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.

Gestion des utilisateurs

Updated 16 August 2026

Ce que fait la gestion des utilisateurs

La gestion utilisateur dans GCXONE contrôle qui peut accéder à la plateforme, ce qu'ils peuvent voir, et avec quelles entités ils peuvent interagir. Chaque utilisateur est rattaché à un locataire et hérite de l'accès de son rôle assigné — avec la possibilité de passer outre ou d'étendre cet accès par utilisateur sans modifier le rôle partagé.

Pourquoi c'est important

Sans utilisateurs correctement configurés, les opérateurs peuvent voir des entités qu'ils ne devraient pas, ou être complètement bloqués. La gestion des utilisateurs garantit que les bonnes personnes ont le bon accès — et que cet accès est immédiatement révocable lorsque nécessaire.

Comment ça fonctionne

> Note
>
> i INFO — Prérequis : Complétez votre structure de rôle avant d'inviter les utilisateurs. Voir Rôles & Autorisations.

Inviter un nouvel utilisateur

Naviguer vers Paramètres → les utilisateurs → inviter de nouveaux utilisateurs.

1. Saisissez l'adresse e-mail de l'utilisateur.
2. Sélectionnez leur rôle dans le menu déroulant (doit exister avant l'invitation).
3. Éventuellement, définissez une dérogation personnalisée d'accès à l'entité au moment de l'invitation.

4. Click Envoyez une invitation.

GCXONE envoie un e-mail d'invitation depuis `no-reply@nxgen.cloud`. Le lien d'invitation expire après 7 jours. Réenvoyer via Paramètres → utilisateurs → [Ligne utilisateur] → Réenvoyer une invitation.

Que se passe-t-il lorsqu'un utilisateur accepte

1. L'utilisateur clique sur le lien d'invitation.
2. Ils sont invités à définir un mot de passe (le jeton expire après 24 heures).
3. Lors de leur première connexion, ils atterrissent sur le module par défaut que leur rôle accorde.
4. Si aucun rôle n'est attribué, ils voient un écran bloqué — attribuez un rôle immédiatement.

Configuration de l'accès à l'entité par utilisateur

Un utilisateur hérite de l'accès à l'entité de son rôle assigné. Vous pouvez écrire ou prolonger cela par utilisateur sans modifier le rôle partagé.

Navigation : Paramètres → utilisateurs → [utilisateur] → Modifier l'accès à l'entité

- Mode de dérogation — Remplace entièrement l'accès à l'entité héritée par le rôle de l'utilisateur. Exemple : le rôle d'opérateur accorde le Client A. Le Contrôle avec le Client B → l'utilisateur ne peut voir que le Client B.
- Mode de fusion — Ajoute l'accès à l'entité en plus de ce que le poste accorde. Exemple : le rôle d'opérateur accorde le client A. Fusion dans le client B → l'utilisateur peut voir les deux. À utiliser pour une couverture croisée temporaire ou un accès unique.

> Tip
>
> Bonnes pratiques : Privilégiez la fusion plutôt que la création d'un nouveau rôle lorsque l'exigence d'accès est temporaire ou spécifique à l'utilisateur. Utilisez Override uniquement lorsque vous devez totalement restreindre à un ensemble d'entités différent.

Modifier un utilisateur existant

1. Naviguer vers Paramètres → utilisateurs.
2. Click Édit sur la ligne utilisateur.
3. Champs modifiables : attribution de rôle, dérogation d'accès à l'entité, e-mail et statut du compte.
4. Les changements entrent immédiatement en vigueur — l'action suivante de l'utilisateur reflète le nouvel accès.

Gestion d'un utilisateur disparu

1. Paramètres → utilisateurs → [utilisateur] → désactiver — révoque immédiatement tout accès.
2. Auditez leurs activités récentes dans Configuration → Audit Avant de désactiver en cas de problème de sécurité.
3. Réattribuez toutes les alarmes ou tickets ouverts qu'ils possédaient.

> Note
>
> i INFO — Ne pas supprimer les enregistrements d'utilisateurs : Les entrées historiques du journal d'audit font référence à l'identifiant utilisateur. La désactivation préserve l'enregistrement tout en bloquant l'accès. Supprimer élimine la traçabilité médico-légale.

Capacités clés

Référence de statut utilisateur

STATUT	SIGNIFICATION
Actifs	L'utilisateur a accepté l'invitation et peut se connecter.
En attente	Invitation envoyée mais pas encore acceptée. Réenvoyez si c'est expiré.
Bloqué	L'utilisateur existe mais n'a pas de rôle assigné. Attribuez un rôle.

Inactifs	Compte désactivé par l'administrateur. Réactivez si besoin.

Gestion massive des utilisateurs via CSV

Exportez le modèle : Naviguer vers Paramètres → utilisateurs → importer → télécharger un modèle.

Colonnes obligatoires : `Email` (obligatoire), `role_name` (doit correspondre exactement à un nom de rôle existant, à la majuscule), `first_name`, `last_name` (optionnel mais recommandé).

Préparez le CSV :

- Un utilisateur par ligne.
- Les noms des rôles doivent correspondre exactement — `NL Operator` non `Opérateur nl`.
- Les e-mails en double sont sautés (les enregistrements utilisateurs existants ne sont pas écrasés).

Téléchargement et critique :

1. Téléchargez le CSV complet.
2. L'analyseur pré-vol met en évidence les lignes avec des erreurs (noms de rôles inconnus, emails invalides).
3. Corrigez les erreurs et téléversez à nouveau, ou procédez uniquement aux lignes valides.
4. Tous les utilisateurs valides reçoivent simultanément des e-mails d'invitation.

Gestion des utilisateurs multi-locataires

Les utilisateurs sont évalués par locataire. Un utilisateur du locataire A n'a aucune visibilité sur le locataire B sauf si un compte séparé est créé dans le locataire B.

Pour changer de locataire en tant qu'administrateur : Paramètres → Switch Tenant.

Cas d'usage réels

- Un nouvel opérateur rejoint l'équipe — l'administrateur l'invite, lui attribue le rôle d'Opérateur, et ils sont opérationnels en quelques minutes.

- Un agent de sécurité a besoin d'un accès temporaire à un second site en cas de pénurie de personnel — l'administration utilise le mode Merge au lieu de créer un nouveau rôle.
- Un fournisseur de services embarque 200 utilisateurs répartis sur plusieurs clients en utilisant BulkImport CSV en un seul upload.
- L'accès d'un employé disparu est immédiatement révoqué via la désactivation — la piste d'audit reste intacte pour un examen médico-légal.

Bonnes pratiques

- Terminez toujours la configuration des rôles avant d'inviter les utilisateurs — un utilisateur sans rôle atterrit sur un écran bloqué.
- Utilisation Mode de fusion pour un accès temporaire ou spécifique à l'utilisateur plutôt que de créer des rôles ponctuels.
- Utilisez BulkImport CSV pour toute intégration impliquant plus de 10 utilisateurs.
- Ne supprimez jamais les enregistrements utilisateurs — désactivez-les plutôt pour préserver l'intégrité des traces d'audit.
- Révision de l'activité récente des utilisateurs quittés dansConfiguration → Audit Avant de désactiver en cas de problème de sécurité.