

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.

Admin-Schulung

Updated 15 September 2026

Inhalt der Admin-Schulung

Admin Training führt neue Administratoren durch alles, was für die Bereitstellung, Konfiguration und Wartung von GCXONE erforderlich ist – vom ersten Login bis zu den täglichen Betriebsabläufen. Dieser Leitfaden behandelt Netzwerkvoraussetzungen, Systemarchitektur-Einrichtung, Vor-Start-Aufgaben und fortlaufende Überwachungszyklen.

Warum es wichtig ist

Eine fehlerhaft konfigurierte Bereitstellung – fehlende Rollen, nicht zugeordnete Sites oder nicht überprüfte Kameragesundheit – führt zu Betriebsstörungen, die im Nachhinein schwer nachzuvollziehen sind. Die Befolgung des strukturierten Schulungswegs stellt sicher, dass jeder Administrator von einer soliden, validierten Basis startet.

Funktionsweise

Vor der Bereitstellung: Browser- und Netzwerkvoraussetzungen

Browser-Voraussetzungen:

BrowserUnterstützungsgradGoogle Chrome v90+Optimal (empfohlen)Mozilla Firefox v88+Unterstützt-Microsoft Edge v90+ (Chromium)UnterstütztApple Safari v14+EingeschränktInternet Explorer (any version)Gesperrt. Nicht unterstützt

Firewall- und Port-Voraussetzungen:

PortRichtungZweck443 (HTTPS)Client → CloudKern-UI; API-Tunneling; Sanity-CDN554 (RTSP) /

443BidirektionalRTSP-Streams oder WebRTC-Verhandlung8000 / 80Gerät → CloudHikvision/ISAPI

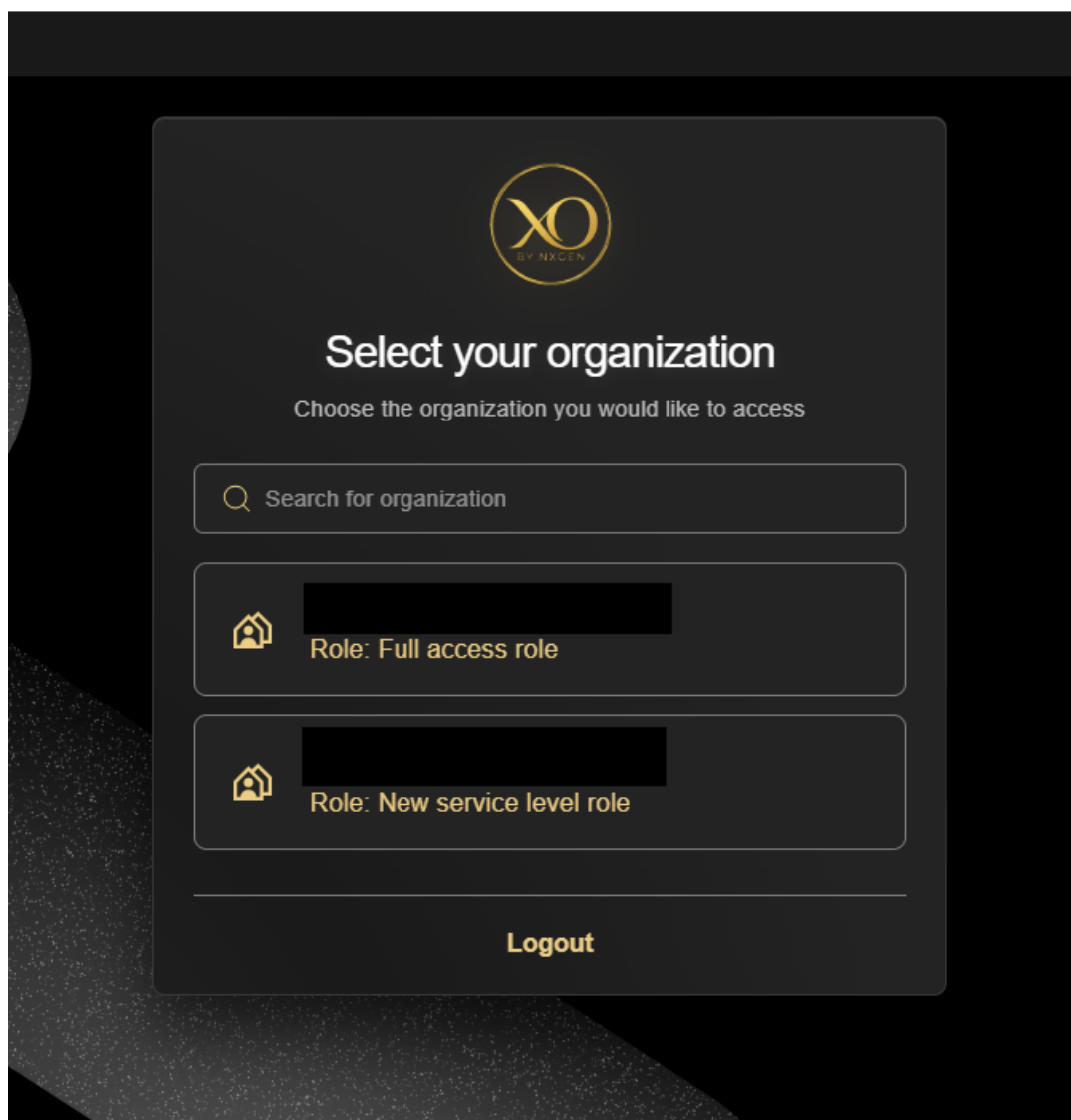
HTTP-EreignisknotenDC09-ProtokollGCXONE → CMSWeiterleitung externer Alarmempfänger

Hinweis: IP-Whitelist — Für gesicherte Firmennetzwerke stellt GCXONE CIDR-Blockbereiche bereit.

Diese Bereiche sind für Edge-Bridge-Hardware kritisch und müssen vor dem Go-Live auf die Whitelist gesetzt werden.

Super-Admin-Onboarding-Pfad

1. Einladungs-E-Mail erhalten — NXGEN sendet eine Willkommens-Einladung an die E-Mail-Adresse des neuen Benutzers.
2. E-Mail-Adresse bestätigen — Öffnen Sie die E-Mail und klicken Sie auf Konto bestätigen, um die Adresse zu verifizieren.
3. Passwort festlegen — Folgen Sie dem Link zum Einrichten des Passworts, der an Ihre E-Mail gesendet wurde, um das Passwort für Ihr Konto zu erstellen.
4. Authentifizieren — Rufen Sie Ihre Mandanten-URL auf. Melden Sie sich mit den vorhandenen Anmeldedaten an. Multi-Mandanten-Betreiber sehen einen Organisations-Auswahlbereich.



Systemarchitektur festlegen

1. Dienstleister-Informationen definieren — Legen Sie das Branding der Stammorganisation, die regionale Locale, betriebliche Zeitzonen und SOC-Kontaktvariablen fest. Navigation: Settings → General
2. Kunden-Entitäten erstellen — Ordnen Sie Ihre Kunden oder internen Abteilungen zu. Für mehr als 100 Entitäten nutzen Sie die BulkImport-Marketplace-Funktion (Excel-basierter Upload). Navigation: Configuration → Customers
3. Standorte bereitstellen — Definieren Sie eindeutige geografische Grenzen und verknüpfen Sie jeden Standort mit dem richtigen Kunden. Navigation: Configuration → Sites

4. Geräte registrieren — Fügen Sie Bridges, NVRs oder Cloud-Direct-Knoten mit korrekten Endpunktdefinitionen und Anmeldedaten hinzu. Navigation: Configuration → Devices

Vier kritische Aufgaben vor dem Start

Wichtig: Rollen konfigurieren, bevor Benutzer eingeladen werden — Ein eingeladener Benutzer ohne zugewiesene Rolle gelangt sofort nach dem Anmelden auf einen gesperrten Bildschirm und bleibt gesperrt, bis ein Administrator ihm manuell eine Rolle zuweist. Entwerfen Sie Ihre Rollenstruktur, erstellen Sie die Rollen und laden Sie dann die Benutzer ein.

Schritt 1: Rollen konfigurieren, bevor Benutzer eingeladen werden — Erstellen Sie Ihre vollständige Rollenstruktur, bevor Sie Benutzereinladungen versenden.

- Rollen sind vollständig anpassbar — Sie definieren den Namen, die Modul-Berechtigungen und den Entitäts-Zugriff für jede Rolle über Settings → Roles → Configure New Role. Übliche Muster umfassen eine Administrator-Rolle mit Vollzugriff, eine reine Überwachungs-Rolle mit Ansicht-Only-Zugriff, beschränkt auf bestimmte Standorte, und eine eingeschränkte Installateur-Rolle, die auf die Geräte-Konfiguration begrenzt ist. Siehe Rollen und Berechtigungen für den vollständigen Konfigurations-Workflow.

Schritt 2: Alarmsystem einrichten — Konfigurieren Sie Ihre CMS-Integration, bevor ein Standort aktiv überwacht wird. Alarme, die von nicht zugeordneten Standorten erzeugt werden, haben kein Ziel und werden stillschweigend verworfen. Minimum: DC-09-Verbindung verifiziert (grün), jeder aktive Standort einem CMS-Account-ID zugeordnet und mindestens ein Testalarm bestätigt im CMS empfangen.

Schritt 3: HealthCheck auf allen Standorten aktivieren — HealthCheck muss abonniert sein, bevor Kameras live gehen — es kann Ereignisse nicht rückwirkend erfassen. Empfohlen: Auf Kundenebene abonnieren mit aktivierter Option Kinder einbeziehen. Navigation: Configuration → [Customer] → Analytics Tab → Health Check Basic / Health Check+

Schritt 4: Mindestens einen geplanten Bericht erstellen — Monatliche HealthCheck-SLA-Berichte

dienen als nachweisbare Verfügbarkeitsnachweise für Kunden. Richten Sie den Zeitplan vor dem Go-Live ein, damit der erste Zyklus Basisdaten erfasst. Navigation: Settings → Reports → + Create New Schedule

Wesentliche Funktionen

Checkliste zur Bereitstellungsvalidierung

ElementBereichFirewalls, Routing und NAT-Regeln geprüftKommunikation/Sicherheit-

Super-Admin-Anmeldung betriebsbereitZugangskontrolleMindest-Kunden/Standort-Topologie

abgebildetTopologieErster Hardware-Knoten verbunden und streamtErfassungTestalarm bei Talos/DC09

empfangenZustellungHealthCheck-Engine auf Knoten 1 aktivDiagnose

Ereignisgesteuerte Workflows

Neuer Standort geht live:

1. Erstellen Sie die Standort-Entität unter dem richtigen Kunden.
2. Registrieren Sie Geräte und bestätigen Sie, dass sie online angezeigt werden.
3. Kartieren Sie den Standort im AMS (setzen Sie die DC09-Account-ID oder die Talos-Synchronisation).
4. Aktivieren Sie HealthCheck auf Standort- oder Geräteebene.
5. Senden Sie einen Testalarm und bestätigen Sie den Empfang im CMS.
6. Weisen Sie sitespezifischen Benutzerzugriff über die Roll-Entitätsauswahl zu.

Kamera geht offline:

1. Prüfen Sie das HealthCheck-Board auf den Diagnosecode.
2. Bei Netzwerk-Timeout: prüfen Sie die physische Verbindung und die Firewall-Regeln.
3. Bei Sabotageerkennung: entsenden Sie einen Techniker vor Ort.
4. Bei Bildqualität — Beleuchtung: prüfen Sie IR/Beleuchtung am Standort.
5. Protokollieren Sie den Vorfall in Ihrem Ticketsystem mit einem HealthCheck-Screenshot als Nachweis.

Alarm erreicht CMS nicht:

1. Öffnen Sie Marketplace → Alarm Management System.
2. Bestätigen Sie, dass die AMS-Karte den grünen Status anzeigt.
3. Öffnen Sie die AMS-Mapping-Tabelle — suchen Sie nach roten Zeilen (nicht zugeordnete Standorte).
4. Für rote Zeilen: klicken Sie auf Bearbeiten, prüfen Sie, dass die DC09-Account-ID exakt (Groß-/Kleinschreibung) mit dem CMS übereinstimmt.
5. Führen Sie einen Testalarm vom betroffenen Standort aus.
6. Falls weiterhin fehlschlägt: prüfen Sie die Firewall-Regeln für die DC09-Receiver-IP und den Port.

Benutzer meldet Zugriffsproblem:

1. Navigieren Sie zu Einstellungen → Benutzer → [User].
2. Prüfen Sie die zugewiesene Rolle.
3. Verifizieren Sie, dass die Rolle das erforderliche Modul aktiviert hat (z. B. Video Viewer).
4. Prüfen Sie den Entitätszugriff — bestätigen Sie, dass der relevante Kunde/Standort enthalten ist.
5. Verwenden Sie „Edit Entity Access“ im Benutzerdatensatz für benutzerspezifische Anpassungen, ohne die geteilte Rolle zu ändern.

Praxisnahe Anwendungsfälle

- Ein neuer Administrator schließt die vollständige Einarbeitung — Super Admin-Anmeldung, Systemarchitektur und ersten Testalarm — an einem einzigen Tag über diesen Schulungsweg ab.
- Ein Administrator erledigt die Deployment Validation Checklist und erkennt ein fehlendes HealthCheck-Abonnement, bevor die Site live geht.
- Ein Administrator folgt dem Camera Goes Offline-Workflow und identifiziert einen Sabotage Detected-Code — er schickt einen Techniker vor der Morgenschicht.

- Ein neuer Operator meldet sich an und sieht einen gesperrten Bildschirm — der Administrator führt dies sofort auf eine fehlende Rollen-Zuweisung zurück und löst das Problem in Minuten.

Best Practices

- Konfigurieren Sie Rollen immer, bevor Sie Benutzer einladen — ein Benutzer ohne Rolle wird beim Login sofort gesperrt.
- Erledigen Sie die Deployment Validation Checklist, bevor eine Site aktiv überwacht wird.
- Aktivieren Sie HealthCheck auf Kundenebene mit Include Children — das macht die zukünftige Einarbeitung neuer Sites automatisch zukunftssicher.
- Führen Sie nach jeder neuen Site, die live geht, einen Testalarm aus — gehen Sie nie davon aus, dass die Zustellung funktioniert.
- Befolgen Sie die Daily- und Weekly-Cadences konsequent — die meisten Betriebsfehler werden bei Routineprüfungen entdeckt, nicht bei der Vorfallreaktion.

Zusätzliche Details

Tägliche Überwachungs-Cadence

- Dashboard-KPIs — ungewöhnlicher Anstieg der Gesamtalarme; erhöhter Unhealthy-Kameras-Zähler.
- Echter-vs-Falscher-Alarm-Verhältnis — ein starker Rückgang des echten Alarm-% kann auf übermäßige KI-Blockierung hinweisen.
- HealthCheck-Board — alle neuen Critical-Offline- oder Sabotage-Detected-Kameras.
- AMS-Verbindungsstatus — Grün = Weiterleitung; Rot = Alarme erreichen das CMS nicht.
- Veralterte Alarmwarteschlange — nicht bestätigte Alarme, die älter als das Schichtfenster sind, benötigen Nachverfolgung.

Wöchentliche Betriebs-Cadence

- Überprüfen Sie die Offline-Kamera-Liste — Kameras, die länger als 48 h offline sind, an den Site-Kontakt eskalieren.
- Auditieren Sie die Benutzer-Liste — prüfen Sie auf Tippfehler, Duplikate oder Benutzer, die unerwartet als Inaktiv markiert sind.
- Prüfen Sie die Bericht-Zustellungs-Protokolle — fehlgeschlagene Zustellungen deuten auf Probleme im E-Mail-Routing hin.
- Überprüfen Sie das Audit-Log auf Anomalien — suchen Sie nach unerwarteten Rollenänderungen oder massenhaften Konfigurationsänderungen.
- Validieren Sie die DC-09-Site-Mappings — jede rote Zeile im AMS-Mapping bedeutet nicht zugeordnete Alarmer.