What should I do if the video conferencing feature is blocked by my hospital?

The video conferencing feature of CPMS 2.0 is based on WebRTC, a web technology that allows for real-time video and audio traffic over the internet. Sometimes this technology is blocked by hospital firewalls. We advise you to take the following measures:

- Ensure you are using a standard browser such as Microsoft Edge, Mozilla Firefox or Google Chrome.
- If you experience issues such as missing audio or video, inability to share screen, or intermittent connection problems, the network firewall should be checked to ensure the following traffic is allowed between client devices and the BigBlueButton (BBB) server.
- If you face any of these issues, contact your IT team and raise a ticket with the information given below:

To allow CPMS 2.0 to properly work, please whitelist the IPs as follows:

- For Production main IP address: 52.19.244.38
- For Production backup IP address: 34.252.60.133

The main IP is the one that works all the time, the backup will be used only in case AWS services are down (which is a very unlikely scenario).

Also allowing the following network traffic:

1. **WebRTC Media Traffic (Required)**
    - Protocol: UDP
    - Ports**:** 16384–32768

This port range carries the real-time media streams used for:

- Microphone audio
- Webcam video
- Screen sharing

This is the most critical firewall requirement. If these UDP ports are blocked, users can often join a meeting successfully but will experience one or more of the following issues:

- No microphone audio
- No webcam video
- Screen sharing does not work

2. **HTTPS (Required)**
    - Protocol: TCP
    - Port 443

This connection is required for:

- Accessing the BigBlueButton web interface
- User authentication
- API communication
- WebSocket signalling
- Chat, presentations and polls
- Screen sharing control

Important: SSL/TLS inspection (SSL interception) should be disabled for this traffic, as it can interfere with WebRTC and prevent audio, video and screen sharing from working correctly.

3. **STUN/TURN Services (Required)**
    - Protocols**:** UDP and TCP
    - Port**:** 3478

STUN/TURN services are used by WebRTC to establish media connections, particularly when users are behind NAT devices or restrictive firewalls.

These services are responsible for:

- Discovering the client's public IP address
- NAT traversal
- Establishing reliable audio, video and screen sharing connections

If port 3478 is blocked, users may still be able to join meetings, but they may experience:

- Audio or video failing to connect
- Intermittent media connectivity
- Screen sharing failures

BigBlueButton FQDN: video.cpms2.ern-net.eu

Summary

Please ensure the following outbound connections from client devices to the BigBlueButton server are permitted:

Protocol	Port(s)	Purpose
TCP	443	Web interface, authentication, signalling and application traffic
UDP	16384–32768	Audio, video and screen sharing media
UDP/TCP	3478	STUN/TURN services for WebRTC connectivity

Please be aware that, regardless of the video conferencing tool being used, network traffic policies and security measures at your hospital may cause connectivity issues that will require a case-by-case analysis.

If the above ports are correctly configured and you continue to experience issues after contacting your IT team, please reach out to DG SANTE support team ((SANTE-ERN-CPMS-ITSUPPORT@ec.europa.eu) and provide details of the network environment and any firewall or proxy solutions in use to receive personalised advice.