

SURVEILLANCE GUARDIAN

CCTV Health Monitoring & Remote Access

User Guide & Training Manual

Everything an installer's office, engineers and site managers need to know a CCTV system is working, get footage out of it, and give the right people access to it — without a site visit.

Version 1.0

Engineer M8 · em8portal.com

Surveillance Guardian at a glance

Surveillance Guardian is a small hub fitted beside the CCTV recorder on a site. Every five minutes it checks the whole system — every camera, every hard drive, the recorder itself — and every half hour it takes a snapshot from each camera and has it scored for image quality. The results reach you in the EM8 Portal and the EM8 HQ app, in a daily report, and as an email the moment a fault appears.

The same hub is the way in. Footage is pulled from the recorder through it, an engineer can open the recorder's own interface through it, and an alarm receiving centre can be connected through it — all without a single port opened on the site's router.

Every site has its own Surveillance Guardian dashboard, split into the tabs below.

Every feature, in one table

Tab	What it does
Cameras	Every camera with its latest snapshot, status, recording state, model and firmware — and the Vision AI panel scoring each one for evidence quality, day and night. Rename cameras and hide unused channels.
System	The recorder: brand, model, firmware and whether an update is recommended, clock, users, network protocols, and what each camera is capable of (motion, human, vehicle, line crossing).
Storage	Every hard drive with its SMART health — the early warning signs that predict a failure — plus free drive bays for extending retention.
Vault	The reports. Daily fault reports and the individual camera, storage, system and Vision AI fault reports, previewed, downloaded or emailed.
Gatekeeper	Recorder user accounts. Reveal or rotate a password, enable or disable a user, without logging into the recorder. Add-on.
Footage	Request a clip — camera, from, to — and play, download or email it once the hub has retrieved it. Held for 31 days.
Redaction	Turn a clip into one that shows only the person you choose, with everyone and everything else obscured. For subject access and police requests. Add-on.
Logs	Who did what: configuration changes, footage requests and downloads, redaction jobs, password reveals, portal changes.
Remote GUI	Open the recorder's own web interface through the hub for fifteen minutes. Installer roles only.
ARC Connect	Connect the site to your alarm receiving centre — secure video access for their operators and alarm emails relayed to their platform. Add-on.
Hub Settings	The hub's network settings and the recorder(s) it talks to. Installer roles only.

What Surveillance Guardian also gives you

- **A check every five minutes** — not a ping, a full pass: is each camera present, is it recording, is each drive healthy, is the recorder reachable, is its clock right.
- **Vision AI image integrity** — a working camera can still be useless: out of focus, pointing at the ceiling, blinded by glare, or with a spider over the lens. Every snapshot is scored so those are found before the footage is needed.

- **Predictive drive health** — three in four drive failures show SMART warning signs first. Storage flags them so the drive is swapped before the footage is lost.
- **Fault emails and the daily report** — each person chooses whether they want an email the moment a fault appears, a daily summary, both or neither.
- **No port forwarding, ever** — the hub makes outbound connections only. Remote access for you, your customer and the ARC all ride on it, which is why it works on a 4G SIM where the site's own network is off limits.
- **An audit trail** — every footage download, every password reveal, every configuration change is logged against the person who did it.
- **Multiple recorders** — a hub can watch up to four recorders on the same site.

How to use this guide: Section 1 is signing in and roles; Section 2 is the one-off setup on each site. Sections 3 to 12 follow the tabs left to right. If you only read one section, read Section 3 — Cameras — because that is where a fault first shows. If you fit systems, read Sections 11 and 12 as well.

Contents

Section	Covers
1. Getting started	Signing in, sites, who sees what, the app, email preferences
2. Setting up a site	Hub, recorder, channels, camera names, the first daily report
3. Cameras	Status, snapshots, Vision AI, managing channels
4. System	Recorder details, firmware, users, protocols, camera capabilities
5. Storage	Drives, SMART warnings, free bays
6. Vault	The reports and what to do with them
7. Gatekeeper	Recorder accounts, reveal and rotate
8. Footage	Requesting, playing, downloading, emailing, the 31-day rule
9. Redaction	Producing a clip that shows one person only
10. Logs	The audit trail
11. Remote GUI and Hub Settings	The installer tabs
12. ARC Connect	Connecting an alarm receiving centre
13. The EM8 HQ app	Surveillance Guardian on a phone
14. Quick reference	The routine, and the glossary
15. Common questions	Troubleshooting

1. Getting started

1.1 Signing in and finding a site

1. Go to your EM8 Portal address in any modern browser and sign in with the email address and password supplied when your account was created.
2. From the left-hand menu choose **Surveillance Guardian**. You land on your sites, filtered to the ones with a hub.
3. Each site card shows its status — **Active** (hub activated), **Partial** (some hubs on the site not yet activated) or **Inactive** — and how many hubs it has. Search by site, customer or postcode.
4. Click a site. Its Surveillance Guardian dashboard opens on the Cameras tab, with the site name in the title.

Every part of the dashboard is a tab across the top. The web address includes the site, so a bookmark takes you straight back to that site.

If you see an upgrade screen instead: your account does not yet have an active Surveillance Guardian subscription. Contact Engineer M8 or visit Billing.

1.2 Who sees what

Surveillance Guardian is built for the installer. The installer's staff see everything; the end customer's users see the monitoring and footage side but not the tabs that change the system.

Role	Typically	What they can reach
Customer	The end user — site manager, store manager	Cameras, System, Storage, Vault, Footage, Logs, and the add-ons if enabled. In Gatekeeper they can manage ordinary recorder users but cannot reveal an admin or engineer password.
Customer Admin	The customer's own manager	As Customer, plus creating Customer logins for their own site(s).
Office / Engineer / Admin	The installer's staff	All of the above plus Remote GUI, Hub Settings, the full Gatekeeper, and ARC Connect.

Which sites a person can see is set on their user record under **Associated Sites**. A hotel manager sees their hotel; a regional manager sees five; the installer's engineers see every site the installer looks after.

1.3 Finding your way around

Where everything lives

One dashboard per site. Eleven tabs; three are paid add-ons; three are installer-only.

Cameras	System	Storage	Vault	Gatekeeper	Footage	Redaction	Logs	Remote GUI	ARC Connect	Hub Settings
Status table	Recorder details	Drive health	Fault reports	Recorder users	Request clip	Pick person	Changes	Open recorder	Choose ARC	Network
Vision AI	Firmware	SMART	Daily report	Reveal/rotate	Play, email	Queue job	Requests	15-min tunnel	Alarm email	Recorders
Manage channels	Users, protocols	Free bays	Email/download	ADD-ON	Download	ADD-ON	Reveals	INSTALLER	ADD-ON	INSTALLER

Add-ons show a padlock until they are enabled for the site. Installer-only tabs are hidden from end-customer logins altogether.

Eleven tabs. Padlocked tabs are add-ons not yet enabled for this site.

- **Tabs with a padlock** are add-ons — Gatekeeper, Redaction, ARC Connect — that are not enabled for this site. Clicking one shows what it does and what it costs; a Customer Admin or installer admin can enable it from there and it is added to the site's subscription (Section 1.5).
- **Coloured status** is consistent: green is fine, amber needs a look, red is a fault, grey is unknown — usually a check that has not run for a day.
- **Snapshots** are the last still the hub took from that camera, not live video. That is deliberate: it shows the camera is working without anyone watching people.
- **Every action on a site is logged** — the Logs tab (Section 10) is the answer to "who did that?".

1.4 Choosing which emails you get

Two switches on your Profile (your name at the top right) under Surveillance Guardian:

- **Daily summary** — one email a day with the daily fault report for your sites.
- **New fault emails** — an email the moment a new fault is detected on a camera, drive or recorder.

They are per person. The installer's service desk wants both; a store manager may want neither and rely on the app.

1.5 Add-ons

Three tabs are paid add-ons, billed per site on top of the site's Surveillance Guardian subscription:

Add-on	What it gives you	Term
Gatekeeper	Recorder user management from the portal — reveal, rotate, enable, disable.	Rolling monthly
ARC Connect	Secure access for your alarm receiving centre, and alarm email relay.	Rolling monthly
Redaction	Privacy-redacted clips for subject access and police requests.	Minimum term applies

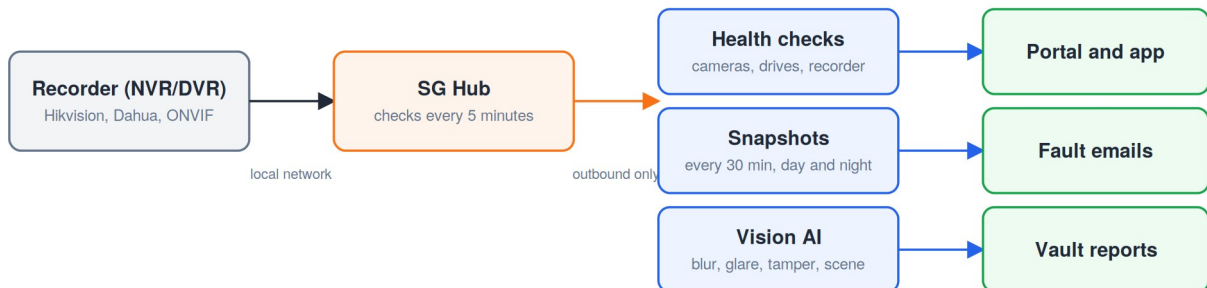
Open the padlocked tab, read the price, and click to enable. The first month is pro-rated to your billing date and it then bills with the site. Cancelling stops future charges and access continues to the end of the paid period. Only an account administrator can add or cancel an add-on.

2. Setting up a site

Engineer M8 supplies the hub. The installer fits it beside the recorder, activates it, and does the ten minutes below. After that the site looks after itself.

How Surveillance Guardian watches a site

A hub on site talks to the recorder. Nothing is opened on your firewall.



Footage, the remote GUI and ARC access all travel through the same hub, so no port forwarding is ever needed on site.

The hub sits on the same network as the recorder and connects outward to EM8.

2.1 Fitting and activating the hub

1. Connect the hub to the same network as the recorder — or, on a 4G hub, to power only. A dual-port hub can have one port on the CCTV network and the other on the site's network for internet, with nothing bridged between them.
2. On the portal, add the site if it does not exist, then activate the hub against it using the serial number and activation code printed on the hub.
3. Open the site's **Hub Settings** tab (Section 11.2) and enter the recorder's IP address, port, username and password. Add further recorders if the site has more than one — up to four.
4. Save. Within a few minutes the Cameras tab fills in.

Nothing inbound. The hub only ever connects outward, to EM8. No port forwarding, no DDNS, no changes to the site's firewall. If the site's IT department asks what the hub needs, the answer is outbound internet on standard ports and nothing else.

2.2 Tidy the cameras

A recorder reports every channel it has, whether or not a camera is plugged into it. Before the first report goes out:

1. On the **Cameras** tab click **Manage Channels**.
2. Untick every channel that has no camera on it. They move to the Unused Channels list and stop appearing in fault reports as "camera missing".
3. Rename each camera to what it actually looks at — "Front door", "Loading bay" — using **Rename a camera** on the same screen. Names are what the reports and the ARC see.

An unused channel that is left active is a permanent fault on every daily report, and a daily report with a permanent fault on it stops being read within a fortnight.

2.3 Turn on the emails

Ask each person who should know about faults to set their Profile switches (1.4). Nothing is emailed to anyone who has not opted in.

2.4 Enable any add-ons

If the site is monitored by an ARC, enable ARC Connect (Section 12). If the customer wants control of recorder accounts, Gatekeeper (Section 7). Both are per site.

3. Cameras

The Cameras tab is where a fault shows first. It has two halves: the Vision AI panel across the top, and the camera status table underneath.

3.1 The status table

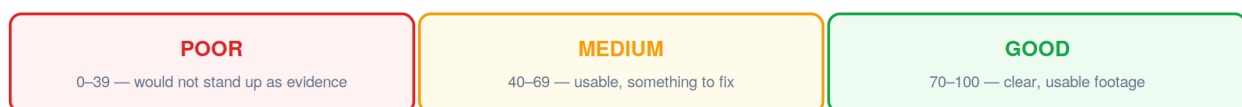
Column	Shows
Camera No.	The channel number as the recorder reports it — this is the number quoted in fault reports.
Camera Name	The name you gave it (2.2).
Recorder	Which recorder it is on, where a site has more than one.
Snapshot	The latest still from the camera. Click to enlarge.
Status	A tick if the last check found no fault, a cross if it did, a grey mark if the last check is more than a day old or the state is unknown.
Recording Status	What the recorder says about recording on that channel.
Model / Firmware	The camera's own model and firmware, where the recorder exposes it.
Last Checked	When the hub last checked this camera. Should be within the last five minutes on a healthy site.

The counters above the table — Total, Healthy, Faults, Outdated, Deleted — are the site in one line. Filter the Status column to see just the faults.

3.2 Vision AI — camera health and image integrity

Reading a Vision AI score

Every snapshot is scored out of 100 for evidence quality, day and night separately.



evidence quality score

Underneath the score: blur, too dark, glare, noise, occlusion, IR washout, colour cast, compression, scene change, tamper.
A low score with all checks clean is worth a second look — and a correction, which trains the model.

The evidence quality score, and the checks that sit under it.

A camera that is online and recording can still be producing footage nobody could use. Every snapshot is scored out of 100 for **evidence quality** — could this image identify a person or a vehicle? — separately for day and night, and checked for the faults that drag the score down:

Check	What it catches
Blur	Out of focus, or a smeared dome.
Too dark / Exposure	A scene too dark or too bright to read.
Glare	Light in the lens — a security light, low sun.

Check	What it catches
Noise	Grain that swallows detail, usually low light.
Occlusion	Something in the way — a cobweb, a sticker, a parked vehicle.
IR washout / IR flood	Night infrared bouncing back off something close to the lens.
Colour cast	A tint that suggests a failing sensor or IR cut filter.
Compression	Artefacts that mean the recorder is starving the stream.
Scene changed	The view is not what it was — the camera has been moved.
Blind tamper	The camera may have been covered or redirected.

Each camera's panel shows its day and night scores with a GOOD / MED / POOR badge, the health checks with their severity, and when it was last analysed. Tap the panel for the full breakdown.

Score looks wrong? Under any camera's breakdown is **Correct this assessment**. Enter what the score should be and why — "false tamper, camera has not moved". Your correction is weighted ten times over the automatic score when the model is next retrained, so a fisheye lens that keeps scoring low gets fixed at the source rather than argued about every week.

3.3 Managing channels

Manage Channels opens three tools:

- **Active cameras** — untick channels with no camera to move them to Unused. Restore them from the same list when a camera is fitted.
- **Rename a camera** — pick the camera, type the new name (letters and numbers, up to 24 characters).
- **Remove / restore a camera** — take a camera out of the dashboard and reports without deleting its history, and bring it back later.

Removing a channel here does not touch the recorder. It only changes what Surveillance Guardian reports on.

4. System

The System tab is the recorder itself — one card per recorder on the site.

4.1 Recorder details

Brand, model, type (NVR or DVR), the user the hub connects as, IP address and HTTP port, the installed firmware, the recorder's system clock, and when the hub last checked it. **Recheck recorder connectivity** runs the check now; **Refresh hub connection status** confirms the hub itself is reachable.

The password is masked. **Show Password** reveals it to installer roles only, and the reveal is logged.

Firmware. Where EM8 knows the current firmware for the recorder model, the card says whether an update is available and, for security-relevant releases, that it is recommended. Updating is still done on the recorder — through Remote GUI (Section 11.1) — not from here.

4.2 System users

The user accounts on the recorder and their level (admin, operator, user). This is the read-only view; managing them is Gatekeeper (Section 7).

4.3 Protocols

Each network protocol the recorder supports — HTTP, HTTPS, RTSP, ONVIF, SDK — with whether it is enabled and on which port. This is the first place to look when an ARC or a third-party system cannot connect: the protocol they need is usually supported but not enabled.

4.4 Camera configuration

One row per camera showing which smart features it supports and which are switched on: motion detection, human detection, vehicle detection, line crossing, field entry (intrusion), audio and two-way audio. Three states: not supported by the camera, supported but not enabled, supported and enabled. A camera that supports human detection but has it off is a camera generating false alarms it does not need to.

4.5 Configuration log

Every change the hub has seen to the recorder or a camera — field, previous value, new value, when. If a camera's name, a port or a user changed and nobody owns up, it is here.

5. Storage

Recorders fail at the hard drive. The Storage tab shows each drive on each recorder with the SMART data that predicts a failure before it happens.

5.1 Reading it

Field	Means
Status	Healthy, Advisory, Warning or Error, from the SMART figures below.
Power-on hours / Age	How long the drive has been running. Surveillance drives are rated for a number of years, not for ever.
Temp	Current temperature. Sustained high temperatures shorten drive life.
Reallocated sectors	Bad sectors the drive has already swapped out. Any at all is worth watching; a rising count is a drive on its way out.
Pending sectors	Sectors the drive could not read and is waiting to retry. These are the strongest predictor of imminent failure.
Uncorrectable sectors	Sectors that failed for good.
UDMA CRC errors	Usually a cable or connector problem rather than the drive itself.

The thresholds come from large-scale drive failure studies: around three in four drives that fail show one of these warnings first. A drive flagged Warning should be replaced at the next visit, not the one after.

5.2 Free bays

Where the recorder model is known, the tab shows how many drive bays it has and how many are empty. An empty bay is retention you have not bought yet — worth knowing before a customer asks for 60 days instead of 30.

Refresh HDDs asks the hub to re-read the drives now. Storage is otherwise checked on the normal five-minute cycle, and a drive fault raises a Storage Fault Report in the Vault and a fault email.

6. Vault

The Vault holds every report the site has produced, grouped by type, newest first, with a preview and the option to download or email each one.

Report	When it is produced
Daily Fault Report	Every day, for the whole site — every camera, drive and recorder fault open that day. The one to read each morning.
Camera Fault Report	When a camera goes missing, stops recording, or comes back.
Storage Fault Report	When a drive fails or its SMART data crosses a threshold (marked "risk" for the predictive ones).
System Fault Report	When the recorder cannot be reached, its clock is wrong, or a health check fails.
Vision AI Fault Report	When a camera's image fails a Vision AI check, or its scene has changed.

6.1 Finding a report

- Scroll each category with the arrows, or search by name, type or camera.
- **Advanced Filters** narrow by report type, camera and date range — past week, past month, or all time.
- Click a report to preview it in place. **Download** saves the PDF; **Email Report** sends it to an address you type, from EM8 on your behalf.

A report is a PDF on your letterhead. The daily one is what a customer's facilities manager wants forwarded; the individual fault reports are what goes on a job sheet when an engineer is sent.

The daily report is the habit to build. Turn on the daily summary email (1.4) and read it with the first coffee. A fault that has been on three consecutive daily reports is a visit that should already be booked.

7. Gatekeeper

Gatekeeper manages the user accounts on the recorder from the portal, so nobody needs to log into the recorder — or know the admin password — to give a new manager access or take a leaver's away. It is a per-site add-on.

7.1 The user list

Every account on the recorder with its role, username, ID, whether it is enabled, and when it last changed. **Reload Users** re-reads the recorder.

7.2 Reveal a password

1. Select the user in the table.
2. Click **Reveal Password**. The current password is shown and can be copied to the clipboard.
3. The reveal is written to the Logs tab under Admin Password Requests, with your name and the time.

Who can reveal what. Passwords for privileged accounts — admin, engineer, installer — are only ever shown to the installer's own staff (Office, Engineer, Admin). A Customer or Customer Admin login sees those rows marked Restricted. Ordinary operator and viewer accounts can be revealed by the customer.

7.3 Rotate a password

Select the user and click **Rotate Password**. A new random password is generated and set on the recorder; reveal it as above to read it. Rotate when an engineer leaves, when a password has been shared too widely, or on a schedule. Installer roles only.

7.4 Enable and disable users

Disabling a user locks the account on the recorder without deleting it — the right move for a leaver, because deleting loses the audit trail on the recorder. Enable it again if they come back. Disabling also rotates the password, so a disabled account cannot be quietly re-enabled with the old credentials.

If the tab says **Gatekeeper is Disabled**, the add-on is not enabled for this site (1.5).

8. Footage

From a footage request to a redacted clip

Footage is pulled from the recorder through the hub. Redaction hides everyone except the person you choose.



Every request, download, email and redaction is written to the Logs tab with who asked for it.

A request goes to the hub, the hub pulls the clip from the recorder, and it appears in the list.

8.1 Requesting a clip

1. On the **Footage** tab pick the **camera** (and the recorder, where there is more than one).
2. Set **From** and **To** — at least one minute apart, no more than an hour, and not in the future.
3. Click **Request**. The progress panel steps through Request Sent → Device Received → Uploading → Processing → Request Complete.

You can close the page, or the browser. The retrieval runs on the hub and the clip appears in the list when it is done. Short clips on a wired site take a couple of minutes; an hour of 4K footage, or a site on a weak 4G signal, can take up to an hour. Some recorder models simply retrieve more slowly than others.

8.2 Playing, downloading and emailing

The list shows every clip with camera, start and end, and size. Click one to play it in the portal. Then:

- **Download Footage** — an MP4 to your machine.
- **Email Footage** — sent to an address you enter, from EM8 on your behalf, with the clip attached or linked.
- **Redact Footage** — moves the clip into the site's redaction folder to be privacy-edited (Section 9).

Footage is deleted after 31 days. Every clip retrieved to the portal is removed automatically 31 days later, on every site. Download or email anything you need to keep before then. The recorder's own recording is unaffected — this is only the copy that was pulled out.

8.3 If a request fails

"Device did not respond" means the hub did not pick the request up — check the site is online on the System tab and try again. "Transcoding failed" means the recorder returned something the hub could not convert; try a shorter window. Every request, successful or not, is on the Logs tab with who asked for it.

9. Redaction

A subject access request, a police request for one person's movements, an insurer wanting a clip of an incident — all of them need footage with everybody else taken out of it. Redaction produces that from a clip in a few clicks. It is a per-site add-on with a minimum term, because the video processing behind it is expensive.

9.1 How it works

Redaction here is the inverse of blurring faces. The **whole frame is obscured** and only the person you choose is revealed, followed through the clip — including when they turn away from the camera. Where the system cannot follow them confidently for a moment, the frame stays fully redacted rather than risk revealing someone else, so short gaps in the reveal are expected and safe.

9.2 Producing a redacted clip

1. On the Footage tab, play the clip and click **Redact Footage** to move it into the redaction folder. Or open the **Redaction** tab and pick from the source clips already there.
2. **Step 1 — Select source clip.** Pick the clip.
3. **Step 2 — Generate previews.** The system takes a series of snapshots through the clip.
4. **Step 3 — Choose a snapshot.** Click one where the person you want is clearly visible. People in it are detected and outlined.
5. **Step 4 — Select the person to keep.** Click them. The panel says how much of the clip they are visible in — good, partial or low coverage — so you know what you will get.
6. Click **Start Redaction**. The job is queued; you get an email when it is done, which can be up to an hour for a long clip.

The finished clip appears in the **Redacted Clips Library** on the same tab. Play it in the browser (HLS is smoother; MP4 is the file to download and hand over).

Check the coverage figure before you start. If the snapshot picker says "subject visible in 12% of frames", the person is mostly out of shot or the tracker lost them. Choose a snapshot where they are large and unobstructed, or a shorter clip that starts when they enter. A low-coverage clip is still safe — it is just mostly black.

9.3 What is logged

Every redaction job — source file, snapshot time, the person index chosen, who requested it, the status — is on the Logs tab. When the data protection officer asks how a clip was produced, that is the record.

10. Logs

Everything done to or through a site is written down. The Logs tab has six lists:

Log	Records
Device Changes	Configuration changes seen on the recorder and cameras — what, from, to, when.
Footage Requests	Every clip requested: camera, window, who asked, result.
Footage Segment Log	The pieces the hub actually retrieved for each request, with sizes and times.
Redaction Requests	Every redaction job: source file, snapshot time, person chosen, who asked, status.
Admin Password Requests	Every password reveal from Gatekeeper or the System tab: which recorder user, who revealed it, when.
Portal Changes	Changes made to the site in the portal itself — names, channels, settings, add-ons — with the user.

Logs are read-only. Nothing here can be edited or deleted from the portal, which is what makes them worth showing an auditor.

11. Remote GUI and Hub Settings

These two tabs change the system, so they are only shown to the installer's own staff — Office, Engineer and Admin. Customer logins do not see them at all.

11.1 Remote GUI

Remote GUI opens the recorder's own web interface — the same screens you would see standing in front of it — in a new browser window, through the hub.

1. Open the **Remote GUI** tab and pick the recorder if the site has more than one.
2. Click **Open Remote GUI**. A tunnel is set up and the recorder's login page opens in a popup.
3. Log in with the recorder credentials — reveal them on the System tab if you need to — and work as normal.

The tunnel lasts **fifteen minutes** and then closes; click the button again for another. The tab shows when it was last opened and by whom. If nothing opens, the browser has blocked the popup — allow popups for the portal and try again.

This is what replaces the site visit. Adding a camera, changing a recording schedule, updating firmware, fixing a motion zone — anything you would do on the recorder's interface can be done here, from the office, with no port forwarding on the site. It is also what lets a customer give their maintenance company remote access without giving them the keys to the network.

11.2 Hub Settings

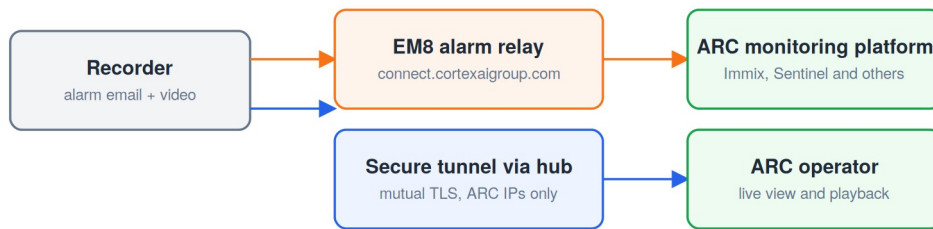
- **Hub network** — DHCP on or off, and the hub's IP and gateway if static. Change these only with someone on site; a wrong gateway takes the hub offline.
- **Recorder details** — brand (Hikvision, Dahua), type (NVR, DVR), IP address, HTTP port, username and password. This is the account the hub uses for its checks; give it a dedicated recorder user rather than the admin account where you can.
- **Additional recorders** — up to three more, each with a label, so a site with a separate DVR for the car park is one site in the portal.

Save Changes pushes the settings to the hub. The Cameras tab picks up a new recorder within a few minutes.

12. ARC Connect

ARC Connect

Two things go to the alarm receiving centre, by two routes, neither of which opens your site to the internet.



The ARC sees the relay and the tunnel, never your site's own IP address. Every connection is logged on the tab.

Alarm emails go by relay; operator access goes by tunnel. Neither exposes the site.

ARC Connect links a site to your alarm receiving centre in two ways at once: a secure tunnel through the hub for the ARC's operators to view and play back video, and an alarm email relay so the recorder's alarm notifications reach the ARC's monitoring platform. It is a per-site add-on.

12.1 Enabling it

1. Open the **ARC Connect** tab. Installer roles only.
2. Choose your ARC under **Select Your ARC**. If yours is not listed, contact Engineer M8 — each ARC is registered once, with its platform and the IP range its connections come from.
3. Enter the **alarm email address** the ARC assigned to this site — for example S124085@immixalarms.com. It is used as both sender and recipient, which is how the ARC's platform files the alarm against the right site.
4. Click **Enable ARC Access**. Provisioning the tunnel usually takes under a minute.

12.2 What the tab then shows

- **Assigned ARC** — organisation, platform, contact.
- **Connection Details** — the host and ports (RTSP, HTTP/ISAPI, SDK) the ARC uses to reach the recorder through the tunnel. **Download PDF** gives you these on one sheet to send to the ARC.
- **Alarm Email Configuration** — the SMTP server and port, and the sender and recipient, to enter on the recorder's email alarm settings. Open the recorder through Remote GUI and copy them in.
- **Recent Access Log** — every connection the ARC has made, with time and source.

Mobile SIM sites. Some mobile networks block the standard outgoing mail port. If alarm emails from a 4G site are not arriving at the ARC, use the alternative SMTP port shown on the tab, or ask Engineer M8 which port to set on the recorder.

12.3 Disabling

Disable ARC Access revokes the tunnel and the ARC loses access immediately. The CCTV system carries on as normal. Every connection is restricted to the ARC's registered IP range and uses mutual TLS, so changing ARC, or updating an ARC's IP range, is done through Engineer M8 rather than on the site.

13. The EM8 HQ app

EM8 HQ is the Engineer M8 app for iPhone and Android. Surveillance Guardian in the app is the monitoring side — the same information as the portal's Cameras, System, Storage, Logs and Vault tabs, on a phone. Changing the system — Remote GUI, Hub Settings, ARC Connect — stays in the browser.

13.1 Installing and signing in

1. Install **EM8 HQ** from the App Store or Google Play.
2. Sign in with the same email address and password as the portal.
3. Turn on Face ID, Touch ID or fingerprint when asked. The app locks when it goes into the background.
4. Allow notifications so that fault alerts reach you.

13.2 What is in it

- **Sites** — every site you have access to, with its status. Tap one to open it.
- **Cameras** — each camera with its latest snapshot, status and Vision AI score. Tap for the breakdown.
- **System** — the recorder's details, firmware, clock and connectivity.
- **Storage** — the drives and their SMART health, the same flags as the portal.
- **Logs and Vault** — the audit trail and the reports, with the PDFs opening in the phone's viewer.

What the app shows is snapshots — the last still from each camera — not live video. That is enough to see that a camera is working and pointing the right way, which is what a site manager needs and what an installer's engineer needs before a visit.

If a site is missing from the app: the site is not in the user's Associated Sites. The installer's admin adds it on the user's record in the portal. If access has just been changed, sign out and back in.

14. Quick reference

14.1 The routine

When	What	Where
Every morning	Read the daily fault reports	Email, or Vault → Daily Fault Report
On a fault email	Open the site, confirm on Cameras or Storage, book the visit if needed	Cameras / Storage
Weekly	Look for cameras with a POOR Vision AI score — usually cleaning or refocusing	Cameras → Vision AI
Monthly	Look for drives at Warning; plan the swap	Storage
Monthly	Look for recorders with a recommended firmware update	System
On a footage request	Request the clip, download or email it within 31 days	Footage
On a subject access or police request	Redact the clip, hand over the MP4	Footage → Redact, then Redaction
New site	Activate hub, Hub Settings, Manage Channels, rename cameras, emails on	Sections 2 and 11
Staff leaver	Disable their recorder user; remove their portal login	Gatekeeper; Users
New ARC contract	Enable ARC Connect, send the ARC the PDF, set the alarm email on the recorder	ARC Connect, Remote GUI

14.2 Glossary

Term	Meaning
Hub	The Surveillance Guardian device on site, beside the recorder. One per site; can watch up to four recorders.
Recorder	The NVR or DVR the cameras record to.
Channel	A camera input on the recorder. Unused channels should be moved to Unused so they are not reported as missing cameras.
Snapshot	A single still taken from a camera every 30 minutes. What the portal and app show; not live video.
Vision AI	The image-quality analysis run on every snapshot — evidence quality score plus the health checks.
Evidence quality	A 0–100 score for whether the image could identify a person or vehicle. 70+ is good, under 40 is poor.
SMART	The self-monitoring data a hard drive reports about itself; used to predict failure.
Daily Fault Report	The PDF produced every day listing every open fault on the site.

Term	Meaning
Gatekeeper	The add-on for managing recorder user accounts from the portal.
Redaction	The add-on that produces a clip revealing one chosen person with everything else obscured.
ARC	Alarm receiving centre — the monitoring station that watches the site.
ARC Connect	The add-on that gives the ARC secure video access through the hub and relays alarm emails.
Remote GUI	The recorder's own web interface, opened through the hub for fifteen minutes at a time.
Associated Sites	The list on a user's record of the sites they are allowed to see.

15. Common questions

A camera shows a grey status.

The last check is more than a day old, or the state came back unknown. Usually the hub has lost its internet connection — check the System tab's hub connection status. If the hub is fine, the recorder may have stopped answering; Recheck recorder connectivity.

Every daily report lists a missing camera that does not exist.

A channel on the recorder with no camera on it. Cameras → Manage Channels, untick it. It moves to Unused and stops being reported.

A camera scores POOR on Vision AI but looks fine to me.

Open the breakdown. If a specific check has fired — glare, blur, IR washout — go and look at that. If every check is clean and the score is still low, use Correct this assessment: your correction is weighted ten times in the next retrain and the model stops making that mistake on that camera.

The night score is much lower than the day score.

Normal to a degree — infrared images carry less detail. A large gap usually means IR bouncing off something close to the lens (a wall, a sign, a cobweb), which the IR washout check should be naming.

A drive says Warning but the recorder says it is fine.

Recorders only report a drive that has already failed. Warning here means the SMART data shows the signs that come before a failure. Replace it at the next visit.

Footage request has said Uploading for forty minutes.

An hour of footage, a 4K camera, or a weak 4G signal can take up to an hour. Leave it; it carries on without you. If it goes to Request Failed, the hub or the recorder did not respond — check the System tab and retry.

A clip I retrieved last month has gone.

Retrieved footage is deleted after 31 days on every site. Request it again from the recorder if it is still within the recorder's own retention.

The redaction picker says it found four people and there were two.

It occasionally detects a person-shaped object — a jacket on a hook, a pallet of bags. Choose the outline that is actually your subject; the others are ignored.

The redacted clip goes black for a few seconds.

The tracker lost the subject for that moment and redacted the whole frame rather than risk revealing someone else. That is by design. If it is most of the clip, choose a snapshot where the subject is larger, or a shorter clip.

I cannot see Gatekeeper, Redaction or ARC Connect.

If the tab has a padlock, the add-on is not enabled for this site — open it and enable it, or ask your account administrator. If the tab is not there at all, your login is a customer role and the tab is installer-only.

Gatekeeper shows Restricted against the admin user.

Privileged recorder passwords are only shown to the installer's staff. Ask your installer.

Remote GUI opens nothing.

The browser blocked the popup. Allow popups for the portal address and click Open Remote GUI again. If the tunnel fails outright, the hub is offline or the recorder IP on Hub Settings is wrong.

The ARC says they cannot connect.

Three things in order: is ARC access enabled on the tab; are they using the host and ports on the Connection Details PDF; is the protocol they need enabled on the recorder (System → Protocols). Their connection must also come from the IP range they registered with Engineer M8.

Alarm emails are not reaching the ARC.

Check the recorder's email settings match the Alarm Email Configuration on the tab exactly — server, port, sender and recipient. On a 4G site, use the alternative port. If it still fails, Engineer M8 can see the relay log.

I am not getting fault emails.

Your name at the top right → Profile → the two Surveillance Guardian switches. Nothing is sent to anyone who has not turned them on.

A user can see a site they should not.

Their Associated Sites list includes it. Edit their user record and remove it. Note that the installer's own Office, Engineer and Admin users see every site the installer looks after.

The hub is offline.

On a wired site, check power and the network cable, and that the site's firewall still allows outbound connections. On a 4G site, check signal and that the SIM is active. The hub needs nothing inbound, so a firewall change that only added rules should not have broken it.

A page shows an error after an update.

Refresh the page. This almost always follows a new release and clears once the browser picks up the new version.

Need help? Your Engineer M8 contact is your first port of call for anything this guide does not cover — including feature requests. The system is actively developed and customer suggestions do get built.

Engineer M8 · em8portal.com