


Network firewall settings for Kaltura Meetings and Virtual Classroom

 This article is designated for administrators.


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. 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	443	*-turn.newrow.com	3.70.195.32/27
TCP/TLS	443		44.199.182.96/27
UDP	80,443		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
		*-turn.kme.kaltura.com.cn	3.26.132.224/28
			35.76.250.144/28
			16.163.33.96/28
TCP	443		71.131.196.48/28
TCP/TLS	443		
UDP	80,443		

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

It is also recommended to whitelist the following domains:

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

 You can use our test page <https://smart.newrow.com/turn-test/test/> to test your traffic rules and see if any of the IPs or ports might still be blocking traffic from your end.

This document is maintained by Kaltura's Knowledge team. Please send comments or



corrections to knowledge@kaltura.com. We are committed to improving our documentation and your feedback is appreciated.

[template("cat-subscribe")]
