YZW PRODUCT GUIDE / CUSTOMER EDITION

YZW300L / YZW900L

LoRaWAN Gateway Deployment and Device Activation Guide

Installation, activation, data exchange and troubleshooting

Install YZW300L / YZW900L, match region/channels, configure LNS forwarding, activate devices and verify the complete path using application uplinks and authorized downlinks.

Install
Antenna, power, channels

Connect LNS
Web entry, gateway online

Activate
Identity, keys, sessions

Verify
Data, diagnosis, acceptance

Combined deployment and activation guide with one contents list and continuous chapters.

English • V1.4 • 2026-11-05

Applicable models: YZW300L / YZW900L

Contents

Page numbers refer to this PDF. Select a chapter to open it; use Contents in the footer to return.

01 Choose the gateway role 3

02 Install, power and access the Web UI 3

03 Complete the installation worksheet 3

04 Set and save gateway forwarding 5

05 Match the region, sub-band and RF plan 6

06 Connect the LNS and verify gateway presence 9

- Open the local LNS from the gateway Web UI 9
- Use an external LNS 13

07 Verify the path from device to MQTT 14

- Message path: device, gateway, LNS and customer application 14
- Payload comparison: radio frames are not application MQTT data 15

08 Troubleshoot from the last successful stage 16

09 Gateway stage record and device configuration 16

10 Identify gateways and end devices 16

11 Gather device information 17

12 Create the device objects in the LNS 17

- Create profiles, applications and devices in the same tenant 17

13 OTAA: enter root keys and join 19

14 ABP: configure the session and preserve counters 19

15 Set class, intervals and operating policy 20

16 Send and verify an application uplink 20

17 Verify application MQTT and an authorized downlink 21

- Start with a non-actuating downlink test 21

18 Ongoing operation and troubleshooting 22

19 Acceptance record and support information 23

01 Choose the gateway role

This guide covers YZW300L and YZW900L, which share the LoRaWAN/LNS Web workflow. Follow one common procedure and use the model differences below for power and concentrator count.

Item	YZW300L	YZW900L
DC input	9–36 V DC	9–48 V DC; no PoE input
Concentrator	One SX1302, eight multi-SF channels	One SX1302 / eight channels as standard; a second concentrator is optional
Instances	Configure the one fitted concentrator	Configure a second instance only with a second fitted module

Shared data path: LoRaWAN device → concentrator gateway → Semtech UDP → local or external LNS → application MQTT/platform. Regions/sub-bands depend on ordered RF hardware and licensing. Running does not establish device activation or application receipt.

02 Install, power and access the Web UI

1. With power disconnected, connect a LoRaWAN antenna matched to the ordered band, then the fitted cellular and other antennas. Keep cellular/Wi-Fi antennas on their labeled connectors. Attach the LoRa antenna before any transmit test.
2. Apply DC within the model-specific range in Section 01, with the correct V+ / V− polarity after checking the label and supply output. Secure the terminals and check for voltage drop or loose contacts.
3. Connect the maintenance PC to the assigned management LAN and log in using the address and credentials in the label or delivery record. If the address was changed, consult the site record before resetting.
4. Configure the chosen wired, cellular or delivered Wi-Fi uplink. Check time, DNS, default route and server-name resolution. Web access establishes management connectivity only.
5. Record the current settings and site network, and save an available configuration backup. Avoid changing region, server and device credentials together on a live system.

03 Complete the installation worksheet

Record	Value / source
Hardware identity	Model, unit ID, number of fitted concentrators and gateway EUI.
Region and frequencies	Country, fitted RF band, antenna band, LNS region plan and any required sub-band.

Record	Value / source
Server	Local or external LNS; UDP receiver hostname/IP, uplink and downlink UDP ports.
Access	Web account and LNS tenant/account. Store keys separately from public acceptance records.
Test device	Actual DevEUI, activation mode, LoRaWAN version, class, payload specification and normal uplink interval.
Application output	Actual MQTT broker, TCP/TLS port, credentials, application ID, topic and payload encoding.

Gateway EUI and device DevEUI identify different things. Both commonly contain 16 hexadecimal characters, but belong in Gateways and Devices respectively. Equal length does not make them interchangeable.

04 Set and save gateway forwarding

Open Application → LoRaWAN. Read the actual gateway EUI and service state before editing the intended instance.

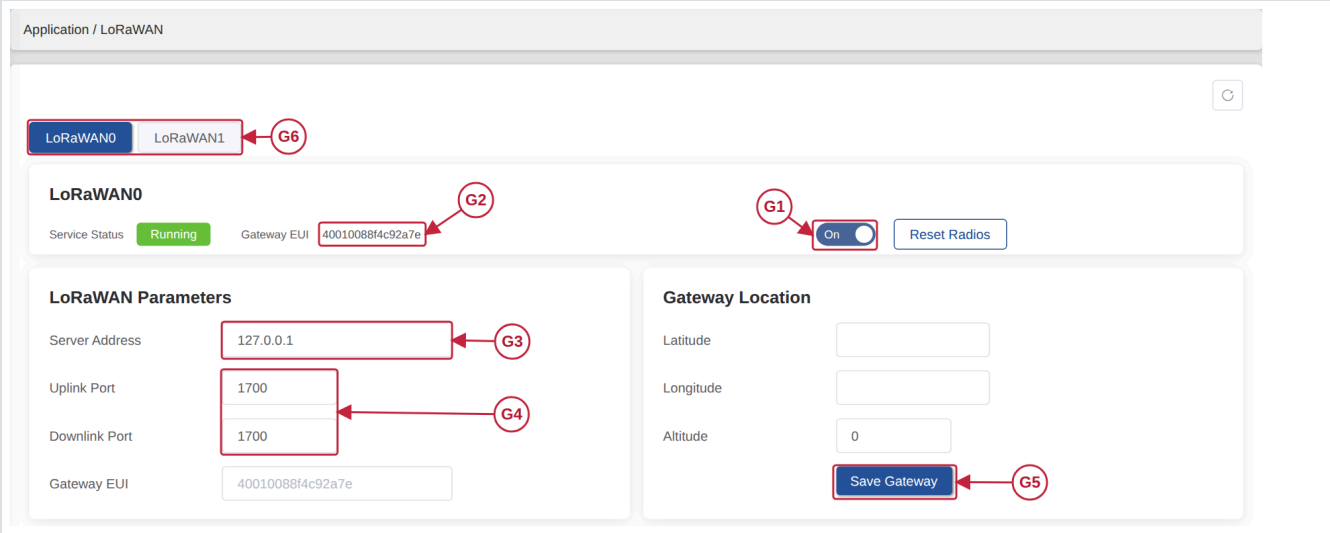


Figure 01. Native LoRaWAN forwarding and identity UI. Native same-platform YZW900L reference; 300L has one concentrator, while a second on 900L requires fitted optional hardware. Markers correspond to the table below.

Marker	Entry / action	Check the result
G1	Enable: enable the fitted concentrator instance and wait for the service state.	The local service shows Running; verify LNS presence separately.
G2	Gateway EUI: read the actual value and register the same unique value under LNS Gateways.	Both sides match; use the unit’s value, not the reference image.
G3	Server Address: local LNS reference 127.0.0.1; for external LNS enter its actual UDP receiving host, without a Web scheme/path.	After saving and refreshing, the destination matches the chosen local/external path.
G4	Uplink/Downlink Port: match the UDP receiver; replace the common 1700 example with actual service ports.	Ports read back correctly; MQTT/Web ports have not been used here.
G5	Save Gateway: save identity/forwarding for this instance; save radio settings separately at S3.	Observe success and refresh to check. Saving is not device-uplink acceptance.
G6	Instance tabs: one concentrator on 300L; configure a second on 900L only if optional hardware is fitted.	The selected tab maps to fitted hardware; each fitted instance uses its own correct EUI.

Enter the actual installed latitude, longitude and altitude. Region and antenna gain are identified by R1 and R4 in Figure 02.

1. Add the gateway under Gateways in the LNS. Select the tenant and region plan, and enter the displayed gateway EUI as Gateway ID.

2. Enter the forwarding host and uplink/downlink UDP ports on the unit, then check the EUI and enabled state.
3. Select Save Gateway. If radio settings have a separate Save Radio Settings button, save those too. Wait for success and refresh to confirm.
4. Observe the local service state and whether Last seen keeps updating in the LNS. If only the local service is running, check the receiving service and UDP path before changing device keys.

05 Match the region, sub-band and RF plan

Check in order: fitted RF module and antenna → permitted local region → gateway receive channels → LNS region plan → device region/channel mask → RX1/RX2 downlink settings. Receiving an uplink does not eliminate a downlink-plan mismatch.

For plans such as AU915/US915 that require a channel subset, obtain the actual region configuration ID, enabled channels and sub-band from the LNS administrator, then compare the device channel mask. Some systems number from zero and installers from one. Verify frequencies rather than inferring a mapping from “FSB2” or a suffix such as “_1”. An eight-channel concentrator does not simultaneously listen to every uplink channel in a full 915 MHz plan.

Mode	Correct use
Auto	Select a region template supported by both hardware and LNS. Save and compare the device channels. Keep the verified template unchanged for the first test.
Manual	Use only when the delivered UI exposes the fields and a complete RF plan is available. Record RF-chain centers, CH0–CH7 chain/IF assignments and standard LoRa/FSK settings. Do not bypass missing UI controls by writing configuration files.
Units	Use the displayed Hz, kHz or MHz units. Channel frequency = selected RF-chain center + IF; convert to the same unit first.
Transmit and downlink	Match transmit enable, RX2 frequency/data rate and the LNS downlink plan. A received JoinRequest is not proof that JoinAccept reached the device.

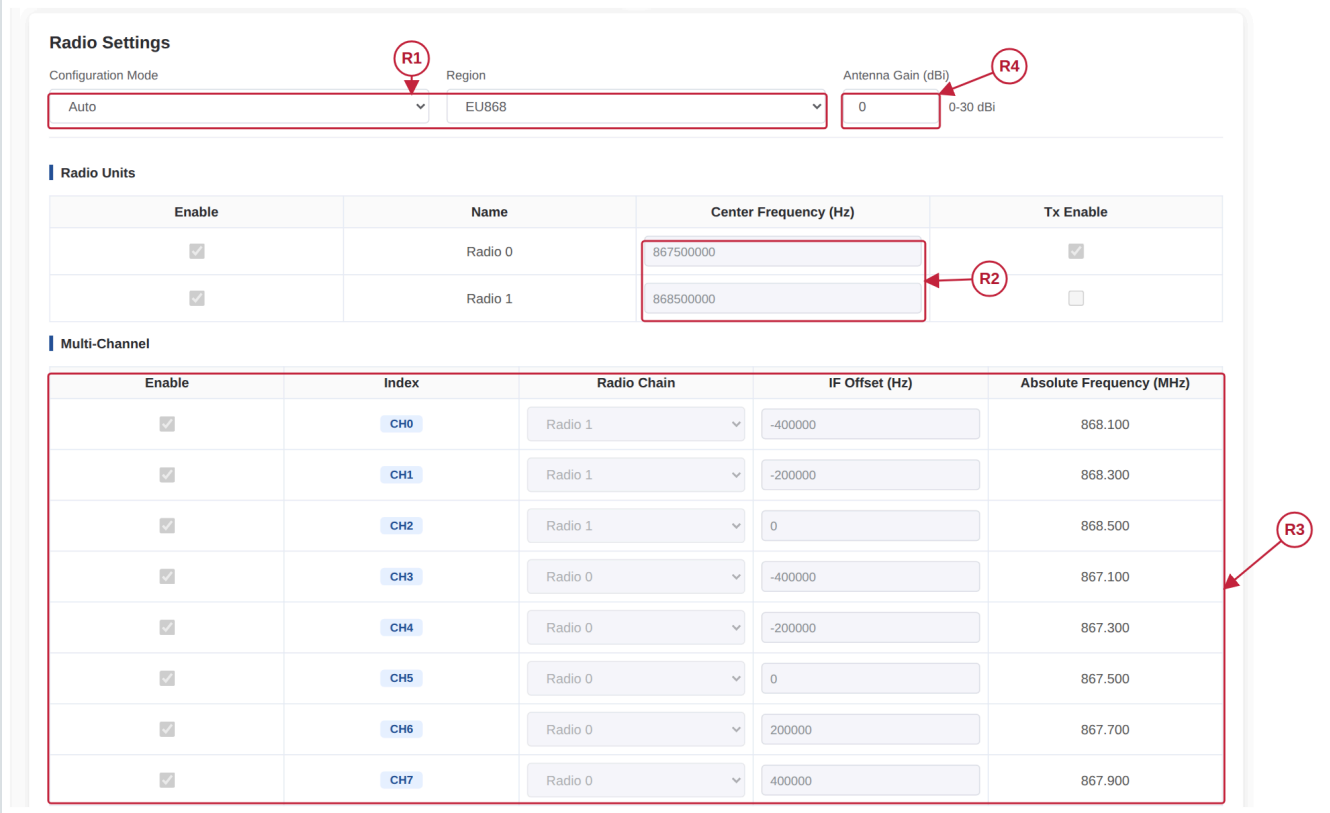


Figure 02. Native region, RF-chain and multi-channel detail. The displayed region locates the setting; it does not define every delivery variant. Markers correspond to the table below.

Marker	Entry / action	Check the result
R1	Mode/Region: start with a verified Auto regional template. Use Manual only with delivered controls and a complete plan.	The region matches ordered hardware, LNS and devices; do not copy the pictured region blindly.
R2	RF-chain centers: check units and TX enable against one plan. Preserve read-only Auto template values.	RF 0/1 are radio chains, not two concentrators; values match the plan.
R3	CH0–CH7: check enable, RF chain, IF and absolute frequency. Use common units for center + IF.	The actual receive channels match device channel masks/sub-bands.
R4	Antenna Gain: enter the installed antenna’ s actual dBi value and save using S3.	The value reads back correctly; increasing this value is not a way to obtain more TX power.

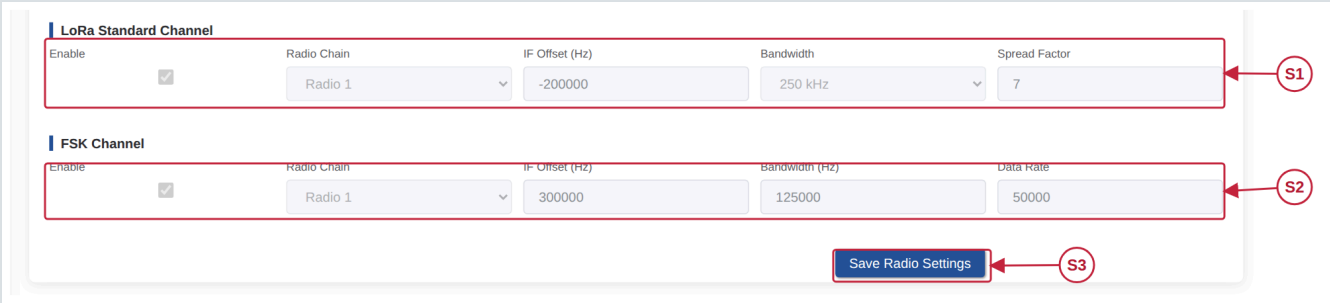


Figure 03. Native detail of standard LoRa, FSK and Save on the same radio page. Preserve the verified plan instead of overwriting site settings with the pictured values. Markers correspond to the table below.

Marker	Entry / action	Check the result
S1	Standard LoRa channel: check RF chain, IF, bandwidth and SF against the verified plan.	The settings match the plan; do not rewrite the template to match one device’ s SF.
S2	FSK channel: retain or apply the project-approved enable, IF, bandwidth and data rate.	The delivered plan is retained where no change is needed.
S3	Save Radio Settings: save changes to the region/radio parameters here.	Observe success and refresh; G5 still saves gateway forwarding parameters.

Configure one concentrator on YZW300L. YZW900L has one as standard and an optional second: verify antenna paths and unique EUIs, register each in the LNS, and save each instance’ s server, ports and plan. A tab does not prove fitted hardware; overlapping plans do not create 16 distinct frequencies.

06 Connect the LNS and verify gateway presence

Open the local LNS from the gateway Web UI

Local LNS path: log in to the gateway Web UI → Application → LNS Server → enable and verify Running → Open Console → ChirpStack login in a new tab → project tenant. The interface markers correspond to each figure’ s action table.

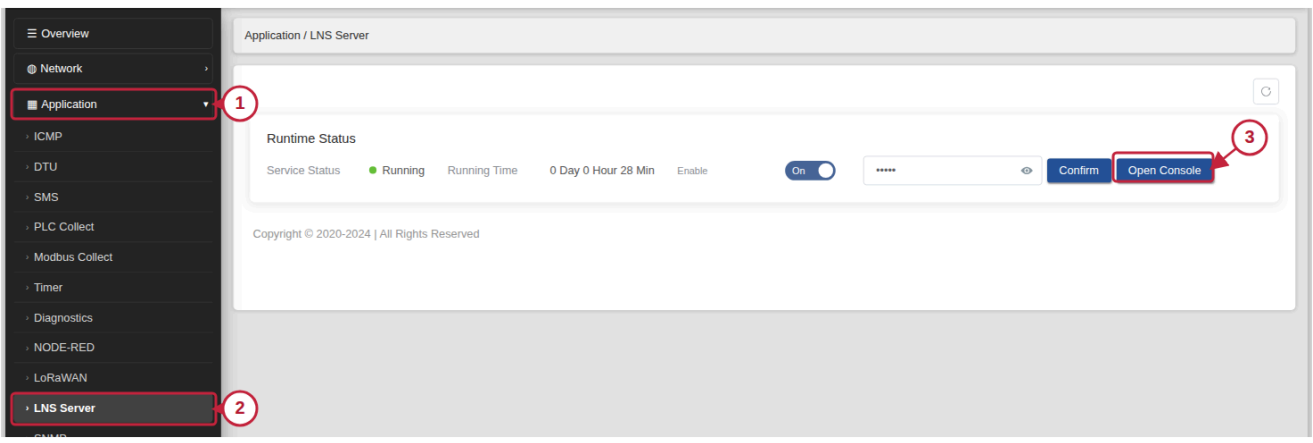


Figure 04. Web navigation and console button: 1 Application, 2 LNS Server, 3 Open Console. Historical native same-platform reference; labels are preserved, not recreated.

Marker	Entry / action	Check the result
1	Expand Application.	Application submenu entries appear.
2	Select LNS Server.	Runtime Status, service enable and Open Console appear.
3	Once available and running, select Open Console.	A new tab opens the local console; use the external Web URL for an external LNS.

1. Log in to the gateway Web UI using the delivered management address/account. The PC must reach the gateway management network. This is the device management login.
2. Expand 1 Application and select 2 LNS Server. The right panel should show Runtime Status and Open Console. Opening the LoRaWAN forwarding page does not open the LNS console.
3. In Figure 05, turn A Enable On and wait for B Service Status to show Running. If already running, leave it enabled. Opening the console does not require Confirm beside the password field.
4. Select 3 in Figure 04 or C Open Console in Figure 05. A new tab opens. If disabled, first check service state, availability and account permissions rather than repeatedly resetting the unit.

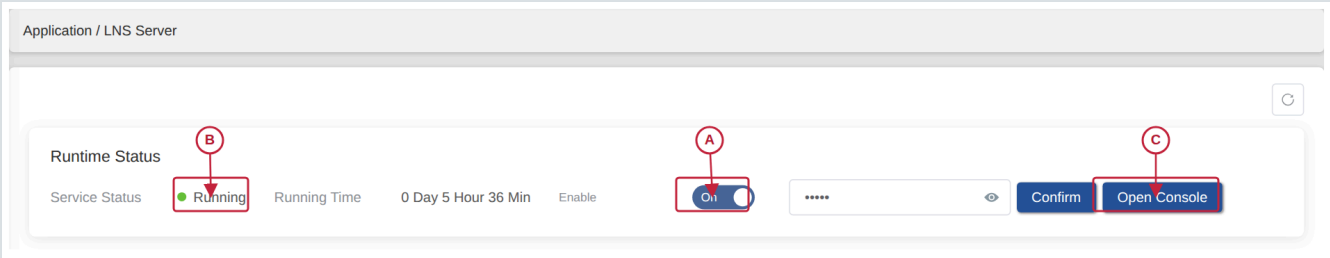


Figure 05. A service enable; B running state; C console entry. Confirm is an administrator-password action, not the console entry. The reference state is not a new site acceptance result.

Marker	Entry / action	Check the result
A	Turn Enable On; leave it enabled if already running.	Wait for the service state to settle.
B	Inspect Service Status.	Running establishes local service startup only.
C	Select Open Console; the adjacent Confirm handles administrator-password actions.	The ChirpStack login appears; Confirm is not required for navigation.

Open Console targets port 8080 on the current gateway host, for example `http://<GATEWAY_MANAGEMENT_IP>:8080`, using the protocol configured for the actual service. If the gateway is 192.168.10.1 and the console uses HTTP, the target is `http://192.168.10.1:8080`. This illustrates navigation, not a factory-default IP.

Do not enter 127.0.0.1 on the PC browser: that addresses the PC itself. In the gateway forwarding settings it addresses the gateway, a different use. The local forwarding reference is 127.0.0.1 with UDP 1700 for uplink/downlink, separate from browser TCP 8080.

Initial local LNS login: username admin; password admin. These credentials apply only to the local LNS while its initial credentials remain unchanged. Change the initial password after the first login. For a changed local account or an external LNS, use the current credentials supplied by its administrator. This is not a universal gateway Web or MQTT password.

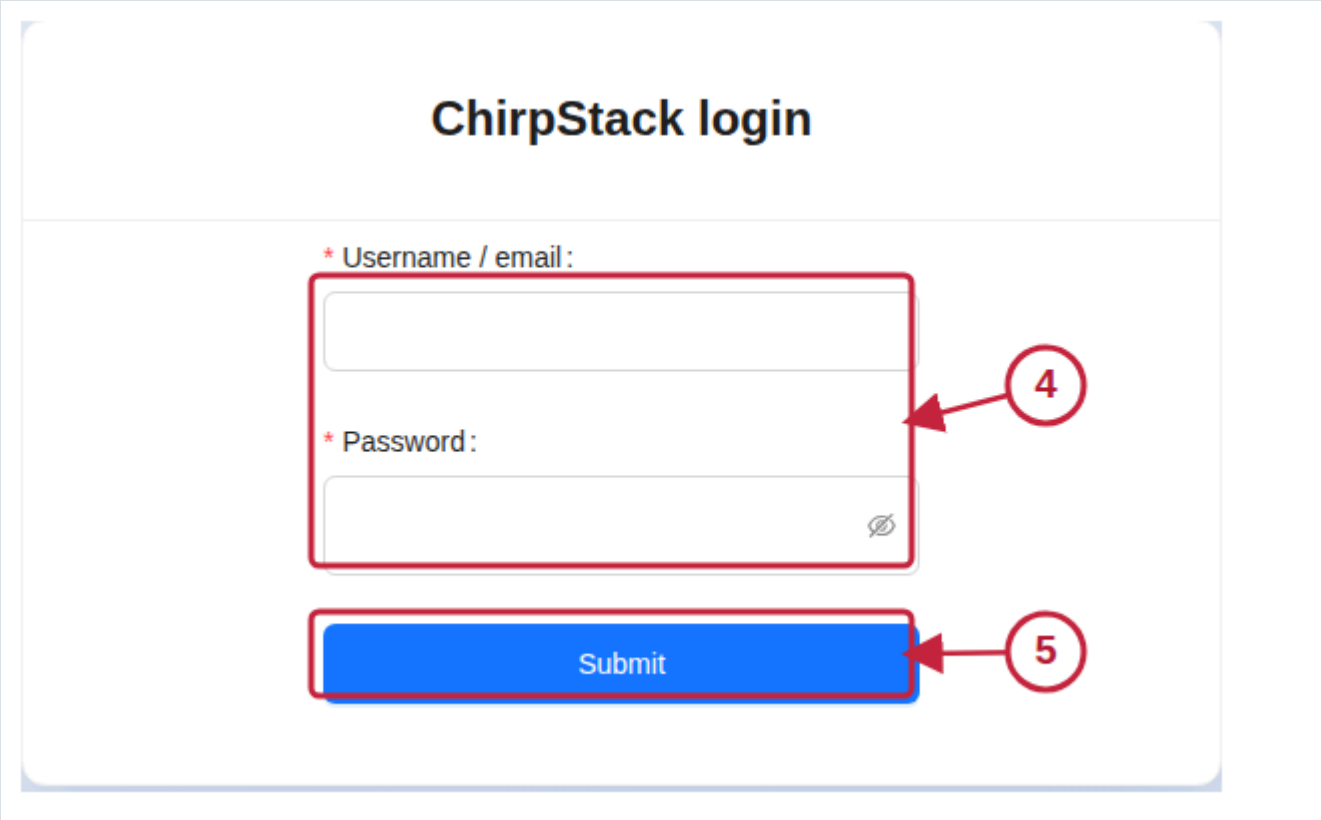


Figure 06. Native ChirpStack login reference after navigation. 4 LNS credentials; 5 Submit. Fields are blank. The gateway Web account is not automatically the LNS account.

Marker	Entry / action	Check the result
4	For the local LNS with unchanged initial credentials, enter username admin and password admin. Otherwise use the current account supplied by its administrator.	The account belongs to this LNS, rather than assuming the gateway Web account.
5	Select Submit.	Open an authorized project tenant, or check credentials/permissions if login fails.

1. At 4, enter the initial local LNS username admin and password admin, then select 5 Submit. If changed, use the current credentials in the delivery record or supplied by the administrator. This is the ChirpStack login, not the gateway Web account. Change the initial password after the first login.
2. After login, enter the project tenant through Tenants or the tenant selector as permitted by the account. Marker 6 in Figure 07 identifies the current tenant menu. Keep subsequent registrations in that tenant.

3. First register the gateway EUI under 7 Gateways. Then create a region/MAC-matched device profile under 8 Device Profiles. Finally use 9 Applications to open an application, create devices and enter keys.

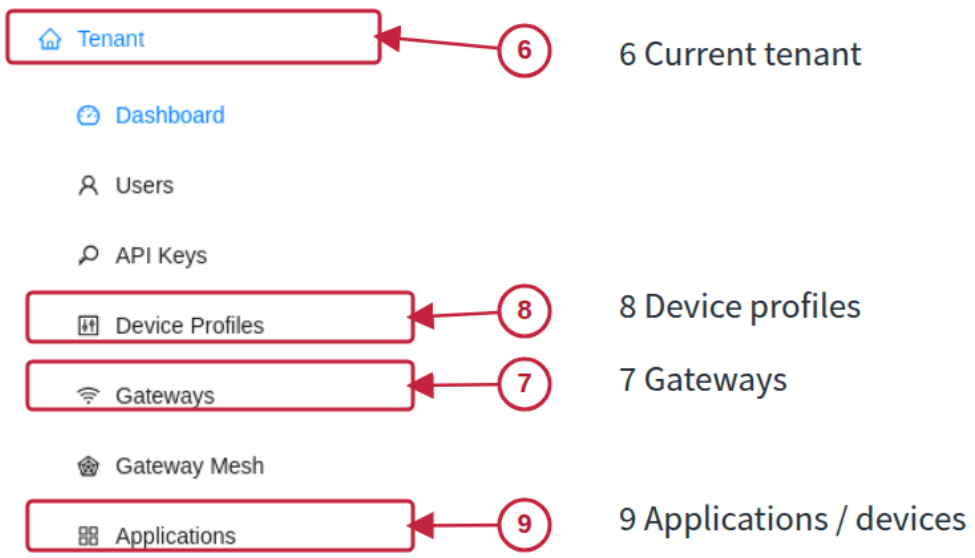


Figure 07. Native tenant menu detail after login: 6 tenant, 7 gateways, 8 device profiles, 9 applications/devices. The text at right is an annotation, not a translated UI.

Marker	Entry / action	Check the result
6	Confirm the project tenant before registering objects.	Gateways, applications and devices belong to the intended tenant.
7	Open Gateways and register/open the actual Gateway EUI.	Last seen and frame records belong to the intended gateway.
8	Open Device Profiles to select/create matching region, MAC and activation settings.	The profile matches the device’ s actual capabilities.
9	Open Applications and create/open the device in the project application.	Continue with device keys and application events on that device page.

Symptom	Next action
No new tab	Check the browser popup blocker. Allow a new tab for this management site or open the gateway host on port 8080 with the actual protocol.
New tab unreachable	Check gateway reachability, LNS Running, routing/firewall and the console protocol/listener. Device Web access does not prove access to 8080. Do not start with an upgrade or factory reset.
Login fails / no project menu	Verify the LNS account, password and tenant permission rather than changing gateway UDP ports. Have the project administrator handle account recovery.

Symptom	Next action
Using an external LNS	Open Console still targets the local console. It does not follow the LoRaWAN Server Address. Open the external LNS Web URL supplied by its administrator.

Use an external LNS

For customer-hosted ChirpStack, provide a Semtech UDP receiving component, such as a configured Gateway Bridge, which passes gateway traffic to the network server. A ChirpStack Web page or MQTT broker alone is insufficient; MQTT port 1883 is not the gateway UDP destination. Confirm protocol, region and downlink compatibility with a managed platform.

With cellular CGNAT, verify outbound UDP and its return path. Exposing the gateway Web interface is not a prerequisite. The public server, firewall or VPN route must carry the actual UDP traffic. A successful ping does not validate UDP reception or downlinks. Semtech UDP is not an encrypted tunnel; use a supported VPN when encrypted transport is required.

Browser entry for an external platform: open the full Web URL supplied by its administrator, rather than local Open Console. Sign in with the external LNS account and open the project tenant, then use Gateways, Device Profiles and Applications. Forward to its Semtech UDP receiver; do not enter a Web URL or MQTT 1883 in the UDP fields.

07 Verify the path from device to MQTT

Message path: device, gateway, LNS and customer application

Trigger one normal application uplink from a known device and follow that same message from left to right in Figure A. The five boxes are logical stages, not five required physical devices; several services may run on one gateway in a local deployment.



A LoRaWAN RF uplink
B Semtech UDP → receive/bridge layer → LNS; local reference: UDP 1700
C LNS application integration publishes to its configured MQTT broker
D Subscribe on that same broker/topic and match the same uplink

Figure A. Application uplink path. The receive/bridge layer is included in the gateway-to-LNS processing chain. MQTT here is the LNS application integration, not raw gateway frames or statistics topics.

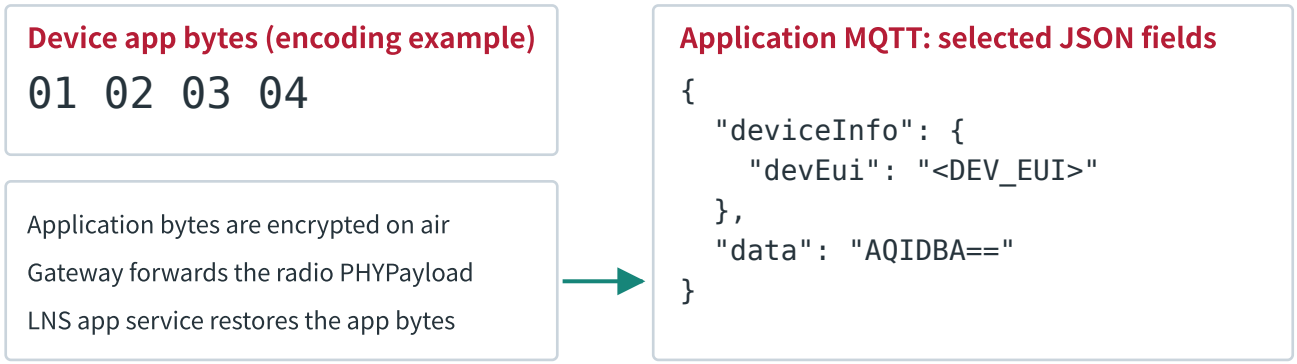
Stage	Evidence of success
1 Gateway service	Running with no persistent RF error. This establishes local service startup only.
2 Gateway at LNS	Last seen for the actual EUI updates and gateway statistics arrive.
3 Radio frame	Trigger a known device once and find the matching time, frequency and receive information in gateway frames.
4 Activation	For OTAA, inspect JoinRequest, JoinAccept and device state. For ABP, verify the active session and a valid application uplink.
5 Application event	Find up for the intended DevEUI in device Events/Data, with matching FPort, counter and payload.
6 Customer application	The application MQTT subscription or API integration receives that same event and decodes/displays it.

Local MQTT ports: the internal LNS broker uses TCP 1883. Configure the user MQTT Broker on another free port, for example 1884. These are separate services. A connection to 1884 does not prove that ChirpStack publishes there. Identify the broker used by the LNS integration and whether LAN client access is enabled on that broker.

Reference application uplink topic: `application/<APPLICATION_ID>/device/<DEV_EUI>/event/up`. Application ID is not JoinEUI. Gateway statistics and raw gateway frames are not application uplinks. Verify an LNS up event before application MQTT, using the actual topics and credentials.

Payload comparison: radio frames are not application MQTT data

Figure B illustrates only the encoding of application bytes 01 02 03 04 as Base64 AQIDBA==. It is not a site capture, measurement or instruction to transmit a test command. Read the actual FPort, frame counter, device identity and application meaning from the event and device protocol.



Application uplink topic (template)

`application/<APPLICATION_ID>/device/<DEV_EUI>/event/up`

Base64: AQIDBA== → 01 02 03 04; interpret bytes using the device protocol

Figure B. Selected fields from a ChirpStack JSON application uplink; other fields are omitted. Substitute the actual DEV_EUI. Gateway rxpk.data encodes the radio PHYPayload, so it must not be compared directly with application data.

1. Gateway frames: identify the new uplink by time, frequency and receive quality. A received RF frame does not establish correct keys, successful activation or decoded application data.
2. LNS device event: open the project tenant, then Applications > the application > Devices > the actual DevEUI > Events/Data and find up. Match DevEUI, event time, FPort, frame counter and data. Actual page labels depend on the delivered version.
3. Application MQTT: start the subscriber first, connect to the same broker used by the LNS integration, then trigger a new uplink. Match the received topic, DevEUI, time, FPort and frame counter against the same LNS up event. A TCP connection or gateway statistics alone is not a pass.
4. Decode: restore application data from Base64 to bytes, then apply the device vendor protocol. A configured matching codec may also produce object. Missing object does not necessarily mean missing data; AQIDBA== is not itself a temperature or another measurement.
5. Locate the break: gateway frame but no device up means check activation/session, keys and counters; up but no MQTT means check the integration target, listener/network/authentication, topic and permissions; MQTT with wrong values means check Base64, FPort, codec and device protocol.

> Keep the ports separate: local references use UDP 1700 for forwarding and TCP 8080 for the LNS Web UI. The internal LNS broker uses TCP 1883. A user broker, for example one configured on 1884, is a separate service and does not automatically receive LNS messages without an explicitly configured integration or bridge. Verify actual hosts, ports, TLS and permissions against the delivered configuration.

Diagram references: ChirpStack MQTT ChirpStack uplink events Semtech UDP / Gateway Bridge

08 Troubleshoot from the last successful stage

Symptom	First checks / next action
Stopped / not detected	Check power, fitted module, antenna and service errors before enabling again.
Running locally; offline at LNS	Check actual EUI, destination receiver, UDP ports, DNS/routes, firewall and LNS receiving component.
Online; no radio frames	Check that the known device transmits, then band/sub-band, antennas, placement and channel plan before changing AppKey.
JoinRequest; no activation	Check DevEUI, JoinEUI, keys and MAC version, then whether JoinAccept is generated and reaches the device on the correct downlink plan.
Radio frames; no application up	Check device registration, session, MIC/counter errors and regional configuration. Preserve the original error.
LNS has up; no MQTT	Check actual broker, listener/access, integration destination, topic, subscription timing and permissions. Resolve a refused TCP connection before inspecting event publication.
Queued downlink; not received	Check class, the next Class A uplink window, TX status, regional RX settings and device receive records. Queue acceptance is not execution success.

Reset Radios reinitializes concentrators. It is not a factory reset and does not correct a wrong region, key or LNS address. Save logs/settings and use a maintenance window. Confirm any interruption to another running concentrator before proceeding.

09 Gateway stage record and device configuration

Record the model, fitted concentrator count, Gateway EUI, region/sub-band, forwarding destination, external LNS URL or local console address, and last-seen time. Complete device activation and data-exchange evidence in the final acceptance in chapter 19. An online gateway alone does not pass device or application acceptance.

Continue with chapters 10–19 of this guide for device identity, OTAA/ABP, class, application uplinks, authorized downlinks and ongoing operation. No separate device guide is needed.

10 Identify gateways and end devices

YZW300L / YZW900L acts as the concentrator gateway and, when selected, the local LNS host. Sensors, meters and control devices are external LoRaWAN end devices. Set gateway region/forwarding in the gateway UI, set radio/device parameters in the device vendor’ s tool, and register device identities in ChirpStack or the customer LNS.

This guide does not use a gateway LoRaNode menu to configure external sensors. Console references preserve the native English ChirpStack fields so they can be matched on site.

Both models use this common device registration and verification procedure. Gateway instance registration reflects fitted hardware: one concentrator on YZW300L and an optional second on YZW900L. End-device registration is the same.

11 Gather device information

First complete the gateway deployment steps in chapters 01–09 of this guide and verify that the actual gateway EUI stays online at the LNS. Start with one known-good device before expanding the deployment.

Item	Actual value required
Region/channels	Device RF band, regional plan and channel mask/sub-band, matching gateway and LNS.
DevEUI	16 hexadecimal characters from the device label/tool, not Gateway EUI.
OTAA	JoinEUI/AppEUI (normally 16 hex characters) and AppKey (32 hex characters); confirm root-key requirements for the device LoRaWAN version.
ABP	DevAddr (8 hex characters), session keys, current counters, RX settings and session origin.
Protocol/operation	LoRaWAN MAC version, regional-parameters revision, Class A/C, power source, FPort, payload protocol and interval.
Management/application	LNS account/tenant, application name, decoder, MQTT destination and subscribe permission.

Hex lengths count characters, not bytes. Compare keys exactly and use the device/LNS format without reversing byte order on your own. Store and transfer real keys separately; keep them out of screenshots, group chats and public documents.

12 Create the device objects in the LNS

Open the console using the Web → local LNS steps in chapter 06, verify the gateway is online and select the same project tenant. For an external LNS use its administrator-provided URL. Continue below with device objects.

Create profiles, applications and devices in the same tenant

1. Open Tenant → Device Profiles → Add/Create. Set a name, actual region, LoRaWAN MAC version and regional-parameters revision. Enable Supports OTAA for OTAA, or use the matching ABP profile. Enable Class C only when the device supports and needs it.
2. Create an application under Applications → Add/Create. In its Devices → Add device, enter a name, actual Device EUI and Join EUI where requested, then select the matching Device profile.

3. Keep Device is disabled off. In normal operation, keep Disable frame-counter validation off; do not hide replay, session or power-loss counter problems by disabling validation. Select Submit.

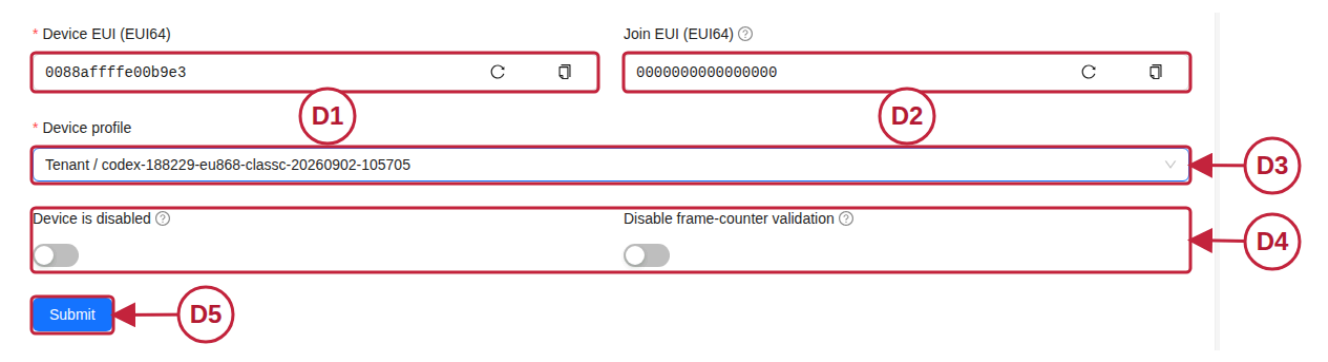


Figure 08. Native ChirpStack identity/profile fields. The historical laboratory EUI locates the field; do not reuse it for your installation. Markers correspond to the table below.

Marker	Entry / action	Check the result
D1	Device EUI: enter the actual 16-hex device DevEUI, not gateway EUI.	It matches the device label/tool rather than the laboratory example.
D2	Join EUI: for OTAA, use the device’ s actual JoinEUI/AppEUI.	It matches the device/LNS; the pictured zeros are not a universal value.
D3	Device profile: select a profile with matching region and MAC version.	Activation mode and class also match the device.
D4	Switches: normally keep both Device is disabled and Disable frame-counter validation off.	The device is enabled and frame-counter validation remains active.
D5	Submit: create the device record, then complete OTAA keys or Activation as appropriate.	The record is created; activation and an application up event still need verification.

Make the test profile match the device. An EU868 label does not justify selecting LoRaWAN 1.1 or Class C. MAC version, regional-parameters revision and RF hardware band are separate settings.

13 OTAA: enter root keys and join

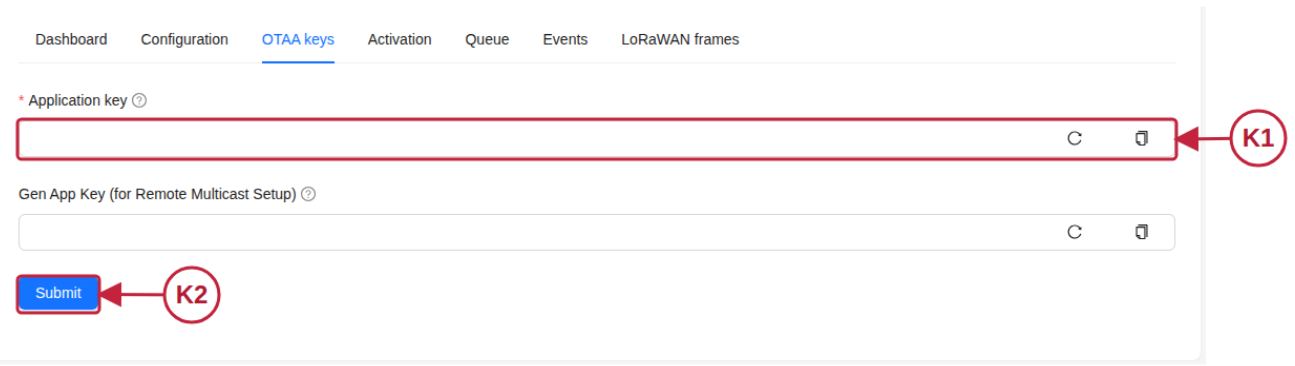


Figure 09. Native blank ChirpStack OTAA keys form, before entering keys. Application key is AppKey for the LoRaWAN 1.0.x example. Markers correspond to the table below.

Marker	Entry / action	Check the result
K1	Application key: enter the matching 32-hex AppKey here for this LoRaWAN 1.0.x example.	Use the actual key; blank/reference fields and other key rows are not defaults.
K2	Submit: save the root key, then trigger OTAA using the device's own procedure.	Check join and up events; saving a key does not establish activation.

1. Open OTAA keys, enter the actual device AppKey and select Submit. For LoRaWAN 1.1 devices, verify NwkKey/AppKey according to the device and profile. The illustrated 1.0.x form does not establish a single-key requirement for every version.
2. In the vendor device tool, match region, sub-band/channel mask, DevEUI, JoinEUI, AppKey, LoRaWAN version and class to the LNS. Save, then trigger Join or restart according to the device manual.
3. Inspect JoinRequest in gateway frames and the JoinAccept/join result in device events, then verify the device's own joined state. A server sending JoinAccept is not proof that the device received it.
4. Trigger a short application uplink and verify its up event, FPort, FCnt and payload. This completes activation plus application-uplink acceptance.

14 ABP: configure the session and preserve counters

ABP does not exchange OTAA JoinRequest/JoinAccept. Use it when the project requires ABP and complete session parameters are available. For a new installation, prefer OTAA when the device supports it.

1. Create the device with an ABP profile. In Activation or its equivalent, enter the actual DevAddr and session keys. LoRaWAN 1.0.x uses NwkSKey/AppSKey; other versions require their corresponding session fields.
2. Select ABP in the device tool and match DevAddr, session keys, region and RX parameters to the LNS.

3. Verify session continuity and uplink/downlink counters, then trigger an uplink and inspect up or any MIC/counter error. Do not reset live counters to “force joining”, and do not expect an ABP join event.

After power loss, an old backup or an LNS change, sessions/counters may diverge. Have the administrator verify recovery requirements. If a new session is needed, update both sides together and record it. Disabling frame-counter validation is not a long-term recovery method.

15 Set class, intervals and operating policy

Setting	Selection and cautions
Class A	Suitable for periodic reporting. Downlinks wait for receive windows after an uplink; do not assume immediate delivery.
Class C	Requires actual device support and suitable power. Match the device and LNS profile. Reception is still interrupted by activities such as transmission.
Uplink interval	Set it in the device’s supported controls. A one-off Send action does not create periodic acquisition where no interval control exists. Consider airtime, payload size, battery and regional limits.
ADR / data rate	Use only as supported by the device, LNS and delivered implementation. An LNS ADR option does not make a fixed-rate implementation adaptive.
Confirmed uplinks	Do not make every frequent report confirmed by default. Choose according to reliability needs and observe retries, downlink use and capacity.

After a region change, recheck device sub-band, LNS profile and RX settings. A gateway region change does not reconfigure external sensors. Validate one device first, then register unique DevEUIs from the deployment list.

16 Send and verify an application uplink

1. Trigger a normal report using the device vendor’s method and record the time. Use the real sensor payload; do not write arbitrary test control commands to the device.
2. Find the corresponding radio frame in gateway LoRaWAN frames, then verify up, DevEUI, FPort, FCnt and payload in device Events/Data. RSSI/SNR describe the link and do not replace successful decryption or application receipt.
3. If a test device supports custom uplinks, agree on fPort=10 and Hex=01020304 for a non-control connectivity test. Restore the actual business port/protocol afterwards.

Location	Representation of the same test payload
Device hex / raw bytes	01020304 (four bytes: 01 02 03 04).
MQTT JSON data	AQIDBA== (Base64), not corrupted text or a hexadecimal string.

Location	Representation of the same test payload
Decoded object	Produced by the configured decoder; a valid raw uplink can exist without a decoded object.

If application decoding is needed, configure Codec in the actual device profile according to the device protocol. This JavaScript only exposes the port and bytes; it does not infer temperature, switches or units and does not require Node.js.

```
function decodeUplink(input) {
  return {data: {fPort: input.fPort, bytes: input.bytes}};
}
```

17 Verify application MQTT and an authorized downlink

Connect the MQTT client to the broker actually used by the LNS integration. Verify host, TCP/TLS port, account, certificates and subscription permissions, then subscribe to the actual application uplink topic. Subscribe before triggering a fresh uplink; history may not be retained.

Reference uplink topic: `application/<APPLICATION_ID>/device/<DEV_EUI>/event/up`. Topic matching is case-sensitive; Application ID is not AppEUI/JoinEUI. Match DevEUI, FPort and raw payload before debugging the decoder.

Local services: TCP 1883 for the internal LNS broker and a user MQTT Broker, for example configured on 1884, are separate endpoints. A working 1884 connection does not locate ChirpStack publications. Check the LNS integration destination and that broker’ s listener/access. Working Web access does not establish LAN MQTT access.

Start with a non-actuating downlink test

1. Obtain the device protocol and test authorization, and ensure the payload cannot operate relays, valves or equipment. Without an approved test payload, observe normal downlinks rather than guessing a command.
2. In the device Queue, enter a supported FPort and payload using the format requested, Hex or Base64. Bytes 01020304 encode as AQIDBA==; use them only when the device protocol defines them as safe test data.
3. For Class A, trigger the next uplink and wait for its receive windows. For Class C, confirm the device is actually operating in that class. Observe the queue, LNS downlink/TX events and the device receive record.
4. Match the received payload in the device tool/log. If an application action is involved, verify the actual state and feedback separately. Gateway transmit success is not proof of device execution.

For MQTT downlinks, use the configured `application/<APPLICATION_ID>/device/<DEV_EUI>/command/down` topic and the LNS message schema, including devEui, fPort, confirmed and Base64 data. Validate a safe console-queue test before

integrating software. The uplink event/up topic is not a downlink entry.

18 Ongoing operation and troubleshooting

Symptom / action	Check and response
Gateway online; no device join	Look for JoinRequest first. No frame: check region/sub-band/RF. Frame present: check registration, keys and MAC, then JoinAccept delivery.
Joined; no up	Confirm an application transmission, then inspect FPort, counters, MIC, session and LNS errors. A join event is not application data.
up exists; platform empty	Check broker/topic/permissions, subscription timing and raw Base64 data before decoder fields and platform mappings.
Only some reports arrive	Record transmit time, actual frequency, SF/BW and reception. Check sub-band/channel mask, airtime and the site link.
ABP fails after power loss	Check session/counter continuity; do not permanently disable validation or repeatedly reset counters.
Class A downlink delayed	Check the receive windows following the next uplink. For lower latency, evaluate actual Class C support and power first.

Local ChirpStack tenants, devices and sessions belong to the service database, separate from a normal gateway configuration backup. Do not use ordinary upgrades or configuration factory reset as a database-erasure method. Before backup, migration or replacement, preserve both network configuration and LNS data and confirm database recovery with support.

19 Acceptance record and support information

Record one complete sequence: gateway online → device OTAA activation or valid ABP session → application up → MQTT/platform receipt → device receipt of an authorized downlink. Then observe normal reporting, recovery after restart and application feedback for the project’ s required period. One success does not establish long-term reliability.

Support evidence	Include
Context	Gateway and device models, region/sub-band, gateway EUI, DevEUI, MAC version, activation mode and class.
Matched evidence	Device state, gateway frames, LNS events, FPort/FCnt, payload and MQTT topic from the same period, including time zone.
Fault boundary	Last known-good time, last successful stage, changed fields and original error, with root/session keys and passwords excluded.

The combined acceptance record must include the model and fitted concentrator count, gateway EUI, region/sub-band, forwarding destination, test DevEUI, time, FPort/FCnt/payload of a valid uplink, device receipt of an authorized downlink, and data received by the application. For failure, retain the last successful stage and original error; do not submit root/session keys or passwords.

Product basis: the current YZW300L / YZW900L datasheet and user manual. Use the entries on the delivered unit. Figures locate fields; their EUIs, addresses and regions are not installation settings.

Protocol and console references: ChirpStack device connection, device profiles and MQTT integration. Other LNS products can use different field names.

Integration references: ChirpStack gateway connection and LoRa Alliance regional parameters. Confirm the regional-parameters revision supported by the devices and LNS; a listed region does not authorize a hardware band conversion.