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.

Aperçu du tableau de bord

Updated 14 August 2026

Ce que montre le tableau de bord

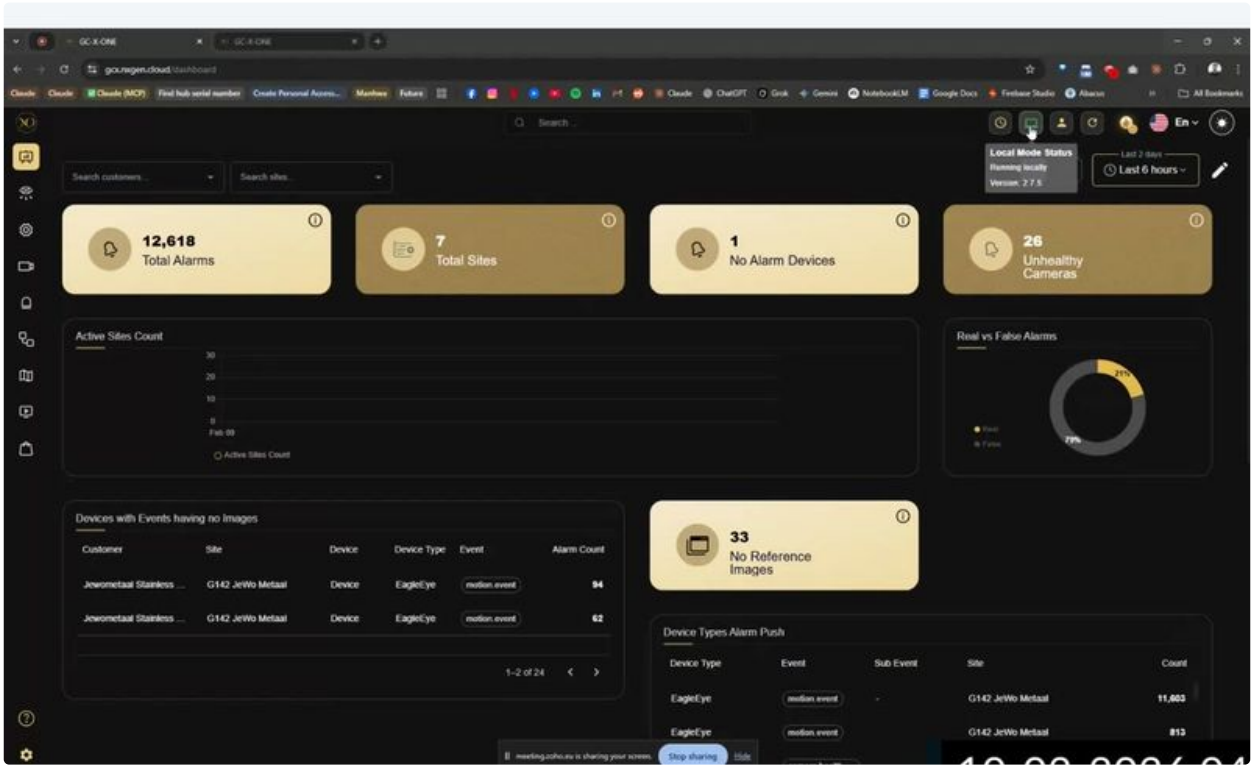
GCXONE est une plateforme cloud de surveillance et d'opérations alimentée par l'IA, offrant des services unifiés de vidéosurveillance et d'IoT en tant que SaaS de gestion de la sécurité. Il permet une surveillance centralisée à distance sans infrastructure locale — une interface intelligente unique pour les alarmes, l'état des appareils, les tableaux de bord, les flux de travail et les outils d'IA.

- Alimenté par l'IA — NOVA99x filtre jusqu'à 99 % des fausses alertes avant qu'une alarme n'atteigne un opérateur.
- SaaS natif des nuages — Aucune infrastructure locale. Entièrement multi-locataire avec une isolation stricte des données par organisation.
- Conscient du rôle — Chaque utilisateur ne voit que les modules, entités et tableaux de bord assignés — appliqués par RBAC.
- Construit à l'échelle — Intégrer des centaines de sites avec BulkImport. Exploitation de culture sans effectifs proportionnels.
- Intégration de Talos — Travaille main dans la main avec Evalink Talos en tant que couche de workflow opérateur pour la gestion des alarmes.
- Santé des dispositifs — HealthCheck surveille en continu chaque caméra pour détecter les états hors ligne, obstrués ou dégradés.

Quatre cartes KPI sont affichées en haut du tableau de bord pour la période de temps sélectionnée (par défaut : 2 derniers jours) :

- Alarmes totales — Le nombre total d'événements d'alarme générés sur tous les sites surveillés.

- Total Sites — Le nombre de sites actuellement configurés sous votre compte de fournisseur de services.
- Aucun dispositif d'alarme — Dispositifs actifs mais sans alarme durant la période. Un nombre élevé peut indiquer des problèmes de connexion ou de capteurs.
- Caméras malsaines — Des caméras qui ont échoué à leur dernier HealthCheck. Directement lié au module HealthCheck.



Pourquoi c'est important

Le Tableau de bord est votre interface unique et intelligente pour surveiller les alarmes, l'état de l'état des appareils et les flux de travail opérationnels sur tous les sites — sans avoir besoin d'infrastructure locale.

Comment ça fonctionne

Chaque alarme suit un cycle de vie strictement structuré et traçable en 5 étapes :

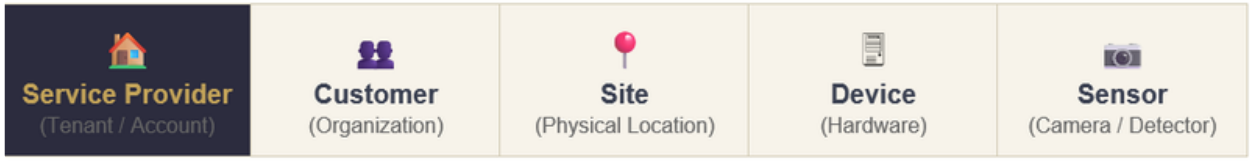
1. Appareils et caméras — Les capteurs détectent les événements et envoient des signaux à GCXONE.

2. Filtre IA NOVA99x — Le pipeline d'IA évalue l'événement en temps réel ; Les fausses alertes sont écartées avant d'atteindre un opérateur.
3. Vérifié → Talos — Les alarmes confirmées sont transmises via DC-09 ou Talos REST à la Station Centrale de Surveillance.
4. Avis sur l'opérateur — L'opérateur CMS reçoit l'alarme avec des images pré-événement, un flux en direct et des superpositions de boîtes englobantes IA.
5. Résolu + Audit — Le résultat est enregistré avec une trace d'audit cryptographiquement scellée et immuable.

Hiérarchie des entités multi-locataires

Chaque objet que vous gérez dans GCXONE s'inscrit dans une hiérarchie à cinq niveaux. Comprendre cette structure est essentiel avant de configurer les alarmes d'accès ou de routage.

- Fournisseur de services (locataire) — Au niveau de la racine. Opérations de flotte mondiales, reporting macro SLA, gouvernance des rôles multi-sites.
- Client (Organisation) — Groupes clients discrets avec tableaux de bord segmentés et logique de facturation.
- Site (Emplacement physique) — Géo-repérages tangibles avec cartographie des incidents et opérateurs locaux.
- Appareil (NVR / Bridge / Boîtier IA) — Frontière de connectivité avec la configuration en streaming et la surveillance de l'état des appareils.
- Capteur (caméra / détecteur) — Granularité de données fine — vecteur d'application de règles individuelles.



> Tip
>
> ASTUCE — Héritage en cascade : Les arbres d'entités cascadent nativement. Sélectionner un client complet donne automatiquement accès à tous les sous-sites, appareils et capteurs en dessous. Il est essentiel de comprendre lors de la structuration des cartes d'accès pour les administrateurs seniors par rapport aux rôles de garde uniquement sur site.

Capacités clés

Tableaux de bord

- Nombre des sites actifs — Graphique linéaire montrant combien de sites transmettaient activement des données durant la période sélectionnée.
- Réel vs. Fausse alerte — Graphique en forme de donut montrant le ratio entre les alarmes réelles confirmées et les fausses alarmes filtrées par la plateforme. Dans un déploiement typique, 75 à 80 % des événements sont automatiquement filtrés.
- Appareils avec événements sans images — Tableau des dispositifs qui déclenchaient des événements mais n'y attachaient pas d'image. Indique les caméras nécessitant une calibration à l'aide d'images de référence ou une revue de la configuration du streaming.
- Types d'appareils Alert Push — Décomposition de la fréquence d'alarme par type d'appareil et type d'événement. Cela aide à identifier quelles intégrations causent le plus de fausses alarmes.

Navigation à gauche dans la barre latérale

- Tableau de bord — Page de présentation des indicateurs clés de performance.
- Alarmes — File d'attente d'alarme et gestion du flux de travail Talos.
- Sites — Vue d'ensemble et statut au niveau du site.

- Explorateur de périphériques — Visualiseur vidéo en direct avec structure hiérarchique du site/caméra.
- Carte — Vue satellite avec caméra et positionnement des capteurs.
- Rapports — HealthCheck et autres modules de rapport.
- Configuration — Paramètres d'administration pour les clients, sites, appareils et capteurs.
- Paramètres (icône d'engrenage) — Rôles, utilisateurs, tags et paramètres de compte.

Commandes de barre supérieure

- Recherche — Recherche globale dans toutes les entités. Raccourci clavier : Ctrl+K.
- Statut du mode local — Indique si vous êtes en mode cloud ou en mode de secours local.
- Filtre à plage de temps — Ajuste la fenêtre temporelle pour toutes les métriques du tableau de bord.
- Sélection de la langue — Modifie le langage de l'interface.

GCXONE vs. Evalink Talos

- Côté GCXONE : Ingère des flux en temps réel provenant de flottes connectées. Il exécute des pipelines IA NOVA99x pour rejeter les fausses alertes. Permet aux opérateurs la vidéo en direct et la lecture. Prend en charge une configuration profonde à travers les hiérarchies d'entités.
- Équipe Evalink Talos : Reçoit des signaux d'alarme vérifiés et effacés de GCXONE. Agit comme la couche de commandement tactique pour les files d'attente des opérateurs. Initie des chaînes d'escalade rapides et des règles SLA. Applique les organigrammes « Next Steps » pour la résolution de crises.

Cas d'usage réels

- Un fournisseur de services surveille des centaines de sites depuis un seul tableau de bord sans visiter aucun endroit.

- Un opérateur remarque un pic de caméras malsaines et oriente immédiatement un technicien pour la calibration.
- Un gestionnaire utilise le tableau de donuts Real vs. Fake Alerts pour vérifier que NOVA99x filtre correctement pendant une période de forte fréquentation.

Bonnes pratiques

- Vérifiez toujours le Caméras malsaines KPI au début de chaque service.
- Utilisation Appareils avec événements sans images Régulièrement pour capter les caméras qui nécessitent un recalibrage.
- Réglez le filtre par plage de temps pour qu'il corresponde à votre période de rapport avant de consulter les cartes KPI.
- Utilisation Ctrl+K Pour une recherche rapide d'entités au lieu de naviguer manuellement.

Détails supplémentaires

Naviguer dans les paramètres

Cliquez sur l'icône d'engrenage en bas de la barre latérale de navigation à gauche. Dans les Paramètres, vous pouvez gérer :

- Généralités — Paramètres au niveau de l'organisation.
- Profil utilisateur — Vos informations personnelles de compte.
- Rôles — Définir et configurer l'accès basé sur les rôles.
- Utilisateurs — Inviter et gérer les comptes utilisateurs.
- Rapports — Paramètres pour les rapports planifiés et à la demande.
- Gestion des tags — Gérer les dossiers des étiquettes des caméras.
- Locataire de commutateur — Passer d'un locataire fournisseur de services si vous en gérez plusieurs.