Network firewall settings for Kaltura Meetings and Virtual Classroom

Last Modified on 07/15/2024 12:59 pm IDT

This article is designated for administrators.

About

Is your organization using a Firewall or VPN? To configure your firewall to work effectively with Kaltura's Real-Time Communication (RTC) solutions, you need to allow specific network traffic to pass through the firewall.

Checklist

To participate in Kaltura Webinars, Kaltura Meetings and Kaltura Virtual Classroom, please ensure that the network you are connecting from allows for the following:

Protocol	Ports	URL	Addresses
TCP TCP/TLS UDP	443 443 80,443	*-turn.newrow.com	3.70.195.32/27 44.199.182.96/27 3.99.123.208/28 15.228.143.96/28 35.86.65.48/28 13.214.124.16/28 3.110.59.16/28 3.38.131.128/28 3.26.132.224/28 35.76.250.144/28 16.163.33.96/28
TCP TCP/TLS UDP	443 443 80,443	*-turn.kme.kaltura.com.cn	71.131.196.48/28

⚠ TURN protocol messages should not be blocked to the above addresses.

To ensure uninterrupted real-time connections, you must allow all traffic to the following domains through any VPN, firewall, or security software:

- *.newrow.com

- *.kaltura.com
- *.kaltura.com.cn
- *.kme.kaltura.com.cn

✓ You can use this test page to test your traffic rules and see if any IPs or ports are blocking traffic from your end.

Kaltura’s Knowledge team maintains this document. Please send comments or corrections to knowledge@kaltura.com. We are committed to improving our documentation and your feedback is appreciated.