

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.

Full Deployment Journey

Updated 23 September 2026

Summary

This guide is an end-to-end, step-by-step guide for bringing a new customer or new site cluster onto GC Surge. Use it as a pre-deployment checklist, a reference for tracking progress during rollout, and a post-deployment validation reference. Covers: About This Guide, Phase 1: Account and User Setup, Phase 2: Site Creation, Phase 3: Site Key Distribution, Phase 4: Field Activation, Phase 5: Operational Setup, Phase 6: Go-Live Confirmation, Ongoing Operations.

About This Guide

This guide is for Super Admins responsible for bringing a new customer or site cluster onto GC Surge. Follow the phases in order — each phase builds on the previous one. Plan for a pause between them: Phase 5 asks you to read the filter rate after 24 to 48 hours of alarm flow, so go-live sign-off in Phase 6 lands a day or two after field activation, not the same afternoon. The guide covers six phases: account and user setup, site creation, Site Key distribution, field activation, operational setup, and go-live confirmation. Use it as a pre-deployment checklist before you start, a progress tracker during rollout, and a validation reference before handing off to the operations team.

Phase 1: Account and User Setup

Step 1 – Create the account

1. Navigate to the GC Surge signup page.

2. Complete all required fields: Email, Phone number (use the flag on the left to select your country code), Company name, Password (minimum 8 characters — the strength indicator shows 5 requirements: 8+ characters, uppercase, lowercase, symbol, and number), and Retype password. Check I have read and agree to the Terms of Use, then click Create account.
3. After you click Create account, GC Surge sends a verification email and a trial welcome email to your inbox and shows a Check your email screen. You must confirm your email before the account setup wizard opens: open the verification email and click Verify Email Address.
4. Once your email is verified, complete the Account Setup Wizard: Welcome (choose your platform language), Your profile (set your display name), and Site & Device (add your first site, or click Skip for now). You then land on the Home dashboard.
5. Because you verify your email during sign-up, the Verify your email item in the Getting Started Checklist on the Home dashboard is already complete when you arrive.

Video — available online at </api/media/file/setup-2.mp4?prefix=media>

Step 2 – Invite all required users

1. Navigate to the Users module and click Invite New User. Enter the user's First Name, Last Name, and Email Address — phone number is optional — then select their role, Operator or Super Admin, from the GC Surge Role dropdown in the invitation modal. Choosing Operator reveals a Shift dropdown beside it, pre-filled with Default (Default) — pick the shift the operator will work before you send the invitation. The field does not appear for Super Admins. Click Send Invitation.
2. Invite all Super Admins first – they need access to complete the remaining steps.
3. Then invite all operators who will handle incoming alarm events during shifts.
4. After each invitation is sent, confirm the user appears in the User List with the correct GC Surge Role.

5. Each invitee receives an email from `fromnoreply@nxgen.io` with the subject “You’ve been invited to GC Surge”. They click Set Password & Verify Email, set a password meeting all five criteria (8+ characters, uppercase, lowercase, number, symbol), and sign in. Invitations expire after 72 hours. Have operators complete this before you start assigning them sites in Alarm Center — their shift is already set from the invitation.

Video — available online at </api/media/file/invite%20operator-20260722-055815.mp4?prefix=media>

Phase 2: Site Creation

Step 3 – Create sites in Configuration

1. In the left sidebar, go to Configuration. If you already added a site during the account setup wizard in Step 1, it is listed here — add the remaining sites the same way.
2. Click Add sites & devices and choose the method that fits your deployment:
 - Guided setup (*Recommended*) — walks you through each step interactively. Best for first-time onboarding or when you want to verify every setting as you go
 - Add sites manually — fills in a single-site form directly. Fast when you already know all camera details and connection type
 - Import from spreadsheet — upload an `.xlsx` file to add multiple sites and devices at once. Best for large deployments. See [Bulk Spreadsheet Import](#) for the spreadsheet format and column definitions
 - Universal device support — for devices that push alarms to GC Surge on their own via REST API, SMTP, or FTP, rather than being polled directly.

3. For each site, complete the required fields. Required fields vary by connection type:
 - Public IP (direct connection): Site name, Device name, Device IP or hostname, Device brand, HTTP/S port, HTTPS (secure) toggle, Username, Password. Contact Info is optional for Public IP sites.
 - Private network, VPN, or GC Edge : all of the above, plus a choice under WHO INSTALLS THE LOCAL AGENT? — pick I am on-site if you will run the Local Agent yourself (no contact details needed), or Delegate installation and fill in Contact person, Contact email, and Contact phone. When you delegate, the Site Key is sent to that contact email (and optionally WhatsApp); leaving those fields empty blocks Site Key delivery. For full field definitions by connection type, see [Setting Up Sites](#).
4. Use consistent site naming conventions. Site names appear in Video Search, Analytics, and subscription filters. Inconsistent names create operational confusion downstream — agree on a naming format before you start.
5. After creating all sites, open the Added sites table and confirm every Private/VPN and Edge site has a Contact email populated. The Site Key is delivered to this address. Public IP sites do not require contact info.

Step 4 – Validate site data before proceeding

1. Confirm the Device brand field is correct for each site. An incorrect brand prevents automatic alarm configuration.
2. For any Private/VPN or Edge site you delegated, confirm the Contact Info fields are populated — empty fields block Site Key delivery. Sites you set up yourself with I am on-site need no contact details, and Public IP sites do not use a Site Key at all.
3. Confirm site names follow your agreed naming convention before you distribute Site Keys. Site names are difficult to change once sites are active and alarms are flowing.

Phase 3: Site Key Distribution

Step 5 – Distribute Site Keys to onsite contacts

This phase applies only to Private/VPN and Edge sites you chose to Delegate installation for. If you selected I am on-site, or you will run the Local Agent yourself over remote access, the key is already shown in the Site key column and there is nobody to send it to — skip to Phase 4. Public IP sites do not use a Site Key at all. Each site has a unique Site Key, beginning with the GCSK- prefix. When you delegate, this key must reach the person who will run the Local Agent at the site before they travel there. For delivery options, security guidance, and troubleshooting, see [Site Key Distribution and Field Activation](#)

1. In Configuration, locate the site in the Added sites table. The key is shown in the Site key column.
2. Open the site Actions menu and select Send site key.
3. Under Send site key (Step 1 of 2) pick how to send it: WhatsApp to the contact phone, or Email to the site owner address; the second step collects the recipient. The modal also shows the key as a QR code the contact can scan in person, and Activate site key activates it in Surge for 30 minutes. Confirm receipt before they travel.
4. Treat Site Keys as temporary passwords. Do not share them via unsecured channels or public messages.

Phase 4: Field Activation

Step 6 – Activate cameras using the Local Agent

This step applies to Mode 2 (Private/VPN) and Mode 3 (Edge) sites. Mode 1 (Public IP) sites do not require this step — devices are configured automatically by GC Surge when the site is created in Configuration.

- Mode 2 (Private/VPN) — the Local Agent runs on a Windows PC on the same network as the cameras, either by you over remote access or by an on-site delegate; a mobile app (iOS / Android) covers on-site activation. See [Setting Up Sites](#) for the local agent option.

- Mode 3 (Edge) — GC Edge is installed on a Windows PC at the site, by you over remote access or by an on-site delegate. GC Edge connects to the device's RTSP stream, automatically scans the network for cameras, and runs NOVA99x filtering locally. After setup, GC Edge must be manually armed before alarms begin flowing — it does not arm automatically.

When you submit a private or edge site, a **Confirm Before Proceeding** dialog warns that one or more sites are not publicly reachable and asks you to confirm you have permission — click **Proceed**. The **Device added** screen that follows already carries everything the next two phases need: the **SITE KEY**, a **SETUP PROGRESS** block, an **Agent connected (v1.2.0)** chip once an agent has checked in, and the **Apply via local agent**, **Manual Configuration** and **Refresh status** buttons. The 30-minute activation window starts on its own here — the chip counts down as *Activated — retry in mm:ss* without anyone pressing **Activate site key**. Someone must be able to reach the camera network. If you already have remote access to a Windows PC on that network you can run the Local Agent yourself — no site visit needed. Otherwise send a delegate, who can use the Local Agent mobile app on site. Either way, the agent discovers all ONVIF-compatible devices on the local network and configures event forwarding to GC Surge automatically.

1. Ensure the PC running the Local Agent is connected to the same local network as the cameras — same Wi-Fi network or switched Ethernet segment. If devices are on a separate VLAN, additional network configuration is required before activation. See [Local Agent — Field Activation](#) for network topology options.
2. Open the Local Agent and enter the Site Key when prompted.
3. The app runs WS-Discovery to find all ONVIF-compatible devices on the subnet. Review the discovered camera list and confirm the count matches what is expected.
4. If devices are missing from the discovered list, confirm ONVIF is enabled on the devices and that UDP multicast is not blocked on the network switch.

5. Confirm activation in the app. Local Agent configures event forwarding for all discovered cameras automatically — no per-device manual steps required. Automatic setup is not guaranteed: if it does not complete, the Device added screen says so (*“Your device was added, but automatic SMTP setup did not complete. Use the manual steps below to finish configuration on the device.”*) and expands Manual SMTP settings with the host, port, credentials and addresses to copy into the device instead.

Step 7 – Confirm activation status in Configuration

1. Return to Configuration and monitor the Site Status. A site’s Site Status reaches Done once all its devices are configured and events begin flowing. (The separate Status column shows the site as Active once it is enabled, regardless of onboarding progress.)
2. Allow up to 10 minutes after the Local Agent confirms success. The cloud status update is not instantaneous.
3. Verify the device count shown in the Added sites table matches the number of cameras activated at the site.
4. If a site remains Pending after 10 minutes, open [Video Search](#) and check whether events are arriving. If events are visible, the activation succeeded and the status display has a lag.

Phase 5: Operational Setup

Step 8 – Verify NOVA99x Is Filtering

NOVA99x is always active on every device from the moment devices are connected — no action is required to enable it. There is nothing to configure or confirm in [My Subscription](#).

After 24 to 48 hours of alarm flow, open [Analytics](#) and check the filter rate . A high filter rate confirms NOVA99x is actively removing noise before alarms reach your operators. On a paid subscription, each device includes 3,000 alarms per month in the base price.

Step 9 – Verify event flow in Video Search

1. Navigate to [Video Search](#).
2. Video Search opens across all sites — the **Total Alarms** counter reflects everything received. Use **Select Site** and, optionally, a device to narrow the results.
3. Confirm events are appearing. If no events appear within 10 minutes of a confirmed camera trigger, follow the “Events are not appearing in Video Search” section in the [Troubleshooting Guide](#), which walks through the site and device filters, site status, activation, and (for SMTP cameras) delivery checks.
4. Open one event and confirm the event detail view loads correctly with image and metadata.
5. Confirm operators can navigate Video Search filters confidently and locate events without assistance. If they struggle, run a short training session on the filter panel before go-live.

Phase 6: Go-Live Confirmation

Step 10 – Final validation checklist

Before marking the deployment complete, confirm each of the following:

- All sites show a Site Status of **Done** in Configuration (no sites left in Pending, Partial Pending, Error, or Partial Error).
- All operator accounts are listed in the [Users & Shifts Management](#) with the correct role, and operators can log in successfully.
- Events are flowing in Video Search for all active sites.
- NOVA99x is active on all sites — confirm the filter rate is visible in [Analytics](#).
- At least one operator has completed a live monitoring session in [ZenMode](#).
- The [Alarm Center - Admin View](#) dashboard shows operator activity during an active shift.
- [Analytics](#) shows data for all active sites.

- The primary Super Admin has reviewed [My Subscription](#) and confirmed all device counts are as expected.

Ongoing Operations

Once go-live is confirmed, hand the platform to the operations team with the following standing instructions:

- Super Admins check [Alarm Center - Admin View](#) at the start of each shift to review active operator status and overnight performance.
- Operators use [ZenMode](#) during active monitoring shifts and Video Search for investigations and evidence review.
- [My Subscription](#) is reviewed monthly to monitor usage and identify any unexpected overage exposure.
- Configuration is audited monthly — remove any sites or devices that are no longer active to keep counts accurate.