Business Talk & BTIP Configuration Guidelines with Ribbon Edge Customer eSBC

versions addressed in this guide: Ribbon Edge eSBC V.11 & V12

Version of 21/11/2025

Table of Contents

1. General

1.1 Scope of the document

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

1.2 References documents

Title	Link
Documentation & Software Update for Ribbon SBCs 1000, 2000 and Swe Lite Version 9	https://doc.rbbn.com/display/UXDOC90/Getting+Started
Documentation & Software Update for Ribbon SBCs 1000, 2000 and Swe Lite Version 12.1	https://publicdoc.rbbn.com/spaces/UXDOC121/overview
Documentation & Software Update for Ribbon SBCs 1000, 2000 and Swe Lite Version 12.2	https://publicdoc.rbbn.com/spaces/UXDOC122/overview
Documentation & Software Update for Ribbon SBCs 1000, 2000 and Swe Lite Version 12.3	https://publicdoc.rbbn.com/spaces/UXDOC123/overview

1.3 Prerequisites

1.3.1 Certificates

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

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

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

1.3.2 Public DNS configuration

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

1.3.3 NTP

The configuration of NTP servers on the eSBC is not fully detailed (still some typical example is described in annex) in this document but it is mandatory to implement an NTP server (public reliable NTP server) on Ribbon Edge eSBC to ensure that the eSBC receives the current date and time.
This is necessary for validating Certificates of remote parties during TLS "Handcheck".

1.3.4 Firewall flows for BTIP over Internet and BT over Internet

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

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

Refer to the 'Business Talk IP over Internet pre-requesites' and "Business Talk STAS" documents provided by your sales/project manager team for more details about firewall rules needed to be open.

1.4 Orange BTalk/ BTIP specifications

The information in this chapter is the SIP trunk specifications required to interconnect Orange BT/BTIP network. The Enterprise SBC must be compliant with those specifications. Those information's were used to define the configuration described in this document.

✓ ***Supported RFC's***
- *RFC 3261 : Session initiation protocol*
- *RFC 3264 : An offer/answer Model with the Session Description Protocol*
- *RFC 3262 : Reliability of provisional responses in Session Initiation protocol (please refer to provisional response and PRACK section)*
- *RFC 3311 : The Session Initiation Protocol UPDATE Method*
- *RFC 3323 : A privacy Mechanism for the session Initiation Protocol*
- *RFC 3325 : Session Initiation Protocol for Asserted Identity within Trusted Networks*
- *RFC 3204 : MIME media types for ISUP and QSIG Objects*
- *RFC 3550 : RTP : A transport Protocol for Real Time Applications*
- *RFC 3711: SRTP: Secure Real-time Transport Protocol*
- *RFC 3960 : Early Media and Ringing Tone generation in the Session Initiation Protocol*
- *RFC 4566 : SDP: Session Description Protocol*
- *RFC 4568: SDP: Security Descriptions for Media Streams*
- *RFC 2833/4733 : RTP payload for DTMF digits, Telephony Tones and telephony signals*
- *RFC 5621 : Message Body Handling in the Session Initiation Protocol (SIP)*
- *RFC 5806 : Diversion Indication in SIP*
- *RFC 5009 : Private Header Extension to the Session Initiation Protocol for Authorization of early*
- *RFC 8147: Next-Generation Pan-European eCall*

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

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

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

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

✓ ***SIP signaling specifications are:***
- *For* ***unencrypted architecture*** *we need to configure* ***UDP port 5060***
- *For* ***encrypted architecture*** *(TLS) we need to configure* ***TCP port 5061***

✓ ***Media specifications are by default listed below and should be adapted to your customer service offer:***
- *For* ***unencrypted architecture*** *we need to configure RTP port* ***6 000 to 20 000***
- *For* ***encrypted architecture*** *(TLS) we need to configuration* ***SRTP port 6 000 to 20 000 for Business Talk over Internet or SRTP port 6 000 to 38 000 for Business talk IP over Internet.***

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

✓ ***Encryption specifications are:***
- **TLS V1.3 (Recommended)**

The corresponding Cipher suites below are supported as Cipher Client/Server:
- **TLS_AES_256_GCM_SHA384 (Recommended)**
- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256

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

The corresponding Cipher suites below are supported as Cipher Client/Server:
- **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (Recommended)**
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

✓ ***Media encryption specifications are as follows:***
- SDES key exchange protocol (MIKEY not supported)
- Crypto suite: AES_CM_128_HMAC_SHA1_80
- Both RTP and RTCP are encrypted

✓ ***Codec/Packet Rate specifications are (prefer order list) :***
- List of supported audio codecs and frame size:
  - G.722 20 ms
  - G.711 A law 20 ms, G.711 µ law 20 ms
  - G.729 20 ms, annexb = no

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

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

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

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

✓ Voice Activity Detection (VAD) is not supported

✓ ***DTMF:***

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

✓ ***SIP probing:***

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

Commenté [SC1]: Add timer 300s min

Commenté [SC2R1]: DOne

✓ *FAX support:*

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

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

- ✓ ***Packet marking:***
  - Both SIP signaling and audio must be marked with DSCP 46 (Expedited Forwarding).

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

- ✓ ***Media session modification:***
  - Modification of media (IP, codec, attributes ...) in reception/transmission based on UPDATE (With SDP) in Early Dialog and Re-INVITE in confirmed Dialog (with or without SDP)
  - Attributes “a=” must be equal to “send only, recvonly, inactive, sendrecv”.
  - Same Methods/Attributes/headers may be sent from BTalk/BTIP to Customer SBC.
  - Call Transfer
    - For supervised call transfer, sends RE-INVITE in confirmed dialog
    - For blind call transfer:
      - send RE-INVITE in confirmed dialog
  - Call Forward
    - In case of Call Forward, the diversion header must be provided by the Customer SBC to maintain the original caller information.
  - Call on Hold
    - Send SDP with a=inactive; Setting connection to 0.0.0.0 FORBIDDEN.
  - Music on Hold
    - Initiate a new INVITE to the media server
    - Use Re-INVITE to stop, closing the second dialog.

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

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

- If "P-Early-Media" header is not set in 18x responses, SIP endpoint SHOULD generate local tones unless it can detect early media sent by the remote party.

✓ ***Anonymous calls:***

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

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

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

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

✓ ***Rerouting scenario:***

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

✓ ***Call defection:***

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

✓ ***RTCP***

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

✓ ***STIR SHAKEN***

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

2. Certified Architecture

2.1 Introduction to architecture components and features

This document provides configuration guidelines for the Ribbon Edge E-SBC north (carrier) interface used by the Orange Business (OB) within the VISIT Program.
It outlines the configuration requirements necessary to ensure interoperability between the Ribbon Edge E-SBC and the Business Talk (BT) and Business Talk IP (BTIP) SIP infrastructure, including the A-SBC, Application Server, and interconnections with the PSTN or SIP carriers.
These guidelines apply specifically to the north (carrier) side of the Ribbon Edge E-SBC, which interfaces with BT and BTIP services:

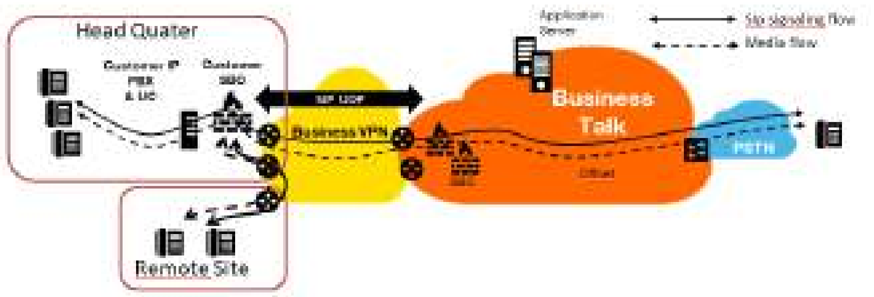
- The configuration will only consider the Carrier aspect of the Ribbon Edge E-SBC (north side), which faces BT/BTIP offers.
- The E-SBC's North-side SIP termination will act as the demarcation point for Orange Business.
- The south side of the Ribbon Edge E-SBC falls outside of OB's control and responsibility.

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

Note: Fax communications via Business Talk are currently allowed but not officially supported.

2.2 Architecture with Ribbon "customer" Edge eSBC with Orange Business SIP North Carrier configuration

2.2.1 Unencrypted SIP Trunk (UDP)

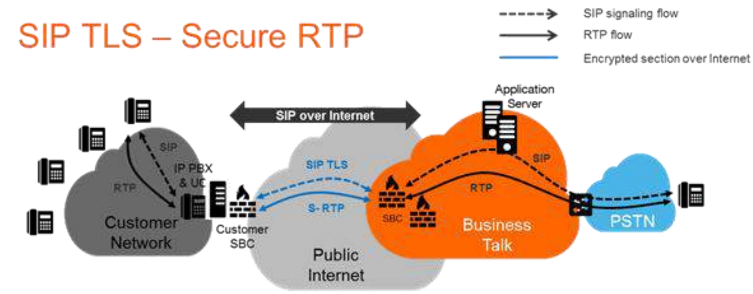


In this architecture:

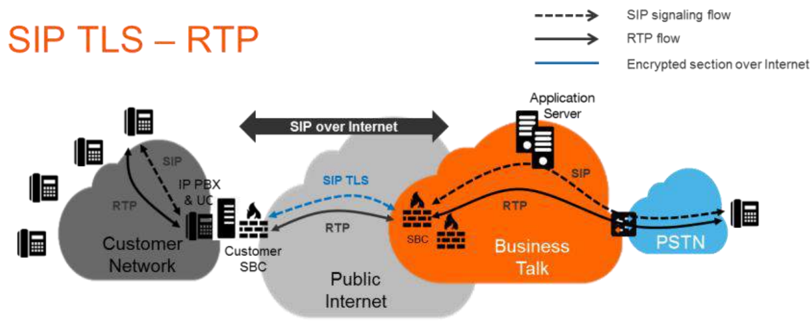
- Both 'SIP trunking' and RTP media flows between endpoints and the Business Talk/BTIP are anchored by the "customer eSBC":
- For Head Quarter & remote sites, media flows are routed through the Customer eSBC and the main BVPN connection.

2.2.2 Encrypted SIP Trunk Over Internet (TLS)

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



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



2.3 Parameters to be provided by customers to access the service.

Unencrypted SIP Trunk through BVPN

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

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

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

Encrypted SIP Trunk through Internet

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

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

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

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

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

2.3.1 Objects

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

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

- Network Interfaces
- Static Routes
- SIP Profiles
- SIP Server Tables
- Message Manipulations
- Media Profiles
- Media Lists
- Signaling Groups
- Transformations Tables
- Call Routing Tables

Note: All configuration parts listed above are present in the menu "SETTINGS" of the Ribbon eSBC WebUI interface:

Ribbon Web User interface

Note: All configuration options are under this tab.

Warning:
Before applying the configuration described in this document, **you need to do a Backup** of your Ribbon eSBC configuration (save the configuration file on your laptop). When you have finished the configuration do an "Apply" of your eSBC configuration and do again of Backup of your new configuration.

Note:
For more information regarding backing up and restoring go to this link

2.3.2 Information and Syntax

The **naming** of the different objects 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, FQDN, capacity, …) in this document are given as example and **must be replaced by the real values** specifically for each interconnection.

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

Examples

Description	Host/domain	Server Lookup	Port number	Protocol
Orange_BTalk	N/A	<IP>	<5060>	<UDP >
Orange_BTalk_TLS	<BT_Public IP_Nominal> <BT-Public_IP_Backup	<Public_IP>	<5061>	<TCP>
Orange_BTIP	N/A	<IP>	<5060>	<UDP >
Orange_BTIP_TLS	BTIP_Public FQDN_Nominal> <BTIP-Public_FQDN_Backup>	<Public_IP>	<5061>	<TLS 5061>
IPPBX	<ippbx.example.com>	IP/FQDN	<Port >	<PROTOCOL >

2.4 Business Talk & BTIP Ribbon Edge eSBC certified versions

<table>
<tr><th colspan="5">Ribbon Edge eSBC * – software versions</th></tr>
<tr><th>Reference product</th><th>Hardware or Virtual Model</th><th>Software Major version</th><th>Certified "Loads"</th><th>Certification</th></tr>
<tr><td rowspan="6">eSBC Edge</td><td>1000</td><td rowspan="3">V.11</td><td rowspan="3">Load(s) 0.3**(min)</td><td rowspan="3">✓
*** With restrictions</td></tr>
<tr><td>2000</td></tr>
<tr><td rowspan="4">SWe Edge (Ex Swe Lite)</td></tr>
<tr><td rowspan="3">V.12</td><td>Load(s) 1.0 build 19**(min)</td><td>✓</td></tr>
<tr><td>Load(s) 2.0 build 29 **(min)</td><td>✓</td></tr>
<tr><td>Load(s) 3.0 build 40 **(min)</td><td>✓</td></tr>
</table>

** Minimum Load for implementation, last most up-to-date Load is recommended per Ribbon.
*** Supported only on Ribbon Swe Edge product are covered by this certification and specifically develop as Local Gateway for Interop with Cisco WebEx Calling, Ribbon Core SWe product are not covered and not certified.

Note:
Ribbon eSBC technical documentations are available on the Ribbon Publci Documentation Center (Link in §2)

2.5 Orange Business Business Talk & BTIP Carrier North unencrypted SIP configuration for Ribbon Edge eSBC (UDP)

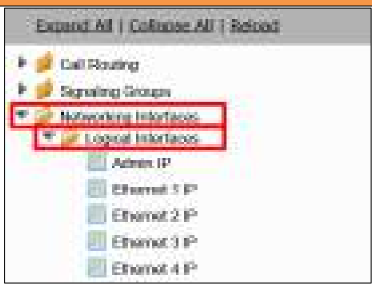
As a prerequisite Ribbon recommends reading the eSBC Edge Security Hardening Checklist to understand how to secure the eSBC into your network infrastructure

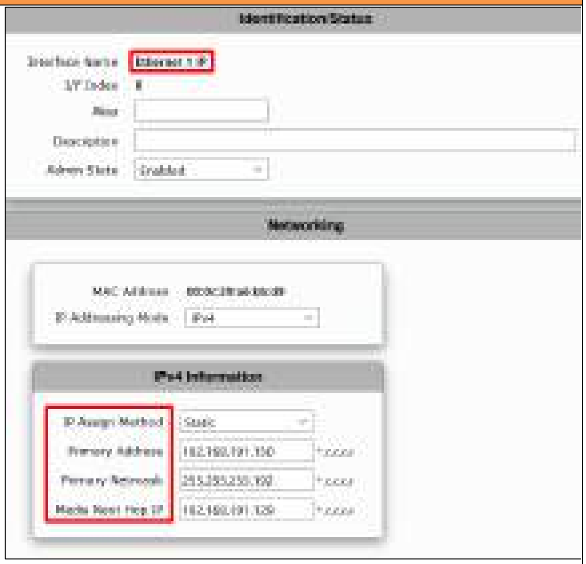
2.5.1 Configure Network Interfaces

No configuration is required in this section if existing Public Node Interface exist and could be reused.

It is anyway highly recommended to have a dedicated Node Interface for SIP Trunking Service provider like Orange to differentiate Traffic SIP Internal and Traffic SIP of the Service Provider.

The Networking Interfaces > Logical Interfaces menu path allows you to configure the IP addresses (both IPv4 and IPv6) for the Ethernet ports and VLANs.

Actions	Screenshot
1. Go to *Networking Interfaces > Logical Interfaces* menu path	

Actions	Screenshot
2. Click on the *Ethernet interface* you want to configure and set the IP information.	
3. Repeat step 2 in case you want to configure additional *Ethernet interfaces* as per your network topology	

Note: The Media Next Hop IP field which is available on SWe Lite only, must be configured with the Default Gateway for this interface.

2.5.2 Message size limit

Orange BTalk/BTIP specifications require to limit the size of the SIP message to 4096 Bytes and SDP Body to 1024 Bytes. To do so,

Ribbon eSBC Edge (SBC1000, SBC2000 and SWe Lite) do not limit the size of SIP/SDP at the application level (sip stack), the packet size is limited by the socket's default size value set by OS

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

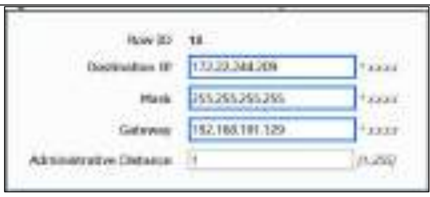
Actions	Screenshot
No action	Set as by design

2.5.3 Configure Static Routes

The *Protocols > IP > Static Route Table* menu path allows one to manually specify the next hop routers used to reach other networks. This is also where you specify the default routes for the connected IP networks (which use 0.0.0.0 as the Destination and Mask).

Note**:**

When DHCP is configured on an interface, the default Static Route (0.0.0.0/0) will be removed and configured dynamically. To view the dynamically created default route, access the WebUI and navigate to ***Protocols > IP > Routing Table****.*

Actions	Screenshot
1. Go to *Protocols > IP > Static Route Table* menu path	
2. To add a new *Static Route* click on the *plus icon (+)*	
3. Set the routing information	
4. Repeat previous steps in case you want to add additional static routes	

2.5.4 Configure SIP Profiles

The SIP Profile enables configuration for parameters, such as SIP Header customization, option tags, etc.

The *SIP > SIP Profiles* menu path controls how the eSBC Edge communicates with SIP devices. They control important characteristics such as: session timers, SIP header customization, SIP timers, MIME payloads, and option tags.

SIP Profile must be configured to be compliant with Orange BTalk/BTIP specifications:

- ✓ Transfer allowed via Re-INVITE
- ✓ Session Timer is not supported

Note:
For **Transfer**, the Ribbon eSBC will be able to **convert REFER** into RE-INVITE.
In some case SIP Provisional Response ACKnowledgement (PRACK RFC 3262))
could be required (such as for Cisco CUCM) to be interworked with Orange which not support PRACK. eSBC device can be configured to resolve this interoperable issue and enable sessions between such endpoints. SIP PRACK handling is configured using the SIP Profile parameter, eSBC PRACK Mode: Mandatory on the SIP profile of the Customer IPPBX.

When Blind and Consultative transfer are handled by the SIP REFER method, the eSBC will generate a new INVITE towards the transfer target. The eSBC does not proxy or send SIP REFER to the transferee. In short, the eSBC handles the REFER message and sends an INVITE to the new target.

The eSBC supports PRACK messages, the flag 100rel at the SIP profile supports this feature.

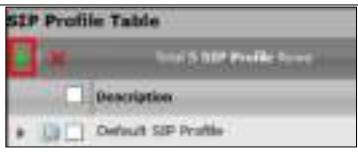
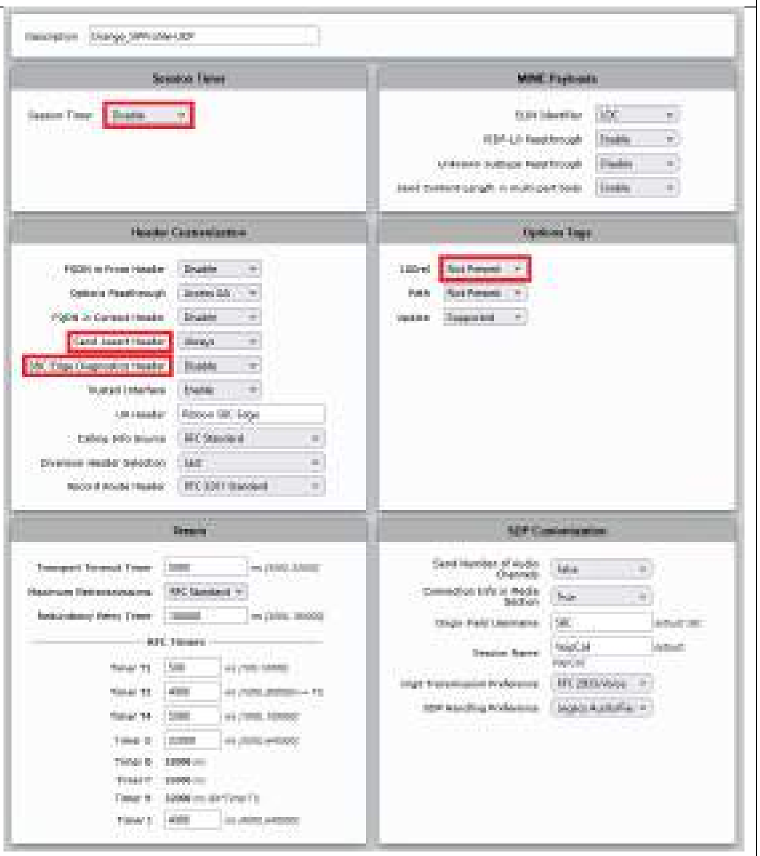
The History-Info header to Diversion header conversion is done automatically.

All of those conversions will stay under customer responsibilities depending on the South private architecture context.

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

Description	Parameter	Value
When enabled (set as Always), the eSBC always sends a P-Asserted-Identity header in the outbound INVITE message	Send Assert Header	Always
Specifies whether or not to use the session timer to verify the SIP session	Session Timer	Disable
Specifies whether the eSBC support 100rel (PRACK support)	100rel	Not Present
Specifies if the X-eSBC Edge -Diagnostics header is added to the outbound SIP signaling messages	eSBC Edge Diagnostics Header	Disable

Orange_SIP Profile-UDP

Actions	Screenshot
1. Go to *SIP > SIP Profiles* menu path	
2. To add a new *SIP Profile* click on the *plus icon (+).*	
3. Set the SIP Profile parameter like aside	

2.5.5 Configure Media Profile

The Media Profile defines codecs that will be used.

Media Profile list is used to remove codecs from an SDP offer and/or to modify the order or preference in the codecs list.

The *Media > Media Profiles* menu path allows you to specify the individual voice and fax compression codecs and their associated settings, for inclusion in a Media List. Different codecs provide varying levels of compression, allowing one to reduce bandwidth requirements at the expense of voice quality.

Orange BTalk/BTIP accepts the following codecs in this order or preference:
- G.722 (If used)
- G.711 A-law 20 ms
- G.729 20 ms (annexb = no).

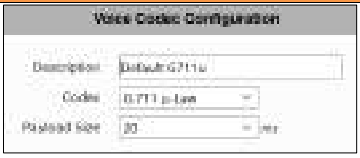
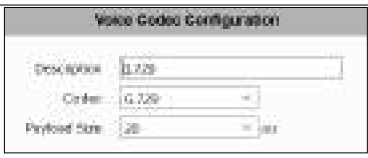
Note:
G.711 µ-law 20 ms can be requested, specifically on demand.

We are going to create a new "Voice Codec Profile" per Codec type specific to Orange BTalk.

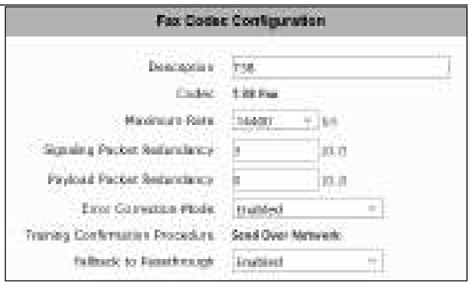
Description	Codec	Payload Size	Comments
G.722	G.722	20 ms	
Default G711A	G.711 A-Law	20 ms	
G.729	G.729	20 ms	
Default G711U	G711 U-Law	20 ms	Optional on request

Voice Codecs

Actions	Screenshot
1. Go to *Media > Media Profiles* menu path	
2. Click on the *Create Media Profile > Voice Codec Profile* icon	
3. Set G711 A codec configuration	

Actions	Screenshot
4. Repeat step 2 and set G711 U codec configuration NOTE: This codec is optional on request	
5. Repeat step 2 and set G729 codec configuration	

Fax Codec

Actions	Screenshot
1. Go to *Media > Media Profiles* menu path	
2. Click on the *Create Media Profile > Fax Codec Profile* icon	
3. Set T38 codec configuration	

Note:
For eSBC 1000 and eSBC 2000, refer to the following link to create the Fax Profile Codec.
Super G3 to G3 Fallback is applicable to fax calls in TDM-to-IP or IP-to-TDM directions. It is not applicable to TDM-to-TDM or IP-to-IP fax calls.

2.5.6 Configure Media List

The Media List defines the codecs and if the crypto mechanism will be used.

The *Media > Media List* menu path allows you to specify a set of codecs and fax profiles that are allowed on a given SIP Signaling Group. They contain one or more Media Profiles, which must first be defined in Media Profiles. These lists allow you to accommodate specific transmission requirements, and SIP devices that only implement a subset of the available voice codecs.

Transport tag must be configured to be compliant with Orange BTalk/BTIP specifications:

- ✓ Transport tag require EF (DSCP 46) for Media and Signaling
- ✓ RTCP must be activated.
- ✓ Silence suppression is not supported and must be deactivated.
- ✓ DTMF via RFC 2833/4733

Note:
For DTMF, the Ribbon eSBC will be able to convert SIP INFO message to RFC2833/4733. On SWE Lite, the License with partial RTP media manipulation is required.

The eSBC supports the RFC 6086 'Session Initiation Protocol (SIP) INFO Method and Package Framework' so it can handle SIP INFO messages carrying DTMF.

Media Lists in case of multiple codecs into SDP Audio m line (Optional):

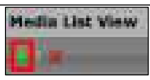
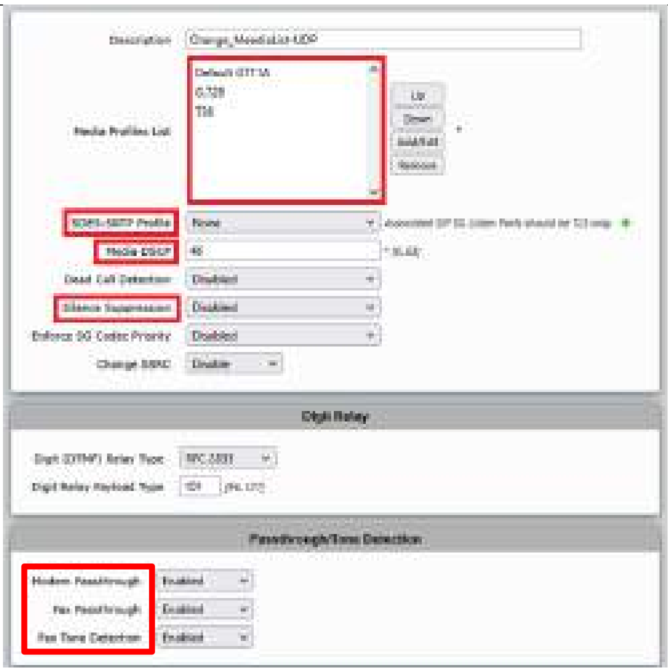
Even if this not the standard behaviors, some customer IPBX/device could send several "codec" in the SDP answer (SDP with multiple codecs into Audio M Lines). This behavior is not supported by Orange BTIP-BTalk network. As solution on the Ribbon eSBC, it is required to implement a different "Media List" to filter the answers. This will force all calls to the selected a unique "G711 A-law" codec (or on demand specific *G.711 µ-law)* .

We are going to create a new "Media list" specific to Orange BTalk.

Description	Media Profile List	SDES-SRTP profile	Media DSCP
Orange_MediaList-UDP	Default G711A, G.729, T38	None	46

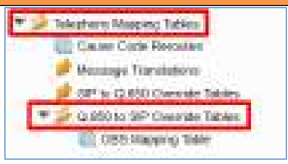
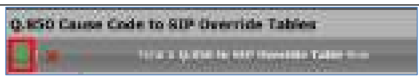
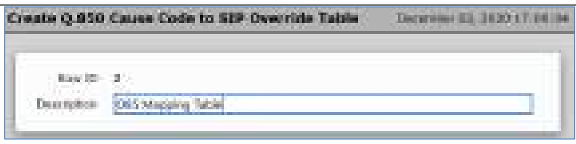
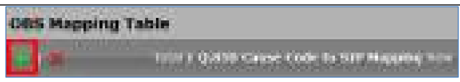
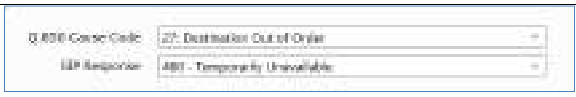
Description	DTMF Relay type	Digit Relay Payload Type
Orange_MediaList-UDP	RFC 2833	101

Orange Business UDP Media List (Orange_MediaList-UDP)

Actions	Screenshot
1. Go to Media > Media List menu path	
2. To add a new *Media List,* click on the *plus icon (+).*	
3. Set Media List configuration	

2.5.7 Q.850 to SIP Override Table

SIP and ISDN use different response messages to communicate why a call failed or could not be connected (Q.850 for ISDN and SIP Responses for SIP). By default, the eSBC Edge uses RFC 4497 to map these to each other. The *Telephony Mapping Tables > Q.850 to SIP Override Tables* menu path allows you to override one or more of these mappings to a different message, which is useful for interoperating with nonstandard equipment.

Actions	Screenshot
1. Go to Telephony Mapping Tables > Q.850 to SIP Override Tables menu path	
2. To add a new *Q.850 to SIP Override Table,* click on the *plus icon (+).*	
3. Set the *Description*	
4. On the left menu path, click on the *Q.850 to SIP Override Table* you have just created	
5. Click on the *plus icon (+).* To add a new entry	
6. Configure the new entry as per the right picture	

2.5.8 Configure Media System Port range

The Media System Configuration allows range media defined on eSBC depending on traffic.

Port Pairs Considerations:

For SWe Lite Release 7.0 and later only: The number of RTP Port Pairs must be configured slightly larger than the actual number of ports required to support the projected number of calls. We recommend you over-allocate the number of port pairs by approximately 25 - 30% above the number of calls you want to support.

eSBC Reserved Ports – Example :

Projected number of calls	Approximate number of Port Pairs	Applies To
2000 sessions	5000	Audio calls only *

* Multiple audio and video stream proxy calls will require twice the number of RTP port pairs with the examples provided above.

Note: The minimum and maximum port numbers supported by the eSBC SWe Lite are 16384, 32767, respectively. The maximum number of port pairs supported by the eSBC SWe Lite is 5000.

The minimum and maximum port numbers supported by the eSBC Edge (1K/2K) are 1024, 32767, respectively.
The maximum number of port pairs supported by the eSBC Edge (1K/2K) is 4800.

To determine the last corresponding port number fllow ewample for SWe Lite Example :
Given: For starting port number (16384) and the number for port pairs is 5000.
There are 5000 pairs, meaning there are 10000 individual ports. 16384 + (10000-1) = 26383

Paraemeter	Value
Start Port	16384
Number of Port Pairs	5000

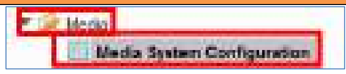
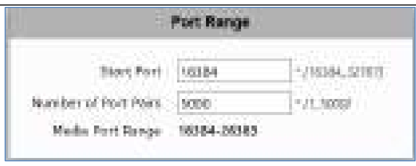
Commenté [CSS3]: please adapt wording in yellow in your example above and eSBC Ribbon Edge context.

Commenté [GA4R3]: It was already done. The wording in yellow was taken from the Ribbon Wiki page so it is OK to keep it with no changes. The example was already done; please check the numbers, they match with the screenshots.

Commenté [CSS5R3]:

Commenté [GA6R3]: I do not see any issue with this text, could you be more specific?

Commenté [DM7R3]:

Actions	Screenshot
1. Go to Media > Media System Configuration menu path	
2. Set the Media System Configuration	

2.5.9 Configure SIP Server Tables

SIP server tables allow you to define the information for the SIP interfaces connected to the Ribbon eSBC.

The *SIP > SIP Server Tables* menu path allows you to create or modify SIP servers and their parameters.

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

SIP Server will be configured to be compliant with Orange BTalk/BTIP 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

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

Orange Business BT/BTIP

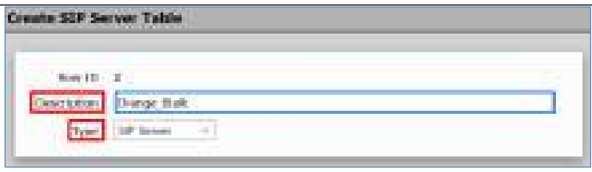
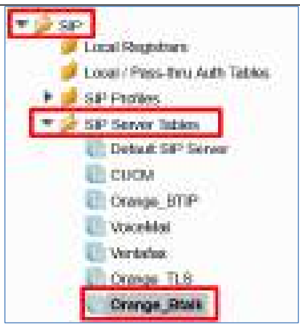
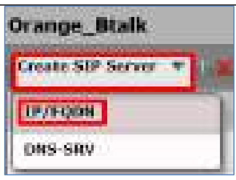
Priority	Host IP	Port	Protocol	Transport
1	<BT_Nominal_IP> or <BTIP_Nominal_IP>	5060	UDP	Monitor: Sip Options Keep Alive Frequency: 300 Recovery frequency: 5
2	<BT_Backup_IP> or <BTIP_Backupl_IP>	5060	UDP	Monitor: Sip Options Keep Alive Frequency: 300 Recovery frequency: 5

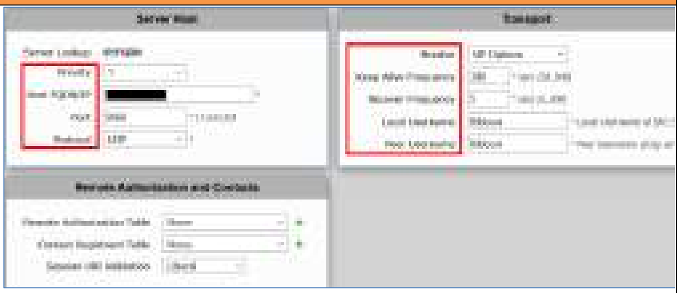
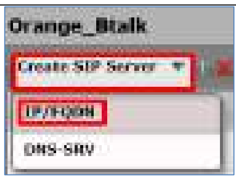
Commenté [CSS8]: Replace OBS Lab IP's Sip Termination with variable like <BT_Nominal_IP>:> & < BT_Backup_IP >, color code those in Green and if you can mask those into all screenshots.

Note : <BT/BTIP_Nominal_IP> or <BT/BTIP_Backup_IP>, needed to be configured bellow, are provided by your Orange project manager contact team.

Note2:
IP's set in the "Host IP" are the one's provided by Orange for the BTalk/BTIP SIP trunk. "Options" message will be sent by the Ribbon eSBC to verify if the Orange BTalk/BTIP network is reachable.

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

Actions	Screenshot
1. Go to SIP > SIP Server Tables menu path	
2. To add a new SIP Server Table, click on the *plus icon (+).*	
3. Set the *Description* and select *SIP Server* at the *Type* dropdown menu	
4. On the left menu path, click on the *SIP Server Table* you have just created	
5. Click on the IP/FQDN icon to add a new entry	

Actions	Screenshot
6. Set the first entry as the right picture. Host FQDN/IP being the <BT_Nominal_IP> or <BTIP_Nominal_IP> values	
7. Repeat step *5* to add a new entry. Host FQDN/IP being <BT_Backup_IP> or <BTIP_Backup_IP> values	
8. Set the second entry (backup) as the right picture	

2.5.10 SIP Message Manipulation

For unencrypted or encrypted BTalk/BTIP SIP Trunk architecture, it is required to implement some Message Manipulation for the outgoing message toward Orange BTalk/BTIP. Those Manipulations Rules are detailed on the chapter SIP Messages Manipulations . Please jump to this Chapter directly.

2.5.11 Configure Signaling Group

Signaling groups allow telephony channels to be grouped together for the purposes of routing and shared configuration. They are the entity to which calls are routed, as well as the location from which Call Routes are selected. They are also the location from which Tone Tables and Action Sets are selected.

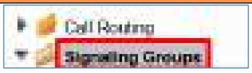
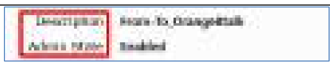
The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

Description	Call Routing Table	SIP Profile	SIP Server Table	Media List ID	Federated IP
From-To_OrangeBtalk	To_IPPBX	Orange_SIPProfile-UDP	Orange_Btalk	Orange_MediaList-UDP	<BT_Nominal_IP> <BT_Backup_IP> Or <BTIP_Nominal_IP> <BTIP_Backup_IP>

Description	Signaling DSCP	Inbound Message Manipulation	Outbound Message Manipulation
From-To_OrangeBtalk	46	N/A	Orange Business_SIP_ Profile_Adaptation_02 Orange Business_SIP_ Profile_Adaptation_01 Add_P-Early-Media

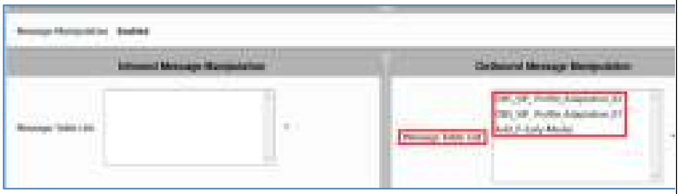
Note:
'Call Routing Tables' will be defined in the next section *2.5.12 Configure Voice routing*. Therefore, we will use the default Route Table to define the Signaling Groups; this parameter will be modified in the next section.

From-To_OrangeBTalk/BTIP

Actions	Screenshot
1. On the left menu go to the *Signaling Groups* menu path	
2. To add a new *SIP Signaling Group,* click on the *Add SIP Signaling Group icon.*	
3. Configure the new *Signaling Group* as per right picture.	
4. Remember to use the *Default Route Table* in the *Call Routing Table* field, this parameter will be modified once the correct table is defined.	

Actions	Screenshot
	

Actions	Screenshot
	
5. In the Signaling/Media Source IP field select the IP interface as per your network design. In the Federated IP/FQDN field set depending of the offer concerned, the <BT_Nominal_IP> or <BTIP_Nominal_IP> and the <BT_Backup_IP> or <BTIP_Backup_IP> Values.	

6. In the *Message Manipulation* field select *Enabled* to configure the *Message Manipulations rules* used by this *Signaling Group.* Refer to the section 2.7.3. In the *Outbound Message Manipulation* section select the Message Manipulations Rules associated with this Signaling Group	

2.5.12 Configure Voice routing

Call Routing Table allows calls to be carried between Signaling Groups, thus allowing calls to be carried between ports, and between protocols (like ISDN to SIP). Routes are defined into the Call Routing Tables, which allow a flexible configuration to carry calls and how they are translated .

Note:

> *These tables are one of the central connection points of the eSBC, linking Transformation Tables, Message Translations, Cause Code Reroute Tables, Media Lists and the three types of Signaling Groups (ISDN, SIP and CAS). For information on the Ribbon eSBC call routing system as a whole, see Working with Telephony Routing.*

This document provides the minimum of configuration needed to route calls between the Signaling Group facing BTalk/BTIP SIP trunk and the Signaling Group facing the IPPBX. You could be invited to customize them according to your own requirements.

Configure Transformation Table

Transformation Tables facilitate the conversion of names, numbers and other fields in the SIP signaling when the eSBC is routing a call. They can, for example, convert a public PSTN number into a private extension number, or into a SIP address (URI). Every entry in a *Call Routing Table* requires a *Transformation Table*, and they are selected from there.

Orange_BTalk/BTIP Table

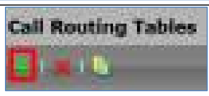
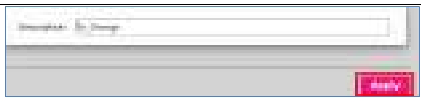
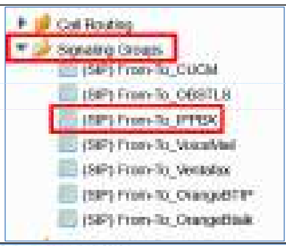
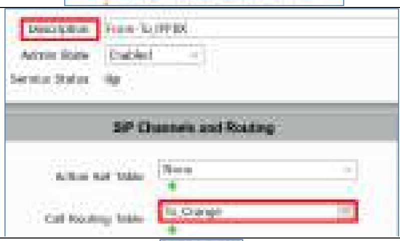
Actions	Screenshot
1. On the left menu go to the *Call Routing > Transformation* menu path	
2. To add a new Transformation Table, click on the *plus icon (+).*	
3. Set the *Description* of the new table	

Note:
Go to *Section 2.7.1* to have more information regarding how to create transformation entries.

Configure Call Routing Table

Description	Name
Call Routing Table	To_Orange
Call Routing Table	To_IPPBX

To_Orange Table

Actions	Screenshot
1. On the left menu go to the *Call Routing > Call Routing table* menu path	
2. To add a new Call Routing Table, click on the *plus icon (+).*	
3. Set the *Description* of the new table	
4. Commit the changes by clicking on the Apply icon	
5. On the left menu, go to the *From-To_IPPBX* Signaling Group ▪ Note: it is the name of the Signaling Group facing the IPPBX	
6. Edit the Signaling Group by selecting *To_Orange* in the *Call Routing Table* field.	
7. Commit the changes by clicking on the Apply icon	

Commenté [DM9]: Adrian, could you add info to configure at minimum this element.

Commenté [CSS10]: When needed, specify IPBX instead of your lan context CISCO CUCM

Commenté [CSS11R10]: Are you able to update the screenshot showing IPBX instead of Cisco ?

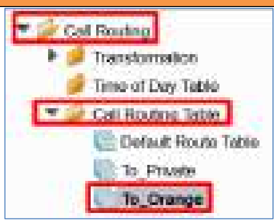
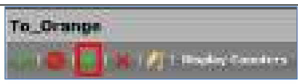
Commenté [GA12R10]: Done

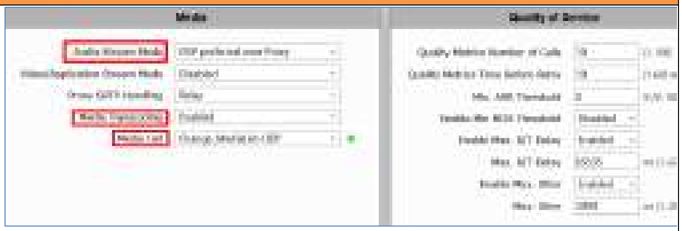
To_Orange Call Route Entries

Description	Priority	Transformation Table	Signaling Group	Destination Type
To_OrangeBtalk	1	Orange_Btalk	From-To_OrangeBtalk	Normal
To_OrangeTLS	1	Orange_TLS	From-To_Orange BusinessTLS	Normal

Note:
To_OrangeTLS will be defined in section 2.6.14 'Configuring Voice routing (TLS)'.

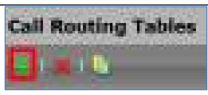
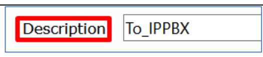
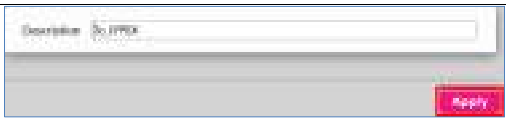
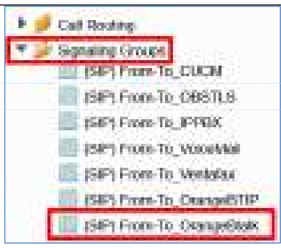
To_Orange

Actions	Screenshot
1. On the left menu path click on the *To_Orange* table you created	
2. To add a new entry, click on the *plus icon (+).*	
3. Set the new *Call Route* as per right picture. Under *Number/Name Transformation Table*, select the table 'Orange_Btalk' previously created – see above	

Actions	Screenshot
Under *Destination Information* section click on the *Add/Edit* icon to set the *Destination Signaling Groups.* It is the SignalingGroup facing Orange	

Note:
The Call Routing Table 'To_Orange' shall be used within the Signaling group facing to the IP PBX.

To_IPPBX Table

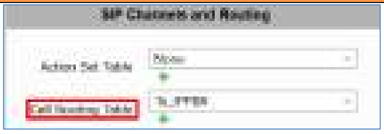
Actions	Screenshot
1. On the left menu go to the *Call Routing > Call Routing table* menu path	
2. To add a new Call Routing Table, click on the **plus** *icon (+).*	
3. Set the *Description* of the new table	
4. Commit the changes by clicking on the Apply icon	
5. On the left menu, go to the *From-To_OrangeBtalk* Signaling Group. Note: it is the name of the Signaling Group facing Orange Business	

Commenté [DM13]: Adrian, repeat here to apply the call routing table into the SG facing to BTalk

Commenté [CSS14]: When needed, specify IPBX instead of your lan context CISCO CUCM

Commenté [CSS15R14]: Are you able to update the screenshot showing IPBX instead of Cisco ?

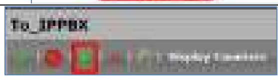
Commenté [GA16R14]: Done

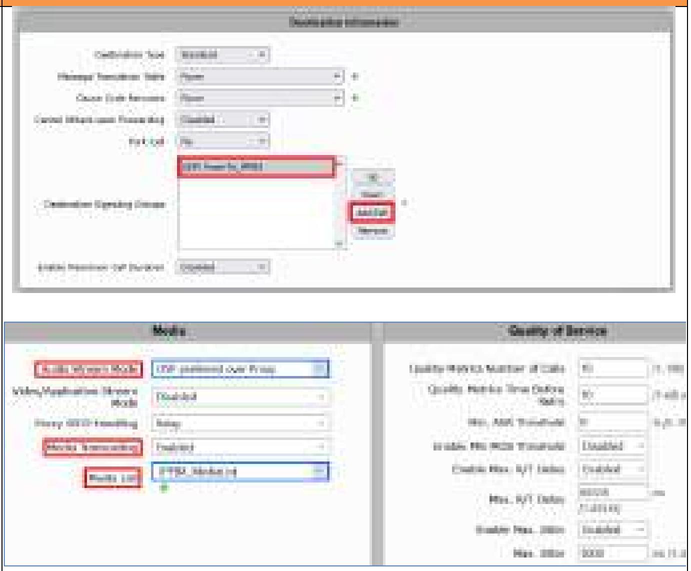
Actions	Screenshot
6. Edit the Signaling Group by selecting *To_IPPBX* in the *Call Routing Table* field.	
7. Commit the changes by clicking on the *Apply* icon	

To_IPPBX Call Route Entries

Description	Priority	Transformation Table	Signaling Group	Destination Type
To_IPPBX	1	IPPBX_Prefixes	From-To_IPPBX	Normal

To_IPPBX

Actions	Screenshot
1. On the left menu path click on the *To_IPPBX* table you created	
2. To add a new entry, click on the *plus icon (+).*	
3. Set the new *Call Route* as per right picture. Under *Number/Name Transformation Table*, select the table 'IPPBX_Prefixes' previously created – see above Under *Destination*	

Actions	Screenshot
Information section click on the *Add/Edit* icon to set the *Destination Signaling Groups.* It is the Signaling Group facing the IPPBX	

Note:
The Call Routing Table ‘To_IPPBX’ shall be used within the Signaling group facing to the Orange BTalk

2.6 Orange Business- Business Talk over Internet & BTIP over Internet Carrier North encrypted SIP configuration for Ribbon Edge eSBC (TLS)

As a prerequisite Ribbon recommends reading the [eSBC Edge Security Hardening Checklist] to understand how to secure the eSBC into your network infrastructure and especially facing Internet.

2.6.1 Configure a Certificate for the eSBC

Business Talk Over Internet & Business Talk IP Over Internet only allows TLS connections from the eSBC for SIP traffic with a certificate signed by one of the trusted public certification authorities.

To obtain this Certificate Authority (CA) you must generate your CSR base on the information of the eSBC and Company with SHA-256 encryption.

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

Common Name	Organizational Unit	Company name	Locality or city name	Country code
SBC123@COMPANY.com	Organization X	COMPANY Enterprise	Paris	FR

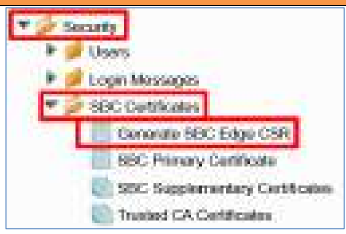
1st Subject Alternative Name	2nd Subject Alternative Name	3rd Subject Alternative Name	Signature Algorithm	Private Key size
IP 83.206.61.113	__	__	SHA-256	2048

Note : As soon you received the CA Root/Intermediate from Orange project team, you will have to load those 2 on the Ribbon eSBC on the TLS Context created for this interconnection with Orange BTALK.

Create a Service Request Certificate for the eSBC External interface and its configuration is based on the following example :

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

Note:
Customer will ensure their eSBC FQDN's must be resolved through a public DNS before generating the CSR. Customer Ribbon eSBC SIP "FQDN/Hostname" peer must be populated through "Common Name" field Orange will have to trust.

Actions	Screenshot
1. On the left menu path click on *Generate eSBC Edge CSR*	
2. Complete the information requested by the eSBC. Note: Those information's will be used to generate the Certificate Signing Request (CSR)	
3. Click on the *OK* icon	

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 Certificates (crt files) must be transmitted to Orange Business Services team.

When you get the CA files (p7b and bundle), please deploy it like bellow. Only **Base64 (PEM)** encoded X.509 certificates can be loaded to the Ribbon eSBC.

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

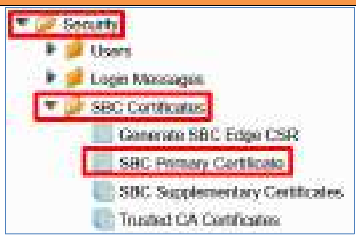
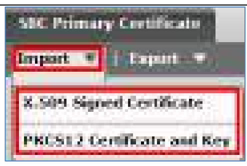
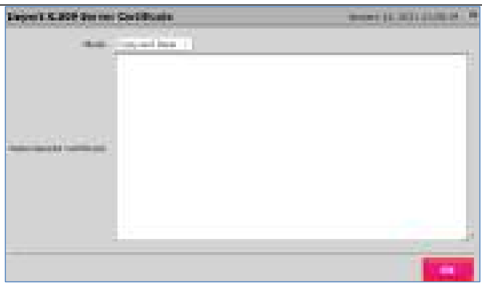
```
-----BEGIN CERTIFICATE-----
MIIDkzCCAnugAwIBAgIEAgAAADANBgkqhkiG9w0BAQQFADA/MQswCQYDVQQGEwJGUjETMBEGA1UEChMKQ2VydGlwb3N0ZTEbMBkGA1UEAxM
SQ2VydGlwb3N0ZSBTZXJ2ZXVyMB4XDTk4MDYyNDA4MDAwMFoXDTE4MDYyNDA4MDAwMFowPzELMAkGA1UEBhMCRlIxEzARBgNVBAoTCkNlcn
RpcG9zdGUxGzAZBgNVBAMTEkNlcnRpcG9zdGUgU2VydmV1cjCCASEwDQYJKoZIhvcNAQEBBQADggEOADCCAQkCggEAPqd4MziR4spWldGRx
```

8bQrhZkonWnNm`+Yhb7+4Q67ecf1janH7GcN/SXsfx7jJpreWULf7v7Cvpr4R7qIJcmdHIntmf7JPM5n6cDBv17uSW63er7NkVnMFHwK1Qa
GFLMybFkzaeGrvFm4k3lRefiXDmuOe+FhJgHYezYHf44LvPRPwhSrzi9+Aq3o8pWDguJuZDIUP1F1jMa+LPwvREXfFcUW+w==
-----END

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

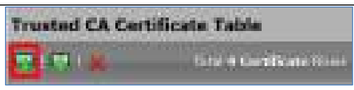
After receiving the certificate from the certification authority, install the eSBC Certificate and Root/Intermediate Certificates as follows:

eSBC Certificate

Actions	Screenshot
1. On the left menu path click on *eSBC Primary Certificate*	
2. Under the Import menu, click on the certificate format you want to use (X.509 or PKCS12)	
3. If you select X.509, a window will appear requesting the certificate. 4. Copy and paste the certificate 5. Click on the *OK* icon.	
6. If you select PKCS12, a window will appear requesting the password and the certificate file. 7. Type the password and select the certificate file.	

Actions	Screenshot
8. Click on the *OK* icon	

Customer Root / Intermediate Certificates authority:

Actions	Screenshot
1. On the left menu path click on *Trusted CA Certificates*	
2. Click on the Import Trusted CA Certificate	
3. A window will appear requesting the certificate. 4. Copy and paste the certificate 5. Click on the *OK* icon.	
6. Repeat previous steps if you want to import additional certificates	

STEP 3 : Communicate Customer Public Certificates Authorities (Root and Intermediate) information's which signed your eSBC certificate to Orange BTALK Team

Orange Root / Intermediate Certificates authority:

STEP 4: Import Orange Certificates Authorities (Root and Intermediate described in BTIP/BT Stas) like done for the Customer Root / Intermediate Certificates authority

2.6.2 Configure TLS Profile

The TLS profile defines the crypto parameters for the SIP protocol.

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 be created.

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

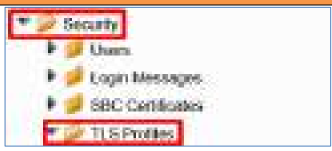
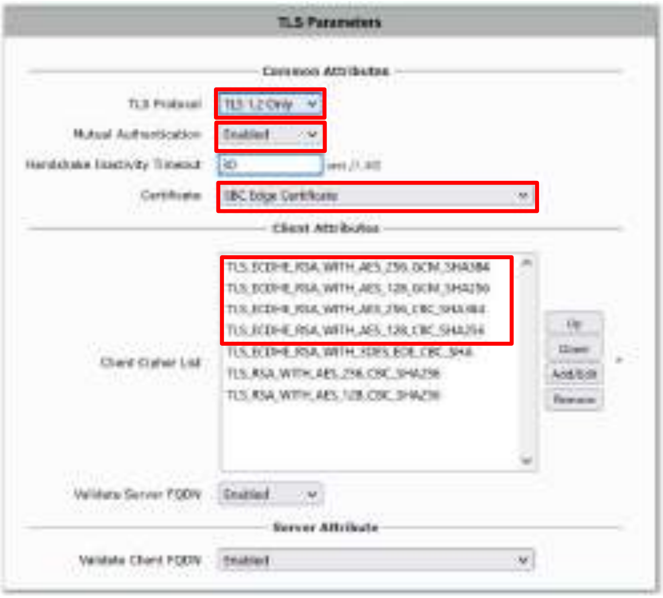
- ✓ For encrypted BTALK/BTIP SIP Trunk architecture we need to configure most secure TLS V1.3 (Recommended) or TLS V1.2 (Compatible depending of SBC major version used)
- ✓ Key size 2048
- ✓ Cipher list per below is recommended as Cipher Client/Server through TLS V1.3:
  - o TLS_AES_256_GCM_SHA384 (Recommended)
  - o TLS_AES_128_GCM_SHA256
  - o TLS_CHACHA20_POLY1305_SHA256
- ✓ Cipher list per below is compatible as Cipher Client/Server through TLS V1.2:
  - o TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (Compatible)
  - o TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - o TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  - o TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- ✓ TLS Mutual authentication activated.

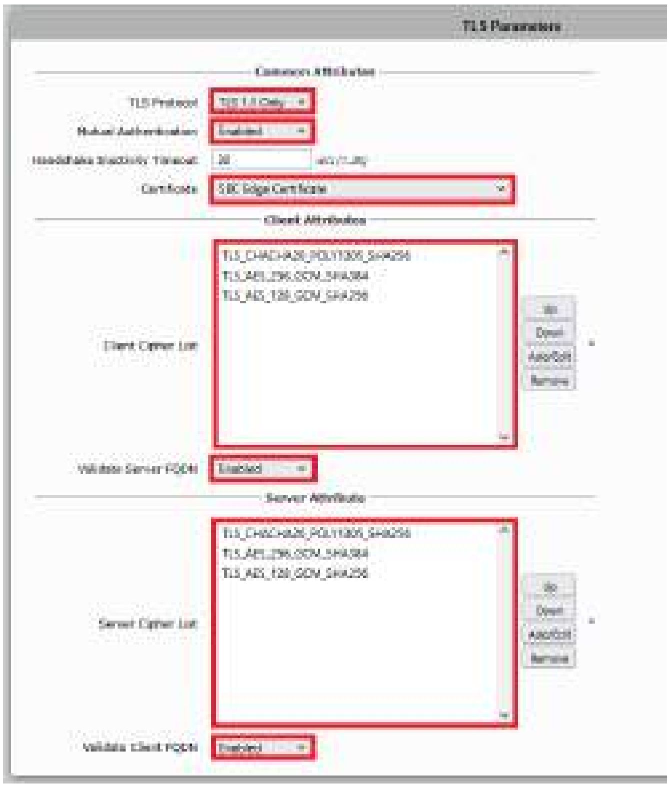
The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

Parameter	Value for V11	Value for V12
TLS Profile	TLS Orange	
TLS protocol	TLS 1.2 Only	TLS 1.3 Only
Mutual Authentication	Enabled	
Client Cipher	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384
Validate Server FQDN	Enabled *	
Client Certificate	<eSBC Edge Certificate>	
Validate Client FQDN	Enabled (highly recommended to make a reverse DNS lookup of Orange peer FQDN's in order to verify the identity of the Orange SIP peer client certificate.)	
Server Certificate	<eSBC Edge Certificate>	

Note:
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 is the highest cipher suite supported on Ribbon eSBC through TLS V1.2.
TLS_AES_256_GCM_SHA384 is the highest cipher suite supported on Ribbon eSBC through TLS V1.3

* SBC Edge Portfolio does not validate IP addresses to identify a peer server, but only Fully Qualified Domain Names (FQDN). Make sure “Validate Server FQDN” parameter is set to Disabled if the Orange peer server if you using an Orange BToI public IP’s address instead of our FQDN’s. (Source : https://publicdoc.rbbn.com/spaces/UXDOC123/pages/495978734/Creating+and+Modifying+TLS+Profiles)

Actions	Screenshot
1. On the left menu path click on *TLS Profiles*	
2. Click on the Create TLS Profile Icon	
3. Set the configuration as per right picture. Caution: Do not change the client & Server cipher suites order.	 V11 (TLS V1.2) 

Actions	Screenshot
	V12 (TLS V1.3): 
4. Click on the *Apply* icon	

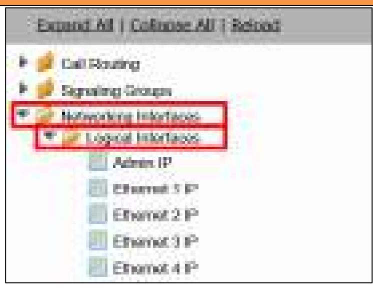
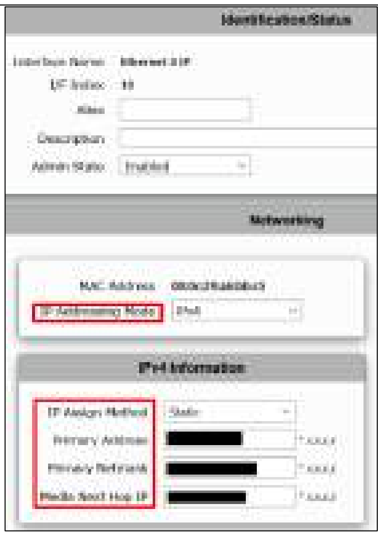
2.6.3 Configure Node Interface

No configuration is required in this section. Existing Node Interface could be used.

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

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

The *Networking Interfaces > Logical Interfaces* menu path allows you to configure the IP addresses (both IPv4 and IPv6) for the Ethernet ports and VLANs.

Actions	Screenshot
1. Go to *Networking Interfaces > Logical Interfaces* menu path	
2. Click on the *Ethernet interface* you want to configure and set the Public IP/ Netmask informations.	
3. Click on the *Apply* icon	

Actions	Screenshot
4. Repeat steps 2 and 3 in case you want to configure additional *Ethernet interfaces* as per your network topology	

Note:
The Media Next Hop IP field (available on SWe Lite only) must be configured with the Default Gateway for this interface.

2.6.4 Message size limit

Orange BTALK specifications require to limit the size of the SIP message to 4096 Bytes and SDP Body to 1024 Bytes. To do so,

Ribbon eSBC Edge (SBC1000, SBC2000 and SWe Lite) do not limit the size of SIP/SDP at the application level (sip stack), the packet size is limited by the socket's default size value set by OS

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

Actions	Screenshot
No action	Set as by design

2.6.5 Configure SIP Profile

The SIP Profile enables configuration for parameters, such as SIP Header customization, option tags, etc.

Sip Profile must be configured to be compliant with Orange BTalk:BTIP specification:

- ✓ Transfer allowed via Re-invite
- ✓ Session Timer is not supported
- ✓ DTMF via RFC 2833/4733

Note:
For **Transfer**, the Ribbon eSBC will be able to **convert REFER** into RE-INVITE.
In some case SIP Provisional Response ACKnowledgement (PRACK RFC 3262))
could be required (such as for Cisco CUCM) to be interworked with Orange which not support PRACK. eSBC device can be configured to resolve this interoperable issue and enable sessions between such endpoints. SIP PRACK handling is configured using the SIP Profile parameter, eSBC PRACK Mode: Mandatory on the SIP profile of the Customer IPPBX.

When **Blind and Consultative transfer** are handled by the **SIP REFER** method, the eSBC will generate a new INVITE towards the transfer target. The eSBC does not proxy or send SIP REFER to the transferee. In short, the eSBC handles the REFER message and sends an INVITE to the new target.

The eSBC supports **PRACK** messages facing private South Side, the flag 100rel at the SIP profile supports this feature.

The History-Info header to Diversion header conversion is done automatically in order to be compliant with Orange specification.

All of those conversions will stay under customer responsibilities depending on the South private architecture context.

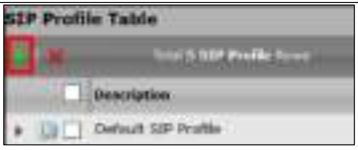
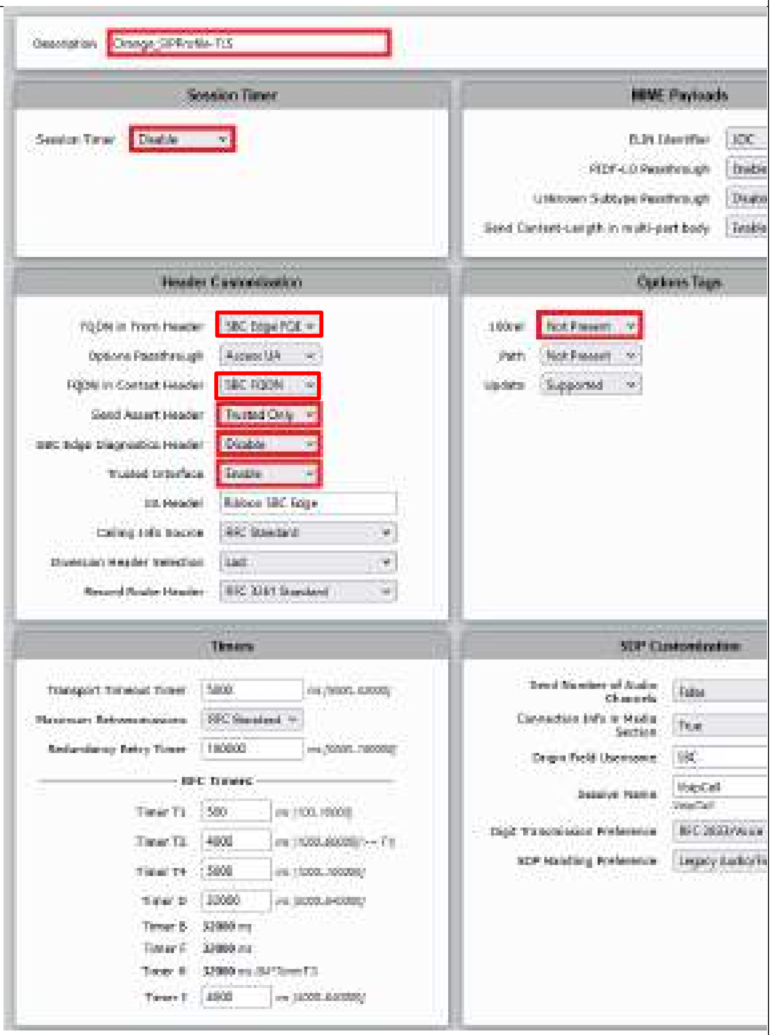
The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

Description	Parameter	Value
When enabled (set as Always), the eSBC always sends a P-Asserted-Identity header in the outbound INVITE message	Send Assert Header	Trusted Only
Specifies whether or not to use the session timer to verify the SIP session	Session Timer	Disable
Specifies whether the eSBC support 100rel (PRACK support)	100rel	Not Present
Specifies if the X-eSBC Edge -Diagnostics header is added to the outbound SIP signaling messages	eSBC Edge Diagnostics Header	Disable

Commenté [DM17]: @Adrian, this value is not correct as you select below 'Trusted Only'. To correct here

Orange_SIP Profile-TLS

Actions	Screenshot
1. Go to *SIP > SIP Profiles* menu path	

<table>
<tr><td>2.</td><td>To add a new SIP Profile click on the plus icon (+).</td><td>
</td></tr>
<tr><td>3.</td><td>Set the SIP Profile parameters as per right picture</td><td>
</td></tr>
</table>

2.6.6 Configure Media SDES-SRTP Profile

This section allows to Enable the media security protocol (SRTP). This is needed in the case where the media connections with BTALK are using encrypted connections 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».

Description	Parameter	Value
Profile name	Description	Orange Business_SRTP
Specifies the way encryption is supported in the profile.	Operation Option	Required
Specifies the crypto suite that the Ribbon uses to negotiate with a peer device.	Crypto Suite	AES_CM_128_HMAC_SHA1_80

Actions	Screenshot
1. Go to *media > SDES-SRTP Profiles* menu path	
2. To add a new *Profile,* click on the *plus icon (+).*	
3. Set the Profile parameters as per right picture	

2.6.7 Configure Media Profile

The Media Profile defines codecs that will be used

Media Profile list is used to remove codecs from an SDP offer and/or to modify the order or preference in the codecs list.

Orange accepts the following codecs in this order or preference:

- G.711 A-law 20 ms

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

Commenté [CSS18]: Update the Note accordingly including G722, only *G.711 µ-law 20 ms* can be requested spefically.

Commenté [DM19R18]: Done

Refer to section 2.5.5 Configure Media Profile to get further information.

Please note a known issue is still there for T38 over TLS : eSBC Edge currently doesn't support Fax T.38 UDP conversion to FAX T.38 TLS. It will be fixed by Ribbon within a future release.

2.6.8 Configure Media List

The Media List defines the codecs and if the crypto mechanism will be used.

Transport tag must be configured to be compliant with Orange BTalk/BTIP specifications:

- ✓ Transport tag require EF (DSCP 46) for Media and Signaling
- ✓ RTCP must be activated
- ✓ Silence suppression is not supported and must be deactivated
- ✓ DTMF via RFC 2833/4733
- ✓ SRTP SDES encryption

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

Note2: The eSBC supports the RFC 6086 'Session Initiation Protocol (SIP) INFO Method and Package Framework' so it can handle SIP INFO messages carrying DTMF.

Note3: *Media List* lists all codecs into the SDP Audio MLine (Optional):

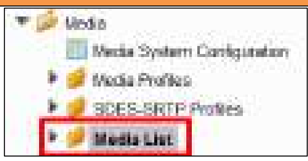
Even if this not the standard behaviors, some customer IPBX/device could send several "codec" in the SDP answer (SDP with multiple codecs into Audio M Lines). This behavior is not supported by Orange BTalk network. As solution on the Ribbon eSBC, it is required to implement a different "Media List" to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

We are going to create a new “Media list” specific to Orange BTalk/BTIP.

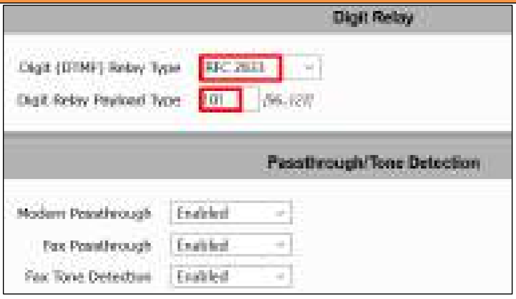
Description	Media Profile List	SDES-SRTP profile	Media DSCP
Orange_MediaList-TLS	Default G711A, T38	Orange Business_SRTP	46

Description	DTMF Relay type	Digit Relay Payload Type
Orange_MediaList-TLS	RFC 2833	101

Orange Business TLS Media List (Orange_MediaList-TLS)

Actions	Screenshot
1. Go to Media > Med_SRTPia List menu path	
2. To add a new *Media List,* click on the *plus icon (+).*	
3. Set Media List configuration	

Commenté [CSS20]: Please delete G729
Commenté [DM21R20]: I keep T38 . correct ?

Actions	Screenshot
	

2.6.9 Q.850 to SIP Override Table

Refer to section 2.5.7 Q.850 to SIP Override Table to get further information.

2.6.10 Configure Media System Port range

Refer to section 4.3.8 Configure Media System Port range to get further information.

2.6.11 Configure SIP Server Tables

SIP server table defines the information of the SIP interfaces of the remote SIP Servers which the eSBC is connected with.

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

The *SIP Server 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/BTIP.

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

- ✓ For encrypted BTalk/BTIP over Internet 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».

Orange BTIP TLS

Priority	Host FQDN	Port	Protocol	TLS Profile	Transport
1	<BTIP_Public FQDN_Nominal >	TCP 5061	TLS	Orange_TLS_Profile	Monitor: Sip Options Keep Alive Frequency: 300 Recovery frequency: 5
2	< BTIP-Public_FQDN_Backup >	TCP 5061	TLS	Orange_TLS_Profile	Monitor: Sip Options Keep Alive Frequency: 300 Recovery frequency: 5

Note:

FQDNs set in the "Host FQDN" are the one's provided by Orange for the SIP trunk BTalk. "Options" message will be sent by the Ribbon eSBC to verify if the Orange BTalk network is reachable.

DNS Servers must be configured in System> Node-Level Settings section.

Note2:

All the screenshots below showing some FQDN's are given as example. You should replace them by the correct FQDN provided.

Orange BT TLS

Priority	Host FQDN	Port	Protocol	TLS Profile	Transport
1	<BT_Public IP_Nominal_or BT_Public FQDN_Nominal >	5061	TLS	Orange_TLS_Profile	Monitor: Sip Options Keep Alive Frequency: 300 Recovery frequency: 5
2	< BT-Public_IP_Backup_or BT_Public FQDN_Backup >	5061	TLS	Orange_TLS_Profile	Monitor: Sip Options Keep Alive Frequency: 300 Recovery frequency: 5

Note : Refer to the 'Business Talk IP over Internet prerequisites STAS' and "Business Talk STAS" documents provided by your Orange sales or project manager contact teams for more details about BT_Public IP's/ Public FQDN's type A and BTIP_Public_FQDN's type A nominal & Backup or our SRV Record (For Signalization) needed to be configured bellow.

Commenté [CSS22]: Please replace <OBS_FQDN> by *<BT_Public FQDN_Nominal>* and add a line for the backup <BT-Public_FQDN_FQDN_Backup>, only FQDN must be configured, no pubic IP's

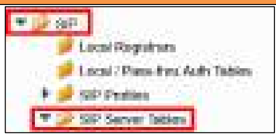
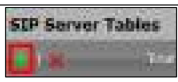
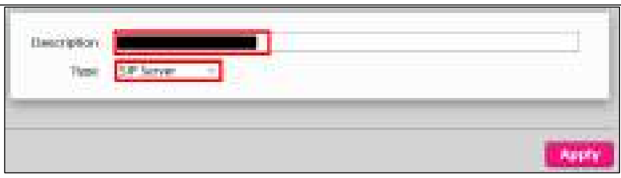
Commenté [CSS23]: Please replace <OBS_FQDN> by *<BT_Public FQDN_Nominal>* and add a line for the backup <BT-Public_FQDN_FQDN_Backup>, only FQDN must be configured, no pubic IP's

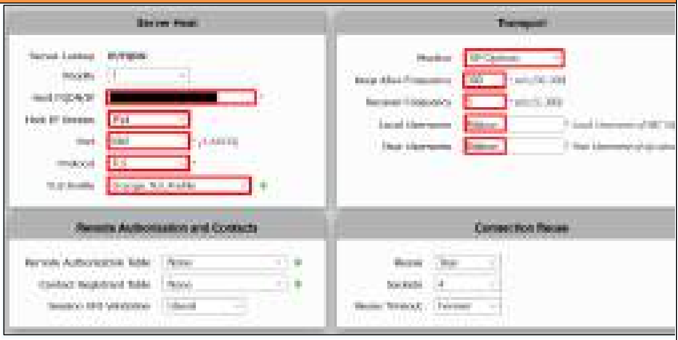
Commenté [CSS24]: Please complete where to configure public DNS relay

Commenté [DM25R24]: Sentence completed

Commenté [CSS26]: Please replace <OBS_FQDN> by *<BT_Public FQDN_Nominal>* and add a line for the backup <BT-Public_FQDN_FQDN_Backup>, only FQDN must be configured, no pubic IP's

Commenté [CSS27]: Please replace <OBS_FQDN> by *<BT_Public FQDN_Nominal>* and add a line for the backup <BT-Public_FQDN_FQDN_Backup>, only FQDN must be configured, no pubic IP's

Actions	Screenshot
1. On the left menu, go to SIP > *SIP Server Tables*	
2. To add a new entry, click on the *plus icon (+)*	
3. Set *Description* and select *SIP Server* on the *Type* field 4. Click on the *Apply* icon **Note:** The Description is hidden as it is the public Orange Business FQDN/ IP	
5. On the left menu path, click on the *SIP Server Table* you have just created **Note:** The table name is hidden as it is the public Orange Business FQDN/ IP	
6. Click on the IP/FQDN icon to add a new entry **Note:** The table name is hidden as it is the public Orange Business FQDN	

Actions	Screenshot
7. Set the new entry as the right picture. Host FQDN/IP being the < BTIP_Public FQDN_Nominal> or < BT_Public IP_Nominal> **Note:** The *Host FQDN/IP* is hidden as it is the public Orange Business IP/FQDN	
8. Repeat step *6* and *7* to add a new entry. Host FQDN/IP being <BTIP-Public_FQDN_Backup> or <BT-Public_IP_Backup by setting Priority to 2.	

Commenté [CSS28]: Add a line to repeat the configuration for the BT Backup FQDN and specify the redundancy (set priority) like in § 2.5.9

2.6.12 SIP Message Manipulation

For unencrypted and encrypted Orange BTalk/BTIP SIP Trunk architecture, it is required to implement some Message Manipulations for the outgoing messages toward Orange BTalk/BTIP.

Those *Manipulations Rules* are detailed on the chapter SIP rules & manipulations (eSBC Application). Please jump to this Chapter directly.

2.6.13 Configure Signaling Group

Signaling Groups allow telephony channels to be grouped together for the purposes of routing and shared configuration. They are the entity to which calls are routed, as well as the location from which Call Routes are selected. They are also the location from which Tone Tables and Action Sets are selected.

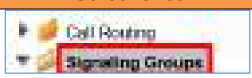
The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

Description	Call Routing Table	SIP Profile	SIP Server Table	Media List ID	Federated IP/FQDN
From-To_Orange BusinessTLS	To_IPPBX	Orange_SIP Profile-TLS	Orange_BTalk _TLS	Orange _Media List-TLS	< BTIP_Public FQDN_Nominal> or < BT_Public IP_Nominal> <BTIP-Public_FQDN_Backup> or <BT-Public_IP_Backup

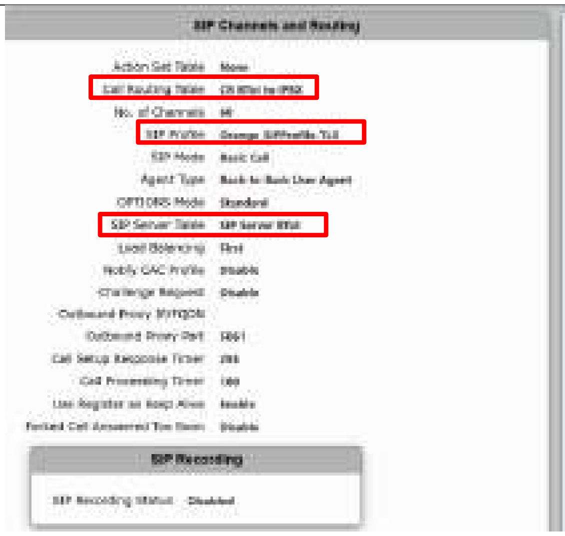
Description	Proxy Local SRTP Crypto Profile ID	Signaling DSCP	Inbound Message Manipulation	Outbound Message Manipulation
From-To_Orange BusinessTLS	Orange Business_SRTP	46	N/A	Orange Business_SIP_ Profile_Adaptation_02
				Orange Business_SIP_ Profile_Adaptation_01
				Add_P-Early-Media

Note:
'Call Routing Tables' will be defined in the next section '*Configure Voice routing*' . Therefore, we will use the default Route Table to define the Signaling Groups; this parameter will be modified in the next section.

From-To_Orange BusinessTLS

Actions	Screenshot
1. On the left menu go to the *Signaling Groups* menu path	

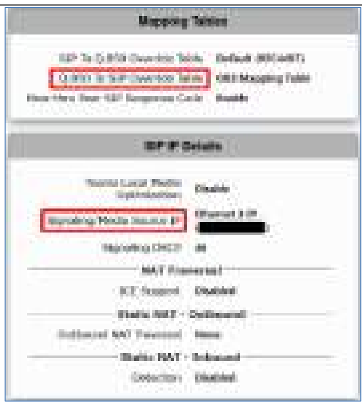
Actions	Screenshot
2. To add a new *SIP Signaling Group*, click on the *Add SIP SG* icon.	
3. Configure the new *Signaling Group* as per right picture.	

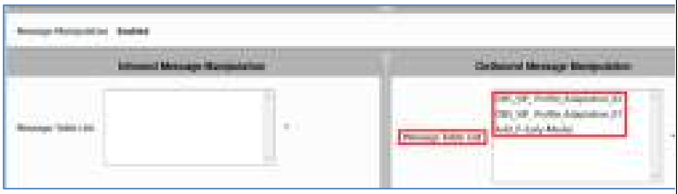
4. Remember to use the *Default Route Table* in the *Call Routing Table* field, this parameter will be modified once the correct table is defined. Select the *SIP Server Table* previously created in section 2.6.11 In the *Signaling/Media Source IP* field. Select the IP interface as per your network design. In the *Federated IP/FQDN's* field set, depending of the offer concerned, the Nominal SIP Server *<BT_Public IP_Nominal>* Or <BTIP_Public_FQDN> And the Backup SIP Server <BT_Public_IP_Backup> Or *<BTIP-Public_FQDN_Backup>*	

Commenté [CSS29]: Please replace <OBS_FQDN> by *<BT_Public FQDN_Nominal>* and add a line for the backup <BT-Public_FQDN_FQDN_Backup>, only FQDN must be configured, no pubic IP's
Add screenshot including both

Media Information
Supported Audio Modes
DSP
Proxy
Direct
Proxy with Local SRTP
Supported Video/ Application Modes
Proxy
Direct
Media List ID
Orange MediaList-TLS
Proxy Local SRTP Crypto Profile ID
OBS SRTP
Play Ringback
Auto on 180
Tone Table
Default Tone Table
Play Congestion Tone
Disable
Early 183
Disable
Allow Refresh SDP
Enable
Music on Hold
Disabled
RTCP Multiplexing
Disable
Media Codec Latch
Enable

5. In the *Message Manipulation* field select *Enabled* to configure the *Message Manipulations rules* used by this *Signaling Group.* Refer to the section 2.7.3. In the *Outbound Message Manipulation* section select the Message Manipulations Rules associated with this Signaling Group	

2.6.14 Configure Voice routing

Call Routing Table allows calls to be carried between Signaling Groups, thus allowing calls to be carried between ports, and between protocols (like ISDN to SIP). Routes are defined into the Call Routing Tables, which allow a flexible configuration to carry calls and how they are translated .

Note :

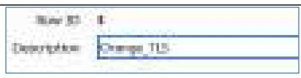
These tables are one of the central connection points of the eSBC, linking Transformation Tables, Message Translations, Cause Code Reroute Tables, Media Lists and the three types of Signaling Groups (ISDN, SIP and CAS). For information on the Ribbon eSBC call routing system as a whole, see Working with Telephony Routing.

This document provides the minimum of configuration needed to route calls between the Signaling Group facing BTalk SIP trunk and the Signaling Group facing the IPPBX. You could be invited to customize them according to your own requirements.

Configure Transformation Table

Transformation Tables facilitate the conversion of names, numbers and other fields in the SIP signaling when the eSBC is routing a call. They can, for example, convert a public PSTN number into a private extension number, or into a SIP address (URI). Every entry in a *Call Routing Table* requires a *Transformation Table*, and they are selected from there.

Orange_TLS Table

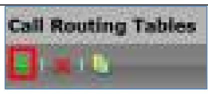
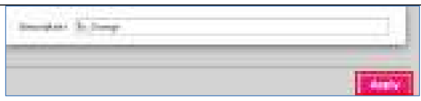
Actions	Screenshot
1. On the left menu go to the *Call Routing > Transformation* menu path	
2. To add a new Transformation Table, click on the *plus icon (+).*	
3. Set the *Description* of the new table	

Note:
Go to *Section 2.7.1* to have more information regarding how to create transformation entries.

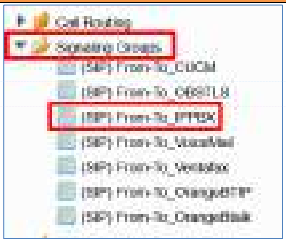
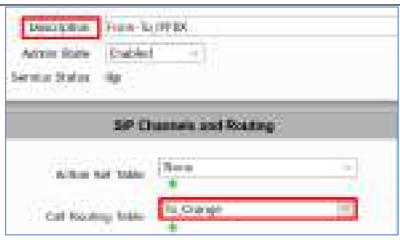
Configure Call Routing Table

Description	Name
Call Routing Table	To_Orange
Call Routing Table	To_IPPBX

To_Orange Table

Actions	Screenshot
1. On the left menu go to the *Call Routing > Call Routing table* menu path	
2. To add a new Call Routing Table, click on the *plus icon (+).*	
3. Set the *Description* of the new table	
4. Commit the changes by clicking on the Apply icon	

Commenté [DM30]: Adrian, could you add info to configure at minimum this element.

Actions	Screenshot
5. On the left menu, go to the *From-To_IPPBX* Signaling Group Note: it is the name of the Signaling Group facing the IPPBX	
6. Edit the Signaling Group by selecting *To_Orange* in the *Call Routing Table* field.	
7. Commit the changes by clicking on the Apply icon	

To_Orange Call Route Entries

Description	Priority	Transformation Table	Signaling Group	Destination Type
To_OrangeBtalk	1	Orange_Btalk	From-To_OrangeBtalk	Normal
To_OrangeTLS	1	Orange_TLS	From-To_Orange BusinessTLS	Normal

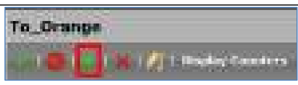
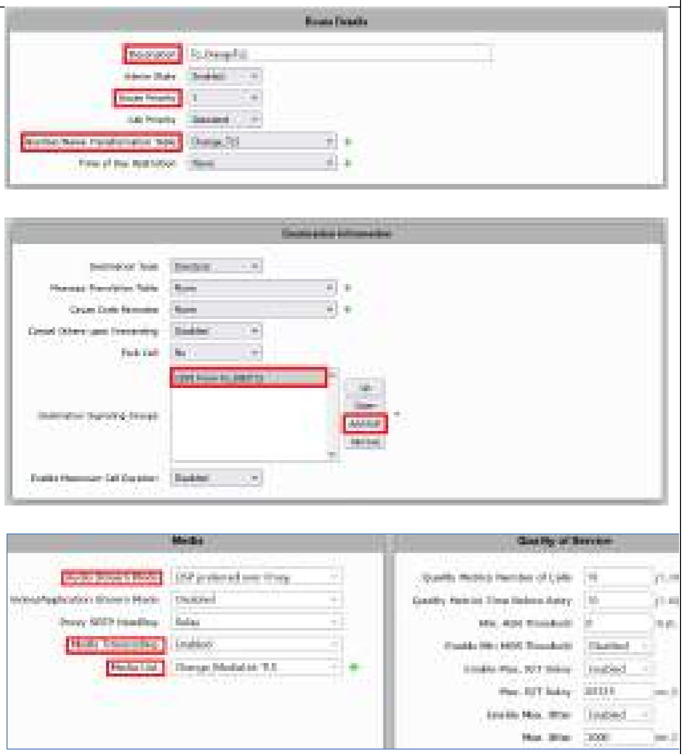
Note:
'To_OrangeBtalk' was defined in section 2.5.12 'Configure Voice routing (UDP)'.

Commenté [CSS31]: When needed, specify IPBX instead of your lan context CISCO CUCM

Commenté [CSS32R31]: Are you able to update the screenshot showing IPBX instead of Cisco ?

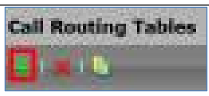
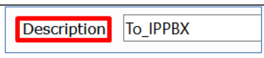
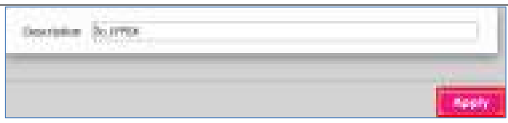
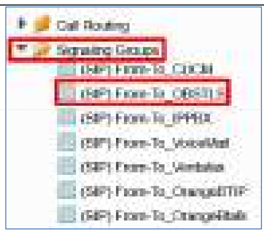
Commenté [GA33R31]: Done

<u>*To_OrangeTLS*</u>

Actions	Screenshot
1. On the left menu path click on the *To_Orange* table you created	
2. To add a new entry, click on the *plus icon (+).*	
3. Set the new *Call Route* as per right picture. ▪ Under *Number/Name Transformation Table*, select the table 'Orange_TLS' previously created – see above ▪ Under *Destination Information* section click on the *Add/Edit* icon to set the *Destination Signaling Groups.* It is the Signaling Group facing Orange TLS	

<u>Note</u>:
The Call Routing Table 'To_Orange' shall be used within the Signaling group facing to the IP PBX.

To_IPPBX Table

Actions	Screenshot
1. On the left menu go to the *Call Routing > Call Routing table* menu path	
2. To add a new Call Routing Table, click on the *plus icon (+).*	
3. Set the *Description* of the new table	
4. Commit the changes by clicking on the Apply icon	
5. On the left menu, go to the '*From-To_Orange BusinessTLS*' Signaling Group. ▪ Note: This is the name of the Signaling Group facing Orange Business TLS	
6. Edit the Signaling Group by selecting '*To_IPPBX*' in the *Call Routing Table* field.	
7. Commit the changes by clicking on the *Apply* icon	

Note:
The Call Routing Table 'To_IPPBX' shall be used within the Signaling group facing to the Orange BTalk Trunk.

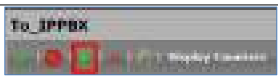
Commenté [DM34]: Adrian, repeat here to apply the call routing table into the SG facing to BTalk

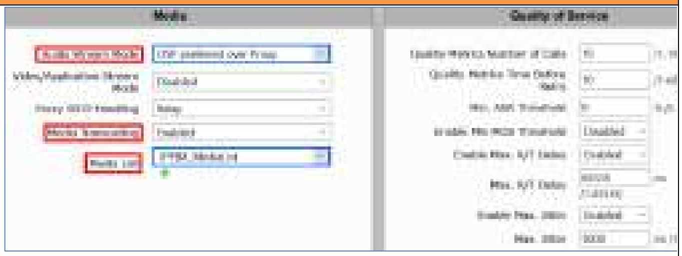
Commenté [CSS35]: When needed, specify IPBX instead of your lan context CISCO CUCM

To_IPPBX Call Route Entries

Description	Priority	Transformation Table	Signaling Group	Destination Type
To_IPPBX	1	IPPBX_Prefixes	From-To_IPPBX	Normal

To_IPPBX

Actions	Screenshot
1. On the left menu path click on the '*To_IPPBX*' table you created	
2. To add a new entry, click on the *plus icon (+).*	
3. Set the new *Call Route* as per right picture. ▪ Under *Number/Name Transformation Table*, select the table 'IPPBX_Prefixes' previously created – see above ▪ Under *Destination Information* section click on the *Add/Edit* icon to set the *Destination Signaling Groups.* It is the Signaling Group facing the IPPBX	

Actions	Screenshot
	

2.7 SIP rules & manipulations (eSBC Application)

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

2.7.1 Numbers Manipulations

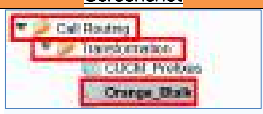
This chapter is about the Number manipulation for precisely the "Called Number" in the URI. Orange Phone numbers must be sent to Orange in E164 format.
The following example manipulations will transform Called numbers received from Customer IPPBX in National format (0ZABPQMCDU or 00xxxxxxxx) to E164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

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

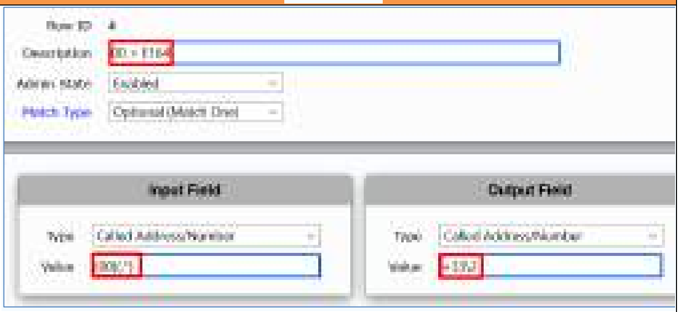
Orange_BTalk Transformations

Description	Match Type	Input Field Type	Input Field Value	Output Field Type	Output Field Value
00 > E164	Optional (Match One)	Called Address/Number	(00)(.*)	Called Address/Number	+33\2
0 > E164	Optional (Match One)	Called Address/Number	(0)(.*)	Called Address/Number	+33\2
Add Plus Calling Number	Optional (Match One)	Calling Address/Number	(\+)?(.*)	Calling Address/Number	+\2

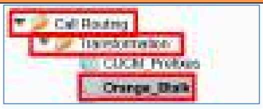
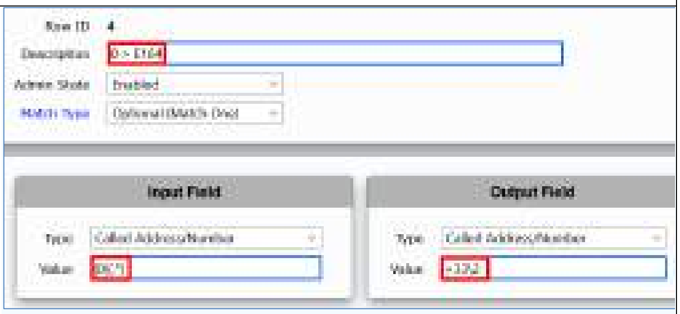
00 > E164

Actions	Screenshot
1. On the left menu path click on the *Orange_Btalk* table you created	
2. To add a new entry, click on the *plus icon (+).*	

Commenté [CSS36]: Please complete corresponding regex rule
Commenté [GA37R36]: This info is in the table above
Commenté [CSS38R36]: Please complete in case of reception of number starting with 00 transform to E.164 french format +33
Commenté [GA39R36]: done
Commenté [CSS43]: Please adapt with new table above

Actions	Screenshot
3. Set the new entry as per right picture	

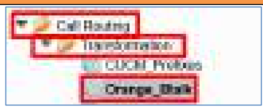
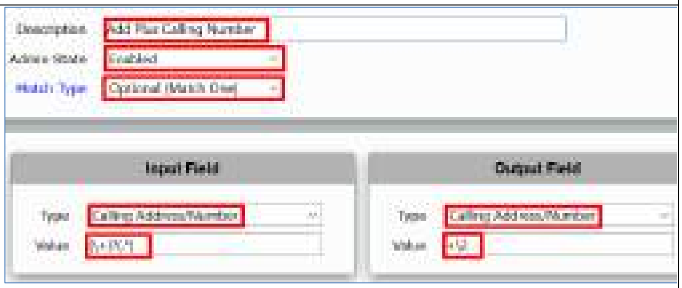
0 > E164

Actions	Screenshot
1. On the left menu path click on the *Orange_Btalk* table you created	
2. To add a new entry, click on the *plus icon* (+).	
3. Set the new entry as per right picture	

Commenté [CSS40]: Same as above, please describe rule and condution number starting with 00 transformation to E.164 french format +33

Commenté [GA41R40]: done

Add Plus Calling Number

Actions	Screenshot
1. On the left menu path click on the *Orange_Btalk* table you created	
2. To add a new entry, click on the *plus icon (+).*	
3. Set the new entry as per right picture	

You should have the following entries in your transformation table:

Admin State	Input Field Type	Input Field Value	Output Field Type	Output Field Value	Match Type	Description
	Called Address/Number	(00)(.*)	Called Address/Number	+3392	Optional (Match One)	00 = E164
	Called Address/Number	(0)(.*)	Called Address/Number	+3392	Optional (Match One)	0 = E164
	Calling Address/Number	(\+)?(.*)	Calling Address/Number	+\2	Optional (Match One)	Add Plus Calling Num...

Commenté [GA42R40]: done
Commenté [GA44R43]: This info is on the table above
Commenté [CSS45R43]: OK

2.7.2 SIP Messages Manipulations

Commenté [CSS46]: Please add and describe Diversion to History-Info Message manipulation from OBS BT toward IPBX

Commenté [CSS47]: How the topology hiding (Request-Uri, To, From, Contact, PAI, Diversion) occurred without any Message manipulation ?

Commenté [CSS48]: Can you add a message Manipulation description in order to remove SDP Body Multipart ?

Several SIP Message manipulations (SMM) 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 Orange BTIP/BTalk services.

The SIP > Message Manipulation menu path allows you to create rules to manipulate the incoming or outgoing messages. This feature is intended to enhance interoperability with different vendor equipment and applications, and for correcting any fixable protocol errors in SIP messages on fly without any changes to firmware/software.

There are cases where a compliant message may be modified to adapt to an application specific requirement . In a typical deployment there may be hundreds or even thousands of endpoints that use the services of the eSBC. In these environments when an interoperability issue arises or an application expects a specific behavior the only remedy is to escalate the issue and wait for a maintenance release. This is neither scalable nor very responsive, so the SIP Message Manipulation feature was developed to solve this issue.

This capability consists of two components, condition rules and message rules. Condition rules provide a means to identify which messages and what components in the message must present before any modifications are performed. The message rule does the actual modification of a message. Once the conditions of a rule have been met the message rule(s) are applied.

Commenté [CSS49]: Please adapt this wording to iyr Ribbon eSBC Message Manipulations application context

Commenté [CSS50R49]: Following last exchange, please review this wording with Marc.

Note:
For more information on Sip Message Manipulation function go to the Ribbon support web site *SMM catalog*

Condition Rules

Description	Match Type	Operation	Match Value Type	Match Value
Match_Content-Type	SG User Value 1	Equals	Literal	application/sdp
Match_Anonymous	from.displayname	Equals	Literal	Anonymous

Commenté [CSS51]: Please explain what's SG User value ?

Commenté [GA52R51]: That is the predefined name for SMM and Transformations variables

Commenté [GA53R51]:

Commenté [CSS54R51]: Is SG User Value 1 is a temporary variable token used ?

Match_Content-Type

The *Condition Rule* matches only if *SG User Value 1 = application/sdp.* This condition is created to identify whether the SDP is present or not in the SIP messages.

Note:
The SG User Value 1 is stored using a Message Rule (Store_Content-Type) that will be defined in the next section.
'SG User Value 1' is the predefined name used by the eSBC to store a value on purpose.

Actions	Screenshot
1. Go to the SIP > Message Manipulation > Condition Rule Table menu path	
2. To add a new Condition Rule, click on the *plus icon (+).*	
3. Set the new entry as per the right picture	

Match_Anonymous

This Condition Rule matches only if from.displayname = Anonymous
It compares whether the *display name* that is in the *From* header is equals to *Anonymous.*

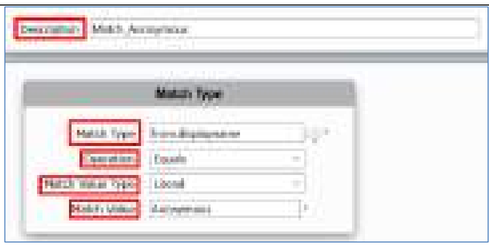
Note:
This condition will be used by a Message Rule (Modify_From_Anonymous) that will be defined in the next section. That rule is used to set the format requested by Orange Business (sip:anonymous@anonymous.invalid)

Commenté [CSS55]: Explain why you have to specify this condition ?

Commenté [CSS56R55]: Also review this title in order to be more explicit

Commenté [GA57R55]: Explanation is already in the document.
From my point of view it is very explicit, it matches when Anonymous is present in the display name

Commenté [CSS58R55]: OK

Actions	Screenshot
1. Go to the SIP > Message Manipulation > Condition Rule Table menu path	
2. To add a new Condition Rule, click on the *plus icon (+).*	
3. Set the new entry as per the right picture	

Messages Rules Tables

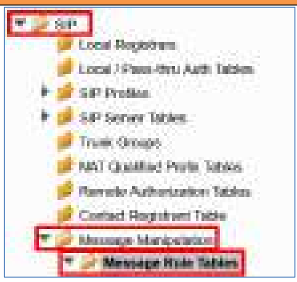
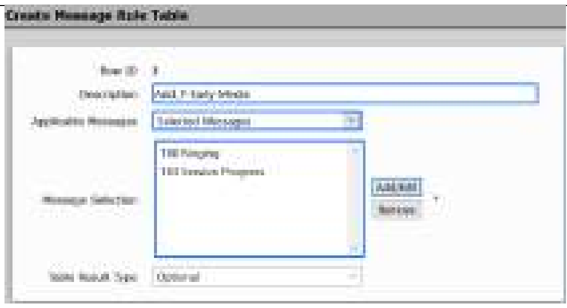
The *Message Rule Tables* collect *SIP Messages Manipulations Rules* that are applied according to the *Message Type* defined in the Message Rule Tables.

Description	Result Type	Message Type	Comments
Add_P-Early-Media	Optional	180, 183	It applies only to 180 and 183 respond messages
Store_Content-Type	Optional	180, 183	It applies only to 180 and 183 respond messages
Store_User-Agent_Value	Optional	All	It applies to all messages
Orange Business_SIP_Profile_Adaptation_01	Optional	All	It applies to all messages
Orange Business_SIP_Profile_Adaptation_02	Optional	Requests	It applies only to request messages

Description	Remark
Add_P-Early-Media	This table collects the rules used to insert the P-Early-Media header as per chapter 1.4
Store_Content-Type	This table collects the rules used to store the Content-type header value. This value is used to know whether the SIP message contains an SDP or not
Store_User-Agent_Value	This table collects the rule used to store the PBX User-Agent and Server headers values to set the format as per chapter 1.4
Orange Business_SIP_Profile_Adaptation_01	This table collects the rules used to set the format as per chapter 1.4
Orange Business_SIP_Profile_Adaptation_02	This table collects the rules used to set the format as per chapter 1.4

Add P-Early-Media

This table collects the rules that are used to add the *P-Early-Media* header in SIP 180, SIP 183 responses.

Actions	Screenshot
1. Go to the SIP > Message Manipulation > Message Rule Tables menu path	
2. To add a new Message Rule Table, click on the *plus icon (+).*	
3. Set the new entry as per the right picture	

Store Content-Type

This table collects the rule that is used to store the *Content-Type* value in the *SG User Value 1.*

Note:
This table must be applied on the Signaling Group facing the IPPBX, set it as Inbound Message Manipulation

Commenté [CSS59]: Explain why to do that, pointed to orange spec.

Commenté [CSS60R59]: Also review this title in order to be more explicit

Commenté [GA61R59]: It is too explicit, it is used to add the P-Early-Media

Commenté [GA62R59]: This is not the rule that adds the P-Early-Media, it is the table that store the rules used to add the P-Early-Media

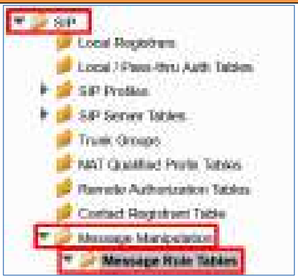
Commenté [CSS63R59]: OK

Commenté [CSS64]: Explain why to do that pointed to OBS specs.

Commenté [CSS65R64]: Also review this title in order to be more explicit

Commenté [GA66R64]: It is too explicit, it stores the Content-Type Value

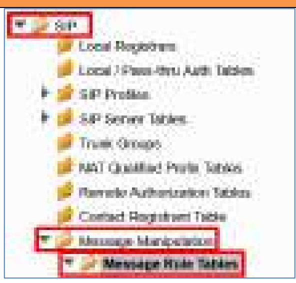
Commenté [CSS67R64]: OK

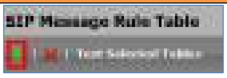
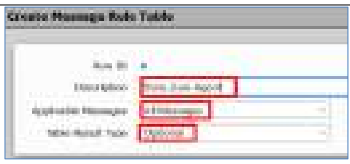
Actions	Screenshot
1. Go to the SIP > Message Manipulation > Message Rule Tables menu path	
2. To add a new Message Rule Table, click on the *plus icon (+).*	
3. Set the new entry as per the right picture	

Store_User-Agent

This table collects the rules used to store the PBX User-Agent header value

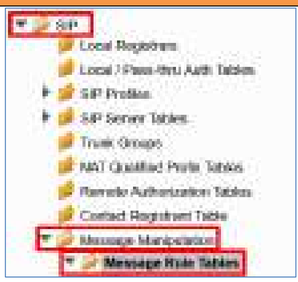
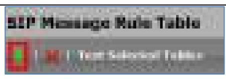
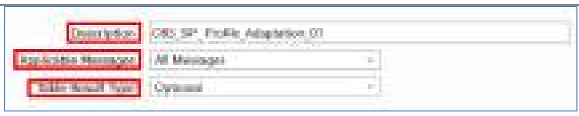
Note:
This table must be applied on the Signaling Group facing the IPPBX, set it as Inbound Message Manipulation

Actions	Screenshot
1. Go to the SIP > Message Manipulation > Message Rule Tables menu path	

Actions	Screenshot
2. To add a new Message Rule Table, click on the *plus icon (+).*	
3. Set the new entry as per the right picture	

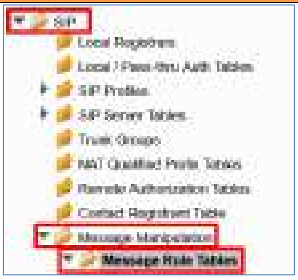
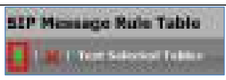
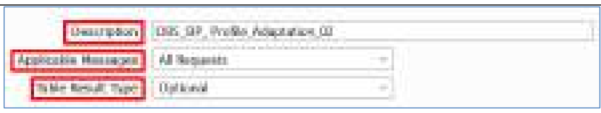
Orange Business_SIP_ Profile_Adaptation_01

This table collects some rules that are used to accomplish the SIP format requested by Orange Business

Actions	Screenshot
1. Go to the SIP > Message Manipulation > Message Rule Tables menu path	
2. To add a new Message Rule Table, click on the *plus icon (+).*	
3. Set the new entry as per the right picture	

Orange Business_SIP_ Profile_Adaptation_02

This table collects some rules that are used to accomplish the SIP format requested by Orange Business.

Actions	Screenshot
1. Go to the SIP > Message Manipulation > Message Rule Tables menu path	
2. To add a new Message Rule Table, click on the *plus icon (+).*	
3. Set the new entry as per the right picture	

Messages Rules (Per table)

Add_P-Early-Media Rules

Description	Rule Type	Result Type	Comments
Add P-Early-Media supported	Header Rule	Optional	It adds the P-Early-Media header value = supported
Del_P-Early-Media	Header Rule	Optional	It deletes the P-Early-Media header to avoid duplicate headers
Add_P-Early-Media sendrecv	Header Rule	Optional	It adds the P-Early-Media header value = sendrecv

Note:
For more information, please go to Messages Rules Tables and section 2.7.3 Outbound Manipulations.

Commenté [GA69R68]: The explanation is in the comments. Remember that rules are stored on tables, that tables are applied to SIP messages / responses; have you read the Message Rule Table part? In that section is specified on what messages / responses the tables are applied.
Go to the table rules and Outbound Manipulations sections to get more information regarding when the rules tables are applied

Commenté [GA70R68]: Go to the top of the section 'Messages Rules Tables' to get more information.

Commenté [CSS68]: Explain why you have to perform 3 rules ? And on which messages this applied ?

Commenté [CSS71]: If this applied to all Sip messages going through Ribbon eSBC including those send/received from private Sip trunk only ?

Commenté [GA72R71]: Just for messages sent to OBS

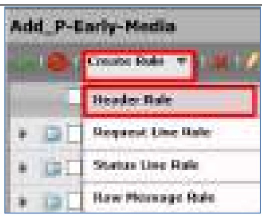
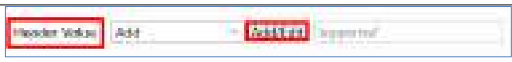
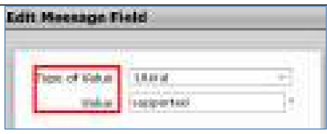
Commenté [GA73R71]: Go to the top of the section 'Messages Rules Tables' to get more information.

Commenté [GA74R71]: Go to section 2.7.3 and 2.7.4 for more information

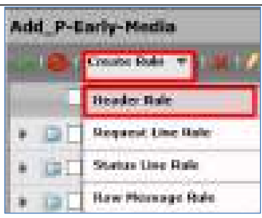
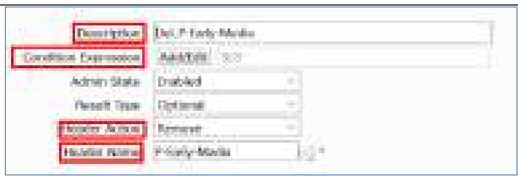
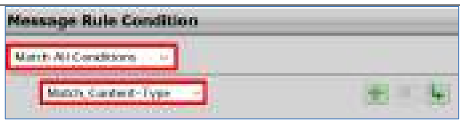
Commenté [CSS75R71]: Please add a Note "Go to section 2.7.3 and 2.7.4 for more information
"

Commenté [GA76R71]: Done

Add P-Early-Media supported

Actions	Screenshot
1. On the left menu path, click on the *Add_P-Early-Media* table you created	
2. To add a new Message Rule, click on the Create Rule > Header Rule icon.	
3. Set the new entry as per the right picture	
4. Once you select *Add* in the *Header Action* field, the bottom section will change its options. Select *Add* in the *Header Value* field and click on the *Add/Edit* icon	
5. Once you click on the *Add/Edit* icon a popup screen appears. Set the configuration as per right picture	

Del_P-Early-Media

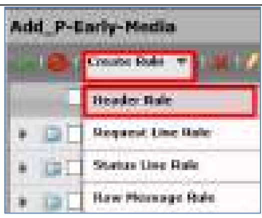
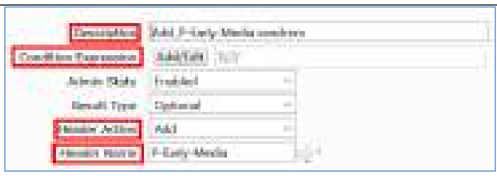
Actions	Screenshot
1. On the left menu path, click on the *Add_P-Early-Media* table you created	
2. To add a new Message Rule, click on the Create Rule > Header Rule icon.	
3. Set the new entry as per the right picture. For *Condition Expression* field go to next step.	
4. Click the *Add/Edit* icon at the *Condition Expression* field. A popup screen appears. Set the configuration as per right picture	

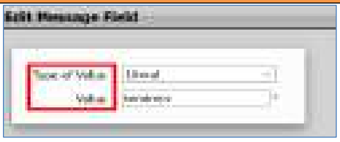
Commenté [CSS77]: Explain why you have to do this removing PEM? And on which context ?

Commenté [GA78R77]: That info is in the table that describe the rules, have you read the comments on that table?

Commenté [CSS79R77]: OK

Add_P-Early-Media sendrecv

Actions	Screenshot
1. On the left menu path, click on the *Add_P-Early-Media* table you created	
2. To add a new Message Rule, click on the Create Rule > Header Rule icon.	
3. Set the new entry as per the right picture. For *Condition Expression* field go to next step.	
4. Click the *Add/Edit* icon at the *Condition Expression* field. A popup screen appears. Set the configuration as per right picture	
5. Once you select *Add* in the *Header Action* field, the bottom section will change its options. Select *Add* in the *Header Value* field and click on the *Add/Edit* icon	

Actions	Screenshot
6. Once you click on the *Add/Edit* icon a popup screen appears. Set the configuration as per right picture	

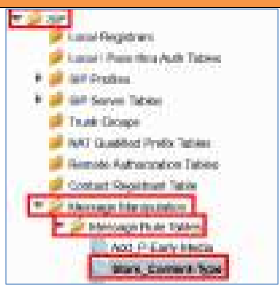
You should have the following entries in the *Add_P-Early-Media* table after configuring all the Message Manipulations rules:

Store_Content-Type Rules

Description	Rule Type	Result Type	Comments
Store Content-Type	Header Rule	Optional	It stores the *Content-Type* value in the *SG User Value 1*

Note:
For more information, please go to Messages Rules Tables *and section* 2.7.4 Inbound Manipulations.

Store Content-Type

Actions	Screenshot
1. On the left menu path, click on the *Store_Content-Type* table you created	

Commenté [CSS80]: Explain why you have to do this removing PEM? And on which context ?

Commenté [GA81R80]: Removing PEM?

Commenté [GA83R82]: Remember that rules are not applied on the SGs, the tables are the entities that are applied on the SGs.
The table that stores this rule is applied on the IPPBX Signaling Group (the SIP trunk group facing the IPPBX), it should be applied as inbound SMM, check the note that is in the table section.

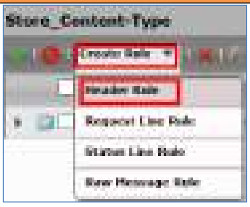
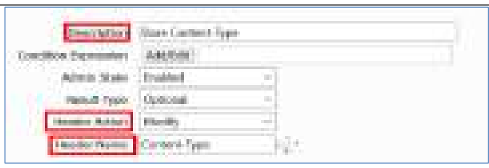
Commenté [GA84R82]: Go to the top of the section 'Messages Rules Tables' to get more information.

Commenté [GA85R82]: Go to section 2.7.3 and 2.7.4 for more information

Commenté [CSS86R82]: Add a Note "Go to section 2.7.3 and 2.7.4 for more information
"

Commenté [GA87R82]: Done

Commenté [CSS82]: If this applied to all Sip messages going through Ribbon eSBC including those send/received from private Sip trunk ? What an SG ?

Actions	Screenshot
2. To add a new Message Rule, click on the Create Rule > Header Rule icon.	
3. Set the new entry as per the right picture.	
4. Once you select *Modify* in the *Header Action* field, the bottom section will change its options. Select *Copy Value to* in the *Header Value* field and click on the *Add/Edit* icon	
5. Once you click on the *Add/Edit* icon a popup screen appears. Set the configuration as per right picture	

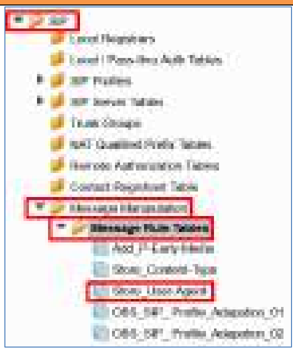
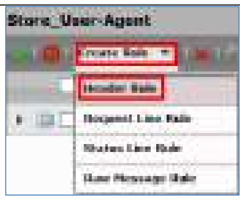
You should have the following entry in the *Store_Content-Type* table after configuring the Message Manipulations rule:

Store_User-Agent Rules

Description	Rule Type	Result Type	Comments
Store_User-Agent_Value	Header Rule	Optional	It stores the *User-Agent* value in the *SG User Value 2*
Store_Server_Value	Header Rule	Optional	It stores the Sever value in the *SG User Value 3*

Note:
For more information, please go to Messages Rules Tables and section 2.7.4 Inbound Manipulations.

Store_User-Agent_Value

Actions	Screenshot
1. On the left menu path, click on the *Store_User-Agent* table you created	
2. To add a new Message Rule, click on the Create Rule > Header Rule icon.	
3. Set the new entry as per the right picture.	

Commenté [GA90R88]: Go to section 2.7.3 and 2.7.4 for more information

Commenté [GA91R88]: Go to the top of the section 'Messages Rules Tables' to get more information.

Commenté [CSS92R88]: Add a Note "Go to section 2.7.3 and 2.7.4 for more information
"

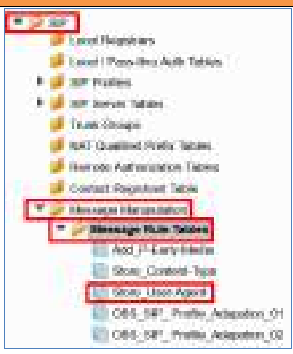
Commenté [GA93R88]: Done

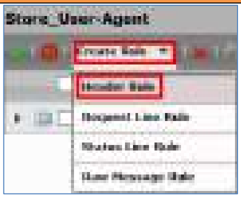
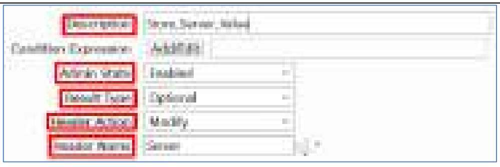
Commenté [CSS88]: If this applied to all Sip messages going through Ribbon eSBC including those send/received from private Sip trunk ? What an SG ?

Commenté [GA89R88]: Remember that rules are not applied on the SGs, the tables are the entities that are applied on the SGs.
The table that stores this rule is applied on the IPPBX Signaling Group (the SIP trunk group facing the IPPBX), it should be applied as inbound SMM, check the note that is in the table section.

4. Once you select *Modify* in the *Header Action* field, the bottom section will change its options. Select *Copy Value to* in the *Header Value* field and click on the *Add/Edit* icon	
5. Once you click on the Add/Edit icon a popup screen appears. Set the configuration as per right picture. *'SG User Value 2'* is a key to store a value on purpose. Here the key will store the content of the User-Agent of the IPPBX.	6. 

Store_Server_Value

Actions	Screenshot
1. On the left menu path, click on the *Store_User-Agent* table you created	

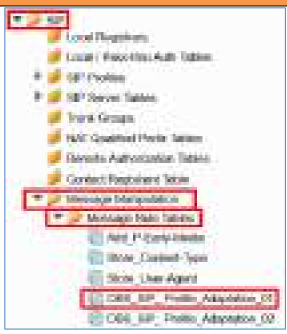
Actions	Screenshot
2. To add a new Message Rule, click on the Create Rule > Header Rule icon.	
3. Set the new entry as per the right picture.	
4. Once you select *Modify* in the *Header Action* field, the bottom section will change its options. Select *Copy Value to* in the *Header Value* field and click on the *Add/Edit* icon	
5. Once you click on the Add/Edit icon a popup screen appears. Set the configuration as per right picture. *'SG User Value 3'* is a key to store a value on purpose. Here the key will store the content of the Value header of the IPPBX.	

Orange Business_SIP_ Profile_Adaptation_01 Rules

Description	Rule Type	Result Type	Comments
Remove_SGID_From_Header	Header Rule	Optional	It removes the *sgid* parameter from the FROM header
Remove_SGID_To_Header	Header Rule	Optional	It removes the *sgid* parameter from the TO header
Modify_User-Agent_header	Header Rule	Optional	It modifies the User-Agent header as per Orange Business requirements
Modify_Server_header	Header Rule	Optional	It modifies the Server header as per Orange Business requirements
Modify_Allow_header	Header Rule	Optional	It modifies the Allow header as per Orange Business requirements

Note:
For more information, please go to Messages Rules Tables and section 2.7.3 Outbound Manipulations.

Remove_SGID_From_Header

Actions	Screenshot
1. On the left menu path, click on the *Orange Business_SIP_ Profile_Adaptation _01* table you created	
2. To add a new Message Rule, click on the Create Rule > Header Rule icon.	

Commenté [CSS95R94]: Please specify globally relation between all the rules described and signaling group application afterward

Commenté [GA96R94]: Remember that rules are not applied to SGs, the entities that are applied on the SGs are the tables rules. Go to the table rules and Outbound Manipulations sections to get more information regarding when the rules tables are applied

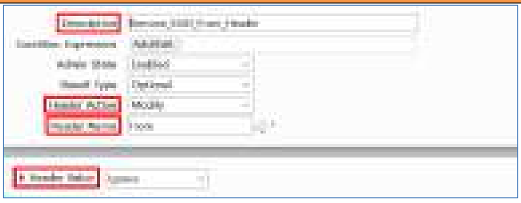
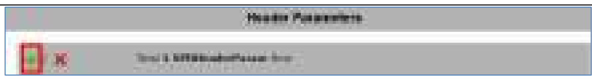
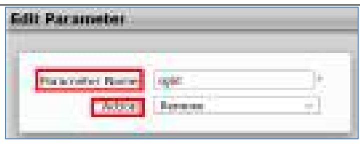
Commenté [GA97R94]: Go to section 2.7.3 and 2.7.4 for more information

Commenté [GA98R94]: Go to the top of the section 'Messages Rules Tables' to get more information.

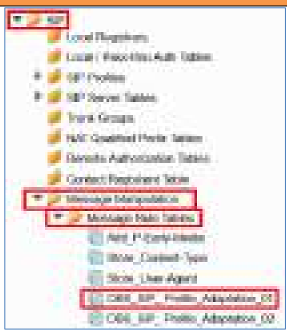
Commenté [CSS99R94]: Add a NOTE "Go to section 2.7.3 and 2.7.4 for more information
"

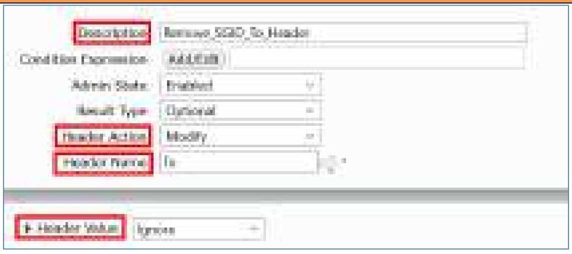
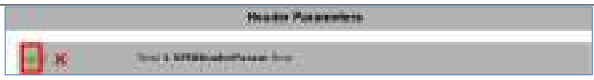
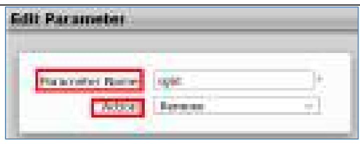
Commenté [GA100R94]: Done

Commenté [CSS94]: How this is applied only to OBS Sip Trunk Sip messages ?

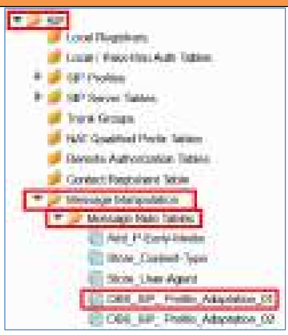
Actions	Screenshot
3. Set the new entry as per the right picture.	
4. Under *Header Parameters* click on the *plus icon (+)* to add a new entry	
5. Once you click on the *plus icon (+)* a popup screen appears. Set the configuration as per right picture	

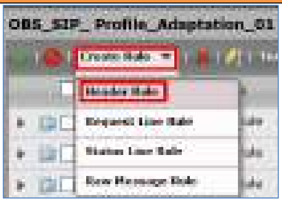
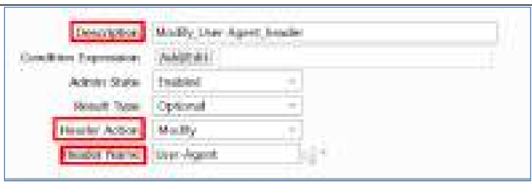
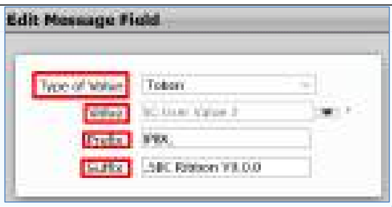
Remove_SGID_To_Header

Actions	Screenshot
1. On the left menu path, click on the *Orange Business_SIP_ Profile_Adaptation _01* table you created	
2. To add a new Message Rule, click on the Create Rule > Header Rule icon.	

<table>
<tr><th>Actions</th><th>Screenshot</th></tr>
<tr><td>3. Set the new entry as per the right picture.</td><td>
</td></tr>
<tr><td>4. Under Header Parameters click on the plus icon (+) to add a new entry</td><td>
</td></tr>
<tr><td>5. Once you click on the plus icon (+) a popup screen appears.
Set the configuration as per right picture</td><td>
</td></tr>
</table>

Modify_User-Agent_header

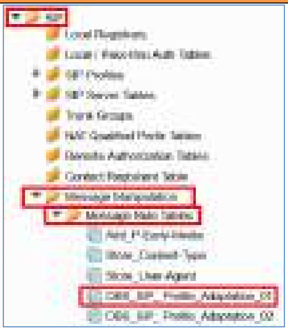
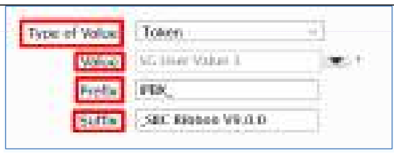
<table>
<tr><th>Actions</th><th>Screenshot</th></tr>
<tr><td>1. On the left menu path, click on the Orange Business_SIP_Profile_Adaptation_01 table you created</td><td></td></tr>
</table>

Actions	Screenshot
2. To add a new Message Rule, click on the Create Rule > Header Rule icon.	
3. Set the new entry as per the right picture.	
4. Once you select *Modify* in the *Header Action* field, the bottom section will change its options. Select *Modify* in the *Header Value* field and click on the *Add/Edit* icon	
5. Once you click on the *Add/Edit* icon a popup screen appears. Set the configuration as per right picture	

Commenté [CSS101]: fIs it a fix entry for thr Prefi or a variable retrieve from INVITE received from the IPBX ? We need to have this populate dynamically from what a received for IPBX identification from BTalk perspective.

Commenté [GA102R101]: It is dynamically. The format is described below:
IPBX_$SGUSERVALUE2_SBC Ribbon V9.0.0.
So, if the CUCM sends the model and version to the SBC, it would be stored in the SGUSERVALUE2 and the final result would be something like this:
IPBX_CUCM12.5_SBC Ribbon V9.0.0
NOTE: The $SGUSERVALUE2 depends on the value sent by the IPPBX

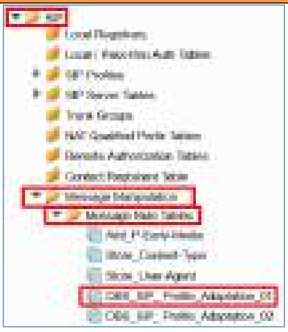
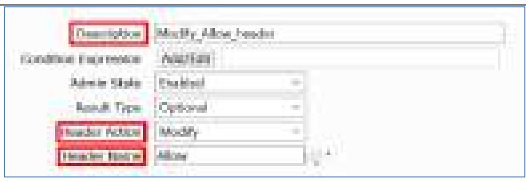
Modify_Server_header

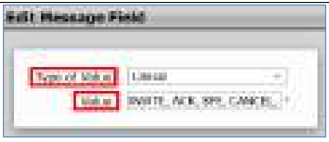
Actions	Screenshot
1. On the left menu path, click on the *Orange Business_SIP_ Profile_Adaptation _01* table you created	
2. To add a new Message Rule, click on the Create Rule > Header Rule icon.	
3. Set the new entry as per the right picture.	
4. Once you select *Modify* in the *Header Action* field, the bottom section will change its options. Select *Modify* in the *Header Value* field and click on the *Add/Edit* icon	
5. Once you click on the *Add/Edit* icon a popup screen appears. Set the configuration as per right picture	

Commenté [CSS103]: Is it a fix entry for thr Prefi or a variable retrieve from INVITE received from the IPBX ? We need to have this populate dynamically from what a received for IPBX identification from BTalk perspective.

Commenté [GA104R103]: It is dynamically. The format is described below:
IPBX_$SGUSERVALUE2_SBC Ribbon V9.0.0.
So, if the CUCM sends the model and version to the SBC, it would be stored in the SGUSERVALUE2 and the final result would be something like this:
IPBX_CUCM12.5_SBC Ribbon V9.0.0
NOTE: The $SGUSERVALUE2 depends on the value sent by the IPPBX

Modify_Allow_header

Actions	Screenshot
1. On the left menu path, click on the *Orange Business_SIP_ Profile_Adaptation _01* table you created	
2. To add a new Message Rule, click on the Create Rule > Header Rule icon.	
3. Set the new entry as per the right picture.	
4. Once you select *Modify* in the *Header Action* field, the bottom section will change its options. Select *Modify* in the *Header Value* field and click on the *Add/Edit* icon	

5. Once you click on the *Add/Edit* icon a popup screen appears. Set the configuration as per right picture	 **Note:** The Value should contain the following information: *INVITE, ACK, BYE, CANCEL, OPTIONS, UPDATE*

You should have the following entries in the *Orange Business_SIP_ Profile_Adaptation_01* table after configuring all the Message Manipulations rules:

OBS_SIP_ Profile_Adaptation_01

Create Rule | Test Message | Total 5 Message Manipulation Rules Rows

Admin State	Rule Type	Result Type	Description
	Header Rule	Optional	Remove_SGID_From_Header
	Header Rule	Optional	Remove_SGID_To_Header
	Header Rule	Optional	Modify_User-Agent_Header
	Header Rule	Optional	Modify_Server_header
	Header Rule	Optional	Modify_Allow_header

Orange Business_SIP_ Profile_Adaptation_02 Rules

Description	Rule Type	Result Type	Comments
Modify_From_Anonymous	Header Rule	Optional	It set the anonymous format as per Orange Business requirements
Modify_Diversion	Header Rule	Optional	It configures the Public IP address in the *Diversion* header and adds the counter parameter
Modify_PAI	Header Rule	Optional	It configures the Public IP address in the *P-Asserted-Identity* header
Add plus P-Asserted-Identity	Header Rule	Optional	It adds the plus sign (+) in the *P-Asserted-Identity* header

Note:
For more information, please go to Messages Rules Tables and section 4.7.3 Outbound Manipulations.

Commenté [CSS105]: Please review this title in order to be more explicit

Commenté [GA106R105]: It would be difficult as it applies several rules to set the format requested by OBS. I mean, it applies several modifications to adapt the SIP format.
Again, it is just the name of the Table that stores the rules used to set the correct format; that is why I named as OBS_Format.
A description of this table has been set in the section 'Message Rule Table'

Commenté [GA107R105]: I have modified the table name as per Marc's comments

Commenté [CSS108R105]: OK

Commenté [GA110R109]: Remember that rules are not applied to SGs, the entities that are applied on the SGs are the tables rules. Go to the table rules and Outbound Manipulations sections to get more information regarding when the rules tables are applied

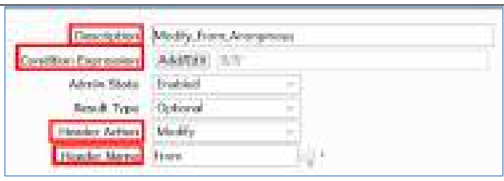
Commenté [GA111R109]: Go to section 2.7.3 and 2.7.4 for more information

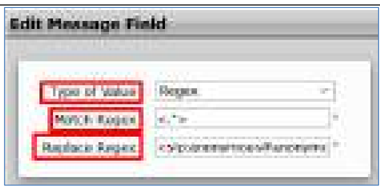
Commenté [GA112R109]: Go to the top of the section 'Messages Rules Tables' to get more information.

Commenté [CSS113R109]: OK Add a not referring to "Go to the top of the section 'For more information please go to Messages Rules Tables."

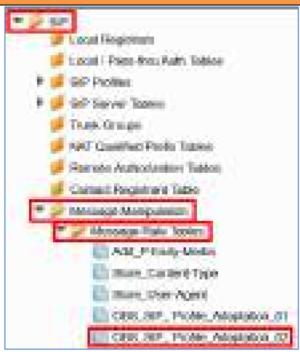
Commenté [CSS109]: How this is applied only to OBS Sip Trunk Sip messages ?

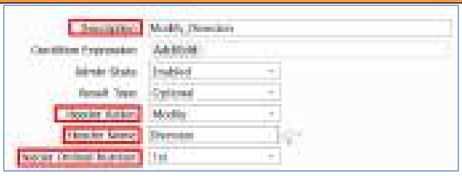
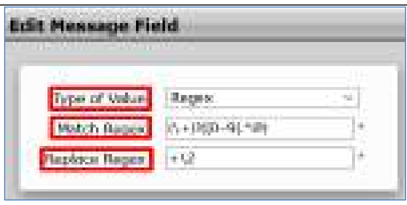
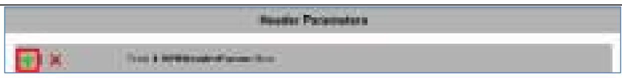
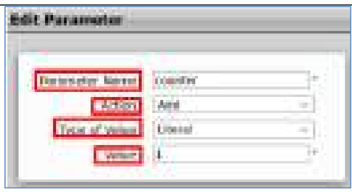
Modify_From_Anonymous

Actions	Screenshot
1. On the left menu path, click on the *Orange Business_SIP_ Profile_Adaptation _02* table you created	
2. To add a new Message Rule, click on the Create Rule > Header Rule icon.	
3. Set the new entry as per the right picture. For *Condition Expression* field go to next step.	
4. Click the *Add/Edit* icon at the *Condition Expression* field. A popup screen appears. Set the configuration as per right picture	
5. Once you select *Modify* in the *Header Action* field, the bottom section will change its options.	

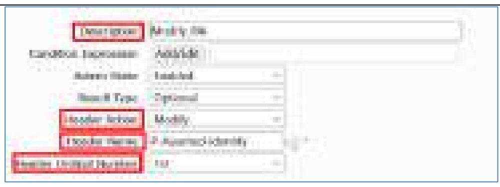
Actions	Screenshot
Select *Modify* in the *Header Value* field and click on the *Add/Edit* icon	
6. Once you click on the *Add/Edit* icon a popup screen appears. Set the configuration as per right picture	 Note: The *Replace Regex* field should contain the following information: <sip:anonymous@anonymous.invalid>

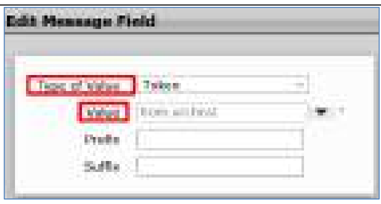
Modify Diversion

Actions	Screenshot
1. On the left menu path, click on the *Orange Business_SIP_ Profile_Adaptation _02* table you created	
2. To add a new Message Rule, click on the Create Rule > Header Rule icon.	

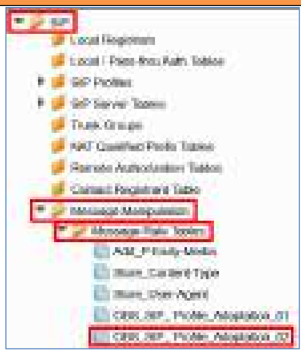
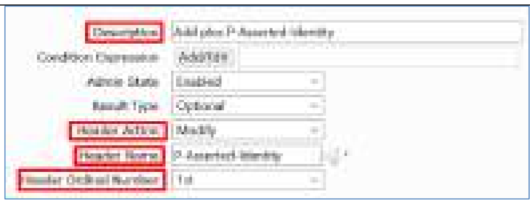
Actions	Screenshot
3. Set the new entry as per the right picture.	
4. Once you select *Modify* in the *Header Action* field, the bottom section will change its options. Select *Modify* in the *Header Value* field and click on the *Add/Edit* icon	
5. Once you click on the *Add/Edit* icon a popup screen appears. Set the configuration as per right picture	
6. Under *Header Parameters* click on the *plus icon (+)* to add a new entry	
7. Once you click on the *plus icon (+)* a popup screen appears. Set the configuration as per right picture	

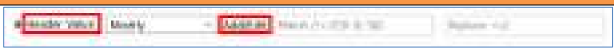
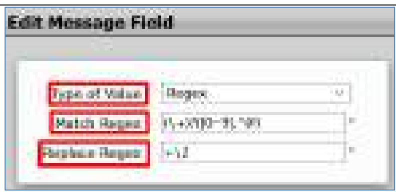
Modify_PAI

Actions	Screenshot
1. On the left menu path, click on the *Orange Business_SIP_ Profile_Adaptation _02* table you created	
2. To add a new Message Rule, click on the Create Rule > Header Rule icon.	
3. Set the new entry as per the right picture.	
4. Once you select *Modify* in the *Header Action* field, the bottom section will change its options. Click on the arrow that is next to the *Header Value* field to display more options. Click on the arrow that is next to the *URI* field to display additional options.	

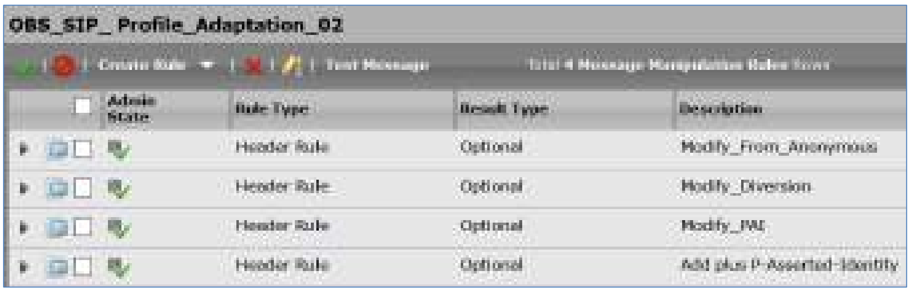
Actions	Screenshot
Set the configuration and click on the *Add/Edit* icon as per right picture	
5. Once you click on the *Add/Edit* icon a popup screen appears. Set the configuration as per right picture	

Add plus P-Asserted-Identity

Actions	Screenshot
1. On the left menu path, click on the *Orange Business_SIP_Profile_Adaptation_02* table you created	
2. To add a new Message Rule, click on the Create Rule > Header Rule icon.	
3. Set the new entry as per the right picture.	

Actions	Screenshot
4. Once you select *Modify* in the *Header Action* field, the bottom section will change its options. Select *Modify* in the *Header Value* field and click on the *Add/Edit* icon	
5. Once you click on the *Add/Edit* icon a popup screen appears. Set the configuration as per right picture	

You should have the following entries in the *Orange Business_SIP_ Profile_Adaptation_02* table after configuring all the Message Manipulations rules:



OBS_SIP_ Profile_Adaptation_02

Admin State	Rule Type	Result Type	Description
	Header Rule	Optional	Modify_From_Anonymous
	Header Rule	Optional	Modify_Diversion
	Header Rule	Optional	Modify_PAI
	Header Rule	Optional	Add plus P-Asserted-Identity

Commenté [CSS114]: Please review this title in order to be more explicit

Commenté [GA115R114]: It would be difficult as it applies several rules to set the format requested by OBS. I mean, it applies several modifications to adapt the SIP format.
Again, it is just the name of the Table that stores the rules used to set the correct format; that is why I named as OBS_Format.
A description of this table has been set in the section 'Message Rule Table'

Commenté [GA116R114]: I have modified the table name as per Marc's comments

Commenté [CSS117R114]: OK

2.7.3 Outbound Manipulations

At the egress, SIP messages already processed by the eSBC are modified to meet the SIP requirements of the upstream device.

Set the Message Rules Tables as per the following information:

Signaling Group	Message Table List	Comment
From-To_OrangeBtalk	Orange Business_SIP_Profile_Adaptation_02	Set the Table Lists as Outbound Message Manipulation
	Orange Business_SIP_Profile_Adaptation_01	
	Add_P-Early-Media	
From-To_OrangeBTIP	Orange Business_SIP_Profile_Adaptation_02	
	Orange Business_SIP_Profile_Adaptation_01	
	Add_P-Early-Media	
From-To_ORANGE-TLS	Orange Business_SIP_Profile_Adaptation_02	
	Orange Business_SIP_Profile_Adaptation_01	
	Add_P-Early-Media	

Note:
Refer to the section 4.5.11 and 4.6.13 to attach these SIP Message Manipulation rules into the corresponding Signaling group.

Commenté [GA119R118]: It would be difficult as it applies several rules to set the format requested by OBS. I mean, it applies several modifications to adapt the SIP format.
Again, it is just the name of the Table that stores the rules used to set the correct format; that is why I named as OBS_Format.
A description of this table has been set in the section 'Message Rule Table'

Commenté [GA120R118]: I have modified the table name as per Marc's comments

Commenté [CSS118]: Please review Message table list naming related to previous comments. OBS_Format_XX is not explicit.

2.7.4 Inbound Manipulations

At the ingress, inbound SIP messages are modified to permit proper handling by the eSBC's routing function.

Set the Message Rule Tables as per the following information:

Signaling Group	Message Table List	Comment
<Signaling Group facing the IPPBX>	Store_Content-Type	Set the Table Lists as Inbound Message Manipulation
	Store_User-Agent	

3. Annexes

3.1 Example of SIP INVITE message

From IPPBX toward Orange BTALK

INVITE sip:+960012144326845@172.22.244.209:5060;user=phone SIP/2.0
Allow: INVITE, ACK, BYE, CANCEL, OPTIONS, UPDATE
Call-ID: call-EF01CD00-0000-0010-161E-5F@192.168.191.150
Contact: <sip:+33296086974@192.168.191.150:5060;transport=UDP>
Content-Length: 317
Content-Type: application/sdp
CSeq: 2 INVITE
From:<sip:+33296086974@192.168.191.150:5060;user=phone>;tag=c0a8bf96-b230
Max-Forwards: 69
P-Asserted-Identity: <sip:+33296086974@192.168.191.150>
Supported: replaces,update
To:<sip:+960012144326845@172.22.244.209:5060;user=phone>
User-Agent: IPBX_Cisco-CUCM12.5_eSBC Ribbon V12.3.0
Via: SIP/2.0/UDP 192.168.191.150:5060;branch=z9hG4bK-UX-c0a8-bf96-9133

v=0
o=eSBC 87 1001 IN IP4 192.168.191.150
s=VoipCall
c=IN IP4 192.168.191.150
t=0 0
m=audio 16390 RTP/AVP 8 18 101
c=IN IP4 192.168.191.150
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=maxptime:40
a=sendrecv
a=rtcp:16391

From Orange BTALK toward Customer IPPBX

INVITE sip:+33296086974@192.168.191.150:5060;user=phone SIP/2.0
Via: SIP/2.0/UDP 172.22.244.209:5060;branch=z9hG4bK5u1md81040d54rql4av0.1
To: <sip:+33296086974@192.168.191.150;user=phone>
From: <sip:+2144326845@172.22.244.209;user=phone>;tag=SDlncc101-Onh6fA
Call-ID: SDlncc101-2b66c18972b3c53171a36d538d79cf17-v300g00060
CSeq: 931329 INVITE
Max-Forwards: 66
Contact: <sip:172.22.244.209:5060;transport=udp>

Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, INFO, UPDATE, OPTIONS, REFER
Supported: uui
P-Charging-Vector: icid-value="tTY5fQeY1wXyntN4eK"
Accept: application/sdp,application/isup,application/xml
Content-Type: application/sdp
Content-Length: 262

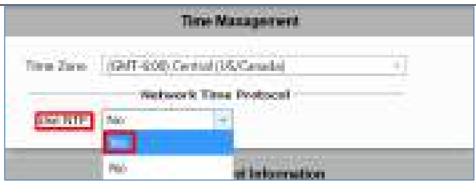
v=0
o=- 1560297477 1 IN IP4 172.22.244.209
s=-
c=IN IP4 172.22.244.209
t=0 0
m=audio 18852 RTP/AVP 8 18 101
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sqn:0
a=cdsc: 1 audio RTP/AVP 8
a=cdsc: 2 image udptl t38
a=ptime:20

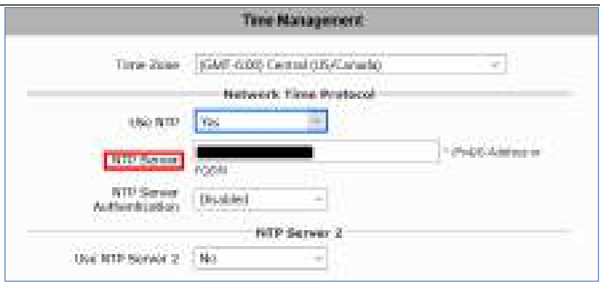
3.1.1 NTP server configuration

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 eSBC receives the current date and time. This is necessary for validating certificates of remote parties. It is important, that NTP Server will locate on the OAMP IP Interface (LAN_IF in our case) or will be accessible through it.

To configure the NTP server address:

Commenté [CSS121]: Please complete

Actions	Screenshot
1. Go to *System* > *Node-Level Settings* menu path	
2. Under the *Time Management* section select *Yes* on the *Use NTP* field	

3. Set the NTP server IP address on the *NTP Server* field. **Note:** Enable the NTP Server Authentication and a second NTP server if needed.	

Go to the following link to get further information about configuring an NTP time Source.

4. Glossary

BTalk: Business Talk

BTIP: Business Talk IP

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

eSBC: Session Border Controller

SDP : Session Description protocol

Sg : Signaling group

SIP: Session Initiation Protocol

TCP: Transmission Control Protocol

TLS: Transport Layer Security

UDP: User Datagram Protocol

UE : User Equipment (Customer Sip termination)

WAN: Wide Area Network