SIP Trunk Programming

Clearfly SIP Trunk Programming Guide

SIP Trunk Programming Guide

Follow the programming steps below to for SIP trunk direct connection to the ECS:

Step 1: Gather the Following Information from the Carrier

1. Register Domain (Carrier terms: Proxy Server, Register Server, etc.)--This is the Registrar Primary Server setting.

2. Invite Domain (Carrier terms: Proxy Server, Invite Server, etc.)--This is the Invite Primary Server.

3. Username (This is usually the first DID phone number)--This is the User ID-1.

4. Password (If authentication is necessary)--This is the Password-1. Note: Generally this is only required if the trunk requires registration.

5. Incoming Domain in To: header (This is usually your customer's static public IP address)--This is the Domain Name.

6. How many total calls? This will determine how many SIP license you need and how many SIP trunks need to be programmed.

7. What are the DNIS numbers? These must be programmed in the DNIS table. Also, the main DNIS number is usually used for User ID-1 and the CNIS entry.

8. Do the calls have to be sent as ENUM? (i.e., +12145551212)

Sample:

- Proxy server - peer.cfly.co
- username – 4065551212
- DIDs – 4065551212, 4065551213

Step 2: ECS Database Programming

System > Hardware

1. Create the **VTRUNK** Card.
   - Set the card **Type** to **VTRUNK** (The number is automatically programmed).
   - Upload Hardware (Communication > Upload Database to System).
   - Disconnect (Communication > Disconnect).
   - Wait 10 seconds.
   - Reconnect to the ECS and download Hardware (Communication > Download Database from System).
   - 8 Trunk ports are created for you.

2. Configure the **SIP Trunk Ports**.

- **Parameter 1**: This is the DTMF mode. ECS software version 7.0 and higher supports all three modes (In-band, RFC 2833, and SIP Info Event).

- **RFC 2833** is most common.

- **Parameter 3**: VPN or Non-VPN.

  - **Non-VPN** assumes the trunks will use public IP addresses. This setting is used for direct connections to the SIP carrier. This mode is only supported in ECS software version 8.0 or higher.

  - **VPN** assumes that the trunks will use private IP addresses. This setting is used for the SPA 3102, the Ingate Siparator or the carrier uses a private IP address for connection.

Cards

#	Type	1	2	Sys.	Remote VCIF	Remote Card	Sys. Name
▶ 33	VTRUNK	1		0			Main
34	VTRUNK	2		0			Main
35	VTRUNK	3		0			Main
36	VTRUNK	4		0			Main
37 *	VTRUNK	5		0			Main

Ports

#	Type	Logical	Definition	Function	1	2	3
▶ 225	Trunk	1	IP Trunk	SIP or H.323 Trun	RFC2833 Eve	SIP	Non-VPN
226	Trunk	2	IP Trunk	SIP or H.323 Trun	RFC2833 Eve	SIP	Non-VPN
227	Trunk	3	IP Trunk	SIP or H.323 Trun	RFC2833 Eve	SIP	Non-VPN
228	Trunk	4	IP Trunk	SIP or H.323 Trun	RFC2833 Eve	SIP	Non-VPN
229	Trunk	5	IP Trunk	SIP or H.323 Trun	RFC2833 Eve	SIP	Non-VPN
230	Trunk	6	IP Trunk	SIP or H.323 Trun	RFC2833 Eve	SIP	Non-VPN
231	Trunk	7	IP Trunk	SIP or H.323 Trun	RFC2833 Eve	SIP	Non-VPN
232	Trunk	8	IP Trunk	SIP or H.323 Trun	RFC2833 Eve	SIP	Non-VPN

Step 3: VTRUNK Carrier Information Programming

Trunks > SIP Settings

1. Set the **Protocol 1** parameter to **SIP** for each of the SIP Trunk Ports.

2. If required, set the **DNS Server** table number. Note: If the Invite or Registrar Primary Server is a name, then DNS server is required.

Trunks > SIP Settings

SIP Virtual Trunk Cards

VTrunk Card #	Protocol 1	DNS Server	Invite Primary Server	Invite Secondary Server	Registrar Primary Server
✒1	SIP	1	peer.cfly.co		

3. Program the **DNS Primary** server and the **Secondary** server in **Trunks > SIP Settings > SIP DNS Settings**.

Trunks > SIP Settings > SIP DNS Settings

#	DNS Primary IP	DNS Primary Port	DNS Secondary IP	DNS Secondary Port
1	4 .2 .2 .1	53	4 .2 .2 .2	53
2	. . . .	53	. . . .	53
3	. . . .	53	. . . .	53
4	. . . .	53	. . . .	53

4. Program the **Invite Primary Server**. This is the **Invite Domain** setting from **Step 1**

Trunks > SIP Settings

SIP Virtual Trunk Cards

VTrunk Card #	Protocol 1	DNS Server	Invite Primary Server	Invite Secondary Server	Registrar Primary Server
1	SIP	1	peer.cfly.co		

5. **If** the **IP trunk requires Registration**, then set **Register** to **Enable**.

6. **If** the **IP trunk requires a password** when **registering**, then set **Auth. Register** to **Enable**.

7. **If** the **IP trunk requires** a **password** when **calling**, then set **Auth. INVITE** to **Enable**.

Registrar Primary Server	Registrar Secondary IP	Register	Auth. Register	Auth. INVITE
		Disable	Disable	Disable

5

Step 4: SIP Trunk Programming

Trunks > SIP Settings > Virtual Trunk Card "N" Channels

1. Program **VTRUNK** card settings (make sure you are displaying the correct card).

2. Verify the logical port number. If the port is set to zero, you did not program your VTRUNK card correctly.

3. **Port Activation**: Each trunk that is set to **Enabled** requires and will use a **SIP license**.

   - If you have 8 "trunks" from the SIP carrier, you will need 8 licenses and need to enable 8 SIP trunks.

   - If you have 48 "trunks" from the carrier, you will need 48 SIP licenses and need to enable 48 SIP trunks. You will also need 48 MBU channels.

4. **User ID-1**: Set the Username given by the SIP carrier or programmed in the SPA 3102. This is usually the main or first DID from the carrier. The User ID-1 is required.

5. **Password-1**: If you set **Auth. Registration** or **Auth. Invite** to **Enable**, program the password for your account here.

6. **Domain Name**: **VERY IMPORTANT!** This is generally the customer's public IP address.

   Note: If incoming calls are failing, this is probably programmed incorrectly.

7. **DID Feature**: If the setting is **DID**, then the incoming call is checked against the Domain only and routed via the DNIS or ANI table.

   - **DID** setting is used when connecting to SIP carriers.

   - If the setting is set to **Line**, the user ID-1 is checked with the Domain name and the call is routed via the logical port number programming in Class 11.32 and Class 11.34. Note: **Line** setting is used for connecting to the SPA 3102 or Ingate Siparator.

Virtual Trunk Card 1 Channels

Channel #	Log.	Port Activation	User ID-1	Password-1	Domain Name	DID Feature	Registration
1	1	Enable	4065551212		71.97.234.12	DID	Disable
▶ 2	2	Enable	4065551212		71.97.234.12	DID	Disable
3	3	Enable	4065551212		71.97.234.12	DID	Disable
4	4	Enable	4065551212		71.97.234.12	DID	Disable
5	5	Enable	4065551212		71.97.234.12	DID	Disable
6	6	Enable	4065551212		71.97.234.12	DID	Disable
7	7	Enable	4065551212		71.97.234.12	DID	Disable
8	8	Enable	4065551212		71.97.234.12	DID	Disable

8. **Registration**: If the Line is set to Enable, it will send a Register request. If it is set to Disable a Register request will not be sent.

   - **Both Register** (IP 1.02.14.3) and **Registration** (IP 1.02.19.2) **Must Be Enabled** for the line to send a Register request.

   - **In most cases** – Only one line per carrier needs to register.

Step 5: ENUM Programming

Trunks > Trunk Features

1. If the trunks are required to send + in front of the call, then set the ENUM format to "Add + sign to calling/called number.

    - **Outgoing calls** will automatically be modified when this is set.

    - **Incoming calls** do not require this setting.

Trunks > Trunk Features

Log #	Access No.	E&M On-Hook Detect	Forced Rel. Condition	E911 Trunk	Short Flash Time	Short Flash Guard Time	MOH Input Port	ENUM Format
1	1001	1	Loop Close	Normal	4	2	0	None
2	1002	1	Loop Close	Normal	4	2	0	None
3	1003	1	Loop Close	Normal	4	2	0	None
4	1004	1	Loop Close	Normal	4	2	0	None
5	1005	1	Loop Close	Normal	4	2	0	None
6	1006	1	Loop Close	Normal	4	2	0	None
7	1007	1	Loop Close	Normal	4	2	0	None
8	1008	1	Loop Close	Normal	4	2	0	None

Step 6: General trunk programming

1. **Program DNIS or ANI Routing**: The carrier usually sends the DNIS and ANI as 10 or 11 digits.

2. **Program Optimized Routing**: In some instances the carrier will require all calls to be sent as 11 digits. ALL carriers who use ENUM REQUIRE the number to be 11 digits. If you set the ENUM setting, then you MUST send all calls as 11 digits. Note: Optimized routing is required for dialing out on SIP trunks.

3. **Program CNIS**: You can program the caller ID number (Class 10.79) sent to the carrier. If the number is not programmed there, we send the number in Class 29.09 (Trunk Group). If neither are programmed, we send the **TRUNK ACCESS NUMBER**. Some carriers route this, so you will send a four digit access code as your caller ID.

    Important: Iwatsu only supports modification to the From: header. Other methods of sending CNIS are not supported. Also, we do not send a different name. If you need these services, use the Ingate Siparator.

# Step 7: Network programming

Signaling Port: UDP 5080

Audio Ports: UDP 6004-6999

Public IP Address and NAT

Note: Proper port forwarding on a NAT router is the sole responsibility of the distributor / installer. Icon Voice Networks is not responsible for customer premise equipment configuration.
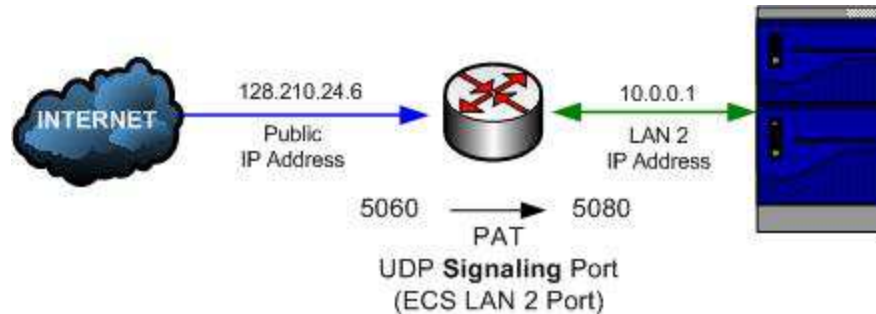
Port Address Translation (PAT) for audio

- **Audio** ports **UDP 6004-6999 must** be routed to **UDP 6004-6999** at **ECS MBU** IP Address.
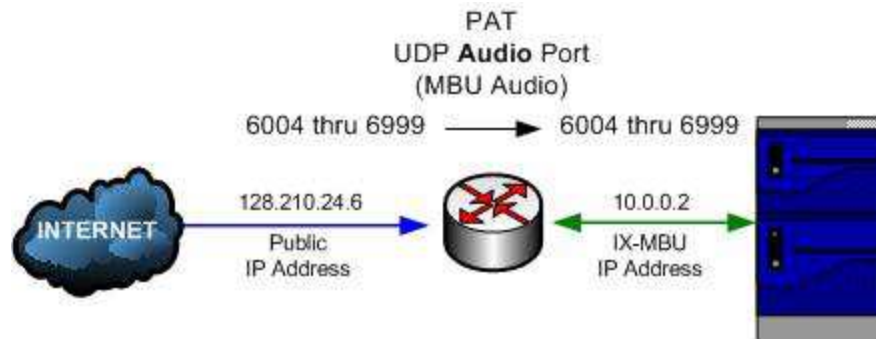
Port Address Translation (PAT) for SIP signaling

- **Signaling** port **UDP 5060** from carrier **must** be routed to **UDP 5080** at **ECS LAN 2** IP Address.

Port Forwarding

A Non-VPN SIP Trunk call will specify port **5060** as the contact port for the internet side of the router.
Routers used for this application **must be** programmed to **forward all inbound SIP packets to ECS SIP Trunk port 5080**.

Public IP Address

Direct connection requires a static pubic IP address. This public IP address is programmed in the ECS database under **Trunks** > **SIP Settings** > **SIP IP Settings: Non VPN IP address** and is used for a SIP Trunk Port that is marked as a Non-VPN port under **System** > **Hardware** (Class 01).
Note: Iwatsu supports only static public IP addressing, but some carriers do support DHCP with far-end NAT traversal.

Notes

1. Request that g711 passthrough is enabled for fax for this circuit.

2. Iwatsu ECS does not authenticate Bye. Registration/Authentication is not supported for this circuit. Carrier must configure this circuit for IP address authentication.

Disclaimers

The information published in this document is intended to provide a general overview of Iwatsu Enterprise-CS interoperability with third party SIP products and services. ICON Voice Networks has tested the performance of the SIP stations, soft phones, Wifi handsets and ATAs listed in this document. Please note, however, that since changes, modifications and availability of third party equipment and services are beyond the control of ICON Voice Networks, interoperability and/or compatibility with said products and services are subject to change without notice.

Due to the changes in service offering by various alternate carriers and the lack of a unified interoperability standard, ICON Voice Networks recommends that the Dealer contact ICON Voice Networks Engineering to verify interoperability with a specific carrier or to request interoperability testing with any carrier not included in this document.

WARRANTY DISCLAIMER:
ICON VOICE NETWORKS DISCLAIMS ALL WARRANTIES AND CONDITIONS, EXPRESS, IMPLIED, OR STATUTORY OF ANY NATURE WHATSOEVER, CONCERNING THE SERVICES AND PERFORMANCE OF THE SIP STATIONS, SOFTPHONES, WIFI HANDSETS, AND SIP TRUNKS LISTED HEREIN, INCLUDING FITNESS FOR A PARTICULAR PURPOSE AND MERCHANTABILITY.

LIMITATION OF LIABILITY:
IN NO EVENT SHALL ICON VOICE NETWORKS BE LIABLE IN CONTRACT, TORT, STRICT LIABILITY, NEGLIGENCE OR OTHERWISE FOR ANY PUNITIVE, CONSEQUENTIAL, INCIDENTAL, SPECIAL, OR INDIRECT DAMAGES, OR FOR LOST PROFITS, LOSS OF DATA, LOSS OF USE OF DATA, DAMAGE OR EXPENSE, DIRECTLY OR INDIRECTLY ARISING FROM USE OF OR INABILITY TO USE THE EQUIPMENTOR SERVIVES, EITHER SEPARATELY OR IN COMBINATION WITH ANY OTHER EQUIPMENT, OR FROM ANY OTHER CAUSE WHETHER OR NOT ICON VOICE NETWORKS HAS RECEIVED NOTICE OF THE POSSIBILITY OR CERTAINTY OF SUCH DAMAGES OR LOSSES.

DEALER ADVISEMENT:

Dealers are advised to include similar disclaimers in their sales agreements with their customers. When using equipment providing telephony over Transmission Control Protocol/Internet Protocol (TCP/IP) and Session Initiation Protocol (SIP) wired and/or wireless facilities, a user may experience certain compromises in performance, reliability and security, even when the equipment performs to the specifications. Dealer's customer should be advised of these risks and acknowledge, under its purchase agreement with the Dealer, that it aware of these risks and that it has determined that they are acceptable for its application of the equipment. In addition, if the customer is solely responsible for ensuring that its networks and transmission facilities QoS and security are adequate for the purpose intended, the customer should acknowledge the same in its purchase agreement with the Dealer. Confer with your legal advisor as to the wording and the requirements when making disclaimers in your jurisdiction.