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 21/11/2025

Table of contents

1. General 4
1.1 Scope of the document 4
1.2 References documents 4
1.3 Pre- requisites 5
1.3.1 Certificates 5
1.3.2 Public DNS configuration: 5
1.3.3 NTP 5
1.3.4 Firewall flows for BTIP over Internet and BT over Internet 5
1.4 Orange BTalk/BTIP specifications 6
2. Certified Architecture 13
2.1 Introduction to architecture components and features 13
2.2 Architecture with Audiocodes "customer" eSBC 14
2.2.1 Unencrypted SIP Trunk through BVPN 14
2.2.2 Encrypted SIP Trunk Over Internet 15
2.2.3 Parameters to be provided by customers to access the service 16
Unencrypted SIP Trunk through BVPN 16
Encrypted SIP Trunk through Internet 16
2.3 BTalk & BTIP Audiocodes eSBC certified versions 18
2.4 Audiocodes Global configuration 19
2.4.1 Objects 19
2.4.2 Information and Syntax 19
2.5 Orange Business BTalk & BTIP Carrier unencrypted SIP configuration for AudioCodes eSBC (UDP) 21
2.5.1 Configure IP Network 21
2.5.2 Message Manipulation Policy 21
Message Policy 21
2.5.3 Coders and Profiles 22
Allowed Audio Coders Groups 22
IP Profile Settings 26
2.5.4 Core Entities 30
SRD Table 30
SIP Interface Table 30
Media Realm Table 32
Proxy Set Table and Address 34
IP Group Table 37
2.5.5 SIP Message Manipulation 40
2.6 Orange Business- BTalk over Internet & BTIP over Internet encrypted SIP configuration for AudioCodes eSBC (TLS) 41
2.6.1 Configure IP Network 41
2.6.2 TLS profile 41
TLS Context 41
Through TLS V1.3 for V.7.40A : 42
Through TLS V1.2 for V7.20A 42
eSBC Certificate 46
Customer Root / Intermediate Certificates authority: 47
Mutual TLS Authentication 47
2.6.3 Media Security 49
2.6.4 Public IP Network 49
2.6.5 Coders and Profiles 51
Allowed Audio Coders Groups 51
Allowed Audio Coders Groups in case of multiple codecs into SDP Audio MLine (Optional) 54
IP Profile Settings 56

2.6.6 Core Entities 60
SRD Table 60
SIP Interface Table 60
Media Realm Table 62
Proxy Set Table and Address 64
IP Group Table 67
2.6.7 SIP Message Manipulation 69
2.7 SIP rules & manipulations (eSBC Application) 70
2.7.1 IP-to-IP Routing Table 70
2.7.2 Outbound Manipulations 70
2.7.3 Inbound Manipulations 71
2.7.4 SIP Messages Manipulations 72
3. Annexes 76
3.1 Import Manipulations Rules via Incrementation INI file 76
3.2 Example of SIP INVITE message 77
From IPPBX toward Orange BT/BTIP 77
From Orange BT/BTIP toward Customer IPPBX 78
3.3 NTP server configuration 78
Glossary 80

1. General

1.1 Scope of the document

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

1.2 References documents

Title	Link
Business Talk IP/ Business Talk Guidelines Direct for Microsoft Teams Direct routing with Audiocodes eSBC (Oct 2024)	https://documentscontractuels.orange.fr/versions-anglaises_ann_4224.pdf
Business Talk IP / Business Talk Guidelines for Alcatel Lucent OXE with OTSBC /Audiocodes eSBC (June 2025)	https://documentscontractuels.orange.fr/versions-anglaises_ann_4212.pdf
Software Update for AudioCodes eSBCs & Gateways Version 7.20A.XXX.XXX /7.40A.XXX.XXX--	https://www.audiocodes.com/library/firmware https://services.audiocodes.com/
Audiocodes eSBC Portfolio Overview	https://www.audiocodes.com/media/3020/audiocodes-mediant-enterprise-session-border-controllers-sbc-family-brochure.pdf

1.3 Pre- requisites

1.3.1 Certificates

In case of encrypted SIP trunk architecture, TLS configuration is mandatory to exchange a certificate with Orange BT/BTIP A-SBC. Orange's TLS implementation operates in "Mutual Authentication" mode (also known as "two-way" authentication).

The customer must generate on the Audiocodes E-SBC a Certificate Signing Request (CSR) and submit it to a trusted public Certificate Authority (CA) to obtain a publicly signed certificate. After that, the Root CA and any intermediate CA certificates (all in PEM format) must be transmitted to Orange BT/BTIP team.

In return, the Orange BT/BTIP team will provide you with our public Root and intermediate Certificate Authority (CA) certificates. These are the certificates that signed our Orange BT/BTIP A-SBC's certificate and must be imported onto your Audiocodes E-SBC to ensure proper trust and communication.

1.3.2 Public DNS configuration:

For encrypted SIP trunk architecture, public DNS servers must be used for outgoing calls (e.g., from the customer's SIP endpoints to BTol/BTIPol). To meet this requirement, you can configure, in E-SBC configuration, either the IP addresses of two private DNS servers that relay queries to the Internet, or the IPs of two accessible public DNS servers, such as Orange's public DNS (80.10.246.2 and 80.10.246.129).

1.3.3 NTP

The configuration of NTP on the Audiocodes E-SBC is not detailed in this document; however, it is recommended to implement an NTP server to ensure the E-SBC maintains accurate date and time, which is essential for validating remote party certificates. The configuration details are provided in the annex.
This is necessary for validating Certificates of remote parties during TLS "Handcheck".

1.3.4 Firewall flows for BTIP over Internet and BT over Internet

Firewalls in the way of traffic between Audiocodes 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.

1.4 Orange BTalk/BTIP specifications

The information in this chapter is the SIP trunk specifications required to interconnect Orange BT/BTIP network. The Enterprise SBC must be compliant with those specifications. Those information's 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 5621 : Message Body Handling in the Session Initiation Protocol (SIP)*
- *RFC 5806 : Diversion Indication in SIP*
- *RFC 5009 : Private Header Extension to the Session Initiation Protocol for Authorization of early*
- *RFC 8147: Next-Generation Pan-European eCall*

Note : RFC's not listed above are not supported in this context

✓ ***Sip Methods supported:***
- *INVITE*
- *ACK*
- *CANCEL*
- *UPDATE (negotiated)*
- *BYE*
- *OPTIONS*
- *INFO*

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

✓ ***SIP Message size specifications are:***
- *SIP message limited to 4096 Bytes and 1500 Bytes on BTIP*
- *SDP Body limited to 1024 Bytes*

✓ ***SIP signaling 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.***

✓ ***Customer equipment identification***

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

✓ ***Encryption specifications are:***

- **TLS V1.3 (Recommended)**

The corresponding Cipher suites below are supported as Cipher Client/Server:

- **TLS_AES_256_GCM_SHA384 (Recommended)**
- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256

- **TLS V.1.2 (Compatible)**

The corresponding Cipher suites below are 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

✓ ***Media encryption specifications are as follows:***

- SDES key exchange protocol (MIKEY not supported)
- Crypto suite: AES_CM_128_HMAC_SHA1_80
- Both RTP and RTCP are encrypted

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

- List of supported audio codecs and frame size:
  - G.722 20 ms
  - G.711 A law 20 ms, G.711 µ law 20 ms
  - G.729 20 ms, annexb = no

- **Business Talk (BVPN) – international**
  - Either G.711A or µ, G.729 (most preferred codecs list)
  - Or G.711A or µ
  - Or G.729

- **Business Talk over Internet – international**
  - Only G711A or µ is supported.

- **Business Talk P (BVPN) – France**
  - Either G.722, G.711A, G.729 (most preferred codecs list)
  - Or G.722, G.711A
  - Or G.711A, G.729
  - Or G.711A
  - Or G.729

- Business Talk over Internet– France
  - Only G711A is supported.

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

✓ ***DTMF:***

- For Human to Machine, the "telephone-event" [RFC 4733] MUST be used for DTMF transport.
- Only events 0 through 15 are supported.
- Payload type value SHALL be configurable (recommended value is 101).

✓ ***SIP probing:***

- BT/BTIP SIP trunk relies on SIP OPTIONS method to “probe” the E-SBC, both within-dialog and out-of-dialog.

- The following answers are expected:
  - Out of dialog: 200 OK (or any error responses) if the UE is up, no response if the UE is down.
  - Within dialog: 200 OK if the call is active and 481 if the call is no more active.
- The Customer SBC may periodically send OPTIONS messages, each 300s, with Max-Forwards = 0 to probe the BT/BTIP SIP trunk. In this case, the BT/BTIP infrastructure will respond with a 483.
- Session Timer [RFC 4028] is not supported

Commenté [SC1]: Add timer 300s min

Commenté [SC2R1]: DOne

✓ ***FAX support:***

T.38 parameters	Expected value	Parameters' value importance
T.38 Fax over UDP	UDPTL over UDP	Mandatory
Use of NSF/NSC requests	Optional	Optional
NSF value	0	Recommended
		NSF value matching to an existing NSF vendor value is forbidden
		Expected NSF value is 000000 or FFFFFF
Use of NTE ([RFC 4733]) or NSE (Cisco)	No	Mandatory
Fax rate management method	Transferred TCF	Mandatory
UDP redundancy method	T38UDPredundancy	Mandatory
Coding method (fillbitRemoval, JBIG, MMR)	No (MH only)	Mandatory
T.38 version parameter	0	Mandatory
T.30 data	V.21	Mandatory
Data signaling rate	V.17, V.29, V.27ter	At least one of those modulations is mandatory
		Those three modulations are highly recommended
		Any other modulation (like V.34) is forbidden
Error Correction Method	Enabled	Highly recommended
V.8 parameter	Disabled	Mandatory
Polling mode	Disabled	Mandatory
Fax rate	14400 bps	Recommended
		Any fax rate greater than 14,4kbps is forbidden
Low speed T.38 redundancy	4	LS redundancy is mandatory
		Level 4 is recommended
High speed T.38 redundancy	1	HS redundancy is mandatory
		Level higher than 1 is forbidden
SG3-G3 fallback method	Either ANSam removal	Mandatory
	or CM removal	
T.38 payload size	40 ms	Highly recommended
		Any payload size different from 40 and 20 ms is forbidden
Switching from voice mode to fax mode	T.38 Re-INVITE sent as callee AND as caller (BTalk and BTIP)	Mandatory

Note: For T.38 the Ribbon E-SBC will be transparent. No adaptation will be done at the SBC level; DSP resources would be required in certain conditions.

✓ ***Packet marking:***

- Both SIP signaling and audio must be marked with DSCP 46 (Expedited Forwarding).

✓ ***Call initiation:***

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

✓ ***Media session modification:***

- 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".
- Same Methods/Attributes/headers may be sent from BTalk/BTIP to Customer SBC.
- Call Transfer
  - For supervised call transfer, sends RE-INVITE in confirmed dialog
  - For blind call transfer:
    - send RE-INVITE in confirmed dialog
- Call Forward
  - In case of Call Forward, the diversion header must be provided by the Customer SBC to maintain the original caller information.
- Call on Hold
  - Send SDP with a=inactive; Setting connection to 0.0.0.0 FORBIDDEN.
- Music on Hold
  - Initiate a new INVITE to the media server
  - Use Re-INVITE to stop, closing the second dialog.

✓ ***3-Way Conference***

- Use a media mixer with existing dialogs
- "Join" header [RFC 3911] NOT SUPPORTED by Orange.

✓ ***Ring back tone and early media:***

- ***Incoming calls***
  - Use the "P-Early-Media" header in 18x responses to signal early media transmission. Nevertheless, the service does not guarantee to relay this early media (depending on specific agreement)
  - If SIP endpoint sends a 18x response with SDP without "P-Early-Media", it SHOULD send a ring back tone. However, this tone may not be heard by the remote party.
- ***Outgoing calls***
  - Presence of "P-Early-Media" header with "sendrecv" or "sendonly" values in 18x responses indicates that early media will be sent. SIP endpoint SHALL inhibit local tones generation and wait for incoming audio.
  - If "P-Early-Media" header with "inactive" or "recvonly" values is set in 18x responses, SIP endpoint SHALL generate local tones.
  - If "P-Early-Media" header is not set in 18x responses, SIP endpoint SHOULD generate local tones unless it can detect early media sent by the remote party.

✓ ***Anonymous calls:***

- If anonymization is requested, the Customer SBC should:
  - Set the Privacy header to at least "user" and ensure the From header contains the calling party's identity.

    Or
  - Set the Privacy header to at least "id". Ensure the From header contains an anonymous URI (such as "Anonymous" sip:anonymous@anonymous.invalid), and the P-Asserted-Identity header contains the calling party's identity.

✓ ***Number format specifications are:***

- Called party identities must be sent to the Orange network in E.164 format (i.e. +CCNSN).
- Calling party identities must be sent to the Orange network in E.164 format (i.e. +CCNSN).

✓ ***Rerouting scenario:***

- On reception of an error response, the customer SIP endpoint must try a second route towards the backup BT/BTIP A-SBC if response code is either **408** or **5xx**.
- When a customer has multiple components (e.g., active/backup servers), upon receiving an error response from a SIP endpoint, the BT/BTIP core network will reroute the call to a backup SIP endpoint if the response code is **408** or **5xx**.

✓ ***Call defection:***

- Sends only RE-INVITE in confirmed dialog.
- INVITE sent to the deflection destination SHOULD include Diversion header with Deflection reason.
- 3xx Sip messages are not supported by BTalk/BTIP services. Those messages will be converted into SIP error messages.
- "Retry-After" ignored by Orange.

✓ ***RTCP***

- Customer SBC will receive reports every 5 seconds from Orange backbone, and it is recommended that SIP endpoint generates RTCP reports

✓ ***STIR SHAKEN***

- If caller identity authentication is requested, SIP endpoint MUST accept to receive the following information:
  - Identity (up to 650 bytes), P-Attestation-Indicator, P-Origination-ID headers
  - Verstat parameter in user-part of From, P-Asserted-Identity and Diversion headers.

2. Certified Architecture

2.1 Introduction to architecture components and features

This document provides configuration guidelines for the Audiocodes E-SBC north (carrier) interface used by the **Orange Business (OB)** within the **VISIT Program**.

It outlines the configuration requirements necessary to ensure interoperability between the Audiocodes E-SBC and the Business Talk (BT) and Business Talk IP (BTIP) SIP infrastructure, including the A-SBC, Application Server, and interconnections with the PSTN or SIP carriers.

These guidelines apply specifically to the north (carrier) side of the Audiocodes E-SBC, which interfaces with BT and BTIP services:

- The configuration will **only consider the Carrier aspect** of the Audiocodes E-SBC (north side), which faces BT/BTIP offers.
- The **E-SBC's North-side SIP termination will act as the demarcation point for Orange Business.**
- The **south side of the Audiocodes E-SBC falls outside of OB's control and responsibility.**

The primary objective of these guidelines is to ensure that the Audiocodes E-SBC configuration complies with the requirements (SIP/T.38 profile) of BT and BTIP offers. **Any complexities introduced by diverse UC/IPBX environments must be managed on the south side and fall outside of OB's responsibility**

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.

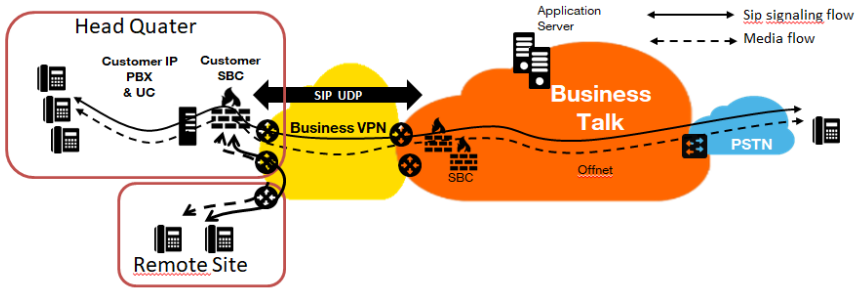
Concerning the fax support, BTalk and BTIP support the following usage:

- 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.

.

2.2 Architecture with Audiocodes “customer” eSBC

2.2.1 Unencrypted SIP Trunk through BVPN

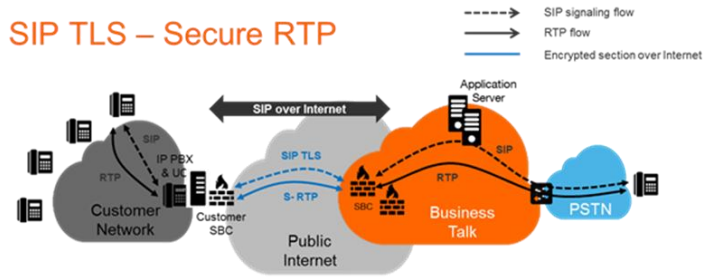


In this architecture:

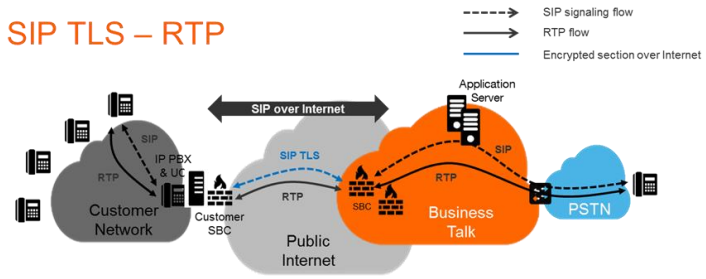
- Both SIP SIG and RTP media flows between endpoints and the BT/BTIP are anchored by the customer SBC.
- For Headquarter, SIP SIG flows are routed through the Customer SBC and RTP media flows are direct to private “South” interface of the E-SBC through the main BVPN connection.
- For remote sites interconnected through BVPN, SIG flows are routed through the Customer SBC and RTP media flows are direct to private “South” interface of the E-SBC and the main BVPN connection.
- For remote sites interconnected through 3rd Party Wan, both SIP SIG & RTP media flows are routed through the Customer SBC direct to private “South” interface of the E-SBC through the main BVPN connection.

2.2.2 Encrypted SIP Trunk Over Internet

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



- **SIP over TLS + (unencrypted) RTP**: all SIP messages are encrypted on the public internet between Orange and the customer's SIP endpoints. RTP flows are shared without encryption between the customer media endpoints and Orange's backbone. This solution is not recommended by Orange but is allowed as an alternative when customers face encryption/decryption limitations.



2.2.3 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 SBC – architecture with E-SBC	Level of Service	@IP used by service	
1 Single Customer SBC	No redundancy	E-SBC @IP	
2 Customer SBC Nominal / Backup mode	- **Local redundancy**: both SBC are hosted on the same site *OR* - **Geographical redundancy** both SBC are hosted on 2 different sites	E-SBC1 @IP	E-SBC2 @IP
2 Customer SBC in Load Sharing	- **Local redundancy**: both SBC are hosted on the same site *OR* - **Geographical redundancy** both SBC are hosted on 2 different sites	E-SBC1 @IP E-SBC2 @IP	
2 Customer SBC in HA mode (Cluster)	- **Local redundancy:** both SBC are hosted on the same site *OR* **- Geographical redundancy** both SBC are hosted on 2 different sites **warning:** Link level 2 between SBC with max delay 50ms required for geo-redundancy	E-SBC VIP @IP	

Encrypted SIP Trunk through Internet

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

Customer SBC – architecture with E-SBC	Level of Service	@IP used by service	
1 Single Customer SBC	No redundancy	E-SBC1 @IP or Public FQDN	
2 Customer SBC Nominal / Backup mode	- **Local redundancy**: both SBC are hosted on the same site *OR* - **Geographical redundancy** both SBC are hosted on 2 different sites	E-SBC1 @IP or Public FQDN	E-SBC2 @IP or Public FQDN
2 Customer SBC in Load Sharing	- **Local redundancy**: both SBC are hosted on the same site *OR* - **Geographical redundancy** both SBC are hosted on 2 different sites	E-SBC1 @IP or Public FQDN E-SBC2 @IP or Public FQDN	
2 Customer SBC in HA mode (Cluster)	- **Local redundancy:** both SBC are hosted on the same site *OR* **- Geographical redundancy** both SBC are hosted on 2 different sites **warning:** Link level 2 between SBC with max delay 50ms required for geo-	E-SBC VIP @IP	

	redundancy	

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

Customer SBC – architecture with E-SBC	Level of Service	@IP used by service	
1 Single Customer SBC	No redundancy	E-SBC1 FQDN Type A	
2 Customer SBC Nominal / Backup mode (**DNS Resiliency model**)	- **Local redundancy**: both SBC are hosted on the same site OR - **Geographical redundancy** both SBC are hosted on 2 different sites	E-SBC public FQDN DNS Type **SRV**	
2 Customer SBC Nominal / Backup mode (**SIP Resiliency model**)	- **Local redundancy**: both SBC are hosted on the same site OR - **Geographical redundancy** both SBC are hosted on 2 different sites	E-SBC1 FQDN Type A *	E-SBC2 FQDN Type A*
2 Customer SBC in Load Sharing (**SIP Resiliency model**)	- **Local redundancy**: both SBC are hosted on the same site OR - **Geographical redundancy** both SBC are hosted on 2 different sites	E-SBC1 FQDN Type A* E-SBC2 FQDN Type A*	
2 Customer SBC in HA mode (Cluster) **(IP Resiliency model)**	- **Local redundancy:** both SBC are hosted on the same site OR - **Geographical redundancy** both SBC are hosted on 2 different sites **warning:** Link level 2 between SBC with max delay 50ms required for geo-redundancy	E-SBC VIP FQDN type A*	

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

2.3 BTalk & BTIP Audiocodes eSBC certified versions

Audiocodes eSBC – software versions				
Reference product	Hardware or Virtual Model	Software version	Certified "Loads"	Certification
Hybrid enterprise eSBC	**Mediant 500 /500L**	V.7.20A	LTS Load(s) 7.20A.252.254*	✓
	Mediant 800			
	Mediant 1000			
	Mediant 3100			
Pure enterprise eSBC	**Mediant 2600**	V.7.40A	LTS Load(s) 7.40A.501.871*	✓
	Mediant 4000			
	Mediant 9000			
	Mediant Server Edition			
	Mediant Virtual Edition			
	Mediant Cloud Edition (MS Azure, AWS, Google Cloud)			

* Minimum Load supported for implementation.

Note: Last most up-to-date Load is recommended per Audiocodes vendor: By default, Long Term Support (LTS) versions/ Loads, and on specific, Lastest Release (LR).

2.4 Audiocodes Global configuration

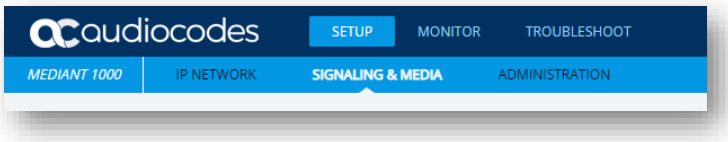
2.4.1 Objects

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.

2.4.2 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 Or PS_BTIP	SI_BT Or SI_BTIP	--	Using OPTIONS	** @IP_eSBC_BT:5060 ** Or ** @IP_eSBC_BTIP:5060 **	UDP
2	*PS_IPBX*	*SI_IPBX*	*--*	*Using OPTIONS*	*** @IP_IPBX:5060 *****	*UDP*

Example

2.5 Orange Business BTalk & BTIP Carrier unencrypted SIP configuration for AudioCodes eSBC (UDP)

2.5.1 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.

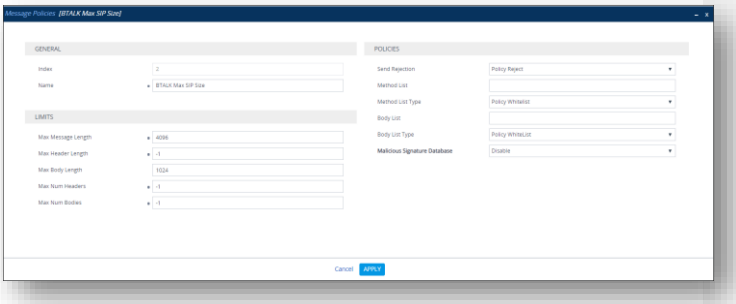
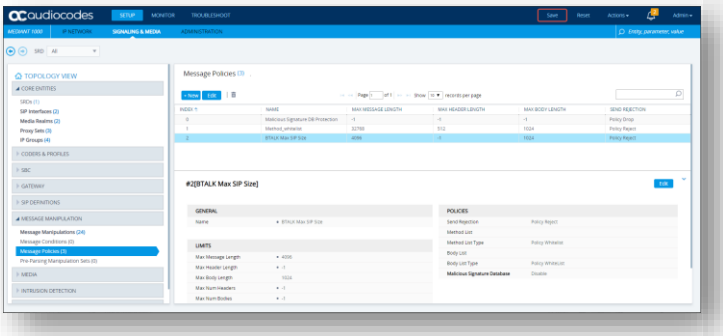
2.5.2 Message Manipulation Policy

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
1. Open SETUP > SIGNALING & MEDIA > MESSAGE MANIPULATION >MESSAGE POLICIES 2. Click on "+ New" 3. Enter a meaningful name ex" **BTALK Max SIP Size**" 4. Click on "Apply"	
The number Policy will appear in the list	

2.5.3 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).***

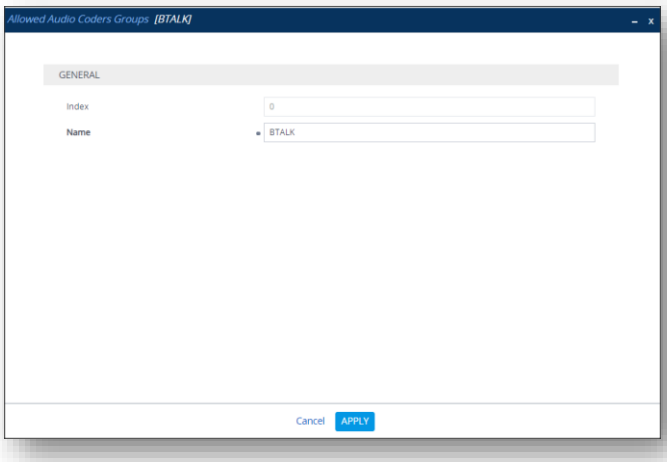
Note: G.711 µ-law 20 ms can be requested to Orange, specifically on demand. If this is the case, it should just be added to the codec list in this VoIP profile. ***G.722 isn't currently supported through Business Talk over Internet context.***

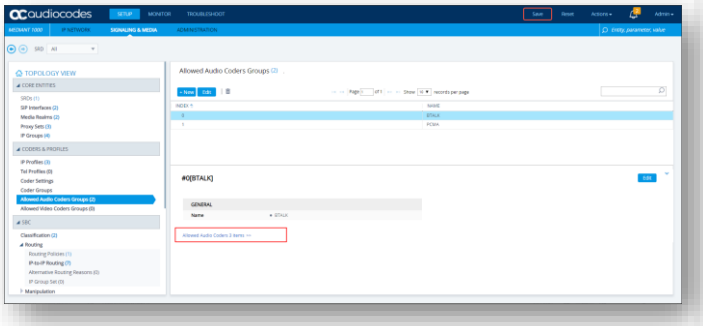
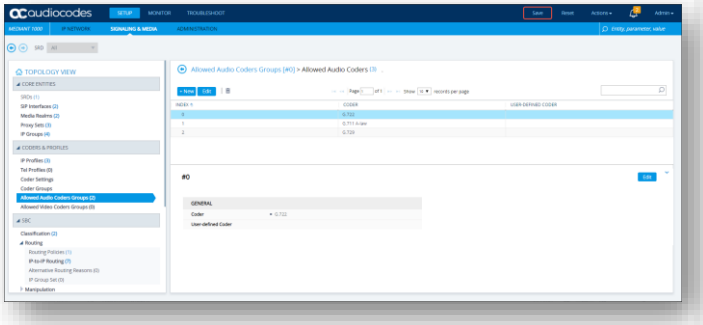
We are going to create a new "Coders Groups" specific to Orange BTIP (please adapt it for BTalk).

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
1. Open SETUP > SIGNALING & MEDIA > CODERS & PROFILES > Allowed Audio Coders Groups 2. Click on "+ New" 3. Enter a meaningful name ex" BTALK" or "BTIP" 4. Click on "Apply" 5. Click on "Allowed Audio Coders 0 items"	

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

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.

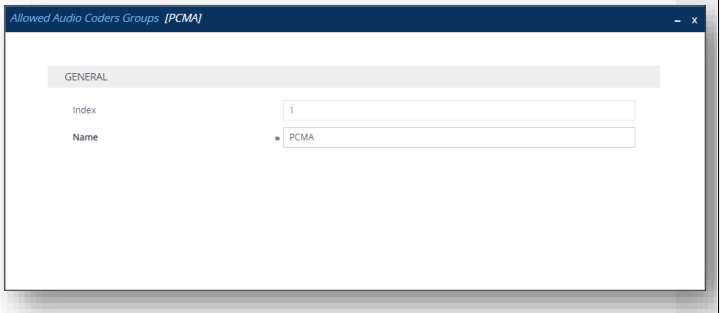
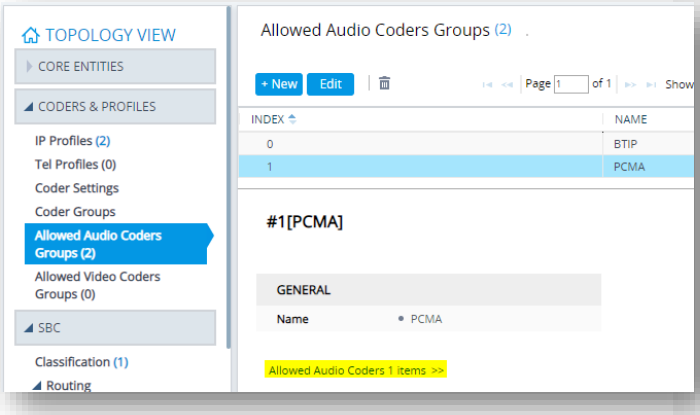
***Note:** If you are in this case you don't need to create the "BT/BTIP" "Allow Coders Group" described in the previous chapters.*

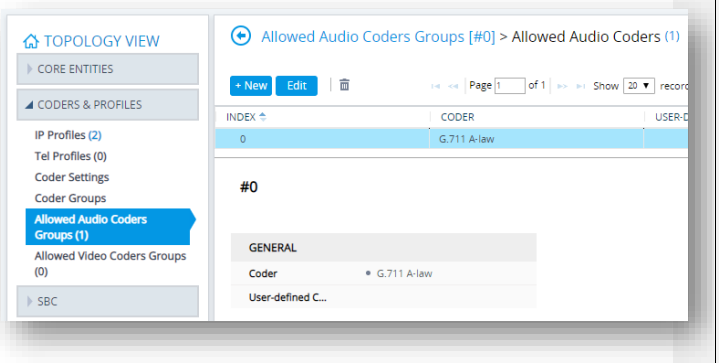
We are going to create a new "Coders Groups" specific to Orange BTalk.

Index	Name
1	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
1. Open SETUP > SIGNALING & MEDIA > CODERS & PROFILES > Allowed Audio Coders Groups **2.** Click on “+ New” **3.** Enter a meaningful name ex” **PCMA**” **4.** Click on “Apply” **5.** Click on “Allowed Audio Coders 0 items”	
6. Click on “+ New” **7.** Select the coders as mentioned in the table of parameters above, in the same order **Please note:** Do not select “G711 A-law VBD” or “EG-711 A-law” as they are not regular G711a codecs	

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**"*

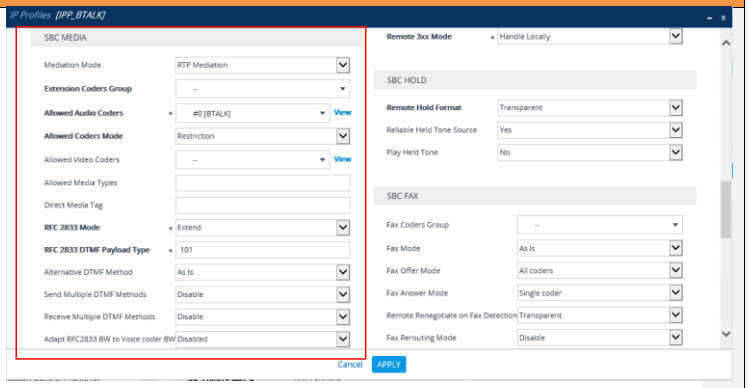
Index	Name	Allowed Audio Coders	Allowed Coders Mode	RFC2833 Mode	RFC2833 DTMF Payload Type	Use Silence Suppression	RTP Redundancy Mode
1	IPP_BTALK Or IPP_BTIP	BTALK Or BTIP	Restriction	Extend	101	Remove	Disable

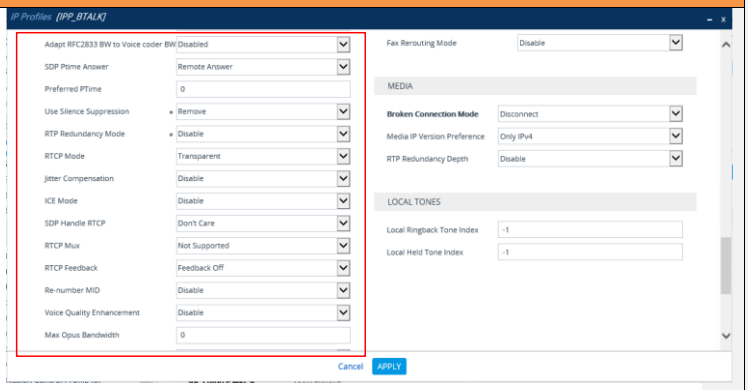
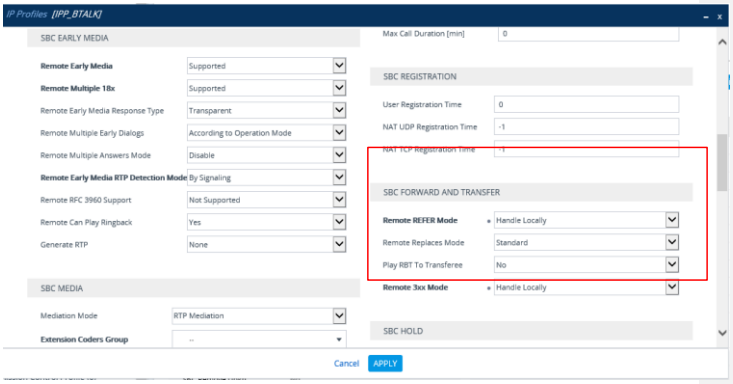
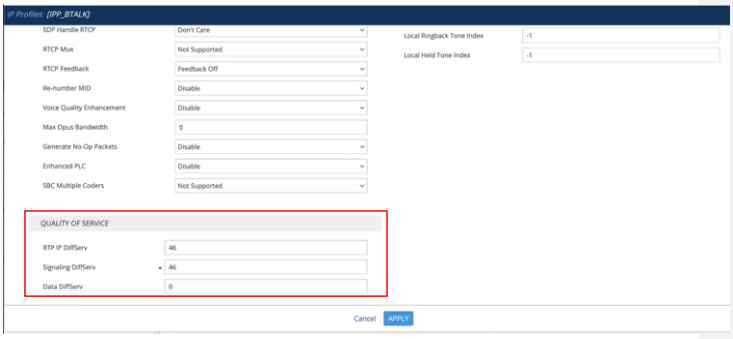
*"Section: **Quality of Service**"*

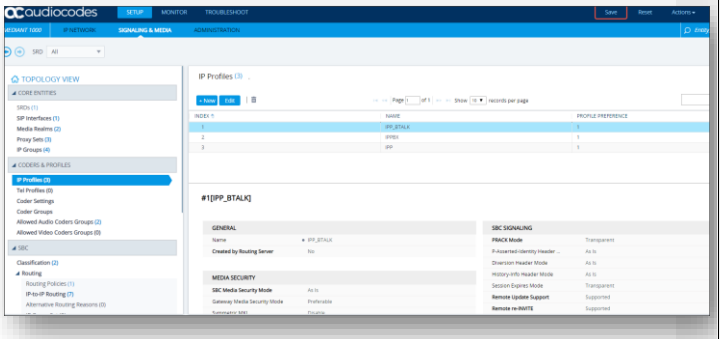
Signaling DiffServ
46

*"Section: **eSBC Forward and Transfer**"*

Remote REFER Mode	Remote 3xx Mode
Handle Locally	Handle Locally

Actions	Screenshot
1. Open SETUP > SIGNALING & MEDIA > CODERS & PROFILES > IP Profiles 2. Click on "+ New" Enter a meaningful name, ex" IPP_BTALK" or "IPP_BTIP" 3. Change the parameters indicated above as follow	

Actions	Screenshot
	
	
	

Actions	Screenshot
Click on “Apply” The new Objects will appear in the list.	

2.5.4 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.

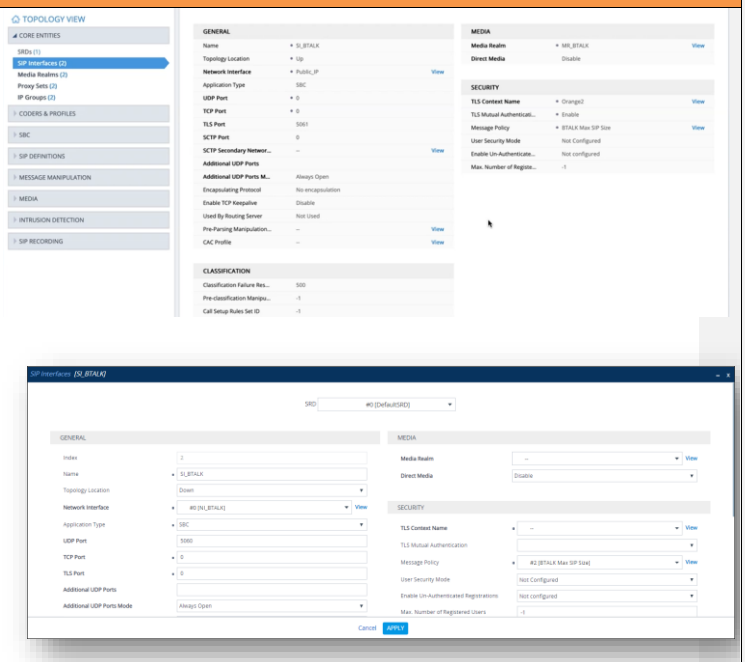
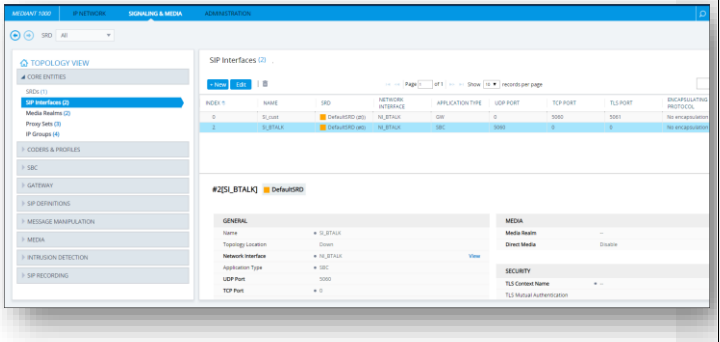
This SIP signaling will be configured to be compliant with Orange BTalk specifications:

- ✓ 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
1. Open SETUP > SIGNALING & MEDIA > CORE ENTITIES > SIP Interfaces 2. Click on "+ New" Enter a meaningful name Ex: "**SI_BTALK**" or "**SI_BTIP**" 3. Change the parameters indicated above as follow	
Click on "Apply" The new Objects will appear in the list.	

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:

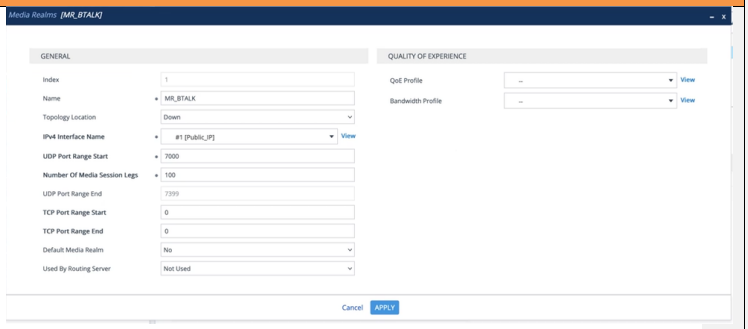
- ✓ For **unencrypted BT/BTIP SIP Trunk** architecture, we need to configure **RTP port 6 000 to 20 000**

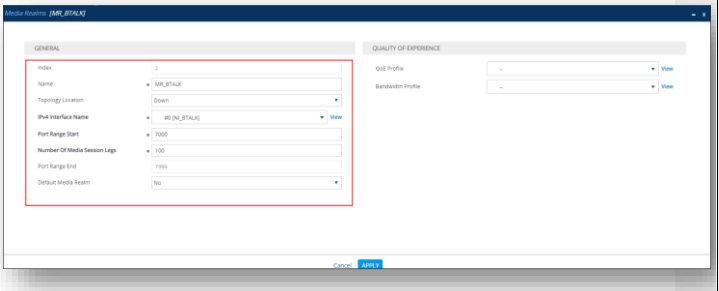
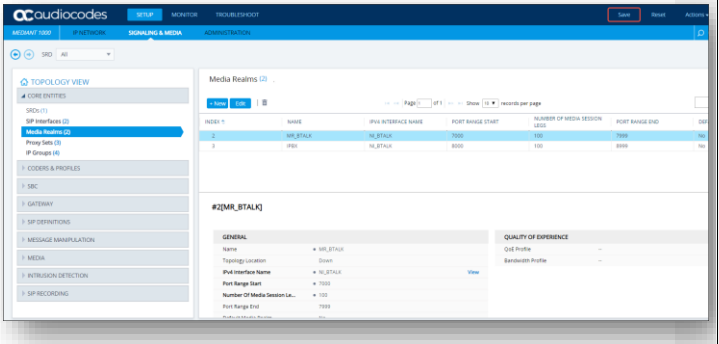
Note: On Audiocodes eSBC, for RTP port range keep in mind that the RTP UDP port spacing is "10". This mean that for example 5 sessions SIP, 5*10 ports RTP from 6000 to 60050 will be reserved.

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
1. Open SETUP > SIGNALING & MEDIA > CORE ENTITIES > MEDIA REALMS 2. Click on "+ New" Enter a meaningful name ex" **MR_BTALK**" or **MR_BTIP** 3. Change the parameters indicated above as follow	

Actions	Screenshot
	
Click on “Apply” The new Objects will appear in the list.	

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.

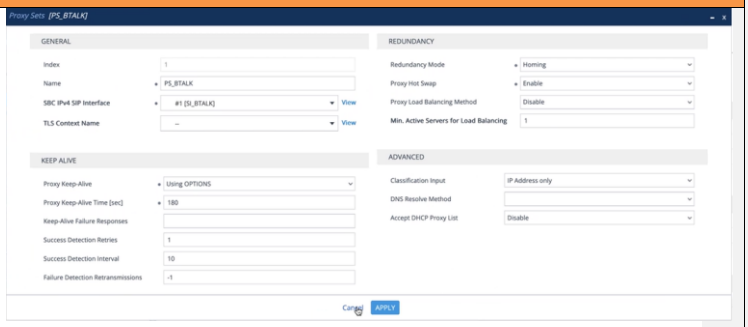
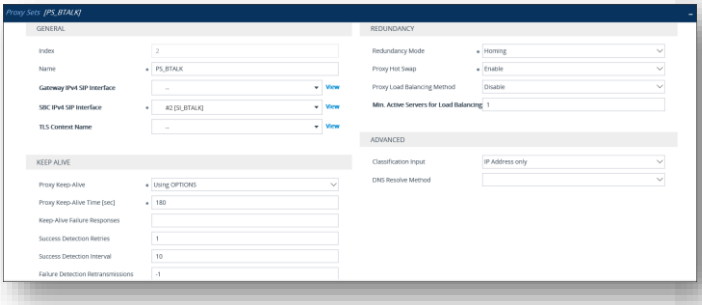
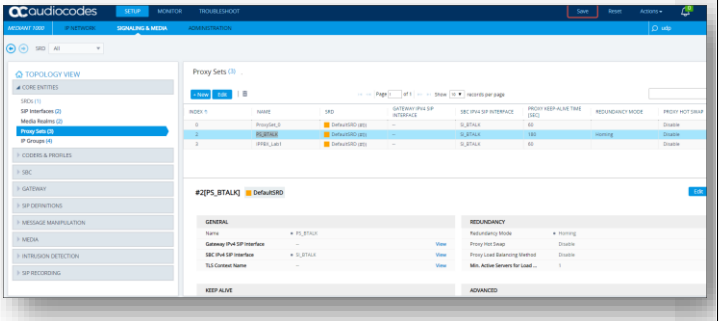
This Proxy will be configured to be compliant with Orange BTalk specification:

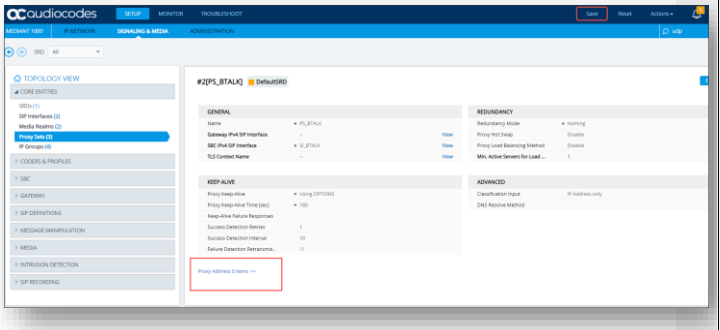
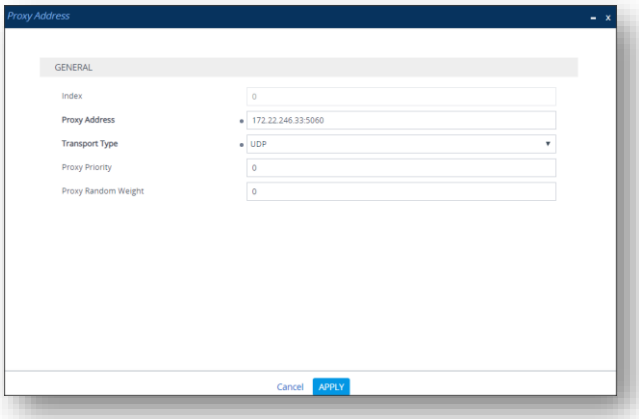
- ✓ For **unencrypted BT/BTIP SIP Trunk** architecture, we need to configure **UDP port 5060**
- ✓ For Sip trunk keep alive done with "**Options**" message (every 300 seconds)
- ✓ For Sip trunk redundancy **Homing** (the first Proxy Address is always select if available) and Proxy Hot swap **Enable** (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

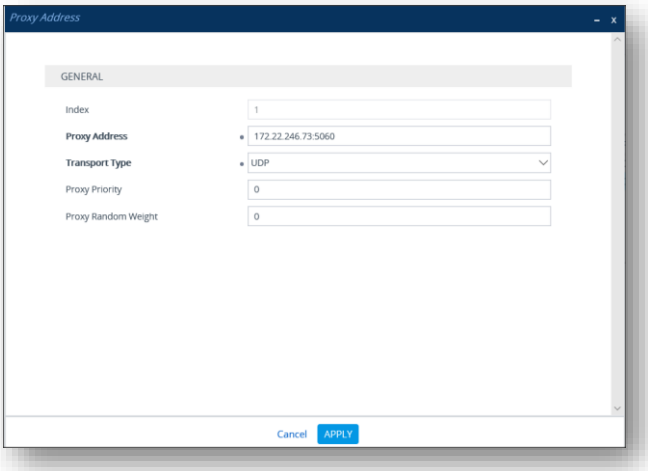
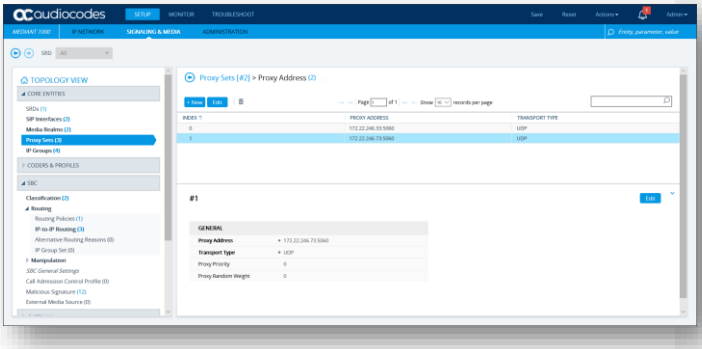
Index	Name	SIP Interface	TLS Context Name	Proxy Keep-Alive	Redundancy Mode	Proxy Hot Swap	Index Proxy Address	Proxy Address	Transport Type
1	PS_BTALK Or PS_BTIP	SI_BTALK Or SI_BTIP	--	Using OPTIONS	Homing	Enable	0 1 0 1	<BT_Nominal IP>:5060 <BT_Backup IP>:5060 <BTIP_Nominal IP>:5060 <BTIP_Backup IP>:5060	UDP UDP
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
1. Open SETUP > SIGNALING & MEDIA > CORE ENTITIES > PROXY SETS 2. Click on "+ New" Enter a meaningful name ex "**PS_BTALK**" or "**PS_BTIP**" 3. Change the parameters indicated above as follow	 
4. Click on "Apply". The new Objects will appear in the list.	
5. To configure "**Proxy Address**" and "**Transport Type**", you have to configure to select the "Proxy Set" just created.	

Actions	Screenshot
6. Click on the "Proxy Address 0 items" link at the bottom of the page. **7.** Configure though **index 0 for the nominal Proxy address** <BT_Nominal__IP> or <BTIP_Nominal_IP> . **8.** You have to configure though **Index 1 for the backup Proxy address** to backup the nominal ones with <BT_Backupl_Public_IP> or <BTIP_Backup_Public FQDN > . **1.** At the End at least 2 Proxy Items should be configured: - Index 0 for Nominal within BT nominal IP (first IP) or BTIP nominal IP (Second IP) - Index 1 for BT backup IP (first IP) or BTIP backup IP (Second IP)	 

Actions	Screenshot
	 

IP Group Table

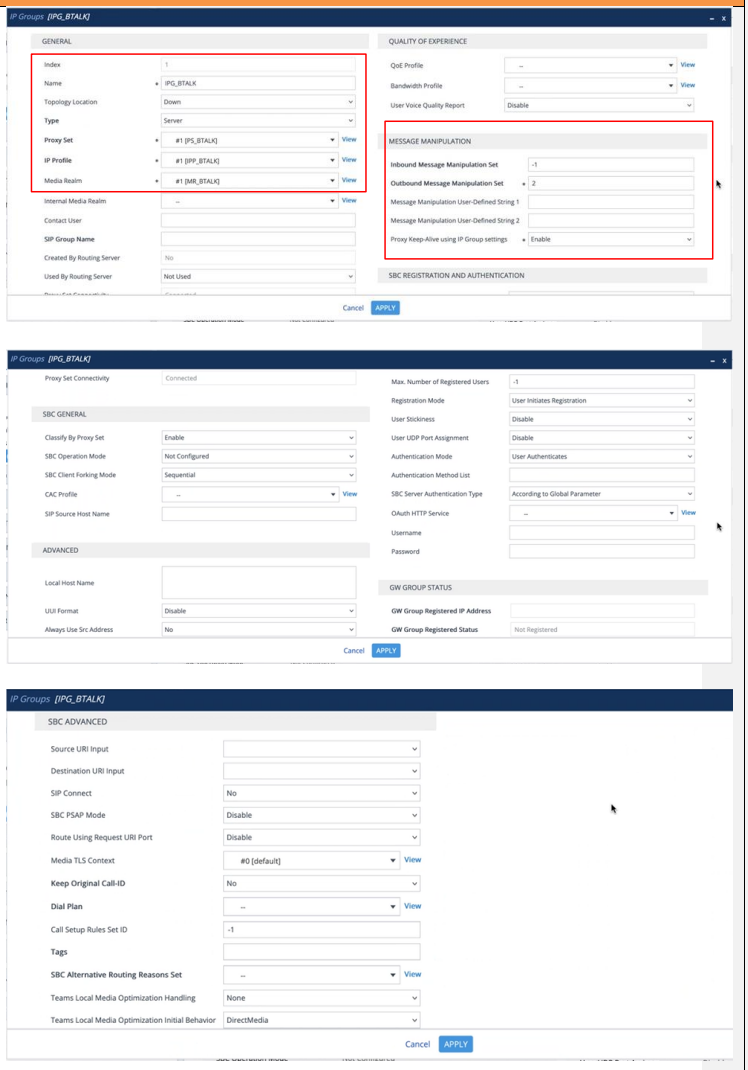
The IP Group table allows logical IP entities creation with a set of parameters such as Proxy set ID, IP profile ID to separate provenance and destination traffic.

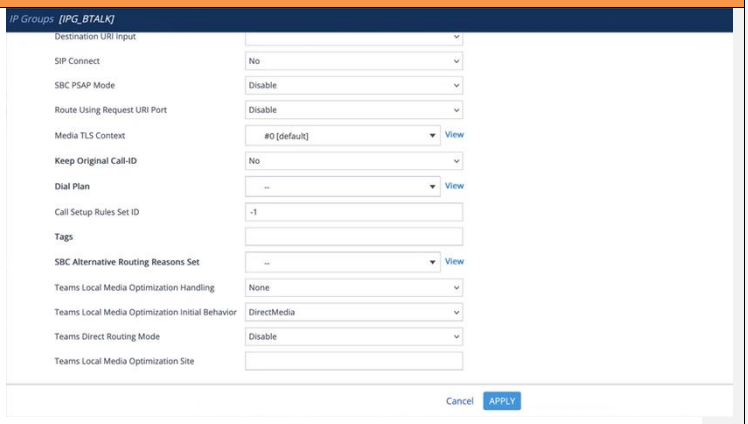
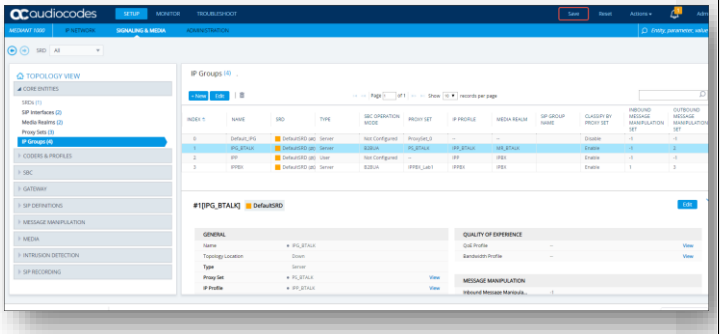
A new IP Group specific to Orange BT/BTIP SIP Trunk needs to be create as **Server Back-to-back** (B2BUA) with message **Manipulation on the outgoing Orange side**. The IP Group will be composed of the objects previously created in the table: Media Realm, Proxy Set and IP Profile.

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
1. Open SETUP > SIGNALING & MEDIA > CORE ENTITIES >IP_GROUP 2. Click on "+ New" Enter a meaningful name ex " **IPG_BTALK**" or "**IPG_BTIP**" 3. Click on "Apply" 4. Click on "Allowed Audio Coders 0 items"	

Actions	Screenshot
	
5. Click on “Apply”. The new Objects will appear in the list.	

2.5.5 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

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

As a prerequisite Audiocodes recommends reading the Audiocodes Security vulnerabiliy handling to understand how to secure the eSBC into your network infrastructure, especially facing Internet.

2.6.1 Configure IP Network

Same recommendations as in § 2.5.1

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

2.6.2 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 V1.3** or most possibly supported **TLS V1.2**
- ✓ **Key size 2048**
- ✓ **Cipher list per below is recommended as Cipher Client/Server through TLS V1.3:**
  - **TLS_AES_256_GCM_SHA384 (Recommended)**
  - TLS_AES_128_GCM_SHA256
  - TLS_CHACHA20_POLY1305_SHA256
- ✓ **Cipher list per below is compatible as Cipher Client/Server through TLS V1.2:**
  - **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (Compatible)**
  - 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 Mutual authentication activated.**

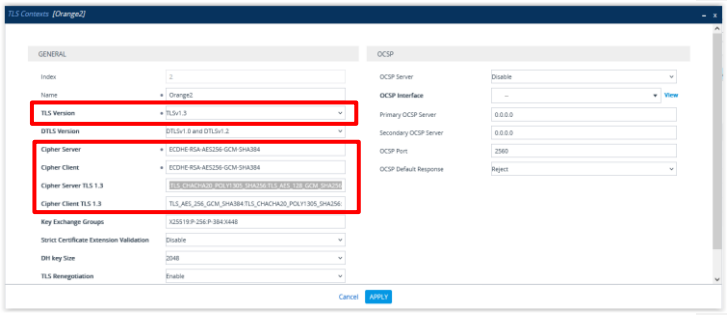
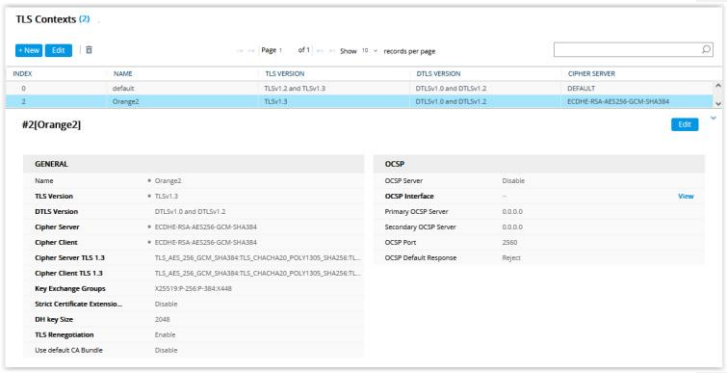
The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

Through TLS V1.3 for V.7.40A :

Index	Name	Cipher Server	Cipher Client	DH key Size
1	Orange2	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256	TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256	2048

Through TLS V1.2 for V7.20A

Index	Name	Cipher Server	Cipher Client	DH key Size
1	Orange2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	2048

Actions	Screenshot
1. Open SETUP > IP NETWORK > SECURITY > TLS CONTEXTS 2. Click on "+ New" Enter a meaningful name ex" **Orange**" 3. Change the parameters indicated above as follow and referring at parameters tables above depending of eSBC/ TLS version supported.	
Click on "Apply" The new Objects will appear in the list.	

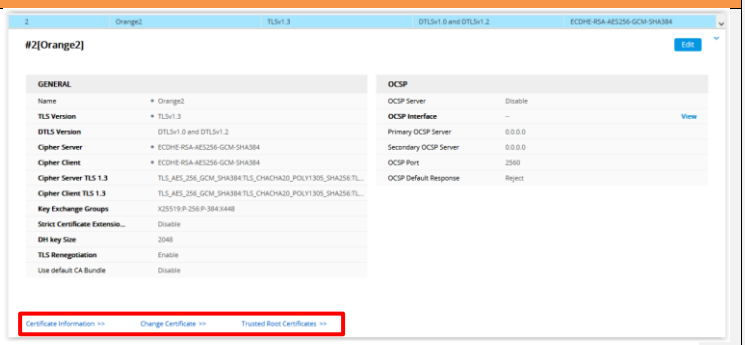
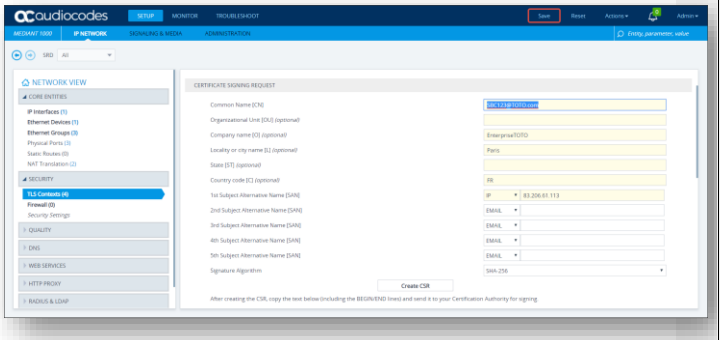
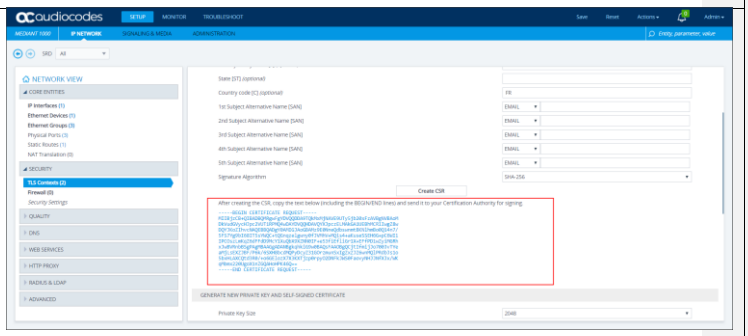
STEP 1: Generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority (CA)

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
SBC123@TOTO.com	-Group X	Enterprise TOTO	Paris	FR

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	
1. On the TLS context you just create go on the Bottom page and click on “Change Certificate” 2. Change the parameters indicated above 3. Click “Create CSR”	 
4. On the page should appear a text in blue which represent your CSR.	

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.

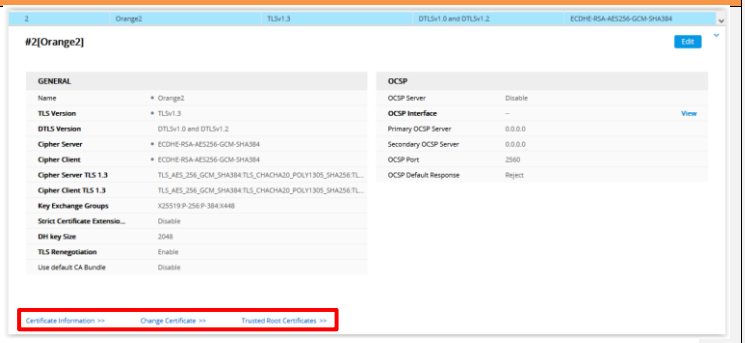
STEP 2: Deploy the eSBC and Root/Intermediate Certificates on the eSBC

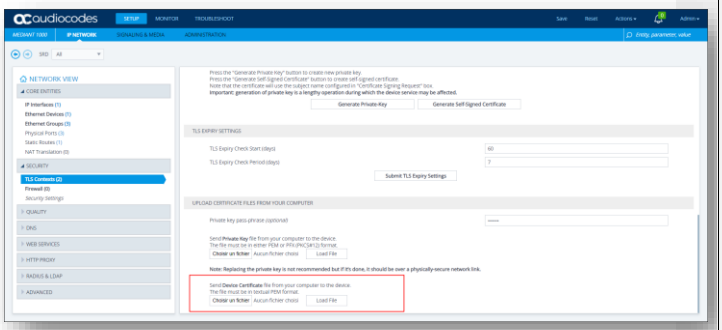
When you have the CA files (p7b and bundle), please load it on the TLS Context just create. Only **Base64 (PEM)** encoded X.509 certificates can be loaded to the Audiocodes eSBC.

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/MQswCQYDVQQGEwJGUjETMBEGA1U
EChMKQ2VydGlwb3N0ZTEbMBkGA1UEAxMSQ2VydGlwb3N0ZSBTZXJ2ZXVyMB4XDTk4MDYyNDA4MD
AwMFoXDTE4MDYyNDA4MDAwMFowPzELMAkGA1UEBhMCRlIxEzARBgNVBAoTCkNlcnRpcG9zdGUxG
zAZBgNVBAMTEkNlcnRpcG9zdGUgU2VydmV1cjCCASEwDQYJKoZIhvcNAQEBBQADggEOADCCAQkC
ggEAPqd4MziR4spWldGRx8bQrhZkonWnNm`+Yhb7+4Q67ecf1janH7GcN/SXsfx7jJpreWULf7v
7Cvpr4R7qIJcmdHIntmf7JPM5n6cDBv17uSW63er7NkVnMFHwK1QaGFLMybFkzaeGrvFm4k3lRe
fiXDmuOe+FhJgHYezYHf44LvPRPwhSrzi9+Aq3o8pWDguJuZDIUP1F1jMa+LPwvREXfFcUW+w==
-----END
```

eSBC Certificate

Actions	
5. On the TLS context you created go on the Bottom page and click on "Change Certificate" 6. Scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the cert.txt file, and then click **Load File**. 7. After the certificate successfully loads to the device, save the configuration with a device reset. 8. Verify that the private key is correct: -Open the TLS	

Actions	
Contexts table. -Select the required TLS Context index row. -Click the Certificate Information link located below the table.	

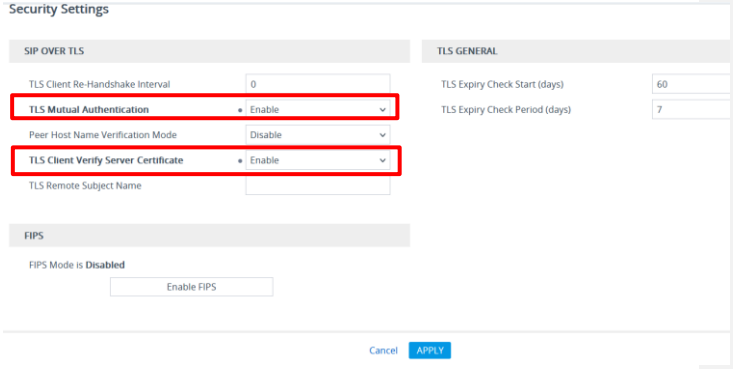
Customer Root / Intermediate Certificates authority:

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

STEP 3: Import Orange Certificates Authorities (Root and Intermediate) like done for the Customer Root / Intermediate Certificates authority

STEP 4 : Communicate Customer Public Certificates Authorities (Root and Intermediate) information's which signed your eSBC certificate to Orange BTALK Team

Mutual TLS Authentication

Actions	
1. Select SECURITY, Security settings options 2. Enable both " TLS Mutual Authentication" & "TLS Client Verify Server Certificate" options 3. Apply changes then Save config	

2.6.3 Media Security

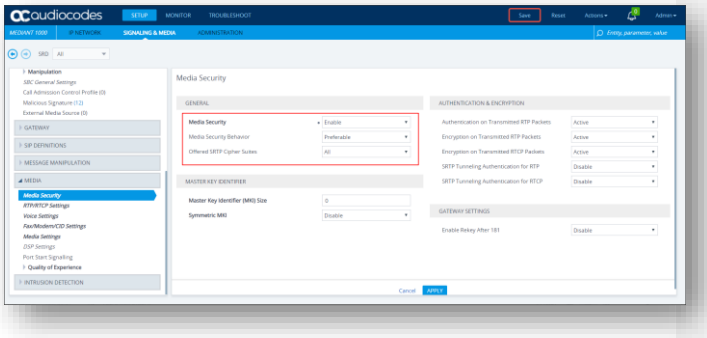
This section allows to Enable the media security protocol (SRTP). This is needed only in case the connection with BTALK is using Media encryption in addition of encrypted SIP connection via TLS encryption.

This Media encryption must be configured to be compliant with Orange BTalk crypto suite specification:

- ✓ AES_CM_128_hmac_SHA1_80

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	Comments
Enable	Preferable	All (AES_CM_128_HMAC_SHA1_32, **AES_CM_128_HMAC_SHA1_80**, AES_256_CM_HMAC_SHA1_32, AES_256_CM_HMAC_SHA1_80)	AES_CM_128_HMAC_SHA1_80 will be negotiated though SIP SDP offer

Actions	Screenshot
1. Open SETUP > SIGNALING & MEDIA > MEDIA >MEDIA SECURITY 2. Change the parameters indicated above as follow 3. Click on “Apply	

2.6.4 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

2.6.5 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.

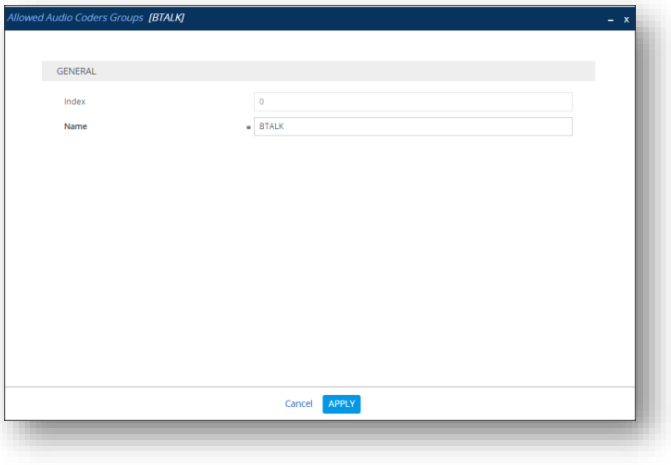
Orange accepts the following codecs in this order or preference:
- G.711 A-law 20 ms for French BTIPol / BTol Offers (or G.711 µ-law 20 ms for International BT Offer).

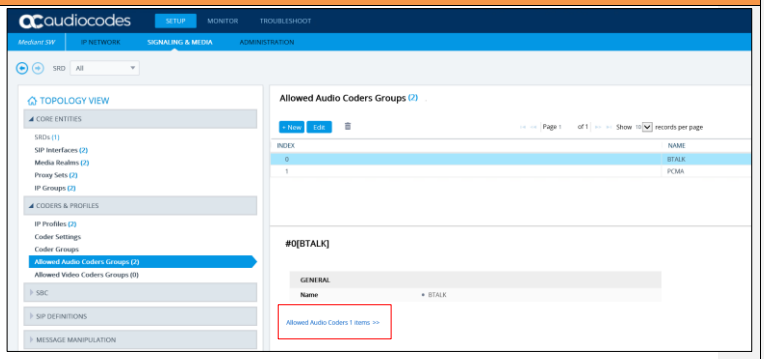
We are going to create a new "Coders Groups" specific to Orange BTalk.

Index	Name
0	BTALK
1	*PS_IPBX*

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

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

Actions	Screenshot
1. Open SETUP > SIGNALING & MEDIA > CODERS & PROFILES > Allowed Audio Coders Groups 2. Click on "+ New" 3. Enter a meaningful name ex" **BTALK**" 4. Click on "Apply" 5. Click on "Allowed Audio Coders 0 items"	

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

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.

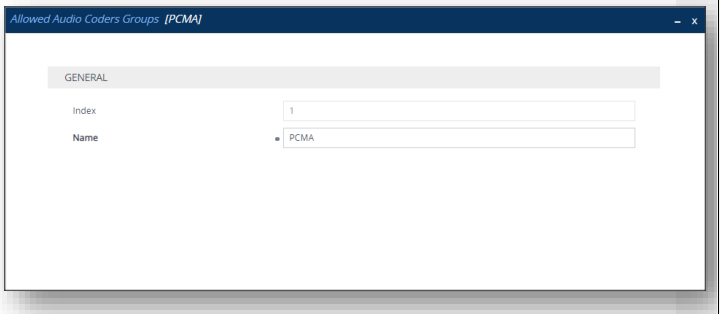
***Note:** If you are in this case you don't need to create the "BTIP" "Allow Coders Group" describe in the previous chapters.*

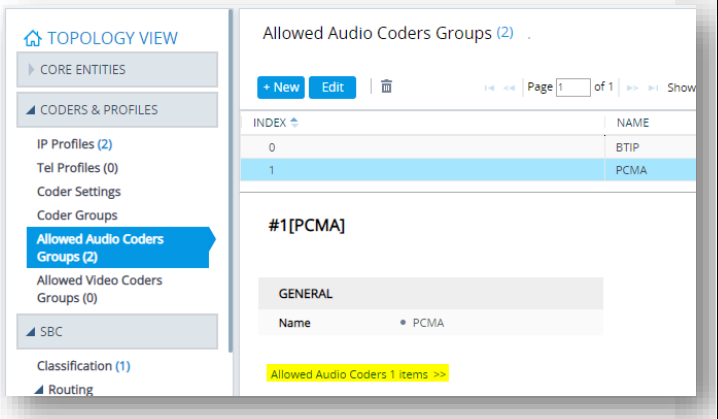
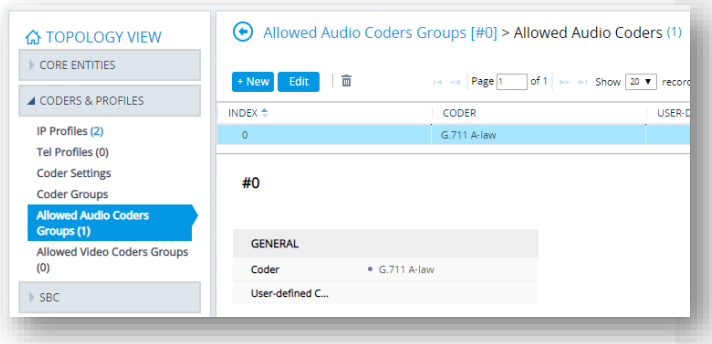
We are going to create a new "Coders Groups" specific to Orange BTalk.

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
8. Open SETUP > SIGNALING & MEDIA > CODERS & PROFILES > Allowed Audio Coders Groups **9.** Click on "+ New" **10.** Enter a meaningful name ex" **PCMA**" **11.** Click on "Apply" **12.** Click on "Allowed Audio Coders 0 items"	

Actions	Screenshot
13. Click on "+ New" **14.** Select the coders as mention in the table of parameters above, in the same order Please note: Do not select "G711 A-law VBD" or "EG-711 A-law" as they are not regular G711a codecs	 

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, e**SBC Prack Mode** : **Mandatory** on the IP profile of the Customer IPPBX.*
All of those conversions will stayed under customer responsabilities 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
SRTP	YES
RTP	*No*

"*Section: **eSBC Media***"

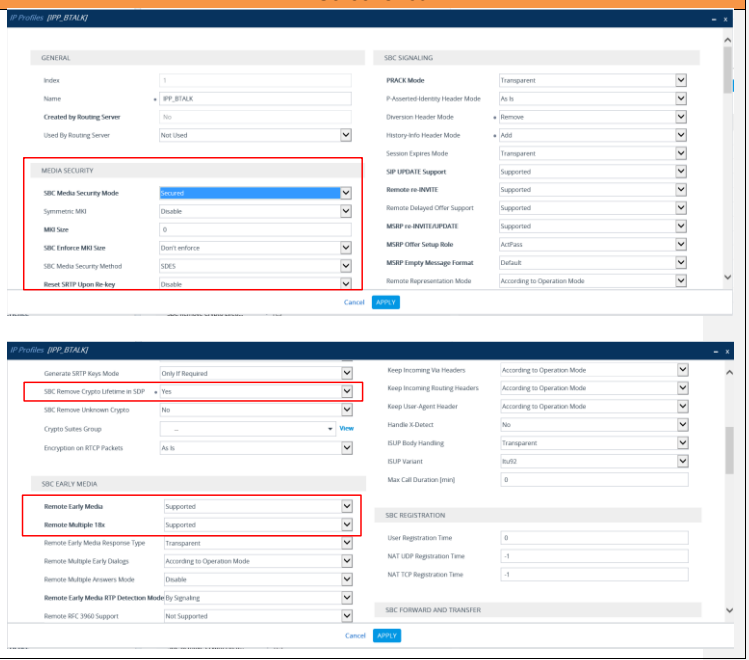
Index	Name	Allowed Audio Coders	Allowed Coders Mode	RFC2833 Mode	RFC2833 DTMF Payload Type	Use Silence Suppression	RTP Redundancy Mode
1	IPP_BTALK	BTALK	Restriction	Extend	101	Remove	Disable

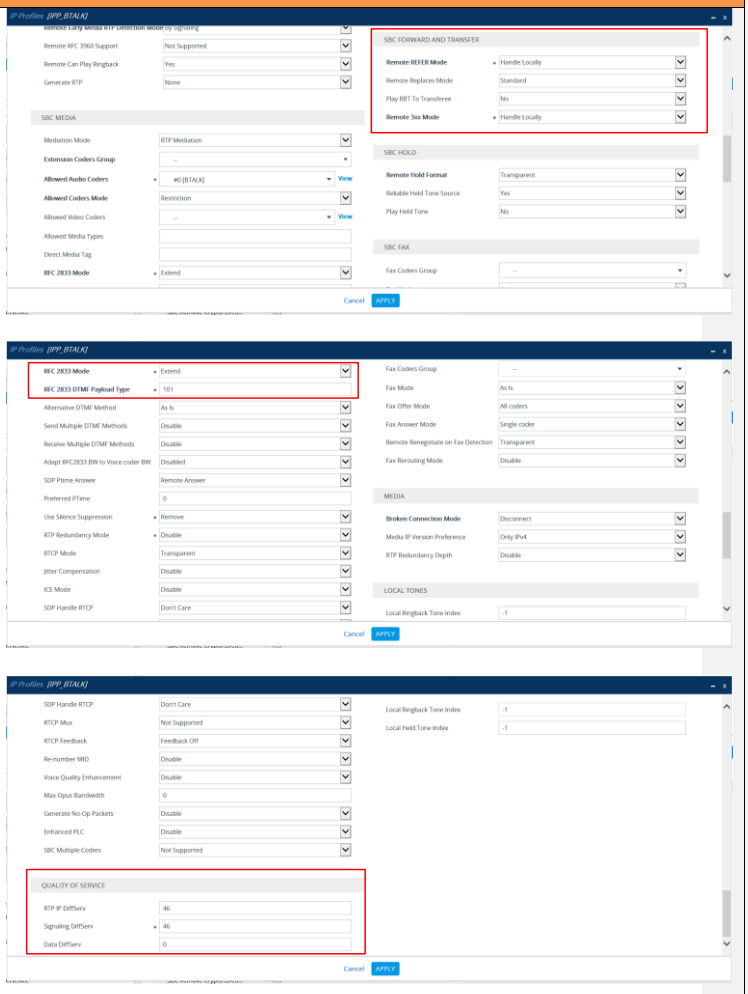
"*Section: **Quality of Service***"

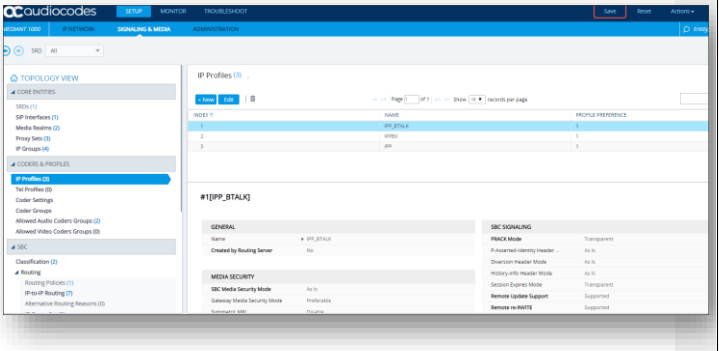
Signaling DiffServ
46

"*Section: **eSBC Forward and Transfer***"

Remote REFER Mode	Remote 3xx Mode
Handle Locally	Handle Locally

Actions	Screenshot
1. Open SETUP > SIGNALING & MEDIA > CODERS & PROFILES > IP Profiles 2. Click on "+ New" Enter a meaningful name ex" IPP_BTALK" 3. Change the parameters indicated above as follow	

Actions	Screenshot
	

Actions	Screenshot
Click on “Apply” The new Objects will appear in the list.	

2.6.6 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.

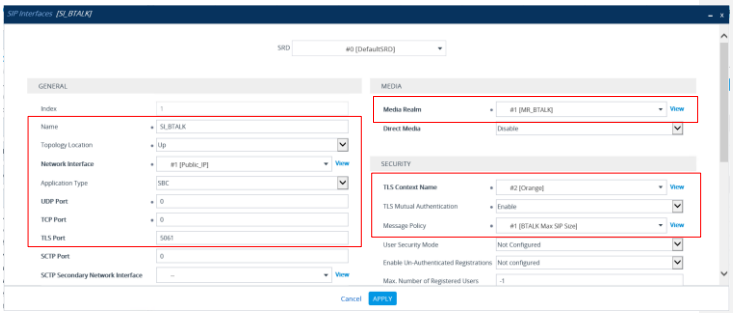
This SIP signaling will be configured to be compliant with Orange BTalk specification:

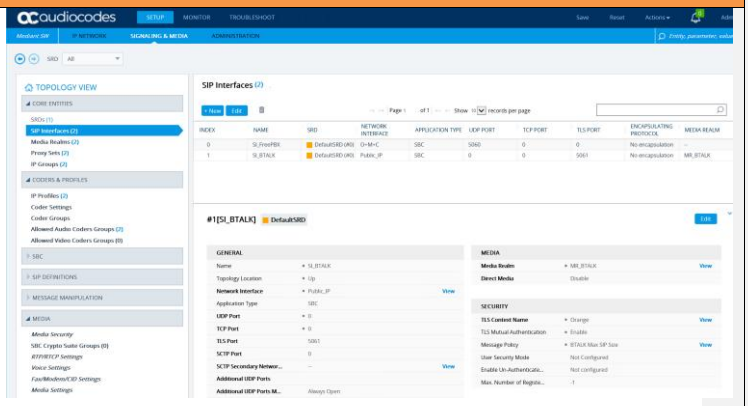
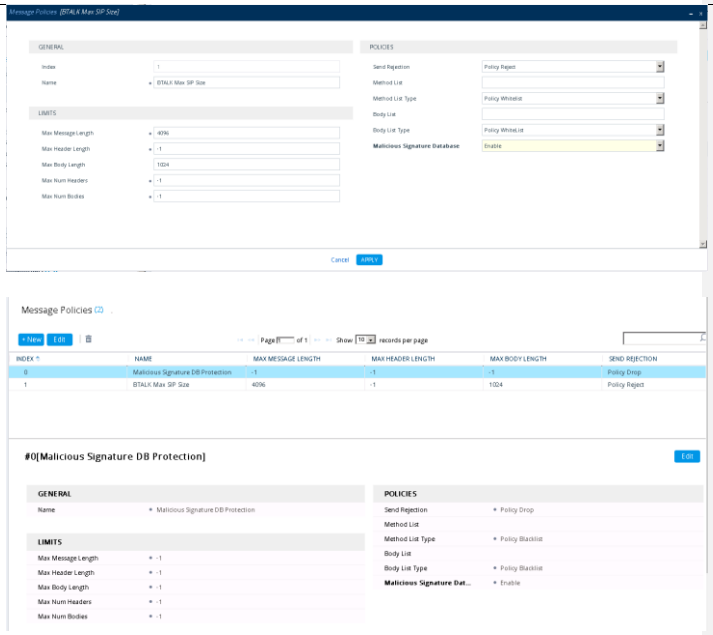
- ✓ For **encrypted BTALK SIP Trunk** architecture we need to configure **TLS port 5061**
- ✓ **TLS Mutual authentication activated.**

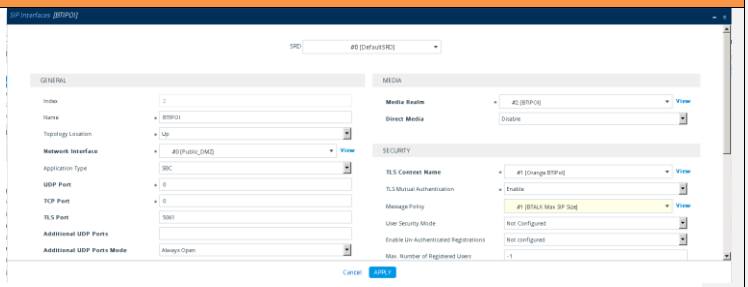
The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

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

Note: "Network Interface" will defined by the Customer itself.

Actions	Screenshot
4. Open SETUP > SIGNALING & MEDIA > CORE ENTITIES > SIP Interfaces **5.** Click on "+ New" Enter a meaningful name ex" **SI_BTALK**" **6.** Change the parameters indicated above as follow	

Actions	Screenshot
7. Click on “Apply” The new Objects will appear in the list.	
8. 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	

Actions	Screenshot
2. Then Message Policies "BTALK Max Sip Size" is called into the Sip Interface Ex: BToI	

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:

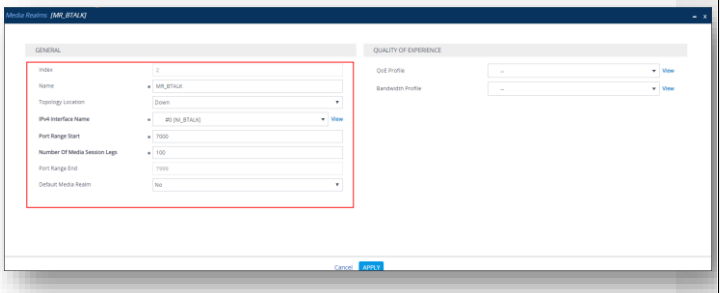
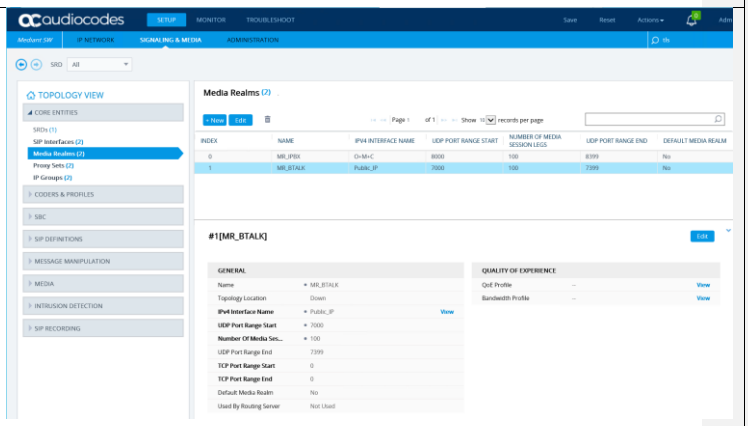
- ✓ For **encrypted BTALK over Internet SIP Trunk** architecture we need to configure **RTP port 6 000 to 20 000**
- ✓ For **encrypted BTIP over Internet SIP Trunk** architecture we need to configure **RTP port 6 000 to 38 000**

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
2	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 defined by the Customer itself.

Actions	Screenshot
1. Open SETUP > SIGNALING & MEDIA > CORE ENTITIES > MEDIA REALMS 2. Click on "+ New" Enter a meaningful name ex" **MR_BTALK**" 3. Change the parameters indicated above as follow	
Click on "Apply" The new Objects will appear in the list.	

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:

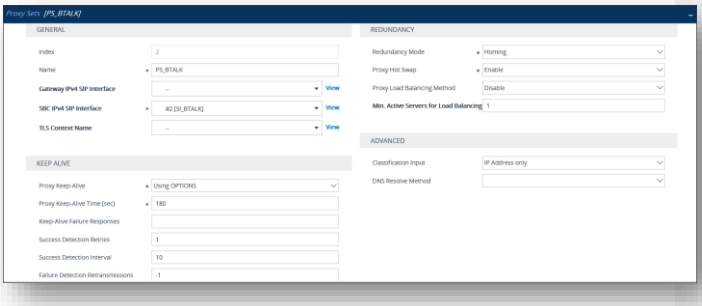
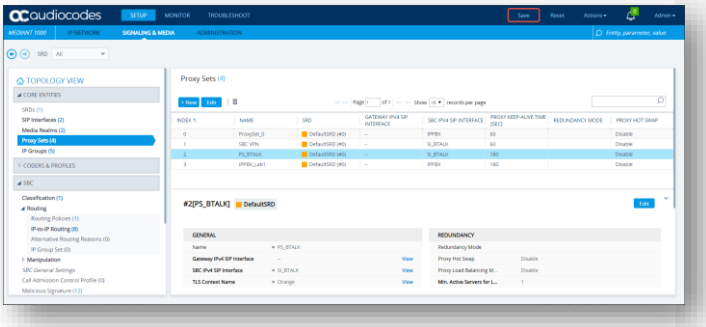
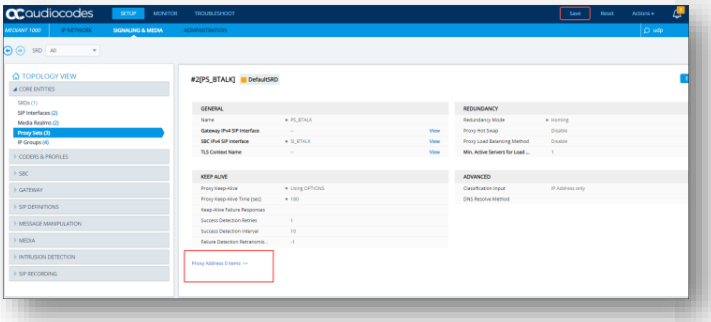
- ✓ For **encrypted BT/BTIP over Internet SIP Trunk** architecture we need to configure **TCP port 5061**
- ✓ For Sip trunk keep alive done with "**Options**" message (every 300 seconds)
- ✓ For Sip trunk redundancy **Homing** (the first Proxy Address is always select if available) and Proxy Hot swap **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.

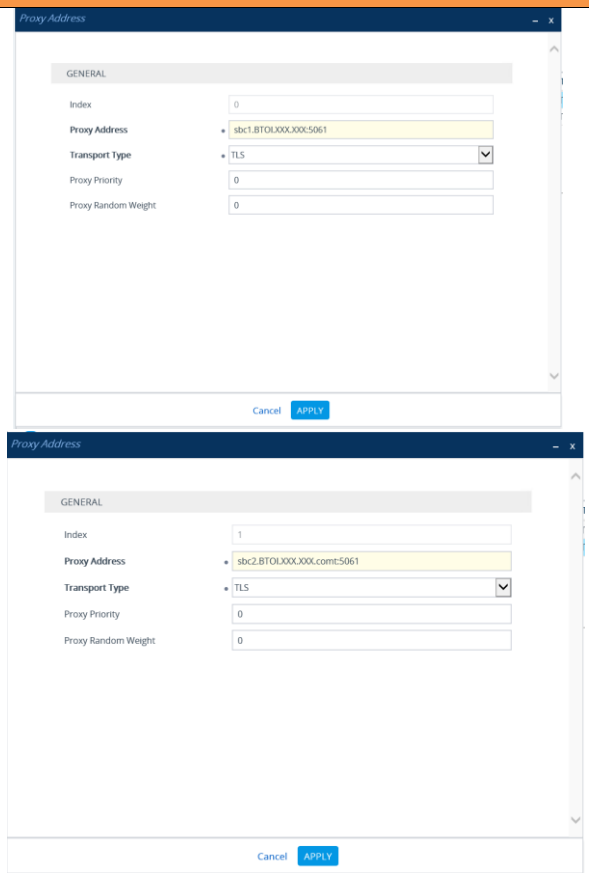
The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

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 1	*<BT_Nominal_Public_IP> or <BTIP_Nominal_Public FQDN >*:5061 *<BT_Backup_Public_IP> or <BTIP_Backup_Public FQDN >*:5061	TLS 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 BTIPol** or "**Public IP**" **for BTol** 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
3. Open SETUP > SIGNALING & MEDIA > CORE ENTITIES > PROXY SETS **4.** Click on "+ New" Enter a meaningful name ex" **PS_BTALK**" **5.** Change the parameters indicated above as follow	
6. Click on "Apply". The new Objects will appear in the list.	
7. To configure "**Proxy Address**" and "**Transport Type**", you have to configure and select the "Proxy Set" just created. **8.** Click on the "Proxy Address 0 items" link at the bottom of the page	

Actions	Screenshot
9. Configure though **index 0 for** <BT_Nominal_Public_IP> or <BTIP_Nominal_Public FQDN > . **10.** You have to configure though **Index 1 for the backup Proxy address** to backup the nominal ones with <BT_Backupl_Public_IP> or <BTIP_Backup_Public FQDN > . **11.** At the End at least 2 Proxy Items should be configured: - Index 0 for Nominal within BT nominal Public IP (first public IP) or BTIP nominal FQDN (First DNS record type) - Index 1 for Backup within BT backup Public IP (second public IP) or BTIP backup FQDN (Second DNS record type) In case of usage of BTIP over Internet SRV Record Index 0 must be configured	

IP Group Table

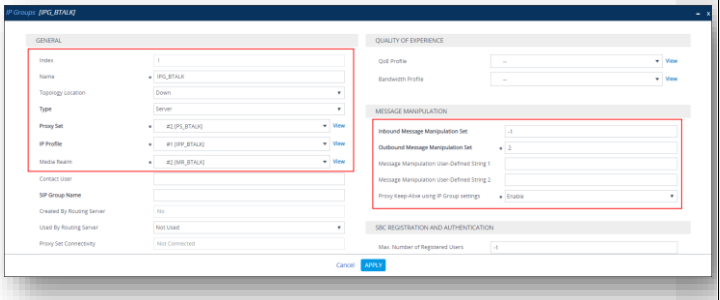
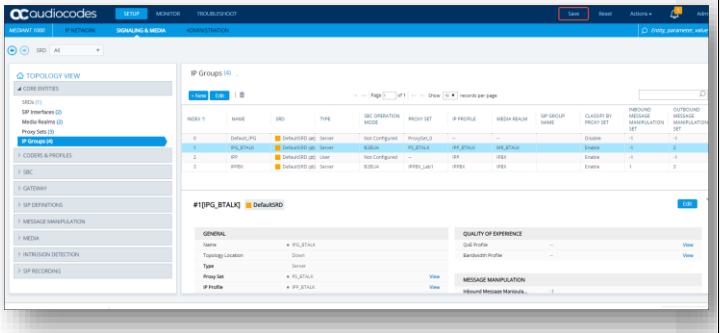
The IP Group table allows logical IP entities creation with a set of parameters such as Proxy set ID, IP profile ID to separate provenance and destination traffic.

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
1. Open SETUP > SIGNALING & MEDIA > CORE ENTITIES >IP_GROUP 2. Click on "+ New" Enter a meaningful name ex" **IPG_BTALK**" 3. Click on "Apply" 4. Click on "Allowed Audio Coders 0 items"	
5. Click on "Apply". The new Objects will appear in the list.	

2.6.7 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

2.7 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.

2.7.1 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*		

2.7.2 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 00xxxxxxxx) 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.

2.7.3 Inbound Manipulations

No inbound manipulation Number is required for default installation.

2.7.4 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, INFO'
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	3	invite.request	body.application/vnd.orange.indata exists	body.application/vnd.orange.indata	Remove	

Commenté [SC3]: Add INFO

	Multipart						

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.

3. Annexes

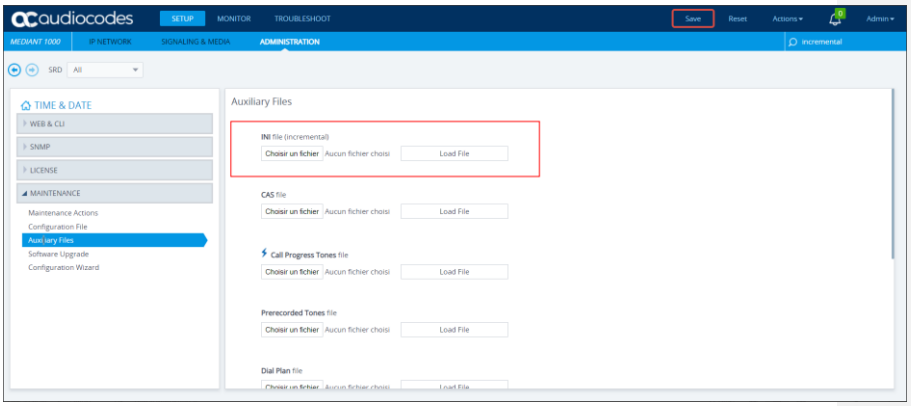
3.1 Import Manipulations Rules via Incrementation INI file

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.ini

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.



3.2 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=lc1454061318
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

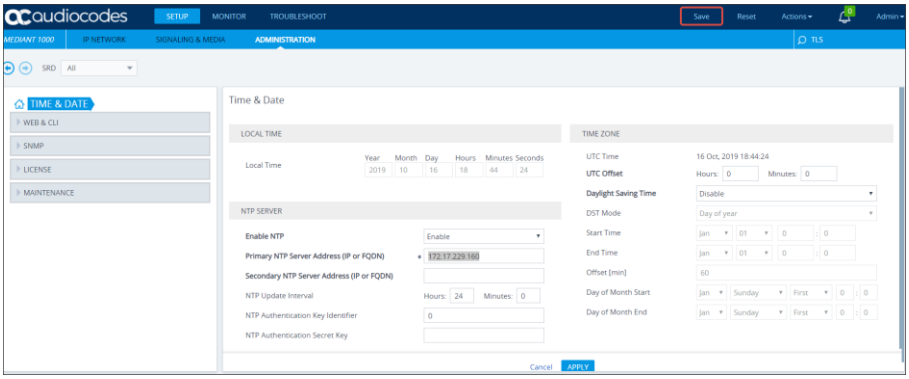
```
INVITE sip:+33299281695@172.17.229.118:5060;user=phone SIP/2.0
Via: SIP/2.0/UDP 172.22.246.33:5060;branch=z9hG4bKq4e6eb109ot6a7e3t140.1
From: "+33786002931" <sip:+33786002931@172.22.246.33;user=phone>;tag=SDkrgc301-S2maIg
To: <sip:+33299281695@172.17.229.118;user=phone>
Call-ID: SDkrgc301-6d41631ae590323a0ca28275a72b7aa4-v300g00060
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
```

3.3 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**.


audiocodes
SETUP
MONITOR
TROUBLESHOOT
Save
Reset
Actions
Admin
MEDIANT 1000
IP NETWORK
SIGNALING & MEDIA
ADMINISTRATION
TLS
SRD
All
TIME & DATE
WEB & CLI
SNMP
LICENSE
MAINTENANCE
Time & Date
LOCAL TIME
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
End Time
Offset [min]
60
Day of Month Start
Day of Month End
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