

Disclaimer

Legal disclaimer

This guide and its contents (the "Guide") are provided by NXGEN. All rights to the Guide and to the intellectual property embodied in it — including, without limitation, trademarks, trade names, logos and similar marks appearing in or on it — are protected by law. All right, title and interest in the Guide and in any related intellectual property rights belong to and remain with NXGEN and its licensors.

The Guide is provided free of charge, "as is" and for informational purposes only, without warranty of any kind. It is neither intended nor suitable to establish any legal relationship between the reader and NXGEN or its affiliates, including, without limitation, any obligation of NXGEN or its affiliates toward the reader.

The obligations of NXGEN and its affiliates in respect of NXGEN products or services purchased by a customer are governed exclusively by the terms of the agreement under which those products or services were purchased.

For clarification

The reader bears the entire risk as to the use, results and performance of the Guide. To the fullest extent permitted by applicable law, NXGEN disclaims and excludes all warranties, whether statutory, express or implied — including, without limitation, implied warranties of merchantability, fitness for a particular purpose, title and non-infringement of third-party rights — as well as any liability or warranty arising from suggestions, specifications or samples related to the Guide.

IP Whitelisting

Updated 11 August 2026

What IP Whitelisting Does

IP Whitelisting ensures that GCXONE servers can communicate securely with customer devices over the internet. By allowing only the specified IP addresses and ports, customers can maintain a secure and controlled network environment while enabling full platform functionality.

Why It Matters

Without proper IP whitelisting, GCXONE may be unable to reach devices behind customer firewalls, resulting in failed connections, missing alarms, and unavailable video streams. Whitelisting the required IPs guarantees seamless connectivity between customer devices and GCXONE infrastructure.

How It Works

Mandatory IPs

The following IP addresses must be whitelisted for all customers regardless of device type:

IP ADDRESS	PURPOSE
18.185.17.113	Genesis Primary Gateway
3.124.50.242	Genesis Secondary Gateway
3.126.237.150	Streaming Primary Gateway
3.75.73.51	Streaming Secondary Gateway
18.156.39.63	Streaming Secondary Gateway
3.127.50.212	Messaging Services

Device-Specific IPs

In addition to the mandatory IPs, customers must whitelist the following IPs based on their device type:

DEVICE	IP ADDRESS	PURPOSE
Camect	3.122.169.231	Camect Alarm Receiver Gateway
Dahua	52.59.60.20	Dahua Alarm Receiver Gateway
Hikvision	35.156.60.98	Hikvision Alarm Receiver Gateway
Hanwha	18.184.110.24	Hanwha Alarm Receiver Gateway
Milestone	3.66.98.181	Milestone Alarm Receiver Gateway
Uniview	18.158.140.99	Uniview Alarm Receiver Gateway
Heitel	3.123.206.197	Heitel Gateway 1 (Live Video)
Heitel	3.124.38.48	Heitel Gateway 2 (Events)
ADPRO	Upon request	ADPRO Alarm Receiver Gateway

Key Capabilities

Talos Customers

Customers using Evalink Talos must additionally whitelist the following:

Inbound Connections

- 195.8.103.10
- 195.8.103.11
- 195.8.103.12
- 193.151.94.10
- 193.151.94.11
- 193.151.94.12

Outbound Connections

- 91.240.18.20

- 91.240.19.20

Wildcard Allow-List

- *.evalink.io
- *.talos-app.io
- *.eu.auth0.com

Port Enabling Guidelines

For customers using public devices, the required ports depend on the specific device type. The following port types must be enabled based on the customer's setup:

- Web console ports
- Server ports
- RTSP ports

Any custom port-forwarded ports configured at the customer's environment IP Whitelisting (Wildcard Support)

Domains, Ports and Protocols

For Firewalls that Support Wildcard Domain Whitelisting

IP/DOMAIN	PORT	PROTOCOL	PURPOSE
*.nxgen.cloud	443	HTTPS	Genesis Web App Access
*.eu.auth0.com	443	HTTPS	Auth0 Login Access
*.auth0.com	443	HTTPS	Genesis Web App Dependency
*.cloudflare.com	443	HTTPS	Genesis Web App Dependency
*.fontawesome.com	443	HTTPS	Genesis Web App Dependency

unpkg.com	443	HTTPS	Genesis Web App Dependency
*.googleapis.com	443	HTTPS	Genesis Web App Dependency
*.what3words.com	443	HTTPS	Genesis Web App Dependency
fonts.gstatic.com	443	HTTPS	Genesis Web App Dependency
*.amazonaws.com	443	HTTPS	Genesis Web App Dependency
*.evalink.io	443	HTTPS	Talos CMS Web Application
meetbeta.nxgen.cloud (3.126.237.150)	1880 10000 to 10500	HTTP/S WSS	Genesis Streaming Server Individual Streaming Agents to handle multiple streaming requests
meetbeta02.nxgen.cloud (3.75.73.51)	80	443 14891	HTTP/S HTTPS
monitor.nxgen.cloud (3.127.50.212)	80	443 1883	HTTP/S MQTT
streaming03.nxgen.cloud (18.156.39.63)	1880 8005 to 9005	51984	HTTP/S HTTP/STCP/UDP
*.twilio.com	443	HTTPS	Genesis VOIP Manager
*.us1.twilio.com	443	HTTPS	Genesis VOIP Agent
*.sip.twilio.com	443	HTTPS	Genesis VOIP Agent
registry.npmjs.org	443	HTTPS	Genesis Dependency Management
*.hik-partner.com	443	HTTPS	Hik Partner Access
open.dolynkcloud.com	443	HTTPS	Dahua DoLynk Portal Access
18.158.38.178	1880	19225 to 19232	19245

Note

Other than the above Domains, Ports and Protocols, in case if the user is trying to access Customer's devices (for ex. hikvision), its IP might be public/VPN based, those customer IP, Ports and Protocols need to be added in the whitelist/rules to make sure Genesis Access those devices in Peer-2-Peer mode to enable faster streaming access.

For Firewalls that Do Not Support Wildcard Domain Whitelisting

IP/DOMAIN	PORT	PROTOCOL	PURPOSE
tenantname.nxgen.cloud	443	HTTPS	Genesis Web Application Access
api.nxgen.cloud	443	HTTPS	API Access for Genesis Web
nxgen.eu.auth0.com	443	HTTPS	Auth0 Login Access
cdn.auth0.com	443	HTTPS	Genesis Web App Dependency
cdn.eu.auth0.com	443	HTTP	Genesis Web App Dependency
cdnjs.cloudflare.com	443	HTTPS	Genesis Web App Dependency
use.fontawesome.com	443	HTTPS	Genesis Web App Dependency
unpkg.com	443	HTTPS	Genesis Web App Dependency
maps.googleapis.com	443	HTTPS	Genesis Web App Dependency
khms0.googleapis.com	443	HTTPS	Genesis Web App Dependency
khms1.googleapis.com	443	HTTPS	Genesis Web App Dependency
assets.what3words.com	443	HTTPS	Genesis Web App Dependency
fonts.googleapis.com	443	HTTPS	Genesis Web App Dependency

fonts.gstatic.com	443	HTTPS	Genesis Web App Dependency
events-snapshots.s3-eu-central-1.amazonaws.com	443	HTTPS	Genesis Web App Dependency
nxgen-multi-language.s3-eu-central-1.amazonaws.com	443	HTTPS	Genesis Web App Dependency
nxgen-organization-images.s3-eu-central-1.amazonaws.com	443	HTTPS	Genesis Web App Dependency
nxg-reference-img-upload-test.s3-eu-central-1.amazonaws.com	443	HTTPS	Genesis Web App Dependency
nxgen-sensor-icons.s3-eu-central-1.amazonaws.com	443	HTTPS	Genesis Web App Dependency
talos.evalink.io	443	HTTPS	Talos CMS Web Application
login.evalink.io	443	HTTPS	Talos CMS Web App Dependency
sitasys-prod.eu.auth0.com	443	HTTPS	Talos CMS Web App Dependency
assets.what3words.com	443	HTTPS	Genesis Web App Dependency
insightsbeta.nxgen.cloud	443	HTTPS	Genesis Web App Dependency
insightsbeta02.nxgen.cloud	443	HTTPS	Genesis Web App Dependency
meetbeta.nxgen.cloud (3.126.237.150)	1880	HTTP/S	Genesis Streaming Server
meetbeta.nxgen.cloud (3.126.237.150)	10000 to 10500	WSS	Individual Streaming Agents to handle multiple streaming requests
meetbeta02.nxgen.cloud (3.75.73.51)	80	443	HTTP/S
meetbeta02.nxgen.cloud (3.75.73.51)	14891	HTTPS	WSS
monitor.nxgen.cloud (3.127.50.212)	80	443	HTTP/S
monitor.nxgen.cloud (3.127.50.212)	1883	MQTT	Genesis Alerts Service
streaming.nxgen.cloud	443	HTTPS	Genesis Streaming Server Fallback

streaming03.nxgen.cloud (18.156.39.63)	1880	HTTP/S	Genesis Proprietary Streaming Service
streaming03.nxgen.cloud (18.156.39.63)	8005-9005	51984	HTTP/S
sdk.twilio.com	443	HTTPS	Genesis VOIP Manager
chunderw-vpc-gll.twilio.com	443	HTTPS	Genesis VOIP Agent
eventgw.us1.twilio.com	443	HTTPS	Genesis VOIP Agent
genesisaudio.sip.twilio.com	443	HTTPS	Genesis VOIP Agent
registry.npmjs.org	443	HTTPS	Genesis Dependency Management
ieu.hik-partner.com	443	HTTPS	Hik Partner Access
open.dolynkcloud.com	443	HTTPS	Dahua DoLynk Portal Access
18.158.38.178	1880	19225 to 19232	19245

Note

Other than the above Domains, Ports and Protocols, in case if the user is trying to access Customer's devices (for ex. hikvision), its IP might be public/VPN based, those customer IP, Ports and Protocols need to be added in the whitelist/rules to make sure Genesis Access those devices in Peer-2-Peer mode to enable faster streaming access.

Real-World Use Cases

- A new customer onboards with Hikvision NVRs — the IT team whitelists the mandatory IPs plus the Hikvision-specific IP before go-live, ensuring alarms and video streams reach GCXONE without interruption.
- A customer using Evalink Talos cannot receive alarm dispatches — IT discovers the Talos inbound IPs are blocked by the corporate firewall and adds them to the whitelist.
- A customer's firewall supports wildcard domain whitelisting — IT uses the *.evalink.io and *.talos-app.io entries instead of managing individual IPs.

Best Practices

- Always whitelist the mandatory IPs first before adding device-specific IPs — these are required for all customers regardless of device type.
- Whitelist device-specific IPs based on the exact device type deployed — do not whitelist IPs for devices that are not in use.
- For Talos customers, whitelist both inbound and outbound IPs — missing either direction will break alarm delivery.
- Contact support before go-live to obtain the ADPRO Alarm Receiver Gateway IP if ADPRO devices are in use.