exotel DOCS

Dynamic SIP Trunking

CONTENTS

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**
- Completed **KYC**
- **API credentials**
- At least one **Exophone** (DID)
- SIP system (PBX / SBC / Contact Center) with:
  - Public static IP/Credentials
  - 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

```
curl -s -X POST "https://<api_key>:<api_token>@<subdomain>/v2/accounts/<account_sid>/trunks" \
  -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

```
curl -s -X POST "https://<api_key>:<api_token>@<subdomain>/v2/accounts/<account_sid>/trunks/<trunk_sid>/phone-numbers" \
  -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

```
curl -s -X POST "https://<api_key>:<api_token>@<subdomain>/v2/accounts/<account_sid>/trunks/<trunk_sid>/whitelisted-ips" \
  -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

```
curl -s -X POST \
  "https://${API_KEY}:${API_TOKEN}@${SUBDOMAIN}/v2/accounts/${ACCOUNT_SID}/trunks/${TRUNK_SID}/credentials" \
  -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

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

Using FQDN

(No IP whitelist required)

curl

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

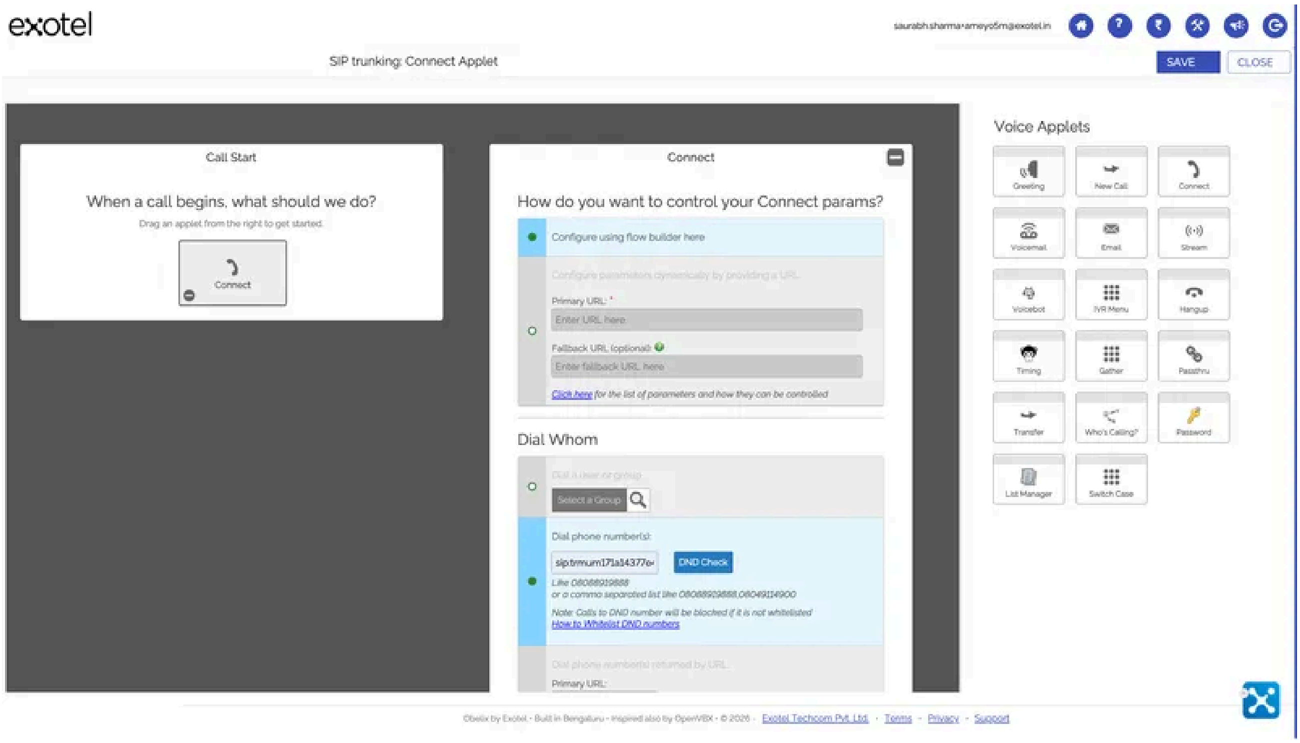
Step 5: Create Flow for Inbound Calls

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:

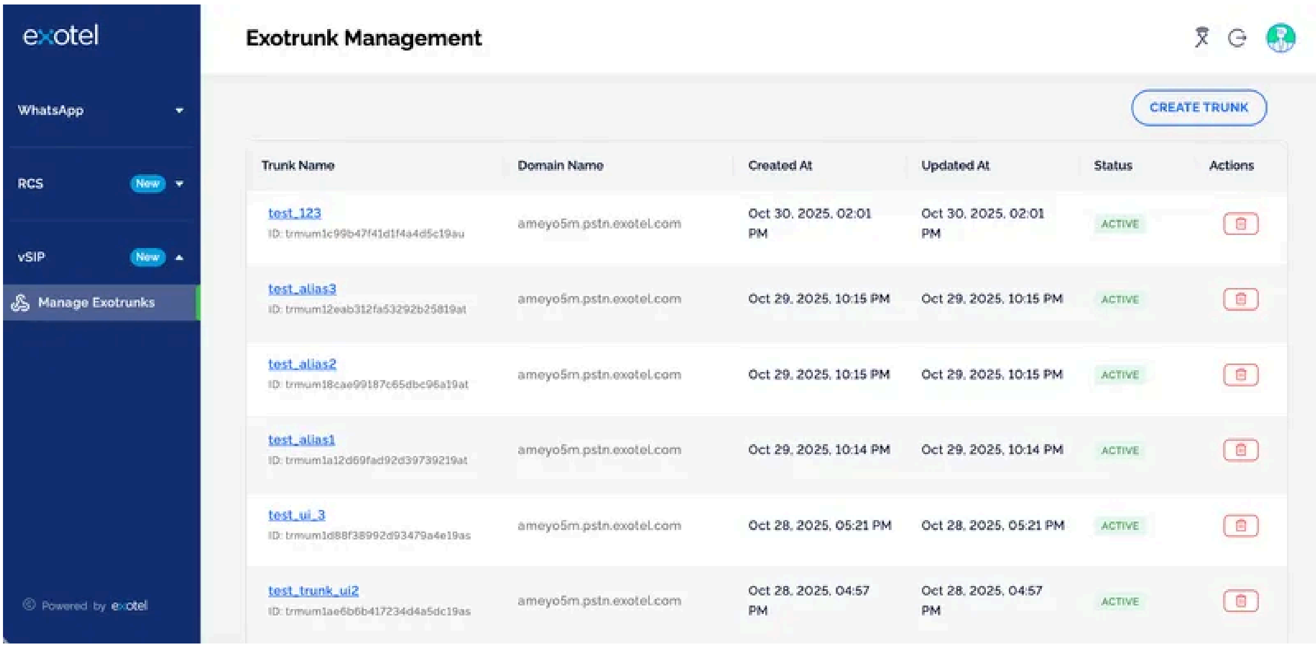
Field	Description
Trunk Name	The user-defined name of the SIP trunk.
Domain Name	The SIP domain through which Exotel routes your traffic.
Created At / Updated At	Timestamps showing when the trunk was created and last modified.
Status	The current operational state (e.g., *Active*).
Actions	Allows you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

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

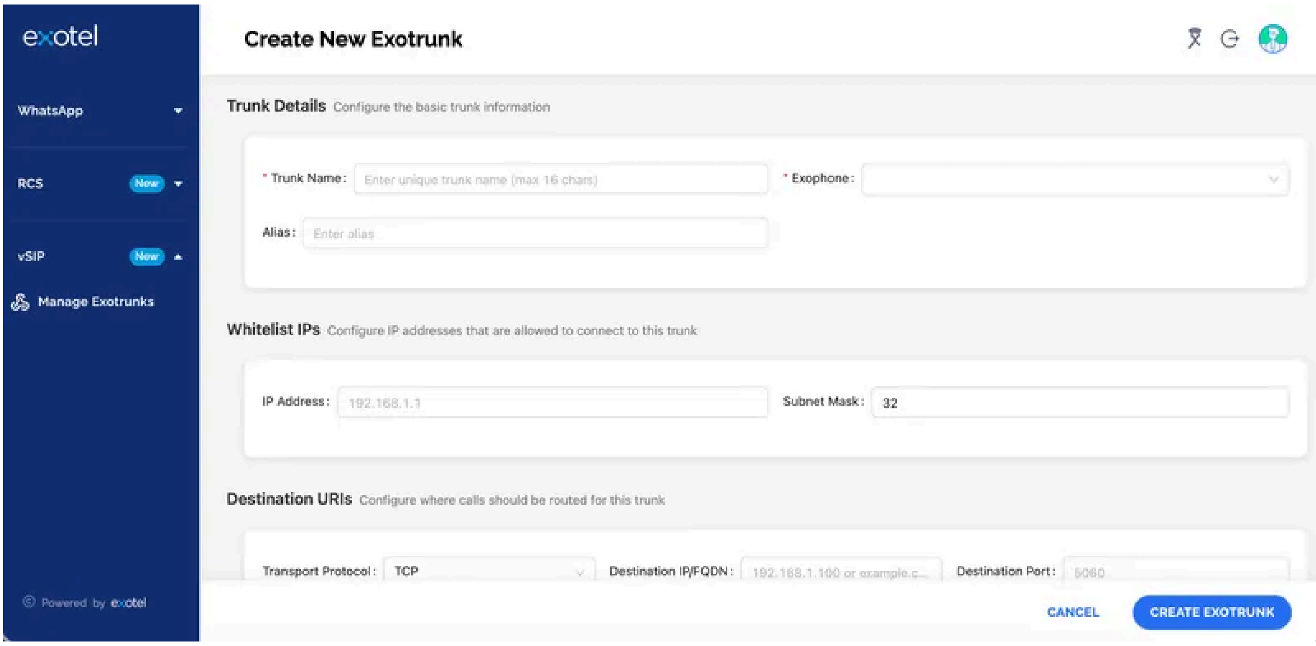
Creating a New Exotrunk

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

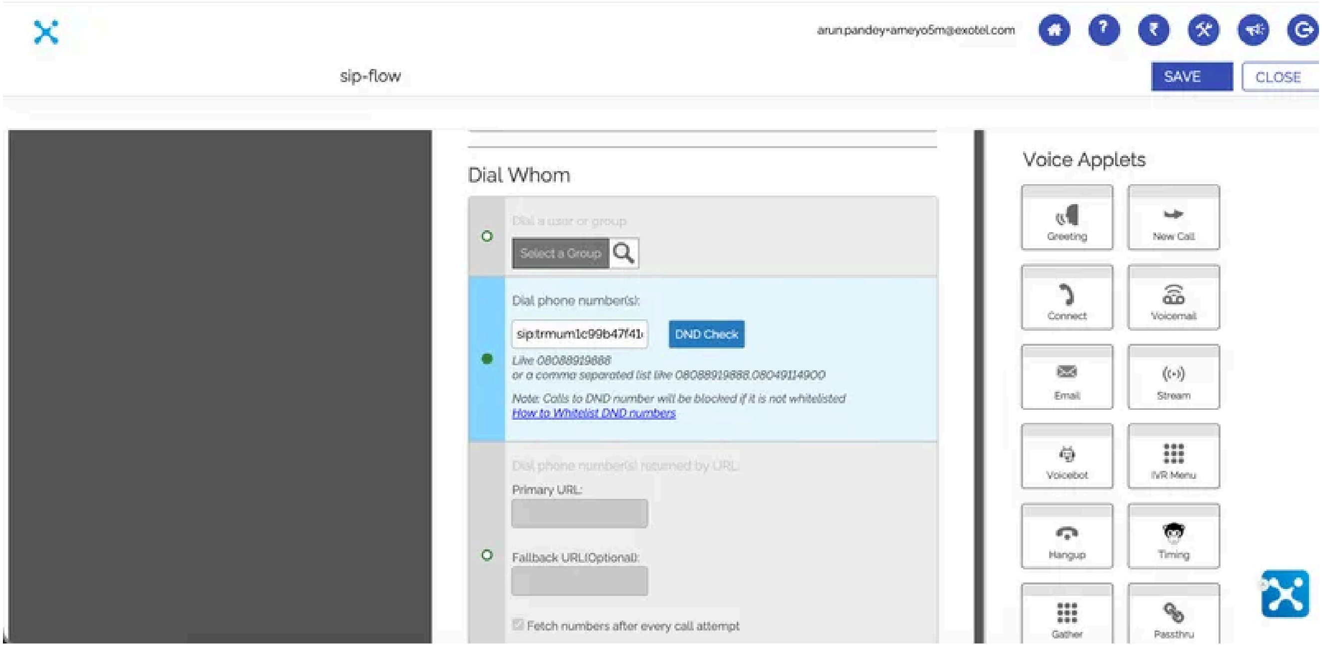
1. Click **CREATE** in the App Bazaar section.
   A pop-up will appear prompting you to **Add New Flow**.
2. Enter a name for your flow (e.g., `sip-flow`) and click **OK**.
3. You will be redirected to the visual **Flow Builder** interface.

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) or Create Credentials(Digest Auth) for trunk(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)
```

1.4.1. 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
date_updated	String; ISO 8601 timestamp when trunk was last updated

1.4.2. 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

1.4.3. 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.
- Recommended in case of Elevenlabs, Livekit, Retell etc SIP trunking setups

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).

1.4.4. 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>/whitelisted-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>/whitelisted-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

1.4.5. 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>/credentials" \
  -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": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
  "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>/credentials"
```

HTTP Response

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

Example Response

```
{
  "request_id": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
  "method": "GET",
  "http_code": 200,
  "metadata": {
    "total": 1,
    "page_size": 50,
    "page": 1,
```

```
    "first_page_uri": "/v2/accounts/exotelveenotesting1m/trunks/trmum17d8e9a37a3732ecbf91a3u/credentials?
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>/credentials?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

1.4.6. 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>/destination-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>/destination-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 **Connect Applet Setup for Inbound SIP Trunking**

1.4.7. Manage & View

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

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

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>/whitelisted-ips
```

Example Request

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

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>/destination-uris
```

Example Request

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

```
  ]
}
```

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": "trmum1f708622631150902801a1n",
      "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)

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>/settings
```

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>/settings" \
  -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": "trmum1f70862263115090280la1n",
        "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

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.

List Trunks

Retrieves all SIP trunks for the account with pagination. Optionally filter to a single trunk using trunk_sid.

HTTP Request

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

Request Headers

Header	Value
Content-Type	application/json

Query Parameters

Parameter Name	Mandatory/Optional	Value
page_size	Optional	Integer; number of results per page. Default: 50
offset	Optional	Integer; pagination offset. Default: 0
trunk_sid	Optional	String; when provided, returns only the matching trunk

Example Request

:::BlockQuote curl -s -X GET "https://<your_api_key>:<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks?page_size=50&offset=0" :::

Example Request (single trunk filter)

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

HTTP Response

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

Example Response


```
{
"request_id": "785471d288054cbf8c677b75e0b5f2f8",
```

```
"method": "GET",
"http_code": 200,
"metadata": { "page_size": 50, "first_page_uri": "/v2/accounts/<your_sid>/trunks?offset=0&page_size=50",
"prev_page_uri": null, "next_page_uri": null },
"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
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
metadata.next_page_uri	String or null; URI for next page
response[]	Array; list of trunk objects (same fields as Create Trunk response)

Update Trunk

Partially updates trunk properties such as trunk_name, auth_type, or nso_code.

HTTP Request

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

Request Headers

Header	Value
Content-Type	application/json

Request Parameters

Parameter Name	Mandatory/Optional	Value
trunk_name	Optional	String; Unique identifier for the trunk. Must be alphanumeric with underscores only, maximum 16 characters.
auth_type	Optional	String; Authentication type (e.g. IP-WHITELIST)
nso_code	Optional	String; Network Service Operator code. Use ANY-ANY for standard configuration.

Example Request

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

HTTP Response

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

Example Response


```
{
"request_id": "c719cd56eb5943e789e1bdbd4ce1515a",
"method": "PUT",
"http_code": 200,
"response":
{ "code": 200,
"error_data": null,
"status": "success",
"data":
{ "trunk_name": "my_pbx_trunk",
"date_created": "2026-01-23T09:24:59Z",
"date_updated": "2026-01-23T14:10:12Z",
"trunk_sid": "trmum1f708622631150902801a1n",
"status": "active",
"domain_name": "<accounsid>.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
trunk_sid	String; Unique identifier for the trunk
trunk_name	String; Updated trunk name
date_updated	String; ISO 8601 timestamp when trunk was last updated
status	String; Current trunk status (active / inactive)

Trunk Map Lookup (Exophone)

Resolves which trunk a virtual number (ExoPhone / DID) is mapped to.

HTTP Request

```
GET https://<your_api_key>:<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunk-maps
```

Request Headers

Header	Value
Content-Type	application/json

Query Parameters

Parameter Name	Mandatory/Optional	Value
exophone	Mandatory	String; Virtual number / DID in E.164 format. Example: +919876543210
trunk_sid	Optional	String; optionally constrain lookup to a specific trunk

Example Request

```
curl -s -X GET "https://<your_api_key>:<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunk-maps?
exophone=+919876543210"
```

HTTP Response

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

Example Response

```
{
"request_id": "13ab9319cf574486ba299c364f82cade",
"method": "GET",
"http_code": 200,
"response":
{ "code": 200,
"error_data": null,
"status": "success",
"data":
```

```
{ "exophone": "+919876543210",
"trunk_sid": "trmum1f708622631150902801a1n",
"phone_number_id": "41512",
"mode": "pstn"
}
}
}
```

Response Parameters

Parameter Name	Type & Value
exophone	String; The queried virtual number in E.164 format
trunk_sid	String; Trunk SID associated with this number
phone_number_id	String; Numeric mapping id (same id used by Update Phone Number Mode / Delete Phone Number Mapping)
mode	String or null; Routing mode (pstn / flow / null)

Delete Phone Number Mapping

Detaches a phone number (DID/ExoPhone) from the trunk.

Important: Pass the numeric mapping id returned when you mapped the phone number (e.g. 41523), **not** the phone number itself. The id is passed as query parameter id.

HTTP Request

```
DELETE https://<your_api_key>:<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/phone-numbers?id=<phone_number_id>
```

Example Request

```
curl -s -X DELETE "https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/phone-numbers?id=41523"
```

HTTP Response

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

Example Response

```
{
"request_id": "c719cd56eb5943e789e1bdbd4ce1515a",
"method": "DELETE",
"http_code": 200,
"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
id	String; Deleted phone number mapping id
phone_number	String; The detached phone number in E.164 format
trunk_sid	String; The trunk this mapping belonged to
mode	String or null; Routing mode at time of delete

Update Whitelisted IP

Updates an existing ACL (whitelisted IP) entry – for example to change IP or subnet mask.

Important: \<whitelist_entry_id> is the numeric id returned when you mapped the ACL (e.g. 1153), **not** the IP address itself.

HTTP Request

```
PUT https://<your_api_key>:<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/whitelisted-ips/<whitelist_entry_id>
```

Request Headers

Header	Value
Content-Type	application/json

Request Parameters

Parameter Name	Mandatory/Optional	Value
ip	Mandatory	String; IPv4 address. Example: 44.248.146.11
mask	Mandatory	Integer; Subnet mask in CIDR notation. Example: 32, 24

Example Request

```
curl -s -X PUT "https://<your_api_key>:<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/whitelisted-ips/1153" \ -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": "PUT",
"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": "2026-01-23T15:02:10Z"
}
}
}
```

Response Parameters

Parameter Name	Type & Value
id	String; Unique identifier for this ACL entry
ip	String; The whitelisted IP address
mask	Integer; Subnet mask in CIDR notation
trunk_sid	String; The trunk this ACL is associated with
date_updated	String; ISO 8601 timestamp when ACL was last updated

Delete Whitelisted IP

Removes an ACL (whitelisted IP) entry from the trunk.

Important: Whitelist entry id is passed as query param id (not /whitelisted-ips/\<id>).

HTTP Request

```
DELETE https://<your_api_key>:<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/whitelisted-ips?id=<whitelist_entry_id>
```

Example Request

```
curl -s -X DELETE "https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/whitelisted-ips?id=1153"
```

HTTP Response

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

Example Response

```
{
"request_id": "91dc982ca79846479c6f9678c788cfc1",
```

```
"method": "DELETE",
"http_code": 200,
"response":
{ "code": 200,
"error_data": null,
"status": "success",
"data":
{ "id": "1153",
"mask": 32,
"trunk_sid": "trmum1f70862263l150902801a1n",
"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; Deleted ACL entry id
ip	String; The IP that was removed
mask	Integer; Subnet mask that was configured
trunk_sid	String; The trunk this ACL belonged to

Update Destination URI

Updates load-balancing attributes (priority, weight) for an existing destination URI.

Important: \<destination_id> is the numeric id returned when you mapped the destination URI (e.g. 2543).

HTTP Request

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

Request Headers

Header	Value
Content-Type	application/json

Request Parameters

Parameter Name	Mandatory/Optional	Value
priority	Optional	Integer; Lower values = higher priority. Default: 0
weight	Optional	Integer; Higher values = more traffic. Default: 1

Example Request

```
curl -s -X PUT "https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/destination-uris/2543" \ -H "Content-Type:
application/json" \ -d '{ "priority": 0, "weight": 5 }'
```

HTTP Response

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

Example Response


```
{
"request_id": "63999f0a98a24a0aa58ab5b74aec9f0a",
"method": "PUT",
"http_code": 200,
"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": "2026-01-23T16:05:01Z",
"type": "public",
"priority": 0,
"weight": 5,
"trunk_sid": "trmum1f708622631150902801a1n"
}
}
}
```


Response Parameters

Parameter Name	Type & Value
id	String; Destination URI id
destination	String; The SIP URI
priority	Integer; Updated priority
weight	Integer; Updated weight
trunk_sid	String; The associated trunk
date_updated	String; ISO 8601 timestamp when destination was last updated

Delete Destination URI

Removes a destination URI from the trunk.

Important: Destination id is passed as query param id (not /destination-uris/\<id>).

HTTP Request

```
DELETE https://<your_api_key>:<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/destination-uris?id=<destination_id>
```

Example Request

```
curl -s -X DELETE "https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/destination-uris?id=2543"
```

HTTP Response

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

Example Response

```
{
"request_id": "bfc1544ab0ab4df3ae49173ccc744331",
"method": "DELETE",
"http_code": 200,
"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
id	String; Deleted destination URI id
destination	String; The SIP URI that was removed
trunk_sid	String; The trunk this destination belonged to

Update SIP Credential

Updates an existing SIP digest credential entry (rotate password, rename label, or change username).

Important: Credential id is in the **path** (/credentials/\<credential_id>), unlike Delete Credentials which uses query ?id=.

HTTP Request

```
PUT https://<your_api_key>:
```

```
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/credentials/<credential_id>
```

Request Headers

Header	Value
Content-Type	application/json

Request Parameters

Parameter Name	Mandatory/Optional	Value
user_name	Optional	String; New SIP digest username
password	Optional	String; New SIP digest password (use a strong secret)
friendly_name	Optional	String; Label to identify where the creds are used (max 32 chars)

Example Request

```
curl -s -X PUT "https://<your_api_key>:
<your_api_token>@<subdomain>/v2/accounts/<your_sid>/trunks/<trunk_sid>/credentials/1234" \ -H "Content-Type:
application/json" \ -d '{ "friendly_name": "elevenlabs_prod", "password": "replace_with_strong_password" }'
```

HTTP Response

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

Example Response


```
{
"request_id": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
"method": "PUT",
"http_code": 200,
"response":
{ "code": 200,
"error_data": null,
"status": "success",
"data": { "id": "1234",
"trunk_sid": "trmum17d8e9a37a3732ecbf91a3u",
"user_name": "voice_ai_user",
"friendly_name": "elevenlabs_prod",
"date_created": "2026-01-23T11:37:36Z",
"date_updated": "2026-01-23T16:20:00Z"
}
}
}
```


Response Parameters

Parameter Name	Type & Value
id	String; Credential entry id
trunk_sid	String; The associated trunk
user_name	String; SIP digest username
friendly_name	String or null; Optional label
date_updated	String; ISO 8601 timestamp when credential was last updated

List Trunk Settings

Retrieves settings configured on the trunk (for example trunk_external_alias / caller ID).

HTTP Request

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

Example Request

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

HTTP Response

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

Example Response


```
{
"request_id": "8ce98845365f43fd97c2f46df38438c6",
"method": "GET",
"http_code": 200,
"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
name	String; Setting name (e.g. trunk_external_alias)
value	String; Setting value (e.g. caller ID in E.164)
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

Delete Trunk Setting

Removes a trunk setting by name (for example clears the outbound caller ID alias).

Important: Setting key is passed as query param name.

HTTP Request

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

Query Parameters

Parameter Name	Mandatory/Optional	Value
name	Mandatory	String; Setting key to remove. Example: trunk_external_alias

Example Request

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

HTTP Response

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

Example Response


```
{
"request_id": "8ce98845365f43fd97c2f46df38438c6",
"method": "DELETE",
"http_code": 200,
"response":
{ "code": 200,
"error_data": null,
"status": "success",
"data":
{ "name": "trunk_external_alias",
"value": "+919876543210",
"trunk_sid": "trmum1f70862263115090280la1n",
"date_created": "2026-01-23T13:34:50Z",
"date_updated": "2026-01-23T13:34:50Z"
}
```

```
}
}
```

Response Parameters

Parameter Name	Type & Value
name	String; Deleted setting name
value	String; Value that was removed
trunk_sid	String; The associated trunk

1.4.8. Reference

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
List Trunks	GET	/v2/accounts/{sid}/trunks
Update Trunk	PUT	/v2/accounts/{sid}/trunks/{trunk_sid}
Delete Trunk	DELETE	/v2/accounts/{sid}/trunks?trunk_sid={trunk_sid}
Trunk Map Lookup	GET	/v2/accounts/{sid}/trunk-maps?exophone={number}
Map Phone Number	POST	/v2/accounts/{sid}/trunks/{trunk_sid}/phone-numbers
Get Phone Numbers	GET	/v2/accounts/{sid}/trunks/{trunk_sid}/phone-numbers
Update Phone Number Mode	PUT	/v2/accounts/{sid}/trunks/{trunk_sid}/phone-numbers/{id}
Delete Phone Number Mapping	DELETE	/v2/accounts/{sid}/trunks/{trunk_sid}/phone-numbers?id={id}
Map ACL	POST	/v2/accounts/{sid}/trunks/{trunk_sid}/whitelisted-ips
Get ACLs	GET	/v2/accounts/{sid}/trunks/{trunk_sid}/whitelisted-ips
Update Whitelisted IP	PUT	/v2/accounts/{sid}/trunks/{trunk_sid}/whitelisted-ips/{id}
Delete Whitelisted IP	DELETE	/v2/accounts/{sid}/trunks/{trunk_sid}/whitelisted-ips?id={id}
Create Credentials	POST	/v2/accounts/{sid}/trunks/{trunk_sid}/credentials
List Credentials	GET	/v2/accounts/{sid}/trunks/{trunk_sid}/credentials
Update Credentials	PUT	/v2/accounts/{sid}/trunks/{trunk_sid}/credentials/{id}
Delete Credentials	DELETE	/v2/accounts/{sid}/trunks/{trunk_sid}/credentials?id={id}
Map Destination URI	POST	/v2/accounts/{sid}/trunks/{trunk_sid}/destination-uris
Get Destination URIs	GET	/v2/accounts/{sid}/trunks/{trunk_sid}/destination-uris
Update Destination URI	PUT	/v2/accounts/{sid}/trunks/{trunk_sid}/destination-uris/{id}
Delete Destination URI	DELETE	/v2/accounts/{sid}/trunks/{trunk_sid}/destination-uris?id={id}
Set Trunk Alias	POST	/v2/accounts/{sid}/trunks/{trunk_sid}/settings
List Trunk Settings	GET	/v2/accounts/{sid}/trunks/{trunk_sid}/settings
Delete Trunk Setting	DELETE	/v2/accounts/{sid}/trunks/{trunk_sid}/settings?name={name}

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
98.130.5.99	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)

1.7. FAQs

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.

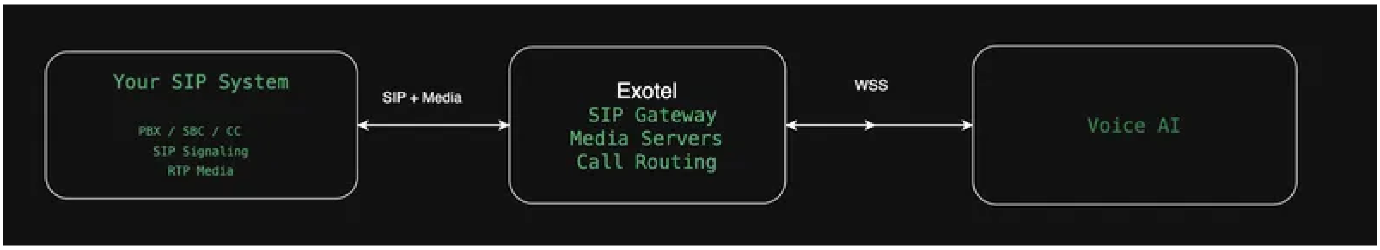
15. Which audio codec should I use in India?

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: 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
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>/whitelisted-
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>/whitelisted-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]

1.9. Connect Applet Setup for Inbound SIP Trunking

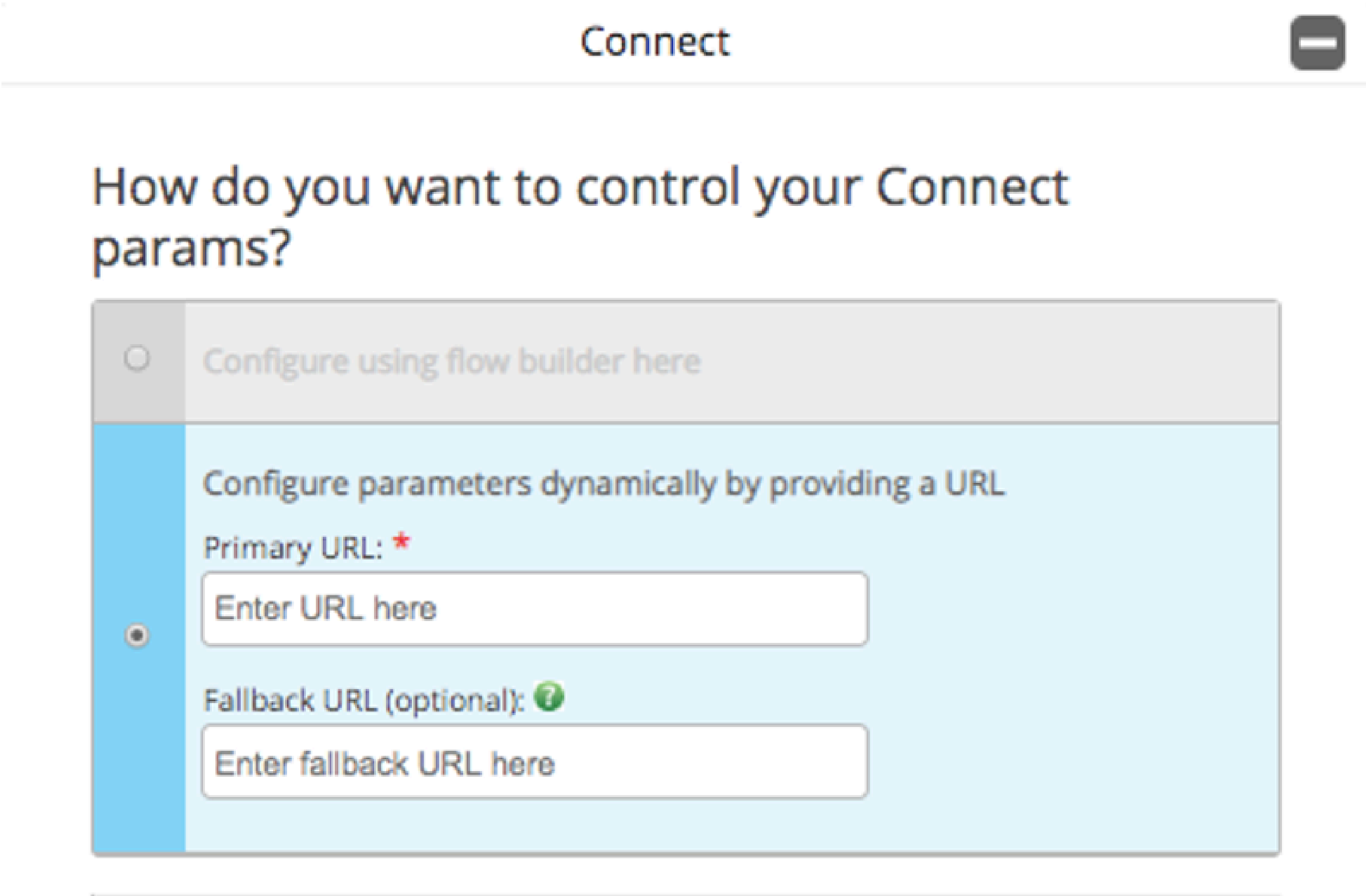
Connect Applet: Configuration, Dynamic URL, and Escalation via Passthru for Agent handover

Your System receive calls from PSTN

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

Overview

You can configure the Connect applet's parameters in one of two ways:



1. **Flow Builder** – set `sip:<TrunkID>` in the **Dial Whom** field parameters directly in the applet's UI.
2. **Dynamic URL** – control parameters at runtime via your own application endpoint.

Regardless of which method you choose, you must still configure the **transitions** (which applet runs next) while building the flow.

If you configure parameters dynamically, you set:

- A **Primary URL**, which handles the requests.
- An optional **Fallback URL**, contacted if something goes wrong with the Primary URL.

Request (Exotel → Your Application)

If an application URL is set for the Connect applet, Exotel makes a **GET** request to that URL with call details as URL-encoded HTTP query parameters. Only some parameters may be passed, depending on where the Connect applet sits in the flow.

Header

Header	Description
Exotel-Version	Version of Connect applet parameters against which your endpoint's response will be validated. Current version: 1.0.

Query Parameters

Parameter	Description
CallSid	Unique identifier of the call.
CallFrom	Outgoing call: number the call is made from. Incoming call: number the call is received from.
CallTo	Outgoing call: number being dialed out. Incoming call: number where the call landed.
Direction	incoming or outbound-dial.
Created	Timestamp when the call is created (yyyy-mm-dd hh:mm:ss).
DialCallDuration	Seconds from when the call is triggered to when the second leg ends (including conversation time). Can be 0 depending on the previous applet and if there's no second leg.
StartTime	Timestamp when the call started (yyyy-mm-dd hh:mm:ss).
EndTime	Constant value 1970-01-01 05:30:00 (Unix epoch). Use the Call Details API a few minutes after the call ends to get accurate end time.
CallType	See table below.
DialWhomNumber	Number of the agent who was dialed last.
flow_id	Flow ID associated with the call.
From	Incoming call: caller's number. Outgoing call: number of the first leg.
To	Incoming call: the ExoPhone the call came into. Outgoing call: the number dialed.
CurrentTime	Current server time (yyyy-mm-dd hh:mm:ss).

CallType values:

Scenario	Value
IVR only, no Connect applet	call-attempt
Call conversation happened	completed
Client hung up during Connect applet	client-hangup
Connect applet, no agent picked up	incomplete
Went to voicemail applet	voicemail

Conditional Parameters

Passed only if certain conditions are met:

Parameter	Description
DialCallStatus	What happened on the second leg if the previous applet was "Connect". Values: completed, busy, no-answer, failed, canceled.
digits	Passed if a Gather or IVR applet preceded this one; equals the digits entered. Note: comes wrapped in double quotes (") – trim them to get the actual digits.
CustomField	If the call was initiated via API, the value passed as CustomField in that API call.
RecordingUrl	Populated if the previous applet was "voicemail"; contains the voicemail recording URL. There may be a delay before it's accessible, depending on recording length.

Response (Your Application → Exotel)

This is what Exotel expects back from your GET request. It decides how Connect executes during the call to PSTN number

Response header: Content-Type: application/json

Sample response

JSON

```json
{
  "fetch_after_attempt": false,
  "destination": {
    "numbers": ["+919812345678"]
  },
  "outgoing_phone_number": "+918047115777",
  "record": true,
  "recording_channels": "dual",
  "max_ringing_duration": 45,
  "max_conversation_duration": 3600,
  "music_on_hold": {
    "type": "operator_tone"
  },
  "start_call_playback": {
    "playback_to": "both",
    "type": "text",
    "value": "This text would be spoken out to the callee"
  }
}
```

1. For custom routing to Inbound SIP trunk, use a **Dynamic URL** to fetch the destination URI and pass headers, as described above.
2. Up to 5 custom SIP headers are supported (e.g. X-param1=value1, max 4000 bytes total). Headers prefixed with Exotel- or Veeno- are reserved by the platform.

Connect Applet – Dynamic URL response example for SIP Transfer:

JSON

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

Response parameters

Parameter	Mandatory/Optional	Description
fetch_after_attempt	Optional; default false	Whether to re-fetch parameters (including destination numbers) after each unsuccessful dial attempt. false: dial happens based on the initial response only, no subsequent hits to the URL. true: Connect re-fetches parameters (hits the URL again) if a dial attempt fails. If two consecutive fetches return the exact same destination numbers, Exotel will not retry further even if this is true. Re-fetch request includes standard params plus <connect> params from previous dial attempts; response format is the same as above.
destination	Mandatory	The destination(s) to dial. See sub-parameters below.
destination.numbers	–	Array of E.164-format numbers to dial, in the order they appear. Example: "destination": {"numbers": ["+622131921111", "+622131921112"]}.
destination.trunk	–	Route the call to a SIP trunk instead of a number, e.g. "destination": {"trunk": "trunk-2134"}. Used for SIP Transfer to agents/contact centers (see Escalation via Passthru Applet below).
outgoing_phone_number	Optional; default = incoming ExoPhone	ExoPhone to dial out from (E.164 format). Must exist in your account. Subject to telecom circle/region restrictions (e.g., outgoing ExoPhone in Delhi can't be used if the incoming ExoPhone is in Bangalore). Both legs' ExoPhones can be on the same server. If the ExoPhone isn't in your account or fails validation, Exotel falls back to using the same ExoPhone as the first leg. Consult Exotel support before using this.
record	Optional; default false	Whether to record the call.
recording_channels	Optional; default single	single or dual (caller and callee in separate channels).
max_ringing_duration	Optional; default 30	Ringing duration limit, in seconds. Can be increased up to 60.
max_conversation_duration	Optional; default 900 (15 min)	Conversation duration limit, in seconds. Can be increased up to 4500 (75 min).
music_on_hold	Optional; default default_tone	default_tone (Exotel's default), operator_tone (audio returned by the operator on the dialing channel as-is), or custom_tone (audio URL provided in the response). Example: {"type": "custom_tone", "value": "<audio_url>"}.
parallel_ringing	Optional	Dial all destination numbers simultaneously: {"activate": true, "max_parallel_attempts": 5}. max_parallel_attempts range 1–10, default 5. Chargeable feature – confirm with your Account Manager or hello@exotel.in before use.

Parameter	Mandatory/Optional	Description
dial_passthru_event_url	Optional	URL requested for dial start and dial end events.
start_call_playback	Optional	Play a recording or TTS to the called number. playback_to: both or callee. type: audio_url or text. Example: {"playback_to": "both", "type": "text", "value": "hello, this is a sample text"}. Audio file requirements: 8 kHz sample rate, 16-bit depth, 128 kbps bit rate, mono channel, .wav format. If reusing the same audio_url filename, it will be cached by Exotel servers – use dynamic filenames if the audio content changes each time.
custom_params	Optional	Custom SIP headers passed with a trunk-routed call, e.g. "custom_params": "param1=value1&param2=value2". Up to 3 custom headers, max 200 bytes total. Headers prefixed with Exotel- or Veeno- are platform-reserved.

All of the above can also be set via the dashboard if you configure the Connect applet through the Flow Builder instead of a Dynamic URL.

Fallback URL triggers

The Fallback URL is called when:

- The Primary URL doesn't return HTTP 200 OK.
- The Primary URL doesn't respond within the timeout period (5 seconds).
- The Primary URL returns an invalid response:
  - Content-Type is not application/json.
  - Mandatory parameters are missing.
  - audio_url / text isn't a valid HTTP/HTTPS URL returning 200.

Transition to Next Applet

Set these transitions in the Flow Builder to decide what runs next:

References

- **Programmable Connect: Working with Connect Applet (Dynamic URL)**
- **Passthru Applet**

2. SIP Trunk Configuration

2.1. Overview

This article provides a complete overview of how enterprises can integrate with Exotel's SIP Trunking (SIP). It includes configuration options (TCP, TLS, FQDN), onboarding steps, best practices, and supported use cases.

1. What is Exotel SIP Trunking (SIP)?

Exotel SIP Trunking allows enterprise PBX/SBC systems to connect directly with Exotel's voice infrastructure using SIP over TCP or TLS. It supports both inbound and outbound PSTN calling through IP connectivity, with optional FQDN-based flexibility.

2. Supported Use Cases

Use Case	**Description**
Outbound SIP (IP → PSTN)	Calls from customer SIP infra routed to Exotel → PSTN
Inbound SIP (PSTN → IP)	Incoming calls to Exophone routed to customer SIP server
IP–PSTN Intermix	Bi-directional call routing between IP infra and Exotel VNs
SIP Bot Integration	Direct SIP-to-Bot integration with no agent involvement
FQDN-based Load Balanced SIP	FQDNs resolve dynamically to multiple IPs for cloud/hybrid setups
Native SIP Voicebot Integration	Direct SIP call to customer-hosted SIP-native voicebot platform

3. Transport Options

Transport	Port	Encryption	DNS Support	Use Case
TCP	5070	No	Yes	Default, legacy infra
TLS	443	Yes	Yes	Encrypted SIP + SRTP flows
FQDN	Any	TCP/TLS	Required	Cloud, autoscaling, HA SIP infra

4. Integration Path – High-Level Flow

What is Supported

- SIP Trunking with TCP and TLS transport
- SIP trunk routing using static IPs or FQDN
- Bi-directional call support (IP to PSTN and PSTN to IP)

- Exophones (Virtual Numbers) mapped to SIP trunks
- **SIP-to-Flow integration using Connect or IVR — See: SIP-to-Flow Integration Guide**
- **SIP-to-SIP integration for native voicebot routing — See: Native SIP Voicebot Integration Guide**

Note – vSIP Throttling

Exotel enforces a default vSIP rate-limit of 200 calls per minute (CPM) per trunk to safeguard carrier capacity and call quality.

If your traffic profile requires a higher burst rate, raise a request via your CSM or Support ticket. The capacity-planning team will review historical traffic, carrier limits, and QoS requirements and can increase the throttling threshold accordingly.

What is Not Supported

- SIP over UDP (not supported)
- SIP registration-based authentication
- SIP traffic without prior account upgrade/KYC

Supported Regional Exophones for MUM SIP Setup

- Veeno KA, DL, Mum, AP, GJ

Getting Started with Exotel vSIP (Veeno Accounts)

1. **Create your Exotel account** via my.in.exotel.com
2. **Complete KYC and upgrade the account** with help from your Exotel Account Manager: link
3. **Procure Exophones** by emailing hello@exotel.com (mention region-specific need)
4. **Decide trunking mode**: TCP or TLS, Static IP or FQDN
5. **Collect and share with Exotel**:
    - Account SID
    - Exophones
    - Trunk source IPs (for outbound trunking)
    - Trunk destination IPs/FQDN (for inbound trunking)
    - Chosen transport protocol (TCP/TLS)

Once provisioned, your SIP traffic will be routed via Exotel's regional edge PoP.

KYC Verification based on the setup required

Convert to Full Account – Exotel team upgrades it

Share Configuration Details:

- Account SID
- Exophones (required for PSTN origination)
- Source IP(s) (for outbound)
- Destination IP(s) or FQDN (for inbound)

- Transport type (TCP/TLS)

Provisioning:

- VOIP and VOIP-PSTN enabled
- SIP trunk created in backend by Tech Support
- Dial Whom URI format configured

Testing:

- Inbound and Outbound calls validated
- SIP packets reviewed using tools like sngrep

5. Configuration Types

a. TCP Trunking (Port 5070) – See: Exotel Exotel SIP Trunking TCP Integration Guide

- Uses format: sip:<number>@pstn.in4.exotel.com:5070;transport=tcp
- Requires static IP whitelisting

b. TLS Trunking (Port 443) – See: Exotel Exotel SIP Trunking TLS Integration Guide

- Uses format: sip:<number>@pstn.in4.exotel.com:443;transport=tls
- Encrypted SIP signaling and SRTP media
- Recommended for secure communication

c. FQDN-based Trunking – See: Exotel Exotel SIP Trunking FQDN Integration Guide

- No IP whitelisting required
- Uses DNS lookup to resolve SIP server IP dynamically
- Ideal for cloud or redundant infrastructure

6. FQDN Configuration Guidance

If you are using a DNS-resolvable FQDN instead of a static IP for your SIP server, please ensure the following:

- Your SIP server is accessible via a public FQDN (e.g., sip.customer.com)
- It resolves to an IP address reachable by Exotel
- Specify the port (e.g., 5070 for TCP or 443 for TLS) and transport protocol
- Share the FQDN, port, and transport protocol with your Exotel Account Manager

Exotel will configure the trunk to use your FQDN. This enables dynamic IP handling and is ideal for cloud-hosted or HA infrastructures.

Once this is provisioned, you can begin testing:

- Map your VN to the SIP trunk and initiate a test call
- Use tools like sngrep or tcpdump to validate INVITE requests and SRTP media flow
- In the Dial Whom field, use format: sip:<number>@<fqdn>:<port>;transport=tcp|tls

- Confirm the P-Asserted-Identity header shows the correct Leg1 number (caller identity)

7. Best Practices for vSIP Integration

- Use FQDN if infra is cloud-based, HA, or load-balanced
- Keep DNS TTL between 30–60 seconds for fast recovery
- Avoid SIP ALG in NAT/firewall appliances
- Use PCMA (G.711 A-law) as primary codec
- Use TLS + SRTP for security-sensitive traffic
- Validate trunk reachability before mapping VNs
- **Restrict RTP media port range to 10000–20000 (10K ports only)**
- Each SIP call uses 2 ports
- Exotel media servers support 3000 concurrent calls → 6000 ports
- A 50% buffer ensures capacity during retries, hold-ups, or port conflicts
- Helps avoid NAT-related media drops and ensures predictable firewall rules

8. Support Channels

Provisioning Support:

- Contact your Exotel CSM or email: hello@exotel.com

Technical Support:

- Visit: support.exotel.com
- Share the following:
  - Account SID
  - Trunk transport type (TCP/TLS/FQDN)
  - Sample Call SIDs
  - SIP trace logs (from sngrep/Wireshark)

2.2. Exotel SIP Trunking – TCP (India)

This article provides enterprise customers with technical steps to integrate Exotel's SIP Trunking (vSIP) with your PBX, SIP server, or SBC over TCP (Mumbai PoP). It outlines configuration practices, header formats, best practices, and validation techniques.

1. Product Overview

Exotel's SIP Trunking allows secure SIP-based PSTN call origination and termination between your SIP infrastructure and Exotel's platform using IP authentication.

2. Architecture

- Call Type: PSTN <-> SIP Gateway Interconnect
- Transport: SIP over TCP (Port 5070)
- Media: RTP over UDP (Ports 10000–40000)
- Authentication: IP Whitelisting (Registration-based auth not supported)
- Edge Location: Mumbai PoP (India)

Note – SIP Throttling

Exotel enforces a default SIP rate-limit of 200 calls per minute (CPM) per trunk to safeguard carrier capacity and call quality.

If your traffic profile requires a higher burst rate, raise a request via your CSM or Support ticket. The capacity-planning team will review historical traffic, carrier limits, and QoS requirements and can increase the throttling threshold accordingly.

3. Required Configuration

IP Whitelisting

- Your static public IP must be whitelisted by Exotel.
- Registration (SIP REGISTER) is not supported.

Ports to Open

Type	Port Range	Protocol	Purpose
Signaling	5070	TCP	SIP signaling
Media	10000–40000	UDP	RTP streams

SIP Domain and Proxy Details

Network & Firewall Configuration

Use this proxy for configuring Exotel as a peer/trunk on your SBC or PBX.

4. Sample Configuration – Asterisk PBX

```
[general]

externip = <your_public_ip>

localnet = 192.168.0.0/16

[exotelvsip]

type = friend

context = incoming

fromdomain = <accountsid>.pstn.exotel.com

host = pstn.in2.exotel.com

port = 5070

transport = tcp

disallow = all

allow = alaw

allow = ulaw

nat = force_rport

insecure = port

canreinvite = no

sendrpid = yes

trustrpid = yes

relaxdtmf = yes

transport=tcp
```

5: SIP Message Format

A. INVITE from Exotel Trunk (Exotel → Customer)

This is triggered when Exotel routes an inbound call to the customer SIP gateway over **TCP**.

Sample SIP INVITE

Sip

```
INVITE sip:+91XXXXXXXXXX@<customer-ip>:5061;transport=tcp SIP/2.0

Record-Route: sip:<exotel-ip>:443;transport=tls;lr

Via: SIP/2.0/TCP <exotel-ip>:443;branch=z9hG4bK2414...

From: "+91AAAAAAAAAA" <sip:+91AAAAAAAAAA@exotelt.pstn.exotel.com>;tag=as2aefddf2
```

```
To: <sip:+91XXXXXXXXXX@<customer-ip>>

Call-ID: <UUID>@pstn.mum1.exotel.com

CSeq: 102 INVITE

Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE

Supported: replaces

X-Exotel-LegSid: <leg-id>

X-Exotel-CallSid: <call-id>

X-Exotel-TrunkSid: <trunk-id>

P-Asserted-Identity: <sip:+91AAAAAAAAAA@exotelt.pstn.exotel.com>

P-Early-Media: supported

Contact: <sip:+91AAAAAAAAAA@<public-ip>:port;transport=tcp>

Content-Type: application/sdp

Content-Length: 1168

Max-Forwards: 67

v=0

o=root 1683048786 1683048786 IN IP4 <exotel-media-ip>

c=IN IP4 <exotel-media-ip>

t=0 0

m=audio 37456 RTP/AVP 8 0 96

a=rtpmap:8 PCMA/8000

a=rtpmap:0 PCMU/8000

a=rtpmap:96 telephone-event/8000

a=fmtp:96 0-15

a=sendrecv

a=rtcp:37457

a=ptime:20
```

Header Reference Table – INVITE from Exotel

Header	Mandatory	Description
Request URI	Yes	Destination SIP URI (Exophone mapped to customer SIP IP).
Via	Yes	Routing path for SIP responses. Uses TCP in this case.
Record-Route	Optional	Ensures Exotel remains in signaling path for subsequent requests.
From	Yes	Caller party number (CLI) received by Exotel (e.g., end-user).
To	Yes	Exophone provisioned by Exotel for this customer.
Call-ID	Yes	Unique identifier for the call.
CSeq	Yes	Command sequence number, must increment with each new transaction.
Allow	Yes	List of SIP methods supported by Exotel.
Supported	Optional	SIP extensions like replaces, timer.
X-Exotel-CallSid	Yes	Unique ID for the call session (tracking/debugging).
X-Exotel-LegSid	Optional	Call leg identifier; unique to this direction of the call.
X-Exotel-TrunkSid	Optional	Identifies which SIP trunk was used.
P-Asserted-Identity	Optional	Validated caller ID presented to customer SIP server.
P-Early-Media	Optional	Indicates support for early media before call is answered.
Contact	Optional	Where Exotel can be reached for further in-dialog SIP messages.
Content-Type	Yes	Indicates media description follows (SDP).
Content-Length	Yes	Length of the SDP body.
Max-Forwards	Yes	Prevents infinite loops by limiting hop count.
SDP (v=...)	Yes	Contains RTP setup: IP, codecs (PCMA/PCMU), RTP/DTMF, etc. (unencrypted RTP).

B. INVITE to Exotel Trunk (Customer → Exotel)

Customer initiates an outbound call over **TCP**, using a registered Exophone as the CLI and targeting any mobile/landline via Exotel.

Sample SIP INVITE

Sip

```
INVITE sip:+91YYYYYYYYYY@<exotel-ip>:5070 SIP/2.0

Via: SIP/2.0/TCP <customer-ip>:5061;branch=z9hG4bKbK4041f853

Max-Forwards: 70

From: "+91XXXXXXXXXX" <sip:+91XXXXXXXXXX@exotelt.pstn.exotel.com>;tag=as63e4d7f1

To: <sip:+91YYYYYYYYYY@<exotel-ip>>

Contact: <sip:+91XXXXXXXXXX@<customer-ip>:5061;transport=tcp>

Call-ID: <UUID>@exotelt.pstn.exotel.com
```

`CSeq: 102 INVITE`

`Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE`

`Supported: replaces, timer`

`Content-Type: application/sdp`

`Content-Length: 371`

`v=0`

`o=root 1002281923 1002281923 IN IP4 <customer-media-ip>`

`c=IN IP4 <customer-media-ip>`

`t=0 0`

`m=audio 18232 RTP/AVP 8 0 101`

`a=rtpmap:8 PCMA/8000`

`a=rtpmap:0 PCMU/8000`

`a=rtpmap:101 telephone-event/8000`

`a=fmtp:101 0-16`

`a=ptime:20`

`a=maxptime:150`

`a=sendrecv`

Header Reference Table – INVITE to Exotel

Header	Mandatory	Description
Request URI	Yes	Final destination number (callee) to be dialed via Exotel trunk.
Via	Yes	Describes how to return SIP responses to customer (over TCP).
From	Yes	CLI being used – must be a valid Exophone registered with Exotel.
To	Yes	Destination number (callee, Called Party Number); not used for routing.
Call-ID	Yes	Unique identifier for the call session.
CSeq	Yes	SIP sequence number and method (e.g., INVITE).
Contact	Optional	Where Exotel can reach back for in-dialog requests.
Allow	Yes	Methods supported by customer.
Supported	Optional	SIP extensions.
Content-Type	Yes	MIME type of message body (SDP).
Content-Length	Yes	Byte length of SDP content.
Max-Forwards	Yes	Used to control and limit SIP hops.
SDP (v=...)	Yes	Media negotiation block, including codecs and ports. RTP only (unencrypted).

Recap – CLI & Exophone Roles

Direction	From (CLI)	Request URI (Destination)	Notes
Exotel → You	Customer's end-user CLI	Your SIP URI (Exophone)	Used in inbound flows to your system
You → Exotel	Your Exophone (CLI)	Final user number to dial	Must use registered CLI in From, else call will be rejected

6. Best Practices and Pre-checks

Before Configuration

- Confirm you have a static public IP with no CG-NAT or port masking.
- Make sure your firewall allows TCP 5070 and UDP 10000–40000 bidirectionally.
- Validate that your PBX/SBC supports SIP over TCP and G.711 codecs (PCMA/PCMU).

During Configuration

- Prefer PCMA as the first codec in media negotiations; PCMU as fallback.
- Disable registration and use static peer trunking.
- Use nat=force_rport for NAT traversal if behind a firewall.
- Monitor and log Call-ID, X-Exotel-* headers for debugging.

After Configuration

- Run test calls and inspect SIP INVITEs and RTP.

- Monitor audio quality, latency, and early media (ringback).
- Use tcpdump or sngrep to validate SIP dialogues and media ports.

Quick sanity checks

1. **Transport match** – your Via: …;transport=tcp must align with port **5070**.
2. **Caller-ID hygiene** – the **From:** number in your outbound INVITE must be an authorised CLI/Exophone.
3. **Log Exotel headers** – X-Exotel-CallSid, LegSid, TrunkSid are read-only but invaluable for troubleshooting.

7. How to Test Your Setup

Inbound Test (Exotel → Your SIP Server)

- Trigger a call to your Exotel VN mapped to the SIP trunk.
- Check if your server receives an INVITE from pstn.in2.exotel.com.
- Confirm RTP is flowing from 182.76.143.61 or 122.15.8.184.

Outbound Test (Your Server → Exotel)

- Send a SIP INVITE to pstn.in2.exotel.com:5070 with the To URI set to a valid destination (e.g., mobile number).
- Ensure correct formatting of headers and the contact field.
- Look for 100/180/200 OK responses and RTP flow.

8. Troubleshooting Tips

Issue	Potential Cause	Resolution
No INVITE received	IP not whitelisted	Contact Exotel to confirm IP ACL
Call drops in 30s	NAT binding lost	Enable symmetric RTP / force_rport
One-way audio	Media ports blocked	Open UDP 10000–40000
403 Forbidden	Incorrect domain or auth	Use correct fromdomain and no auth creds

9. Support and Next Steps

This guide covers Exotel vSIP over TCP via the Mumbai PoP.

For support:

- Contact your Exotel account manager.
- Or raise a ticket via https://support.exotel.com with:
  - Account SID
  - Call time and number
  - SIP trace logs (.pcap or .txt)

2.3. Exotel SIP Trunking – TLS (India)

This article provides technical integration steps for enterprise customers setting up Exotel's SIP Trunking (vSIP) over TLS via the Mumbai PoP. It includes configuration guidelines, SIP headers, and best practices for secure SIP-based PSTN interconnects.

1. Product Overview

Exotel's SIP Trunking over TLS enables secure, encrypted PSTN call origination and termination between your SIP infrastructure and Exotel's platform.

2. Architecture

- Call Type: PSTN <-> SIP Gateway Interconnect
- Transport: SIP over TLS (Port 443)
- Media: Secure RTP (SRTP) over UDP (Ports 10000–40000)
- Authentication: IP Whitelisting (no SIP registration)
- Edge Location: Mumbai PoP (India)

Note – SIP Throttling

Exotel enforces a default vSIP rate-limit of 200 calls per minute (CPM) per trunk to safeguard carrier capacity and call quality.

If your traffic profile requires a higher burst rate, raise a request via your CSM or Support ticket. The capacity-planning team will review historical traffic, carrier limits, and QoS requirements and can increase the throttling threshold accordingly.

3. Required Configuration

IP Whitelisting

- Provide your static public IP to Exotel for ACL entry.
- Dynamic IPs or NAT setups are not recommended.

Ports to Open

Type	Port Range	Protocol	Purpose
Signaling	443	TCP	SIP over TLS
Media	10000–40000	UDP	SRTP streams

SIP Domain and Proxy Details

Network & Firewall Configuration

Use this FQDN in your trunk peer setup.

4. Sample Configuration – Asterisk PBX

[general]

`externip = <your_public_ip>`

`localnet = 192.168.0.0/16`

`[exotelvsip]`

`type = friend`

`context = incoming`

`fromdomain = <accountsid>.pstn.exotel.com`

`host = pstn.in2.exotel.com`

`port = 443`

`transport = tls`

`disallow = all`

`allow = alaw`

`allow = ulaw`

`nat = force_rport`

`insecure = port`

`canreinvite = no`

`sendrpid = yes`

`trustrpid = yes`

`relaxdtmf = yes`

`encryption = yes`

5. SIP Message Format

A. INVITE from Exotel Trunk (Exotel → Customer)

When a customer receives an inbound call from Exotel over **TLS**, Exotel uses the customer's SIP URI as the request URI and includes customer CLI, Exophone, and media parameters securely.

SIP INVITE Examples

Inbound INVITE (Exotel → Customer)

`INVITE sip:+91XXXXXXXXXX@<customer-ip>:5061;transport=tls SIP/2.0`

`Record-Route: sip:<exotel-ip>:443;transport=tls;lr`

```
Via: SIP/2.0/TLS <exotel-ip>:443;branch=z9hG4bK2414...

From: "+91AAAAAAAAAA" <sip:+91AAAAAAAAAA@exotelt.pstn.exotel.com>;tag=as2aefddf2

To: <sip:+91XXXXXXXXXX@<customer-ip>>

Call-ID: <UUID>@pstn.mum1.exotel.com

CSeq: 102 INVITE

Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE

Supported: replaces

X-Exotel-LegSid: <leg-id>

X-Exotel-CallSid: <call-id>

X-Exotel-TrunkSid: <trunk-id>

P-Asserted-Identity: <sip:+91AAAAAAAAAA@exotelt.pstn.exotel.com>

P-Early-Media: supported

Contact: <sip:+91AAAAAAAAAA@<public-ip>:port;transport=tls>

Content-Type: application/sdp

Content-Length: 1168

Max-Forwards: 67

v=0

o=root 1683048786 1683048786 IN IP4 <exotel-media-ip>

c=IN IP4 <exotel-media-ip>

t=0 0

m=audio 37456 RTP/SAVP 8 0 96

a=rtpmap:8 PCMA/8000

a=rtpmap:0 PCMU/8000

a=rtpmap:96 telephone-event/8000

a=fmtp:96 0-15

a=sendrecv

a=rtcp:37457

a=ptime:20

a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:<srtp-key>
```

Header Reference Table – INVITE from Exotel

Header	Mandatory	Description
Request URI	Yes	Destination SIP URI (customer Exophone)
From	Yes	Caller CLI shown to customer – e.g., original end-user number
To	Yes	Exophone provisioned in Exotel system
X-Exotel-CallSid	Yes	Unique identifier for this call session
X-Exotel-LegSid	Optional	Unique identifier for this leg of the call
X-Exotel-TrunkSid	Optional	Exotel trunk ID through which the call is routed
P-Asserted-Identity	Optional	Caller ID verification (especially for CLI masking)
Contact	Optional	Contact URI of SIP UA for future dialog messages
Content-Type / SDP	Yes	Contains secure media negotiation (RTP/SAVP with crypto key)

B. INVITE to Exotel Trunk (Customer → Exotel)

This message is used when the customer initiates a secure outbound call using their Exophone as CLI. TLS is used for SIP signalling, and SRTP for media encryption.

Outbound INVITE (Customer → Exotel)

```
INVITE sip:+91YYYYYYYYYY@<exotel-ip>:5070 SIP/2.0

Via: SIP/2.0/TLS <customer-ip>:5061;branch=z9hG4bKbK4041f853

Max-Forwards: 70

From: "+91XXXXXXXXXX" <sip:+91XXXXXXXXXX@exotelt.pstn.exotel.com>;tag=as63e4d7f1

To: <sip:+91YYYYYYYYYY@<exotel-ip>>

Contact: <sip:+91XXXXXXXXXX@<customer-ip>:5061;transport=tls>

Call-ID: <UUID>@exotelt.pstn.exotel.com

CSeq: 102 INVITE

Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE

Supported: replaces, timer

Content-Type: application/sdp

Content-Length: 371

v=0

o=root 1002281923 1002281923 IN IP4 <customer-media-ip>

c=IN IP4 <customer-media-ip>

t=0 0
```

```
m=audio 18232 RTP/SAVP 8 0 101
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=maxptime:150
a=sendrecv
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:<srtp-key>
```

Header Reference Table – INVITE to Exotel

Header	Mandatory	Description
Request URI	Yes	Number to be dialed (callee) via Exotel's SIP IP
From	Yes	CLI of customer (must be Exophone registered with Exotel)
To	Yes	Callee number (may not affect routing)
Contact	Optional	Customer's contact URI for SIP dialog continuation
Call-ID	Yes	Unique SIP session ID from the customer's SIP server
CSeq	Yes	Command sequence used in SIP transactions
Allow	Yes	Supported SIP verbs
Supported	Optional	SIP extensions like replaces, timer
Content-Type / SDP	Yes	Secure media parameters, codecs, ports, and SRTP crypto key (RTP/SAVP)

Key Identity Fields

Direction	Caller ID (CLI) in From	Called Number in Request URI	Comment
Exotel → Customer	Customer’s CLI (real caller)	Exophone assigned to the customer	CLI → customer via Exotel trunk
Customer → Exotel	Exophone (as CLI)	Final user’s number	Exotel uses From to verify CLI

6. Best Practices and Pre-checks

- Use only static IPs and TLS-compliant SBCs.
- Validate G.711 codec support with PCMA as preferred.
- Confirm SRTP support and crypto attribute handling in your SIP stack.

- Avoid SIP ALG or NAT devices without explicit RTP pinholes.

7. How to Test Your Setup

Inbound Test (Exotel → Your SIP Server)

- Map a VN to your SIP trunk in the dashboard.
- Dial the VN and capture traffic via sngrep or tcpdump.
- Confirm receipt of TLS INVITE and correct SRTP flow.

Outbound Test (Your SIP Server → Exotel)

- Initiate SIP INVITE to pstn.in2.exotel.com:443.
- Confirm 200 OK with SRTP attributes negotiated.
- Check the RTP/SAVP audio path and Exotel response headers.

8. Troubleshooting Tips

Issue	Cause	Solution
No INVITE received	IP not whitelisted	Confirm ACL entry with Exotel support
403 Forbidden	Wrong domain or auth config	Check the fromdomain and peer trunk settings
Call drops in 30s	RTP timeout or NAT	Enable symmetric RTP / force_rport
No audio	SRTP failure or media block	Confirm UDP 10000–40000 and SRTP config

9. Support and Next Steps

This guide documents Exotel vSIP over TLS via Mumbai PoP.

For support:

- Contact your Exotel account manager.
- Or file a ticket via https://support.exotel.com with:
  - Account SID
  - Timestamp of test
  - SIP trace logs (.pcap or raw headers)

2.4. Exotel SIP Trunking to Flow Integration Guide

This guide outlines how to integrate Exotel's SIP Trunking (vSIP) with your voice application flow (e.g., IVR or agent connect) using SIP signaling. It focuses on the use case of routing **inbound SIP calls from external SIP systems into Exotel Flow Applets**

1. Use Case: External SIP System to Exotel Flow

This guide is meant for customers who:

- Host their own SIP PBX or Bot Platform.
- Want to initiate SIP calls into Exotel to trigger flows (like Connect or IVR).
- Require SIP-over-TLS or TCP transport.

Example Scenarios

Scenario	Description
SIP Bot to Exotel Flow	External SIP bot initiates call to Exotel VN → Exotel triggers IVR flow
SIP PBX to Exotel Flow	SIP endpoint dials into Exotel Flow for agent routing or IVR processing
Regional SIP → Flow (cross-border PoP)	Enterprise infra routes call to Exotel PoP (SG/Mum/KA) for flow handling

2. SIP Integration Requirements

What You Need to Share with Exotel

- Account SID
- Exophone (VN) that should route to flow
- Source IP or FQDN from where SIP INVITE will originate
- Transport type (TCP/TLS)

Note – vSIP Throttling

Exotel enforces a default vSIP rate-limit of 200 calls per minute (CPM) per trunk to safeguard carrier capacity and call quality.

If your traffic profile requires a higher burst rate, raise a request via your CSM or Support ticket. The capacity-planning team will review historical traffic, carrier limits, and QoS requirements and can increase the throttling threshold accordingly.

What Exotel Will Do

- Provision SIP trunk mapping on the VN
- Route incoming INVITE on SIP trunk to your assigned Flow (via Connect Applet)

3. SIP Configuration Reference (Customer Side)

Here is an Asterisk-style example for TLS:

[general]

```
externip = <your_public_ip>

localnet = 192.168.0.0/16

[exotelvsip]

type = friend

context = outgoing

fromdomain = <accountsid>.pstn.exotel.com

host = pstn.sgp1.exotel.com

port = 443

transport = tls

disallow = all

allow = ulaw

allow = alaw

nat = force_rport

insecure = port

canreinvite = no

sendrpid = yes

trustrpid = yes

relaxdtmf = yes

encryption = yes
```

Ports to Open

Type	Port	Protocol	Description
SIP	443 / 5070	TLS/TCP	SIP signaling
RTP Media	10000-40000	UDP	Media/audio ports

4. Sample SIP INVITE to Exotel (Flow Integration)

Sip

```
INVITE sip:+91XXXXXXXXXX@pstn.sgp1.exotel.com SIP/2.0

Via: SIP/2.0/TLS your-sbc.domain.com:5061;branch=z9hG4bK4041f853

From: "+91YYYYYYYYYY" <sip:+91YYYYYYYYYY@exotelt.pstn.exotel.com>;tag=as63e4d7f1

To: <sip:+91XXXXXXXXXX@pstn.sgp1.exotel.com>
```

`Call-ID: abcdef1234567890@exotelt.pstn.exotel.com`

`CSeq: 102 INVITE`

`Contact: sip:+91YYYYYYYYYY@your-sbc.domain.com:5061;transport=tls`

`Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE`

`Supported: replaces, timer`

`X-Exotel-AccountSid: exotelt`

`Content-Type: application/sdp`

Header Reference – SIP INVITE to Exotel (Flow Integration)

Header	Mandatory	Example (Redacted)	Description
Request URI	Yes	sip:+91XXXXXXXXXX@pstn.in2.exotel.com	Target Exophone (VN) to route the call into a Flow or PSTN leg.
X-Exotel-AccountSid	Yes	Exxxxxx	Identifies your Exotel account. Required for Flow integration.(Tenant name)
Via	Yes	SIP/2.0/TLS your-sbc.domain.com:5061	Your SBC's transport, used by Exotel to route responses.
From	Yes	"Sales" <sip:+91YYYYYYYYYY@customer.com>	CLI of Customer(Callee)
To	Yes	<sip:+91XXXXXXXXXX@pstn.in2.exotel.com>	Exophone
Contact	Yes	<sip:+91YYYYYYYYYY@your-sbc.domain.com:5061>	Your contact URI for Exotel to send 200 OK, BYE, and other dialog messages.
Call-ID	Yes	abc123xyz@your-sbc	Unique identifier for SIP session; echoed in Exotel response.
CSeq	Yes	102 INVITE	SIP sequence number.
Max-Forwards	Yes	70	Prevents SIP loops by limiting hops.
Supported	Optional	replaces, timer	Advertises SIP extensions your UA supports.
Allow	Optional	INVITE, ACK, BYE, CANCEL, OPTIONS	SIP methods your SBC is willing to process.
Content-Type	Yes	application/sdp	Indicates the message contains SDP for media negotiation.

Important Notes

- Only use **X-Exotel-AccountSid** for Flow routing. This is essential for Exotel to associate the call with the correct Flow.
- Do **not** add X-Exotel-CallSid, X-Exotel-LegSid, or X-Exotel-TrunkSid. These headers are auto-injected by Exotel in the inbound leg.
- Ensure your SIP infrastructure handles:

  - G.711 PCMA (preferred codec)
  - SIP over TLS (port 443)
  - SRTP if TLS is enabled

5. Edge PoPs and IPs to Whitelist

Network & Firewall Configuration

6. Testing Steps

- Place a SIP INVITE to the Exophone you've been assigned.
- Confirm that the call lands in the expected flow (e.g., Connect applet rings agent).
- Use sngrep, sip set debug on, or Wireshark to validate SIP path.
- Ensure RTP is established from your system to Exotel's media IP.

7. Best Practices

- Ensure Exophone is mapped to a live flow before testing.
- Always share your SIP signaling IP/FQDN and transport in advance.
- Prefer PCMA (G.711 A-law) for better regional PSTN compatibility.
- Use TLS transport when possible to ensure encryption and SRTP.
- Confirm DNS resolves FQDN correctly if not using static IP.

8. Support

- Contact your Exotel Account Manager with:
  - Account SID
  - Flow/Exophone ID
  - SIP signaling IP or FQDN
  - Preferred Transport (TCP or TLS)
- Technical Help:
  - support.exotel.com
  - Share call samples and SIP logs for troubleshooting

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

1. Background & Objective

Voice AI and Contact Center (CC) platforms often operate robust SIP-based (vSIP) infrastructures for AI-led and agent-assisted conversations. However, they typically lack direct access to India's PSTN (landline and mobile networks) due to licensing and regulatory restrictions.

Exotel, operating as a Unified License (UL) Virtual Network Operator (VNO), bridges this gap by offering compliant PSTN ingress/egress via its SIP Trunking solution.

Objective:
To provide a plug-and-play, regulatory-compliant PSTN connectivity layer for both Voice AI and CC platforms without disrupting their current SIP infrastructure, bot orchestration logic, or agent workflow.

- Enable Voice AI and Contact Center platforms to access Indian PSTN via Exotel's UL VNO.
- Provide a plug-and-play SIP trunking layer without disrupting existing bot or agent logic.
- Support both inbound and outbound PSTN call flows using Exotel's vSIP infrastructure.
- Streamline onboarding via APIs for trunk creation, DID mapping, and IP whitelisting.

This solution is ideal for:

- Voice AI platforms using SIP-based infrastructure (e.g., FreeSWITCH, Kamailio, Asterisk, custom SBCs)
- Contact Center platforms with on-prem or cloud SIP setups requiring PSTN termination or origination
- Companies seeking elastic and compliant PSTN connectivity without managing telco licensing
- AI-led and hybrid inbound/outbound voice workflows

2. Solution Overview

2.1 Architecture

- **Partner Side**: Existing vSIP Endpoint / SBC / PBX (Voice AI or CC layer)
- **Exotel Side**: UL VNO SIP Gateway connected to Indian PSTN via multiple telcos

Connectivity Options:

- Public Internet (default)
- MPLS or VPN (optional for BFSI/secure deployments; contact CSM)

Media: RTP/SRTP, supporting PCMA (G.711 A-law) and PCMU (G.711 μ-law)
Signaling: SIP over TCP or TLS

Call Flow:

1. **Outbound**: Partner SBC sends SIP INVITE (only from static IP) → Exotel SIP Gateway → Indian PSTN → Customer Phone
2. **Inbound**: PSTN Call → Exotel DID → SIP INVITE (from static IP or FQDN) to Partner SBC (for bot or agent)

Exotel SIP Trunking – TCP Integration Guide

Exotel SIP Trunking – TLS Integration Guide

2.2 Key Capabilities

- Dynamic Channel Allocation for scale management
- Multi-Telco Failover with 100% connectivity SLA
- DID Management: Purchase & KYC compliant with Indian regulations
- Secure Interconnects: IP whitelisting, TLS support
- Regulatory Compliance: SDCA mapping, lawful interception readiness

Exotel SIP Trunking – To-Flow Guide

3. Onboarding & Integration

3.1 Exotel Account Setup & KYC

1. **Create Account** – **Sign up on Exotel** and select **Browser Calling** during setup
2. **Complete KYC/CAF** – Upload KYC Documents

3.2 SIP Trunk Enablement

1. **Enable SIP Trunking** – Email hello@exotel.com to activate trunking & provision a Virtual Number/Exophone
2. **Retrieve API Credentials** – Visit API Settings to get account_sid, key, and token

To configure silence ring or remove ring duration, contact your Exotel CSM or email hello@exotel.com

3.3 Trunk Configuration via API

Use:

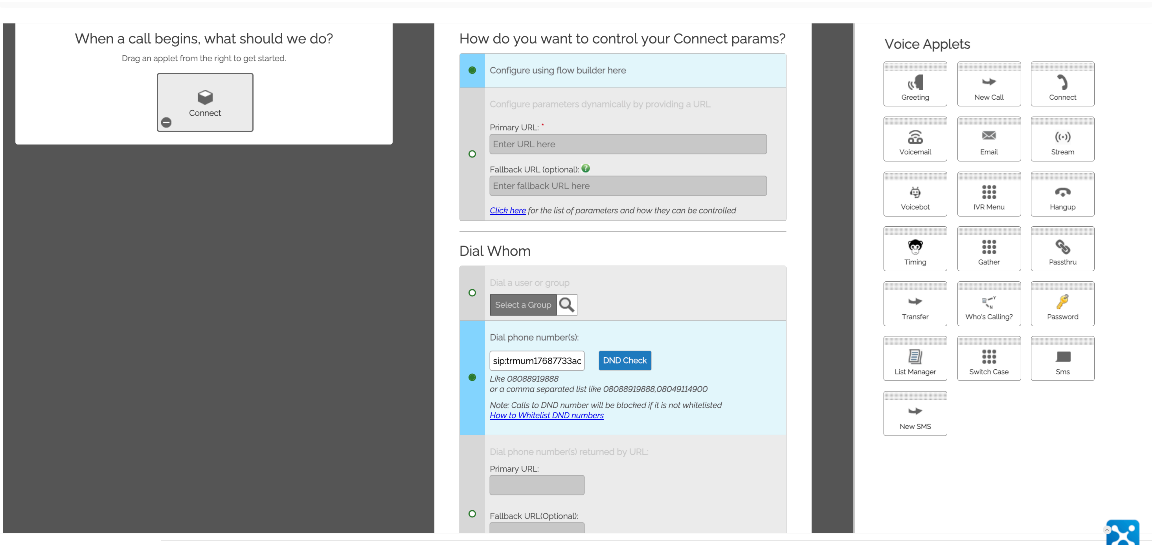
- **GitHub Repo**
- **Postman Collection**

API Steps:

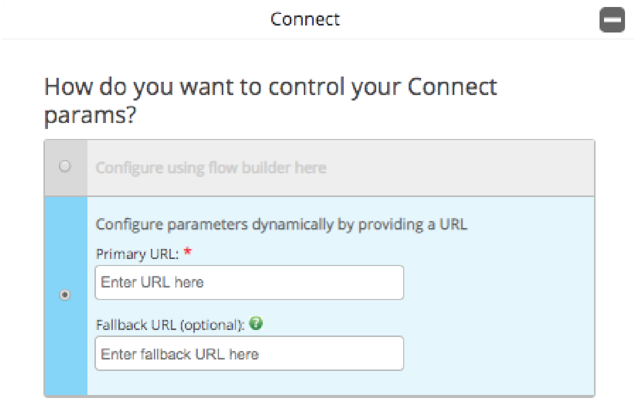
- `Create Trunk (/trunks)`
- `Map DIDs (/trunks/{trunk_sid}/phone-numbers)`
- `Whitelist IPs (/trunks/{trunk_sid}/whitelisted-ips)`
- `Add Destination URIs ( TCP, TLS)`
- Set trunk_external_alias for VN-FQDN mapping if required (for VAPI, LiveKit,OpenAI etc.)

4. Inbound Call Setup (PSTN → SIP Platform)

- Create a Flow using **Connect Applet** in App Bazaar
- Use `sip:<TrunkID>` in the **Dial Whom** field



- For custom routing, use a Dynamic URL to fetch destination URI and pass headers



- 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"
}
```

Reference: Connect Applet – Dynamic URL

5. Outbound Call Setup (Platform → PSTN)

5.1 Static IP Setup

- Request IP whitelisting via Exotel Support or use above repo to get it done.
- Once approved, initiate SIP outbound calls to Indian PSTN

5.2 FQDN-based Setup (API-triggered)

- Configure trunk destination via API (only for FQDN-based use cases)
- Use Click-to-Call API or Connect Customer to Flow API
- Set destination as sip:<TrunkID> in Connect Applet

6. Voicebot to Agent Handoff (SIP Flow)

Flow:

- Voicebot runs on Connect Applet over vSIP
- Bot disconnects → Flow moves to Passthru Applet → calls webhook
- Webhook Response:
  - 200 OK: Route to Connect Applet (agent group or SIP trunk)
  - 302/404: Move to Hangup Applet

Example:

`User says “Talk to human” → Bot ends → Passthru Applet → webhook (200 OK) → SwitchCase → Connect Applet (sip:<TrunkID>)`

7. Benefits for Voice AI and CC Platforms

- Plug-and-play PSTN access via Exotel’s UL VNO
- Elastic scaling with dynamic channel allocation
- Regulatory assurance with lawful interception readiness
- TLS security for sensitive verticals
- Real-time programmable call routing

8. Example Use Cases

- AI-led outbound campaigns (sales/NPS)
- Inbound IVR bots or reception assistants
- Agent-bot hybrid support models
- KYC calls and OTP verification for BFSI
- Order confirmations and fraud checks for e-commerce

9. Next Steps

- Share SIP endpoint details: IP/FQDN, transport type, supported codecs
- Exotel team initiates CAF/KYC validation

- Integration testing with live traffic
- Commercial onboarding & production go-live

2.6. Exotel Virtual SIP Trunking – FQDN-based

This support article explains how to configure Exotel's Virtual SIP Trunking (vSIP) using Fully Qualified Domain Name (FQDN) based trunking instead of fixed IPs. It details how the FQDN-based approach works, when it should be used, and why it offers benefits in enterprise-grade SIP deployments.

1. Product Overview

Exotel's FQDN-based Virtual SIP Trunking allows customers to use DNS-resolvable hostnames (e.g., trunk.customer.com) instead of static IPs to establish SIP trunking with Exotel's PoPs. This method enables greater flexibility and reliability, especially for deployments on cloud infrastructure or load-balanced SIP setups.

2. What is an FQDN-based Trunk?

An FQDN (Fully Qualified Domain Name) is a domain name that maps dynamically to one or more IPs. In this model:

- Your SIP gateway/SBC is reachable via a DNS-resolvable FQDN
- Exotel performs DNS resolution during SIP call setup
- No static IP whitelisting is required from customer side

Exotel supports both **static FQDN** and **dynamic DNS-based FQDN** approaches.

3. When to Use FQDN Instead of Static IP

Scenario	Recommendation
SIP infra hosted on cloud (AWS, Azure, GCP)	Use FQDN
Customer SBC has load balancer or HA proxy	Use FQDN
IP addresses change due to autoscaling/load shifting	Use FQDN
On-prem setup with fixed static IPs	Use static IP

FQDN is best suited when your IP address is not guaranteed to remain fixed or you have redundant/public-facing SIP endpoints.

4. How It Works

1. Customer provides an FQDN that resolves to their SBC/public SIP gateway.
2. Exotel adds this FQDN in the trunk configuration.
3. During each SIP call, Exotel queries DNS to resolve the IP.
4. Call is routed based on the returned A/AAAA record(s).

Note: Exotel performs DNS resolution on each call attempt to support failover and dynamic environments.

Note – vSIP Throttling

Exotel enforces a default vSIP rate-limit of 200 calls per minute (CPM) per trunk to safeguard carrier capacity and call quality.

If your traffic profile requires a higher burst rate, raise a request via your CSM or Support ticket. The capacity-planning team will review historical traffic, carrier limits, and QoS requirements and can increase the throttling threshold accordingly.

5. Configuration Requirements

On Customer Side

- Expose SIP server using a public FQDN (e.g., sip.companydomain.com)
- Ensure DNS A or AAAA records point to valid, routable IP(s)
- SIP server must be reachable on TCP or TLS as applicable
- Support G.711 codecs and standard RTP port ranges

On Exotel Side (done by Exotel Ops)

- Default:Trunk is configured with FQDN instead of IP
- Default:DNS lookups are enabled in trunk routing logic
- Default:Media IP range is kept open as per standard PoP setup

6. SIP Trunk Parameters (via FQDN)

Sample Configuration (Asterisk)

[general]

```
externip = <your_public_ip>

localnet = 192.168.0.0/16

[exotelvsip-fqdn]

type = friend

context = incoming

fromdomain = <accountsid>.pstn.exotel.com

host = sip.customerdomain.com

port = 5070 ; or 443 for TLS

transport = tcp ; or tls if using encrypted trunk

disallow = all

allow = alaw

allow = ulaw

nat = force_rport

insecure = port

canreinvite = no
```

`sendrpid = yes`

`trustrpid = yes`

`relaxdtmf = yes`

`encryption = yes ; only if using TLS with SRTP`

SIP Parameters Summary

Parameter	Example
SIP Peer FQDN	sip.customerdomain.com
Port	5070 (TCP) / 443 (TLS)
Transport	TCP or TLS
Media IP Range	10000–40000 (UDP)
DNS Record Type	A (IPv4) / AAAA (IPv6)

Parameter	Example
SIP Peer FQDN	sip.customerdomain.com
Port	5070 (TCP) / 443 (TLS)
Transport	TCP or TLS
Media IP Range	10000–40000 (UDP)
DNS Record Type	A (IPv4) / AAAA (IPv6)

7. Advantages of FQDN-based Approach

- **No need for IP whitelisting**: Reduces manual ACL changes
- **Supports redundancy**: Load balancer IPs can be rotated behind the same FQDN
- **Cloud-friendly**: Ideal for cloud-native SIP deployments
- **Failover-friendly**: Multiple A-records supported for active/passive routing

8. Best Practices

- TTL for DNS entries should be low (e.g., 30s–60s) for fast failover
- Use reliable DNS hosting with high availability
- Ensure SIP firewall rules allow calls from Exotel media IPs
- Avoid using CNAME records for SIP endpoints (use A/AAAA directly)

8.1 SIP Message Format and Header Behavior

SIP Message Format (FQDN Mode – TCP Transport)

A. INVITE from Exotel to Customer via FQDN (Inbound)

This is how Exotel delivers a call to your SBC or PBX using a **public DNS hostname** instead of a static IP.

Sample INVITE (Inbound via FQDN)

Sip

```
INVITE sip:+91XXXXXXXXXX@sip.customer.com:5070;transport=tcp SIP/2.0

Via: SIP/2.0/TCP pstn.in2.exotel.com;branch=...

From: "+91AAAAAAAAAA" <sip:+91AAAAAAAAAA@exotelt.pstn.exotel.com>

To: sip:+91XXXXXXXXXX@sip.customer.com

Call-ID: abcd1234efgh@pstn.mum1.exotel.com

CSeq: 102 INVITE

Contact: sip:+91AAAAAAAAAA@<exotel-media-ip>:port;transport=tcp

X-Exotel-CallSid: <auto-generated-by-exotel>

X-Exotel-LegSid: <leg-id>

X-Exotel-TrunkSid: <trunk-id>

P-Asserted-Identity: sip:+91AAAAAAAAAA@pstn.in2.exotel.com

P-Early-Media: supported

Content-Type: application/sdp

Content-Length: ...
```

Inbound SIP Header Reference (Exotel → Customer via FQDN)

Header	Mandatory	Description
Request URI	Yes	Your registered Exophone and SIP FQDN
Via	Yes	Exotel's signaling IP + transport (TCP)
From	Yes	Caller CLI (could be real, masked, or Exophone)
To	Yes	Your PBX's FQDN URI target
Call-ID	Yes	Dialog identifier for SIP trace correlation
CSeq	Yes	Command sequence, starts with INVITE
Contact	Yes	Exotel's signaling contact (for BYE, ACK, etc.)
Content-Type	Yes	application/sdp
Content-Length	Yes	SDP payload length
Max-Forwards	Yes	Loop control
X-Exotel-CallSid	Yes	Exotel's global call ID – key for webhook/CDR correlation
X-Exotel-LegSid	Yes	Call leg identifier
X-Exotel-TrunkSid	Yes	Identifies the virtual SIP trunk provisioned to you
P-Asserted-Identity	Yes	Validated CLI presented by Exotel
P-Early-Media	Optional	Indicates early RTP media (if Exotel connects media pre-200 OK)

Key take-aways for FQDN mode

1. **DNS resolution** – Exotel resolves your FQDN on every call; keep TTL ≤ 60s for rapid fail-over.
2. **Certificates (TLS)** – For secure trunks, your SBC's cert CN/SAN should match the FQDN Exotel is dialling.
3. **Logging** – Always capture X-Exotel-CallSid + Call-ID to join SIP pcaps with Exotel dashboards.

9. Troubleshooting

Issue	Cause	Fix
Call fails to reach SBC	FQDN not resolving or DNS TTL delay	Use dig/nslookup to verify resolution
One-way audio	Media ports blocked	Open UDP 10000–40000
Repeated 408 errors	DNS record TTL mismatch	Reduce DNS TTL and ensure IP is reachable

10. Support

For FQDN-based trunk configuration:

- Share your FQDN and port with your Exotel account manager
- Exotel will provision the trunk using DNS-based routing
- Test connectivity using SIPp, sngrep, or call traces

For help:

- Contact support.exotel.com with FQDN, DNS setup, and logs