1. Overview

1.1. Overview

This document explains what Exotel SIP Trunking is, how it works, and what problems it solves.

What is SIP Trunking?

SIP (Session Initiation Protocol) Trunking allows you to make and receive phone calls over the internet instead of traditional telephone lines (PRI / ISDN).

With Exotel SIP Trunking, your PBX, Contact Center, or SIP-enabled system connects directly to the telephone network (PSTN) using Exotel's cloud infrastructure.

This eliminates physical telephony hardware while enabling scalable, programmable voice connectivity.

What Exotel Provides

Exotel acts as the SIP gateway between your system and the telephone network.

- SIP signaling and media handling
- Routing to mobile, landline, and toll-free numbers
- High availability across multiple regions
- Optional routing to Voice AI using StreamKit

High-Level Architecture

Your system communicates with Exotel using SIP.
Exotel handles connectivity to the telephone network.

Call Directions

Exotel SIP Trunking supports the following call directions.

Outbound (SIP → PSTN)

Your system initiates a call to a phone number.

```
Your SIP System → Exotel → PSTN → Customer Phone
```

Typical use cases:

- Agent outbound calling
- Dialer campaigns
- Click-to-call from applications

Outbound calls require your server's public IP to be whitelisted.

Inbound (PSTN → SIP)

Your system receives calls from phone numbers.

```
Customer Phone → PSTN → Exotel → Your SIP System
```

Typical use cases:

- Customer support numbers
- IVR and call routing
- Contact center queues

Inbound calls are routed to an IP address or FQDN configured on the trunk.

StreamKit (Voice AI Routing)

In addition to PSTN routing, Exotel SIP Trunking can route calls to Voice AI bots using StreamKit.

```
Your SIP System → Exotel → Voice AI (WebSocket)
```

This is enabled using mode: flow when mapping a phone number to a trunk.

Typical use cases:

- AI-powered IVR
- Voice bots
- Speech analytics
- Agent assist

Supported Routing Modes

Mode	Description
pstn	Routes calls to the telephone network (default)
flow	Routes calls to Voice AI using StreamKit

The routing mode is configured per phone number.

What You Can Build with SIP Trunking

- Enterprise contact centers
- Outbound calling platforms
- Automated voice systems
- Voice AI integrations
- Hybrid human + bot call flows

What's Next

- To make your first call, go to **Quick Start**
- To understand routing behavior, see **Call Directions & Modes**

- To configure SIP Trunking, see **Setup**

1.2. Exotel SIP Trunking – Quick Start

This guide helps you make your **first outbound and inbound call** using Exotel SIP Trunking.

By the end of this guide, you will:

- Make outbound calls from your SIP system to PSTN
- Receive inbound calls from PSTN to your SIP system

Prerequisites

- Create or use Exotel account
  https://my.in.exotel.com/auth/register
- Completed KYC
  https://docs.exotel.com/business-phone-system/kyc-verification
- API credentials
  https://my.in.exotel.com/apisettings/site#api-credentials
- At least one Exophone (DID)
  https://my.in.exotel.com/numbers
- SIP system (PBX / SBC / Contact Center) with:
  - Public static IP
  - SIP over TLS or TCP enabled
  - refer **Network & Firewall Configuration**

You will need:

- API Key
- API Token
- Account SID

Step 1: Create SIP Trunk

Create a logical SIP trunk.

```
curl -s -X POST "https://<api_key>:<api_token>@<subdomain>/v2/accounts/<account_sid>/trun
  -H "Content-Type: application/json" \
  -d '{
    "trunk_name": "my_trunk",
    "nso_code": "ANY-ANY",
    "domain_name": "<account_sid>.pstn.exotel.com"
  }'
```

Save the trunk_sid.

Step 2: Map Phone Number to Trunk

Associate your Exophone (DID) with the trunk.

```
curl -s -X POST "https://<api_key>:<api_token>@<subdomain>/v2/accounts/<account_sid>/trun
  -H "Content-Type: application/json" \
  -d '{
    "phone_number": "+919876543210"
  }'
```

- Default mode is pstn
- Save the numeric id from the response

Step 3(a): Map ACL for Outbound SIP(Whitelist IPs)

This is required for **Outbound/Termination** SIP - allowing your system to send calls through the trunk.

Use **only** when your Voice AI provider gives a **single static egress IP** that you must allow. **Repeat the call for each distinct static IP** (no CIDR ranges on trunk, or you have a dedicated call server).

Required for:

- Outbound calls

- SIP authentication
- IP-based inbound destinations

```
curl -s -X POST "https://<api_key>:<api_token>@<subdomain>/v2/accounts/<account_sid>/trui
  -H "Content-Type: application/json" \
  -d '{
    "ip": "<your_public_ip>",
    "mask": 32
  }'
```

Step 3(b): Create SIP digest credentials (outbound auth)

POST /v2/accounts/{ACCOUNT_SID}/trunks/{TRUNK_SID}/credentials

Use the **same** `user_name` and `password` on the Voice AI platform (ElevenLabs SIP digest, LiveKit authUsername / authPassword, Retell termination, etc.).

```
curl -s -X POST \
  "https://${API_KEY}:${API_TOKEN}@${SUBDOMAIN}/v2/accounts/${ACCOUNT_SID}/trunks/${TRUNI
  -H "Content-Type: application/json" \
  -d '{
    "user_name": "SIP_USER",
    "password": "SIP_PASS",
    "friendly_name": "voice_ai_platform"
  }'
```

Step 4: Map Destination URI for Inbound SIP (Mandatory)

Configures where incoming calls should be routed. This is required for **Inbound/Origination** calls - routing calls from the telephone network to your system.

This defines the **network endpoint** of the trunk.

Using IP

(IP must be whitelisted in Step 3)

```
curl -s -X POST "https://<api_key>:<api_token>@<subdomain>/v2/accounts/<account_sid>/trun
-H "Content-Type: application/json" \
  -d '{
    "destinations": [
      {
        "destination": "<your_public_ip>:5061;transport=<tls/tcp>"
      }
    ]
  }'
```

Using FQDN

(No IP whitelist required)

```
curl -s -X POST "https://<api_key>:<api_token>@<subdomain>/v2/accounts/<account_sid>/trun
  -H "Content-Type: application/json" \
  -d '{
    "destinations": [
      {
        "destination": "sip.yourcompany.com:5061;transport=<tls/tcp>"
      }
    ]
  }'
```

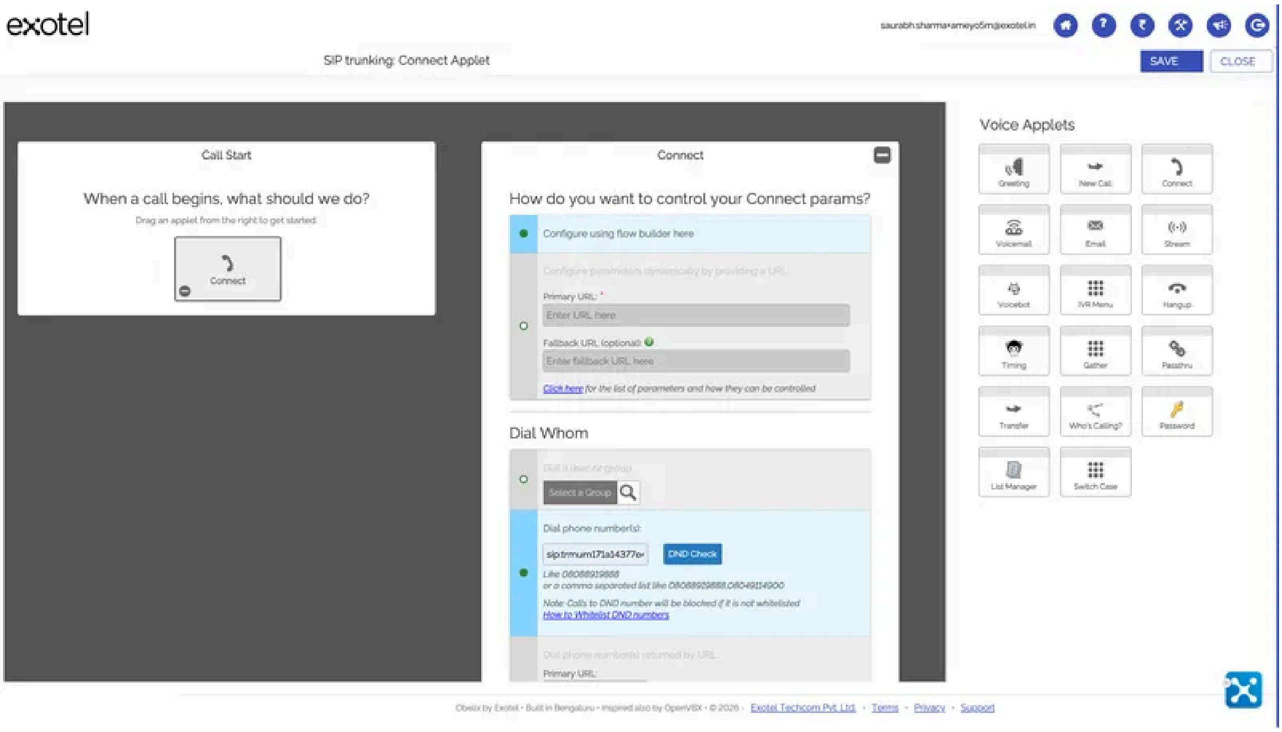
Step 5: Create Flow for Inbound Calls

Inbound calls are routed through **Exotel Flow**.

1. Go to App Bazaar
   https://my.in.exotel.com/apps
2. Create a new Flow
3. Add **Connect Applet**
4. In **Dial Whom**, enter:

```
sip:<trunk_sid>
```

6.



This connects the Flow to your SIP Trunk.

Step 6: Map DID to Flow

Bind the Exophone (DID) to the Flow.

1. Go to Exophone Manager
   https://my.in.exotel.com/numbers
2. Select your number or purchase
3. Set Exopone to the Flow created above

Inbound call path is now:

`PSTN → Exotel → DID→ Flow(Connect Applet)→ SIP Trunk → Destination URI → Your SIP system`

Step 7: Configure SIP System

Setting	Value
SIP Domain	<account_sid>.pstn.exotel.com
Port	443 (TLS) or 5070 (TCP)
Transport	TCP or TLS
Authentication	IP-based

Ensure RTP ports (UDP 10000–40000) are open.

Step 8: Test Calls

Outbound

- Dial any PSTN number from your SIP system

Inbound

- Call your Exophone from a mobile phone

If both succeed, setup is complete.

Flow Mode Clarification (Important)

Flow Type	Phone Number Mode
Connect Applet (sip:<trunk_sid>)	pstn
Voicebot / other App Bazaar applets	flow

Destination URI is required **in all cases**.

1.2.1. Manage Exotrunks

The **Exotrunk Management** section in your **Exotel Platform Dashboard** allows you to create, configure, and manage SIP trunks for your account. SIP trunks enable seamless connectivity between your Voicebot provider and Exotel's cloud communication platform.

To access Exotrunk Management, log in to your Exotel Dashboard based on your account cluster.

- **Mumbai cluster: platform.in.exotel.com**
- **Singapore cluster: Currently Unavailable**

Use your registered Exotel credentials to sign in.

> Exotrunk Managment is a limited access feature. If you are unable to see Exotrunk management feature on your Platform Dashboard please contact hello@exotel.com

Overview

The **Exotrunk Management** page lists all SIP trunks created within your account along with key details such as:

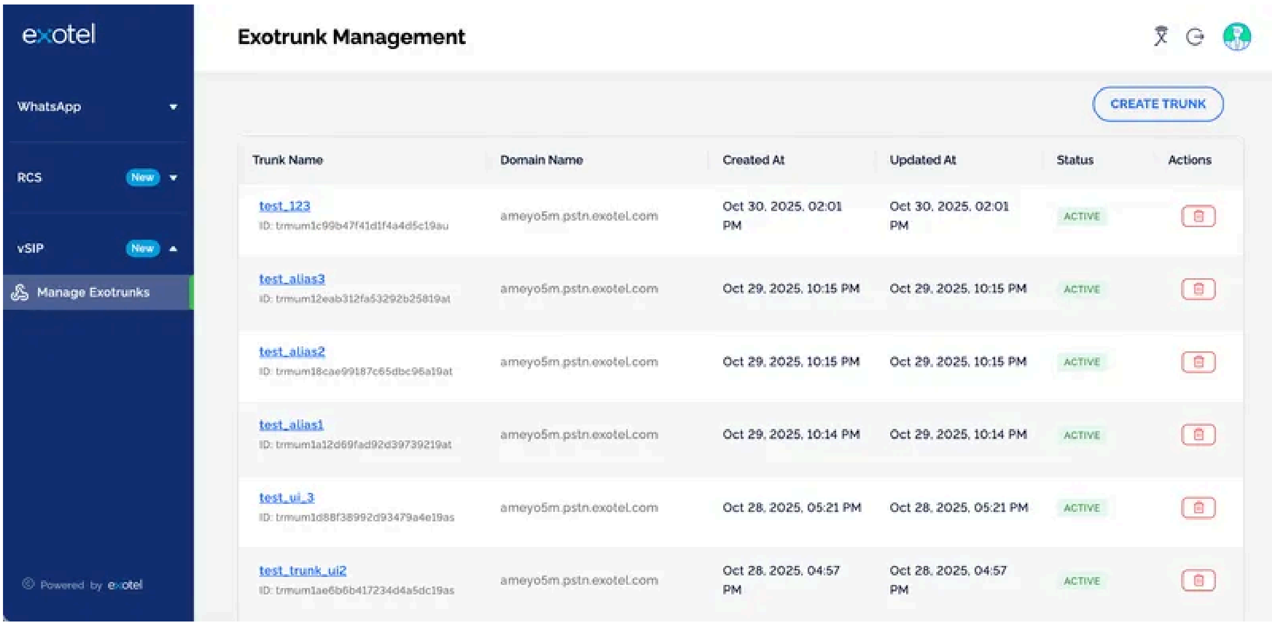
Field	Description
Trunk Name	The user-defined name of the SIP trunk.
Domain Name	The SIP domain through which Exotel routes your traffic.
Created At / Updated At	Timestamps showing when the trunk was created and last modified.
Status	The current operational state (e.g., *Active*).
Actions	Allows you to delete an existing trunk.

> Use the **Create Trunk** button on the top-right to add a new SIP trunk.

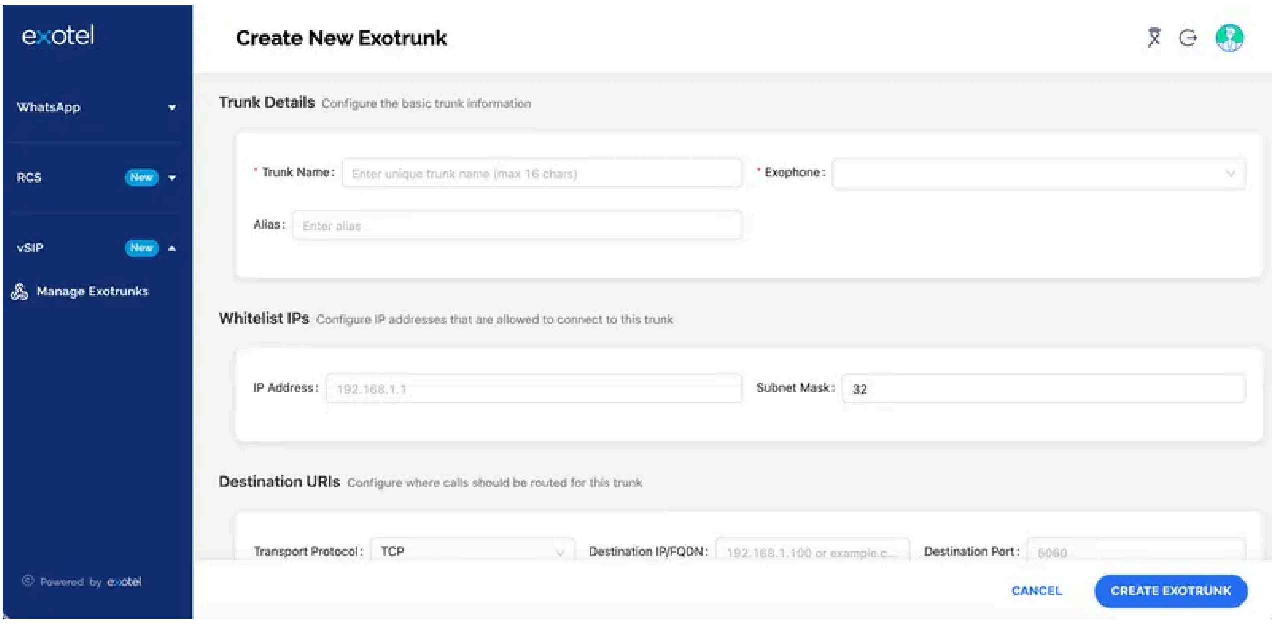
Creating a New Exotrunk

To create a new SIP trunk, follow these steps:

1. Click **Create Trunk** in the top-right corner of the Exotrunk Management page.



2. Fill in the required details in the **Create New Exotrunk** form.



Trunk Details

Field	Description	Required
Trunk Name	Enter a unique name (maximum 16 characters).	✅
Exophone	Select the Exophone to beassociated with this trunk.	✅
Alias	(Optional) Provide an alias name for reference	❌

Map ACL(Whitelist IPs)

Whitelist IPs ensure that only trusted systems can connect to your SIP trunk. IP Whiltisting is optional.

Field	Description
IP Address	Enter the IP address of your PBX or SIP endpoint.
Subnet Mask	Define the subnet range (default: 32).

> You can currently only whitelist 1 IP range from the Platform Dashboard. To whitelist additional IPs, contact hello@exotel.com

Destination URIs

Specify where calls should be routed for this trunk.

Field	Description
Transport Protocol	Choose between TCP or TLS.
Destination IP/FQDN	Enter the IP address or FQDN of your destination server.
Destination Port	Specify the SIP port

Click **Create Exotrunk** to save the configuration.

Viewing Trunk Details

Once created, each Exotrunk has a dedicated **Trunk Details** page that displays its configuration and status.

Basic Information

Field	Description
Trunk Name	The name assigned to the trunk.
Trunk ID	Unique system identifier for the trunk.
Alias	Alias name, if configured.
Domain Name	Exotel SIP domain assigned to the trunk.
Auth Type	The authentication mode used (*IP-Whitelist*).
Created / Last Updated	Timestamps of creation and last update.

Phone Numbers

Displays phone number assigned to the trunk for handling inbound calls.

If no numbers are assigned, this section will show:

```
No phone numbers assigned — Assign phone numbers to this trunk for incoming calls.
```

Destination URIs

Lists all configured SIP destination endpoint.

If none are configured, the message will show:

```
No destination URIs configured — Configure destination URIs to route calls from this trunk.
```

Whitelisted IPs

Shows all IP addresses authorized to connect to the trunk.

If none are added, you'll see:

```
No whitelisted IPs configured — Add IP addresses to restrict trunk access and enhance security.
```

Managing Existing Trunks

You can manage your trunks directly from the **Exotrunk Management** dashboard.

Action	Description
View Details	Click the trunk name to open the full configuration page.
Delete	Click the trash icon to remove a trunk permanently.

Next Steps

Once your SIP trunk is created and configured:

- **Setup up call flow** to define how inbound calls should be handled.

> If you encounter any issue with when managing exotrunks please reach out to Exotel Support with the Trunk ID and error logs for investigation.

1.2.2. Setup Call Flow with Exotrunk

You can set up and manage call flows in Exotel using the **App Bazaar**.
Call flows allow you to define how incoming or outgoing calls should be handled – for example, routing calls to agents, triggering voicebots, or forwarding to SIP endpoints.

Accessing App Bazaar

1. From the **Exotel Dashboard**, go to **Manage** → **App Bazaar**.
2. Under **Custom Apps**, you will see a list of existing call flows.

To create a new flow, click **CREATE**.

Creating a New Call Flow

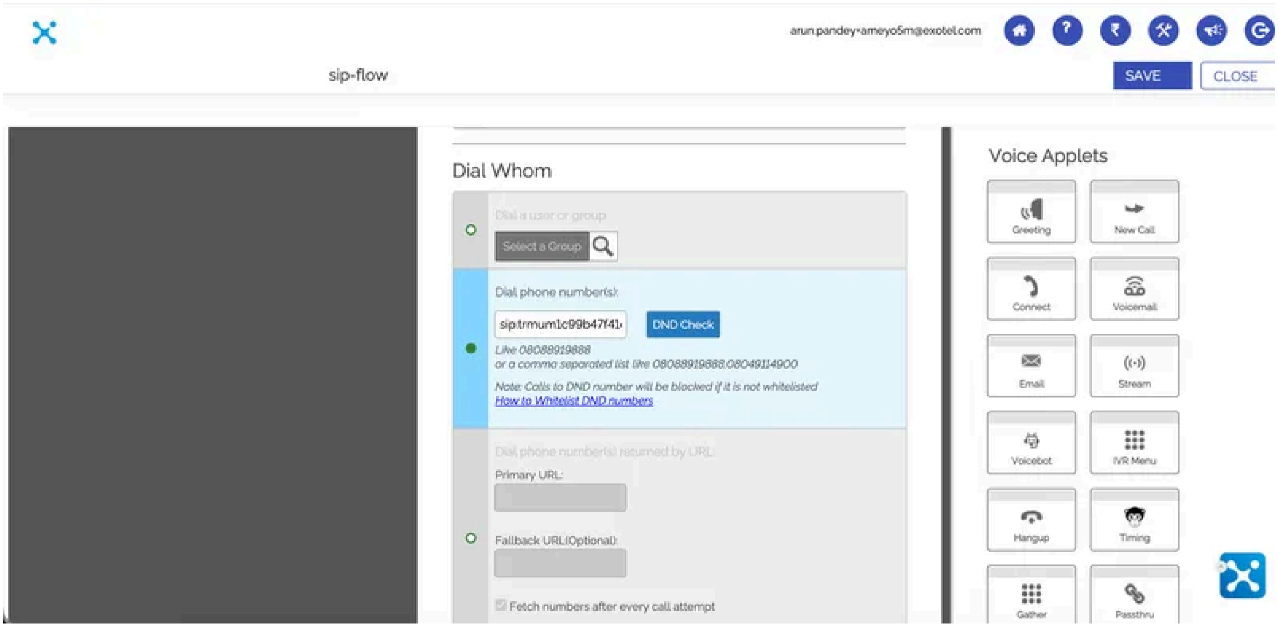
1. Click **CREATE** in the App Bazaar section.
   A pop-up will appear prompting you to **Add New Flow**.
2. Enter a name for your flow (e.g., `sip-flow`) and click **OK**.
3. You will be redirected to the visual **Flow Builder** interface.

Designing Your Flow

You can route calls to your SIP trunk created under **Exotrunk Management**.

1. Drag the **Connect** applet to the **Call Start** block.
2. Under **Connect**, choose:
   - **Configure using flow builder here** (default)
   - Skip dynamic URL configuration unless required.
3. In the **Dial Whom** section, specify the number or SIP endpoint to connect.

Field	Description
Dial phone number(s)	Enter SIP URI to connect the call. **Example** (`sip:trmun1c99b77f41d1f4a4d2c19au`)



When routing to a SIP trunk, use the Trunk ID from your Exotrunk details page in the format:

```
sip:<trunk-id>
```

4 You can optionally configure:

Setting	Description
Record this call?	Enable call recording for monitoring or compliance.

5 **Save Your Flow**

1. After configuring your applets, click **SAVE** on the top-right.
2. Your new flow will now appear under **Custom Apps** in the App Bazaar list.
3. The new flow is ready to be assigned to an **Exophone** or used in your API Integrations

> Deleting a flow will immediately stop all calls associated with it.
> Ensure that the flow is not mapped to active Exophones before deletion.

Setup up Inbound Calls

Once your call flow with exotrunk is created, you can assign it to an Exophone to handle incoming calls.

1. Go to **Manage** → **ExoPhones** in your Exotel Dashboard.
2. In the **Installed App** column, select the dropdown next to the Exophone you want to configure.
3. Choose your newly created flow from the list (for example, **sip-flow**).
4. The selected flow will now handle all calls made to that Exophone.

Setup up Outbound Calls

You can initiate outbound calls from Exotel using APIs.
Outbound calls can either connect directly to a SIP trunk or trigger a call flow that handles call routing, announcements, or logic.

There are two recommended methods:

Option 1: Using the Click-to-Call API

The **Click-to-Call API** lets you initiate a call between two endpoints – typically an agent and a customer. You can also use this API to initiate outbound calls through a SIP trunk.

Example usage:
Call the Click-to-Call API and specify:

- `From` as your customer number
- `To` as your SIP Trunk ID in the format **sip:<trunk_id>**
- `CallerId` as the Exophone configured in the Exotrunk

For complete details, see **Make a Call API**.

Option 2: Using Outbound Call to Call Flow API

The **Outbound Call to Call Flow API** allows you to trigger a pre-configured flow directly from your app or system. This is useful when you have additional logic defined in a call flow.

Example usage:

Call the Outbound Call API and provide:

- `From` as your agent or system number
- `To` as the customer's phone number or SIP endpoint
- `Url` pointing to your call flow app (using the **App ID** found in App Bazaar)

You can find the App ID in **App Bazaar → Custom Apps** under the *App ID* column.

1.3. Call Directions

Call Directions

Outbound (SIP → PSTN)

Calls initiated from your SIP system to external phone numbers.

Call path:

```
Your SIP System → Exotel SIP Trunk → PSTN
```

Used for:

- Agent outbound calling
- Dialers and campaigns
- Click-to-call from CRM
- Alerts and notifications

Key requirements:

- IP whitelisting (ACL) on the trunk
- Phone number mapped to trunk (Caller ID)

Inbound (PSTN → SIP)

Calls initiated from the telephone network to your SIP system.

Call path:

```
PSTN → Exotel → DID → Flow(Connect Applet) → SIP Trunk → Destination URI →
Your SIP System
```

Used for:

- Customer support lines
- Sales inbound numbers

- IVR and call routing to PBX

Key requirements:

- DID mapped to an Exotel Flow
- Flow uses **Connect Applet** with sip:<trunk_sid>
- Destination URI configured on the trunk (IP or FQDN)

Bidirectional (SIP ↔ PSTN)

The same SIP Trunk is used for **both outbound and inbound calls**.

Call paths:

```
Outbound:  Your SIP System → Exotel → PSTN
```

```
Inbound:   PSTN → Exotel → Flow(Connect Applet) → SIP Trunk → Destination URI → Your SIP System
```

Used for:

- Contact centers
- PBX integrations
- Unified inbound + outbound calling
- Agent calling with inbound callbacks

Key requirements:

- Phone number mapped to trunk
- IP whitelisting enabled (for outbound)
- Destination URI configured (for inbound)
- Exotel Flow with Connect Applet (sip:<trunk_sid>)

This is the **most common SIP Trunking setup**.

Routing Modes

Routing mode defines **how Exotel handles calls** once they reach the DID/Exophone/Virtual Number.

The mode is set while mapping a phone number to a trunk.

mode: pstn (Default)

Standard telephony routing.

Used for:

- Outbound calls to PSTN
- Inbound calls routed to SIP systems
- Bidirectional SIP Trunking
- Flows using **Connect Applet** (sip:<trunk_sid>)

Behavior:

- Calls behave like standard SIP/PSTN calls
- Media flows directly between Exotel and your SIP system
- No Voice AI or Flow applet execution

mode: flow

Flow-controlled routing.

Used for:

- Voicebot / AI integrations
- App Bazaar applets
- StreamKit use cases

Behavior:

- Calls are routed into Flow execution
- Audio may be streamed to Voice AI platforms
- Required for Voicebot and other non-Connect applets

Mode Selection Summary

Use Case	Flow Applet Used	Mode
Outbound only	None	pstn
Inbound only	Connect (sip:<trunk_sid>)	pstn
Bidirectional SIP Trunk	Connect (sip:<trunk_sid>)	pstn
Voicebot / AI	Voicebot / Applets	flow

Important Notes

- **Destination URI is mandatory** for all SIP Trunking setups
- **Flow is mandatory** for inbound calls
- mode controls call handling, not trunk termination

Bidirectional uses the **same trunk** for inbound and outbound

1.4. Detailed SIP Trunking API Reference

This section documents the APIs required to configure and manage **SIP Trunking** with Exotel.

Use these APIs to:

- Make outbound calls to the PSTN
- Receive inbound calls on your SIP system
- Integrate SIP with Exotel Flows and Voice AI (StreamKit)

Base URL & Authentication

All APIs use **HTTP Basic Authentication**.

Base URLs

Region	Base URL
India (Mumbai)	https://api.in.exotel.com
Singapore	https://api.exotel.com

All endpoints are prefixed with:

/v2/accounts/{account_sid}

Required Headers

Authorization: Basic <api_key:api_token>

Content-Type: application/json

Rate Limits

Limit Type	Value
Requests per minute	200

API Workflow Overview

Typical PSTN setup follows this order:

→ Create Trunk

→ Map Phone Number

→ Map ACL (Outbound)

→ Map Destination URI (Inbound)

GETTING STARTED (PSTN Setup)

This section covers the APIs required to set up SIP Trunking for standard PSTN (telephone network) connectivity.

Postman Collection

Github Repo

Setup Flow:

```
Create Trunk → 2. Map Phone Number → 3. Map ACL (for Outbound) → 4. Map
Destination URI (for Inbound)
```

1. Create Trunk

Creates a new SIP trunk. This is the first step for all SIP Trunking use cases.

A SIP Trunk acts as a virtual connection between your communication system (PBX/Contact Center) and Exotel's telephony network.

HTTP Request

```
POST https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks
```

Request Headers

Header	Value
Content-Type	application/json

Request Parameters

The following parameters are sent as JSON in the body of the request:

Parameter Name	Mandatory/Optional	Value
trunk_name	Mandatory	String; Unique identifier for the trunk. Must be alphanumeric with underscores only, maximum 16 characters. Example: outbound_trunk, my_pbx_trunk
nso_code	Mandatory	String; Network Service Operator code. Use ANY-ANYfor standard configuration.
domain_name	Mandatory	String; SIP domain for the trunk. Format: <your_sid>.pstn.exotel.com. Example: ameyo5m.pstn.exotel.com

Example Request

```
curl -s -X POST "https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks" \
  -H "Content-Type: application/json" \
  -d '{
    "trunk_name": "outbound_trunk",
    "nso_code": "ANY-ANY",
    "domain_name": "<your_sid>.pstn.exotel.com"
  }'
```

HTTP Response

On success, the HTTP response status code will be 200 OK.

The trunk_sidis the unique identifier of the trunk - **save this value** as it will be required for all subsequent API calls.

Example Response

```
{
  "request_id": "10a67da360d446378d5c2b66407b7f18",
  "method": "POST",
  "http_code": 200,
  "response": {
    "code": 200,
    "error_data": null,
    "status": "success",
    "data": {
      "trunk_name": "outbound_trunk",
      "date_created": "2026-01-23T09:24:59Z",
      "date_updated": "2026-01-23T09:24:59Z",
      "trunk_sid": "trmum1f708622631150902801a1n",
      "status": "active",
      "domain_name": "ameyo5m.pstn.exotel.com",
      "auth_type": "IP-WHITELIST",
      "registration_enabled": "disabled",
      "edge_preference": "auto",
      "nso_code": "ANY-ANY",
      "secure_trunking": "disabled",
      "destination_uris":
"/v2/accounts/ameyo5m/trunks/trmum1f708622631150902801a1n/destination-uris",
      "whitelisted_ips":
"/v2/accounts/ameyo5m/trunks/trmum1f708622631150902801a1n/whitelisted-ips",
      "credentials":
"/v2/accounts/ameyo5m/trunks/trmum1f708622631150902801a1n/credentials",
      "phone_numbers":
"/v2/accounts/ameyo5m/trunks/trmum1f708622631150902801a1n/phone-numbers"
    }
  }
}
```


Response Parameters

Parameter Name	Type & Value
request_id	String; Unique identifier for this API request
method	String; HTTP method used (POST)
http_code	Integer; HTTP status code (200 for success)
trunk_sid	String; **Important** - Unique identifier for the trunk. Save this for subsequent API calls. Example: trmum1f708622631150902801a1n
trunk_name	String; Name of the trunk as provided in request
domain_name	String; SIP domain for the trunk
status	String; Current trunk status: active- Trunk is ready for use, inactive- Trunk is disabled
auth_type	String; Authentication type. Currently only IP-WHITELISTis supported
registration_enabled	String; SIP registration status: enabledor disabled
edge_preference	String; Edge server preference. Default: auto
nso_code	String; Network Service Operator code
secure_trunking	String; TLS status: enabledor disabled
destination_uris	String; API path to manage destination URIs for this trunk
whitelisted_ips	String; API path to manage ACLs (whitelisted IPs) for this trunk
credentials	String; API path to credentials for this trunk
phone_numbers	String; API path to manage phone numbers for this trunk
date_created	String; ISO 8601 timestamp when trunk was created

Parameter Name	Type & Value
date_updated	String; ISO 8601 timestamp when trunk was last updated

2. Map Phone Number to Trunk

Associates a phone number (DID/ExoPhone) with the trunk. This phone number will be used for making and receiving calls through the trunk.

HTTP Request

```
POST https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/phone-
numbers
```

Request Headers

Header	Value
Content-Type	application/json

Request Parameters

Parameter Name	Mandatory/Optional	Value
phone_number	Mandatory	String; The phone number to map to the trunk. Must be in E.164 format (with country code). Example: +919876543210, +912247790597
mode	Optional	String; Routing mode for the phone number. Can be: pstn(default) - Routes calls to telephone network, flow- Routes calls to Voice AI bot (StreamKit). If not specified, defaults to nulland behaves as pstn.

Example Request

```
curl -s -X POST "https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/phone-
numbers" \
  -H "Content-Type: application/json" \
  -d '{
    "phone_number": "+919876543210"
  }'
```

For StreamKit (Voice AI) mode:

```
curl -s -X POST "https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/phone-
numbers" \
  -H "Content-Type: application/json" \
  -d '{
    "phone_number": "+919876543210",
    "mode": "flow"
  }'
```

HTTP Response

On success, the HTTP response status code will be 200 OK.

Important: Save the idfrom the response - this numeric ID is required for the Update Phone Number Mode API.

Example Response

```
{
  "request_id": "13ab9319cf574486ba299c364f82cade",
  "method": "POST",
  "http_code": 200,
  "response": {
    "code": 200,
    "error_data": null,
    "status": "success",
    "data": {
      "id": "41512",
      "phone_number": "+919876543210",
      "trunk_sid": "trmum1f708622631150902801a1n",
      "date_created": "2026-01-23T10:26:54Z",
      "date_updated": "2026-01-23T10:26:54Z",
      "mode": null
    }
```

```
  }
}
```

Response Parameters

Parameter Name	Type & Value
id	String; **Important** - Numeric identifier for this phone number mapping. Save this value - required for Update Phone Number Mode API. Example: 41512
phone_number	String; The mapped phone number in E.164 format
trunk_sid	String; The trunk this phone number is associated with
mode	String or null; Routing mode: pstn- PSTN routing, flow- StreamKit/Voice AI routing, null- Default (same as pstn)
date_created	String; ISO 8601 timestamp when mapping was created
date_updated	String; ISO 8601 timestamp when mapping was last updated

3(a). Map ACL to Trunk (Whitelist IP)

Registers your server's public IP address for authentication. This is required for **Outbound/Termination** calls - allowing your system to send calls through the trunk.

ACL (Access Control List) ensures only authorized IP addresses can use your trunk for outbound calling.

HTTP Request

```
POST https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/whitel
isted-ips
```

Request Headers

Header	Value
Content-Type	application/json

Request Parameters

Parameter Name	Mandatory/ Optional	Value
ip	Mandatory	String; Your server's public IP address. Must be a valid IPv4 address. Example: 44.248.146.11, 203.0.113.50
mask	Optional	Integer; Subnet mask in CIDR notation. Default: 32(single IP). Use 24for /24 subnet, 16for /16 subnet. Example: 32, 24

Example Request

```
curl -s -X POST "https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/whitel
isted-ips" \
  -H "Content-Type: application/json" \
  -d '{
    "ip": "44.248.146.11",
    "mask": 32
  }'
```

HTTP Response

On success, the HTTP response status code will be 200 OK.

Example Response

```
{
  "request_id": "3daaed4cd05d443f854e07e60dd4c008",
  "method": "POST",
  "http_code": 200,
  "response": {
    "code": 200,
    "error_data": null,
    "status": "success",
    "data": {
      "id": "1153",
      "mask": 32,
```

```
      "trunk_sid": "trmum1f70862263115090280la1n",
      "ip": "44.248.146.11",
      "friendly_name": null,
      "date_created": "2026-01-23T11:37:36Z",
      "date_updated": "2026-01-23T11:37:36Z"
    }
  }
}
```

Response Parameters

Parameter Name	Type & Value
id	String; Unique identifier for this ACL entry. Example: 1153
ip	String; The whitelisted IP address
mask	Integer; Subnet mask in CIDR notation
trunk_sid	String; The trunk this ACL is associated with
friendly_name	String or null; Optional friendly name for the IP
date_created	String; ISO 8601 timestamp when ACL was created
date_updated	String; ISO 8601 timestamp when ACL was last updated

3(b). Create credentials (digest auth) API for a Trunk

1. Create credentials (SIP digest)

Creates a **username/password** pair for **SIP Digest authentication** on the trunk. Configure the same values on your Voice AI platform's SIP trunk settings.

HTTP Request

```
POST https://<API_KEY>:<API_TOKEN>@<SUBDOMAIN>/v2/accounts/<ACCOUNT_SID>/trunks/<TRUNK_SID>/credentials
```

Request Headers

Header	Value
Content-Type	application/json

Request Parameters

The following parameters are sent as JSON in the body of the request:

Parameter Name	Mandatory/ Optional	Value
user_name	Mandatory	String; SIP digest username. Example: voice_ai_user
password	Mandatory	String; SIP digest password. Use a strong secret.
friendly_name	Optional	String; Label to identify where the creds are used (max 32 chars). Example: elevenlabs-prod, livekit-staging

Example Request

```
curl -s -X POST "https://<API_KEY>:
<API_TOKEN>@<SUBDOMAIN>/v2/accounts/<ACCOUNT_SID>/trunks/<TRUNK_SID>/credenti
als" \
  -H "Content-Type: application/json" \
  -d '{
    "user_name": "voice_ai_user",
    "password": "REPLACE_WITH_STRONG_PASSWORD",
    "friendly_name": "voice_ai_platform"
  }'
```

HTTP Response

On success, the HTTP response status code will be **200 OK**.

Example Response

```
{
  "request_id": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
  "method": "POST",
  "http_code": 200,
  "response": {
    "code": 200,
    "error_data": null,
    "status": "success",
```

```
    "data": {
      "id": "1234",
      "trunk_sid": "trmum17d8e9a37a3732ecbf91a3u",
      "user_name": "voice_ai_user",
      "friendly_name": "voice_ai_platform",
      "date_created": "2026-01-23T11:37:36Z",
      "date_updated": "2026-01-23T11:37:36Z"
    }
  }
}
```

Response Parameters

Parameter Name	Type & Value
request_id	String; Unique identifier for this API request
method	String; HTTP method used (POST)
http_code	Integer; HTTP status code (200 for success)
id	String; Unique identifier for this credential entry. Example: 1234
trunk_sid	String; The trunk these credentials are associated with
user_name	String; The SIP digest username you set
friendly_name	String or null; Optional label
date_created	String; ISO 8601 timestamp when credentials were created
date_updated	String; ISO 8601 timestamp when credentials were last updated

2. List credentials (verify)

Lists credentials configured for the trunk.

HTTP Request

```
GET https://<API_KEY>:<API_TOKEN>@<SUBDOMAIN>/v2/accounts/<ACCOUNT_SID>/trunks/<TRUNK_SID>/credentials
```

Example Request

```
curl -s "https://<API_KEY>:<API_TOKEN>@<SUBDOMAIN>/v2/accounts/<ACCOUNT_SID>/trunks/<TRUNK_SID>/credenti
```

```
als"
```

HTTP Response

On success, the HTTP response status code will be **200 OK**.

Example Response


```
{
  "request_id": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
  "method": "GET",
  "http_code": 200,
  "metadata": {
    "total": 1,
    "page_size": 50,
    "page": 1,
    "first_page_uri":
"/v2/accounts/exotelveenotesting1m/trunks/trmum17d8e9a37a3732ecbf91a3u/creden
tials?page_size=50&offset=0",
    "prev_page_uri": null,
    "next_page_uri": null
  },
  "response": [
    {
      "code": 200,
      "error_data": null,
      "status": "success",
      "data": {
        "id": "1234",
        "trunk_sid": "trmum17d8e9a37a3732ecbf91a3u",
        "user_name": "voice_ai_user",
        "friendly_name": "voice_ai_platform",
        "date_created": "2026-01-23T11:37:36Z",
        "date_updated": "2026-01-23T11:37:36Z"
      }
    }
  ]
}
```


Response Parameters

Parameter Name	Type & Value
request_id	String; Unique identifier for this API request
method	String; HTTP method used (GET)
http_code	Integer; HTTP status code (200 for success)
metadata.total	Integer; Total credential records available
metadata.page_size	Integer; Page size applied
metadata.page	Integer; Page number (if present)
metadata.first_page_uri	String; URI for first page
metadata.prev_page_uri	String or null; URI for previous page
metadata.next_page_uri	String or null; URI for next page
response	Array; List of credential objects
response[].data.id	String; Unique identifier for the credential entry
response[].data.trunk_sid	String; The trunk these credentials are associated with
response[].data.user_name	String; SIP digest username
response[].data.friendly_name	String or null; Optional label
response[].data.date_created	String; ISO 8601 timestamp when created
response[].data.date_updated	String; ISO 8601 timestamp when updated

3. Delete credentials (rotate / revoke)

Deletes a credential entry when rotating credentials or removing access for a provider environment.

HTTP Request

```
DELETE https://<API_KEY>:<API_TOKEN>@<SUBDOMAIN>/v2/accounts/<ACCOUNT_SID>/trunks/<TRUNK_SID>/credentials?id=<CREDENTIAL_ID>
```

Important: credential id is passed as **query param** id (not /credentials/<CREDENTIAL_ID>).

Example Request

```
curl -s -X DELETE "https://<API_KEY>:
<API_TOKEN>@<SUBDOMAIN>/v2/accounts/<ACCOUNT_SID>/trunks/<TRUNK_SID>/credenti
als?id=<CREDENTIAL_ID>"
```

HTTP Response

On success, the HTTP response status code will be **200 OK**.

Example Response

```
{
  "request_id": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
  "method": "DELETE",
  "http_code": 200,
  "response": {
    "code": 200,
    "error_data": null,
    "status": "success",
    "data": {
      "id": "1234",
      "trunk_sid": "trmum17d8e9a37a3732ecbf91a3u",
      "user_name": "voice_ai_user",
      "friendly_name": "voice_ai_platform",
      "date_created": "2026-01-23T11:37:36Z",
      "date_updated": "2026-01-23T11:37:36Z"
    }
  }
}
```

Response Parameters

Parameter Name	Type & Value
request_id	String; Unique identifier for this API request
method	String; HTTP method used (DELETE)
http_code	Integer; HTTP status code (200 for success)
id	String; Deleted credential identifier
trunk_sid	String; Trunk SID this credential belonged to
user_name	String; SIP digest username that was deleted
friendly_name	String or null; Optional label
date_created	String; ISO 8601 timestamp when credential was originally created
date_updated	String; ISO 8601 timestamp when credential was last updated

4.When to use Credentials vs ACL (Whitelisted IPs)

Use these guidelines to decide whether you should configure **credentials**, **ACL (whitelisted IPs)**, or **both** on a trunk.

Credentials (SIP Digest) – recommended for Voice AI direct trunking

Use **credentials** when your SIP endpoint is a **cloud Voice AI platform** (or any environment where source IPs are dynamic/unknown), and you want to **avoid managing IP allowlists**.

- **Best for**: Voice AI direct trunking, dynamic SBCs, multi-tenant provider networks.
- **Typical choice**: **Credentials-only** (skip ACL whitelisting) when IPs are not stable.

ACL (Whitelisted IPs) – recommended for static enterprise PBX/SBC

Use **ACL-only** when your trunk connects to a customer-controlled PBX/SBC with **stable, known egress IPs**.

- **Best for**: On-prem SBCs, fixed datacenter IPs, tightly controlled networks.
- **Typical choice**: **ACL-only** if credentials are not required and IPs are stable.

Combination (ACL + Credentials) – highest security when IPs are stable

Use **both** when you have credentials *and* stable IPs and want a stricter security posture.

- **Best for**: Production trunks with fixed IP ranges and stricter access controls.

- **Why**: Reduces blast radius—credentials alone aren't sufficient without also matching the allowlist (and vice-versa).

4. Map Destination URI to Trunk

Configures where incoming calls should be routed. This is required for **Inbound/Origination** calls - routing calls from the telephone network to your system.

The destination can be an IP address or FQDN (Fully Qualified Domain Name) of your PBX/SBC.

Important Notes

- **For IP-based destinations:** You MUST whitelist the IP using the "Map ACL to Trunk" API first
- **For FQDN-based destinations:** No whitelisting required (e.g., sip.yourcompany.com)
- The destination format is: <ip_or_fqdn>:<port>;transport=<protocol>
- You need to set

HTTP Request

```
POST https://<your_api_key>:<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/destination-uris
```

Request Headers

Header	Value
Content-Type	application/json

Request Parameters

Parameter Name	Mandatory/Optional	Value
destinations	Mandatory	Array; List of destination objects. Each object contains a destinationfield.
destinations[].destination	Mandatory	String; SIP URI in format <ip_or_fqdn>:<port>;transport=<protocol>. Port is typically 5061for TLS or 5060for TCP. Transport can be tls(recommended) or tcp. Example: 44.248.146.11:5061;transport=tls, sip.company.com:5061;transport=tls

Example Request (IP-based destination)

Note: Ensure the IP 44.248.146.11is whitelisted first using Map ACL API.

```
curl -s -X POST "https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/destin
ation-uris" \
  -H "Content-Type: application/json" \
  -d '{
    "destinations": [
      {
        "destination": "44.248.146.11:5061;transport=tls"
      }
    ]
  }'
```

Example Request (FQDN-based destination)

```
curl -s -X POST "https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/destin
ation-uris" \
  -H "Content-Type: application/json" \
  -d '{
    "destinations": [
      {
        "destination": "sip.yourcompany.com:5061;transport=tls"
      }
    ]
  }'
```

HTTP Response

On success, the HTTP response status code will be 200 OKor 207 Multi-Status(for partial success/failure).

The response includes metadatawith counts of successful and failed destinations.

Example Response (Success)

```
{
  "request_id": "63999f0a98a24a0aa58ab5b74aec9f0a",
  "method": "POST",
  "http_code": 200,
  "metadata": {
    "total": 1,
    "success": 1,
    "failed": 0
  },
  "response": [
    {
      "code": 200,
      "error_data": null,
      "status": "success",
      "data": {
        "id": "2543",
        "destination": "sip:44.248.146.11:5061;transport=tls",
        "date_created": "2026-01-23T13:38:32Z",
        "date_updated": "2026-01-23T13:38:32Z",
        "type": "public",
        "priority": 0,
        "weight": 1,
        "trunk_sid": "trmum1f708622631150902801a1n"
      }
    }
  ]
}
```

Response Parameters

Parameter Name	Type & Value
metadata.total	Integer; Total number of destinations in request
metadata.success	Integer; Number of successfully added destinations
metadata.failed	Integer; Number of failed destinations
id	String; Unique identifier for this destination URI. Example: 2543
destination	String; The SIP URI (prefixed with sip:)
type	String; Destination type: public
priority	Integer; Priority for load balancing. Lower values = higher priority. Default: 0
weight	Integer; Weight for load balancing. Higher values = more traffic. Default: 1
trunk_sid	String; The trunk this destination is associated with
date_created	String; ISO 8601 timestamp when destination was created
date_updated	String; ISO 8601 timestamp when destination was last updated

for Inbound SIP

a. Create a Flow using Connect Applet in App Bazaar: https://my.in.exotel.com/apps

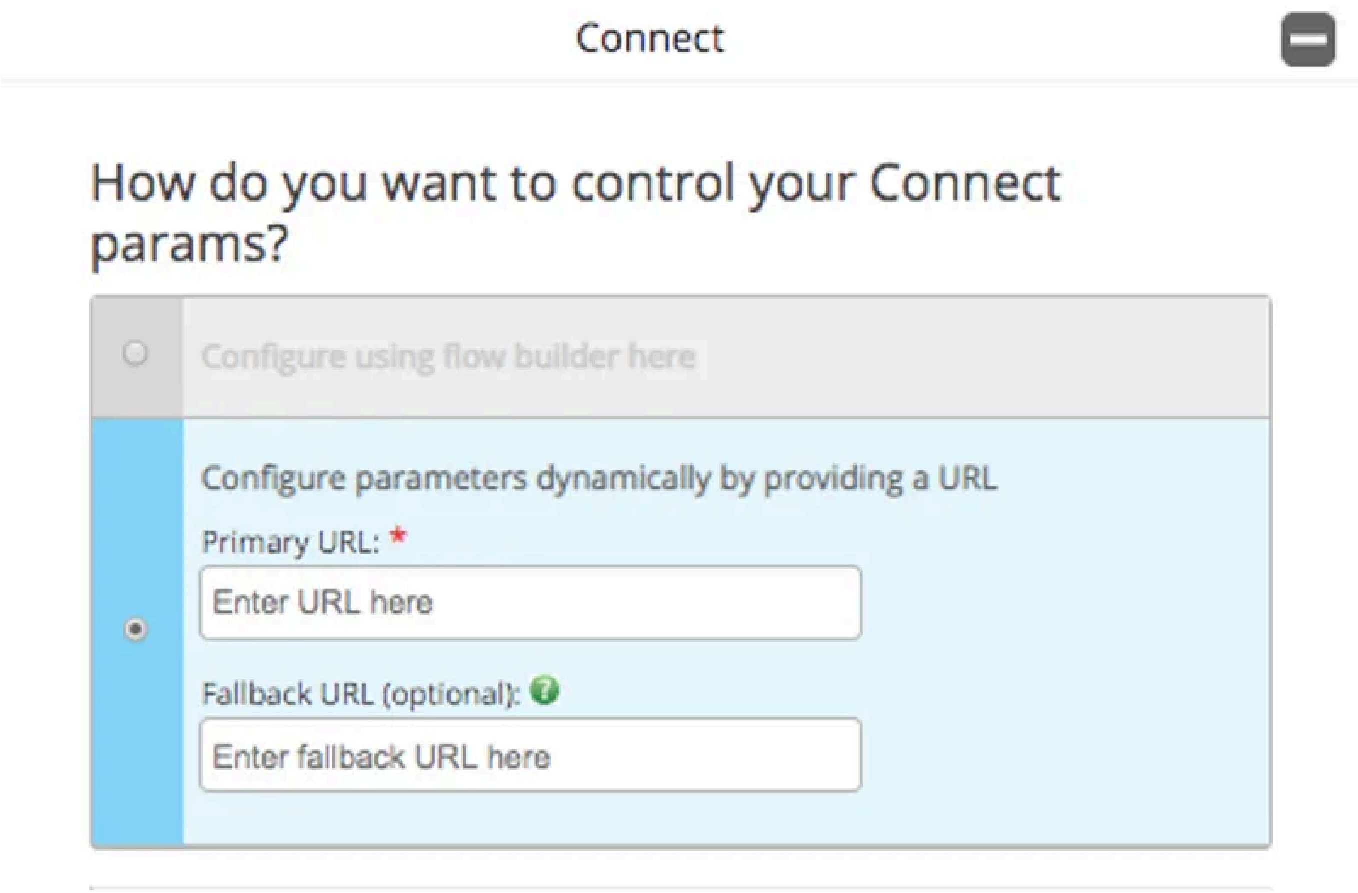
b. Use sip:<trunk_sid> in the Dial Whom field

c. Map DID to flow through Exophone: https://my.in.exotel.com/numbers

d. Check inbound call flow by dialling Exophone/phonenumber to your system via Exotel SIP trunking

e. Follow detailed steps here :**Setup Call Flow with Exotrunk**

f. Advance Routing: For custom routing, use a Dynamic URL to fetch the destination URI and pass headers or define failover use programmable connect



- Supports **up to 3 custom SIP headers**, e.g., X-param1=value1 (max 200 bytes total)
- Headers prefixed with Exotel- or Veeno- are platform-reserved

Connect Applet – Dynamic URL Response Example:

```
{
"fetch_after_attempt": false,
"destination": { "trunk": "trunk-2134" },
"custom_params": "param1=value1&param2=value2",
"record": true,
"recording_channels": "dual"
}
```

MANAGE & VIEW

APIs for viewing configurations, updating settings, and managing your trunk.

5. Get Phone Numbers

Retrieves all phone numbers mapped to a trunk.

HTTP Request

```
GET https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/phone-
numbers
```

Example Request

```
curl -s -X GET "https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/phone-
numbers"
```

Example Response


```
{
  "request_id": "785471d288054cbf8c677b75e0b5f2f8",
  "method": "GET",
  "http_code": 200,
  "metadata": {
    "page_size": 50,
    "first_page_uri":
"/v2/accounts/ameyo5m/trunks/trmum1f708622631150902801a1n/phone-numbers?
offset=0&page_size=50",
    "prev_page_uri": null,
    "next_page_uri": null
  },
  "response": [
    {
      "code": 200,
      "error_data": null,
      "status": "success",
      "data": {
        "id": "41523",
        "phone_number": "+918040264208",
        "trunk_sid": "trmum1f708622631150902801a1n",
        "date_created": "2026-01-23T13:28:11Z",
        "date_updated": "2026-01-23T13:41:59Z",
        "mode": "flow"
      }
    }
  ]
}
```

Response Parameters

Parameter Name	Type & Value
metadata.page_size	Integer; Number of results per page
metadata.first_page_uri	String; URI for the first page
metadata.prev_page_uri	String or null; URI for previous page (null if on first page)
metadata.next_page_uri	String or null; URI for next page (null if on last page)
response[]	Array; List of phone number objects

6. Get ACLs (Whitelisted IPs)

Retrieves all whitelisted IP addresses for a trunk.

HTTP Request

```
GET https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/whitel
isted-ips
```

Example Request

```
curl -s -X GET "https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/whitel
isted-ips"
```

Example Response


```
{
  "request_id": "91dc982ca79846479c6f9678c788cfc1",
  "method": "GET",
  "http_code": 200,
  "metadata": {
    "page_size": 50,
    "first_page_uri":
"/v2/accounts/ameyo5m/trunks/trmum1f708622631150902801a1n/whitelisted-ips?
offset=0&page_size=50",
    "prev_page_uri": null,
    "next_page_uri": null
  },
```

```
  "response": [
    {
      "code": 200,
      "error_data": null,
      "status": "success",
      "data": {
        "id": "1154",
        "mask": 32,
        "trunk_sid": "trmum1f708622631150902801a1n",
        "ip": "44.248.146.11",
        "friendly_name": null,
        "date_created": "2026-01-23T13:30:04Z",
        "date_updated": "2026-01-23T13:30:04Z"
      }
    }
  ]
}
```


7. Get Destination URIs

Retrieves all destination URIs configured for a trunk.

HTTP Request

```
GET https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/destin
ation-uris
```

Example Request

```
curl -s -X GET "https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/destin
ation-uris"
```

Example Response


```
{
  "request_id": "bfc1544ab0ab4df3ae49173ccc744331",
  "method": "GET",
  "http_code": 200,
  "metadata": {
    "page_size": 50,
    "first_page_uri":
```

```
"/v2/accounts/ameyo5m/trunks/trmum1f708622631150902801a1n/destination-uris?
offset=0&page_size=50",
    "prev_page_uri": null,
    "next_page_uri": null
  },
  "response": [
    {
      "code": 200,
      "error_data": null,
      "status": "success",
      "data": {
        "id": "2544",
        "destination": "sip:sip.company.com:5061;transport=tls",
        "date_created": "2026-01-23T13:39:06Z",
        "date_updated": "2026-01-23T13:39:06Z",
        "type": "public",
        "priority": 0,
        "weight": 1,
        "trunk_sid": "trmum1f708622631150902801a1n"
      }
    },
    {
      "code": 200,
      "error_data": null,
      "status": "success",
      "data": {
        "id": "2543",
        "destination": "sip:44.248.146.11:5061;transport=tls",
        "date_created": "2026-01-23T13:38:32Z",
        "date_updated": "2026-01-23T13:38:32Z",
        "type": "public",
        "priority": 0,
        "weight": 1,
        "trunk_sid": "trmum1f708622631150902801a1n"
      }
    }
  ]
}
```

8. Update Phone Number Mode

Updates the routing mode for a mapped phone number. Use this to switch between PSTN and StreamKit (Voice AI) modes.

HTTP Request

```
PUT https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/phone-
numbers/<phone_number_id>
```

Important: The <phone_number_id>is the **numeric ID** returned when you mapped the phone number (e.g., 41523), NOT the phone number itself.

Request Headers

Header	Value
Content-Type	application/json

Request Parameters

Parameter Name	Mandatory /Optional	Value
phone_number	Mandatory	String; The phone number in E.164 format. Must match the phone number associated with the ID. Example: +919876543210
mode	Mandatory	String; The new routing mode. Can be: pstn- Route calls to telephone network, flow- Route calls to Voice AI bot (StreamKit)

Example Request (Switch to Flow mode)

```
curl -s -X PUT "https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/phone-
numbers/41523" \
  -H "Content-Type: application/json" \
  -d '{
    "phone_number": "+918040264208",
    "mode": "flow"
  }'
```

Example Request (Switch to PSTN mode)

```
curl -s -X PUT "https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/phone-
numbers/41523" \
  -H "Content-Type: application/json" \
  -d '{
```

```
    "phone_number": "+918040264208",
    "mode": "pstn"
  }'
```

Example Response


```
{
  "request_id": "c719cd56eb5943e789e1bdbd4ce1515a",
  "method": "PUT",
  "http_code": 200,
  "response": {
    "code": 200,
    "error_data": null,
    "status": "success",
    "data": {
      "id": "41523",
      "phone_number": "+918040264208",
      "trunk_sid": "trmum1f70862263115090280 1a1n",
      "date_created": "2026-01-23T13:28:11Z",
      "date_updated": "2026-01-23T13:41:59Z",
      "mode": "flow"
    }
  }
}
```


Response Parameters

Parameter Name	Type & Value
id	String; The phone number mapping ID
phone_number	String; The phone number in E.164 format
trunk_sid	String; The associated trunk
mode	String; The updated routing mode (pstn or flow)
date_created	String; ISO 8601 timestamp when mapping was created
date_updated	String; ISO 8601 timestamp when mapping was updated (will be updated after this call)

9. Set Trunk Alias (Caller ID)

Sets the phone number displayed to called parties on outbound calls. This is useful when you want to display a specific caller ID regardless of which phone number is mapped to the trunk.

HTTP Request

```
POST https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/settin
gs
```

Request Headers

Header	Value
Content-Type	application/json

Request Parameters

Parameter Name	Mandatory/ Optional	Value
settings	Mandatory	Array; List of setting objects
settings[].name	Mandatory	String; Setting name. Use trunk_external_aliasfor caller ID
settings[].value	Mandatory	String; The phone number to display as caller ID. Should be in E.164 format. Example: +919876543210

Example Request

```
curl -s -X POST "https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/settin
gs" \
  -H "Content-Type: application/json" \
  -d '{
    "settings": [
      {
        "name": "trunk_external_alias",
        "value": "+919876543210"
      }
```

```
  ]
}'
```

Example Response

```
{
  "request_id": "8ce98845365f43fd97c2f46df38438c6",
  "method": "POST",
  "http_code": 200,
  "metadata": {
    "total": 1,
    "success": 1
  },
  "response": [
    {
      "code": 200,
      "error_data": null,
      "status": "success",
      "data": {
        "name": "trunk_external_alias",
        "value": "+919876543210",
        "trunk_sid": "trmum1f708622631150902801a1n",
        "date_created": "2026-01-23T13:34:50Z",
        "date_updated": "2026-01-23T13:34:50Z"
      }
    }
  ]
}
```

Response Parameters

Parameter Name	Type & Value
metadata.total	Integer; Total number of settings in request
metadata.success	Integer; Number of successfully applied settings
name	String; Setting name (trunk_external_alias)
value	String; The caller ID phone number
trunk_sid	String; The associated trunk
date_created	String; ISO 8601 timestamp when setting was created
date_updated	String; ISO 8601 timestamp when setting was last updated

10. Delete Trunk

Permanently deletes a trunk and all its associated configurations (phone numbers, ACLs, destination URIs).

⚠ **Warning:** This action cannot be undone. All associated phone number mappings, whitelisted IPs, and destination URIs will be permanently deleted.

HTTP Request

```
DELETE https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks?trunk_sid=
<trunk_sid>
```

Example Request

```
curl -s -X DELETE "https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks?trunk_sid=
<trunk_sid>"
```

Example Response


```
{
  "request_id": "f708818c79f547b3aee31c4a480367a5",
  "method": "DELETE",
  "http_code": 200,
  "response": {
    "code": 200,
    "error_data": null,
    "status": "success",
    "data": {
      "trunk_name": "my_trunk1234",
      "date_created": "2026-01-23T13:25:39Z",
      "date_updated": "2026-01-23T13:25:39Z",
      "trunk_sid": "trmum15f77c83605998cdb9d1a1n",
      "status": "active",
      "domain_name": "ameyo5m.pstn.exotel.com",
      "auth_type": "IP-WHITELIST",
      "registration_enabled": "disabled",
      "edge_preference": "auto",
      "nso_code": "ANY-ANY",
      "secure_trunking": "disabled",
      "destination_uris":
```

```
"/v2/accounts/ameyo5m/trunks/trmum15f77c83605998cdb9d1a1n/destination-uris",
      "whitelisted_ips":
"/v2/accounts/ameyo5m/trunks/trmum15f77c83605998cdb9d1a1n/whitelisted-ips",
      "credentials":
"/v2/accounts/ameyo5m/trunks/trmum15f77c83605998cdb9d1a1n/credentials",
      "phone_numbers":
"/v2/accounts/ameyo5m/trunks/trmum15f77c83605998cdb9d1a1n/phone-numbers"
    }
  }
}
```

Response Parameters

The response returns the full trunk data that was deleted, allowing you to verify which trunk was removed.

Error Codes Reference

Error Code	HTTP Status	Message	Description
1000	404	Not Found	Resource not found (invalid trunk_sid, phone_number_id, etc.)
1001	400	Mandatory Parameter missing	Required parameter not provided
1002	400	Invalid parameter	Parameter value is invalid or malformed
1007	400	Invalid request body	JSON parsing error or malformed request body
1008	409	Duplicate resource	Resource already exists (duplicate trunk name, IP already whitelisted, etc.)
1011	415	Unsupported content type	Wrong Content-Type header. Use application/json

Quick Reference

API Endpoints Summary

API	Method	Endpoint
Create Trunk	POST	/v2/accounts/{sid}/trunks
Map Phone Number	POST	/v2/accounts/{sid}/trunks/{trunk_sid}/phone-numbers
Map ACL	POST	/v2/accounts/{sid}/trunks/{trunk_sid}/whitelisted-ips
Map Destination URI	POST	/v2/accounts/{sid}/trunks/{trunk_sid}/destination-uris
Get Phone Numbers	GET	/v2/accounts/{sid}/trunks/{trunk_sid}/phone-numbers
Get ACLs	GET	/v2/accounts/{sid}/trunks/{trunk_sid}/whitelisted-ips
Get Destination URIs	GET	/v2/accounts/{sid}/trunks/{trunk_sid}/destination-uris
Update Phone Number Mode	PUT	/v2/accounts/{sid}/trunks/{trunk_sid}/phone-numbers/{id}
Set Trunk Alias	POST	/v2/accounts/{sid}/trunks/{trunk_sid}/settings
Delete Trunk	DELETE	/v2/accounts/{sid}/trunks?trunk_sid={trunk_sid}

Mode Options

Mode	Description	Use Case
pstn	Routes calls to telephone network	Standard PBX/Contact Center integration
flow	Routes calls to Voice AI bot	StreamKit/Voice AI integration

Notes

- Duplicate resource errors (1008) are safe and can be ignored if the configuration already exists
- Destination URI must always be configured, even when using Exotel Flows
- flow mode is required only for Voicebot or non-Connect applets

1.5. Network & Firewall Configuration

This page explains exactly what needs to be configured on your firewall so your SIP system can:

- Make outbound calls (SIP → PSTN)
- Receive inbound calls (PSTN → SIP)

1) Ports to Open

SIP signalling (call control)

Transport	Port	Protocol	When to use
TLS (recommended)	443	TLS	Production use (secure, enterprise friendly)
TCP	5070	TCP	Use only if TLS is not enabled

Media (audio / RTP)

Type	Port Range	Protocol	Purpose
RTP / SRTP	10000–40000	UDP	Voice media (audio)

Important:
If calls connect but audio is missing or one-way, this port range is usually blocked.

2) Exotel Connectivity Model

Exotel connectivity has **two independent paths**:

1. **Signaling** – SIP INVITE / 100 Trying / 200 OK
2. **Media** – RTP audio packets

Both must be allowed for calls to work correctly.

3) Signaling Endpoints (SIP Proxy)

A) Outbound calling (SIP → PSTN)

Your SIP system sends SIP requests to Exotel.

Use these FQDNs in your trunk / peer configuration:

Use case	Primary FQDN	Secondary FQDN	Notes
Domestic India	edge.mum.in.exotel.com	edge.hyd.in.exotel.com	Configure both for failover
Domestic India (single DNS)	edge.in.exotel.com	–	DNS resolution and retry required
Domestic India (single DNS)	in.voip.exotel.com		DNS resolution and retry required(Specifically used for SIP Auth)

Failover note:
Your SIP system should retry the secondary FQDN if the primary is unreachable.

B) Inbound calling (PSTN → SIP)

Exotel sends SIP INVITEs to your SIP server.

Allow inbound signaling from the following **Exotel signaling source IPs**:

Source IP	Data Center
35.154.174.161	AWS Mumbai
98.130.67.66	AWS Hyderabad
129.154.231.198	OCI(Legacy- Signaling IP)

4) Media IPs (RTP Audio)

These IPs send and receive RTP audio during calls.

Media Pool

Region / POP	Media IPs	DC / Provider
India	3.6.59.115, 13.127.39.217, 43.205.221.135, 13.203.184.147, 13.203.182.84, 13.203.81.133, 3.7.34.113, 13.126.206.147, 35.154.177.121, 13.205.31.133, 35.154.118.78 40.192.25.80, 98.130.133.120, 16.112.157.119, 16.112.117.9, 18.61.59.229, 18.61.247.215	AWS(Mum/Hyd)

Legacy / Other Media Pools

Region / POP	Media IPs	DC / Provider
West Bengal / TN / KA / Delhi / Gujarat / AP	141.148.205.58, 144.24.101.99, 80.225.231.27, 140.245.21.212, 141.148.216.227	OCI
Karnataka	14.194.10.247, 61.246.82.75, 141.148.205.58, 144.24.101.99, 80.225.231.27	KA DC
Mumbai DC	14.142.38.122, 182.76.143.61	MUM DC
Madhya Pradesh DC	121.242.97.185, 182.73.254.178	MP DC
Pune	13.203.182.84, 13.203.81.133	AWS MUM

5) Firewall Rules (What to Allow)

A) Inbound calls (PSTN → SIP)

Allow inbound traffic **to your SIP server**:

Traffic	Source	Destination	Port / Protocol
SIP signaling	Exotel signaling IPs	Your SIP server	443/TLS or 5070/TCP
RTP media	Exotel media IPs	Your RTP ports	10000–40000/UDP

B) Outbound calls (SIP → PSTN)

Allow outbound traffic **from your SIP system**:

Traffic	Source	Destination	Port / Protocol
SIP signaling	Your SIP server	Exotel edge FQDNs	443/TLS or 5070/TCP
RTP media	Your RTP ports	Exotel media IPs	10000–40000/UDP

6) Important: How Inbound Firewalling Works

For inbound calls, **source ports are dynamic** and **must not be fixed**.

What you must configure

- Fixed destination port on your SIP server: 443 or 5070
- UDP media port range: 10000–40000
- Allow Exotel IPs as source

What you must NOT configure

- Do **not** restrict source ports
- Do **not** expect a single fixed port from Exotel

Required behavior (Inbound Signaling)

Item	Value
Destination IP	Your SIP server
Destination port	443 or 5070
Source IP	Exotel signalling IPs
Source port	ANY
Protocol	TCP

Example firewall rule (signaling):

ALLOW TCP

SRC IP: Exotel signaling IPs

SRC PORT: ANY

DST IP: Your SIP server

DST PORT: 443

Required behavior (Inbound Media)

Item	Value
Protocol	UDP
Destination ports	10000–40000
Source IPs	Exotel media IPs
Source ports	ANY

Example firewall rule (media):

ALLOW UDP

SRC IP: Exotel media IPs

SRC PORT: ANY

DST IP: Your SIP server

DST PORT: 10000–40000

7) Which IP List Should You Use?

If you only do India domestic calling

Use:

- **Signaling:** edge.mum.in.exotel.com + edge.hyd.in.exotel.com (or edge.in.exotel.com)
- **Media:** India proposed media IP pool (Circle Specific)

If you are unsure

Allow:

- Exotel signaling IPs (for inbound)
- India proposed media pool
- Any additional country media pool you actively use
- Reachout to support for updated IPs

1.5.1. Network Requirements for VoIP – QoS & Bandwidth

Overview

For a voice call to sound clear and natural, three network conditions must be met: packets must arrive quickly, arrive consistently, and not be dropped. When any of these degrade beyond acceptable limits, callers hear echo, robotic audio, clipping, or complete audio loss.

This document defines the QoS and bandwidth requirements your network must meet to deliver high-quality calls on the Exotel platform.

QoS Requirements

These are the network performance thresholds Exotel measures and recommends for all voice traffic.

Metric	Recommended	Acceptable	What happens if exceeded
One-way latency	≤ 130 ms	≤ 150 ms	Echo, conversational overlap
Round-trip time (RTT)	≤ 260 ms	≤ 300 ms	Unnatural conversation delay
Jitter	≤ 20 ms	≤ 40 ms	Choppy, robotic audio
Packet loss	0%	≤ 1%	Clipping, gaps in speech
MOS score (G.711)	≥ 4.2	≥ 3.6	Poor call experience
MOS score (OPUS)	≥ 4.3	≥ 3.6	Poor call experience

```
Exotel's platform contributes < 20 ms of processing delay. The remaining
latency budget is your network, ISP, and endpoint.
```

Why these thresholds?
Latency and RTT are derived from **ITU-T G.114**, which specifies ≤ 150 ms one-way for high-quality voice. Jitter and packet loss targets follow **ITU-T Y.1541**. MOS is measured using the

ITU-T G.107 E-model – the real-world ceiling for G.711 is ~4.4 and OPUS is ~4.5, so the recommended targets reflect consistently good quality, not just a passing grade.

Bandwidth Requirements

Per Call

Codec	Used For	Bandwidth per Call
G.711	SIP Trunking, IP Calling, PSTN	**100 kbps**
OPUS	WebRTC, Audio Streaming, Voice for AI	**60–80 kbps**

```
Always provision 1.5× your peak concurrent call bandwidth to allow headroom
for signaling and traffic bursts.
```

Concurrent Call Capacity (G.711)

Concurrent Calls	Minimum Bandwidth	Recommended Link
10	1 Mbps	1.5 Mbps
50	5 Mbps	7.5 Mbps
100	10 Mbps	15 Mbps
500	50 Mbps	75 Mbps

Applicability by Channel

Not all QoS parameters apply the same way across channels. Use this as a quick reference.

Parameter	SIP Trunking	IP Calling	WebRTC	Audio Streaming	PSTN
Latency / RTT	Applicable	Applicable	Applicable	RTT affects AI response	Carrier
Jitter	Applicable	Applicable	Applicable	TCP absorbs jitter	Carrier
Packet loss	Applicable	Applicable	Applicable	TCP retransmits	Carrier
Bandwidth planning	Applicable	Applicable	Applicable	Per stream	Carrier

Notes:

- **PSTN** – QoS applies only to the IP leg between your network and Exotel's media gateway. The PSTN leg is carrier-managed.
- **Audio Streaming** – Uses TCP/WebSocket. Jitter and packet loss behave differently from RTP. What matters most is **round-trip latency** for AI pipeline responsiveness (target RTT ≤ 300 ms).
- **WebRTC** – DSCP marking is typically stripped by browsers. QoS must be applied at the network edge.

Network Checklist Before Go-Live

- Average ping to Exotel SIP endpoints **< 50 ms**; no spikes > 150 ms
- UDP jitter test (iperf3) for ≥ 5 minutes under load – target **< 20 ms**
- Packet loss test under simulated call load – must be **< 1%**
- Bandwidth confirmed for peak concurrent call volume (see table above)
- **SIP ALG disabled** on all routers and firewalls
- UDP ports **10000–20000 open bidirectionally**
- 10 test calls placed and MOS reviewed in Exotel dashboard – target **≥ 4.0**

Common Issues

Symptom	Likely Cause	Fix
One-way audio	SIP ALG enabled	Disable SIP ALG on router/firewall
Choppy / robotic voice	Jitter > 40 ms or packet loss > 1%	Check network congestion; enable DSCP EF (46) marking
Calls drop at 30–60 s	Firewall UDP timeout too low	Set UDP session timeout ≥ 180 s
Echo	Latency > 150 ms	Use the nearest Exotel PoP; enable echo cancellation
DTMF not detected	RTP UDP ports blocked	Verify UDP 10000–40000 fully open
SIP 429 errors	CPS/CPM limit exceeded	Reduce call pace; contact support to increase limits

```
SIP ALG is the #1 cause of VoIP issues. Always disable it — on Cisco ASA,
Fortinet, Juniper, Mikrotik, pfSense, and ISP-provided routers.
```

Exotel Platform Commitments

What Exotel guarantees	Value
Platform processing latency	< 20 ms
Inter-datacenter latency	< 10 ms
Media server uptime	99.5% SLA
Redundancy	Multiple PoPs, automatic failover
Encryption	SIP-TLS (signaling) + SRTP (media)
Quality reporting	MOS scores in CDR and dashboard (RTCP-XR)

```
Exotel guarantees QoS within its own infrastructure only. Your last-mile ISP,
LAN/WAN, and endpoint are outside Exotel's control.
```

For support: hello@exotel.com · docs.exotel.com

1.6. SIP Error Codes & Troubleshooting Guide

This table lists **SIP response codes you may encounter**, what they usually mean in real deployments, **where the issue most likely lies**, and **what to check next**.

1) Provisional Responses (1xx – Informational)

SIP Code	Meaning	What It Means	What to Check
100	Trying	SIP request received and being processed	Normal behavior
180	Ringing	Destination endpoint is ringing	Normal behavior
183	Session Progress	Early media (IVR / announcements)	If audio missing → RTP ports

2) Successful Responses (2xx)

SIP Code	Meaning	What It Means	What to Check
200	OK	Call successfully connected	If no audio → RTP / NAT

3) Client Errors (4xx – Most Common)

SIP Code	Meaning	Likely Root Cause	What to Check
400	Bad Request	Malformed SIP headers or SDP	SIP logs for invalid headers
401	Unauthorized	Authentication required	Credentials (if applicable)
403	Forbidden	IP not allowed	ACL / whitelisted IP
404	Not Found	Invalid DID or routing	Phone number mapping
408	Request Timeout	No SIP response	Firewall / reachability
410	Gone	Number inactive or removed	DID status
415	Unsupported Media	Codec not supported	Ensure **G.711 A-law** enabled
480	Temporarily Unavailable	Endpoint unreachable	PBX availability
484	Address Incomplete	Invalid number format	E.164 format
486	Busy Here	Destination busy	Normal behavior
488	Not Acceptable Here	SDP / codec mismatch	G.711 A-law only

4) Server Errors (5xx)

SIP Code	Meaning	Likely Root Cause	What to Check
500	Server Error	Internal processing failure	Retry call
502	Bad Gateway	Upstream routing issue	Retry
503	Service Unavailable	Destination unreachable	Network / routing
504	Gateway Timeout	No upstream response	Firewall / latency
580	Precondition Failure	Media negotiation failed	RTP / NAT

5) Global Failures (6xx)

SIP Code	Meaning	Likely Root Cause	What to Check
600	Busy Everywhere	All endpoints busy	Retry
603	Decline	Call rejected by endpoint	PBX dialplan
604	Does Not Exist Anywhere	Invalid number	DID correctness
606	Not Acceptable	Media policy failure	Codec / SDP

6) Media (Audio) Issues – No SIP Error Shown

These are **the most common issues** and do **not always show SIP error codes**.

Symptom	Likely Cause	What to Check
No audio both ways	RTP blocked	UDP 10000–40000 open
One-way audio	NAT / firewall	Public IP in SDP
Audio drops after answer	RTP timeout	Firewall idle timeout
IVR audio but no agent audio	Asymmetric RTP	Symmetric RTP enabled

7) Codec Requirements (India)

Item	Requirement
Supported codec	**G.711 A-law**
Other codecs	Not supported
Common failure	415 / 488 errors

Ensure:

- G.711 A-law is enabled
- No other codec is forced ahead of it
- Transcoding is disabled (recommended)

8) API-Level Errors (Exotel)

API Error Code	HTTP Status	Meaning	What It Indicates	Common Endpoints	What the Customer Should Do
1000	404	Not Found	Resource does not exist	POST /trunks/{trunk_sid}/phone-numbers POST /trunks/{trunk_sid}/whitelisted-ips POST /trunks/{trunk_sid}/destination-uris PUT /trunks/{trunk_sid}/phone-numbers/{id}	Verify trunk_sid, phone number ID, or API path
1001	400	Mandatory parameter missing	Required field not sent in request	POST /trunks POST /phone-numbers PUT /phone-numbers/{id}	Ensure all mandatory fields are present
1002	400	Invalid parameter	Field value is invalid or not allowed	POST /trunks POST /destination-uris POST /whitelisted-ips	Validate parameter format (IP, FQDN, E.164 number)
1007	400	Invalid request body	JSON is malformed or not parsable	All POST / PUT APIs	Fix JSON syntax, remove trailing commas, ensure valid JSON

1008	409	Duplicate resource	Resource already exists	POST /trunks POST /phone-numbers POST /whitelisted-ips	Safe to ignore if config already exists
1011	415	Unsupported content type	Incorrect Content-Type header	All POST / PUT APIs	Use Content-Type: application/json

9) Before Contacting Exotel Support

Please verify:

- SIP signaling port (443 / 5070) reachable
- UDP 10000–40000 open
- Correct Exotel IPs allowed
- Correct trunk domain used
- Correct mode (pstn or flow)
- Correct destination URI configured
- G.711 A-law enabled

10) When to Contact Exotel Support

Raise a ticket at **support.exotel.com(hello@exotel.com)** only after verification.

Please share:

- Trunk SID
- CallSID
- Call direction (Inbound / Outbound)
- SIP response code (if any)
- Timestamp (with timezone)
- PBX SIP logs or PCAP (if available)

FAQ – Exotel SIP Trunking

1. What is Exotel SIP Trunking?

Exotel SIP Trunking connects your PBX, Contact Center, or Voice AI system to the telephone network over SIP.
It supports inbound, outbound, and bi-directional calling.

2. What systems can I connect using SIP Trunking?

Any SIP-compliant system such as Asterisk, FreePBX, SBCs, Contact Centers, or Voice AI platforms can be connected.

3. What are inbound and outbound calls?

Outbound calls go from your SIP system to phone numbers.
Inbound calls come from phone numbers to your SIP system.

4. What is mode: pstn?

pstn routes calls to and from the telephone network.
This is the default mode for standard calling.

5. What is mode: flow?

flow routes calls to Exotel Flows such as Voicebot or App Bazaar applets.
It is required for Voicebot and non-Connect applets.

6. Do I need to set a Destination URI even when using Flow?

Yes. A Destination URI is mandatory on the trunk for routing and validation, even if the call later goes to Flow.

7. Do I need a static IP?

A static IP is required for outbound calls and StreamKit.
Inbound calls can use either IP or FQDN.

8. Can I use FQDN instead of IP?

Yes, FQDN is supported only for inbound calls (PSTN → SIP).
Outbound calls require IP-based whitelisting.

9. Do I need to whitelist IPs for inbound calls?

No. For inbound calls, Exotel initiates the connection and you only need to allow Exotel source IPs in your firewall.

10. Do I need to whitelist IPs for outbound calls?

Yes. Your SIP server IP must be whitelisted using the Map ACL API, otherwise outbound calls will fail.

11. Which ports should I open on my firewall?

Open 443 (TLS) or 5070 (TCP) for signaling and UDP 10000–40000 for RTP media.

12. Do I need to fix source ports for inbound calls?

No. Source ports are dynamic by design.
You only need to expose a fixed destination port on your SIP server.

13. Calls are connecting but there is no audio. Why?

This usually means RTP ports are blocked.
Ensure UDP ports 10000–40000 are open in your firewall.

14. What does "Duplicate resource" error mean?

It means the configuration already exists (IP, number, or trunk).
This error is safe to ignore.

15. Which audio codec should I use in India?

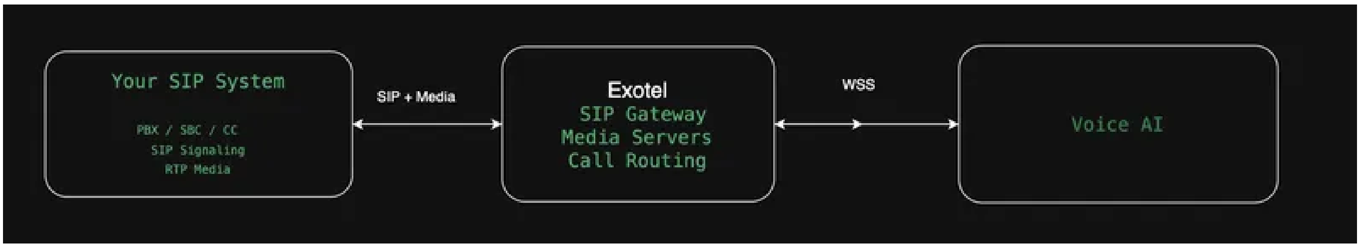
Use G.711 (India standard).

Avoid configuring unnecessary codecs.

1.8. StreamKit Cloud SIP trunking Setup

StreamKit Cloud Setup (for Voice AI)

StreamKit enables you to connect your Contact Center to Voice AI bots. The setup is similar to PSTN, but uses mode: flow when mapping phone numbers.



Setup Flow:

```
Create Trunk → 2. Map Phone Number (mode: flow) → 3. Map ACL to Trunk
```

StreamKit: Create Trunk

1. Create Trunk

Creates a new SIP trunk. This is the first step for all SIP Trunking use cases.

A SIP Trunk acts as a virtual connection between your communication system (PBX/Contact Center) and Exotel's telephony network.

HTTP Request

```
POST https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks
```

Request Headers

Header	Value
Content-Type	application/json

Request Parameters

The following parameters are sent as JSON in the body of the request:

Parameter Name	Mandatory/Optional	Value
trunk_name	Mandatory	String; Unique identifier for the trunk. Must be alphanumeric with underscores only, maximum 16 characters. Example: outbound_trunk, my_pbx_trunk
nso_code	Mandatory	String; Network Service Operator code. Use ANY-ANYfor standard configuration.
domain_name	Mandatory	String; SIP domain for the trunk. Format: <your_sid>.pstn.exotel.com. Example: ameyo5m.pstn.exotel.com

Example Request

```
curl -X POST "https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks" \
  -H "Content-Type: application/json" \
  -d '{
    "trunk_name": "outbound_trunk",
    "nso_code": "ANY-ANY",
    "domain_name": "<your_sid>.pstn.exotel.com"
  }'
```

HTTP Response

On success, the HTTP response status code will be 200 OK.

The trunk_sidis the unique identifier of the trunk - **save this value** as it will be required for all subsequent API calls.

Example Response

```
{
  "request_id": "10a67da360d446378d5c2b66407b7f18",
  "method": "POST",
  "http_code": 200,
  "response": {
    "code": 200,
    "error_data": null,
    "status": "success",
    "data": {
      "trunk_name": "outbound_trunk",
      "date_created": "2026-01-23T09:24:59Z",
      "date_updated": "2026-01-23T09:24:59Z",
      "trunk_sid": "trmum1f708622631150902801a1n",
      "status": "active",
      "domain_name": "ameyo5m.pstn.exotel.com",
      "auth_type": "IP-WHITELIST",
      "registration_enabled": "disabled",
      "edge_preference": "auto",
      "nso_code": "ANY-ANY",
      "secure_trunking": "disabled",
      "destination_uris":
"/v2/accounts/ameyo5m/trunks/trmum1f708622631150902801a1n/destination-uris",
      "whitelisted_ips":
"/v2/accounts/ameyo5m/trunks/trmum1f708622631150902801a1n/whitelisted-ips",
      "credentials":
"/v2/accounts/ameyo5m/trunks/trmum1f708622631150902801a1n/credentials",
      "phone_numbers":
"/v2/accounts/ameyo5m/trunks/trmum1f708622631150902801a1n/phone-numbers"
    }
  }
}
```


Response Parameters

Parameter Name	Type & Value
request_id	String; Unique identifier for this API request
method	String; HTTP method used (POST)
http_code	Integer; HTTP status code (200 for success)
trunk_sid	String; **Important** - Unique identifier for the trunk. Save this for subsequent API calls. Example: trmum1f70862263115090280la1n
trunk_name	String; Name of the trunk as provided in request
domain_name	String; SIP domain for the trunk
status	String; Current trunk status: active- Trunk is ready for use, inactive- Trunk is disabled
auth_type	String; Authentication type. Currently only IP-WHITELISTis supported
registration_enabled	String; SIP registration status: enabledor disabled
edge_preference	String; Edge server preference. Default: auto
nso_code	String; Network Service Operator code
secure_trunking	String; TLS status: enabledor disabled
destination_uris	String; API path to manage destination URIs for this trunk
whitelisted_ips	String; API path to manage ACLs (whitelisted IPs) for this trunk
credentials	String; API path to credentials for this trunk
phone_numbers	String; API path to manage phone numbers for this trunk
date_created	String; ISO 8601 timestamp when trunk was created

Parameter Name	Type & Value
date_updated	String; ISO 8601 timestamp when trunk was last updated

StreamKit: Map Phone Number (Flow Mode)

Same endpoint as PSTN, but with mode: flowto route calls to Voice AI bot.

Example Request

```
curl -X POST "https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/phone-
numbers" \
  -H "Content-Type: application/json" \
  -d '{
    "phone_number": "+919876543210",
    "mode": "flow"
  }'
```

Example Response

```
{
  "request_id": "9351dabddc21476e8351d662f1ce31e1",
  "method": "POST",
  "http_code": 200,
  "response": {
    "code": 200,
    "error_data": null,
    "status": "success",
    "data": {
      "id": "41523",
      "phone_number": "+919876543210",
      "trunk_sid": "trmum1f708622631150902801a1n",
      "date_created": "2026-01-23T13:28:11Z",
      "date_updated": "2026-01-23T13:28:11Z",
      "mode": "flow"
    }
  }
}
```

StreamKit: Map ACL to Trunk

Registers your server's public IP address for authentication. This is required for **Outbound/Termination** calls - allowing your system to send calls through the trunk.

ACL (Access Control List) ensures only authorized IP addresses can use your trunk for outbound calling.

HTTP Request

```
POST https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/whitel
isted-ips
```

Request Headers

Header	Value
Content-Type	application/json

Request Parameters

Parameter Name	Mandatory/ Optional	Value
ip	Mandatory	String; Your server's public IP address. Must be a valid IPv4 address. Example: 44.248.146.11, 203.0.113.50
mask	Optional	Integer; Subnet mask in CIDR notation. Default: 32(single IP). Use 24for /24 subnet, 16for /16 subnet. Example: 32, 24

Example Request

```
curl -X POST "https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/whitel
isted-ips" \
  -H "Content-Type: application/json" \
  -d '{
    "ip": "44.248.146.11",
    "mask": 32
  }'
```

HTTP Response

On success, the HTTP response status code will be 200 OK.

Example Response


```
{
  "request_id": "3daaed4cd05d443f854e07e60dd4c008",
  "method": "POST",
  "http_code": 200,
  "response": {
    "code": 200,
    "error_data": null,
    "status": "success",
    "data": {
      "id": "1153",
      "mask": 32,
      "trunk_sid": "trmum1f708622631150902801a1n",
      "ip": "44.248.146.11",
      "friendly_name": null,
      "date_created": "2026-01-23T11:37:36Z",
      "date_updated": "2026-01-23T11:37:36Z"
    }
  }
}
```


Response Parameters

Parameter Name	Type & Value
id	String; Unique identifier for this ACL entry. Example: 1153
ip	String; The whitelisted IP address
mask	Integer; Subnet mask in CIDR notation
trunk_sid	String; The trunk this ACL is associated with
friendly_name	String or null; Optional friendly name for the IP
date_created	String; ISO 8601 timestamp when ACL was created
date_updated	String; ISO 8601 timestamp when ACL was last updated

5. Build Flow and Map VoIP Exophone follow for all steps **StreamKit Cloud**

b. Create flow in AppBazaar with Voicebot applet and passthru applet:
https://my.in.exotel.com/apps

c. Procure VoIP exophone or contact support

d. Map DID to flow through Exophone: https://my.in.exotel.com/numbers

Github Repo

Postman Collection

2. Voice AI Ecosystem

2.1. Exotel SIP trunk API Reference for Voice AI Ecosystem

Use these snippets from the support articles for **ElevenLabs**, **LiveKit**, **Retell**, **Bolna**, **Pipecat (via Daily SIP)**, **Smallest AI (Atoms)**, **Vocallabs**, **Rapida AI**, and **NLPearl.AI** integrations. Replace placeholders; do not commit real secrets.

GitHub repo (reference): https://github.com/exotel/AgentStream-VoiceAIEcosystem

Placeholder	Description
Account Creation	**Exotel Indian Account**
API_KEY	Exotel API Key **(API Settings**)
API_TOKEN	Exotel API Token
ACCOUNT_SID	Exotel Account SID
SUBDOMAIN	api.in.exotel.com (India) or api.exotel.com (Singapore)
TRUNK_SID	Returned when you create a trunk (trunk_sid in response)

Authentication: HTTP Basic – https://API_KEY:API_TOKEN@SUBDOMAIN/...

Trunk API rate limit: 200 requests per minute on these trunk configuration APIs (Exotel SIP API reference).

Outbound call rate (default): Exotel typically allows **200 outbound call attempts per minute** by default (account-level). If you need a higher outbound initiation limit, contact your **CSM**.

Where to get API credentials: API Settings (India) (or your cluster dashboard).

Headers: Content-Type: application/json on POST/PUT.

Exotel edge: IP and port

Exotel documents **SIP signaling toward their gateway** using **edge IP addresses and ports** – for example **TLS on port 443** or **TCP on port 5070** – per Exotel network and firewall. Use the **IP:port** (and transport) Exotel gives you in onboarding or support.

Exotel may also share **edge hostnames** (instead of raw IPs). Common India examples you may see are:

- **TCP:** in.voip.exotel.com:5070
- **TLS:** in.voip.exotel.com:443

Use the exact **host/IP + port + transport** Exotel assigns to your account/cluster. If a provider UI requires an **IPv4 literal** (no hostname), resolve the hostname to the IPv4 Exotel intends you to use (or request the explicit edge IPs from Exotel support).

The **domain_name** field in **Create trunk** is Exotel's **account SIP domain** for the trunk record ({ACCOUNT_SID}.pstn.exotel.com). That is separate from the **edge IP:port** your Voice AI platform uses to send SIP to Exotel.

Outbound trunk vs inbound SIP trunk

Flow	Exotel API steps
Outbound SIP (Voice AI → Exotel → PSTN)	**1.** Create trunk → **2.** Map DID → **3.** POST …/credentials (digest). **Optional:** POST …/whitelisted-ips **only** if the Voice AI provider gives you a **fixed static egress IP** to allow – see below. **Do not** use destination URI for this path unless Exotel instructs you otherwise.
Inbound SIP (PSTN → Exotel → Voice AI)	After trunk + DID, **map destination URI** on the trunk to the partner's SIP host/port/transport. Use **Flow → Connect** with **sip:<trunk_sid>** in **Dial whom** (see support articles).

Trunk ACL (whitelisted-ips)

Exotel trunk ACL is for **static IP allowlisting** from your Voice AI provider when they give you a **single fixed egress IP**. **Exotel does not support CIDR range whitelist on the trunk** – use **one IP per POST** with mask: 32. If the provider only offers non-static or range-based egress, use **digest credentials** and coordinate with Exotel on what is supported.

Trunk ACL (whitelisted-ips)

Exotel trunk ACL is for **static IP allowlisting** from your Voice AI provider when they give you a **single fixed egress IP**. **Exotel does not support CIDR range whitelist on the trunk** – use **one IP per POST** with mask: 32. If the provider only offers non-static or range-based egress, use **digest credentials** and coordinate with Exotel on what is supported.

Important (auth precedence): Avoid mixing **IP allowlisting** and **digest auth** unless Exotel support has confirmed the expected behavior for your account. In some SIP deployments, once an **IP allowlist** is enabled, the platform may treat **source-IP** as the primary trust signal, and digest behavior can become confusing (especially if a provider publishes **shared / multi-tenant** egress ranges). If your provider only publishes **CIDR ranges** (no dedicated static /32 IPs), do **not** attempt to “whitelist the range” on Exotel – rely on **digest** and work with Exotel/provider support for the correct model.

Create trunk

POST /v2/accounts/{ACCOUNT_SID}/trunks

```
curl -s -X POST "https://${API_KEY}:${API_TOKEN}@${SUBDOMAIN}/v2/accounts/${ACCOUNT_SID}/
  -H "Content-Type: application/json" \
  -d '{
    "trunk_name": "my_trunk_name",
    "nso_code": "ANY-ANY",
    "domain_name": "'"${ACCOUNT_SID}"'.pstn.exotel.com"
  }'
```

trunk_name: alphanumeric + underscores, max 16 characters.

Map phone number (DID) to trunk

POST /v2/accounts/{ACCOUNT_SID}/trunks/{TRUNK_SID}/phone-numbers

```
curl -s -X POST "https://${API_KEY}:${API_TOKEN}@${SUBDOMAIN}/v2/accounts/${ACCOUNT_SID}/
  -H "Content-Type: application/json" \
  -d "{\"phone_number\": \"+9198XXXXXXXX\"}"
```

Optional: "mode": "flow" for StreamKit/Voice AI routing. Save the returned ID for updates.

Create SIP digest credentials (outbound auth)

POST /v2/accounts/{ACCOUNT_SID}/trunks/{TRUNK_SID}/credentials

```
Use the **same** `user_name` and `password` on the Voice AI platform (ElevenLabs SIP digest, LiveKit authUsername / authPassword, Retell termination, etc.).
```

```
curl -s -X POST \
  "https://${API_KEY}:${API_TOKEN}@${SUBDOMAIN}/v2/accounts/${ACCOUNT_SID}/trunks/${TRUNK
  -H "Content-Type: application/json" \
  -d '{
    "user_name": "SIP_USER",
    "password": "SIP_PASS",
    "friendly_name": "voice_ai_platform"
  }'
```

Whitelist IP (ACL) – static provider IP only

POST /v2/accounts/{ACCOUNT_SID}/trunks/{TRUNK_SID}/whitelisted-ips

Use **only** when your Voice AI provider gives a **single static egress IP** you must allow. **Repeat the call for each distinct static IP** (no CIDR ranges on trunk).

```
curl -s -X POST "https://${API_KEY}:${API_TOKEN}@${SUBDOMAIN}/v2/accounts/${ACCOUNT_SID}/
  -H "Content-Type: application/json" \
  -d '{"ip": "203.0.113.50", "mask": 32}'
```

Set destination URI (inbound SIP – PSTN toward Voice AI partner)

POST /v2/accounts/{ACCOUNT_SID}/trunks/{TRUNK_SID}/destination-uris

Used for **inbound** routing: PSTN → Exotel → your SIP partner (FQDN or host/port/transport per partner docs). **Not** part of the minimal **outbound** SIP setup.

```
curl -s -X POST "https://${API_KEY}:${API_TOKEN}@${SUBDOMAIN}/v2/accounts/${ACCOUNT_SID}/
  -H "Content-Type: application/json" \
  -d '{
    "destinations": [
      { "destination": "partner.example.com:5061;transport=tls" }
    ]
  }'
```

Verify (GET)

```
curl -s "https://${API_KEY}:${API_TOKEN}@${SUBDOMAIN}/v2/accounts/${ACCOUNT_SID}/trunks/$
curl -s "https://${API_KEY}:${API_TOKEN}@${SUBDOMAIN}/v2/accounts/${ACCOUNT_SID}/trunks/$
curl -s "https://${API_KEY}:${API_TOKEN}@${SUBDOMAIN}/v2/accounts/${ACCOUNT_SID}/trunks/$
curl -s "https://${API_KEY}:${API_TOKEN}@${SUBDOMAIN}/v2/accounts/${ACCOUNT_SID}/trunks/$
```

2.2. Connect Exotel SIP Trunk to ElevenAgents by ElevenLabs

This guide explains how to connect **Exotel SIP trunking** to **ElevenAgents by ElevenLabs** so you can place and receive PSTN calls in India through Exotel while your agent runs on ElevenLabs.

GitHub repo (reference): https://github.com/exotel/AgentStream-VoiceAIEcosystem

What you will set up

Integration	Direction	When to use
Outbound SIP (digest)	ElevenLabs → Exotel → PSTN	Agent **places outbound** calls via your Exotel DID
Inbound SIP	PSTN → Exotel DID → ElevenLabs	Callers **dial** your Exotel number and reach the agent

Separate the API work: Outbound SIP uses only **create trunk** → **map DID** → **credentials**. **Inbound SIP** adds **destination URI** on the trunk (and Flow). **Trunk ACL** (whitelisted-ips) applies **only** when your Voice AI provider gives you a **static egress IP** – Exotel trunk **does not support CIDR range** allowlisting; use **one static IP per API call** (mask: 32) if needed.

Architecture

Outbound SIP (digest)

```
ElevenLabs → SIP digest → Exotel edge IP:port → Indian PSTN → Customer
```

Inbound SIP

```
Customer → PSTN → Exotel DID → Flow (Connect) → sip:<trunk_sid> → … →
sip.rtc.elevenlabs.io → ElevenLabs Agent
```

Destination URI on the trunk defines where Exotel sends **inbound** SIP toward ElevenLabs. In the **Connect** applet **Dial whom**, use **sip:<trunk_sid>** only – the **trunk_sid** string returned from **Create trunk** (not a full sip:user@host URI).

For FQDN-only inbound (no digest on trunk), **do not** add POST …/credentials unless Exotel requires it for your design.

Prerequisites

Exotel

- my.in.exotel.com with **SIP trunking** enabled.
- **KYC**; Exophone (DID) in **E.164** (+91…).
- **API Key**, **API Token**, **Account SID** from API credentials.
- APIs: **https://api.in.exotel.com** (India).

ElevenLabs

- Agents / Conversational AI and **SIP** phone import.
- **Published agent**; **API key** if testing outbound via HTTP API.

Network

- SIP: **TCP** or **TLS**; RTP: **UDP** per Exotel network doc.

Part A — ElevenLabs (dashboard)

Outbound SIP (digest)

1. **Agents** → create/publish agent.
2. **Phone Numbers** → **Import a phone number from SIP trunk**.
3. **E.164** Exotel DID; **Transport** TCP/TLS per Exotel; **SIP digest** = same values you will set in Exotel POST …/credentials.
4. **Outbound address** = **Exotel edge IP:port** from Exotel.
5. Import → **assign** number to agent. Note **agent_phone_number_id** for API tests.

Inbound SIP (ACL path)

1. Import number; leave digest **empty** if using ACL on ElevenLabs.

2. Allowlist **Exotel signaling IPs** on ElevenLabs if required (Exotel network doc).

Part B – Exotel console

- Numbers, KYC, App Bazaar / Flows for **Connect** when using inbound.

Part C – Exotel APIs

Auth: https://API_KEY:API_TOKEN@api.in.exotel.com/…

Rate limit: 200 requests/minute.

Templates: _exotel-trunk-api-snippets.md.

Outbound SIP – required steps only

1. **Create trunk**
2. **Map DID** to trunk
3. **POST …/credentials** – digest; must match ElevenLabs import

Optional (only if ElevenLabs gives a static egress IP): POST …/whitelisted-ips with that **single IP**, mask: 32. Repeat per static IP if Exotel and your provider agree. **Do not** assume CIDR range whitelist on trunk.

```
curl -s -X POST \
  "https://${API_KEY}:${API_TOKEN}@${SUBDOMAIN}/v2/accounts/${ACCOUNT_SID}/trunks/${TRUNI
  -H "Content-Type: application/json" \
  -d '{
    "user_name": "SIP_USER",
    "password": "SIP_PASS",
    "friendly_name": "eleven_labs"
  }'
```

```
Applicability: UI-driven (ElevenLabs console for agents + phone numbers) with
optional API-driven outbound triggering.
```

Exotel edge: Exotel provides **SIP edge IP address(es) and port(s)** for signaling (for example **TLS 443** or **TCP 5070** per Exotel network and firewall). Configure **<EXOTEL_EDGE_IP>:<PORT>** in ElevenLabs — use the values Exotel assigns for your account.

Edge hostnames you may see (India): in.voip.exotel.com:5070 (TCP) and in.voip.exotel.com:443 (TLS). Use the exact host/IP + port + transport Exotel assigns. See _exotel-trunk-api-snippets.md for details.

ACL vs digest (important): Avoid trying to whitelist **CIDR ranges**. Exotel trunk ACL is intended for **static /32 IPs** only (mask: 32). If a provider publishes only **CIDR** / shared egress ranges, prefer **digest** and coordinate with Exotel/provider support—mixing allowlists and digest can cause auth/routing issues in multi-tenant egress setups.

Inbound SIP — destination URI on trunk

Map **inbound** SIP toward ElevenLabs (host/port/transport per ElevenLabs):

```
curl -s -X POST "https://${API_KEY}:${API_TOKEN}@${SUBDOMAIN}/v2/accounts/${ACCOUNT_SID}/
  -H "Content-Type: application/json" \
  -d '{
    "destinations": [
      { "destination": "sip.rtc.elevenlabs.io:5060;transport=tcp" }
    ]
  }'
```

Connect applet (inbound)

1. App Bazaar → Flow → **Connect** applet.
2. **Dial whom: sip:<trunk_sid>** – paste the **trunk_sid** from the create-trunk API response (prefix sip: only; **not** a full SIP URI).
3. Map the Exophone to this Flow.

Overview: Exotel Voice AI / SIP trunking.

Test calls

Lab validation (outbound)

Outbound SIP has been **tested** end-to-end when trunk + DID + digest + (optional) static-IP ACL align. A **connected call** does not guarantee the **agent speaks** – see below.

Outbound API

Use ElevenAgents by ElevenLabs **outbound call** API – confirm the current URL in ElevenLabs API docs (paths change over time).

```
curl -s -X POST "https://api.elevenlabs.io/v1/convai/<outbound-call-endpoint-per-current
  -H "xi-api-key: ${ELEVENLABS_API_KEY}" \
  -H "Content-Type: application/json" \
  -d '{
    "agent_id": "YOUR_AGENT_ID",
    "agent_phone_number_id": "YOUR_PHONE_NUMBER_ID",
    "to_number": "+91XXXXXXXXXX"
  }'
```

Inbound

Dial your Exotel DID; agent should answer via ElevenLabs.

Call connects but agent does not speak (no bot audio)

This section applies when the **call is triggered** but the **agent does not play** audio.

Check	Action
Assignment	Imported DID **assigned** to the agent used in the API
IDs	agent_phone_number_id matches the imported SIP number
Agent	Published; first message / voice configured
Logs	ElevenLabs ConvAI traces for session errors
RTP	If total silence, check UDP/RTP per Exotel network doc

Troubleshooting

Symptom	Likely cause
SIP **401**	Digest mismatch (Exotel /credentials vs ElevenLabs)
SIP **403** inbound	ElevenLabs ACL vs Exotel source IPs
408 / timeout	DNS/firewall to ElevenLabs FQDN
Connect does nothing	**Dial whom** must be **sip:<trunk_sid>**, not a full URI
Call triggers, no speech	See Call connects but agent does not speak (no bot audio)

Official references

Resource	URL
Exotel SIP API	https://docs.exotel.com/dynamic-sip-trunking/detailed-sip-trunking-api-reference
Exotel + ElevenLabs	https://docs.exotel.com/dynamic-sip-trunking/elevenlabs-and-exotel-sip-trunking-integration-guide-for-voice-ai
Exotel network	https://docs.exotel.com/dynamic-sip-trunking/network-and-firewall-configuration
ElevenLabs SIP	https://elevenlabs.io/docs/agents-platform/phone-numbers/sip-trunking

2.3. Connect Exotel SIP Trunk to LiveKit

This guide connects **Exotel SIP trunking** to **LiveKit Cloud** telephony so PSTN calls can reach **LiveKit rooms** and outbound calls can use Exotel as the Indian PSTN leg.

GitHub repo (reference): https://github.com/exotel/AgentStream-VoiceAIEcosystem

What you will set up

Direction	Path
Inbound PSTN → LiveKit	PSTN → Exotel DID → trunk **destination URI** → LiveKit SIP endpoint → dispatch → room
Outbound PSTN ← LiveKit	LiveKit outbound trunk → digest → Exotel edge **IP:port** → PSTN

Exotel trunk ACL: use **whitelisted-ips only** when LiveKit (or your network) provides a **fixed static egress IP** to allow. Exotel trunk **does not support CIDR range** allowlisting – use **mask: 32** and **one POST per static IP**. Otherwise rely on **digest** (POST …/credentials).

Architecture

```
Inbound:  PSTN → Exotel DID → destination URI on trunk → LiveKit SIP host →
room → agent
Outbound: LiveKit → Exotel edge IP:port (digest) → PSTN
```

Prerequisites

- Exotel: KYC, DID **E.164**, API credentials, https://api.in.exotel.com.
- LiveKit: Cloud project, Telephony, SIP URI from **Project settings** (SIP trunk setup).

Part A – LiveKit Cloud

SIP endpoint and region (inbound)

Copy **SIP URI** from project settings. For India pinning: {subdomain}.india.sip.livekit.cloud (region pinning).

Inbound trunk

Telephony → **SIP trunks** → **Inbound** – include your Exotel DID in E.164 (Inbound trunk).

Dispatch rule

At least one rule so calls land in a room (**Dispatch rule**).

Outbound trunk

- **address** – Exotel **edge IP:port** from Exotel.
- **numbers** – Exotel DID **E.164**.
- **authUsername / authPassword** – same as Exotel **POST …/credentials**.

```
{
  "name": "Exotel outbound",
  "address": "YOUR_EXOTEL_EDGE_IP:443",
  "numbers": ["+9198XXXXXXXX"],
  "authUsername": "SIP_USER",
  "authPassword": "SIP_PASS"
}
```

Agent in the same room

OUTBOUND-EXOTEL-NOTES.md – ring without bot audio usually means no publisher in the room.

Part B – Exotel APIs

Rate limit: 200/minute. Snippets: _exotel-trunk-api-snippets.md.

Outbound SIP – three steps

1. **Create trunk**

2. **Map DID** to trunk
3. **POST …/credentials** (user_name, password) – must match LiveKit outbound trunk auth

Optional: POST …/whitelisted-ips **only if** LiveKit gives you a **static SIP egress IP** to allow – **single IP**, mask: 32 per entry. No CIDR range on trunk.

Inbound only: POST …/destination-uris toward your LiveKit SIP host (not required for minimal outbound-only testing).

```
curl -s -X POST \
  "https://${API_KEY}:${API_TOKEN}@${SUBDOMAIN}/v2/accounts/${ACCOUNT_SID}/trunks/${TRUNI
  -H "Content-Type: application/json" \
  -d '{
    "user_name": "SIP_USER",
    "password": "SIP_PASS",
    "friendly_name": "livekit"
  }'
```

Inbound SIP – destination URI on trunk

```
curl -s -X POST "https://${API_KEY}:${API_TOKEN}@${SUBDOMAIN}/v2/accounts/${ACCOUNT_SID}/
  -H "Content-Type: application/json" \
  -d '{
    "destinations": [
      { "destination": "YOUR_SUBDOMAIN.india.sip.livekit.cloud:5061;transport=tls" }
    ]
  }'
```

Connect applet (inbound)

Dial whom: sip:<trunk_sid> – use the **trunk_sid** from create trunk (**not** a full SIP URI). Map DID to Flow. **Detailed SIP Trunking API Reference**

Testing

Outbound SIP was validated with correct **edge IP:port**, **digest**, and **E.164**; optional static-IP ACL when applicable. Audio still requires an **agent** in the **same** room as the SIP participant.

```
Applicability: UI-driven + developer-driven (LiveKit Cloud console for trunks/dispatch; your app/agent joins rooms). Not a single “import trunk” wizard like some providers.
```

```
Exotel edge: Signaling toward Exotel uses edge IP:port from Exotel (network and firewall). Configure IP:port as Exotel assigns — not an assumed carrier hostname.
```

```
Edge hostnames you may see (India): in.voip.exotel.com:5070 (TCP) and in.voip.exotel.com:443 (TLS). Use the exact host/IP + port + transport Exotel assigns. See _exotel-trunk-api-snippets.md.
```

```
ACL vs digest (important): Exotel trunk ACL (whitelisted-ips) is intended for static /32 IPs only (mask: 32), not CIDR ranges. If the provider/network only has CIDR/shared egress, prefer digest and coordinate with Exotel support—IP allowlisting can become the primary trust signal and cause intermittent auth/routing issues in shared egress setups.
```

```
Scope: LiveKit Cloud with Telephony enabled. See OUTBOUND-EXOTEL-NOTES.md for 403, E.164, and “no audio” patterns.
```

Troubleshooting

Symptom	What to check
403 / 4001	Digest; optional static-IP ACL; correct **edge IP:port**
Wrong format	**E.164** for India
Ring, no bot	Agent + room (OUTBOUND-EXOTEL-NOTES.md)
Connect broken	**sip:<trunk_sid>** only in Dial whom

References

Resource	URL
LiveKit Cloud	https://cloud.livekit.io/
LiveKit SIP trunk setup	https://docs.livekit.io/telephony/start/sip-trunk-setup/
Exotel SIP API	https://docs.exotel.com/dynamic-sip-trunking/detailed-sip-trunking-api-reference

2.4. Connect Exotel SIP trunking to Pipecat (via Daily)

This guide aligns **Exotel SIP trunking** with **Pipecat** using the same **Exotel** patterns as the other Voice AI integrations in this repository: **outbound** = create trunk → map DID → credentials; **optional ACL** = static IPs only (mask: 32), no CIDR ranges on the trunk; **inbound** = destination URI on the trunk when routing toward a **fixed** SIP partner; **Connect** = **sip:<trunk_sid>** where Exotel's product uses that form.

GitHub repo (reference): https://github.com/exotel/AgentStream-VoiceAIEcosystem

```
Applicability: API/engineering-driven (Pipecat orchestration + Daily
rooms/SIP). Inbound is typically a dynamic Daily sip_uri bridge, not a single
static destination URI.
```

Pipecat is not a SIP trunk provider. Pipecat agents typically use **Daily** for **WebRTC** and **SIP dial-in / dial-out**. Pipecat publishes a **PSTN + Daily SIP walkthrough** (upstream doc path). Treat **Exotel** as the **PSTN carrier**: your **webhook server** still creates a **Daily room with SIP** and bridges the live call to Daily's **sip_uri** after **on_dialin_ready**.

What Pipecat + Daily expect

Topic	Detail
SIP on rooms	**Daily SIP** – sip_uri on the room, dialin-ready / Pipecat **on_dialin_ready**
PSTN example	**Pipecat PSTN + Daily SIP guide** – webhook → Daily room → forward to **sip_endpoint**
PSTN without Exotel	**Daily PSTN** – Daily-provisioned numbers

What you will set up

Direction	Summary
Inbound (typical)	PSTN → Exotel → **your webhook** → Daily room + SIP → **bridge** to Daily **sip_uri** (same **shape** as Pipecat's PSTN guide; use **Exotel** call-control APIs to attach the live leg to **sip_uri**)
Outbound	Daily **SIP dial-out** / start_dialout → **Exotel edge IP:port** (digest) → PSTN – **Exotel** trunk + DID + **POST …/credentials**

Part A – Pipecat + Daily

1. Follow **Pipecat's PSTN + Daily SIP guide** to implement **DailyTransport**, **on_dialin_ready**, and bridging to **sip_endpoint**.
2. Replace the **sample carrier** control APIs from that guide with **Exotel's** documented way to **connect the active carrier leg** to an **external SIP URI** (your Daily sip_uri for that session). Confirm details with **Exotel** if needed.
3. For **outbound**, use Daily's **dial-out** / **SIP dial-out** toward **Exotel** as the next SIP hop, then complete **Part B**.

Note: Daily exposes a **per-room** sip_uri. The **static trunk destination** pattern (single SIP host for all calls) matches some Voice AI platforms but **differs** from typical **Daily** room SIP – prefer the **dynamic bridge** unless you operate an **SBC** or fixed ingress.

Part B – Exotel (outbound SIP toward PSTN)

When **Daily** (or your SIP client) sends media to **Exotel** to reach PSTN:

1. **Create trunk**
2. **Map DID** – POST …/trunks/{TRUNK_SID}/phone-numbers
3. **POST …/credentials** – user_name, password (digest aligned with the SIP client leg)

Optional: POST …/whitelisted-ips **only** if Daily (or your egress) publishes a **single static IP** you must allow. Use **mask: 32**.

Part C – Exotel (inbound PSTN toward a fixed SIP host)

Use **only** when your **partner SIP** destination is **fixed** (not the usual **per-room Daily sip_uri** case):

1. **POST …/destination-uris** on the trunk toward that host/port/transport.
2. **Flow → Connect** applet: **Dial whom** = **sip:<trunk_sid>** (the **trunk_sid** from Exotel **create trunk** – not a full SIP URI).
3. Map the Exophone to the Flow.

Exotel API snippets

Authentication: https://API_KEY:API_TOKEN@api.in.exotel.com/…
Rate limit: 200 requests/minute on trunk configuration APIs.

Exotel SIP trunk API Reference for Voice AI Ecosystem

Troubleshooting

Symptom	What to check
Call never reaches Daily	Exotel **bridge** to the **current** sip_uri; room **SIP** enabled; **dialin-ready** / on_dialin_ready
One-way audio / codec mismatch	**SDP** codecs – Daily **PCMU/PCMA** vs Exotel PSTN leg
Outbound fails	Trunk **credentials**; **Exotel edge IP:port** and transport; DID on trunk
Connect misrouted	**sip:<trunk_sid>** only in **Dial whom** (when using that applet pattern)

Official references

Resource	URL
Daily dashboard	https://dashboard.daily.co/
Pipecat – PSTN + Daily SIP	https://docs.pipecat.ai/guides/telephony/twilio-daily-sip
Pipecat – Daily PSTN	https://docs.pipecat.ai/guides/telephony/daily-pstn
Daily – SIP	https://docs.daily.co/guides/products/dial-in-dial-out/sip
Pipecat phone example	https://github.com/pipecat-ai/pipecat-examples/tree/main/phone-chatbot
Exotel SIP API	https://docs.exotel.com/dynamic-sip-trunking/detailed-sip-trunking-api-reference

2.5. Connect Exotel SIP trunking to Bolna Voice AI

This guide aligns **Exotel SIP trunking** with **Bolna AI** using the same patterns as the other Voice AI integrations in this repository: **outbound Exotel** = create trunk → map DID → credentials; **inbound** = destination URI on the trunk; **Connect** = **sip:<trunk_sid>**; **ACL** = static IPs only (mask: 32), no CIDR ranges on the trunk.

GitHub repo (reference): https://github.com/exotel/AgentStream-VoiceAIEcosystem

```
Applicability: Hybrid — BYOT is API/config-driven (SIP trunk objects) and may
also have portal steps depending on account access (SIP is Beta).
```

Outbound SIP is supported. With BYOT, Bolna **places outbound PSTN calls over SIP** through your trunk: it resolves from_number to your trunk, then signals to your **gateway** (Exotel **edge IP:port**) using **userpass** (or **ip-based**) auth. That is the flow described in Make Outbound Calls via Your SIP Trunk. **Part B** below is exactly what Exotel needs on the **carrier** side for that outbound SIP leg.

Bolna also offers a **dashboard connector** for Exotel (REST API link) – see Connect Your Exotel Account to Bolna. This article focuses on **SIP BYOT** where you configure **Exotel SIP trunking** and a **Bolna SIP trunk** together.

```
Bolna: SIP trunking is Beta; SRTP is not supported (plain RTP). See Bring
Your Own SIP Trunk.
Engineering detail: [bolna/integrations/exotel-vsip/bolna-exotel-voice-ai-
connector.md](../../bolna/integrations/exotel-vsip/bolna-exotel-voice-ai-
connector.md) Quickstart: [bolna/integrations/exotel-vsip/QUICKSTART.md]
(../../bolna/integrations/exotel-vsip/QUICKSTART.md)
```

What Bolna expects (BYOT)

Topic	Detail
Create trunk	**Create SIP Trunk API** – POST https://api.bolna.ai/sip-trunks/trunks with Bearer token
Auth	userpass (username/password) or ip-based with IP identifiers on Bolna
Gateway	Points to your carrier – for Exotel, use **Exotel edge IP:port** from **Exotel network doc**
Inbound origination	Carrier sends traffic to **sip:13.200.45.61:5060** per **Receive Inbound Calls via Your SIP Trunk** – confirm in current Bolna docs
Outbound calls	**Make Outbound Calls via Your SIP Trunk** – agent telephony_provider: sip-trunk, from_number on trunk

What you will set up

Direction	Summary
Outbound	Bolna → SIP digest → Exotel edge → PSTN
Inbound	PSTN → Exotel DID → trunk **destination URI** toward Bolna (13.200.45.61:5060 per Bolna) → Bolna agent

Part A – Bolna

1. Obtain **SIP trunk / BYOT** access (enterprise@bolna.ai if required).
2. **Create SIP trunk** with gateway = **Exotel edge IP:port** and userpass matching Exotel POST …/credentials – this is what enables **outbound SIP** from Bolna → Exotel → PSTN.
3. **Add phone numbers** to the Bolna trunk (required for from_number on outbound calls).
4. Set agent telephony_provider to sip-trunk, then place outbound calls with the **call API** (from_number must be a DID on the trunk).
5. For **inbound** only: map numbers to agents per **inbound BYOT** and ensure Exotel routes to **sip:13.200.45.61:5060** per Bolna (Part C).

Alternative: Use **Exotel provider connection** in Bolna **Providers** instead of manual SIP BYOT when that product path fits.

Part B – Exotel (outbound SIP)

1. **Create trunk**
2. **Map DID** – POST .../trunks/{TRUNK_SID}/phone-numbers
3. POST .../credentials – user_name, password (same as Bolna auth_username / auth_password for userpass)

Optional: POST .../whitelisted-ips **only** if Bolna publishes a **single static IP** you must allow on Exotel (Bolna docs reference **13.200.45.61** in troubleshooting – **always confirm** with current Bolna documentation). Use **mask: 32**.

Part C – Exotel (inbound SIP)

1. POST .../destination-uris on the trunk so **inbound** PSTN is routed toward Bolna's SIP entry (host/port per Bolna – typically aligned with **13.200.45.61:5060**; format per Exotel API).
2. **Flow** → **Connect** applet: **Dial whom** = **sip:<trunk_sid>** (the trunk_sid from Exotel **create trunk** – not a full SIP URI).
3. Map the Exophone to the Flow.

Exotel API snippets

Authentication: https://API_KEY:API_TOKEN@api.in.exotel.com/...
Rate limit: 200 requests/minute on trunk configuration APIs.

Full reference: **Detailed SIP Trunking API Reference**

Troubleshooting

Symptom	What to check
No media / failed SDP	**SRTP** – Bolna does not support SRTP; use plain RTP
Outbound fails	Trunk is_active on Bolna; gateway IP:port; digest match
Inbound never hits Bolna	Exotel **destination URI**; Bolna inbound_enabled; number mapping
Connect misrouted	**sip:<trunk_sid>** only in Dial whom

Official references

Resource	URL
Bolna BYOT setup (start here)	https://www.bolna.ai/byot-setup
Bolna SIP introduction	https://www.bolna.ai/docs/sip-trunking/introduction
Bolna + Exotel (dashboard)	https://www.bolna.ai/docs/exotel-connect-provider
Bolna Create SIP Trunk	https://www.bolna.ai/docs/api-reference/sip-trunks/create
Bolna BYOT outbound	https://www.bolna.ai/docs/sip-trunking/byot-outbound-calls
Bolna BYOT inbound	https://www.bolna.ai/docs/sip-trunking/byot-inbound-calls
Exotel SIP API	https://docs.exotel.com/dynamic-sip-trunking/detailed-sip-trunking-api-reference

2.6. Connect Exotel SIP trunking to Rapida AI

This guide aligns **Exotel** with **Rapida AI** for voice assistants. Rapida documents **two** relevant patterns:

GitHub repo (reference): https://github.com/exotel/AgentStream-VoiceAIEcosystem

```
Applicability: Hybrid — UI-driven native Exotel integration
(webhook/streaming) OR SIP-driven SIP trunk path.
```

1. **Native Exotel integration** – Exotel **app / Flow** calls Rapida's **webhook + bidirectional media stream** (no Exotel SIP trunk API required for this path).
2. **SIP trunk** – Exotel as **SIP carrier** (SIP trunking) ↔ Rapida's **SIP server** at **sip-01.in.rapida.ai:5060** – same **trunk / credentials / destination-uris** patterns as other articles in this repo.

```
Primary Rapida reference: Exotel integration · SIP trunk integration · Phone
deployment
```

```
Engineering detail: rapida/integrations/exotel-vsip/rapida-exotel-voice-ai-
connector.md
```

```
Quickstart: rapida/integrations/exotel-vsip/QUICKSTART.md
```

Choose a path

Path	Best when	Exotel work	Rapida work
A – Native Exotel	You want Rapida's documented **streaming** integration	Configure **App / Flow** webhook to Rapida; assign DID	**Integration** → **Tools** → Exotel credentials; **Phone** deployment with **App ID** + number
B – SIP trunk (SIP trunking)	You need **SIP** toward Rapida from Exotel (or digest toward Exotel for outbound)	**Create trunk** → **map DID** → **credentials**; **destination-uris** toward Rapida SIP host; **Connect sip:<trunk_sid>**	**SIP Trunk** credential + **Phone** deployment with **SIP** as provider

If you use **Path A**, you may not need **POST …/trunks** at all – follow Rapida's Exotel guide first.

Path A – Native Exotel (webhook + media stream)

From Rapida – Exotel:

Rapida – credentials

1. **Integration** → **Tools** → **Exotel** → **Setup Credential**.
2. Fields (per Rapida): **Account SID**, **Client ID**, **Client Secret** – sourced from the Exotel dashboard (API / app settings).
    - Exotel India often labels credentials **API Key** and **API Token**; map them to whatever Rapida's form expects (Exotel API credentials for India).

Rapida – phone deployment

1. Assistant → **Deploy** → **Phone**.
2. **Telephony:** provider **Exotel**, select credential, **Phone number** (Exotel virtual number), **App ID** (Exotel applet / flow id that will hit Rapida).

Exotel – applet / Flow

Set the inbound URL Rapida documents (replace placeholders):

```
https://websocket-01.in.rapida.ai/v1/talk/exotel/call/{your-assistant-id}?x-api-key={your-api-key}
```

Assign your Exotel number to this app. **Confirm the exact hostname and path** in Rapida's Exotel guide if it changes.

Outbound

Use Rapida **SDK** or **REST** (POST https://api.rapida.ai/v1/talk/call) – examples in Rapida – Exotel.

Path B – Exotel SIP trunking + Rapida SIP trunk

From **Rapida – SIP trunk**:

Rapida SIP endpoint (for routing to Rapida)

```
sip:sip-01.in.rapida.ai:5060
```

Transport **UDP** or **TCP**; codecs **G.711 PCMU** (preferred) / **PCMA**. Allow **RTP** per Rapida + your firewall docs.

Exotel – inbound PSTN → Rapida

1. **Create trunk** → **map DID** → (optional) **POST .../credentials** if your design requires digest on the Exotel side.
2. **POST .../destination-uris** toward Rapida, e.g.:

```
curl -s -X POST
"https://${API_KEY}:${API_TOKEN}@${SUBDOMAIN}/v2/accounts/${ACCOUNT_SID}/trun
ks/${TRUNK_SID}/destination-uris" \
  -H "Content-Type: application/json" \
  -d '{
    "destinations": [
      { "destination": "sip-01.in.rapida.ai:5060;transport=udp" }
    ]
  }'
```

1. **Flow** → **Connect: Dial whom** = **sip:<trunk_sid>** (Voice AI / SIP trunking).

Rapida – SIP trunk credential

Integration → **Tools** → **SIP Trunk**: set **SIP URI** to your **Exotel edge IP:port** (and digest if used) for **outbound** from Rapida toward Exotel – mirror **ElevenLabs-style** termination. Use

Exotel network and firewall for edge values.

Optional Exotel ACL: POST .../whitelisted-ips **only** if Rapida publishes **fixed static SIP egress IPs** to allow – **one IP per POST**, **mask: 32** (Exotel trunk does not support arbitrary CIDR ranges).

Exotel SIP trunk API Reference for Voice AI Ecosystem

Troubleshooting

Symptom	What to check
Inbound never hits Rapida (Path A)	Webhook URL, **assistant id**, **x-api-key**, number linked to correct app
SIP failures (Path B)	**sip-01.in.rapida.ai** reachability, **UDP/TCP**, **codec**; **destination-uris** format
Outbound fails	Rapida credential + deployment; **from** number is your Exotel DID
Connect misrouted	**sip:<trunk_sid>** only in Dial whom (Path B)

References

Resource	URL
Rapida – Exotel	https://doc.rapida.ai/integrations/telephony/exotel
Rapida – SIP trunk	https://doc.rapida.ai/integrations/telephony/sip
Rapida – Phone deployment	https://doc.rapida.ai/voice-deployment-options/phone
Rapida – Credentials	https://doc.rapida.ai/credential/rapida-credentials
Rapida – Overview	https://doc.rapida.ai/introduction/overview
Exotel SIP API	https://docs.exotel.com/dynamic-sip-trunking/detailed-sip-trunking-api-reference

2.7. Connect Exotel SIP trunking to Retell AI

This guide connects **Exotel SIP trunking** to **Retell AI** using elastic SIP per Retell custom telephony, with Exotel as the Indian PSTN provider.

GitHub repo (reference): https://github.com/exotel/AgentStream-VoiceAIEcosystem

```
Applicability: UI-driven (Retell dashboard custom telephony) with optional API-driven call control.
```

```
Exotel edge: Use IP:port from Exotel for SIP toward their gateway (network and firewall).
```

```
Edge hostnames you may see (India): in.voip.exotel.com:5070 (TCP) and in.voip.exotel.com:443 (TLS). Use the exact host/IP + port + transport Exotel assigns. See _exotel-trunk-api-snippets.md.
```

```
ACL vs digest (important): Exotel trunk ACL is intended for static /32 IPs only (mask: 32), not CIDR ranges. If Retell provides CIDR ranges (common), do not attempt to whitelist ranges on Exotel—prefer digest and coordinate with Exotel/provider support if you see auth/routing issues.
```

```
Full reference: retell/integrations/exotel-vsip/retell-exotel-voice-ai-connector.md
```

```
Quickstart: retell/integrations/exotel-vsip/QUICKSTART.md
```

Retell (from official docs)

- **SIP server:** sip:sip.retellai.com with ;transport=tcp (or tls / udp) – **Custom telephony.**

- Retell publishes **IP ranges** for carriers to allowlist **toward Retell**; on **Exotel trunk ACL**, you can only add **static single IPs** (mask: 32) per Exotel – **not** full CIDR ranges on the trunk. If Retell gives ranges, coordinate with Exotel or use **digest** auth.

Flows

Direction	What to configure
Outbound SIP	Exotel: **create trunk** → **map DID** → **credentials**. Optional **whitelisted-ips** only if Retell provides a **fixed static egress IP** (one IP per POST, mask: 32).
Inbound SIP	Exotel: **destination URI** on trunk toward Retell (sip.retellai.com host/port/transport per Retell). **Connect** applet: **sip:<trunk_sid>** in **Dial whom** (value = API trunk_sid, not a full URI).

Part A – Retell

1. Configure agent; **import** Exotel DID after Exotel trunk exists (Custom telephony).
2. Match **digest** to Exotel POST .../credentials for outbound termination.

Part B – Exotel APIs

Auth: API_KEY:API_TOKEN@api.in.exotel.com · **200 requests/minute (SIP trunk APIs)** ·

Exotel SIP trunk API Reference for Voice AI Ecosystem

Outbound SIP

1. Create trunk
2. Map DID
3. POST .../credentials
4. *(Optional)* whitelisted-ips – **only** for a **static IP** from Retell, mask: 32

Inbound SIP

POST .../destination-uris – example shape (confirm port/transport with Retell):

```
curl -s -X POST
"https://${API_KEY}:${API_TOKEN}@${SUBDOMAIN}/v2/accounts/${ACCOUNT_SID}/trun
ks/${TRUNK_SID}/destination-uris" \
  -H "Content-Type: application/json" \
  -d '{
    "destinations": [
      { "destination": "sip.retellai.com:5060;transport=tcp" }
    ]
  }'
```

Connect: sip:<trunk_sid> in Dial whom.

Dial to SIP URI (alternative)

Register Phone Call → dial sip:{call_id}@sip.retellai.com within **5 minutes** – **Method 2.**

References

Resource	URL
Retell dashboard	https://dashboard.retellai.com/
Retell – custom telephony	https://docs.retellai.com/deploy/custom-telephony
Retell – quick start	https://docs.retellai.com/get-started/quick-start
Exotel SIP API	https://docs.exotel.com/dynamic-sip-trunking/detailed-sip-trunking-api-reference

2.8. Connect Exotel SIP trunking to Smallest AI (Atoms)

2.9. Connect Exotel SIP trunking with Vocallabs (Superflow B2B API)(Alpha)

2.10. Connect Exotel SIP trunking to NLPearl.AI

3. SIP Trunk Configuration

3.1. Overview

3.2. Exotel SIP Trunking – TCP (India)

3.3. Exotel SIP Trunking – TLS (India)

3.4. Exotel SIP Trunking to Flow Integration Guide

3.5. Flow and API Configuration Guide for Voice AI & Contact Centre Platforms

3.6. Exotel Virtual SIP Trunking – FQDN-based