

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.

Inviting Users

Updated 16 August 2026

What Inviting Users Does

Onboarding new team members in GCXONE is handled through an automated email workflow. This ensures every user securely verifies their identity and sets their own private credentials before accessing the platform.

Only users with Admin or Super Admin roles can invite new users.

Why It Matters

A secure and structured invitation process ensures no user accesses the platform without verified credentials and an assigned role — preventing unauthorized access and blocked login screens from day one.

How It Works

When you invite a user, GCXONE automatically sends them two emails:

1. Email Confirmation — Verifies the email address is active.
2. Password Setup Link — Allows the user to create their secure password.

Once the user completes both steps, their account becomes active and they are directed to the appropriate section based on their assigned role.

What Happens After Invitation

1. The user receives an email titled *"Changing your password for the NXGEN application."*
2. They click the password reset link in the email.

3. They create a new password for their account.
4. Upon first login, they are directed based on their role — to the Dashboard if enabled, or to the first accessible section such as Configuration.

Key Capabilities

Step 1 — Navigate to Users

Go to Settings → Users and click Invite New User.

Step 2 — Enter User Information

Fill in the required fields:

Personal Information:

- Photo — Optional. Upload a square image, at least 200x200px.
- First Name
- Last Name
- Email Address — Required. Serves as the login ID and must be unique.
- Phone Number — Optional. Used for SMS alerts.
- Phone number fields preserve the country code and phone number values.

Address Information (optional):

- Street Name
- Building Number
- Zip Code
- City
- Country

Step 3 — Configure Account Settings

- **Genesis Role** — Required. Selects the user's role in the underlying Genesis platform.
- **GCXONE Role** — Required. Selects the role that defines what this user can access in GCXONE (e.g., End User, Admin, or Operator). For more details, refer to [Roles & Permissions](#).
- **Customer Group** — Optional. Assigns the user to a customer group.
- **Session Timeout** — Set the session timeout period. Default is 30 minutes. Range is 30 to 1440 minutes (0.5 to 24 hours).
- **Enable Partner Login** — Toggle to allow this user to log in as a partner.
- **Enable Multi-Factor Authentication** — Toggle to require MFA for this user.

Step 4 — Send Invitation

Click **Send Invitation**. The user will receive the two automated emails described above.

Error messages are clearer when required user setup information is missing.

Multi-Organization Access

Users invited to multiple tenants use the same email address.

- **Single Identity** — They only need one password across all organizations.
- **Tenant Selection** — Upon login, they are prompted to choose which organization to access for that session.
- **Switching** — They can switch between tenants anytime via **Settings** → **Switch Tenant**.

Service provider and event provider information is resolved from the selected tenant context.

Real-World Use Cases

- A new operator joins the team — admin invites them, assigns the Operator role, and they're operational within minutes after completing the two-step email flow.

- A service provider manages multiple tenants — the same user is invited to three organizations and uses one password to access all of them, selecting the tenant at login.
- An invitation email expires after 24 hours — admin resends it directly from the Users table without creating a new account.

Best Practices

- Always assign a role before clicking Send Invitation — a user with no role lands on a blocked screen at first login.
- Set the Session Timeout based on the operator's environment — shorter for shared workstations, longer for dedicated monitoring stations.
- Ask users to check their Spam or Junk folder if they don't receive the invitation within a few minutes.
- Ensure users click the Verification Link in the first email before attempting to use the password setup link.

Additional Details

Troubleshooting

Password Setup Link Expired The password setup link expires after 24 hours. If a user misses this window, resend the invitation from the Users table.

Email Not Received Ask the user to check their Spam or Junk folder for mail from @nxgen.cloud.

Login Issues Ensure the user clicked the Verification Link in the first email before attempting to use the password setup link.