


GoTo Webinar

Minimal Firewall Settings for Using the V10 GoTo Meeting, GoTo Webinar, and GoTo Training Desktop App

Please review the minimal settings for firewall/proxy configuration that outline the IP ranges and DNS domains that must be allowed through the firewall/proxy respectively and excluded from any deep packet inspection. This is for version 10 of the classic GoTo Meeting, GoTo Webinar, and GoTo Training desktop app.

Status: Verified

This document and sample scenarios are recommendations made by the GoTo Engineering team. There are other considerations and configurations on which traffic goes through a proxy or directly through a firewall.

 **Note:** This setup has been tested to work in the GoTo network lab but may not cover all environments and scenarios.

GoTo IP Ranges

All critical media services are tied to these ranges. Ideally, they should go directly through any network perimeter and not through a proxy.

The hypothesis is that all GoTo Meeting traffic **not** going to these ranges uses plain HTTPS or WebSocket and can easily be redirected through an inspecting HTTPS proxy.

TCP port 443 (Connection)

Connection setup for all media, the download of various application parts, and Telemetry — we use TLS over plain TCP, HTTPS, as well as WebSocket.

Range	Use
23.239.228.0/22 23.239.232.0/23 23.239.234.0/23 23.239.236.0/23	VCS (Video servers)
67.217.64.0/19	VGW (Audio servers)
68.64.0.0/19	VCS (Video servers), VGW and Edge (Audio servers)
78.108.112.0/20	VCS (Video servers)
173.199.0.0/18	VCS (Video servers), VGW and Edge (Audio servers), attendee.gotowebinar.com, global.gotowebinar.com, global.gototraining.com
202.173.24.0/21	MCS (Screen sharing servers)

Range	Use
216.115.208.0/20	VGW (Audio servers), egwglobal.gotomeeting.com, egw.gotomeeting.com (Connection detection)

UDP port 1853, 8200 (Audio/Video)

If these UDP ports are not open, GoTo Meeting will fall back to TCP (which may affect media and connection quality). We run encrypted, non-standard traffic on these connections so any firewall trying to detect something smart will fail

Range	Use
23.239.228.0/22 23.239.232.0/23 23.239.234.0/23 23.239.236.0/23	VCS (Video servers)
67.217.64.0/19	VGW (Audio servers)
68.64.0.0/19	VCS (Video servers), VGW (Audio servers), see TCP
78.108.112.0/20	VCS (Video servers)
173.199.0.0/18	VCS (Video servers), VGW (Audio servers) see TCP
216.115.208.0/20	VGW (Audio servers)

Domains

The list of domains used by the GoTo Meeting, GoTo Webinar, and GoTo Training desktop app currently includes (but is not limited to) the following:

Domain	Use	Points to IP addresses in	
1	*.goto.com	Central domain for starting sessions	AWS
2	*.getgo.com	Various services	AWS
3	*.gotomeeting.com	Various services	GoTo/AWS
4	*.expertcity.com	Audio and Screen sharing servers	GoTo
5	*.goto-rtc.com	Audio and Video servers	GoTo
6	*.logmeininc.com	Authentication (critical)	AWS

Domain	Use	Points to IP addresses in	
7	*.gotowebinar.com	Central domain (required for GoToWebinar only)	GoTo/AWS
8	*.gototraining.com	Central domain (required for GoTo Training only)	GoTo
9	*.launchdarkly.com	External service provider for feature enablement (does not work through proxy, not critical)	Google Cloud
10	api-pub.mltree.net	GoTo Marketing (not critical)	AWS

GoTo Opener

This is a separate program used to download and start native GoTo Meeting. It uses the following domains (HTTPS, port 443 TCP).

Domain	Use	Points to IP addresses in
launch.getgo.com	Conference Launch Service	GoTo
join.servers.getgo.com	Conference Launch Service	AWS
builds.cdn.getgo.com	Download CDN for GoTo Meeting builds	AWS
builds.getgocdn.com	Download CDN for GoTo Meeting builds	GoTo

General network configuration modes

In an unrestricted network, GoTo Meeting will open a number of TCP and UDP connections to a variety of ports, some of them essential e.g., to transmit audio data and others non-essential e.g., the one for marketing pop-ups. The first eight (8) domains in the list above need to be excluded from deep packet inspection, if there are any on the network path.

Furthermore, the connections initiated by GoTo Meeting can be split into three (3) categories:


- TCP towards GoTo IP ranges
- UDP towards GoTo IP ranges
- TCP towards other IP ranges (currently AWS and Google Cloud address spaces)

Based on this distinction, there are four (4) different ways to configure your network.

Mode	Pros & Cons	Configuration steps

Mode	Pros & Cons	Configuration steps
<p>All TCP using port 443 over HTTPS proxy, no use of UDP</p>	<p>Pros This is the simplest configuration mode.</p> <p>Cons</p> <ul style="list-style-type: none"> • The exclusive use of TCP for media can lead to bad audio and video quality and interruptions (if there is any packet loss on the underlying IP connection from the client machine to the GoTo servers). As the majority of servers are US-based, this will impact customers outside of the United States. • Connection establishment takes longer in unrestricted networks due to extended probing. 	<ol style="list-style-type: none"> 1. On your firewall, block the following: <ul style="list-style-type: none"> • All outbound TCP traffic towards port 443, 80, and 8200. • All outbound UDP traffic towards port 1853 and 8200. 2. On client computers, configure a HTTPS proxy for port 443.

Mode	Pros & Cons	Configuration steps
<p>All TCP using port 443 over HTTPS proxy, UDP goes directly through the firewall</p>	<p>Pros</p> <ul style="list-style-type: none"> • Media can use UDP which improves perceived audio and video quality. • It is comparably easier to configure and debug as TCP and UDP is clearly separated. <p>Cons</p> <p>Connection establishment takes longer than in unrestricted networks due to extended probing.</p>	<ol style="list-style-type: none"> 1. On your firewall, configure the following: <ul style="list-style-type: none"> • Block all outbound TCP traffic towards ports 443, 80, and 8200. • Allow outbound UDP traffic towards ports 1853 and 8200 (you may also restrict the address ranges to the GoTo IP ranges for UDP listed above). 2. On client computers, configure a HTTPS proxy.
<p>TCP and UDP towards GoTo IP ranges goes directly through the firewall, TCP to other IP ranges goes through HTTPS proxy</p>	<p>Pros</p> <p>Best media and screen sharing performance, quick connection establishment.</p> <p>Cons</p> <p>Configuration is more complex and harder to debug.</p>	<ol style="list-style-type: none"> 1. On your firewall, configure the following: <ul style="list-style-type: none"> • Allow outbound TCP traffic towards port 443 only for the address ranges designated in GoTo IP ranges for TCP above. • Block all other outbound TCP traffic towards port 443, 80, and 8200.

Mode	Pros & Cons	Configuration steps
		<ul style="list-style-type: none"> Allow outbound UDP traffic towards port 1853 and 8200 – you may also restrict the address ranges to the LMI IP ranges for UDP list above. <p> Note: Make sure that inbound return traffic is also passed through (stateful).</p> <p>2. On client computers, configure a HTTPS proxy.</p>
<p>Run a stateful firewall and allow all outbound TCP and UDP traffic and return traffic based on state</p>	<p>Pros No configuration required as all traffic is initiated from the client. The firewall will open the required inbound connections automatically.</p> <p>Cons This is the default configuration for many firewalls, but rarely used in more complex networks due to additional security requirements.</p>	<p>Does not need additional configuration.</p>

VPN configuration

If you use a VPN, there are several ways to route the different streams. The options reflect the modes listed in the table above; however, you will have to use routing to decide which traffic goes where (which makes it difficult to separate UDP from TCP traffic).

For this reason, we recommend one of the following options:

- Route everything through the VPN tunnel.
- Allow all GoTo IP ranges to go directly to the Internet (TCP and UDP), send all other traffic through the VPN.

- Send only internal traffic (i.e., 10.X.X.X and 192.168.X.X) into the VPN tunnel, and send the rest directly to the internet.

TCP traffic sent through the VPN tunnel may or may not go through a proxy after traversing through the tunnel. There are other configurations that can be discussed with the GoTo Engineering team on a case-by-case basis.

Proxy configuration notes

If your proxy is performing deep packet inspection, please be sure that all domains listed above are allowlisted. Deep packet inspection can impact the initial TLS connection and slow down media streams due to processing delays. Although GoTo Meeting reads many sources for proxy configuration (e.g., system proxy, Firefox proxy, PAC files, WPAD), the proxy detection might yield unexpected results. One aspect is that the logic used to parse PAC files does not support all variations of possible rules. The other aspect is that proxies stored in the GoTo Meeting registry are sometimes used in the connection detection. As soon as GoTo Meeting finds out it can establish a connection through a stored proxy, it might also use it, although other configurations might indicate another proxy.

The easiest way to verify proxy usage is through the GoTo Meeting log file.

macOS and Mac OS X

Log files are stored here: `/Users/username/Library/Logs/com.logmein.GoToMeeting`.

To clear existing proxy entries, delete these keys: `defaults -currentHost read com.logmein.GoToMeeting |grep ConnectionInfo`.

Windows

Log files are stored here: `%Temp%\LogMeInLogs\GoToMeeting`. Look for the folder with the latest date.

To clear existing proxy entries, delete these keys:

`HKEY_CURRENT_USER\SOFTWARE\LogMeInInc\GoToMeeting\ConnectionInfo`.