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.

Admin Training

Updated 14 August 2026

What Admin Training Covers

Admin Training walks new administrators through everything needed to deploy, configure, and maintain GCXONE — from first login to daily operational routines. This guide covers network requirements, system architecture setup, pre-launch tasks, and ongoing monitoring cadences.

Why It Matters

A misconfigured deployment — missing roles, unmapped sites, or unchecked camera health — creates operational failures that are hard to trace after the fact. Following the structured training path ensures every admin starts from a solid, validated foundation.

How It Works

Pre-Deployment: Browser & Network Requirements

Browser Requirements:

BROWSER	SUPPORT LEVEL
Google Chrome v90+	Optimal (recommended)
Mozilla Firefox v88+	Supported
Microsoft Edge v90+ (Chromium)	Supported
Apple Safari v14+	Limited
Internet Explorer (any version)	Blocked. Not supported

Firewall & Port Requirements:

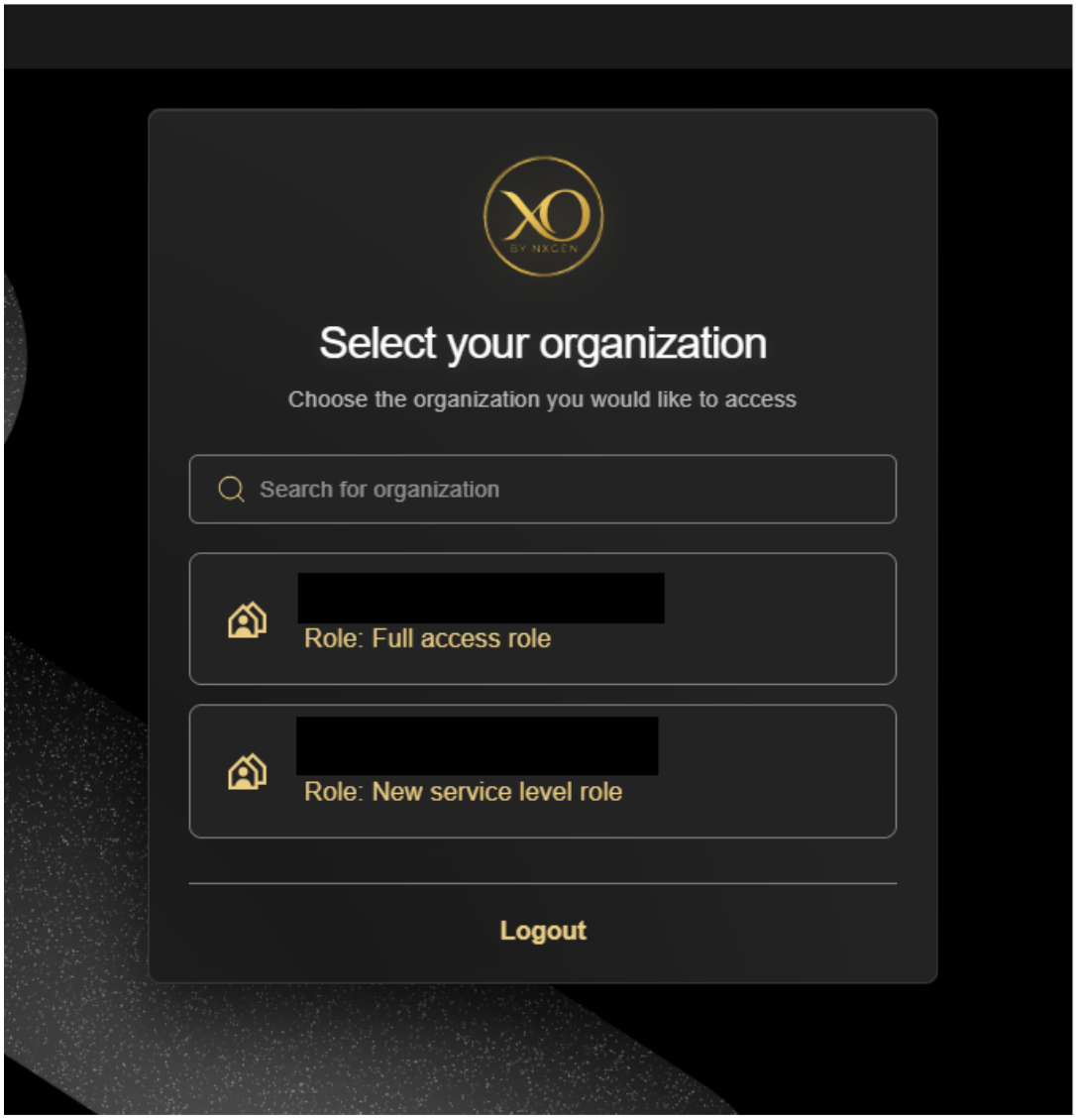
PORT	DIRECTION	PURPOSE
443 (HTTPS)	Client → Cloud	Core UI

554 (RTSP) / 443	Bidirectional	RTSP streams or WebRTC negotiation
8000 / 80	Device → Cloud	Hikvision/ISAPI HTTP event nodes
DC09 Protocol	GCXONE → CMS	External alarm receiver forwarding

> IP Whitelisting
>
> For secured corporate networks, GCXONE provides CIDR block ranges. These ranges are critical for edge-bridge hardware and must be whitelisted before go-live.

Super Admin Onboarding Path

1. Receive Invitation Email — NXGEN sends a welcome invitation to the new user's email address.
2. Confirm Email Address — Open the email and click Confirm my account to verify the address.
3. Set Your Password — Follow the password setup link sent to your email to create your account password.
4. Authenticate — Return to your tenant URL. Log in with established credentials. Multi-tenant operators will see an organization selector.



Establishing System Architecture

1. Define Service Provider Info — Set root organization branding, regional locale, operational timezones, and SOC contact variables. Navigation: Settings → Service Provider
2. Create Customer Entities — Map your clients or internal divisions. For 100+ entities, use the BulkImport CSV framework. Navigation: Configuration → Customers
3. Deploy Sites — Define unique geographical constraints and link each site to its correct customer. Navigation: Configuration → Sites
4. Register Devices — Add bridges, NVRs, or cloud-direct nodes with correct endpoint definitions and credentials. Navigation: Configuration → Devices

Four Critical Pre-Launch Tasks

> **Configure Roles Before Inviting Users**
>
> A user invited without a role assigned lands on a blocked screen the moment they log in and stays blocked until an admin manually assigns them a role. Design your role structure, create the roles, then invite users.

1. Configure Roles Before Inviting Users — Create your complete role structure before sending any user invitations.

- Roles are fully custom — you define the name, module privileges, and entity access for each one via Settings → Roles → Configure New Role. Common patterns include a full-access admin role, a view-only monitoring role restricted to specific sites, and a limited installer role scoped to device configuration. See Roles and Permissions for the full configuration workflow.

1. Set Up the Alarm Management System — Configure your CMS integration before any site goes monitoring-active. Alarms generated by unmapped sites have no destination and are silently discarded. Minimum: DC-09 connection verified (green), every active site mapped to a CMS Account ID, and at least one test alarm confirmed received at CMS.
2. Enable HealthCheck on All Sites — HealthCheck must be subscribed before cameras go live — it cannot retroactively capture events. Recommended: Subscribe at Customer level with Include Children enabled. Navigation: Configuration → [Customer] → Analytics Tab → Health Check Basic / Health Check+
3. Create at Least One Scheduled Report — Monthly HealthCheck SLA reports serve as verifiable uptime evidence for customers. Set up the schedule before go-live so the first cycle captures baseline data. Navigation: Settings → Reports → + Create New Schedule

Key Capabilities

Deployment Validation Checklist

ITEM	AREA
Firewalls	routing
Super Admin login operational	Access Control
Minimum Customer/Site topology mapped	Topology
First hardware node connected and streaming	Ingestion
Test alarm received at Talos/DC09	Delivery
HealthCheck engine active on node 1	Diagnostic

Event-Driven Workflows

New Site Goes Live:

1. Create the Site entity under the correct Customer.
2. Register Devices and confirm they show Online.
3. Map the site in AMS (set DC09 Account ID or Talos sync).
4. Enable HealthCheck at site or device level.
5. Send a test alarm and confirm receipt at CMS.
6. Assign any site-specific user access via role entity selection.

Camera Goes Offline:

1. Check HealthCheck board for the diagnostic code.
2. If Network Timeout: verify physical connection and firewall rules.
3. If Sabotage Detected: dispatch field technician.
4. If Image Quality — Illumination: check IR/lighting at site.
5. Log the incident in your ticket system with HealthCheck screenshot as evidence.

Alarm Not Reaching CMS:

1. Open Marketplace → Alarm Management System.
2. Confirm the AMS card shows green status.
3. Open the AMS mapping table — look for red rows (unmapped sites).
4. For red rows: click Edit, verify DC09 Account ID matches CMS exactly (case-sensitive).
5. Run a test alarm from the affected site.
6. If still failing: check firewall rules for DC09 Receiver IP and Port.

User Reports Access Issue:

1. Navigate to Settings → Users → [User].
2. Check their assigned role.
3. Verify role has the required module enabled (e.g. Video Viewer).
4. Check entity access — confirm the relevant Customer/Site is included.
5. Use Edit Entity Access on the user record for per-user adjustments without changing the shared role.

Real-World Use Cases

- A new admin completes full onboarding — Super Admin login, system architecture, and first test alarm — in a single day using this training path.
- An admin completes the Deployment Validation Checklist and catches a missing HealthCheck subscription before the site goes live.
- An admin follows the Camera Goes Offline workflow and identifies a Sabotage Detected code — dispatches a technician before the morning shift.
- A new operator logs in and sees a blocked screen — the admin traces it immediately to a missing role assignment and resolves it in minutes.

Best Practices

- Always configure roles before inviting any users — a user with no role is immediately blocked on login.
- Complete the Deployment Validation Checklist before any site goes monitoring-active.
- Enable HealthCheck at the Customer level with Include Children — this future-proofs new site onboarding automatically.
- Run a test alarm after every new site goes live — never assume delivery is working.
- Follow the Daily and Weekly cadences consistently — most operational failures are caught during routine checks, not incident response.

Additional Details

Daily Monitoring Cadence

- Dashboard KPIs — Unusual spike in Total Alarms; elevated Unhealthy Cameras count.
- Real vs. False Alarm ratio — Sharp drop in real alarm % may indicate AI over-blocking.
- HealthCheck board — Any new Critical Offline or Sabotage-Detected cameras.
- AMS connection status — Green = forwarding; red = alarms not reaching CMS.
- Stale alarm queue — Unacknowledged alarms older than shift window need follow-up.

Weekly Operational Cadence

- Review offline camera list — Escalate cameras offline > 48h to site contact.
- Audit new user invitations — Confirm all pending invitations have been accepted.
- Check report delivery logs — Failed deliveries indicate email routing issues.
- Review Audit Log for anomalies — Look for unexpected role changes or mass configuration edits.
- Validate DC-09 site mappings — Any red rows in AMS mapping = unrouted alarms.