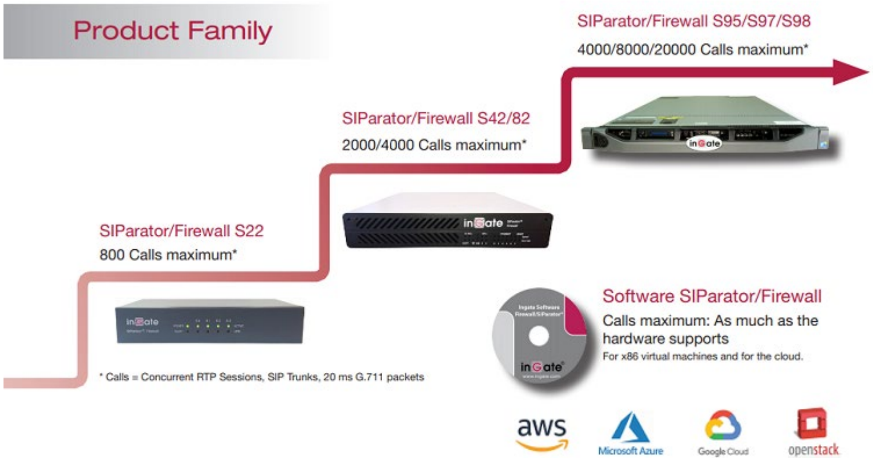
ThinkTel® Business Services by DISTRIBUTEL

inGate®

Enabling SIP to the Enterprise


Product Family
SIParator/Firewall S95/S97/S98
4000/8000/20000 Calls maximum*
SIParator/Firewall S42/82
2000/4000 Calls maximum*
SIParator/Firewall S22
800 Calls maximum*
* Calls = Concurrent RTP Sessions, SIP Trunks, 20 ms G.711 packets
Software SIParator/Firewall
Calls maximum: As much as the hardware supports
For x86 virtual machines and for the cloud.
aws
Microsoft Azure
Google Cloud
openstack

ThinkTel SIP Trunking with Mitel MiVoice connect and Ingate

Prepared by:
Gerrie Joubert
ThinkTel Communications Ltd.

2/24/2021

Contents

Overview

Welcome to Ingate/ThinkTel SIP provisioning guide. This document covers the basic steps required to activate your new SIP service and provides an introduction on how to configure the Ingate SIParator.

This Ingate is setup as a DMZ/LAN SIParator in this example.

Requirements

Before you start

1. Ingate license code(s) and activation instruction;
2. Mitel SIP license(s);
3. ThinkTel SIP Trunk INFO:
    a. IP Addresses & Proxy addresses.
    b. Username & Password.
4. Private IP address information:
    a. IP, Subnet & Gateway.
5. Private DMZ IP address information (*if required*).
    a. IP, Subnet & Gateway.
6. Public IP address information:
    a. IP, Subnet & Gateway.
7. Customers DNS Server IP addresses.
8. ShoreTel/Mitel SIP trunk appliance IP address.
9. An Ingate account (support representative must create an account with ingate);
10. Download the Ingate setup tool: http://www.ingate.com/Startup_Tool.php
11. Download the Ingate setup tool guide: https://www.ingate.com/appnotes/Ingate_Startup_Tool_Getting_Started_Guide.pdf
12. Download the Mitel Implementation Guide: https://oneview.mitel.com/s/article/SIP-Trunking-MItel-Connect-ONSITE-with-Ingate-App-Note

Please note without the above listed prerequisites the customer or engineer will not be able to proceed with the deployment.

Deployment Check List

Before starting the installation, please confirm you have all the information required to continue:

Received	Description:	Info:
	Mitel SIP license(s):	
	Ingate License(s):	
	ThinkTel SIP trunk Binding info:	**Toronto Binding**
	• Username/Number:	
	• Account Password:	
	• Contact End Point (External IP):	
	• Proxy End Point:	
	• SIP Domain Name:	
	• SIP Proxy 1:	*208.68.17.32 /27*
	• SIP Proxy 2:	*206.80.250.96 /27*
	• SIP Proxy 3:	*209.197.133.0 /26*
	• SIP Channels:	
	ThinkTel SIP trunk Binding info:	**Edmonton Binding**
	• Username/Number:	
	• Account Password:	
	• Contact End Point External IP):	
	• Proxy End Point:	
	• SIP Domain Name:	
	• SIP Proxy 1:	*208.68.17.32 /27*
	• SIP Proxy 2:	*206.80.250.96 /27*
	• SIP Proxy 3:	*209.197.133.0 /26*
	• SIP Channels:	
	• SIP allowed codecs:	*G711 u-law, G729*
	• Protocol:	*UDP / TCP*
	• SIP Signaling Port(s):	*5060 / 5061*
	• SIP Media Ports start:	*58024*
	• SIP Media Ports end:	*60999*
Received	**Description:**	**Info:**
	Private IP address Info:	
	• IP Address:	
	• Netmask:	
	• Gateway:	
	• Primary DNS:	
	• Secondary DNS:	
	Private DMZ IP Address Info:	
	• IP Address:	
	• Netmask:	
	• Gateway:	
	Public IP address Info:	
	• IP Address:	
	• Netmask:	
	• Gateway:	
	Mitel Appliance IP Address:	

ThinkTel SIP trunk account information

ThinkTel SIP trunk account information

***NOTE:** Your configuration might look different form the example in this document therefore if you require any further assistance please contact Ingate Support, +1 (866) 809-0002*

***Operational Hours:** Monday – Friday 9am – 6pm Eastern*

Requirements

Downloading the Ingate ISO file

1. Log on to www.ingate.com and click “Account Login”
2. Login with your Support Account, if you haven't got an account here, please register.
3. Once in your “Account Home Page”, if you haven’t already done so, choose the option “Register a new unit”, enter the Serial Number of your Ingate, then press “Register”.
4. In your “Account Home Page”, choose the option ”Download Upgrades”
5. Understand the upgrade path provide in the table, and select the Software Version.
6. Enter the Serial Number of the machine you wish to upgrade, or select “Load my units” and remove all units except the one you wish to upgrade.
7. Press “Download Upgrade” and a software file “upgrade.fup” will be downloaded to the PC.
8. Login to the Ingate unit, go to “Administration - Upgrade” page. Browse to the “upgrade.fup” file and Press “Upgrade” and follow the instructions on the unit.

Installation of the Ingate ISO file

If the customer is providing the hardware or virtualized environment for the Ingate ISO, then the file needs to be provided to the customer for installation.

If the Unity support representative is installing the ISO in the Mitel VMware environment, then the Mitel installation document must be followed for the installation and deployment of the ISO image.

Configure the Ingate using the setup tool

Download and install the Ingate setup tool on the local network and/or the Mitel HQ or DVS servers. The Ingate installed image must be reachable via the setup tool on the customers local phone network.

With the setup tool guide downloaded from the prerequisite list follow the Ingate setup tool guide for a step-by-step basic installation.

NOTE: *Once the basic configuration and licenses have been installed and setup have been completed, the support representative will log into the Ingate’s web interface using the private IP address that have been configured.*

Complete the Ingate configuration using the web interface

In this example we will be using the following IP addresses information and the SIP trunk info:

Private IP Info:

Interface:	eth0
IP Address:	172.29.255.10
Subnet Mask:	255.255.255.0
Gateway:	172.29.255.1
DNS Server 1:	172.29.100.101
DNS Server 2:	172.29.97.101
Mitel Appliance:	172.29.128.33

DMZ IP Info:

Interface:	eth1
IP Address:	10.20.255.10
Subnet Mask:	255.255.255.0
Gateway:	10.20.255.1

Public IP Info:

IP Address:	72.xxx.xxx.xx6

ThinkTel SIP trunk Binding info:	**Toronto Binding**
Username/Number:	24xxxxxxx3
Account SIP Password:	*******************
Contact End Point (External IP):	72.xxx.xxx.xx6
Proxy End Point:	*20x.xx.xxx.100*
SIP Domain Name:	*tor.xxx.xxx.ca*
SIP Proxy 1:	*208.68.17.32 /27*
SIP Proxy 2:	*206.80.250.96 /27*
SIP Proxy 3:	*209.197.133.0 /26*
SIP Channels:	30
ThinkTel SIP trunk Binding info:	**Edmonton Binding**
Username/Number:	24xxxxxxx3
Account SIP Password:	*******************
Contact End Point (External IP):	72.xxx.xxx.xx6
Proxy End Point:	*20x.xxx.xxx.52*
SIP Domain Name:	*edm.xxx.xxx.ca*
SIP Proxy 1:	*208.68.17.32 /27*
SIP Proxy 2:	*206.80.250.96 /27*
SIP Proxy 3:	*209.197.133.0 /26*
SIP Channels:	30
Protocol:	UCP / TCP

ThinkTel SIP trunk account information

ThinkTel SIP trunk account information

SIP Signaling Port(s):	*5060 / 5061*
SIP Media Ports start:	*58024*
SIP Media Ports end:	*60999*
SIP allowed codecs:	*G711 u-law, G729*

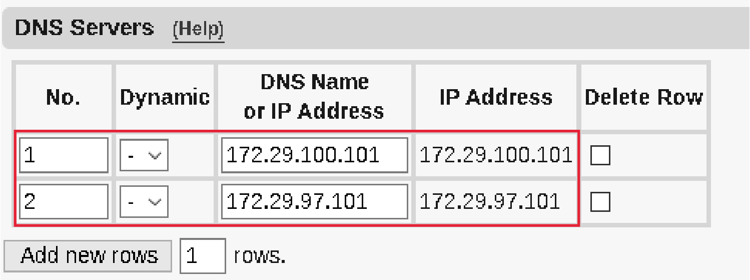
***NOTE:** The IP addresses listed in this document is only an example and the support representative will need to utilize their own IP addresses when configuring the Ingate siparator / SBC.*

Step 1:

Log into the Ingate's web interface and navigate to **Basic Configuration>Basic Configuration tab.**

Scroll down to the DNS Servers section and confirm the DNS IP addresses are correct, if they do not appear the support representative will be required to add the DNS server IP addresses. Select the **Add new rows** button to add 1 new row.

Once the IP addresses are added select the **Save** button to save your entries.

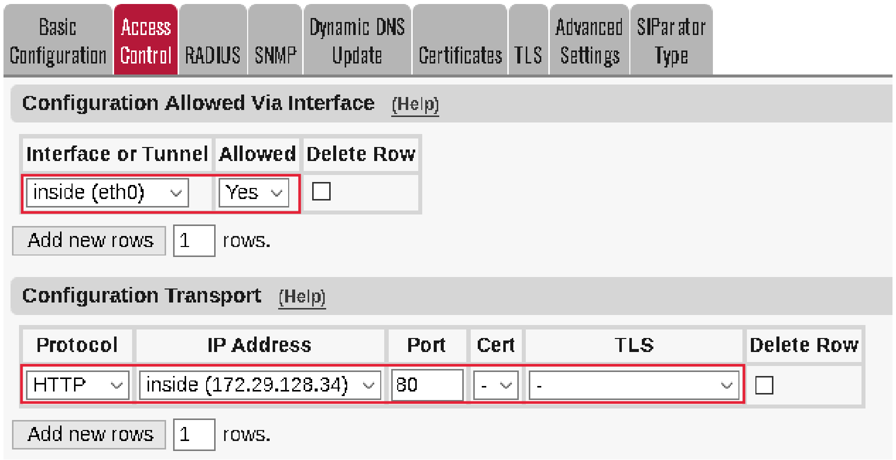


No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	172.29.100.101	172.29.100.101	□
2	-	172.29.97.101	172.29.97.101	□

Step 2:

Navigate to **Basic Configuration>Access Control tab**.

1. Under the Configure Allowed Via Interface menu,
2. Confirm the following info is set:
3. **Interface or Tunnel:** Inside (eth0)
4. **Allowed:** Yes
5. Under the Configuration Transport menu,
6. Confirm the following info is set:
7. **Protocol:** HTTP
8. **IP Address:** Inside (172.29.128.34)
9. **Port:** 80



Configuration Allowed Via Interface (Help)

Interface or Tunnel	Allowed	Delete Row
inside (eth0)	Yes	☐

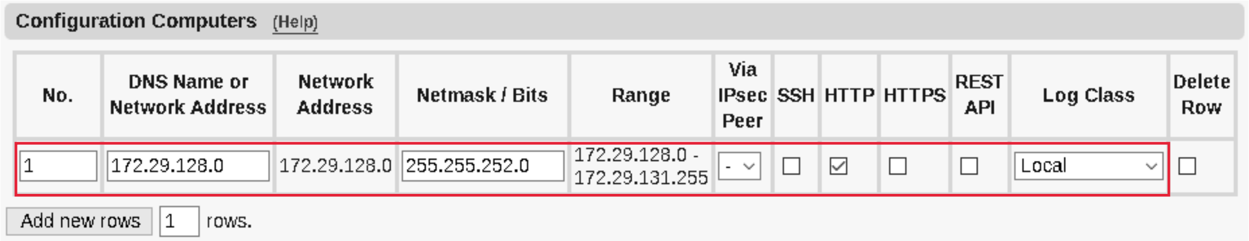
Add new rows 1 rows.

Configuration Transport (Help)

Protocol	IP Address	Port	Cert	TLS	Delete Row
HTTP	inside (172.29.128.34)	80	-	-	☐

Add new rows 1 rows.

10. Under the Configuration Computers menu,
11. Confirm the following info is set for line 1:
12. **No.:** 1
13. **DNS Name:** 172.29.128.0
14. **Network Address:** 172.29.128.0
15. **Netmask / Bits:** 255.255.252.0
16. **Range:** 172.29.128.0 – 172.29.131.255
17. **HTTP:** HTTP is checked
18. **Log Class:** Local



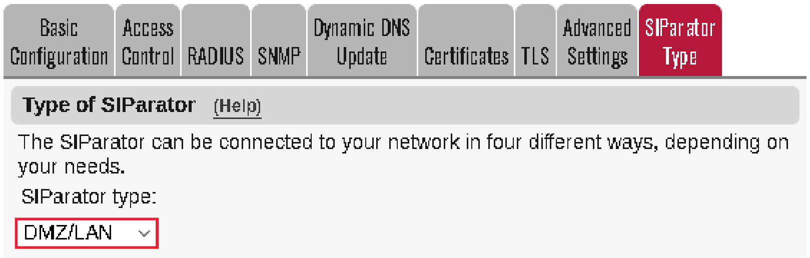
Configuration Computers (Help)

No.	DNS Name or Network Address	Network Address	Netmask / Bits	Range	Via IPsec Peer	SSH	HTTP	HTTPS	REST API	Log Class	Delete Row
1	172.29.128.0	172.29.128.0	255.255.252.0	172.29.128.0 - 172.29.131.255	-	☐	☑	☐	☐	Local	☐

Add new rows 1 rows.

Navigate to **Basic Configuration>SIParator Type tab**.

19. Under the Type of SIParator menu,
20. **SIParator Type:** DMZ/LAN



Type of SIParator (Help)

The SIParator can be connected to your network in four different ways, depending on your needs.

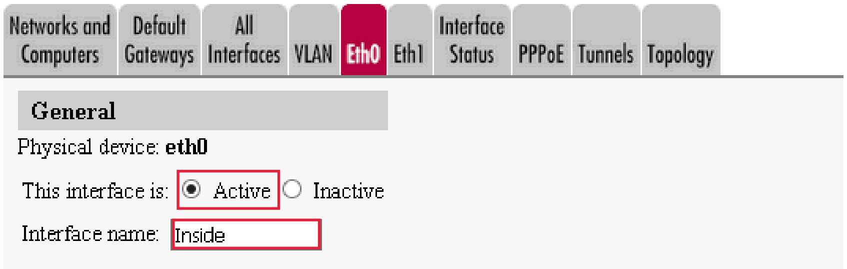
SIParator type:

DMZ/LAN

Step 3:

Navigate to **Network>ETH0 tab**.

1. Under the General menu, Time to configure the Interfaces
   a. Confirm the following info is set for **General**:
      i. **This Interface:** Active
      ii. **Interface Name:** Inside



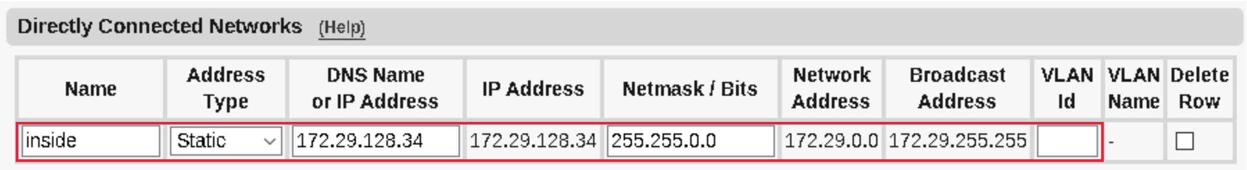
General

Physical device: **eth0**

This interface is: ● Active ○ Inactive

Interface name: Inside

   b. Confirm the following info is set for **Directly Connected Networks**:
      i. **Name:** Inside
      ii. **Address Type:** Static
      iii. **DNS Name:** 172.29.128.34 (This is your internal IP range)
      iv. **IP Address:** 172.29.128.34
      v. **Netmask:** 255.255.0.0
      vi. **Network Address:** 172.29.0.0
      vii. **Broadcast Address:** 172.29.222.255



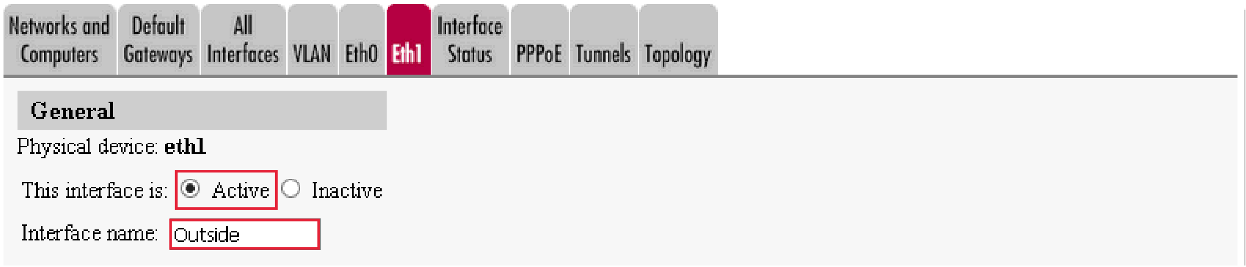
Directly Connected Networks (Help)

Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row
inside	Static	172.29.128.34	172.29.128.34	255.255.0.0	172.29.0.0	172.29.255.255		-	□

Step 4:

Navigate to **Network>ETH1 tab**.

1. Under the General menu,
   a. Confirm the following info is set for **General**:
      i. **This Interface:** Active
      ii. **Interface Name:** Outside



General

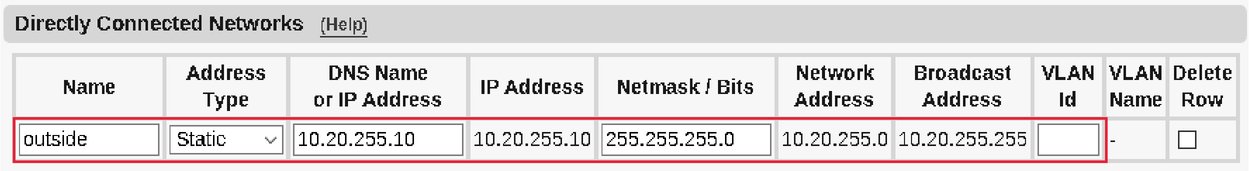
Physical device: **eth1**

This interface is: ● Active ○ Inactive

Interface name: Outside

b. Confirm the following info is set for **Directly Connected Networks**:

- i. **Name:** Outside
- ii. **Address Type:** Static
- iii. **DNS Name:** 10.20.255.10 (This is your public IP range)
- iv. **IP Address:** 10.20.255.10
- v. **Netmask:** 255.255.255.0
- vi. **Network Address:** 10.20.255.0
- vii. **Broadcast Address:** 10.20.255.255

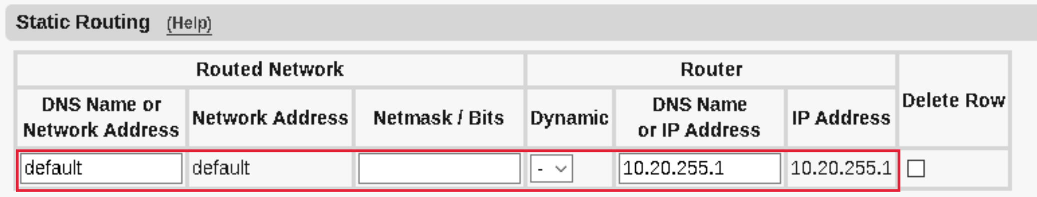


Directly Connected Networks (Help)

Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	VLAN Id	VLAN Name	Delete Row
outside	Static	10.20.255.10	10.20.255.10	255.255.255.0	10.20.255.0	10.20.255.255		-	□

c. Confirm the following info is set for **Static Routing**:

- i. Routed Network
  1. **DNS Name:** default
  2. **Network Address:** default
  3. **Netmask / Bits:**
- ii. Router
  1. **DNS Name:** 10.20.255.1
  2. **Network Address:** 10.20.255.1



Static Routing (Help)

Routed Network			Router			Delete Row
DNS Name or Network Address	Network Address	Netmask / Bits	Dynamic	DNS Name or IP Address	IP Address	
default	default		-	10.20.255.1	10.20.255.1	□

Step 5:

Navigate to **Network>Network and Computers tab**.

1. Under the Network and Computers menu, (The IP addresses will depend on the customers deployment and IP address ranges)

   a. Confirm the following info is set for the LAN on line 1:

Name	Subgroup	Lower Limit		Upper Limit		Interface/VLAN
		DNS / IP	IP Address	DNS / IP	IP Address	
LAN	-	172.29.128.0	172.29.128.0	172.29.131.255	172.29.131.255	inside (eth0 untagged)

   b. Confirm the following info is set for the Mitel-vTrunk on line 2:

Name	Subgroup	Lower Limit		Upper Limit		Interface/VLAN
		DNS / IP	IP Address	DNS / IP	IP Address	
Mitel-vTrunk	-	172.29.128.33	172.29.128.33			-

c. Confirm the following info is set for the ThinkTel on line 3:

Name	Subgroup	Lower Limit		Upper Limit		Interface/VLAN
		DNS / IP	IP Address	DNS / IP	IP Address	
ThinkTel	ThinkTel EDM					outside (eth1 untagged)
	ThinkTel Tor					outside (eth1 untagged)

d. Confirm the following info is set for the ThinkTel EDM on line 5:
The below IP's are 3 ThinkTel SIP proxies that have been sub netted:

- **SIP Proxy 1:** 208.68.17.32 /27
- **SIP Proxy 2:** 206.80.250.96 /27
- **SIP Proxy 3:** 209.197.133.0 /26

Subnets for the ThinkTel Proxies
208.68.17.32 - 208.68.17.62
206.80.250.96 - 206.80.250.126
209.197.133.1 - 209.80.250.126

Name	Subgroup	Lower Limit		Upper Limit		Interface/VLAN
		DNS / IP	IP Address	DNS / IP	IP Address	
ThinkTel EDM	-	206.80.250.96	206.80.250.96	206.80.250.126	206.80.250.126	outside (eth1 untagged)
	-	208.68.17.32	208.68.17.32	208.68.17.62	208.68.17.62	outside (eth1 untagged)
	-	20[redacted]52	20[redacted]52	20[redacted]52	20[redacted]52	outside (eth1 untagged)
	-	209.197.133.1	209.197.133.1	209.80.250.126	209.80.250.126	outside (eth1 untagged)

***NOTE:** These IP's are important as ThinkTel uses them to pass SIP traffic thus the reason for adding them as well.*

e. Confirm the following info is set for the ThinkTel Tor on line 9:
The below IP's are 3 ThinkTel SIP proxies that have been sub netted:

- **SIP Proxy 1:** 208.68.17.32 /27
- **SIP Proxy 2:** 206.80.250.96 /27
- **SIP Proxy 3:** 209.197.133.0 /26

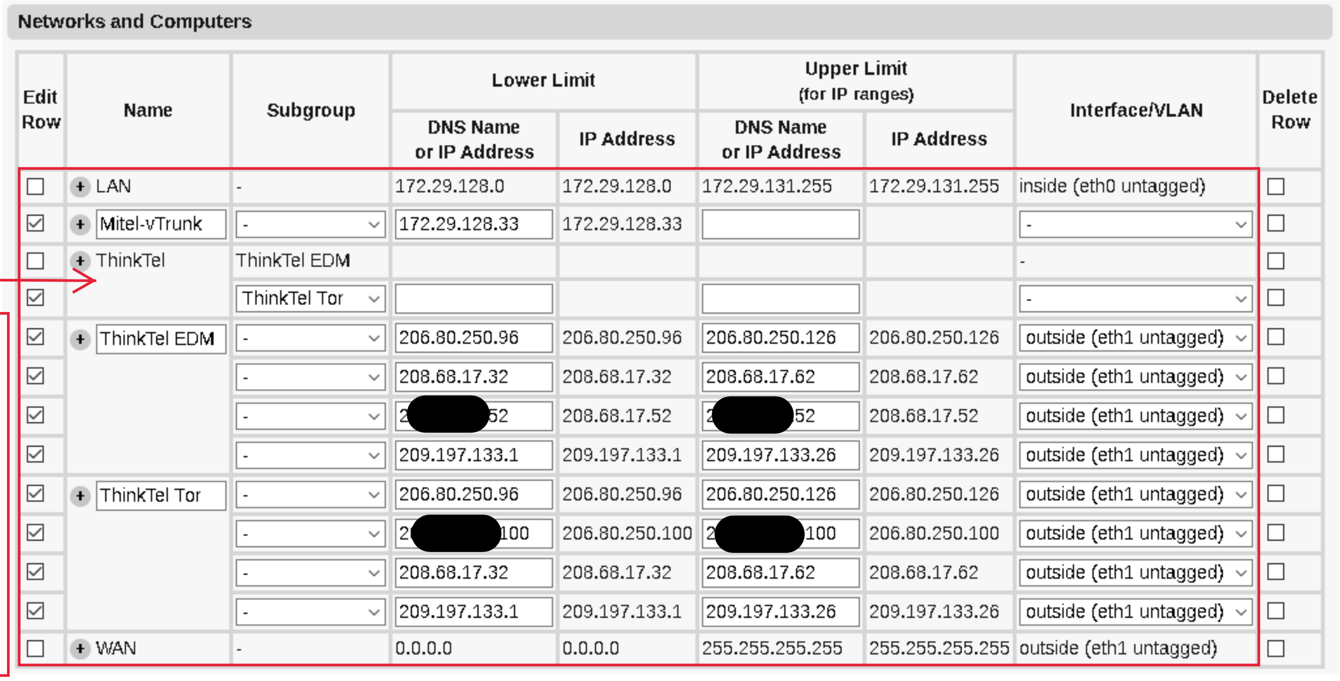
Subnets for the ThinkTel Proxies
208.68.17.32 - 208.68.17.62
206.80.250.96 - 206.80.250.126
209.197.133.1 - 209.80.250.126

Name	Subgroup	Lower Limit		Upper Limit		Interface/VLAN
		DNS / IP	IP Address	DNS / IP	IP Address	
ThinkTel Tor	-	206.80.250.96	206.80.250.96	206.80.250.126	206.80.250.126	outside (eth1 untagged)
	-	20[redacted]100	20[redacted]100	20[redacted]100	20[redacted]100	outside (eth1 untagged)
	-	208.68.17.52	208.68.17.52	608.68.17.52	608.68.17.52	outside (eth1 untagged)
	-	209.197.133.1	209.197.133.1	209.80.250.126	209.80.250.126	outside (eth1 untagged)

NOTE: These IP's are important as ThinkTel uses them to pass SIP traffic thus the reason for adding them as well.

f. Confirm the following info is set for the ShoreTel on line 13:

Name	Subgroup	Lower Limit		Upper Limit		Interface/VLAN
		DNS / IP	IP Address	DNS / IP	IP Address	
WAN	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	outside (eth1 untagged)



Networks and Computers

Edit Row	Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
			DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
☐	+ LAN	-	172.29.128.0	172.29.128.0	172.29.131.255	172.29.131.255	inside (eth0 untagged)	☐
☑	+ Mitel-vTrunk	-	172.29.128.33	172.29.128.33			-	☐
☐	+ ThinkTel	ThinkTel EDM					-	☐
☑		ThinkTel Tor					-	☐
☑	+ ThinkTel EDM	-	206.80.250.96	206.80.250.96	206.80.250.126	206.80.250.126	outside (eth1 untagged)	☐
☑		-	208.68.17.32	208.68.17.32	208.68.17.62	208.68.17.62	outside (eth1 untagged)	☐
☑		-	2[redacted]52	208.68.17.52	2[redacted]52	208.68.17.52	outside (eth1 untagged)	☐
☑		-	209.197.133.1	209.197.133.1	209.197.133.26	209.197.133.26	outside (eth1 untagged)	☐
☑	+ ThinkTel Tor	-	206.80.250.96	206.80.250.96	206.80.250.126	206.80.250.126	outside (eth1 untagged)	☐
☑		-	2[redacted]100	206.80.250.100	2[redacted]100	206.80.250.100	outside (eth1 untagged)	☐
☑		-	208.68.17.32	208.68.17.32	208.68.17.62	208.68.17.62	outside (eth1 untagged)	☐
☑		-	209.197.133.1	209.197.133.1	209.197.133.26	209.197.133.26	outside (eth1 untagged)	☐
☐	+ WAN	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	outside (eth1 untagged)	☐

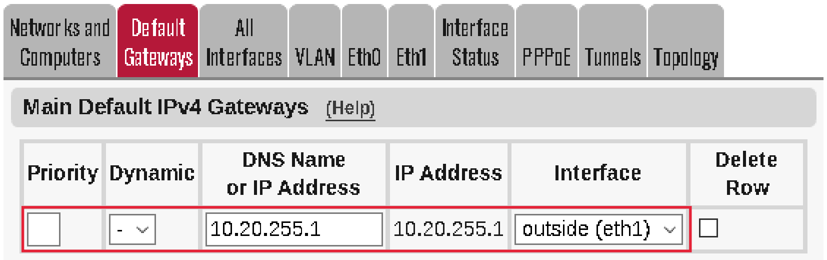
The 2 ThinkTel SIP bindings are added here as the Binding addresses will be added under the Ingate SIP Trunk selection.

This is done to add a layer of redundancy at the SIP provider level.

Step 6:

Navigate to **Network>Default Gateways tab**.

1. Under the Main Default IPv4 Gateway menu,
   a. Confirm the following info is set for the ***Main Default IPV4 Gateway***:
      i. **DNS Name/IP Address:** 10.20.255.1
      ii. **IP Address:** 10.20.255.1
      iii. **Interface:** outside (eth1)



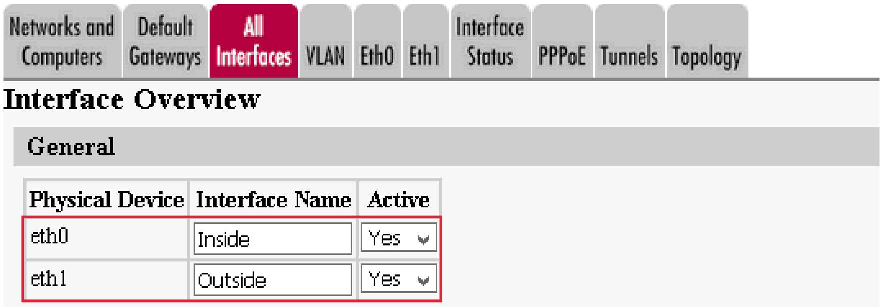
Main Default IPv4 Gateways (Help)

Priority	Dynamic	DNS Name or IP Address	IP Address	Interface	Delete Row
	-	10.20.255.1	10.20.255.1	outside (eth1)	☐

Step 7:

Navigate to **Network>All Interfaces tab**.

1. Under the General menu,
   a. Confirm the following info is set for **General**:
      i. **Physical Device:** eth0
      ii. **Interface Name:** Inside
      iii. **Active:** Yes
      iv. **Physical Device:** eth1
      v. **Interface Name:** Outside
      vi. **Active:** Yes



Interface Overview

General

Physical Device	Interface Name	Active
eth0	Inside	Yes
eth1	Outside	Yes

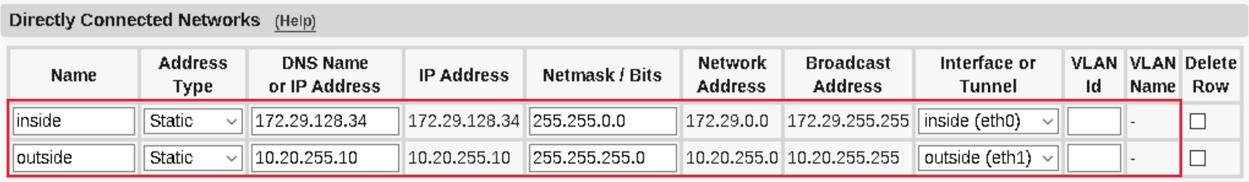
b. Confirm the following info is set for *Directly Connected Networks Menu*:

A. Inside Interface:

i.	**Name:**	inside
ii.	**Address Type:**	Static
iii.	**DNS Name:**	172.29.128.34
iv.	**IP Address:**	172.29.128.34
v.	**Netmask/Bits:**	255.255.0.0
vi.	**Network Address:**	179.29.0.0
vii.	**Broadcast Address:**	172.29.255.255
viii.	**Interface:**	inside (eth0)

B. Outside Interface:

i.	**Name:**	outside
ii.	**Address Type:**	Static
iii.	**DNS Name:**	10.20.255.10
iv.	**IP Address:**	10.20.255.10
v.	**Netmask/Bits:**	255.255.255.0
vi.	**Network Address:**	10.20.255.0
vii.	**Broadcast Address:**	10.20.255.255
viii.	**Interface:**	outside (eth1)



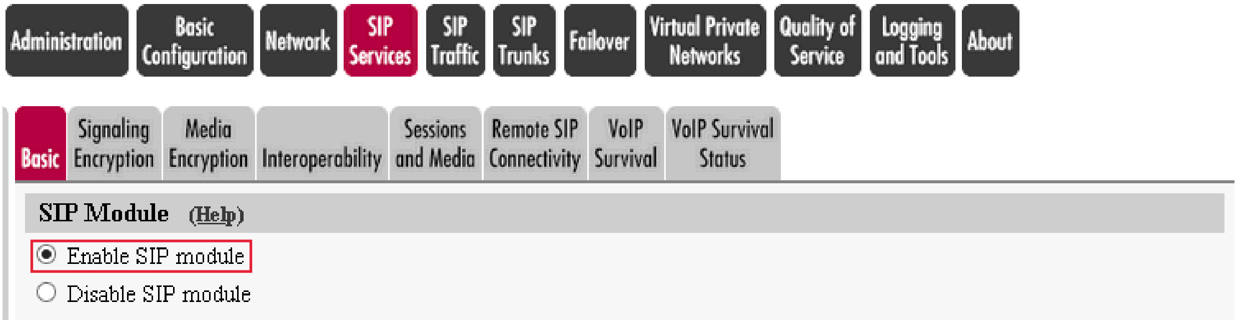
Directly Connected Networks (Help)

Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	Interface or Tunnel	VLAN Id	VLAN Name	Delete Row
inside	Static	172.29.128.34	172.29.128.34	255.255.0.0	172.29.0.0	172.29.255.255	inside (eth0)		-	□
outside	Static	10.20.255.10	10.20.255.10	255.255.255.0	10.20.255.0	10.20.255.255	outside (eth1)		-	□

Step 8:

Navigate to **SIP Services>Basic tab**.

1. Under the SIP Module menu,
   a. Ensure Enable SIP module is selected.

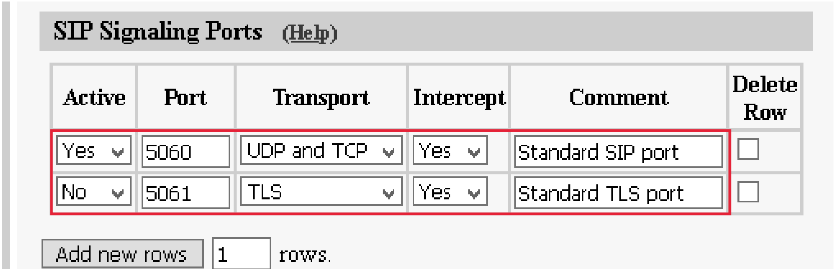


SIP Module (Help)

● Enable SIP module

○ Disable SIP module

2. Under the SIP Signaling Ports menu,
   a. Line 1:
      i. **Active:** Yes
      ii. **Port:** 5060
      iii. **Transport:** UDP and TCP
      iv. **Intercept:** Yes
      v. **Comment:** standard SIP port
   b. Line 2:
      vi. Active: No
      vii. **Port:** 5061
      viii. **Transport:** TLS
      ix. **Intercept:** Yes
      x. **Comment:** standard TLS port

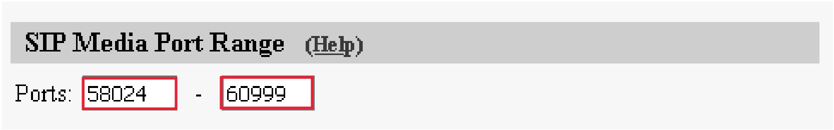


SIP Signaling Ports (Help)

Active	Port	Transport	Intercept	Comment	Delete Row
Yes	5060	UDP and TCP	Yes	Standard SIP port	□
No	5061	TLS	Yes	Standard TLS port	□

Add new rows 1 rows.

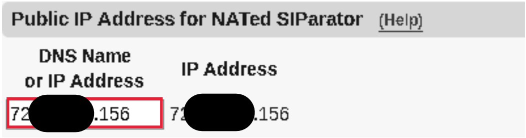
3. Under the SIP Media Port Range menu,
   a. **Set Ports to the following:** 58024 - 60999



SIP Media Port Range (Help)

Ports: 58024 - 60999

4. Under the Public IP Address for NATed SIParator menu,
   a. **Set the Public IP:** 72.xxx.xxx.156



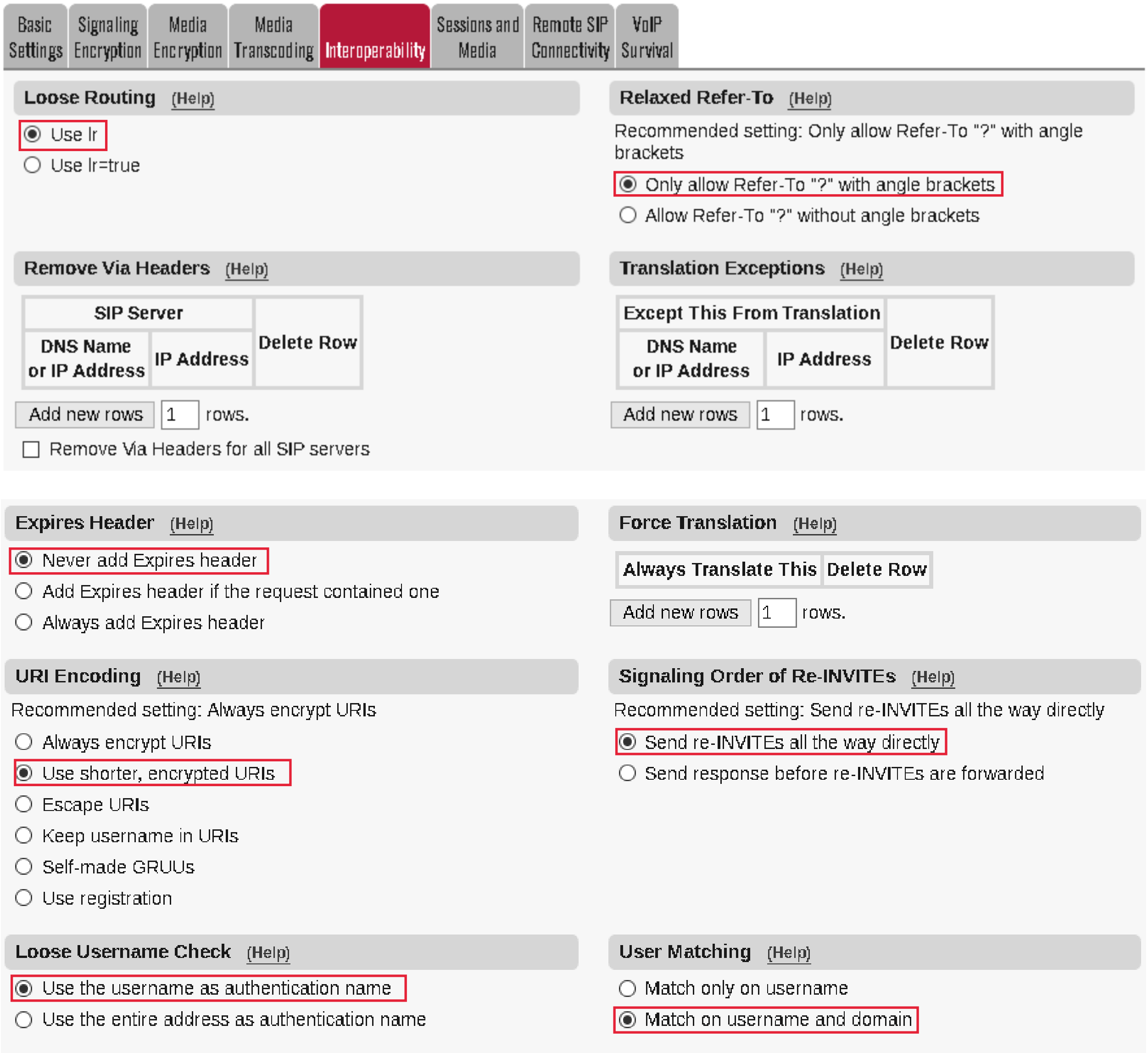
Public IP Address for NATed SIParator (Help)

DNS Name or IP Address	IP Address
72[redacted].156	7[redacted].156

Step 9:

Navigate to **SIP Services>Interoperability tab**.

1. Ensure the following fields are set in the below windows



Loose Routing (Help)

● Use lr

○ Use lr=true

Relaxed Refer-To (Help)

Recommended setting: Only allow Refer-To "?" with angle brackets

● Only allow Refer-To "?" with angle brackets

○ Allow Refer-To "?" without angle brackets

Remove Via Headers (Help)

SIP Server		Delete Row
DNS Name or IP Address	IP Address	

Add new rows [1] rows.

□ Remove Via Headers for all SIP servers

Translation Exceptions (Help)

Except This From Translation		Delete Row
DNS Name or IP Address	IP Address	

Add new rows [1] rows.

Expires Header (Help)

● Never add Expires header

○ Add Expires header if the request contained one

○ Always add Expires header

Force Translation (Help)

Always Translate This	Delete Row

Add new rows [1] rows.

URI Encoding (Help)

Recommended setting: Always encrypt URIs

○ Always encrypt URIs

● Use shorter, encrypted URIs

○ Escape URIs

○ Keep username in URIs

○ Self-made GRUUs

○ Use registration

Signaling Order of Re-INVITEs (Help)

Recommended setting: Send re-INVITEs all the way directly

● Send re-INVITEs all the way directly

○ Send response before re-INVITEs are forwarded

Loose Username Check (Help)

● Use the username as authentication name

○ Use the entire address as authentication name

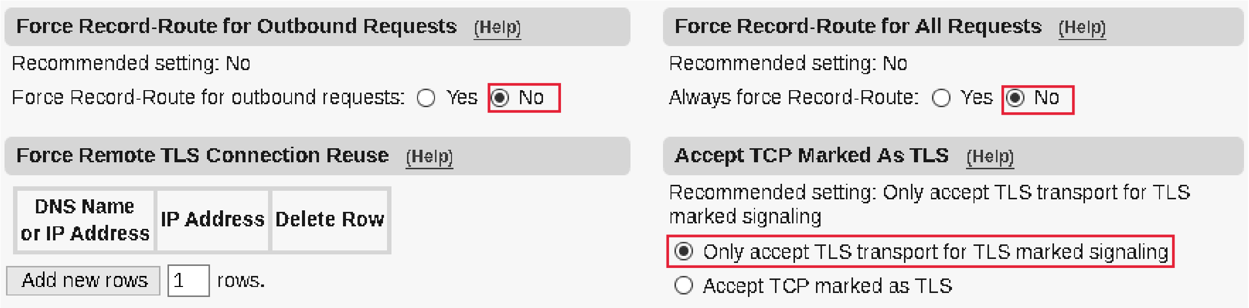
User Matching (Help)

○ Match only on username

● Match on username and domain

***NOTE:** Your configuration might look different form the example in this document therefore if you require any further assistance please contact Ingate Support, +1 (866) 809-0002*

***Operational Hours:** Monday – Friday 9am – 6pm Eastern*



Force Record-Route for Outbound Requests (Help)

Recommended setting: No

Force Record-Route for outbound requests: ○ Yes ● No

Force Remote TLS Connection Reuse (Help)

DNS Name or IP Address	IP Address	Delete Row

Add new rows 1 rows.

Force Record-Route for All Requests (Help)

Recommended setting: No

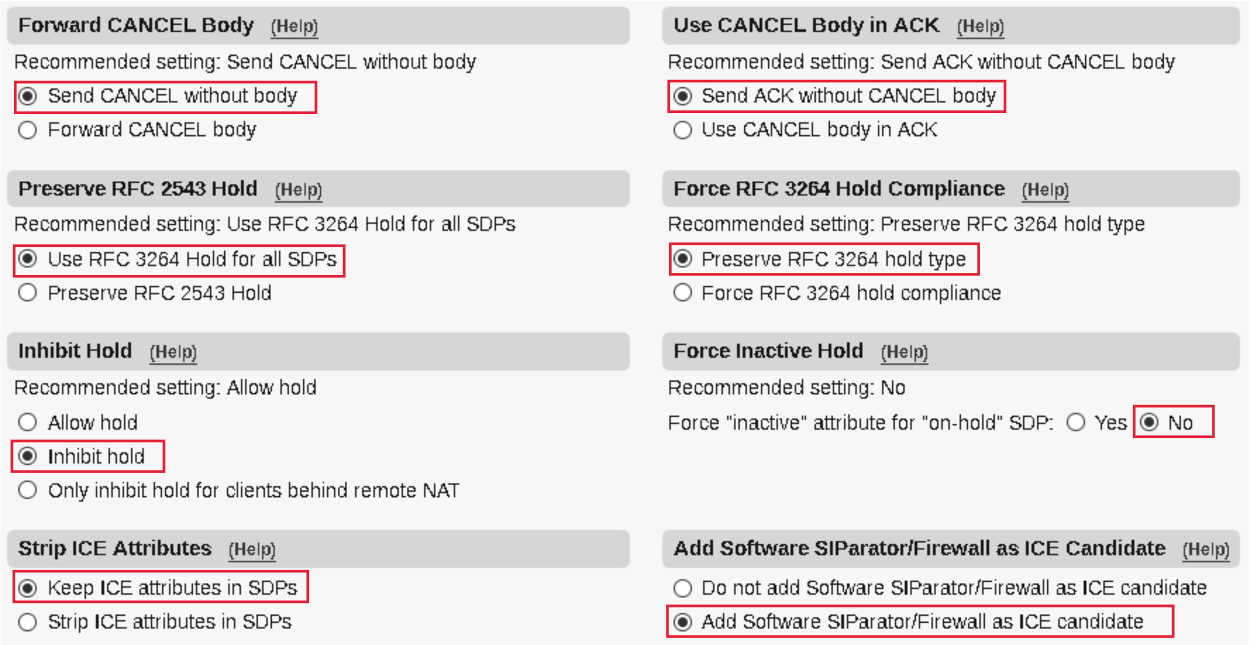
Always force Record-Route: ○ Yes ● No

Accept TCP Marked As TLS (Help)

Recommended setting: Only accept TLS transport for TLS marked signaling

● Only accept TLS transport for TLS marked signaling

○ Accept TCP marked as TLS



Forward CANCEL Body (Help)

Recommended setting: Send CANCEL without body

● Send CANCEL without body

○ Forward CANCEL body

Preserve RFC 2543 Hold (Help)

Recommended setting: Use RFC 3264 Hold for all SDPs

● Use RFC 3264 Hold for all SDPs

○ Preserve RFC 2543 Hold

Inhibit Hold (Help)

Recommended setting: Allow hold

○ Allow hold

● Inhibit hold

○ Only inhibit hold for clients behind remote NAT

Strip ICE Attributes (Help)

● Keep ICE attributes in SDPs

○ Strip ICE attributes in SDPs

Use CANCEL Body in ACK (Help)

Recommended setting: Send ACK without CANCEL body

● Send ACK without CANCEL body

○ Use CANCEL body in ACK

Force RFC 3264 Hold Compliance (Help)

Recommended setting: Preserve RFC 3264 hold type

● Preserve RFC 3264 hold type

○ Force RFC 3264 hold compliance

Force Inactive Hold (Help)

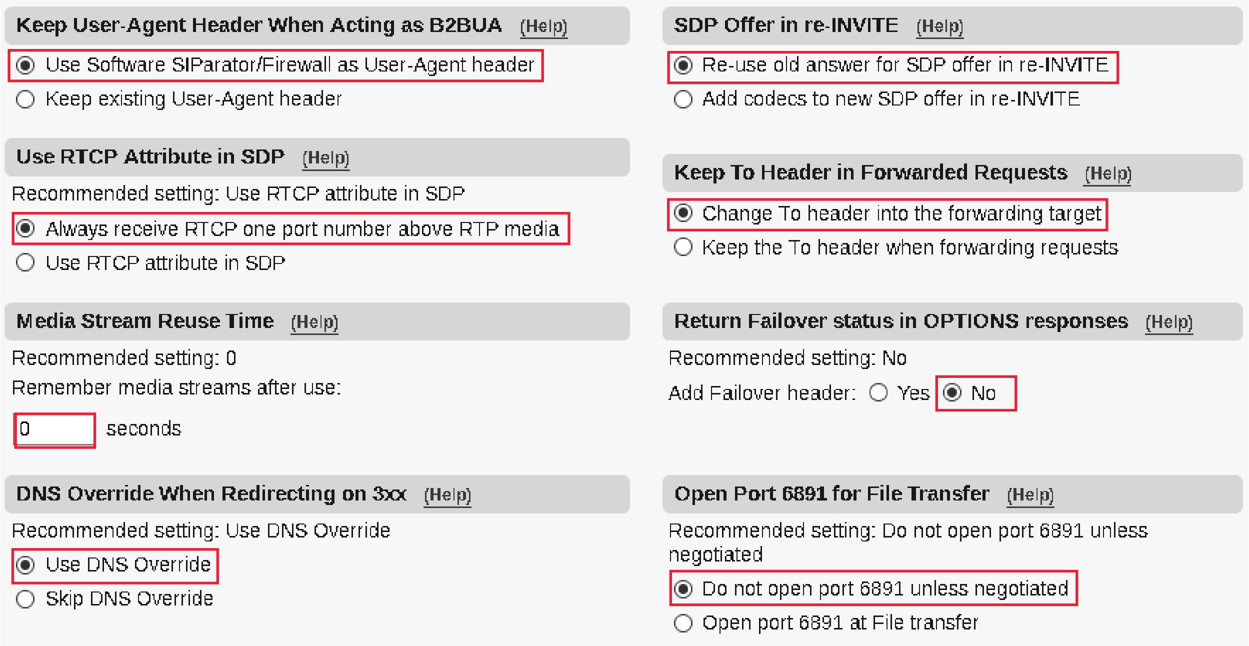
Recommended setting: No

Force "inactive" attribute for "on-hold" SDP: ○ Yes ● No

Add Software SIParator/Firewall as ICE Candidate (Help)

○ Do not add Software SIParator/Firewall as ICE candidate

● Add Software SIParator/Firewall as ICE candidate



Keep User-Agent Header When Acting as B2BUA (Help)

● Use Software SIParator/Firewall as User-Agent header

○ Keep existing User-Agent header

Use RTCP Attribute in SDP (Help)

Recommended setting: Use RTCP attribute in SDP

● Always receive RTCP one port number above RTP media

○ Use RTCP attribute in SDP

Media Stream Reuse Time (Help)

Recommended setting: 0

Remember media streams after use:

0 seconds

DNS Override When Redirecting on 3xx (Help)

Recommended setting: Use DNS Override

● Use DNS Override

○ Skip DNS Override

SDP Offer in re-INVITE (Help)

● Re-use old answer for SDP offer in re-INVITE

○ Add codecs to new SDP offer in re-INVITE

Keep To Header in Forwarded Requests (Help)

● Change To header into the forwarding target

○ Keep the To header when forwarding requests

Return Failover status in OPTIONS responses (Help)

Recommended setting: No

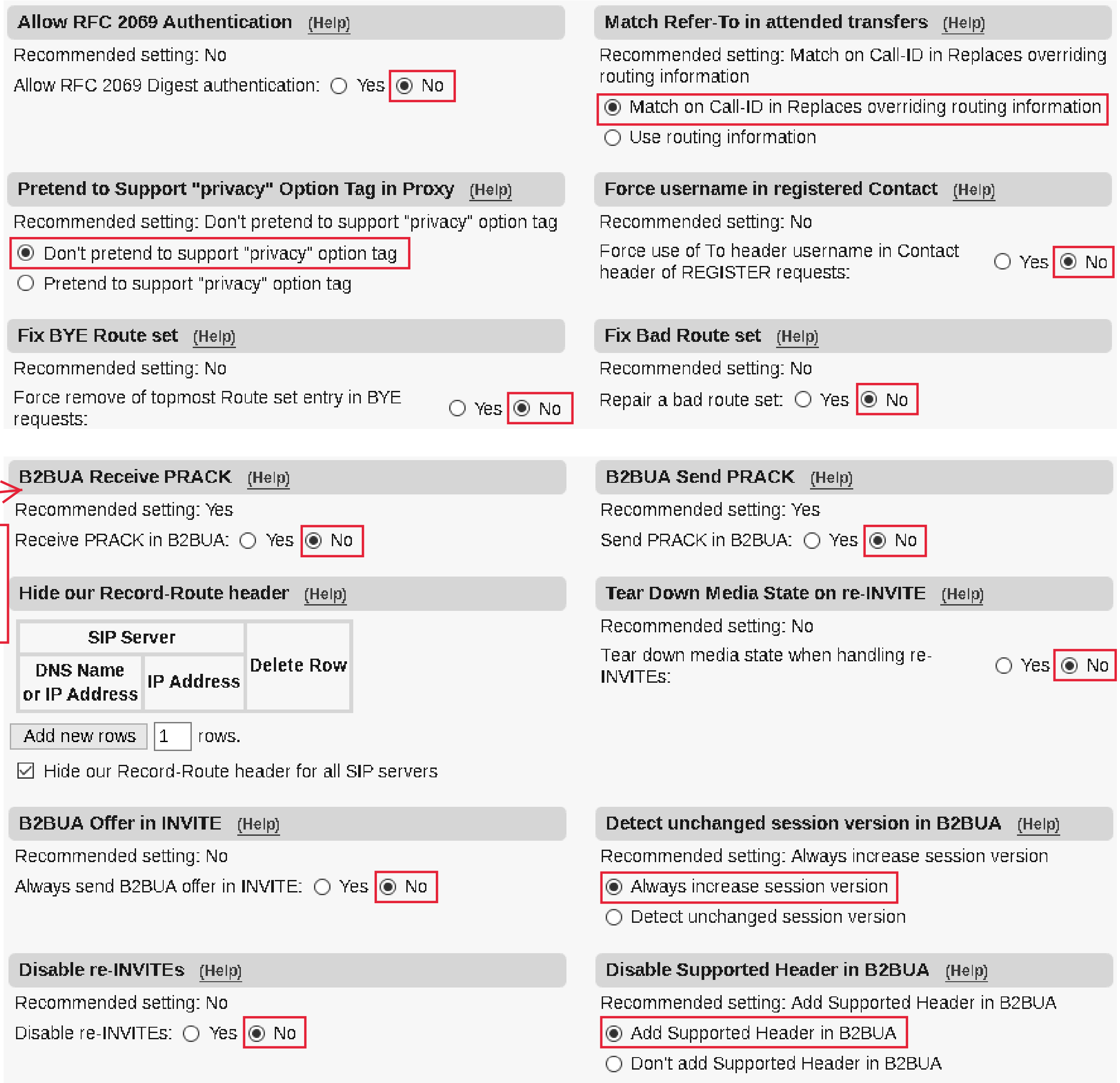
Add Failover header: ○ Yes ● No

Open Port 6891 for File Transfer (Help)

Recommended setting: Do not open port 6891 unless negotiated

● Do not open port 6891 unless negotiated

○ Open port 6891 at File transfer



Allow RFC 2069 Authentication (Help)

Recommended setting: No

Allow RFC 2069 Digest authentication: ○ Yes ● No

Pretend to Support "privacy" Option Tag in Proxy (Help)

Recommended setting: Don't pretend to support "privacy" option tag

● Don't pretend to support "privacy" option tag

○ Pretend to support "privacy" option tag

Fix BYE Route set (Help)

Recommended setting: No

Force remove of topmost Route set entry in BYE requests: ○ Yes ● No

B2BUA Receive PRACK (Help)

Recommended setting: Yes

Receive PRACK in B2BUA: ○ Yes ● No

PRACK is turned off as it is known to cause issues with SIP

Hide our Record-Route header (Help)

SIP Server		Delete Row
DNS Name or IP Address	IP Address	

Add new rows [1] rows.

☑ Hide our Record-Route header for all SIP servers

B2BUA Offer in INVITE (Help)

Recommended setting: No

Always send B2BUA offer in INVITE: ○ Yes ● No

Disable re-INVITEs (Help)

Recommended setting: No

Disable re-INVITEs: ○ Yes ● No

Match Refer-To in attended transfers (Help)

Recommended setting: Match on Call-ID in Replaces overriding routing information

● Match on Call-ID in Replaces overriding routing information

○ Use routing information

Force username in registered Contact (Help)

Recommended setting: No

Force use of To header username in Contact header of REGISTER requests: ○ Yes ● No

Fix Bad Route set (Help)

Recommended setting: No

Repair a bad route set: ○ Yes ● No

B2BUA Send PRACK (Help)

Recommended setting: Yes

Send PRACK in B2BUA: ○ Yes ● No

Tear Down Media State on re-INVITE (Help)

Recommended setting: No

Tear down media state when handling re-INVITEs: ○ Yes ● No

Detect unchanged session version in B2BUA (Help)

Recommended setting: Always increase session version

● Always increase session version

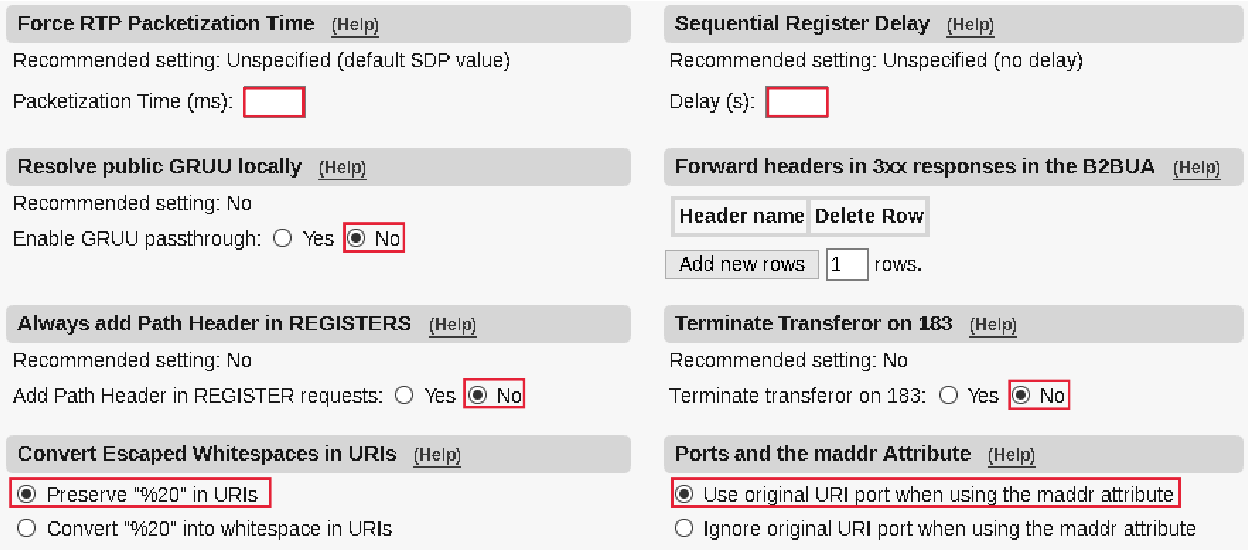
○ Detect unchanged session version

Disable Supported Header in B2BUA (Help)

Recommended setting: Add Supported Header in B2BUA

● Add Supported Header in B2BUA

○ Don't add Supported Header in B2BUA



Force RTP Packetization Time (Help)

Recommended setting: Unspecified (default SDP value)

Packetization Time (ms): [ ]

Resolve public GRUU locally (Help)

Recommended setting: No

Enable GRUU passthrough: ○ Yes ● No

Always add Path Header in REGISTERS (Help)

Recommended setting: No

Add Path Header in REGISTER requests: ○ Yes ● No

Convert Escaped Whitespaces in URIs (Help)

● Preserve "%20" in URIs
○ Convert "%20" into whitespace in URIs

Sequential Register Delay (Help)

Recommended setting: Unspecified (no delay)

Delay (s): [ ]

Forward headers in 3xx responses in the B2BUA (Help)

Header name	Delete Row

Add new rows [1] rows.

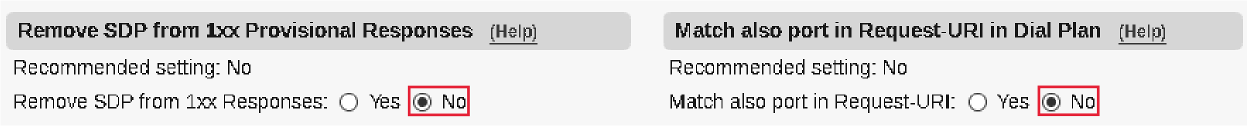
Terminate Transferor on 183 (Help)

Recommended setting: No

Terminate transferor on 183: ○ Yes ● No

Ports and the maddr Attribute (Help)

● Use original URI port when using the maddr attribute
○ Ignore original URI port when using the maddr attribute



Remove SDP from 1xx Provisional Responses (Help)

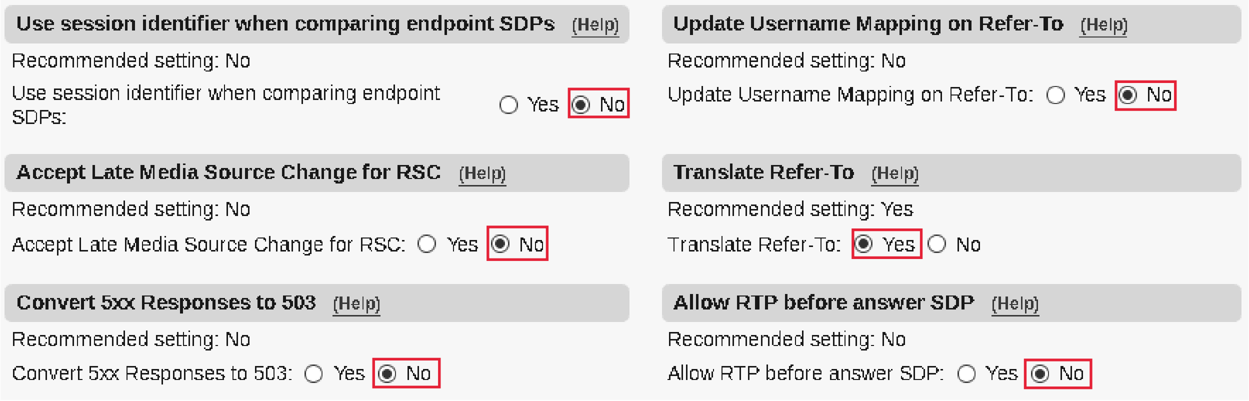
Recommended setting: No

Remove SDP from 1xx Responses: ○ Yes ● No

Match also port in Request-URI in Dial Plan (Help)

Recommended setting: No

Match also port in Request-URI: ○ Yes ● No



Use session identifier when comparing endpoint SDPs (Help)

Recommended setting: No

Use session identifier when comparing endpoint SDPs: ○ Yes ● No

Accept Late Media Source Change for RSC (Help)

Recommended setting: No

Accept Late Media Source Change for RSC: ○ Yes ● No

Convert 5xx Responses to 503 (Help)

Recommended setting: No

Convert 5xx Responses to 503: ○ Yes ● No

Update Username Mapping on Refer-To (Help)

Recommended setting: No

Update Username Mapping on Refer-To: ○ Yes ● No

Translate Refer-To (Help)

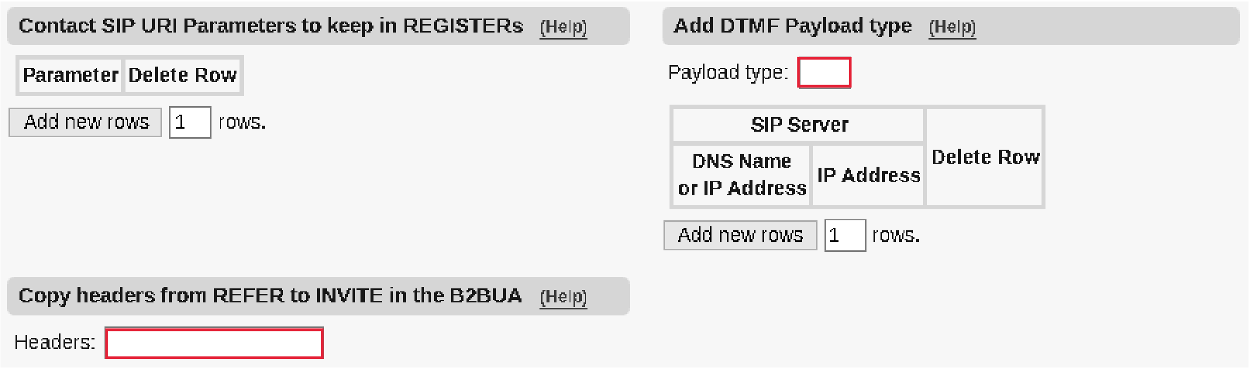
Recommended setting: Yes

Translate Refer-To: ● Yes ○ No

Allow RTP before answer SDP (Help)

Recommended setting: No

Allow RTP before answer SDP: ○ Yes ● No



Contact SIP URI Parameters to keep in REGISTERs (Help)

Parameter	Delete Row

Add new rows [1] rows.

Copy headers from REFER to INVITE in the B2BUA (Help)

Headers: [ ]

Add DTMF Payload type (Help)

Payload type: [ ]

SIP Server		Delete Row
DNS Name or IP Address	IP Address	

Add new rows [1] rows.

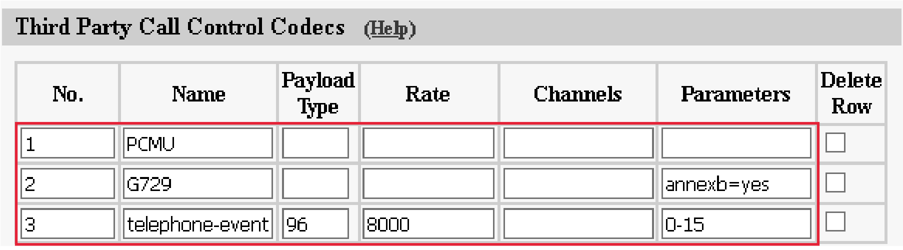
Step 10:

Navigate to **SIP Services>Session and Media tab**.

2. Under the Third Party Call Control Codecs menu,
   a. Ensure the following is set for Line 1:
      i. **No:** 1
      ii. **Name:** PCMU
      iii. **Payload Type:** blank
      iv. **Rate:** blank
      v. **Channels:** blank
      vi. **Parameters:** blank

   b. Ensure the following is set for Line 2:
      i. **No:** 2
      ii. **Name:** G729
      iii. **Payload Type:** blank
      iv. **Rate:** blank
      v. **Channels:** blank
      vi. **Parameters:** annexb=yes

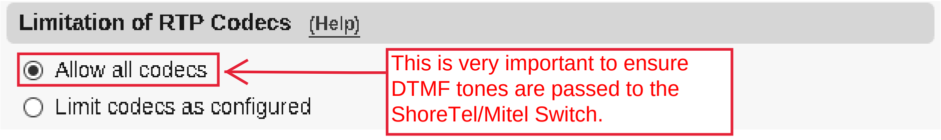
   c. Ensure the following is set for Line 3:
      i. **No:** 3
      ii. **Name:** telephone event
      iii. **Payload Type:** 96
      iv. **Rate:** 8000
      v. **Channels:** blank
      vi. **Parameters:** 0-15



Third Party Call Control Codecs (Help)

No.	Name	Payload Type	Rate	Channels	Parameters	Delete Row
1	PCMU					□
2	G729				annexb=yes	□
3	telephone-event	96	8000		0-15	□

3. Under the Limitation of RTP Codes menu,
   a. Ensure that Allow all codes are set:
      i. If this option is not selected and specific codecs are selected then the Ingate will not pass any DTMF tones to the Mitel, this is important to take note of as the caller will not be able to navigate any Auto Attendant Menu.



Limitation of RTP Codecs (Help)

● Allow all codecs

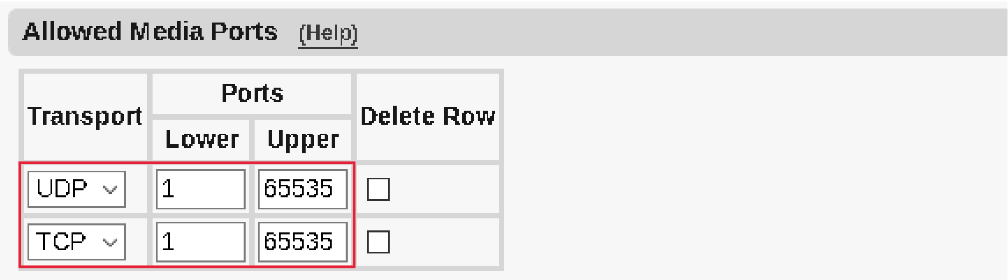
○ Limit codecs as configured

This is very important to ensure DTMF tones are passed to the ShoreTel/Mitel Switch.

4. Under the Allowed Media Ports menu,
    a. Ensure the following is set for Line 1:
        i. **Transport:** UDP
        i. **Ports Lower:** 1
        ii. **Ports Upper:** 65535

    b. Ensure the following is set for Line 2:
        i. **Transport:** TCP
        ii. **Ports Lower:** 1
        iii. **Ports Upper:** 65535

The lower TCP/UDP ports set to 1 will allow older ShoreTel devices to pass calls as they traditionally listen on lower ports than the default set ports.



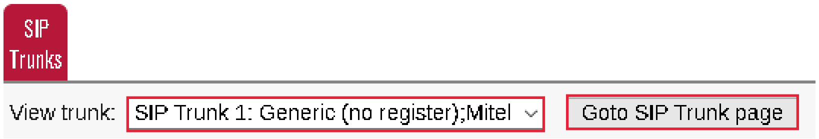
Allowed Media Ports (Help)

Transport	Ports		Delete Row
	Lower	Upper	
UDP	1	65535	□
TCP	1	65535	□

Step 11:

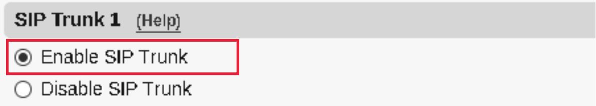
Navigate to **SIP Trunks>SIP Trunks tab**.

1. Under the Goto SIP Trunk page,
   Select the Goto SIP Trunk button will allow the creation of the SIP Trunk



View trunk: SIP Trunk 1: Generic (no register);Mitel

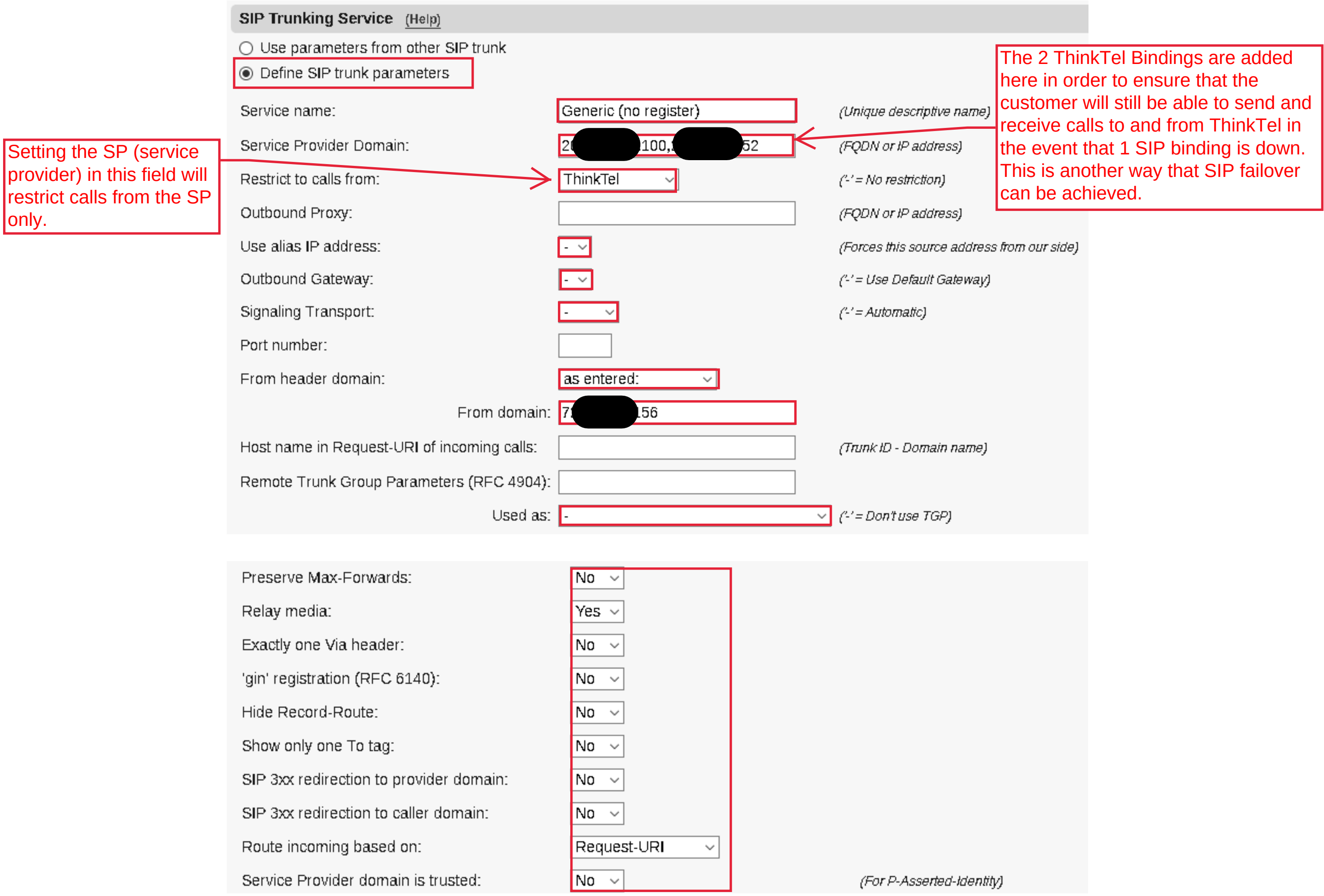
2. Under the SIP Trunk 1 menu,
    a. Ensure the Enable SIP Trunk is set:



SIP Trunk 1 (Help)

● Enable SIP Trunk
○ Disable SIP Trunk

3. Under the SIP Trunking Service menu,
    a. Ensure the following is set:
        i. **Define SIP Trunk Parameters:** Selected
        ii. **Service Name:** Generic (no register)
        iii. **Service Provider Domain:** 206.80.250.100,208.68.17.52
        iv. **Restrict to calls from:** ThinkTel
        v. **From header domain:** as entered:
        vi. **From Domain:** 72.xxx.xxx.156
        vii. **Route incoming based on:** Request-URI



SIP Trunking Service (Help)

○ Use parameters from other SIP trunk
● Define SIP trunk parameters

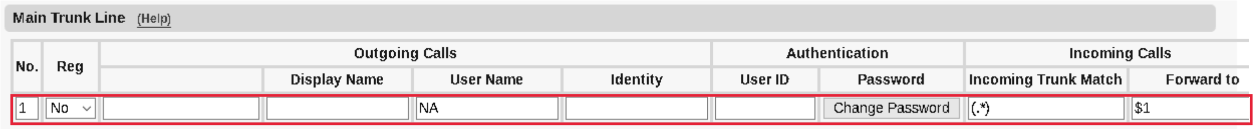
Service name:	Generic (no register)	(Unique descriptive name)
Service Provider Domain:	2[redacted]100,[redacted]52	(FQDN or IP address)
Restrict to calls from:	ThinkTel	('-' = No restriction)
Outbound Proxy:		(FQDN or IP address)
Use alias IP address:	-	(Forces this source address from our side)
Outbound Gateway:	-	('-' = Use Default Gateway)
Signaling Transport:	-	('-' = Automatic)
Port number:		
From header domain:	as entered:	
From domain:	7[redacted]56	
Host name in Request-URI of incoming calls:		(Trunk ID - Domain name)
Remote Trunk Group Parameters (RFC 4904):		
Used as:	-	('-' = Don't use TGP)

Preserve Max-Forwards:	No	
Relay media:	Yes	
Exactly one Via header:	No	
'gin' registration (RFC 6140):	No	
Hide Record-Route:	No	
Show only one To tag:	No	
SIP 3xx redirection to provider domain:	No	
SIP 3xx redirection to caller domain:	No	
Route incoming based on:	Request-URI	
Service Provider domain is trusted:	No	(For P-Asserted-Identity)

Setting the SP (service provider) in this field will restrict calls from the SP only.

The 2 ThinkTel Bindings are added here in order to ensure that the customer will still be able to send and receive calls to and from ThinkTel in the event that 1 SIP binding is down. This is another way that SIP failover can be achieved.

4. Under the Main Trunk Line menu,
   a. Ensure the following is set:
      i. **No:** 1
      ii. **Reg:** No
      iii. **Username:** NA
      iv. **Incoming Trunk Match:** (.*)
      v. **Forward to:** $1

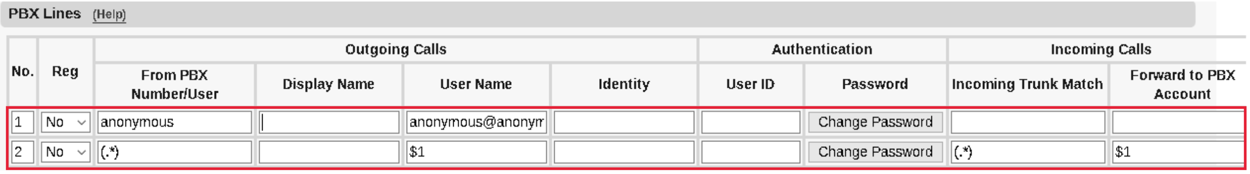


Main Trunk Line (Help)

No.	Reg	Outgoing Calls				Authentication		Incoming Calls	
			Display Name	User Name	Identity	User ID	Password	Incoming Trunk Match	Forward to
1	No			NA			Change Password	(.*)	$1

5. Under the PBX Line menu,
   a. Ensure the following is set:
      i. **No:** 1
      ii. **Reg:** No
      iii. **From PBX:** anonymous
      iv. **Username:** anonymous@anonymous

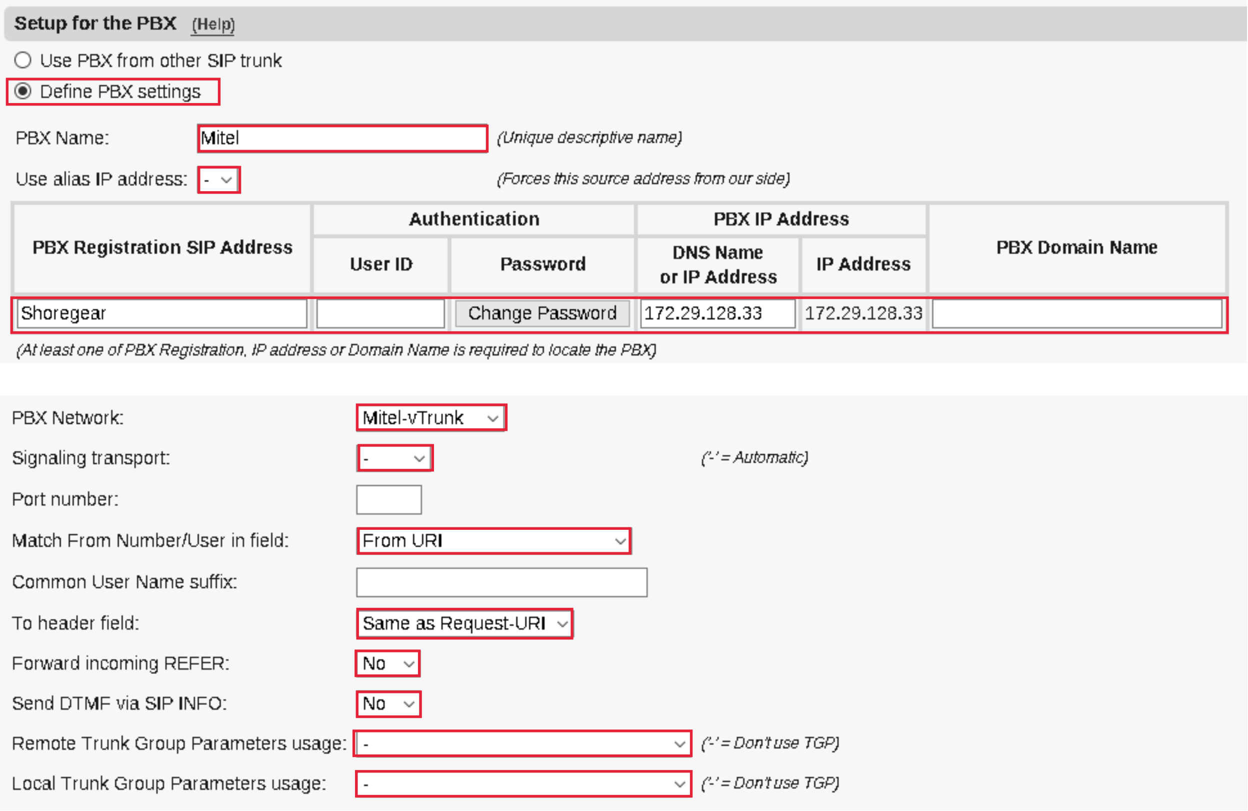
i. **No:** 2
ii. **Reg:** No
iii. **From PBX:** (.*)
iv. **Username:** $1
v. **Incoming Trunk Match:** (.*)
vi. **Forward to:** $1



PBX Lines (Help)

No.	Reg	Outgoing Calls				Authentication		Incoming Calls	
		From PBX Number/User	Display Name	User Name	Identity	User ID	Password	Incoming Trunk Match	Forward to PBX Account
1	No	anonymous		anonymous@anonym			Change Password		
2	No	(.*)		$1			Change Password	(.*)	$1

6. Under the Setup for the PBX menu,
   a. Ensure the following is set:
      i. **Define PBX settings:**
      ii. **PBX Name:** Mitel
      iii. **PBX Registration:** Shoregear
      iv. **DNS Name:** 172.29.128.33
      v. **IP Address:** 172.19.128.33
      vi. **PBX Network:** Mitel-vTrunk
      vii. **Match From Number:** From URI
      viii. **To header field:** Same as Request-URI
      ix. **Forward incoming REFER:** No
      x. **Send DTMF via SIP INFO:** No



Setup for the PBX (Help)

○ Use PBX from other SIP trunk
● Define PBX settings

PBX Name: Mitel *(Unique descriptive name)*

Use alias IP address: - *(Forces this source address from our side)*

PBX Registration SIP Address	Authentication		PBX IP Address		PBX Domain Name
	User ID	Password	DNS Name or IP Address	IP Address	
Shoregear		Change Password	172.29.128.33	172.29.128.33	

(At least one of PBX Registration, IP address or Domain Name is required to locate the PBX)

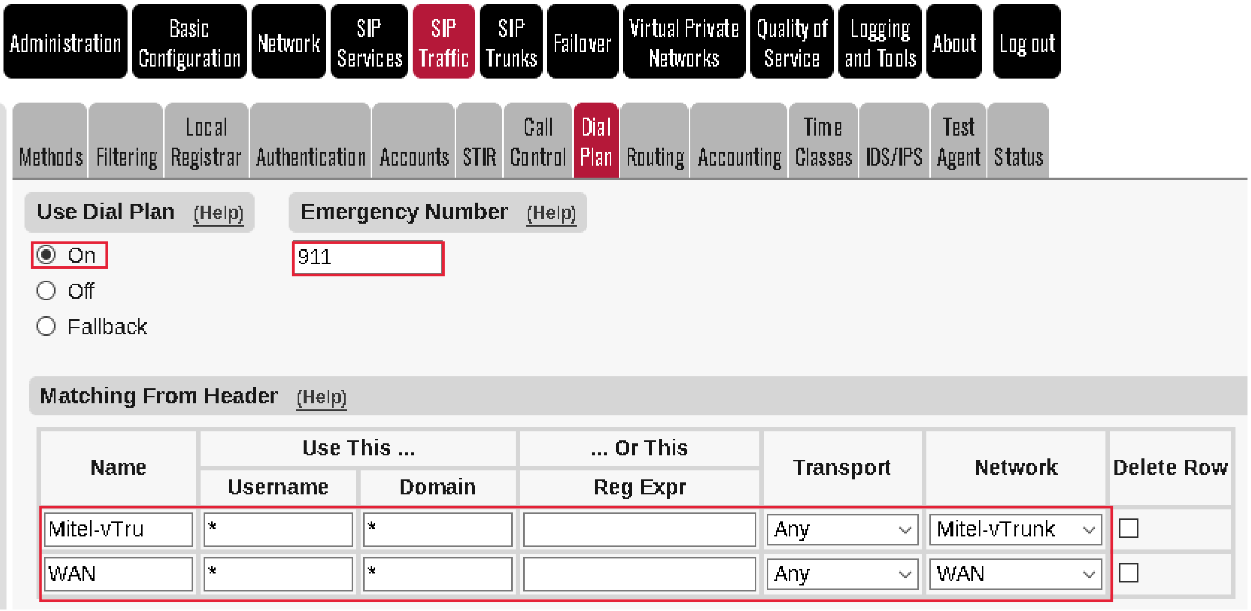
PBX Network:	Mitel-vTrunk	
Signaling transport:	-	*('-' = Automatic)*
Port number:		
Match From Number/User in field:	From URI	
Common User Name suffix:		
To header field:	Same as Request-URI	
Forward incoming REFER:	No	
Send DTMF via SIP INFO:	No	
Remote Trunk Group Parameters usage:	-	*('-' = Don't use TGP)*
Local Trunk Group Parameters usage:	-	*('-' = Don't use TGP)*

Step 11:

Navigate to **SIP Traffic>Dial Plan tab**.

1. Under the Matching From Header menu,
   a. Ensure the following is set for Line 1:
      i. **Name:** Mitel-vTrunk
      ii. **Use This Username:** *
      iii. **Use This Domain:** *
      iv. **Transport:** Any
      v. **Network:** Mitel-vTrunk

   b. Ensure the following is set for Line 2:
      i. **Name:** WAN
      ii. **Use This Username:** *
      iii. **Use This Domain:** *
      iv. **Transport:** Any
      v. **Network:** WAN



Use Dial Plan (Help)

● On
○ Off
○ Fallback

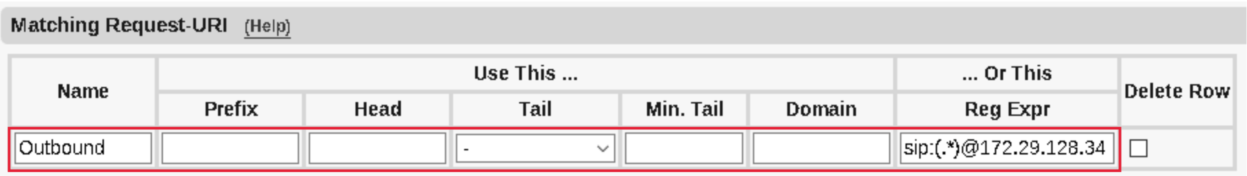
Emergency Number (Help)

911

Matching From Header (Help)

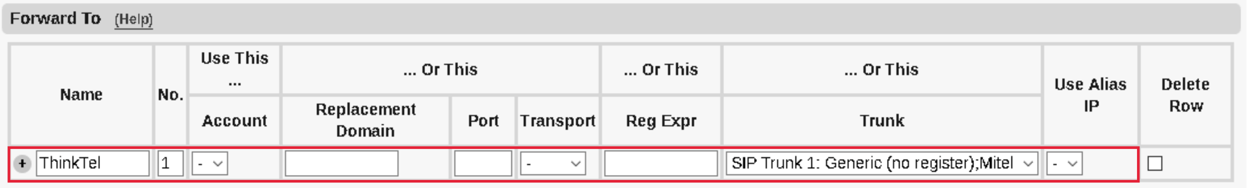
Name	Use This ...		... Or This	Transport	Network	Delete Row
	Username	Domain	Reg Expr			
Mitel-vTru	*	*		Any	Mitel-vTrunk	□
WAN	*	*		Any	WAN	□

2. Under the Matching Request-URI menu,
   a. Ensure the following is set for Line 1:
      i. **Name:** Outbound
      ii. **Reg Expr:** sip:(.*)@172.29.128.34


Matching Request-URI (Help)

Name	Use This ...					... Or This	Delete Row
	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
Outbound			-			sip:(.*)@172.29.128.34	□

3. Under the Forward To menu,
    a. Ensure the following is set for Line 1:
        i. **Name:** ThinkTel
        ii. **No:** 1
        iii. **Trunk:** SIP Trunk 1: Generic (no register);Mitel

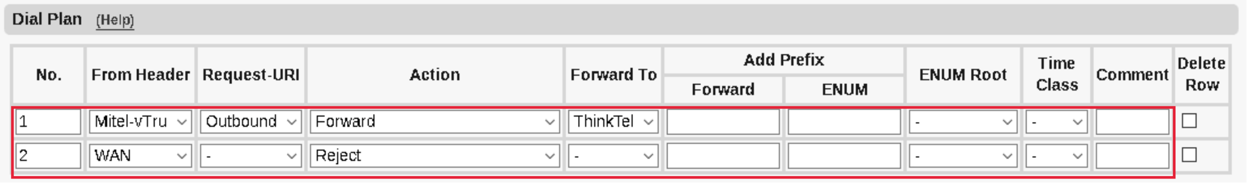


Forward To (Help)

Name	No.	Use This …	… Or This			… Or This	… Or This	Use Alias IP	Delete Row
		Account	Replacement Domain	Port	Transport	Reg Expr	Trunk		
ThinkTel	1	-			-		SIP Trunk 1: Generic (no register);Mitel	-	□

4. Under the Dial Plan menu,
    a. Ensure the following is set for Line 1:
        i. **No:** 1
        ii. **From Header:** Mitel-vTrunk
        iii. **Request-URI:** Outbound
        iv. **Action:** Forward
        v. **Forward To:** ThinkTel

    b. Ensure the following is set for Line 2:
        i. **No:** 2
        ii. **From Header:** WAN
        iii. **Request-URI:** -
        iv. **Action:** Reject
        v. **Forward To:** -



Dial Plan (Help)

No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
					Forward	ENUM				
1	Mitel-vTru	Outbound	Forward	ThinkTel			-	-		□
2	WAN	-	Reject	-			-	-		□

***NOTE:** Your configuration might look different form the example in this document therefore if you require any further assistance please contact Ingate Support, +1 (866) 809-0002*
***Operational Hours:** Monday – Friday 9am – 6pm Eastern*

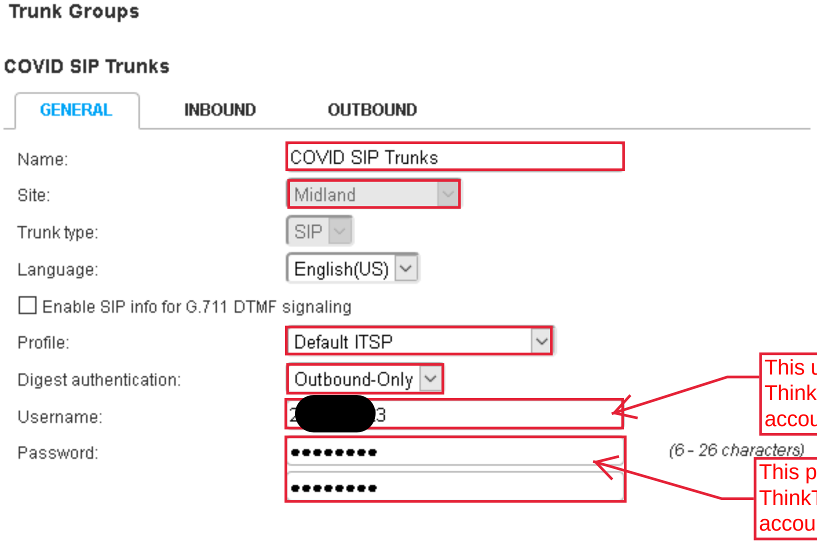
Mitel Installation

Trunk Configuration

When creating the SIP trunks within the Mitel Director please be aware of the following:

1. Under the *Trunk Groups menu,*
   a. Creating the new Trunk group the following info will be required in General tab:
      i. **Name:** COVID SIP Trunk
      ii. **Profile:** Default ITSP
      iii. **Digest authentication:** Outbound-Only
      iv. **Username:** 24xxxxxxx3
      v. **Password:** ********************

ThinkTel account username and password, refer to your ThinkTel account information



Trunk Groups

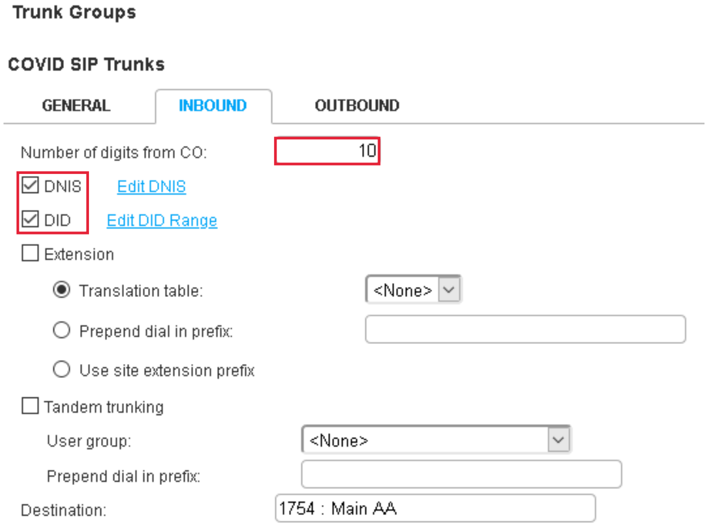
COVID SIP Trunks

Name: COVID SIP Trunks
Site: Midland
Trunk type: SIP
Language: English(US)
□ Enable SIP info for G.711 DTMF signaling
Profile: Default ITSP
Digest authentication: Outbound-Only
Username: [redacted]
Password: ••••••••
••••••••
(6 - 26 characters)

This username is provided by ThinkTel for the SIP trunk account.

This password is provided by ThinkTel for the SIP trunk account.

   b. Inbound Tab:
      i. **CO Digits:** 10
      ii. **DNIS:** checked
      iii. **DID:** checked
      iv. **Translation Table:** <none>
      v. **User group:** <none>
      vi. **Destibnation:** Default AA



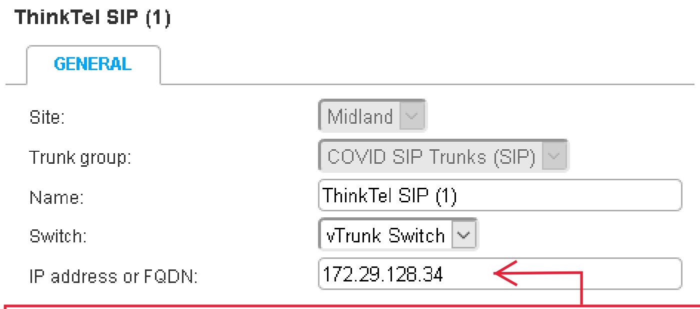
Trunk Groups

COVID SIP Trunks

Number of digits from CO: 10
☑ DNIS Edit DNIS
☑ DID Edit DID Range
□ Extension
● Translation table: <None>
○ Prepend dial in prefix:
○ Use site extension prefix
□ Tandem trunking
User group: <None>
Prepend dial in prefix:
Destination: 1754 : Main AA

2. Under the *Trunks menu,*
   c. Creating the new SIP Trunk Channels the following info will be required in General tab:

i.	**Site:**	Midland
ii.	**Trunk Group:**	COVID SIP Trunks (SIP)
iii.	**Name:**	ThinkTel SIP
iv.	**Switch:**	vTrunk Switch
v.	**IP address or FQDN:**	172.29.138.34 (*This is eth0 IP of the Ingate*)


ThinkTel SIP (1)

Site:	Midland
Trunk group:	COVID SIP Trunks (SIP)
Name:	ThinkTel SIP (1)
Switch:	vTrunk Switch
IP address or FQDN:	172.29.128.34

The Ingate eth0 interface IP address must be entered here to bind the Mitel SIP trunk channels to the Ingate SIParator in order to send and receive calls to and from ThinkTel through the Ingate SIParator.

Neglecting to enter the Ingate eth0 IP address here will result in a total failure of SIP traffic.

NOTE: *Your configuration might look different form the example in this document therefore if you require any further assistance please contact Ingate Support, +1 (866) 809-0002*
Operational Hours: *Monday – Friday 9am – 6pm Eastern*