Technical Setup Documentation

If you are on a work network or any network behind a firewall, you may need to speak with your IT department or network administrator to ensure you have the best setup to enjoy your Jugo event. When you do, please give them the websites below to whitelist, and the ports to open.

Websites

*jugo.io

Ports

Minimum Requirement:

The minimum requirement is that TCP port 443 is open. Some firewall/proxy rules only allow for SSL traffic over port 443. You will need to make sure that non-web traffic can also pass over this port.

STUN is a network protocol used primarily for real-time voice/video and messaging and it may impact video and chat feed, we recommend not blocking STUN traffic over port 443.

Better Experience:

In addition to the minimum requirements being met, we also recommend that UDP port 3478 is open. This port is used by a piece of hardware called STUN server that helps establish the connection between the participants in the call with a firewall in the middle.

Best Experience:

For the best possible experience, we recommend that UDP ports 1025 - 65535 be open. Once these ports are open, there is no need for intermediary STUN/TURN servers which removes a hop from the media traffic.

Affects audio/video: Backstage, Sessions, and Networking.

Since all segments affected make use of UDP to deliver the best video quality via media streams. When the ports are blocked, the audio/video quality will be impacted and result in: drops in quality, freezes of the stream, downscaling resolution, or even audio/video being completely inaccessible as a result of very restrictive firewalls that don't allow even TCP traffic unless whitelisted.

Whitelisting

Some companies might have restrictive network configurations and may not be able or willing to whitelist all TCP/UDP traffic to have successful sessions.

That is why we share the full list of IPv4 addresses to whitelist for the Sessions and the Stage to function properly.

For WebRTC signalling server: Name: signalling.app.jugo.io Port/Protocol: 3478 (TCP/UDP) Address: 44.197.56.84	For Attendee WebSocket Connections: Name: psp.app.jugo.io Port/Protocol: 443 (TCP)	For Broadcast connections: Name: Millicast (Dolby) URL: live-phx-1.millicast.com

Note:

- In case the UDP ranges are blocked, real-time communications (i.e. video/audio in Sessions / Networking / Backstage) will fall back to TCP.
  TCP is not recommended for media transfer (plus causes more loads on the internet bandwidth and CPU time) because it requires the receiver to acknowledge the data has been received and the sender tries to send again if there is no acknowledgment within the certain window.
  Since media data that failed to be delivered a second ago is not that relevant especially when the following seconds of media were delivered seamlessly.
- QUIC is a protocol introduced by Google to make the web faster and more efficient. It's on by default in Google Chrome and used by a growing list of websites. Unfortunately, most, if not all, firewalls do not currently recognize QUIC traffic as 'web' traffic, therefore it is not inspected, logged, or reported on, leaving a hole in a network's security.
  Blocking QUIC at the firewall will force the browser and server to fall back to standard HTTP or HTTPS, allowing the traffic to be inspected, protected, and reported on as usual.
  The advice from most firewall vendors is to block QUIC until support is officially added to their products. This recommended method will vary from the firewall to firewall. Some firewalls allow QUIC by default while others block it by default, but all firewalls are able to allow or block it. It shouldn't affect Hopin's functionality if QUIC traffic is blocked. More info here: https://en.wikipedia.org/wiki/QUIC and here: https://www.chromium.org/quic/.

Feel free to reach out to us at support@jugo.io in case you have questions or need assistance.