

Remote Invigilation Firewall and Network Requirements

Purpose and intended audience

This document is intended for customer IT teams, network administrators and technical support teams.

Highfield operates its remote invigilation service using two systems: **ProctorExam** and **Invigilate by Wayvero**. The system used for an individual session booking can be identified by checking the login URL sent in the candidate invite.

Highfield may choose to use either system for remote invigilated sessions. Customers should therefore allow both systems through their firewall to ensure candidates can access their remote invigilated sessions.

Most standard firewall configurations will allow access without additional changes. Where a customer network uses strict firewall rules, proxy filtering, SSL inspection, web filtering or browser extension control, the domains and ports listed in this document should be permitted.

These requirements relate to outbound access from the candidate or user device/network to the listed services. Inbound firewall rules are not normally required.

Customers should allow access by domain or hostname where possible. IP addresses for cloud-hosted services may change and should not be relied on unless a static IP range has been specifically provided.

ProctorExam Firewall Requirements

The ProctorExam requirements listed below are based on ProctorExam's published firewall guidance. Please check ProctorExam's latest guidance before making firewall changes:

<https://support.proctorexam.com/hc/en-us/articles/12390349250445>

Europe

HOST / DOMAIN	PROTOCOL	PORT
d3tjv75rqu87aa.cloudfront.net	HTTPS	TCP 443
d6qianmj5t13p.cloudfront.net	HTTPS	TCP 443
eu-central-1-proctorexam-uploads.s3.eu-central-1.amazonaws.com	HTTPS	TCP 443
coturn-eu4-signaling-alb-a0450aabc29b7703.elb.eu-central-1.amazonaws.com	TCP/UDP	3478
coturn-eu5-signaling-alb-ed668e7664539109.elb.eu-	TCP/UDP	3478

central-1.amazonaws.com		
netdna.bootstrapcdn.com	HTTPS	TCP 443
embed.tawk.to	HTTPS	TCP 443

United States

HOST / DOMAIN	PROTOCOL	PORT
dux3ypxpr5g7o.cloudfront.net	HTTPS	TCP 443
d6qianmj5t13p.cloudfront.net	HTTPS	TCP 443
us-east-2-proctorexam-uploads.s3.us-east-2.amazonaws.com	HTTPS	TCP 443
coturn-us1-signaling-alb-1430da6650baf6b3.elb.us-east-2.amazonaws.com	TCP/UDP	3478
netdna.bootstrapcdn.com	HTTPS	TCP 443
embed.tawk.to	HTTPS	TCP 443

Canada

HOST / DOMAIN	PROTOCOL	PORT
d29qqmp99xovac.cloudfront.net	HTTPS	TCP 443
d6qianmj5t13p.cloudfront.net	HTTPS	TCP 443
ca-central-1-proctorexam-uploads.s3.ca-central-1.amazonaws.com	HTTPS	TCP 443
coturn-ca1-signaling-alb-72e7fc3558ce8c17.elb.ca-central-1.amazonaws.com	TCP/UDP	3478
netdna.bootstrapcdn.com	HTTPS	TCP 443
embed.tawk.to	HTTPS	TCP 443

ProctorExam browser extension and mobile app requirements

REQUIREMENT	DETAILS
Browser extension requirements	Candidates must be able to install and run the required Chrome browser extension. Browser extension policies should not block communication.
Mobile app requirements	Candidates will need access to the Apple App Store or Google Play Store to download the required mobile app. The mobile app must also be allowed to communicate with the web application.

Invigilate by Wayvero Firewall Requirements

All regions

HOST / DOMAIN	PROTOCOL	PORT
invigilate.wayvero.co.uk	HTTPS	TCP 443
invigilate-admin.wayvero.co.uk	HTTPS	TCP 443
highfieldproctor-p89hb5vd.livekit.cloud	WSS	TCP 443
*.livekit.cloud	HTTPS/WSS	TCP 443
*.turn.livekit.cloud	HTTPS/TURN	TCP 443
*.host.livekit.cloud	UDP	3478
LiveKit media service hosts	UDP	50000-60000
LiveKit media service hosts	TCP	7881
authentication.highfieldqualifications.com	HTTPS	TCP 443
cdn-live.highfieldqualifications.com	HTTPS	TCP 443
secure-cdn.highfieldqualifications.com	HTTPS	TCP 443

The Invigilate by Wayvero web application uses WebSocket/SignalR traffic over HTTPS/TCP 443. WebSocket traffic should not be blocked by proxy, firewall or SSL inspection policies.

The LiveKit media service requirements relate to outbound connections from the candidate or user device/network to the remote invigilation media services.

Invigilate by Wayvero browser extension and mobile app requirements

REQUIREMENT	DETAILS
Browser extension requirements	Candidates must be able to install and run the required Chrome browser extension. Browser extension policies should not block communication with invigilate.wayvero.co.uk.
Mobile app requirements	Candidates will need access to the Apple App Store or Google Play Store to download the required mobile app. The mobile app must also be allowed to communicate with the web application.

Highfield Exam Platform Requirements

Candidates may also need access to the relevant Highfield exam platform used for their assessment. Where customer networks restrict access, the following domains should also be permitted.

Highfield Core

HOST / DOMAIN	PROTOCOL	PORT
*.highfieldqualifications.com	HTTPS	TCP 443
*.highfieldcore.com	HTTPS	TCP 443
cdn.highfieldqualifications.com	HTTPS	TCP 443

Highfield Works / HWorks

HOST / DOMAIN	PROTOCOL	PORT
*.highfieldworks.com	HTTPS	TCP 443

Notes for customer IT teams

- These requirements relate to outbound access from the candidate or user device/network to the listed services. Inbound firewall rules are not normally required.
- Allow access by domain or hostname where possible.
- IP addresses for cloud-hosted services may change and should not be relied on unless a static IP range has been specifically provided.
- WebSocket traffic over HTTPS/TCP 443 should be permitted.
- SSL inspection, proxy filtering, content filtering, application control or browser extension restrictions may prevent the remote invigilation session from working correctly.
- UDP traffic should be permitted where listed to support live audio and video during remote invigilated sessions.