Business Talk & BTIP
3CX IPBX

version addressed in this guide: 20.x

Version of 16/10/2026

Table of contents

1 Goal of this document 3
2 Certified architectures 4
2.1 Introduction to architecture components and features 4
2.2 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 Mutual Authentication regarding public certificate Extended Key Usage (EKU) 8
2.3.7 TLS v1.3 and v1.2 cipher suites 10
3 Parameters to be provided by customer to access service 11
3.1 3CX IPBX – BTIP/BTalk over BVPN 11
3.2 3CX IPBX – BTIP/BTalk over Internet 11
4 Certified software and hardware versions 12
4.1 3CX certified versions 12
4.1 3CX Supported IP Phones 12
5 3CX IPBX over BVPN configuration guidelines 13
5.1 SIP Trunks configuration for 3CX v20 13
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 23
6.2 3CX IPBX configuration with your own Public Certificate Authority 24
6.5 Public Certificate Authority renewal 26
Glossary 29

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

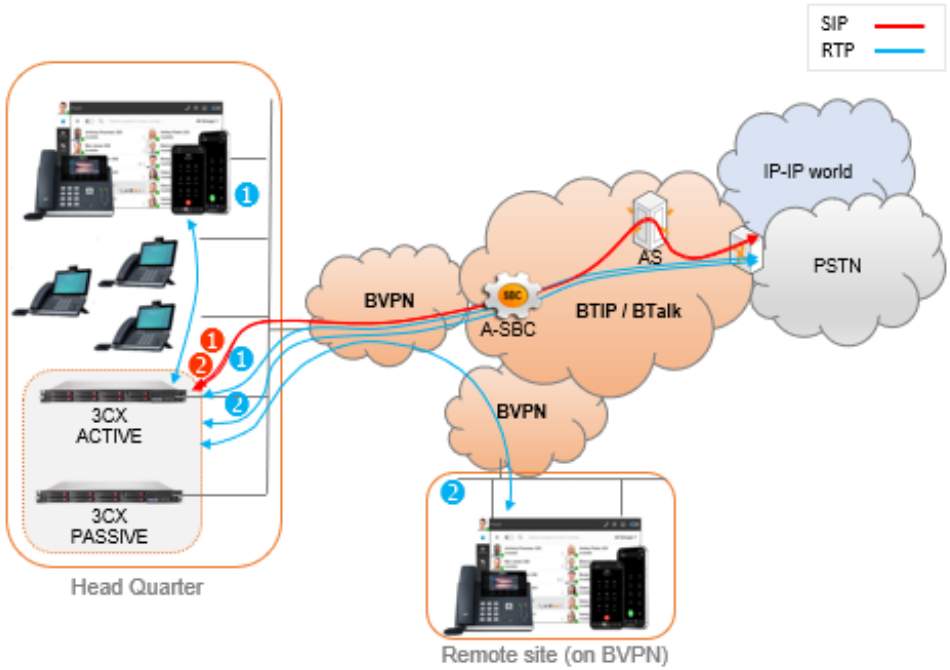
2.1 Introduction to architecture components and features

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 (Differenciated 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.

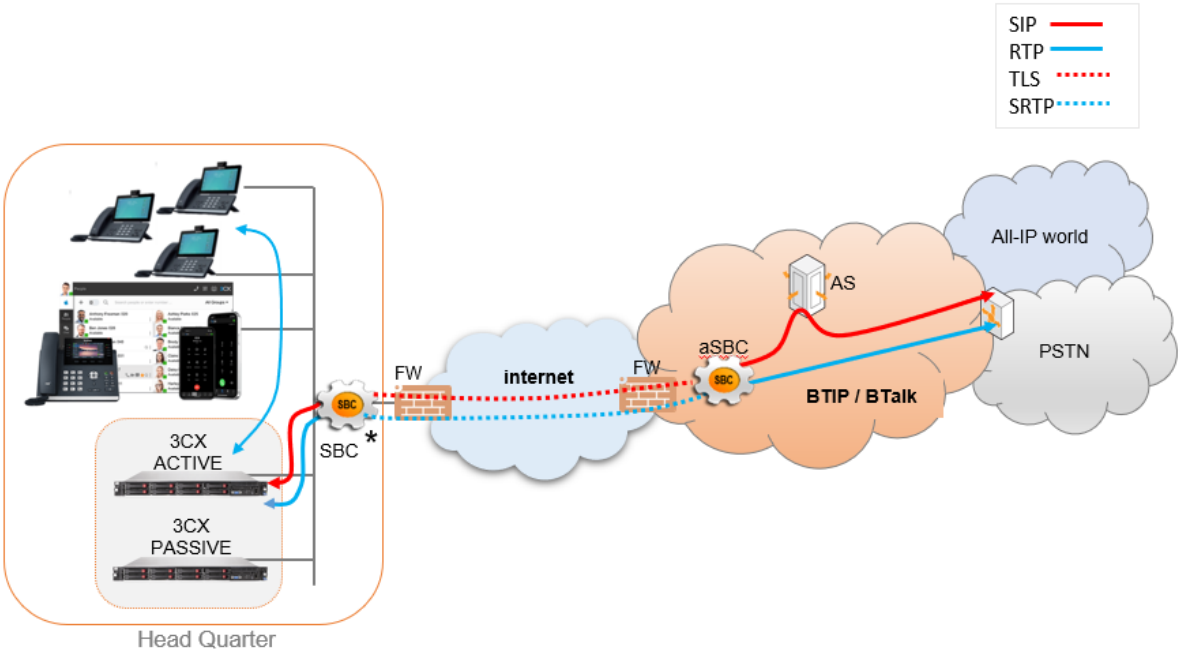
BTIP in French overseas departments are also supported. Dedicated aSBC pairs in Caribbean and Indian Ocean zones are deployed for local calls. For a trunking point of view, the mechanism is similar to “Business Talk French customers”, the IPBX must support international dial plans and route local calls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

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. BTIPoI can be reached using FQDN only, whereas BToI can be reached either via public IP address or FQDN.

- BTIPoI (France) supports type SRV & type A for DNS resolution and do not support direct public IP connections.
- BToI (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. BToI and BTIPoI vary concerning the UDP port range.

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

BTIPoI/BToI 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	BTIPoI: UDP 6000-38000 BToI: UDP 6000-20000	Orange aSBC public @IP	BTIPoI: UDP 6000-38000 BToI: UDP 6000-20000	SRTP media
Orange aSBC public @IP	BTIPoI: UDP 6000-38000 BToI: UDP 6000-20000	SBC*/3CX public @IP	BTIPoI: UDP 6000-38000 BToI: 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 IPPBX.

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 Mutual Authentication 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:

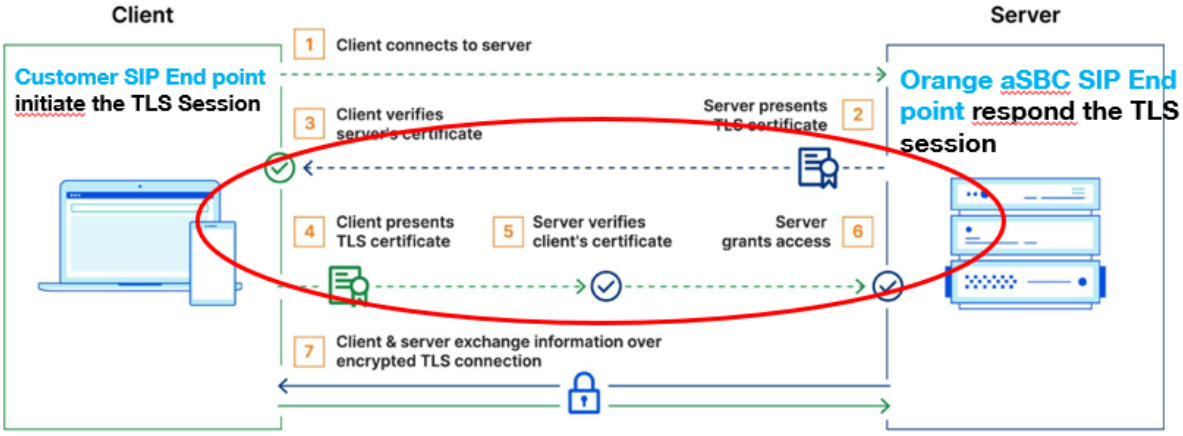
- which endpoint acts as the TLS client or TLS server.
- and the vendor capabilities for handling certificates without the Client Authentication EKU

3CX TLS Handshake behaviour

Case 1 – 3CX initiates the TLS handshake

The 3CX acts as the TLS client, and the **Orange aSBC SIP Endpoint** acts as the TLS server.

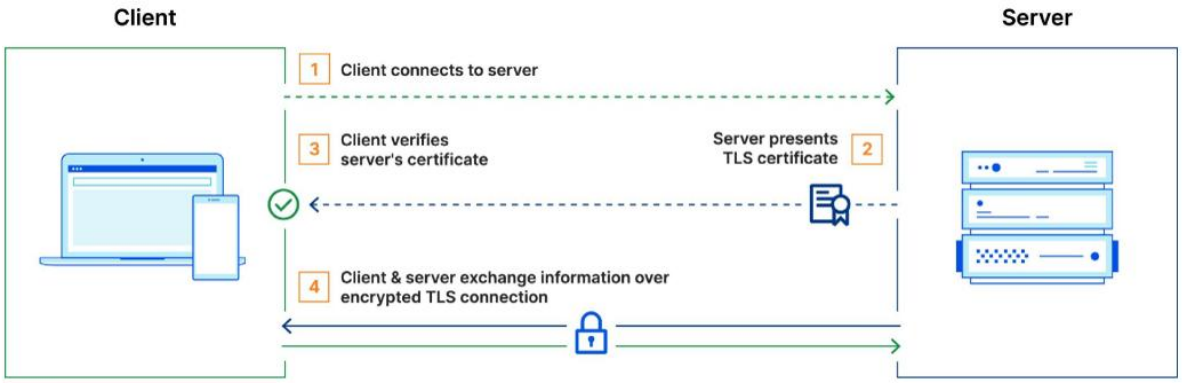
1. The Orange aSBC requests the customer certificate (TLS message “Certificate request”)
2. The 3CX presents its certificate with **Server Authentication (serverAuth) EKU only [4].**
3. The Orange aSBC verifies the certificate **[5]** and grants access **[6]**.



Case 2 – no mTLS occurred

Orange aSBC SIP Endpoint acts as the TLS client, and the 3CX acts as the TLS server.

3CX grants access directly without this verification, TLS handshake success.



2.3.7 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)

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

*BTIPoI can be reached using FQDN only, whereas BToI 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 10
3CX PBX	R20.x	✓	Load 20.0 Update 6
3CX PBX	R20.x	✓	Load 20.0 Update 5

4.1 3CX Supported IP Phones

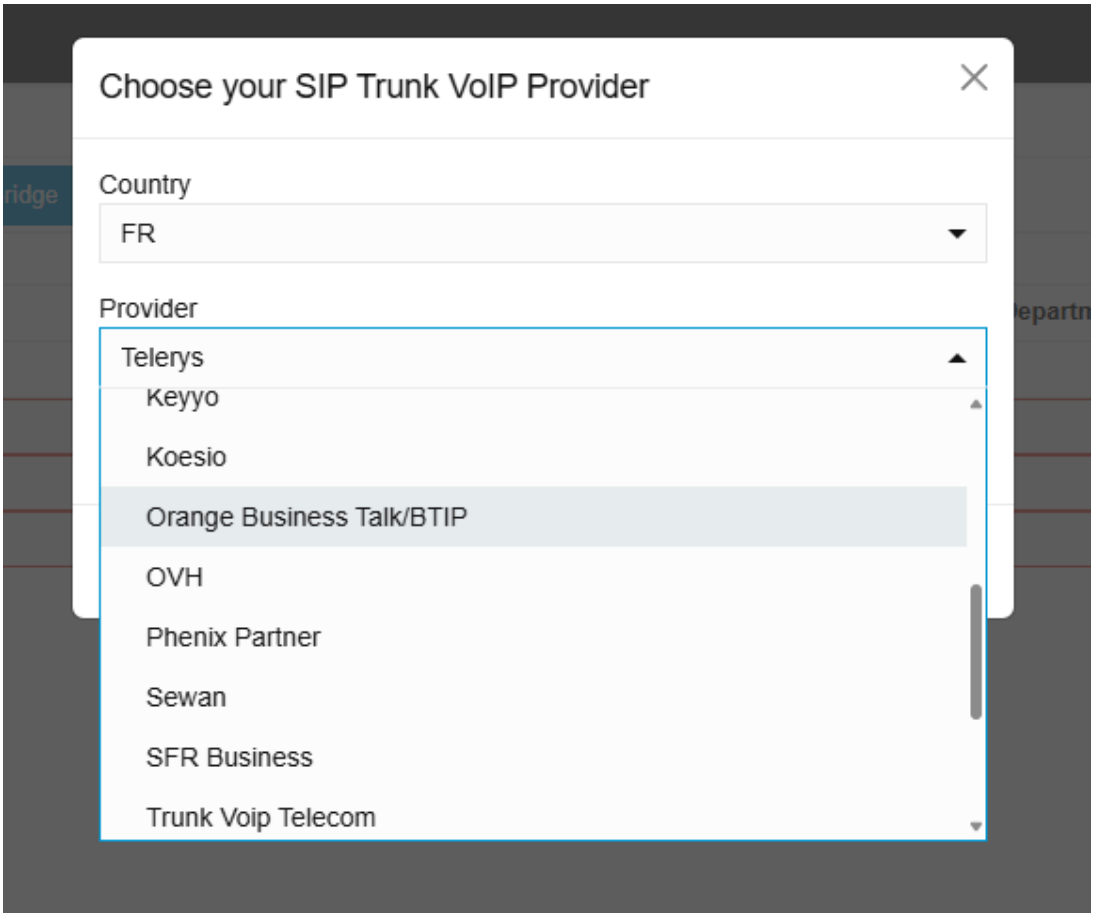
Supported models can be found on the official 3CX website: Which IP Phones work with 3CX

5 3CX IPBX over BVPN configuration guidelines

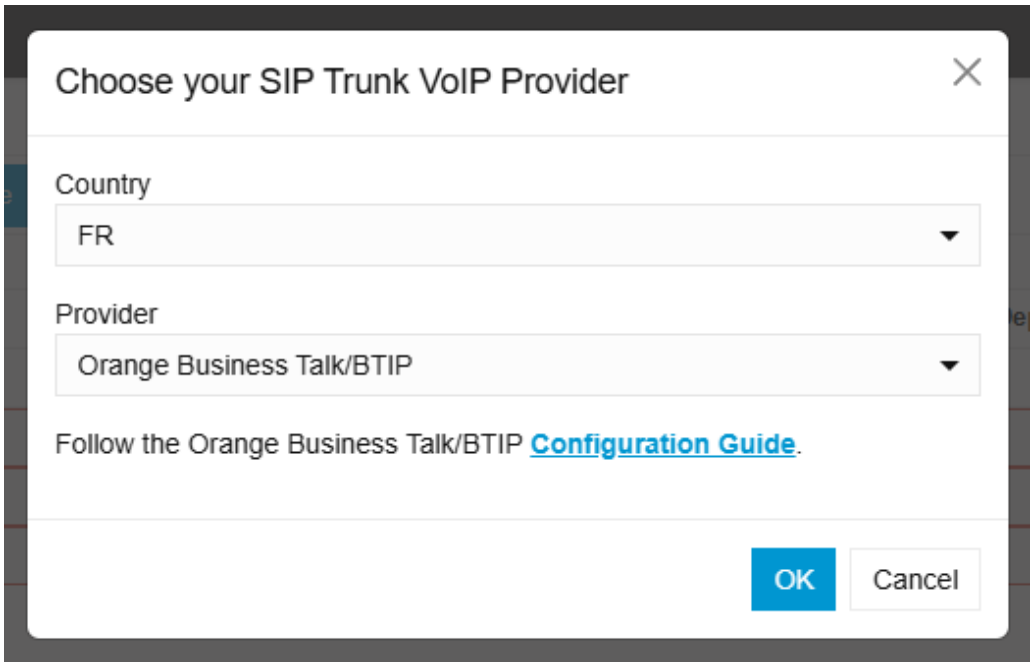
The checklists below present all the configuration steps required for interoperability between the BTalk/BTIP service over BVPN and 3CX IPBX only.
Refer to the official 3CX documentation for the IPBX installation and other telephony settings.

5.1 SIP Trunks configuration for 3CX v20

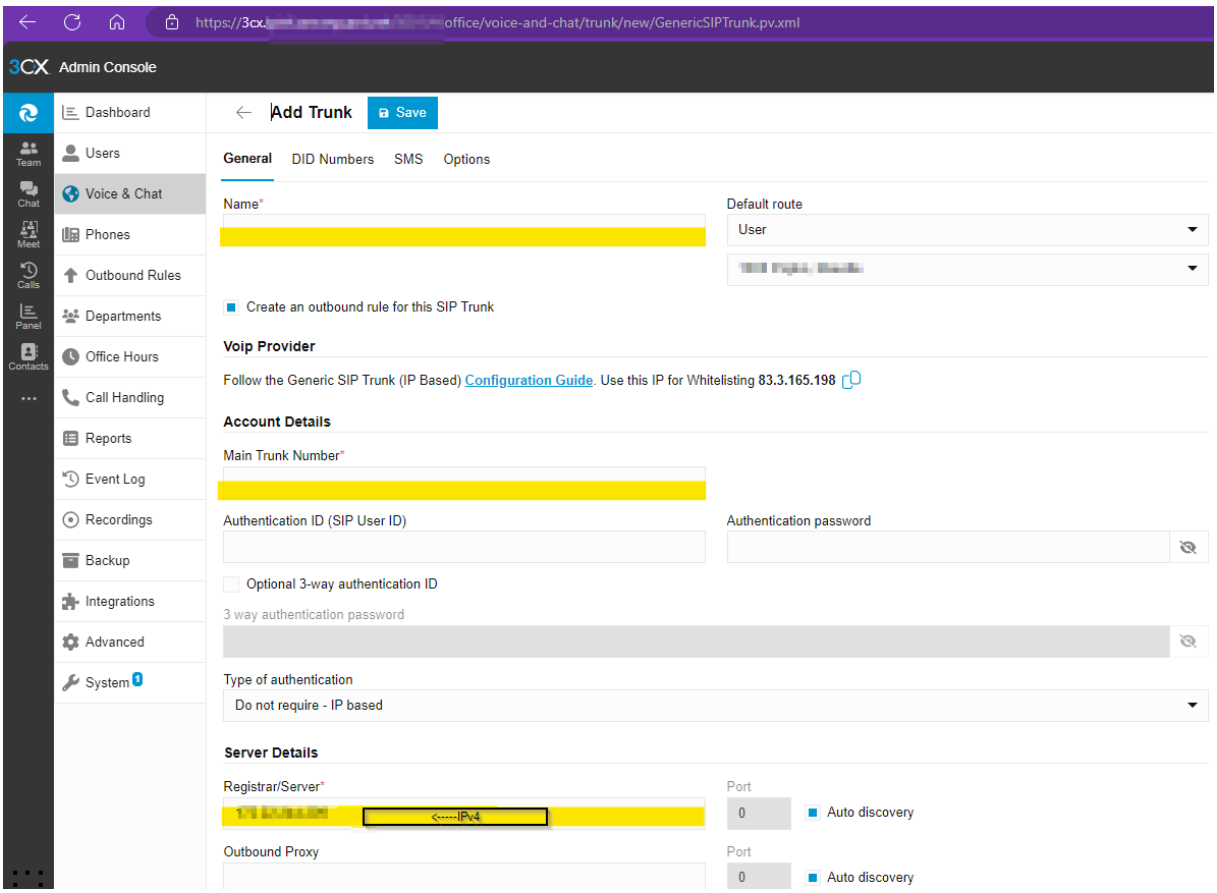
For 3CX IPBX v20 the SIP trunk configuration parameters have been implemented in the build-in template. To start configuring the SIP trunk, you need to select **Voice & Chat** tab. Next, select the **Add Trunk** option to open "**Choose your SIP Trunk VoIP Provider"** menu window.



The **"Choose your SIP Trunk VoIP Provider"** menu includes options for selecting a country, with "FR" (France) currently chosen. Below the country selection, there is a list of VoIP providers. Select **Orange Business Talk/BTIP** from the list of providers.



After filling out the "**Choose your SIP Trunk VoIP Provider**" menu, click the OK button and complete the SIP Trunk configuration.



To configure the SIP trunk, start by entering a descriptive name in the "**Name**" field. Next, input the main trunk number in the "**Main Trunk Number**" field. Then, enter the SIP server address in the "**Registrar/Server**" field, ensuring it matches your provider's details. Set the port number as default and enable "**Auto discovery**" for setup.

The tab **General:**

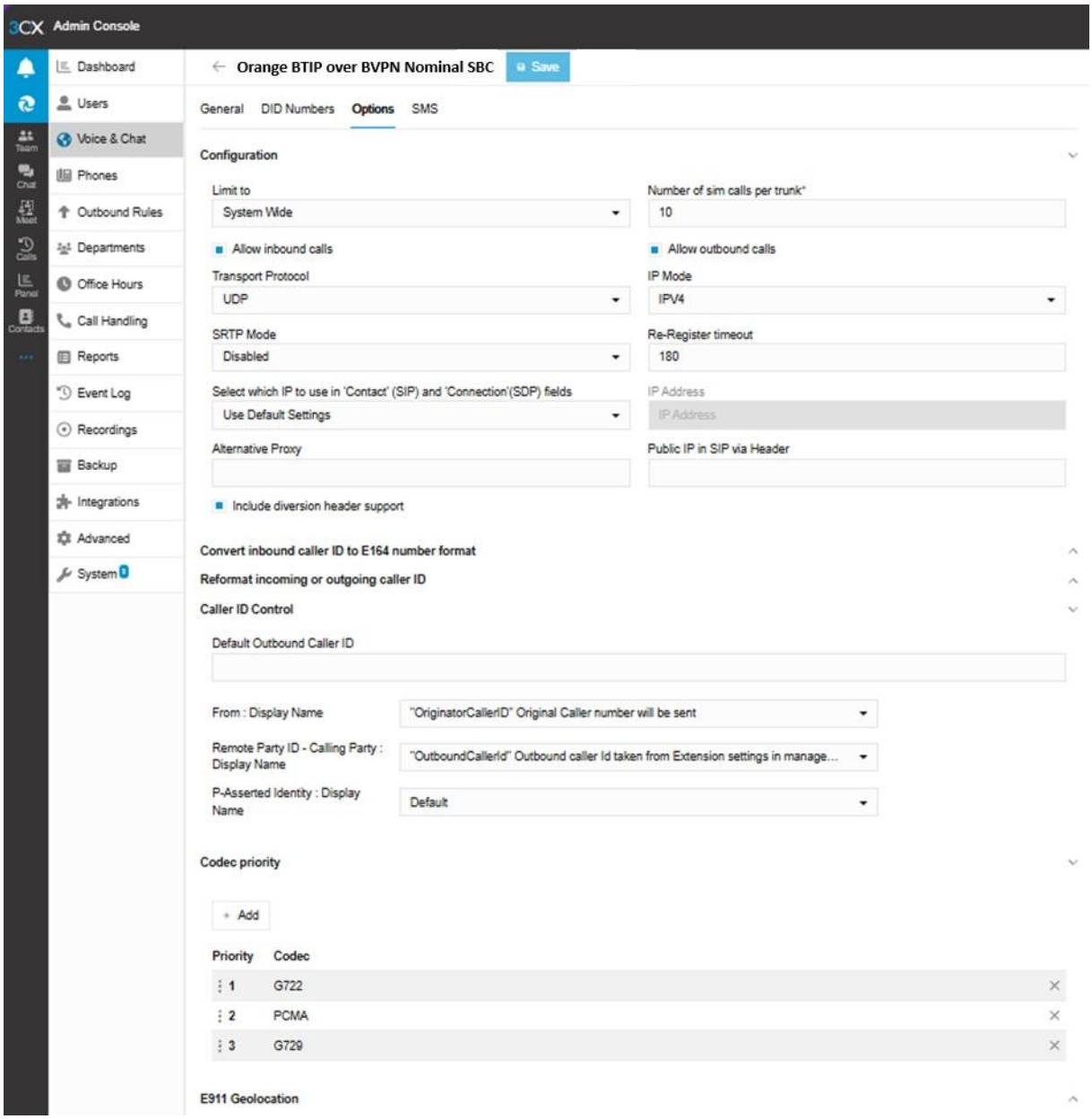
Parameter	Value	Comment
Name	Orange Business Talk/BTIP	Configure service name e.g.: Orange Business TalkBTIP
Main Trunk Number	*DID*	Configure DID number of the main SIP Trunk
Registrar/Server	*IPv4*	the Orange aSBC IPv4 address
Registrar/Server -> Port	Port * 0 Auto discovery	"Auto discovery" checkbox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

After completing the "**General**" tab, proceed to the "**Options**" tab.

The "**Options**" tab allows you to customize various settings for your SIP trunk. At the top, you can set the limit for the number of simultaneous calls per trunk, with the default set to 10. Enable inbound and outbound calls using the checkboxes "**Allow inbound calls**" and "**Allow outbound calls**." In the "Options" tab, set the "Transport Protocol" to **UDP**. Ensure the "IP Mode" is set to **IPv4**. The "Re-Register timeout" should be set to **180 seconds**. In the **"Caller ID Control**" section, specify the **default outbound caller ID** and configure how the caller ID appears in outgoing calls, including the display name for both the originator and remote party. Set the "**P-Asserted-Identity**" to **default**. To prioritize codecs, add codecs to the list and set their order of priority. The available codecs are **G722**, **PCMA**, and **G729**, with **G722** set as the highest priority.

After completing click "**Save**" to finalize the configuration.

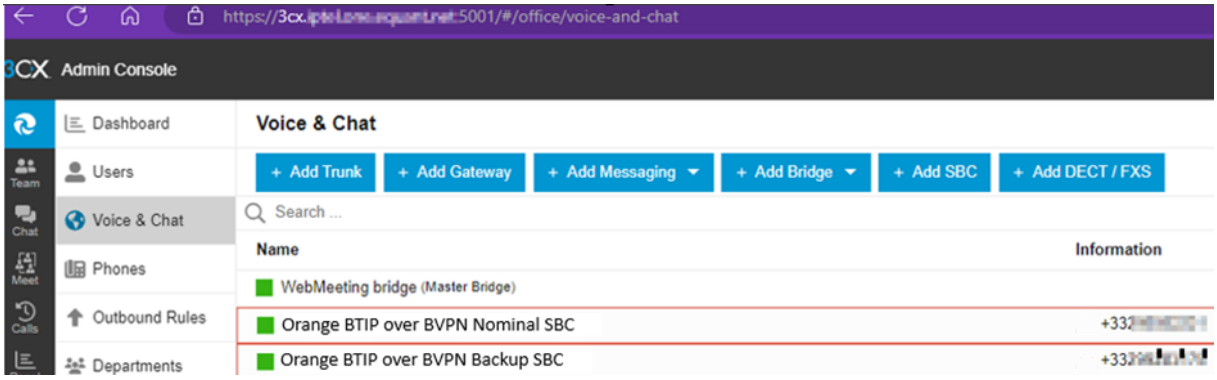


The next tab **Options:**

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	

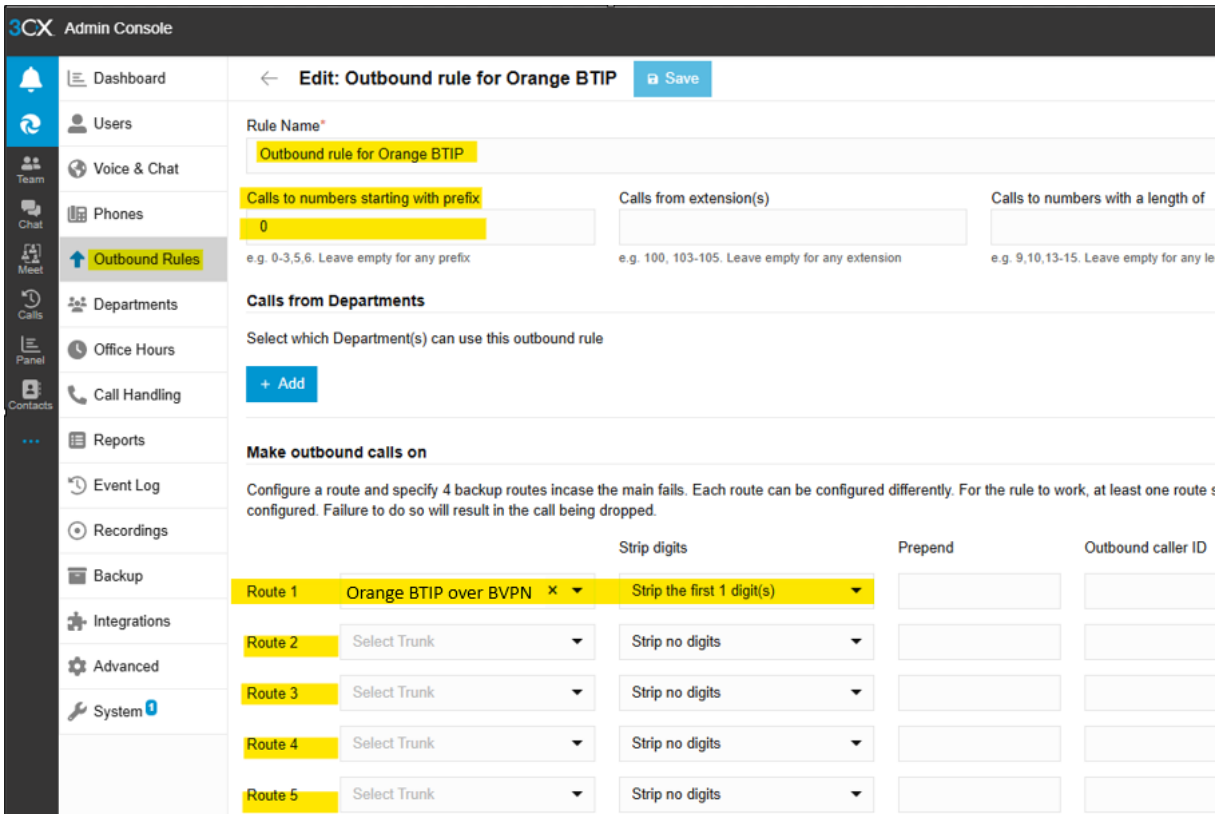
The created SIP Trunk is listed under **Voice & Chat.**



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

5.1.1 Outbound Rules configuration

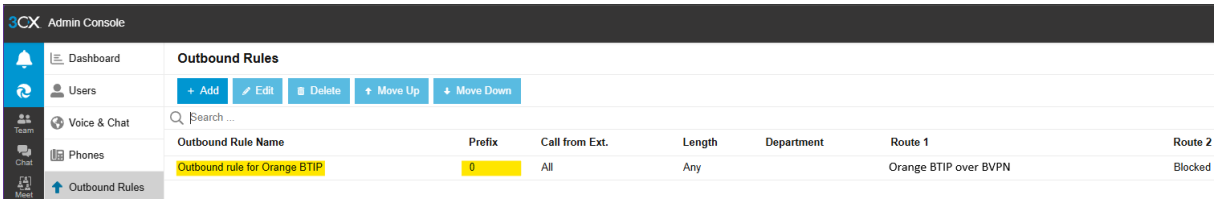
For 3CX v 20 add Outbound Rules, prioritizing the Route order, according to customer preferences.



Parameter	Value	Comment
Rule Name	*BTIP/BTalk Outgoing*	Choose relevant rule name
Calls to numbers starting with prefix	0	Select relevant prefix (e.g. leading 0)
Route [1-5]	*BTIP/BTalk SIP trunk*	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 "**Outbound Rules**" configuration in the admin console shows a list of rules that define how outgoing calls are handled. On the above screen, there is one rule named "**Outbound rule for Orange BTIP**," highlighted in yellow.

The rule has a "Prefix" set to **0**, which means that all outgoing calls will include this prefix. The "**Call from Ext.**" column is set to **All**, indicating that the rule applies to calls from any extension.

The "**Length**," "**Department**," "**Route 1**," and "**Route 2**" columns specify additional routing details. In this case, calls matching this rule are routed through "**Orange BTIP over BVBN**," and the second route is marked as "**Blocked**," meaning calls matching this rule will be blocked from using the second route.

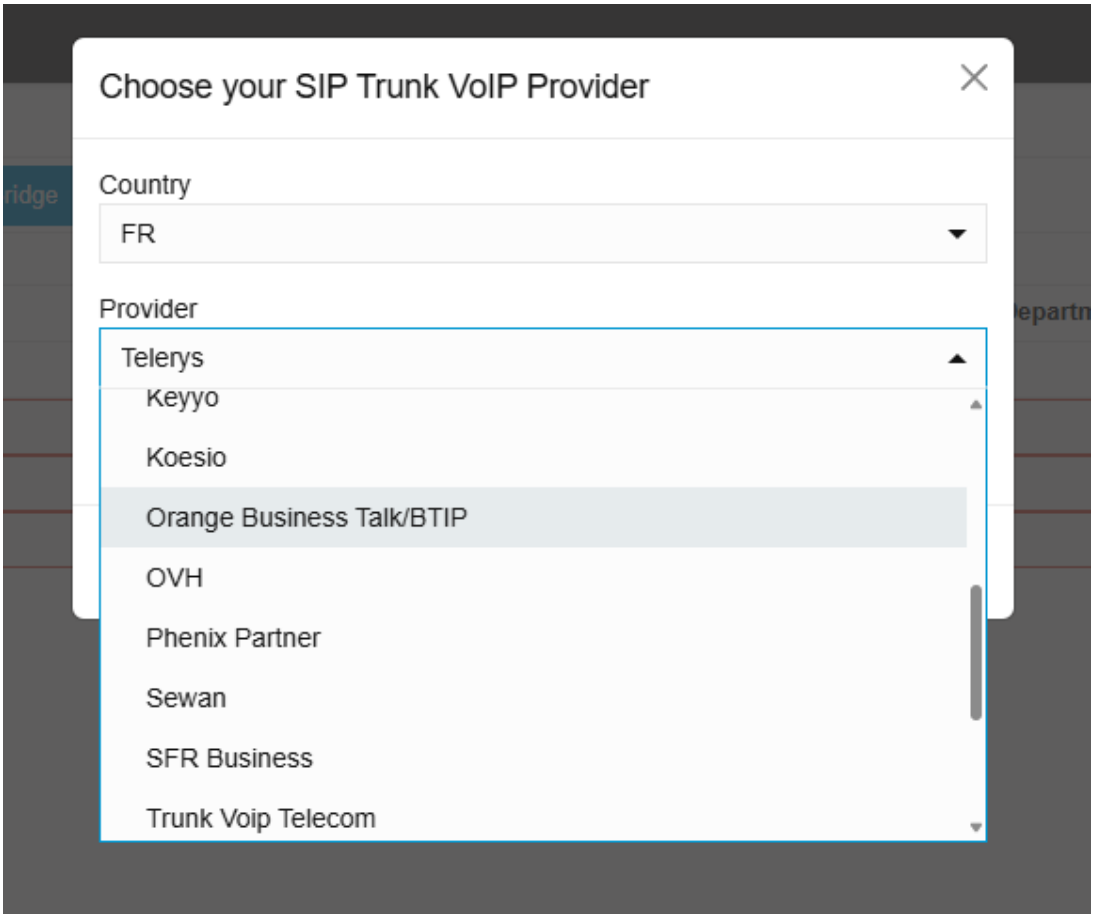
This setup allows you to define specific rules for outgoing calls, including prefixes, routing paths, and restrictions.

6 3CX IPBX over Internet configuration guidelines

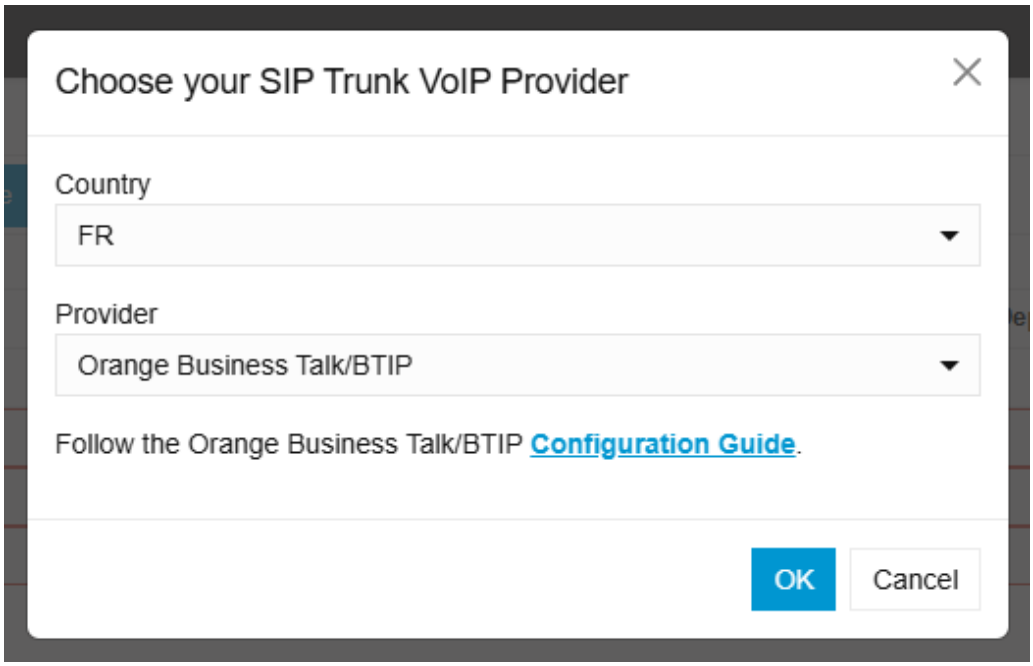
The checklists below present all the configuration steps required for interoperability between the BTalk/BTIP service over Internet and 3CX IPBX only.
Refer to the official 3CX documentation for the IPBX installation and other telephony settings.

6.1 SIP Trunks configuration for 3CX v20

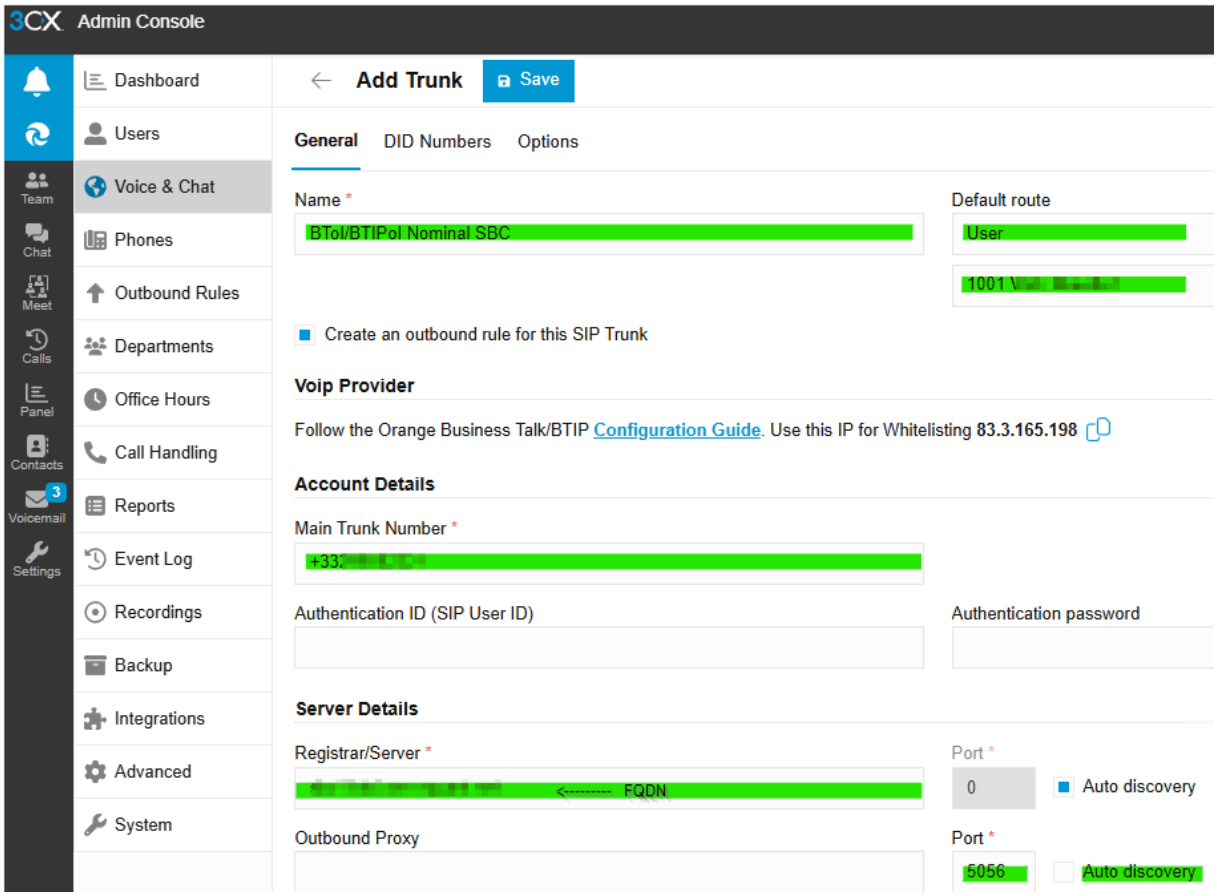
For 3CX IPBX v20 the SIP trunk configuration parameters have been implemented in the build-in template. To start configuring the SIP trunk, you need to select **Voice & Chat** tab. Next, select the **Add Trunk** option to open "**Choose your SIP Trunk VoIP Provider"** menu window.



The **"Choose your SIP Trunk VoIP Provider"** menu includes options for selecting a country, with "FR" (France) currently chosen. Below the country selection, there is a list of VoIP providers. Select **Orange Business Talk/BTIP** from the list of providers.



After filling out the "**Choose your SIP Trunk VoIP Provider**" menu, click the OK button and complete the SIP Trunk configuration.



To set up SIP Trunk over Internet, start by entering a descriptive name in the "**Name**" field, such as "**BTol/BTIPol Nominal SBC**," highlighted in green. If you want to create an outbound rule for this SIP trunk, check the box labeled "**Create an outbound rule for this SIP Trunk**." In the "**Account Details**" section, input the "**Main Trunk Number**," e.g. starting with +33 for French clients. Under "**Server Details**," enter the "**Registrar/Server**" address, which is a **FQDN** - Fully Qualified Domain Name. Set "**Auto discovery**" for the server registration. For the outbound proxy, leave the field empty and set the "**Port**" to **5056**, and ensure the "**Auto discovery**" option is disabled.

The tab **General:**

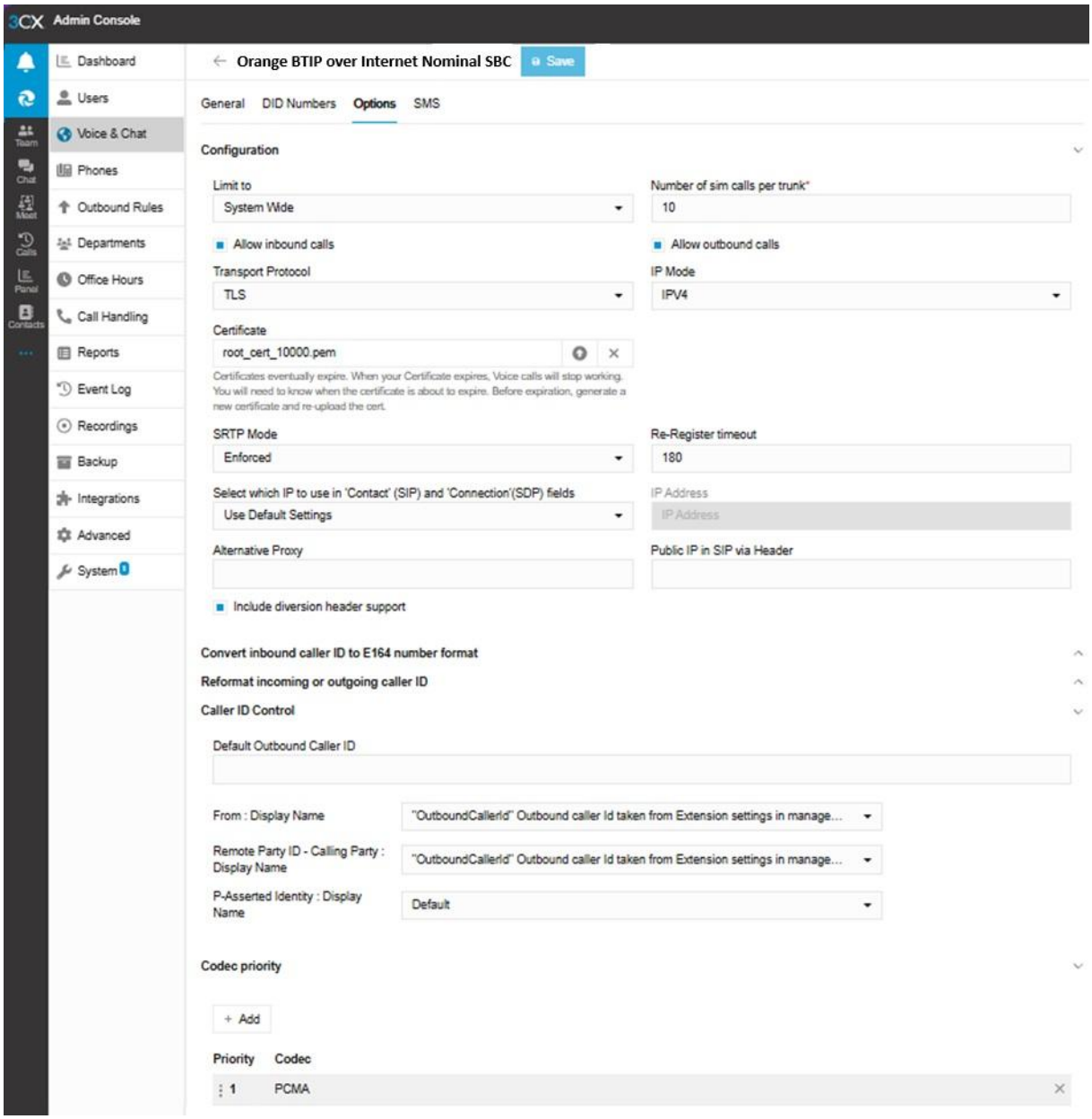
Parameter	Value	Comment
Name	**service name*	Configure service name e.g.: Orange Business Talk/BTIP
Main Trunk Number	*DID*	Configure DID number of the main SIP Trunk
Registrar/Server	*FQDN*	Configure the Orange aSBC FQDN
Outbound Proxy -> **Port**	Port * 5061 Auto discovery	Uncheck checkbox "Auto discovery"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

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

After completing the "**General**" tab, proceed to the "**Options**" tab.

The "**Options**" tab allows you to customize various settings for your SIP trunk. At the top, you can set the limit for the **number of simultaneous calls per trunk**, with the default set to **10**. Make sure to check the boxes for "**Allow inbound calls**" and "**Allow outbound calls**" to enable both directions. Next, under "**Transport Protocol**," select "**TLS**," and for "**IP Mode**," choose "**IPv4.**" In the "**Certificate**" field, upload the *Orange SBC Root Certificate* file. After upload of the certificate, it will automatically change name for: **"root_cert_10000.pem**" to ensure secure communication. Set the "**SRTP Mode**" to "**Enforced**" for encrypted media, and in **"Re-Register timeout**," enter **180 seconds** to define how often the trunk re-registers with the server. For "**Select which IP to use in 'Contact' (SIP) and 'Connection' (SDP) fields**," choose "**Use Default Settings**." Make sure to check "**Include diversion header support**" to support caller ID diversion headers. Finally, under "**Codec priority**," click "+ **Add**" to include codecs, and set the priority order. In BTol/ BTIPol the "PCMA" codec is selected as the highest priority codec.

Once all fields are filled correctly, click "Save" to apply the configuration.

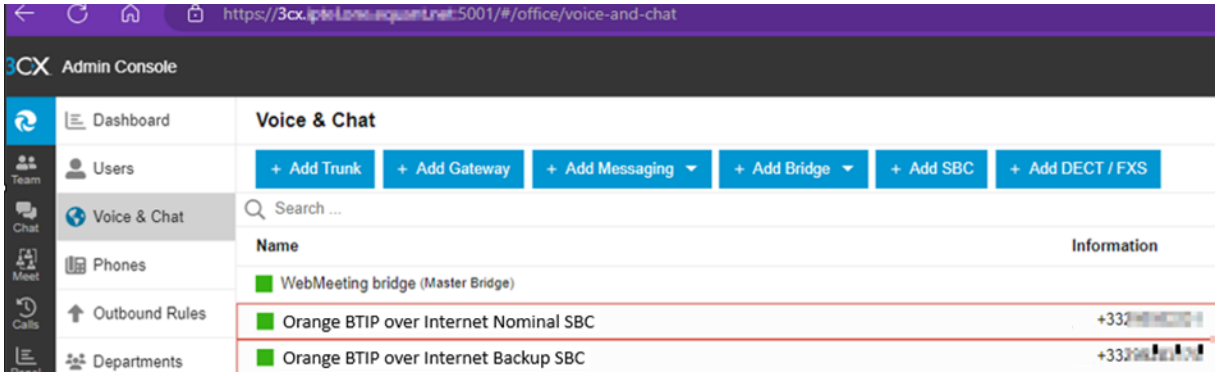


The next tab **Options:**

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	

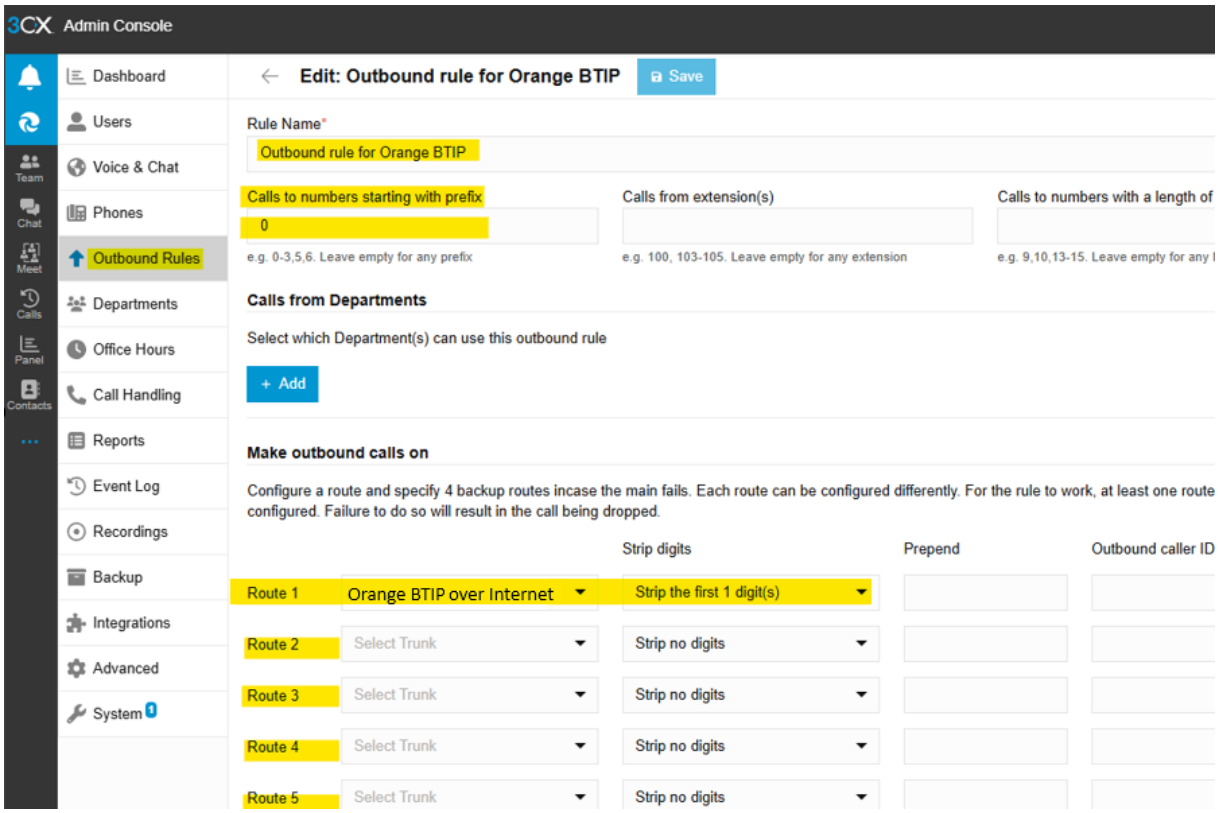
The created SIP Trunk is listed under **Voice & Chat.**



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

6.1.1 Outbound Rules configuration

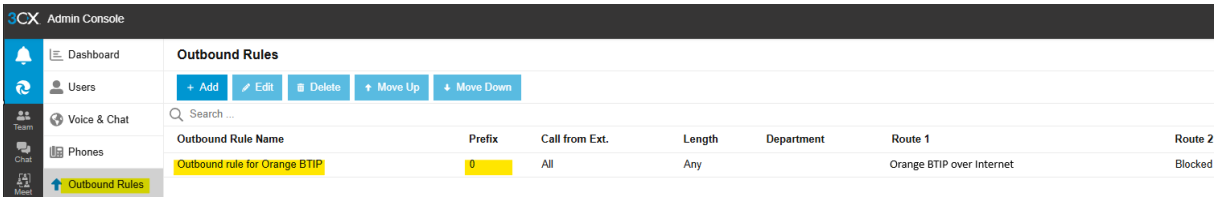
For 3CX v 20 add Outbound Rules, prioritizing the Route order, according to customer preferences.



Parameter	Value	Comment
Rule Name	*BTIP/BTalk Outgoing*	Choose relevant rule name
Calls to numbers starting with prefix	0	Select relevant prefix (e.g. leading 0)
Route [1-5]	*BTIP/BTalk SIP trunk*	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.



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 file generation using OpenSSL tool:

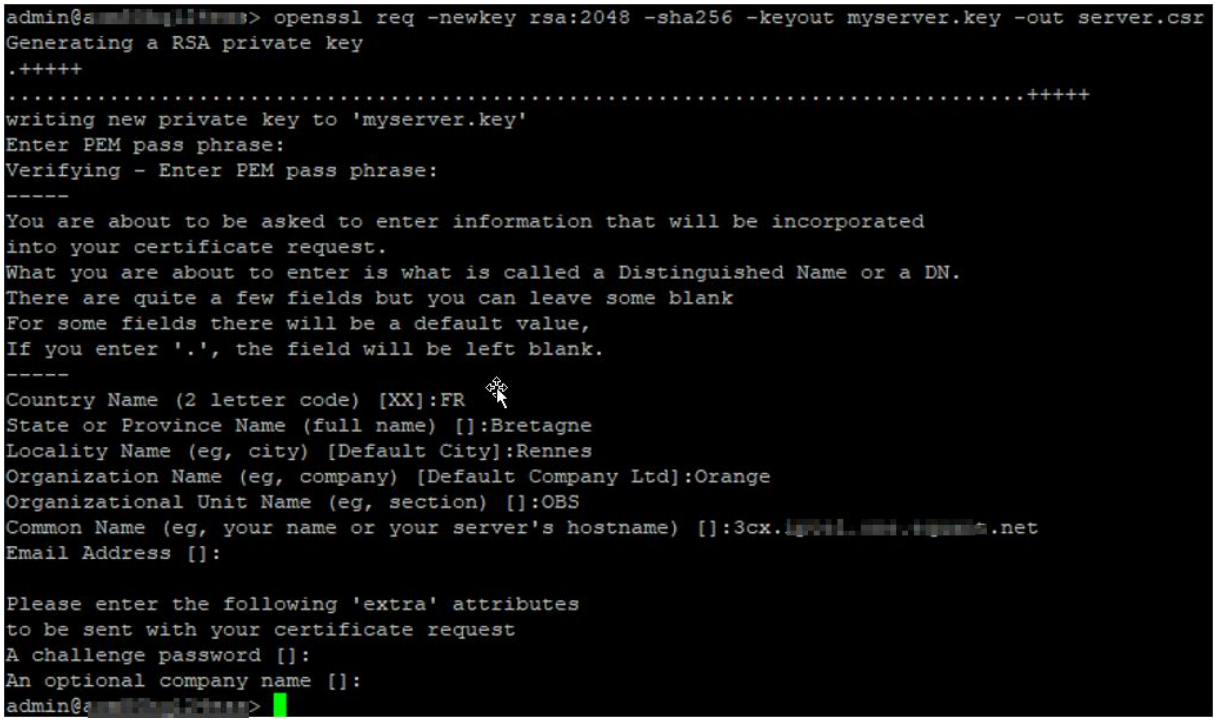
The OpenSSL command below will generate a 2048-bit RSA private key and CSR:
openssl req -newkey rsa:2048 -sha256 -keyout myserver.key -out server.csr
Let's break the command down:

- *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.



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:

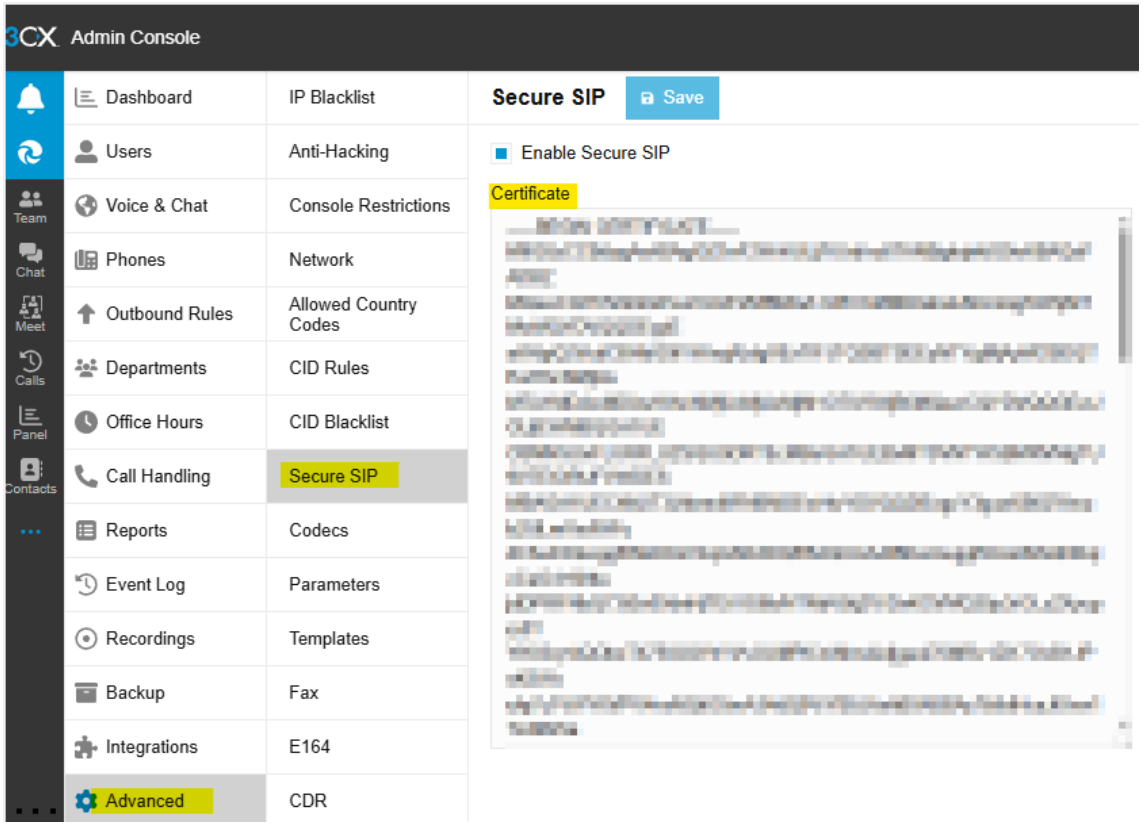
Parameter	Value	Comment
Security – Secure SIP – Secure SIP TLS	checked	Select checkbox
Security – Secure SIP	Certificate	Paste 3CX PBX identity certificate
Security – Secure SIP	Private Key	Paste decrypted 3CX PBX private key

6.5 Public Certificate Authority renewal

When certificate is about to expire it must be renewed.

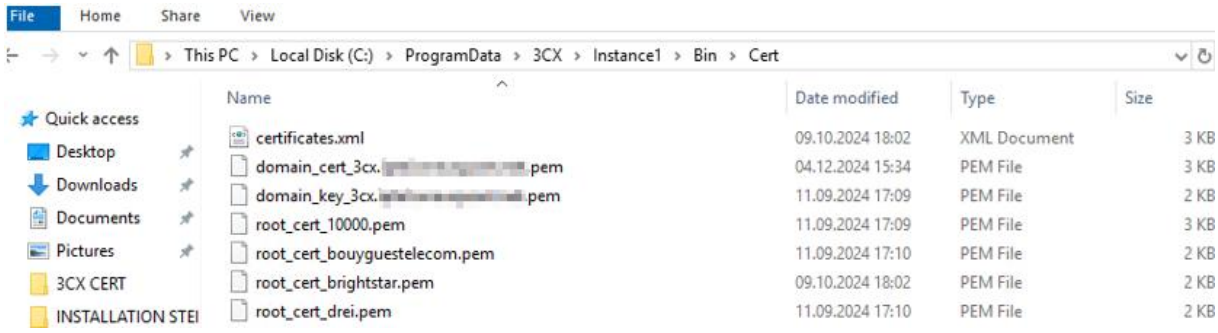
The new identity certificate from Public Certificate Authority need to be uploaded to 3CX via web.

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

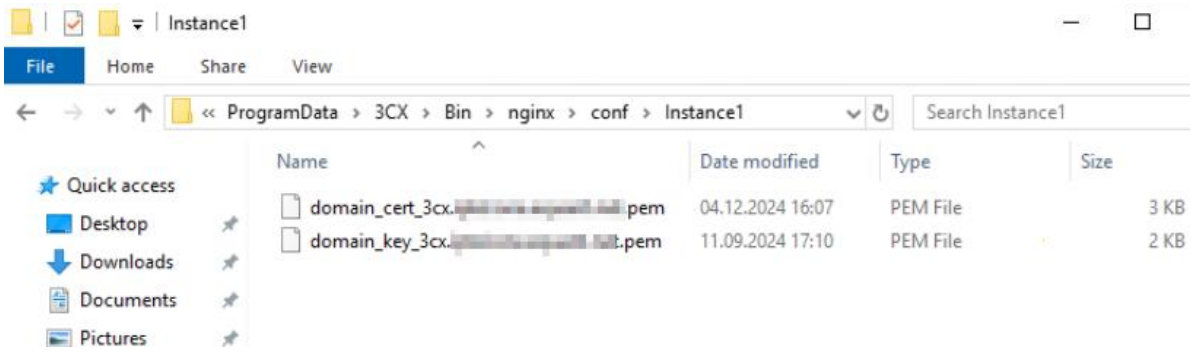


For Windows the SIP Server Certificates for the SIP Trunk are stored here: *C:\ProgramData\3CX\Instance1\Bin\Cert*

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.



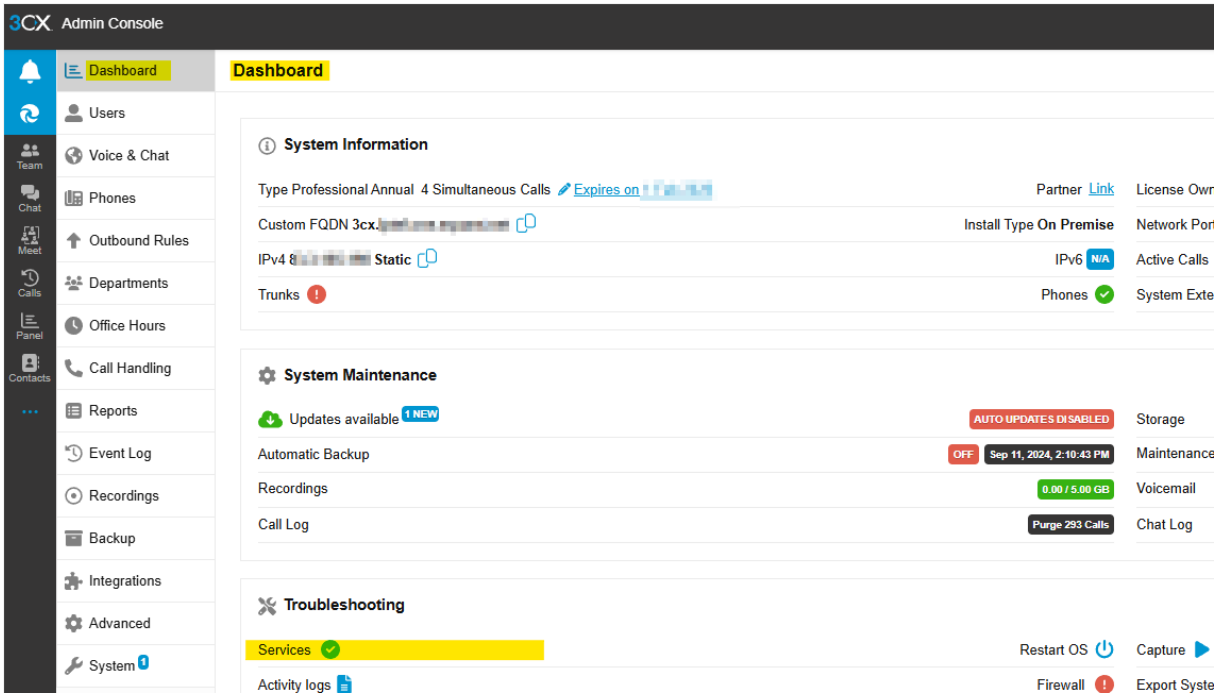
For Windows the Nginx Certificates are stored here: *C:\ProgramData\3CX\Bin\nginx\conf\Instance1*



This certificate is needed to access 3CX web management.

Replace the ***domain_cert_****FQDN.pem* and restart the Nginx and SIP services.

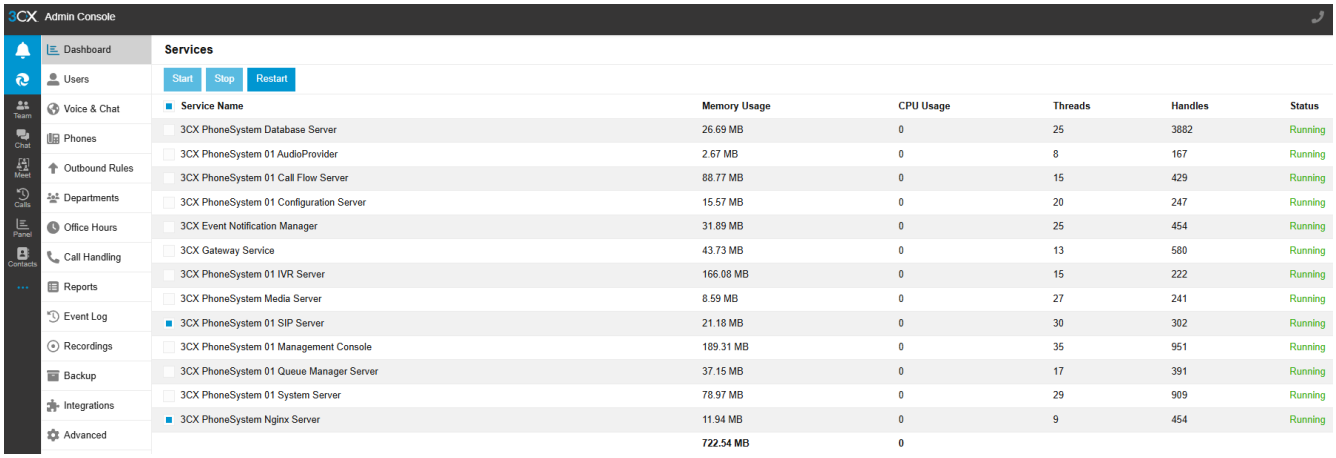
To restart 3CX Services go to **3CX** --> **Dashboard** --> form section Troubleshooting chose the **Services:**



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:



Glossary

- BVPN : Business Virtual Private Network (Orange Business MPLS network)
- BTIP : Business Talk IP (France) over BVPN
- BTalk : Business Talk (International) over BVPN
- BTIPoI : Business Talk IP over Internet (France)
- BToI : 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.