



Business Talk & BTIP 3CX IPBX

version addressed in this guide: 20.x

Version of 27/06/2025

Table of contents

1	Goal of this document	3
2	Certified architectures.....	4
2.1	Introduction to architecture components and features.....	4
2.2	3CX Architecture over BVPN	5
2.3	3CX Centralized architecture over Internet	6
2.3.1	Prerequisites.....	6
2.3.2	Public IP assignement.....	7
2.3.3	Public DNS record	7
2.3.4	Firewall updates.....	7
2.3.5	Certificates	8
2.3.6	TLS v1.3 and v1.2 cipher suites	8
3	Parameters to be provided by customer to access service	10
3.1	3CX IPBX – BTIP/BTalk over BVPN	10
3.2	3CX IPBX – BTIP/BTalk over Internet	10
4	Certified software and hardware versions	11
4.1	3CX certified versions	11
4.1	3CX Supported IP Phones.....	11
5	3CX IPBX over BVPN configuration guidelines.....	12
5.1	SIP Trunks configuration for 3CX v20.....	12
5.1.1	Outbound Rules configuration.....	17
6	3CX IPBX over Internet configuration guidelines.....	19
6.1	SIP Trunks configuration for 3CX v20.....	19
6.1.1	Outbound Rules configuration.....	24
6.2	3CX IPBX configuration with your own Public Certificate Authority.....	25
6.5	Public Certificate Authority renewal	27
	Glossary.....	30

1 Goal of this document

The aim of this document is to list technical requirements to ensure the interoperability between 3CX IPBX with Business Talk IP, hereafter so-called “service”.

2 Certified architectures

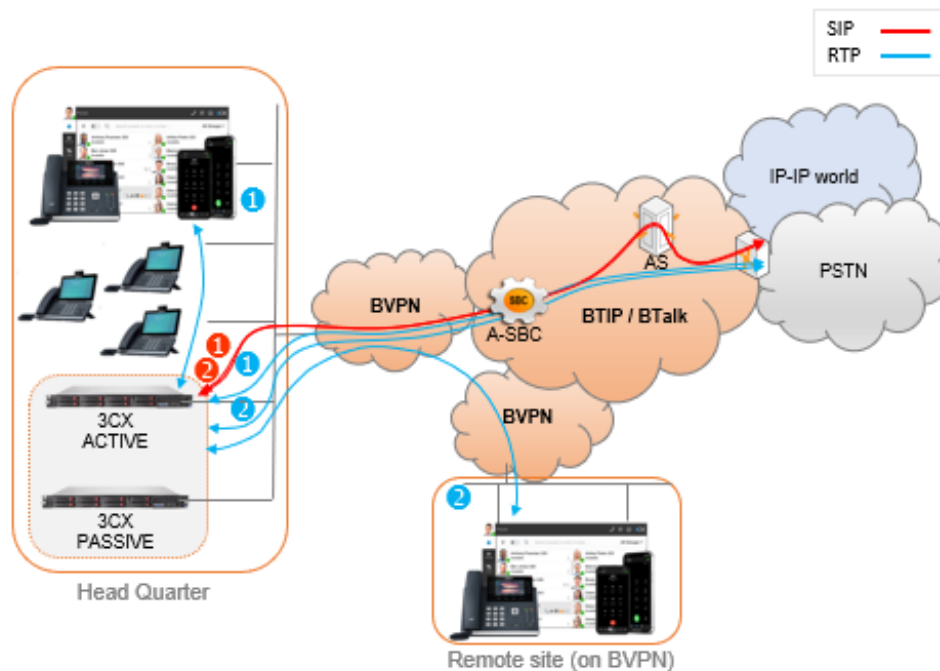
2.1 Introduction to architecture components and features

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...)

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

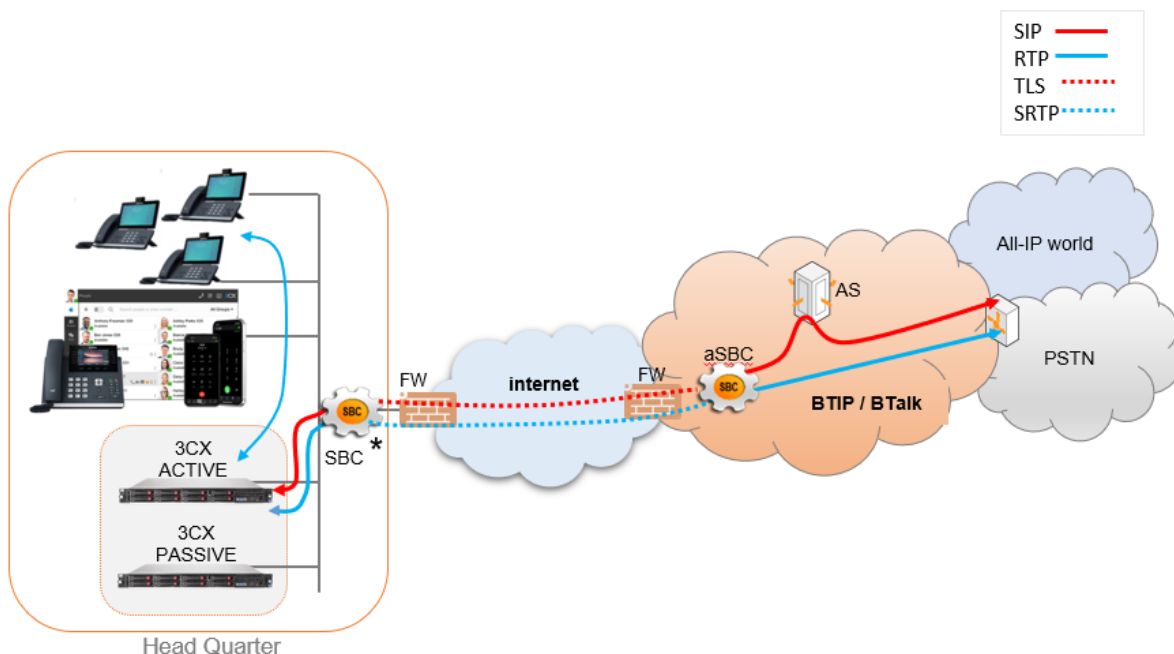
BTIP in French overseas departments are also supported. Dedicated aSBC pairs in Caribbean and Indian Ocean zones are deployed for local calls. For a trunking point of view, the mechanism is similar to “Business Talk French customers”, the IPBX must support international dial plans and route local calls to the dedicated local aSBC pair.

2.2 3CX Architecture over BVPN



- All SIP signaling flows are carried by the 3CX IPBX and routed on the main Orange BVPN access.
- Media flows between endpoints and the Business Talk/BTIP terminate on 3CX IPBX:
 - for the Head Quarter site, media flows are routed through the 3CX,
 - for Remote Sites media flows transit through the Head Quarter 3CX and use the BTIP/BTalk connection (= centralized architecture).

2.3 3CX Centralized architecture over Internet



- All SIP signaling flows are carried by the 3CX IPBX and routed on the main Internet access.
- Media flows between endpoints and the Business Talk/BTIP terminate on 3CX IPBX.
- 3CX IPBX supports natively TLS/SRTP encryption feature.
- In this architecture, both SIP signaling and RTP media flows between the 3CX IPBX and the Business Talk/BTIP infrastructure are anchored by the IPBX.

**a "customer SBC" is optional since encrypted call flows are natively managed by the 3CX IPBX*

2.3.1 Prerequisites

In order to establish the connection with public interface of SBC*/3CX, 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 TLS v1.2 cypher suites compliance
- SRTP encryption

2.3.2 Public IP assignment

The certified solution requires the use of a public IP address configured directly on the SBC or the 3CX IPBX and placed in the DMZ.

No NAT must be performed between the interface of the SBC or the 3CX IPBX carrying the public IP address and the BTIP infrastructure.

2.3.3 Public DNS record

Orange aSBC can be reached via a Fully Qualified Domain Name (FQDN) type SRV or type A deployed on a public DNS. Customer premise SBC*/3CX requires a record on public DNS that enables to reach it using FQDN via public internet. BTIPol can be reached using FQDN only, whereas BTol can be reached either via public IP address or FQDN.

- BTIPol (France) supports type SRV & type A for DNS resolution and do not support direct public IP connections.
- BTol (International) supports both public IP and type A for DNS resolution and do not provide any type SRV record connections.

2.3.4 Firewall updates

Firewalls in the way of traffic between SBC*/3CX and aSBC have to be updated in order to open required ports. BTol and BTIPol vary concerning the UDP port range.

The media UDP port ranges required by **Orange BTIPol SIP Trunk (France)** is **6000-38000** and for **Orange BTol SIP Trunk (International)** is **6000-20000**.

BTIPol/BTol port matrix				
Source device	Source ports	Destination device	Destination ports	Purpose
SBC*/3CX public @IP	Defined Signaling port range on SBC*/3CX: Network & Flows -> Advanced Options e.g. TCP 51001-55000 Depending on customer context or needs.	Orange aSBC public @IP	TCP 5061	TLS SIP signaling
Orange aSBC public @IP	TCP Any	SBC*/3CX public @IP	TCP 5061	
SBC*/3CX public @IP	BTIPol: UDP 6000-38000 BTol: UDP 6000-20000	Orange aSBC public @IP	BTIPol: UDP 6000-38000 BTol: UDP 6000-20000	SRTP media
Orange aSBC public @IP	BTIPol: UDP 6000-38000 BTol: UDP 6000-20000	SBC*/3CX public @IP	BTIPol: UDP 6000-38000 BTol: UDP 6000-20000	

2.3.5 Certificates

To ensure the security of traffic, public root & intermediate certificates need to be exchanged between the 3CX IPBX and the Orange BTIP/BTalk access SBC.

Customer IPBX or SBC requires an identity certificate signed by a root certificate from a public Certification Authority (including any intermediate certificate involved in the chain of trust).

3CX IPBX uses the Let's Encrypt Certification Authority by default to facilitate certificate generation and renewal. It is an automatic process. BTIP/Btalk aSBCs include the Let's Encrypt CA (Root = ISRG Root X2 and Intermediate = Let's Encrypt R3)

However, it is still possible to generate manually the private key and the Certificate Signing Request (CSR) file to be signed by a public Certification Authority. In a such case, the customer should send the Orange BTIP/Btalk team the public root and intermediate certificates from this same public certification authority, in PEM (X509 V3) format.

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 the 3CX IPBX.

Import the **Root and the Intermediate Orange CA** included in the DigiCert CA. 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**

More details are described in following chapters of 3CX secure configuration.

Note: that it is not possible to generate a CSR file directly on the 3CX IPBX. The customer must therefore generate the Certificate Signing Request file within a private key file (e.g. by using OpenSSL tool on Linux or Windows). Then use the CSR file to obtain signed Identity Certificate signed by a public Certification Authority before installing it onto the 3CX IPBX.

2.3.6 TLS v1.3 and v1.2 cipher suites

The following cipher suites are supported by Orange SBC for TLS 1.3 and TLS 1.2. 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)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)

These cipher suites use RSA for key exchange and the AES block cipher for encryption. Provide strong security for protecting SIP signaling and media traffic between endpoints. It's important to ensure that the 3CX system is kept up to date with the latest security patches and updates.

Warning: 3CX does not support a complete mutual authentication mechanism and therefore does not comply with the security requirements requested by Orange for BTIP over Internet. This could result in security flaws on customer side for which Orange cannot be held responsible.

3 Parameters to be provided by customer to access service

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

3.1 3CX IPBX – BTIP/BTalk over BVPN

Head Quarter (HQ) architecture	Level of Service	Customer IP addresses used by service	
		Nominal	Backup
3CX IPBX (1 Primary)	No Redundancy	Primary IP@	N/A
3CX IPBX (1 Primary + 1 Secondary)	Local redundancy Primary (Nominal) / Secondary (Backup) Primary and Secondary are on different servers)	Primary IP@	Secondary IP@

3.2 3CX IPBX – BTIP/BTalk over Internet

Head Quarter (HQ) architecture	Level of Service	Customer IP addresses used by service	
		Nominal	Backup
3CX IPBX	No redundancy	3CX public FQDN* DNS type A	N/A
3CX IPBX (1 Primary + 1 Secondary)	Local redundancy Primary (Nominal) / Secondary (Backup) Primary and Secondary are on different servers)	Primary IP@ or Public FQDN* type A	Secondary IP@ or Public FQDN* type A

*BTIPol can be reached using FQDN only, whereas BTol can be reached either via FQDN or public IP address.

4 Certified software and hardware versions

Orange supports the last 2 major IPBX versions 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.

Warning: As the Orange Business BTIP and BTalk trunking offers are still being validated, they do not yet appear on the 3CX portal for certified carriers. In the meantime, you should use the “generic carrier” in the settings below.

4.1 3CX certified versions

3CX IPBX			
Equipment	Equipment Version	validation status	IPBX Version
3CX PBX	R20.x	✓	Load 20.0 Update 5

4.1 3CX Supported IP Phones

Supported models can be found on the official 3CX website: [Which IP Phones work with 3CX](#)

5 3CX IPBX over BVPN configuration guidelines

The checklists below present all the configuration steps required for interoperability between the BTalk/BTIP service over BVPN and 3CX IPBX only.

Refer to the official 3CX documentation for the IPBX installation and other telephony settings.

5.1 SIP Trunks configuration for 3CX v20

For 3CX IPBX v20 the SIP trunk configuration parameters have been implemented in the template.

To implement .xml Orange provider template you can download it, right-click on the file below *Orange Business TalkBTIP.pv.xml*, select "copy" from the context menu, save the file locally to implement it later into 3CX.



Orange Business TalkBTIP.pv.xml

or you can create the .xml file which contains the following configuration inside:

```
<doc>
  <header>
    <name>Orange Business Talk/BTIP</name>
    <time>2024-11-27T07:23:48.4948629Z</time>
    <template>
      <!--Do not change this field-->GenericSIPTrunk.pv.xml</template>
    </template>
    <!--Do not change this field-->gateway-template</type>
  </header>
  <data>
    <device>
      <field name="Name">Orange Business Talk/BTIP</field>
      <type>provider</type>
      <manufacturer></manufacturer>
      <model>provider</model>
      <field name="RegistrarHost"></field>
      <field name="RegistrarPort">0</field>
      <field name="ProxyHost"></field>
      <field name="ProxyPort">0</field>
      <field name="IpInContactReg">1</field>
      <field name="TimeBetweenRegistration">180</field>
      <field name="SecondaryRegistrar"></field>
      <field name="IPRestriction">IPV4</field>
      <field name="TransportRestriction"></field>
      <field name="RequireAuthFor">1</field>
      <field name="IpInContactRegValue"></field>
      <field name="RegistrarInvite">0</field>
      <field name="IsSupportReinvite">0</field>
      <field name="IsSupportReplaces">0</field>
      <field name="DisableVideo">1</field>
      <field name="SRTPMode"></field>
      <field name="IsBindToMS">1</field>
      <codecs>
        <codec rfcname="G722" />
        <codec rfcname="PCMA" />
        <codec rfcname="G729" />
      </codecs>
      <field name="ParameterIn" custom="" parameter="FromUserPart">$CallerNum</field>
      <field name="ParameterIn" custom="" parameter="FromUserPart">$CallerName</field>
      <field name="ParameterIn" custom="" parameter="ToUserPart">$CalledNum</field>
      <field name="ParameterOut" custom="" parameter="RequestLineURIUser">$CalledNum</field>
    </device>
  </data>
</doc>
```

```

    <field name="ParameterOut" custom="" parameter="RequestLineURIHost">$GWHostPort</field>
    <field name="ParameterOut" custom="" parameter="ContactUser">$OriginatorCallerId</field>
    <field name="ParameterOut" custom="" parameter="ContactHost">$ContactUri</field>
    <field name="ParameterOut" custom="" parameter="ToDisplayName">$CalledName</field>
    <field name="ParameterOut" custom="" parameter="ToUserPart">$CalledNum</field>
    <field name="ParameterOut" custom="" parameter="ToHostPart">$GWHostPort</field>
    <field name="ParameterOut" custom=""
parameter="FromDisplayName">$OriginatorCallerId</field>
    <field name="ParameterOut" custom=""
parameter="FromUserPart">$OriginatorCallerId</field>
    <field name="ParameterOut" custom="" parameter="FromHostPart">$ContactUri</field>
    <field name="ParameterOut" custom=""
parameter="RemotePartyIDCallingPartyDisplayName">$OutboundCallerId</field>
    <field name="ParameterOut" custom=""
parameter="RemotePartyIDCallingPartyUserPart">$OutboundCallerId</field>
    <field name="ParameterOut" custom=""
parameter="RemotePartyIDCallingPartyHostPart">$GWHostPort</field>
    <field name="ParameterOut" custom="" parameter="P-
AssertedIdentityUserPart">$EnforcedOutboundCallerId</field>
    <field name="ParameterOut" custom="" parameter="P-
AssertedIdentityHostPart">$ContactUri</field>
  </device>
  <sms>
    <variable name="MESSAGING_API_KEY">
      <option></option>
    </variable>
    <variable name="PROVIDER_URL">
      <option></option>
    </variable>
    <field name="Enabled">0</field>
    <field name="OptionalProvider">1</field>
    <field name="ProviderType">generic</field>
    <field name="OutboundRouting">1</field>
    <field name="ProviderName">Generic</field>
  </sms>
</data>
</doc>

```

To implement template with SIP Trunk configuration Go to **Advance** -> **Templates** -> **Provider Templates** -> **Import Provider** and upload .provider.xml file.

Dashboard	IP Blacklist	Templates	
Users	Anti-Hacking	Phone Templates	DECT / FXS Templates
Voice & Chat	Console Restrictions	Provider Templates	Email Templates
Phones	Network	1tel.pv.xml	
Outbound Rules	Allowed Country Codes	Import Provider	
Departments	CID Rules	<pre> 1 <?xml version="1.0"?> 2 <doc xmlns:tcx="http://www.3cx.com"> 3 <header> 4 <type>gateway-template</type> 5 <version>150003</version> 6 <time>2017-07-11 10:00:00</time> 7 <name>1TEL</name> 8 <url>https://www.3cx.com/docs/manual/sip-trunks/</url> 9 <image></image> 10 <description>DK</description> 11 <tags>e164,registrar,port</tags> 12 <templatetype>preferred</templatetype> 13 </header> 14 <data> 15 <device> 16 <type>provider</type> 17 <manufacturer> 18 </manufacturer> 19 <model>provider</model> 20 <!-- Friendly Name --> 21 <field name="Name">1TEL.DK</field> 22 <!-- Hostnames and Port Numbers --> 23 <field name="RegistrarHost" status="readonly">sip3.1tel.dk</field> 24 <field name="RegistrarPort" status="readonly">5060</field> 25 <field name="ProxyHost" status="readonly"></field> 26 <field name="ProxyPort" status="readonly">5060</field> 27 <field name="StunServerHost" status="readonly"> 28 </field> 29 <field name="StunServerPort" status="readonly"> 30 </field> </pre>	
Office Hours	CID Blacklist		
Call Handling	Secure SIP		
Reports	Codecs		
Event Log	Parameters		
Recordings	Templates		
Backup	Fax		
Integrations	E164		
Advanced	CDR		
System			

In the next step the SIP Trunk configuration needs to be completed in the 3CX section **Voice & Chat**. For the tab **General**: In the section **Account Details** add DID to the field **Main Trunk Number**. In the section **Server Details** add the IP address of the Orange SBC in the **Registrar/Server** field.

The screenshot shows the 'Add Trunk' configuration page in the 3CX Admin Console. The 'General' tab is active. The form includes the following sections and fields:

- General:** Name (text field), Default route (dropdown menu), and a checkbox to 'Create an outbound rule for this SIP Trunk'.
- Voip Provider:** A note to follow the Generic SIP Trunk (IP Based) Configuration Guide and use IP 83.3.165.198 for whitelisting.
- Account Details:** Main Trunk Number (text field), Authentication ID (SIP User ID) (text field), Authentication password (password field), and a checkbox for 'Optional 3-way authentication ID'.
- Server Details:** Registrar/Server (text field), Port (dropdown menu), and a checkbox for 'Auto discovery'.

The tab **General**:

Parameter	Value	Comment
Name	Orange Business Talk/BTIP	Configure service name e.g.: Orange Business TalkBTIP
Main Trunk Number	<i>DID</i>	Configure DID number of the main SIP Trunk
Registrar/Server	<i>IPv4</i>	the Orange aSBC IPv4 address
Registrar/Server -> Port	Port * 0 ☒ Auto discovery	"Auto discovery" checkbox is on
Outbound Proxy -> Port	Port * 0 ☒ Auto discovery	"Auto discovery" checkbox is on

For the next Tab **DID Numbers**, you can add required numbers or import them from a file.

3CX Admin Console

Orange BTIP over BVPN Nominal SBC [Save](#)

General DID Numbers **Options** SMS

Configuration

Limit to: System Wide Number of sim calls per trunk*: 10

☒ Allow inbound calls ☒ Allow outbound calls

Transport Protocol: UDP IP Mode: IPV4

SRTP Mode: Disabled Re-Register timeout: 180

Select which IP to use in 'Contact' (SIP) and 'Connection'(SDP) fields: Use Default Settings IP Address: IP Address

Alternative Proxy: Public IP in SIP via Header:

☒ Include diversion header support

Convert inbound caller ID to E164 number format

Reformat incoming or outgoing caller ID

Caller ID Control

Default Outbound Caller ID:

From : Display Name: "OriginatorCallerID" Original Caller number will be sent

Remote Party ID - Calling Party : Display Name: "OutboundCallerId" Outbound caller Id taken from Extension settings in manage...

P-Asserted Identity : Display Name: Default

Codec priority

+ Add

Priority	Codec
1	G722
2	PCMA
3	G729

E911 Geolocation

The next tab **Options**:

Parameter	Value	Comment
Transport Protocol	UDP	
IP Mode	IPV4	
SRTP Mode	Disabled	
Re-Register timeout	180	
Select which IP to use in 'Contact' (SIP) and 'Connection'(SDP) fields	Use Default Settings	
☒ Include diversion header support	yes	The check-box needs to be checked
☒ Allow inbound calls	yes	The check-box needs to be checked
☒ Allow outbound calls	yes	The check-box needs to be checked

Codec priority	1	G722
	2	PCMA
	3	G729

The created SIP Trunk is listed under **Voice & Chat**.

3CX Admin Console

Voice & Chat

+ Add Trunk + Add Gateway + Add Messaging + Add Bridge + Add SBC + Add DECT / FXS

Search ...

Name	Information
WebMeeting bridge (Master Bridge)	
Orange BTIP over BVPN Nominal SBC	+332...
Orange BTIP over BVPN Backup SBC	+332...

Note: Create Backup SIP Trunk the same way Nominal SIP Trunk was created.

5.1.1 Outbound Rules configuration

For 3CX v 20 add Outbound Rules, prioritizing the Route order, according to customer preferences.

3CX Admin Console

Edit: Outbound rule for Orange BTIP Save

Rule Name*
Outbound rule for Orange BTIP

Calls to numbers starting with prefix: 0
e.g. 0-3,5,6. Leave empty for any prefix

Calls from extension(s):
e.g. 100, 103-105. Leave empty for any extension

Calls to numbers with a length of:
e.g. 9,10,13-15. Leave empty for any length

Calls from Departments
Select which Department(s) can use this outbound rule
+ Add

Make outbound calls on
Configure a route and specify 4 backup routes in case the main fails. Each route can be configured differently. For the rule to work, at least one route must be configured. Failure to do so will result in the call being dropped.

Route	Trunk	Strip digits	Prepend	Outbound caller ID
Route 1	Orange BTIP over BVPN	Strip the first 1 digit(s)		
Route 2	Select Trunk	Strip no digits		
Route 3	Select Trunk	Strip no digits		
Route 4	Select Trunk	Strip no digits		
Route 5	Select Trunk	Strip no digits		

Parameter	Value	Comment
Rule Name	<i>BTIP/BTalk Outgoing</i>	Choose relevant rule name
Calls to numbers starting with prefix	0	Select relevant prefix (e.g. leading 0)
Route [1-5]	<i>BTIP/BTalk SIP trunk</i>	Select destination SIP Trunks in order of preference
Strip Digits	1	Remove leading prefix 0
Prepend	<i>+33</i>	Add Prefix if needed (Country Code e.g. +33 for France)

There are additional options that can be configured if needed for call routing customization.

Note: the correct prefix must be set.

3CX Admin Console																				
- Dashboard - Users - Voice & Chat - Phones - Outbound Rules		Outbound Rules + Add ✎ Edit 🗑 Delete ⬆ Move Up ⬇ Move Down																		
🔍 Search ... <table> <tr> <th>Outbound Rule Name</th> <th>Prefix</th> <th>Call from Ext.</th> <th>Length</th> <th>Department</th> <th>Route 1</th> <th>Route 2</th> </tr> <tr> <td>Outbound rule for Orange BTIP</td> <td>0</td> <td>All</td> <td>Any</td> <td></td> <td>Orange BTIP over BVPN</td> <td>Blocked</td> </tr> </table>							Outbound Rule Name	Prefix	Call from Ext.	Length	Department	Route 1	Route 2	Outbound rule for Orange BTIP	0	All	Any		Orange BTIP over BVPN	Blocked
Outbound Rule Name	Prefix	Call from Ext.	Length	Department	Route 1	Route 2														
Outbound rule for Orange BTIP	0	All	Any		Orange BTIP over BVPN	Blocked														

6 3CX IPBX over Internet configuration guidelines

The checklists below present all the configuration steps required for interoperability between the BTalk/BTIP service over Internet and 3CX IPBX only.

Refer to the official 3CX documentation for the IPBX installation and other telephony settings.

6.1 SIP Trunks configuration for 3CX v20

For 3CX IPBX v20 the SIP trunk configuration parameters have been implemented in the template.

To implement .xml Orange provider template you can download it, right-click on the file below *Orange Business TalkBTIP.pv.xml*, select "copy" from the context menu, save the file locally to implement it later into 3CX.



Orange Business TalkBTIP.pv.xml

or you can create the .xml file which contains the following configuration inside:

```
<doc>
  <header>
    <name>Orange Business Talk/BTIP</name>
    <time>2024-11-27T07:23:48.4948629Z</time>
    <template>
      <!--Do not change this field-->GenericSIPTrunk.pv.xml</template>
    <type>
      <!--Do not change this field-->gateway-template</type>
    </header>
  <data>
    <device>
      <field name="Name">Orange Business Talk/BTIP</field>
      <type>provider</type>
      <manufacturer></manufacturer>
      <model>provider</model>
      <field name="RegistrarHost"></field>
      <field name="RegistrarPort">0</field>
      <field name="ProxyHost"></field>
      <field name="ProxyPort">0</field>
      <field name="IpInContactReg">1</field>
      <field name="TimeBetweenRegistration">180</field>
      <field name="SecondaryRegistrar"></field>
      <field name="IPRestriction">IPV4</field>
      <field name="TransportRestriction"></field>
      <field name="RequireAuthFor">1</field>
      <field name="IpInContactRegValue"></field>
      <field name="RegistrarInvite">0</field>
      <field name="IsSupportReinvite">0</field>
      <field name="IsSupportReplaces">0</field>
      <field name="DisableVideo">1</field>
      <field name="SRTPMode"></field>
      <field name="IsBindToMS">1</field>
      <codecs>
        <codec rfcname="G722" />
        <codec rfcname="PCMA" />
        <codec rfcname="G729" />
      </codecs>
      <field name="ParameterIn" custom="" parameter="FromUserPart">$CallerNum</field>
      <field name="ParameterIn" custom="" parameter="FromUserPart">$CallerName</field>
      <field name="ParameterIn" custom="" parameter="ToUserPart">$CalledNum</field>
      <field name="ParameterOut" custom="" parameter="RequestLineURIUser">$CalledNum</field>
      <field name="ParameterOut" custom="" parameter="RequestLineURIHost">$GWHostPort</field>
    </device>
  </data>
</doc>
```

```

    <field name="ParameterOut" custom="" parameter="ContactUser">$OriginatorCallerId</field>
    <field name="ParameterOut" custom="" parameter="ContactHost">$ContactUri</field>
    <field name="ParameterOut" custom="" parameter="ToDisplayName">$CalledName</field>
    <field name="ParameterOut" custom="" parameter="ToUserPart">$CalledNum</field>
    <field name="ParameterOut" custom="" parameter="ToHostPart">$GWHostPort</field>
    <field name="ParameterOut" custom=""
parameter="FromDisplayName">$OriginatorCallerId</field>
    <field name="ParameterOut" custom=""
parameter="FromUserPart">$OriginatorCallerId</field>
    <field name="ParameterOut" custom="" parameter="FromHostPart">$ContactUri</field>
    <field name="ParameterOut" custom=""
parameter="RemotePartyIDCallingPartyDisplayName">$OutboundCallerId</field>
    <field name="ParameterOut" custom=""
parameter="RemotePartyIDCallingPartyUserPart">$OutboundCallerId</field>
    <field name="ParameterOut" custom=""
parameter="RemotePartyIDCallingPartyHostPart">$GWHostPort</field>
    <field name="ParameterOut" custom="" parameter="P-
AssertedIdentityUserPart">$EnforcedOutboundCallerId</field>
    <field name="ParameterOut" custom="" parameter="P-
AssertedIdentityHostPart">$ContactUri</field>
</device>
<sms>
  <variable name="MESSAGING_API_KEY">
    <option></option>
  </variable>
  <variable name="PROVIDER_URL">
    <option></option>
  </variable>
  <field name="Enabled">0</field>
  <field name="OptionalProvider">1</field>
  <field name="ProviderType">generic</field>
  <field name="OutboundRouting">1</field>
  <field name="ProviderName">Generic</field>
</sms>
</data>
</doc>

```

To implement template with SIP Trunk configuration Go to **Advance** -> **Templates** -> **Provider Templates** -> **Import Provider** and upload .provider.xml file.

Dashboard	IP Blacklist	Templates	
Users	Anti-Hacking	Phone Templates	DECT / FXS Templates
Voice & Chat	Console Restrictions	Provider Templates	Email Templates
Phones	Network	1tel.pv.xml	
Outbound Rules	Allowed Country Codes	Import Provider	
Departments	CID Rules	<pre> 1 <?xml version="1.0"?> 2 <doc xmlns:tcx="http://www.3cx.com"> 3 <header> 4 <type>gateway-template</type> 5 <version>150003</version> 6 <time>2017-07-11 10:00:00</time> 7 <name>1TEL</name> 8 <url>https://www.3cx.com/docs/manual/sip-trunks/</url> 9 <image></image> 10 <description>DK</description> 11 <tags>e164,registrar,port</tags> 12 <templatetype>preferred</templatetype> 13 </header> 14 <data> 15 <device> 16 <type>provider</type> 17 <manufacturer> 18 </manufacturer> 19 <model>provider</model> 20 <!-- Friendly Name --> 21 <field name="Name">1TEL.DK</field> 22 <!-- Hostnames and Port Numbers --> 23 <field name="RegistrarHost" status="readonly">sip3.1tel.dk</field> 24 <field name="RegistrarPort" status="readonly">5060</field> 25 <field name="ProxyHost" status="readonly"></field> 26 <field name="ProxyPort" status="readonly">5060</field> 27 <field name="StunServerHost" status="readonly"> 28 </field> 29 <field name="StunServerPort" status="readonly"> 30 </field> </pre>	
Office Hours	CID Blacklist		
Call Handling	Secure SIP		
Reports	Codecs		
Event Log	Parameters		
Recordings	Templates		
Backup	Fax		
Integrations	E164		
Advanced	CDR		
System			

In the next step the SIP Trunk configuration needs to be completed in the 3CX section **Voice & Chat**. For the tab **General**: In the section **Account Details** add DID to the field the **Main Trunk Number**. In the section **Server Details** add the FQDN of the Orange SBC in the **Registrar/Server** field.

3CX Admin Console

Dashboard Users Voice & Chat Phones Outbound Rules Departments Office Hours Call Handling Reports Event Log Recordings Backup Integrations Advanced System

← Add Trunk Save

General DID Numbers SMS Options

Name *

Default route

User

1000

☐ Create an outbound rule for this SIP Trunk

Voip Provider

Follow the Generic SIP Trunk (IP Based) [Configuration Guide](#). Use this IP for Whitelisting 83.3.165.198

Account Details

Main Trunk Number *

Authentication ID (SIP User ID)

Authentication password

☐ Optional 3-way authentication ID

3 way authentication password *

Type of authentication

Do not require - IP based

Server Details

Registrar/Server *

Port *

0 ☒ Auto discovery

Outbound Proxy

Port *

5061 ☐ Auto discovery

The tab **General**:

Parameter	Value	Comment
Name	<i>*service name</i>	Configure service name e.g.: Orange Business Talk/BTIP
Main Trunk Number	<i>DID</i>	Configure DID number of the main SIP Trunk
Registrar/Server	<i>FQDN</i>	Configure the Orange aSBC FQDN
Outbound Proxy -> Port	Port * 5061 ☐ Auto discovery	Uncheck checkbox "Auto discovery" and add Port 5061

For the next Tab **DID Numbers**, you can add required numbers or import them from a file.

3CX Admin Console

← Orange BTIP over Internet Nominal SBC [Save](#)

General DID Numbers **Options** SMS

Configuration

Limit to: System Wide Number of sim calls per trunk*: 10

☒ Allow inbound calls ☒ Allow outbound calls

Transport Protocol: TLS IP Mode: IPV4

Certificate: root_cert_10000.pem
Certificates eventually expire. When your Certificate expires, Voice calls will stop working. You will need to know when the certificate is about to expire. Before expiration, generate a new certificate and re-upload the cert.

SRTP Mode: Enforced Re-Register timeout: 180

Select which IP to use in 'Contact' (SIP) and 'Connection'(SDP) fields: Use Default Settings IP Address: IP Address

Alternative Proxy: Public IP in SIP via Header

☒ Include diversion header support

Convert inbound caller ID to E164 number format

Reformat incoming or outgoing caller ID

Caller ID Control

Default Outbound Caller ID

From : Display Name: "OutboundCallerId" Outbound caller Id taken from Extension settings in manage...

Remote Party ID - Calling Party : Display Name: "OutboundCallerId" Outbound caller Id taken from Extension settings in manage...

P-Asserted Identity : Display Name: Default

Codec priority

+ Add

Priority	Codec
1	PCMA

The next tab **Options**:

Parameter	Value	Comment
Transport Protocol	TLS	
Certificate		Upload Orange SBC Root Certificate
IP Mode	IPV4	
SRTP Mode	Enforced	
Re-Register timeout	180	
Select which IP to use in 'Contact' (SIP) and 'Connection'(SDP) fields	Use Default Settings	
☒ Include diversion header support	yes	The check-box needs to be checked
☒ Allow inbound calls	yes	The check-box needs to be checked

☒ Allow outbound calls	yes	The check-box needs to be checked
Codec priority	1 PCMA	

The created SIP Trunk is listed under **Voice & Chat**.

Note: Create Backup SIP Trunk the same way Nominal SIP Trunk was created.

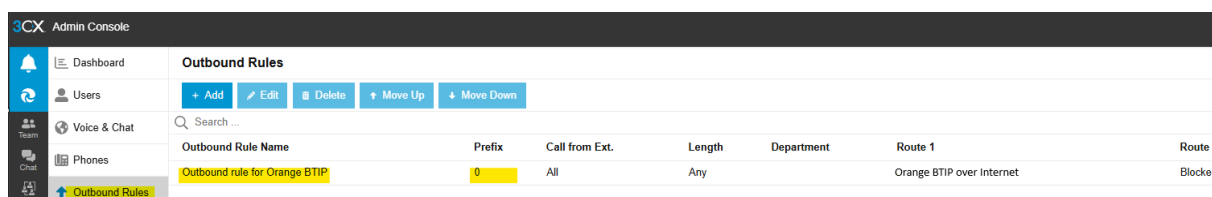
6.1.1 Outbound Rules configuration

For 3CX v 20 add Outbound Rules, prioritizing the Route order, according to customer preferences.

Parameter	Value	Comment
Rule Name	<i>BTIP/BTalk Outgoing</i>	Choose relevant rule name
Calls to numbers starting with prefix	0	Select relevant prefix (e.g. leading 0)
Route [1-5]	<i>BTIP/BTalk SIP trunk</i>	Select destination SIP Trunks in order of preference
Strip Digits	1	Remove leading prefix 0
Prepend	+33	Add Prefix if needed (Country Code e.g. +33 for France)

There are additional options that can be configured if needed for call routing customization.

Note: the correct prefix must be set.



The screenshot shows the 3CX Admin Console interface. On the left is a sidebar with navigation icons for Dashboard, Users, Voice & Chat, Phones, and Outbound Rules. The main area is titled 'Outbound Rules' and contains a table with the following data:

Outbound Rule Name	Prefix	Call from Ext.	Length	Department	Route 1	Route 2
Outbound rule for Orange BTIP	0	All	Any		Orange BTIP over Internet	Blocked

6.2 3CX IPBX configuration with your own Public Certificate Authority

Reminder: 3CX IPBX uses the Let's Encrypt Certification Authority by default. However for customers that prefer to manage their IPBX via their own Domain Server and Domain, a FQDN certificate needs to be provided during 3CX installation for the IPBX. You can obtain a certificate from a public certificate authority, e.g. DigiCert, GlobalSign, etc... It is the recommended method by Orange Business.

Prerequisites: To use a trusted certificate for your custom FQDN you need:

- A static public IP address assigned to your 3CX Phone System.
- Your own public domain name, e.g. mycompany.com.
- Your own public and manageable DNS, e.g. Google Cloud DNS.
- An FQDN certificate for the 3CX PBX, e.g. 3cx.mycompany.com.

To obtain an Identity Certificate signed by a public Certificate Authority, first you must generate your CSR and private key based on the information of the IPBX and Company with SHA-256 encryption (and standard private key size = 2048 bytes).

Note that it is not possible to generate a CSR file directly on the 3CX IPBX. The customer must therefore generate the Certificate Signing Request file within a private key file (e.g. by using OpenSSL tool on Linux or Windows). Then use the CSR file to obtain signed Identity Certificate signed by a public Certification Authority before installing it onto the 3CX IPBX.

Here is the example of CSR and private key generation using OpenSSL tool:

The OpenSSL command below will generate a 2048-bit RSA private key and CSR:

openssl req -newkey rsa:2048 -sha256 -keyout myserver.key -out server.csr

Let's break the command down:

- *openssl* - is the command for running OpenSSL.
- *req* - is the OpenSSL utility for generating a CSR.
- *newkey rsa:2048* - tells OpenSSL to generate a new 2048-bit RSA private key. If you would prefer a 4096-bit key, you can change this number to 4096.
- *keyout myserver.key* - specifies where to save the private key file.
- *out server.csr* - specifies where to save the CSR file.
- With these last two items, remember to use your own paths and filenames for the private key and CSR, not the placeholders.

After typing the command, press **enter**. You will be presented with a series of prompts:

- First create and verify a pass phrase. **Remember this pass phrase because you will need it again to access your private key.**
- You will now be prompted to enter the information which will be included into your CSR. This information is also known as the **Distinguished Name**, or **DN**. The **Common Name** field is required by SSL.com when submitting your CSR, but the others are optional. If you would like to skip an optional item, simply type **enter** when it appears:
 - The **Country Name** (optional) takes a two-letter country code.
 - The **Locality Name** field (optional) is for your city or town.
 - The **Organization Name** field (optional) is for the name of your company or organization.
 - The **Common Name** field (required) is used for the Fully Qualified Domain Name (FQDN) of the website this certificate will protect.
 - **Email Address** (optional)
 - The **Challenge** Password field is optional and can be skipped as well.

Upon completion of this process, you will be returned to a command prompt. You will not receive any notification that your CSR was successfully created.

```
admin@am...> openssl req -newkey rsa:2048 -sha256 -keyout myserver.key -out server.csr
Generating a RSA private key
.+++++
.....+++++
writing new private key to 'myserver.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:FR
State or Province Name (full name) []:Bretagne
Locality Name (eg, city) [Default City]:Rennes
Organization Name (eg, company) [Default Company Ltd]:Orange
Organizational Unit Name (eg, section) []:OBS
Common Name (eg, your name or your server's hostname) []:3cx.ig...net
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
admin@am...>
```

After you receive the Identity Certificate (e.g. .pem format), load it during the 3CX IPBX installation phase within a decrypted private key file. Also upload an identity certificate and a decrypted private key file on the 3CX PBX web management configuration page. Go to 3CX menu **Security – Secure SIP**, according to the table below:

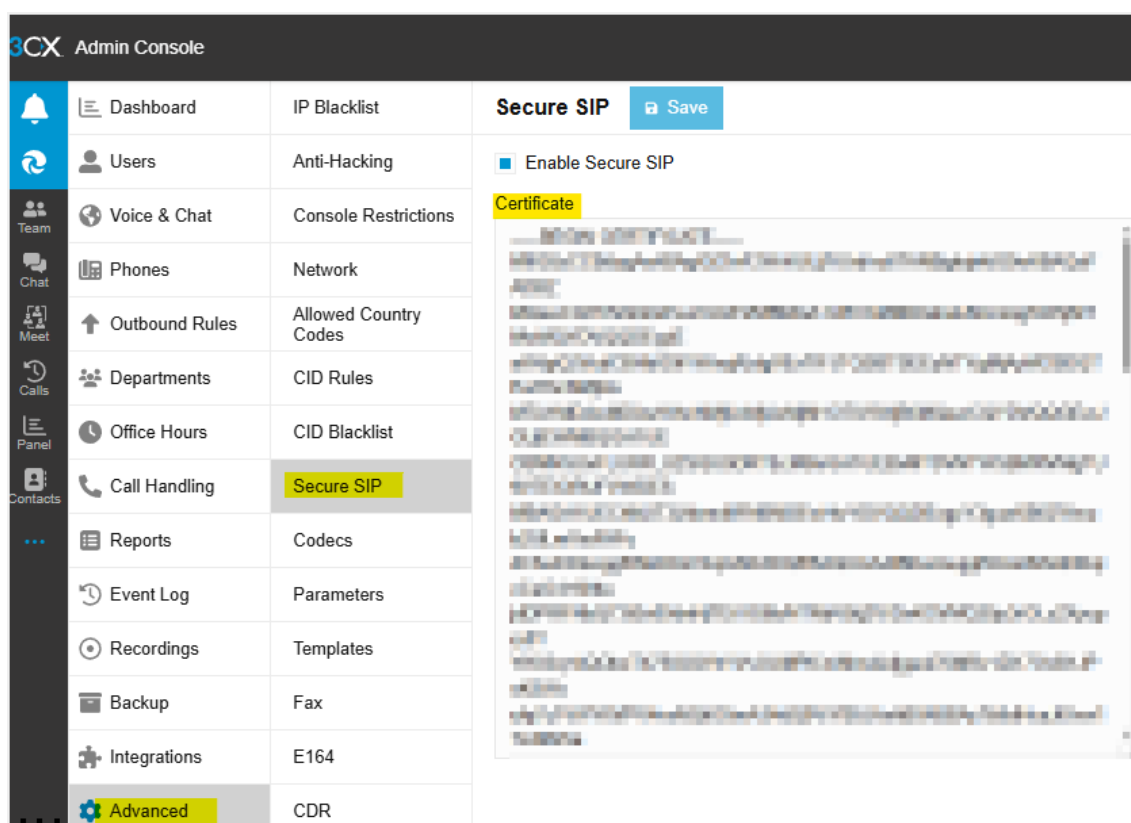
Parameter	Value	Comment
Security – Secure SIP – Secure SIP TLS	checked	Select checkbox
Security – Secure SIP	Certificate	Paste 3CX PBX identity certificate
Security – Secure SIP	Private Key	Paste decrypted 3CX PBX private key

6.5 Public Certificate Authority renewal

When certificate is about to expire it must be renewed.

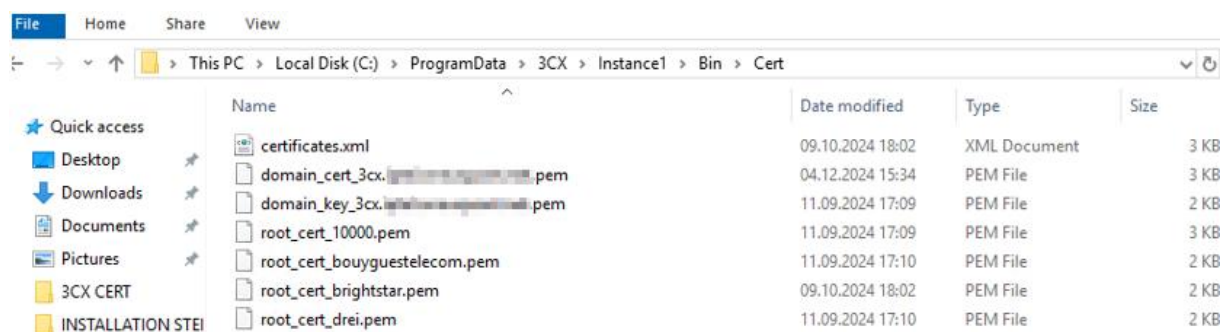
The new identity certificate from Public Certificate Authority need to be uploaded to 3CX via web.

Go to **3CX --> Advanced --> Secure SIP -->** and paste new certificate in **Certificate** field and restart the SIP service.

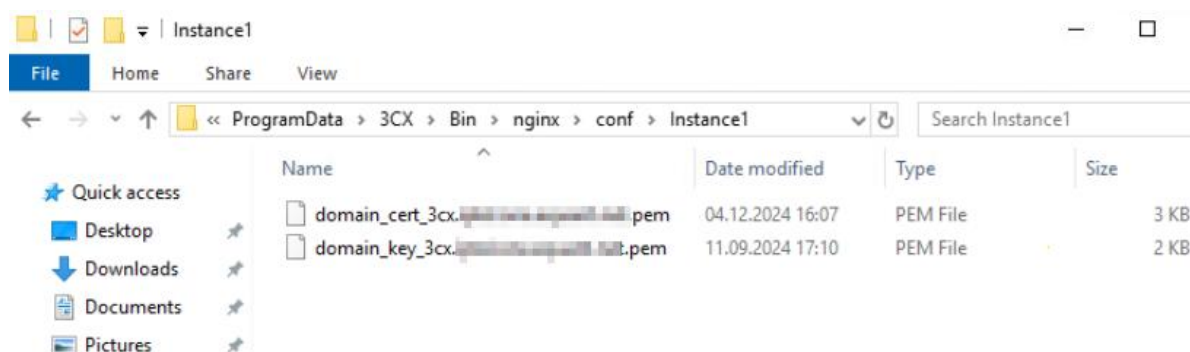


For Windows the SIP Server Certificates for the SIP Trunk are stored here:
C:\ProgramData\3CX\Instance1\Bin\Cert

After uploading new certificate via web in above step, the certificate will be updated in following folder after SIP service restart, described at the end of this chapter.



For Windows the Nginx Certificates are stored here: *C:\ProgramData\3CX\Bin\nginx\conf\Instance1*



This certificate is needed to access 3CX web management.

Replace the *domain_cert_FQDN.pem* and restart the Nginx and SIP services.

To restart 3CX Services go to **3CX --> Dashboard --> form section Troubleshooting chose the Services:**

3CX Admin Console

Dashboard

System Information

Type Professional Annual 4 Simultaneous Calls Expires on Partner Link License Ovr

Custom FQDN 3cx. Install Type On Premise Network Port

IPv4 8 Static IPv6 N/A Active Calls

Trunks Phones System Ext

System Maintenance

Updates available 1 NEW

AUTO UPDATES DISABLED

Automatic Backup OFF Sep 11, 2024, 2:10:43 PM Maintenance

Recordings 0.00 / 5.00 GB Voicemail

Call Log Purge 293 Calls Chat Log

Troubleshooting

Services Restart OS Capture

Activity logs Firewall Export System

Select services:

- 3CX PhoneSystem 01 SIP Server
- 3CX PhoneSystem Nginx Server

And select the **Restart** option from the menu at the top of the screen:

3CX Admin Console

Services

Start Stop Restart

Service Name	Memory Usage	CPU Usage	Threads	Handles	Status
3CX PhoneSystem Database Server	26.69 MB	0	25	3882	Running
3CX PhoneSystem 01 AudioProvider	2.67 MB	0	8	167	Running
3CX PhoneSystem 01 Call Flow Server	88.77 MB	0	15	429	Running
3CX PhoneSystem 01 Configuration Server	15.57 MB	0	20	247	Running
3CX Event Notification Manager	31.89 MB	0	25	454	Running
3CX Gateway Service	43.73 MB	0	13	580	Running
3CX PhoneSystem 01 IVR Server	166.08 MB	0	15	222	Running
3CX PhoneSystem Media Server	8.59 MB	0	27	241	Running
3CX PhoneSystem 01 SIP Server	21.18 MB	0	30	302	Running
3CX PhoneSystem 01 Management Console	189.31 MB	0	35	951	Running
3CX PhoneSystem 01 Queue Manager Server	37.15 MB	0	17	391	Running
3CX PhoneSystem 01 System Server	78.97 MB	0	29	909	Running
3CX PhoneSystem Nginx Server	11.94 MB	0	9	454	Running
	722.54 MB	0			

Glossary

- BVPN : Business Virtual Private Network (Orange Business MPLS network)
- BTIP : Business Talk IP (France) over BVPN
- BTalk : Business Talk (International) over BVPN
- BTIPol : Business Talk IP over Internet (France)
- BTol : Business Talk over Internet (International)
- aSBC : access Session Border Controller (Orange Business Services infrastructure)
- SBC*/3CX : enterprise Session Border Controller on customer side. Customer SBC is optional.
- AS : Application Server Business Talk / BTIP
- EOL : "End of life" in the context of manufacturing and product lifecycles, is the final stages of a product's existence.