

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

Version 7.2



Table of Contents

1	Introduction	7
1.1	Intended Audience	7
1.2	About AudioCodes SBC Product Series	7
2	Component Information.....	9
2.1	AudioCodes SBC Version.....	9
2.2	DTAG SIP Trunking Version.....	9
2.3	SWYX IP-PBX Version	9
2.4	Interoperability Test Topology	10
2.4.1	Environment Setup	11
2.4.2	Known Limitations.....	11
3	Configuring SwyxWare 2015 Server.....	13
3.1	Configuring AudioCodes E-SBC Trunk on SwyxWare 2015 Server	13
4	Configuring AudioCodes SBC	23
4.1	IP Network Interfaces Configuration	23
4.1.1	Configure VLANs	24
4.1.2	Configure Network Interfaces	25
4.2	Configure Media Realms	26
4.3	Configure SIP Signaling Interfaces	27
4.4	Configure Proxy Sets and Proxy Address	28
4.4.1	Configure a Proxy Address.....	29
4.5	Configure Coders	31
4.6	Configure IP Profiles.....	33
4.7	Configure IP Groups.....	36
4.8	Configure IP-to-IP Call Routing Rules	38
4.9	Configure Number Manipulation Rules	39
4.10	Configure Message Manipulation Rules	40
4.11	Configure Registration Accounts	51
4.12	Miscellaneous Configuration.....	52
4.12.1	DTMF Interworking for Fax and Modem.....	52
4.12.2	Optimizing CPU Cores Usage for a Specific Service (relevant for Mediant 9000 and Software SBC only)	53
A	AudioCodes INI File	55

This page is intentionally left blank.

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from <https://www.audiocodes.com/library/technical-documents>.

This document is subject to change without notice.

Date Published: November-24-2019

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 website at <https://www.audiocodes.com/services-support/maintenance-and-support>.

Stay in the Loop with AudioCodes



Abbreviations and Terminology

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

Document Revision Record

LTRT	Description
12760	Initial document release for Version 7.2.
12761	Updated according to the latest implementation changes.

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://online.audiocodes.com/doc-feedback>.

This page is intentionally left blank.

1 Introduction

This Configuration Note describes how to set up the AudioCodes Enterprise Session Border Controller (hereafter, referred to as *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 SBC based on this interoperability setup. However, it is recommended to read through this document to better understand the various configuration options. For more information on AudioCodes' SBC Wizard including the download option, visit AudioCodes Web site at <https://www.audiocodes.com/partners/sbc-interoperability-list>.

1.1 Intended Audience

This 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 SBC.

1.2 About AudioCodes SBC Product Series

AudioCodes' family of SBC devices enables reliable connectivity and security between the Enterprise's 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 platforms, or as a software-only solution for deployment with third-party hardware. The SBC can be offered as a Virtualized SBC, supporting the following platforms: Hyper-V, AWS, AZURE, AWP, KVM and VMWare.

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 Gateway & E-SBC ▪ Mediant 500L Gateway & E-SBC ▪ Mediant 800B Gateway & E-SBC ▪ Mediant 800C Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 SBC ▪ Mediant 4000B SBC ▪ Mediant 9000 SBC ▪ Mediant 9030 SBC ▪ Mediant 9080 SBC ▪ Mediant Software SBC (VE/SE/CE)
Software Version	7.20A.254.202 or later
Protocol	▪ SIP/TCP (to the DTAG SIP Trunk) ▪ SIP/UDP (to the SWYX IP-PBX)
Additional Notes	None

2.2 DTAG SIP Trunking Version

Table 2-2: DTAG 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	None

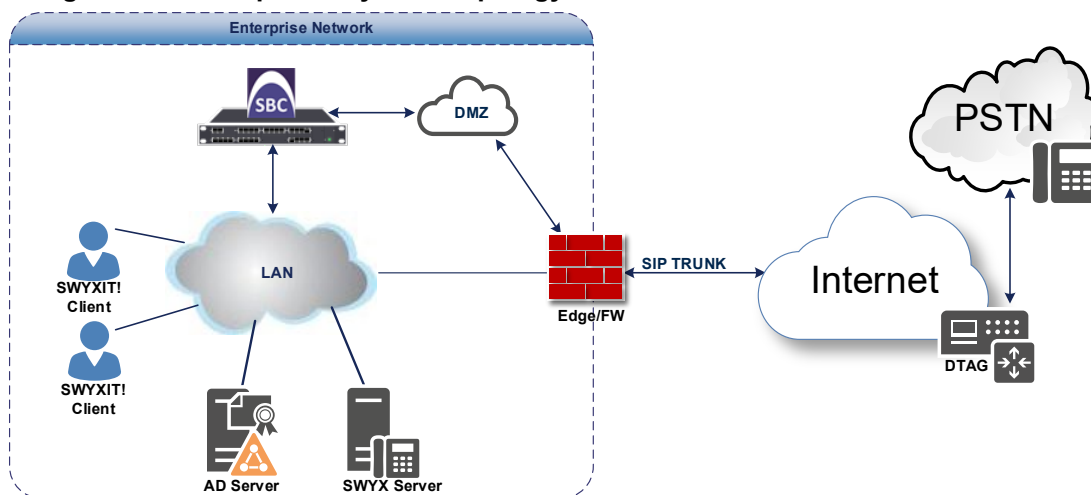
2.4 Interoperability Test Topology

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 4.10 on page 40).

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.

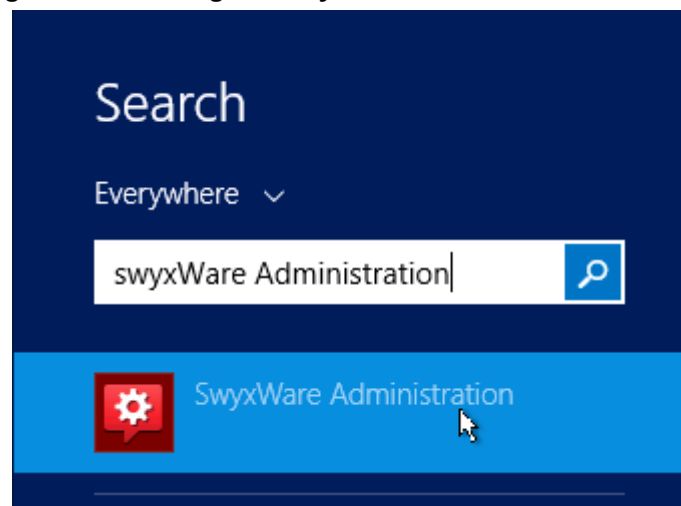
3.1 Configuring AudioCodes E-SBC Trunk on SwyxWare 2015 Server

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

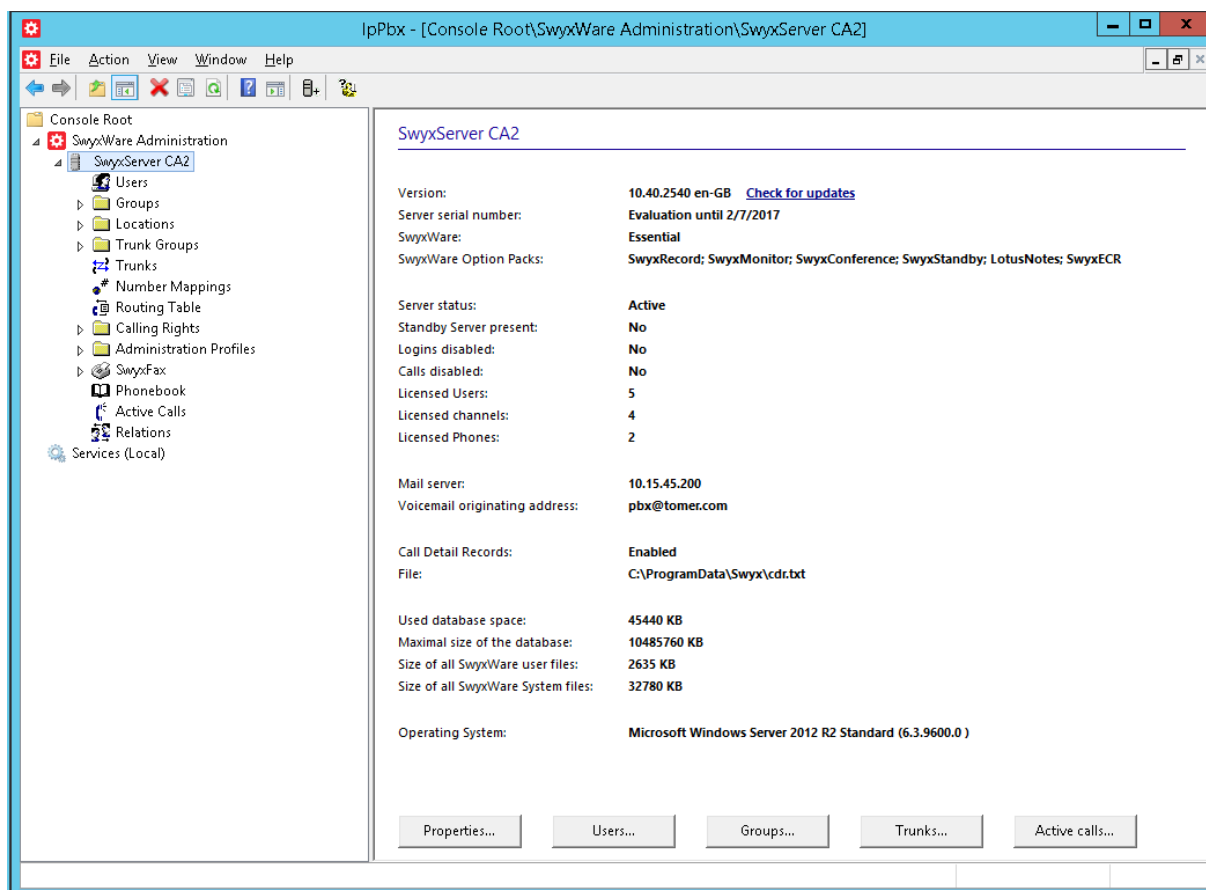
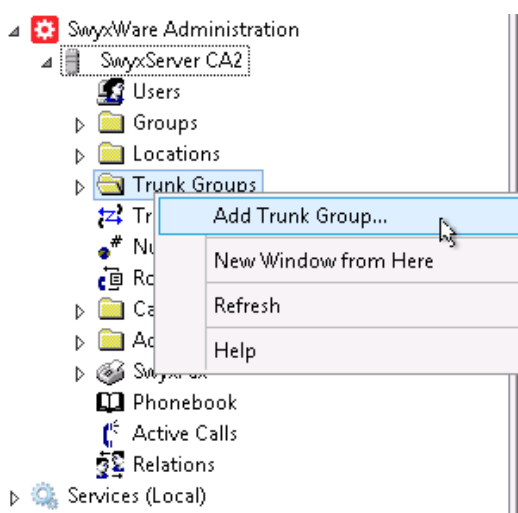


Figure 3-3: Add Trunk Group Dialog Box



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

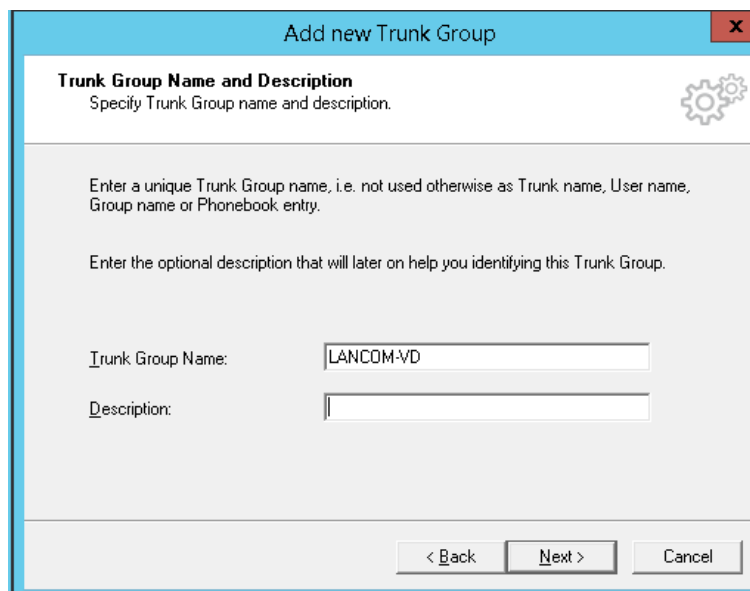
The Trunk Group wizard is displayed:

Figure 3-4: Trunk Group Wizard



3. Click **Next**.

Figure 3 6: Add LANCOM-VD Trunk Group Name



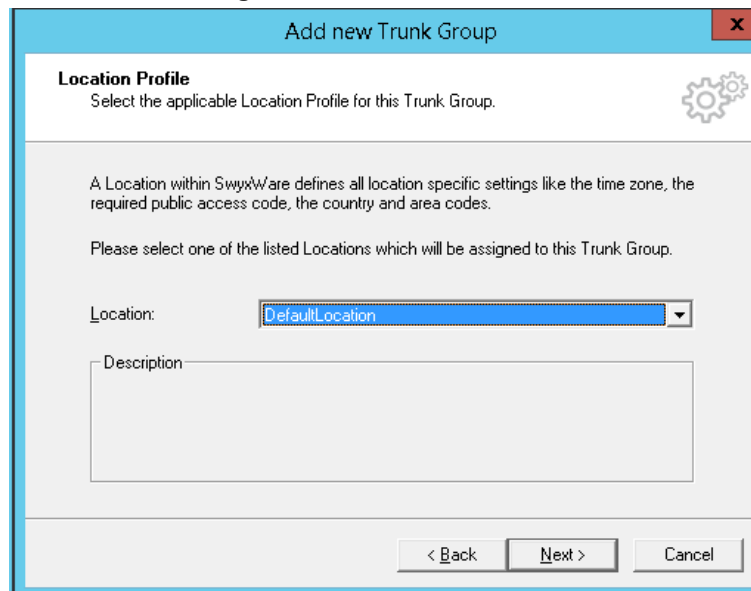
4. Under the **Trunk Group Name** write descriptive name (for e.g., **LANCOM-VD**) and then click **Next**.

Figure 3-5: Define the Trunk Group

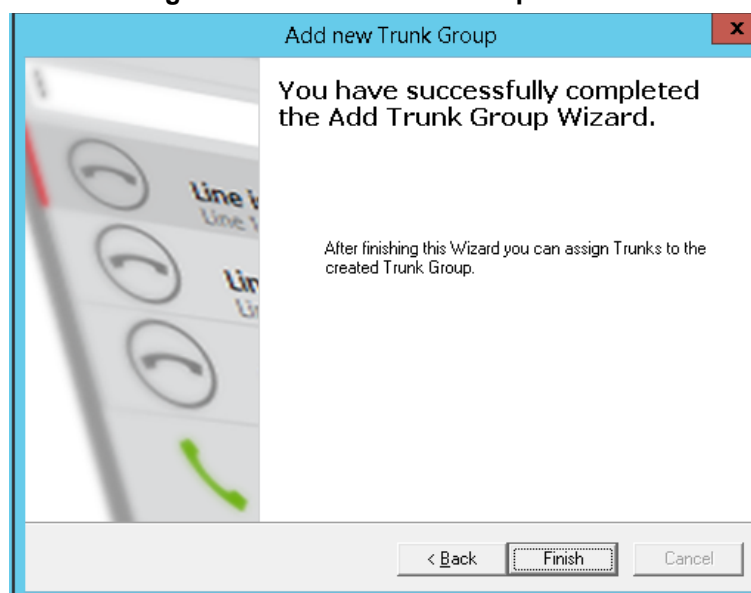
5. Under Trunk Group Type choose **SIP Gateway**
6. Under Profile choose **Lancom VD**
7. Click **Next**

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:

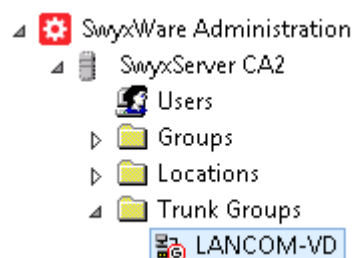
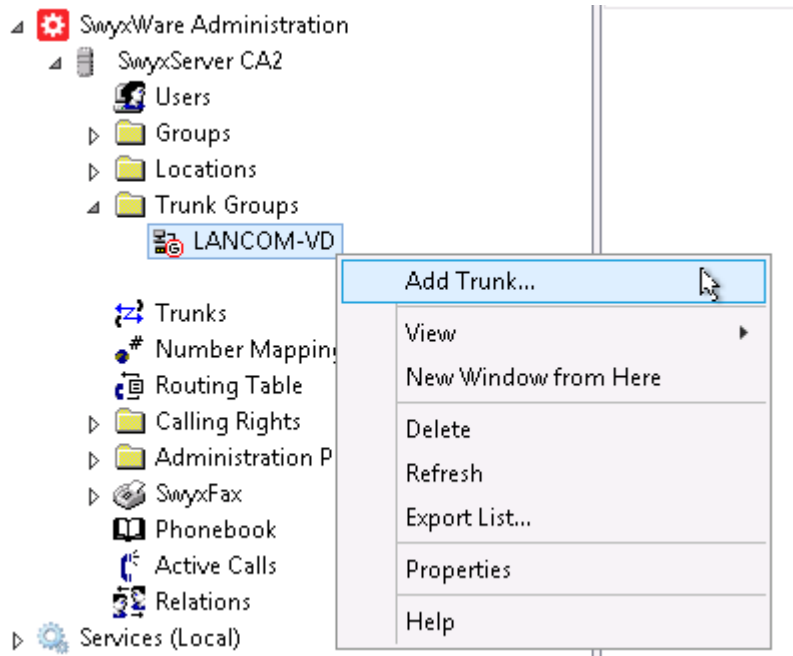
Figure 3-9: LANCOM-VD added as Trunk Group

Figure 3-10: Add Trunk



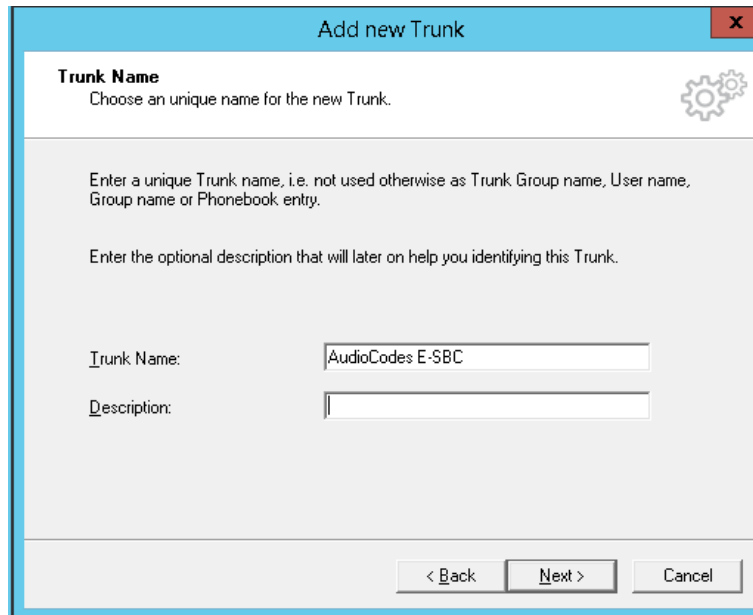
11. Select the created trunk group (LANCOM-VD), right-click it to **Add Trunk**

The Trunk wizard is displayed:

Figure 3-11: Trunk Wizard



12. Click **Next**.

Figure 3 6: Add AudioCodes E-SBC Trunk Name

Add new Trunk

Trunk Name
Choose an unique name for the new Trunk.

Enter a unique Trunk name, i.e. not used otherwise as Trunk Group name, User name, Group name or Phonebook entry.

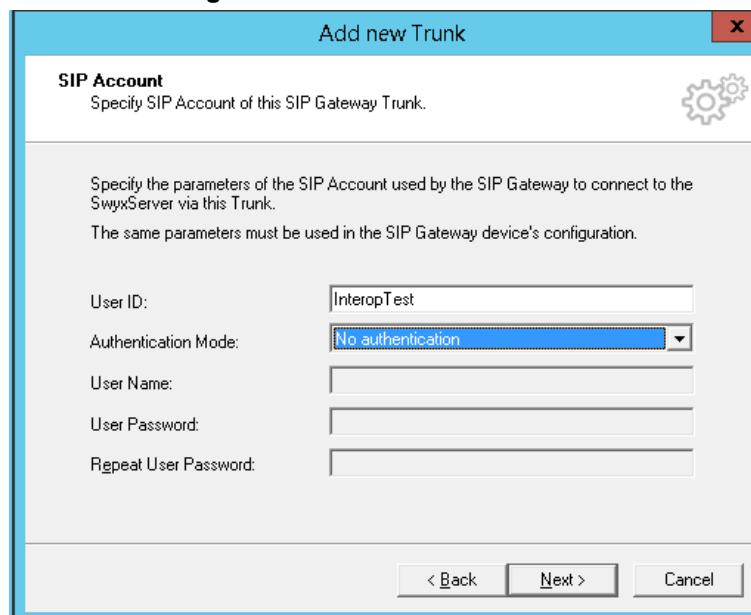
Enter the optional description that will later on help you identifying this Trunk.

Trunk Name: AudioCodes E-SBC

Description:

< Back Next > Cancel

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

Figure 3-12: Define SIP Account

Add new Trunk

SIP Account
Specify SIP Account of this SIP Gateway Trunk.

Specify the parameters of the SIP Account used by the SIP Gateway to connect to the SwyxServer via this Trunk.
The same parameters must be used in the SIP Gateway device's configuration.

User ID: InteropTest

Authentication Mode: No authentication

User Name:

User Password:

Repeat User Password:

< Back Next > Cancel

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

Subscriber Numbers
Specify Subscriber Numbers.

Enter the subscriber number part of the Public Numbers that are terminated by this Trunk.
If your set of subscriber numbers is incoherent enter only the first subscriber number and add the other subscriber numbers later via the Trunk's properties.
If this Trunk does not add any Public Numbers to the system, leave all fields empty and click 'Next'.
Note: Country Code and Area Code have been pre-determined by the Trunk Group's location.

Country Code	Area Code	First Subscriber Number	Last Subscriber Number
49	69	8740935401	8740935409

< Back Next > Cancel

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

Codecs
Select the codecs to be used for data transmission.

The selected codec filter defines the type of compression for calls using this Trunk. Therefore the selected codec has an impact on the used bandwidth and the quality of the call.

Codecs Preference and Filter

Prefer Quality

- ☒ G.722 (approx. 84 kBit/s per call)
- ☒ G.711a (approx. 84 kBit/s per call)
- ☒ G.711μ (approx. 84 kBit/s per call)
- ☒ G.729 (approx. 24 kBit/s per call)
- ☒ Fax over IP (T.38, approx. 20 kBit/s per call)

< Back Next > Cancel

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

Figure 3-15: Define Number of Channels

Add new Trunk

Number of Channels
Select number of Channels to be used by this Trunk.

The number of concurrent calls via a specific Trunk is usually limited by the Trunk's physics, the available bandwidth or by a provider limitation.

Furthermore the number of simultaneous calls can artificially be limited to reserve (e.g. ISDN) channels or bandwidth for other applications.

Usually ISDN BRI interfaces would allow to make up to 2 simultaneous calls, while ISDN PRI interfaces allow up to 30 calls.

Number of simultaneous calls on this Trunk:

< Back Next > Cancel

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

Figure 3-16: Finish Trunk Wizard

Add new Trunk

Computer Name
Define the computer name where the Trunk is hosted.

The Trunk may be hosted on another computer than the SwyxServer. In this case, the computer name must be provided here, otherwise keep the proposed default.

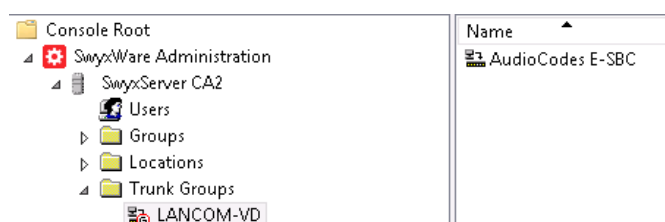
Please enter the computer name as it is given in the Windows Server's system properties.

Computer Name:

< Back Finish Cancel

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 SBC

This section provides step-by-step procedures on how to configure AudioCodes SBC for interworking between SWYX IP-PBX and the 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:

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

This configuration is done using the 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.

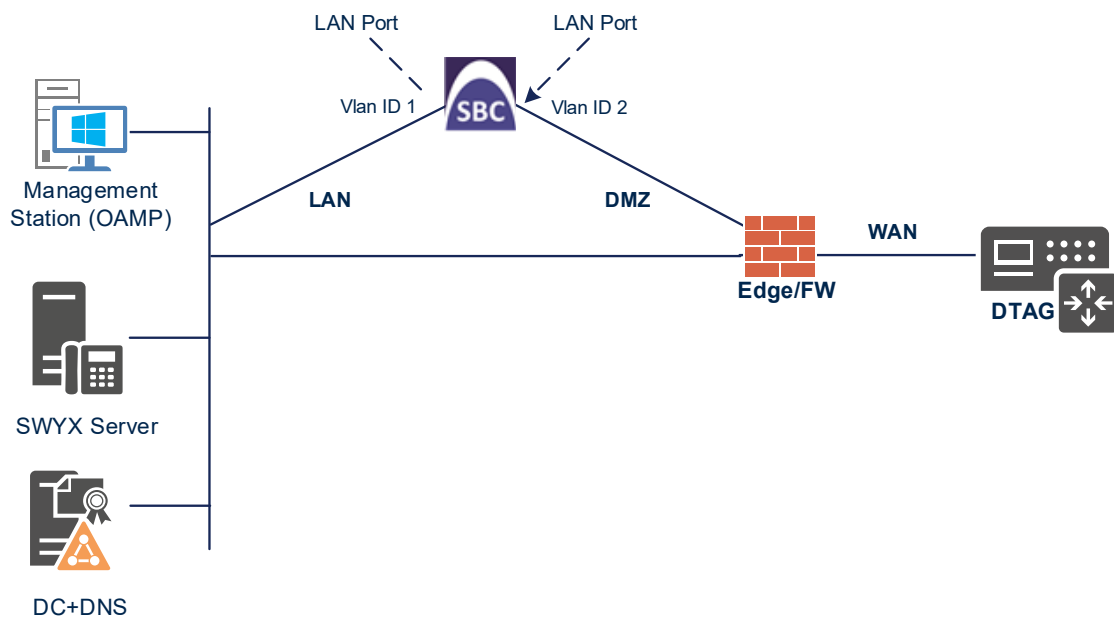
- The scope of this interoperability test and document does **not** cover all security aspects for connecting the SIP Trunk to the SWYX IP-PBX environment. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products,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

4.1 IP Network Interfaces Configuration

This section describes how to configure the SBC's IP network interfaces. There are several ways to deploy the 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 Configure VLANs

This section describes how to configure 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**).
2. There will be one existing row for VLAN ID 1 and underlying interface GROUP_1.
3. Add another VLAN ID 2 for the WAN side

Figure 4-2: Configured VLAN IDs in Ethernet Device

Ethernet Devices (2)				
+ New Edit Page 1 of 1 Show 10 records per page				
INDEX	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING
0	1	GROUP_1	vlan 1	Untagged
1	2	GROUP_2	vlan 2	Untagged

4.1.2 Configure Network Interfaces

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

- LAN Interface (assigned the name "LAN_IF")
- WAN Interface (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. Configure the IP interfaces as follows (your network parameters might be different):

Table 4-1: Configuration Example of the Network Interface Table

Index	Application Types	Interface Mode	IP Address	Prefix Length	Gateway	DNS	I/F Name	Ethernet Device
0	OAMP+ Media + Control	IPv4 Manual	10.15.77.77	16	10.15.0.1	10.15.27.1	LAN_IF	vlan 1
1	Media + Control (as this interface points to the internet, enabling OAMP is not recommended)	IPv4 Manual	195.189.192.157 (DMZ IP address of SBC)	25	195.189.192.129 (router's IP address)	According to your Internet provider's instructions	WAN_IF	vlan 2

The configured IP network interfaces are shown below:

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

INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	LAN_IF	OAMP + Media +	IPv4 Manual	10.15.17.77	16	10.15.0.1	10.15.27.1	0.0.0.0	vlan 1
1	WAN_IF	Media + Control	IPv4 Manual	195.189.192.157	25	195.189.192.129	80.179.52.100	80.179.55.100	vlan 2

4.2 Configure Media Realms

This section describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for the SIP Trunk traffic and one for the SWYX IP-PBX traffic.

➤ **To configure Media Realms:**

1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Configure Media Realms as follows (you can use the default Media Realm (Index 0), but modify it):

Table 4-2: Configuration Example Media Realms in Media Realm Table

Index	Name	Topology Location	IPv4 Interface Name	Port Range Start	Number of Media Session Legs
0	SWYX (arbitrary name)		LAN_IF	6000	100 (media sessions assigned with port range)
1	DTAG (arbitrary name)	Up	WAN_IF	7000	100 (media sessions assigned with port range)

The configured Media Realms are shown in the figure below:

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

Media Realms (2)						
+ New Edit 🗑️ ⏪ ⏩ Page 1 of 1 Show 10 records per page						
INDEX	NAME	IPv4 INTERFACE NAME	UDP PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	UDP PORT RANGE END	DEFAULT MEDIA REALM
0	SWYX	LAN_IF	6000	100	6999	No
1	DTAG	WAN_IF	7000	100	7999	No

4.3 Configure SIP Signaling Interfaces

This section describes how to configure SIP Interfaces. For the interoperability test topology, towards the SIP Trunk and towards the SWYX IP-PBX SIP Interfaces must be configured for the SBC.

➤ **To configure SIP Interfaces:**

1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
2. Configure SIP Interfaces. You can use the default SIP Interface (Index 0), but modify it as shown in the table below. The table below shows an example of the configuration. You can change some parameters according to your requirements.

Table 4-3: Configured SIP Interfaces in SIP Interface Table

Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Classification Failure Response Type	Media Realm
0	SWYX (arbitrary name)	LAN_IF	SBC	5060 (according to Service Provider requirement)	0	0	500 (leave default value)	SWYX
1	DTAG (arbitrary name)	WAN_IF	SBC	0	5060 (according to Service Provider requirement)	0	0 (Recommended to prevent DoS attacks)	DTAG

The configured SIP Interfaces are shown in the figure below:

Figure 4-5: Configured SIP Interfaces in SIP Interface Table

SIP Interfaces (2)									
+ New Edit 🗑 Page 1 of 1 Show 10 records per page									
INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATION PROTOCOL	MEDIA REALM
0	SWYX	DefaultSRD	LAN_IF	SBC	5060	0	0	No encapsulation	SWYX
1	DTAG	DefaultSRD	WAN_IF	SBC	0	5060	0	No encapsulation	DTAG

4.4 Configure Proxy Sets and Proxy Address

This section 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 Trunk

The Proxy Sets will later be applied 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. Configure Proxy Sets as shown in the table below:

Table 4-4: Configuration Example Proxy Sets in Proxy Sets Table

Index	Name	SBC IPv4 SIP Interface	Proxy Keep-Alive	Redundancy Mode	Proxy Hot Swap	DNS Resolve Method
1	SWYX (arbitrary name)	SWYX	Using Options		-	-
2	DTAG (arbitrary name)	DTAG	Using Options	Homing	Enable	SRV

The configured Proxy Sets are shown in the figure below:

Figure 4-6: Configured Proxy Sets in Proxy Sets Table

Proxy Sets (3)							
+ New Edit 🗑️ ⏪ ⏩ Page 1 of 1 Show 10 records per page							
INDEX	NAME	SRD	GATEWAY IPV4 SIP INTERFACE	SBC IPV4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	ProxySet_0	DefaultSRD (#0)	--	SWYX	60		Disable
1	SWYX	DefaultSRD (#0)	--	SWYX	60		Disable
2	DTAG	DefaultSRD (#0)	--	DTAG	60	Homing	Enable

4.4.1 Configure a Proxy Address

This section shows how to configure a Proxy Address.

➤ **To configure a Proxy Address for IP-PBX:**

1. Open the Proxy Sets table (Setup menu > Signaling & Media tab > Core Entities folder > Proxy Sets) and then click the Proxy Set **SWYX**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
2. Click **+New**; the following dialog box appears:

Figure 4-7: Configuring Proxy Address for SwyxWare IP-PBX

The screenshot shows a 'Proxy Address' configuration window. It has a title bar with the text 'Proxy Address' and standard window controls. Below the title bar is a tab labeled 'GENERAL'. The configuration fields are as follows:

- Index:** A text field containing the value '0'.
- Proxy Address:** A text field containing the value '10.50.252.102:5060'.
- Transport Type:** A dropdown menu with 'UDP' selected.
- Proxy Priority:** A text field containing the value '0'.
- Proxy Random Weight:** A text field containing the value '0'.

3. Configure the address of the Proxy Set according to the parameters described in the table below:

Table 4-5: Configuration Proxy Address for SwyxWare Server 2015

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	10.50.252.102:5060 (SwyxWare IP-PBX IP address and destination port)	UDP	0	0

4. Click **Apply**.

➤ **To configure a Proxy Address for SIP Trunk:**

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**) and then click the Proxy Set **DTAG**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
2. Click **+New**; the following dialog box appears:

Figure 4-8: Configuring Proxy Address for DTAG SIP Trunk

The screenshot shows a 'Proxy Address' configuration window. It has a title bar with a minus, maximize, and close button. Below the title bar is a 'GENERAL' tab. The configuration fields are as follows:

Field	Value
Index	0
Proxy Address	reg.sip-trunk.telekom.de
Transport Type	TCP
Proxy Priority	0
Proxy Random Weight	0

3. Configure the address of the Proxy Set according to the parameters described in the table below:

Table 4-6: Configuration Proxy Address for DTAG SIP Trunk

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	reg.sip-trunk.telekom.de	TCP	0	0

4. Click **Apply**.

4.5 Configure Coders

This section describes how to configure coders (termed *Coder Group*). As SWYX IP-PBX supports the list of the coders while the network connection to DTAG SIP Trunk may restrict operation with a dedicated coders list, you need to add a Coder Group with the supported coders for each leg, the SWYX IP-PBX and the DTAG SIP Trunk.

Note that the Coder Group ID for this entity will be assigned to its corresponding IP Profile in the next step.

➤ **To configure coders:**

1. Open the Coder Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Coder Groups**).
2. Configure Extension Coder Group:

Parameter	Value
Coder Group Name	AudioCodersGroups_0
Coder Name	▪ G.711 A-law ▪ G.711 U-law

Figure 4-9: Configuring Extension Coder Group

Coder Groups

Coder Group Name 0 : AudioCodersGroups_0 Delete Group

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression	Coder Specific
G.711A-law ▼	20 ▼	64 ▼	8	Disabled ▼	
G.711U-law ▼	20 ▼	64 ▼	0	Disabled ▼	
▼	▼	▼		▼	

3. Click **Apply**, and then confirm the configuration change in the prompt that pops up.

The procedure below describes how to configure an Allowed Coders Group to ensure that voice sent to the DTAG SIP Trunk uses the dedicated coders list whenever possible. Note that this Allowed Coders Group ID will be assigned to the IP Profile belonging to the DTAG SIP Trunk in the next step.

➤ **To set a preferred coder for the DTAG SIP Trunk:**

1. Open the Allowed Audio Coders Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Allowed Audio Coders Groups**).
2. Click **New** and configure a name for the Allowed Audio Coders Group for DTAG SIP Trunk.

Figure 4-10: Configuring Allowed Coders Group for DTAG SIP Trunk

Allowed Audio Coders Groups [Telekom]

GENERAL

Index
0

Name
Telekom

3. Click **Apply**.
4. Select the new row that you configured, and then click the **Allowed Audio Coders** link located below the table; the Allowed Audio Coders table opens.
5. Click **New** and configure an Allowed Coders as follows:

Parameter	Value
Index	0
Coder	G.711 A-law
Index	1
Coder	G.711 U-law

Figure 4-11: Configuring Allowed Coders for DTAG SIP Trunk

Allowed Audio Coders Groups [#0] > Allowed Audio Coders (2)

+ New Edit

Page 1 of 1 Show 10 records per page

INDEX	CODER	USER-DEFINED CODER
0	G.711 A-law	
1	G.711 U-law	

4.6 Configure IP Profiles

This section 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 an IP Profile for the SWYX IP-PBX:**

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Click **New**, and then configure the parameters as follows:

Parameter	Value
General	
Index	1
Name	SWYX
SBC Early Media	
Remote Early Media RTP Detection Mode	By Media
SBC Media	
Extension Coders Group	AudioCodersGroups_0
Allowed Audio Coders	Telekom
Allowed Coders Mode	Preference (lists Allowed Coders first and then original coders in received SDP offer)
RFC 2833 Mode	Disallow
Alternative DTMF Method	INFO - Cisco
SBC Signaling	
PRACK Mode	Optional
P-Asserted-Identity Header Mode	Add (required for anonymous calls)
Remote Update Support	Not Supported
Remote re-INVITE Support	Supported Only With SDP
Remote Delayed Offer Support	Not Supported
SBC Forward and Transfer	
Remote REFER Mode	Handle Locally
Remote 3xx Mode	Handle Locally

Figure 4-12: Configuring IP Profile for SWYX IP-PBX

3. Click **Apply**.

➤ **To configure IP Profile for the DTAG SIP Trunk:**

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Click **New**, and then configure the parameters as follows:

Parameter	Value
General	
Index	2
Name	DTAG (arbitrary descriptive name)
SBC Early Media	
Remote Multiple 18x	Not Supported
SBC Media	
Extension Coders Group	AudioCodersGroups_0
Allowed Audio Coders	Telekom
Allowed Coders Mode	Preference (lists Allowed Coders first and then original coders in received SDP offer)
RFC 2833 Mode	Extend
RFC 2833 DTMF Payload Type	102
Alternative DTMF Method	In Band
SBC Signaling	
P-Asserted-Identity Header Mode	Add (required for anonymous calls)
Diversion Header Mode	Remove

History-Info Header Mode	Remove
SBC Forward and Transfer	
Remote REFER Mode	Handle Locally
SBC Hold	
Remote Hold Format	Send Only

Figure 4-13: Configuring IP Profile for DTAG SIP Trunk

The screenshot shows the 'IP Profiles [DTAG]' configuration window. It has three main sections: GENERAL, MEDIA SECURITY, and SBC SIGNALING. The GENERAL section includes fields for Index (2), Name (DTAG), and Created by Routing Server (No). The MEDIA SECURITY section includes dropdowns for SBC Media Security Mode (As Is), Gateway Media Security Mode (Preferable), Symmetric MKI (Disable), MKI Size (0), SBC Enforce MKI Size (Don't enforce), SBC Media Security Method (SDES), and Reset SRTP Upon Re-key (Disable). The SBC SIGNALING section includes dropdowns for PRACK Mode (Transparent), P-Asserted-Identity Header Mode (Add), Diversion Header Mode (Remove), History-Info Header Mode (Remove), Session Expires Mode (Transparent), SIP UPDATE Support (Supported), Remote re-INVITE (Supported), Remote Delayed Offer Support (Supported), MSRP re-INVITE/UPDATE (Supported), MSRP Offer Setup Role (ActPass), MSRP Empty Message Format (Default), and Remote Representation Mode (According to Operation Mode). At the bottom, there are 'Cancel' and 'APPLY' buttons.

3. Click **Apply**.

4.7 Configure IP Groups

This section describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the SBC communicates. This can be a server (e.g., IP PBX or ITSP) or 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. 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. Configure an IP Group for the SWYX IP-PBX:

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. Configure an IP Group for the DTAG SIP Trunk:

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 4-14: Configured IP Groups in IP Group Table

IP Groups (3)

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

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATION SET	OUTBOUND MESSAGE MANIPULATION SET
0	Default_IPG	 DefaultSRD	Server	Not Configured	ProxySet_0	--	--		Disable	-1	-1
1	SWYX	 DefaultSRD	Server	Not Configured	SWYX	SWYX	SWYX	sip-trunk.tele	Enable	-1	-1
2	DTAG	 DefaultSRD	Server	Not Configured	DTAG	DTAG	DTAG	sip-trunk.tele	Enable	-1	-1

4.8 Configure IP-to-IP Call Routing Rules

This section describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, 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.

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between SWYX IP-PBX and DTAG SIP Trunk:

- Terminate SIP OPTIONS messages on the SBC that are received from any entity
- Calls from SWYX IP-PBX to DTAG SIP Trunk
- Calls from DTAG SIP Trunk to SWYX IP-PBX

➤ To configure IP-to-IP routing rules:

1. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. Configure routing rules as shown in the table below:

Table 4-7: Configuration IP-to-IP Routing Rules

Index	Name	Source IP Group	Request Type	Call Trigger	ReRoute IP Group	Dest Type	Dest IP Group	Dest Address
0	Terminate OPTIONS	Any	OPTIONS			Dest Address		internal
1	SWYX -> DTAG (arbitrary name)	SWYX				IP Group	DTAG	
2	DTAG -> SWYX (arbitrary name)	DTAG				IP Group	SWYX	

The configured routing rules are shown in the figure below:

Figure 4-15: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

IP-to-IP Routing (3)											
+ New Edit Insert Page 1 of 1 Show 10 records per page											
INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PATTERN	DESTINATION USERNAME PATTERN	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	Terminate O	Default_SBC	Route Row	Any	OPTIONS	*	*	Dest Address:	--	--	internal
1	SWYX -> DTA	Default_SBC	Route Row	SWYX	All	*	*	IP Group	DTAG	--	
2	DTAG -> SWY	Default_SBC	Route Row	DTAG	All	*	*	IP Group	SWYX	--	



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

4.9 Configure Number Manipulation Rules

This section 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 4.7 on page 30) to denote the source and destination of the call.



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

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. Configure the rules according to your setup.

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

Figure 4-16: Example of Configured IP-to-IP Outbound Manipulation Rules

Outbound Manipulations (2)													
+ New		Edit	Insert	↑	↓	🗑️	Page 1 of 1		»	«	Show 10 records per page		
INDEX	NAME	ROUTING POLICY	ADDITION/ MANIPULA	SOURCE IP GROUP	DESTINATI IP GROUP	SOURCE USERNAME PATTERN	DESTINATI USERNAME PATTERN	MANIPULA ITEM	REMOVE FROM LEFT	REMOVE FROM RIGHT	LEAVE FROM RIGHT	PREFIX TO ADD	SUFFIX TO ADD
0	SWYX->DTA	Default_SB	No	SWYX	DTAG	*	*	Source URI	0	0	255	+	
1	SWYX->DTA	Default_SB	No	SWYX	DTAG	*	00	Destination	2	0	255	+	

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.

4.10 Configure Message Manipulation Rules

This section 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 0) 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	0
Condition	Any.Response.5xx
Action Subject	Header.Request-URI.MethodType
Action Type	Modify
Action Value	'600'

Figure 4-17: Configuring SIP Message Manipulation Rule 0 (for DTAG SIP Trunk)

Message Manipulations [Reject Cause]

GENERAL		ACTION	
Index	0	Action Subject	Header.Request-URI.MethodType Editor
Name	Reject Cause	Action Type	Modify
Manipulation Set ID	0	Action Value	'600' Editor
Row Role	Use Current Condition		

MATCH	
Message Type	Any.Response.5xx Editor
Condition	Editor

Cancel **APPLY**

3. Configure another manipulation rule (Manipulation Set 0) for DTAG SIP Trunk. This rule is applied to INVITE request messages sent to the DTAG SIP Trunk IP. This rule remove SIP P-Preferred-Identity Header, if it's exists.

Parameter	Value
Index	1
Name	Remove P-Preferred
Manipulation Set ID	0
Message Type	Invite.Request
Condition	Header.P-Preferred-Identity exists
Action Subject	Header.P-Preferred-Identity
Action Type	Remove

Figure 4-18: Configuring SIP Message Manipulation Rule 1 (for DTAG SIP Trunk)

Message Manipulations [Remove P-Preferred]

GENERAL

Index: 1

Name: Remove P-Preferred

Manipulation Set ID: 0

Row Role: Use Current Condition

ACTION

Action Subject: Header.P-Preferred-Identity

Action Type: Remove

Action Value:

MATCH

Message Type: Invite.Request

Condition: Header.P-Preferred-Identity exists

Cancel APPLY

4. Configure another manipulation rule (Manipulation Set 1) for SWYX IP-PBX. This rule is applied to INVITE request messages received from the SWYX IP-PBX. This replace the user part of the SIP From Header with the value from the P-Asserted-Identity Header, if it's exists.

Parameter	Value
Index	2
Name	map PAI to From
Manipulation Set ID	1
Message Type	Invite.Request
Condition	Header.P-Asserted-Identity.0 exists
Action Subject	Header.From.URL.User
Action Type	Modify
Action Value	Header.P-Asserted-Identity.0.URL.User

Figure 4-19: Configuring SIP Message Manipulation Rule 2 (for SWYX IP-PBX)

Message Manipulations [map PAI to From]

GENERAL

Index
Name •
Manipulation Set ID •
Row Role

ACTION

Action Subject • [Editor](#)
Action Type •
Action Value • [Editor](#)

MATCH

Message Type • [Editor](#)
Condition • [Editor](#)

Cancel

APPLY

5. Configure another manipulation rule (Manipulation Set 1) for SWYX IP-PBX. This rule is applied to INVITE request messages received from the SWYX IP-PBX. This remove the second index of the SIP P-Asserted-Identity Header, if it's exists.

Parameter	Value
Index	3
Name	Remove second PAI if exists
Manipulation Set ID	1
Message Type	Invite.Request
Condition	Header.P-Asserted-Identity.1 exists
Action Subject	Header.P-Asserted-Identity.1
Action Type	Remove

Figure 4-20: Configuring SIP Message Manipulation Rule 3 (for SWYX IP-PBX)

Message Manipulations [Remove second PAI if exists]

GENERAL

Index: 3

Name: Remove second PAI if exists

Manipulation Set ID: 1

Row Role: Use Current Condition

ACTION

Action Subject: Header.P-Asserted-Identity.1

Action Type: Remove

Action Value:

MATCH

Message Type: Invite.Request

Condition: Header.P-Asserted-Identity.1 exists

Cancel APPLY

6. Configure another manipulation rule (Manipulation Set 2) for SWYX IP-PBX. This rule is applied to INVITE request messages sent to the SWYX IP-PBX. This replace the user part of the SIP Contact Header with value 'SipGwTrunk', if it's not equal to it already.

Parameter	Value
Index	4
Name	Contact correction
Manipulation Set ID	2
Message Type	Invite.Request
Condition	Header.Contact.URL.User != 'SipGwTrunk'
Action Subject	Header.Contact.URL.User
Action Type	Modify
Action Value	'SipGwTrunk'

Figure 4-21: Configuring SIP Message Manipulation Rule 4 (for SWYX IP-PBX)

Message Manipulations [Contact correction]

GENERAL

Index: 4
Name: Contact correction
Manipulation Set ID: 2
Row Role: Use Current Condition

MATCH

Message Type: Invite.Request
Condition: Header.Contact.URL.User != 'SipGwTrunk'

ACTION

Action Subject: Header.Contact.URL.User
Action Type: Modify
Action Value: 'SipGwTrunk'

Cancel

APPLY

7. Configure another manipulation rule (Manipulation Set 2) for SWYX IP-PBX. This rule is applied to INVITE request messages sent to the SWYX IP-PBX in anonymous call scenario. This replace the host part of the SIP P-Asserted-Identity Header with value 'anonymous.invalid', if the user part of the SIP P-Asserted-Identity Header equal to 'anonymous'.

Parameter	Value
Index	5
Name	AnonymousPAI
Manipulation Set ID	2
Message Type	Invite.Request
Condition	Header.P-Asserted-Identity.URL.User == 'anonymous'
Action Subject	Header.P-Asserted-Identity.URL.Host
Action Type	Modify
Action Value	'anonymous.invalid'

Figure 4-22: Configuring SIP Message Manipulation Rule 5 (for SWYX IP-PBX)

Message Manipulations [AnonymousPAI]

GENERAL	ACTION
Index: 5	Action Subject: Header.P-Asserted-Identity.URL.Host Editor
Name: AnonymousPAI	Action Type: Modify
Manipulation Set ID: 2	Action Value: 'anonymous.invalid' Editor
Row Role: Use Current Condition	
MATCH	
Message Type: Invite.Request Editor	
Condition: Header.P-Asserted-Identity.URL.User == 'anony' Editor	

Cancel [APPLY](#)

8. If the manipulation rule Index 5 (above) is executed, then the following rule is also executed on the same SIP message. This add the SIP Privacy Header with value 'id'.

Parameter	Value
Index	6
Name	AnonymousPrivacy
Manipulation Set ID	2
Row Role	Use Previous Condition
Action Subject	Header.Privacy
Action Type	Add
Action Value	'id'

Figure 4-23: Configuring SIP Message Manipulation Rule 6 (for SWYX IP-PBX)

Message Manipulations [AnonymousPrivacy]

GENERAL

Index

6

Name

AnonymousPrivacy

Manipulation Set ID

2

Row Role

Use Previous Condition

ACTION

Action Subject

Header.Privacy

Editor

Action Type

Add

Action Value

'id'

Editor

MATCH

Message Type

Editor

Condition

Editor

Cancel

APPLY

9. Configure another manipulation rule (Manipulation Set 2) for SWYX IP-PBX. This rule is applied to INVITE request messages sent to the SWYX IP-PBX in anonymous call scenario. This replace the SIP P-Asserted-Identity Header with value from the SIP From Header, if the the SIP From Header doesn't contains 'anonymous' in the user part.

Parameter	Value
Index	7
Name	AnonymousPAI
Manipulation Set ID	2
Message Type	Invite.Request
Condition	Header.From.URL.User !contains 'anonymous'
Action Subject	Header.P-Asserted-Identity
Action Type	Modify
Action Value	Header.From

Figure 4-24: Configuring SIP Message Manipulation Rule 7 (for SWYX IP-PBX)

Message Manipulations [From 2 PAI]

GENERAL

Index: 7

Name: From 2 PAI

Manipulation Set ID: 2

Row Role: Use Current Condition

ACTION

Action Subject: Header.P-Asserted-Identity

Action Type: Modify

Action Value: Header.From

MATCH

Message Type: Invite.Request

Condition: Header.From.URL.User !contains 'anonymous'

Cancel APPLY

Figure 4-25: Example of Configured SIP Message Manipulation Rules

Message Manipulations (8)								
+ New Edit Insert Page 1 of 1 Show 10 records per page								
INDEX	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	ROW ROLE
0	Reject Cause	0	Any.Response.5		Header.Reques	Modify	'600'	Use Current Co
1	Remove P-Prefe	0	Invite.Request	Header.P-Prefe	Header.P-Prefe	Remove		Use Current Co
2	map PAI to For	1	Invite.Request	Header.P-Asse	Header.From.U	Modify	Header.P-Asse	Use Current Co
3	remove second	1	Invite.Request	Header.P-Asse	Header.P-Asse	Remove		Use Current Co
4	Contact correct	2	Invite.Request	Header.Contact	Header.Contact	Modify	'SipGwTrunk'	Use Current Co
5	AnonymousPAI	2	Invite.Request	Header.P-Asse	Header.P-Asse	Modify	'anonymous.in	Use Current Co
6	AnonymousPriv	2			Header.Privacy	Add	'id'	Use Previous C
7	From 2 PAI	2	invite.request	header.from.ur	header.p-asser	Modify	header.from	Use Current Co

The table displayed below includes SIP message manipulation rules which are grouped together under Manipulation Set IDs (Manipulation Set IDs 0, 1, and 2) and which are executed for messages sent to and from the DTAG SIP Trunk IP Group as well as the SWYX IP-PBX IP Group. These rules are specifically required to enable proper interworking between DTAG SIP Trunk and SWYX IP-PBX. Refer to the *User's Manual* for further details concerning the full capabilities of header manipulation.

Rule Index	Rule Description	Reason for Introducing Rule
0	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).	DTAG SIP Trunk does not disconnect the call immediately after receiving '5xx' method types.
1	This rule is applied to INVITE request messages sent to the DTAG SIP Trunk IP. This rule removes SIP P-Preferred-Identity Header, if it's exists.	DTAG SIP Trunk requirement.
2	This rule is applied to INVITE request messages received from the SWYX IP-PBX. This rule replaces the user part of the SIP From Header with the value from the P-Asserted-Identity Header, if it's exists.	DTAG SIP Trunk requirement.
3	This rule is applied to INVITE request messages received from the SWYX IP-PBX. This rule removes the second index of the SIP P-Asserted-Identity Header, if it's exists.	DTAG SIP Trunk requirement.
4	This rule is applied to INVITE request messages sent to the SWYX IP-PBX. This rule replaces the user part of the SIP Contact Header with value 'SipGwTrunk', if it's not already equivalent to it..	SWYX IP-PBX requirement.
5	This rule is applied to INVITE request messages sent to the SWYX IP-PBX in an anonymous call scenario. This rule replaces the host part of the SIP P-Asserted-Identity Header with value 'anonymous.invalid', on the condition that the user part of the SIP P-Asserted-Identity Header is equivalent to 'anonymous'.	SWYX IP-PBX requirement.

Rule Index	Rule Description	Reason for Introducing Rule
6	If the manipulation rule Index 5 (above) is executed, then the following rule is also executed on the same SIP message. This rule adds the SIP Privacy Header with value 'id'.	SWYX IP-PBX requirement.
7	This rule is applied to INVITE request messages sent to the SWYX IP-PBX in an anonymous call scenario. This rule replaces the SIP P-Asserted-Identity Header with value from the SIP From Header, on the condition that the SIP From Header doesn't contain 'anonymous' in the user part.	SWYX IP-PBX requirement.

10. Assign Manipulation Set IDs 1 and 2 to the SWYX IP-PBX IP Group:

- a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
- b. Select the row of the Teams Direct Routing IP Group, and then click **Edit**.
- c. Set the 'Inbound Message Manipulation Set' field to **1**.
- d. Set the 'Outbound Message Manipulation Set' field to **2**.

Figure 4-26: Assigning Manipulation Set to the SWYX IP-PBX IP Group

IP Groups [SWYX]

SRD: #0 [DefaultSRD]

GENERAL

Index: 1

Name: SWYX

Topology Location: Down

Type: Server

Proxy Set: #1 [SWYX] [View](#)

IP Profile: #1 [SWYX] [View](#)

Media Realm: #0 [SWYX] [View](#)

Internal Media Realm: -- [View](#)

Contact User:

SIP Group Name: sip-trunk.telekom.de

QUALITY OF EXPERIENCE

QoE Profile: -- [View](#)

Bandwidth Profile: -- [View](#)

MESSAGE MANIPULATION

Inbound Message Manipulation Set: 1

Outbound Message Manipulation Set: 2

Message Manipulation User-Defined String 1:

Message Manipulation User-Defined String 2:

Proxy Keep-Alive using IP Group settings: Disable

[Cancel](#) [APPLY](#)

- e. Click **Apply**.

11. Assign Manipulation Set ID 0 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 **0**.

Figure 4-27: Assigning Manipulation Set 4 to the DTAG SIP Trunk IP Group

IP Groups [DTAG]

SRD #0 [DefaultSRD]

GENERAL		QUALITY OF EXPERIENCE	
Index	2	QoE Profile	-- View
Name	DTAG	Bandwidth Profile	-- View
Topology Location	Up		
Type	Server	MESSAGE MANIPULATION	
Proxy Set	#2 [DTAG] View	Inbound Message Manipulation Set	-1
IP Profile	#2 [DTAG] View	Outbound Message Manipulation Set	0
Media Realm	#1 [DTAG] View	Message Manipulation User-Defined String 1	
Internal Media Realm	-- View	Message Manipulation User-Defined String 2	
Contact User		Proxy Keep-Alive using IP Group settings	Disable
SIP Group Name	sip-trunk.telekom.de		

Cancel APPLY

- d. Click **Apply**.

4.11 Configure Registration Accounts

This section 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 account:

1. Open the Accounts table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Accounts**).
2. Click **New**.
3. Configure the account according to the provided information from the DTAG, for example:

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

4. Configure a new account according to the provided information from the SWYX, for example:

Parameter	Value
Served IP Group	DTAG
Application Type	SBC
Serving IP Group	SWYX
Host Name	As provided by the SWYX IP-PBX
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

4.12 Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

4.12.1 DTMF Interworking for Fax and Modem

This section describes how to configure the SBC's handling of the fax and modem interworking.

➤ **To configure DTMF interworking for fax and modem:**

1. Open the RTP/RTCP Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **RTP/RTCP Settings**).
2. Configure 'Fax Bypass Payload Type' parameter with value **126**.
3. Configure 'Modem Bypass Payload Type' parameter with value **127**.

Figure 4-28: DTMF Interworking for Fax and Modem

PAYLOAD TYPES	
RFC 2833 TX Payload Type	96
RFC 2833 RX Payload Type	96
RFC 2198 Payload Type	104
➔ Fax Bypass Payload Type	• 126
➔ Modem Bypass Payload Type	• 127
Enable RFC 3389 CN Payload Type	Enable ▼

4. Click **Apply**.

4.12.2 Optimizing CPU Cores Usage for a Specific Service (relevant for Mediant 9000 and Software SBC only)

This section describes how to optimize the SBC's CPU cores usage for a specified profile to achieve maximum capacity for that profile. The supported profiles include:

- SIP profile – improves SIP signaling performance, for example, SIP calls per second (CPS)
- SRTP profile – improves maximum number of SRTP sessions
- Transcoding profile – enables all DSP-required features, for example, transcoding and voice in-band detectors

➤ **To optimize core allocation for a profile:**

1. Open the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC General Settings**).
2. From the 'SBC Performance Profile' drop-down list, select the required profile:

SBC Performance Profile

• Optimized for transcoding ▼ ⚡

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

This page is intentionally left blank.

A AudioCodes INI File

The *ini* configuration file of the 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: M800B
;Board Type: 72
;Serial Number: 4807217
;Slot Number: 1
;Software Version: 7.20A.254.475
;DSP Software Version: 5014AE3_R => 710.19
;Board IP Address: 10.15.77.77
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 512M   Flash size: 64M   Core speed: 300Mhz
;Num of DSP Cores: 3
;Num of physical LAN ports: 4
;Profile: NONE
;;;Key features;;Board Type: M800B ;BRITrunks=4 ;Security: IPSEC
MediaEncryption StrongEncryption EncryptControlProtocol ;Channel Type:
DspCh=30 IPMediaDspCh=30 ;ElTrunks=1 ;TlTrunks=1 ;FXSPorts=4 ;FXOPorts=0
;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 ;QOE features: VoiceQualityMonitoring
MediaEnhancement ;DSP Voice features: RTCP-XR ;Control Protocols: MGCP
SIP SBC=100 MSFT FEU=100 TestCall=100 TEAMS ;Default features;;Coders:
G711 G726;

;----- HW components -----
;
; Slot # : Module type : # of ports
;-----
;      1 : FALC56      : 1
;      2 : FXS         : 4
;      3 : BRI         : 4
;-----

[SYSTEM Params]

SyslogServerIP = 10.15.77.100
EnableSyslog = 0
TR069ACSPASSWORD = '$1$gQ=='
TR069CONNECTIONREQUESTPASSWORD = '$1$gQ=='
NTPServerIP = '10.15.27.1'
SBCWizardFilename = 'templates4.zip'
SyslogLogLevel = 5
```

```
[BSP Params]

PCMLawSelect = 3
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[Analog Params]

[ControlProtocols Params]

AdminStateLockControl = 0

[PSTN Params]

V5ProtocolSide = 0

[Voice Engine Params]

FaxBypassPayloadType = 126
ModemBypassPayloadType = 127
PLThresholdLevelsPerMille_0 = 5
PLThresholdLevelsPerMille_1 = 10
PLThresholdLevelsPerMille_2 = 20
PLThresholdLevelsPerMille_3 = 50
CallProgressTonesFilename = 'germany.dat'

[WEB Params]

Languages = 'en-US', '', '', '', '', '', '', '', ''

[SIP Params]

GWDEBUGLEVEL = 5
MSLDAPPRIMARYKEY = 'telephoneNumber'
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144

[SNMP Params]

[ PhysicalPortsTable ]

FORMAT Index = Port, Mode, SpeedDuplex, PortDescription, GroupMember;
PhysicalPortsTable 0 = "GE_4_1", 1, 4, "User Port #0", "GROUP_1";
PhysicalPortsTable 1 = "GE_4_2", 1, 4, "User Port #1", "GROUP_1";
PhysicalPortsTable 2 = "GE_4_3", 1, 4, "User Port #2", "GROUP_2";
PhysicalPortsTable 3 = "GE_4_4", 1, 4, "User Port #3", "GROUP_2";

[ \PhysicalPortsTable ]

[ EtherGroupTable ]
```

```

FORMAT Index = Group, Mode, Member1, 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", 0, "", "";
EtherGroupTable 3 = "GROUP_4", 0, "", "";

[ \EtherGroupTable ]

[ DeviceTable ]

FORMAT Index = VlanID, UnderlyingInterface, DeviceName, Tagging, MTU;
DeviceTable 0 = 1, "GROUP_1", "vlan 1", 0, 1500;
DeviceTable 1 = 2, "GROUP_2", "vlan 2", 0, 1500;

[ \DeviceTable ]

[ InterfaceTable ]

FORMAT Index = ApplicationTypes, InterfaceMode, IPAddress, PrefixLength,
Gateway, InterfaceName, PrimaryDNSServerIPAddress,
SecondaryDNSServerIPAddress, UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.77.77, 16, 10.15.0.1, "LAN_IF",
10.15.27.1, 0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 195.189.192.157, 24, 195.189.192.129, "WAN_IF",
80.179.52.100, 80.179.55.100, "vlan 2";

[ \InterfaceTable ]

[ WebUsers ]

FORMAT Index = Username, Password, Status, PwAgeInterval, SessionLimit,
CliSessionLimit, SessionTimeout, BlockTime, UserLevel, PwNonce,
SSHPublicKey;
WebUsers 0 = "Admin",
"$1$LU$YHlEHV1JWAlIFDgAKCQQPWax2ICNyJiB3fioqfnN5LHgtZmJnY2FmZmBta2NqbWQ9P
VNQVlZRUVcBWloOCV4=", 1, 0, 5, -1, 15, 60, 200,
"074838fa9c9fdb7dbbc2a6efc2b782c9", "";
WebUsers 1 = "User",
"$1$CWhrOTk7Nz0mKSJxIXYlCS0pLCgseykuFkIbGxUVEkIRTRwfGEweTgJQBwcDA1MEAA4LW
goLWw54IHJzcyclJX0=", 1, 0, 5, -1, 15, 60, 50,
"4f507127bd4bd8351a32d9e96801e2e3", "";

[ \WebUsers ]

[ TLSContexts ]

FORMAT Index = Name, TLSVersion, DTLSVersion, ServerCipherString,
ClientCipherString, RequireStrictCert, TlsRenegotiation, OcspEnable,
OcspServerPrimary, OcspServerSecondary, OcspServerPort,
OcspDefaultResponse, DHKeySize;
TLSContexts 0 = "default", 0, 0, "DEFAULT", "DEFAULT", 0, 1, 0, 0.0.0.0,
0.0.0.0, 2560, 0, 1024;
TLSContexts 1 = "Teams", 4, 0, "DEFAULT", "DEFAULT", 0, 1, 0, 0.0.0.0,
0.0.0.0, 2560, 0, 1024;

```

```
[ \TLSContexts ]

[ AudioCodersGroups ]

FORMAT Index = Name;
AudioCodersGroups 0 = "AudioCodersGroups_0";

[ \AudioCodersGroups ]

[ AllowedAudioCodersGroups ]

FORMAT Index = Name;
AllowedAudioCodersGroups 0 = "Telekom";

[ \AllowedAudioCodersGroups ]

[ IpProfile ]

FORMAT Index = ProfileName, IpPreference, CodersGroupName, IsFaxUsed,
JitterBufMinDelay, JitterBufOptFactor, IPDiffServ, SigIPDiffServ,
RTPRedundancyDepth, CNMode, VxxTransportType, NSEMode, IsDTMFUsed,
PlayRBTone2IP, EnableEarlyMedia, ProgressIndicator2IP,
EnableEchoCanceller, CopyDest2RedirectNumber, MediaSecurityBehaviour,
CallLimit, DisconnectOnBrokenConnection, FirstTxDtmfOption,
SecondTxDtmfOption, RxDTMFOption, EnableHold, InputGain, VoiceVolume,
AddIEInSetup, SBCExtensionCodersGroupName, MediaIPVersionPreference,
TranscodingMode, SBCAssowedMediaTypes, SBCAssowedAudioCodersGroupName,
SBCAssowedVideoCodersGroupName, SBCAssowedCodersMode,
SBCMediaSecurityBehaviour, SBCRFC2833Behavior, SBCAlternativeDTMFMethod,
SBCSendMultipleDTMFMethods, SBCAssertIdentity,
AMDSensitivityParameterSuit, AMDSensitivityLevel, AMDMaxGreetingTime,
AMDMaxPostSilenceGreetingTime, SBCDiversiionMode, SBCHistoryInfoMode,
EnableQSIGTunneling, SBCFaxCodersGroupName, SBCFaxBehavior,
SBCFaxOfferMode, SBCFaxAnswerMode, SbcPrackMode, SBCSessionExpiresMode,
SBCRemoteUpdateSupport, SBCRemoteReinviteSupport,
SBCRemoteDelayedOfferSupport, SBCRemoteReferBehavior,
SBCRemote3xxBehavior, SBCRemoteMultiple18xSupport,
SBCRemoteEarlyMediaResponseType, SBCRemoteEarlyMediaSupport,
EnableSymmetricMKI, MKISize, SBCEnforceMKISize, SBCRemoteEarlyMediaRTP,
SBCRemoteSupportsRFC3960, SBCRemoteCanPlayRingback, EnableEarly183,
EarlyAnswerTimeout, SBC2833DTMFPayloadType, SBCUserRegistrationTime,
ResetSRTPStateUponRekey, AmdMode, SBCReliableHeldToneSource,
GenerateSRTPKeys, SBCPlayHeldTone, SBCRemoteHoldFormat,
SBCRemoteReplacesBehavior, SBCSDPptimeAnswer, SBCPreferredPTime,
SBCUseSilenceSupp, SBCRTPRedundancyBehavior, SBCPlayRBTToTransferee,
SBCRTPMode, SBCJitterCompensation, SBCRemoteRenegotiateOnFaxDetection,
JitterBufMaxDelay, SBCUserBehindUdpNATRegistrationTime,
SBCUserBehindTcpNATRegistrationTime, SBCSDPHandleRTCPAttribute,
SBCRemoveCryptoLifetimeInSDP, SBCIceMode, SBCRTPMux,
SBCMediaSecurityMethod, SBCHandleXDetect, SBCRTPFeedback,
SBCRemoteRepresentationMode, SBCKeepVIAHeaders, SBCKeepRoutingHeaders,
SBCKeepUserAgentHeader, SBCRemoteMultipleEarlyDialogs,
SBCRemoteMultipleAnswersMode, SBCDirectMediaTag,
SBCAdaptRFC2833BWToVoiceCoderBW, CreatedByRoutingServer,
SBCFaxReroutingMode, SBCMaxCallDuration, SBCGenerateRTP,
SBCISUPBodyHandling, SBCISUPVariant, SBCVoiceQualityEnhancement,
SBCMaxOpusBW, SBCEnhancedPlc, LocalRingbackTone, LocalHeldTone,
SBCGenerateNoOp, SBCRemoveUnknownCrypto, SBCMultipleCoders, DataDiffServ,
SBCMSRPREinviteUpdateSupport, SBCMSRPOfferSetupRole, SBCMSRPEmpMsg;
```

```

IpProfile 1 = "SWYX", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0, 0,
2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "",
"AudioCodersGroups_0", 0, 0, "", "Telekom", "", 1, 0, 2, 2, 0, 1, 0, 8,
300, 400, 0, 0, 0, "", 0, 0, 1, 1, 0, 1, 1, 0, 3, 2, 1, 0, 1, 0, 0, 0, 1,
0, 1, 0, 0, 0, 0, 0, 0, 1, 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, 0, -1, -1, 0, 0, 0, 0, 1, 2, 0;
IpProfile 2 = "DTAG", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0, 0,
2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, "",
"AudioCodersGroups_0", 0, 0, "", "Telekom", "", 1, 0, 1, 1, 0, 1, 0, 8,
300, 400, 2, 2, 0, "", 0, 0, 1, 3, 0, 2, 2, 1, 3, 0, 0, 0, 1, 0, 0, 0, 0,
0, 1, 0, 0, 102, 0, 0, 0, 1, 0, 0, 1, 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, 0, -1, -1, 0, 0, 0, 0, 1, 2, 0;

[ \IpProfile ]

[ CpMediaRealm ]

FORMAT Index = MediaRealmName, IPv4IF, IPv6IF, RemoteIPv4IF,
RemoteIPv6IF, PortRangeStart, MediaSessionLeg, PortRangeEnd,
TCPPortRangeStart, TCPPortRangeEnd, IsDefault, QoeProfile, BWProfile,
TopologyLocation;
CpMediaRealm 0 = "SWYX", "LAN_IF", "", "", "", 6000, 100, 6999, 0, 0, 0,
"", "", 0;
CpMediaRealm 1 = "DTAG", "WAN_IF", "", "", "", 7000, 100, 7999, 0, 0, 0,
"", "", 1;

[ \CpMediaRealm ]

[ SBCRoutingPolicy ]

FORMAT Index = Name, LCREnable, LCRAverageCallLength, LCRDefaultCost,
LdapServerGroupName;
SBCRoutingPolicy 0 = "Default_SBCRoutingPolicy", 0, 1, 0, "";

[ \SBCRoutingPolicy ]

[ SRD ]

FORMAT Index = Name, BlockUnRegUsers, MaxNumOfRegUsers,
EnableUnAuthenticatedRegistrations, SharingPolicy, UsedByRoutingServer,
SBCOperationMode, SBCRoutingPolicyName, SBCDialPlanName,
AdmissionProfile;
SRD 0 = "DefaultSRD", 0, -1, 1, 0, 0, 0, "Default_SBCRoutingPolicy", "",
"";

[ \SRD ]

[ MessagePolicy ]

FORMAT Index = Name, MaxMessageLength, MaxHeaderLength, MaxBodyLength,
MaxNumHeaders, MaxNumBodies, SendRejection, MethodList, MethodListType,
BodyList, BodyListType, UseMaliciousSignatureDB;
MessagePolicy 0 = "Malicious Signature DB Protection", -1, -1, -1, -1, -
1, 1, "", 0, "", 0, 1;

```

```
[ \MessagePolicy ]

[ SIPInterface ]

FORMAT Index = InterfaceName, NetworkInterface,
SCTPSecondaryNetworkInterface, ApplicationType, UDPPort, TCPPort,
TLSPort, SCTPPort, AdditionalUDPPorts, AdditionalUDPPortsMode, SRDName,
MessagePolicyName, TLSContext, TLSMutualAuthentication,
TCPKeepaliveEnable, ClassificationFailureResponseType,
PreClassificationManSet, EncapsulatingProtocol, MediaRealm,
SBCDirectMedia, BlockUnRegUsers, MaxNumOfRegUsers,
EnableUnAuthenticatedRegistrations, UsedByRoutingServer,
TopologyLocation, PreParsingManSetName, AdmissionProfile,
CallSetupRulesSetId;
SIPInterface 0 = "SWYX", "LAN_IF", "", 2, 5060, 0, 0, 0, "", 0,
"DefaultSRD", "", "default", -1, 0, 500, -1, 0, "SWYX", 0, -1, -1, -1, 0,
0, "", "", -1;
SIPInterface 1 = "DTAG", "WAN_IF", "", 2, 0, 5060, 0, 0, "", 0,
"DefaultSRD", "", "default", -1, 0, 0, -1, 0, "DTAG", 0, -1, -1, -1, 0,
1, "", "", -1;

[ \SIPInterface ]

[ ProxySet ]

FORMAT Index = ProxyName, EnableProxyKeepAlive, ProxyKeepAliveTime,
ProxyLoadBalancingMethod, IsProxyHotSwap, SRDName, ClassificationInput,
TLSContextName, ProxyRedundancyMode, DNSResolveMethod,
KeepAliveFailureResp, GWIPv4SIPInterfaceName, SBCIPv4SIPInterfaceName,
GWIPv6SIPInterfaceName, SBCIPv6SIPInterfaceName, MinActiveServersLB,
SuccessDetectionRetries, SuccessDetectionInterval,
FailureDetectionRetransmissions;
ProxySet 0 = "ProxySet_0", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "",
"", "SWYX", "", "", 1, 1, 10, -1;
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 Index = Type, Name, ProxySetName, SIPGroupName, ContactUser,
SipReRoutingMode, AlwaysUseRouteTable, SRDName, MediaRealm,
InternalMediaRealm, ClassifyByProxySet, ProfileName, MaxNumOfRegUsers,
InboundManSet, OutboundManSet, RegistrationMode, AuthenticationMode,
MethodList, SBCServerAuthType, OAuthHTTPService, EnableSBCCClientForking,
SourceUriInput, DestUriInput, ContactName, Username, Password, UIFormat,
QOEProfile, BWProfile, AlwaysUseSourceAddr, MsgManUserDef1,
MsgManUserDef2, SIPConnect, SBCPSAPMode, DTLContext,
CreatedByRoutingServer, UsedByRoutingServer, SBCOperationMode,
SBCRouteUsingRequestURIPort, SBCKeepOriginalCallID, TopologyLocation,
SBCDialPlanName, CallSetupRulesSetId, Tags, SBCUserStickiness,
UserUDPPortAssignment, AdmissionProfile, ProxyKeepAliveUsingIPG,
SBCAltRouteReasonsSetName, TeamsMediaOptimization;
IPGroup 0 = 0, "Default_IPG", "ProxySet_0", "", "", -1, 0, "DefaultSRD",
"", "", 0, "", -1, -1, -1, 0, 0, "", -1, "", 0, -1, -1, "", "",
```

```

"$1$gQ==" , 0, "", "", 0, "", "", 0, 0, "default", 0, 0, -1, 0, 0, 0, "",
-1, "", 0, 0, "", 0, "", 0;
IPGroup 1 = 0, "SWYX", "SWYX", "sip-trunk.telekom.de", "", -1, 0,
"DefaultSRD", "SWYX", "", 1, "SWYX", -1, 1, 2, 0, 0, "", -1, "", 0, -1,
1, "", "", "$1$gQ==" , 0, "", "", 0, "", "", 0, 0, "default", 0, 0, -1, 0,
0, 0, "", -1, "", 0, 0, "", 0, "", 0;
IPGroup 2 = 0, "DTAG", "DTAG", "sip-trunk.telekom.de", "", -1, 0,
"DefaultSRD", "DTAG", "", 1, "DTAG", -1, -1, 0, 0, 0, "", -1, "", 0, -1,
-1, "", "", "$1$gQ==" , 0, "", "", 0, "", "", 0, 0, "default", 0, 0, -1,
0, 0, 1, "", -1, "", 0, 0, "", 0, "", 0;

[ \IPGroup ]

[ ProxyIp ]

FORMAT Index = ProxySetId, ProxyIpIndex, IpAddress, TransportType,
Priority, Weight;
ProxyIp 0 = "0", 0, "10.50.252.100:5060", 0, 0, 0;
ProxyIp 1 = "1", 0, "10.50.252.102:5060", 0, 0, 0;
ProxyIp 2 = "2", 0, "reg.sip-trunk.telekom.de", 1, 0, 0;

[ \ProxyIp ]

[ IP2IPRouting ]

FORMAT Index = RouteName, RoutingPolicyName, SrcIPGroupName,
SrcUsernamePrefix, SrcHost, DestUsernamePrefix, DestHost, RequestType,
MessageConditionName, ReRouteIPGroupName, Trigger, CallSetupRulesSetId,
DestType, DestIPGroupName, DestSIPInterfaceName, DestAddress, DestPort,
DestTransportType, AltRouteOptions, GroupPolicy, CostGroup, DestTags,
SrcTags, IPGroupSetName, RoutingTagName, InternalAction;
IP2IPRouting 0 = "Terminate OPTIONS", "Default_SBCRoutingPolicy", "Any",
"*, ", ", ", ", ", 6, ", ", "Any", 0, -1, 1, ", ", ", ", "internal", 0, -1, 0,
0, ", ", ", ", ", ", "default", ", ";
IP2IPRouting 1 = "SWYX -> DTAG", "Default_SBCRoutingPolicy", "SWYX", ", ",
"*, ", ", ", ", 0, ", ", "Any", 0, -1, 0, "DTAG", ", ", ", ", 0, -1, 0, 0, ", ",
", ", ", ", "default", ", ";
IP2IPRouting 2 = "DTAG -> SWYX", "Default_SBCRoutingPolicy", "DTAG", ", ",
"*, ", ", ", ", 0, ", ", "Any", 0, -1, 0, "SWYX", ", ", ", ", 0, -1, 0, 0, ", ",
", ", ", ", "default", ", ";

[ \IP2IPRouting ]

[ IPOutboundManipulation ]

FORMAT Index = ManipulationName, RoutingPolicyName,
IsAdditionalManipulation, SrcIPGroupName, DestIPGroupName,
SrcUsernamePrefix, SrcHost, DestUsernamePrefix, DestHost,
CallingNamePrefix, MessageConditionName, RequestType, ReRouteIPGroupName,
Trigger, ManipulatedURI, RemoveFromLeft, RemoveFromRight, LeaveFromRight,
Prefix2Add, Suffix2Add, PrivacyRestrictionMode, DestTags, SrcTags;
IPOutboundManipulation 0 = "SWYX->DTAG (Src)",
"Default_SBCRoutingPolicy", 0, "SWYX", "DTAG", ", ", ", ", ", ", ", ",
", ", 0, 0, 0, 0, 0, 255, "+", ", ", 0, ", ", ", ";
IPOutboundManipulation 1 = "SWYX->DTAG (Dst)",
"Default_SBCRoutingPolicy", 0, "SWYX", "DTAG", ", ", ", ", "00", ", ", ", ",
", ", 0, "Any", 0, 1, 2, 0, 255, "+", ", ", 0, ", ", ", ";

```

```
[ \IPOutboundManipulation ]

[ MessageManipulations ]

FORMAT Index = ManipulationName, ManSetID, MessageType, Condition,
ActionSubject, ActionType, ActionValue, RowRole;
MessageManipulations 0 = "Reject Cause", 0, "Any.Response.5xx", "",
"Header.Request-URI.MethodType", 2, "'600'", 0;
MessageManipulations 1 = "Remove P-Preferred", 0, "Invite.Request",
"Header.P-Preferred-Identity exists", "Header.P-Preferred-Identity", 1,
"", 0;
MessageManipulations 2 = "map PAI to From", 1, "Invite.Request",
"Header.P-Asserted-Identity.0 exists", "Header.From.URL.User", 2,
"Header.P-Asserted-Identity.0.URL.User", 0;
MessageManipulations 3 = "Remove second PAI if exists", 1,
"Invite.Request", "Header.P-Asserted-Identity.1 exists", "Header.P-
Asserted-Identity.1", 1, "", 0;
MessageManipulations 4 = "Contact correction", 2, "Invite.Request",
"Header.Contact.URL.User != 'SipGwTrunk'", "Header.Contact.URL.User", 2,
"'SipGwTrunk'", 0;
MessageManipulations 5 = "AnonymousPAI", 2, "Invite.Request", "Header.P-
Asserted-Identity.URL.User == 'anonymous'", "Header.P-Asserted-
Identity.URL.Host", 2, "'anonymous.invalid'", 0;
MessageManipulations 6 = "AnonymousPrivacy", 2, "", "", "Header.Privacy",
0, "'id'", 1;
MessageManipulations 7 = "From 2 PAI", 2, "Invite.Request",
"Header.From.URL.User !contains 'anonymous'", "Header.P-Asserted-
Identity", 2, "Header.From", 0;

[ \MessageManipulations ]

[ GwRoutingPolicy ]

FORMAT Index = Name, LCREnable, LCRAverageCallLength, LCRDefaultCost,
LdapServerGroupName;
GwRoutingPolicy 0 = "GwRoutingPolicy", 0, 1, 0, "";

[ \GwRoutingPolicy ]

[ ResourcePriorityNetworkDomains ]

FORMAT Index = Name, Ip2TelInterworking;
ResourcePriorityNetworkDomains 1 = "dsn", 1;
ResourcePriorityNetworkDomains 2 = "dod", 1;
ResourcePriorityNetworkDomains 3 = "drsn", 1;
ResourcePriorityNetworkDomains 5 = "uc", 1;
ResourcePriorityNetworkDomains 7 = "cuc", 1;

[ \ResourcePriorityNetworkDomains ]

[ MaliciousSignatureDB ]

FORMAT Index = Name, Pattern;
MaliciousSignatureDB 0 = "SIPVicious", "Header.User-Agent.content prefix
'friendly-scanner'";
```

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

[ \MaliciousSignatureDB ]

[ AllowedAudioCoders ]

FORMAT Index = AllowedAudioCodersGroupName, AllowedAudioCodersIndex,
CoderID, UserDefineCoder;
AllowedAudioCoders 0 = "Telekom", 0, 1, "";
AllowedAudioCoders 1 = "Telekom", 1, 2, "";

[ \AllowedAudioCoders ]

[ AudioCoders ]

FORMAT Index = AudioCodersGroupId, AudioCodersIndex, Name, pTime, rate,
PayloadType, Sce, CoderSpecific;
AudioCoders 0 = "AudioCodersGroups_0", 0, 1, 2, 90, -1, 0, "";
AudioCoders 1 = "AudioCodersGroups_0", 1, 2, 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.

200 Cottontail Lane
Suite A101E
Somerset NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

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

website: <https://www.audiocodes.com>

©2019 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VolPerfect, VolPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, AudioCodes Room Experience and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-12761

