VANTAG / RETAIL NAZAR

1. Start here: choose the correct package

Audience and release status

This manual covers the Windows Offline Site Console development candidate (agent 1.11.5 workflow), not the standard online Edge Agent. Public offline installation remains UNDER VALIDATION. Clean-PC disconnected qualification, commercial model redistribution approval and representative fall/theft accuracy testing are still outstanding. Do not promise production readiness or distribute model assets until approved.

Download on an internet-connected PC

1. Sign in to your regional Vantag / Retail Nazar website. Open Install Edge Agent / Downloads.
2. Find the separate Offline Site Console section. If it says Under validation, there is no approved public offline installer to download. Ask the administrator for an authorised controlled-testing package; do not substitute the online Windows ZIP.
3. Obtain the complete package, its stated version and checksum if supplied, this manual and the authorised licence procedure before going to site. A device-bound licence may need a second file-transfer round trip after first launch.

What the package contains

The offline build includes VantagAgent.exe, a private bundled Python runtime, application/native libraries, local browser-console assets, packaged AI model files and public licence-verification keys. Keep the _internal folder with the executable. No separate Python, pip, Ollama or Jupyter installation is required for this workflow. GPU drivers are not installed or replaced automatically. The online and offline packages are not interchangeable.

Before travelling

Use a compatible Windows 10/11 64-bit PC and test that exact package on that PC first. Confirm free disk space for extraction, evidence and backups; there is no validated universal RAM/GPU/camera-capacity specification. Have the NVR LAN IP, RTSP port, channel map and an authorised device account with remote live-view/RTSP rights. Carry a USB drive for licence transfer. Keep the PC awake and powered. Ethernet is preferable to unreliable exhibition Wi-Fi.

Three different logins

Website account: internet downloads, billing and administration. Local owner: access to this PC's Offline Site Console. NVR/camera account: permission to decode video. These passwords are independent. Never give the demo team the superadmin password.

2. Extract, launch and create the local owner

Install the controlled package

1. Copy the complete authorised ZIP to the camera PC, using USB if necessary.
2. Right-click the ZIP and choose Extract All. Choose a stable folder your Windows user can access. Wait for extraction to finish.
3. Open the extracted folder and run START-OFFLINE.cmd (or VantagAgent.exe with the supplied offline config.json). Do not run from inside the ZIP or separate the EXE from _internal.
4. Check that the agent status window appears. Avoid repeated launches: a second instance is not a remedy for slow startup. Only run packages from a trusted source; do not disable Windows security globally to force an unknown file to run.

Open the console on the same PC

The agent opens a local browser address beginning http://127.0.0.1: followed by a port. Use the current address opened or shown by the agent: the port can change. It is not retail-vantag.com or retailnazar.com. This loopback console cannot be opened from another laptop or phone. If the browser was closed, reopen the console using the running agent rather than an old bookmark.

First run versus existing site

At Set up this PC, enter a local username and a password of at least 12 characters, then choose Create local owner. Save them securely. At Welcome back, an owner already exists: use that local account, not the website login or camera credentials. There is no default password in this manual. If forgotten, request a supported recovery procedure; do not delete site data to reset it.

Set site name and time

Open Overview. In Site settings, enter a recognisable Site name and an IANA Timezone, then Save site. Examples: Asia/Kolkata (India), Asia/Jakarta (western Indonesia), Asia/Makassar (central Indonesia), Asia/Jayapura (eastern Indonesia), Asia/Singapore, Asia/Kuala_Lumpur or Asia/Manila. Choose the actual site timezone. Check the Windows date/time too; changing the clock backwards may invalidate offline licensing.

Preserve an existing installation

Do not copy a working installation with its owner, licence, camera passwords or evidence to customers. Before an upgrade, download a private backup and use the approved update procedure. Keep the same Windows user/profile: local data and protected credentials belong to it. Re-extracting application files does not intentionally erase site data, and should never be used as a factory-reset method.

3. Activate this PC: request out, licence back

Step A - demo PC, no internet needed

Open Licence & health and choose Export device renewal request. Save vantag-renewal-request.json to the USB drive. The Device ID identifies this local installation/PC; it is not the NVR IP, channel number or customer email. Do not invent it or type the NVR address into the website's Device ID field.

Step B - connected PC, superadmin only

1. The administrator signs in to the website and opens Admin > Offline demos.
2. Choose Import device renewal request (JSON) and select the request exported by the target PC. This fills the Device ID and may fill the tenant.
3. Choose account and confirm Account / tenant ID. A first-time request can have no tenant; the administrator must select the correct account.
4. Choose Usage policy. Customer / dealer evaluation needs Evaluation days (1-365). Internal team demo has no expiry and is for authorised team PCs only.
5. Set Concurrent camera entitlement to the approved number. It is a licence ceiling, not a hardware performance promise.
6. Click Issue and download device licence. The downloaded signed response is normally vantag-demo-entitlement.json. Copy it back to the USB drive.

Step C - return to the same demo PC

In Licence & health, use Import signed entitlement JSON and select the SIGNED RESPONSE, not the original request. Wait for the import confirmation and check licence status. Only the correct device-bound, correctly signed and current entitlement is accepted. Keep the request and signed response in clearly named folders so the team does not mix them up.

Validity and renewal

A customer entitlement follows authorised paid/trial/extension validity, then seven days of grace. After grace, live viewing and new AI stop; saved records, exports and renewal stay accessible. Export a new request, obtain an authorised newer signed renewal and import it. A payment or extension made online does not reach a disconnected PC until the new file is imported. Internal demo licences do not change customer invoices or subscription dates and cannot be used on unlimited PCs.

What the yellow warning means

The development/release-validation warning is separate from licence status. A valid licence permits the configured local use; it does not establish model accuracy, legal redistribution rights or clean-PC qualification. Do not remove the warning by changing the clock or reimporting files. Fully offline installations cannot receive immediate remote revocation.

4. Add cameras and get a real decoded frame

Fill Cameras, one stream at a time

Camera name: a unique location, such as Pantry - NVR channel 1. NVR / camera LAN IP: the recorder IP when connecting through an NVR, without rtsp://, port or path. RTSP port: normally 554 unless configured otherwise. NVR username / Actual NVR password: the recorder account allowed to view that channel; not the website account. Use Show to check a typed password privately.

Password containing

In the separate Actual NVR password field, type the ORIGINAL password with # unchanged. The wizard URL-encodes credentials once. Do not type %23 there unless those three characters are literally part of the real password. In a full RTSP URL assembled outside the wizard, encode # as %23 inside the password only. Do not change the password stored on the NVR to its encoded URL spelling. Never send a credential-bearing URL in a public screenshot.

Choose a documented path

Stream setup chooses a manufacturer template, not automatic identification. Choose the actual NVR channel and the desired main/substream. Start with an H.264 substream if the device supports it. Hikvision common examples: channel 1 main /Streaming/Channels/101, sub /Streaming/Channels/102; channel 2 main /Streaming/Channels/201, sub /Streaming/Channels/202; channel 4 sub /Streaming/Channels/402. The last two digits select the stream, not the next camera. Dahua commonly uses /cam/realmonitor?channel=1&subtype=1 for channel 1 substream. Paths vary by device/model/configuration; these templates are not universal hardware-tested guarantees.

Prove video, then save

1. Click Test decoded video. Read the result next to the action.
2. Confirm an actual current frame from the intended room. Ping success or device found alone is not a video test.
3. Click Save camera. Check that Saved cameras increased and verify its channel/path identity.
4. Use New camera for the next channel; do not overwrite a saved camera to add another one. Test saved checks the protected stored connection without retyping it.
5. For an existing camera, leave IP blank to preserve credentials. To replace the connection, enter the full replacement IP, username and actual password.

Unknown brand or rejected path

Expand Advanced connection tools. Auto-detect / diagnose stream checks limited candidate paths at this IP/port and stops at authentication rejection; it never guesses passwords. For ONVIF-capable equipment, enable ONVIF on the device and use an authorised ONVIF account if required. Read device profiles, choose the actual video source/profile, then Test selected profile. Only a decoded frame confirms it. /onvif/device_service is an HTTP control endpoint, not a video path.

5. Monitor, use the video wall and save zones

Start and confirm monitoring

On Overview choose Start / apply configuration. Confirm Monitoring is Running and compare Configured cameras with Connected video streams. Running alone does not mean every stream is healthy. On Cameras, check each saved camera for Live / No video and its connection reason. A fourth or fifth stream may expose an NVR session, network, licence or PC capacity limit; saving more cameras does not guarantee concurrent decoding/inference capacity.

Professional multi-camera view

Open Video wall. Choose Auto-fit or 2 x 2 (4), 3 x 3 (9) or 4 x 4 (16). Use Previous wall page / Next wall page if more cameras exist than fit. Compact tiles saves space; switch it off to see more metrics. Fullscreen wall uses the browser fullscreen feature; press Esc to return. The wall shares capture with monitoring rather than opening another NVR login per tile. It displays periodically refreshed frames, not guaranteed full-motion CCTV playback.

Draw a zone

1. Open Zones and choose the saved Camera.
2. Select Shelf / inventory, People count, Restricted area or Exclude from detection.
3. Drag a rectangle over the image. Yellow: inventory; teal: count; purple: restricted entry; red: exclusion.
4. Choose Save zones and wait for the confirmation beside the action. Unsaved zone changes means it has not been committed.
5. Re-select the camera and check that the outline remains. Saved outlines also appear in Cameras; do not assume every video-wall tile has a zone overlay. Clear selected zone type clears that type in the editor; Save zones commits the change.

Apply changes without stopping every camera

Camera and zone saves apply automatically while monitoring runs; only the changed camera reconnects. A brief interruption on that camera can occur. There is no normal need to stop all monitoring to add each new camera. If monitoring is stopped, saves do not start it: use Start on Overview. If the save says it could not apply, read that error and verify the saved record before repeating the action.

Daily operating check

Keep the agent running, PC awake, LAN/NVR powered and disk space available. Inspect frame age and capture FPS where shown. A stale image is not a live feed. Sign out to protect local console access when unattended. Stop monitoring using the controls when intentionally ending a session. Do not turn off network access to cameras when testing internet disconnection: disconnect only public internet while retaining the camera LAN.

6. Enable AI and demonstrate it honestly

Enable explicitly and check readiness

In Cameras, select the saved camera. Expand AI detection and schedules. Tick the required functions and Save camera. They are off until selected. Shelf detection also needs a saved shelf zone. Check Detection readiness on that camera and Licence & health for runtime status. A checkbox, architecture label or successful synthetic startup calibration does not prove a real event will be detected.

Schedules

Use daily schedule uses the saved site timezone. Overnight windows are supported; equal start/end means all day. IMPORTANT: enabled theft detection remains active at all times in this build. Other enabled AI functions follow the daily window. Do not tell a customer that the schedule suppresses theft alerts.

What each function actually means

People count reports visible people and tracked appearances, not guaranteed unique visitors or directional door entries. Shelf/inventory reports visual-change candidates after a stable baseline, not reliable SKU stock or exact box quantities. Theft uses proximity/concealment heuristics; an alert is not proof of shoplifting and local VLM visual verification is unavailable. Fall detection needs working pose inference and an observed upright-to-horizontal transition. Occlusion, view angle, sampling rate and missed frames can prevent detection.

Limitations that must be disclosed

Restricted areas need a saved restricted rectangle and enabled Restricted zone. First observed person-centre presence creates a review candidate; continuous occupancy is not a fresh entry, and identity/access rights are not checked. Loitering, suspicious behaviour and crowding remain unvalidated heuristics. Staff matching, visual search, local language-model assistant, offline visual verification and high-value-counter capabilities are unavailable. Help with this screen provides offline, rule-based guidance using the page and runtime status, not screenshot interpretation or a language model. GPU/CPU capacity and field fall/theft accuracy remain unqualified.

Controlled test record

Use one camera first. Record site-local time, camera/channel, enabled feature, zone, schedule and the expected action. Observe live video, perform an authorised safe test, then inspect Incidents and evidence. For fall tests use approved recordings or a supervised safe protocol; never ask someone to deliberately fall. Record observed event time, delay, correct/wrong location, person visibility, missed events and false alerts. Repeat negative cases. Label simulated incidents as UI demonstrations, not real AI evidence. If a real test fails, log it as failed rather than claiming detection works.

7. Reports, health, storage and private backups

People count

Open People count and choose the Site-local date. Review People visible at last sample, Tracked appearances and Last sample for each camera. No sample means no measurement, not zero. Stale means the sample is old. Counts can include the same person in overlapping cameras and new tracks after restart; do not compare them to a guaranteed unique-visitor total. Download CSV exports the selected date; Print report uses the browser print dialog.

Incidents and evidence

Open Incidents for saved local candidates. Check camera name, site-local time and evidence image. Print report with evidence opens browser printing; inspect print preview before saving a PDF. Not visually verified offline means the system has no qualified offline VLM confirmation. An empty incident list is not proof that the scene was safe or detection worked. Offline records do not automatically synchronise to hosted dashboards.

Licence & health without developer clutter

Runtime health summary shows monitoring, health, verified preferred detector architecture, execution provider, connected streams, successful model-call total and last latency. CPU (ONNX Runtime) is a valid CPU path, not GPU acceleration. CPU fallback or Needs attention must not be hidden. Model-call totals include startup calibration and do not establish recent live-camera inference. Technical details (for support) is collapsed by default and contains only selected diagnostics, not local file paths or camera passwords.

Disk quota

In Storage & backup, inspect used space and available disk. Set Site data quota (MB) and Save quota. New recording stops at the configured quota or below 256 MB free disk space; this can explain missing new evidence. Internet loss does not intentionally evict existing incidents. Increasing the quota helps only if the disk has real free space. Back up before moving or deleting data.

Back up and restore

Choose Download private backup ZIP. Store it encrypted/access-controlled: it contains evidence and protected camera credentials. Restoring credentials requires the original Windows user account. To restore, first make a current backup, choose Restore a private backup and read the replacement confirmation. Console uploads are limited to 2 GB. Restore replaces site camera/configuration/count/incident data and stops monitoring, while preserving the current local owner, device binding and entitlement. Review cameras, then start monitoring again. This is not a portable cross-PC licence or credential migration tool.

8. Troubleshooting and demo handover checklist

Console will not open / invalid credentials

Check that VantagAgent.exe is running from the fully extracted folder. Open its current 127.0.0.1 address on that same PC; old ports/bookmarks can fail. Website login does not work locally. Welcome back requires the existing local owner, not a new signup. Request supported recovery if that password is lost. If you still see a large raw JSON block, you may be running an older local UI; a website deployment cannot update an already-extracted offline installation. Apply the approved local update and refresh the page.

RTSP 401 / rejected authentication

The device refused that RTSP request. Verify the actual username/password, remote live-view/RTSP and per-channel rights, account lockout and any separate ONVIF user. A working web login or ping does not prove RTSP permission. Type literal # in the separate password field. Stop repeated attempts if locked out; do not keep changing brand templates or guessing passwords. Never weaken NVR security globally to bypass the failure.

Timeout / reachable device but no picture

Check the PC is on the correct LAN, the recorder IP/RTSP port and channel are correct and the channel is online in the NVR. Review Windows/network firewall policy without disabling all protection. Test an H.264 substream, close competing VLC/viewers and inspect NVR session/bandwidth limits. Unknown brand: read actual ONVIF profiles where supported. A successful Test decoded video must show the intended room, not just a success message.

Some cameras work, another fails / no AI incident

Compare saved channel/path identities to avoid duplicates. Check licence concurrent-camera entitlement, enabled state, NVR sessions, CPU load, frame freshness and network quality. Test the failing channel alone to separate device access from concurrency. For missing AI, check feature saved, schedule, zone, runtime/model readiness, video quality and storage. No alert may be a genuine miss. Preserve the exact local test time and observations for engineering; do not fabricate a successful result.

Before showing a customer

[ ] Correct controlled package and version; no public-release claim.
[ ] Local owner stored securely; no superadmin credentials shared.
[ ] Correct device licence active; expiry/policy understood.
[ ] Each intended room has a current decoded frame.
[ ] Zone saves persist; enabled features and schedules checked.
[ ] Real positive and negative demo tests documented, including failures.
[ ] Evidence/report timestamps and selected dates checked.
[ ] Disk space and private backup verified.
[ ] Internet-disconnected test keeps LAN connected.
[ ] Customer told which features are experimental/unavailable. Record PC, package version, camera/channel, local time, visible error and the privacy-filtered technical summary when escalating; omit passwords and private footage unless authorised.