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 Setup

Updated 16 August 2026

Overview

GCXONE uses a Role-Based Access Control (RBAC) system to manage user permissions across the platform. Access is defined through roles, module privileges, and entity assignments.

> Key Concept Privileges determine WHAT a user can do. Entity access determines WHICH customers, sites, and devices they can see. These are two separate things.

Review Default Roles

GCXONE provides predefined roles to simplify initial configuration:

ROLE	ACCESS LEVEL
Super Admin	Full platform access — complete control over all modules; users; roles; and settings
Admin	Administrative access — can manage users; roles; configuration; and reports; but not billing
Operator	Operational access — can view and manage configuration and reports; but cannot delete or administer users/roles
Installer	Field technician access — can manage devices; sensors; and network configuration
User	Read-only access to dashboards; configuration; and reports

These roles can be used directly or customized depending on your operational requirements.

Create or Modify Roles

Navigate to Settings → Roles → Configure New Role

The role creation wizard walks you through 4 steps:

- Role Info — Name, description, and optional default role toggle
- Users — Select which users belong to this role
- Privileges — Enable or disable access per module (Dashboard, Video Viewer, Alarm Manager, Map, and more)
- Entity Assignment — Choose which customers, sites, and devices users of this role can access

Enable Include Children when selecting entities so any new devices or sensors added later are automatically accessible — no manual updates needed.

Invite Users

Navigate to Settings → Users and invite users by email.

During the invitation process:

- A role is assigned to the user
- Module privileges are inherited from the assigned role
- Entity access is applied based on role configuration

After invitation, users receive an email to activate their account.

- For further information, visit the Roles and Permissions page.