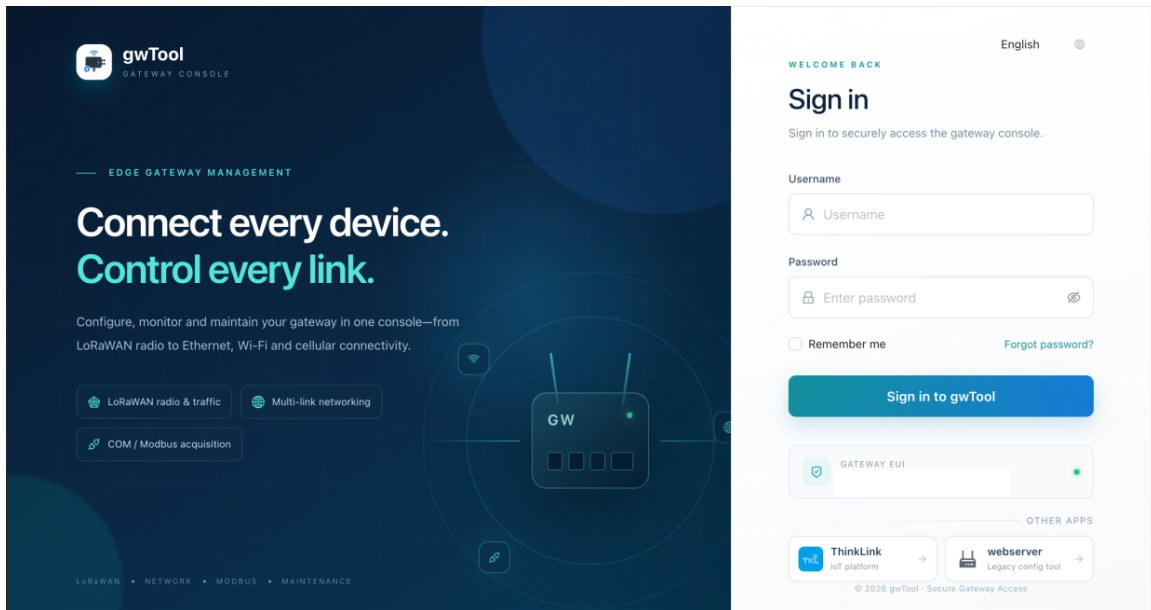


gwTool7

LoRaWAN Gateway

Standardized Device Manual



VERSION
1.0

DOCUMENT
Device Manual

Revision History

Version	Change Description
1.0	Current published version

Contents

1. Sign-in, Sign-out, and Language

- Purpose
- Sign-in Procedure
- Change Language and Sign Out
- Verification

2. Overview

- Purpose
- Key Areas
- Procedure and Verification

3. LoRaWAN

- 3.1 LoRaWAN NS
- 3.2 Radio
- 3.3 Traffic

4. ThinkLink

- 4.1 ThinkLink General
- 4.2 ThinkLink Advanced

5. COM and Serial Services

- 5.1 COM General
- 5.2 Pollers
- 5.3 MODBUS Records
- 5.4 COM Advanced

6. Network

- 6.1 Status
 - Purpose
 - Key Fields and Controls
 - Procedure and Verification
 - Troubleshooting
- 6.2 Ethernet
 - Purpose
 - Key Fields and Controls
 - DHCP Configuration
 - Static Address Configuration
- 6.3 Wi-Fi
- 6.4 Bluetooth
- 6.5 Cellular

6.6 Network Advanced

7. System

7.1 Device

7.2 Account & Security

8. Upgrade

8.1 ThinkLink Upgrade

8.2 GwSerial Upgrade

8.3 GwTool Upgrade

8.4 Firmware Upgrade

9. Maintenance

9.1 Self-check

9.2 System Logs

9.3 Terminal

9.4 Services and Gateway Reboot

Purpose

Service Status Check

Manual Gateway Reboot

Automatic Reboot Schedule

Verification and Recovery

10. General Safety and Recovery

Product: gwTool GD7

Document version: 1.0

Screenshot language: English

Screenshot source: authorized test device; device identifiers, network addresses, and account information have been cropped or masked

This manual is intended for distributors, system administrators, and field engineers. It explains how to inspect status, configure the gateway through the gwTool web interface, and recognize operations that require extra care.

NOTE Fields and page layouts may vary slightly between firmware versions. Back up the current configuration and schedule a maintenance window before changing settings, upgrading software, or rebooting the gateway.

1. Sign-in, Sign-out, and Language

Purpose

The sign-in page authenticates an administrator before opening the gateway console. After signing in, the interface language can be changed from the selector in the upper-right corner.

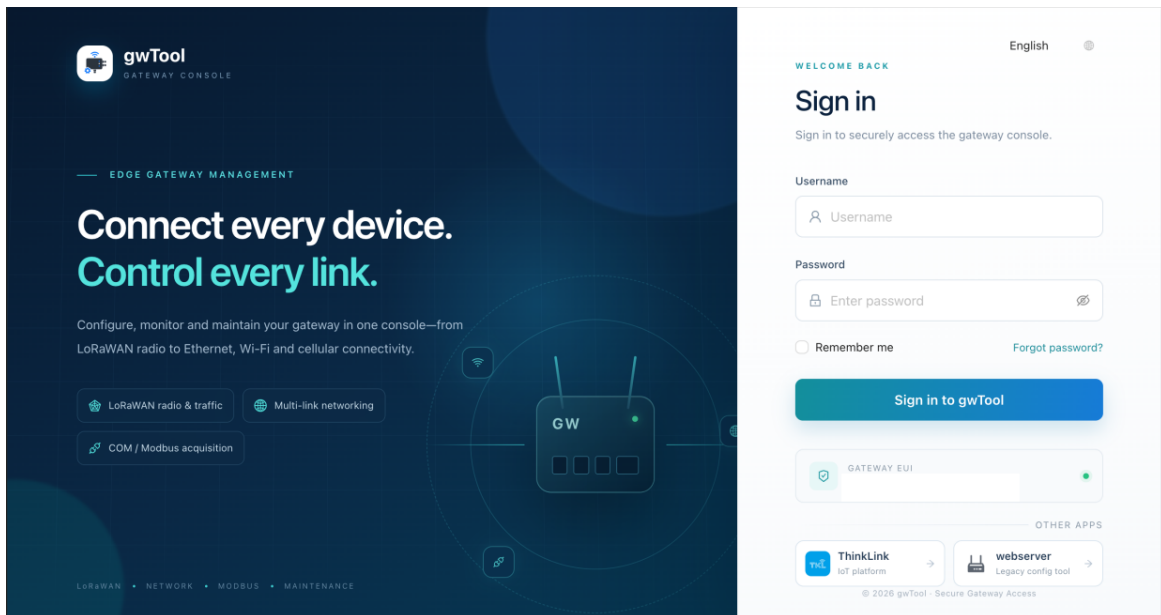


Figure GD7 English sign-in page

Figure 1: English sign-in page. The form is empty, and the gateway identifier has been masked.

Sign-in Procedure

1. Connect the management computer to a network that is allowed to reach the gateway console.
2. Open `http://<gateway-management-address>/` in a browser.
3. Enter the administrator username and password, then select **Sign in to gwTool**.
4. Confirm that the left navigation and the language selector appear.

Change Language and Sign Out

- Use the language selector in the upper-right corner to switch between English and the available Chinese interfaces.
- After switching, verify that the page title and navigation labels have changed before continuing.
- When administration is complete, sign out from the account menu. Do not rely on closing the browser tab alone.

Verification

- Success: the Overview page opens, the navigation is available, and no session-expired message appears.
- Failure: check the management address, network path, account status, and keyboard case. Do not repeatedly try an uncertain password.

NOTE Do not save administrator credentials on a shared computer or transmit them through screenshots, chat messages, or support tickets.

2. Overview

Navigation: Overview

Purpose

The Overview page summarizes gateway identity, the primary network link, local services, software versions, and resource utilization. Use it for a health check before configuration or maintenance.

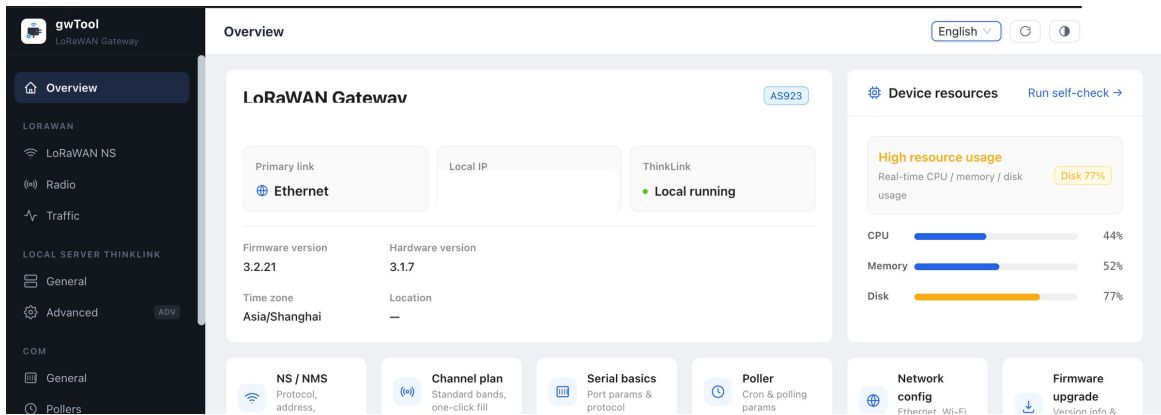


Figure GD7 English Overview page

Figure 2: Gateway, network, service, and resource status. Unique identifiers, active addresses, and account information are masked.

Key Areas

Area	Description	Administrator check
LoRaWAN Gateway	Region and basic gateway status	Confirm that the regional setting matches the deployment site
Primary link	Network currently preferred by the gateway	Confirm that the link type matches the site design
ThinkLink	Local service state	Record an abnormal state before troubleshooting
Version and device information	Firmware, hardware, and time-zone information	Record versions before upgrades or support escalation
Device resources	CPU, memory, and disk usage	Investigate sustained high utilization

Procedure and Verification

1. Open **Overview** and wait for all status cards to load.
2. Check the primary link and ThinkLink state.
3. Review CPU, memory, and disk usage; record the time and affected resource if an alert is present.
4. Continue to the relevant network, service, or upgrade page only after identifying the affected area.

NOTE Overview values represent the most recent refresh. Reload the page and confirm that an alert is still present before maintenance.

3. LoRaWAN

3.1 LoRaWAN NS

Navigation: LORAWAN → LoRaWAN NS

This page selects where the gateway sends LoRaWAN data: a local server or a remote network-server platform. Tabs are provided for the NS1 primary server, NS2 backup, and NMS management.

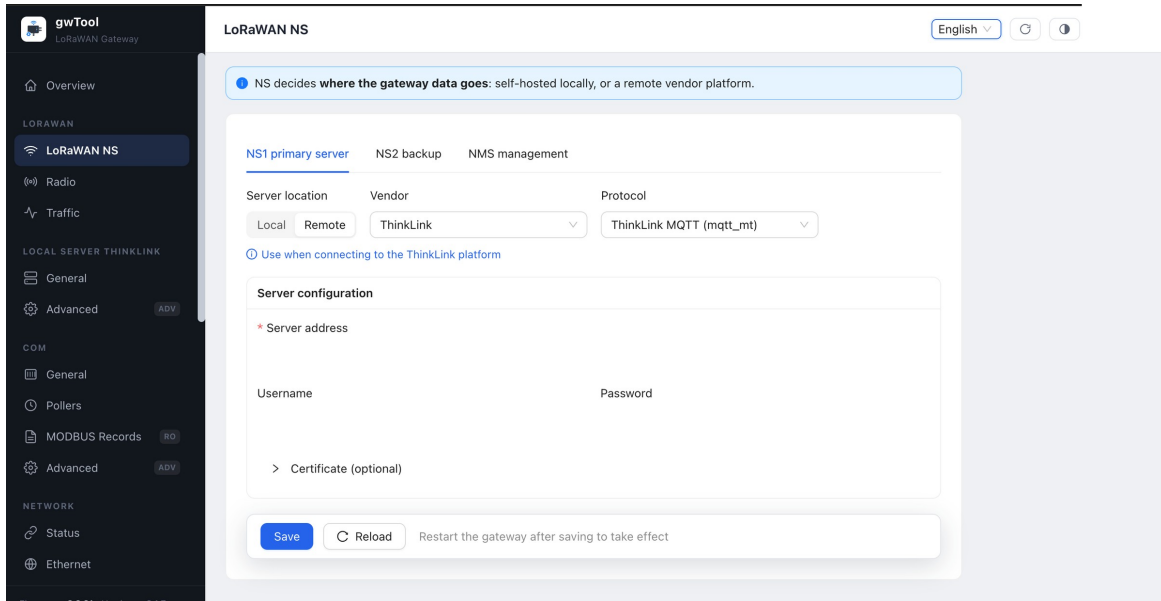


Figure GD7 English LoRaWAN NS page

Figure 3: NS1 primary-server configuration. Server address, username, and password values are masked.

Key fields: server location, vendor, protocol, server address, username, password, and optional certificates. UDP normally also requires uplink and downlink ports. MQTT uses a Broker endpoint, while Basic Station uses the **Server URI** field.

Current gwTool7 firmware offers **ChirpStack** and **The Things Network** in Remote mode. Use **BasicStation LNS** for ChirpStack. For TTN, select **BasicStation LNS** or **BasicStation CUPS** according to the deployment design.

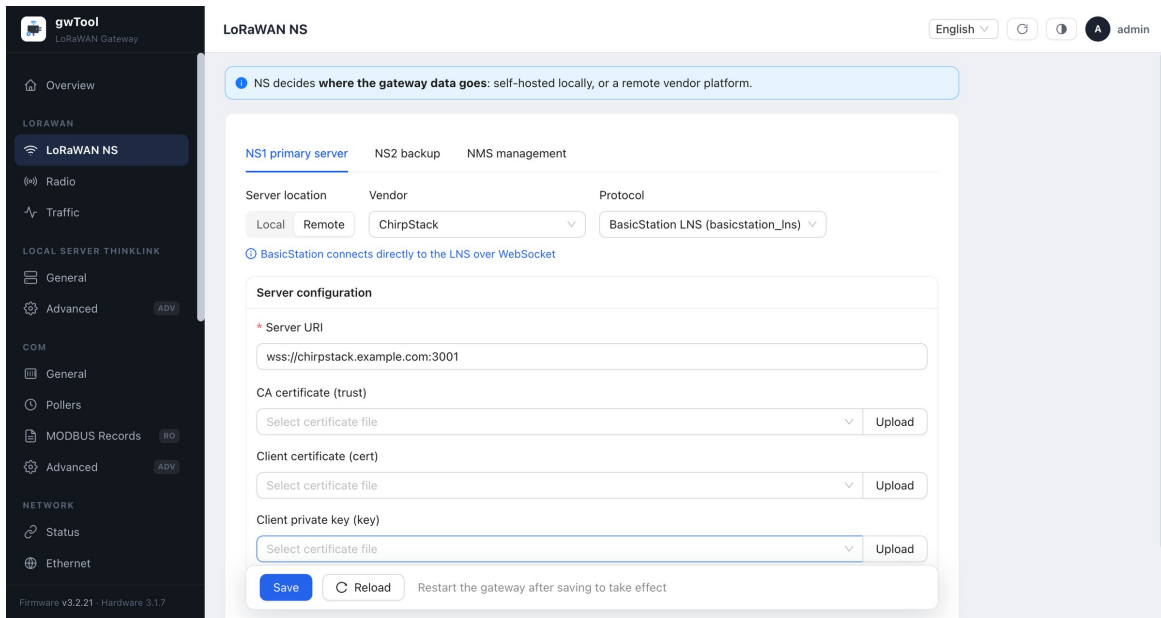


Figure gwTool7 ChirpStack BasicStation LNS configuration in English

Figure 3A: ChirpStack BasicStation LNS example. The endpoint is a documentation-only example and certificate fields are empty.

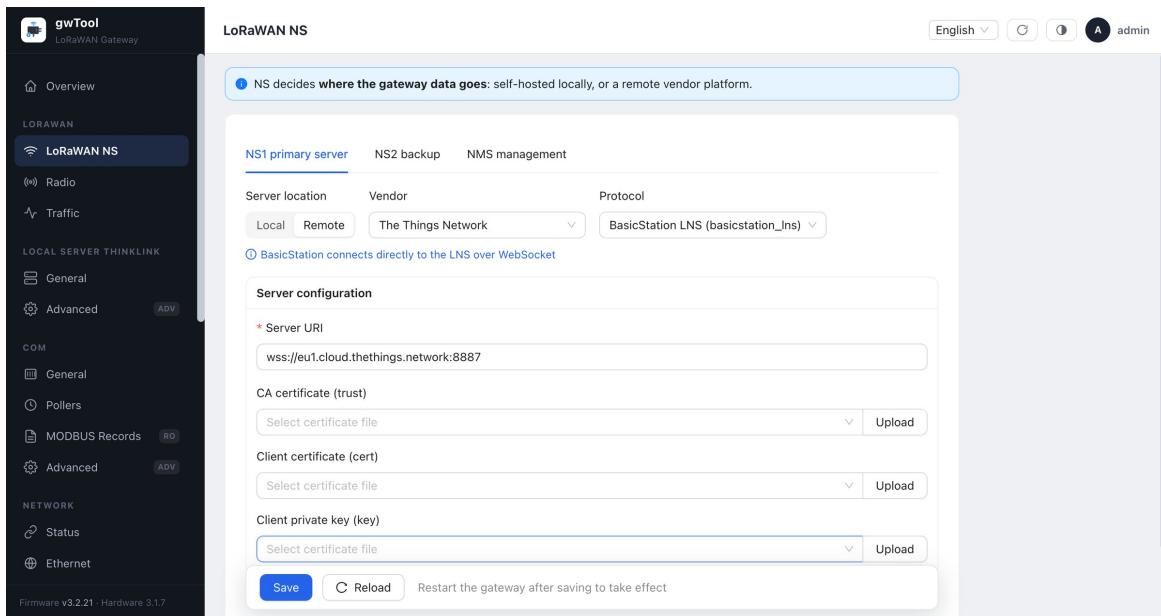


Figure gwTool7 TTN BasicStation LNS configuration in English

Figure 3B: TTN BasicStation LNS example. Use the actual Server Address, trust certificate, and key supplied through the TTN Console.

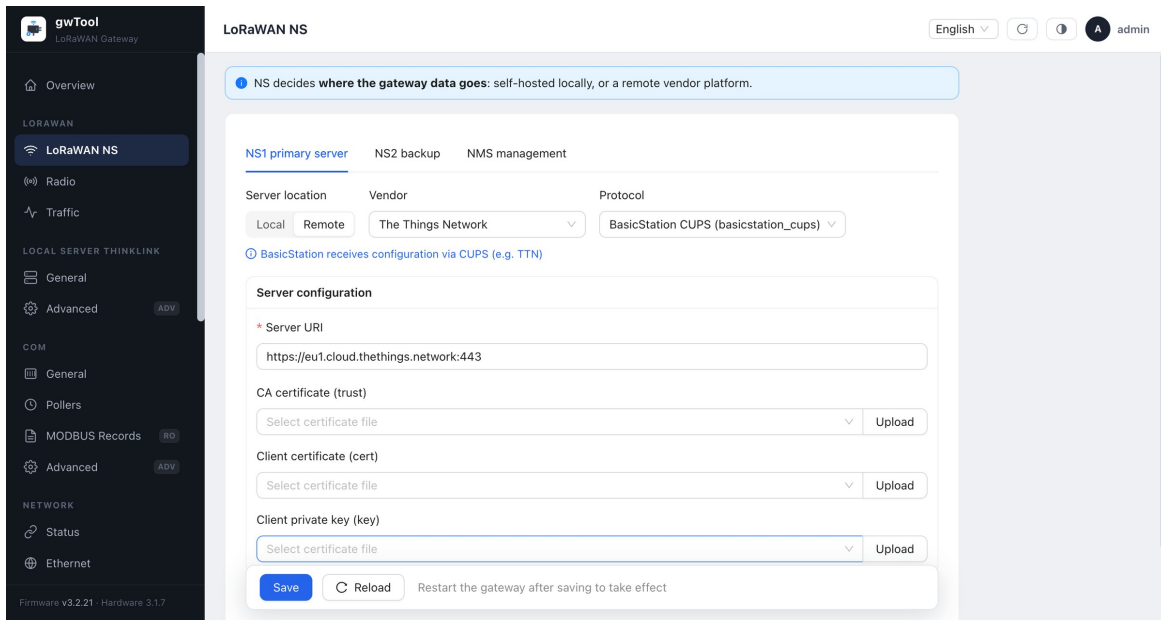


Figure gwTool7 TTN BasicStation CUPS configuration in English

Figure 3C: TTN BasicStation CUPS example. CUPS delivers the LNS settings to the gateway.

Procedure and verification:

1. Record the existing NS configuration and obtain the approved protocol, address, ports, and credentials from the platform owner.
2. Select the vendor and protocol in NS1, then complete the fields required by that protocol. See the dedicated [ChirpStack Basic Station guide](#) and [TTN Basic Station guide](#) for the full procedures.
3. A blank password field normally preserves the stored value; enter a new one only when rotating credentials.
4. Save, wait for the related service to recover, then verify uplink and downlink traffic on both the Traffic page and the server platform.

NOTE NS2, certificate, and mode controls may be wired differently across firmware releases. A visible control does not prove that a configuration is active; verify traffic after saving.

3.2 Radio

Navigation: LORAWAN → Radio

Use this page to select the regional standard, set keepalive and status-report intervals, and configure channel-plan frequencies, bandwidth, and spreading factors.

Radio

Radio sets which frequencies the gateway uses. First pick a **region standard** to auto-fill the channel plan, then fine-tune as needed. Values shown in MHz (6 decimals).

Region standard & keepalive

Region standard Gateway current loraStandard (read-only): AS923

Keepalive interval keepalive_interval-s: 60

Status report interval stat_interval-s: 60

RF1 - First radio chain

Channel plan Channel Plan: as923 One-click fill

Step MHz: 0.2 Fill width count: 8 Start channel Count from this channel: Channel 1

Single-channel bandwidth bw: 250000 Frequency MHz: 924.500000 Spreading factor sf: 7

Enable single channel: ☒

Channel 1 freq1-MHz: 923.200000 Channel 2 freq2-MHz: 923.400000 Channel 3 freq3-MHz: 923.600000 Channel 4 freq4-MHz: 923.800000

On submit, MHz→Hz conversion is applied and pushed; saving takes a few seconds to take effect

Reset Submit

Figure GD7 English Radio page

Figure 4: Example AS923 channel plan. Actual frequencies must comply with local regulations and the network plan.

Procedure and verification:

1. Confirm the LoRaWAN regional standard permitted at the deployment location.
2. Select the matching band plan and use the one-click fill function before applying operator-specific adjustments.
3. Verify RF1/RF2, single-channel bandwidth, frequency, spreading factor, and every channel frequency.
4. Submit the change, wait several seconds, reload the page, and verify device joins and traffic.

NOTE Incorrect frequencies can prevent devices from joining and may violate radio regulations. Preserve the original channel plan before making changes.

3.3 Traffic

Navigation: LORAWAN → Traffic

Traffic provides a live view of uplink and downlink LoRaWAN frames. Filter by all, uplink, or downlink, and expand a record to inspect raw and decoded data.

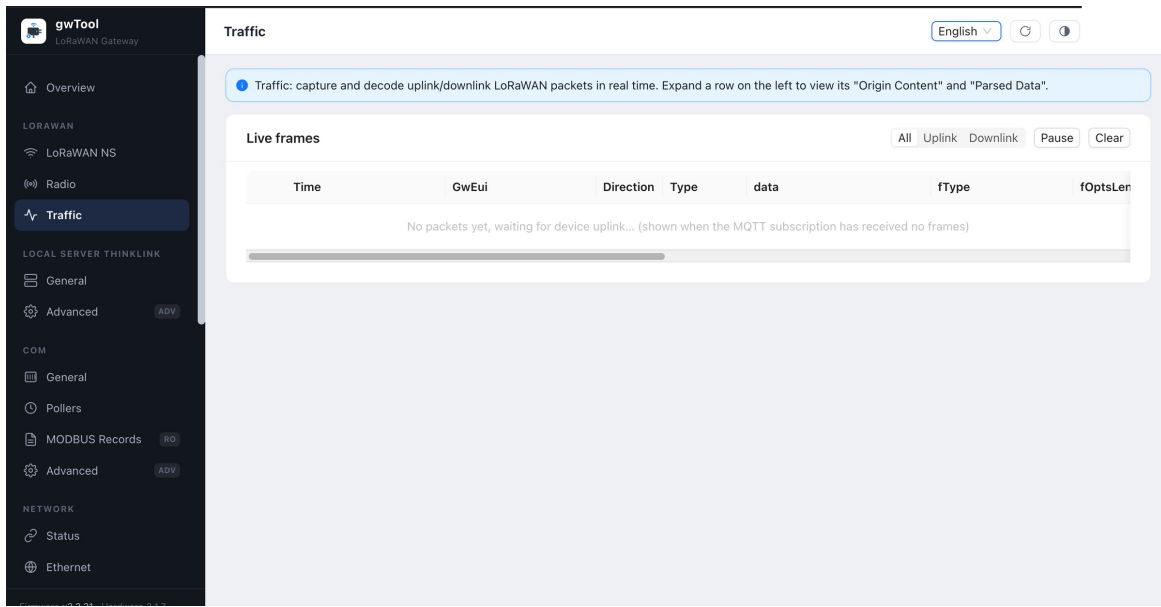


Figure GD7 English Traffic page

Figure 5: Idle live-traffic table. No field payload is included in the screenshot.

Procedure and verification:

1. Keep the page open and trigger a known end-device uplink.
2. Filter by direction and confirm the time, gateway reference, direction, and frame type.
3. Expand the target row to inspect the raw and decoded content. Pause or clear the list before starting a new observation period.

NOTE Frames may contain device identifiers and business data. Redact them according to organizational data-handling rules before exporting or taking screenshots.

4. ThinkLink

4.1 ThinkLink General

Navigation: LOCAL SERVER THINKLINK → General

Use this page to enable the local ThinkLink server, control downlink capability, and review core-service and local-connection status.

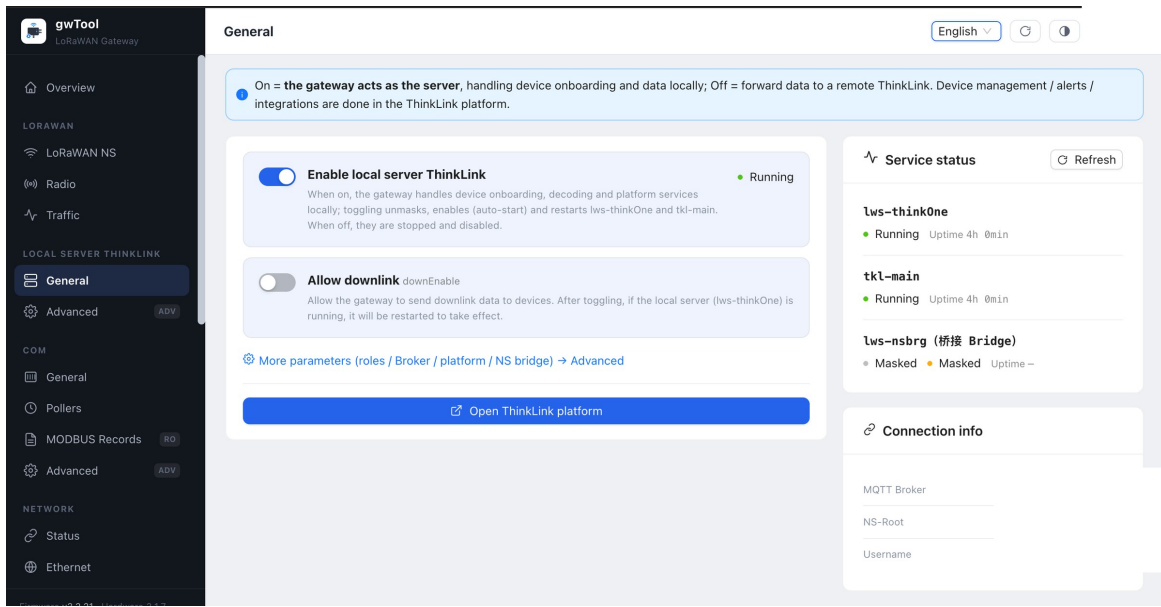


Figure GD7 English ThinkLink General page

Figure 6: Local-server controls, service state, and connection area. Connection values are masked.

Procedure and verification:

1. Decide whether the local ThinkLink server should be enabled according to the deployment architecture.
2. Enable downlink only when the service is authorized to send data to end devices.
3. Refresh and verify lws-think0ne, tkl-main, and bridge-service states.
4. Open the ThinkLink platform and confirm device, alarm, and data-processing functions.

NOTE Changing the local-server role changes the data path. Confirm the responsibility boundary between the local gateway and the remote platform before saving.

4.2 ThinkLink Advanced

Navigation: LOCAL SERVER THINKLINK → Advanced

This engineering page configures local-server roles, brokers, certificates, and platform parameters.

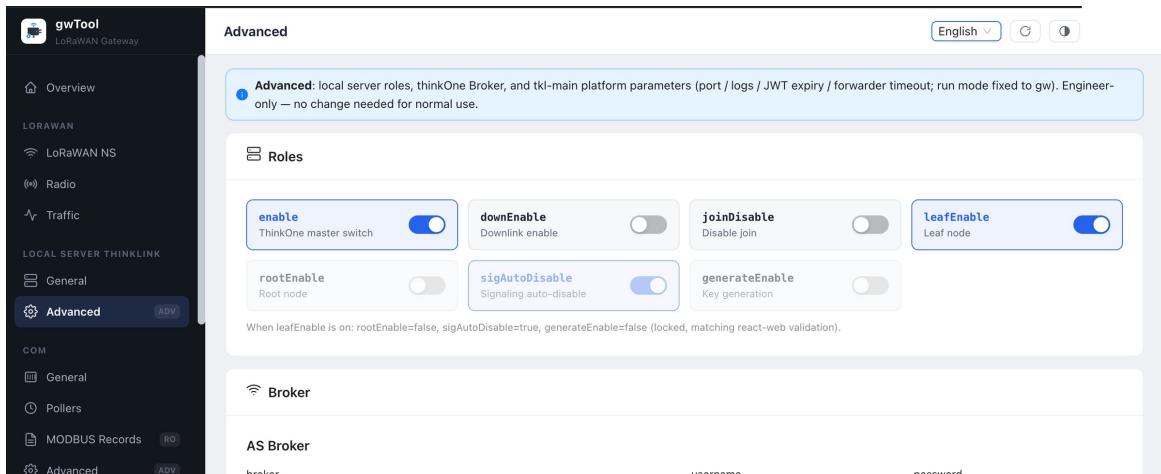


Figure GD7 English ThinkLink Advanced page

Figure 7: Role and Broker sections. Address, username, and password values are not shown.

Procedure and verification:

1. Select leaf, root, downlink, automatic-disable, and key-generation roles according to the approved architecture.
2. Enter the Broker address and account. When TLS is enabled, also verify the CA, client certificate, and client key.
3. Save, restart only the service identified by the interface, and then verify the General page.

NOTE Role combinations have dependencies. Do not override locked or mutually exclusive roles, and do not experiment with Broker credentials on a production gateway.

5. COM and Serial Services

5.1 COM General

Navigation: COM → General

Use this page to configure the serial-device path, baud rate, data bits, stop bits, and parity, and to inspect the gw-serial service state.

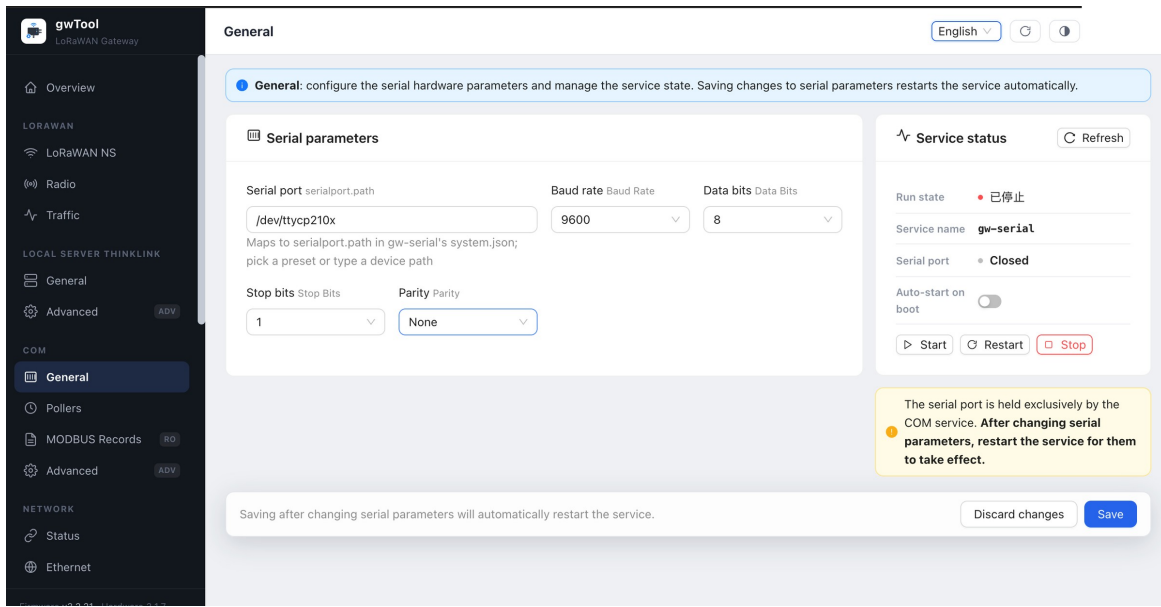


Figure GD7 English COM General page

Figure 8: Serial parameters and service status. The service was stopped during capture; no start action was performed.

Procedure and verification:

1. Obtain the serial path and communication settings from the connected-device documentation.
2. Verify baud rate, data bits, stop bits, and parity before saving.
3. Saving may restart the serial service. Refresh the status and confirm that the serial port opens and the service runs normally.

NOTE Mismatched settings cause timeouts, corrupt text, or invalid frames. Record the original settings and prevent multiple services from using the same port.

5.2 Pollers

Navigation: COM → Pollers

Use this page to manage scheduled tasks and Modbus pollers. A task may use a fixed interval or cron expression and may carry JSON parameters.

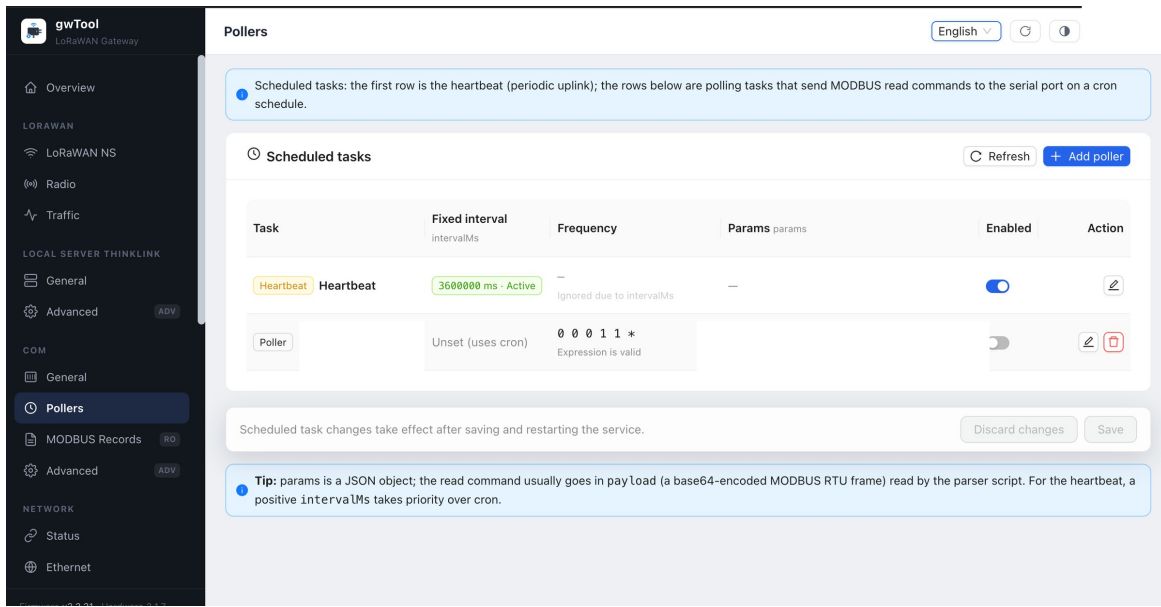


Figure GD7 English Pollers page

Figure 9: Heartbeat and poller list. The field task name and payload are masked.

Procedure and verification:

1. Determine the slave address, function code, registers, and polling interval, and validate the request frame in a test environment.
2. Add or edit a poller, then enter its task name, fixed interval or cron schedule, and JSON parameters.
3. Save, confirm the enabled state, and inspect request and response frames in MODBUS Records.

NOTE An excessively short interval can saturate the serial bus or overload the slave. Confirm dependencies before deleting, disabling, or modifying a task.

5.3 MODBUS Records

Navigation: COM → MODBUS Records

This read-only page displays the most recent cached serial requests and responses for diagnosing timeouts, exception responses, and protocol-setting errors.

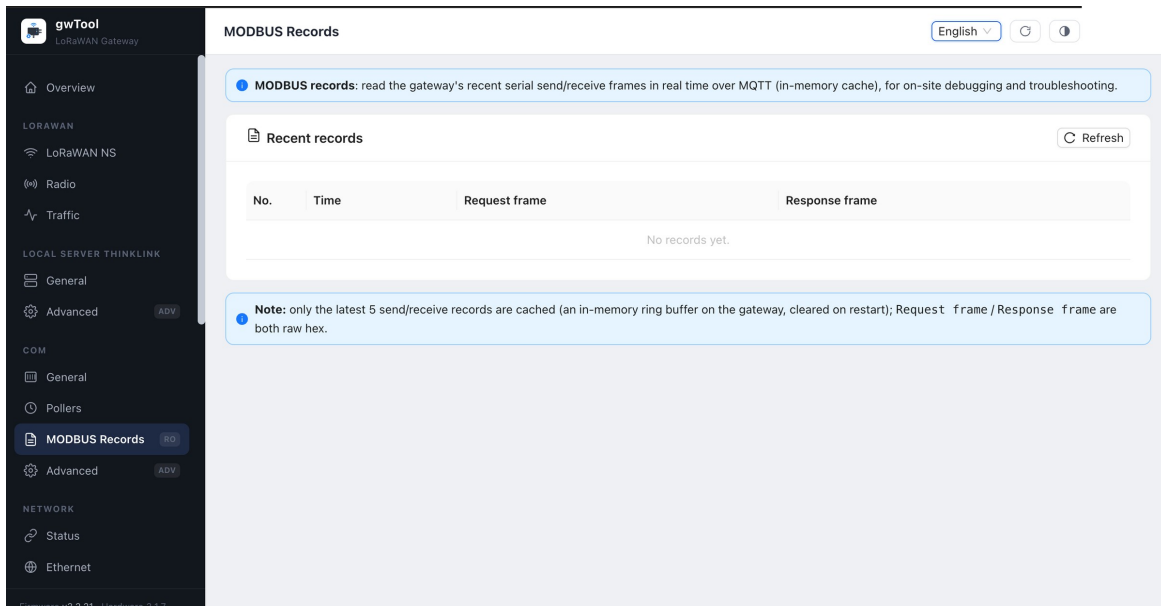


Figure GD7 English MODBUS Records page

Figure 10: Page state when there are no recent records.

Procedure and verification:

1. Confirm that the COM service and authorized poller are running.
2. Refresh and match request and response frames by time.
3. Record abnormal frames and compare them with the slave protocol. Only a small number of recent entries are retained, and a reboot may clear them.

5.4 COM Advanced

Navigation: COM → Advanced

Use this page to configure MQTT connectivity, serial timing, queue limits, logging, device attributes, and parser scripts.

Advanced

English

Advanced: MQTT connection, serial timing, device attributes and parsing scripts. Mostly engineer-level items — scripts and attributes are usually pushed by the platform via downlink, exposed here for on-site debugging. Saving changes to MQTT / timing / script / attributes **restarts the service** to take effect.

MQTT connection

Broker address mqtt.url Username username Keepalive keepalive-seconds 60

Password Stored with AES encryption ☐ Encrypted ☐ Plaintext Reset password (leave blank to keep, plaintext is auto-en...)

Reconnect interval reconnectPeriod-milliseconds 3000 Connect timeout connectTimeout-ms 30000

Clean session clean-discard session on disconnect ☒ Do not keep session

Save MQTT connection

Serial timing & reporting

Frame gap frameGapMs 100 Downlink timeout downlinkTimeoutMs 2000 Poll queue limit maxPollQueue 200 Pass-through queue limit maxPassThroughQueue 200

Figure GD7 English COM Advanced page

Figure 11: MQTT and serial-timing settings. Broker, username, and password values are masked.

Procedure and verification:

1. Record the current Broker, reconnect interval, timeout, and queue parameters.
2. When changing the MQTT address or account, also verify TLS, ACL, and upstream-service settings.
3. Save timing, script, or attribute changes and wait for the service restart.
4. Verify the service state, MODBUS records, and upstream Broker together.

NOTE Advanced parameters and parser scripts can affect every serial workflow. Do not modify them without a rollback file and test results.

6. Network

6.1 Status

Navigation: NETWORK → Status

Purpose

The Status page summarizes Ethernet, Wi-Fi, and cellular connectivity, the active interfaces, and shortcuts to their configuration pages.

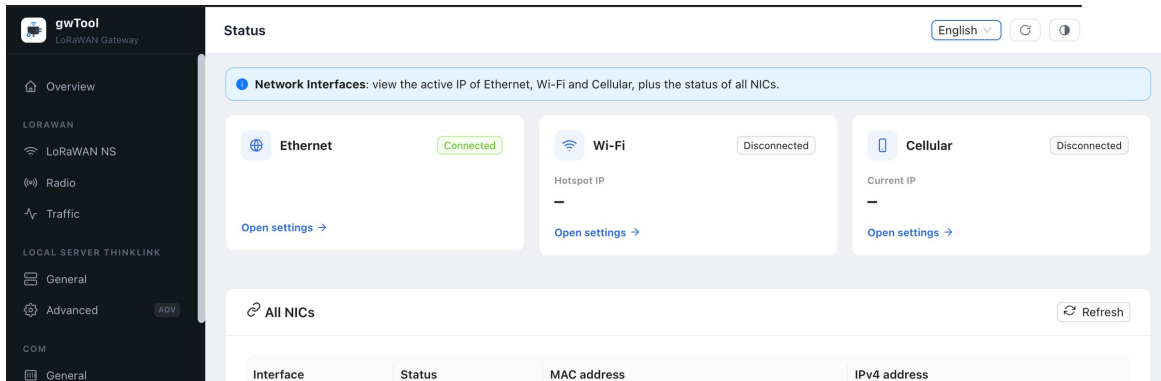


Figure GD7 English Network Status page

Figure 12: Link summary and network-interface table header. Active addresses and MAC addresses are not shown.

Key Fields and Controls

Field or control	Description
Connected / Disconnected	Whether a link is currently established
Current IP / Hotspot IP	Active address; record or share it only when authorized
Open settings	Opens the corresponding network configuration page
All NICs	Lists interface name, state, MAC address, and IPv4 address
Refresh	Reads current state without changing configuration

Procedure and Verification

1. Check the three network cards and confirm that the intended link is connected.
2. In **All NICs**, verify that the corresponding interface state is UP.
3. Select **Refresh** and confirm that status updates normally.
4. Open a configuration page only when that network type needs adjustment.

Troubleshooting

- If a card is disconnected, inspect cabling, signal, SIM service, and the upstream network before refreshing.
- If a card disagrees with the NIC table, wait several seconds and refresh; record the time and screenshot if the mismatch remains.
- If the active business path is uncertain, do not disable an interface. First confirm the primary link and site topology.

6.2 Ethernet

Navigation: NETWORK → Ethernet

Purpose

The Ethernet page enables or disables the wired interface and selects DHCP or static addressing.

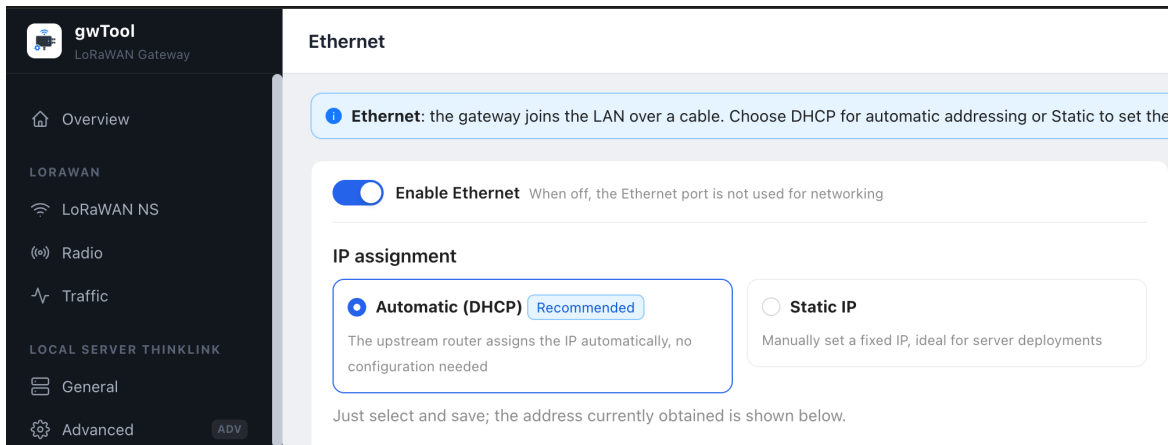


Figure GD7 English Ethernet page

Figure 13: Ethernet enable control and address mode. Active site addresses are outside the cropped image.

Key Fields and Controls

Field or control	Description
Enable Ethernet	Determines whether the wired interface participates in networking
Automatic (DHCP)	Obtains address, gateway, and DNS settings from an upstream server
Static IP	Manually specifies IP address, subnet mask, gateway, and DNS
Currently active	Shows settings that are actually in effect
Save	Applies the page changes and may interrupt the management session

DHCP Configuration

1. Confirm that DHCP is available on the upstream network.
2. Keep **Enable Ethernet** on.
3. Select **Automatic (DHCP)**.
4. Record the current management address and prepare to find the new address in the DHCP lease table.

5. Save, reconnect to the management page, and verify Ethernet on the Status page.

Static Address Configuration

1. Obtain an unused address, subnet mask, default gateway, and DNS setting from the network administrator.
2. Select **Static IP** and complete all required fields.
3. Verify that the address and gateway belong to a reachable network.
4. Save, reconnect using the new address, and verify the **Currently active** section.

NOTE Changing the management address, disabling Ethernet, or entering an incorrect gateway can immediately end the session. Prepare an alternate access path or on-site recovery assistance before remote changes.

6.3 Wi-Fi

Navigation: NETWORK → Wi-Fi

Use this page to select Hotspot (AP), Client, or Off mode and configure wireless security, NAT, and wired extension.

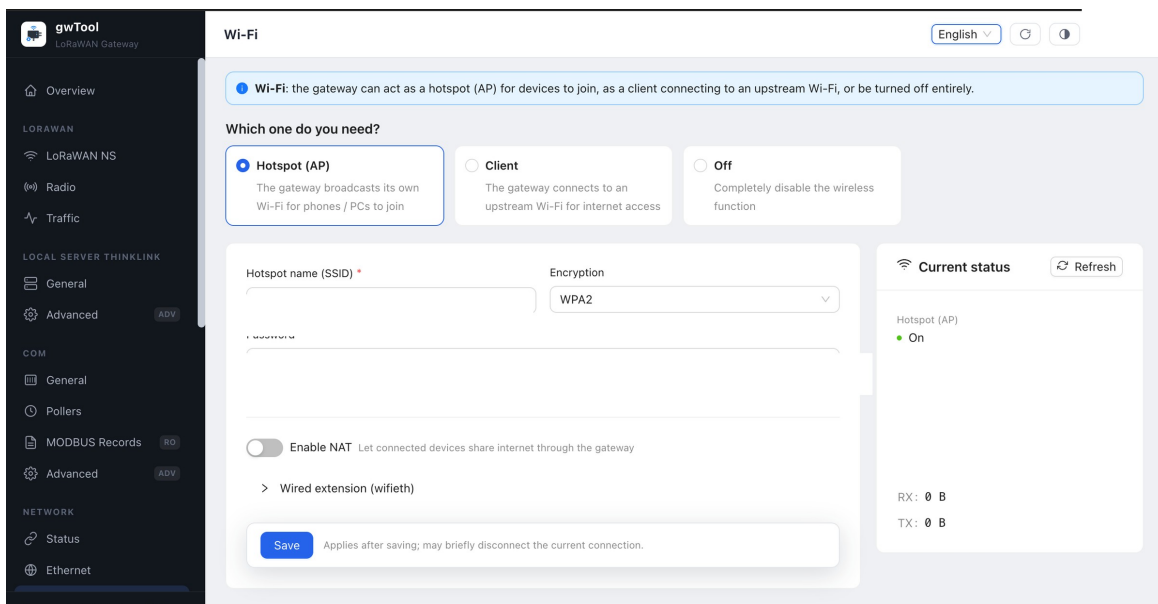


Figure GD7 English Wi-Fi page

Figure 14: Hotspot mode. SSID, password, hotspot address, and MAC information are masked.

Mode summary:

- Hotspot (AP): the gateway publishes a wireless network for local devices.

- Client: the gateway connects to upstream Wi-Fi; verify SSID, BSSID, signal, and encryption.
- Off: disables both hotspot and client operation.
- NAT and wired extension: control traffic forwarding and DHCP or static addressing according to the site topology.

Procedure and verification:

1. Preserve a working wired management path and record the current settings.
2. Select the mode and enter the SSID, encryption, and password. An open network is not recommended for production.
3. Configure NAT and wired extension if required, read the disconnection warning, and save.
4. Reconnect through the backup path, refresh, and verify mode, interface state, address, and traffic counters.

NOTE Changing mode, SSID, key, NAT, or address can immediately end the session. If access is lost, use the alternate wired path to restore the previous settings.

6.4 Bluetooth

Navigation: NETWORK → Bluetooth

Use this page to inspect the Bluetooth worker, advertisement and backend-connection states, and recent command logs.



Figure GD7 English Bluetooth page

Figure 15: Bluetooth service area. Log entries are cropped out to avoid exposing the advertisement identifier.

Procedure and verification:

1. Check whether the worker is running and whether the live connection matches expectations.
2. Inspect recent logs only when troubleshooting, and redact device identifiers before sharing a screenshot.
3. Record state and logs before an authorized engineer investigates the adapter and backend service.

NOTE Toggling the Bluetooth worker changes device-access capability. Do not switch it without confirming the business impact.

6.5 Cellular

Navigation: NETWORK → Cellular

Use this page to enable 4G/LTE dialing, enter an APN, inspect SIM and signal status, and test cellular-path connectivity.

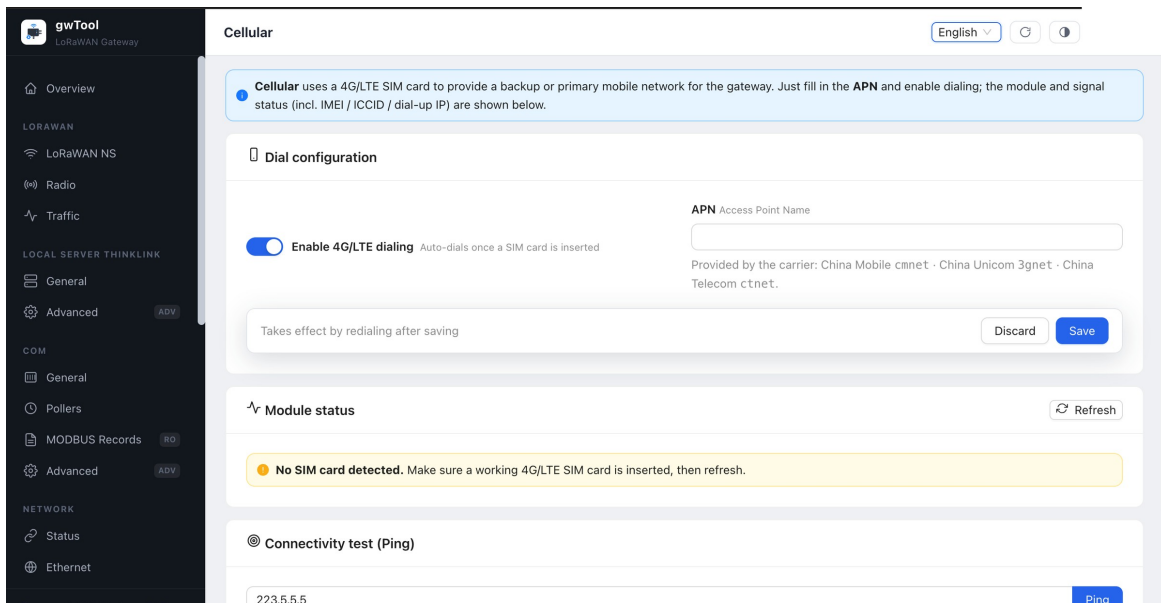


Figure GD7 English Cellular page

Figure 16: Cellular configuration and Ping area when no SIM card is detected.

Procedure and verification:

1. Power down or follow the device procedure before installing a valid SIM, then refresh the module state.
2. Enter the carrier-approved APN, enable dialing, and save.
3. Wait for redial and verify signal, carrier, assigned address, and interface state.
4. Ping only an approved target to confirm public or private-network reachability.

NOTE IMEI, ICCID, phone number, APN, and assigned address are sensitive. Redact them from tickets and screenshots.

6.6 Network Advanced

Navigation: NETWORK → Advanced

Use this page to manage OpenVPN files and state, the netCheck connectivity watchdog, and outbound-link selection.

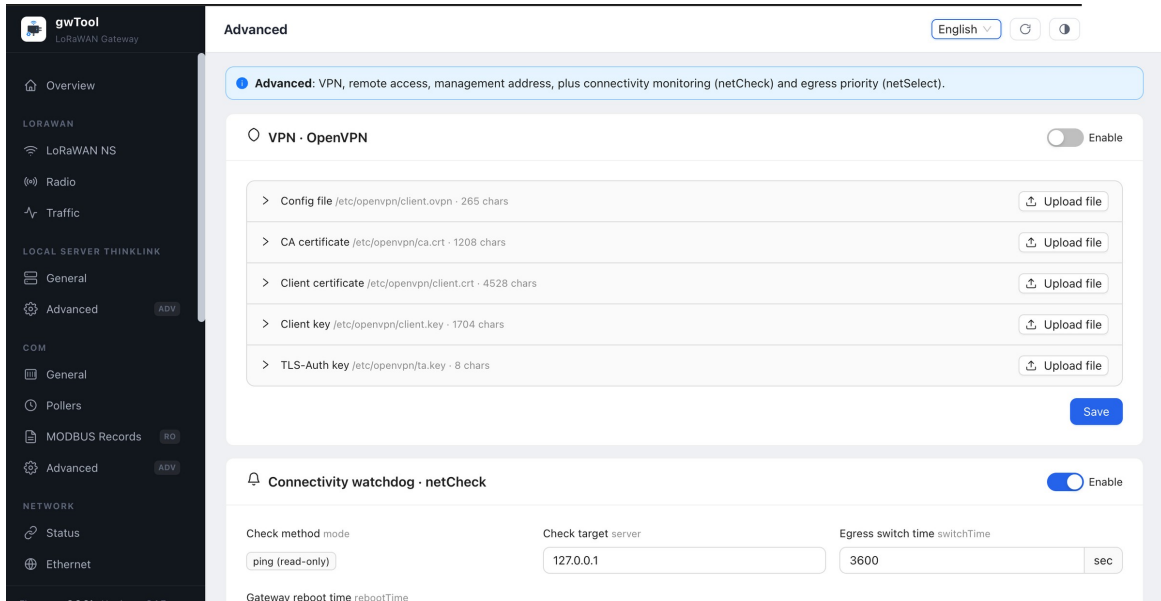


Figure GD7 English Network Advanced page

Figure 17: OpenVPN file controls and netCheck settings. Certificate contents are not expanded.

Procedure and verification:

1. For OpenVPN, confirm that the configuration, CA, client certificate, client key, and TLS-Auth key belong together.
2. Verify each uploaded file and its approved source before enabling VPN during a maintenance window.
3. For netCheck, select a stable reachable target and reasonable failover and reboot thresholds.
4. Save and verify management access, the VPN tunnel, and outbound routing; do not rely only on a switch state.

NOTE VPN keys and certificates must not appear in screenshots or tickets. Incorrect routes, probe targets, or thresholds may cause repeated failover or reboot.

7. System

7.1 Device

Navigation: SYSTEM → Device

Use this page to inspect device identity and versions, configure time and time zone, and back up or restore configuration.

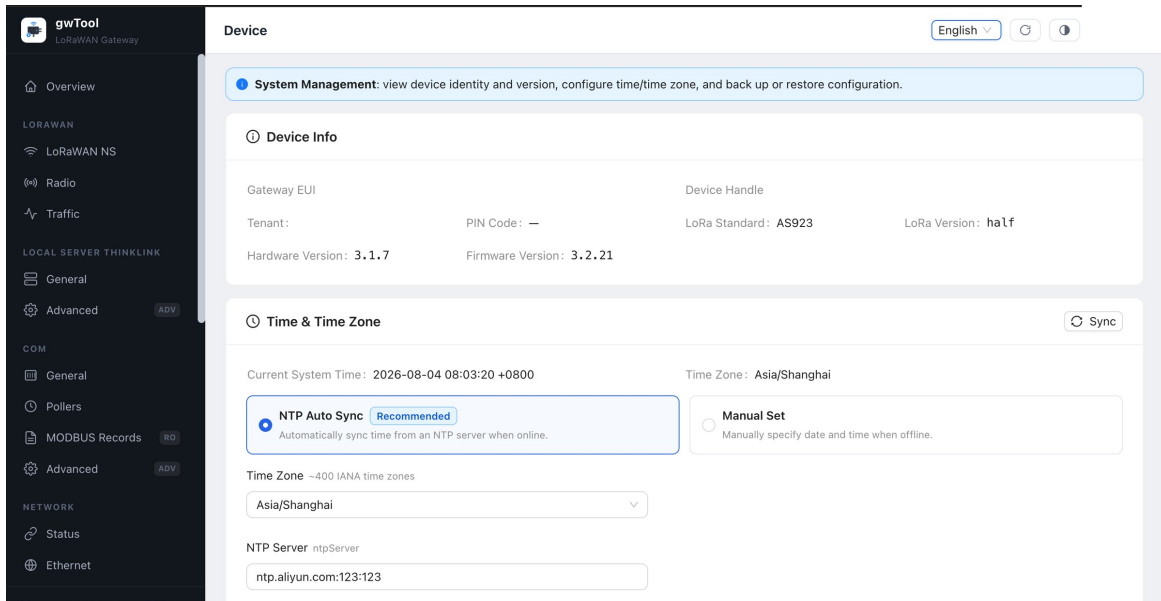


Figure GD7 English Device page

Figure 18: Device information and time settings. Gateway EUI, tenant, and device handle are masked.

Procedure and verification:

1. Record firmware, hardware, LoRa version, and time zone before support escalation or upgrade.
2. Prefer NTP Auto Sync on connected gateways and use a reachable, trusted NTP server.
3. Use manual time only when offline, and verify the time zone at the same time.
4. After synchronizing or saving, reload and compare the system time with a trusted reference.

NOTE Incorrect time affects certificates, logs, scheduled tasks, and data timestamps. Before restoring a backup, confirm its source, gateway model, and firmware compatibility.

7.2 Account & Security

Navigation: SYSTEM → Account & Security

Use this page to change the web administrator password.

The screenshot shows the gwTool7 web interface. On the left is a dark sidebar with navigation links: Overview, LORAWAN (LoRaWAN NS, Radio, Traffic), LOCAL SERVER THINKLINK (General, Advanced), COM (General, Pollers, MODBUS Records), and NETWORK (Status, Ethernet). The main content area is titled 'Account & Security' and includes a language dropdown set to 'English'. A blue notification bar at the top states: 'Account & Security: change the gateway login password.' Below this is a 'Change Password' section with three input fields: 'Current Password' (placeholder: 'Enter your current password'), 'New Password' (placeholder: 'At least 8 characters, with letters and digits'), and 'Confirm New Password' (placeholder: 'Enter again'). A 'Change Password' button is located at the bottom right of the form.

Figure GD7 English Account and Security page

Figure 19: Password-change form with all fields empty.

Procedure and verification:

1. Enter the current password and then enter and confirm a new password that meets policy.
2. Before submitting, store the new password in the approved password manager.
3. Sign out after the change and sign in again with the new password.

NOTE Do not reuse a default or shared password. If sign-in fails after a change, follow the approved account-recovery procedure instead of guessing repeatedly.

8. Upgrade

Before any upgrade, verify product and hardware compatibility, the package source and checksum, export the configuration, ensure stable power and management access, and schedule business downtime.

8.1 ThinkLink Upgrade

Navigation: UPGRADE → ThinkLink Upgrade

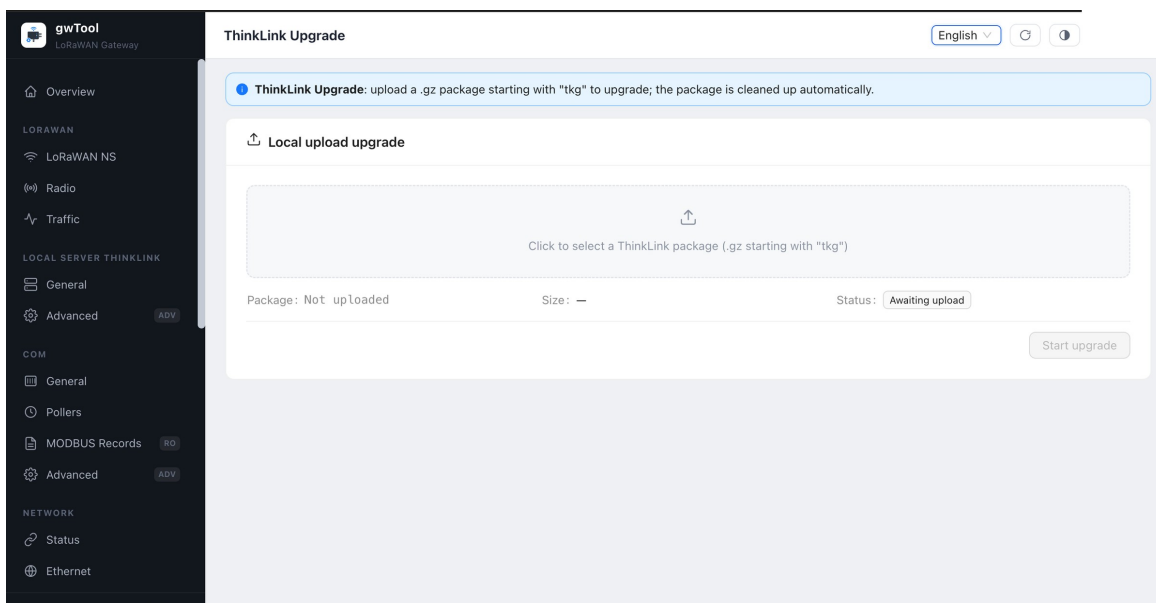


Figure GD7 English ThinkLink Upgrade page

Figure 20: Safe initial state before selecting an upgrade package.

Select an approved .gz ThinkLink package whose filename begins with tkg. Verify the name and size before starting. After completion, sign in again and check ThinkLink General and the required services.

8.2 GwSerial Upgrade

Navigation: UPGRADE → GwSerial Upgrade

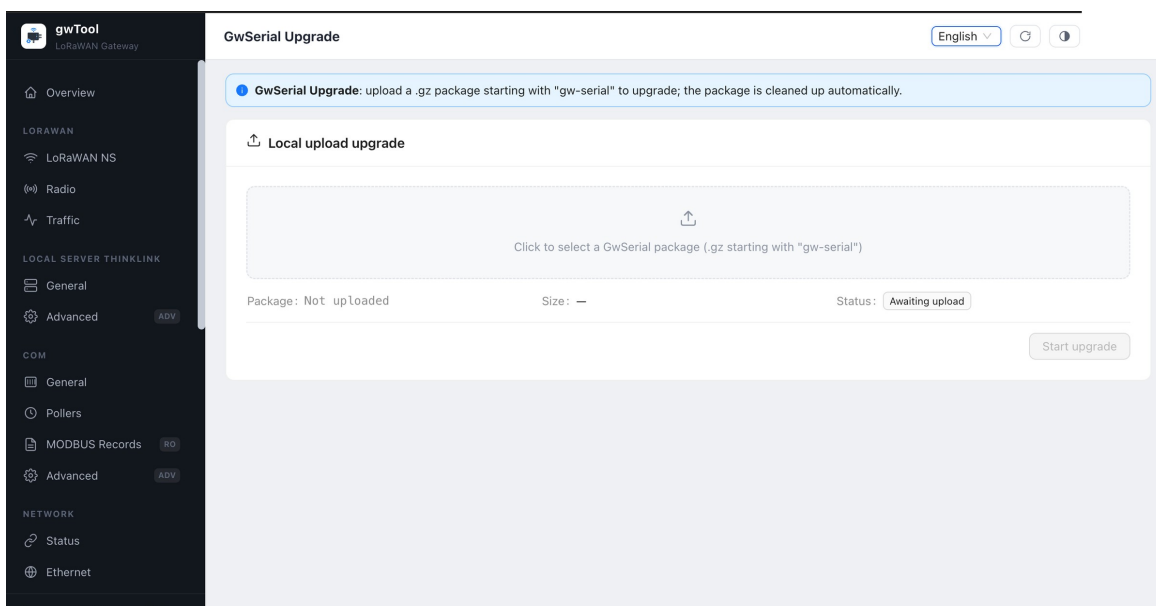


Figure GD7 English GwSerial Upgrade page

Figure 21: GwSerial package selector with no file uploaded.

Select an approved .gz package whose filename begins with gw-serial. After upgrading, verify COM service state, serial-port availability, pollers, and records.

8.3 GwTool Upgrade

Navigation: UPGRADE → GwTool Upgrade

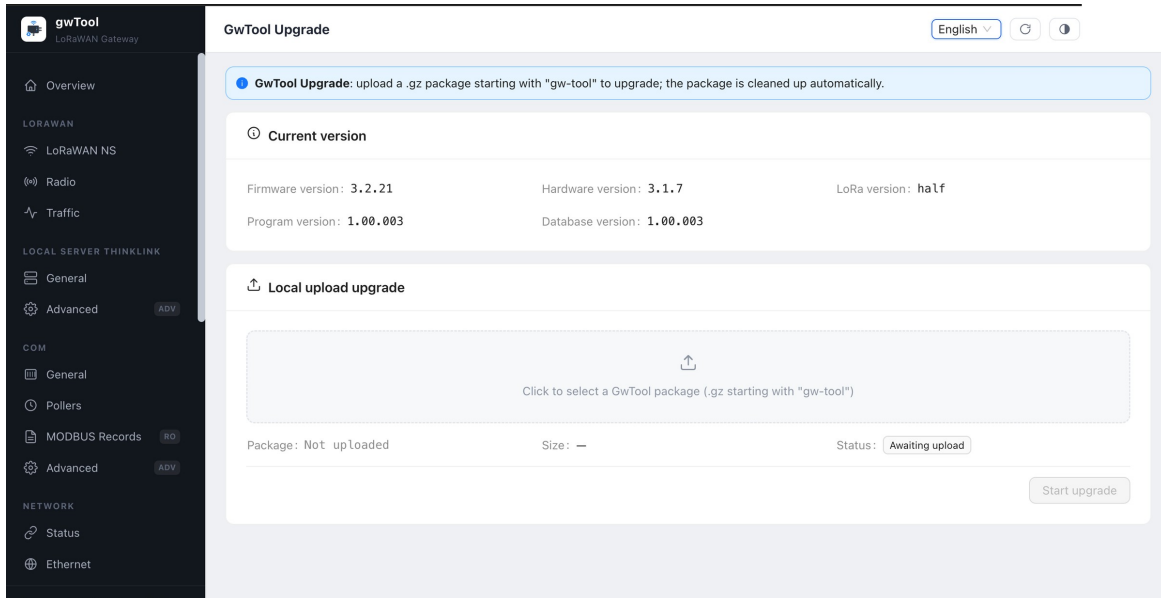


Figure GD7 English GwTool Upgrade page

Figure 22: Current version and GwTool package selector.

Select an approved .gz package whose filename begins with gw-tool. Record firmware, hardware, application, and database versions first; after upgrading, force-refresh the browser and sample the core configuration pages.

8.4 Firmware Upgrade

Navigation: UPGRADE → Firmware Upgrade

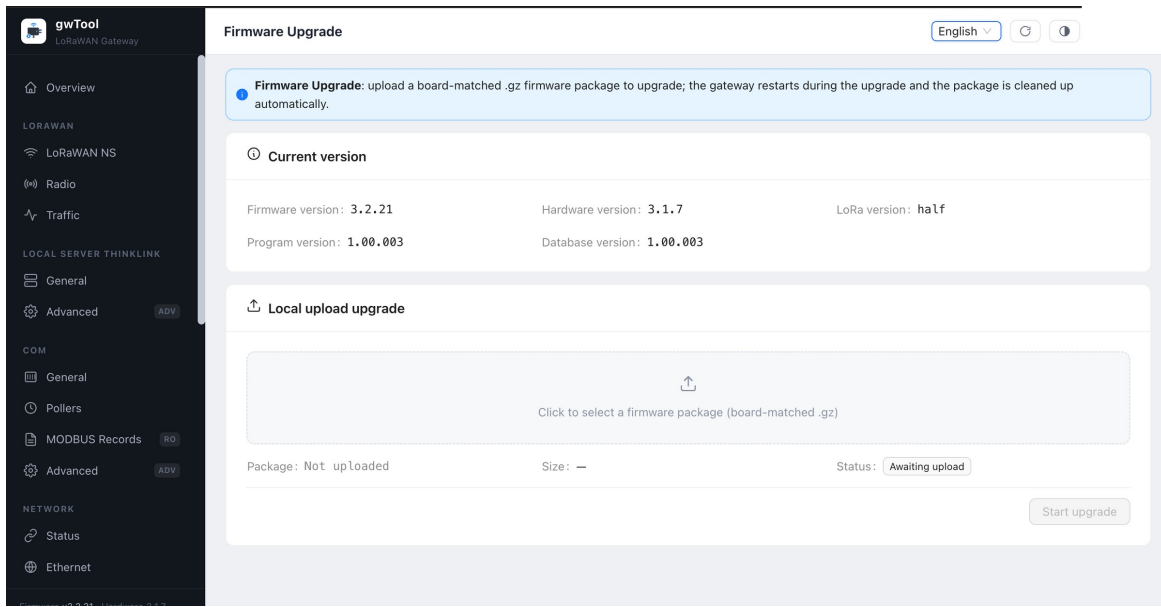


Figure GD7 English Firmware Upgrade page

Figure 23: Firmware version and package selector.

Use only an approved .gz firmware package named for the target board. The gateway reboots during firmware upgrade. Do not remove power, close the page, or change networks; after recovery, verify version, network, LoRaWAN, ThinkLink, and COM operation.

NOTE The four package types are not interchangeable. Do not upload packages with an unknown source, failed checksum, or mismatched model. Stop repeated attempts after a failure and retain the logs.

9. Maintenance

9.1 Self-check

Navigation: MAINTENANCE → Self-check

Self-check evaluates system resources, service state, business health, and network links, and groups results as pass, attention, failure, or information.

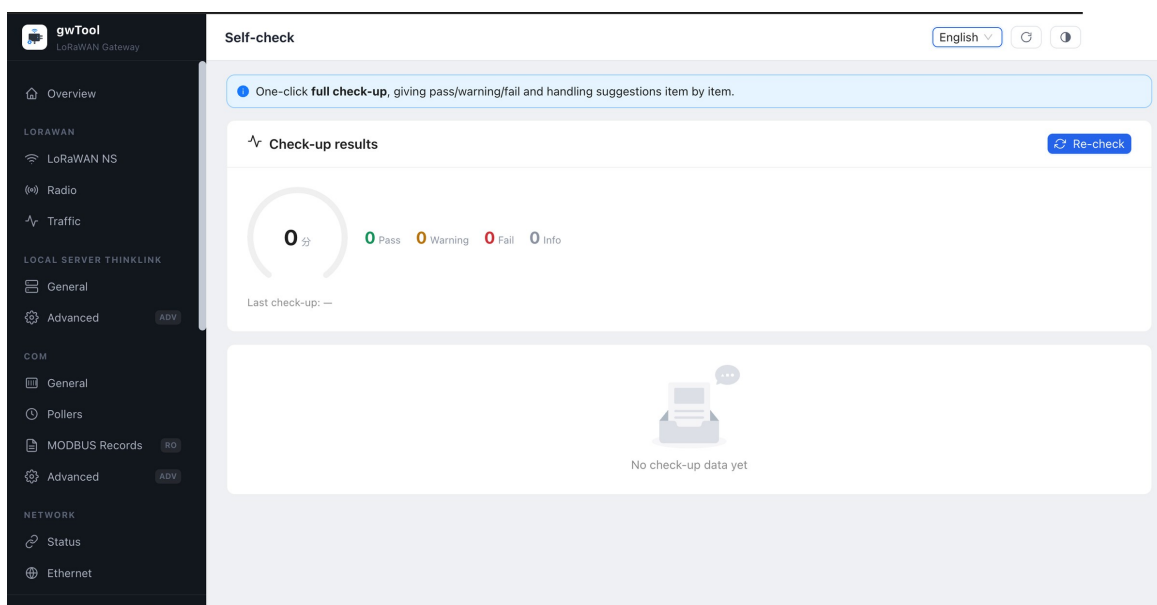


Figure GD7 English Self-check page

Figure 24: Initial state before a health check. The capture did not trigger the self-check action.

Procedure and verification: Run the check only when business conditions permit, wait for every group to complete, resolve failures before attention items, and retain only redacted results. A passing self-check does not replace end-to-end traffic and platform verification.

9.2 System Logs

Navigation: MAINTENANCE → Logs

Use the log viewer to select a file, read from the tail or head, filter by keyword, control live refresh, and download logs.

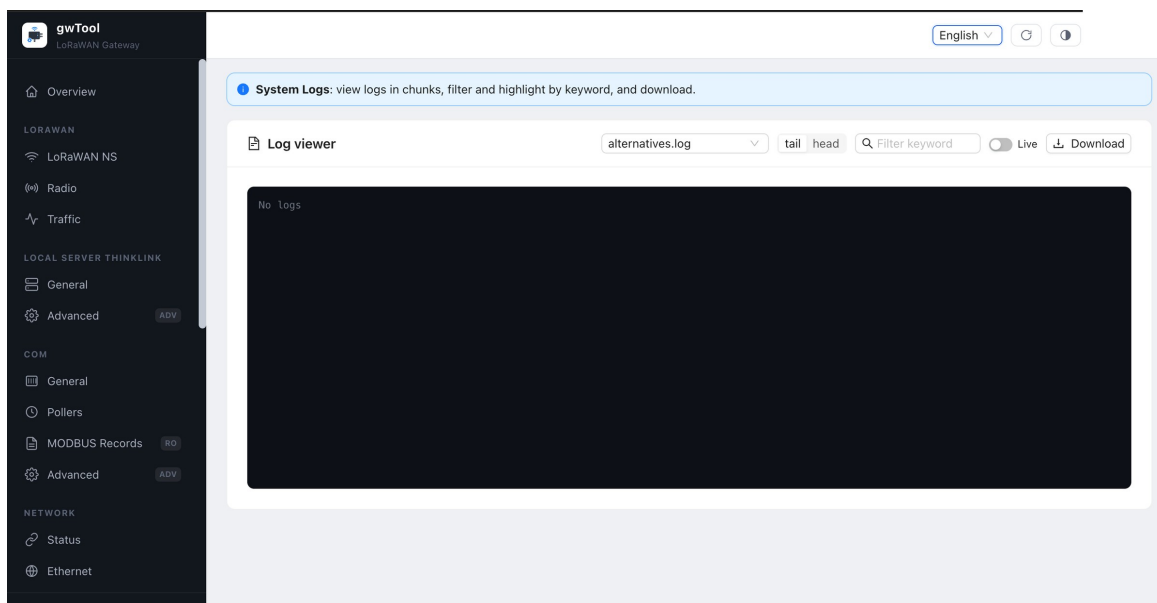


Figure GD7 English System Logs page

Figure 25: Log viewer with no displayed entries.

Procedure and verification: Select the log for the affected module, start from `tail` for recent events, filter by time and error keyword, and download only when offline analysis is required. Turn off **Live** before leaving the page.

NOTE Logs may contain addresses, device identifiers, accounts, or business data. Review and redact them before downloading or sharing.

9.3 Terminal

Navigation: MAINTENANCE → Terminal

The page provides an authenticated WebSocket terminal to the gateway SSH service for separately authorized diagnostics.

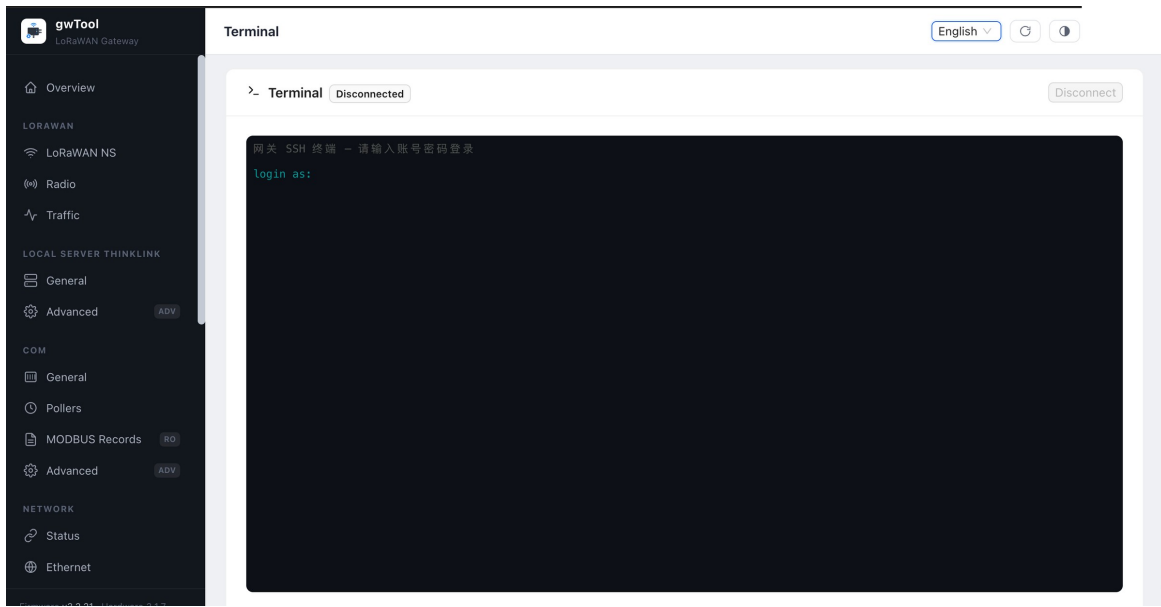


Figure GD7 English Terminal page

Figure 26: Terminal sign-in prompt. No username, password, or command was entered during capture.

Controlled use:

1. Obtain change authorization and define permitted read-only commands, recording requirements, and exit conditions.
2. Confirm the target device identity after signing in and perform only the minimum necessary checks.
3. Record only required output, disconnect explicitly, and close the page when finished.

NOTE Terminal access can bypass web-interface safeguards. This manual does not authorize shell operations, service control, or device control; execute only commands approved under a separate

9.4 Services and Gateway Reboot

Navigation: MAINTENANCE → Services

Purpose

The Services page shows service state, auto-start setting, and uptime. It also provides per-service controls, full-gateway reboot, and an automatic reboot schedule. The screenshot focuses on the highest-risk reboot area.

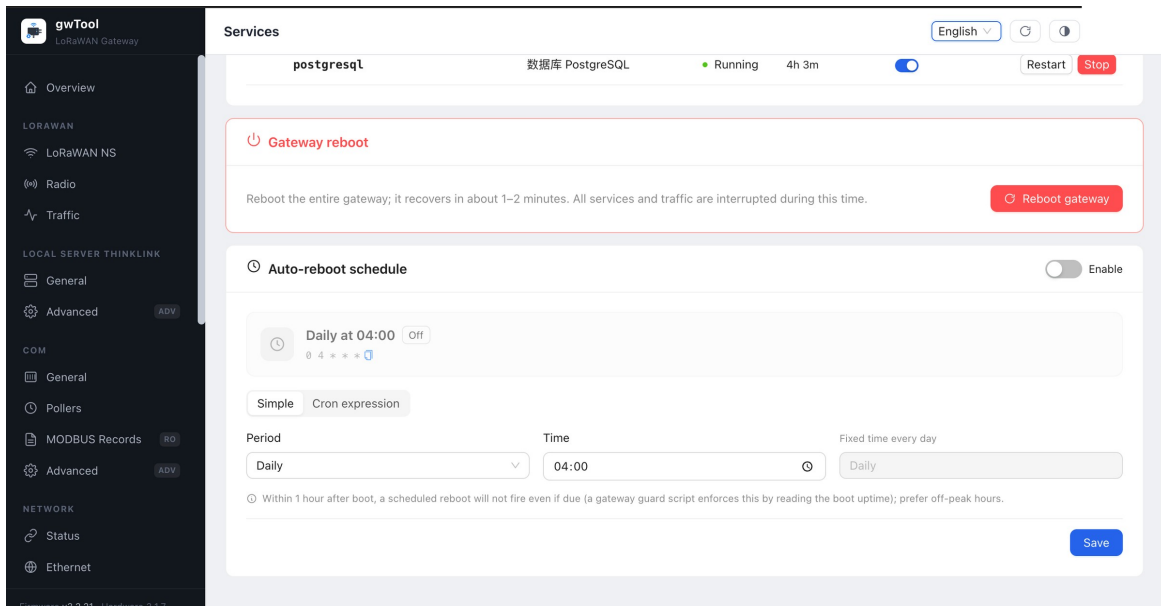


Figure GD7 English gateway reboot area

Figure 27: Gateway reboot and automatic reboot schedule. No reboot or save action was performed during capture.

Service Status Check

1. Review service **Status** and **Uptime**.
2. Record the name, state, uptime, and observation time for an abnormal service.
3. Use **Refresh** to rule out a transient display state.
4. Do not change auto-start or start, stop, or restart a service before confirming dependencies.

Manual Gateway Reboot

1. Notify stakeholders and schedule at least a 1–2 minute interruption window.
2. Confirm that no upgrade, configuration write, or critical data transfer is in progress.
3. Record the current management address and critical-service states.
4. Select **Reboot gateway** and follow the confirmation prompt.
5. Wait for recovery, sign in again, and verify Overview, network status, and critical services.

Automatic Reboot Schedule

- **Enable** determines whether the schedule is active.
- **Simple** generates a schedule from period and time; **Cron expression** is intended for administrators familiar with cron.
- The page states that a scheduled reboot is suppressed during the first hour after boot.

- Select an off-peak time and verify the gateway time zone before saving.

NOTE Reboot interrupts all services and traffic. An incorrect schedule can create recurring outages; verify recovery at the next approved schedule window.

Verification and Recovery

- After a manual reboot, wait for the gateway to recover, sign in, and check Overview, network, and service status.
- After saving a schedule, reopen the page and verify enabled state, displayed time, and cron expression.
- If the gateway does not return, inspect power and connectivity and follow the site recovery procedure. Do not issue repeated reboot requests.

10. General Safety and Recovery

- Record current values and firmware versions before changes, and retain an approved configuration backup when appropriate.
- Change one functional area at a time and verify the result immediately after saving.
- Schedule network, service, upgrade, and reboot work in a maintenance window with a tested rollback path.
- A fault record should include time, page, before-and-after state, and actions already taken. Exclude passwords, tokens, and unique device identifiers.
- If the interface differs from this manual, treat the current formal interface and version-specific documentation as authoritative. Stop uncertain high-risk work and escalate for confirmation.

Revision: 2026-08-04. English administrator manual 1.0 covers the sign-in page and all 26 formal application pages.