



nexVortex Setup Guide

ASTERISK



September 2015



Asterisk Setup Guide

Copyright nexVortex 2015

This document is the exclusive property of nexVortex, Inc. and no part may be disclosed, copied, or used without the prior, express written approval of nexVortex, Inc. Distribution for any purpose is prohibited.

WHILE THE INFORMATION IN THIS DOCUMENT IS BELIEVED TO BE ACCURATE, NEXVORTEX MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. NexVortex shall not be liable for errors contained therein or for damages of any kind, including incidental or consequential damages in connection with the furnishing, performance or use of this material. The information contained in this document is subject to change without notice.

This document contains information that is protected by copyright (All Rights Reserved). Except as otherwise provided herein, no part of this work may be reproduced or used in any form or by any means graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems without the permission of the copyright owner. All copies of this document must include the copyright and other information contained on this page.

Table of Contents

1	Introduction	4
2	Step 1: Trunk Configuration	5
3	Step 2: Trunk Settings	5
4	Best Practices	7
	4.1 Security	7
	4.1.1 PBX Extensions	7
	4.1.2 GUI Access	7
	4.1.3 Access Units	7
	4.1.4 Dialplan Restrictions	7
	4.2 IVR	7
5	Setup Instructions	8-14
6	Troubleshooting	15
	6.1 Customer System will not register with nexVortex:	15
	6.2 Customer System cannot make a call:	15
	6.3 Customer System cannot receive a call:	15
	6.4 One way audio or no audio after call is setup:	15

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>).

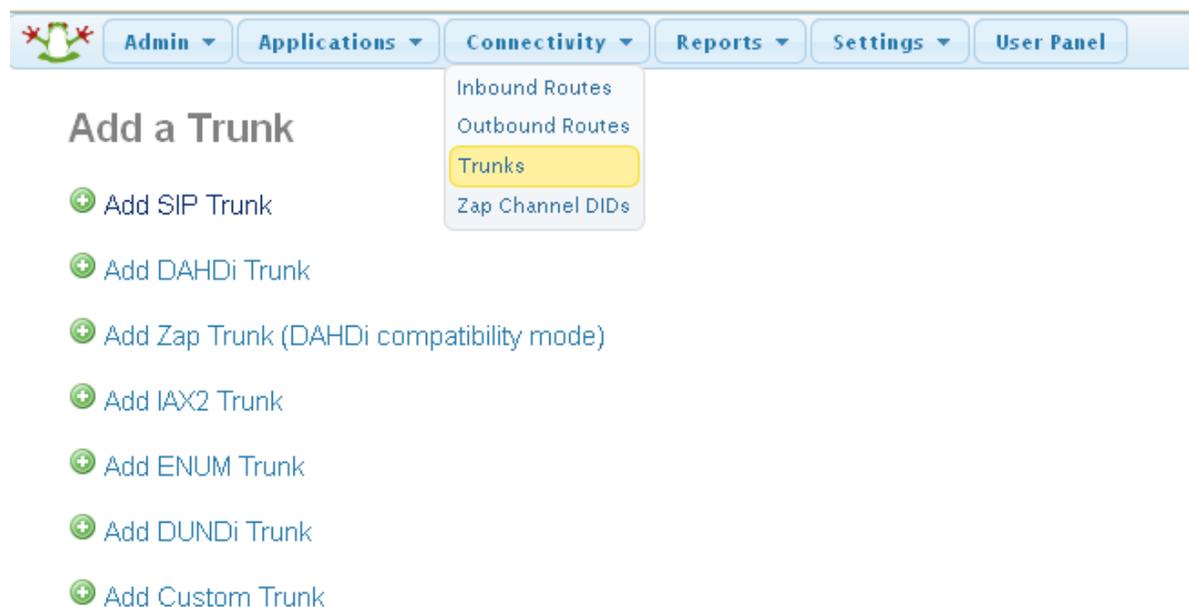
4.2 IVR

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).



The screenshot shows the top navigation bar of the nexVortex interface with the following tabs: Admin, Applications, Connectivity, Reports, Settings, and User Panel. The 'Connectivity' tab is active, and its dropdown menu is open, showing the following options: Inbound Routes, Outbound Routes, Trunks (highlighted in yellow), and Zap Channel DIDs. Below the navigation bar, the 'Add a Trunk' section is visible, listing the following options:

- + Add SIP Trunk
- + Add DAHDi Trunk
- + Add Zap Trunk (DAHDi compatibility mode)
- + Add IAX2 Trunk
- + Add ENUM Trunk
- + Add DUNDi Trunk
- + Add Custom Trunk

Click Add Sip Trunk to create your first nexVortex trunk.



Add SIP Trunk

General Settings

Trunk Name :

Outbound CallerID :

CID Options :

Maximum Channels :

Disable Trunk : Disable

Monitor Trunk Failures : Enable

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).

Outgoing Settings

Trunk Name :

PEER Details :

```
host=px1.nexvortex.com
username=AHaghoaug834ythq
secret=naNBmTjq31194th
type=peer
qualify=no
insecure=port,invite
dtmfmode=rfc2833
```

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

Incoming Settings

USER Context

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

PEER Details :

```

host=px5.nexvortex.com
username=b13f2487ogtabqe
secret=nablidubfv1q3wi4u
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

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.

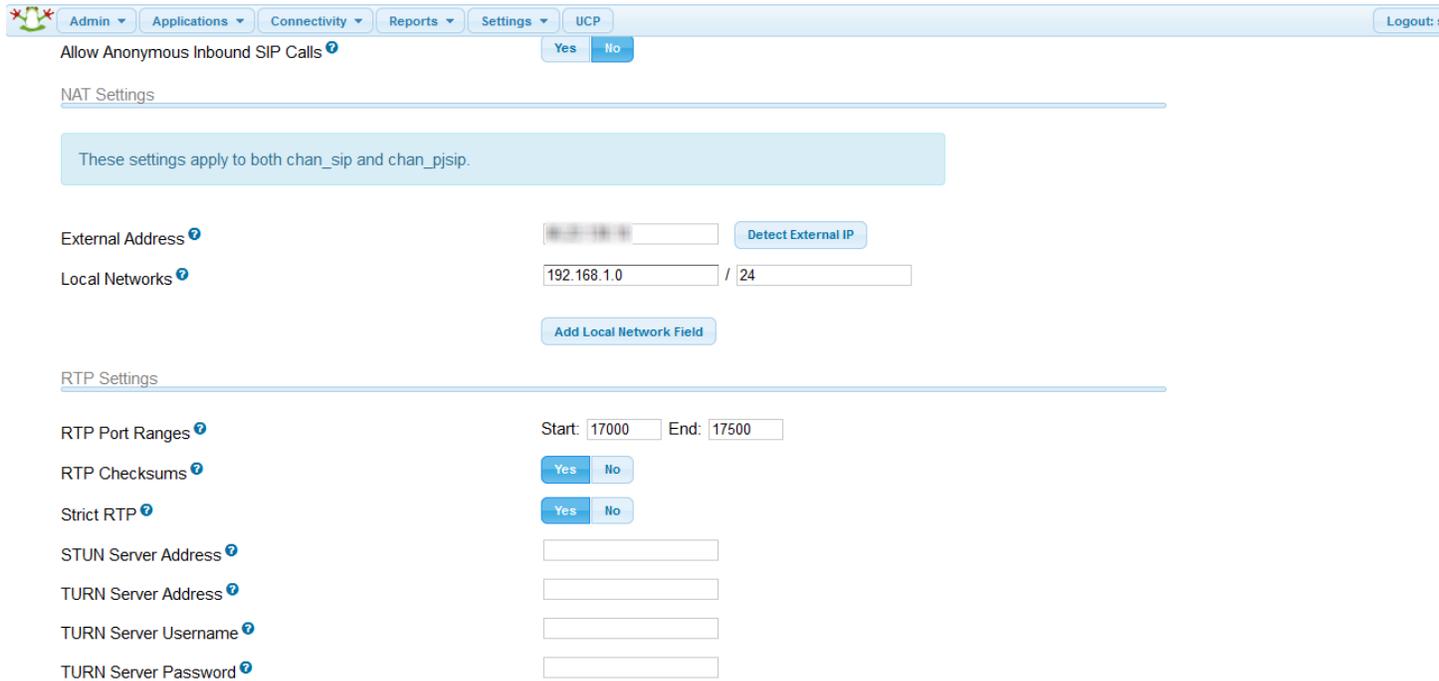


Trunk Settings

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

Device Settings	
Show all Device Setting on Add	<input type="button" value="True"/> <input checked="" type="button" value="False"/>
Require Strong Secrets	<input checked="" type="button" value="True"/> <input type="button" value="False"/>
Remove mailbox Setting when no Voicemail	<input type="button" value="True"/> <input checked="" type="button" value="False"/>
SIP canrenvite (directmedia)	no
SIP trustpid	yes
SIP sendrpid	pai
SIP nat	yes
SIP encryption	no
SIP qualifyfreq	60
SIP and IAX qualify	yes
SIP and IAX allow	
SIP and IAX disallow	
SIP and DAHDi callgroup	
SIP and DAHDi pickupgroup	

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



The screenshot shows the Asterisk SIP Settings web interface. At the top, there is a navigation bar with tabs for Admin, Applications, Connectivity, Reports, Settings, and UCP. Below the navigation bar, there is a section for 'Allow Anonymous Inbound SIP Calls' with 'Yes' and 'No' radio buttons. The main section is titled 'NAT Settings' and contains a blue box stating 'These settings apply to both chan_sip and chan_pjsip.' Below this, there are fields for 'External Address' (with a 'Detect External IP' button), 'Local Networks' (with a value of '192.168.1.0 / 24' and an 'Add Local Network Field' button), and 'RTP Settings'. The 'RTP Settings' section includes 'RTP Port Ranges' (Start: 17000, End: 17500), 'RTP Checksums' (Yes/No), 'Strict RTP' (Yes/No), and fields for 'STUN Server Address', 'TURN Server Address', 'TURN Server Username', and 'TURN Server Password'.

First, update 'External address' by entering your static PUBLIC IP 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 actual 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:



Add Route

Route Settings

Route Name:

Route CID: Override Extension

Route Password:

Route Type: Emergency Intra-Company

Music On Hold?:

Time Group:

Route Position:

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



Dial Patterns that will use this Route

<input type="text" value="(1"/>	<input type="text" value=") + prefix"/>	<input type="text" value=" [NXXNXXXXXX"/>	<input type="text" value="/ CallerID"/>	<input type="text" value="]"/>	<input type="text" value=""/>
<input type="text" value="(prepend"/>	<input type="text" value=") + prefix"/>	<input type="text" value=" [1NXXNXXXXXX"/>	<input type="text" value="/ CallerID"/>	<input type="text" value="]"/>	<input type="text" value=""/>
<input type="text" value="(prepend"/>	<input type="text" value=") + prefix"/>	<input type="text" value=" [411"/>	<input type="text" value="/ CallerID"/>	<input type="text" value="]"/>	<input type="text" value=""/>

[+ Add More Dial Pattern Fields](#)

Dial patterns wizards:

Trunk Sequence for Matched Routes

0

1

2

[Submit Changes](#)

[Duplicate Route](#)

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:**

Add Route

Route Settings

Route Name:
 Route CID: Override Extension
 Route Password:
 Route Type: Emergency Intra-Company
 Music On Hold?:
 Time Group:
 Route Position:

Additional Settings

Dial Patterns that will use this Route

(prepend)	+	prefix		[911]	/	CallerID	
(prepend)	+	prefix		[933]	/	CallerID	
(prepend)	+	prefix		[311]	/	CallerID	

[+ Add More Dial Pattern Fields](#)

Dial patterns wizards:

Trunk Sequence for Matched Routes

0
 1
 2

[Submit Changes](#)

[Duplicate Route](#)

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:

- Device Info

Description:
 Emergency CID:
 Device Type:
 Default User:

[Submit](#)

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