

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.

Local Agent - Field Activation

Updated 23 September 2026

Summary

The Local Agent is a desktop application (Windows) that runs on a PC connected to the same local network as your cameras. It discovers all ONVIF-compatible cameras and automatically configures event forwarding to GC Surge — no per-camera manual setup required. The Local Agent must remain running on that PC after activation; it handles ongoing alarm forwarding for private network sites.

Covers: What the Local Agent Does, Platform Support, Delegate Installation Flow, Before You Start, How You Receive the Site Key, Network Requirements, Activation Steps, If Cameras Are Not Discovered, What the App Configures, After Activation, Error Messages, Edge Deployments.

What the Local Agent Does

- Connects to the same local network as your cameras.
- Discovers all ONVIF-compatible cameras using the WS-Discovery protocol.
- Pushes SMTP event forwarding settings to each discovered camera automatically, using credentials tied to your Site Key.
- Must remain running on the PC after setup — it handles ongoing alarm forwarding for private network sites.

Platform Support

PLATFORM	SUPPORTED
Windows	Yes
macOS	Not supported
Mobile app (iOS / Android)	Yes — for on-site field activation only

Supported camera brands for automatic configuration: Hikvision, Dahua, AXIS, and NX Witness. Hanwha and SpykeBox cameras run on the NX Witness platform — select NX Witness when prompted.

Delegate Installation Flow

When a Super Admin creates a new site in [Configuration](#) and selects Delegate installation :

1. The Super Admin enters the onsite contact's name, email, and phone number.
2. GC Surge sends the Site Key and installation steps to the contact.
3. The onsite contact installs the Local Agent on a Windows PC at the site.
4. The contact opens the Local Agent and enters the Site Key.
5. The agent discovers cameras on the local network and configures event forwarding automatically.

To handle installation yourself without delegating, select I'm at the site instead. See [Setting Up Sites](#) for the full site creation workflow.

Before You Start

Before running the Local Agent, confirm the following:

- A Windows PC is available on the same local network as the cameras.
- All cameras are powered on and connected to the network.
- You have received the Site Key (GCSK-...) from your Super Admin.
- ONVIF is enabled on each camera — if you are unsure, see *If Cameras Are Not Discovered* below.

Mobile App (on-site activation)

Use the Local Agent mobile app when you do not have remote network access to the site and need to send someone there in person. When cameras are added for a site with no local agent, the system generates a site key and QR code.

The on-site person:

1. Installs the Local Agent mobile app on their device.
2. Scans the QR code or enters the site key manually to link the app to the site.
3. Connects their device to the same local network as the cameras.
4. The app automatically finds all cameras for the site and configures each reachable one.
5. The portal status updates to Configured once complete.

The mobile app has no login — access is controlled through the site key only. Share the QR code with trusted personnel only. Each site key is tied to a single site; a separate key is needed per site.

How You Receive the Site Key

Your Super Admin sends the Site Key from [Site Key Distribution and Field Activation](#). It is delivered in one of three ways:

WhatsApp — the Site Key is sent as a WhatsApp message. Copy the key from the message and enter it in the Local Agent on your PC.

Email — the email contains the full Site Key (GCSK-...) along with download links for the Windows installer. Enter the key in the Local Agent after installation.

QR code — if your Super Admin is on-site with you, they can display the QR code from Configuration. Scan it with your phone to read the Site Key, then enter it manually in the Local Agent on your PC.

How WS-Discovery Works

WS-Discovery (Web Services Dynamic Discovery) is the standard ONVIF protocol for discovering devices on a local network. When the Local Agent initiates discovery, it sends a UDP multicast broadcast to the local subnet (address 239.255.255.250). ONVIF-compatible cameras that receive the broadcast respond

with their service endpoint address. The application collects all responses and configures each discovered camera automatically.

For discovery to work, the following conditions must be met:

- The PC running the Local Agent and the cameras must be on the same network segment (same subnet or VLAN).
- UDP multicast must not be blocked by the network switch or router.
- ONVIF must be enabled on each camera. This is enabled by default on most modern cameras.

Network Requirements

The Local Agent discovers cameras using multicast broadcasts, which means the PC and cameras must be able to communicate on the same network segment. Different network setups require different preparation:

Flat network (recommended): All cameras and the PC are on the same Wi-Fi or Ethernet network.

Discovery works automatically with no additional configuration.

VLAN-segmented network: If cameras are on a separate VLAN from the PC, WS-Discovery will not reach them. Options: temporarily connect the PC to the camera VLAN during activation, have your IT team configure multicast routing between VLANs, or enter camera IP addresses manually.

Multiple subnets at one location: Each subnet must be activated separately. Connect the PC to each subnet in turn and run discovery for each.

Activation Steps

1. Download and install the Local Agent from the link in your setup email, or from Configuration — select Windows Installer .
2. Open the Local Agent on your PC.

3. Enter the Site Key sent by your Super Admin.
4. The agent connects to GC Surge, discovers cameras on the local network, and configures event forwarding on each one automatically — no per-camera steps required.
5. Wait for the success confirmation before leaving the site. Do not close the Local Agent — it must remain running on this PC.

If cameras are missing from the discovered list, see *If Cameras Are Not Discovered* below before completing activation.

If Cameras Are Not Discovered

If cameras do not appear in the discovery results, ONVIF may be disabled on the camera. Enable it through the camera's web interface:

Hikvision

1. Log in to the camera web interface.
2. Go to Configuration → Network → Advanced Settings → Integration Protocol.
3. Enable ONVIF.

Dahua

1. Log in to the camera web interface.
2. Go to Setting → System → Account and confirm an ONVIF user is configured.
3. Then go to Setting → Network → Advanced Settings and enable ONVIF.

AXIS

ONVIF is enabled by default. No action is usually required.

If a camera still does not appear after enabling ONVIF, confirm that the camera and the PC running the Local Agent are on the same network segment.

What the Local Agent Configures on Each Camera

For each discovered camera, the Local Agent automatically pushes SMTP event forwarding settings. You do not need to enter these manually — the agent retrieves the correct credentials from GC Surge using your Site Key and injects them directly into each camera. The following is configured on each camera:

- SMTP server: `smtp.zeptomail.eu`
- SMTP port: `587`
- Encryption: `TLS`
- Authentication credentials: unique to this site, retrieved from the cloud using the Site Key
- Sender address: `alerts@nxgen.io`
- Receiver: the GC Surge ingest address specific to this site, assigned automatically
- Image attachments: enabled — each alarm event includes a camera snapshot
- Send interval: minimum 5 seconds between alarm emails

After Activation: Verifying the Pipeline

After the Local Agent completes configuration, allow up to 10 minutes for the cloud to finish processing. In Configuration, open the site and check each camera's Configuration status — it should move from pending to Created (not Error). The site's own Status shows Active as soon as it is added, so that is not a sign that configuration finished.

Then verify that alarms are reaching the platform:

1. Generate a test event at the site — trigger motion detection or walk through the camera's field of view.
2. Wait 30–60 seconds.

3. In GC Surge, go to [Video Search](#).
4. Select the newly activated site.
5. Confirm the test event appears as an event card.

If no events appear after 5 minutes:

- Check that the camera has outbound internet access to smtp.zeptomail.eu on port 587.
- Verify that motion or detection triggers are enabled on the camera.
- Check the camera's clock — incorrect timestamps can cause events to be processed out of order.
- Log into the camera's web interface and use the built-in Test button in the email or SMTP settings to send a test email directly.

Error Messages

The Local Agent displays an error message for every failure. If anything goes wrong at any step — connecting with the Site Key, discovering cameras, or pushing configuration — the application shows the specific error on screen. Share a screenshot of the error with your Super Admin or the NXGen support team for faster resolution.

Edge Deployments — Not Applicable

The Local Agent is used exclusively for Private/VPN field activation. It is not involved in Edge deployments.

Edge sites use GC Edge — a Windows PC application that connects to cameras via RTSP, runs NOVA99x classification on the PC, and forwards classified events to GC Surge. The Local Agent does not run, stream, or classify for Edge sites. For Edge setup instructions, see [Setting Up Sites](#).