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.

Managing Users

Updated 8 October 2026

experience — not included in the PDF

What Managing Users Does

Once users are onboarded, administrators can modify their access, permissions, and entity visibility as their responsibilities evolve. All user management is done from Settings → Users.

Why It Matters

User access that isn't maintained becomes a security risk. Operators who change roles, leave the organization, or take on new sites need their access updated immediately — Managing Users ensures access always reflects current responsibilities.

How It Works

Each user in GCXONE has two layers of access control:

- Role — Defines what the user can do (privileges and module access).
- Entity Access — Defines which customers, sites, devices, and sensors the user can see.

Both can be updated independently at any time. Changes take effect immediately — the user may need to refresh their browser to see updates.

Entity access can be adjusted per user without creating or editing a role at all: Override replaces whatever the role grants with a custom selection, and Merge adds a custom selection on top of it — useful for temporary or one-off access without disturbing the shared role.

Key Capabilities

Viewing and Searching Users

Navigate to Settings → Users. Use the search bar to find a user by name or email.

Editing a User

Editing a user opens the same Personal Information, Address Information, and Account Settings fields set when they were invited — including their Genesis Role, GCXONE Role, Customer Group, Session Timeout, Partner Login, and MFA — pre-filled for update. Saving takes effect immediately; the user's next action reflects the new access. For the full field list and the exact dialog, refer to User Management.

Editing User Entity Access

Entity access is changed independently of the role, through Override or Merge mode (see How It Works above), with an Include Children option so a parent customer or site automatically carries any current and future sub-entities without being re-selected one by one. For the click-by-click steps, refer to User Management.

Removing a User

Removing a user deletes their record from the platform immediately, with no confirmation step — the user disappears from the Users table as soon as you click Remove User, and the action cannot be undone. There is no way to restore a removed user's account; for temporary access removal, restrict their role or entity access instead of removing them outright.

Real-World Use Cases

- An operator is promoted to admin — their role is updated in under a minute and changes take effect immediately without re-inviting them.
- A new site is added to a customer — admin uses Merge mode to add the site to the relevant operators' entity access without touching their existing permissions.

- A team member leaves — admin removes their access immediately from the Users table and confirms during the next quarterly audit that no inactive accounts remain.

Best Practices

- Quarterly Audits — Review your user list every 3 months. Remove or restrict access for users who are no longer active.
- Offboarding — Remove user access immediately when a team member leaves the organization.
- Avoid Shared Accounts — Never share a single login between multiple people, as this destroys the audit trail.
- Double-check before removing — Remove User has no confirmation prompt, so confirm you have the right row selected before clicking it.

Additional Details

Troubleshooting

User Cannot See a Site or Camera Check their entity access via Edit User Entities. Ensure the relevant site or customer is selected with Include Children enabled.

Permission Changes Not Reflected Changes take effect within 5 seconds. Ask the user to refresh their browser tab.

User Locked Out Remove and re-invite the user if they cannot reset their password through the standard flow.

Talos Page Does Not Load in a Private Window If the user opens GCXONE in a private (incognito) browser window, the Talos page may not load. Ask them to allow third-party cookies for the page; it reloads and Talos opens.

Cannot Sign In to Local Mode Check that the user has the latest version of Local Mode. See Local Mode.