



# Business Talk & BTIP Configuration Guidelines With Audiocodes Customer eSBC

versions addressed in this guide: Audiocodes eSBC V.720A & .7.40A

Information included in this document is dedicated to customer equipment (IPBX, TOIP ecosystems) connection to Business Talk & BTIP service: it shall not be used for other goals or in another context.

Version of 04/04/2024



## Table of contents

<b>1.</b>	<b>Goal of this document.....</b>	<b>4</b>
<b>2.</b>	<b>References documents .....</b>	<b>5</b>
<b>3.</b>	<b>Prerequisites .....</b>	<b>6</b>
3.1	Certificates.....	6
3.2	Public DNS configuration: .....	6
3.3	NTP .....	6
3.4	Firewall flows for BTIP over Internet and BT over Internet .....	6
3.5	Orange BTalk/BTIP specifications .....	7
<b>4.</b>	<b>Certified Architecture.....</b>	<b>10</b>
4.1	Introduction to architecture components and features .....	10
4.2	Architecture with Audiocodes “customer” eSBC with OBS SIP unencrypted configuration .....	11
4.2.1	Unencrypted SIP Trunk .....	11
4.2.2	Encrypted SIP Trunk Over Internet .....	12
4.2.3	Parameters to be provided by customers to access the service .....	13
	Unencrypted SIP Trunk through BVPN.....	13
	Encrypted SIP Trunk through Internet.....	13
4.3	BTalk & BTIP Audiocodes eSBC certified versions .....	15
4.4	Audiocodes Global configuration .....	16
4.4.1	Objects .....	16
4.4.2	Information and Syntax .....	16
4.5	Orange Business BTalk & BTIP Carrier unencrypted SIP configuration for AudioCodes eSBC (UDP).....	18
4.5.1	Configure IP Network.....	18
4.5.2	Message Manipulation Policy .....	18
	Message Policy.....	18
4.5.3	Coders and Profiles .....	19
	Allowed Audio Coders Groups .....	19
	IP Profile Settings.....	23
4.5.4	<b>Core Entities</b> .....	27
	SRD Table .....	27
	SIP Interface Table.....	27
	Media Realm Table .....	29
	Proxy Set Table and Address.....	31
	IP Group Table.....	34
4.5.5	<b>SIP Message Manipulation</b> .....	37
4.6	Orange Business- BTalk over Internet & BTIP over Internet encrypted SIP configuration for AudioCodes eSBC (TLS).....	38
4.6.1	Configure IP Network.....	38
4.6.2	<b>TLS profile</b> .....	38
	TLS Context.....	38
	Certificate Signing Request (CSR) .....	39
4.6.3	Media Security.....	43
4.6.4	Public IP Network .....	44
4.6.5	Coders and Profiles .....	44
	Allowed Audio Coders Groups .....	44
	Allowed Audio Coders Groups in case of multiple codecs into SDP Audio	
	MLine (Optional).....	48
	IP Profile Settings.....	50
4.6.6	<b>Core Entities</b> .....	54
	SRD Table .....	54
	SIP Interface Table.....	54
	Media Realm Table .....	56

	Proxy Set Table and Address .....	58
	IP Group Table.....	61
4.6.7	<b>SIP Message Manipulation</b> .....	63
4.7	<b>SIP rules &amp; manipulations (eSBC Application)</b> .....	64
4.7.1	IP-to-IP Routing Table.....	64
4.7.2	Outbound Manipulations.....	64
4.7.3	Inbound Manipulations.....	65
4.7.4	SIP Messages Manipulations .....	66
<b>5.</b>	<b>Annexes</b> .....	<b>70</b>
5.1	Import Manipulations Rules via Incrementation INI file.....	70
5.2	Example of SIP INVITE message.....	71
	From IPPBX toward Orange BT/BTIP .....	71
	From Orange BT/BTIP toward Customer IPPBX.....	72
5.3	NTP server configuration.....	72
	<b>Glossary</b> .....	<b>74</b>

## 1. Goal of this document

The aim of this document is to provide configuration guidelines to ensure the interoperability between AudioCodes eSBC with Business Talk (BTalk) or Business Talk IP (BTIP) service from Orange Business Services, hereafter so-called “service”.

## 2. References documents

Title	Link
Business Talk IP/ Business Talk Guidelines Direct for Microsoft Teams Direct routing with Audiocodes eSBC (Dec 2023)	<a href="https://documentscontractuels.orange.fr/versions-anglaises_ann_4224.pdf">https://documentscontractuels.orange.fr/versions-anglaises_ann_4224.pdf</a>
Business Talk IP / Business Talk Guidelines for Microsoft Skype for Business 2015/2019 with Audiocodes eSBC (Dec 2023)	<a href="https://documentscontractuels.orange.fr/versions-anglaises_ann_4223.pdf">https://documentscontractuels.orange.fr/versions-anglaises_ann_4223.pdf</a>
Business Talk IP / Business Talk Guidelines for Alcatel Lucent OXE with OTSBC /Audiocodes eSBC (Fev 2024)	<a href="https://documentscontractuels.orange.fr/versions-anglaises_ann_4212.pdf">https://documentscontractuels.orange.fr/versions-anglaises_ann_4212.pdf</a>
Software Update for AudioCodes eSBCs & Gateways Version 7.20A.XXX.XXX /7.40A.XXX.XXX--	<a href="https://www.audiocodes.com/library/firmware">https://www.audiocodes.com/library/firmware</a> <a href="https://services.audiocodes.com/">https://services.audiocodes.com/</a>
Audiocodes eSBC Portfolio Overview	<a href="https://www.audiocodes.com/media/3020/audiocodes-mediante-enterprise-session-border-controllers-sbc-family-brochure.pdf">https://www.audiocodes.com/media/3020/audiocodes-mediante-enterprise-session-border-controllers-sbc-family-brochure.pdf</a>

## 3. Prerequisites

### 3.1 Certificates

In case of encrypted SIP trunk architecture, mutual TLS configuration is mandatory in order to exchange public certificates with Orange BTalk infrastructure in both ways.

Customer public trusted certificates chain is used by both the eSBC to authenticate the connection with our infrastructure and Orange public trusted certificates chain is used by the eSBC to authenticate the connection

The customer must generate on the Ribbon Edge eSBC a Certificate Signing Request (CSR) and request to a public Certificate Authority (CA) a public certificate.

Then only that the Root and intermediate Certificate Authorities (PEM format) must be communicated to Orange BTalk team.

### 3.2 Public DNS configuration:

Following requirements regarding Public DNS configuration must be follow:

- In eSBC configuration, public DNS is used for outgoing calls to PSTN (e.g. From iPBX/eSBC to BTol/BTIPol)
- Internet-naming resolution (FQDN): either enter the IP addresses of 2 private DNS, that relay DNS queries to Internet, or enter the IPs of 2 accessible public DNS such as those of Orange (80.10.246.2, 80.10.246.129)

### 3.3 NTP

The configuration of NTP servers on the eSBC is not fully detailed (still some typical example is described in annex) in this document but it is mandatory to implement an NTP server (public reliable NTP server) on Ribbon eSBC to ensure that the eSBC receives the current date and time.

This is necessary for validating Certificates of remote parties during TLS "Handcheck".

### 3.4 Firewall flows for BTIP over Internet and BT over Internet

Firewalls in the way of traffic between Ribbon eSBC and Orange infrastructure have to be updated in order to open required ports for BT over Internet or BTIP over Internet vary concerning the UDP Media ports range.

For BTIP over Internet, please note the Orange infrastructure Media public IP termination is different from Orange infrastructure SIP Signaling public FQDN/Public IP termination.

Refer to the 'BTalk over Internet & BTIP pre-requisites' and "BTalk/BTIP STAS" documents provided by your sales/project manager team for more details about firewall rules needed to be open.

### 3.5 Orange BTalk/BTIP specifications

The information in this chapter are the SIP trunk specifications required in order to interconnect Orange BTalk/BTIP network. The Enterprise SBC must be compliant with those specifications. This information were used to define the configuration described in this document.

#### ✓ **Supported RFC's**

- *RFC 3261 : Session initiation protocol*
- *RFC 3264 : An offer/answer Model with the Session Description Protocol*
- *RFC 3262 : Reliability of provisional responses in Session Initiation protocol (please refer to provisional response and PRACK section)*
- *RFC 3311 : The Session Initiation Protocol UPDATE Method*
- *RFC 3323 : A privacy Mechanism for the session Initiation Protocol*
- *RFC 3325 : Session Initiation Protocol for Asserted Identity within Trusted Networks*
- *RFC 3204 : MIME media types for ISUP and QSIG Objects*
- *RFC 3550 : RTP : A transport Protocol for Real Time Applications*
- *RFC 3711: SRTP: Secure Real-time Transport Protocol*
- *RFC 3960 : Early Media and Ringing Tone generation in the Session Initiation Protocol*
- *RFC 4566 : SDP: Session Description Protocol*
- *RFC 4568: SDP: Security Descriptions for Media Streams*
- *RFC 2833/4733 : RTP payload for DTMF digits, Telephony Tones and telephony signals*
- *RFC 5806 : Diversion Indication in SIP*
- *RFC 5009 : Private Header Extension to the Session Initiation Protocol for Authorization of early*

#### ✓ **Sip Methods supported:**

- *INVITE*
- *ACK*
- *CANCEL*
- *UPDATE (negotiated)*
- *BYE*
- *OPTIONS*

**Note : Sip methods not listed are not supported in this context**

#### ✓ **SIP Message size specifications are:**

- *SIP message limited to 4096 Bytes*
- *SDP Body limited to 1024 Bytes*

#### ✓ **SIP signalling specifications are:**

- *For unencrypted architecture we need to configure **UDP port 5060***
- *For encrypted architecture (TLS) we need to configure **TCP port 5061***

#### ✓ **Media specifications are by default listed below and should be adapted to your Customer service offer:**

- *For unencrypted architecture we need to configure **RTP port 6 000 to 20 000***
- *For encrypted architecture (TLS) we need to configuration **SRTP port 6 000 to 20 000 for Business Talk over Internet or SRTP port 6 000 to 38 000 for Business talk IP over Internet.***

#### ✓ **Identification**

- *For Audit purpose eSBC “User Agent” connected to BTalk/BTIP infrastructure require following format: “**IPBX/UC Vendor < Product> <Version>.<build> \ Patton eSBC<SBC model> <Version>.<build>**”*
- *Same requirement applies on Server Agent in provisional response.*

✓ **Encryption specifications are:**

- **TLS V.1.2**

The following Cipher list is supported as Cipher Client/Server:

- **TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384** (Recommended)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256

✓ **Codec/Packet Rate specifications are (prefer order list) :**

- G722 20 ms.(Only if specifically used)
- G.711 A-law 20 ms (or on demand specific G.711  $\mu$ -law 20 ms)
- G.729 20 ms (annexb = no)
- For BTIP over Internet and BTalk over Internet (TLS) only G.711 A-law 20 ms (or on demand specific G.711  $\mu$ -law 20 ms) is supported

✓ **Voice Activity Detection (VAD) is not supported**

✓ **T.38 for FAX specifications are:**

- T.38 Fax over UDP
- T.38 payload size 20 ms or 40 ms
- NSF value 0
- Fax rate management method Transferred TCF
- UDP redundancy method T38UDPRedundancy
- T.38 version parameter 0
- T.30 data V.21
- Data signaling rates: V.17 or V.29 or V.27ter
- Error Correction Method (ECM) Enabled
- Fax rate max 14400 bps
- SG3-G3 fallback method Either ANSam removal or CM removal
- Switching from voice mode to fax mode T.38 re-INVITE sent by called party

✓ **DTMF transport specifications are:**

RFC 2833/4733

✓ **Signalisation/ Media network Qos Tag specifications are:**

- ✓ DSCP 46 (EF)

✓ **SIP Probing**

- BTalk/BTIP SIP Trunk relies on OPTIONS method to “probe” the eSBC, in dialog and out of dialog.
- The following answers are expected:
  - Out of dialog: 200 OK (or any error responses) if UE is up, nothing if down
  - In dialog: 200 OK if Call is active and 481 if Call is not active
- The UE could use OPTIONS with max-forward=0 to probe BTalk/BTIP SIP Trunk, in this case, Business Talk will send back a 200 OK.
- 

✓ **Call initiation**

- eSBC shall provide an SDP within his initial INVITE, delay offer (INVITE without SDP) is not supported.



- ✓ **Media Session Modification/ Transfer – Call Forward:**
  - Modification of media (IP, codec, attributes ...) in reception/transmission based on UPDATE (With SDP) in Early Dialog and Re-INVITE in confirmed Dialog (with or without SDP)
  - Attributes "a=" must be equal to send only, recvonly, inactive, sendrecv.
  - In case of Call Forward, the diversion header must be provided by the UE.
  - Same Methods/Attributes/headers may be sent from BTalk/BTIP to UE.
  
- ✓ **Ring back Tone and Early Media**
  - Presence of an SDP in provisional response does not indicate presence of a distant early media (only p-early-media indicate presence of distant early media).
  - On reception of a 180 (without SDP) from BTalk/ BTIP, eSBC must play local Ring Back Tone.
  - eSBC can indicate an early media, within presence of P-Early-Media header into his provisional response.
  
- ✓ **Anonymous calls**
  - If anonymization is requested, the UE should:
    - Set privacy header to "user" with From containing Calling identity
    - Or: set privacy header to id with From containing anonymous ("anonymous" sip:anonymous@anonymous.invalid, P-A-I must contain the Calling party identification.
  - Same Settings could be used when BTalk/BTIP request anonymous calls.
  
- ✓ **Number format specifications are:**
  - Called Number sent to Orange network must be at E164 format
  - Calling Number sent to Orange network must be in National format (0ZABPQMCDU or 00xxxxxxx) or E164 format.
  
- ✓ **Rerouting scenario:**
  - On reception of a Sip Error message, User Equipement must reroute in case of 408 et 50x (500/501/502/503/504/505/513)
  - Transmission of a SIP error message to BTalk/BTIP, UE must send 5xx if a rerouting is expected from BTalk/BTIP service.
  - It's recommended to do not send 408 to BTalk/BTIP. If it's the case, UE will be considered out of service until next Sip probing.
  
- ✓ **Call defection:**
  - 3xx Sip messages are not supported by BTalk/BTIP services. Those messages will be converted into SIP error messages.

## 4. Certified Architecture

### 4.1 Introduction to architecture components and features

This document describes “only” the main supported architectures either strictly used by our customers or used as reference to add specific usages often required in enterprise context (specific redundancy, specific ecosystems, multi-PBX environment, multi-codec and/or transcoding, recording...)

Those configuration guidelines considered:

- **Only considering Carrier North side of AudioCodes eSBC facing Btalk and BTIP offers.**
- **Consider the eSBC as this SIP North eSBC termination as a demarcation point for OBS, South eSBC side is out of Orange control and responsibility**
- Stop considering the ecosystem behind the AudioCodes eSBCs on South Side (IPPBX vendor/version, mono vs multi vendors, complexity of the ecosystem,...)

Those configuration guidelines don't consider existing VISIT certified Premium vendor:

- Microsoft and Alcatel specific configuration guidelines for AudioCodes eSBC which cover both North and South side are available on OBS websites.

Concerning the fax support, BTalk and BTIP support the following usage:

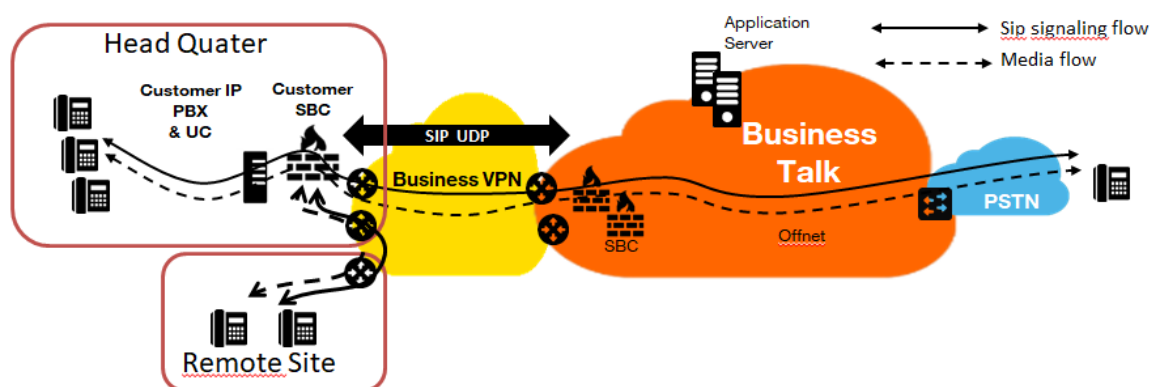
- fax servers connected to the IPBX\* -and sharing same dial plan-, or as separate ecosystems and separate dial plan.
- analog fax machines, usually connected behind and passing through AudioCodes eSBC
- Fax flows must handle via T.38 transport only.

**Note: Fax communications via Business Talk will still be allowed but will no longer be officially supported by the Orange support teams from April 2023 for new customer implementations.**

\* Please note: This AudioCodes eSBC SIP North Carrier Side template configuration main objective is offering compliancy in front of BTIP / Btalk offers. Accordingly multi- vendor IPBX which added complexity must be addressed on AudioCodes eSBC SIP/T38 South side and are considered outside of OBS responsibilities.

## 4.2 Architecture with Audiocodes “customer” eSBC with OBS SIP unencrypted configuration

### 4.2.1 Unencrypted SIP Trunk

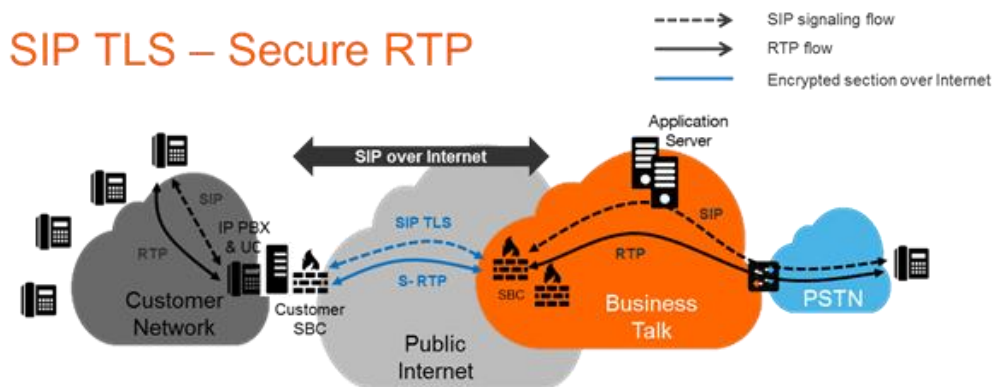


In this architecture:

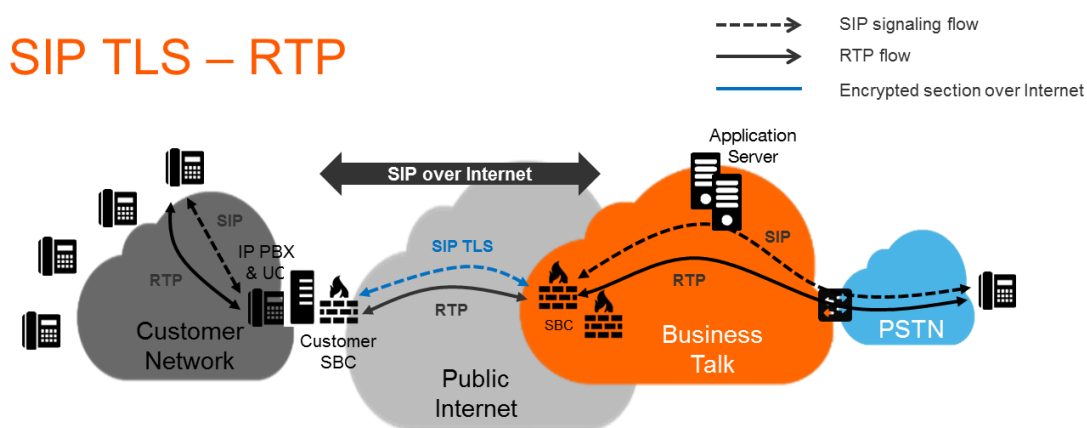
- both ‘SIP trunking’ and RTP media flows between endpoints and the BTalk/BTIP are anchored by the “customer eSBC”:
- for Head Quarter & remote sites, media flows are routed through the Customer eSBC and the main BVPN connection.

### 4.2.2 Encrypted SIP Trunk Over Internet

- SIP TLS + Secured RTP: all SIP messages and media packets are encrypted on the public internet between Orange and the customer Internet SIP & Media endpoints. This is the level of encryption recommended by default by Orange to ensure security & privacy



- SIP TLS + (unencrypted) RTP: all SIP messages are encrypted on the public internet between Orange and the customer internet SIP endpoints. RTP flows are shared without encryption between the customer media endpoints and Orange backbone. This solution is less recommended by Orange, but allowed as customers can have encryption/decryption limitations



#### 4.2.3 Parameters to be provided by customers to access the service

##### Unencrypted SIP Trunk through BVPN

Depending on Customer architecture scenario selected, several IP addresses (V4) have to be provided by the Customer. The table below sum-up the IP Address (marked in red) required according to the scenario.

##### Applicable to all Session Border Controller with BTIP or BTalk over BVPN

Customer eSBC – architecture with eSBC	Level of Service	@IP used by service	
1 Single Customer eSBC	No redundancy	eSBC @IP	
2 Customer eSBC Nominal / Backup mode	- <b>Local redundancy:</b> both eSBC are hosted on the same site OR - <b>Geographical redundancy</b> both eSBC are hosted on 2 different sites	eSBC1 @IP	eSBC2 @IP
2 Customer eSBC in Load Sharing	- <b>Local redundancy:</b> both eSBC are hosted on the same site OR - <b>Geographical redundancy</b> both eSBC are hosted on 2 different sites	eSBC1 @IP eSBC2 @IP	

##### Encrypted SIP Trunk through Internet

##### Applicable to Customer SBC with BTalk over internet only (International)

Customer SBC – architecture with eSBC	Level of Service	@IP used by service	
1 Single Customer eSBC	No redundancy	eSBC1 @IP or Public FQDN	
2 Customer eSBC Nominal / Backup mode	- <b>Local redundancy:</b> both eSBC are hosted on the same site OR - <b>Geographical redundancy</b> both eSBC are hosted on 2 different sites	eSBC1 @IP or Public FQDN	eSBC2 @IP or Public FQDN
2 Customer eSBC in Load Sharing	- <b>Local redundancy:</b> both eSBC are hosted on the same site OR - <b>Geographical redundancy</b> both eSBC are hosted on 2 different sites	eSBC1 @IP or Public FQDN eSBC2 @IP or Public FQDN	

## Applicable to Customer SBC with BTalk IP over internet only (French)

Customer SBC – architecture with eSBC	Level of Service	@IP used by service	
1 Single Customer eSBC	No redundancy	eSBC1 FQDN Type A	
2 Customer eSBC Nominal / Backup mode (DNS Resiliency model)	- <b>Local redundancy:</b> both eSBC are hosted on the same site OR - <b>Geographical redundancy</b> both eSBC are hosted on 2 different sites	eSBC public FQDN DNS Type SRV	
2 Customer eSBC Nominal / Backup mode (SIP Resiliency model)	- <b>Local redundancy:</b> both eSBC are hosted on the same site OR - <b>Geographical redundancy</b> both eSBC are hosted on 2 different sites	eSBC1 FQDN Type A *	eSBC2 FQDN Type A *
2 Customer eSBC in Load Sharing (SIP Resiliency model)	- <b>Local redundancy:</b> both eSBC are hosted on the same site OR - <b>Geographical redundancy</b> both eSBC are hosted on 2 different sites	eSBC1 FQDN Type A* eSBC2 FQDN Type A*	
2 Customer eSBC in HA mode (Cluster) (IP Resiliency model)	- <b>Local redundancy:</b> both eSBC are hosted on the same site OR - <b>Geographical redundancy</b> both eSBC are hosted on 2 different sites <b>warning:</b> Link level 2 between SBC with max delay 50ms required for geo-redundancy	eSBC VIP FQDN type A *	

\* Only eSBC public FQDN's SIP Termination will be supported, eSBC public IP's Termination will not.

### 4.3 BTalk & BTIP Audiocodes eSBC certified versions

Audiocodes eSBC – software versions				
Reference product	Hardware or Virtual Model	Software version	Certified "Loads"	Certification
Hybrid enterprise eSBC	<b>Mediant 500 /500L</b>	V.7.20A	Load(s) <u>7.20A.252.254*</u>	✓
	<b>Mediant 800</b>			
	<b>Mediant 1000</b>			
	<b>Mediant 3100</b>			
Pure enterprise eSBC	<b>Mediant 2600</b>	V.7.40A	Load(s) <u>7.40A.500.775*</u>	✓
	<b>Mediant 4000</b>			
	<b>Mediant 9000</b>			
	<b>Mediant Server Edition</b>			
	<b>Mediant Virtual Edition</b>			
	<b>Mediant Cloud Edition (MS Azure, AWS)</b>			

\* Minimum Load for implementation.

**Note:** Last most up-to-date Load is recommended per Audiocodes vendor : Lastest Release (LR) or Long Term Support (LTS) versions/ Loads.

## 4.4 Audiocodes Global configuration

### 4.4.1 Objects

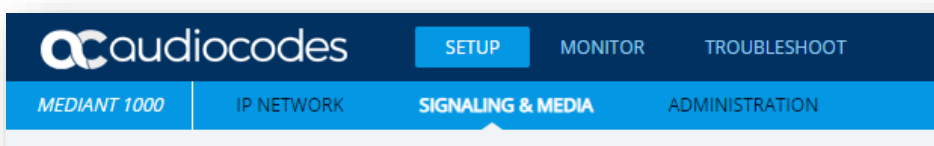
This chapter describes the AudioCodes eSBC necessary configuration steps for a correct interoperability with the Orange Business SIP Trunking offers.

AudioCodes configuration parts listed below will be detailed step by step:

- Coders and Profiles
- VoIP Network
- Core Entities
- Security
- Media
- SBC
- Message Manipulation

Note: All configuration parts listed above are present in the menu “**SETUP**” of the Audiocodes eSBC WebGui interface under the following tab:

“**IP NETWORK**”, “**SIGNALING & MEDIA**”, “**ADMINISTRATION**”



*AudioCodes Web User interface*

#### **Warning:**

Before applying the configuration described in this document, you need to do a Backup of your Audiocodes eSBC configuration (save the INI file on your laptop). When you have finished the configuration do a “Save” of your eSBC configuration and do again of Backup of your new configuration.

### 4.4.2 Information and Syntax

Inside the configuration pages described in the following Chapters, the tables include an “**Index**” column. Those “Index” is given as example. The real indexation will depend on the current Configuration present on the eSBC . This is had “no impact” on the configuration except in the “Message Manipulation” step where **you must respect the order** of rules in manipulations tables.

The **naming** of the different object created (Network interface, Rules names...) **must be respected** in order to guaranty the coherence of the configuration and easy to check by Orange in case of issue.



Few parameters highlighted in "Green" color (IP Address, capacity...) in this document are given as example and **must be replaced by the real value** specific of this interconnection.

Several tables in the following Chapters, will contain lines in "Grey" color. Those lines are indicated as **example and reminder of the existing configuration** of the "south" side (IPPBX side) inside the eSBC. If the eSBC used is a new one without existing configuration, you must replace those "Grey" lines according to the specifications of your IPBX/UC Device you want to interconnect to BT/BTIP network.

Index	Name	SIP Interface	TLS Context Name	Proxy Keep-Alive	Proxy Address	Transport Type
1	PS_BT	SI_BT	--	Using OPTIONS	** @IP_eSBC_BT:5060 **	UDP
	Or	Or			Or	
	PS_BTIP	SI_BTIP			** @IP_eSBC_BTIP:5060 **	
2	PS_IPBX	SI_IPBX	--	Using OPTIONS	** @IP_IPBX:5060 **	UDP

Example

## 4.5 Orange Business BTalk & BTIP Carrier **unencrypted** SIP configuration for AudioCodes eSBC (UDP)

### 4.5.1 Configure IP Network

Specific configuration is required in this section. Existing public IP Interface, Ethernet Device and Device Group could be reused.

It is anyway recommended to have a dedicated public IP Interface for SIP Trunking Service provider like Orange in order to differentiate Traffic between Sip Internal Traffic and public Sip traffic of the Service Provider.

### 4.5.2 Message Manipulation Policy

#### **Message Policy**

Orange BTALK specifications require to **limit the size of the SIP message** to 4096 Bytes and SDP Body to 1024 Bytes. To do so, it is necessary to create a dedicated "Message Policy" name "BTALK Max SIP Size". This Message Policy will be associated to the "SIP Interface" dedicated to Orange BTALK interconnexion.

The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

Index	Name	Max Message Length	Max Body Length	Send Rejection
2	BTALK(or BTIP) Max SIP Size	4096	1024	Policy Reject

Actions	Screenshot
<ol style="list-style-type: none"> <li>Open SETUP &gt; SIGNALING &amp; MEDIA &gt; MESSAGE MANIPULATION &gt; MESSAGE POLICIES</li> <li>Click on "+ New"</li> <li>Enter a meaningful name ex" BTALK Max SIP Size"</li> <li>Click on "Apply"</li> </ol>	
<p>The number Policy will appear in the list</p>	

### 4.5.3 Coders and Profiles

This section describes configuration of the Voice Settings: Coders and SIP profiles.

#### **Allowed Audio Coders Groups**

Allowed Audio Coders Groups are used to remove codecs from an SDP offer and/or to modify the order or preference in the codecs list.

Orange accepts the following codecs in this order or preference:

*VoIP Codec Profile specific to Orange BTIP /.BTalk:*

- **G.722 (If only used through BTIP only, not supported for BTalk)**
- **G.711 A-law 20 ms**
- **G.729 20 ms (annexb = no).**

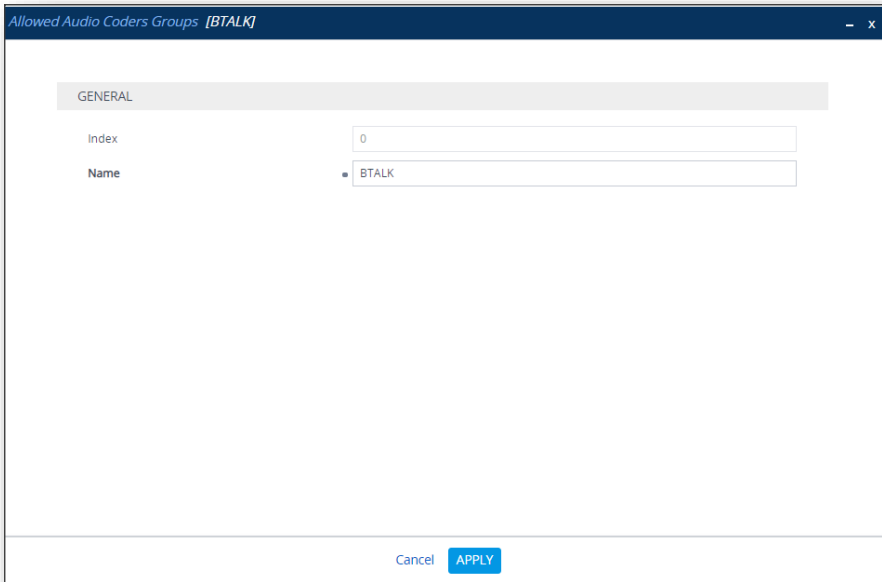
**Note:** G.711  $\mu$ -law 20 ms can be requested to OBS, specifically on demand. If this is the case, it should just be added to the codec list in this VoIP profile. **G.722 isn't currently supported through Business Talk over Internet context.**

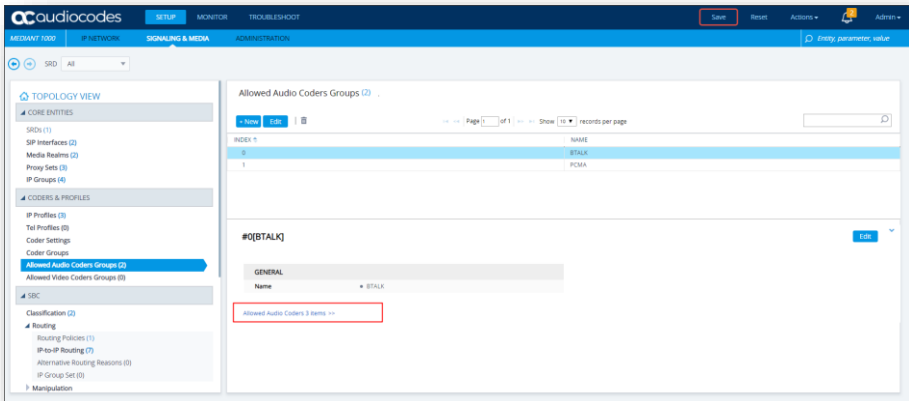
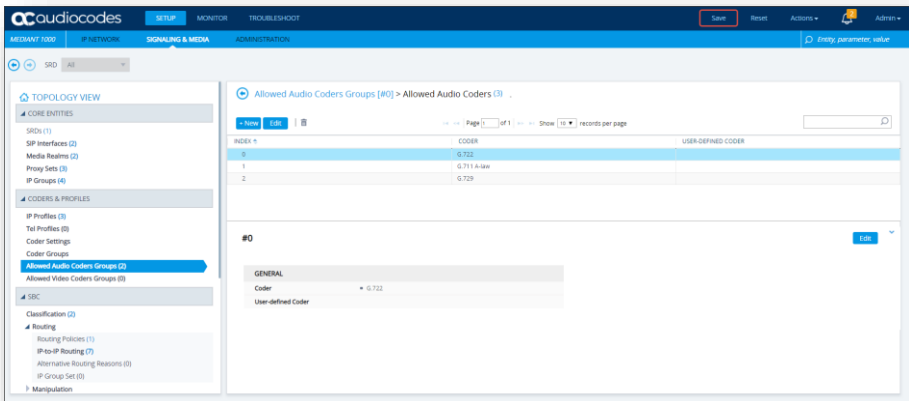
We are going to create a new "Coders Groups" specific to Orange BTIP (please adapt it for BTalk).

Index	Name
0	BT or BTIP

This "Coders Groups" will manage the Codec specific to Orange BTIP.

Index	Coder	User-defined Coder
0	G.722	(Empty)
1	G.711 A-Law	(Empty)
2	G.729	(Empty)

Actions	Screenshot
<ol style="list-style-type: none"> <li>1. Open SETUP &gt; SIGNALING &amp; MEDIA &gt; CODERS &amp; PROFILES &gt; Allowed Audio Coders Groups</li> <li>2. Click on "+ New"</li> <li>3. Enter a meaningful name ex" BTALK" or "BTIP"</li> <li>4. Click on "Apply"</li> <li>5. Click on "Allowed Audio Coders 0 items"</li> </ol>	

Actions	Screenshot
<p>6. Click on “+ New”</p> <p>7. Select the coders as mention in the table of parameters above, in the same order</p> <p><b>Please note:</b> Do not select “G711 A-law VBD” or “EG-711 A-law” as they are not regular G711a codecs</p>	 

Allowed Audio Coders Groups in case of multiple codecs into SDP Audio MLine (Optional)  
 Even if this not the standard behaviors, some customer IPBX/device could send several “codec” in the SDP answer (SDP with multiple codecs into Audio M Lines). This behavior is not supported by Orange BT/BTIP network. As solution on the Audiocodes eSBC, it is required to implement a different “Allowed Coder Group” to filter the answers. This will force all calls to the selected a unique “G711 A-law” codec.

**Note:** If you are in this case you don’t need to create the “BT/BTIP” “Allow Coders Group” described in the previous chapters.

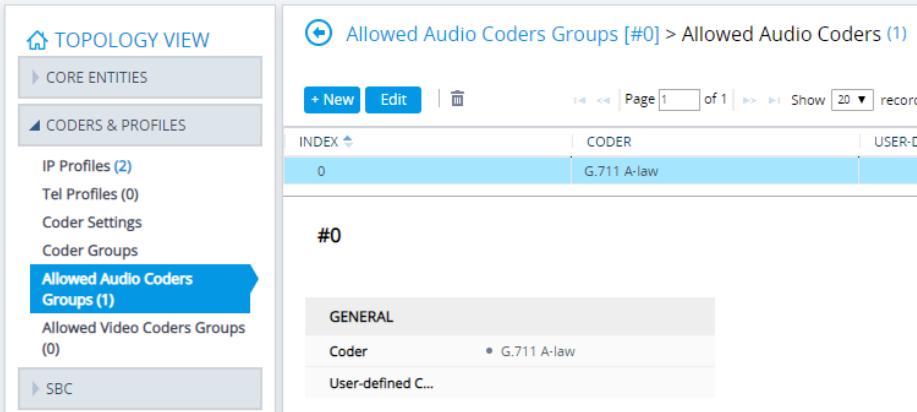
We are going to create a new “Coders Groups” specific to Orange BTalk.

Index	Name
<b>1</b>	PCMA

This “Coders Groups” will managed only 1 Codec supported in Orange BT/BTIP.

Index	Coder	User-defined Coder
0	G.711 A-Law	(Empty)

Actions	Screenshot
<ol style="list-style-type: none"> <li>Open SETUP &gt; SIGNALING &amp; MEDIA &gt; CODERS &amp; PROFILES &gt; Allowed Audio Coders Groups</li> <li>Click on “+ New”</li> <li>Enter a meaningful name ex” PCMA”</li> <li>Click on “Apply”</li> <li>Click on “Allowed Audio Coders 0 items”</li> </ol>	
<ol style="list-style-type: none"> <li>Click on “+ New”</li> <li>Select the coders as mentioned in the table of parameters above, in the same order</li> </ol> <p><b>Please note:</b> Do not select “G711 A-law VBD” or “EG-711 A-law” as they are not regular G711a codecs</p>	

Actions	Screenshot
	

### IP Profile Settings

The IP Profile settings is a set of parameters with user-defined settings relating to signaling and media. The IP Profile will be assigned later to specific IP calls.

This IP Profile will re-use the “Allowed Audio Coders” object created in the previous chapter in order to compliant with Orange BT or BTIP codec list. In case of **Standard installation** will use the “**BTALK**” as example or in **particular case** the “**PCMA**” Allow Audio Coders.

This IP Profile will be configured to be compliant with Orange BTIP/BTalk specification:

- ✓ Transfer allowed via Re-invite
- ✓ DTMF via RFC 2833/4733
- ✓ Transport tag require EF (DSCP 46) for Media and Signaling

**Note:**

*For **DTMF**, the Audiocodes eSBC will be able to **convert SIP INFO** message to RFC2833/4733. DTMF inbound will be not converted by the eSBC because it requires DSP resources on SBC.*

*For **Transfer**, the Audiocodes eSBC will be able to **convert REFER** into RE-Invite.*

*In some case SIP Provisional Response ACKnowledgement (PRACK RFC 3262)) could be required (For Cisco CUCM) to be interworked with Orange which not support PRACK. SBC device can be configured to resolve this interoperable issue and enable sessions between such endpoints. SIP PRACK handling is configured using the IP Profile parameter, **eSBC Prack Mode** :*

**Mandatory** on the IP profile of the Customer IPPBX

**All of those conversions will stay under customer responsibilities depending of South private architecture context**

The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

“Section: **eSBC Media**”

Index	Name	Allowed Audio Coders	Allowed Coders Mode	RFC2833 Mode	RFC2833 DTMF Payload Type	Use Silence Suppression	RTP Redundancy Mode
1	IPP_BTALK Or IPP_BTIP	BTALK Or BTIP	Restriction	Extend	101	Remove	Disable

“Section: **Quality of Service**”

Signaling DiffServ

46

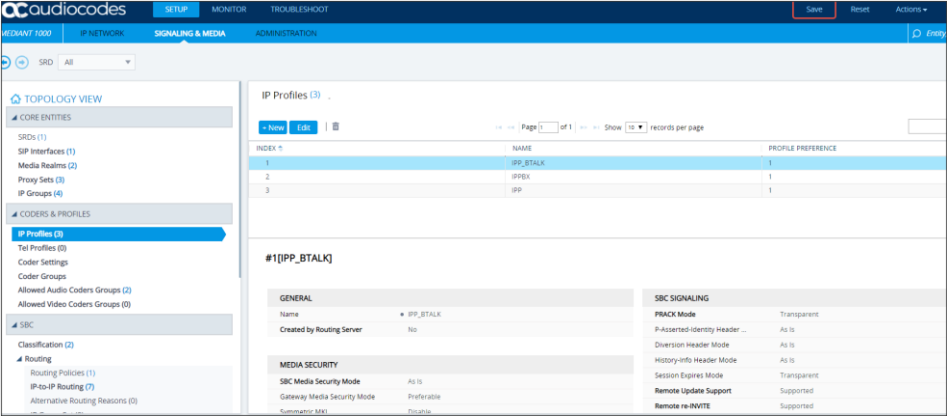
“Section: **eSBC Forward and Transfer**”

Remote REFER Mode	Remote 3xx Mode
Handle Locally	Handle Locally

Actions	Screenshot
<ol style="list-style-type: none"> <li>Open SETUP &gt; SIGNALING &amp; MEDIA &gt; CODERS &amp; PROFILES &gt; IP Profiles</li> <li>Click on “+ New” Enter a meaningful name, ex” <b>IPP_BTALK</b>” or <b>“IPP_BTIP”</b></li> <li>Change the parameters indicated above as follow</li> </ol>	



Actions	Screenshot

Actions	Screenshot												
<p>Click on “Apply” The new Objects will appear in the list.</p>	 <p>The screenshot shows the AudioCodes management console. The left sidebar contains a navigation menu with categories like 'CORE ENTITIES', 'CODERS &amp; PROFILES', 'SBC', and 'Routing'. The 'IP Profiles' section is selected. The main area displays a table of IP Profiles with columns for INDEX, NAME, and PROFILE PREFERENCE. Below the table, the configuration details for the selected profile '#1[PP_BTALK]' are shown, including sections for GENERAL, MEDIA SECURITY, and SBC SIGNALING.</p> <table border="1" data-bbox="786 533 1490 595"> <thead> <tr> <th>INDEX</th> <th>NAME</th> <th>PROFILE PREFERENCE</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>PP_BTALK</td> <td>1</td> </tr> <tr> <td>2</td> <td>IPPEX</td> <td>1</td> </tr> <tr> <td>3</td> <td>IPP</td> <td>1</td> </tr> </tbody> </table>	INDEX	NAME	PROFILE PREFERENCE	1	PP_BTALK	1	2	IPPEX	1	3	IPP	1
INDEX	NAME	PROFILE PREFERENCE											
1	PP_BTALK	1											
2	IPPEX	1											
3	IPP	1											

#### 4.5.4 Core Entities

##### SRD Table

No configuration is required in this section. We will use the existing “DefaultSRD”

##### SIP Interface Table

The SIP Interface table allows to define a local, listening port number and type (e.g. UDP or TCP), and assigning an IP Network interface for SIP signaling traffic.

This SIP signaling will be configured to be compliant with Orange BTalk specifications:

- ✓ For **unencrypted BT SIP Trunk** architecture, we need to configure **UDP port 5060**

The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

Index	Name	Network Interface	UDP Port	TCP Port	TLS Port	TLS Context	Classification Failure Response Type	Message Policy
2	SI_BTALK Or SI_BTIP	NI_Existing	5060	0	0	-	0	BTALK/BTIP Max SIP Size
1	SI_IPBX	NI_IPBX	5060	0	0	-	0	

**Note:** “Network Interface” will define by the Customer itself.

Actions	Screenshot
<ol style="list-style-type: none"> <li>Open SETUP &gt; SIGNALING &amp; MEDIA &gt; CORE ENTITIES &gt; SIP Interfaces</li> <li>Click on "+ New" Enter a meaningful name Ex: <b>SI_BTALK</b> or <b>SI_BTIP</b></li> <li>Change the parameters indicated above as follow</li> </ol>	
<p>Click on "Apply" The new Objects will appear in the list.</p>	

**Media Realm Table**

The Media Realm Table allows allowed range media defined on gateway depending on traffic.

This Media will be configured to be compliant with Orange BTalk specification:

- ✓ For **unencrypted BT/BTIP SIP Trunk** architecture, we need to configure **RTP port 6 000 to 20 000**

**Note:** On Audiocodes eSBC, for RTP port range keep in mind that the RTP UDP port spacing is “10”. This mean that for example 5 sessions SIP, 5\*10 ports RTP from 6000 to 60050 will be reserved.

The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

Index	Media Realm Name	IP Interface Name	Port Range Start	Media Session Legs
2	MR_BT Or MR_BTIP	NI_Existing	7000	100
1	MR_IPBX	NI_IPBX	8000	100

**Note:** The table above shows the configuration for 100 calls maximum with Orange. The “Media Session Legs” should be adapted to your Customer service offer. “Port Range Start” and “IP interface name” will defined by the Customer itself.

Actions	Screenshot
<ol style="list-style-type: none"> <li>1. Open SETUP &gt; SIGNALING &amp; MEDIA &gt; CORE ENTITIES &gt; MEDIA REALMS</li> <li>2. Click on “+ New” Enter a meaningful name ex” <b>MR_BTALK</b>” or <b>MR_BTIP</b></li> <li>3. Change the parameters indicated above as follow</li> </ol>	

Actions	Screenshot
<p>Click on "Apply" The new Objects will appear in the list.</p>	

### Proxy Set Table and Address

The Proxy Set Table allows proxy set definition. There you will configure the IP/ FQDN of Orange BTALK extremity and Keep-alive.

This Proxy will be configured to be compliant with Orange BTalk specification:

- ✓ For **unencrypted BT/BTIP SIP Trunk** architecture, we need to configure **UDP port 5060**
- ✓ For Sip trunk keep alive done with “**Options**” message (every 300 seconds)
- ✓ For Sip trunk redundancy **Homing** (the first Proxy Address is always select if available) and Proxy Hot swap **Enable** ( In case of Invite reject or no answer ,the call is moved to the next Proxy Address)
- ✓ 2 Proxy Address will be configured for redundancy purpose

Index	Name	SIP Interface	TLS Context Name	Proxy Keep-Alive	Redundancy Mode	Proxy Hot Swap	Index Proxy Address	Proxy Address	Transport Type
1	PS_BTALK	SI_BTALK	--	Using OPTIONS	Homing	Enable	0	<BT_Nominal IP>:5060	UDP
							1	<BT_Backup IP>:5060	
	Or	Or					0	<BTIP_Nominal IP>:5060	UDP
							1	<BTIP_Backup IP>:5060	
2	PS_IPBX	SI_IPBX	--	Using OPTIONS			** @IP_IPBX:5060 **	UDP	

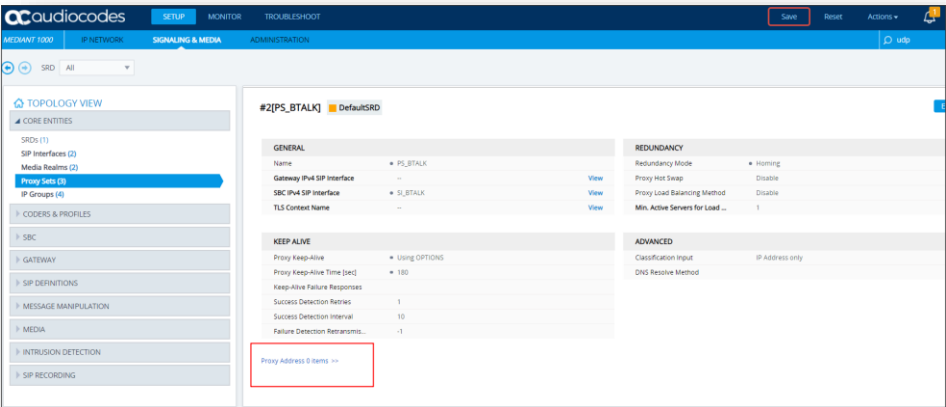
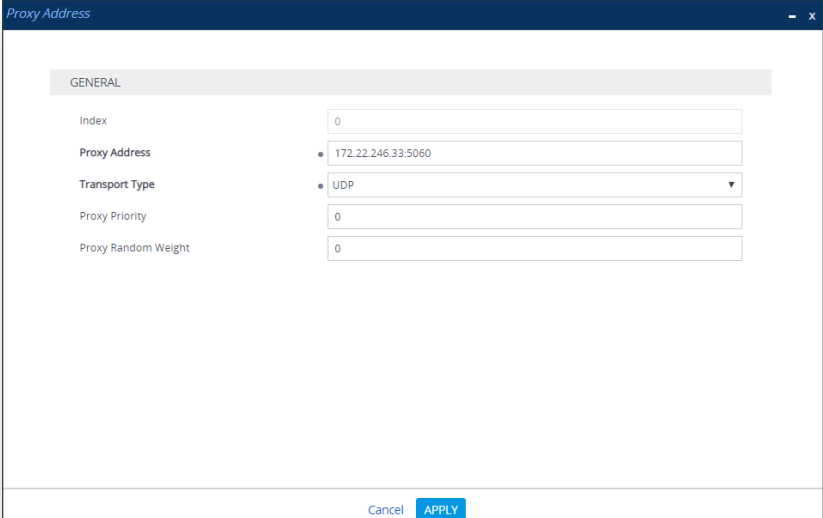
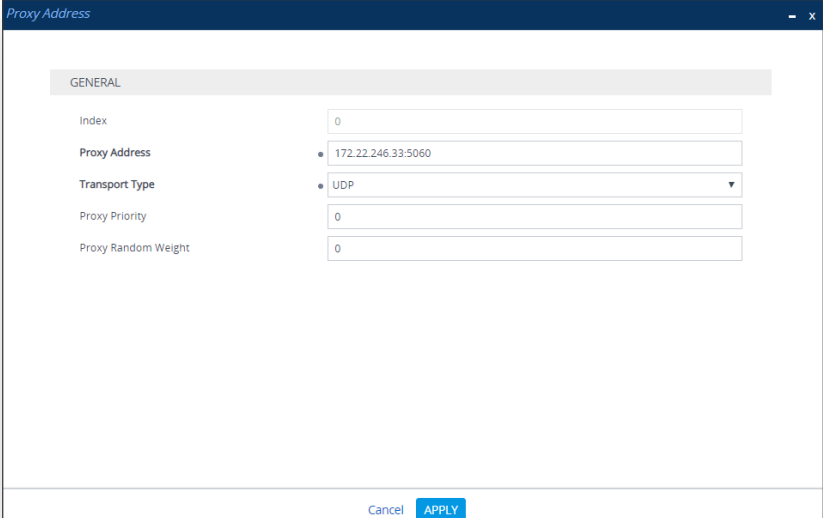
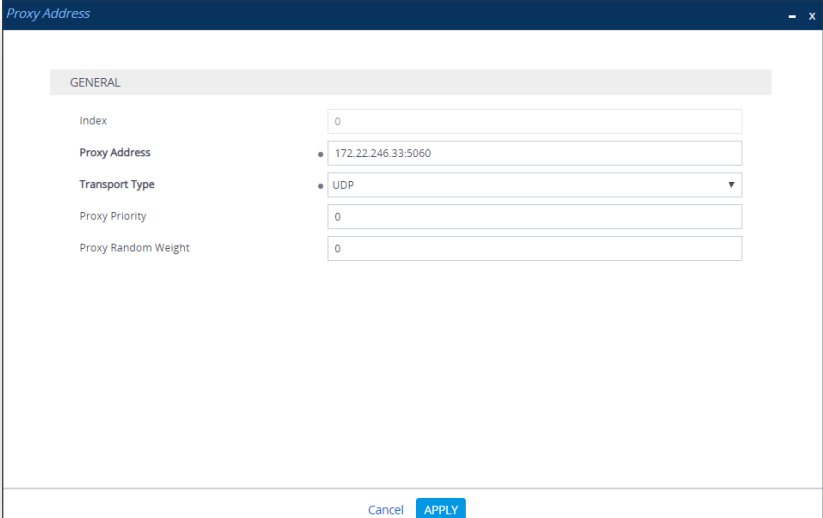
The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

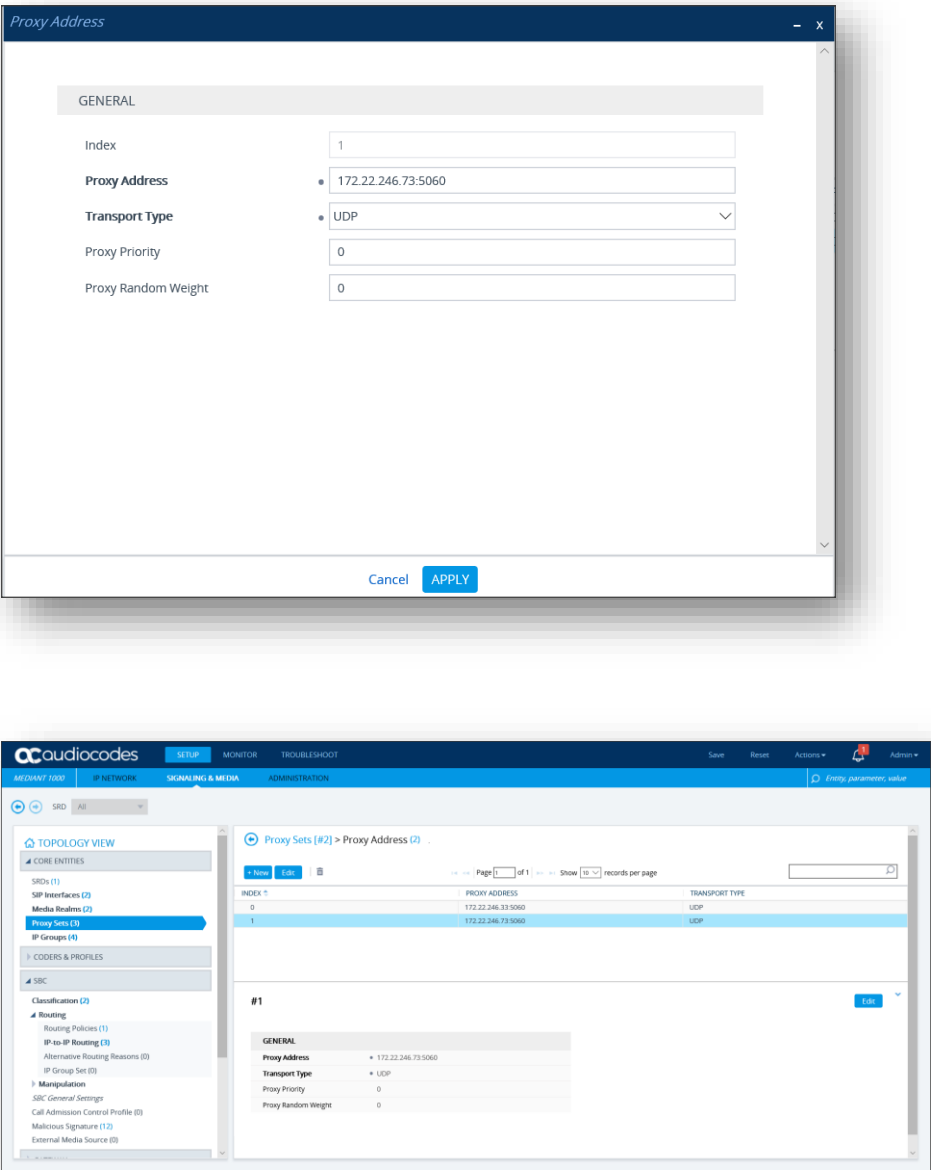
**Note:** Please avoid using Proxy Set 0 Index. The IP set in the “Proxy Address” is the IP provided by Orange for the SIP trunk BT/BTIP. “Options” message will be sent by the Audiocodes eSBC to verify if the Orange BT/BTIP network is reachable.

**All the screenshots below showing some IP address are given as example. You should replace them by the correct IP or FQDN**

Actions	Screenshot
<ol style="list-style-type: none"> <li>Open SETUP &gt; SIGNALING &amp; MEDIA &gt; CORE ENTITIES &gt; PROXY SETS</li> <li>Click on "+ New" Enter a meaningful name ex "PS_BTALK" or "PS_BTIP"</li> <li>Change the parameters indicated above as follow</li> </ol>	
<ol style="list-style-type: none"> <li>Click on "Apply". The new Objects will appear in the list.</li> </ol>	
<ol style="list-style-type: none"> <li>To configure "Proxy Address" and "Transport Type", you have to configure to select the "Proxy Set" just created.</li> </ol>	



Actions	Screenshot
<p>6. Click on the “Proxy Address 0 items” link at the bottom of the page.</p>	
<p>7. Configure though <b>index 0</b> for the <b>nominal Proxy address</b> &lt;BT_Nominal_IP&gt; or &lt;BTIP_Nominal_IP&gt;</p>	
<p>8. You have to configure though <b>Index 1</b> for the <b>backup Proxy address</b> to backup the nominal ones with &lt;BT_Backup_Public_IP&gt; or &lt;BTIP_Backup_Public FQDN &gt;</p>	
<p>1. At the End at least 2 Proxy Items should be configured:</p> <ul style="list-style-type: none"> <li>- Index 0 for Nominal within <b>BT nominal IP</b> (first IP) or <b>BTIP nominal IP</b> (Second IP)</li> <li>- Index 1 for <b>BT backup IP</b> (first IP) or <b>BTIP backup IP</b> (Second IP)</li> </ul>	

Actions	Screenshot									
	 <p>The top screenshot shows a 'Proxy Address' configuration dialog with the following fields:</p> <ul style="list-style-type: none"> <li>Index: 1</li> <li>Proxy Address: 172.22.246.73:5060</li> <li>Transport Type: UDP</li> <li>Proxy Priority: 0</li> <li>Proxy Random Weight: 0</li> </ul> <p>The bottom screenshot shows the main interface with a table of Proxy Sets:</p> <table border="1"> <thead> <tr> <th>INDEX</th> <th>PROXY ADDRESS</th> <th>TRANSPORT TYPE</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>172.22.246.33:5060</td> <td>UDP</td> </tr> <tr> <td>1</td> <td>172.22.246.73:5060</td> <td>UDP</td> </tr> </tbody> </table> <p>Below the table, the configuration for index #1 is shown, matching the dialog above.</p>	INDEX	PROXY ADDRESS	TRANSPORT TYPE	0	172.22.246.33:5060	UDP	1	172.22.246.73:5060	UDP
INDEX	PROXY ADDRESS	TRANSPORT TYPE								
0	172.22.246.33:5060	UDP								
1	172.22.246.73:5060	UDP								

**IP Group Table**

The IP Group table allows logical IP entities creation with a set of parameters such as Proxy set ID, IP profile ID to separate provenance and destination traffic.

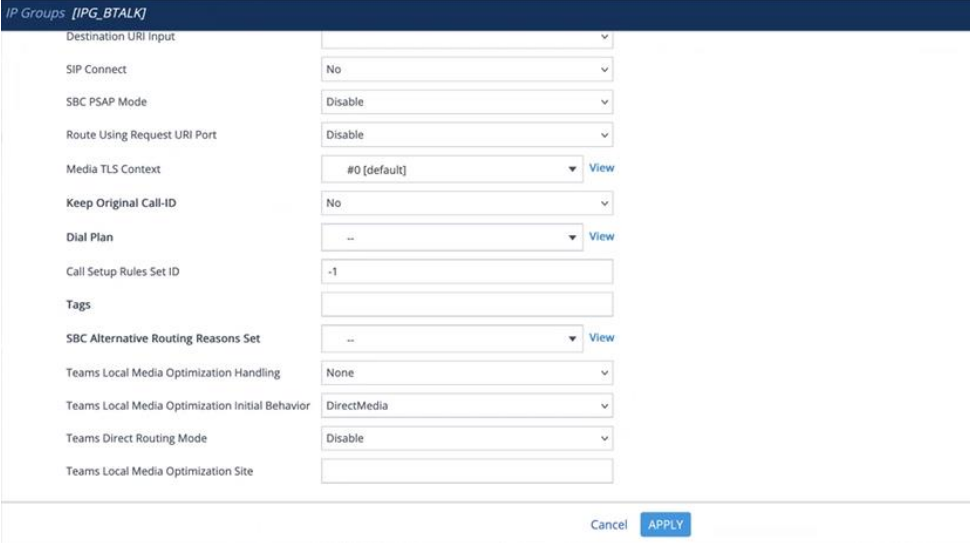
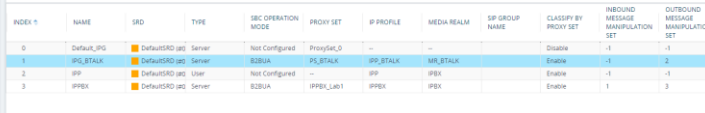
A new IP Group specific to Orange BT/BTIP SIP Trunk needs to be create as **Server Back-to-back (B2BUA)** with message **Manipulation on the outgoing Orange side**. The IP Group will be composed of the objects previously created in the table: Media Realm, Proxy Set and IP Profile.

The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

Index	Name	Proxy Set	Media Realm	IP Profile	Inbound Message Manipulation Set	Outbound Message Manipulation Set	Proxy Keep-Alive using IP Group settings
1	IPG_BTALK Or IPG_BTIP	PS_BTALK Or PS_BTIP	MR_BTALK Or MR_BTIP	IPP_BTALK Or IPP_BTIP	-1	2	Enable
2	IPG_IPBX	PS_IPBX	MR_IPBX	IPP_IPBX	1	3	Enable

**Note:** Please avoid using IP Group Index “0”. The value “-1” inside the «Inbound Message Manipulation set” parameter indicate that “None” Manipulation is needed for incoming message from Orange BT/BTIP. The value “2” inside the «Outbound Message Manipulation Set” parameter indicate a set of Manipulations (inside the Man Set ID “2”) are required for outgoing message toward Orange BTalk Network. Those Manipulations are described in the next chapters.

Actions	Screenshot
<ol style="list-style-type: none"> <li>1. Open SETUP &gt; SIGNALING &amp; MEDIA &gt; CORE ENTITIES &gt; IP_GROUP</li> <li>2. Click on "+ New" Enter a meaningful name ex "IPG_BTALK" or "IPG_BTIP"</li> <li>3. Click on "Apply"</li> <li>4. Click on "Allowed Audio Coders 0 items"</li> </ol>	<p>The screenshots show the configuration interface for IP Groups. The first screenshot is the 'GENERAL' tab, the second is the 'SBC GENERAL' and 'ADVANCED' tabs, and the third is the 'SBC ADVANCED' tab. Red boxes in the first screenshot highlight the 'GENERAL' fields and the 'MESSAGE MANIPULATION' section.</p>

Actions	Screenshot																																																												
																																																													
<p>5. Click on “Apply”. The new Objects will appear in the list.</p>	 <thead> <tr> <th>INDEX #</th> <th>NAME</th> <th>SRD</th> <th>TYPE</th> <th>SBC OPERATION MODE</th> <th>PROXY SET</th> <th>IP PROFILE</th> <th>MEDIA REALM</th> <th>SIP GROUP NAME</th> <th>CLASSIFY BY PROXY SET</th> <th>INBOUND MESSAGE MANIPULATION SET</th> <th>OUTBOUND MESSAGE MANIPULATION SET</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Default_IPG</td> <td>DefaultSRD (as)</td> <td>Server</td> <td>Not Configured</td> <td>ProxySet_0</td> <td>--</td> <td>--</td> <td>--</td> <td>Disable</td> <td>-1</td> <td>-1</td> </tr> <tr> <td>1</td> <td>IPG_BTALK</td> <td>DefaultSRD (as)</td> <td>Server</td> <td>B2BUA</td> <td>IPG_BTALK</td> <td>IPG_BTALK</td> <td>IPG_BTALK</td> <td>IPG_BTALK</td> <td>Enable</td> <td>-1</td> <td>2</td> </tr> <tr> <td>2</td> <td>IPP</td> <td>DefaultSRD (as)</td> <td>User</td> <td>Not Configured</td> <td>--</td> <td>IPP</td> <td>IPEX</td> <td>IPEX</td> <td>Enable</td> <td>-1</td> <td>-1</td> </tr> <tr> <td>3</td> <td>IPEX</td> <td>DefaultSRD (as)</td> <td>Server</td> <td>B2BUA</td> <td>IPPEX_LAB1</td> <td>IPEX</td> <td>IPEX</td> <td>IPEX</td> <td>Enable</td> <td>1</td> <td>3</td> </tr> </tbody>	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 (as)	Server	Not Configured	ProxySet_0	--	--	--	Disable	-1	-1	1	IPG_BTALK	DefaultSRD (as)	Server	B2BUA	IPG_BTALK	IPG_BTALK	IPG_BTALK	IPG_BTALK	Enable	-1	2	2	IPP	DefaultSRD (as)	User	Not Configured	--	IPP	IPEX	IPEX	Enable	-1	-1	3	IPEX	DefaultSRD (as)	Server	B2BUA	IPPEX_LAB1	IPEX	IPEX	IPEX	Enable	1	3
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 (as)	Server	Not Configured	ProxySet_0	--	--	--	Disable	-1	-1																																																		
1	IPG_BTALK	DefaultSRD (as)	Server	B2BUA	IPG_BTALK	IPG_BTALK	IPG_BTALK	IPG_BTALK	Enable	-1	2																																																		
2	IPP	DefaultSRD (as)	User	Not Configured	--	IPP	IPEX	IPEX	Enable	-1	-1																																																		
3	IPEX	DefaultSRD (as)	Server	B2BUA	IPPEX_LAB1	IPEX	IPEX	IPEX	Enable	1	3																																																		

 Below the table, the configuration for the selected group #1[IPG\_BTALK] is shown, including fields for Name (IPG\_BTALK), Type (Server), Proxy Set (IPG\_BTALK), and IP Profile (IPG\_BTALK).
 

### 4.5.5 SIP Message Manipulation

For unencrypted or encrypted BT SIP Trunk architecture, it is required to implement some Message Manipulation for the outgoing message toward Orange BTalk. Those Manipulations Rules are detailed on the chapter “*SIP rules & manipulations (eSBC Application)*”. Please jump to this Chapter directly

## 4.6 Orange Business- BTalk over Internet & BTIP over Internet **encrypted** SIP configuration for AudioCodes eSBC (TLS)

As a prerequisite Audiocodes recommends reading the [Audiocodes Security vulnerability handling](#) to understand how to secure the eSBC into your network infrastructure and especially facing Internet.

### 4.6.1 Configure IP Network

Same recommendations as in § 4.5.1

Specifically in the TLS profile used for BTol / BTIPol (SIP/TLS) the **WAN interface is usually exposed to the public internet from a DMZ, so it is strongly recommended to use an Access Control List on eSBC in order to restrict access only to Orange public IP's**

### 4.6.2 TLS profile

#### TLS Context

The encrypted architecture requires the usage of an encryption Key and Ciphers present in a TLS Context in order. A specific Orange BTALK TLS Context have to created.

This SIP signaling will be configured to be compliant with Orange BTalk specification:

- ✓ For **encrypted BTALK SIP Trunk** architecture we need to configure **TLS V1.2**
- ✓ **Key size 2048**
- ✓ **Cipher list bellow are supported as Client/Server through TLS V1.2:**
  - TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (Recommended)
  - TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
  - TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
  - TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
  - TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
  - TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
  - TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
  - TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- ✓ **TLS Mutual authentication activated.**

The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

Index	Name	Cipher Server	Cipher Client	DH key Size
1	Orange2	ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA-AES256-GCM-SHA384	2048

Actions	Screenshot
<ol style="list-style-type: none"> <li>Open SETUP &gt; IP NETWORK &gt; SECURITY &gt; TLS CONTEXTS</li> <li>Click on "+ New" Enter a meaningful name ex" <b>Orange</b>"</li> <li>Change the parameters indicated above as follow</li> </ol>	
<p>Click on "Apply" The new Objects will appear in the list.</p>	

**Certificate Signing Request (CSR)**

The TLS Context need a Certificate signed. To obtain this Certificate Authority (CA) you must generate your CSR base on the information of the eSBC and Company with SHA-256 encryption. As soon you received the CA, you will load it on the Audiocodes eSBC on the TLS Context create for this interconnexion with Orange BTALK.

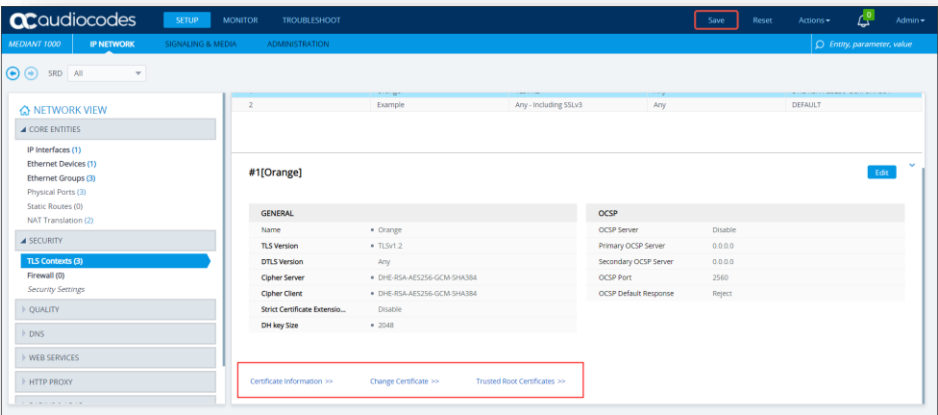
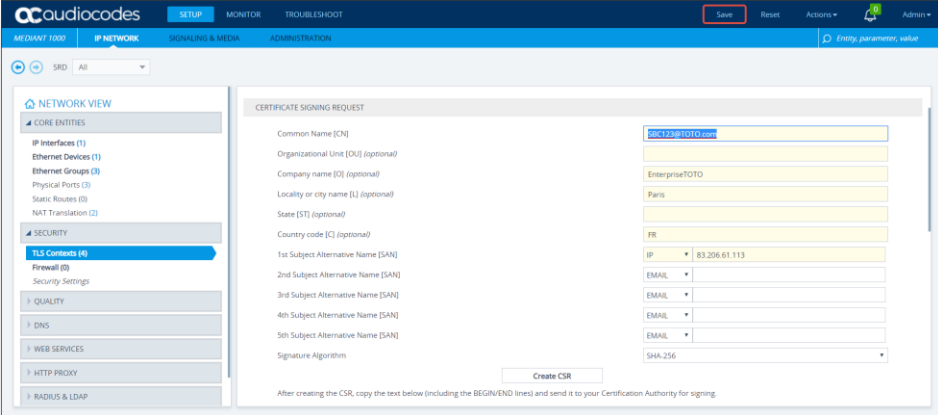
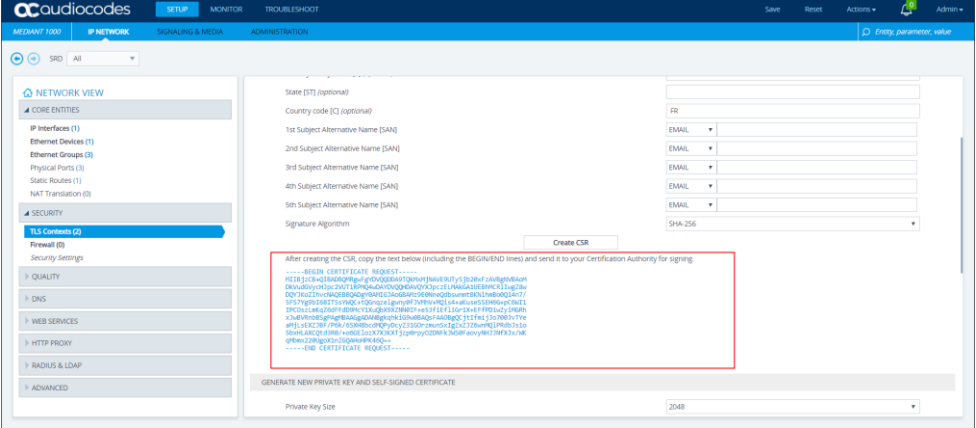
The mentioned parameters in the table below are the one specific to Customer. It is just an example of CSR for a Company "EnterpriseTOTO" located in Paris France with an eSBC with FQDN name "SBC123@TOTO.com" resolving Public IP 83.206.61.113

Common Name	Organizational Unit	Company name	Locality or city name	Country code
<b>SBC123@TOTO.com</b>	<b>-Group X</b>	<b>Enterprise TOTO</b>	<b>Paris</b>	<b>FR</b>



1st Subject Alternative Name	2nd Subject Alternative Name	3rd Subject Alternative Name	Signature Algorithm	Private Key size
IP 83.206.61.113			SHA-256	2048



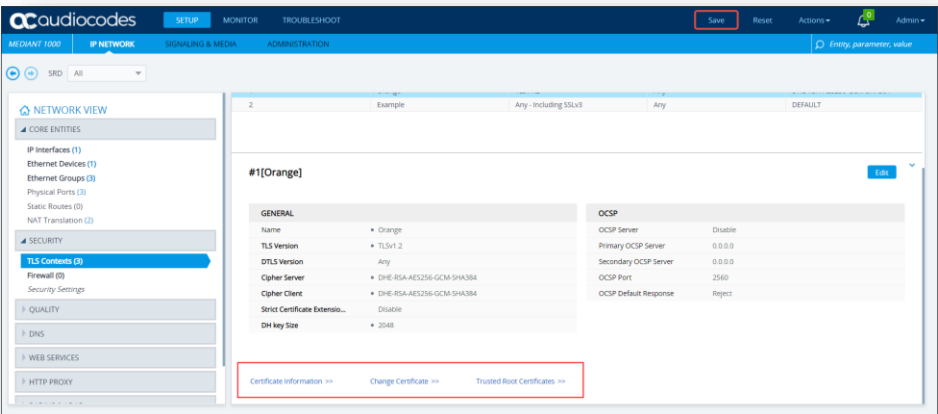
Actions	
<ol style="list-style-type: none"> <li>On the TLS context you just create go on the Bottom page and click on "Change Certificate"</li> <li>Change the parameters indicated above</li> <li>Click "Create CSR"</li> </ol>	 
<ol style="list-style-type: none"> <li>On the page should appear a text in blue which represent your CSR.</li> </ol>	

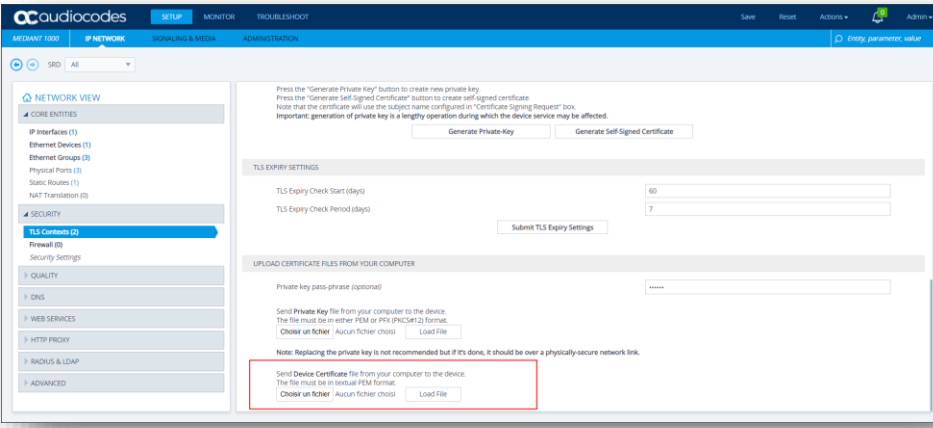
When the CSR is generated copy the CSR text and send it to Organization to be signed and get a Certificate Authority (CA). The Root and intermediate Certificate (crt files) must be transmitted to Orange Business Services team.

When you have the CA files (p7b and bundle), please load it on the TLS Context just create. Only **Base64 (PEM)** encoded X.509 certificates can be loaded to the Audiocodes eSBC.

Make sure that the file is a plain-text file containing the "BEGIN CERTIFICATE" header, as shown in the example of a Base64-Encoded X.509 Certificate below:

```
-----BEGIN CERTIFICATE-----
MIIDkzCCAnugAwIBAgIEAgAAADANBgkqhkiG9w0BAQQFADA/MQswCQYDVQQGEwJGUjETMBEGA1UEChMKQ2VydG1wb3N0ZTEbMBkGA1UEAxMSQ2VydG1wb3N0ZSBTZXJ2ZXVYMB4XDTE4MDYyNDA4MDAwMFoXDTE4MDYyNDA4MDAwMFowPzELMAkGA1UEBhMCRLIxEzARBgNVBAoTCkN1cnRpcG9zdGUxGzAZBgNVBAMTEkN1cnRpcG9zdGUxGzU2VydMv1cjCCASEwDQYJKoZIhvcNAQEBBQADggEADCCAQkCggEAPqd4MziR4spWldGRx8bQrhZkonWnNm`+Yhb7+4Q67ecf1janH7GcN/SXsfx7jJpreWULf7v7Cvpr4R7qIJcmdHIntmf7JPM5n6cDBv17uSW63er7NkVnMFHwK1QaGFLMybFkzaeGrvFm4k3lRelfiXDmuOe+FhJgHYezYHf44LvPRPwhSrzi9+Aq3o8pWDguJuZDIUP1F1jMa+LPwvREXfFcUW+w==
-----END
```

Actions	
<ol style="list-style-type: none"> <li>5. On the TLS context you created go on the Bottom page and click on "Change Certificate"</li> <li>6. Scroll down to the Upload certificates files from your computer group, click the <b>Browse</b> button corresponding to the 'Send Device Certificate...' field, navigate to the cert.txt file, and then click <b>Load File</b>.</li> <li>7. After the certificate successfully loads to the device, save the configuration with a device reset.</li> <li>8. Verify that the private key is correct: -Open the TLS Contexts table.</li> </ol>	

Actions	
<p>-Select the required TLS Context index row.</p> <p>-Click the Certificate Information link located below the table.</p>	

After this step, the Public Root and intermediate Certificate authorities (PEM format) which signed your eSBC FQDN/ Public IP must be communicated to Orange BTALK/BTIP project team.

### 4.6.3 Media Security

This section allows to Enable the media security protocol (SRTP). This is needed only in case the connection with BTALK is using encrypted connection via TLS encryption.

The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

Media security	Media Security behavior	Offered SRTP Cipher Suite
<b>Enable</b>	Preferable	all

Actions	Screenshot
<ol style="list-style-type: none"> <li>1. Open SETUP &gt; SIGNALING &amp; MEDIA &gt; MEDIA &gt; MEDIA SECURITY</li> <li>2. Change the parameters indicated above as follow</li> <li>3. Click on "Apply"</li> </ol>	

#### 4.6.4 Public IP Network

No configuration is required in this section. Existing IP Interface, Ethernet Device and Device Group can be reused.

It is anyway strongly recommended to have a dedicated IP Interface for Service provider SIP Trunk like Orange in order to differentiate Traffic Sip Internal and Traffic Sip of the Service Provider. In the TLS profile used for BTol / BTIPol (SIP/TLS) **the WAN or public IP interface is usually exposed to the public internet through a DMZ, so it is strongly recommended to use an Access Control List in order to restrict access**

#### 4.6.5 Coders and Profiles

This section describes configuration of the Voice Settings: Coders and SIP profiles.

##### **Allowed Audio Coders Groups**

Allowed Audio Coders Groups are used to remove codecs from an SDP offer and/or to modify the order or preference in the codecs list.

Orange accepts the following codecs in this order or preference:

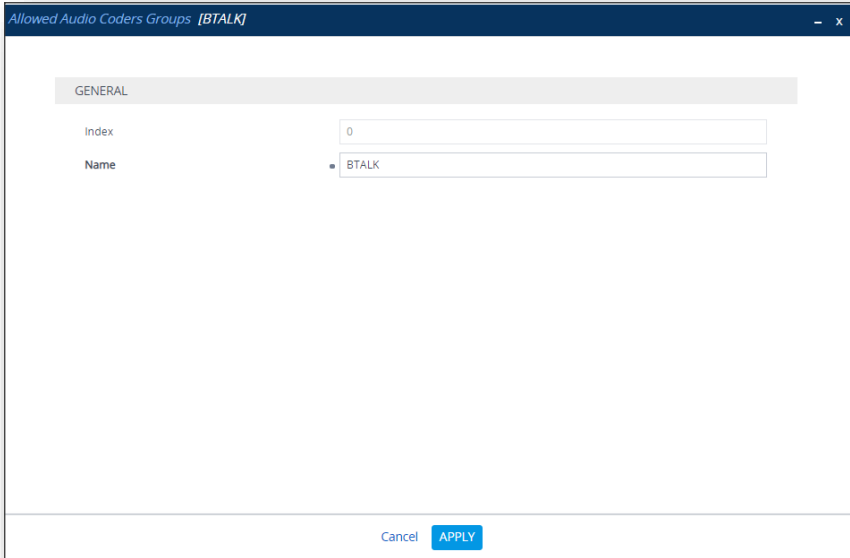
- *G.711 A-law 20 ms for French BTIPol / BTol Offers (or G.711 μ-law 20 ms for International BT Offer).*

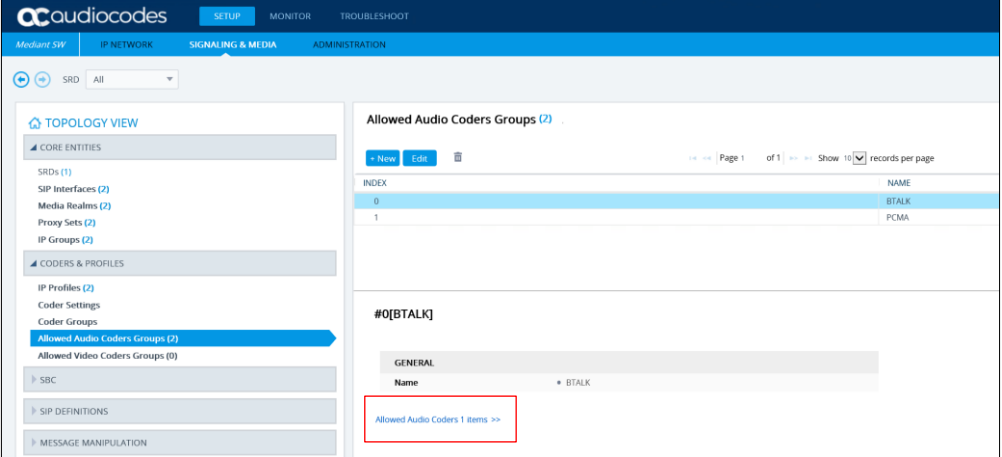
We are going to create a new "Coders Groups" specific to Orange BTalk.

Index	Name
<b>0</b>	BTALK
<i>1</i>	<i>PS_IPBX</i>

This “Coders Groups” will manage the Codec specific to Orange BTalk.

Index	Coder	User-defined Coder
<b>0</b>	G.711 A-Law (or G.711 $\mu$ -law)	(Empty)

Actions	Screenshot
<ol style="list-style-type: none"> <li>1. Open SETUP &gt; SIGNALING &amp; MEDIA &gt; CODERS &amp; PROFILES &gt; Allowed Audio Coders Groups</li> <li>2. Click on "+ New"</li> <li>3. Enter a meaningful name ex" BTALK"</li> <li>4. Click on "Apply"</li> <li>5. Click on "Allowed Audio Coders 0 items"</li> </ol>	

Actions	Screenshot
<p>6. Click on "+ New"</p> <p>7. Select the coders as mention in the table of parameters above, in the same order</p> <p><b>Please note:</b> Do not select "G711 A-law VBD" or "EG-711 A-law" as they are not regular G711a codecs</p>	 <p>The screenshot displays the AudioCodes management console. The left sidebar lists various configuration categories, with 'Allowed Audio Coders Groups (2)' selected. The main panel shows a table of allowed audio coders. The table has two columns: 'INDEX' and 'NAME'. The first row has index '0' and name 'BTALK'. The second row has index '1' and name 'PCMA'. Below the table, there is a 'GENERAL' section with a 'Name' field containing '#0[BTALK]'. A red box highlights a link 'Allowed Audio Coders 1 items &gt;&gt;' at the bottom of the configuration page.</p>

**Allowed Audio Coders Groups in case of multiple codecs into SDP Audio MLine (Optional)**

Even if this not the standard behaviors, some customer IPPBX/device could send several “codec” in the SDP answer (SDP with multiple codecs into Audio M Lines). This behavior is not supported by Orange BTalk network. As solution on the Audiocodes eSBC, it is required to implement a different “Allowed Coder Group” to filter the answers. This will force all calls to the selected a unique “G711 A-law” codec.

**Note:** *If you are in this case you don’t need to create the “BTIP” “Allow Coders Group” describe in the previous chapters.*

We are going to create a new “Coders Groups” specific to Orange BTalk.

Index	Name
1	PCMA
2	PS_IPBX

This “Coders Groups” will managed only 1 Codec supported in Orange BTalk over Internet.

Index	Coder	User-defined Coder
0	G.711 A-Law	(Empty)

Actions	Screenshot
<p>8. Open SETUP &gt; SIGNALING &amp; MEDIA &gt; CODERS &amp; PROFILES &gt; Allowed Audio Coders Groups</p> <p>9. Click on “+ New”</p> <p>10. Enter a meaningful name ex” PCMA”</p> <p>11. Click on “Apply”</p> <p>12. Click on “Allowed Audio Coders 0 items”</p>	



Actions	Screenshot												
<p>13. Click on "+ New"</p> <p>14. Select the coders as mention in the table of parameters above, in the same order</p> <p><b>Please note:</b> Do not select "G711 A-law VBD" or "EG-711 A-law" as they are not regular G711a codecs</p>	<p>The top screenshot shows the 'Allowed Audio Coders Groups (2)' configuration page. The left sidebar has 'Allowed Audio Coders Groups (2)' highlighted. The main content area shows a table with 2 items:</p> <table border="1"> <thead> <tr> <th>INDEX</th> <th>NAME</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>BTIP</td> </tr> <tr> <td>1</td> <td>PCMA</td> </tr> </tbody> </table> <p>Below the table, the configuration for group #1 [PCMA] is shown under the 'GENERAL' tab, with 'Name' set to 'PCMA'.</p> <p>The bottom screenshot shows the 'Allowed Audio Coders Groups [#0] &gt; Allowed Audio Coders (1)' configuration page. The left sidebar has 'Allowed Audio Coders Groups (1)' highlighted. The main content area shows a table with 1 item:</p> <table border="1"> <thead> <tr> <th>INDEX</th> <th>CODER</th> <th>USER-D</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>G.711 A-law</td> <td></td> </tr> </tbody> </table> <p>Below the table, the configuration for group #0 is shown under the 'GENERAL' tab, with 'Coder' set to 'G.711 A-law'.</p>	INDEX	NAME	0	BTIP	1	PCMA	INDEX	CODER	USER-D	0	G.711 A-law	
INDEX	NAME												
0	BTIP												
1	PCMA												
INDEX	CODER	USER-D											
0	G.711 A-law												

### IP Profile Settings

The IP Profile settings is a set of parameters with user-defined settings relating to signaling and media. The IP Profile will be assigned later to specific IP calls.

This IP Profile will re-use the “Allowed Audio Coders” created in the previous chapter in order to compliant with Orange BTalk codec list. In case of **Standard installation** will use the “**BTALK**” or in **particular case** the “**PCMA**” Allow Audio Coders.

This IP Profile will be configured to be compliant with Orange BTalk specification:

- ✓ Transfer allowed via Re-invite
- ✓ DTMF via RFC 2833/4733
- ✓ Transport tag require EF (DSCP 46) for Media and Signaling
- ✓ SRTP encryption

**Note:**

For **DTMF**, the Audiocodes eSBC will be able to **convert SIP INFO** message to RFC2833/4733. DTMF inbound will be not converted by the eSBC because it requires DSP resources on eSBC.

For **Transfer**, the Audiocodes eSBC will be able to **convert REFER** into RE-Invite.

For encryption, the Audiocodes eSBC will encrypt the RTP tower Orange BT/BTIP based on the TLS context. By default, the Audiocodes SBC will deliver the RTP encryption to the IPPBX. If you want to decrypt the RTP toward the customer IPPBX the parameter “SBC Media Security Mode = RTP” on the IP Profile of the Customer IPPBX must be set.

In some case SIP Provisional Response ACKnowledgement (PRACK RFC 3262)) could be required (For Cisco CUCM) to be interworked with Orange which not support PRACK. eSBC device can be configured to resolve this interoperable issue and enable sessions between such endpoints. SIP PRACK handling is configured using the IP Profile parameter, **eSBC Prack Mode : Mandatory** on the IP profile of the Customer IPPBX.

**All of those conversions will stayed under customer responsibilities depending of South private architecture context.**

The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

“Section: **Media Security**”

eSBC Media Security Mode	eSBC Remove Crypto Lifetime in SDP
<b>SRTP</b>	YES
<i>RTP</i>	<i>No</i>

“Section: eSBC Media”

Index	Name	Allowed Audio Coders	Allowed Coders Mode	RFC2833 Mode	RFC2833 DTMF Payload Type	Use Silence Suppression	RTP Redundancy Mode
1	IPP_BTALK	BTALK	Restriction	Extend	101	Remove	Disable

“Section: Quality of Service”

Signaling DiffServ

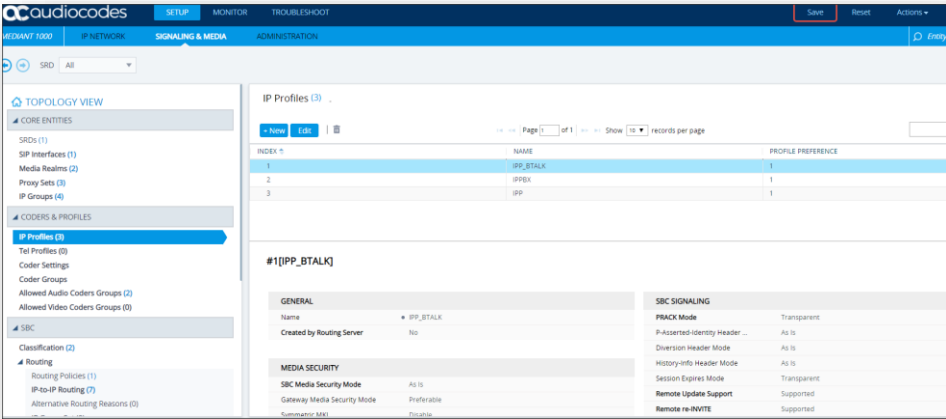
46

“Section: eSBC Forward and Transfer”

Remote REFER Mode	Remote 3xx Mode
Handle Locally	Handle Locally

Actions	Screenshot
<ol style="list-style-type: none"> <li>Open SETUP &gt; SIGNALING &amp; MEDIA &gt; CODERS &amp; PROFILES &gt; IP Profiles</li> <li>Click on “+ New” Enter a meaningful name ex” IPP_BTALK”</li> <li>Change the parameters indicated above as follow</li> </ol>	

Actions	Screenshot
	<p><b>SBC FORWARD AND TRANSFER</b></p> <ul style="list-style-type: none"> <li>Remote REFER Mode: Handle Locally</li> <li>Remote Replaces Mode: Standard</li> <li>Play RBT To Transferee: No</li> <li>Remote 3xx Mode: Handle Locally</li> </ul>
	<p><b>RFC 2833 Mode</b>: Extend</p> <p><b>RFC 2833 DTMF Payload Type</b>: 101</p>
	<p><b>QUALITY OF SERVICE</b></p> <ul style="list-style-type: none"> <li>RTP IP DiffServ: 46</li> <li>Signaling DiffServ: 46</li> <li>Data DiffServ: 0</li> </ul>

Actions	Screenshot												
<p>Click on “Apply” The new Objects will appear in the list.</p>	 <p>The screenshot shows the 'IP Profiles' configuration page in the AudioCodes eSBC interface. The left sidebar contains a 'TOPOLOGY VIEW' with categories like CORE ENTITIES, CODERS &amp; PROFILES, and SBC. The 'IP Profiles (3)' category is selected. The main area displays a table of IP Profiles:</p> <table border="1"> <thead> <tr> <th>INDEX</th> <th>NAME</th> <th>PROFILE PREFERENCE</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>IPP_BTALK</td> <td>1</td> </tr> <tr> <td>2</td> <td>IPPEX</td> <td>1</td> </tr> <tr> <td>3</td> <td>IPP</td> <td>1</td> </tr> </tbody> </table> <p>Below the table, the configuration for the selected profile '#1[IPP_BTALK]' is shown, divided into sections: GENERAL, MEDIA SECURITY, and SBC SIGNALING.</p> <p><b>GENERAL</b></p> <ul style="list-style-type: none"> <li>Name: IPP_BTALK</li> <li>Created by Routing Server: No</li> </ul> <p><b>MEDIA SECURITY</b></p> <ul style="list-style-type: none"> <li>SBC Media Security Mode: As Is</li> <li>Gateway Media Security Mode: Preferable</li> </ul> <p><b>SBC SIGNALING</b></p> <ul style="list-style-type: none"> <li>FRACK Mode: Transparent</li> <li>P-Asserted-Identity Header Mode: As Is</li> <li>Diversion Header Mode: As Is</li> <li>History-Info Header Mode: As Is</li> <li>Session Expires Mode: Transparent</li> <li>Remote Update Support: Supported</li> <li>Remote re-INVITE: Supported</li> </ul>	INDEX	NAME	PROFILE PREFERENCE	1	IPP_BTALK	1	2	IPPEX	1	3	IPP	1
INDEX	NAME	PROFILE PREFERENCE											
1	IPP_BTALK	1											
2	IPPEX	1											
3	IPP	1											

### 4.6.6 Core Entities

#### SRD Table

No configuration is required in this section. We will use the existing “DefaultSRD”

#### SIP Interface Table

The SIP Interface table allows to define a local, listening port number and type (e.g. UDP or TCP), and assigning an IP Network interface for SIP signaling traffic. We are going to use the **TLS context “Orange”** with the Certificate shared with Orange BTALK.

This SIP signaling will be configured to be compliant with Orange BTalk specification:

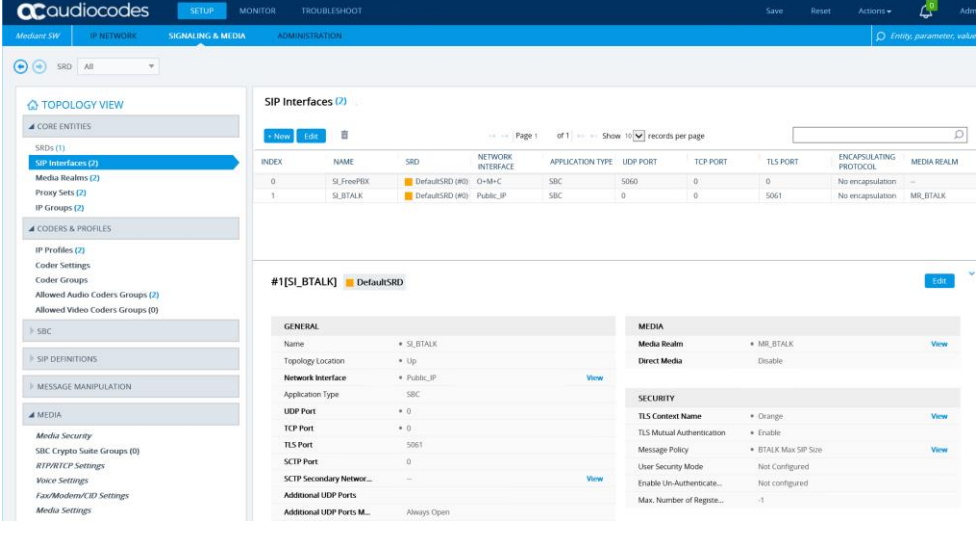
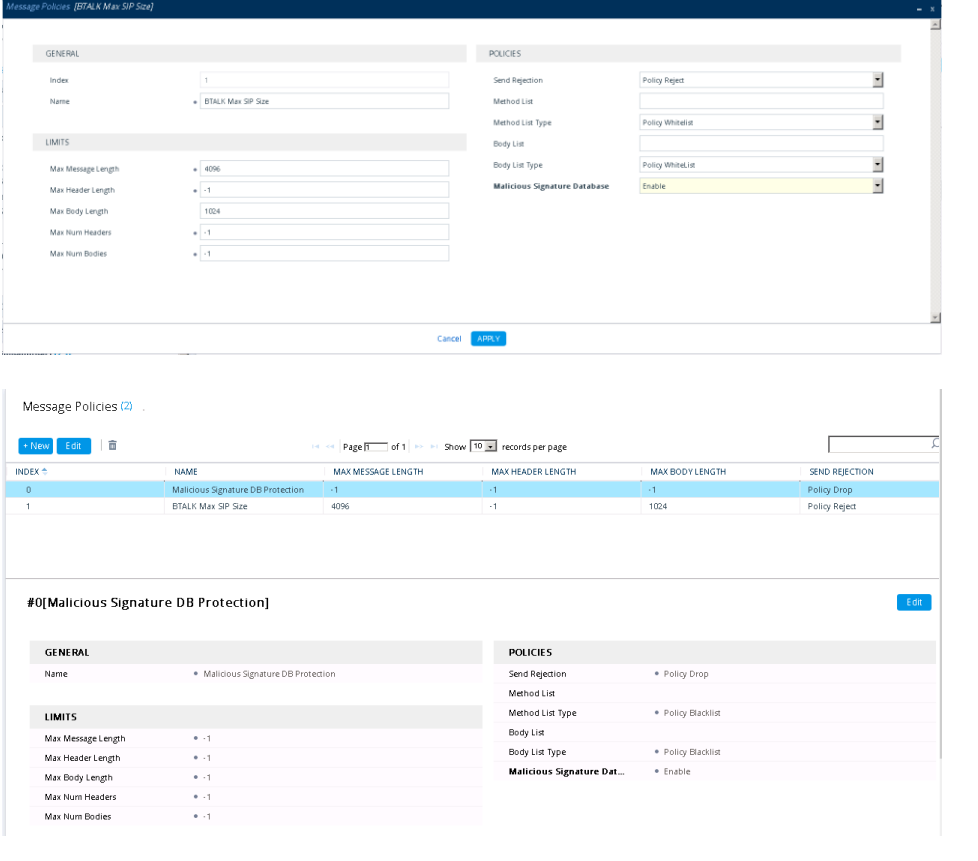
- ✓ For **encrypted BTALK SIP Trunk** architecture we need to configure **TLS port 5061**

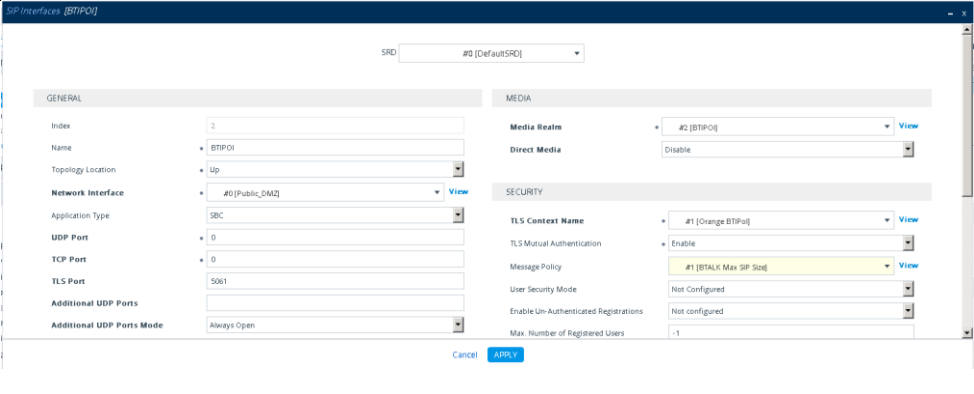
The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

Index	Name	Network Interface	UDP Port	TCP Port	TLS Port	TLS Context	Classification Failure Response Type	Message Policy
2	SI_BTALK	NI_Existing	0	0	5061	Orange	0	BTALK Max SIP Size
1	SI_IPBX	NI_IPBX	5060	0	0	-	0	

**Note:** “Network Interface” will be defined by the Customer itself.

Actions	Screenshot
<p>9. Open SETUP &gt; SIGNALING &amp; MEDIA &gt; CORE ENTITIES &gt; SIP Interfaces</p> <p>10. Click on “+ New” Enter a meaningful name ex” <b>SI_BTALK</b>”</p> <p>11. Change the parameters indicated above as follow</p>	

Actions	Screenshot																														
<p><b>12.</b> Click on “Apply” The new Objects will appear in the list.</p>	 <p>The screenshot shows the 'SIP Interfaces' configuration page. A table lists the following interfaces:</p> <table border="1"> <thead> <tr> <th>INDEX</th> <th>NAME</th> <th>SRD</th> <th>NETWORK INTERFACE</th> <th>APPLICATION TYPE</th> <th>UDP PORT</th> <th>TCP PORT</th> <th>TLS PORT</th> <th>ENCAPSULATING PROTOCOL</th> <th>MEDIA REALM</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>SI_SIPREX</td> <td>DefaultSRD (M0)</td> <td>On-Box</td> <td>SBC</td> <td>5060</td> <td>0</td> <td>0</td> <td>No encapsulation</td> <td>-</td> </tr> <tr> <td>1</td> <td>SI_BTALK</td> <td>DefaultSRD (M0)</td> <td>Public_IP</td> <td>SBC</td> <td>0</td> <td>0</td> <td>5061</td> <td>No encapsulation</td> <td>MR_BTALK</td> </tr> </tbody> </table> <p>The configuration for the selected interface '#1[SI_BTALK]' is shown below:</p> <ul style="list-style-type: none"> <li><b>GENERAL:</b> Name: SI_BTALK, Topology Location: Up, Network Interface: Public_IP, Application Type: SBC, UDP Port: 0, TCP Port: 0, TLS Port: 5061, SCTP Port: 0, SCTP Secondary Network: --, Additional UDP Ports: Always Open.</li> <li><b>MEDIA:</b> Media Realm: MR_BTALK, Direct Media: Disable.</li> <li><b>SECURITY:</b> TLS Context Name: Change, TLS Mutual Authentication: Enable, Message Policy: BTALK Max SIP Size, User Security Mode: Not Configured, Enable Un-Authenticate: Not configured, Max. Number of Register: -1.</li> </ul>	INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATING PROTOCOL	MEDIA REALM	0	SI_SIPREX	DefaultSRD (M0)	On-Box	SBC	5060	0	0	No encapsulation	-	1	SI_BTALK	DefaultSRD (M0)	Public_IP	SBC	0	0	5061	No encapsulation	MR_BTALK
INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATING PROTOCOL	MEDIA REALM																						
0	SI_SIPREX	DefaultSRD (M0)	On-Box	SBC	5060	0	0	No encapsulation	-																						
1	SI_BTALK	DefaultSRD (M0)	Public_IP	SBC	0	0	5061	No encapsulation	MR_BTALK																						
<p><b>13.</b> In case of SIP trunking Over Internet like BTol offer usage, we advise you to enable the “Malicious Signature Database” included in the Message Policies “BTALK Max Sip Size” called into the SIP Interface</p>	 <p>The screenshot shows the 'Message Policies' configuration page. The 'BTALK Max SIP Size' policy is selected, and the 'Malicious Signature Database' checkbox is checked under the 'POLICIES' section.</p> <p>The configuration for the selected policy '#0[Malicious Signature DB Protection]' is shown below:</p> <ul style="list-style-type: none"> <li><b>GENERAL:</b> Name: Malicious Signature DB Protection.</li> <li><b>LIMITS:</b> Max Message Length: -1, Max Header Length: -1, Max Body Length: -1, Max Num Headers: -1, Max Num Bodies: -1.</li> <li><b>POLICIES:</b> Send Rejection: Policy Drop, Method List: Policy Blacklist, Method List Type: Policy Blacklist, Body List: Policy Blacklist, Body List Type: Policy Blacklist, Malicious Signature Database: Enable.</li> </ul>																														

Actions	Screenshot
<p>2. Then Message Policies “BTALK Max Sip Size” is called into the Sip Interface Ex: BTol</p>	

**Media Realm Table**

The Media Realm Table allows allowed range media defined on gateway depending on traffic.

This Media will be configured to be compliant with Orange BTalk specification:

- ✓ For **encrypted BTALK over Internet SIP Trunk** architecture we need to configure **RTP port 6 000 to 20 000**
- ✓ For **encrypted BTIP over Internet SIP Trunk** architecture we need to configure **RTP port 6 000 to 38 000**

**Note:** On Audiocodes eSBC, for RTP port range keep in mind that the RTP UDP port spacing is “10”. This mean that for example 5 sessions SIP, 5\*10 ports RTP from 6000 to 60050 will be reserved.

The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

Index	Media Realm Name	IP Interface Name	Port Range Start	Media Session Legs
<b>2</b>	MR_BTALK	NI_Existing	7000	100
1	MR_IPBX	NI_IPBX	8000	100

**Note:** The table above shows the configuration for 1000 calls maximum with Orange. The “Media Session Legs” should be adapted to your BTIP/BT service offer. “Port Range Start” and “IP interface name” will be defined by the Customer itself.



Actions	Screenshot																					
<ol style="list-style-type: none"> <li>1. Open SETUP &gt; SIGNALING &amp; MEDIA &gt; CORE ENTITIES &gt; MEDIA REALMS</li> <li>2. Click on "+ New" Enter a meaningful name ex" <b>MR_BTALK</b>"</li> <li>3. Change the parameters indicated above as follow</li> </ol>																						
<p>Click on "Apply" The new Objects will appear in the list.</p>	<table border="1"> <caption>Media Realms (2)</caption> <thead> <tr> <th>INDEX</th> <th>NAME</th> <th>IPv4 INTERFACE NAME</th> <th>UDP PORT RANGE START</th> <th>NUMBER OF MEDIA SESSION LEGS</th> <th>UDP PORT RANGE END</th> <th>DEFAULT MEDIA REALM</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>MR_BTALK</td> <td>0-M-C</td> <td>8000</td> <td>100</td> <td>8999</td> <td>No</td> </tr> <tr> <td>1</td> <td>MR_BTALK</td> <td>Public_IP</td> <td>7000</td> <td>100</td> <td>7999</td> <td>No</td> </tr> </tbody> </table>	INDEX	NAME	IPv4 INTERFACE NAME	UDP PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	UDP PORT RANGE END	DEFAULT MEDIA REALM	0	MR_BTALK	0-M-C	8000	100	8999	No	1	MR_BTALK	Public_IP	7000	100	7999	No
INDEX	NAME	IPv4 INTERFACE NAME	UDP PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	UDP PORT RANGE END	DEFAULT MEDIA REALM																
0	MR_BTALK	0-M-C	8000	100	8999	No																
1	MR_BTALK	Public_IP	7000	100	7999	No																

### Proxy Set Table and Address

The Proxy Set Table allows proxy set definition. There you will configure the IP/ FQDN of Orange BTALK extremity and Keep-alive. **We are going to use the TLS context “Orange” with the Certificate shared with Orange BTALK for the encryption.**

This Proxy will be configured to be compliant with Orange BTalk specification:

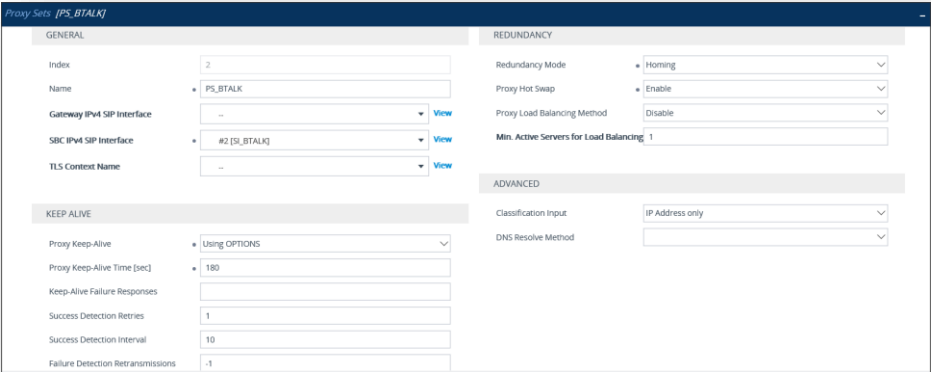
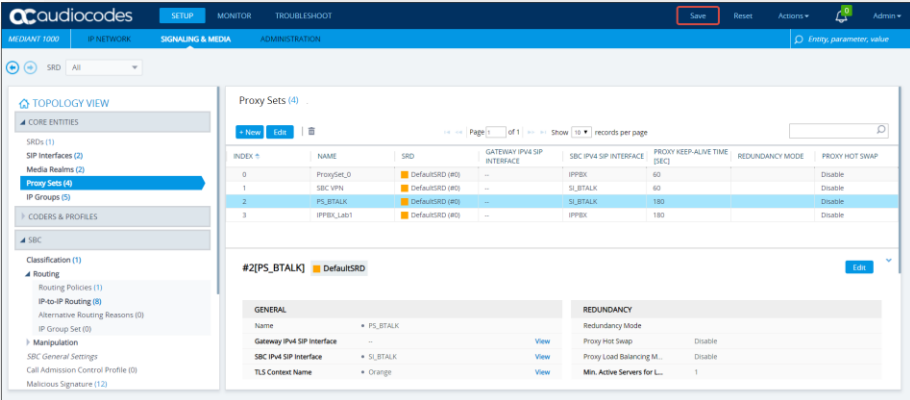
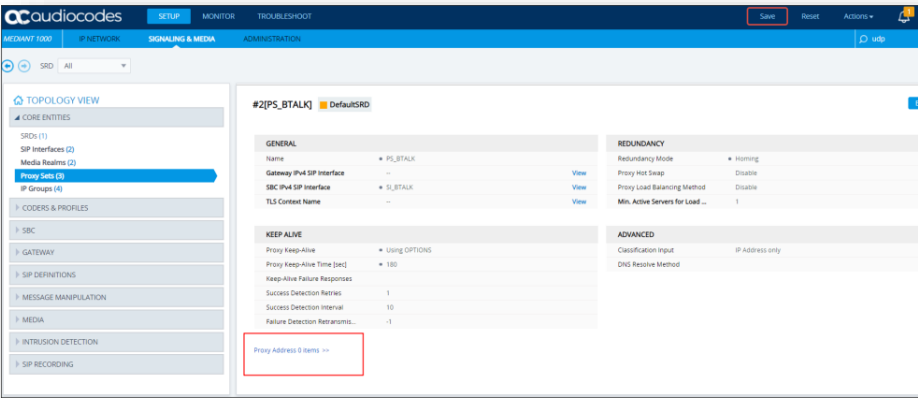
- ✓ For **encrypted BT/BTIP over Internet SIP Trunk** architecture we need to configure **TCP port 5061**
- ✓ For Sip trunk keep alive done with “**Options**” message (every 300 seconds)
- ✓ For Sip trunk redundancy **Homing** (the first Proxy Address is always select if available) and Proxy Hot swap **Enable** ( In case of Invite reject or no answer ,the call is moved to the next Proxy Address)
- ✓ **2 Proxy Address must be configured for redundancy purpose** or a single 1 in case of BTIP over Internet DNS SRV record usage.

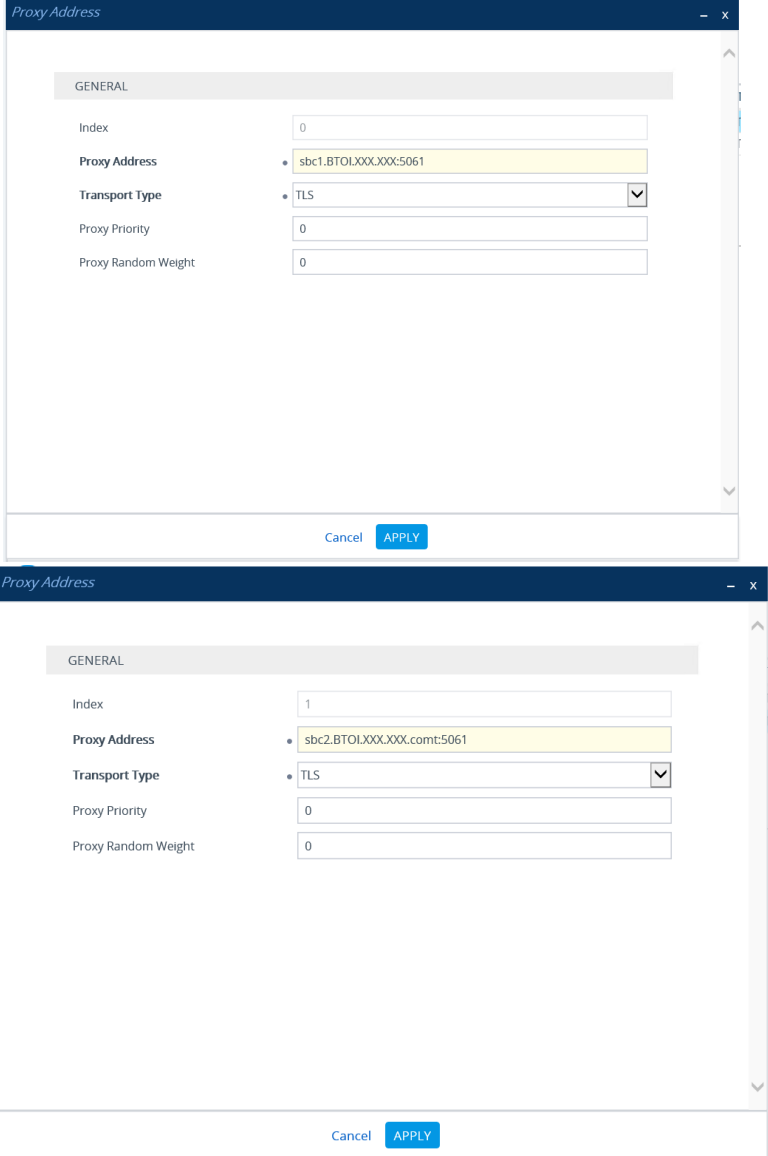
The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

Index	Name	SIP Interface	TLS Context Name	Proxy Keep-Alive	Redundancy Mode	Proxy Hot Swap	Index Proxy Address	Proxy Address	Transport Type
1	PS_BTALK or PS_BTIP	SI_BTALK or SI_BTIPK	Orange	Using OPTIONS	Homing	Enable	0	<BT_Nominal_Public_IP> or <BTIP_Nominal_Public FQDN >:5061	TLS
							1	<BT_Backup_Public_IP> or <BTIP_Backup_Public FQDN >:5061	TLS
2	PS_IPBX	SI_IPBX	--	Using OPTIONS				** @IP_IPBX:5060 **	UDP

**Note:** Please avoid using Proxy Set 0 Index. The Public FQDN (Type A or SRV) or Public IP set in the “Proxy Address” is the “**Public FQDN**” for BTIPoI or “**Public IP**” for BTIoI provided by Orange for the SIP trunk BTALK. “Options” message will be sent by the Audiocodes eSBC to verify if the Orange BTalk network is reachable. We recommend to use primarily ours Public FQDN which required DNS Servers must be configured in “Public” network interface.

**All the screenshots below showing some IP address are given as example. You should replace them by correct Orange IP’s or FQDN’s (Type A or SRV)**

Actions	Screenshot
<ol style="list-style-type: none"> <li>Open SETUP &gt; SIGNALING &amp; MEDIA &gt; CORE ENTITIES &gt; PROXY SETS</li> <li>Click on "+ New" Enter a meaningful name ex" PS_BTALK"</li> <li>Change the parameters indicated above as follow</li> </ol>	
<ol style="list-style-type: none"> <li>Click on "Apply". The new Objects will appear in the list.</li> </ol>	
<ol style="list-style-type: none"> <li>To configure "Proxy Address" and "Transport Type", you have to configure and select the "Proxy Set" just created.</li> <li>Click on the "Proxy Address 0 items" link at the bottom of the page</li> </ol>	

Actions	Screenshot
<p>9. Configure though <b>index 0</b> for <b>&lt;BT_Nominal_Public_IP&gt;</b> or <b>&lt;BTIP_Nominal_Public FQDN &gt;</b>.</p> <p>10. You have to configure though <b>Index 1 for the backup Proxy address</b> to backup the nominal ones with <b>&lt;BT_Backup_Public_IP&gt;</b> or <b>&lt;BTIP_Backup_Public FQDN &gt;</b>.</p> <p>11. At the End at least 2 Proxy Items should be configured:</p> <ul style="list-style-type: none"> <li>- Index 0 for Nominal within <b>BT nominal Public IP (first public IP) or BTIP nominal FQDN (First DNS record type)</b></li> <li>- Index 1 for <b>Backup</b> within <b>BT backup Public IP (second public IP) or BTIP backup FQDN (Second DNS record type)</b></li> </ul> <p>In case of usage of BTIP over Internet SRV Record Index 0 must be configured</p>	 <p>The top screenshot shows the 'Proxy Address' configuration window for Index 0. The fields are: Index: 0, Proxy Address: sbc1.BTOI.XXX.XXX:5061, Transport Type: TLS, Proxy Priority: 0, and Proxy Random Weight: 0. The bottom screenshot shows the same window for Index 1. The fields are: Index: 1, Proxy Address: sbc2.BTOI.XXX.XXX.comt:5061, Transport Type: TLS, Proxy Priority: 0, and Proxy Random Weight: 0. Both screenshots have 'Cancel' and 'APPLY' buttons at the bottom.</p>

## IP Group Table

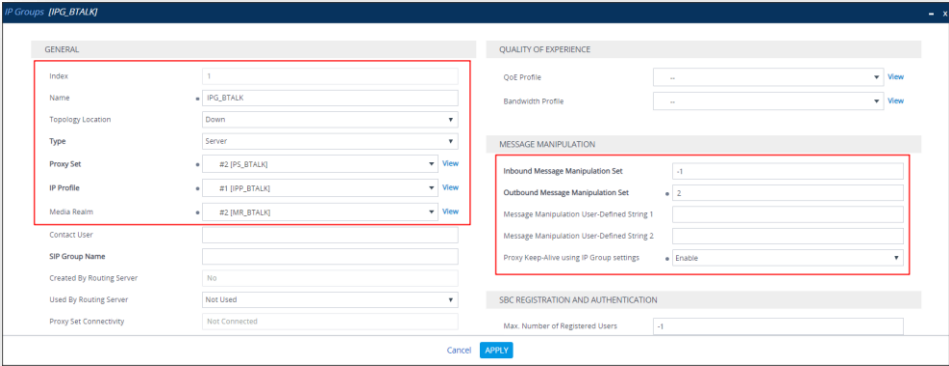
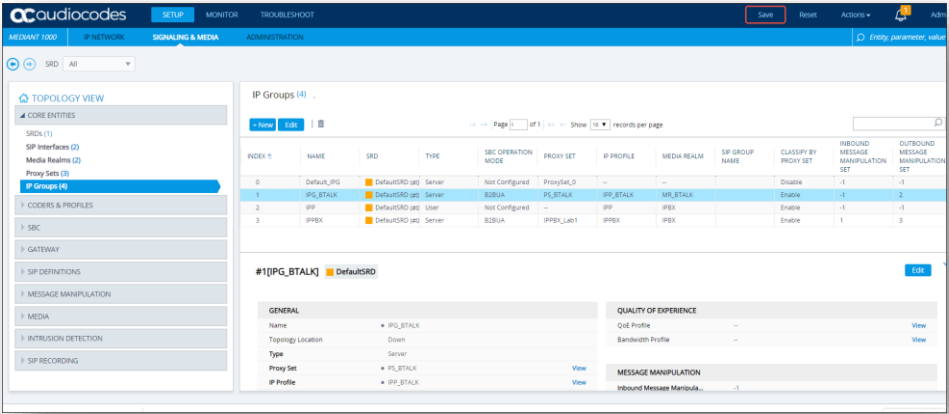
The IP Group table allows logical IP entities creation with a set of parameters such as Proxy set ID, IP profile ID to separate provenance and destination traffic.

A new IP Group specific to Orange BTIP or BT SIP Trunk need to be create as **Server Back-to-back** (B2BUA) with message **Manipulation on the outgoing Orange side**. The IP Group will be composed of the objects previously created in the table: Media Realm, Proxy Set and IP Profile.

The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

Index	Name	Proxy Set	Media Realm	IP Profile	Inbound Message Manipulation Set	Outbound Message Manipulation Set	Proxy Keep-Alive using IP Group settings
1	IPG_BT or IPG_BTIP	PS_BTALK	MR_BTALK	IPP_BTALK	-1	2	Enable
2	IPG_IPBX	PS_IPBX	MR_IPBX	IPP_IPBX	1	3	Enable

**Note:** Please avoid using IP Group Index "0". The value "-1" inside the "Inbound Message Manipulation set" parameter indicate that "**None**" Manipulation is needed for incoming message from Orange BTALK. The value "2" inside the "Outbound Message Manipulation Set" parameter indicate a set of **Manipulations (inside the Man Set ID "2") are required** for outgoing message toward Orange BTalk Network. Those Manipulations are described in the next chapters.

Actions	Screenshot
<ol style="list-style-type: none"> <li>1. Open SETUP &gt; SIGNALING &amp; MEDIA &gt; CORE ENTITIES &gt; IP_GROUP &gt; IP_GROUP</li> <li>2. Click on "+ New" Enter a meaningful name ex" <b>IPG_BTALK</b>"</li> <li>3. Click on "Apply"</li> <li>4. Click on "Allowed Audio Coders 0 items"</li> </ol>	
<ol style="list-style-type: none"> <li>5. Click on "Apply". The new Objects will appear in the list.</li> </ol>	



## 4.6.7 SIP Message Manipulation

For unencrypted or encrypted BT SIP Trunk architecture, it is required to implement some Message Manipulation for the outgoing message toward Orange BTalk.

Those Manipulations Rules are detailed in chapter “*SIP rules & manipulations (eSBC Application)*”.

Please jump to this Chapter directly

## 4.7 SIP rules & manipulations (eSBC Application)

This section provides the configuration regarding the device's eSBC application, which is used for IP-to-IP message rules & manipulations as described below. This chapter is common to Orange BTalk eSBC encrypted or unencrypted BT SIP Trunk architecture.

### 4.7.1 IP-to-IP Routing Table

This section provide configuration about IP-to-IP routing rules for eSBC application. We are configuring a simple routing from Orange BTalk SIP trunk (IP Group) toward Customer IPPBX SIP trunk (IP Group) and vice versa. This configuration could be changed according the complexity of the VoIP routing in the Customer environment (multi IPPBX, lines specific,...).

We are going also to implement OPTIONS answer message (via 200 OK), in order to answer the Keep Alive messages send by Orange BTALK. This last implementation could be optional if already present on the eSBC for a different SIP trunk.

For all IP-to-IP traffic, configuration has to be performed at least for:

- **SIP Options** message
- **Outgoing** message = **South Side (Ex: IPBX)** towards **BTalk North side**
- **Incoming** message = **BTalk North side** towards **South Side (Ex: IPBX)**

The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

Index	Name	Source IP Group	Request Type	Destination Type	Destination IP Group	Internal Action
0	OPTIONS	Any	OPTIONS	Internal	--	reply(response='200')
1	IPBX > BTIP	IPG_IPBX	Any	IP Group	IPG_BTALK	
2	BTIP > IPBX	IPG_BTALK	Any	IP Group	IPG_IPBX	

### 4.7.2 Outbound Manipulations

This chapter is about the Number manipulation for precisely the "Called Number" in the URI. Orange Phone numbers must be sent to Orange in E164 format. The following manipulations will transform Called numbers received from Customer IPPBX in National format (0ZABPQMCDU or 00xxxxxxx) to E164 (+CCZABPQMCDU) before sending the Call tower Orange BTALK.

The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».





Index	Manipulation Name	Src IP Group	Dest IP Group	Source Username Pattern	Destination Username Pattern	Manipulated Item	Remove from Left	Prefix 2 Add
0	00 > E164	Any	IPG_BTALK	*	00	Destination URI	2	+
1	0 > E164	Any	IPG_BTALK	*	0	Destination URI	1	+CC

Note: +CC prefix is the Country Code of the country where the eSBC or IPBX is installed. It is up to the Customer to indicate the correct +CC. ex +33 for France  
If the IPBX is using a local dial plan (Private numbering Plan), then the manipulation has to adapted in consequence by the Customer.

### 4.7.3 Inbound Manipulations

No inbound manipulation Number is required for default installation.

## 4.7.4 SIP Messages Manipulations

Several SIP manipulations (aka “MMS”) are required to manipulate the SIP headers and the SDP body, in order to control the content of the messages, and ensure the interoperability with the BTIP/BT services.

### Important note:

- Manipulation **Man Set ID “1”** include only **1 manipulation** Index “0”. This is applied to messages incoming from the customer IPBX (IPBX=>eSBC).
- Manipulation **Man Set ID “2”** include **21 manipulations** Index “1” to “21”. They are applied on messages outgoing towards Orange BT/BTIP SIP trunk (eSBC=> BT/BTIP). Manipulation Index 14 to 20 modify the phone number inside different Headers to be compliant with E164 Format. Replace “+CC” by the corresponding Country Code of your country
- Manipulation **Man Set ID “3”** include only **1 manipulation** Index “22”. This is applied to messages outgoing to the customer IPBX (eSBC=> IPBX).

The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value». If the Man set Id indicated in the table below are already used by existing Manipulation, feel free to change those number, but don’t forget to report the correct Id Number in the “IP Group” ( please refer to chapter IP Group Table). Due to the complexity of the manipulation and to avoid mistake, you can load the partial INI in “Annexes” chapter which contain only the Manipulation Rules.

Index	Name	Man Set ID	Message Type	Condition	Action Subject	Action Type	Action Value
0	Store User-Agent BTIP	1	any	header.user-agent exists and header.user-agent regex (.*)	var.session.agent	Modify	\$1
1	Modify User-Agent BTIP	2	any	header.user-agent exists and var.session.agent len> '1'	header.user-agent	Modify	var.session.agent + '+' + header.user-agent
2	Hide IP From	2	any	header.from.url.host !contains 'Anonymous'	header.from.url.host	Modify	header.via.host
3	Hide IP To	2	any		header.to.url.host	Modify	param.message.address.dst.ip
4	Hide IP Request-URI	2	any.request		header.request-uri.url.host	Modify	param.message.address.dst.ip
5	Hide IP PAI	2	any	header.p-asserted-identity exists	header.p-asserted-identity.url.host	Modify	header.via.host

6	Hide IP Diversion	2	any	header.diversion exists	header.diversion.url.host	Modify	header.via.host
7	Remove BYE Contact	2	bye.request		header.contact	Remove	
8	Remove 200OK BYE Contact	2	bye.response.200		header.contact	Remove	
9	Remove Supported	2	any	header.Supported exists	header.Supported	Remove	
10	Modify Allow	2	any	header.Allow exists	header.Allow	Modify	'INVITE,ACK,BYE,CANCEL,OPTIONS,UPDATE'
11	Remove Allow in ACK	2	ack	header.allow exists	header.allow	Remove	
12	Fix Anonymous	2	invite	header.from.url.user == 'anonymous' AND header.privacy !exists	header.privacy	Add	'id'
13	Normalize Message	2	any		Message	Normalize	
14	Diversion to E164	2	invite.request	header.diversion.url.user regex (^00)(\d+)	header.diversion.url.user	Modify	'+' + \$2
15	Diversion to E164	2	invite.request	header.diversion.url.user regex (^0)(\d+)	header.diversion.url.user	Modify	'+CC' + \$2
16	Remove diversion in 181	2	invite.response.181	header.diversion exists	header.diversion	Remove	
17	From to E164	2	any	header.from.url.user regex (^00)(\d+)	header.from.url.user	Modify	'+' + \$2
18	From to E164	2	any	header.from.url.user regex (^0)(\d+)	header.from.url.user	Modify	'+CC' + \$2
19	PAI to E164	2	any	header.p-asserted-identity.url.user regex (^00)(\d+)	header.p-asserted-identity.url.user	Modify	'+' + \$2
20	PAI to E164	2	any	header.p-asserted-identity.url.user regex (^0)(\d+)	header.p-asserted-identity.url.user	Modify	'+CC' + \$2
21	Add p-early-media on 18x with SDP	2	invite.response.18x	body.sdp exists and header.p-early-media !exists	header.P-Early-Media	Add	'sendrecv'
22	Remove Multipart	3	invite.request	body.application/vnd.orange.indata exists	body.application/vnd.orange.indata	Remove	

Below a brief description of each manipulation:

0. Stores the "User-Agent" or "Server" header from the customer side into a variable which will be used in another manipulation.
1. Concatenates eSBC "User-Agent" and IPBX "User-Agent" stored in previous manipulation.
2. Topology hiding modifies "From host" part with eSBC IP address.
3. Topology hiding: modifies "To host" part with remote proxy IP address.
4. Topology hiding: modifies "Request-URI" host part with remote proxy IP address.
5. Topology hiding: modifies "P-Asserted-Identity host" part with eSBC IP address.
6. Topology hiding: modifies "Diversion host" part with eSBC IP address.
7. Removes "Contact" header from "BYE" requests.
8. Removes "Contact" header from "200 OK" answers to a "BYE" request.
9. Removes "Supported" header.
10. Modifies "Allow" header to BTALK supported value.
11. Removes "Allow" header in "ACK" messages.
12. Adds a "Privacy" header with value "id" if the "From" header is "anonymous" and the "Privacy" header is missing.
13. Normalize messages. This feature does an automatic cleaning of SIP messages proposed by Audiocodes eSBC base on the SIP standard format. It will remove unknown and proprietary header (X-). Malformed headers will also be fixed or removed.
14. Converts "Diversion" international phone numbers from "00" format to E164.
15. Converts "Diversion" national phone numbers from "0" format to E164. Note that "+CC" must be replaced by the current Country Code (ex: +33 for France).
16. Removes "Diversion" header from 181 answers.
17. Converts "From" international phone numbers from "00" format to E164.
18. Converts "From" national phone numbers from "0" format to E164. Note that "+CC" must be replaced by the current Country Code (ex: +33 for France).



19. Converts "P-Asserted-Identity" international phone numbers from "00" format to E164.
20. Converts "P-Asserted-Identity" national phone numbers from "0" format to E164. Note that "+CC" must be replaced by the current Country Code (ex: +33 for France).
21. Adds "P-Early-Media" with value "sendrecv" to 18x answers that contains SDP.
22. Removes "multipart body" coming from BTALK.

## 5. Annexes

### 5.1 Import Manipulations Rules via Incrementation INI file

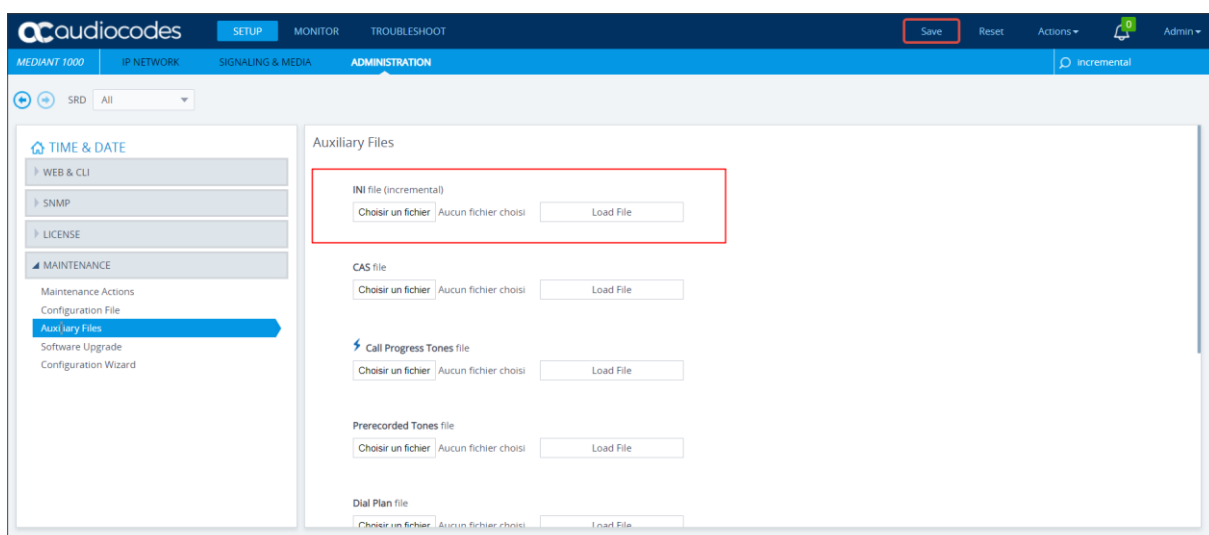
The INI incremental File attachment will allow you to load the Manipulation Rules need for this configuration. Before loading the INI file on the Audiocodes eSBC, it is necessary to check if the “Index” and “Man Set ID” number present in the INI incremental file are not already present on the eSBC. If you have the same number, you must change the number on the INI partial file.



manips\_incremental.i  
ni

The Incremental INI file must be loaded via the WebGui on the section ADMINISTRATION/MAINTENANCE/AUXILIARY FILES/ INI file (Incremental)

Note: please do a backup of the Audiocodes eSBC configuration before doing this step.



## 5.2 Example of SIP INVITE message

### From IPPBX toward Orange BT/BTIP

```
INVITE sip:+33399103825@172.22.246.33 SIP/2.0
Via: SIP/2.0/UDP 172.17.229.118:5060;branch=z9hG4bKac848491555
Max-Forwards: 70
From: "NBI_0033296082933" <sip:+33296082933@172.17.229.118>;tag=1c1454061318
To: <sip:+33399103825@172.22.246.33>
Call-ID: 1446761085582019101759@172.17.229.118
CSeq: 1 INVITE
Contact: <sip:0033296082933@172.17.229.118:5060>
Allow: INVITE,ACK,BYE,CANCEL,OPTIONS,UPDATE
User-Agent: FPBX-14.0.10.3(13.22.0)+Mediant 1000/v.7.20A.252.269
Content-Type: application/sdp
Content-Length: 255

v=0
o=root 1460554499 2025434629 IN IP4 172.17.229.118
s=Asterisk PBX 13.22.0
c=IN IP4 172.17.229.118
t=0 0
m=audio 7870 RTP/AVP 8 101
a=ptime:20
a=maxptime:150
a=sendrecv
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

**From Orange BT/BTIP toward Customer IPPBX**

```
INVITE sip:+33299281695@172.17.229.118:5060;user=phone SIP/2.0
Via: SIP/2.0/UDP 172.22.246.33:5060;branch=z9hG4bKq4e6eb109ot6a7e3t140.1
From: "+33786002931" <sip:+33786002931@172.22.246.33;user=phone>;tag=SDkrgc301-S2maIg
To: <sip:+33299281695@172.17.229.118;user=phone>
Call-ID: SDkrgc301-6d41631ae590323a0ca28275a72b7aa4-v300g00060
CSeq: 864377 INVITE
Max-Forwards: 64
Allow: INVITE,ACK,CANCEL,BYE,INFO,UPDATE, OPTIONS, REFER
Contact: <sip:172.22.246.33:5060;transport=udp>
P-Charging-Vector: icid-value=ae409ce0-04f7-1038-00-00-00-10-6b-03-d1-00
P-Early-Media: supported
Privacy: none
Diversion: <sip:+33299281695@172.22.246.33>;limit=10;reason=unconditional;counter=1
Content-Length: 281
Content-Disposition: session; handling=required
Content-Type: application/sdp

v=0
o=- 1636835357 40660 IN IP4 172.22.246.33
s=-
c=IN IP4 172.22.246.33
t=0 0
m=audio 6548 RTP/AVP 8 18 9 101
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:9 G722/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv
a=ptime:20
[Time: 02-09-2015 15:34:07]
```

### 5.3 NTP server configuration

This section describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (Microsoft NTP server or another global server) to ensure that the eSBC receives the current date and time. This is necessary for validating certificates of remote parties. It is important, that NTP Server will locate on the OAMP IP Interface (LAN\_IF in our case) or will be accessible through it.

➤ **To configure the NTP server address:**

1. Open the Time & Date page (**Setup** menu > **Administration** tab > **Time & Date**).
2. In the 'Primary NTP Server Address' field, enter the IP address of the NTP server. If you have an OVOC installed in your network you can indicate the OVOC as NTP Server.
3. Click **Apply**.



The screenshot shows the Audiocodes web interface for configuring Time & Date. The interface is divided into three main sections: LOCAL TIME, NTP SERVER, and TIME ZONE.

**LOCAL TIME**

Year	Month	Day	Hours	Minutes	Seconds
2019	10	16	18	44	24

**NTP SERVER**

Enable NTP:  Enable

Primary NTP Server Address (IP or FQDN): 172.17.229.160

Secondary NTP Server Address (IP or FQDN):

NTP Update Interval: Hours: 24 Minutes: 0

NTP Authentication Key Identifier: 0

NTP Authentication Secret Key:

**TIME ZONE**

UTC Time: 16 Oct, 2019 18:44:24

UTC Offset: Hours: 0 Minutes: 0

Daylight Saving Time:  Disable

DST Mode: Day of year

Start Time: Jan 01 00:00

End Time: Jan 01 00:00

Offset (min): 60

Day of Month Start: Jan Sunday First 00:00

Day of Month End: Jan Sunday First 00:00

Buttons: Cancel, APPLY

## Glossary

**BTalk:** Business Talk

**BTIP:** Business Talk IP

**BTol :** Business Talk over Internet

**BTIPol :** Business Talk IP over internet

**CC:** Country Code

**CSBC/eSBC:** Customer/Enterprise Session Border Controller

**CSR:** Certificate Signing Request

**DTMF:** Dual Tone Multi Frequency

**FQDN:** Fully Qualified Domain Name

**IP:** Internet Protocol

**LAN:** Local Area Network

**LLDP:** Link Layer Discovery Protocol

**MMS:** Message Manipulation SIP

**NET:** Network Equipment Technologies

**PBX:** Private Branch eXchange

**PSTN:** Public Switched Telephone Network

**RS:** Remote Site

**SBC:** Session Border Controller

**SIP:** Session Initiation Protocol

**TCP:** Transmission Control Protocol

**TLS:** Transport Layer Security

**UDP:** User Datagram Protocol

**WAN:** Wide Area Network