Session Border Controllers (SBC)

AudioCodes Mediant™ Series

Interoperability Lab

Configuration Note

Genesys Contact Center & Colt SIP Trunk using AudioCodes Mediant SBC

June 2014

Document # LTRT-12310

Table of Contents

1 Introduction 7

1.1 Intended Audience 7
1.2 About AudioCodes SBC Product Series 7
1.3 About Genesys Contact Center 7

2 Component Information 9

2.1 AudioCodes SBC Version 9
2.2 Colt SIP Trunking Version 9
2.3 Genesys Contact Center Version 9
2.4 Interoperability Test Topology 10
2.4.1 Environment Setup 12
2.4.2 Known Limitations/Restrictions 12

3 Configuring AudioCodes SBC 13

3.1 Step 1: Configure IP Network Interfaces 14
3.1.1 Step 1a: Configure VLANs 15
3.1.2 Step 1b: Configure Network Interfaces 15
3.1.3 Step 1c: Configure the Native VLAN ID 17
3.2 Step 2: Enable the SBC Application 17
3.3 Step 3: Configure Signaling Routing Domains 18
3.3.1 Step 3a: Configure Media Realms 18
3.3.2 Step 3b: Configure SRDs 20
3.3.3 Step 3c: Configure SIP Signaling Interfaces 21
3.4 Step 4: Configure Proxy Sets 23
3.5 Step 5: Configure IP Groups 26
3.6 Step 6: Configure IP Profiles 31
3.7 Step 7: Configure Coders 36
3.8 Step 8: Configure IP-to-IP Call Routing Rules 37
3.9 Step 9: Configure IP-to-IP Manipulation Rules 43
3.10 Step 10: Remote Agents 46
3.10.1 Step 10a: Configure Media Realm for Remote Agent 46
3.10.2 Step 10b: Configure SRD for Remote Agent 47
3.10.3 Step 10c: Configure SIP Signaling Interfaces for Remote Agent 48
3.10.4 Step 10d: Configure Remote (User) Agents IP Group 49
3.10.5 Step 10e: Configure IP Profiles for Remote Agents 51
3.10.6 Step 10f: Configure Classification Table for Remote Agents 53
3.10.7 Step 10g: Configure IP-to-IP Call Routing Rules for Remote (User) Agent 55
3.11 Step 11: Reset the SBC 60

A AudioCodes *ini* File 61

This page is intentionally left blank

Notice

This Note shows how to connect a Genesys Contact Center and Colt SIP Trunk using AudioCodes Mediant SBC product series.

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published, nor can it accept responsibility for errors or omissions. Updates to this document and other documents as well as software files can be viewed by registered customers at http://www.audiocodes.com/downloads.

Date Published: June-24-2014

Trademarks

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our Web site at www.audiocodes.com/support.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at http://www.audiocodes.com/downloads.

This page is intentionally left blank

1 Introduction

This document shows how to configure AudioCodes' Session Border Controller (hereafter referred to as SBC) for interworking between Colt's 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 Colt's SIP Trunk and Genesys Contact Center for enabling VoIP calls using AudioCodes' SBC.

1.2 About AudioCodes SBC Product Series

AudioCodes' family of SBC devices enables reliable connectivity and security between the enterprise and the Service Provider's VoIP networks.

The SBC provides perimeter defense as a way of protecting enterprises from malicious VoIP attacks; mediation for allowing the connection of any PBX and/or IP PBX to any Service Provider; and Service Assurance for service quality and manageability.

Designed as a cost-effective appliance, the SBC is based on field-proven VoIP and network services with a native host processor, allowing the creation of purpose-built multiservice appliances, providing smooth connectivity to cloud services, with integrated quality of service, SLA monitoring, security and manageability.

The native implementation of SBC provides a host of additional capabilities that are not possible with standalone SBC appliances such as VoIP mediation, PSTN access survivability, and third-party value-added services applications. This enables enterprises to utilize the advantages of converged networks and eliminate the need for standalone appliances.

AudioCodes' SBC is available as an integrated solution running on top of its field-proven Mediant Media Gateway and Multi-Service Business Router (MSBR) platforms, or as a software-only solution for deployment with third-party hardware.

1.3 About Genesys Contact Center

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

This page is intentionally left blank

2 Component Information

2.1 AudioCodes SBC Version

Table 2-1: AudioCodes SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 500 E-SBC ▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 4000 SBC ▪ Mediant 9000 SBC ▪ Mediant Software SBC (Server Edition and Virtual Edition)
Software Version	SIP_ 6.80A.218.002
Protocol	▪ SIP/UDP (to the Colt SIP Trunk) ▪ SIP/UDP, TCP or TLS (to the Genesys Contact Center system)
Additional Notes	None

2.2 Colt SIP Trunking Version

Table 2-2: Colt Version

Vendor/Service Provider	Colt
SSW Model/Service	Sonus
Software Version	8.4.4
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 Colt ITSP SIP Trunk Provider via an SBC in similar way to an IP-PBX.

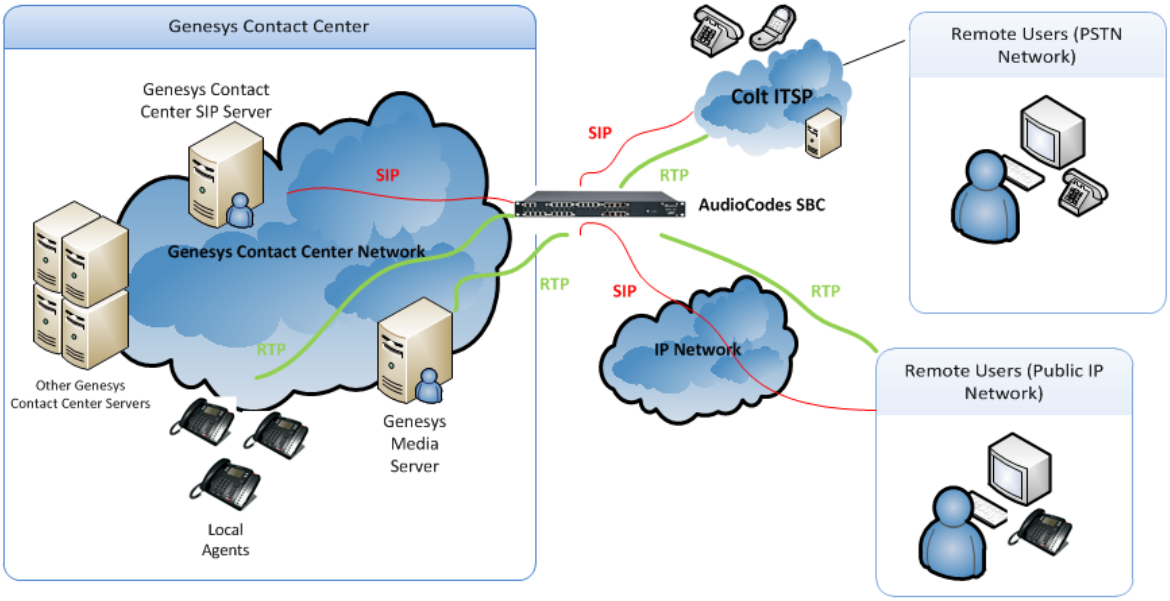
Note: Contact your Genesys Contact Center support channel for more information about topological scenarios.

Interoperability testing between AudioCodes SBC and Colt 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 the Genesys Contact Center system to the PSTN network using Colt's SIP Trunking service (Internet Telephony Service Provider / ITSP).
- The Colt SIP Trunk connected to the enterprise using the public external network.
- The AudioCodes' SBC is deployed to interconnect between the Genesys Contact Center 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 Colt SIP Trunk located on the public network.
  - RTP from/to Colt 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	▪ Genesys Contact Center environment as a service is located on the Genesys Contact Center network ▪ Genesys Contact Center agent DN's (SIP phones) are located on the enterprise's LAN. Remote agent DN's are located in the public network ▪ Colt SIP Trunk is located on the WAN
Signaling Transcoding	▪ Genesys Contact Center operates with SIP-over-UDP, TCP or TLS transport type ▪ Colt SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	▪ Genesys Contact Center supports G.729, G.711A-law, G.711U-law, G.723 and G722.2 and G.726 coders ▪ Colt SIP Trunk supports G.729, G.711A-law, and G.726 coders
Media Transcoding	▪ Genesys Contact Center and Colt SIP Trunk operate with RTP
DTMF	▪ Genesys Contact Center supports delivering DTMF using SIP INFO message, RFC 2833 Named Telephony events, and in-band per ITU-T Recommendation Q.23 ▪ Colt supports only RFC 2833

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

2.4.2 Known Limitations/Restrictions

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

- SIP 302 Temporarily Moved. Colt ACKs the SIP 302, however does not re-route the call into the external network. This scenario can be mitigated by handling the SIP 302 locally on the SBC.
- SIP Authentication for outbound calls. Colt does not support challenging the SIP User Agent on receiving a SIP Request (outbound from the Contact Center).
- SIP Authentication for inbound calls. Colt does not support challenge/authentication for outbound calls from Colt (inbound to the Contact Center).

3 Configuring AudioCodes SBC

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

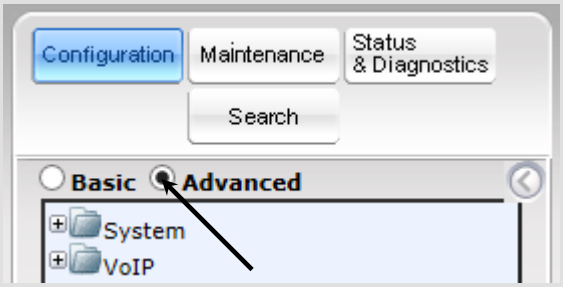
- SBC WAN interface - Colt SIP Trunking environment
- SBC LAN interface - Genesys Contact Center environment

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

Notes:

- To implement the Genesys Contact Center and Colt 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:



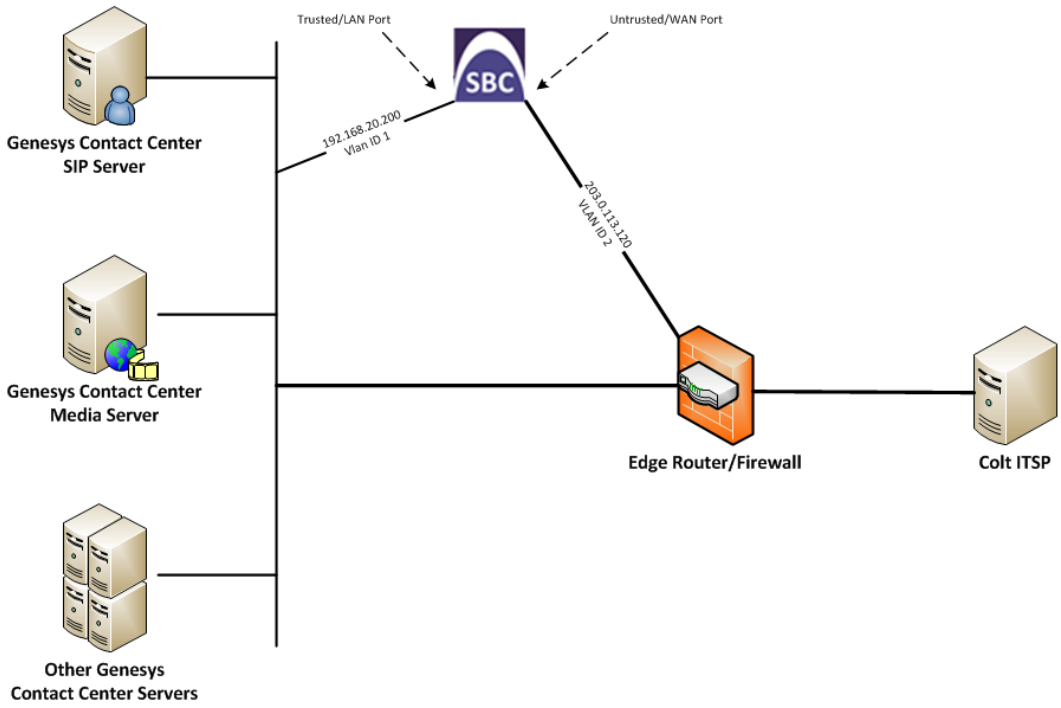
Note that when the SBC is reset, the navigation tree reverts to **Basic** display mode.

3.1 Step 1: Configure IP Network Interfaces

This step shows 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)
  - Colt 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 shows how to define VLANs for each of the following interfaces:

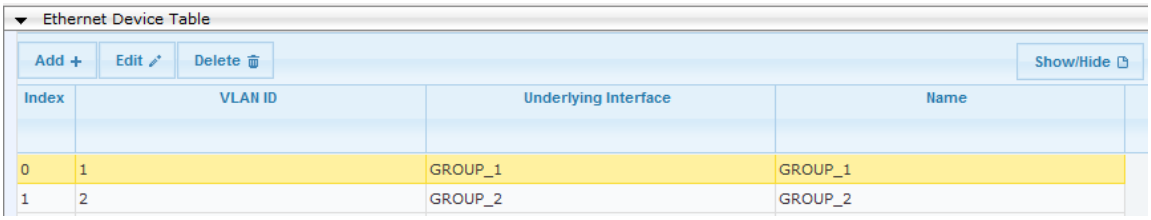
- LAN VoIP (assigned the name "Call Center")
- WAN VoIP (assigned the name "Provider")

➢ **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



3.1.2 Step 1b: Configure Network Interfaces

This step shows 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**

Parameter	Value
VLAN ID	**1**
Interface Name	**Trusted** (arbitrary descriptive name)
Primary DNS Server IP Address	Add DNS Server IP address in this network
Underlying Device	**GROUP_1**

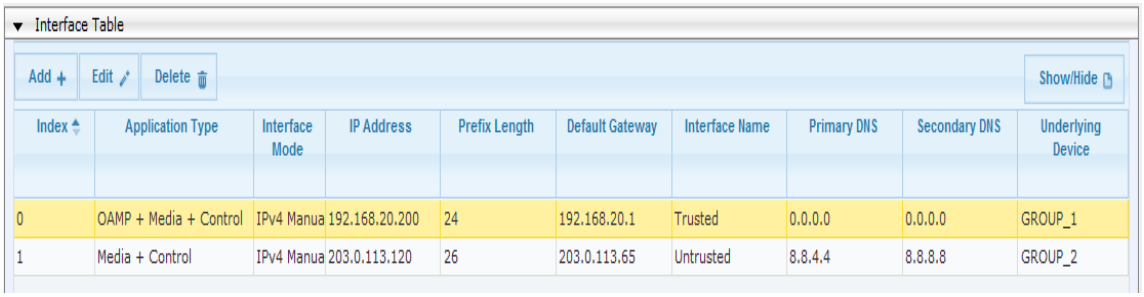
3. Add a network interface for the WAN side:
   a. Enter **1**, and then click **Add Index**.
   b. Configure the interface as follows:

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)
VLAN ID	**2**
Interface Name	**Untrusted**
Primary DNS Server IP Address	**8.8.4.4** (as specificed 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



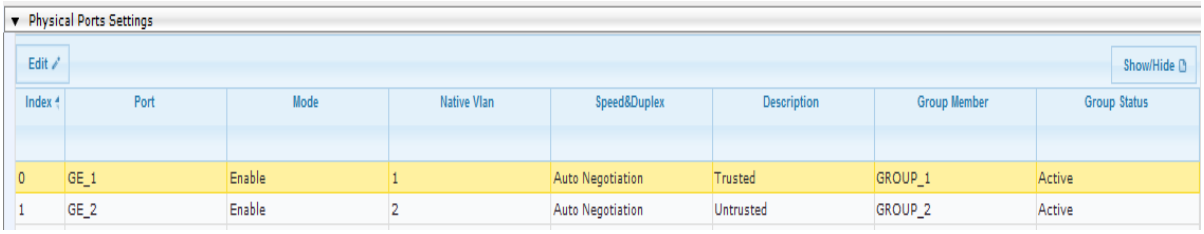
3.1.3 Step 1c: Configure the Native VLAN ID

This step shows 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



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 shows 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 3.11 on page 60).

3.3 Step 3: Configure Signaling Routing Domains

This step shows 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

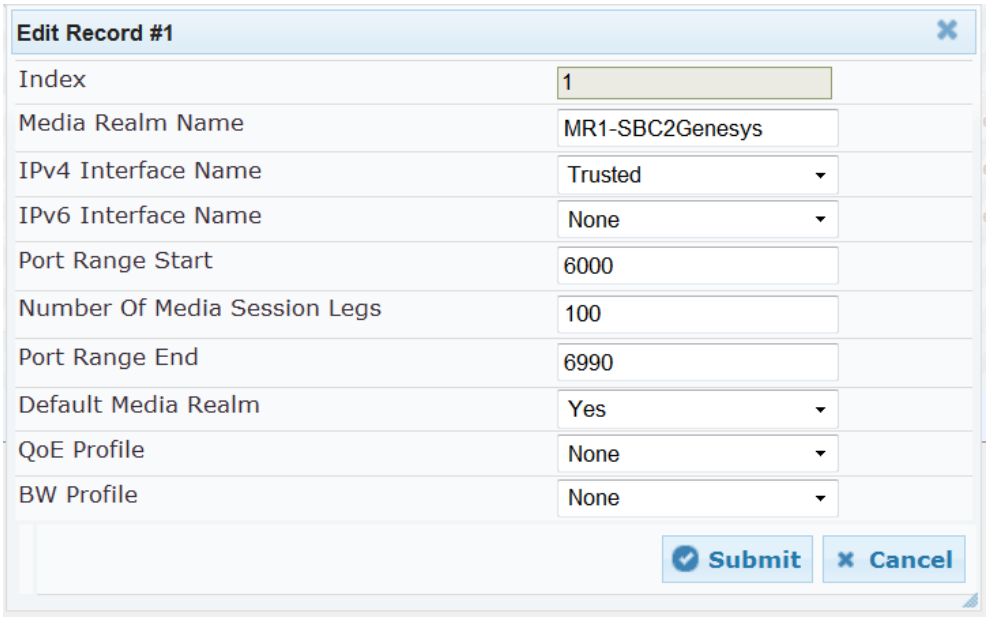
This step shows how to configure Media Realms. The simplest way is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➢ **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)

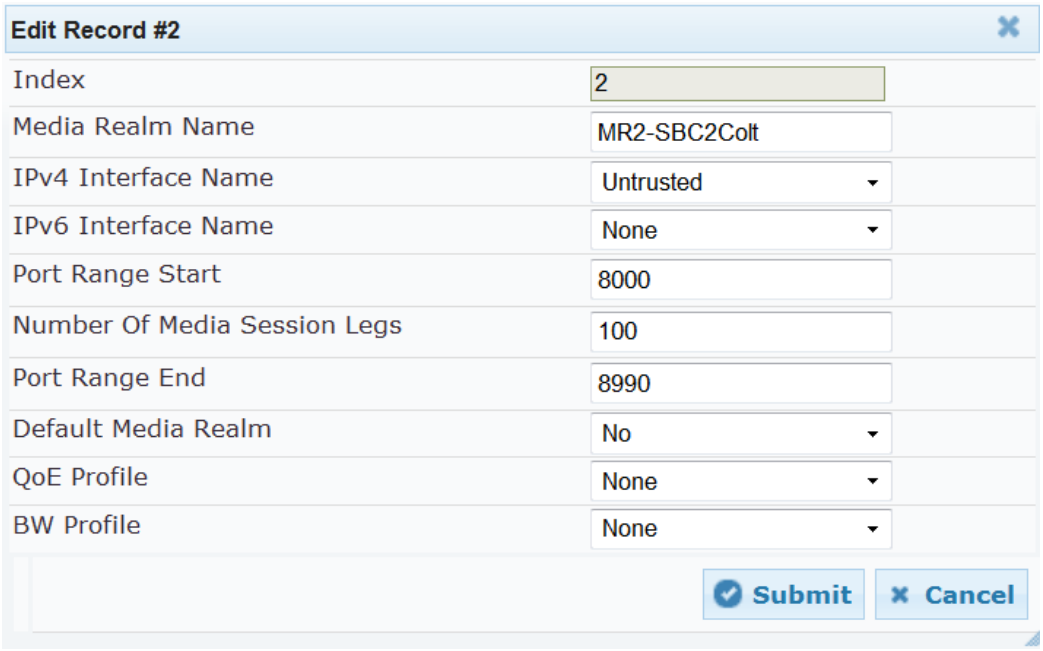
Figure 3-6: Configuring Media Realm for LAN



3. Configure a Media Realm for WAN traffic:

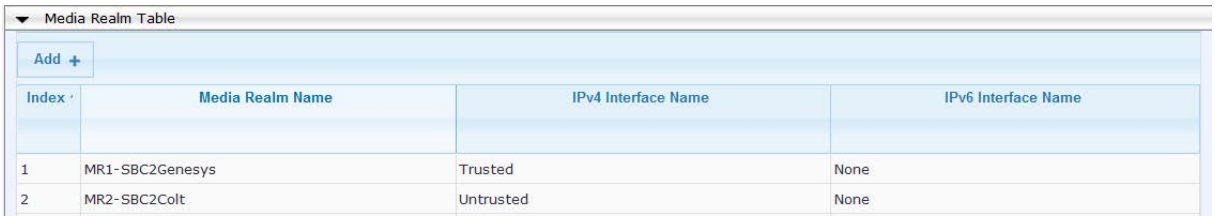
Parameter	Value
Index	**2**
Media Realm Name	**MR2-SBC2Colt** (arbitrary name)
IPv4 Interface Name	**Provider**
Port Range Start	**8000** (represents lowest UDP port number used for media on WAN)
Number of Media Session Legs	**100** (media sessions assigned with port range)

Figure 3-7: Configuring Media Realm for WAN



The configured Media Realms are shown in the figure below:

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



3.3.2 Step 3b: Configure SRDs

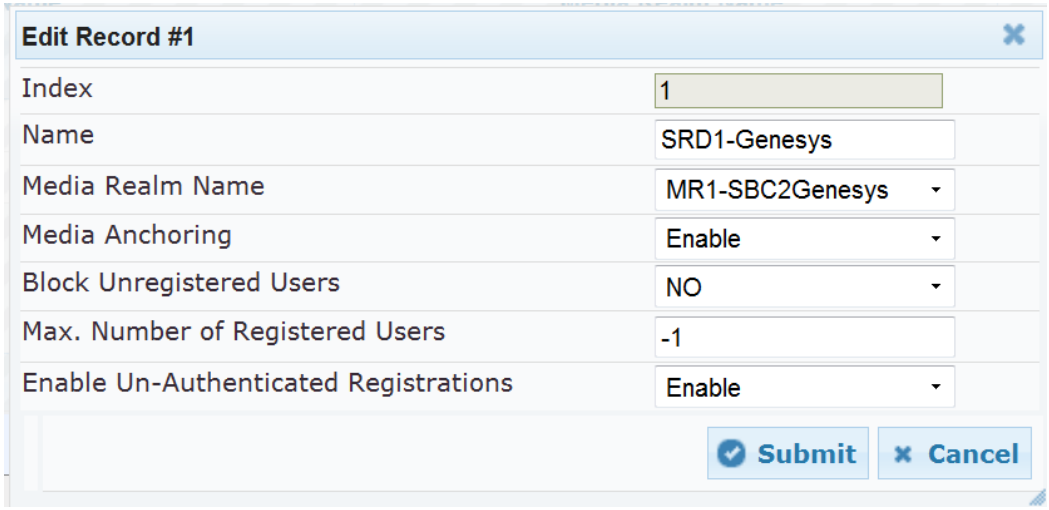
This step shows how to configure SRDs. For the interoperability test topology, an SRD for the SBC's internal (toward Genesys Contact Center) and external interfaces (toward the Colt SIP Trunk) are defined.

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

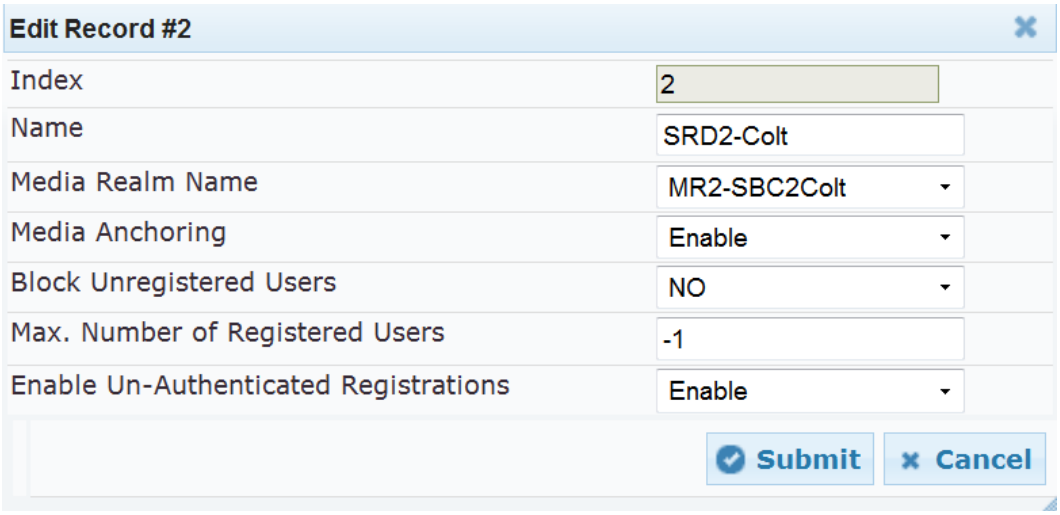
Figure 3-9: Configuring LAN SRD



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

Parameter	Value
SRD Index	**2**
SRD Name	**SRD2-Colt**
Media Realm	**MR2-SBC2Colt**

Figure 3-10: Configuring WAN SRD



3.3.3 Step 3c: Configure SIP Signaling Interfaces

This step shows 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:

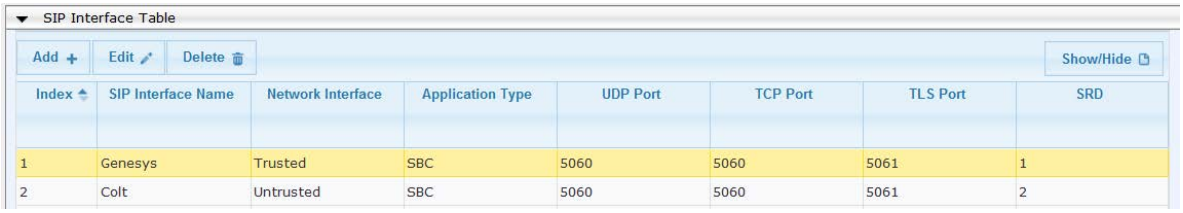
Parameter	Value
Index	**1**
Interface Name	**Genesys** (arbitrary descriptive name)
Network Interface	**Trusted**
Application Type	**SBC**
TCP and UDP	**5060**
TLS Port	**5061**
SRD	**1**

3. Configure a SIP interface for the WAN:

Parameter	Value
Index	**2**
Interface Name	**Colt** (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	Colt	Untrusted	SBC	5060	5060	5061	2

3.4 Step 4: Configure Proxy Sets

This step shows 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
- Colt SIP Trunk

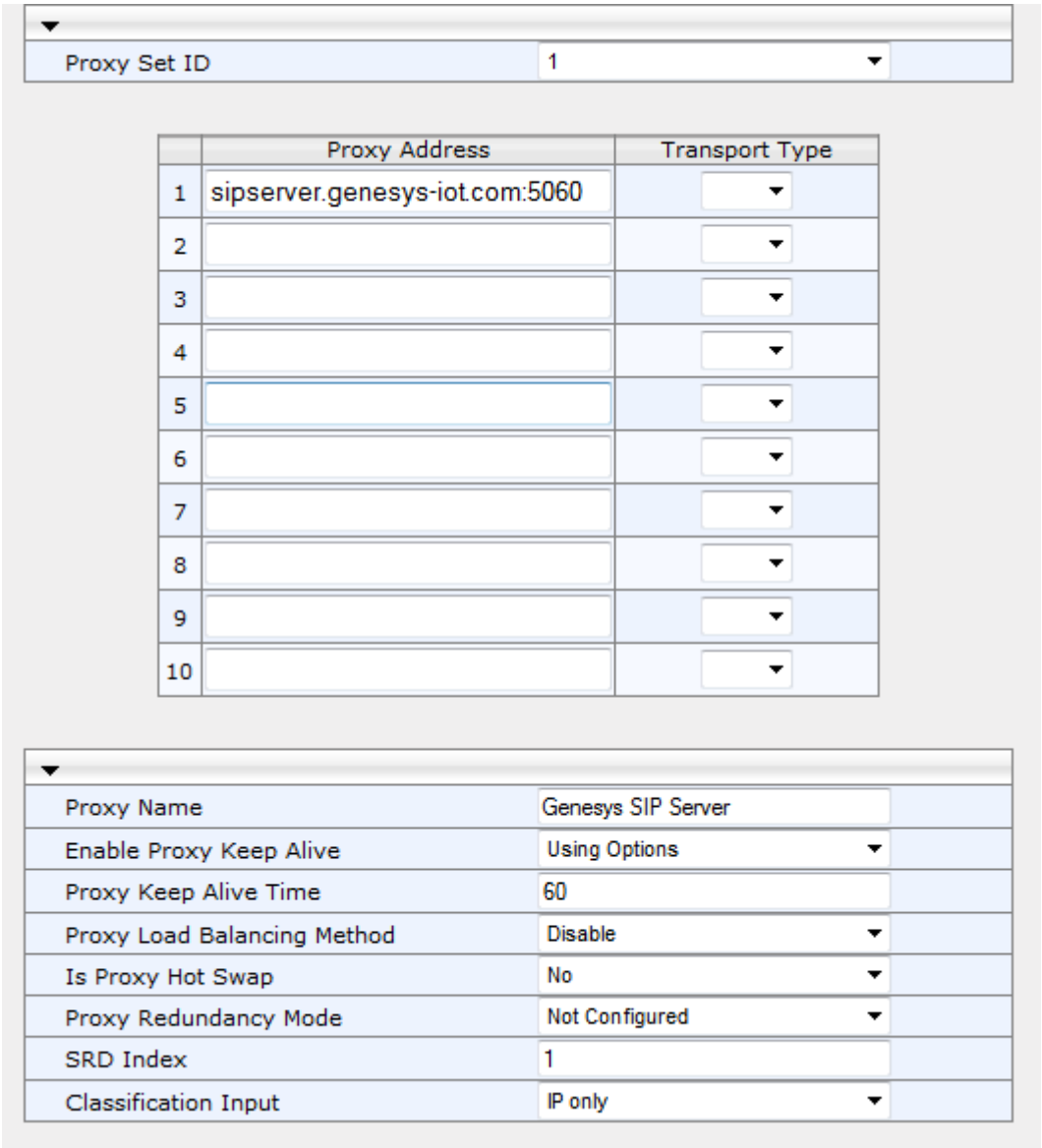
These Proxy Sets will later be associated with IP Groups.

➢ **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**

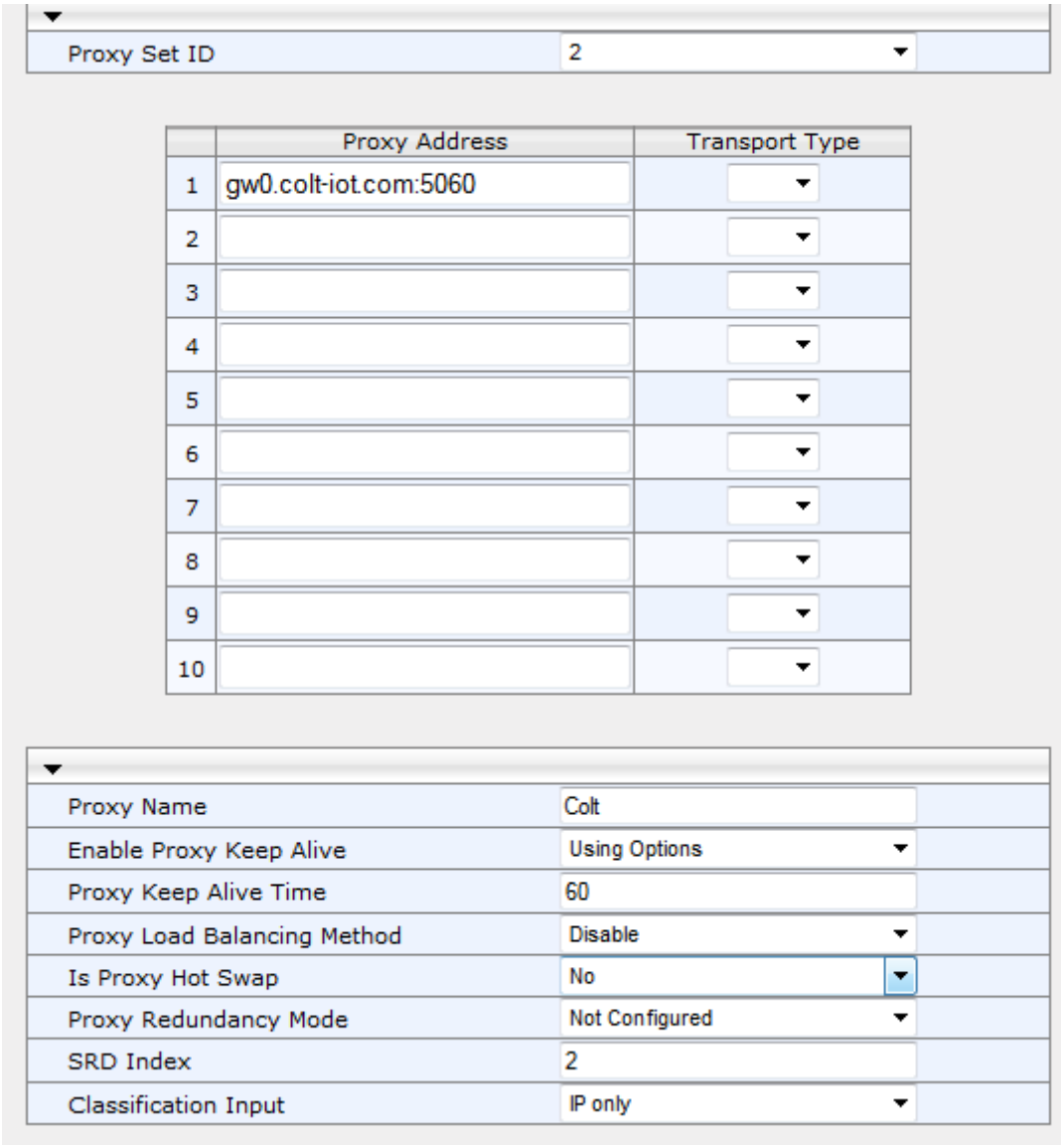
Figure 3-12: Configuring Proxy Set for Genesys Contact Center SIP Server



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

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

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



3.5 Step 5: Configure IP Groups

This step shows how to configure IP Groups. The IP Group represents an IP entity on the network with which the SBC communicates. This can be a server (e.g., IP PBX or ITSP) or it can be a group of users (e.g., LAN IP phones). For servers, the IP Group is typically used to define the server's IP address by associating it with a Proxy Set. 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)
- Colt SIP Trunk located on WAN (Server Group)
- Remote User Agents located in the WAN (User Group) (see Section 3.10 on page 46)

➢ **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)

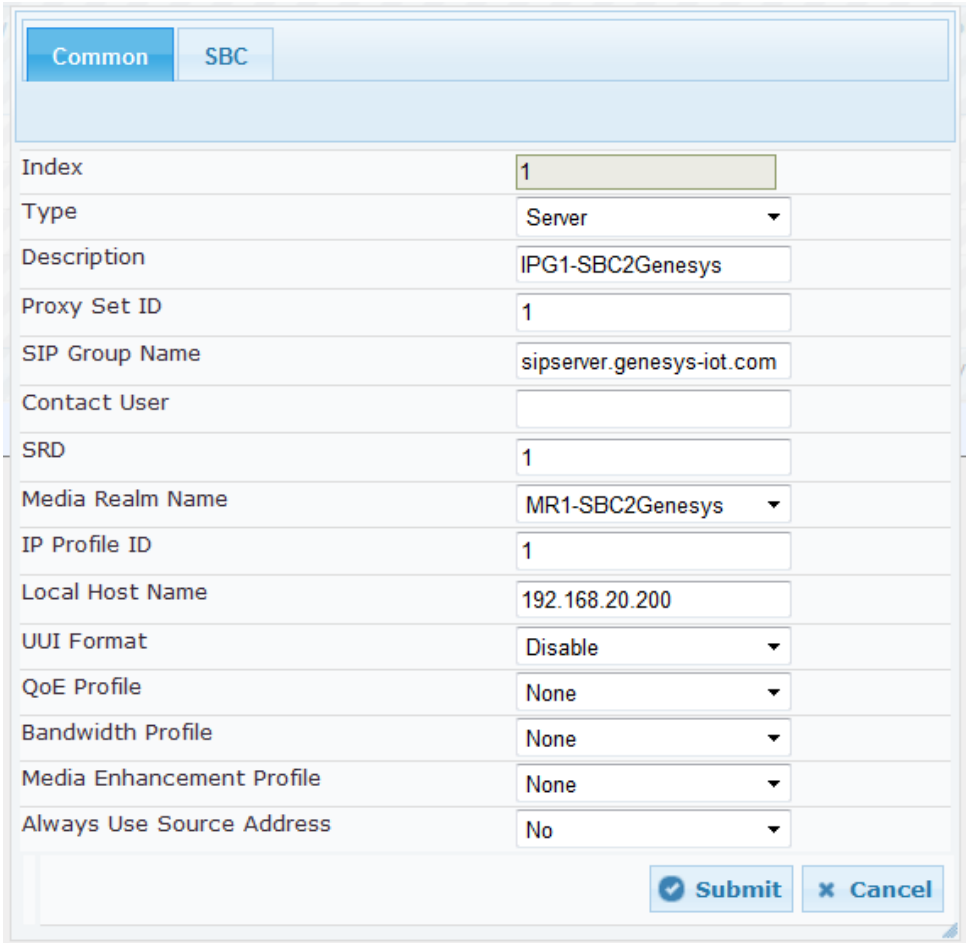
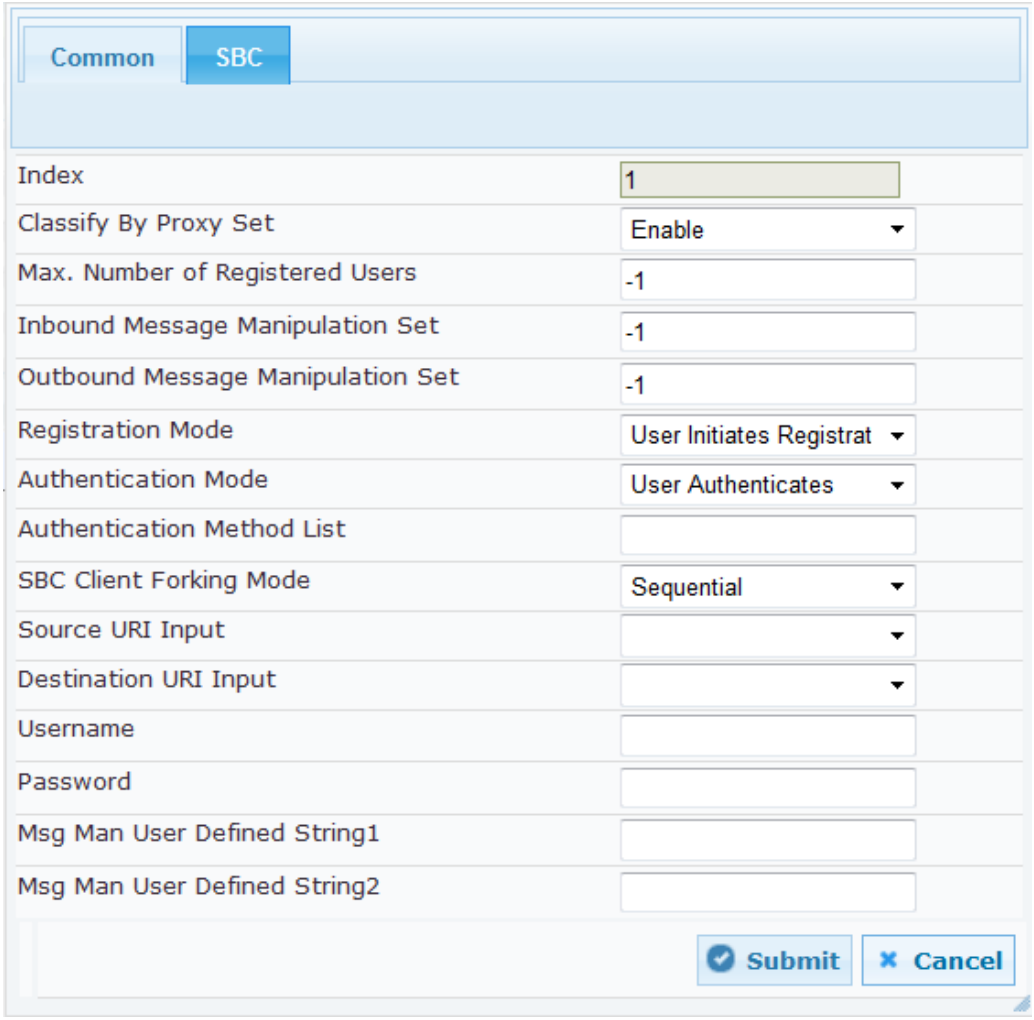


Figure 3-15: Configuring an IP Group for the Genesys Call Center (SBC Tab)



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

Parameter	Value
Index	**2**
Type	**Server**
Description	**IPG2-SBC2Colt** (arbitrary descriptive name)
Proxy Set ID	**2**
SIP Group Name	**217.110.230.98** (according to ITSP requirement)
SRD	**2**
Media Realm Name	**MR2-SBC2Colt**
IP Profile ID	**2**
Local Host Name	**208.0.113.120**

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

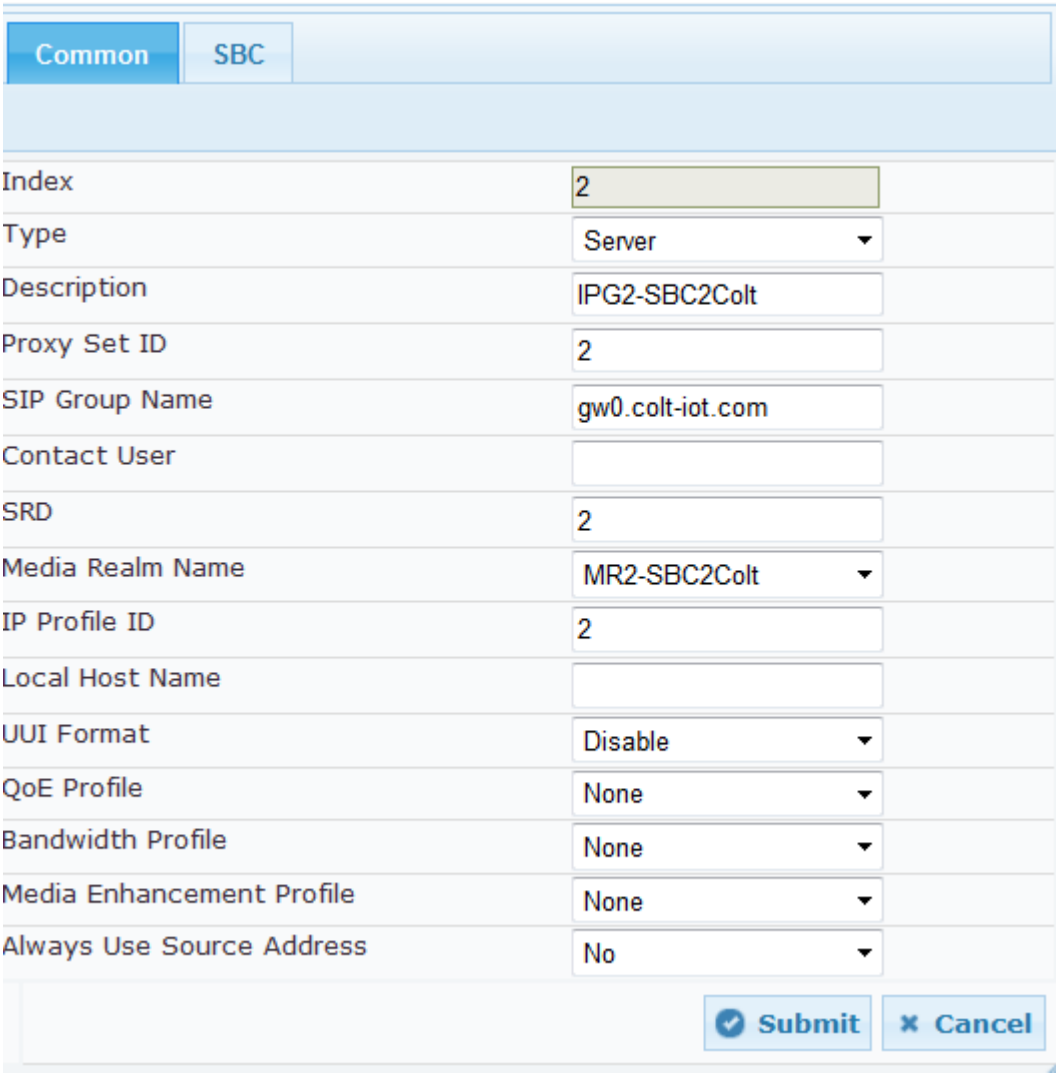
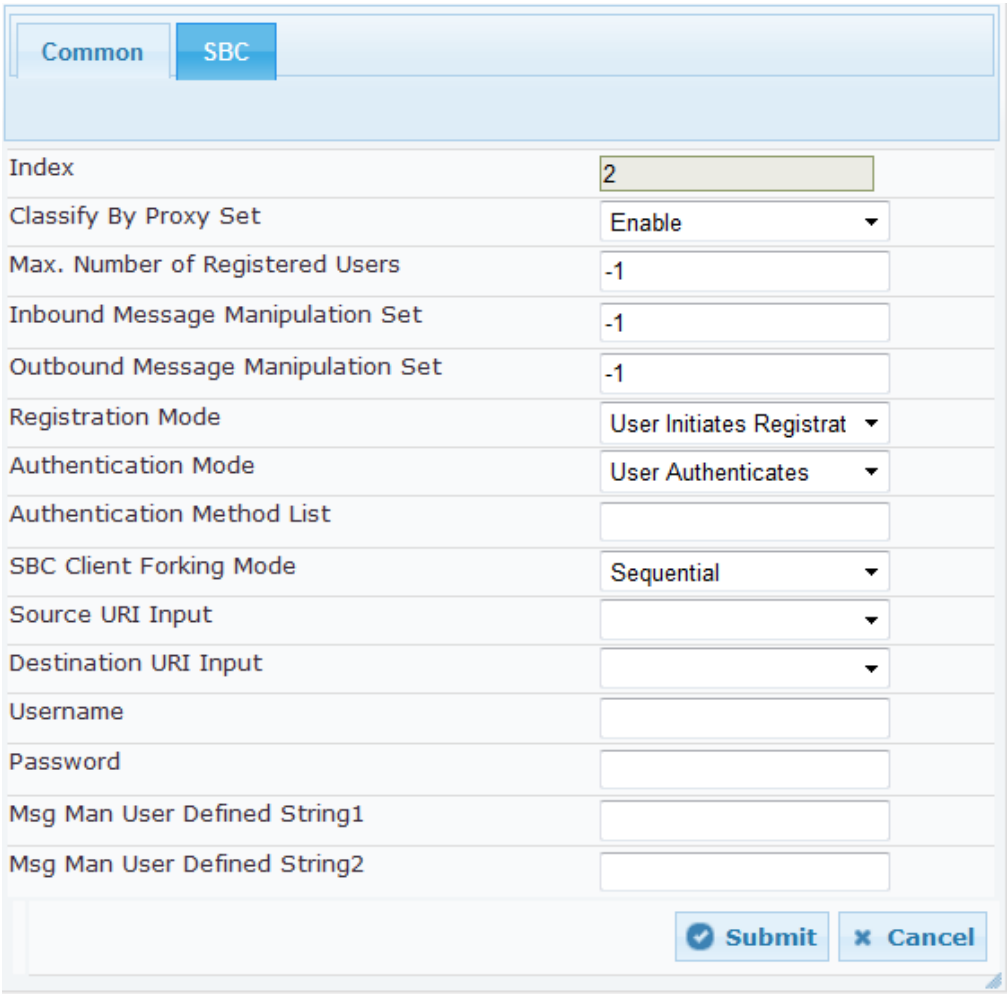
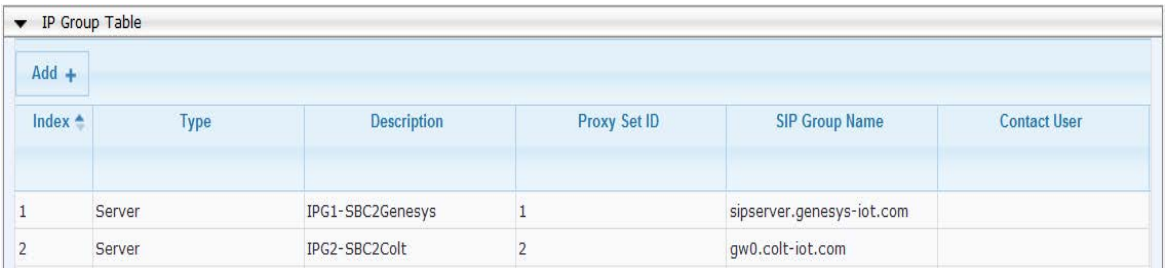


Figure 3-17: Configuring an IP Group for the Colt SIP Trunk (SBC Tab)



The configured IP Groups are shown in the figure below:

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



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
- Colt SIP trunk

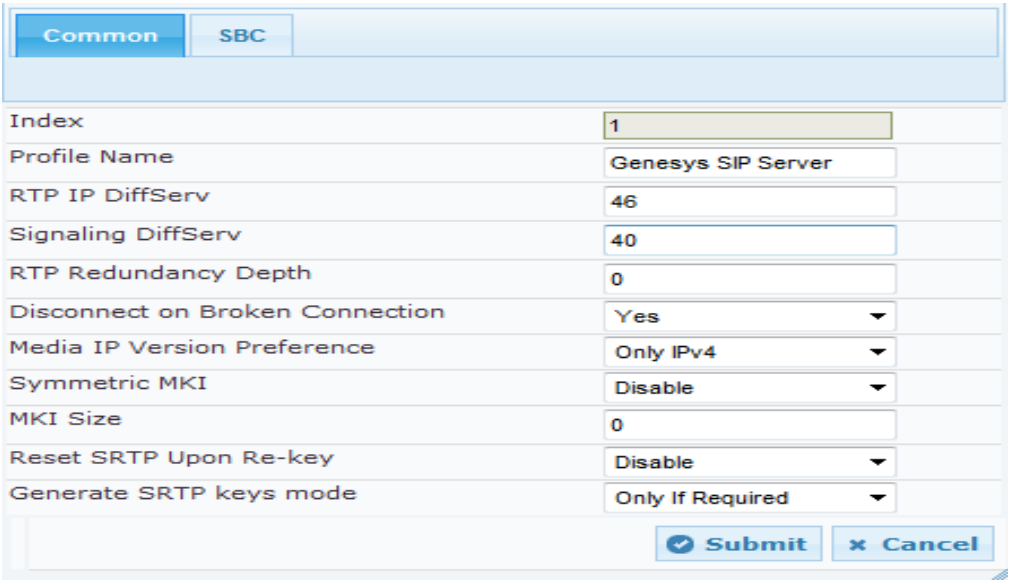
Note: The IP Profile index values were assigned to the IP Groups in the previous step (see Section 3.5 3.5on page 26).

➢ **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:

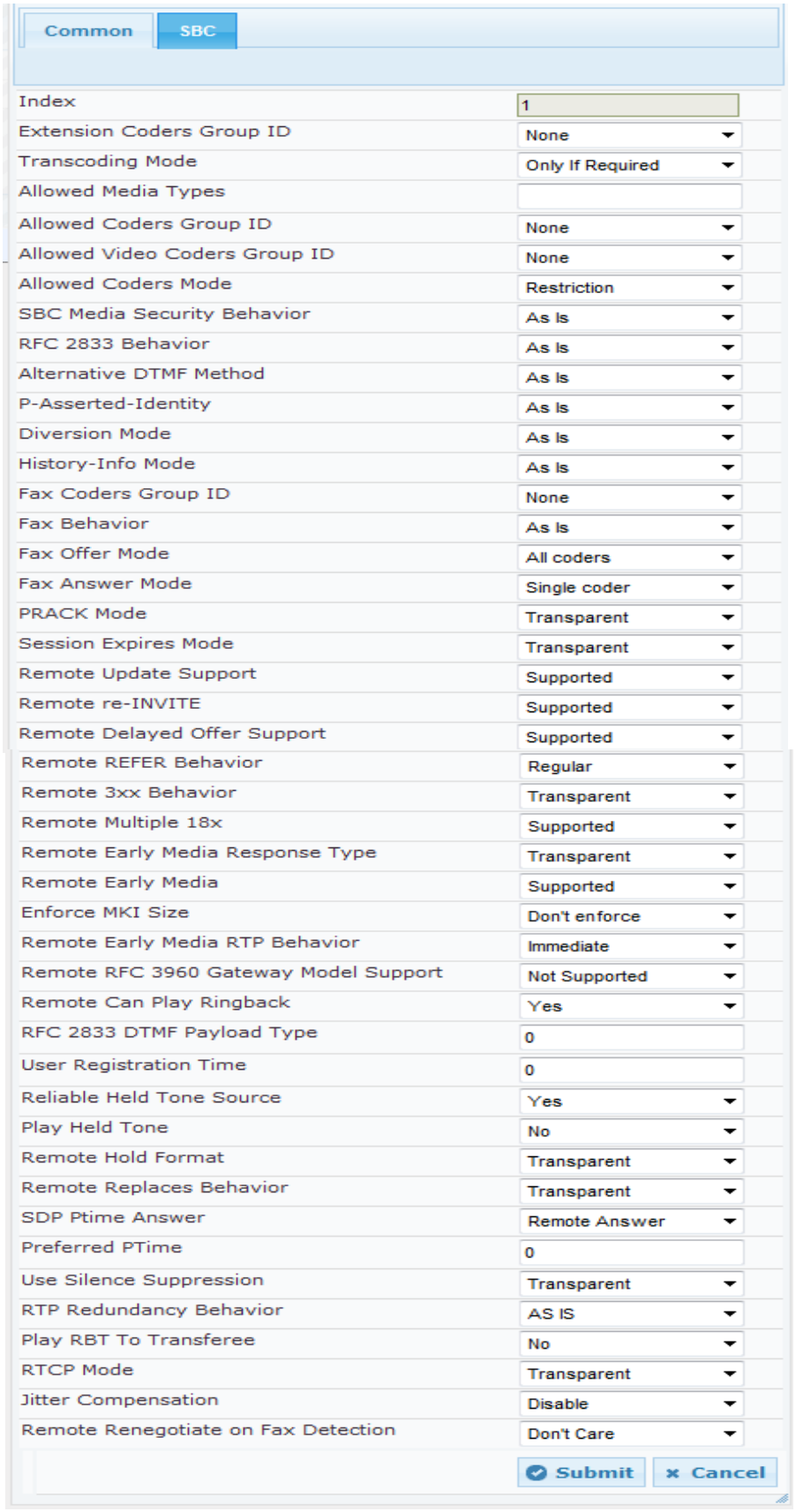
Parameter	Value
Index	**1**
Profile Name	**Genesys SIP Server** (arbitrary descriptive name)

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



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.

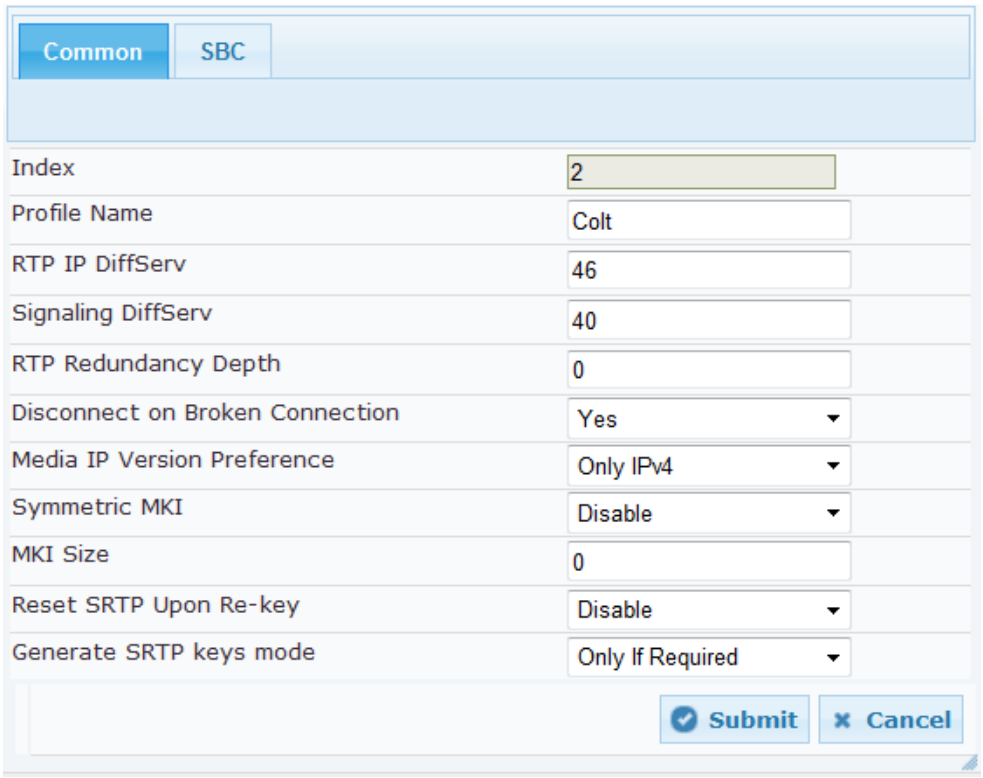
Figure 3-20: Configuring IP Profile for Genesys Contact Center (SBC Tab)



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

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

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



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

Parameter	Value
Media Security Behavior	**'As Is'**
Remote REFER Behavior	**IP Group Name** (To change the host name on the Refer-To header, to the ITSP host name)

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

Note: Colt does not support the re-routing of a call into the external (PSTN) network upon the receipt of a SIP 302 Moved Temporarily response. Consequently, the SBC transparently passes the 302 Moved Temporarily response from Genesys to Colt. This response is then ACK'd by the Colt ITSP; however, there is no subsequent routing of the call by Colt to the external DN. This issue is overcome by the SBC locally; the 302 Moved Temporarily response from the SIP Server is ACK'd by the SBC, and then the SBC sends a subsequent INVITE to the temporary external number via Colt. The call is then 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 Colt IP Group, and by setting an IP2IP route for calls originating from the Colt IP Group to trigger on 3xx/REFER and route to the Colt ITSP IP Group.

Note that when adding the trigger route, i.e. this scenario is a specific instance of the normal routing rule and should therefore should precede it in the IP-to-IP Routing table, i.e. route "Colt2Genesys" later defined (see Section 3.8 on page 37).

The configured IP Groups are shown in the figure below:

Figure 3-23: Configured IP Profiles in IP Profile Table

3.7 Step 7: Configure Coders

The Colt SIP Trunk supports G.729, G.711A-law, and G.726 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, no transcoding is needed; therefore no special SBC configuration is required.

However, if support is required in the deployment for G.711U-law or G.726 (not supported on either), an SBC transcoding configuration is required (refer to the *SBC User's Manual*) for Coder Transcoding configuration.

Note: The 'DSP channels' Feature Key and definition is required for activating Coder Transcoding.

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

This step shows how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. 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 25, IP Group 1 represents the Genesys Contact Center, and IP Group 2 represents the Colt 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 Colt SIP Trunk (WAN):

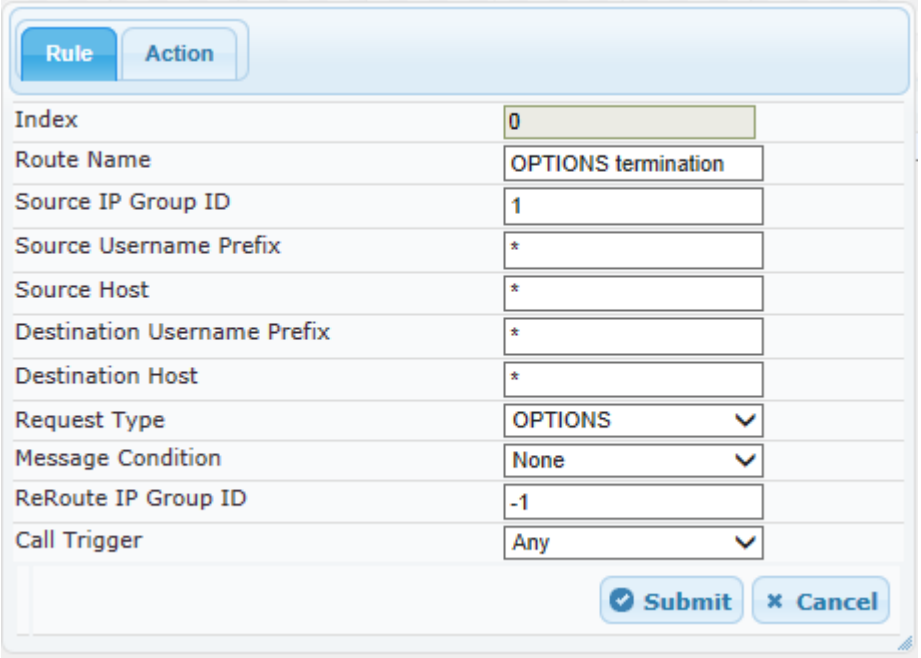
- Terminate SIP OPTIONS messages on the SBC that are received from the LAN
- Calls from Genesys Contact Center to Colt SIP Trunk
- Calls from Colt SIP Trunk to Gensys Contact Center

➢ **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**
Destination Type	**Dest Address**
Destination Address	**internal**

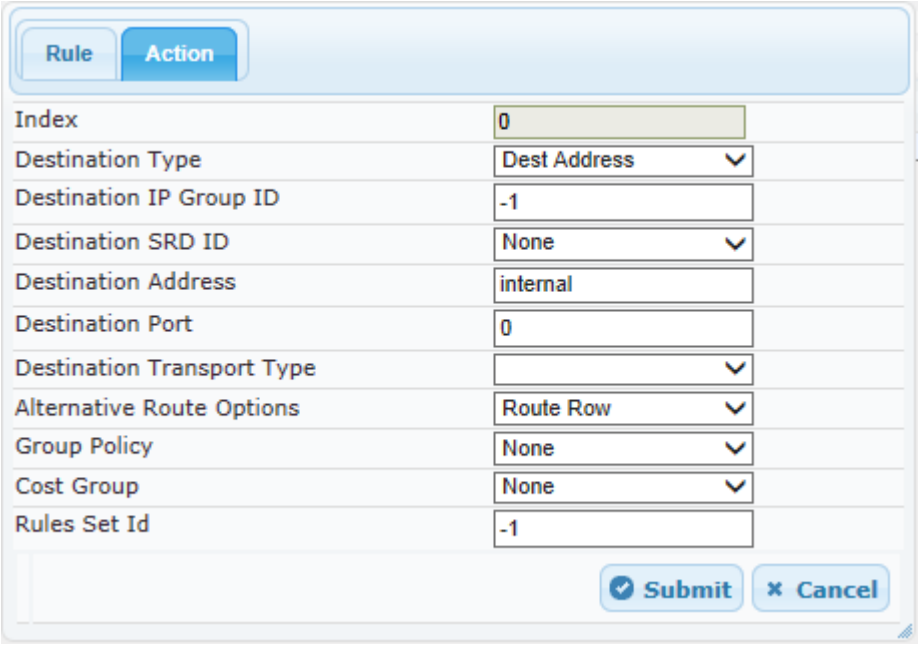
Figure 3-24: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Rule Tab



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

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

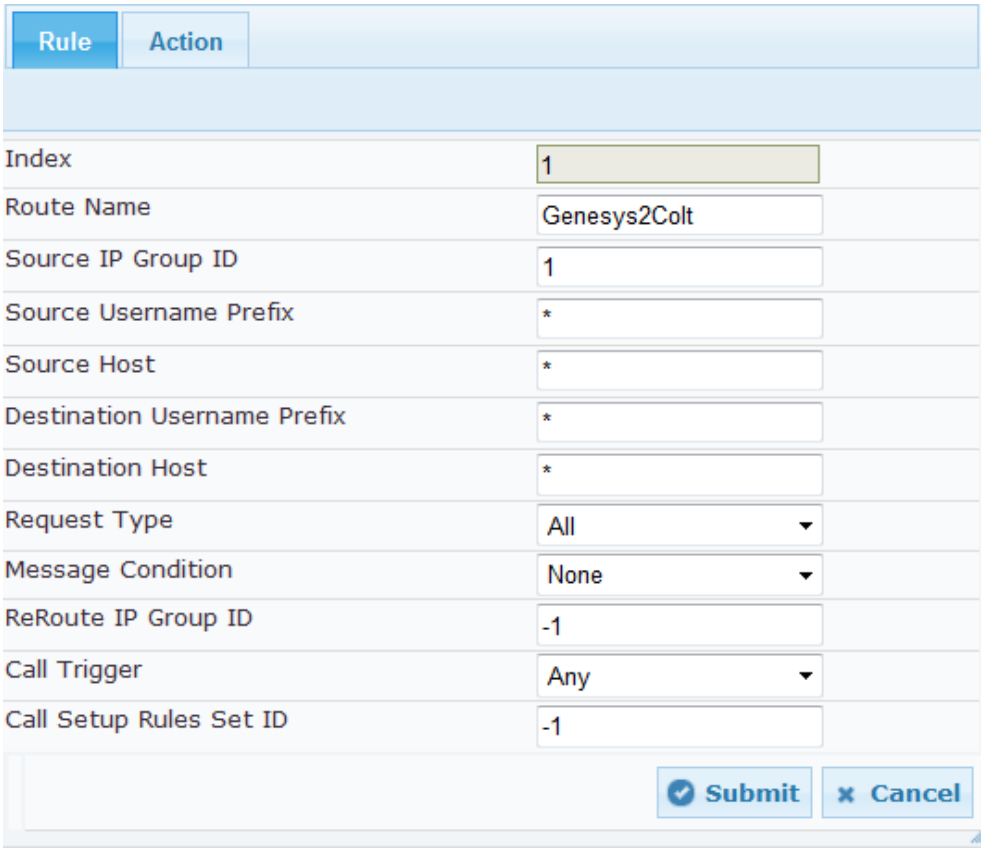
Figure 3-25: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS from LAN – Action Tab



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

Parameter	Value
Index	**1**
Route Name	**Genesys2Colt** (arbitrary descriptive name)
Source IP Group ID	**1**

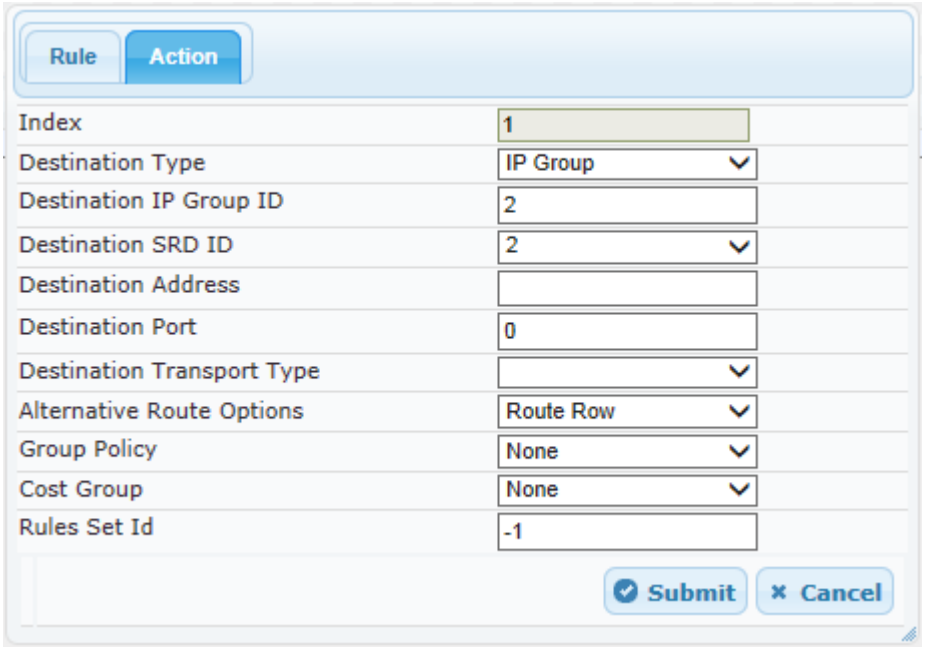
Figure 3-26: Configuring IP-to-IP Routing Rule for Genesys to Colt – Rule tab



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

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

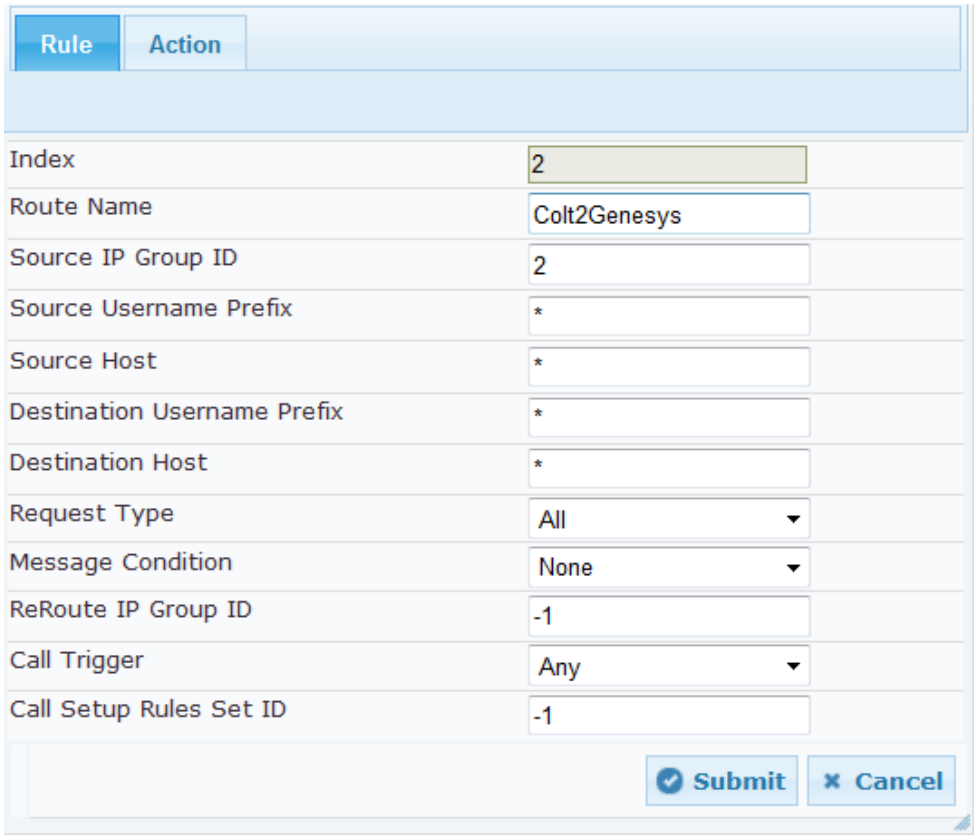
Figure 3-27: Configuring IP-to-IP Routing Rule for Genesys to Colt – Action tab



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

Parameter	Value
Index	**2**
Route Name	**Colt2Genesys** (arbitrary descriptive name)
Source IP Group ID	**2**

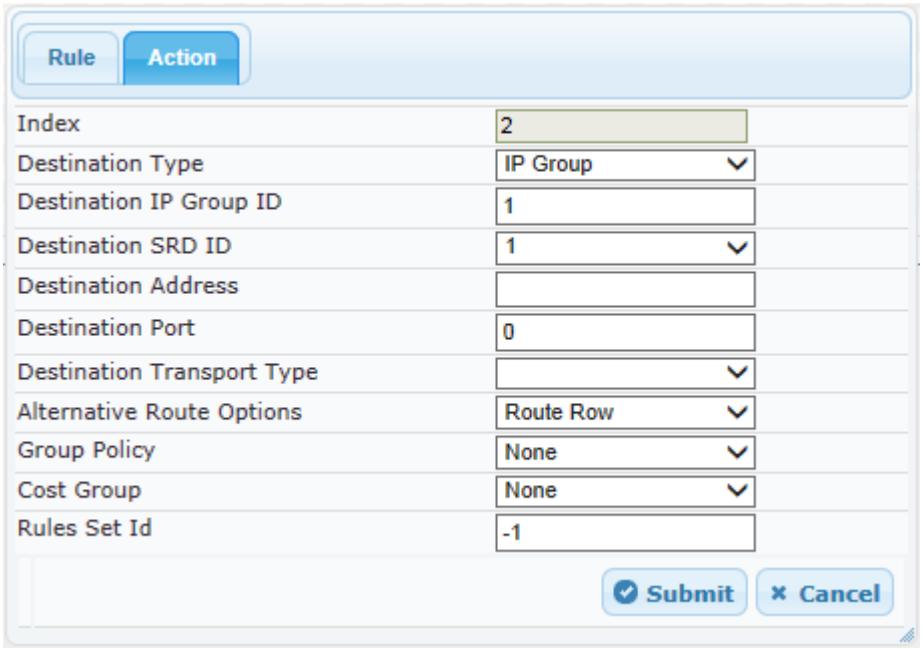
Figure 3-28: Configuring IP-to-IP Routing Rule for Colt to Genesys – Rule tab



7. 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 3-29: Configuring IP-to-IP Routing Rule for Colt to Genesys – Action tab



The configured routing rules are shown in the figure below:

Figure 3-30: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

IP-to-IP Routing Table

Add | Insert | Edit | Delete | Up | Down | Show/Hide

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 SRD ID
0	OPTIONS termination	*	*	*	None	-1	Any	-1	Dest Address	None
1	Genesys2Colt	*	*	*	None	-1	Any	-1	IP Group	2
2	Colt2Genesys	*	*	*	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 shows 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 25, IP Group 1 represents Genesys Contact Center, and IP Group 2 represents Colt SIP Trunk.

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

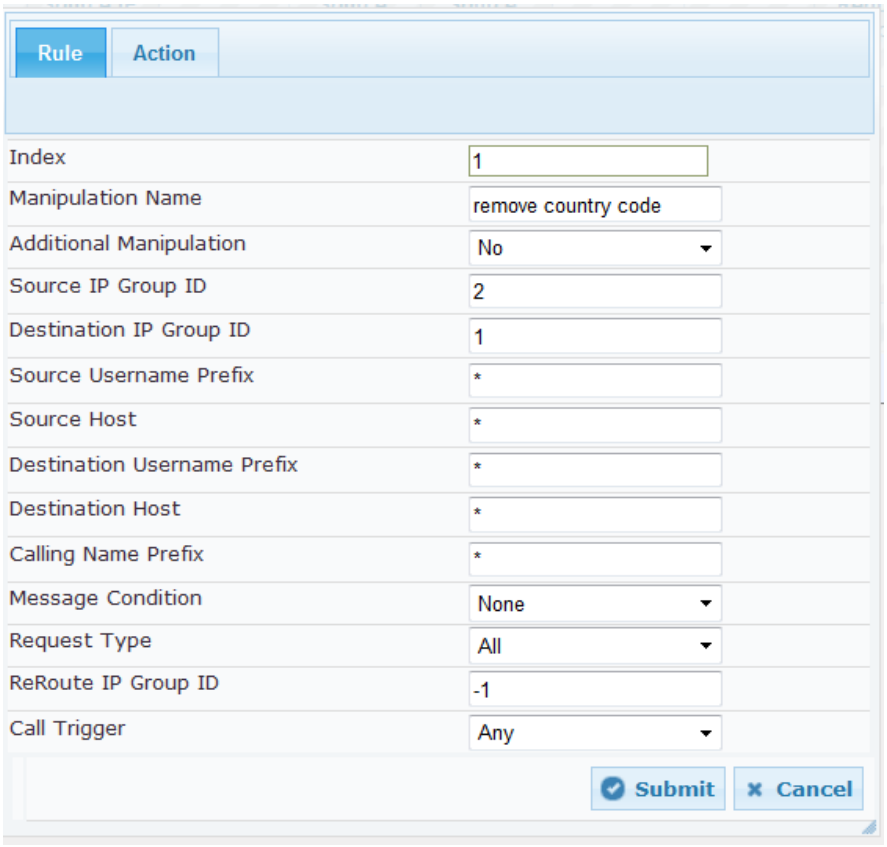
For this interoperability test topology, a manipulation is configured to remove the first 3 digits from the destination number for calls from IP Group 2 (Colt SIP Trunk) to IP Group 1 (i.e., Genesys Contact Center) for any destination username prefix.

➢ **To configure a number manipulation rule:**

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

Parameter	Value
Index	**1**
Source IP Group	**2**
Destination IP Group	**1**
Destination Username Prefix	***** (asterisk sign)

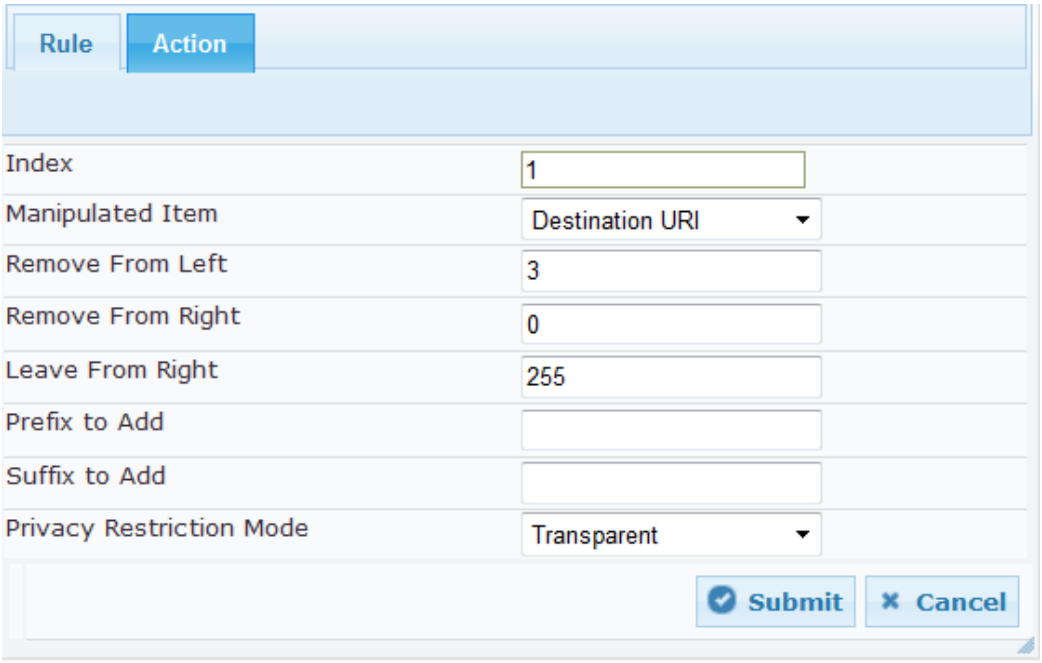
Figure 3-31: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab



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

Parameter	Value
Manipulated Item	**Destination URI**
Remove from Left	**3**

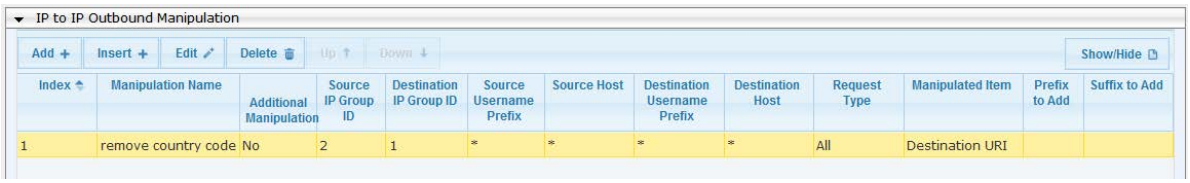
Figure 3-32: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab



5. Click **Submit**.

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

Figure 3-33: Example of Configured IP-to-IP Outbound Manipulation Rules



Rule Index	Description
1	Calls from IP Group 2 to IP Group 1 with any destination number (*), remove first 3 digits (country code) of the destination number.

3.10 Step 10: Remote Agents

This section 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 the Interoperability testing scenario, the Remote Agents are configured on a new Signaling Routing Domain over an existing untrusted interface.

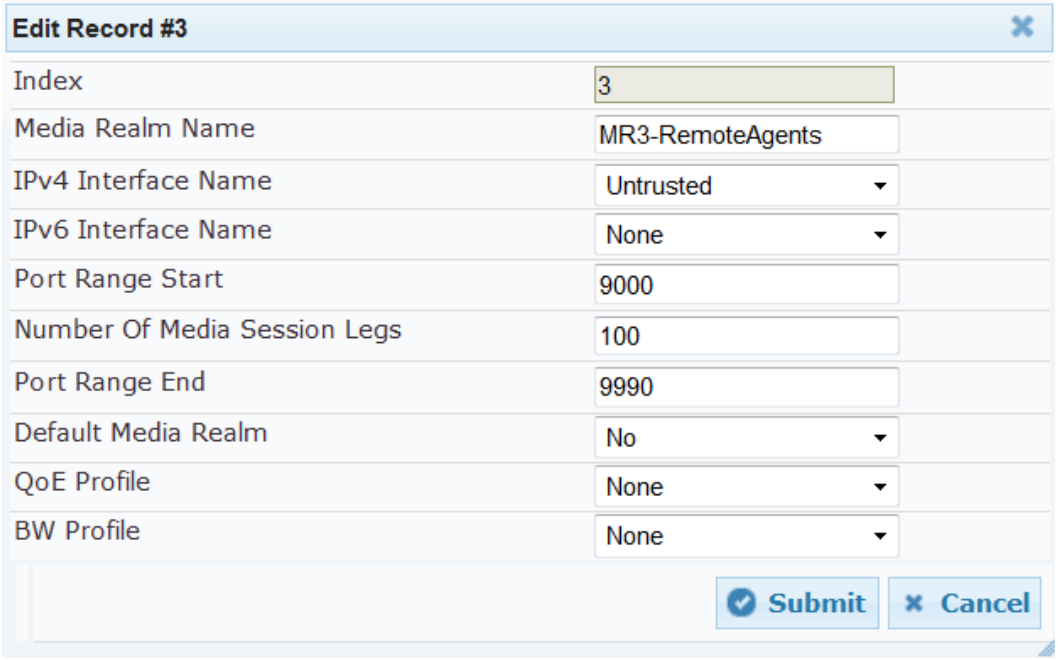
3.10.1 Step 10a: Configure Media Realm for Remote Agent

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:**

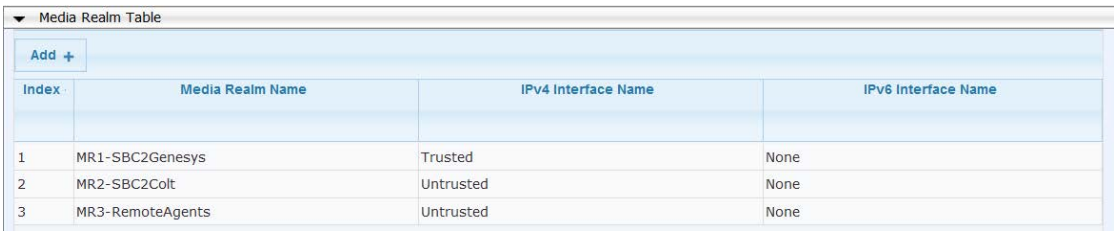
1. Open the **Advanced Parameters** page (**Configuration** tab > **VoIP** menu > **Media Realm Table**).

Figure 3-34: Configuring Remote Agent Media Realm



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

Figure 3-35: Configuring Remote Agent Media Realm



3.10.2 Step 10b: Configure SRD for Remote Agent

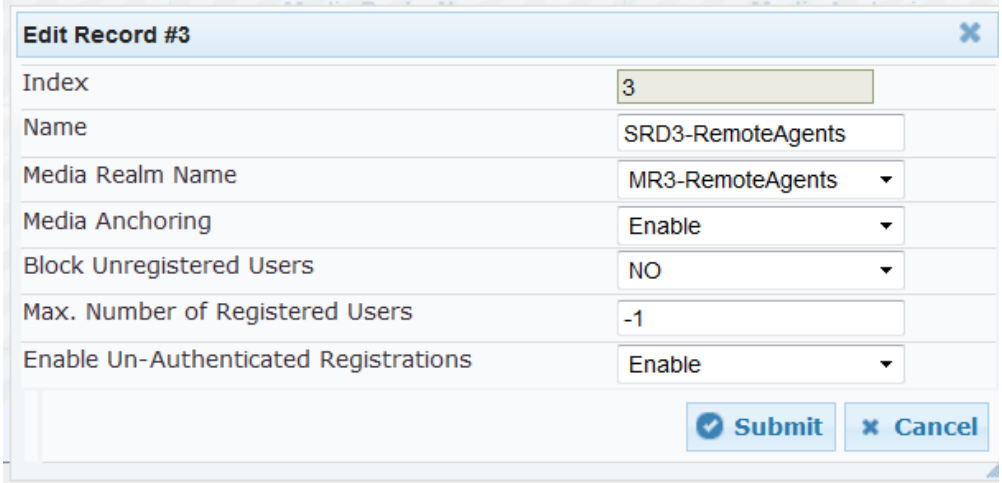
This step shows how to create a new SRD for the Remote Agents.

➢ **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):

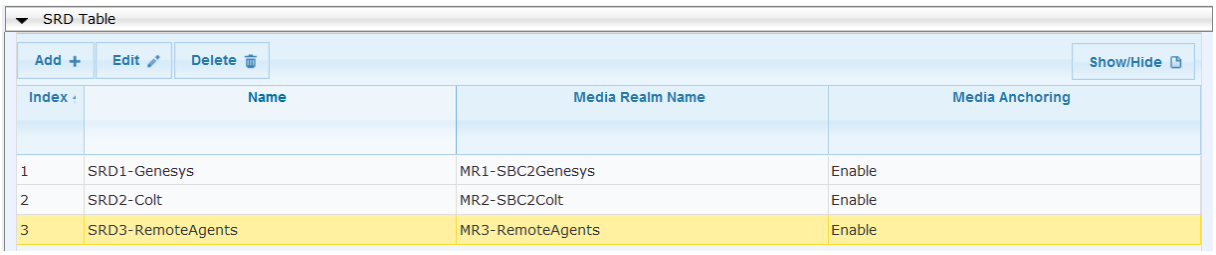
Parameter	Value
SRD Index	**3**
SRD Name	**SRD3-RemoteAgents** (descriptive name for SRD)
Media Realm	**MR3-RemoteAgents** (associates SRD with Media Realm)

Figure 3-36: Configuring SRD for Remote Agents



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

Figure 3-37: Configuring Remote Agent Media Realm



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

Create a new SIP Signaling interface on the Untrusted Network Interface for the Remote Agents.

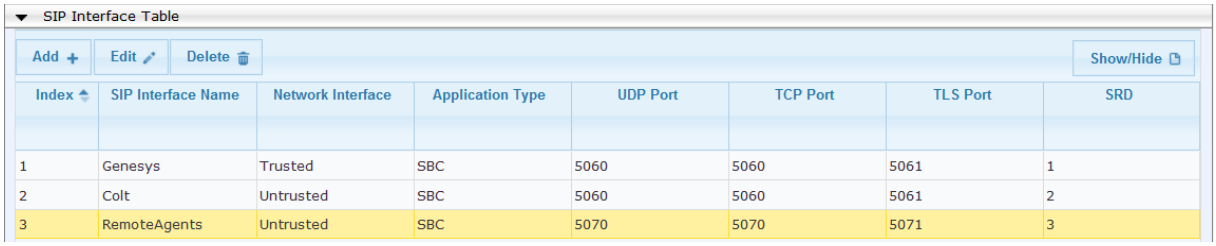
➢ **To configure SIP Interfaces for remote agent:**

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	**5070**
SRD	**3**

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

Figure 3-38: ConfiguredSIP Interfaces for Remote Agents in SIP Interface Table



3.10.4 Step 10d: 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 3-39: Configuring an IP Group for the Remote (User) Agents (Common Tab)

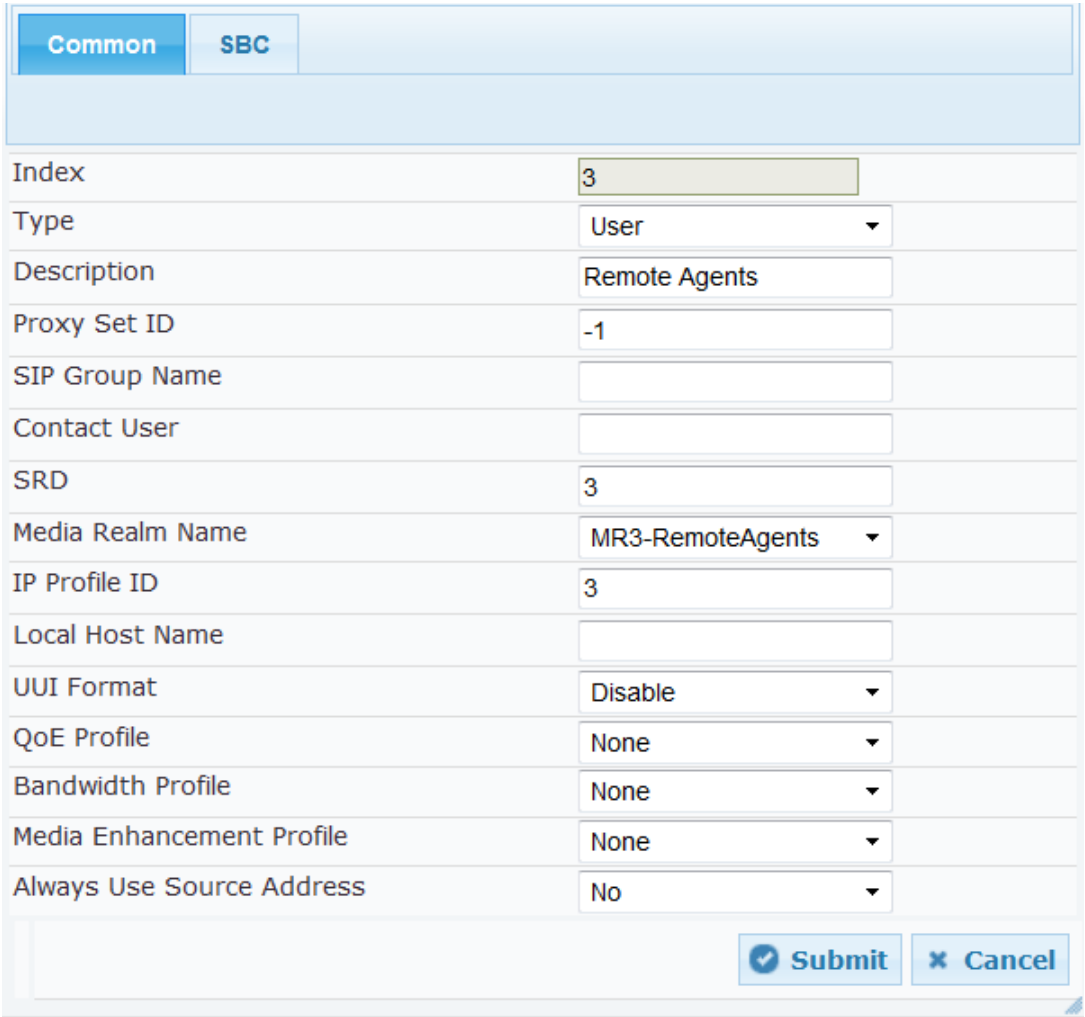
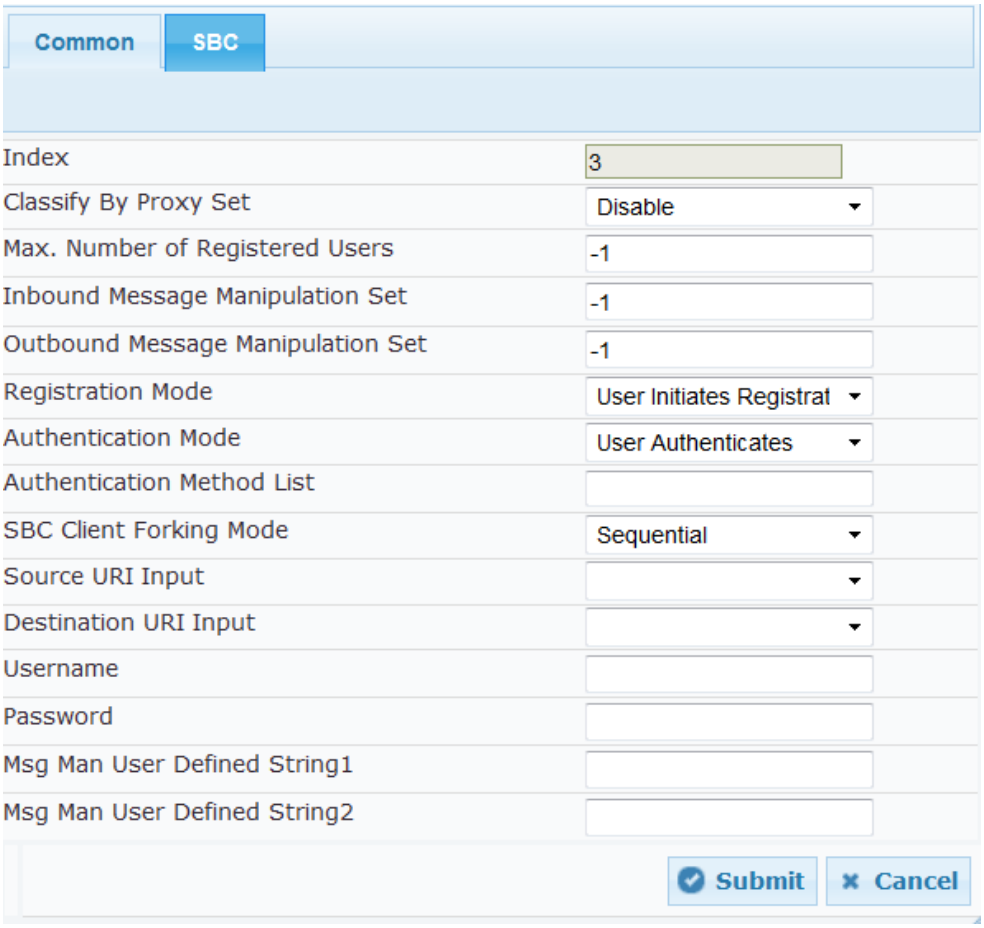
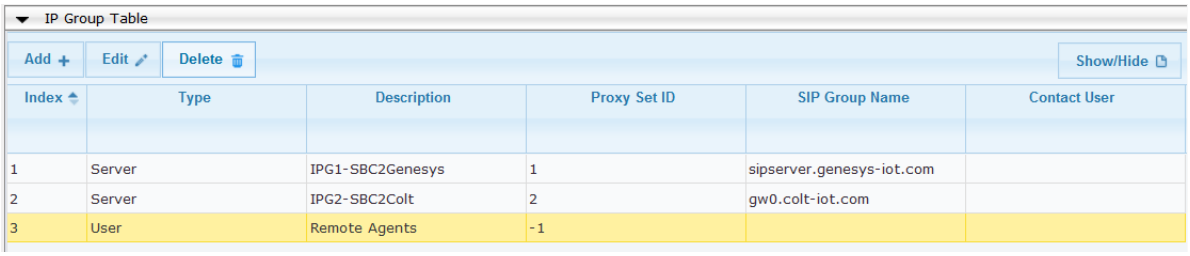


Figure 3-40: Configuring an IP Group for the Genesys Call Center (SBC Tab)



The configured IP Groups are shown in the figure below:

Figure 3-41: Configured IP Group for Remote Users in IP Group Table



3.10.5 Step 10e: Configure IP Profiles for Remote Agents

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

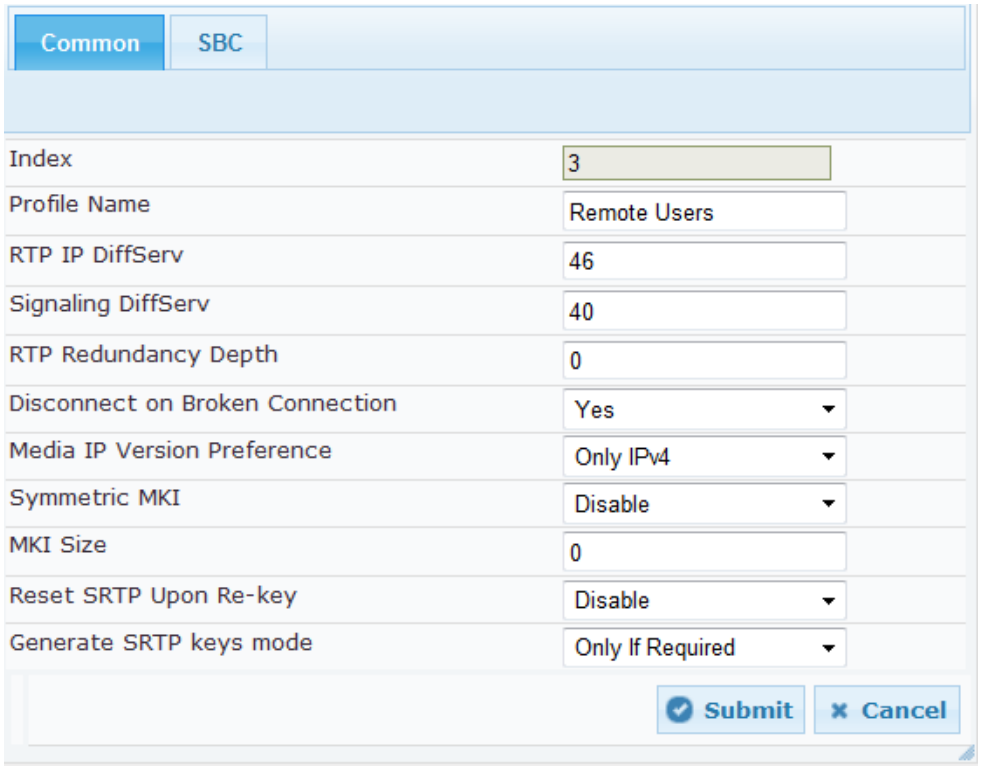
Note: The IP Profile index values were assigned to the IP Groups in the previous step (see Section 3.5 on page 26).

➢ **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 3-42: Configuring IP Profile for Remote Users (Common Tab)



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 3-43: Configuring IP Profile for Remote (User) Agents (SBC Tab)

Figure 3-44: Configured IP Profiles in IP Profile Table

3.10.6 Step 10f: Configure Classification Table for Remote Agents

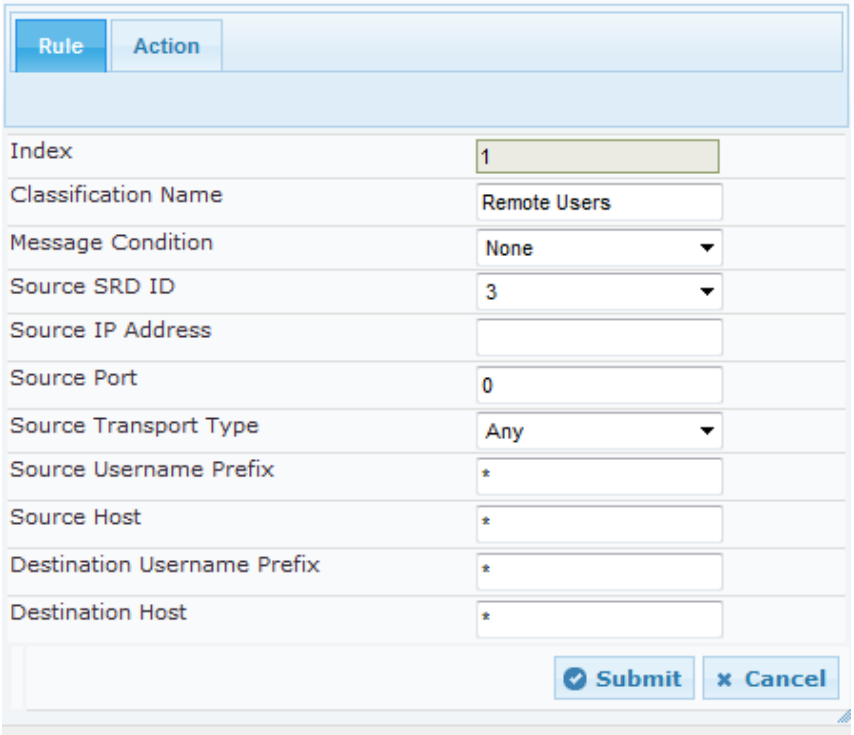
The Classification rules classify incoming SIP dialog-initiating requests to an IP Group from where the SIP dialog request was received. The identified IP Group is then used in the manipulation and routing processes. For Remote Users arriving on an interface with multiple IP Groups, the classification 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**
Profile Name	**Remote Users** (arbitrary descriptive name)
Source SRD ID	**3**

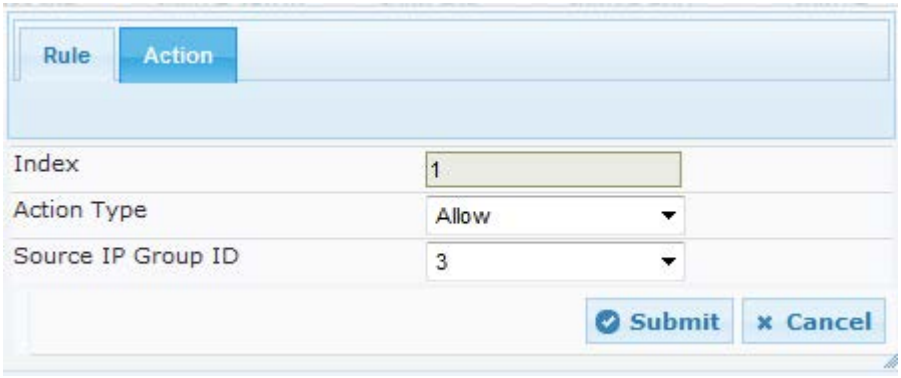
Figure 3-45: Configuring Rule Tab of the Classification Table



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

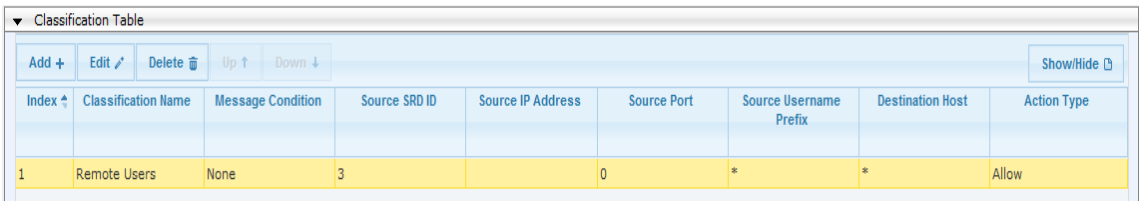
Parameter	Value
Source SRD ID	**3**

Figure 3-46: Configured IP Profiles in IP Profile Table



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

Figure 3-47: Configured Classification Rule for Remote (Users) Agents



3.10.7 Step 10g: Configure IP-to-IP Call Routing Rules for Remote (User) Agent

The following IP-to-IP call routing rules were configured (see Section 3.8 on page 37):

- Terminate SIP OPTIONS messages on the SBC that are received from the LAN
- Calls from Genesys Contact Center to Colt SIP Trunk
- Calls from Colt SIP Trunk to Gensys Contact Center

This step shows 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 3.10.6) and the Genesys SIP Server.

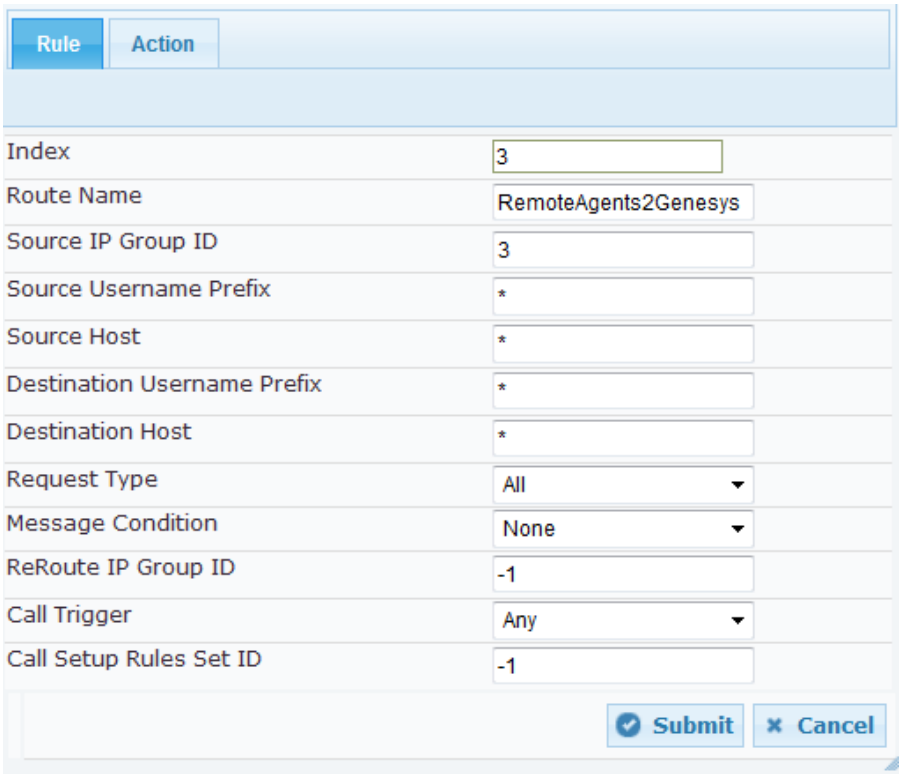
For the interoperability test topology, IP-to-IP routing rules were configured to route SIP messages between the Remote (User) Agents and the Genesys SIP Server, and to ensure that the messages are routed back to the correct user group to reach the intended agent.

➢ **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 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	**3**
Route Name	**RemoteAgents2Genesys** (arbitrary descriptive name)
Source IP Group ID	**3**

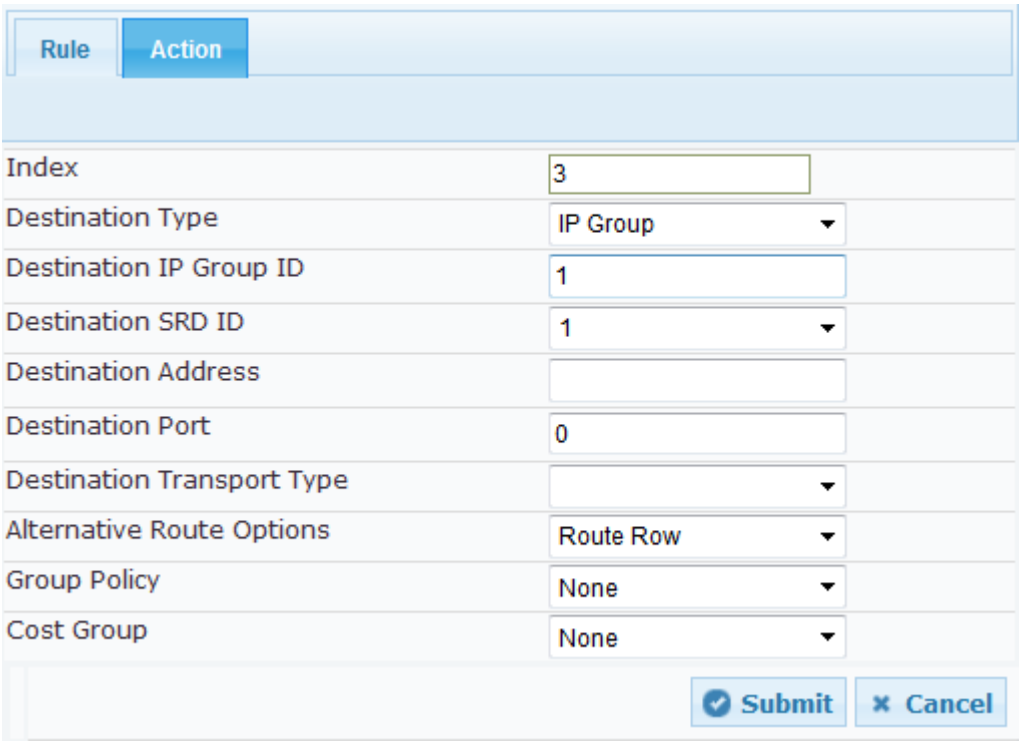
Figure 3-48: Configuring IP-to-IP Routing Rule for Terminating RemoteAgents2Genesys – Rule Tab



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

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

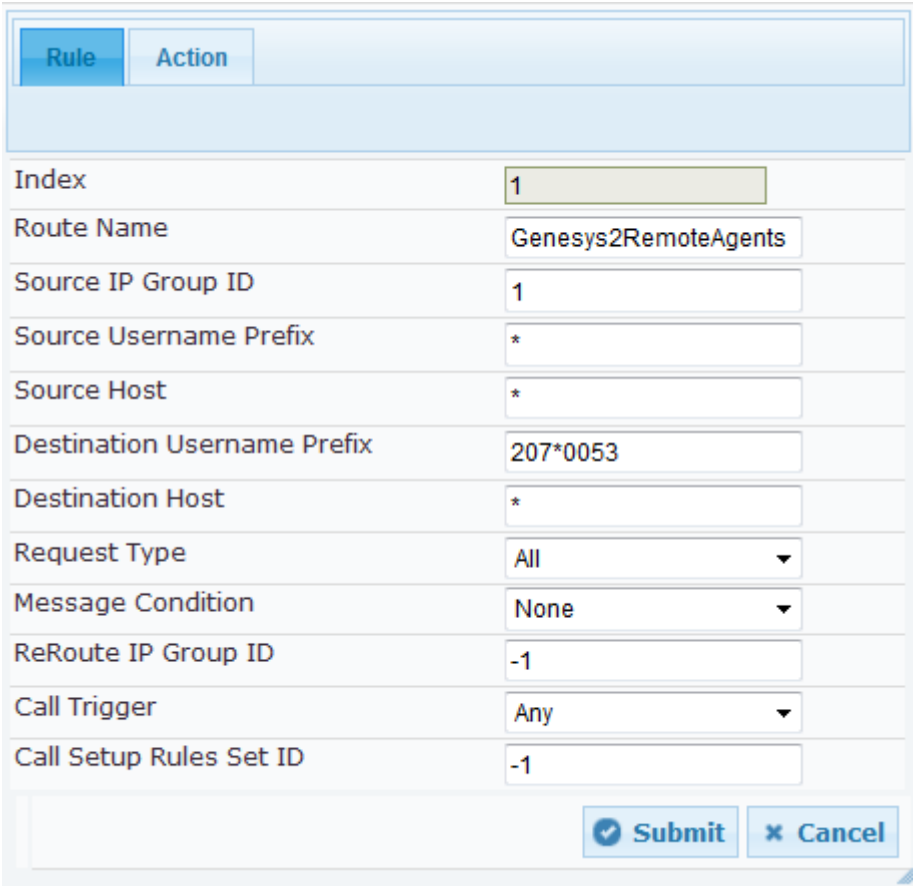
Figure 3-49: Configuring IP-to-IP Routing Rule for Terminating RemoteAgents2Genesys – Action Tab



4. Configure a rule to route calls from the Genesys Contact Center to the Remote User Agent Group. Note 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 Colt 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 Colt ITSP. For calls in the Remote Agent group, the SBC will determine the next destination from the AOR.
   a. Select Index 1 (Genesys2Colt route), and then click **Insert +**.
   b. Click the **Rule** tab, configure the parameters as follows, and then click **Submit**.

Parameter	Value
Index	**1**
Route Name	**Genesys2RemoteAgents** (arbitrary descriptive name)
Source IP Group ID	**1**
Destination Username Prefix	**207*0053** (block of number allocated to remote agents)

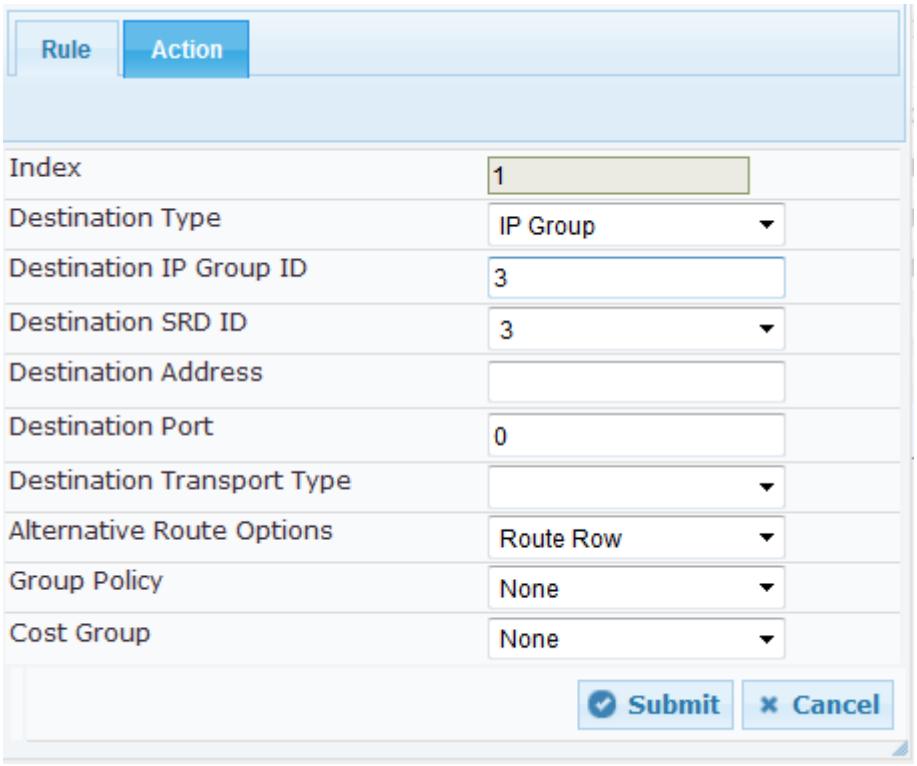
Figure 3-50: Configuring IP-to-IP Routing Rule for Genesys to Remote Agent Group – Rule tab



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

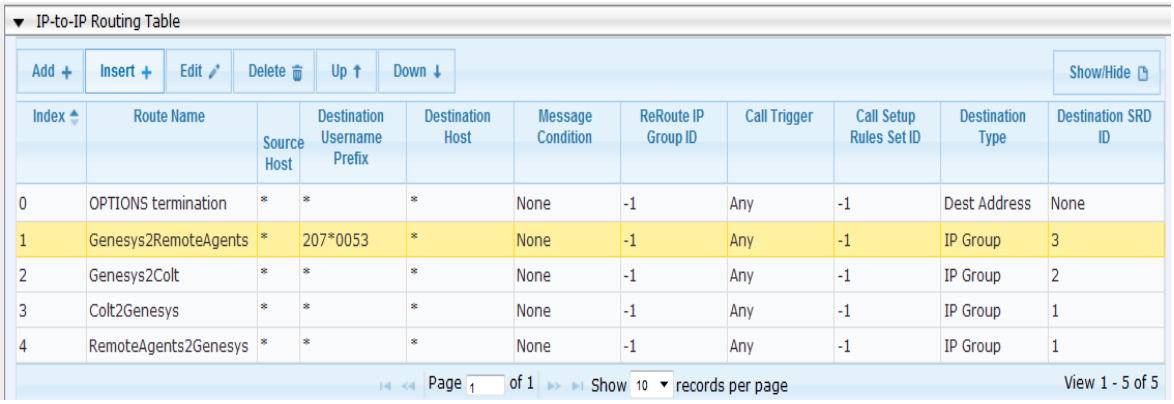
Parameter	Value
Destination Type	**IP Group**
Destination IP Group ID	**3**
Destination SRD ID	**3**

Figure 3-51: Configuring IP-to-IP Routing Rule for Genesys to Colt – Action tab



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

Figure 3-52: 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 SRD ID
0	OPTIONS termination	*	*	*	None	-1	Any	-1	Dest Address	None
1	Genesys2RemoteAgents	*	207*0053	*	None	-1	Any	-1	IP Group	3
2	Genesys2Colt	*	*	*	None	-1	Any	-1	IP Group	2
3	Colt2Genesys	*	*	*	None	-1	Any	-1	IP Group	1
4	RemoteAgents2Genesys	*	*	*	None	-1	Any	-1	IP Group	1

Page 1 of 1 Show 10 records per page View 1 - 5 of 5

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.

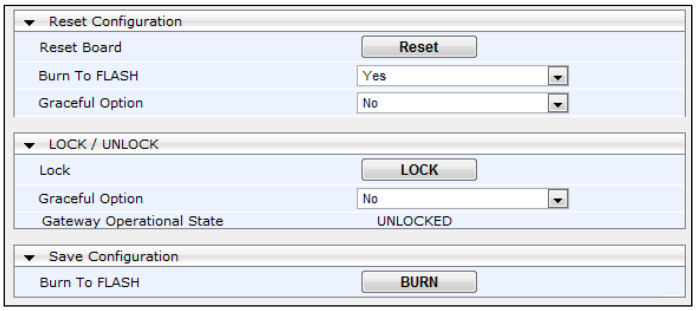
3.11 Step 11: Reset the SBC

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 3-53: Resetting the SBC



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

A AudioCodes *ini* File

This appendix shows the *ini* configuration file of the SBC, corresponding to the Web-based configuration described in Section 3 on page 13.

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

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

;Board: Mediant SW
;Board Type: 73
;Serial Number: 115991455101440
;Product Key:
;Slot Number: 1
;Software Version: 6.80A.216.008
;DSP Software Version: SOFTDSP => 660.01
;Board IP Address: 192.168.20.200
;Board Subnet Mask: 255.255.255.0
;Board Default Gateway: 192.168.20.1
;Ram size: 7832M   Flash size: 0M
;Num of DSP Cores: 0  Num DSP Channels: 0
;Profile: NONE
;Key features:;Board Type: Mediant SW ;Max SW Ver: 9.80;QOE features:
VoiceQualityMonitoring MediaEnhancement ;Coders: G723 G729 G728 NETCODER
GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-WB G722 EG711 ;DSP
Voice features: RTCP-XR ;Security: IPSEC MediaEncryption
EncryptControlProtocol ;Channel Type: DspCh=2000 IPMediaDspCh=2000 ;HA
;Control Protocols: FEU=500 MGCP MEGACO H323 SIP SASurvivability SBC=1000
;Default features:;Coders: G711 G726;


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


[SYSTEM Params]

;VpFileLastUpdateTime is hidden but has non-default value
NTPServerIP = '0.0.0.0'
;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
```

```
[BSP Params]

PCMLawSelect = 3
EnableLANWatchdog = 0
AuthorizedTPNCPServers_0 = 0.0.0.0
AuthorizedTPNCPServers_1 = 0.0.0.0
AuthorizedTPNCPServers_2 = 0.0.0.0
AuthorizedTPNCPServers_3 = 78.75.78.85
RoutingTableHopsCountColumn = 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[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]

BrokenConnectionEventTimeout = 100
FarEndDisconnectSilenceMethod = 1
FarEndDisconnectSilencePeriod = 120

[WEB Params]

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

[SIP Params]

;ISPRACKREQUIRED is hidden but has non-default value
PROGRESSINDICATOR2IP = -1
```

```
CDRSYSLOGSERVERIP = 0.0.0.0
PSTNALERTTIMEOUT = 180
EmergencyNumbers = '', '', '', ''
SBCREGISTRATIONTIME = 0
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
SESSIONEXPIRESDISCONNECTTIME = 32
ENERGYDETECTORCMD = 104
ANSWERDETECTORCMD = 12582952

[IPsec Params]


[SNMP Params]


[ 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, "Trusted", "GROUP_1", "Active";
PhysicalPortsTable 1 = "GE_2", 1, 2, 4, "Untrusted", "GROUP_2", "Active";
PhysicalPortsTable 2 = "GE_3", 1, 3, 4, "User Port #2", "GROUP_3",
"Active";
PhysicalPortsTable 3 = "GE_4", 1, 4, 4, "User Port #3", "GROUP_4",
"Active";

[ \PhysicalPortsTable ]


[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 1, "GE_1", "";
EtherGroupTable 1 = "GROUP_2", 1, "GE_2", "";
EtherGroupTable 2 = "GROUP_3", 1, "GE_3", "";
EtherGroupTable 3 = "GROUP_4", 1, "GE_4", "";

[ \EtherGroupTable ]


[ DeviceTable ]

FORMAT DeviceTable_Index = DeviceTable_VlanID,
DeviceTable_UnderlyingInterface, DeviceTable_DeviceName;
DeviceTable 0 = 1, "GROUP_1", "GROUP_1";
DeviceTable 1 = 2, "GROUP_2", "GROUP_2";
DeviceTable 2 = 3, "GROUP_3", "GROUP_3";
DeviceTable 3 = 4, "GROUP_4", "GROUP_4";
```

```
[ \DeviceTable ]


[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 192.168.20.200, 24, 192.168.20.1, 1, "Trusted",
0.0.0.0, 0.0.0.0, "GROUP_1";
InterfaceTable 1 = 5, 10, 203.0.113.120, 26, 203.0.113.65, 2,
"Untrusted", 8.8.4.4, 8.8.8.8, "GROUP_2";

[ \InterfaceTable ]


[ DspTemplates ]

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

[ \DspTemplates ]


[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile;
CpMediaRealm 1 = "MR1-SBC2Genesys", "Trusted", "", 6000, 100, 6990, 1,
"", "";
CpMediaRealm 2 = "MR2-SBC2Colt", "Untrusted", "", 8000, 100, 8990, 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-Colt", "MR2-SBC2Colt", 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 = "sipserver.genesys-iot.com:5060", -1, 1;
ProxyIp 1 = "gw0.colt-iot.com:5060", -1, 2;

[ \ProxyIp ]


[ IpProfile ]

; ** NOTE: Changes were made to active configuration.
; **       The data below is different from current values.
FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupID, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,
IpProfile_CNGmode, IpProfile_VxxTransportType, IpProfile_NSEMode,
IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP,
IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP,
IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber,
IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit,
IpProfile_DisconnectOnBrokenConnection, IpProfile_FirstTxDtmfOption,
IpProfile_SecondTxDtmfOption, IpProfile_RxDTMFOption,
IpProfile_EnableHold, IpProfile_InputGain, IpProfile_VoiceVolume,
IpProfile_AddIEInSetup, IpProfile_SBCExtensionCodersGroupID,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedCodersGroupID,
IpProfile_SBCAllowedVideoCodersGroupID, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,
IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel,
IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime,
IpProfile_SBCDiversionMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,
IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode,
IpProfile_SBCFaxAnswerMode, IpProfile_SbcPrackMode,
IpProfile_SBCSessionExpiresMode, IpProfile_SBCRemoteUpdateSupport,
IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType,
IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI,
IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey,
IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource,
IpProfile_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone,
IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior,
IpProfile_SBCSDPPtimeAnswer, IpProfile_SBCPreferredPTime,
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,
```

```
IpProfile_SBCPlayRBTToTransferee, IpProfile_SBCRTCPMode,
IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection,
IpProfile_JitterBufMaxDelay;
IpProfile 1 = "Genesys SIP Server", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0,
2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", -
1, -1, 0, 0, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2,
1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 300;
IpProfile 2 = "Colt", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0,
-1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", -1, -1, 0, 0, 0,
0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 2, 0, 1, 0, 1,
0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 300;
IpProfile 3 = "Remote Users", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0,
0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", -1, -1,
0, 0, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 0, 0,
1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 300;

[ \IpProfile ]


[ 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 ]


[ 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, "0", -1, -1, "";
ProxySet 1 = "Genesys SIP Server", 1, 60, 0, 0, 1, 0, "", -1, -1, "";
ProxySet 2 = "Colt", 1, 60, 0, 0, 2, 0, "", -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_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_MediaEnhancementProfile,
IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2;
IPGroup 1 = 0, "IPG1-SBC2Genesys", 1, "sipserver.genesys-iot.com", "", 0,
-1, -1, 0, -1, 1, "MR1-SBC2Genesys", 1, 1, -1, -1, -1, 0, 0, "", 0, -1, -
1, "192.168.20.200", "", "$1$gQ==", 0, "", "", "", 0, "", "";
IPGroup 2 = 0, "IPG2-SBC2Colt", 2, "gw0.colt-iot.com", "", 0, -1, -1, 0,
-1, 2, "MR2-SBC2Colt", 1, 2, -1, -1, -1, 0, 0, "", 0, -1, -1, "", "",
"$1$gQ==", 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, "", "";

[ \IPGroup ]


[ 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 0 = "OPTIONS termination", 1, "*", "*", "*", "*", 0, "", -1,
0, -1, 1, -1, "", "internal", 0, -1, 0, 0, "";
IP2IPRouting 1 = "Genesys2RemoteAgents", 1, "*", "*", "207*0053", "*", 0,
"", -1, 0, -1, 0, 3, "3", "", 0, -1, 0, 0, "";
IP2IPRouting 2 = "Genesys2Colt", 1, "*", "*", "*", "*", 0, "", -1, 0, -1,
0, 2, "2", "", 0, -1, 0, 0, "";
IP2IPRouting 3 = "Colt2Genesys", 2, "*", "*", "*", "*", 0, "", -1, 0, -1,
0, 1, "1", "", 0, -1, 0, 0, "";
IP2IPRouting 4 = "RemoteAgents2Genesys", 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 1 = "Remote Users", "", "3", "", 0, -1, "*", "*", "*",
"*", 1, "3";

[ \Classification ]


[ 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 1 = "Genesys", "Trusted", 2, 5060, 5060, 5061, 1, "", "", -
1, 0, 500;
SIPInterface 2 = "Colt", "Untrusted", 2, 5060, 5060, 5061, 2, "", "", -1,
0, 500;
SIPInterface 3 = "RemoteAgents", "Untrusted", 2, 5070, 5070, 5071, 3, "",
"", -1, 0, 500;

[ \SIPInterface ]


[ 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 1 = "remove country code", 0, 2, 1, "*", "*", "*",
"*", "*", "", 0, -1, 0, 1, 3, 0, 255, "", "", 0;

[ \IPOutboundManipulation ]


[ CodersGroup0 ]

FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;
```

```
CodersGroup0 0 = "g711Alaw64k", 20, 255, -1, 0;

[ \CodersGroup0 ]


[ RoutingRuleGroups ]

FORMAT RoutingRuleGroups_Index = RoutingRuleGroups_LCREnable,
RoutingRuleGroups_LCRAverageCallLength, RoutingRuleGroups_LCRDefaultCost;
RoutingRuleGroups 0 = 0, 0, 1;

[ \RoutingRuleGroups ]


[ 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 ]
```

AudioCodes

Configuration Note

www.audiocodes.com