FORTRA

Operation Ringing Rascal

Setting up your own social engineering infrastructure

Kyle Gaertner

FORTRA

What this talk is about

- Bio
- How this project started
- Setting it up
- Legal stuff
- The payoff
- What's next?

/usr/bin/whoami

- Kyle Gaertner
- Pentester wrangler with Fortra's Digital Defense
- CISSP, OSCP, OSWP, CRTO, GPEN, GWAPT, GAWN, CEH, CCNA, MCSA, LMNOP, and the alphabet soup goes on...
- MS and BS from WGU
- Pentesting for 7 years
- Other IT for 6 years
- Former welder

How this project started

- Phone system migration
- Boredom
- Bsides
- What if?

The phases

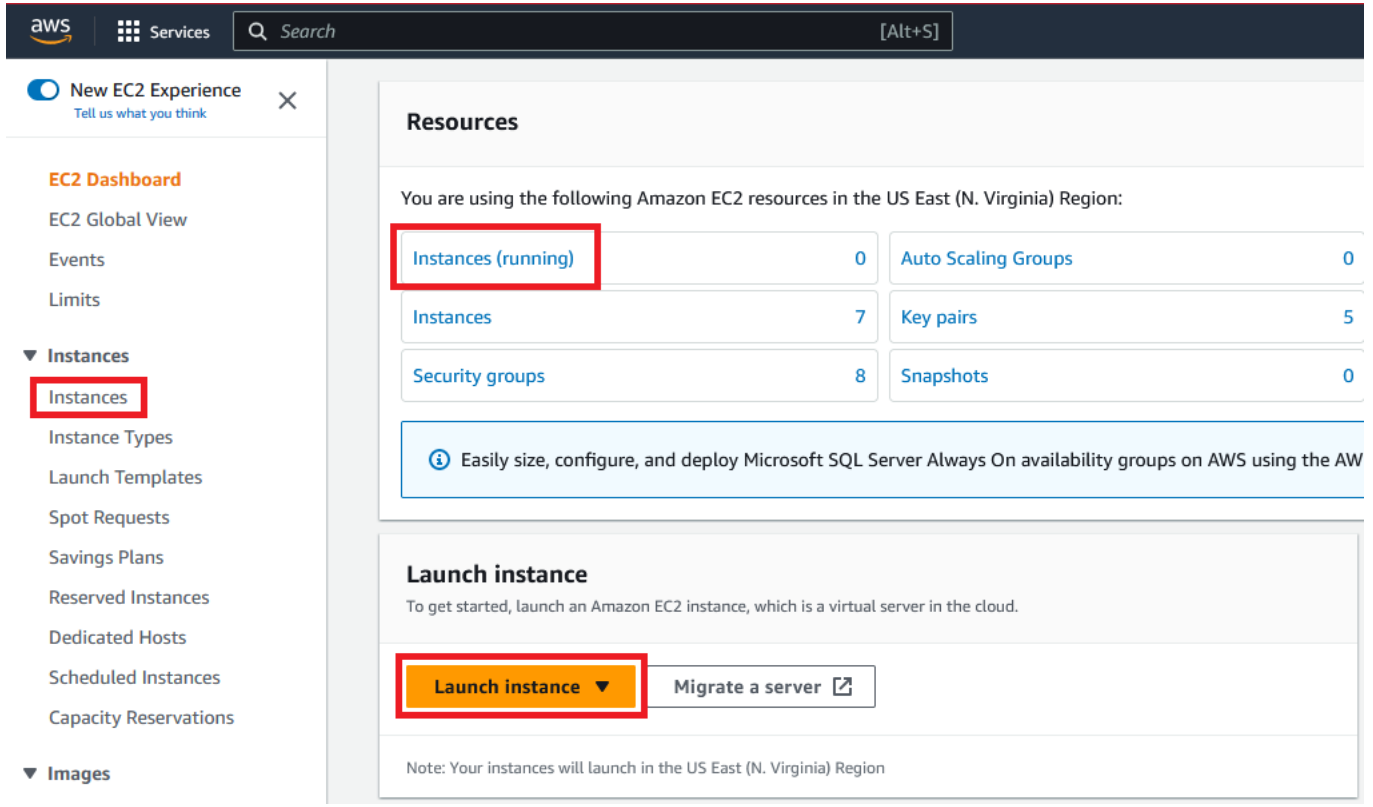
- AWS
- SIP Trunk
- FreePBX
- Voice Mod

AWS

- EC2
- AWS FreePBX
- t2.small (could go smaller)
- Security Groups!

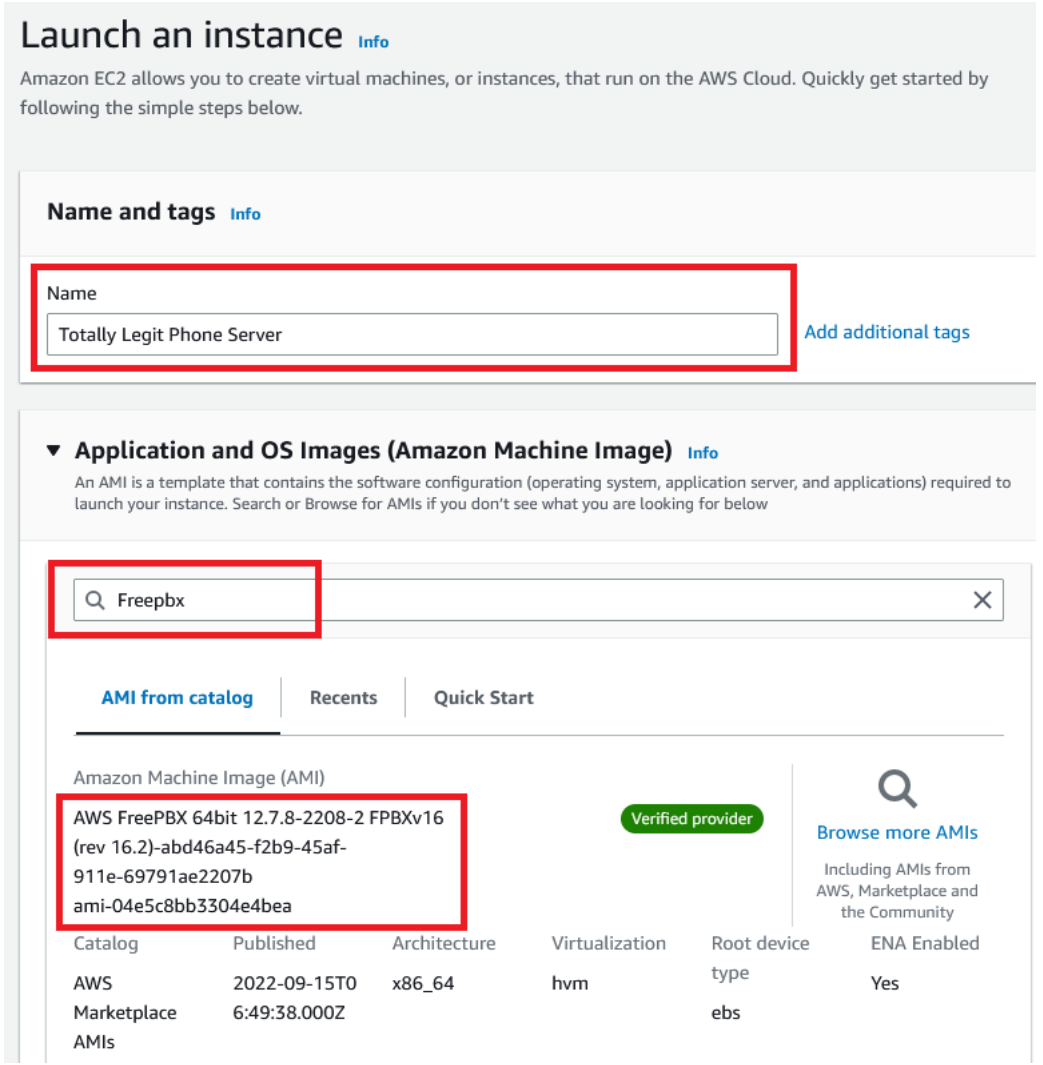
AWS crash course 1

EC2



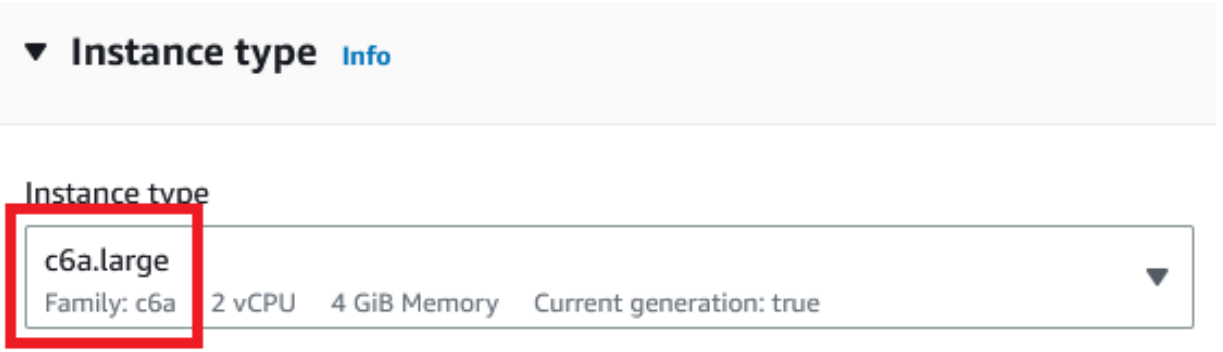
FORTRA

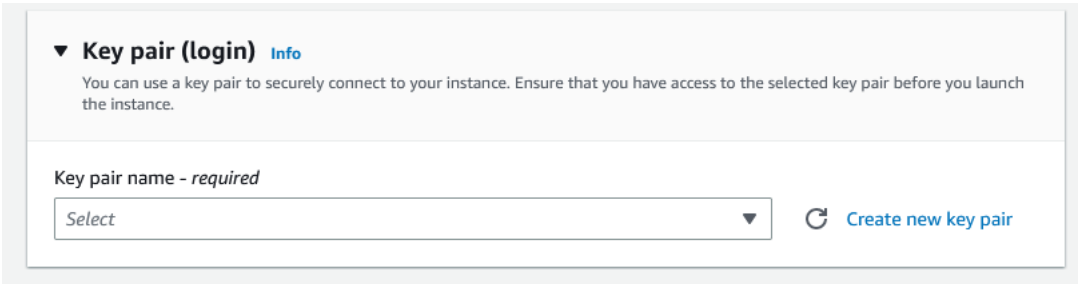
AWS crash course 2

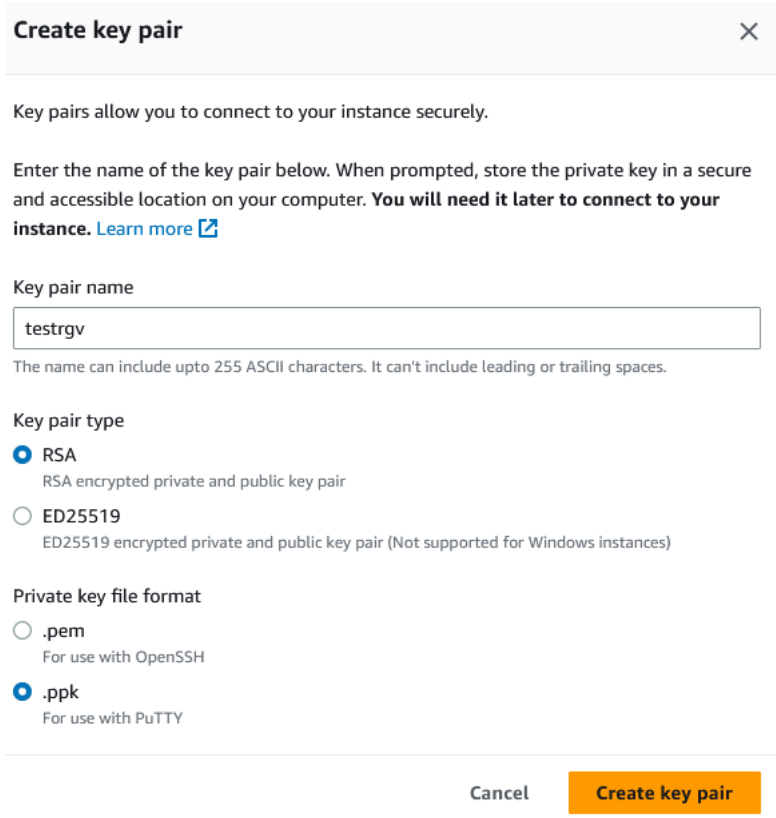


FORTRA

AWS crash course 3

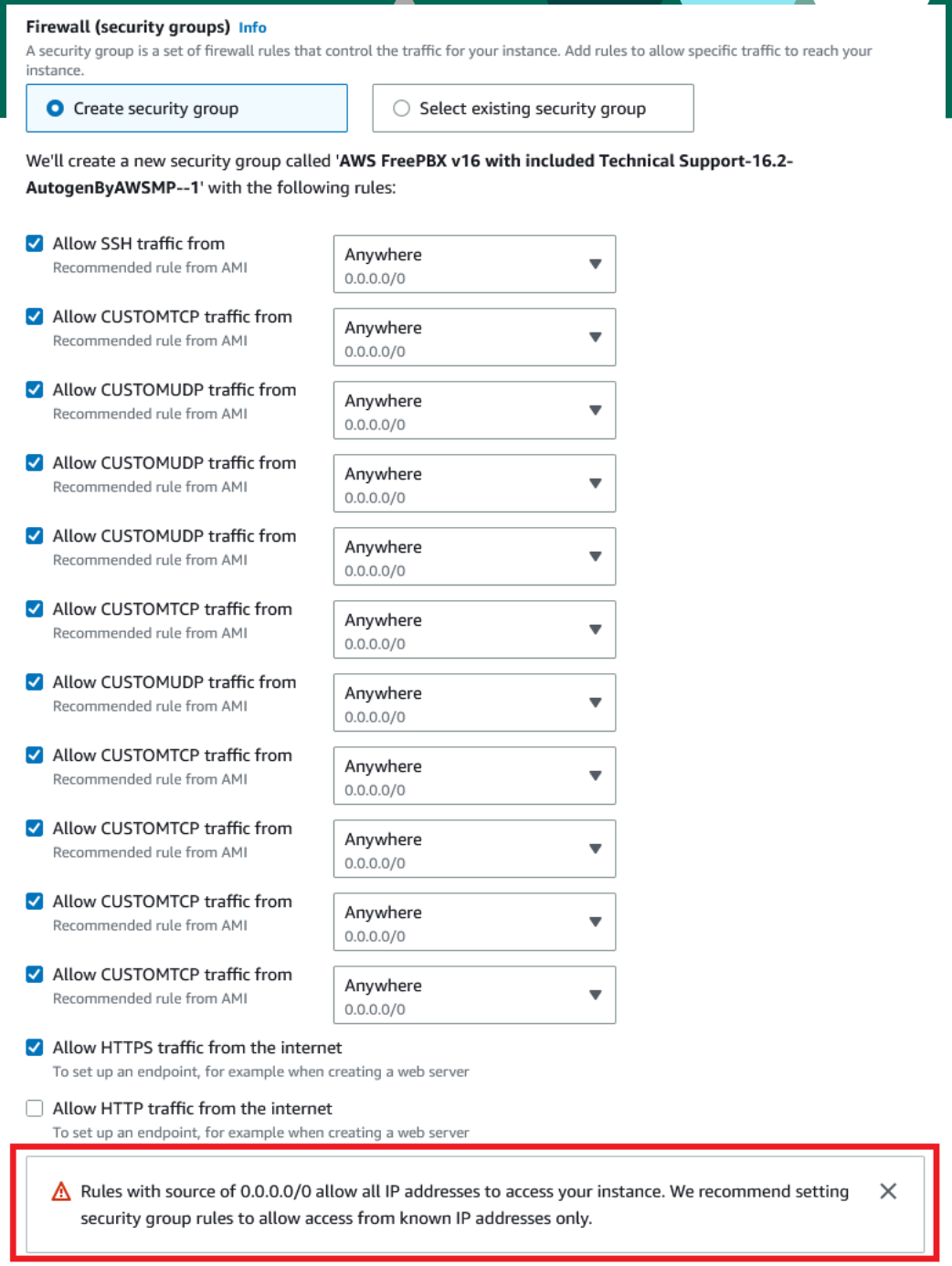






FORTRA

AWS crash course 4



FORTRA

AWS crash course 5

Edit inbound rules Info

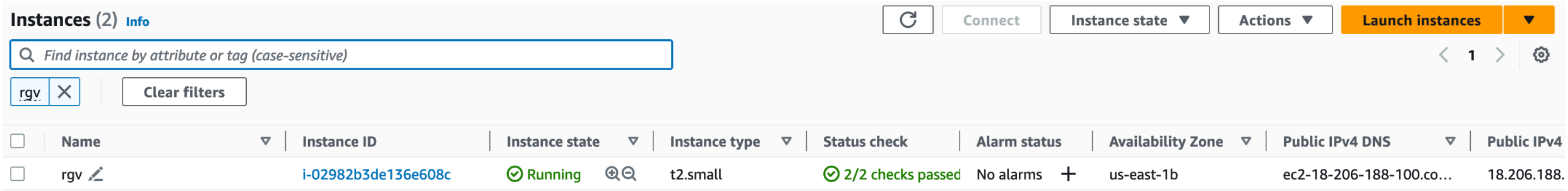
Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

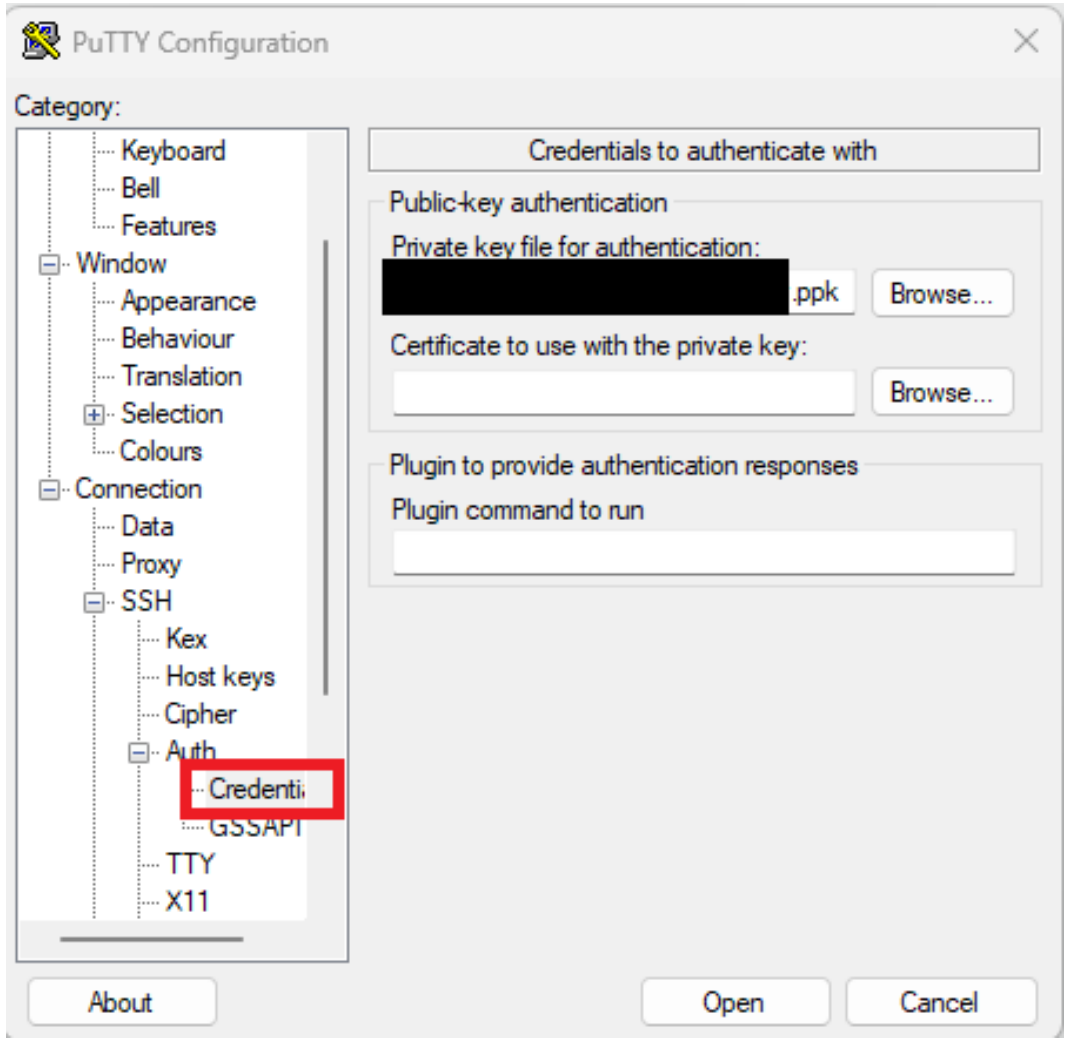
Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-[redacted]	Custom UDP	UDP	10000 - 64000	Custom	128.136.235.202/32	questblue (sip trunk)	Delete
sgr-[redacted]	Custom UDP	UDP	10000 - 20000	Custom	[redacted]/32	[redacted] - voice portion	Delete
sgr-[redacted]	SSH	TCP	22	Custom	[redacted]/32	ssh - [redacted]	Delete
sgr-[redacted]	Custom UDP	UDP	5060	Custom	[redacted]/32	[redacted] - chan_sip signaling	Delete
sgr-[redacted]	HTTPS	TCP	443	Custom	[redacted]/32	[redacted] - https	Delete

FORTRA

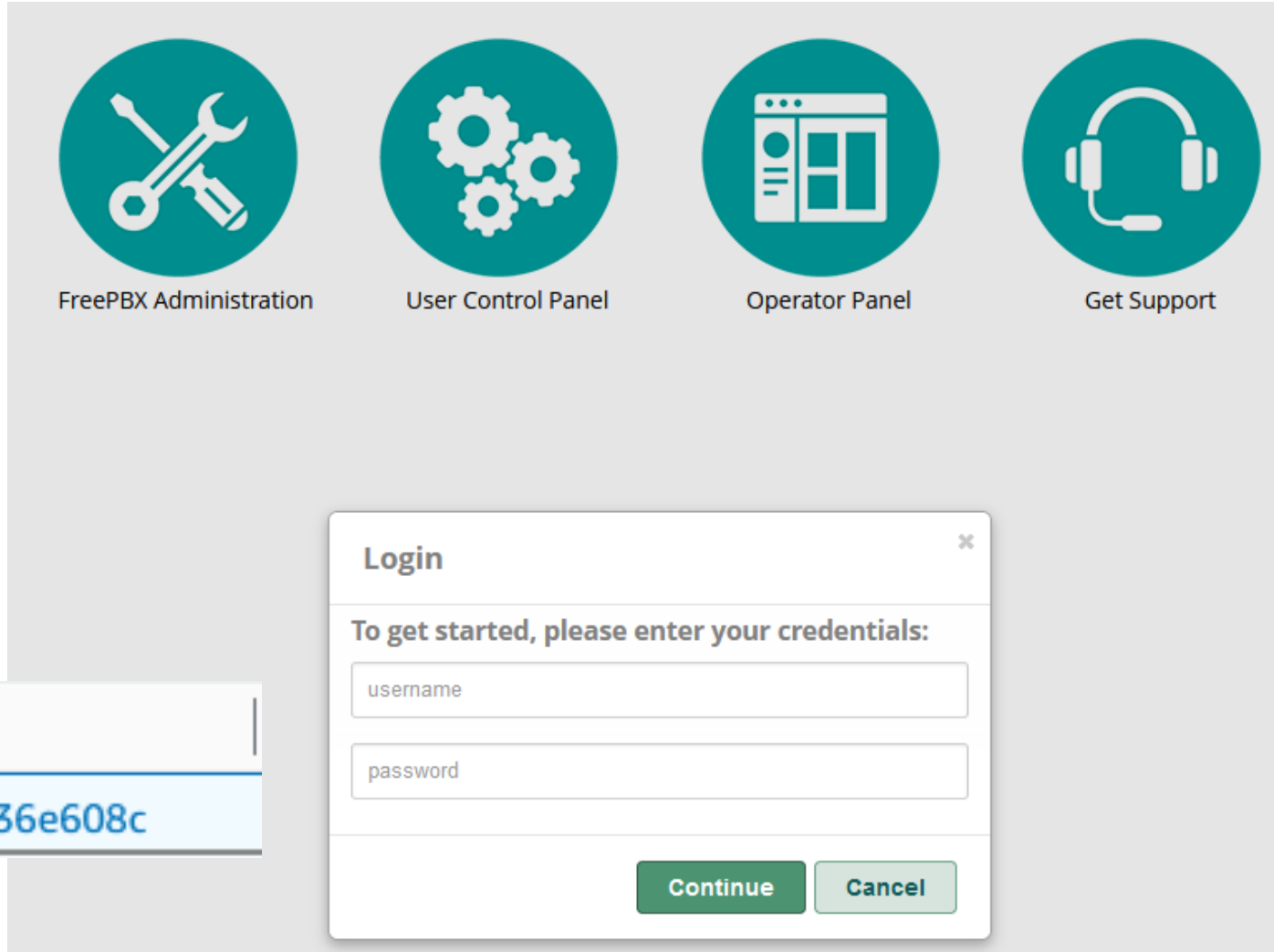
AWS crash course 6



AWS crash course 7



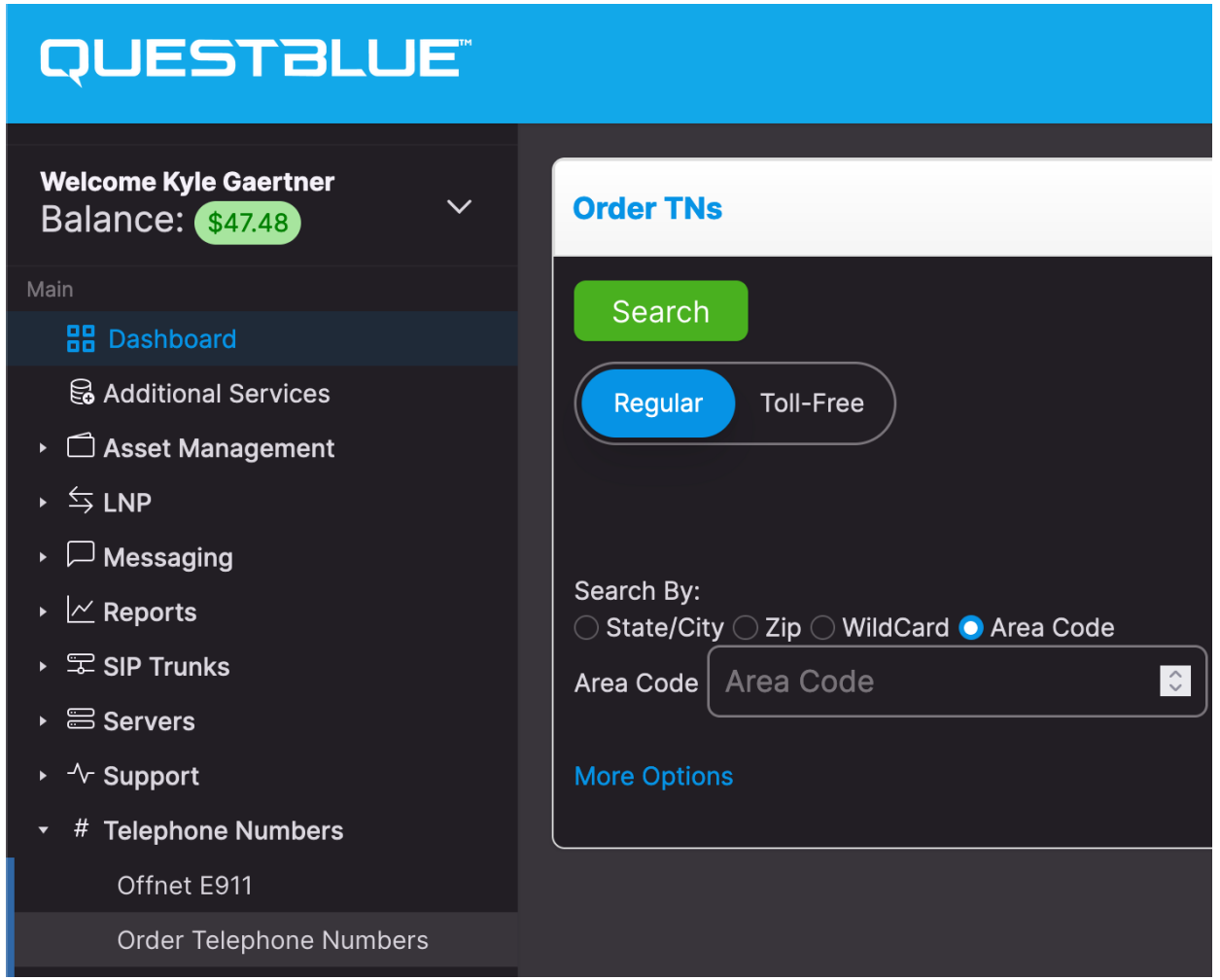
AWS crash course 8



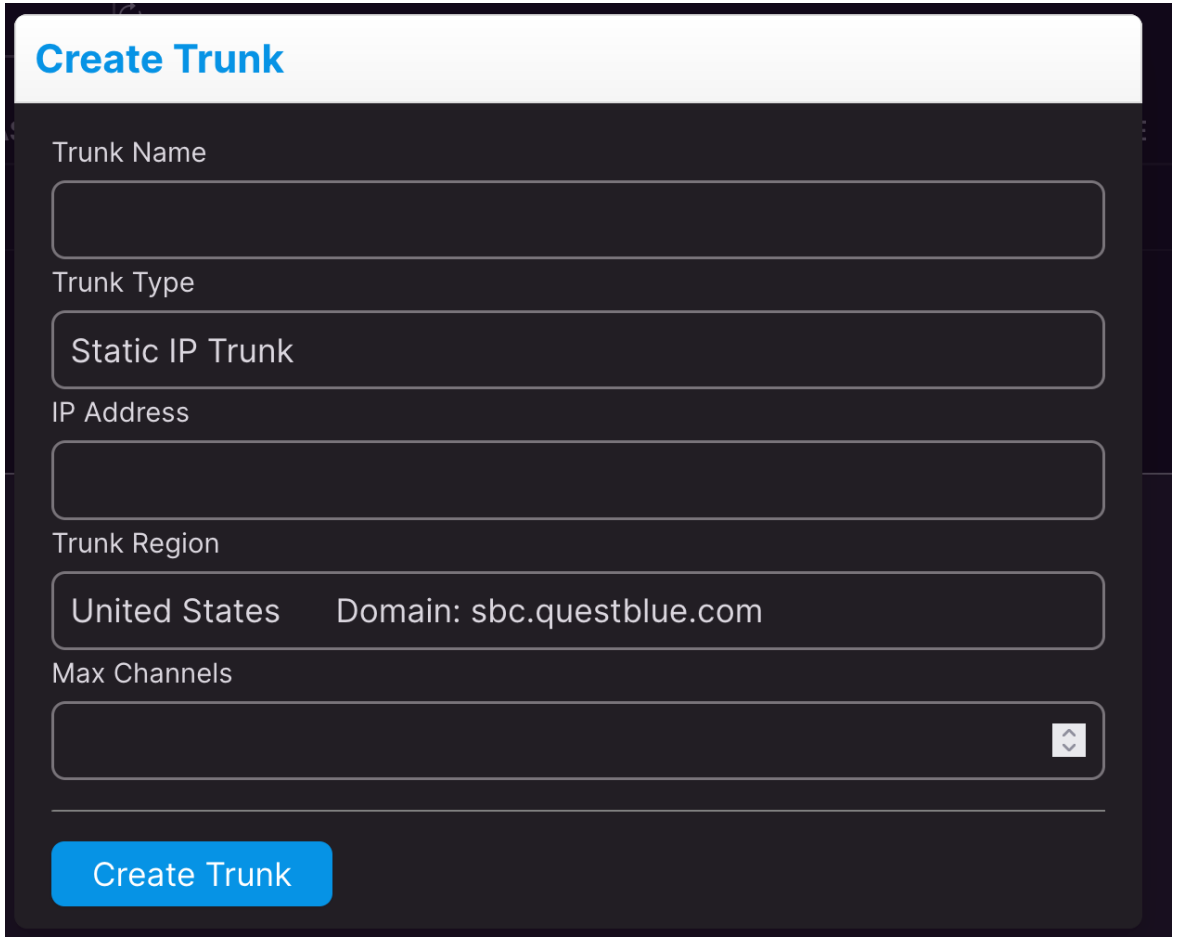
Name	Instance ID
rgv	i-02982b3de136e608c

AWS crash course 9

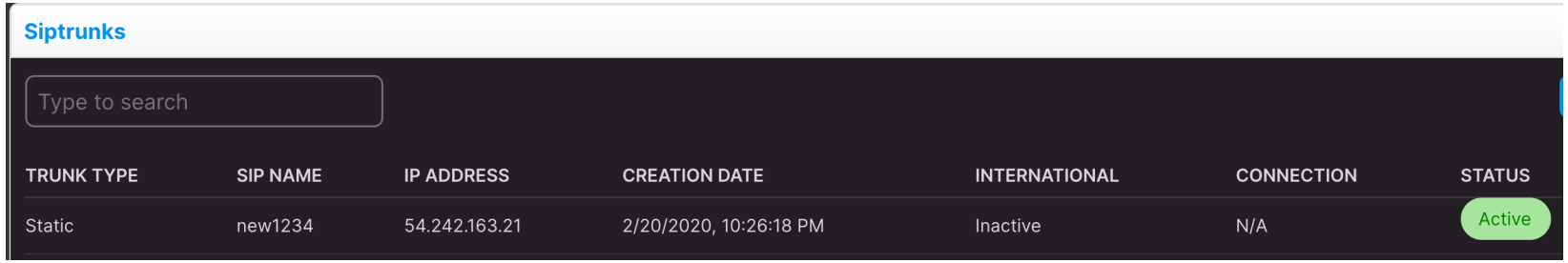
SIP Trunk 1


QUESTBLUE
Welcome Kyle Gaertner
Balance: $47.48
Main
Dashboard
Additional Services
Asset Management
LNP
Messaging
Reports
SIP Trunks
Servers
Support
Telephone Numbers
Offnet E911
Order Telephone Numbers
Order TNs
Search
Regular
Toll-Free
Search By:
State/City
Zip
WildCard
Area Code
Area Code
Area Code
More Options

SIP Trunk 2

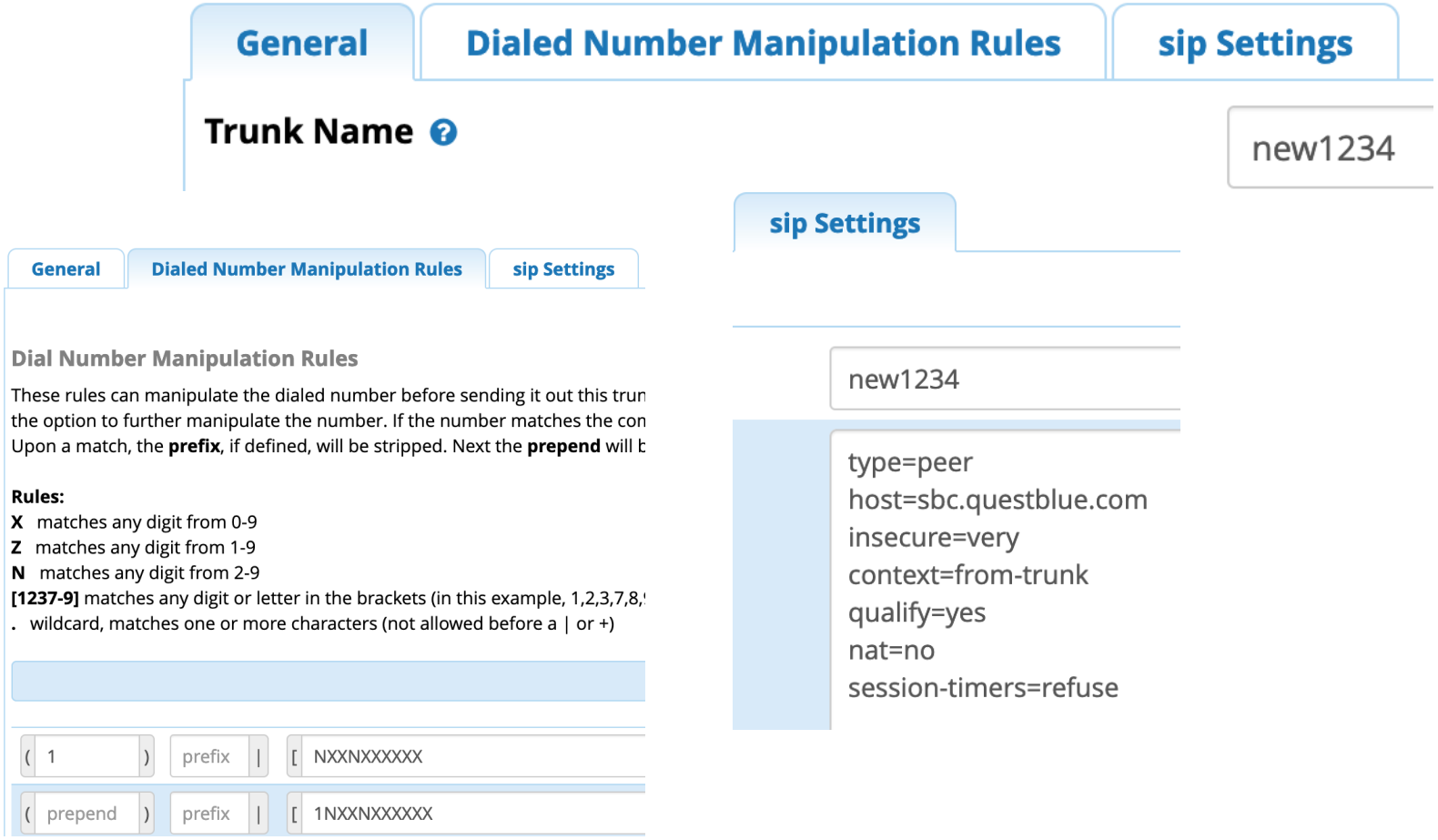

Create Trunk
Trunk Name
Trunk Type
Static IP Trunk
IP Address
Trunk Region
United States
Domain: sbc.questblue.com
Max Channels
Create Trunk

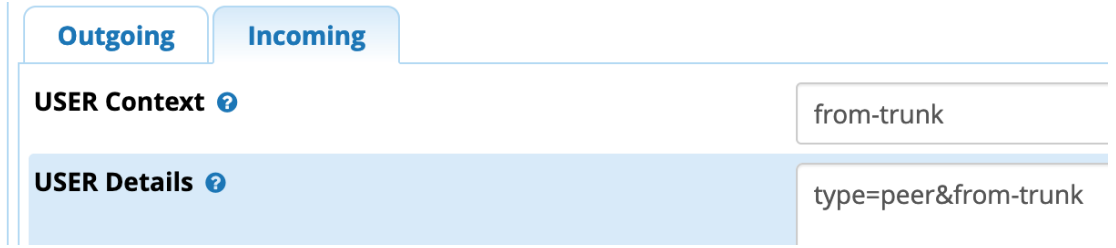
SIP Trunk 3


Siptrunks
Type to search
TRUNK TYPE
SIP NAME
IP ADDRESS
CREATION DATE
INTERNATIONAL
CONNECTION
STATUS
Static
new1234
54.242.163.21
2/20/2020, 10:26:18 PM
Inactive
N/A
Active

FreePBX 1

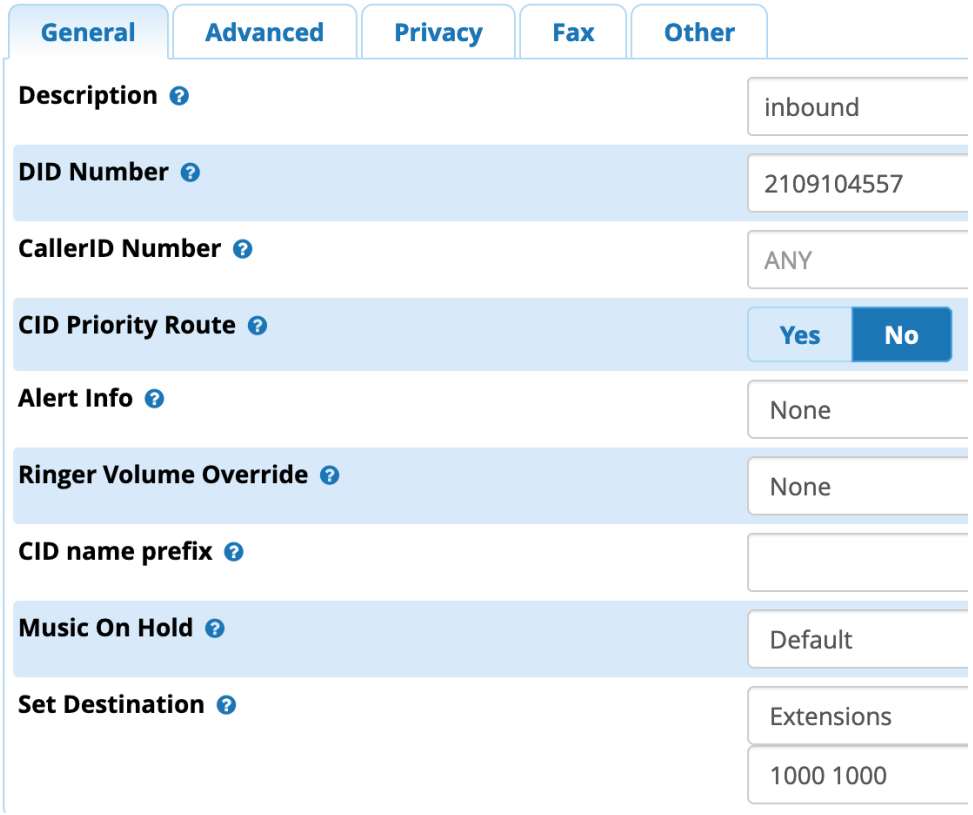
- Connectivity \ Trunks





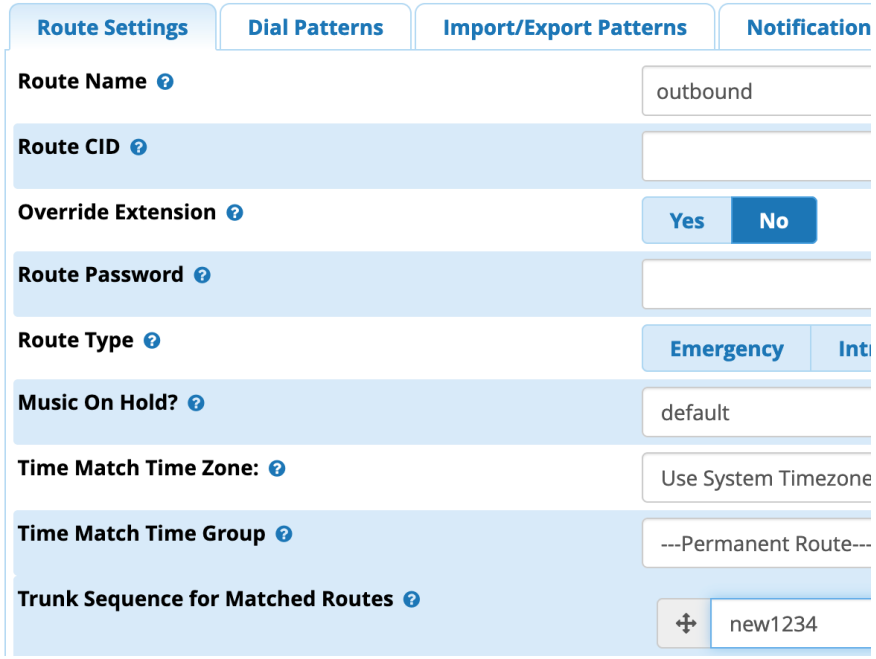
FreePBX 2

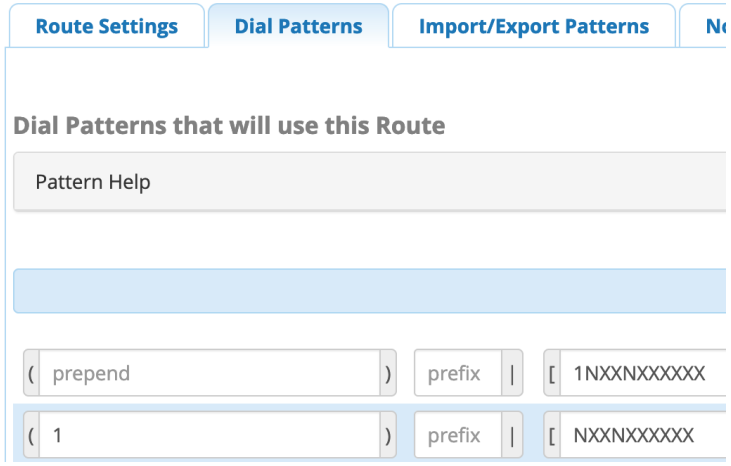
- Connectivity \ Inbound Routes



FreePBX 3

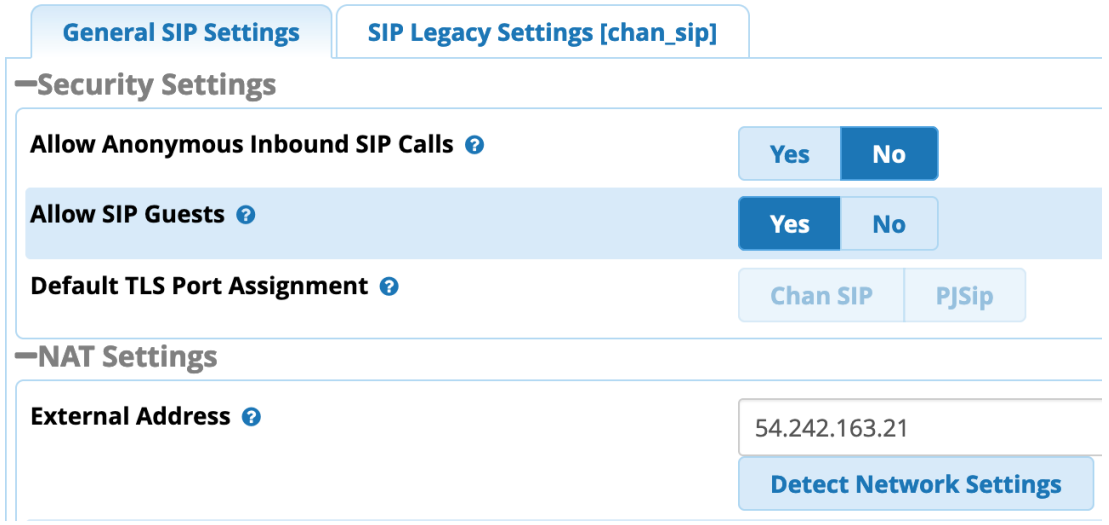
- Connectivity \ Outbound Routes

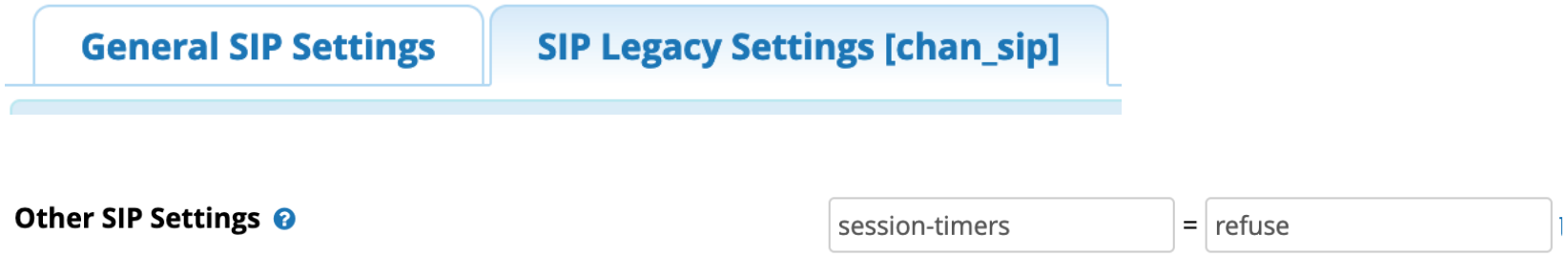




FreePBX 4

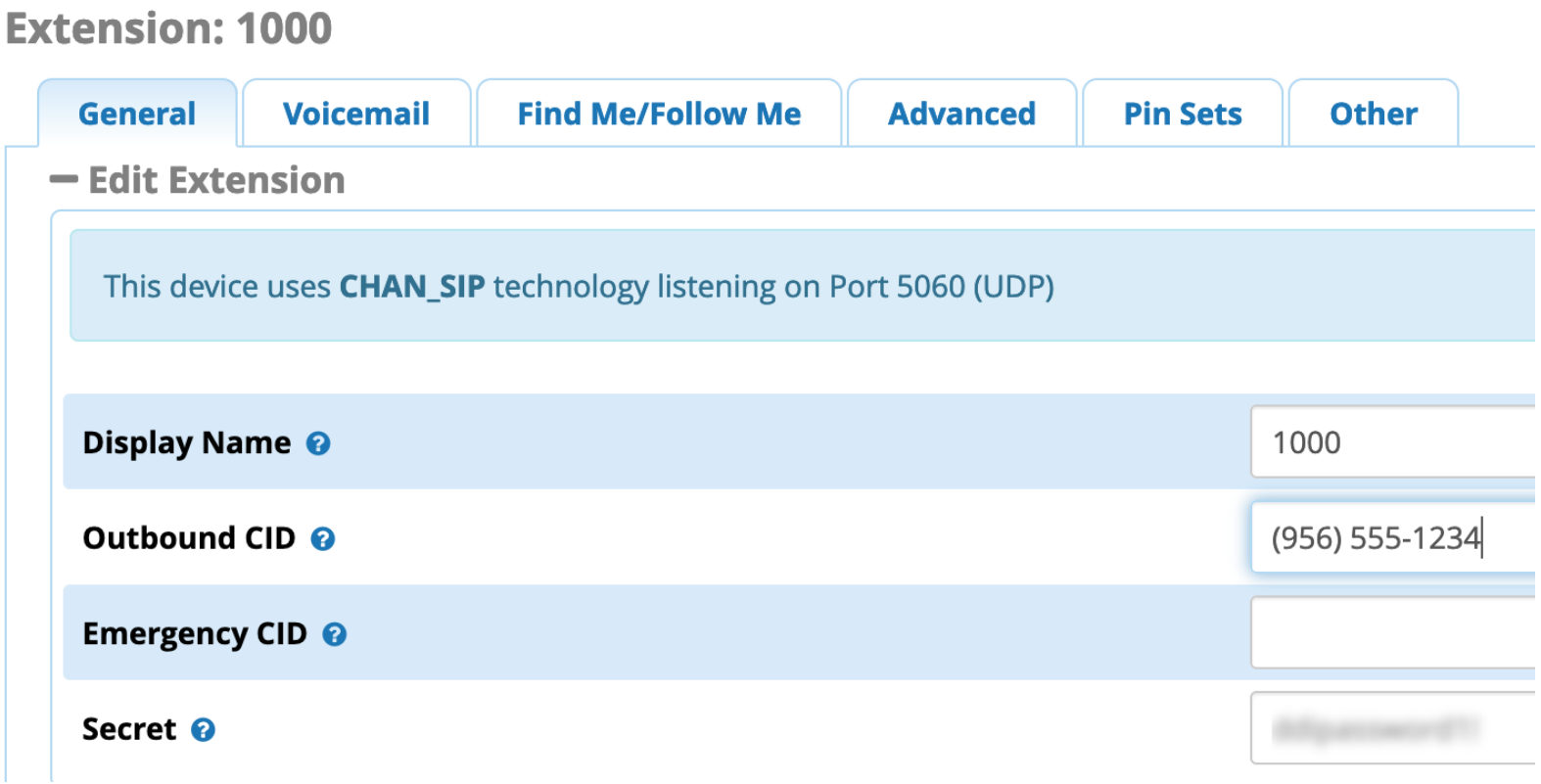
- Settings \ Asterisk SIP Settings





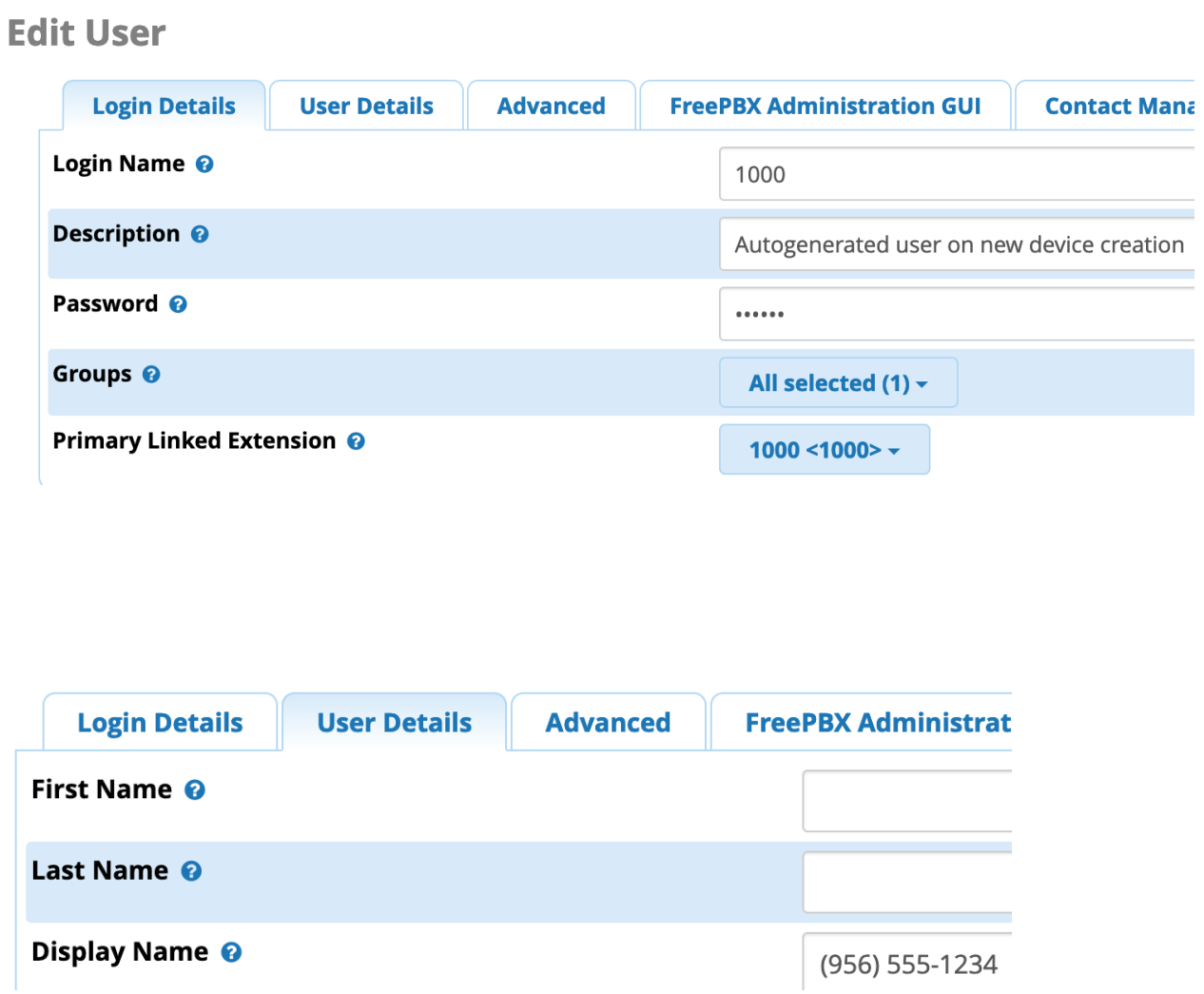
FreePBX 5

- Applications \ Extensions



FreePBX 6

- Admin \ User Management



Linphone

ACCOUNT ASSISTANT

Create or manage your Linphone account.

ASSISTANT

USE A SIP ACCOUNT

USE A SIP ACCOUNT

Username

Display name (optional)

SIP Domain

Password

Transport

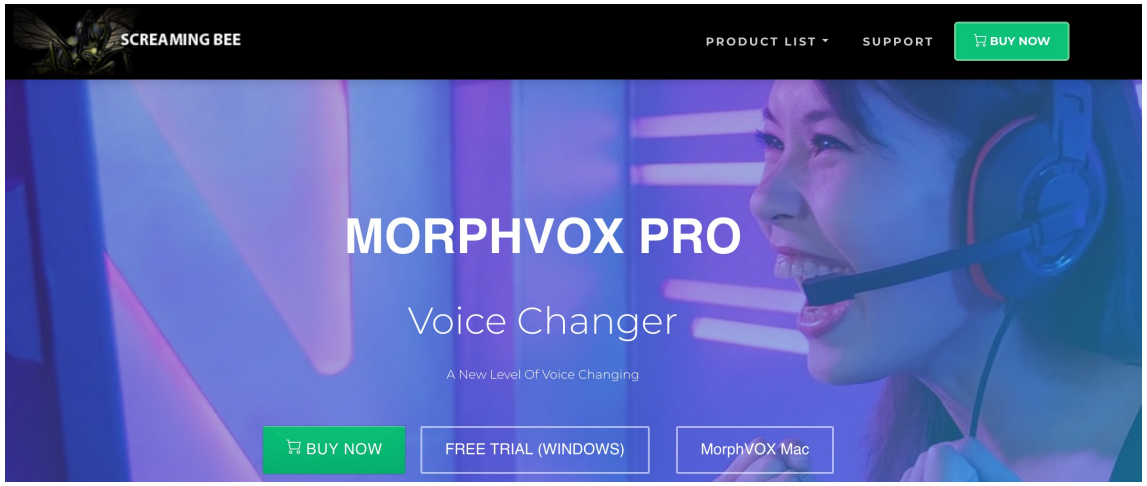
UDP

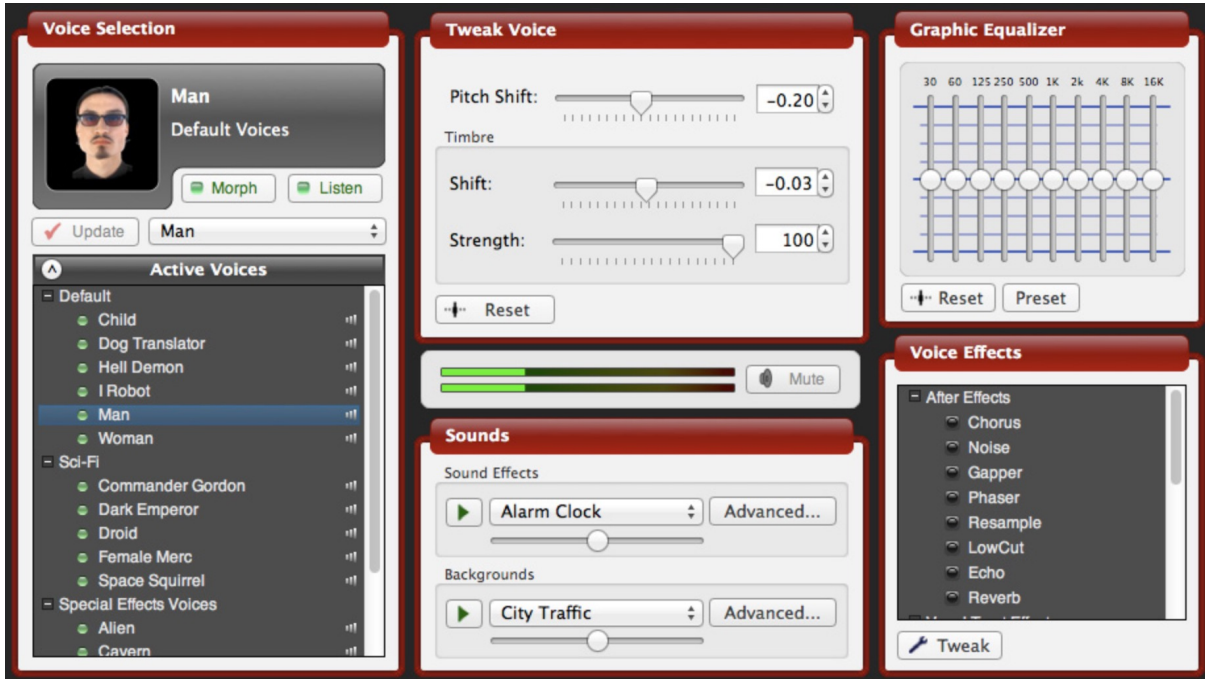
BACK

USE

Voice Mod

- Voice Packs
- Backgrounds





Legal Stuff

- Truth in Caller ID Act of 2009
- STIR/SHAKEN

Truth in Caller ID Act of 2009

- “Truth in Caller ID Act of 2009 - Amends the Communications Act of 1934 to make it unlawful for any person in the United States, in connection with any telecommunications service or Internet protocol (IP)-enabled voice service, to cause any caller identification (ID) service to transmit misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value, unless such transmission is exempted in connection with: (1) authorized activities of law enforcement agencies; or (2) a court order specifically authorizing the use of caller ID manipulation.”

*https://www.congress.gov/bill/111th-congress/senate-bill/30

- Fines up to $10,000

STIR/SHAKEN

- STIR/SHAKEN is a framework of interconnected standards. STIR/SHAKEN are acronyms for the Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENs (SHAKEN) standards. This means that calls traveling through interconnected phone networks can have their caller ID "signed" as legitimate by originating carriers and validated by other carriers before reaching consumers. STIR/SHAKEN digitally validates the handoff of phone calls passing through the complex web of networks, allowing the phone company of the consumer receiving the call to verify that a call is in fact from the number displayed on Caller ID.
- tl;dr: certificate authorities, verification, trusts, fines

*https://www.fcc.gov/call-authentication

It works? It works!

- Convincing premise?
- Emotional response
- Pressure


DIGITA
DEFEN E
INCORPO ED


DIGITAL DEFENSE
INCORPORATED

FORTRA

The payoff

- Is my face red?
- Solved a few problems
- Had a few laughs

What's this talk really about?

- Nothing groundbreaking
- Based on the work of others

Credits

Jonathan Stines - https://www.rapid7.com/blog/post/2018/05/24/how-to-build-your-own-caller-id-spoofer-part-1/

Ventz - https://blog.vpetkov.net/2011/07/10/spoofing-caller-id-on-the-fly-from-any-phone-for-legal-and-legitimate-purposes/

Questions

kyle.gaertner@fortra.com

@unskilledk

https://github.com/unskilledk/slides/2023RGV