miniSQL Documentation

DevOpSec

Nov 01, 2023

CONTENTS

dSIPRouter allows you to quickly turn Kamailio into an easy to use SIP Service Provider platform, which enables the following two basic use cases:

- **SIP Trunking services:** Provide services to customers that have an on-premise PBX such as FreePBX, FusionPBX, Avaya, etc. We have support for IP and credential based authentication.
- **Hosted PBX services:** Proxy SIP Endpoint requests to a multi-tenant PBX such as FusionPBX or single-tenant such as FreePBX. We have an integration with FusionPBX that make is really easy and scalable!
- **Microsoft Teams Direct Routing:** We can provide SBC functionality that allows dSIPRouter to interconnect your existing voice infrastructure or VoIP carrier to your Microsoft Teams environment.

You can checkout our demo system by clicking the link below and enter the listed username and password:

http://demo.dsiprouter.net:5000

username: admin

password: ZmIwMTdmY2I5NjE4

API Token: 9lyrny3HOtwgjR6JIMwRaMej9LijIS835zhVbD8ywHDzXT07Xm6vem1sgfvWkFz3

I'd like to say thank you to Nicole D., John O. and Courtney G. for their time in fulfilling this document. I'd also like to give a hardy thank you to dOpensource for their monetary support in funding this document.

Free support is available via our group and Slack

Paid support is available here

CHAPTER

ONE

INSTALLING DSIPROUTER

1.1 Installing dSIPRouter

The following video shows you the install process:

We maintain installation documentation for the following operating systems. Please open a pull request if you want to add and maintain addtional documentation:

- debian_install
- rhel_install

Install times vary by depending on OS and system hardware. On debian/centos, expect a short install time, typically around 12 minutes. On amazon linux, expect long compilation times, typically around 45 minutes.

dSIPRouter should be installed on a clean install of the OS. To upgrade your dSIPRouter platform, see instead *Upgrading dSIPRouter*

1.1.1 Prerequisites:

- Must run this as the root user (you can use sudo)
- git needs to be installed
- Hostname needs to be set to a FQDN (for certbot to get LetsEncrypt certificate)
- The installer will handle all other dependencies

1.1.2 Install Options

- Proxy SIP Traffic Only (Don't Proxy audio (RTP) traffic)
- Proxy SIP Traffic, Audio and it configures the system to work properly when the PBX's and dSIPRouter are behind a NAT.

1.1.3 OS Support

OS / Distro	Current Support
Debian 12 (bookworm)	STABLE
Debian 11 (bullseye)	STABLE
Debian 10 (buster)	STABLE
Debian 9 (stretch)	DEPRECATED
CentOS 9 (stream)	STABLE
CentOS 8 (stream)	STABLE
CentOS 7	DEPRECATED
RedHat Linux 8	ALPHA
Alma Linux 8	ALPHA
Rocky Linux 8	ALPHA
Amazon Linux 2	STABLE
Ubuntu 22.04 (jammy)	ALPHA
Ubuntu 20.04 (focal)	DEPRECATED

1.1.4 Amazon AMI's

We now provide Amazon AMI's (pre-built images) which allows you to get up and going even faster. You can find a list of the images here. The images are a nominal fee, which goes toward supporting the project.

CHAPTER

TWO

COMMAND LINE OPTIONS

2.1 Command Line Options

Execute "./dsiprouter.sh" followed by one of the listed commands. **NOTE** Once installed the command will be available globally as *dsiprouter* with tab-completion.

Command	What does it do?
install	Installs dSIPRouter and related services
uninstall	Uninstall dSIPRouter and related services
clusterinstall	Install dSIPRouter (via SSH) on a cluster of nodes
upgrade	Upgrade dSIPRouter platform (requires license)
start	Starts dSIPRouter
stop	Stops dSIPRouter
restart	Restarts dSIPRouter
chown	Update file permissions for dSIPRouter and related services
configurekam	Reconfigures the Kamailio configuration file based on dSIPRouter settings
configuredsip	Reconfigures the dSIPRouter configuration file, updating dynamic settings
renewsslcert	Renew configured letsencrypt SSL certificate
configuresslcert	Reconfigures SSL certificate used by Kamailio and dSIPRouter
installmodules	Install / uninstall dDSIProuter modules
resetpassword	Generate new random dSIPRouter admin account password
setcredentials	Set various credentials manually
version	Show dSIPRouter version
help	List all of the options

Refer to *Installing dSIPRouter* to get the complete one line version of the command.

To start dSIPRouter:

```
dsiprouter start
```

To stop dSIPRouter:

```
dsiprouter stop
```

To restart dSIPRouter:

```
dsiprouter restart
```

To uninstall dSIPRouter:

```
dsiprouter uninstall -all
```

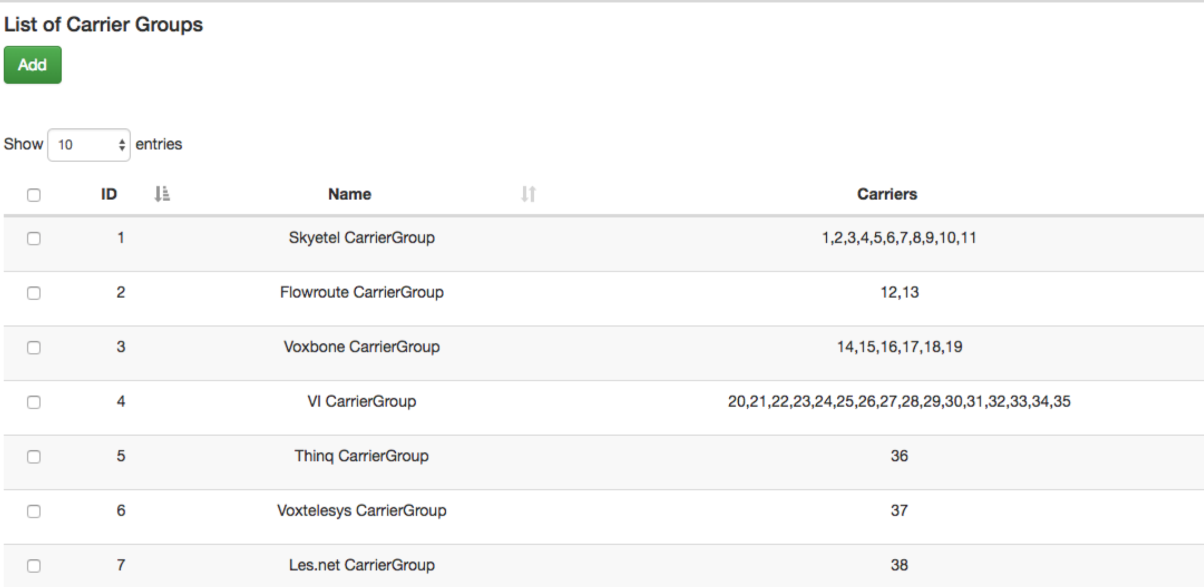
CHAPTER THREE

CONFIGURING DSIPROUTER

3.1 dSIPRouter GUI Intro

3.1.1 Carrier Groups

The Carrier Group section of dSIPRouter allows you to define which carriers will be used to provide Internet service (aka ISP) for your VOIP (Voice Over IP) services. Carrier groups support IP Authentication and Username/Password authentication. Below is an example of a carrier groups list.



List of Carrier Groups

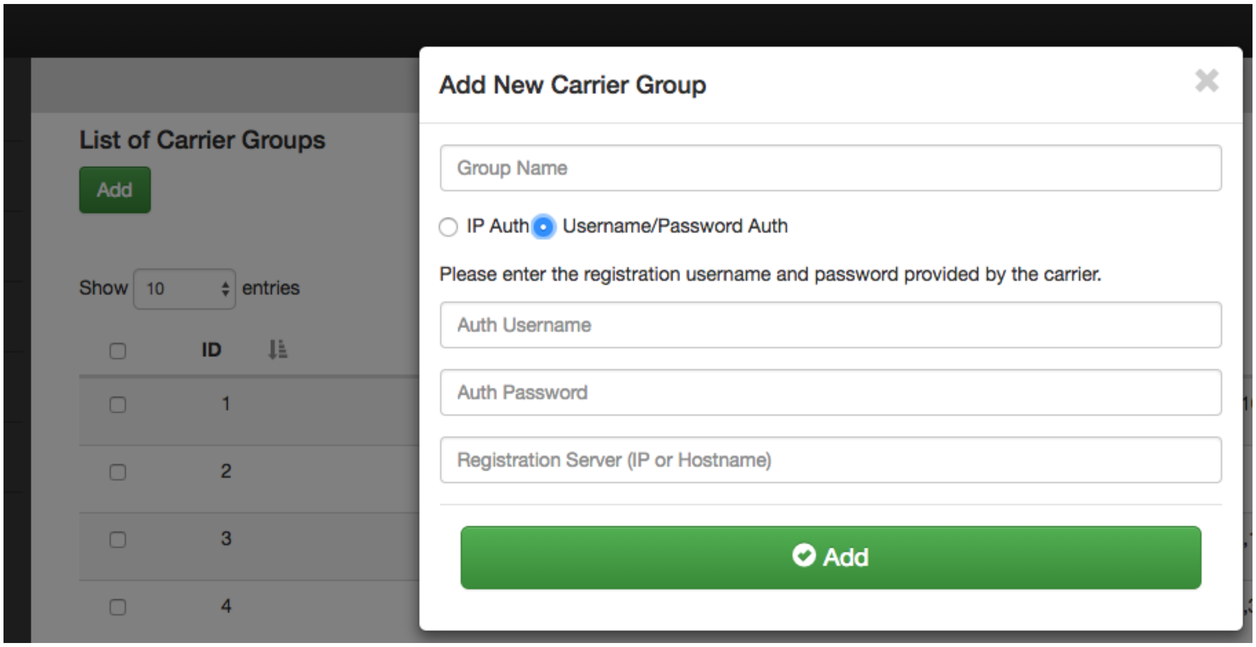
Add

Show 10 entries

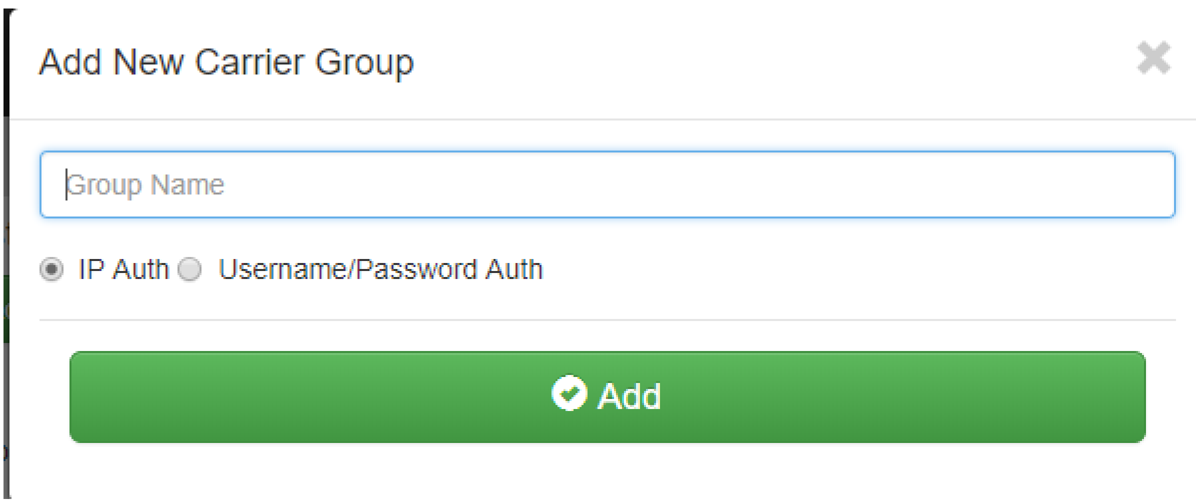
	ID	Name	Carriers
	1	Skyetel CarrierGroup	1,2,3,4,5,6,7,8,9,10,11
	2	Flowroute CarrierGroup	12,13
	3	Voxbone CarrierGroup	14,15,16,17,18,19
	4	VI CarrierGroup	20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35
	5	Thinq CarrierGroup	36
	6	Voxtelesys CarrierGroup	37
	7	Les.net CarrierGroup	38

3.1.2 Adding a Carrier

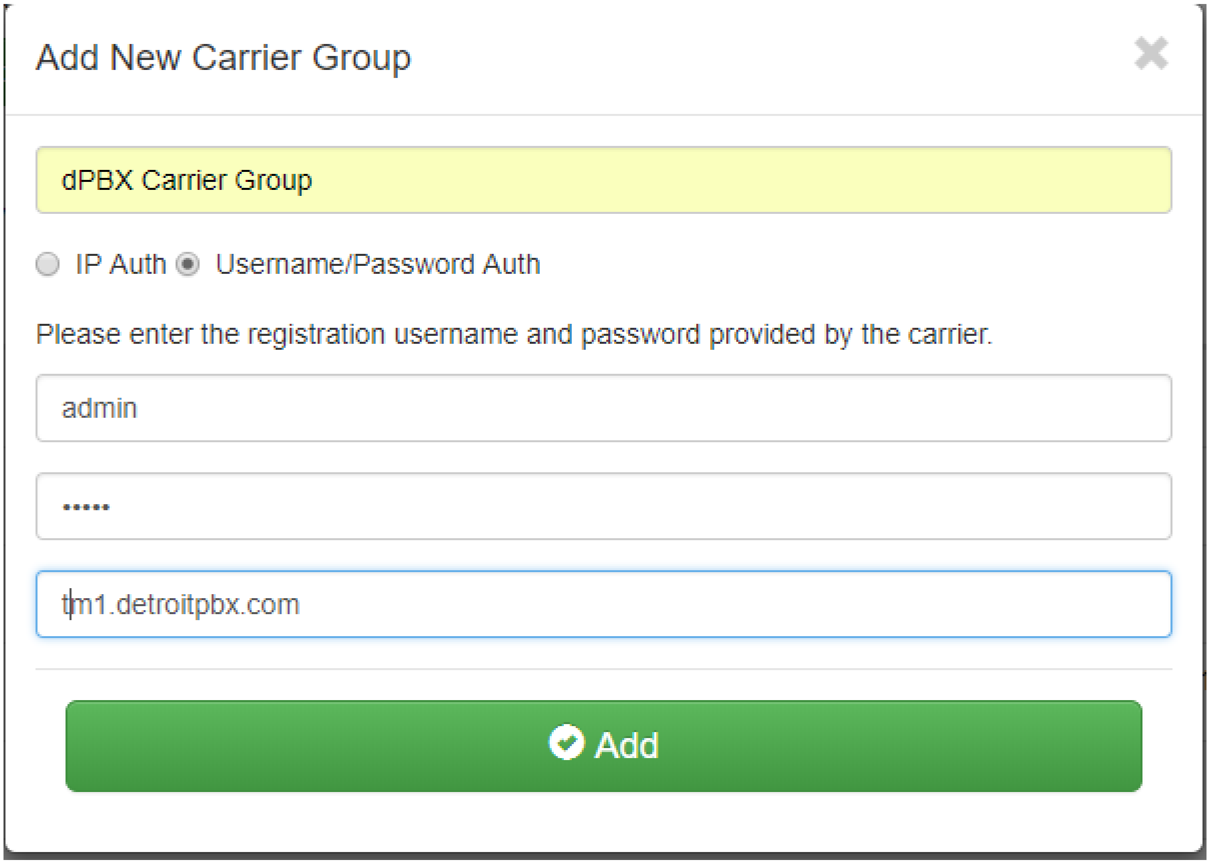
- Log into dSIPRouter using proper username and password.
- Click "Add" to create a Carrier Group. A carrier group can contain 1 or more SIP endpoints provided by the carrier. A SIP Endpoint represents a device that makes or receives calls via your Gateway. This could be a physical IP phone, a softphone app such as Skype, on a PC or smartphone, an Analog Telephone Adapter (ATA) such as for fax machines, or even a PBX system.
- Select Username/Password Auth, fill in the username, password of your registration server and the registration server name. Then click ADD.



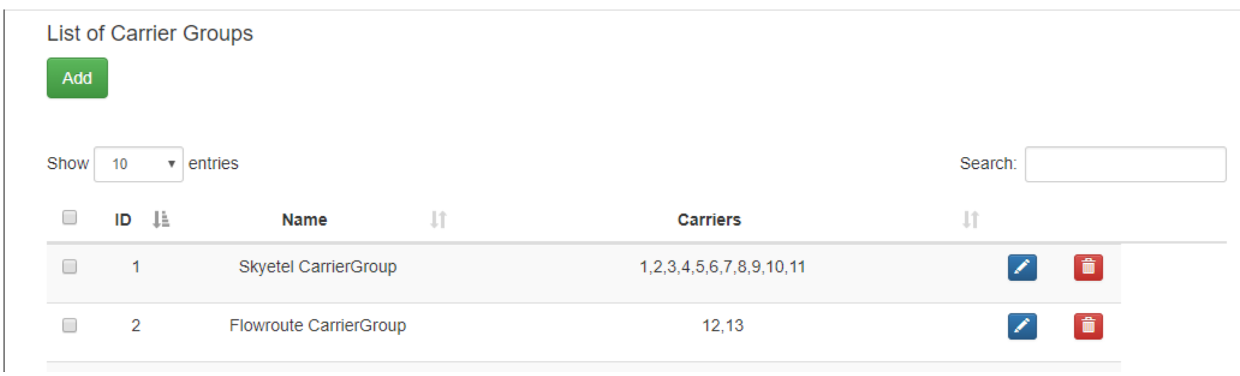
NOTE: Click IP authenication to use only the IP address of your PBX/endpoint.



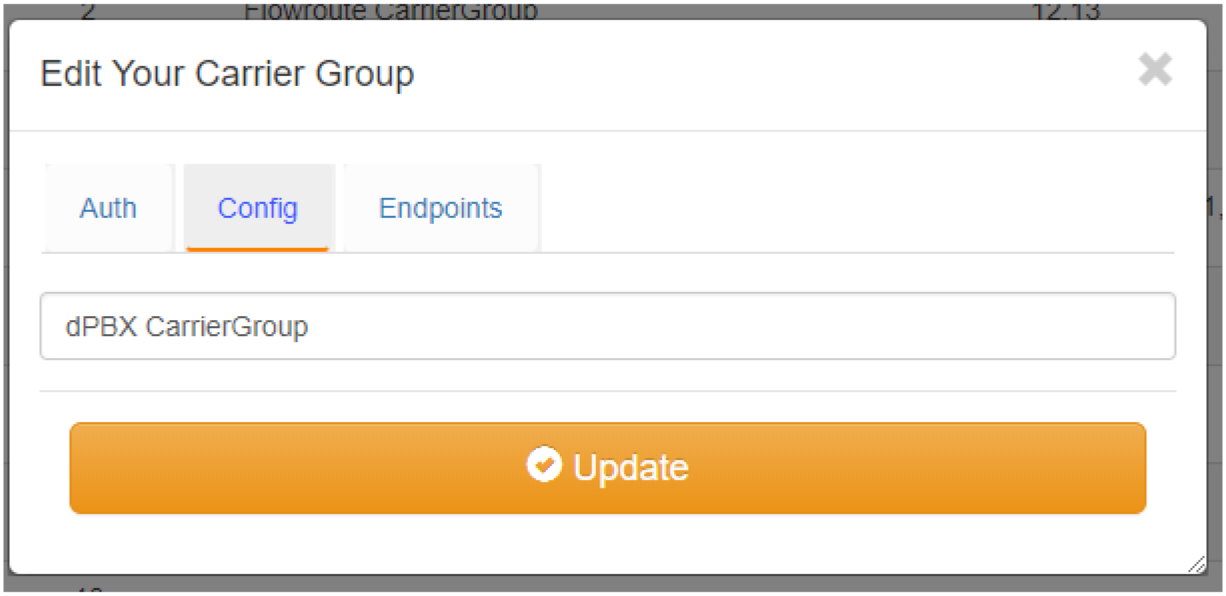
For example:



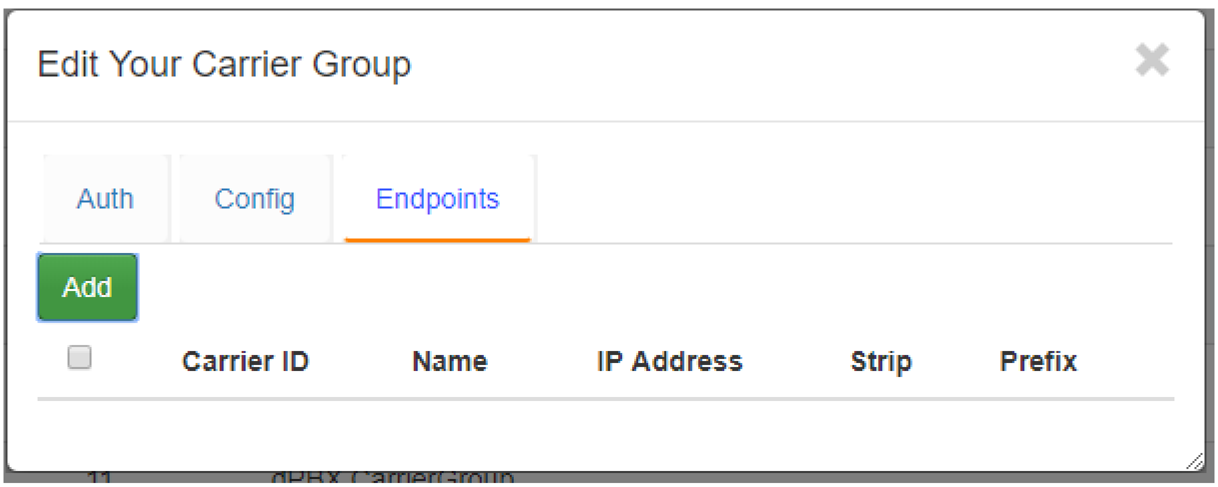
After you have added the new group, the screen will return back to the List of Carriers Group page. Select the pencil in the blue box to the right to allow editing the Config and Endpoints.



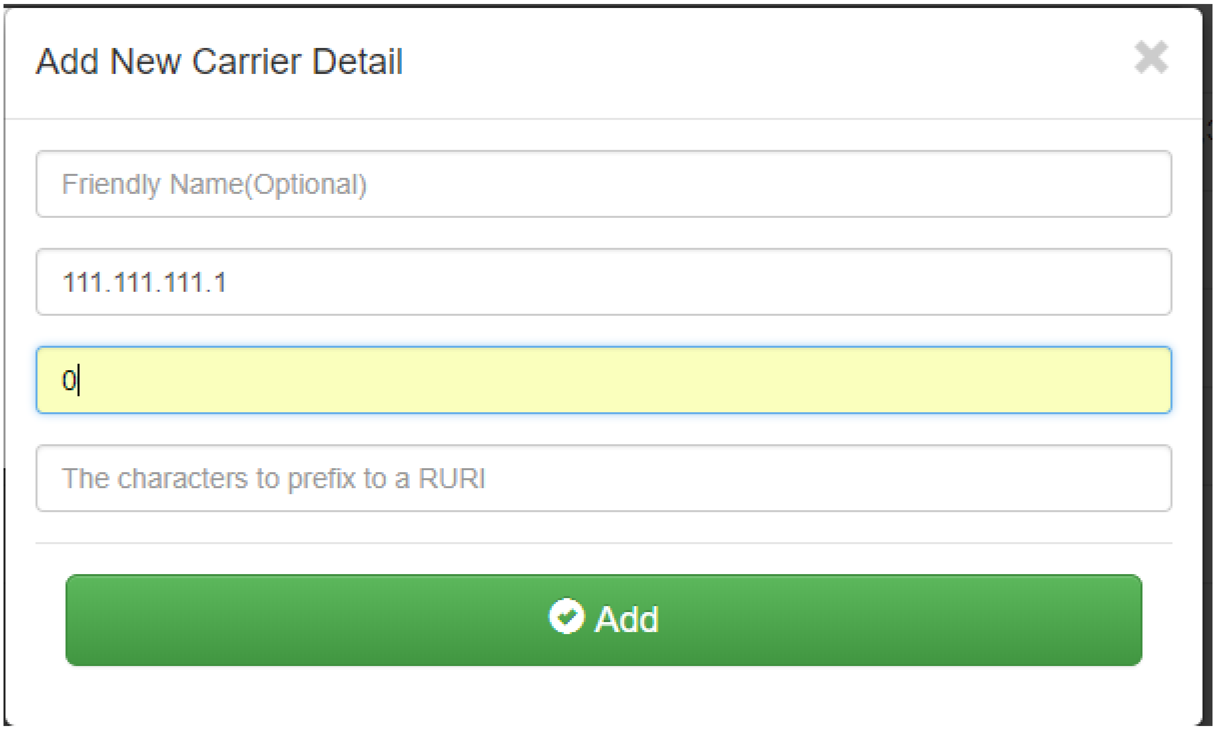
Select the Config tab. The Config tab allows you to edit/change the Carrier group name. Then click Update.



To add an Endpoint, click the Endpoint tab.

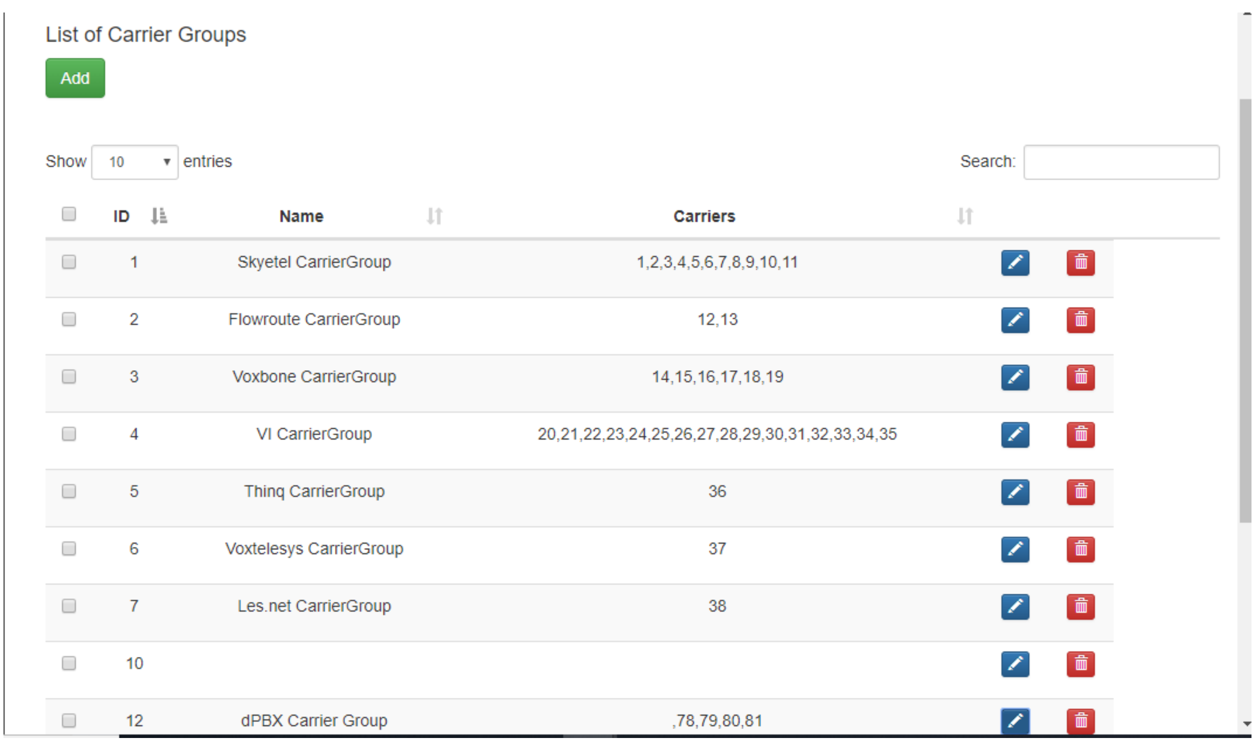


Click ADD, enter the Friendly name (optional), the IP address of the endpoint/device, # of characters to strip from RURI, the character to prefix to a RURI then click ADD again. For example, if a PBX sends a number over as 9144433322222 but the carrier wants the number to be sent as 14443332222 then the # of characters to strip should be defined as 1, which would strip off the 9. Some carriers request added digits (aka Prefixes) in front of the phone number.

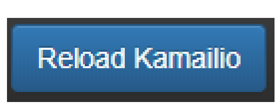


Edit and click ADD again to add addtional endpoints. Click the gray X in that box to save the window and close.

You should now see your added carrier with endpoints in the Carrier Group List.



Be sure to click the Reload Kamailio button to apply changes.

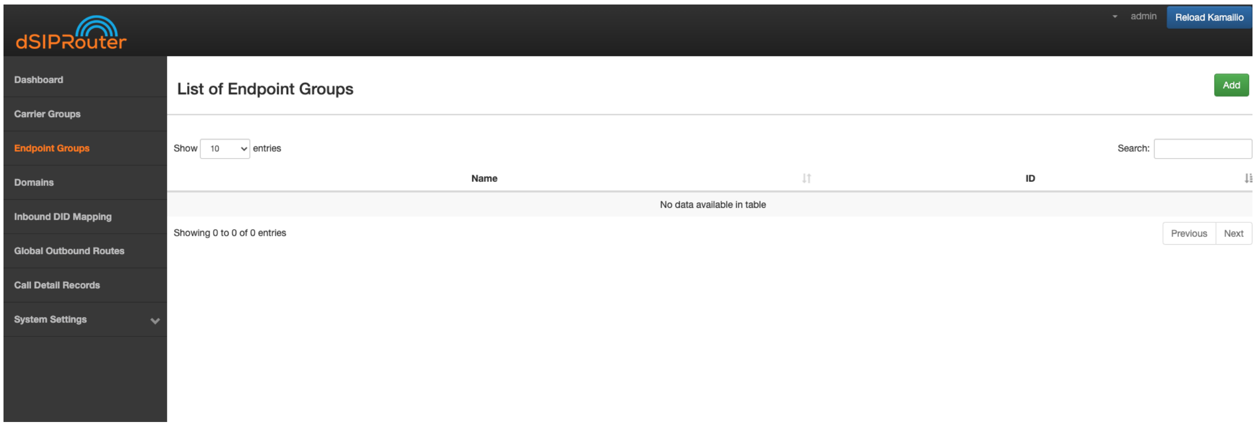


3.1.3 PBX(s) and Endpoints

Allows you to define a PBX or Endpoint that will send or receive calls from dSIPRouter. The PBX or Endpoint can use IP authentication or a username/password can be defined.

To add an Endpoint Group:

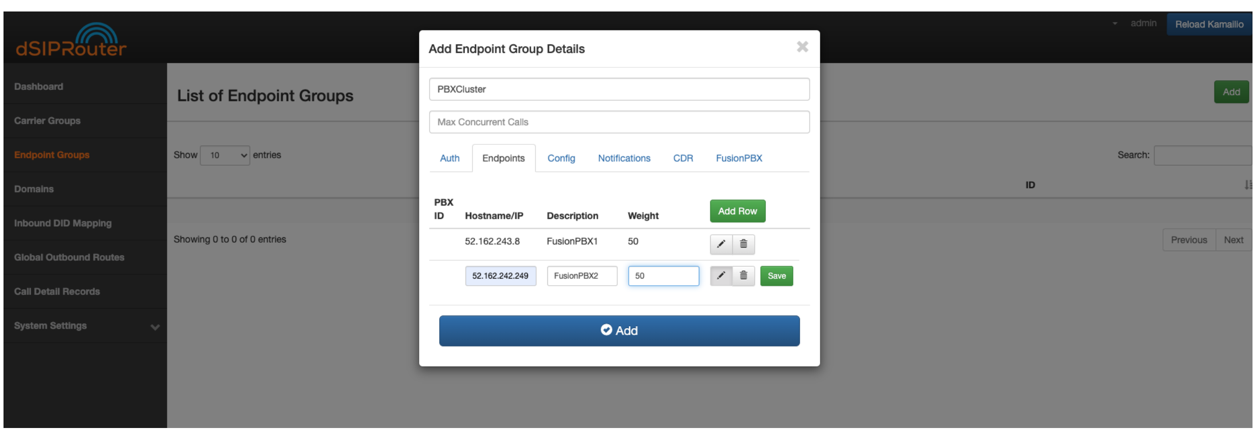
1) Click on Endpoints Groups.
2) Click on the green Add button.



3) Configure the Endpoint Group

   The Endpoint Tab is where you specify the endpoints that will be signaling with dSIPRouter. The weight field allows you to define how much SIP traffic is distributed to a particular endpoint. If you don't specify a weight for an endpoint the system will automatically generate a weight. If you are using FusionPBX Domain Auth then Register and INVITE requests will be distributed to the endpoints based upon the weights. You will also have the option to route Inbound calls to the endpoints based on the weights by selecting the name of the Endpoint Group with an LB concatenated to the name. For example, if the name of the Endpoint Group is **PBXCluster** then you would select **PBXCluster LB** from the Inbound Mapping Endpoint Group drop down.

b) Click the green Add button.

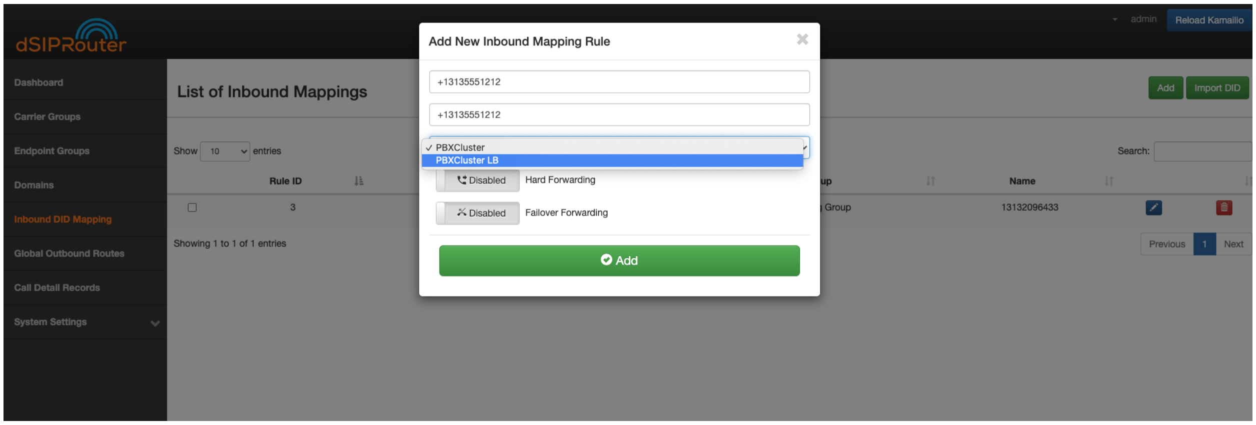


4) Click on the Reload Kamailio button in order for the changes to be updated.

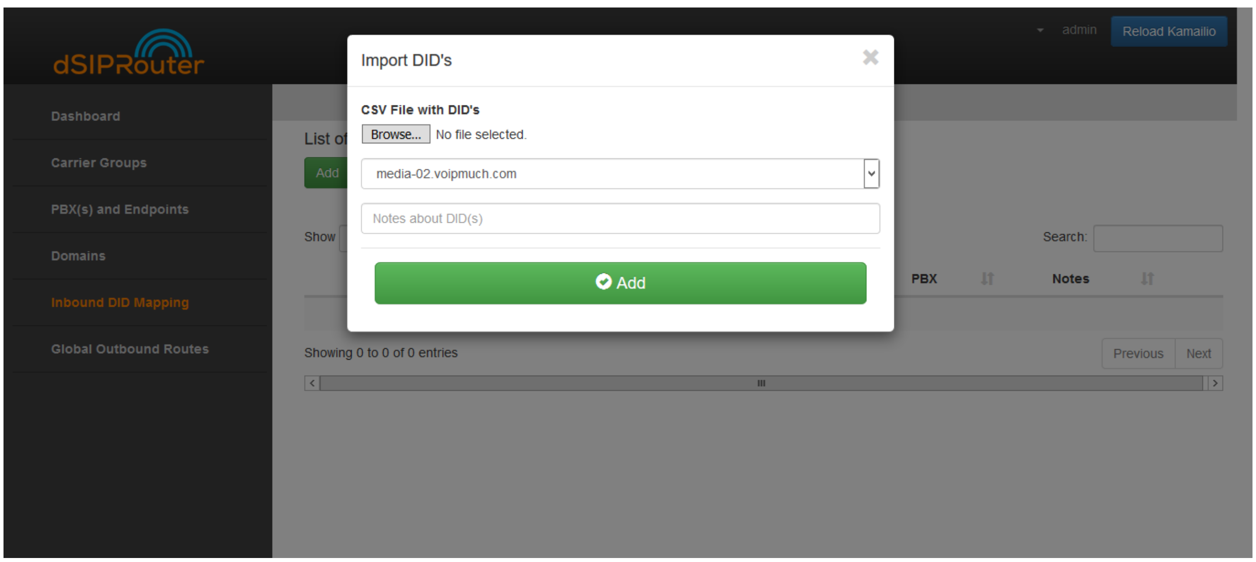
3.1.4 Inbound DID Mapping

To Import a DID from a CSV file:

1) Click on Inbound DID Mapping.



2) Click on the green Import DID button underneath List on Inbound Mappings.



3) Click the Browse button and select the file that contains the DID numbers that you wish to use.

4) Click the green Add button.

   Click CSV Example to view a sample of the .CSV file

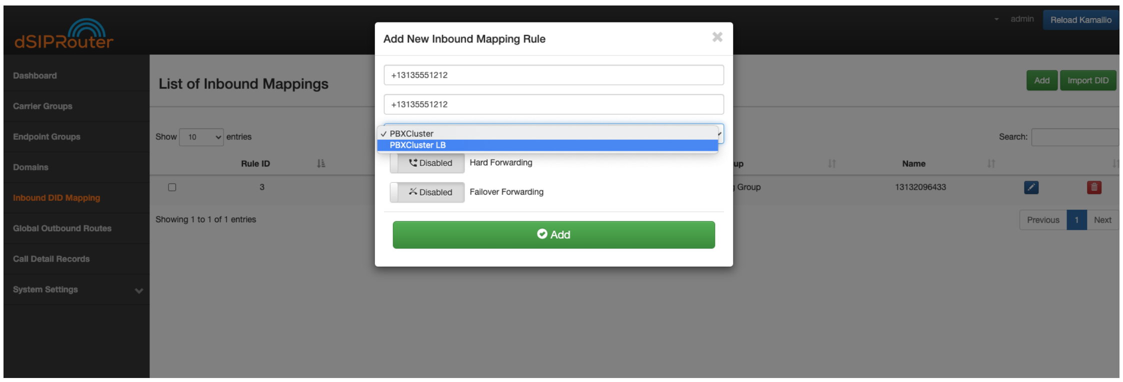
5) Click on the Reload Kamailio button in order for the changes to be updated.

To Manually import a DID:

1) Click on Inbound DID Mapping
2) Click on the green ADD button.
    - Enter the name of the Inbound mapping
    - Enter the DID number in the DID field.
    - Select the Endpoint Group from the drop-down list

      Note: Each endpoint will contain at least two entries. One that leverages load balancing weights and another that randomly selects an endpoint. The one denoted with a LB is the one that uses the load balancing algorithm. If FusionPBX Domain Support is enabled you will see an additional entry for routing to the external interface of the FusionPBX server.

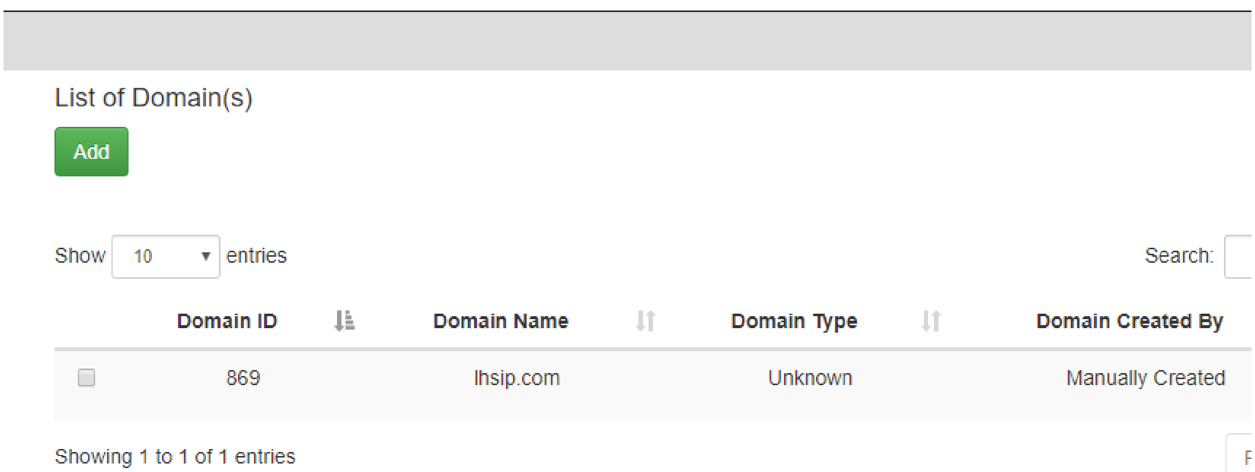
    - Click the green Add button.



3) Click on the Reload Kamailio button in order for the changes to be updated.

3.1.5 Adding a Domain

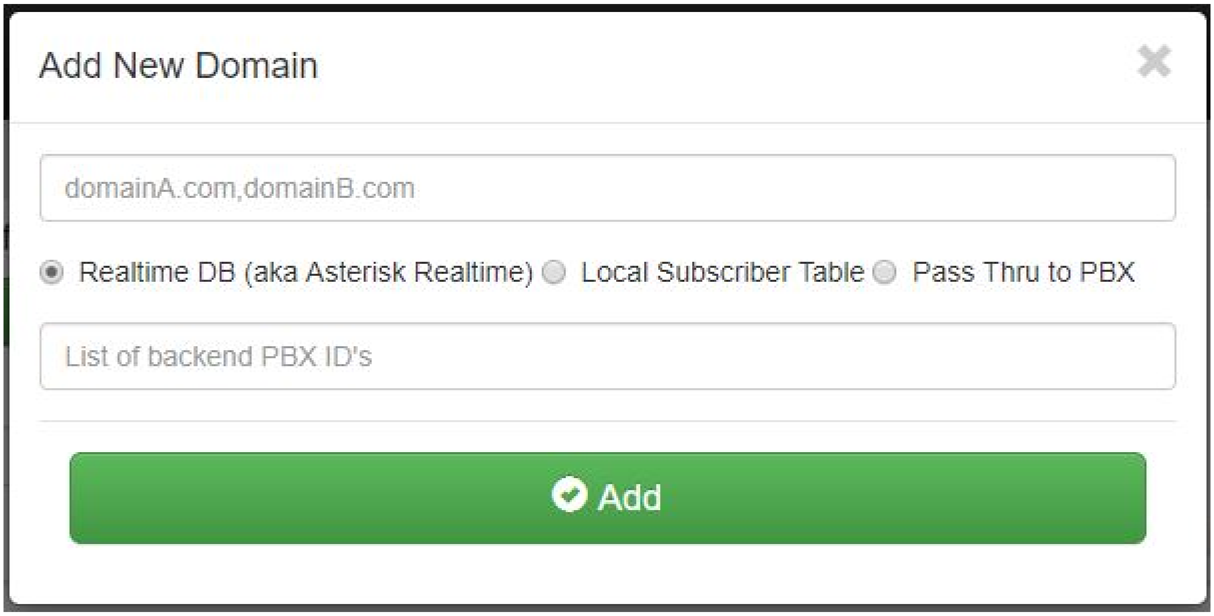
To add a domain click on Domains then click the green add button.



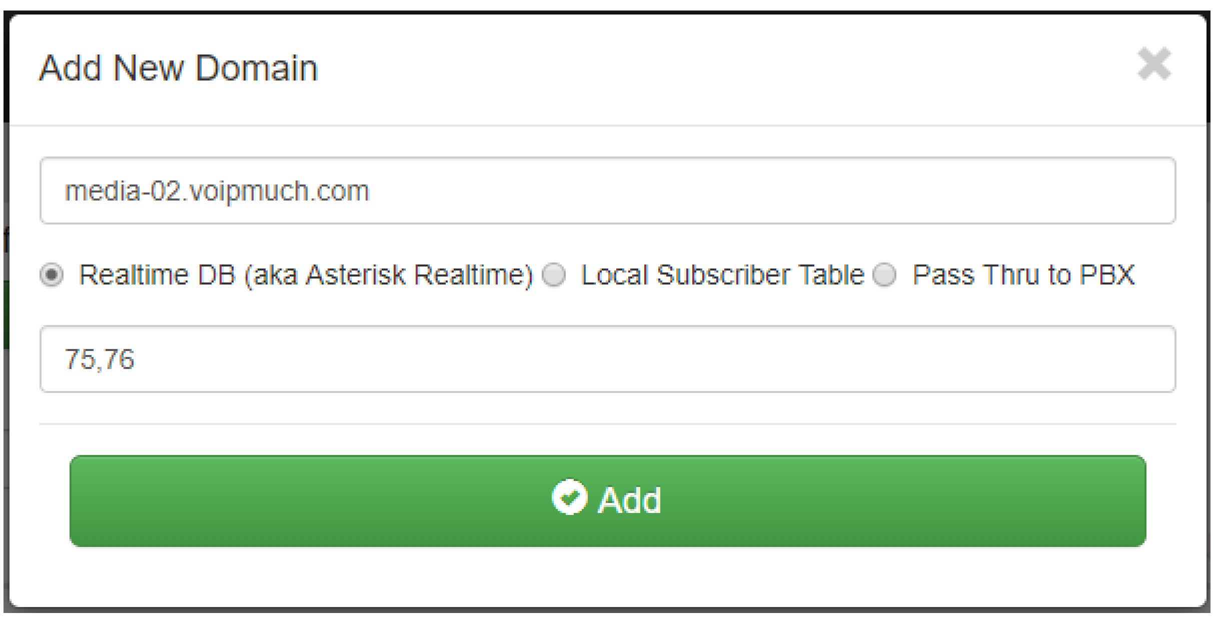
Fill in the domain name. (Note: You can create 1 or more domains by separating them with commas).

- Select Realtime DB or Local Subscriber table (for multiple domains)
- Select Pass Thru to PBX (single domain).

Note: Details can be found in Realtime DB if you want to ensure that the Kamailio configuration file is setup to point to the Asterisk Realtime database configuration. Details on how to populate the table can be found in the Local Suscriber table if you want to use the built in subscriber table that's part of Kamailio. Use the pass thru to register info to the FreePBX server so that you don't have to change how authentication is done.

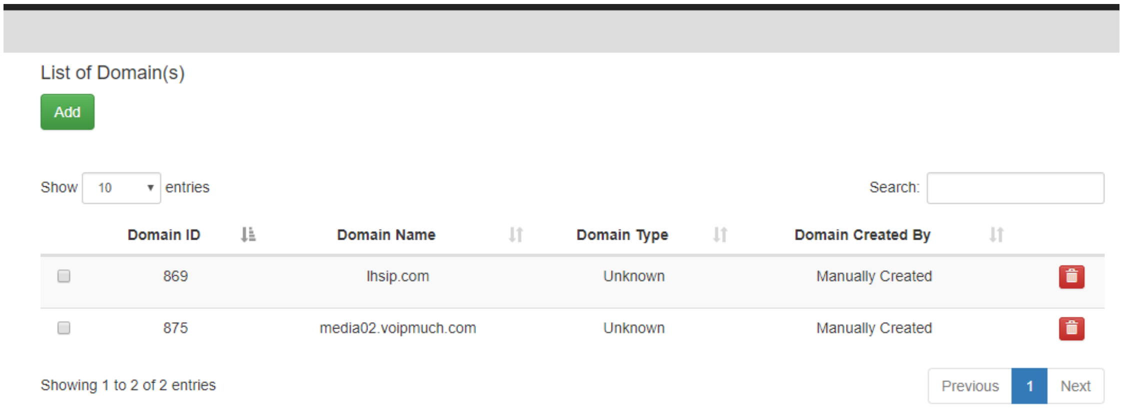


- For the List of backend PBX ID's you should use the ID assigned to each PBX that you want to be part of that domain. Such as naming the ID number thats assigned to media-02.voipmuch.com for example in *PBX(s) and Enpoints*.

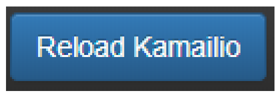


- Click ADD

You will then be returned back to the List of domains page and you should see your new domain added. You can delete this domain by clicking the red trash can to the right of the page.

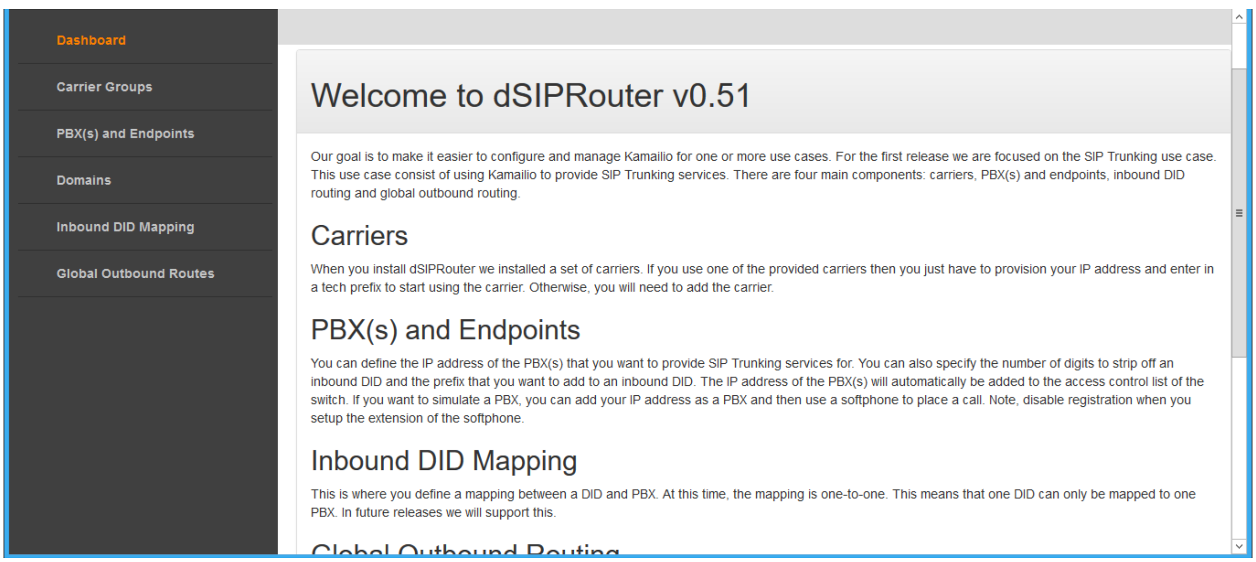


Be sure to click the Reload Kamailio button to apply changes.



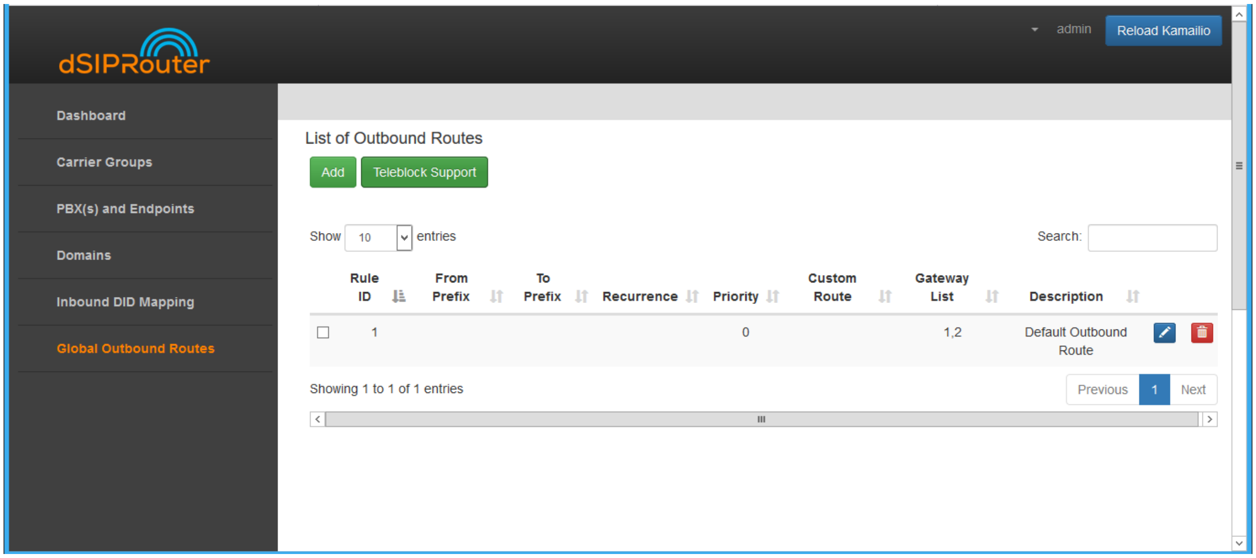
3.1.6 Global Outbound Routes

1) Go to the Dashboard screen.



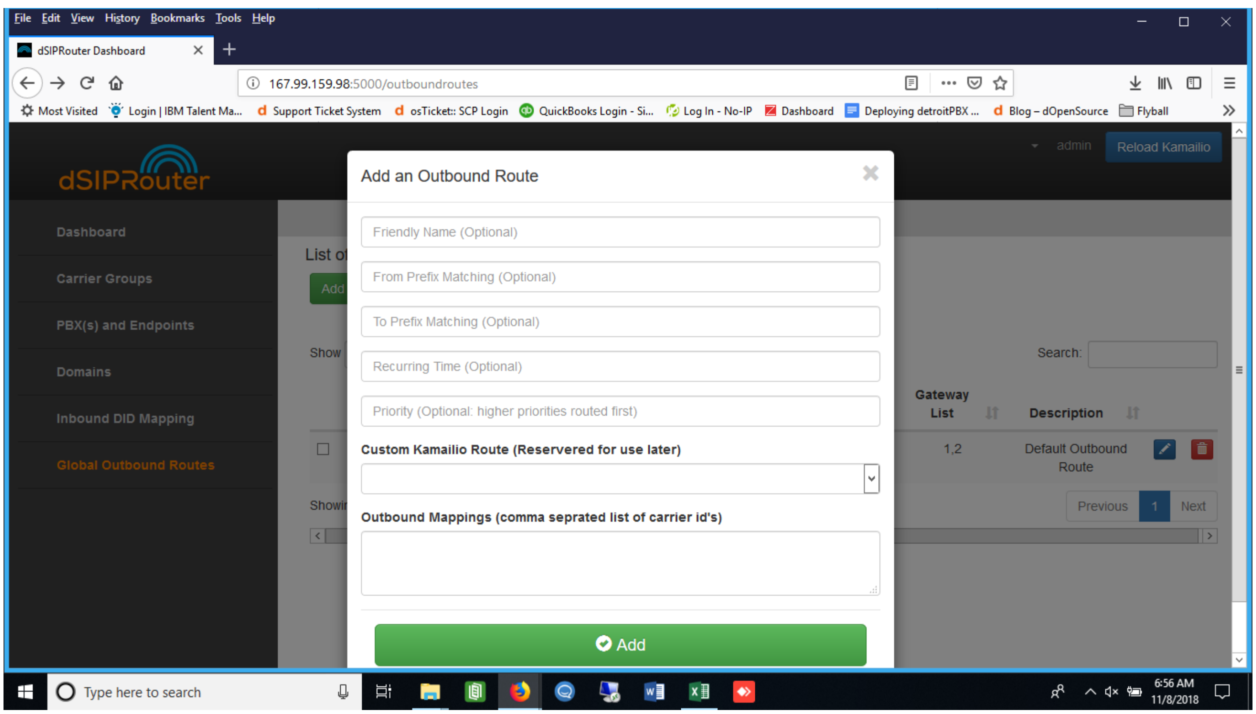
2) Click on Global Outbound Routes.

3) Click on the green Add button.



4) a) Enter in the Outbound Route information.

b) Click on the green Add button.



5) Click on the blue Reload Kamailio button in order for the changes to be updated.

CHAPTER

FOUR

IMPLEMENTING USE CASES

4.1 Common Use Cases

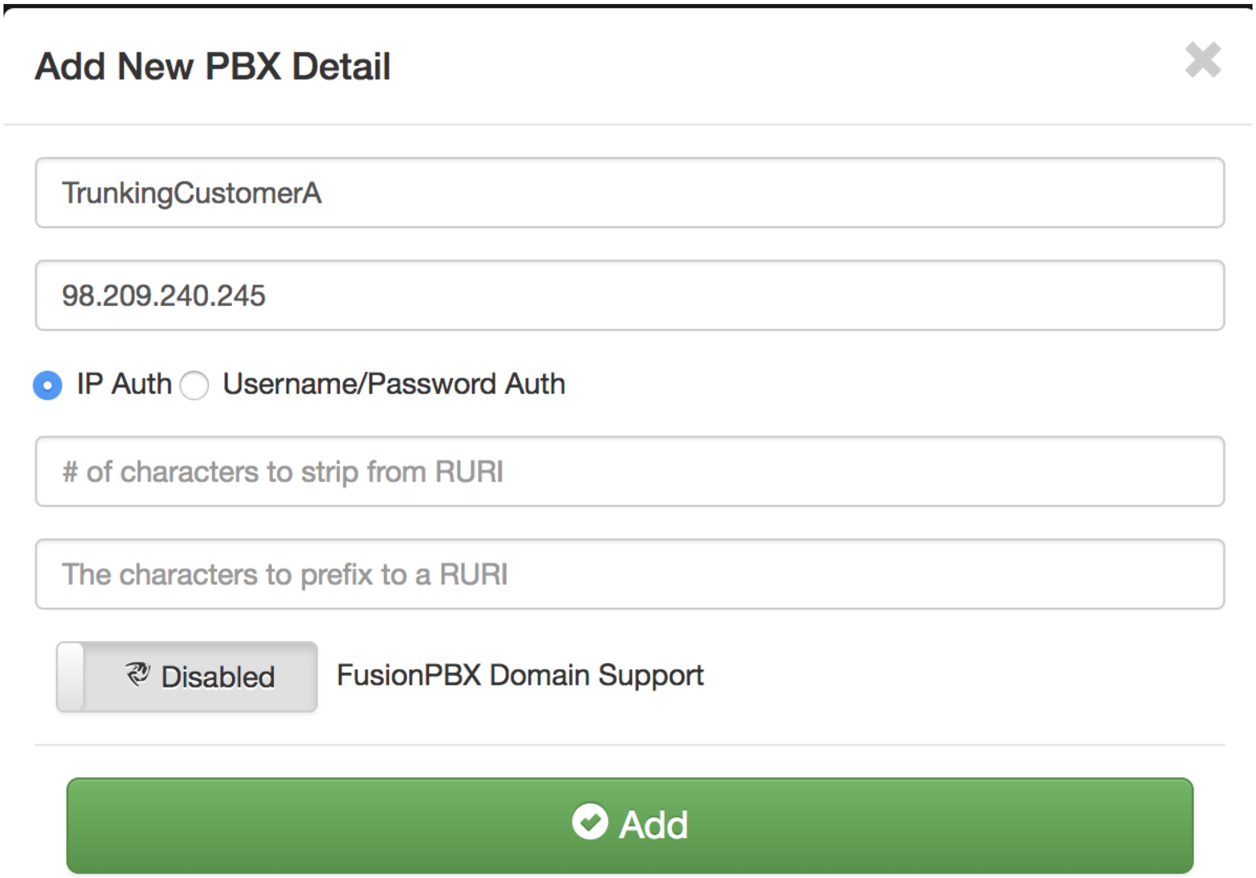
This section contains a list of the common use cases that are implemented using dSIPRouter

4.1.1 SIP Trunking Using IP Authentication

dSIPRouter enables an organization to start supporting SIP Trunking within minutes. Here are the steps to set it up using IP Authentication:

1. Login to dSIPRouter
2. Validate that your carrier is defined and specified in the Global Outbound Routes. If not, please follow the steps in **:ref:`carrier_groups`_** and/or **:ref:`global_outbound_routes`_** documentation.
3. Click on PBX's and Endpoints
4. Click "Add"
5. Select **IP Authentication** and fill in the fields specified below:

- Friendly Name
- IP Address of the PBX or Endpoint Device



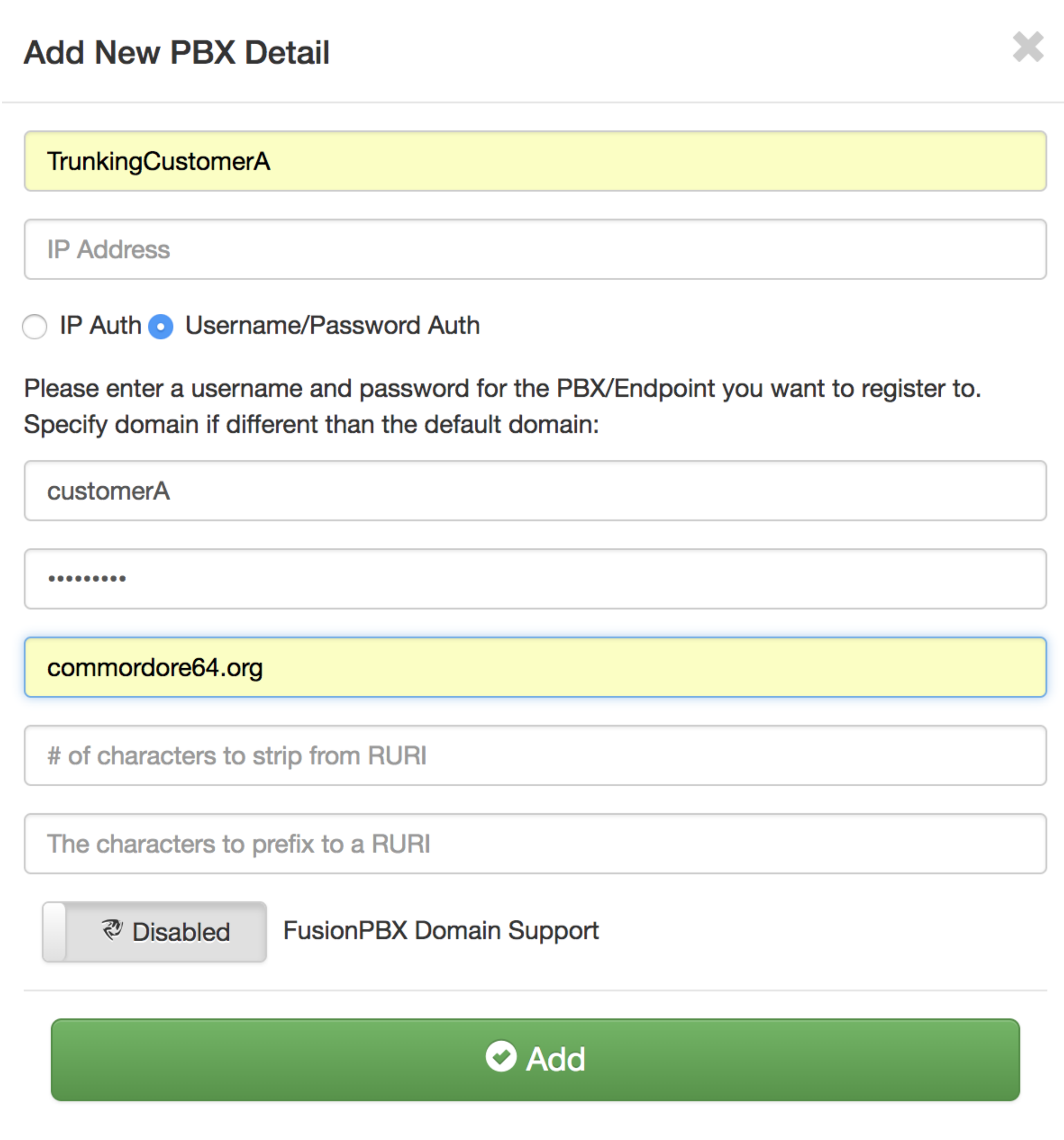
6. Click “Add”
7. Click “Reload” to make the change active.

4.1.2 SIP Trunking Using Username/Password Authentication

Here are the steps to set it up using Username/Password Authentication:

1. Login to dSIPRouter
2. Valiate that your carrier is defined and specified in the Global Outbound Routes. If not, please follow the steps in carrier_groups.rst and/or global_outbound_routes documentation.
3. Click on PBX’s and Endpoints
4. Click “Add”
5. Select **Username/Password Authentication** and fill in the fields specified below:

- Friendly Name
- Click the “Username/Password Auth” radio button
- Enter a username
- Enter a domain. Note, you can make up the domain name. If you don’t specify one then the default domain will be used, which is sip.dsiprouter.org by default.
- Enter a password

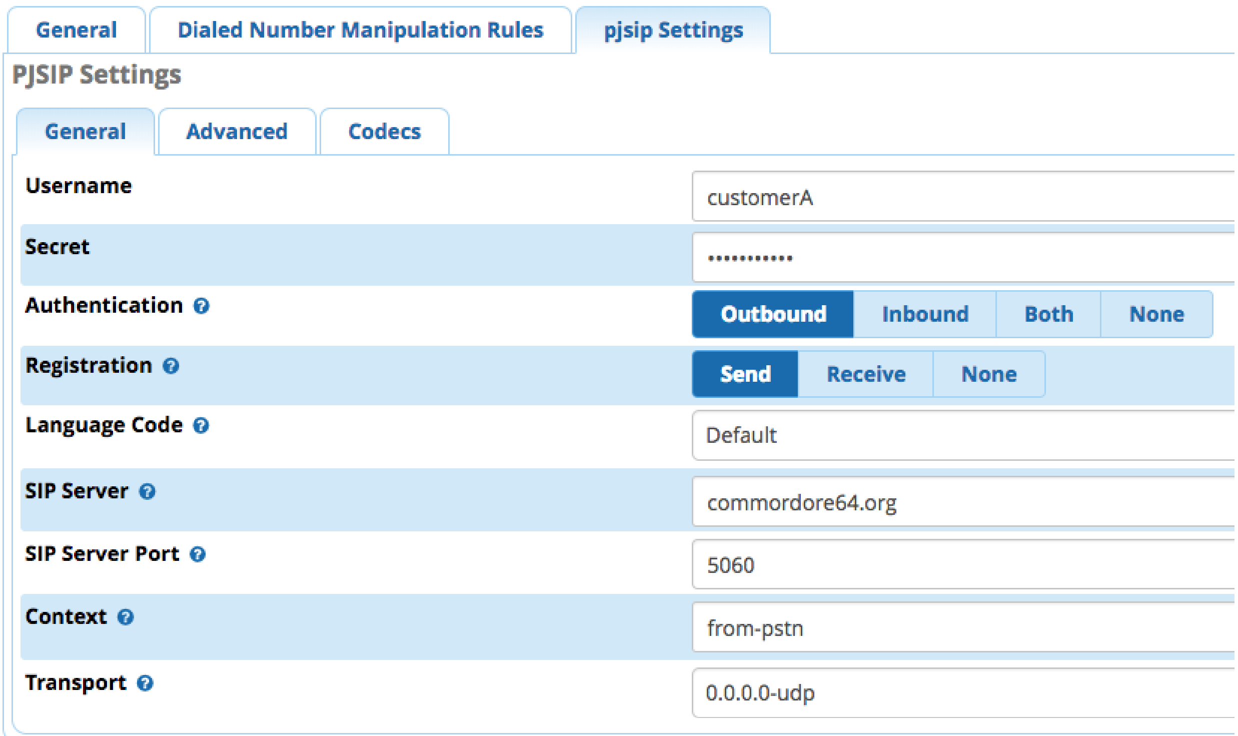


6. Click “Add”
7. Click “Reload” to make the change active.

4.1.3 Using PJSIP Trunking - FreePBX Example

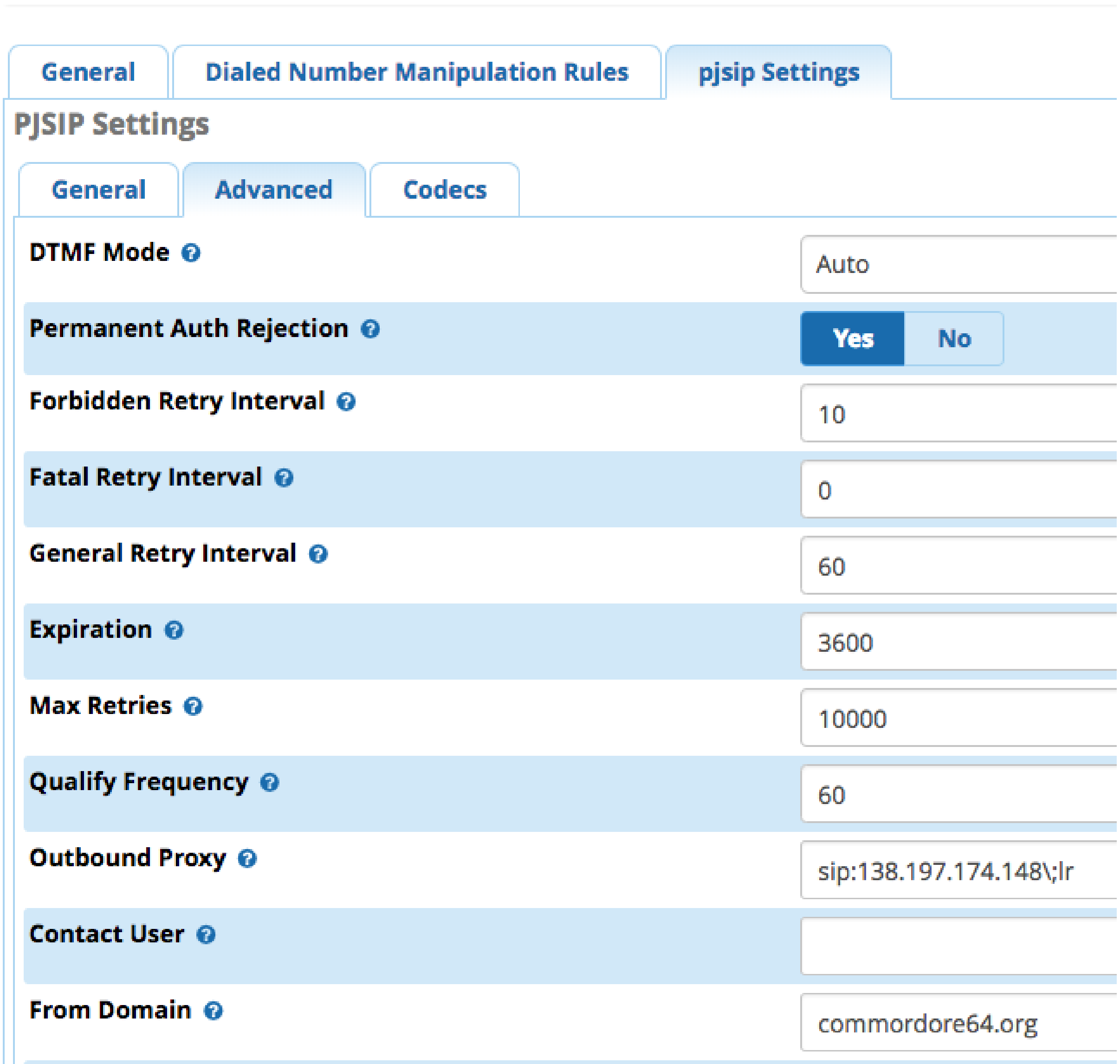
The following screenshot(s) shows how to configure a PJSIP trunk within FreePBX for Username/Password Authentication.

The first screenshot shows the General tab of the "pjsip settings" page:



The following fields needs to be entered

Field	Value
Username	Username from dSIPRouter PBX Setup
Secret	Password from dSIPRouter PBX Setup
Authentication	Outbound
Registration	Send
SIP Server	Domain name defined in the dSIPRouter PBX Setup
SIP Server	SIP port, which is 5060 in dSIPRouter



The following fields needs to be entered

Field	Value
Outbound Proxy	IP address of dSIPRouter - must include the ";lr" at the end
From Domain	The name of the domain defined in the dSIPRouter PBX Setup

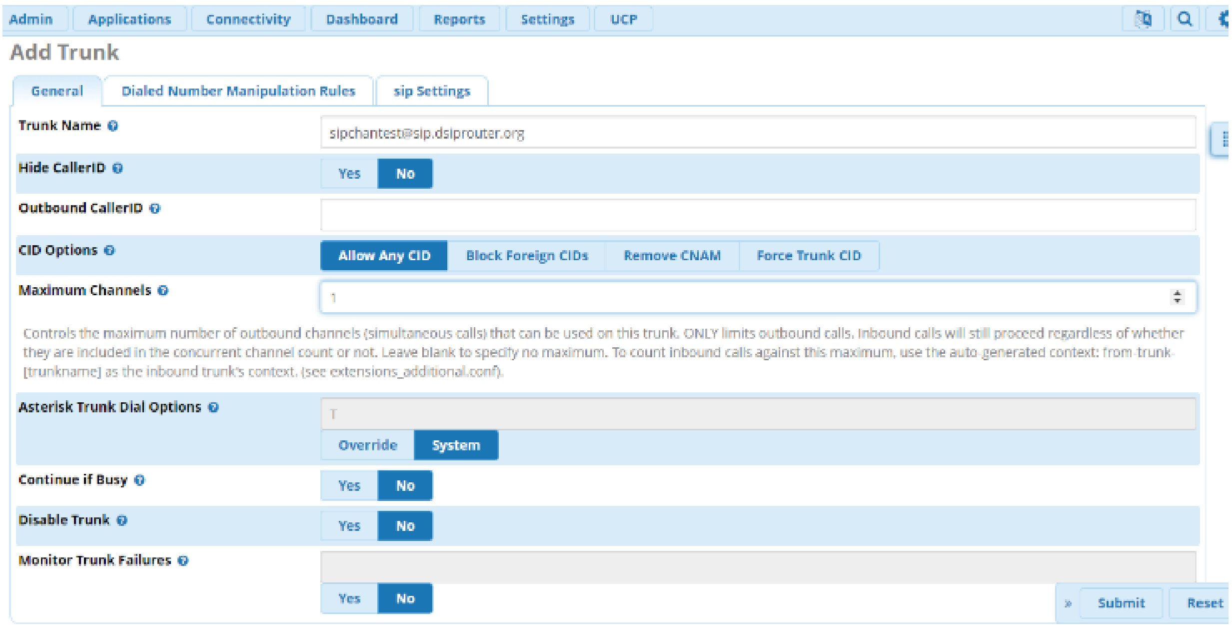
4.1.4 Using chanSIP Trunking - FreePBX Example

The following screenshot(s) shows how to configure a chanSIP trunk within FreePBX for Username/Password Authentication.

1. Log into FreePBX server
2. Click Connectivity→Trunks
3. Select Add SIP (chan_sip) Trunk
4. Under General tab enter

The following fields needs to be entered

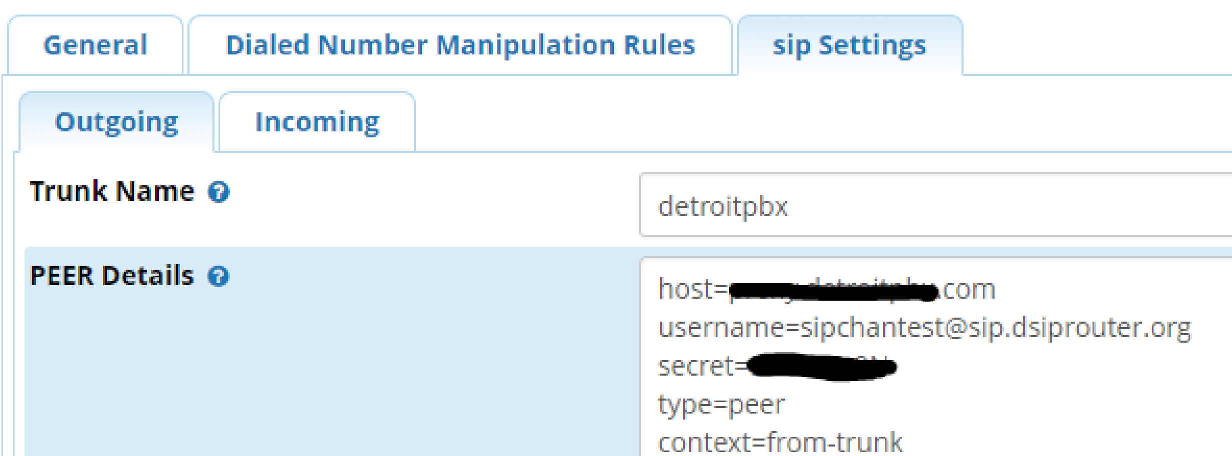
Field	Value
Trunk Name	Labeled in dsiprouter
Outbound Caller ID	Phone# that you want to appear during a outbound call (if applicable)



5. Next you will enter the configurations under the SIP Settings. Here you will enter the SIP settings for outgoing calls by selecting the **Outbound** tab. You will need the following information: The following fields needs to be entered

Field	Value
Host	<host name or IP address of dsiprouter>
Username	<Specified in dsiprouter@domainname>
Secret	<Specified in dsiprouter>
Type	peer
Context	from-trunk

The domain name has to be included and correct.

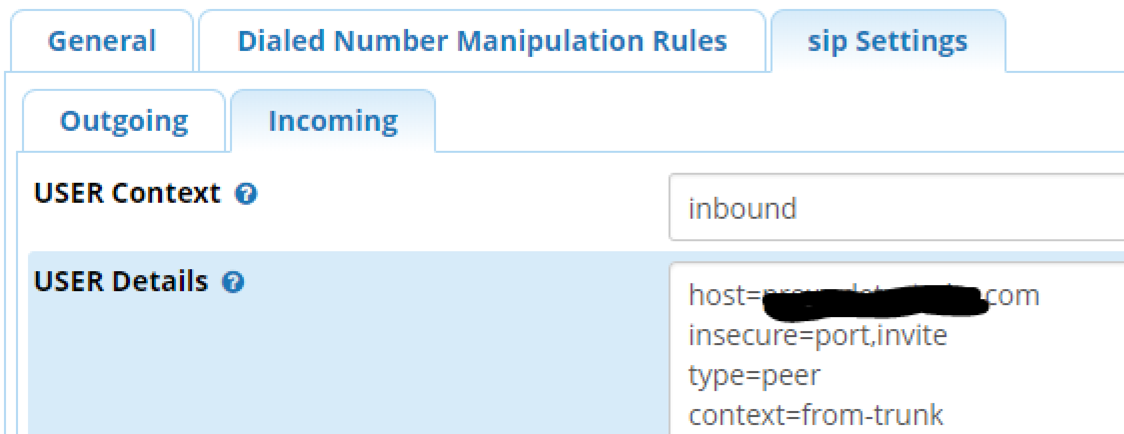


NOTE:** Type <context=from-trunk> underneath the <type=peer> in the Peer Details box if it does not appear.

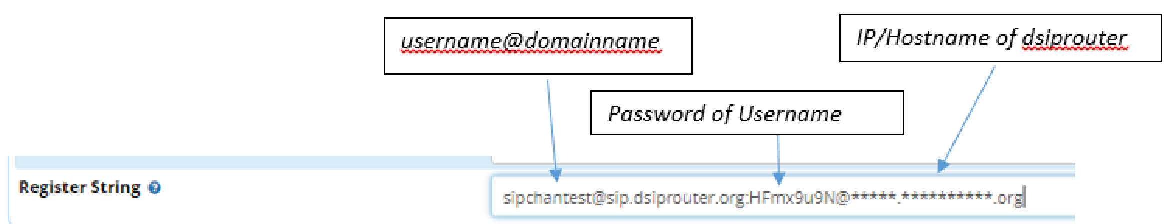
6. Next you will enter the configurations for incoming by selecting the **Incoming** tab in the SIP Settings. Here you will enter the SIP settings for inbound calls. You will need:

User Context: This is most often the account name or number your provider expects. In this example we named it "inbound". The following User Details needs to be entered:

Field	Value
Host	<host name or IP address of dsiprouter>
Insecure	port,invite
Type	peer
Context	from-trunk

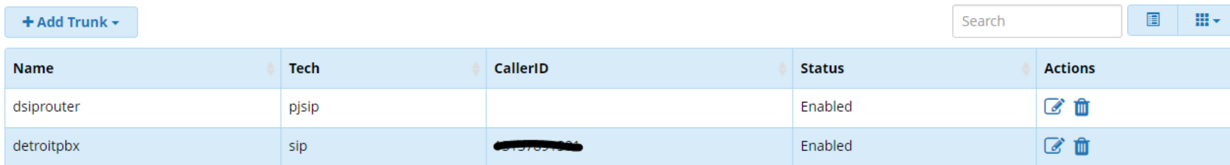


In the **Register String** enter: <username@domainname>:<password>@<ip address **or** hostname>. In this example it would be sipchantest@sip.dsiprouter.org:HFmx9u9N@demo.dsiprouter.org. **The domain name has to be included and correct.**



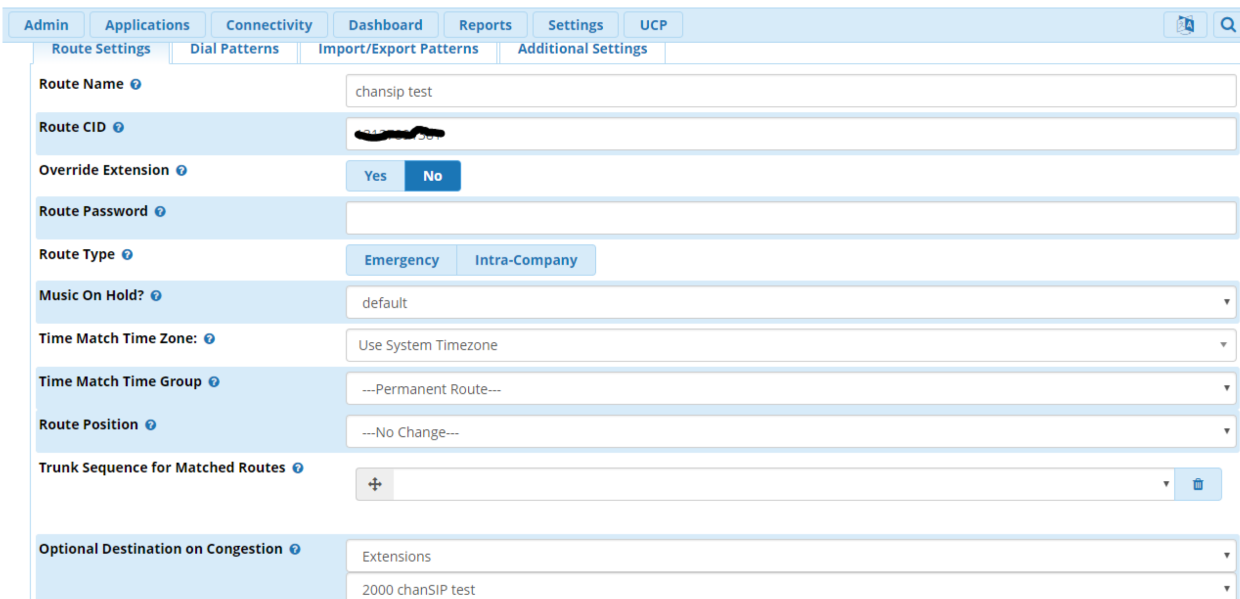
7. Click Submit
8. Be sure to click the **Apply Config** button after submitting to confirm.

You will now be able to see the new chanSIP added in the truck.

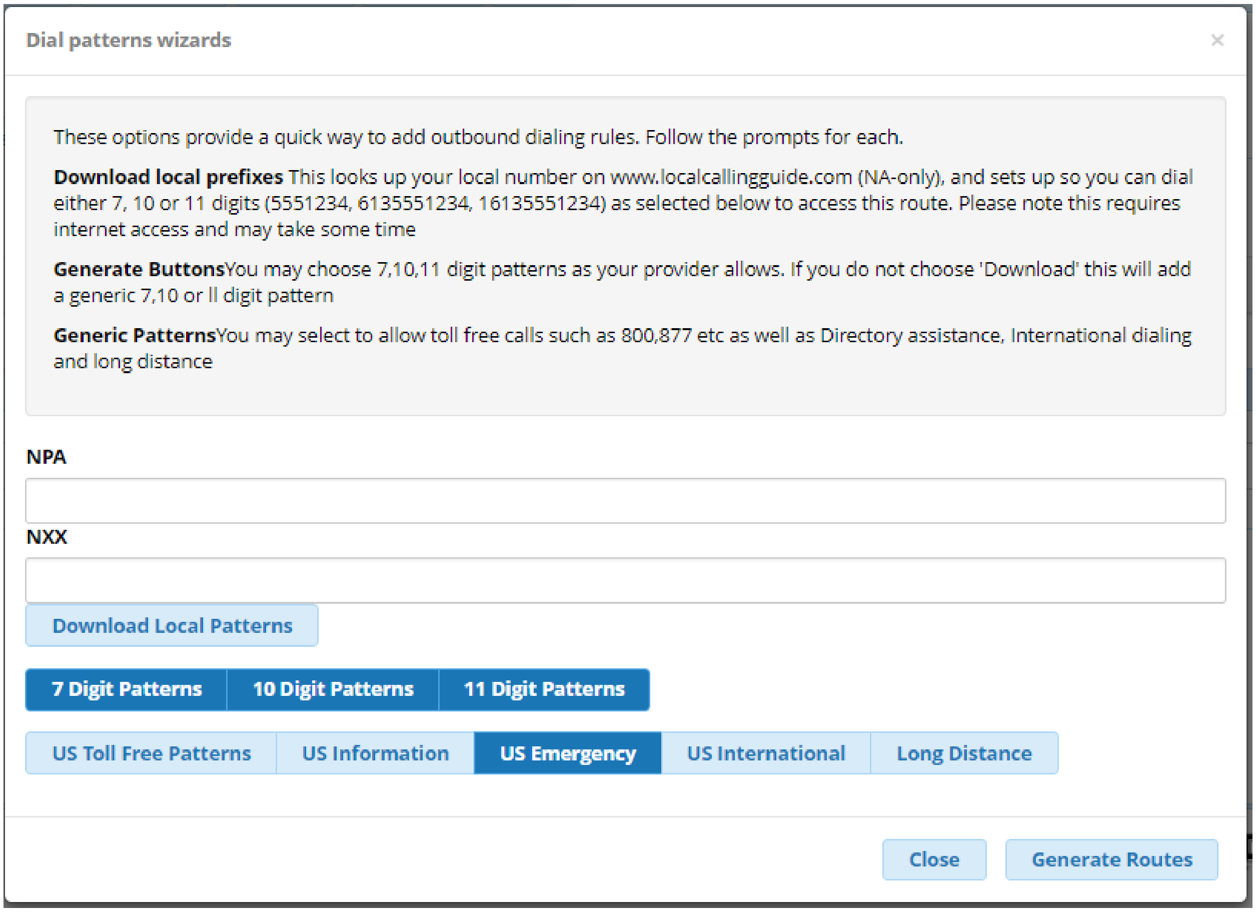


9. Next you will need to setup an outbound route. Select Connectivity→ Outbound Routes. Click the "+" sign to add a outbound route. In this tab you will need to enter:

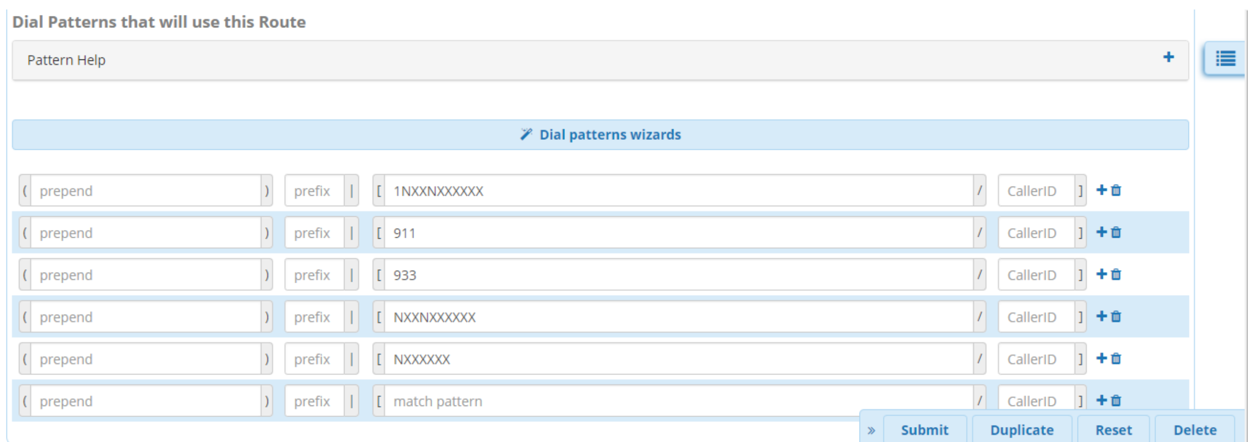
Field	Value
Route Name	Type desired name
Route CID	Number you want to appear on caller ID
Trunk Sequence for Matched Routes	Trunk name (select from drop down box)



10. Click the Dial Patterns tab to set the dial patterns. If you are familiar with dial patterns, you can enter the dial patterns manually or you can click the Dial Patterans Wizard to auto create dial patterns if you like. You can choose 7, 10 or 11 digit patterns. Click Generate Routes.



Dial pattern is set to your preference. Prefixes are optional, not required.

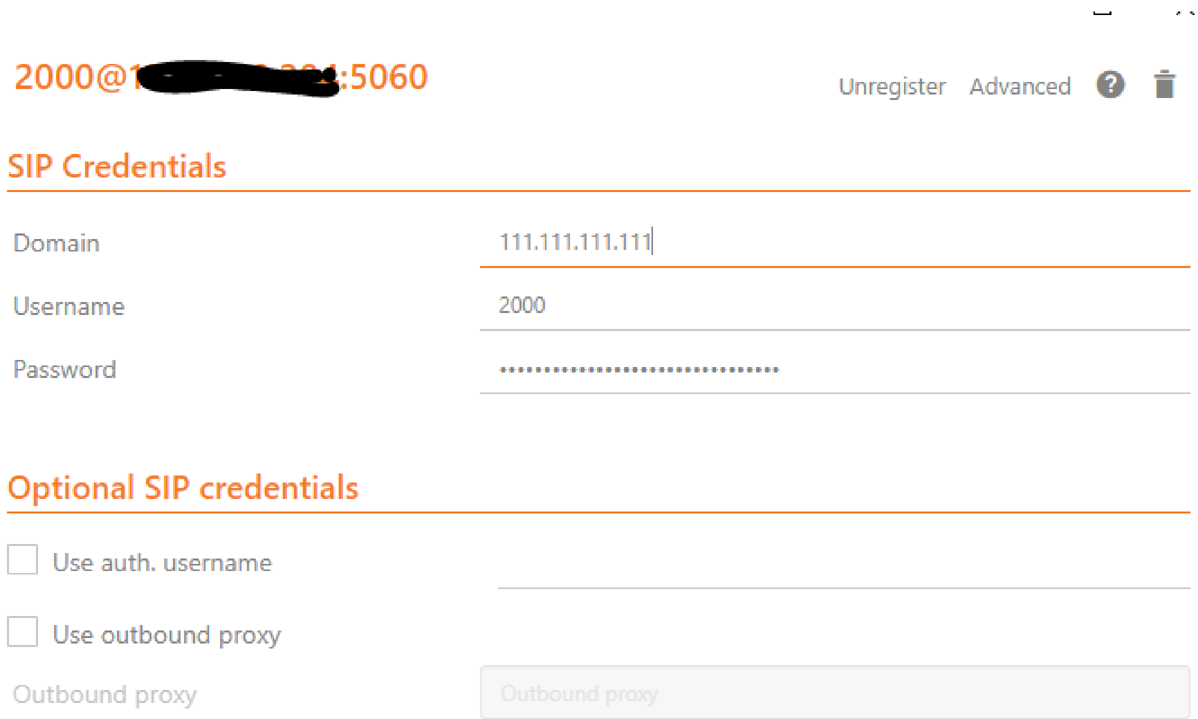


11. Click Submit and Apply Config button.

Assuming you already have an extention created in your FreePBX, you can validate incoming/outgoing calls by configuring a softphone or a hard phone. Below is an example of the information you would enter if you use a softphone: In this example we are using Zoiper. Once you've downloaded Zoiper application on your PC or smart device you would enter the following to configure the soft phone:

Field	Value
Username	<extension>@<siptrunkipaddress>
secret	<Password of that extension>
Hostname	<IP address of your FreePBX> (should autofill)

Note Skip Authenication and Outbound Proxy

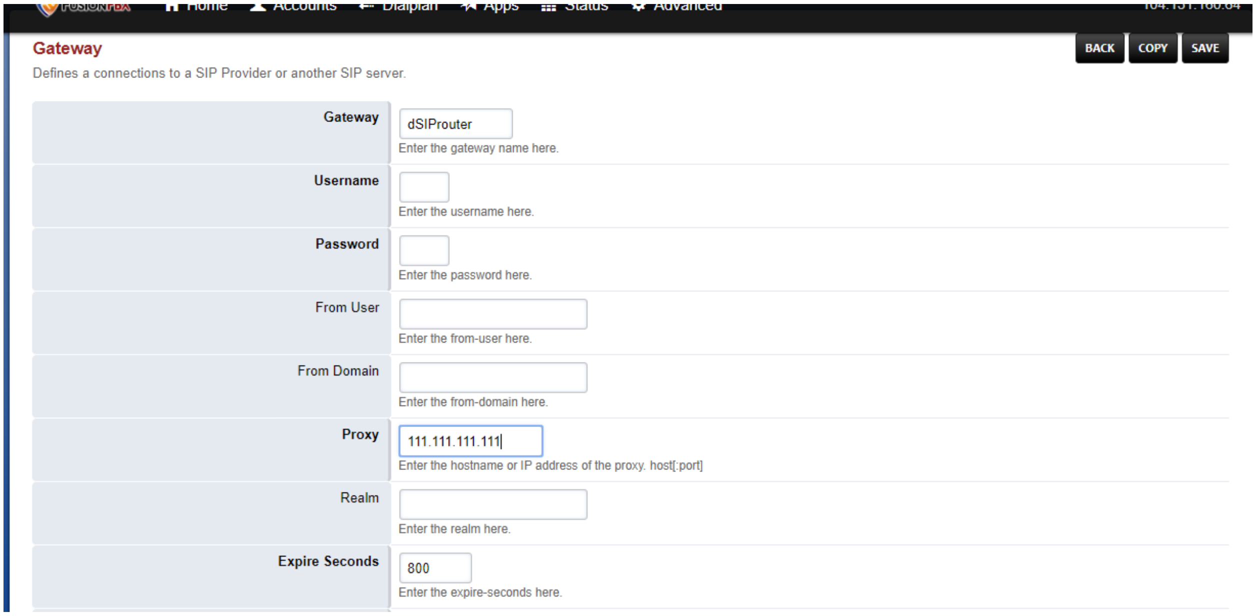


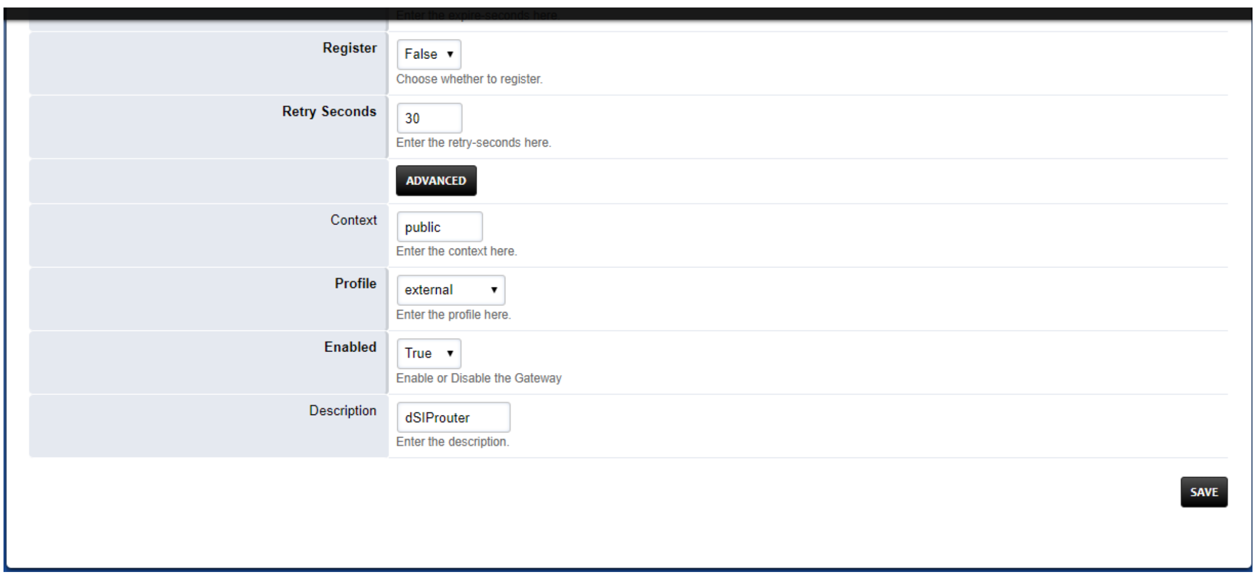
You should now be able to make a inbound and outbound call successfully!

4.1.5 Using SIP Trunking - FusionPBX IP Authenication

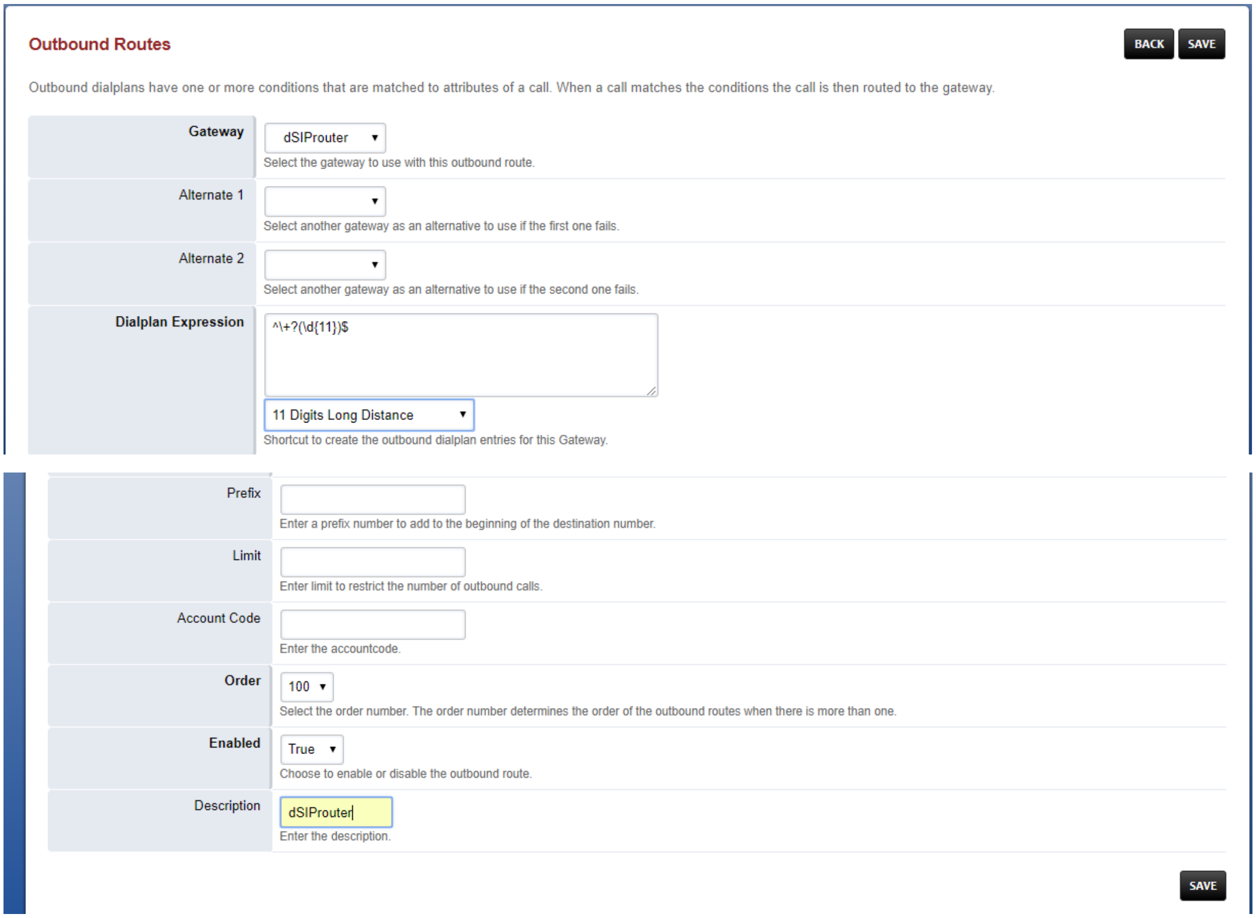
The following screenshot(s) shows how to configure a SIP trunk within FusionPBX for IP Authenication.

1. Log into your FusionPBX.
2. **Click Accounts –> Gateways–>Click the + sign to add a gateway/SIP Trunk. The only fields you will need to fill here are:**
    - Gateway= Name of the SIP Trunk
    - Proxy= IP address of the SIP trunk
    - Register= Change to False because you are using IP authenication

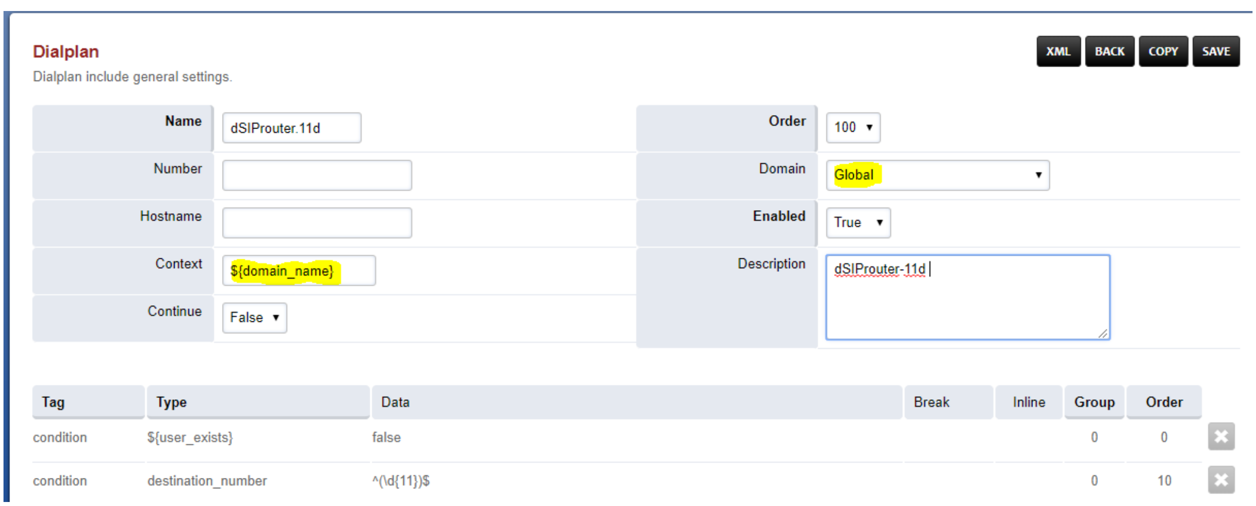




3. Click Save
4. **Click DialPlan–>Outboung Routes–>Click the + sign to add a outbound route. Here you will enter in the following fields:**
    - Gateway= Name of the SIP Trunk
    - Alternate gateways (if applicable)
    - DialPlan Expression= 11d (standard setup in FusionPBX). To change the dialplan expression click on the dropdown box where it says "Shortcut to create the outbound dialplan entries for this Gateway."
    - Description= (if desired)
5. Click Save



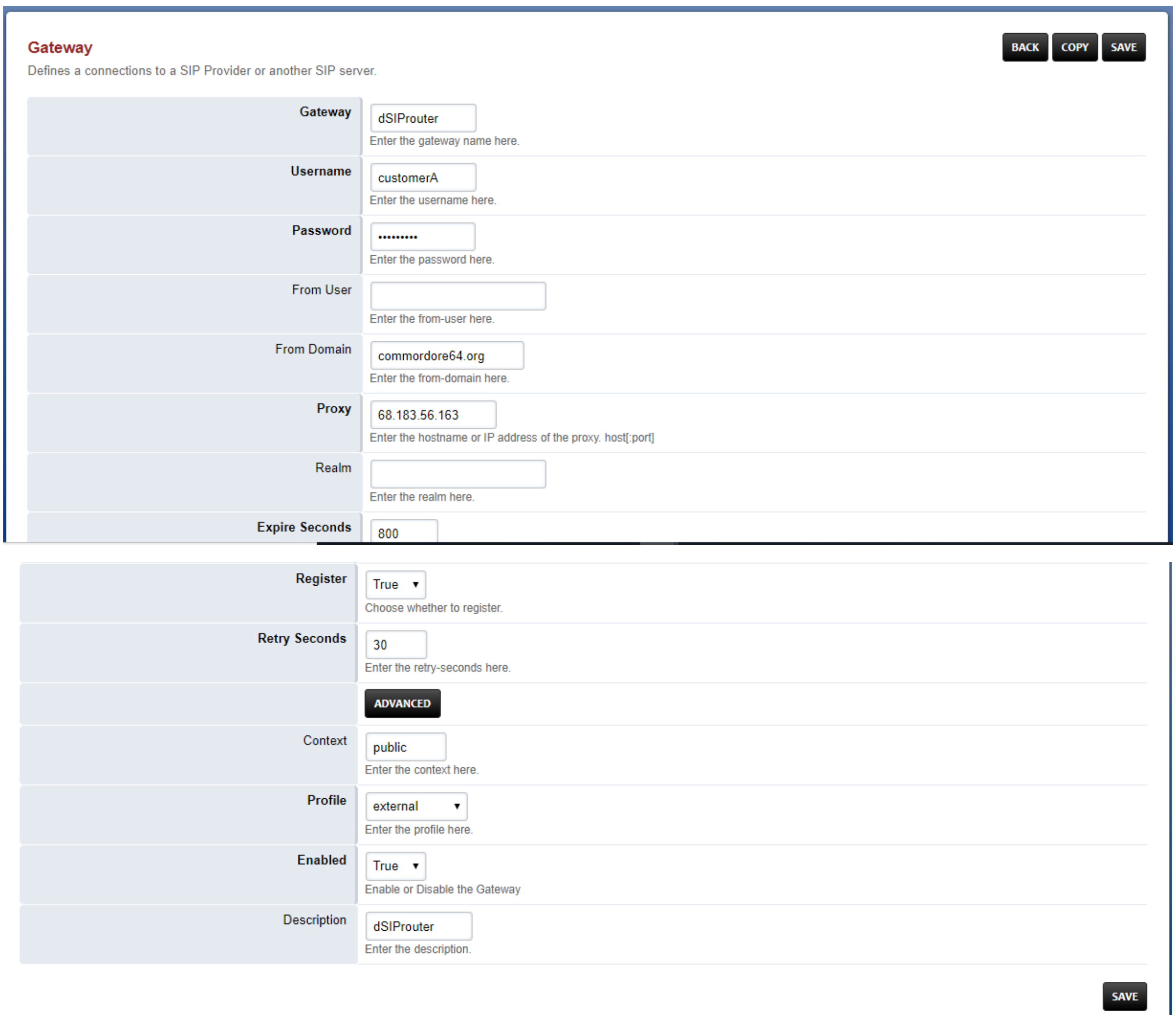
NOTE To make these changes global for ALL domains for this SIP Trunk: reopen outbound routes and change the Domain to Global and the Context to ${domain_name} as shown below.



4.1.6 Using SIP Trunking - FusionPBX Username/Password Authenication

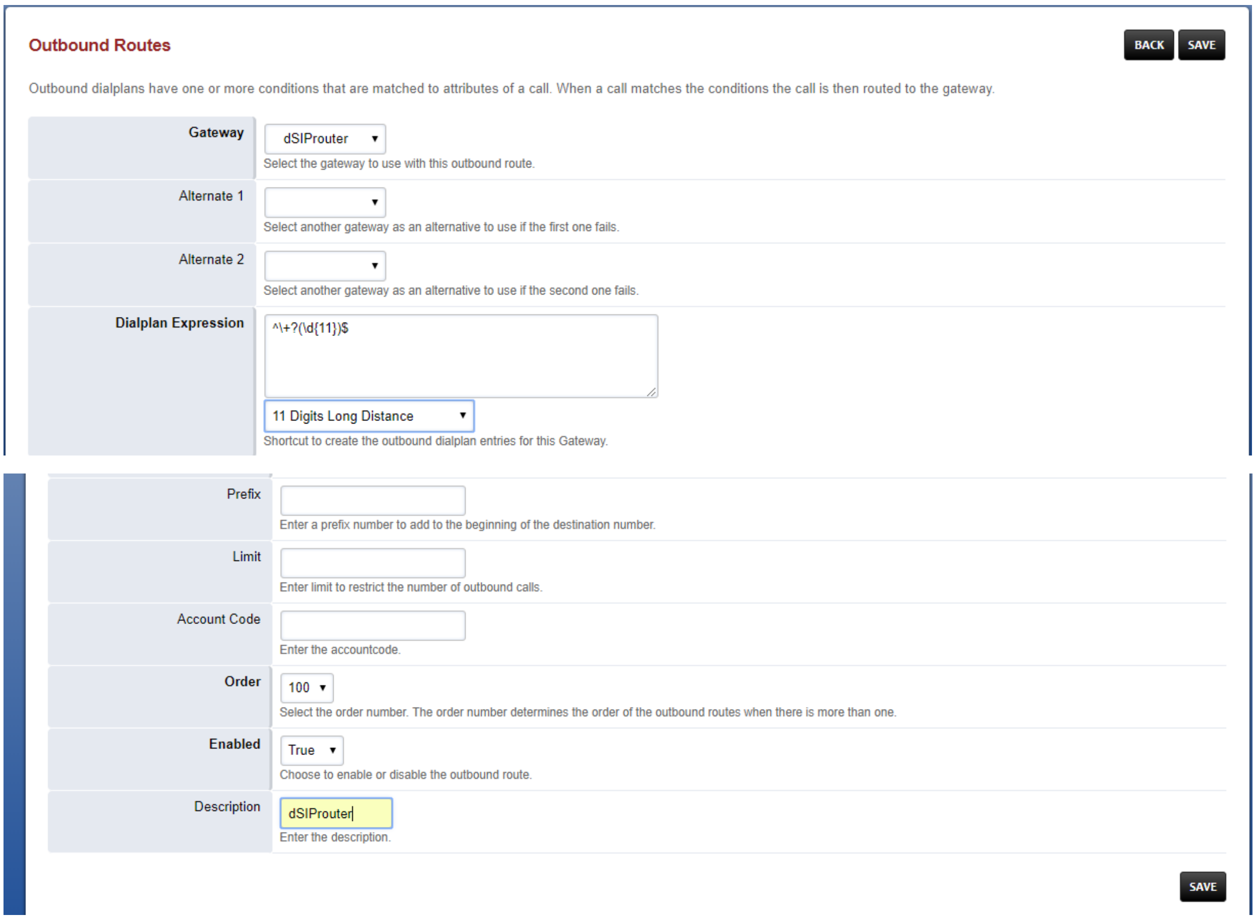
The following screenshot(s) shows how to configure a SIP trunk within FusionPBX for Username/Password Autheni-cation with IP Authenication off.

1. Log into your FusionPBX.
2. **Click Accounts –> Gateways–>Click the + sign to add a gateway/SIP Trunk. The following fields you will need to fill here are:**
    - Gateway= Name of the SIP Trunk
    - Username= specified by dSIPRouter provider
    - Password= specified by dSIPRouter provider
    - From Domain= Specified or set by default
    - Proxy= IP address of the SIP trunk
    - Register= set to True because you are using Username/Password authenication.



3. Click Save.

4. **Click DialPlan–>Outboung Routes–>Click the + sign to add a outbound route. Here you will enter in the following fields:**
    - Gateway= Name of the SIP Trunk
    - Alternate gateways (if applicable)
    - DialPlan Expression= 11d (standard setup in FusionPBX). To change the dialplan expression click on the dropdown box where it says "Shortcut to create the outbound dialplan entries for this Gateway."
    - Description= (if desired)



5. Click Save

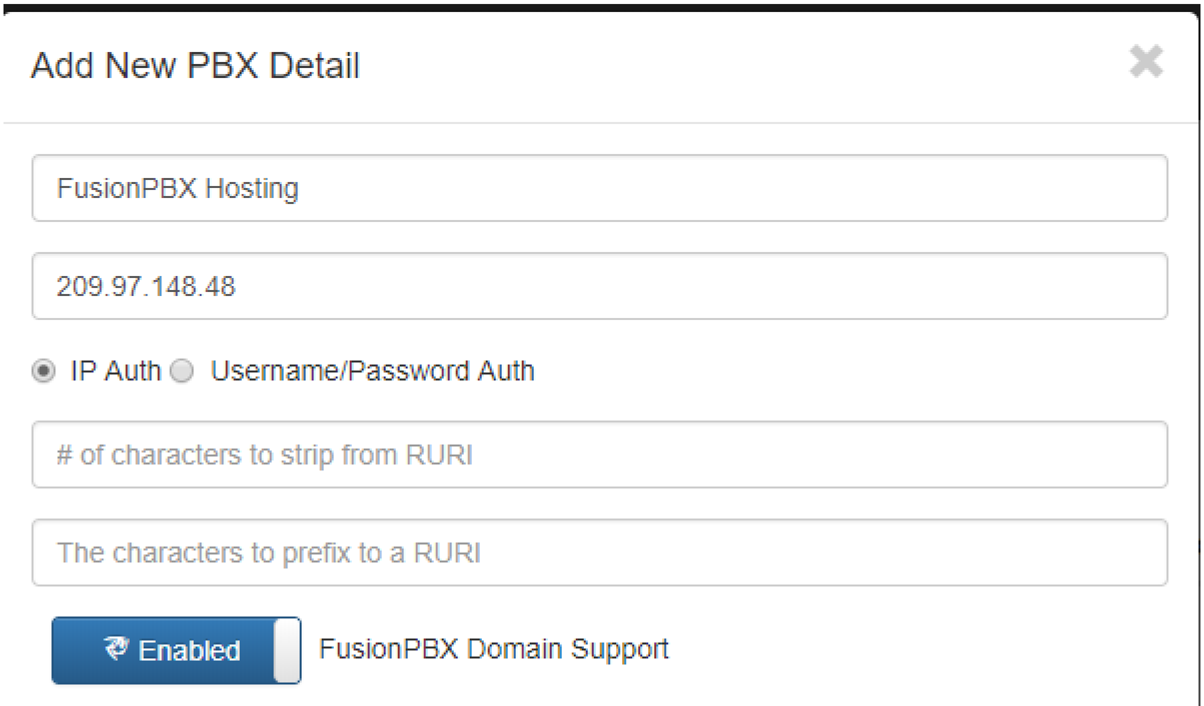
4.1.7 FusionPBX Hosting

Here we will demostrate how to setup dSIPRouter to enable hosting FusionPBX. We have built-in support for FusionPBX that allows domains to be dynamically pulled from FusionPBX.

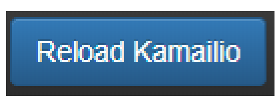
1. Login to dSIPRouter
2. Click PBX(s) and EndPoints
3. **Click ADD; enter the following fields**
    - Friendly Name (opional)
    - IP address

- IP Auth
- Click to enable FusionPBX Domain Support
- FusionPBX Database IP or Hostname

4. Click ADD

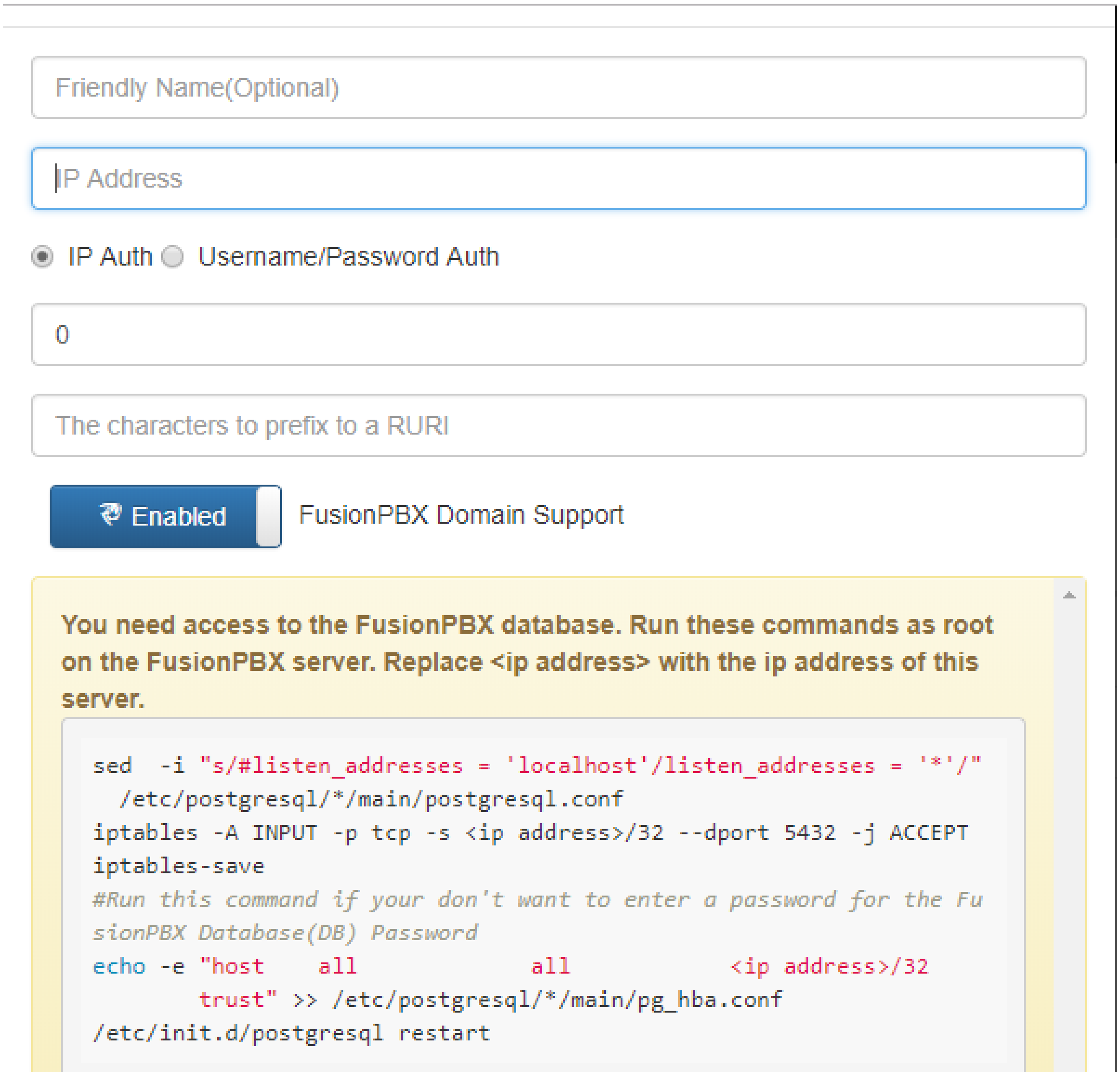


5. Click Reload Kamailio. (when changes are made reload button will change to orange)

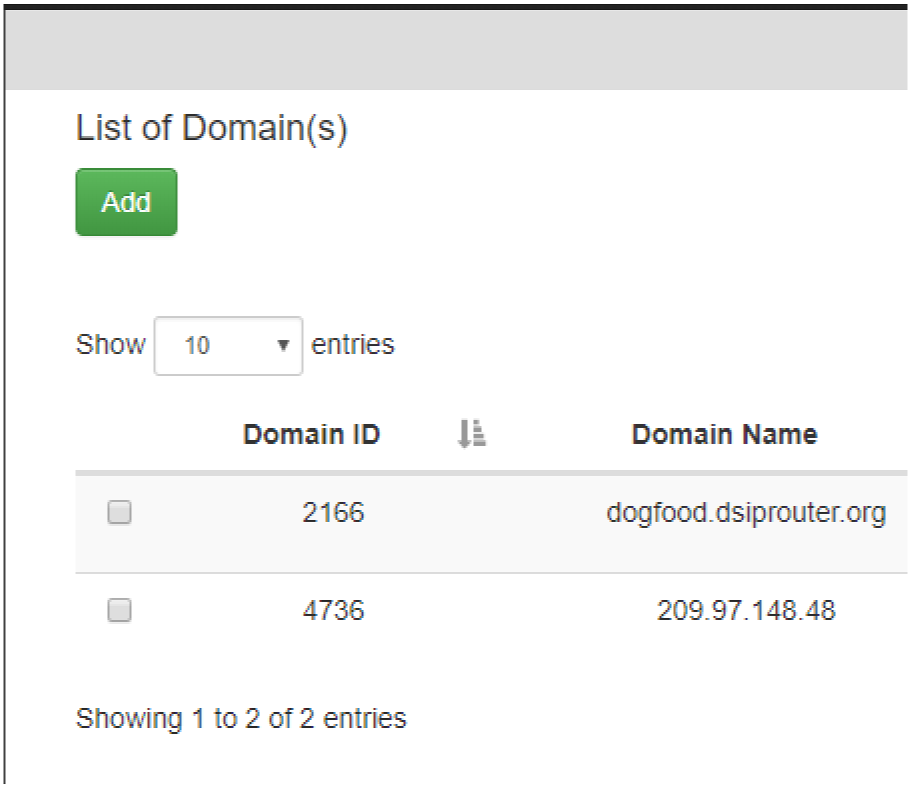


6. Access your FusionPBX database via ssh.
7. Run the command as illustrated in the "Edit your PBX Detail" window as root on the FusionPBX server. Replace <ip address> (not including the brackets) with the IP address of the dSIPRouter server you're adding. Command line will look simulair to the following picture.

NOTE After you have entered the first two lines of commands you will not see a form of reply. If command is entered correctly it will return back to your root line. If the command line is incorrect you will receive a "command not found" error message. Recheck the command line and IP address.



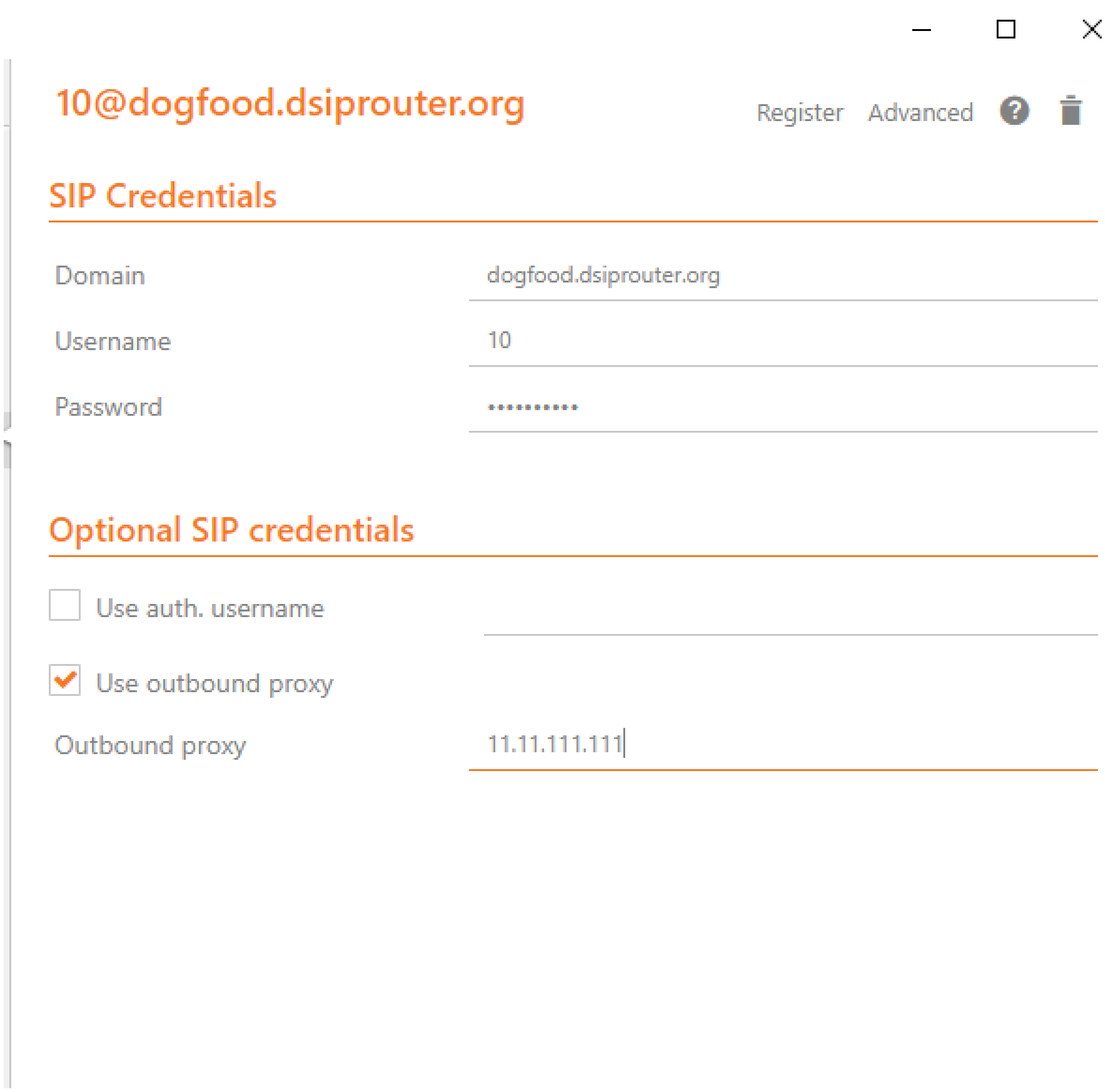
After the command is run you should now be able to see the domains of that PBX in dSIPRouter.



You can test PBX Hosting is valid by configuring a softphone or a hard phone. Below is an example using a softphone:

Now that domains have been synced in dSIPRouter you are able to register a softphone. In this example we are using Zoiper. Once you've downloaded Zopier appliaction on your PC or smart device you would add:

- username (extension@domainname)
- password (password of that extension)
- outbound proxy (IP address of the dSIPRouter)

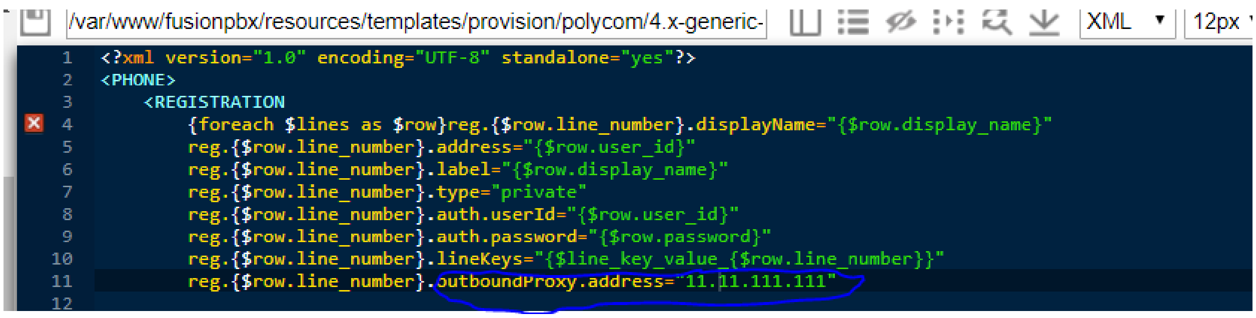


4.1.8 Provisioning and Registering a Polycom VVX Phone

Now that domains have been synced in dSIPRouter you are able to register a endpoint/hard-phone. In this example we are using a Polycom VVX410 desk phone.

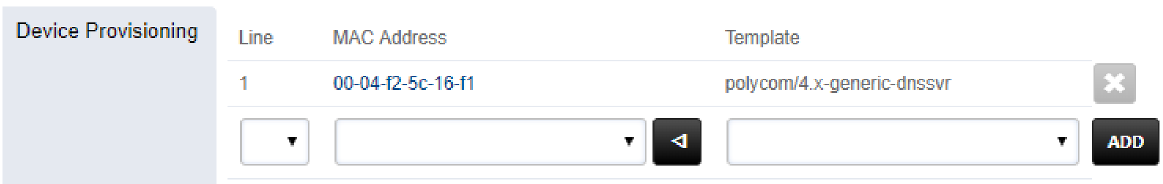
1. **Log into your FusionPBX box**

    a) Update the "outboundProxy.address" of the template with the IP address or hostname of the dSIPRouter in the provisioning editor.

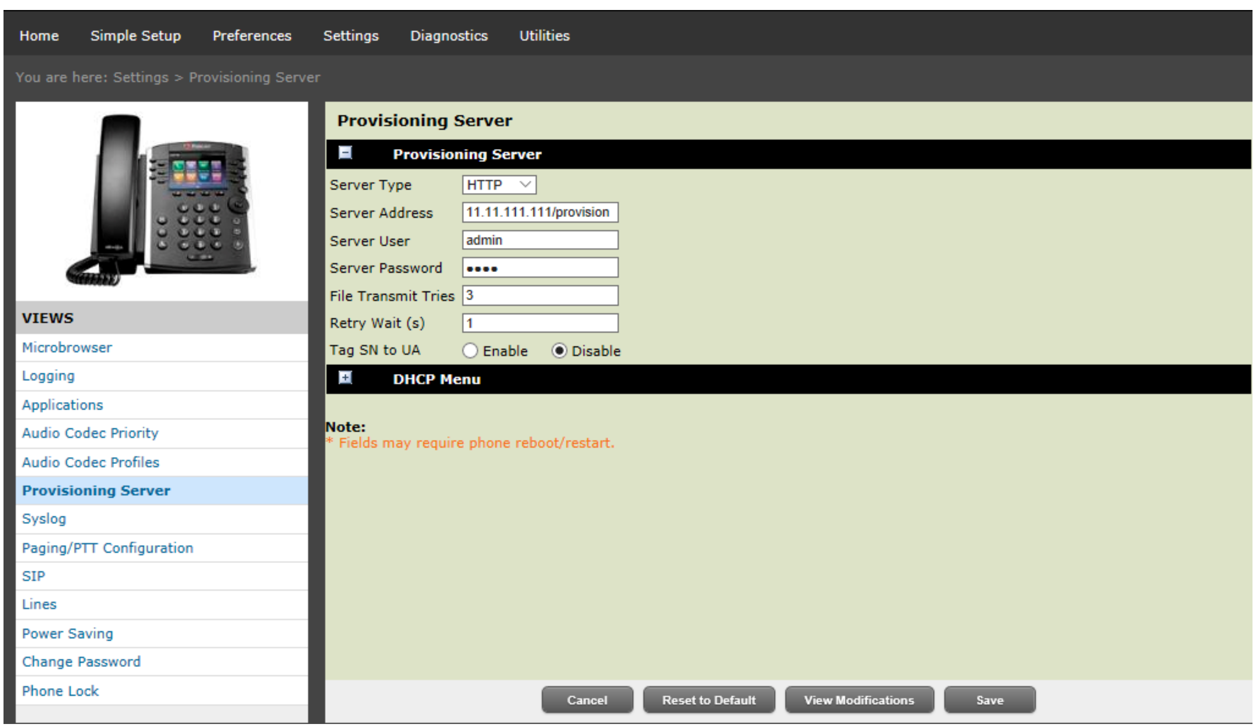



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<PHONE>
    <REGISTRATION
        {foreach $lines as $row}reg.{$row.line_number}.displayName="{$row.display_name}"
        reg.{$row.line_number}.address="{$row.user_id}"
        reg.{$row.line_number}.label="{$row.display_name}"
        reg.{$row.line_number}.type="private"
        reg.{$row.line_number}.auth.userId="{$row.user_id}"
        reg.{$row.line_number}.auth.password="{$row.password}"
        reg.{$row.line_number}.lineKeys="{$line_key_value_{$row.line_number}}"
        reg.{$row.line_number}.outboundProxy.address="11.11.111.111"
```

2. Assign the phone to a template.



3. **Configuring the Provisioning Server section of the phone. Enter the appropriate information into the fields.**
    a) Server Type (dSIPRouter uses HTTP by default)
    b) Server Address
    c) Server Username (device provisioning server name)
    d) Server Password
4. Click Save



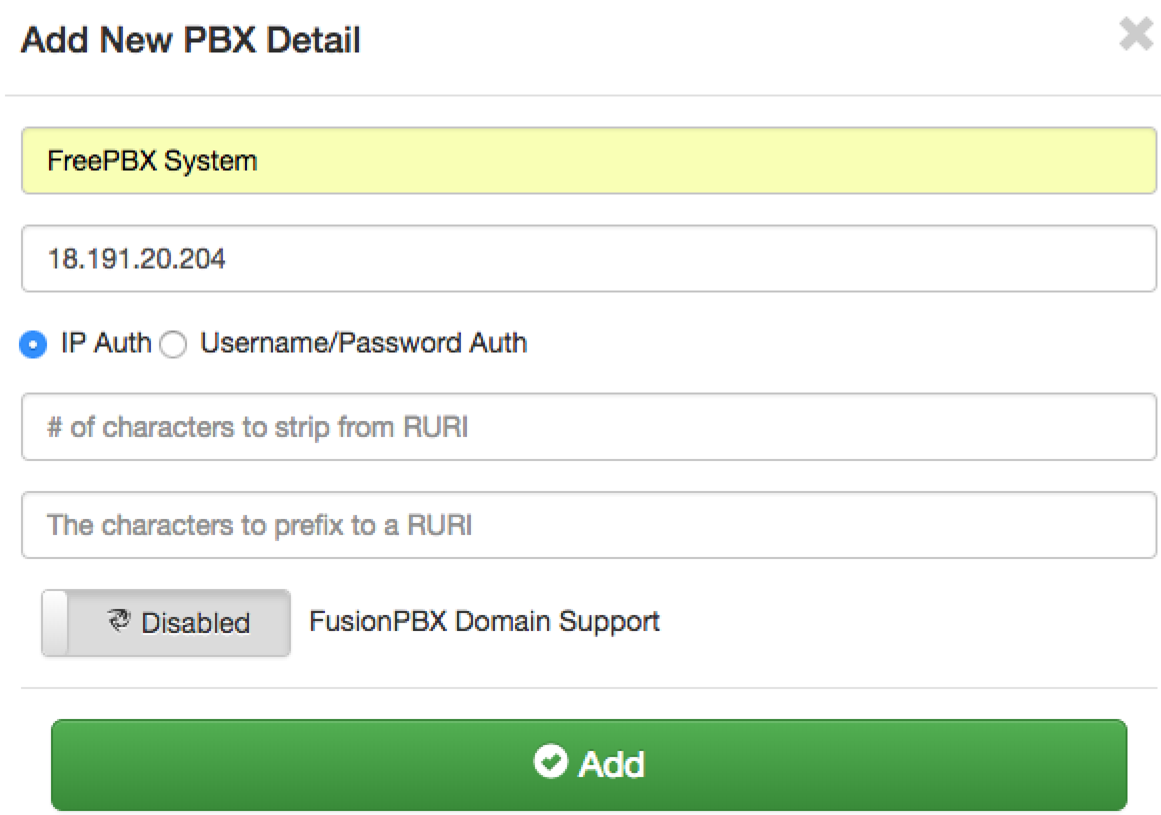
5. Reboot the phone

4.1.9 FreePBX Hosting - Pass Thru Authentication

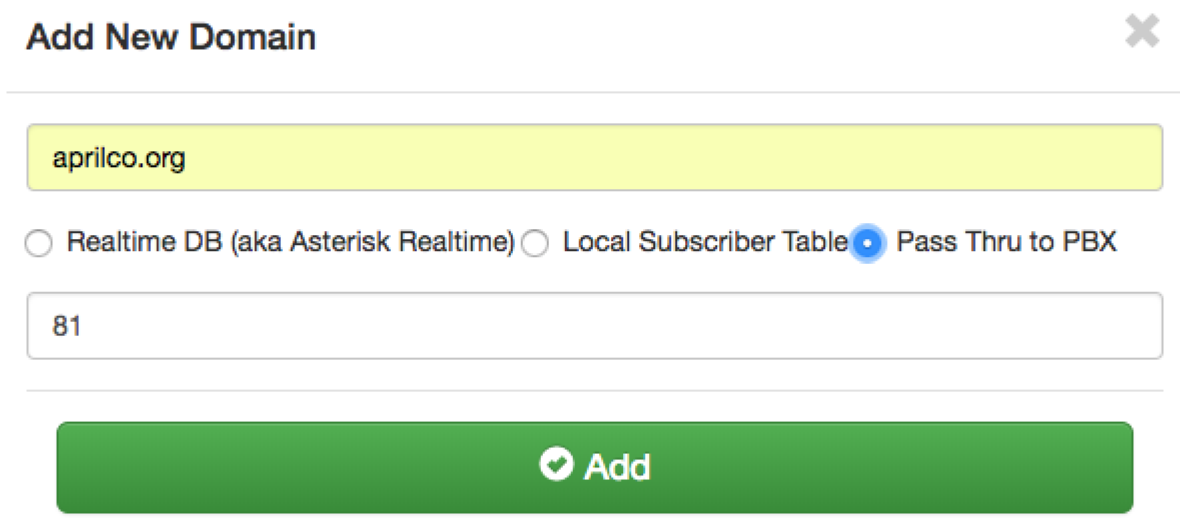
Here we will demostrate how to setup dSIPRouter to enable hosting FreePBX using Pass Thru Authentication. FreePBX is designed to be a single tenant system or in other words, it was built to handle one SIP Domain. So, we use dSIPRouter to define a SIP Domain and we pass thru Registration info to the FreePBX server so that you don't have to change how authentication is done. However, this will only work for one FreePBX server. If you have a cluster of FreePBX servers then use "Local Subscriber Table" authentication. The value of having dSIPRouter in front of FreePBX is to provide you with flexibility. After setting this up you will have the ability upgrade or migrate users from one FreePBX instance to another without having to take an outage. The following video shows how to configure this. The steps to implement this is below the video.

Steps to Implement

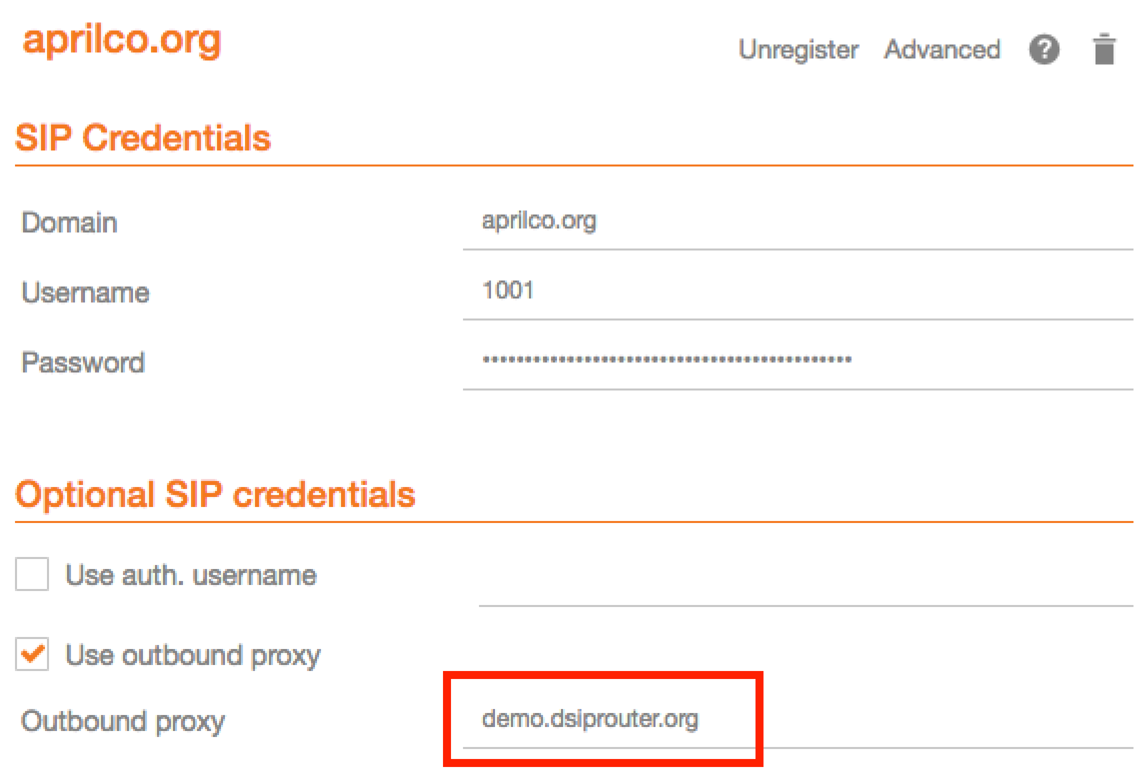
1. Click PBX and Endpoints
2. Click Add



3. Reload Kamailio
4. Click Domains
5. Click Add



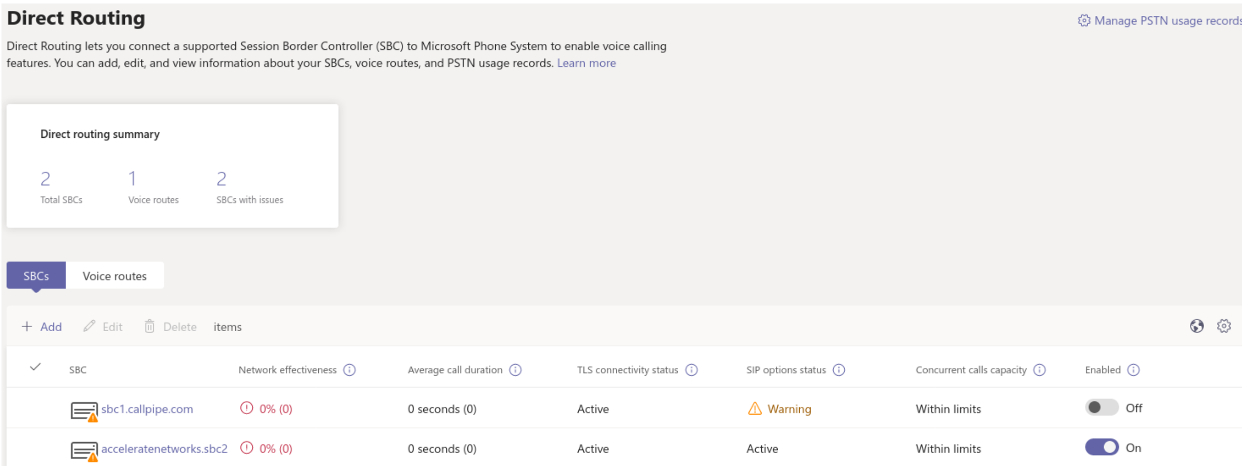
6. Reload Kamailio
7. Register a phone via dSIPRouter - notice that we used the hostname of dSIPRouter as the Outbound Proxy. This forces the registration thru the proxy.



4.1.10 Microsoft Teams Direct Routing (SUBSCRIPTION REQUIRED)

dSIPRouter can act as an intermediary Session Border Controller between Microsoft Teams Direct Routing and your SIP provider or SIP servers.

An instance of dSIPRouter can either be a single tenant configuration (like sbc.example.com) or multi-tenant under a single wildcard subdomain (like *.sbc.example.com where * is the tenant's name).



Steps to Implement

1. Buy a license and follow the license installation instructions that are emailed to you.
2. Add any carriers you need for inbound and outbound routing, define appropriate routes.
3. Authorize your SBC's domain with Microsoft 365 by adding a TXT record starting with ms= per Microsoft's documentation. Note: For multi-tenant use, authorizing the root subdomain or domain (if you use *.sbc.example.com, you would authorize sbc.example.com) should avoid the need to authorize each subdomain below this (like clientname.example.com)
4. Create a global admin user with proper Teams licensing associated with the domain (or for multi-tenant both the root subdomain (eg: sbc.example.com) and client's domain (eg: client.sbc.example.com))
5. Add the Teams session border controller in Teams Admin Center. Ensure the SIP port is correct (usually 5061) and the SBC is enabled!
6. Install PowerShell type pwsh then:

```
Install-Module -Name MicrosoftTeams
Import-Module MicrosoftTeams
$userCredential = Get-Credential
Connect-MicrosoftTeams -Credential $userCredential
```

Login Note:

If your using multi-factor authentication (MFA/2FA), log in by typing Connect-MicrosoftTeams

Debian 10 Note:

If you run into this OpenSSL issue , here is a workaround! **Replace sbc.example.com, user@example.com and +13137175555** with your SBC's FQDN, the user's email address and their phone number (with + then country code, use +1 if you are in the North American Numbering Plan)

```
Set-CsOnlinePstnUsage -Identity Global -Usage @{Add="US and Canada"}
Set-CsOnlineVoiceRoute -Identity "LocalRoute" -NumberPattern ".*" -OnlinePstnGatewayList␣
↪sbc.example.com
New-CsOnlineVoiceRoutingPolicy "US Only" -OnlinePstnUsages "US and Canada"

# This is suppose to stop MSTeams from using the Microsoft Dialing Plan and using the␣
↪routing policies that was defined above
Set-CsTenantHybridConfiguration -UseOnPremDialPlan $False

# Apply and the US Only Voice Routing Policy to the user
Grant-CsOnlineVoiceRoutingPolicy -Identity “user@example.com“ -PolicyName "US Only"

# If it doesn't return a value of US Only, then wait 15 minutes and try it again.  It␣
↪sometime takes a while for the policy to be ready.
Get-CsOnlineUser “user@example.com" | select OnlineVoiceRoutingPolicy

# Define a outgoing phone number (aka DID) and set Enterprise Voice and Voicemail
Set-CsUser -Identity "user@example.com" -OnPremLineURI tel:+13137175555 -
↪EnterpriseVoiceEnabled $true -HostedVoiceMail $true
```

Note: Log out by typing `Disconnect-MicrosoftTeams`

Credits to Mack at dSIPRouter for the SkypeForBusiness script and this blog post for helping me update these commands for the new MicrosoftTeams PowerShell module.

Add a single Teams User

If you have an existing dSIPRouter SBC configured in Teams and have added a DID as an inbound route already, then run the commands below in PowerShell to add an additional user.

Replace user@example.com and +13137175555 with your SBC's FQDN, the user's email address and their phone number (with + then country code, use +1 if you are in the North American Numbering Plan)

```
# Get Credentials, if using MFA/2FA just run Connect-MicrosoftTeams
$userCredential = Get-Credential
Connect-MicrosoftTeams -Credential $userCredential

# Apply and the US Only Voice Routing Policy to the user
Grant-CsOnlineVoiceRoutingPolicy -Identity “user@example.com“ -PolicyName "US Only"

# Define a outgoing phone number (aka DID) and set Enterprise Voice and Voicemail
Set-CsUser -Identity "user@example.com" -OnPremLineURI tel:+13137175555 -
↪EnterpriseVoiceEnabled $true -HostedVoiceMail $true
```

Note: Log out by typing `Disconnect-MicrosoftTeams`

4.1.11 Configure STIR/SHAKEN (SUBSCRIPTION REQUIRED)

dSIPRouter enables an organization to start signing calls by enabling the STIR/SHAKEN module. This module will sign outbound calls and validate that inbound calls are signed. It also have the ability to add a prefix to the callerid if calls have an attestion of an A, B or C. You can also specify a callerid prefix if callers aren't validated. Lastly, you have the option to block invalidated callers.

1. Login to dSIPRouter
2. Purchase a license from the dSIPRouter Marketplace
3. Click System Settings -> License Manager
4. Add the license to the system
5. If testing, connect to your dSIPRouter instance using ssh, run the command below and enter the requested information to create a self-signed certificate

```
/opt/dsiprouter/resources/stir_shaken/generate_self_signed_cert.sh
```

If not testing, obtain a valid STIR/SHAKEN certificate and place them in the /etc/dsiprouter/certs/stirshaken/ directory. For the purpose of these instructions, please name the certificate sp-cert.pem and name the key sp-key.pem

6. Check that the certificate can be accessed via https. Open a web browser and enter the following into the URL. This will be used by other VoIP servers to validate the signature of the the call.

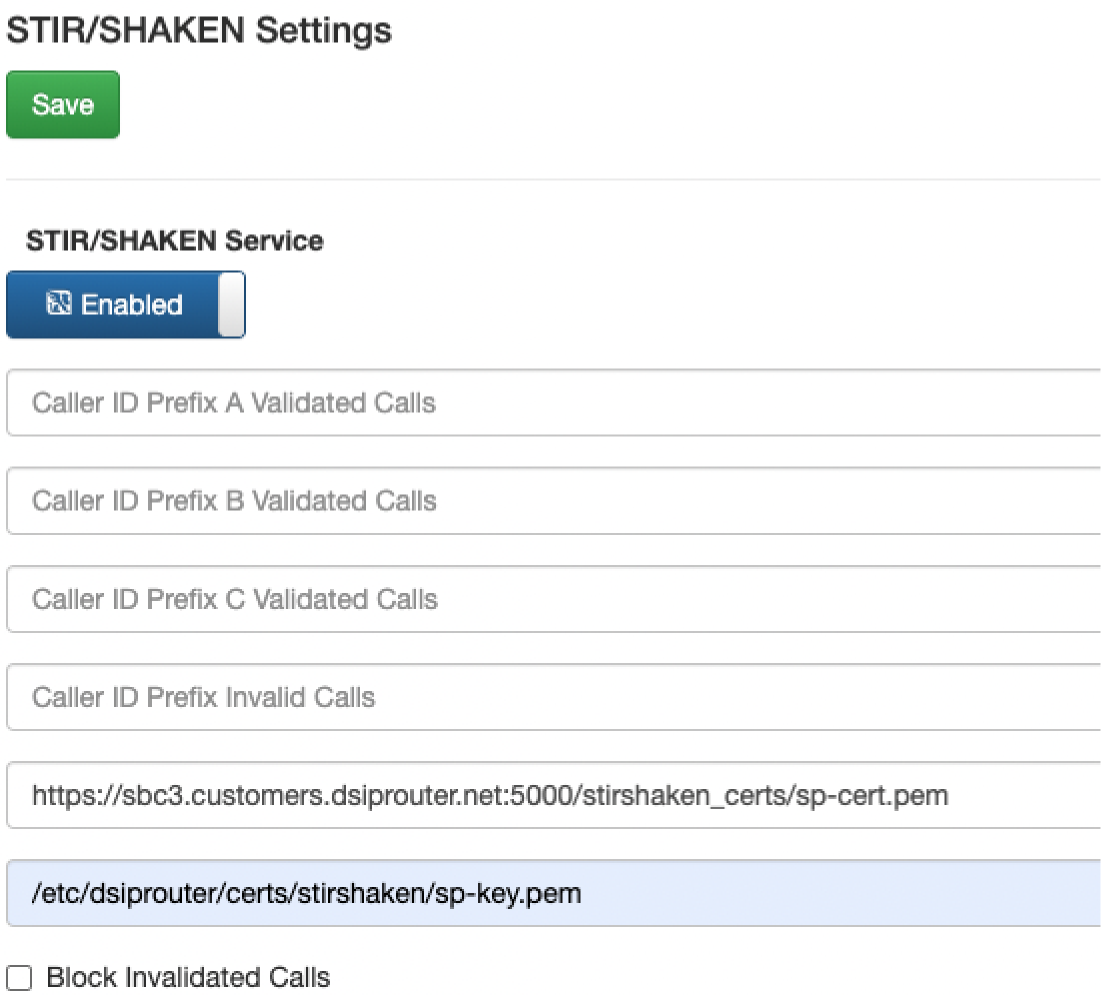
```
https://<replace with ip or hostname>:5000/stirshaken_certs/sp-cert.pem
```

7. Click System Settings -> STIR/SHAKEN
8. Slide the Disabled toggle to Enabled
9. Enter the Certificate URL from Step 6
10. Enter the Key Path, which by default will be

```
/etc/dsiprouter/certs/stirshaken/sp-key.pem
```

11. Click Save

The STIR/SHAKEN page should look like this:


STIR/SHAKEN Settings
Save
STIR/SHAKEN Service
Enabled
Caller ID Prefix A Validated Calls
Caller ID Prefix B Validated Calls
Caller ID Prefix C Validated Calls
Caller ID Prefix Invalid Calls
https://sbc3.customers.dsiprouter.net:5000/stirshaken_certs/sp-cert.pem
/etc/dsiprouter/certs/stirshaken/sp-key.pem
Block Invalidated Calls

CHAPTER

FIVE

REST API

5.1 dSIPRouter API Intro

The complete API is defined as a public Postman Workspace, which can be found here

The steps to obtain the API Token key and examples of using the API via curl are below, but we highly recommend using Postman for testing the API.

5.1.1 Getting Your Token

Your token was provided to you after you installed dSIPRouter. You can reset your token if you didn't write it down, by executing the following command

```
DSIP_HOSTNAME=<your ip or hostname>
DSIP_TOKEN=<your token>
dsiprouter setcredentials -ac $DSIP_TOKEN
```

5.1.2 Executing Kamailio stats API

```
curl -k -H "Authorization: Bearer $DSIP_TOKEN" -X GET https://$DSIP_HOSTNAME:5000/api/v1/
↪kamailio/stats
```

5.1.3 Executing Lease Point API

Create a new endpoint lease

```
curl -k -H "Authorization: Bearer $DSIP_TOKEN" -H "Content-Type: application/json" -X␣
↪GET "https://$DSIP_HOSTNAME:5000/api/v1/endpoint/lease?ttl=15&email=mack@dsiprouter.org
↪"
```

Revoking and replacing with your own lease ID

```
curl -k -H "Authorization: Bearer $DSIP_TOKEN" -H "Content-Type: application/json" -X␣
↪PUT "https://$DSIP_HOSTNAME:5000/api/v1/endpoint/lease/1/revoke"
```

Further Reading

All available routes are documented in the routes documentation.

CHAPTER

SIX

SUPPORTED CONFIGURATIONS

6.1 Supported Configurations

6.1.1 Pass Thru to PBX Authentication Supported Configurations

PBX Distribution	PBX Version	Driver Type	Registration Test	Ext to Ext Test	Notes
FreePBX	Asterisk 13.22.0	chan_sip	Pass	Pass	see *Enabling the Path Header for Asterisk chan_sip*
FreePBX	Asterisk 13.22.0	chan_pjsip	Pass	Not Tested	suppport_path needs to be enabled
FusionPBX	FreeSWITCH 1.6	Sofia	Pass	Pass	

6.1.2 Enabling the Path Header for Asterisk chan_sip

1. Login into the FreePBX Admin GUI
2. Click Settings -> Asterisk SIP Settings
3. Click Chan SIP Settings
4. Find the "Other SIP Settings" field
5. Add the following field and click "Add Field"

   supportpath = yes
6. Click Submit
7. Click the red "Apply" settings button at the very top of the page

CHAPTER

SEVEN

TROUBLESHOOTING

7.1 Troubleshooting

Here you can troubleshoot logs for dSIPRouter, Kamailio and rtpengine:

All of our services are using syslog. For more information on syslog click here.

Default log facilities:

Log Facility	Service
local0	kamailio
local1	rtpengine
local2	dsiprouter

7.1.1 Kamailio Logging

1. How to turn logging on

Edit /etc/rsyslog.d/kamailio.conf and ensure the line beginning with local0 is not commented out:

```
vi /etc/rsyslog.d/kamailio.conf
```

Then restart syslog:

```
systemctl restart rsyslog
```

2. How to turn logging off

Edit /etc/rsyslog.d/kamailio.conf and ensure the line beginning with local0 is commented out:

```
vi /etc/rsyslog.d/kamailio.conf
```

Then restart syslog:

```
systemctl restart rsyslog
```

3. Location of the log files

The default location is found here: /var/log/kamailio.log

4. How to configure it

Edit /etc/kamailio/kamailio.conf and change the variable ‘debug’ to the syslog logging verbosity of your choice.

```
vi /etc/kamailio/kamailio.conf
```

5. For more information see the documentation below:

https://www.kamailio.org/wiki/tutorials/3.2.x/syslog

7.1.2 RTPEngine Logging

1. How to turn logging on

Edit /etc/rsyslog.d/rtpengine.conf and ensure the line beginning with local1 is not commented out:

```
vi /etc/rsyslog.d/rtpengine.conf
```

Then restart syslog:

```
systemctl restart rsyslog
```

2. How to turn logging off

Edit /etc/rsyslog.d/rtpengine.conf and ensure the line beginning with local1 is commented out:

```
vi/etc/rsyslog.d/rtpengine.conf
```

Then restart syslog:

```
systemctl restart rsyslog
```

3. Location of the log files

The default location is found here: /var/log/rtpengine.log

4. How to configure it

Edit /etc/rtpengine/rtpengine.conf and change the variable 'debug' to the syslog logging verbosity of your choice.

```
vi /etc/rtpengine/rtpengine.conf
```

5. For more information see the documentation below:

https://github.com/sipwise/rtpengine

7.1.3 dSIPRouter Logging

1. How to turn logging on

Edit /etc/rsyslog.d/dsiprouter.conf and ensure the line beginning with local2 is not commented out:

```
vi /etc/rsyslog.d/dsiprouter.conf
```

Then restart syslog:

```
systemctl restart rsyslog
```

2. How to turn logging off

Edit /etc/rsyslog.d/dsiprouter.conf and ensure the line beginning with local2 is commented out:

```
vi /etc/rsyslog.d/dsiprouter.conf
```

Then restart syslog:

```
systemctl restart rsyslog
```

3. Location of the log files

The default location is found here: /var/log/dsiprouter.log

4. How to configure it

Edit /etc/dsiprouter/gui/settings.py and change the variable 'DSIP_LOG_LEVEL' to the syslog logging verbosity of your choice.

```
vi /etc/dsiprouter/gui/settings.py
```

5. For more infornation see the documentation below:

https://success.trendmicro.com/solution/TP000086250-What-are-Syslog-Facilities-and-Levels

CHAPTER

EIGHT

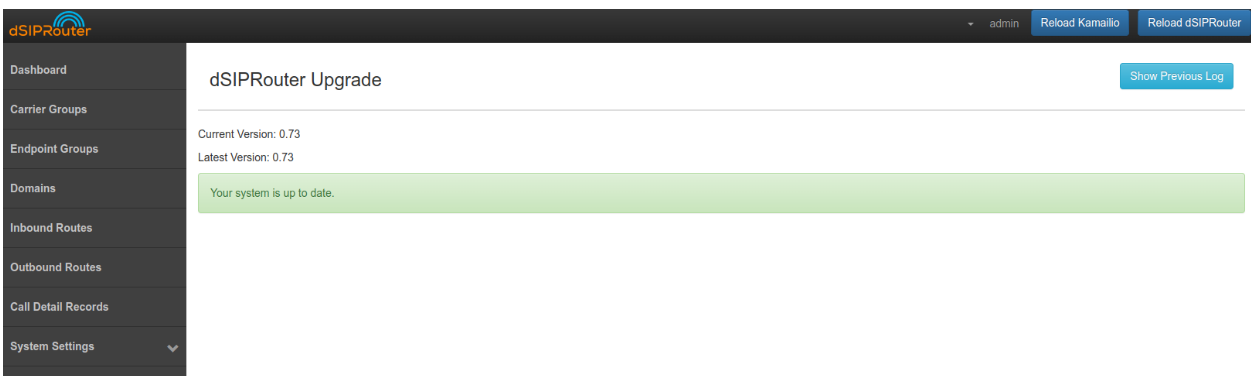
UPGRADING DSIPROUTER

8.1 Upgrading dSIPRouter

8.1.1 Auto Upgrade Feature

The dSIPRouter auto upgrade feature was released in 0.72 but was not feature complete until 0.73. It allows you to upgrade dSIPRouter from the User Interface (UI) and the command line (CLI). If you are upgrading from 0.70, 0.72, or 0.721 you can boostrap to the latest release to get the auto-upgrade feature.

Upgrading to 0.73 doesn't require a dSIPRouter Core Subscription license because the auto-upgrade framework was not yet feature complete. However, future releases of dSIPRouter will require a Core Subscription License to use the auto-upgrade feature. A core license can be purchased from the dSIPRouter Marketplace.



8.1.2 Upgrade 0.72x to 0.73

Upgrading to 0.73 can be done from 0.72 or 0.721 by doing the following

1. SSH to your dSIPRouter Instance
2. Run the following command

```
curl -s https://raw.githubusercontent.com/dOpensource/dsiprouter/v0.73/resources/upgrade/
↪v0.73/scripts/bootstrap.sh | bash
```

3. Login to the dSIPRouter UI to validate that the upgrade was successful.

Note, if you are upgrading from a debian 9 system you must first upgrade OS versions to a supported version. See the debian upgrade documentation for more information.

Note, if the upgrade fails you can purchase a dSIPRouter Core Subscription from the dSIPRouter Marketplace. This will provide you with support hours so that we can help with the upgrade.

8.1.3 Upgrade 0.70 to 0.721

You can upgrade from 0.70 by doing the following

1. SSH to your dSIPRouter Instance
2. Run the following command

```
curl -s https://raw.githubusercontent.com/dOpensource/dsiprouter/v0.721/resources/
↪upgrade/v0.721/scripts/bootstrap.sh | bash
```

3. Login to the dSIPRouter UI to validate that the upgrade was successful.

Note, if the upgrade fails you can purchase a dSIPRouter Core Subscription which can be purchased from the dSIPRouter Marketplace. This will provide you with support hours so that we can help with the upgrade.

8.1.4 Upgrade 0.70 to 0.72

This upgrade path is deprecated. Upgrade to the **0.721** release instead.

8.1.5 Upgrade 0.644 to 0.70

There is no automated upgrade available from 0.644 to 0.70. Support is available via a dSIPRouter Core Subscription which can be purchased from the dSIPRouter Marketplace.This will provide you with support hours so that we can help with the upgrade.

8.1.6 Upgrade 0.621 to 0.63

In this section we will show you how to upgrade from 0.621 to 0.63. This is the first release to contain our new upgrade approach.

The following steps will upgrade your Kamailio configuration from 0.621 to 0.63.

```
cd /opt/dsiprouter
git stash
git checkout v0.63
dsiprouter upgrade -rel 0.63
```

You should now be able to login to dSIPRouter and see that the new release has been applied.

8.1.7 Upgrade 0.522 to 0.523

In this section we will show you how to upgrade from 0.522 to 0.523.

Before starting the upgrade process you will need to backup your kamailio database using the following command:

```
cd /opt/
mysqldump kamailio > kamailio-bk.sql
```

After you've backed up your database you can now uninstall dsiprouter v0.50 by running the following commands:

```
cd /opt/dsiprouter
./dsiprouter.sh uninstall
```

Once the uninstall is complete you will need to either move or delete the /dsiprouter directory using the following command.

```
mv /dsiprouter /usr/local/src (moving directory)
```

Alternatively:

```
rm -r /dsiprouter (removing directory)
```

Installing dsiprouter v0.523

```
cd /opt/
apt-get update
apt-get install -y git curl
cd /opt
git clone -b v0.523 https://github.com/dOpensource/dsiprouter.git
cd dsiprouter
./dsiprouter.sh install
```

Note: please take note of the credentials given after the script has completed.

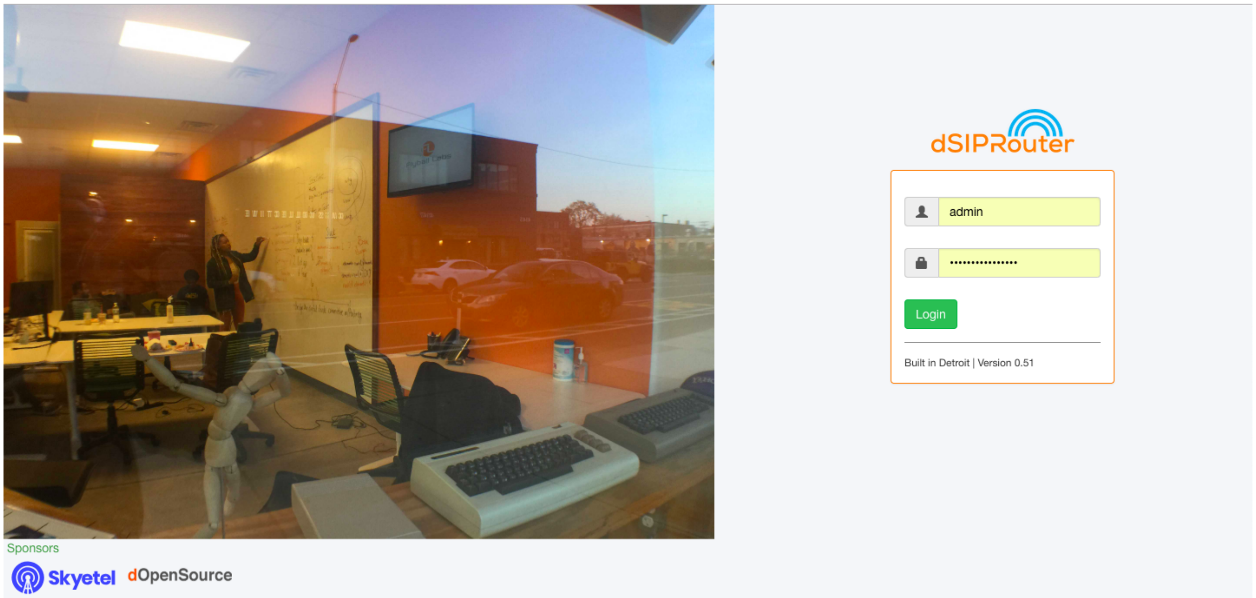
After the install is completed you can now restore your kamailio database using the following command:

```
cd /opt/
mysql  kamailio < kamailio-bk.sql
mysql kamailio -e "alter table dsip_multidomain_mapping add column domain_list_hash␣
↪varchar(255) after domain_list;"
```

Now please restart dsiprouter using the following commands:

```
cd /opt/disprouter/
./dsiprouter.sh restart
```

After the install is complete and the dsiprouter service has been restarted, the login screen should now reflect v0.51 and you should be able to login with the dsiprouter credentials provided after the install completed.



8.1.8 Upgrade 0.50 to 0.51

In this section we will show you how to upgrade from 0.50 to 0.51.

Before starting the upgrade process you will need to backup your kamailio database using the following command:

```
cd /opt/
mysqldump kamailio > kamailio-bk.sql
```

After you've backed up your database you can now uninstall dsiprouter v0.50 by running the following commands:

```
cd /opt/dsiprouter
./dsiprouter.sh uninstall
```

Once the uninstall is complete you will need to either move or delete the /dsiprouter directory using the following command.

```
mv /dsiprouter /usr/local/src (moving directory)
```

Alternatively:

```
rm -r /dsiprouter (removing directory)
```

Installing dsiprouter v0.51

```
cd /opt/
apt-get update
apt-get install -y git curl
cd /opt
git clone -b v0.51 https://github.com/dOpensource/dsiprouter.git
cd dsiprouter
./dsiprouter.sh install
```

Note: please take note of the credentials given after the script has completed.

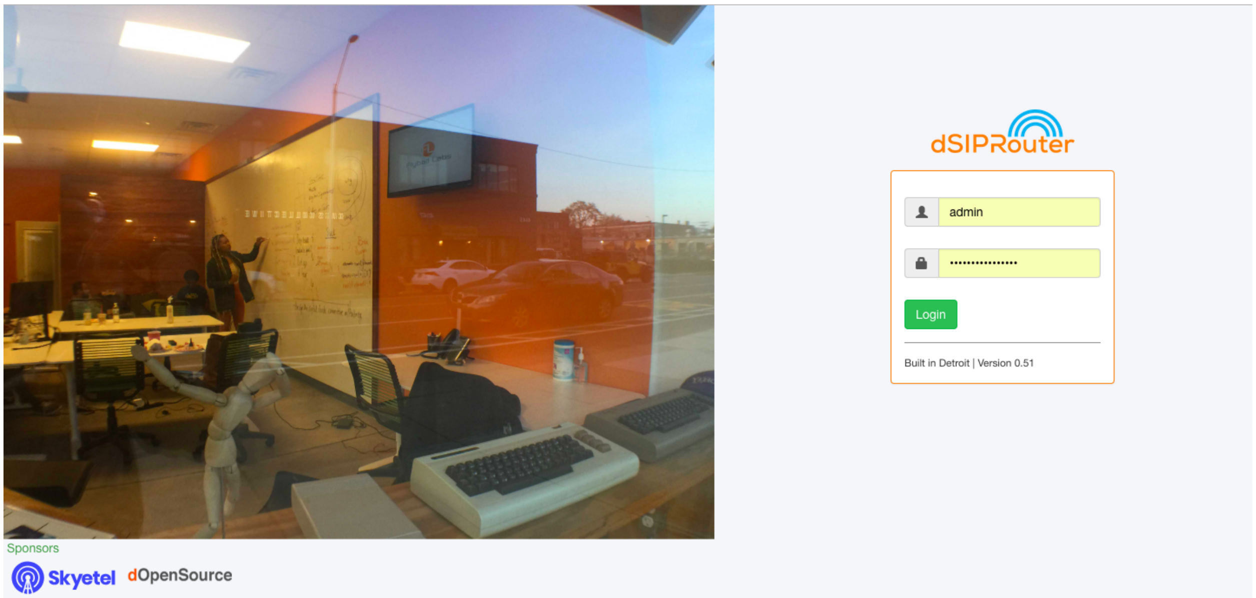
After the install is completed you can now restore your kamailio database using the following command:

```
cd /opt/
mysql  kamailio < kamailio-bk.sql
```

After the kamailio database is restored you need to restart dsiprouter using the following commands:

```
cd /opt/disprouter/
./dsiprouter.sh restart
```

After the install is complete and the dsiprouter service has been restarted, the login screen should now reflect v0.51 and you should be able to login with the dsiprouter credentials provided after the install completed.



CHAPTER

NINE

EXTRA RESOURCES

9.1 Extra Resources

9.1.1 Uploading CSVs

CSV Example

9.1.2 Proxy FusionPBX UI

Add the following stanza before "location /images/" stanza to proxy the FusionPBX UI thru dSIPRouter. Once the following text is added to /opt/dsiprouter/gui/modules/fusionpbx/dsiprouter.nginx.tpl you will be able to access the FusionPBX GUI via: https://dSIPRouter_IP/ or https://dSIPRouter_IP:

```
location / {
    proxy_pass https://fusionpbx;
    proxy_redirect off;
    proxy_next_upstream error timeout http_404 http_403 http_500 http_502 http_503 http_
↪504 non_idempotent;
}
```