

Business Talk & BTIP Configuration Guidelines With Audiocodes Customer eSBC Certified Border

versions addressed in this guide: Audiocodes eSBC V.7.2

Latest Edition : 03/03/2021

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

Table of contents

1	General	3
1.1	Goal of the document	3
1.2	References documents.....	3
2	Certified Architecture.....	4
2.1	Introduction to architecture components and features.....	4
2.2	Prerequisites.....	5
2.2.1	Certificates	5
2.2.2	Public DNS configuration:	5
2.2.3	NTP.....	5
2.3	Orange BTalk specifications	6
2.4	Architecture with Audiocodes “customer” SBC with OBS SIP North Carrier configuration	11
2.4.1	Unencrypted SIP Trunk through BVPN.....	11
2.4.2	Encrypted SIP Trunk Over Internet.....	12
2.4.4	Parameters to be provided by customers to access the service	13
2.5	Business Talk IP Audiocodes eSBC certified versions	15
2.6	Audiocodes Global configuration	16
2.6.1	Objects	16
2.6.2	Information and Syntax.....	16
2.7	OBS Business Talk IP Carrier North unencrypted SIP configuration for AudioCodes SBC (IPSEC).....	18
2.7.1	IP Network.....	18
2.7.2	Message Manipulation Policy	18
2.7.3	Coders and Profiles	19
2.7.4	Core Entities	27
2.7.5	SIP Message Manipulation	36
2.7.6	TLS profile	36
2.7.7	Media Security	41
2.7.8	IP Network.....	43
2.7.9	Coders and Profiles	43
2.7.10	Core Entities	52
2.7.11	SIP Message Manipulation	62
2.8	OBS Business Talk & BTIP Carrier North encrypted SIP configuration for AudioCodes SBC (TLS)	63
2.8.1	TLS profile	63
2.8.2	Media Security	69
2.8.3	IP Network.....	71
2.8.4	Coders and Profiles	71
2.8.5	Core Entities	80
2.8.6	SIP Message Manipulation	90
2.9	SIP rules & manipulations (SBC Application).....	91
2.9.1	IP-to-IP Routing Table.....	91
2.9.2	Outbound Manipulations.....	92
2.9.3	Inbound Manipulations.....	92
2.9.4	SIP Messages Manipulations	93
3	Annexes.....	97
3.1	Import Manipulations Rules via Incrementation INI file.....	97
3.2	Example of SIP INVITE message.....	98
3.2.1	NTP server configuration.....	99
4	Glossary	101

1 General

1.1 Goal of the document

The aim of this document is to provide configuration guideline for AudioCodes eSBC North OBS Carrier profile in VISIT Program.

The document presents configuration requirements on the AudioCodes eSBC, in order to ensure the interoperability with Business Talk and Business Talk IP SIP infrastructure (SIP proxy aSBC, Class 5, Appliance Server and Gateways Devil+/Neo).

1.2 References documents

Title	Link
Software Update for AudioCodes eSBCs	https://www.audiocodes.com/library/firmware https://services.audiocodes.com/
Audiocodes eSBC Overview	https://www.audiocodes.com/media/3020/audiocodes-mediant-enterprise-session-border-controllers-sbc-family-brochure.pdf

2 Certified Architecture

2.1 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...)

These configuration guidelines taken into account:

- **Only considering Carrier North side of AudioCodes eSBC facing Business talk 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,...)

These configuration guidelines don't take into account 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, Business talk 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.

* 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.

2.2 Prerequisites

2.2.1 Certificates

In case of encrypted SIP trunk architecture, TLS configuration is mandatory in order to exchange a certificate with Orange BTalk A-SBC. The certificate is used by the E-SBC to authenticate the connection with the management station (i.e., the computer used to manage the E-SBC through its embedded Web server).

The customer must generate on the Audiocodes SBC a Certificate Signing Request (CSR) and request to a public Certificate Authority (CA) a public certificate. After that the Root and intermediate Certificate (PEM format) must be transmitted to Orange BTalk team.

Accordingly Orange team will transmit ours public Root and intermediate Certificate Authority (CA) which signed Orange BTalk A-SBC's and should import on your Audiocodes eSBC.

2.2.2 Public DNS configuration:

Following requirements regarding Public DNS configuration:

- In the SBC configuration, public DNS is used for outgoing calls (e.g. From PBX to BTol/BTIPol)
- Internet-Facing LAN: either enter the IP addresses of 2 private DNSs, 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)

2.2.3 NTP

The configuration of the NTP on the SBC is not fully detailed in this document but it is recommended to implement an NTP server (Microsoft NTP server or another global server) on Audiocodes SBC to ensure that the SBC receives the current date and time. This is necessary for validating Certificates of remote parties.

2.3 Orange BTalk specifications

The information in this chapter are the SIP trunk specifications required in order to interconnect Orange BTalk 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 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 configuration **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> \ Audiocodes eSBC<SBC model> <Version>.<build>**”
 - Same requirement apply 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) :**
 - G.711 A-law 20 ms (or on demand specific G.711 μ -law 20 ms)
 - G.729 20 ms (annexb = no)
 - G722 20 ms.

- ✓ **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

Note: For T.38 the Audiocodes eSBC will be transparent. No adaptation will be done at SBC level and needs DSP resources .

- ✓ **DTMF transport specifications are:**
 - RFC 2833/4733
- ✓ **Signalisation/ Media 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/emission 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, recv only, inactive, send recv.
 - 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 Business Talk request anonymous calls.
- ✓ **Number format specifications are:**
 - Called Number send to Orange network must be at E164 format
 - Calling Number send to Orange network must be in National format (0ZABPQMCDU or 00xxxxxxx) or E164 format.

✓ **Rerouting scenario :**

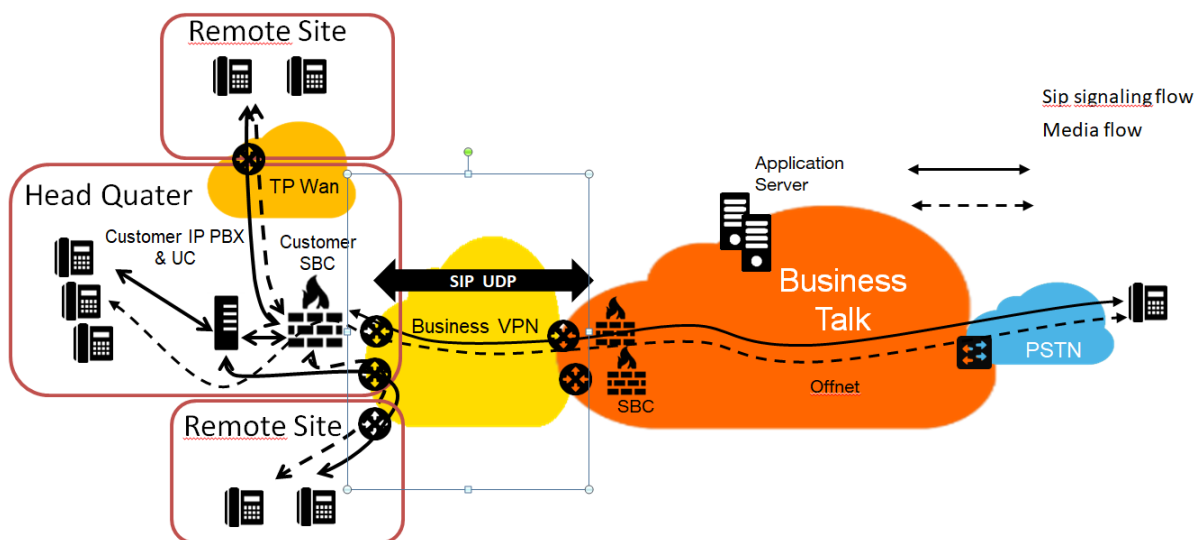
- On reception of a Sip Error message, UE must reroute in case of 408 et 50x (500/501/502/503/504/505/513)
- Emission of a Sip error message to Btalk/BTIP, UE must send 5xx if a rerouting is expected from Btalk/BTIP service.
- It's recommend to do not send 408 to Btalk/BTIP. If it's the case, UE will be considered out of service until next Sip probing

✓ **Call defection :**

- 3xx Sip message are not supported by Btalk/BTIP services. Those message will be convert into Sip error messages.

2.4 Architecture with Audiocodes “customer” SBC with OBS SIP North Carrier configuration

2.4.1 Unencrypted SIP Trunk through BVPN



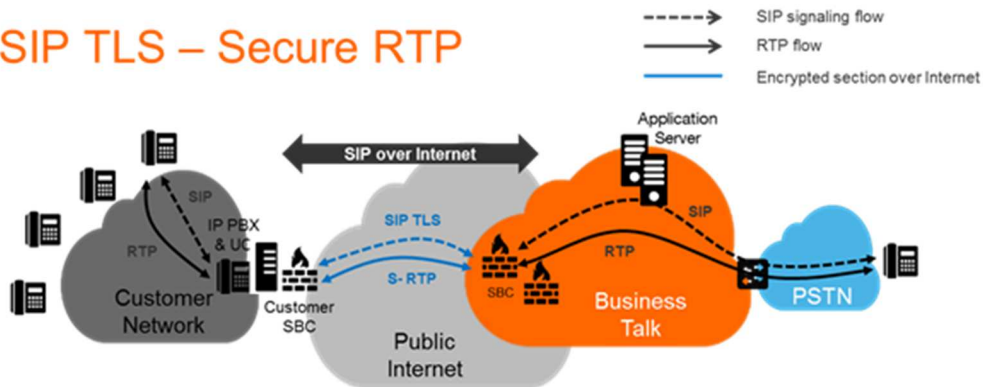
In this architecture:

- both ‘SIP trunking’ and RTP media flows between endpoints and the Business Talk IP are anchored by the “customer SBC”:
- for Head Quarter, SIG flows are routed through the Customer SBC and media flows are direct to private “South” interface of the eSBC through the main BVPN connection.
- for remote sites interconnected through BVPN SIG flows are routed through the Customer SBC and media flows are direct to private “South” interface of the eSBC and the main BVPN connection.
- for remote sites interconnected through 3rd Party Wan, both SIG & Media flows are routed through the Customer SBC direct to private “South” interface of the eSBC through the main BVPN connection.

2.4.2 Encrypted SIP Trunk Over Internet

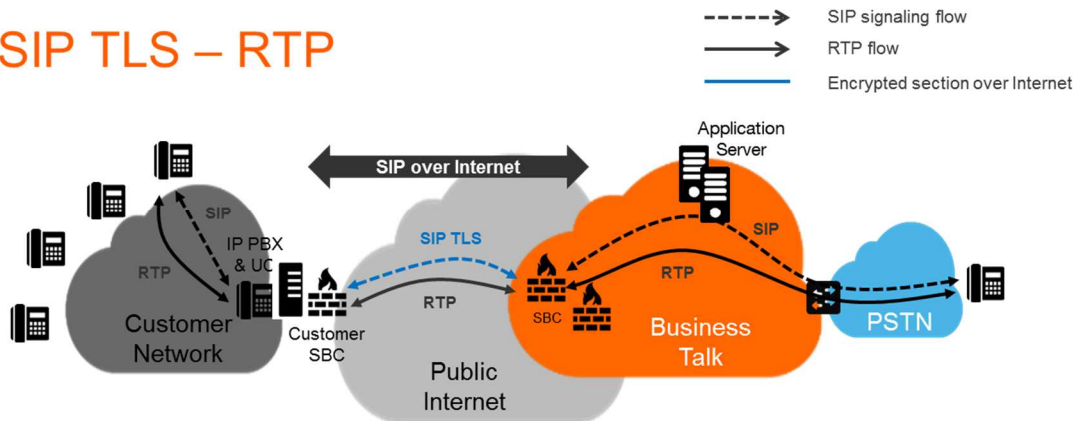
- SIP TLS + Secured RTP: all SIP messages and media packets are encrypted on the public internet between Orange and the customer Internet SIP & Media endpoints. This is the level of encryption recommended by default by Orange to ensure security & privacy

SIP TLS – Secure RTP



- 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

SIP TLS – RTP



2.4.4 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 the scenario .

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

Customer SBC – architecture with eSBC	Level of Service	@IP used by service	
1 Single Customer SBC	No redundancy	eSBC @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	eSBC1 @IP	eSBC2 @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	eSBC1 @IP eSBC2 @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	eSBC VIP @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 SBC	No redundancy	eSBC1 @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	eSBC1 @IP or Public FQDN	eSBC2 @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	eSBC1 @IP or Public FQDN eSBC2 @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	eSBC VIP @IP v	

	warning: Link level 2 between SBC with max delay 50ms required for geo-redundancy	
--	--	--

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 SBC	No redundancy	eSBC1 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	eSBC 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	eSBC1 FQDN Type A *	eSBC2 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	eSBC1 FQDN Type A* eSBC2 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	eSBC VIP FQDN type A*	

Note: BTalk IP over Internet (BTIP over Internet) service is not yet open at the time this document is produced. Please check with your sales contact.

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

2.5 Business Talk IP Audiocodes eSBC certified versions

Audiocodes eSBC – software versions				
Reference product	Hardware or Virtual Model	Software version	Certified "Loads"	Certification
Hybrid enterprise SBC	Mediant 500	V.7.2	<u>Load(s) 7.2.254 *</u>	✓
	Mediant 800			
	Mediant 1000			
Pure enterprise SBC	Mediant 2600			
	Mediant 4000			
	Mediant 9000			
	Mediant Server Edition			
	Mediant Virtual Edition			
	Mediant Cloud Edition (MS Azure, AWS)			

* Minimum Load for implementation, last most up-to-date Load is recommend per Audiocodes

2.6 Audiocodes Global configuration

2.6.1 Objects

This chapter describes the AudioCodes SBC necessary configuration steps for a correct interoperability with the Orange Business Trunking Business Talk.

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 SBC 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 SBC configuration (save the INI file on your laptop). When you have finished the configuration do a “Save” of your SBC configuration and do again of Backup of your new configuration.

2.6.2 Information and Syntax

Inside the configuration pages described in the following Chapters, the tables include an “**Index**” column. Those “Index” are given as example. The real indexation will depend on the current Configuration present on the SBC . This is have “no impact” on the configuration except in the “Message Manipulation” step were **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 in your context.

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 SBC. If the SBC used is a new one without existing configuration, you must replace those "Grey" lines according the specifications of your IPPbx/UC Device you want to interconnect to BTalk/BTIP network.

Index	Name	SIP Interface	TLS Context Name	Proxy Keep-Alive	Proxy Address	Transport Type
1	PS_BTALK	SI_BTALK	--	Using OPTIONS	** @IP_SBC_BTALK:5060 **	UDP
2	<i>PS_IPBX</i>	<i>SI_IPBX</i>	--	<i>Using OPTIONS</i>	<i>** @IP_IPBX:5060 **</i>	<i>UDP</i>

Example

2.7 OBS Business Talk IP Carrier North **unencrypted** SIP configuration for AudioCodes SBC (IPSEC)

2.7.1 IP Network

No configuration is required in this section. Existing IP Interface, Ethernet Device and Device Group could be used. It is anyway 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.

2.7.2 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 Max SIP Size	4096	1024	Policy Reject

Actions	Screenshot
<ol style="list-style-type: none"> 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" 	
<p>The number Policy will appear in the list</p>	

2.7.3 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:
G.722 20 ms, G.711 A-law 20 ms and G.729 20 ms (annexb = no).
Note: G.722 isn't supported in Business Talk over Internet context

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

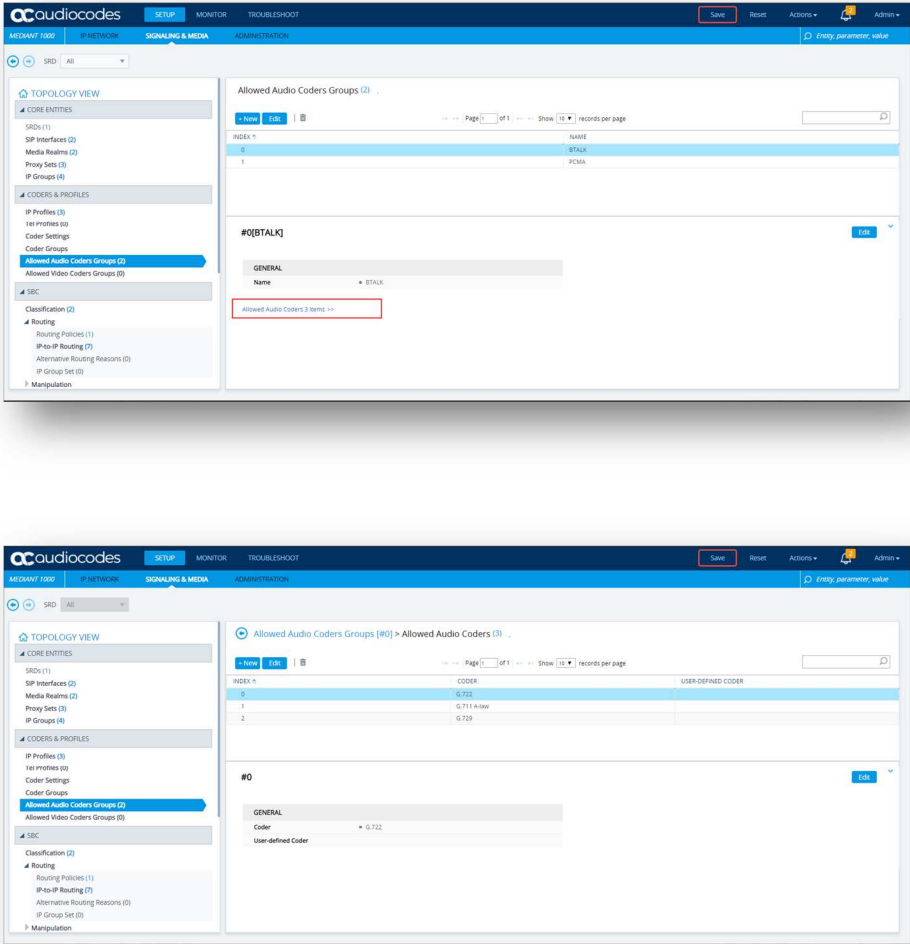
Index	Name
0	BTALK

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

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

* If specific Customer request it

Actions	Screenshot
<ol style="list-style-type: none"> 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
<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>Please note: 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 BTalk network. As solution on the Audiocodes SBC, it is required to implemented 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” 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 BTalk.

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

Actions	Screenshot
<ol style="list-style-type: none"> 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" 	

Actions	Screenshot
<p>6. Click on “+ New” 7. Select the coders as mention in the table of parameters above, in the same order</p> <p>Please note: 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 columns 'INDEX' and 'NAME'. Row 1 is selected, showing 'PCMA'. Below the table, the 'GENERAL' section shows 'Name' set to 'PCMA'. A yellow banner at the bottom indicates 'Allowed Audio Coders 1 items >>'. The bottom screenshot shows the 'Allowed Audio Coders Groups [#0] > Allowed Audio Coders (1)' configuration page. The left sidebar has 'Allowed Audio Coders Groups (1)' highlighted. The main content area shows a table with columns 'INDEX', 'CODER', and 'USER-D'. Row 0 is selected, showing 'G.711 A-law'. Below the table, the 'GENERAL' section shows 'Coder' set to 'G.711 A-law'.</p>

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

Note:

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

For **Transfer**, the Audiocodes SBC 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, **SBC 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: **SBC Media**”

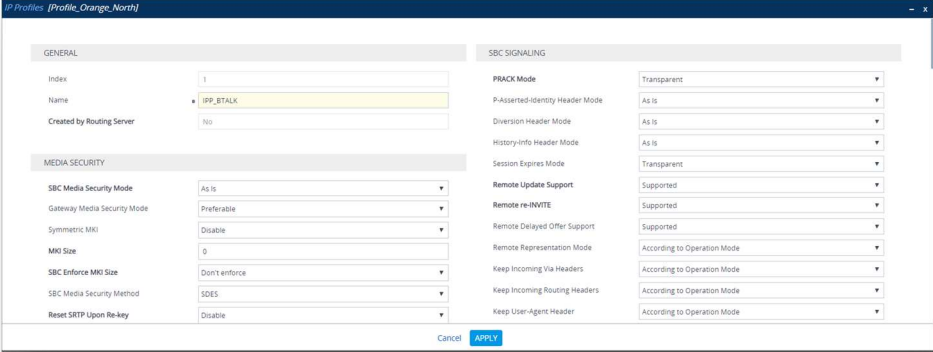
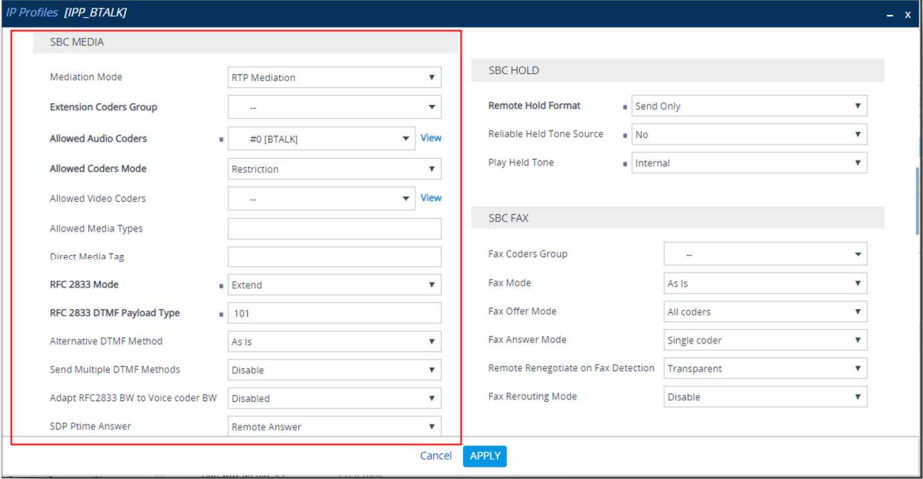
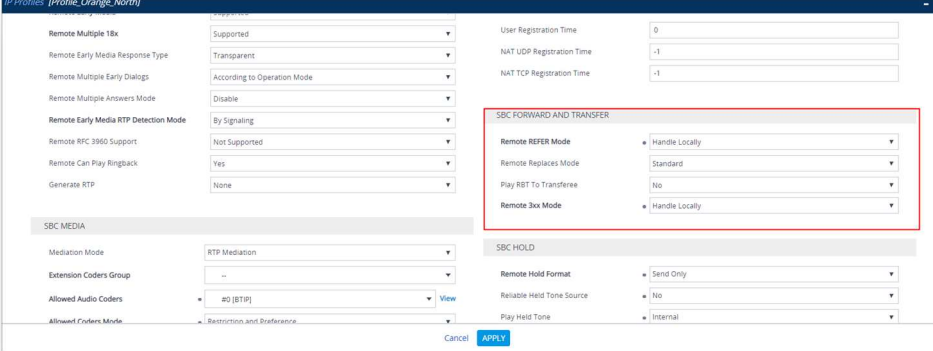
Index	Name	Allowed Audio Coders	Allowed Coders Mode	RFC2833 Mode	RFC2833 DTMF Payload Type	Use Silence Suppression	RTP Redundancy Mode
1	IPP_BTALK	BTALK	Restriction	Extend	101	Remove	Disable

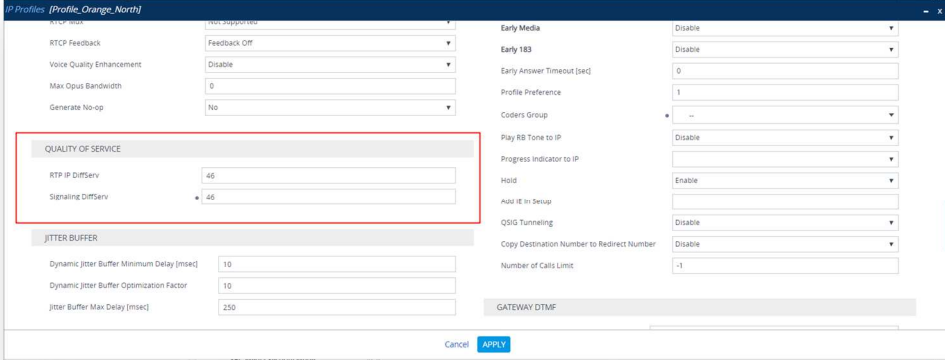
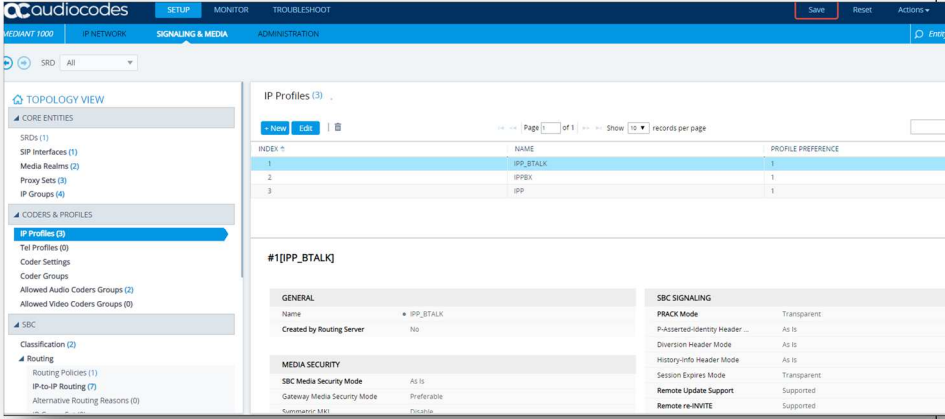
“Section: **Quality of Service**”

Signaling DiffServ
46

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

Remote REFER Mode	Remote 3xx Mode
Handle Locally	Handle Locally

Actions	Screenshot
<ol style="list-style-type: none"> 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
	
<p>Click on “Apply” The new Objects will appear in the list.</p>	

2.7.4 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:

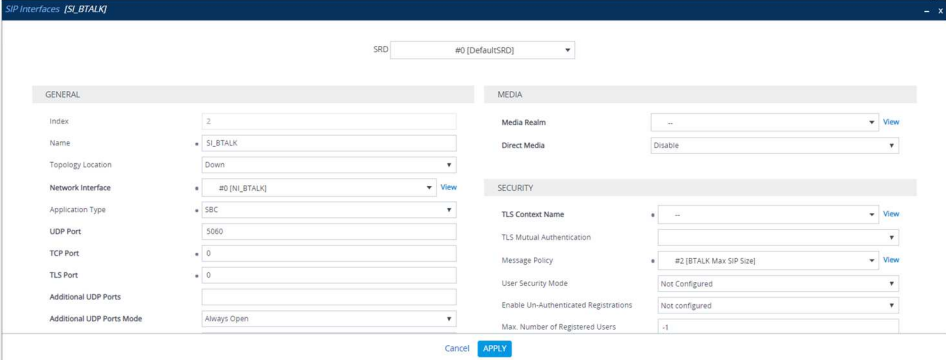
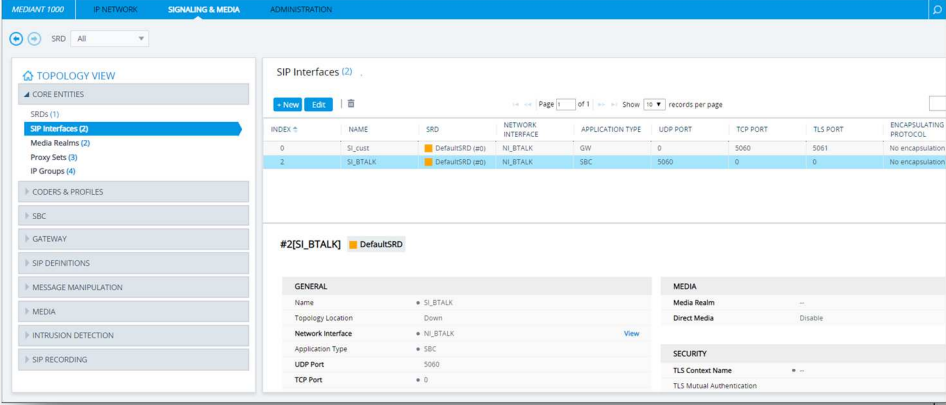
- ✓ For **unencrypted BT SIP Trunk** architecture, we need to configure **UDP port 5060**

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	NI_Existing	5060	0	0	-	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
<ol style="list-style-type: none"> 1. Open SETUP > SIGNALING & MEDIA > CORE ENTITIES > SIP Interfaces 2. Click on “+ New” Enter a meaningful name ex” SI_BTALK” 3. Change the parameters indicated above as follow 	

Actions	Screenshot
	
<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:

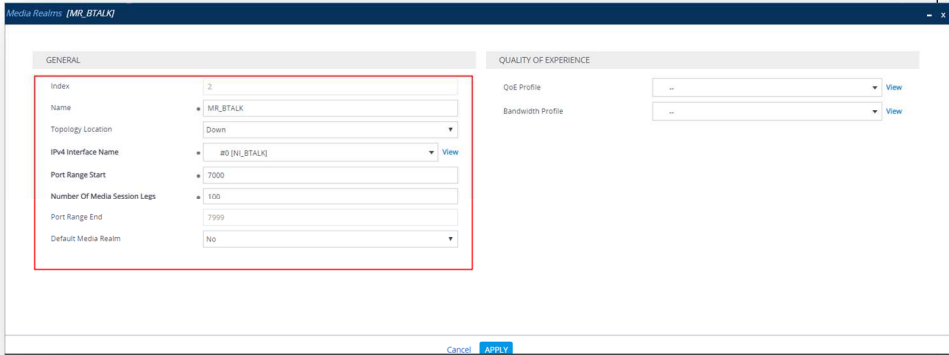
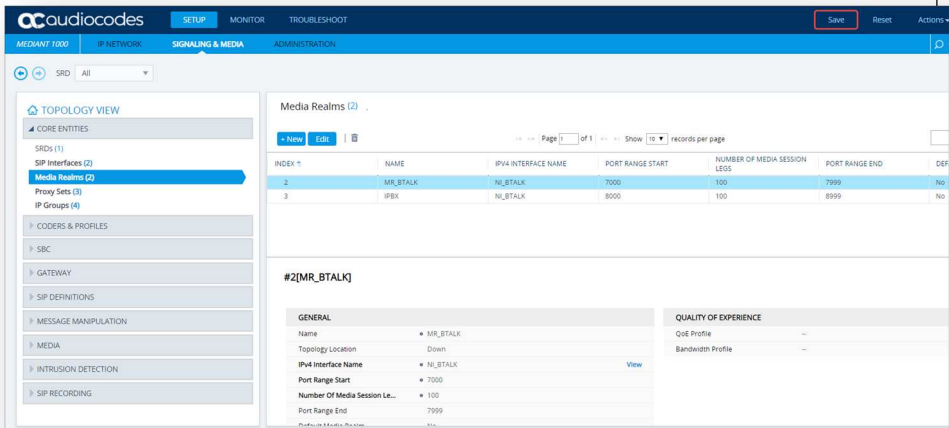
- ✓ For **unencrypted BT SIP Trunk** architecture, we need to configure **RTP port 6 000 to 20 000**

Note: On Audiocodes SBC, for RTP port range keep in mind that the RTP UDP port spacing must be "10". This mean that for example 5 sessions SIP, 5*10 ports RTP from 6000 to 6050 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 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 be defined by the Customer itself.

Actions	Screenshot
<ol style="list-style-type: none"> 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 	
<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 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

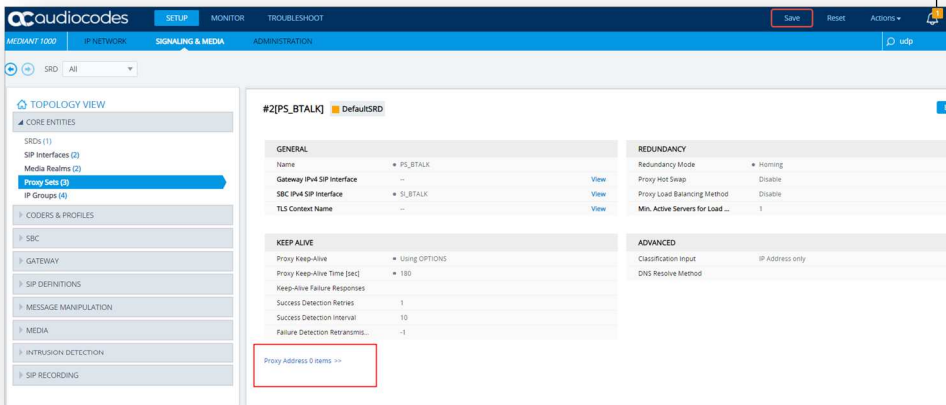
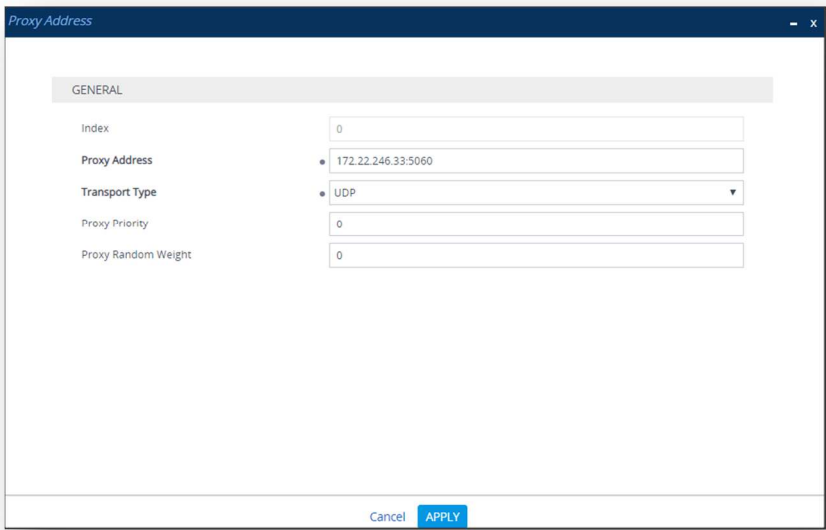
Index	Name	SIP Interface	TLS Context Name	Proxy Keep-Alive	Redundancy Mode	Proxy Hot Swap	Index Proxy Address	Proxy Address	Transport Type
1	PS_BTALK	SI_BTALK	--	Using OPTIONS	Homing	Enable	0	<BT_Nominal IP>:5060	UDP UDP
							1	<BT_Backup IP>:5061 0	
2	PS_IPBX	SI_IPBX	--	Using OPTIONS				** @IP_IPBX:5060 **	UDP

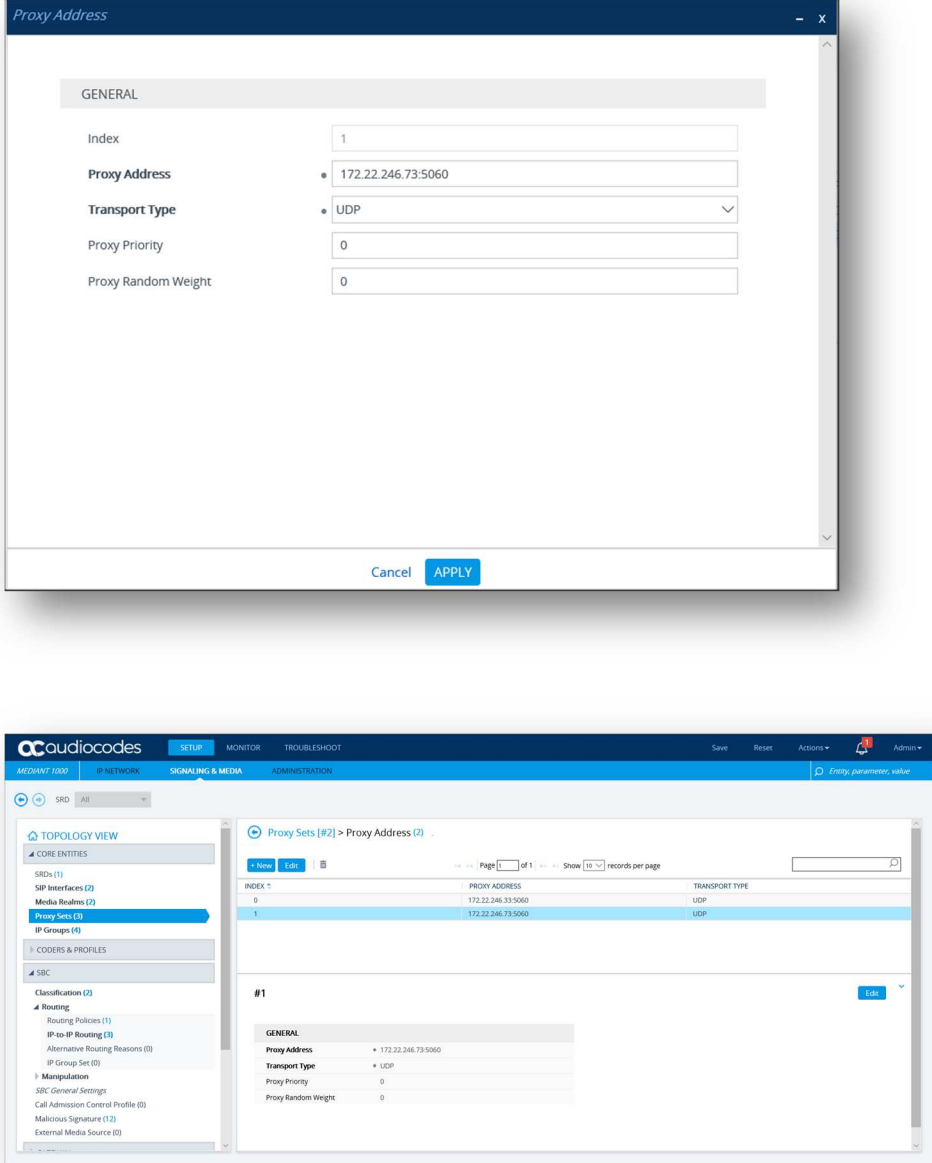
The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

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 BTALK. “Options” message will be sent by the Audiocodes SBC to verify if the Orange BTalk 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"> 1. Open SETUP > SIGNALING & MEDIA > CORE ENTITIES > PROXY SETS 2. Click on "+ New" Enter a meaningful name ex" PS_BTALK" 3. Change the parameters indicated above as follow 	
<ol style="list-style-type: none"> 4. Click on "Apply". The new Objects will appear in the list. 	

Actions	Screenshot
<p>5. To configure “Proxy Address” and “Transport Type”, you have to configure to select the “Proxy Set” just created.</p> <p>6. Click on the “Proxy Address 0 items” link at the bottom of the page.</p>	
<p>7. If you want to backup the nominal BT Proxy address index 0, you can add a second “Proxy Address” as backup with the Index 1</p> <p>8. At the End at least 1 Proxy Items should create (2 items in case of Backup)</p>	

Actions	Screenshot									
	 <p>The screenshot shows two parts of the software interface. The top part is a 'Proxy Address' configuration dialog box with the following fields:</p> <ul style="list-style-type: none"> Index: 1 Proxy Address: 172.22.246.73:5060 Transport Type: UDP Proxy Priority: 0 Proxy Random Weight: 0 <p>Buttons for 'Cancel' and 'APPLY' are at the bottom. The bottom part of the screenshot shows the main application interface with a sidebar menu and a central table of Proxy Sets.</p> <table border="1" data-bbox="783 1182 1465 1256"> <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 the selected item (Index 1) is shown in a 'GENERAL' section:</p> <ul style="list-style-type: none"> Proxy Address: 172.22.246.73:5060 Transport Type: UDP Proxy Priority: 0 Proxy Random Weight: 0 	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 BTALK 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	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"> 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" 	
<ol style="list-style-type: none"> 5. Click on "Apply". The new Objects will appear in the list. 	

2.7.5 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 in chapter “[SIP rules manipulations \(SBC Application\)](#)”.

Please jump to this Chapter directly

2.7.6 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 is supported as Cipher Client/Server:**
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 - 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 (Recommended)
 - 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 activate**

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	Orange	DHE-RSA-AES256-GCM-SHA384	DHE-RSA-AES256-GCM-SHA384	2048

Actions	Screenshot
<ol style="list-style-type: none"> 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 	

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

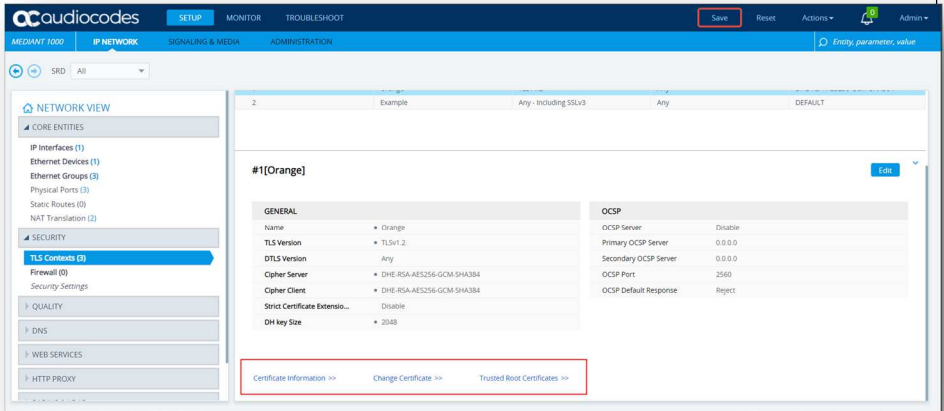
Certificate Signing Request (CSR)

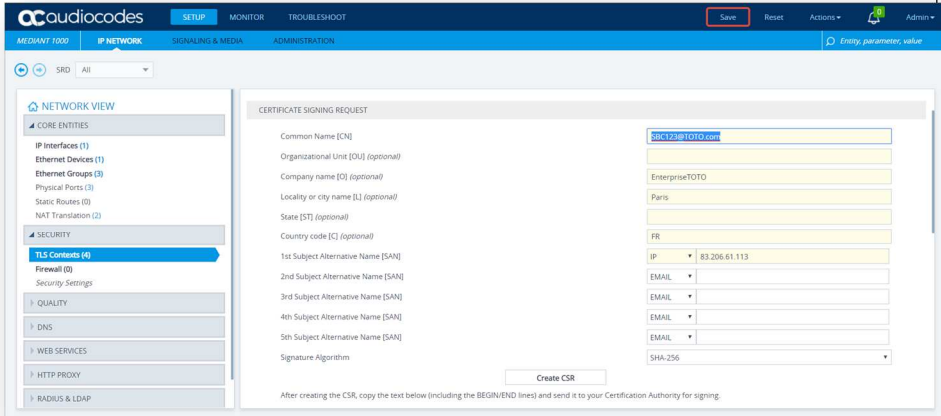
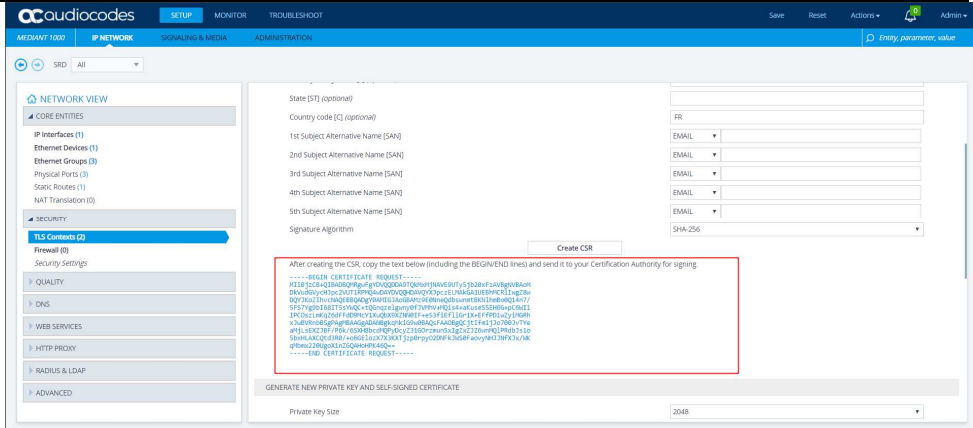
The TLS Context need a Certificate signed. To obtain this Certificate Authority (CA) you must generate your CSR base on the information of the SBC and Company with SHA-256 encryption. As soon you received the CA, you will load it on the Audiocodes SBC on the TLS Context create for this interconnexion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

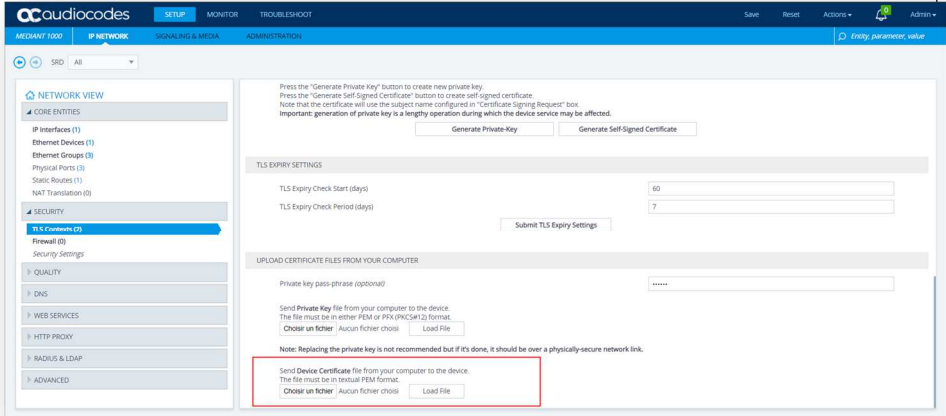
The mentioned parameters in the table below are the one specific to Customer. It is just an example of CSR for a Company "EnterpriseTOTO" located in Paris France with an SBC with FQDN name "SBC123@TOTO.com" resolving Public IP 83.206.61.113

Common Name	Organizational Unit	Company name	Locality or city name	Country code
SBC123@TOTO.com	-	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	
<ol style="list-style-type: none"> On the TLS context you just create go on the Bottom page and click on "Change Certificate" Change the parameters indicated above Click "Create CSR" 	

Actions	
	
<p>On the page should appear a text in blue which represent your CSR.</p>	

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

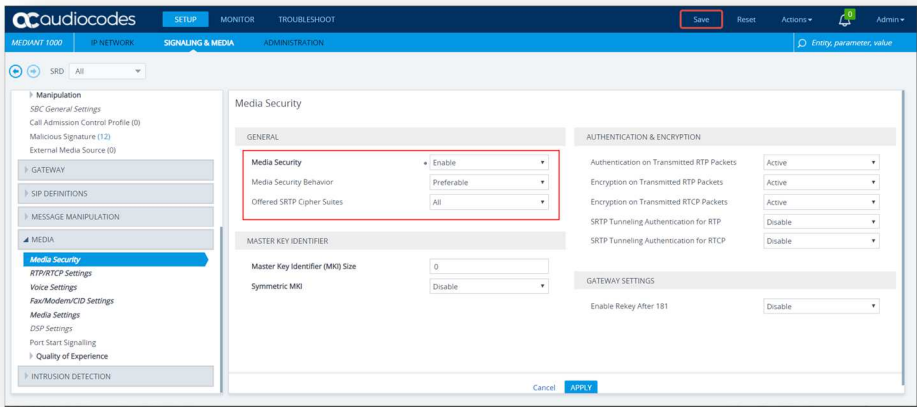
After that the Root and intermediate Certificate (PEM format) must be transmitted to Orange BTALK.

2.7.7 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
Enable	Preferable	all

Actions	Screenshot
<ol style="list-style-type: none"> 1. Open SETUP > SIGNALING & MEDIA > MEDIA > MEDIA SECURITY 2. Change the parameters indicated above as follow 3. Click on “Apply 	 <p>The screenshot shows the 'Media Security' configuration page in the AudioCodes eSBC interface. The 'GENERAL' section is highlighted with a red box, containing the following settings:</p> <ul style="list-style-type: none"> Media Security: Enable (dropdown menu) Media Security Behavior: Preferable (dropdown menu) Offered SRTP Cipher Suites: All (dropdown menu) <p>Other sections visible include:</p> <ul style="list-style-type: none"> Authentication & Encryption: Authentication on Transmitted RTP Packets (Active), Encryption on Transmitted RTP Packets (Active), SRTP Tunneling Authentication for RTP (Disable), SRTP Tunneling Authentication for RTCP (Disable). MASTER KEY IDENTIFIER: Master Key Identifier (MKI) Size (0), Symmetric MKI (Disable). GATEWAY SETTINGS: Enable Rekey After 181 (Disable).

2.7.8 IP Network

No configuration is required in this section. Existing IP Interface, Ethernet Device and Device Group could be used. It is anyway 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.

2.7.9 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 accept the following codecs in this order or preference:

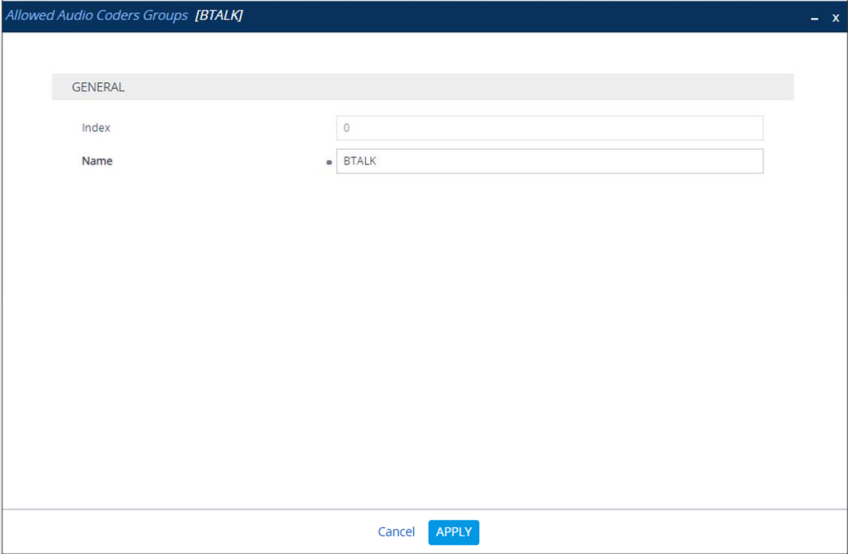
G.722 20 ms, G.711 A-law 20 ms for French BTIP Offer (or G.711 μ -law 20 ms for International BT Offer) and G.729 20 ms (annexb = no).

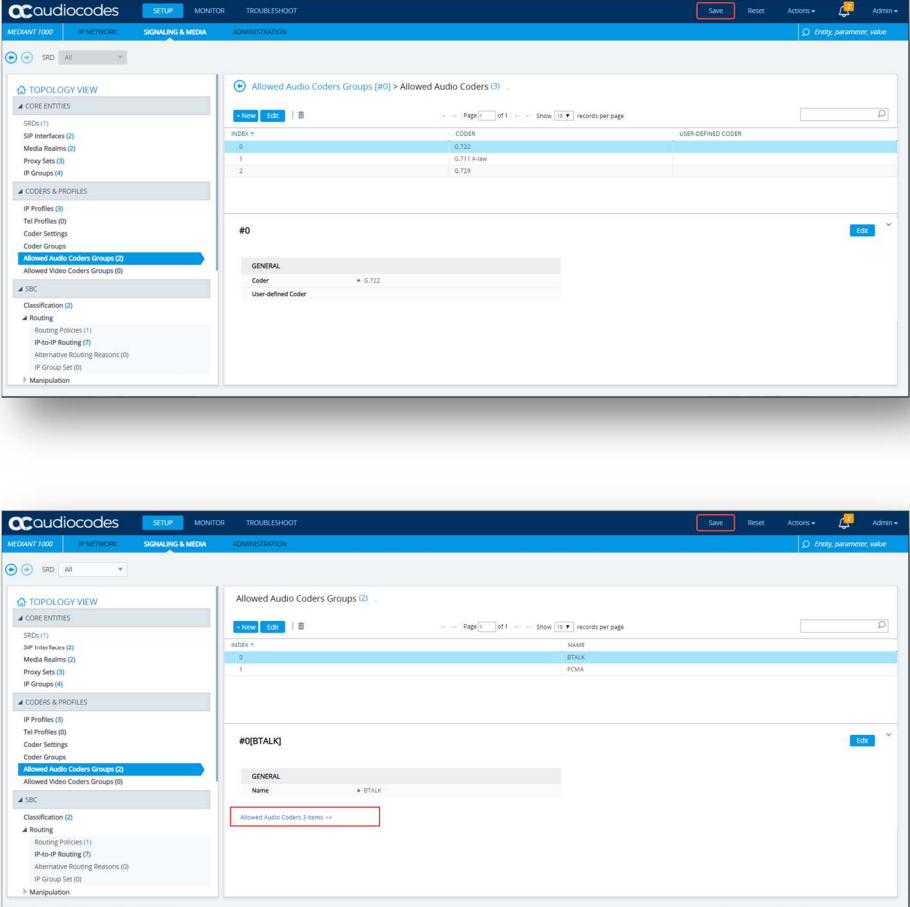
We are going to create a new “Coders Groups” specific to Orange BTalk.

Index	Name
0	BTALK
1	PS_IPBX

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

Index	Coder	User-defined Coder
0	G.722 (If used)	(Empty)
1	G.711 A-Law (or G.711 μ -law)	(Empty)
2	G.729 (If used)	(Empty)

Actions	Screenshot
<ol style="list-style-type: none">1. Open SETUP > SIGNALING & MEDIA > CODERS & PROFILES > Allowed Audio Coders Groups2. Click on "+ New"3. Enter a meaningful name ex" BTALK"4. Click on "Apply"5. Click on "Allowed Audio Coders 0 items"	

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>Please note: 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 configuration page for 'Allowed Audio Coders Groups [#0]'. It features a table with the following data:</p> <table border="1"> <thead> <tr> <th>INDEX</th> <th>CODER</th> <th>USER-DEFINED CODER</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>G722</td> <td></td> </tr> <tr> <td>1</td> <td>G711 A-law</td> <td></td> </tr> <tr> <td>2</td> <td>G729</td> <td></td> </tr> </tbody> </table> <p>The bottom screenshot shows the configuration page for 'Allowed Audio Coders Groups [2]'. It features a table with the following data:</p> <table border="1"> <thead> <tr> <th>INDEX</th> <th>NAME</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>BTALK</td> </tr> <tr> <td>1</td> <td>PCMA</td> </tr> </tbody> </table>	INDEX	CODER	USER-DEFINED CODER	0	G722		1	G711 A-law		2	G729		INDEX	NAME	0	BTALK	1	PCMA
INDEX	CODER	USER-DEFINED CODER																	
0	G722																		
1	G711 A-law																		
2	G729																		
INDEX	NAME																		
0	BTALK																		
1	PCMA																		

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 SBC, 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.

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

Actions	Screenshot
<p>8. Open SETUP > SIGNALING & MEDIA > CODERS & PROFILES > 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>Please note: 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 configuration for 'Allowed Audio Coders Groups (2)'. The left sidebar lists navigation options like 'CORE ENTITIES', 'CODERS & PROFILES', and 'SBC'. The main area shows a table with columns 'INDEX' and 'NAME'. The table contains two rows: index 0 with name BTIP, and index 1 with name PCMA. Below the table, there is a section for '#1[PCMA]' with a 'GENERAL' tab and a 'Name' field set to 'PCMA'. A yellow highlight indicates 'Allowed Audio Coders 1 items >>'. The bottom screenshot shows the configuration for 'Allowed Audio Coders Groups [#0] > Allowed Audio Coders (1)'. The table has columns 'INDEX', 'CODER', and 'USER-D'. It contains one row: index 0 with coders G.711 A-law. Below the table, there is a section for '#0' with a 'GENERAL' tab and a 'Coder' field set to 'G.711 A-law'.</p>

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

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

For encryption, the Audiocodes SBC will encrypt the RTP tower Orange BTALK 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. 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, **SBC 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**”

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

“Section: **SBC 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**”

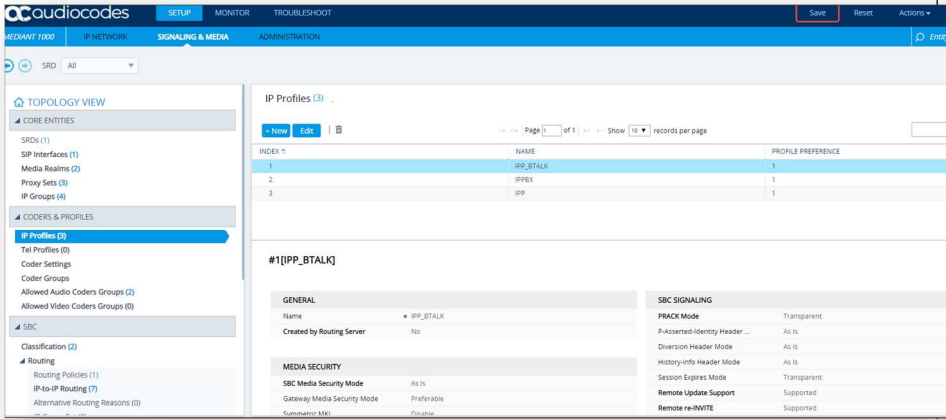
Signaling DiffServ
46

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

Remote REFER Mode	Remote 3xx Mode
Handle Locally	Handle Locally

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

Actions	Screenshot
	<p>IP Profiles [IPP_BTALK]</p> <p>SBC MEDIA</p> <ul style="list-style-type: none"> Mediation Mode: RTP Mediation Extension Coders Group: -- Allowed Audio Coders: #0 [BTALK] View Allowed Coders Mode: Restriction Allowed Video Coders: -- View Allowed Media Types: Direct Media Tag: RFC 2833 Mode: Extend RFC 2833 DTMF Payload Type: 101 Alternative DTMF Method: As Is Send Multiple DTMF Methods: Disable Adapt RFC2833 BW to Voice coder BW: Disabled SDP Ptime Answer: Remote Answer <p>SBC HOLD</p> <ul style="list-style-type: none"> Remote Hold Format: Send Only Reliable Held Tone Source: No Play Held Tone: Internal <p>SBC FAX</p> <ul style="list-style-type: none"> Fax Coders Group: -- Fax Mode: As Is Fax Offer Mode: All coders Fax Answer Mode: Single coder Remote Renegotiate on Fax Detection: Transparent Fax Rerouting Mode: Disable <p>Cancel APPLY</p>
	<p>IP Profiles [Profile_Orange_North]</p> <p>SBC FORWARD AND TRANSFER</p> <ul style="list-style-type: none"> Remote REFER Mode: Handle Locally Remote Replaces Mode: Standard Play RBT to Transferee: No Remote Box Mode: Handle Locally <p>SBC MEDIA</p> <ul style="list-style-type: none"> Mediation Mode: RTP Mediation Extension Coders Group: -- Allowed Audio Coders: #0 [BTIP] View Allowed Coders Mode: Restriction and Preference <p>SBC HOLD</p> <ul style="list-style-type: none"> Remote Hold Format: Send Only Reliable Held Tone Source: No Play Held Tone: Internal <p>User Registration Time: 0 NAT UDP Registration Time: -1 NAT TCP Registration Time: -1</p> <p>Cancel APPLY</p>
	<p>IP Profiles [Profile_Orange_North]</p> <p>QUALITY OF SERVICE</p> <ul style="list-style-type: none"> RTP IP Diffserv: 46 Signaling Diffserv: 46 <p>JITTER BUFFER</p> <ul style="list-style-type: none"> Dynamic Jitter Buffer Minimum Delay [msec]: 10 Dynamic Jitter Buffer Optimization Factor: 10 Jitter Buffer Max Delay [msec]: 250 <p>SBC MEDIA</p> <ul style="list-style-type: none"> Mediation Mode: RTP Mediation Extension Coders Group: -- Allowed Audio Coders: #0 [BTIP] View Allowed Coders Mode: Restriction and Preference <p>SBC HOLD</p> <ul style="list-style-type: none"> Remote Hold Format: Send Only Reliable Held Tone Source: No Play Held Tone: Internal <p>GATEWAY DTMF</p> <p>Cancel APPLY</p>

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 'TOPOLOGY VIEW' menu with categories like CORE ENTITIES, CODERS & PROFILES, SBC, and Routing. The 'IP Profiles (3)' item 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>IPPBX</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, including sections for GENERAL, MEDIA SECURITY, and SBC SIGNALING.</p>	INDEX #	NAME	PROFILE PREFERENCE	1	IPP_BTALK	1	2	IPPBX	1	3	IPP	1
INDEX #	NAME	PROFILE PREFERENCE											
1	IPP_BTALK	1											
2	IPPBX	1											
3	IPP	1											

2.7.10 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>8. Open SETUP > SIGNALING & MEDIA > CORE ENTITIES > SIP Interfaces</p> <p>9. Click on “+ New” Enter a meaningful name ex” SI_BTALK”</p> <p>10. Change the parameters indicated above as follow</p>	

Actions	Screenshot
<p>11. Click on “Apply” The new Objects will appear in the list.</p>	
<p>12. 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>	

Actions	Screenshot																		
	<p>Message Policies (2)</p> <p>Page 1 of 1 Show 10 records per page</p> <table border="1"> <thead> <tr> <th>INDEX</th> <th>NAME</th> <th>MAX MESSAGE LENGTH</th> <th>MAX HEADER LENGTH</th> <th>MAX BODY LENGTH</th> <th>SEND REJECTION</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Malicious Signature DB Protection</td> <td>-1</td> <td>-1</td> <td>-1</td> <td>Policy Drop</td> </tr> <tr> <td>1</td> <td>BTALK Max Sip Size</td> <td>4096</td> <td>-1</td> <td>1024</td> <td>Policy Reject</td> </tr> </tbody> </table> <p>#0[Malicious Signature DB Protection] Edit</p> <p>GENERAL</p> <p>Name: Malicious Signature DB Protection</p> <p>LIMITS</p> <p>Max Message Length: -1 Max Header Length: -1 Max Body Length: -1 Max Num Headers: -1 Max Num Bodies: -1</p> <p>POLICIES</p> <p>Send Rejection: Policy Drop Method List: Method List Type: Policy Blacklist Body List: Body List Type: Policy Blacklist Malicious Signature Dat...: Enable</p>	INDEX	NAME	MAX MESSAGE LENGTH	MAX HEADER LENGTH	MAX BODY LENGTH	SEND REJECTION	0	Malicious Signature DB Protection	-1	-1	-1	Policy Drop	1	BTALK Max Sip Size	4096	-1	1024	Policy Reject
INDEX	NAME	MAX MESSAGE LENGTH	MAX HEADER LENGTH	MAX BODY LENGTH	SEND REJECTION														
0	Malicious Signature DB Protection	-1	-1	-1	Policy Drop														
1	BTALK Max Sip Size	4096	-1	1024	Policy Reject														
<p>1. Then Message Policies "BTALK Max Sip Size" is called into the Sip Interface Ex: BTol</p>	<p>SIP Interfaces [BTIP01]</p> <p>SID: #0 [DefaultSRC]</p> <p>GENERAL</p> <p>Index: 2 Name: BTIP01 Topology Location: Up Network Interface: #0 [Public_DMZ] Application Type: SBC UDP Port: 0 TCP Port: 0 TLS Port: 5061 Additional UDP Ports: Additional UDP Ports Mode: Always Open</p> <p>MEDIA</p> <p>Media Realm: #2 [BTIP01] Direct Media: Disable</p> <p>SECURITY</p> <p>TLS Context Name: #1 [Orange BTIP01] TLS Mutual Authentication: Enable Message Policy: #1 [BTALK Max SIP Size] User Security Mode: Not configured Enable Un-Authenticated Registrations: Not configured Max. Number of Registered Users: -1</p> <p>Cancel APPLY</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:

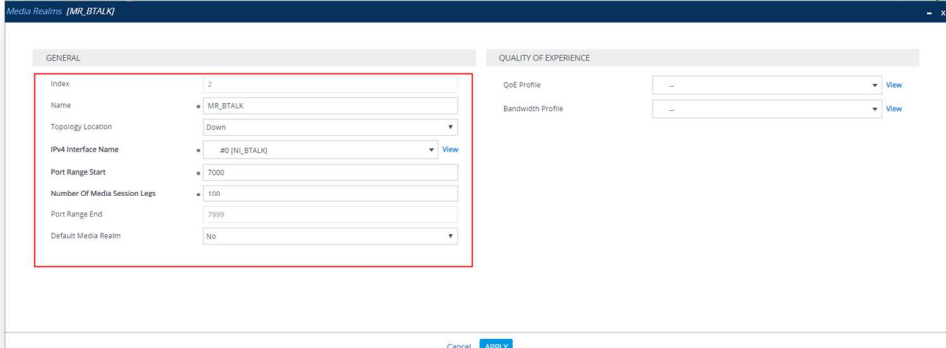
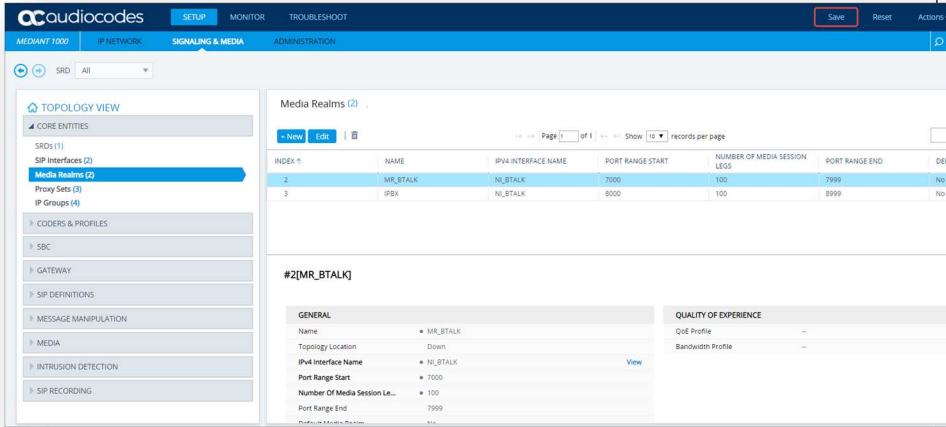
- ✓ For **encrypted BTALK French & International SIP Trunk** architecture we need to configure **RTP port 6 000 to 20 000**

Note: On Audiocodes SBC, 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 6050 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 Customer service offer. “Port Range Start” and “IP interface name” will defined by the Customer itself.

Actions	Screenshot
<ol style="list-style-type: none"> 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 	
<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. **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 BTALK 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 will be configured for redundancy purpose

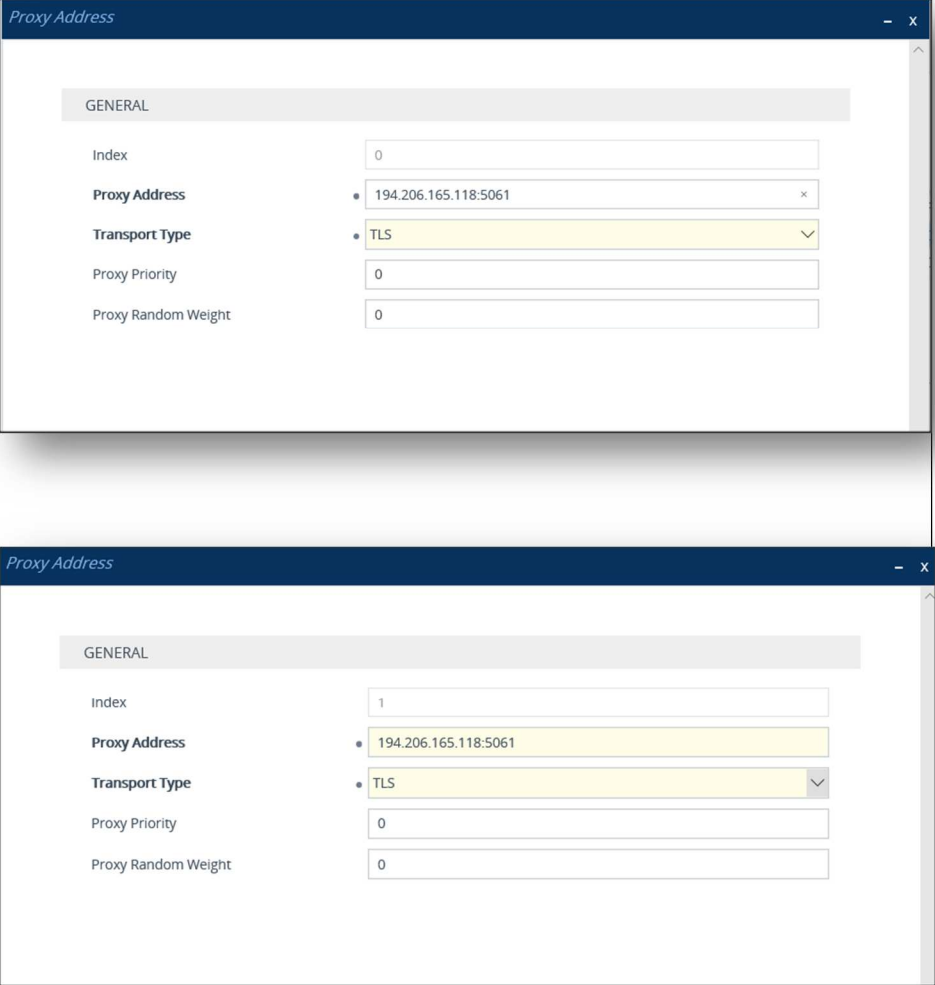
The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

Index	Name	SIP Interface	TLS Context Name	Proxy Keep-Alive	Redundancy Mode	Proxy Hot Swap	Index Proxy Addresses	Proxy Address	Transport Type
1	PS_BTALK	SI_BTALK	Orange	Using OPTIONS	Homing	Enable	0	<BT- Public FQDN, Nominal or IP>;5061	TLS
							1	<BT- Public FQDN, FQDN Backup or IP>;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 IP set in the “Proxy Address” is the “**Public FQDN**” or “**Public IP**” provided by Orange for the SIP trunk BTALK. “Options” message will be sent by the Audiocodes SBC 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 the correct IP or FQDN

Actions	Screenshot
<p>2. Open SETUP > SIGNALING & MEDIA > CORE ENTITIES > PROXY SETS</p> <p>3. Click on "+ New" Enter a meaningful name ex" PS_BTALK"</p> <p>4. Change the parameters indicated above as follow</p>	
<p>5. Click on "Apply". The new Objects will appear in the list.</p>	
<p>6. To configure "Proxy Address" and "Transport Type", you have to configure to select the "Proxy Set" just created.</p> <p>7. Click on the "Proxy Address 0 items" link at the bottom of the page</p>	

Actions	Screenshot
<p>8. If you want to backup the nominal BT Proxy address index 0, you can add a second "Proxy Address" as backup with the Index 1</p> <p>9. At the End at least 1 Proxy Items should created (2 items in case of Backup)</p>	 <p>The top screenshot shows the configuration for Index 0. The fields are: Index: 0, Proxy Address: 194.206.165.118:5061, Transport Type: TLS, Proxy Priority: 0, and Proxy Random Weight: 0.</p> <p>The bottom screenshot shows the configuration for Index 1. The fields are: Index: 1, Proxy Address: 194.206.165.118:5061, Transport Type: TLS, Proxy Priority: 0, and Proxy Random Weight: 0.</p>

IP Group Table

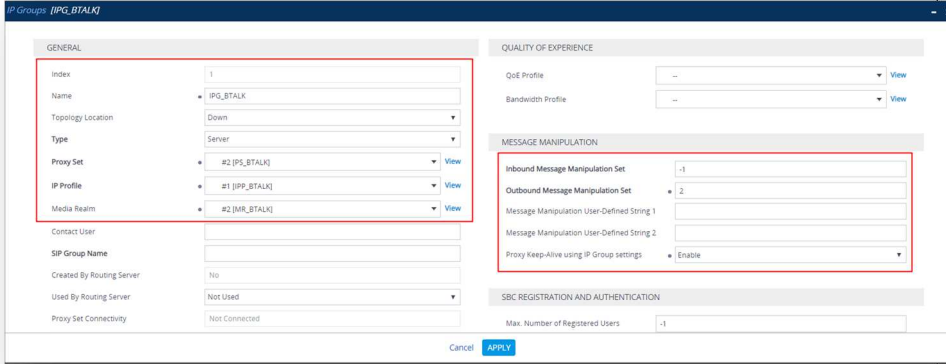
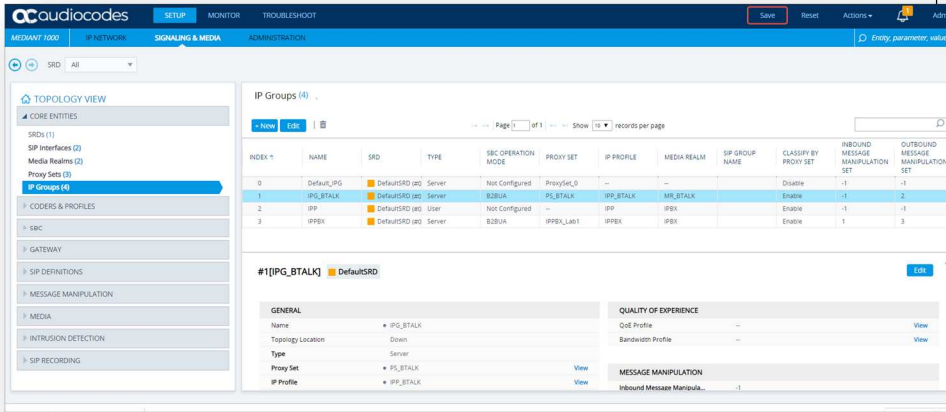
The IP Group table allows logical IP entities creation with a set of parameters such as Proxy set ID, IP profile ID to separate provenance and destination traffic.

A new IP Group specific to Orange BTALK 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_BTALK	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"> 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" 	
<ol style="list-style-type: none"> 5. Click on "Apply". The new Objects will appear in the list. 	

2.7.11 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 \(SBC Application\)](#)”.

Please jump to this Chapter directly

2.8 OBS Business Talk & BTIP Carrier North **encrypted** SIP configuration for AudioCodes SBC (TLS)

2.8.1 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 is supported as Cipher Client/Server:**
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 - 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 (Recommended)
 - 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 activate**

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	Orange	DHE-RSA-AES256-GCM-SHA384	DHE-RSA-AES256-GCM-SHA384	2048

Actions	Screenshot
<ol style="list-style-type: none"> 4. Open SETUP > IP NETWORK > SECURITY > TLS CONTEXTS 5. Click on "+ New" Enter a meaningful name ex" Orange" 6. Change the parameters indicated above as follow 	

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

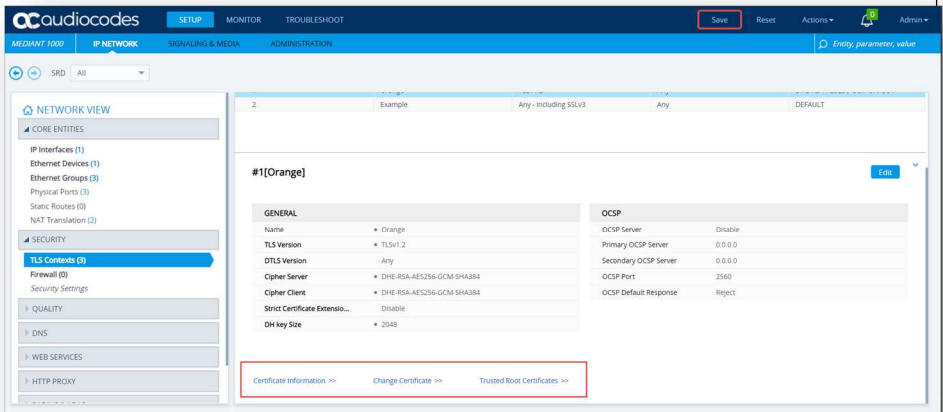
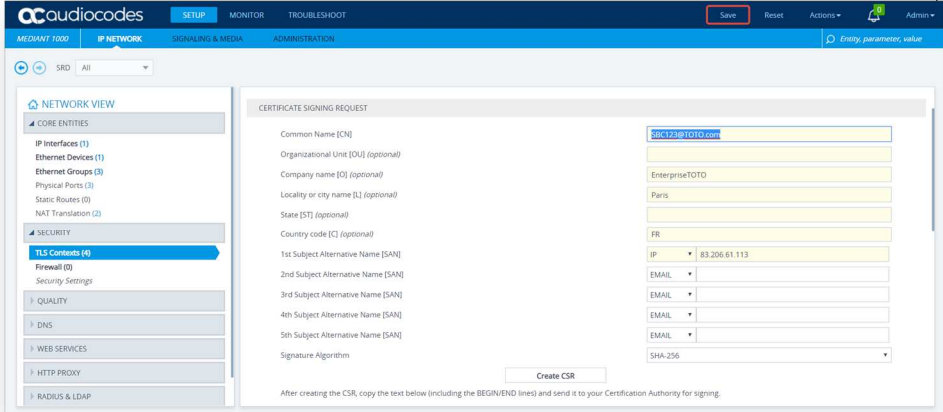
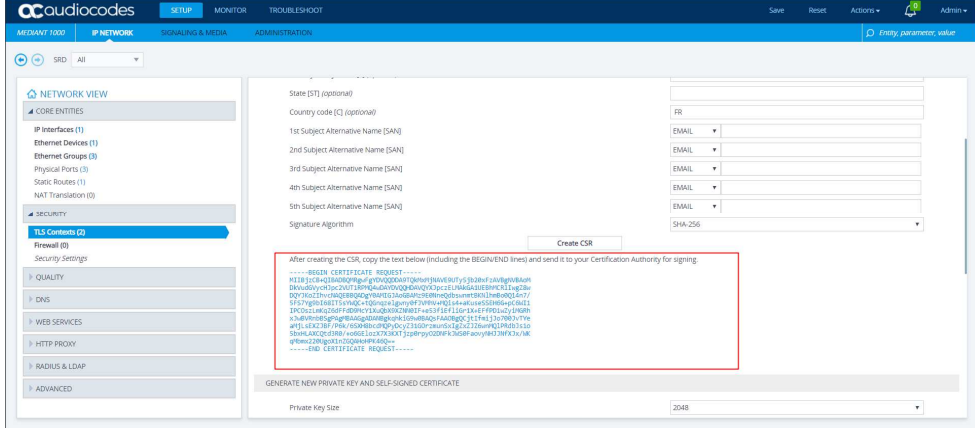
Certificate Signing Request (CSR)

The TLS Context need a Certificate signed. To obtain this Certificate Authority (CA) you must generate your CSR base on the information of the SBC and Company with SHA-256 encryption. As soon you received the CA, you will load it on the Audiocodes SBC 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 SBC 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	-	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	
<p>13. On the TLS context you just create go on the Bottom page and click on "Change Certificate"</p> <p>14. Change the parameters indicated above</p> <p>15. Click "Create CSR"</p>	 
<p>On the page should appear a text in blue which represent your CSR.</p>	

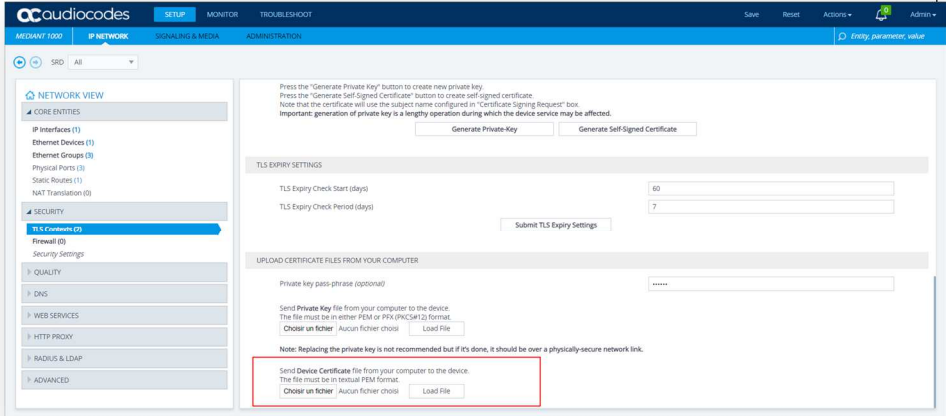
When the CSR is generated copy the CSR text and send it to Organization to be signed and get a Certificate Authority (CA). The Root and intermediate Certificate (crt files) must be transmitted to Orange Business Services team.

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 SBC.

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/MQswCQYDVQQGEwJGUjE'ETMBEGA1U
EChMKQ2VydG1wb3N0ZTEbMBkGA1UEAxMSQ2VydG1wb3N0ZSBTZXJ2ZXVYMB4XDTE4MDYyNDA4MD
AwMFoXDTE4MDYyNDA4MDAwMFowPzELMAkGA1UEBhMCRLIxEzARBgNVBAoTCkNlcnRpcG9zdGUxG
zAZBgNVBAMTEkNlcnRpcG9zdGUxG9zZG9U2VydM1VlcjCCASEwDQYJKoZIhvcNAQEBBQADggEoADCCAQkC
ggEAPqd4MziR4spWldGRx8bQrhZkonWnNm`+Yhb7+4Q67ecf1janH7GcN/SXsf7jJpreWULf7v
7Cvpr4R7qIJcmdHIntmf7JPM5n6cDBv17uSW63er7NkVnMFHwK1QaGFLMybFkzaeGrvFm4k3lRe
fiXDmuOe+FhJgHYezYHf44LvPRPwhSrzi9+Aq3o8pWDguJuZDIUP1F1jMa+LPwvREXfFcUW+w==
-----END
```

Actions	
<p>16. On the TLS context you created go on the Bottom page and click on "Change Certificate"</p> <p>17. 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.</p> <p>18. After the certificate successfully loads to the device, save the configuration with a device reset.</p> <p>19. Verify that the private key is correct: -Open the TLS Contexts table.</p>	

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

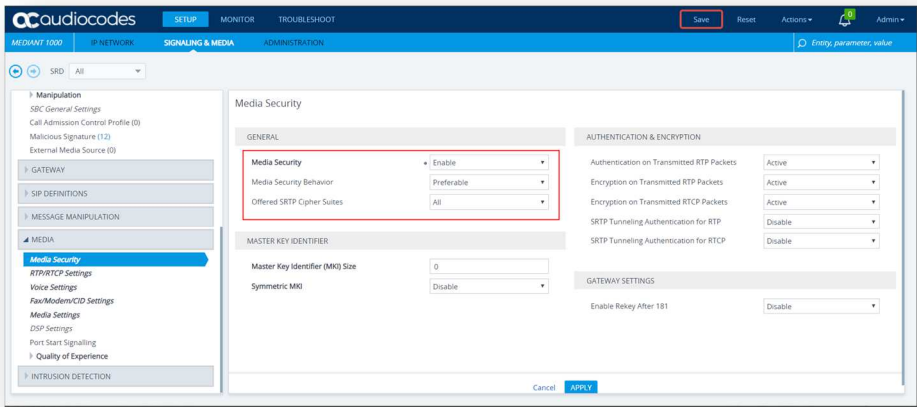
After that the Root and intermediate Certificate (PEM format) must be transmitted to Orange BTALK.

2.8.2 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
Enable	Preferable	all

Actions	Screenshot
<ol style="list-style-type: none"> 4. Open SETUP > SIGNALING & MEDIA > MEDIA > MEDIA SECURITY 5. Change the parameters indicated above as follow 6. Click on “Apply 	 <p>The screenshot shows the 'Media Security' configuration page in the AudioCodes eSBC interface. The 'GENERAL' section is highlighted with a red box, containing the following settings:</p> <ul style="list-style-type: none"> Media Security: Enable (dropdown) Media Security Behavior: Preferable (dropdown) Offered SRTP Cipher Suites: All (dropdown) <p>Other sections visible include:</p> <ul style="list-style-type: none"> AUTHENTICATION & ENCRYPTION: <ul style="list-style-type: none"> Authentication on Transmitted RTP Packets: Active Encryption on Transmitted RTP Packets: Active Encryption on Transmitted RTCP Packets: Active SRTP Tunneling Authentication for RTP: Disable SRTP Tunneling Authentication for RTCP: Disable MASTER KEY IDENTIFIER: <ul style="list-style-type: none"> Master Key Identifier (MKI) Size: 0 Symmetric MKI: Disable GATEWAY SETTINGS: <ul style="list-style-type: none"> Enable Rekey After 181: Disable

2.8.3 IP Network

No configuration is required in this section. Existing IP Interface, Ethernet Device and Device Group could be used. It is anyway 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.

2.8.4 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 accept the following codecs in this order or preference for SIP trunking over Internet:
G.711 A-law 20 ms (G.711 μ -law 20 ms for International BT Offer cane requested).

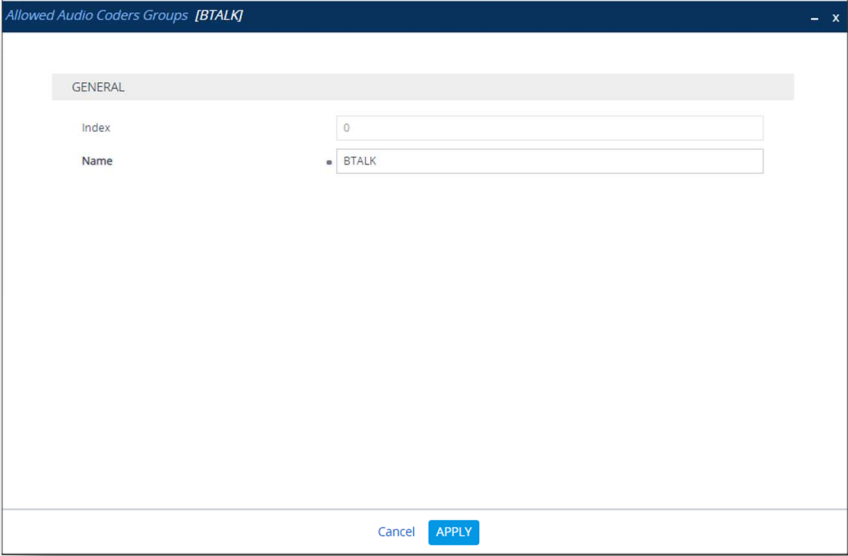
We are going to create a new “Coders Groups” specific to Orange BTalk.

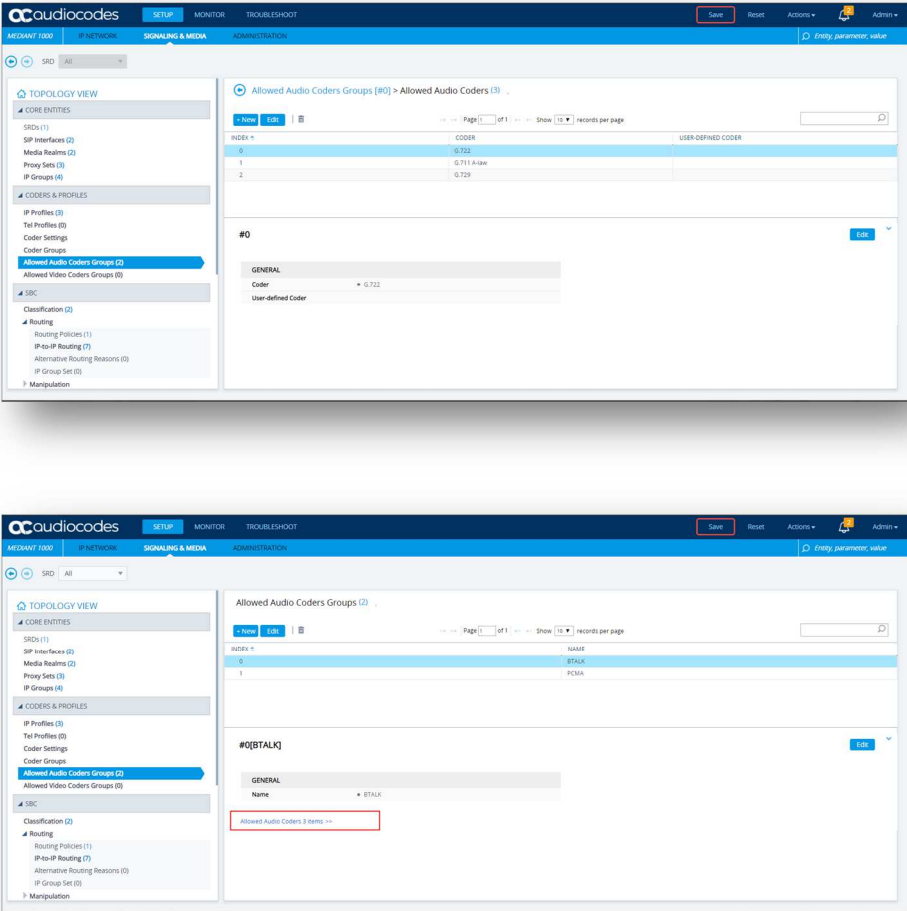
Index	Name
0	BTALK
1	PS_IPBX

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

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

Note: G.711 μ -law 20 ms can be request specifically on demand

Actions	Screenshot
<p>8. Open SETUP > SIGNALING & MEDIA > CODERS & PROFILES > Allowed Audio Coders Groups</p> <p>9. Click on "+ New"</p> <p>10. Enter a meaningful name ex" BTALK"</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>Please note: 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 configuration page for 'Allowed Audio Coders Groups' with the following table:</p> <table border="1"> <thead> <tr> <th>INDEX</th> <th>CODER</th> <th>USER-DEFINED CODER</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>G722</td> <td></td> </tr> <tr> <td>1</td> <td>G711 A-law</td> <td></td> </tr> <tr> <td>2</td> <td>G729</td> <td></td> </tr> </tbody> </table> <p>The bottom screenshot shows the configuration page for 'Allowed Audio Coders Groups' with the following table:</p> <table border="1"> <thead> <tr> <th>INDEX</th> <th>NAME</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>BTALK</td> </tr> <tr> <td>1</td> <td>PCMA</td> </tr> </tbody> </table>	INDEX	CODER	USER-DEFINED CODER	0	G722		1	G711 A-law		2	G729		INDEX	NAME	0	BTALK	1	PCMA
INDEX	CODER	USER-DEFINED CODER																	
0	G722																		
1	G711 A-law																		
2	G729																		
INDEX	NAME																		
0	BTALK																		
1	PCMA																		

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 SBC, 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.

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

Actions	Screenshot
<p>15. Open SETUP > SIGNALING & MEDIA > CODERS & PROFILES > Allowed Audio Coders Groups</p> <p>16. Click on “+ New”</p> <p>17. Enter a meaningful name ex” PCMA”</p> <p>18. Click on “Apply”</p> <p>19. Click on “Allowed Audio Coders 0 items”</p>	

Actions	Screenshot
<p>20. Click on "+ New"</p> <p>21. Select the coders as mention in the table of parameters above, in the same order</p> <p>Please note: 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 configuration for 'Allowed Audio Coders Groups (2)'. The left sidebar lists navigation options like 'CORE ENTITIES', 'CODERS & PROFILES', and 'SBC'. The main area shows a table with columns 'INDEX' and 'NAME'. The table contains two rows: index 0 with name 'BTIP' and index 1 with name 'PCMA'. Below the table, there is a section for '#1[PCMA]' with a 'GENERAL' tab and a 'Name' field set to 'PCMA'. A yellow highlight indicates 'Allowed Audio Coders 1 items >>'. The bottom screenshot shows the configuration for 'Allowed Audio Coders Groups [#0] > Allowed Audio Coders (1)'. The table has columns 'INDEX', 'CODER', and 'USER-D'. It contains one row: index 0 with coders 'G.711 A-law'. Below the table, there is a section for '#0' with a 'GENERAL' tab and a 'Coder' field set to 'G.711 A-law'.</p>

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

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

For encryption, the Audiocodes SBC will encrypt the RTP tower Orange BTALK 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. 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, **SBC 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**”

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

“Section: **SBC 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**”

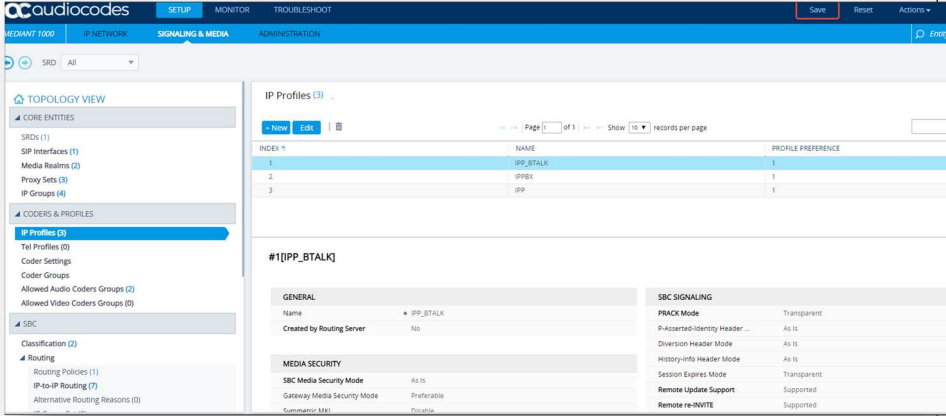
Signaling DiffServ
46

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

Remote REFER Mode	Remote 3xx Mode
Handle Locally	Handle Locally

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

Actions	Screenshot
	<p>The screenshots illustrate the configuration of SBC profiles. The first screenshot shows the 'SBC MEDIA' configuration for profile [IPP_BTALK], where the 'Allowed Audio Coders' is set to '#0 [BTALK]'. The second screenshot shows the 'SBC FORWARD AND TRANSFER' configuration for profile [Profile_Orange_North], where the 'Remote REFER Mode' is set to 'Handle Locally'. The third screenshot shows the 'QUALITY OF SERVICE' configuration for profile [Profile_Orange_North], where the 'RTP IP Diffserv' is set to '46'.</p>

Actions	Screenshot												
<p>Click on “Apply” The new Objects will appear in the list.</p>	 <p>The screenshot shows the AudioCodes management console. On the left is a 'TOPOLOGY VIEW' sidebar with a tree structure including 'CORE ENTITIES', 'CODERS & PROFILES', 'SBC', and 'Routing'. The 'IP Profiles (3)' item 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>IPPBX</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 in a form with sections for 'GENERAL', 'MEDIA SECURITY', and 'SBC SIGNALING'. The 'GENERAL' section includes fields for Name (IPP_BTALK), Created by Routing Server (No), and SBC Media Security Mode (As Is). The 'SBC SIGNALING' section includes fields for FRACK Mode (Transparent), P-Asserted-Identity Header Mode (As Is), Diversion Header Mode (As Is), History-Info Header Mode (As Is), Session Expires Mode (Transparent), Remote Update Support (Supported), and Remote re-INVITE (Supported).</p>	INDEX #	NAME	PROFILE PREFERENCE	1	IPP_BTALK	1	2	IPPBX	1	3	IPP	1
INDEX #	NAME	PROFILE PREFERENCE											
1	IPP_BTALK	1											
2	IPPBX	1											
3	IPP	1											

2.8.5 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:

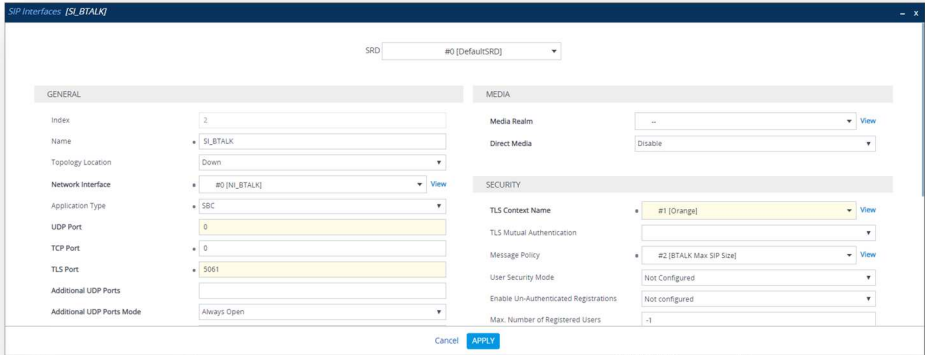
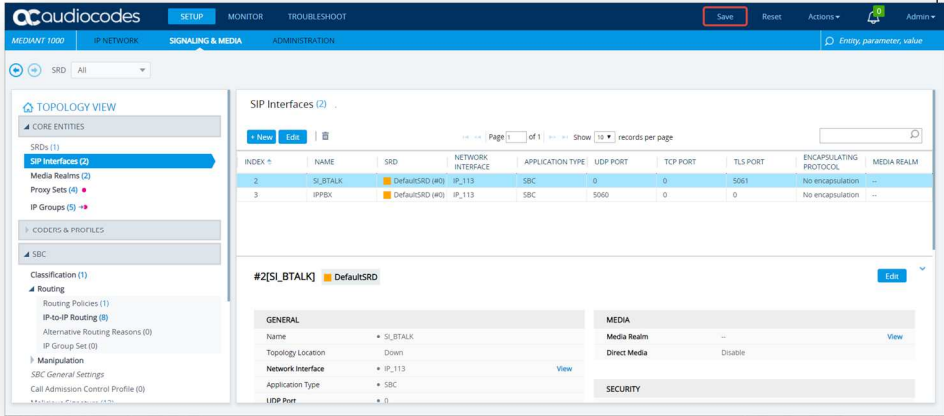
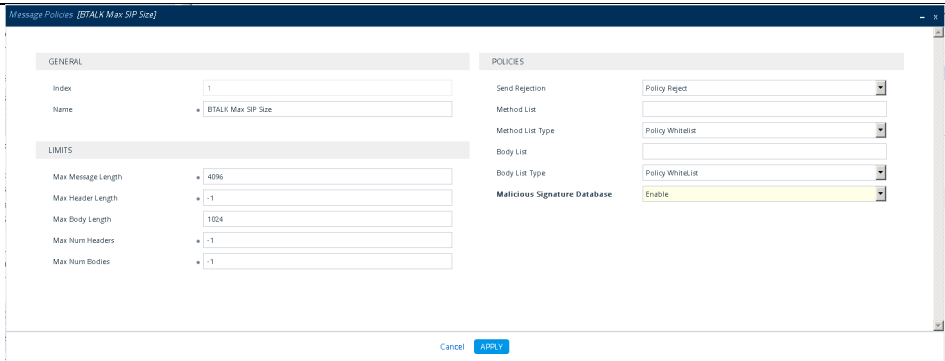
- ✓ For **encrypted BTALK SIP Trunk** architecture we need to configure **TLS port 5061**

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>20. Open SETUP > SIGNALING & MEDIA > CORE ENTITIES > SIP Interfaces</p> <p>21. Click on “+ New” Enter a meaningful name ex” SI_BTALK”</p> <p>22. Change the parameters indicated above as follow</p>	

Actions	Screenshot
	
<p>23. Click on “Apply” The new Objects will appear in the list.</p>	
<p>24. 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>	

Actions	Screenshot																		
	<p>Message Policies (2)</p> <p>Page 1 of 1 Show 10 records per page</p> <table border="1"> <thead> <tr> <th>INDEX</th> <th>NAME</th> <th>MAX MESSAGE LENGTH</th> <th>MAX HEADER LENGTH</th> <th>MAX BODY LENGTH</th> <th>SEND REJECTION</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Malicious Signature DB Protection</td> <td>-1</td> <td>-1</td> <td>-1</td> <td>Policy Drop</td> </tr> <tr> <td>1</td> <td>BTALK Max Sip Size</td> <td>4096</td> <td>-1</td> <td>1024</td> <td>Policy Reject</td> </tr> </tbody> </table> <p>#0[Malicious Signature DB Protection] Edit</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>GENERAL</p> <p>Name: Malicious Signature DB Protection</p> <p>LIMITS</p> <p>Max Message Length: -1 Max Header Length: -1 Max Body Length: -1 Max Num Headers: -1 Max Num Bodies: -1</p> </div> <div style="width: 45%;"> <p>POLICIES</p> <p>Send Rejection: Policy Drop Method List: Method List Type: Policy Blacklist Body List: Body List Type: Policy Blacklist Malicious Signature Dat...: Enable</p> </div> </div>	INDEX	NAME	MAX MESSAGE LENGTH	MAX HEADER LENGTH	MAX BODY LENGTH	SEND REJECTION	0	Malicious Signature DB Protection	-1	-1	-1	Policy Drop	1	BTALK Max Sip Size	4096	-1	1024	Policy Reject
INDEX	NAME	MAX MESSAGE LENGTH	MAX HEADER LENGTH	MAX BODY LENGTH	SEND REJECTION														
0	Malicious Signature DB Protection	-1	-1	-1	Policy Drop														
1	BTALK Max Sip Size	4096	-1	1024	Policy Reject														
<p>10. Then Message Policies “BTALK Max Sip Size” is called into the Sip Interface Ex: BTol</p>	<p>SIP Interfaces [BTIP01]</p> <p>SID: #0 [DefaultSRC]</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>GENERAL</p> <p>Index: 2 Name: BTIP01 Topology Location: Up Network Interface: #0 [Public_DMZ] Application Type: SBC UDP Port: 0 TCP Port: 0 TLS Port: 5061 Additional UDP Ports: Additional UDP Ports Mode: Always Open</p> </div> <div style="width: 45%;"> <p>MEDIA</p> <p>Media Realm: #2 [BTIP01] Direct Media: Disable</p> <p>SECURITY</p> <p>TLS Context Name: #1 [Orange BTIP01] TLS Mutual Authentication: Enable Message Policy: #1 [BTALK Max Sip Size] User Security Mode: Not configured Enable Un-Authenticated Registrations: Not configured Max. Number of Registered Users: -1</p> </div> </div> <p style="text-align: right;">Cancel APPLY</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:

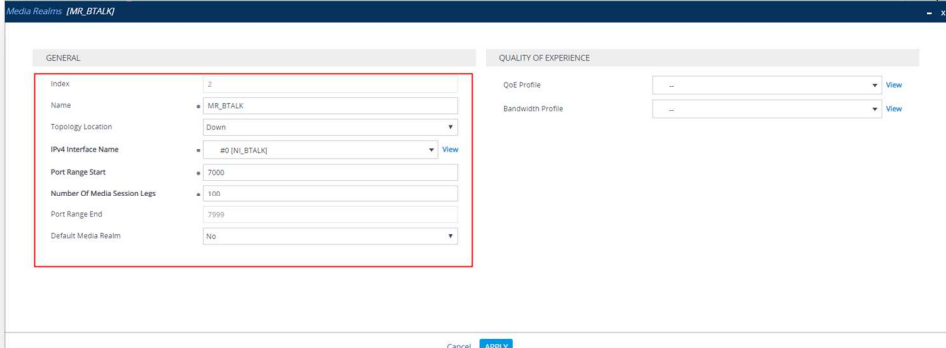
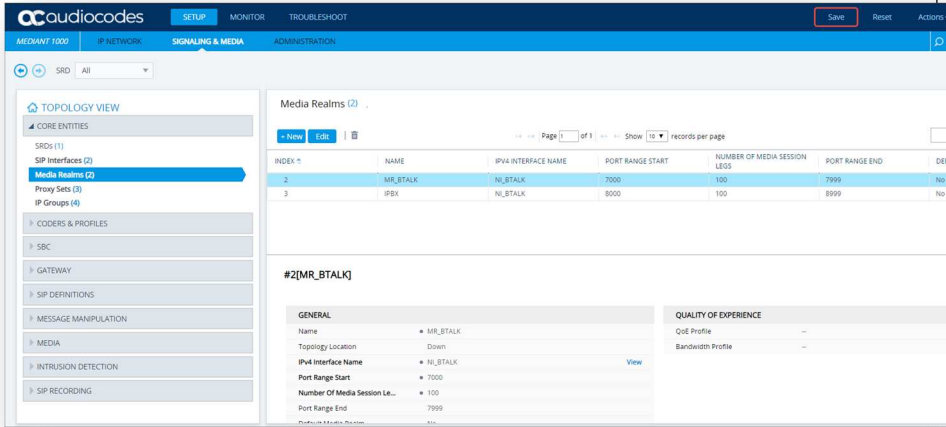
- ✓ For **encrypted BTALK over Internet International SIP Trunk** architecture we need to configure **RTP port 6 000 to 20 000**
- ✓ For **encrypted BTALK IP over Internet French SIP Trunk** architecture we need to configure **RTP port 6 000 to 38 000**

Note: On Audiocodes SBC, 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 6050 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 Customer service offer. “Port Range Start” and “IP interface name” will defined by the Customer itself.

Actions	Screenshot
<ol style="list-style-type: none"> 4. Open SETUP > SIGNALING & MEDIA > CORE ENTITIES > MEDIA REALMS 5. Click on "+ New" Enter a meaningful name ex" MR_BTALK" 6. Change the parameters indicated above as follow 	
<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. **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 BTALK 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 will be configured for redundancy purpose

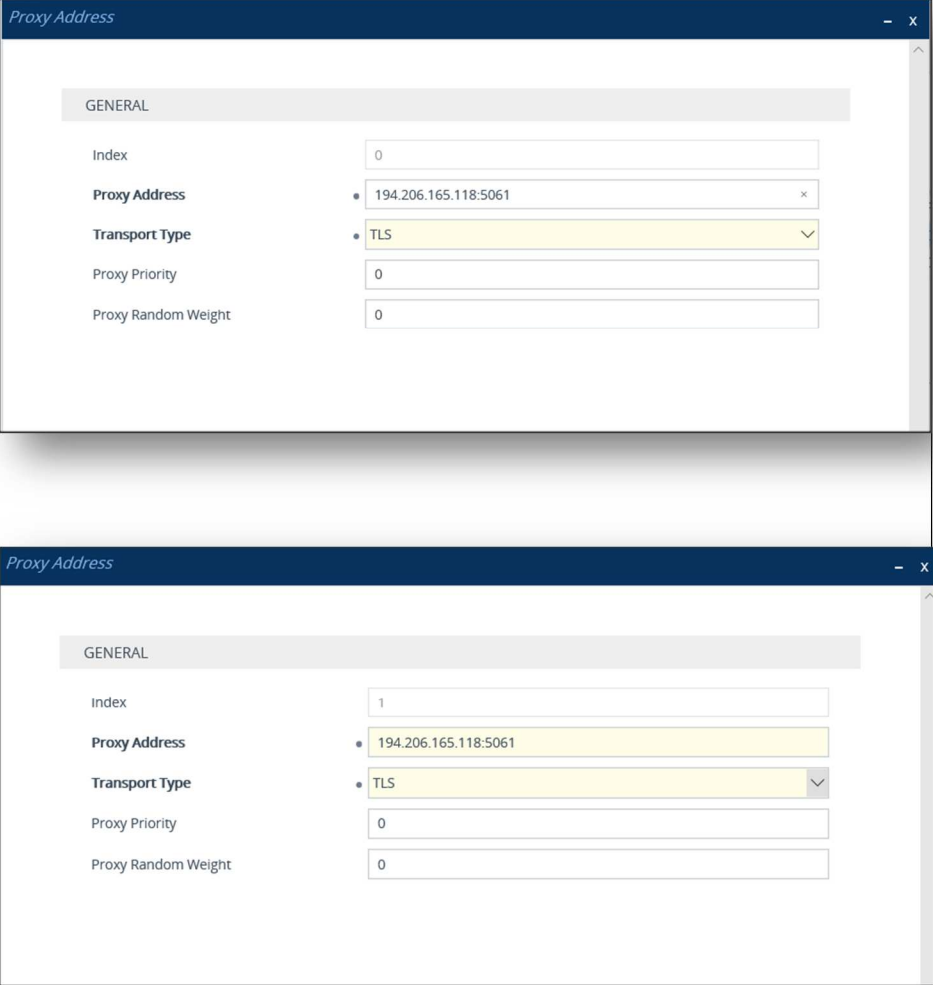
The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

Index	Name	SIP Interface	TLS Context Name	Proxy Keep-Alive	Redundancy Mode	Proxy Hot Swap	Index Proxy Addresses	Proxy Address	Transport Type
1	PS_BTALK	SI_BTALK	Orange	Using OPTIONS	Homing	Enable	0	<BT- Public FQDN_Nominal or IP>:5061	TLS TLS
							1	<BT- Public FQDN_FQDN_Backup or IP>:5061	
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 IP set in the “Proxy Address” is the “**Public FQDN**” or “**Public IP**” provided by Orange for the SIP trunk BTALK. “Options” message will be sent by the Audiocodes SBC 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 the correct IP or FQDN

Actions	Screenshot
<p>11. Open SETUP > SIGNALING & MEDIA > CORE ENTITIES > PROXY SETS</p> <p>12. Click on "+ New" Enter a meaningful name ex" PS_BTALK"</p> <p>13. Change the parameters indicated above as follow</p>	
<p>14. Click on "Apply". The new Objects will appear in the list.</p>	
<p>15. To configure "Proxy Address" and "Transport Type", you have to configure to select the "Proxy Set" just created.</p> <p>16. Click on the "Proxy Address 0 items" link at the bottom of the page</p>	

Actions	Screenshot
<p>17. If you want to backup the nominal BT Proxy address index 0, you can add a second "Proxy Address" as backup with the Index 1</p> <p>18. At the End at least 1 Proxy Items should created (2 items in case of Backup)</p>	 <p>The top screenshot shows the configuration for Index 0. The fields are: Index: 0, Proxy Address: 194.206.165.118:5061, Transport Type: TLS, Proxy Priority: 0, and Proxy Random Weight: 0.</p> <p>The bottom screenshot shows the configuration for Index 1. The fields are: Index: 1, Proxy Address: 194.206.165.118:5061, Transport Type: TLS, Proxy Priority: 0, and Proxy Random Weight: 0.</p>

IP Group Table

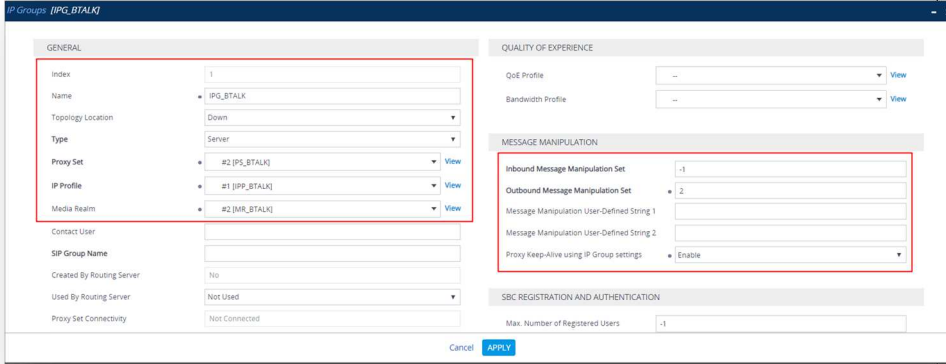
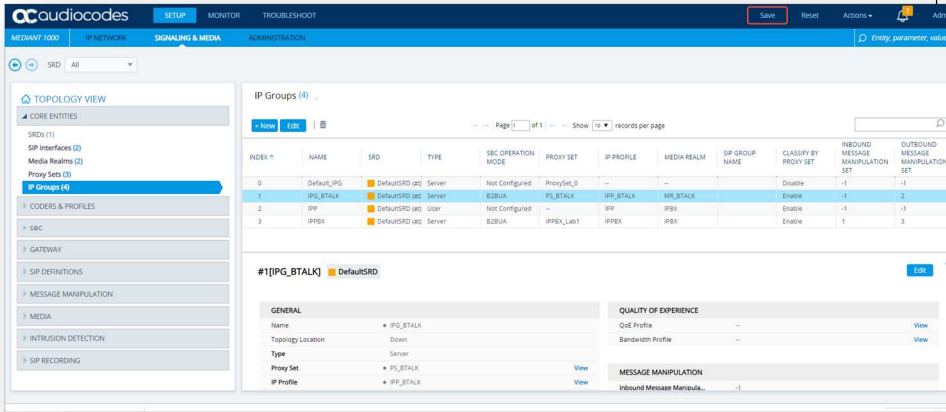
The IP Group table allows logical IP entities creation with a set of parameters such as Proxy set ID, IP profile ID to separate provenance and destination traffic.

A new IP Group specific to Orange BTALK 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_BTALK	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
<p>6. Open SETUP > SIGNALING & MEDIA > CORE ENTITIES > IP_GROUP</p> <p>7. Click on “+ New” Enter a meaningful name ex” IPG_BTALK”</p> <p>8. Click on “Apply”</p> <p>9. Click on “Allowed Audio Coders 0 items”</p>	
<p>10. Click on “Apply”. The new Objects will appear in the list.</p>	

2.8.6 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 \(SBC Application\)](#)”.

Please jump to this Chapter directly

2.9 SIP rules & manipulations (SBC Application)

This section provides the configuration regarding the device's SBC 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.

2.9.1 IP-to-IP Routing Table

This section provide configuration about IP-to-IP routing rules for SBC 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 SBC 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	<i>IPBX > BTIP</i>	<i>IPG_IPBX</i>	Any	IP Group	IPG_BTALK	
2	<i>BTIP > IPBX</i>	IPG_BTALK	Any	IP Group	<i>IPG_IPBX</i>	

2.9.2 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 SBC 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.

2.9.3 Inbound Manipulations

No inbound manipulation Number is required for default installation.

2.9.4 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=>SBC).
- Manipulation **Man Set ID “2”** include **21 manipulations** Index “1” to “21”. They are applied on messages outgoing towards Orange BTALK SIP trunk (SBC=> BTALK). 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 (SBC=> 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 SBC "User-Agent" and IPBX "User-Agent" stored in previous manipulation.
2. Topology hiding modifies "From host" part with SBC 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 SBC IP address.
6. Topology hiding: modifies "Diversion host" part with SBC 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 SBC 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

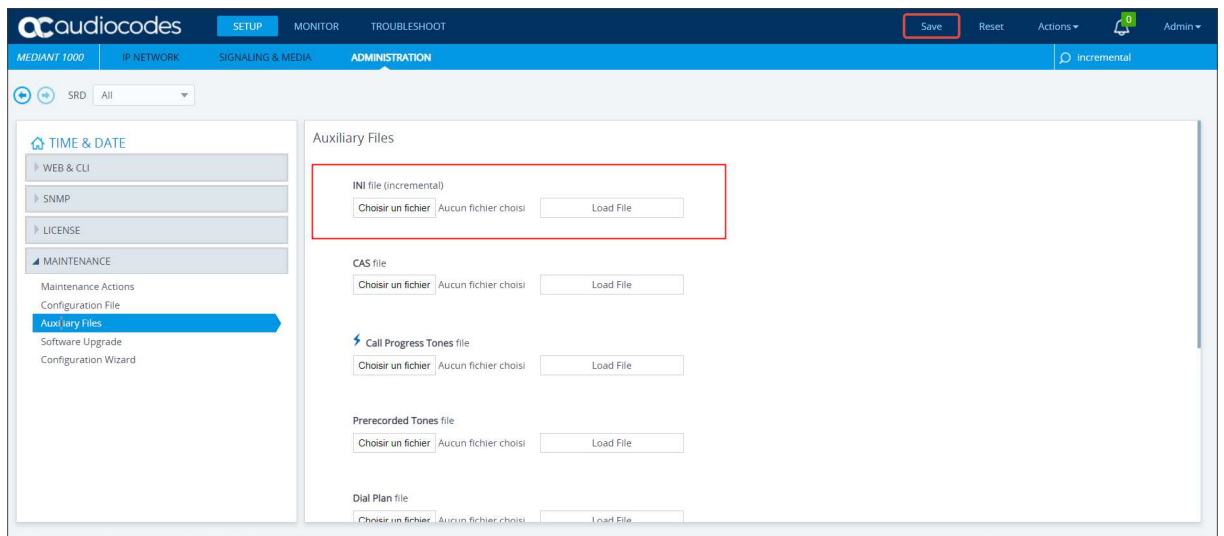
The INI incremental File attachment will allow you to load the Manipulation Rules need for this configuration. Before loading the INI file on the Audiocodes SBC, it is necessary to check if the “Index” and “Man Set ID” number present in the INI incremental file are not already present on the SBC. If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



Please note, “manips_incremental.ini” file can be requested to OBS delivery teams and will be included in the future into the Audiocodes eSBC Configuration Wizard available on Audiocodes web site :

<https://online.audiocodes.com/mediant-sbc-configuration-wizard>

3.2 Example of SIP INVITE message

From IPPBX toward Orange BTALK

```
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 BTALK 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 09:15:25:34 071]
```

3.2.1 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 SBC 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 Mediant 1000 Administration web interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The 'ADMINISTRATION' tab is active, with sub-tabs for 'IP NETWORK', 'SIGNALING & MEDIA', and 'ADMINISTRATION'. The left sidebar shows a navigation menu with 'TIME & DATE' selected. The main content area is titled 'Time & Date' and is divided into two columns: 'LOCAL TIME' 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

4 Glossary

AS : Application Server Business Talk / Business Talk IP

A-SBC : Access Session Border Controller (Orange Business Services infrastructure)

BTalk: Business Talk

BTIP: Business Talk IP

BVPN : Business Virtual Private Network (Orange Business Services)

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

TP WAN : Third Party WAN (on customer side)

UDP: User Datagram Protocol

WAN: Wide Area Network