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 Roles & Permissions

Updated 16 August 2026

Understanding RBAC in GCXONE

GCXONE uses role-based access control (RBAC) to determine exactly what each user can see and do.

Every user must be assigned a role — without one, they land on a blocked screen immediately after login.

Roles combine three things: the modules they can access, the actions they can perform within each module, and which customers and sites they can operate on.

> ⚠ Warning — Set up Roles Before Inviting Users: A user invited without a role assigned lands on a blocked screen the moment they log in and stays blocked until an admin manually assigns them a role. Design your role structure, create the roles, then invite users.

The Role Management Screen

Navigate to Settings → Roles. The Role Management screen lists every role in the tenant with user counts and actions.

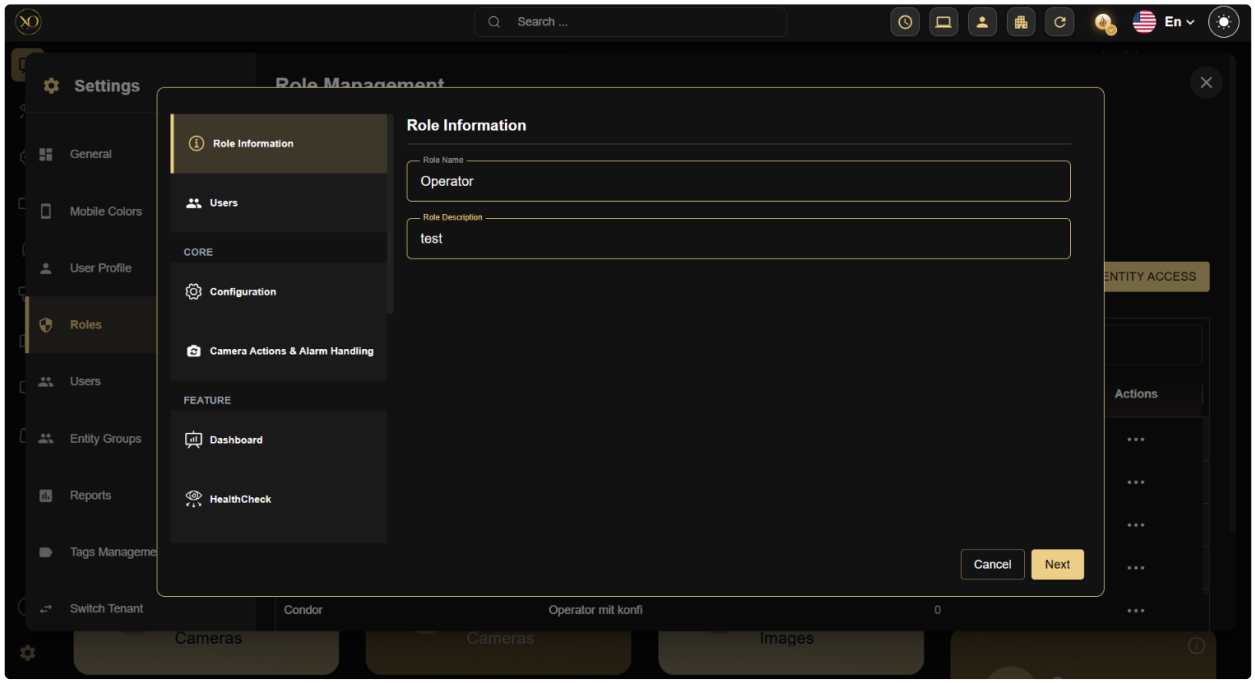
Creating a Custom Role

Navigate to Settings → Roles → Configure New Role.

Step 1 — Role Information

Enter the role Name and Description.

Name roles specifically — it's more useful in audit logs than *"Operator 2"*.



Configure New Role wizard — Role Information step

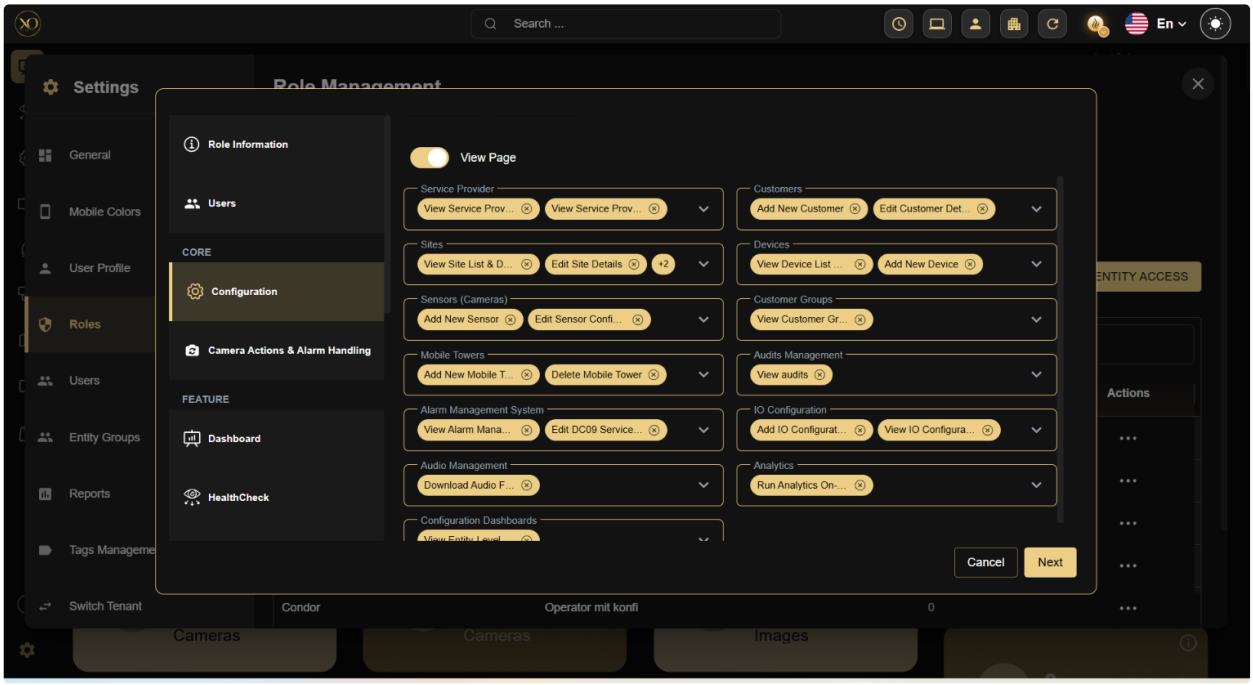
The role wizard opens with Role Information. Name the role specifically.

Step 2 — Users

Select which users should be assigned to this role from the searchable user grid. Use Select All, Remove All, or search to manage the list in bulk.

Step 3 — Module Privileges

Work through each platform module in the left panel, grouped into Core, Feature, and System. Grant or remove specific capabilities per module — Dashboard, Configuration, Video Activity Search, Marketplace, Camera Actions & Alarm Handling, Talos, and more.



Configuration module permission settings

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

Step 4 — Entity Access

Set which customers, sites, and devices this role can operate on. Enable Include Children on any parent to auto-include all sub-entities — including future additions.

Entity Access Modes

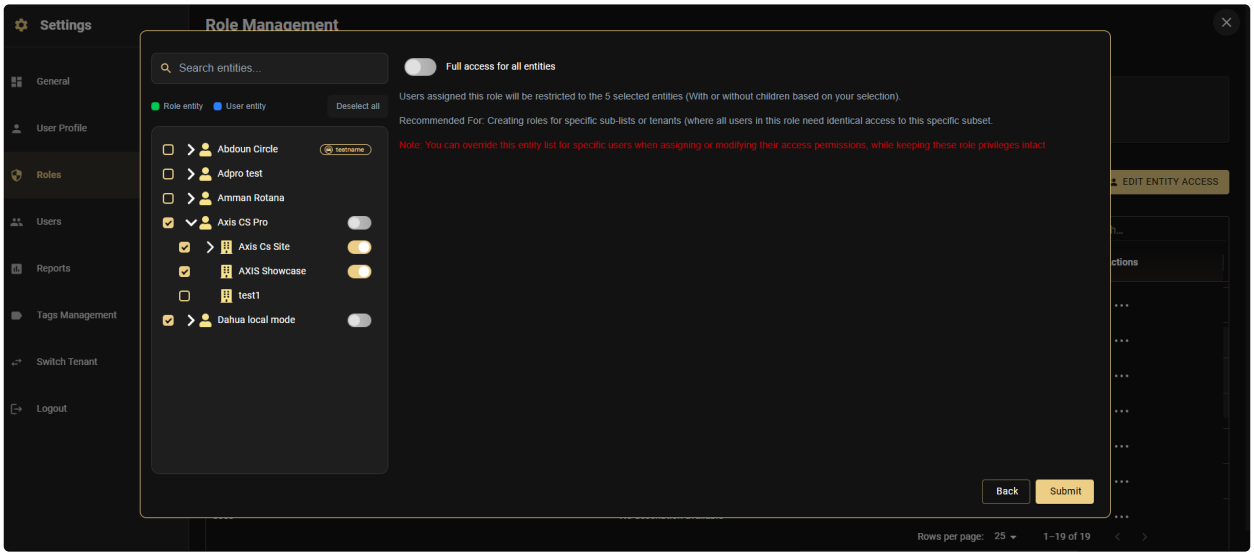
No Entity Access

Users assigned this role get no entities by default. Assign entities per user afterward via Edit Entity Access.

Best for a shared role where each user needs a different set of customers or sites.

Selected Entities

Assign specific customers and sites. Enable Include Children to auto-include any sub-entities added in future.

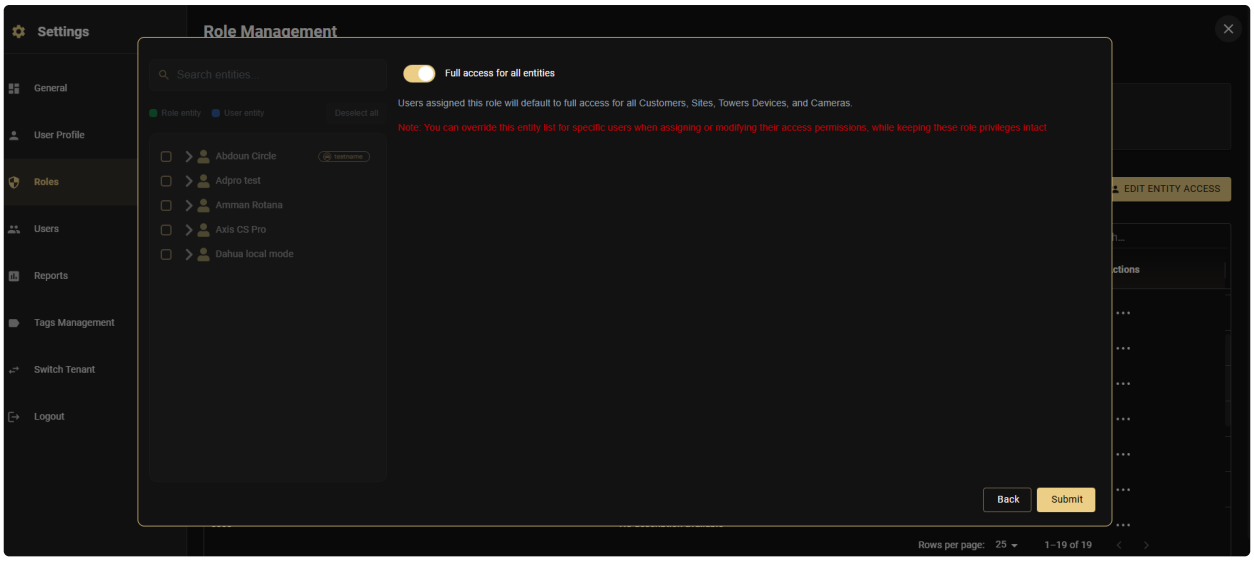


Selected entities with Include Children toggle

Selected Entities mode with Include Children toggle.

Full Access

Role sees every customer and site in the tenant. Use only for internal admin accounts.



Full access for all entities enabled

Full Access mode. Use only for internal admin accounts.

Role Configuration Reference

- Super Admin — All modules. Entity: Full Access.

- Admin — Dashboard, Configuration, User Management, Roles & Permissions, Reports. Cannot access billing.
- Operator — Configuration (view-only), Camera Actions & Alarm Handling, Dashboard, HealthCheck, ZenMode, Video Activity Search, Map, Video Viewer. No Settings, Talos, Marketplace, or Genie access.
- Installer — Configuration (Devices, Sensors, Network Settings), Video Viewer (Live). Cannot manage users or roles.
- End User — Dashboard, basic Configuration view, Reports, Video Viewer (Live), Arm/Disarm for assigned devices. No ability to change settings.

Per-User Entity Access Override

Customize entity access for an individual user without creating a separate role. This is where Override and Merge mode — the two ways to layer a user's own entities on top of their role — come in:

> Important — Override Mode: Acts as a complete replacement. Setting an Override to "Site Beta" entirely revokes access to any previously-held "Site Alpha". Use for strict geographic confinement.

> Note — Merge Mode: Acts additively. Role grants "Site Alpha" + Merge "Site Beta" = both sites accessible. Ideal for temporary cross-coverage when operators aid a different locale.

1. Navigate to Settings → Roles → Edit Entity Access and select the user from the list — or, for a shortcut straight to one user, go to Settings → Users, open their Actions menu, and choose Edit User Entities.
2. Choose Override or Merge mode.
3. Add or remove specific customers, sites, or devices.
4. Save — the change applies immediately.

Post-Migration Role Recovery

User Sees Access Denied on a Module They Had Before

1. Open their role → Module Privileges → verify the capability was not removed during the role edit.
2. Check Audit Log → filter by user and date.

User Cannot See a Recently Added Site

1. Check if their role uses Selected Entities without Include Children.
2. Either enable Include Children on the parent customer, or manually add the new site to the role.

User Has Access to Sites They Should Not

1. Check for active Merge overrides on the user.
2. Navigate to Settings → Roles → Edit Entity Access .
3. Remove the unwanted Merge entries.

Related Resources

- For the conceptual overview of RBAC, roles, and entity access, refer to Understanding Roles & Permissions
- For the full catalog of every individual permission, refer to Privileges