

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, expresse ou implicite — 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.

Configuration de l'alarme

Updated 16 August 2026

Ce que fait la configuration d'alarme

La configuration des alarmes dans GCXONE contrôle la manière dont les alarmes sont traitées, filtrées, transmises au CMS et présentées aux opérateurs. Elle régit l'ensemble du parcours de chaque alarme — de la détection à la résolution.

Pourquoi c'est important

Sans une configuration adéquate des alarmes, les alarmes vérifiées peuvent ne jamais atteindre le CMS, les opérateurs peuvent recevoir des alarmes sans contexte vidéo, ou des fausses alarmes peuvent inonder la station de surveillance. Une configuration correcte garantit que seules les alarmes vérifiées et exploitables atteignent les opérateurs — avec des preuves vidéo complètes jointes.

Comment ça fonctionne

Le cycle de vie de l'alarme

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

1. Appareils et caméras — Le capteur détecte un événement et envoie un signal à GCXONE.
2. Filtre IA NOVA99x — Le pipeline d'IA évalue l'événement. Les fausses alertes sont écartées.
3. Vérifié → CMS — Les alarmes confirmées sont transmises via DC-09 ou Talos.
4. Avis sur l'opérateur — L'opérateur CMS reçoit l'alarme avec les images pré-événement et le flux en direct.
5. Résolu + Audit — Le résultat est enregistré ; une trace d'audit immuable créée.

Deux chemins d'intégration CMS

- SIA DC-09 — Protocole standard de l'industrie pour la transmission d'alarmes IP. GCXONE étend chaque signal en injectant un lien web sécurisé intégrant des séquences pré-événement, des flux en direct et des encadrements IA dans la vue navigateur CMS.
- Evalink Talos — Plateforme native cloud avec architecture REST. Permet une synchronisation d'état bidirectionnelle, un déclenchement dynamique des opérateurs, et élimine complètement les contraintes de mappage IP héritées.

Configuration de l'intégration CMS DC-09

Naviguer vers Marketplace → système de gestion d'alarme.

1. Naviguer vers AMS sur Marketplace — Rendez-vous dans l'onglet Marketplace → Système de gestion d'alarme pour filtrer les intégrations de transmission disponibles.
2. Sélectionnez votre fournisseur CMS — Cliquez sur Explorer sur votre CMS (Amwin, Lisa, Immix, Manitou). Pour les fournisseurs non listés, sélectionnez « Autre système CMS » pour un canal DC-09 brut.
3. Spécifier les vecteurs de connexion — Entrer l'adresse IP du récepteur DC09 (IP publique WAN) et le port récepteur DC09 (port TCP sur le pare-feu du récepteur).
4. Initialiser le socket TCP — GCXONE envoie un ping au récepteur. Une poignée de main réussie met la carte à Configuré. Les alarmes ne circulent que pour les sites cartographiés.
5. Exécuter la cartographie site-compte-compte — Cliquez sur modifier sur chaque site. Définissez l'ID de compte DC09 (doit correspondre EXACTEMENT à la chaîne CMS — sensible aux majuscules) et une clé de chiffrement optionnelle.
6. Vérification de la transmission — Exécuter une séquence de test via l'onglet diagnostic. Les feux verts confirment que les paquets sont confirmés par le CMS.

Note

IMPORTANT — Défaillance la plus fréquente : Décalage de l'ID de compte : Plus de 85 % des échecs de transmission DC-09 résultent d'un identifiant de compte incompatible. Si le CMS attend « Site-A200 » mais que GCXONE envoie « Site_a200 », le récepteur défaisse silencieusement le paquet. Copier-coller depuis la configuration CMS plutôt que de retaper.

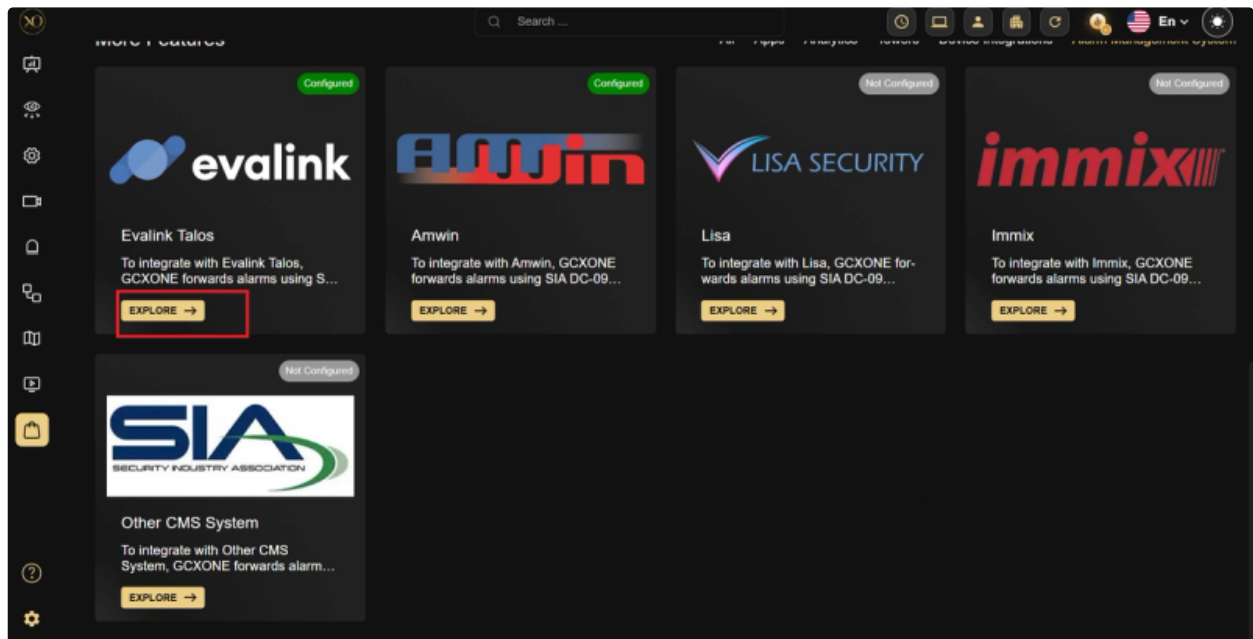
Customer	Site	Account Id	CMS	Action
Testing	syncstest	-	●	
Axis	Axis IO	-	●	
spykebox	New spyke box	-	●	
Testing Account 2026	2026	-	●	
Siemens Energy Inc	Siemens Bangalore	-	●	
Siemens Energy Inc	Sample	-	●	
Abdoun Circle	Map Demo	-	●	
Demo test	hikpro	-	●	
A.IAX	Coimbatore Office	-	●	

1-10 of 58 < > 1 row selected

Configuration de l'intégration Evalink Talos

Navigation : Système de gestion d'alarme → Marketplace → Evalink Talos → Configurer

1. **Crédentiels Harvest Talos** — Dans votre tableau de bord Talos, allez dans la gestion des API. Extraire votre clé API et l'identifiant de l'entreprise.
2. **Injecter des identifiants dans le marché** — Ouvrez la carte Evalink Talos dans GCXONE Marketplace. Collez les deux jetons et soumettez.
3. **Synchronisation bidirectionnelle confirmée** — Une bannière verte confirme la connexion. La synchronisation relie immédiatement les topologies GCXONE à Talos — aucun mappage manuel n'est nécessaire.



Cartographie des codes d'alarme

Naviguer vers Marketplace → AMS → Configuration du code d'alarme. Chaque code d'alarme est configuré selon un mode de livraison :

- Avec téléchargement de clips — Alarme envoyée au CMS + clip vidéo pré-événement téléchargé et attaché automatiquement. À utiliser lorsque des preuves médico-légales sont requises au CMS.
- Diffusion uniquement en direct — Alarme envoyée au CMS + l'opérateur CMS reçoit un lien en direct. Utilisez pour la réponse en temps réel lorsque la latence de téléchargement est inacceptable.
- Handicapé — Type d'alarme supprimé, non transmis au CMS. Utilisez pour les sources faussement positives connues en attendant l'ajustement de l'IA.

AutoStream Configuration

AutoStream ouvre automatiquement un flux de caméra en direct dans la vue opérateur lorsqu'une alarme vérifiée arrive.

Navigation : Configuration → [Site] → [Appareil] → Paramètres AutoStream

1. Activez l'AutoStream pour l'appareil.

2. Réglez le tampon pré-événement (quelques secondes avant le déclenchement). Point de départ recommandé : 10 secondes.
3. Réglez le tampon post-événement (quelques secondes après le déclenchement). Point de départ recommandé : 20 secondes.
4. Sélectionnez quels types d'alarmes déclenchent l'AutoStream pour cet appareil.

Capacités clés

Dépannage du flux d'alarme

SYMPTÔME	CAUSE	CORRECTION
L'alarme affiche Envoyé en GCXONE mais CMS ne la reçoit jamais	Incompatibilité d'identifiant de compte	Copier-coller l'ID de compte depuis CMS ; vérifier le cas exact et les caractères
La carte AMS affiche rouge / déconnectée	Pare-feu bloquant l'IP ou le port DC09	Vérifiez que l'IP WAN et le port TCP sont ouverts
Alarme reçue au CMS mais pas de liaison vidéo	AutoStream non activé pour l'appareil	Activer AutoStream dans la configuration de l'appareil
Toutes les alarmes sont supprimées après la modification du code mapping	Code mappé en mode désactivé	Examiner la configuration du code d'alarme dans AMS
Talos ne reçoit pas de mises à jour topologiques	ID d'entreprise ou clé API invalides	Re-paste les identifiants depuis Talos API Management

Cas d'usage réels

- Un fournisseur de services connecte GCXONE à un CMS Immix via DC-09 — les opérateurs reçoivent des alarmes avec des images pré-événement intégrées directement dans la vue navigateur.
- Un administrateur passe de DC-09 à Evalink Talos pour éliminer la cartographie manuelle site-à-compte et obtenir une synchronisation bidirectionnelle.

- Un opérateur remarque que toutes les alarmes d'un appareil spécifique sont supprimées — l'administrateur examine la configuration du code d'alarme et constate que le code a été réglé sur Désactivé en attendant l'ajustement de l'IA.
- Un nouveau site est mis en ligne mais les alarmes n'arrivent jamais au CMS — l'administrateur détecte un défaut d'identification de compte et le corrige en copiant-collant depuis le CMS.

Bonnes pratiques

- Copier-coller toujours l'ID de compte DC09 directement depuis le CMS — ne le retape jamais manuellement.
- Utilisation Evalink Talos sur DC-09 lorsque possible afin d'éliminer la cartographie manuelle et d'obtenir une synchronisation bidirectionnelle.
- Réglez AutoStream Pre-Event Buffer à au moins 10 secondes pour fournir aux opérateurs suffisamment de contexte avant le déclenchement.
- Utilisation Handicapé le mode dans la cartographie du code d'alarme uniquement comme mesure temporaire pendant l'ajustement de l'IA — pas comme une suppression permanente.
- Effectuez le test de transmission de diagnostic après chaque changement de configuration avant de passer en ligne.