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.

Rôles et permissions

Updated 16 August 2026

Comprendre RBAC dans GCXONE

GCXONE utilise le contrôle d'accès basé sur les rôles (RBAC) pour déterminer exactement ce que chaque utilisateur peut voir et faire. Chaque utilisateur doit se voir attribuer un rôle — sans celui-ci, il se retrouve immédiatement sur un écran bloqué après la connexion. Les rôles combinent trois éléments : les modules auxquels ils peuvent accéder, les actions qu'ils peuvent effectuer dans chaque module, ainsi que les clients et sites sur lesquels ils peuvent opérer.

⚠ 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.

L'écran de gestion des rôles

Naviguer vers Cadres → rôles . L'écran de gestion des rôles liste chaque rôle dans le tenant avec le nombre d'utilisateurs et les actions.

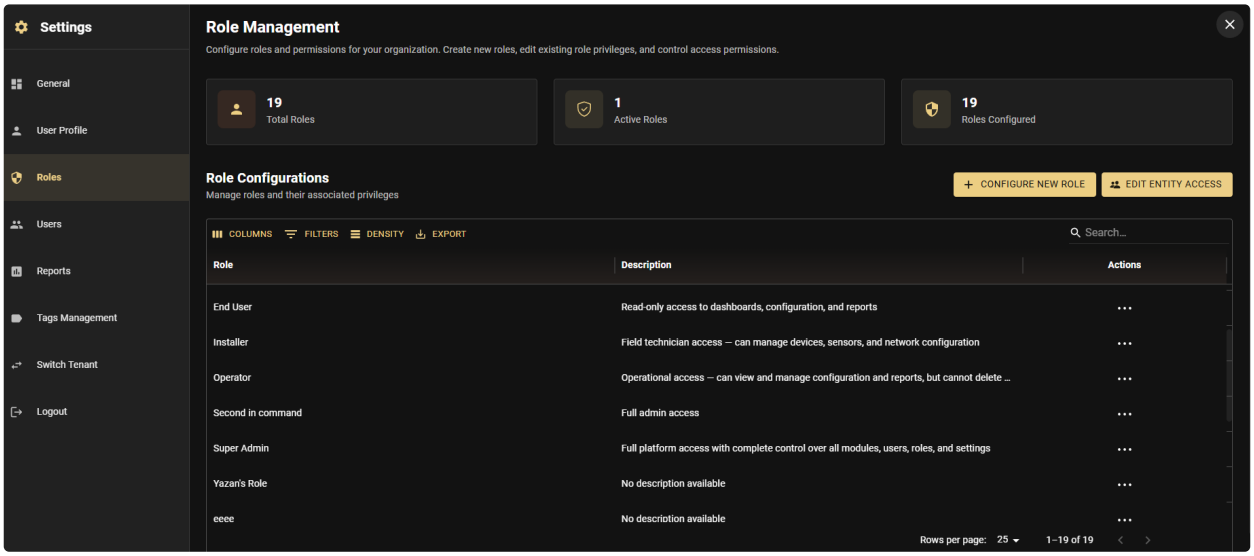

Figure 3.1 — Settings → Roles. Lists every role with user counts and edit actions.

Création d'un rôle personnalisé

Naviguer vers Paramètres → rôles → Configurer un nouveau rôle .

Étape 1 — Informations sur le rôle

Entrez dans le rôle Nom et Description . Bascule Rôle par défaut On demande si chaque nouvel utilisateur invité doit recevoir automatiquement ce rôle.

Nommer les rôles spécifiquement — « *NL Operator – Securitas* » est plus utile dans les journaux d'audit que « *Opérateur 2* ».

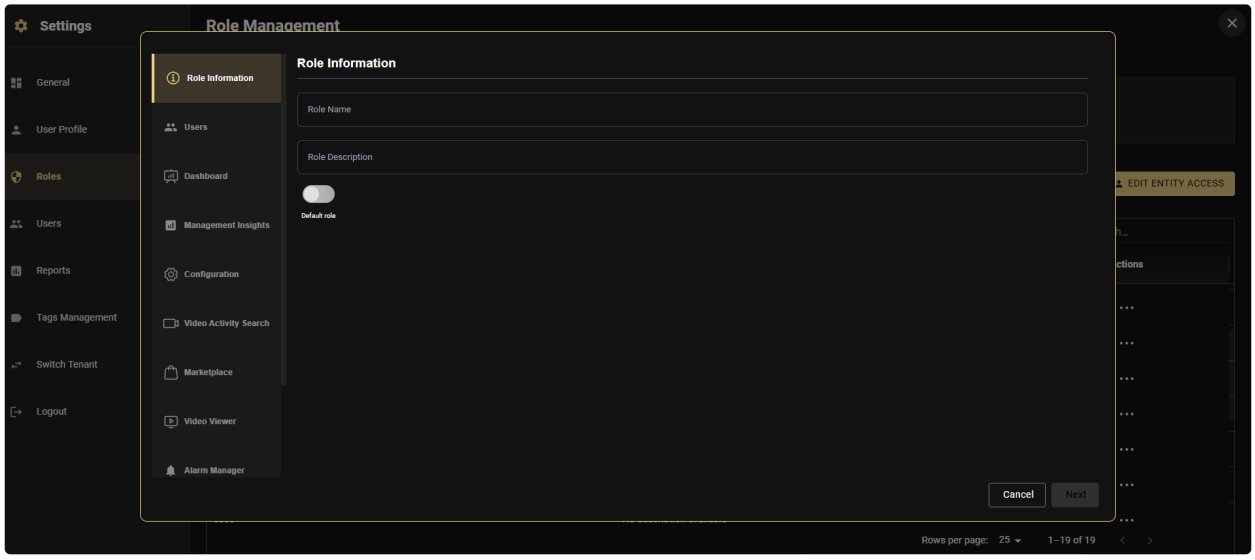

Figure 3.2 — The role wizard opens with Role Information. Name the role specifically.

Étape 2 — Permissions des modules

Parcourez chaque module de plateforme dans le panneau de gauche. Accordez ou supprimez des fonctionnalités spécifiques par module — tableau de bord, configuration, recherche d'activité vidéo, marketplace, gestionnaire d'alarmes, Talos, et plus encore.

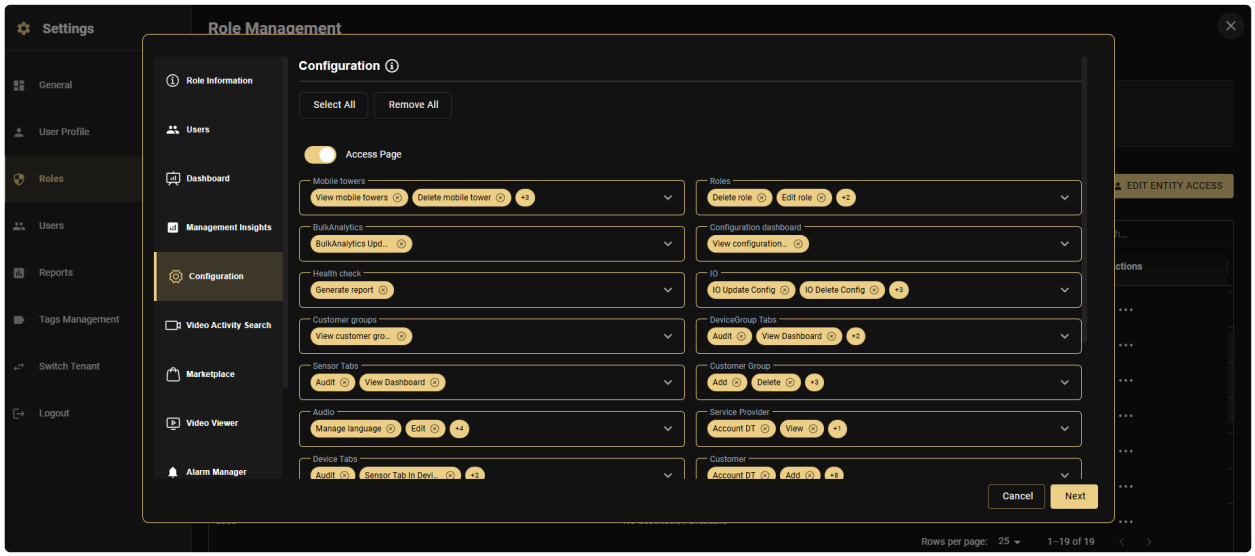

Figure 3.3 — Each module has granular capabilities. The Configuration tab controls adding customers and editing device credentials — Admin only.

Étape 3 — Accès à l'entité

Définissez quels clients, sites et appareils ce rôle peut opérer. ActiverInclure les enfants sur tout parent pour inclure automatiquement toutes les sous-entités — y compris les ajouts futurs.

Modes d’accès à l’entité

Accès complet

Le rôle voit chaque client et site dans le locataire. Utilisez uniquement pour les comptes administratifs internes.

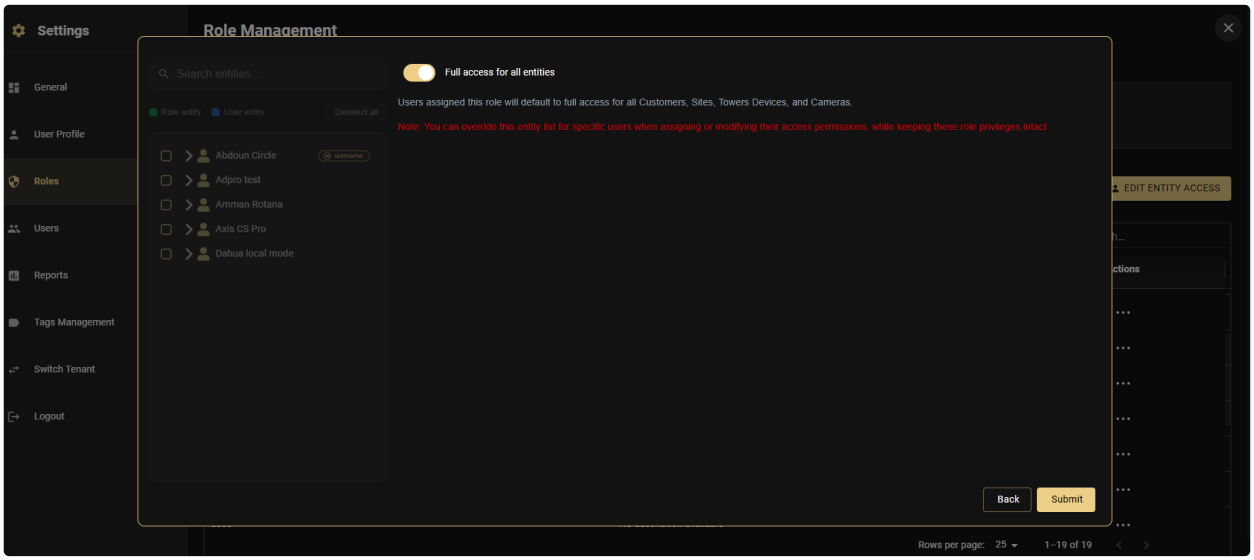

Figure 3.4 — Full Access mode. Use only for internal admin accounts.

Entités sélectionnées

Attribuez des clients et des sites spécifiques. ActiverInclure les enfants pour inclure automatiquement toute sous-entité ajoutée à l’avenir.

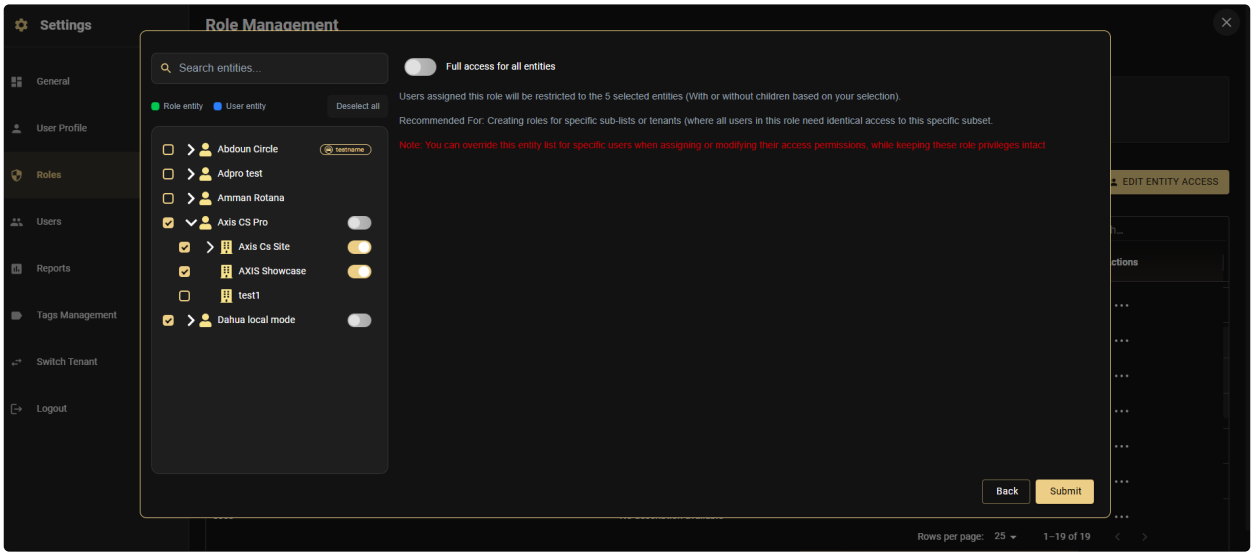

Figure 3.5 — Selected Entities mode with Include Children toggle.

Mode de dérogation

IMPORTANT — Mode de dérogation : Ça agit comme un remplacement complet. Définir une Outremise sur « Site Beta » révoque entièrement l'accès à toute « Site Alpha » précédemment détenue. À utiliser pour une confinement géographique strict.

Mode de fusion

REMARQUE — Mode de fusion : Agit de façon additive. Attribution de rôle « Site Alpha » + Fusion « Site Beta » = les deux sites accessibles. Idéal pour une couverture croisée temporaire lorsque les opérateurs assistent un autre local.

Référence de configuration des rôles

- Super Admin — Tous les modules. Entité : Accès complet.
- Administration — Tableau de bord, configuration, insights, rapports, marché. Entité : Complète ou Sélectionnée.
- Opérateur — tableau de bord, gestionnaire d'alarmes, visualiseur vidéo, carte. Entité : Entités sélectionnées.
- Installateur — Configuration (Appareils), Visualiseur vidéo (Live). Entité : Par site via Override.

- Utilisateur final — tableau de bord, visualiseur vidéo (en direct uniquement). Entité : Sites sélectionnés.
- Technicien de terrain — Visualiseur vidéo, gestionnaire d'alarme (armement/désamorçage), carte. Entité : Outremise par technicien.

Outrecommande d'accès à l'entité par utilisateur

Personnalisez l'accès à l'entité pour un utilisateur individuel sans créer un rôle séparé.

1. Naviguer vers Paramètres → utilisateurs → [utilisateur] → Modifier l'accès à l'entité .
2. Sélectionner Outremise ou Fusion mode.
3. Ajouter ou supprimer des clients, sites ou appareils spécifiques.
4. Sauvegarder — l'override s'applique immédiatement.

Redressement des rôles après la migration

L'utilisateur voit un accès refusé sur un module qu'il avait auparavant

1. Ouvrez leur rôle → permissions du module → vérifiez que la capacité n'a pas été supprimée lors de la modification du rôle.
2. Vérifiez le journal d'audit → filtrez par utilisateur et date.

L'utilisateur ne peut pas voir un site récemment ajouté

1. Vérifiez si leur rôle utilise des entités sélectionnées sans inclure des enfants.
2. Soit activez Inclure les enfants sur le client parent, soit ajoutez manuellement le nouveau site au rôle.

L'utilisateur a accès à des sites qu'il ne devrait pas

1. Vérifiez s'il existe des dérogations de fusion actives sur l'utilisateur.
2. Naviguer vers Paramètres → utilisateurs → Modifier l'accès à l'entité .
3. Supprimez les entrées de fusion non désirées.