

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.

Understanding Roles & Access Control

Updated 23 September 2026

Summary

GC Surge uses role-based access control (RBAC) to ensure each user can only access the platform features and data appropriate for their organizational function. Roles are assigned at invitation and control which sidebar modules are visible, which actions are available, and what data can be accessed. Covers: What Roles & Access Control Does, GC Surge Roles, The User List, How Role Assignment Works, Principle of Least Privilege, Access Governance Best Practices.

What Roles & Access Control Does

Proper role governance is both a security requirement and an operational efficiency tool. Over-privileged accounts create unnecessary risk. Under-privileged accounts create friction and support burden.

GC Surge Roles

Super Admin

Full platform access. Super Admins can create and modify sites, manage users (invite, assign roles, and remove users), configure NOVA99x, manage the subscription, view all analytics, and access all event review tools.

Super Admins should be limited to the individuals who genuinely need full platform control. Every Super Admin account is a potential attack surface — if one is compromised, the attacker gains access to all platform functions.

Operator

Access to operational tools. The Operator sidebar shows two modules: Alarm Center and Operator Performance. Opening a site from Alarm Center with View launches ZenMode, the alarm-processing screen. Video Search is also available to Operators, though it is not a sidebar entry. Operators cannot manage sites, users, or subscription settings. This is the appropriate role for monitoring center operators and shift supervisors who need event access but should not make administrative changes.

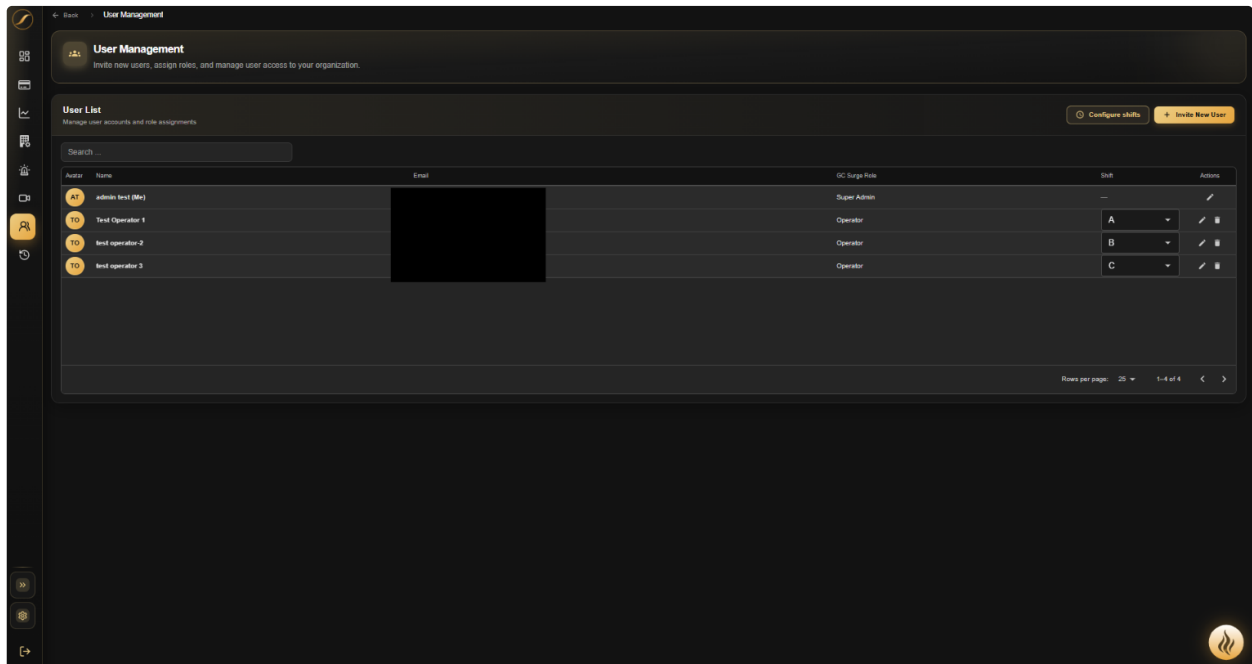


image-20260726-073443.png

The User List

Users & Shifts Management is accessible from the sidebar and opens the User List — a table showing every user on the account. The subtitle reads: *Invite new users, assign roles, and manage user access to your organization.*

Table columns

- Avatar — a color-coded initials badge (or uploaded photo) identifying the user at a glance.
- Name — the user's first and last name.
- Email — the email address used to log in and receive platform notifications.

- GC Surge Role — either Super Admin or Operator .
- Shift — a dropdown to assign the user to one of the configured shifts (Default, or any shift created via Configure shifts).
- Actions — two icons visible directly in the row: a pencil icon (Edit User) and a trash icon (Remove User).

Pagination

Rows per page controls how many users appear per page. The counter on the right (e.g. 1–5 of 5) shows the visible range and total count. Use the arrow buttons to navigate between pages.

User Actions

- Edit User — opens a modal to update the user's name, photo, phone number, or role.
- Remove User — deactivates the user account. All active sessions end immediately and the user loses access. Their historical actions are preserved in the [audit trail](#).

Inviting a New User

The + Invite New User button (top right of the User List) opens the invitation modal. Required fields are marked with an asterisk (*):

- First Name* and Last Name* — used for the display name and the initials avatar.
- Email Address* — the address where the invitation link is sent. This becomes the user's login email.
Email address is immutable after the invitation is accepted — it is the user's account identity. To change it later, invite a new user with the new email, transfer their role and entity assignments, then deactivate the old account.
- Phone Number — optional. Includes a country code selector (flag + dial code). Useful if the user is an on-site contact whose Site Key is sent over WhatsApp.

- **GC Surge Role** — select either **Operator** or **Super Admin** from the dropdown. The role determines which platform features are accessible from the moment the user accepts the invitation. An info icon next to the field label identifies it as an account setting that cannot be left blank.
- **Upload Photo** — optional profile photo. Recommended: square image, at least 200×200 px. If no photo is uploaded, the platform generates an initials badge automatically.

The same form appears when selecting **Edit User** for an existing user, allowing role and personal information to be updated after onboarding. When inviting, clicking **Send Invitation** sends an invitation email and displays a “User invited successfully” banner. The invited user receives an email from noreply@nxgen.io with the subject “You’ve been invited to GC Surge”, prompting them to set a password and complete onboarding. The user can log in immediately after activating their account. Role assignments apply from the first login — no additional approval step.

Once the invitation is sent, share the following guide with the new operator: [Accept Your Invitation as an Operator](#).

How Role Assignment Works

Roles are assigned when a user is invited to the platform. The inviting Super Admin selects the role from a dropdown in the invitation modal. The invitee receives the role as part of their account from the moment they accept the invitation — they do not need to request access separately.

To change an existing user’s role, a Super Admin opens the User List, locates the user, and clicks the pencil icon (**Edit User**) on the user’s row to update their role assignment. The change takes effect immediately on the user’s next page load or login.

Principle of Least Privilege

Always assign the minimum role that allows the user to perform their function:

- **Monitoring operators:** **Operator** role. They need **Alarm Center** (for ZenMode alarm processing and Video Search) and **Operator Performance** to review their shift results. They do not need **Configuration**

- Shift supervisors: Operator role. Operators can already review their own shift performance from Operator Performance. If a supervisor also needs access to organization-wide analytics or site management, Super Admin is required — document and review this access regularly.
- Site administrators responsible for onboarding: Super Admin role, but this should be a small group.
- Finance contacts reviewing billing: Super Admin role. If Super Admin access must be granted, document and review it regularly.

Access Governance Best Practices

- Review the user roster regularly — at minimum monthly for active deployments, quarterly for stable ones. Use Remove User for any user who has left the organization or no longer needs access.
- Document your role assignment policy. Write down the rules your organization uses to determine who gets which role. This prevents inconsistency and makes onboarding new staff easier.
- Audit Super Admin accounts explicitly. Know exactly who has Super Admin access at all times. The list should be short and intentional.
- Use business email addresses. Personal email addresses make account management and recovery harder, and create risk if a user leaves the organization but retains access to their personal email.
- Handle departures immediately. When an employee leaves, remove their account using Remove User on their last day. Do not wait for the next review cycle.