



MANUFACTURED BY **LAWNSWOOD TECHNOLOGY
LIMITED**



User Manual

Intelligent HART Gateway

HG1v4

Contents

Product Overview	5
In the box	5
Getting Started	6
Before you begin	6
Power up	6
Reach the web interface	6
A tour of the Home page	7
Add your first HART devices	7
First Modbus read	8
Where to go next	9
Specifications	10
Electrical	10
Interface protocols	10
Mechanical	10
Environmental	11
Compliance	11
Cybersecurity	11
Hardware Layout	13
Front-panel LEDs	13
Power	14
Ethernet	14
HART Loop Connection	15
Serial Interface	17
Installation & First Power-On	18
What you will need	18
Steps	18
LED quick reference	18
Reaching the Web Interface	20
Find the gateway's address	20
Browser support	20

If the page does not load	20
Home Page	21
Layout	21
Status Strip	21
System Panel	22
Device Tabs	22
Page Links	22
Action Dialogs	23
Tips	24
Configuration	25
The Save / Build / Deploy Workflow	25
System Settings	26
Serial Port	26
Network Ports	26
Devices	26
Scan Devices	27
New Configuration	28
Export / Import	28
Things to Know	28
Commissioning	29
Workflow	29
Field Groups	30
Editing Tips	31
Actions	31
Things to Know	32
Modbus Map	33
How the Map is Built	33
The Map Table	34
Saving Changes	34
Accessing Modbus Data	34
Things to Know	35
System Update	36
When to Use	36
How an Update Runs	36
A/B Partitions and Rollback	37

Update Channels	37
Local / Off-Network Update	37
Things to Know	38
KFD2 Multiplexor Mode	39
Wiring	39
Configuration	40
Differences from Gateway mode	40
Remote Access	41
Enabling remote access	41
Disabling and re-enabling	41
Rotating passwords	41
Indicators	41
Notes	42
Beyond the web UI	42
Roles & Access Control	43
oper	43
engr	43
Choosing a role	43
PC Software	44
HG1Discover	44
HG1VspManager	45
Troubleshooting	46
Power and boot	46
Reaching the web interface	46
HART communication	46
Configuration Save / Build / Deploy	47
System Update	47
Remote access	47
KFD2 multiplexor	47
Modbus	48
Raising a support ticket	48
Glossary	49
Support & Contact	51

Product Overview

The HG1v4 is the latest revision of the HG1 Intelligent HART Gateway family. It provides convenient and reliable access to field-instrument data for any device that supports the HART communication standard.

The HG1v4 can be used as:

- A **HART modem** over the on-board RS-232 / RS-422 / RS-485 serial port, allowing PACTware, FieldCare, RadarMaster and other configuration software to talk directly to your transmitters.
- A **HART modem over Ethernet** using a virtual serial port (the HG1VspManager PC application) for remote access.
- A **HART-IP** server over Ethernet.
- A **Modbus TCP** gateway, exposing HART variables as Modbus registers for SCADA / DCS / PLC integration.
- A **Modbus RTU** gateway over the serial port.
- An **encapsulated RTU Modbus** server over Ethernet (RTU-over-TCP).

The modem and gateway functions can be used **simultaneously**. The gateway arbitrates HART loop access automatically so a SCADA system can keep polling a transmitter while a field engineer is configuring another one with PACTware on the same loop.

When used as a Modbus gateway the HG1v4 supports all mandatory and common-practice HART commands. Device-specific commands can be added via configuration templates, and the Modbus register layout can be left auto-generated, customised, or left in a legacy layout for backwards compatibility.

In the box

- HG1v4 gateway in DIN-rail enclosure
- Quick Start Guide leaflet (this document is the full manual; the Quick Start covers power-up and first connection)

No software is shipped on media — everything you need is on the device itself, and updates download automatically when the gateway has internet access.

Getting Started

This chapter walks you from an unopened box to a HART variable showing up on Modbus. It is the shortest complete path through the gateway — enough to prove the system works end-to-end. Reference detail for every step lives in the chapters that follow.

If the gateway is already on the bench in front of you, the printed Quick Start leaflet in the box covers the same procedure in poster form.

Before you begin

You will need:

- The HG1v4 gateway and a suitable 24 V DC power supply
- An Ethernet cable and a PC or laptop
- **Either** at least one HART transmitter wired on a powered 4–20 mA loop
- **Or** a Pepperl+Fuchs KFD2-HMM-16 multiplexer system with field transmitters connected to its termination boards

You do not need any Windows software installed. Everything you need is on the gateway itself.

Power up

Wire the gateway to your 24 V DC supply — the terminal locations are shown in Hardware Layout. Connect an Ethernet cable to your network (or directly to your PC for bench testing).

When power is applied, the front-panel indicators come up in this order:

- The **PWR** indicator lights immediately.
- The **RUN** indicator blinks while the firmware boots, then goes solid green after around fifteen seconds.
- The **Ethernet** indicators show link and activity as soon as the cable negotiates.

A gateway that has RUN solid green and Ethernet lit is ready.

Reach the web interface

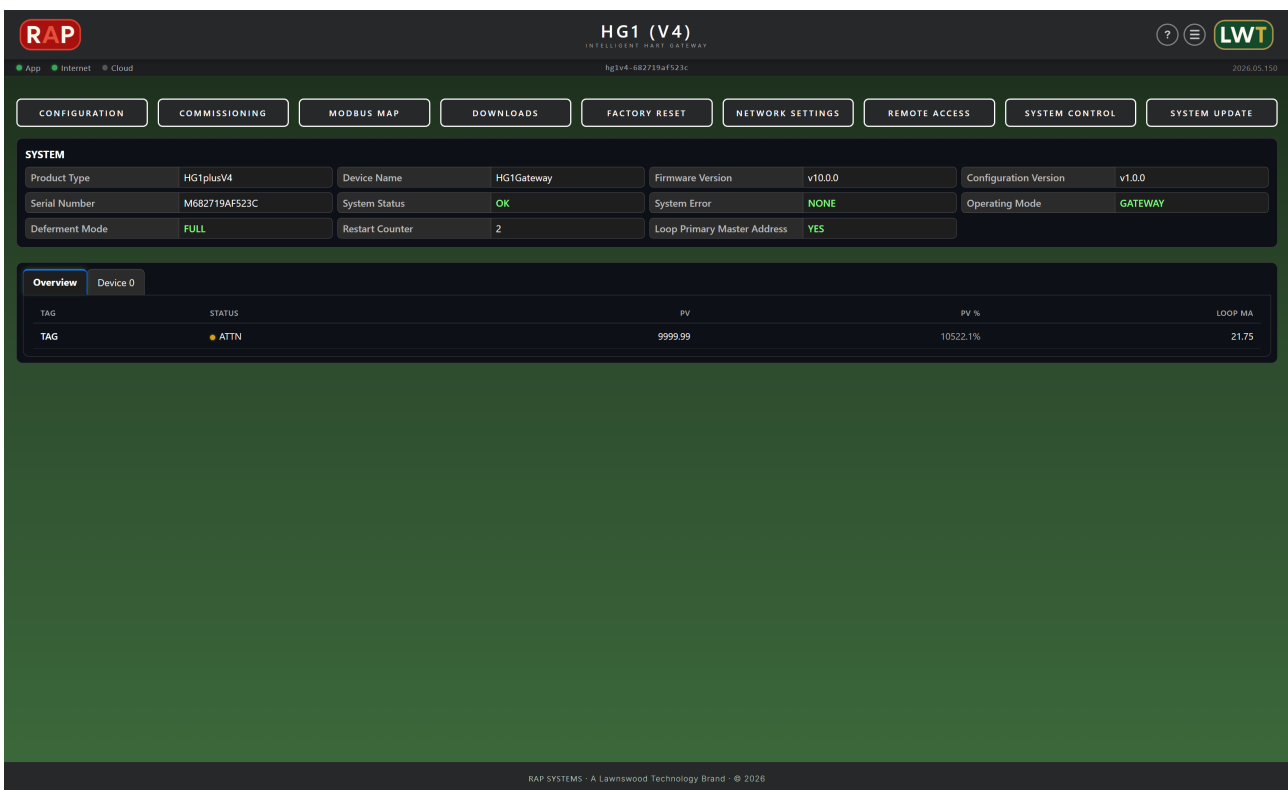
All configuration and diagnostics is done through the gateway's built-in web interface. There are three ways to find it:

1. **Router DHCP table.** Look for a hostname beginning with `hg1v4-` in your router's list of connected clients.

2. **HG1Discover.** The Windows utility (available from the support site) broadcasts on your LAN and lists every HG1v4 it can see with its IP, hostname and firmware version.
3. **Direct-cable link-local.** Connect the gateway to your PC by a single Ethernet cable, leave the PC's adapter on "obtain IP automatically", and browse to `http://169.254.100.1`. This always works, regardless of DHCP state.

Once the browser loads the Home page you are in. If the page does not load, see Reaching the Web Interface for the full troubleshooting checklist.

A tour of the Home page



At a glance:

- **Status tile** — gateway name, firmware version, uptime, and overall health.
- **Device tabs** — one tab per configured HART device, showing PV, SV, TV, QV, loop current and status.
- **Update** — visible when a firmware update is available.
- **Downloads** — links to the datasheet, manuals and PC utilities.

A full reference for every panel is in Web UI Overview.

Add your first HART devices

Two variants, depending on how your transmitters are wired. Pick the one that matches your system.

GATEWAY MODE — A DIRECT HART LOOP

You have one or more transmitters wired directly to the HG1v4's HART terminals.

1. Wire the loop to the HG1v4's HART terminals. Polarity is marked on the terminal label.
2. In the web interface, open **Configuration**. Confirm that **Operating Mode** shows Gateway. If it does not, click **New Standard** to start a fresh Gateway configuration.
3. Click **Scan Devices**. The gateway sweeps HART poll addresses 0–15 on the loop and lists what answers.
4. Tick the transmitters you want to add, then click **Import**.
5. Click **Save**, then **Build**, then **Deploy**. The gateway briefly restarts with the new configuration; live data on the Home page will pause and come back.
6. Return to the **Home** page. Each transmitter now has its own tab with live PV, SV and status.

MULTIPLEXER MODE — A KFD2-HMM-16 SYSTEM

You have a KFD2 multiplexer on the DIN rail with field transmitters wired to its termination boards.

1. Wire the KFD2's serial input to the HG1v4's **TX+** / **TX-** RS-485 terminals. The **L1** / **L2** HART terminals are not used in this mode.
2. In the web interface, open **Configuration**. Click **New Multiplexor** to start a fresh MUX configuration.
3. Click **Scan Devices**. The gateway reads the device list that the KFD2 already has cached. If the KFD2 has not scanned its own loops yet, click **Rebuild & Scan** instead — this asks the KFD2 to physically re-scan and can take several minutes.
4. Tick the field transmitters you want to import, then click **Import**.
5. Click **Save**, then **Build**, then **Deploy**.
6. Return to the **Home** page. The first tab is the KFD2 multiplexer itself; the tabs that follow are your field transmitters, each showing live PV from the KFD2's cache.

If Scan Devices returns an empty list, or a device shows COMM in the status column, see Troubleshooting.

First Modbus read

The gateway exposes every polled HART variable as one or more Modbus registers. To confirm the whole chain is working, read one back.

1. Open the **Modbus Map** page.
2. Find the row for a transmitter's Primary Variable (PV) and note the register address.
3. From any Modbus TCP client — Modbus Poll, mbpoll, or your SCADA / DCS — connect to the gateway's IP address on port 502 and read that register.
4. The value returned should match the PV shown on the gateway's Home page, within one poll cycle.

At this point the gateway is doing its job: polling the field, and answering Modbus queries with live data.

Where to go next

- Change transmitter tag, descriptor or poll address, and issue standard HART commands — Commissioning.
- Trim the Modbus register layout to a minimal map, hand-build a custom one, or preserve the legacy v2 layout — Modbus Map.
- Reach the gateway from anywhere over a secure tunnel — Remote Access.
- Set up role-based access so an operator can view but not change configuration — Roles.
- Keep firmware current with signed over-the-air updates — System Update.
- Connect a KFD2 multiplexer for the first time — KFD2 Multiplexor Mode.
- Something is not working as expected — Troubleshooting.

Specifications

Provisional figures. Mechanical, connector and environmental figures in this chapter are shared with the previous HG1 generation, which the HG1v4 retains for drop-in replacement. Final electrical and compliance figures for the HG1v4 are published in the Product Datasheet at <https://downloads.lawnswoodtechnology.com/hg1v4/HG1v4-Datasheet.pdf> once formal type-testing is complete.

Electrical

Parameter	Value
Nominal supply voltage	+24 V DC
Supply voltage range	See Datasheet
Power consumption	See Datasheet
HART interfaces	1 × Primary/Secondary master, multi-drop supported
HART loop resistance (minimum, external)	250 Ω
Serial port	1 × software-selectable RS-232 / RS-422 / RS-485
Ethernet	1 × 10/100 Base-T RJ-45

Interface protocols

- Modbus TCP/IP
- Modbus RTU (over the serial port)
- Encapsulated RTU Modbus (RTU-over-TCP)
- HART-IP
- Raw HART modem (over serial or virtual COM port)

Mechanical

Parameter	Value
Mounting	Snap-on DIN rail
Rail compatibility	DIN EN 60715 TH 35

Parameter	Value
Enclosure material	Flame-retardant PA 66 (UL 94 V-0)
Dimensions (W × D × H)	75 × 26 × 112 mm
Weight	See Datasheet
IP rating	See Datasheet
Ethernet connector	RJ45
All other signal connectors	5.08 mm pitch screw terminals, accepting up to 4 mm ² wire

Environmental

Parameter	Value
Operating temperature	–40 to +85 °C ambient
Storage temperature	–50 to +125 °C
Humidity	5 to 90 % non-condensing
Altitude	up to 12,000 ft (≈ 3,660 m)

Compliance

The HG1v4 is designed to meet CE, UKCA, FCC Part 15 (Class A), ICES-003 and HART registration. Current certification status is published in the Product Datasheet — refer there for the marks currently issued and their revision dates.

Cybersecurity

The HG1v4 is designed around the EU Cyber Resilience Act (CRA) and the industrial-automation standard IEC 62443, which is the framework most UK, US and international asset owners specify against. In practice this means:

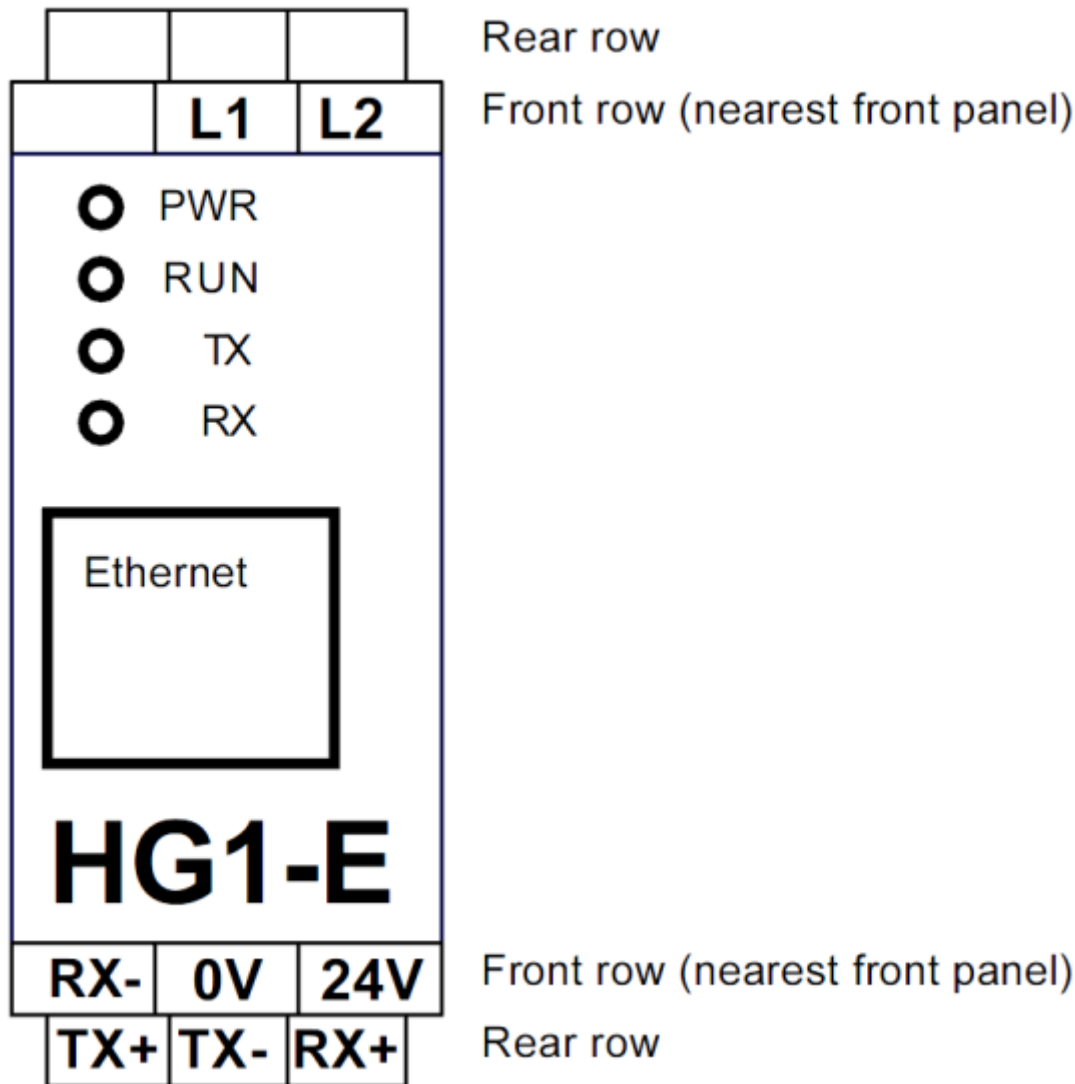
- Firmware is signed and installed to a standby A/B partition with automatic rollback on boot failure.
- Remote access is an outbound TLS-only tunnel with no inbound ports.
- Interactive SSH login is disabled.
- Every release ships with published notes and a version-pinned update channel.

A published vulnerability-disclosure policy and per-release Software Bill of Materials (SBOM) will follow ahead of the September 2026 and December 2027 CRA milestones, giving asset owners a

clear path to CRA-compliant procurement and to the equivalent obligations emerging in the UK (Cyber Security and Resilience Bill) and US (federal SBOM / SSDF procurement rules).

Hardware Layout

The HG1v4 uses a DIN-rail enclosure with screw terminals along the top and bottom edges. Power, the HART loop and the serial port are all on screw terminals. Ethernet is via an RJ45 connector on the front face.



Front-panel LEDs

LED	Indicates
PWR	Illuminates when the device is powered.
RUN	

LED	Indicates
	Illuminates when the gateway has booted normally. A flashing RUN LED indicates a problem with the configuration or firmware version.
TX	Illuminates when transmitting HART data.
RX	Illuminates when receiving HART data.

Power

Apply a regulated **24 V DC** supply across the **24V** and **0V** terminals. The PWR LED should illuminate immediately; the RUN LED follows 10–15 seconds later once the firmware has finished booting.

Ethernet

Standard 10/100 Mbps RJ45. Out of the factory the gateway uses **DHCP**, with a fixed link-local address of **169.254.100.1** always present as a fallback.

- **On a managed LAN**, the gateway picks up an IP from your DHCP server.
- **For a direct PC connection**, set your adapter to obtain an IP automatically and reach the gateway at **http://169.254.100.1**.

Once you can reach the home page, the **Network Settings** dialog lets you assign a static IP if you prefer.

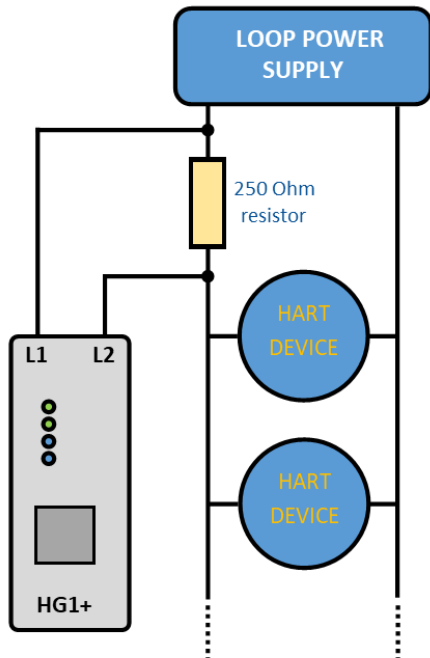
HART Loop Connection

Loop connections are made on the **L1** and **L2** terminals. The HG1v4 is **polarity insensitive** on these terminals. The gateway does **not** embed a loop sense resistor — one must be provided externally.

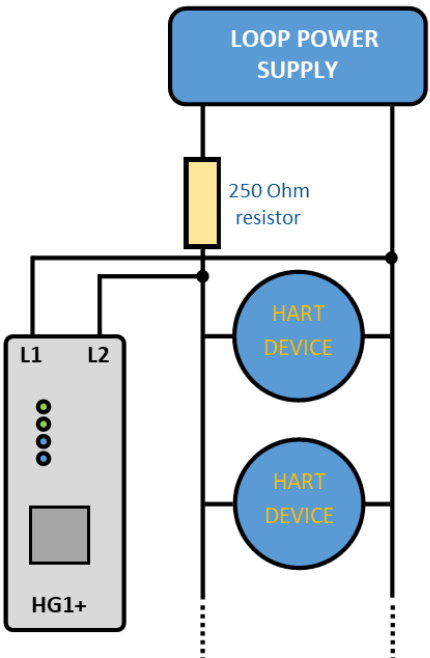
For HART communications the loop must present a resistance of at least **250 Ω** . This can be achieved by inserting a 250 Ω resistor in series with the loop.

Note: If the loop is also being used for 4–20 mA signalling (for example to a PLC analogue input), the analogue input's series resistance counts towards the 250 Ω total. If the input is 100 Ω , add a 150 Ω resistor to make 250 Ω end-to-end. Anything below 250 Ω will degrade HART signal integrity.

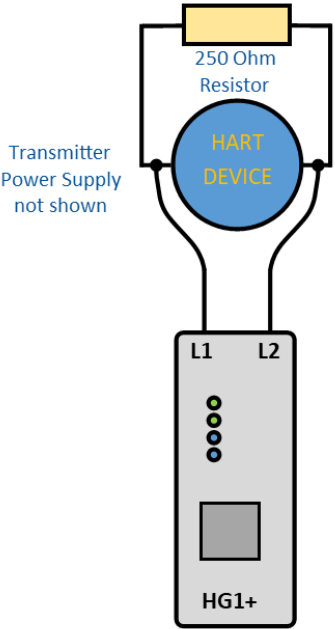
Loop powered transmitters Option A:
HG1 CONNECTED ACROSS SENSE RESISTOR



Loop Powered transmitters Option B:
HG1 CONNECTED ACROSS LOOP



Active Transmitter
HG1 CONNECTED ACROSS LOOP



SERIAL INTERFACE CONNECTIONS

	SIGNAL	HG1 TERMINAL
RS232	TX DATA	TX-
	RX DATA	RX-
RS422	TX DATA +	TX+
	TX DATA -	TX-
	RX DATA +	RX+
	RX DATA -	RX-
RS485	DATA +	TX+
	DATA -	TX-

Serial Interface

The on-board serial port supports RS-232, RS-422 and RS-485. Pick the standard you need on the **Configuration** page; the same physical terminals serve all three with different pin assignments.

Standard	Signal	HG1 Terminal
RS-232	TX DATA	TX-
RS-232	RX DATA	RX-
RS-422	TX DATA +	TX+
RS-422	TX DATA –	TX-
RS-422	RX DATA +	RX+
RS-422	RX DATA –	RX-
RS-485	DATA +	TX+
RS-485	DATA –	TX-

Installation & First Power-On

The Quick Start Guide that ships in the box covers this in compact form (and is reproduced as a printable PDF at <https://downloads.lawnswoodtechnology.com/hg1v4/HG1v4-QuickStart.pdf>). The same steps are reproduced here so the manual is self-contained.

What you will need

- A regulated **24 V DC** power supply
- An **Ethernet RJ45** patch cable (straight or crossover — the gateway auto-negotiates)
- A PC with a web browser

Steps

1. Mount the gateway on a 35 mm DIN rail.
2. Connect the power supply to the **24V** and **0V** terminals as shown on the connection diagram printed on the side of the module.
3. Connect the Ethernet cable between the gateway and your PC, or to your network switch.
4. Apply power. The **PWR** LED illuminates immediately; the **RUN** LED follows 10–15 seconds later.
5. Open a web browser and connect to the gateway:
 - **On a managed LAN**, find the gateway's DHCP-assigned address using your router's connected-clients list, or by running the HG1Discover utility on your PC.
 - **Direct PC connection**, set your network adapter to obtain an IP automatically and browse to <http://169.254.100.1>. The gateway is always reachable on this address.
6. Use the on-device **Help** menu (the ? button at the top of every page) for context-sensitive guidance, or read the chapters that follow for the full reference.

If the RUN LED stays off after 30 seconds, power-cycle once. If it persists, raise a support ticket at <https://support.lawnswoodtechnology.com>.

LED quick reference

LED	State	Meaning
PWR	Solid	24 V supply present.
RUN	Solid	Firmware running normally (10–15 s after power-up).
RUN	Off after 30 s	Firmware not running — power-cycle; if it persists, raise a support ticket.

LED	State	Meaning
RUN	Blinking	Start-up failure detected — raise a support ticket.

Reaching the Web Interface

All configuration, commissioning and diagnostics is done through the gateway's built-in web interface. There is no PC software to install for routine use — point a browser at the gateway and you are in.

Find the gateway's address

Out of the factory the gateway uses DHCP. There are three reliable ways to locate it on your network:

1. **Router DHCP table.** Most home / office routers list their connected clients; look for a hostname starting with `hg1v4-`.
2. **HG1Discover** (Windows). The PC utility broadcasts a discovery packet on the local network and lists every HG1v4 it can see, with its current IP, hostname and firmware version. Available from <https://support.lawnswoodtechnology.com>.
3. **Link-local fallback.** The gateway always answers on `169.254.100.1` regardless of DHCP state. With your PC's adapter set to "obtain an IP automatically" and connected directly to the gateway via Ethernet, browse to <http://169.254.100.1>. This is the simplest method on the bench.

Browser support

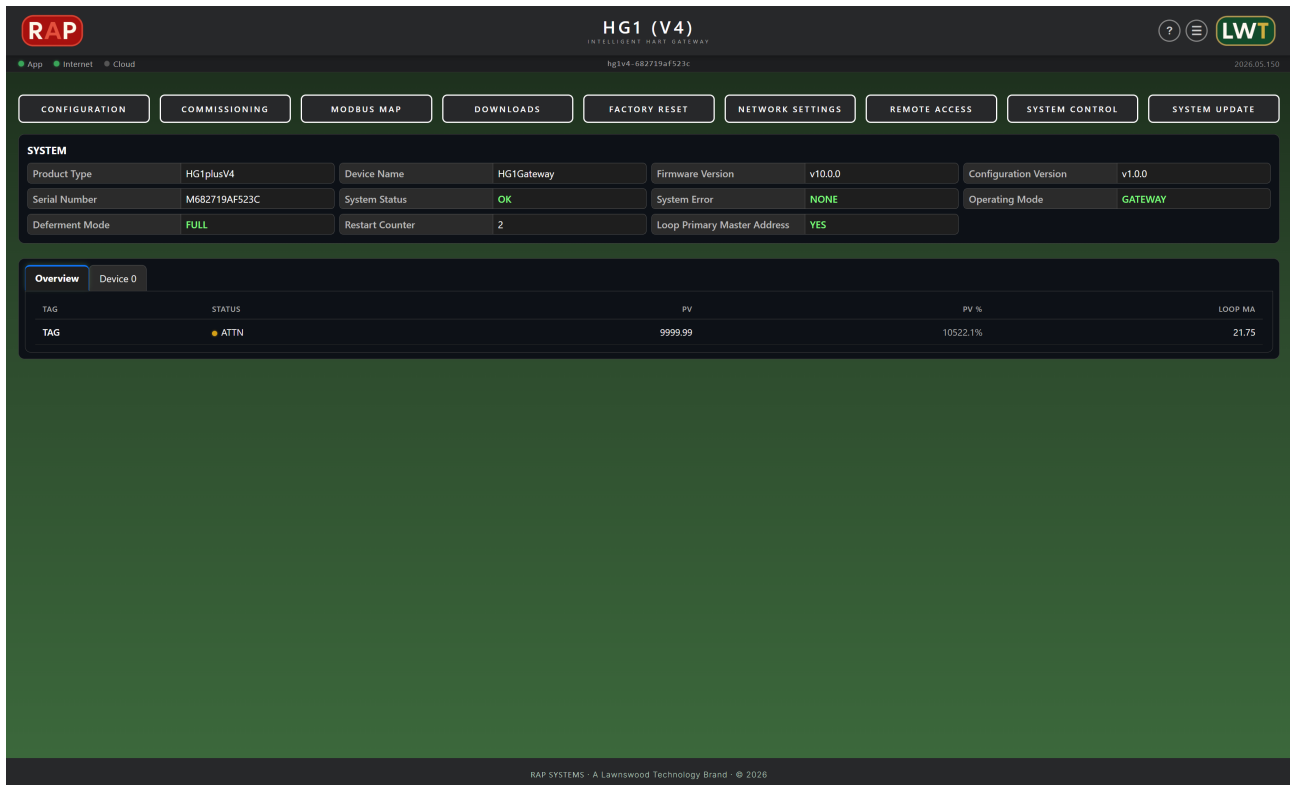
Any current desktop browser will do — Chrome, Edge, Firefox or Safari. The interface is responsive and works on mobile, but the full configuration and commissioning workflow is best on a desktop screen.

If the page does not load

- Make sure the **RUN** LED is solid green. If it is off, the firmware has not booted.
- On a direct connection, confirm your PC adapter has picked up a `169.254.x.x` link-local address.
- On a managed LAN, the address may have changed at the last DHCP lease renewal. Re-run HG1Discover or check your router.
- Some corporate networks block link-local — try a direct Ethernet connection in that case.
- If your browser shows a TLS warning, you have probably typed `https://` — the on-device interface uses plain HTTP. Remote access (covered in Remote Access) is HTTPS.

Home Page

The home page is the entry point to the gateway. It shows live data from the running application and gives you access to every other page and dialog.



Layout

- A **slim status strip** along the very top of every page shows ambient health: App, Internet, Cloud (remote access tunnel), the device hostname, and the firmware version.
- The **action grid** at the top of the home page is your menu — page links on the left, action dialogs on the right.
- The **System** panel and the per-device tabs below it stream live values from the gateway every few seconds.

Status Strip

Each indicator is a coloured dot plus a one-word state.

- **App** — Running (green) or Stopped (red). If the app is stopped the live data area is dimmed and the value tabs go stale.
- **Internet** — Up or Down. Used by remote-access checks and System Update.

- **Cloud** — Connected, Disconnected, or Disabled. "Disabled" (grey) means you have not enabled the remote access tunnel; "Disconnected" (red) means the tunnel is enabled but the device cannot reach the remote access service.
- **Device name** — your gateway's hostname, useful when you have several devices on the bench.
- **Version** — the firmware version currently running.

System Panel

Top of the live area. Shows gateway-level fields:

- **Product Type** — hardware identifier
- **Device Name** — the configurable name (set on the Configuration page)
- **Firmware Version / Configuration Version** — what is running, and what configuration it is running
- **Serial Number** — derived from the gateway's MAC address
- **System Status** — OK (green) or shows an error code in red
- **Deferment Mode** — how the gateway handles HART command queueing (None / Partial / Full)
- **Restart Counter** — how many times the gateway application has restarted since the last reboot

Each value has a small dot — green = received and valid, grey = stale / not yet received.

Device Tabs

Each connected HART transmitter has its own tab below the System panel.

- Click a tab to see that device's variables, status bits, and communication health.
- Variables with named states (OK, ERROR, FAILED) are coloured — green for OK, red for fault.
- The **Device Status** sub-panel decodes the eight standard HART status bits as ticked / unticked boxes.
- The **Communications** sub-panel shows whether HART traffic is healthy. If errors are seen the individual HART error bits are shown.

In **MUX mode** the first tab is the KFD2 multiplexor itself; the rest are the field transmitters behind it.

Page Links

The buttons on the left of the action grid take you to other pages.

- **Configuration** — manage HART devices, polls, network ports. Save / Build / Deploy workflow.
- **Commissioning** — configure HART transmitters in the field (read settings, change them, write back). Per-transmitter UX, like a DTM.

- **Modbus Map** — see how HART variables are exposed as Modbus registers; build a custom map.

Action Dialogs

The buttons on the right of the action grid open dialogs without leaving the home page.

DOWNLOADS

Lists data files the gateway has produced (configuration backups, exported logs). Each file has a download button.

FACTORY RESET

Erases user configuration and restores defaults. Asks for confirmation before doing anything.

The following is **preserved** by Factory Reset: network settings, SSH host keys, remote-access credentials. Use the dialog when you want to start a configuration over without losing remote management.

NETWORK SETTINGS

Configure the Ethernet interface — DHCP or static (address in CIDR notation, gateway, DNS servers — add multiple DNS rows if needed).

Changes take effect immediately. If the gateway's IP changes you may need to reload the page at the new address.

REMOTE ACCESS

Enable or disable the remote access tunnel. When enabled the gateway is reachable from anywhere via `<hostname>.lwtdevices.cloud` (HTTPS, basic auth).

There are two roles:

- **oper** — view-only (read configuration, see live data, cannot change anything)
- **engr** — full control (configure, run actions, install updates)

The dialog shows the public address with a clipboard icon next to it for copy/paste. Each role has a **Regen** button (red) to rotate that role's password — the old password stops working immediately.

The first time you click **Enable** on a brand-new gateway, both passwords are generated and shown to you once — record them straight away. They cannot be retrieved later, only regenerated.

Stored credentials persist when the tunnel is disabled — you can rotate a password with the tunnel off and the new one will take effect when you next Enable.

SYSTEM CONTROL

A small dialog with four destructive actions:

- **Restart App** — restart the gateway application without rebooting the device
- **Stop App** — stop the gateway application (live data goes blank)
- **Reboot** — full device reboot (the loop drops out for ~30 s)
- **Shutdown** — power the device down (will not come back without a power cycle)

A countdown overlay appears for ~5 s before Reboot or Shutdown actually fires so you have a chance to cancel.

SYSTEM UPDATE

Opens the System Update modal. See the help on that page for the full update flow.

Tips

- Hovering the ? icon at the top of any page opens this style of help. Each page has its own help text.
- Use the **burger** menu (next to the ?) to jump between Configuration, Commissioning, and Modbus Map without going via the home page.

Configuration

The Configuration page is where you set up the HART gateway: which devices it talks to, what it polls them for, and how it exposes that data on its serial and network ports.

The screenshot shows the RAP Configuration page with a dark green background. At the top, there's a header with the RAP logo, a status bar (App, Internet, Cloud), a title bar (CONFIGURATION), and a user profile (LWT). Below the header, there are navigation buttons: HOME, NEW STANDARD, NEW MULTIPLEXOR, and SCAN DEVICES. The main content area is divided into four sections: System, Serial Port, Network Ports, and Devices. The System section includes fields for Name (HGTGateway), Operating Mode (Gateway (Standard)), HART Master (Primary), Deferral Mode (Full), Float Swap Mode (4 - Swap Longs), NaN on Comm Error (Enabled), NTP Time Sync (Enabled), and NTP Server (pool.ntp.org). The Serial Port section includes fields for Function (MODBUS), Interface (RS422), Baud Rate (9600), Parity (None), Stop Bits (1), and Modbus Address (1). The Network Ports section includes fields for Modbus TCP (502), Virtual COM (VCP) (772), Modbus Enc RTU (1100), and HART-IP (5094). The Devices section includes a table with columns for Slot, Type, Address, and Polling, and an ADD DEVICE button. At the bottom, there are buttons for EXPORT, IMPORT, SAVE, BUILD, and DEPLOY.

The Save / Build / Deploy Workflow

Configuration changes are not live until you push them through three steps. The **Save**, **Build**, and **Deploy** buttons enable in sequence as you progress.

1. **Save** — your edits are persisted to the gateway. Re-loading the page now would still show your edits.
2. **Build** — the source file is compiled into the runtime configuration that the gateway actually executes. This is where errors in your configuration are caught.
3. **Deploy** — the runtime configuration is activated and the gateway application restarts with the new setup. Live data on the home page will pause briefly while the application comes back up.

You can edit and Save as many times as you like before clicking Build. Once Built and Deployed, the **Save** button reads "Saved", **Build** reads "Built", and **Deploy** is disabled until you next make a change.

If you abandon a partial edit, click **Reload** to throw away your unsaved changes and re-read the file.

System Settings

Top of the page. Gateway-wide options:

- **Name** — gateway identifier (letters, digits, underscore, dot — no hyphens). Shown on the home page.
- **Operating Mode** — Gateway (direct HART loop) or Multiplexor (KFD2 MUX). Set when you create a new configuration; cannot be changed in place.
- **HART Master** — Primary or Secondary master role on the HART bus. Use Secondary if a hand-held configurator or other DCS is also a master on the same loop.
- **Deferment Mode** — controls how the gateway handles HART command queueing under load (None / Partial / Full).
- **Float Swap Mode** — byte / word ordering for floating-point Modbus registers. Match the convention your Modbus client expects.
- **NaN on Comm Error** — when enabled, returns NaN for variables when the upstream device is not responding (instead of the last-known value).

Serial Port

Settings for the on-board RS-485 serial port. Function selector chooses what the port runs:

- **HART modem** — direct HART loop (Gateway mode)
- **Modbus RTU** — slave port for Modbus RTU clients
- **VCP / Pass-through** — exposes the port over TCP

In MUX mode the function is locked to MODEM (the link to the KFD2) and cannot be changed.

Network Ports

TCP port numbers for the gateway's network services:

- **Modbus TCP** — default 502
- **VCP** — default 4001
- **HART-IP** — default 5094 (read-only; reserved)
- **Web UI** — default 80 (changing this needs a network reconfiguration; consult support before adjusting)

Devices

The devices table lists every HART device the gateway is configured to talk to. Each row shows slot, type, address, polling status, and per-row Edit / Delete buttons.

- **Add Device** — opens the device editor for a new device.
- **Edit** — change a device's type, address, or polling commands.

- **Delete** — remove a device. Not available for the KFD2 multiplexor at slot 0 — that row is locked because the system depends on it.

DEVICE EDITOR — TAG PICKER

Inside the device editor, polling is described as a list of HART **tags** rather than raw command numbers. The picker is grouped by category:

- **Process** — PV, SV, TV, QV, units, loop current
- **Device Variables** — individual DV codes (per-device-type extras)
- **Status** — communication, device status bits
- **Tag info** — Tag, Long Tag, Descriptor, Message, Date

Each tag has a small “live” dot when editing an existing device, showing whether that tag is currently producing data on the gateway. Use it to see at a glance which polled tags are actually populating.

Some tags are managed automatically by the gateway and cannot be unticked — they appear as a **greyed, ticked checkbox** with a “Always polled” tooltip. These tags are always included; the gateway runs them on a schedule the application controls (typically writes and configuration-reload triggers).

The **Search** box at the top filters the list by tag name or description.

ADVANCED — RAW HART COMMANDS

Below the tag picker is an **Advanced** section for raw HART command numbers. This is for commands that don’t map to a categorised tag (for example, vendor-specific commands you have documentation for). Commands you tick via the tag picker are hidden from the Advanced dropdown so the two lists can’t conflict.

In MUX mode, field transmitters (KFD2FIELD) receive PV / SV / TV / QV and loop current from the multiplexor’s cache automatically — so individual polling for those tags is unnecessary and hidden.

Scan Devices

Discovers HART devices on the bus.

- **Gateway mode** — polls addresses 0–15 and reports what answers
- **MUX mode** — reads the cached device list from the KFD2
- **Rebuild & Scan** (MUX only) — tells the KFD2 to physically re-scan its loops first, then reads the new list. This can take several minutes; a progress overlay covers the page until it completes.

After a scan, a picker dialog lets you choose which discovered devices to import. Devices you already have configured are unticked by default — re-ticking one will overwrite that slot (and wipe its polls).

New Configuration

- **New Standard** — replaces the current configuration with a fresh Gateway setup
- **New Multiplexor** — replaces the current configuration with a fresh MUX setup

Both wipe everything else. The gateway will need re-deploying after either action.

Export / Import

- **Export** — downloads the current configuration as a `.tar.gz` backup. Includes the source configuration, the compiled runtime, and any custom Modbus map.
- **Import** — restores from a previously exported backup. After importing, click Deploy to activate.

Things to Know

- **You need the engr role** to make any configuration changes; **oper** can view but not Save / Build / Deploy.
- An unsuccessful Build leaves the gateway running on the previous (last successfully Built) configuration — you cannot break the running gateway with a bad edit.
- Changes you Save but don't Build are persisted on disk — the next time you open this page they will still be there as unbuilt edits.
- Some sections (Serial / Network / individual fields) may be locked or hidden in MUX mode because the multiplexor controls them.

Commissioning

The commissioning page lets you read and modify the configuration of HART transmitters connected to the gateway, in the same way a DTM or hand-held configurator would.

The screenshot shows the 'COMMISSIONING' page for a device 'LODO — HARTGENDEV @ addr 0'. The interface is divided into several sections:

- IDENTITY (READ-ONLY):** Fields for Device ID number (2809973), Software revision (1), Hardware revision (32), Primary variable transducer units code (32), Primary variable transducer lower limit (-200), Primary variable transducer upper limit (850), and Primary variable transducer minimum span (0.01).
- IDENTITY / RECORD-KEEPING:** Fields for Tag (TAG), Descriptor (DESC), Date (100), Message (MSG), Final assembly number (0), and Primary variable transducer serial number (0).
- LOOP:** Fields for Polling address (0) and Minimum number of preambles required (6).
- PRIMARY VARIABLE / 4-20 MA RANGE:** Fields for Primary variable units code (32 °C — degrees Celsius), Primary variable range units code (32 °C — degrees Celsius), Primary variable upper range value (99), Primary variable lower range value (4), Primary variable damping value (0), Primary variable transfer function (0), and Primary variable alarm selection code (0 High (drive PV high)).
- LIVE READINGS:** Fields for Primary variable (9999.99), Analogue output level (0), and Analogue output percent of range (0).
- STATUS:** Fields for Device status (128), Config xfer state (3), and Device online status flag (1).
- ACTIONS:** Fields for ONLINE-1 (yes), CFGSTATE-3 (done), DEVSTAT-0x00 (fault), EXTDEVSTAT-0x00, and CFGCHGT-0. Buttons for RESET CHANGED FLAG, SELF TEST, and MASTER RESET.

You can use it to:

- Set transmitter identification (Tag, Long Tag, Descriptor, Message, Date)
- Adjust ranging (URV, LRV, units, damping, transfer function)
- Change loop current behaviour (poll address, alarm code, fixed-current mode)
- See live process variables, status bits, and device errors
- Run one-shot device actions (Reset Changed Flag, Self Test, Master Reset)

Workflow

1. Pick a device from the Device dropdown in the toolbar
2. Click **Read** — the gateway queries the transmitter and fills in the form

3. Edit any field that needs changing — modified fields are highlighted in **amber**
4. Click **Write** — only the highlighted (modified) fields are sent to the device
5. After the write completes, the form re-reads automatically so you can see the actual values the device adopted

If a write changes a field the device wasn't able to accept, that field is shown in red after the re-read so you can correct it.

Field Groups

Fields are grouped by purpose so you can find the one you want quickly.

IDENTITY

The free-text labels stored in the transmitter:

- **Tag** — short tag (8 chars, packed ASCII)
- **Long Tag** — long tag (32 chars, available on HART 6+)
- **Descriptor** — 16-char description
- **Message** — 32-char free-text message
- **Date** — last-modified date

These fields don't change device behaviour — they are documentation that travels with the transmitter.

RANGING

Controls how the transmitter scales its 4–20 mA loop output:

- **PV Units** — engineering units of the primary variable (°C, bar, etc.)
- **URV / LRV** — upper and lower range values (the values that map to 20 mA and 4 mA)
- **Damping** — first-order filter time in seconds applied to the PV
- **Transfer Function** — linear, square root, etc. (for level / flow setups)

For multi-channel transmitters the same fields appear per analogue output (AOUT2, AOUT3, ...). Single-channel devices hide the AOUT2+ groups automatically.

LOOP SETTINGS

- **Poll Address** — HART poll address (0–63). On a multi-drop bus each transmitter must have a unique address; on a single-device loop this is normally 0.
- **Loop mA Mode** — Active (transmitter drives the loop) or Disabled (transmitter ignores PV, loop sits at the fixed current). Used when commissioning so the loop doesn't swing while you're working.
- **Alarm Code** — what the loop does on a device fault: high (≥ 21.75 mA), low (≤ 3.6 mA), or last-known.

LIVE VALUES & STATUS

Read-only — populated on each Read so you can sanity-check the current process state and any active faults before committing changes.

- **PV / SV / TV / QV** — the dynamic variables and units, as the transmitter reports them now
- **Loop Current** — actual mA on the loop and percent of range
- **Device Status** — the eight standard HART status bits (decoded into pills above the Actions panel — green = OK, amber = warning, red = error)

Editing Tips

- The amber border on a field means “I haven’t been written to the device yet”. After a successful write the highlight clears.
- If you want to discard your edits, click **Read** again — the form re-fills from the device and all amber goes away.
- Long string fields (Tag, Long Tag, Descriptor, Message) show a small character counter that turns amber when you hit the protocol’s limit. Anything beyond the limit is silently truncated by the device, so the counter is the safety net.
- Some fields are hidden on older transmitters — for example, Long Tag only appears on HART 6 and above. The page checks the device’s reported HART revision and hides fields the transmitter cannot accept.

Actions

The bottom **Actions** panel runs one-shot HART commands against the selected device. They are independent of any unsaved edits in the form.

RESET CHANGED FLAG

Clears the transmitter’s “configuration changed” status bit. Use this after you have reviewed and accepted the changes — it tells downstream control systems “the new configuration is the intended one, stop flagging it as suspicious”.

SELF TEST

Asks the transmitter to run its built-in self test. Result is shown in the status line next to the buttons. The transmitter’s own diagnostics decide what’s tested — typically internal RAM, EEPROM, sensor electronics.

MASTER RESET

Confirmation required. Issues a hard reset to the transmitter — equivalent to a power cycle. The loop current will glitch while the device boots back up. Use only when you really need to reset internal state (e.g. after firmware-level changes the transmitter requires a restart to apply).

Things to Know

- The page works one device at a time. Picking a different device from the dropdown discards any unsaved edits without warning.
- If the gateway is in MUX mode, devices in the dropdown are the field transmitters behind the multiplexor — the multiplexor itself is not commissionable from this page.
- Reads and writes go through the gateway's HART driver. While a write is in flight the busy overlay covers the page so you can't accidentally double-click a button. A typical Write cycle takes 5–15 seconds depending on how many fields you changed.
- You need the **engr** role to write changes or run actions; the **oper** role can Read but cannot modify.

Modbus Map

The Modbus Map page shows how the gateway exposes HART data over Modbus. Modbus clients on the network read registers from the gateway's Modbus TCP server (and from the serial port if configured for Modbus RTU); this page is where you decide which HART tags appear at which register addresses.

How the Map is Built

The gateway can produce its register map in three ways. Pick the one that matches your situation.

MINIMAL (RECOMMENDED)

A compact, predictable layout designed for typical SCADA integration. Each device is given a fixed slot of **72 registers** starting at register 1000 — slot 1 is 1000-1071, slot 2 is 1072-1143, and so on. The slot always contains the same fields in the same order:

- Process variables (PV / SV / TV / QV) and their units
- Loop current and percent
- Device status and communication status
- Tag info

Use the Minimal map if you want a layout that is easy to predict, easy to document for your SCADA team, and consistent across devices of the same type. It is the default for new configurations.

CUSTOM

A map you write yourself, listing which tag goes at which register. Useful when you need to fit a fixed layout the SCADA system already expects, or when you only want a small set of variables exposed.

To upload a Custom map:

1. Click **Generate** in the page toolbar to produce a starter CSV from the current configuration. Edit it locally to match the layout you want.
2. Save the file as **MBMAP1.csv** (the filename must be uppercase).
3. Click **Upload** and pick your file. The page validates the CSV and previews the result before you save.

LEGACY

The original auto-generated layout from earlier firmware revisions, kept for backwards compatibility with sites that have already integrated against it. New installations should not start with Legacy.

The Map Table

The main table on the page lists every register the current map produces:

- **Address** — Modbus register number (decimal)
- **Type** — Holding Register, Input Register, etc.
- **Tag** — the HART tag the register represents (or a fixed label like “Loop Current”)
- **Device** — which configured device this register belongs to
- **Description** — short description of what the value means
- **Type / Size** — data type (16-bit int, 32-bit float, string) and number of registers consumed

FILTERING & SEARCHING

Use the toolbar above the table to narrow what is shown:

- **Scope** — show all registers, just one device, or just one slot
- **Category** — process variables / status / tag info / etc.
- **Availability filter** — hides rows for tags the device cannot produce because its HART command set does not cover them. Turn the filter off if you want to see the empty rows too (e.g. when planning before the device is connected).
- **Search** — text filter over tag, description, and address.

Saving Changes

Generating or uploading a new map is **preview-only** until you click **Save**. The preview lets you walk through the proposed layout in the table without affecting the running gateway.

When you click Save, the new map is written to disk and the gateway application restarts so the Modbus TCP server picks it up. Modbus clients reconnect automatically; expect a 2-3 second gap in polling while the application restarts.

Accessing Modbus Data

The Modbus TCP server runs on the port configured on the **Configuration** page (default **502**). Any Modbus TCP client can read the registers using standard function codes — typically Read Holding Registers (FC 03) for the data registers and Read Input Registers (FC 04) for read-only telemetry.

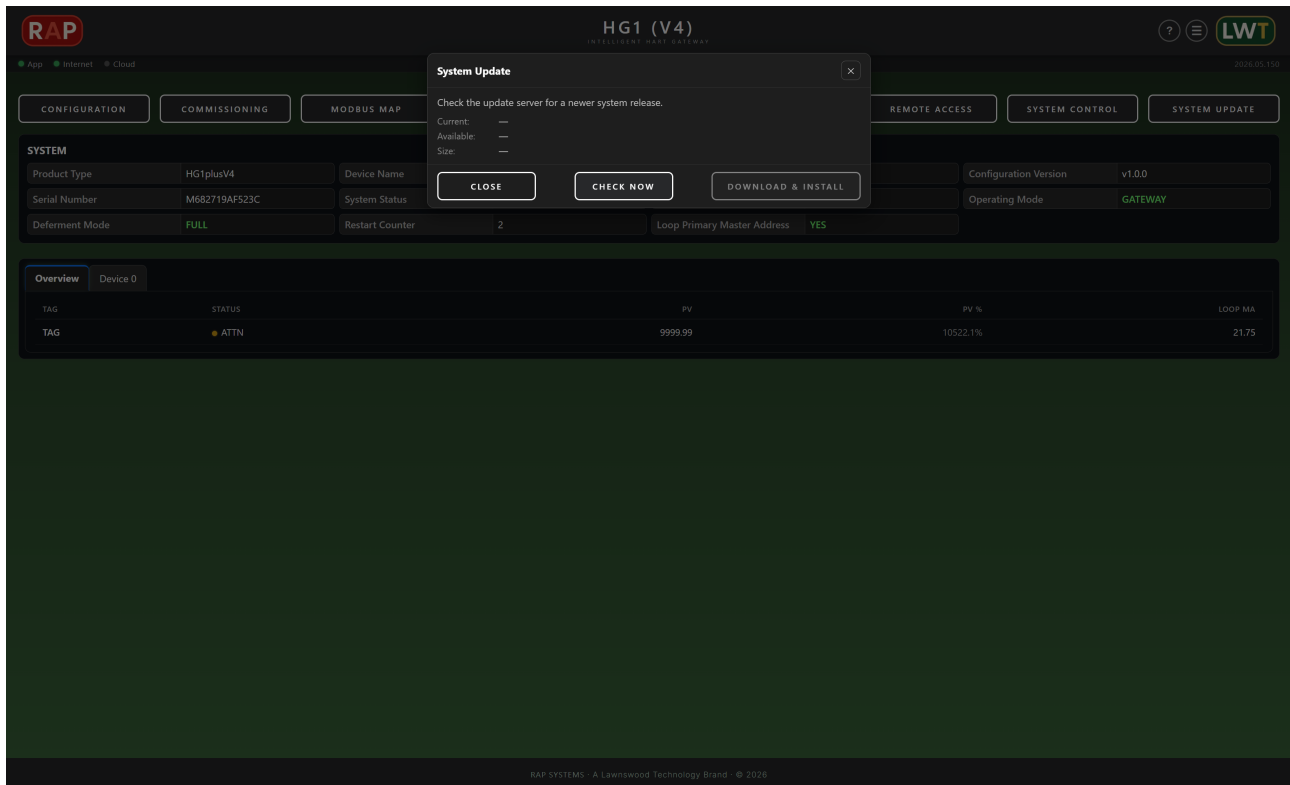
The serial port can also serve Modbus RTU when the **Serial Port** function on the Configuration page is set to Modbus RTU. The same map is served over both transports.

Things to Know

- You need the **engr** role to upload or save map changes; **oper** can view the map but not modify it.
- The Custom upload requires the filename to be exactly **MBMAP1.csv** (case-sensitive). Other filenames are rejected.
- Switching between Minimal / Custom / Legacy is a one-click swap once each map exists — the gateway keeps all three on disk so you can compare or roll back.
- A Modbus client polling at high rate may briefly see exception responses while the gateway restarts after a Save. Configure your client to retry; a 5-second timeout is a comfortable margin.

System Update

The System Update modal upgrades the gateway's firmware over the internet. Open it from the **System Update** button on the home page.



When to Use

You should run a check whenever you want to confirm the device is on the latest firmware. The modal will tell you whether a newer release is available and, if so, let you install it.

The gateway does not auto-upgrade. Updates are always initiated by you from this modal.

How an Update Runs

1. Click **Check Now** — the gateway contacts the Lawnswood Technology update server and reads the manifest for your release channel.
2. The modal shows the **currently installed** version.
3. If a newer release is available, the modal also shows: - the **available** version (highlighted green) - the **download size** - the **changelog** for the new release - and the **Download & Install** button becomes enabled.
4. If you are already up to date, only the current version and a "You are up to date" message are shown — the available version, size, and changelog rows stay hidden.

5. Click **Download & Install** to begin. The gateway downloads the update file and installs it to the standby firmware partition. Live progress is shown — current step (downloading, writing rootfs, etc.) and a percentage bar.
6. When installation finishes the gateway automatically reboots into the new firmware.
7. The modal waits for the gateway to come back online, then reloads the page so you are looking at the new firmware version.

The whole cycle takes around 5–10 minutes on a normal home / office connection. Most of the time is the download itself; the install onto NAND flash is fast.

A/B Partitions and Rollback

The gateway holds two complete firmware copies — A and B. The currently-running copy is left untouched while updates are written to the standby copy. On reboot, the bootloader switches to the new copy.

If the new firmware fails to boot three times in a row the bootloader automatically rolls back to the previous (known-good) copy. You can then reboot, run a fresh **Check Now**, and try again — typically pinned to a specific older release if there is a problem with the latest one.

This means an update can never brick the gateway. The worst case is that the new firmware doesn't start, the unit rolls itself back, and you are running on the previous version with the loop intact.

Update Channels

There are two release channels:

- **Stable** — the default for production devices. New releases are tested in-house and on field trial units before being promoted to stable.
- **Beta** — pre-release builds for early access and in-house testing. May contain unfinished features.

The channel is set per device. To switch between stable and beta, contact support — we will move your device to the requested channel from our side.

Local / Off-Network Update

If the gateway has no internet connection, the on-device modal cannot help — it requires the update server to be reachable.

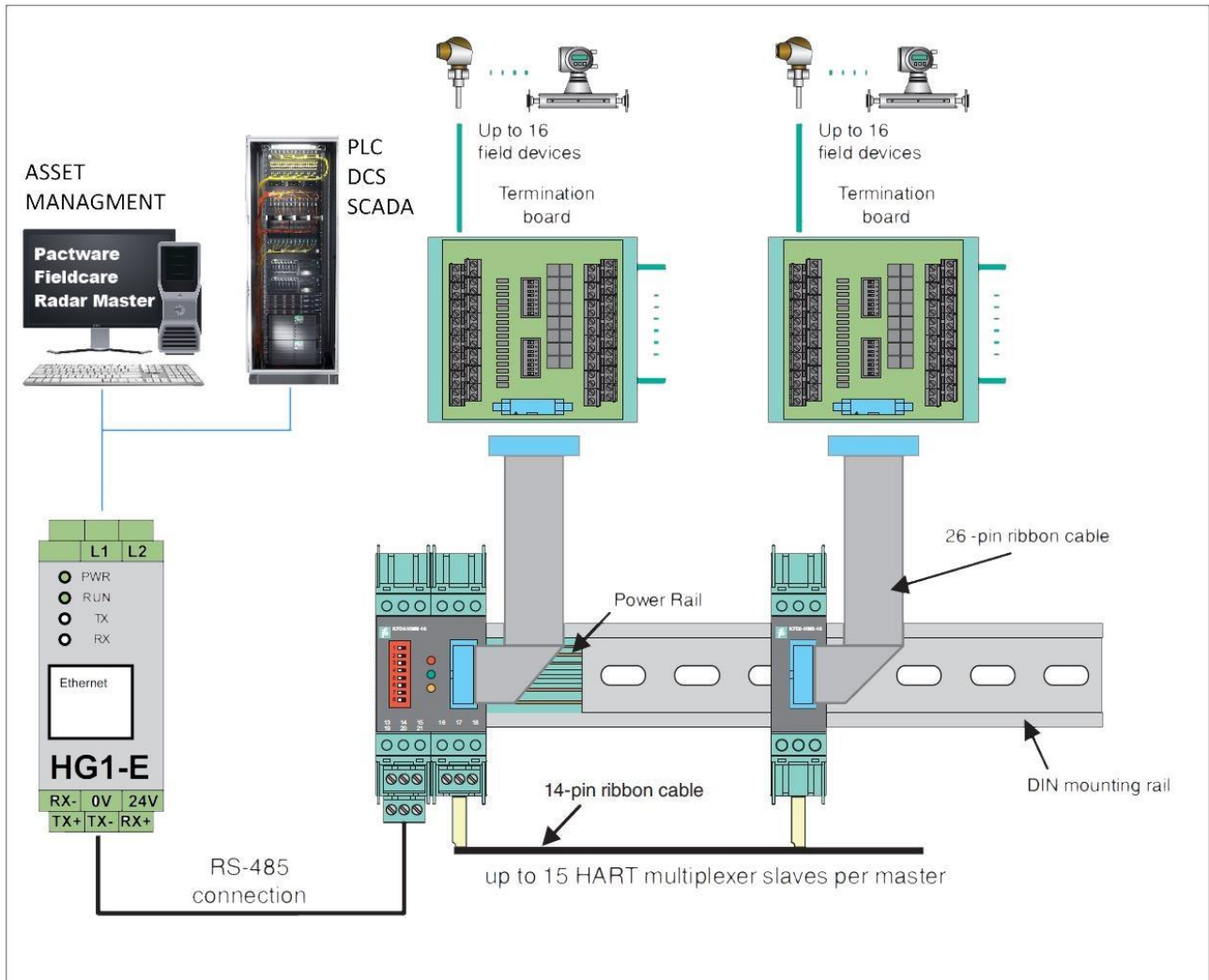
For air-gapped sites, use the **HG1 Discover** PC application (Windows). It can push a downloaded `.swu` file to the gateway over the local network. Contact support for the latest installer.

Things to Know

- You need the **engr** role to install an update. The **oper** role can run Check Now and see what is available, but cannot click Download & Install.
- Network configuration (IP address, gateway, DNS) is preserved across updates — the gateway will be reachable at the same address after the reboot.
- HART configuration (devices, polls, modbus map) is preserved.
- Remote access credentials are preserved.
- A shutdown or power loss during the install is safe — the running firmware is untouched. You will simply be back where you started, with no half-installed state.

KFD2 Multiplexor Mode

The HG1v4 can act as a HART master for a Pepperl+Fuchs KFD2-HMM-16 multiplexor system. In this mode the gateway connects to the KFD2 over **RS-485** (the L1 / L2 loop terminals are not used). The HG1v4 addresses up to **16 field transmitters per gateway** across the KFD2's channel bank.



Wiring

- **Gateway → KFD2 master:** RS-485 from the HG1v4 TX+ / TX- terminals to the KFD2's serial input.
- **KFD2 → KFD2 (slaves):** 14-pin power-rail ribbon cable between modules on the DIN rail.
- **KFD2 → field termination board:** 26-pin ribbon cable; each termination board hosts up to 16 transmitters.

Configuration

Set the gateway's **Operating Mode** to Multiplexor and the serial port to HART modem, RS-485 on the Configuration page. Then run **Scan Devices** to discover what the KFD2 currently sees on its loops, and tick the devices you want imported. The gateway addresses devices behind a multiplexor by their HART **Unique Address** rather than their short poll address — the scan handles this automatically.

Differences from Gateway mode

When the gateway is configured for Multiplexor mode some pages and fields behave differently:

- The first device tab on the **Home** page is the KFD2 multiplexor itself; the rest are the field transmitters behind it.
- On the **Configuration** page, the serial port function is locked to MODEM (the link to the KFD2) and cannot be changed.
- For field transmitters (KFD2FIELD) the gateway reads PV / SV / TV / QV and loop current from the multiplexor's cache, so individual polling for those tags is unnecessary and is hidden from the tag picker.
- The KFD2 multiplexor itself is not commissionable from the **Commissioning** page — it appears in the device dropdown only if you have configured it for direct addressing.
- The **Scan Devices** dialog has an extra **Rebuild & Scan** button that tells the KFD2 to physically re-scan its loops. This can take several minutes; a progress overlay covers the page until it completes.

Remote Access

Each gateway can be reached over the internet via a secure remote access tunnel. When enabled, the gateway is accessible at:

- **Web UI:** `https://<hostname>.lwtdevices.cloud`

Web access is protected by HTTPS plus HTTP basic authentication. Two roles are available:

- **oper** — view-only. Can read configuration, see live data, but cannot make changes.
- **engr** — full control. Can configure, run actions, install updates.

Enabling remote access

1. Open the **Remote Access** dialog from the home page.
2. Click **Enable**. On a brand-new gateway, both `oper` and `engr` passwords are generated at this point and **shown to you once** — record them straight away. They cannot be retrieved later, only regenerated.
3. The dialog shows the public address and a clipboard icon next to it for copy/paste.

Disabling and re-enabling

You can toggle the tunnel on and off at any time. Stored credentials persist when the tunnel is disabled — you can rotate a password with the tunnel off and the new one will take effect when you next Enable.

Rotating passwords

Each role has a **Regen** button (red) in the Remote Access dialog. Clicking it generates a fresh password for that role and shows it once. The previous password stops working immediately.

Rotate passwords:

- After hand-over to a new operator or engineer.
- If a password may have been seen by someone outside the team.
- On a regular schedule as part of your site's security policy.

Indicators

The **Cloud** dot in the page header reflects tunnel state:

State	Meaning
Connected (green)	Tunnel is up; the gateway is reachable from the internet at its <code>lwtdevices.cloud</code> address.
Disconnected (red)	Tunnel is enabled but the gateway cannot reach the remote access service. Check internet connectivity and outbound firewall rules.
Disabled (grey)	Remote access tunnel is not enabled on this gateway.

Notes

- Outbound connections only — the gateway initiates an outbound TLS connection to the remote access service and the tunnel rides on top. No inbound port-forwarding or public IP is required at the customer site.
- The tunnel uses TLS end-to-end. On-LAN access via plain HTTP continues to work alongside the tunnel.

Beyond the web UI

The remote access tunnel is not limited to the browser — any tool that speaks HTTPS and can send basic-auth credentials can reach the gateway, including `curl`, scripts, and lightweight integration platforms. A typical integrator use case is to pull a periodic JSON snapshot of live HART data from a central server, rather than running a full Modbus client over the WAN:

```
curl --user oper:<password> \
https://<hostname>.lwtdevices.cloud/live/data.json
```

The response is the same live state the home page renders — every configured device, current variable values, communication status, device status bits — as JSON.

Use the **oper** role for this. It is read-only, so a credential captured by a third-party logging system or shared with a contractor cannot be used to change configuration, write to transmitters, or install firmware. If the oper credential is later compromised, regenerate it from the Remote Access dialog without affecting the engr password.

Roles & Access Control

The gateway has two roles. Both apply to local web access on the LAN and to remote access over the internet.

oper

Read-only. The **oper** role can:

- See live data on the home page (status strip, system panel, device tabs).
- View the current configuration (Configuration page is read-only).
- View the Modbus map.
- Read transmitter values from the Commissioning page.
- Run **Check Now** on System Update to see if a newer release is available.

The **oper** role **cannot**:

- Save / Build / Deploy configuration changes.
- Write changes from the Commissioning page or run device actions.
- Upload or save Modbus map changes.
- Install firmware updates.
- Toggle remote access or rotate passwords.

engr

Full control. The **engr** role can do everything **oper** can, plus all configuration and modification actions. Use **engr** for commissioning, configuration changes, firmware updates and remote-access management.

Choosing a role

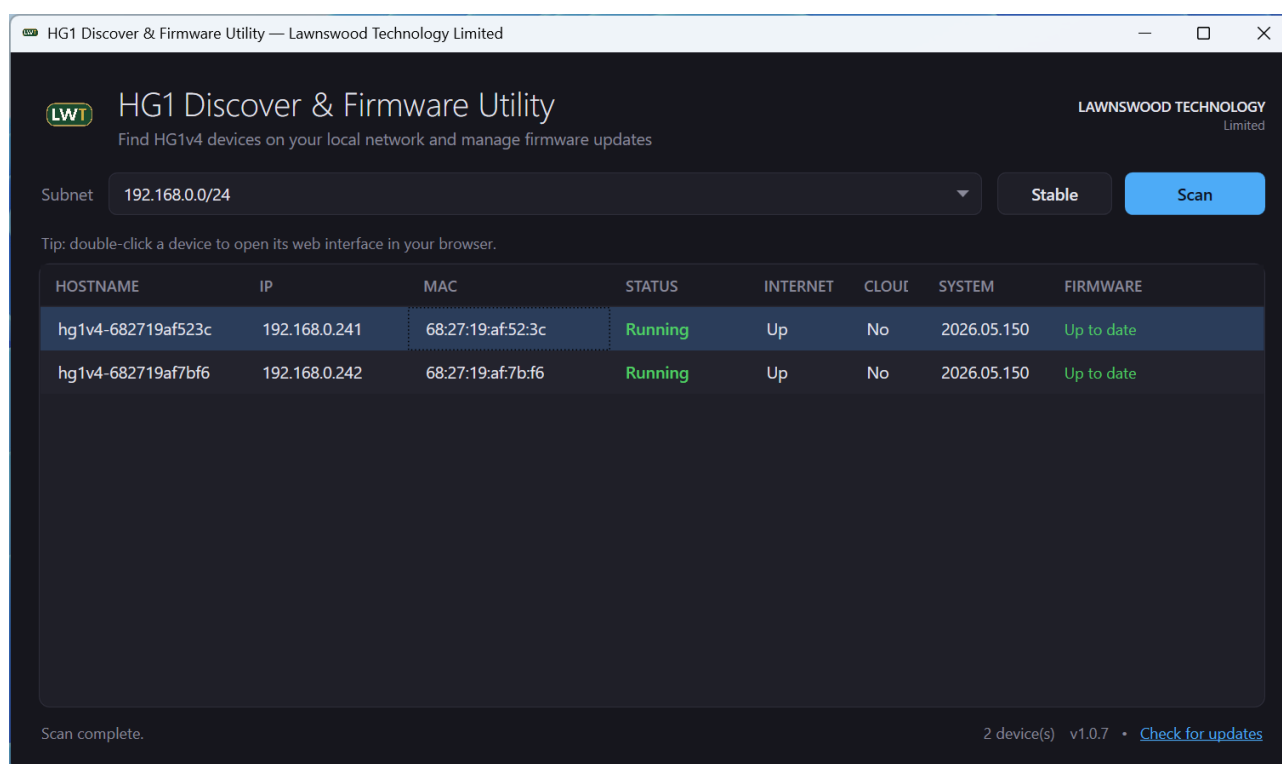
For day-to-day monitoring on a customer site, hand operators the **oper** password — they can see the gateway's state without being able to change anything by accident. Reserve **engr** for site engineering staff and the original installer.

The two passwords are independent. Rotate them separately when staff change.

PC Software

Day-to-day configuration and monitoring is done from the on-device web interface — no PC software is required. Two optional Windows applications are available from <https://support.lawnswoodtechnology.com> for situations the web interface does not cover.

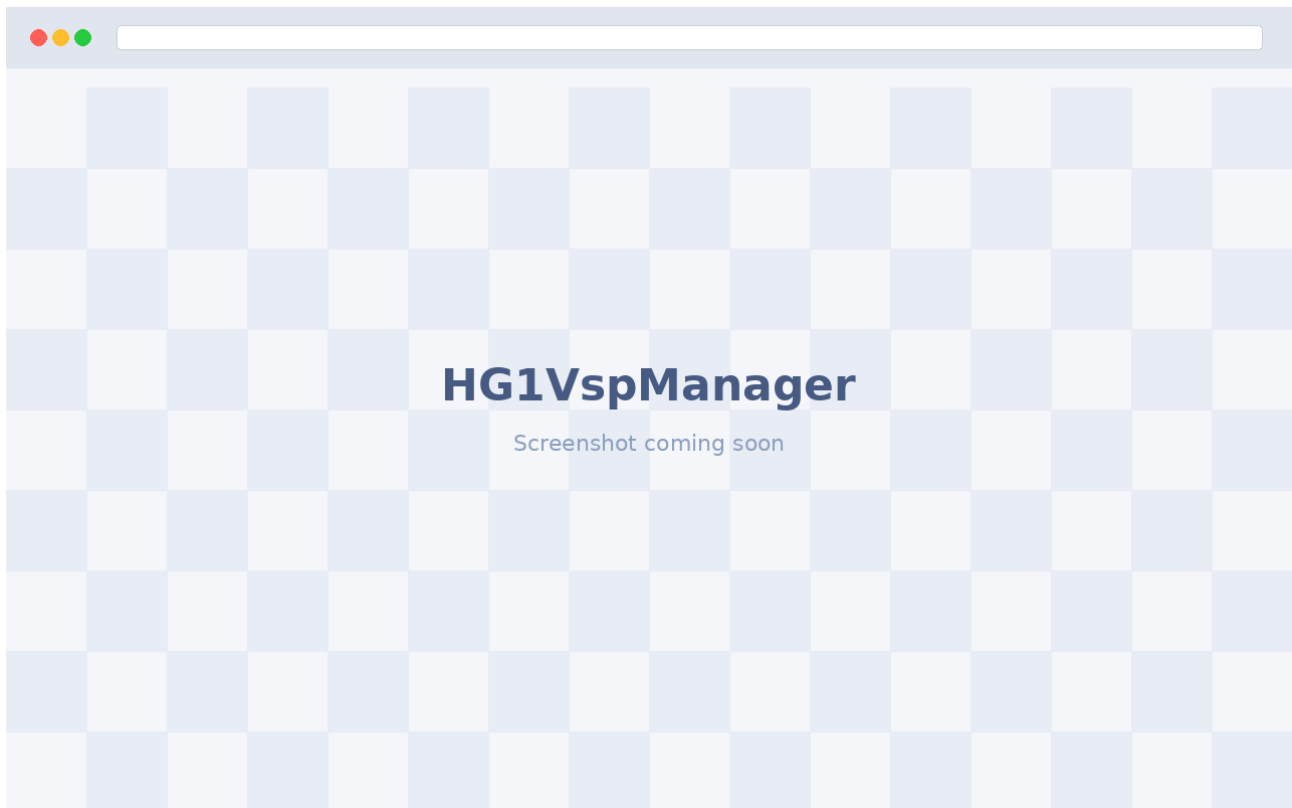
HG1Discover



Finds gateways on your network and pushes firmware updates to them locally.

- **Network discovery** — broadcasts a discovery packet on the LAN and lists every HG1v4 it can see, with current IP, hostname and firmware version. Useful when you cannot consult the router's DHCP table, or when mDNS is unreliable on your network.
- **Off-network firmware updates** — pushes a `.swu` firmware file to a gateway over the local network. Use this when the gateway has no internet access and so cannot use the on-device System Update modal.

HG1VspManager



Creates a Windows **virtual COM port** that tunnels to the gateway's HART modem over Ethernet. Asset-management software running on the PC — PACTware, FieldCare, RadarMaster, ProComm, etc. — sees it as a normal local serial port and can talk to the HART loop without a physical HART modem on the PC.

Use HG1VspManager when:

- You want to use existing PC-based DTM software with a remote loop.
- You do not have a USB HART modem to hand, or it is not practical to bring one to the gateway.
- You want a single PC to drive several gateways across the site (each one mapped to its own virtual COM port).

The gateway side of this is the **VCP / Pass-through** function on the **Configuration** page, with the network port configured under **Network Ports** (default 4001). HG1VspManager points at that address; Windows then sees a new COM port number that the asset-management tool opens like any other.

Troubleshooting

This chapter groups the most common issues by symptom. Every check listed here can be made from the gateway's front panel or the web interface — no shell access, no PC utilities beyond a browser.

Power and boot

PWR LED off. Check the 24 V DC supply is connected and turned on; check the polarity of the 24V / 0V terminals; check any inline fuse. A regulated 24 V supply within its rated range should light PWR the instant power is applied.

PWR on, RUN LED stays off after 30 seconds. The firmware has not booted. Power-cycle once. If RUN still does not come solid green, raise a support ticket — include the gateway's serial number and hostname if you know them.

RUN LED blinking. A start-up failure has been detected. Note the blink pattern if visible and raise a support ticket.

Reaching the web interface

Cannot reach the web UI on a managed LAN. Confirm the gateway has a DHCP lease (check the router's connected-clients table for a hg1v4- hostname). Try the HG1Discover Windows utility (see PC Software) which broadcasts on the LAN and lists every gateway it finds. Clear the browser's DNS / redirect cache if the address recently changed. If your network policy blocks direct HTTP to devices, use a direct Ethernet link-local connection.

Cannot reach the web UI on a direct Ethernet connection. Set the PC adapter to "obtain an IP automatically" and confirm it has picked up a 169.254.x.x link-local address. Browse to http://169.254.100.1 — the URL must be http://, not https://. Some corporate laptops block link-local; a personal laptop or phone hot-spot is a fast workaround.

Browser shows a TLS certificate warning. You have typed https:// — the on-device interface uses plain HTTP. Type http:// explicitly. HTTPS is used only for remote access via <hostname>.lwtdevices.cloud.

HART communication

No HART devices found on Scan Devices (Gateway mode). Check loop wiring polarity and the 250 Ω minimum loop resistance (see HART Loop Connection). Confirm the transmitter is powered and its HART poll address is inside 0–15. If a hand-held configurator or DCS is also active on the loop, one master must be Secondary — set the HG1v4 to Secondary on the Configuration page's HART Master setting.

HART comms errors on a working configuration. Check the shield is grounded at one end only, that the loop cable is twisted-pair, and that the loop resistance is within spec. Long or noisy loops sometimes need higher loop resistance (up to 500 Ω) for reliable HART.

Configuration Save / Build / Deploy

Configuration Build fails. Read the error banner at the top of the page — it names the offending field. Common causes: duplicate slot numbers, an invalid device name (letters, digits, underscore, dot only — no hyphens), or engineering units the configured device does not support. Fix the field and click Build again. An unsuccessful Build never affects the running configuration.

Deploy succeeds but the gateway misbehaves after restart. Check the Restart Counter on the home page's System panel — a rapidly rising count means the application is crashing. Export the configuration (Configuration → **Export**) and attach the backup to a support ticket.

System Update

Check Now reports "up to date" but you expected a newer release. Confirm the Internet status dot in the page header is green. If a release was promised but is not showing, your device may be on the Stable channel while the release is still on Beta — contact support to move your device between channels.

Install starts, then stalls or fails. Usually caused by an unstable internet connection. The A/B partition scheme means a failed install cannot brick the gateway — the running firmware is untouched, and the update rolls back automatically. Retry when the connection is stable.

Remote access

Cloud dot shows Disconnected. Remote access is enabled but the gateway cannot reach the tunnel service. Check the Internet dot is also green — no internet means no tunnel. If your site restricts outbound HTTPS to a whitelist, ask IT to allow outbound HTTPS to the tunnel service (contact support for the firewall entries to add). After any network change, toggle Remote Access off and on again from the home-page dialog to force a reconnect.

Basic-auth prompt at `<hostname>.lwtdevices.cloud` rejects the password. The password shown at first Enable is displayed once and cannot be retrieved later. Regenerate it from the Remote Access dialog on the LAN side — the new password appears immediately and the old one stops working.

KFD2 multiplexor

Scan Devices in MUX mode returns an empty list. Check RS-485 wiring between the HG1v4 `TX+` / `TX-` terminals and the KFD2's serial input. Confirm the KFD2 is powered (the 14-pin power-rail ribbon between KFD2 modules must be seated). If the KFD2 has not yet scanned its own loops, click Rebuild & Scan rather than Scan Devices — this asks the KFD2 to physically re-scan and can take several minutes.

A field transmitter shows COMM in the device status column. The KFD2 is not receiving a valid response from that transmitter. Check the transmitter's loop wiring on the KFD2 termination board, and its HART poll address. On a re-scan the transmitter should return with a green status.

Modbus

Modbus TCP client times out or connection is refused. Confirm the client is pointed at the correct IP and port (default 502; check the Network Ports section of the Configuration page). Confirm the register range and function code — the map lists Holding vs Input registers per row. If you are polling during a Deploy or Save-to-Modbus-Map, expect a 2–3 second gap while the application restarts; configure your client with a 5-second retry timeout.

Values look wrong (byte-swapped). Try changing Float Swap Mode on the Configuration page. Different SCADA / DCS vendors default to different byte / word orderings; the correct choice depends on your client.

Raising a support ticket

If none of the checks above resolve the issue, raise a ticket at <https://support.lawnswoodtechnology.com> and include:

- The gateway's hostname and firmware version (visible in the page header).
- The Restart Counter value from the home page.
- An exported configuration backup (Configuration → **Export**) — useful for any HART or Modbus-map question.
- A short description of what you expected vs what you observed.

Glossary

Short definitions of the terms used throughout the manual.

- **A/B partitions** — the gateway's two-slot firmware layout. Updates are written to the standby slot and activated on reboot, with automatic rollback on boot failure.
- **Build** — second step of the configuration workflow. Compiles your edits into the runtime configuration.
- **Burst mode** — a HART feature where a transmitter periodically broadcasts its variables without being polled.
- **Deferment mode** — controls how the gateway queues HART commands under load (None / Partial / Full).
- **Deploy** — third step of the configuration workflow. Activates the runtime configuration; the application restarts.
- **DTM** — Device Type Manager. A vendor-supplied software module that knows how to commission a particular transmitter.
- **engr / oper** — the two access roles (engineering / operator). See Roles & Access Control.
- **FIM** — Field Instrument Manager. Generic term for asset-management software like PACTware or FieldCare.
- **HART** — Highway Addressable Remote Transducer. A digital protocol that rides on top of the 4–20 mA analogue signal.
- **HART-IP** — HART over Ethernet, defined by the HART Communication Foundation.
- **HG1Discover** — Windows utility for finding gateways on the network and pushing `.swu` firmware files to gateways without internet access. See PC Software.
- **HG1VspManager** — Windows utility that creates a virtual COM port pointing at a gateway's VCP / Pass-through service, so PC asset-management software sees the gateway's HART loop as a local serial port. See PC Software.
- **KFD2-HMM-16** — Pepperl+Fuchs HART multiplexor. Lets the HG1v4 address up to 16 field transmitters across the KFD2's channel bank via RS-485.
- **Link-local address** — `169.254.100.1` on the gateway. Always present, used as a fallback when no DHCP lease is available.
- **Long Tag** — 32-character device tag introduced in HART revision 6. Older transmitters (HART 5) only support the 8-character Tag.
- **MUX mode** — gateway operating mode where the device acts as a HART master for a KFD2 multiplexor.
- **PV / SV / TV / QV** — Primary, Secondary, Tertiary, Quaternary Variable — the four dynamic variables a HART transmitter can report.

- **Remote access tunnel** — outbound-initiated TLS tunnel that gives the gateway a public address at `<hostname>.lwtdevices.cloud` without requiring inbound port-forwarding. Enabled and disabled from the home-page **Remote Access** dialog.
- **Save** — first step of the configuration workflow. Writes pending edits to disk without activating them.
- **SWU** — software update file format used by the gateway's update system.
- **URV / LRV** — Upper / Lower Range Value. The PV values that map to 20 mA and 4 mA on the loop.
- **VCP** — Virtual COM Port. The gateway can expose its serial port over TCP so PC software sees it as a remote COM port.

Support & Contact

Per-page help (the ? button at the top of every page on the gateway) covers each part of the web interface in detail. The documentation set is shipped with the firmware so it always matches the version you are running.

For additional product documentation and technical support:

- **Datasheet:** <https://downloads.lawnswoodtechnology.com/hg1v4/HG1v4-Datasheet.pdf>
- **Quick Start Guide:** <https://downloads.lawnswoodtechnology.com/hg1v4/HG1v4-QuickStart.pdf>
- **Support site:** <https://support.lawnswoodtechnology.com>
- **Downloads:** <https://downloads.lawnswoodtechnology.com>
- **Manufacturer:** Lawnswood Technology Limited

When raising a support ticket please include:

- Gateway hostname and firmware version (visible in the page header).
- The Restart Counter from the home page if you suspect a stability problem.
- An exported configuration backup (Configuration page → **Export**) for any commissioning or HART-loop questions.
- A short description of what you expected vs what you observed.