# Why can’t I register my VoIP device?

Santiago Garcia - 2024-07-27 - Troubleshooting

# Why can’t I register my VoIP device?

Firewalls are a common cause of SIP registration failure with your VoIP device where the firewall blocks incoming traffic required by our SIP registration process. Remember that the process of any SIP registration comprises a sequential number of requests and challenges between your PBX or handset and 2talk as the registration server.

The underlying logic is that our Cloud PBX authenticates your credentials, and secondly stores your IP address and port number at the moment of registration. When a call hits 2talk we, in turn, redirect that call to the last successfully registered IP address and port on your router. If your router blocks our incoming traffic, the call will fail.

Registration – Inbound only

We don’t require you to register to make an outbound call as we check your credentials on each call. Registration is merely the mechanism we use to direct incoming calls through to your router /firewall and ultimately phone or PBX (if using registration).

SIP Keep-Alive

For security, routers are oblivious to the requirements of SIP and by design regularly close the ports preventing 2talk from redirecting to your PBX or handset. To avoid this, set your phone's “Keep-Alive” values to 180 seconds an interval generally well inside the period most routers close their incoming ports. This means every 3 minutes your phone updates our 2talk registration server with its latest IP address and port setting. When an incoming call is received to our network, we can be confident of your IP and port numbers.

## Recommendations

- **SIP ALG:** We recommend disabling SIP ALG as most implementations outside of Juniper and Cisco incorrectly modify SIP and ultimately corrupt SIP packets rendering them unreadable causing unexpected behaviors such as registration and incoming calls failing.
- **TLS:** This is a reliable workaround that alleviates interference caused by SIP ALG as TLS packets are encrypted ultimately preventing corruption. To use TLS set your phones or endpoints to port 5061.
- **Port Forwards:** We recommend port forwarding all traffic on UDP port 5060 to your device. Additionally, we strongly recommend you set your firewall access control lists (ACL) to limit traffic on 5060 to our trunking IP address (27.111.13.68) or our subnet

27.111.13.0/24. Note: we have also configured port 50600 on our end to receive SIP traffic.