

Disclaimer

Legal disclaimer

This guide and its contents (the "Guide") are provided by NXGEN. All rights to the Guide and to the intellectual property embodied in it — including, without limitation, trademarks, trade names, logos and similar marks appearing in or on it — are protected by law. All right, title and interest in the Guide and in any related intellectual property rights belong to and remain with NXGEN and its licensors.

The Guide is provided free of charge, "as is" and for informational purposes only, without warranty of any kind. It is neither intended nor suitable to establish any legal relationship between the reader and NXGEN or its affiliates, including, without limitation, any obligation of NXGEN or its affiliates toward the reader.

The obligations of NXGEN and its affiliates in respect of NXGEN products or services purchased by a customer are governed exclusively by the terms of the agreement under which those products or services were purchased.

For clarification

The reader bears the entire risk as to the use, results and performance of the Guide. To the fullest extent permitted by applicable law, NXGEN disclaims and excludes all warranties, whether statutory, express or implied — including, without limitation, implied warranties of merchantability, fitness for a particular purpose, title and non-infringement of third-party rights — as well as any liability or warranty arising from suggestions, specifications or samples related to the Guide.

User Management

Updated 16 August 2026

What User Management Does

User Management in GCXONE controls who can access the platform, what they can see, and which entities they can interact with. Every user is scoped to a tenant and inherits access from their assigned role — with the option to override or extend that access per user without modifying the shared role.

Why It Matters

Without properly configured users, operators may see entities they shouldn't, or be blocked entirely. User Management ensures the right people have the right access — and that access is immediately revocable when needed.

How It Works

Prerequisites

Complete your role structure before inviting users. See Roles & Permissions.

Inviting a New User

Navigate to Settings → Users → Invite New User.

1. Enter the user's email address.
2. Select their role from the dropdown (must exist before invitation).
3. Optionally set a custom entity access override at invitation time.
4. Click Send Invitation.

GCXONE dispatches an invitation email from `no-reply@nxgen.cloud`. The invitation link expires after 7 days. Resend via Settings → Users → [User Row] → Resend Invitation.

What Happens When a User Accepts

1. User clicks the invitation link.
2. They are prompted to set a password (token expires after 24 hours).
3. On first login, they land on the default module their role grants.
4. If no role was assigned, they see a blocked screen — assign a role immediately.

Configuring Entity Access Per User

A user inherits entity access from their assigned role. You can override or extend this per user without modifying the shared role.

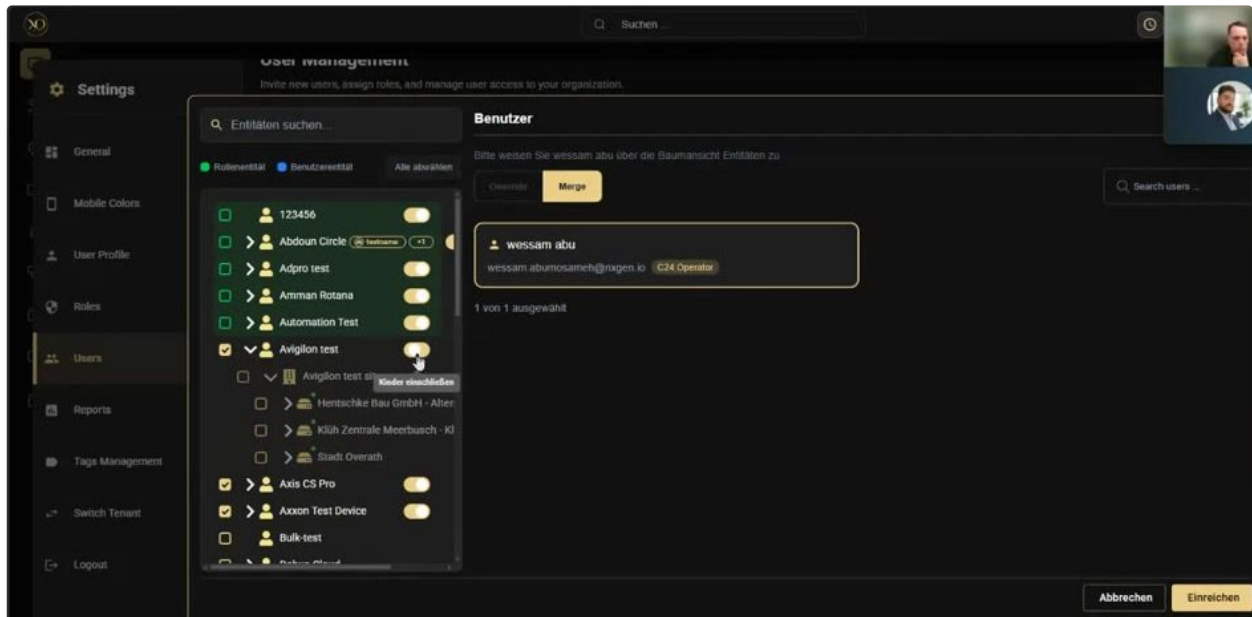
Navigation: Settings → Users → [User] → Edit Entity Access

- **Override Mode** — Replaces the user's role-inherited entity access entirely. Example: Operator role grants Customer A. Override with Customer B → user can only see Customer B.
- **Merge Mode** — Adds entity access on top of what the role grants. Example: Operator role grants Customer A. Merge in Customer B → user can see both. Use for temporary cross-coverage or one-off access.

Tip

Best Practice: Prefer Merge over creating a new role when the access requirement is temporary or user-specific. Use Override only when you need to fully restrict to a different entity set.

Editing an Existing User



User entity access tree allowing granular customer and site assignment

1. Navigate to Settings → Users.
2. Click Edit on the user row.
3. Changeable fields: role assignment, entity access override, email, and account status.
4. Changes take effect immediately — the user's next action reflects the new access.

Managing a Departed User

1. Settings → Users → [User] → Deactivate — immediately revokes all access.
2. Audit their recent activity in Configuration → Audit before deactivating if there's a security concern.
3. Reassign any open alarms or tickets they owned.

Do Not Delete User Records

Historical audit log entries reference the user ID. Deactivation preserves the record while blocking access. Deleting removes forensic traceability.

Key Capabilities

User Status Reference

STATUS	MEANING
Active	User accepted invitation and can log in.
Pending	Invitation sent but not yet accepted. Resend if expired.
Blocked	User exists but has no role assigned. Assign a role.
Inactive	Account disabled by admin. Re-enable if needed.

Bulk User Management via CSV

Export the Template: Navigate to Settings → Users → Import → Download Template. Required columns:

email (required), role_name (must exactly match an existing role name, case-sensitive), first_name, last_name (optional but recommended).

Prepare the CSV:

- One user per row.
- Role names must match exactly — `NL Operator` not `nL operator`.
- Duplicate emails are skipped (existing user records are not overwritten).

Upload and Review:

1. Upload the completed CSV.
2. The pre-flight parser highlights rows with errors (unknown role names, invalid emails).
3. Fix errors and re-upload, or proceed with valid rows only.
4. All valid users receive invitation emails simultaneously.

Multi-Tenant User Management

Name	Email	Customer Group	Contact Number	Active	Actions
Ritoma Scania Drachten		N/A	N/A	●	...
Gede verpakkingen Alkmaar		N/A	N/A	●	...
Schol Alkmaar		N/A	N/A	●	...
Eurohall		N/A	N/A	●	...
Spykebox13	spyke@joon.nl	N/A	N/A	●	...
Parkmanagement Hoon PMH		N/A	N/A	●	...
Tebstar 1963		N/A	N/A	●	...
Gallerij Colorado		N/A	N/A	●	...
Bijlgroep Alkmaar		N/A	N/A	●	...
Bijlgroep Haarlem		N/A	N/A	●	...
Vlaagredde		N/A	N/A	●	...
Zonnepark Albero Montfort		N/A	N/A	●	...
Windpark Westfriesland		N/A	N/A	●	...
Toka Kranen		N/A	N/A	●	...

Customer configuration table in the admin panel

Users are scoped per tenant. A user in Tenant A has no visibility into Tenant B unless a separate account is created in Tenant B.

To switch tenants as an admin: Settings → Switch Tenant.

Real-World Use Cases

- A new operator joins the team — admin invites them, assigns the Operator role, and they're operational within minutes.
- An Operator needs temporary access to a second site during staff shortage — admin uses Merge Mode instead of creating a new role.
- A service provider onboards 200 users across multiple customers using BulkImport CSV in a single upload.
- A departed employee's access is revoked instantly via Deactivate — audit trail remains intact for forensic review.

Best Practices

- Always complete role configuration before inviting users — a user with no role lands on a blocked screen.
- Use Merge Mode for temporary or user-specific access rather than creating one-off roles.
- Use BulkImport CSV for any onboarding involving more than 10 users.
- Never delete user records — deactivate instead to preserve audit trail integrity.
- Review departed users' recent activity in Configuration → Audit before deactivating if there's a security concern.