

# Firewall Requirements (Business Edition)

## Overview

To use the CrisisGo app and related features within your organization network, the outgoing traffic from your network to the IP addresses, corresponding domain names, and third-party services listed in this section must be allowed.

## IP Addresses

Please make sure **all traffic** to the following IP addresses and ports are permitted within all your network security appliances, including router, firewall, etc.

Category	IP Address	Protocol: Port	Description
<b>REQUIRED</b>	34.200.34.240 34.199.19.160	TCP:443  Please also whitelist the Jabber/XMPP or Google Talk application in your firewall if applicable.	CrisisGo real-time app communication traffic based on XMPP.
<b>REQUIRED</b>	75.2.42.231 99.83.198.240	TCP:443	HTTPS traffic.

## Domain Names

Please make sure **all the required** Domain Names / URLs are permitted within all your network security appliances, including router, firewall, etc, and allow feature-specific Domain Names / URLs as needed.

Category	Product / Feature	Domain Name / URL	Description
<b>REQUIRED</b>	CrisisGo Platform	<ul style="list-style-type: none"><li>https://icontrol.crisisgo.net</li><li>https://crisisgo.net</li><li>https://http-login.crisisgoapps.com</li><li>https://http-server-11400002.crisisgo.net</li><li>https://forgotpassword.crisisgo.com</li><li>https://integration.crisisgo.net</li><li>https://saml.crisisgo.net</li><li>https://signup.org.crisisgo.net</li><li>https://capi.crisisgo.net</li><li>https://sapi.crisisgo.net</li><li>https://webapp.crisisgo.net</li><li>https://url.crisisgo.net</li><li>https://wss.crisisgo.net</li></ul>	CrisisGo Platform's basic domain names and URLs are required to be whitelisted.
<b>RECOMMENDED</b>	CrisisGo Platform	<ul style="list-style-type: none"><li>*.crisisgo.net</li><li>*.crisisgo.com</li><li>*.crisisgoapps.com</li></ul>	It is highly recommended to whitelist all the subdomains for the above basic domain names.
<b>OPTIONAL</b>	Threat Assessment	<ul style="list-style-type: none"><li>https://assessment.crisisgo.net</li></ul>	If your organization needs to use these features, please whitelist as needed.
<b>OPTIONAL</b>	Safety iPass, Report	<ul style="list-style-type: none"><li>https://report.crisisgo.net</li></ul>	
<b>OPTIONAL</b>	Safety CheckIn	<ul style="list-style-type: none"><li>https://report.crisisgo.net</li><li>https://checkin.crisisgo.net</li><li>https://checkin-admin.crisisgo.net</li></ul>	

## Third-Party Services

CrisisGo uses some third-party services (e.g. Amazon S3), so you will also need to whitelist those services, IP addresses, and domains for the respective features to function well.

Category	Product / Feature	Service	Description
----------	-------------------	---------	-------------

<b>REQUIRED</b>	CrisisGo Offline Messages for iOS and Mac.	Apple Push Notification Service (APNs)	<p>CrisisGo uses the APNs to push offline notifications to the user when the CrisisGo app is offline on their iOS and Mac devices.</p> <p>Please follow Apple's instruction to whitelist its ports and hosts <a href="#">APNs Required Ports and Hosts</a></p>
<b>REQUIRED</b>	CrisisGo Offline Messages for Android.	Google Firebase Cloud Messaging (FCM)	<p>CrisisGo uses the FCM to push offline notifications to the user when the CrisisGo app is offline on their Android devices.</p> <p>Please follow Google's instruction to whitelist its ports and hosts <a href="#">FCM Ports and Your Firewall</a></p>
<b>OPTIONAL</b>	CrisisGo videos in Safety Awareness, Training Center, and Safety News.	Amazon S3	<p>CrisisGo uses Amazon S3 to store our video files used in Training Center, Safety News, etc.</p> <p>If your organization needs to use these features, please whitelist the Amazon S3 domain <a href="#">s3.amazonaws.com</a>, <a href="#">port 443</a>.</p> <p>If you are implementing IP-based firewall rules, you can get the IP address ranges used by Amazon S3 here <a href="#">How can I find the IP address ranges used by Amazon S3?</a></p>