

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.

Opleiding voor beheerders

Updated 14 August 2026

Wat Admin Training Bestrijkt

Admin Training leidt nieuwe beheerders door alles wat nodig is om GCXONE in te zetten, configureren en onderhouden — van eerste inloggen tot dagelijkse operationele routines. Deze handleiding bestrijkt netwerkvereisten, systeemarchitectuurconfiguratie, taken vóór lancering en doorlopende controlefrequenties.

Waarom Dit Belangrijk Is

Een verkeerd geconfigureerde implementatie — ontbrekende rollen, niet-toegewezen sites of niet-gecontroleerde camerastatus — leidt tot operationele storingen die achteraf moeilijk zijn na te trekken. Het volgen van het gestructureerde trainingspad garandeert dat elke beheerder vanuit een solide, gevalideerde basis begint.

Hoe Het Werkt

Pre-Deployment: Browser- en Netwerkvereisten

Browservereisten:

BROWSER	ONDERSTEUNINGSNIVEAU
Google Chrome v90+	Optimaal (aanbevolen)
Mozilla Firefox v88+	Ondersteund
Microsoft Edge v90+ (Chromium)	Ondersteund
Apple Safari v14+	Beperkt
Internet Explorer (elke versie)	Geblokkeerd. Niet ondersteund

Firewall- en Poortvereisten:

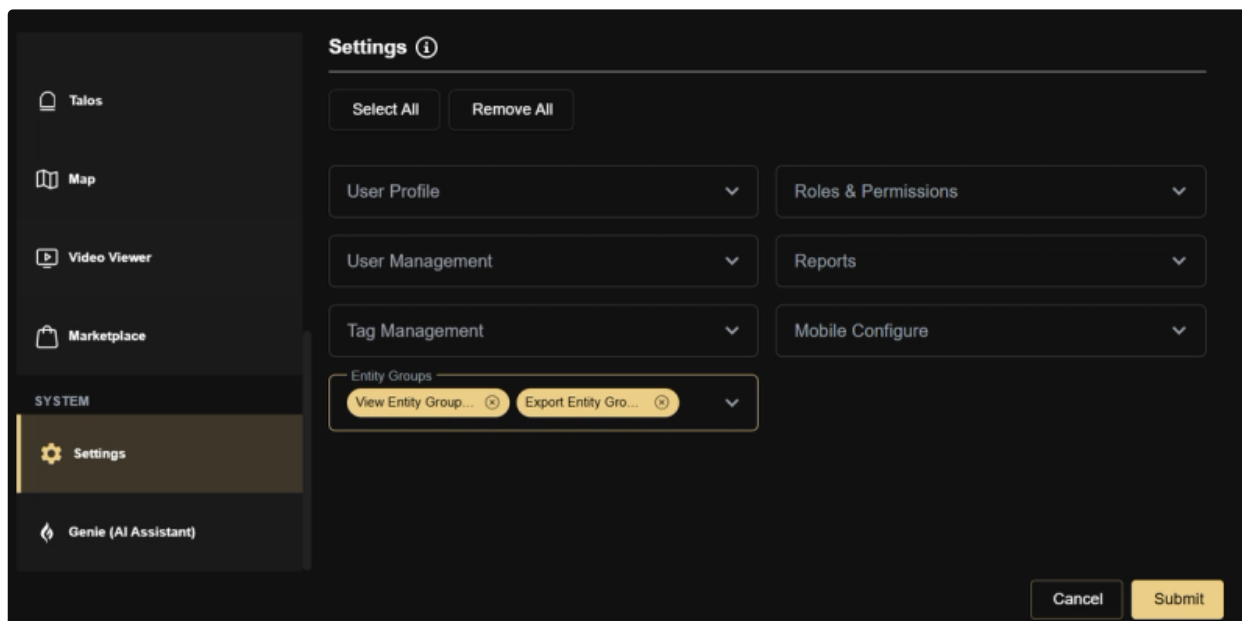
POORT	RICHTING	DOEL
443 (HTTPS)	Client → Cloud	Core UI
554 (RTSP) / 443	Bidirectioneel	RTSP videostreams of WebRTC-onderhandeling
8000 / 80	Apparaat → Cloud	HTTP-gebeurtenisknooppunten voor Hikvision/ISAPI
DC09-Protocol	GCXONE → CMS	Doorsturen van externe alarmontvangers

Note

!INFO — IP-whitelist:Voor beveiligde bedrijfsnetwerken levert GCXONE CIDR-blokbereiken. Deze bereiken zijn kritiek voor randapparatuur en moeten worden goedgekeurd vóór live gaan.

Super Admin Onboardingpad

1. Ontvang Uitnodigingse-mail — NXGEN dispatch stuurt een welkomstuitnodiging naar het zakelijke e-mailadres van de Super Admin `vanno-reply@nxgen.cloud`.
2. Bevestig E-mailadres — Klik op E-mail bevestigen om het domein te valideren. Dit vermindert routeringsfouten en vergrendelt het gebruikersschema tegen namaak.
3. Stel Cryptografisch Wachtwoord In — Klik op het token voor Wachtwoordconfiguratie. Deze lading verloopt exact 24 uur na afgifte.
4. Verifieer — Keer terug naar uw tenantURL. Meld u aan met vastgestelde referenties. Operators met meerdere tenants zien een organisatiekiezer.



cfb5864a6a30a9e5e507a125b016e562beae6576-1435x711

Systeemarchitectuur Vaststellen

1. Definieer Serviceprovidergegevens — Stel branding van hoofdorganisatie, regionale landinstellingen, operationele tijdzones en SOC-contactvariabelen in. Navigatie:Instellingen → Serviceprovider
2. Maak Klantentiteiten — Wijs uw clients of interne divisies toe. Voor meer dan 100 entiteiten gebruikt u het BulkImport CSV-framework. Navigatie:Configuratie → Klanten
3. Zet Sites In — Definieer unieke geografische beperkingen en koppel elke site aan de juiste klant. Navigatie:Configuratie → Sites
4. Registreer Apparaten — Voeg bruggen, NVR's of cloudrechtstreekse knooppunten toe met correcte eindpuntdefinities en referenties. Navigatie:Configuratie → Apparaten

Vier Kritieke Taken Vóór Lancering

Note

⚠️ **WAARSCHUWING** — Configureer Rollen Vóór Het Uitnodigen van Gebruikers: Een gebruiker die zonder toegewezen rol is uitgenodigd, belandt op een geblokkeerd scherm op het moment van aanmelden en blijft geblokkeerd totdat een beheerder handmatig een rol aan hem of haar toewijst. Ontwerp uw rolstructuur, maak de rollen aan en nodig vervolgens gebruikers uit.

1. **Configureer Rollen Vóór Het Uitnodigen van Gebruikers** — Maak uw volledige rolstructuur vóór het verzenden van gebruikersuitnodigingen.
 - Super Admin — volledige toegang, alleen intern.
 - Operator — alarmwachtrij, videokijker, kaart.
 - Installer — apparaatconfiguratie, beperkt tot toegewezen sites.
 - Eindgebruiker / Klantviewer — dashboard en Live View alleen.
1. **Zet Het Alarmbeheerssysteem Op** — Configureer uw CMS-integratie voordat een site monitoringactief gaat. Alarmen die door niet-toegewezen sites zijn gegenereerd, hebben geen bestemming en worden stilzwijgend verwijderd. Minimum: DC-09-verbinding geverifieerd (groen), elke actieve site toegewezen aan een CMS Account ID, en minstens één testalarm bevestigd ontvangen bij CMS.
2. **Schakel HealthCheck In Voor Alle Sites** — HealthCheck moet zich abonneren voordat camera's live gaan — het kan niet achteraf gebeurtenissen vastleggen. Aanbevolen: Abonneren op klantniveau met Include Children ingeschakeld. Navigatie: Configuratie → [Klant] → Analyticstabblad → Camera Health Check
3. **Maak Minstens Één Gepland Rapport** — Maandelijkse HealthCheck SLA-rapporten dienen als controleerbare uptime-evidentie voor klanten. Stel het schema in vóór live gaan zodat de eerste cyclus basisgegevens vastlegt. Navigatie: Instellingen → Rapporten → + Nieuw Schema Maken

Kernfunctionaliteiten

Controlelijst implementatievalidatie

ITEM	GEBIED
Firewalls	routing en NAT-regels geverifieerd
Super Admin-aanmelding operationeel	Toegangsbeheer
Minimale Customer/Site-topologie in kaart gebracht	Topologie
Eerste hardwareknooppunt verbonden en gestreamd	Opname
Teststoring ontvangen op Talos/DC09	Aflevering
HealthCheck-engine actief op knooppunt 1	Diagnose

Op gebeurtenissen gebaseerde workflows

Nieuwe site gaat live:

1. Maak de site-entiteit onder de juiste Customer.
2. Registreer apparaten en bevestig dat ze online zijn.
3. Wijs de site toe in AMS (stel DC09-account-ID of Talos-synchronisatie in).
4. Activeer HealthCheck op siteniveau of apparaatniveau.
5. Stuur een teststoring en bevestig ontvangst op CMS.
6. Wijs site-specifieke gebruikerstoegang toe via selectie van rolentiteit.

Camera gaat offline:

1. Controleer het HealthCheck-dashboard op de diagnostische code.
2. Indien netwerktime-out: controleer fysieke verbinding en firewall-regels.
3. Indien sabotage gedetecteerd: stuur een veldtechnicus.
4. Indien afbeeldingskwaliteit - verlichting: controleer IR/verlichting op locatie.
5. Leg het incident vast in uw ticketsysteem met HealthCheck-schermafbeelding als bewijs.

Storing bereikt CMS niet:

1. OpenMarketplace → Alarmbeheer-systeem.
2. Bevestig dat de AMS-kaart groene status toont.
3. Open de AMS-toewijzingstabel - zoek naar rode rijen (niet-toegewezen sites).
4. Voor rode rijen: klik op Bewerken, controleer of DC09-account-ID exact overeenkomt met CMS (hoofdlettergevoelig).
5. Voer een teststoring uit vanaf de betreffende site.
6. Indien nog steeds niet geslaagd: controleer firewall-regels voor DC09 Receiver IP en poort.

Gebruiker rapporteert toegangsprobleem:

1. Navigeer naar Instellingen → Gebruikers → [Gebruiker].
2. Controleer hun toegewezen rol.
3. Controleer of de rol de vereiste module ingeschakeld heeft (bijvoorbeeld Video Viewer).
4. Controleer entiteitstoegang - bevestig dat de relevante Customer/Site is opgenomen.
5. Gebruik Entiteitstoegang bewerken op de gebruikersrecord voor aanpassingen per gebruiker zonder de gedeelde rol te wijzigen.

Praktijkvoorbeelden

- Een nieuwe beheerder voltooit de volledige onboarding - Super Admin-aanmelding, systeemarchitectuur en eerste teststoring - in één dag met behulp van dit trainingspad.
- Een beheerder voltooit de controlelijst implementatievalidatie en ontdekt een ontbrekend HealthCheck-abonnement voordat de site live gaat.
- Een beheerder volgt de workflow camera gaat offline en identificeert een sabotage-gedetecteerde code - stuurt een technicus vóór de ochtendploeg.

- Een nieuwe operator meldt zich aan en ziet een geblokkeerd scherm - de beheerder traceert het onmiddellijk naar een ontbrekende roltoewijzing en lost het in minuten op.

Aanbevolen werkwijzen

- Configureer altijd rollen voordat u gebruikers uitnodigt - een gebruiker zonder rol wordt onmiddellijk geblokkeerd bij aanmelding.
- Voltooi de controlelijst implementatievalidatie voordat een site monitoring-actief wordt.
- Activeer HealthCheck op Customer-niveau met Onderliggende elementen opnemen - dit maakt toekomstige site-onboarding automatisch toekomstbestendig.
- Voer na elke nieuwe site die live gaat een teststoring uit - neem nooit aan dat aflevering werkt.
- Volg de dagelijkse en wekelijkse cadensen consistent - de meeste operationele fouten worden opgemerkt tijdens routinecontroles, niet bij incidentrespons.

Aanvullende informatie

Dagelijkse monitoringcadans

- Dashboard-KPI's - ongebruikelijke piek in totale alarmen; verhoogde telling van ongezonde camera's.
- Verhouding echte versus valse alarmen - scherpe daling in percentage echte alarmen kan wijzen op AI-overblokkering.
- HealthCheck-dashboard - alle nieuwe kritieke offline of sabotage-gedetecteerde camera's.
- AMS-verbindingsstatus - groen = doorsturen; rood = alarmen bereiken CMS niet.
- Verouderde alarmwachtrij - niet-beantwoorde alarmen ouder dan het werkschuifvenster hebben vervolgacties nodig.

Wekelijkse operationele cadans

- Controleer offline camera-lijst - escaleer camera's offline > 48 uur naar site-contactpersoon.

- Controleer nieuwe gebruikersuitnodigingen - bevestig dat alle openstaande uitnodigingen zijn geaccepteerd.
- Controleer rapportageafleverslogboeken - mislukte afleveringen geven problemen met e-mailrouting aan.
- Controleer auditlogboek op afwijkingen - zoek naar onverwachte rolwijzigingen of massale configuratiebewerkingen.
- Valideer DC-09 site-toewijzingen - rode rijen in AMS-toewijzing = niet-gerouteerde alarmen.