Clause de non-responsabilité

Avertissement juridique

Ce guide et son contenu (le « Guide ») sont fournis par NXGEN. Tous les droits sur le Guide et sur la propriété intellectuelle qu'il incorpore — y compris, sans s'y limiter, les marques, noms commerciaux, logos et signes similaires figurant dans ou sur le Guide — sont protégés par la loi. L'ensemble des droits, titres et intérêts relatifs au Guide et aux droits de propriété intellectuelle qui s'y rapportent appartiennent et demeurent à NXGEN et à ses concédants.

Le Guide est fourni gratuitement, « en l'état » et à titre d'information uniquement, sans garantie d'aucune sorte. Il n'est ni destiné ni propre à établir une quelconque relation juridique entre le lecteur et NXGEN ou ses sociétés affiliées, y compris, sans s'y limiter, une quelconque obligation de NXGEN ou de ses sociétés affiliées envers le lecteur.

Les obligations de NXGEN et de ses sociétés affiliées concernant les produits ou services NXGEN achetés par un client sont régies exclusivement par les termes du contrat au titre duquel ces produits ou services ont été achetés.

Pour clarification

Le lecteur assume l'intégralité du risque quant à l'utilisation, aux résultats et aux performances du Guide. Dans toute la mesure permise par la loi applicable, NXGEN décline et exclut toutes garanties, qu'elles soient légales, expresses ou implicites — y compris, sans s'y limiter, les garanties implicites de qualité marchande, d'adéquation à un usage particulier, de titre et de non-contrefaçon des droits de tiers — ainsi que toute responsabilité ou garantie découlant de suggestions, spécifications ou échantillons liés au Guide.

Formation administrative

Updated 14 August 2026

Ce que couvre la formation administrative

La formation administrative guide les nouveaux administrateurs à travers tout ce qui est nécessaire pour déployer, configurer et maintenir GCXONE — de la première connexion aux routines opérationnelles quotidiennes. Ce guide couvre les exigences réseau, la configuration de l'architecture système, les tâches de pré-lancement et les cadences de surveillance continue.

Pourquoi c'est important

Un déploiement mal configuré — rôles manquants, sites non cartographiés ou état de santé non contrôlé de la caméra — engendre des défaillances opérationnelles difficiles à retracer après coup. Suivre le parcours de formation structuré garantit que chaque administrateur commence sur une base solide et validée.

Comment ça fonctionne

Pré-déploiement : Exigences en navigateur et réseau

Exigences du navigateur :

NAVIGATEUR	NIVEAU DE SOUTIEN
Google Chrome v90+	Optimal (recommandé)
Mozilla Firefox v88+	Soutenu
Microsoft Edge v90+ (Chromium)	Soutenu
Apple Safari v14+	Limité
Internet Explorer (n'importe quelle version)	Bloqué. Non supporté

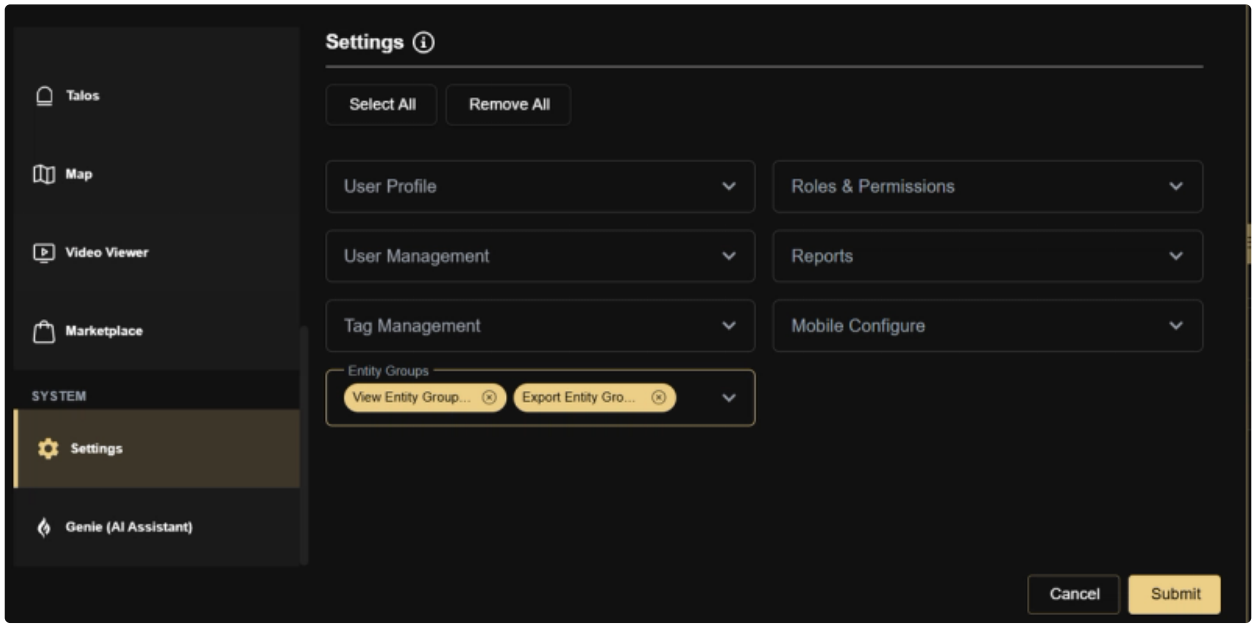
Exigences du pare-feu et des ports :

PORT	RÉALISATION	OBJECTIF
443 (HTTPS)	Client → Cloud	Interface de base
554 (RTSP) / 443	Bidirectionnel	Flux RTSP ou négociation WebRTC
8000 / 80	Dispositif → Cloud	Nœuds d'événements HTTP Hikvision/ISAPI
Protocole DC09	GCXONE → CMS	Transmission d'alarme externe

> Note
>
> i INFO — Liste blanche de la propriété intellectuelle : Pour les réseaux d'entreprise sécurisés, GCXONE fournit des plages de blocs CIDR. Ces plages sont essentielles pour le matériel de pont de bord et doivent être placées sur liste blanche avant la mise en service.

Parcours d'intégration Super Admin

1. Recevoir un e-mail d'invitation — Le dispatch de NXGEN envoie une invitation bienvenue à l'email professionnel du Super Admin depuis `no-reply@nxgen.cloud`.
2. Confirmer l'adresse e-mail — Cliquez sur Confirmer l'e-mail pour valider le domaine. Cela atténue les erreurs de routage et verrouille le schéma utilisateur contre l'usurpation.
3. Définir un mot de passe cryptographique — Cliquez sur le jeton de configuration du mot de passe. Cette charge utile expire précisément 24 heures après l'émission.
4. Authentifier — Retourner à l'URL de votre locataire. Connectez-vous avec des références établies. Les opérateurs multi-locataires verront un sélecteur d'organisation.



cfb5864a6a30a9e5e507a125b016e562beae6576-1435x711

Établissement de l'architecture système

1. Définir les informations du fournisseur de services — Définir l'image de marque de l'organisation root, la localisation régionale, les fuseaux horaires opérationnels et les variables de contact SOC. Navigation : Paramètres → Fournisseur de services
2. Créer des entités clients — Cartographiez vos clients ou divisions internes. Pour 100+ entités, utilisez le framework CSV BulkImport. Navigation : Configuration → clients
3. Sites de déploiement — Définir des contraintes géographiques uniques et relier chaque site à son client approprié. Navigation : Configuration → Sites
4. Dispositifs de registre — Ajouter des ponts, des NVR ou des nœuds directs au cloud avec des définitions et identifiants corrects des points de terminaison. Navigation : Configuration → Dispositifs

Quatre tâches critiques avant le lancement

Note

⚠ AVERTISSEMENT — Configurez les rôles avant d'inviter les utilisateurs : Un utilisateur invité sans rôle attribué apparaît sur un écran bloqué dès qu'il se connecte et reste bloqué jusqu'à ce qu'un administrateur lui attribue manuellement un rôle. Concevez votre structure de rôle, créez les rôles, puis invitez les utilisateurs.

1. Configurez les rôles avant d'inviter les utilisateurs — Créez la structure complète de vos rôles avant d'envoyer toute invitation utilisateur.

- Super Admin — accès complet, uniquement en interne.
- Opérateur — file d'alarme, visualiseur vidéo, carte.
- Installateur — configuration de l'appareil, limitée aux sites assignés.
- Visualiseur utilisateur final / Client — tableau de bord et vue en direct uniquement.

1. Installez le système de gestion des alarmes — Configurez votre intégration CMS avant qu'un site ne devienne activé en surveillance. Les alarmes générées par des sites non cartographiés n'ont pas de destination et sont discrètement rejetées. Minimum : connexion DC-09 vérifiée (vert), chaque site actif mappé à un identifiant de compte CMS, et au moins une alarme de test confirmée reçue au CMS.
2. Activez HealthCheck sur tous les sites — HealthCheck doit être abonné avant que les caméras ne soient activées — il ne peut pas capturer rétroactivement les événements. Recommandé : Abonnez-vous au niveau du client avec Inclure les enfants activé. Navigation :Onglet → → de configuration [client] → Contrôle de l'état de la caméra
3. Créer au moins un rapport programmé — Les rapports mensuels HealthCheck SLA servent de preuves vérifiables de disponibilité pour les clients. Configurez le planning avant la mise en service afin que le premier cycle capture les données de base. Navigation : Paramètres → rapports → + Créer un nouveau planning

Capacités clés

Liste de contrôle pour la validation du déploiement

OBJET	SUPERFICIE
Règles de pare-feu	routage et NAT vérifiées
Connexion Super Admin opérationnelle	Contrôle d'accès
Topologie minimale client/site cartographiée	Topologie
Premier nœud matériel connecté et en streaming	Ingestion
Alarme de test reçue à Talos/DC09	Livraison
Moteur HealthCheck actif sur le nœud 1	Diagnostic

Flux de travail pilotés par les événements

Nouveau site mis en ligne :

1. Créez l'entité Site sous le bon Client.
2. Enregistrez les appareils et confirmez qu'ils affichent en ligne.
3. Cartographiez le site dans AMS (définissez l'ID de compte DC09 ou la synchronisation Talos).
4. Activez HealthCheck au niveau du site ou de l'appareil.
5. Envoyez une alarme de test et confirmez la réception au CMS.
6. Attribuez un accès utilisateur spécifique au site via la sélection d'entités de rôle.

La caméra est hors ligne :

1. Vérifiez le code de diagnostic sur le tableau HealthCheck.
2. Si le délai d'attente réseau : vérifiez les règles de connexion physique et de pare-feu.
3. Si un sabotage est détecté : technicien de terrain de répartition.
4. Si la qualité de l'image — Éclairage : vérifiez l'infrarouge/éclairage sur le site.

5. Enregistrez l'incident dans votre système de tickets avec une capture d'écran HealthCheck comme preuve.

Alarme qui ne parvient pas au CMS :

1. Ouvre Marketplace → système de gestion d'alarme.
2. Confirmez que la carte AMS affiche un statut vert.
3. Ouvrez la table de cartographie AMS — cherchez les lignes rouges (sites non cartographiés).
4. Pour les lignes rouges : cliquez sur Modifier, vérifier que l'ID de compte DC09 correspond exactement à CMS (sensible à la casse).
5. Lancez une alarme de test depuis le site concerné.
6. Si cela ne fonctionne toujours pas : vérifiez les règles du pare-feu pour l'IP et le port du récepteur DC09.

Problème d'accès aux rapports utilisateurs :

1. Naviguer vers Paramètres → utilisateurs → [utilisateur].
2. Vérifiez leur rôle assigné.
3. Le rôle de vérification a activé le module requis (par exemple le Visualiseur vidéo).
4. Vérifiez l'accès à l'entité — vérifiez que le client/site concerné est inclus.
5. Utilisez l'Édition de l'Accès à l'Entité sur l'enregistrement utilisateur pour des ajustements par utilisateur sans changer le rôle partagé.

Cas d'usage réels

- Un nouvel administrateur complète l'intégration complète — connexion Super Admin, architecture système et première alarme de test — en une seule journée en utilisant ce parcours de formation.
- Un administrateur remplit la liste de vérification de validation du déploiement et détecte un abonnement HealthCheck manquant avant que le site ne soit mis en ligne.

- Un administrateur suit le flux de travail Camera Goes Offline et identifie un code de Sabotage Détecté — dépêche un technicien avant le service du matin.
- Un nouvel opérateur se connecte et voit un écran bloqué — l'administrateur le remonte immédiatement à une affectation de rôle manquante et le résout en quelques minutes.

Bonnes pratiques

- Configurez toujours les rôles avant d'inviter des utilisateurs — un utilisateur sans rôle est immédiatement bloqué à la connexion.
- Complétez la liste de contrôle de validation du déploiement avant qu'un site ne devienne activé en surveillance.
- Activez HealthCheck au niveau du client avec Inclure les enfants — cela garantit l'intégration automatique de nouveaux sites pour l'avenir.
- Lancez une alarme de test après chaque nouvelle mise en ligne — ne supposez jamais que la livraison fonctionne.
- Suivez systématiquement les cadences Quotidienne et Hebdomadaire — la plupart des défaillances opérationnelles sont détectées lors de contrôles de routine, pas lors de la réponse aux incidents.

Détails supplémentaires

Cadence de surveillance quotidienne

- KPI du tableau de bord — Pic inhabituel du nombre total d'alarmes ; un nombre élevé de caméras malsaines.
- Ratio réel vs. fausse alerte — Une forte baisse du pourcentage d'alarme réel peut indiquer un surblocage par l'IA.
- Tableau HealthCheck — Toute nouvelle caméra critique hors ligne ou détectée par sabotage.
- État de la connexion AMS — Green = redirection ; rouge = alarmes qui n'atteignent pas le CMS.

- File d’alarme obsolète — Les alarmes non accusées de plus de temps que la plage horaire de service doivent être suivies.

Cadence opérationnelle hebdomadaire

- Consultez la liste des caméras hors ligne — Escaladez les caméras hors ligne > 48h vers le contact du site.
- Auditer les nouvelles invitations des utilisateurs — Confirmez que toutes les invitations en attente ont été acceptées.
- Consultez les journaux de livraison des rapports — Les livraisons ratées indiquent des problèmes de routage des e-mails.
- Consultez le journal d’audit pour détecter les anomalies — Recherchez des changements de rôle inattendus ou des modifications massives de configuration.
- Valider les cartographies de site DC-09 — Toutes les lignes rouges dans la cartographie AMS = alarmes non routées.