

Haftungsausschluss

Rechtlicher Hinweis

Dieser Leitfaden und seine Inhalte (der „Leitfaden“) werden von NXGEN bereitgestellt. Alle Rechte am Leitfaden und am darin verkörperten geistigen Eigentum — einschließlich, aber nicht beschränkt auf Marken, Handelsnamen, Logos und ähnliche Kennzeichen im oder am Leitfaden — sind gesetzlich geschützt. Sämtliche Rechte, Ansprüche und Anteile am Leitfaden und an damit verbundenen Schutzrechten verbleiben bei NXGEN und seinen Lizenzgebern.

Der Leitfaden wird unentgeltlich, „wie besehen“ und ausschließlich zu Informationszwecken bereitgestellt, ohne jegliche Gewährleistung. Er ist weder dazu bestimmt noch geeignet, ein Rechtsverhältnis zwischen dem Leser und NXGEN oder seinen verbundenen Unternehmen zu begründen, einschließlich, aber nicht beschränkt auf Verpflichtungen von NXGEN oder seinen verbundenen Unternehmen gegenüber dem Leser.

Die Verpflichtungen von NXGEN und seinen verbundenen Unternehmen in Bezug auf von einem Kunden erworbene NXGEN-Produkte oder -Dienstleistungen richten sich ausschließlich nach den Bedingungen des Vertrags, unter dem diese Produkte oder Dienstleistungen erworben wurden.

Zur Klarstellung

Der Leser trägt das gesamte Risiko hinsichtlich der Nutzung, der Ergebnisse und der Leistung des Leitfadens. Soweit gesetzlich zulässig, schließt NXGEN alle Gewährleistungen aus, ob gesetzlich, ausdrücklich oder stillschweigend — einschließlich, aber nicht beschränkt auf stillschweigende Gewährleistungen der Marktgängigkeit, der Eignung für einen bestimmten Zweck, des Rechtsbestands und der Nichtverletzung von Rechten Dritter — sowie jegliche Haftung oder Gewährleistung aus Vorschlägen, Spezifikationen oder Mustern im Zusammenhang mit dem Leitfaden.

IP-Whitelisting

Updated 11 August 2026

Was IP-Whitelisting bewirkt

Durch die IP-Whitelist wird sichergestellt, dass GCXONE-Server über das Internet sicher mit den Geräten der Kunden kommunizieren können. Indem nur die angegebenen IP-Adressen und Ports zugelassen werden, können Kunden eine sichere und kontrollierte Netzwerkumgebung aufrechterhalten und gleichzeitig den vollen Funktionsumfang der Plattform nutzen.

Warum das wichtig ist

Ohne eine ordnungsgemäße IP-Whitelist kann GCXONE möglicherweise nicht auf Geräte hinter den Firewalls der Kunden zugreifen, was zu Verbindungsfehlern, fehlenden Alarmen und nicht verfügbaren Videostreams führen kann. Die Aufnahme der erforderlichen IP-Adressen in die Whitelist gewährleistet eine nahtlose Verbindung zwischen den Geräten der Kunden und der GCXONE-Infrastruktur.

Obligatorische IP-Adressen

Die folgenden IP-Adressen müssen für alle Kunden unabhängig vom Gerätetyp auf die Whitelist gesetzt werden:

- 18.185.17.113 – Genesis-Primärgateway
- 3.124.50.242 – Sekundäres Genesis-Gateway
- 3.126.237.150 – Primäres Streaming-Gateway
- 3.75.73.51 – Sekundäres Streaming-Gateway
- 18.156.39.63 – Sekundäres Streaming-Gateway
- 3.127.50.212 – Messaging-Dienste

Gerätespezifische IPs

Zusätzlich zu den obligatorischen IP-Adressen müssen Kunden je nach Gerätetyp die folgenden

IP-Adressen auf die Whitelist setzen:

Camect

- 3.122.169.231 – Camect-Alarmempfänger-Gateway

Dahua

- 52.59.60.20 – Dahua-Alarmempfänger-Gateway

Hikvision

- 35.156.60.98 – Hikvision-Alarmempfänger-Gateway

Hanwha

- 18.184.110.24 – Hanwha Alarmempfänger-Gateway

Meilenstein

- 3.66.98.181 – Milestone-Alarmempfänger-Gateway

Uniview

- 18.158.140.99 – Uniview-Alarmempfänger-Gateway

Heitel

- 3.123.206.197 – Heitel Gateway 1 (Live-Video)
- 3.124.38.48 – Heitel Gateway 2 (Ereignisse)

ADPRO

- Die IP-Adresse des ADPRO-Alarmempfänger-Gateways wird auf Anfrage mitgeteilt

Talos-Kunden

Kunden, die Evalink Talos nutzen, müssen zusätzlich Folgendes auf die Whitelist setzen:

Eingehende Verbindungen

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

Ausgehende Verbindungen

- 91.240.18.20
- 91.240.19.20

Wildcard-Zulassungsliste

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

Richtlinien zur Portfreigabe

Bei Kunden, die öffentliche Geräte nutzen, hängen die erforderlichen Ports vom jeweiligen Gerätetyp ab.

Je nach Konfiguration des Kunden müssen die folgenden Porttypen aktiviert werden:

- Webkonsole-Ports
- Server-Ports
- RTSP-Ports

Alle benutzerdefinierten Ports, die in der Umgebung des Kunden für die Portweiterleitung konfiguriert wurden IP-Whitelisting (Unterstützung von Platzhaltern)

Domains, Ports und Protokolle

Für Firewalls, die die Whitelisting-Funktion mit Platzhaltern für Domänen unterstützen

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

Hinweis

Abgesehen von den oben genannten Domänen, Ports und Protokollen müssen, falls der Benutzer versucht, auf Geräte des Kunden (z. B. Hikvision) zuzugreifen, deren IP-Adressen – unabhängig davon, ob es sich um öffentliche oder VPN-basierte Adressen handelt – in die Whitelist bzw. die Regeln aufgenommen werden, um sicherzustellen, dass Genesis im Peer-to-Peer-Modus auf diese Geräte zugreifen kann und so einen schnelleren Streaming-Zugang ermöglicht.

Für Firewalls, die keine Whitelists mit Platzhalter-Domains unterstützen

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

Abgesehen von den oben genannten Domänen, Ports und Protokollen müssen, falls der Benutzer versucht, auf Geräte des Kunden (z. B. Hikvision) zuzugreifen, deren IP-Adressen – unabhängig davon, ob es sich um öffentliche oder VPN-basierte Adressen handelt – in die Whitelist bzw. die Regeln aufgenommen werden, um sicherzustellen, dass Genesis im Peer-to-Peer-Modus auf diese Geräte zugreifen kann und so einen schnelleren Streaming-Zugang ermöglicht.

Weiterführende Ressourcen

- Informationen zur Konfiguration der Firewall finden Sie unter Firewall-Konfiguration
- Informationen zu den Netzwerkanforderungen finden Sie unter Netzwerkeinrichtung
- Informationen zur Kontaktaufnahme mit dem Support finden Sie unter [Support kontaktieren](#)