PCS405 – Issue 1
Classification – Public
PCSG – Client Advisories & Best Practices

Pure Cloud Solutions Ltd
6 The Pavilions, Tamworth, B77 4RP
T: 0333 150 6780
E: info@purecloudsolutions.com

Company No: 08033253
VAT No: 133702933

PCS IT Services Limited
6 The Pavilions, Tamworth, B77 4RP
T: 0333 150 6780
E: info@purecloudsolutions.com

Company No: 8500006
VAT No: 161614625

PCS Mobile Solutions Limited
6 The Pavilions, Tamworth, B77 4RP
T: 0333 150 6780
E: info@purecloudsolutions.com

Company No: 8500006
VAT No: 161614625

Client Advisories 'Works with PCS'

Overview
This document offers guidance for customers looking to deploy Pure Cloud Solutions voice services. It outlines essential configuration requirements, recommended best practices, and advice for resolving common issues.

Given the critical importance of call quality and the availability of voice services within an organisation, and considering the wide variety of phones, routers, and internet connectivity options, Pure Cloud Solutions cannot support installations that do not adhere to the practices outlined in this document.

Pure Cloud Solutions offers a complete voice solution, including supported VoIP lines with full Quality of Service controls, along with qualified phones, routers, and network switches. In most cases, we recommend that customers consider this option to maximise service quality.

Where this approach has been implemented on a site, all best practices outlined in this document will already be incorporated into the overall solution.

However, Pure Cloud Solutions recognises that installing a complete voice solution at every site may not always be cost-effective, particularly for roaming or home-based users. Accordingly, this document provides guidance to support such deployments while setting clear expectations.

We strongly recommend that all customers considering the deployment of Pure Cloud Solutions voice services read the following guidance.

Use of third-party data lines

Connectivity Speed Requirements

80 kbps per concurrent call:

Phones on the Pure Cloud Solutions platform require 80 kbps for both upload and download per concurrent call. Customers must ensure that sufficient bandwidth is available or reserved to meet their needs. As upload speeds are often slower than download speeds, this may limit the number of concurrent calls you can make.

For example, if your connection provides 8 Mbps download and 1 Mbps upload, the upload speed would limit you to approximately 12 concurrent calls (1 ÷ 0.08 = 12.5).

The real-time nature of telephone calls requires an underlying transport infrastructure that is reliable, uncongested, and consistent in delivering voice packets. If any of these conditions cannot be maintained, call quality may be affected.

From a customer's perspective, the relevant infrastructure includes everything from the phone itself through to the Pure Cloud Solutions platform. This encompasses the customer's network, router, and the public internet path connecting to the Pure Cloud Solutions platform.

Common issues include:

- Congested IP data lines where voice traffic is shared with other data traffic (e.g., web browsing, streaming media).
- Broadband connections with high contention ratios (xDSL, FTTC, SoGEA & FTTP) that restrict bandwidth, particularly upstream.
- Broadband connections optimised for data that use techniques such as interleaving, which can affect voice quality.
- Bonded connections, which may introduce additional complexity or latency.

As part of Pure Cloud Solutions total voice solution, we recommend providing dedicated internet connections for each site where voice services are required. We also advise installing a separate voice network within the customer's premises to prevent data congestion and ensure optimal call quality.

Customers should be aware that Pure Cloud Solutions cannot manage the quality parameters of third-party IP data lines. As a result, we are unable to guarantee call quality for voice traffic carried over such connections, including those used by roaming users on home networks, public Wi-Fi hotspots, or 4G/5G mobile connections.

Firewalls
The Pure Cloud Solutions voice service uses SIP and RTP protocols to manage calls between your phones and the service. To ensure reliable operation and avoid issues such as one-way audio or call setup failures, several firewall ports must be opened for outbound traffic.

Wildix

Updated: August 2025

Permalink: https://wildix.atlassian.net/wiki/x/NhXOAQ

CDS
Access to external servers:

Service / Purpose	Protocol	Port	Destination
To upload files	TCP	443, outbound	• cds-pbx.wildix.com • data-storage.wildix.com
To display CDS usage statistics in WMS interface	TCP	443, outbound	• cds-console.wildix.com
Other	TCP	443 or another custom secure port, inbound, outbound	• auth.wildix.com • 3.65.155.111 • 3.65.155.145 • 3.123.63.95, 443 or another custom secure port
	TCP	443 or another custom secure port, outbound	• 35.158.75.80 • 3.125.194.126 • 52.57.202.156

	TCP	443, outbound	• wildix-data-storage-af-south-1.s3.af-south-1.amazonaws.com • wildix-data-storage-ap-east-1.s3.ap-east-1.amazonaws.com • wildix-data-storage-ap-northeast-1.s3.ap-northeast-1.amazonaws.com • wildix-data-storage-ap-northeast-2.s3.ap-northeast-2.amazonaws.com • wildix-data-storage-ap-south-1.s3.ap-south-1.amazonaws.com • wildix-data-storage-ap-southeast-1.s3.ap-southeast-1.amazonaws.com • wildix-data-storage-ap-southeast-2.s3.ap-southeast-2.amazonaws.com • wildix-data-storage-ca-central-1.s3.ca-central-1.amazonaws.com • wildix-data-storage-eu-central-1.s3.eu-central-1.amazonaws.com • wildix-data-storage-eu-central-2.s3.eu-central-2.amazonaws.com • wildix-data-storage-eu-north-1.s3.eu-north-1.amazonaws.com • wildix-data-storage-eu-south-1.s3.eu-south-1.amazonaws.com • wildix-data-storage-eu-south-2.s3.eu-south-2.amazonaws.com • wildix-data-storage-eu-west-1.s3.eu-west-1.amazonaws.com • wildix-data-storage-eu-west-2.s3.eu-west-2.amazonaws.com • wildix-data-storage-eu-west-3.s3.eu-west-3.amazonaws.com • wildix-data-storage-il-central-1.s3.il-central-1.amazonaws.com • wildix-data-storage-us-east-1.s3.us-east-1.amazonaws.com • wildix-data-storage-us-east-2.s3.us-east-2.amazonaws.com • wildix-data-storage-us-west-1.s3.us-west-1.amazonaws.com • wildix-data-storage-us-west-2.s3.us-west-2.amazonaws.com

Cloud analytics in Collaboration and x-bees
Access to external servers:

Service / Purpose	Protocol	Port	Destination
Cloud analytics (CDR-View 2.0)	TCP	443 or another custom secure port, inbound, outbound	• auth.wildix.com • cognito-idp.eu-central-1.amazonaws.com • cognito-identity.eu-central-1.amazonaws.com • sts.amazonaws.com • 3.65.155.111 • 3.65.155.145 • kinesis.eu-central-1.amazonaws.com • wam.wildix.com
	TCP	443, outbound	• wda.wildix.com • cognito-idp.eu-central-1.amazonaws.com/eu-central-1_4mprRMCca

Cloud PBX
Outgoing ports:

- Outgoing traffic towards Cloud PBX to the Internet is not limited: any port from 1-65536 range

Incoming ports:

Service / Purpose	Protocol	Port	Destination
Cloud PBX	TCP	• 80 HTTP • 443 HTTPS • all types ICMP • 5060-5061 SIP • 5222-5223, 5269, 5280 ejabberd • 7008 smsd • 4222 gnats • 10050 zabbix • 514 rsyslog	
	UDP	• 5060 SIP • 10000-59999 RTP • 123 NTP • 514 rsyslog	
Access to external servers			• addons.wildix.com (also for HW / VM PBXs)

Also, give access to the following external servers:

Service / Purpose	Protocol	Port	Destination
License activation / check	TCP	443, outbound	• wmp.wildix.com • pbx-api.wildix.com
Authorization	TCP	443, outbound	• configs.wildix.com • auth.wildix.com
Upgrade	TCP	443, outbound	WMS-5.04, WMS-6.xx and WMS-7.xx: • ○ wmp.wildix.com + packages.wildix.com WMS-5.01-5.03: • ○ wmp.wildix.com + aptly.wildix.com WMS-4.xx: • ○ wmp.wildix.com + apt.wildix.com
Upgrade of devices *(starting from WMS 6.05, in case of Hardware or Virtual PBX)*	TCP	443, outbound	• firmwares-cdn.wildix.com • wps.wildix.com
SSL certificate renew	TCP	443, outbound	• ssl.wildix.com
Text-to-speech	TCP	443, outbound	• tts.wildix.com • auth.wildix.com
Speech-to-text	TCP	443, outbound	• stt.wildix.com

Firewall Checker
Access to external servers:

Service / Purpose	Protocol	Port	Destination
Check open ports	TCP	443, outbound	• api.wildix.com
	TCP	443 or another custom secure port, inbound	• api.wildix.com
Check External IP	TCP	80 and 443, outbound	• checkip.wildix.com

NAT IP List
Access to the following NAT IPs should be allowed:

Service / Purpose	Protocol	Port	NAT IP
WIM	TCP	443 or another secure port, outbound	• 3.70.35.54 • 18.156.115.202 • 3.70.163.200
x-bees	TCP	443 or another secure port, outbound	• 18.157.166.13 • 3.64.177.85 • 3.67.254.94

x-hoppers	TCP	443 or another secure port, outbound	• 18.153.143.38 • 18.194.77.233 • 18.153.158.217

Remote Collaboration Apps

Service / Purpose	Protocol	Port	Destination
Collaboration and Web Phone	TCP	• 443 (default) or another external secure port (SIP-RTP page in WMS Settings -> PBX (VM and HW PBXs), outbound	• addons.wildix.com
	UDP	• VM/ HW PBX: e.g. UDP 10000 - 15000 (Note: The range depends on the number and type of licenses on the PBX; check SIP-RTP page for details) • Cloud PBX: UDP 10000-59999	
Cloud-stored group chats	TCP	• outgoing: TCP 5269 • incoming: TCP 443 or another custom secure port	• chats1.meet.wildix.com • chats2.meet.wildix.com
File / image sharing (both PBX and Client)	TCP	443, outbound	• auth.wildix.com • fs.wildix.com
Geolocation services			• Maps in Collaboration are available only via .*wildixin.com domain
WebRTC Kite service	TCP	• 443, outbound • 5061, outbound	• kite.wildix.com
	UDP	10000-1500, outbound	
	TCP	443 or another custom secure port, inbound	• ws2sip.wildix.com
	UDP	10000-1500, inbound	

WIService
(Wildix Integration Service, used by CDR-View, Screen Sharing, Headset Integration, Fax printer, Click2call from Windows, Popup App and other Wildix applications):

- Make sure that FQDN “wildixintegration.eu” is correctly resolved with the IP: 127.0.0.1 by your DNS (on the user PC or on the router side)

iOS/Android

Service / Purpose	Protocol	Port	Destination / Notes
SIP, XMPP, Configuration	TCP	443	
Incoming:	TCP	443 or another external secure port (SIP-RTP page in WMS Settings -> PBX (VM and HW PBXs)	Add the port manually on the app login page: Account > Domain, example: pbx.wildixin.com:443 (for iOS works only with public IP)
• RTP (VM / HW PBX)	UDP	10000 - 15000 (Note: The range depends on the number and type of licenses on the PBX; check SIP-RTP page for details)	
• RTP (Cloud PBX)	UDP	10000-59999	
Outgoing:			
• For push notifications	TCP	443	To notifications.wildix.com; PBX must be connected to the internet and be able to communicate with notifications.wildix.com server
• Android: a direct, unproxied connection to the Google Cloud Messaging	TCP	• 5228 • 5229 • 5230 • 443	
• iOS: a direct, unproxied connection to the Apple Push Notification servers from smartphone	TCP	• 5223 • 2195 • 2196 • 443	

Important: use a transparent port forwarding scheme between the external port on the firewall and the external custom secure port on the PBX, example: 4443 – 4443
Note: Starting from WMS 6.06.20240425.1, the service used for sending push notifications was changed from push.wildix.com to notifications.wildix.com. Make sure to use notifications.wildix.com for WMS 6.06.20240425.1 and higher.

Remote Wildix IP Phones
Access to external servers:

Service / Purpose	Protocol	Port	Destination / Notes
Devices sync with portal	TCP	443, outbound	• api.wildix.com
Remote provisioning of devices	TCP	443 (default) or another external secure port (SIP-RTP page in WMS Settings -> PBX (VM and HW PBXs), inbound	
	UDP	5060 – TCP 5061 for SIP registration, inbound	
RTP (VM/ HW PBX)	UDP	10000 - 15000 (Note: The range depends on the number and type of licenses on the PBX; check SIP-RTP page for details), inbound	

RTP (Cloud PBX)	UDP	10000-59999, inbound	
Multicast paging	UDP	9000-9009	• IP 224.0.0.1 or IP 239.1.1.10 (2N support)
Vision (EOL)/ SuperVision SIP, XMPP, Configuration	TCP	443	
	TCP	443 or another secure external port, incoming (SIP-RTP page in WMS Settings -> PBX (VM and HW PBXs)	On app login page, add manually: pbx.wildixin.com:443
RTP (VM/HW PBX)	UDP	10000 - 15000 (Note: The range depends on the number and type of licenses on the PBX; check SIP-RTP page for details)	
RTP (Cloud PBX)	UDP	10000-59999	
Upgrade of firmware/ applications			• firmwares.wildix.com

Video Conference
Access to external servers (both on the PBX's and on the Client's side):

Service / Purpose	Protocol	Port	Destination
WebRTC Wizyconf videoconference	TCP	443, outbound	• conference.wildix.com • conference-turn.wildix.com Note: TCP 443 and UDP 10000 need to be open on the Client's side only, as well as any port within 40000 - 65535 UDP/ TCP range
	TCP	• 443, outbound, • 443 or another custom secure port (from any remote address), inbound	
	UDP	10000 (to any remote address)	
Screen sharing	TCP	443, outbound	• vnc.wildix.com • kite.wildix.com

Note:

- For support of SIP access from the PBX, enable the rules specified in this section: WebRTC Kite service.
- For file/ image sharing, enable the rules specified in this section: File / image sharing.

WMS Network

Service / Purpose	Protocol	Port	Destination / Note
WMS Network	TCP	443 or another custom secure port	On the side of the Server PBX
	UDP	1194	
Access to WMS network nodes between PBXs	UDP	1194, inbound	
For the correct work of calls between nodes	TCP	443 or another custom secure port	

	UDP	check SIP-RTP page for details	
Access to external servers			• turn.wildix.com (to find a PBX public IP address for WMS Network correct functioning)

x-bees
x-bees also requires the following external servers to be open on your router/ firewall:

Service / Purpose	Protocol	Port	Destination / Note
x-bees	TCP	443, outbound	• app.x-bees.com • api.x-bees.com • login.x-bees.com • chat.wildix-chat.com • avatars.wildix.com • cognito-idp.eu-central-1.amazonaws.com • wda.wildix.com • wda-ws.wildix.com • wim.wildix.com • fs.wildix.com
Videoconference	TCP	443, outbound	• conference-turn.wildix.com
Transcription	TCP	443 or another custom secure port, inbound, outbound	• transcribe.eu-central-1.amazonaws.com

Other Services
Access to external servers:

Service / Purpose	Protocol	Port	Destination / Note
Cloud integrations	TCP	443, outbound	• wim.wildix.com • https://cognito-idp.eu-central-1.amazonaws.com
		443, inbound, outbound	• sts.amazonaws.com
Remote support	TCP	443, outbound	WMS-4.xx PBXs: • vpn4.wildix.com

Rsyslog	TCP	20514, outbound	WMS 6.xx PBXs:
			•
			  ○ pbxlogging6-<minor version>.wildix.com (dynamic IP list)
			WMS 5.02+ PBXs:
			•
			  ○ pbxlogging5-<minor version>.wildix.com (dynamic IP list)

	UDP	514, outbound	WMS 4.0 PBXs: • ○ pbxlogging4-<minor version>.wildix.com (dynamic IP list)
SMS sending with remote GSM gateway	TCP	7008, inbound	On the side of the PBX

Zabbix monitoring	TCP	8099	• IP 63.32.222.64
	TCP	10050	For local Zabbix

LG Ericsson / iPECS

Source / Destination	Protocol	Port / Port Range	Purpose
185.110.180.0/24 ↔ Your Network	UDP	5588	IPKTS Handset Registration / Signaling / Provisioning
185.110.180.0/24 ↔ Your Network	UDP	30000-65525	Media (voice) for IPKTS / LIP / iPECS ONE media etc.
185.110.180.0/24 ↔ Your Network	UDP / TCP	5060	SIP Signaling (if you use SIP devices / trunks)
185.110.180.0/24 ↔ Your Network	UDP	16384-17384	SIP Media / RTP for SIP devices
185.110.180.0/24 ↔ Your Network	TCP	80, 443	SIP Signalling (if you use SIP devices / trunks)
185.110.180.0/24 ↔ Your Network	TCP / UDP	Ports for video / collaboration: e.g. 10000 for video etc.	If using iPECS ONE or similar UC features

SIP-ALG
One of the most common causes of telephony issues is SIP-ALG being enabled on edge firewalls or routers. SIP-ALG (Session Initiation Protocol – Application Layer Gateway) is a feature that is typically enabled by default on many routers and some firewalls. It is intended to assist IP telephony in traversing the NAT between the internal private network and the public internet.

However, within the IP telephony community, it is widely recognised that SIP-ALG services are, at best, unreliable and, at worst, can cause significant issues. For this reason, we strongly recommend disabling SIP-ALG on any routers and firewalls handling Pure Cloud Solutions telephony traffic.

If SIP ALG is enabled, Pure Cloud Solutions would expect to see some, if not all, of the following errors:

- One-way audio
- Call cut off after 15 minutes
- Delays in calls connecting
- Inability to transfer calls
- Problems with inbound calls

Pure Cloud Solutions therefore recommends that SIP-ALG be disabled on all edge routers and firewalls. If you do not manage these devices in-house, we suggest contacting your IT provider, who will be able to apply these changes on your behalf.

Routers
Routers may be provided as standalone devices or integrated with the firewall. Some routers can interpret the SIP protocol, while others simply pass the traffic through without modification.

To correctly route voice calls to and from your phones, the Pure Cloud Solutions service interacts with your router's Network Address Translation (NAT) tables to map IP addresses between the external and internal networks. The service expects the router to pass all SIP traffic without modification.

Router Configuration Requirements

To ensure optimal operation of the Pure Cloud Solutions voice service, please ensure the following:

- Disable any SIP-ALG (Application Layer Gateway) support on your router.
- Review and disable any other SIP translation or modification settings.
- Enable Quality of Service (QoS) parameters for voice traffic.
- Ensure that the IP ranges used within your network are reserved, non-routable ranges as defined by IANA:
    - 10.0.0.0 – 10.255.255.255
    - 172.16.0.0 – 172.31.255.255
    - 192.168.0.0 – 192.168.255.255

Use of Third-Party Phones
The Pure Cloud Solutions service is designed to be compatible with many SIP-based phones. However, each manufacturer implements the core protocol differently and supports different features.

While Pure Cloud Solutions strives to maintain compatibility with the telephones and softphones chosen by our customers, we cannot guarantee support for all features and functionalities.

Our preferred handset models include those that are proprietary to the systems to which they belong.

Wildix models:

- Start
- WorkForce
- ForcePro
- WelcomeConsole
- SuperVision

iPECS models:

- iPECS 1000i Series
    - 1010i
    - 1020i
    - 1030i
    - 1040i
    - 1050i
    - 1080i

Important Note: We recognise that customers may occasionally need to use phones from other manufacturers. Such requirements are usually addressed during the discovery stage, and, where necessary, testing can be conducted to ensure the phone is fully qualified for use with the service. These assessments are carried out on a case-by-case basis.

For more information, please contact support@purecloudsolutions.com