Video streaming in security-conscious settings (whitelisting)

Last Modified on 02/28/2025 1:49 am EST

Video streaming in security-conscious settings (whitelisting)

Due to either your own or your customer's IT and security requirements, you may need to take special care to avoid triggering firewalls, by pre-testing your connections and whitelisting IP addresses.

The information below is offered for your convenience and may change as a result of changes to third-party platforms mentioned (e.g. Wowza, Vonage and Twilio).

AIRCast – Test the connection

To help prepare for trouble-free connection, Vonage offers this general pre-call test to evaluate network latency and bandwidth, and troubleshoot any potential problems: https://tokbox.com/developer/tools/precall/

This Vonage guide is designed to help you allow connection even when either you or your attendees are on strict networks and/or devices: https://tokbox.com/developer/guides/restricted-networks/

See elswehere in this article for RTMP – Wowza information.

Whitelisting

For Vonage, there are recommended ports and domains to whitelist, and a number of other connectivity requirements. This article has more information:

https://api.support.vonage.com/hc/en-us/articles/11117874324508-What-are-the-Vonage-Video-API-network-connectivity-requirements

Whitelisting for the OnAIR portal

The OnAIR portal has other domains that should remain unblocked (whitelisted) to help prevent connection problems. These are the minimum firewall access requirements and Wowza recommendations:

*.video.wowza.com

[your EventsAir alias here, without the square brackets].eventsair.com

azurewebsites.net

cdn3.wowza.com

endpoint.twilio.com

eventsair.com

eventsairmobileaueprod.table.core.windows.net

*.flowplayer.com

global.vss.twilio.com

gstatic.com

*.lwcdn.com

*.millicast.com

mobile-endpoint.twilio.com

msecdn.net

onairprod.azurewebsites.net

onairprod.queue.core.windows.net

opentok.com

portalapp.*ALIAS*.eventsair.com

sdkgw.us1.twilio.com

tokbox.com

twilio.com

vonage.com

windows.net

*.wowza.com

PLUS

Port 1935/1934 for RTMP (only if required) – see Wowza information below also.

Otherwise, services do not use reserved ports and communicate over 80/443/8080/8443.

If you're using Twilio for meetings or live support, you should ensure the Twilio and Vonage domains listed above are whitelisted, and also use the Twilio network test:

networktest.twilio.com

Find out more about Twilio connectivity and bandwidth requirements here:

https://help.twilio.com/articles/223180888-Twilio-Voice-JavaScript-and-Mobile-SDK-Network-Connectivity-and-Bandwidth-Requirements;

Whitelisting when using RTMP

You should refer to the latest Wowza documentation for updated information re codecs, network ports, IP addresses & Wowza RTS Platform requirements.

We have reproduced some of this information below for your convenience.

Codecs

RTMP, internet transfer protocols that can be transmuxed to WebRTC supports only the H.264 video codec.

Read more on Broadcasting to Wowza Video™ Real-Time Streaming at Scale.

Network Ports & Domains

If behind a restrictive network, use the information below to configure your firewall whitelist correctly to allow Real-time Streaming services to pass through:

Traffic Type	Ports	Type
WebRTC Connection	443	TCP
WebRTC Media Server	49152-65535	UDP
STUN/TURN Servers	443, 3478, 5349	TCP and UDP
RTMP Publishing	1935	TCP

We also recommend whitelisting the following domains:

*.wowza.com
*.flowplayer.com
*.lwcdn.com
*.cloudflare.com
*.millicast.com
*.twilio.com

IP Addresses

Publishing

Wowza has said they can't provide a definitive list of IP addresses to whitelist as, due to the dynamic scaling of the Wowza service, they can't guarantee the same range. If you need to whitelist IP ranges, Wowza recommends referring to the region-specific IP addresses lists published by cloud providers.

Region	IP Range Details
Bangalore, India	not published by provider (Digital Ocean)
Phoenix, AZ, USA	us-phoenix-1
Singapore	not published by provider (Digital Ocean)
Sydney, Australia	ap-sydney-1

* *See Oracle's IP list for a detailed IP range for publishing ingress servers.*

STUN/TURN

STUN and TURN servers are crucial in WebRTC communication, allowing users to connect and stream content effectively. These servers follow IETF standard protocols to manage Network Address Translation (NAT) during communication sessions.

The Session Traversal Utilities for NAT (STUN) assist servers and clients in determining their public IP addresses when they are behind a NAT/Firewall. When a host wants to accept an incoming connection, it provides this public IP address as a possible connection point. If the NAT/Firewall still prevents direct connectivity between the viewer and media server, a connection is established using the Traversal Using Relay around NAT (TURN) service, which enables media relay between the two parties.

STUN/TURN IP addresses were last updated 2024-11-04

Region	IP Range Details
Bangalore, India	139.59.49.50 139.59.49.86 64.225.87.21 64.225.87.66 64.225.87.164 174.138.120.21 68.183.247.136 139.59.49.159

Ashburn, VA, USA	129.213.172.222 141.148.39.122 193.122.165.132 129.80.107.22 129.80.49.52 141.148.63.222 150.230.164.20 150.136.130.194
Frankfurt, Germany	141.144.229.61 89.168.103.9 144.24.168.81 141.147.50.224 144.24.169.241 130.162.224.118 129.159.200.0 130.162.224.21
London, UK	132.226.128.169 84.8.154.194 150.230.127.97 79.72.91.241 141.147.64.72 141.147.113.177 150.230.118.111 141.147.96.45
Phoenix, AZ, USA	129.153.95.186 129.146.214.35 129.153.84.129 141.148.160.171 129.153.216.166 144.24.9.249 152.70.155.112 129.146.10.49
São Paulo, Brazil	136.248.75.56 168.138.254.134 136.248.109.105 167.234.230.239 136.248.127.209 144.22.189.247 136.248.68.90 150.230.78.100

Singapore	146.190.195.233 146.190.200.127 146.190.200.155 144.126.241.168 139.59.220.163 157.230.192.175 139.59.192.127 139.59.192.132
Sydney, Australia	192.9.182.131 192.9.177.241 192.9.181.7 192.9.176.25 159.13.38.8 159.13.55.70 158.178.143.49 152.69.174.63

In rare cases where vendor failover is required, we may use Twilio's service.
Consult the Twilio's IP list for a detailed IP range for STUN/TURN servers.

Wowza Flowplayer

Wowza Flowplayer uses several subdomains. This product is deployed within the AWS infrastructure. The Amazon AWS complete list of IP ranges are available here. Wowza also suggest checking firewall / network restrictions to enable http/3 QUIC if this option is available. Suggested subdomains for whitelisting are listed below.

- cdn.flowplayer.com
- embed-input.flowplayer.com
- embed.flowplayer.com
- embed.wowza.com
- ihi.flowplayer.com
- ljsp.lwcdn.com
- player.video.wowza.com
- player.ws.flowplayer.com
- pmi.flowplayer.com
- ptm.flowplayer.com

- sai.wowza.com
- wv-cdn-00-00.wowza.com
- wv-cdn-00-01.wowza.com