Business Talk & BTIP Configuration Guidelines With Ribbon Edge Customer eSBC Certified Border

versions addressed in this guide: Ribbon Edge eSBC V.9.0.0

Latest Edition: 02/09/2021

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

Table of contents

1 General

1.1 Scope of the document

The aim of this document is to provide configuration guideline for Ribbon SBC Edge 1000, 2000 and Swe Lite North OBS Carrier profile in VISIT Program.

The document presents configuration requirements on the Ribbon SBC Edge, in order to ensure the interoperability with Business Talk IP and Business Talk, Business Talk Over Internet SIP infrastructure (SIP proxy aSBC, Class 5, Appliance Server and Gateways Devil+/NCIS/NBI/Neo).

1.2 References documents

Title	Link
Software Update for Ribbon SBCs 1000, 2000 and Swe Lite Version 9	https://support.sonus.net/pages/viewpage.action?pageId=229474489
Ribbon SBC Edge Documentation	https://support.sonus.net/display/UXDOC90

1.3 Prerequisites

1.3.1 Certificates

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

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

1.3.2 Public DNS configuration:

Following requirements regarding Public DNS configuration:

- In the SBC configuration, public DNS is used for outgoing calls (e.g. From PBX to BToI/BTIPoI)
- Internet-Facing LAN: either enter the IP addresses of 2 private DNSs, that relay DNS queries to Internet, or enter the IPs of 2 accessible public DNS such as those of Orange (80.10.246.2, 80.10.246.129)

1.3.3 NTP

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

1.4 Orange BTalk/ BTIP specifications

The information in this chapter are the SIP trunk specifications required in order to interconnect Orange Business Talk network. The Enterprise SBC must be compliant with those specifications.

Those information's were used to define the configuration described in this document.

✓ ***Supported RFC's***

- *RFC 3261 : Session initiation protocol*
- *RFC 3264 : An offer/answer Model with the Session Description Protocol*
- *RFC 3262 : Reliability of provisional responses in Session Initiation protocol (please refer to provisional response and PRACK section)*
- *RFC 3311 : The Session Initiation Protocol UPDATE Method*
- *RFC 3323 : A privacy Mechanism for the session Initiation Protocol*
- *RFC 3325 : Session Initiation Protocol for Asserted Identity within Trusted Networks*
- *RFC 3204 : MIME media types for ISUP and QSIG Objects*
- *RFC 3550 : RTP : A transport Protocol for Real Time Applications*
- *RFC 3711: SRTP: Secure Real-time Transport Protocol*
- *RFC 3960 : Early Media and Ringing Tone generation in the Session Initiation Protocol*

- *RFC 4566 : SDP: Session Description Protocol*
- *RFC 4568: SDP: Security Descriptions for Media Streams*
- *RFC 2833/4733 : RTP payload for DTMF digits, Telephony Tones and telephony signals*
- *RFC 5806 : Diversion Indication in SIP*
- *RFC 5009 : Private Header Extension to the Session Initiation Protocol for Authorization of early*

✓ ***Sip Methods supported :***

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

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

- ***SIP Message size specifications are:***
  - *SIP message limited to 4096 Bytes*
  - *SDP Body limited to 1024 Bytes*

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

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

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

- ***Encryption specifications are :***
  - **TLS V.1.2**

The following Cipher list is supported as Cipher Client/Server:
  - **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** (Recommended)
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

- ***Codec/Packet Rate specifications are (prefer order list) :***
  - G.711 A-law 20 ms (or on demand specific G.711 µ--law 20 ms)
  - G.729 20 ms (annexb = no)
  - G722 20 ms.
  - <u>For BTIP over Internet and BTalk over Internet only (TLS)</u> G.711 A-law 20 ms (or on demand specific G.711 µ--law 20 ms) is supported

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

- ***T.38 for FAX specifications are:***
  - T.38 Fax over UDP
  - T.38 payload size 20 ms or 40 ms
  - NSF value 0
  - Fax rate management method Transferred TCF
  - UDP redundancy method T38UDPredundancy
  - T.38 version parameter 0
  - T.30 data V.21
  - Data signaling rates: V.17 or V.29 or V.27ter
  - Error Correction Method (ECM) Enabled
  - Fax rate max 14400 bps
  - SG3-G3 fallback method Either ANSam removal or CM removal

- Switching from voice mode to fax mode T.38 re-INVITE sent by called party

Note: For T.38 , the Ribbon SBC will be transparent. No adaptation will be done at SBC level as it requires DSP resources .

- ✓ ***DTMF transport specifications are:***
  RFC 2833/4733

- ✓ ***Signalisation/ Media Tag specifications are:***
  - ✓ DSCP 46 (EF)

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

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

- ✓ ***Media Session Modification/ Transfer – Call Forward:***
  - Modification of media (IP, codec, attributes ..) in reception/emission based on UPDATE (With SDP) in Early Dialog and Re-INVITE in confirmed Dialog (with or without SDP)
  - Attributes “a=” must be equal to send only, recv only, inactive, send recv.
  - In case of Call Forward, the diversion header must be provided by the UE.
  - Same Methods/Attributes/headers may be sent from BTalk/BTIP to UE.

- ✓ ***Ring back Tone and Early Media***
  - Presence of an SDP in provisional response does not indicate presence of a distant early media (only p-early-media indicate presence of distant early media).
  - On reception of a 180 (without SDP) from BTalk/ BTIP, eSBC must play local Ring Back Tone.
  - eSBC can indicate an early media, within presence of P-Early-Media header into his provisional response.

- ✓ ***Anonymous calls***
  - If anonymization is requested, the UE should:
  - Set privacy header to “user” with From containing Calling identity
  - Or: set privacy header to id with From containing anonymous (“anonymous” sip:anonymous@anonymous.invalid, P-A-I must contain the Calling party identification.
  - Same Settings could be used when Business Talk request anonymous calls.

- ✓ ***Number format specifications are:***
  - Called Number send to Orange network must be at E164 format
  - Calling Number send to Orange network must be in National format (0ZABPQMCDU or 00xxxxxxxx) or E164 format.

- ✓ ***Rerouting scenario :***
  - On reception of a Sip Error message, User Equipement must reroute in case of 408 et 50x (500/501/502/503/504/505/513)

- Emission of a Sip error message to BTalk/BTIP, UE must send 5xx if a rerouting is expected from BTalk/BTIP service.
- It’s recommended to do not send 408 to BTalk/BTIP. If it’s the case, UE will be considered out of service until next Sip probing

Note: the eSBC comply with the RFC4497

✓ ***Call defection :***
  - 3xx Sip message are not supported by BTalk/BTIP services. Those messages will be converted into SIP error messages.

2 Certified Architecture

2.1 Introduction to architecture components and features

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

These configuration guidelines taken into account:

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

These configuration guidelines don't take into account existing VISIT certified Premium vendor:

- Microsoft specific configuration guidelines for Ribbon SBC Edge which cover both North and South side are available on OBS websites.

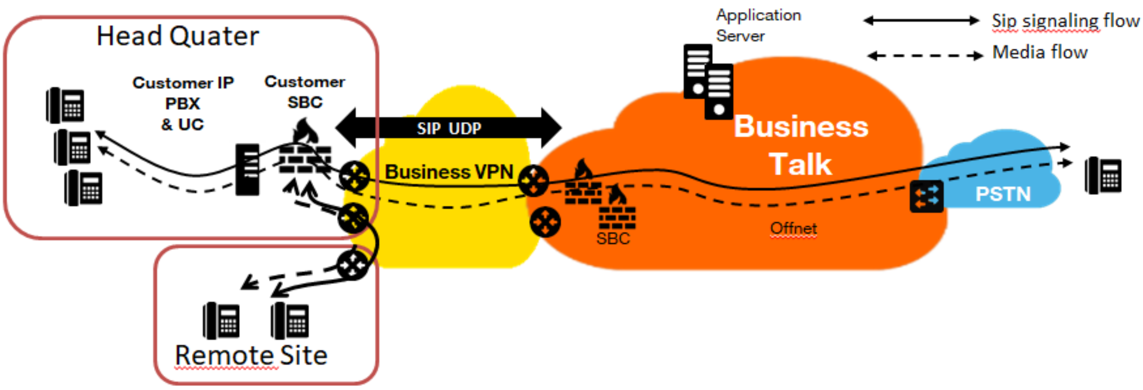
Concerning the fax support, Business Talk and BTIP support the following usage:

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

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

2.2 Architecture with Ribbon "customer" SBC with OBS SIP North Carrier configuration

2.2.1 Unencrypted SIP Trunk (UDP)

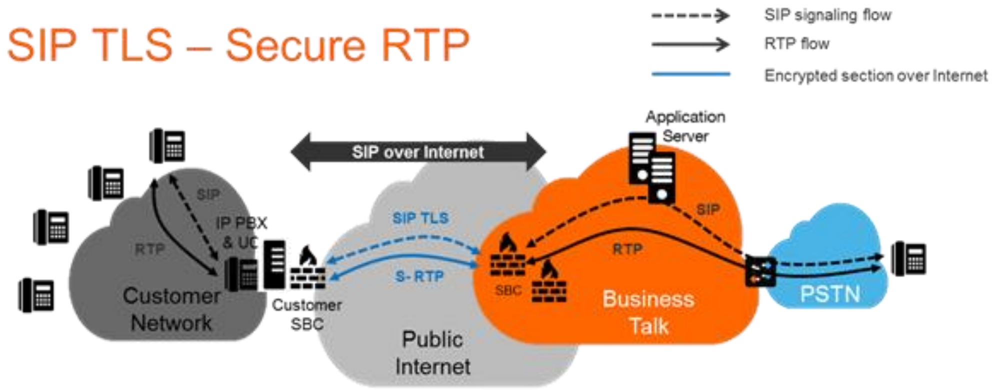


In this architecture:

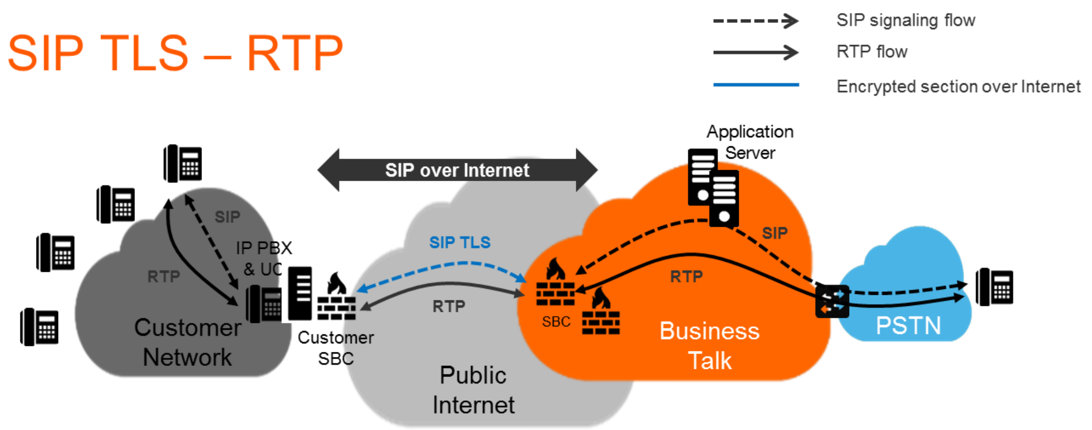
- Both 'SIP trunking' and RTP media flows between endpoints and the Business Talk/BTIP are anchored by the "customer SBC":
- For Head Quarter & remote sites, media flows are routed through the Customer SBC and the main BVPN connection.

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



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

Unencrypted SIP Trunk through BVPN

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

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

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

Encrypted SIP Trunk through Internet

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

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

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

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

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

2.3 Business Talk & BTIP Ribbon Edge eSBC certified versions

Ribbon Edge SBC – software versions				
Reference product	Hardware or Virtual Model	Software Major version	Certified "Loads"	Certification
SBC Edge	**1000**	v.9	Load(s) 0.0*	✓
	2000			
SBC Edge	**SWe Lite**			

* Minimum Load for implementation, last most up-to-date Load is recommended per Ribbon.

Note:

Ribbon SBC technical documentation is available on the Web [Ribbon SBC Edge Portal]

2.4 Ribbon Global configuration

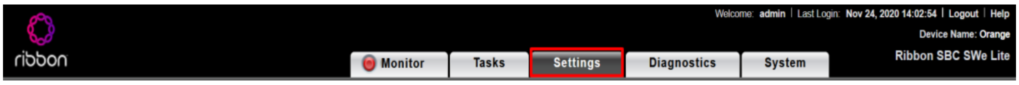
2.4.1 Objects

This chapter describes the Ribbon SBC 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 SBC 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 SBC configuration (save the configuration file on your laptop). When you have finished the configuration do an "Apply" of your SBC configuration and do again of Backup of your new configuration.

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

2.4.2 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, capacity, …) in this document are given as example and **must be replaced by the real value** specific of this interconnection.

Several tables in the following Chapters, will contain **lines in "Grey" color.** Those lines are indicated as **example and reminder of the existing configuration** of the "south" side

(IPPBX side) inside the SBC. If the SBC 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.

Example

Description	Host/domain	Server Lookup	Port	Protocol
Orange_BTalk	<orange.example.com>	IP/FQDN	<Port_Number>	<Protocol>
IPPBX	<ippbx.example.com>	IP/FQDN	<Port_Number>	<Protocol>

2.5 OBS Business Talk & BTIP Carrier North unencrypted SIP configuration for Ribbon SBC (UDP)

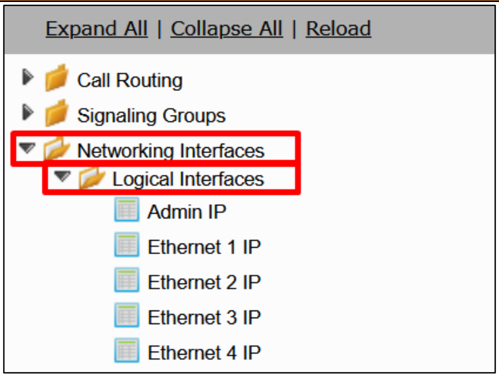
As a prerequisite Ribbon recommends reading the SBC Edge Security Hardening Checklist to understand how to secure the SBC into your network infrastructure

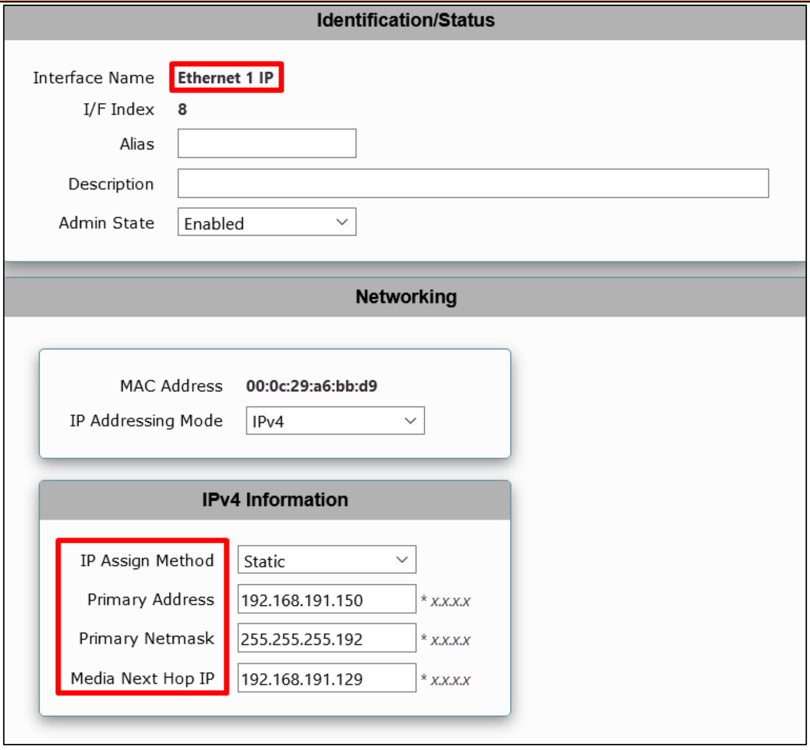
2.5.1 Configure Network Interfaces

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.

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 SBC 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».

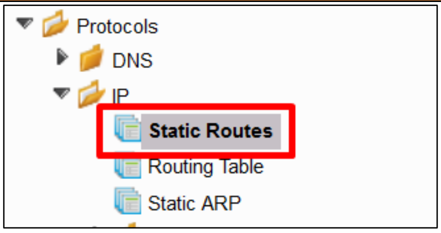
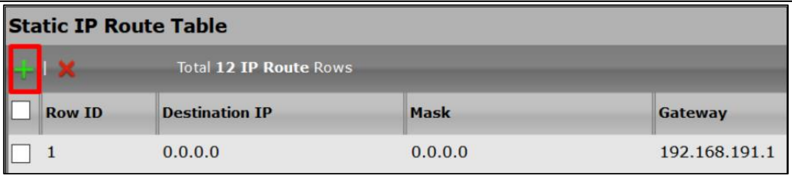
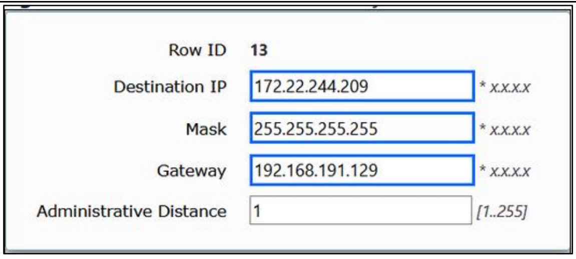
Actions	Screenshot
No action	Set as by design

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****.*

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

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 SBC 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 SBC 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. SBC 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, SBC PRACK Mode: Mandatory on the SIP profile of the Customer IPPBX.

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

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

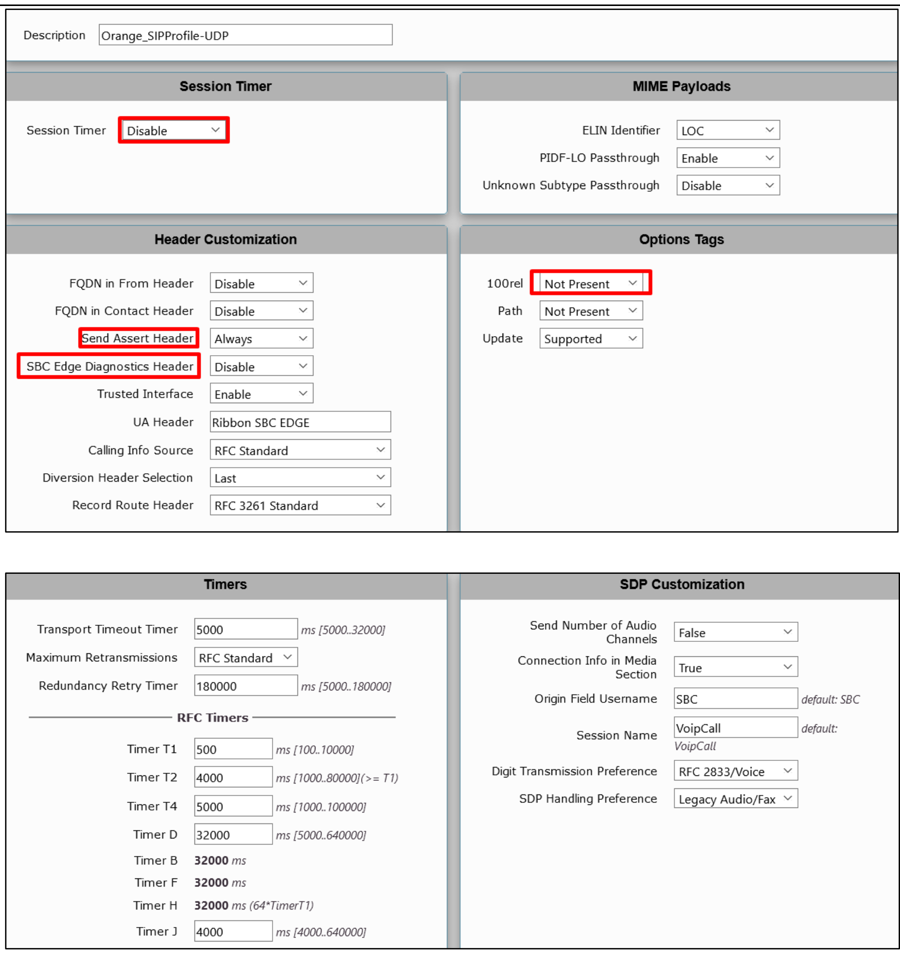
The History-Info header to Diversion header conversion is done automatically.

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 SBC 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 SBC support 100rel (PRACK support)	100rel	Not Present
Specifies if the **X-SBC Edge -Diagnostics** header is added to the outbound SIP signaling messages	SBC Edge Diagnostics Header	Disable

Orange_SIP Profile-UDP

<table>
<tr><th>Actions</th><th>Screenshot</th></tr>
<tr><td>1. Go to SIP > SIP Profiles menu path</td><td>
</td></tr>
<tr><td>2. To add a new SIP Profile click on the plus icon (+).</td><td>
</td></tr>
<tr><td>3. Set the SIP Profile parameters</td><td>
</td></tr>
</table>

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).***

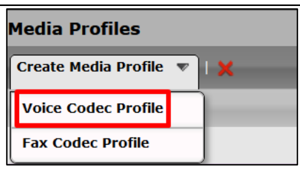
Note:

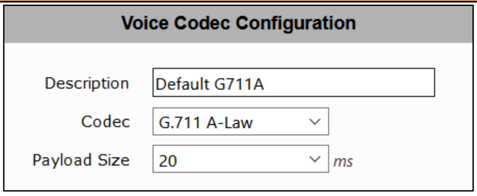
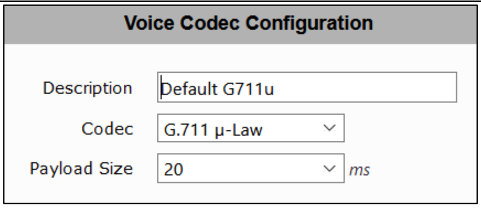
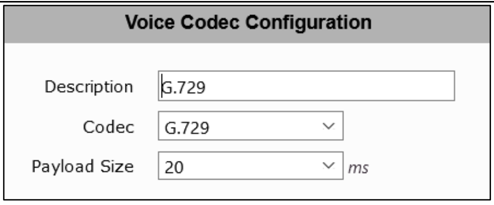
G.711 µ-law 20 ms can be requested, specifically on demand.

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

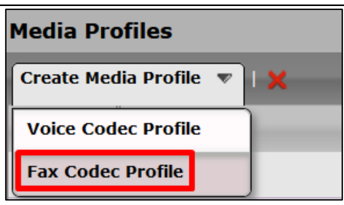
Description	Codec	Payload Size	Comments
G.722	G.722	20 ms	
Default G711A	G.711 A-Law	20 ms	
G.729	G.729	20 ms	
Default G711U	G711 U-Law	20 ms	Optional on request

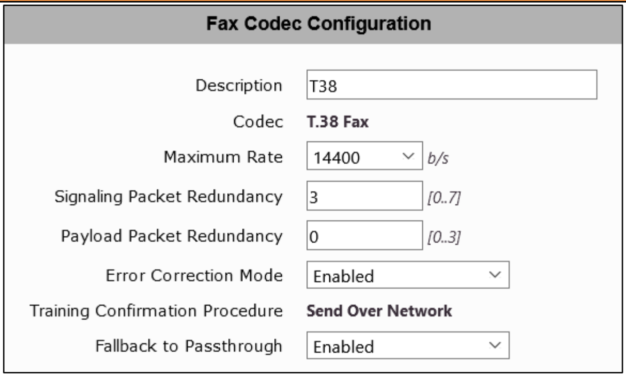
Voice Codecs

Actions	Screenshot
1. Go to *Media* > *Media Profiles* menu path	
2. Click on the *Create Media Profile* > *Voice Codec Profile* icon	

Actions	Screenshot
3. Set G711 A codec configuration	
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	

Actions	Screenshot
3. Set T38 codec configuration	

Note:

for SBC 1000 and SBC 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 SBC will be able to convert SIP INFO message to RFC2833/4733. On SWE Lite, the License with partial RTP media manipulation is required.

The SBC 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):

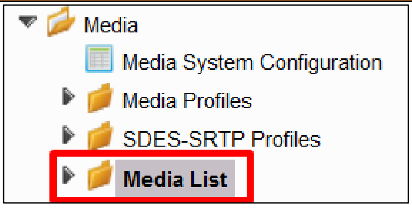
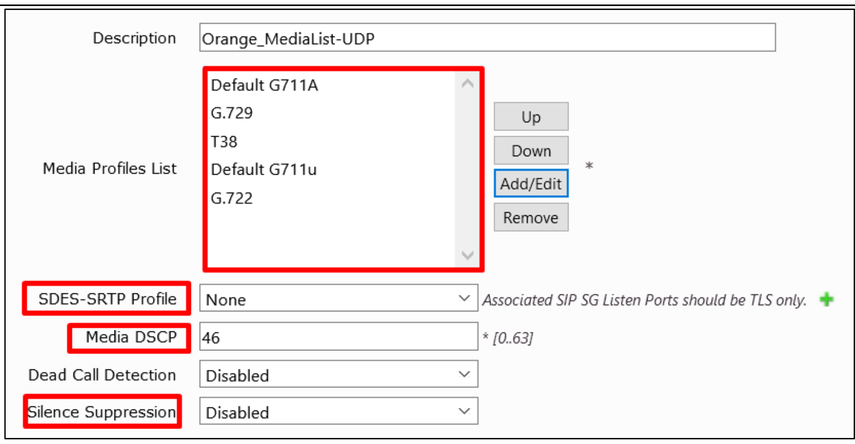
Even if this not the standard behaviors, some customer IPBX/device could send several "codec" in the SDP answer (SDP with multiple codecs into Audio M Lines). This behavior is not supported by Orange BTalk network. As solution on the Ribbon SBC, it is required to implement a different "Media List" to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

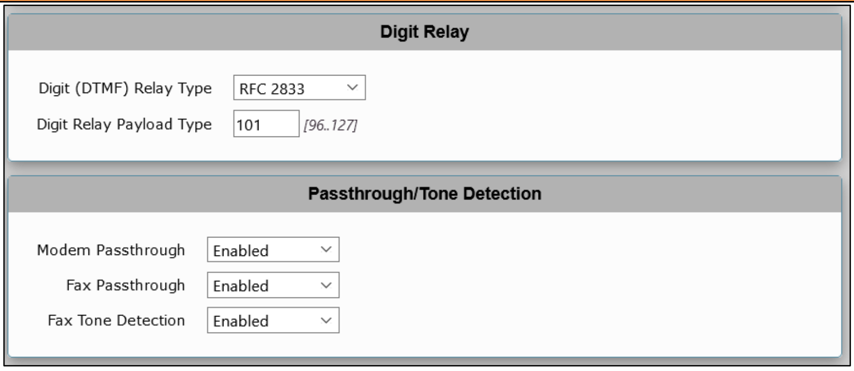
We are going to create a new “Media list” specific to Orange BTalk.

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

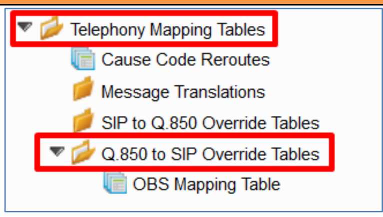
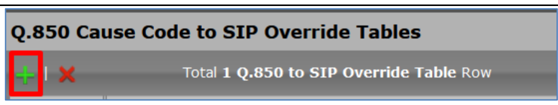
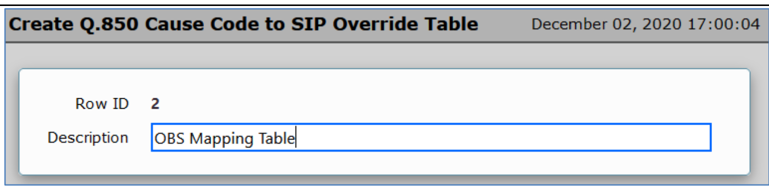
<u>OBS UDP Media List (Orange_MediaList-UDP)</u>

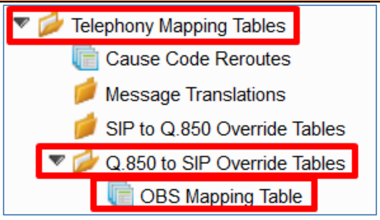
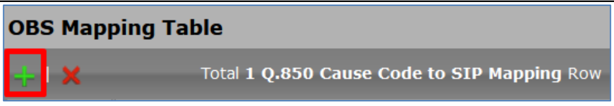
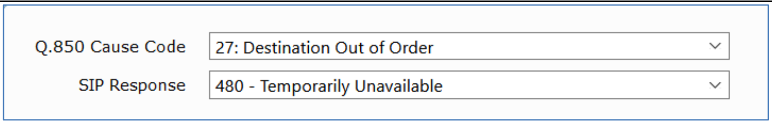
Actions	Screenshot
1. Go to *Media > Media List* menu path	
2. To add a new *Media List,* click on the *plus icon (+).*	
3. Set Media List configuration	

<table>
<tr><th>Actions</th><th>Screenshot</th></tr>
<tr><td></td><td>
</td></tr>
</table>

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 SBC 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.

<table>
<tr><th>Actions</th><th>Screenshot</th></tr>
<tr><td>1. Go to Telephony Mapping Tables > Q.850 to SIP Override Tables menu path</td><td>
</td></tr>
<tr><td>2. To add a new Q.850 to SIP Override Table, click on the plus icon (+).</td><td>
</td></tr>
<tr><td>3. Set the Description</td><td>
</td></tr>
</table>

Actions	Screenshot
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 SBC 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.

SBC 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:

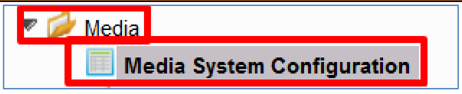
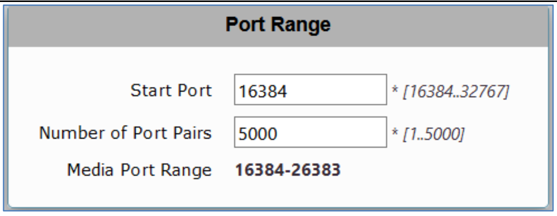
The minimum and maximum port numbers supported by the SBC SWe Lite are 16384, 32767, respectively.
The maximum number of port pairs supported by the SBC SWe Lite is 5000.

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

<u>To determine the last corresponding port number</u>:

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

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 SBC.

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

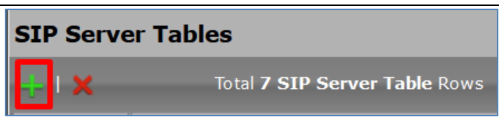
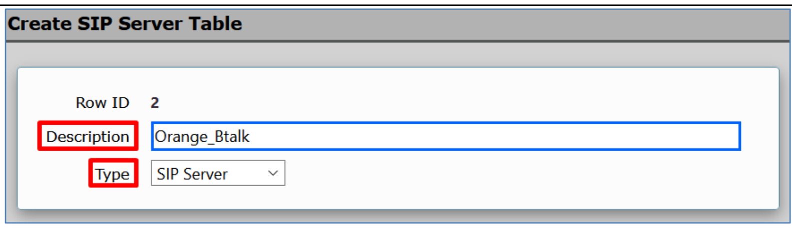
The mentioned parameters in the tables below are the one specific to Orange Profile. All the other parameters must be left as «default value».

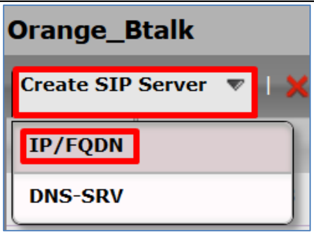
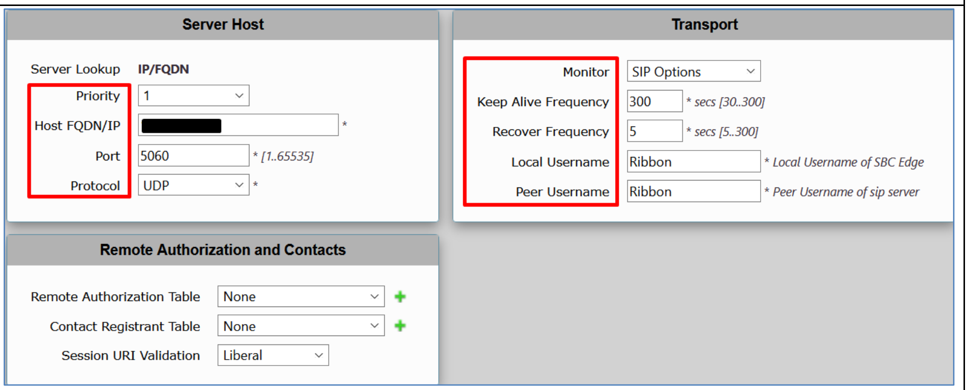
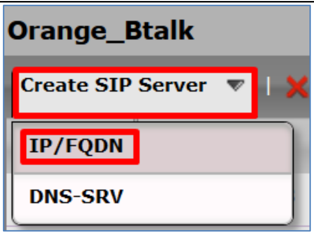
OBS BTalk/BTIP

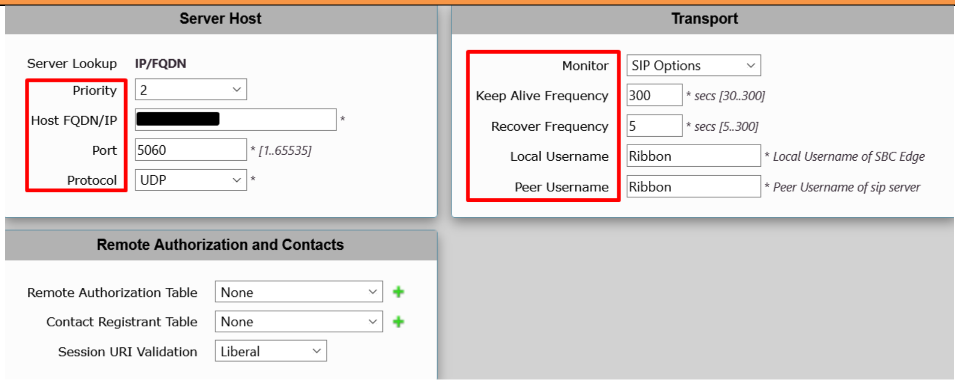
Priority	Host FQDN/IP	Port	Protocol	Transport
1	<BT_Nominal_IP>	5060	UDP	Monitor: Sip Options Keep Alive Frequency: 300 Recovery frequency: 5
2	<BT_Backup_IP>	5060	UDP	Monitor: Sip Options Keep Alive Frequency: 300 Recovery frequency: 5

Note:

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 SBC to verify if the Orange BTalk/BTIP network is reachable.
All the screenshots below showing some IP address are given as example. You should replace them by the correct IP or FQDN.

Actions	Screenshot
1. 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	

<table>
<tr><th>Actions</th><th>Screenshot</th></tr>
<tr><td>4. On the left menu path, click on the SIP Server Table you have just created</td><td>
</td></tr>
<tr><td>5. Click on the IP/FQDN icon to add a new entry</td><td>
</td></tr>
<tr><td>6. Set the first entry as the right picture. Host FQDN/IP being the <BT_Nominal_IP></td><td>
</td></tr>
<tr><td>7. Repeat step 5 to add a new entry. Host FQDN/IP being <BT_Backup_IP></td><td>
</td></tr>
</table>

Actions	Screenshot
8. Set the second entry 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».

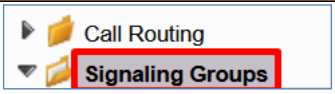
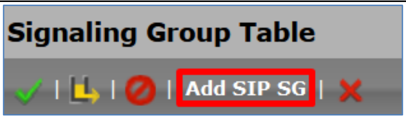
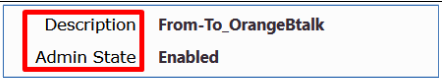
Description	Call Routing Table	SIP Profile	SIP Server Table	Media List ID	Federated IP/FQDN
From-To_OrangeBtalk	To_IPPBX	Orange_SIPProfile-UDP	Orange_Btalk	Orange_Media List-UDP	<BT_Nominal_IP> <BT_Backup_IP>

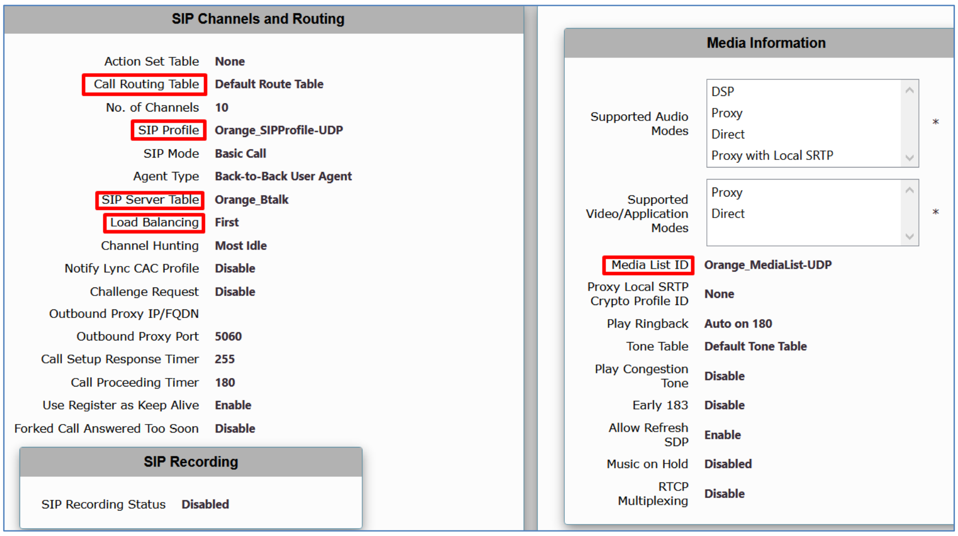
Description	Signaling DSCP	Inbound Message Manipulation	Outbound Message Manipulation
From-To_OrangeBtalk	46	N/A	OBS_SIP_ Profile_Adaptation_02
			OBS_SIP_ Profile_Adaptation_01
			Add_P-Early-Media

Note:

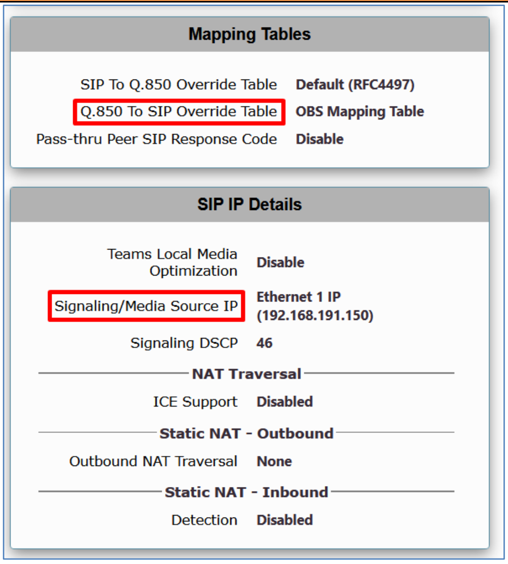
‘Call Routing Tables’ *will be defined in the next section* *2.5.12 Configure Voice routing*. *Therefore, we will use the default Route Table to define the Signaling Groups; this parameter will be modified in the next section.*

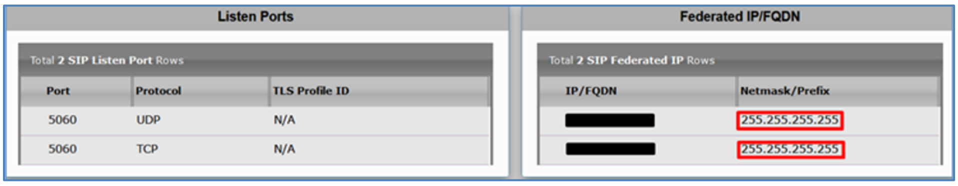
From-To_OrangeBTalk/BTIP

<table>
<tr><th>Actions</th><th>Screenshot</th></tr>
<tr><td>1. On the left menu go to the Signaling Groups menu path</td><td>
</td></tr>
<tr><td>2. To add a new SIP Signaling Group, click on the Add SIP Signaling Group icon.</td><td>
</td></tr>
<tr><td>3. Configure the new Signaling Group as per right picture.
Remember to use the Default Route Table in the Call Routing Table field, this parameter will be modified once the correct table is defined.
In the Signaling/Media Source IP field select the IP interface as per your network design.
In the Federated IP/FQDN field set the <BT_Nominal_IP> and <BT_Backup_IP> values</td><td>


</td></tr>
</table>

<table>
<tr><th>Actions</th><th>Screenshot</th></tr>
<tr><td></td><td>



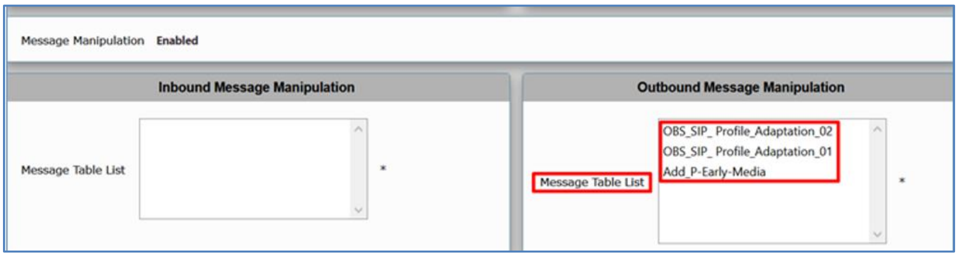


</td></tr>
<tr><td>

4. 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

</td><td>



</td></tr>
</table>

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 :

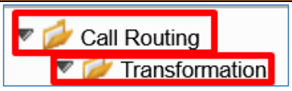
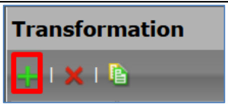
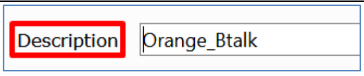
> *These tables are one of the central connection points of the SBC, linking [Transformation Tables](), [Message Translations](), [Cause Code Reroute Tables](), [Media Lists]() and the three types of Signaling Groups ([ISDN](), [SIP]() and [CAS]()). For information on the Ribbon SBC call routing system 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 SBC 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:

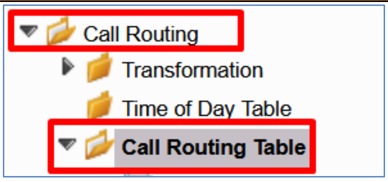
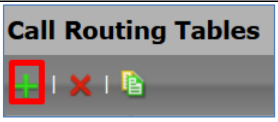
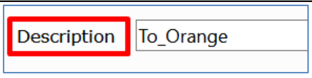
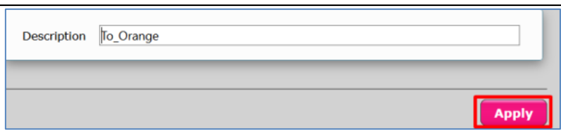
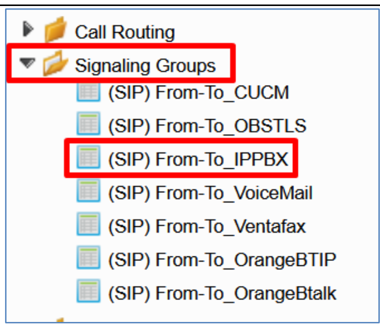
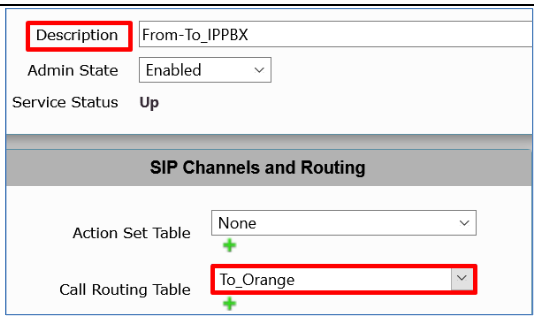
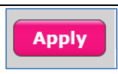
Go to [Section 2.7.1]() to have more information regarding how to create transformation entries.

Configure Call Routing Table

Description	Name
Call Routing Table	To_Orange

Call Routing Table	To_IPPBX

_To_Orange Table_

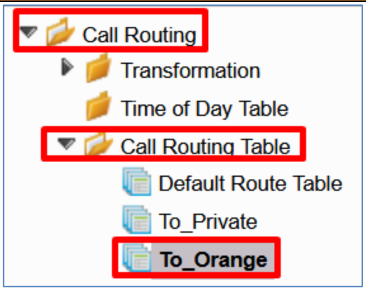
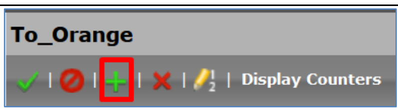
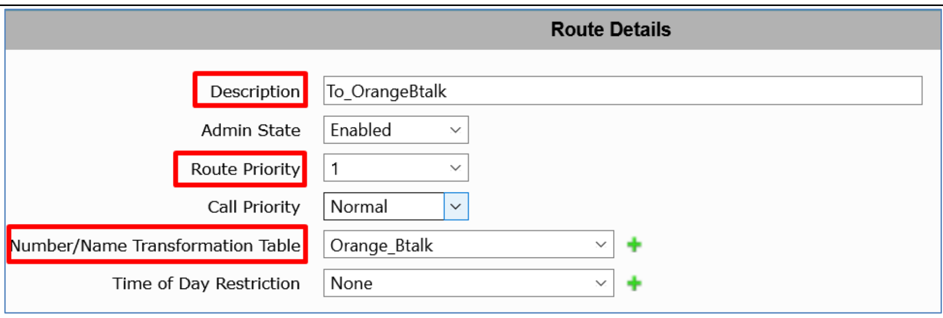
Actions	Screenshot
1. On the left menu go to the *Call Routing > Call Routing table* menu path	
2. To add a new *Call Routing Table,* click on the *plus icon (+).*	
3. Set the *Description* of the new table	
4. Commit the changes by clicking on the Apply icon	
5. On the left menu, go to the *From-To_IPPBX*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

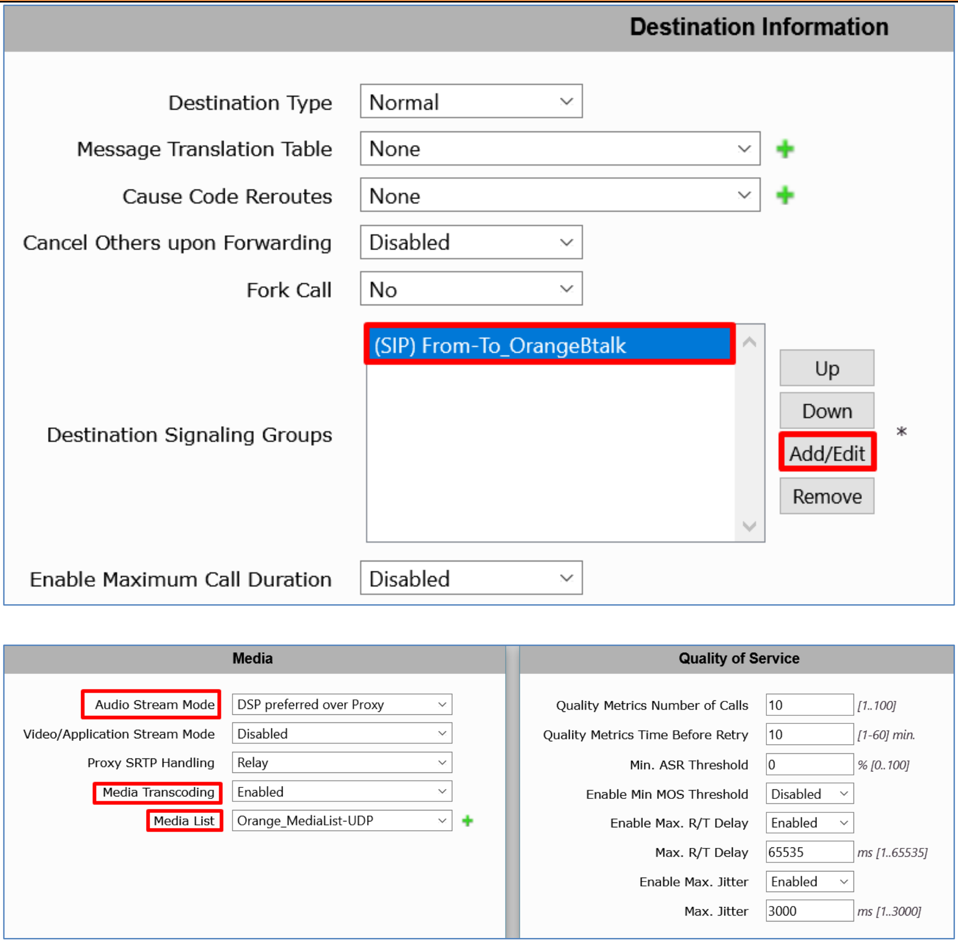
_To_Orange Call Route Entries_

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

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

_To_Orange_

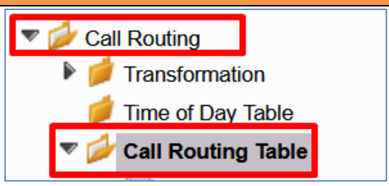
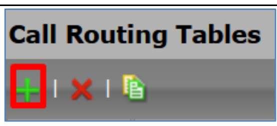
Actions	Screenshot
1. On the left menu path click on the *To_Orange* table you created	
2. To add a new entry, click on the *plus icon (+).*	
3. Set the new *Call Route* as per right picture. Under *Number/Name Transformation Table*, select the table 'Orange_Btalk' previously created – see above Under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

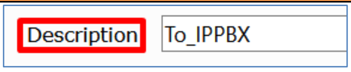
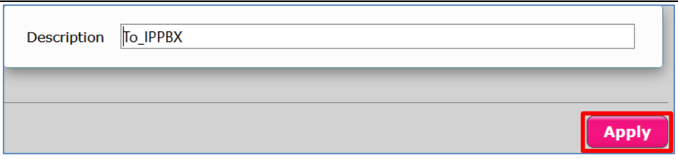
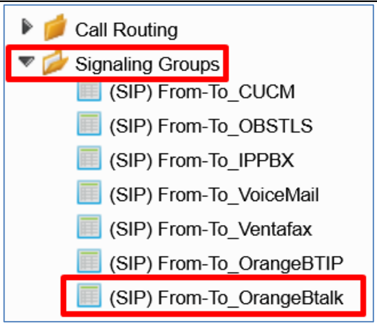
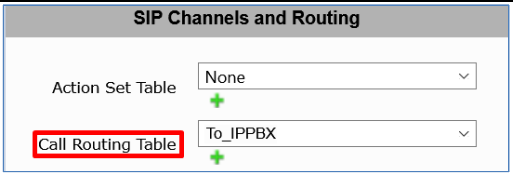
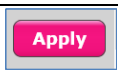
Actions	Screenshot
	

Note:

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

To_IPPBX Table

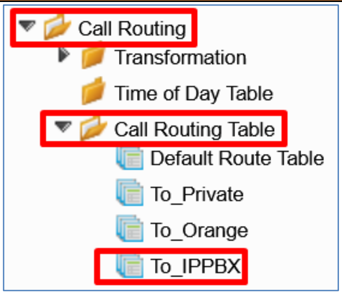
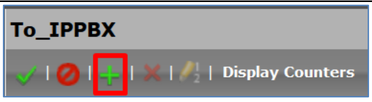
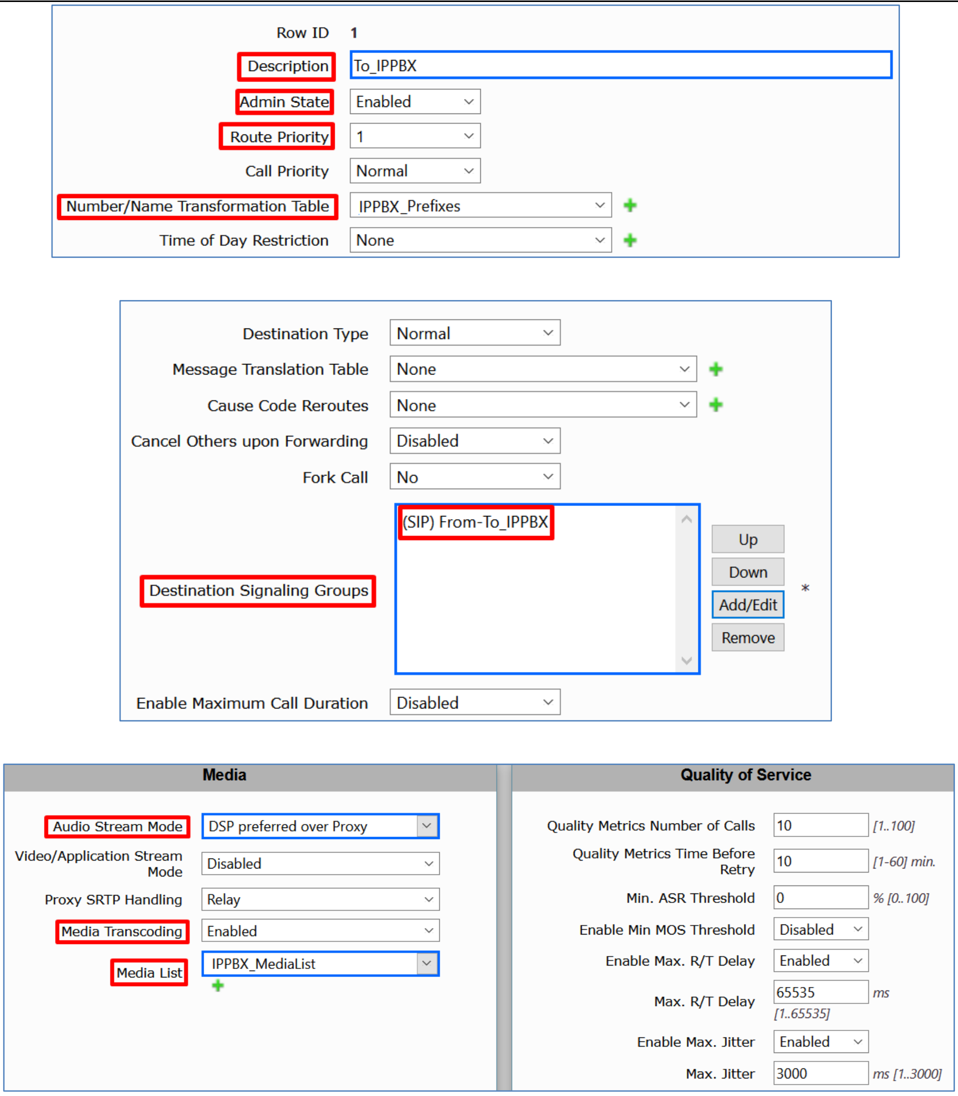
Actions	Screenshot
1. On the left menu go to the *Call Routing > Call Routing table* menu path	
2. To add a new *Call Routing Table,* click on the *plus icon (+).*	

Actions	Screenshot
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 OBS	
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 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 OBS Business Talk over Internet & BTIP over Internet Carrier North encrypted SIP configuration for Ribbon SBC (TLS)

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

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 SBC 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 SBC with FQDN name "SBC123@TOTO.com" resolving Public IP 83.206.61.113

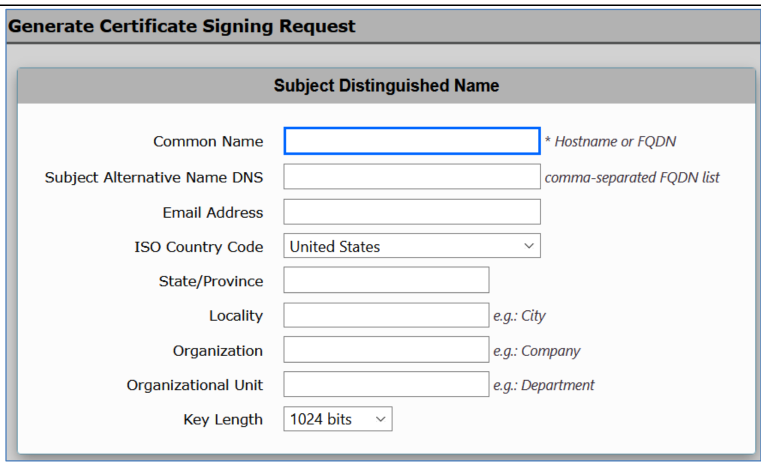
Common Name	Organizational Unit	Company name	Locality or city name	Country code
SBC123@COMPANY.com	-	COMPANy Enterprise	Paris	FR

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

As soon you received the CA Root/Intermediate, you will have to load those on the Ribbon eSBC on the TLS Context created for this interconnection with Orange BTALK.
Request a 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 need to ensure their eSBC FQDN's must be resolved through a public DNS before generating the CSR

Actions	Screenshot
1. On the left menu path click on *Generate SBC Edge CSR*	
2. Complete the information requested by the SBC. Note: This information will be used to generate the certificate	
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 SBC.

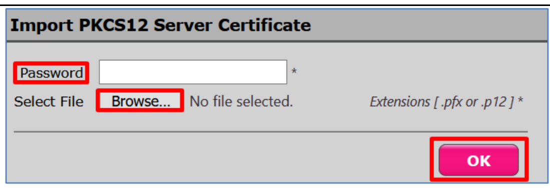
Make sure that the file is a plain-text file containing the "BEGIN CERTIFICATE" header, as shown in the example of a Base64-Encoded X.509 Certificate below:


```
-----BEGIN CERTIFICATE-----
MIIDkzCCAnugAwIBAgIEAgAAADANBgkqhkiG9w0BAQQFADA/MQswCQYDVQQGEwJGUjETMBEGA1UEChMKQ2VydGlwb3N0ZTEbMBkGA1UEAxM
SQ2VydGlwb3N0ZSBTZXJ2ZXVyMB4XDTk4MDYyNDA4MDAwMFoXDTE4MDYyNDA4MDAwMFowPzELMAkGA1UEBhMCRlIxEzARBgNVBAoTCkNlcn
RpcG9zdGUxGzAZBgNVBAMTEkNlcnRpcG9zdGUgU2VydmV1cjCCASEwDQYJKoZIhvcNAQEBBQADggEOADCCAQkCggEAPqd4MziR4spWldGRx
8bQrhZkonWnNm`+Yhb7+4Q67ecf1janH7GcN/SXsfx7jJpreWULf7v7Cvpr4R7qIJcmdHIntmf7JPM5n6cDBv17uSW63er7NkVnMFHwK1Qa
GFLMybFkzaeGrvFm4k3lRefiXDmuOe+FhJgHYezYHf44LvPRPwhSrzi9+Aq3o8pWDguJuZDIUP1F1jMa+LPwvREXfFcUW+w==
-----END
```

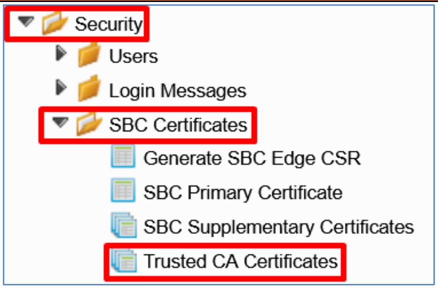
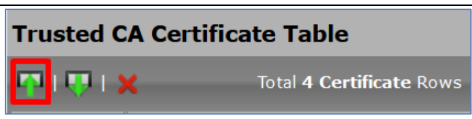
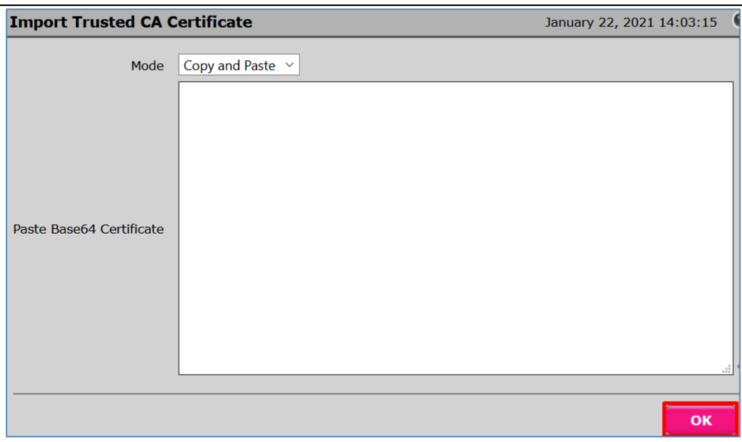
STEP 2: Deploy the SBC and Root/Intermediate Certificates on the SBC

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

SBC Certificate

Actions	Screenshot
1. On the left menu path click on *SBC 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. **8.** Click on the *OK* icon	

Root / Intermediate Certificates:

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: Send Public CA Root and Intermediate if exist Certificates which signed your eSBC certificate to Orange BTALK Team

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.

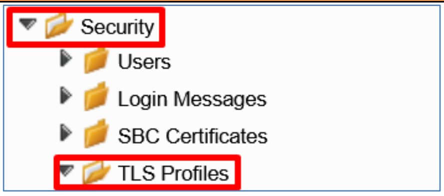
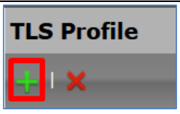
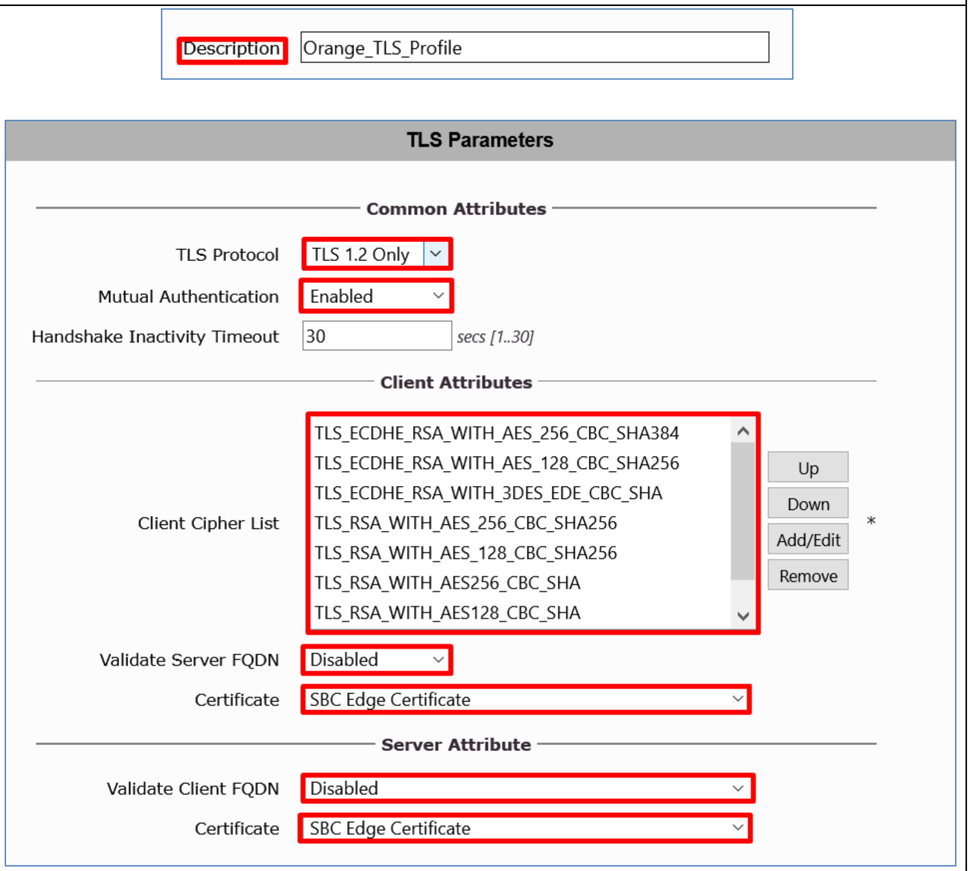
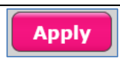
This SIP signaling will be configured to be compliant with Orange BTalk specifications:

- ✓ For **encrypted BTALK/BTIP SIP Trunk** architecture we need to configure **TLS V1.2**
- ✓ **Key size 2048**
- ✓ **Cipher list is supported as Cipher Client/Server:**
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (Recommended)
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- ✓ **TLS Mutual authentication activate**

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

Parameter	Value
TLS Profile	TLS Orange
TLS protocol	TLS 1.2 Only
Mutual Authentication	Enabled
Client Cipher	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
Validate Server FQDN	Disabled
Client Certificate	<SBC Edge Certificate>
Validate Client FQDN	Disabled
Server Certificate	<SBC Edge Certificate>

Note:
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 *is the highest cipher supported on Ribbon SBC.*

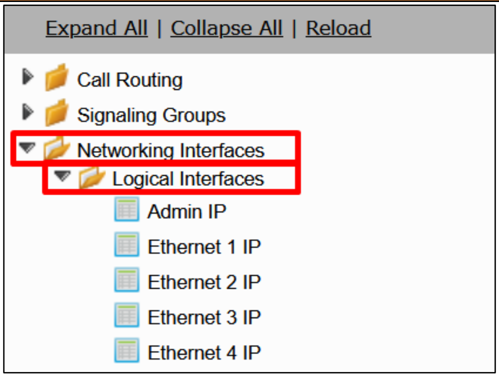
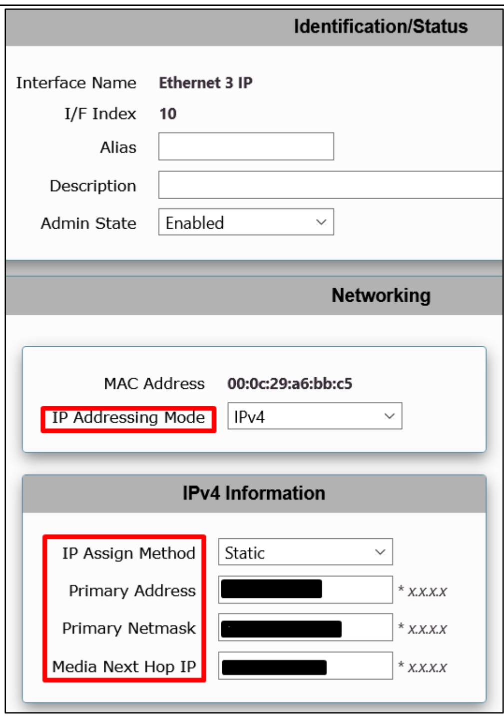
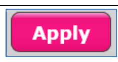
<table>
<tr><th>Actions</th><th>Screenshot</th></tr>
<tr><td>1. On the left menu path click on TLS Profiles</td><td></td></tr>
<tr><td>2. Click on the Create TLS Profile Icon</td><td></td></tr>
<tr><td>3. Set the configuration as per right picture.
Caution: Do not change the client cipher order.</td><td></td></tr>
<tr><td>4. Click on the Apply icon</td><td></td></tr>
</table>

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.

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

<table>
<tr><th>Actions</th><th>Screenshot</th></tr>
<tr><td>1. Go to Networking Interfaces > Logical Interfaces menu path</td><td>
</td></tr>
<tr><td>2. Click on the Ethernet interface you want to configure and set the IP information.</td><td>
</td></tr>
<tr><td>3. Click on the Apply icon</td><td>
</td></tr>
<tr><td>4. Repeat steps 2 and 3 in case you want to configure additional Ethernet interfaces as per your network topology</td><td></td></tr>
</table>

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 SBC 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 SBC 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. SBC 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, SBC PRACK Mode: Mandatory on the SIP profile of the Customer IPPBX.

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

The SBC 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.

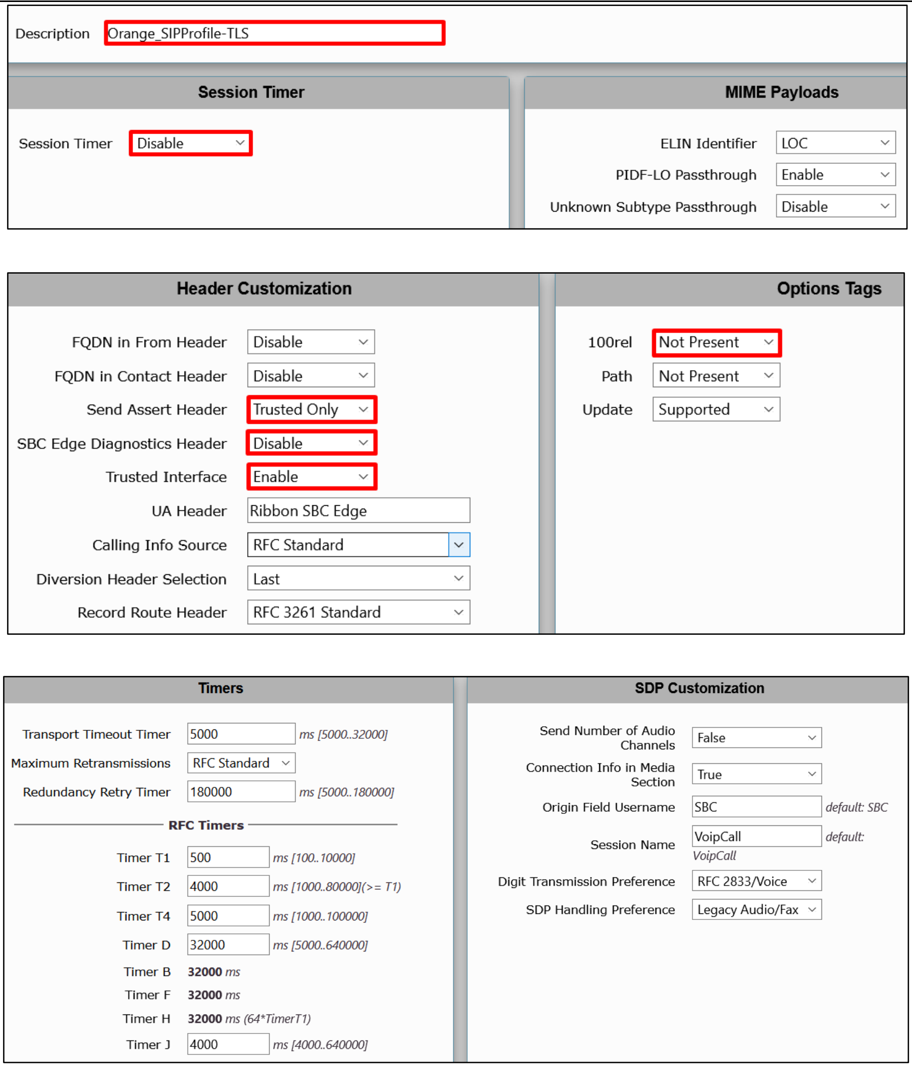
The mentioned parameters in the table below are the one specific to Orange Profile. All the other parameters must be left as «default value».

Description	Parameter	Value
When enabled (set as **Always**), the SBC 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 SBC support 100rel (PRACK support)	100rel	Not Present
Specifies if the **X-SBC Edge -Diagnostics** header is added to the outbound SIP signaling messages	SBC Edge Diagnostics Header	Disable

Orange_SIP Profile-TLS

<table>
<tr><th>Actions</th><th>Screenshot</th></tr>
<tr><td>1. Go to SIP > SIP Profiles menu path</td><td>


</td></tr>
<tr><td>2. To add a new SIP Profile click on the plus icon (+).</td><td>


</td></tr>
<tr><td>3. Set the SIP Profile parameters as per right picture</td><td>


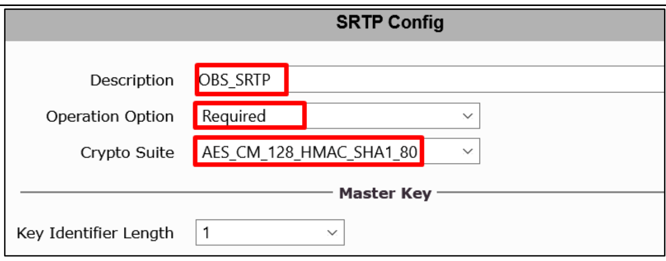
</td></tr>
</table>

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	OBS_SRTP
Specifies the manner in which 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

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

Note:

known Issue: SBC Edge doesn't support Fax T.38 UDP conversion to FAX T.38 TLS. It will be fixed 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 SBC will be able to **convert SIP INFO** message to RFC2833/4733. DTMF inbound will be not converted by the SBC because it requires DSP resources on SBC.*

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

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

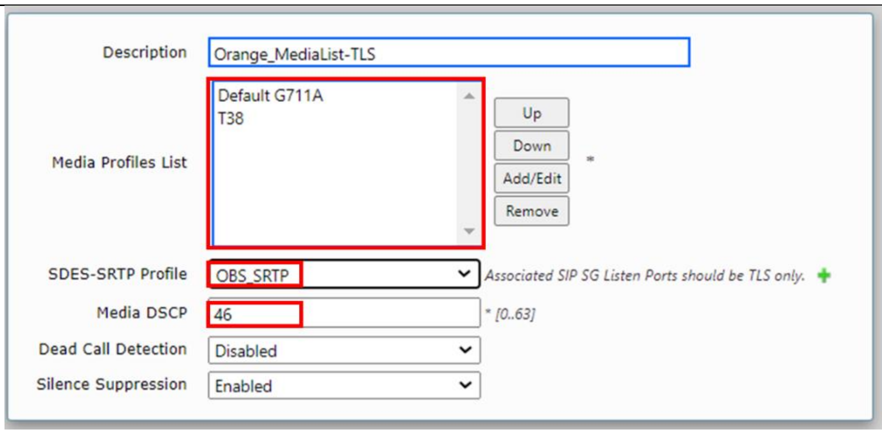
Even if this not the standard behaviors, some customer IPBX/device could send several "codec" in the SDP answer (SDP with multiple codecs into Audio M Lines). This behavior is not supported by Orange BTalk network. As solution on the Ribbon SBC, it is required to implement a different "Media List" to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

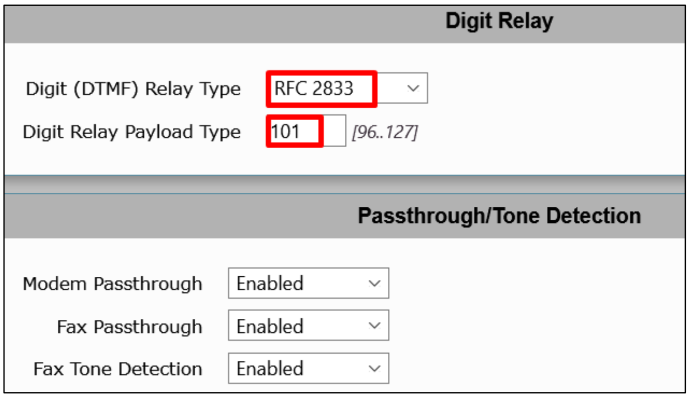
We are going to create a new “Media list” specific to Orange BTalk/BTIP.

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

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

OBS TLS Media List (Orange_MediaList-TLS)

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


</td></tr>
</table>

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 2.5.8 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 SBC 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 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 BTalk TLS

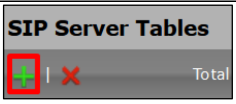
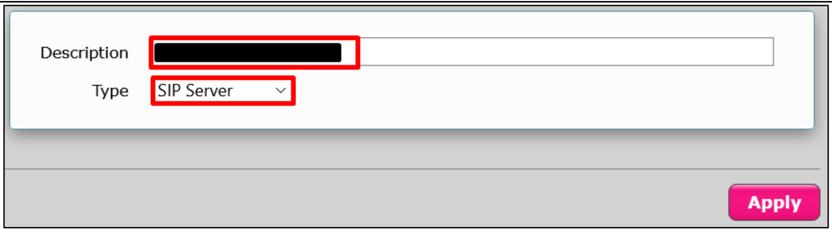
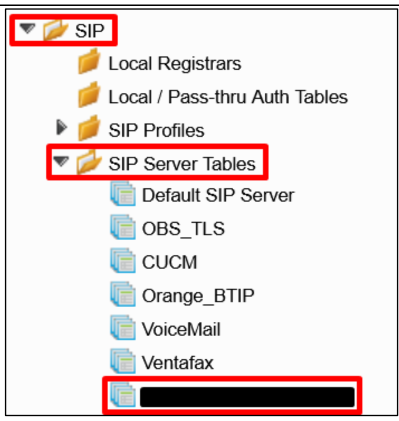
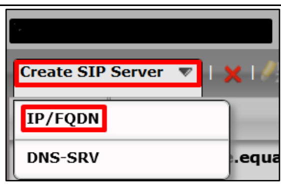
Priority	Host FQDN	Port	Protocol	TLS Profile	Transport
1	<BT_Public FQDN_Nominal >	5061	TLS	Orange_TLS_Profile	Monitor: Sip Options Keep Alive Frequency: 300 Recovery frequency: 5
2	< BT-Public_FQDN_FQDN_Backup >	5061	TLS	Orange_TLS_Profile	Monitor: Sip Options Keep Alive Frequency: 300 Recovery frequency: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

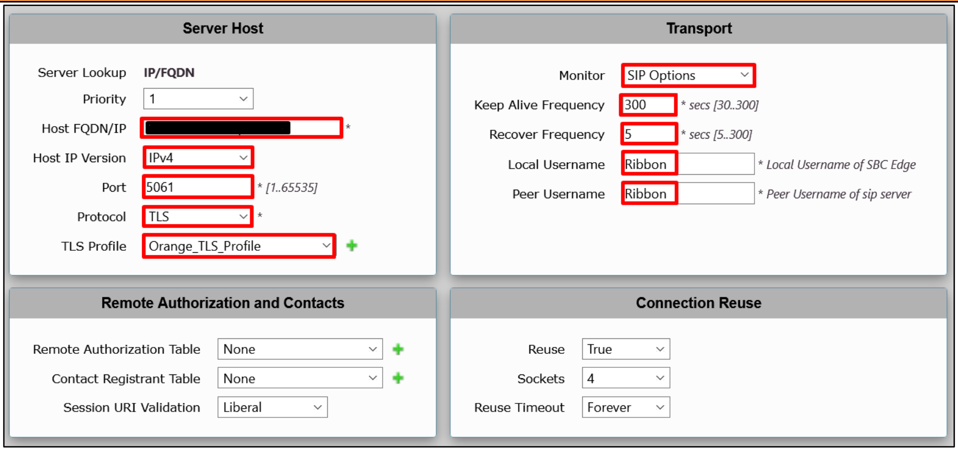
Note:

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 SBC to verify if the Orange BTalk network is reachable.
DNS Servers must be configured in System> Node-Level Settings section.

Note:

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

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 OBS FQDN	
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 OBS FQDN	
6. Click on the IP/FQDN icon to add a new entry **Note:** The table name is hidden as it is the public OBS FQDN	

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

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 (SBC 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_OBSTLS	To_IPPBX	Orange_SIPProfile-TLS	Orange_BTalk_TLS	Orange_Media List-TLS	< BT_Public FQDN_Nominal> <BT-Public_FQDN_FQ

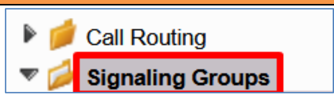
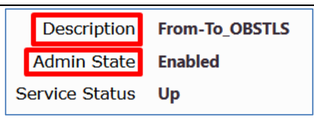
					DN_Backup>

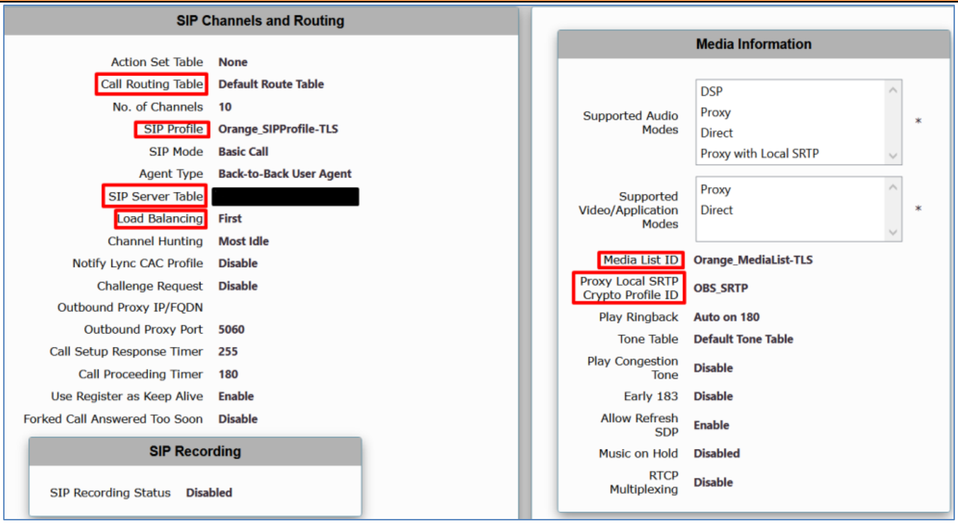
Description	Proxy Local SRTP Crypto Profile ID	Signaling DSCP	Inbound Message Manipulation	Outbound Message Manipulation
From-To_OBSTLS	OBS_SRTP	46	N/A	OBS_SIP_ Profile_Adaptation_02
				OBS_SIP_ Profile_Adaptation_01
				Add_P-Early-Media

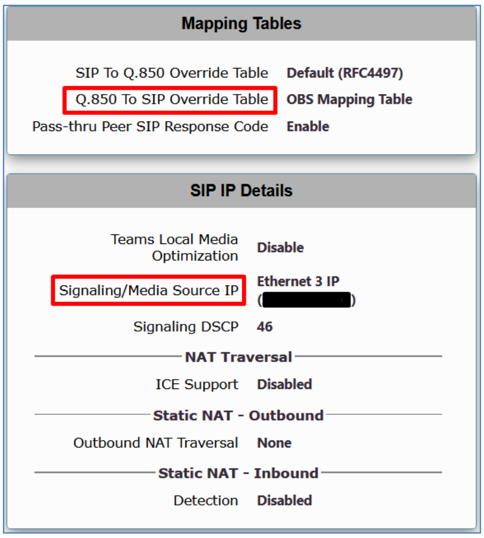
Note:

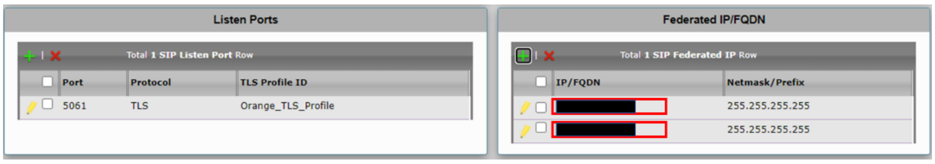
'Call Routing Tables' will be defined in the next section '[Configure Voice routing](#)' . Therefore, we will use the default Route Table to define the Signaling Groups; this parameter will be modified in the next section.

From-To_OBSTLS

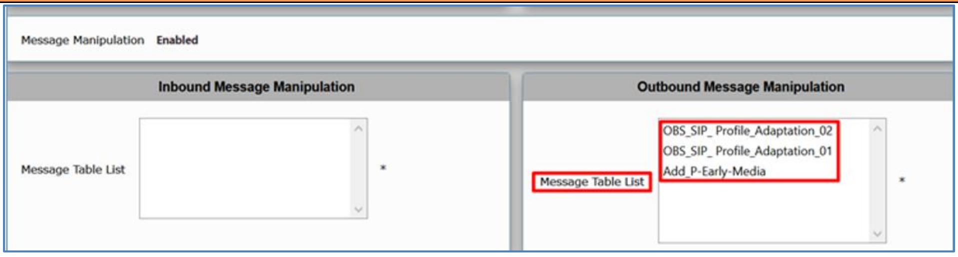
Actions	Screenshot
1. On the left menu go to the *Signaling Groups* menu path	
2. To add a new *SIP Signaling Group*, click on the *Add SIP SG icon.*	
3. Configure the new *Signaling Group* as per right picture. Remember to use the *Default Route Table* in the *Call Routing Table* field, this parameter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

<table>
<tr><th>Actions</th><th>Screenshot</th></tr>
<tr><td><i>Source IP</i> field select the IP interface as per your network design.
In the <i>Federated IP/FQDN</i> field set the < <i>BT_Public FQDN_Nominal</i> >
And the <<i>BT-Public_FQDN_FQDN_Backup</i>></td><td>






</td></tr>
<tr><td>4. 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.</td><td></td></tr>
</table>

Actions	Screenshot
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 :

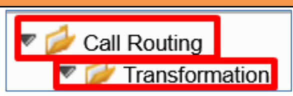
These tables are one of the central connection points of the SBC, linking Transformation Tables, Message Translations, Cause Code Reroute Tables, Media Lists and the three types of Signaling Groups (ISDN, SIP and CAS). For information on the Ribbon SBC call routing system as a whole, see Working with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

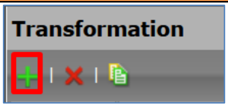
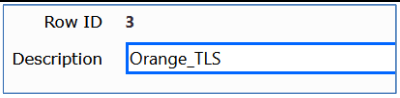
This document provides the minimum of configuration needed to route calls between the Signaling Group facing BTalk SIP trunk and the Signaling Group facing the IPPBX. You could be invited to customize them according to your own requirements.

Configure Transformation Table

Transformation Tables facilitate the conversion of names, numbers and other fields in the SIP signaling when the SBC 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	

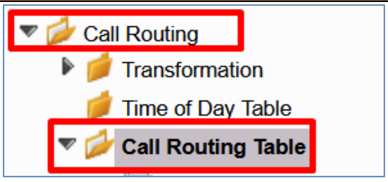
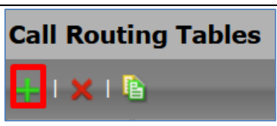
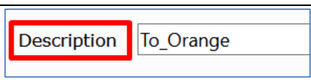
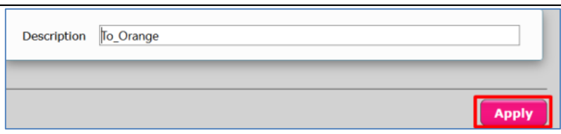
Actions	Screenshot
2. To add a new Transformation Table, click on the *plus icon (+).*	
3. Set the *Description* of the new table	

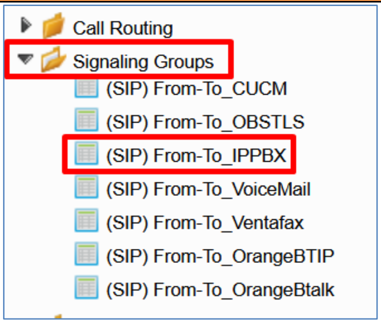
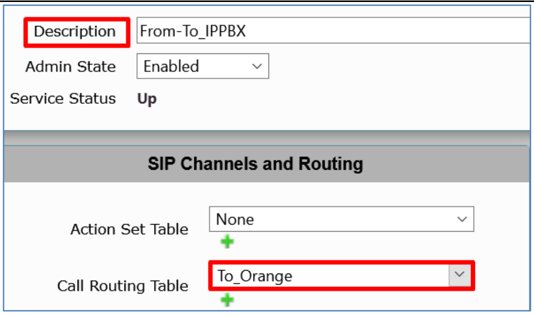
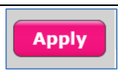
Note:
Go to *Section 2.7.1* to have more information regarding how to create transformation entries.

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	

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	

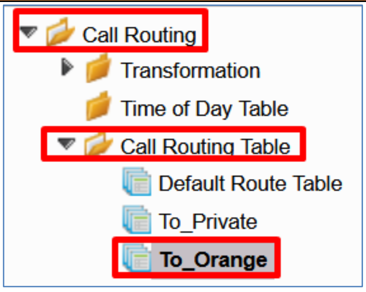
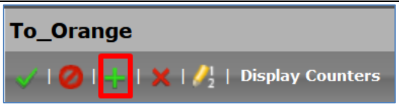
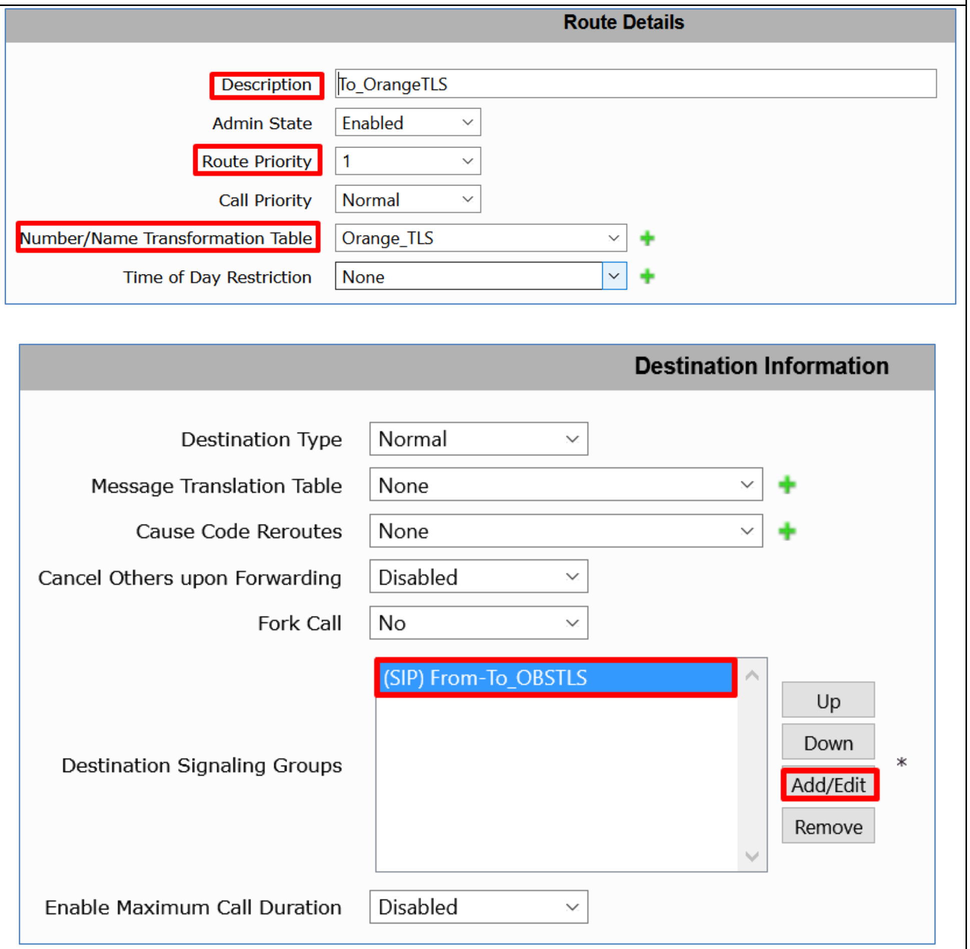
To_Orange Call Route Entries

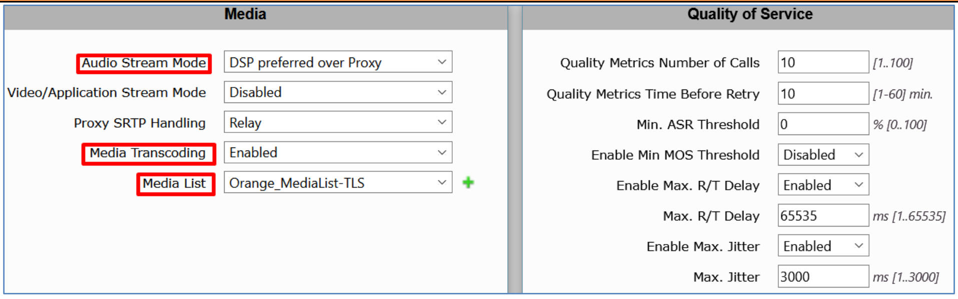
Description	Priority	Transformation Table	Signaling Group	Destination Type
To_OrangeBtalk	1	Orange_Btalk	From-To_OrangeBtalk	Normal
To_OrangeTLS	1	Orange_TLS	From-To_OBSTLS	Normal

Note:

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

To_OrangeTLS

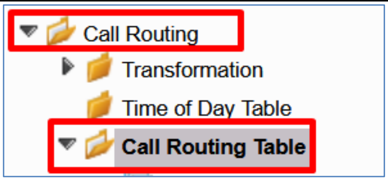
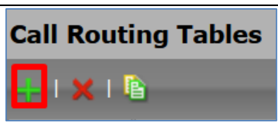
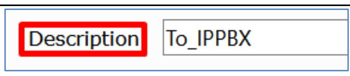
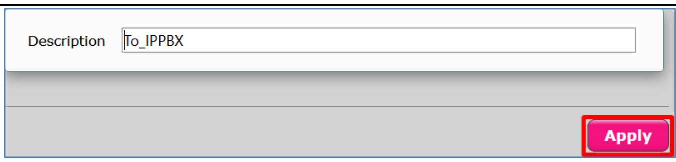
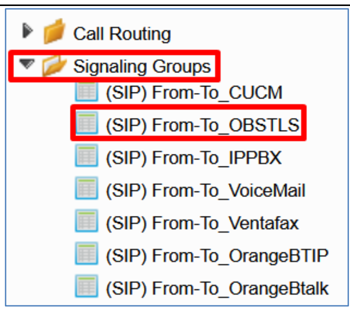
Actions	Screenshot
1. On the left menu path click on the *To_Orange* table you created	
2. To add a new entry, click on the *plus icon (+).*	
3. Set the new *Call Route* as per right picture. Under *Number/Name Transformation Table*, select the table 'Orange_TLS' previously created – see above Under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

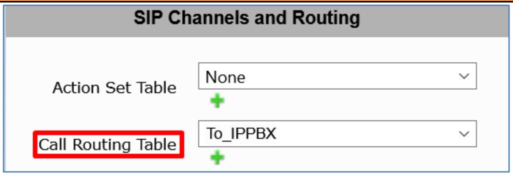
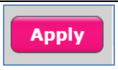
Actions	Screenshot
	

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_OBSTLS* Signaling Group. Note: it is the name of the Signaling Group facing OBS TLS	

<table>
<tr><th>Actions</th><th>Screenshot</th></tr>
<tr><td>6. Edit the Signaling Group by selecting To_IPPBX in the Call Routing Table field.</td><td>
</td></tr>
<tr><td>7. Commit the changes by clicking on the Apply icon</td><td>
</td></tr>
</table>

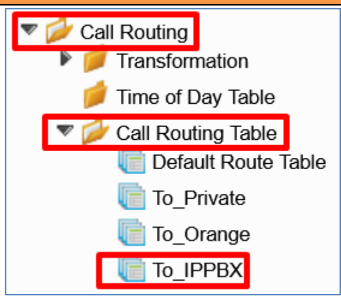
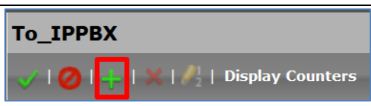
Note:

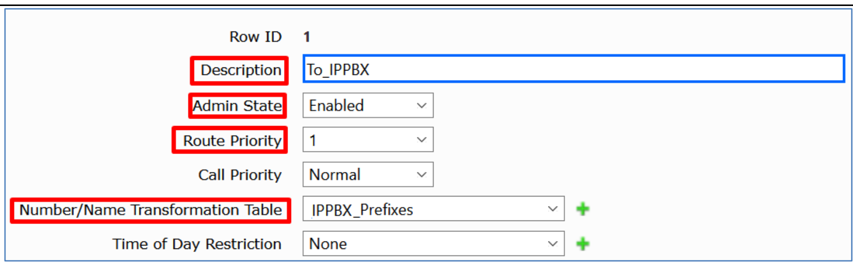
The Call Routing Table 'To_IPPBX' *shall be used within the Signaling group facing to the Orange BTalk Trunk.*

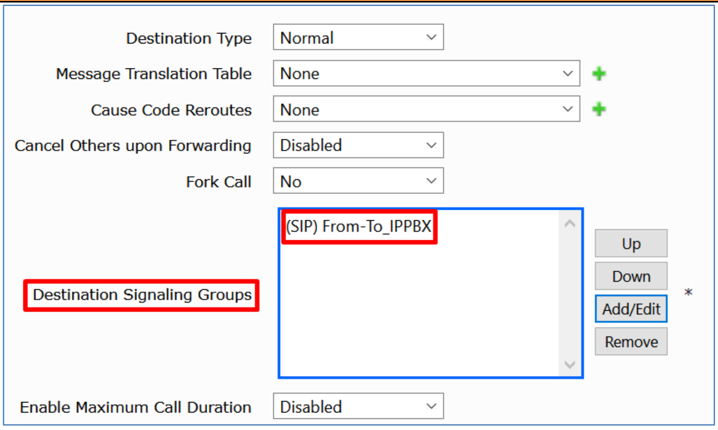
To_IPPBX Call Route Entries

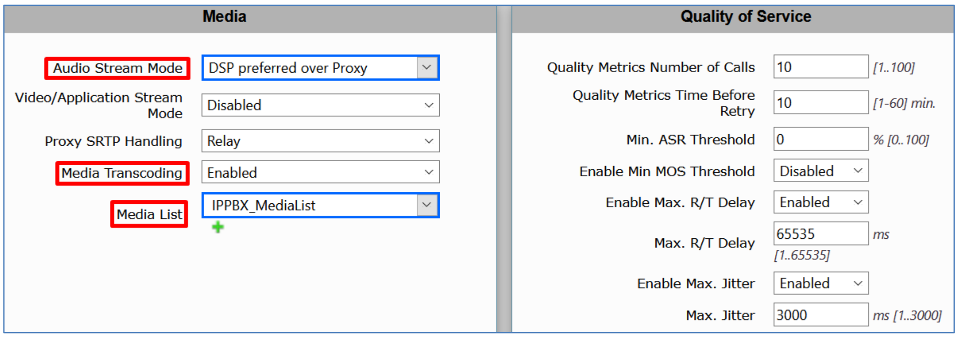
Description	Priority	Transformation Table	Signaling Group	Destination Type
To_IPPBX	1	IPPBX_Prefixes	From-To_IPPBX	Normal

To_IPPBX

<table>
<tr><th>Actions</th><th>Screenshot</th></tr>
<tr><td>1. On the left menu path click on the To_IPPBX table you created</td><td>
</td></tr>
<tr><td>2. To add a new entry, click on the plus icon (+).</td><td>
</td></tr>
<tr><td>3. Set the new Call Route as per right picture.

Under Number/Name Transformation Table, select the table 'IPPBX_Prefixes' previously created – see above</td><td>
</td></tr>
</table>

<table>
<tr><th>Actions</th><th>Screenshot</th></tr>
<tr><td>Under Destination Information section click on the Add/Edit icon to set the Destination Signaling Groups. It is the Signaling Group facing the IPPBX</td><td>


</td></tr>
</table>

2.7 SIP rules & manipulations (SBC Application)

This section provides the configuration regarding the device's SBC application, which is used for message rules & manipulations as described below. This chapter is common to Orange BTalk ASBC 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.

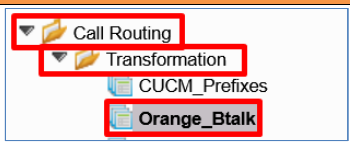
Note:

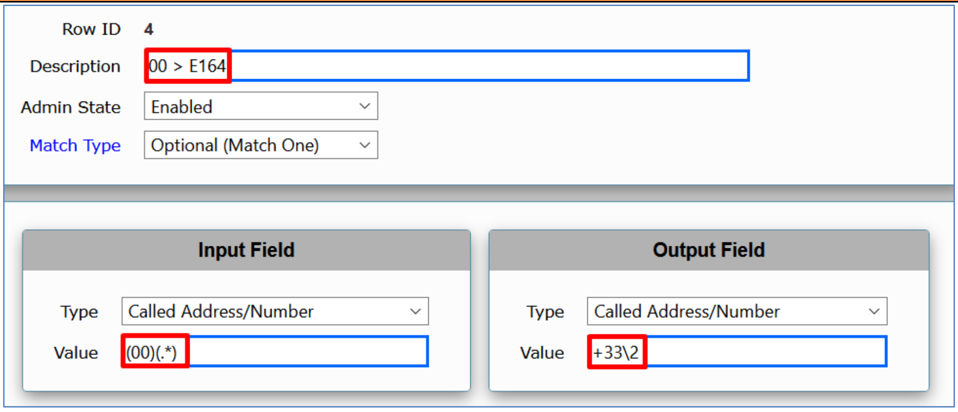
+CC prefix is the Country Code of the country where the SBC or IPBX is installed. It is up to the Customer to indicate the correct +CC. ex +33 for France.
If the IPBX is using a local dial plan (Private numbering Plan), then the manipulation has to adapted in consequence by the Customer.

Orange_BTalk Transformations

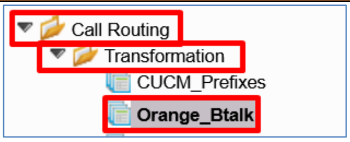
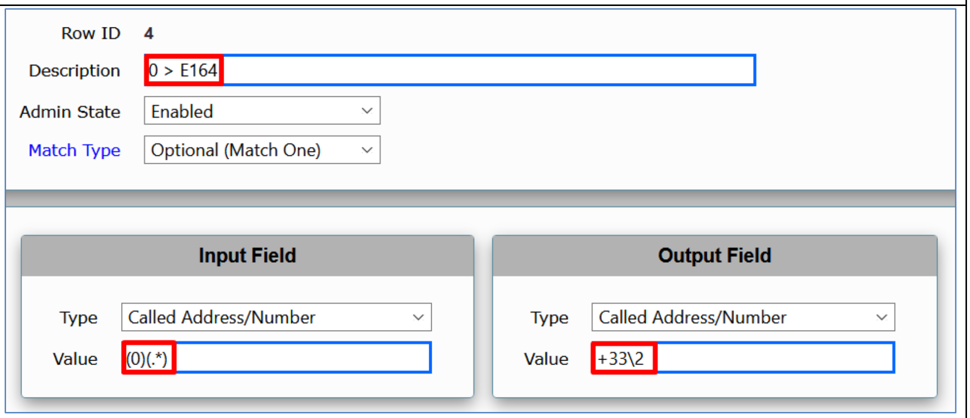
Description	Match Type	Input Field Type	Input Field Value	Output Field Type	Output Field Value
00 > E164	Optional (Match One)	Called Address/Number	(00)(.*)	Called Address/Number	+33\2
0 > E164	Optional (Match One)	Called Address/Number	(0)(.*)	Called Address/Number	+33\2
Add Plus Calling Number	Optional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

00 > E164

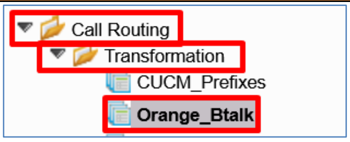
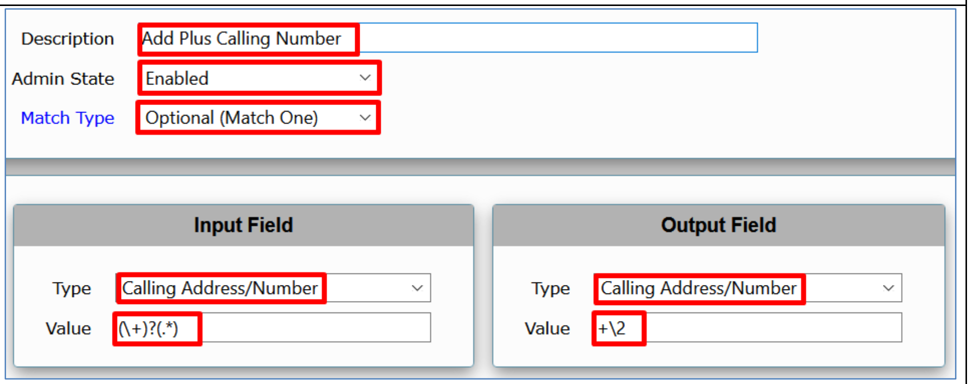
Actions	**Screenshot**
1. On the left menu path click on the *Orange_Btalk* table you created	
2. To add a new entry, click on the *plus icon (+).*	

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	

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	+33\2	Optional (Match One)	00 > E164
	Called Address/Number	(0)(.*)	Called Address/Number	+33\2	Optional (Match One)	0 > E164
	Calling Address/Number	(\+)?(.*)	Calling Address/Number	+\2	Optional (Match One)	Add Plus Calling Num...

2.7.2 SIP Messages Manipulations

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 SBC. 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.

Note:

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

Condition Rules

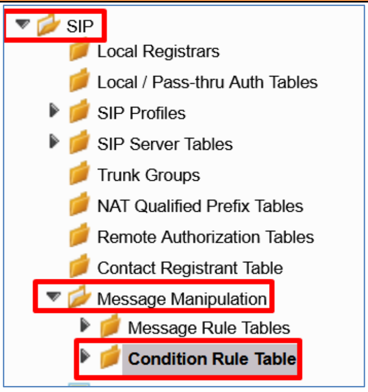
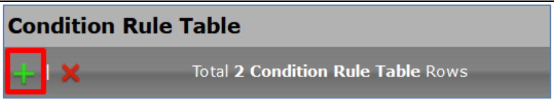
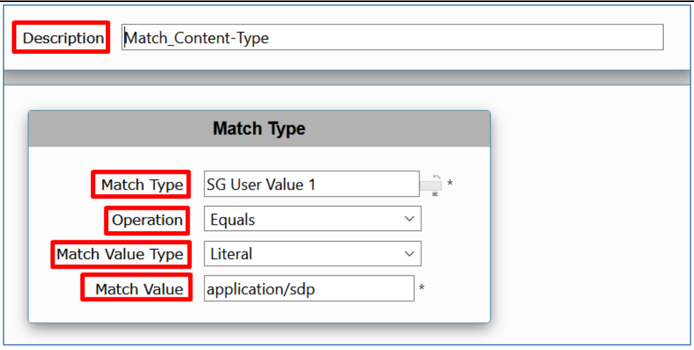
Description	Match Type	Operation	Match Value Type	Match Value
Match_Content-Type	SG User Value 1	Equals	Literal	application/sdp
Match_Anonymous	from.displayname	Equals	Literal	Anonymous

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 SBC to store a value on purpose.

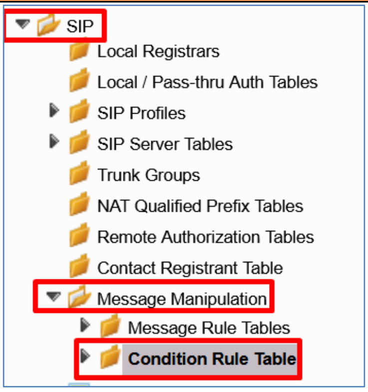
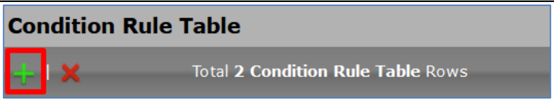
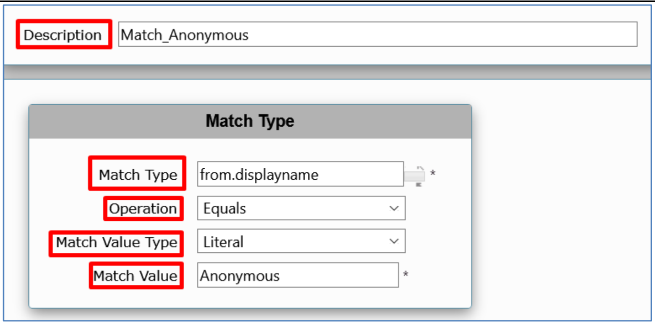
<table>
<tr><th>Actions</th><th>Screenshot</th></tr>
<tr><td>1. Go to the SIP > Message Manipulation > Condition Rule Table menu path</td><td>
</td></tr>
<tr><td>2. To add a new Condition Rule, click on the plus icon (+).</td><td>
</td></tr>
<tr><td>3. Set the new entry as per the right picture</td>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

<u>***Match_Anonymous***</u>

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 OBS (sip:anonymous@anonymous.invalid)

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

<u>Messages Rules Tables</u>

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

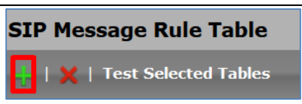
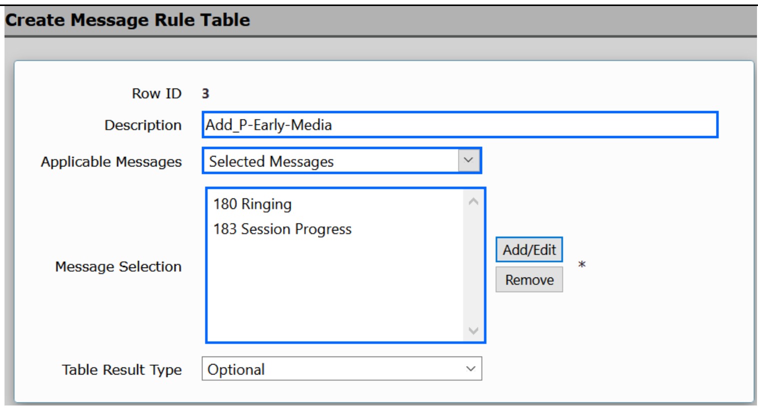
Description	Result Type	Message Type	Comments
Add_P-Early-Media	Optional	180, 183	It applies only to 180 and 183 respond messages
Store_Content-Type	Optional	180, 183	It applies only to 180 and 183 respond messages
Store_User-Agent_Value	Optional	All	It applies to all messages
OBS_SIP_ Profile_Adaptation_01	Optional	All	It applies to all messages
OBS_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
OBS_SIP_ Profile_Adaptation_01	This table collects the rules used to set the format as per chapter 1.4
OBS_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.

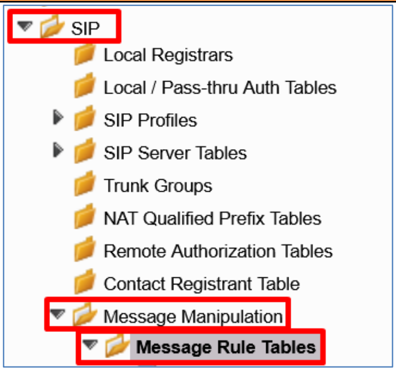
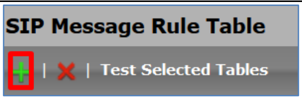
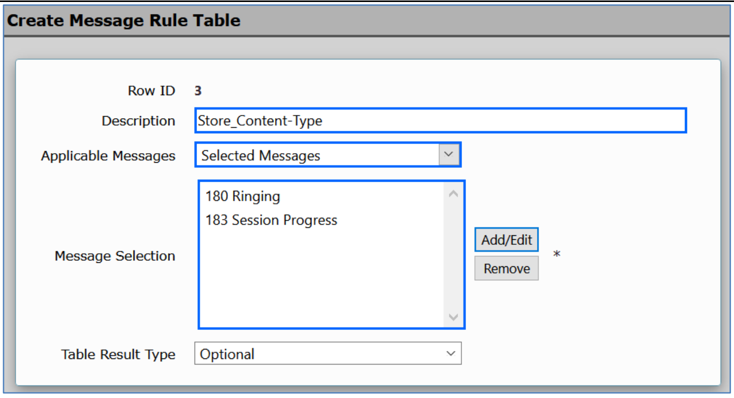
Actions	Screenshot
1. Go to the *SIP > Message Manipulation > Message Rule Tables* menu path	
2. To add a new *Message Rule Table*, click on the *plus icon (+).*	
3. Set the new entry as per the right picture	

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

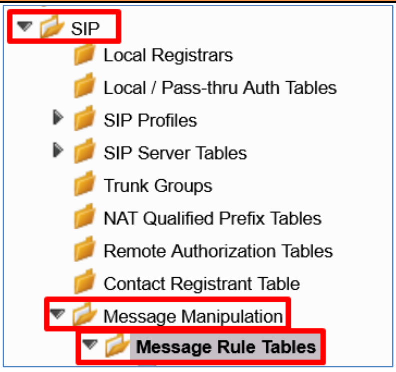
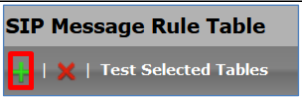
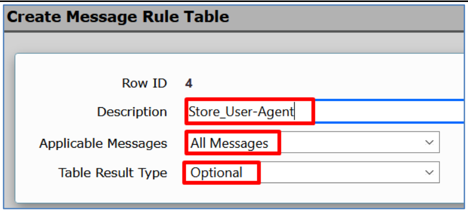
<table>
<tr><th>Actions</th><th>Screenshot</th></tr>
<tr><td>1. Go to the SIP > Message Manipulation > Message Rule Tables menu path</td><td>
</td></tr>
<tr><td>2. To add a new Message Rule Table, click on the plus icon (+).</td><td>
</td></tr>
<tr><td>3. Set the new entry as per the right picture</td>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

Store_User-Agent

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

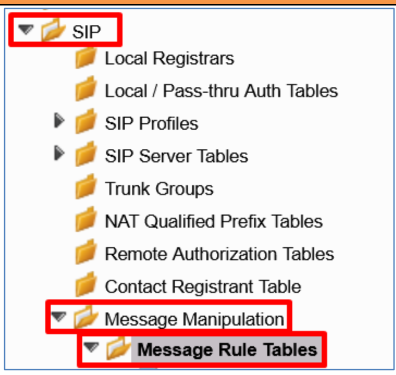
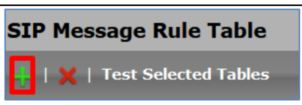
Note:

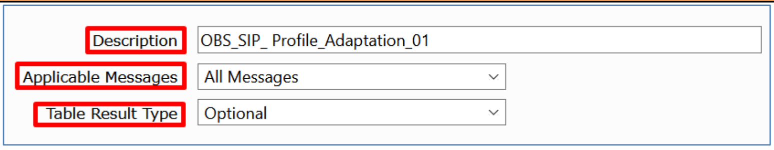
This table must be applied on the Signaling Group facing the IPPBX, set it as Inbound Message Manipulation

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

OBS_SIP_ Profile_Adaptation_01

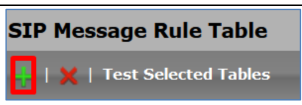
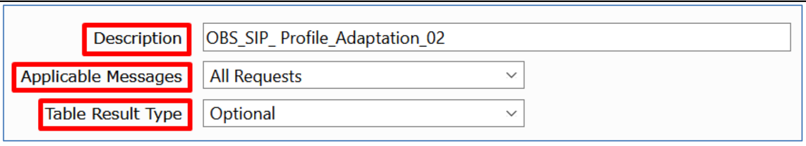
This table collects some rules that are used to accomplish the SIP format requested by OBS

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 (+).*	

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

OBS_SIP_ Profile_Adaptation_02

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

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)

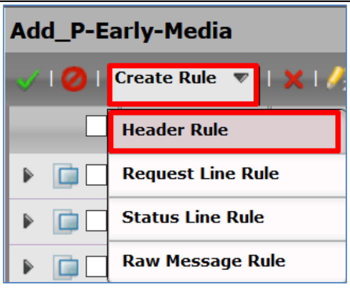
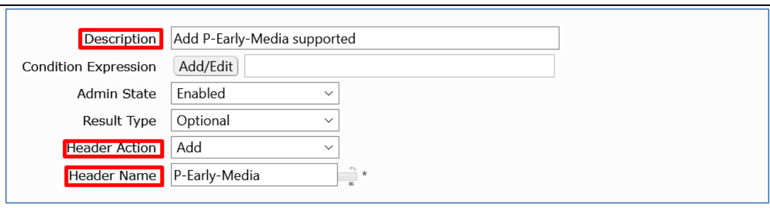
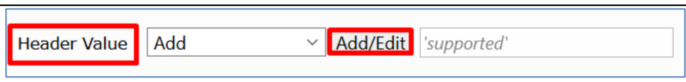
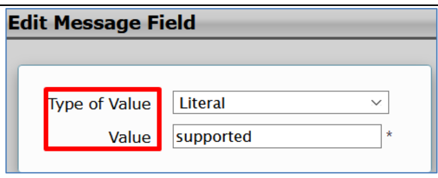
Add_P-Early-Media Rules

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

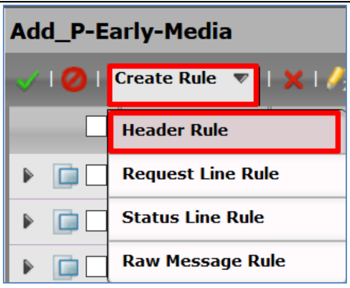
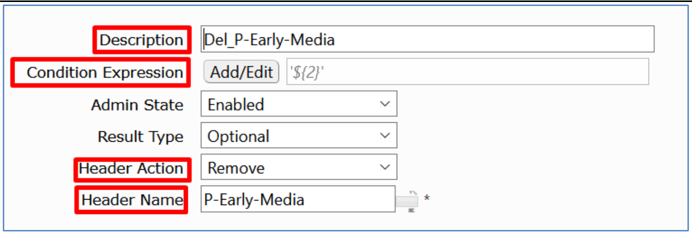
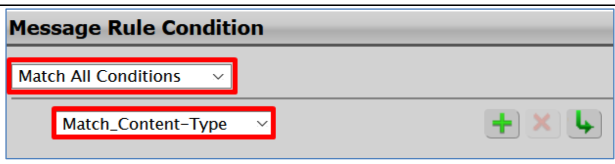
Note:

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

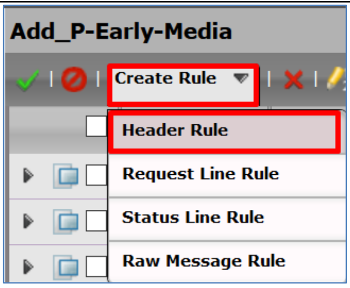
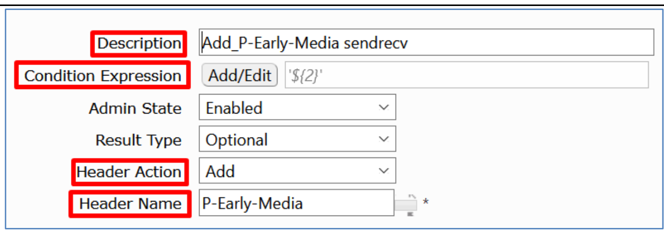
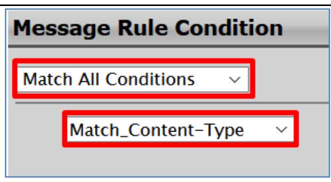
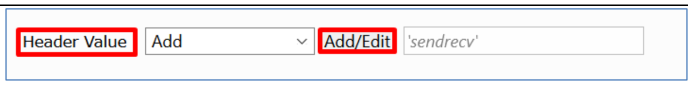
Add P-Early-Media supported

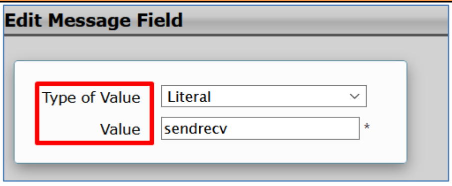
<table>
<tr><th>Actions</th><th>Screenshot</th></tr>
<tr><td>1. On the left menu path, click on the Add_P-Early-Media table you created</td><td>
</td></tr>
<tr><td>2. To add a new Message Rule, click on the Create Rule > Header Rule icon.</td><td>
</td></tr>
<tr><td>3. Set the new entry as per the right picture</td><td>
</td></tr>
<tr><td>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</td><td>
</td></tr>
<tr><td>5. Once you click on the Add/Edit icon a popup screen appears.
Set the configuration as per right picture</td><td>
</td></tr>
</table>

Del_P-Early-Media

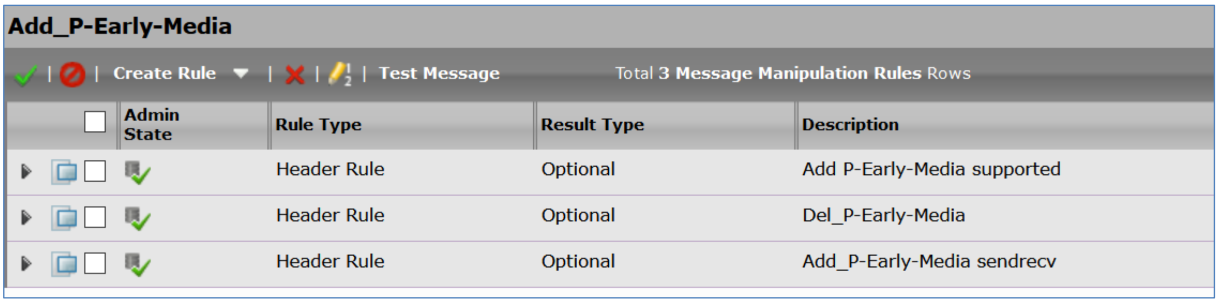
Actions	Screenshot
1. On the left menu path, click on the *Add_P-Early-Media* table you created	
2. To add a new *Message Rule*, click on the *Create Rule > Header Rule* *icon.*	
3. Set the new entry as per the right picture. For *Condition Expression* field go to next step.	
4. Click the *Add/Edit*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

Add_P-Early-Media sendrecv

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

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:



Add_P-Early-Media

Create Rule | Test Message — Total 3 Message Manipulation Rules Rows

Admin State	Rule Type	Result Type	Description
	Header Rule	Optional	Add P-Early-Media supported
	Header Rule	Optional	Del_P-Early-Media
	Header Rule	Optional	Add_P-Early-Media sendrecv

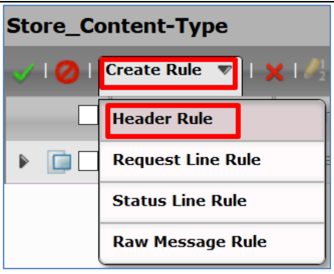
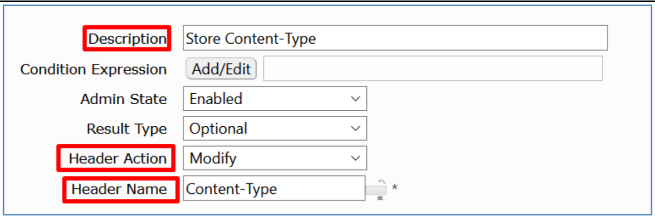
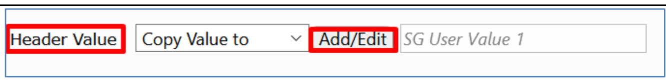
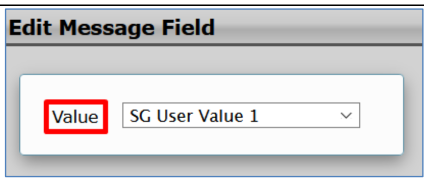
Store_Content-Type Rules

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	
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_Content-Type

Create Rule | Test Message   Total **1 Message Manipulation Rules** Row

Admin State	Rule Type	Result Type	Description
	Header Rule	Optional	Store Content-Type

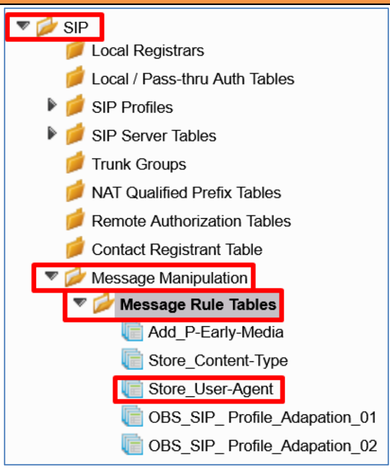
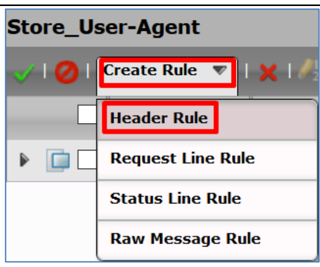
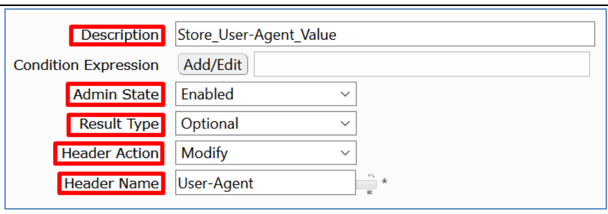
Store_User-Agent Rules

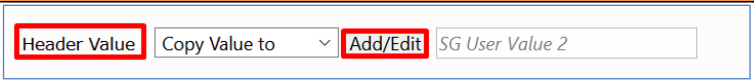
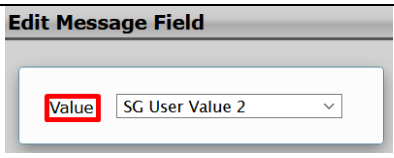
Description	Rule Type	Result Type	Comments
Store_User-Agent_Value	Header Rule	Optional	It stores the *User-Agent* value in the *SG User Value 2*
Store_Server_Value	Header Rule	Optional	It stores the Sever value in the *SG User Value 3*

Note:

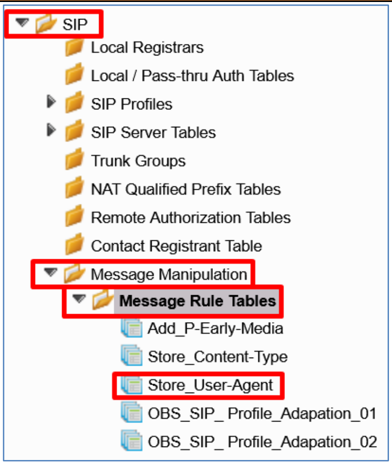
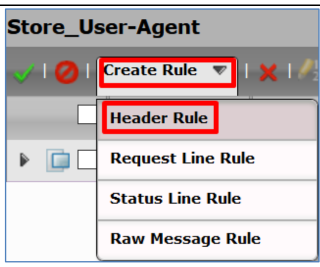
For more information, please go to Messages Rules Tables and section 2.7.4 Inbound Manipulations.

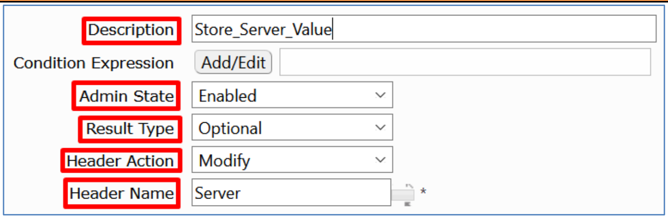
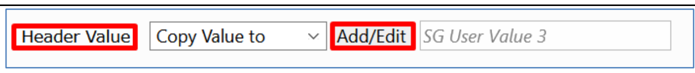
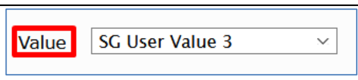
Store_User-Agent_Value

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.	

Actions	Screenshot
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	
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 *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.	

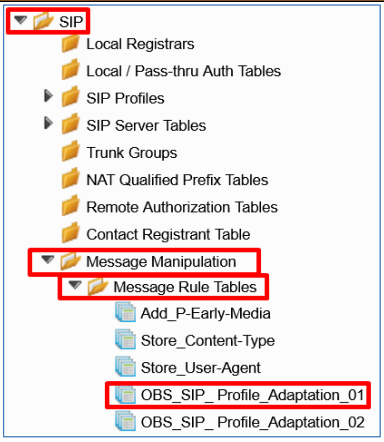
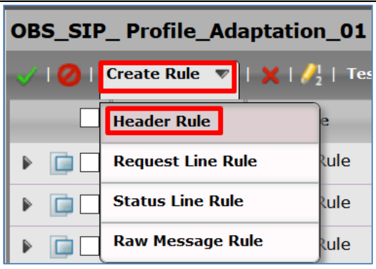
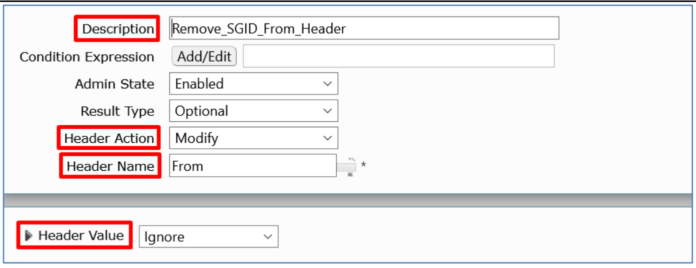
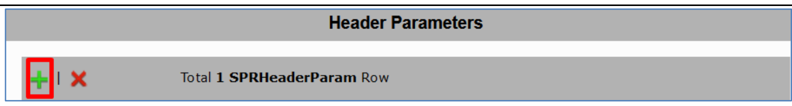
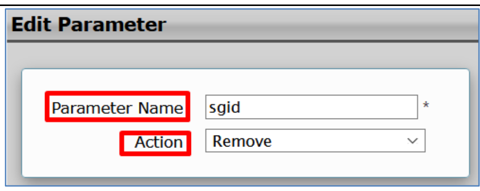
OBS_SIP_ Profile_Adaptation_01 Rules

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 OBS requirements
Modify_Server_header	Header Rule	Optional	It modifies the Server header as per OBS requirements
Modify_Allow_header	Header Rule	Optional	It modifies the Allow header as per OBS requirements

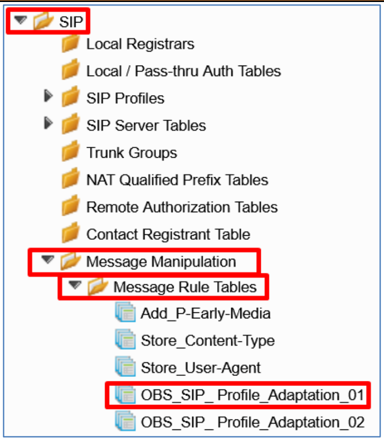
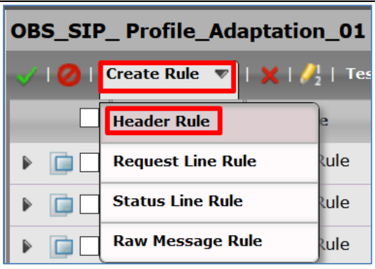
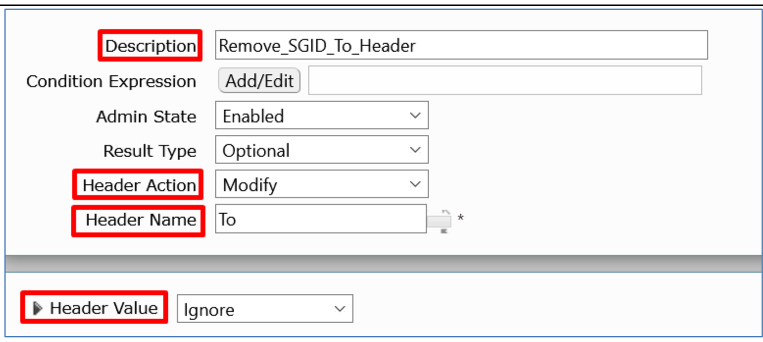
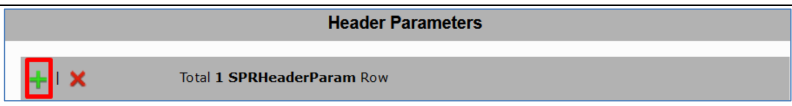
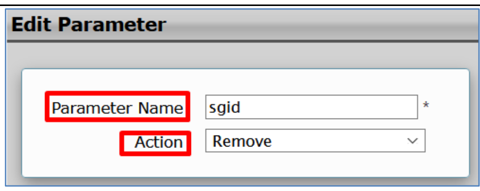
Note:

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

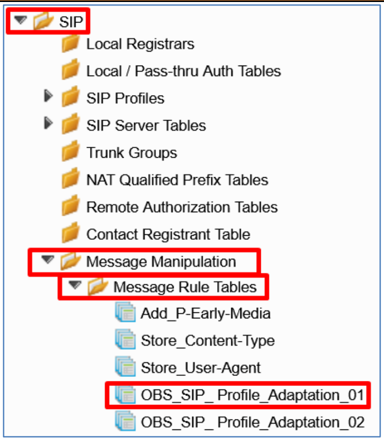
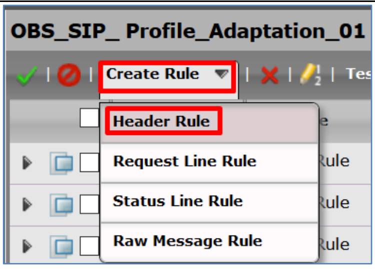
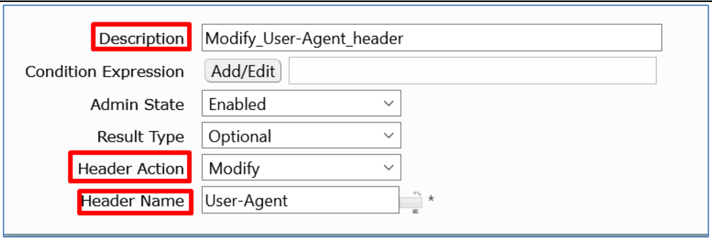
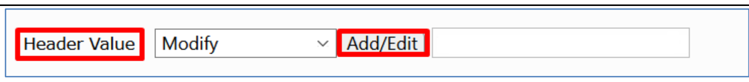
Remove_SGID_From_Header

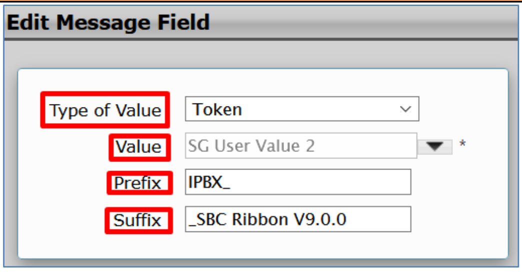
<table>
<tr><th>Actions</th><th>Screenshot</th></tr>
<tr><td>1. On the left menu path, click on the OBS_SIP_ Profile_Adaptation_ 01 table you created</td><td>
</td></tr>
<tr><td>2. To add a new Message Rule, click on the Create Rule > Header Rule icon.</td><td>
</td></tr>
<tr><td>3. Set the new entry 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>

Remove_SGID_To_Header

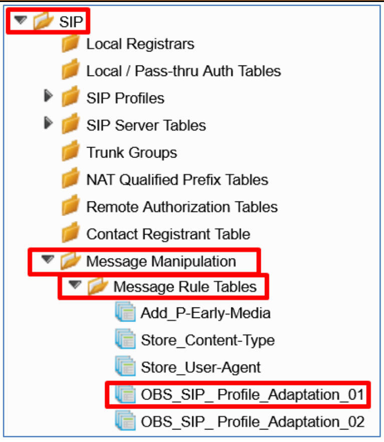
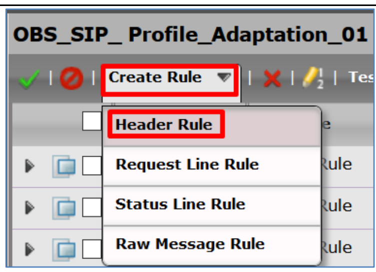
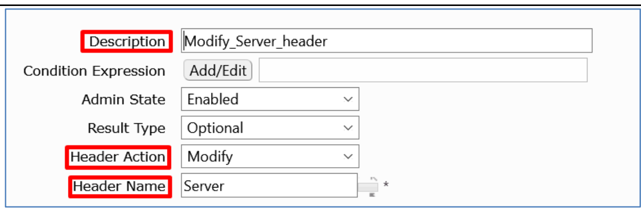
Actions	Screenshot
1. On the left menu path, click on the *OBS_SIP_ Profile_Adaptation_01* table you created	
2. To add a new *Message Rule*, click on the *Create Rule > Header Rule icon.*	
3. Set the new entry as per the right picture.	
4. Under *Header Parameters* click on the *plus icon (+)* to add a new entry	
5. Once you click on the *plus icon (+)* a popup screen appears. Set the configuration as per right picture	

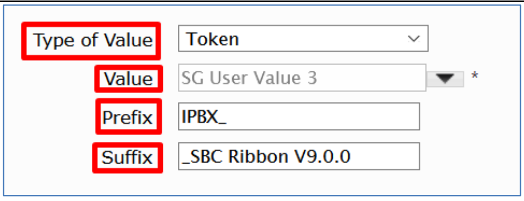
Modify_User-Agent_header

Actions	Screenshot
1. On the left menu path, click on the *OBS_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	

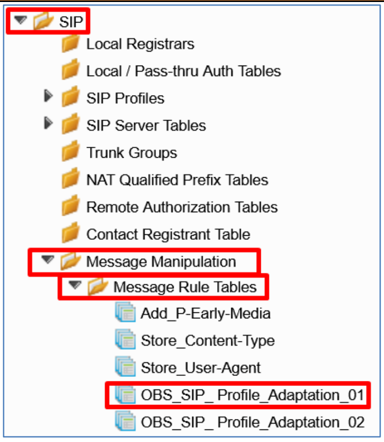
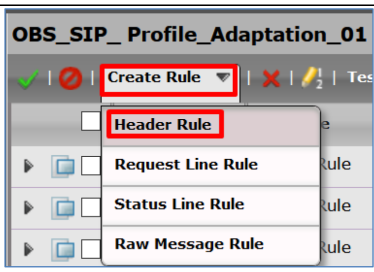
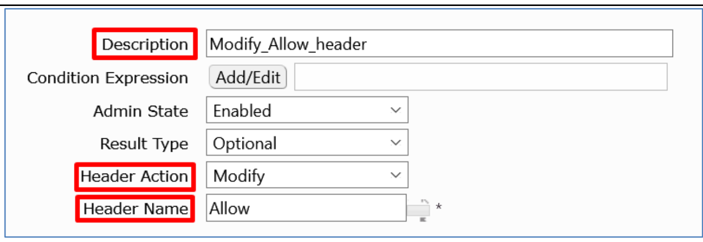
Actions	Screenshot
5. Once you click on the *Add/Edit* icon a popup screen appears. Set the configuration as per right picture	

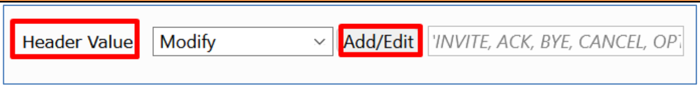
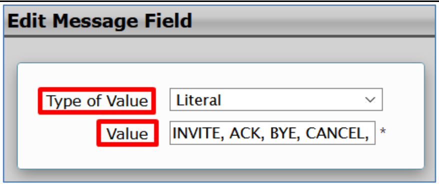
Modify_Server_header

Actions	Screenshot
1. On the left menu path, click on the *OBS_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.	

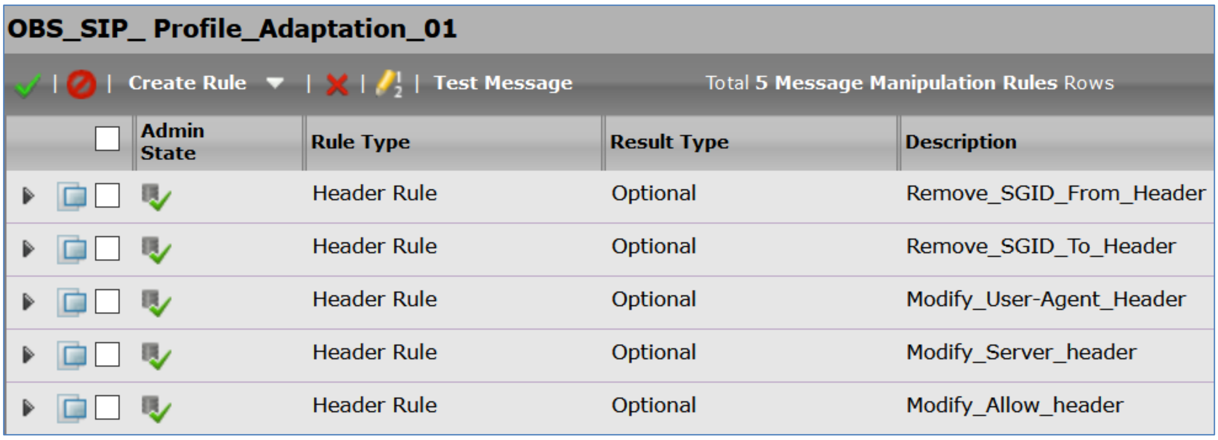
Actions	Screenshot
Select *Modify* in the *Header Value* field and click on the *Add/Edit* icon	
5. Once you click on the *Add/Edit* icon a popup screen appears. Set the configuration as per right picture	

Modify_Allow_header

Actions	Screenshot
1. On the left menu path, click on the *OBS_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.	

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	 **Note:** The Value should contain the following information: *INVITE, ACK, BYE, CANCEL, OPTIONS, UPDATE*

You should have the following entries in the *OBS_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

OBS_SIP_ Profile_Adaptation_02 Rules

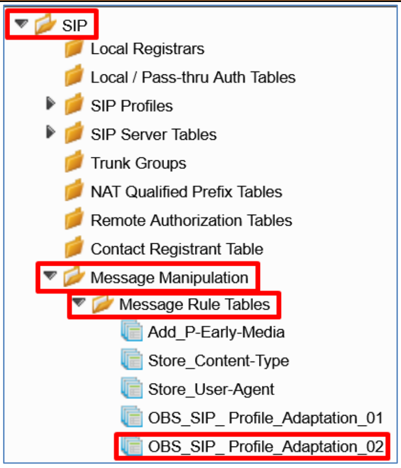
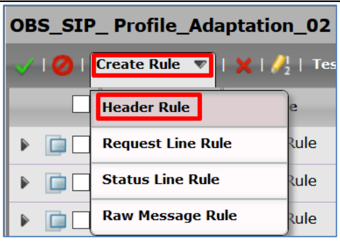
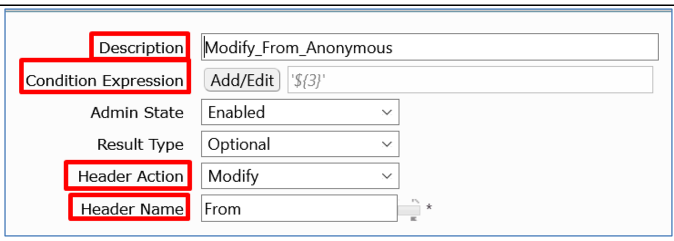
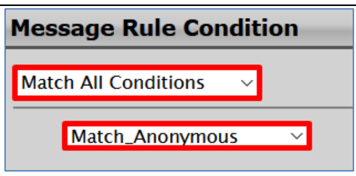
Description	Rule Type	Result Type	Comments
Modify_From_Anonymous	Header Rule	Optional	It set the anonymous format as per OBS requirements
Modify_Diversion	Header Rule	Optional	It configures the Public IP address in the *Diversion* header and adds the counter parameter

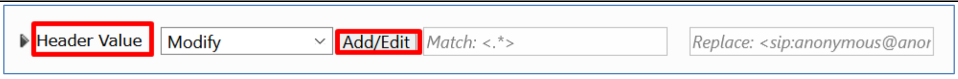
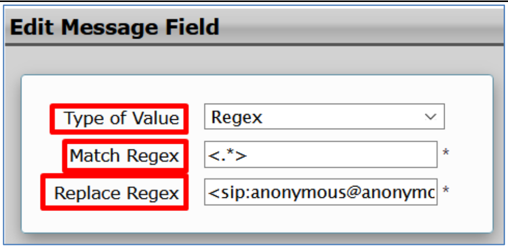
Modify_PAI	Header Rule	Optional	It configures the Public IP address in the *P-Asserted-Identity* header
Add plus P-Asserted-Identity	Header Rule	Optional	It adds the plus sign (+) in the *P-Asserted-Identity* header

Note:

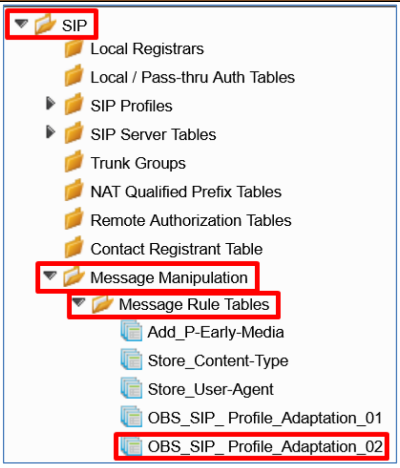
For more information, please go to Messages Rules Tables and section *2.7.3 Outbound Manipulations.*

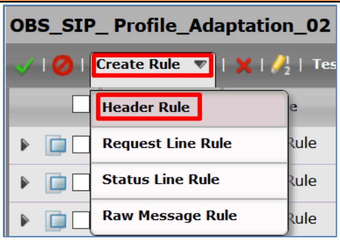
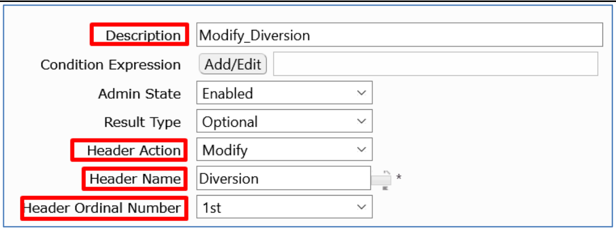
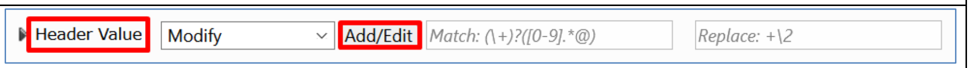
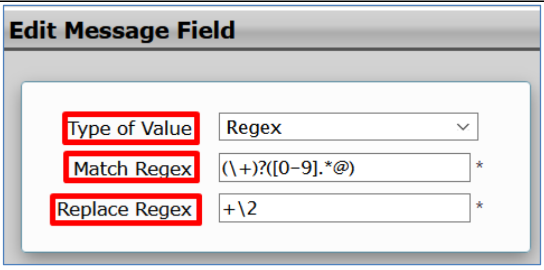
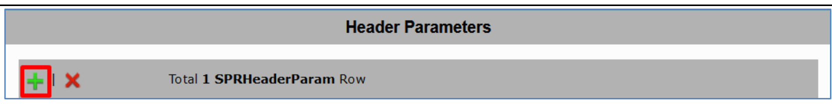
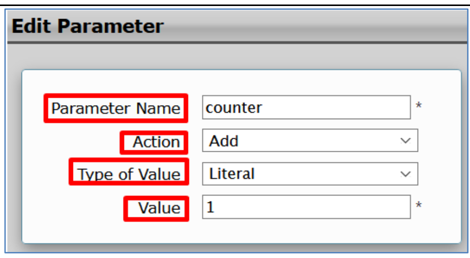
Modify_From_Anonymous

Actions	Screenshot
1. On the left menu path, click on the *OBS_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	

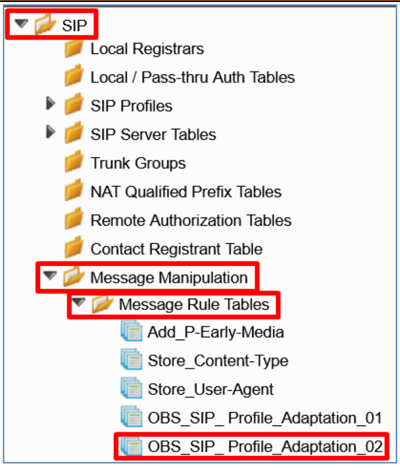
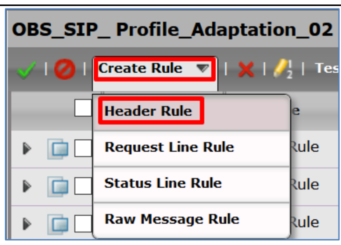
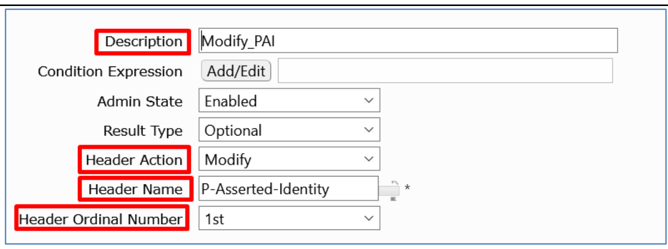
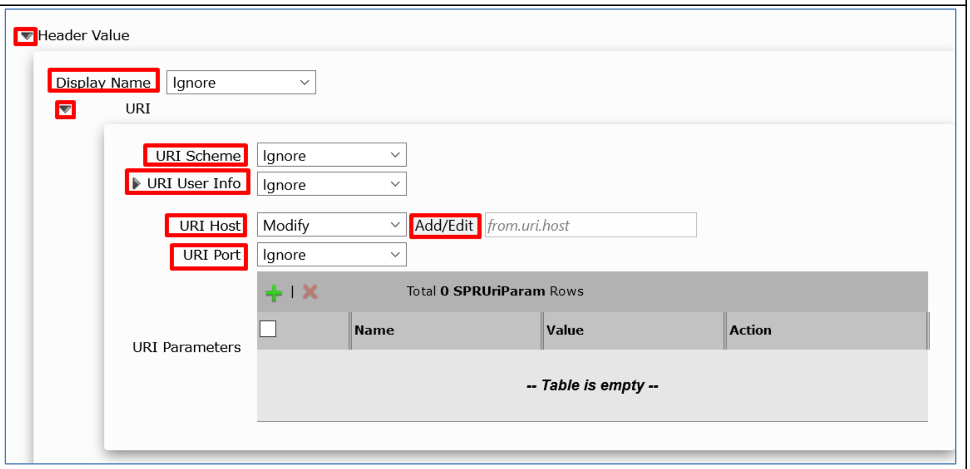
Actions	Screenshot
configuration as per right picture	
5. Once you select *Modify* in the *Header Action* field, the bottom section will change its options. Select *Modify* in the *Header Value* field and click on the *Add/Edit* icon	
6. Once you click on the *Add/Edit* icon a popup screen appears. Set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

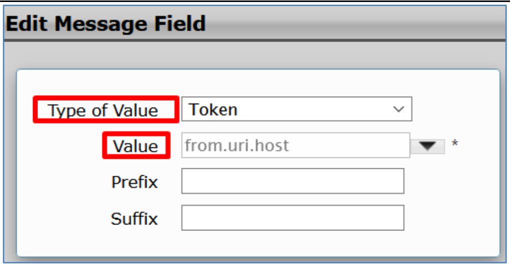
Modify_Diversion

Actions	Screenshot
1. On the left menu path, click on the *OBS_SIP_ Profile_Adaptation_ 02* table you created	

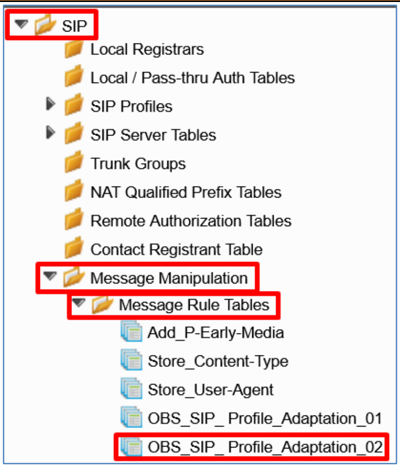
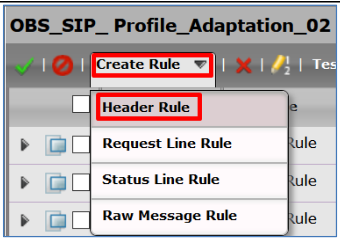
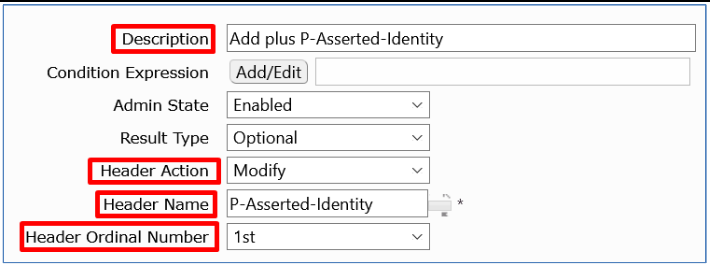
Actions	Screenshot
2. To add a new *Message Rule*, click on the *Create Rule > Header Rule icon.*	
3. Set the new entry as per the right picture.	
4. Once you select *Modify* in the *Header Action* field, the bottom section will change its options. Select *Modify* in the *Header Value* field and click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

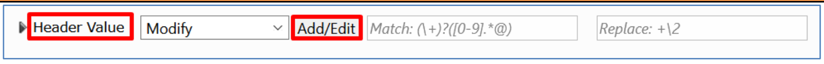
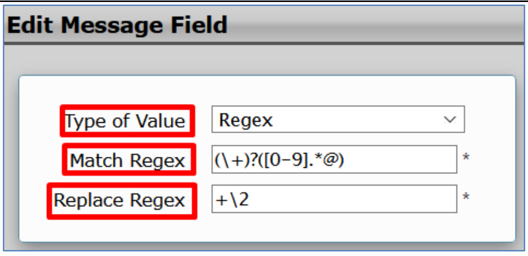
Modify_PAI

Actions	Screenshot
1. On the left menu path, click on the *OBS_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. Set the configuration and click on the *Add/Edit* icon as	

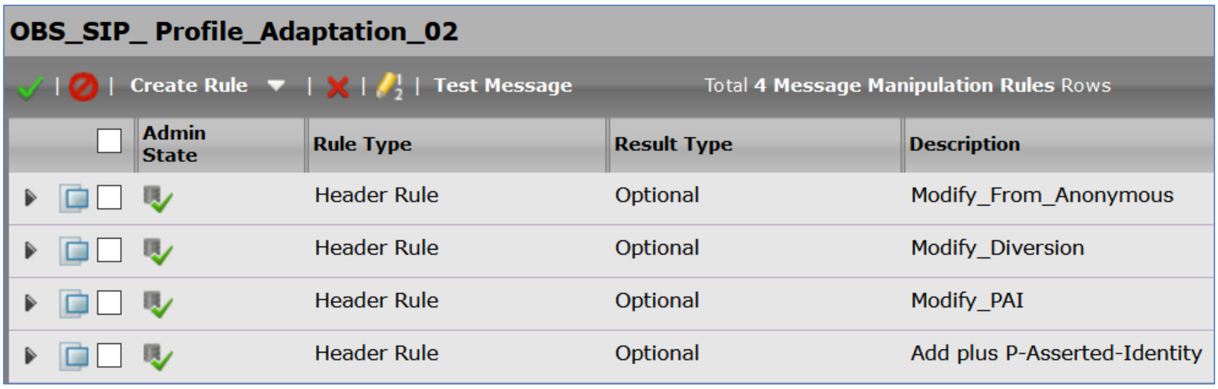
Actions	Screenshot
per right picture	
5. Once you click on the *Add/Edit* icon a popup screen appears. Set the configuration as per right picture	

Add plus P-Asserted-Identity

Actions	Screenshot
1. On the left menu path, click on the *OBS_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.	

<table>
<tr><th>Actions</th><th>Screenshot</th></tr>
<tr><td>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</td><td>
</td></tr>
<tr><td>5. Once you click on the Add/Edit icon a popup screen appears.
Set the configuration as per right picture</td><td>
</td></tr>
</table>

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



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

2.7.3 Outbound Manipulations

At the egress, SIP messages already processed by the SBC 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	OBS_SIP_ Profile_Adaptation_02	Set the Table Lists as Outbound Message Manipulation
	OBS_SIP_ Profile_Adaptation_01	
	Add_P-Early-Media	
From-To_OrangeBTIP	OBS_SIP_ Profile_Adaptation_02	
	OBS_SIP_ Profile_Adaptation_01	
	Add_P-Early-Media	
From-To_ORANGE-TLS	OBS_SIP_ Profile_Adaptation_02	
	OBS_SIP_ Profile_Adaptation_01	
	Add_P-Early-Media	

Note:

Refer to the section 2.5.11 and 2.6.13 to attach these SIP Message Manipulation rules into the corresponding Signaling group.

2.7.4 Inbound Manipulations

At the ingress, inbound SIP messages are modified to permit proper handling by the SBC'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

<u>From IPPBX toward Orange BTALK</u>

```
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_SBC Ribbon V9.0.0
Via: SIP/2.0/UDP 192.168.191.150:5060;branch=z9hG4bK-UX-c0a8-bf96-9133

v=0
o=SBC 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
```

<u>From Orange BTALK toward Customer IPPBX</u>

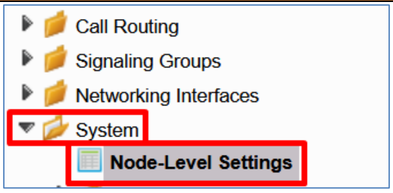
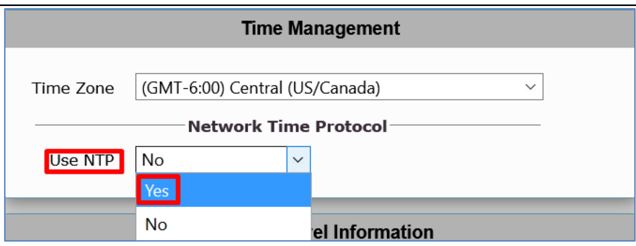
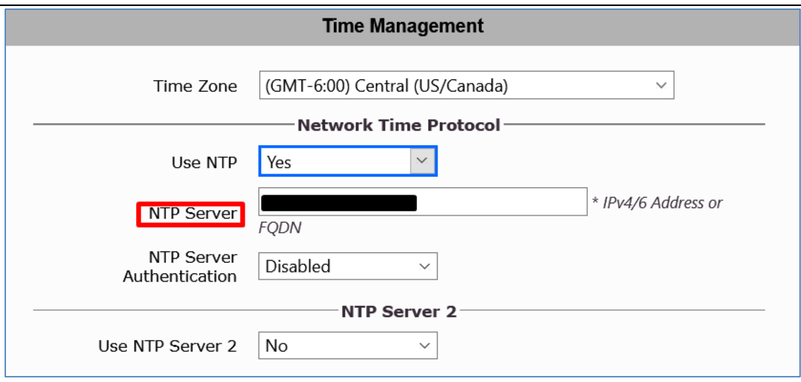
```
INVITE sip:+33296086974@192.168.191.150:5060;user=phone SIP/2.0
Via: SIP/2.0/UDP 172.22.244.209:5060;branch=z9hG4bK5u1md81040d54rql4av0.1
To: <sip:+33296086974@192.168.191.150;user=phone>
From: <sip:+2144326845@172.22.244.209;user=phone>;tag=SDlncc101-Onh6fA
Call-ID: SDlncc101-2b66c18972b3c53171a36d538d79cf17-v300g00060
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 SBC receives the current date and time. This is necessary for validating certificates of remote parties. It is important, that NTP Server will locate on the OAMP IP Interface (LAN_IF in our case) or will be accessible through it.

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

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

SBC: 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

WAN: Wide Area Network