-55: Configuring IP-to-IP Routing Rule for Terminating RemoteAgents2Genesys – Action Tab	69
Figure 3-56: Configuring IP-to-IP Routing Rule for Genesys to Remote Agent Group – Rule tab	70
Figure 3-57: Configuring IP-to-IP Routing Rule for Genesys to SIP Trunk – Action tab	71
Figure 3-58: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table	72
Figure 3-59: Resetting the SBC	73

List of Tables

Table 2-1: AudioCodes SBC Version	11
Table 2-2: Telenor Version	11
Table 2-3: Genesys Contact Center Version	11
Table 2-4: Environment Setup	14

This page is intentionally left blank

Notice

This document describes how to connect the Telenor 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>.

© Copyright 2015 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: June-11-2015

Trademarks

AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNOM and One Box 365 are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

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 Telenor 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 Telenor 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	<ul style="list-style-type: none"> ▪ 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_6.80A.261.013
Protocol	<ul style="list-style-type: none"> ▪ SIP/UDP (to the Telenor ITSP SIP Trunk) ▪ SIP/UDP, TCP or TLS (to the Genesys Contact Center system)
Additional Notes	None

2.2 Telenor SIP Trunking Version

Table 2-2: Telenor Version

Vendor/Service Provider	Telenor
SSW Model/Service	Sonus-UAC
Software Version	Not Available
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 v8.1.1/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 Telenor ITSP SIP Trunk Provider via an SBC in similar way to an IP-PBX.



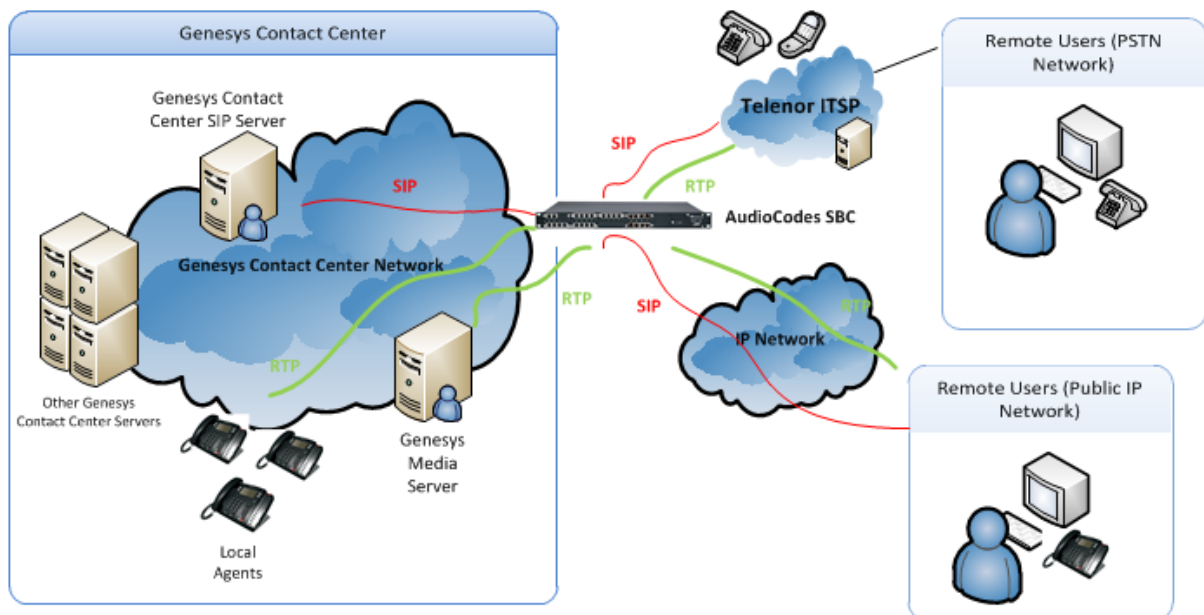
Note: Contact your Genesys Contact Center support channel for more information about topological scenarios.

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

- The Enterprise is 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 is connected to the Genesys Contact Center system to the PSTN network using the Telenor ITSP SIP Trunking service.
- The Telenor ITSP SIP Trunk is connected to the enterprise using the public external network.
- The AudioCodes' SBC is deployed to interconnect between the enterprise's LAN and the SIP trunk.
 - The SBC is connected to the Genesys Contact Center SIP server on the Genesys Contact Center internal network, and to the Telenor ITSP SIP Trunk located on the public network.
 - RTP traffic from/to Telenor ITSP SIP trunk flows 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	<ul style="list-style-type: none"> 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 DN's are located in the public network Telenor ITSP SIP Trunk is located on the WAN
Signaling Transcoding	<ul style="list-style-type: none"> Genesys Contact Center operates with SIP-over-UDP, TCP or TLS transport type Telenor SIP Trunk operates with SIP-over-UDP transport type. Telenor can also support SIP-over-TCP IOT environment uses SIP-over-UDP
Codecs Transcoding	<ul style="list-style-type: none"> Genesys Contact Center supports G.729, G.711A-law, G.711U-law, G.723, G722.2 and G.726 coders Telenor SIP Trunk supports G.711A-law (mandatory) and G.711U-law (recommended) coders
Media Transcoding	<ul style="list-style-type: none"> Genesys Contact Center and Telenor SIP Trunk operate with RTP media Type
DTMF	<ul style="list-style-type: none"> Genesys Contact Center supports delivering DTMF using SIP INFO message, RFC 2833 Named Telephony events, and in-band per ITU-T Recommendation Q.23 Telenor supports RFC 2833 (preferred) and in-band DTMF over G.711



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

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

- **SIP REFER:** The Telenor 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 Telenor 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 the Request Single Step Transfer succeed; 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:** Telenor 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).



Note: SIP Server Version 8.1.101.48 or later is required if multiple tokens are in the qop-options (Qop="auth, auth-int").

- **SIP Authentication for Inbound Calls:** Telenor does not support challenge/authentication for outbound calls from Telenor (inbound to the Contact Center). If required, SIP authentication response can be handled on the SBC as part of the Trunk-Side Equipment (TSE).

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

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

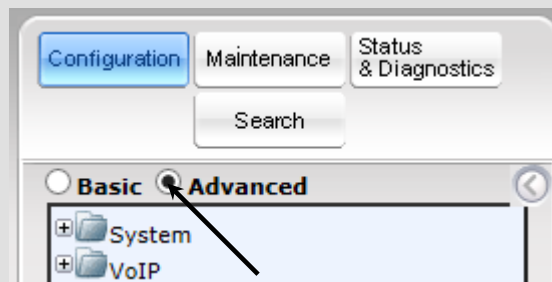
Notes:

- To implement the Genesys Contact Center and Telenor 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:



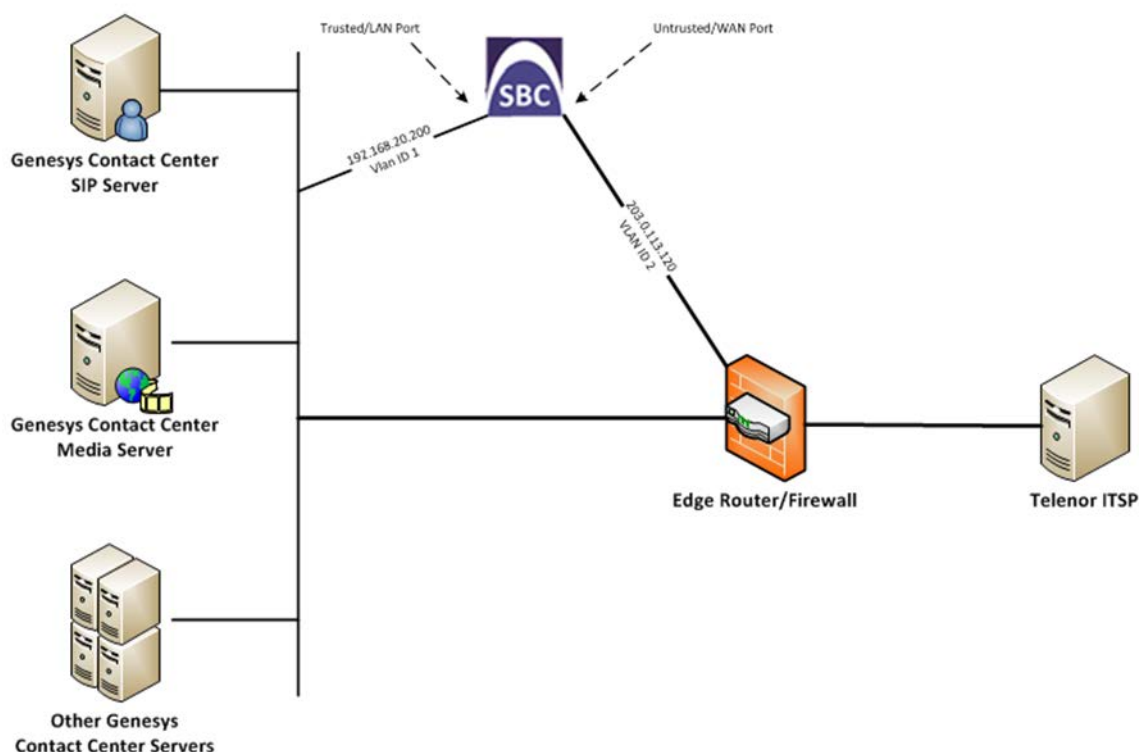
Note that when the SBC is reset, the navigation tree reverts to **Basic** display mode.

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)
 - Telenor 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")

➤ **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

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

Ethernet Device Table			
Add +		Edit ✎	Delete 🗑
		Show/Hide 📄	
Index	VLAN ID	Underlying Interface	Name
0	1	GROUP_1	GROUP_1
1	2	GROUP_2	GROUP_2

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")

➤ **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	Trusted (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**.
 - b. 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	Untrusted (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									
Add + Edit ✎ Delete 🗑️									Show/Hide 📄
Index ↕	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Interface Name	Primary DNS	Secondary DNS	Underlying Device
0	OAMP + Media + Control	IPv4 Manual	192.168.20.200	24	192.168.20.1	Trusted	0.0.0.0	0.0.0.0	GROUP_1
1	Media + Control	IPv4 Manual	203.0.113.120	26	203.0.113.65	Untrusted	8.8.4.4	8.8.8.8	GROUP_2

3.1.3 Step 1c: Configure the Native VLAN ID

This step describes how to configure the Native VLAN ID for the LAN and WAN interfaces.

➤ **To configure the Native VLAN ID for the IP network interfaces:**

1. Open the Physical Ports Settings page (**Configuration** tab > **VoIP** menu > **Network** > **Physical Ports Table**).
2. For the **GROUP_1** member ports, set the 'Native Vlan' field to **1**. This VLAN is assigned to network interface "Call Center" and is the trusted interface.
3. For the **GROUP_2** member ports, set the 'Native Vlan' field to **2**. This VLAN is assigned to network interface "Provider" and is the untrusted interface.

Figure 3-4: Configured Port Native VLAN

Physical Ports Settings							
Edit		Show/Hide					
Index	Port	Mode	Native Vlan	Speed&Duplex	Description	Group Member	Group Status
0	GE_1	Enable	1	Auto Negotiation	Trusted	GROUP_1	Active
1	GE_2	Enable	2	Auto Negotiation	Untrusted	GROUP_2	Active

3.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

➤ **To enable the SBC application:**

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

Figure 3-5: 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 73).

3.3 Step 3: Configure Signaling Routing Domains

This step describes how to configure Signaling Routing Domains (SRDs). The SRD represents a logical VoIP network. Each logical or physical connection requires an SRD, for example, if the SBC interfaces with both the LAN and WAN, a different SRD is required for each such connection.

The SRD comprises the following:

- **Media Realm:** Defines a UDP port range for RTP/SRTP (media) traffic on a specific logical IP network interface of the SBC.
- **SIP Interface:** Defines a listening port and type (UDP, TCP, or TLS) for SIP signaling traffic on a specific logical IP network interface of the SBC.

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.

➤ **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	Trusted
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: Configuring Media Realm for LAN

Edit Record #1

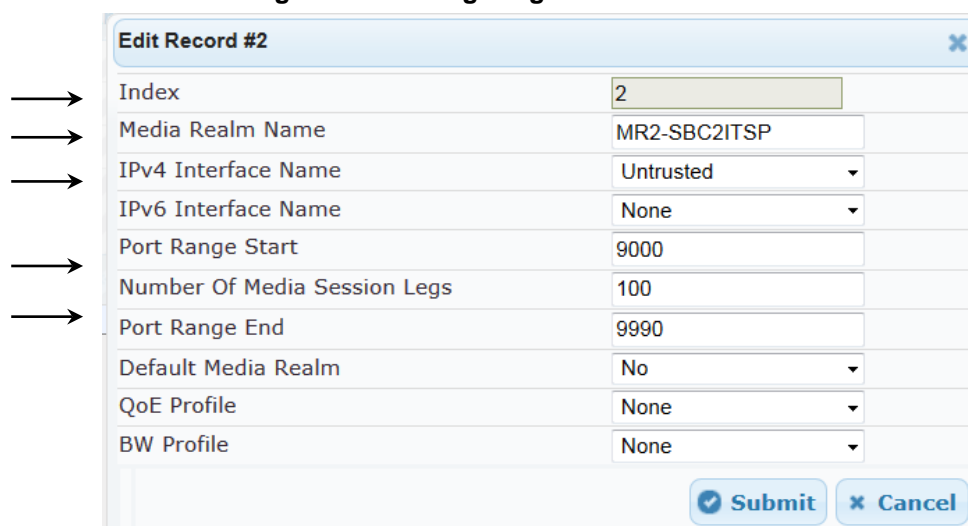
Index	1
Media Realm Name	MR1-SBC2Genesys
IPv4 Interface Name	Trusted
IPv6 Interface Name	None
Port Range Start	6000
Number Of Media Session Legs	100
Port Range End	6990
Default Media Realm	Yes
QoS Profile	None
BW Profile	None

Submit Cancel

3. Configure a Media Realm for WAN traffic:

Parameter	Value
Index	2
Media Realm Name	MR2-SBC2ITSP (arbitrary name)
IPv4 Interface Name	Provider
Port Range Start	8000 (represents the lowest UDP port number used for media on WAN). Telenor uses media port range 10000 to 10999 for UDP as signaled in the SDP.
Number of Media Session Legs	100 (media sessions assigned with port range).

Figure 3-7: Configuring Media Realm for WAN



Edit Record #2	
Index	2
Media Realm Name	MR2-SBC2ITSP
IPv4 Interface Name	Untrusted
IPv6 Interface Name	None
Port Range Start	9000
Number Of Media Session Legs	100
Port Range End	9990
Default Media Realm	No
QoE Profile	None
BW Profile	None

Submit Cancel

The configured Media Realms are shown in the figure below:

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

Media Realm Table		
Add + Edit Delete		
Index	Media Realm Name	IPv4 Interface Name
1	MR1-SBC2Genesys	Trusted
2	MR2-SBC2ITSP	Untrusted

3.3.2 Step 3b: Configure SRDs

This step describes how to configure SRDs. For the interoperability test topology, an SRD for the SBC's internal (toward Genesys Contact Center) and external interfaces (toward the ITSP SIP Trunk) are defined.

➤ **To configure SRDs:**

1. Open the SRD Settings page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SRD Table**).
2. Configure an SRD for the SBC's internal interface (toward Genesys Contact Center):

Parameter	Value
Index	1
Name	SRD1-Genesys (descriptive name for SRD)
Media Realm Name	MR1-SBC2Genesys (associates SRD with Media Realm)

Figure 3-9: Configuring LAN SRD

The screenshot shows a web-based configuration interface for editing an SRD record. The title bar reads 'Edit Record #1'. The form contains the following fields and values:

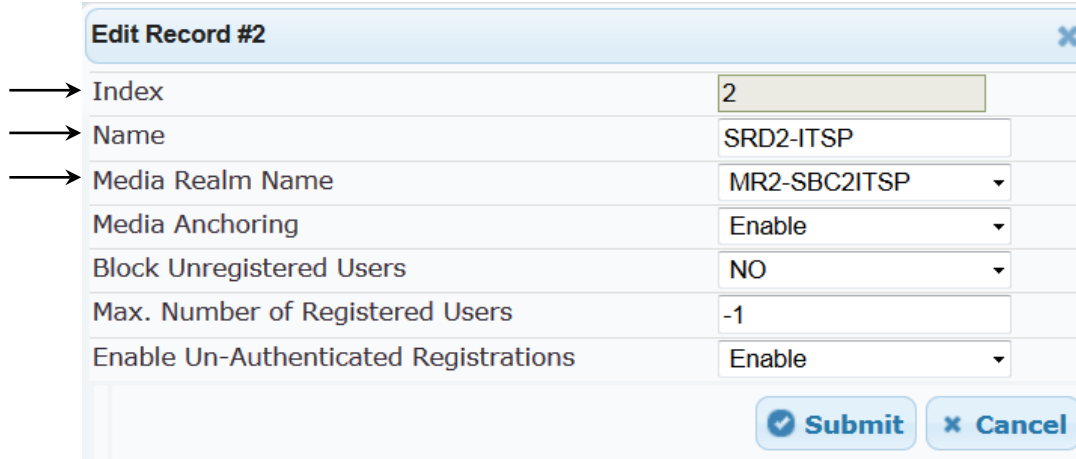
Index	1
Name	SRD1-Genesys
Media Realm Name	MR1-SBC2Genesys
Media Anchoring	Enable
Block Unregistered Users	NO
Max. Number of Registered Users	-1
Enable Un-Authenticated Registrations	Enable

At the bottom right, there are two buttons: 'Submit' (with a checkmark icon) and 'Cancel' (with an 'x' icon). Three arrows on the left side of the form point to the 'Index', 'Name', and 'Media Realm Name' fields.

3. Configure an SRD for the SBC's external interface (toward the ITSP SIP Trunk):

Parameter	Value
Index	2
Name	SRD2-ITSP
Media Realm Name	MR2-SBC2ITSP

Figure 3-10: Configuring WAN SRD



Edit Record #2 [Close]

→ Index	2
→ Name	SRD2-ITSP
→ Media Realm Name	MR2-SBC2ITSP
Media Anchoring	Enable
Block Unregistered Users	NO
Max. Number of Registered Users	-1
Enable Un-Authenticated Registrations	Enable

[Submit] [Cancel]

3.3.3 Step 3c: 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.

➤ **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	Trusted
Application Type	SBC
TCP and UDP	5060
TLS Port	5061
SRD	1

3. Configure a SIP interface for the WAN:

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

The configured SIP Interfaces are shown in the figure below:

Figure 3-11: Configured SIP Interfaces in SIP Interface Table

SIP Interface Table							
Add + Edit Delete				Show/Hide			
Index	SIP Interface Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD
1	Genesys	Trusted	SBC	5060	5060	5061	1
2	ITSP	Untrusted	SBC	5060	5060	5061	2

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 need to be configured for the following IP entities:

- Genesys Contact Center SIP Server
- Telenor ITSP SIP Trunk

These Proxy Sets will later be associated with IP Groups.

➤ 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
Proxy Address	sipserver.genesys-domain.com:5060 Genesys Contact Center IP address / FQDN and destination port. For UDP and TCP, the port is 5060 . If TLS is used, the port must be 5061 .
Transport Type	UDP, TCP or TLS depends on the configuration of Genesys Contact Center Transport Type (Default is UDP).
Proxy Name	Genesys SIP Server (arbitrary descriptive name).
Enable Proxy Keep Alive	Using Options
SRD Index	1

Figure 3-12: Configuring Proxy Set for Genesys Contact Center SIP Server

Proxy Set ID: 1

	Proxy Address	Transport Type
1	sipserver.genesys-iot.com:5060	
2		
3		
4		
5		
6		
7		
8		
9		
10		

Proxy Name: Genesys SIP Server

Enable Proxy Keep Alive: Using Options

Proxy Keep Alive Time: 60

Proxy Load Balancing Method: Disable

Is Proxy Hot Swap: No

Proxy Redundancy Mode: Not Configured

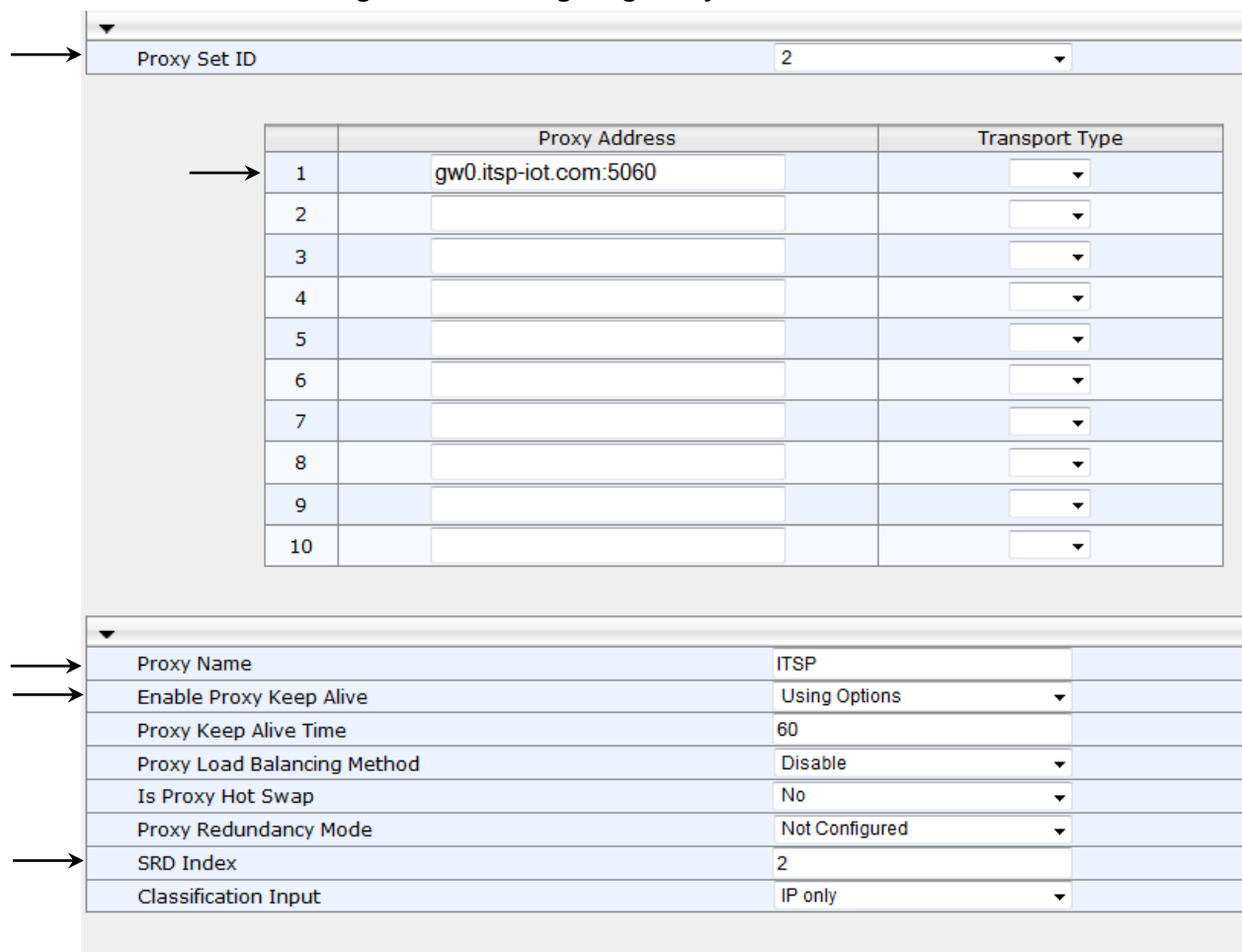
SRD Index: 1

Classification Input: IP only

3. Configure a Proxy Set for the ITSP SIP Trunk:

Parameter	Value
Proxy Set ID	2
Proxy Address	gw0.itsp-iot.com:5060 (ITSP IP address / FQDN and destination port)
Transport Type	UDP
Proxy Name	ITSP (arbitrary descriptive name)
Enable Proxy Keep Alive	Using Options
SRD Index	2 (enables classification by Proxy Set for SRD of IP Group belonging to Telenor SIP Trunk)

Figure 3-13: Configuring Proxy Set for ITSP SIP Trunk



Proxy Set ID: 2

	Proxy Address	Transport Type
1	gw0.itsp-iot.com:5060	
2		
3		
4		
5		
6		
7		
8		
9		
10		

Proxy Name: ITSP

Enable Proxy Keep Alive: Using Options

Proxy Keep Alive Time: 60

Proxy Load Balancing Method: Disable

Is Proxy Hot Swap: No

Proxy Redundancy Mode: Not Configured

SRD Index: 2

Classification Input: IP only

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 two LAN IP PBXs sharing the same SRD, and two ITSPs / SIP Trunks sharing the same SRD. 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:

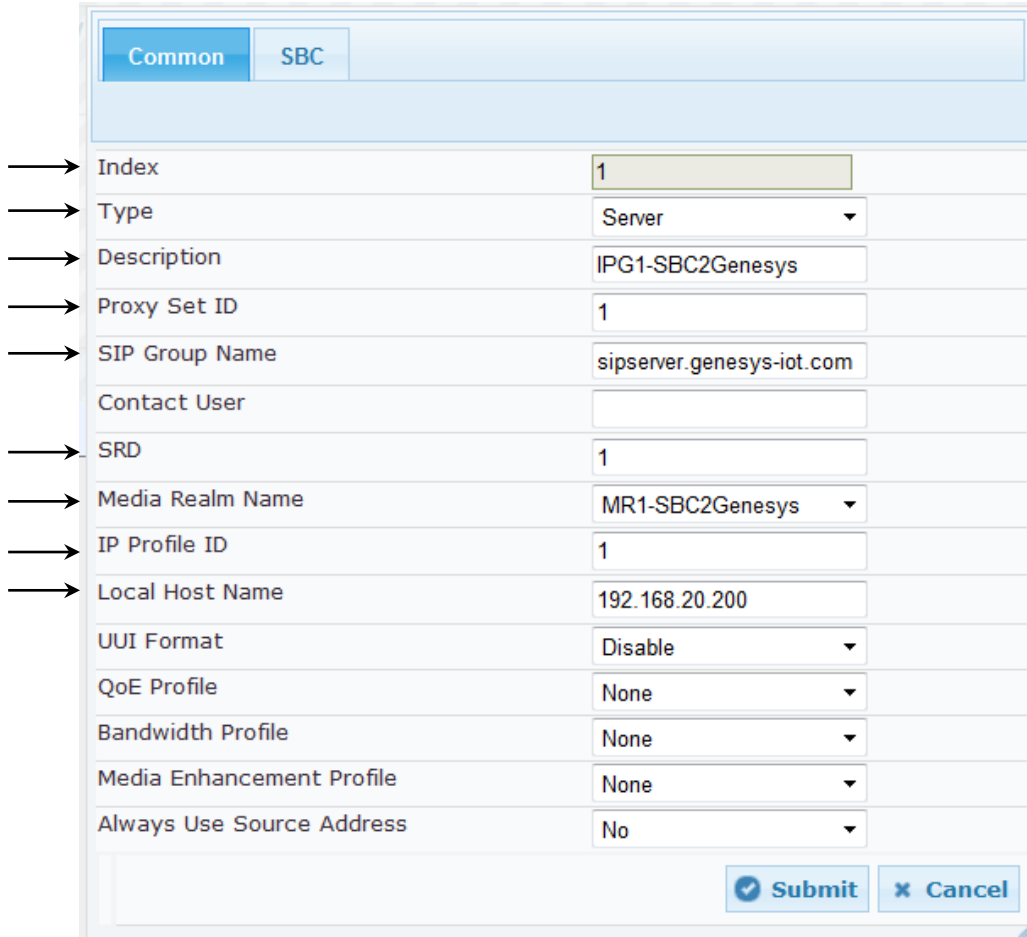
- Genesys Contact Center located on LAN (Server Group)
- ITSP SIP Trunk located on WAN (Server Group)
- Remote User Agents located in the WAN (User Group) (see Section 3.10 on page 57)

➤ **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	IPG1-SBC2Genesys (arbitrary descriptive name)
Proxy Set ID	1
SIP Group Name	sipserver.genesys-iot.com (according to ITSP requirement)
SRD	1
Media Realm Name	MR1-SBC2Genesys
IP Profile ID	1
Local Host Name	192.168.20.200

Figure 3-14: Configuring an IP Group for the Genesys Call Center (Common Tab)



Common		SBC
Index	1	
Type	Server	
Description	IPG1-SBC2Genesys	
Proxy Set ID	1	
SIP Group Name	sipserver.genesys-iot.com	
Contact User		
SRD	1	
Media Realm Name	MR1-SBC2Genesys	
IP Profile ID	1	
Local Host Name	192.168.20.200	
UUI Format	Disable	
QoE Profile	None	
Bandwidth Profile	None	
Media Enhancement Profile	None	
Always Use Source Address	No	
		Submit Cancel

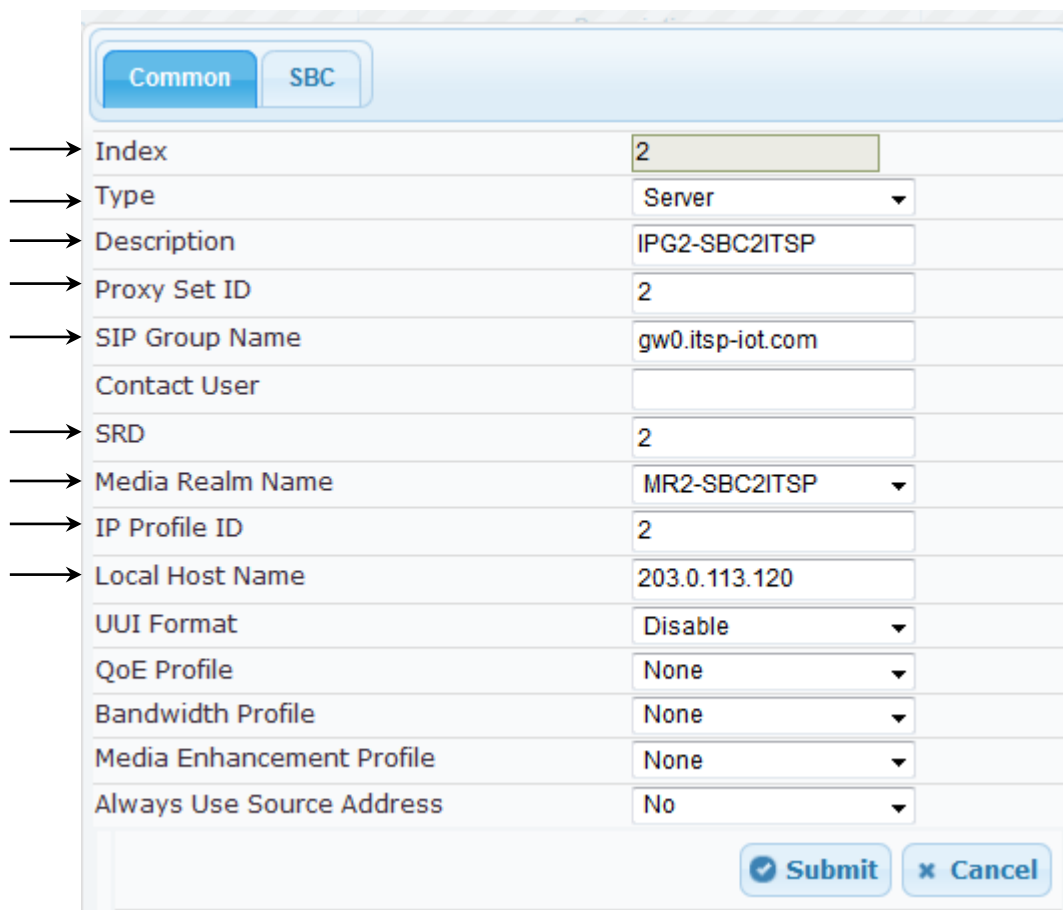
Figure 3-15: Configuring an IP Group for the Genesys Call Center (SBC Tab)

Common SBC	
Index	1
Classify By Proxy Set	Enable
Max. Number of Registered Users	-1
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	-1
Registration Mode	User Initiates Registrat
Authentication Mode	User Authenticates
Authentication Method List	
SBC Client Forking Mode	Sequential
Source URI Input	
Destination URI Input	
Username	
Password	
Msg Man User Defined String1	
Msg Man User Defined String2	
<div>Submit Cancel</div>	

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

Parameter	Value
Index	2
Type	Server
Description	IPG2-SBC2ITSP (arbitrary descriptive name)
Proxy Set ID	2
SIP Group Name	gw0.itsp-iot.com
SRD	2
Media Realm Name	MR2-SBC2ITSP
IP Profile ID	2
Local Host Name	203.0.113.120

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



The screenshot shows a configuration window with two tabs: 'Common' (selected) and 'SBC'. The 'Common' tab contains the following fields and values:

- Index: 2
- Type: Server
- Description: IPG2-SBC2ITSP
- Proxy Set ID: 2
- SIP Group Name: gw0.itsp-iot.com
- Contact User: (empty)
- SRD: 2
- Media Realm Name: MR2-SBC2ITSP
- IP Profile ID: 2
- Local Host Name: 203.0.113.120
- UUI Format: Disable
- QoE Profile: None
- Bandwidth Profile: None
- Media Enhancement Profile: None
- Always Use Source Address: No

At the bottom right, there are 'Submit' and 'Cancel' buttons.

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

Common	SBC
Index	2
Classify By Proxy Set	Enable
Max. Number of Registered Users	-1
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	-1
Registration Mode	User Initiates Registr:
Authentication Mode	User Authenticates
Authentication Method List	
SBC Client Forking Mode	Sequential
Source URI Input	
Destination URI Input	
Username	
Password	
Msg Man User Defined String1	
Msg Man User Defined String2	
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

The configured IP Groups are shown in the figure below:

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

IP Group Table				
Add +				
Index	Type	Description	Proxy Set ID	SIP Group Name
1	Server	IPG1-SBC2Genesys	1	sipserver.genesys-iot.com
2	Server	IPG2-SBC2ITSP	2	gw0.itsp-iot.com

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



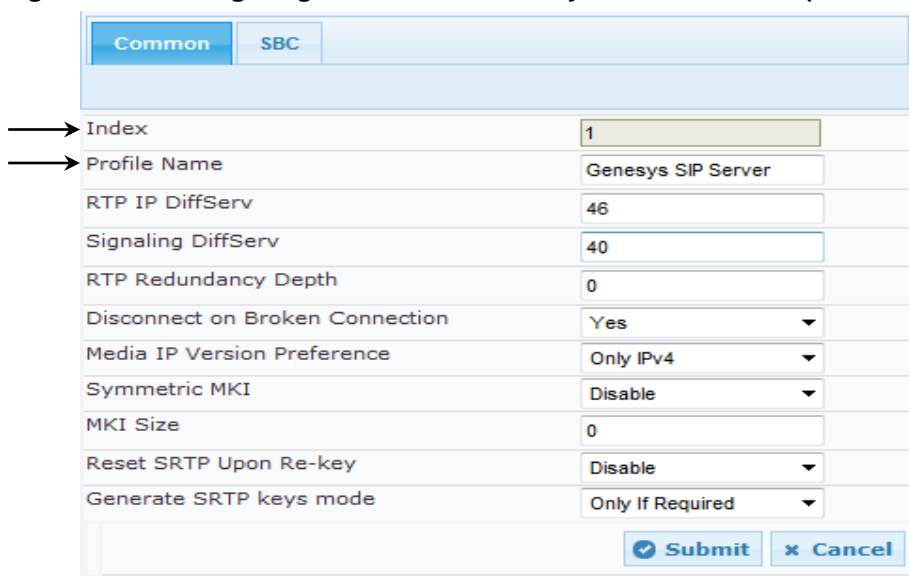
Note: The IP Profile index values were assigned to the IP Groups in the previous step (see Section 3.5 on page 31).

➤ **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: Configuring IP Profile for Genesys Contact Center (Common Tab)



Parameter	Value
Index	1
Profile Name	Genesys SIP Server
RTP IP DiffServ	46
Signaling DiffServ	40
RTP Redundancy Depth	0
Disconnect on Broken Connection	Yes
Media IP Version Preference	Only IPv4
Symmetric MKI	Disable
MKI Size	0
Reset SRTP Upon Re-key	Disable
Generate SRTP keys mode	Only If Required

Submit Cancel

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

Parameter	Value
Allowed Coders Group ID	'Coders Group 1'

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

Common SBC

Index	1
Extension Coders Group ID	None
Transcoding Mode	Only If Required
Allowed Media Types	
→ Allowed Coders Group ID	Coders Group 1
Allowed Video Coders Group ID	None
Allowed Coders Mode	Restriction
SBC Media Security Behavior	As Is
RFC 2833 Behavior	As Is
Alternative DTMF Method	As Is
P-Asserted-Identity	As Is
Diversion Mode	As Is
History-Info Mode	As Is
Fax Coders Group ID	None
Fax Behavior	As Is
Fax Offer Mode	All coders
Fax Answer Mode	Single coder
PRACK Mode	Transparent
Session Expires Mode	Transparent
Remote Update Support	Supported
Remote re-INVITE	Supported
Remote Delayed Offer Support	Supported
Remote REFER Behavior	Regular
Remote 3xx Behavior	Transparent
Remote Multiple 18x	Supported
Remote Early Media Response Type	Transparent
Remote Early Media	Supported
Enforce MKI Size	Don't enforce
Remote Early Media RTP Detection Mode	By Signaling
Remote RFC 3960 Gateway Model Support	Not Supported
Remote Can Play Ringback	Yes
RFC 2833 DTMF Payload Type	0
User Registration Time	0
Reliable Held Tone Source	Yes
Play Held Tone	No
Remote Hold Format	Transparent
Remote Replaces Behavior	Standard
SDP Ptime Answer	Remote Answer
Preferred PTime	0
Use Silence Suppression	Transparent
RTP Redundancy Behavior	AS IS
Play RBT To Transferee	No
RTCP Mode	Transparent
Jitter Compensation	Disable
Remote Renegotiate on Fax Detection	Transparent
Remote Multiple Answers Mode	Disabled
Keep VIA Headers	Not Configured
Keep User-Agent Header	Not Configured
User Behind NAT UDP Registration Time	-1
User Behind NAT TCP Registration Time	-1

Submit Cancel

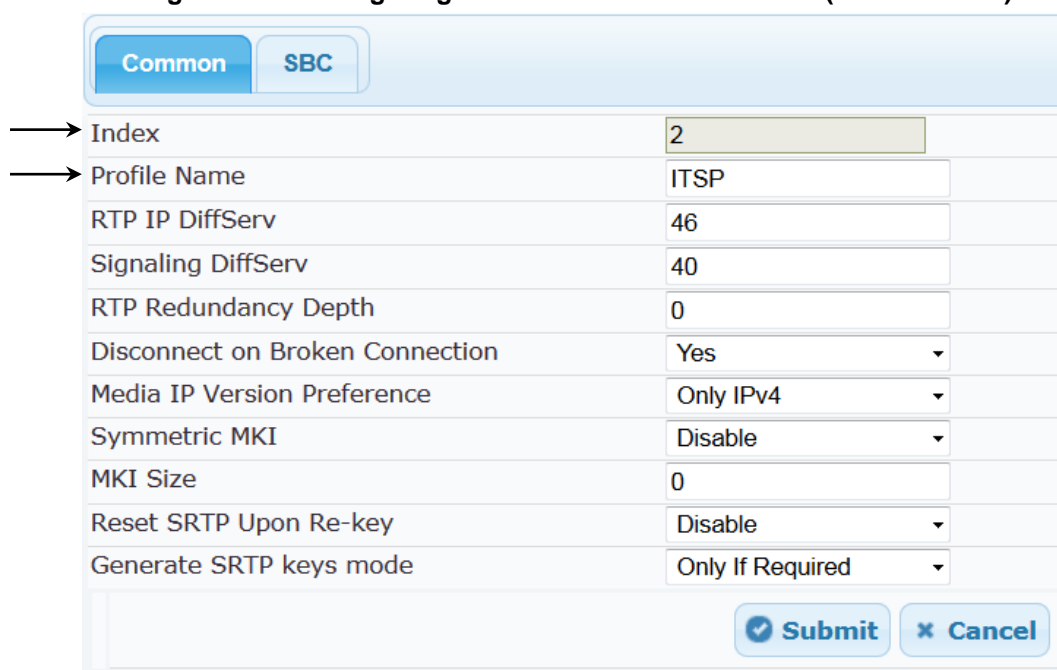
5. Configure an IP Profile for the ITSP SIP Trunk:

c. Click **Add**.

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

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

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



Parameter	Value
Index	2
Profile Name	ITSP
RTP IP DiffServ	46
Signaling DiffServ	40
RTP Redundancy Depth	0
Disconnect on Broken Connection	Yes
Media IP Version Preference	Only IPv4
Symmetric MKI	Disable
MKI Size	0
Reset SRTP Upon Re-key	Disable
Generate SRTP keys mode	Only If Required

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

Parameter	Value
Allowed Coders Group ID	'Coders Group 1'
Remote REFER Behavior	'Handle Locally'
Session Expires Mode	'Transparent' : one of Remote Update Support or Remote Re-INVITE support must be supported to refresh the session. 'Not Supported' : If Remote UPDATE/Re-INVITE is 'Not Supported', Session Expires Mode should be made 'not supported' also.
Remote Update Support (Optional)	'Supported'/'Not Supported'
Remote Re-INVITE Support (Optional)	'Supported'/'Not Supported'

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

Common		SBC
Index	2	
Extension Coders Group ID	None ▼	
Transcoding Mode	Only If Required ▼	
Allowed Media Types	audio	
→ Allowed Coders Group ID	Coders Group 1 ▼	
Allowed Video Coders Group ID	None ▼	
Allowed Coders Mode	Restriction and Pret ▼	
SBC Media Security Behavior	As Is ▼	
RFC 2833 Behavior	As Is ▼	
Alternative DTMF Method	As Is ▼	
P-Asserted-Identity	Add ▼	
Diversion Mode	Add ▼	
History-Info Mode	As Is ▼	
Fax Coders Group ID	None ▼	
Fax Behavior	As Is ▼	
Fax Offer Mode	All coders ▼	
Fax Answer Mode	Single coder ▼	
PRACK Mode	Transparent ▼	
→ Session Expires Mode	Not Supported ▼	
→ Remote Update Support	Not Supported ▼	
→ Remote re-INVITE	Not Supported ▼	
Remote Delayed Offer Support	Supported ▼	
→ Remote REFER Behavior	Handle Locally ▼	
Remote 3xx Behavior	Transparent ▼	
Remote Multiple 18x	Supported ▼	
Remote Early Media Response Type	Transparent ▼	
Remote Early Media	Supported ▼	
Enforce MKI Size	Don't enforce ▼	
Remote Early Media RTP Detection Mode	By Signaling ▼	
Remote RFC 3960 Gateway Model Support	Not Supported ▼	
Remote Can Play Ringback	No ▼	
RFC 2833 DTMF Payload Type	0	
User Registration Time	0	
Reliable Held Tone Source	Yes ▼	
Play Held Tone	No ▼	
Remote Hold Format	Transparent ▼	
Remote Replaces Behavior	Standard ▼	
SDP Ptime Answer	Remote Answer ▼	
Preferred PTime	0	
Use Silence Suppression	Transparent ▼	
RTP Redundancy Behavior	AS IS ▼	
Play RBT To Transferee	Yes ▼	
RTCP Mode	Transparent ▼	
Jitter Compensation	Disable ▼	
Remote Renegotiate on Fax Detection	Transparent ▼	
Remote Multiple Answers Mode	Disabled ▼	
Keep VIA Headers	Not Configured ▼	
Keep User-Agent Header	Not Configured ▼	
User Behind NAT UDP Registration Time	-1	
User Behind NAT TCP Registration Time	-1	

Submit Cancel


Notes:

- Telenor supports the re-routing of a call into the external (PSTN) network upon the receipt of a SIP 302 Moved Temporarily response. The SBC transparently passes the 302 Moved Temporarily request from Genesys to the ITSP. This response is accepted by the ITSP (SIP 202 Accepted) with subsequent routing of the call by the ITSP to the external DN.
- Optionally, 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 3-23: 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 G.711 coders only. The Telenor SIP Trunk supports G.711A-law and G.711U-law 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).

However, 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 Telenor 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.711A-Law
Coder Name	G.711U-Law

Allowed Audio Coders Group

Allowed Audio Coders Group ID: 1

Coder Name

- G.711A-law
- G.711U-law
-
-
-
-
-
-
-

3. **Submit**

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 30, 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 ITSP SIP Trunk
- Calls from ITSP SIP Trunk to Genesys Contact Center
- Trigger rules for handling SIP 3xx/REFER for local agents and external DN

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

Parameter	Value
Index	0
Route Name	OPTIONS termination (arbitrary descriptive name)
Source IP Group ID	-1
Request Type	OPTIONS

Figure 3-24: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS - Rule Tab

Rule	
Index	1
Route Name	OPTIONS termination
Source IP Group ID	-1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	OPTIONS
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	Any
Call Setup Rules Set ID	-1

Submit Cancel

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

Parameter	Value
Destination Type	Dest Address
Destination Address	internal

Figure 3-25: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS - Action Tab

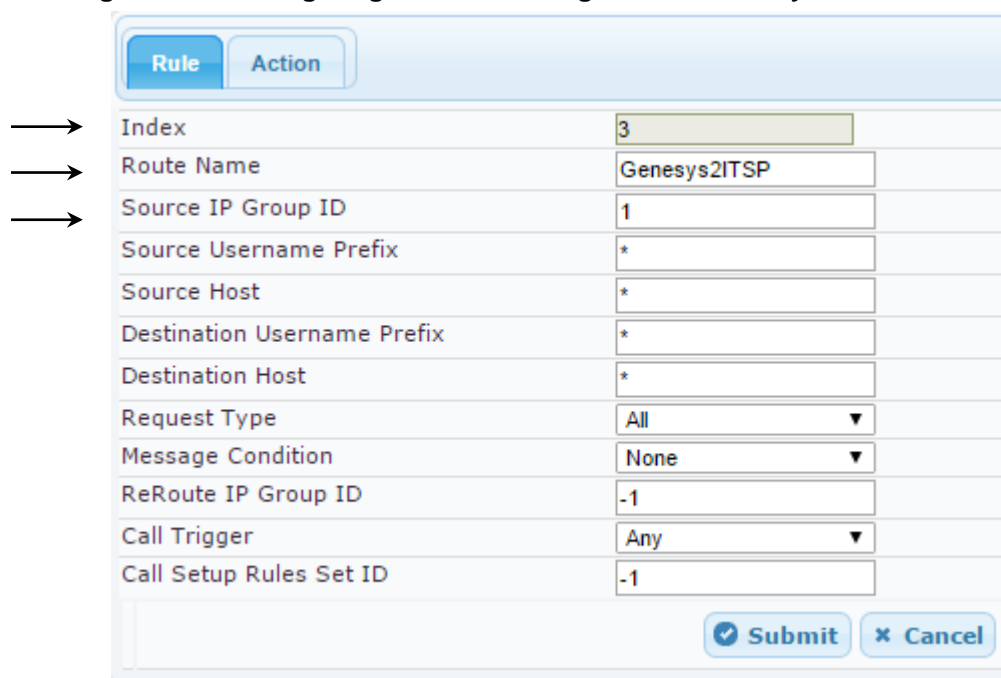
Action	
Index	0
Destination Type	Dest Address
Destination IP Group ID	-1
Destination SRD ID	None
Destination Address	internal
Destination Port	0
Destination Transport Type	
Alternative Route Options	Route Row
Group Policy	None
Cost Group	None
Rules Set Id	-1

Submit Cancel

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

Parameter	Value
Index	3
Route Name	Genesys2ITSP (arbitrary descriptive name)
Source IP Group ID	1

Figure 3-26: Configuring IP-to-IP Routing Rule for Genesys to ITSP – Rule tab



The screenshot shows the 'Rule' tab of the configuration interface. The 'Rule' tab is selected, and the 'Action' tab is also visible. The form contains the following fields and values:

- Index: 3
- Route Name: Genesys2ITSP
- Source IP Group ID: 1
- Source Username Prefix: *
- Source Host: *
- Destination Username Prefix: *
- Destination Host: *
- Request Type: All
- Message Condition: None
- ReRoute IP Group ID: -1
- Call Trigger: Any
- Call Setup Rules Set ID: -1

At the bottom right, there are 'Submit' and 'Cancel' buttons. Three arrows on the left point to the 'Index', 'Route Name', and 'Source IP Group ID' fields.

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

Parameter	Value
Destination Type	IP Group
Destination IP Group ID	2
Destination SRD ID	2

Figure 3-27: Configuring IP-to-IP Routing Rule for Genesys to ITSP – Action tab

The screenshot shows the 'Action' tab configuration for an IP-to-IP Routing Rule. The form has two tabs: 'Rule' and 'Action'. The 'Action' tab is selected. The form contains the following fields and values:

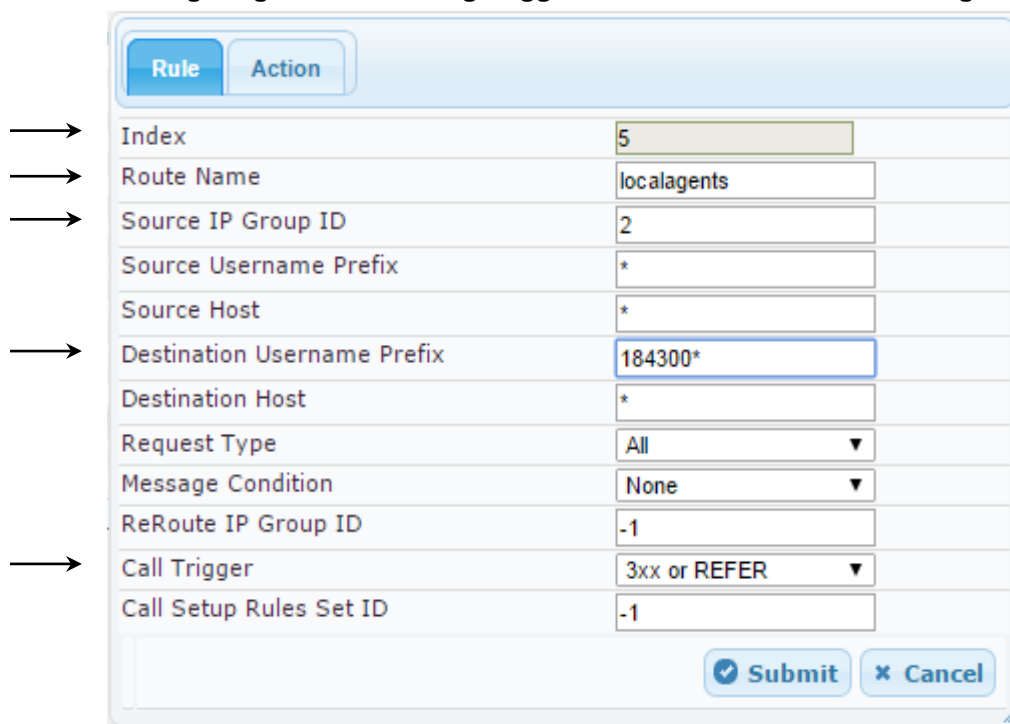
Index	3
Destination Type	IP Group
Destination IP Group ID	2
Destination SRD ID	2
Destination Address	
Destination Port	0
Destination Transport Type	
Alternative Route Options	Route Row
Group Policy	None
Cost Group	None

At the bottom right, there are two buttons: 'Submit' and 'Cancel'.

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	5
Route Name	3xx/Refer local (arbitrary descriptive name)
Source IP Group ID	2
Destination Username Prefix	184300* (based on local agent DN assignment)
Call Trigger	3xx or REFER

Figure 3-28: Configuring IP-to-IP Routing Trigger Rule for 3xx/REFER to local agents – Rule tab



Parameter	Value
Index	5
Route Name	localagents
Source IP Group ID	2
Source Username Prefix	*
Source Host	*
Destination Username Prefix	184300*
Destination Host	*
Request Type	All
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	3xx or REFER
Call Setup Rules Set ID	-1

Submit Cancel

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

Parameter	Value
Destination Type	IP Group
Destination IP Group ID	1 (route back to Genesys SIP Server)
Destination SRD ID	1

Figure 3-29: Configuring IP-to-IP Routing Rule for Trigger Rule for 3xx/REFER to local agents – Action Tab

Rule Action

Index 5

Destination Type IP Group

Destination IP Group ID 1

Destination SRD ID 1

Destination Address

Destination Port 0

Destination Transport Type

Alternative Route Options Route Row

Group Policy None

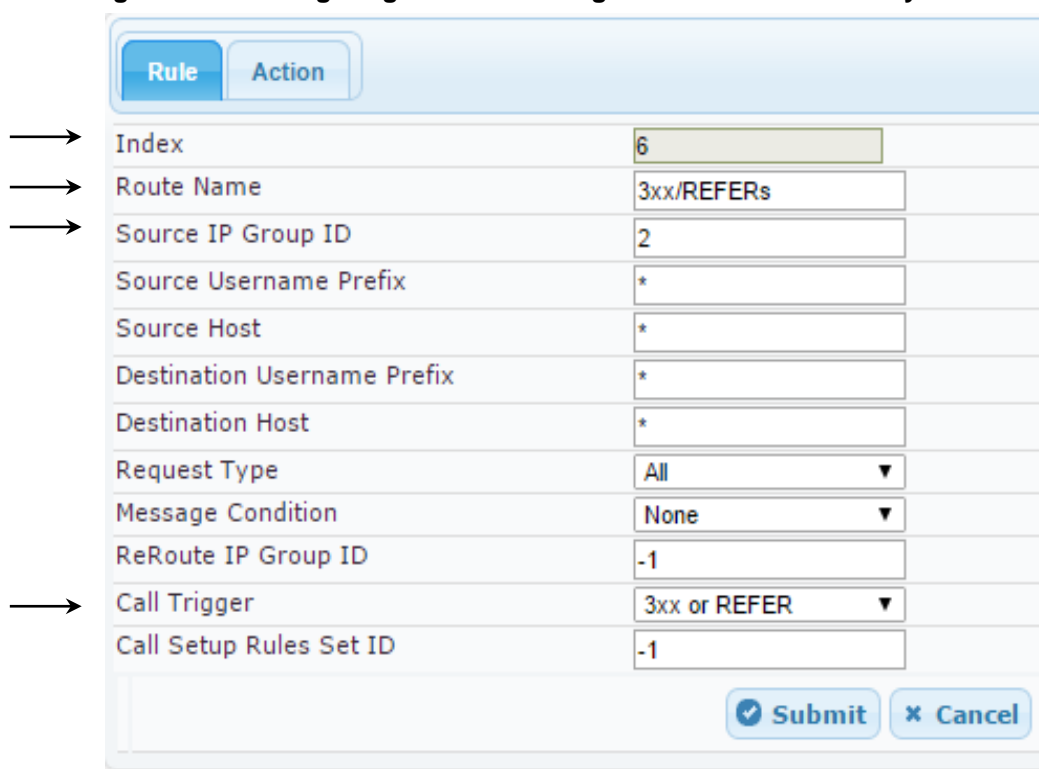
Cost Group None

Submit Cancel

8. Configure a trigger rule to route calls for external REFERS to the network from the Genesys Contact Center to the Telenor SIP Trunk:
 - a. Click **Add**.
 - b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	6
Route Name	3xx/Refer external (arbitrary descriptive name)
Source IP Group ID	2
Call Trigger:	3xx or REFER

Figure 3-30: Configuring IP-to-IP Routing Rule for ITSP to Genesys – Rule tab



The screenshot shows the 'Rule' tab of the configuration interface. The fields and their values are as follows:

Field	Value
Index	6
Route Name	3xx/REFERs
Source IP Group ID	2
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	3xx or REFER
Call Setup Rules Set ID	-1

At the bottom right, there are 'Submit' and 'Cancel' buttons.

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

Parameter	Value
Destination Type	IP Group
Destination IP Group ID	2
Destination SRD ID	2

Figure 3-31: Configuring IP-to-IP Routing Rule for Telenor ITSP to Genesys – Action tab

Rule Action

Index 6

Destination Type IP Group ▼

Destination IP Group ID 2

Destination SRD ID 2 ▼

Destination Address

Destination Port 0

Destination Transport Type ▼

Alternative Route Options Route Row ▼

Group Policy None ▼

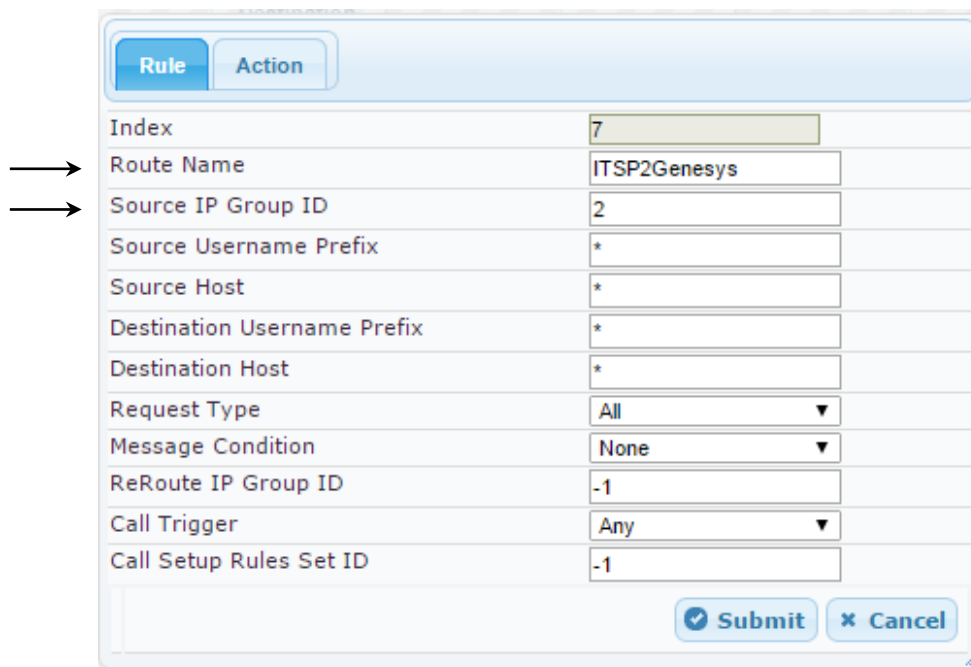
Cost Group None ▼

Submit Cancel

10. 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	7
Route Name	ITSP2Genesys (arbitrary descriptive name)
Source IP Group ID	2

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



The screenshot shows the 'Rule' tab of the configuration interface. The 'Rule' tab is selected, and the 'Action' tab is also visible. The form contains the following fields and values:

- Index: 7
- Route Name: ITSP2Genesys
- Source IP Group ID: 2
- Source Username Prefix: *
- Source Host: *
- Destination Username Prefix: *
- Destination Host: *
- Request Type: All
- Message Condition: None
- ReRoute IP Group ID: -1
- Call Trigger: Any
- Call Setup Rules Set ID: -1

Arrows point to the 'Route Name' and 'Source IP Group ID' fields, indicating they are the focus of the configuration.

11. 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: Configuring IP-to-IP Routing Rule for ITSP to Genesys – Action tab

Rule Action

Index: 7

Destination Type: IP Group

Destination IP Group ID: 1

Destination SRD ID: 1

Destination Address:

Destination Port: 0

Destination Transport Type:

Alternative Route Options: Route Row

Group Policy: None

Cost Group: None

Submit Cancel

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

IP-to-IP Routing Table										
Add +		Insert +								
Index *	Route Name	Source Host	Destination Username Prefix	Destination Host	Message Condition	ReRoute IP Group ID	Call Trigger	Call Setup Rules Set ID	Destination Type	Destination
1	OPTIONS termination	*	*	*	None	-1	Any	-1	Dest Address	None
3	Genesys2ITSP	*	*	*	None	-1	Any	-1	IP Group	2
5	localagents	*	18430052*	*	None	-1	3xx or REFER	-1	IP Group	1
6	3xx/REFERS	*	*	*	None	-1	3xx or REFER	-1	IP Group	2
7	ITSP2Genesys	*	*	*	None	-1	Any	-1	IP Group	1



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

For example, 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. As configured in Section 3.5 on page 30, IP Group 1 represents Genesys Contact Center, and IP Group 2 represents ITSP SIP Trunk.



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 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)	remove +46 CC
Source IP Group ID	2
Request Type	INVITE and REGISTER
Manipulated URI	Destination

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

The screenshot shows a configuration window titled "Rule Tab" with two tabs: "Rule" (selected) and "Action". The form contains the following fields and values:

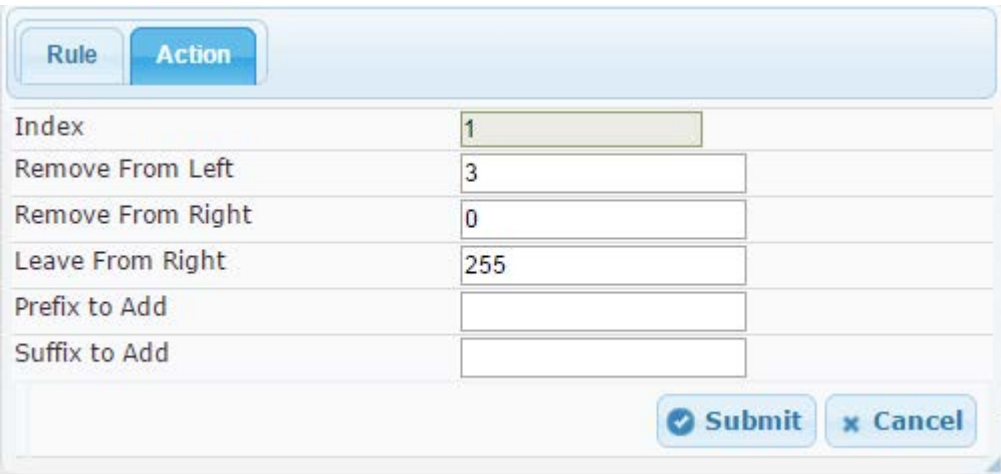
Field	Value
Index	1
Manipulation Name	remove +46 CC
Additional Manipulation	No
Manipulation Purpose	Normal
Source IP Group ID	2
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	INVITE and REGISTE
Manipulated URI	Destination

At the bottom right, there are two buttons: "Submit" (with a checkmark icon) and "Cancel" (with an 'x' icon).

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

Parameter	Value
Remove from Left	6

Figure 3-36: Configuring IP-to-IP Inbound Manipulation Rule - Action Tab



→

5. Click **Submit**.

➤ **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	2
Manipulation Name (optional)	rm SBC access code
Source IP Group ID	1
Destination Username Prefix	77
Request Type	All
Manipulated URI	Destination

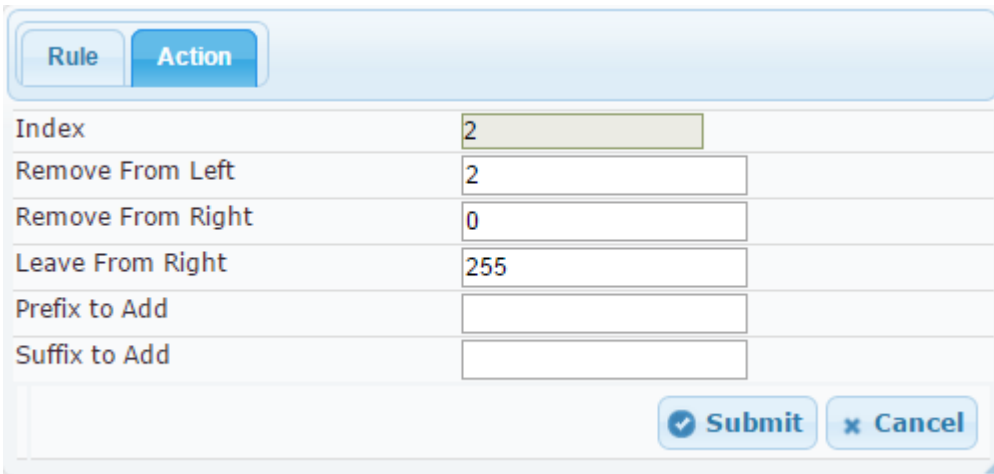
Figure 3-37: Configuring IP-to-IP Inbound Manipulation Rule – Rule Tab

	Rule	Action
	Index	2
→	Manipulation Name	rm SBC access code
	Additional Manipulation	No ▼
	Manipulation Purpose	Normal ▼
→	Source IP Group ID	1
	Source Username Prefix	*
	Source Host	*
→	Destination Username Prefix	77
	Destination Host	*
→	Request Type	All ▼
→	Manipulated URI	Destination ▼
	<div>Submit Cancel</div>	

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

Parameter	Value
Remove from Left	2

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



→

7. 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 3-39: Example of Configured IP-to-IP Inbound Manipulation Rules

IP to IP Inbound Manipulation											
Add + Insert + Edit ✎ Delete 🗑 Up ↑ Down ↓ Show/Hide 📄											
Index	Manipulation Name	Addition Manipulation	Manipulation Purpose	Source IP Group ID	Source Username Prefix	Source Host	Destination Username Prefix	Destination Host	Request Type	Manipulated URI	Prefix to Add
1	remove +46 CC	No	Normal	2	*	*	*	*	INVITE and REGISTER	Destination	
2	rm SBC access code	No	Normal	1	*	*	77	*	All	Destination	

3.10 Step 10: 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 ITSP's 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 IOT, 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 (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Click **Add**. The following dialog box appears:

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

Manipulation Set ID	Message Type	Condition	Action Subject
Add Record			
Index	0		
Manipulation Name			
Manipulation Set ID	0		
Message Type			
Condition			
Action Subject			
Action Type	Add		
Action Value			
Row Role	Use Current Condition		
		Submit	Cancel

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 for this IOT.

[MessageManipulations]

Index	Manipulation Name	Man Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
1	dest ip in r-uri	3	invite.request		header.request-uri.url.host	Modify	param.message.address.dst.address	Use Current Condition
2	add user=p r-uri	3	invite.request		header.request-uri.url.userphone	Modify	'1'	Use Current Condition
3	add user=phone To	3	Invite.Request		header.to.url.userphone	Modify	'1'	Use Current Condition
4	add user=phone From	3	invite.request		header.from.url.userphone	Modify	'1'	Use Current Condition
5	topology hide From	3	invite.request		header.from.url.host	Modify	param.message.address.src.address	Use Current Condition
6	dest in To host	3	Invite.Request		header.to.url.host	Modify	param.message.address.dst.address	Use Current Condition
7	topology hide PAI	3	invite.request	header.p-asserted-identity exists	header.p-asserted-identity.url.host	Modify	param.message.address.dst.address	Use Current Condition
8	contact header e164	3	invite.request		header.contact.url.user	Add Prefix	'46'	Use Current Condition
9	302 MT diversion	3	invite.response.302		header.diversion	Add	header.to.url.user + '<sip: + header.to.url.user + '@imtx.telenor.se;user=phone>'	Use Current Condition
10	REFER Contact e164	3	invite.response.302	header.contact regex (<sip:)(.*)@(.*)(>)	header.contact	Modify	\$1+'+'\$2+'@'+imtx.telenor.se'+';user=phone'+\$4	Use Current Condition
11	REFER from +	3	refer.request		header.from.url.user	Add Prefix	'+'	Use Current Condition
12	REFER To	3	refer.request	header.refer-to.url.user !contains '18430052'	header.refer-to.url.user	Add Prefix	'+'	Use Current Condition
13	hdr refer to hosts	3	refer.request		header.refer-to.url.host	Modify	'xxx.xxx.xxx.xx';user=phone'	Use Current Condition
14	REFER-by host	3	refer.request		header.referred-by.url.host	Modify	'xxx.xxx.xxx.xx'	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. For this IOT, Manipulation Set 3 should be applied to ITSP IP Group 2.

3.11 Step 10: 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 10a: 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 remote agent:**

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

Figure 3-40: Configuring Remote Agent Media Realm

Edit Record #3	
Index	3
Media Realm Name	MR3-RemoteAgents
IPv4 Interface Name	Untrusted
IPv6 Interface Name	None
Port Range Start	9000
Number Of Media Session Legs	100
Port Range End	9990
Default Media Realm	No
QoE Profile	None
BW Profile	None
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

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

Figure 3-41: Configuring Remote Agent Media Realm

Media Realm Table		
<input type="button" value="Add +"/> <input type="button" value="Edit ✎"/> <input type="button" value="Delete 🗑"/>		
Index	Media Realm Name	IPv4 Interface Name
1	MR1-SBC2Genesys	Trusted
2	MR2-SBC2ITSP	Untrusted
3	MR3-RemoteAgents	Untrusted

3.11.2 Step 10b: Configure SRD for Remote Agent

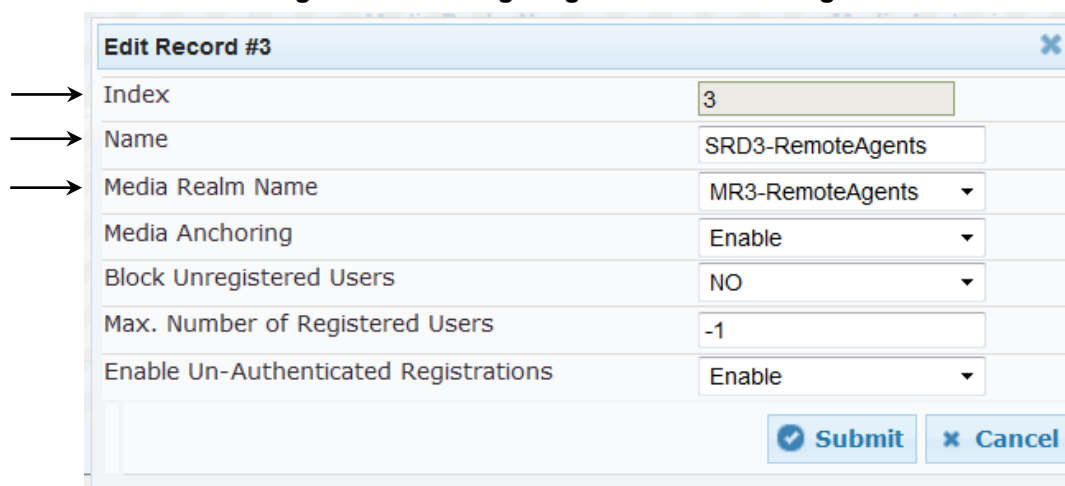
This step describes how to create a new SRD for the Remote Agents.

➤ To configure the SRD for remote agent:

1. Open the SRD Settings page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SRD Table**).
2. Configure an SRD for the SBC's internal interface (toward Genesys Contact Center):

Parameter	Value
Index	3
Name	SRD3-RemoteAgents (descriptive name for SRD)
Media Realm Name	MR3-RemoteAgents (associates SRD with Media Realm)

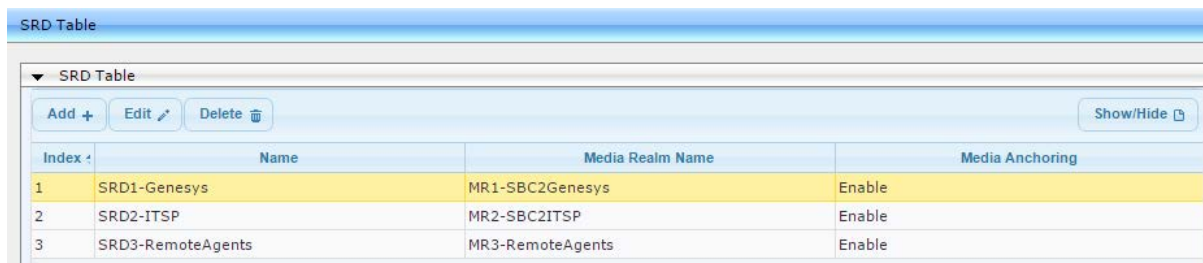
Figure 3-42: Configuring SRD for Remote Agents



Edit Record #3	
Index	3
Name	SRD3-RemoteAgents
Media Realm Name	MR3-RemoteAgents
Media Anchoring	Enable
Block Unregistered Users	NO
Max. Number of Registered Users	-1
Enable Un-Authenticated Registrations	Enable
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

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

Figure 3-43: Configuring Remote Agent Media Realm



SRD Table			
<div> Add + Edit ✎ Delete 🗑️ Show/Hide 📄 </div>			
Index	Name	Media Realm Name	Media Anchoring
1	SRD1-Genesys	MR1-SBC2Genesys	Enable
2	SRD2-ITSP	MR2-SBC2ITSP	Enable
3	SRD3-RemoteAgents	MR3-RemoteAgents	Enable

3.11.3 Step 10c: Configure SIP Signaling Interfaces for Remote Agent

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 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	Untrusted
Application Type	SBC
TCP and UDP	5070
TLS Port	5071
SRD	3

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

Figure 3-44: Configured SIP Interfaces for Remote Agents in SIP Interface Table

The screenshot shows the 'SIP Interface Table' configuration page. At the top, there are buttons for 'Add', 'Edit', and 'Delete', and a 'Show/Hide' button on the right. The table below has eight columns: Index, SIP Interface Name, Network Interface, Application Type, UDP Port, TCP Port, TLS Port, and SRD. There are three rows of data:

Index	SIP Interface Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD
1	Genesys	Trusted	SBC	5060	5060	5061	1
2	ITSP	Untrusted	SBC	5060	5060	5061	2
3	RemoteAgents	Untrusted	SBC	5070	5070	5071	3

3.11.4 Step 10d: Configure Remote (User) Agents IP Group

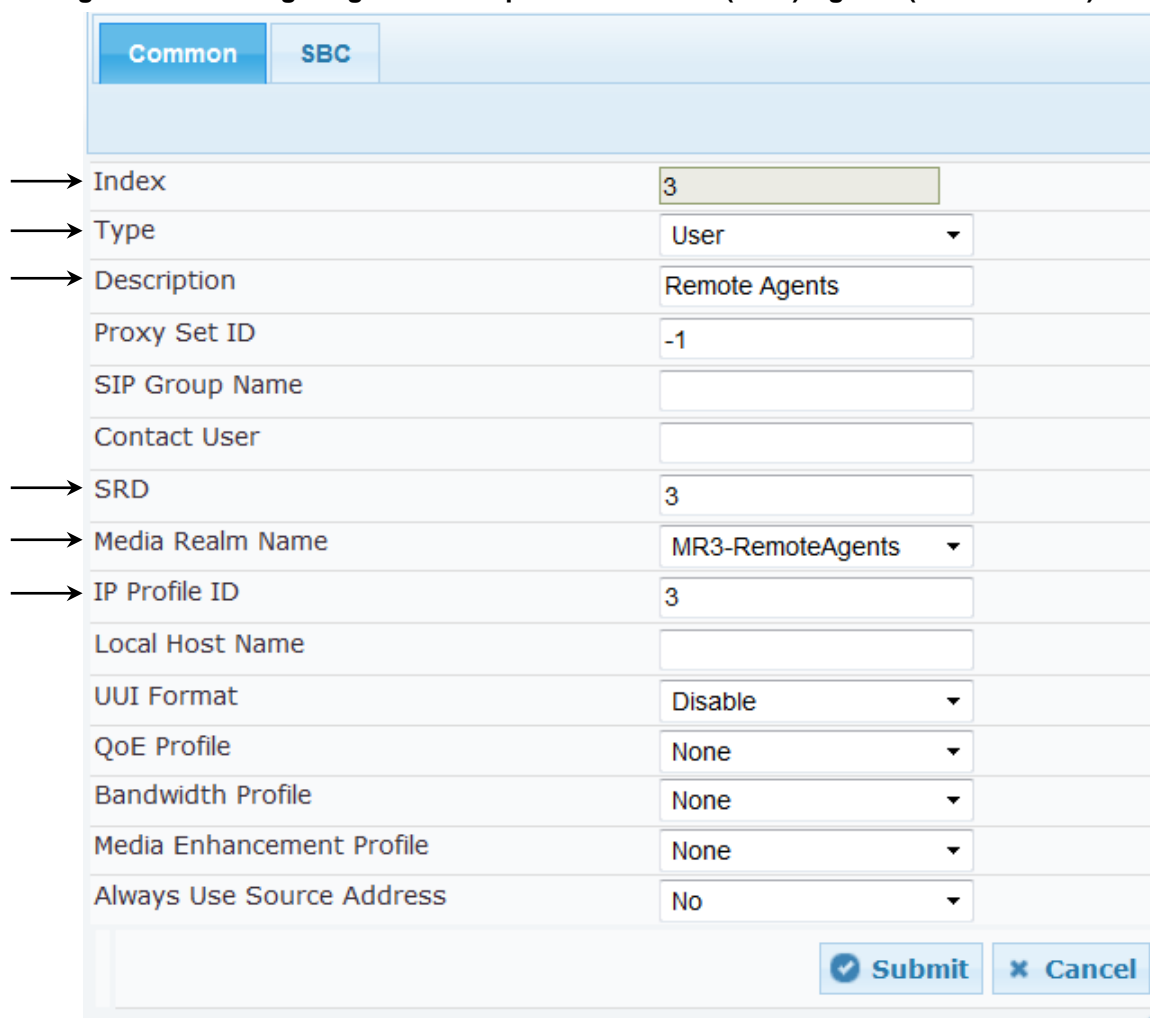
This step describes how to configure remote (User) agents IP Group. In the interoperability test topology, an IP User Group was configured for Remote (User) Agents registering from the WAN.

➤ **To configure an IP User Group:**

1. Open the IP Group Table page (**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	1
Media Realm Name	MR3-RemoteAgents
IP Profile ID	3

Figure 3-45: Configuring an IP Group for the Remote (User) Agents (Common Tab)



Common SBC	
Index	3
Type	User
Description	Remote Agents
Proxy Set ID	-1
SIP Group Name	
Contact User	
SRD	3
Media Realm Name	MR3-RemoteAgents
IP Profile ID	3
Local Host Name	
UUI Format	Disable
QoE Profile	None
Bandwidth Profile	None
Media Enhancement Profile	None
Always Use Source Address	No

Submit Cancel

Figure 3-46: Configuring an IP Group for Remote User Agents (SBC Tab)

Common	SBC
Index	3
Classify By Proxy Set	Disable
Max. Number of Registered Users	-1
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	-1
Registration Mode	User Initiates Registrat
Authentication Mode	User Authenticates
Authentication Method List	
SBC Client Forking Mode	Sequential
Source URI Input	
Destination URI Input	
Username	
Password	
Msg Man User Defined String1	
Msg Man User Defined String2	
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

The configured IP Groups are shown in the figure below:

Figure 3-47: Configured IP Group for Remote Users in IP Group Table

IP Group Table				
<input type="button" value="Add +"/> <input type="button" value="Edit ✎"/> <input type="button" value="Delete 🗑"/>				
Index	Type	Description	Proxy Set ID	SIP Group Name
1	Server	IPG1-SBC2Genesys	1	sipserver.genesys-iot.com
2	Server	IPG2-SBC2ITSP	2	gw0.itsp-iot.com
3	User	Remote Agents	-1	

3.11.5 Step 10e: Configure IP Profiles for Remote Agents

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



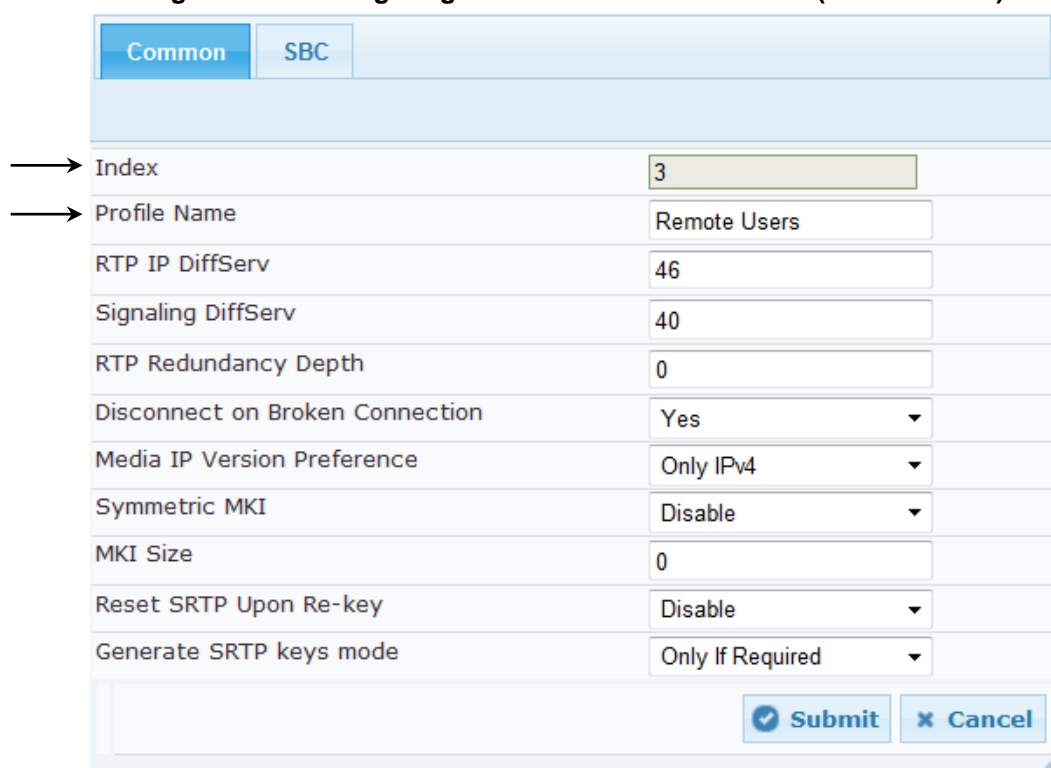
Note: The IP Profile index values were assigned to the IP Groups in the previous step (see Section 3.5 on page 31).

➤ **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 3-48: Configuring IP Profile for Remote Users (Common Tab)



The screenshot shows the 'Common' tab of the IP Profile Settings page. The 'Index' field is set to 3, and the 'Profile Name' is 'Remote Users'. Other parameters are set to their default values: RTP IP DiffServ (46), Signaling DiffServ (40), RTP Redundancy Depth (0), Disconnect on Broken Connection (Yes), Media IP Version Preference (Only IPv4), Symmetric MKI (Disable), MKI Size (0), Reset SRTP Upon Re-key (Disable), and Generate SRTP keys mode (Only If Required). The 'SBC' tab is also visible but not selected. Arrows point to the 'Index' and 'Profile Name' fields.

Parameter	Value
Index	3
Profile Name	Remote Users
RTP IP DiffServ	46
Signaling DiffServ	40
RTP Redundancy Depth	0
Disconnect on Broken Connection	Yes
Media IP Version Preference	Only IPv4
Symmetric MKI	Disable
MKI Size	0
Reset SRTP Upon Re-key	Disable
Generate SRTP keys mode	Only If Required



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

Figure 3-49: Configuring IP Profile for Remote (User) Agents (SBC Tab)

Common		SBC
Index	3	
Extension Coders Group ID	None	
Transcoding Mode	Only If Required	
Allowed Media Types		
Allowed Coders Group ID	None	
Allowed Video Coders Group ID	None	
Allowed Coders Mode	Restriction	
SBC Media Security Behavior	As Is	
RFC 2833 Behavior	As Is	
Alternative DTMF Method	As Is	
P-Asserted-Identity	As Is	
Diversion Mode	As Is	
History-Info Mode	As Is	
Fax Coders Group ID	None	
Fax Behavior	As Is	
Fax Offer Mode	All coders	
Fax Answer Mode	Single coder	
PRACK Mode	Transparent	
Session Expires Mode	Transparent	
Remote Update Support	Supported	
Remote re-INVITE	Supported	
Remote Delayed Offer Support	Supported	
Remote REFER Behavior	Regular	
Remote 3xx Behavior	Transparent	
Remote Multiple 18x	Supported	
Remote Early Media Response Type	Transparent	
Remote Early Media	Supported	
Enforce MKI Size	Don't enforce	
Remote Early Media RTP Behavior	Immediate	
Remote RFC 3960 Gateway Model Support	Not Supported	
Remote Can Play Ringback	Yes	
RFC 2833 DTMF Payload Type	0	
User Registration Time	0	
Reliable Held Tone Source	Yes	
Play Held Tone	No	
Remote Hold Format	Transparent	
Remote Replaces Behavior	Transparent	
SDP Ptime Answer	Remote Answer	
Preferred PTime	0	
Use Silence Suppression	Transparent	
RTP Redundancy Behavior	AS IS	
Play RBT To Transferee	No	
RTCP Mode	Transparent	
RTCP Mode	Transparent	
Jitter Compensation	Disable	
Remote Renegotiate on Fax Detection	Don't Care	
		<input type="button" value="Submit"/> <input type="button" value="Cancel"/>

Figure 3-50: Configured IP Profiles in IP Profile Table

IP Profile Settings	
<div> Add + Edit ✎ Delete 🗑️ </div>	
Index ↕	Profile Name
1	Genesys SIP Server
2	ITSP
3	Remote User Agent

3.11.6 Step 10f: 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 (**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 SRD ID	3

Figure 3-51: Configuring Rule Tab of the Classification Table

Rule	
Index	1
Classification Name	Remote Users
Message Condition	None
Source SRD ID	3
Source IP Address	
Source Port	0
Source Transport Type	Any
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

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

Parameter	Value
Source IP Group ID	3

Figure 3-52: Configured IP Profiles in IP Profile Table

Action	
Index	1
Action Type	Allow
Source IP Group ID	3
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

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

Figure 3-53: Configured Classification Rule for Remote (Users) Agents

Classification Table								
Add +		Edit ✎	Delete 🗑	Up ↑	Down ↓	Show/Hide ☑		
Index	Classification Name	Message Condition	Source SRD ID	Source IP Address	Source Port	Source Username Prefix	Destination Host	Action Type
1	Remote Users	None	3		0	*	*	Allow

3.11.7 Step 10g: 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 3.11.6 on page 66) and the Genesys SIP Server.

The following IP-to-IP call routing rules were configured (see Section 3.8 on page 42):

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

Parameter	Value
Index	8
Route Name	RemoteAgents2Genesys (arbitrary descriptive name)
Source IP Group ID	3

Figure 3-54: Configuring IP-to-IP Routing Rule for Terminating RemoteAgents2Genesys – Rule Tab

Rule	
Index	8
Route Name	Remote2Genesys
Source IP Group ID	3
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	Any
Call Setup Rules Set ID	-1

Submit Cancel

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

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

Figure 3-55: Configuring IP-to-IP Routing Rule for Terminating RemoteAgents2Genesys – Action Tab

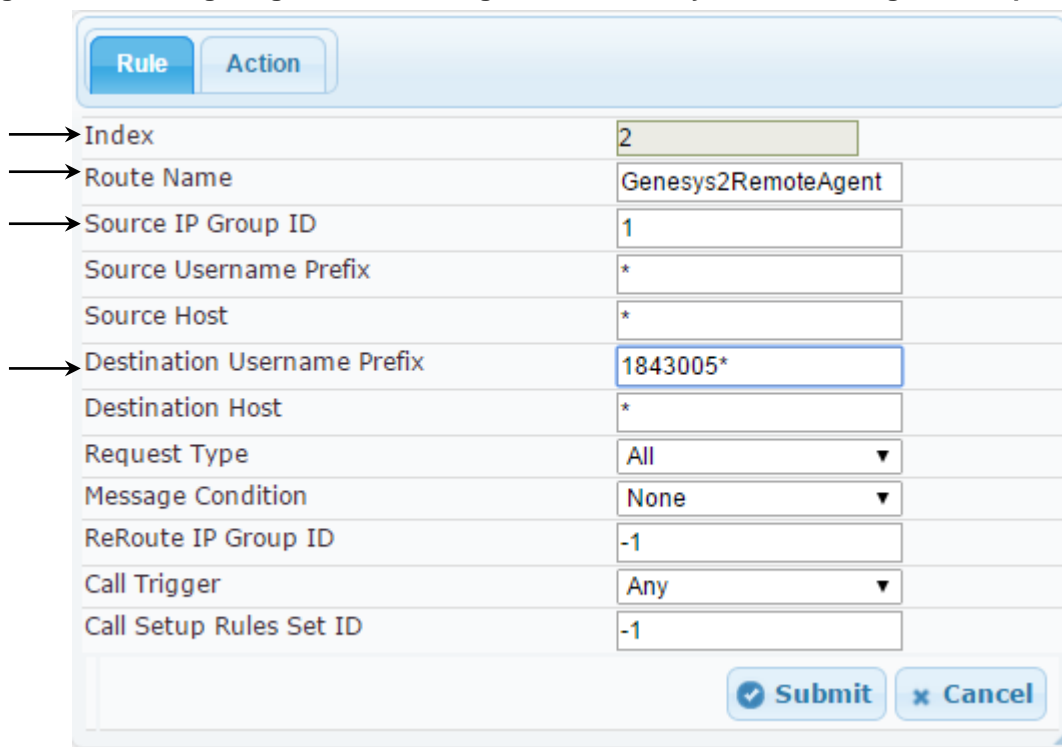
Action	
Index	8
Destination Type	IP Group
Destination IP Group ID	1
Destination SRD ID	1
Destination Address	
Destination Port	0
Destination Transport Type	
Alternative Route Options	Route Row
Group Policy	None
Cost Group	None

Submit Cancel

4. Configure a rule to route calls from the Genesys Contact Center to the Remote User Agent Group. Note 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 AOR.
 - 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	2
Route Name	Genesys2RemoteAgents (arbitrary descriptive name)
Source IP Group ID	1
Destination Username Prefix	1843005*

Figure 3-56: Configuring IP-to-IP Routing Rule for Genesys to Remote Agent Group – Rule tab



Rule	
Index	2
Route Name	Genesys2RemoteAgent
Source IP Group ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	1843005*
Destination Host	*
Request Type	All ▼
Message Condition	None ▼
ReRoute IP Group ID	-1
Call Trigger	Any ▼
Call Setup Rules Set ID	-1

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

Parameter	Value
Destination Type	IP Group
Destination IP Group ID	3
Destination SRD ID	3

Figure 3-57: Configuring IP-to-IP Routing Rule for Genesys to SIP Trunk – Action tab

The screenshot shows the 'Action' tab configuration for a routing rule. The 'Rule' tab is active. The 'Index' is set to 2. The 'Destination Type' is 'IP Group'. The 'Destination IP Group ID' is 3. The 'Destination SRD ID' is 3. The 'Destination Address' is empty. The 'Destination Port' is 0. The 'Destination Transport Type' is empty. The 'Alternative Route Options' is 'Route Row'. The 'Group Policy' is 'None'. The 'Cost Group' is 'None'. There are 'Submit' and 'Cancel' buttons at the bottom right.

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 lab 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 properly 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 3-58: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

Index	Route Name	Source Host	Destination Username Prefix	Destination Host	Message Condition	ReRoute IP Group ID	Call Trigger	Call Setup Rules Set ID	Destination Type	Destination ID
1	OPTIONS termination	*	*	*	None	-1	Any	-1	Dest Address	None
2	Genesys2RemoteAgents	*	18430052[3,4]	*	None	-1	Any	-1	IP Group	3
3	Genesys2ITSP	*	*	*	None	-1	Any	-1	IP Group	2
5	localagents	*	18430052*	*	None	-1	3xx or REFER	-1	IP Group	1
6	3xx/REFERS	*	*	*	None	-1	3xx or REFER	-1	IP Group	2
7	ITSP2Genesys	*	*	*	None	-1	Any	-1	IP Group	1
8	Remote2Genesys	*	*	*	None	-1	Any	-1	IP Group	1



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 11: Reset the SBC

After completing the configuration of the SBC, as described in this chapter, 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:**

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

Figure 3-59: Resetting the SBC

The screenshot displays a web-based configuration interface for an SBC. It is organized into three main sections, each with a dropdown arrow on the left:

- Reset Configuration:** This section contains three rows. The first row is 'Reset Board' with a 'Reset' button to its right. The second row is 'Burn To FLASH' with a dropdown menu set to 'Yes'. The third row is 'Graceful Option' with a dropdown menu set to 'No'.
- LOCK / UNLOCK:** This section contains three rows. The first row is 'Lock' with a 'LOCK' button to its right. The second row is 'Graceful Option' with a dropdown menu set to 'No'. The third row is 'Gateway Operational State' with the text 'UNLOCKED' to its right.
- Save Configuration:** This section contains one row: 'Burn To FLASH' with a 'BURN' button to its right.

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

This page is intentionally left blank.

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 4000
;Board Type: 70
;Serial Number: 3968219
;Slot Number: 1
;Software Version: 6.80A.261.013
;DSP Software Version: 5039AE3_R => 680.28
;Board IP Address: 10.38.20.40
;Board Subnet Mask: 255.255.255.0
;Board Default Gateway: 10.38.20.1
;Ram size: 2048M   Flash size: 252M
;Num of DSP Cores: 24   Num DSP Channels: 1584
;Num of physical LAN ports: 8
;Profile: NONE

;;Key features;;Board Type: Mediant 4000 ;Security: IPSEC MediaEncryption StrongEncryption
EncryptControlProtocol ;Channel Type: DspCh=2000 IPMediaDspCh=2000 ;HA ;QOE features:
VoiceQualityMonitoring MediaEnhancement ;DSP Voice features: RTCP-XR ;Coders: G723 G729
GSM-FR G727 G722 ;IP Media: VXML ;Control Protocols: MGCP SIP SBC=1000 MSFT CLI FEU=500
;Default features;;Coders: G711 G726;
```

[SYSTEM Params]

```
SyslogServerIP = 10.38.5.76
EnableSyslog = 1
;NTPServerIP_abs is hidden but has non-default value
NTPServerUTCOffset = -18000
DebugRecordingDestIP = 10.38.5.76
;VpFileLastUpdateTime is hidden but has non-default value
DayLightSavingTimeStart = '03:SUN/02:02:00'
DayLightSavingTimeEnd = '11:SUN/01:02:00'
DayLightSavingTimeEnable = 1
DebugRecordingStatus = 1
NTPServerIP = '10.38.5.73'
NTPSecondaryServerIP = '46.166.138.172'
LDAPSEARCHDNSINPARALLEL = 0
;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
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95
```

[Analog Params]

[ControlProtocols Params]

```
AdminStateLockControl = 0
```

[MGCP Params]

[MEGACO Params]

```
EP_Num_0 = 0
EP_Num_1 = 1
EP_Num_2 = 1
EP_Num_3 = 0
EP_Num_4 = 0
```

[Voice Engine Params]

```
NatMode = 2
ENABLEMEDIASEcurity = 1
```

[WEB Params]

```
LogoWidth = '145'
HTTPSCipherString = 'RC4:EXP'
;WebSessionTimeout is hidden but has non-default value
```

[SIP Params]

```
MEDIACHANNELS = 50
GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
ISUSERPHONEINFROM = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
GWOUTBOUNDMANIPULATIONSET = 19
```

ENERGYDETECTORCMD = 587202560

ANSWERDETECTORCMD = 10486144

[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_NativeVlan, PhysicalPortsTable_SpeedDuplex,
PhysicalPortsTable_PortDescription, PhysicalPortsTable_GroupMember,
PhysicalPortsTable_GroupStatus;

PhysicalPortsTable 0 = "GE_1", 1, 1, 4, "User Port #0", "GROUP_1", "Active";

PhysicalPortsTable 1 = "GE_2", 0, 1, 4, "User Port #1", "None", " ";

PhysicalPortsTable 2 = "GE_3", 1, 305, 4, "User Port #2", "GROUP_2", "Active";

PhysicalPortsTable 3 = "GE_4", 0, 305, 4, "User Port #3", "None", " ";

PhysicalPortsTable 4 = "GE_5", 1, 254, 4, "User Port #4", "GROUP_3", "Active";

PhysicalPortsTable 5 = "GE_6", 0, 254, 4, "User Port #5", "None", " ";

PhysicalPortsTable 6 = "GE_7", 0, 1, 4, "User Port #6", "None", " ";

PhysicalPortsTable 7 = "GE_8", 0, 1, 4, "User Port #7", "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_3", "";

EtherGroupTable 2 = "GROUP_3", 1, "GE_5", "";

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 ]
```

```
[ DeviceTable ]
```

```
FORMAT DeviceTable_Index = DeviceTable_VlanID, DeviceTable_UnderlyingInterface,  
DeviceTable_DeviceName;
```

```
DeviceTable 0 = 1, "GROUP_1", "vlan 1";
```

```
DeviceTable 1 = 305, "GROUP_2", "vlan 2";
```

```
DeviceTable 2 = 254, "GROUP_3", "vlan 3";
```

```
[ \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 = 0, 10, 10.38.20.40, 24, 10.38.20.1, "NETMGMT", 10.38.5.20, 0.0.0.0, "vlan 1";
```

```
InterfaceTable 1 = 5, 10, 10.38.5.12, 24, 10.38.5.1, "Trusted", 0.0.0.0, 0.0.0.0, "vlan 2";
```

```
InterfaceTable 2 = 5, 10, 173.227.254.68, 26, 173.227.254.65, "Untrusted", 0.0.0.0, 0.0.0.0, "vlan  
3";
```

```
[ \InterfaceTable ]
```

```
[ DspTemplates ]
```

```
;
```

```
; *** TABLE DspTemplates ***
```

```
; This table contains hidden elements and will not be exposed.
```

```
; This table exists on board and will be saved during restarts.
```

```
;
```

```
[ \DspTemplates ]
```

```
[ CpMediaRealm ]
```

```
FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName, CpMediaRealm_IPv4IF,  
CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart, CpMediaRealm_MediaSessionLeg,  
CpMediaRealm_PortRangeEnd, CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile,  
CpMediaRealm_BWPProfile;
```

```
CpMediaRealm 1 = "MR1-SBC2Genesys", "Trusted", "", 6000, 100, 6990, 1, "", "";
```

```
CpMediaRealm 2 = "MR2-SBC2ITSP", "Untrusted", "", 10000, 100, 10990, 0, "", "";
```

```

CpMediaRealm 3 = "MR3-RemoteAgents", "Untrusted", "", 9000, 100, 9990, 0, "", "";

[ \CpMediaRealm ]

[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_MediaRealm, SRD_IntraSRDMediaAnchoring,
SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers, SRD_EnableUnAuthenticatedRegistrations;
SRD 1 = "SRD1-Genesys", "MR1-SBC2Genesys", 0, 0, -1, 1;
SRD 2 = "SRD2-ITSP", "MR2-SBC2ITSP", 0, 0, -1, 1;
SRD 3 = "SRD3-RemoteAgents", "MR3-RemoteAgents", 0, 0, -1, 1;

[ \SRD ]

[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType, ProxyIp_ProxySetId;
ProxyIp 0 = "10.38.5.107", -1, 1;
ProxyIp 1 = "195.54.103.138", 0, 2;

[ \ProxyIp ]

[ 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_SBCDiversionsMode,
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_SBCPlayRBTTToTransferee,
IpProfile_SBCRTCPMode, IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection, IpProfile_JitterBufMaxDelay,
IpProfile_SBCRemoteMultipleAnswersMode, IpProfile_SBCKeepVIAHeaders,
IpProfile_SBCKeepUserAgentHeader, IpProfile_SBCUserBehindUdpNATRegistrationTime,
IpProfile_SBCUserBehindTcpNATRegistrationTime;

```

```

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, 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, 0, 0, 0, 0, 0, 0, 0, 300, 0, -1, -1, -1, -1;
IpProfile 2 = "Telenor", 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, "audio", 1, -1, 2, 0, 0, 0, 1, 0, 8, 300, 400, 1, 0, 0, -1, 0, 0, 1, 3, 2, 0, 0, 1, 3, 0, 1, 0, 1,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 300, 0, -1, -1, -1, -1;
IpProfile 3 = "Remote Agents", 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, 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, 0, 0, 0, 0, 0, 0, 0, 300, 0, -1, -1, -1, -1;

```

[\IpProfile]

[ProxySet]

```

FORMAT ProxySet_Index = ProxySet_ProxyName, ProxySet_EnableProxyKeepAlive,
ProxySet_ProxyKeepAliveTime, ProxySet_ProxyLoadBalancingMethod,
ProxySet_IsProxyHotSwap, ProxySet_SRD, ProxySet_ClassificationInput, ProxySet_TLSContext,
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,
ProxySet_KeepAliveFailureResp;
ProxySet 0 = "", 0, 60, 0, 0, 0, 0, "-1", -1, -1, "";
ProxySet 1 = "Genesys SIP Server", 1, 60, 0, 0, 1, 0, "-1", -1, -1, "";
ProxySet 2 = "Telenor ITSP", 1, 60, 0, 0, 2, 0, "-1", -1, -1, "";

```

[\ProxySet]

[IPGroup]

```

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description, IPGroup_ProxySetId,
IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_EnableSurvivability,
IPGroup_ServingIPGroup, IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable,
IPGroup_RoutingMode, IPGroup_SRD, IPGroup_MediaRealm, IPGroup_ClassifyByProxySet,
IPGroup_ProfileId, IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet,
IPGroup_OutboundManSet, IPGroup_RegistrationMode, IPGroup_AuthenticationMode,
IPGroup_MethodList, IPGroup_EnableSBCCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username, IPGroup_Password,
IPGroup_UUIFormat, IPGroup_QOEProfile, IPGroup_BWProfile,
IPGroup_MediaEnhancementProfile, IPGroup_AlwaysUseSourceAddr,

```

```

IPGroup_MsgManUserDef1, IPGGroup_MsgManUserDef2, IPGGroup_SIPConnect,
IPGroup_SBCRouteUsingRequestURIPort;
IPGroup 1 = 0, "IPG1-SBC2Genesys", 1, "", "", 0, -1, -1, 0, -1, 1, "MR1-SBC2Genesys", 1, 1, -1, -1, -
1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "", "", 0, "", "", 0, 0;
IPGroup 2 = 0, "IPG2-SBC2ITSP", 2, "", "", 0, -1, -1, 0, -1, 2, "MR2-SBC2ITSP", 1, 2, -1, -1, 3, 0, 0, "",
0, -1, -1, "", "", "$1$gQ==", 0, "", "", "", 0, "", "", 0, 0;
IPGroup 3 = 1, "Remote Agents", -1, "", "", 0, -1, -1, 0, -1, 3, "MR3-RemoteAgents", 0, 3, -1, -1, -1,
0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "", "", 0, "", "", 0, 0;

[ \IPGroup ]

[ Account ]

FORMAT Account_Index = Account_ServedTrunkGroup, Account_ServedIPGroup,
Account_ServingIPGroup, Account_Username, Account_Password, Account_HostName,
Account_Register, Account_ContactUser, Account_ApplicationType;
Account 0 = -1, 2, 1, "1234567890", "$1$S3p+fno=", "", 0, "", 2;

[ \Account ]

[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName, IP2IPRouting_SrcIPGroupID,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost, IP2IPRouting_DestUsernamePrefix,
IP2IPRouting_DestHost, IP2IPRouting_RequestType, IP2IPRouting_MessageCondition,
IP2IPRouting_ReRouteIPGroupID, IP2IPRouting_Trigger, IP2IPRouting_CallSetupRulesSetId,
IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID, IP2IPRouting_DestSRDID,
IP2IPRouting_DestAddress, IP2IPRouting_DestPort, IP2IPRouting_DestTransportType,
IP2IPRouting_AltRouteOptions, IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup;
IP2IPRouting 1 = "OPTIONS termination", -1, "*", "*", "*", "*", 6, "", -1, 0, -1, 1, -1, "", "internal",
0, -1, 0, 0, "";
IP2IPRouting 2 = "Genesys2RemoteAgent", 1, "*", "*", "18430052[3,4]", "*", 0, "", -1, 0, -1, 0, 3,
"3", "", 0, -1, 0, 0, "";
IP2IPRouting 3 = "Genesys2ITSP", 1, "*", "*", "*", "*", 0, "", -1, 0, -1, 0, 2, "2", "", 0, -1, 0, 0, "";
IP2IPRouting 5 = "localagents", 2, "*", "*", "18430052*", "*", 0, "", -1, 3, -1, 0, 1, "1", "", 0, -1, 0,
0, "";
IP2IPRouting 6 = "3xx/REFERS", 2, "*", "*", "*", "*", 0, "", -1, 3, -1, 0, 2, "2", "", 0, -1, 0, 0, "";
IP2IPRouting 7 = "ITSP2Genesys", 2, "*", "*", "*", "*", 0, "", -1, 0, -1, 0, 1, "1", "", 0, -1, 0, 0, "";
IP2IPRouting 8 = "Remote2Genesys", 3, "*", "*", "*", "*", 0, "", -1, 0, -1, 0, 1, "1", "", 0, -1, 0, 0, "";

[ \IP2IPRouting ]

[ Classification ]

FORMAT Classification_Index = Classification_ClassificationName,
Classification_MessageCondition, Classification_SrcSRDID, Classification_SrcAddress,
Classification_SrcPort, Classification_SrcTransportType, Classification_SrcUsernamePrefix,

```

```

Classification_SrcHost, Classification_DestUsernamePrefix, Classification_DestHost,
Classification_ActionType, Classification_SrcIPGroupID;
Classification 2 = "home", "", "3", "71.65.244.160", 0, -1, "*", "*", "*", "*", 1, "3";
Classification 3 = "remote Agent", "", "3", "50.52.146.54", 0, -1, "*", "*", "*", "*", 1, "3";

[ \Classification ]

[ 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, 0.0.0.0, 0.0.0.0, 2560, 0;

[ \TLSContexts ]

[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName, SIPInterface_NetworkInterface,
SIPInterface_ApplicationType, SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
SIPInterface_SRD, SIPInterface_MessagePolicy, SIPInterface_TLSContext,
SIPInterface_TLSMutualAuthentication, SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType, SIPInterface_PreClassificationManSet;
SIPInterface 1 = "Genesys", "Trusted", 2, 5060, 5060, 5061, 1, "", "", -1, 0, 500, -1;
SIPInterface 2 = "ITSP", "Untrusted", 2, 5060, 5060, 5061, 2, "", "", -1, 0, 500, -1;
SIPInterface 3 = "RemoteAgents", "Untrusted", 2, 5070, 5070, 5071, 3, "", "", -1, 0, 500, -1;

[ \SIPInterface ]

[ IPInboundManipulation ]

FORMAT IPInboundManipulation_Index = IPInboundManipulation_ManipulationName,
IPInboundManipulation_IsAdditionalManipulation,
IPInboundManipulation_ManipulationPurpose, IPInboundManipulation_SrcIPGroupID,
IPInboundManipulation_SrcUsernamePrefix, IPInboundManipulation_SrcHost,
IPInboundManipulation_DestUsernamePrefix, IPInboundManipulation_DestHost,
IPInboundManipulation_RequestType, IPInboundManipulation_ManipulatedURI,
IPInboundManipulation_RemoveFromLeft, IPInboundManipulation_RemoveFromRight,
IPInboundManipulation_LeaveFromRight, IPInboundManipulation_Prefix2Add,
IPInboundManipulation_Suffix2Add;
IPInboundManipulation 1 = "remove +46 CC", 0, 0, 2, "*", "*", "*", "*", 4, 1, 3, 0, 255, "", "";
IPInboundManipulation 2 = "rm SBC access code", 0, 0, 1, "*", "*", "77", "*", 0, 1, 2, 0, 255, "", "";

[ \IPInboundManipulation ]

[ IPOutboundManipulation ]

```

```

FORMAT IPOutboundManipulation_Index = IPOutboundManipulation_ManipulationName,
IPOutboundManipulation_IsAdditionalManipulation, IPOutboundManipulation_SrcIPGroupID,
IPOutboundManipulation_DestIPGroupID, IPOutboundManipulation_SrcUsernamePrefix,
IPOutboundManipulation_SrcHost, IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_DestHost, IPOutboundManipulation_CallingNamePrefix,
IPOutboundManipulation_MessageCondition, IPOutboundManipulation_RequestType,
IPOutboundManipulation_ReRouteIPGroupID, IPOutboundManipulation_Trigger,
IPOutboundManipulation_ManipulatedURI, IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight, IPOutboundManipulation_LeaveFromRight,
IPOutboundManipulation_Prefix2Add, IPOutboundManipulation_Suffix2Add,
IPOutboundManipulation_PrivacyRestrictionMode;
IPOutboundManipulation 0 = "20 ext dest REFER HL", 0, 2, 2, "*", "*", "*", "*", "", 0, -1, 0, 1,
0, 0, 255, "+", "", 0;
IPOutboundManipulation 1 = "rm CC from To:", 0, 10, 2, "46*", "*", "*", "*", "", 0, -1, 0, 1, 2,
0, 255, "", "", 0;
IPOutboundManipulation 2 = "e164 international", 0, 1, 2, "*", "*", "*", "*", "", 0, -1, 0, 1, 0,
0, 255, "+", "", 0;
IPOutboundManipulation 3 = "e164 source", 0, 1, 2, "*", "*", "*", "*", "", 0, -1, 0, 0, 0, 255,
"+46", "", 0;

[ \IPOutboundManipulation ]

[ CodersGroup0 ]

FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce,
CodersGroup0_CoderSpecific;
CodersGroup0 0 = "g711Alaw64k", 20, 0, -1, 0, "";
CodersGroup0 1 = "g711Ulaw64k", 20, 0, -1, 0, "";

[ \CodersGroup0 ]

[ CodersGroup1 ]

FORMAT CodersGroup1_Index = CodersGroup1_Name, CodersGroup1_pTime,
CodersGroup1_rate, CodersGroup1_PayloadType, CodersGroup1_Sce,
CodersGroup1_CoderSpecific;
CodersGroup1 0 = "g711Alaw64k", 20, 0, -1, 0, "";
CodersGroup1 1 = "g711Ulaw64k", 20, 0, -1, 0, "";

[ \CodersGroup1 ]

[ AllowedCodersGroup1 ]

FORMAT AllowedCodersGroup1_Index = AllowedCodersGroup1_Name;
AllowedCodersGroup1 0 = "g711Alaw64k";
AllowedCodersGroup1 1 = "g711Ulaw64k";

```

```
[ \AllowedCodersGroup1 ]

[ AllowedCodersGroup2 ]

FORMAT AllowedCodersGroup2_Index = AllowedCodersGroup2_Name;
AllowedCodersGroup2 0 = "g711Alaw64k";

[ \AllowedCodersGroup2 ]

[ MessageManipulations ]

FORMAT MessageManipulations_Index = MessageManipulations_ManipulationName,
MessageManipulations_ManSetID, MessageManipulations_MessageType,
MessageManipulations_Condition, MessageManipulations_ActionSubject,
MessageManipulations_ActionType, MessageManipulations_ActionValue,
MessageManipulations_RowRole;
MessageManipulations 1 = "dest ip in r-uri", 3, "invite.request", "", "header.request-uri.url.host",
2, "param.message.address.dst.address", 0;
MessageManipulations 2 = "add user=p r.uri", 3, "invite.request", "", "header.request-
uri.url.userphone", 2, "'1'", 0;
MessageManipulations 3 = "add user=phone To", 3, "Invite.Request", "",
"header.to.url.userphone", 2, "'1'", 0;
MessageManipulations 4 = "add user=phone From", 3, "invite.request", "",
"header.from.url.userphone", 2, "'1'", 0;
MessageManipulations 5 = "topology hide From", 3, "invite.request", "", "header.from.url.host",
2, "param.message.address.src.address", 0;
MessageManipulations 6 = "dest in To host", 3, "Invite.Request", "", "header.to.url.host", 2,
"param.message.address.dst.address", 0;
MessageManipulations 7 = "topology hide PAI", 3, "invite.request", "header.p-asserted-identity
exists", "header.p-asserted-identity.url.host", 2, "param.message.address.src.address", 0;
MessageManipulations 8 = "contact header e164", 3, "invite.request", "",
"header.contact.url.user", 3, "'+46'", 0;
MessageManipulations 9 = "302 MT diversion", 3, "invite.response.302", "", "header.diversion",
0, "header.to.url.user + '<sip:' + header.to.url.user + '@imtx.telenor.se;user=phone>'";
MessageManipulations 10 = "REFER Contact e164", 3, "invite.response.302", "header.contact
regex (<sip:)(.*)@(.*)(>)", "header.contact", 2, "$1+ '+'$2+'@'+imtx.telenor.se'
+';user=phone'+$4", 0;

[ \MessageManipulations ]

[ RoutingRuleGroups ]

FORMAT RoutingRuleGroups_Index = RoutingRuleGroups_LCReEnable,
RoutingRuleGroups_LCRAverageCallLength, RoutingRuleGroups_LCRDefaultCost;
RoutingRuleGroups 0 = 0, 0, 1;
```

```
[ \RoutingRuleGroups ]
```

```
[ LoggingFilters ]
```

```
FORMAT LoggingFilters_Index = LoggingFilters_FilterType, LoggingFilters_Value,  
LoggingFilters_Syslog, LoggingFilters_CaptureType;  
LoggingFilters 0 = 1, "", -1, 3;
```

```
[ \LoggingFilters ]
```

```
[ ResourcePriorityNetworkDomains ]
```

```
FORMAT ResourcePriorityNetworkDomains_Index = ResourcePriorityNetworkDomains_Name,  
ResourcePriorityNetworkDomains_Ip2TelInterworking;  
ResourcePriorityNetworkDomains 1 = "dsn", 0;  
ResourcePriorityNetworkDomains 2 = "dod", 0;  
ResourcePriorityNetworkDomains 3 = "drsn", 0;  
ResourcePriorityNetworkDomains 5 = "uc", 1;  
ResourcePriorityNetworkDomains 7 = "cuc", 0;
```

```
[ \ResourcePriorityNetworkDomains ]
```




Configuration Note

