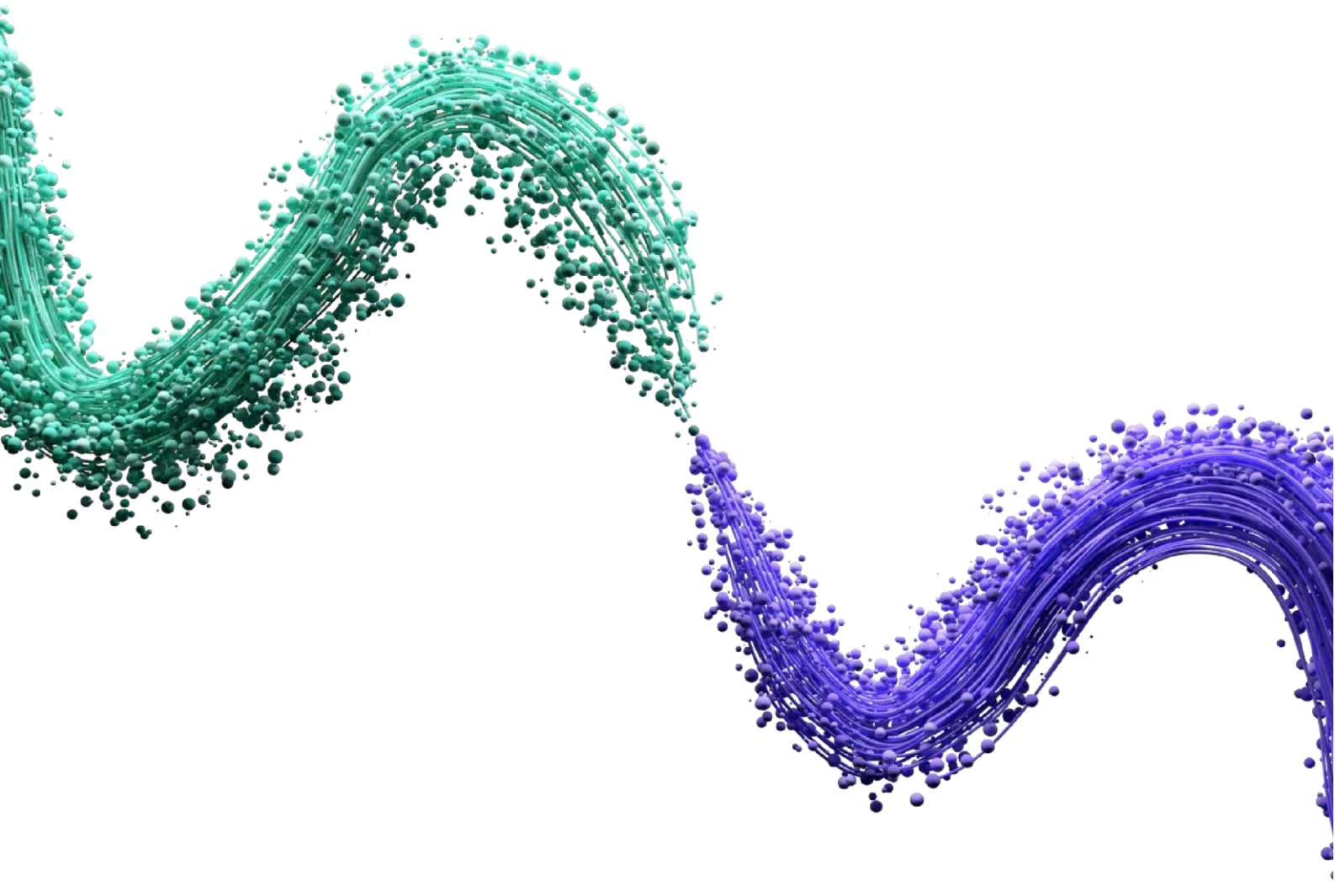
CloudCall

Network Configuration

Guidelines & Reference



Contents

Introduction

The purpose of this document is to provide an outline of the key configurational requirements when using the CloudCall suite of products and services.

The network setup and Internet connectivity are the single biggest factors that will determine the call quality and reliability following your move to CloudCall services. With this in mind, we have a team dedicated to working with your company and/or IT support providers to advise and assist with this aspect of our service delivery.

As each customer's circumstances are different, the exact requirements and implementation will differ from network to network. It's for this reason we have outlined the "core" requirements followed by reference information that may be useful depending on your circumstances.

Target Audience

This document is intended for a technical audience who have the necessary skillset to configure, manage and troubleshoot the equipment present at site.
It may be the case that a given setting or function mentioned in this document has been given a different name by the manufacturer of your equipment, or the implementation may vary between vendor, hardware and/or firmware versions.
It is expected that the reader will be able to take the information in this document and apply it correctly to the equipment at hand.
IT IS NOT intended to be a "step by step" walkthrough of any given configuration.
Our network team can be contacted to advise if you have any specific questions regarding the contents of this document.

Key Configurations

These are considered essential for the functioning of our service. Failure to correctly implement these settings can result in service reliability issues, or in some cases, no service at all.
CloudCall recommends that you have a static Public IP address on a strong business grade internet connection.
Please Note: Any calls in progress if your Public IP address changes will be disconnected and you will not be able to receive calls until the phones re-register.

Firewall/Router

Your router should support and be configured for the following:

- UDP IDLE TIMEOUT of 180 seconds or greater
- Set to allow UDP fragmented packets.
- SIP ALG (or equivalent) disabled.
- Exceptions set in any local web cache proxy.
- UPnP should be disabled.

Voice Quality Optimization

These are settings that are intended to facilitate optimum audio quality.

- QoS rule prioritizing all traffic to our FQDN of **Cloudcall.com**
- **Enable DSCP** on all switching and add DSCP tags EF and AF31 (46 & 26 respectively) to the highest priority low loss queue.
- Where necessary, a bandwidth reservation can also be set to facilitate consistent call quality.

Network Ports used for CloudCall VoIP

There are cases where it may be preferable to define port ranges in the QoS of your equipment. Below are the ports and protocols used by CloudCall Voice services for those who require them.

- SIP - UDP ports 5060 & 6250 as well as TCP ports 19306, 5061, 443.
- RTP - UDP ports 10000 – 65000
- NTP – UDP 123
- ZTP – TCP 80, 443

IP's

- 52.212.101.39 • 54.76.150.31
- 15.156.241.66 • 99.79.21.231
- 52.10.172.218
- 52.40.255.109
- 52.64.204.55
- 54.153.186.77
- 54.229.54.212
- 54.246.36.246
- 54.77.13.41
- 99.81.142.32
- 52.30.145.89
- 15.157.54.153
- 52.60.126.189
- 15.157.0.238
- 99.79.16.159
- 15.157.5.69

RTP IPS

- 52.223.28.241
- 35.71.169.191

DNS

Our VoIP service and integrations must be able to resolve and communicate with the following to operate correctly. **Where a local web cache/proxy is in use, these will need to set to be excluded from and bypass such systems.**

FQDN

- europe.pool.ntp.org
- 0.pool.ntp.org
- cloudcall.com

We suggest using Google or similar DNS for phones where possible.

Antivirus / Software Firewalls

Where the CloudCall App is in use, anti-virus (particularly those with proprietary software firewalls) are required to allow the CloudCall Softphone both inbound and outbound access to the internet. CloudCall's program directory will need to be added as an exception for the Antivirus scanner. Ensure that this is configured locally/centrally where appropriate.

WIFI and Wireless Internet

We do not recommend or support the use of wireless internet, WIFI or IP over Mains (e.g. HomePlug) technologies for VoIP services, as there are many external factors that can affect service delivery that are beyond the control of both ourselves and local IT support.

Wherever possible, a wired network should be used using Cat5e or Cat6 Ethernet cabling from router to phone/PC.