YZW PRODUCT GUIDE / CUSTOMER EDITION

YZW300X

LoRaWAN Gateway Deployment and Device Activation Guide

Installation, activation, data exchange and troubleshooting

Install YZW300X, 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 model: YZW300X

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 4

05 Match the region, sub-band and RF plan 5

06 Connect the LNS and verify gateway presence 6

- External LNS: distinguish the two destinations 6
- Address example for the worksheet 7
- Step 1: sign in to the external LNS and register the gateway 7
- Step 2: save external forwarding in the YZW300X Web UI 9
- Step 3: verify arrival at the external LNS 10

07 Verify the path from device to MQTT 10

08 Troubleshoot from the last successful stage 11

09 Gateway stage record and device configuration 11

10 Identify gateways and end devices 12

11 Gather device information 12

12 Create the device objects in the LNS 13

13 OTAA: enter root keys and join 13

14 ABP: configure the session and preserve counters 14

15 Set class, intervals and operating policy 15

16 Send and verify an application uplink 16

17 Verify application MQTT and an authorized downlink 17

- Start with a non-actuating downlink test 17

18 Ongoing operation and troubleshooting 17

19 Acceptance record and support information 18

01 Choose the gateway role

YZW300X receives LoRaWAN radio frames and forwards them to a LoRaWAN network server (LNS) using Semtech UDP. The LNS handles device registration, activation, sessions and application data. A running gateway does not establish that a device has joined or that a customer application has received its data.

Data path: field LoRaWAN sensor → YZW300X concentrator → IP uplink → external LNS Semtech UDP endpoint → LNS application integration → customer platform. Provide a customer-hosted or managed external LNS. This model has no built-in LNS.

Item	Scope for this model
Radio reception	One concentrator with eight multi-SF receive channels; SX1302-compatible. This guide covers the verified EU868 scope.
Region	EU868; AU915/US915 are not software upgrade choices.
Network server	An external LNS is required.
Independent device	LoRaNode uses a separate device identity and does not replace gateway configuration.

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 9–36 V DC 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.

Record	Value / source
Region and frequencies	Country, fitted RF band, antenna band, LNS region plan and any required sub-band.
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.

Use the field map below; some delivered pages retain English labels. “Use Local LNS” only fills a loopback address and does not add a local LNS to this model. Enter an external LNS UDP receiver for YZW300X.

UI field	Entry and check
Enable	Enable the intended instance, save and read its state again.
Gateway EUI	Prefer the actual factory EUI. If overridden, keep it unique and update the LNS registration. Do not copy an all-zero placeholder.
Server Address	External: use the Semtech UDP receiving host supplied by the LNS administrator, without a Web URL or https:// prefix. Do not use an MQTT endpoint.
Uplink / Downlink Port	Match the UDP receiving service. 1700 is a common example, not a fixed requirement for every service.
Configuration Mode / Region	Start with a verified automatic regional template, within this model’s delivered band scope.
Antenna gain / location	Enter the actual antenna gain rather than increasing it to obtain more RF power. Record the installed location.

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 for the intended instance, wait for Saved 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.

YZW300X: use the documented EU868 scope. AU915/US915 choices on another model do not apply here. A center-frequency edit cannot convert the antenna and RF front end to another band.

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.

06 Connect the LNS and verify gateway presence

YZW300X does not provide a local ChirpStack console. Have the LNS administrator provide a hosted or customer server with a working Semtech UDP receiving service. The local LoRaNode page configures a separate end-device function; it does not create external sensors or an LNS.

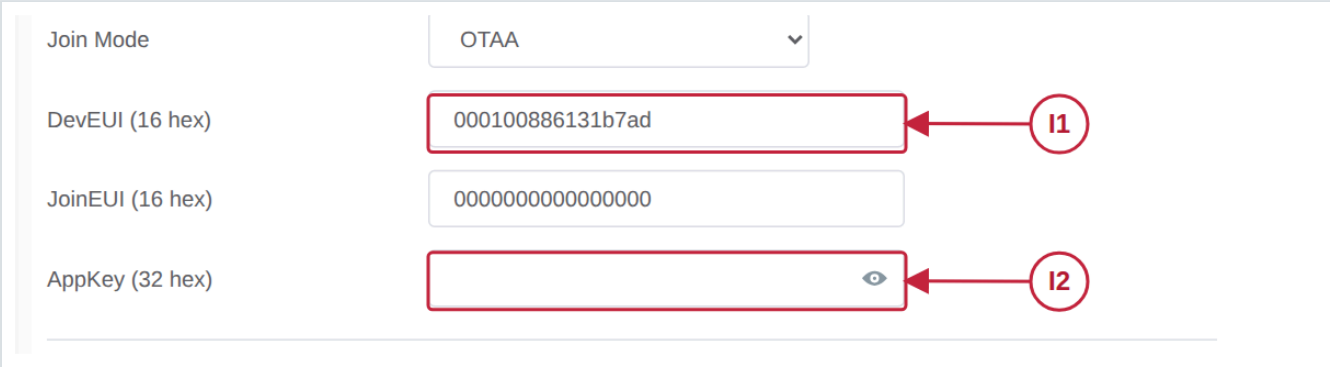


Figure 01. Native standalone LoRaNode reference (the manual uses the same-platform YZW1010 UI). DevEUI/AppKey identify a device; these are not the gateway's LNS forwarding settings. Markers correspond to the table below.

Marker	Entry / action	Check the result
I1	This is the standalone LoRaNode DevEUI. Use Gateway EUI from the LoRaWAN page for gateway registration.	Device and gateway identities are registered separately.
I2	This is the standalone node AppKey. Configure gateway Server Address and UDP ports on the LoRaWAN page.	Node keys are not used as gateway forwarding settings; follow the external-LNS table below.

External LNS: distinguish the two destinations

YZW300X uses an external LNS. This section uses external ChirpStack as the reference; obtain equivalent entries from the administrator for another LNS. The gateway sends packets to a UDP receiver. A person signs in at a Web console URL. These can use different hosts, ports and protocols.

Required item	Confirm with the LNS administrator
UDP receiver	A running Semtech UDP receiving component, for example Gateway Bridge; its actual host/IP and uplink/downlink ports. A Web page or MQTT broker alone is insufficient.
Web console	Full HTTP/HTTPS URL, actual Web port, LNS account and tenant permissions. Do not paste this URL into gateway Server Address.
Region plan	Use the verified EU868 scope for this model and match gateway, LNS and end-device uplink/downlink plans.
Network path	Allow gateway UDP and its replies. On a public server, check security groups/firewalls and bind address. A private destination reached over cellular needs an existing private/VPN route.

Address example for the worksheet

This is an example plan for one test LAN, not factory defaults or an existing server: gateway management IP 192.168.10.1, external LNS server 192.168.10.20, and a reachable maintenance PC on that network. The LNS already offers UDP 1700 and HTTP 8080. Replace every example with administrator-approved values. Do not copy private LAN IPs for a public-Internet path.

Entry location	Example value	Purpose
Gateway management Web	http://192.168.10.1	Configure the gateway, not the LNS login.
LoRaWAN → Server Address	192.168.10.20	Host/IP only, without http://, a path or :8080.
Uplink Port / Downlink Port	1700 / 1700 (UDP)	Match the external UDP receiver.
PC browser to external LNS	http://192.168.10.20:8080	Sign in and register gateways/devices here. A real platform may use HTTPS 443 or another URL.

Step 1: sign in to the external LNS and register the gateway

1. Open the full external LNS Web URL provided by its administrator. The example is http://192.168.10.20:8080. Do not use the gateway local Open Console or UDP 1700 as a Web port.
2. On the native login shown in Figure 02, enter the external LNS credentials at 4 and select 5 Submit. Obtain them from the external platform; they are not automatically the gateway management credentials.

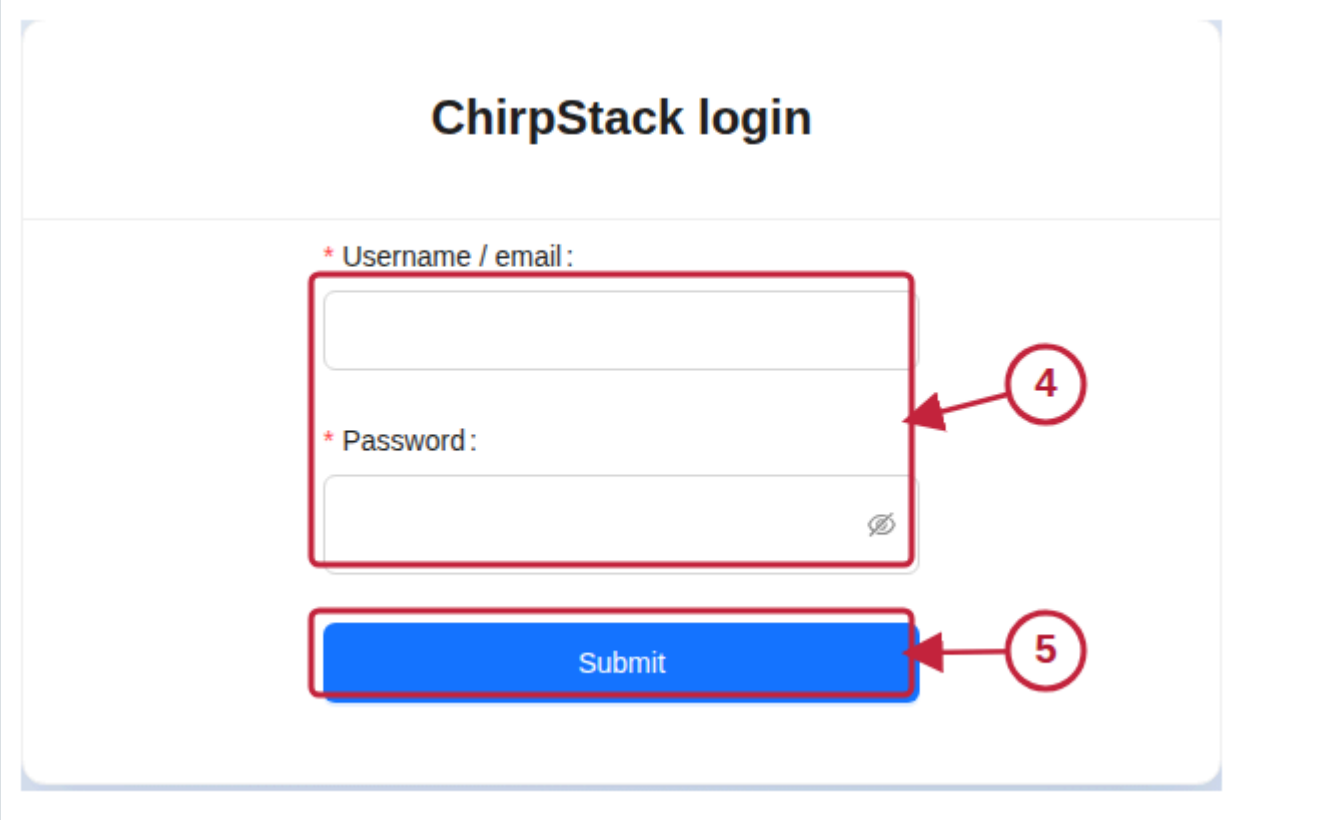


Figure 02. Native external ChirpStack login reference: 4 LNS credentials; 5 Submit. This shows the form only; obtain the actual external URL from its administrator.

Marker	Entry / action	Check the result
4	Enter the LNS username/email and password supplied by the project 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.

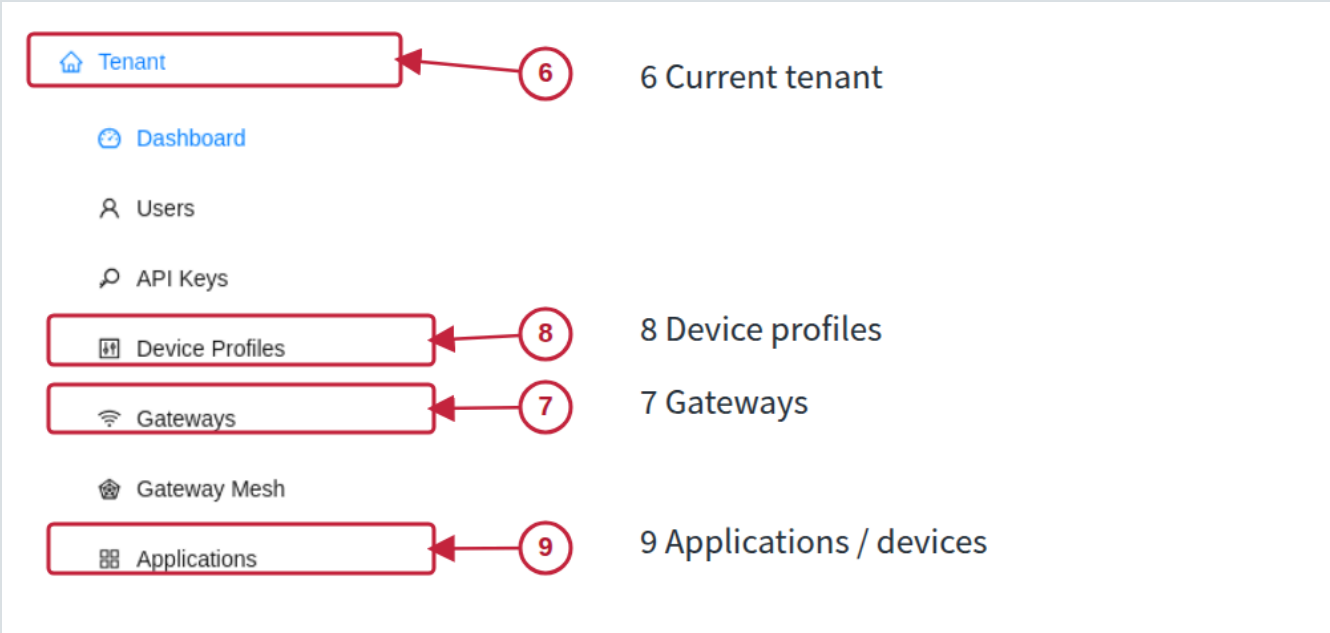


Figure 03. Native external LNS tenant-menu reference: 6 project tenant, 7 Gateways, 8 Device Profiles, 9 Applications.

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.

1. Select the project tenant and open 7 Gateways → Add/Create. Enter a name and the actual 16-hex Gateway EUI shown on the gateway LoRaWAN page as Gateway ID. Select a matching regional plan where the platform requests it, then save.
2. Do not substitute DevEUI for gateway EUI or copy an all-zero reference value. If overriding the gateway EUI, use the same unique value on the gateway and external LNS.

Step 2: save external forwarding in the YZW300X Web UI

In another tab, log in to the gateway Web UI and open Application → LoRaWAN. The following maps verified fields for this model; it is not an image of another model presented as a YZW300X screenshot.

Field / button	Action for the example
Enable	On for the intended concentrator instance.
Configuration Mode / Region	Auto / EU868 within the verified scope, with a matching channel plan.

Field / button	Action for the example
Server Address	192.168.10.20; in a real project, enter the external UDP receiver, not the browser URL.
Uplink Port / Downlink Port	1700 / 1700 using UDP; substitute the actual external ports.
Gateway EUI / Custom Gateway EUI	Use the registered actual EUI. Keep the factory EUI unless an override is required; device keys do not belong here.
Use Local LNS	This model has no built-in LNS. Do not use the shortcut to enter 127.0.0.1.
Save Gateway 1 / instance save	Save the intended instance, wait for Saved and refresh to verify settings/Running. This confirms local settings only.

Step 3: verify arrival at the external LNS

1. Return to external LNS Gateways, open the intended EUI and refresh Last seen/statistics. Allow the configured statistics interval. A newly created Never seen record is not evidence of a device-key fault.
2. Trigger a known EU868 device, verify its frame in gateway LoRaWAN frames, then use the separate device guide to check activation, device up and application MQTT.
3. If Web login works but the gateway remains Never seen, check the UDP receiver, actual EUI, Server Address, UDP ports, gateway routes/DNS and server security groups/firewall. Establish UDP reception before changing device AppKey.

The path is YZW300X Semtech UDP → external UDP receiving component → LNS gateway/network processing → application integration. The ChirpStack receiving component and network server must also use matching regional topic prefixes and MQTT connectivity, confirmed by the LNS administrator. Reachable Web TCP 8080 or broker TCP 1883 alone does not prove the gateway UDP path.

07 Verify the path from device to MQTT

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.

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.

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

The YZW300X concentrator gateway and standalone LoRaNode can run together, with separate settings and identities. This device stage covers registering the local EU868 LoRaNode on an external LNS, sending a test uplink and inspecting received events. Register external sensors on that LNS using each sensor’ s own parameters.

Object	Configuration / identity
Concentrator gateway	Local Application → LoRaWAN; Gateway EUI belongs in LNS Gateways.
Local standalone LoRaNode	Local Application → LoRaNode; DevEUI belongs in LNS Devices.
External sensor	Its vendor tool or device UI; use that sensor’ s own DevEUI and keys.

This model has no built-in LNS. Provide an external LNS and a compatible gateway covering the device. Housing gateway and node functions together is not proof of RF communication; use actual receive records and LNS events for acceptance.

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. This guide covers local LoRaNode in EU868 only.
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

Obtain the external LNS account and tenant. The following uses ChirpStack as a field reference; use equivalent entries on other LNS products. If no LNS account or UDP gateway receiver is available, prepare the server before entering keys on the local node.

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.

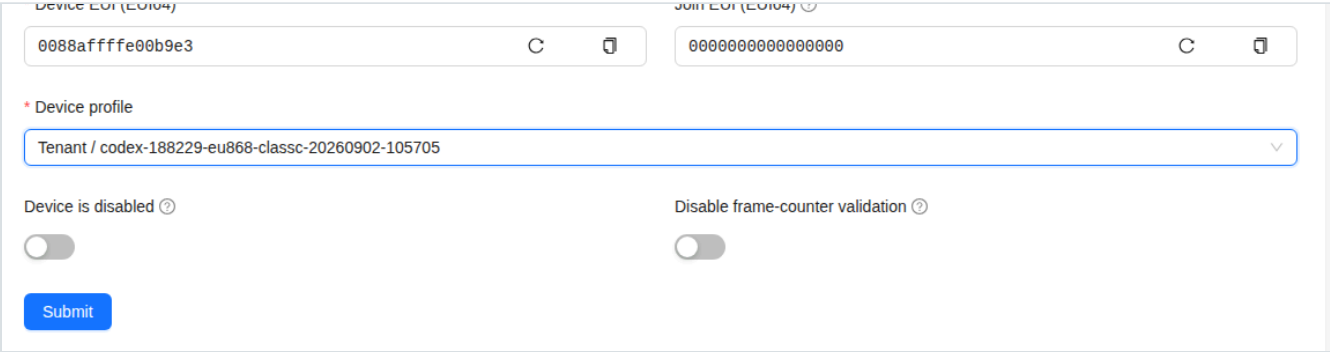


Figure 04. Native ChirpStack identity/profile fields. The historical laboratory EUI locates the field; do not reuse it for your installation.

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

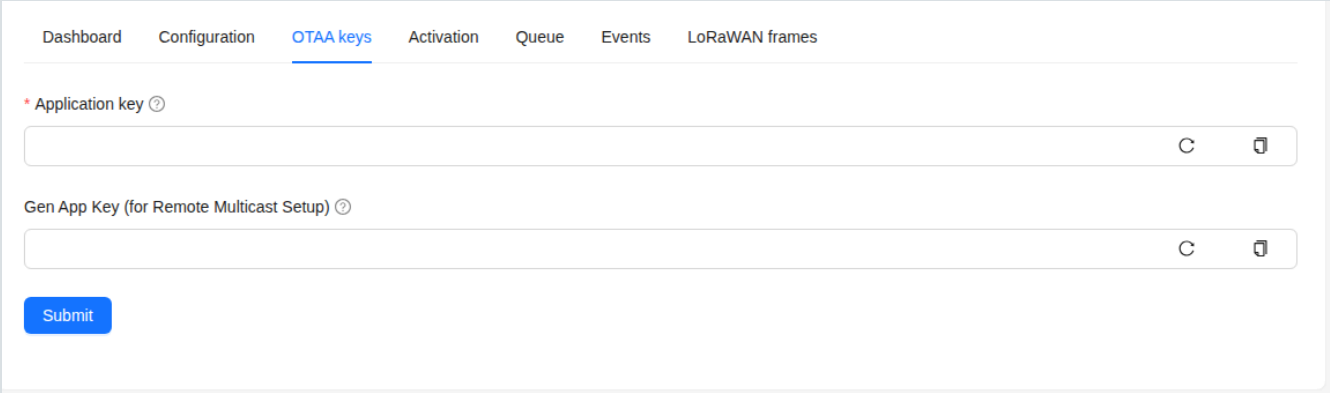


Figure 05. Native blank ChirpStack OTAA keys form, before entering keys. Application key is AppKey for the LoRaWAN 1.0.x example.

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 local Application → LoRaNode, choose OTAA, enter the same DevEUI/JoinEUI/AppKey, set EU868, the actual LoRaWAN version and class, then save and enable.
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.

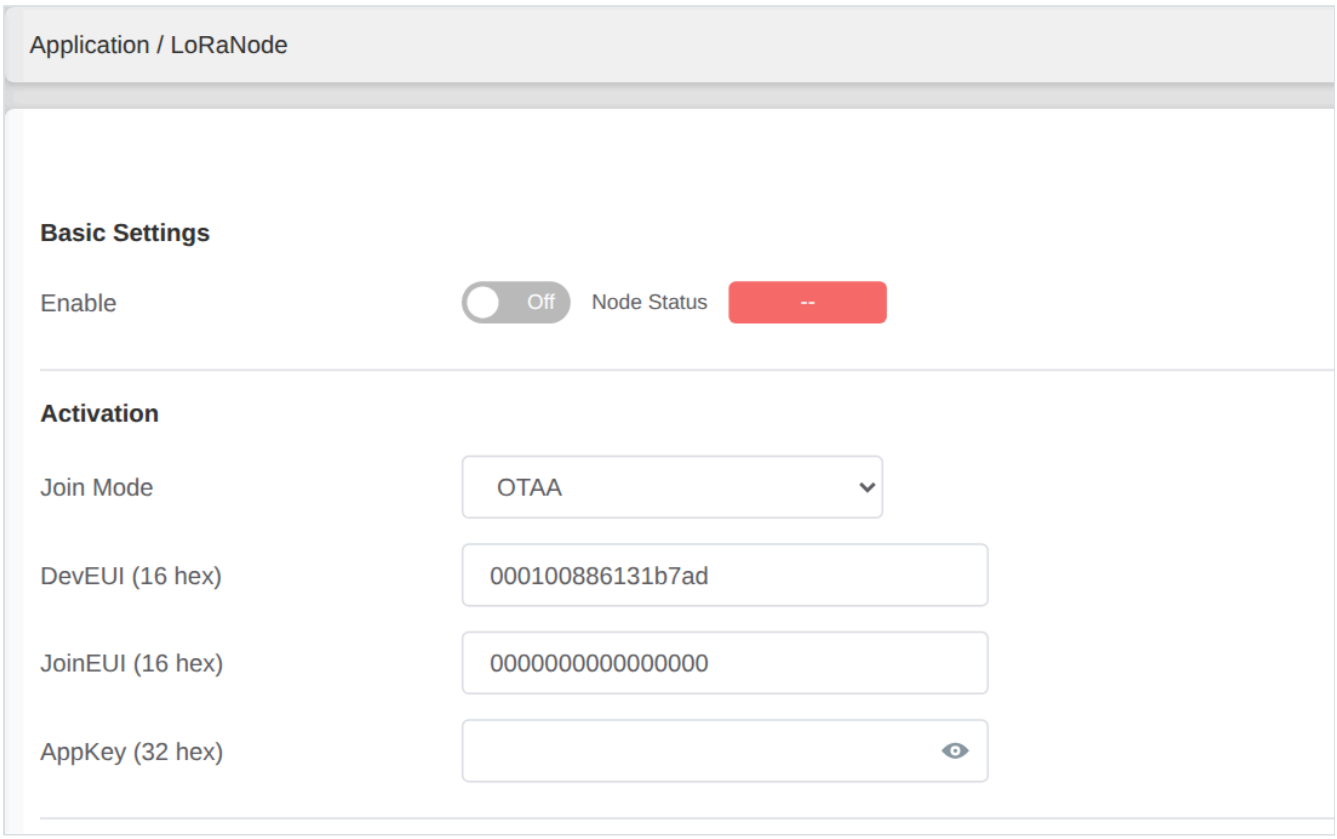


Figure 06. Native same-platform YZW1010 LoRaNode activation reference retained in the YZW300X manual. Values locate fields and are not credentials to copy.

The verified local LoRaNode page offers LoRaWAN 1.0.3 / 1.0.4; match the selected value in the LNS profile. This guide does not claim LoRaWAN 1.1 for the local node. A delivered implementation displaying DR5 / SF7 / BW125 uses a fixed uplink data rate; this is not a freely editable rate control.

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. Choose ABP in local LoRaNode, enter the same DevAddr (8 hex), NwkSKey/AppSKey (32 hex each) and actual DevEUI, then save.

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

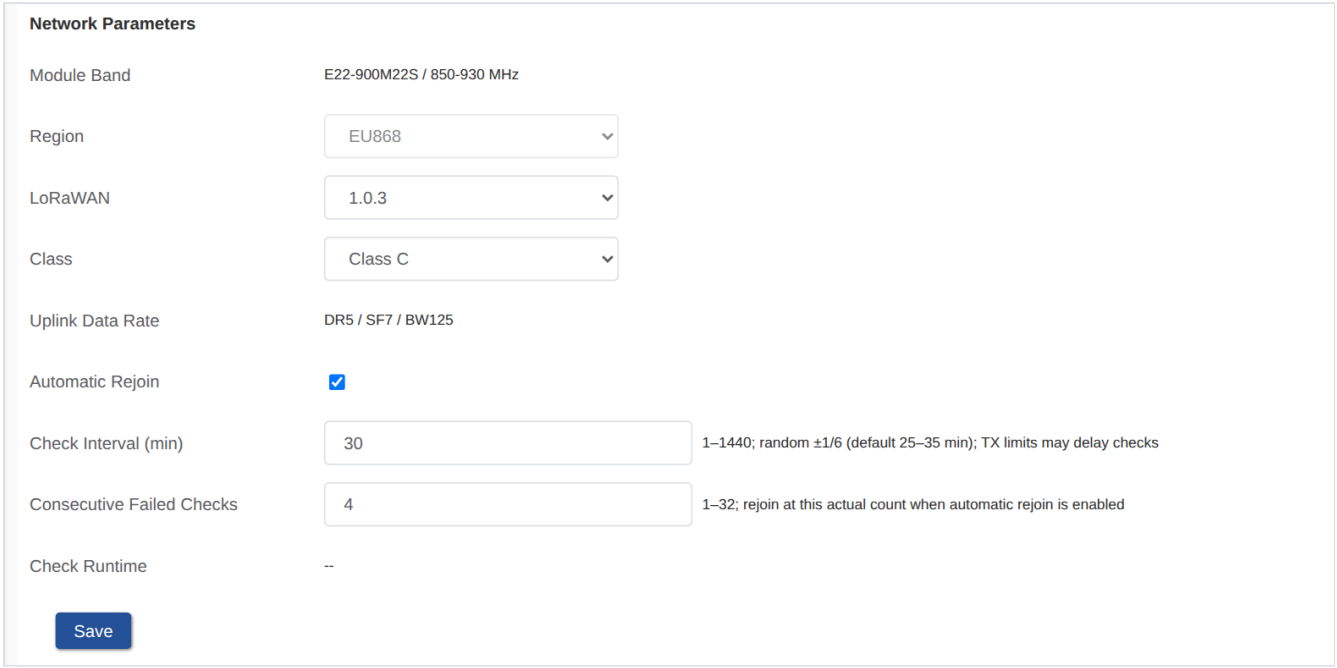


Figure 07. Native node network parameters. Use optional controls such as automatic rejoin only when present on the delivered page; the reference does not establish that every firmware includes them.

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.

Where Automatic Rejoin is delivered, use it for OTAA link-check/rejoin handling only. The reference UI gives an interval in minutes (1–1440) and a consecutive-failure threshold (1–32). Rejoin timing depends on accumulated failures, random timing and transmit limits. ABP must not initiate OTAA or clear session counters through this feature. If the controls are absent, do not edit configuration files to add them.

16 Send and verify an application uplink

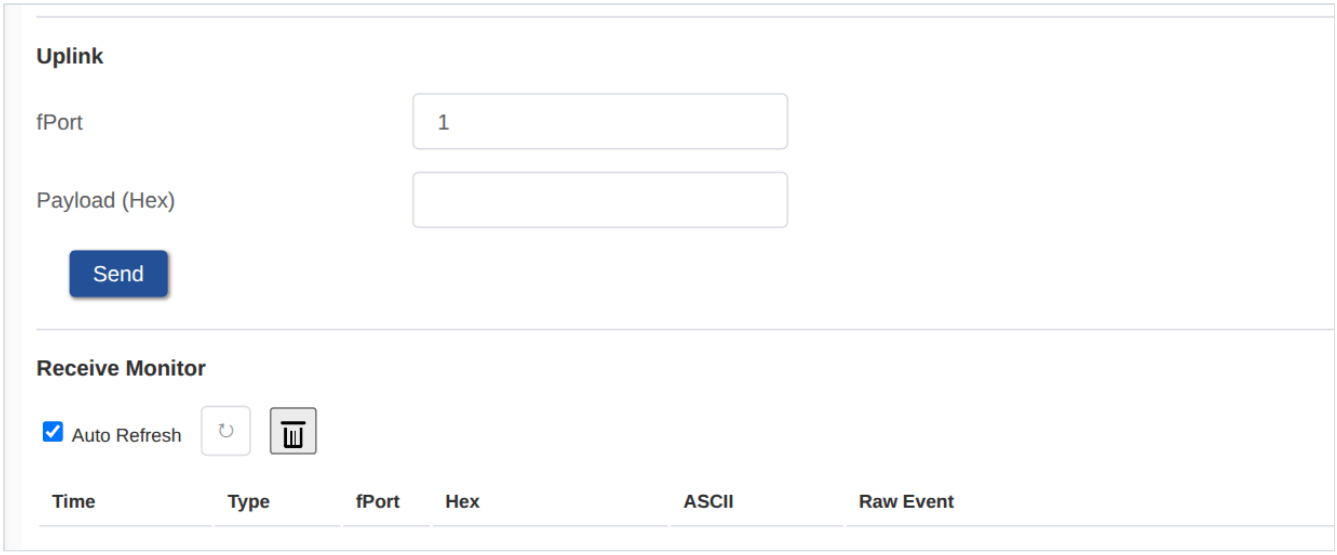


Figure 08. Native uplink and receive-monitor reference. Clear Display clears the UI record; it does not clear an LNS session.

1. After local LoRaNode activation, enter a test fPort such as 10 in Uplink; the local UI allows 1–223. Use a test port not assigned to business control.
2. Enter `01020304` in Payload (Hex), using an even number of contiguous hexadecimal characters without 0x, spaces or punctuation. Select Send. This tests bytes only and is not a universal sensor command.
3. Inspect the send result, then match DevEUI, fPort=10, FCnt and bytes in LNS device events. A local send indication does not establish LNS receipt.

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.
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.

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. Refresh local LoRaNode Receive Monitor and compare time, type, fPort, Hex/ASCII or the raw event. Receiving bytes does not automatically map them to DO, Modbus or an application action.

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.

Symptom / action	Check and response
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.

A shared LoRa application RUN LED indicates that a gateway or node service is running. It is not sufficient evidence of node activation, RF communication or customer-platform data.

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 YZW300X 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.