nexVortex Setup Guide

ASTERISK

September 2015

510 SPRING STREET | HERNDON VA 20170 | +1 855.639.8888

Table of Contents

1 Introduction

1. This document is intended only for nexVortex customers and resellers as an aid to setting up the Asterisk PBX software to connect to the nexVortex Business Grade SIP Trunking Service. Please reference the nexVortex SIP Trunking Implementation and Planning Guide at http://www.nexvortex.com/pdf_files/nexVortex-Implementation-Guide.pdf for additional information. Further Asterisk information can also be found at http://asterisk.org

Further help may be obtained by emailing at support@nexvortex.com.

If you find any errors in this document or have any suggestions, please email us at support@nexvortex.com so that we can make updates to this document.

> **Important! DNS Address**
>
> A specific DNS address was provided in the Account Set Up email you received the day you opened your account. Your Authentication User ID and password are also in this email. If you need assistance locating this information, please contact at support@nexvortex.com.
>
> Note: For all instructions throughout this Guide, you must substitute the provided DNS address wherever xx.xx.xxx.xxx is referenced.

Proxy Servers

To connect to the nexVortex network, you will need to add our proxy address into your phone system or device. The address of our proxy server will be a fully qualified domain name (FQDN). It was automatically sent to you when your account was setup. If you no longer have this information or would like us to issue a new proxy key, please contact us at support@nexvortex.com.

Note: If your system does not support a fully qualified domain name format, please contact our technical support team at support@nexvortex.com for a list of valid IP addresses for your account.

Special Characters

Please note that special characters should not be used anywhere in SIP configurations. These include, but are not limited to, @#$%&! and spaces.

2 Step 1: Trunk Configuration

Inbound service – You may receive SIP signaling from nexVortex from any of the following IP addresses:

- 66.23.129.253
- 66.23.138.162
- 66.23.190.100
- 66.23.190.200
- 209.193.79.80

If you need additional assistance ensuring your local PBX configuration meets this requirement, please contact technical support for Asterisk directly.

Outbound service – The most efficient way to ensure redundancy for outbound calling is to utilize DNS SRV for routing traffic to nexVortex. At present, if your PBX supports DNS SRV, pointing to 'nexvortex.com' as your Proxy IP address is all that should be necessary to ensure outbound redundancy.

If your PBX does not support DNS SRV, hopefully it supports configuration of multiple outbound proxies. In this case, you must configure two trunks in order to be redundant across the nexVortex service. The two proxy IP addresses are px5.nexvortex.com and px1.nexvortex.com. If you need additional assistance with DNS SRV or configuring multiple outbound proxy IPs on your PBX, please contact technical support for Asterisk directly.

3 Step 2: Trunk Settings

Your trunks MUST be configured to present your provisioned E911 number(s), (i.e. the E911 settings you created for your account at nexVortex.com) for Emergency calls (911) or emergency TEST calls (311 or 933). Either a proper FROM or P-Asserted-Identity (preferred) header containing your provisioned Emergency number, if you require additional information, please contact our technical support team at support@nexvortex.com

In order to provide the highest level of service availability possible, nexVortex utilizes an n+1 architectural model for our call processing. You will need to ensure that your network edge (router and/or firewall) is configured to accommodate this architecture.

You may receive SIP signaling from nexVortex from any of the following IP addresses:

- 66.23.129.253
- 66.23.138.162
- 66.23.190.100
- 66.23.190.200
- 209.193.79.80

You must ensure that each of these IPs are allowed to pass UDP 5060 traffic into your network and that this traffic is port-forwarded (if necessary) to the internal IP of your PBX.

You will also need to open the RTP or audio ports. This is different for each customer premise device. Please reference Asterisk for this detail. Your edge device must be configured to allow inbound RTP traffic on this port range from ALL IP addresses.

4 Best Practices

SIP, unfortunately, is a high-value target for hackers. There are a few things you should do to ensure that your PBX installation is secure and well protected against the normal attack vectors for this technology.

4.1 Security

4.1.1 PBX Extensions

If your PBX is configured to allow external extensions (outside the private LAN), then you must configure your extensions with strong passwords. Password extensions should NEVER be the same as the extension number itself.

4.1.2 GUI Access

If your PBX is configurable via a web browser GUI, it should NOT be accessible via a public IP. If you MUST make changes to your PBX configuration from outside your network, you should only enable remote access while you are working on the configuration and then immediately remove access when your updates are complete.

4.1.3 Access Lists

If your PBX supports access lists for IP authorization, these should be extremely conservative. Allowing unauthorized users to place calls through your network is a good way to rack up thousands of dollars in fraudulent charges if someone identifies this weakness in your configuration.

4.1.4 Dialplan Restrictions

An effective way to keep unauthorized users from using your PBX to place fraudulent calls is to restrict your dialplan. If you do not make International calls, do not allow users to dial 011 as their first three digits. If you do make International calls, consider restricting allowable dial strings to only the country codes to which you place calls.

Don't forget to protect your dialplan against Caribbean dialing (Check here for Caribbean area codes http://www.everythinglongdistance.com/caribbean-area-codes.htm).

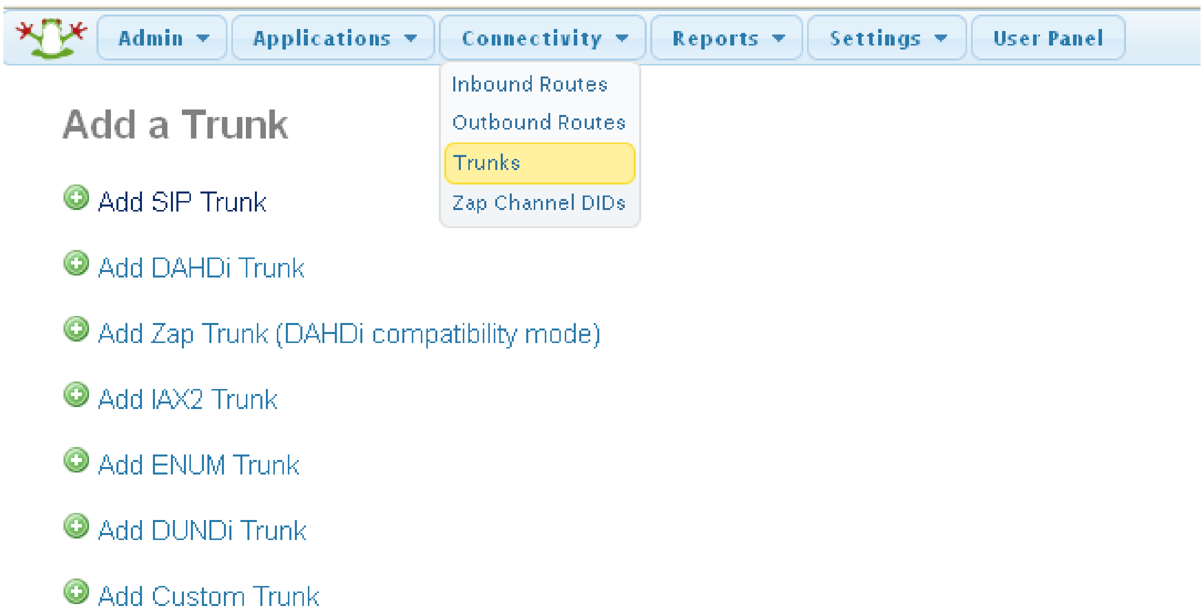
4.2 IVR

IVRs should always be configured to utilize a timeout-based call disconnect rule. Failure to do so could result in long calls of up to, or exceeding, 24 hours. By configuring automatic disconnects into your IVRs, you will ensure that you do not pay excessive usage fees for these types of calls.

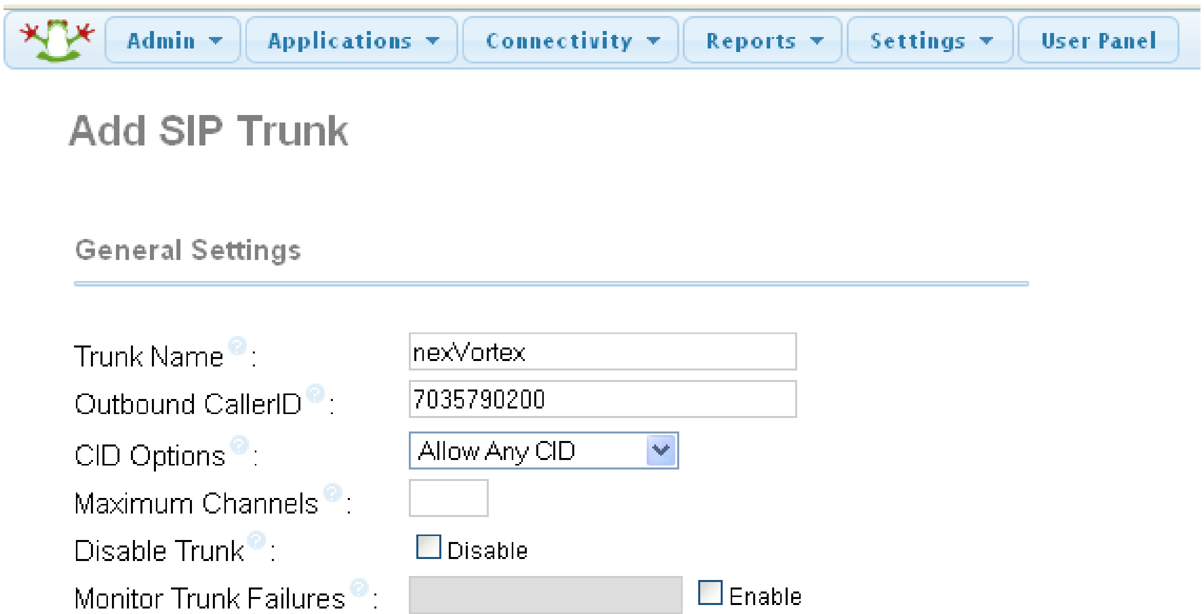
5 Asterisk Set up Instructions

Trunk Configuration

You will need to add **TWO** trunks to ensure that your PBX is configured for redundancy (both to accept inbound calls from multiple nexVortex nodes, but also to attempt multiple nexVortex nodes on outbound calling).

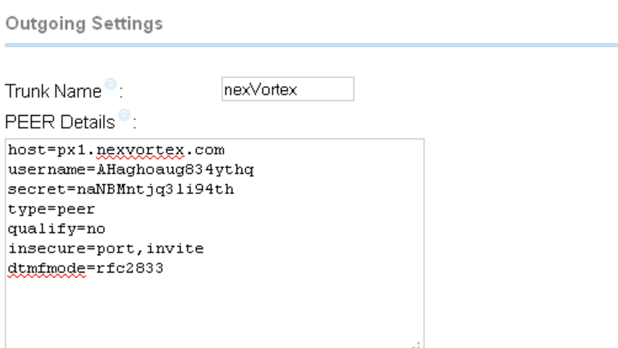


Click Add Sip Trunk to create your first nexVortex trunk.



If you need to allow 7-digit dialing, your dial pattern should include an entry like this (this example assumes your local area code is 608):

Your Peer Configuration should look similar to this for 'Outgoing Settings' (Your username and password should be replaced with the credentials that you received in your Setup Email).



Your USER configuration should look similar to this for ‘Incoming Settings’:

Incoming Settings

USER Context : from-trunk

USER Details :

```
type=user
context=from-trunk
qualify=no
insecure=port,invite
host=your.local.ip.com
```

Now, create your 2nd trunk using almost identical settings. The only thing that changes here is the host IP in your Peer Details and the name of your trunk.

Outgoing Settings

Trunk Name : nexVortex2

PEER Details :

```
host=px5.nexvortex.com
username=bl3f2487ogtabqe
secret=nablidubfvlq3wi4u
type=peer
qualify=no
insecure=port,invite
dtmfmode=rfc2833
```

Your User Configuration is identical to those of the 1st trunk you created.

Incoming Settings

USER Context : from-trunk

USER Details :

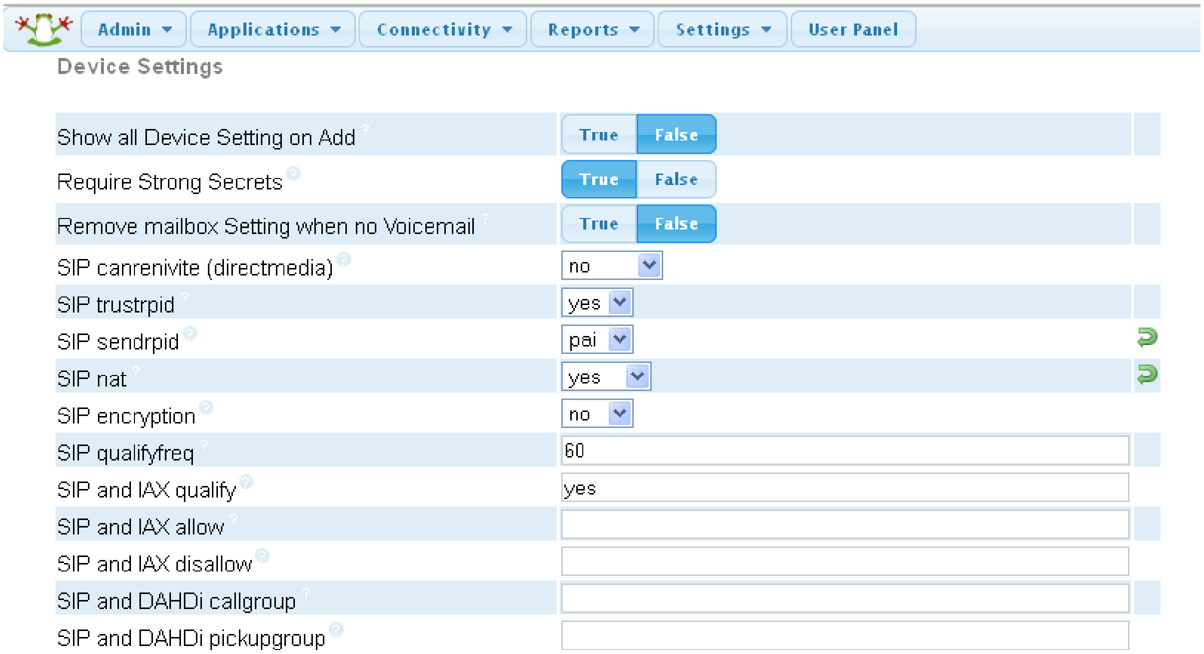
```
type=user
context=from-trunk
qualify=no
insecure=port,invite
host=your.local.ip.com
```

After you submit changes, you will need to click the ‘Apply Config’ button to implement your changes into the active configuration.

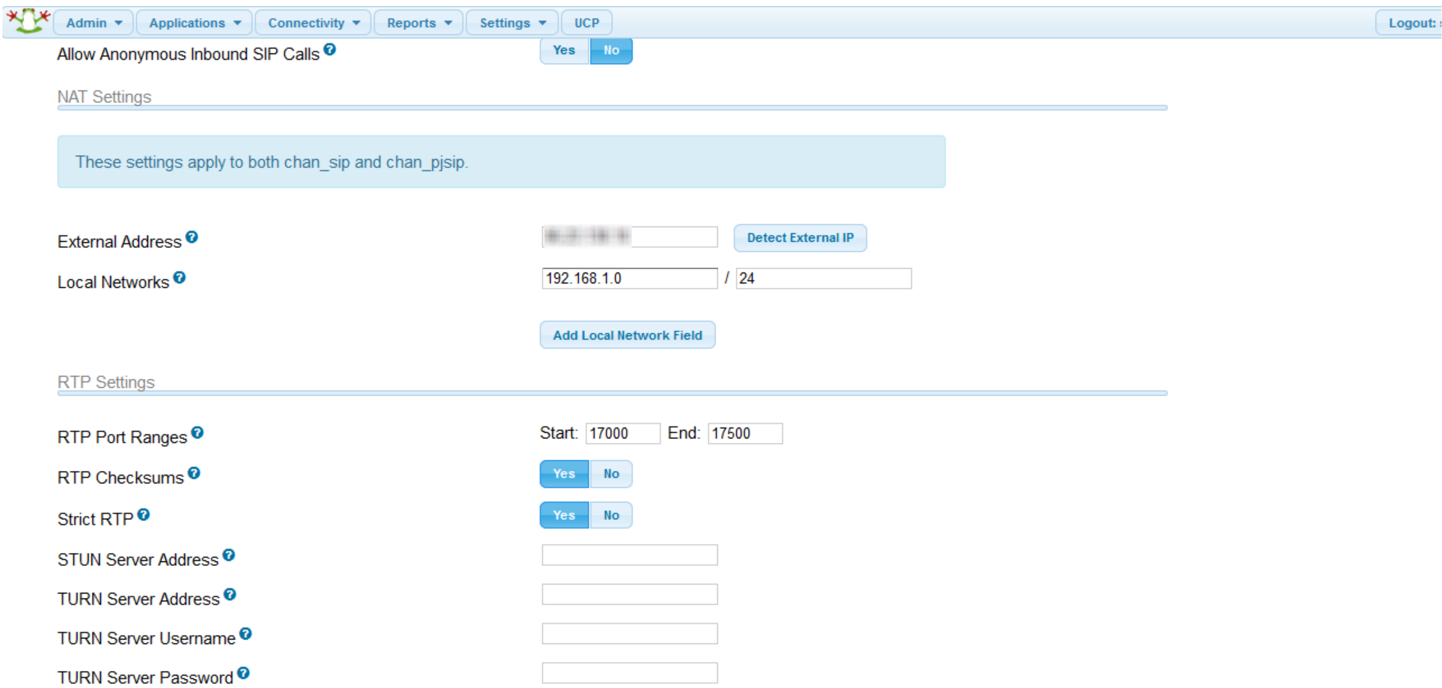
Admin ▾ | Applications ▾ | Connectivity ▾ | Reports ▾ | Settings ▾ | User Panel | **Apply Config**

Trunk Settings

Update your Advanced Settings to utilize RPID (Remote-Party-ID), PAI (P-Asserted-Identity), and SIP nat:



Under the Settings Tab, Select Asterisk SIP Settings to configure NAT for your installation.



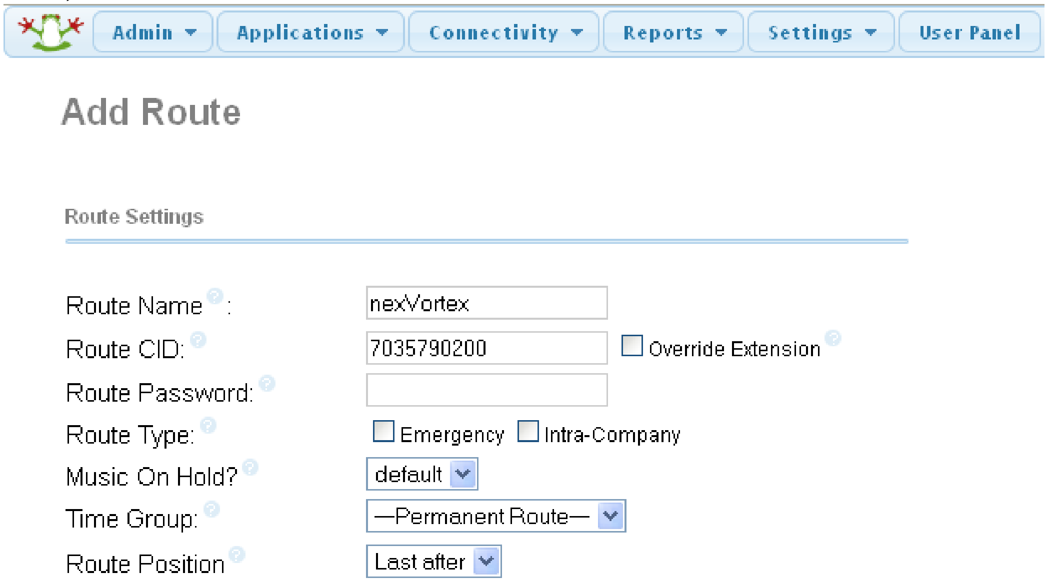
First, update ‘External address’ by entering your static PUBLIC P address (be sure to modify ‘Local Networks’ to reflect your actual local LAN):

If you are using dyndns for your public IP, your ‘External Address’ entry would look something like ‘mydomain.dyndns.org’ (of course, this would be your actualy DynDNS name)

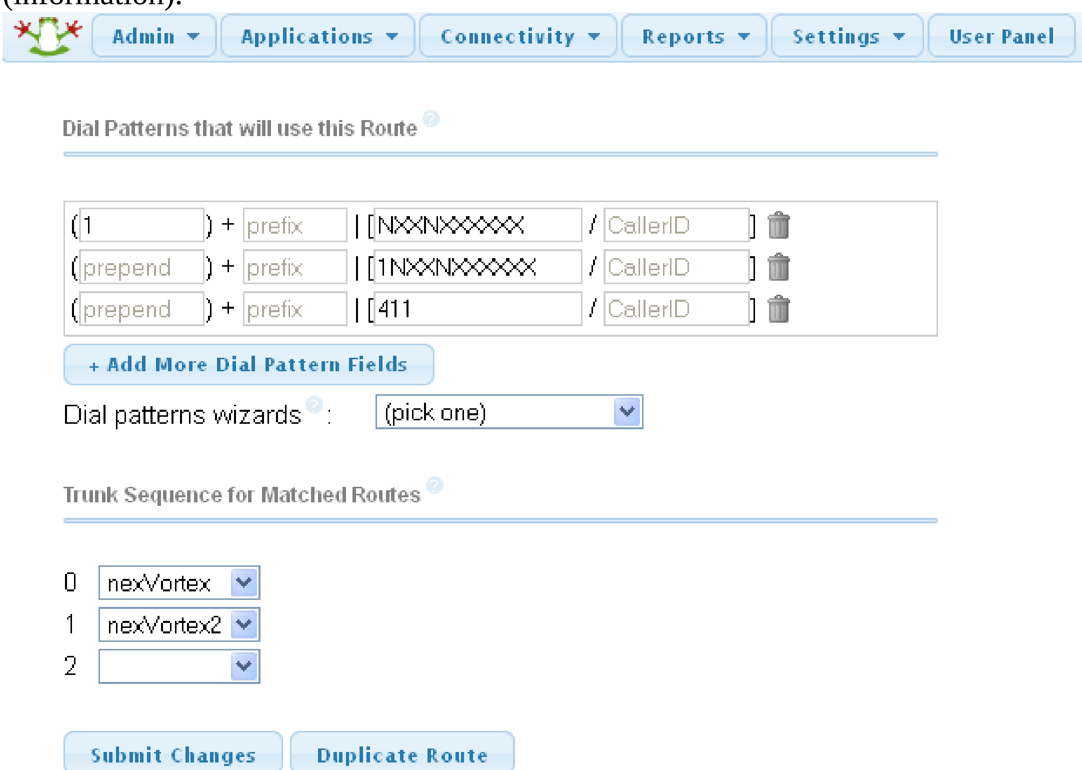
Now, modify the RTP Port Ranges from the default values of 10000-20000. This is a huge port range that is likely not necessary. You will generally need no more than 1 port for every simultaneous call you expect to carry (then, double it to be safe!). Using the screenshot above as a guide, this configuration would allow 501 RTP ports (thus, allowing for up to 501 simultaneous calls).

MAKE SURE YOUR FIREWALL CONFIGURATION ALLOWS THESE UDP PORTS and, if necessary, port-forward them to your Asterisk’s private IP address.

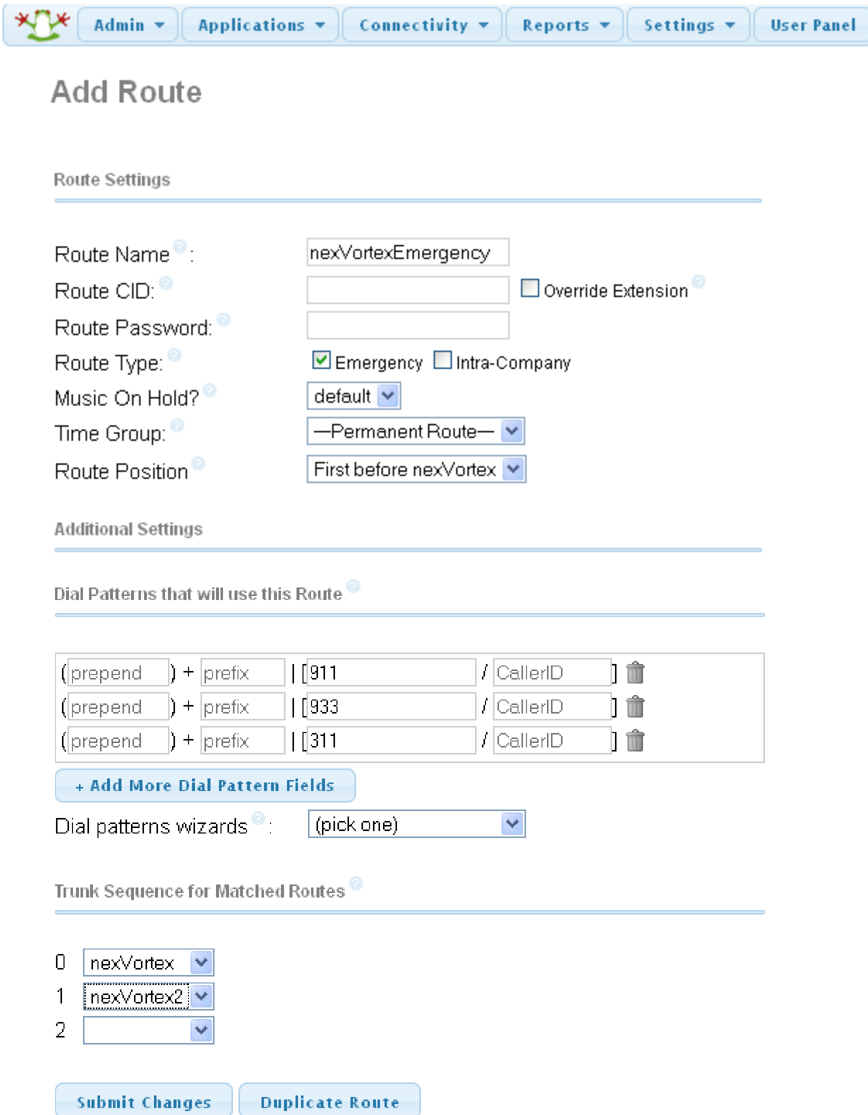
Now, we need to create an outbound route:



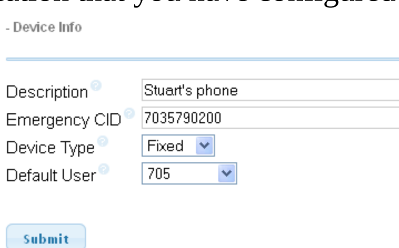
The dialplan examples included here show both 10 and 11-digit dialing, as well as 411 (information).



Now, create another outbound route for Emergency calling. Emergency calling includes 911 (actual emergency calls) and 311/933 for emergency call testing. YOU SHOULD ALWAYS VERIFY YOUR 911 CONFIGURATION BY DIALING 311 OR 933 BEFORE CALLING 911:



Every extension (or Device, depending on how you configure your end-users) configured should also include an Emergency CID configuration. This MUST match an existing E911 location that you have configured via your account at nexVortex.com:



6 Troubleshooting

Following are troubleshooting steps which you can follow:

6.1 Customer System will not register with nexVortex:

- Check the system is pointing at our registrar domain (reg.nexvortex.com)
- Check UDP port 5060 is open on the firewall
- Check NAT translation is correct between LAN private IP address and public IP address
- Check you have the correct proxy user name and password configured.

6.2 Customer System cannot make a call:

- Check that the system is pointing at the DNS address provided in your set up email.
- Check UDP port 5060 is open on the firewall.
- Check NAT translation is correct between LAN private IP address and public IP address.
- Check you have the correct proxy user name and password configured.

6.3 Customer System cannot receive a call:

- Some systems require our IP Address to be configured as an allowed gateway.
- Check UDP port 5060 is open on the firewall.
- Check NAT translation is correct between LAN private IP address and public IP address.
- Check that you have setup the IP route for the number correctly with nexVortex. This is done through the customer or reseller Partner Connect portal->Settings-> Number Routing.
- Check that the dial plan is configured to route the number to a valid location on the customer system.

6.4 One way audio or no audio after call is setup:

- Check the RTP audio ports are open on the firewall.
- Check that you are presenting the proper PUBLIC IP for your network.

Important! DNS Address

A specific DNS address was provided in the Account Set Up email you received the day you opened your account. Your Authentication User ID and password are also in this email. If you need assistance locating this information, please contact support@nexvortex.com.

Note: For all instructions throughout this Guide, you must substitute the provided DNS address wherever xx.xx.xxx.xxx is referenced.

Further help may be obtained by emailing support@nexvortex.com.

September 23, 2015