

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.

Site Key Distribution and Field Activation

Updated 8 October 2026

experience — not included in the PDF

Summary

This page covers field activation for Mode 2 (Private/VPN) and Mode 3 (Edge) sites, where an on-site agent uses the Site Key to activate cameras. Mode 1 (Public IP) cameras are configured directly by the cloud with no on-site agent, so they do not need the Site Key for activation — although a key is still generated for every site. Covers: What Site Key Distribution Does, Format and Security, Delivery Channels, How to Send a Site Key, Field Activation Overview, Large Deployment Guidance, If a Site Key Reaches the Wrong Contact, Troubleshooting.

What Site Key Distribution Does

A Site Key is the secure credential that connects a physical site's cameras to the GC Surge cloud. When a site is created in Configuration, a Site Key is generated automatically. Distributing that key to the onsite contact is the step that triggers field activation — without it, cameras cannot be configured and the site cannot go live.

The onsite contact completes activation with the Local Agent (Windows). For download and installation steps, see [Setting Up Sites](#).

This process bridges cloud-side administration and physical camera setup. Getting it right determines whether a site goes live on schedule.

How it connects to the cloud

During activation, the Site Key binds the local discovery session to the site record already created in GC Surge. That is what allows cameras discovered in the field to land in the correct tenant and the correct site without manual remapping after the fact.

Format and Security

The `GCSK-` prefix identifies the string as a Site Key. The Key is unique per site and serves as the authentication token for that site's activation.

- Treat the Site Key as a one-site activation secret.
- Share it only with the technician or partner responsible for activation.
- If it was sent to the wrong person, update the contact in the Added sites table and resend it to the correct contact.
- Once a site is active, the Site Key can be rotated freely — it only matters during the one-time activation handshake, so rotating it afterwards has no operational impact.

Delivery Channels

- WhatsApp deep link (recommended) — The Site Key is sent as a WhatsApp message. The onsite contact copies it into the Local Agent on their PC. Fast delivery with a timestamped record.
- Email — The Site Key is sent as plain text. The onsite contact must copy it manually into the Local Agent. This works but is more error-prone — one character error in the key prevents activation.
- QR code — The site key modal displays a QR code. When scanned, the QR code displays the Site Key for the onsite contact to enter into the Local Agent on their PC. Useful for in-person handoffs.

How to Send a Site Key

1. Open [Configuration](#) from the sidebar.
2. Locate the target site in the Added Sites table.

3. Click the ... Actions menu for that site and select Send site key . Alternatively, select the site to open the detail panel and click the Send site key button at the top right of the panel.
4. The Surge Onboarding – Mobile App – site key modal opens, displaying the Site Key in full and a QR code. The contact email and phone number are shown for confirmation.
5. Choose your delivery method: click Resend WhatsApp or Resend email . If the onsite contact is present, they can scan the QR code directly from the screen.
6. Confirm the onsite contact has received the key before proceeding to field activation.

Field Activation (Overview)

Once the onsite contact has the Site Key, they activate the cameras on-site: on the same local network as the cameras, they open the activation tool, enter the Site Key, let it discover the ONVIF cameras, and confirm — the cameras then show as configured . The Local Agent must remain running on the PC — it handles ongoing alarm forwarding for private sites.

For the full activation procedure — prerequisites, network requirements, ONVIF setup per camera brand, what gets configured on each camera, and pipeline verification — see [Local Agent - Field Activation](#) .

Large Deployment Guidance

- Log every dispatch — record site name, Site Key sent date, delivery method, recipient name, and confirmation date.
- Confirm receipt before moving to the next site — a key that was sent but not received delays activation by days.
- Set an activation deadline — sites that have received their key but not activated within 48 hours need a follow-up.
- Pre-test the delivery method — test WhatsApp, email, and QR internally before using them with external onsite contacts.

- Assign one dispatch owner — divided ownership leads to duplicated sends, missed confirmations, and delays.

If a Site Key Reaches the Wrong Contact

If a Site Key was sent to the wrong person, re-send it to the correct contact directly from the Send site key modal — you do not need to edit the site first:

1. In Configuration, open the site and click Send site key (from the Actions (...) menu, or the Send site key button in the detail panel).
2. In the Surge Onboarding modal, enter the correct Phone and/or Email in the optional fields.
3. Click Resend WhatsApp or Resend email to send the key to the corrected contact.

A Site Key has no effect on cameras that are already active — it is only used during the one-time activation handshake, so once a site is active the key plays no further operational role.

Troubleshooting

- Key not received via WhatsApp — confirm the recipient's WhatsApp number includes the correct country code and that the message was delivered. If undelivered, resend via email.
- WhatsApp message not opening correctly — resend via email. The onsite contact needs only the Site Key text.
- Key rejected by the Local Agent — typo during manual entry. Re-copy the key carefully from the WhatsApp message or email.
- Cameras not reaching configured status — cameras are not on the same network as the Local Agent device, or WS-Discovery is blocked. Confirm network connectivity and check for VLAN isolation between cameras and the Local Agent device.



- Camera not discovered during activation — ONVIF not enabled, camera on a different subnet, or unsupported model. Enable ONVIF on the camera via its web interface and verify subnet matching.
- Key sent to the wrong contact — open Send site key , enter the correct phone or email in the modal's optional fields, and click Resend . See “If a Site Key Reaches the Wrong Contact” above.