Business Talk & BTIP
For IPBX Avaya IP Office

Versions addressed in this guide: Avaya IP Office 11.0, 11.1, 12.0, 12.2 and 12.3

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

Latest edition: October 2026

Table of Contents

1 Goal of this document 3
2 Certified architectures 4
2.1 Introduction to architecture components and features 4
2.2 SIP trunk on Avaya IP Office over BVPN 5
2.2.1 Architecture 5
2.2.2 Resiliency consideration 6
2.2.3 Codecs consideration 6
2.2.4 Sizing approach 6
2.3 SIP trunk on customer SBC over BVPN 7
2.3.1 Architecture 7
2.3.2 Resiliency consideration 8
2.3.3 Codecs consideration 8
2.3.4 Sizing approach 8
2.4 SIP trunk on customer SBC over Internet 9
2.4.1 Architecture 9
2.4.2 Prerequisites 10
2.4.3 Public IP address assignment 11
2.4.4 Public DNS record 11
2.4.5 Firewall updates 11
2.4.6 Certificate updates 11
2.4.7 TLS Mutual Authentication Mechanism Support regarding public certificate Extended Key Usage (EKU) 12
2.4.8 TLS v1.3 and v1.2 cipher suites compliance 14
2.4.9 SRTP encryption on BTIPol/BTol 16
2.4.10 Supported codecs on BTIPol/BTol 16
3 Parameters to be provided by customer to access BTIP service 17
3.1 Architecture without “Customer SBC” over BVPN 17
3.2 Architecture with “Customer SBC” over BVPN 18
3.3 Architecture with “Customer SBC” over Internet for BTIPol 19
3.4 Architecture with “Customer SBC” over Internet for BTol 20
4 BTIP/BTalk/BTIPol/BTol IP Office certified versions 22
4.1 Avaya IP Office versions supported with BTIP/BTalk/BTIPol/BTol 22
4.2 Avaya IP Office endpoints and applications 23
5 IP Office SIP trunking configuration checklist 25
6 IP Office + ASBCE SIP trunking configuration over BVPN checklist 51
7 IP Office + ASBCE SIP trunking configuration over Internet checklist 63
8 ASBCE dynamic license allocation since version 10.2.1 70
9 Fax configuration with Avaya IP500v2 gateway 71
9.1 T.38 Fax 71
9.2 G.711 Inband Fax 75
10 Ecosystems and endpoints configuration 76
10.1 Avaya Communicator for Windows 76
10.2 Avaya B179 Conference Station 76
10.3 Avaya DECT IP Base Station 77
10.4 Avaya One-X Portal 79
10.5 Avaya One-X Mobile 79

1 Goal of this document

The aim of this document is to list technical requirements to ensure the interoperability between Avaya IP Office IPBX with Orange Business Talk IP SIP service, hereafter so-called “service”.

2 Certified architectures

2.1 Introduction to architecture components and features

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

Fax transmissions are allowed by both BTIP and BTalk:

* With BTIP, inband fax (G.711 passthrough) is available by default. T.38 support is available upon request.

* With BTalk, both inband fax (G.711 passthrough) and T.38 are available by default.

T.38 and G.711 Fax are opened on BTIP and BTalk networks with no end-to-end guarantee, as Orange cannot certify the reliability of the fax interop that might occur at interconnection points with terminating carriers.

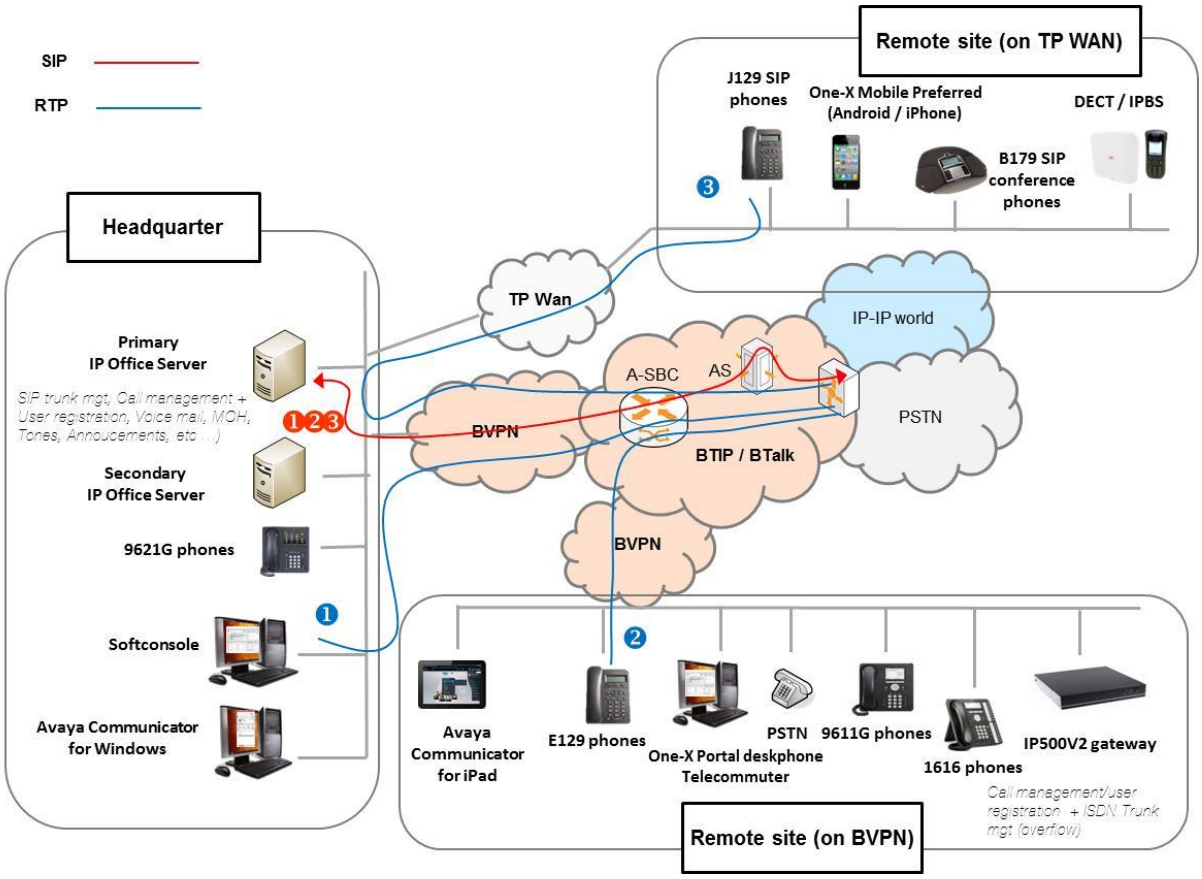
Concerning the Quality of Service, Business VPN and BTIP/Btalk networks trust the DSCP (Differenciated Services Code Point) values sent by customer voice equipment. That’s why Orange strongly recommends setting the IPBX, IP phones and other voice applications with a DiffServ/TOS value* = 46 (or PHB value = EF) at least for media.

“BTIP DROM” architectures are now supported. Dedicated aSBC pairs have been installed in Caribbean and Indian Ocean zones for local calls. For a trunking point of view, the mechanism is similar to “BTIP out of France”, the IPBX must support international dial plans and route local calls to the dedicated aSBC pair.

*cf QoS parameters in the Configuration Checklist → “System configuration – DSCP configuration”.

2.2 SIP trunk on Avaya IP Office over BVPN

2.2.1 Architecture



Notes:

- In the diagram above, the SIP and proprietary internal flows are hidden.

❶ call from/to Headquarter
❷ call from/to remote site (on Business VPN)
❸ call from/to remote site (on Third Party WAN)

- Call flows will be the similar with or without IPO Call Server redundancy.

In this architecture

- All 'SIP trunking' signaling flows are carried by the IP Office server and routed on the main BVPN connection.
- Media flows are direct between endpoints and the Business Talk/BTIP but IP routing differs from one site to another:
    - For the Head Quarter site, media flows are just routed on the main BVPN connection.
    - For Remote sites on BVPN, media flows are just routed on the local BVPN connection (= distributed architecture).

- For Remote sites on Third Party WAN, media flows are routed through the Head Quarter (but not through the IPBX) and use the main BVPN connection (= centralized architecture, cf sizing below).

Call scenario	nb of voice channels/media resources used		
	IPBX	WAN router*	BTIP
1 offnet call from/to the headquarter (HQ)	**1** in HQ	**1** in HQ	**1** in HQ
1 offnet call from/to a remote site (RS) on BVPN	0 in HQ **1** in RS	0 in HQ **1** in RS	0 in HQ **1** in RS
1 offnet call from/to a remote site (RS) on TP Wan	0 in HQ **1** in RS	**1** in HQ BVPN **1** in HQ TP Wan **1** in RS TP Wan	0 in HQ **1** in RS
1 offnet call from/to a remote site **with put on hold**	**1** in HQ **1** in RS	**1** in HQ **1** in RS	0 in HQ **1** in RS
1 offnet call from/to a remote site **after transfer/forward to BTIP**	0 in HQ **0** in RS	0 in HQ **0** in RS	0 in HQ **2** in RS
1 **forced onnet** call from Headquarter to a remote site (= through Business Talk IP infrastructure)	**2** in HQ **2** in RS	**1** in HQ **1** in RS	**0** in HQ **0** in RS

*On the WAN router, 1 voice channel= 80Kb/s

2.2.2 Resiliency consideration

Secondary IP office server can be located on the same site as the primary IP Office server or on a remote site.

All users are registered initially to a nominal central server. Then in case of failure of the primary server:

- HQ users register to the backup server located near the nominal server or distant from the nominal server
- Some remote users may register to their local GW if it is available
- Some remote users may register to the GW located on another remote site or on the backup server

2.2.3 Codecs consideration

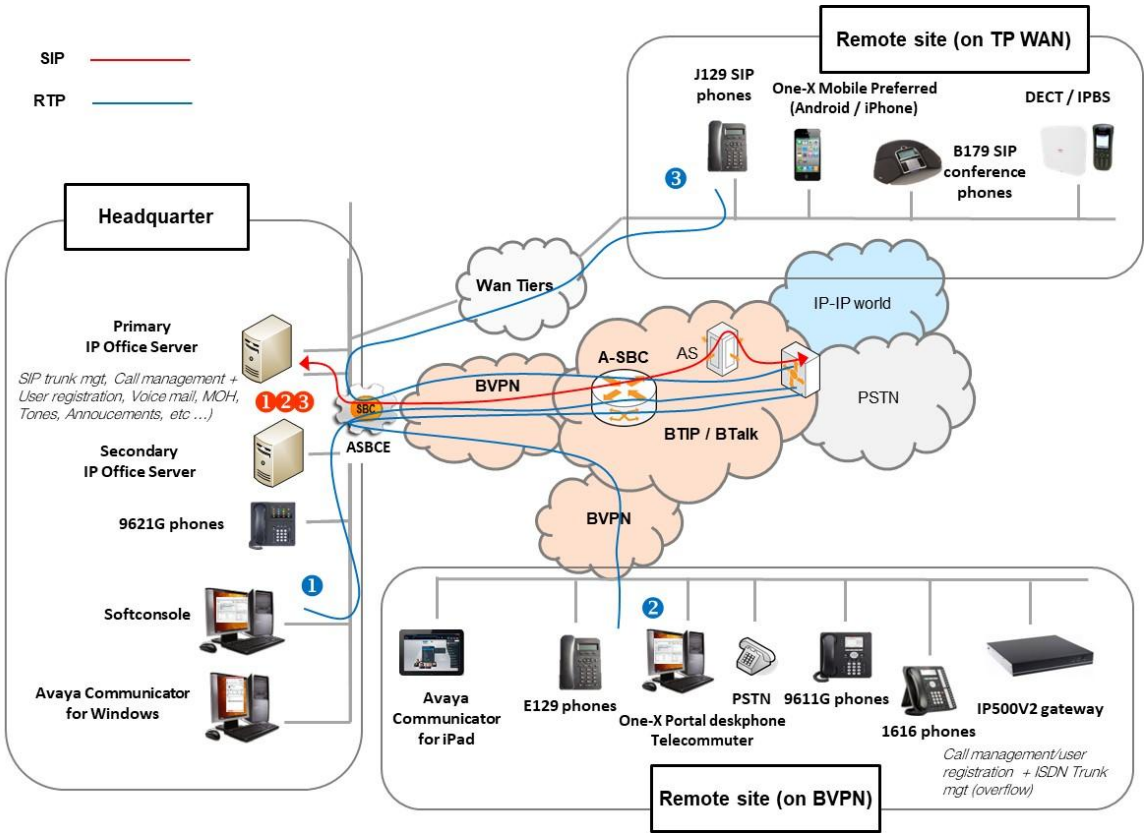
Only G711A and G722 codecs are supported.
G711U can be supported in option.
G729A codec is not certified.

2.2.4 Sizing approach

There is no specific sizing approach to be considered with IP Office solution. The RTP flow is direct between Avaya phones and Orange a-SBC.

2.3 SIP trunk on customer SBC over BVPN

2.3.1 Architecture



Notes:

- In the diagram above, the SIP and proprietary internal flows are hidden.

  ❶ call from/to Headquarter
  ❷ call from/to remote site (on Business VPN)
  ❸ call from/to remote site (on Third Party WAN)

- Call flows will be the similar with or without IPO Call Server redundancy.

Avaya Session Border Controller for Enterprise (ASBCE) is standard, so doesn't need any specific implementation request.

If the Avaya IPO customer solution is complemented by a SBC equipment, which is not an Avaya SBCE, Orange will offer one of the following approaches:

- A "Certified Border" approach (or "Certified SBC equipment"), if the SBC used is already certified by Orange, regardless of the PBX solution used. Recommendations on this SBC are also available on the Orange Business Services website.
- A "Generic Offer" approach, if the SBC is not certified by Orange. Orange will not be able to give any recommendation on the choice of hardware, software or configuration, but offers a 'Validation Assistance Service' for the SBC+PBX architecture.

In this architecture, both 'SIP trunking' and RTP media flows between endpoints and the Business Talk/BTIP are anchored by the enterprise SBC:

- for the Headquarter site, media flows are routed through the enterprise SBC and the main BVPN connection
- for Remote Sites either on BVPN or Third-Party WAN, media flows transit through the Headquarter enterprise SBC and use the central BVPN connection (= centralized architecture, cf sizing below).

Warning: site access capacity must be sized adequately on the Headquarter. Here below a table with a few sizing elements:

Call scenario	nb of voice channels/media resources used		
	IPBX	WAN router*	BTIP
1 offnet call from/to the headquarter (HQ)	**1** in HQ	**1** in HQ	**1** in HQ
1 offnet call from/to a remote site (RS) on BVPN	0 in HQ **1** in RS	**2** in HQ **1** in RS	0 in HQ **1** in RS
1 offnet call from/to a remote site (RS) on TP Wan	0 in HQ **1** in RS	**1** in HQ BVPN **1** in HQ TP Wan **1** in RS TP Wan	0 in HQ **1** in RS
1 offnet call from/to a remote site **with put on hold**	**1** in HQ **1** in RS	**3** in HQ **1** in RS	0 in HQ **1** in RS
1 offnet call from/to a remote site **after transfer/forward to BTIP**	0 in HQ **0** in RS	0 in HQ*/**3** in HQ** **0** in RS	0 in HQ **2** in RS
1 **forced onnet** call from Headquarter to a remote site (= through Business Talk IP infrastructure)	**2** in HQ **2** in RS	**3** in HQ **1** in RS	**0** in HQ **0** in RS

*on the WAN router, 1 voice channel = 80Kb/s

**if media release is activated on the enterprise SBC

***if media release is not activated on the enterprise SBC

2.3.2 Resiliency consideration

Secondary ASBCE can be located on the same site as the primary ASBCE or on a remote site.

2.3.3 Codecs consideration

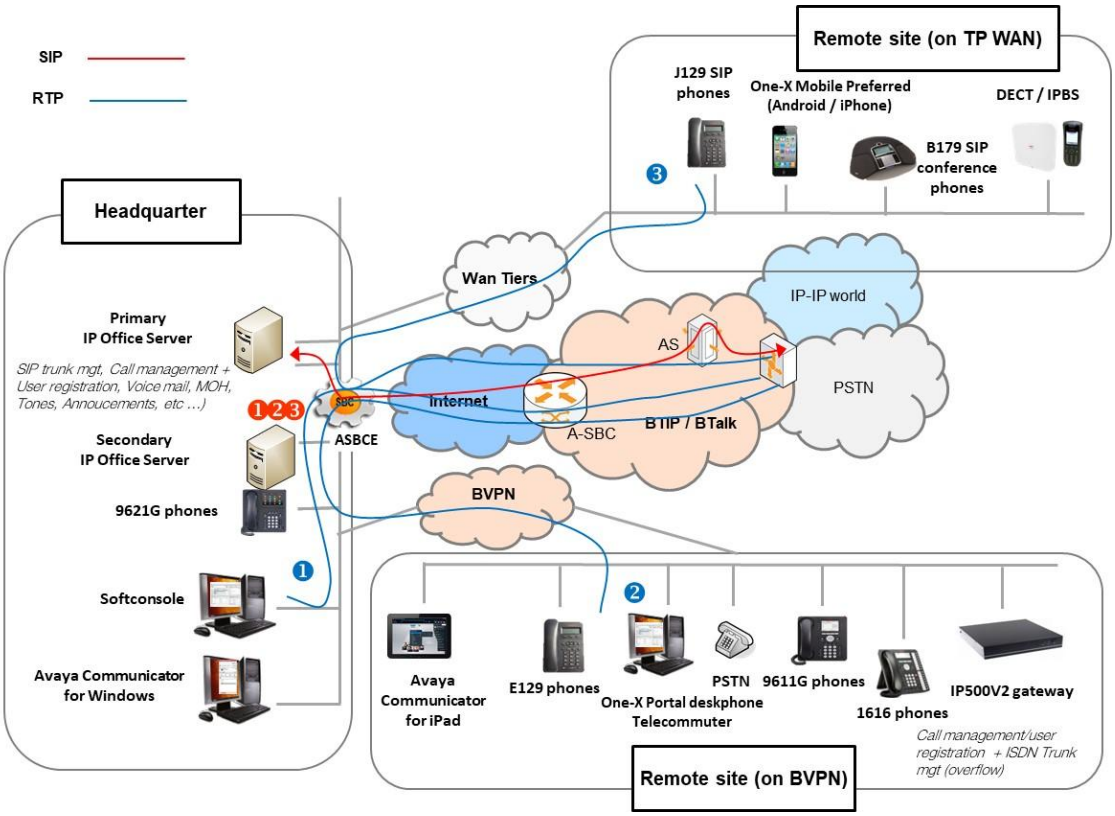
Only G711A and G722 codecs are supported.
G711U can be supported in option.
G729A codec is not certified.

2.3.4 Sizing approach

Specific sizing approach to be considered with ASBCE solution as the RTP flow is not direct between Avaya phones and Orange a-SBC but anchored by the enterprise SBC.

2.4 SIP trunk on customer SBC over Internet

2.4.1 Architecture



Notes:

- In the diagram above, the SIP and proprietary internal flows are hidden.

  ❶ call from/to Headquarter
  ❷ call from/to remote site (on Business VPN)
  ❸ call from/to remote site (on Third Party WAN)

- Call flows will be the similar with or without IPO Call Server redundancy.

  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. Refer to the dedicated configuration section chapter 7 for more details.

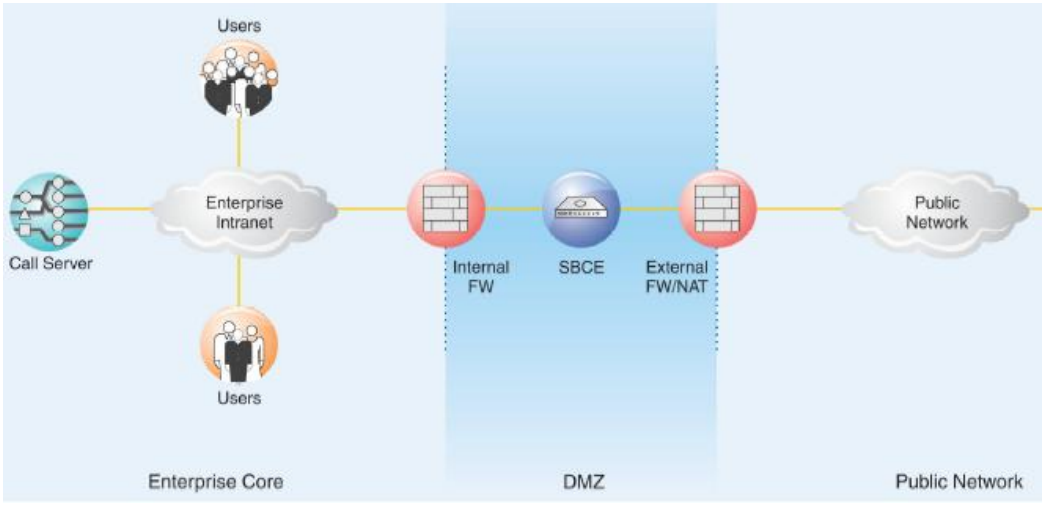
  In this architecture, both 'SIP trunking' and RTP media flows between endpoints and the Business Talk/BTIP are anchored by the enterprise SBC*:

  - For the Headquarter site, media flows are routed through the SBC and the Internet access
  - For Remote Sites, media flows transit **through the Headquarter SBC** and use the BTIP over Internet (BTIPoI) / Business Talk over Internet (BToI) connection (= **centralized architecture**).

  * Avaya Session Border Controller is standard, so doesn't need any other specific implementation request.

Note: To avoid any security risk the clients should always install on ASBCE the latest mandatory patch/hotfix released by the Avaya vendor.

Concerning the deployment of the ASBCE, the two-wire topology, also referred to as inline, is the simplest and most basic model.



Avaya SBCE is positioned at the edge of the network in the DMZ. Avaya SBCE is directly in line with the call servers, and protects the enterprise network against all inadvertent and malicious intrusions and attacks.
In this configuration, the Avaya SBCE performs border access control functionality such as internal and external Firewall or Network Address Translation (FW/NAT) traversal, access management and control. These functions are based on domain policies that the user can configure, and intrusion functionality to protect against DoS, spoofing, stealth attacks, and voice SPAM.

The two-wire Avaya SBCE deployment enables TLS encryption of the signaling traffic and SRTP encryption of the media traffic carried over public internet between ASBCE and Orange A-SBC.

An X.509 v3 public key certificate is used to identify the Avaya SBCE when performing a TLS handshake for incoming and outgoing connections.

Media must be anchored on ASBCE to perform media transcoding between internal RTP and external SRTP.

2.4.2 Prerequisites

In order to establish the connection with public interface of A-SBC, several preliminary configuration steps have to be performed. These involve the following:

- Public IP address assignment
- Public DNS record
- Firewall updates
- Certificate updates
- TLS v1.3 and v1.2 cypher suites compliance

- SRTP encryption
- Supported codecs on BTIPoI/BToI

2.4.3 Public IP address assignment

The certified solution is using a public IP address directly configured on ASBCE interface placed within DMZ.

2.4.4 Public DNS record

Orange A-SBC can be reached via Fully Qualified Domain Name (FQDN) type SRV or type A deployed on public DNS. Customer premise ASBCE requires a record on public DNS that enables to reach it using FQDN via public internet. BTIPoI can be reached using FQDN only, whereas BToI can be reached either via public IP address or FQDN.

- BTIPoI supports type SRV & type A for DNS resolution and do not support direct public IP connections.
- BToI supports both public IP and type A for DNS resolution and do not provide any type of SRV record connections.

2.4.5 Firewall updates

Firewalls in the way of traffic between ASBCE and A-SBC must be updated in order to open required ports. BToI and BTIPoI vary concerning the UDP port range.

The media UDP port ranges required by Orange BTIPoI SIP Trunk is **6000-38000** and for Orange BToI SIP Trunk is **6000-20000**.

BTIPoI/BToI port matrix				
Source device	Source ports	Destination device	Destination ports	Purpose
ASBCE public @IP	Defined Signaling port range on ASBCE: Network & Flows -> Advanced Options e.g. TCP 51001-55000 Depending on customer context or needs.	A-SBC public @IP	TCP 5061	TLS SIP signaling
A-SBC public @IP	TCP Any	ASBCE public @IP	TCP 5061	
ASBCE public @IP	BTIPoI: UDP 6000-38000 BToI: UDP 6000-20000	A-SBC public @IP	BTIPoI: UDP 6000-38000 BToI: UDP 6000-20000	SRTP media
A-SBC public @IP	BTIPoI: UDP 6000-38000 BToI: UDP 6000-20000	ASBCE public @IP	BTIPoI: UDP 6000-38000 BToI: UDP 6000-20000	

2.4.6 Certificate updates

To ensure the security of traffic, public root & intermediate certificates need to be exchanged between ASBCE and Orange A-SBC. ASBCE would require an identity certificate signed by a public root CA certificate (including any intermediate certificates in the path). The customer should send public Root & Intermediate certificates which signed ASBCE identity certificate to OBS to be uploaded on Orange A-SBC in case of using a different Public Certificate Authority on their side. This is described in detail in following chapters of ASBCE secure configuration.

In case of different public Root & intermediate certificates used by Orange (Digicert) Customer should retrieve ours which signed Orange A-SBC's certificates and upload them to ASBCE. The **Root and the Intermediate Orange CA** included in the DigiCert CA by following the procedure described below. Connect to the Digicert site: https://www.digicert.com/digicert-root-certificates.htm then download and import (pem format):

- the Root CA: **DigiCert Global Root CA**
- the Intermediate CA: **DigiCert TLS RSA SHA256 2020 CA1**

Upload of the Root and Intermediate Orange CA to ASBCE is described in detail in following chapters of ASBCE secure configuration.

2.4.7 TLS Mutual Authentication Mechanism Support regarding public certificate Extended Key Usage (EKU)

Since mid-2026 public Certificate Authorities (CA's) have progressively issued TLS certificates with the **Server Authentication Extended Key Usage only (EKU),** removing Client Authentication EKU by default, in all end-entity public certificate.

This change follows the **Google Chrome Root Program requirement** (decision made in last October 2024) that publicly **trusted TLS x.509 certificates must no longer support both Server Authentication and Client Authentication purposes, leaving only Server Authentication EKU in.**

Some CAs, such as DigiCert, offer a **grace period** during which End- Entity certificates with both Server Authentication and Client Authentication EKUs can still be requested. By default, DigiCert issues certificates with Server Authentication EKU only. This dual-EKU option is available on request until 1 March 2027. After that date, only Server Authentication EKU will be included.

Source: https://knowledge.digicert.com/alerts/sunsetting-client-authentication-eku-from-digicert-public-tls-certificates

Please check your CA provider policy:

1. Grace period available: dual-EKU certificates remain supported for a limited period of time
2. No grace period: both the Orange aSBC and the customer SBC/IPBX must use Server Authentication–only certificates.

In the 2nd scenario, where both endpoints use public certificates with the Server Authentication EKU only, **Orange validates mutual TLS interoperability through testing**.

The impact on mutual authentication may depend on:

- which endpoint acts as the TLS client or TLS server.
- and the vendor capabilities for handling certificates without the Client Authentication EKU

Case 1: Avaya ASBCE initiates the TLS handshake.

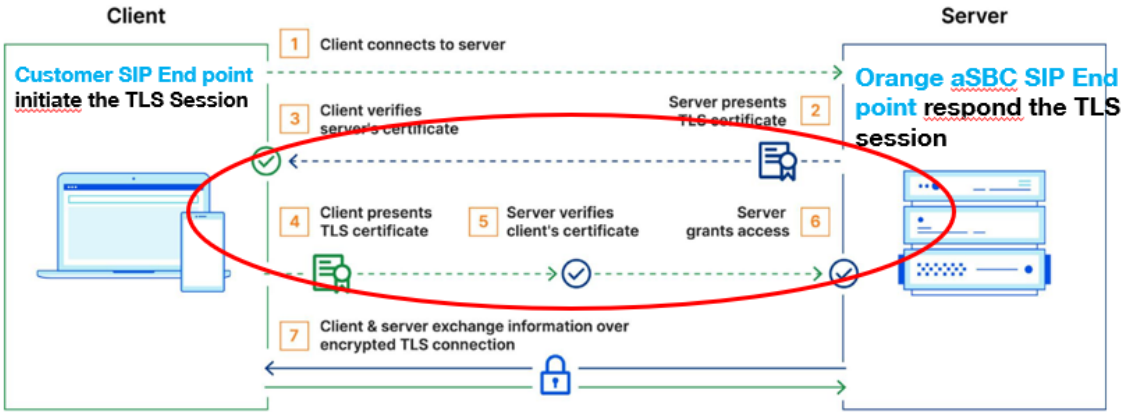
In this scenario:

- The Avaya ASBCE acts as the TLS client.
- The Orange aSBC acts as the TLS server.
- The Avaya ASBCE initiates the TLS handshake.

The Orange aSBC requests a certificate from the Avaya ASBCE to perform mutual TLS authentication.

TLS handshake sequence

1. The Orange aSBC requests the customer certificate (TLS message “Certificate request”)
2. The Avaya ASBCE presents its certificate with Server Authentication (serverAuth) EKU only [4].
3. The Orange aSBC verifies the certificate [5] and grants access [6].



Result: Mutual TLS continues to work when the Avaya ASBCE initiates the connection, even if the customer public certificate contains the serverAuth EKU only.

No specific Avaya ASBCE change is required for this scenario.

Case 2: Orange aSBC initiates the TLS

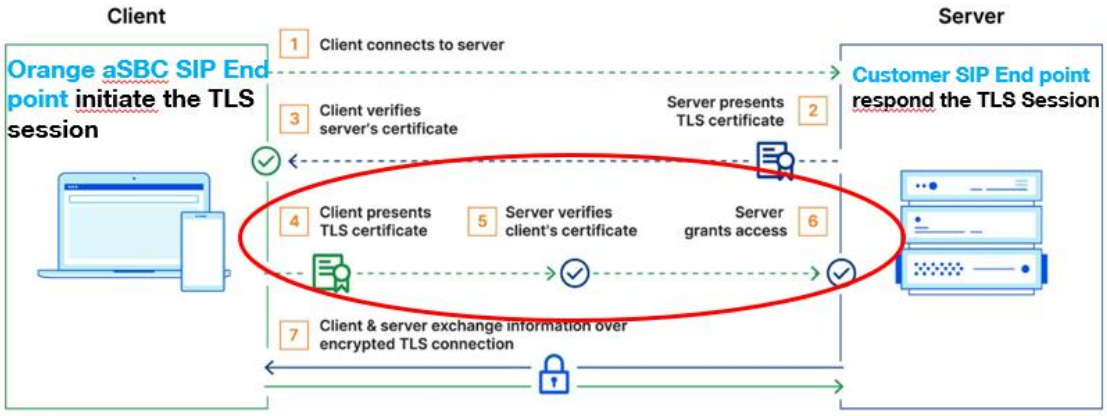
In this scenario:

- The Orange aSBC acts as the TLS client.
- The Avaya ASBCE acts as the TLS server.
- The Orange aSBC initiates the TLS handshake.

The Avaya ASBCE requests a certificate from the Orange aSBC in order to perform mutual TLS authentication. Orange aSBC presents its public certificate containing the serverAuth EKU only.

TLS handshake sequence

1. The Avaya ASBCE requests the Orange certificate.
2. The Orange aSBC presents its certificate with Server Authentication (serverAuth) EKU only **[4]**.
3. The Avaya ASBCE verifies the certificate **[5]** and grants access **[6]**.



Result: Mutual TLS continues to work when the Orange aSBC initiates the connection, even if the customer public certificate contains the serverAuth EKU only.

No specific Avaya ASBCE change is required for this scenario.

2.4.8 TLS v1.3 and v1.2 cipher suites compliance

The following cipher suites are supported by Orange SBC for TLS 1.3 (recommended version) and TLS 1.2 (alternative version). Compliant cypher suites with Orange SBC are marked in bold.

TLS 1.3

- **TLS_AES_256_GCM_SHA384** (0x1302)
- **TLS_AES_128_GCM_SHA256** (0x1301)
- **TLS_CHACHA20_POLY1305_SHA256** (0x1303)

TLS 1.2

- **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** (0xc030)
- **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** (0xc02f)

Cipher suites supported by ASBCE version from 10.2 release for TLS 1.3 and TLS 1.2 are listed below. Compliant cipher suites with Orange SBC are marked in bold. At least one ASBCE cipher suite must be compliant with BTol/BTIPol to work.

- **TLS_AES_256_GCM_SHA384** (0x1302)
- **TLS_CHACHA20_POLY1305**_SHA256 (0x1303)
- **TLS_AES_128_GCM_SHA256** (0x1301)
- TLS_AES_128_CCM_SHA256 (0x1304)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
- **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** (0xc030)
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
- **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** (0xc02f)
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)

ASBCE and A-SBC will negotiate the most TLS 1.3 secure matched cipher suite (**TLS_AES_256_GCM_SHA384** (0x1302)) to establish TLS connection.

Cipher suites supported by **ASBCE versions 8.1.2 hotfix1 and 10.1 hotfix 1** for TLS 1.2 (TLS 1.3 is not supported by both ASBCE versions) are listed below. Compliant cipher suites with Orange SBC are marked in bold. At least one ASBCE cipher suite must be compliant with BTol/BTIPol to work.

- **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** (0xc030)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)
- TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084)
- **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** (0xc02f)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)
- TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0041)

ASBCE and A-SBC will negotiate the most TLS 1.2 secure matched cipher suite (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(0xc030)) to establish TLS connection.

Note: The Avaya “ASBCE encryption license” is required to activate TLS on ASBCE SIP trunk.

2.4.9 SRTP encryption on BTIPoI/BToI

Media encryption preferred format: AES_CM_128_HMAC_SHA1_80

2.4.10 Supported codecs on BTIPoI/BToI

Supported codec is G.711A (20ms) for BTIPoI and BToI.
G.711u (20ms) can be requested on specific case for BToI.

3 Parameters to be provided by customer to access BTIP service

IP addresses marked in red must be indicated by the Customer, depending on Customer architecture scenario.

3.1 Architecture without "Customer SBC" over BVPN

Head Quarter (HQ) architecture	Level of Service	Customer IP addresses used by the service	
		Nominal	Backup
ARCHITECTURE 1: NO REDUNDANCY			
1 IPO Server (Call Server) or 1 IPO IP500V2 system	No redundancy 1 single call server or 1 IP500v2 system	IPO IP@	N/A
ARCHITECTURE 2: REDUNDANCY - 2 IPO systems (active/active) - 1 NUMBERING PLAN			
2 IPO systems (active/active), nominal/backup for a group of users (1 numbering plan). The IPO systems can be hosted by the same site or by 2 different physical sites. Each IPO system (IPO1 and IPO2) has its own SIP trunk but IPO2 is only used as a backup. Both IPO systems are independent but considered as being part of one HQ. - Nominal mode: All users register with IPO1 - Backup mode: All users re-register with IPO2 Remark: 1 IPO system can be 1 IPO Server (Call Server) or 1 IPO IP500V2 system	User registration redundancy (IP phones only) Rerouting at SBC level	IPO1 IP@	IPO2 IP@
ARCHITECTURE 3: REDUNDANCY - 2 IPO systems (active/active) - 2 NUMBERING PLANS			
2 IPO systems (active/active) hosted by 2 different physical sites. Each IPO system manages a range of users (2 numbering plans). Each IPO system (IPO1 and IPO2) has its own SIP trunk and each manages its own group of users in nominal mode. - Nominal mode: All HQ1 users register with IPO1 HQ1 All HQ2 users register with IPO2 HQ2 - Backup mode: In case of IPO1 HQ1 crash, all HQ1 users re-register onto IPO2 HQ2 In case of IPO2 HQ2 crash, all HQ2 users re-register with IPO1 HQ1 Remark: 1 IPO system can be 1 IPO Server (Call Server) or 1 IPO IP500V2 system Warnings: Both HQ accesses capacity to be sized adequately	**For IPO1 HQ1** User registration redundancy (IP phones only) Rerouting at AS level	IPO1 HQ1 IP@	N/A
	For IPO2 HQ2 User registration redundancy (IP phones only) Rerouting at AS level	IPO2 HQ2 IP@	N/A

Remote Site (RS) architecture Any Remote site architecture can be associated to any Head Quarter Architecture listed above	Level of Service	Customer IP addresses used by the service	
		Nominal	Backup
Remote site without Avaya media gateway (IP500v2) / **ARCHITECTURES 1 or 2**	No survivability, no trunk redundancy	N/A	N/A
Remote site without Avaya media gateway (IP500v2) / **ARCHITECTURE 3**		N/A	N/A
Remote site with Avaya media gateway (IP500v2) / **ARCHITECTURES 1 or 2**	Local site survivability and trunk redundancy via PSTN only	N/A	N/A
Remote site with Avaya media gateway (IP500v2) / **ARCHITECTURE 3**		N/A	N/A
Remote site with Avaya gateway (IP500v2) + SIP trunk as backup / **ARCHITECTURES 1 or 2**	Local survivability for the remote site hosting the gateway/SIP Trunk in case of non-access to HQ (HQ crash) Nominal outgoing and incoming traffic goes through HQ	GW IP@	N/A
Remote site with Avaya gateway (IP500v2) + SIP trunk as backup / **ARCHITECTURE 3**		GW IP@	N/A

3.2 Architecture with "Customer SBC" over BVPN

Architecture with Customer SBC over BVPN	Level of Service	Customer IP addresses used by the service	
		Nominal	Backup
ARCHITECTURE 4: Avaya Session Border Controller Enterprise (ASBCE)			
Single ASBCE	No redundancy	ASBCE IP@	NA
One ASBCE pair **in High Availability vendor mode** A pair consists in one SBCE server acting as primary (active) and another one server as secondary (standby). Both SBCE servers share the same IP@ (ASBCE VIP@).	Local vendor redundancy with nominal/backup behaviour. The 2 SBCE servers can be located on two different geographic sites but Layer 2 connection between servers 150 ms max round Trip is required. Loss of audio for all active calls on primary SBCE by only 1 second when it fails and its connection with the secondary ASBCE server is up. Loss of audio for all active calls on primary SBCE by 15 seconds when it fails and its connection with the secondary ASBCE server is down.	ASBCE VIP@	NA

Two ASBCE (ASBCE1 and ASBCE2) **in Nominal/Backup mode on vendor side**	Local vendor redundancy with nominal/backup behaviour. Both ASBCE are hosted on the same site. Nominal/Backup mode on Orange a-SBC side for incoming traffic to the customer ASBCE. Loss of active calls handled by the ASBCE that fails.	ASBCE1 IP@	ASBCE2 IP@
Two ASBCE pairs in High Availability and in Nominal/Backup mode on vendor side One ASBCE1 pair (2 ASBCE servers) with shared ASBCE1 VIP@ and one ASBCE2 pair (2 ASBCE servers) with shared ASBCE2 VIP@).	Local/geographical redundancy. The two ASBCE pairs are hosted on the same site or on 2 different geographic sites. Nominal/Backup mode on Orange a-SBC side for incoming traffic to the customer ASBCE pairs. If a full ASBCE pair fails, active calls are lost. Loss of audio for all active calls on primary SBCE of a pair by only 1 second when it fails and its connection with the secondary ASBCE server is up. Loss of audio for all active calls on primary SBCE of a pair by 15 seconds when it fails and its connection with the secondary ASBCE server is down.	ASBCE1 VIP@	ASBCE2 VIP@

Remote Site (RS) architecture Any Remote site architecture can be associated to any Customer SBC Architecture listed above	Level of Service	Customer IP addresses used by the service	
		Nominal	Backup
Remote site without Avaya media gateway (IP500v2) / **ARCHITECTURE 4**	No survivability, no trunk redundancy	N/A	N/A
Remote site with Avaya media gateway (IP500v2) / **ARCHITECTURE 4**	Local site survivability and trunk redundancy via PSTN only	N/A	N/A

3.3 Architecture with "Customer SBC" over Internet for BTIPoI

Architecture with Customer SBC over Internet	Level of Service	Customer IP addresses used by the service	
		Nominal	Backup
ARCHITECTURE 5: Avaya Session Border Controller Enterprise (ASBCE)			
Single ASBCE	No redundancy	ASBCE public FQDN DNS type A or type SRV	NA
One ASBCE pair **in High Availability vendor mode** A pair consists in one SBCE server acting as primary (active) and another one server as secondary (standby). Both SBCE servers share the same IP@ (ASBCE VIP@).	Local vendor redundancy with nominal/backup behaviour. The 2 SBCE servers can be located on two different geographic sites but Layer 2 connection between servers 150 ms max round Trip is required. Loss of audio for all active calls on primary SBCE by only 1 second when it fails and its connection with the secondary ASBCE	ASBCE public FQDN DNS type A or type SRV	NA

	server is up. Loss of audio for all active calls on primary SBCE by 15 seconds when it fails and its connection with the secondary ASBCE server is down.		
Two ASBCE (ASBCE1 and ASBCE2) **in Nominal/Backup mode on vendor side**	Local vendor redundancy with nominal/backup behaviour. Both ASBCE are hosted on the same site. Nominal/Backup mode on Orange a-SBC side for incoming traffic to the customer ASBCE. Loss of active calls handled by the ASBCE that fails.	ASBCE1 public FQDN DNS type A or type SRV	ASBCE2 public FQDN DNS type A or type SRV
Two ASBCE pairs in High Availability and in Nominal/Backup mode on vendor side One ASBCE1 pair (2 ASBCE servers) with shared ASBCE1 VIP@ and one ASBCE2 pair (2 ASBCE servers) with shared ASBCE2 VIP@).	Local/geographical redundancy. The two ASBCE pairs are hosted on the same site or on 2 different geographic sites. Nominal/Backup mode on Orange a-SBC side for incoming traffic to the customer ASBCE pairs. If a full ASBCE pair fails, active calls are lost. Loss of audio for all active calls on primary SBCE of a pair by only 1 second when it fails and its connection with the secondary ASBCE server is up. Loss of audio for all active calls on primary SBCE of a pair by 15 seconds when it fails and its connection with the secondary ASBCE server is down.	ASBCE1 public FQDN DNS type A or type SRV	ASBCE2 public FQDN DNS type A or type SRV

Remote Site (RS) architecture Any Remote site architecture can be associated to any Customer SBC Architecture listed above	Level of Service	Customer IP addresses used by the service	
		Nominal	Backup
Remote site without Avaya media gateway (IP500v2) / **ARCHITECTURE 5**	No survivability, no trunk redundancy	N/A	N/A
Remote site with Avaya media gateway (IP500v2) / **ARCHITECTURE 5**	Local site survivability and trunk redundancy via PSTN only	N/A	N/A

3.4 Architecture with "Customer SBC" over Internet for BToI

Architecture with Customer SBC over Internet	Level of Service	Customer IP addresses used by the service	
		Nominal	Backup
ARCHITECTURE 6: Avaya Session Border Controller Enterprise (ASBCE)			
Single ASBCE	No redundancy	ASBCE public IP@ or public FQDN DNS type A	NA
One ASBCE pair **in High Availability vendor mode** A pair consists in one SBCE server acting as primary (active) and another one server as secondary (standby).	Local vendor redundancy with nominal/backup behaviour. The 2 SBCE servers can be located on two different geographic sites but Layer 2 connection between servers 150 ms max	ASBCE public IP@ or public FQDN DNS type A	NA

Both SBCE servers share the same IP@ (ASBCE VIP@).	round Trip is required. Loss of audio for all active calls on primary SBCE by only 1 second when it fails and its connection with the secondary ASBCE server is up. Loss of audio for all active calls on primary SBCE by 15 seconds when it fails and its connection with the secondary ASBCE server is down.		
Two ASBCE (ASBCE1 and ASBCE2) **in Nominal/Backup mode on vendor side**	Local vendor redundancy with nominal/backup behaviour. Both ASBCE are hosted on the same site. Nominal/Backup mode on Orange a-SBC side for incoming traffic to the customer ASBCE. Loss of active calls handled by the ASBCE that fails.	ASBCE1 public IP@ or public FQDN DNS type A	ASBCE2 public IP@ or public FQDN DNS type A
Two ASBCE pairs in High Availability and in Nominal/Backup mode on vendor side One ASBCE1 pair (2 ASBCE servers) with shared ASBCE1 VIP@ and one ASBCE2 pair (2 ASBCE servers) with shared ASBCE2 VIP@).	Local/geographical redundancy. The two ASBCE pairs are hosted on the same site or on 2 different geographic sites. Nominal/Backup mode on Orange a-SBC side for incoming traffic to the customer ASBCE pairs. If a full ASBCE pair fails, active calls are lost. Loss of audio for all active calls on primary SBCE of a pair by only 1 second when it fails and its connection with the secondary ASBCE server is up. Loss of audio for all active calls on primary SBCE of a pair by 15 seconds when it fails and its connection with the secondary ASBCE server is down.	ASBCE1 public IP@ or public FQDN DNS type A	ASBCE2 public IP@ or public FQDN DNS type A

Remote Site (RS) architecture Any Remote site architecture can be associated to any Customer SBC Architecture listed above	Level of Service	Customer IP addresses used by the service	
		Nominal	Backup
Remote site without Avaya media gateway (IP500v2) / **ARCHITECTURE 6**	No survivability, no trunk redundancy	N/A	N/A
Remote site with Avaya media gateway (IP500v2) / **ARCHITECTURE 6**	Local site survivability and trunk redundancy via PSTN only	N/A	N/A

4 BTIP/BTalk/BTIPol/BTol IP Office certified versions

Orange supports the last 2 major IPBX versions only if still supported by Avaya and will ensure Business Talk and BTIP infrastructure evolutions will rightly interwork with the related architectures. Orange will assist customers running supported IPBX versions and facing issues.

Avaya standard support policy is to provide support for the most current major releases via standard software service pack processes.

For more details about the versions supported by Avaya, please refer to Lifecycle Summary Matrix and PCN and PSN Reports available on the Avaya Support Web site https://support.avaya.com.

4.1 Avaya IP Office versions supported with BTIP/BTalk/BTIPol/BTol

AVAYA IP OFFICE IPBX – software versions						
Reference products & versions		✓: Certified NS : No supported				Comments/restrictions
AVAYA IP Office Select edition	With Avaya Session Border Controller for Enterprise	**Orange Services**				
		BTIP	**BTIPol**	**BTalk**	**BTol**	
Avaya 12.3 (12.3.0.0.0 build 26)	10.2.1.3-111-25777	✓	✓	✓	✓	**To avoid any security risk the clients should always install on ASBCE but also on IP Office platforms the latest mandatory patch/hotfix released by the Avaya vendor.**
Avaya 12.2 (12.2.0.0.0 build 58)	10.2.1.0-101-24795 + SSP007	✓	✓	✓	✓	
Avaya 12.0 (12.0.0.0.0 build 56)	10.2.1.0-101-24795	✓	✓	✓	✓	
Avaya 12.0 (12.0.0.0.0 build 56)	10.2.0.1-89-24401	✓	✓	✓	✓	
Avaya 11.1 FP3 (11.1.3.0.0 build 23)	10.1.2.0-64-23285	✓	✓	✓	✓	
Avaya 11.1 FP2 SP4 (11.1.2.4.0 build 18)	8.1.3.2-38-22279 + Hotfix-3 sbce-8.1.3.2-38-23109-hotfix-03082023.tar.gz	✓	✓	✓	✓	
Avaya 11.1 FP2 SP2 (11.1.2.2.0 build 20)	*From 8.1.3.1-38-21632 + Hotfix-3 sbce-8.1.3.1-39-22407-hotfix-08232022.tar.gz*	**Versions not supported**				**These IP Office versions limit the tag value in SIP headers to 80 characters. During Full-IP transition or with third-party operators, this limit can be exceeded, causing call cancellations. Upgrading to version 11.1 FP2 SP4 or higher is recommended.**
Avaya 11.1 FP2 SP1 (11.1.2.1.0 build 3)	*From 8.1.3.1-38-21632 + Hotfix-3 sbce-8.1.3.1-39-22407-hotfix-08232022.tar.gz*					
Avaya 11.1 FP1 (11.1.1.0 build 209)	*From 8.1.2.0-31-19809 + Hotfix-8 sbce-8.1.2.0-37-21486-hotfix-01062022.tar.gz*					
Avaya 11.0 FP4 SP2 (11.0.4.2.0 build 58)	*NA*					
Avaya 11.0 FP4 (11.0.4.0 build 74)	*NA*					

4.2 Avaya IP Office endpoints and applications

Reference product		Software version NA: not applicable	Certification ✓: Certified ✓: Not certified NS: No supported	Comments
Avaya IPBX components	IP Office Server Edition	12.3.0.0.0 build 26	✓	
		12.2.0.0.0 build 58	✓	
		12.0.0.0.0 build 56	✓	
		11.1.3.0 build 23	✓	
		11.1.2.4.0 build 18	✓	
	IP Office UC module	Not supported on R12.3	NS	
		11.1.3.0 build 23		
		11.1.2.4.0 build 18	✓	
Avaya Gateway	IP500v2	12.3.0.0 build 26	✓	
		12.2.0.0 build 58	✓	
		12.0.0.0 build 56	✓	
		11.1.3.0 build 23	✓	
		11.1.2.4.0 build 18	✓	
Avaya Voice Mail	VoiceMail Pro	12.3.0.0 build 7	✓	
		12.2.0.0 build 12	✓	
		12.0.0.0 build 14	✓	
		11.1.3.0 build 7	✓	
		11.1.2.4.0 build 2	✓	
Avaya Unified Communications and Mobility	One-X Portal	12.3.0.0 build 47	✓	
		12.2.0.0 build 50	✓	
		12.0.0.0 build 21	✓	
		11.1.3.0 build 26	✓	
		11.1.2.4.0 build 3	✓	
Third-party endpoints & Applications	ISI-COM Interact	7.x/8.x	✓	
Avaya endpoints	B179 SIP conference phones	Please consult the Product Compatibility Matrix tool available at :https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml to identify the software releases compatible with each Avaya IP Office release.	✓	
	J129 SIP phones			
	J129/J139/J169/J179 SIP phones			
	1603L, 1608L, 1616L IP phones			
	1603, 1608, 1616 IP phones			
	9608, 9611G, 9621G, 9641G, 9641GS IP phones			
Avaya Attendant	IP Office Softconsole		✓	
Avaya Softphone	Workplace client (for Windows, Android, iOS)		✓	
Avaya DECT	Avaya 3730,3735 DECT phones		✓	
	Avaya 3720,3725 DECT phones			
	Avaya 3749 DECT phones			
	Avaya 3740,3745 DECT phones			
	DECT R4 – IPBS3		✓	

Fax	Analog fax on IP500v2 Gateway	NA	✓	T.38 and G.711 inband fax are enabled on the BTalk network without an end-to-end guarantee. Orange cannot certify the reliability of fax interoperability that may occur at interconnection points with terminating carriers.

5 IP Office SIP trunking configuration checklist

The checklist below presents all the steps of configuration required for interoperability between **BTIP/BT** and Avaya IP Office.

Trunk configuration - IP Office Server Edition

Access type: IP Office Web Manager page.

Platform	Configuration place	Configuration details
Services		
Primary IPO	System	running services: ▪ IP Office ▪ Voicemail ▪ One-X Portal ▪ Web Manager ▪ Web License Manager ▪ Web Collaboration ▪ WebRTC Gateway ▪ Web Client

Access type: IP Office Manager application.

Platform	Menu	Object	Tab	Parameter	Value
System configuration – Locale configuration					
Every platform in the solution[1]	System	-	System	Locale	France2 (French)
System configuration – DSCP configuration					
Every platform in the solution	System	-	LAN1 -> VoIP	DSCP (Hex) / DSCP	B8 / 46
				Video DSCP (Hex) / Video DSCP	88 / 34
				SIG DSCP (Hex) / SIG DSCP	B8 / 46
DHCP configuration offer					
Primary IPO	System	-	LAN1 -> DHCP Poll	Start address	Start IP address
				Subnet Mask	Subnet Mask
				Default Router	Router IP address
				Pool size	DHCP pool size

[1] Every platform in the solution: primary IPO, secondary IPO (if used), expansion units (if used)

Codec configuration					
Every platform in the solution	System	-	Telephony -> Telephony	Companding Law	A-Law
				High Quality Conferencing	Checked
			VoIP	Ignore DTMF Mismatch For Phones	Checked
				RFC2833 Default Payload	101
				Default Codec Selection -> Selected	G.722 64K G.711 ALAW 64K* (*or G.711 ULAW 64K in option)
Call Admission Control & Location configuration[2]					
Solution level	Location	Location	Location	Location Name	Ex:RS140
				Subnet Address	6.201.40.0
				Subnet Mask	255.255.255.0
				Parent Location for CAC	<None>
				Call Admission Control -> Total Maximum Calls	99
				Call Admission Control -> External Maximum Calls	99
				Call Admission Control -> Internal Maximum Calls	99
Every platform in the solution	System	-	System	Location	Ex: HQ313
Fallback configuration[3]					
Primary IPO	Location	Location	Location	Fallback System	Local GW's IP address
SCN lines configuration					
Primary IPO[4]	Line	IP Office line [5]	Line	Outgoing Group ID	99998
				Transport Type	Proprietary
				Networking Level	SCN
				Gateway -> Address	Backup IPO's IP address
				Gateway -> Location	Location name

[2] For each physical site (Headquarter and Remote Sites) dedicated location has to be created, mainly for Call Admission Control and emergency calls management. This section provides example values.

[3] For each location where local gateway should act as a backup system in case of primary server failure Fallback System should be defined.

[4] Repeat the steps on primary IPO to create separate SCN line for each local gateway in the solution.

[5] SCN Line to secondary server

				SCN Resiliency Options -> Supports Resiliency	Checked
				- Backs up my IP Phones	Checked
				- Backs up my Hunt Groups	Checked
				- Backs up my Voicemail	Checked
				- Backs up my IP Dect Phones	Checked
				- Backs up my One-x Portal	Checked
			VoIP settings	Allow Direct Media Path	Checked
		IP Office Line [6]	Line	Outgoing Group ID	99901 - 99930
				Transport Type	Proprietary
				Networking Level	SCN
				Gateway -> Address	Local GW's IP address
				Gateway -> Location	Location name
				SCN Resiliency Options -> Supports Resiliency	Checked
				- Backs up my IP Phones	Unchecked
				- Back up my Hunt Groups	Unchecked
				- Back up my IP Dect Phones	Unchecked
			VoIP settings	Allow Direct Media Path	Checked
Secondary IPO (if used)[7]	Line	IP Office line [8]	Line	Outgoing Group ID	99999
				Transport Type	Proprietary
				Networking Level	SCN
				Gateway -> Address	Primary IPO's IP address
				Gateway -> Location	Location name
				SCN Resiliency Options -> Supports Resiliency	Checked
				- Backs up my IP Phones	Checked
				- Backs up my Hunt Groups	Checked

[6] SCN Line to expansion gateway

[7] Repeat the steps on secondary IPO (if used) to create separate SCN line for each local gateway in the solution.

[8] SCN Line to Primary server

				- Back up my Voicemail	Checked
				- Back up my IP Dect Phones	Checked
				- Back up my one-X Portal	Checked
			VoIP settings	Allow Direct Media Path	Checked
		IP Office Line [9]	Line	Outgoing Group ID	99901 - 99930
				Transport Type	Proprietary
				Networking Level	SCN
				Gateway -> Address	Local GW's IP address
				Gateway -> Location	Location name
				SCN Resiliency Options -> Supports Resiliency	Unchecked
			VoIP settings	Allow Direct Media Path	Checked
Expansion Gateway	Line[10]	IP Office line [11]	Line	Outgoing Group ID	99999
				Transport Type	Proprietary
				Networking Level	SCN
				Gateway -> Address	Primary IPO's IP address
				Gateway -> Location	Location name
				SCN Resiliency Options -> Supports Resiliency	Checked
			VoIP Settings	Allow Direct Media Path	Checked
		IP Office Line [12]	Line	Outgoing Group ID	99998
				Transport Type	Proprietary

[9] SCN line to expansion gateway

[10] Redundant architecture only

[11] SCN line to Primary server

[12] SCN line to secondary server

				Networking Level	SCN
				Gateway -> Address	Backup IPO's IP address
				Gateway -> Location	Location name
				SCN Resiliency Options -> Supports Resiliency	Unchecked
			VoIP Settings	Allow Direct Media Path	Checked
SCN lines configuration – local PSTN access					
Expansion Gateway	Line	PRI 30 (Universal)[13]	PRI line	Incoming Group ID	3
				Outgoing Group ID	3
SIP Trunks configuration – Global settings					
Primary IPO	System	-	LAN1 -> VoIP	SIP Trunks Enable	Checked
				SIP Registrar Enable	Checked
				Media Connection Preservation	Enabled
				Inhibit Off-Switch Forward/Transfer	Unchecked
Secondary IPO (if used)	System	-	LAN1 -> VoIP	SIP Trunks Enable	Checked
				SIP Registrar Enable	Checked
				Media Connection Preservation	Enabled
				Inhibit Off-Switch Forward/Transfer	Unchecked
SIP Trunks configuration – SIP line					
Primary IPO	Line	SIP Line	SIP Line	Line Number	10
				Local Domain Name	Primary IPO's IP address
				Location	Cloud
				Prefix	0
				National Prefix	00
				Country Code	33
				International Prefix	000

[13] Line type depends on line type attached to Expansion Gateway

				In service	Checked
				Check OOS	Checked
				Session Timers -> Refresh Nethod	Reinvite
				Session Timers -> Timer (seconds)	14880
				Redirect and Transfer -> Incoming Supervised REFER	Never
				Redirect and Transfer -> Outgoing Supervised REFER	Never
			Transport	ITSP Proxy Address	primary SBC's IP address
				Layer 4 Protocol	UDP
				Network Configuration -> Use Network Topology Info	None
				Send Port	5060
				Listen Port	5060
			Call Details	Incoming Group	10
				Outgoing Group	10
				Max Sessions	Default=10 Range 1 - 250
				Local URI -> Display	Use Internal Data
				Local URI -> Content	Use Internal Data
				Local URI -> Fleld meaning -> Forwarding/Outgoing calls	Caller
				Local URI -> Fleld meaning -> Forwarding/Twinning	Original Caller
				Local URI -> Fleld meaning -> Forwarding/Incoming calls	Called
				Contact-> Display	Use Internal Data
				Contact-> Content	Use Internal Data
				Contact -> Fleld meaning -> Outgoing calls	Caller
				Contact -> Fleld meaning -> Forwarding/Twinning	Original Caller
				Contact -> Fleld meaning -> Incoming calls	Called
				Diversion Header	Checked

				Diversion Header -> Display	Use Internal Data
				Diversion Header -> Content	Use Internal Data
				Diversion Header -> Fleld meaning -> Outgoing Calls	None
				Diversion Header -> Fleld meaning -> Forwarding/Twinning	Caller
				Diversion Header -> Fleld meaning -> Incoming Calls	None
			VoIP	Codec Selection	Custom
				DTMF Support	RFC2833/RFC4733
				Local HOLD Music	Checked
				RE-invite Supported	Checked
				Allow Direct Media Path	Checked
				Force direct media with phones	Checked
				PRACK/100rel Supported	Checked
			SIP Advanced	Use + for International	On/Off [14]
				Caller ID from From Header	Checked
				Send From in Clear	Checked
				Cache Auth Credentials	Unchecked
				Add UUI Header	Checked
				Add UUI Header to redirected calls	Checked
				Media -> P-Early-Media Support	All
				Media -> Force Early Direct Media	Checked
				Media -> Media Connection Preservation	System
				Media -> Media Indicate HOLD	Checked
				Call Control -> Call Initiation Timeout (s)	18

[14] When set to On, outgoing international calls use E.164/International format with a '+' followed by the country code and then the directory number (optional).

				Call Control -> Call Queuing Timeout (m)	1
				Call Control -> Service Busy Response	503 – Service Unavailable
				Call Control -> on No User Responding Send	480-Temporarily Unavailable
				Call Control -> Action on CAC Location limit	Allow Voicemail / Reject Call
				Call Control -> Suppress Q.850 Reason Header	Checked
			Engineering	Custom String	SLIC_NO_USER_AVAIL=480
		SIP Line	SIP Line	Line Number	11
				Local Domain Name	Primary IPO's IP address
				Location	Cloud
				Prefix	0
				National Prefix	00
				Country Code	33
				International Prefix	000
				In service	Checked
				Check OOS	Checked
				Session Timers -> Refresh Nethod	Reinvite
				Session Timers -> Timer (seconds)	14880
				Redirect and Transfer -> Incoming Supervised REFER	Never
				Redirect and Transfer -> Outgoing Supervised REFER	Never
			Transport	ITSP Proxy Address	backup SBC's IP address
				Layer 4 Protocol	UDP
				Network Configuration -> Use Network Topology Info	None
				Send Port	5060
				Listen Port	5060

			Call Details	Incoming Group	11
				Outgoing Group	11
				Max Sessions	Default=10 Range 1 - 250
				Local URI -> Display	Use Internal Data
				Local URI -> Content	Use Internal Data
				Local URI -> Fleld meaning -> Forwarding/Outgoing calls	Caller
				Local URI -> Fleld meaning -> Forwarding/Twinning	Original Caller
				Local URI -> Fleld meaning -> Forwarding/Incoming calls	Called
				Contact-> Display	Use Internal Data
				Contact-> Content	Use Internal Data
				Contact -> Fleld meaning -> Outgoing calls	Caller
				Contact -> Fleld meaning -> Forwarding/Twinning	Original Caller
				Contact -> Fleld meaning -> Incoming calls	Called
				Diversion Header	Checked
				Diversion Header -> Display	Use Internal Data
				Diversion Header -> Content	Use Internal Data
				Diversion Header -> Fleld meaning -> Outgoing Calls	None
				Diversion Header -> Fleld meaning -> Forwarding/Twinning	Caller
				Diversion Header -> Fleld meaning -> Incoming Calls	None
			VoIP	Codec Selection	Custom
				Codec Selected	G.722 64K G.711 ALAW 64K* (*or G.711 ULAW 64K in option)
				DTMF Support	RFC2833/RFC4733
				Local HOLD Music	Checked

				RE-ivite Supported	Checked
				Allow Direct Media Path	Checked
				Force direct media with phones	Checked
				PRACK/100rel Supported	Checked
			SIP Advanced	Use + for International	On/Off [15]
				Caller ID from From Header	Checked
				Send From in Clear	Checked
				Cache Auth Credentials	Unchecked
				Add UUI Header	Checked
				Add UUI Header to redirected calls	Checked
				Media -> P-Early-Media Support	All
				Media -> Force Early Direct Media	Checked
				Media -> Media Connection Preservation	System
				Media -> Indicate HOLD	Checked
				Call Control -> Call Initiation Timeout (s)	18
				Call Control -> Call Queuing Timeout (m)	1
				Call Control -> Service Busy Response	503 – Service Unavailable
				Call Control -> on No User Responding Send	480-Temporarily Unavailable
				Call Control -> Action on CAC Location limit	Allow Voicemail / Reject Call[16]
				Call Control -> Suppress Q.850 Reason Header	Checked
			Engineering	Custom String	SLIC_NO_USER_AVAIL=480

[15] When set to On, outgoing international calls use E.164/International format with a '+' followed by the country code and then the directory number (optional).

[16] Two options are possible, depending on the needs. If CAC is reached on Remote Site call can be rerouted to Voicemail located on main site or rejected with 503 message (configured above). If CAC is reached on the main site call will be always rejected, no matter what is configured in this field.

Secondary IPO (if used)	Line	SIP Line	SIP Line	Line Number	110
				Local Domain Name	Secondary IPO's IP address
				Location	Cloud
				Prefix	0
				National Prefix	00
				Country Code	33
				International Prefix	000
				In service	Checked
				Check OOS	Checked
				Session Timers -> Refresh Method	Reinvite
				Session Timers -> Timer (seconds)	14880
				Redirect and Transfer -> Incoming Supervised REFER	Never
				Redirect and Transfer -> Outgoing Supervised REFER	Never
			Transport	ITSP Proxy Address	primary SBC's IP address
				Layer 4 Protocol	UDP
				Network Configuration -> Use Network Topology Info	None
				Send Port	5060
				Listen Port	5060
			Call Details	Incoming Group	110
				Outgoing Group	110
				Max Sessions	Default=10 Range 1 - 250
				Local URI -> Display	Use Internal Data
				Local URI -> Content	Use Internal Data
				Local URI -> Fleld meaning -> Forwarding/Outgoing calls	Caller
				Local URI -> Fleld meaning -> Forwarding/Twinning	Original Caller
				Local URI -> Fleld meaning -> Forwarding/Incoming calls	Called

				Contact-> Display	Use Internal Data
				Contact-> Content	Use Internal Data
				Contact -> Fleld meaning -> Outgoing calls	Caller
				Contact -> Fleld meaning -> Forwarding/Twinning	Original Caller
				Contact -> Fleld meaning -> Incoming calls	Called
				Diversion Header	Checked
				Diversion Header -> Display	Use Internal Data
				Diversion Header -> Content	Use Internal Data
				Diversion Header -> Fleld meaning -> Outgoing Calls	None
				Diversion Header -> Fleld meaning -> Forwarding/Twinning	Caller
				Diversion Header -> Fleld meaning -> Incoming Calls	None
			VoIP	Codec Selection	Custom
				Codec Selected	G.722 64K G.711 ALAW 64K* (*or G.711 ULAW 64K in option)
				DTMF Support	RFC2833/RFC4733
				Local HOLD Music	Checked
				RE-ivite Supported	Checked
				Allow Direct Media Path	Checked
				Force direct media with phones	Checked
				PRACK/100rel Supported	Checked
			SIP Advanced	Use + for International	On/Off [17]
				Caller ID from From Header	Checked
				Send From in Clear	Checked
				Cache Auth Credentials	Unchecked

[17] When set to On, outgoing international calls use E.164/International format with a '+' followed by the country code and then the directory number (optional).

				Add UUI Header	Checked
				Add UUI Header to redirected calls	Checked
				Media -> P-Early-Media Support	All
				Media -> Force Early Direct Media	Checked
				Media -> Media Connection Preservation	System
				Media -> Indicate HOLD	Checked
				Call Control -> Call Initiation Timeout (s)	18
				Call Control -> Call Queuing Timeout (m)	1
				Call Control -> Service Busy Response	503 – Service Unavailable
				Call Control -> on No User Responding Send	480-Temporarily Unavailable
				Call Control -> Action on CAC Location limit	Allow Voicemail / Reject Call[18]
				Call Control -> Suppress Q.850 Reason Header	Checked
			Engineering	Custom String	SLIC_NO_USER_AVAIL=480[19]
		SIP Line	SIP Line	Line Number	111
				Local Domain Name	Secondary IPO's IP address
				Location	Cloud
				Prefix	0
				National Prefix	00
				Country Code	33
				International Prefix	000
				In service	Checked
				Check OOS	Checked

[18] Two options are possible, depending on the needs. If CAC is reached on Remote Site call can be rerouted to Voicemail located on main site or rejected with 503 message (configured above). If CAC is reached on the main site call will be always rejected, no matter what is configured in this field.

[19] This Custom String is required for triggering DTO option, for an unregistered/unplugged phone located on a remote site without media gateway.

				Session Timers -> Refresh Method	Reinvite
				Session Timers -> Timer (seconds)	14880
				Redirect and Transfer -> Incoming Supervised REFER	Never
				Redirect and Transfer -> Outgoing Supervised REFER	Never
			Transport	ITSP Proxy Address	backup SBC's IP address
				Layer 4 Protocol	UDP
				Network Configuration -> Use Network Topology Info	None
				Send Port	5060
				Listen Port	5060
			Call Details	Incoming Group	111
				Outgoing Group	111
				Max Sessions	Default=10 Range 1 - 250
				Local URI -> Display	Use Internal Data
				Local URI -> Content	Use Internal Data
				Local URI -> Fleld meaning -> Forwarding/Outgoing calls	Caller
				Local URI -> Fleld meaning -> Forwarding/Twinning	Original Caller
				Local URI -> Fleld meaning -> Forwarding/Incoming calls	Called
				Contact-> Display	Use Internal Data
				Contact-> Content	Use Internal Data
				Contact -> Fleld meaning -> Outgoing calls	Caller
				Contact -> Fleld meaning -> Forwarding/Twinning	Original Caller
				Contact -> Fleld meaning -> Incoming calls	Called
				Diversion Header	Checked
				Diversion Header -> Display	Use Internal Data

				Diversion Header -> Content	Use Internal Data
				Diversion Header -> Fleld meaning -> Outgoing Calls	None
				Diversion Header -> Fleld meaning -> Forwarding/Twinning	Caller
				Diversion Header -> Fleld meaning -> Incoming Calls	None
			VoIP	Codec Selection	Custom
				Codec Selected	G.722 64K G.711 ALAW 64K* (*or G.711 ULAW 64K in option)
				DTMF Support	RFC2833/RFC4733
				Local HOLD Music	Checked
				RE-ivite Supported	Checked
				Allow Direct Media Path	Checked
				Force direct media with phones	Checked
				PRACK/100rel Supported	Checked
			SIP Advanced	Use + for International	On/Off [20]
				Caller ID from From Header	Checked
				Send From in Clear	Checked
				Cache Auth Credentials	Unchecked
				Add UUI Header	Checked
				Add UUI Header to redirected calls	Checked
				Media -> P-Early-Media Support	All
				Media -> Force Early Direct Media	Checked
				Media -> Media Connection Preservation	System
				Media Indicate HOLD	Checked
				Call Control ->	18

[20] When set to On, outgoing international calls use E.164/International format with a '+' followed by the country code and then the directory number (optional).

				Call Initiation Timeout (s)	
				Call Control -> Call Queuing Timeout (m)	1
				Call Control -> Service Busy Response	503 – Service Unavailable
				Call Control -> on No User Responding Send	480-Temporarily Unavailable
				Call Control -> Action on CAC Location limit	Allow Voicemail / Reject Call[21]
				Call Control -> Suppress Q.850 Reason Header	Checked
			Engineering	Custom String	SLIC_NO_USER_AVAIL=480
DECT line configuration					
Primary IPO	Line	IP DECT Line	Gateway	Enable Provisioning	Checked
				SARI/PARK	PARK license key[22]
				Subscriptions	Auto-Create / Preconfigured
				Authentication Code	1234[23]
				Enable Resiliency	Checked
			VoIP	Gateway IP Address	DECT IPBS's IP address
				Allow Direct Media Path	Checked
				Codec Selection	Custom
				Codec Selected	G.722 64K G.711 ALAW 64K* (*or G.711 ULAW 64K in option)
Security settings for IP DECT					
Primary IPO	Security	Services	HTTP -> Service details	Service Security Level	Unsecure + Secure
		Right Group	IPDECT Group -> HTTP	DECT R4 Provisioning	Checked

[21] Two options are possible, depending on the needs. If CAC is reached on Remote Site call can be rerouted to Voicemail located on main site or rejected with 503 message (configured above). If CAC is reached on the main site call will be always rejected, no matter what is configured in this field.

[22] License number has to match the one configured on DECT IPBS line under SARI

[23] Authentication code has to match the one configured on DECT IPBS under DECT-> System

		Service Users	IPDECTService -> Service User Details	Name	IPDECTService
				Password	password
				Account status	Enabled
				Account Expiry	No Account Expiry
				Right Group Membership	IPDECT Group
Dial Plan configuration[24]					
Dial Plan – General dialing configuration					
Primary IPO	System	-	Telephony ->Telephony	Dial Delay Time (secs)	10
				Dial Delay Count	0
				Default No Answer Time	15
Secondary IPO (if used)	System	-	Telephony ->Telephony	Dial Delay Time (secs)	10
				Dial Delay Count	0
				Default No Answer Time	15
Dial Plan – Short Codes and ARS configuration when local PSTN access is not used					
Primary IPO	ARS	ARS1	ARS	Route Name	Main
			Add…	Code	N
				Feature	Dial
				Telephone Number	N
				Line Group ID	10
			Add…	Code	N
				Feature	Dial
				Telephone Number	N
				Line Group ID	11
	Short Code	Short Code	-	Code	002XXXXXXXX[25]
				Feature	Dial
				Telephone Number	02N
				Line Group ID	50: Main
		Short Code	-	Code	000N;
				Feature	Dial
				Telephone Number	00N
				Line Group ID	50: Main
Secondary IPO	ARS	ARS1	ARS	Route Name	Main

[24] This is common configuration. It may be required to adjust dial plan configuration per particular system.

[25] It is not possible to add one global entry for immediate national numbers, so such configuration should be repeated for each national numbering pattern 00ZABPQMCDU, where Z is a digit from range 1-9.

(if used)			Add…	Code	N
				Feature	Dial
				Telephone Number	N
				Line Group ID	110
			Add…	Code	N
				Feature	Dial
				Telephone Number	N
				Line Group ID	111
	Short Code	Short Code	-	Code	002XXXXXXXX[26]
				Feature	Dial
				Telephone Number	02N
				Line Group ID	50: Main
		Short Code	-	Code	000N;
				Feature	Dial
				Telephone Number	00N
				Line Group ID	50: Main
Dial Plan – Short Codes and ARS configuration when local PSTN access is used[27]					
Primary IPO	ARS	ARS2[28]	ARS	Route Name	PSTN_for_HQ313
			Add…	Code	N
				Feature	Dial
				Telephone Number	9N
				Line Group ID	99901
		ARS1	ARS	Route Name	HQ313
				Alternate Route	PSTN_for_HQ313
			Add…	Code	N
				Feature	Dial
				Telephone Number	N
				Line Group ID	10
			Add…	Code	N
				Feature	Dial
				Telephone Number	N

[26] It is not possible to add one global entry for immediate national numbers, so such configuration should be repeated for each national numbering pattern 00ZABPQMCDU, where Z is a digit from range 1-9.

[27] Below configuration should be repeated for each location using local PSTN access.

[28] Repeat the configuration steps for all Expansion Units within the IPO solution that will be used for local PSTN access.

				Line Group ID	11
	User Rights	User Rights	User	Name	RS140
			Short Codes	-	Apply User Rights value
				Short Code table (Code, Telephone Number, Feature, Line Group ID)	*Please refer to next section*
			User Rights Membership	Member of this User Rights	All RS140 users
	Short Code	Short Code	-	Code	002XXXXXXXX[29]
				Feature	Dial
				Telephone Number	02N
				Line Group ID	54: RS140
		Short Code	-	Code	000N;
				Feature	Dial
				Telephone Number	00N
				Line Group ID	54: RS140
Note: Before configuring ARS tables on secondary IPO it is necessary to save ARS tables from primary IPO as a templates. This approach is necessary if we are using User Rights (described in next section) as it's not possible to modify ARS number.					
Primary IPO	ARS	1. Select first ARS table created in previous steps and click **Export as Template (Binary)** in top-right window menu. 2. Repeat this action for all other ARS tables created on primary IPO.			
Secondary IPO (if used)	ARS	1. Chose **New from Template (Binary)** and select from the list saved ARS table[30]. 2. Double-click on the Short Code entry within added ARS table and modify Line Group ID with the equivalent number configured on secondary IPO. 3. Repeat the steps above for each ARS table copied from primary IPO.			
Expansion Gateway	Short Code	Short Code	-	Code	9N
				Feature	Dial
				Telephone Number	NS225374380[31]
				Line Group ID	3

[29] It is not possible to add one global entry for immediate national numbers, so such configuration should be repeated for each national numbering pattern 00ZABPQMCDU, where Z is a digit from range 1-9.

[30] It is important to add all ARS tables for local PSTN access first, otherwise it will be required to manually select Alternate Route table later.

[31] Sxxxxxxxx means that provided number is used for CLI in outgoing calls via local PSTN line

Dial Plan – Incoming Call Route configuration - Incoming call to phone user[32]					
-	Incoming Call Route	Incoming Call Route 10	Standard	Line Group ID	10
				Incoming Number	+33296084361
			Destinations	Destination -> Default Value	4701001 Extn4701001
		Incoming Call Route 11	Standard	Line Group ID	11
				Incoming Number	+33296084361
			Destinations	Destination -> Default Value	4701001 Extn4701001
		Incoming Call Route 3[33]	Standard	Line Group ID	3
				Incoming Number	225374381[34]
			Destinations	Destination -> Default Value	4701001 Extn4701001[35]
Dial Plan – Incoming Call Route configuration - Incoming call to destination other than phone user (i.e. voicemail, hunt group)					
Primary IPO	Line	SIP Line 10	Call Details	Incoming Group	10
				Outgoing Group	10
				Max Sessions	Default=10 Range 1 - 250
				Local URI -> Display	Auto
				Local URI -> Content	Auto
				Local URI -> Fleld meaning -> Forwarding/Outgoing calls	Caller
				Local URI -> Fleld meaning -> Forwarding/Twinning	Original Caller
				Local URI -> Fleld meaning -> Forwarding/Incoming calls	Called
				Contact-> Display	Auto
				Contact-> Content	Auto
				Contact -> Fleld meaning -> Outgoing calls	Caller

[32] Each user has to have DID number assigned. To route incoming BTIP calls it is required to have SIP URI tab on primary and backup SIP trunk, configuration of which is described in section: SIP trunks configuration.

[33] Dedicated for local PSTN access (optional)

[34] This field can be used to match the called public number with private one.

[35] Binds public DID with the private extension.

				Contact -> Fleld meaning -> Forwarding/Twinning	Original Caller
				Contact -> Fleld meaning -> Incoming calls	Called
		SIP Line 11	Call Details	Incoming Group	11
				Outgoing Group	11
				Max Sessions	Default=10 Range 1 - 250
				Local URI -> Display	Auto
				Local URI -> Content	Auto
				Local URI -> Fleld meaning -> Forwarding/Outgoing calls	Caller
				Local URI -> Fleld meaning -> Forwarding/Twinning	Original Caller
				Local URI -> Fleld meaning -> Forwarding/Incoming calls	Called
				Contact-> Display	Auto
				Contact-> Content	Auto
				Contact -> Fleld meaning -> Outgoing calls	Caller
				Contact -> Fleld meaning -> Forwarding/Twinning	Original Caller
				Contact -> Fleld meaning -> Incoming calls	Called
-	Incoming Call Route	Incoming Call Route 10	Standard	Line Group ID	10
				Incoming Number	+33296084362
			Destinations	Destination -> Default Value	Voicemail / Hunt group / etc.
		Incoming Call Route 11	Standard	Line Group ID	11
				Incoming Number	+33296084362
			Destinations	Destination -> Default Value	Voicemail / Hunt group / etc.
Dial Plan configuration for Emergency calls					
Dial Plan configuration for Emergency calls – Short Code: Dial Emergency[36]					
Primary IPO	Short Code	Short Code	-	Code	112
				Feature	Dial Emergency

[36] If the system uses prefixes for external dialing, the dialing of emergency numbers with and without the prefix should be allowed.

				Telephone Number	112
				Line Group ID	Blank
	ARS	ARS	ARS	Route Name	HQ313-Emergency
				Alternate Route	PSTN_for_HQ313
			Add…	Code	N
				Feature	Dial
				Telephone Number	N
				Line Group ID	20[37]
			Add…	Code	N
				Feature	Dial
				Telephone Number	N
				Line Group ID	21[38]
	Location	Location	Location	Emergency ARS	HQ313-Emergency
	Line	SIP Line 10	Call Details	Incoming Group	0
				Outgoing Group	20[39]
				Max session	Default=10 Range 1 - 250
				Local URI -> Display	Example: +33296083900
				Local URI -> Content	Example: +33296083900
				Contact -> Fleld meaning -> Outgoing Call	Explicit
				Local URI -> Fleld meaning -> Forwarding/Twinning	Original Caller
				Local URI -> Fleld meaning -> Forwarding/Incoming calls	Called
				Contact-> Display	Example: +33296083900
				Contact-> Content	Example: +33296083900
				Contact -> Fleld meaning -> Outgoing Call	Explicit

[37] This value must be different than the one used for standard calls.

[38] This value must be different than the one used for standard calls.

[39] This value must equal the one configured under emergency ARS on first position!

				Contact -> Fleld meaning -> Forwarding/Twinning	Original Caller
				Contact -> Fleld meaning -> Incoming calls	Called
		SIP Line 11	Call Details	Incoming Group	0
				Outgoing Group	21[40]
				Max session	Default=10 Range 1 - 250
				Local URI -> Display	Example: +33296083900
				Local URI -> Content	Example: +33296083900
				Contact -> Fleld meaning -> Outgoing Call	Explicit
				Local URI -> Fleld meaning -> Forwarding/Twinning	Original Caller
				Local URI -> Fleld meaning -> Forwarding/Incoming calls	Called
				Contact-> Display	Example: +33296083900
				Contact-> Content	Example: +33296083900
				Contact -> Fleld meaning -> Outgoing Call	Explicit
				Contact -> Fleld meaning -> Forwarding/Twinning	Original Caller
				Contact -> Fleld meaning -> Incoming calls	Called
Secondary IPO (if used)	Short Code	Short Code	-	Code	112
				Feature	Dial Emergency
				Telephone Number	112
				Line Group ID	Blank
	ARS	ARS	ARS	Route Name	HQ313-Emergency
				Alternate Route	PSTN_for_HQ313
			Add…	Code	N
				Feature	Dial
				Telephone Number	N

[40] This value must equal the one configured under emergency ARS on second position!

				Line Group ID	120[41]
			Add…	Code	N
				Feature	Dial
				Telephone Number	N
				Line Group ID	121[42]
	Location	Location	Location	Emergency ARS	HQ313-Emergency
	Line	SIP Line 110	Call Details	Incoming Group	0
				Outgoing Group	120[43]
				Max session	Default=10 Range 1 - 250
				Local URI -> Display	Example: +33296083900
				Local URI -> Content	Example: +33296083900
				Contact -> Fleld meaning -> Outgoing Call	Explicit
				Local URI -> Fleld meaning -> Forwarding/Twinning	Original Caller
				Local URI -> Fleld meaning -> Forwarding/Incoming calls	Called
				Contact-> Display	Example: +33296083900
				Contact-> Content	Example: +33296083900
				Contact -> Fleld meaning -> Outgoing Call	Explicit
				Contact -> Fleld meaning -> Forwarding/Twinning	Original Caller
				Contact -> Fleld meaning -> Incoming calls	Called
		SIP Line 111	Call Details	Incoming Group	0
				Outgoing Group	121[44]
				Max Session	Default=10 Range 1 - 250

[41] This value must be different than the one used for standard calls.

[42] This value must be different than the one used for standard calls.

[43] This value must equal the one configured under emergency ARS on first position!

[44] This value must equal the one configured under emergency ARS on second position!

				Local URI -> Display	Example: +33296083900
				Local URI -> Content	Example: +33296083900
				Contact -> Fleld meaning -> Outgoing Call	Explicit
				Local URI -> Fleld meaning -> Forwarding/Twinning	Original Caller
				Local URI -> Fleld meaning -> Forwarding/Incoming calls	Called
				Contact-> Display	Example: +33296083900
				Contact-> Content	Example: +33296083900
				Contact -> Fleld meaning -> Outgoing Call	Explicit
				Contact -> Fleld meaning -> Forwarding/Twinning	Original Caller
				Contact -> Fleld meaning -> Incoming calls	Called
User / Extension creation – manual for IP endpoints[45]					
Primary IPO	User	User	User	Name	Extn3130001
				Password	password[46]
				Audio Conference PIN	PIN
				Extension	3130001
				Profile	Basic User / Power User[47]
			Telephony -> Supervisor Settings	Login Code	login code[48]
	Extension	H.323 / SIP Extension	Manager will automatically prompt for new VoIP extension creation when saving User part and will be filled with all necessary information.		

[45] Below values are examples and should be treated only as a common guideline for new user creation

[46] Password provided here will be used only for user login to applications like One-X Portal or One-X Mobile.

[47] Power user allows to use additional features like Softphone or Telecommuter mode. Separate license is required.

[48] Login code provided here will be used for phone's registration. Not obligatory.

		-	Extn	Phone Password	Password [49]
User / Extension creation - Public numbers assignment: NDI number declaration for non-DID users					
Primary IPO	User	User	SIP	SIP Name	Example: +33296084360
				SIP Display Name (Alias)	Example: +33296084360
				Contact	Example: +33296084360
User / Extension creation - Public numbers assignment: NDI number declaration for DID users[50]					
Primary IPO	User	User	SIP	SIP Name	Example: +33296084361
				SIP Display Name (Alias)	Example: +33296084361
				Contact	Example: +33296084361
User / Extension creation - The "NoUser" configuration					
Primary IPO	User	NoUser	Source Numbers	Source Number	MEDIA_DISABLE_RFC2833_ON_IPO[51]
Secondary IPO (if used)	User	NoUser	Source Numbers	Source Number	MEDIA_DISABLE_RFC2833_ON_IPO[52]
Expansion Gateway (if used)	User	NoUser	Source Numbers	Source Number	MEDIA_DISABLE_RFC2833_ON_IPO[53]

[49] This code will be used by H.323 phone users to login

[50] Each user has to have DID number assigned, so configuration should be repeated for each user.

[51] Configuration of NUSN is mandatory to have direct media for H.323 and DECT users registered to local gateways

[52] Configuration of NUSN is mandatory to have direct media for H.323 and DECT users registered to local gateways

[53] Configuration of NUSN is mandatory to have direct media for H.323 and DECT users registered to local gateways

6 IP Office + ASBCE SIP trunking configuration over BVPN checklist

The aim of this chapter is to provide steps to configure an Avaya Session Border Controller for Enterprise for interworking between the IP Office and BTIP/Business Talk service.
This guide shows only the settings to be checked or changed. The other settings can remain at their default values.

Device Management -> Licensing	
External WebLM Server URL	https://<SMGR_server_IP>:52233/WebLM/LicenseServer or https://<SMGR_server_domain_name>:52233/WebLM/LicenseServer e.g. https://6.5.27.232:52233/WebLM/LicenseServer or https://smgr80.warsaw.lab:52233/WebLM/LicenseServer
Device Management -> Devices -> Add	
Host Name	e.g. asbceipo
Management IP	e.g. 6.3.12.91
Device Management -> Devices -> Install	
Device Configuration Appliance Name	This name will be referenced in another configuration e.g. asbce
DNS Configuration Primary	e.g. 6.3.14.10
Network Configuration Name	Interface name toward IP Office e.g. Int-ASBCE-IPO
Network Configuration Default Gateway	e.g. 6.5.53.254
Network Configuration Subnet Mask or Prefix Length	e.g. 255.255.255.0
Network Configuration Interface	e.g. A2 Note: Interface must be enabled on SBCE virtual machine on ESXi host after installation is complete.
IP Address 1#	IP address of the internal SBCE interface e.g. 6.5.52.62
Network & Flows -> Network Management - > Networks -> Add	
Name	Interface name toward Orange SBC e.g. Ext-SBCE-BTIP
Default Gateway	e.g. 172.22.235.30
Network Prefix or Subnet Mask	e.g. 255.255.255.240
Interface	e.g. B1 Note: Interface must be enabled on SBCE virtual machine on ESXi host after configuration is complete.

IP Address	IP address of the external SBCE interface e.g. 172.22.235.19 Note: Reboot of the SBCE is required after configuration of the IP addresses.
Gateway Override	e.g. 172.22.235.30
Network & Flows -> Network Management - > Interfaces	
Interface name A2	Enabled Note: Previously configured interface must be enabled
Interface name B1	Enabled Note: Previously configured interface must be enabled
Network & Flows -> Signaling Interface -> Add	
Name	Create a signaling interface for the internal side of the SBCE e.g. Sign_Int_SBCE-IPO
IP Address	Select ASBCE internal interface and associated IP address defined in previous step. Int_ASBCE-IPO (A2, VLAN 0) 6.5.53.62
UDP port	This is the port on which SBCE will listen to SIP messages from IP Office. 5060 Note: UDP protocol is used for communication between ASBCE & IP Office.
Network & Flows -> Signaling Interface -> Add	
Name	Create a signaling interface for the external side of the SBCE e.g. Sign_Ext_SBCE-BTIP
IP Address	Select ASBCE external interface and associated IP address defined in previous step. Ext_SBCE-BTIP (B1, VLAN 0) 172.22.235.19
UDP port	This is the port on which SBCE will listen to SIP messages from Orange SBC. 5060 Note: UDP protocol is used for communication between ASBCE & Orange SBC.
Network & Flows -> Advanced Options -> Port Ranges	
Signaling Port Range	Default range: 12000-21000
Config Proxy Internal Signaling Port Range	Default range: 22000 – 31000
Listen Port Range	Default range: 9000 – 9999
HTTP Port Range	Default range: 40001 – 50000
Network & Flows -> Media Interface -> Add	

Name	Create a media interface for the internal side of the SBCE e.g. Media_Int_SBCE-IPO
IP Address	Select ASBCE internal interface and corresponding ip address configured in previous step. Int_ASBCE-IPO (A2, VLAN 0) 6.5.53.62
Port Range	Default range: 35000 – 40000
Network & Flows -> Media Interface -> Add	
Name	Create a media interface for the external side of the SBCE e.g. Media_Ext_SBCE-BTIP
IP Address	Selec ASBCE external interface and corresponding ip address configured in previous step. Ext_SBCE-BTIP (B1, VLAN 0) 172.22.235.19
Port Range	Default range: 35000 – 40000
Configuration Profiles -> Server Interworking -> Interworking Profiles -> Add	
Profile Name	e.g. SBCE-IPO
General tab Leave default parameters and ensure following parameters are selected:	
Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	Unchecked
3xx Handling	Unchecked
Delayed SDP Handling	Unchecked
Re-Invite Handling	Unchecked
Prack Handling	Unchecked
Allow 18X SDP	Unchecked
T.38 Support	Checked - only to enable T.38 capabilities on the SBCE
URI Scheme	SIP
Via Header Format	RFC3261
SIP Timers tab Leave default parameters (blank fields).	
Privacy Leave default parameters (blank fields).	
Interworking Profile Advanced parameters:	
Record Routes	Both Sides

Include End Point IP for Context Lookup	Unchecked
Extensions	Avaya
Diversion Manipulation	Unchecked
Has Remote SBC	Checked
Route Response on Via Port	Unchecked
Relay INVITE Replace for SIPREC	Unchecked
MOBX Re-INVITE Handling	Unchecked
DTMF	
DTMF Support	None Note: Avaya sip phones send DMFs over RTP according to RFC4733.
Configuration Profiles -> Server Interworking -> Interworking Profiles -> Add	
Profile Name	e.g. SBCE-BTIP
General Leave default parameters and ensure following parameters are selected:	
Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	Unchecked
3xx Handling	Unchecked
Delayed SDP Handling	Unchecked
Re-Invite Handling	Unchecked
Prack Handling	Unchecked
Allow 18X SDP	Unchecked
T.38 Support	Checked - only to enable T.38 capabilities on the SBCE
URI Scheme	SIP
Via Header Format	RFC3261
SIP Timers Leave default parameters (blank fields).	
Privacy Leave default parameters (blank fields).	
Interworking Profile Advanced parameters	
Record Routes	Both Sides
Include End Point IP for Context Lookup	Unchecked
Extensions	None
Diversion Manipulation	Unchecked
Has Remote SBC	Checked
Route Response on Via Port	Unchecked
Relay INVITE Replace for SIPREC	Unchecked

MOBX Re-INVITE Handling	Unchecked
DTMF	
DTMF Support	None Note: Avaya sip phones send DMFs over RTP according to RFC4733.
Services -> SIP Servers -> Server profiles -> Add	
Profile Name	Define profile for far away server: Avaya IP Office. Prof_SBCE-IPO
General	
Server Type	Call Server
SIP Domain	Leave empty
DNS Query Type	NONE/A
TLS Client Profile	none
IP Address / FQDN	Add primary and backup IPO if exists. e.g. 6.3.85.1 e.g. 6.3.85.2
Port	This is the port on which IP Office will listen to SIP messages from Avaya SBCE. 5060
Transport	Protocol used for SIP signaling between IP Office and the Avaya SBCE. UDP
Authentication Leave all fields blank.	
Heartbeat Configure Heartbeat to send Options to monitor status of a trunk toward IPO server (Primary and if exists) defined in previous step.	
Enable Heartbeat	Checked
Method	OPTIONS
Frequency	90
From URI	e.g. ping@6.3.85.1
To URI	e.g. ping@warsaw.lab
Registration Leave all fields blank.	
Ping Leave all fields blank.	
Advanced Leave default fields except following:	
Enable DoS Protection	Unchecked
Enable Grooming	With Grooming enabled the system can reuse the same connections for the same subscriber or port. Checked
Interworking Profile	Select the Interworking Profile for IP Office defined previously. SBCE-IPO
Signaling Manipulation Script	None

Securable	Unchecked
Enable FGDN	Unchecked
Tolerant	Unchecked
URI Group	None
Services -> SIP Servers -> Server profiles -> Add	
Profile Name	Define profile for far away server: Orange SBC. Prof_SBCE-BTIP
Server Type	Trunk Server
SIP Domain	Leave empty
DNS Query Type	NONE/A
TLS Client Profile	none
IP Address / FQDN	Add all Orange SBC servers (primary and backup if exists). e.g. 172.22.246.33 e.g. 172.22.246.73
Port	This is the port on which Orange SBC will listen to SIP messages from Avaya SBCE. 5060
Transport	Protocol used for SIP signaling between Orange BTIP SIP trunk service (i.e. Orange SBC primary and backup) UDP
Authentication Leave all fields blank.	
Heartbeat Configure Heartbeat to send Options to monitor status of a trunk toward the Orange SBC (Primary and Backup if exists) defined in previous step.	
Enable Heartbeat	Checked
Method	OPTIONS
Frequency	90
From URI	e.g. ping@172.22.235.19
To URI	e.g. ping@orange.sbc
Registration Leave all fields blank.	
Ping Leave all fields blank.	
Advanced	Leave default fields except following:
Enable DoS Protection	Unchecked
Enable Grooming	Unchecked
Interworking Profile	Select the Interworking Profile for Orange BTIP SIP trunk service defined previously. SBCE-BTIP
Signaling Manipulation Script	None
Securable	Unchecked
Enable FGDN	Unchecked

Tolerant	Unchecked
URI Group	None
Domain Policies -> Application Rules -> default -> Application Rule	
Audio	Regulate the number of audio sessions that are allowed for each trunk server, or a call server. In – checked Out - checked
Domain Policies -> Media Rules -> default-low-med -> Encryption	
Audio Encryption	
Preferred Formats	RTP
Interworking	Checked
Domain Policies -> Media Rules -> default-low-med -> Advanced	
Leave all checkboxes - Unchecked	
Domain Policies -> Media Rules -> default-low-med -> QoS -> Edit	
Media QoS Marking	
Enabled	Checked
DSCP	Selected
DSCP Audio	EF
DSCP Video	EF
Domain Policies -> Signaling Rules -> Add	
Rule Name	e.g. SigR_SBCE-IPO
Inbound Leave default parameters (Allow)	
Outbound Leave default parameters (Allow)	
Content-Type Policy	
Enable Content-Type Checks	Checked
Action	Allow
Multipart Action	Allow
Domain Policies -> Signaling Rules -> SigR_SBCE-IPO -> Signaling QoS	
Enabled	Checked
DSCP	Selected
Value	EF
Domain Policies -> Signaling Rules -> SigR_SBCE-IPO -> UCID	
Enabled	**Unchecked**
Domain Policies -> Signaling Rules -> SigR_SBCE-IPO -> Requests -> Add in Request Control	
Proprietary Request	Unchecked
Method Name	Options
In Dialog Action	Allow
Out of Dialog Action	Select Block with and type in first field 200 then in next field OK
Domain Policies -> Signaling Rules -> Add	

Rule Name	e.g. SigR_SBCE-BTIP
Inbound Leave default parameters (Allow).	
Outbound Leave default parameters (Allow).	
Content-Type Policy	
Enable Content-Type Checks	Checked
Action	Allow
Multipart Action	Allow
Domain Policies -> Signaling Rules -> SigR_SBCE -BTIP -> Signaling QoS	
Enabled	Checked
DSCP	Selected
Value	EF
Domain Policies -> Signaling Rules -> SigR_SBCE-BTIP -> UCID	
Enabled	**Unchecked**
Domain Policies -> Signaling Rules -> SigR_SBCE-BTIP -> Requests -> Add in Request Control	
Proprietary Request	Unchecked
Method Name	Options
In Dialog Action	Allow
Out of Dialog Action	Select Block with and type in first field 200 then in next field OK
Domain Policies -> End Point Policy Groups -> Add	
Group Name	e.g. EPPG_SBCE-IPO
Domain Policies -> End Point Policy Groups -> EPPG_SBCE-IPO -> Edit Policy Set	
Application Rule	default
Border rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	Select created previously: SigR_SBCE-IPO
Charging Rule	None
RTCP Monitoring Report Generation	Off
Domain Policies -> End Point Policy Groups -> Add	
Group Name	e.g. EPPG_SBCE-BTIP
Domain Policies -> End Point Policy Groups -> EPPG_SBCE-BTIP -> Edit Policy Set	
Application Rule	default
Border rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	select created previously: SigR_SBCE-BTIP
Charging Rule	None

RTCP Monitoring Report Generation	Off
Configuration Profiles -> Routing -> Add	
Profile name	e.g. Routing-to-IPO
Configuration Profiles -> Routing -> Routing-to-IPO	
Uri Group	*
Load Balancing	Priority
Transport	None
LDAP Server Profile	None
Matched Attribute Priority	Unchecked
Next Hop Priority	Checked
Ignore Route Header	Unchecked
ENUM	Unchecked
Time of Day	default
NAPTR	Unchecked
LDAP Routing	Unchecked
LDAP Base DN (Search)	None
Alternate Routing	Unchecked
Next Hop In-Dialog	Unchecked
ENUM Suffix	Leave this field blank.
Priority / Weight	1
SIP Server Profile	Select previously created: Prof_SBCE-IPO
Next Hop Address	Select IP address of the IPO Primary e.g. 6.3.85.1: 5060 (UDP)
Priority / Weight	2
SIP Server Profile	Select previously created: Prof_SBCE-IPO
Next Hop Address	Select IP address of the IPO Backup if exists e.g. 6.3.85.2: 5060 (UDP)
Configuration Profiles -> Routing -> Add	
Profile	e.g. Routing-to-BTIP
Configuration Profiles -> Routing -> Routing-to-BTIP	
Uri Group	*
Load Balancing	Priority
Transport	None
LDAP Server Profile	None
Matched Attribute Priority	Unchecked
Next Hop Priority	Checked
Ignore Route Header	Unchecked
ENUM	Unchecked
Time of Day	default

NAPTR	Unchecked
LDAP Routing	Unchecked
LDAP Base DN (Search)	None
Alternate Routing	Unchecked
Next Hop In-Dialog	Unchecked
ENUM Suffix	Leave this field blank.
Priority / Weight	1
SIP Server Profile	Select previously created: Prof_SBCE-BTIP
Next Hop Address	Select IP address of the Orange SBC Primary e.g. 172.22.246.33: 5060 (UDP)
Priority / Weight	2
SIP Server Profile	Select previously created: Prof_SBCE-BTIP
Next Hop Address	Select IP address of the Orange SBC Backup if exists e.g. 172.22.246.73: 5060 (UDP)
Configuration Profiles -> Topology Hiding -> Add	
Profile Name	This profile will be applied for the traffic from the Avaya SBCE to IP Office. e.g. **THP_SBCE-IPO**
Configuration Profiles -> Topology Hiding -> Topology Hiding Profiles -> THP_SBCE-IPO -> Add Header	
Header	Add all following headers: Via Request-Line SDP Record-Route Refer-To To From Referred-By For all headers set the following parameters:
Criteria	IP/Domain
Replace Action	Auto
Configuration Profiles -> Topology Hiding -> Add	
Profile Name	This profile will be applied for the traffic from the Avaya SBCE to Orange Business. e.g. THP_SBCE-BTIP
Configuration Profiles -> Topology Hiding -> Topology Hiding Profile -> THP_SBCE-BTIP -> Add Header	

Header	Add all following headers: Via Request-Line SDP Record-Route Refer-To To From Referred-By For all headers set the following parameters:
Criteria	IP/Domain
Replace Action	Auto
Network & Flows -> End Point Flows -> Server Flows -> Add	
Flow Name	Traffic from Orange SBC through Avaya SBCE toward IP Office: e.g. EPF_SBCE-IPO
SIP Server Profile	Select previously configured profile: Prof_SBCE-IPO
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Select the external signaling interface Sign_Ext_SBCE-BTIP
Signaling Interface	Select the internal signaling interface Sign_Int_SBCE-IPO
Media Interface	Select the internal media interface Media_Int_SBCE-IPO
Secondary Media Interface	None
End Point Policy Group	Select the endpoint policy group defined previously EPPG_SBCE-IPO
Routing Profile	Select the routing profile to direct traffic to BTIP SIP trunk Routing-to-BTIP
Topology Hiding Profile	Select the topology hiding profile defined for IP Office THP_SBCE-IPO
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	Unchecked
Network & Flows -> End Point Flows -> Server Flows -> Add	
Flow Name	Traffic from IP Office through Avaya SBCE toward Orange SBC: e.g. EPF_SBCE-BTIP
SIP Server Profile	Select previously configured profile: Prof_SBCE-BTIP
URI Group	*
Transport	*

Remote Subnet	*
Received Interface	Select the internal signaling interface Sign_Int_SBCE-IPO
Signaling Interface	Select the external signaling interface Sign_Ext_SBCE-BTIP
Media Interface	Select the external media interface Media_Ext_SBCE-BTIP
Secondary Media Interface	None
End Point Policy Group	Select the endpoint policy group defined previously EPPG_SBCE-BTIP
Routing Profile	Select the routing profile to direct traffic to IP Office Routing-to-IPO
Topology Hiding Profile	Select the topology hiding profile defined for BTIP SIP trunk THP_SBCE-BTIP
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	Unchecked

7 IP Office + ASBCE SIP trunking configuration over Internet checklist

Below table focuses on BTol/BTIPol SIP trunk configuration on ASBCE indicating the required update of configuration in addition to already implemented BT/BTIP configuration described in previous chapter.

TLS Management -> Certificates > Create CSR	
Country Name	e.g. FR
State/Province Name	e.g. Bretagne
Locality Name	e.g. Rennes
Organization Name	e.g. Orange
Organizational Unit	e.g. Orange Business
Common Name	FQDN assigned to ASBCE public ip address. CN domain name must be resolved on public DNS. Allowed characters in the CN are alphanumeric and hypen [-]. Special characters must not be used. e.g. external.domain.com
Algorithm	SHA256
Key Size (Modulus Length)	2048 bits
Key Usage Extension(s)	Checked Key encipherment Checked Non-Repudiation Checked Digital Signature
Extended Key Usage	Checked Server Authentication Checked Client Authentication
Subject Alt Name	FQDN for SAN is the same as for CN. e.g. DNS: external.domain.com
Passphrase Confirm Passphrase	Allowed characters are alphanumeric and special character but Avaya recommends not to use the dollar sign ($) in Key Passphrase Specify the passphrase to encrypt the private key.
Contact Name	e.g. Slawomir
Contact E-Mail	Email address
TLS Management -> Certificates -> Install	
Type	Select Certificate
Name	This field is optional. Can be left blank.
Overwrite Existing	Unchecked
Allow Weak Certificate/Key	Unchecked
Certificate File	Upload the Identity certificate file
Trust Chain File	Upload Trust Chain file. If the third-party CA provided separate Root CA and Intermediate certificates for ASBCE, you must combine both files into a single certificate file (trust chain file). To combine the files, add the contents of each certificate file one after the other, with the root certificate at the end. (e.g. IntermediateAndRootCAchain.crt)

Key	Ensure that the Common Name used during generation of CSR matches with the file name of the identity certificate being installed. Select Use Existing Key
Key File	Select from a drop-down list existing key file.
	TLS Management -> Certificates -> Install
Type	Select CA Certificate
Name	This field is optional. Can be left blank.
Overwrite Existing	Unchecked
Allow Weak Certificate/Key	Checked
Certificate File	Upload the public CA root & intermediate certificates file (trust chain file) of the remote entity (Orange A-SBC). e.g. OrangeIntermediateAndRootCAchain.pem
	TLS Management -> Server Profile -> Add
Profile Name	e.g. ThirdPartyServer
Certificate	Select installed ASBCE Identity certificate.
SNI Options	None
Peer Verification	Required
Peer Certificate Authorities	Select public CA root & intermediate certificates file (trust chain file) of the remote entity (Orange A-SBC). e.g. OrangeIntermediateAndRootCAchain.pem
Verification Depth	Depends of the number of bundled certificates. In case the third-party CA provided separate Root CA and Intermediate certificates for the Orange A-SBC that were bundled into one file the value will be set to number 2.
Renegotiation Time	0
Renegotiation Byte Count	0
Version	For encrypted BTIP/BTalk SIP Trunk architecture we need to configure TLS v1.3 or TLS v1.2. Check TLS 1.3 or TLS 1.2
Ciphers	Select: Default The cipher suite recommended by Avaya.
	TLS Management -> Client Profile -> Add
Profile Name	e.g. ThirdPartyClient
Certificate	Select installed ASBCE Identity certificate.
SNI Options	Unchecked Enabled
Peer Certificate Authorities	Select public CA root & intermediate certificates file (trust chain file) of the remote entity (Orange A-SBC). e.g. OrangeIntermediateAndRootCAchain.pem
Verification Depth	Depends of the number of bundled certificates. In case the third-party CA provided separate Root CA and Intermediate certificates for the Orange A-SBC that were bundled into one file the value will be set to number 2.
Extended Hostname Verification	Unchecked
Renegotiation Time	0

Renegotiation Byte Count	0
Version	For encrypted BTIP/BTalk SIP Trunk architecture we need to configure TLS v1.3 or TLS v1.2. Check TLS 1.3 or TLS 1.2
Ciphers	Select: Default
Network & Flows -> Network Management -> Networks → Ext-SBCE-BTIP -> Edit	
Name	Interface name toward Orange A-SBC e.g. Ext-SBCE-BTIP
Default Gateway	e.g. 195.205.163.25
Network Prefix or Subnet Mask	Network prefix or subnet mask e.g.255.255.255.248
Interface	B1
IP Address	Public Ip address of the external ASBCE interface (e.g. 195.205.163.30)
Public IP	Leave blank
Gateway Override	Leave blank
Network & Flows -> Signaling Interface -> Sign_Ext_SBCE_BTIP -> Edit	
Name	Signaling interface of the external side of the ASBCE. e.g. Sign_Ext_SBCE-BTIP
Ip Address	ASBCE external interface and associated public ip address defined in previous step. Ext_SBCE-BTIP (B1, VLAN 0) Public IP address e.g. 195.205.163.30
TLS port	This is the port on which ASBCE will listen to SIP messages from Orange A-SBC. 5061 Remark: TLS protocol is used for communication between ASBCE & Orange A-SBC.
TLS Profile	Select: ThirdPartyServer
Services -> SIP Servers -> Prof_SBCE-BTIP-> Edit	
Profile Name	Edit/add profile for the far end server: Orange A-SBC. Prof_SBCE-BTIP
Server Type	Trunk Server
SIP Domain	Leave blank
DNS Query Type	DNS type Service Record (SRV) allows to query DNS server to receive hostname, priority, port of the target servers. Alternatively, you can configure ip address or DNS Query Type A. SRV NONE/A BTIPoI supports type SRV & type A for DNS resolution and do not support direct public IP connections. BToI supports both public IP and type A for DNS resolution and do not provide any type SRV record connections.
TLS Client Profile	Select ThirdPartyClient

FQDN IP Address / FQDN	FQDN of the Orange A-SBC if DNS Query Type SRV was configured e.g. BTIPOI.iptel.one.equant.net. IP Address or FQDN of the Orange A-SBC if DNS Query Type None/A was configured.
Port	This is the port on which Orange A-SBC will listen to SIP messages from Avaya SBCE. This value will be received from DNS server in SRV response. If DNS query type A was configured, then insert port 5061. Leave blank if DNS Query Type SRV was configured. 5061 if DNS Query Type None/A was configured.
Transport	Protocol used for SIP signaling between ASBCE and Orange A-SBC. It will also result in the ASBCE will add by default SRV type query prefix "_sips._tcp." while querying DNS if DNS Query Type SRV was configured. TLS
Configuration Profiles -> Routing -> Routing-to-BTIP-> Edit	
Uri Group	*
Load Balancing	DNS/SRV if DNS Query Type SRV was configured in previous step. Priority if DNS Query Type None/A was configured in previous step.
Transport	None
Next Hop In-Dialog	Unchecked
Time of Day	default
Next Hop Priority	Unchecked if Load Balancing DNS/SRV was configured. Checked if Load Balancing Priority was configured.
Ignore Route Header	Unchecked
ENUM	Unchecked
NAPTR	Unchecked
ENUM Suffix	Leave this field blank.
Priority / Weight	N/A if Load Balancing DNS/SRV was configured. 1 if Load Balancing DNS/A was configured.
SIP Server Profile	Select previously created: Prof_SBCE-BTIP
Next Hop Address	Select FQDN of the Orange A-SBC if Load Balancing DNS/SRV was configured. e.g. FQDN (TLS) Select IP address or FQDN of the Orange SBC Primary if Load Balancing DNS/A was configured. e.g. 172.22.246.33: 5061 (TLS) or FQDN: 5061 (TLS)
Priority / Weight	2 if Load Balancing Priority was configured.
SIP Server Profile	Select previously created: Prof_SBCE-BTIP
Next Hop Address	Select IP address or FQDN of the Orange SBC Backup if exists. e.g. 172.22.246.33: 5061 (TLS) or FQDN: 5061 (TLS)
Domain Policies -> Media Rules -> Add	
Rule Name	Orange-med-enc
Audio Encryption & Video Encryption	

Preferred Format #1	AES_CM_128_HMAC_SHA1_80
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	Checked
MKI	Unchecked
Lifetime Leave blank to match any value	Leave blank
Interworking	Checked
Miscellaneous	
Capability Negotiation	Unchecked
Audio Codec & Video Codec	
Codec Prioritization	Unchecked
Transcode	Unchecked
Allow Preferred Codecs Only	Unchecked
Transrating	Unchecked
P-Time	20
Silencing	
Silencing Enabled	Unchecked
Binary Flow Control Protocol	
BFCP Enabled	Unchecked
Far End Camera Control	
FECC Enabled	Unchecked
ANAT	
ANAT Enabled	Unchecked
Local Preference	IP4
Use Remote Preference	Unchecked
Media Line Compliance	
Media Line Compliance Enabled	Unchecked
Media QoS Marking	
Enabled	Checked
DSCP	selected
DSCP Audio	EF
DSCP Video	EF
Domain Policies -> End Point Policy Groups -> EPPG_SBCE-BTIP -> Edit Policy Set	
Application Rule	default
Border rule	default
Media Rule	select created previously: Orange-med-enc
Security Rule	default-low

Signaling Rule	SigR_SBCE-BTIP
Network & Flows -> Advanced Options -> Port Ranges	
Signaling Port Range	Depending on customer context or need. ASBCE TLS/TCP/UDP source ports for the SIP signaling. Allocate e.g. range: 51001-55000
Config Proxy Internal Signaling Port Range	50001-51000
Listen Port Range	55001-55999
HTTP Port Range	40001-50000
Network & Flows -> Media Interface -> Media_Int_SBCE-IPO -> Edit	
Name	Edit/Add a media interface for the internal side of the ASBCE e.g. Media_Int_SBCE-IPO
IP Address	ASBCE internal interface and corresponding ip address: Int_SBCE-IPO (A2, VLAN 0) 6.5.53.62
Port Range	The Orange BTIPol/BTol SIP Trunk service specifies media ports that customers use on the internal SIP trunk. ASBCE UDP ports for the RTP media: 6000-38000 for BTIPol 6000-20000 for BTol
Network & Flows -> Media Interface -> Media_Ext_SBCE_BTIP -> Edit	
Name	Edit/Add media interface for the external side of the ASBCE e.g. Media_Ext_SBCE-BTIP
IP Address	ASBCE external interface and corresponding ip address: Ext_SBCE-BTIP (B1, VLAN 0) Public IP Address e.g.195.205.163.30
Port Range	The Orange BTIPol/BTol SIP Trunk service specifies media ports that customers use on the external SIP trunk. ASBCE UDP ports for the SRTP media: 6000-38000 for BTIPol 6000-20000 for BTol
Domain Policies -> Application Rules -> default	
Maximum Concurrent Session	Change the value to 2000
Maximum Sessions Per Endpoint	Change the value to 2000
Configuration Profiles -> Server Interworking -> SBCE-IPO -> Edit	
Profile Name	SBCE-IPO
General	
SIPS Required	No
Configuration Profiles -> Server Interworking -> SBCE-BTIP -> Edit	
Profile Name	SBCE-BTIP
General	
SIPS Required	No

Domain Policies -> Session Policies -> default -> Media	
Media Anchoring	Checked for media anchoring
Media Forking Profile	None
Converged Conferencing	Unchecked
Recording Server	Unchecked
Media Server	Unchecked
Network & Flows -> Session Flows	
Media must be anchored on ASBCE. Session Flows must be default. Remove any session flow if exists.	

8 ASBCE dynamic license allocation since version 10.2.1

Since version 10.2.1 of ASBCE, Avaya implemented license pool management. Licenses must be allocated on each ASBCE for features to allow calls over SIP trunk.

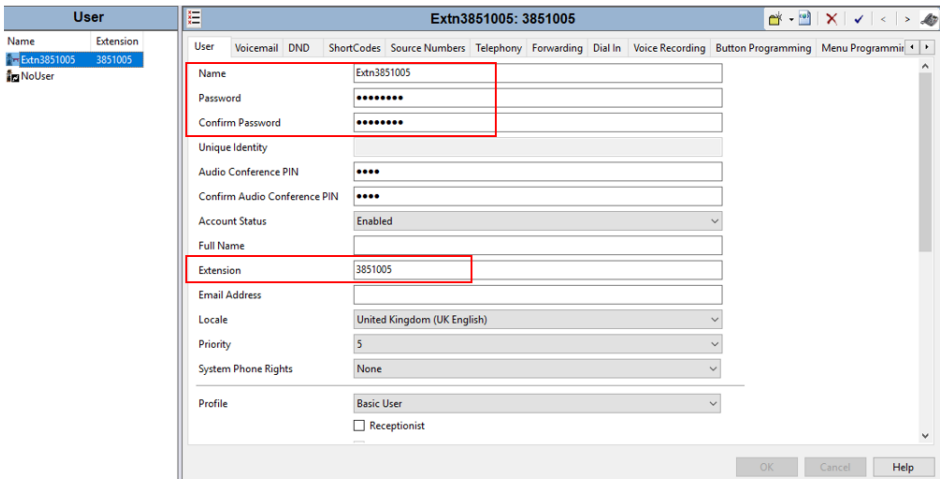
Device Management -> Devices -> select appropriate asbce -> Edit -> Next -> Next -> Dynamic License Settings		
Displayed "Available" value is acquired from WebLM and depends on the purchased licenses quantity available on WebLM	MIN License Allocation (must be allocated at least one if available quantity is higher than 0)	**MAX License Allocation** (can be allocated up to available quantity)
Standard Session Available: e.g. 60	1	**60**
Advanced Session Available: e.g. 30	1	**30**
Transcoding Session Available: e.g. 30	1	**30**
Premium Session Available: e.g. 6	1	**6**
Encryption Available: Yes	Checked	

9 Fax configuration with Avaya IP500v2 gateway

9.1 T.38 Fax

Under the GW configuration site select **User** and configure:

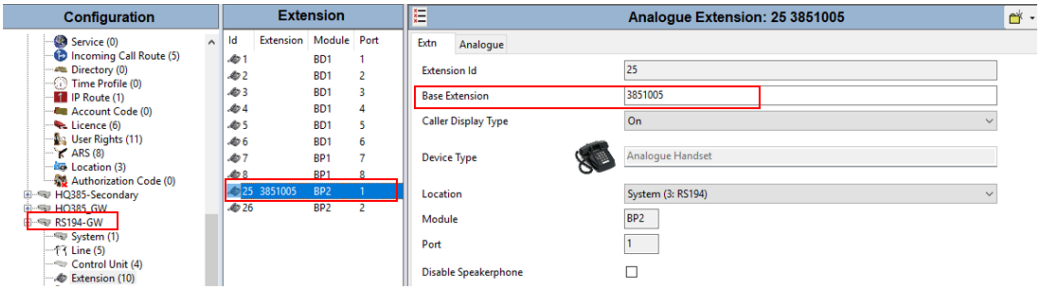
Tab	Parameter	Value	Description
User	Name	Extn3851005	Example value. Name of the user.
	Password	password	Password provided here will be used only for user login to applications like One-X Portal or One-X Mobile. Not obligatory.
	Extension	3851005	Example value. Corresponding extension



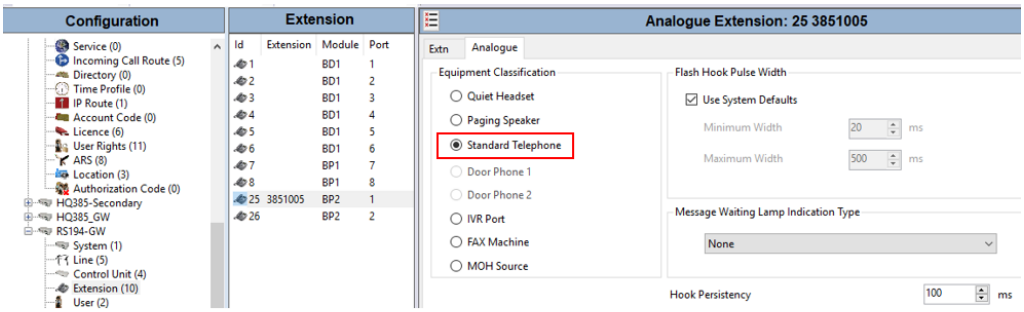
Fax user configuration

Then on the GW select **Extension** and configure analog port:

Tab	Parameter	Value	Description
Extn	Base Extension	3851005	Extension of the previously configured user
Analogue	Standard Telephone	selected	Standard Telephone must be selected. Only codecs capable of supporting fax will be used for that port.



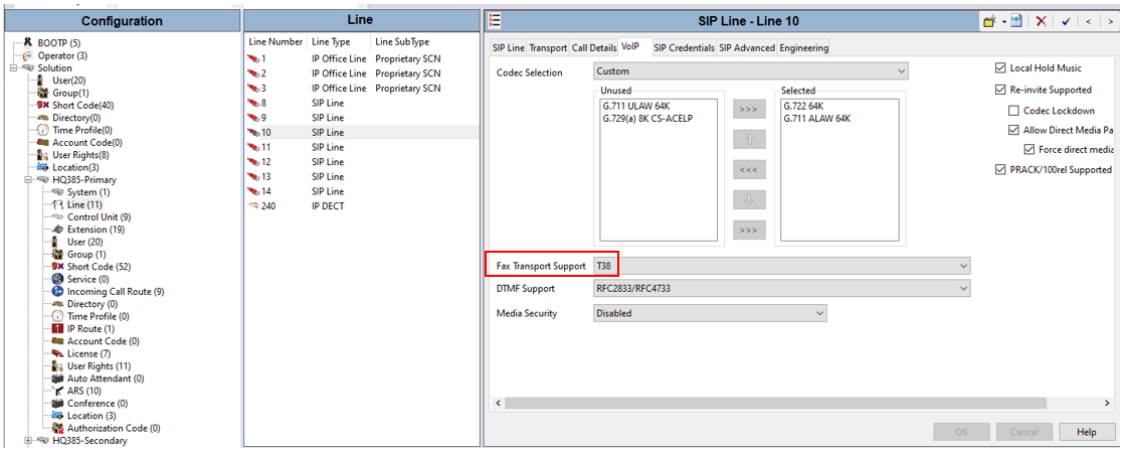
Fax Extension configuration



Fax Extension configuration

On the IPO server **SIP Line** go to VoIP tab and configure additional parameter:

Tab	Parameter	Value	Description
VoIP	Fax transport support	T.38	T38 is used for the sending and receiving of faxes



SIP line configuration – fax transport support

Repeat steps for each SIP lines on primary and secondary IPO servers.

On the IPO server **SIP Line** go to Engineering tab and add parameters:

Tab	Parameter	Value	Description
Engineering	Custom Strings	SLIC_PREFER_ACTIVE_SDP	When IP Office sends reInvite with SDP to switch to fax t.38 transmission, the SDP still contains unnecessary line (m): audio 0 RTP/AVP 8 18 0 101 but this line is moved down. Line (m): image 49154 udptl t38 is moved to the first place.
		SLIC_AUDIO_AFTER_T38	Special string activating the T38 transmission.
		SLIC_ALLOW_ONLY_ACTIVE_SDP_T38	Special string activating the T38 transmission.

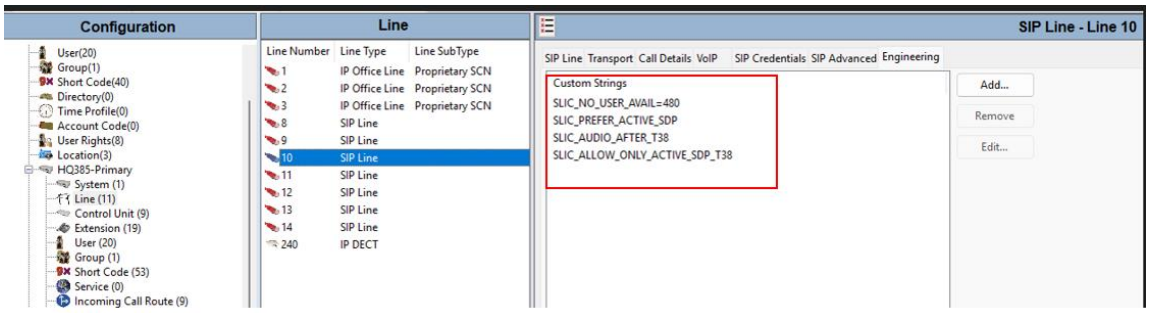
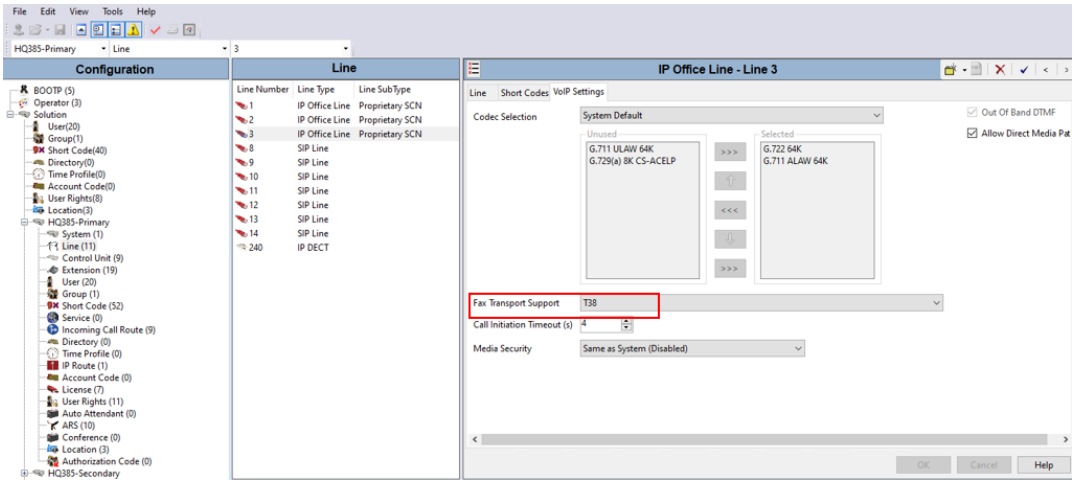


Figure 1: SIP line configuration – custom strings

Repeat steps for each SIP lines on primary and secondary IPO servers.

On the IPO server **SCN Line** to expansion gateway go to **VoIP Settings** tab and configure additional parameter:

Tab	Parameter	Value	Description
VoIP Settings	Fax transport support	T.38	T38 is used for the sending and receiving of faxes



IPO server SCN line configuration – fax transport support

Repeat steps for each SCN lines to expansion gateway on primary and secondary IPO servers.

On the GW system **SCN Line** to IPO server go to **VoIP Settings** tab and configure additional parameter:

Tab	Parameter	Value	Description
VoIP Settings	Fax transport support	T.38	T38 is used for the sending and receiving of faxes

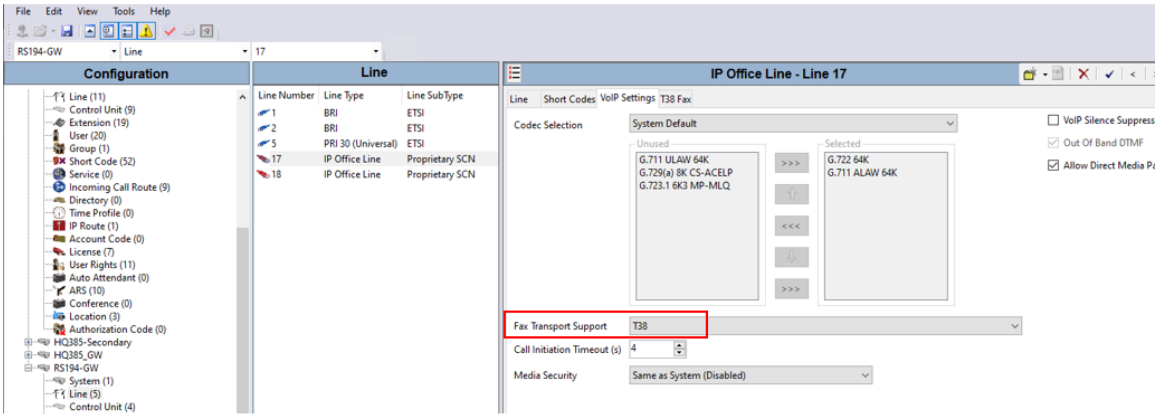


Figure 2: IPO GW SCN line configuration – fax transport support

Repeat steps for each SCN lines to IPO servers (primary and secondary IPO servers).

On the GW system **SCN Line** to IPO server go to **T38 Fax** tab and configure additional parameters:

Tab	Parameter	Value	Description
T38 Fax	T38 Fax Version	0	T38 is used for the sending and receiving of faxes
	Transport	UDPTL	
	Redundancy -> Low Speed	4	
	Redundancy -> High Speed	1	

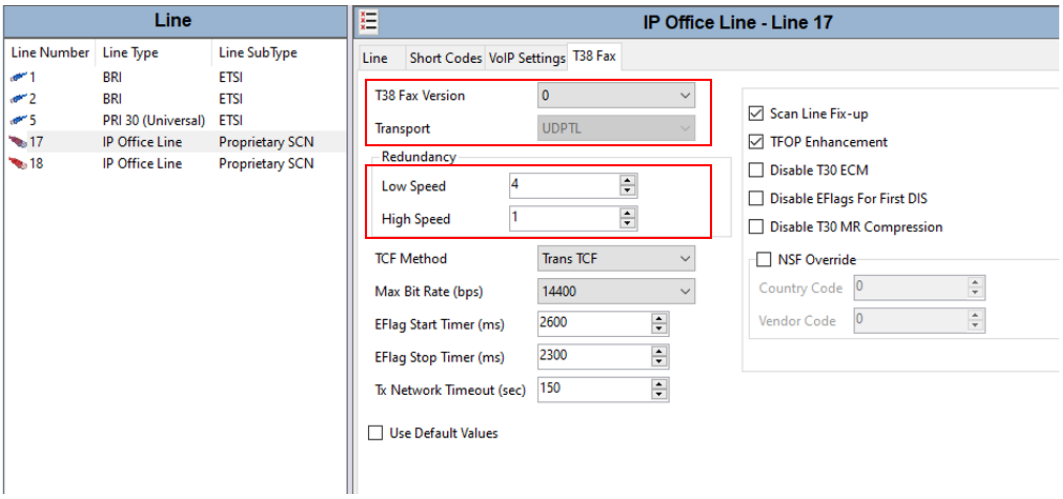


Figure 3: IPO GW SCN line configuration – T38 Fax

9.2 G.711 Inband Fax

For G.711 inband fax transmission, customers may implement any inband fax configuration, including, but not limited to, autonomous mode, passthrough mode, and voice mode. V.152 is explicitly excluded and is not supported.

Customers are solely responsible for configuring their own fax equipment. Orange does not recommend any specific G.711 inband fax configuration, as fax transmission performance may depend

on the behaviour of fax gateways and on any transcoding operations performed within the core network.

Consequently, Orange does not provide technical support for issues related to G.711 inband fax transmission.

10 Ecosystems and endpoints configuration

10.1 Avaya Communicator for Windows

Access type: application.

Avaya Communicator for Windows			
Communicator for windows	Server	Server address	Primary FQDN
		Server port	5060
		Transport type	TCP
		Domain	IPO's Domain Name
	Conference	Conference server address	Example 6.3.13.1

10.2 Avaya B179 Conference Station

Access type: B179 Conference Station's Administration web page.

Menu	Tab	Parameter
Codec configuration – G.722		
Settings	Media	Codec priorities: ▪ G722: 4 – High ▪ G711 Alaw: 3 ▪ G711 Ulaw: 0 – Disabled ▪ G729: 0 – Disabled Or if G711 Ulaw is in option: ▪ G722: 4 – High ▪ G711 Alaw: 0 – Disabled ▪ G711 Ulaw: 3 ▪ G729: 0 – Disabled
SIP settings		
Primary Account	Enable account	YES
	Account name	Extn3133102
	User	3133102
	Registrar	Primary IPO IP address
	Realm	*
	Autentication name	3133102
	Password	Password
Fallback Account	Enable account	YES
	Account name	Extn3133102
	User	3133102
	Registrar	Secondary IPO IP address or Local GW IP address
	Realm	*

	Autentication name	3133102
	Password	Password

10.3 Avaya DECT IP Base Station

Access type: DECT IP Base Station Administration web page.

Menu	Tab	Parameter	Value
LAN configuration			
LAN	DHCP	Mode	disabled
	IP	IP Address	IPBS static IP address
		Network Mask	255.255.255.0
		Default Gateway	default gateway's IP address
DECT configuration			
DECT	Master	Mode	Active * restart required
	Radio	Name	IPBS
		Password	password
		Master IP Address	127.0.0.1
		Authentication Code	1234[54]
	Air Sync	Sync Mode	Master * restart required
	System	System Name	DECT
		Password	password[55]
		Confirm password	password
		Subscriptions	With User AC
	Master	PBX	IPO
		Protocol	H.323/XMobile
	Trunks	Name	Trunk1 (default)
		Local Port	1720 (default)
		CS IP Address	primary IPO's IP address
		CS Port	1720 (default)
	SARI	SARI	license number[56]
PROVISIONING configuration			

[54] Authentication code has to match the one configured on primary IPO for DECT line under Authentication Code

[55] The same password has to be configured as in **Master** tab

[56] License number has to match the one configured on primary IPO for DECT line under SARI/PARK

Services	Provisioning	Current view	Primary
		Enable	Checked
		PBX IP Address	IP address Primary IPO
		User Name	IPDECTService[57]
		Password	Password [58] • reset required
DECT configuration for AIWS			
UNITE	Device Management	Unite IP Address	AIWS' IP address
HTTP Client configuration			
Services	HTTP Client	Password	Password[59]
Switch Resilience configuration			
Services	Provisioning	Current view	Redundant
		Enable	Checked
		PBX IP Address	IP address Backup IPO
		User Name	IPDECTService[60]
		Password	Password[61] • reset required
DECT	Master	PBX Resiliency	Checked
	Trunks	Status Inquiry period	30[62]
		Supervision timeout	120[63]
		Redundant Trunks -> Name	Trunk2 (default)
		Local Port	1720 (default)
		CS IP Address	backup IPO's IP address
		CS Port	1720 (default)

57 "User Name" must be the same as in settings on IPO Manager – go to Security Settings -> Service Users -> IPDECTService

58 " "Password" must be the same as in settings on IPO Manager – go to Security Settings -> Service Users -> IPDECTService

59 Password the same as for Provisioning

60 "User Name" must be the same as in settings on IPO Manager for backup server – go to Security Settings -> Service Users -> IPDECTService

61 "Password" must be the same as in settings on IPO Manager for backup server – go to Security Settings -> Service Users -> IPDECTService

62 Value for "Status Inquiry period" should be the same as in settings on IPO – go to IP DECT Line.

63 Value for "Supervision timeou"t should be the same as in settings on IPO – go to IP DECT Line.

10.4 Avaya One-X Portal

Access type: IP Office Manager application.

Menu	Submenu	Parameter	Value
Primary IPO	LAN1 -> VOIP	SIP Registrar FQDN	Primary FQDN
		SIP Domain Name	IPO's Domain Name
Secondary IPO	LAN1 -> VOIP	SIP Registrar FQDN	Secondary FQDN
		SIP Domain Name	IPO's Domain Name

Access type: One-X Portal Administration web page.

Menu	Submenu	Parameter	Value
Pimary One-x Portal	Configuration	IM/Presence Server -> XMPP Domain Name	IPO's Domain Name
		Resiliency -> Failover	Enebled
		Resiliency -> Failover Detection Time	3
		Resiliency -> Failback	Automatic
		HOST Domain Name -> Primary HOST Domain Name	Primary FQDN
		HOST Domain Name -> Secondary HOST Domain Name	Secondary FQDN
Secondary One-x Portal	Configuration	IM/Presence Server -> XMPP Domain Name	IPO's Domain Name
		Resiliency -> Failover	Enebled
		Resiliency -> Failover Detection Time	3
		Resiliency -> Failback	Automatic
		HOST Domain Name -> Primary HOST Domain Name	Primary FQDN
		HOST Domain Name -> Secondary HOST Domain Name	Secondary FQDN

10.5 Avaya One-X Mobile

Access type: One-X Mobile Preferred for Android application installed on mobile device.

Menu	Submenu	Parameter	Value
Settings	Server ID and user account	Server ID	IPO Domain Name (example: ipo.labobs.com)

		Username	Extn3130001
		Password	password[64]
	Voice Over IP	Voice Over IP	Checked

64 Password used to login.