User Guide | IRIS WG0610-A01-ADE | LoRaWAN EU863-870

Version document	V1.0
Area	LoRaWAN EU863-870
Etat	Terminé
Produit/Service	IRIS
Zone	LoRaWAN EU863-870

PRODUCT INFORMATION AND REGULATORY INFORMATION

This User Guide applies to the following product:
IRIS LoRaWAN Gateway
Reference: WG0610-A01-ADE
APP Version: V1.0.x

DOCUMENT INFORMATION	
Title	IRIS LoRaWAN Gateway - User Guide
Type	User Guide
Version	1.0

DOCUMENTATION GUIDE

DECLARATIONS OF CONFORMITY

DECLARATION UE DE CONFORMITE - WG0610-A01_V3_WebdynEasy LoRaWAN - IRIS.pdf

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Purpose, Audience & What you will Achieve

This User Guide explains how to deploy the IRIS LoRaWAN Gateway from unboxing to first uplink, then how to operate and maintain it safely over time. You should be comfortable with IP networking basics (static IP vs DHCP, HTTPS, TLS certificates) and with the fundamentals of LoRaWAN (end-devices, gateways, network server, application server).

By the end of the “First Run” sequence you will have:

- Established backhaul connectivity (Ethernet or cellular),
- Secured access to the gateway,
- Selected a forwarding approach (Packet Forwarder via UDP or Basics Station, or Embedded LNS),
- Verified the first join and the first uplink.

1.2. General Description of the IRIS Gateway

The **IRIS LoRaWAN Gateway** is a high-performance, next-generation solution developed by Adeunis for **smart building applications** and **IoT networks**.

Serving as the bridge between IoT sensors and IT or cloud platforms, the IRIS Gateway efficiently collects data from various field devices and securely forwards it to network servers and applications.

Whether you're integrating it into an existing LoRaWAN network or using it to build a new one, the IRIS Gateway offers great flexibility and scalability.

The gateway supports **two operational modes** for data forwarding to a Network Server (LNS):

- **Packet Forwarder,**
- **Embedded LoRaWAN Server**.

These modes ensure flexibility in how the gateway can integrate with various LoRaWAN network architectures and meet different deployment requirements.

In **Packet Forwarder Mode,** the IRIS Gateway forwards LoRaWAN data to an **external LoRaWAN Network Server (LNS)**.

This mode acts as a bridge between the LoRaWAN end-devices and the LNS, providing seamless data transmission without complex local processing.

IRIS seamlessly integrates with major third-party LoRaWAN Network Servers such as **Actility, Loriot, and The Things Stack**, ensuring smooth data transmission across networks.

In **Embedded LoRaWAN Network Server Mode,** the IRIS Gateway operates independently, providing a **local LoRaWAN network server** with the ability to manage data routing, network operations, and endpoints management including **payloads decoding** and support of multicast downlink functions.

This mode is best suited for users who want full control over their LoRaWAN network and prefer a self-contained solution.

Distributed by www.texim-europe.com

The IRIS Gateway is an essential component for integrating IoT sensors into a range of use cases, including energy management, environmental monitoring, and predictive maintenance.

By combining affordability with carrier-grade performance, IRIS delivers a compelling value proposition, offering low-cost connectivity solutions without compromising on coverage or reliability.

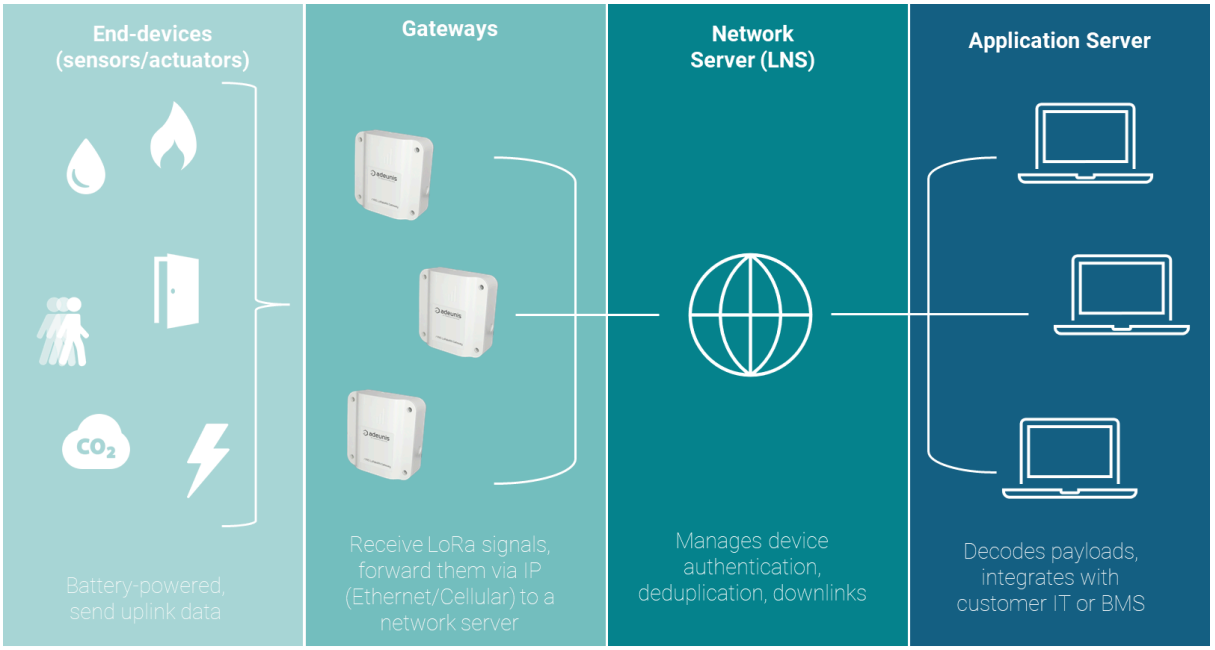
1.3. Key Features of the IRIS Gateway

- **Multi-connectivity Options**: IRIS supports both Ethernet and 2G/3G/4G cellular backhaul, ensuring reliable and redundant connectivity for critical applications. Whether connected through a fixed Ethernet cable or cellular network, the gateway guarantees continuous operation.
- **Built-in Codecs Manager**: The IRIS Gateway features an embedded codec manager, supporting both pre-configured and custom JavaScript payload decoders, simplifying data integration for different IoT sensors.
- **Scalability and Flexibility**: Supporting over 1,000 LoRaWAN endpoints, the IRIS Gateway is ideal for large-scale IoT deployments. Its flexible architecture allows it to forward data to any LoRaWAN Network Server or run a private network locally.
- **Rugged Design**: With an IP67-rated enclosure, the IRIS Gateway is designed for long-term reliability in both indoor and sheltered outdoor environments, ensuring optimal performance even in harsh conditions.
- **Security and Reliability**: The IRIS Gateway is built with robust security features including **TLS 1.2**, and **mutual authentication**, providing secure data transmission and preventing unauthorized access. Furthermore, it offers **periodic auto-reset** functionality, ensuring reliable operation at all times.
- **Made in France:** Product manufactured in France.

1.4. Where IRIS Gateway Fits in a LoRaWAN Network

The LoRaWAN network operates through a layered architecture that enables secure, reliable communication between IoT devices and backend systems.

Distributed by www.texim-europe.com



- **End-devices (sensors/actuators)**: These are the battery-powered devices, such as temperature, humidity, or motion sensors, that transmit uplinks data to the network. They communicate over LoRa, a long-range, low-power radio protocol.
- **Gateways**: They receive LoRa frames over the air and forward them over IP (Ethernet or cellular) to the LoRaWAN Network Server (LNS). IRIS sits in the gateway layer and supports Packet Forwarder with UDP or Basics Station (WSS) implementations, or, alternatively, can host an embedded LNS for local device management.
- **Network Server (LNS)**: This server authenticates devices, deduplicates packets from multiple gateways, manages ADR and downlink scheduling, and enforces LoRaWAN MAC behavior. It acts as a central hub that ensures data integrity and security.
- **Application Server**: The final stage of the communication pipeline where the data from IoT devices is processed. The server decodes payloads from the network server and integrates the data with customer IT systems/BMS (Building Management Systems) for visualization, alerts or control.

This architecture ensures flexibility, scalability, and secure data transmission, making it ideal for a wide range of IoT applications.

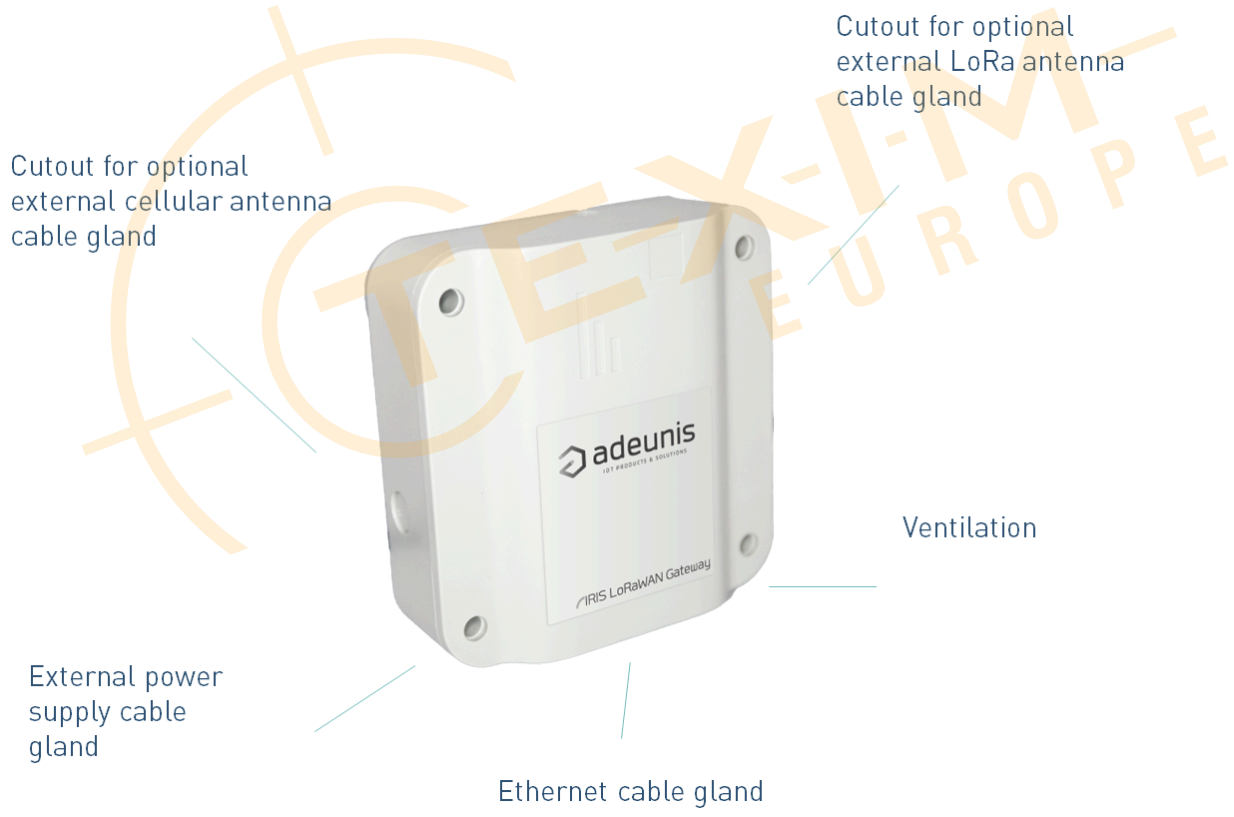
2. SPECIFICATIONS

Distributed by www.texim-europe.com

The compact, rugged housing protects the radio and network electronics while providing cable entries for power and backhaul. An RJ-45 port offers 10/100Base-T Ethernet. Power is supplied via the dedicated DC input. A SIM slot is available inside the enclosure for cellular backhaul. The radio subsystem includes an internal LoRa antenna; an external antenna option may be used where permitted and beneficial for coverage.

2.1. The Box

The **IRIS LoRaWAN Gateway** features an IP67-rated white enclosure to ensure long-term reliability in both indoor and outdoor environments.



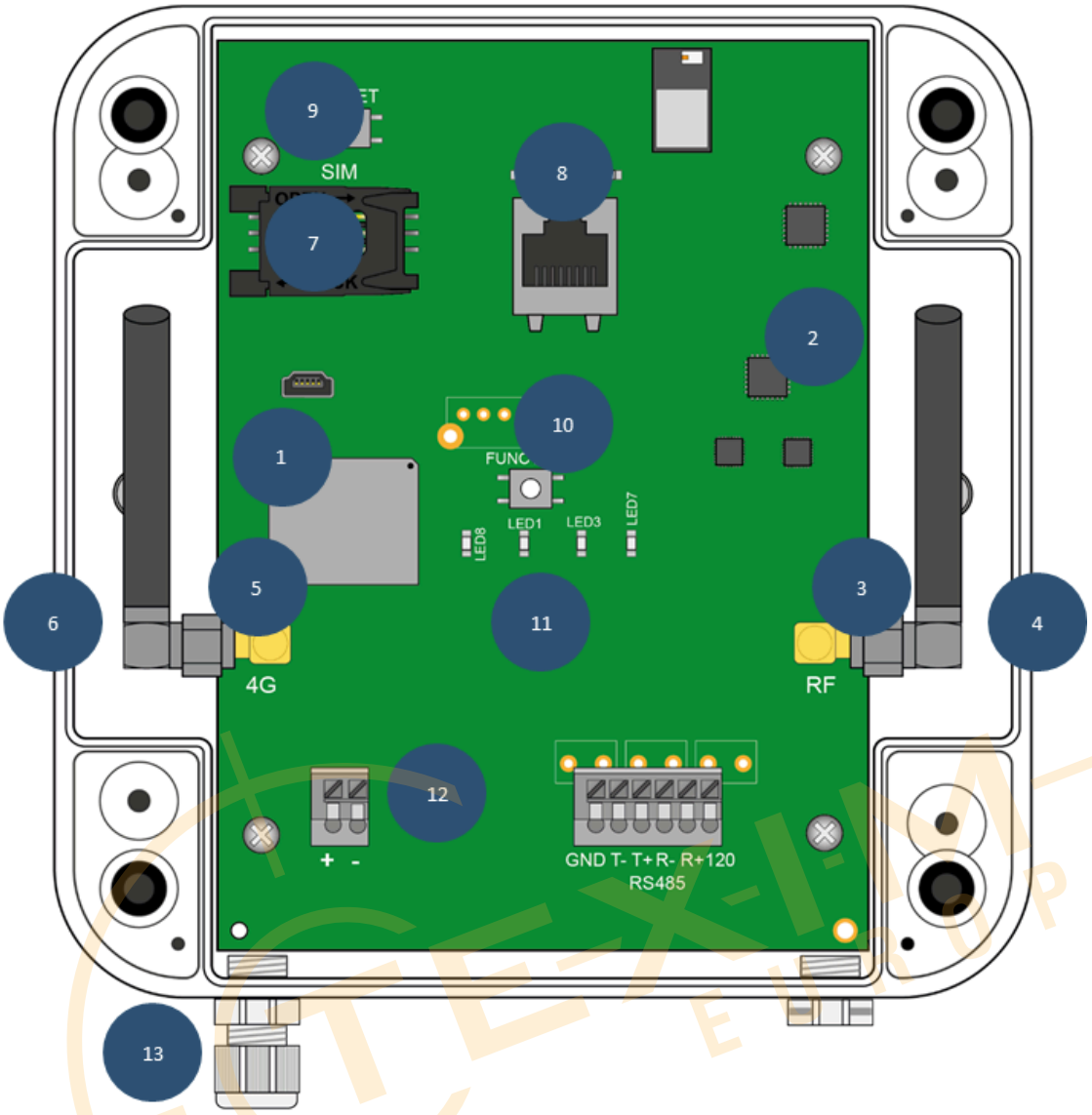
Physical Characteristics	
Box	IP67

Distributed by www.texim-europe.com

Physical Characteristics	
Material & Color	PC V0, White
Installation	Wall, desktop, DIN-rail mounting

Operating Conditions	
Operating Temperature	-20°C / +55°C
Storage Temperature	-20°C / +70°C
Relative Humidity	25% / 75% HR

2.2. The Electronic Board



1. IoT Module: Sierra Wireless WP7607-1
2. Concentrator: SEMTECH SX1302
3. Internal LoRaWAN SMA antenna
4. Box output for the LoRa RF radio external antenna (option)
5. Internal 2G/3G/4G SMA antenna
6. Box output for the 2G/3G/4G modem external antenna (option)
7. SIM card holder
8. RJ45 WAN port (PoE not supported)
9. Reset button
10. Function button
11. LED indicators (power, factory reset)
12. Terminal block for external 12/24V power supply
13. Box output for external power supply

2.3. Dimensions and Weight

Physical Characteristics	
Dimensions	160 × 150 × 55mm
Weight	450gr

2.4. Technical Specifications

2.4.1. Hardware

Hardware System	
IoT Module	Sierra Wireless WP7607-1
Memory	150 MB DDR2 RAM

Distributed by www.texim-europe.com

Hardware System	
Flash	150 MB NAND

LoRaWAN Interface	
Concentrator	SEMTECH SX1302
Channel	8 (Half-Duplex)
Antenna	1x internal LoRa antenna, Box output for external antenna (option)
Frequency Band	EU 868
Sensitivity	-141dBm (125kHz in SF12)
Tx Power	+14dBm max.
Protocol	1.0.x and 1.1.x
Class Support	Class A/C

Ethernet Interface	
Port	1x RJ-45 WAN port (PoE not supported)
Physical Layer	10/100 Base-T (IEEE 802.3)
Data Rate	10/100Mbps (auto-sensing)
Interface	Auto MDI/MDIX
Mode	Full or Half duplex (auto-sensing)

Cellular Interface	
IoT Module	Sierra Wireless WP7607-1
Network	2G/3G/4G LTE
3G Bands	HSPA+, UMTS (B1, B8)
4G Bands	Cat-1 (B1, B3, B7, B8, B20, B28)
Tx Power	23 dBm
Antenna	1× 2G/3G/4G internal antenna, Box output for external antenna (option)
SIM Slot	1x internal mini SIM-2FF

Power Supply	
Power Input	12/24V DC from an external power supply

Buttons	
Reset Button	Gateway reboot (hard reset)

Buttons	
Function Button	Factory reset **Procedure:** - Disconnect the gateway from the main power supply, - Press and hold the button , - Reconnect the gateway to the main power supply while keeping the button pressed, - Wait approximately 1 minute (until the LEDs start flashing), - Release the button, - The device will restart and the LEDs will stop flashing.

LEDs	
LED #8	Lights when the gateway is powered
LED #1	Flashes when the gateway starts a factory reset procedure and continues to flash throughout the entire process
LED #3	Flashes when the gateway starts a factory reset procedure and continues to flash throughout the entire process

2.4.2. Software

LoRaWAN	
LoRaWAN	LoRaWAN 1.0.x and 1.1.x specification LoRaWAN Packet forwarder LoRaWAN Network server Max endpoints supported: around 1,000 (depending on UL/DL frequencies) Supports Class A/C endpoints
Packet Forwarder	
Type	Semtech UDP forwarder LoRa Basics Station TCP forwarder
Compatibility	Seamless integration with mainstream 3rd party LNS: Actility, Loriot, The Things Stack, Chirpstack, etc.
Embedded Network Server	
Provisioning	One-by-one, bulk import of LoRaWAN endpoints for easy deployment
Configuration	Remote configuration for LoRaWAN endpoints via downlink

Distributed by www.texim-europe.com

LoRaWAN	
	Support multicast downlink
Data Decoding	In-built Adeunis payload decoder library Support custom payload decoder setup (JavaScript)
Gateway Fleet	Can work as a Network Server with multiple Packet Forwarding gateways connected (UDP protocol)
Integration	MQTT/s, HTTP/s protocols for data transmission to application server

Network	
Configuration	Supports 2G/3G/4G communication with WAN mobile IP assignment Network selection options Display network status Confgurable APN Keep alive functionality
Protocols	Packet forwarder: UDP, WS, WSS Network server: MQTT/s, HTTP/s Webserver: HTTP/s Clock synchronization: NTP Others: DHCP, DNS, ARP

Security & Firewall	
TLS	1.2, mutual authentication
Access Control	For local/remote access to Web GUI
Firewalls	Access control, Filtering (IP)
Certificate	CA root certifcates management

Reliability	
Autoreset	Configurable periodic Autoreset
Diagnostics	Log server

Device Management	
Configuration	Update, Backup, Restore, Recover configuration via Web GUI
Firmware Update	via Web GUI
Factory Reset	via Web GUI or via Reset button

Certifications	
Certifications	CE, RED, RoHS, REACH

Distributed by www.texim-europe.com

3. UNBOXING, INSTALLATION AND STARTUP

Start by checking the box contents against the packing list and inspect the enclosure for shipping damage.

Choose a mounting location that affords a clear RF path. The gateway can be wall-mounted or installed on DIN-rail with an optional kit. Keep the LoRa antenna as free as possible from metal obstacles and far from dense cabling bundles. Route the power and Ethernet cables and tighten glands to maintain the IP seal.

Connect the DC power supply. If you use cellular backhaul, insert the SIM carefully (contacts oriented as marked) while the unit is powered off.

3.1. Unboxing

3.1.1. Box Contents

Start by checking the box contents before starting any installation work. If there are missing or damaged items, contact Adeunis support.

The cardboard packaging contains the following elements:

- IRIS Gateway
- Curved SMA antenna for the modem (internal)
- Curved SMA antenna for the radio (internal)
- A power adapter
- An Ethernet cable connector

The following accessories can be supplied as options:

- External antenna for the modem
- External magnetic antenna for the radio
- External Omni FIBERGLASS antenna for the radio
- DIN Rail Mounting kit

3.1.2. Identification Label

The gateway can be identified from its identification label located on the box.

This label features:

- Device name
- The date of manufacturing (WW/YY format)
- The serial number in character and 128 barcode format
- The MAC (Ethernet) address in character format

3.1.3. Software Version

The software version can be found on the gateway Web GUI. The software version is given on the “Status” tab.

3.2. Assembly

It is important to comply with the operating conditions described in this User Manual before installing, as well as the following conditions:

- Protect the product from dust, moisture, aggressive substances and corrosion.
- If the Modem connection is used, make sure there is optimum reception when installing. Check the RSRP which is available on the Web GUI “Status” tab.
- To optimize Modem and LoRa radio reception sensitivity, it is essential to leave 20 cm free space around the antennas.

3.2.1. Opening/Closing the Box

Distributed by www.texim-europe.com

To open the gateway box

If the box is wall-mounted:

1. Open the 2 doors on the front panel.
2. Unscrew the 4 wall mounting screws in the recesses under the doors.

Then follow these steps:

1. Unscrew the 4 screws behind the box.
2. Remove the cover.

To close the gateway box

1. Place the cover on the box base, make sure the seal is properly fitted.
2. Screw in the 4 screws on the back of the box.

3.2.2. Cellular Antenna and SIM Card

Cellular Antenna Connection

The gateway has a female SMA connector labelled “4G” on the board to connect a modem antenna.

The gateway is delivered with an internal antenna.

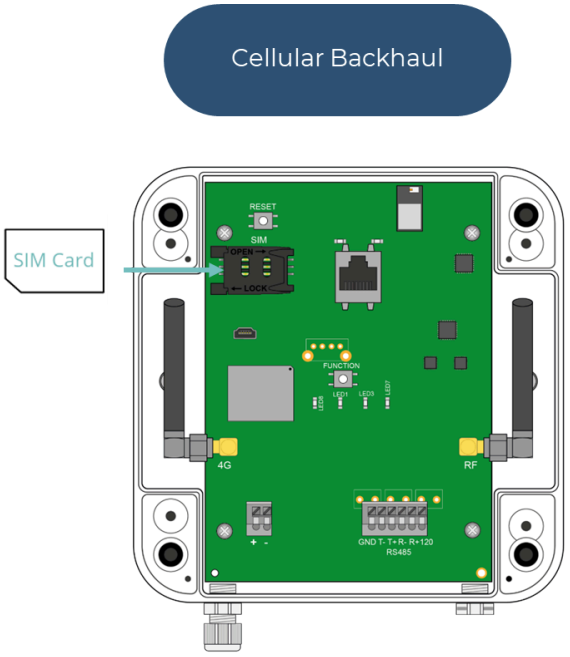
An external antenna can be connected to the gateway. To do this, unscrew the cap on the box and fit a M16*1.5 cable gland (not included).

If the gateway is installed in a metal box or in a location that does not have proper signal reception, the use of a remote antenna is strongly recommended. Be careful to use an antenna compatible with the connector and frequencies used.

SIM Card Insertion

To use the modem connection to communicate with the remote server, the gateway must be opened and a mini SIM card inserted into the SIM card housing on the PCB board.

Distributed by www.texim-europe.com



To insert the SIM card into the product:

1. slide the holder flap to the right (in the OPEN direction).
2. Slide the SIM card into the flap.
3. Then close the flap by sliding it to the left (in the LOCK direction)

By default, the gateway configuration does not request a PIN code.

If you want to enable the PIN code, it is preferable to configure it via the Web GUI before the SIM card is installed.

There are three possibilities:

- The PIN code is disabled: modem communication is active.
- The PIN code is enabled and the entered PIN code is correct: modem communication is active.
- The PIN code is enabled and the entered PIN code is incorrect: modem communication is in error.

📌 If the SIM card has an enabled PIN code and it is incorrect the first time the gateway is started , it will be blocked after 3 attempts.
It can be unlocked using a mobile phone using the PUK code provided by the operator

3.2.3. LoRaWAN Antenna

Distributed by www.texim-europe.com

LoRaWAN Antenna Connection

The gateway has a female SMA connector labelled “RF” on the board to connect a radio antenna.

The gateway is delivered with an internal antenna.

An external antenna can be connected to the gateway. To do this, unscrew the cap on the box and fit a M16*1.5 cable gland (not included).

📌 If the gateway is installed in a metal box or in a location that does not have proper signal reception, the use of a remote antenna is strongly recommended. Be careful to use an antenna compatible with the connector and frequencies used.

3.2.4. Wall Mounting

The IRIS gateway can be wall-mounted. Before wall-mounting, first close the box.

Choose a mounting location that affords a clear RF path. To optimize the radio range, it is important to install the radio antenna as high as possible and to place it carefully, avoiding obstacles as far as possible. As a priority, move it away from any metal (cupboard, beams...) or concrete (reinforced concrete, walls...) obstacles as they greatly attenuate radio waves.

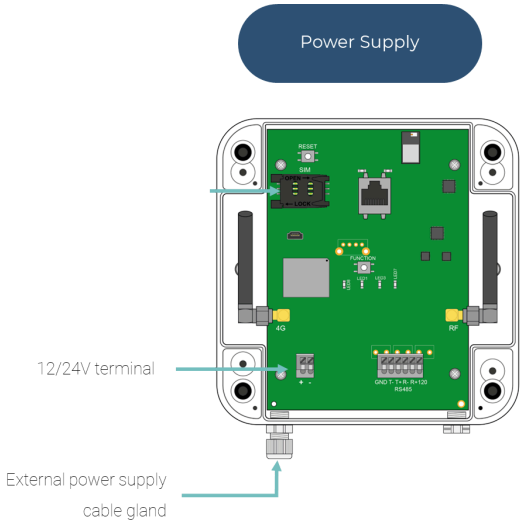
Follow the steps below to fix the gateway to a wall

1. Open the 2 doors on the front panel.
2. Screw the 4 wall mounting screws into the recesses under the doors.
3. Close both doors on the front.

📌 Screws and anchors are not included in the kit.
You must choose the correct type of screw for the type of wall you are fixing the gateway to (4 mm diameter screw, minimum length 25 mm).

Distributed by www.texim-europe.com

3.2.5. Power Supply



The IRIS gateway must have a 12V or 24V DC power supply.

Power is supplied from terminal block J11 on the bottom left side of the board.

Make sure the power supply wires are connected to the proper terminals.

Product power consumption varies depending on its configuration. Make sure the power supply used can provide a minimum power of 10 Watts

📌 End users must use a CE certified power supply of less than 15 Watts.
The distance between the power supply and the product must not exceed 3 meters.

3.3 First Access

This section explains how to power the gateway, set a temporary IP on your laptop, and access the Web GUI for the first time. Follow the steps in order.

3.3.1. Powering On the Gateway

1. **Antennas.** Ensure the **LoRa** and (if used) **cellular** antennas are connected. For radios, always connect antennas **before** applying power.
2. **SIM** (optional)**.** If you plan to use cellular backhaul, insert the SIM while the unit is powered off.
3. **Computer.** Ensure that a computer with a web browser is plugged into the gateway's Ethernet port.

Distributed by www.texim-europe.com

4. **Power.** Connect the DC power cable of the gateway to a suitable external power supply and apply power.

You can now configure the access to the Web GUI

3.3.2. Setting a Temporary Static IP

You need a temporary static IP on your laptop in the same subnet as the gateway.

> 📌 The IRIS gateway default configuration parameters are the following:
> **IP address** `http://192.168.1.2`
> **Subnet mask** `255.255.255.0`
> **DHCP** Deactivated

To configure a temporary static IP address:

1. Go to Control Panel/Network & Internet. The “Network Status” window is displayed.
2. Click on “Ethernet”.
3. The “Ethernet Status” window is displayed.
4. Select “Internet Protocol (TCP/IPv4)” then click the “Change” button.
5. Then click “Advanced”.
6. In the “IP Address” zone, enter IP address `192.168.1.xxx` (xxx between 1 and 254 and not equal to 2) and the subnet mask `255.255.255.0`
7. Save changes.
8. Close the Network connection and remote access window.
9. After commissioning, remember to revert this adapter to DHCP.

Distributed by www.texim-europe.com

It is now possible to easily modify the gateway configuration using the Web GUI.

3.3.3. First Access to the Web GUI

To access the gateway's embedded web interface:

1. Connect your laptop to the gateway's Ethernet port.
2. Open the **web browser** and **go to**: `http://192.168.1.2`
3. An identification window should be displayed
4. Configure your **password** to secure the access to the Web GUI
5. Click on "**Submit**"

📌 The gateway currently does **not** support multiple user roles: access is via the admin account.

3.3.4. Security Hardening

The first time you access the gateway we recommend to configure security and NTP (Network Time Protocol) server for preise time reference. Doing this up front prevents most connection and TLS issues later.

1. **Enable HTTPS and disable HTTP**. Enforce encrypted access to the Web GUI.

Distributed by www.texim-europe.com

5. **Configure NTP and timezone.** Configure your private or reference NTP server, or use some well-known public services such as: europe.pool.ntp.org, pool.ntp.org, time.google.com, or time1.google.com
6. (Optional) **Restrict exposure.** If the Web GUI will be reachable over a routed network, add allow-listed source IPs.

After saving, refresh the browser over HTTPS and go to the **Status** page. Check that time is correct and the Ethernet link is up.

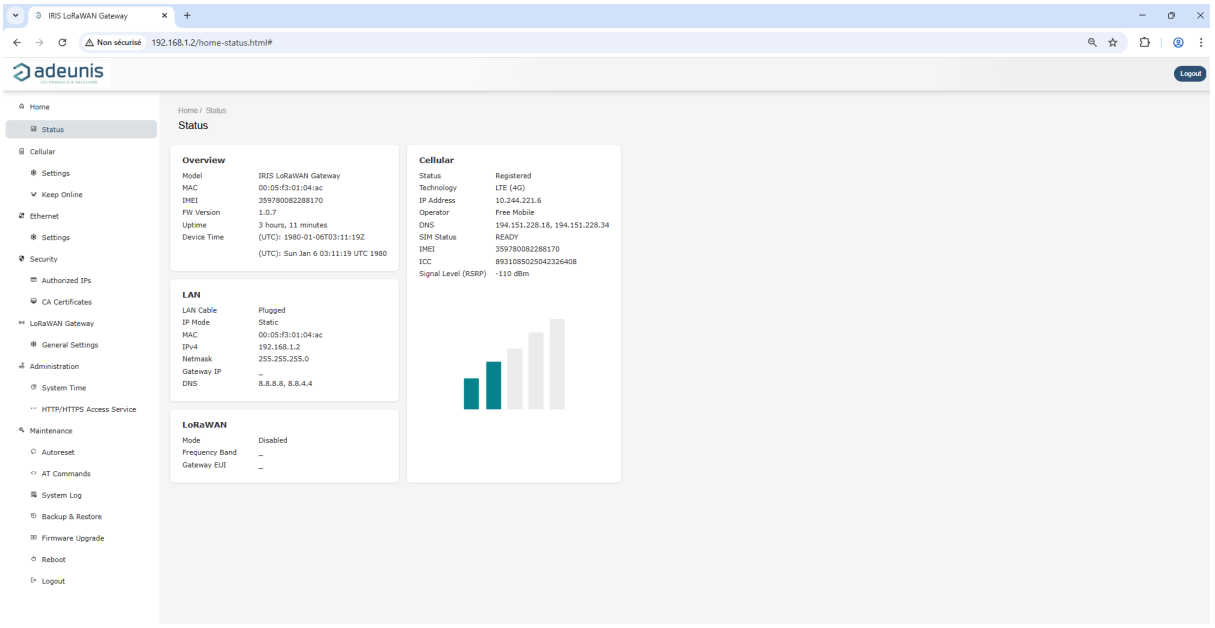
You can now proceed with gateway configuration and LoRaWAN settings.

4. GATEWAY ACCESS, CONNECTIVITY & SECURITY SETUP

4.1. Web GUI Overview

After your first login, take a moment to familiarize yourself with the Web GUI.

The interface is organized into a left-hand navigation menu, a breadcrumb at the top indicating your current location, and a main content area on the right.



Home Page

The landing page is **Home → Status**

It acts as your cockpit: you'll see an Overview card with the model, MAC/IMEI, firmware version, uptime, and device time; a LAN card summarizing cable state and IPv4 parameters; a Cellular card indicating registration state, radio technology, IP address, operator, SIM status and RSRP; and a LoRaWAN card with the current mode, frequency band, and the gateway EUI.

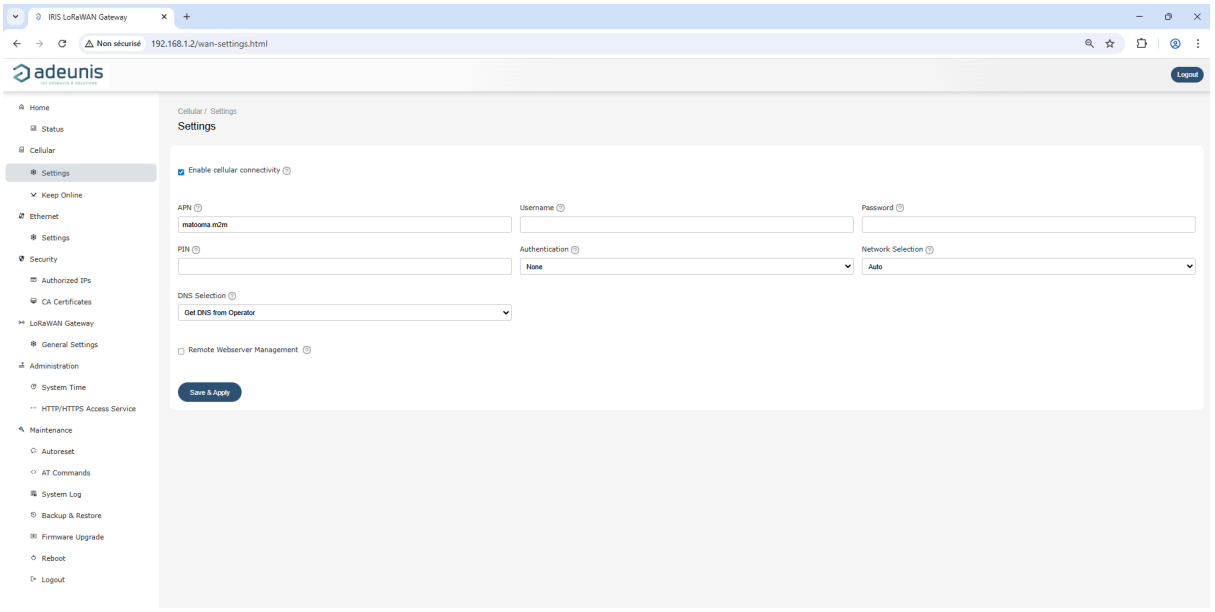
This page is read-only by design and is the quickest way to verify that power, time, and at least one backhaul are healthy before you proceed.

Navigation is grouped by function.

Cellular Section

The **Cellular** section contains the configuration for cellular backhaul. Open **Settings** to enter APN credentials and choose network selection options; use **Keep Online** to configure the connectivity watchdog that periodically pings a target and recovers the active link if it becomes unresponsive.

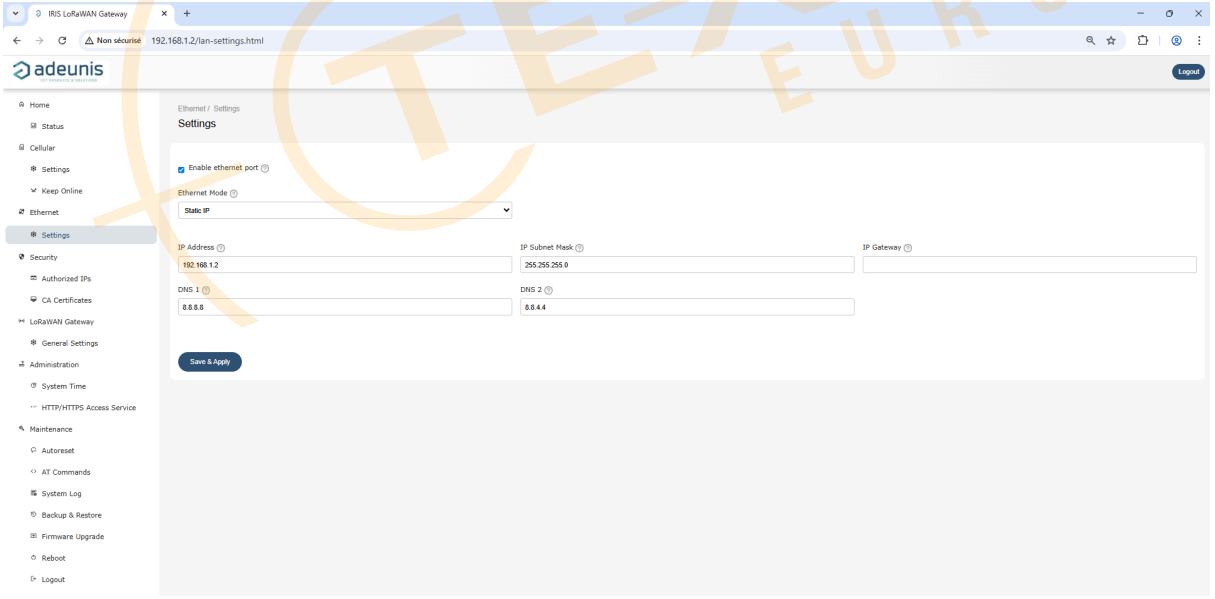
Distributed by www.texim-europe.com



To configure this interface, refer to the Cellular Settings section of the user Guide.

Ethernet Section

The **Ethernet** section provides **Settings** for DHCP or static addressing and lets you define gateway and DNS servers. Once applied, you reconnect to the Web GUI at the new address and confirm the values on the Status page.



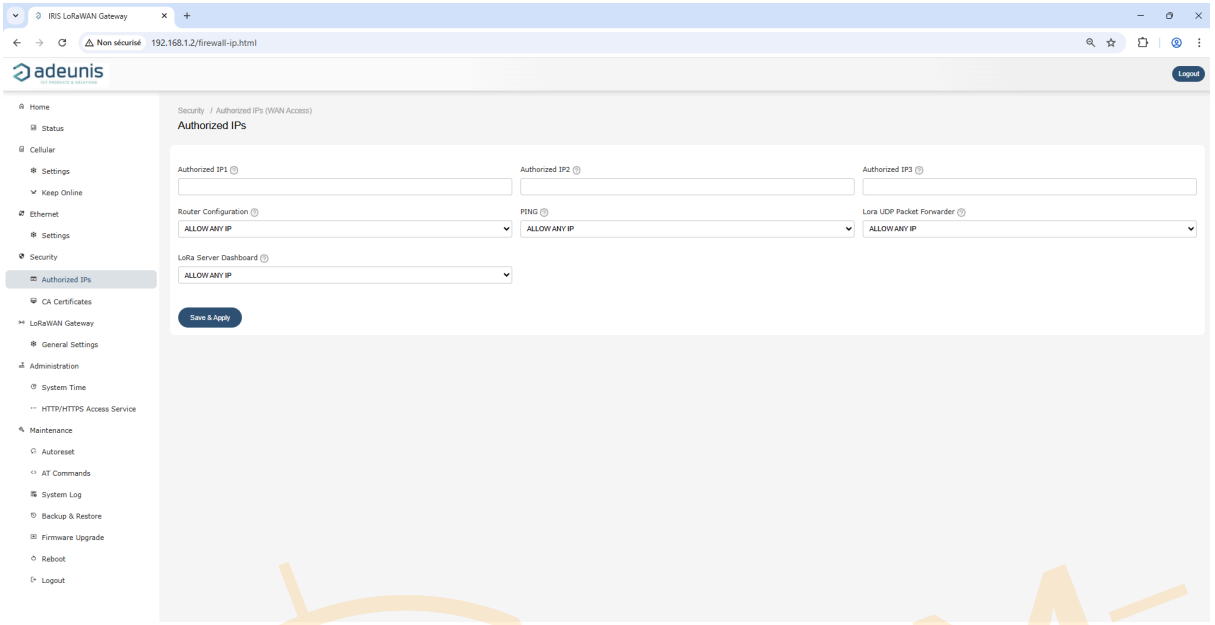
To configure this interface, refer to the Ethernet Settings section of the user Guide.

Security Section

Distributed by www.texim-europe.com

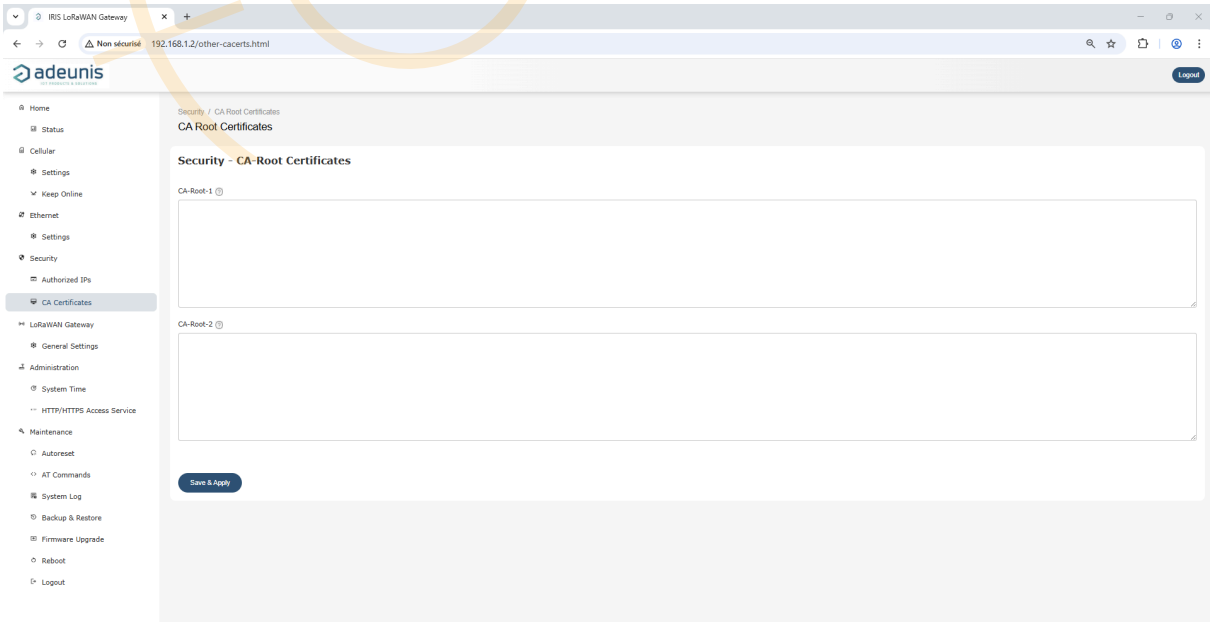
Security-related controls are grouped under **Security**.

Authorized IPs lets you restrict which source addresses may reach the administration services, which is especially important when the GUI is exposed beyond a local commissioning laptop.



To set the mobile WAN allow list, refer to the Authorized IPs section of the user Guide.

CA Certificates is the trust store the gateway uses when it must validate remote TLS servers; populate it when your LoRaWAN Network Server, MQTT broker, or HTTP server are signed by a private or enterprise certificate authority.



Distributed by www.texim-europe.com

To configure, refer to the CA Certificates section of the user Guide.

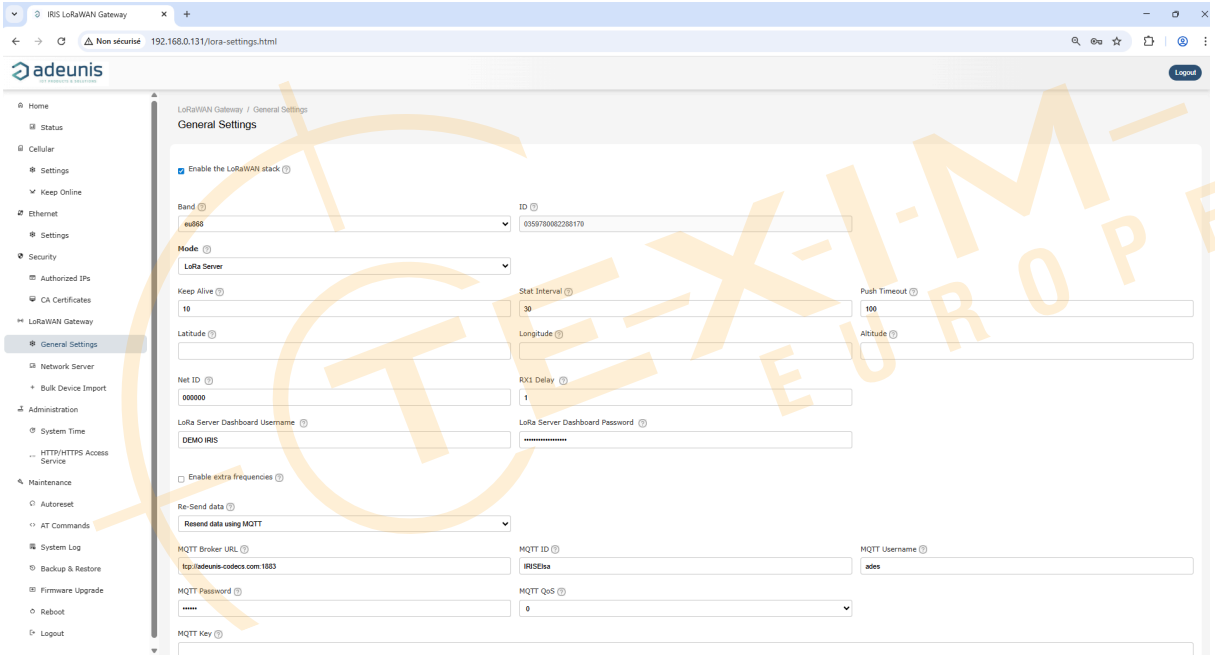
LoRaWAN Section

LoRaWAN functionality is grouped under **LoRaWAN**.

General Settings is where you choose the radio region and select how the gateway forwards traffic to a Network Server, either with Packet Forwarder using UDP or using Basics Station over secure WebSockets, or, alternatively, enable the embedded LoRaWAN Network Server.

When the embedded server is enabled, **Network Server Dashboard** opens the integrated console used to register gateways, register end devices, create applications and device profiles, and monitor frames.

For larger rollouts, **Bulk Device Import function** provides a guided import so you can provision multiple end-devices in one operation.



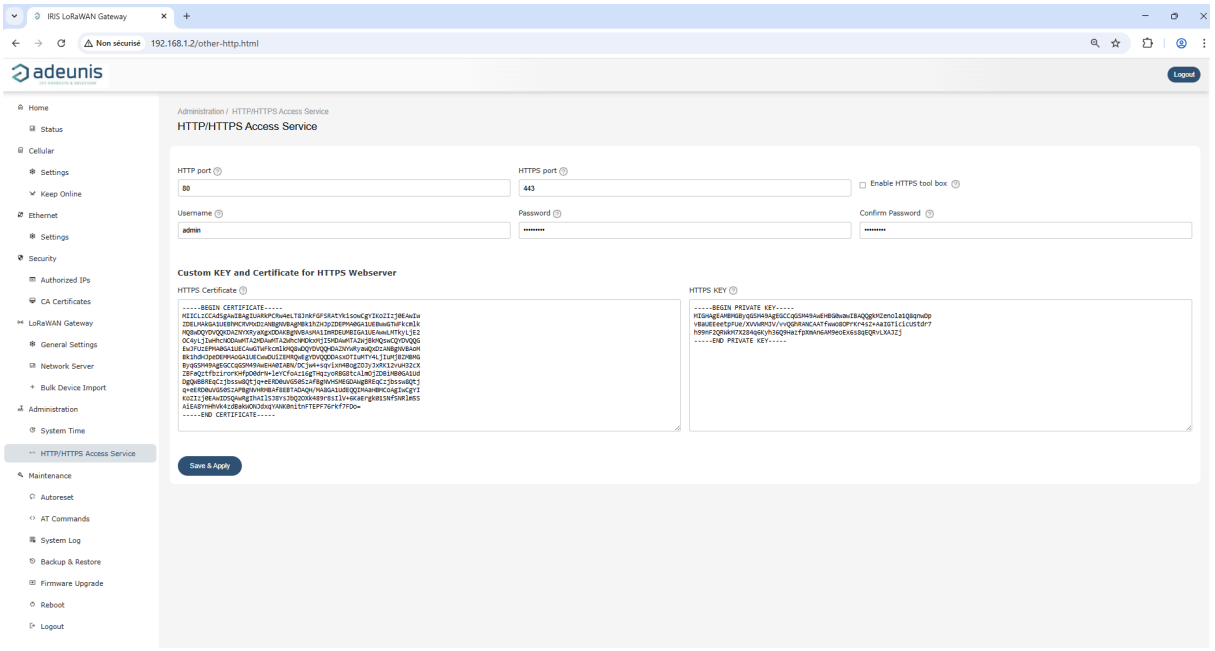
To configure the LoRaWAN interface, refer to the LoRaWAN chapter of the user Guide.

Administration Section

Administration services live under **Administration**.

In **Access Service** you define how the configuration web server is exposed. Use this page to enforce encrypted access by enabling HTTPS and, if required, installing your server certificate and private key.

Distributed by www.texim-europe.com



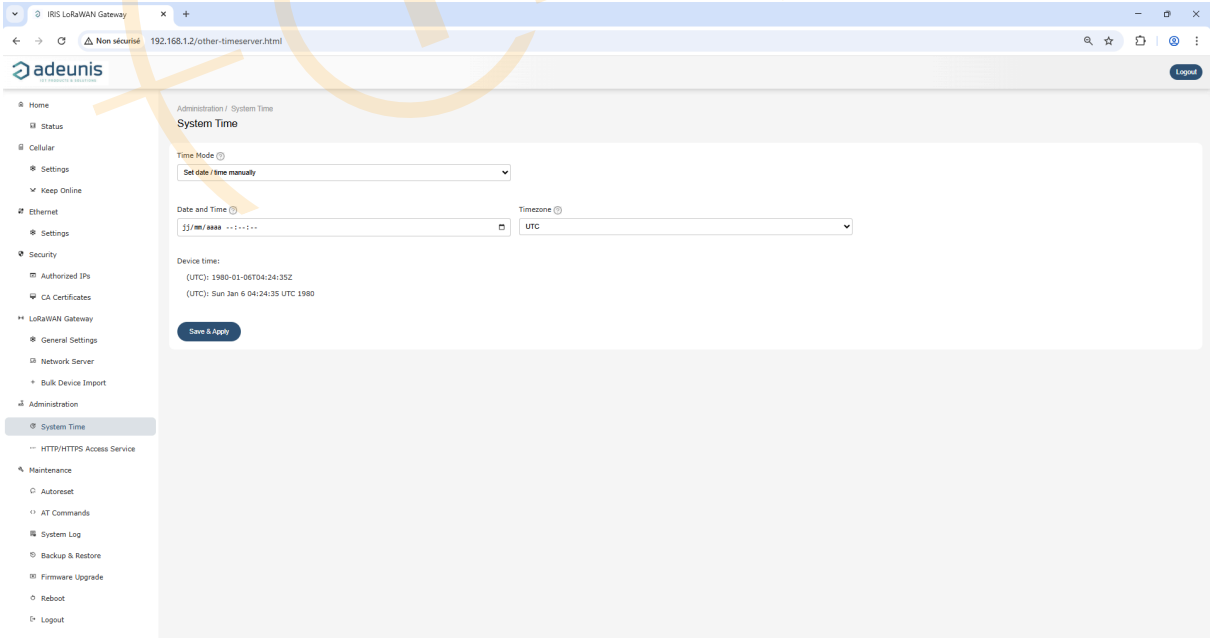
For more information, refer to the Web GUI Access section of the user Guide.

The **System Time** page lets you set the gateway's date, time, and timezone.

You may either:

- **Use NTP servers** (recommended), or
- **Set the date and time manually** when no NTP service is available.

Accurate time is essential for TLS handshakes and correct log timestamps.



Distributed by www.texim-europe.com

When using **NTP mode**, provide at least one reliable NTP server — ideally two for redundancy — and verify that the device time shown on the *Status* page matches the site's local time.

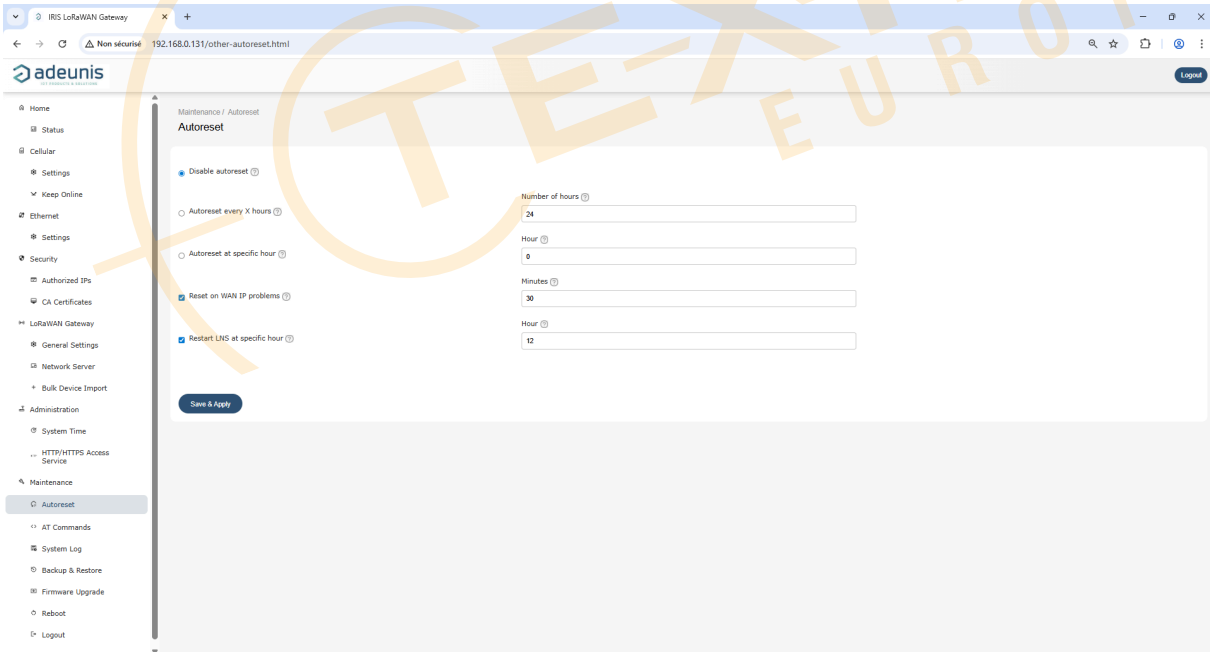
When using **Manual mode**, enter the date and time directly in the interface and select the appropriate timezone. Manual mode is intended for isolated networks or deployments where no NTP service is accessible.

To configure system time, refer to the Time Synchronization section of the user Guide.

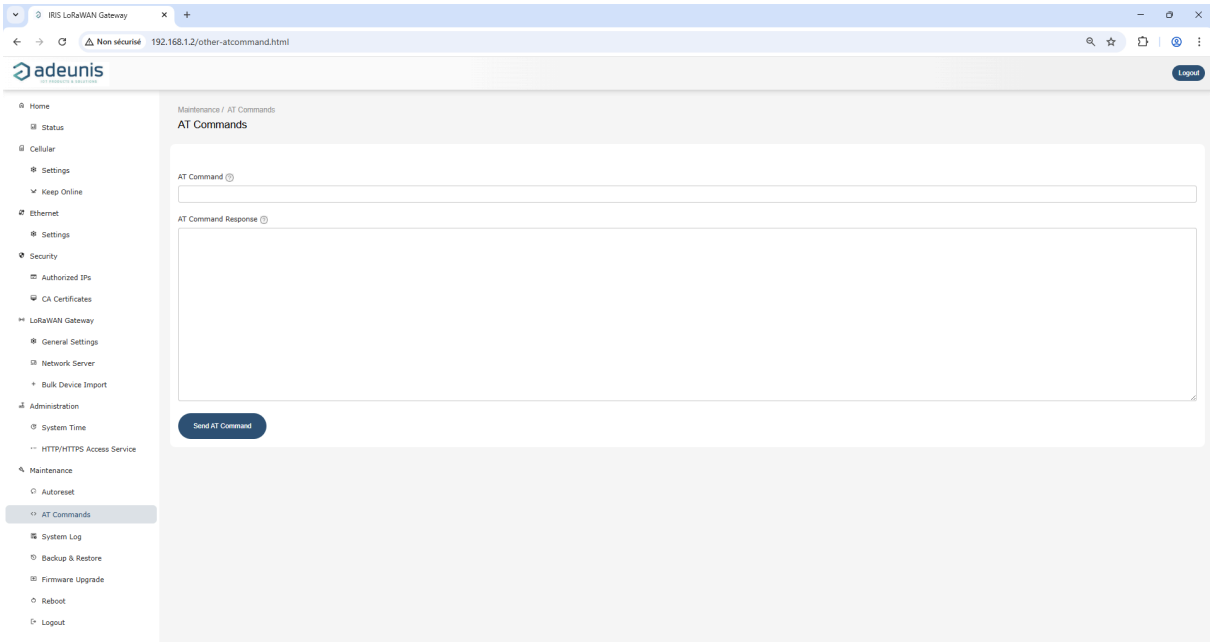
Maintenance Section

The **Maintenance** area brings together everything you need for day-2 operations: scheduling preventive reboots, running diagnostics, collecting logs, safeguarding configuration, updating firmware, and performing controlled restarts. It is the place you will return to after commissioning to keep the gateway healthy over time

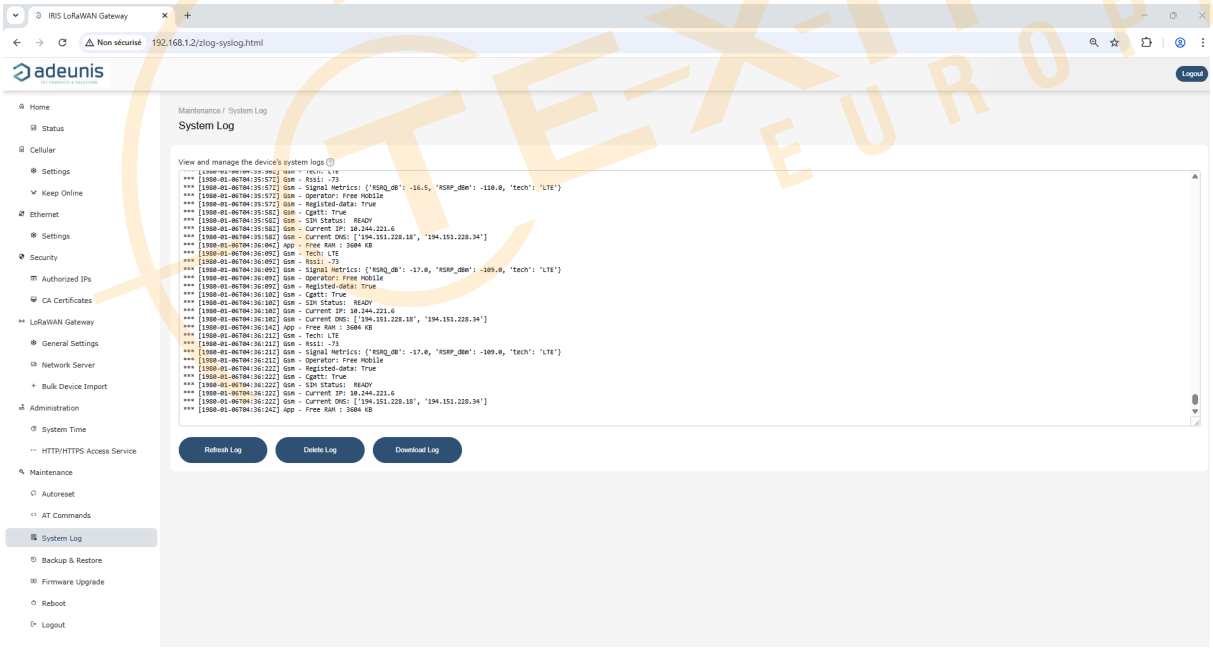
The **Periodic Autoreset** page allows you to schedule an automatic, clean reboot at a defined day and time. This is useful for unattended sites that benefit from routine housekeeping. Choose a maintenance window that does not interfere with production traffic and remember that the gateway will be briefly unavailable during the restart. If you do not have a specific operational reason, leave autoreset disabled; the platform does not require it for normal operation.



AT Commands provides a safe console to query the cellular module for diagnostics.



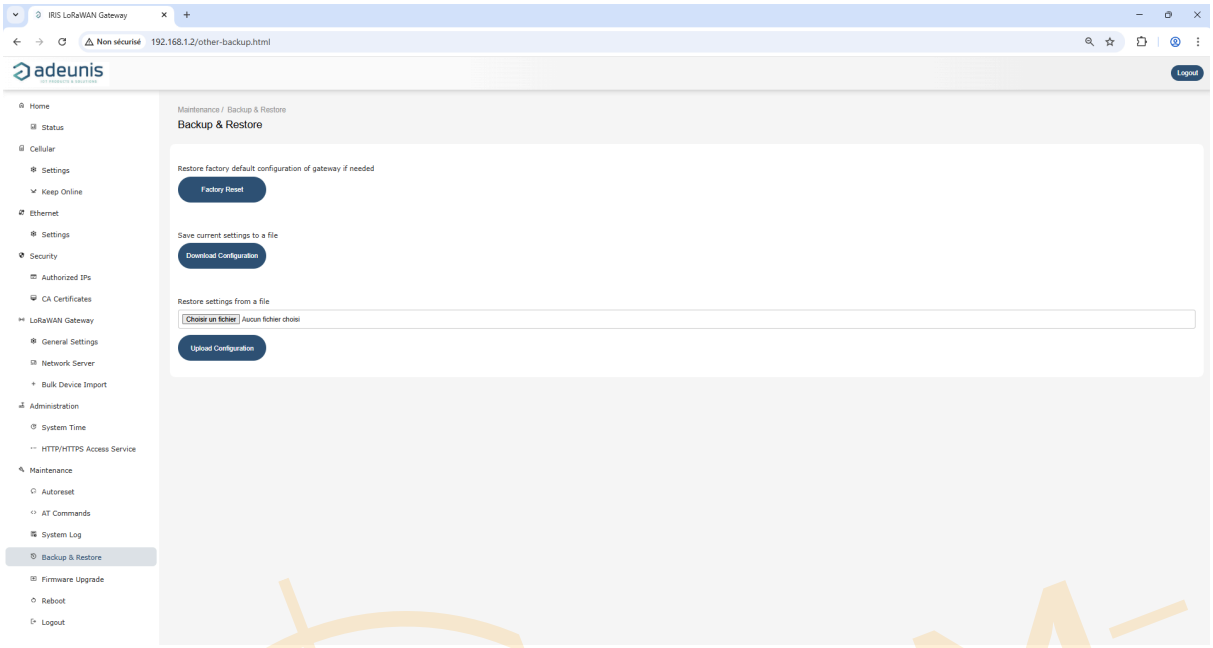
In **Syslog**, you can review recent system logs and, if needed, export the logs. Offloading logs to a central collector is invaluable for fleet-wide correlation and for post-incident analysis. Confirm that NTP is synchronized first so records from multiple gateways align correctly; then verify on your collector that entries from this device are received as expected.



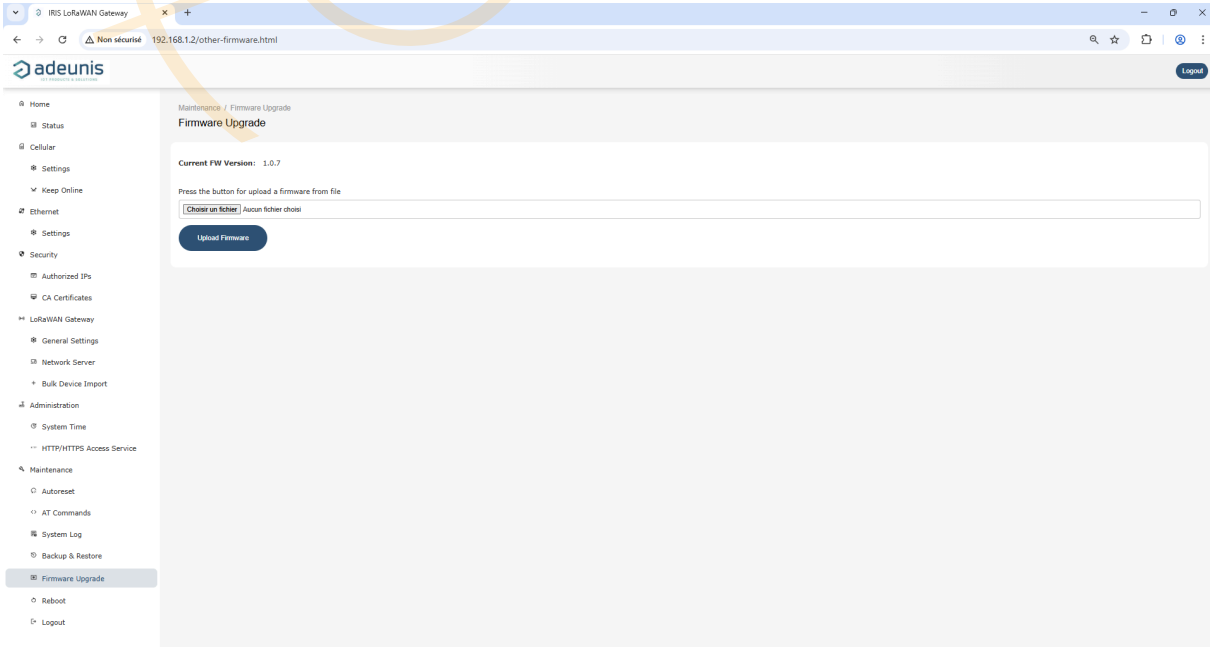
Backup & Restore is your safety net. Use **Download Configuration** to export the current configuration to a file and store it with your site documentation before any significant change. If you ever need to return to a known state, **Upload Configuration** will reapply that configuration.

Distributed by www.texim-europe.com

The **Factory reset** action returns the device to its defaults and erases custom settings; use it only when necessary and only after you have downloaded a fresh backup. A physical long-press on the “Function” button performs the same reset. Prefer the GUI when you can, because it lets you confirm the impact beforehand.

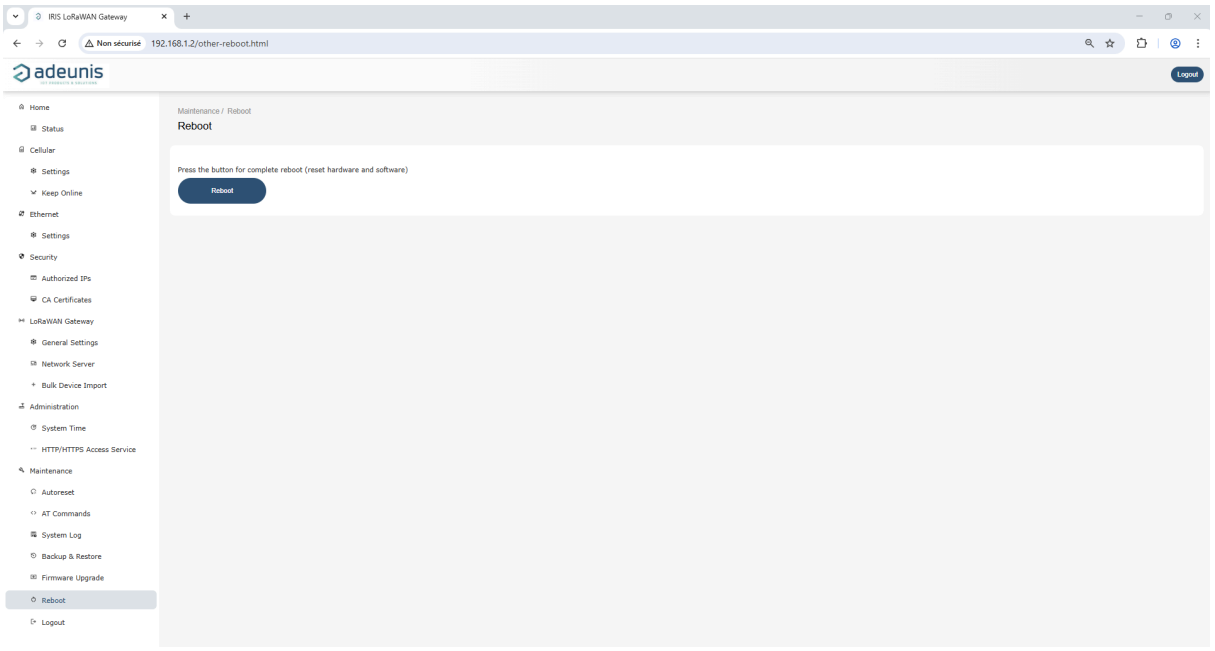


The **Firmware Upgrade** page is used to load a new software image. When you upload an image, the gateway verifies it, applies the update, and performs a controlled reboot. Do not remove power during this process. After the device restarts, open the Status page to confirm the new firmware version, check that time is synchronized, and ensure your forwarding configuration is still active. Keep a configuration backup from just before the upgrade so you can recover quickly if needed.



Distributed by www.texim-europe.com

Finally, **Reboot** performs a standard soft restart without altering configuration, and **Logout** ends the administration session and returns you to the sign-in page.



Most configuration pages follow the same interaction pattern: you edit fields in the right-hand panel, then commit changes explicitly.

> 📌 As a best practice, apply one logical change at a time, return to **Home** → **Status** to verify the expected effect, and only then move on to the next task. This rhythm—configure, save, verify—keeps commissioning predictable and makes any troubleshooting straightforward.

4.2. Network Access

IRIS offers two backhaul options to connect the gateway to your IP network: **Ethernet** or **cellular (2G/3G/4G)**.

Commissioning is usually done on Ethernet for speed and predictability, then you decide which link will remain active for operations.

Distributed by www.texim-europe.com

The objective of this section is not to describe every field on each page, but to help you make the right choices, apply them safely, and verify the result on the **Status** page.

📌 You **use one backhaul at a time,** dual-active operation for resilience is **not supported**.

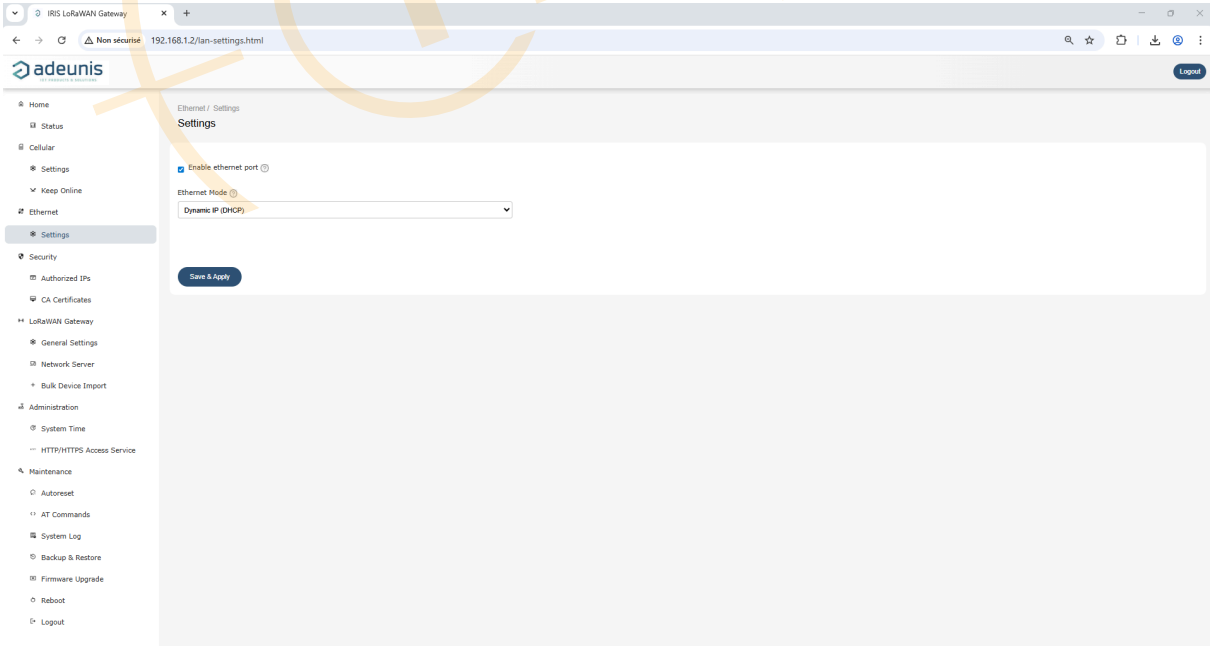
4.2.1. Ethernet Interface

Use Ethernet for first configuration and for sites where the gateway will remain on a LAN or VLAN managed by the customer.

Decide upfront with the site owner whether addressing is provided by DHCP or must be fixed.

Dynamic IP Address Settings

When **DHCP** is available, enabling it is usually the safest option: the gateway will receive its IPv4 address, subnet mask, default gateway, and DNS servers from the DHCP server.



Distributed by www.texim-europe.com

Locating the assigned IP (DHCP)

After you switch **Ethernet** to **Dynamic (DHCP)** and apply the change, the gateway requests an address from your LAN.

To discover which IP was assigned:

- **Check your DHCP/Router lease table.**

Ask your IT team to look up the lease **by the gateway's MAC address** (printed on the product label) or by the **hostname** if they maintain one for the device.

- **Use LAN scanning tools.**

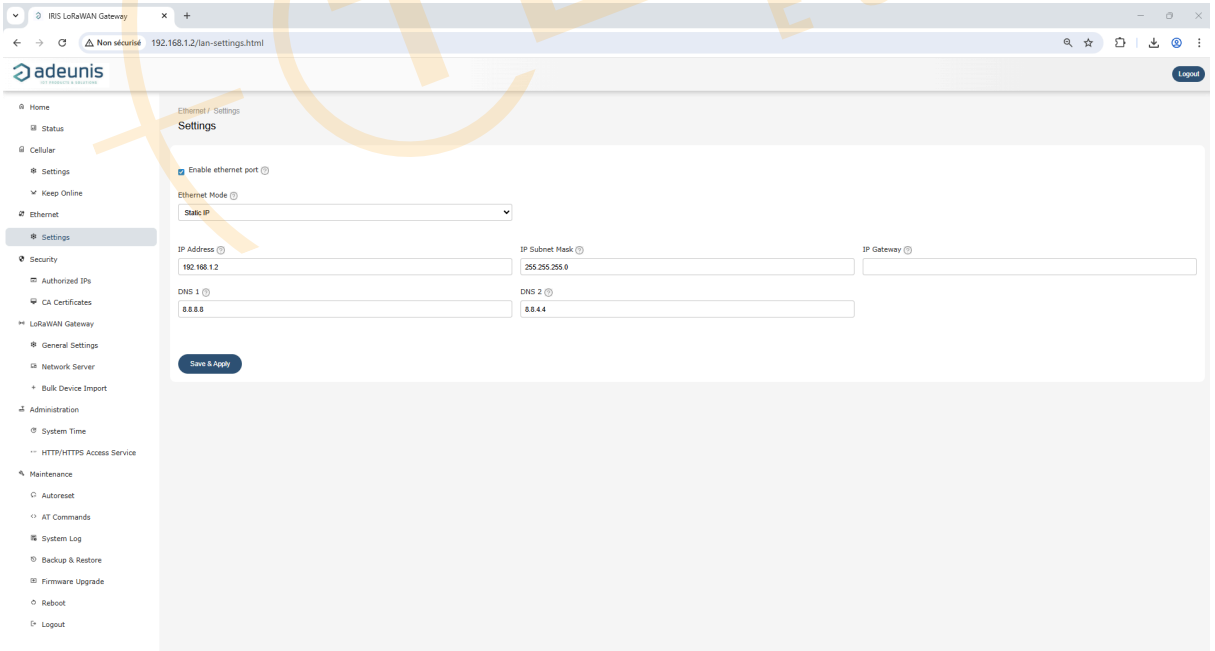
On the same subnet, inspect your ARP/neighbor table or run a network scan (e.g., `arp`, `ip neigh`, `nmap`) to identify the device by its **MAC address** and retrieve the current IP.

Static IP Address Settings

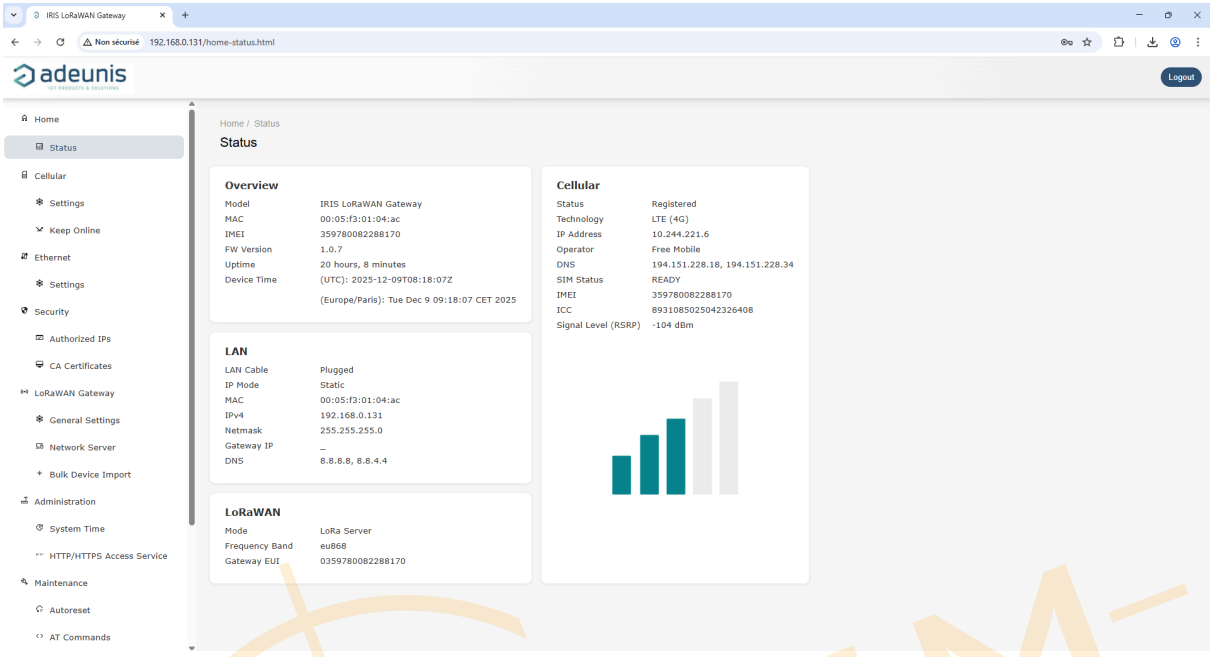
If the site requires a **static IP**, enter an address that is unique on the VLAN, the correct **IP Subnet Mask** (for example `255.255.255.0` for a /24), and the **IP Gateway** that routes traffic out of that subnet.

Without a valid gateway, LoRaWAN traffic to external servers will not leave the LAN.

Provide at least one **DNS** resolver; names will be needed later for NTP and for Basics Station (WSS). Prefer the customer's resolvers unless there is a specific reason to use public ones.



When you apply new Ethernet settings, the Web GUI moves to the new IP; reconnect your browser to that address and confirm on **Home** → **Status** that the IPv4, mask, gateway and DNS values are exactly those agreed with the IT team.



📌 If you lose the session because of an addressing mistake, plug your laptop directly into the gateway, set a temporary IP in the same subnet, and correct the configuration.

Parameter Quick Reference

Parameter	What it controls	Typical value / example	When to change	Validation / notes
Enable Ethernet Port	Brings the Ethernet interface up and activate ethernet settings. Disable this option if you do not want to use the Ethernet interface	Checked	Enable for commissioning or LAN operation	Status → LAN shows “Plugged” and link details

Distributed by www.texim-europe.com

Parameter	What it controls	Typical value / example	When to change	Validation / notes
Ethernet mode	Addressing method. Choose between DHCP (addressing provided by the LAN) and Static IP (you must enter the values)	DHCP or Static IP	Match site policy	If DHCP, verify the leased IP on Status; if Static, reconnect to the new IP
IP Address	Static gateway's address on the LAN; it must be unique on that subnet	`192.168.10.42`	Static deployments	Must be unique on VLAN; record it for support
IP Subnet Mask	Defines the network size; set it to the mask used by the VLAN	`255.255.255.0`	Static deployments	Wrong mask causes reachability issues beyond the subnet
IP Gateway	Router that forwards traffic out of the subnet; without it, external LoRaWAN services are unreachable	`192.168.10.1`	Static deployments	Mandatory for access to external LNS/NTP
DNS 1 / DNS 2	Name resolvers used by the gateway; they are required for NTP and Basics Station (WSS)	Site DNS or `8.8.8.8` / `8.8.4.4`	Static deployments or special DNS needs	Required for NTP names, WSS endpoints (Basics Station)

4.2.2. Cellular Interface

Choose cellular when the gateway must operate independently of the customer's LAN, or when Ethernet is simply not available.

Power the unit off, insert a valid SIM, then power on and open the cellular settings.

Distributed by www.texim-europe.com

📌 Before enabling the link, insert a valid SIM and obtain the APN parameters from your operator.

Cellular Interface Settings

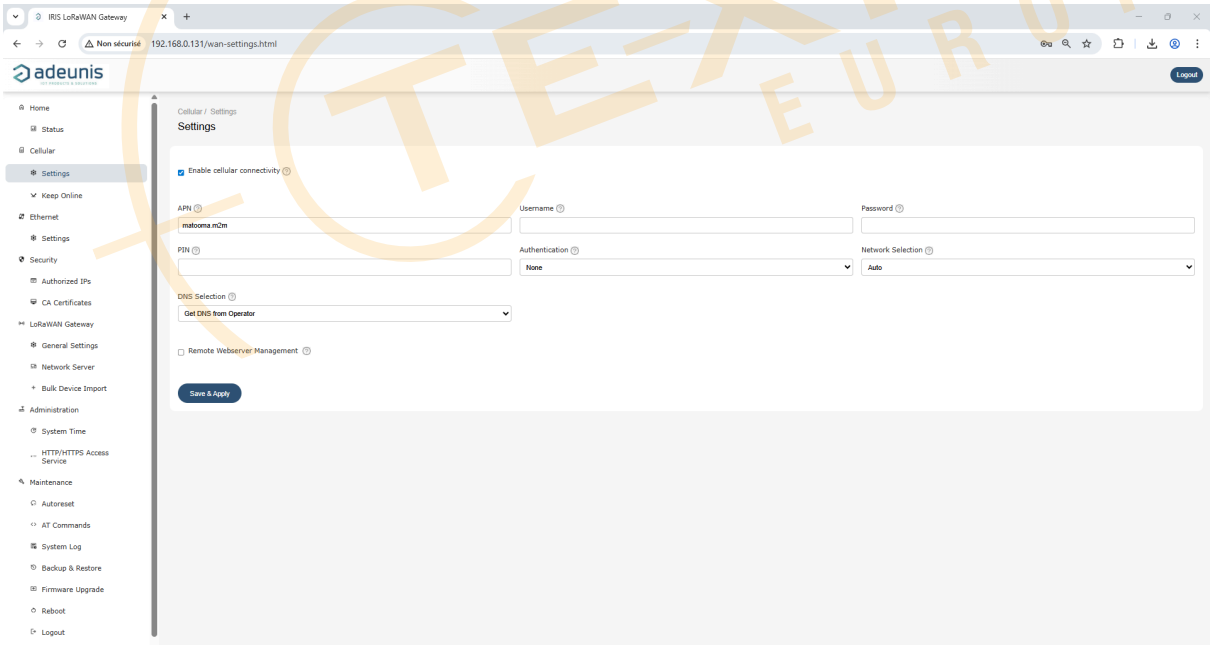
The **APN** is the access point name provided by your operator. Enter it exactly as given (some private APNs are strict about spelling).

If your subscription requires credentials, fill **Username** and **Password** and set **Authentication** to the method requested by the operator (commonly **PAP** or **CHAP**; if nothing is required, leave **None**).

If the SIM is PIN-protected, enter the **PIN** carefully—several wrong attempts will block the card until you use the PUK through your operator's procedure.

Network selection should remain **Auto** unless you have a specific reason to lock to a given technology (for example 4G-only).

For **DNS selection**, "Get DNS from Operator" is appropriate in most cases; switch to Selected DNS servers only if your application requires resolvers that the operator does not provide. In such scenario, we recommended to use Google DNS: `8.8.8.8` and `8.8.4.4`



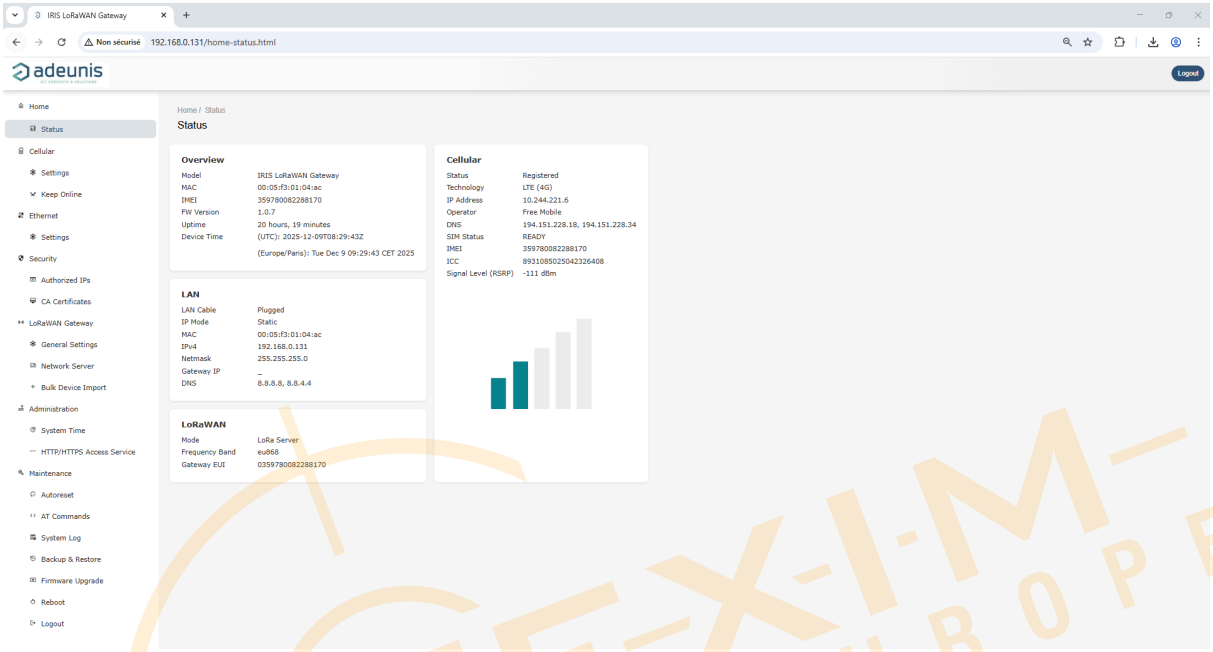
Remote Webserver Access Settings

Distributed by www.texim-europe.com

If you must reach the Web GUI over the mobile network, enable **remote webserver management** only after HTTPS is enforced and only if your APN allows inbound access.

If you do not need remote administration over cellular, keep this option disabled to reduce exposure.

After saving, watch the **Status** page: the modem should register on the network, obtain an IP address and report signal quality (RSRP).



📌 **Remote access to the IRIS Web GUI from outside the local LAN is supported only over the cellular backhaul, and only when the SIM/APN assigns a routable, public static IP address to the gateway.**
If the SIM is behind CGNAT or uses a private/dynamic address, inbound connections will not reach the gateway and remote administration is not possible.

Parameter Quick Reference

Distributed by www.texim-europe.com

Parameter	What it controls	Typical value / example	When to change	Validation / notes
Enable Cellular Connectivity	When Enabled, the modem attaches to the mobile network and establishes a data context using the APN you provide.	Checked	Use cellular as the active backhaul	Status → Mobile shows Registered and an IP
APN	Access point name provided by SIM operator	`matouma.m2m` / operator APN	On SIM / operator change	Exact spelling matters (private APNs can be strict)
Username / Password	APN credentials provided by SIM operator	blank if not required	If operator requires auth	Pair with Authentication method
Authentication	Authentication method for APN	None if not required, PAP, or CHAP	Per operator spec	Wrong mode prevents attach/data
PIN	SIM lock code. Enter it only if your operator has not disabled PIN protection on delivery	e.g., `1234`	If SIM is PIN-protected	3 wrong tries block SIM; PUK then required
Network selection	Radio tech policy	Auto, 4G, 3G, 2G	Rarely (operator request)	Locking tech can reduce coverage while roaming
DNS selection	DNS selection lets you accept operator-provided resolvers or define your own for special cases	Get DNS from Operator	If fixed DNS is required	Manual DNS only if your app needs it
Remote webserver management	Web GUI exposure over cellular	Disabled (recommended)	Enable only with HTTPS and if APN allows inbound access	Many APNs use CGNAT → no inbound reachability

4.2.3. Connectivity watchdog (“Keep Online”)

Distributed by www.texim-europe.com

The watchdog is a simple but effective way to increase the resilience of the gateway, keeping the **active** link healthy. It periodically pings a target you choose and, if the target cannot be reached within the timeout for the configured number of retries, it will reset the cellular connection and attempt to recover.

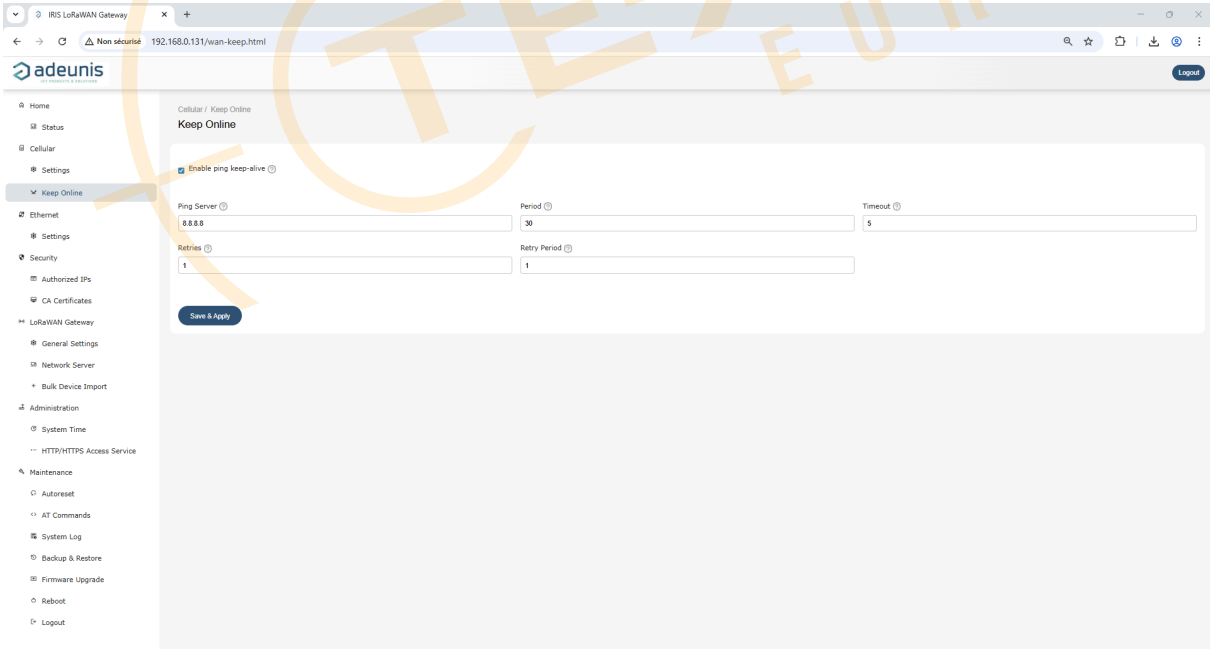
> 📌 The watchdog does not switch between Ethernet and cellular; it only heals the cellular connection.

Choose a **Ping server** that is stable and reachable from the network in use. For example a well-known resolver.

The **Period** is the interval between checks in minutes; balance responsiveness and network load.

Timeout is how long the gateway waits for a reply before considering the attempt failed; several seconds (e.g., 5–10) suit most networks.

Retries defines how many consecutive failures must occur before the gateway triggers recovery. **Retry period** is the wait between recovery attempts, in minutes, if the first one does not succeed.



Short periods and timeouts can create unnecessary resets on congested networks; very long ones delay recovery Start with moderate settings, and verify in your logs that the

Distributed by www.texim-europe.com

link remains stable after commissioning during the first hours of operation. Adjust if you see either unnecessary resets (too aggressive) or slow recovery (too relaxed).

Parameter Quick Reference

Parameter	What it controls	Typical value / example	When to change	Validation / notes
Enable Ping Keep-Alive	Activates the watchdog	Checked for unattended sites	Use on cellular to self-heal the data link	Does **not** switch to Ethernet; heals the active link only
Ping server	Sets the host to probe; pick one that is reachable from your APN and is allowed by any firewalls in the path	A well-known resolver	If APN/firewall path changes	Must be reachable from the APN used
Period	Interval between checks (1-1440 minutes)	30	If too many/too few recoveries	Too short → false resets; too long → slow recovery
Timeout	Wait per check (5-20 seconds)	5	High-latency paths	Longer for congested/remote links
Retries	Failures before recovery (0-9)	1	Noisy networks vs. responsiveness	Higher = fewer false positives
Retry period	Delay between recovery attempts (1-1440 minutes)	1	If recovery storms occur	Prevents back-to-back resets

---

Set the clock before securing the gateway

Backhaul connectivity is up. Before enabling security and LoRaWAN modes, configure system time so the device clock is correct. TLS validation, syslog timestamps, and commissioning evidence all depend on it.

You may either:

- Synchronize automatically using **NTP Time Servers** (recommended), or
- **Set the date and time manually** when no NTP service is available.

Distributed by www.texim-europe.com

4.2.4. Time Synchronization

Accurate time is a prerequisite for a stable deployment. TLS handshakes (e.g., Basics Station over **WSS**), syslog correlation, and commissioning evidence all rely on the gateway clock.

The **System Time** page lets you

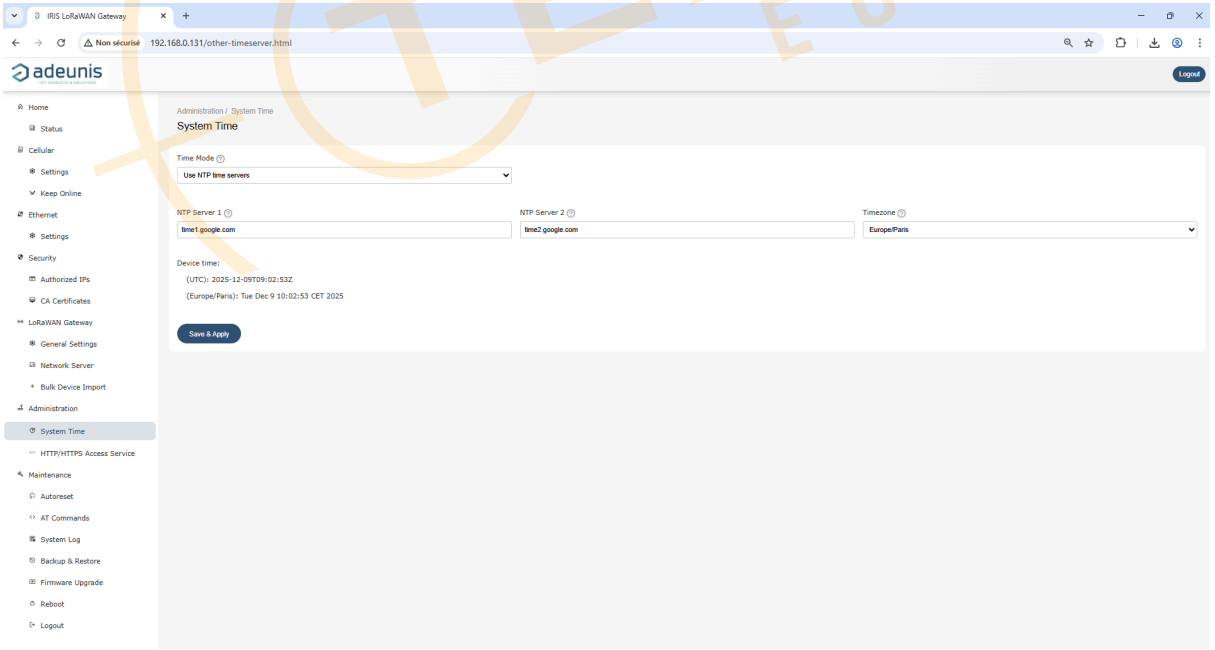
- Choose the **Time Mode** (NTP servers or manual configuration),
- Provide NTP servers when NTP mode is selected, and
- Set the local **Timezone** used for display and logs.

NTP Settings

Choose **Use NTP time servers** to enable automatic synchronization.

Provide at least **one reliable NTP server**, preferably **two** from different infrastructures (e.g., a corporate NTP plus a public fallback). Typical choices are the customer's internal NTP (recommended on corporate LANs) or well-known public services such as `time1.google.com` and `time2.google.com`.

Select the site's **Timezone** (e.g., *Europe/Paris*) so the local time shown on Status and in exported logs matches the installation's time zone.



Distributed by www.texim-europe.com

Synchronization interval
First NTP synchronization is performed upon initial connection.

NTP synchronization is then automatically performed every 24 hours.

Connectivity Requirements

- **Public NTP (time.google.com, pool.ntp.org)**

  Requires outbound **UDP/123** and DNS resolution (UDP/TCP 53) if using hostnames.
- **Corporate or operator NTP**

  No Internet required; only reachability to those servers over **UDP/123**.
- **Private APNs**

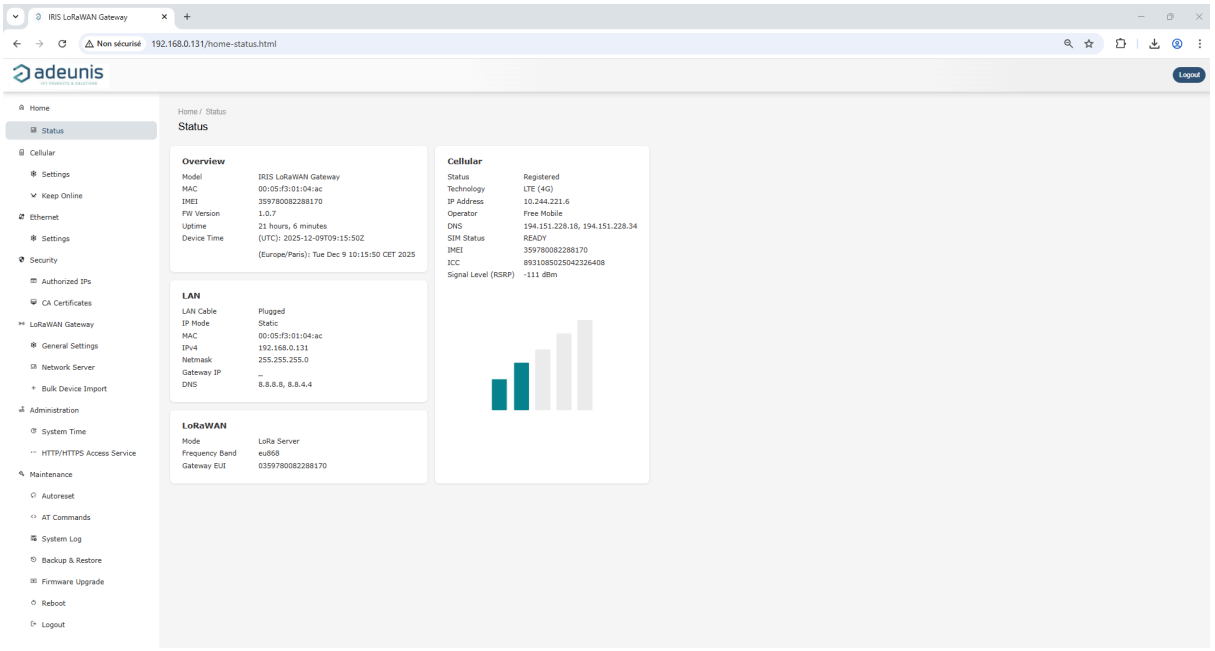
  Internet is often blocked; request an operator-internal NTP or use a reachable corporate server.
- **DNS restrictions**

  If DNS is filtered, use static **IP addresses** provided by IT.

📌 On private APNs or filtered networks, prefer the customer's **internal NTP** or use **IP addresses** supplied by IT.

After saving the configuration, return to **Home** → **Status** and check **Device Time**: the UTC time should be current and the local time line should reflect your selected timezone.

Distributed by www.texim-europe.com



If time does not update within a minute: confirm the active backhaul has **DNS** working (if you used hostnames) and that outbound **UDP/123** to the listed servers is permitted by the site firewall or APN.

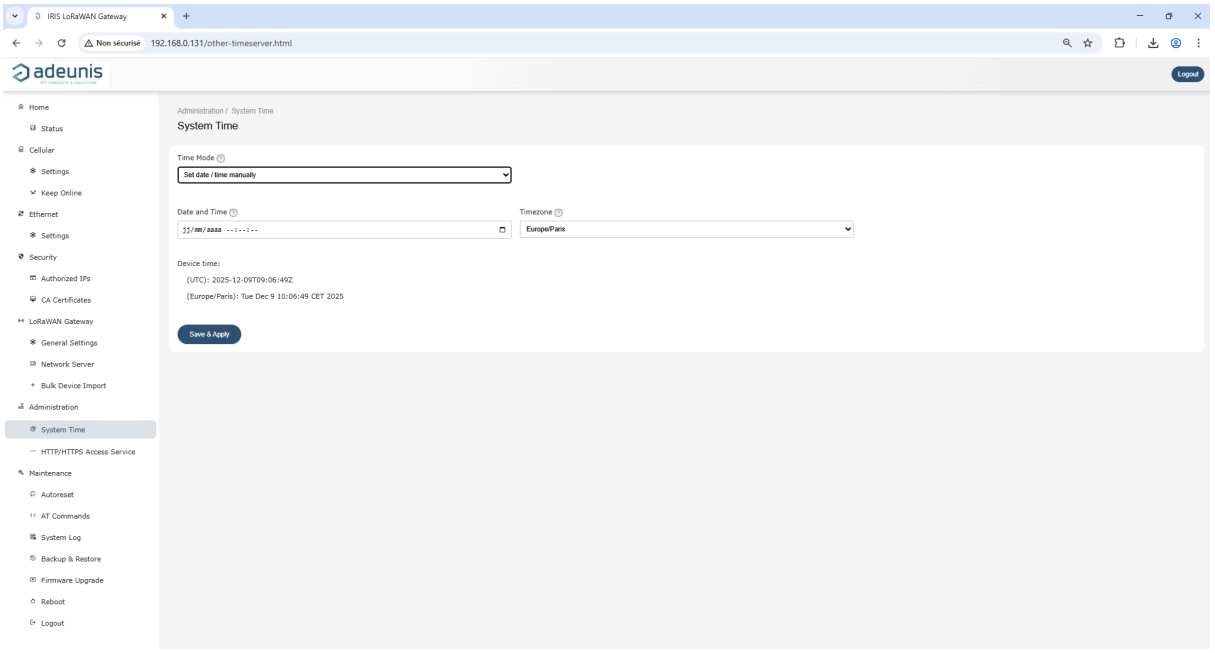
Manual Mode

Choose **Set date/time manually** when the gateway cannot reach any NTP source.

In this mode:

- Enter the **Date and Time** directly in the provided field,
- Select the appropriate **Timezone**,
- Save the configuration to apply the manual clock setting.

Manual mode is intended for isolated networks, restricted APNs, lab environments, or temporary commissioning where NTP is unavailable.



Note that the time will not automatically correct itself; update it manually if the deployment lasts long enough for drift to become noticeable.

📌 If Date/Time is configured manually, it must be updated on every power down or reset of the device

4.2.5. Validation and Handover

A network configuration is considered good when:

1. The chosen backhaul shows a valid IP on **Home** → **Status**,
2. The device time is synchronized,
3. And (if required) the Web GUI is reachable using **HTTPS** over that same path.

Before leaving the site, export a configuration backup, record the final addressing and access method and document the final NTP servers and timezone in your commissioning report, and revert your laptop adapter to **DHCP** so you are not locked into the temporary static settings the next time you connect.

Before you continue

You now have a working backhaul (Ethernet or Cellular) and correct device time.

Distributed by www.texim-europe.com

Now harden administrative access. Start by enforcing **HTTPS** for the Web GUI, then restrict exposure with **Authorized IPs**, and finally load the **CA Root** certificates required for secure outbound connections.

4.3. Security (Access Control & Trust)

With connectivity verified, harden the device now so your first LoRaWAN connection succeeds and the Web GUI isn't exposed longer than necessary. You will define who may reach services on the **Mobile WAN** and install the **certificate authorities** the gateway will trust when it validates secure servers.

4.3.1. Web GUI Access

The first step in securing the gateway is protecting its administration surface.

Enable **HTTPS** for the Web GUI so credentials and sessions are always encrypted in transit.

Only after HTTPS is active should you expose the GUI beyond a directly connected laptop, and then only in combination with the allow-list you will set in **Authorized IPs**.

Remote access prerequisites (Web GUI)

Remote access to the IRIS Web GUI from outside the local LAN is supported only over the **cellular backhaul**, and only when the SIM/APN assigns a routable, **public static IP address** to the gateway.

If the SIM is behind CGNAT or uses a private/dynamic address, inbound connections will not reach the gateway and remote administration is not possible.

Credentials and Ports Settings

Define the **Username** and a strong **Password** for administration.

Leave the **HTTPS port** at **443** unless your environment requires a different port; keep the **HTTP port** for local commissioning only.

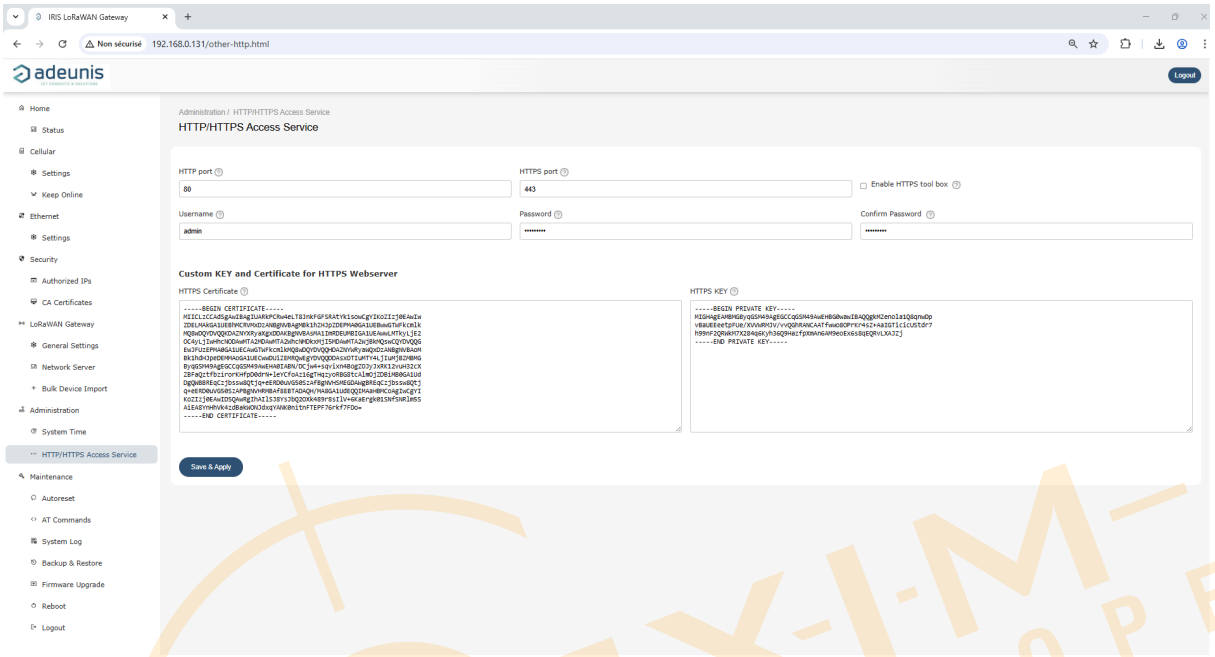
In production, access the GUI via **https://** and block plain HTTP at the site firewall or upstream router. If your policy mandates "no HTTP," coordinate with IT to ensure port 80

Distributed by www.texim-europe.com

is not reachable on the path to the gateway.

Enable HTTPS

Tick **Enable HTTPS .**



Custom Certificate for the Web GUI (recommended)

If administrators will access the GUI over cellular network, install a server certificate that matches the hostname you will use to reach the gateway.

- Paste the full **HTTPS Certificate** (PEM) — include the entire chain if your CA requires it, with the markers `----BEGIN CERTIFICATE-----` … `----END CERTIFICATE-----`.
- Paste the matching **HTTPS KEY** (PEM) — the private key for that certificate (`PKCS#1` or `PKCS#8`).
- The certificate's **CN/SAN** must match the URL hostname (e.g., `gw-iris-01.site.local`); otherwise, browsers will warn about name mismatch.
- Keep the private key secure and rotate it per your security policy.

Reconnect using the intended HTTPS URL.

A closed-lock icon with no warnings confirms the certificate/hostname/time are consistent. If the browser still warns, check: device time (NTP), hostname vs. CN/SAN, full chain pasted, and key/cert pair match.

Parameter Quick Reference

Parameter	What it controls	Typical value / example	When to change	Validation / notes
Enable HTTPS	Turns on encrypted access to the Web GUI	Checked	Always in production	Reconnect with `https://…`; ensure lock icon (no browser warning)
HTTPS port	TCP port for remote configuration via HTTPS	**443**	Only if IT policy requires a non-standard port	Confirm `https://<host>:<port>` loads; document port for ops
HTTP port	TCP port for remote configuration via plain HTTP	**80**	Set/firewall to block in production	Prefer HTTPS only; verify HTTP is not reachable on the intended path
Username	Admin login name for accessing the web GUI	`admin` → change if policy requires	At first setup or per policy	Test login; store in secure password vault
Password / Re-Enter	Admin password for accessing the web GUI	Strong passphrase	At first setup and during rotations	Verify login after save; enforce rotation cadence
HTTPS Certificate (PEM)	**Server** certificate (plus chain) presented by the GUI	PEM with full chain	When exposing GUI over LAN/VPN/APN	CN/SAN must match the URL **hostname**; include `-----BEGIN/END CERTIFICATE-----`
HTTPS KEY (PEM)	Private key matching the server certificate	PEM key (`PKCS#1` / `PKCS#8`)	When installing/rotating the server cert	Must pair with the cert; keep the key secret; rotate per policy

HTTPS is enforced. Continue to **§ 4.3.2 Authorized IPs** to allow **only** known source addresses to reach administrative and LoRaWAN services over Mobile WAN.

4.3.2. Authorized IPs (Mobile WAN allow-list)

This page enforces an allow-list on services reachable over the **cellular/Mobile WAN** interface.

Each service has a selector with two options:

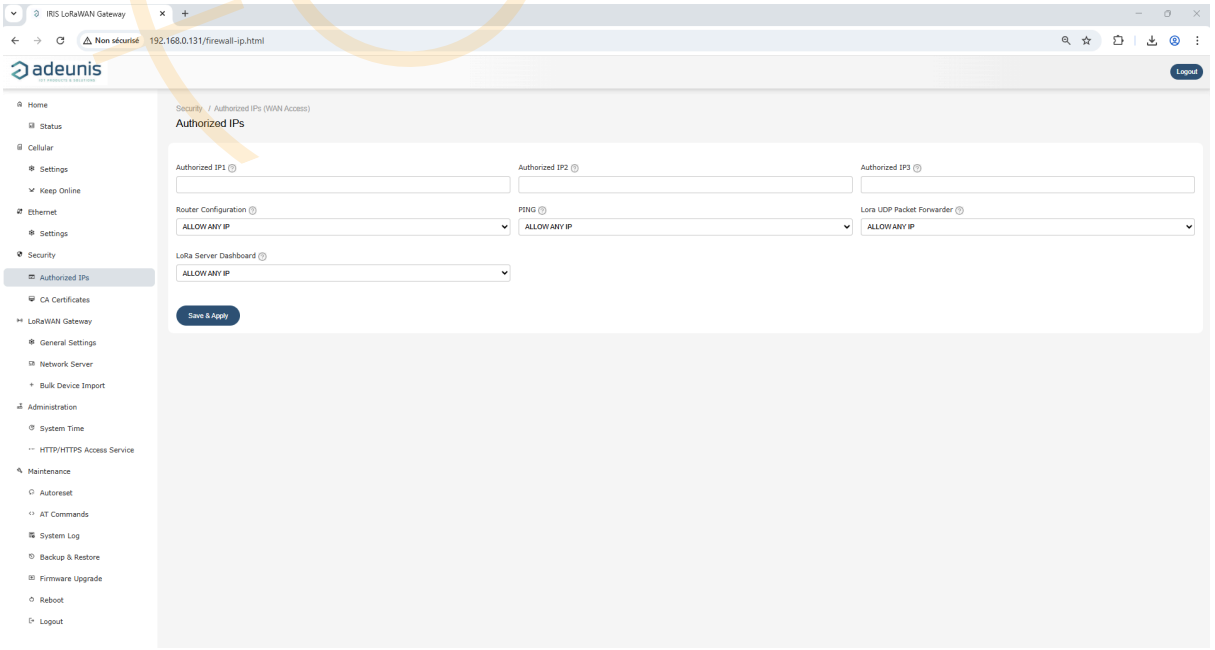
- **ALLOW ANY IP** — no restriction (commissioning convenience only).
- **ALLOW ONLY AUTHORIZED IP** — permit **only** the sources listed in **Authorized IP1–IP3**.

It is your first line of defense when the gateway is accessible outside a private LAN. On Ethernet, prefer to rely on the customer's firewall; use this page to control exposure on cellular.

> 📌 Keep an Ethernet path open as a rescue route while you tune Mobile WAN rules.

Recommended Settings

Populate the three fields **Authorized IP1 / IP2 / IP3** with the **exact** public addresses that must reach the gateway over cellular.



Distributed by www.texim-europe.com

- **Remote Configuration.** Controls who can reach the **Web GUI** over Mobile WAN. Enforce **HTTPS** first, enable remote webserver access then list **your admin/NOC public IP**. If you don't need GUI over cellular, disable the remote webserver access or **ALLOW ONLY AUTHORIZED IPs** and **leave the list empty** to effectively block it.
- **PING.** Controls ICMP echo **responses** on Mobile WAN. Set **ALLOW ONLY AUTHORIZED IPs** and **leave the list empty** unless operations explicitly need ICMP replies.
- **LoRa UDP Packet Forwarder.** Controls **inbound** UDP downlinks from your LNS to the gateway. If you use **UDP** PF over cellular, set this to **Allow only authorized IPs** and make sure the LNS downlink IPs are listed in Authorized IP1–3. If you use **Basics Station (WSS)** instead, this selector is not used by WSS.
- **LoRa Server Dashboard.** Applies to the **embedded LNS** console. Set **ALLOW ONLY AUTHORIZED IPs**; list your admin IP only if you truly need access over cellular, otherwise keep the list empty to block it.

📌 **NOTE 1**
The default ALLOW ANY IP values are convenient for commissioning but are not appropriate for production over cellular. Lock them down as soon as the link is up.

NOTE 2
If you want to block access to a service over the cellular/Mobile WAN interface, set ALLOW ONLY AUTHORIZED IPs and keep the list empty to block it.

Parameter Quick Reference

Control	Recommended in production (Mobile WAN)	Rationale
Remote Configuration	**ALLOW ONLY AUTHORIZED IPs**	Restrict GUI to known admins (or block by empty list)
PING	**ALLOW ONLY AUTHORIZED IPs** (empty list)	Disable ICMP replies unless needed
LoRa UDP Packet Forwarder	**ALLOW ONLY AUTHORIZED IPs** (+ LNS IPs if using UDP PF)	Downlinks are inbound UDP
LoRa Server Dashboard	**ALLOW ONLY AUTHORIZED IPs** (empty list if unused)	Limit embedded LNS console

4.3.3. CA Certificates - Trust Anchors for Secure Remote Services (MQTTs/HTTPs/Basics Station WSS)

This trust store enables TLS for outbound connections from IRIS to **application and network services**:

- **MQTTs** brokers (TCP **8883**)
- **HTTPS** webhooks / APIs (TCP **443**)
- **Basics Station over WSS** to your LNS (TCP **443** or the port specified by your LNS)

By installing the correct **Root CA**(s), the gateway can validate the server's certificate chain during the TLS handshake and establish an encrypted, authenticated session.

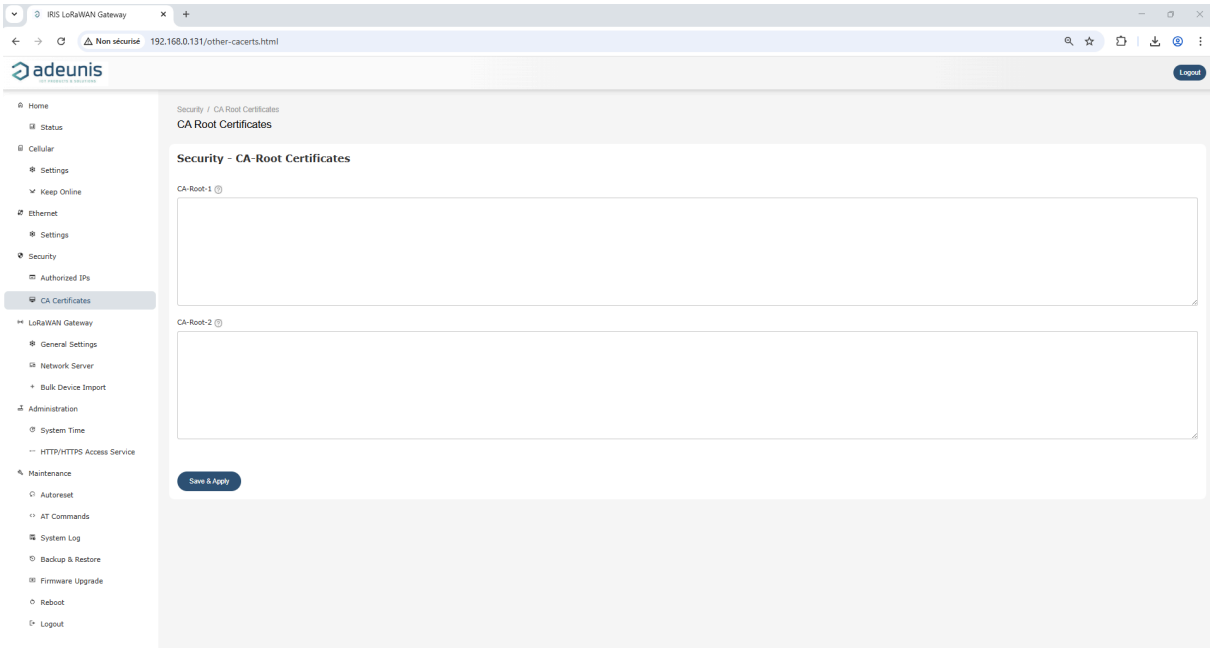
Validation Process

When IRIS connects, the remote server presents its **server certificate** (and any **intermediate** certificates). IRIS verifies that the chain **anchors** in one of the **Root CA** certificates you uploaded here, and that the **hostname** you configured matches the certificate **CN/SAN**.

What to Upload

1. Obtain the CA chain from your provider and verify its fingerprint out-of-band.
2. Paste the full PEM blocks into **CA-Root-1/2** including:
   -----BEGIN CERTIFICATE-----
   ...base64...
   -----END CERTIFICATE-----

Distributed by www.texim-europe.com



3. If validation fails, check clock, CA vs server cert, URL hostname vs certificate CN/SAN, and any TLS-intercepting proxy

---

Supported Trust Models

IRIS support 2 connection models:

- **With self-signed Root CA**

Create your own **Root CA** (self-signed, as all roots are), use it to **sign** the server certificate of your **MQTTs/HTTPS/WSS** endpoint, and **upload that Root CA** to IRIS. Use a **hostname** in IRIS that matches the server certificate **CN/SAN**.

- **With CA-signed server certificate**

Obtain a server certificate from a public or enterprise CA (e.g., Let's Encrypt). Ensure the server sends the **full chain** (server + intermediates). **Upload the Root CA** for that chain (e.g., **ISRG Root X1**) to IRIS and configure the service **hostname** accordingly.

> 📌 IRIS gateway firmware supports up to two custom CA Root entries in PEM format.

Distributed by www.texim-europe.com

4.3.4. Validation and Handover

HTTPS is configured, exposure over Mobile WAN is restricted, and CA roots are loaded.

Use the following checks to validate the setup of gateway security and package the evidence for operations.

1. Open the GUI using **http://<gateway-ip>**. Access should be blocked by site policy or immediately redirected to HTTPS if HTTPS connection is enabled. Then open **https://<gateway-hostname-or-ip>:<https-port>** and log in. Browser shows a **secure session (lock icon)** with **no warning** when you use a custom certificate that matches the hostname. Record screenshot of the browser lock/cert details + the **HTTP/HTTPS** page (ports, “HTTPS enabled”, certificate fingerprint/date).
2. Test the configuration of authorized IPs from an **authorized** source (access OK) and from a **non-authorized** source (access blocked). Document the allow-list; update it if the LNS provider changes IPs.
3. Verify your PEM blocks are present, confirm the expiry date of each certificate and note your rotation date. If your LoRaWAN mode will use **Basics Station (WSS)** or **MQTTs/HTTPs**, verify that the **server hostname** you will configure matches the certificate’s CN/SAN (ask your LNS/broker admin if unsure). Record screenshot of the **CA Certificates** page and a note of each CA’s **issuer** and **expiry.**

You are ready to connect to LoRaWAN

Your gateway is now reachable, time-synchronized, and protected (HTTPS enforced, Authorized IPs applied, CA trust configured).

The next step is to bring the LoRaWAN layer online. In **Chapter 5**, you will choose a single operating mode (Packet Forwarder over **UDP** or **Basics Station/WSS**, or the **Embedded LoRaWAN Server**), set the regional band, complete the mode-specific settings, and verify traffic with a real device.

📌 Save your configuration before you start, then apply changes one block at a time and verify on **Home** → **Status**.

Distributed by www.texim-europe.com

5. LoRaWAN CONFIGURATION & COMMISSIONING

This chapter brings the gateway online on your LoRaWAN network, either by forwarding traffic to an external LoRaWAN Network Server (UDP Packet Forwarder or Basics Station/WSS) or by running a local LoRaWAN server.

Before starting, ensure that:

- Backhaul connectivity is operational,
- System time is correct (NTP or manual),
- HTTPS access and CA trust are configured if using secure transports.

Save your configuration before applying changes and verify progress on **Home** → **Status**.

Have at hand the items you'll need: LNS address/ports for UDP, **WSS URL + matching CA** (and any client token/cert) for Basics Station, or device profiles/keys if you use the embedded server.

5.1. Supported Operating Modes

In LoRaWAN, the gateway receives radio frames from end-devices and forwards them to a LoRaWAN Network Server (LNS).

IRIS supports the following operational modes:

5.1.1. Packet Forwarder

The gateway forwards frames to an **external Network Server**.

Two implementations are available:

- **UDP Packet Forwarder (Semtech UDP)**

  A simple uplink/downlink bridge over UDP. Widely supported by legacy LNS platforms.

- **Basics Station (WSS)**

  A modern, secure transport over WebSockets (WSS recommended).

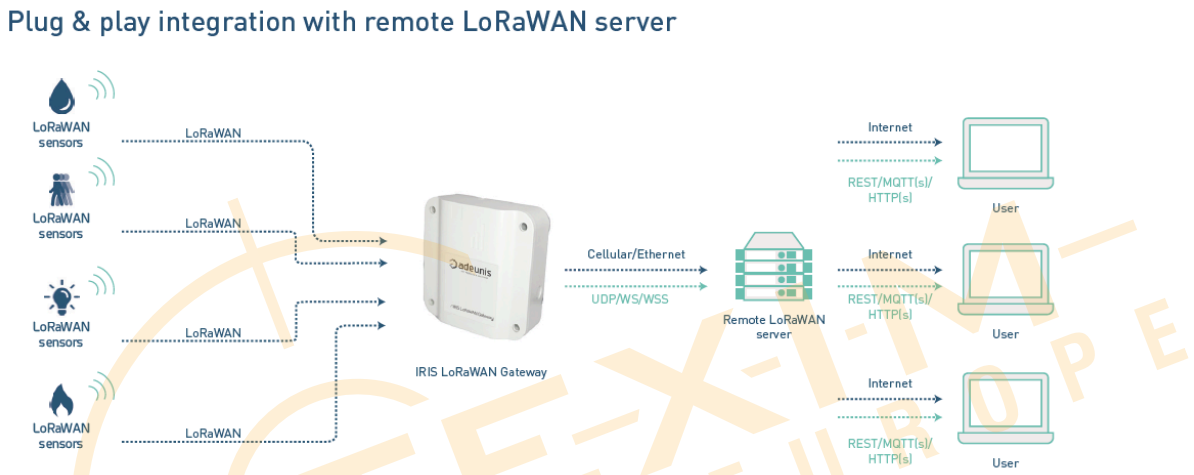
  Basics Station requires valid device time and CA trust to establish TLS sessions with the LNS.

Optional CUPS Bootstrap

Basics Station can be provisioned dynamically using a CUPS (Configuration and Update Server).

CUPS delivers the LNS URI, updated credentials, and configuration files to the gateway.

CUPS is not a forwarding mode: it prepares the Basics Station runtime configuration.

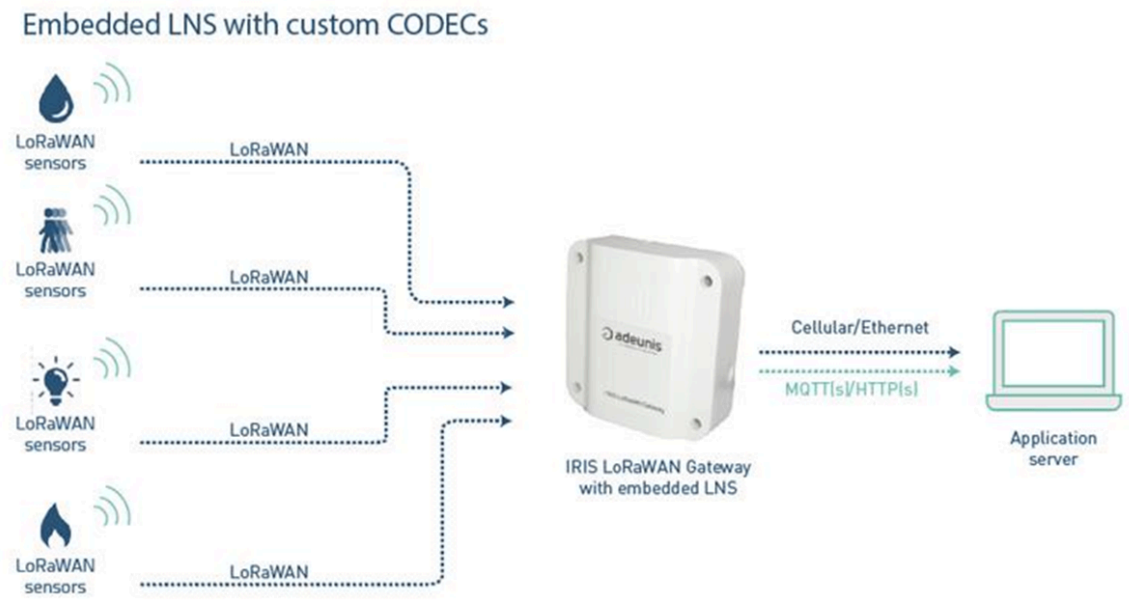


5.1.2. Embedded LoRaWAN Network Server (LNS)

The gateway hosts the network server locally.

Choose this mode when you want to manage LoRaWAN devices directly on IRIS (device registry, profiles, MAC parameters and downlinks).

Distributed by www.texim-europe.com



5.2. Select the Operating Mode

1. Open **LoRaWAN → General Settings**
2. Tick **Enable the LoRaWAN stack**
3. The, select one of the following:

- **Packet Forwarder (UDP)**

Classic Semtech UDP bridge to an external LNS.

Requires the LNS's uplink/downlink ports and reachable IPs.

- **Packet Forwarder (Basics Station)**

Modern, secure forwarding over WSS.

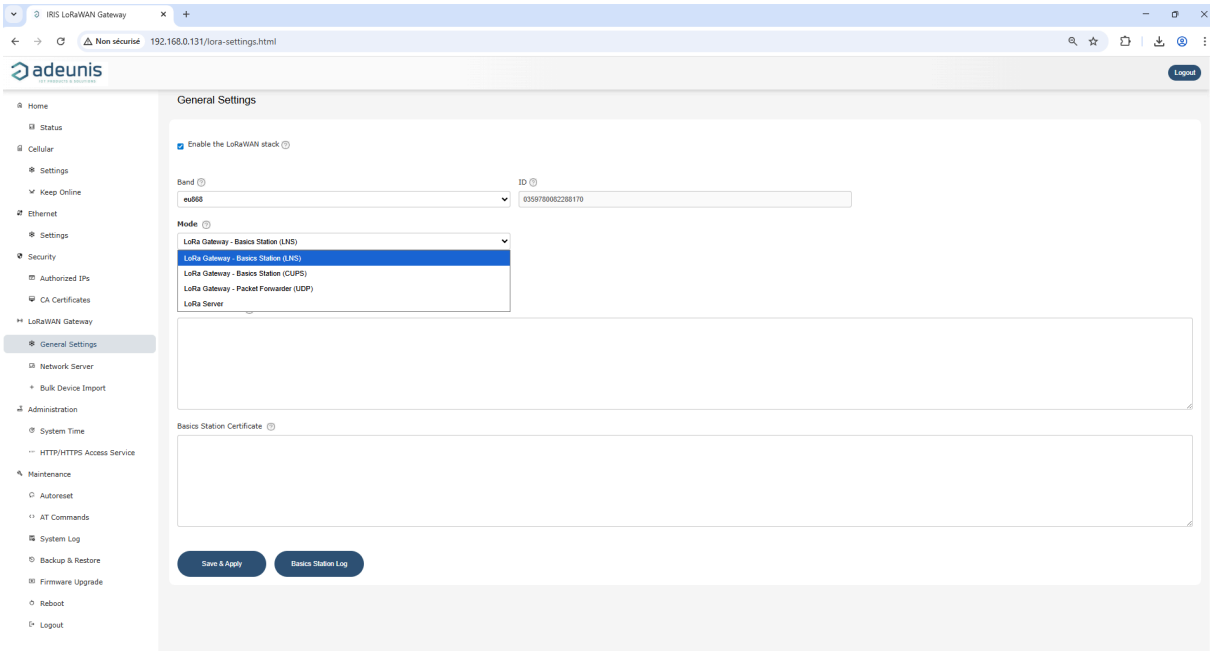
Requires correct time, CA trust, and the LNS WSS URL.

If a CUPS server is provided by your operator, complete **CUPS Settings** before configuring LNS parameters.

- **LoRaWAN Server**

Internal LNS hosted on IRIS (device registry, profiles, downlink scheduling, optional local decoding).

Distributed by www.texim-europe.com

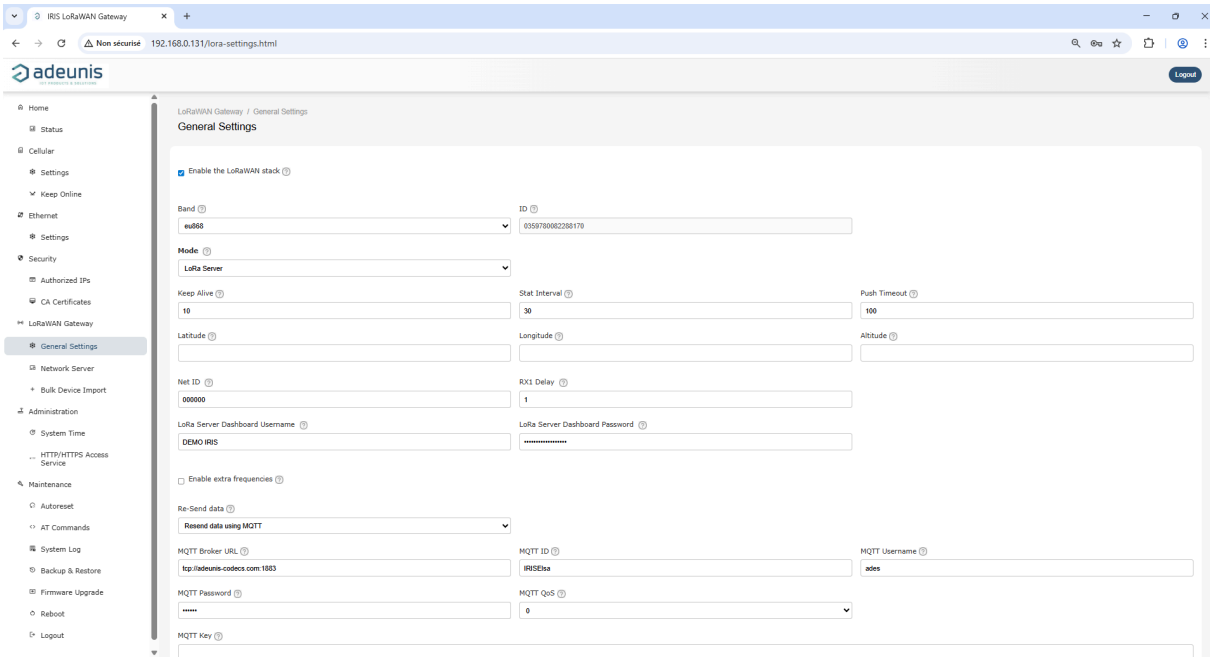


5.3. Set the Radio Band

Still under the **LoRaWAN → General Settings**, set **Band/Region** (e.g., **EU863-870 / EU868**).

Ensure the band corresponds to the country of installation and that antennas are connected / approved for the band.

Regional limits (duty-cycle, TX power, channels) are enforced by the LNS and device profiles. Misalignment leads to failed joins or discarded frames.



📌 The current firmware supports only EU868 Band.

In **LoRa Server** mode only, you may **Enable extra frequencies** and constrain **Minimum/Maximum Data Rate (DR0...DR5)** to match your device population and RF plan. Use this option only if you know the site's channel plan and regulatory constraints.

1. Check the box to **Enable Extra Frequencies**

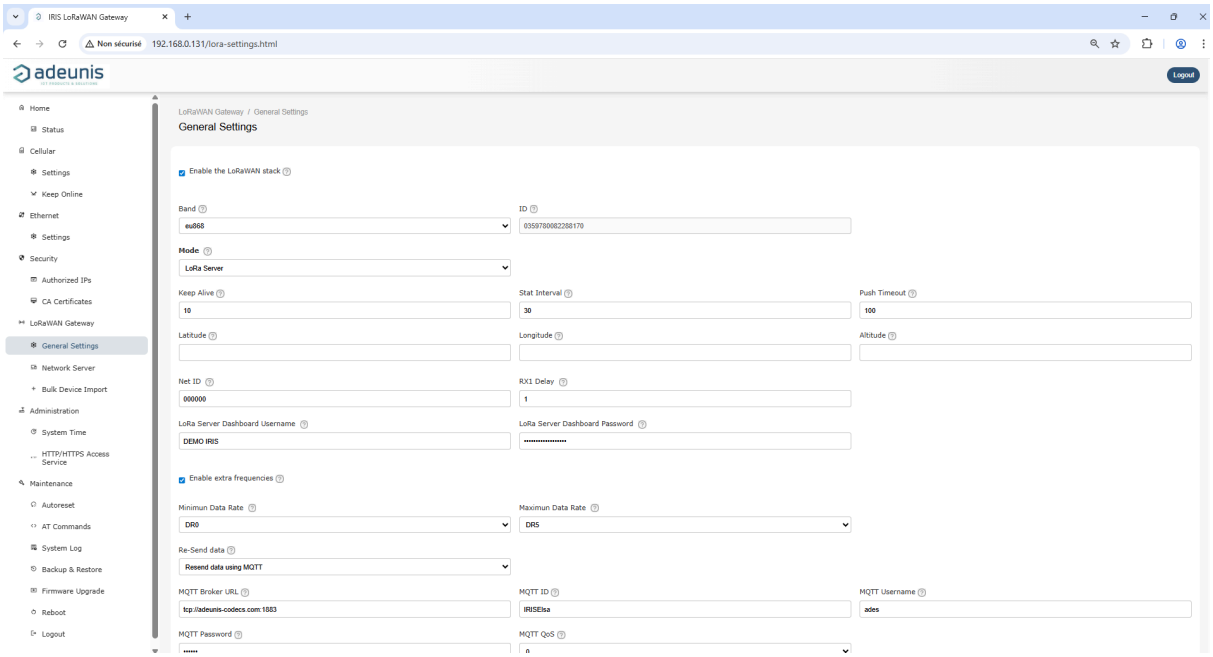
It enables the use of additional channels beyond the 3 mandatory EU868 channels (868.1, 868.3, and 868.5 MHz).

When this option is enabled, the server will also use one of the 5 optional 125 kHz channels at 867.1, 867.3, 867.5, 867.7, and 867.9 MHz.

2. Select the minimum/maximum data rate allowed on theses extra channels.

DR0 is more robust but slower, DR5 is faster but less robust.

Distributed by www.texim-europe.com



DR	Spreading factor / BW	Typical use
DR0	SF12 / 125 kHz	Longest range, slowest
DR1	SF11 / 125 kHz	Long range
DR2	SF10 / 125 kHz	Rural / indoor
DR3	SF9 / 125 kHz	General purpose
DR4	SF8 / 125 kHz	Shorter range
DR5	SF7 / 125 kHz	Short range, fastest
DR6	SF7 / 250 kHz	Optional (downlink)
DR7	FSK 50 kbps	Optional

3. Save & Apply
4. The gateway will automatically start a new join process.

📌 Enabling extra frequencies increases the capacity of the gateway, limits the risk of collisions and ensure better duty-cycle distribution.

Many profiles keep DR0–DR5. Use DR6/DR7 only if your profile and network enable them.

Distributed by www.texim-europe.com

5.4. UDP Packet Forwarder Settings

In **UDP Packet Forwarder Mode**, the IRIS Gateway forwards data received from LoRaWAN end-devices to an external LoRaWAN Network Server (LNS) via **UDP**.

This mode is ideal for use cases where the LNS is hosted externally and the gateway simply acts as a bridge to forward data without any additional processing.

Features:

- Quick integration with major third-party LNS for small deployment and Proof of Concept.
- Data is forwarded via **UDP** for low-latency, reliable communication.
- No local payload decoding or advanced data processing on the gateway.

5.4.1. What you need from the LNS

Before you start, collect:

- **LNS host/IP** and **UDP ports** (uplink/downlink) from your LNS admin.
- Any **site firewall rule** to allow outbound UDP uplink and inbound UDP downlink (as applicable to your network path).

5.4.2. Configuring UDP

Go to **LoRaWAN → General Settings**

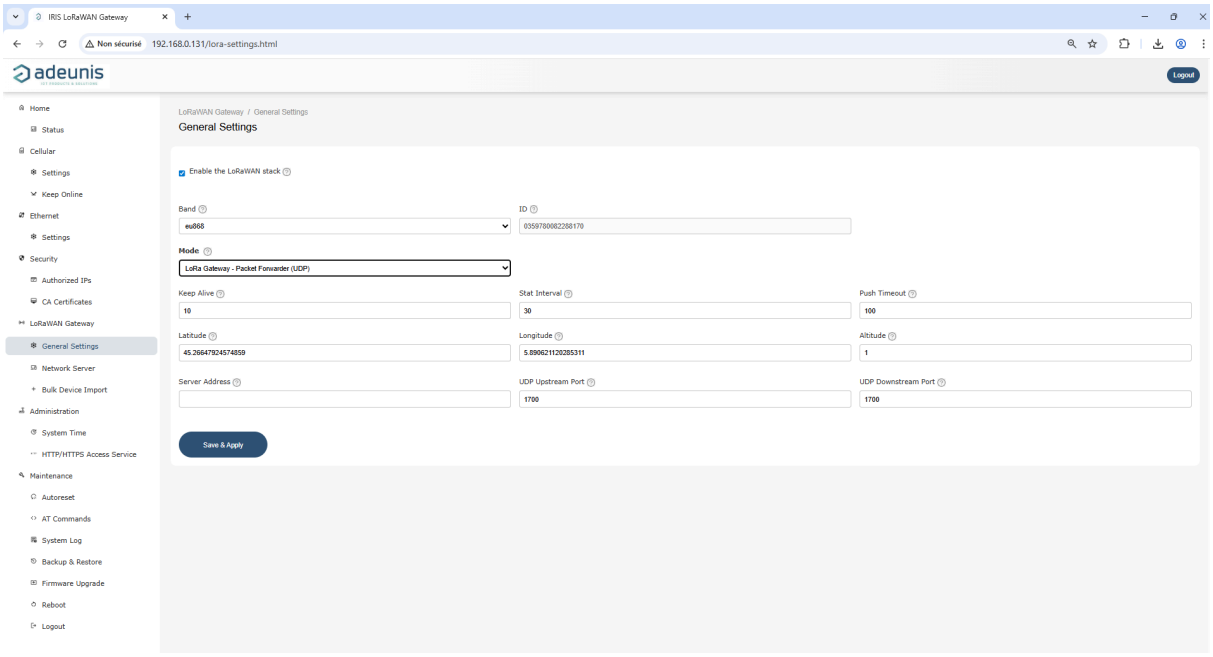
1. Select **Packet Forwarder (UDP)**.
2. Enter **LNS host** and **Up/Down UDP ports** exactly as provided by your LNS.
3. (Optional) Adjust timing parameters such as keep-alive, stat interval, and push timeout to recommended values for your environment:

- **Keep Alive (s)**: heartbeat to LNS (typ. 10).
- **Stat Interval (s)**: telemetry cadence (typ. 30).
- **Push Timeout (ms)**: resend threshold (typ. 100).

Short timeout can create unnecessary retries on congested networks; very long ones delay detection of network issues. Start with moderate settings,100 ms is recommended and verify that the link remains stable after commissioning during the first hours of operation. Adjust if you see either unnecessary retries (too aggressive) or slow recovery (too relaxed).

Distributed by www.texim-europe.com

4. (Optional) Configure the **Latitude / Longitude / Altitude** (for LNS mapping and stats).



5. **Save & Apply**.

Parameter Quick Reference

Parameter	What it controls	Typical/Example
Enable the LoRaWAN Stack	Brings the LoRaWAN interface up and activate LoRaWAN settings	Checked
ID	Gateway unique identifier (EUI-64)	Read-only
Server address	Address of the LNS server that will receive the data and statistics packets	`lns.example.com`
Up port	Remote LNS port for uplink data and statistics packets	1700
Down port	Remote LNS port for downlink packets	1700
Keep Alive (s)	Interval between heartbeat UDP messages to LNS to keep the connection stable and alive	10
Stat Interval (s)	Interval for sending gateway statistics (temperature,	30

Distributed by www.texim-europe.com

Parameter	What it controls	Typical/Example
	counters, average RSSI, etc.) to LNS	
Push Timeout (ms)	Maximum time the gateway waits before retransmitting data to LNS in case of error. If timeout value is too low, it will generate unnecessary transmissions	100
Latitude	Gateway location coordinates in decimal degrees. Optional field	45.2664
Longitude	Gateway location coordinates in decimal degrees. Optional field	5.8906
Altitude	Gateway altitude in meters above sea level. Optional field	1

5.4.3. Validation and Handover

An UDP packet forwarder implementation is considered good when:

- On the gateway **Status** page, the gateway is “connected”.
- On the LNS console, confirm the gateway appears online and is reporting statistics.
- Trigger a test uplink from a known device; the LNS should display frames arriving via your gateway.

If you do not see traffic:

- Re-check site firewalls.
- Re-check exact up/down port numbers.
- And confirm the **band/region** matches the LNS configuration.

5.5. Basics Station Settings (WS/WSS)

In **Basics Station Mode**, the IRIS Gateway functions as a **LoRaWAN base station** that securely communicates with a network server using **WS/WSS (WebSocket Secure)**.

This mode is ideal for users who need more control over their LoRaWAN network and prefer a secure, bidirectional communication channel between the gateway and the LNS.

Distributed by www.texim-europe.com

Features:

- Secure communication via **WebSocket (WSS)** with the LNS.
- Better suited for environments where reliable real-time data transmission is critical.

5.5.1. What you need from the LNS

Before you start, collect:

- **WSS URL + path** from your LNS (for example `wss://lns.example.com/router`).
- **Client token or identity certificate/key** (if your LNS enforces client authentication)
- **Root CA certificate** corresponding to the remote server's TLS certificate
- Correct **time (NTP)** and **DNS** resolution of the LNS hostname.

If your operator uses CUPS, you may receive:

- A **CUPS URL**,
- A **CUPS Key** (JSON credential or token),
- **Root CA** used to sign the CUPS server certificate,
- And optionally a gateway certificate.

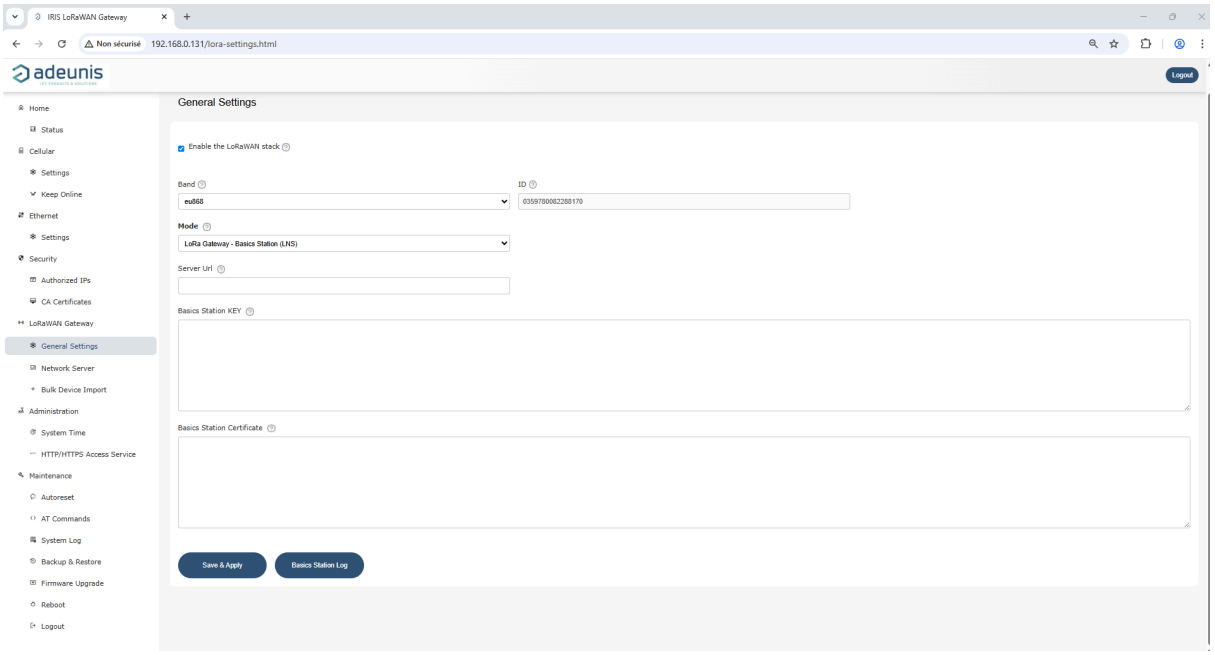
In that case, complete **CUPS Settings.**

5.5.2. Configuring Basics Station

Go to **LoRaWAN → General Settings**

1. Select **Basics Station (LNS)**.
2. Enter the **Server URL** exactly as provided by your LNS (scheme, host, port, **path**).
3. If your LNS requires a **token**, paste it in **Basics Station KEY**. For mTLS deployments, authentication is performed via certificates, upload or select the appropriate CA trust.

Distributed by www.texim-europe.com



4. **Save & Apply**.

Parameter Quick Reference

Parameter	What it controls	Typical
Enable the LoRaWAN Stack	Brings the LoRaWAN interface up and activate LoRaWAN settings	Checked
ID	Gateway unique identifier (EUI-64)	Read-only
Server URL	WSS endpoint + path If TLS is used with certificates,	`wss://<host>:<port>/router` (TLS, recommended) `ws://<host>:<port>/router` (For testing only)
Basics Station key	In some deployments, the Basics Station key is used as a token (sent in the authorization header or in the URL) For mTLS deployments, authentication is performed via certificates. Leave this field empty and download TLS certificate	1700

📌 If mTLS is used with certificates, verify clock/NTP settings is correct

5.5.3. CUPS Settings

CUPS (Configuration and Update Server) provides centralized provisioning for Basics Station gateways.

Use CUPS when:

- your operator provides a CUPS endpoint,
- LNS credentials or URLs are rotated regularly,
- you deploy large fleets and want zero-touch bootstrap.

Network Requirements

CUPS relies on secure outbound HTTPS:

- Outbound **TCP 443** must be allowed.
- DNS resolution must work if using FQDNs.
- System time must be accurate (NTP or manual mode).
- Private APNs may require the operator to expose an internal CUPS endpoint.

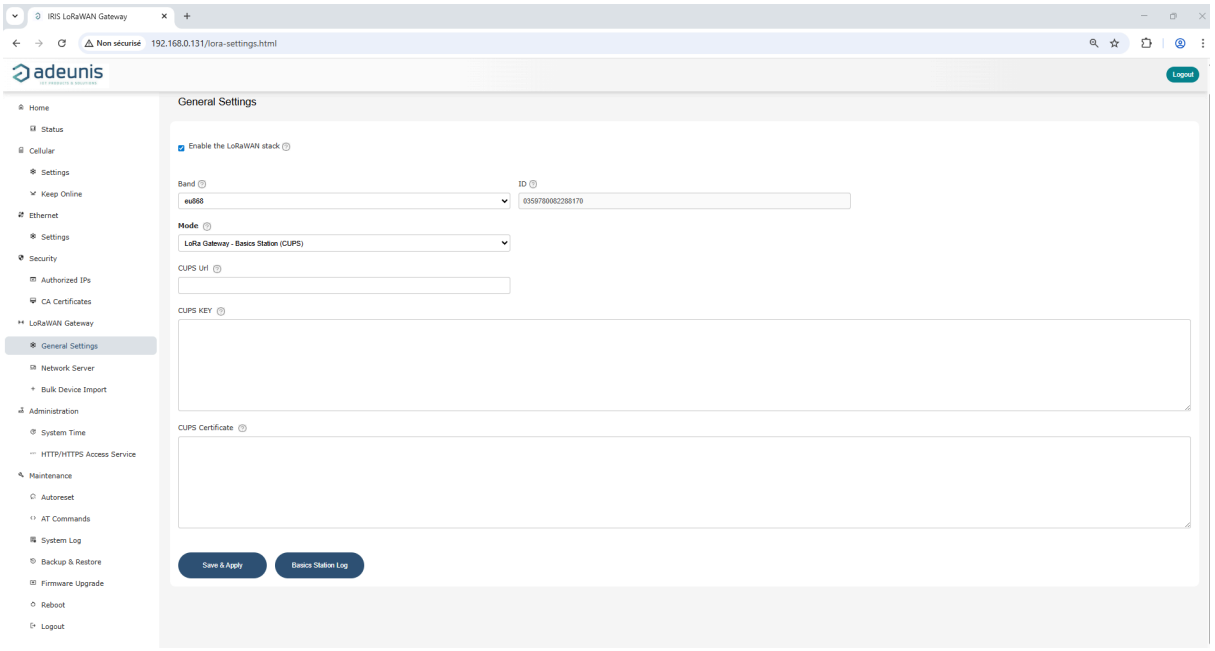
If DNS is filtered, configure the CUPS server using its IP and upload the correct CA.

Configuring CUPS

Go to **LoRaWAN → General Settings**

1. Select **Basics Station (CUPS)**.
2. Enter the **CUPS URL**.
3. Paste the **CUPS Key** provided by your operator.
4. Upload the **Gateway Certificate** if required.
5. Upload the **CA Certificate** matching the CUPS server.

Distributed by www.texim-europe.com



6. Save and apply.

The gateway immediately attempts a bootstrap sequence.

5.5.4. Validation and Handover

A Basics Station packet forwarder implementation is considered good when:

- On the gateway **Status** page, the gateway is “connected”.
- On the LNS console, confirm the gateway appears online and is reporting statistics.
- Trigger a test uplink from a known device; the LNS should display frames arriving via your gateway.

If you do not see traffic:

- Re-check **gateway’s time** is correct.
- Re-check **CA root** presence.
- Confirm **hostname** match (CN/SAN).
- Confirm the exact **WSS URL path.**
- And confirm the **band/region** matches the LNS configuration.

📌 Basics Station uses **outbound TLS**. **Authorized IPs** (Mobile WAN) control inbound exposure (GUI, UDP PF), not WSS. Ensure the firewall **allows outbound** to your LNS endpoint.

Distributed by www.texim-europe.com

5.6. Embedded LoRaWAN Network Server (LNS) Settings

In **Embedded LNS Mode**, the IRIS Gateway operates as a **complete LoRaWAN Network Server**, handling device management, data forwarding, and network operations all locally.

This mode is ideal for users who prefer not to rely on an external LNS and want full control over the entire LoRaWAN network.

Features:

- The gateway itself becomes the **LoRaWAN Network Server**.
- Manages LoRaWAN endpoints, data routing, device authentication, and downlink messages.
- Supports multicast downlink and local payload decoding via the **Codec Manager**.
- Ideal for isolated or private network environments.

You will enable the **server** in LoRaWAN Settings Web GUI interface, then complete the configuration in the **LoRa Server Dashboard** (device profiles, device registry, applications, optional codec, multicast).

5.6.1. Enabling the Embedded LoRaWAN Server

Go to **LoRaWAN → General Settings**

1. Select **LoRa Server**.
2. Set site metadata and timers

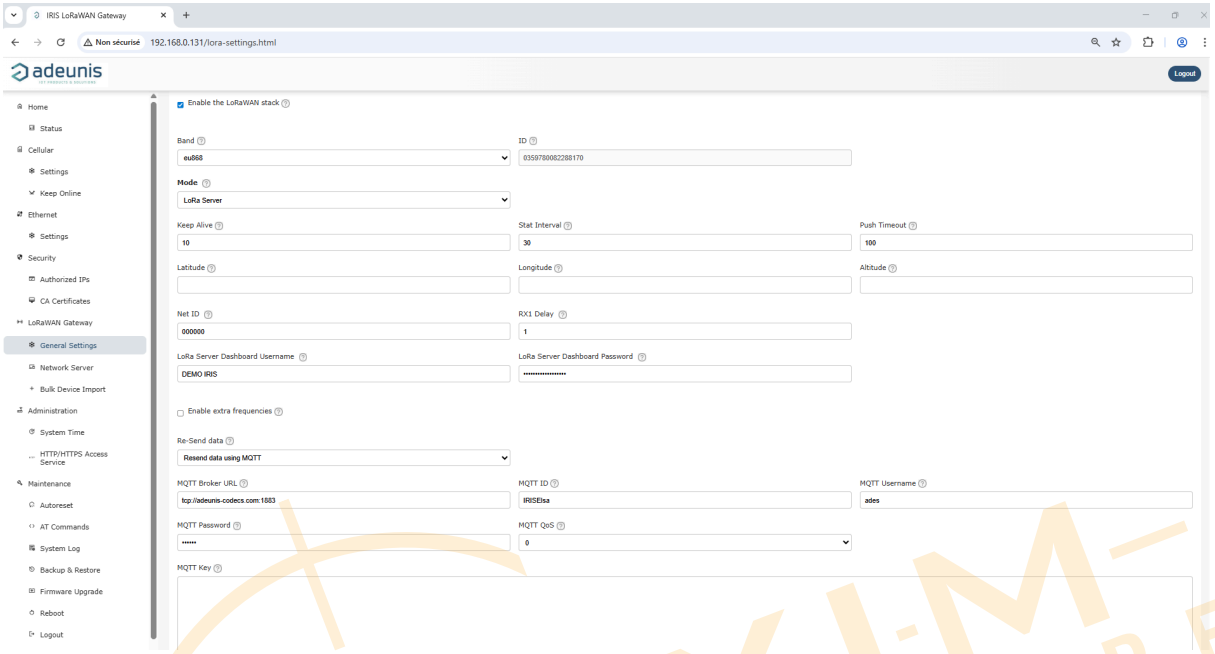
- **Keep Alive (s)**: heartbeat to LNS (typ. 10).
- **Stat Interval (s)**: telemetry cadence (typ. 30).
- **Push Timeout (ms)**: resend threshold (typ. 100).

Short timeout can create unnecessary retries on congested networks; very long ones delay detection of network issues. Start with moderate settings,100 ms is recommended and verify that the link remains stable after commissioning during the first hours of operation. Adjust if you see either unnecessary retries (too aggressive) or slow recovery (too relaxed).

- **Latitude / Longitude / Altitude** (for LNS mapping and stats).

Distributed by www.texim-europe.com

3. Configure **HTTP Port** (dashboard), **Net ID**, **RX1 Delay** (per your policy).
4. Define **LoRa Server Dashboard Username/Password** (credentials for the LoRa server console).
5. (Optional) **Enable extra frequencies** and select **Minimum/Maximum Data Rate** to match your channel plan.



6. **Save & Apply**.

Parameter Quick Reference

Parameter	What it controls	Typical
Enable the LoRaWAN Stack	Brings the LoRaWAN interface up and activate LoRaWAN settings	Checked
ID	Gateway unique identifier (EUI-64)	Read-only
Keep Alive (s)	Interval between heartbeat UDP messages to LNS	10
Stat Interval (s)	Interval for sending gateway statistics (temperature, counters, average RSSI, etc.) to LNS	30
Push Timeout (ms)	Maximum time the gateway waits before retransmitting data to LNS in case of error.	100

Distributed by www.texim-europe.com

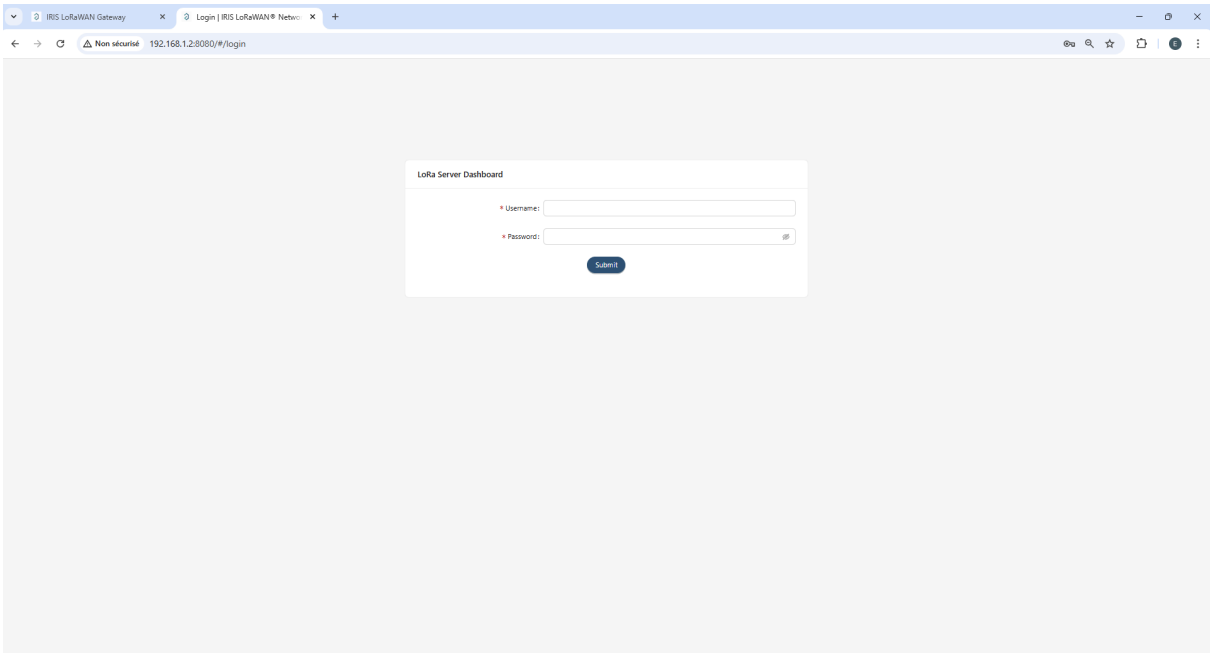
Parameter	What it controls	Typical
	If timeout value is too low, it will generate unassera	
Latitude	Gateway location coordinates in decimal degrees. Optional field	45.2664
Longitude	Gateway location coordinates in decimal degrees. Optional field	5.8906
Altitude	Gateway altitude in meters above sea level. Optional field	1
Net ID	Network identifier for LoRaWAN network server (3 bytes in hexadecimal format). Used to build DevAddr values and for roaming functions. For private networks, use 000000. Changing this parameter in an already operational network may require reprovisioning devices	000000
RX1 Delay (s)	Interval time between the endpoint (class A) sends uplink packet and the endpoint opens RX1 window to receive downlink packet. Standard value: 1. Change the value to 2-5 if the network/server path introduces significant latency. Warning: reducing below 1 is not LoRaWAN-compliant	1
LoRa Server Dashboard Username	Username to access the LoRaWAN network server dashboard	
LoRa Server Dashboard Password	Password to access the LoRaWAN network server dashboard. Requirements: Minimum 10 characters, with at least 1 uppercase letter and & lowercase letter	

5.6.2. Reaching the LoRaWAN Server

When the embedded LoRaWAN Server is enabled, open **LoRaWAN → Network Server** from the Web GUI.

Distributed by www.texim-europe.com

Log in with the **LoRa Server credentials** you just set.

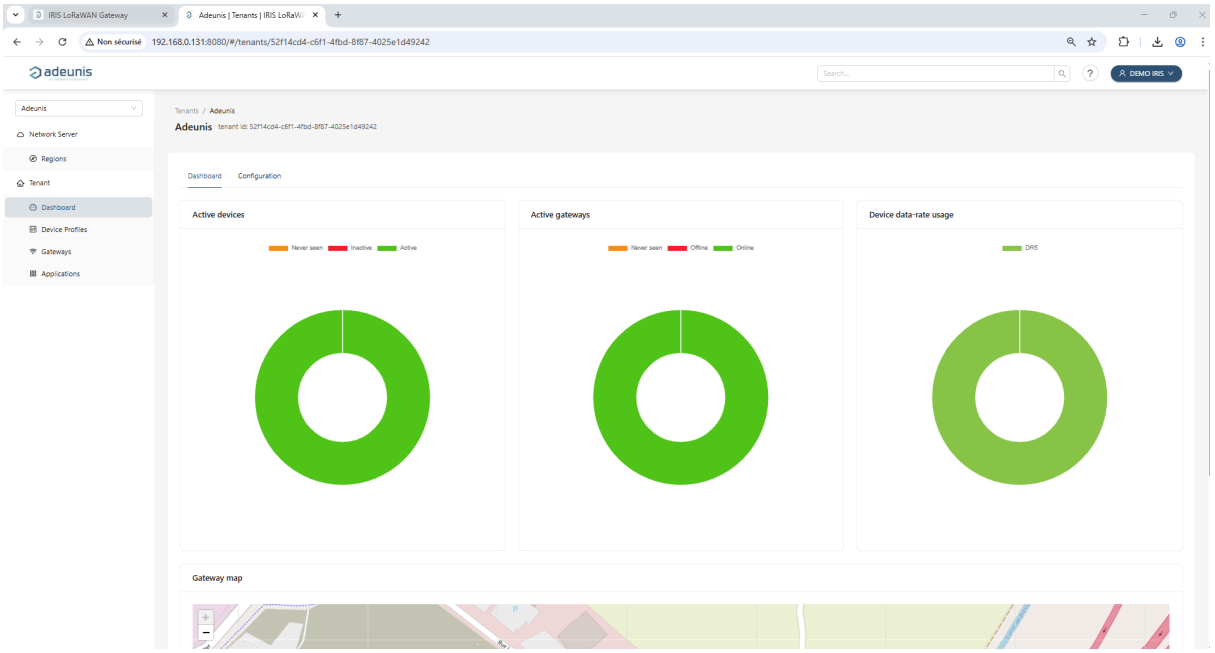


5.6.3. LoRaWAN Server Dashboard

After you log in to the embedded LoRaWAN Server, the dashboard opens in a new tab with:

- A top bar (search field, breadcrumb, tenant selector, user menu),
- A left sidebar for navigation,
- A main workspace that changes with the selected view.

Distributed by www.texim-europe.com



Dashboard:

The default view provides an operational snapshot for the selected tenant:

- **Active devices** donut: Active / Inactive / Never seen.
- **Active gateways** donut: Online (recent stats), Offline, Never seen.
- **Device data-rate usage**: DR distribution for the tenant (useful to verify ADR and coverage).
- **Gateway map**: Gateways plotted at their configured coordinates.

Navigation (Sidebar):

- **Network Server → Regions**: Lists the LoRaWAN region(s) enabled on the server (EU868 on this device).
- **Tenant**: Your isolated workspace grouping applications, devices, and gateways. **Dashboard** shows health; **Configuration** holds basic tenant options.
- **Device profiles**: Library of profiles (Region, LoRaWAN/MAC, ADR policy, join mode, class, codec/mappings). IRIS ships with pre-loaded profiles you can reuse or duplicate.
- **Gateways**: Registered gateways for this tenant (status, last seen, location).
- **Applications**: Logical containers for devices and data routing; from here you'll add devices and configure integrations.

Distributed by www.texim-europe.com

5.6.4. Manage Gateway Fleet

This page manages the LoRaWAN gateways registered under the tenant when the embedded Network Server is in use.

The IRIS gateway that runs the embedded LNS is automatically pre-registered. It represents the local radio and **must not be deleted**.

Add any external gateways that forward traffic to this server via **Semtech UDP Packet Forwarder.**

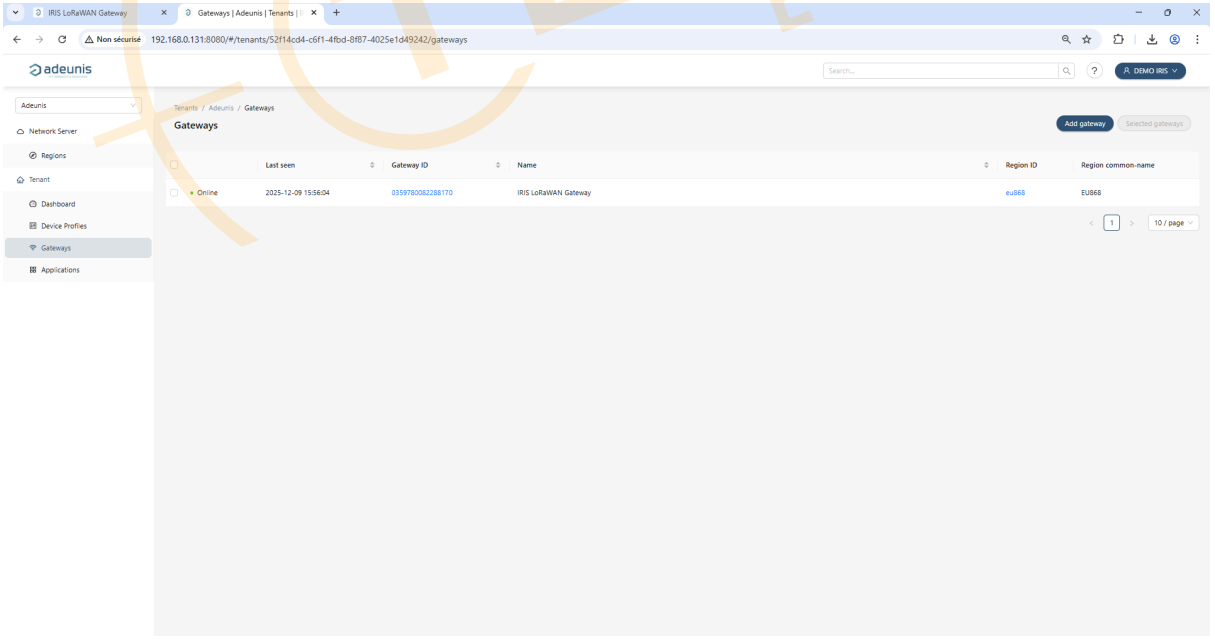
Gateways List

The list shows one row per gateway with search and bulk actions on top.

Columns:

- **Last seen** (with Online/Offline/Never-seen states).
- **Gateway ID** (EUI-64, clickable).
- **Name.**
- **Region ID.**
- **Region common-name**.

The **IRIS gateway** running the embedded LoRa Network Server is **automatically pre-registered** in the list. **Do not delete** this gateway.



Clicking the **Gateway ID** opens the gateway details view.

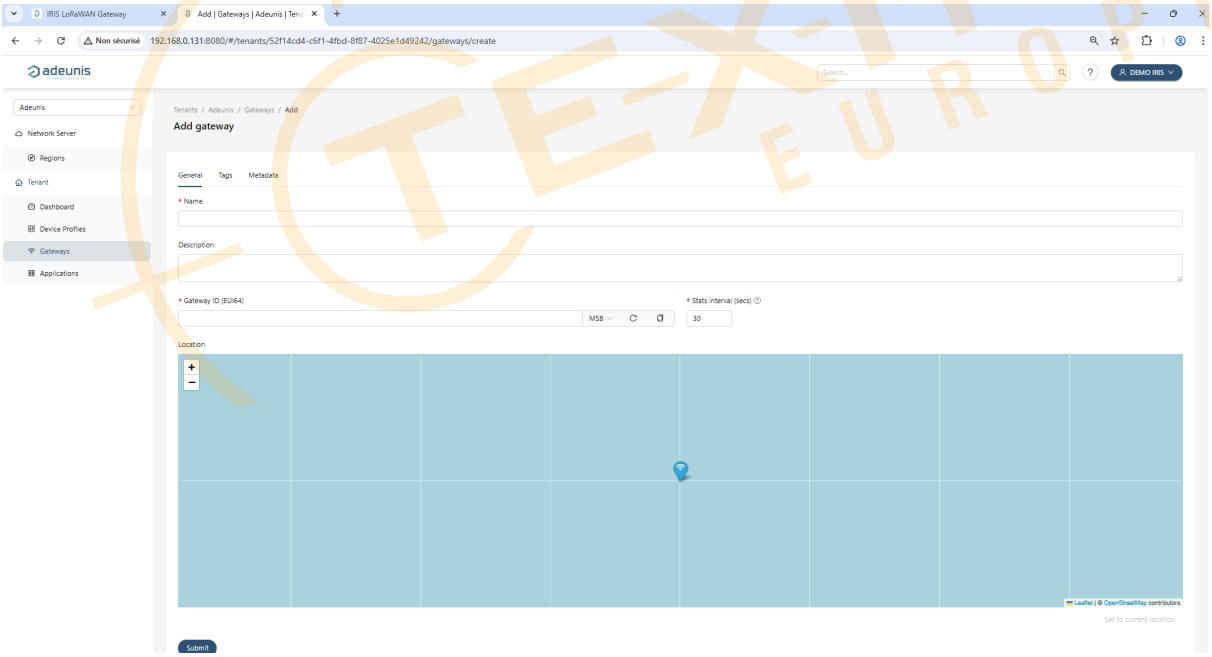
Distributed by www.texim-europe.com

Add an External UDP Packet Forwarder Gateway
Go to **Tenant** → **Gateways** → **Add gateway**.

Registration of a gateway that forwards traffic to this server via UDP Packet Forwarder is completed across three tabs:

1. **Tab: General**

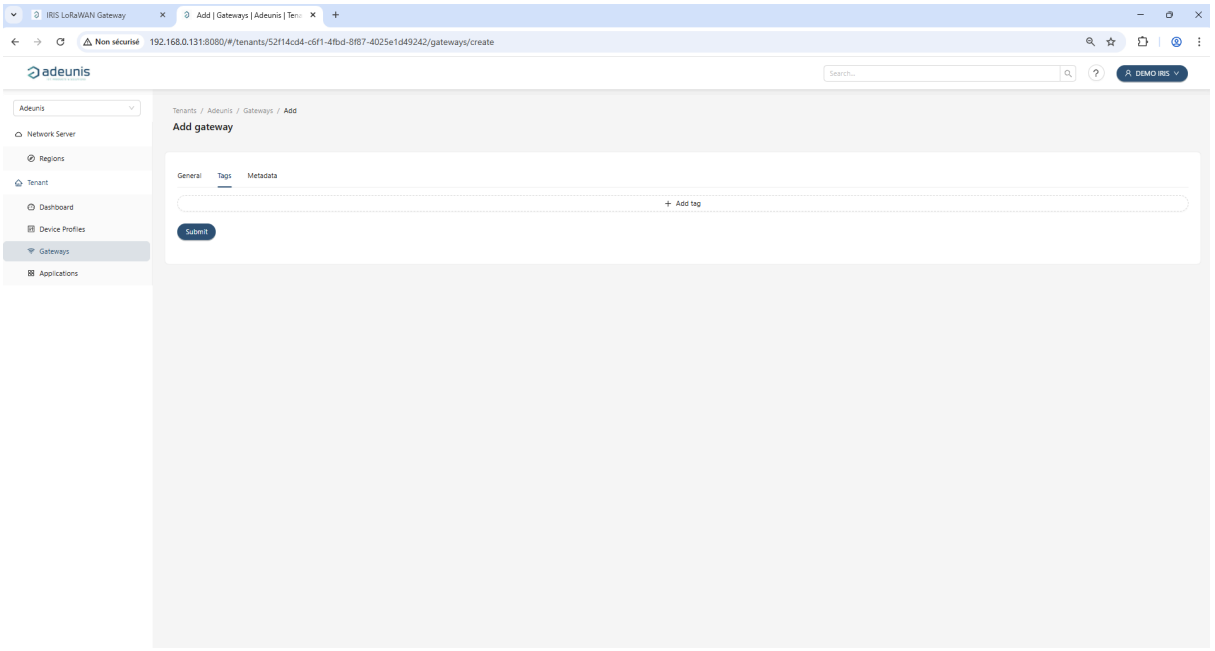
- **Name** (required) and **Description** (free text).
- **Gateway ID (EUI-64)** (required). You can toggle **MSB/LSB** byte order and use the **invert** icon if the EUI is provided LSB-first; the **copy** icon copies the value. **This value must exactly match the EUI configured on the physical gateway.**
- **Stats interval (secs)** (required): expected heartbeat period from the gateway (typical **30 s**). This setting **does not push** anything to the gateway; it must match the interval configured on the gateway. Short intervals raise control traffic; long intervals delay Online/Offline updates.
- Click submit.



2. **Tab: Tags**

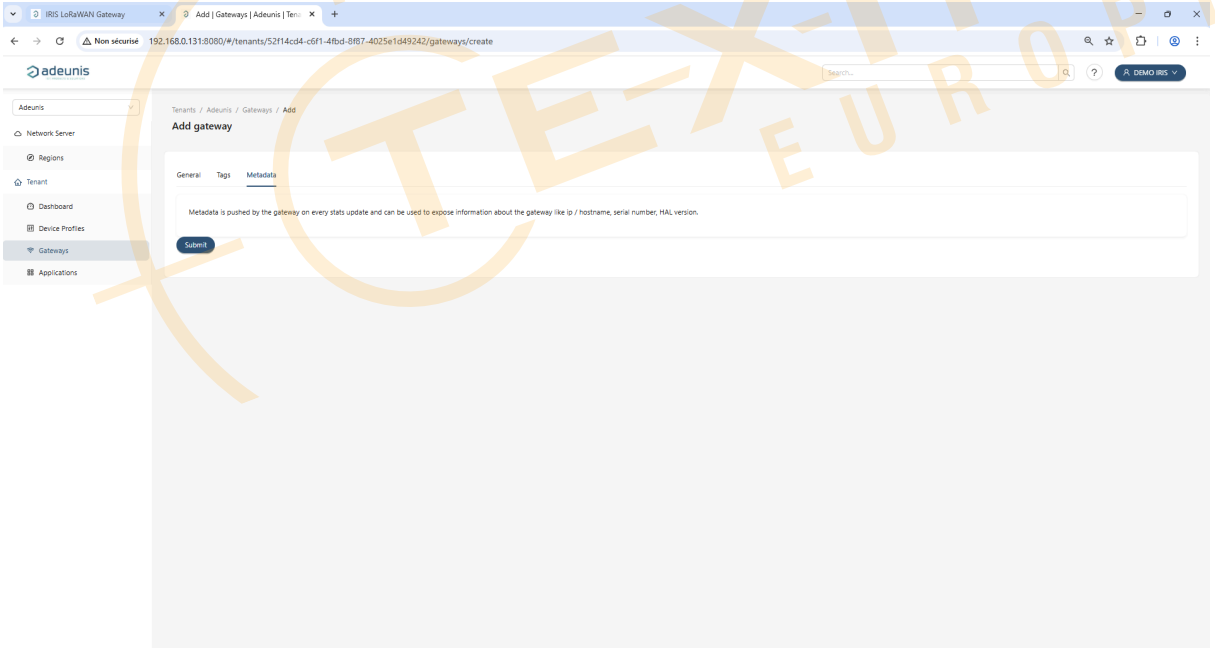
Key–value tags to help search/integrations (e.g., `site=BuildingA`, `backhaul=LTE`). They **do not affect** radio behavior.

Distributed by www.texim-europe.com



3. **Tab: Metadata**

Read-only. The gateway sends metadata with each stats/heartbeat; the server displays and attaches it to events.



Quick checks (when a new Packet Forwarder gateway stays "Never seen")

- `gateway_ID` in the packet forwarder JSON exactly matches the **Gateway ID (EUI64)** you created.

Distributed by www.texim-europe.com

- **server_address** points to the **IRIS IP** running the embedded LNS.
- UDP **1700** (up & down) is open end-to-end.
- Region settings on the physical gateway match your deployment (e.g., **EU868**).

Manage existing Gateways

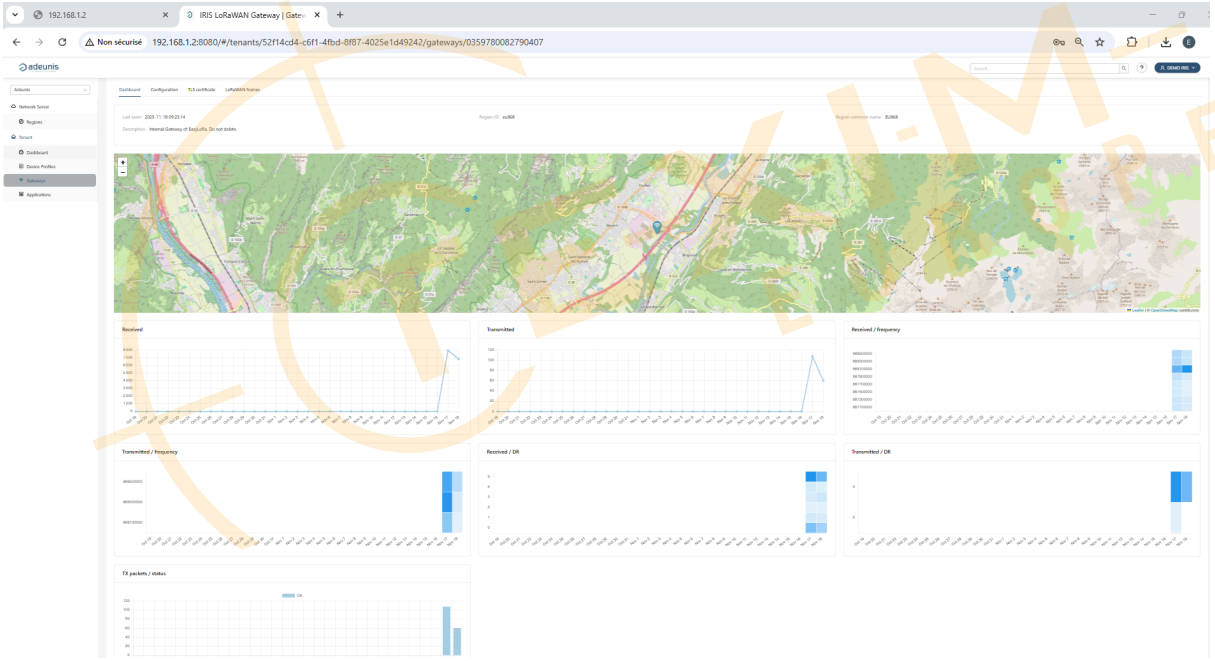
Click a **Gateway ID** in the list to open its detail view.

The header shows **Name** and **Gateway ID (EUI-64)** plus **Delete gateway**.

What you can do from the Gateway details:

- **Dashboard tab**

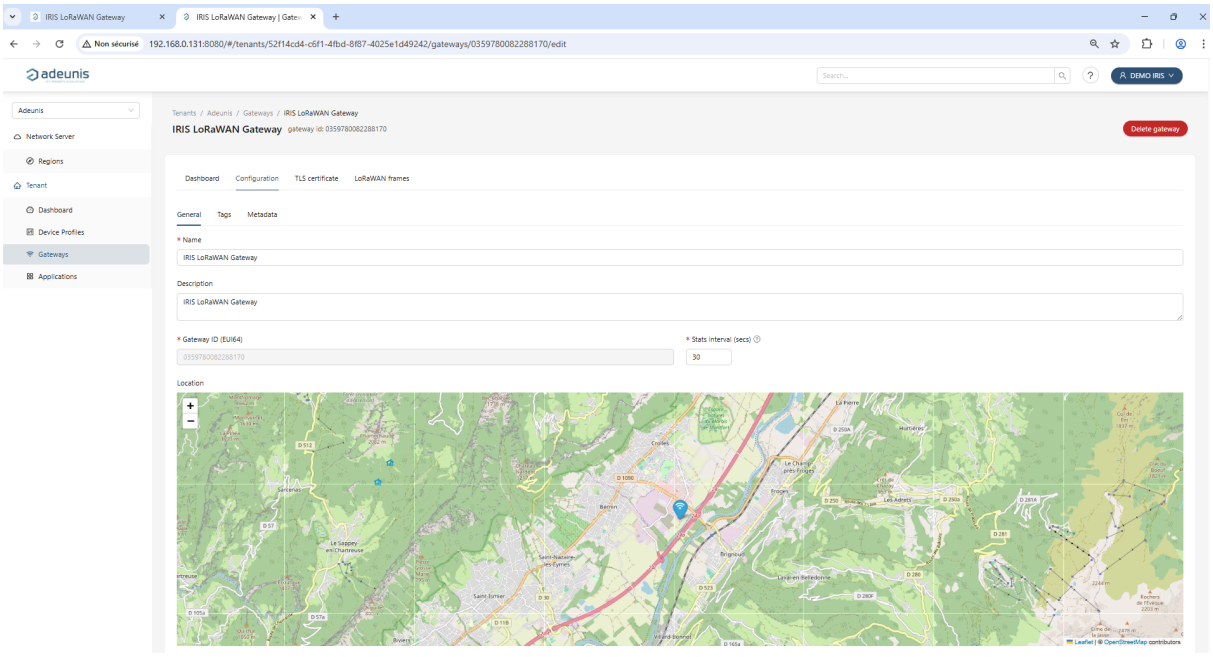
Operational summary with a **map** and charts (uplinks “Received”, downlinks “Transmitted”, frequency and DR distributions, TX status, etc.).



- **Configuration tab**

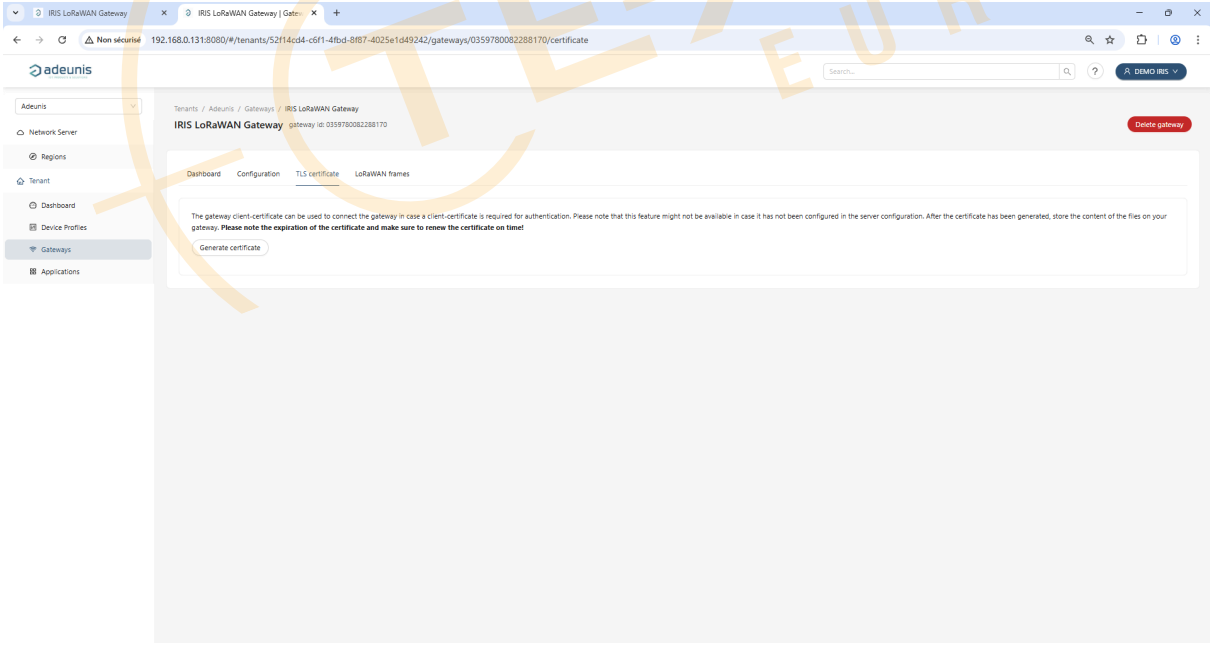
Edit name/description/region and gateway-specific options.

Distributed by www.texim-europe.com



- **TLS Certificate Tab: Not supported in this release.**

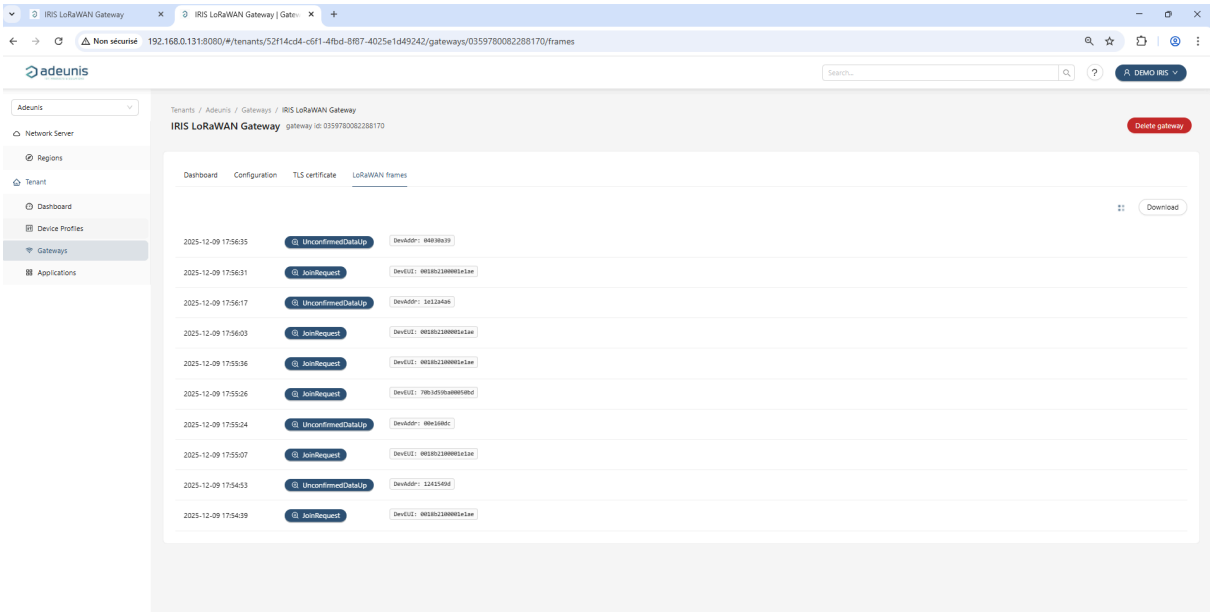
The embedded Network Server accepts traffic from gateways using the **Semtech UDP Packet Forwarder** only. **Basics Station (WS/WSS) and client-certificate authentication are not available** at this time. If this tab appears in the UI, it is informational only and can be ignored; do **not** upload or generate certificates here.



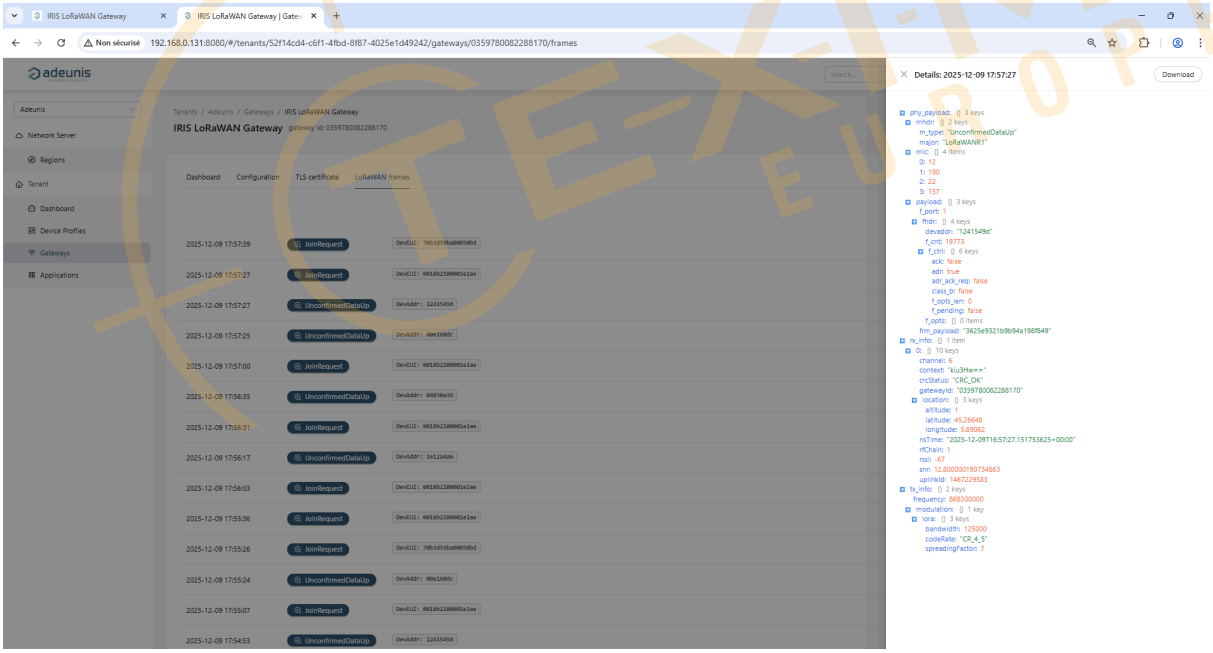
- **LoRaWAN frames tab**

Distributed by www.texim-europe.com

List of RX/TX frames for troubleshooting.



Click a frame to **view full details** (MHDR, DevAddr, FCnt, DR, frequency, MIC, etc.) and use **Download** to export the list for troubleshooting.



From the **LoRa Server Dashboard**, once you've confirmed the tenant and gateway(s) are registered and healthy, the **next step** is to **create an Application**.

An Application is the workspace that will host your device profiles and devices, and it defines how decoded data is routed downstream.

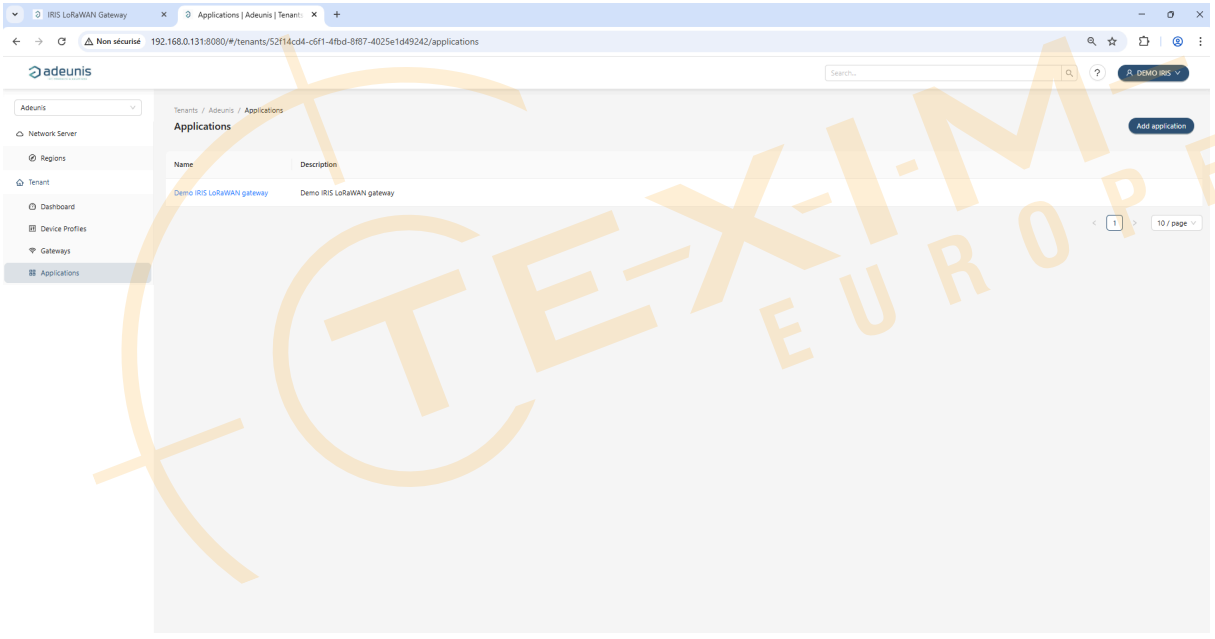
Create one per project/site (or business domain), then proceed to add a **Device Profile** and register **Devices** inside this Application. After that, you can validate joins, decode payloads, and set up MQTT(s)/HTTP(s) integration.

5.6.5. Manage Applications

An application groups LoRaWAN devices typically by purpose, location or type for example, and routes their data to the same server.

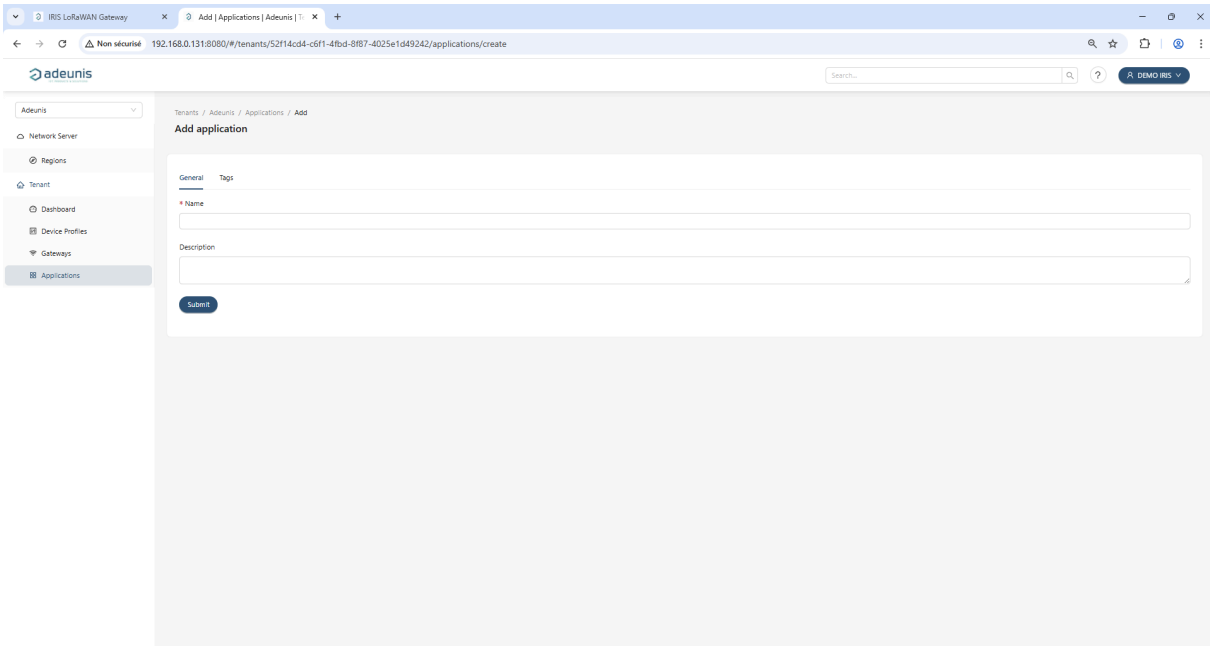
Create a New Application

1. In the dashboard, go to **Applications** → **Add application**.



2. Set **Name** and **Description** (e.g., “HQ Building – Environment Sensors”).
3. (Optional) Add **Tags** for searches and integrations (e.g. Building 1).

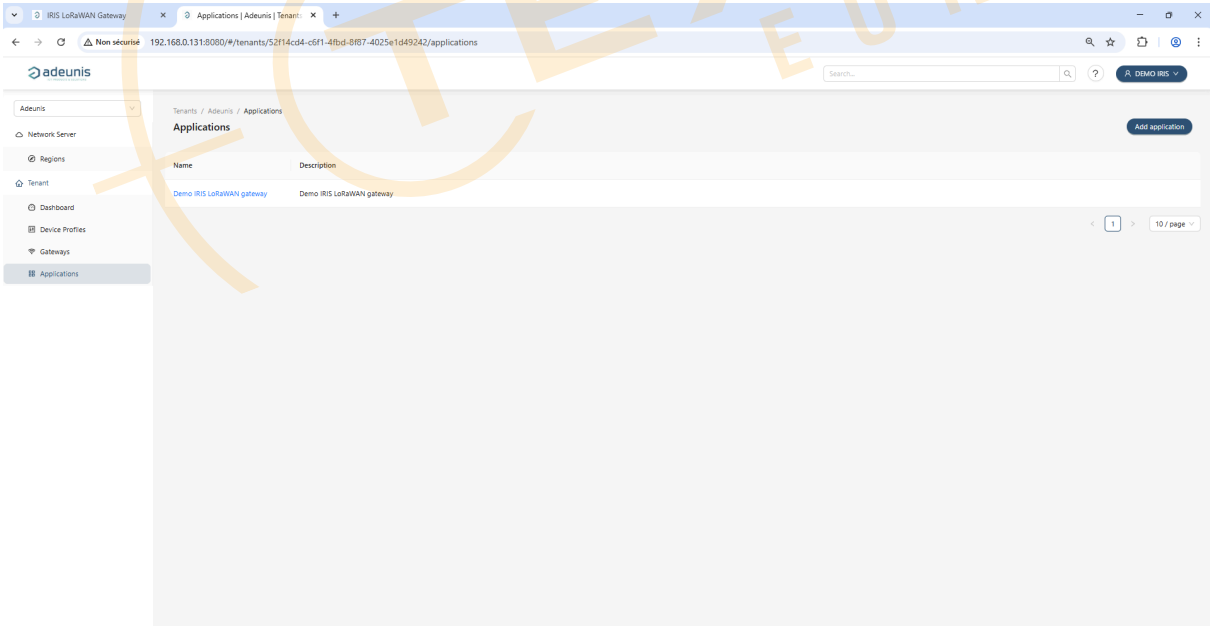
Distributed by www.texim-europe.com



4. Create the application.

Manage Existing Applications

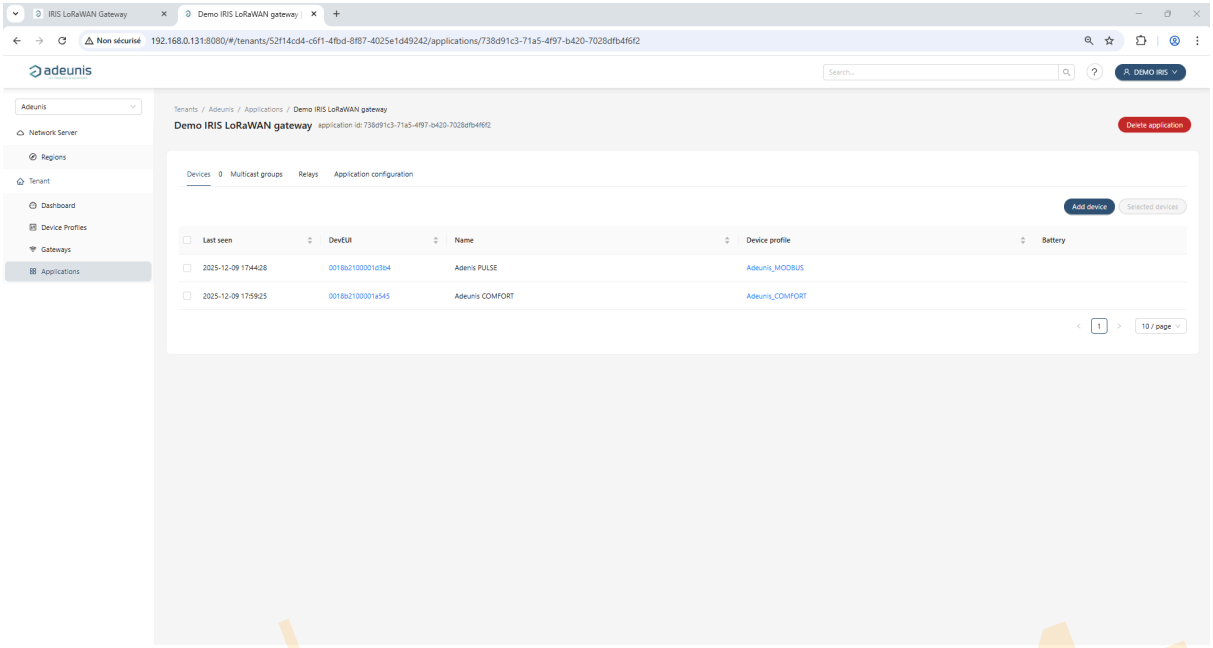
Once the application is created, click its name in **Tenant** → **Applications** to open the **Application details**.



The header shows the **Application Name** and the **Application ID**; the Application Name is useful when preparing a **bulk import** (CSV/JSON) because the `applicationName` column must reference this value.

Distributed by www.texim-europe.com

You can also **Delete application** from this page if needed (this action does not remove devices from other applications).



What you can do from the Application details:

- **Devices** tab: view the list of associated devices (Last seen, DevEUI, Name, Device profile, Battery), **add a device** (Add device), and use bulk actions from **Selected devices**.
- **Multicast groups** tab: create and manage multicast groups (Add multicast-group), assign devices, and schedule multicast downlinks (Class-C, frequency, DR, counters).
- **Relays** tab: manage relay nodes and devices operating through a relay.
- (Optional) **Application configuration** tab: adjust common settings that apply to all devices in the application.

> 📌 Configuration of data transmission to application server using MQTT/s or HTTP/s is detailed in the next chapter.

With the application created, you've defined where your devices will live and how data will be routed. The next step is to describe what each class of device looks like on the

Distributed by www.texim-europe.com

network. Create a **Device Profile** to capture the LoRaWAN specs (region/MAC), RX windows, ADR policy, payload **codec**, and measurement mapping that your sensor family will use. You'll attach this profile when registering devices.

5.6.6. Manage Device Profiles

A **device profile** captures how a family of devices communicates on the network—LoRaWAN/MAC version, LoRaWAN device class, join method (OTAA/ABP), RX windows, ADR, and the payload codec.

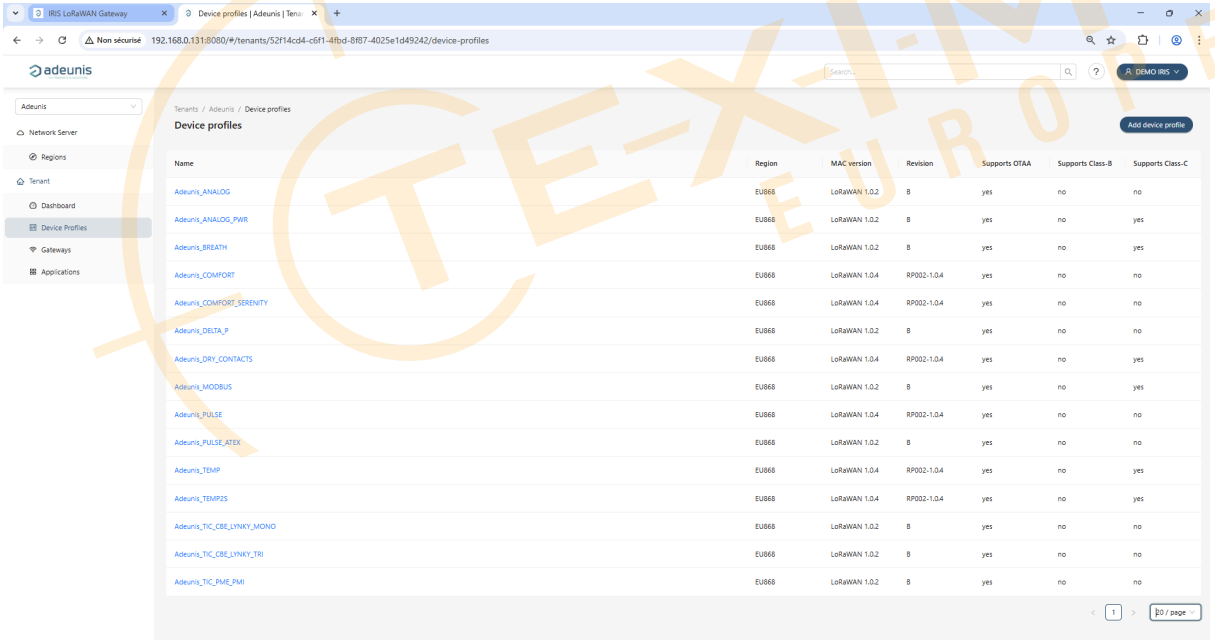
Any sensor registered on the gateway must be associated with a device profile. The embedded server uses it to interpret uplinks, queue downlinks and display measurements.

This information comes from the device manufacturer's documentation and must match the sensor firmware.

Pre-Loaded Device Profiles

IRIS gateway ships with **pre-loaded profiles for Adeunis devices**.

You can use them as-is or duplicate them as templates.



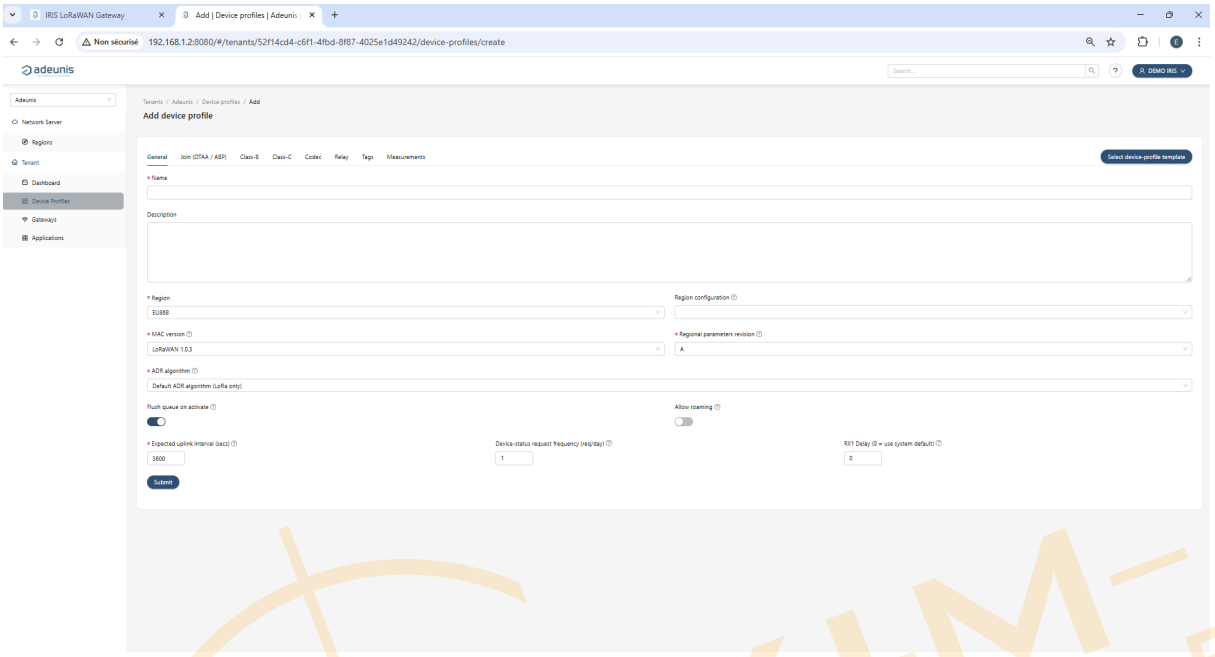
Create a New Device Profile

For other device vendors, **create a new device profile** to match any sensor family you deploy.

Distributed by www.texim-europe.com

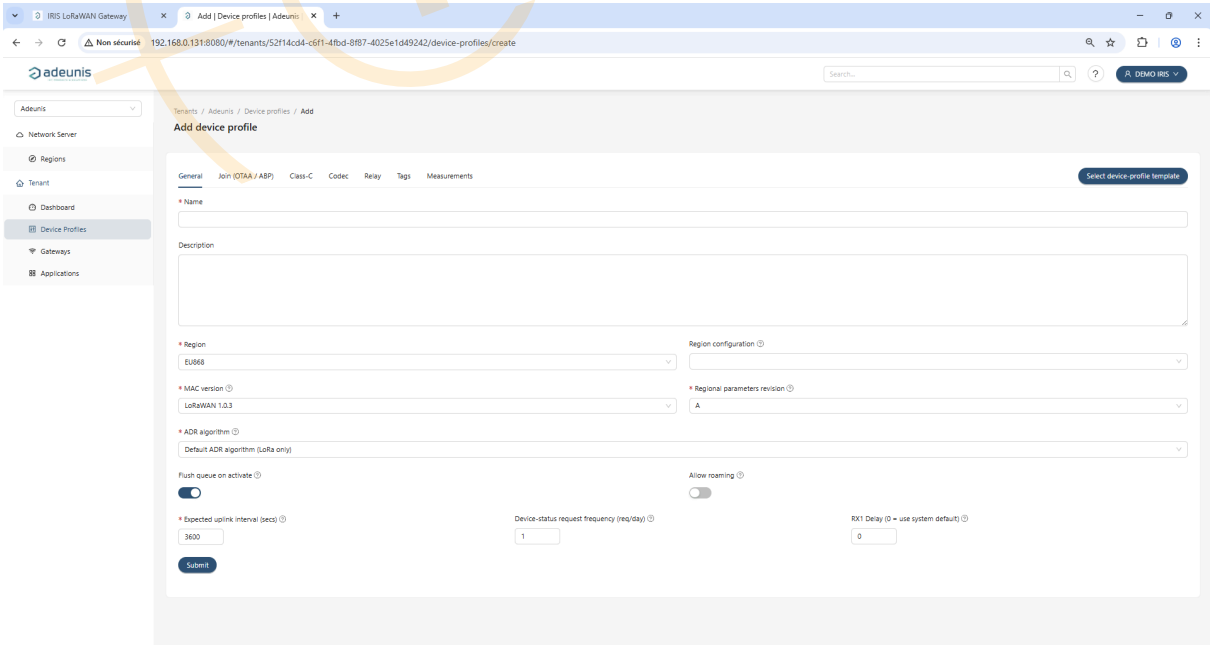
To create one,

1. Open the dashboard and go to **Device profiles → Add device profile**.
2. Fill the 7 tabs described below.
3. Then **Submit.**



Tab: General

This tab defines the base profile for a device type.

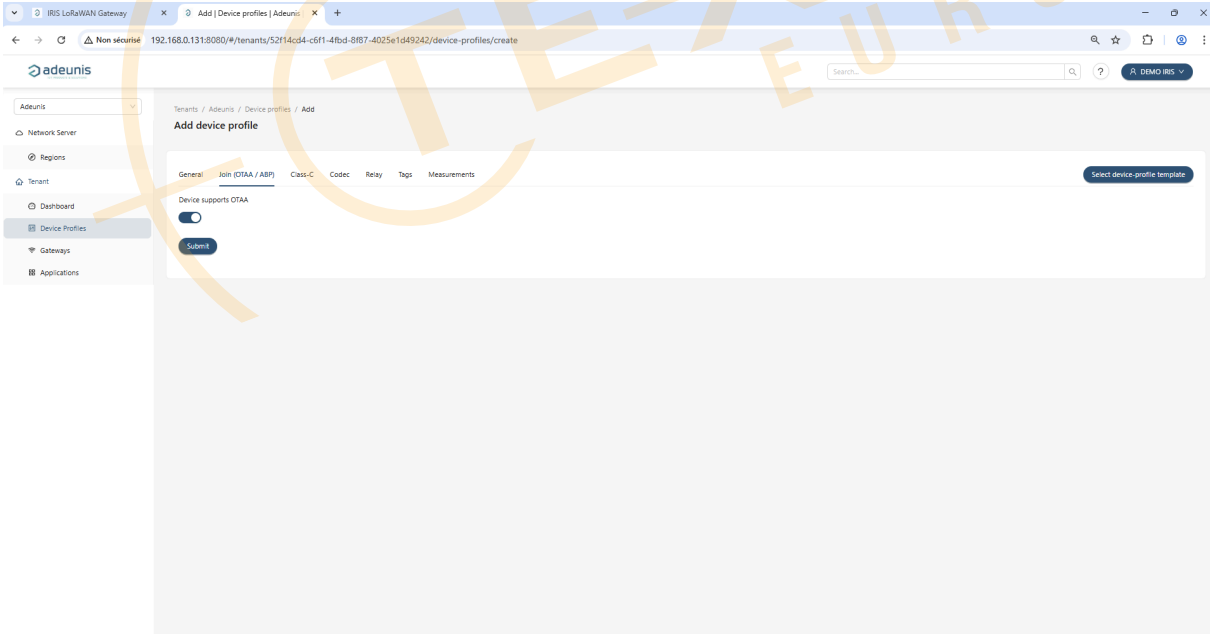


Distributed by www.texim-europe.com

- **Name** the profile with a clear, unique name (e.g., “Motion Sensor-PIR-EU868-ClassA-1.0.2”)
- (Optional) Enter a **description** for the device profile for context
- **Region**: **EU868** (fixed for IRIS).
- **MAC version:** LoRaWAN version used by the device (e.g., 1.0.2, 1.0.3).
- **Region configuration** / **Regional parameters revision:** Select the revision that matches the device (e.g., *RP002-1.0.x / A*).
- **ADR algorithm:** Keep **Default ADR (LoRa only)** unless you have a specific need.
- **Flush queue on activate: On** recommended (clears stale downlinks when a device (re)joins).
- **Allow roaming:** Leave **Off** unless you operate with roaming agreements.
- **Device-status request frequency (req/day):** How often the server requests status (battery, margin). 0 = disabled.
- **Expected uplink interval (sec): Important for health/status**. Set a realistic interval (e.g., 3600 for hourly sensors) so the dashboard can flag missing uplinks.

Tab: Join

This tab defines how devices using this profile we be activated.

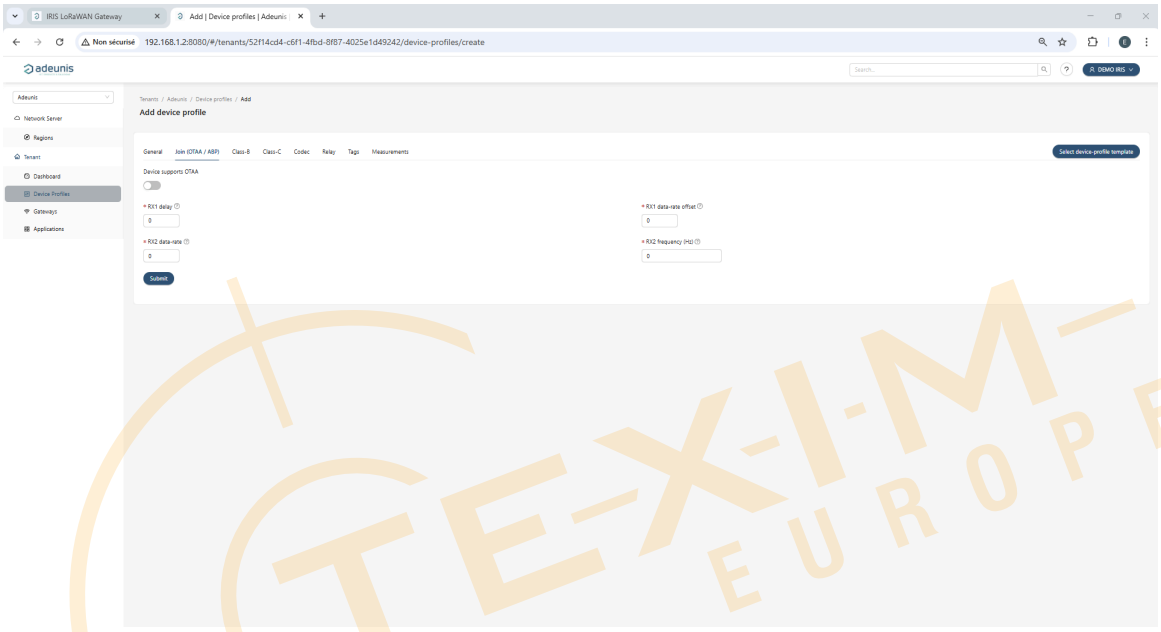


- **Device supports OTAA: On** for OTAA (recommended). **Off** switches to ABP behavior.
- **OTAA Enabled:**

Distributed by www.texim-europe.com

- Device activates via a secure join. When creating each device, OTAA credentials must be provided.
- Advantages: dynamic session keys, higher security, simpler network changes and reprovisioning.

- **ABP Enabled:**
  - The profile uses ABP. When creating the device, fixed keys must be loaded.
  - Advantages: Starts without a join process.
  - Disadvantages: Less secure, keys are not automatically renewed, more sensitive to frame counter desynchronization.

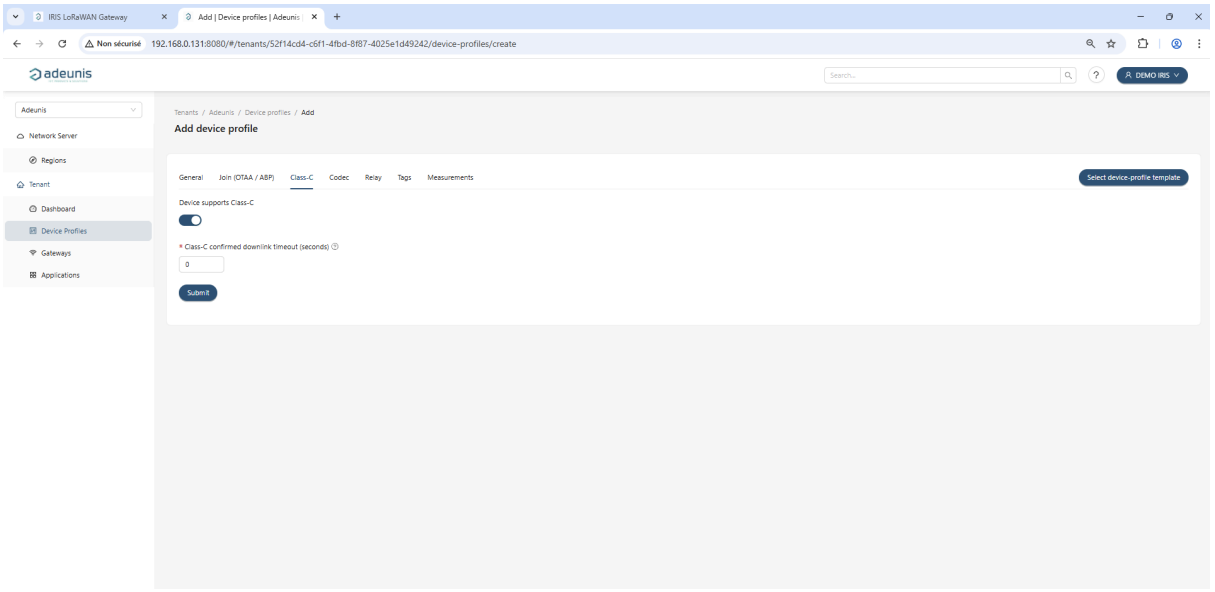


  - **RX1 delay:** Seconds before RX1 opens. Leave **0** to use network defaults unless your device requires a specific value.
  - **RX1 data-rate offset:** Leave **0** unless specified by the device.
  - **RX2 data-rate** / **RX2 frequency (Hz):** Leave **0** to use EU868 defaults, or set explicit values if your device mandates them.

Tab: Class-C (optional)

Class C keeps the receive windows (RX) open almost continuously, closing it only during ulink transmission. This is suitable for actuators that need to receive commands at any time with low latency, at the cost of higher power consumption.

Distributed by www.texim-europe.com

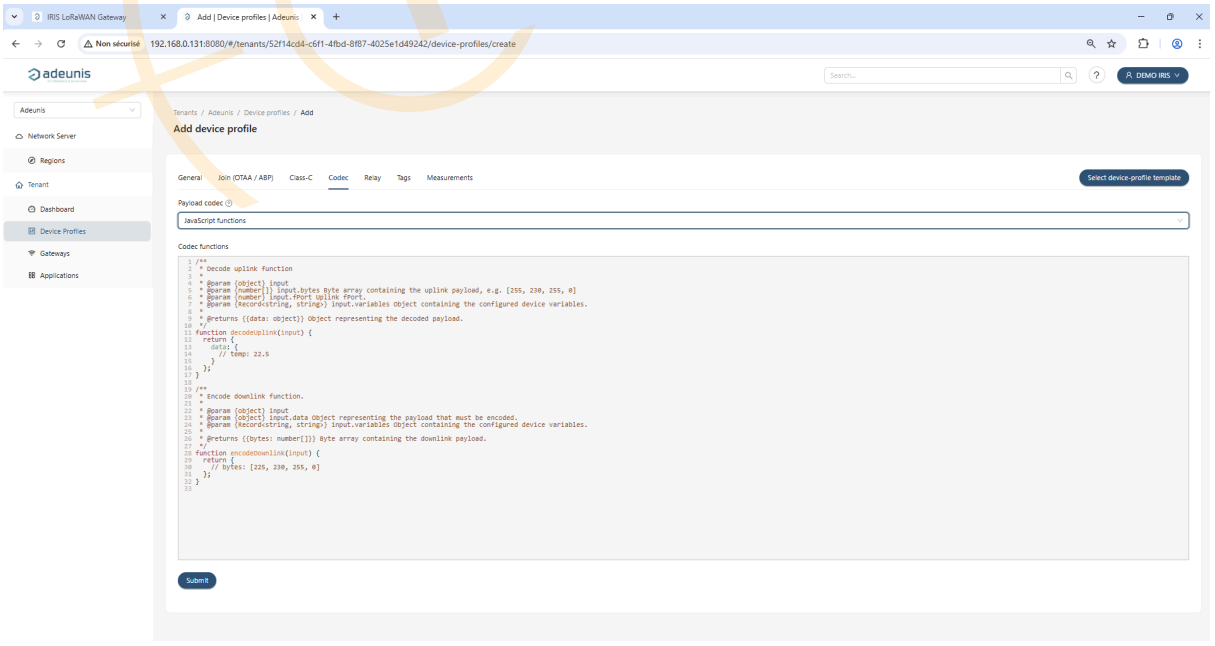


- **Device supports Class-C:** Enable only for devices powered and designed for Class-C.
- **Class-C confirmed downlink timeout (s):** Time the server waits for ACK to a confirmed downlink while in Class-C.

Tab: Codec

This tab defines how the server interprets the received bytes (uplinks) and, optionally, how it generates bytes for transmissions (downlinks).

If you need decoded values on the dashboard or for routing, add a **payload codec.**



Choose how payloads are decoded/encoded:

Distributed by www.texim-europe.com

1. **None:** Raw payloads only.

The payload is kept as a byte array, with representation in base64/Hex depending on the integration.

When to use this option:

- For initial testing.
- When the application server decodes the payload independently.
- For devices with proprietary formats that cannot be decoded on the server.

2. **Cayenne LPP:** Decoded payload following LPP standard.

The payload is decoded automatically following the Cayenne Low Power Payload (LPP) standard.

When to use this option:

- Select if your device speaks LPP.

3. **JavaScript functions:** Allows writing two JavaScript functions
   - `decodeUplink(input)` → converts bytes to JSON
   - `encodeDownlink(input)` → converts JSON to bytes

When to use this option:

- For devices with proprietary payload formats.

📌 Keep all decoders under version control and note the **profile** → **codec** mapping in your site dossier.

Tab: Relay (advanced)

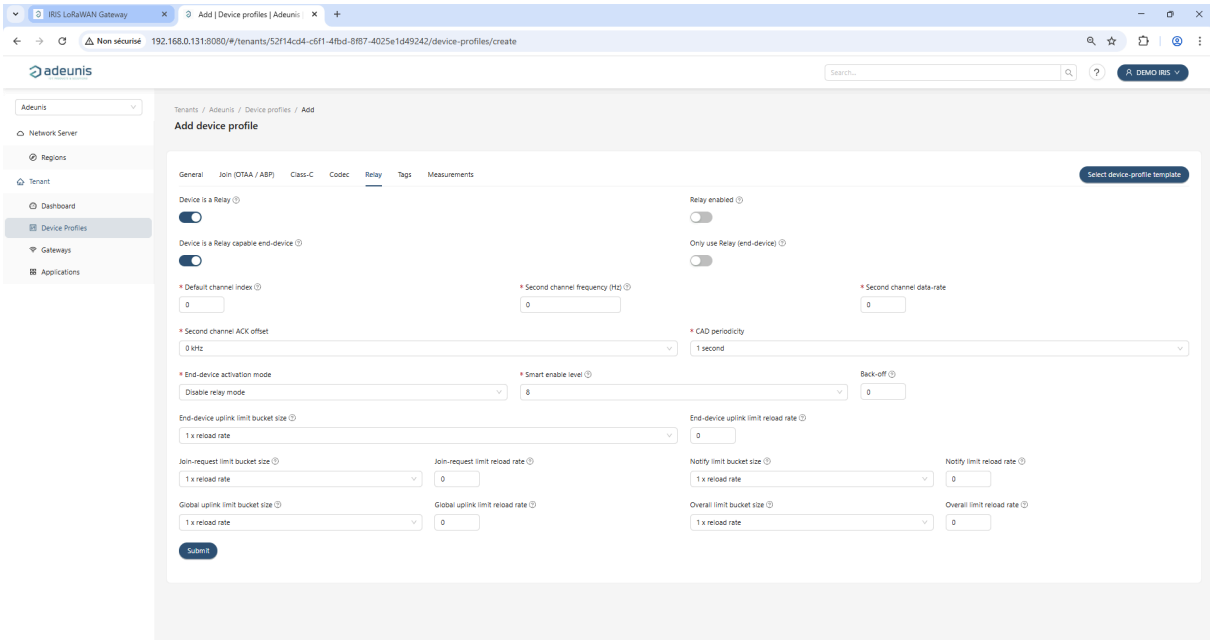
LoRaWAN supports a Relay mode (intelligent repeater) to extend coverage without installing an additional gateway.

A relay listens to nearby devices and forwards their frames to the network; conversely, it can deliver downlinks to those devices.

This tab defines parameters for **LoRaWAN Relay** features.

Unless you deploy relays, **leave everything disabled.**

Distributed by www.texim-europe.com



- **Device is a Relay:** Turn on only for actual relay devices.

The device will act as an intermediary between other end-devices and the network.

It should be placed where there is good coverage to the gateway and proximity to the devices depending on it.

- **Device is a Relay-capable end-device:** For end-devices using a relay path.

This option should be enabled when the profile is for an end-device that can operate through a relay instead of communicating directly with the gateway.

The device and relay must share compatible configuration (regional parameters, RX windows, etc.)

- **Additional fields** (second channel, CAD periodicity, back-off, bucket sizes) are for fine-tuning relay behavior; keep defaults if unsure.

Tab: Tags

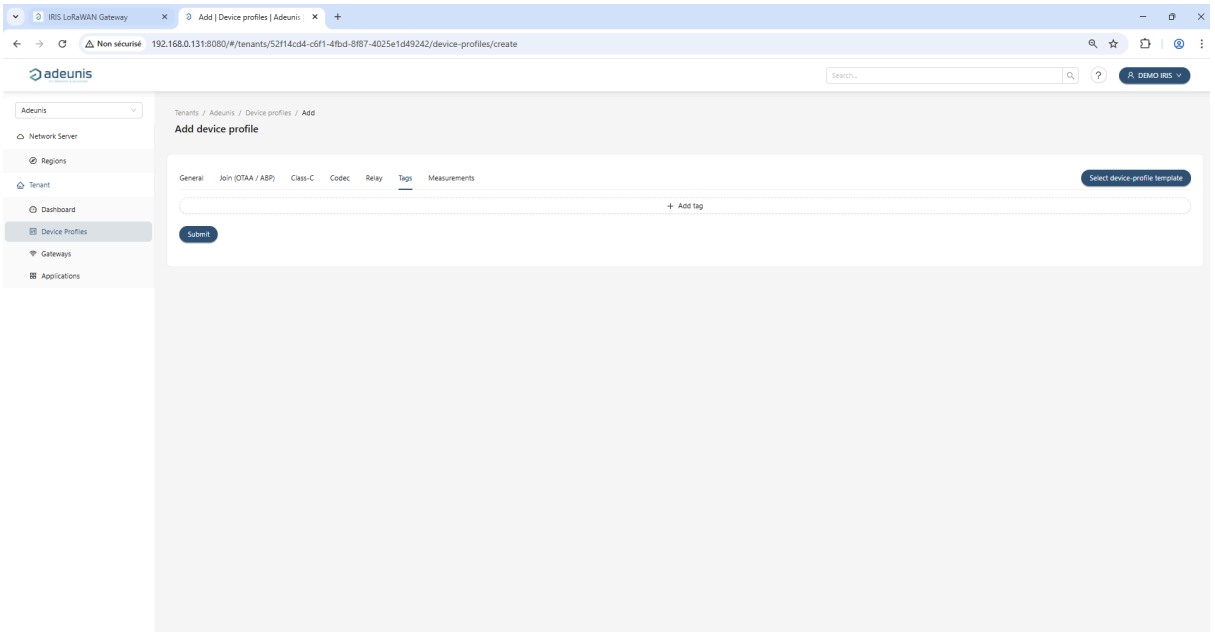
Tags are key–value metadata.

Tags defined in a Device Profile apply to all devices using this profile.

Tags are useful for

- Searching: within the dashboard filter devices by model, vertical, etc.
- Routing: tags are sent along with device events
- Dashboards: group by model, site, customer, etc.

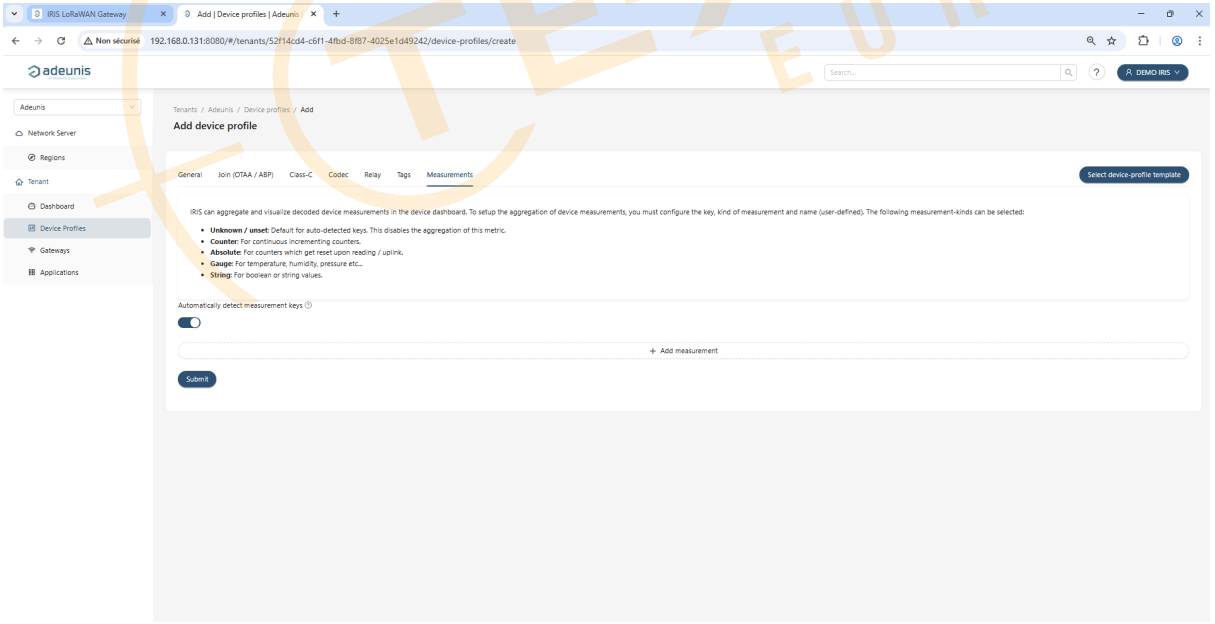
Distributed by www.texim-europe.com



- Click on **Add Tag** to create Key/Value pairs
- **Add as many tags** as needed (e.g., `site=BuildingA`, `usecase=energy`).

Tab: Measurements

This tab defines which decoded keys should be aggregated and how they are interpreted and displayed in dashboards and queries.



- Measurements are read from the data object returned by the decodeUplink() function when using a Javascript codec. For example, if the function returns { data: {

Distributed by www.texim-europe.com

temperature: 21.7, batt: 3.92, pulses: 15 } }, you can map temperature, batt, and pulses.

- **Automatically detect measurement keys:** If enabled the IRIS gateway learns keys from decoded payloads and treat them as metrics with type “Unknown”. This option is good for quick starts but we recommend to disable and define metrics manually to avoid noise.
- **Manual entries:** Add rows to define Key, Kind and Name of each measurement of interest.
  - **Measurement Key**: Exact JSON key produced by your Codec (`temperature`, `kWh`, `state`, ...)
  - **Measurement Kind**: Metric type (how it is aggregated) – `Counter` (monotonic), `Absolute` (reset on read), `Gauge` (e.g., °C, %RH), or `String`
  - **Measurement Name** (optional): Friendly label used in the dashboard (e.g. “Ambient temperature”)

If you enable auto-detection, you can still add explicit rows for critical metrics to control their type and label.

Measurement Types (kind)

Metric	Purpose	Example
Unknown / Unset	No aggregation. Useful for values you do not want to graph or sum	“Motion Sensor-PIR-EU868-ClassA-1.0.2”
Counter	Cumulative counter that never decreases; the platform calculates increments between readings	pulse counters, energy
Absolute	Counter that resets after each uplink or periodically; the absolute value reported is used	events per message
Gauge	Instantaneous measurements Aggregated as average/min/max over intervals	Temperature, humidity, pressure, battery, RSSI, etc.
String	Boolean or text values Not aggregated numerically; displayed as the last known value	Status, alarm

📌 Keep Measurement keys exactly the same as in the Codec (case-sensitive).

Parameter Quick Reference

General Tab

Field	Purpose	Typical value
Name / Description	Identify the profile	“Motion Sensor-PIR-EU868-ClassA-1.0.2”
Region	Radio region	**EU868**
MAC version	LoRaWAN spec implemented by device	1.0.2 or 1.0.3
Region config / RP revision	Regional parameters set	RP002-1.0.x / A
ADR algorithm	Adaptive data rate policy	Default ADR (LoRa only)
Flush queue on activate	Avoids sending stale downlinks after rejoin	**On**
Allow roaming	Inter-NS roaming	Off
Device-status request freq	Battery/margin polling	0–1/day
Expected uplink interval	Offline detection baseline	e.g., 3600 s

Join (OTAA/ABP) Tab

Field	Purpose	Note
Device supports OTAA	Join method	On = OTAA (recommended)
RX1 delay	Opens RX1 after join/uplink	0 = server default
RX1 DR offset	RX1 data-rate offset	0 if unsure
RX2 DR / Freq	RX2 settings	0 = server default (EU868)

Class Tab

Field	Purpose	Note
Class-C support	Continuous RX	Mains-powered devices
C-confirmed downlink timeout	Wait for ACK in Class-C	Seconds

Codec Tab

Option	Use when	Output keys drive...
None	Raw hex handled externally	—
Cayenne LPP	Device sends LPP	Measurements auto-mapped
JavaScript functions	Custom payloads	Dashboard & routing

Measurements Tab

Distributed by www.texim-europe.com

Field	Purpose	Example
Auto-detect	Discover keys seen in `decodeUplink`	✔️ for fast setup
Key / Kind / Name	Manual mapping & label	`temperature` / Gauge / “Room temp”

Good Practices

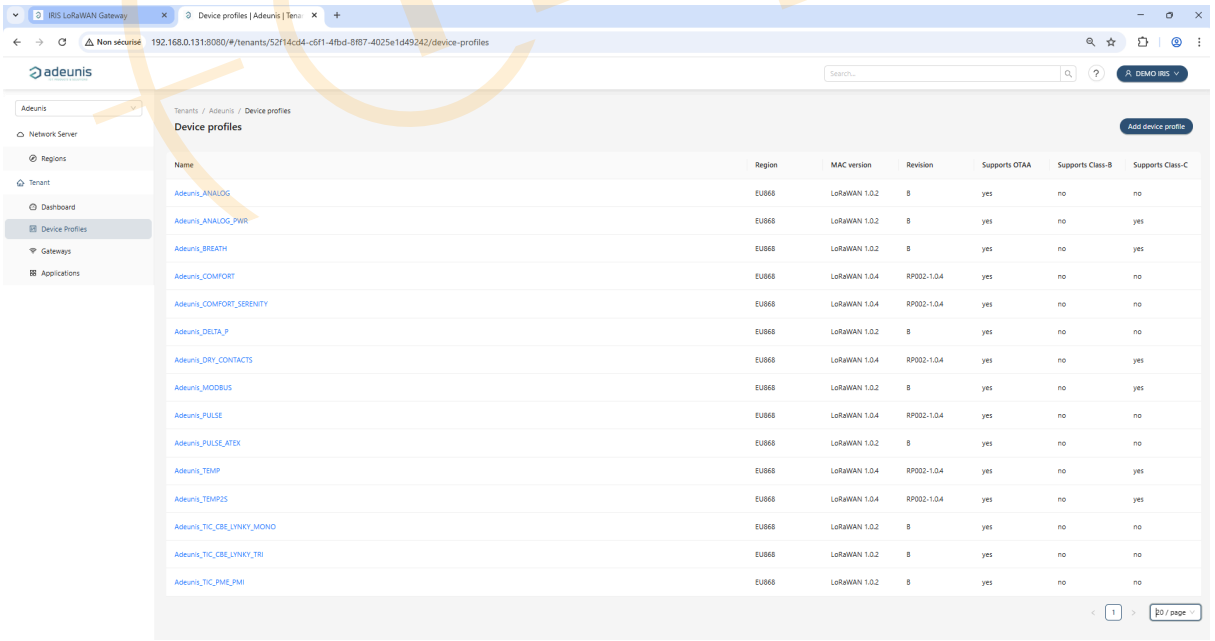
- One profile per **device family & firmware line**; clone and adjust when the vendor changes MAC/RP settings.
- Keep **Expected uplink interval** realistic; it underpins your “online/offline” view.
- Version your **JavaScript codecs** and test them with sample payloads before mass deployment.
- Ignore the **Relay** tab unless you explicitly deploy LoRaWAN Relay.

Manage Existing Device Profiles

The **Device profiles** page lists every profile available on the gateway.

For each line you’ll see the main attributes used by the network server (e.g., **Name**, **Region**, **LoRaWAN MAC version**, **Revision**, **Supports OTAA**, **Supports Class-B/C**).

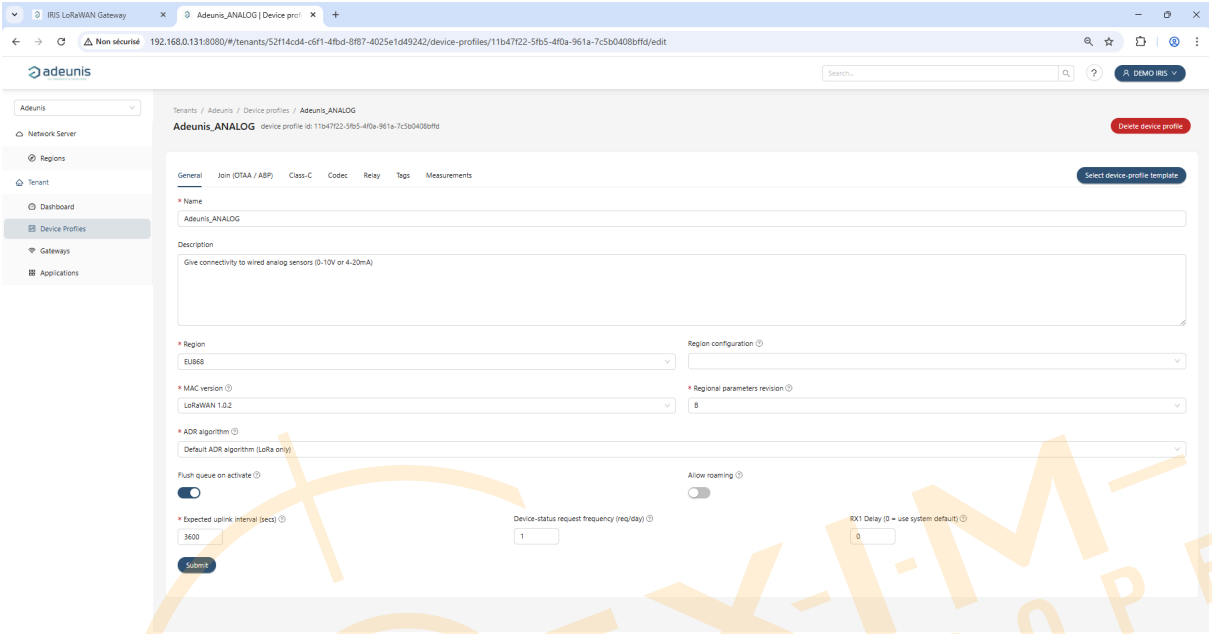
Use the search box (top-right) to filter the list, or **Add device profile** to create a new one.



Distributed by www.texim-europe.com

Click any profile row to access its full configuration tabs (**General**, **Join (OTAA/ABP)**, **Class-C**, **Codec**, **Relay**, **Tags**, **Measurements**).
The header shows the **Device Profile Name** and the **Device Profile ID**; this **Profile Name** is required when preparing a bulk import (CSV/JSON) because the `deviceProfileName` column must reference this value.

From this page, you can also **edit** the profile parameters or **Delete device profile** if needed (ensure no active devices still rely on this profile before deleting it).



With your **Application** and **Device Profile(s)** in place, you can now register end-devices (OTAA or ABP) in the embedded LoRaWAN Server.

5.6.7. Add Devices (Single & Bulk import)

Your profile is ready; now register the actual hardware.

In **Create a device**, you add each physical sensor under the application, select a **Device Profile**, and provide its identifiers/keys (e.g., DevEUI, JoinEUI/AppEUI, AppKey for OTAA).

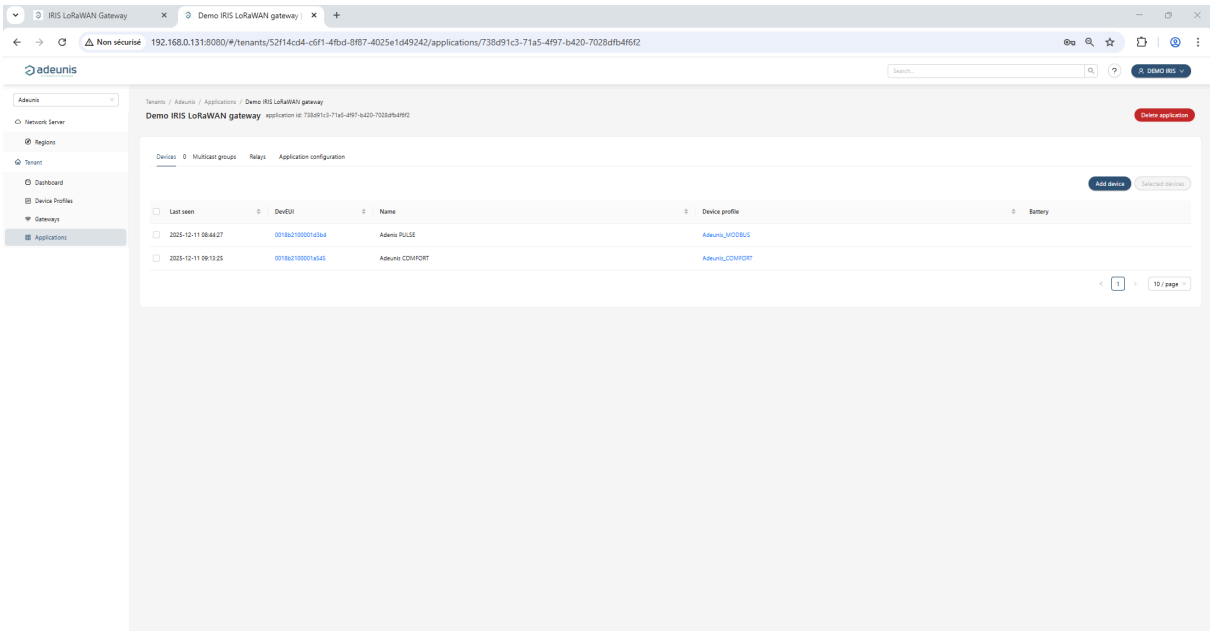
You can add devices one-by-one or import them in bulk—once saved, the device can join and you'll start seeing live frames and decoded measurements.

Add a Single Device

To add a single device,

Distributed by www.texim-europe.com

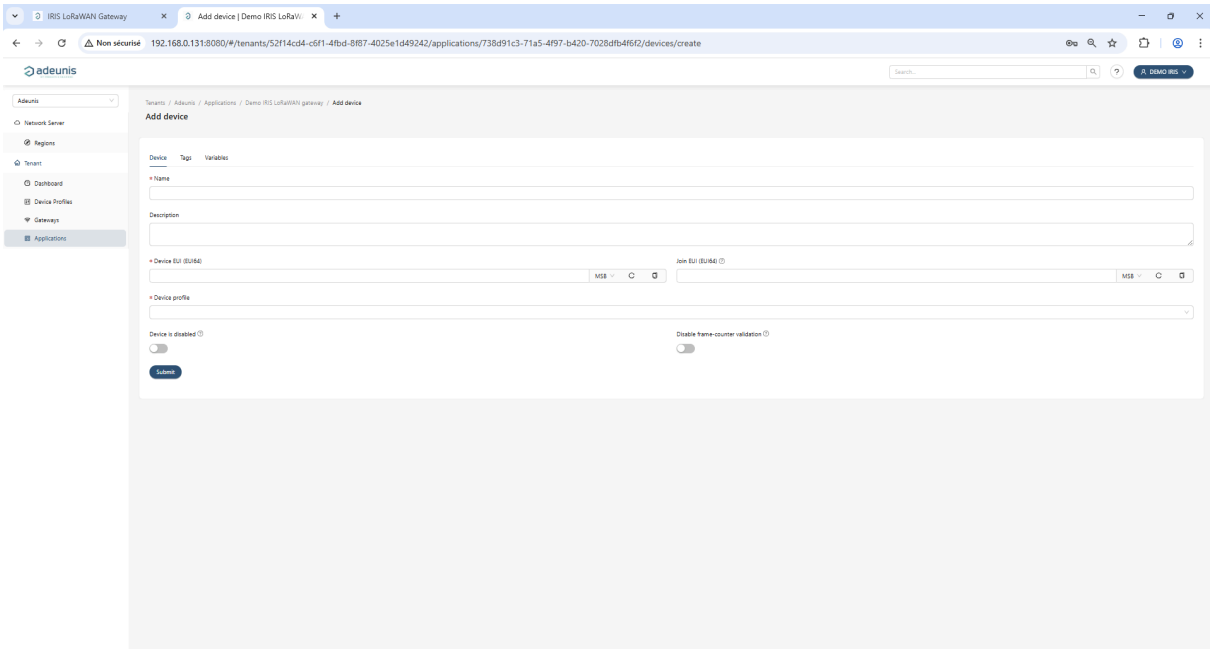
1. Open the dashboard and go to **Applications** → **<your application>** → **Devices** → **Add device.**



2. Complete the **Device Tab**.

- **Name**: Human-readable label (site/room/sensor role).
- **Description**: Optional context.
- **Device EUI (EUI64)**: 16-hex characters (8 bytes). Use the **MSB/LSB** selector to match the label on the device; **MSB** is typical.
- **JoinEUI (EUI64)** (a.k.a. AppEUI): 16-hex, required for most OTAA devices. Respect the **MSB/LSB** selector.
- **Device profile**: Select the profile you created (e.g., *Adeunis_TEMP*).
- **Device is disabled**: Keep **off** for normal operation.
- **Disable frame-counter validation**: **Leave off** (only enable temporarily for ABP troubleshooting).

Distributed by www.texim-europe.com



3. Then click **Submit to create the device.**
4. **Tags tab (optional)**

Add `key = value` pairs (e.g., `building=A`, `floor=2`). Tags help search, filtering, and routing rules.

5. **Variables tab (optional)**

   Add `key = value` pairs consumed by your **payload codec** or integrations (e.g., `temp_unit=°C`, `pulse_factor=1.0`).

6. **Set join or session keys**

   Open the newly created device → **Keys (OTAA/ABP)** and configure:

- **OTAA (LoRaWAN 1.0.x)**: set **AppKey** (32-hex).
- **OTAA (LoRaWAN 1.1.x)**: set **NwkKey** and **AppKey** (both 32-hex).
- **ABP**: set **DevAddr**, **NwkSKey / FNwkSIntKey / SNwkSIntKey / NwkSEncKey** and **AppSKey** as required by your device/profile.

  Save the keys.

7. **Commission and verify**

   Power the device and trigger a join/uplink.

   In **Applications** → **Devices** → **<device>** → **LoRaWAN frames**, verify **Join-Accept** (OTAA) and incoming **uplinks**.

   The **Dashboard** tiles will start populating if you configured **Measurements** in the Device Profile.

Distributed by www.texim-europe.com

Parameter Quick Reference

Parameter	Purpose	Notes
Name	Friendly identifier	Free text
Description	Context	Optional
Device EUI (EUI64)	Unique device identity	16-hex; respect MSB/LSB
JoinEUI (EUI64)	Join scope (OTAA)	16-hex; required for most OTAA
Device profile	Radio/codec behavior	Pick matching profile
Device is disabled	Admin lock	Off = active
Disable frame-counter validation	Security bypass	Keep **off** (test only)
Tags	Metadata	Key/value
Variables	Codec/integration params	Key/value
Keys (OTAA/ABP)	Security material	Configure after creation

📌 If a device never joins, re-check: band (**EU868** only at this firmware), profile MAC version, AppKey/NwkKey endianness, and Authorized IPs / CA Certificates if your routing depends on secure services.

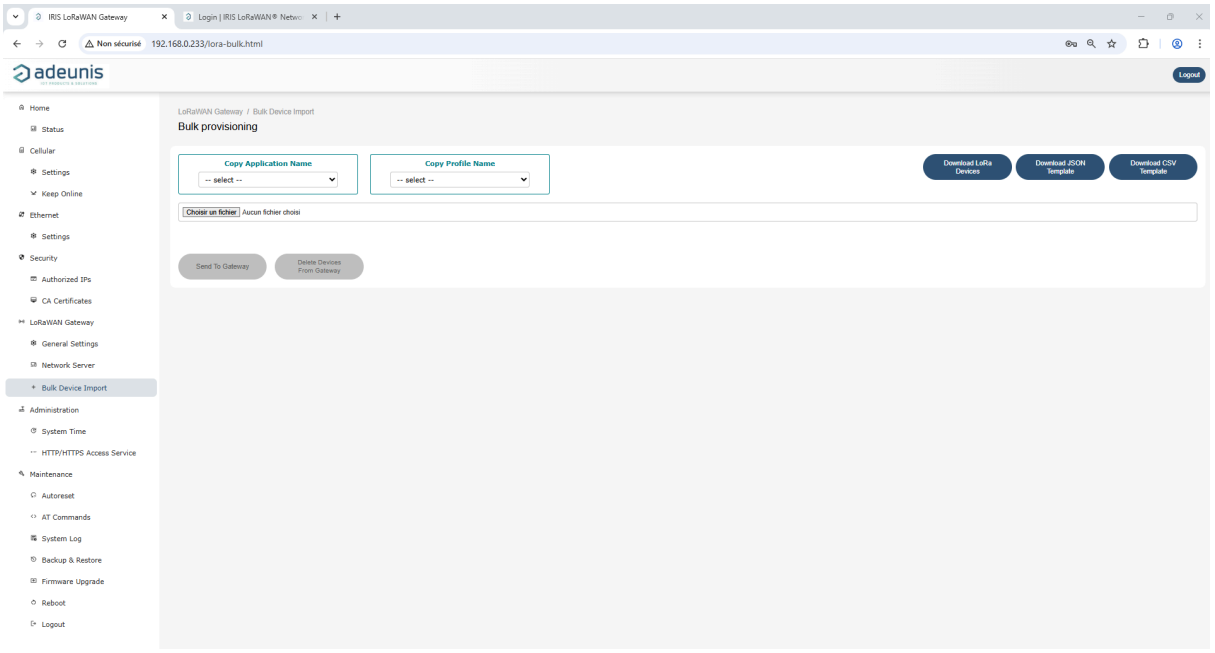
An example is described in **ANNEX 3 REGISTERING AN ADEUNIS COMFORT SENSOR**

Add Multiple Devices (Bulk Import)

This tool lets you import or remove many devices in one operation using a JSON or CSV file.

1. Open the gateway Web GUI and go to **LoRaWAN → Bulk Device Import**

Distributed by www.texim-europe.com



Click **Download JSON template.**


```
{
  "devices": [
    {
      "name": "Example Adeunis Breath Sensor",
      "description": "Sensor for measuring the level of fine particles and TVOCs",
      "devEui": "0018B2100000BC44",
      "appKey": "384E786F39A54445BE9C279E0EF1E0E9",
      "deviceProfileId": "988C290B-2687-44FD-8FFB-21853EF84A8C",
      "applicationId": "33884567-9A15-4A5D-965A-72B7ADA73FB7"
    },
    {
      "name": "Example Adeunis Comfort Sensor",
      "description": "Sensor for measuring temperature, ambient humidity, CO2 and VOC level",
      "devEui": "0018B21000018EBC",
      "appKey": "D2DD78FF18DC47EFBF85EADCCB2C13C9",
      "deviceProfileId": "988C290B-2687-44FD-8FFB-21853EF84A8D",
      "applicationId": "33884567-9A15-4A5D-965A-72B7ADA73FB7"
    },
    {
      "name": "Example Humidity Sensor",
      "description": "Sensor for measuring humidity",
      "devEui": "B2903AD1845CEE82",
      "appKey": "D2DD78FF58DC47EFBFA5EADCCB2C13C0",
      "joinEui": "B31D15AC45E4FFB2",
      "deviceProfileId": "988C290B-2687-41FD-8FFB-21853EF84A80",
      "applicationId": "33884567-9A15-4A5D-965A-72B7ADA73FB7",
      "isDisabled": false,
      "skipFCntCheck": false
    },
    {
```


or **Download CSV template**.

Distributed by www.texim-europe.com

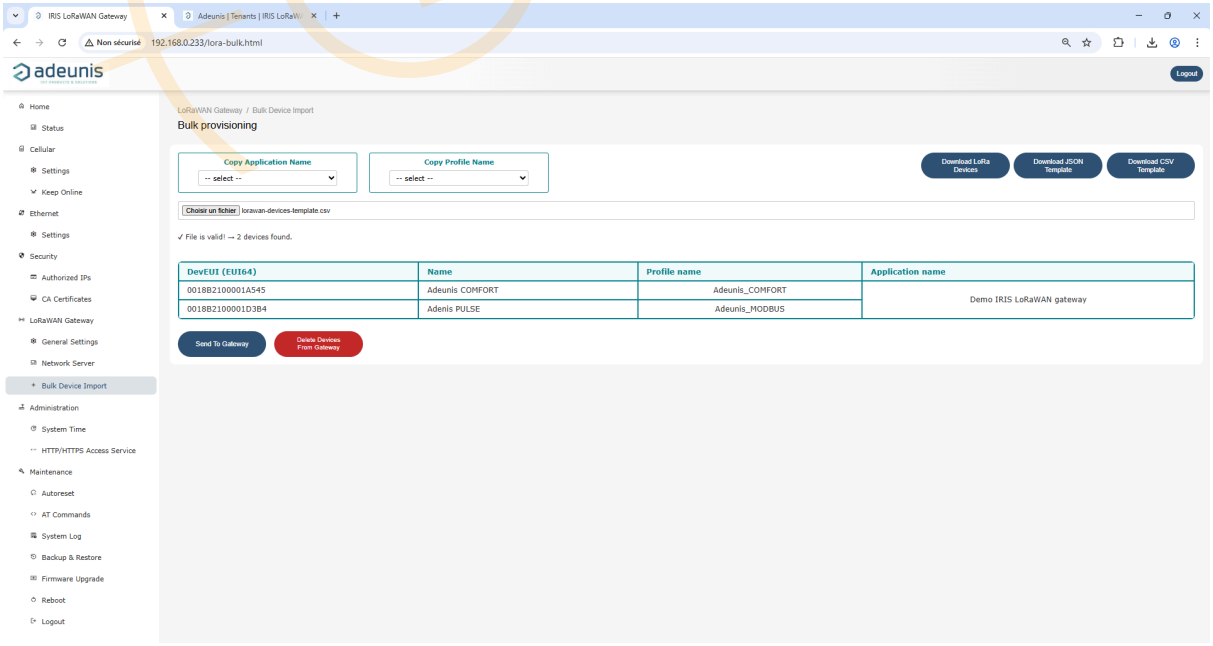
	A	B	C	D	E	F	G	H	I	J	K	L	M
1	name	description	devEui	appKey	nwkKey	joinEui	deviceProfile	applicationN	isDisabled	skipFCntCheck			
2	Example Ade	Sensor for m	0018B210000	384E786F39A54445BE9C279E0EF1E0E9			Adeunis_BRE	LoRaWAN De	false	false			
3	Example Ade	Sensor for m	0018B210000	D2DD78FF18DC47EFBF85EADCCB2C13C9			Adeunis_COI	LoRaWAN De	false	false			
4	Example Hur	Sensor for m	B2903AD184	D2DD78FF58DC47EFBFA5E		B31D15AC45	Brand_XYZ_H	LoRaWAN De	false	false			
5	Light Sensor	Sensor for m	C2903AD184	D2DD78FF58DC47EFBFA5E		C31D15AC45	Brand_XYZ_L	LoRaWAN De	false	false			
6	Motion Sens	Sensor for de	D2903AD184	D2DD78FF58	11223344556	D31D15AC45	Brand_XYZ_M	LoRaWAN De	false	false			
7	Motion Sens	Sensor for de	D2903AD184	D2DD78FF58	11223344556	D31D15AC45	Brand_XYZ_M	LoRaWAN De	false	false			
8	Pressure Ser	Sensor for m	E2903AD184	D2DD78FF58DC47EFBFA5E		E31D15AC45	Brand_XYZ_P	LoRaWAN De	false	false			
9													
10													
11													
12													
13													
14													

2. Fill one row/object per device and provide:

- **name**, **description**
- **devEUI**
- **joinEUI** for OTAA
- **app_key** (and **nwk_key** for 1.1) for OTAA; or ABP session keys when applicable
- **Device Profile Name**
- **Application Name**
- **Device disabled status**
- **Disable frame-counter status**

3. Upload the file

The Web GUI shows a preview of the devices listed in the JSON or CSV file.



Distributed by www.texim-europe.com

4. click **SEND TO GATEWAY**.

To remove a batch you previously uploaded, provide a file with the target **dev_eui** list and click **DELETE DEVICES FROM GATEWAY**.

An example is described in **ANNEX 4 BULK REGISTERING DEVICES**

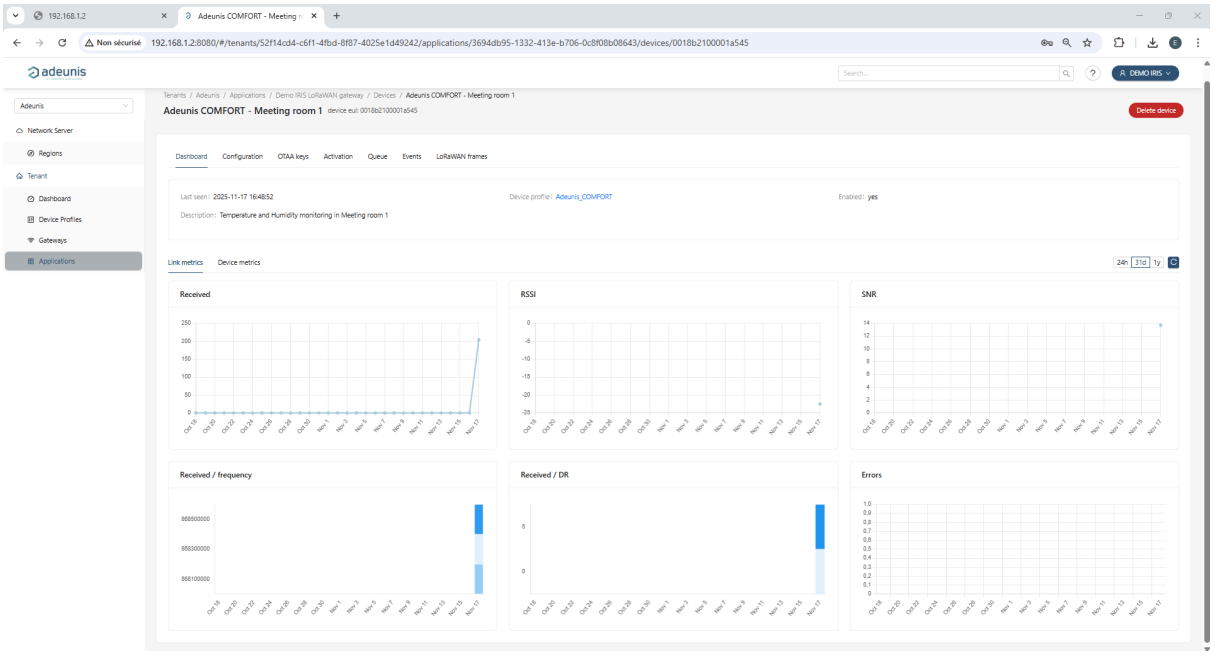
Parameter Quick Reference

Item	Purpose	Notes
JSON/CSV template	Canonical column/field names	Download from the page before preparing your file
Required identifiers	`dev_eui`, `device_profile`	`join_eui` for OTAA
Security keys	`app_key` (1.0.x), `app_key` + `nwk_key` (1.1)	32-hex each
Actions	**SEND TO GATEWAY**, **DELETE DEVICES FROM GATEWAY**	Import or remove

📌 Start with a small pilot file (2–3 devices) to validate the template, then import the full list.

5.6.8. Manage Device Details

This view centralizes the status, metrics and operations for a specific device. The header shows the **Device name**, **DevEUI**, a link to the **Device profile**, and a **Delete device** action.



Tab: Dashboard

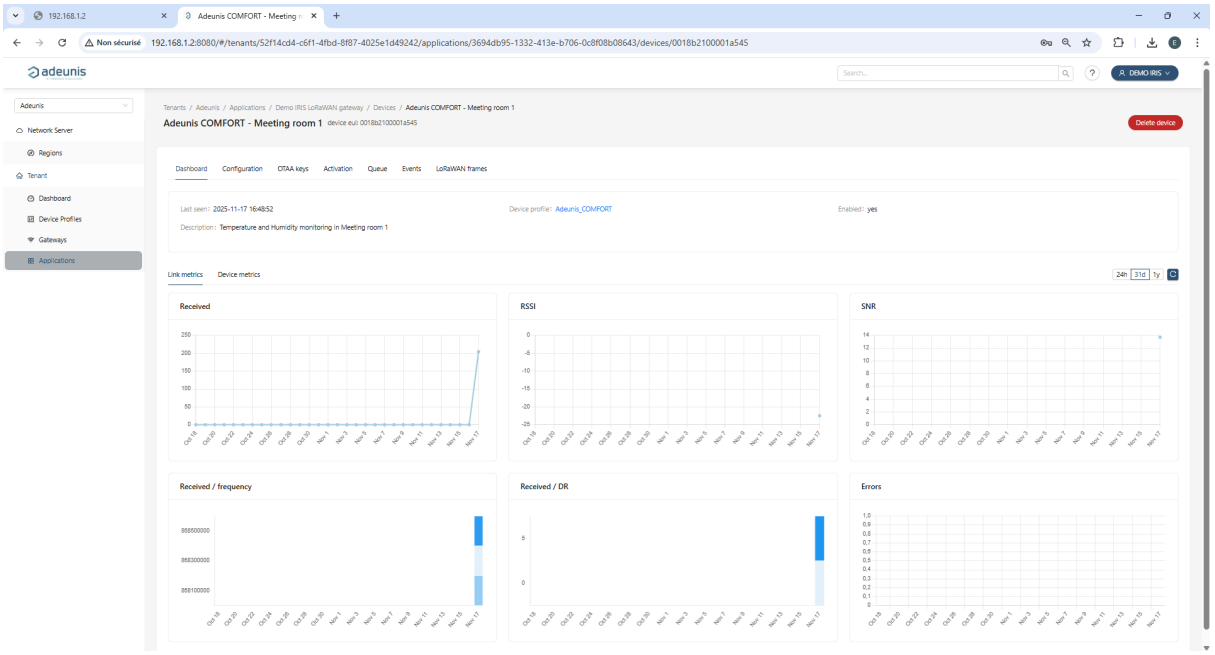
- **Top summary**

Displays **Last seen**, the **Device profile** (clickable), **Enabled** status, and **Description**.

- **Link metrics**

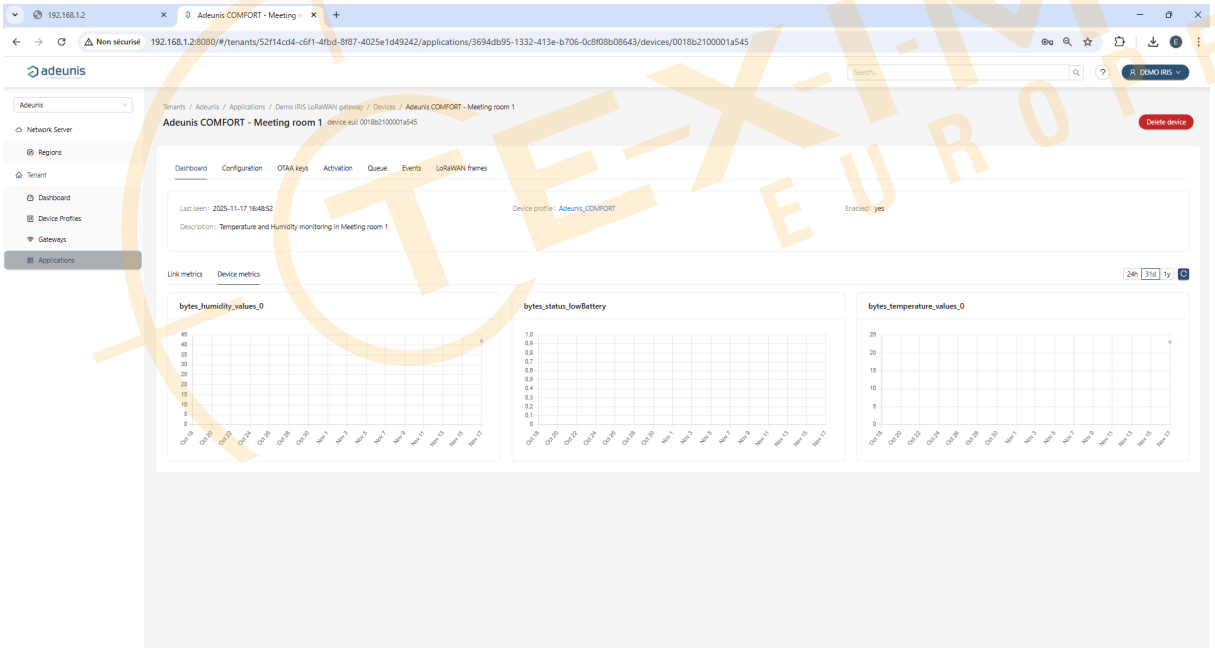
Charts for **Received** uplinks, **RSSI** (dBm), **SNR** (dB), **Received / Frequency**, **Received / DR**, and **Errors** (downlink error ratio). Use these to evaluate coverage/ADR behavior and transmission quality.

Distributed by www.texim-europe.com



- **Device metrics**

When a codec and **Measurements** are defined in the profile, decoded series (e.g., temperature, humidity, battery, pulses) appear here.

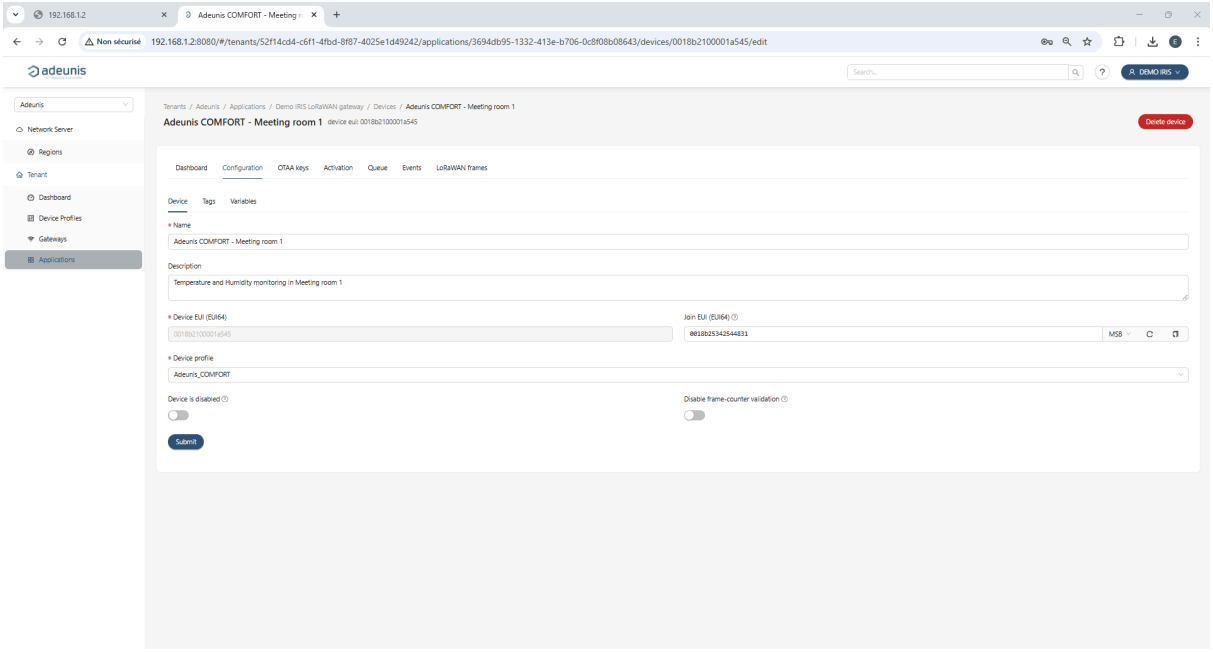


Tab: Configuration

Edit **Name**, **Description**, **Device profile** (changing it affects region/MAC version/classes),

Distributed by www.texim-europe.com

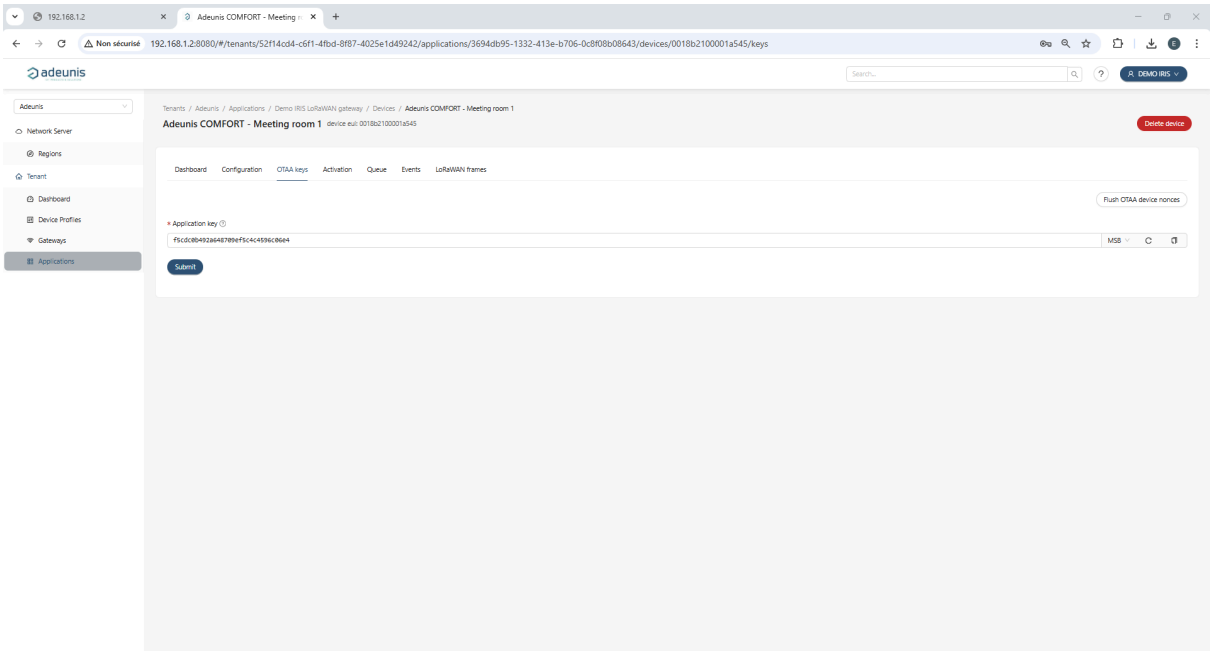
plus **Tags** and **Variables** for the device. (DevEUI and JoinEUI are shown in their respective areas and may be read-only depending on creation method.)



Tab: OTAA keys

For OTAA devices, view or edit **JoinEUI/AppEUI** and the **AppKey** (LoRaWAN 1.0.x) or **NwkKey + AppKey** (LoRaWAN 1.1.x).

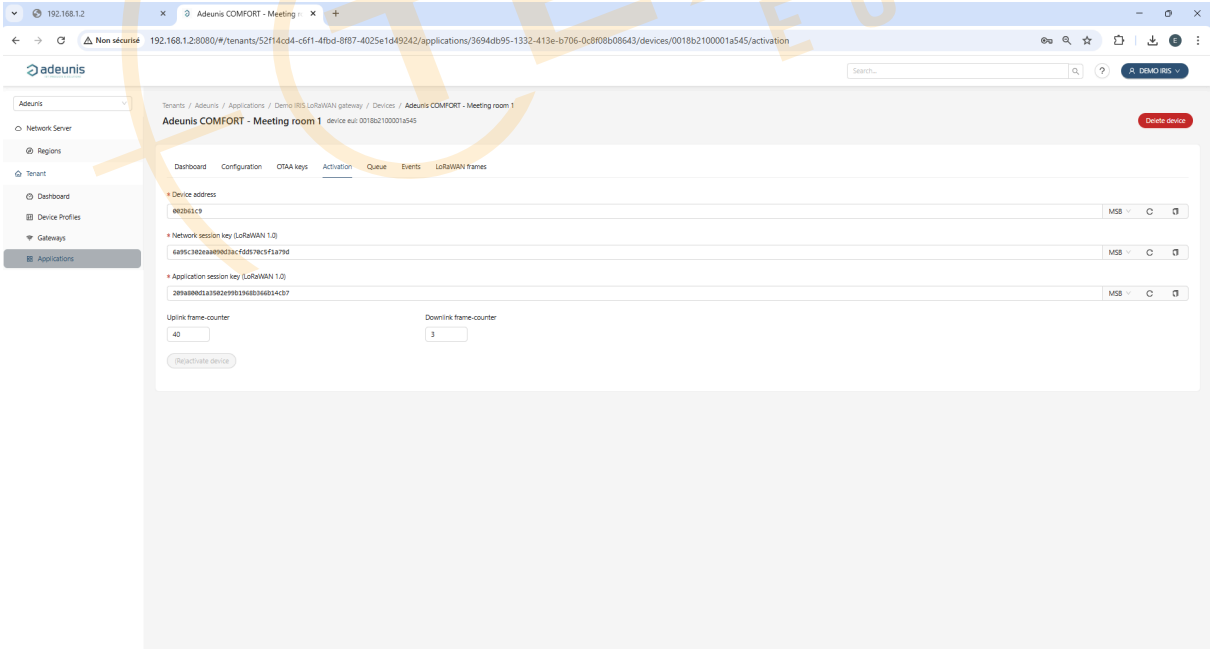
Use **Flush OTAA device nonces** to clear stored nonces if a device has been reset and reuses a DevNonce (common on some 1.0.x stacks), otherwise joins may be rejected as “used DevNonce.”



Tab: Activation

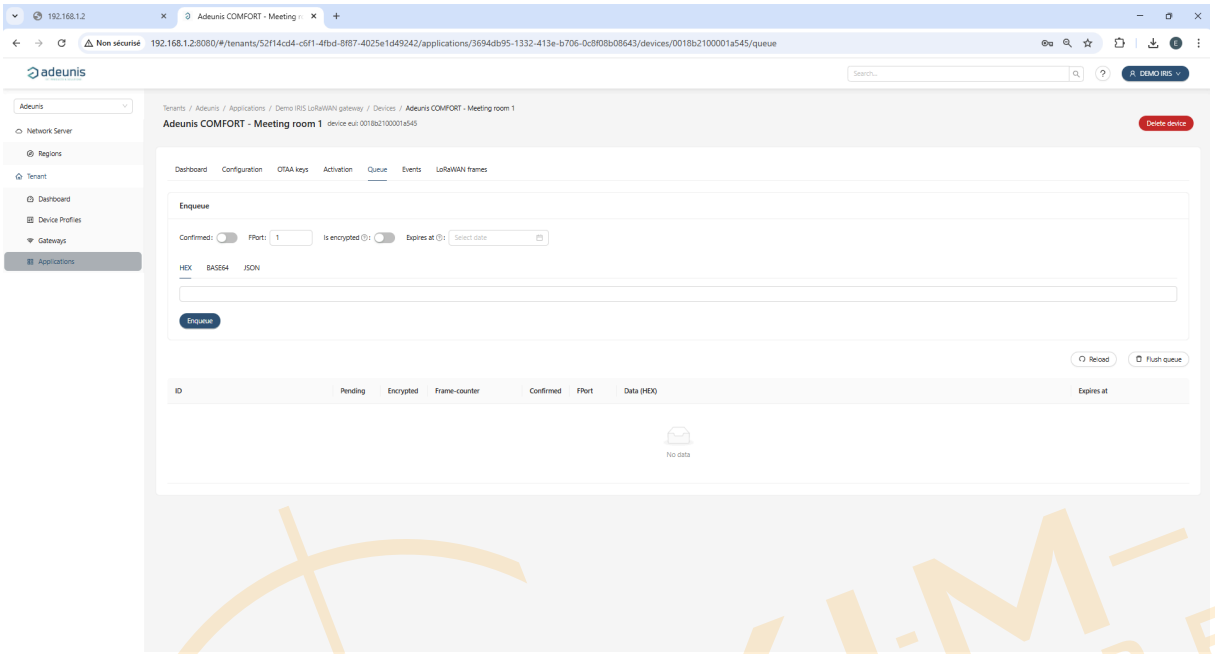
Shows the current session (**DevAddr**, **AppSKey**, **NwkSKey** or 1.1.x equivalents) and the **FCntUp/FCntDown** counters.

You can manually (re)activate ABP devices or clear the session to force a new OTAA join.



Tab: Queue

Use this editor to compose and schedule downlinks (single device). Messages are kept in a FIFO queue and sent during the next valid RX window according to the device class (A/C).

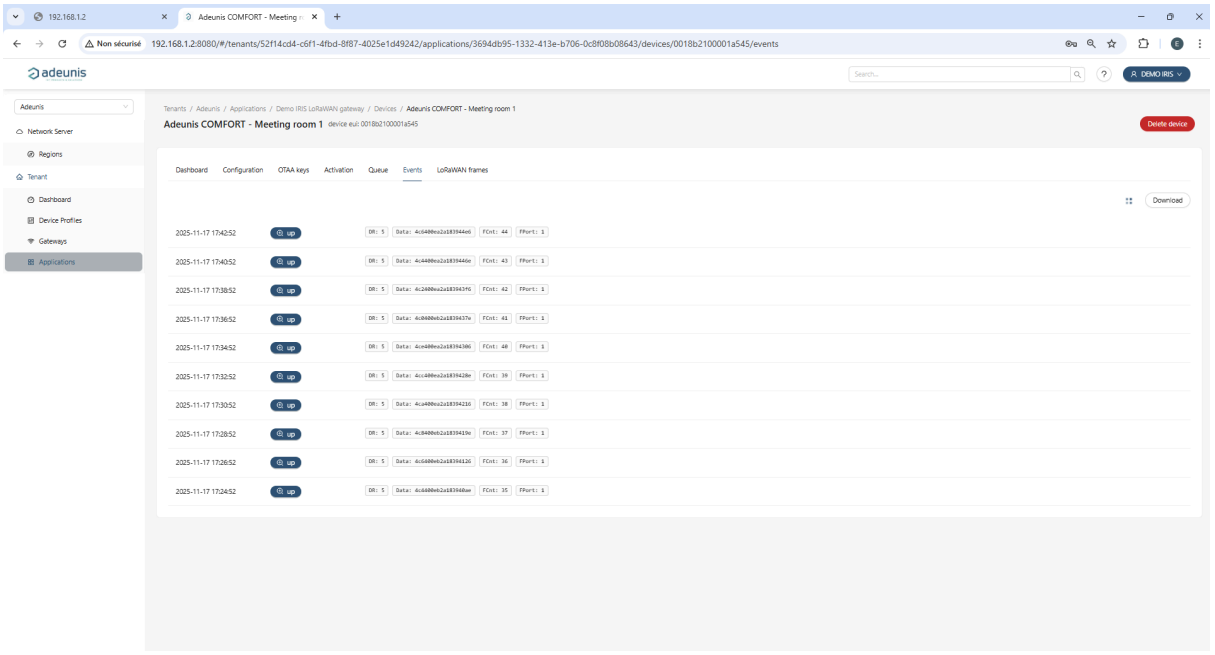


For the full step by step enqueue process, see Downlinks to a Single Device section.

Tab: Events

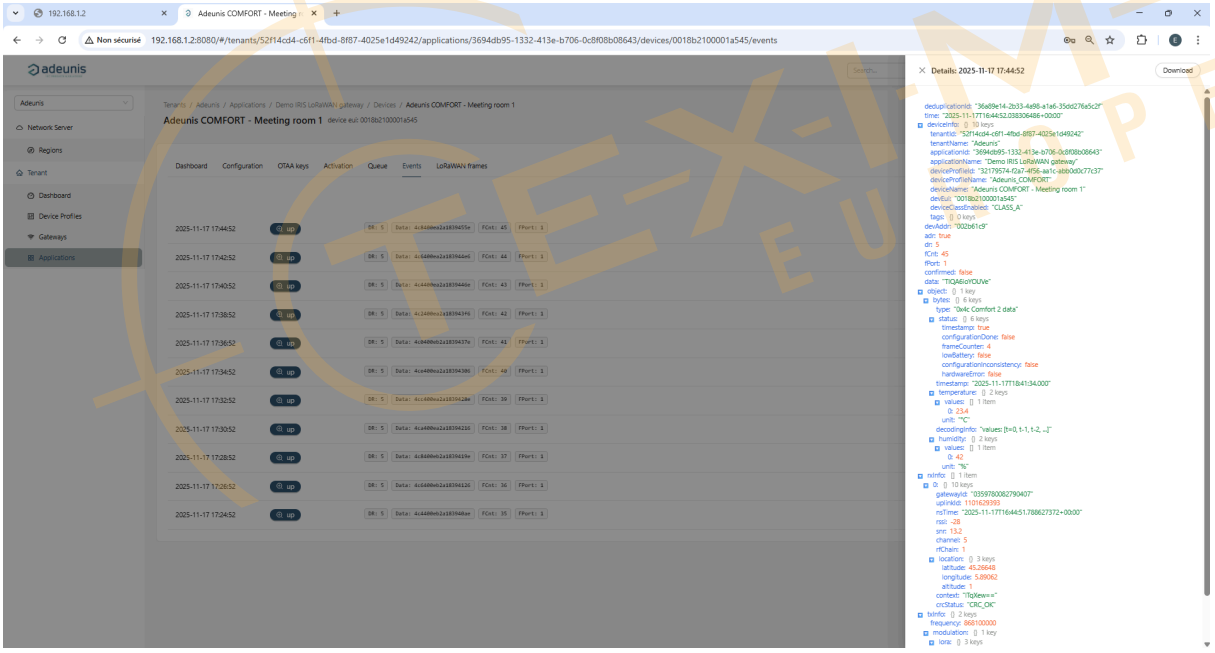
Operational logbook of uplinks, downlinks, joins, ACKs, and status messages.

Distributed by www.texim-europe.com



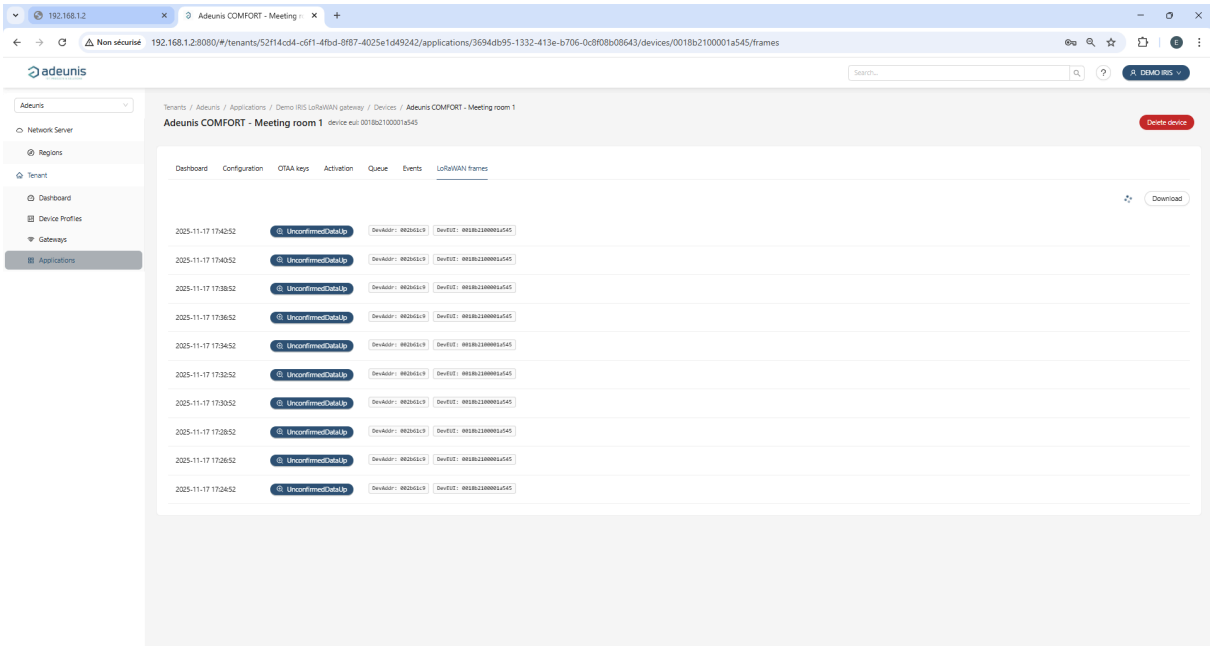
Use **View details** to inspect frequency, DR, RX window, RSSI/SNR, gateway, size, MIC.

The list can be **downloaded (JSON)** for analysis or support.



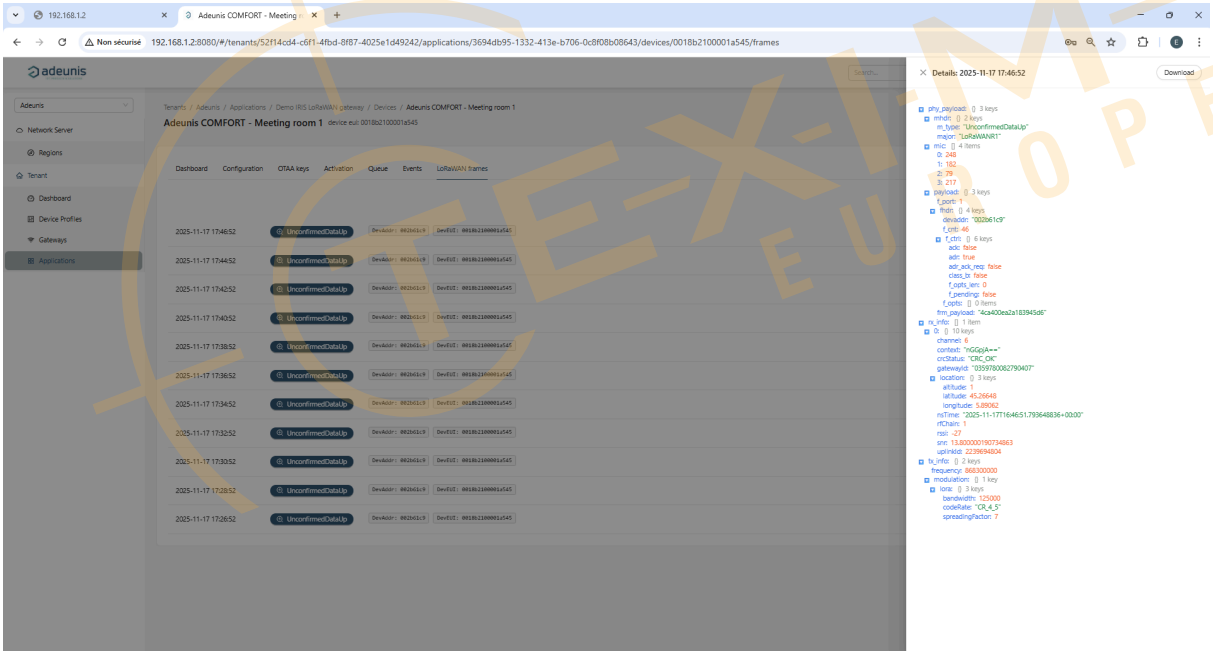
Tab: LoRaWAN frames

Raw MAC/PHY frames related to the device (frequency, DR, RSSI/SNR, FCnt, FPort, flags). Useful for deep debugging or verifying network behavior independently of codecs.



Use **View details** to inspect information.

The list can be **Downloaded** (JSON) for analysis or support.



5.6.9. Downlinks (Single Device & Multicast)

Send application commands/configuration from the embedded LoRaWAN Network Server either to a **single device** (most common) or to a **multicast group** (Class C).

Distributed by www.texim-europe.com

Prerequisites

- The device is already **provisioned** (OTAA joined or ABP activated) and shown **Online** in Applications → Devices → [Device].
- A **Device-profile** is associated and (optionally) a **payload codec** is configured if you plan to use JSON mode.
- For **Class A** devices, an **uplink is required** to open RX1/RX2; your downlink will be delivered after the next uplink.
- For **Class C**, the server can transmit as soon as the gateway duty-cycle allows it.

Single-Device Downlink

Use a downlink when you need to send a command or configuration to one specific end-device (for example: setpoint change, output toggle, reporting interval).

On IRIS, downlinks are scheduled from the embedded network server per device and are sent during the device's next valid receive window according to its LoRaWAN class.

Go to Applications → Devices → [Device] → Queue.

This page lets you compose the payload, choose the application port (FPort), and decide whether the message should be confirmed. Enqueued items are shown in a FIFO list and will be transmitted in the next available RX window (Class A after the next uplink; Class C as soon as duty-cycle permits)

1. **Compose the Downlink**

In Queue, fill the fields as follows

- **Confirmed**

  Turn **ON** to request an ACK from the device on its next uplink; leave **OFF** for best battery/network efficiency. If the ACK is not received, the server will retry automatically.

- **FPort**

  Use **1–223** for application payloads. **0** is reserved for MAC commands and must not be used for application data

- **Is encrypted?**

  Leave **OFF** in normal operation (the server encrypts with the session keys). Turn **ON** only if you supply an **already AppSKey-encrypted** FRMPayload to be sent as-is.

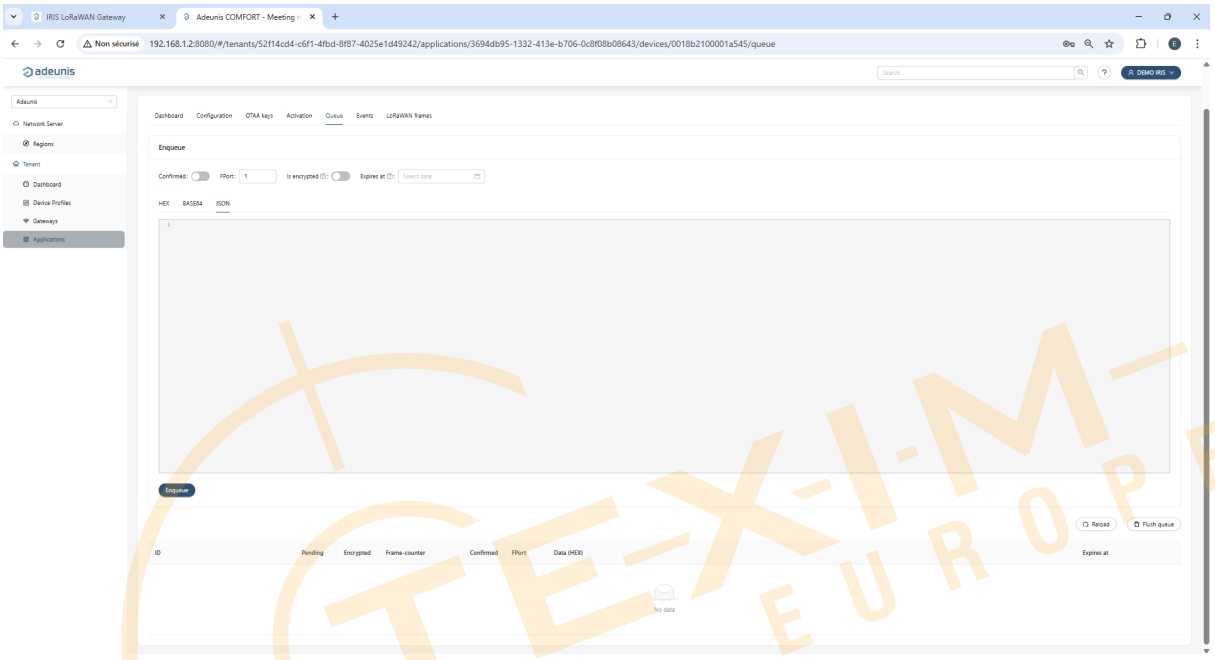
- **Expires at (optional)**

Set a time-to-live; if the device doesn't receive the message before this timestamp (e.g., no uplink from a Class A device), the server discards it to avoid stale actions.

- **Payload format**

Choose **HEX**, **BASE64** or **JSON**.

- **HEX/BASE64:** paste the raw bytes to send.
- JSON: provide a JSON object when a codec is configured in the device profile; the server calls `encodeDownlink(input)` to build the byte array before enqueueing



2. **Payload Entry**

- **HEX/BASE64**

For example, to change sampling period to 1 hour on an Adeunis PULSE sensor: `41150708`

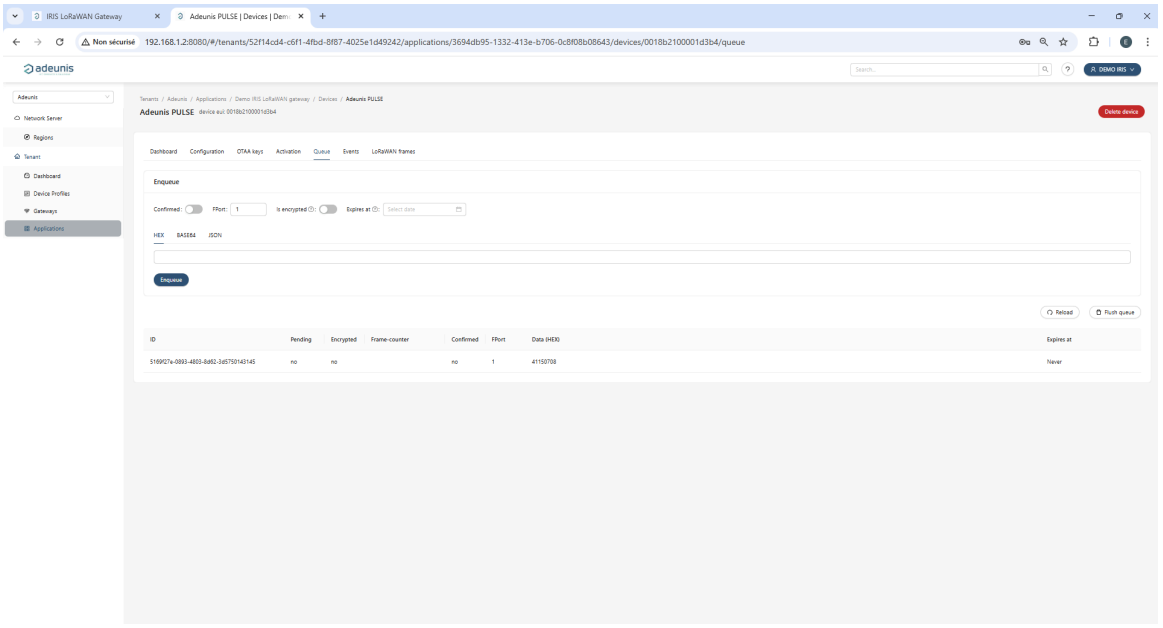
- **JSON**

For example, with a codec expecting a target temperature): { "target": 22.5 }

3. **Enqueue**

Click **Enqueue**. The item appears in the queue with **Pending**, **Encrypted**, **Frame-counter**, **Confirmed**, **FPort**, **Data (HEX)** and **Expires at** columns.

Distributed by www.texim-europe.com



Use **Reload** to refresh the list or **Flush queue** to clear pending items.

5. **Delivery & status**
   - **Class A:** the message is transmitted in RX1/RX2 **after the next uplink** from the device.
   - **Class C:** transmitted as soon as possible (subject to EU868 duty-cycle).

     Use **Reload** to refresh, or **Flush queue** to clear unsent items.

Multicast downlinks (optional, Class C)

Multicast lets you send the same command to many devices at once.

All devices in a multicast group share one **multicast DevAddr** and a pair of **multicast session keys**; frames addressed to that group are received by every member that is listening.

By LoRaWAN design, **multicast frames are not acknowledged (no ACK)**, so delivery must be validated through frames monitoring rather than confirmations.

1. **Create a Multicast Group**

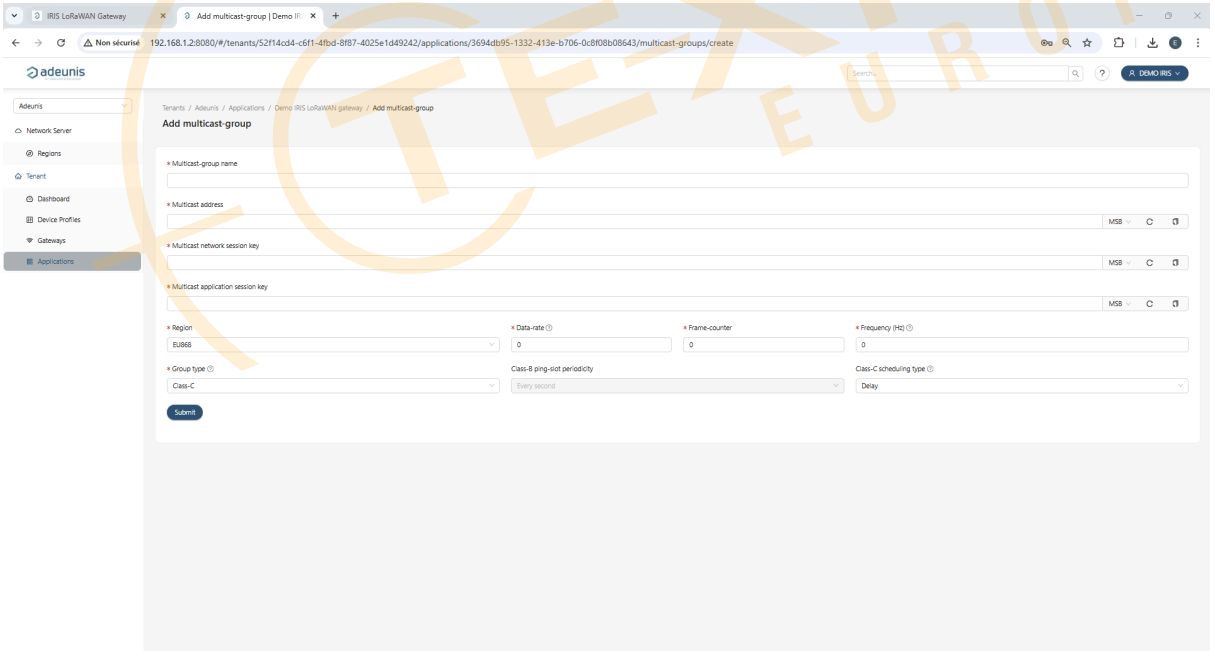
Go to Applications → Multicast groups → Add Multicast group.

Fill the fields as follows

- **Name:** A clear label for operations (e.g., `Lighting_Floor1`).
- **Multicast Address (DevAddr):** 4-byte / 8-hex group address shared by all members.

Distributed by www.texim-europe.com

- **mcNwkSKey / multicast network key** (LoRaWAN 1.0.x): 16-byte hex; **must match** the devices.
- **mcAppSKey / multicast application key:** 16-byte hex; **must match** the devices.
- **Region:** Use **EU868** on IRIS. Must be consistent with your devices and gateway.
- **Data-Rate (DR):** DR0...DR5 in EU868 (lower DR = longer range, higher DR = shorter range).
- **Frequency (Hz):** Downlink carrier for the group (e.g., `869525000`, `868100000`). Ensure it is legal for EU868 and consistent with DR.
- **Downlink Frame-counter:** Group FCntDown; auto-increments per transmission (you can reset it if you re-provision).
- **Group type:** Select **Class-C**. (Class-B is not used on IRIS in this guide.)
- **Class-C Scheduling Type (Class-C only):** Defines when the multicast downlink is transmitted
  - Delay: transmit after a relative delay (in seconds) from the moment you enqueue the message.
  - GPS/Absolute time: transmit at a specific absolute time (GPS/UTC). Use this to trigger a large fleet at the same instant. Ensure the gateway time is correct (NTP) before using absolute scheduling.



2. **Add Devices**

Open the multicast group you created and **Add devices**. Only devices provisioned with the same multicast DevAddr and multicast keys will receive the frames; mismatched keys prevent reception.

Distributed by www.texim-europe.com

Verify the **Devices** tab in the application shows your targets Online.

📌 IRIS supports for creating **Class-C** multicast groups.

3. **Enqueue a Multicast Downlink**

Go to Applications → Multicast groups → [your group].

Compose the downlink using the same editor as for single-device queues

- **Confirmed**

Leave **OFF** (multicast frames do not generate ACKs).

- **FPort**

`1…223` for application data; `0` is reserved for MAC (do **not** use for app data).

- **Is encrypted?**

Leave **OFF** unless you provide an already AppSKey-encrypted FRMPayload.

- **Expires at**

Optional TTL; the item is dropped if it cannot be sent before this time.

- **Payload**

Choose **HEX**, **BASE64**, or **JSON** (when a device-profile codec is configured; the server calls `encodeDownlink()` to build bytes).

4. Click **Enqueue** to schedule.
   The item appears in the queue with **Pending**, **Encrypted**, **Frame-counter**, **FPort**, **Data (HEX)** and **Expires at** columns.

📌 Multicast on the embedded LNS is supported for **Class-C** operation. Class-A devices do not participate in coordinated multicast because they only listen in RX1/RX2 after their own uplinks.

Parameter Quick Reference

Field	Where	Accepted values / Notes
Confirmed	Multicast group → Queue	**OFF** for multicast (no ACK).

Field	Where	Accepted values / Notes
FPort	Multicast group → Queue	`1…223` application ports; `0` is MAC (reserve).
Is encrypted?	Multicast group → Queue	**OFF** recommended. **ON** only for pre-encrypted payloads.
Expires at	Multicast group → Queue	Optional TTL for scheduled item.
Payload format	Multicast group → Queue	**HEX / BASE64** raw bytes, or **JSON** (codec `encodeDownlink`).
Region	Multicast group	**EU868** on IRIS (match devices / gateways).
Data-Rate (DR)	Multicast group	EU868 **DR0…DR5** (coverage vs speed).
Frequency (Hz)	Multicast group	e.g., `869525000`, `868100000` (legal & DR-consistent).
Class-C scheduling type	Multicast group	**Delay** (relative seconds) / **GPS/Absolute time** (UTC). Ensure NTP.
Frame-counter	Multicast group	FCntDown (auto-increments; reset only when re-provisioning).

Validation

- **Events tab (device)**

  Look for `downlink scheduled`, `downlink acknowledged`, or error messages (`frame-counter`, `no channel available`, `mic error`).

- **LoRaWAN frames tab**

  Inspect PHYPayload, `fCnt` evolution, `fPort`, and RX window used.

- **Common causes of failure**
  - No recent **uplink** (Class A never opens RX).
  - **Duty-cycle** saturation on EU868 sub-bands (expect delays under heavy traffic).
  - Wrong **FPort** (0 used for MAC).
  - Codec/JSON mismatch (codec can't build bytes).
  - Frame-counter mismatch after re-provisioning (only temporarily use *Disable frame-counter validation* when resetting ABP devices).

Distributed by www.texim-europe.com

Best practices

- Keep payloads small.
- Plan campaigns during low traffic to limit duty-cycle contention.
- Set **Expires at** to avoid stale commands.
- Document each multicast action (who/when/what) in your ops log for traceability.

5.6.10. Validation

Your embedded LoRaWAN server is ready when:

1. **Gateway is online** in the dashboard with correct **EU868** band and coordinates.
2. **Device-profile** exists, codec attached, and at least one **application** is created.
3. **Device(s) joined** (OTAA) and **uplinks** appear with **decoded JSON** values (not just raw bytes).
4. **Downlink** test succeeds (Class A: delivered after next uplink; Class C: immediate).
5. If used, **MQTT(S)/HTTP(S)** integration receives the expected payloads with the proper TLS setup (Root CA installed on IRIS).
6. **ADR** settles within your configured DR bounds, and RX2 parameters match the device datasheet.
7. You exported a **configuration backup** (IRIS → Backup/Factory) and noted the **dashboard credentials** and **NetID** in the site dossier.

Route data to your application

LoRaWAN is configured and the gateway is online at the Network Server. Next, wire decoded device payloads to your application stack over **MQTT/s** or **HTTP/s**, then run the site acceptance to prove end-to-end delivery.

6. Application Integration & Data Routing (MQTT/s & HTTP/s)

This chapter connects the **decoded** LoRaWAN payloads to your application backends.

IRIS can **re-send** uplinks from the embedded LoRaWAN Network Server to an external system over:

- **MQTT / MQTTS**
- **HTTP / HTTPS**

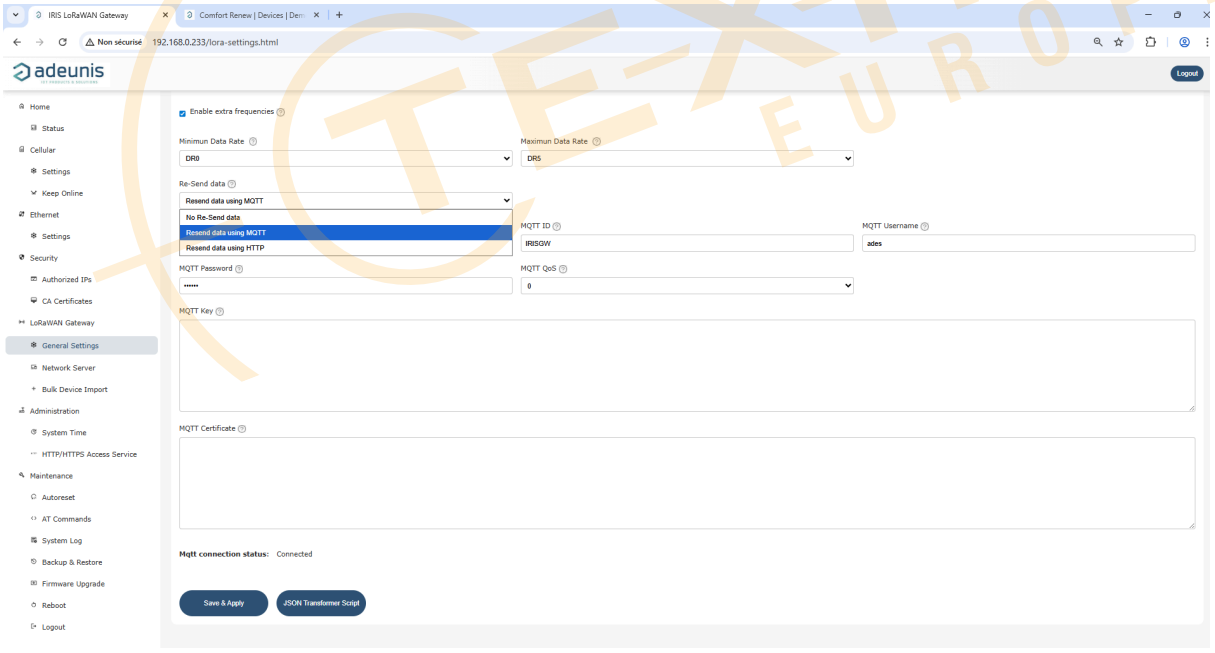
When you use an **external LNS** (UDP Packet Forwarder or Basics Station), integrations are usually configured directly on that LNS; this chapter is then for reference only.

When you use the **embedded LNS**, the gateway itself pushes decoded payloads to your application. In this case:

- Select the integration path in

  LoRaWAN Gateway → General Settings → Re-send data using

  (*Resend data using MQTT* or *Resend data using HTTP*).
- Optionally enable a **JSON Transformer** script to adapt or filter the JSON before it is forwarded.



The guidance below focuses on **what you need ready**, **how to secure transport**, and **how to validate** delivery to the customer's systems.

Distributed by www.texim-europe.com

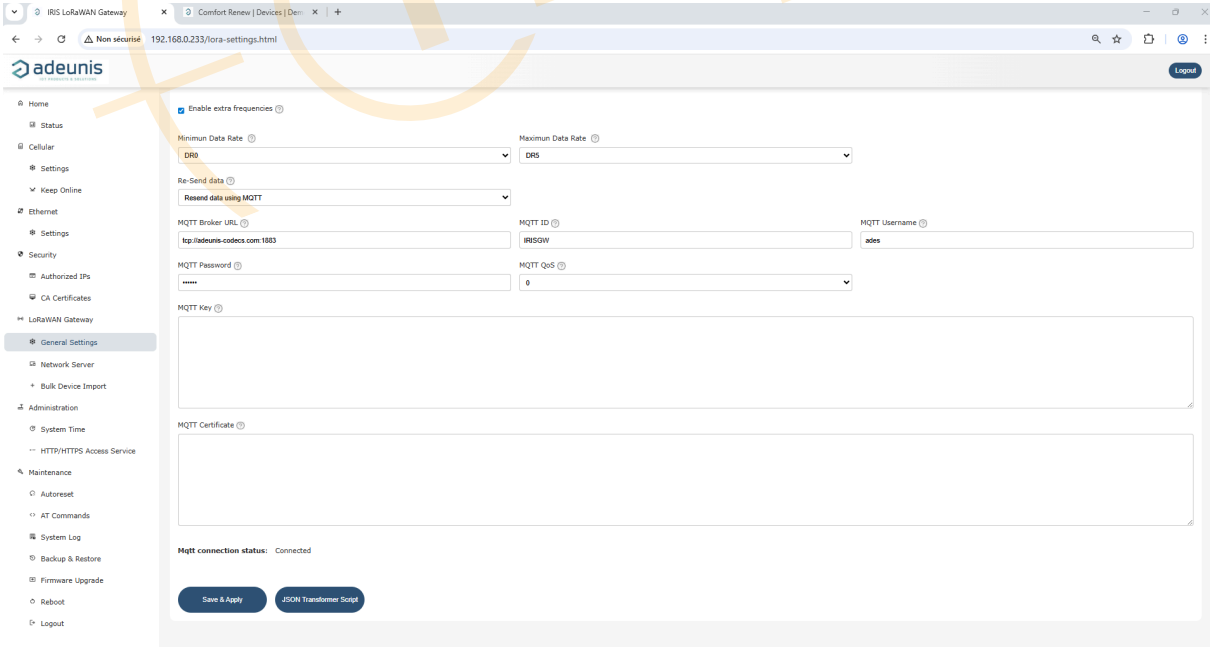
6.1. MQTT/MQTTs Integration

IRIS can publish decoded LoRaWAN uplinks to an external MQTT broker (unencrypted **1883** for lab use, or **8883** with TLS for production).

When the embedded LNS is enabled and **Re-send data using MQTT** is selected in **LoRaWAN Gateway → General Settings**, every decoded uplink is forwarded to the configured broker. If the JSON Transformer is enabled, the MQTT payload is the **transformed JSON** (or the frame is dropped if the script returns `"NULL"`).

What you will need

- **Broker host** (FQDN) and **port** (1883 for MQTT, 8883 for MQTTS).
- **Credentials** (username/password or client certificate, depending on broker policy).
- **QoS** policy (typically **QoS 0** or **QoS 1** for reliable delivery).
- **Trust model**:
  - **Unsecured MQTT (1883)** for lab/isolated networks only.
  - **MQTTS 8883 with self-signed**: upload the **broker's self-signed server certificate** into a CA-Root slot.
  - **MQTTS 8883 with CA-signed**: upload the issuing **Root/Intermediate CA(s)**.



Distributed by www.texim-europe.com

Topic Schema

By default, IRIS publishes each device's uplinks to:

application/<applicationID>/device/<deviceEUI>/event/up

`<applicationID>` is the ID of the LoRa application, and `<deviceEUI>` is the device's EUI.

Example

```
application/98f6ce6d-21f5-442e-8891-842df280bb87/device/0018b2100000bc45/event/up
```

If the JSON Transformer is enabled, you may override the MQTT topic in the script. In that case, the broker will receive the message on the topic returned by the script.

Payload format

Payloads are JSON and include timestamps, identifiers, frame counters, RF metrics, and the decoded fields produced by your codec. Your downstream application should parse these fields directly, or the transformed JSON if you use the JSON Transformer.

Distributed by www.texim-europe.com

Parameter Quick Reference

Parameter	What it controls	Typical value / guidance
URL / Port	Broker address	`mqtt.example.com` / **8883** for TLS
Client ID	MQTT client ID used for the connection	`iris-<site>-gw-<eui>`

Distributed by www.texim-europe.com

Parameter	What it controls	Typical value / guidance
Auth	Username/password or client cert	Per broker policy
QoS	Delivery semantics	0 or 1 (agree with app)
Certificate/Key	Trust model	See §4.3.3 (self-signed vs CA-signed)
Re-send data using	Integration path from embedded LNS	`Resend data using MQTT`
Topic	Routing path	application/<applicationID>/device/<deviceEUI>/event/up
Payload	JSON fields	Timestamp, IDs, counters, RF metrics, decoded

---

Validation and Handover

An MQTT/s integration is considered good when:

1. **Time & DNS** are correct.
2. **TLS session establishes cleanly** to the broker on **8883**: certificate chain validates against the CA(s) you uploaded, and the **hostname matches CN/SAN** (no browser/CLI warnings server side).
3. The broker shows a **successful client connect** from the expected **Client ID** with the intended **authentication method** (user/pass or client cert).
4. A **test uplink** published by the gateway appears on the **exact target topic**
5. The **payload structure** matches the expected JSON (timestamp, IDs, counters, RF metrics, decoded fields), and your application parses it without errors.
6. A **downlink workflow** (if applicable) can be triggered by the application and reaches the LNS/device through the normal path.
7. A **gateway reboot** results in an **automatic reconnect** within the expected window, with the same Client ID and subscriptions in place.
8. **Security posture** is sound: TLS in use; trust store contains only the needed CA(s) (or the single self-signed server cert); any Mobile-WAN inbound exposure is restricted with **Authorized IPs**.

6.2. HTTP/HTTPs Integration

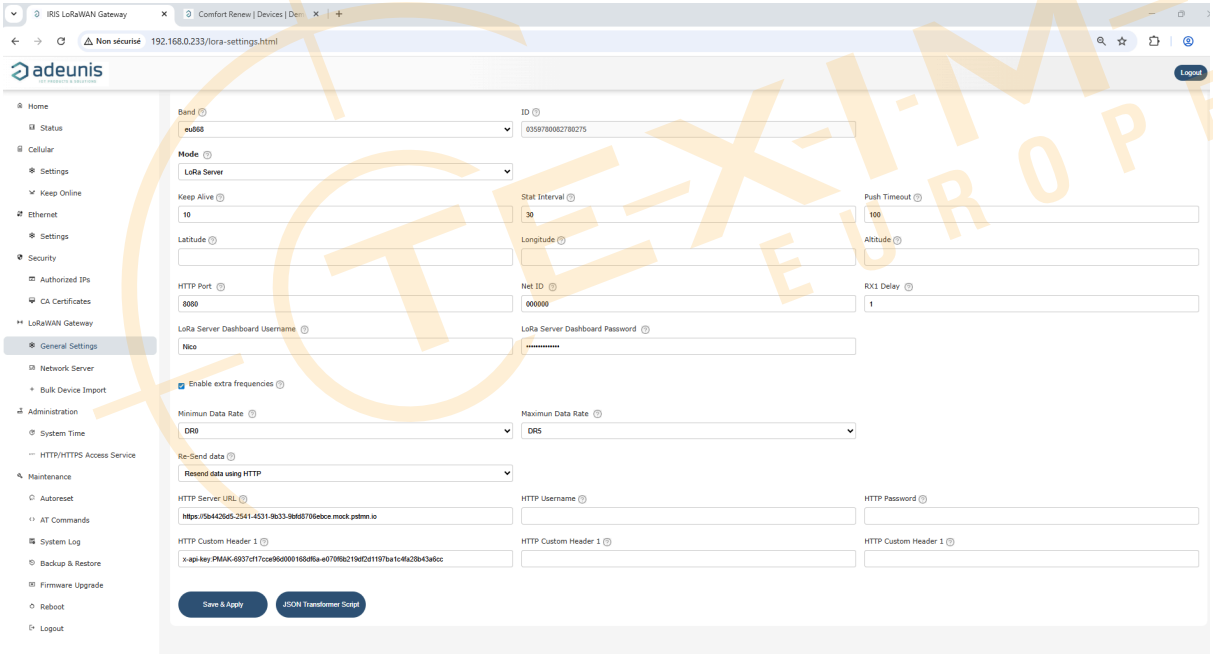
IRIS can also push decoded uplinks to an HTTP/HTTPS endpoint. This is typically used to integrate with application servers that do not expose MQTT.

Distributed by www.texim-europe.com

When the embedded LNS is enabled and **Re-send data using HTTP** is selected in **LoRaWAN Gateway → General Settings**, the gateway issues an HTTP POST per uplink to the configured endpoint. If the JSON Transformer is enabled, the body of the request is the **transformed JSON** (or the request is skipped if the script returns `"NULL"`).

What you will need

- **Endpoint URL** (HTTP for lab, **HTTPS for production**).
- **Method** (POST).
- **HTTP headers** (e.g., `Authorization: Bearer <token>`, `Content-Type: application/json`).
- **TLS trust** if the endpoint is HTTPS.
- **Auth/ACL** on the application side (token, IP allow-list, or both).



Recommended settings

- POST JSON body with the same fields you use for MQTT (timestamp, IDs, counters, RF metrics, decoded values), or the JSON returned by the Transformer.

Distributed by www.texim-europe.com

Parameter Quick Reference

Parameter	What it controls	Typical value / guidance
URL / Method	Where and how to deliver	`https://app.example.com/iot/ingest` / POST
Headers	Auth & content type	`Authorization: Bearer …`, `Content-Type: application/json`
TLS / CA	Trust model	CA roots per §4.3.2
Payload	Body format	JSON with IDs, counters, RF metrics, decoded (or transformed JSON)

Validation and Handover

An HTTP/s integration is considered good when:

1. **Time & DNS** are correct.
2. **TLS session establishes cleanly** to the endpoint on **443**: certificate chain validates against the CA(s) you uploaded, and the **hostname matches CN/SAN**.
3. The endpoint **authenticates the request** as designed (e.g., `Authorization: Bearer …`, mTLS, or IP allow-list) and rejects malformed/unauthorized calls.
4. A **test POST** from the gateway returns a **2xx** within an acceptable latency budget (define your target, e.g., < 2 s on LAN / < 5 s over cellular)
5. The payload structure (after JSON transformation if enabled) matches the contract and the application processes it without mapping errors.
6. **Error handling** is correct: a simulated **5xx** or upstream drop triggers the **configured retry/backoff** from the gateway side; **4xx** client errors are not retried.
7. **Security posture is sound**: HTTPS in use for production; the trust store contains only the required CA(s) or self-signed server cert; Mobile-WAN inbound exposure remains restricted with **Authorized IPs**, while outbound egress to the app endpoint is allowed by the firewall.
8. A **gateway reboot** does not require manual action; subsequent POSTs succeed once backhaul is up.

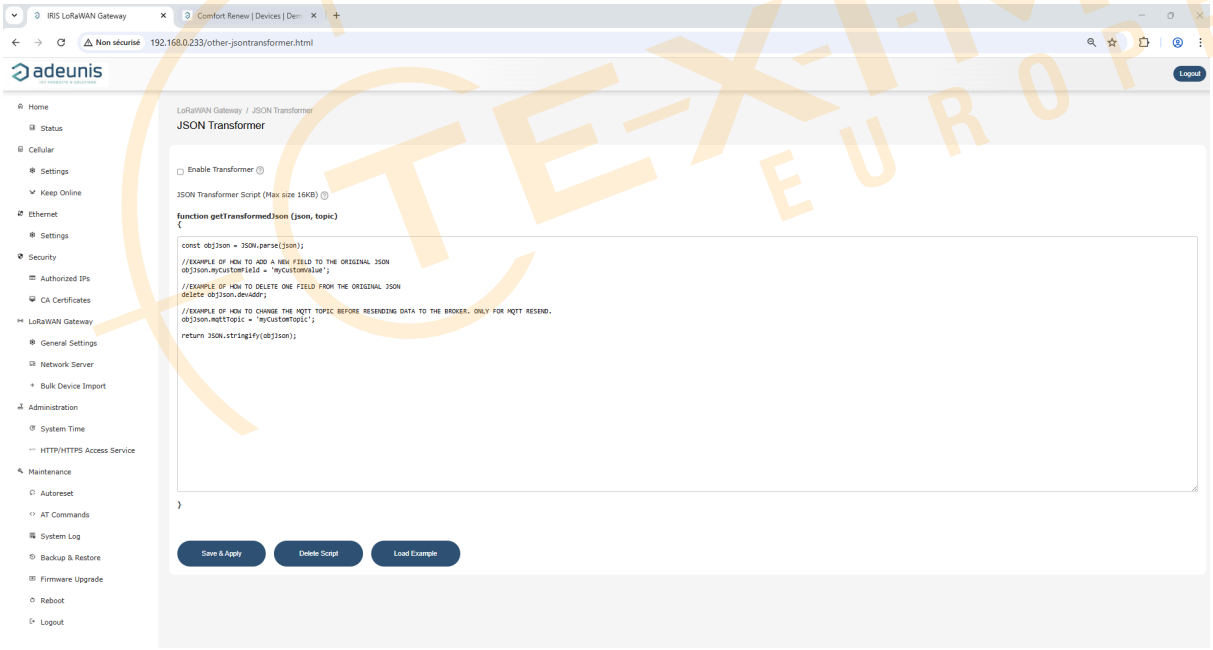
6.3. JSON Transformer

The **JSON Transformer** lets you adapt the payload format and routing **without changing the LNS or the application**:

- remove fields you do not need,
- rename or regroup values,
- add custom fields or tags,
- optionally change the MQTT topic,
- selectively drop frames.

The transformer is applied **after decoding** by the embedded LNS and **before** sending the payload over MQTT or HTTP.

📌 The script is optional; if disabled, the original JSON produced by the embedded LNS is forwarded unchanged.



Use the **Load Example** button in the Web GUI as a starting point and adapt the script to your own JSON structure. Carefully test any change using your MQTT/HTTP integration and logs before deploying to production.

Function signature

You must provide a function with the following signature:

```
function getTransformedJson(json, topic) {
    // json  : stringified JSON payload from the embedded LNS
    // topic : default MQTT topic (application/<appId>/device/<dev
Eui>/event/up)
}
```

The function **must return a string**:

- a JSON string → this payload is forwarded to MQTT/HTTP;
- the literal string `"NULL"` → the frame is **not forwarded**.

Typical use cases

- **Payload reduction**: remove all fields except a small subset needed by the application.
- **Field mapping**: rename or restructure fields to match an existing REST or database schema.
- **Enrichment**: add tags such as site IDs, device groups, or static metadata.
- **Selective forwarding**: only forward frames from a subset of devices, ports, or applications (drop everything else by returning `"NULL"`).
- **Topic customisation (MQTT)**: route different device families to different MQTT topics.

Example of Original JSON


```
{ "deduplicationId": "441351a6-6153-494d-8b8c-460b5770c618", "tim
e": "2025-12-02T08:29:38.637701176+00:00", "deviceInfo": { "tenant
Id": "52f14cd4-c6f1-4fbd-8f87-4025e1d49242", "tenantName": "Adeuni
s", "applicationId": "98f6ce6d-21f5-442e-8891-842df280bb87", "appl
icationName": "LoRaWAN Devices", "deviceProfileId": "bbe319d7-43de
-4010-a6cb-26a2690be53a", "deviceProfileName": "Adeunis_BREATH",
"deviceName": "Breath_Jose", "devEui": "0018b2100000bc45", "device
ClassEnabled": "CLASS_C", "tags": {} }, "adr": true, "dr": 5, "fCn
t": 53, "fPort": 1, "confirmed": false, "data": "bSAAOgAGAAYABQ=
```

```
=", "object": { "bytes": { "type": "0x6d Breath periodic data", "t
voc": { "unit": "µg/m3", "values": [ 58 ] }, "pm10": { "unit": "µ
g/m3", "values": [ 6 ] }, "decodingInfo": "values: [t=0, t-1, t-2,
...]", "pm25": { "unit": "µg/m3", "values": [ 6 ] }, "pm1": { "uni
t": "µg/m3", "values": [ 5 ] }, "status": { "configurationInconsis
tency": false, "configurationDone": false, "frameCounter": 1, "sen
sorError": false, "hardwareError": false, "lowBattery": false } }
}, "rxInfo": [ { "gatewayId": "0359780082780580", "uplinkId": 2412
397231, "nsTime": "2025-12-02T08:29:38.137058989+00:00", "rssi": -
27, "snr": 13.5, "channel": 5, "rfChain": 1, "location": {}, "cont
ext": "AteFLQ==", "crcStatus": "CRC_OK" } ], "txInfo": { "frequenc
y": 868100000, "modulation": { "lora": { "bandwidth": 125000, "spr
eadingFactor": 7, "codeRate": "CR_4_5" } } }, "regionConfigId": "e
u868" }
```

Example 1 – Keep only a subset of fields from this JSON

The script below builds a compact JSON containing a few measurements and status flags plus the original timestamp:

```
function getTransformedJson (json, topic) {
    const obj   = JSON.parse(json);
    const bytes = obj.object?.bytes;

    const out = {
        devEui      : obj.deviceInfo?.devEui || null,
        tvoc        : bytes?.tvoc?.values?.[0] ?? null,
        pm10        : bytes?.pm10?.values?.[0] ?? null,
        pm25        : bytes?.pm25?.values?.[0] ?? null,
        pm1         : bytes?.pm1 ?.values?.[0] ?? null,
        sensorError : bytes?.status?.sensorError  ?? null,
        hardwareError: bytes?.status?.hardwareError ?? null,
        lowBattery  : bytes?.status?.lowBattery   ?? null,
        time        : obj.time || null
    };

    return JSON.stringify(out);
}
```

This significantly reduces payload size while keeping all application-relevant information.

Example 2 – Forward only one device

The next script forwards data **only** for device `0018b2100000bc45`. Frames from any other device are dropped by returning `"NULL"`:

```
function getTransformedJson (json, topic) {
    const obj = JSON.parse(json);

    const dev = obj.deviceInfo?.devEui || null;
    if (dev !== "0018b2100000bc45") {
        // do not forward this frame
        return "NULL";
    }

    const bytes = obj.object?.bytes;

    const out = {
        devEui       : dev,
        tvoc         : bytes?.tvoc?.values?.[0] ?? null,
        pm10         : bytes?.pm10?.values?.[0] ?? null,
        pm25         : bytes?.pm25?.values?.[0] ?? null,
        pm1          : bytes?.pm1 ?.values?.[0] ?? null,
        sensorError  : bytes?.status?.sensorError  ?? null,
        hardwareError: bytes?.status?.hardwareError ?? null,
        lowBattery   : bytes?.status?.lowBattery   ?? null,
        time         : obj.time || null
    };

    return JSON.stringify(out);
}
```

Prove the full path

Routing is configured and secured. Continue with **End-to-End Validation & Site Acceptance** to demonstrate device join, uplink decoding, and delivery **into your application** (and a basic downlink, if applicable).

Distributed by www.texim-europe.com

7. END TO END VALIDATION & SITE ACCEPTANCE

Commissioning is complete when you can demonstrate a clean path from a device to the application.

7.1. Status & Identity

Start on **Home** → **Status** and confirm the device has the correct local time, a healthy backhaul (Ethernet or Cellular) with a valid IP, and that the **LoRaWAN** card shows the chosen mode, regional band, and **Gateway EUI**.

Verify that this **Gateway EUI** is the one registered on your LNS (or visible in the embedded server).

7.2. Gateway ↔ LNS session (mode-specific)

UDP Packet Forwarder

The gateway appears **online** on the LNS with the right frequency plan.

Ensure firewalls/Authorized IPs allow **uplink UDP out** and **downlink UDP in** from the LNS IPs you documented.

Optionally reboot the gateway and verify automatic re-registration.

Basics Station (WSS)

The station shows **connected** on the LNS (router/session UP).

Confirm the **WSS URL** hostname matches the server certificate, your **CA Root** is installed, and there are no TLS errors.

Optionally reboot and confirm session restores.

Embedded LoRaWAN Server

The embedded console shows the gateway **Up**; **Application** and **Device Profile** match the region.

7.3. Device join

Trigger a **join** from your OTAA device.

On the LNS (or embedded console) observe a **Join-request** followed by **Join-accept**; the device shows **joined/activated**.

7.4. Uplink path (RF to application)

Send a **test uplink** from the device.

On the LNS, verify the frame reception with plausible RF metrics (RSSI/SNR consistent with proximity) and confirm your **application decoder** (if any) processes the payload without error and reaches the intended integration (MQTT/HTTP) your program expects.

7.5. Downlink path (network to device)

Schedule a **downlink** to the device (unconfirmed is fine; use **confirmed** if you want an ACK).

- **UDP PF sites:** this specifically validates the **inbound** UDP path and your **Authorized IPs** policy; if you remove the LNS downlink IP from the allow-list, the downlink should fail, add it back and retest.
- **Basics Station (WSS):** verify the station transmits the downlink and the device receives it.

Distributed by www.texim-europe.com

With a validated baseline in hand, you can focus on running the gateway day-to-day. The next chapter shows how to keep configuration safe, logs available, software up to date, and connectivity resilient.

8. OPERATIONS AND MAINTENANCE

Production operation is about avoiding surprises and recovering quickly when they occur. Your objective is a gateway that runs quietly, leaves a clear audit trail, and can be restored in minutes if something changes upstream.

Start by putting a **safety net** in place. Create and archive a configuration **backup** at the end of commissioning and **before every change**. A current snapshot is the fastest way to recover from a misstep or to swap hardware without drama.

Next, ensure **visibility**. Use **Syslog** to capture recent events for diagnosis and, where your environment allows it, export logs to your central collector so you keep history across sites. Accurate time (NTP) underpins trustworthy logs—validate it whenever you review or export records.

Only then perform **planned changes** such as **firmware upgrades**. Treat each upgrade like a mini-release: pick a maintenance window, confirm you have a fresh backup, apply the image, and verify on **Status** that time, backhaul, and LoRaWAN forwarding are healthy. Record the new version in the site dossier.

Autoreset is a contingency tool, not a default. IRIS does not need routine reboots; enable a scheduled restart only if your operational policy requires it or you need a last-resort recovery on unstable upstream networks. Prefer to address root causes and rely on the connectivity watchdog and NTP for continuity.

When issues arise, use **AT Commands** for targeted diagnostics of the cellular modem and the IRIS software, and keep a **clean Reboot** available for controlled restarts during maintenance. Maintain disciplined change control: **apply one change at a time, save & apply, verify on Status, and log the action**. This rhythm keeps operations predictable

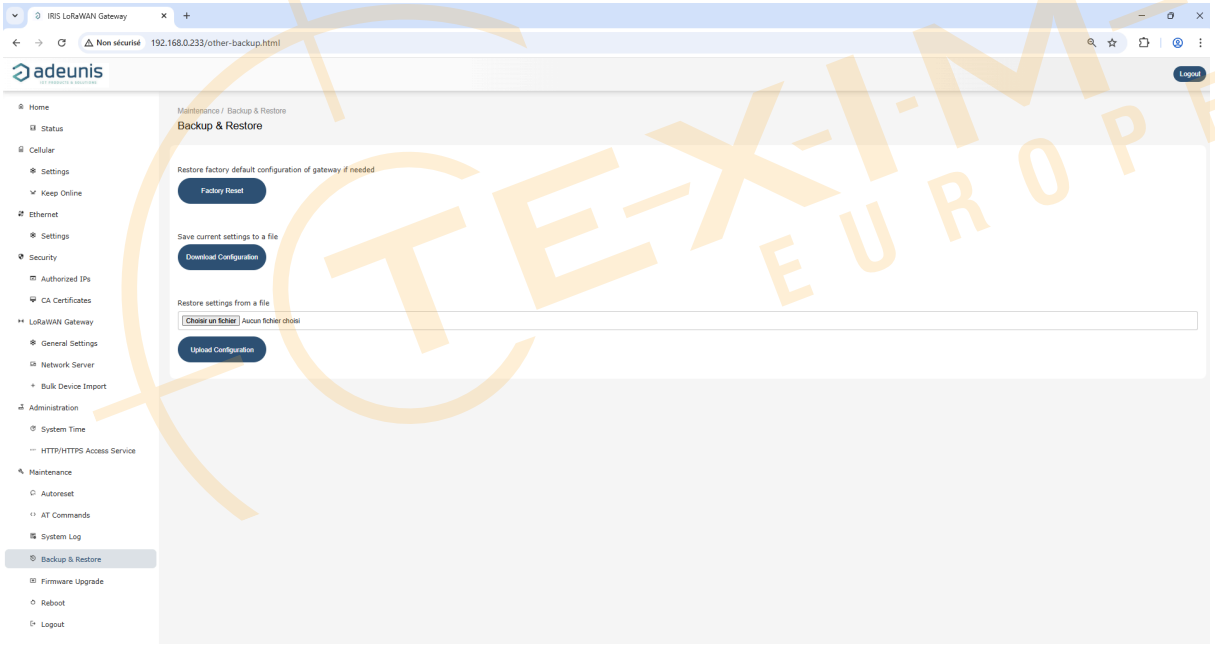
Distributed by www.texim-europe.com

and troubleshooting fast.

8.1. Configuration Backups

Safeguard configuration, perform rapid rollbacks, or return the device to its factory defaults from this menu.

- Click **DOWNLOAD CONFIGURATION** to export the current settings and store the file with your site documentation (always do this **before** firmware upgrades or major changes).
- To restore, select the archive and **UPLOAD CONFIGURATION**. The IRIS application will reapply parameters; verify network access and LoRaWAN forwarding after a restore.
- **FACTORY SETTINGS** returns the device to default configuration and erases custom settings. Use with caution, and only after exporting a fresh backup. A physical long-press on the “Function” button performs the same reset.



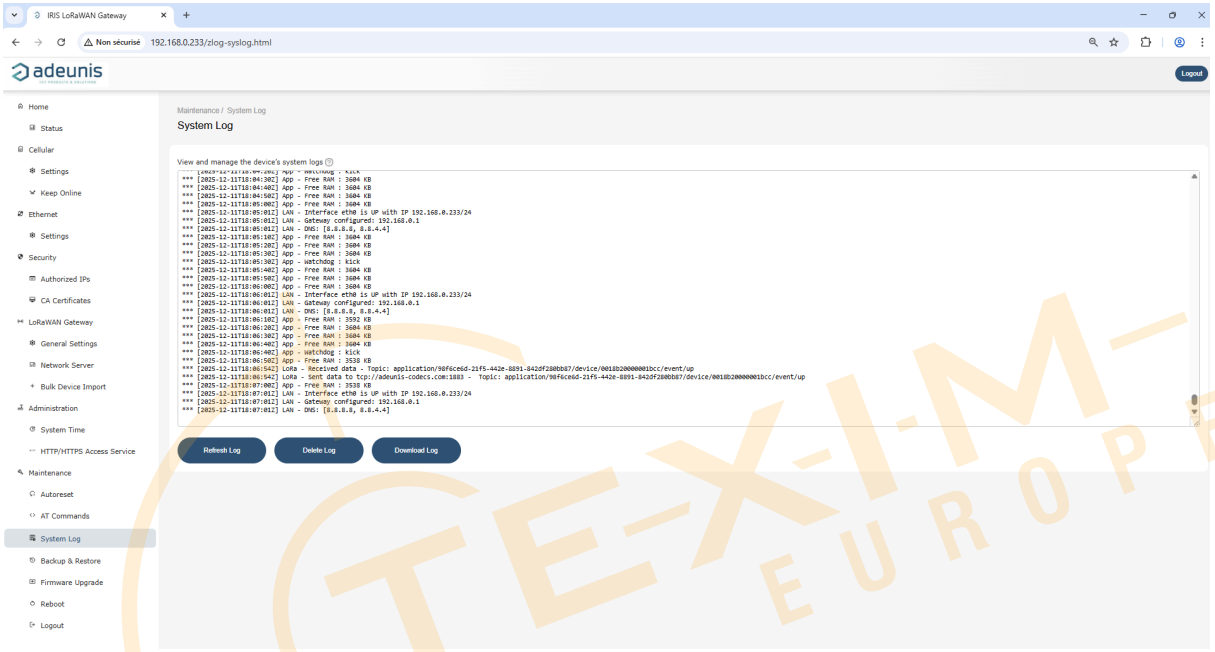
📌 After initial commissioning, export a configuration backup and store it with your site records. Do this again before any firmware update or major change.

Distributed by www.texim-europe.com

8.2. Logs and Diagnostics

Use the built-in logs to review recent system and cellular events directly in the browser, or export them for support.

1. You'll see the rolling device log, including cellular registration messages, link state changes, and application notices (e.g., RSRP/RSRQ samples, IP assignment).
2. Use **REFRESH LOG** to fetch the latest entries, **DELETE LOG** to clear the in-device buffer, and **DOWNLOAD LOG** to export a .mtx file for analysis or to attach to a support ticket.



📌 Make sure NTP is configured and synchronized so log timestamps align with your fleet and backend systems; mismatched clocks make correlation difficult.

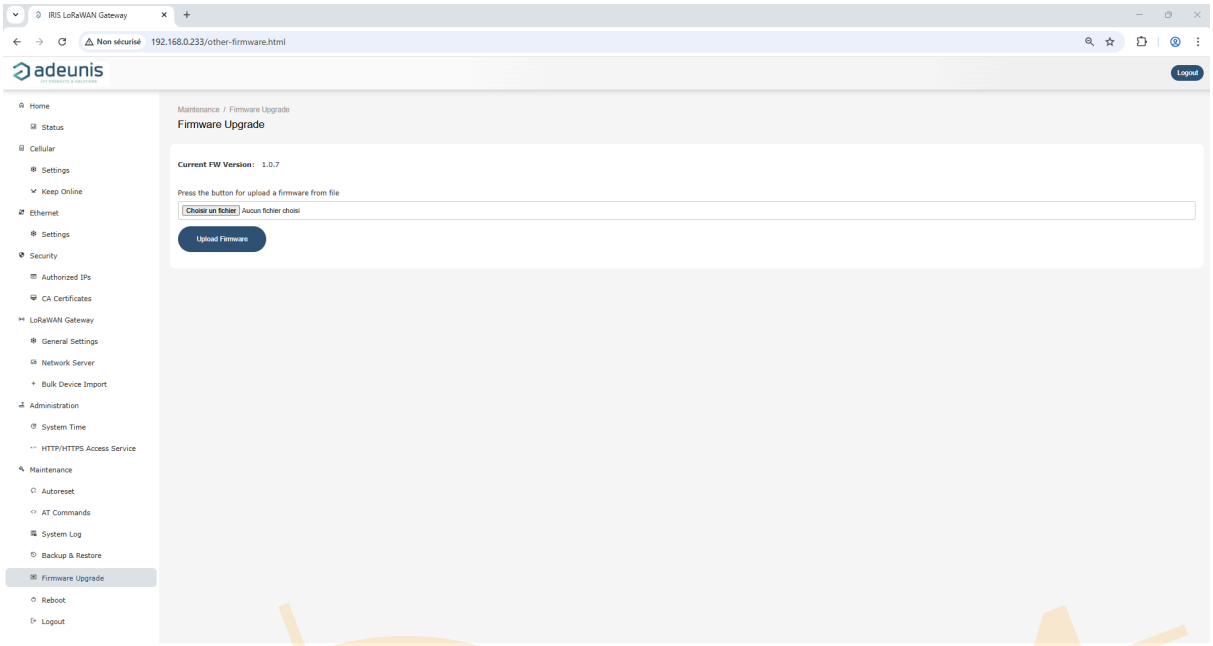
8.3. Firmware Updates

When a new firmware build is provided by the Adeunis Team, upload it through the Web GUI.

1. Check **Current FW Version** and compare with your release note.

Distributed by www.texim-europe.com

2. Click **UPLOAD FIRMWARE**, select the provided image, and wait for verification and install. Do **not** cut power during the process.
3. The gateway will reboot automatically when the upgrade is applied.



3. After the restart, confirm the new version on **Home** → **Status**, check that time is synchronized, and verify that your network access and LoRaWAN configuration are still active.

📌 Keep a configuration backup from just before the upgrade to speed up recovery if required.

8.4. Autoreset

Schedule a clean, unattended reboot during a maintenance window, or trigger an automatic restart when the device detects persistent IP connectivity issues.

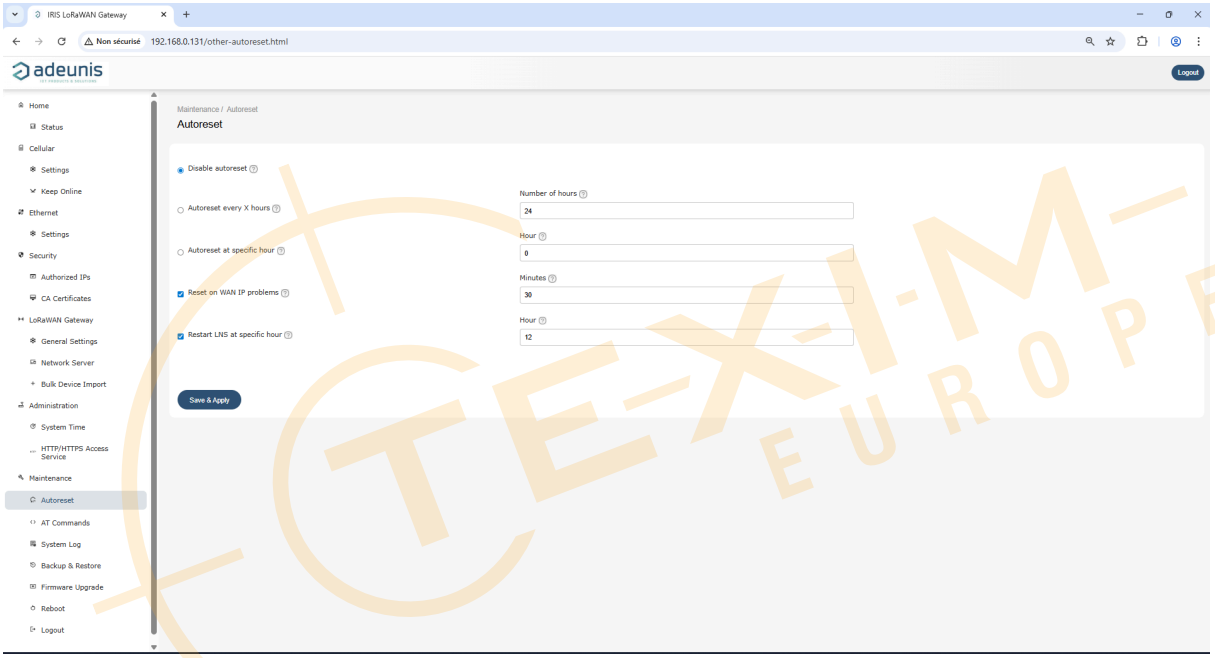
Use this feature sparingly: IRIS does not require routine reboots under normal conditions. Prefer to fix root causes (power, RF coverage, upstream network) and use **Keep Online** and NTP for continuous operation.

1. Choose one of the three modes:

Distributed by www.texim-europe.com

- **Autoreset not enabled:** recommended default.
- **Autoreset every X hours:** useful on remote sites that benefit from regular housekeeping.
- **Autoreset at specific hour:** schedule a daily reboot in a quiet time slot (e.g., 03:30 local time).

2. If you need a safety net for stalled WAN links, enable **Reset if IP problems**. This watchdog causes a reboot only if the gateway fails to recover connectivity on its own.
3. If you use the embedded LoRaWAN server, you can schedule a periodic restart of the service by enabling the **Restart LNS at a specific hour** option. With more than 100 sensors connected to the gateway, we recommend scheduling a regular restart to maintain optimal performance.



8.5. AT Commands

The **AT Command** console is a controlled window to query the cellular module and the IRIS software.

It is intended for diagnostics. Use it to check registration state, signal quality and data context when the Mobile WAN behaves unexpectedly.

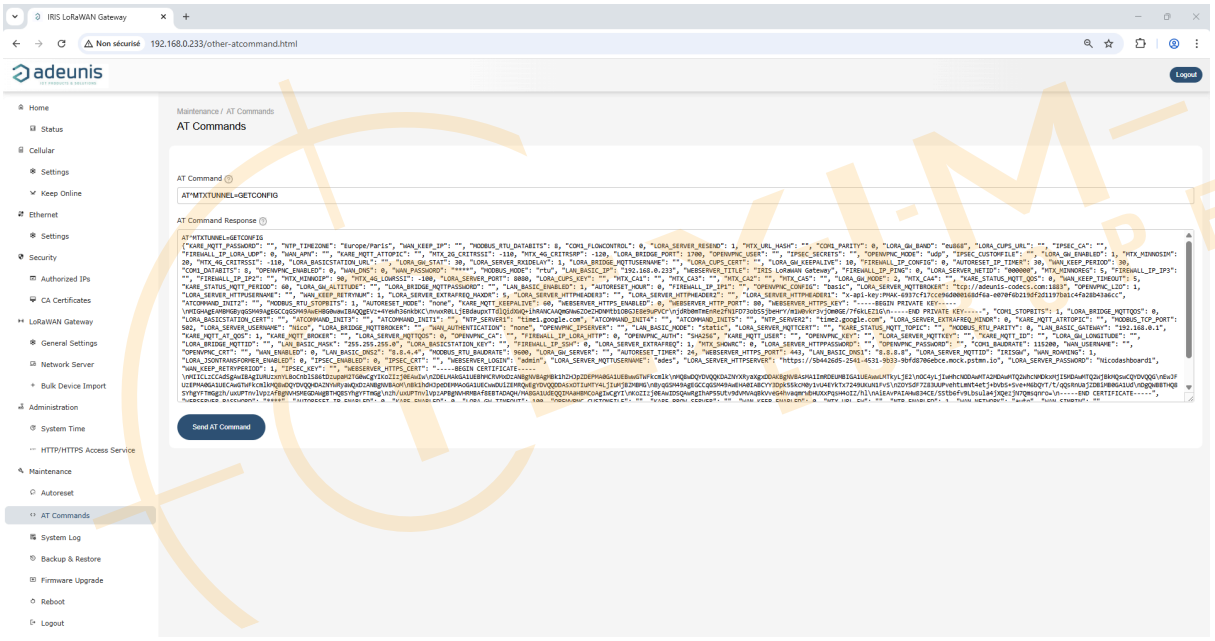
Keep it read-only unless you follow a precise procedure from support.

Distributed by www.texim-europe.com

When investigating an incident, grab the AT output together with timestamps and the last lines of **Syslog**, then attach both to your ticket.

8.5.1. Using the Console Safely

1. Ensure you have a **fresh configuration backup** and a **clear rollback plan.**
2. Enter a command in **AT Command.**
3. Click **SEND AT COMMAND.**
4. And read the gateway's raw response in **AT Command Response.**
5. Apply **one change at a time**.
6. If behavior becomes inconsistent after a change, **re-apply settings via the GUI**, or perform a **controlled Reboot**; use **Factory Settings** only as a last resort with a backup at hand.



As soon as the check is complete, exit the console and validate again on **Home → Status** that the modem is registered and has an IP address.

📌 Use the AT console primarily for **read-only diagnostics.**
Before running **state-changing commands contact Adeunis support** and proceed under guidance.

Distributed by www.texim-europe.com

8.5.2. IRIS Software Helper Commands

The following commands interrogate the IRIS application layer.

Command	Purpose / Example output
`AT^MTXTUNNEL=VERSION`	Return IRIS software version (useful for support tickets).
`AT^MTXTUNNEL=GETTIME`	Return current device time (UTC and local timezone).
`AT^MTXTUNNEL=GETCONFIG`	Dump the current IRIS configuration (use before/after changes).
`AT^MTXTUNNEL=GETPARAM,<KEY>`	Read a specific parameter, e.g., `AT^MTXTUNNEL=GETPARAM,NTP_SERVER1`.
`AT^MTXTUNNEL=GETIP`	Report the last assigned WAN IP.
`AT^MTXTUNNEL=REBOOT`	Trigger a controlled application reboot.

8.5.3. Common Sierra Modem Checks

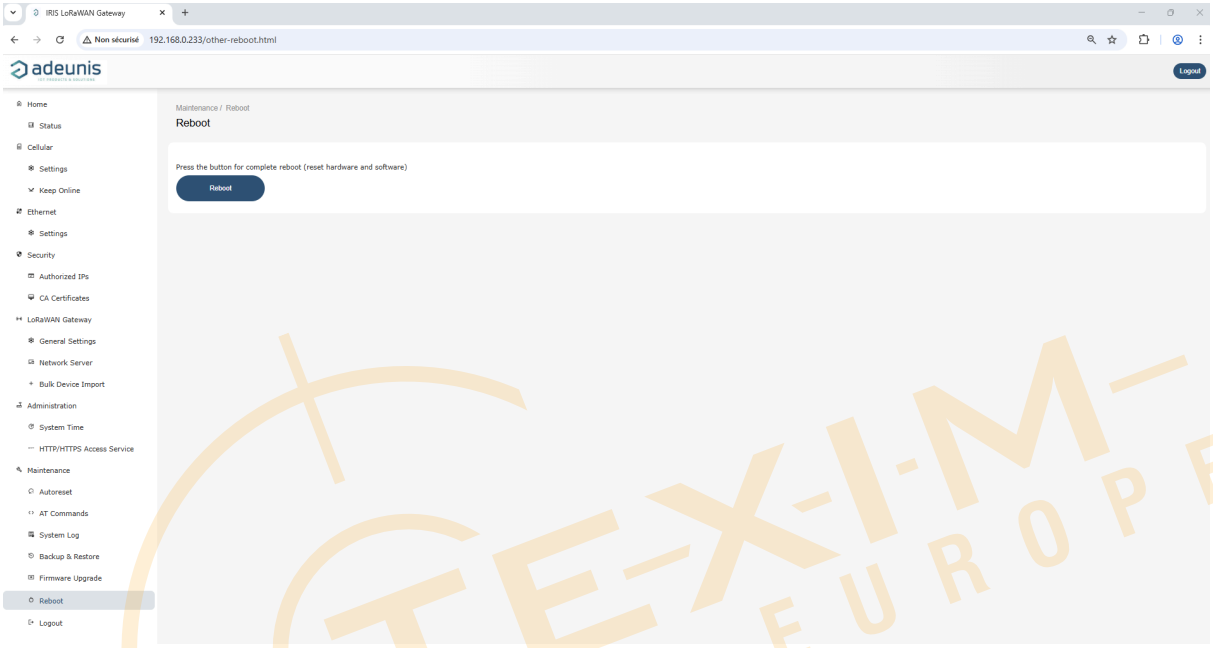
These are standard diagnostics to assess registration and radio quality.

What you want to check	Example command(s)	Notes
Signal quality snapshot	`AT+CSQ`	Returns RSSI (0–31) and BER. Interpretation scale is defined in the guide.
LTE registration status	`AT+CEREG?`	EPS registration state per 27.007; basic outcomes (not registered / searching / registered).
High-level modem status	`AT!GSTATUS?`	Aggregated serving cell, RAT, temperature, etc. (quick health check).
Detailed LTE metrics	`AT!LTEINFO?`	EARFCN, band, PCI, RSRP/RSRQ/SNR, TAC, cell IDs. Useful to assess RF and neighbor list.
Cellular IP context	`AT+CGDCONT?` / `AT+CGPADDR` / `AT+CGCONTRDP`	Verify APN profile and assigned IP.

8.6. Reboot

Use the reboot function to perform a controlled system restart without altering configuration.

1. Click **REBOOT** to start the reboot procedure (hardware & software). The configuration is preserved, but time synchronization may be lost if no NTP server is configured and the clock has been set manually.
2. The device will terminate services cleanly and restart.



Use this when support asks for a clean restart during troubleshooting.

8.7. Validation & Routine Checks

This section gives you a short, repeatable operations routine you run after maintenance windows or periodically to confirm the gateway is healthy and that the LoRaWAN data path (uplink and downlink) works as expected.

8.7.1. When to run it

- At the end of commissioning or a maintenance window.

Distributed by www.texim-europe.com

- After a **firmware upgrade** or a **security/network change** (HTTPS, Authorized IPs, NTP, APN, VLAN).
- **Quarterly** as a preventive check on long-running sites.

8.7.2. Procedure

1. **Status sanity**

Open **Home** → **Status** and confirm:

- **Uptime** is increasing; **Device Time** is correct (NTP).
- The chosen backhaul (**Ethernet** or **Cellular**) shows a valid **IP** and is **Up**.
- LoRaWAN mode/band are as expected (if already configured). **Gateway EUI** is the one registered in your LNS (or visible in the embedded server).

2. **Security posture**
   - Confirm **Web GUI** loads over **HTTPS**; browser shows **lock** with **no warnings** when a custom certificate is installed.
   - **Authorized IPs** on Mobile WAN: selectors are set to **ALLOW ONLY AUTHORIZED IPs** (or functionally blocked by empty allow-list where you want no exposure). Test from one **authorized** and one **non-authorized** source if Mobile WAN access is in scope.

3. **Time & NTP**
   - Check **NTP Time Servers** still lists reachable servers; timezone matches the site.
   - If you used hostnames, validate that **DNS** works on the active backhaul.

4. **Connectivity watchdog (cellular sites)**
   - If applicable, confirm that **Keep Online** watchdog is configured against a stable/reachable ping target.
   - Check period/timeout/retries are reasonable and no recovery storms are visible in logs.

5. **Cellular health (if used)**
   - If cellular interface is used, **Open AT Command** and run `AT+CSQ`, `AT+CEREG?`, `AT!GSTATUS?` / `AT!LTEINFO?` to snapshot signal and registration.

Distributed by www.texim-europe.com

- **Recommendation:** use AT mainly **read-only**; contact support before any state-changing commands.

6. **Backup**
   - Export **CONFIGURATION and store it** with the site ID, date, and firlware version.

7. **Autoreset policy**
   - Confirm **Periodic Autoreset** is aligned with the site's maintenance policy (ideally **Disabled** unless required).

8. **LoRaWAN**
   - Trigger a known device **join / test uplink**.
   - Verify frames at the LNS and (if applicable) a test downlink for UDP PF sites.

Acceptance checklist is available on Annex 5

This routine proves the **full path**: secure admin → time/right band → gateway ↔ LNS session → device join → uplink → downlink.

9. DOCUMENT HISTORY

Version	Content
V 1.0	Creation

ANNEX 1 GLOSSARY & ACRONYMS

Term / Acronym	Expansion	Plain-language definition	Where it appears / why it matters
2G / 3G / 4G (LTE Cat-1)	Second/Third/Fourth-Gen Cellular	Mobile network generations; Cat-1 is an LTE data category widely supported for M2M.	Cellular backhaul capabilities and coverage.
ABP	Activation By Personalization	Devices start with fixed session keys (no join).	Commissioning choice; less common than OTAA.
ACK	Acknowledgement	Confirmation that a frame was received (e.g., confirmed downlink).	Verifies reliable delivery in tests.
ADR	Adaptive Data Rate	Network optimizes data rate/RF power for device.	Affects range, airtime, and battery life.
APN	Access Point Name	Operator profile that gives the modem IP connectivity.	Mandatory in cellular settings.
AppKey / NwkKey	Application/Network Key	OTAA root keys used to derive session keys at join.	Needed to register devices on LNS.
Application Server	—	Consumes decoded device data and integrates to IT/BMS.	End of the LoRaWAN data path.
Authorized IPs	—	Allow-list that restricts who can reach services on Mobile WAN.	First line of defense when exposing the GUI or UDP downlinks over cellular.
Autoreset	—	Scheduled reboot or last-resort recovery if IP is unrecoverable.	Day-2 reliability; use sparingly.
BASICS STATION (WSS)	—	LoRaWAN gateway protocol over (secure) WebSockets to LNS.	Alternative to UDP PF; needs TLS trust (CA) and correct time.
CA (Root CA)	Certificate Authority	Trust anchor used to validate TLS server certificates.	Required for WSS/MQTTs/HTTPs when private CAs are used.
Cat-1	LTE Category 1	LTE modem capability profile (throughput/features).	Modem capability; coverage expectations.

Term / Acronym	Expansion	Plain-language definition	Where it appears / why it matters
CHAP / PAP	Challenge-Handshake / Password Auth	APN credential methods.	Set per operator for cellular attach.
Class A / C	LoRaWAN Device Classes	A: lowest power; C: nearly always listening (more downlink-friendly).	Affects downlink timing and power.
CN / SAN	Common Name / Subject Alt Name	Certificate fields that must match the server hostname.	Avoid TLS warnings when using HTTPS/WSS.
Codec (Payload Decoder)	—	JavaScript (or built-in) logic that decodes payload bytes into fields.	Validates data path in uplink tests.
DevEUI	Device EUI-64	Globally unique device identifier.	Needed to register devices on LNS.
DHCP	Dynamic Host Configuration Protocol	Hands out IP, mask, gateway, DNS automatically.	Simplifies Ethernet commissioning.
DNS	Domain Name System	Resolves hostnames (e.g., NTP, WSS) to IP addresses.	Mandatory for NTP names and WSS URLs.
Downlink	—	Network → device message.	Proves inbound path (esp. UDP PF).
E2E	End-to-End	Full chain from device RF to application.	Site acceptance and quarterly checks.
EARFCN	E-UTRA Absolute RF Channel Number	LTE channel index (implies band and frequency).	AT diagnostics for cellular RF.
EUI-64	Extended Unique Identifier (64-bit)	Format for gateway and device identifiers.	Used as Gateway EUI / DevEUI.
Factory Settings	—	Restores defaults (erases config).	Only after exporting a backup.
FCntUp / FCntDown	Frame Counters	Monotonic counters for uplink/downlink frames.	Helps spot resets/replays; downlink success.
Firmware	—	The gateway software image.	Upgrades under Maintenance → Firmware.
Gateway EUI	—	The gateway's EUI-64 identity as seen by the LNS.	Must match registration on the LNS.

Term / Acronym	Expansion	Plain-language definition	Where it appears / why it matters
HTTP / HTTPS	HyperText Transfer Protocol (Secure)	Browser access to the Web GUI; HTTPS encrypts and authenticates.	Enforce HTTPS in production; install proper cert.
HTTPs Cert / Key (PEM)	—	Server certificate and private key in PEM format.	Needed to remove browser warnings over HTTPS.
IMEI	International Mobile Equipment Identity	Modem hardware identifier.	Appears on Status; useful in tickets.
IP / Subnet Mask / Gateway	—	IP addressing parameters.	Ethernet static deployments and validation.
IP67	—	Dust-tight and protected against immersion up to 1 m (short time).	Environmental rating of enclosure.
Join (OTAA)	Over-The-Air Activation	Device requests to join; LNS accepts and derives session keys.	First functional proof in commissioning.
JoinEUI (AppEUI)	Join/Application EUI	Identifier used during OTAA join.	Must match LNS/app settings.
LAN / VLAN	Local Area Network / Virtual LAN	Customer IP network segments.	Where Ethernet deployments live.
LNS	LoRaWAN Network Server	Manages devices, MAC, ADR, dedup, downlinks.	The gateway forwards to this (or hosts it embedded).
LoRa	Long Range (RF layer)	Chirp spread spectrum radio used by LoRaWAN.	Physical layer from device to gateway.
LoRaWAN	—	Protocol suite above LoRa RF (MAC + network).	The full IoT stack you're deploying.
LTEINFO / GSTATUS	—	Sierra modem AT diagnostics (serving cell, RSRP/RSRQ/SINR, bands).	Quick cellular health snapshot.
MAC (Ethernet)	Media Access Control	Hardware address of Ethernet interface.	Appears on Status; inventory/IT.
MAC Commands	LoRaWAN MAC layer commands	Network control messages (e.g., ADR, LinkCheck).	Seen on LNS during diagnostics.

Distributed by www.texim-europe.com

Term / Acronym	Expansion	Plain-language definition	Where it appears / why it matters
MQTT / MQTTs	Message Queue Telemetry Transport (secure)	Lightweight pub/sub used by some integrations.	Used by embedded LNS integrations.
NAT	Network Address Translation	Maps private ↔ public IPs.	Explains inbound reachability limits.
NOC	Network Operations Center	Operational team managing gateways/LNS.	On allow-lists and tickets.
NTP	Network Time Protocol	Synchronizes device time.	Required for TLS and coherent logs.
OTAA	Over-The-Air Activation	Secure activation method using root keys.	Recommended device activation mode.
Packet Forwarder (UDP)	—	Legacy Semtech UDP uplink/downlink to LNS.	Simple and common; needs inbound UDP allowed for downlinks.
PCI	Physical Cell ID	LTE cell identifier at PHY layer.	AT diagnostics for serving/neighbor cells.
PEM	Privacy-Enhanced Mail (format)	Text format for certs/keys (`-----BEGIN CERTIFICATE-----`).	Required by HTTPS/WSS/CA pages.
PKCS#1 / PKCS#8	—	Encodings for private keys in PEM.	HTTPS Key format accepted by the GUI.
PIN / PUK	Personal ID / Unlock Key	SIM security codes.	Wrong PIN 3× blocks SIM until PUK used.
PoE	Power over Ethernet	Power on RJ45 (not supported on IRIS).	Clarifies power expectations.
PTP (not used here)	Precision Time Protocol	Higher-accuracy timing alternative to NTP.	Not supported; use NTP.
Reboot	—	Controlled restart without changing config.	Use during maintenance or recovery.
RSRP / RSRQ / SINR	LTE signal metrics	Power, quality, and interference indicators.	Assess LTE link quality on cellular sites.
SIM	Subscriber Identity Module	The operator card providing cellular service.	Mandatory for cellular backhaul.
SNR (LoRa)	Signal-to-Noise Ratio	LoRa RF link quality metric.	Sanity check on uplink frames.

Distributed by www.texim-europe.com

Term / Acronym	Expansion	Plain-language definition	Where it appears / why it matters
Static IP	—	Fixed IP addressing (vs DHCP).	Common in enterprise LANs; coordinate with IT.
Status Page	—	Read-only gateway dashboard.	First place to verify time, IP, RF/backhaul health.
Syslog	System Log	Rolling system/application logs; downloadable.	Evidence for diagnostics/tickets.
TAC	Tracking Area Code	LTE tracking area identifier.	AT diagnostics for cellular registration.
TLS 1.2	Transport Layer Security	Modern encryption/auth for HTTPS/WSS/MQTTs.	Security baseline; requires correct time and CA.
Uplink	—	Device → network message.	First visible success after join.
UDP / TCP	User/Transmission Control Protocol	Transport layers for PF (UDP) and HTTPS/WSS (TCP).	Drives firewall rules/Authorized IPs choices.
WSS / WS	(Secure) WebSocket	Persistent TCP (TLS) channel used by Basics Station.	Requires CA trust and correct time.
Watchdog (“Keep Online”)	—	Pings a target and heals stalled cellular data sessions.	Improves resilience on mobile backhaul.

ANNEX 2 QUICK START

Get one end-device online, see uplinks, and send a test downlink.

Prerequisites

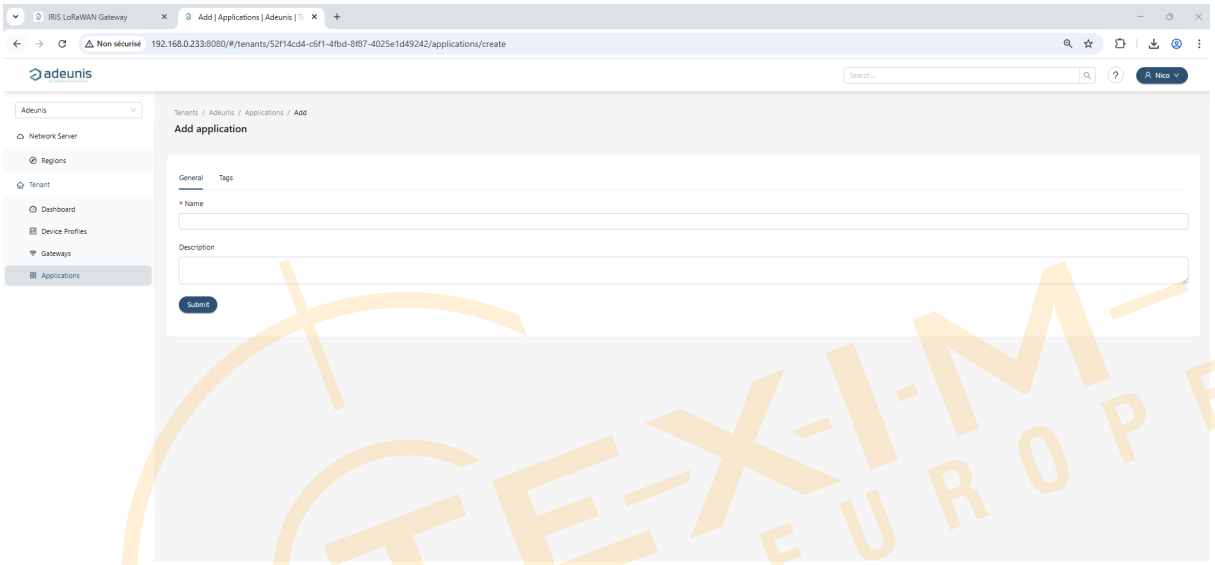
Distributed by www.texim-europe.com

- Gateway is powered and **Online** in **Tenant → Gateways**.
- You know the **DevEUI**, **JoinEUI (AppEUI)** and **AppKey** of the device.

Step-by-step

1. **Create an application**

   Go to **Tenant → Applications → Add application**. Give it a name and save.

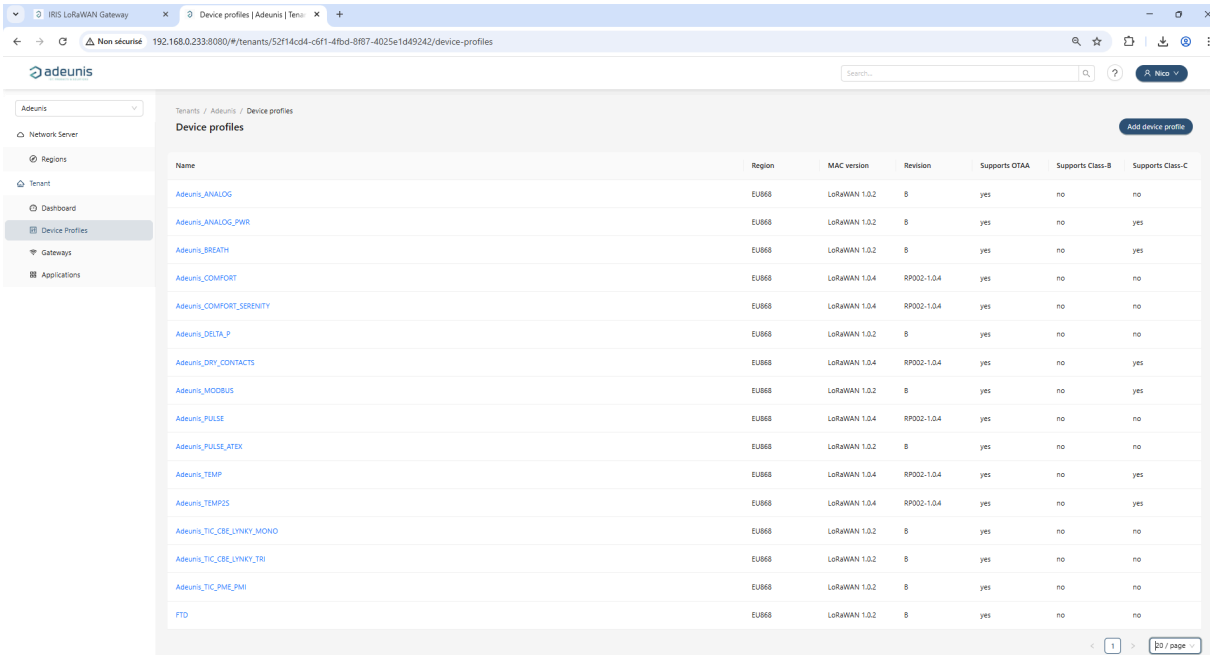


2. **Create / choose a Device-profile**

   Go to **Tenant → Device Profiles** (or use an existing one, e.g., *Adeunis_COMFORT*).

   Confirm **Region = EU868**, **LoRaWAN MAC = 1.0.x**, ADR as needed.

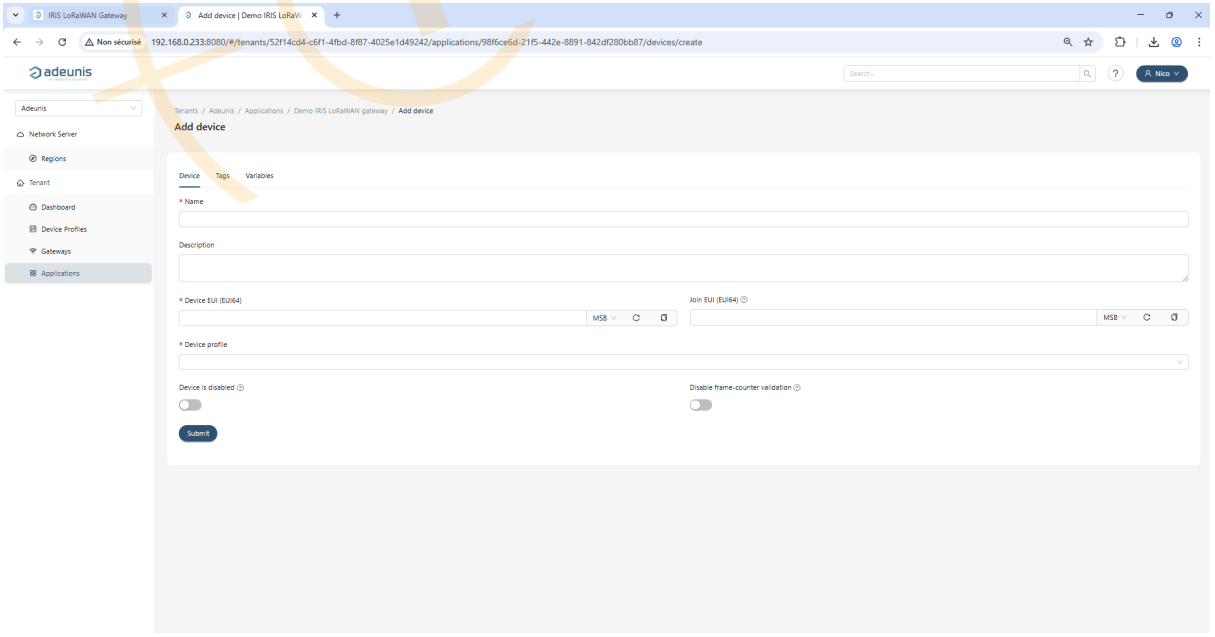
Distributed by www.texim-europe.com



3. **Register the device (OTAA)**

   In **Applications → your application → Devices → Add device**:

   - Set **Name/Description**.
   - **DevEUI**, **JoinEUI** (AppEUI), **Device profile**.
   - In **OTAA keys**, paste the **AppKey**.
   - Save.



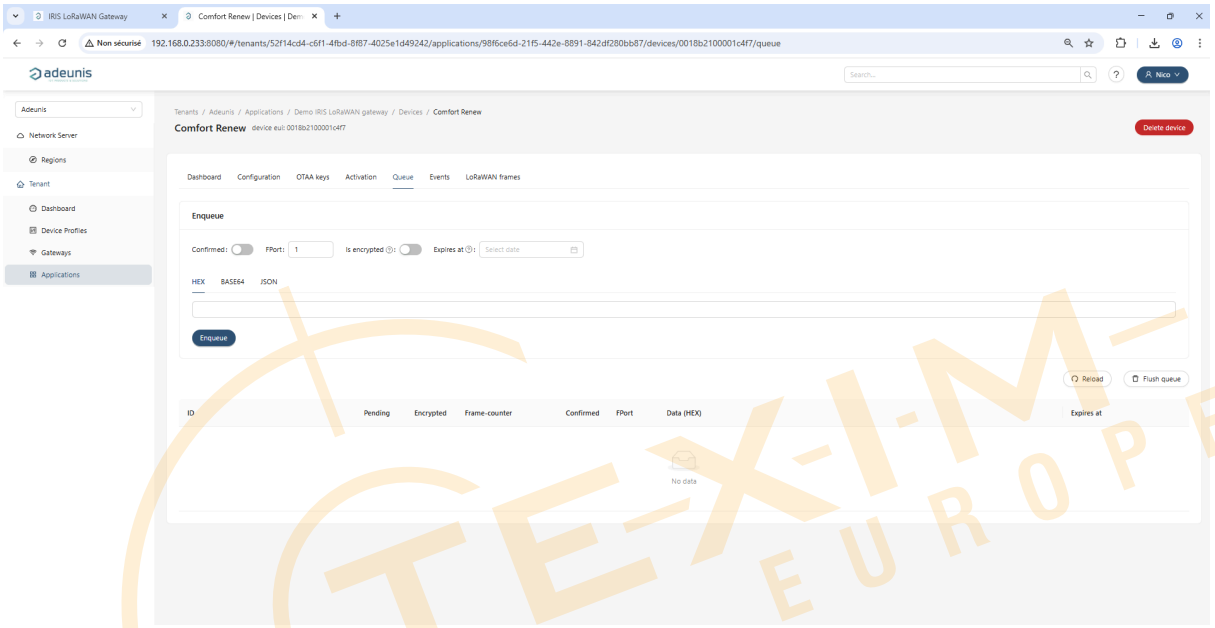
4. **Power / reset the device** and wait for a **Join** event.

   Check **Device** → **LoRaWAN frames / Events** for *JoinRequest/JoinAccept* and first uplinks.

5. **(Optional) Send a test downlink**

   Open **Device** → **Queue**: set **FPort** (≠0), paste payload (HEX/Base64/JSON), choose **Confirmed** if needed, then **Enqueue**.

   The downlink will be delivered in the next receive window (Class A) or immediately (Class C).



ANNEX 3 REGISTERING AN ADEUNIS COMFORT SENSOR

This worked example shows how to register an **Adeunis COMFORT** end device (indoor temperature & humidity) in the embedded LoRaWAN Server UI, following the same flow as section **5.6.7 Add Devices**.

Distributed by www.texim-europe.com

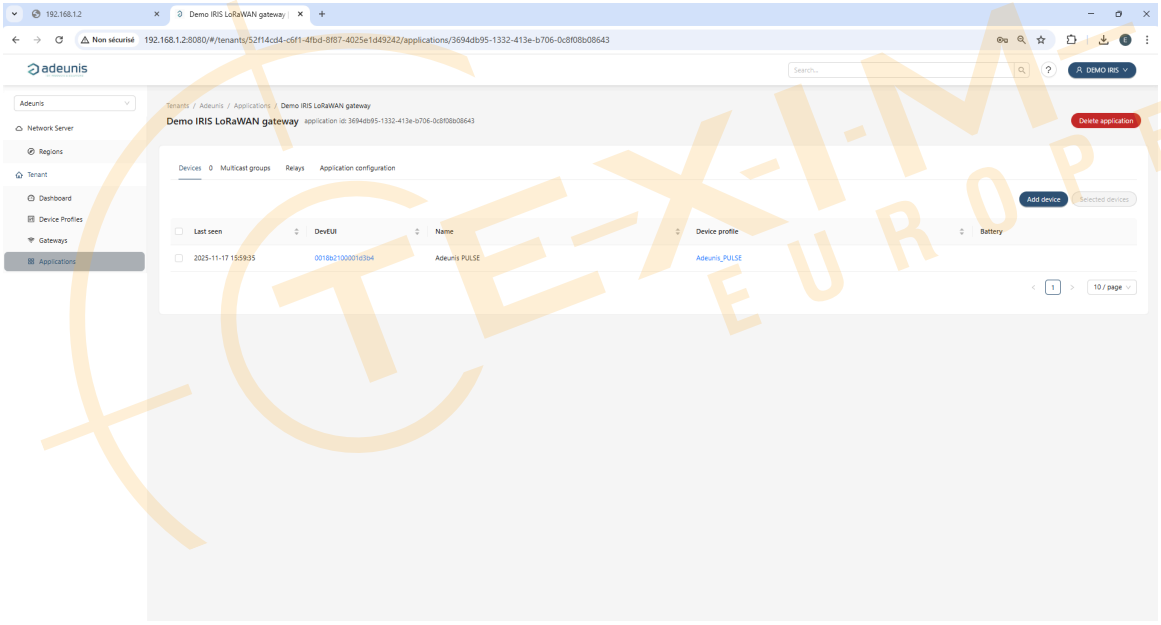
Prerequisites

- The credentials, DevEUI, AppKey, and JoinEUI/AppEUI have been provided by the device manufacturer.
- You already created an **Application**.
- A **Device Profile** matching the device exists (e.g., `Adeunis_COMFORT`, EU868, correct LoRaWAN MAC version / codec).

Step-by-step

1. **Open the add form**

   Go to **Tenant** → **Applications** → ***your application*** → **Devices** → **Click on Add device button**.



2. **Fill the Device tab** (example values below)

   - **Name**

   Enter any desired test, in this example: `Adeunis COMFORT – Meeting room 1`

   - **Description**

   Enter any desired test, in this example: Temperature and Humidity monitoring in Meeting room 1

Distributed by www.texim-europe.com

- **Device EUI (EUI-64)**

Provided by device manufacturer, in this example: `0018b2100001a545`

- **JoinEUI (EUI-64 / AppEUI 1.0.x)**

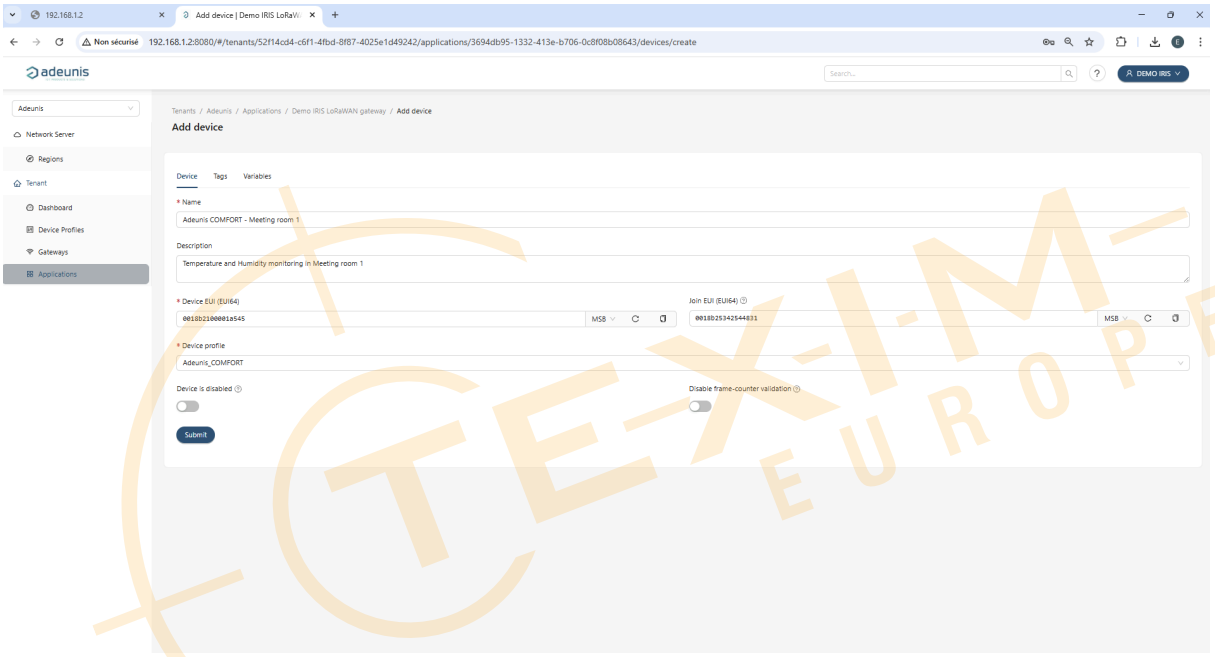
Provided by device manufacturer, in this example: `0018b25342544831`

- **Device profile**

Select the profile corresponding to this device, in this example: `Adeunis_COMFORT`

If the device profile does not exist, it must be created.

- Keep **Device is disabled** OFF and **Disable frame-counter validation** OFF for normal OTAA use,
- Then **Submit**.



3. **Set OTAA keys**

The OTAA keys Tab automatically opens and you can set the last credential, the AppKey:

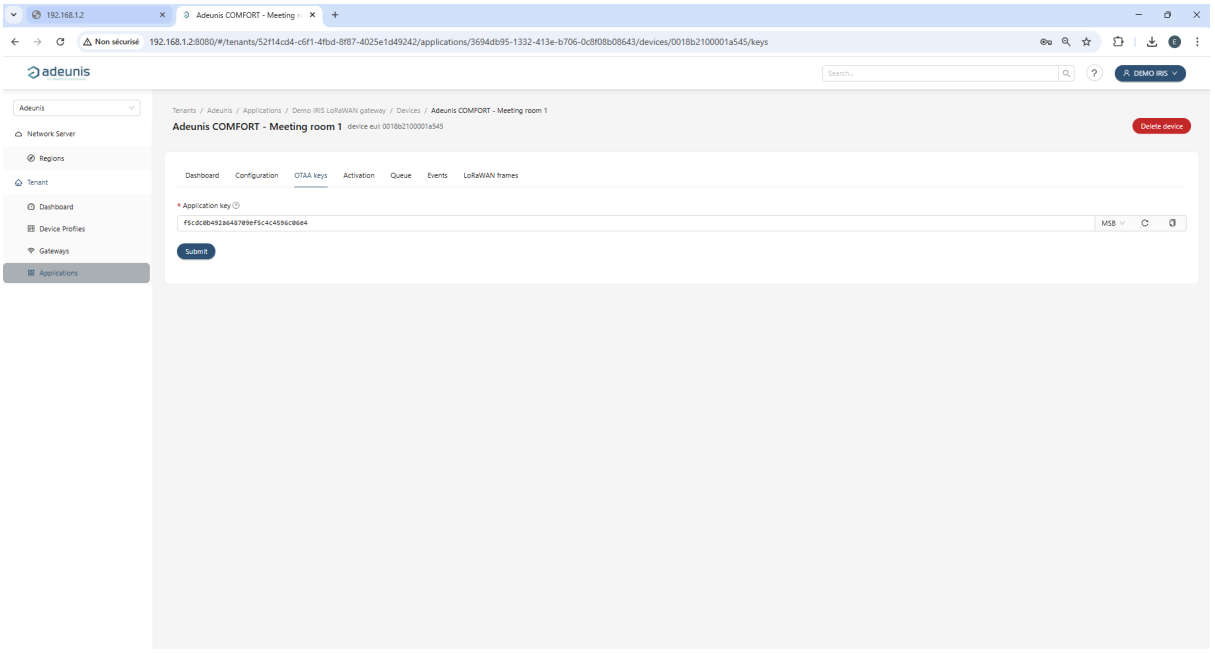
- **AppKey**

Provided by device manufacturer, in this example: `f5cdc0b492a648709ef5c4c4596c06e4`

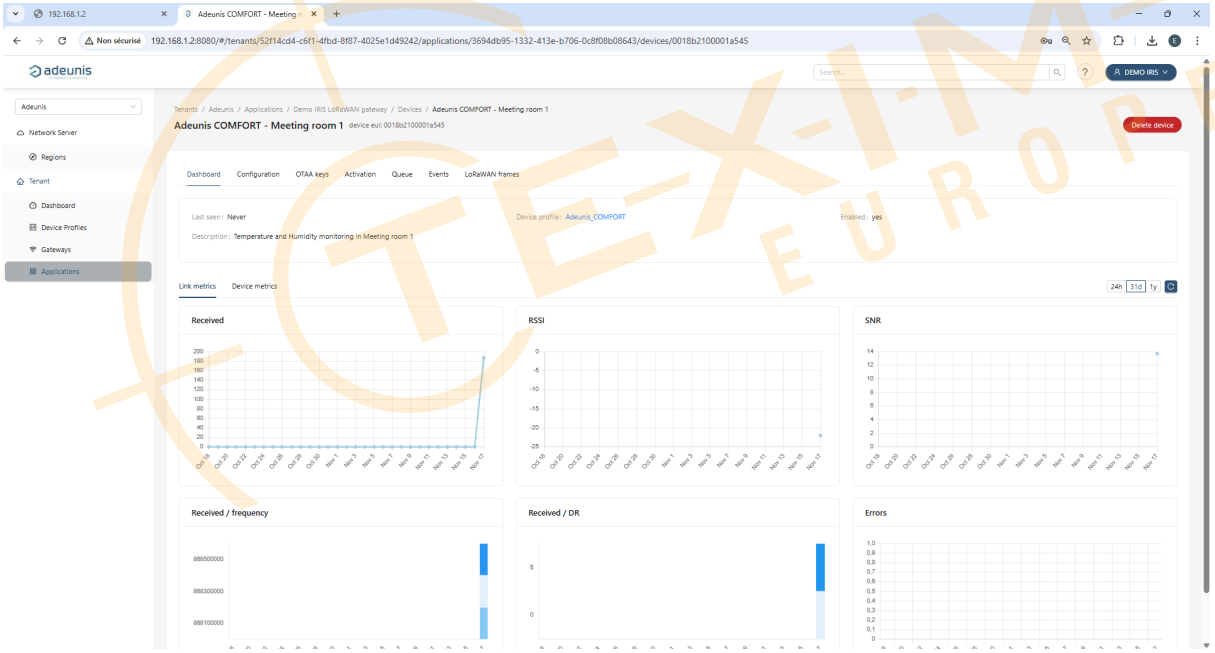
(For LoRaWAN 1.0.x OTAA, only AppKey is required; for 1.1 you would also set NwkKey.)

- **Submit**

Distributed by www.texim-europe.com



The information panel for the newly added device will open



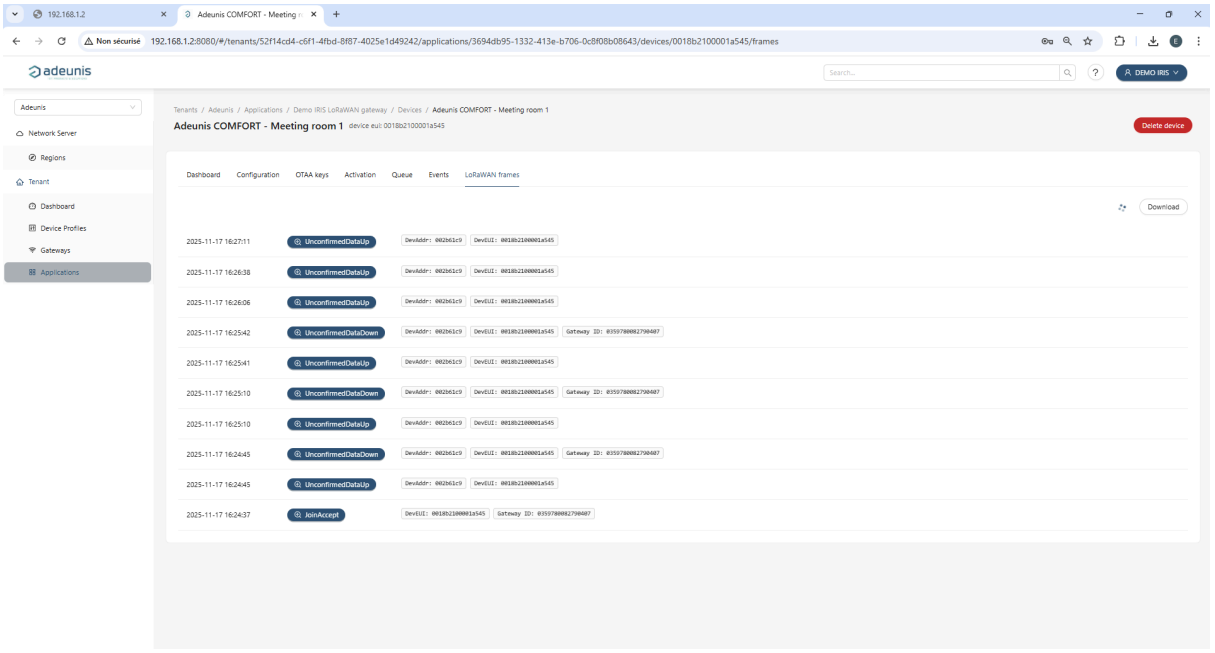
4. **Commission & verify**

Power the sensor to start the join process.

In **Applications** → **Devices** → ***your device*** → **LoRaWAN frames**, verify a **Join-request/Join-accept**

followed by uplinks.

Distributed by www.texim-europe.com



You can also use the **Events / Frames** view for detailed radio and MAC info.

ANNEX 4 BULK REGISTERING DEVICES (CSV/JSON)

This annex explains how to register many LoRaWAN end-devices in one operation using the **Bulk Device Import** tool. Use it for initial roll-outs or when adding batches of sensors to an existing application. This worked example follows the same flow as section **5.6.7 Add Devices**.

Prerequisites

- You have already created the **Application** that will own these devices and you know its **Application ID** (see Where to find it below).
- Each device has its identifiers and keys (DevEUI, JoinEUI/AppEUI, AppKey; for 1.1 also NwkKey). These are provided by the device manufacturer.
- A matching **Device Profile** exists for each device type and you know the **Device Profile Name** (see Where to find it below).

Distributed by www.texim-europe.com

Where to get the IDs and keys before you prepare the CSV/JSON file (quick guide)

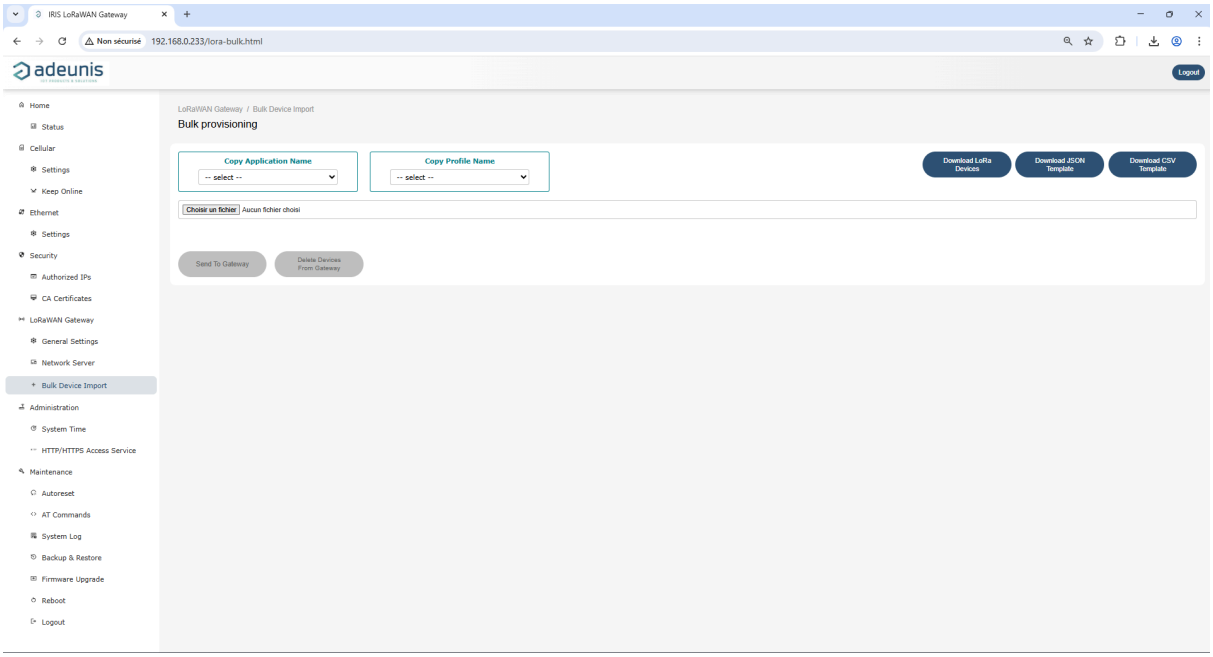
Field (CSV/JSON)	Where to find it	Notes
devEui	On the device label or vendor documentation.	Global EUI-64 identifier provided by the manufacturer.
joinEui (a.k.a. AppEUI for 1.0.x)	Vendor documentation / device label.	Required for most OTAA devices; 1.1 uses JoinEUI, 1.0.x uses AppEUI.
appKey (OTAA 1.0.x)	Vendor documentation / device label / shipment sheet.	32-hex; never guess. For LoRaWAN 1.1, also provide **nwk_key**.
nwkKey (OTAA 1.1)	Vendor documentation.	Present only for 1.1-class devices; if not provided, it's typically a 1.0.x device.
applicationName	LoRa Server Dashboard → **Tenant** → **Applications** → click your application; the **Application Name** is shown in the header.	You'll reference this value in the `applicationName` column during bulk import.
deviceProfileName	LoRa Server Dashboard → **Tenant** → **Device Profiles** → click the profile; the **Device Profile Name** is shown in the header.	Copy this value into the `deviceProfileName` column so devices inherit the correct region/MAC/codec.
isDisabled	Your choice (in template).	`false` for normal operation; `true` to keep devices blocked until you're ready.
skipFCntCheck	Your choice (in template).	Keep `false`. Enable only for temporary ABP troubleshooting.

Step-by-step

1. **Open the Bulk Import Tool**

In the gateway Web GUI, go to **LoRaWAN → Bulk Device Import**.

Distributed by www.texim-europe.com



2. **Download the Template**

Click **Download JSON template** or **Download CSV template**.

Always start from the template to ensure you use the canonical field/column names.

In this example, we are going to use the CSV file template.

	A	B	C	D	E	F	G	H	I	J	K	L
1	name	description	devEui	appKey	nwkKey	joinEui	deviceProfile	applicationN	isDisabled	skipFCntCheck		
2	Example Ade	Sensor for m	0018B210000	384E786F39A54445BE9C279E0EF1E0E9			Adeunis_BRE	LoRaWAN De	false	false		
3	Example Ade	Sensor for m	0018B210000	D2DD78FF18DC47EFBF85EADCCB2C13C9			Adeunis_COI	LoRaWAN De	false	false		
4	Example Hur	Sensor for m	B2903AD184	D2DD78FF58DC47EFBFA5E		B31D15AC45	Brand_XYZ_H	LoRaWAN De	false	false		
5	Light Sensor	Sensor for m	C2903AD184	D2DD78FF58DC47EFBFA5E		C31D15AC45	Brand_XYZ_L	LoRaWAN De	false	false		
6	Motion Sens	Sensor for de	D2903AD184	D2DD78FF58	11223344556	D31D15AC45	Brand_XYZ_M	LoRaWAN De	false	false		
7	Motion Sens	Sensor for de	D2903AD184	D2DD78FF58	11223344556	D31D15AC45	Brand_XYZ_M	LoRaWAN De	false	false		
8	Pressure Ser	Sensor for m	E2903AD184	D2DD78FF58DC47EFBFA5E		E31D15AC45	Brand_XYZ_P	LoRaWAN De	false	false		
9												
10												
11												
12												
13												
14												
15												
16												

3. **Prepare Your File**

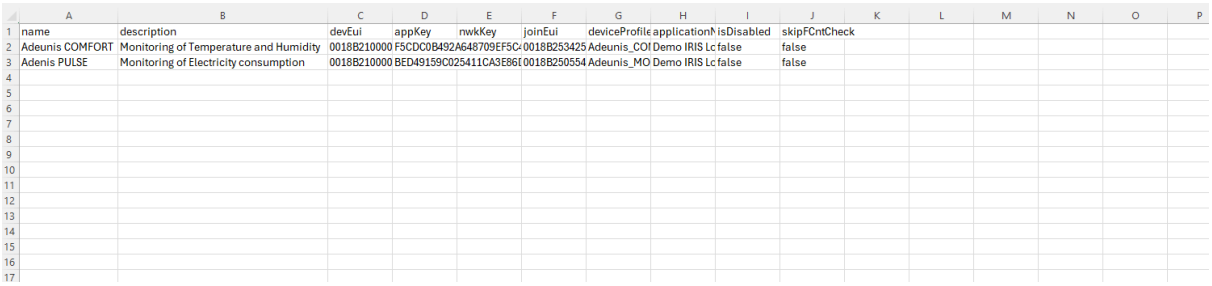
In this example, we want to add 2 sensors to the gateway.

So, we have to fill **one row per device with the following information**:

- **name**, **description**
- **dev_eui** (EUI-64)

Distributed by www.texim-europe.com

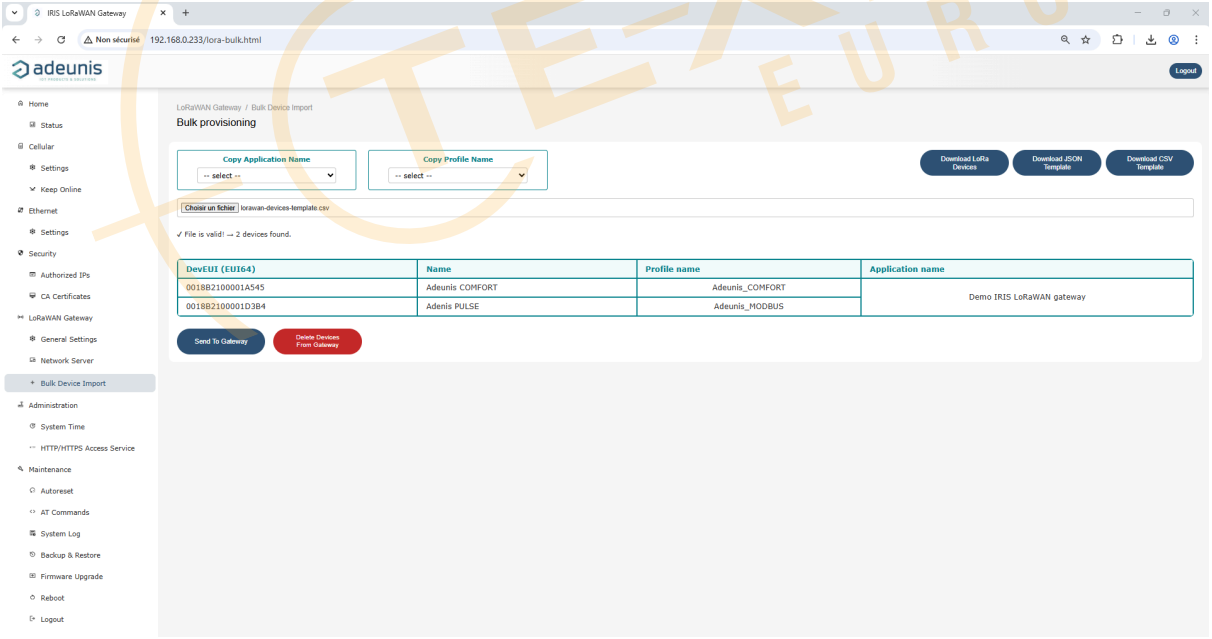
- **join_eui** (EUI-64, OTAA)
- **app_key** (LoRaWAN 1.0.x) and **nwk_key** (add for 1.1) for OTAA; or ABP **session keys** if applicable
- **device_profile_name** (target Device Profile)
- **application_name** (target Application)
- **device_disabled** (true/false)
- **disable_fcnt_check** (true/false)



	A	B	C	D	E	F	G	H	I	J
1	name	description	devEui	appKey	nwkKey	joinEui	deviceProfile	applicationN	isDisabled	skipFCntCheck
2	Adeunis COMFORT	Monitoring of Temperature and Humidity	0018B210000	F5CDC0B492A648709EF5C4		0018B253425	Adeunis_COI	Demo IRIS Lc	false	false
3	Adenis PULSE	Monitoring of Electricity consumption	0018B210000	BED49159C025411CA3E86E		0018B250554	Adeunis_MO	Demo IRIS Lc	false	false

4. **Upload and Execute**

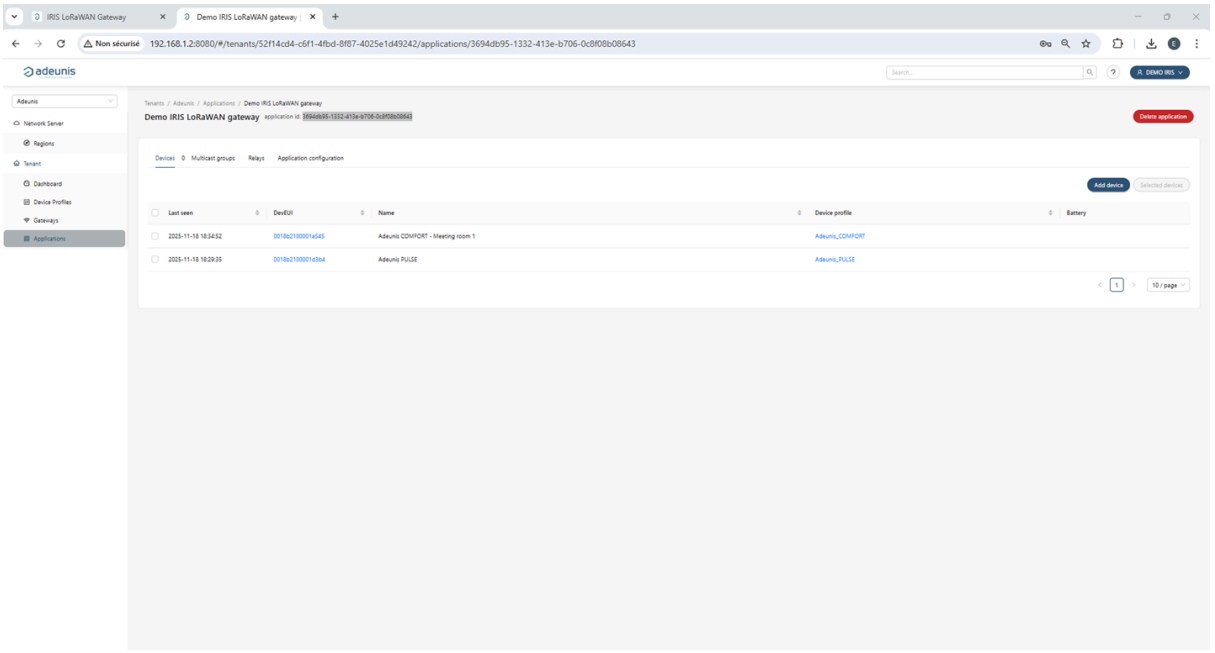
Upload your file in **Bulk Device Import**, review the preview, then choose: **SEND TO GATEWAY** to create listed devices.



5. **Validate**

Distributed by www.texim-europe.com

Open the LoRa Server dashboard and navigate to **Tenant** → **Applications** → **Devices** to confirm the batch created/updated the expected devices.



ANNEX 5 MAINTENANCE CHECKLIST

This checklist gives you a short, repeatable operations routine you run after maintenance windows or periodically to confirm the gateway is healthy and that the LoRaWAN data path (uplink and downlink) works as expected.

When to run it

- At the end of commissioning or a maintenance window.
- After a **firmware upgrade** or a **security/network change** (HTTPS, Authorized IPs, NTP, APN, VLAN).
- **Quarterly** as a preventive check on long-running sites.

Distributed by www.texim-europe.com

Item	Acceptance criteria	Result	Evidence
Status baseline	Uptime ↑, time correct, backhaul up, IP present, mode/band/EUI correct		Status screenshot
Security	GUI over **https** with lock/no warning; Authorized IPs restricted; CA roots present (WSS)		GUI screenshots (HTTP/HTTPS, Authorized IPs, CA page)
NTP	Servers reachable; timezone correct		NTP page + Status time
Cellular health	`AT+CSQ`, `AT+CEREG?`, `AT!GSTATUS? / AT!LTEINFO?` captured		AT console outputs
LNS connectivity	Gateway online (UDP PF) / Station connected (WSS) / Embedded LNS up		LNS/embedded console screenshot
Join flow	Join-request + Join-accept observed; device activated		LNS device event view
Uplink flow	Test uplink received; RSSI/SNR reasonable; decoder OK		LNS frame log
Downlink flow	Downlink transmitted; device receives (ACK for confirmed)		LNS downlink log / device indication
Logs	Syslog exported; no critical errors		Log file
Backup	Config exported (named, archived)		Config file
Autoreset	Policy matches site rules		screenshot / note
Reconnect	Reboot → PF/WSS session restores automatically		Short note / timestamp

This routine proves the **full path**: secure admin → time/right band → gateway ↔ LNS session → device join → uplink → downlink.

Distributed by www.texim-europe.com

ANNEX 6 TROUBLE SHOOTING MATRIX

Use this section to quickly diagnose common issues.

Each row lists the **symptom**, the **most likely causes**, **where to check in the UI**, **how to diagnose**, and the **fix**.

Gateway ↔ Embedded LNS connectivity

Symptom	Likely cause(s)	Where to check	How to diagnose	Fix
Gateway shows **Offline**	No power/WAN; UDP PF not reaching the embedded LNS (firewall/NAT); wrong **Gateway ID (EUI64)**	**Tenant** → **Gateways** list & the gateway **Dashboard**	Verify "Last seen"; confirm the PF endpoint (UDP/1700 default) and **Gateway ID** configured on the gateway	Restore WAN; open/forward UDP/1700 to the embedded LNS; correct the **Gateway ID (EUI64)**; ensure NTP time sync
Gateway **Online** but no uplinks	Region/plan mismatch between gateway and devices; antenna issue	**Gateways** → **[gateway]** → **LoRaWAN frames**	Look for incoming `rx` frames and frequencies; compare to device profile plan	Align region/plan (**EU868**); check antenna, placement, duty-cycle limits
TLS certificate tab unclear	Our implementation supports **UDP Packet Forwarder only**; **client-TLS is not supported**	**Gateways** → **[gateway]** → **TLS certificate**	—	Ignore the TLS tab for now; configure the gateway as **UDP PF** only. See **[Gateways (UDP Packet Forwarder)]**

Device registration & Join (OTAA/ABP)

Symptom	Likely cause(s)	Where to check	How to diagnose	Fix
Device never joins (OTAA)	**DevEUI / JoinEUI / AppKey** mismatch; device disabled; wrong **Device profile** region; OTAA nonces exhausted	**Applications → [app] → Devices → [device] → Configuration / OTAA keys / Events**	Look for `JoinRequest` / `JoinAccept` in **Events**; validate keys	Correct keys; ensure device is **Enabled**; pick **EU868** profile; **Flush OTAA device nonces**
Joins OK, no data afterwards	App sends on FPort=0; device is sleeping; codec not selected	**Device → Events / LoRaWAN frames / Measurements**	Check `UnconfirmedDataUp` and **FPort**; look for decoded fields	Use **FPort ≠ 0** for app payloads; wake device; assign the correct **Codec**
ABP downlink stopped (“frame-counter not valid”)	Counters out of sync	**Device → Activation**	Compare UL/DL counters	Re-activate with correct counters or (temporarily) **Disable frame-counter validation**, then restore. See **[Device details]**

Uplink visibility (data not appearing)

Symptom	Likely cause(s)	Where to check	How to diagnose	Fix
No uplinks visible in the app	Device registered in the wrong **Application**; wrong **Device profile**	**Applications → [app] → Devices** and the **Device → Frames**	Confirm the device appears in the intended app; watch live frames	Move the device to the correct application; set the correct profile
ADR unstable (very high/low DR)	ADR configuration misaligned	**Device profile → General**	Check ADR algorithm and allowed DR range	Adjust ADR settings; restrict DR range to EU868 DR0…DR5 as needed
Decoded fields missing	Codec not assigned / mapping incomplete	**Device → Measurements / Codec**	Raw payload is present but no decoded series	Assign the proper codec and verify field mapping

Downlinks (single device)

Symptom	Likely cause(s)	Where to check	How to diagnose	Fix
Enqueued but never delivered (Class A)	No subsequent uplink; queue expired before uplink; FPort=0	**Device → Queue / Events / Frames**	Check **Expires at** in Queue and if an uplink occurred afterwards	Trigger an uplink (button/reset/report); increase expiry; use **FPort ≠ 0**. See **[Downlink — single device]**
Delivered only via **RX2** (slower)	RX1 DR mapping not possible	**Device profile → General**	Compare UL DR vs RX1=DR-1 rules	Allow a DR window that enables RX1 or accept RX2 latency
Confirmed downlink repeats	No ACK; gateway duty-cycle	**Device → Events**	Repeated `ConfirmedDataDown`	Use **Unconfirmed** where acceptable; reduce frequency; ensure radio margin

Multicast downlinks

Symptom	Likely cause(s)	Where to check	How to diagnose	Fix
Multicast queue never delivers	Devices are Class A (immediate multicast requires **Class C**); device not in group; wrong group keys	**Application → Multicast groups** and **Device → Configuration**	Verify group membership, device class, and group keys	Use **Class C** devices for immediate delivery; add members; validate group root keys; see **[Downlink — multicast]**
Only some members receive	RF differences; mixed classes; duty-cycle	**LoRaWAN frames** per device	Compare RSSI/SNR and DR	Unify device class; choose DR suitable for the group; repeat with spacing

Applications, Device-profiles, Batch import

Symptom	Likely cause(s)	Where to check	How to diagnose	Fix
Bulk import fails / devices land in	Missing or wrong	**Tenant → Applications**	Validate CSV/JSON	Use the exact **applicationId** and

Distributed by www.texim-europe.com

Symptom	Likely cause(s)	Where to check	How to diagnose	Fix
wrong app	**applicationId**; profile name mismatch; bad keys	(copy **Application ID** from app header) and **Tenant → Device Profiles** (exact profile name)	headers and values	**profile name**; ensure **DevEUI/JoinEUI/AppKey** lengths/format. See **[Batch device import]**

Gateways (UDP Packet Forwarder)

Symptom	Likely cause(s)	Where to check	How to diagnose	Fix
PF gateway not visible	Not added in UI; wrong **Gateway ID (EUI64)**; UDP blocked	**Tenant → Gateways** (Add gateway)	Check PF config on the gateway: LNS IP, UDP/1700, and EUI	**Add gateway** with the exact EUI; open firewall/NAT; point PF to the embedded LNS
Online but no frames	Region/plan mismatch; antenna issue	**Gateways → [gateway] → LoRaWAN frames**	No `rx` for expected channels	Align region (**EU868**); verify antenna and placement. See **[Gateways (UDP Packet Forwarder)]**

MQTT / Integration (if enabled)

Symptom	Likely cause(s)	Where to check	How to diagnose	Fix
No messages at subscriber	Wrong broker URL/creds/topic; integration disabled	**Application → Configuration (integration)**	Review connection status and topic format	Fix broker settings and topic; confirm TLS if used; restart consumer
Payload looks base64/raw	Decoder not applied	**Device → LoRaWAN frames / Measurements**	Raw payload present but no decoded fields	Decode in your app or enable/assign the proper codec

Quality & RF

Distributed by www.texim-europe.com

Symptom	Likely cause(s)	Where to look (UI)	Diagnose	Fix
RSSI/SNR very low	Distance/obstacles; antenna	**Device → Dashboard → Link metrics**	RSSI < −120 dBm; SNR < −10 dB	Move device or gateway; external antenna; lower DR
High uplink loss	Interference; duty-cycle	**Gateway dashboard**	Gaps in rx	Spread reporting; check channels; ADR

Disclaimer

ALL PRODUCTS, PRODUCT SPECIFICATIONS AND DATA ARE SUBJECT TO CHANGE WITHOUT NOTICE TO IMPROVE RELIABILITY, FUNCTION OR DESIGN OR OTHERWISE.

Texim Europe B.V. its affiliates, agents, and employees, and all persons acting on its or their behalf (collectively, “Texim”), disclaim any and all liability for any errors, inaccuracies or incompleteness contained in any datasheet or in any other disclosure relating to any product.

Texim makes no warranty, representation or guarantee regarding the suitability of the products for any particular purpose or the continuing production of any product.

It is the customer’s responsibility to validate that a particular product with the properties described in the product specification is suitable for use in a particular application.

Parameters provided in datasheets and / or specifications may vary in different applications and performance may vary over time.

All operating parameters, including typical parameters, must be validated for each customer application by the customer’s technical experts.

Please contact us if you have any questions about the contents of the datasheet.

This may not be the latest version of the datasheet. Please check with us if a later version is available.

Texim Europe - contact details

Headquarters & Warehouse

Elektrostraat 17
NL-7483 PG Haaksbergen
The Netherlands

T: +31 (0)53 573 33 33
E: info@texim-europe.com
Homepage: www.texim-europe.com

The Netherlands

Elektrostraat 17
NL-7483 PG Haaksbergen

T: +31 (0)53 573 33 33
E: nl@texim-europe.com

Belgium

Zuiderlaan 14, box 10
B-1731 Zellik

T: +32 (0)2 462 01 00
E: belgium@texim-europe.com

UK & Ireland

St Mary's House, Church Lane
Carlton Le Moorland
Lincoln LN5 9HS

T: +44 (0)1522 789 555
E: uk@texim-europe.com

Germany

Bahnhofstrasse 92
D-25451 Quickborn

T: +49 (0)4106 627 07-0
E: germany@texim-europe.com

Germany

Martin-Kollar-Strasse 9
D-81829 München

T: +49 (0)89 436 086-0
E: muenchen@texim-europe.com

Austria

Martin-Kollar-Strasse 9
D-81829 München

T: +49 (0)89 436 086-0
E: austria@texim-europe.com

Nordic

Stockholmsgade 45
2100 Copenhagen

T: +45 88 20 26 30
E: nordic@texim-europe.com

Italy

Martin-Kollar-Strasse 9
D-81829 München

T: +49 (0)89 436 086-0
E: italy@texim-europe.com