

# Video Bridge Connectivity Guide

---

## Overview

The GoTo Webinar Extensions platform is a webcast solution that has been supporting the largest global clients for over 20 years. We allow Presenters to connect in a variety of ways and broadcast out to audiences of 100,000+ while including interactive features such as slides, Q&A, polls, and surveys.

Additional features include:

|  |  |
|--|--|
| <ul style="list-style-type: none"><li>Fully branded experience</li></ul>       | <ul style="list-style-type: none"><li>Continuing Education</li></ul>                   |
| <ul style="list-style-type: none"><li>Robust reporting and analytics</li></ul> | <ul style="list-style-type: none"><li>Broadcast live, sim live, or on-demand</li></ul> |
| <ul style="list-style-type: none"><li>CRM Integrations</li></ul>               | <ul style="list-style-type: none"><li>Customized Landing pages</li></ul>               |
| <ul style="list-style-type: none"><li>Managed production services</li></ul>    |  |

## Presenter Requirements

GoTo Webinar Extensions is a broadcast product with defined roles for Presenters and participant / audience members. Network requirements for both roles can be found on our [Network Requirements](#) page. For Presenters, refer to the **Webcast Presenters - Video Events** column along the right for the requirements. Click **Notify Me About Network Updates** in the top right to sign-up to receive email updates regarding any planned network changes. We do our best to minimize updates to avoid impacting your IT and Network teams.

Please be sure to add the domain names, protocols / ports, and IP Ranges for specific to the **Video Bridge**. This will allow your Presenter(s) to connect their webcam(s) through their current Chrome, Edge Chromium, or Firefox browser using WebRTC. It is critical that the IPs are allowed, and not just the domain wild cards, because the connection is established using the ICE protocol,

which negotiates based on IP addresses.

When adding allow rules to the network, it is important to consider how the Presenter(s) will be joining and what security solutions their video/audio traffic could be traversing. For example, will Presenters be on the corporate network on off-site? If they are off-site, will they be on VPN? For Presenters off-site and on VPN, we recommend enabling split tunnel.

Firewalls also need to have allow rules enabled to have traffic flow bi-directionally in order for Presenter(s) to share their video and to see other presenters' videos.

With cloud security services (example: Zscaler) or other products such as cloud proxies, it is important to add allow rules using the information outlined in our [Network Requirements](#) page. When possible, we recommend bypassing proxies as a best practice.

Additionally, please be mindful of security software solutions (example: Netskope) that may be deployed in the corporate environment. Note: Netskope requires a list of FQDNs. Please reach out to [support@webcasts.com](mailto:support@webcasts.com) and include the associated GlobalMeet webcast event ID to receive the FQDNs.

Please review our Knowledge Base article on our [Video Bridge](#) for additional information.

---

Revision #1

Created 9 August 2024 18:45:35 by Matt Engel

Updated 9 August 2024 18:46:19 by Matt Engel