

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.

CMS Forwarding

Updated 8 October 2026

experience — not included in the PDF

Summary

CMS forwarding sends verified alarms from GC Surge to an external Central Monitoring Station (CMS). Configure it per site directly from the Configuration page — no account-team involvement required. Each site can have one or more forwarding destinations. Covers: How to Configure, Supported Protocols, Payload Variables, When Forwarding Triggers, Forwarding Failures.

Image unavailable — alarm-forwarding-to-cms.mp4

How to Configure

CMS forwarding is configured per site from the Configuration page (Sites & devices).

1. Open Configuration from the left sidebar.
2. In the Added sites table, click the three-dot button (...) on the site row you want to configure.
3. Select Forward alarms from the dropdown menu.
4. The Forward Alarms dialog opens. Click + ADD FORWARD ALARM .
5. A dropdown appears with the available forwarding methods — select Webhook or SIA-DC09 .
6. Fill in the configuration fields for the selected method (see below).
7. Click Save to apply. A site can have more than one forwarding destination — repeat from step 4 to add additional endpoints.

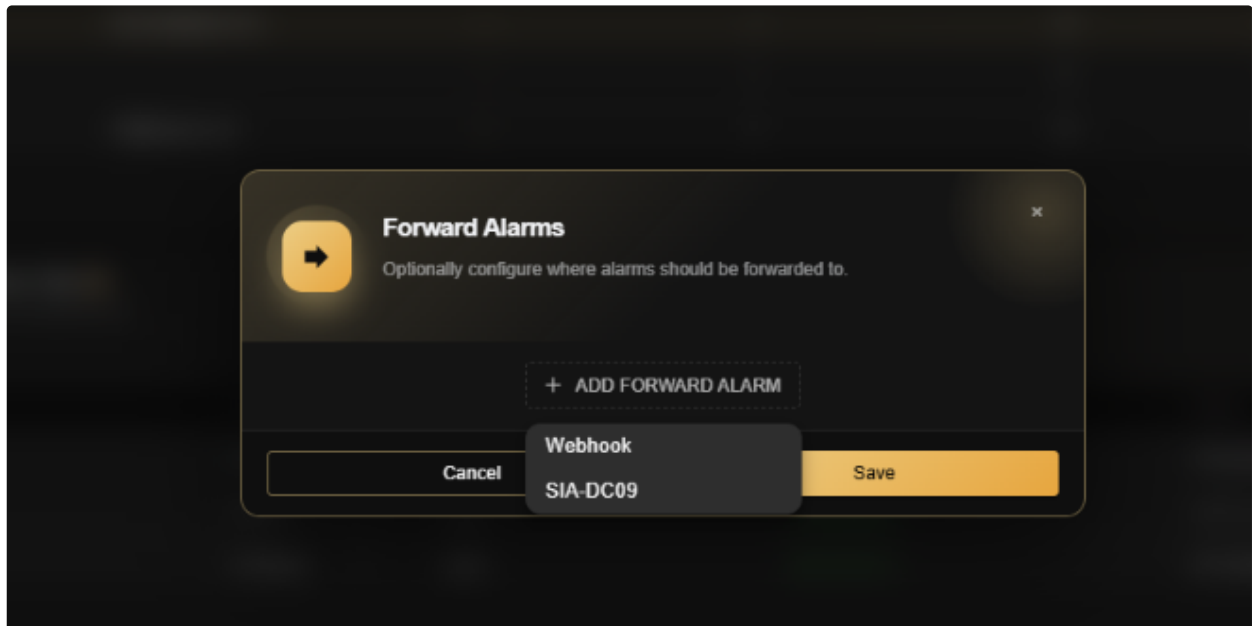


image-20260722-070451.png

Supported Protocols

Webhook

Posts an alarm payload to a CMS HTTP endpoint. Configuration fields:

- **Method** — HTTP method for the request (default: POST).
- **URL** — the endpoint URL of the CMS receiver.
- **Headers** — optional Key / Value pairs (e.g., for authentication tokens). Click + ADD to add a header row.
- **Payload** — Key / Value pairs sent in the request body. Pre-populated with the standard alarm variables.

Click + ADD to add custom fields, or remove any you do not need.

Forward Alarms
×

Optionally configure where alarms should be forwarded to.

Webhook
✖

Method

POST

URL

Headers
+ ADD

Key	Value

Payload
+ ADD

Key	Value
☒ alarmCode	\${ALARMCODE}
☒ alarmMsg	\${ALARMMESSAGE}
☒ alarmUrl	\${ALARMURL}
☒ alarmValue	\${ALARMVALUE}
☒ payload	\${PAYLOAD}
☒ header	\${HEADER}
☒ files	\${FILES}

Authentication

No Auth

☐ Forward Only True Alarms

+ ADD FORWARD ALARM

Cancel

Save

image-20260722-070509.png

SIA-DC09

The standard signalling protocol used by alarm receiving centres. It transmits structured alarm signals (zone, account, event code) over IP to a CMS receiver. Most professional monitoring centres support DC09 natively. Configure the IP address, port, account number, and encryption key supplied by your CMS provider.

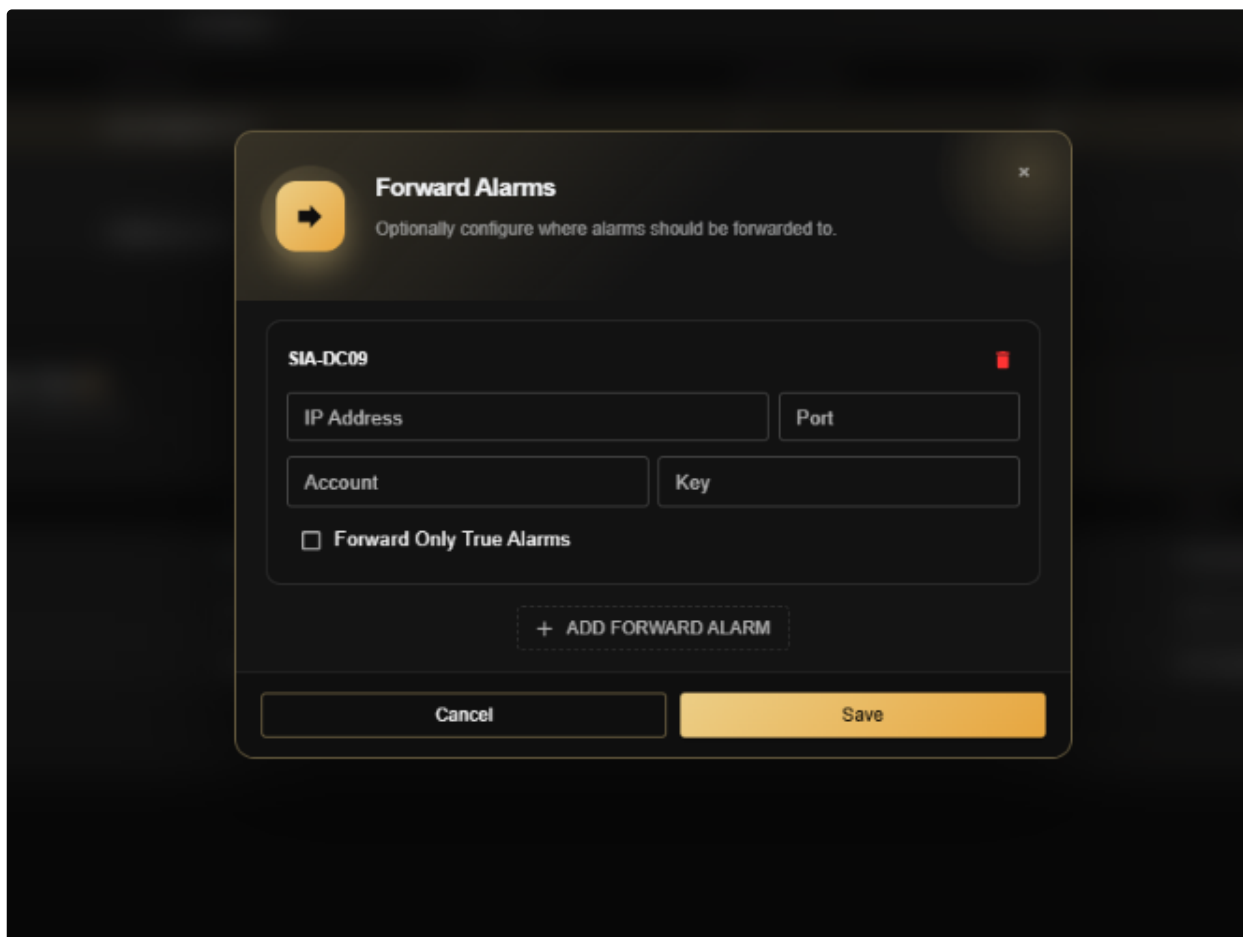


image-20260722-070546.png

Payload Variables

The following dynamic variables are available in the Webhook payload. GC Surge replaces them with the actual alarm values at the time of forwarding:

VARIABLE	VALUE INJECTED
<code>\${ALARMCODE}</code>	Alarm type code
<code>\${ALARMMESSAGE}</code>	Alarm description message
<code>\${ALARMURL}</code>	Direct ZenMode link to the alarm event — include this so the CMS operator can open the alarm video immediately
<code>\${ALARMVALUE}</code>	Alarm severity or value

Always include `${ALARMURL}` in your payload — it carries the ZenMode link so the receiving CMS operator can open the alarm clip directly without searching for it.

When Forwarding Triggers

Forwarding is designed for events that have passed classification and any additional confirmation criteria.

The goal is to send confirmed, relevant events to the CMS — not mirror every event GC Surge received.

Only verified real alarms are eligible for forwarding. Event metadata is included with every handoff — alarm type, timestamp, camera ID, and site — so the CMS can act immediately.

Forwarding Failures

Forwarding failures are logged and visible in the audit trail. A CMS handoff issue is distinct from a classification issue — both are recorded separately so the correct layer can be diagnosed quickly.