

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.

Adding Devices - Universal Device Support

Updated 9 October 2026

experience — not included in the PDF

This page covers adding individual devices through the Universal device support option in Configuration.

It walks through how to choose an alarm method, copy the generated credentials into the device, and validate the setup. Covers: How to Add a Device, Automatic Configuration for Supported Brands, Connection Status After Adding, Manual Fallback, Device Naming Standards.

Use the Universal device support option when you need to connect a device that will push alarms to GC Surge on its own — using REST API, Email (SMTP), or FTP. Select it from the Add sites & devices menu. If you reach this setup through Guided setup, the same option appears as “My device can send alarms (API, FTP or SMTP)” — both entry points lead to the same flow.

For an overview of all four ways to add a device, see [Add a device](#). For adding a new site using Guided setup, manual setup, or spreadsheet import, see [Setting Up Sites](#). This page covers the Universal device support method only.

How to Add a Device

The Add a device modal is a plug-and-play wizard with three guided steps:

1. In Configuration, click Add sites & devices and select Universal device support.

2. Step 1 — How should alarms be sent to GC Surge? Enter a Device name (see Device Naming Standards below), select an existing site or type a new name in the Site name field (optional) (GC Surge creates it automatically if it does not exist yet), then pick the method your device supports : REST API, Email (SMTP), or FTP, then click Add Device .
3. Step 2 — Connection details. GC Surge generates the connection credentials for the method you chose — copy them into your device's alarm-forwarding settings (details per method below). Once you have entered them on the device, click Mark as configured manually; if not, click Skip for now.
4. Step 3 — Forward Alarms (Optional). Optionally add a forward rule with + ADD FORWARD ALARM , or skip it.
5. Click Done. A Device added confirmation screen appears — the device is registered and ready. Click Go To Alarm Center to verify your first alarm, or close the screen to stay in Configuration.

Step 1 — Choose the Alarm Method

In the Add a device modal you choose the alarm-delivery method your device or system supports. The three methods are:

- REST API — the device sends alarms via HTTP POST with structured JSON metadata and inline snapshots, giving sub-second latency. It's the best transport when the device supports it; if the device can't do HTTP POST out of the box, fall back to Email (SMTP), which works everywhere but with higher latency.
- Email (SMTP) — the device emails an alarm (with snapshot attached) to a dedicated GC Surge inbox, which parses the subject, body and attachment into an alarm event. Since almost every IP camera can email motion alerts, it's the universal fallback. End-to-end latency is typically 2–10 seconds.

- FTP — the device uploads an image to an FTP server GC Surge provides, common on older or budget DVRs. FTP carries only the image file and filename — no structured metadata — so GC Surge infers the timestamp from the filename and treats each upload as an alarm. It's the lowest-fidelity transport; use it as a last resort and switch to REST or SMTP when you replace the device.

Video — available online at </api/media/file/Dahua%20SMTP-1.mp4?prefix=media>

Step 2 — Copy the Connection Details

GC Surge generates all connection credentials automatically. Use the copy buttons next to each field — you do not create these credentials.

- REST API: Device ID, Events URL, API token.
- Email (SMTP): Device ID, SMTP host, SMTP port, Username, Password, Encryption type, To email, From email.
- FTP: Device ID, FTP host, FTP port, Username, Password.

Paste these values exactly into the corresponding fields in your device's alarm forwarding configuration.

One character error in any credential field will prevent alarms from reaching GC Surge.

The credentials shown are unique per device and can be regenerated if they leak. For REST API, GC Surge generates a callback (Events) URL to paste into the device's HTTP notification settings; for Email (SMTP) the port is usually 587; for FTP, enter the displayed host, port, username and password into the device's upload settings.

For Email (SMTP), the SMTP host (`smtp.zeptomail.eu`) is shared across devices. Each device receives a unique To address (the `@zeptomail.eu` address the device sends alarms to) and a unique From address (an `@nxgen.io` address) — both are generated automatically. The To address is how GC Surge identifies which device an alarm came from. The `alerts@nxgen.io` address visible in the Forward Alarms section is the optional post-processing forwarding destination, not the device From address.

Step 3 — Forward Alarms (Optional)

Optionally configure where verified real alarms should be forwarded after processing — for example, to an external Central Monitoring Station (CMS) via SIA-DC09 or webhook. Click Done when finished. This step is optional; the device is already registered and receiving alarms before you configure forwarding.

Forwarding doesn't change ingest — only what happens after NOVA99x classification: every alarm marked real (or confirmed by an operator) is forwarded over your chosen protocol. Options are SIA-DC09 for traditional alarm receivers and Webhook for arbitrary integrations; the dropdown offers only these two methods, and the CMS Forwarding guide covers each. Most monitoring stations run their whole workflow inside [ZenMode](#) and don't forward at all; if you do, set it up once per device and the same rule applies to every alarm from that device. See [CMS Forwarding](#) for the full setup guide.

Prefer GC Surge to configure the device for you? If you onboard supported brands (Hikvision, Dahua, AXIS, NX Witness ; for Hanwha and SpykeBox select NX Witness) through Add sites manually , GC Surge connects to the camera and pushes the alarm-forwarding settings automatically — no manual copying required. In the Universal device support flow above, you copy the credentials from Step 2 into the device yourself.

Automatic Configuration for Supported Brands

For Hikvision, Dahua, AXIS, and NX Witness devices on public IP connections added through Add sites manually , GC Surge pushes alarm forwarding credentials directly to the camera — no manual copying required. The platform handles everything after you submit the site. (Hanwha and SpykeBox run on the NX Witness platform — select NX Witness as the brand.)

On a supported camera, GC Surge enables two things automatically: the SMTP/email server settings *and* the event-notification trigger that makes the camera send an email on each alarm. Both are applied with no manual step.

For Private/VPN and Edge connections, configuration is delivered through an on-site agent. See [Setting Up Sites](#) for connection type details and [Local Agent - Field Activation](#) for the on-site activation procedure.

Connection Status After Adding

Configuration shows the current state for every device:

- **Configured** — the device is fully configured and sending alarm events to GC Surge. No action required.
- **Pending** — the device has been added but the cloud has not yet finished pushing configuration or received a confirmation alarm. Resolves automatically; wait a few minutes before taking any action.
- **Error** — GC Surge created the configuration but could not push it to the device, usually because the device was offline during setup or the credentials were wrong. Click **Retry** from the device Actions (...) menu — a Retry integration config confirmation dialog opens. Click **Retry** to push the saved connection details to the device again. You do not need to remove and re-add the device.

Partial Pending and **Partial Error** appear only at the site level — when some, but not all, of a site's devices have finished configuring. A single device shows one of the three states above — or **Manually configured** if you set it up by hand (see [Manual Fallback](#) below).

Manual Fallback

If automated configuration doesn't succeed — for example a device stays in **Error** after a couple of **Retry** attempts, or the device's brand or firmware doesn't accept the automatic push — you can configure it by hand instead:

1. Open the connection details from Step 2 (SMTP/FTP host, port, username, password).
2. Log in to the camera's own web interface and enter those values into its alarm-forwarding (email/FTP) settings manually.

3. Back in GC Surge, confirm you've done it — the device is then marked **Manually configured** instead of staying in **Error**.

A **Manually configured** device sends alarms exactly like an auto-configured one; the only difference is that you entered the settings on the camera yourself. (This is the same manual step used for unsupported brands — here it is just a fallback when the automatic push fails.)

Device Naming Standards

Device names appear in [Video Search](#) event cards, Analytics breakdowns, subscription camera rows, and Configuration device lists. Descriptive names make large deployments manageable; generic names create persistent operational problems at scale.

- Use names that describe physical location: `Front-Gate-Cam-1`, `Parking-Level-B2-Exit-`, `Server-Room-Entrance`.
- Use a consistent format across all devices: `[Location]-[Zone]-[Number]`.
- Avoid generic names like *Camera 1*, *Camera 2*, or *Device A* — these become indistinguishable in views showing 200+ devices.
- Do not duplicate a device name that already exists on a different site — naming conflicts cause confusion in search and billing views.

Post-Registration Validation

After adding a device, confirm the following before marking it as operational:

1. **Configuration check** — confirm the device appears under the correct site and the device count has incremented.
2. **Video Search check** — confirm events from the new device appear in [Video Search](#). This verifies the full alarm pipeline is working. Allow a few minutes after activation for the first events to arrive.

3. Home dashboard check — confirm alarm KPI metrics reflect activity from the new site and device.

This confirms the device is contributing to operational dashboards.

Best Practices

- Check Configuration after adding devices — do not assume all devices configured successfully until you see the status.
- If a device shows Error , correct the credentials and click Retry before contacting support. Most failures are caused by wrong credentials or a temporarily offline device.
- Name devices before deployment begins — names are harder to change consistently after devices are live and appearing in dashboards.