Basic configuration guide

Genesys PureCloud BYOC with International Orange Business Services SIP trunk

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

Document Version

Version of 24-February 2022

Table of Contents

Table of Contents 2
1. GOAL OF THIS DOCUMENT 3
2. ARCHITECTURE OVERVIEW 4
3. EXTERNAL TRUNK SETTINGS FOR ORANGE 5
3.1 EXTERNAL TRUNK: CREATION 5
3.2 EXTERNAL TRUNK: INBOUND/TERMINATION SETTINGS 6
3.3 EXTERNAL TRUNK: OUTBOUND SETTINGS 7
3.4 EXTERNAL TRUNK: CALLING SETTINGS 9
3.5 EXTERNAL TRUNK: SIP ACCESS CONTROL SETTINGS 10
3.6 EXTERNAL TRUNK: EXTERNAL TRUNK CONFIGURATION 11
3.6.1 General section 11
3.6.2 Transport section 11
3.6.3 Identity section 12
3.6.4 Media section 13
3.6.5 Protocol section 15
3.7 EXTERNAL TRUNK: SITE ASSIGNMENT 18

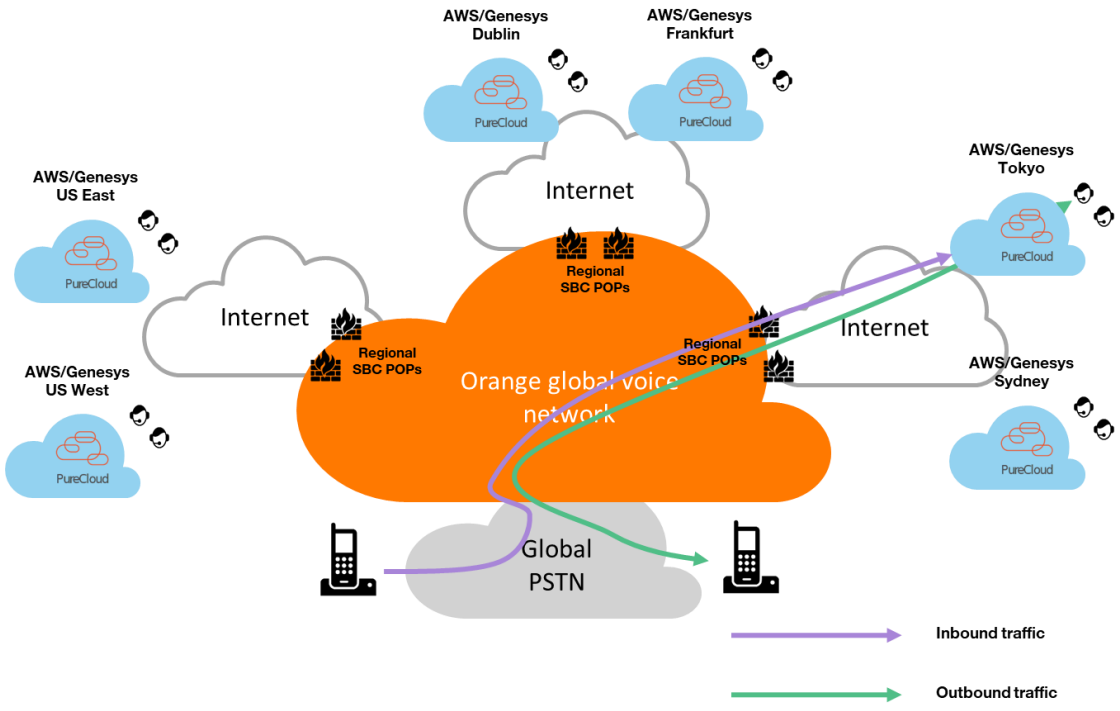
1. GOAL OF THIS DOCUMENT

The aim of this document is to list basic technical requirements to connect International Orange Business Services SIP trunk to Genesys PureCloud BYOC solution.

Please note that the whole settings required for this connection have been discussed with Genesys. Hence Orange Business Services invites the customer's Genesys integrator to contact directly Genesys for any further information.

Also, please be advised that this document assumes that a Genesys Cloud organization is already set up and the BYOC Cloud product added to the Genesys Cloud subscription.

2. ARCHITECTURE OVERVIEW



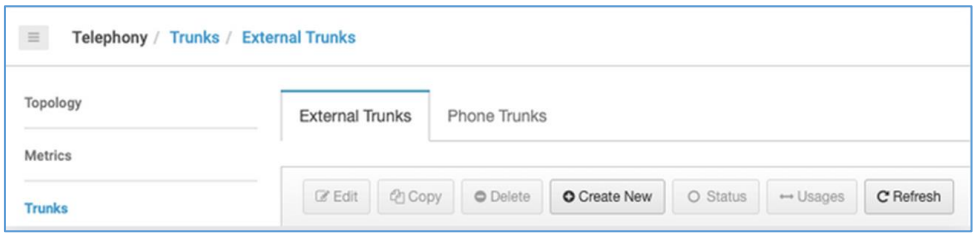
3. EXTERNAL TRUNK SETTINGS FOR ORANGE

The below sections present all the steps of configuration essential for creating an external SIP trunk on PureCloud for using Orange Business Talk service.
Only required settings are mentioned. Mandatory values for Orange are in bold and orange font colour.
This document does not cover customer specific settings like number manipulation.

3.1 EXTERNAL TRUNK: CREATION

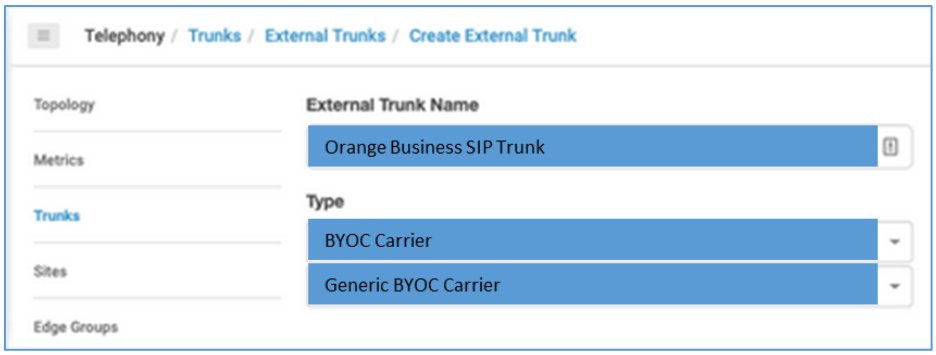
In PureCloud Admin, under *Telephony,* click *Trunks*, then *External Trunks.*

And create a New External Trunk.



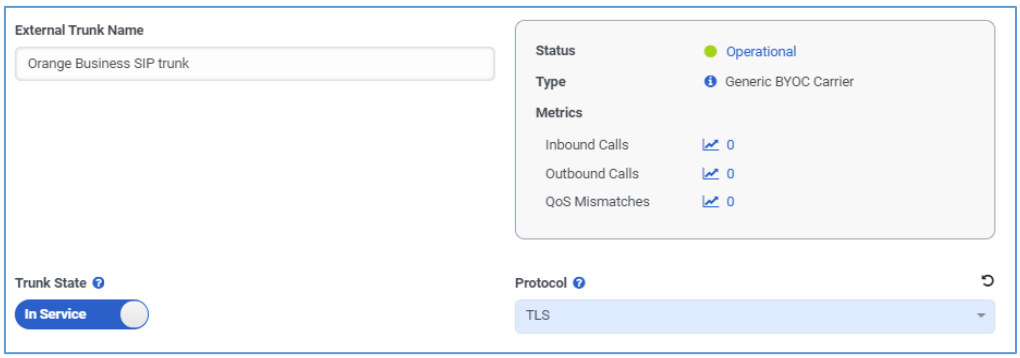
For the different settings appeared select the appropriate value as indicated in the below table:

Setting	Value	Comment
External Trunk Name	Ex: Orange Business SIP Trunk	This filled is used to identify easily the trunk in the inventory, this value can be customized.
Type for the first list	BYOC Carrier	This value is mandatory to work with Orange Business Services SIP service.
Type for the second list	Generic BYOC Carrier	This value is mandatory to work with Orange Business Services SIP service.
Trunk State	In-Service	This parameter allows to activate/deactivate the trunk, by default it is “In-Service”.
Protocol	TLS	TLS is mandatory



Set the Trunk State to In-Service.

Select the appropriate trunk transport protocol from the **Protocol** list.

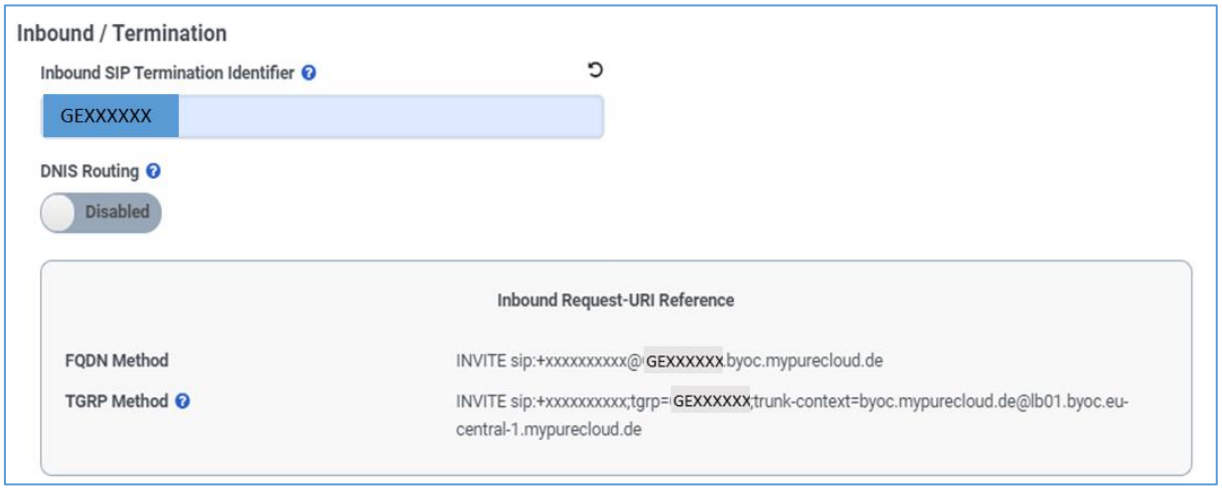


3.2 EXTERNAL TRUNK: INBOUND/TERMINATION SETTINGS

This section needs to be completed to configure Inbound/Termination.

Three modes are available to identify inbound traffic, TGRP, FQDN and DNIS.
Orange Business Service SIP service only supports the TGRP method as identifier to route the traffic.
The TGRP value is provided by Orange Business Services. The format of the TGRP value is an 8 alphanumeric capital characters started by "GE".
For the different settings select the appropriate value as indicated in the below table:

Setting	Value	Comment
Inbound SIP Termination Identifier	GEXXXXXX	The identifier value is provided by Orange Business Services.
DNIS Routing	Disabled	DNIS method must be Disabled.

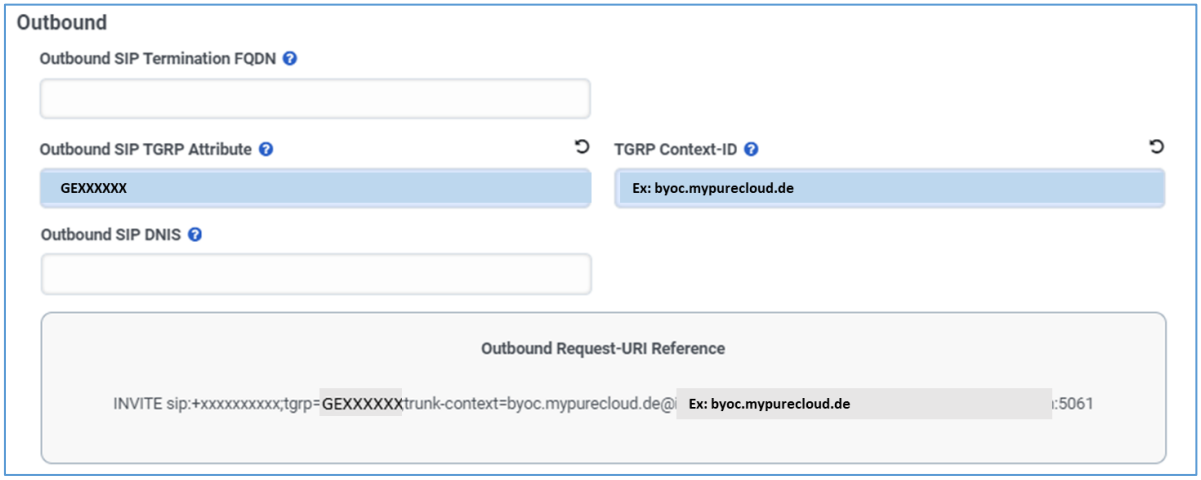


3.3 EXTERNAL TRUNK: OUTBOUND SETTINGS

This section needs to be completed to configure Outbound.

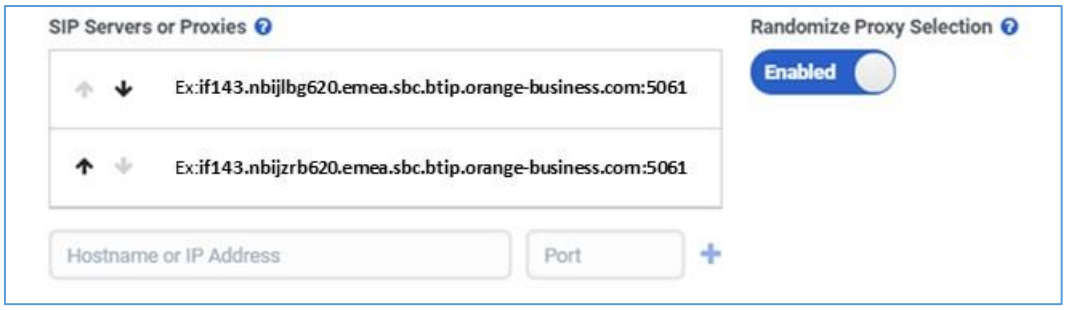
Three modes are available to identify outbound traffic, TGRP, FQDN and DNIS. Orange Business Service SIP service support only the TGRP method as identifier to route the traffic. The TGRP value is provided by Orange Business Services. The format of the TGRP value is an 8 alphanumeric capital characters started by "GE". Other methods have to be disabled.

Setting	Value	Comment
Outbound SIP Termination FQDN		Leave this field free as Orange Business Service doesn't support FQDN method for BYOC.
Outbound SIP TGRP Attribute	GEXXXXXX	The identifier value is provided by Orange Business Services. It is the same value as the one used for Inbound / Termination.
TGRP Context-ID	This field must contain one of the BYOC URLs of the PureCloud BYOC region used.	
	byoc.mypurecloud.de	For eu-central-1 / Frankfurt
	byoc.mypurecloud.ie	For eu-west-1 / Dublin
	byoc.mypurecloud.com	For us-east-1 / US East
	byoc.usw2.pure.cloud	For us-west-2 / US West
	byoc.mypurecloud.jp	For ap-northeast-1 / Tokyo
	byoc.mypurecloud.com.au	For ap-southeast-2 / Sydney
Outbound SIP DNIS		Leave this field free as Orange Business Service doesn't support DNIS method for BYOC



The below table specifies the settings to apply for the SIP Servers or Proxies.

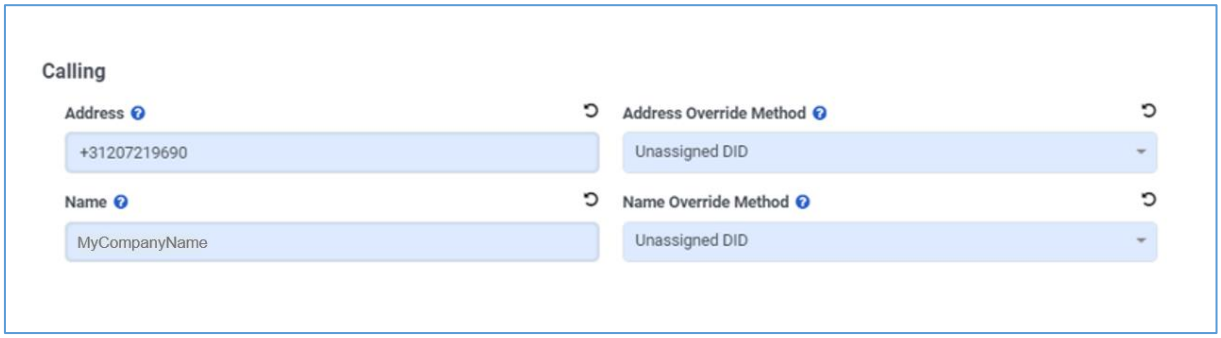
<table>
<tr><th>Setting</th><th colspan="3">Value</th><th>Comment</th></tr>
<tr><td rowspan="8">SIP Servers or Proxies</td><td colspan="3">This field must contain the IP addresses or FQDNs of Orange Business Service SBC used in a given BYOC region. For a given region, 2 IPs or 2 FQDN must be completed based on the values below.
Here, Orange Business Services only supports FQDNs.</td><td></td></tr>
<tr><td>Region</td><td>IPs</td><td>FQDNs</td><td></td></tr>
<tr><td rowspan="2">eu-central-1 / Frankfurt
&
eu-west-1 / Dublin</td><td>SBC1: 57.67.41.253</td><td>SBC2:if143.nbijlbg620.emea.sbc.btip.orange-business.com</td><td>Orange only supports FQDNs</td></tr>
<tr><td>SBC2: 57.66.206.93</td><td>SBC2:if143.nbijzrb620.emea.sbc.btip.orange-business.com</td><td>Orange only supports FQDNs</td></tr>
<tr><td rowspan="2">us-east-1 / US East
&
us-west-2 / US West</td><td>SBC1: 57.77.35.125</td><td>SBC1: if124.nbijlad620.nam.sbc.btip.orange-business.com</td><td>Orange only supports FQDNs</td></tr>
<tr><td>SBC2: 57.68.164.221</td><td>SBC2: if124.nbijlax620.nam.sbc.btip.orange-business.com</td><td>Orange only supports FQDNs</td></tr>
<tr><td rowspan="2">ap-northeast-1 / Tokyo
&
ap-southeast-2 / Sydney</td><td>SBC1: 57.73.72.45</td><td>SBC1: if121.nbijxsp620.apa.sbc.btip.orange-business.com</td><td>Orange only supports FQDNs</td></tr>
<tr><td>SBC2: 57.72.148.221</td><td>SBC2: if121.nbijoko620.apa.sbc.btip.orange-business.com</td><td>Orange only supports FQDNs</td></tr>
<tr><td>Randomize Proxy Selection</td><td colspan="3">At the customer's choice</td><td>Select "Disabled" to use systematically the first SBC to send traffic. Select "Enabled" to use load balancing between the two Orange SBCs.
Both values are supported by Orange Business Services.</td></tr>
<tr><td>Digest Authentication</td><td colspan="3">Disabled</td><td>Orange Business Service SIP service doesn't offer digest authentication.</td></tr>
</table>



3.4 EXTERNAL TRUNK: CALLING SETTINGS

The below table specifies the settings to apply for Outbound Calling.

Setting	Value	Comment
Address	+CCNSN E164 number format	Enter the number to be used as default caller ID for outbound. Number must be written with the e164 format starting with a "+" and the country code.
Address Override Method	At the customer's choice	Use this list to choose the address override method for outbound calls. The two address override methods include: • Always: This setting always uses the number specified in the Address box for the caller ID. • Unassigned DID: This setting only uses the number specified in the Address box for the caller ID, when no DID number is assigned to the user's phone. The default setting is Always. All the numbers used as caller ID (default & end users ones) must be declared on Orange Business Service SIP service for outbound calls. If not, Orange Business Service SIP service will reject the calls.
Name	Ex: **My Company Name**	This name will replace the caller ID for outbound calls.
Name Override Method	At the customer's choice	Use this list to choose the name override method. The two name override methods include: • Always: This setting always uses the origination calling name specified in the Name box for the caller ID. • Unassigned DID: This setting only uses the origination calling name specified in the Name box for the caller ID, when no name is assigned to the user's phone. The default setting is Always.



3.5 EXTERNAL TRUNK: SIP ACCESS CONTROL SETTINGS

In order to allow incoming traffic from Orange SBC to PureCloud instance(s), it is required to whitelist Orange SBC signaling and media IPs.

Under SIP Access Control, build CIDR addresses to which you want to permit SIP access by entering CIDR (Classless Inter-Domain Routing) addresses and clicking Plus.

Use the controls in this section to enter and build CIDR addresses to which you want to allow SIP access.

The below table provides the Orange SBC CIDR addresses to consider for each region.

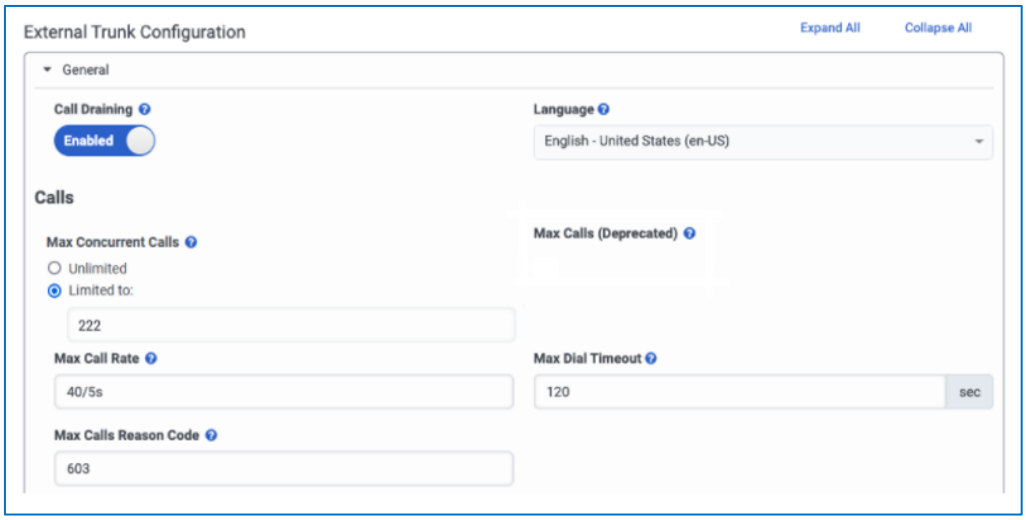
IP addresses used for SIP & Media according to Region	
Region	CIDR addresses
eu-central-1 / Frankfurt & eu-west-1 / Dublin	SBC1: 57.67.41.248/29
	SBC2: 57.66.206.88/29
us-east-1 / US East & us-west-2 / US West	SBC1: 57.77.35.120/29
	SBC2: 57.68.164.216/29
ap-northeast-1 / Tokyo & ap-southeast-2 / Sydney	SBC1: 57.73.72.40/29
	SBC2: 57.72.148.216/29

3.6 EXTERNAL TRUNK: EXTERNAL TRUNK CONFIGURATION

3.6.1 General section

Scroll down to the "External Trunk Configuration" section at the bottom of the page and expand "General" settings.
Under "Calls" apply the following settings with values indicated in the below table.

Setting	Value	Comment
Max Concurrent Calls	Select Limited to: and enter the number of max simultaneous calls to be sent on the trunk.	Orange recommends putting the same value as the number of voice channels configured on the Orange SIP trunk. If the Max Calls value is above the number of voice channels configured on Orange SIP trunk and if this number is reached, the other calls will be rejected.
Max Call Rate	**40/5s** (default value)	
Max Dial Timeout	**120s** (default value)	
Max Calls Reason Code	**603 (default value)**	

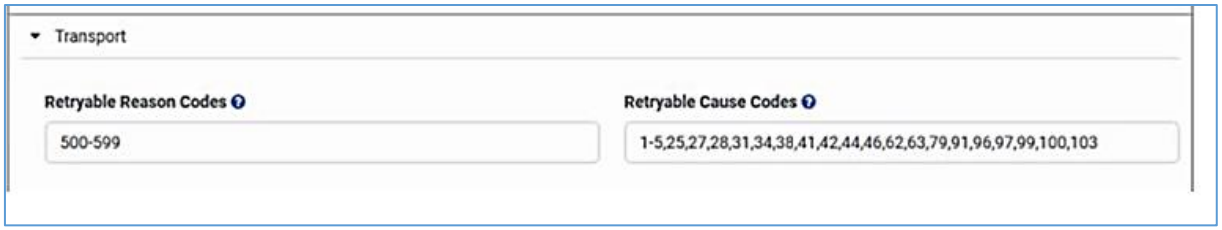


3.6.2 Transport section

Scroll down to the "External Trunk Configuration" section at the bottom of the page and expand "Transport" settings
Apply the following settings with values indicated in the below table.

Setting	Value	Comment
Retryable Reason Codes	500-599	Use the box to enter a list of valid SIP reason codes. If an outbound call that is made on this line returns one of the SIP reason codes in this list, then that call is retried on the next line. You can specify individual reason codes or ranges of reason codes, separated by commas. By default, Genesys Cloud automatically enters a list of the most common retryable codes in the Retryable.

Retryable Cause Codes	1-5, 25, 27, 28, 31, 34, 38, 41, 42, 44, 46, 62, 63, 79, 91, 96, 97, 99, 100, 103	Use this box to enter a list of valid Q.850 cause codes. If an outbound call that is made on this line returns one of the Q.850 cause codes in this list, then that call is retried on the next line. You can specify individual reason codes or ranges of reason codes, separated by commas. By default, Genesys Cloud automatically enters a list of the most common retryable codes in the Retryable Cause Codes field. The default code list: 1-5, 25, 27, 28, 31, 34, 38, 41, 42, 44, 46, 62, 63, 79, 91, 96, 97, 99, 100, 103



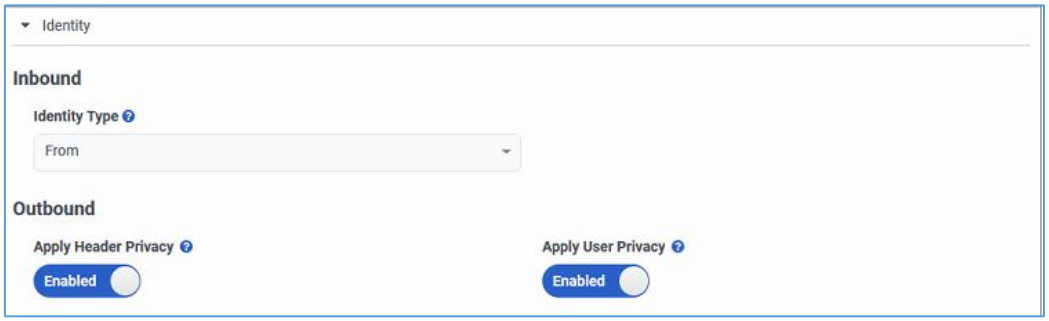
3.6.3 *Identity section*

Under “Inbound” apply the following settings with values indicated in the below table.

Setting	Value	Comment
Identity Type	At the customer’s choice	Use this list to select the type of address you want to use for inbound identity. Available choices are: From First Diversion Entry Last Diversion Entry Remote-Party-ID P-Asserted-Identity

Under “Outbound” apply the following settings with values indicated in the below table.

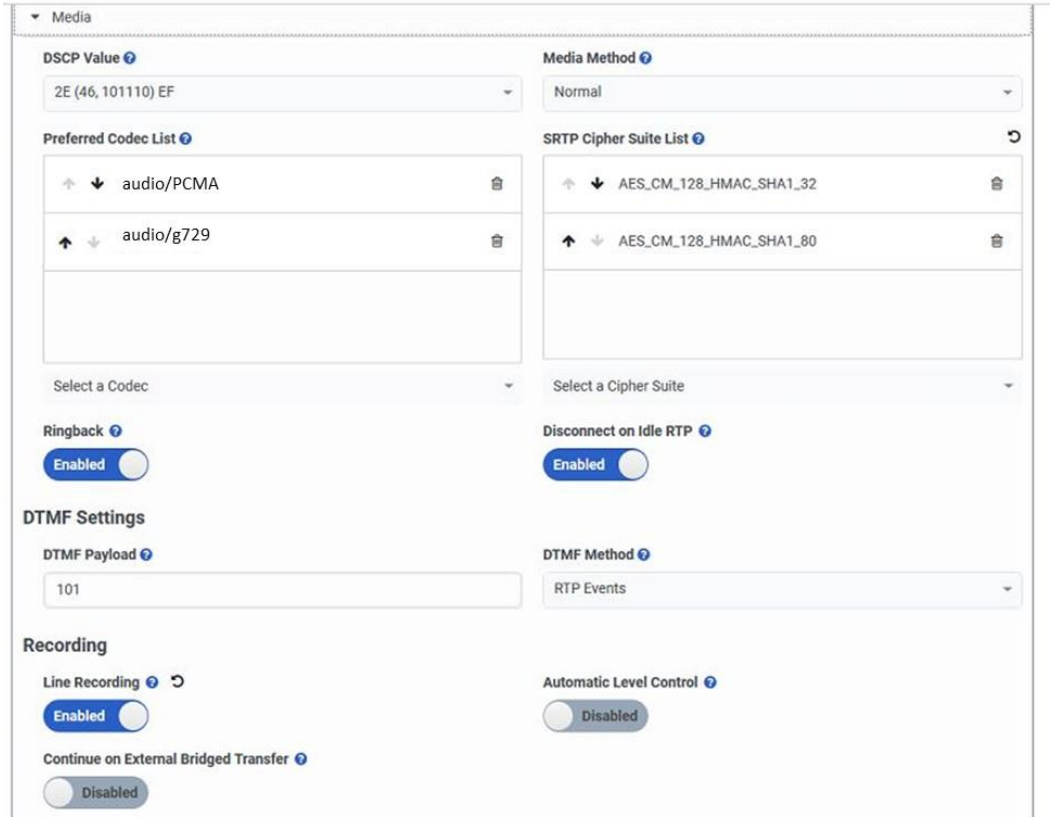
Setting	Value	Comment
Apply Header Privacy	At the customer’s choice	Use this switch to enable or disable Genesys Cloud’s capability to apply header privacy information. When enabled, an agent can use *67 to request privacy. More specifically, this prevents Genesys Cloud from sending the actual header information (typically the contact address) along with the call. Instead, Genesys Cloud replaces the actual header information with the word *Anonymous*. When disabled, an agent cannot use *67. Disable this setting if you do not want agents to represent your organization as private on a public telephony network. The default setting is Enabled.
Apply User Privacy	Disabled	Use this switch to enable or disable Genesys Cloud’s capability to apply user privacy information. When enabled, an agent can use *67 to request privacy. More specifically, this prevents Genesys Cloud from sending ANI information with the call. Instead, Genesys Cloud replaces the actual ANI with *sip:anonymous@anonymous.invalid*. When disabled, an agent cannot use *67. Disable this setting if you do not want agents to represent your organization as private on a public telephony network. The default setting is Enabled. Orange Business Services recommends Disabled value for this setting.



3.6.4 *Media section*

Apply the following settings with values indicated in the below table.

Setting	Value	Comment
DSCP Value	2E (46 101110) EF	Use this list to choose the Differentiated Services Code Point (DSCP) value of Quality of Service (QoS) for RTP and RTCP packets. The system places this value in the upper 6 bits of the TOS (Type Of Service) field. The TOS field is in the IP header of every RTP and RTCP packet. The default value is 2E (46 101110) EF.
Media Method	Normal	Use this list to choose the method that you want to use to offer an SDP (Session Description Protocol) to the other participant when making an outgoing call. The offer proposes the set of media streams and codecs along with the IP addresses and ports to use. There are three choices for the Media Method: • Normal: Use the normal method, which sends an SDP Offer in the initial SIP INVITE request. • Delayed: Use the delayed method, which waits for an SDP Offer in a response before sending an SDP Answer. • Auto: Allow the system to choose between using the normal or the delayed method. Orange Business Services only supports "Normal" method.
Preferred Codec List	Ex : Audio/PCMA	This section allows to choose and build a preferred list of codecs. Supported choices for Orange Business Services are: • audio/g729 • audio/PCMA (g711 A-Law) • audio/PCMU (g711 µ-Law)
SRTP Cipher Suite List	AES_CM_128_HMAC_SHA1_32 AES_CM_128_HMAC_SHA1_80	Use the controls in this section to choose and build a preferred list of SRTP cipher suites to offer or allow in response. Supported choices for Orange Business Services are: • AES_CM_128_HMAC_SHA1_32 • AES_CM_128_HMAC_SHA1_80
Ringback	Enabled	Use this switch to enable or disable the line ringback. When enabled, this setting controls if a ringback should be generated and sent to the incoming trunk when a 18x response message that does not include an SDP is received\relayed from the outbound call. The default setting is Enabled.
Disconnect on idle RTP	Enabled	Use this switch to enable or disable the ability to disconnect a call when RTP is not received for an extended period of time. The default setting is Enabled.

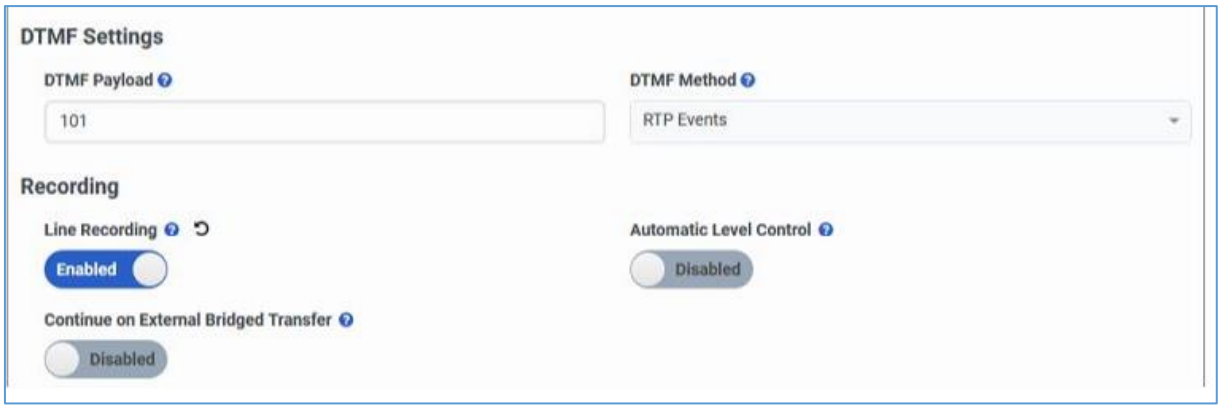


Under “DTMF Settings” apply the following settings with values indicated in the below table.

Setting	Value	Comment
DTMF Payload	101	Use this box to specify the payload type value to use when the DTMF Method type is RTP Events. Valid range is 96–127. The default value is 101. Valid only when DTMF Method value is set to RTP Events. Orange Business Services only supports 101 value for this setting.
DTMF Method	RTP Events	Use the list to select the method to use to transmit dual-tone multifrequency (DTMF) signaling. The default value is RTP Events. There are three choices for the DTMF Method: • RTP Events: Enables out-of-band processing of events from the RTP stream (RFC 2833 or 4733). • In-band Audio: Enables the processing, detection, and synthesis of events from the audio codec stream. • None: Don’t use a DTMF method. Orange Business Services only supports RTP Events value for this setting.

Under “Recording Settings” apply the following settings with values indicated in the below table.

Setting	Value	Comment
Line Recording	At the customer’s choice	Use this switch to enable or disable line recording. The default setting is Disabled.
Automatic Level Control	At the customer’s choice	Use this switch to enable or disable automatic level control for the recordings. The default setting is Disabled.
Continue on External Bridged Transfer	At the customer’s choice	Use this switch to enable or disable the ability to continue active recordings on an external transfer that result in external to external connected calls. The default setting is Disabled.

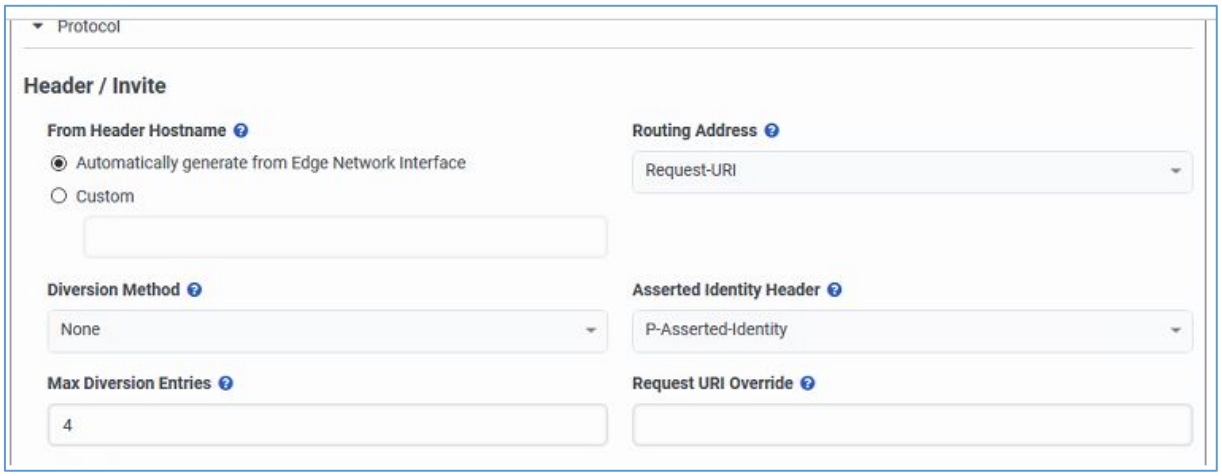


3.6.5 Protocol section

Under “Header / Invite” apply the following settings with values indicated in the below table.

Setting	Value	Comment
From Header Hostname	Set to default	Use one of these options to specify the name to replace default host name value in the From header on a SIP INVITE. Value for Orange Business Services is the default one: “Automatically generate from Edge Network interface”.
Routing Address	At the customer’s choice	Use this list to choose which field in the inbound SIP INVITE request that you want to use for routing decisions. There are two choices: To Header Request-URI
Diversion Method	None	Use this list to choose how you want diversion information delivered to the remote end in the outbound SIP INVITE request. There are two choices: None Diversion Header Note: set to None because OBS accepts only E164 format for diversion header.

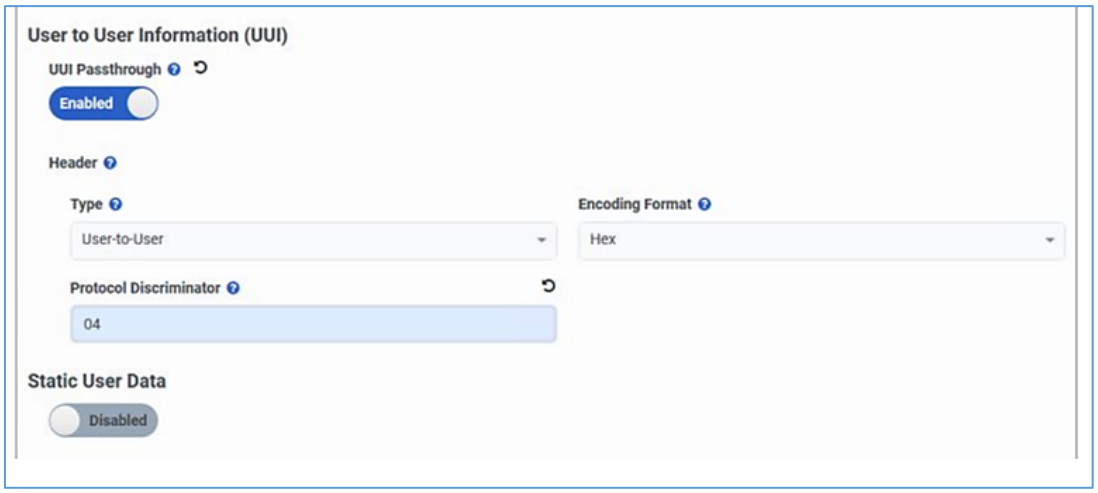
Asserted Identity Header	Asserted –identity	Use this list to choose how you want identity information delivered to the remote end in the outbound SIP INVITE request. There are three choices: P-Asserted –identity First Diversion Entry Remote-Party-ID Orange Business Services recommends Asserted-identity value.
Max Diversion Entries	4	Use this box to specify the maximum number of diversion entries to be included on an outbound call.
Request URI Override		**BYOC Carrier and BYOC PBX** Use this box to specify the destination value for the Request-URI and the TO header, but still send calls to the destinations indicated in the Outbound SIP Servers list.



Under “User to User Information (UUI)” apply the following settings with values indicated in the below table.

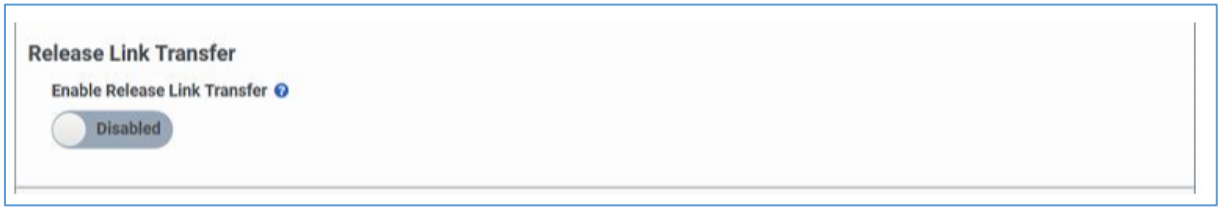
Setting	Value	Comment
UUI Passthrough	At the customer’s choice	Use this switch to enable or disable the sending of UUI data for outgoing calls.
Header / Type	User-To-User	Use this list to choose the type of UUI header information you want to use. There are three choices: • x-UserToUser: This is the Audiocodes proprietary header, which only includes the data. It does not use the protocol discriminator nor any of the other standard parameters and depending on the encoding you select, it is in the format: *x-User-to-User: hexdata* *x-User-to-User: ascii* • User-To-User: This is the general header, which requires the use of the protocol discriminator in the format: *User-to-User: XXhexdata;encoding=hex;purpose=isdn-uui;content=isdn-uui* where XX is the protocol discriminator.

		• User-To-User PD Attribute: This is the type that some gateways use where the protocol discriminator is specified separately in the format: *User-to-User: hexdata;pd=XX;encoding=hex;purpose=isdn-uui;content=isdn-uui* where XX is the protocol discriminator. Orange Business Services only supports User-To-User value for this setting.
Header / Encoding Format	Hex	Use this list to select the encoding format for the header. There are two choices: • Hex • Asci Orange Business Services only supports Hex value for this setting.
Protocol Discriminator	04 or 00	Use this box to specify the two-digit Hexadecimal protocol discriminator. You can specify any integers, lowercase letters from a-f, and uppercase letters from A-F. Note: If you select the X-UserToUser header type, this field is not available. Orange Business Services supports 04 or 00 value for this setting.



Under “Release Link Transfer” apply the following settings with values indicated in the below table.

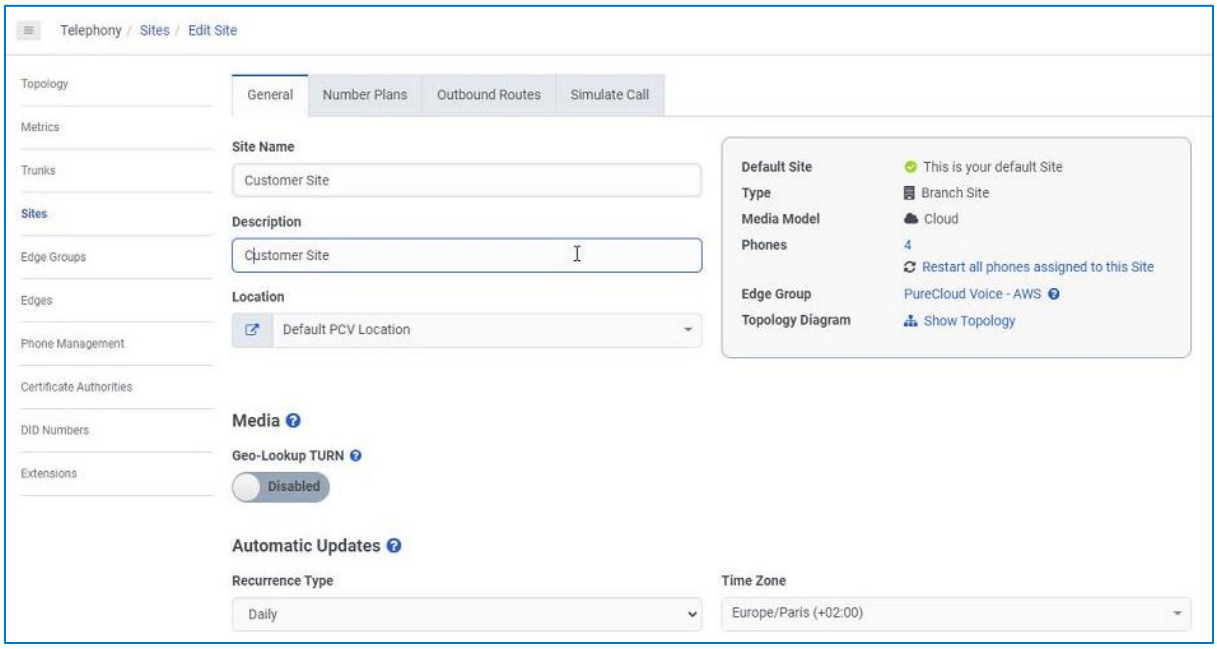
Setting	Value	Comment
Enable Release Link Transfer	Disabled	Use this switch to enable or disable the Release Link Transfer feature. The default setting is Disabled. When you enable the Release Link Transfer feature, you enable the outbound REFER method. Orange Business Services does not support REFER method.



3.7 EXTERNAL TRUNK: SITE ASSIGNMENT

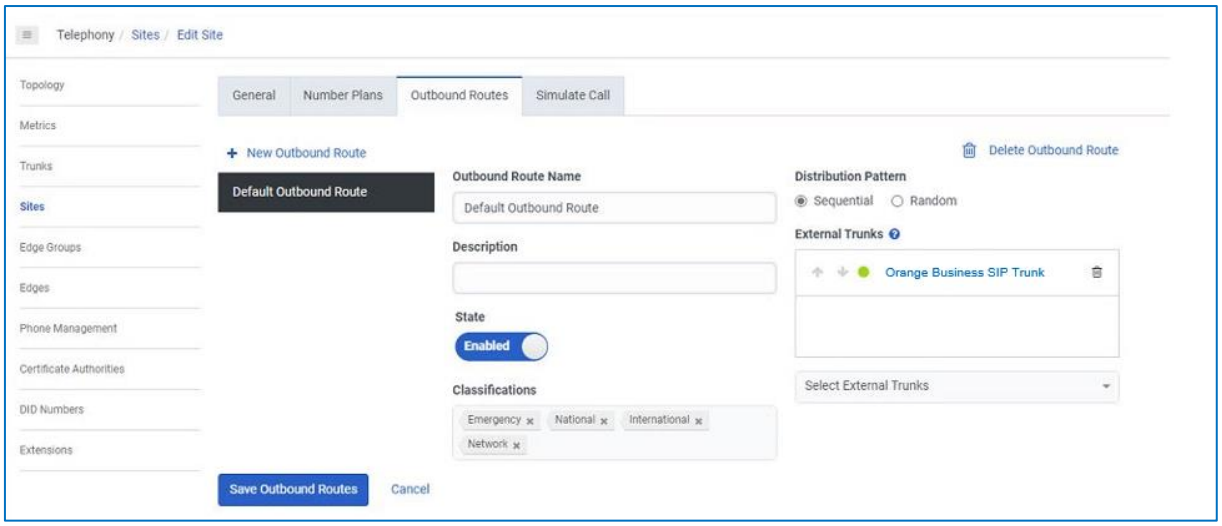
Once the external trunk is configured, it has to be assigned to the default site attached to the Edge.

In PureCloud Admin, under *Telephony,* click *Sites*, then locate and click your site on the *Site Name* list.



Click the *Outbound Routes* tab, then click *Default Outbound Route.*

From the *Select an External Trunk* list, select the external trunk configured formerly.



Setting	Value	Comment
External Trunks	Ex: Orange Business SIP Trunk	Select the external Trunk configured formerly.