BT Cloud Voice

Firewalls and LAN

Firewalls and LAN

To get the best from your BT Cloud Voice service, you need to make sure it connects to the access network across your internal data network. That way, you can make and receive calls of consistently high quality.

Firewalls

Because there are so many different types of firewall available, it's a good idea to simply contact your firewall provider to find out how to configure yours to work best with Cloud Voice.

It may be that you don't need to do anything at all: your IP handset may register on the network without you having to do any further configuration. Or if you're using our Business Hub 5 on its default settings and without a secondary firewall, Cloud Voice will work fine. But if this isn't the case, and you're unable to make calls, you'll need to make a few changes to your firewall so Cloud Voice can connect with our network. We recommend that you talk to your firewall provider before you make any changes, so you can be sure that you don't inadvertently expose your network to any security risks.

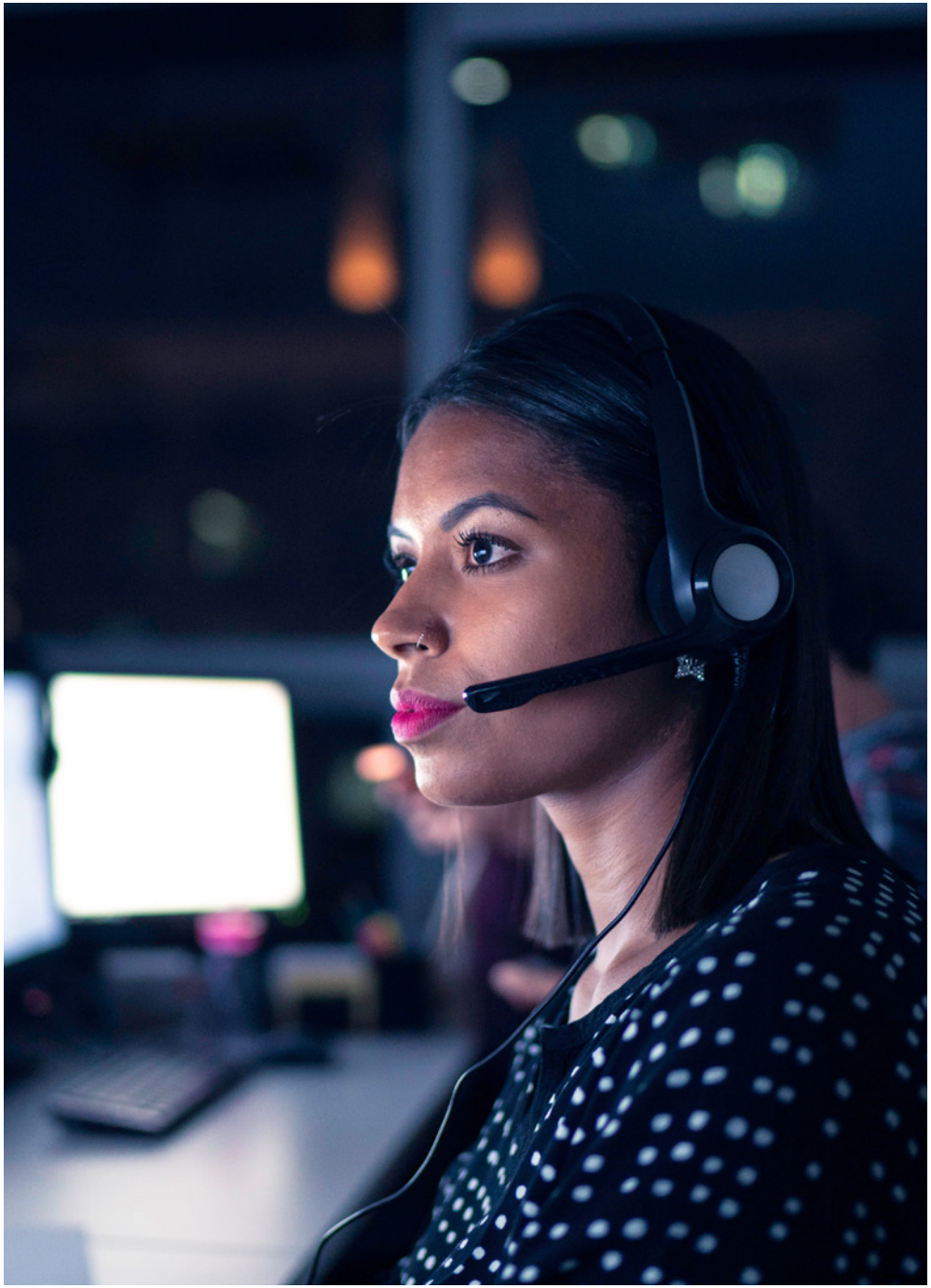
LAN

Cloud Voice has the following network requirements.

If you want to use **address translation**, you'll need access to the protocols and ports detailed in ports.

Depending on the type of firewall you've got, you may not need to open any ports: if your firewall is running 'inside-to-outside' rules, then you'll need to open the ports; there shouldn't be any reason to open ports that are inbound on the firewall.

If your router or firewall is SIP-aware or SIP ALG-enabled, you must turn it off (so the device doesn't interfere with any signalling.



Prioritisation of VoIP traffic

Our Business Internet Access service prioritises your SIP signalling and VoIP traffic over other traffic. But if you're using a non-BT Business access provider, please check that voice traffic is prioritised so you always get the highest quality service.

To make sure you always get good quality calls, your LAN should also prioritise VoIP traffic.

Prioritise traffic to and from these addresses over other competing traffic in your LAN infrastructure

1. Incoming and outgoing BT SIP and VoIP (RTP) traffic should take priority over other traffic through the firewall.
2. If the SIP signalling and VoIP traffic traverses your LAN and competes with other traffic, it should take priority over that traffic.
3. SIP traffic should be prioritised using DSCP value AF31.
4. RTP traffic should be prioritised using DSCP value EF46.

Ports

Our sip platform has a range of IP addresses:

Device	Protocol	Outbound destination		Destination port
Service ports				
Devices and apps (including ATA and BT Cloud Voice Communicator) signalling	SIP	62.7.201.160/27 213.120.60.128/27 213.120.76.0/27 213.120.76.64/27 217.32.186.64/26	62.7.201.128/27 213.120.60.192/27 213.120.76.32/27 217.32.186.0/26 217.32.186.128/26	UDP/TCP 5060-5075 or UDP/TCP 8933
Devices and apps media	RTP	62.7.201.164/27 213.120.60.132/27 213.120.60.164/27 213.120.76.0/27 213.120.76.64/27 217.32.186.64/26	62.7.201.132/27 213.120.60.196/27 213.120.60.228/27 213.120.76.32/27 217.32.186.0/26 217.32.186.128/26	UDP 32766 to 65535

Device	Protocol	Outbound destination	Destination port
Service ports			
IP Phone (including ATA)	NTP	europe.pool.ntp.org uk.pool.ntp.org cn.pool.ntp.org (used by some phone types following a factory reset before BT config is downloaded)	UDP/TCP 123
IP Phone (including ATA)	DNS	Supplied locally	UDP/TCP 53
Handsets			
Cisco Download and Configuration	HTTPS	193.113.10.33 | 193.113.11.35 (dm-csb.yourwhc.co.uk)	TCP 443
Cisco 112 Fax	HTTPS	dm-csb.yourwhc.co.uk	TCP 443
Cisco 122 Fax	HTTPS	dm-csb.yourwhc.co.uk	TCP 443
Cisco Linksys Download and Configuration	HTTPS	193.113.10.34 | 193.113.11.36 (dm-linksys.yourwhc.co.uk)	TCP 443
Poly Download and Configuration	HTTPS	193.113.10.10 | 193.113.11.10 (dm.yourwhc.co.uk)	TCP 443

Device	Protocol	Outbound destination	Destination port
Handsets			
Panasonic Download and Configuration	HTTPS	193.113.10.10 | 193.113.11.10 (dm.yourwhc.co.uk)	TCP 443
Yealink Download and Configuration	HTTPS	193.113.10.10 | 193.113.11.10 (dm.yourwhc.co.uk)	TCP 443
Applications			
Webex (mobile, tablet and desktop) Please see Appendix A for all network requirements to enable Webex Apps and Services	HTTPS	213.121.33.36 | 213.121.34.130 SRV: _xsi-client._tcp.webex-clients-ipcomms.bt.com webex-clients-01-ipcomms.bt.com webex-clients-02-ipcomms.bt.com webex-clients-ipcomms.bt.com	TCP 443
Application and Client Download and Configuration	HTTPS	193.113.10.27 | 193.113.11.27 (dmclients-ipcomms.bt.com)	TCP 443
BT Cloud Voice Communicator operation	XSI	193.113.10.11 | 193.113.11.11 (btbc-ipcomms.bt.com)	TCP 443
BT Cloud Voice Communicator Presence	XMPP + Proprietary	193.113.10.7 (ums01-ipcomms.bt.com) 193.113.11.7 (ums02-ipcomms.bt.com)	TCP 5222 | TCP 1081 TCP 5281 | TCP 5269 | TCP 443

Applications			
BT Cloud Voice Communicator Screen share	Proprietary	193.113.10.8 (uss01-ipcomms.bt.com) 193.113.11.8 (uss02-ipcomms.bt.com)	TCP 8443
BT Cloud Voice Reception Console	Proprietary	193.113.10.12 | 193.113.11.12 (applications-ipcomms.bt.com)	TCP 443
CRM Integrator/ Connect	Proprietary	193.113.10.12 | 193.113.11.12 (applications-ipcomms.bt.com)	TCP 443
CRM Integrator/ Connect Licence check	HTTPS	193.113.10.13 | 193.113.11.13 (ccusage-ipcomms.bt.com)	TCP 443
Network Assessment Test	Proprietary	62.7.201.194 62.7.201.195 62.7.201.202 62.7.201.203	UDP 8090 UDP 2000-2001
Web portal			
BT Cloud Voice Business Portal	HTTPS	193.113.10.13 | 193.113.11.13 (btcloudvoice.bt.com)	TCP 443
Call recording portal	Proprietary	193.113.10.32 | 193.113.11.34 **Note:** browser will be redirected from business portal.	TCP 443

Additional settings

You should also apply these settings for Cloud Voice. **Please remember to reboot all related devices after any changes are made.**

Nat Refresh (UDP Timeout)

Refer to your Manufacturer's guide for information on how to configure Nat Refresh. This needs to be set to 300 seconds. If this is not set correctly you will have problems making and receiving calls or a call may disconnect after 5 minutes.

SIP Transformations sections

Disable these – this setting is also known as SIP ALG. If any one-way transmission is experienced, please disable **Packet Acceleration.**

STUN server

There is no stun server integration with Cloud Voice. SIP ALGs STUN servers are mainly for peer-to-peer SIP, and aren't needed for client/server SIP using SBCs.

A STUN server *(Session Traversal of User Datagram Protocol [UDP] Through Network Address Translators [NATs])* allows NAT clients (i.e. IP phones behind a firewall) to set up phone calls to a VoIP provider hosted outside of the local network.

Appendix A

Customer Network Requirements for Webex Apps and Services

All information within this appendix is regularly updated by the application supplier so please refer to their website for the latest information Link

Domains and URLs that need to be accessed for Webex Services

Domain / URL	Description	Webex Apps and devices using these domains / URLs
***.wbx2.com** ***.ciscospark.com**	**Webex micro-services.** **For example:** Messaging service File management service Key management service Software upgrade service Profile picture service Whiteboarding service Proximity service Presence service Registration service Calendaring service Search service	All
***.webex.com**	Webex Meetings services Identity provisioning Identity storage Authentication OAuth services Device onboarding	All
***.webexcontent.com**	**Webex messaging service – general file storage including**: User files, Transcoded files, Images, Screenshots, Whiteboard content, Client and device logs, Profile pictures, Branding logos, Log files Bulk CSV export files and import files (Control Hub)	All **Note:** File storage using webexcontent.com replaced clouddrive.com in October 2019 Your organization may still be using cloudrive.com to store older files – for more information see (1)

Domain / URL	Description	Webex Apps and devices using these domains / URLs
***.sparkpostmail1.com** ***.sparkpostmail.com**	e-mail service for newsletters, registration info, announcements	All
***.giphy.com**	Allows users to share GIF images. This feature is on by default	Webex App
safebrowsing.googleapis.com	Used to perform safety-checks on URLs before unfurling them in the message stream. This feature is on by default	Webex App
***.walkme.com** **s3.walkmeusercontent.com**	Webex Teams User Guidance client. Provides onboarding and usage tours for new users For more info see support.walkme.com/knowledge-base/access-requirements-for-walkme/	Webex App
msftncsi.com/ncsi.txt **captive.apple.com/hotspot-detect.html**	Third party internet connectivity check to identify cases where there is a network connection, but no connection to the Internet. The Webex app performs its own internet connectivity checks, but can also use these 3rd party URLs as a fallback.	Webex App
***.eum-appdynamics.com**	Performance tracking, error and crash capture, session metrics (3)	Webex App
***.amplitiude.com**	A/B testing and metrics (3)	Webex Web App Webex Android App
***.quovadisglobal.com** ***.digicert.com** ***.godaddy.com**	Certificate Validation	All

Webex Services

Port Numbers and Protocols

The following table describes ports and protocols that need to be opened on your firewall to allow a registered Webex app, and device to communicate with Webex cloud services.

Destination Port	Protocol	Description	Devices using these rules
443	**TLS**	Webex HTTPS signalling. Session establishment to Webex services is based on defined URLs, rather than IP addresses. If you are using a proxy server, or your firewall supports DNS resolution; use these Webex Services URLs to allow signalling access to Webex services.	All
444	**TLS**	Video Mesh Node secure signalling to establish cascade media connections to the Webex cloud	Video Mesh Node
123 (1)	**UDP**	Network Time Protocol (NTP)	All
53 (1)	**UDP / TCP**	Domain Name System (DNS) Used for DNS lookups to discover the IP addresses of services in the Webex cloud. Most DNS queries are made over UDP; however, DNS queries may use TCP as well.	All
5004 and 9000*	**SRTP over UDP**	Encrypted audio, video, and content sharing on the Webex App and Webex Room devices For a list of destination IP subnets see Webex IP subnets for media *The Webex App uses UDP port 9000 to connect to Webex Meetings media services	Webex App* Webex Room Devices Video Mesh Nodes

Webex Services

Port Numbers and Protocols (continued)

The following table describes ports and protocols that need to be opened on your firewall to allow a registered Webex app, and device to communicate with Webex cloud services.

Destination Port	Protocol	Description	Devices using these rules
5004	**SRTP over TCP**	Used for encrypted content sharing on the Webex App and Webex Room devices TCP also serves as a fallback transport protocol for encrypted audio and video if UDP cannot be used. For a list of destination IP subnets see Webex IP subnets for media	Webex App Webex Room Devices Video Mesh Nodes
33434 (2)	**SRTP over UDP** **SRTP over TCP**	**Optional** Port 33434 is used for encrypted media if port 5004 is blocked by your firewall. Note that a TCP socket on port 33434 will be established, but only used if connections fail over TCP and UDP on port 5004 and UDP on port 33434. (2) For a list of destination IP subnets see Webex IP subnets for media	Webex App Webex Room Devices
443 (2)	**SRTP over TLS**	Used as a fallback transport protocol for encrypted audio, video and content sharing if UDP and TCP cannot be used. Media over TLS is not recommended in production environments For a list of destination IP subnets see Webex IP subnets for media	Webex App Webex Room Devices

IP subnets for Webex media services

Configure your firewall to allow access to these destination Webex IP subnets and transport protocol ports for media streams from Webex apps and devices. UDP is Cisco's preferred transport protocol for media and is strongly recommended that only UDP is used to transport media.

TCP and TLS as transport protocols for media are not recommended as these types of protocols can seriously affect media quality.

3.22.157.0/26	18.181.178.128/25	69.26.160.0/19
3.25.56.0/25	18.181.204.0/25	114.29.192.0/19
3.101.70.0/25	18.230.160.0/25	150.253.128.0/17
3.101.71.0/24	20.50.235.0/24	170.72.0.0/16
3.101.77.128/28	20.53.87.0/24	170.133.128.0/18
3.235.73.128/25	40.119.234.0/24	173.39.224.0/19
3.235.80.0/23	44.234.52.192/26	173.243.0.0/20
3.235.122.0/24	52.232.210.0/24	207.182.160.0/19
3.235.123.0/25	62.109.192.0/18	209.197.192.0/19
18.132.77.0/25	64.68.96.0/19	210.4.192.0/20
18.141.157.0/25	66.114.160.0/20	216.151.128.0/19
18.181.18.0/25	66.163.32.0/19	

Important stuff

You should be able to use Cloud Voice to make and receive good quality phone calls – but you'll only be able to do that if your internal network is set up properly. If it isn't, your call quality won't be top-notch.

If you report a fault to us and we find that it's down to a problem with equipment that you own, or due to non-BT access you are using, then we will raise charges relating to the issue.

All the information in this document is for general guidance only. We recommend that you contact the company handling your firewall and switch or an IT consultant, for anything to do with configuring your LAN or firewall.

August 2021