Configuration Note

AudioCodes Professional Services - Interoperability Lab

SWYX IP-PBX and DTAG SIP-Trunk using AudioCodes Mediant™ E-SBC

Version 7.2

Deutsche Telekom

SWYX

HD VoIP Sounds Better

AudioCodes

Table of Contents

This page is intentionally left blank.

Notice

This document describes how to connect the SWYX IP-PBX and DTAG SIP-Trunk using AudioCodes Mediant E-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: February-09-2017

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.

Document Revision Record

LTRT	Description
12760	Initial document release for Version 7.2.

Documentation Feedback

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

This page is intentionally left blank.

1 Introduction

This Configuration Note describes how to set up AudioCodes Enterprise Session Border Controller (hereafter, referred to as *E-SBC*) for interworking between DTAG's SIP Trunk and SWYX IP-PBX environment.

You can also use AudioCodes' SBC Wizard tool to automatically configure the E-SBC based on this interoperability setup. However, it is recommended to read through this document in order to better understand the various configuration options. For more information on AudioCodes' SBC Wizard including download option, visit AudioCodes Web site at http://www.audiocodes.com/sbc-wizard (login required).

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and DTAG Partners who are responsible for installing and configuring DTAG's SIP Trunk and SWYX IP-PBX for enabling VoIP calls using AudioCodes E-SBC.

1.2 About AudioCodes E-SBC Product Series

AudioCodes' family of E-SBC devices enables reliable connectivity and security between the Enterprise's and the service provider's VoIP networks.

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

This page is intentionally left blank.

2 Component Information

2.1 AudioCodes E-SBC Version

Table 2-1: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 500 E-SBC ▪ Mediant 500L Gateway & E-SBC ▪ Mediant 800B Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 SBC ▪ Mediant 4000B SBC ▪ Mediant 9000 SBC ▪ Mediant Software SBC (SE and VE)
Software Version	SIP_7.20A.102.001
Protocol	▪ SIP/TCP (to the DTAG SIP-Trunk) ▪ SIP/UDP (to the SWYX IP-PBX)
Additional Notes	None

2.2 DTAG SIP-Trunk Version

Table 2-2: DTAG SIP-Trunk Version

Vendor/Service Provider	IBM / DTAG
SSW Model/Service	
Software Version	
Protocol	SIP
Additional Notes	None

2.3 SWYX IP-PBX Version

Table 2-3: SWYX IP-PBX Version

Vendor	SWYX
Model	SwyxWare 2015
Software Version	R40
Protocol	SIP
Additional Notes	SIP Client SwyxIt! Version 10.40.2540

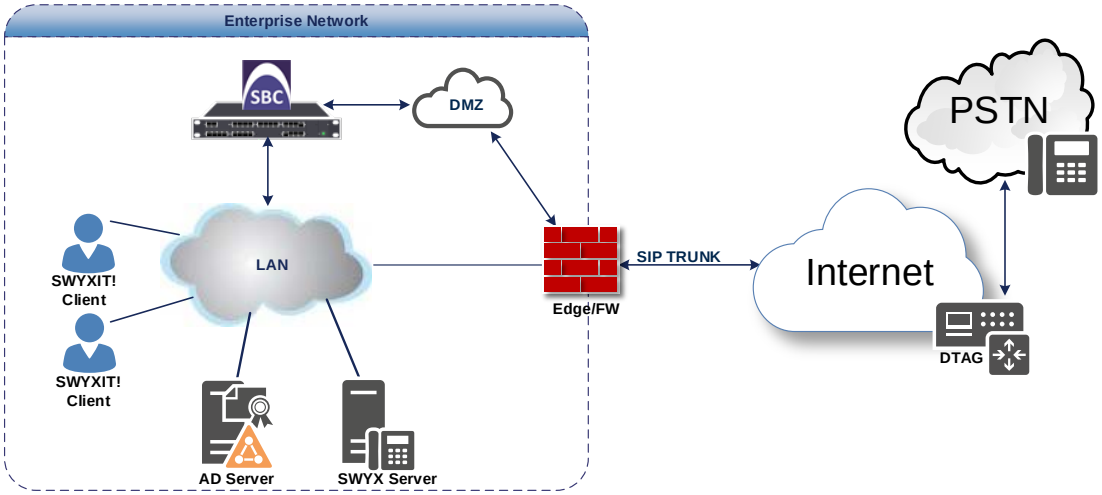
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and DTAG SIP-Trunk with SWYX IP-PBX was done using the following topology setup:

- Enterprise deployed with SwyxWare 2015 Server in its private network for enhanced communication within the Enterprise.
- Enterprise wishes to connect the Enterprise to the PSTN network using DTAG's SIP Trunking service.
- AudioCodes E-SBC is implemented to interconnect between the Enterprise LAN and the SIP Trunk.
  - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
  - **Border:** IP-to-IP network border between SWYX's IP-PBX in the Enterprise LAN and DTAG's SIP Trunk located in the public network.

The figure below illustrates this interoperability test topology:

Figure 2-1: Interoperability Test Topology between E-SBC and SWYX with DTAG SIP Trunk



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	▪ SwyxWare 2015 Server is located on the Enterprise's LAN ▪ DTAG SIP Trunk is located on the WAN
Signaling Transcoding	▪ SwyxWare 2015 operates with SIP-over-UDP transport type ▪ DTAG SIP Trunk operates with SIP-over-TCP transport type
Codecs Transcoding	▪ Both, SwyxWare 2015 and DTAG SIP Trunk supports G.711A-law and G.711U-law coders
Media Transcoding	▪ Both, SwyxWare 2015 and DTAG SIP Trunk operates with RTP media type

2.4.2 Known Limitations

The following limitation was observed during interoperability tests performed for AudioCodes' E-SBC interworking between SWYX's IP-PBX and DTAG 's SIP Trunk:

- If DTAG SIP-Trunk receives one of 5xx responses for example:
  - 503 Service Unavailable
  - 500 Server Internal Error

  DTAG SIP Trunk still sends re-INVITEs and does not disconnect the call.

  To disconnect the call, a message manipulation rule is used to replace the above error response with the '600 Busy Everywhere' response (see Section 4.11 on page 42).

This page is intentionally left blank.

3 Configuring SwyxWare 2015 Server

This chapter describes how to configure SwyxWare 2015 Server to operate with AudioCodes E-SBC.

Note: Number Mapping, Routing Table, and Locations are also necessary for PSTN deployment; however, they are beyond the scope of this document.

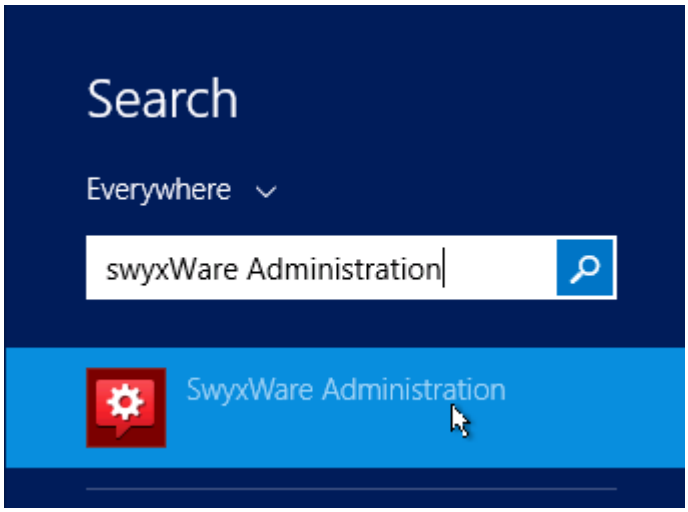
3.1 Configuring AudioCodes E-SBC Trunk on SwyxWare 2015 Server

The procedure below describes how to add the E-SBC in SWYX environment.

➢ **To add E-SBC to the SWYX environment:**

1. On the SwyxWare server, start the SwyxWare Administration (Windows **Start** menu > search for **SwyxWare Administration**), as shown below:

Figure 3-1: Starting the SwyxWare Administration console



The following is displayed:

Figure 3-2: SwyxWare Administration Console

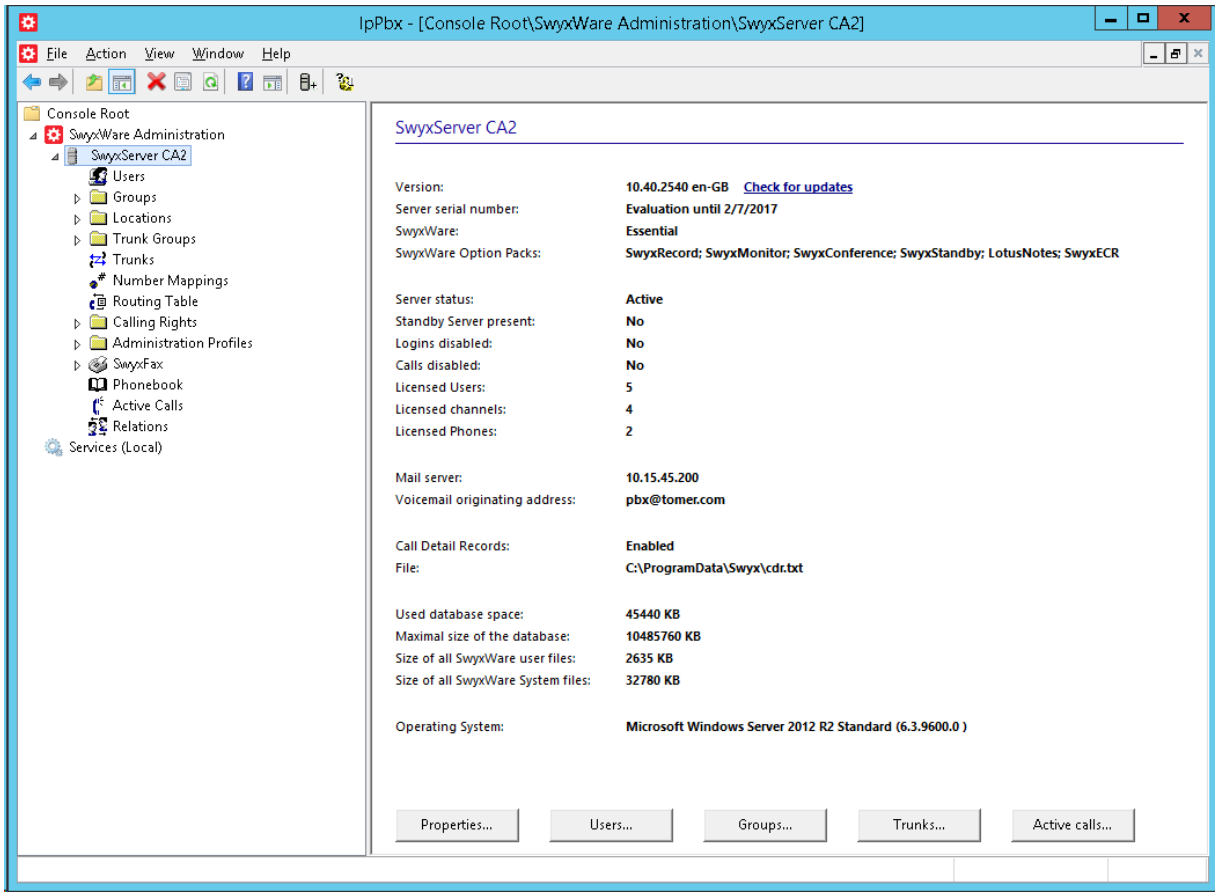
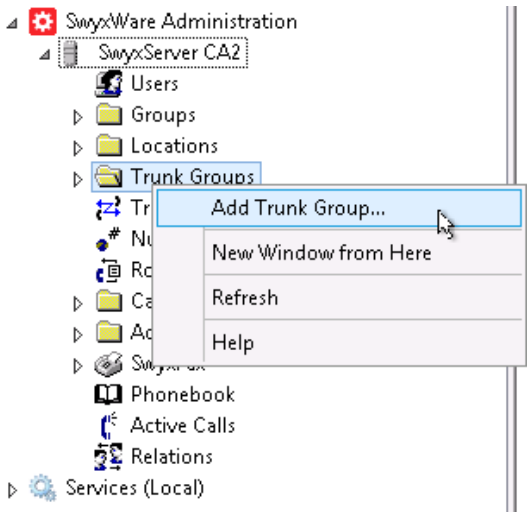


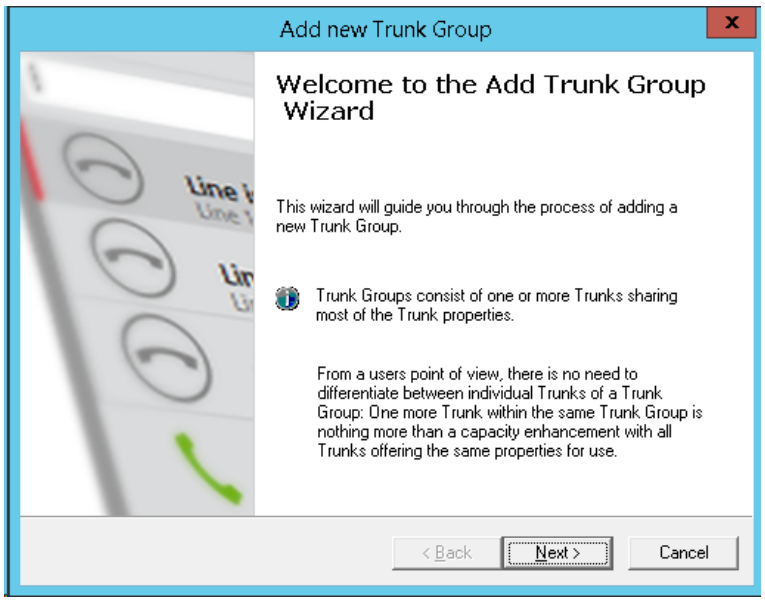
Figure 3-3: Add Trunk Group Dialog Box



2. Select the **Trunk Group** folder, right-click it to **Add Trunk Group**:

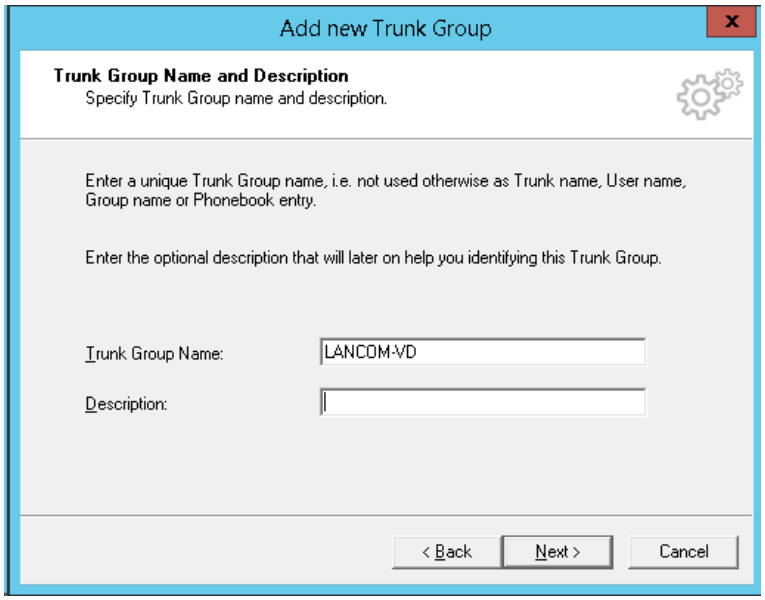
The Trunk Group wizard is displayed:

Figure 3-4: Trunk Group Wizard



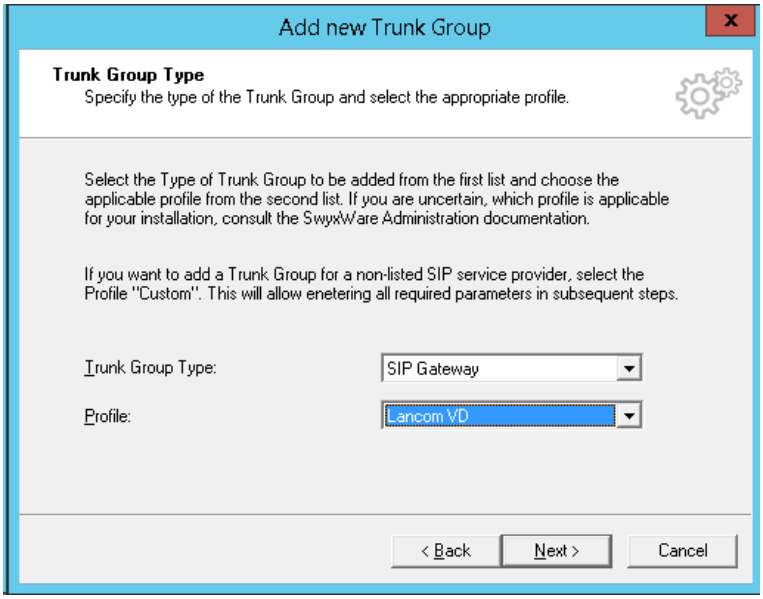
3. Click **Next**.

Figure 3 6: Add LANCOM-VD Trunk Group Name



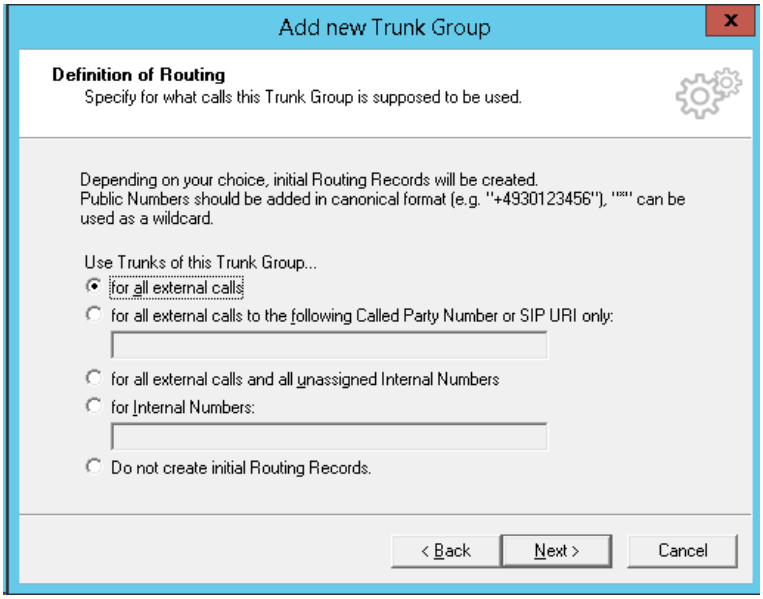
4. Under the **Trunk Group Name** write descriptive name (for e.g., **LANCOM-VD)** and then click **Next.**

Figure 3-5: Define the Trunk Group



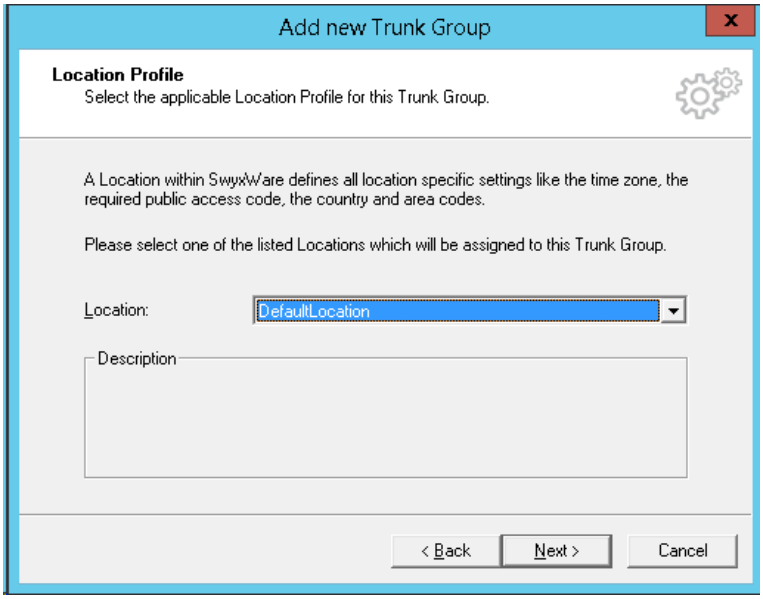
5. Under Trunk Group Type choose **SIP Gateway**
6. Under Profile choose **Lancom VD**
7. Click **Next**

Figure 3-6: Define Routing



8. Set the routing record for your Trunk Group (for example: **for all external calls)** and then click **Next**.

Figure 3-7: Define Location



9. Choose the location profile for your Trunk Group (for example: **DefaultLocation**) and then click **Next.**

Figure 3-8: Finish Trunk Group Wizard

10. Click **Finish** to close the wizard.

The LANCOM-VD Trunk Group is created:

Figure 3-9: LANCOM-VD added as Trunk Group

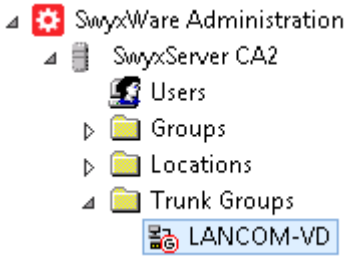
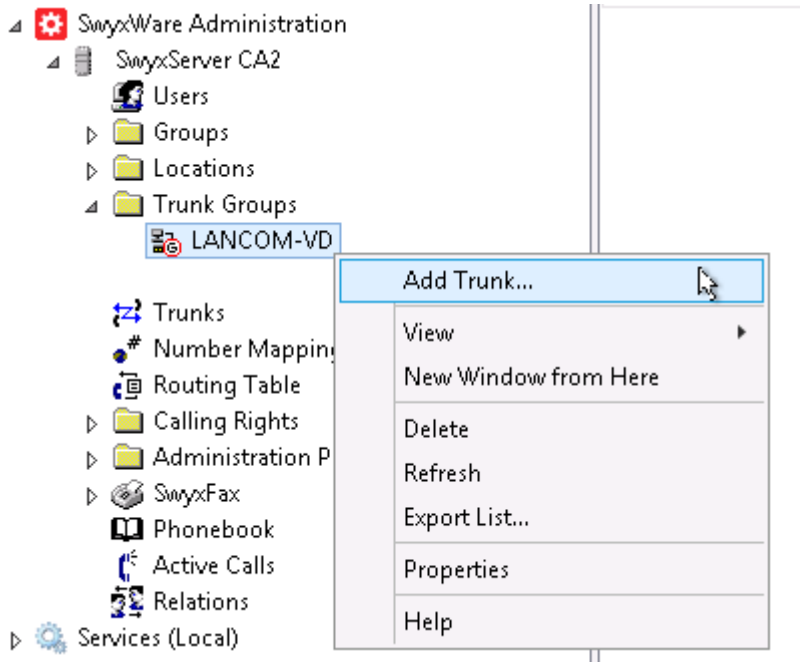


Figure 3-10: Add Trunk



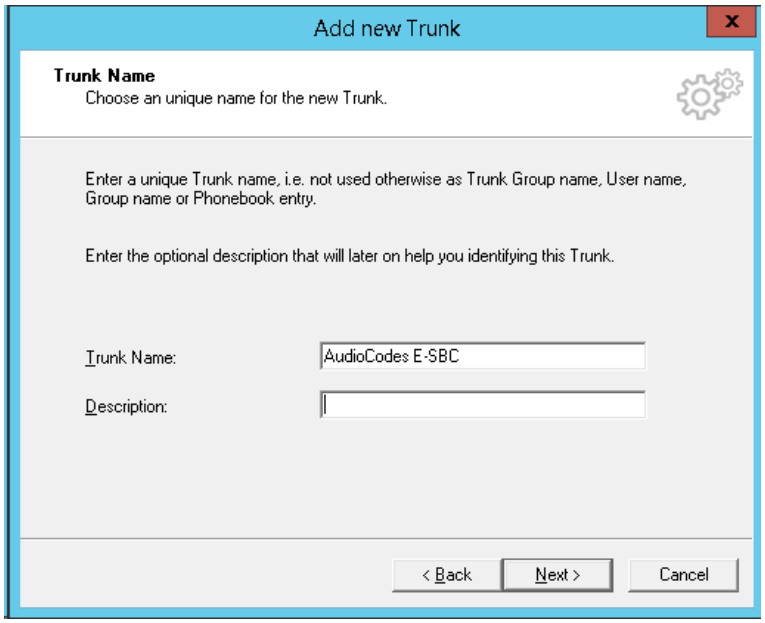
11. Select the created trunk group (LANCOM-VD), right-click it to **Add Trunk**

The Trunk wizard is displayed:

Figure 3-11: Trunk Wizard

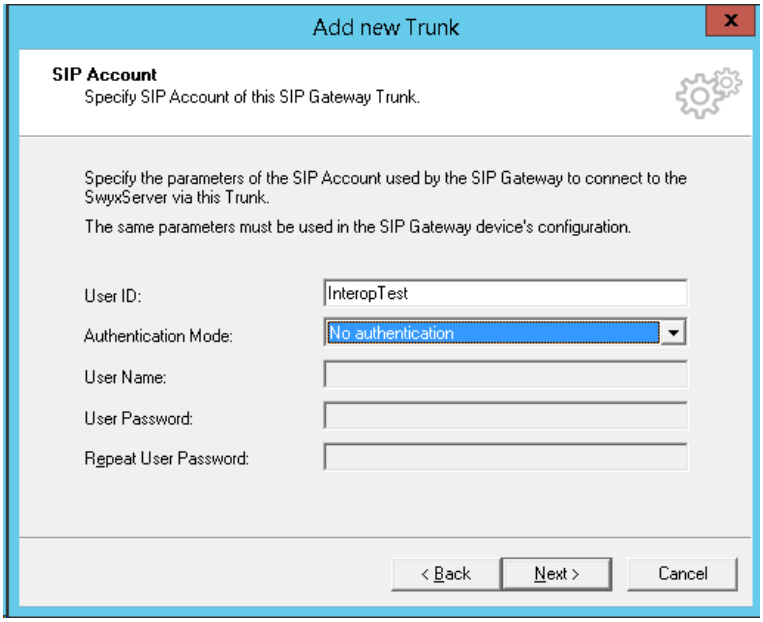
12. Click **Next**.

Figure 3 6: Add AudioCodes E-SBC Trunk Name



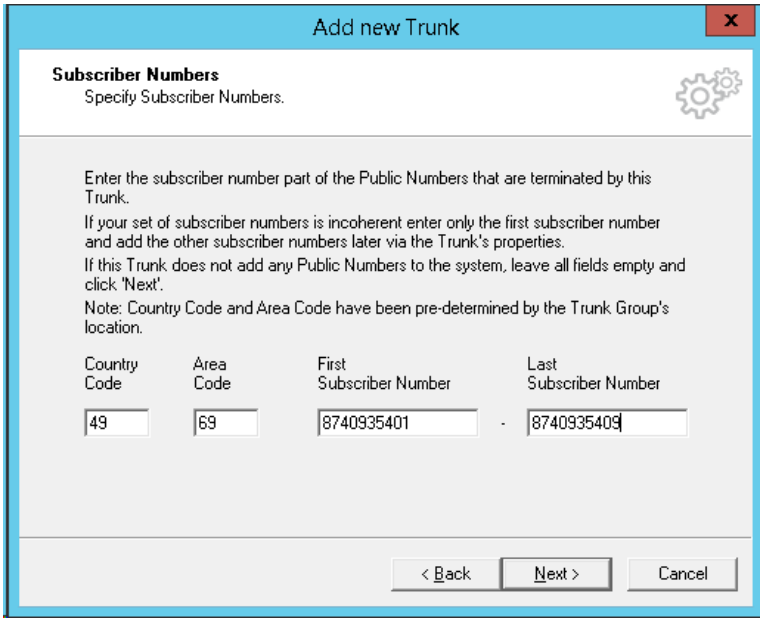
13. Under the **Trunk Name** write the name **AudioCodes E-SBC**, and then click **Next**, as shown below:

Figure 3-12: Define SIP Account



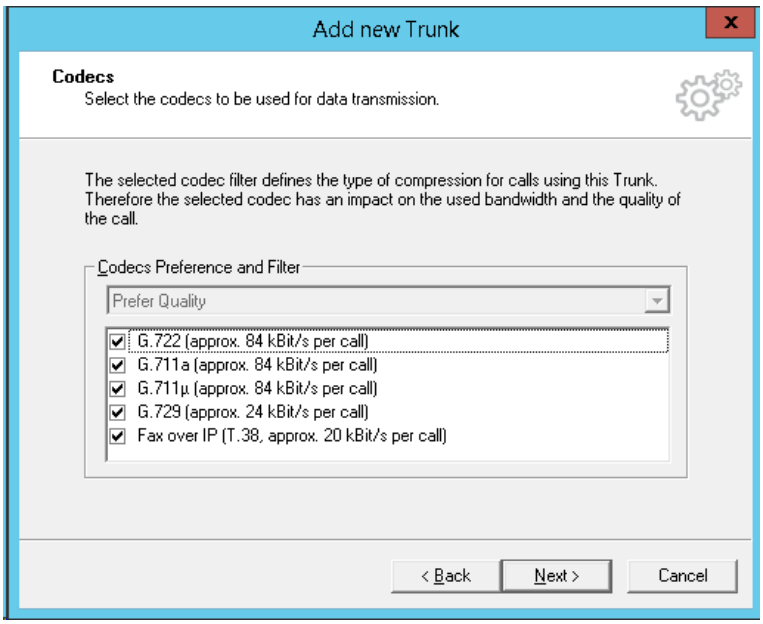
14. Under User ID: Enter the User ID that the SBC will use to register in order to activate the trunk (for example **InteropTest**)
15. Under Authentication Mode choose whether to use authentication or not.
16. If you choose Always Authenticate enter the User Name and Password.
17. Click **Next**.

Figure 3-13: Define Subscriber Numbers



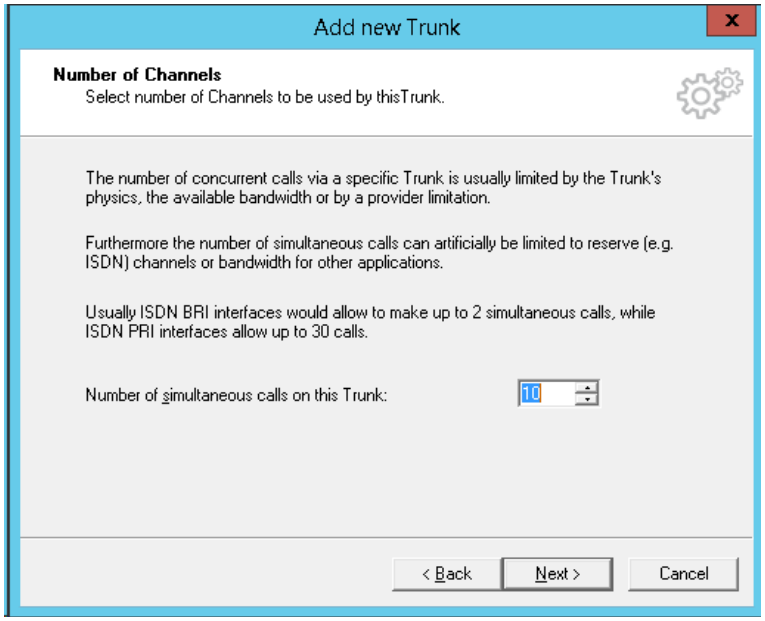
18. Set the subscriber Numbers that associated to the Trunk (for example: **49 69 8740935401 - 8740935409)** and then click **Next**.

Figure 3-14: Define Codecs



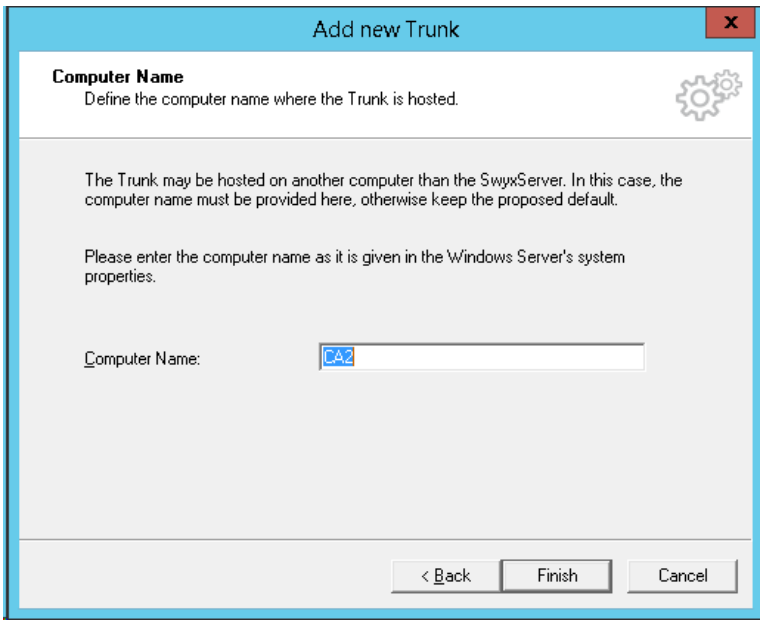
19. Choose the Available Codecs for this Trunk and then click **Next**.

Figure 3-15: Define Number of Channels



20. Choose the Number of Channels available for this Trunk and then click **Next**.

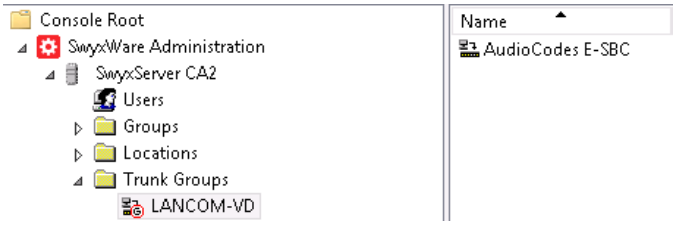
Figure 3-16: Finish Trunk Wizard



21. Click **Finish** to close the wizard.

The AudioCodes E-SBC Trunk is created:

Figure 3-17: AudioCodes E-SBC added as Trunk



This page is intentionally left blank.

4 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between SWYX IP-PBX and DTAG SIP-Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 10, and includes the following main areas:

- E-SBC WAN interface - DTAG SIP Trunking environment
- E-SBC LAN interface - SwyxWare 2015 environment

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

Notes:

- For implementing SWYX IP-PBX and DTAG SIP Trunk based on the configuration described in this section, AudioCodes E-SBC must be installed with a Software License Key that includes the following software features:
  - √ **SBC**
  - √ **Security**
  - √ **RTP**
  - √ **SIP**

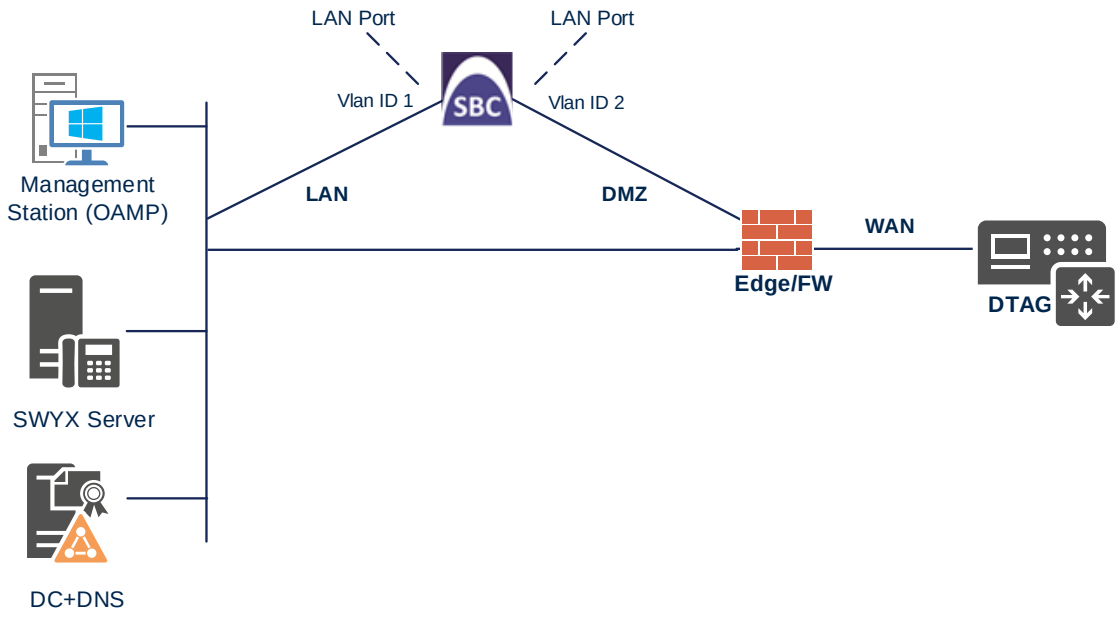
  For more information about the Software License Key, contact your AudioCodes sales representative.
- The scope of this interoperability test and document does **not** cover all security aspects for connecting the SIP Trunk to the SWYX IP-PBX environment. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products, refer to the *Recommended Security Guidelines* document.

4.1 Step 1: IP Network Interfaces Configuration

This step describes how to configure the E-SBC's IP network interfaces. There are several ways to deploy the E-SBC; however, this interoperability test topology employs the following deployment method:

- E-SBC interfaces with the following IP entities:
  - SWYX IP-PBX, located on the LAN
  - DTAG SIP Trunk, located on the WAN
- Physical connection: The type of physical connection to the LAN depends on the method used to connect to the Enterprise's network. In the interoperability test topology, E-SBC connects to the LAN and DMZ using dedicated LAN ports (i.e., two physical ports are used).
- E-SBC also uses two logical network interfaces:
  - LAN (VLAN ID 1)
  - DMZ (VLAN ID 2)

Figure 4-1: Network Interfaces in Interoperability Test Topology



4.1.1 Step 1a: Configure VLANs

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

- LAN VoIP (assigned the name "LAN_IF")
- WAN VoIP (assigned the name "WAN_IF")

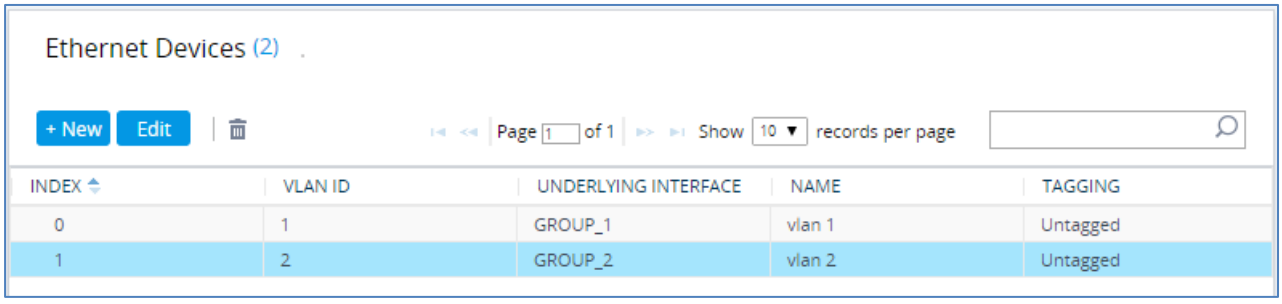
➢ **To configure the VLANs:**

1. Open the Ethernet Device table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Ethernet Devices**).

   There will be one 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	**vlan 2**
Tagging	**Untagged**

Figure 4-2: Configured VLAN IDs in Ethernet Device



4.1.2 Step 1b: Configure Network Interfaces

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

- LAN VoIP (assigned the name "LAN_IF")
- WAN VoIP (assigned the name "WAN_IF")

➢ **To configure the IP network interfaces:**

1. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
2. Modify the existing LAN network interface:
   a. Select the 'Index' radio button of the **OAMP + Media + Control** table row, and then click **Edit**.

b. Configure the interface as follows:

Parameter	Value
Name	**LAN_IF** (arbitrary descriptive name)
Ethernet Device	**vlan 1**
IP Address	**10.15.17.77** (LAN IP address of E-SBC)
Prefix Length	**16** (i.e., 255.255.0.0)
Default Gateway	**10.15.0.1** (LAN router's IP address)
Primary DNS	**10.15.27.1**

3. Add a network interface for the WAN side:

c. Click **New**.

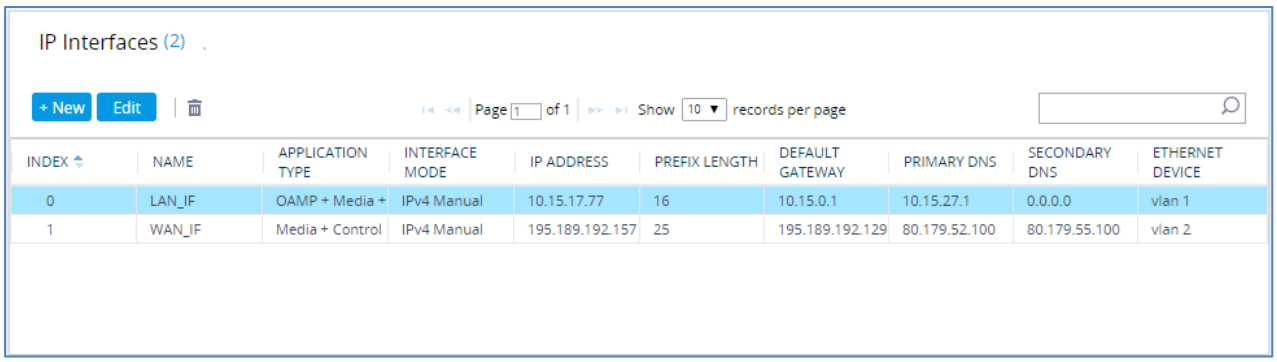
d. Configure the interface as follows:

Parameter	Value
Name	**WAN_IF** (arbitrary descriptive name)
Application Type	**Media + Control**
Ethernet Device	**vlan 2**
IP Address	**195.189.192.157** (DMZ IP address of E-SBC)
Prefix Length	**25** (i.e., 255.255.255.128)
Default Gateway	**195.189.192.129** (DMZ router's IP address)
Primary DNS	**80.179.52.100**
Secondary DNS	**80.179.55.100**

4. Click **Apply**.

The configured IP network interfaces are shown below:

Figure 4-3: Configured Network Interfaces in IP Interfaces Table



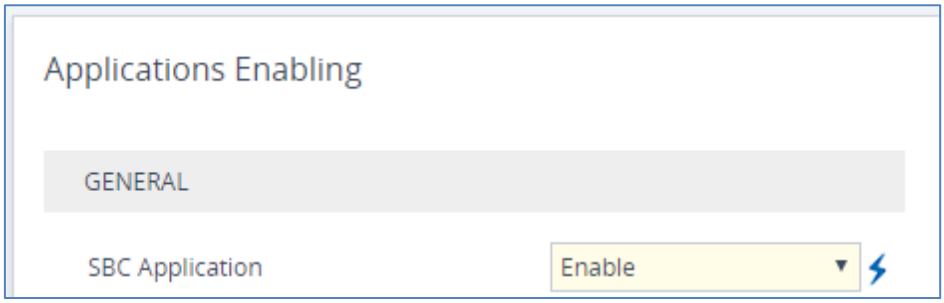
4.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

➢ **To enable the SBC application:**

1. Open the Applications Enabling page (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Applications Enabling**).

Figure 4-4: Enabling SBC Application



2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Apply**.
4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 4.13 on page 46).

4.3 Step 3: Configure Media Realms

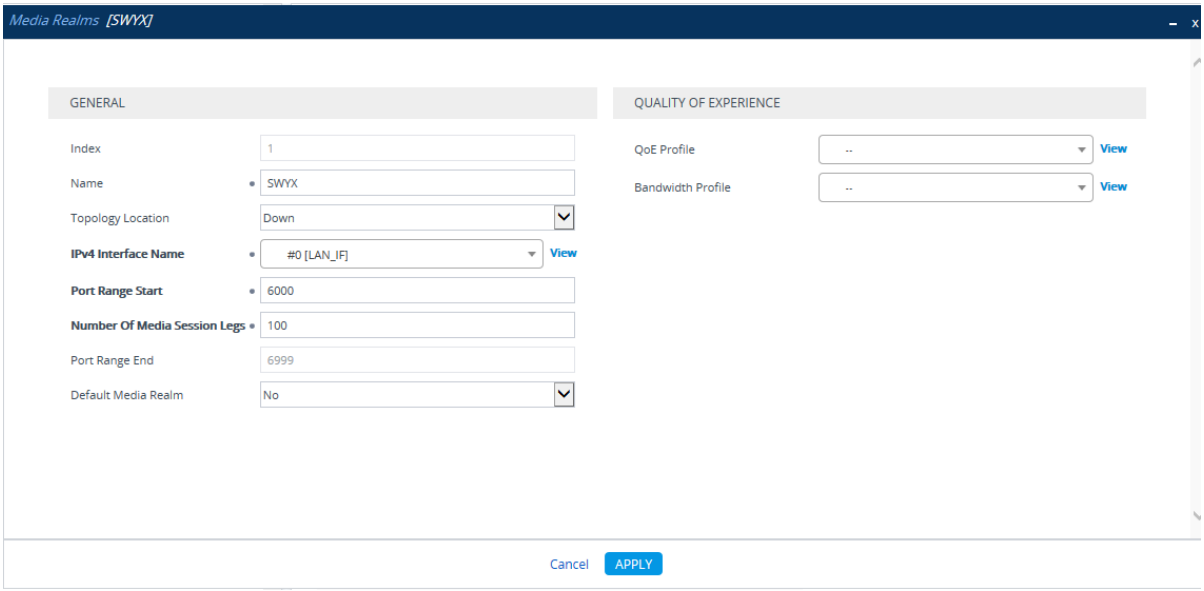
This step describes how to configure Media Realms. The straightforward configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➢ **To configure Media Realms:**

1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Create a new Media Realm for the LAN interface. You can use the default Media Realm (Index 0), but modify it as shown below:

Parameter	Value
Index	**0**
Name	**SWYX** (see note at the end of this section)
IPv4 Interface Name	**LAN_IF**
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)

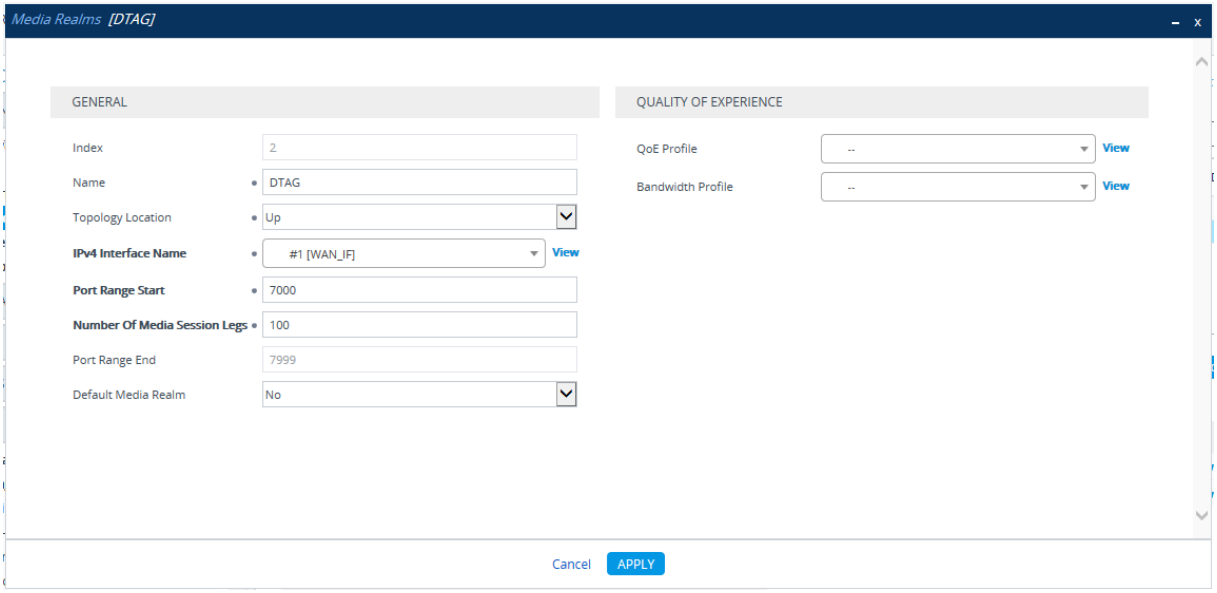
Figure 4-5: Configuring Media Realm for LAN



3. Create New Media Realm for WAN traffic as shown below:

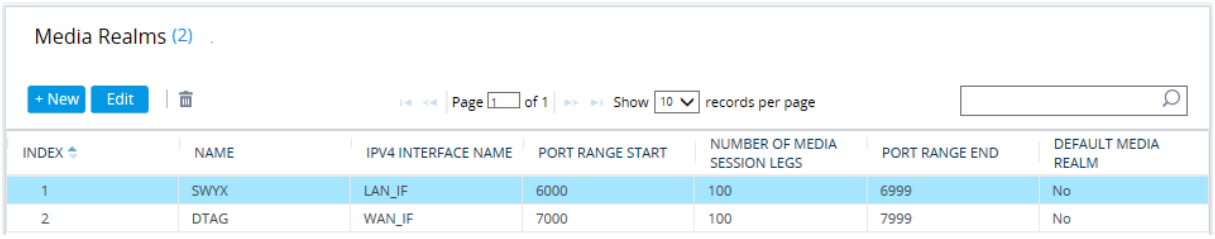
Parameter	Value
Index	**1**
Name	**DTAG** (descriptive name)
Topology Location	**Up**
IPv4 Interface Name	**WAN_IF**
Port Range Start	**7000** (represents lowest UDP port number used for media on WAN)
Number of Media Session Legs	**100** (media sessions assigned with port range)

Figure 4-6: Configuring Media Realm for WAN



The configured Media Realms are shown in the figure below:

Figure 4-7: Configured Media Realms in Media Realm Table



Note: Current software releases uses the string **names** of the configuration entities (e.g., SIP Interface, Proxy Sets, and IP Groups). Therefore, it is recommended to configure each configuration entity with meaningful names for easy identification.

4.4 Step 4: Configure SIP Signaling Interfaces

This step describes how to configure SIP Interfaces. For the interoperability test topology, an internal and external SIP Interface must be configured for the E-SBC.

➢ **To configure SIP Interfaces:**

1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
2. Create New SIP Interface for the LAN interface. You can use the default SIP Interface (Index 0), but modify it as shown below:

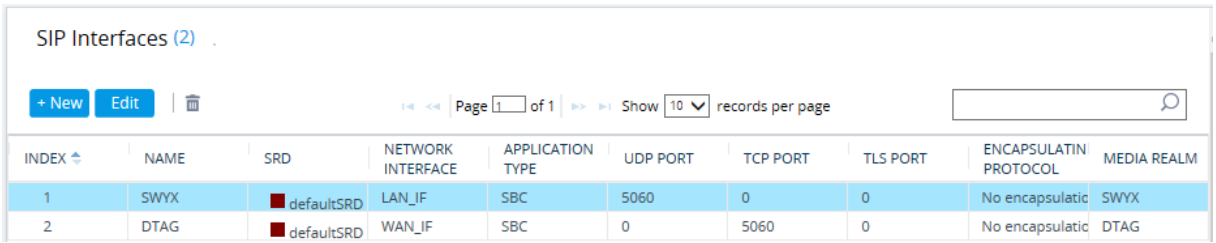
Parameter	Value
Index	**0**
Name	**SWYX**
Network Interface	**LAN_IF**
Application Type	**SBC**
UDP	**5060**
TCP and TLS	**0**
Media Realm	**SWYX**

3. Create New SIP Interface for the WAN as shown below:

Parameter	Value
Index	**1**
Name	**DTAG**
Network Interface	**WAN_IF**
Application Type	**SBC**
TCP Port	**5060**
UDP and TLS	**0**
Media Realm	**DTAG**

The configured SIP Interfaces are shown in the figure below:

Figure 4-8: Configured SIP Interfaces in SIP Interface Table



4.5 Step 5: 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:

- SwyxWare 2015 Server
- DTAG SIP Trunking

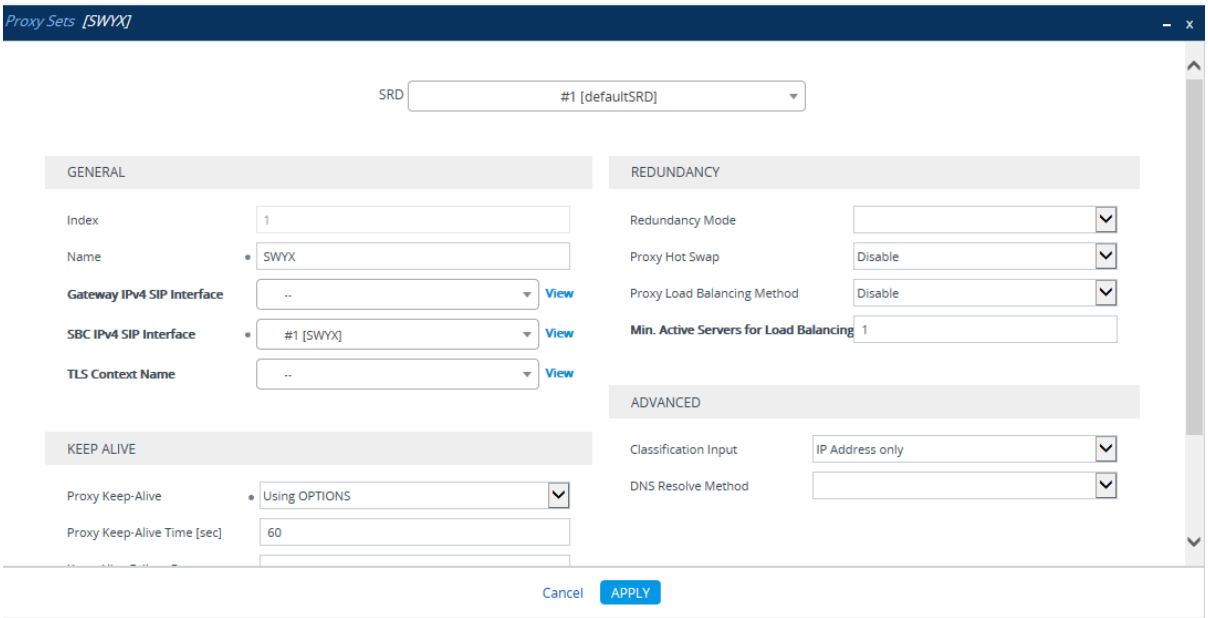
The Proxy Sets will be later applying to the VoIP network by assigning them to IP Groups.

➢ To configure Proxy Sets:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder >**Proxy Sets**).
2. Create New Proxy Set for the SwyxWare Server 2015 as shown below:

Parameter	Value
Index	**1**
Name	**SWYX**
SBC IPv4 SIP Interface	**SWYX**
Proxy Keep-Alive	**Using Options**

Figure 4-9: Configuring Proxy Set for SwyxWare 2015 server



3. Select the index row of the Proxy Set that you added, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
4. Click **New**; the following dialog box appears:

Figure 4-10: Configuring Proxy Address for SwyxWare Server 2015

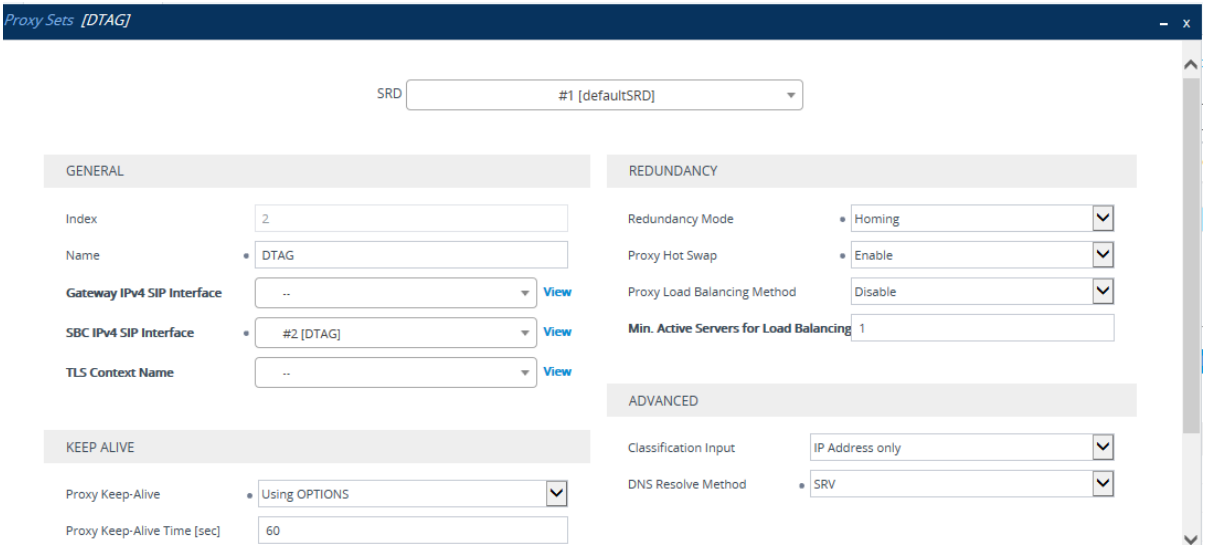
5. Configure a SIP address for the Proxy Set; see example in the table below:

Parameter	Value
Index	**0**
Proxy Address	**10.15.27.3:5060** (SwyxWare Server 2015 IP address / FQDN and destination port)
Transport Type	**UDP**

6. Create a new Proxy Set for the DTAG SIP Trunk as shown below:

Parameter	Value
Index	**2**
Name	**DTAG**
SBC IPv4 SIP Interface	**DTAG**
Proxy Keep-Alive	**Using Options**
Redundancy Mode	**Homing**
Proxy Hot Swap	**Enable**
DNS Resolve Method	**SRV**

Figure 4-11: Configuring Proxy Set for DTAG SIP Trunking



7. Select the index row of the Proxy Set that you added, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
8. Click **New**; the following dialog box appears:

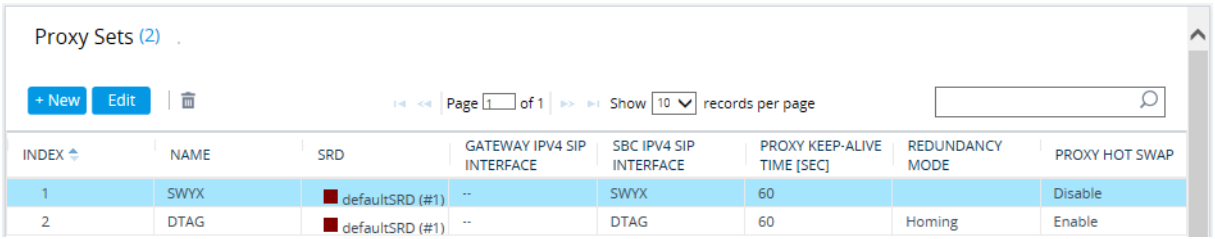
Figure 4-12: Configuring Proxy Address for DTAG SIP Trunking

9. Configure the SIP address for the Proxy Set; see example in the table below:

Parameter	Value
Index	**0**
Proxy Address	**register-test.sip-trunk.telekom.de** (IP address / FQDN and destination port)
Transport Type	**TCP**

The configured Proxy Sets are shown in the figure below:

Figure 4-13: Configured Proxy Sets in Proxy Sets Table



4.6 Step 6: Configure IP Profiles

This step describes how to configure IP Profiles. The IP Profile defines a set of call capabilities relating to signaling (e.g., SIP message terminations such as REFER) and media (e.g., coder and transcoding method).

In this interoperability test topology, IP Profiles need to be configured for the following IP entities:

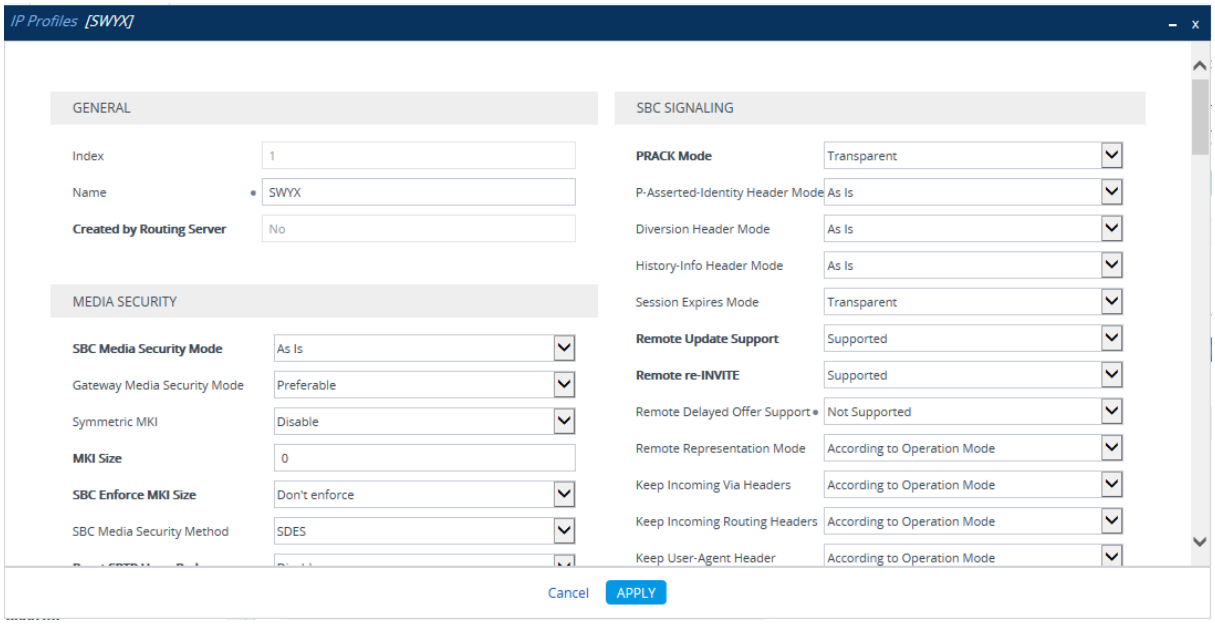
- SWYX IP-PBX
- DTAG SIP-trunk

➢ **To configure IP Profiles:**

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Create New IP Profile for the SYWX IP-PBX as shown below:

Parameter	Value
General	
Index	**1**
Name	**SWYX**
SBC Signaling	
Remote Delayed Offer Support	**Not Supported** (required, as SWYX doesn't support it due incoming REFER)

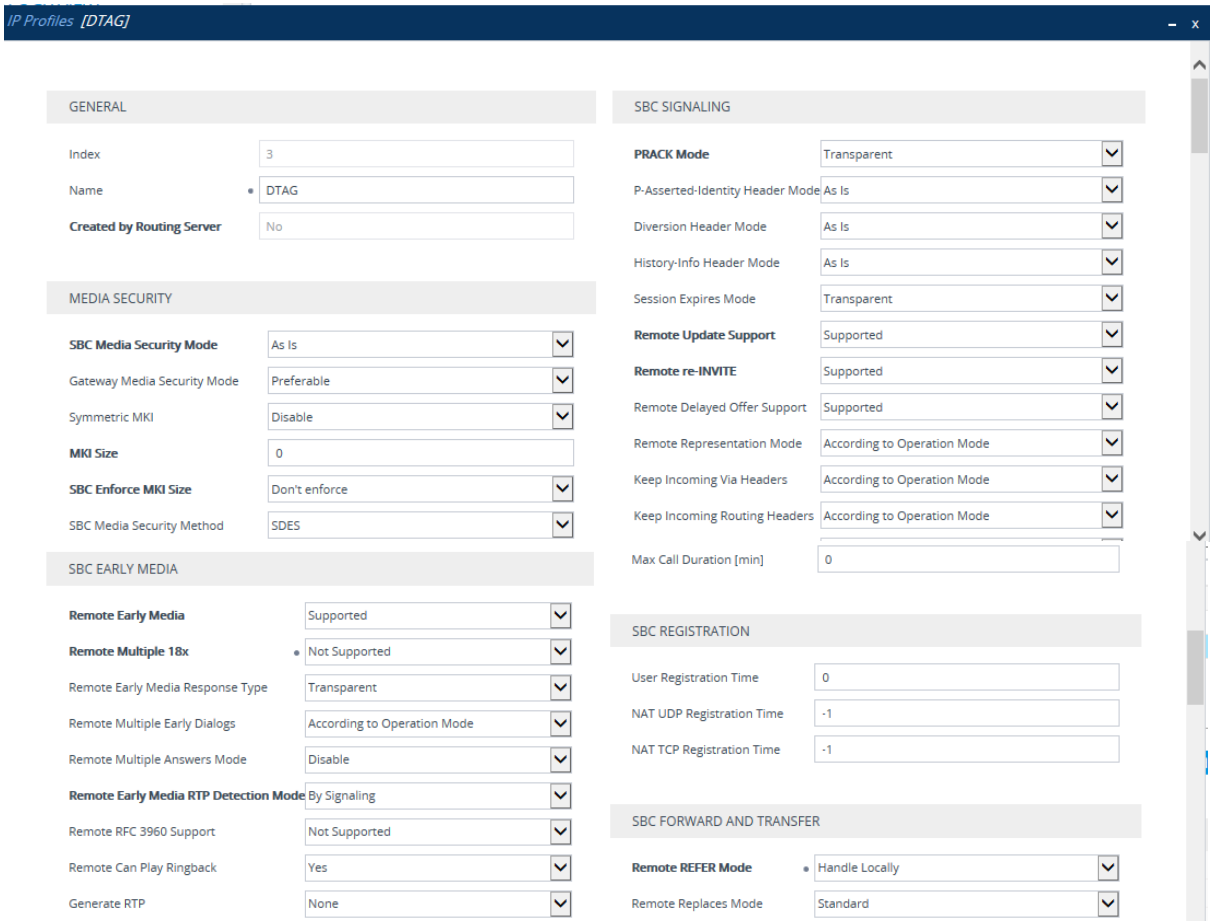
Figure 4-14: Configuring IP Profile for SWYX



3. Create New IP Profile for the DTAG SIP-Trunk as shown below:

Parameter	Value
General	
Index	**2**
Name	**DTAG**
SBC Early Media	
Remote Multiple 18x	**No** (required, as DTAG does not able to handle multiple 18x ringback tone in call forwarding scenario)
SBC Forward and Transfer	
Remote REFER Mode	**Handle Locally** (required, as for DTAG does not support receipt of SIP REFER)

Figure 4-15: Configuring IP Profile for DTAG SIP Trunk



4.7 Step 7: Configure IP Groups

This step describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the E-SBC communicates. This can be a server (e.g., IP PBX or ITSP) or it can be a group of users (e.g., IP phones). For servers, the IP Group is typically used to define the server's IP address by associating it with a Proxy Set. Once IP Groups are configured, they are used to configure IP-to-IP routing rules for denoting source and destination of the call.

In this interoperability test topology, IP Groups must be configured for the following IP entities:

- SWYX IP-PBX
- DTAG SIP-Trunk

➢ **To configure IP Groups:**

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Create a new IP Group for the SYWX IP-PBX as shown below:

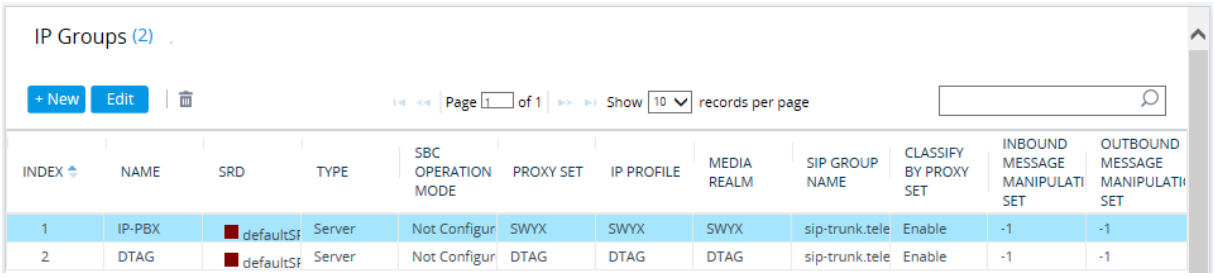
Parameter	Value
Index	**1**
Name	**SWYX**
Type	**Server**
Proxy Set	**SWYX**
IP Profile	**SWYX**
Media Realm	**SWYX**
SIP Group Name	**sip-trunk.telekom.de** (according to ITSP requirement)
Destination URI Input	**TO** (SWYX destination number is located on the to-header)

3. Create a new an IP Group for the DTAG SIP-Trunk as shown below:

Parameter	Value
Index	**2**
Name	**DTAG**
Topology Location	**Up**
Type	**Server**
Proxy Set	**DTAG**
IP Profile	**DTAG**
Media Realm	**DTAG**
SIP Group Name	**sip-trunk.telekom.de** (according to ITSP requirement)

The configured IP Groups are shown in the figure below:

Figure 4-16: Configured IP Groups in IP Group Table



4.8 Step 8: Configure Maximum IP Media Channels

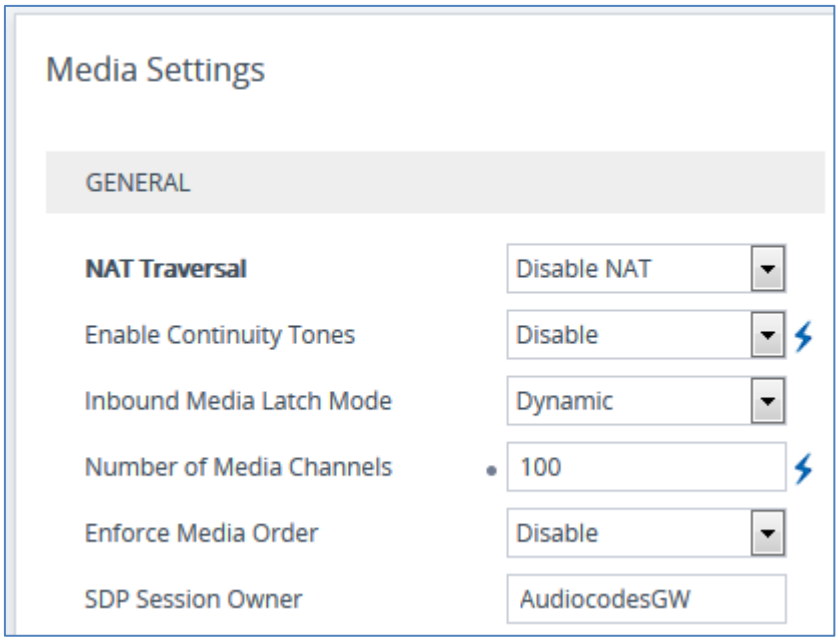
This step describes how to configure the maximum number of required IP media channels. The number of media channels represents the number of DSP channels that the E-SBC allocates to call sessions.

Note: This step is required **only** if transcoding is required. In this Interoperability tests topology Media Channels **wasn't required**.

➢ **To configure the maximum number of IP media channels:**

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

Figure 4-17: Configuring Number of Media Channels



2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g., **100**).
3. Click **Apply**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.13 on page 46).

4.9 Step 9: 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 E-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 typically uses the configured IP Groups (as configured in Section 4.6 on page 33,) to denote the source and destination of the call.

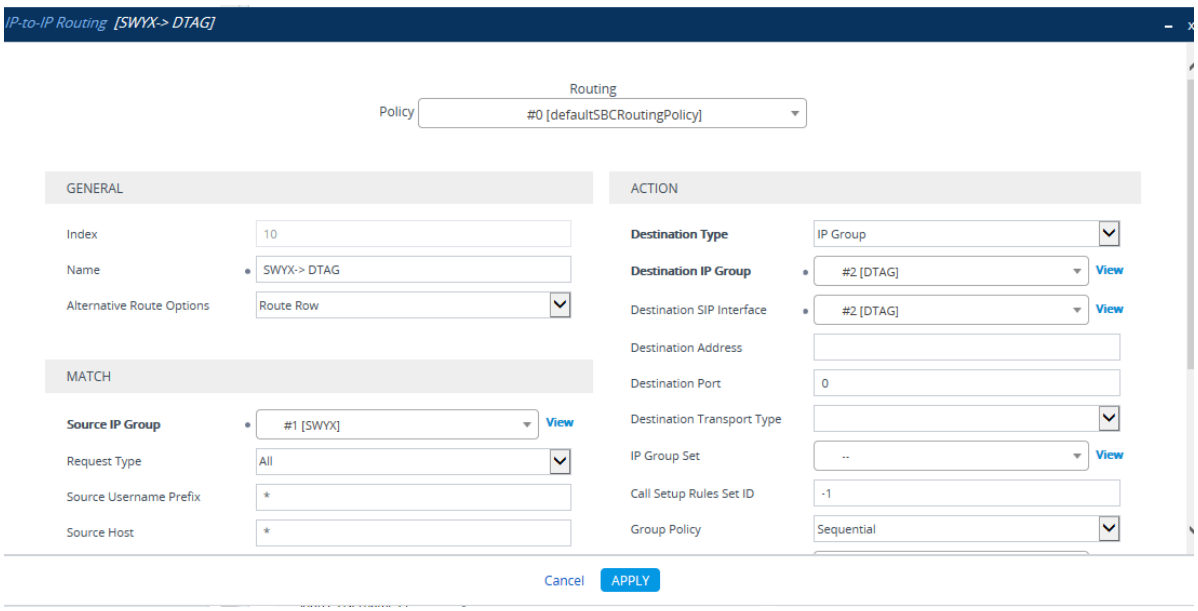
For the interoperability test topology, the following IP-to-IP routing rules need to be configured:

- Calls from SWYX IP-PBX to DTAG SIP Trunk
- Calls from DTAG SIP Trunk to SWYX IP-PBX

1. Create a new rule to route calls from SWYX IP-PBX to DTAG SIP Trunk as shown below:

Parameter	Value
Index	**1**
Route Name	**SWYX → DTAG** (descriptive name)
Source IP Group	**SWYX**
Destination Type	**IP Group**
Destination IP Group	**DTAG**
Destination SIP Interface	**DTAG**

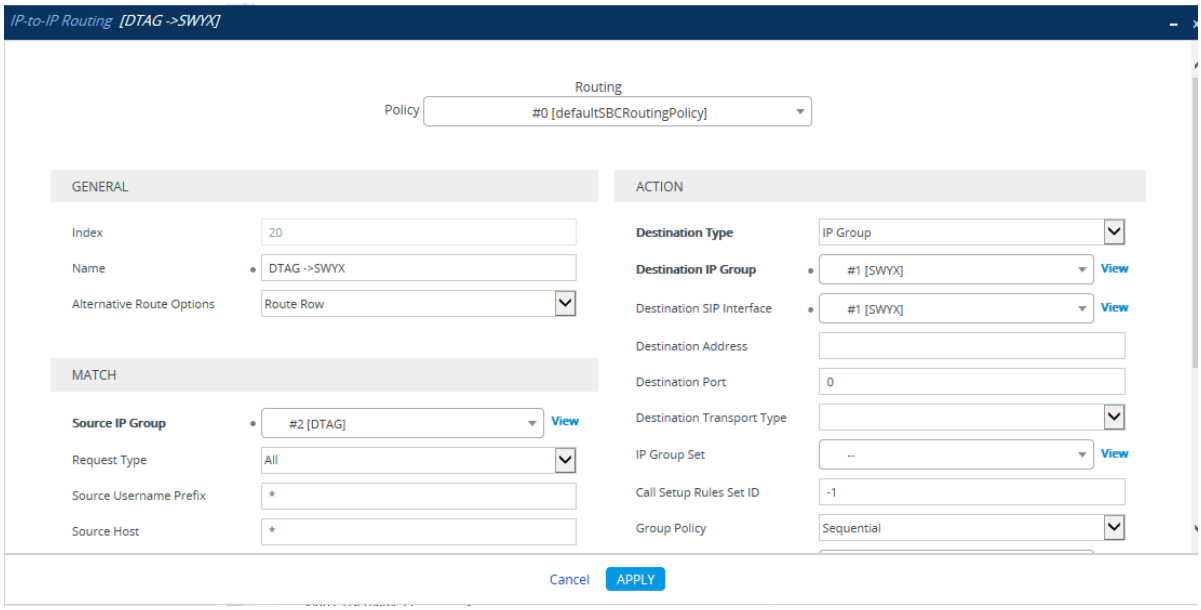
Figure 4-18: Configuring IP-to-IP Routing Rule from SWYX to DTAG



2. Create a new rule to route calls from DTAG SIP to SWYX IP-PBX Trunk as shown below:

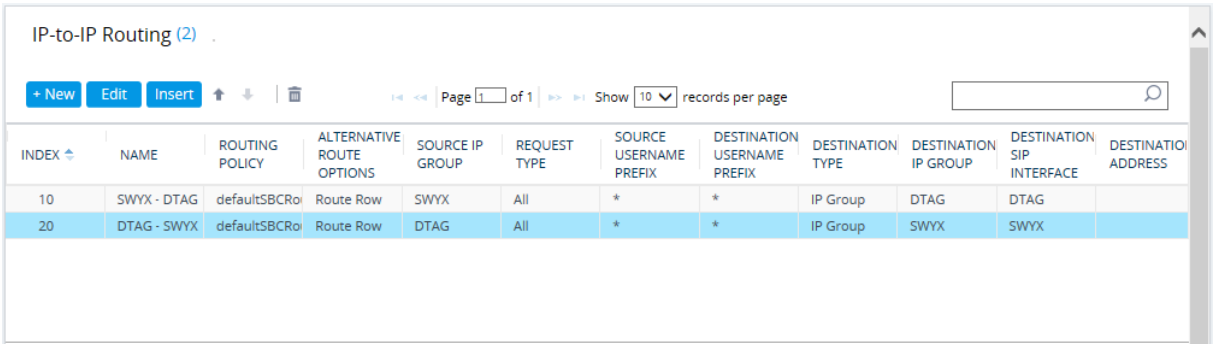
Parameter	Value
Index	**2**
Route Name	**DTAG → SYWX** (descriptive name)
Source IP Group	**DTAG**
Destination Type	**IP Group**
Destination IP Group	**SYWX**
Destination SIP Interface	**SYWX**

Figure 4-19: Configuring IP-to-IP Routing Rule from DTAG to SYWX



The configured routing rules are shown in the figure below:

Figure 4-20: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table



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

4.10 Step 10: Configure IP-to-IP Manipulation Rules

This step describes how to configure IP-to-IP manipulation rules. These rules manipulate the SIP Request-URI user part (source or destination number). The manipulation rules use the configured IP Groups (as configured in Section 4.6 on page 33) to denote the source and destination of the call.

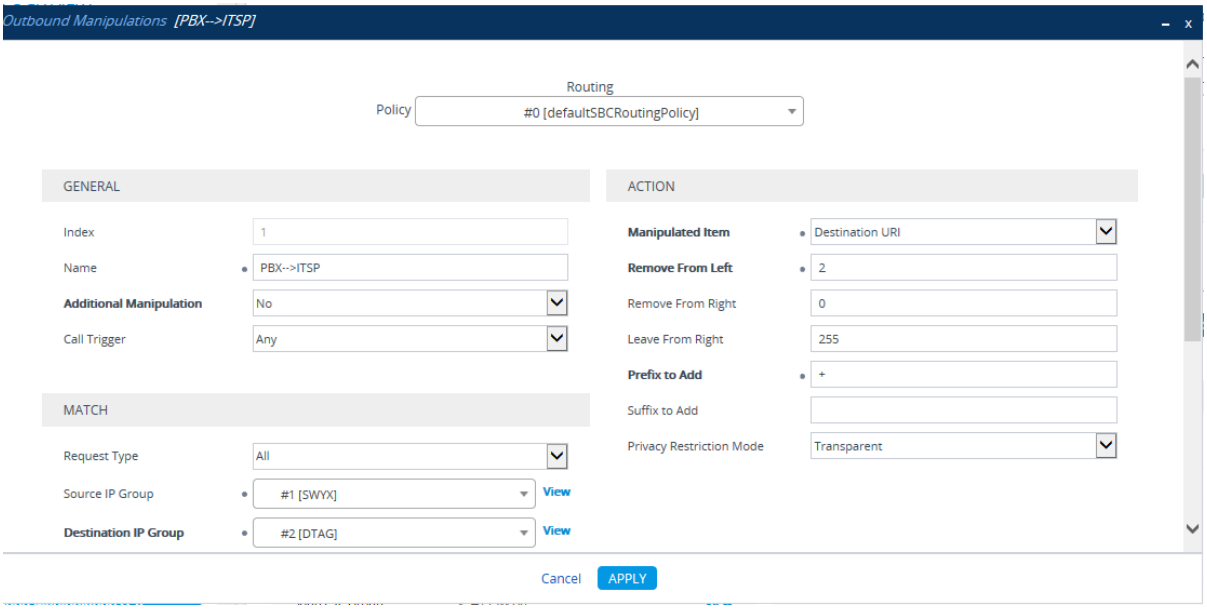
For this interoperability test topology, a manipulation rule is configured for "00" destination username prefix to remove the "00" and add the "+" (plus sign) to the destination number for calls from SWYX IP Group to DTAG IP Group.

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

1. Open the Outbound Manipulations table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Manipulation** > **Outbound Manipulations**).
2. Create a new Number Manipulation rule as shown below:

Parameter	Value
Index	**0**
Name	**PBX→ITSP**
Source IP Group	**SWYX**
Destination IP Group	**DTAG**
Destination Username Prefix	**00**
Manipulated Item	**Destination URI**
Remove From Left	**2**
Prefix to Add	**+** (plus sign)

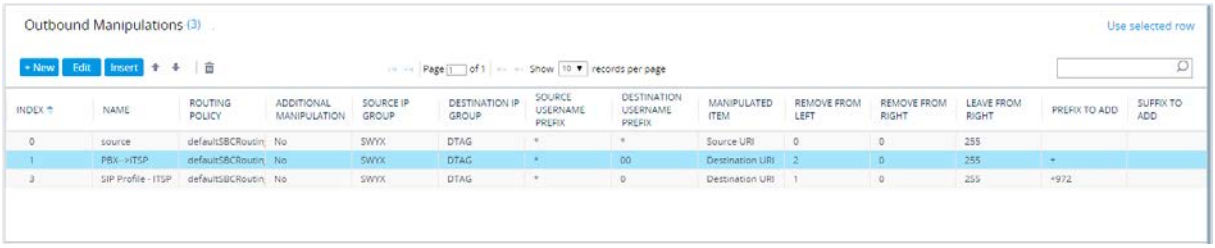
Figure 4-21: Configuring IP-to-IP Outbound Manipulation Rule



The table below shows an example of configured IP-to-IP outbound manipulation rules for calls between SWYX IP Group and DTAG SIP Trunk IP Group:

Rule Index	Description
0	For calls from SWYX IP Group to DTAG IP Group with any Source (*), add "+" to the prefix of the Source number.
1	For calls from SWYX IP Group to DTAG IP Group with the prefix destination number "00", remove "00" from this prefix and add "+" to the prefix of the destination number.
2	For calls from SWYX IP Group to DTAG IP Group with the prefix destination number "0", remove "0" from this prefix and add "+972" to the prefix of the destination number.

Figure 4-22: Example of Configured IP-to-IP Outbound Manipulation Rules



Note: Adapt the manipulation table according to your environment dial plan.

4.11 Step 11: Configure Message Manipulation Rules

This step describes how to configure SIP message manipulation rules. SIP message manipulation rules can include insertion, removal, and/or modification of SIP headers. Manipulation rules are grouped into Manipulation Sets, enabling you to apply multiple rules to the same SIP message (IP entity).

Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

➢ **To configure SIP message manipulation rule:**

1. Open the Message Manipulations page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 4) for DTAG SIP Trunk. This rule applies to response messages sent to the DTAG SIP Trunk IP Group for Rejected Calls initiated by the SWYX IP Group or SBC. This rule replaces the method types '5xx' with the value '600' (Busy Everywhere), since DTAG SIP Trunk does not disconnect the call immediately after receiving '5xx' method types.

Parameter	Value
Index	**0**
Name	**Reject Cause**
Manipulation Set ID	**4**
Message Type	**any.response.5xx**
Action Subject	**header.request-uri.methodtype**
Action Type	**Modify**
Action Value	**'600'**

Figure 4-23: Configuring SIP Message Manipulation Rule 0 (for DTAG SIP Trunk)

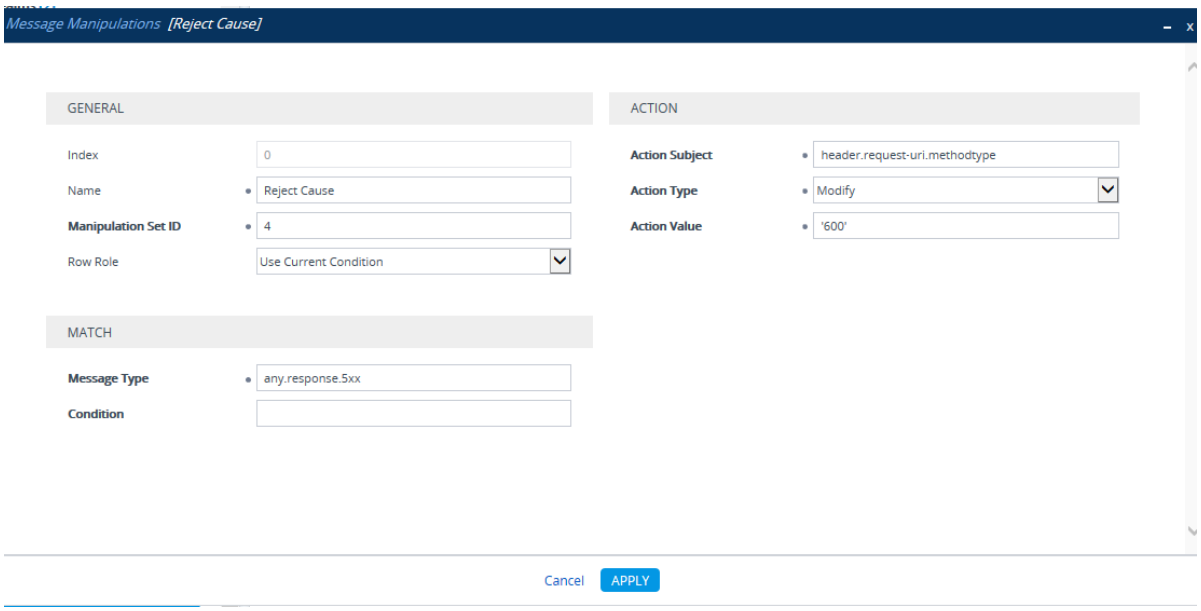
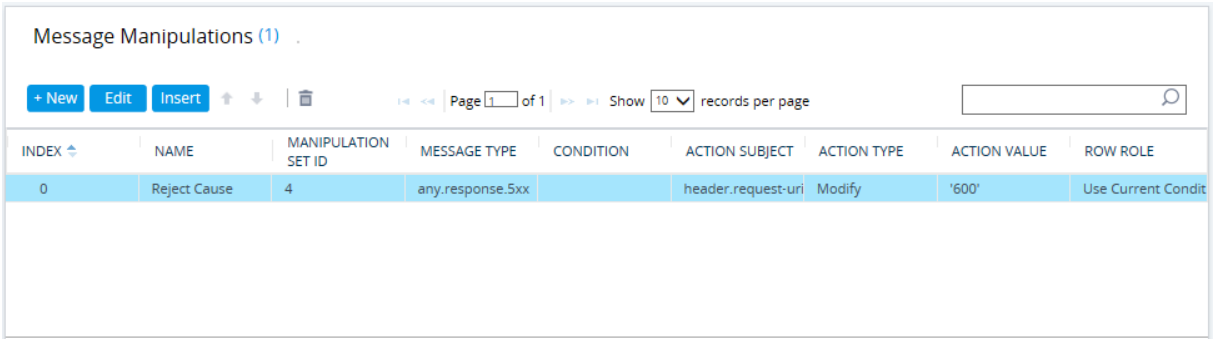
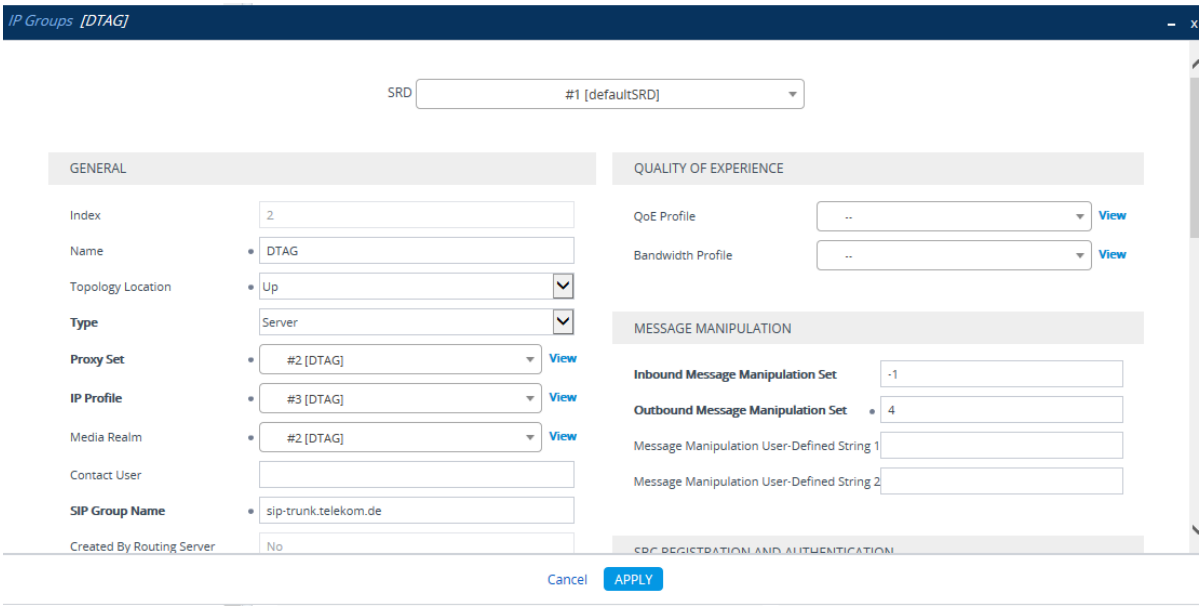


Figure 4-24: Configured SIP Message Manipulation Rule



3. Assign Manipulation Set ID 4 to the DTAG SIP Trunk IP Group:
   a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
   b. Select the row of the DTAG SIP trunk IP Group, and then click **Edit**.
   c. Set the 'Outbound Message Manipulation Set' field to **4**.

Figure 4-25: Assigning Manipulation Set 4 to the DTAG SIP Trunk IP Group



   d. Click **Apply**.

4.12 Step 12: Configure Registration Accounts

This step describes how to configure SIP registration accounts, which are required for the following:

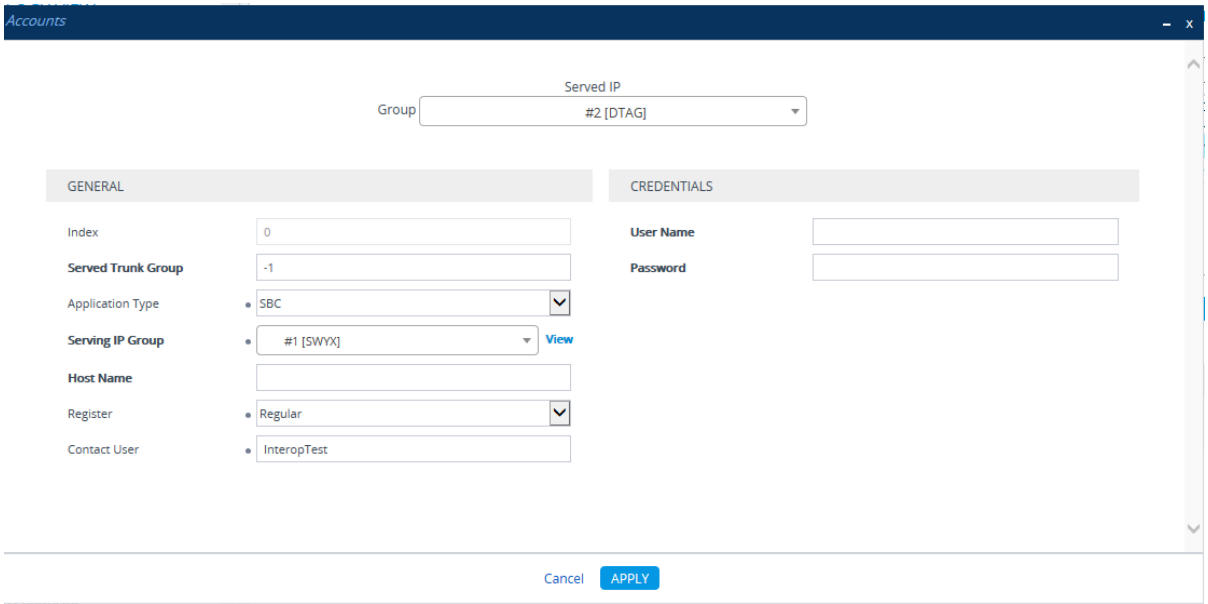
- DTAG SIP Trunk. The DTAG SIP Trunk requires registration and authentication to provide service.
- SWYX IP-PBX. The SwyxWare 2015 Lancom-VD Trunk Group requires registration in order to activate it.

➢ **To configure a registration accounts:**

1. Open the Account Table page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Account Table**).
2. Create a new account according to the provided information from the SWYX, for example:

Parameter	Value
Served IP Group	**2** (DTAG)
Application Type	**SBC**
Serving IP Group	**1** (SWYX)
Register	**Regular**
Contact User	**InteropTest** (as configured in the SwyxWare Trunk)
Username	if configured in the SwyxWare Trunk
Password	if configured in the SwyxWare Trunk

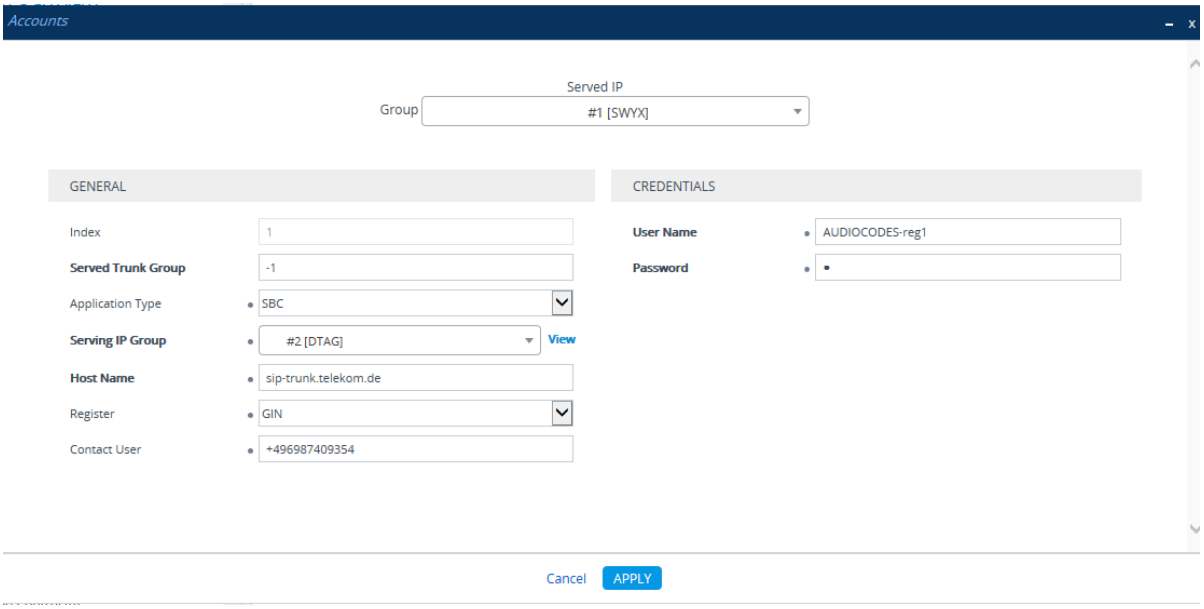
Figure 4-26: Configuring a SIP Registration Account for SWYX



3. Create a new account according to the provided information from DTAG , for example:

Parameter	Value
Served IP Group	**1** (SWYX)
Application Type	**SBC**
Serving IP Group	**2** (DTAG)
Host Name	**sip-trunk.telekom.de**
Register	**GIN**
Contact User	**+496987409354** (trunk main line)
Username	as provided by DTAG
Password	as provided by DTAG

Figure 4-27: Configuring a SIP Registration Account for DTAG



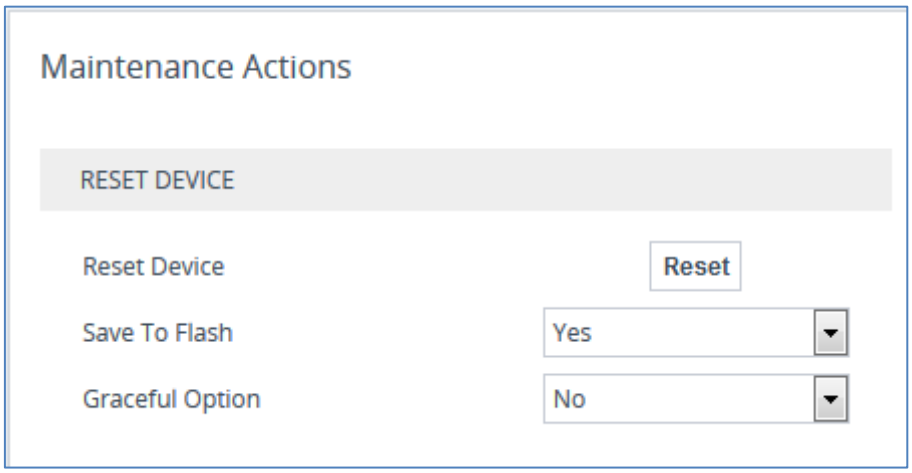
4.13 Step 13: Reset the E-SBC

After you have completed the configuration of the E-SBC described in this chapter, save ("burn") the configuration to the E-SBC's flash memory with a reset for the settings to take effect.

➢ **To reset the device through Web interface:**

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

Figure 4-28: Resetting the E-SBC



2. Ensure that the ' Save To Flash' field is set to **Yes** (default).
3. Click the **Reset** button; a confirmation message box appears, requesting you to confirm.
4. Click **OK** to confirm device reset.

A AudioCodes INI File

The *ini* configuration file of the E-SBC, corresponding to the Web-based configuration as described in Section 4 on page 23, is shown below:

Note: To load or save an *ini* file, use the Configuration File page (**Setup** menu > **Administration** tab > **Maintenance** folder > **Configuration File**).

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

;Board: Mediant 800B
;HW Board Type: 69  FK Board Type: 72
;Serial Number: 7622916
;Slot Number: 1
;Software Version: 7.20A.102.001
;DSP Software Version: 5014AE3_R => 721.07
;Board IP Address: 10.15.45.49
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 512M   Flash size: 64M   Core speed: 500Mhz
;Num of DSP Cores: 1  Num DSP Channels: 59
;Num of physical LAN ports: 12
;Profile: NONE
;;;Key features:;Board Type: Mediant 800B ;DATA features: ;Channel Type:
RTP DspCh=250 IPMediaDspCh=250 ;E1Trunks=2 ;T1Trunks=2 ;FXSPorts=8
;FXOPorts=8 ;Coders: G723 G729 G728 NETCODER GSM-FR GSM-EFR AMR EVRC-
QCELP G727 ILBC EVRC-B AMR-WB G722 EG711 MS_RTA_NB MS_RTA_WB SILK_NB
SILK_WB SPEEX_NB SPEEX_WB OPUS_NB OPUS_WB ;DSP Voice features: ;Security:
IPSEC MediaEncryption StrongEncryption EncryptControlProtocol ;Control
Protocols: MGCP SIP SBC=250 ;Default features:;Coders: G711 G726;

;------  HW components------
;
; Slot # : Module type : # of ports
;-----------------------------------------------
;      1 : FXS         : 4
;      2 : FXS         : 4
;      3 : Empty
;-----------------------------------------------


[SYSTEM Params]

SyslogServerIP = 10.33.33.200
EnableSyslog = 1
;NTPServerIP_abs is hidden but has non-default value
;VpFileLastUpdateTime is hidden but has non-default value
SSHAdminKey = '.]☼ '
TR069ACSPASSWORD = '$1$gQ=='
TR069CONNECTIONREQUESTPASSWORD = '$1$gQ=='
NTPServerIP = '10.1.1.11'
;LastConfigChangeTime is hidden but has non-default value
```

```
;PM_gwINVITEDialogs is hidden but has non-default value
;PM_gwSBCMediaLegs is hidden but has non-default value
;PM_gwSBCTranscodingSessions is hidden but has non-default value

[BSP Params]

PCMLawSelect = 3
INIFileVersion = 2199
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

[PSTN Params]


[SS7 Params]


[Voice Engine Params]


[WEB Params]

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

[SIP Params]

MEDIACHANNELS = 0
REGISTRATIONTIME = 3600
GWDEBUGLEVEL = 5
USEGATEWAYNAMEFOROPTIONS = 1
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value
```

```
[IPsec Params]


[SNMP Params]


[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_SpeedDuplex,
PhysicalPortsTable_PortDescription, PhysicalPortsTable_GroupMember,
PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_4_1", 1, 4, "LAN Port#1", "GROUP_1", "Active";
PhysicalPortsTable 1 = "GE_4_2", 1, 4, "LAN Port#2", "GROUP_1",
"Redundant";
PhysicalPortsTable 2 = "GE_4_3", 1, 4, "WAN Port#1", "GROUP_2",
"Redundant";
PhysicalPortsTable 3 = "GE_4_4", 1, 4, "WAN Port#2", "GROUP_2", "Active";
PhysicalPortsTable 4 = "FE_5_1", 1, 4, "User Port #4", "GROUP_3",
"Active";
PhysicalPortsTable 5 = "FE_5_2", 1, 4, "User Port #5", "GROUP_3",
"Redundant";
PhysicalPortsTable 6 = "FE_5_3", 1, 4, "User Port #6", "GROUP_4",
"Active";
PhysicalPortsTable 7 = "FE_5_4", 1, 4, "User Port #7", "GROUP_4",
"Redundant";
PhysicalPortsTable 8 = "FE_5_5", 1, 4, "User Port #8", "GROUP_5",
"Active";
PhysicalPortsTable 9 = "FE_5_6", 1, 4, "User Port #9", "GROUP_5",
"Redundant";
PhysicalPortsTable 10 = "FE_5_7", 1, 4, "User Port #10", "GROUP_6",
"Active";
PhysicalPortsTable 11 = "FE_5_8", 1, 4, "User Port #11", "GROUP_6",
"Redundant";

[ \PhysicalPortsTable ]


[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, "GE_4_1", "GE_4_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_4_3", "GE_4_4";
EtherGroupTable 2 = "GROUP_3", 2, "FE_5_1", "FE_5_2";
EtherGroupTable 3 = "GROUP_4", 2, "FE_5_3", "FE_5_4";
EtherGroupTable 4 = "GROUP_5", 2, "FE_5_5", "FE_5_6";
EtherGroupTable 5 = "GROUP_6", 2, "FE_5_7", "FE_5_8";
EtherGroupTable 6 = "GROUP_7", 0, "", "";
EtherGroupTable 7 = "GROUP_8", 0, "", "";
EtherGroupTable 8 = "GROUP_9", 0, "", "";
EtherGroupTable 9 = "GROUP_10", 0, "", "";
EtherGroupTable 10 = "GROUP_11", 0, "", "";
EtherGroupTable 11 = "GROUP_12", 0, "", "";

[ \EtherGroupTable ]


[ DeviceTable ]
```

```
FORMAT DeviceTable_Index = DeviceTable_VlanID,
DeviceTable_UnderlyingInterface, DeviceTable_DeviceName,
DeviceTable_Tagging, DeviceTable_MTU;
DeviceTable 0 = 1, "GROUP_1", "LAN_DEV", 0, 1500;
DeviceTable 1 = 2, "GROUP_2", "WAN_DEV", 0, 1500;

[ \DeviceTable ]


[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.45.49, 16, 10.15.0.1, "LAN_IF",
10.1.1.11, 0.0.0.0, "LAN_DEV";
InterfaceTable 1 = 5, 10, 195.189.192.143, 25, 195.189.192.129, "WAN_IF",
80.179.55.100, 8.8.8.8, "WAN_DEV";

[ \InterfaceTable ]


[ WebUsers ]

FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password,
WebUsers_Status, WebUsers_PwAgeInterval, WebUsers_SessionLimit,
WebUsers_SessionTimeout, WebUsers_BlockTime, WebUsers_UserLevel,
WebUsers_PwNonce, WebUsers_SSHPublicKey;
WebUsers 0 = "Admin",
"$1$v9n5p/r18v31pvnx/an/qa2qteXht+Hl7u/g7rm967juudSCgYGChN+BjNjTidyL197Cl
ZORwszEk8/Ons7IxMs=", 1, 0, 2, 15, 60, 200,
"5df441ffbe5e92e7e573686f8fea3562", ".]♀ ";
WebUsers 1 = "User",
"$1$2bjrvevo6u7Z2dfS19fVht7bjNLe1NqLk8XEx8SXk5TIwZzLnpmcmzI2MjoxNjQ2bWo8O
TVrPDtyKHdxci1wIns=", 1, 0, 2, 15, 60, 50,
"9bc1106c693143ef05caccb0b6eafc95", ".]♀ ";

[ \WebUsers ]


[ TLSContexts ]

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

[ \TLSContexts ]


[ AudioCodersGroups ]
```

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

[ \AudioCodersGroups ]


[ IpProfile ]

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

```
IpProfile_SBCISUPBodyHandling, IpProfile_SBCISUPVariant,
IpProfile_SBCVoiceQualityEnhancement, IpProfile_SBCMaxOpusBW;
IpProfile 1 = "SWYX", 1, "", 0, 10, 10, 46, 24, 0, 0, 0, 2, 0, 0, 0, 0, -
1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", "", 0, 0, "", "", "", 0, 0, 0,
0, 0, 0, 8, 300, 400, 0, 0, 0, "", 0, 0, 1, 3, 0, 2, 2, 0, 0, 0, 1, 0, 1,
0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0, 0, 0,
0, 0, 0, 0, 0, 0;
IpProfile 2 = "DTAG", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0, 0,
0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "", "", 0, 0,
"", "", "", 0, 0, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, "", 0, 0, 1, 3, 0, 2,
2, 1, 3, 0, 0, 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, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1,
-1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0, 0;

[ \IpProfile ]


[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile,
CpMediaRealm_TopologyLocation;
CpMediaRealm 1 = "SWYX", "LAN_IF", "", 6000, 100, 6999, 0, "", "", 0;
CpMediaRealm 2 = "DTAG", "WAN_IF", "", 7000, 100, 7999, 0, "", "", 1;

[ \CpMediaRealm ]


[ SBCRoutingPolicy ]

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

[ \SBCRoutingPolicy ]


[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers,
SRD_EnableUnAuthenticatedRegistrations, SRD_SharingPolicy,
SRD_UsedByRoutingServer, SRD_SBCOperationMode, SRD_SBCRoutingPolicyName,
SRD_SBCDialPlanName;
SRD 1 = "defaultSRD", 0, -1, 1, 0, 0, 0, "defaultSBCRoutingPolicy", "";

[ \SRD ]


[ MessagePolicy ]

FORMAT MessagePolicy_Index = MessagePolicy_Name,
MessagePolicy_MaxMessageLength, MessagePolicy_MaxHeaderLength,
MessagePolicy_MaxBodyLength, MessagePolicy_MaxNumHeaders,
MessagePolicy_MaxNumBodies, MessagePolicy_SendRejection,
MessagePolicy_MethodList, MessagePolicy_MethodListType,
MessagePolicy_BodyList, MessagePolicy_BodyListType,
MessagePolicy_UseMaliciousSignatureDB;
```

```
MessagePolicy 0 = "Malicious Signature DB Protection", -1, -1, -1, -1, -
1, 1, "", 0, "", 0, 1;

[ \MessagePolicy ]


[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
SIPInterface_SRDName, SIPInterface_MessagePolicyName,
SIPInterface_TLSContext, SIPInterface_TLSMutualAuthentication,
SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,
SIPInterface_PreClassificationManSet, SIPInterface_EncapsulatingProtocol,
SIPInterface_MediaRealm, SIPInterface_SBCDirectMedia,
SIPInterface_BlockUnRegUsers, SIPInterface_MaxNumOfRegUsers,
SIPInterface_EnableUnAuthenticatedRegistrations,
SIPInterface_UsedByRoutingServer, SIPInterface_TopologyLocation;
SIPInterface 1 = "SWYX", "LAN_IF", 2, 5060, 0, 0, "defaultSRD", "",
"default", -1, 0, 500, -1, 0, "SWYX", 0, -1, -1, -1, 0, 0;
SIPInterface 2 = "DTAG", "WAN_IF", 2, 0, 5060, 0, "defaultSRD", "",
"default", -1, 0, 500, -1, 0, "DTAG", 0, -1, -1, -1, 0, 1;

[ \SIPInterface ]


[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap,
ProxySet_SRDName, ProxySet_ClassificationInput, ProxySet_TLSContextName,
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,
ProxySet_KeepAliveFailureResp, ProxySet_GWIPv4SIPInterfaceName,
ProxySet_SBCIPv4SIPInterfaceName, ProxySet_GWIPv6SIPInterfaceName,
ProxySet_SBCIPv6SIPInterfaceName, ProxySet_MinActiveServersLB,
ProxySet_SuccessDetectionRetries, ProxySet_SuccessDetectionInterval,
ProxySet_FailureDetectionRetransmissions;
ProxySet 1 = "SWYX", 1, 60, 0, 0, "defaultSRD", 0, "", -1, -1, "", "",
"SWYX", "", "", 1, 1, 10, -1;
ProxySet 2 = "DTAG", 1, 60, 0, 1, "defaultSRD", 0, "", 1, 1, "", "",
"DTAG", "", "", 1, 1, 10, -1;

[ \ProxySet ]


[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Name, IPGroup_ProxySetName,
IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_SipReRoutingMode,
IPGroup_AlwaysUseRouteTable, IPGroup_SRDName, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileName,
IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet, IPGroup_OutboundManSet,
IPGroup_RegistrationMode, IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IPGroup_SIPConnect, IPGroup_SBCPSAPMode,
IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer,
```

```
IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup_SBCRouteUsingRequestURIPort, IPGroup_SBCKeepOriginalCallID,
IPGroup_TopologyLocation, IPGroup_SBCDialPlanName,
IPGroup_CallSetupRulesSetId;
IPGroup 1 = 0, "SWYX", "SWYX", "sip-trunk.telekom.de", "", -1, 0,
"defaultSRD", "SWYX", 1, "SWYX", -1, -1, -1, 0, 0, "", 0, -1, 1, "",
"Admin", "$1$aCkNBwIC", 0, "", "", 0, "", "", 0, 0, "default", 0, 0, -1,
0, 0, 0, "", -1;
IPGroup 2 = 0, "DTAG", "DTAG", "sip-trunk.telekom.de", "", -1, 0,
"defaultSRD", "DTAG", 1, "DTAG", -1, -1, 0, 0, 0, "", 0, -1, -1, "",
"Admin", "$1$aCkNBwIC", 0, "", "", 0, "", "", 0, 0, "default", 0, 0, -1,
0, 0, 1, "", -1;

[ \IPGroup ]


[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex,
ProxyIp_IpAddress, ProxyIp_TransportType;
ProxyIp 1 = "1", 0, "10.15.27.3:5060", 0;
ProxyIp 3 = "2", 0, "register-test.sip-trunk.telekom.de", 1;

[ \ProxyIp ]


[ Account ]

FORMAT Account_Index = Account_ServedTrunkGroup,
Account_ServedIPGroupName, Account_ServingIPGroupName, Account_Username,
Account_Password, Account_HostName, Account_Register,
Account_ContactUser, Account_ApplicationType;
Account 0 = -1, "DTAG", "SWYX", "InteropTest", "$1$tIWHhYONjw==", "", 1,
"test1", 2;
Account 1 = -1, "SWYX", "DTAG", "AUDIOCODES-reg1",
"$1$rsyd4P/RhMLdwcDdiw==", "sip-trunk.telekom.de", 2, "+496987409354", 2;

[ \Account ]


[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_RoutingPolicyName, IP2IPRouting_SrcIPGroupName,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,
IP2IPRouting_RequestType, IP2IPRouting_MessageConditionName,
IP2IPRouting_ReRouteIPGroupName, IP2IPRouting_Trigger,
IP2IPRouting_CallSetupRulesSetId, IP2IPRouting_DestType,
IP2IPRouting_DestIPGroupName, IP2IPRouting_DestSIPInterfaceName,
IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup, IP2IPRouting_DestTags,
IP2IPRouting_SrcTags, IP2IPRouting_IPGroupSetName;
IP2IPRouting 10 = "SWYX-> DTAG", "defaultSBCRoutingPolicy", "SWYX", "*",
"*", "*", "*", 0, "", "Any", 0, -1, 0, "DTAG", "DTAG", "", 0, -1, 0, 0,
"", "", "", "";
IP2IPRouting 20 = "DTAG ->SWYX", "defaultSBCRoutingPolicy", "DTAG", "*",
"*", "*", "*", 0, "", "Any", 0, -1, 0, "SWYX", "SWYX", "", 0, -1, 0, 0,
"", "", "", "";
```

```
[ \IP2IPRouting ]


[ IPOutboundManipulation ]

FORMAT IPOutboundManipulation_Index =
IPOutboundManipulation_ManipulationName,
IPOutboundManipulation_RoutingPolicyName,
IPOutboundManipulation_IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupName,
IPOutboundManipulation_DestIPGroupName,
IPOutboundManipulation_SrcUsernamePrefix, IPOutboundManipulation_SrcHost,
IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_DestHost,
IPOutboundManipulation_CallingNamePrefix,
IPOutboundManipulation_MessageConditionName,
IPOutboundManipulation_RequestType,
IPOutboundManipulation_ReRouteIPGroupName,
IPOutboundManipulation_Trigger, IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_LeaveFromRight, IPOutboundManipulation_Prefix2Add,
IPOutboundManipulation_Suffix2Add,
IPOutboundManipulation_PrivacyRestrictionMode,
IPOutboundManipulation_DestTags, IPOutboundManipulation_SrcTags;
IPOutboundManipulation 0 = "source", "defaultSBCRoutingPolicy", 0,
"SWYX", "DTAG", "*", "*", "*", "*", "*", "", 0, "Any", 0, 0, 0, 0, 255,
"", "", 0, "", "";
IPOutboundManipulation 1 = "PBX-->ITSP", "defaultSBCRoutingPolicy", 0,
"SWYX", "DTAG", "*", "*", "00", "*", "*", "", 0, "Any", 0, 1, 2, 0, 255,
"+", "", 0, "", "";
IPOutboundManipulation 3 = "SIP Profile - ITSP",
"defaultSBCRoutingPolicy", 0, "SWYX", "DTAG", "*", "*", "0", "*", "*",
"", 0, "Any", 0, 1, 1, 0, 255, "+972", "", 0, "", "";

[ \IPOutboundManipulation ]

[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Reject Cause", 4, "any.response.5xx", "",
"header.request-uri.methodtype", 2, "'600'", 0;

[ \MessageManipulations ]


[ GwRoutingPolicy ]

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

[ \GwRoutingPolicy ]



[ ResourcePriorityNetworkDomains ]
```

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

[ \ResourcePriorityNetworkDomains ]


[ DialPlanRule ]

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

[ \DialPlanRule ]


[ MaliciousSignatureDB ]

FORMAT MaliciousSignatureDB_Index = MaliciousSignatureDB_Name,
MaliciousSignatureDB_Pattern;
MaliciousSignatureDB 0 = "SIPVicious", "Header.User-Agent.content prefix
'friendly-scanner'";
MaliciousSignatureDB 1 = "SIPScan", "Header.User-Agent.content prefix
'sip-scan'";
MaliciousSignatureDB 2 = "Smap", "Header.User-Agent.content prefix
'smap'";
MaliciousSignatureDB 3 = "Sipsak", "Header.User-Agent.content prefix
'sipsak'";
MaliciousSignatureDB 4 = "Sipcli", "Header.User-Agent.content prefix
'sipcli'";
MaliciousSignatureDB 5 = "Sivus", "Header.User-Agent.content prefix
'SIVuS'";
MaliciousSignatureDB 6 = "Gulp", "Header.User-Agent.content prefix
'Gulp'";
MaliciousSignatureDB 7 = "Sipv", "Header.User-Agent.content prefix
'sipv'";
MaliciousSignatureDB 8 = "Sundayddr Worm", "Header.User-Agent.content
prefix 'sundayddr'";
MaliciousSignatureDB 9 = "VaxIPUserAgent", "Header.User-Agent.content
prefix 'VaxIPUserAgent'";
MaliciousSignatureDB 10 = "VaxSIPUserAgent", "Header.User-Agent.content
prefix 'VaxSIPUserAgent'";
MaliciousSignatureDB 11 = "SipArmyKnife", "Header.User-Agent.content
prefix 'siparmyknife'";

[ \MaliciousSignatureDB ]


[ AudioCoders ]
```

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

[ \AudioCoders ]
```

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

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

Contact us: www.audiocodes.com/info
Website: www.audiocodes.com

Document #: LTRT-12760

AudioCodes