



**ZULTYS**  
 INNOVATE | COMMUNICATE | COLLABORATE

# BRISNORTH COMMUNICATIONS

## ZULTYS-IVOX ITSP INTEROPERABILITY DOCUMENT

This document is produced in good faith by Brisnorth Communications (Zultys Authorised Dealers) for the mutual benefit of the Zultys and iVox Dealer Channels. The examples shown below are based on actual site commissioning of iVox SIP Trunks. Users of this document must accept that the information is provided in good faith, and that neither Brisnorth Communications nor Zultys Inc, nor iVox, nor any of their agents are responsible for any acts, omissions or causes as a result of using this document. Any errors or amendments should be emailed to [support@brisnorth.com.au](mailto:support@brisnorth.com.au). Your revision will be incorporated and you will receive by return an updated version.

### IVOX SIP TRUNKS

#### IVOX CONFIGURATION

- 1.1 SERVICE ACTIVATION/DELIVERY..... 2
- 1.2 IVOX PARAMETERS..... 2

#### ZULTYS CONFIGURATION

- 2.1 CREATE ITSP ACCOUNT..... 3
- 2.2 CONFIGURE CODECS..... 4
- 2.3 CREATE DIAL PLAN ..... 5
- 2.4 SET SYSTEM MAIN PHONE NUMBER ..... 5
- 2.5 TESTING WITH A USER/DEVICE ON MX SYSTEM..... 6
- 2.6 MULTIPLE ITSP CONNECTIONS TO A SINGLE MX ..... 6

#### NUMBER PORTING & CUTOVERS

- 3.1 HOW TO PORT CUSTOMERS EXISTING NUMBERS..... 7
- 3.2 “OVERSTAMPING” OF NUMBERS..... 7
- 3.3 ADVANCE “CUT-OVER” PRIOR TO PORTING..... 7

#### EXCEPTIONS

- 4.1 TELSTRA “VOIP” MODEMS..... 7



## iVox CONFIGURATION

### 1.1 SERVICE ACTIVATION/DELIVERY

The iVox Dealer will have created a Customer Account in iVox's "NICE" Billing Platform

To this account, the Dealer will have assigned as many endpoints (DIDs) as the Customer has ordered.

Value (per Type)	Value (per Type)	Net Elem	Type	Status	Sub#	Description	Belongs To
61731237398	TITB09CL	IIVOIP	A Party	Active	10000		Brisnorth Commander Pty Ltd
61731237399	41827516	IIVOIP	A Party	Active	10000		Brisnorth Commander Pty Ltd

The first Column titled "Value(perType)" gives the endpoint/DID numbers and is given in International format; however **when deploying in the field one should use FNN format , that is 0731237399 , not 61731237399**

The 2nd Column strangely also titled "Value(perType)" gives the password for that endpoint. It may be AlphaNumeric or purely numeric, or even blank (often the case where you port-in a 100-number range) . By default the passwords are numeric, you may request Alphanumeric from the ITSP. However, this is academic as **you will not be authenticating with password, but with the Customers static IP address instead.**

Initially, all iVox endpoints are set to Authenticate with the password shown in the Endpoint Configuration. However, it is always preferable from a Security and a convenience point of view to request that iVox change Authentication so that the Endpoint **authenticates with the Customer's Static IP address**, rather than a password which might be useable elsewhere if compromised.



Send an email to [support@ivox.com.au](mailto:support@ivox.com.au) and request that Endpoints (FNNs) for Customer (Name) be Authenticated on IP address (xxx.xxx.xxx.xxx) You will usually receive a response within 15minutes that the request has been actioned.

### 1.2 iVox PARAMETERS

- Proxy Server: sip.ivox.net.au **OR 202.83.183.33**
- Proxy Server port: 5060 (or 5061 , 5062 etc if there are more devices/lines)
- Registration interval: 240sec
- Codecs supported are G.729 & G.711
- Packet rate is 20ms
- Support for DTMF out-of-band using RFC2833, payload 101
- SIP Auth: e.g. 0282520000

Prior to setting up the SIP-Trunks, you should ensure that the following Firewall ports have been forwarded; **Because your MX authenticates on IP-address instead of password**, you will need to set port-forwarding on your firewall for "All/Any external IP" to forward all UDP packets to the **FIXED –IP** address of the MX.

If the firewall/Manager does not allow All/Any IP access, you may instead open to traffic from **202.83.183.33** UDP to device IP-address (for SIP) and open traffic from **27.34.224.0-255** UDP to device IP-address (for RTP)

**NB : If modem/Router has SIP-ALG, this should be disabled.** Also, see Paragraph 4.1 for anomallies encountered when the Modem/Router is a Telstra-provisioned "VoIP modem".

It is best to have a standard document (as shown below) to give to the Customers' IT-Manager :

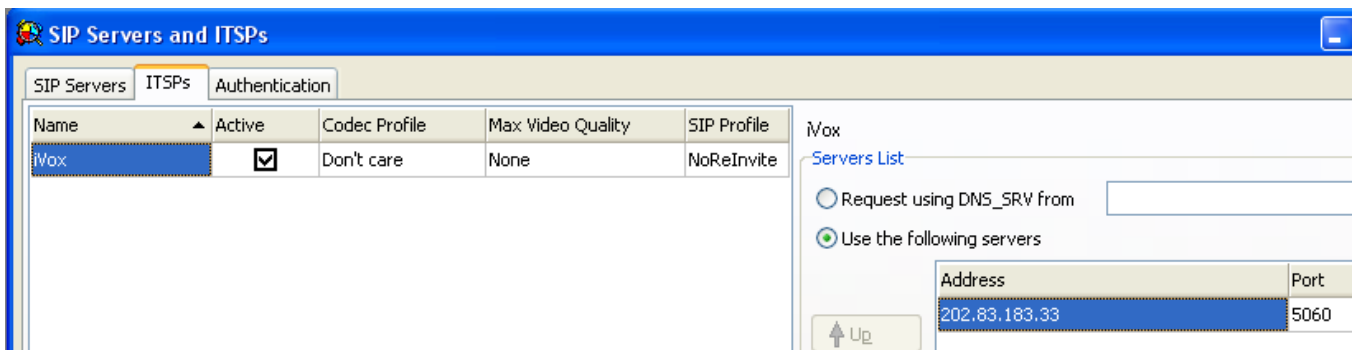
Please ask your IT Manager to port forward the described ports on your Router (Firewall options) to the addresses given. [Note ALG should be disabled] If you do not have an IT Manager, please advise us, and we can provide a Support Consultant (you will need divulge the User Login & Password in this case)				
Firewall Ports used by ZULTYS VoIP system				
Port No.	Type	Direction	Description/Purpose	Point to IP address
5060 - 5066	UDP	bothway	VoIP & SIP	192.168.____.____ (the Zultys)
20,000-21,239	UDP	bothway	RTP for SIP	192.168.____.____ (the Zultys)
7100-7167	TCP	in	MX remote admin	192.168.____.____ (the Zultys)
7505	TCP	bothway	MXIE and Mxadmin	192.168.____.____ (the Zultys)

## **ZULTYS CONFIGURATION**

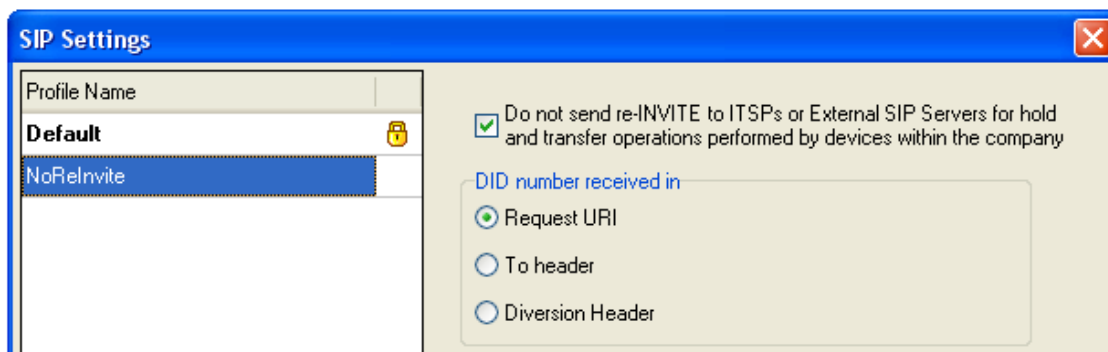
(This Document is produced with reference to Zultys Version 9.0.4)

### **2.1 CREATE ITSP ACCOUNT**

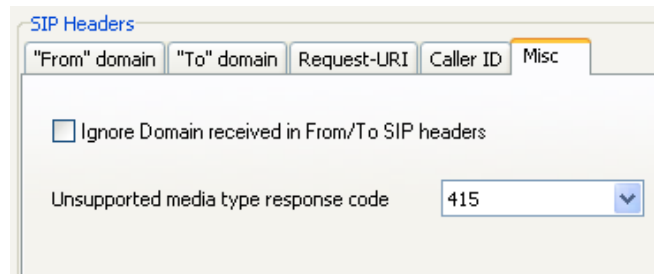
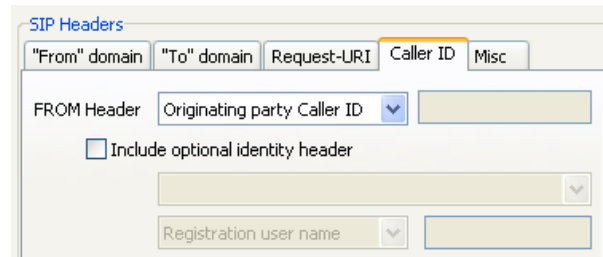
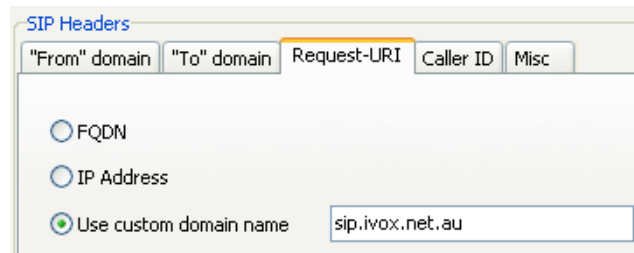
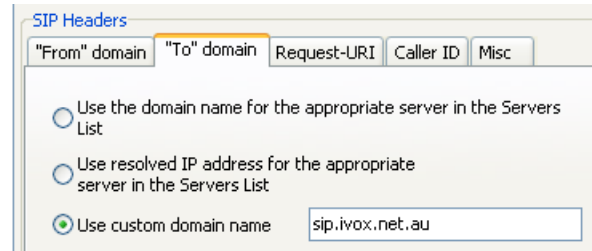
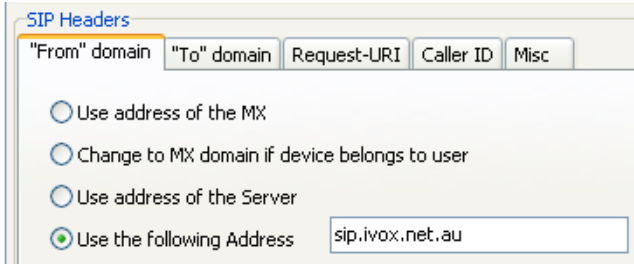
In MX-Admin : Provision > Sip Server and ITSP create "iVox" ITSP with the server address **202.83.183.33** :



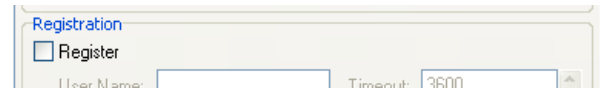
Create a SIP Profile called "NoReInvite", and assign it to that account:



Then set your SIP-Header info as follows:

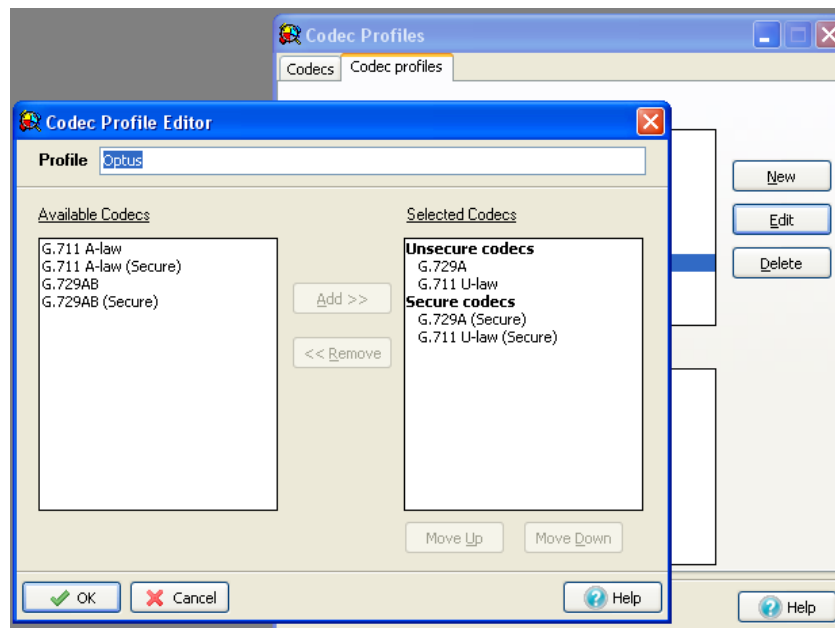


**NOTE: Registration/Authentication is NOT REQUIRED when Authenticating with IP - leave this unticked/blank**



## 2.2 CONFIGURE CODECS

Typically use the Zultys default “Don’t Care” for Codec, which will allow the MX to negotiate with iVox:



Alternatively, select “Voice Quality” from the drop-down choices.

### 2.3 CREATE A (TEST) DIAL PLAN

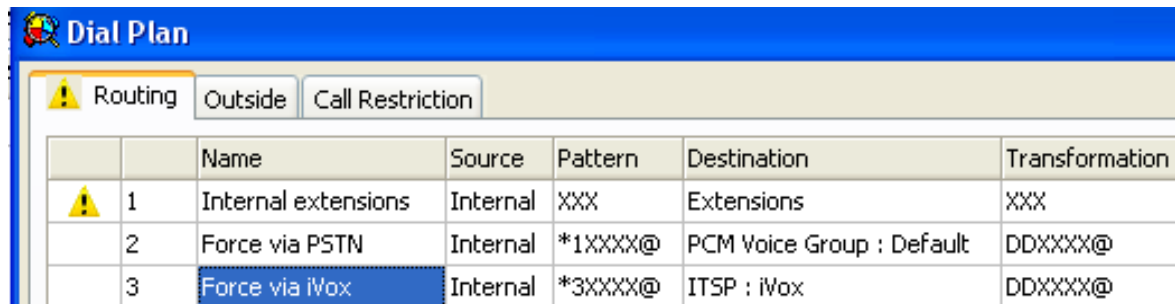
In MX-Admin :

Configure > Dial Plan > Routing, and right-click to add/create a new plan for External :

Ultimately, post-commissioning, you will create a Dial-plan that looks like this:

External	Internal	XXXX@	ITSP : iVox	XXXX@
			PCM Voice Group : Default	XXXX@

But for testing purposes, so as not to interfere with a Live/Production system call routing, create a TEST prefixed Dial Plan something like this : (example shows prefix \*3 used for Route called “Force via iVox”)



	Name	Source	Pattern	Destination	Transformation
1	Internal extensions	Internal	XXX	Extensions	XXX
2	Force via PSTN	Internal	*1XXXX@	PCM Voice Group : Default	DDXXXX@
3	Force via iVox	Internal	*3XXXX@	ITSP : iVox	DDXXXX@

Place the TEST Dial-Plan at the top of the dial plan table below Extensions , MXfax etc . Now you will be able to force calls out via the test-route using a prefix of \*3 in front of any number you dial. All other calls will progress as normal.

Tip : It is a good idea to create “Force Codes” for each route as shown above; That way if there is a problem with routing, you can always ask the customer to make test calls with prefix “\*1” and/or “\*3” to establish if the problem lies with the route selected.



### 2.4 SET SYSTEM MAIN PHONE NUMBER

iVox signaling will check the CallerID of the call sent from the MX to ensure that it matches the numbers allocated to the Customers endpoints/DIDs . If the CND is not within Service Number Range, the call will fail. The Caller ID is contained in the SIP-header packet, and the MX takes this from the field “Main Phone Number” in the Company info under System Settings.

!! Be sure that your test user’s account has a Caller-ID that is of the number-range as described in Para 1.1 above :

In MX-Admin > Provision>System Settings>Company

Main phone number	0734121200
-------------------	------------

If the Customer is using DIDs assigned to users, you will still need to programme the iVox endpoint FNN number into the MX’s System Settings so that it is presented in the SIP-header for Authentication.

## 2.5 TESTING WITH A USER/DEVICE ON MX SYSTEM



MX's built-in SIP-Trace Call Monitor can be used to diagnose any issues with SIP-call progress.

iVox's Support Staff are amongst the most knowledgeable and highly responsive in the Industry; Indeed experience has established that compared to other ITSPs, iVox's Dealer Support is unsurpassed.

If you have not managed to diagnose problems yourself using the MX's Call Monitor, or if you wish to confirm that your diagnosis correlates to what is seen at the ITSP end -

**For Tech Support, call iVox Support on 02 8252 0205**

## 2.6 MULTIPLE ITSP CONNECTIONS TO A SINGLE MX

Zultys MX allows for multiple ITSPs where the ITSPs authenticate based on PASSWORD Authentication. However, only one IP-Authenticated ITSP can be deployed (MX V9.0.4 and below), as the identifier used in the SIP-Header is taken from the Customers' "Main Phone Number" setting under Provision|System Settings| Company info.

An example of Multiple ITSP config is shown below:

The screenshot shows the 'SIP Servers and ITSPs' configuration window. The 'ITSPs' tab is active, displaying a table of ITSP configurations:

Name	Active	Codec Profile	Max Video Quality	SIP Profile
iVox	<input checked="" type="checkbox"/>	Voice Quality	None	NoReInvite
VoIPstunt	<input checked="" type="checkbox"/>	Voice Quality	None	NoReInvite
ClubTelco	<input checked="" type="checkbox"/>	Low Bandwidth	None	NoReInvite

Below the table, the 'VoIPstunt' configuration is detailed:

- Servers List:**  Request using DNS\_SRV from [ ]  Use the following servers
- Address/Port Table:**

Address	Port
77.72.169.134	5060
- Registration:**  Register
- User Name: dontTRYthis Timeout: 3600
- Force Symmetric NAT Traversal: Auto
- Send OPTIONS to refresh connection through NAT every 30 sec.

The screenshot shows the 'SIP Servers and ITSPs' configuration window with the 'Authentication' tab active. It displays a table of authentication settings:

Realm	User Name	Password
sip.voipstunt.com	XXXXXXXXXX	*****
192.168.1.1	GSM	*****
stratus.com	XXXXXXXXXX	*****

### 3.1 HOW TO PORT CUSTOMERS EXISTING NUMBERS

Almost any Geographical number may be ported to iVox services (including 1300s and 1800s). Customer will be required to fill in the “Porting” Form and submit copy of their current bill, evidencing that they are the owners of those numbers. Once the form has been submitted by the Dealer to iVox, iVox will confirm category of port (simple port =Cat.A , complex port= Cat.C) Thereafter iVox will set a date and time for the porting of the number/s to their services.

### 3.2 OVERSTAMPING OF NUMBERS

“Overstamping” of a VoIP carrier’s CallerID with their PSTN CallerID was common practice amongst ITSPs in the past; However, Australian Authorities no longer allow this. The exception to this being made only when numbers are being ported to another Service Provider.

### 3.3 ADVANCE “CUT-OVER” PRIOR TO PORTING

Usually, when porting, there is an Outage time when the Technician on site has to cut-over from the loosing Carrier to the new Carrier. A lot of the anxiety can be avoided and the entire process can be completed **WITH NO SERVICE OUTAGE WHATSOEVER** if the following simple steps are followed:

- Provide the Customer with a temporary endpoint from your Pool of endpoints in iVox NICE.
- Get the endpoint working as described in the purpose of this document. Test it inbound and outbound
- Whereas the numbers are Porting, you may request overstamping of the CallerID from iVox
- Then, as you already have the SIP-Trunks in-place and working, and overstamped, and you have set the Dial Plan to route outbound to iVox in its Pattern/Route; it is as if the customer has already ported in their experience of the Phone System. Their outbound calls commence tolling with you/iVox.
- All that happens then at time of Porting is that incoming calls flick seamlessly from one Carrier to the other; As both inbound connections are already established, nothing needs to be done. If porting a 100-number range, all DID’s, AA’s etc function just as they normally would.

**Post-port, it is wise to test that the numbers have fully ported and are mapped by other carriers; Use other Carriers to make inbound calls to check.**

## EXCEPTIONS

### 4.1 TELSTRA “VOIP” MODEMS

Telstra “VoIP” modems can be identified by the “Phone” or FXS ports on the device that are used to plug in an analogue phone (i.e. the modem has built-in Analogue Terminal Adaptor)

Field experience with various models of Telstra “VoIP” modems has demonstrated that the firewall ports used for VoIP (UDP:5060) typically are commandeered by the proprietary firmware that Telstra install: Thus you may find that regardless of any firewall port-forwarding rule you may create, the modem still will not pass port 5060 to anything other than its own internal FXS ports.

The solution in this case is to replace the modem, or if that is not an option, request that iVox change UDP port from 5060 to, say, 5070. Ensure you change your ITSP and SBC settings to match !