Administrator Guide

Fuze Service Requirements

Last updated: 05/13/2022

2 Copley Place, Boston, MA | 800-890-1553 | www.fuze.com

Introduction

This document describes network requirements for Fuze services, specifically relating to the necessary ports which are used to transport data to and from Fuze servers and data centers.

Important Note

This first section and its associated sub-sections detail crucial information that should be understood before attempting to configure your ports for use with Fuze services.

Table of contents

Fuze UC Services – Production Traffic

Fuze Unified Communication (UC) services production traffic communicates via the networks described in the following table.

Please note: Customers with a global presence may need to allow subnets from regions beyond their home region for voice service connectivity. This allows users who travel beyond their home region to reach voice service data centers when required.

Location	Networks (IP Ranges)		
North America	● 70.42.233.0/24 ● 66.151.176.0/24 ● 162.223.96.0/23	● 170.76.188.0/22	● 45.252.184.128/29 ** ● 45.252.184.136/29 **
EMEA	● 162.223.96.0/22 ● 170.76.188.0/22	● 185.155.144.0/22 ● 66.151.176.0/24	● 13.244.176.0/27 ● 45.252.184.144/29 **
Asia	● 162.223.96.0/23 ● 170.76.188.0/22 ● 66.151.176.0/24	● 103.197.96.0/22 ● 64.209.246.0/24	● 205.139.23.0/24 ● 45.252.184.0/22
Australia	● 170.76.188.0/22 ● 66.151.176.0/24	● 103.197.96.0/22	● 162.223.96.0/23
South America	We recommend speaking to a Fuze Network Consultant for IP targets.		
	** Denotes IP ranges that are required for Fuze-MyTest tool.		

Subnets in Meeting by component type		
Location	**Audio subnet**	**Video subnet**
US (San Jose, CA and Ashburn, VA)	206.81.176.0/26 206.81.177.0/26	206.81.176.128/25 206.81.177.128/25
EU (Frankfurt)	206.81.181.0/26	206.81.181.128/25
LON (London)	206.81.184.0/26	206.81.184.128/25
Australia (Sydney)	206.81.185.0/26	206.81.185.128/25
Singapore	206.81.182.0/26	206.81.182.128/25

Fuze Services and Ports

For a full summary, see the Addendum for FW Rules and QOS and DSCP Tagging.

Please adhere to the following:

- The **source** for **ALL services below** should be a **Trusted LAN**.
- The **direction with stateful filter** for **ALL services below** should be **Outbound Only**.
- For all **Source** and **Destination** ports, if a stateless filter is used, reciprocating ports are required.
- When accessing Fuze services over a DIA or Broadband connection, HTTPS authentication is required.
- NTP and DNS services are obtained through external public hosts.
- Network routing and rules for NTP, DNS, and HTTPS may need to be adjusted to accommodate this traffic.

Priority	Source Ports	Destination Ports / Timeouts	Additional Comments
Service: Audio RTP - Media Transmission			
DSCP: 46(ef) IP Precedence: 5 Audio : CS7 on Windows OS without admin rights	UDP 11780-12780 (Yealink) 2000-3000 (Polycom) 4000-4999 (Mobile apps) 5000-5499 (Softphones) 6000-6230 (Analog/Fax) 9000-20000 (Aux devices)	UDP 9000-20000 (30 sec) UDP 4000-4599 (30 sec, T38 Fax services)	Performance Guidelines: Delay <150ms; Jitter <30ms; Packet Loss <1% **NOTE:** Ports may vary if NAT is in use.
Fuze also optionally supports sRTP for encrypting audio transmissions. This is not enabled by default, but can be requested by contacting your Fuze representative.			
Service: SIP Signaling			
DSCP 26(af31) IP Precedence 3 (applies to CoS set up on switches) SIP : CS5 on Windows OS without admin rights	UDP 5060 TCP 5060 TCP 5061: TLS	UDP 5060 (360 sec) TCP 5060 (600 sec) TCP 5061: TLS (600 sec)	Performance Guidelines: Delay <150ms; Jitter <30ms; Packet Loss <1%
Service: Voice calls with added Video			
N/A	Dynamic (P2P connection)	Dynamic (P2P connection) TCP 443 for prodturn*.fuzemeeting.com domains (with dynamic IP range) (STUN and TURN)	ICE services allow voice calls with video, using P2P connections. The ICE framework detects which port/IP combination is available to establish the connection between peers (either using local network or Internet) (STUN protocol). If no possible connection is found, then all content is relayed to *.fuzemeeting.com (TURN protocol)

Priority	Source Ports	Destination Ports / Timeouts	Additional Comments
Service: Fuze Meeting			
Audio : CS7 Video : CS5 Screenshare : CS5 SIP : CS5 Fuze automatically applies the correct DSCP tags.	N/A	TCP 80 TCP 443 SSL Audio UDP 50,000 – 54,999 Video UDP 55,000 – 65,000 **Destination IPs/Domain** 206.81.176.0/20 Fuzebox.com	Only ports 80 and 443 are **strictly** required. All other ports are for improved performance and reliability. If Fuze traffic is still blocked, please report the specifics using the "Submit Feedback" link while in a Fuze meeting which allows our support team to receive key details relating to your meeting and local Fuze application. **Note:** See QOS Policy Management for details about how and why windows will override our settings when our application is not run as admin.
Service: NTP - Date / Time			
N/A	N/A	UDP 123	Fuze recommends the use of public, free NTP services. Please see the preceding section for more information.
Service: HTTP & HTTPS - Provisioning / Administration			
N/A	N/A	TCP 80	HTTP and HTTP-like transactions are using this port to allow egress from customer sites with strict outbound policies. If you have a deep inspection firewall, ensure that this traffic from your clients to the Fuze cloud is not rejected by over aggressive rules as this traffic doesn't always strictly look like HTTP.
N/A	N/A	TCP 443	HTTPS, tunneled RTMP, custom TCP, and other TLS encrypted traffic such video in the event that the high-range UDP ports are blocked. Again, packet inspection firewalls should be configured to not discard packets to these ports on addresses within our network block.

Priority	Source Ports	Destination Ports / Timeouts	Additional Comments
Fuze Contact Center (FCC)			
N/A	N/A	TCP 40000-40003 TCP 50000-50002	N/A
ICMP - Monitoring/Troubleshooting			
N/A	N/A	ICMP	Inbound ICMP to EDGE also recommended
Telepresence Connect			
N/A	N/A	TCP 1720 (for H.323 call setup) TCP 50,000-60,000 (for RTP traffic H.323 signaling) UDP 5060 (for SIP signaling) UDP 50,000-60,000 (for RTP traffic SIP/H.323)	Note that Fuze calls originate from 206.81.176.0/20. If your telepresence implementation requires a domain, you can use fuzemeeting.com h323 - 1720 SIP/TLS - 5060/5061 RTP/RTCP - 50000-60000

Fuze Apps and Services — Network Ports

The following networks must be accessible to allow Fuze applications and services function.

Location	Network Ports
All	Ports 443 (https://) and 80 (http://) FuzeNode (audio): UDP 50000-54999, TCP 443 MediaHub (next gen Video): UDP 55000-65000, TCP 443 For optimal performance, Fuze Meeting video conferencing and VoIP will attempt to use UDP on 50,000 - 65,000, however, this traffic will failover to TCP 443 if Fuze determines that the ports are blocked. UDP reduces latency and is more ideal for real-time communication. TCP should only be used as a last resort as it introduces delay and can cause out-of-sync and/or delay issues between video and audio. In rare cases where the network is particularly lossy, using TCP can reduce packet loss and improve video/audio quality. Some IT admins prefer to block UDP, as most network traffic these days is over HTTP which is TCP underneath. In these cases, Fuze falls back to using TCP but it's recommended that UDP be opened up for Fuze traffic for the aforementioned reasons.

Stateful Firewalls / Filters

All enterprise communication sessions from Fuze phones, Fuze desktop applications and Fuze mobile applications (over WLAN) are initiated from the respective phone or application to a Fuze data center, and are accounted for in the table below. Typically, when enterprise communication for these phones and applications are passing through a stateful firewall, only the ports noted below need to be opened outbound.

NOTE: Some non-standard Fuze SIP Trunk and PRi/Analog conversion productions require inbound communication and management that is not listed below.

If using a stateful filter:

- Inbound traffic from Fuze will access the network via ports opened by outbound sessions initiated by Fuze phones and desktop applications.
- Any inbound troubleshooting protocols or access/visibility initiated from Fuze will need to be allowed inbound into the network *(For example, ICMP traffic)*.
- The exact configuration of these protocols varies for device, vendor, package, and firmware revision. Fuze recommends that you request information or open a service ticket through the vendor specific to your exact gear and configuration.
- **UDP timeouts**, **SIP/RTP timeouts**, and/or **Application-Level Gateways (ALGs)** may need to be modified in order to support Fuze service timeouts noted below. Fuze recommends contacting the vendor for confirmation specific to the exact hardware, revision, and configuration.

NOTE: If using a device with one or more ALGs relevant to Fuze services, the ALG(s) may need to be disabled, enabled, or further adjusted for Fuze services to work properly. Fuze recommends contacting your vendor for support if ALGs are causing connectivity issues with Fuze devices on your network.

Additional Guidelines

- Fuze does not support not recommend double-NATing of Fuze UC Services production traffic.
- Fuze UC Services production traffic route paths between Fuze UC endpoints and Fuze UC production facilities should be symmetric at all times.
- Fuze UC Services production traffic should be Full-Duplex at all times.
- Fuze UC Services production traffic should not be ACTIVE/ACTIVE load balanced.
- Fuze UC Services production traffic should not pass through WAN accelerator. If this traffic must pass through a WAN accelerator, it should be white-listed so as not to be acted on in any manner by the WAN accelerator.

  Note: For troubleshooting Fuze UC Services production traffic through a WAN accelerator, it may be required to physically remove the WAN accelerator from the traffic path.

- Fuze strongly recommends enabling QoS enforcement for all VOICE or VIDEO related aspects of the environment communicating to or from Fuze.
- If QoS is enforced in the environment, performing packet captures is recommended to validate that both ingress and egress packets are appropriately marked as packets pass through the WAN, based on the services guidelines below.

Required Third Party Service Domains

IPs hosted in Fuze Public subnets are static, but third party cloud companies constantly update their IP ranges and therefore only provide dynamic IPs. The following table lists and describes domains for third party services that must be allowed for Fuze apps and services to function.

Note: All domains in this table with a protocol of HTTPS use the default port (443).

Required Third Party Services			
Service	**Domains**	**Protocol**	**Used For**
Amazon Cloudfront	d1j2or3azepuq.cloudfront.net	HTTPS	Avatar and roster pictures
	d1yyftelocodol.cloudfront.net dtjaodtk8r3ge.cloudfront.net		Application update servers
Amazon AWS	fuze-floppy-live-us-east-1.s3.amazonaws.com	HTTPS	File storage, used for chat attachments, meeting content, etc. Amazon recommendations: AWS IP Blog post and JSON
	clientlogsprod.s3.amazonaws.com	HTTPS	Client logs
	callwave.s3.amazonaws.com	HTTPS	Avatars, content, etc
	amazonses.com	HTTPS	Required for email domain authentication. Fuze supports SPF, DKIM, and DMARC for email domain authentication.
	ec2-54-196-93-240.compute-1.amazonaws.com ec2-54-165-236-172.compute-1.amazonaws.com ec2-52-6-107-167.compute-1.amazonaws.com ec2-52-6-107-167.compute-1.amazonaws.com ec2-35-168-0-209.compute-1.amazonaws.com ec2-3-81-191-163.compute-1.amazonaws.com	HTTPS	Application update servers
	s3-1.amazonaws.com		Avatars, content, etc.
	a34184085d13e29e6.awsglobalaccelerator.com a33a57c21e64f1e07.awsglobalaccelerator.com	HTTPS	Networking Accelerator/Load Balancer
	Note: For all AWS IPs, Fuze Web uses TURNS over port 443, and STUN and TURN over port 3478 (TCP & UDP).		
Google Maps	maps.google.com	HTTPS	Maps images on the contact profile section
Google Auth/Google Firebase	No Longer Applicable	N/A	Google Firebase urls are not required for Fuze Desktop versions 5.2 or later. Due to improvements in our software, these features are now handled by api.fuze.com, chat.fuze.com,

			presence.fuze.com. See the June 12th, 2019 entry in the Change History Appendix for more details.
Google Cloud	25.25.190.35.bc.googleusercontent.com	HTTPS	Temp files (images, chat...) Caching
Mixpanel	api.mixpanel.com	HTTPS	Our analytics for the apps for the R&D team to be data driven in our designs and improvements.
Segment	api.segment.io	HTTPS	Logs, crashes, analytics, etc. for the R&D Team.

DNS Recommendations and Requirements

Fuze uses and recommends the use of open DNS services for primary and secondary DNS servers for all customers. Popular open DNS providers, and links to their respective IPs include:

  - Google
  - OpenDNS
  - Cloudflare

- The primary DNS technical requirement for Fuze services is to allow SRV as defined in RFC 2782, and NAPTR as defined in RFC 2915.

- Unless your organization has experience managing an internal corporate DNS service, Fuze recommends a free, internet-based service from one of the major entities such as Google, Open DNS, Cloudflare, etc.

- Fuze Voice endpoints do not function properly without access to a DNS service, so a redundant, diverse setting, with multiple network paths is recommended. Many endpoints can receive up to 2 DNS Servers via their DHCP options.
  For example:

  - **Server 1**: Internal customer provided DNS; accessible via internal network
  - **Server 2**:
    - 8.8.8.8 (external Google DNS; accessible via internet egress)
    - or 208.67.222.222 and 208.67.220.220 (Open DNS; accessible via internet egress)
    - or 1.1.1.1 and 1.0.0.1 (Cloudflare DNS; accessible via internet egress)

- For desk phone deployments, Fuze recommends utilizing a Voice VLAN separate from the Data VLAN. Options provided by DHCP, such as DNS, SNTP, and VLAN Discovery, will have precedence over Fuze provided configuration parameters. DHCP options given out in the Voice VLAN should not provide any values for DHCP Options 66, 160, or 161 as this can impact the provisioning of new devices, and even the stability of previously provisioned devices. DHCP Options for DNS should only include two IP addresses, one for the primary server and secondary server.
  - At the time of this recommendation, the devices supported by Fuze, both Polycom and Yealink, only support 2 DNS Server IP addresses provided via DHCP (or via a downloaded config file from Fuze) within their configuration.

If your organization must connect to Fuze privately due to specific security or network configuration challenges, please contact your Fuze support representative to discuss your options in further detail.

NTP Recommendations and Requirements

Fuze uses and recommends the use of free, internet-based or ISP-provided NTP services for all customers.
If your organization does not currently use one, popular providers include:

- Google
- Cloudflare
- NTP Pool
- US Government

NTP Pool and multiple servers: If your organization is able to enter multiple servers, you can use **0.pool.ntp.org**, **1.pool.ntp.org**, **2.pool.ntp.org**, **3.pool.ntp.org**. See https://www.ntppool.org/en/use.html for more information.

If your organization must connect to Fuze privately due to specific security or network configuration challenges, please contact your Fuze support representative to discuss your options in further detail.

URL filtering and HTTP proxy

Below is an explanation of URLs that are currently used by all Fuze products (including URLs for things like software clients and desk phones). This is important for URL filtering and HTTP proxy.

Please Note: When using a proxy-server with SSL inspections (like Zscaler or Symantec) we strongly recommend disabling SSL inspection for all domains and FQDNs listed in the table below. If Fuze is not included in your proxy whitelist, please reach out to Fuze Support so that we can work with the vendor to be officially whitelisted in the future.

Fuze Services			
Service	**Domain / IPs**	**Domain IP Type**	**Used For**
Core Fuze Meeting	206.81.176.0/20	N/A	Fuze Meeting backend
	*.fuzebox.com	Dynamic	Meetings backend
	*.fuzemeeting.com	Dynamic	Meetings, Recordings, Video, Voice Calls with Video, and Fuze Web Softphone features
Core Fuze Voice and Authentication Services	*.thinkingphones.com	Dynamic	Voice, Provisioning, Authentication, portal, Desktop Web UX
	warden.thinkingphones.com	Dynamic	Authentication and Login - Can be configured with static IP, see Network Consultant or Support for more info. Please note when configuring authentication through our Warden service: ● Some client and device authentication services require HTTPS access to warden.thinkinghones.com, which resolves variable IP Addresses - IP Addresses not noted in Fuze UC Services production traffic. ● If HTTPS (tcp_443) is allowed out to general internet, or to any destination from the client or device: no additional filter adjustments are required. If HTTPS is not allowed, then a dynamic filter rule that can resolve warden.thinkingphones.com is required.
	*.fuze.com	Dynamic	Authentication, Support, Help, Web, Desktop URL
	*.thinkingphones.net	Static	NTP server, Deskphones Provisioning

continues on next page

Fuze Services (continued)

Service	Domain / IPs	Domain IP Type	Used For
Core Fuze Voice and Authentication Services (continued)	Polycom: x.fuze.com, ztp.polycom.com Yealink: Y.fuze.com rps.yealink.com	Static	Deskphones, Provisioning **Please Note**: Beginning 11/20/18, the device provisioning server addresses x.fuze.com (Polycom), and y.fuze.com (Yealink) will replace x.adgjmp.net and y.adgjmp.net. After 11/20/18 voice functionality will be retained for devices that remain on a legacy domain, however the device(s) will not receive configuration or updates from Fuze. The device provisioning server will still support Cisco and Panasonic devices. ztp.polycom.com, and rps.yealink.com are manufacturer-specific addresses that facilitate Zero Touch Provisioning (ZTP), a process that greatly simplifies and improves efficiency of device provisioning. For more details, please contact your Fuze sales engineering representative.
	170.76.189.0/25 170.76.189.128/25 These IP addresses are subject to change but will stay within this range.	Static	Deskphones, Provisioning non-Polycom or Yealink brands. **Please Note**: Configuration updates for the following legacy IPs are no longer available as of 11/20/18. These have been replaced by the ranges currently listed in the **Domains / IPs** column. 66.151.176.95 66.151.176.120 66.151.176.30 66.151.176.31
	170.76.189.109 185.155.147.44 103.197.99.34 activation.uc.fuze.site	Static	Device activation for all brands. NAPTR Record: activation.uc.fuze.site
Email Domain Authentication, Fuze APIs, Chat, and presence	*.fuze.com	Dynamic (email) and HTTPS	Fuze supports SPF, DKIM, and DMARC for email domain authentication. Individual urls for APIs, Chat, and Presence include: api.fuze.com, chat.fuze.com, and presence.fuze.com. **Please note** Fuze Welcome Emails will arrive from the following service, please allow traffic from this domain and/or IP address, as to ensure email is received from Fuze: outbound-mail.sendgrid.net (o1.ptr4056.email.fuze.com. [168.245.74.51]
Fuze Contactive	*.contactive.com	Dynamic	Contacts and Insights (Contactive).
Fuze Desktop Application Logging	http-inputs-fuze.splunkcloud.com	Dynamic	Fuze Desktop logs for troubleshooting

Connected Account Network Requirements

The services and domains described in the following table allow you to take advantage of connected calendar and cloud accounts, as well as other add-ons for Fuze Desktop and Fuze for Salesforce.

Connected accounts - other services		
Service	**Domains**	**Used For**
O365	Follow Microsoft guidelines	Allows users to connect their O365 accounts to integrate with their address book and calendar.
Google Apps / G Suite	Follow Google guidelines	Allows users to connect their G Suite accounts to integrate with their address book and calendar.
Salesforce	Follow Salesforce guidelines	Allows users to connect their Salesforce accounts to integrate with their address book and calendar.
Dropbox	Follow Dropbox guidelines	Allows users to connect their Dropbox accounts to integrate and share in-meeting content. Access to these services can be deactivated by opening a support request.
Box	Follow Box guidelines	Allows users to connect their Box accounts to integrate and share in-meeting content. Access to these services can be deactivated by opening a support request.

Integrated Authentication and SSO

Integrated authentication and single-sign-on (SSO) are optional technologies that Fuze supports for organizations that use them for user provisioning and authentication.

Fuze Desktop 5.0 adds support for Integrated Authentication using your own authentication service. This is an optional feature for organizations who choose to use Integrated Authentication for Fuze Desktop. Integrated Authentication uses intranet server or proxy details to allow users to sign in to Fuze without being prompted for their username or password. This is accomplished by using cached credentials which are established when the user initially logs in to the machine on which Fuze Desktop is running. Integrated Authentication for both Windows and macOS users and is supported for Negotiate and NTLM challenges only.

Fuze also supports a variety of providers of single-sign-on (SSO) technology, which is a software technology that integrates with most applications that require user credentials. When implemented, SSO allows users manage their credentials and easily log in to Fuze applications from a single interface.

See the article User Provisioning and SSO in Fuze Community for more details about these features.

Logging and Packet Drops

Fuze strongly recommends enabling logging on any filtering device during network validation and/or trouble-shooting. Additionally, to allow logging for Fuze apps,

- Any **TCP/UDP packet drops** with Fuze UC Services production networks as a **source or destination**, especially those passing through ports **5060** or **5061**, **strongly suggests there is a problem with the configuration of the device that is reporting the drops**.
- Packet drops can occur even when filters allow **ANY:ANY**, due to other services/rules that maybe running on the filtering devices.
- Ensure that all Fuze UC Services production traffic is white-listed and matches the appropriate rules, and that there are no drops associated with Fuze UC Services production traffic.
- If passing Fuze UC Services traffic through a non-Fuze-provided device, please be prepared to provide packet captures of Fuze UC Services traffic on the device.

Addendum

Required Fuze Services FW Rules

Source	Source device	Source Ports	Port Type	Stream	Destination Ports	Destination	Usage
Voice and Data VLANs	Yealink	11780-12780	UDP	Audio	4000-4599, 9000-20000	162.223.96.0/22 170.76.188.0/22 185.155.144.0/22 66.151.176.0/24 13.244.176.0/27 45.252.184.144/29 162.223.96.0/23 170.76.188.0/22 66.151.176.0/24 103.197.96.0/22 64.209.246.0/24 205.139.23.0/24 45.252.184.0/22 170.76.188.0/22 66.151.176.0/24 103.197.96.0/22 162.223.96.0/23 206.81.176.0/26 206.81.177.0/26 206.81.181.0/26 206.81.184.0/26 206.81.185.0/26 206.81.182.0/26 206.81.176.128/25 206.81.177.128/25 206.81.181.128/25 206.81.184.128/25 206.81.185.128/25 206.81.182.128/25	Audio RTP - Media Transmission
	Polycom	2000-3000	UDP	Audio	4000-4599, 9000-20000		Audio RTP - Media Transmission
	Mobile Apps	4000-4999	UDP	Audio	4000-4599, 9000-20000		Audio RTP - Media Transmission
	Soft Phones	5000-5499	UDP	Audio	4000-4599, 9000-20000		Audio RTP - Media Transmission
	Analog/Fax	6000-6230	UDP	Audio	4000-4599, 9000-20000		Audio RTP - Media Transmission
	Aux devices	9000-20000	UDP	Audio	4000-4599, 9000-20000		Audio RTP - Media Transmission
	All Phones	5060	UDP	Audio	5060		SIP Signaling
		5060-5061	TCP	Audio	5060-5061		SIP Signaling
		80, 443	TCP	Audio, Video, Data	80, 443		Fuze Apps and Services FuzeNode, MediaHub
		50000-54999	UDP	Audio	50000-54999		Fuze Apps and Services FuzeNode, MediaHub
		55000-65000	UDP	Video	55000-65000		Fuze Apps and Services FuzeNode, MediaHub
		80, 443	TCP	Data	80, 443		HTTP & HTTPS - Provisioning / Administration
	Soft Phones	443	TCP	Audio, Video, Data	443	fuzemeeting.com	Fuze Meeting Voice calls with added Video

Continues on Next Page

Voice and Data VLANs	Soft Phones	80, 443	TCP	Audio, Video, Data	80, 443	206.81.176.0/20	Fuze Meeting - Audio / Video / Signaling / Authentication
	Soft Phones	50,000 – 54,999	UDP	Audio	50,000 – 54,999		Fuze Meeting - Audio / Video / Signaling / Authentication
	Soft Phones	55,000 – 65,000	UDP	Video	55,000 – 65,000		Fuze Meeting - Audio / Video / Signaling / Authentication
	Soft Phones	40000-40003, 50000-50002	TCP	Data	40000-40003, 50000-50002		Fuze Contact Center (FCC)
	Conf Room	1720	TCP	Audio, Video	1720		H.323 call setup
	Conf Room	50,000-60,000	TCP	Audio, Video	50,000-60,000		RTP traffic H.323 signaling
	Conf Room	5060	UDP	Audio, Video	5060		SIP signaling
	Conf Room	50,000-60,000	UDP	Audio, Video	50,000-60,000		RTP traffic SIP/H.323
	Edge CPE/FW	ICMP	TCP	Data	ICMP		Monitoring/Troubleshooting
	Yealink	80, 443	TCP	Data	80, 443	y.fuze.com	Provisioning
	Yealink	80, 443	TCP	Data	80, 443	rps.yealink.com	Provisioning
	Polycom	80, 443	TCP	Data	80, 443	x.fuze.com,	Provisioning
	Polycom	80, 443	TCP	Data	80, 443	ztp.polycom.com	Provisioning
	Soft Phone	80, 443	TCP	Data	80, 443	170.76.189.0/25	Provisioning
	Soft Phone	80, 443	TCP	Data	80, 443	170.76.189.128/25	Provisioning
	All Phones	80, 443	TCP	Data	80, 443	170.76.189.109	Activation
	All Phones	80, 443	TCP	Data	80, 443	185.155.147.44	Activation
	All Phones	80, 443	TCP	Data	80, 443	103.197.99.34	Activation
	All Phones	80, 443	TCP	Data	80, 443	activation.uc.fuze.site	Activation
	All Phones	80, 443	TCP	Data	80, 443	http-inputs-fuze.splunkcloud.com	Monitoring/Troubleshooting
	~~All Phones~~	~~80, 443~~	~~TCP~~	~~Data~~	~~80, 443~~	~~contactive.com~~	
	Soft Phone	443	TCP	Data	443	fuze.com	email
	All Phones	80, 443	TCP	Data	80, 443	api.fuze.com	APIs
	All Phones	80, 443	TCP	Data	80, 443	chat.fuze.com	Chat
	Conf Room	80, 443	TCP	Audio, Video, Data	80, 443	presence.fuze.com	Telepresence

Required Third Party Services FW Rules

Source	Source device	Source Ports	Port Type	Stream	Destination Ports	Destination	Usage
Voice and Data VLANs	Soft Phone	443, 3478	TCP, UDP	Data	443, 3478	d1j2or3azepuq.cloudfront.net	Amazon Cloudfront Avatar and roster pictures
	Soft Phone	443, 3478	TCP, UDP	Data	443, 3478	d1yyftelocodol.cloudfront.net	Amazon Cloudfront Application update servers
	Soft Phone	443, 3478	TCP, UDP	Data	443, 3478	dtjaodtk8r3ge.cloudfront.net	Amazon Cloudfront Application update servers
	Soft Phone	443, 3478	TCP, UDP	Data	443, 3478	fuze-floppy-live-us-east-1.s3.amazonaws.com	AWS File storage, used for chat attachments, meeting content etc
	Soft Phone	443, 3478	TCP, UDP	Data	443, 3478	clientlogsprod.s3.amazonaws.com	AWS Client logs
	Soft Phone	443, 3478	TCP, UDP	Data	443, 3478	callwave.s3.amazonaws.com	AWS Avatars, content, etc
	Soft Phone	443, 3478	TCP, UDP	Data	443, 3478	amazonses.com	AWS email domain authentication
	Soft Phone	443	TCP	Data	443	maps.google.com	Google Maps images on the contact profile section
	Soft Phone	443	TCP	Data	443	api.mixpanel.com	Mixpanel analytics for the apps for the R&D team t
	Soft Phone	443	TCP	Data	443	api.segment.io	Segment Logs, crashes, analytics for the R&D Team.

Added (05/10/2022) Third Party Services FW Rules

Source	Source device	Source Ports	Port Type	Stream	Destination Ports	Destination	Usage
Voice and Data VLANs	Soft Phone	443, 3478	TCP, UDP	Data	443, 3478	ec2-54-196-93-240.compute-1.amazonaws.com	AWS Application update servers
	Soft Phone	443, 3478	TCP, UDP	Data	443, 3478	ec2-54-165-236-172.compute-1.amazonaws.com	
	Soft Phone	443, 3478	TCP, UDP	Data	443, 3478	ec2-52-6-107-167.compute-1.amazonaws.com	
	Soft Phone	443, 3478	TCP, UDP	Data	443, 3478	ec2-35-168-0-209.compute-1.amazonaws.com	
	Soft Phone	443, 3478	TCP, UDP	Data	443, 3478	ec2-3-81-191-163.compute-1.amazonaws.com	
	Soft Phone	443, 3478	TCP	Data	443, 3478	s3-1.amazonaws.com	AWS Content, Avatars, etc.
	Soft Phone	443, 3478	TCP	Data	443, 3478	a34184085d13e29e6.awsglobalaccelerator.com	Networking Accelerator/Load Balancer
	Soft Phone	443, 3478	TCP	Data	443, 3478	a33a57c21e64f1e07.awsglobalaccelerator.com	
	Soft Phone	443	TCP	Data	443	25.25.190.35.bc.googleusercontent.com	Google Cloud Temp files (images, chat...) Caching

QOS and DSCP Tagging

	QOS DSCP Tagging	Source Ports	Destination Ports / Timeouts
Media Transmission	DSCP: 46 (EF) or 34 (AF41) on RTR/FW CS7 on Windows OS	UDP 11780-12780 (Yealink) 2000-3000 (Polycom) 4000-4999 (Mobile apps) 5000-5499 (Softphones) 6000-6230 (Analog/Fax) 9000-20000 (Aux devices)	UDP 9000-20000 UDP 4000-4599 (30 sec)
SIP Signaling	DSCP 26 (AF31) or 34 (AF41) on RTR/FW CS5 on Windows OS	UDP 5060 TCP 5060 TCP 5061: TLS	UDP 5060 (360 sec) TCP 5060 (600 sec) TCP 5061: TLS (600 sec)
Fuze Meeting	on Windows OS Audio : CS7 SIP, Video, Screenshare : CS5	N/A	TCP 80, TCP 443 Audio: UDP 50,000 – 54,999 Video: UDP 55,000 – 65,000

Change History

5/13/2022

- Added updated QOS and DSCP Tagging summary as Addendum
- Renamed “Service: Fuze Meeting - Audio / Video / Signaling / Authentication” to Service Fuze Meeting and moved above Service NTP
- Removed “If Windows users have admin access to their machines”
- Added links to FW Rules Addendum and QOS DSCP tagging summary addendum on the first page of Fuze Services and Ports
- Removed “Reference for QOS Set Outgoing DSCP Value” links in Fuze Services and Ports pages
- Moved Fuze Services and Ports pages before the DNS Recommendations and Requirements page
- Moved Required Third Party Service Domains pages after Fuze Services and Ports pages
- Removed Realtime Network Monitoring Requirements page (AppNeta related)
- Renamed Appendix Change History to “Change History”
- Did a quick pass of whole doc and updated formatting to be more consistent
- Updated Table of Contents to reflect new changes

5/11/2022

- Added Third Party Domains/URLs for Amazon AWS and Google Cloud

1/7/21

- Added DHCP recommendations for desk phone deployments

6/25/20

- Removed port 7777 from Telepresence Connect table
- Added new LON subnets for Meetings [206.81.184.0/26 as audio subnet and 206.81.184.128/25 as video subnet]
- Formatting updated for consistency

1/27/20

- Added Singapore information to Subnets in Meeting by Component Type table.
- Relocated the DNS Recommendations section to precede the Services and Ports table.
- Added an NTP Recommendations section before the Services and Ports table.
- Updated Services and Ports table to de-prioritize private DNS and NTP recommendations.
- Added the following language to the URL Filtering and HTTP Proxy table for Fuze Welcome emails: “Please note that Fuze Welcome Emails will come from the following service, please allow traffic from this domain and/or IP address, as to ensure email is received from Fuze: outbound-mail.sendgrid.net (o1.ptr4056.email.fuze.com. [168.245.74.51]”

10/1/19

Added https://http-inputs-fuze.splunkcloud.com to URL Filtering and HTTP Proxy table for Fuze Desktop logging for troubleshooting scenarios.

8/23/19

Added information about sRTP for audio streams in the Audio RTP section of the Services and Ports table.

6/12/19:

The Google Firebase urls listed in the following table are not required for Fuze Desktop versions 5.2 or later. As a result, these have been removed from the Required Third Party Services table, and a temporary explanatory note has been added.
Due to improvements in our software, these features are now handled by api.fuze.com, chat.fuze.com, presence.fuze.com.

Service	Domains	Protocol	Formerly Used For
Google Auth	www.googleapis.com apis.google.com	HTTPS	Google Firebase authentication.
Google Firebase	ngchat-tenant-1-live.firebaseapp.com ngchat-tenant-2-live.firebaseapp.com ngchat-tenant-3-live.firebaseapp.com ngchat-tenant-4-live.firebaseapp.com ngchat-tenant-5-live.firebaseapp.com ngchat-tenant-6-live.firebaseapp.com ngchat-tenant-7-live.firebaseapp.com ngchat-tenant-8-live.firebaseapp.com ngchat-tenant-9-live.firebaseapp.com ngchat-tenant-10-live.firebaseapp.com lmp.firebaseapp.com	HTTPS	Chat (IM) signaling.
Google Firebase	*.firebaseio.com	WSS	Chat and meeting notes.

4/26/19:

- Updated all instances of 170.76.188.0/23 to 170.76.188.0/22 in the Fuze UC Services - Production Traffic table.
- Added the following IPs and NAPTR record domain, all of which are required for activating devices, to the **Core Fuze Voice and Authentication Services** section of the URL filtering and HTTP proxy table: 170.76.189.109; 185.155.147.44; 103.197.99.34; activation.uc.fuze.site

4/1/19:

- Added web-specific ports information in the AWS section of the Required Third Party Service Domains table.
- Added an Email Authentication row to the URL filtering and HTTP proxy table.
- Fixed TOC reference and updated Cloudflare link in the DNS Recommendations section to refer to Cloudflare's free product. Also added the following language to the Server 2 details within this section: "or 1.1.1.1 and 1.0.0.1 (Cloudflare DNS; accessible via internet egress)"
- Removed the Customer Hosted Mail Service section.

3/15/19:

- Removed 185.155.144.0/22 from the "Fuze Meeting - Audio / Video / Signaling / Authentication" section of the Ports Table.
- The following IP ranges are no longer required for Fuze Meetings and are removed from the Core Fuze Meeting section of the Ports Table: 185.155.147.192/26, 170.76.188.0/22, and 185.155.144.0/22.
- The IP range 206.81.176.0/20 is removed from the Core Fuze Meeting row of the Ports Table, as it is already covered by 206.81.176.0/20.

3/4/19:

- Updated DNS Recommendations and Requirements section to reflect recommended open DNS going forward.
- Removed Fuze DNS section and row from the Ports Table.

2/1/19:

- Added an important note to precede the URL filtering and HTTP proxy table that recommends disabling SSL inspection for all domains and FQDNs listed in the table when using a proxy-server with SSL inspections (like Zscaler or Symantec).

1/15/19:

- Revised the Integrated Authentication section to combine with SSO and clarify that both are optional features rather than specific requirements for Fuze service. Relocated key configuration details to an Integrated Authentication and SSO-specific article in Fuze Community.
- Added ztp.polycom.com, and rps.yealink.com to the Ports Table. ztp.polycom.com, and rps.yealink.com are manufacturer-specific addresses that facilitate Zero Touch Provisioning (ZTP), a process that greatly simplifies and improves efficiency of device provisioning. For more details, please contact your Fuze sales engineering representative.

11/16/18:

- Added a new section to the Ports Table (p.4) titled ***Service: Voice calls with added Video*** that addresses requirements for the Voice calls with Video feature introduced in Fuze Desktop 5.2.
- In the URL filtering and HTTP proxy table, Added Voice Calls with Video, and Fuze Web Softphone features to the list of features for which *fuzemeeting.com must be whitelisted.
- Moved DNS Recommendations section to a more prominent location on page 6.
- Updated Yealink UDP range to 11780-12780 in the Audio RTP section of the Ports table in accordance with a correction to Yealink's support documentation.
- Restored Polycom: x.adgjmp.net and Yealink: y.adgjmp.net to the URL filtering and HTTP proxy table (p.10) as they are technically still live, and instead added clarifying language to cover the forthcoming switch to Polycom: x.fuze.com and Yealink: y.fuze.com, as well as info about the new CIDR Blocks 170.76.189.0/25 170.76.189.128/25.
- Added the following note to the intro of the Fuze UC Services – Production Traffic section: "**Please note**: Customers with a global presence may need to allow subnets from regions beyond their home region for voice service connectivity. This allows users who travel beyond their home region to reach voice service data centers when required."
- Added the subnet 170.76.188.0/23 to all regions in the Fuze UC Services – Production Traffic table. 170.76.188.0/23 is the new config server subnet is intended to eventually replace 66.151.176.0/24

(but is not a full replacement at this time).

10/12/18:

- Removed the following IP addresses from the EAA (Australia) region of the UC Services production traffic table: 52.62.2.56, 52.62.46.100, 52.62.82.19, 52.62.88.91, 52.62.19.160, 52.62.77.253 ,52.62.57.82, 52.62.108.111
- Added Telepresence section to the Ports table.
- Added updated desk phone/provisioning domains and IPs to URL filtering and HTTP proxy table.
- Consolidated Service column content in into each section header within the Ports table to free up more space and reduce redundancy.
- Consolidated "*Protocol Rules"* section into the intro paragraph of the Ports Table
- Added Optional Connected Accounts intro details to Connected Accounts table, and links to relevant third-party network guidelines within table.
- Consolidated the section "*Authentication through warden service"* into the warden.thinkingphones.com row (addtl notes section) of the URL Filtering and HTTP Proxy table.
- Remaned "*IP Ranges from 3rd Party Services"* to Required Third Party Domains and added clarifying intro language to the intro paragraph. 3rd party services
- Removed *"QOS Tagging on Windows Machines"* section, as this information was redundant to the Fuze Meetings row of the Ports table.
- The section "*Fuze Desktop and Fuze Addins (Browser, Outlook, etc.)*" is renamed "Fuze Apps and Services Network Ports".
- Renamed Appneta section to Realtime Network monitoring Reqs.
- Re-arranged multiple sections to bring ports-related ones to the top, under a broader ports section.

9/21/18:

- Ports table:
  - Modified DSCP language to "on Windows OS without admin rights" in multiple rows.
  - SIP row - Added clarification to IP Precedence 3, and corrected "Video CS5" to "SIP CS5".
  - Audio RTP row - removed "Realtime Audio".
  - Removed Video RTP row as Fuze no longer supports video-enabled hard phones.
  - Meetings row:
    - Removed IP ranges 206.81.181.0/26, 170.76.188.0/22, and domain Fuzemeeting.com from the Destination column.
    - Destination port TCP/UDP 3478 in not required (443 is recommended) and has been removed.
    - Destination port TCP 7443, is no longer used and has been removed.
    - Destination port Video UDP values have been updated from 55,000-65,00 to 50,000-60,000.
    - Added relevant details from Video RTP row and QOS section.
- Renamed "Protocol" column to "Domain IP Type" in URL filtering and HTTP proxy table.
- Removed QOS section on Page 13 and consolidated with Fuze Meeting row of Ports table.
- Removed Removed VideoHub and Screensharing ports lists from Fuze Desktop and Fuze Addins table. These now roll up under MediaHub. Also added language to clarify why UDP is recommended in most scenarios.
- Revised and added configuration details to note in QOS Tagging on Windows Machines section.
- Revised phrasing of Customer Hosted Mail Service section.

- Removed all “DIA-only” 52.x.x.x IP addresses from the EMEA section of the UC Services production traffic table.
- Added new Sydney region and IPs to the Subnets in Meeting by component type table.

9/4/18:

- All ports content condensed into a single Ports table at the beginning of the document.
- Updated class selector to CS5 for Video RTP and SIP services in the Ports table, and for Video, SIP, and Screen Share in the QOS Tagging section.
- Added AppNeta section.
- Removed “Port table Legacy Devices” section.
- Added Subnets in Meeting by component type table.

8/4/18: Content reformatted and updated branding applied.

Fuze, Inc
2 Copley Place, Suite 7000
Boston MA 02116
800.890.1553