

Disclaimer

Juridische disclaimer

Deze gids en de inhoud ervan (de "Gids") worden aangeboden door NXGEN. Alle rechten op de Gids en op de daarin vervatte intellectuele eigendom — met inbegrip van, maar niet beperkt tot, merken, handelsnamen, logo's en vergelijkbare tekens in of op de Gids — worden beschermd door de wet. Alle rechten, aanspraken en belangen met betrekking tot de Gids en de bijbehorende intellectuele-eigendomsrechten berusten en blijven bij NXGEN en zijn licentiegevers.

De Gids wordt kosteloos, "zoals deze is" en uitsluitend ter informatie verstrekt, zonder enige garantie. De Gids is niet bedoeld en evenmin geschikt om enige rechtsverhouding tot stand te brengen tussen de lezer en NXGEN of zijn gelieerde ondernemingen, met inbegrip van, maar niet beperkt tot, enige verplichting van NXGEN of zijn gelieerde ondernemingen jegens de lezer.

De verplichtingen van NXGEN en zijn gelieerde ondernemingen met betrekking tot door een klant afgenomen NXGEN-producten of -diensten worden uitsluitend beheerst door de voorwaarden van de overeenkomst waaronder die producten of diensten zijn afgenomen.

Ter verduidelijking

De lezer draagt het volledige risico ten aanzien van het gebruik, de resultaten en de prestaties van de Gids. Voor zover toegestaan door het toepasselijke recht wijst NXGEN alle garanties af, hetzij wettelijk, uitdrukkelijk of stilzwijgend — met inbegrip van, maar niet beperkt tot, stilzwijgende garanties van verhandelbaarheid, geschiktheid voor een bepaald doel, eigendom en niet-inbreuk op rechten van derden — evenals iedere aansprakelijkheid of garantie die voortvloeit uit suggesties, specificaties of voorbeelden met betrekking tot de Gids.

IP-whitelisting

Updated 11 August 2026

Wat een IP-whitelist doet

Met IP-whitelisting wordt gewaarborgd dat GCXONE-servers via internet veilig kunnen communiceren met de apparaten van klanten. Door uitsluitend de opgegeven IP-adressen en poorten toe te staan, kunnen klanten een veilige en gecontroleerde netwerkomgeving handhaven en tegelijkertijd de volledige functionaliteit van het platform benutten.

Waarom dit belangrijk is

Zonder een correcte whitelist voor IP-adressen kan GCXONE mogelijk geen verbinding maken met apparaten achter de firewalls van klanten, wat kan leiden tot mislukte verbindingen, ontbrekende alarmen en onbeschikbare videostreams. Door de benodigde IP-adressen op de whitelist te plaatsen, wordt een naadloze verbinding tussen de apparaten van klanten en de infrastructuur van GCXONE gegarandeerd.

Hoe het werkt

Verplichte IP-adressen

De volgende IP-adressen moeten voor alle klanten op de witte lijst worden geplaatst, ongeacht het type apparaat:

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

Apparaatspecifieke IP-adressen

Naast de verplichte IP-adressen moeten klanten de volgende IP-adressen op basis van hun apparaattype op de witte lijst zetten:

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

Belangrijkste mogelijkheden

Klanten van Talos

Klanten die Evalink Talos gebruiken, moeten bovendien de volgende adressen op de witte lijst zetten:

Inkomende verbindingen

- 195.8.103.10
- 195.8.103.11
- 195.8.103.12
- 193.151.94.10
- 193.151.94.11

- 193.151.94.12

Uitgaande verbindingen

- 91.240.18.20
- 91.240.19.20

Wildcard-toegangslijst

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

Richtlijnen voor het inschepen

Voor klanten die gebruikmaken van openbare apparaten, zijn de vereiste poorten afhankelijk van het specifieke type apparaat. Afhankelijk van de configuratie van de klant moeten de volgende poorttypes worden ingeschakeld:

- Webconsole-poorten
- Serverpoorten
- RTSP-poorten

Alle aangepaste poorten voor poortdoorsturing die in de omgeving van de klant zijn geconfigureerd

IP-whitelisting (ondersteuning voor jokertekens)

Domeinen, poorten en protocollen

Voor firewalls die het toevoegen van domeinen aan de witte lijst met jokertekens ondersteunen

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

Opmerking

Naast de hierboven genoemde domeinen, poorten en protocollen geldt dat, indien de gebruiker toegang probeert te krijgen tot apparaten van de klant (bijv. Hikvision), het IP-adres van de gebruiker openbaar of via een VPN kan zijn; deze IP-adressen van de klant, poorten en protocollen moeten aan de whitelist of regels worden toegevoegd om ervoor te zorgen dat Genesis toegang krijgt tot die apparaten in Peer-2-Peer-modus, zodat snellere streamingtoegang mogelijk is.

Voor firewalls die het toevoegen van domeinen aan de witte lijst met jokertekens niet ondersteunen

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

Naast de hierboven genoemde domeinen, poorten en protocollen geldt het volgende: als de gebruiker toegang probeert te krijgen tot apparaten van de klant (bijv. Hikvision), kan het IP-adres van de gebruiker openbaar of via een VPN zijn; deze IP-adressen van de klant, poorten en protocollen moeten aan de whitelist of de regels worden toegevoegd om ervoor te zorgen dat Genesis toegang krijgt tot die apparaten in Peer-2-Peer-modus, zodat snellere streaming mogelijk is.

Praktijkvoorbeelden

- Een nieuwe klant gaat aan de slag met NVR's van Hikvision — het IT-team voegt de verplichte IP-adressen en het Hikvision-specifieke IP-adres toe aan de whitelist vóór de ingebruikname, zodat alarmen en videostreams zonder onderbreking bij GCXONE terechtkomen.

- Een klant die Evalink Talos gebruikt, kan geen alarmmeldingen ontvangen — de IT-afdeling ontdekt dat de inkomende IP-adressen van Talos door de bedrijfsfirewall worden geblokkeerd en voegt ze toe aan de whitelist.
- De firewall van een klant ondersteunt het toevoegen van domeinen aan de whitelist met jokertekens — de IT-afdeling gebruikt de vermeldingen *.evalink.io en *.talos-app.io in plaats van afzonderlijke IP-adressen te beheren.

Beste praktijken

- Zet de verplichte IP-adressen altijd eerst op de witte lijst voordat u apparaatspecifieke IP-adressen toevoegt — deze zijn voor alle klanten verplicht, ongeacht het type apparaat.
- Zet apparaatspecifieke IP-adressen op de witte lijst op basis van het exacte type apparaat dat in gebruik is — zet geen IP-adressen op de witte lijst voor apparaten die niet in gebruik zijn.
- Voor Talos-klanten geldt dat zowel inkomende als uitgaande IP-adressen op de whitelist moeten worden geplaatst — als een van beide richtingen ontbreekt, wordt de alarmverzending verstoord.
- Neem vóór de ingebruikname contact op met de helpdesk om het IP-adres van de ADPRO-alarmontvanger-gateway te verkrijgen, indien er ADPRO-apparaten in gebruik zijn.