

From first setup to your MQTT integration.

A practical manual for LRS firmware and FieldOps Control v0.20.3.

Updated 20 October 2026 Local / offline Control release

Getting started

An LRS extends a dry-contact control signal over LoRa. One LRS is configured as the gateway; the others are remotes. The gateway is the same board, with a different configuration. Wi-Fi is optional for LoRa control and is used for MQTT integration, network logs and firmware downloads. Only the gateway connects to MQTT; it represents its remotes on the broker.

Use the onboard relay to switch a suitably rated relay or contactor coil. We do not recommend switching the load itself directly with the onboard relay.

Choose how the installation is controlled

Control source	Use it for	What owns relay commands
Gateway input	Extend a float switch, contact closure or other dry contact across the site	The gateway's input drives its paired remote relays.
MQTT	Integrate with Node-RED, an automation controller or an existing MQTT system	Non-retained MQTT relay commands.
FieldOps Automate	Run sensor or contact rules without a running desktop or Internet connection	Rules saved on the gateway.

Select one source in Device settings → Control. MQTT can remain connected for viewing and configuration in all three modes, but ordinary MQTT relay commands work only in MQTT control mode. There is no separate standalone operating mode.

What to have ready

Use matching regional LRS hardware and firmware, FieldOps Control, a USB data cable and a suitable supply for each board. For a networked installation, also have a 2.4 GHz Wi-Fi network and a local MQTT broker. Keep the site's Fleet Key and device admin credentials with the installation record.

The available firmware profiles are 433_za and 915_us. Flash the profile that matches the board and installation. Frequency is set by the firmware build; it is not a Wi-Fi channel setting.

First installation

1. Install FieldOps Control from Downloads. Connect the intended gateway by USB.
2. Open Flash, choose the USB port and use Read device info. Check the board's identity and firmware. If an update is needed, choose the matching regional release and Flash firmware. Keep Erase flash before write off for a normal update; erasing also removes stored setup.

3. Power the intended remote. Use the same regional firmware on both boards. For first setup, keep the boards close enough to verify communication before fitting them at the final locations.
4. Open Provision → Pair. Select USB Serial Gateway and the gateway's port, then Load Gateway. A factory device can be commissioned here; a device already configured as a remote must be changed/recommissioned before it can serve as the selected gateway.
5. Set Max remotes to 1 for this example. Generate a new site Fleet Key or enter the existing site's key. Copy it into the installation record. Use the gateway's admin password shown or required by Control.
6. Choose Provision. Control prepares the gateway, discovers powered factory remotes, assigns addresses and verifies the setup. Wait for Verified; a discovered device alone has not yet been commissioned. Scan prepares the gateway with the entered key and discovers remotes without commissioning those remotes.
7. Open Fleet. The gateway normally uses address 254; the first remote uses 1. Give the devices clear names such as Control panel and Borehole. Names are stored on the gateway and follow each board's physical chip ID.
8. Open the gateway's Device settings → Control, select Gateway input and Save config. With equipment safely isolated for the test, change the gateway dry-contact input and check the remote relay response in both states. Check command confirmation as well as the physical installation.

The gateway relay follows the group state only after every configured remote confirms the requested state, for both On and Off. An unconfirmed operation can leave some remote relays changed while the gateway relay remains unchanged. Do not treat the gateway relay as electrical feedback from the connected equipment.

Add MQTT

1. With the gateway still on USB, open Device settings → Network. Enter the Wi-Fi SSID and password, enable WiFi, then Save config. Reopen Device check to verify connection and IP address.
2. Open MQTT. Enter the broker's LAN hostname or IP address, port, topic root and broker credentials. The usual port is 1883 and the default root is `lora`.
3. For telemetry while retaining dry-contact control, enable the MQTT client and keep Control set to Gateway input. For relay commands from MQTT, select MQTT on Control; this also enables the client. Save config.
4. In your MQTT tool, subscribe to `lora/#` or your chosen root. Find the gateway's discovery and retained status topics. Publish relay commands non-retained using the MQTT API guide.
5. Control can also connect to the same broker: open Connections, select MQTT and configure the matching broker and topic root. This app connection is separate from the gateway's saved broker settings. Select the gateway and enter its admin password when prompted.

Current MQTT traffic is plaintext and has no TLS. Use a trusted, operator-managed LAN. Do not expose the broker port to the Internet. Broker credentials control access but do not encrypt the connection.

Control includes a Local MQTT Broker for isolated setup/testing. Selecting it in Connections starts an unauthenticated broker on port 1883, or a port you choose if 1883 is already used. The broker stops when Control exits. Use a continuously available site broker for an installation that must keep running without the laptop. When configuring the LRS, use the laptop's reachable LAN address, not `localhost`.

Give remotes Wi-Fi when needed

Provision → WiFi lets you scan, Save on Gateway and Send to Remotes. A remote does not need Wi-Fi for normal LoRa control or MQTT telemetry through its gateway. Enable it when you need that remote's network firmware downloads or temporary UDP logs. In Fleet, Remote Settings → WiFi can send credentials to one remote.

Control walkthrough

View or control	What to do there
Flash	Read USB identity, choose a regional release or local firmware file, flash one board or selected USB boards, and inspect the activity log.
Provision	Commission a gateway and factory remotes with a Fleet Key, then distribute optional Wi-Fi credentials.
Fleet	Inspect the gateway and configured remotes, rename devices, view relay/input and sensors, open remote settings, and perform supported service actions or firmware updates.
Logs	Capture USB or temporary network logs, focus one source or merge several, filter, copy or export JSONL.
Automate	Create, inspect and save rules that execute on the gateway.
Device settings cog	Open the selected device's configuration and Device check. Defaults to the Fleet gateway.
Connections	Choose USB, an existing MQTT broker or Control's local broker for the gateway session.

There is no separate Monitor tab in this release. USB monitoring is available in Flash's Activity log. Enable Start monitor when flash complete for immediate inspection after an update, or use Start monitor / Stop monitor in the activity panel. Logs is the dedicated multi-source diagnostic view.

Fleet: understand the readings

Fleet first reads the gateway's known membership and cache, then refreshes devices progressively. It does not need a manual scan each time. Relay/input values shown as `-` are unknown, not Off or Open. A Cached label or advancing Age means the reading is historical; a saved or retained value does not prove the remote is currently reachable.

Edit Name inline; Enter or leaving the field saves, Escape cancels, and blank clears the name. Use Flash LED to identify a physical board. An acknowledged LED request means the remote accepted it; it does not mean somebody observed the LED.

Read diagnostics requests a bounded memory/health pass; it is not continuous polling. Find remotes performs a deliberate same-key discovery and offers responsive candidates for individual adoption. Use Provision for factory-key devices. Remove from Gateway/Forget removes gateway membership without resetting the remote. Factory reset is a different action and should be chosen deliberately.

Firmware updates

USB updates belong in Flash. Network updates belong in Fleet. Fleet selects the regional profile reported by the gateway; Profile unavailable means it cannot safely select one. Update order follows the selected release's upgrade policy.

A remote firmware update needs the remote's Wi-Fi and reachability to Control's temporary firmware server. LoRa carries the request, not the firmware file. Control starts and stops that server automatically. Wait for the reboot and a fresh report of the target version; a sent command or completed HTTP transfer is not enough to confirm the device update. Keep the `.bin` and matching `.upgrade.json` together when using downloaded files.

Settings walkthrough

Open the top-right Device settings cog, or gateway Actions → Settings. Check the `lrs-...` ID before editing. The dialog defaults to Fleet's gateway and fetches settings when it opens. Change device exposes the target and USB/MQTT connection. Use Fleet gateway restores the default. Manual target choices last only for the current app session.

Fetch settings before editing. Save config applies changes; editing a field alone does not. Blank fetched secret fields mean preserve the existing secret. A tick beside a secret indicates that a value is stored, not that it has been revealed.

Device check

Read/refresh a direct status snapshot: relay, input, temperature, tank level and Wi-Fi state. Check receipt age and sensor states. Missing, faulted, disabled or stale measurements are different from a valid zero. Device-reported sample time may be unavailable even when status was received recently.

General

Field	Meaning
Role	Gateway sends control and manages the fleet. Remote receives through its configured controller.
Local addr	This board's LoRa address. Normal gateway 254; remotes 1-12. Each remote must be unique.
Controller addr	Remote-only: the gateway that owns this remote, normally 254. It must not equal the remote's local address.
Fleet key	Site's shared LoRa encryption/authentication passphrase. It is separate from the device admin password. Blank keeps the stored key.

Use Provision for first commissioning and Fleet for membership/readdressing workflows. Manually changing a board's role or address does not automatically update every gateway record. Changing a Fleet Key on only one side interrupts communication until both sides match.

Control

On gateways, select MQTT, Gateway input or FieldOps Automate. On remotes, configure the controller-loss failsafe instead.

Field	Guidance
Input sync sec / Enabled	In Gateway input mode, periodically repeat the gateway input command. Default 60 s; editable range 60-3600 s. Turning periodic sync off does not turn off input-change commands.
Retry window sec	How long the gateway retries an unconfirmed input command. Default 180 s; range 5-3600 s.
Remote failsafe Action	Hold last, Force off or Force on after controller silence. Choose to suit the equipment and test the result. Default Hold last.
Remote failsafe Timeout sec	Default 180 s; range 5-3600 s. Coordinate it with periodic input sync and the site's required response to link loss.

Changing modes changes who may command outputs. Saving the new mode confirms configuration, not completion of all resulting relay operations. When leaving Automate for MQTT, owned outputs use their configured fallback actions; missing remote outputs use their lease timeout. Entering Automate waits for fresh, qualified inputs.

Network

Field	Guidance
WiFi SSID / Scan WiFi	Select or type the site's 2.4 GHz SSID. Blank SSID means no Wi-Fi network.
New WiFi password	Blank keeps the stored password in this Device settings form.
WiFi Enabled	Enable the device's station networking. LoRa control does not require it.
Hostname	Blank uses the board's <code>lrs-...</code> identity.
TX power	Wi-Fi output power, not LoRa range control. Keep the regional default; the US profile limits it to 19.37 dBm (other profile maximum 20.5 dBm).
Channel	Wi-Fi scan filter: 0 means automatic; nonzero restricts connection to that channel. US channels 1-11; the other profile allows 1-13. Prefer 0 unless the site needs a fixed filter.
WiFi sleep	Wi-Fi power saving; separate from remote Power Save listen-only mode.
Static IP / IP address / Gateway / Subnet	Use DHCP unless the site's network plan requires fixed addressing. If enabled, enter an unused valid address, router and subnet.

Saving networking changes can restart the connection. Allow the board to settle, reconnect if needed, then Fetch settings or refresh Device check to confirm. The UI's Channel field is not a LoRa frequency/channel selector.

MQTT

Field	Guidance
MQTT host / port	Reachable site broker. Default port 1883.
Topic root	Prefix for discovery, state and commands. Default <code>lora</code> . API examples must use the same root.
MQTT client	Enable status publishing and administration. Automatically enabled while MQTT is the control source.
MQTT control	Shows the choice made on Control. It is not a second independent switch.
Background refresh	Optional low-priority remote relay/input refresh while Control is closed. Default off. Fresh reports suppress unnecessary polls; relay/input control takes priority.
Fleet cycle sec	Target time for one refresh cycle across the fleet, not an interval for every remote. Default 60 s; range 60-3600 s.
MQTT user / New MQTT password	Broker login. Blank replacement password preserves the stored value in Device settings.

Remote devices do not run MQTT clients. Their MQTT tab explains that the gateway publishes their state and forwards supported commands over LoRa. The gateway's broker/topic settings are distinct from Control's Connections settings.

Sensors

Enable installed DS18B20 temperature and/or the conditioned 4-20 mA tank sender. Both may operate alongside the separate dry-contact input. The current desktop form exposes enable switches; it does not provide a general sensor calibration editor.

The released tank implementation uses one A0/AIN measurement path, a current-to-voltage converter, 120 Ω conversion, 5000 mm range and 3553 mV board ADC calibration. A KIT0139-style sender requires the intended external loop supply and conditioning. Never connect an industrial current loop directly to AIN. A nominal 4-20 mA input yields roughly 480-2400 mV with the 120 Ω converter. Do not substitute a raw ADC count for millivolts.

The DS18B20 uses the board's fixed firmware pin assignment. CN1 GPIO0/GPIO2 are boot-sensitive and already serve LoRa/temperature and LED functions. SSD1306 and general I²C devices are not supported by the current deployed LRS firmware. Electrical experiments with separate sketches do not add those capabilities to this release.

System

Save config writes the configuration to the board. Reboot restarts it and clears live status in Control. Factory reset returns settings to defaults and reboots; Keep fleet key and Keep WiFi selectively preserve those parts of setup. Read the confirmation for the chosen target before proceeding.

An unchecked Keep WiFi clears both application credentials and the ESP8266 station profile. Remote Reset but keep in fleet preserves the Fleet Key, role, assigned address and controller, but does not itself preserve Wi-Fi. A full remote reset removes membership only after the reset is confirmed; an unconfirmed reset leaves a retry-safe warning.

Reference

Copy common USB admin examples and MQTT topics. USB serial is 115200 baud, 8N1; requests are one-line JSON prefixed `LRS:` and followed by a newline. The MQTT API section contains examples for normal integration. Retained `config/...` topics are a read-only snapshot; publishing there does not change device configuration.

Remote settings

Remote Actions → Settings uses the gateway to change supported settings over LoRa. It is different from the full local USB Device settings dialog.

Tab	Action
Sensors	Enable temperature and tank sensors; Apply Sensor Configuration stores them on the remote.
Power	Enable/Disable Power Save. LoRa command reception stays active; Wi-Fi, serial admin, OTA, UDP logging, LEDs and background sensor polling stop while Power Save is active.
WiFi	Send SSID and password to this remote. This sends replacement credentials: do not assume a blank password preserves the old value as it does in Device settings.
Security	Change the remote Fleet Key with explicit confirmation. It becomes unreachable on the old gateway key until both sides match.

Power Save is intended for remote listen-only use. It does not suit a source that must keep sampling sensors, provide local USB administration or perform network updates. Disable it through the gateway before maintenance. If LoRa recovery is impossible, local bootloader erase/reflash is the fallback; simply plugging in USB does not re-enable the sleeping firmware's serial admin.

Automate

1. In Connections, choose the commissioned gateway. Open Automate; installed rules load automatically.
2. Add rule and give it a clear name. Up to eight rules are available; each supports one to four conditions and one to four explicit relay outputs.
3. Choose each source device and measurement: dry-contact input, temperature or tank level. Enabled sensor configuration determines the available measurements.
4. For a contact choose OPEN/CLOSED. For a measurement choose Above, At least, Below or At most and a threshold in °C or mm. Hysteresis creates a dead band to prevent rapid switching near the threshold.
5. Qualify for is how long a true or false condition must persist. Maximum data age determines when a reading becomes unavailable. For remote sources, set Maximum data age to at least 180 s; remote sensors normally report about once per minute. Missing/stale data interrupts qualification.
6. Choose ANY (OR) or ALL (AND). ANY matches when at least one qualified condition is true. ALL matches when every condition is true; one qualified false condition makes it false. Otherwise, unresolved data may make the result unavailable.
7. Set each output's True, False and Fallback states. True/False are ON or OFF. Fallback may also be HOLD to retain the current state. Each relay may have only one enabled rule owner.
8. Save to gateway. Then select FieldOps Automate in Device settings → Control and save. Saving rules alone does not change the control source.
9. Verify fresh readings, qualification and command acknowledgements with safely isolated equipment. The installed gateway rules continue after closing Control and without Internet.

Example: a pump serving two tanks can use one ANY rule with a Below condition for each tank, True=ON and False=OFF. Choose thresholds, hysteresis and fallback for the actual plumbing and pump protection; this example does not replace those controls.

Rules wait for valid qualified readings after reboot or Resume; an unavailable reading does not immediately establish a startup state. The board's normal boot relay state is Off. Remote outputs use their fallback after 180 s without renewed automation control. Pausing stops renewals and lasts until Resume, reboot or a control-mode change; disabling and saving persists through reboot. Leaving the Automate tab does not stop rules. Actions across devices are not electrically verified or atomic; partial acknowledgements remain visible.

MQTT API

Applies to released LRS firmware **0.20.3**, MQTT administration contract revision **4**.

The Wi-Fi-connected LRS gateway connects to your MQTT broker. Remote LRS boards exchange control and sensor data with that gateway over LoRa; they do not run their own MQTT clients. Once the gateway is configured, Node-RED, MQTT Explorer or another MQTT client can read telemetry and operate it without keeping FieldOps Control open.

Connect and find your devices

Configure the gateway's broker host, port, credentials and topic root in FieldOps Control. The default topic root is `lora`; the usual broker port is `1883`. Use an installer-managed broker on a trusted LAN. Firmware 0.20.3 uses plaintext MQTT without TLS: broker passwords and the device admin password do not encrypt the connection. Do not expose its broker port to the public Internet. FieldOps Live/cloud service is outside this release's local MQTT workflow.

Subscribe to `lora/#` initially, or replace `lora` with your configured root. MQTT wildcard characters `+` and `#` are for subscriptions, not publish destinations. With FieldOps Control's embedded local broker, remove MQTT Explorer's default `sys/#` subscription if it causes connection trouble.

The following names are used below:

Name	Pattern	Fictional example
Root <code>R</code>	Configured <code>mqtt_topic_root</code>	<code>lora</code>
Gateway base <code>G</code>	<code>R/lrs-<gateway-chip-id></code>	<code>lora/lrs-00a1b2c3</code>
Peer base <code>P</code>	<code>G/peers/<NN>_lrs-<peer-chip-id></code>	<code>lora/lrs-00a1b2c3/peers/03_lrs-00112233</code>
Discovery	<code>R/discovery/lrs-<gateway-chip-id></code>	<code>lora/discovery/lrs-00a1b2c3</code>

Chip IDs are eight lowercase hexadecimal digits. `NN` is the remote's two-digit decimal LoRa address, normally `01-12`. The gateway is normally address `254` (`0xFE`). Discover the real chip-qualified peer path rather than copying the fictional IDs above. A custom root can contain several path segments. Discovery sits outside `G/#`, so subscribe separately to `R/discovery/#` if you need it.

Discovery is retained JSON containing `chip_id`, boolean `role_tx`, `addr`, firmware version/profile, Wi-Fi station details, uptime and build identity. The role field is `role_tx`, not `role`. Use your own MQTT client ID; do not reuse the gateway's `LRS-<chip-id>` client ID.

Relay commands

Select **MQTT** as the gateway's control mode before issuing relay commands. A connected MQTT client can publish telemetry while control is assigned to Gateway input or FieldOps Automate; broker connectivity alone does not grant relay control.

Publish with **QoS 0, Retain off**. The payload must be exactly one ASCII character, `1` for On or `0` for Off. Do not send JSON, `true`, `on`, a quoted JSON string, whitespace or a trailing newline.

Target	Publish topic	Payload
Gateway's own relay	G/set/relay	1 or 0
One remote	P/set/relay	1 or 0
All configured remotes	G/peers/all/set/relay	1 or 0

For example, to switch remote 3 on:

```
Topic: lora/lrs-00a1b2c3/peers/03_lrs-00112233/set/relay
Payload: 1
QoS: 0
Retain: false
```

The address-only shorthand `G/peers/03/set/relay` is also accepted. Both forms route by the numeric address; a chip suffix on the command path is not an identity check. Recheck gateway membership after commissioning or changing addresses.

Relay messages do not include an administrator password or caller request ID. Restrict broker publishing rights to authorised clients. Never retain a command or configure an MQTT birth/will message to operate a relay. Do not wire a wildcard state subscription straight back into command publishing.

The onboard relay should only switch the coil of a suitably rated external relay or contactor, not the equipment load directly.

Confirm the result

Subscribe before commanding. Gateway-local changes are read back on `G/relay`; they do not produce the remote command-result event. Remote and all-remotes operations report non-retained JSON on `G/event/cmd_result`:

```
{"address":255,"command_id":17,"outcome":"Confirmed"}
```

`address` is the remote's decimal address, or `255` for an all-remotes operation. `command_id` is generated by the gateway; it is not your MQTT packet ID or an administration request `id`.

Outcome	Interpretation
Confirmed	Firmware acknowledged the requested state; address <code>255</code> requires every configured remote to confirm.
Timeout	Required confirmation did not arrive. Some remotes may already have changed.
Mismatch	A remote reported a different relay state.
Superseded	A later command or configuration change replaced the operation.
Untracked	The gateway could not track the individual operation; it was not sent as an untracked command.
Unavailable	The operation could not start, for example during provisioning.

For all-remotes control, the gateway relay follows the requested On or Off state only after every configured remote confirms. A timeout can leave some remotes changed while the gateway relay remains at its previous state. A group command supersedes older pending individual commands.

A broker accepting a publication is not confirmation of remote action. Invalid payloads, a blocked control mode or an empty configured fleet can produce no result event. Events are not retained, so reconnecting cannot recover a missed result. Avoid competing command writers and keep one outstanding operation per target when interpreting results. An acknowledgement confirms firmware state, not electrical continuity or the connected equipment's physical operation.

Status and sensors

Firmware state is published as **retained QoS 0**. Except for JSON discovery and event/admin responses, values are individual text leaves. Parse `0` and `1` explicitly: the JavaScript string `"0"` is truthy.

Topic	Payload / units
G/availability	online; the retained MQTT last will is offline. This describes gateway MQTT presence, not every remote's health.
G/relay, P/relay	0 Off, 1 On.
G/input, P/input	0 Open, 1 Closed.
G/display_name, P/display_name	Optional configured name, up to 16 characters.
G/addr	Hexadecimal address with prefix, for example 0xFE.
P/addr_hex, P/addr_dec, P/chip_id	Address as unprefixed hex, padded decimal, and eight-digit chip ID.
P/ack_state	unknown, pending, ok, timeout, mismatch, untracked or superseded. Successful state is ok.
P/last_seen_age_s	Seconds since the gateway observed peer contact, measured when this leaf was published.
P/last_seen_ms	Peer receipt time in gateway milliseconds since boot; not UTC.
G/last_updated, G/uptime_ms, P/uptime_ms	Milliseconds since the relevant device boot; not wall-clock timestamps.
P/uplink_rssi_dbm	LoRa signal strength at the gateway, in dBm.
P/wifi_rssi_dbm	Remote Wi-Fi station signal strength, in dBm.
P/wifi, P/wifi_connected	Wi-Fi enabled / connected flags, 0 or 1; unknown values can be deleted. wifi is also a command leaf.
P/fw_version, P/ip	Cached remote firmware and station IP address.
G/heap_free, P/heap_free	Free heap, bytes.
G/heap_max_block, P/heap_max_block	Largest free allocation block, bytes.
G/heap_frag_pct, P/heap_frag_pct	Heap fragmentation, percent.
P/poll_state	pending or idle; not an actuator acknowledgement.

Topic	Payload / units
P/last_cmd_counter	Radio/control counter; not a caller request ID.
P/power_save_listen_only, P/power_save_active	0 / 1 power-save flags.

Sensor topics exist beneath either `G` or `P`; the current fixed sensor instance is `0`:

Sensor topic suffix	Meaning
sensor/input/0/value	Dry-contact value, 0 Open / 1 Closed.
sensor/temperature/0/value	Temperature in degrees Celsius, decimal text.
sensor/tank_level/0/level_mm	Calculated tank depth in whole millimetres.
sensor/tank_level/0/voltage_mv	Measured board-input voltage, integer millivolts.
sensor/tank_level/0/current_ma	Calculated sensor current, milliamps with two decimals.
sensor/<kind>/0/state	disabled, missing, fault, ok, overrange, waiting, Or unknown.

Read a value together with its state and freshness. A numeric value can be retained for `overrange`; other invalid states clear the generic value. Tank voltage/current may remain available during a low-current fault or overrange to aid diagnosis. These are diagnostic values for the configured tank conversion, not additional independent sensors. The remote supplies its own conversion resistance and full-scale range; the gateway does not substitute its settings.

An empty retained publication deletes a broker topic. It means the value is unavailable, not Off, Open, zero or disabled. Display unknown state as `-`. Retained delivery after a reconnect is cached evidence, not a new reading. Keep the receive time and age the value locally; `last_seen_age_s` is a snapshot, not a clock maintained by the broker.

The gateway attempts status publication about every ten seconds and discovery about every minute, but it does not obtain a new radio reading from every remote on each pass. With background refresh disabled, unchanged peer cache records may not be republished. Enable the optional background remote-state refresh only when you need operational MQTT data kept current with Control closed; its configured interval is a target whole-fleet cycle, not a per-peer guarantee.

Maintenance API

Use these when needed, not as an aggressive dashboard polling loop. Keep every request non-retained.

Publish topic	Payload and scope
G/poll_fleet	Zero-length payload selects the configured fleet; a decimal comma-separated list such as 1,3 selects configured addresses. Not JSON and not a discovery scan. Available with the MQTT client even outside MQTT relay-control mode.
P/poll_now	An explicit configured-peer poll; payload is ignored, so use 1. Requires MQTT control mode.
P/wifi	1 / 0 recommended. Also accepts case-insensitive on/off, enable/disable, enabled/disabled, true/false, or JSON {"enabled":true} / {"enabled":false}. Requires MQTT control mode.
P/forget	1 requests destructive removal from the gateway. 0 or empty does not remove. Requires MQTT control mode; use Control's confirmed Forget workflow for routine fleet management.

The `wifi` leaf serves both telemetry and commands. Do not replay retained telemetry as a new command. A refresh or Wi-Fi publication is not confirmation of relay operation.

Settings API

Settings requests go to `G/admin_command`; correlated JSON replies arrive on `G/admin_response`, non-retained. Subscribe before sending. Broker authentication, the LoRa Fleet Key and the gateway administrator password have different purposes; use the gateway's administrator password for privileged settings requests.

Read `G/config/#` first and retain it as the settings baseline. These are individual scalar text leaves or JSON arrays, not one JSON document. `config/_complete` is `false` during a publication pass and `true` after successful publication. Retained leaves can arrive out of order, including after that marker. Wait for the fields you require; the marker alone does not make the read atomic or prove a new save.

1. Establish an admin session

Publish this JSON, QoS 0 and Retain off:

```
{"id":"example-session-1","cmd":"admin_challenge"}
```

A successful reply has this shape; 123456 below is only an illustrative numeric placeholder:

```
{"cmd":"admin_challenge","id":"example-session-1","session_id":123456,"expires_in_ms":300000,"ok":true}
```

Use the actual returned numeric session ID. Sessions last five minutes and are lost on reboot. Only one MQTT admin session is active per gateway: another client's challenge replaces it. Coordinate admin writers, including FieldOps Control.

2. Send a small settings patch

For a gateway already connected to MQTT, this example selects MQTT relay control. Replace the fictional session ID and password privately:

```
{
  "id": "example-mode-1",
  "cmd": "set_config",
  "session_id": 123456,
  "seq": 1,
  "flasher_compat_revision": 4,
  "admin_password": "YOUR_GATEWAY_ADMIN_PASSWORD",
  "config": {
    "gateway_control_mode": "mqtt"
  }
}
```

The fields to change belong inside `config`. The top-level `admin_password` authenticates the command; a deliberate replacement belongs in `config/admin_password`. `flasher_compat_revision` is an administration contract revision, not the firmware version.

Mode values are `mqtt`, `input`, `automate`, and `none`. Send the mode without conflicting derived boolean flags. When switching from Gateway input to MQTT, the gateway releases paired-input authority without changing relay state, but handover across remotes must settle before relying on new control. Leaving Automate can apply the rules' configured fallback outputs. Selecting `input` can resume input-driven synchronization and is not a neutral read-only action.

Use a new request `id` and a higher `seq` for each command in the session, including retries after password or settings errors. A validated sequence is consumed before those checks. Start a new session after reboot, expiry or loss of sequence state; reconnecting the broker alone does not reset it.

3. Confirm persistence and read back

Match the response `id`. A successful mode-only save resembles:

```
{"cmd":"set_config","id":"example-mode-1","network_restarted":false,"rebooting":false,"ok":true}
```

`ok:true` confirms the gateway saved its settings. Afterwards confirm `config/gateway_control_mode` is `mqtt` in a completed readback. Changing control mode reconnects MQTT to change subscriptions even when `network_restarted` is `false`; that flag describes network settings, not every MQTT reconnect. A saved gateway setting is not proof that every remote completed handover or acted on a later relay command.

If the reply is missing, the save is uncertain. Read back before retrying; a lost reply is not proof the save failed.

Patch rules

- Send only fields changed from the baseline, not a complete settings document. Split larger changes into sequential patches and wait for each correlated result.
- Omit unchanged secrets. Blank Wi-Fi, MQTT, Fleet Key and administrator password replacements preserve the current value. Secret values are not retained; readback publishes metadata such as `mqtt_password_set`.
- The MQTT packet budget is 1,024 bytes including topic and protocol overhead. Keep JSON comfortably below this; FieldOps Control uses a conservative bounded patch budget. A long topic root reduces the available payload.
- Apply ordinary changes first. Group Wi-Fi, broker, topic-root, client-disable, control-mode and reboot-triggering changes into the final bounded patch because they can end the connection being used.
- Not every reported config field is writable. `schema_version` and `commissioned` are read-only; known fleet membership uses its separate management commands. Unknown/protected fields are rejected.

- Common settings include `gateway_control_mode`; `remote_refresh_enabled` / `remote_refresh_cycle_ms`; Wi-Fi and MQTT connection fields; temperature/tank enablement and intervals; and timing/failsafe settings. Names ending `_ms` use milliseconds; sensor intervals ending `_s` use seconds. Use the settings UI for validation and commissioning rather than inventing field names or values.

Publishing directly to `G/config/<field>` changes a broker message only; it does not apply or save the device setting and can mislead readers. Use authenticated `set_config`.

Retired topics and aliases

- `.../control` is removed. Use the exact `.../set/relay` topic.
- `.../relay` is reported state, not a command destination.
- `sensor/tank_level/0/value` is retired and explicitly cleared. Use `sensor/tank_level/0/level_mm`; temperature and input still use `value`.
- Peer `poll_interval_s` and `last_poll_tx_ms` are retired retained leaves and cleared. Use supported explicit refresh or configured background refresh.
- MQTT wildcard publishing, invented `role` discovery fields and invented whole-fleet status endpoints are not supported.
- Retired admin aliases such as top-level `command`, `request_id`, `password`, `addr`, `target_address`, `ssid`, `password_value`, `fleet_key`, `keep_fleet_key`, and `keep_wifi` are rejected. Use the canonical command contract.

MQTT Explorer and Node-RED

Check the broker in MQTT Explorer

1. Connect MQTT Explorer to the same LAN broker, port and credentials saved on the gateway. Use a unique client ID.
2. Subscribe to `lora/#`, replacing `lora` if you changed the topic root. Remove `$SYS/#` if it causes trouble with Control's embedded broker.
3. Find `lora/discovery/lrs-<gateway-chip-id>` and the gateway tree. Expand `peers` to discover the real chip-qualified remote paths.
4. Check `availability`, `last_seen_age_s`, `relay/input` and sensor state together. Opening an old retained tree does not refresh the physical device.
5. To test control, deliberately select MQTT in the gateway's Control settings first. Select the exact target's `set/relay` topic, choose QoS 0 and Retain off, and send the text `1` or `0`. Check the result event and observed state.

All identifiers in the following examples are fictional. Replace them with your gateway and configured remote.

Node-RED: command one remote

Create a manual Inject node, a Function node and an MQTT out node. Leave automatic startup and repeating Inject disabled while commissioning.

The Function node can prepare a command for remote 3:

```
msg.topic = "lora/lrs-00a1b2c3/peers/03_lrs-00112233/set/relay";
msg.payload = "1";           // Exactly one character; use "0" for Off.
msg.qos = 0;
msg.retain = false;
return msg;
```

Configure MQTT out for the correct broker, QoS 0 and Retain false. Use a blank fixed Topic if the node should take `msg.topic`. Use a separate manual Off action for "0".

Add MQTT in nodes for the target's `relay`, `ack_state` and the gateway's `event/cmd_result`, then connect them to Debug nodes. Parse the event payload as JSON. Keep command submission, firmware acknowledgement and physical equipment feedback separate in your flow.

Node-RED: read a temperature

Subscribe with MQTT in to:

```
lora/lrs-00a1b2c3/peers/03_lrs-00112233/sensor/temperature/0/value
```

A Function node can reject absent or non-numeric readings before using the value:

```
const raw = String(msg.payload).trim();
if (raw === "") return null; // Unknown/deleted is not zero.
const temperature = Number(raw);
if (!Number.isFinite(temperature)) return null;
msg.payload = temperature;
return msg;
```

Also subscribe to the matching `sensor/temperature/0/state`, `peer last_seen_age_s` and gateway `availability`. Your flow should check state and age before acting on a number. Tank depth follows the same approach with `sensor/tank_level/0/level_mm`; its units are millimetres.

Command-line examples

Read the tree:

```
mosquitto_sub -h BROKER_HOST -t 'lora/#' -v
```

Publish one non-retained remote command:

```
mosquitto_pub -h BROKER_HOST -q 0 \
  -t 'lora/lrs-00a1b2c3/peers/03_lrs-00112233/set/relay' -m '1'
```

These examples assume your client is already configured for the broker's access requirements. Do not add `-r`: it would retain the command.

Troubleshooting

Open gateway or remote Actions → View Logs for a focused session. USB gateway logs use the serial connection; network logs need Wi-Fi and temporary UDP forwarding. Use Stop forwarding when finished; merely leaving Logs does not stop capture. UDP is best-effort, so missing lines do not prove a failed device or command. Export a short relevant JSONL session for support, and remove credentials before sharing.

Symptom	Check first
USB board absent	USB data cable, correct port and board power. Close another app that owns the port. If Power Save is active, wake through the gateway before serial administration.
Remote missing or unconfirmed	Board power, matching regional firmware and Fleet Key, unique address/controller, and antenna/link. For new factory devices use Provision; for an existing same-key device use Find remotes.
Relay command rejected	Gateway's Control source. MQTT commands require MQTT mode; Automate owns its configured outputs.
MQTT connected but no fresh remote readings	Match topic root/gateway identity; inspect age and sensor state. Retained values are historical. Enable background refresh only if operational MQTT state must stay current with Control closed.
Broker will not connect	Gateway Wi-Fi/IP, correct broker LAN address and port, login/ACLs and topic root. A laptop broker must run and remain reachable.
Local broker port busy	Select an unused port in Connections and use that same port in the gateway.
Wi-Fi stopped after a save	Reconnect and Fetch settings after networking restarts. Check static addressing and channel filter.
Remote update will not start	Remote Full Power, Wi-Fi/IP, matching profile and release, and reachability to Control's firmware server. OTA bytes do not travel over LoRa.
Temperature/tank absent	Sensor enabled on the correct device, correct wiring/power/conditioning and reading state. Power Save suppresses normal sensor sampling.
Automate saved but inactive	Control must be FieldOps Automate; rule enabled, source/target identities correct, data fresh and qualified. A draft is not installed until saved.
Settings save interrupted	Reconnect and Fetch settings to see what was stored before retrying. A network/topic change can end the current session.

MQTT errors

Symptom	Check
Connected to MQTT but relays do not change	MQTT control mode, exact topic, one-byte payload, configured target, provisioning and the active control owner.
Only the gateway relay changes	<code>G/set/relay</code> is local. Use the peer or exact <code>peers/all/set/relay</code> path.
<code>admin_session_required</code> , <code>admin_session_invalid</code> , <code>admin_session_expired</code>	Establish a new session and stop competing admin clients from replacing it.
<code>admin_sequence_replay</code>	Increase <code>seq</code> ; a failed command may already have consumed its number.
<code>auth_failed</code>	Use the gateway administrator password, not the broker password or Fleet Key.
<code>control_busy</code>	Let the active control operation finish, then submit with a new sequence.
<code>flasher_update_required</code>	Match the installed release's protocol/client; do not raise the revision blindly.
<code>invalid_config</code> , <code>unsupported_field</code> , <code>security_write_restricted_over_mqtt</code> , <code>fleet_targets_managed_separately</code>	Check the nested config object, canonical spelling and field permissions.
<code>save_failed</code>	Persistence was not confirmed. Resolve the problem and read back.
Old values look healthy after reconnect	Retained state is cached; compare observation age and command confirmation.

Use one MQTT client per application with its own client ID, a restricted broker account, and permissions limited to the required namespace. Keep real credentials out of public examples, exported Node-RED flows and outgoing Debug nodes. Disable repeating/startup Inject actions while testing control flows.

Need help with a site?

Email sales@thanda.solar or [WhatsApp +27 83 779 7094](https://wa.me/9198737797094). Include the firmware version, selected gateway, device address and the exact error. Keep credentials out of screenshots and log exports.