



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

≡ Version document	V1.0
≡ Area	LoRaWAN EU863-870
⦿ Etat	En création
⦿ Produit/Service	IRIS
≡ Zone	LoRaWAN EU863-870

INFORMATIONS PRODUIT ET INFORMATIONS RÉGLEMENTAIRES



Ce guide utilisateur s'applique au produit suivant :

IRIS LoRaWAN Gateway

Référence: WG0610-A01-ADE

Version de l'application : V1.0.x

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

DOCUMENTATION GUIDE

PREAMBLE

[DISCLAIMER](#)

[TECHNICAL SUPPORT](#)

[RECOMMENDATIONS](#)

[INTRODUCTION](#)

DECLARATION DE CONFORMITE

[DECLARATION UE DE CONFORMITE - WG0610-A01_V3_WebdynEasy LoRaWAN - IRI S.pdf](#)

TABLE DES MATIERES

▼ TABLE DES MATIERES

[INFORMATIONS PRODUIT ET INFORMATIONS RÉGLEMENTAIRES](#)

[DECLARATION DE CONFORMITE](#)

[TABLE DES MATIERES](#)

[1. INTRODUCTION](#)

[1.1. Objectif, public visé et résultats attendus](#)

[1.2. Description générale de la passerelle IRIS](#)

[1.3. Principales fonctionnalités de la passerelle IRIS](#)

[1.4. Positionnement de la passerelle IRIS dans un réseau LoRaWAN](#)

[2. SPECIFICATIONS](#)

[2.1. Le boîtier](#)

[2.2. La carte électronique](#)

[2.3. Dimensions et poids](#)

[2.4. Spécifications techniques](#)

[2.4.1. Hardware](#)

[2.4.2. Software](#)

[3. DÉBALLAGE, INSTALLATION ET MISE EN SERVICE](#)

[3.1. Déballage](#)

[3.1.1. Contenu du colis](#)

[3.1.2. Etiquette d'identification](#)

[3.1.3. Version logicielle](#)

3.2. Assemblage	
3.2.1. Ouverture / fermeture du boîtier	
3.2.2. Antenne cellulaire et carte SIM	
3.2.3. Antenne LoRaWAN	
3.2.4. Fixation murale	
3.2.5. Power Supply	
3.3 Premier accès	
3.3.1. Mise sous tension de la passerelle	
3.3.2. Configuration d'une adresse IP statique temporaire	
3.3.3. Premier accès à la Web GUI	
3.3.4. Renforcement de la sécurité	
4. ACCÈS À LA PASSERELLE, CONNECTIVITÉ ET CONFIGURATION DE LA SÉCURITÉ	
4.1. Présentation de l'interface Web	
Home Page	
Section Cellulaire	
Section Ethernet	
Section Sécurité	
Section LoRaWAN	
Section Administration	
Maintenance Section	
4.2. Accès réseau	
4.2.1. Interface Ethernet	
4.2.2. Interface cellulaire	
4.2.3. Supervision de connectivité ("Keep Online")	
4.2.4. Synchronisation de l'heure	
4.2.5. Validation et transfert	
4.3. Sécurité (contrôle d'accès et confiance)	
4.3.1. Accès à l'interface Web	
4.3.2. Adresses IP autorisées (Mobile WAN allow-list)	
4.3.3. CA Certificates – ancres de confiance pour les services distants sécurisés (MQTTs/HTTPs/Basic Station WSS)	
4.3.4. Validation et transfert	
5. CONFIGURATION LoRaWAN & MISE EN SERVICE	
5.1. Modes de fonctionnement	
5.1.1. Packet Forwarder	
5.1.2. Serveur LoRaWAN embarqué (LNS)	
5.2. Sélectionner le mode de fonctionnement	
5.3. Définir la bande radio	
5.4. Paramètres du Packet Forwarder UDP	
5.4.1. Informations nécessaires côté LNS	
5.4.2. Configuration UDP	
5.4.3. Validation et transfert	
5.5. Paramètres Basic Station (WS/WSS)	
5.5.1. Informations nécessaires côté LNS	
5.5.2. Configuration de Basic Station	
5.5.3. Paramètres CUPS	
5.5.4. Validation et transfert	
5.6. Paramètres du serveur réseau LoRaWAN intégré (LNS)	

5.6.1. Activer le serveur LoRaWAN intégré	
5.6.2. Accéder au serveur LoRaWAN	
5.6.3. Tableau de bord du serveur LoRaWAN	
5.6.4. Gérer un parc de passerelles	
5.6.5. Gérer les applications	
5.6.6. Gérer les profils d'équipements (Device Profiles)	
5.6.7. Ajouter un capteur (Import unitaire et en masse)	
5.6.8. Visualiser les informations détaillées d'un équipement	
5.6.9. Downlinks (Vers un capteur & en Multicast)	
5.6.10. Validation	
6. Intégration applicative & routage des données (MQTT/s & HTTP/s)	
6.1. Intégration MQTT/MQTTs	
6.2. Intégration HTTP/HTTPs	
6.3. JSON Transformer	
7. VALIDATION & RECETTE DE SITE	
7.1. Statut & Identité	
7.2. Session Gateway ↔ LNS (selon le mode)	
7.3. Association (join) d'un équipement	
7.4. Uplink (RF vers application)	
7.5. Downlink (réseau vers équipement)	
8. EXPLOITATION ET MAINTENANCE	
8.1. Sauvegarde de configuration	
8.2. Logs et Diagnostics	
8.3. Mises à jour Firmware	
8.4. Autoreset	
8.5. AT Commands	
8.5.1. Utiliser la console de manière sûre	
8.5.2. Commandes d'aide IRIS (logiciel)	
8.5.3. Vérifications courantes du modem Sierra	
8.6. Reboot	
8.7. Validation & contrôles de routine	
8.7.1. Quand l'exécuter	
8.7.2. Procédure	
9. HISTORIQUE DU DOCUMENT	
ANNEXE 1 GLOSSAIRE & ACRONYMES	
ANNEXE 2 DEMARRAGE RAPIDE	
Prérequis	
Etapes	
ANNEXE 3 ENREGISTRER UN CAPTEUR ADEUNIS COMFORT	
Prérequis	
Etapes	
ANNEXE 4 ENREGISTRER UN LOT DE CAPTEURS (CSV/JSON)	
Prérequis	
Etapes	
ANNEXE 5 CHECKLIST DE MAINTENANCE	
ANNEXE 6 MATRICE DE DEPANNAGE	

1. INTRODUCTION

1.1. Objectif, public visé et résultats attendus

Ce guide utilisateur explique comment déployer la passerelle IRIS LoRaWAN, depuis le déballage jusqu'au premier uplink, puis comment l'exploiter et la maintenir en toute sécurité dans la durée. Il est recommandé d'être à l'aise avec les bases des réseaux IP (adresse IP statique vs DHCP, HTTPS, certificats TLS) ainsi qu'avec les fondamentaux de LoRaWAN (objets/capteurs, passerelles, serveur réseau, serveur applicatif).

À l'issue de la séquence « First Run », vous aurez :

- Établi la connectivité de backhaul (Ethernet ou cellulaire),
- Sécurisé l'accès à la passerelle,
- Choisi une méthode de transfert (Packet Forwarder via UDP ou Basics Station, ou Embedded LNS),
- Vérifié le premier join et le premier uplink.

1.2. Description générale de la passerelle IRIS

La **passerelle IRIS LoRaWAN** est une solution de nouvelle génération, haute performance, développée par Adeunis pour les **applications smart building** et les **réseaux IoT**.

Véritable passerelle entre les capteurs IoT terrain et les plateformes IT ou cloud, IRIS collecte efficacement les données de nombreux équipements et les transfère de manière sécurisée vers les serveurs réseau et les applications.



Que vous l'intégriez à un réseau LoRaWAN existant ou que vous l'utilisiez pour en déployer un nouveau, la passerelle IRIS offre une grande flexibilité et une excellente évolutivité.

La passerelle prend en charge **deux modes de fonctionnement** pour le transfert des données vers un serveur réseau LoRaWAN (LNS) :

- **Packet Forwarder,**
- **Serveur LoRaWAN intégré.**

Ces deux modes permettent d'adapter l'intégration de la passerelle à différentes architectures LoRaWAN et à divers besoins de déploiement.

En **mode Packet Forwarder**, la passerelle IRIS transfère les données LoRaWAN vers un **serveur réseau LoRaWAN (LNS) externe**.

Dans ce mode, elle joue le rôle de pont entre les objets LoRaWAN et le LNS, assurant une transmission fluide des données sans traitement local complexe.

IRIS s'intègre nativement avec les principaux serveurs réseau LoRaWAN tiers tels que **Actility, Lorient et The Things Stack**, garantissant une transmission fiable des données sur ces différents environnements.

En **mode serveur LoRaWAN intégré**, la passerelle IRIS fonctionne de manière autonome et fournit un **serveur réseau LoRaWAN local**, capable d'assurer le routage des données, les fonctions réseau et la gestion des endpoints, y compris le **décodage des payloads** et la prise en charge des fonctions de downlink multicast.

Ce mode convient particulièrement aux utilisateurs souhaitant garder la maîtrise complète de leur réseau LoRaWAN et privilégier une solution autonome.

La passerelle IRIS est un composant clé pour intégrer des capteurs IoT dans de nombreux cas d'usage, notamment la gestion énergétique, le suivi environnemental et la maintenance

prédictive.

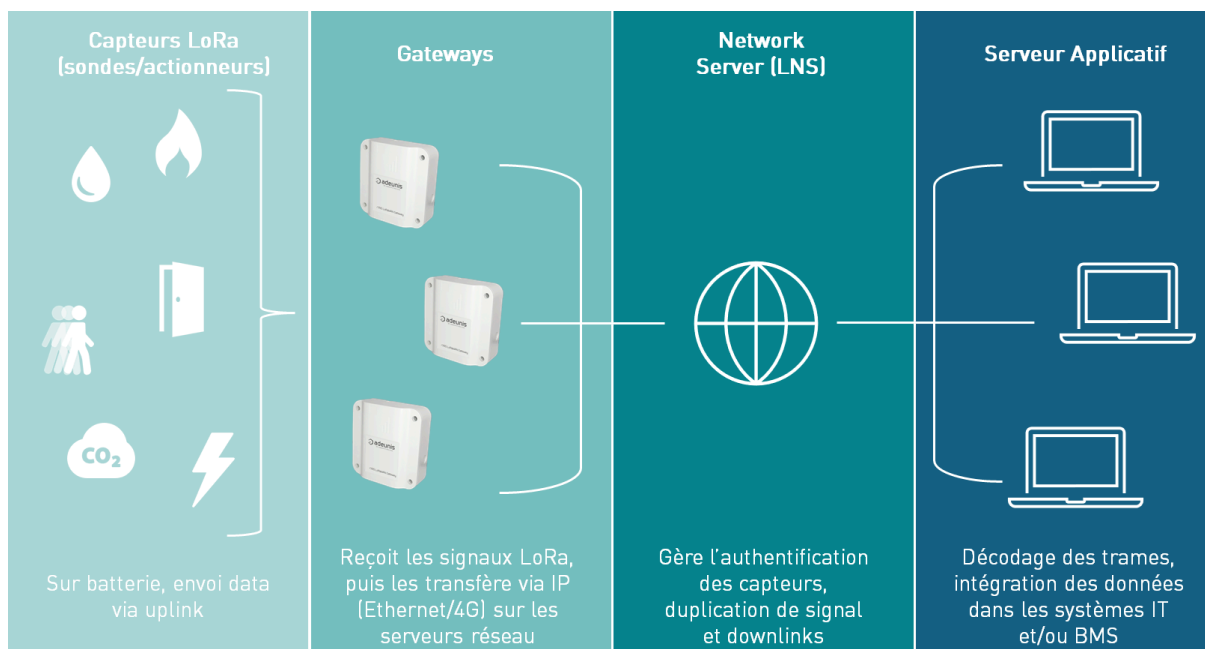
En combinant un positionnement économique avec des performances de niveau opérateur, IRIS propose une valeur particulièrement attractive : une connectivité à coût maîtrisé sans compromis sur la couverture ni sur la fiabilité.

1.3. Principales fonctionnalités de la passerelle IRIS

- **Options de connectivité multiples** : IRIS prend en charge la connectivité Ethernet ainsi que la connectivité cellulaire 2G/3G/4G, garantissant une connectivité fiable et redondante pour les applications critiques. Qu'elle soit raccordée via un câble Ethernet fixe ou via un réseau cellulaire, la passerelle assure une continuité de service.
- **Codecs Manager intégré** : la passerelle IRIS intègre un gestionnaire de codecs, compatible avec des décodeurs de payloads JavaScript préconfigurés ou personnalisés, afin de simplifier l'intégration des données pour différents capteurs IoT.
- **Évolutivité et flexibilité** : capable de supporter plus de 1 000 endpoints LoRaWAN, la passerelle IRIS convient aux déploiements IoT à grande échelle. Son architecture flexible permet soit de transférer les données vers n'importe quel serveur réseau LoRaWAN, soit d'exécuter un réseau privé en local.
- **Conception robuste** : grâce à un boîtier certifié IP67, la passerelle IRIS est conçue pour une fiabilité long terme, en environnements intérieurs comme en extérieur abrité, avec des performances optimales même en conditions difficiles.
- **Sécurité et fiabilité** : IRIS intègre des mécanismes de sécurité renforcés, notamment **TLS 1.2** et l'**authentification mutuelle**, afin de sécuriser les transmissions et d'empêcher les accès non autorisés. Elle propose également une fonction de **réinitialisation automatique périodique**, pour garantir un fonctionnement fiable en permanence.
- **Made in France** : produit fabriqué en France.

1.4. Positionnement de la passerelle IRIS dans un réseau LoRaWAN

Un réseau LoRaWAN repose sur une architecture en couches, conçue pour assurer une communication sécurisée et fiable entre les objets IoT et les systèmes backend.



- **Objets (capteurs/actionneurs)** : ce sont des équipements généralement alimentés sur batterie (capteurs de température, d'humidité, de mouvement, etc.) qui transmettent des données en uplink vers le réseau. Ils communiquent en LoRa, un protocole radio longue portée et basse consommation.
- **Passerelles** : elles reçoivent les trames LoRa par voie hertzienne et les transfèrent sur IP (Ethernet ou cellulaire) vers le serveur réseau LoRaWAN (LNS). IRIS se situe à ce niveau et prend en charge Packet Forwarder en implémentation UDP ou Basics Station (WSS). En alternative, elle peut héberger un **LNS intégré** pour la gestion locale des équipements.
- **Serveur réseau (LNS)** : il authentifie les objets, déduplique les paquets reçus via plusieurs passerelles, gère l'ADR et la planification des downlinks, et applique le comportement MAC LoRaWAN. Il agit comme un point central garantissant l'intégrité et la sécurité des données.
- **Serveur applicatif (Application Server)** : dernière étape de la chaîne de communication, où les données des objets IoT sont exploitées. Le serveur decode les payloads transmis par le serveur réseau et intègre les données aux systèmes IT du client / à la GTB (Building Management Systems) pour la visualisation, les alertes ou le pilotage.

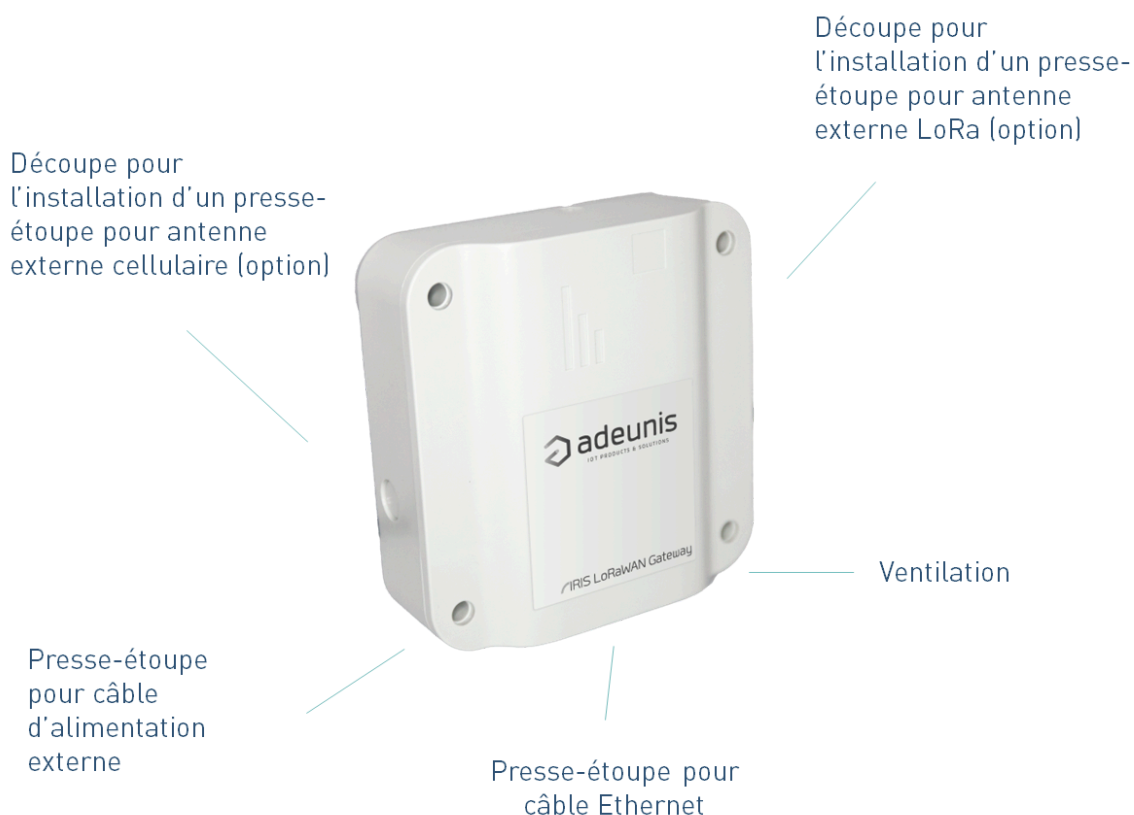
Cette architecture apporte flexibilité, évolutivité et sécurité des échanges, et convient à un large éventail d'applications IoT.

2. SPECIFICATIONS

Le boîtier compact et robuste protège l'électronique radio et réseau, tout en offrant des entrées de câbles pour l'alimentation et la connectivité amont. Un port RJ-45 fournit une interface Ethernet 10/100Base-T. L'alimentation est assurée via l'entrée DC dédiée. Un emplacement SIM est disponible à l'intérieur du boîtier pour la connectivité cellulaire. Le sous-système radio comprend une antenne LoRa interne ; une option d'antenne externe peut être utilisée lorsque cela est autorisé et pertinent pour améliorer la couverture.

2.1. Le boîtier

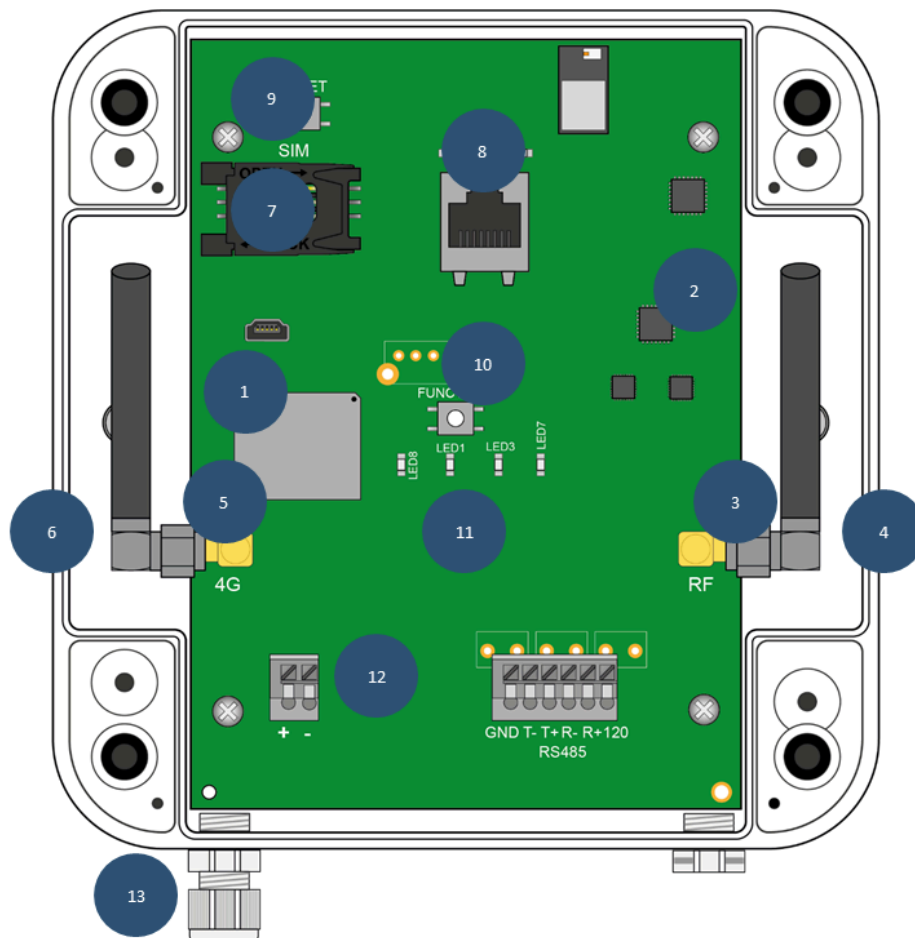
La **passerelle IRIS LoRaWAN** dispose d'un boîtier blanc certifié IP67, conçu pour garantir une fiabilité long terme en environnements intérieurs comme extérieurs.



Caractéristiques physiques	
Boîtier	IP67

Caractéristiques physiques	
Matériau & couleur	PC V0, blanc
Installation	Montage mural, sur bureau, sur rail DIN
Conditions de fonctionnement	
Température de fonctionnement	-20°C / +55°C
Température de stockage	-20°C / +70°C
Humidité relative	25% / 75% HR

2.2. La carte électronique



- | | |
|--|---|
| 1. Module IoT : Sierra Wireless WP7607-1 | 7. Support de carte SIM |
| 2. Concentrateur: SEMTECH SX1302 | 8. Port WAN RJ45 (PoE non pris en charge) |
| 3. Antenne LoRaWAN SMA interne | 9. Bouton Reset |

- 4. Sortie boîtier pour antenne radio LoRa RF 10. Bouton Function externe (option)
- 5. Antenne SMA 2G/3G/4G interne
- 6. Sortie boîtier pour antenne externe du modem 2G/3G/4G (option)
- 11. Voyants LED (alimentation, retour usine)
- 12. Bornier pour alimentation externe 12/24V
- 13. Sortie boîtier pour alimentation externe

2.3. Dimensions et poids



Caractéristiques physiques	
Dimensions	160 × 150 × 55mm
Poids	450gr

2.4. Spécifications techniques

2.4.1. Hardware

Hardware	
Module IoT	Sierra Wireless WP7607-1
Mémoire	150 MB DDR2 RAM
Flash	150 MB NAND
Interface LoRaWAN	
Concentrateur	SEMTECH SX1302
Canaux	8 (Half-Duplex)
Antenne	1x antenne LoRa interne, sortie boîtier pour antenne externe (option)
Bande de fréquences	EU 868
Sensibilité	-141dBm (125kHz en SF12)
Puissance TX	+14dBm max.
Protocole	1.0.x et 1.1.x
Classes supportées	Class A/C
Interface Ethernet	
Port	1x port WAN RJ-45 (PoE non pris en charge)
Couche physique	10/100 Base-T (IEEE 802.3)
Débit	10/100Mbps (auto-sensing)
Interface	Auto MDI/MDIX
Mode	Full ou Half duplex (auto-sensing)
Interface cellulaire	
Module IoT	Sierra Wireless WP7607-1
Réseau	2G/3G/4G LTE
Bandes 3G	HSPA+, UMTS (B1, B8)
Bandes 4G	Cat-1 (B1, B3, B7, B8, B20, B28)
Puissance TX	23 dBm
Antenne	1x antenne interne 2G/3G/4G, sortie boîtier pour antenne externe (option)
Emplacement SIM	1x mini SIM-2FF interne
Alimentation	
Entrée d'alimentation	12/24V DC via une alimentation externe

Boutons	
Bouton Reset	Redémarrage de la passerelle (hard reset)
Bouton Function	Retour configuration usine Procédure : - Déconnecter la passerelle de l'alimentation principale, - Appuyer et maintenir le bouton enfoncé,- - Reconnecter la passerelle à l'alimentation principale en maintenant le bouton enfoncé, - Attendre environ 1 minute (jusqu'à ce que les LED commencent à clignoter), - Relâcher le bouton, - L'équipement redémarre et les LED cessent de clignoter.
LEDs	
LED #8	S'allume lorsque la passerelle est alimentée
LED #1	Clignote lorsque la passerelle démarre une procédure de retour usine et continue de clignoter pendant toute la durée du processus
LED #3	Clignote lorsque la passerelle démarre une procédure de retour usine et continue de clignoter pendant toute la durée du processus

2.4.2. Software

LoRaWAN	
LoRaWAN	Spécification LoRaWAN 1.0.x et 1.1.x LoRaWAN Packet forwarder Serveur réseau LoRaWAN Nombre max. d'endpoints supportés : environ 1 000 (selon les fréquences UL/DL) Prise en charge des endpoints Class A/C
Packet Forwarder	
Type	Semtech UDP forwarder LoRa Basics Station TCP forwarder
Compatibilité	Intégration transparente avec les principaux LNS tiers : Actility, Loriot, The Things Stack, Chirpstack, etc.
Serveur LoRaWAN intégré	
Provisioning	Déclaration unitaire, import en masse des endpoints LoRaWAN pour un déploiement

LoRaWAN	
	simplifié
Configuration	Configuration à distance des endpoints LoRaWAN via downlink Prise en charge du downlink multicast
Décodage des données	Bibliothèque de décodeurs Adeunis intégrée Prise en charge de décodeurs personnalisés (JavaScript)
Parc de passerelles	Peut fonctionner comme serveur réseau avec plusieurs passerelles Packet Forwarding connectées (protocole UDP)
Intégration	Protocoles MQTT/s, HTTP/s pour le transfert de données vers le serveur applicatif
Réseau	
Configuration	Prend en charge les communications 2G/3G/4G avec attribution d'une IP mobile WAN Sélection du réseau (options) Affichage de l'état du réseau APN configurable Fonction "keep-alive"
Protocoles	Packet forwarder : UDP, WS, WSS Serveur réseau : MQTT/s, HTTP/s Serveur web : HTTP/s Synchronisation de l'horloge : NTP Autres : DHCP, DNS, ARP
Sécurité & pare-feu	
TLS	1.2, authentification mutuelle
Contrôle d'accès	Pour l'accès local/distant au Web GUI
Pare-feu	Contrôle d'accès, filtrage (IP)
Certificat	Gestion des certificats racines CA
Fiabilité	
Autoreset	Autoreset périodique configurable
Diagnostics	Serveur de logs
Gestion de l'équipement	
Configuration	Mise à jour, sauvegarde, restauration, récupération de la configuration via le Web GUI
Mise à jour firmware	via le Web GUI
Retour usine	via le Web GUI ou via le bouton Reset

Certifications	
Certifications	CE, RED, RoHS, REACH

3. DÉBALLAGE, INSTALLATION ET MISE EN SERVICE

Commencez par vérifier le contenu du colis par rapport à la liste de colisage, puis inspectez le boîtier afin de détecter d'éventuels dommages liés au transport.

Choisissez un emplacement de montage offrant un chemin RF dégagé. La passerelle peut être fixée au mur ou installée sur rail DIN à l'aide d'un kit optionnel. Veillez à maintenir l'antenne LoRa aussi dégagée que possible des obstacles métalliques et éloignée des faisceaux de câbles denses. Faites passer les câbles d'alimentation et Ethernet, puis serrez les presse-étoupes afin de préserver l'étanchéité IP.

Raccordez l'alimentation DC. Si vous utilisez une connectivité cellulaire, insérez la carte SIM avec précaution (contacts orientés comme indiqué) lorsque l'équipement est hors tension.

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

3.1. Déballage

3.1.1. Contenu du colis

Avant de commencer toute installation, vérifiez le contenu du colis. En cas d'élément manquant ou endommagé, contactez le support Adeunis.

L'emballage carton contient les éléments suivants :



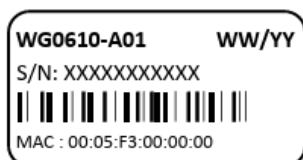
- Passerelle IRIS
- Antenne SMA coudée pour le modem (interne)
- Antenne SMA coudée pour la radio (interne)
- Adaptateur secteur
- Connecteur de câble Ethernet

Les accessoires suivants peuvent être fournis en option :

- Antenne externe pour le modem
- Antenne magnétique externe pour la radio
- Antenne externe "cierge" pour la radio
- Kit de montage sur rail DIN

3.1.2. Etiquette d'identification

La passerelle peut être identifiée à l'aide de son étiquette d'identification située sur la boîte.



Cette étiquette indique :

- Le nom de l'équipement
- La date de fabrication (format WW/YY)
- Le numéro de série au format alphanumérique et code-barres 128
- L'adresse MAC (Ethernet) au format alphanumérique

3.1.3. Version logicielle

La version logicielle est disponible dans la **Web GUI** de la passerelle. Elle est indiquée dans l'onglet "Status".

3.2. Assemblage

Avant l'installation, il est important de respecter les conditions de fonctionnement décrites dans ce manuel, ainsi que les points suivants :

- Protéger le produit de la poussière, de l'humidité, des substances agressives et de la corrosion.
- Si la connexion modem est utilisée, s'assurer d'une réception optimale lors de l'installation. Vérifier le RSRP disponible dans la Web GUI, onglet "Status".
- Pour optimiser la sensibilité de réception du modem et de la radio LoRa, il est essentiel de laisser un espace libre de 20 cm autour des antennes.

3.2.1. Ouverture / fermeture du boîtier

Pour ouvrir le boîtier de la passerelle

Si le boîtier est fixé au mur :

1. Ouvrir les 2 trappes en face avant.
2. Dévisser les 4 vis de fixation murale situées dans les logements sous les trappes.

Puis suivre ces étapes :

3. Dévisser les 4 vis à l'arrière du boîtier.
4. Retirer le couvercle.
- 5.

Pour refermer le boîtier de la passerelle

1. Positionner le couvercle sur la base du boîtier et s'assurer que le joint est correctement en place.
2. Revisser les 4 vis à l'arrière du boîtier.

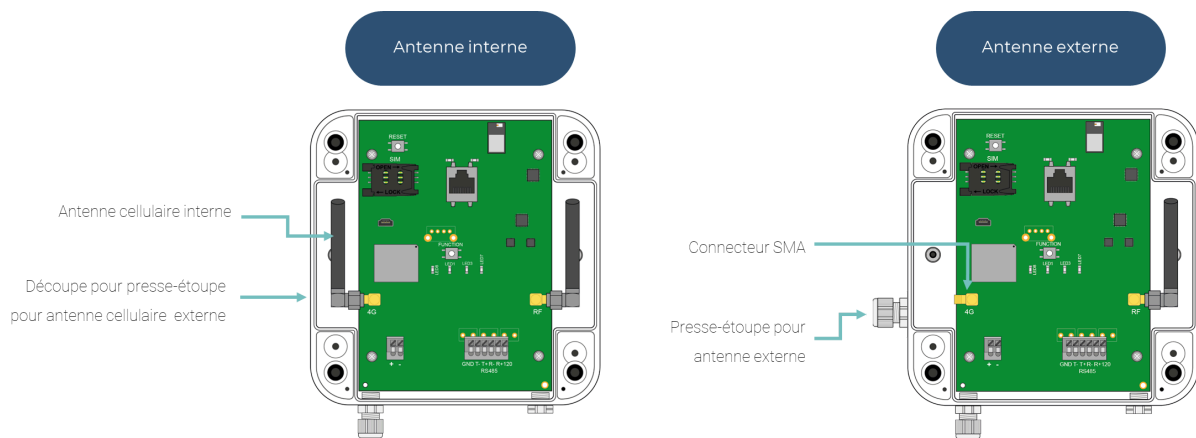
3.2.2. Antenne cellulaire et carte SIM

Raccordement de l'antenne cellulaire

La passerelle dispose d'un connecteur SMA femelle repéré "4G" sur la carte, destiné au raccordement de l'antenne modem.

La passerelle est livrée avec une antenne interne.

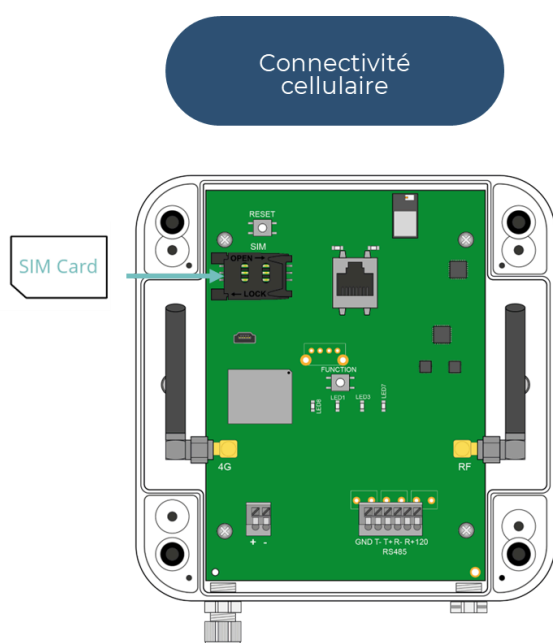
Une antenne externe peut être raccordée à la passerelle. Pour cela, dévisser le bouchon sur le boîtier et installer un presse-étoupe M16*1.5 (non fourni).



Si la passerelle est installée dans un coffret métallique ou dans un emplacement ne permettant pas une bonne réception du signal, l'utilisation d'une antenne déportée est fortement recommandée. Veillez à utiliser une antenne compatible avec le connecteur et les fréquences utilisées.

Insertion de la carte SIM

Pour utiliser la connexion modem afin de communiquer avec le serveur distant, le boîtier doit être ouvert et une carte mini SIM insérée dans le support SIM de la carte électronique (PCB).



Pour insérer la carte SIM dans le produit :

1. Faire coulisser le clapet du support vers la droite (direction OPEN).
2. Glisser la carte SIM dans le clapet.
3. Refermer le clapet en le faisant coulisser vers la gauche (direction LOCK).

Par défaut, la configuration de la passerelle ne demande pas de code PIN.

Si vous souhaitez activer le code PIN, il est préférable de le configurer via la Web GUI avant d'installer la carte SIM.

Trois cas sont possibles :

- Le code PIN est désactivé : la communication modem est active.
- Le code PIN est activé et le code saisi est correct : la communication modem est active.
- Le code PIN est activé et le code saisi est incorrect : la communication modem est en erreur.



Si la carte SIM a un code PIN activé et que celui-ci est incorrect au premier démarrage de la passerelle, la carte sera bloquée après 3 tentatives. Elle peut être débloquée à l'aide d'un téléphone mobile, via le code PUK fourni par l'opérateur.

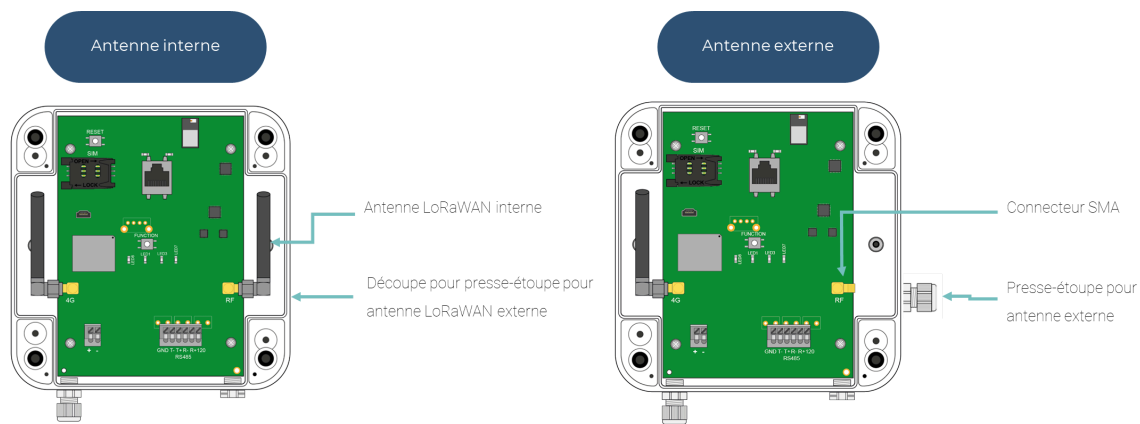
3.2.3. Antenne LoRaWAN

Raccordement de l'antenne LoRaWAN

La passerelle dispose d'un connecteur SMA femelle repéré "RF" sur la carte, destiné au raccordement de l'antenne radio.

La passerelle est livrée avec une antenne interne.

Une antenne externe peut être raccordée à la passerelle. Pour cela, dévisser le bouchon sur le boîtier et installer un presse-étoupe M16*1.5 (non fourni).



Si la passerelle est installée dans un coffret métallique ou dans un emplacement ne permettant pas une bonne réception du signal, l'utilisation d'une antenne déportée est fortement recommandée. Veillez à utiliser une antenne compatible avec le connecteur et les fréquences utilisées.

3.2.4. Fixation murale

La passerelle IRIS peut être fixée au mur. Avant la fixation murale, refermez d'abord le boîtier.

Choisissez un emplacement offrant un chemin RF dégagé. Pour optimiser la portée radio, il est important d'installer l'antenne radio le plus haut possible et de la positionner avec soin, en évitant autant que possible les obstacles. En priorité, éloignez-la de tout obstacle métallique (armoire, poutres, etc.) ou en béton (béton armé, murs, etc.), car ces matériaux atténuent fortement les ondes radio.

Suivre les étapes ci-dessous pour fixer la passerelle au mur

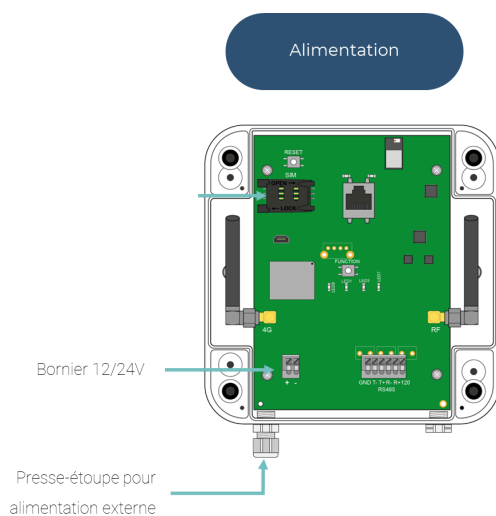
1. Ouvrir les 2 trappes en face avant.
2. Visser les 4 vis de fixation murale dans les logements sous les trappes.
3. Refermer les deux trappes en face avant.



Les vis et chevilles ne sont pas fournies.

Vous devez choisir des vis adaptées au type de mur sur lequel la passerelle est fixée (vis de 4 mm de diamètre, longueur minimale 25 mm).

3.2.5. Power Supply



La passerelle IRIS doit être alimentée en 12 V ou 24 V DC.

L'alimentation est raccordée sur le bornier J11, situé en bas à gauche de la carte.

Vérifiez que les fils d'alimentation sont connectés aux bonnes bornes.

La consommation du produit varie selon sa configuration. Assurez-vous que l'alimentation utilisée peut fournir une puissance minimale de 10 W.



Les utilisateurs finaux doivent utiliser une alimentation certifiée CE, d'une puissance inférieure à 15 W.

La distance entre l'alimentation et le produit ne doit pas dépasser 3 mètres.

3.3 Premier accès

Cette section explique comment alimenter la passerelle, configurer une adresse IP statique temporaire sur votre ordinateur, puis accéder à la Web GUI pour la première fois. Suivez les étapes dans l'ordre.

3.3.1. Mise sous tension de la passerelle

1. **Antennes.** Vérifiez que les antennes **LoRa** et (le cas échéant) **cellulaire** sont connectées. Pour les radios, connectez toujours les antennes **avant** la mise sous tension.
2. **SIM (optionnel).** Si vous prévoyez d'utiliser la connectivité cellulaire, insérez la carte SIM lorsque l'équipement est hors tension.
3. **Ordinateur.** Assurez-vous qu'un ordinateur équipé d'un navigateur web est connecté au port Ethernet de la passerelle.

4. **Alimentation.** Raccordez le câble d'alimentation DC de la passerelle à une alimentation externe adaptée et mettez sous tension.

Vous pouvez maintenant configurer l'accès à la Web GUI

3.3.2. Configuration d'une adresse IP statique temporaire

Vous devez configurer une adresse IP statique temporaire sur votre ordinateur, dans le même sous-réseau que la passerelle.



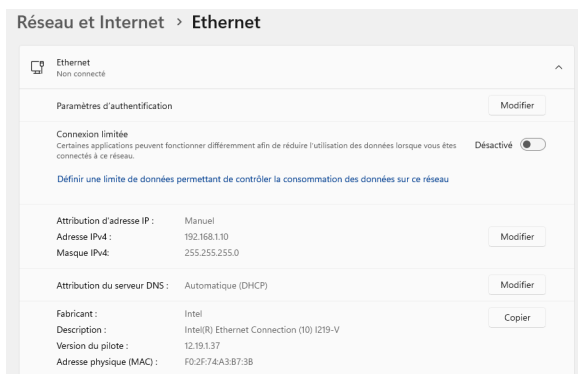
Les paramètres de configuration par défaut de la passerelle IRIS sont les suivants :

Adresse IP `192.168.1.2`

Masque de sous-réseau `255.255.255.0`

DHCP Désactivé

Pour configurer une adresse IP statique temporaire :



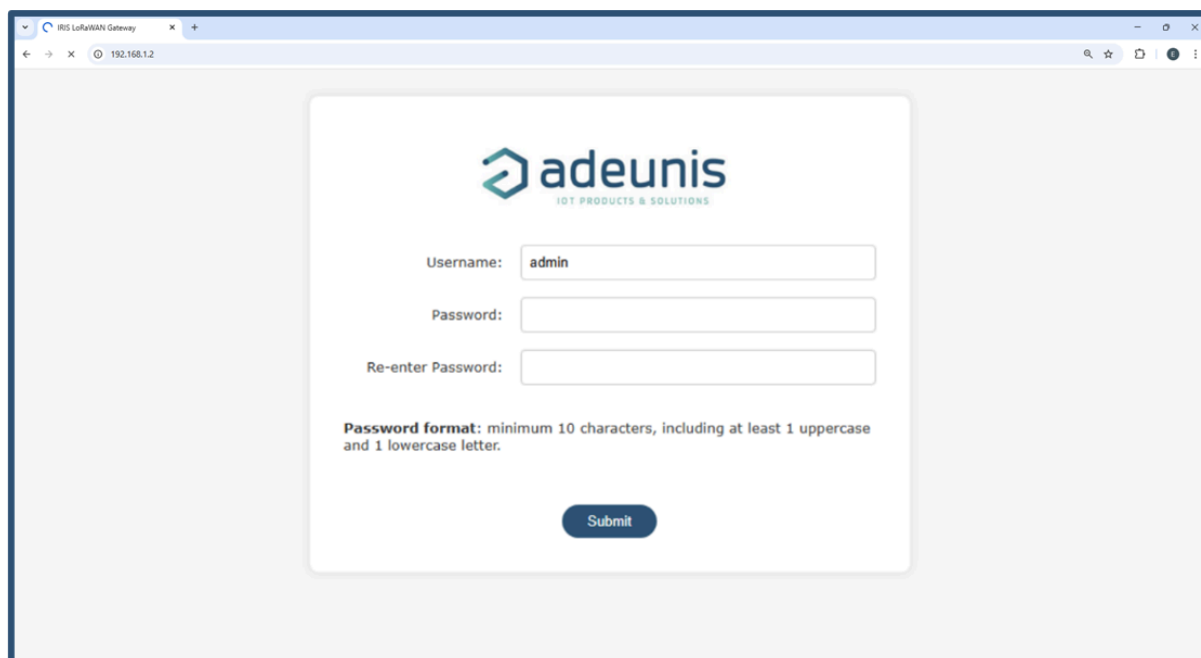
1. Aller dans "Réseau et Internet". La fenêtre "Status réseau" s'affiche.
2. Cliquer sur "Ethernet".
3. La fenêtre "Ethernet Status" s'affiche.
4. Cliquer sur le bouton "Modifier" du paramètre "Attribution d'adresse IP"
5. Sélectionner le mode d'attribution "Manuel" et activer "IPv4"
6. Dans la zone "Adresse IP", saisir l'adresse IP `192.168.1.xxx` (xxx compris entre 1 et 254, et différent de 2) et le masque `255.255.255.0`.
7. Enregistrer les modifications.
8. Fermer la fenêtre de connexion réseau et d'accès à distance.
9. Après la mise en service, penser à repasser en mode DHCP.

Il est désormais possible de modifier facilement la configuration de la passerelle via la Web GUI.

3.3.3. Premier accès à la Web GUI

Pour accéder à l'interface web intégrée de la passerelle :

1. Connecter votre ordinateur au port Ethernet de la passerelle.
2. Ouvrir le navigateur web et se rendre sur : `http://192.168.1.2`
3. Une fenêtre d'identification doit s'afficher.
4. Configurer votre **password** afin de sécuriser l'accès à la Web GUI.
5. Cliquer sur "**Submit**".



The screenshot shows a web browser window with the address bar displaying '192.168.1.2'. The page content features the Adeunis logo at the top, followed by a login form. The form includes three input fields: 'Username:' with 'admin' entered, 'Password:', and 'Re-enter Password:'. Below the fields is a note: 'Password format: minimum 10 characters, including at least 1 uppercase and 1 lowercase letter.' At the bottom of the form is a blue 'Submit' button.



La passerelle ne prend actuellement **pas** en charge plusieurs rôles utilisateurs : l'accès se fait via le compte admin.

3.3.4. Renforcement de la sécurité

Lors du premier accès à la passerelle, nous recommandons de configurer la sécurité et l'heure. Réaliser ces réglages dès le départ permet d'éviter la plupart des problèmes de connexion et de TLS par la suite.

1. **Activer HTTPS and désactiver HTTP**. Forcer un accès chiffré à la Web GUI.

2. **Configurer Serveur NTP et fuseau horaire.** Configurez votre serveur NTP privé/de référence, ou utilisez un service public reconnu, par exemple : `europa.pool.ntp.org` , `pool.ntp.org` , `time.google.com` OU `time1.google.com` .
3. (Optionnel) **Limiter l'exposition.** Si la Web GUI doit être accessible via un réseau routé, ajouter des adresses IP sources en liste d'autorisation.

Après enregistrement, rafraîchir le navigateur en HTTPS et aller sur la page **"Status"**. Vérifier que l'heure est correcte et que le lien Ethernet est opérationnel.

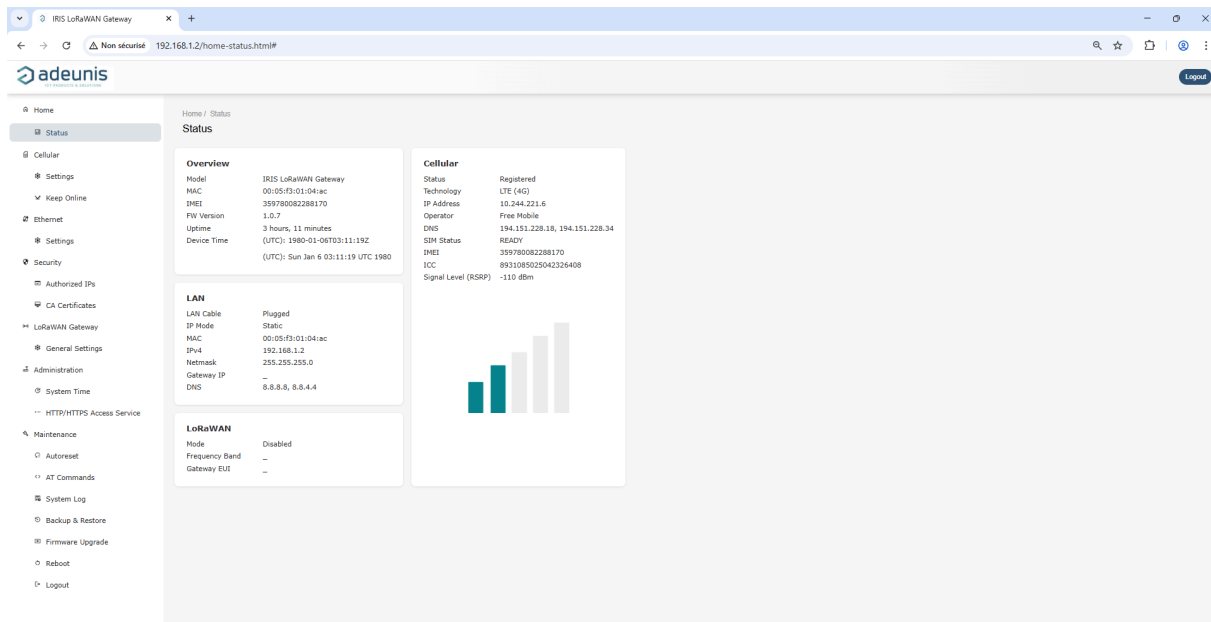
Vous pouvez maintenant poursuivre la configuration de la passerelle et les paramètres LoRaWAN.

4. ACCÈS À LA PASSERELLE, CONNECTIVITÉ ET CONFIGURATION DE LA SÉCURITÉ

4.1. Présentation de l'interface Web

Après votre première connexion, prenez un moment pour vous familiariser avec la Web GUI.

L'interface est organisée autour d'un menu de navigation à gauche, d'un fil d'Ariane en haut indiquant votre position actuelle, et d'une zone de contenu principale à droite.



Home Page

La page d'accueil est **Home** → **Status**.

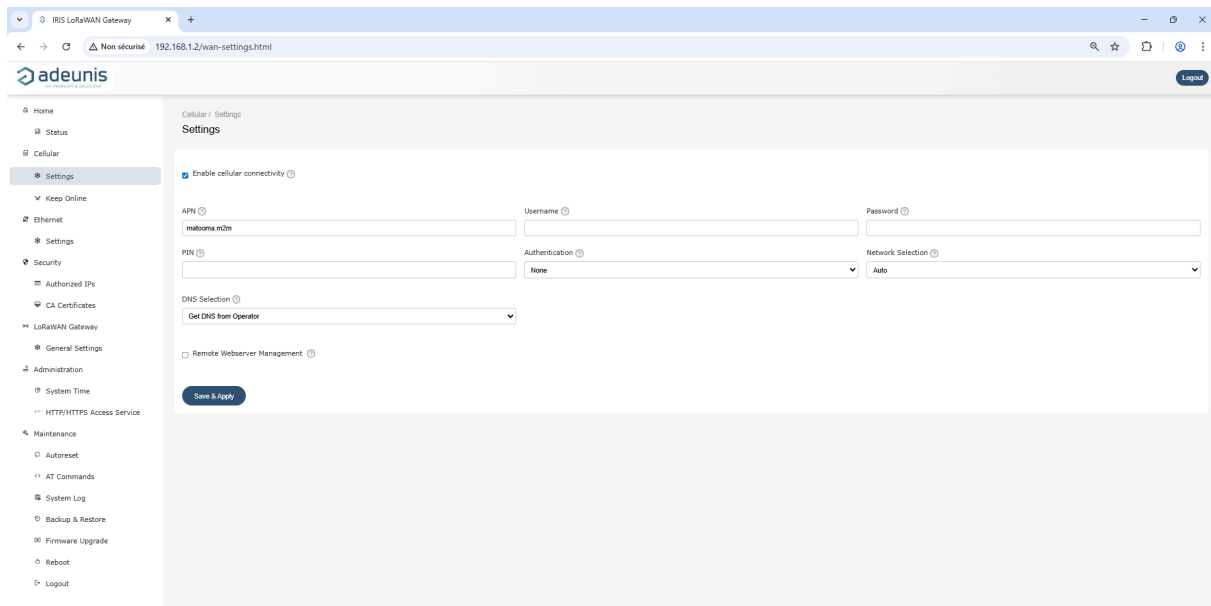
Elle sert de tableau de bord : vous y trouverez une carte Overview (modèle, MAC/IMEI, version firmware, uptime et heure de l'équipement), une carte LAN résumant l'état du lien filaire et les paramètres IPv4, une carte Cellular indiquant l'état d'enregistrement, la technologie radio, l'adresse IP, l'opérateur, l'état de la SIM et le RSRP, ainsi qu'une carte LoRaWAN indiquant le mode actif, la bande de fréquences et l'EUI de la passerelle.

Cette page est volontairement en lecture seule : c'est le moyen le plus rapide de vérifier que l'alimentation, l'heure et au moins une connectivité amont sont opérationnelles avant de poursuivre.

La navigation est regroupée par fonction.

Section Cellulaire

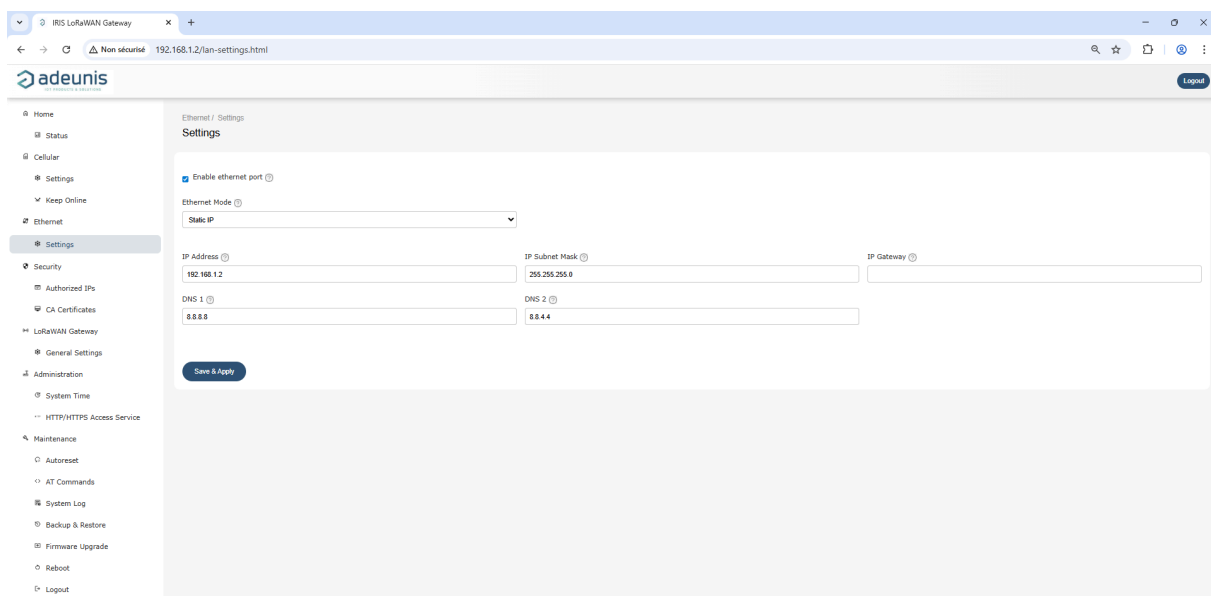
La section "**Cellular**" regroupe la configuration de la connectivité cellulaire. Ouvrez "**Settings**" pour saisir les paramètres APN et choisir les options de sélection réseau ; utilisez "**Keep Online**" pour configurer le mécanisme de supervision de connectivité, qui ping périodiquement une cible et rétablit le lien actif s'il devient non réactif.



Pour configurer cette interface, reportez-vous à la section Paramètres de la connectivité cellulaire de ce Guide Utilisateur.

Section Ethernet

La section “**Ethernet**” vous permet d’activer DHCP ou de définir une adresse statique, et permet de renseigner la passerelle par défaut ainsi que les serveurs DNS. Une fois les paramètres appliqués, reconnectez-vous à la Web GUI via la nouvelle adresse, puis confirmez les valeurs sur la page Status.

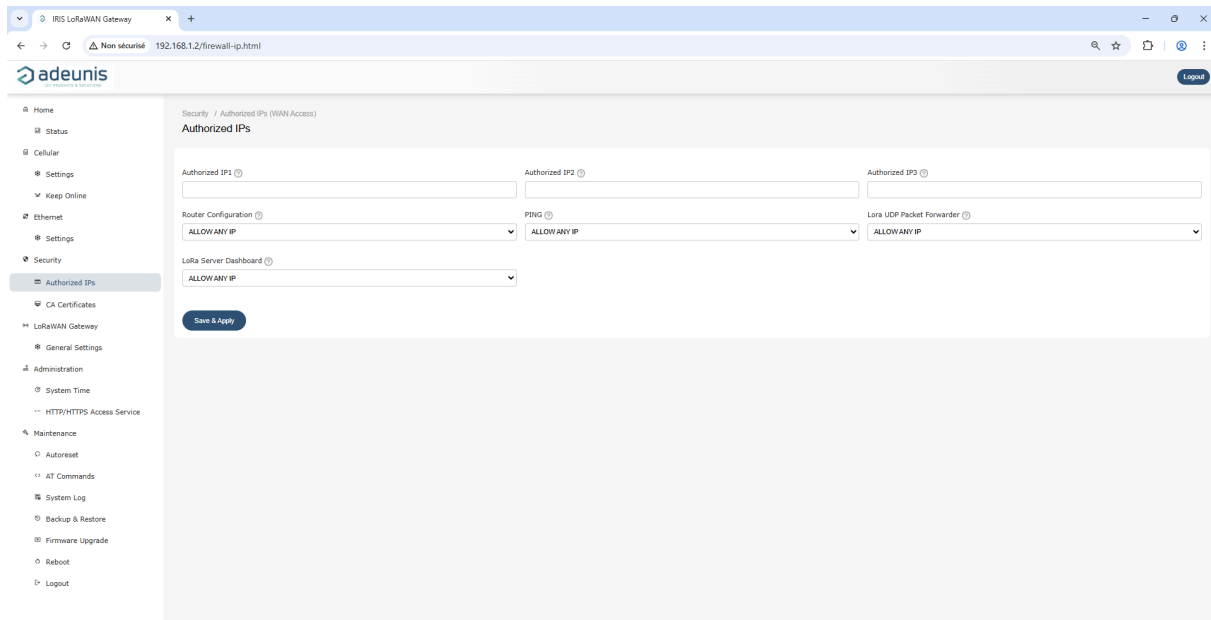


Pour configurer cette interface, reportez-vous à la section Paramètres de la connectivité Ethernet de ce Guide Utilisateur.

Section Sécurité

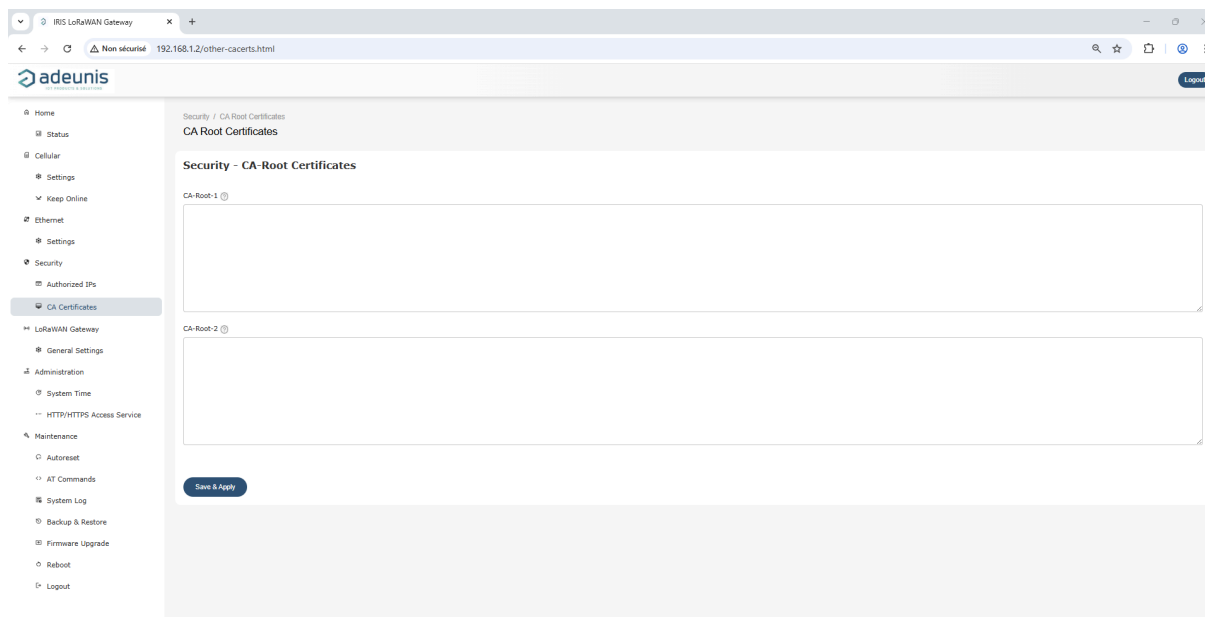
Les réglages liés à la sécurité sont regroupés sous **"Security"**.

"Authorized IPs" permet de restreindre les adresses sources autorisées à accéder aux services d'administration, ce qui est particulièrement important lorsque l'interface web est accessible au-delà d'un ordinateur connecté localement lors la mise en service de la passerelle.



Pour configurer la liste d'autorisation de l'accès WAN mobile, reportez-vous à la section [IPs autorisés](#) de ce Guide Utilisateur.

"CA Certificates" correspond au référentiel des certificats racines (CA) utilisé par la passerelle lorsqu'elle doit valider des serveurs TLS distants ; renseignez-le notamment si votre serveur réseau LoRaWAN, votre broker MQTT ou votre serveur HTTP sont signés par une autorité de certification privée ou d'entreprise.



Pour configurer, reportez-vous à la section CA Certificates du Guide Utilisateur.

Section LoRaWAN

Les fonctions LoRaWAN sont regroupées sous **“LoRaWAN”**.

Dans **“General Settings”**, vous choisissez la région radio et définissez la manière dont la passerelle transfère le trafic vers un serveur réseau : soit en Packet Forwarder via UDP, soit via Basics Station en WebSockets sécurisés, soit, en alternative, en activant le serveur LoRaWAN intégré.

Lorsque le serveur intégré est activé, **“Network Server Dashboard”** ouvre la console intégrée permettant d’enregistrer des passerelles, d’enregistrer des objets, de créer des applications et des profils d’équipement, et de superviser les trames.

Pour les déploiements plus importants, la fonction **“Bulk Device Import function”** propose un import guidé afin de provisionner plusieurs capteurs en une seule opération.



Dans "**Access Service**", vous définissez comment le serveur web de configuration est exposé. Utilisez cette page pour imposer un accès chiffré en activant HTTPS et, si nécessaire, en installant votre certificat serveur et votre clé privée.

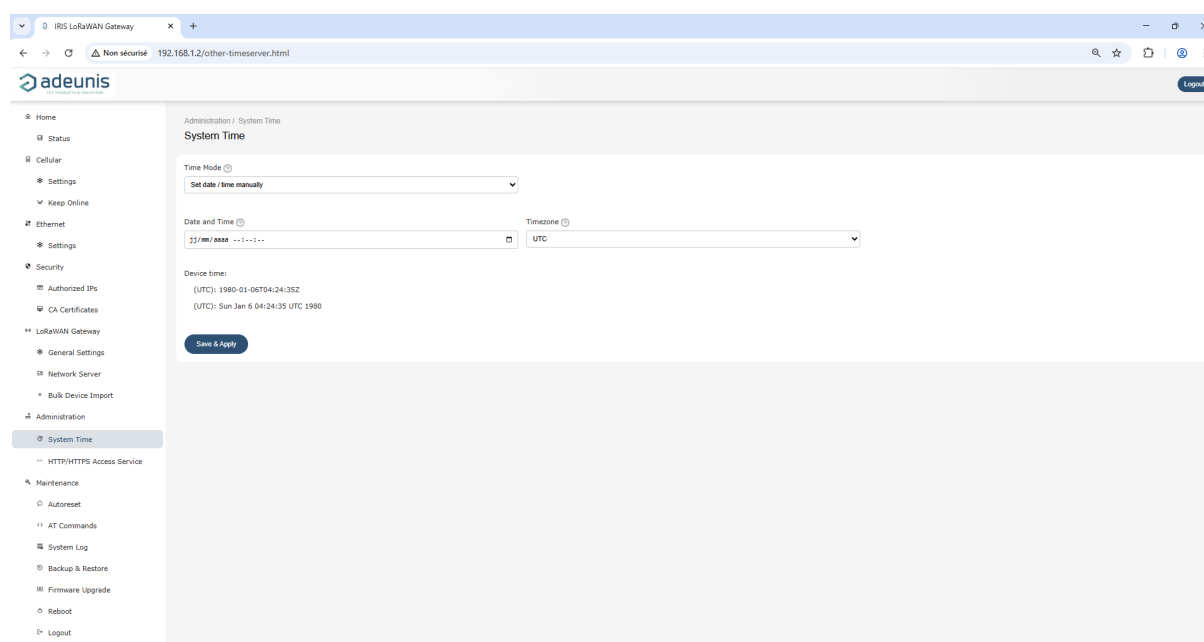
Pour plus d'informations, reportez-vous à la section [Web GUI Access](#) du Guide Utilisateur.

La page "**System Time**" permet de définir la date, l'heure et le fuseau horaire de la passerelle.

Vous pouvez soit :

- **Utiliser un serveur NTP** (recommandé), ou
- **Configurer la date et l'heure manuellement** lorsqu'aucun service NTP n'est disponible.

Une heure exacte est essentielle pour les échanges TLS et pour l'horodatage correct des logs.



En mode **NTP**, renseignez au moins un serveur NTP fiable — idéalement deux pour la redondance — puis vérifiez que l'heure affichée sur la page *Status* correspond bien à l'heure locale du site.

En mode **Manual**, saisissez directement la date et l'heure dans l'interface et sélectionnez le fuseau horaire approprié. Le mode manuel est destiné aux réseaux isolés ou aux déploiements où aucun service NTP n'est accessible.

Pour configurer l'heure système, reportez-vous à la section [Time Synchronization](#) du Guide Utilisateur.

Maintenance Section

L'espace "**Maintenance**" regroupe tout ce dont vous avez besoin pour l'exploitation au quotidien : planification de redémarrages préventifs, diagnostics, collecte des logs, sauvegarde de la configuration, mise à jour firmware et redémarrages. C'est l'endroit où

vous reviendrez après la mise en service pour maintenir la passerelle en bon état dans la durée.

La page "**Periodic Autoreset**" permet de planifier un redémarrage automatique à un jour et une heure définis. C'est utile pour des sites non supervisés qui bénéficient d'un entretien périodique. Choisissez une fenêtre de maintenance en gardant à l'esprit que la passerelle sera indisponible pendant un court instant lors du redémarrage. Si vous n'avez pas de raison opérationnelle particulière, laissez l'autoreset désactivé : la plateforme n'en a pas besoin pour fonctionner normalement.

The screenshot shows the 'Autoreset' configuration page in the IRIS LoRaWAN Gateway web interface. The page has a sidebar on the left with a navigation menu. The main content area is titled 'Autoreset' and contains several configuration options:

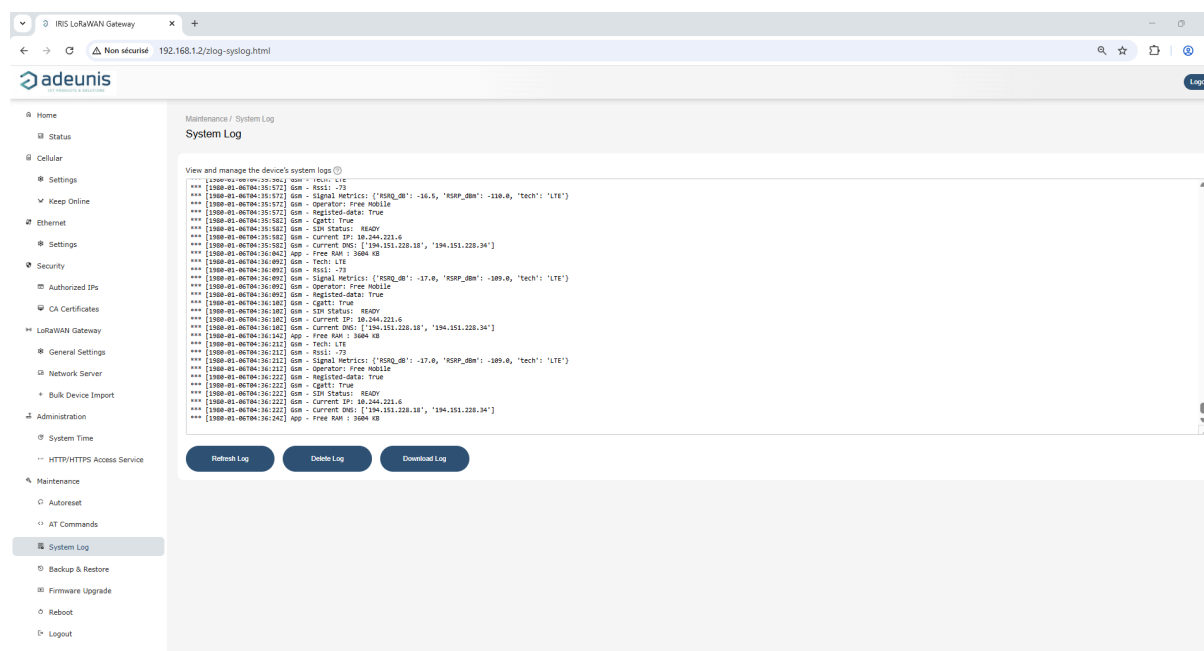
- ☒ Disable autoreset
- ☐ Autoreset every X hours: Number of hours (24)
- ☐ Autoreset at specific hour: Hour (0)
- ☒ Reset on WAN IP problems: Minutes (30)
- ☒ Restart LMS at specific hour: Hour (12)

A 'Save & Apply' button is located at the bottom of the configuration area.

La page "**AT Commands**" met à disposition une console sécurisée permettant d'interroger le module cellulaire à des fins de diagnostic.

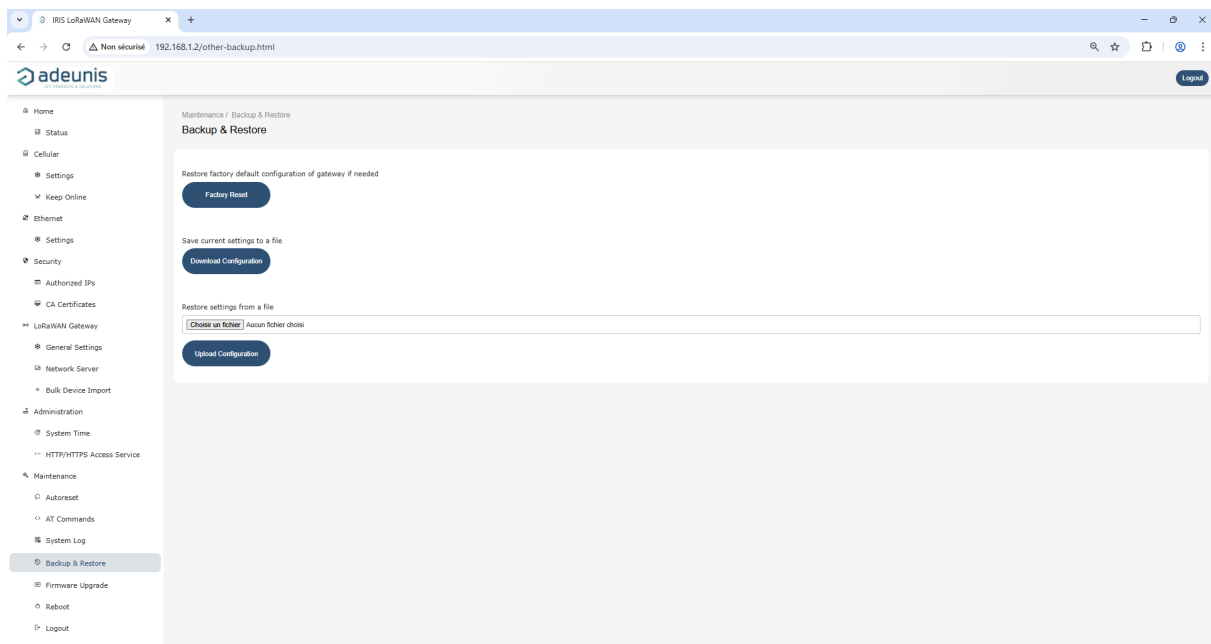
The screenshot shows the 'AT Commands' console page in the IRIS LoRaWAN Gateway web interface. The page has a sidebar on the left with a navigation menu. The main content area is titled 'AT Commands' and contains a text input field for the 'AT Command' and a larger text area for the 'AT Command Response'. A 'Send AT Command' button is located at the bottom of the console area.

Dans "**Syslog**", vous pouvez consulter les logs système récents et, si nécessaire, les exporter. Centraliser les logs dans un serveur de logs est très utile pour corréliser les événements à l'échelle d'un parc et pour l'analyse post-incident. Commencez par vérifier que NTP est synchronisé afin que les enregistrements provenant de plusieurs passerelles soient alignés ; puis vérifiez sur votre serveur de logs que les entrées de cet équipement sont bien reçues.

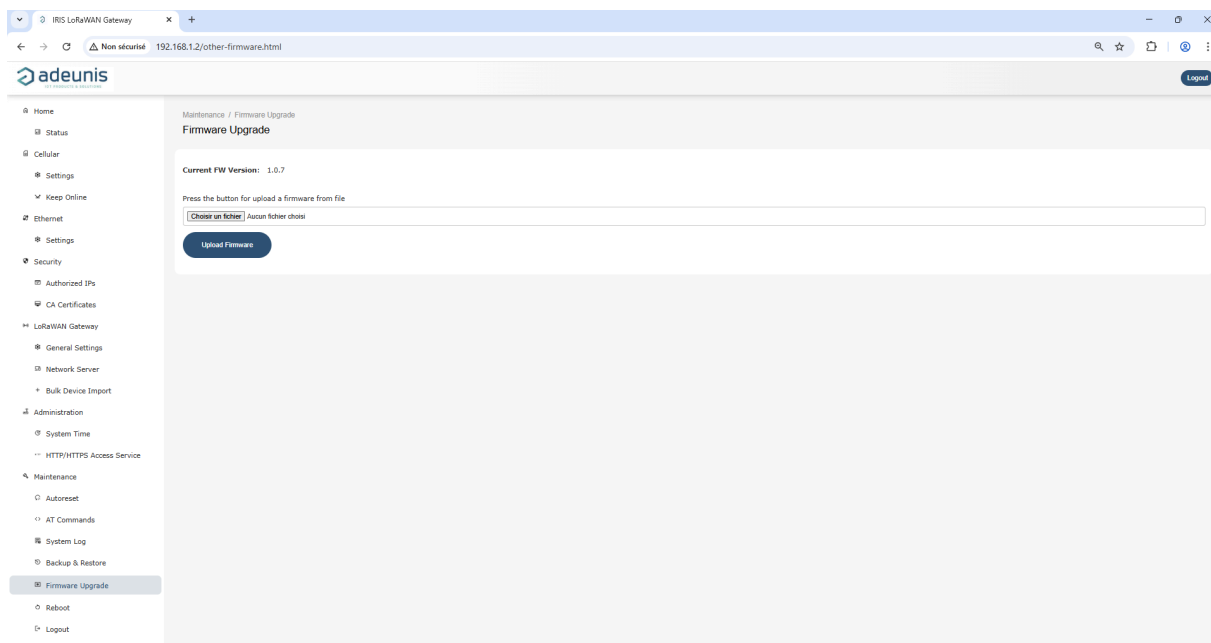


"**Backup & Restore**" est votre filet de sécurité. Utilisez "**Download Configuration**" pour exporter la configuration actuelle dans un fichier et l'archiver avec la documentation du site avant tout changement important. Si vous devez revenir à un état connu, "**Upload Configuration**" permet de réappliquer cette configuration.

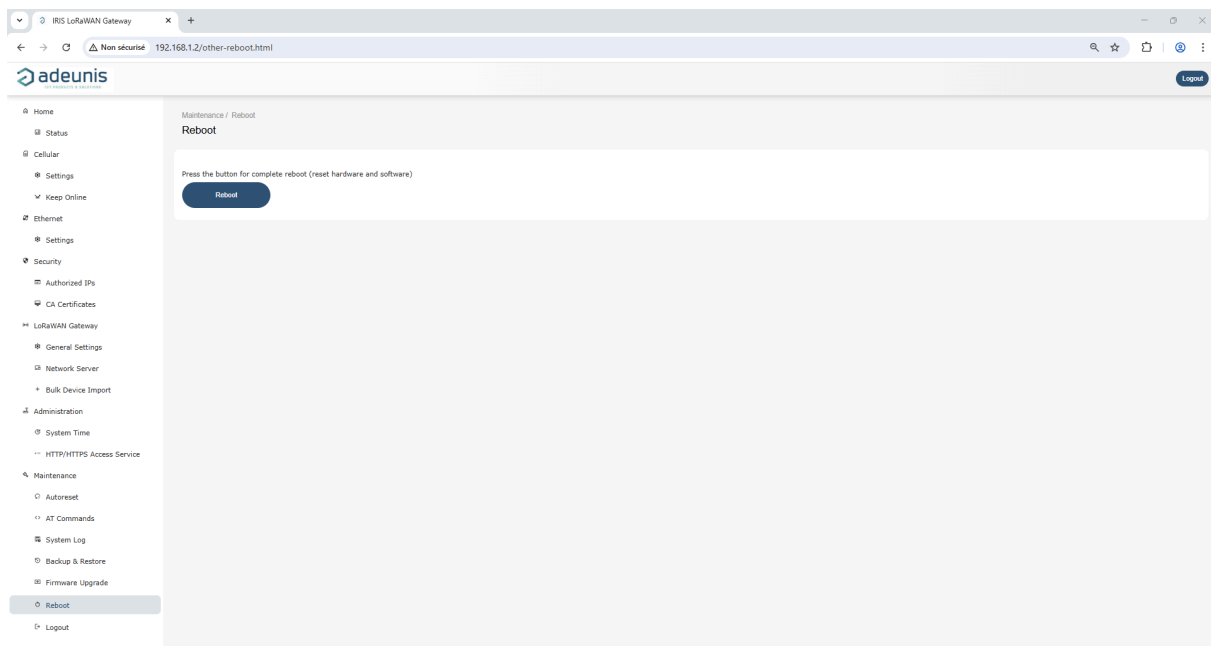
L'action "**Factory reset**" rétablit les paramètres d'usine et efface les réglages personnalisés ; ne l'utilisez qu'en cas de nécessité et uniquement après avoir téléchargé une sauvegarde récente. Un appui long sur le bouton "Function" réalise la même remise à zéro. Dans la mesure du possible, privilégiez l'interface, car elle permet de confirmer l'impact avant de lancer l'action.



La page “**Firmware Upgrade**” permet de charger une nouvelle version logicielle. Lors de l’upload, la passerelle vérifie l’image, applique la mise à jour, puis effectue un redémarrage contrôlé. Ne coupez pas l’alimentation pendant ce processus. Après le redémarrage, ouvrez la page Status pour confirmer la nouvelle version firmware, vérifier que l’heure est synchronisée et vous assurer que la configuration de transfert est toujours active. Conservez une sauvegarde de configuration réalisée juste avant la mise à jour afin de pouvoir restaurer rapidement si nécessaire.



Pour finir, “**Reboot**” lance un redémarrage logiciel standard sans modifier la configuration, et “**Logout**” met fin à la session d’administration et vous ramène à la page de connexion.



La plupart des pages de configuration suivent le même schéma d'utilisation : vous modifiez les champs dans le panneau de droite, puis vous validez explicitement les changements.



Bonne pratique : appliquez une seule modification logique à la fois, revenez sur **Home** → **Status** pour vérifier l'effet attendu, puis passez à la tâche suivante. Ce rythme — configurer, enregistrer, vérifier — rend la mise en service plus prévisible et facilite le dépannage.

4.2. Accès réseau

IRIS propose deux options pour raccorder la passerelle à votre réseau IP : **Ethernet** ou **cellulaire (2G/3G/4G)**.

La mise en service se fait généralement en Ethernet, pour des raisons de rapidité et de prévisibilité, puis vous choisissez quel lien restera actif en exploitation.

L'objectif de cette section n'est pas de décrire chaque champ de chaque page, mais de vous aider à faire les bons choix, à les appliquer en toute sécurité, puis à vérifier le résultat

sur la page **"Status"**.



Vous utilisez une seule liaison à la fois : le fonctionnement **dual-actif** pour la résilience **n'est pas pris en charge**.

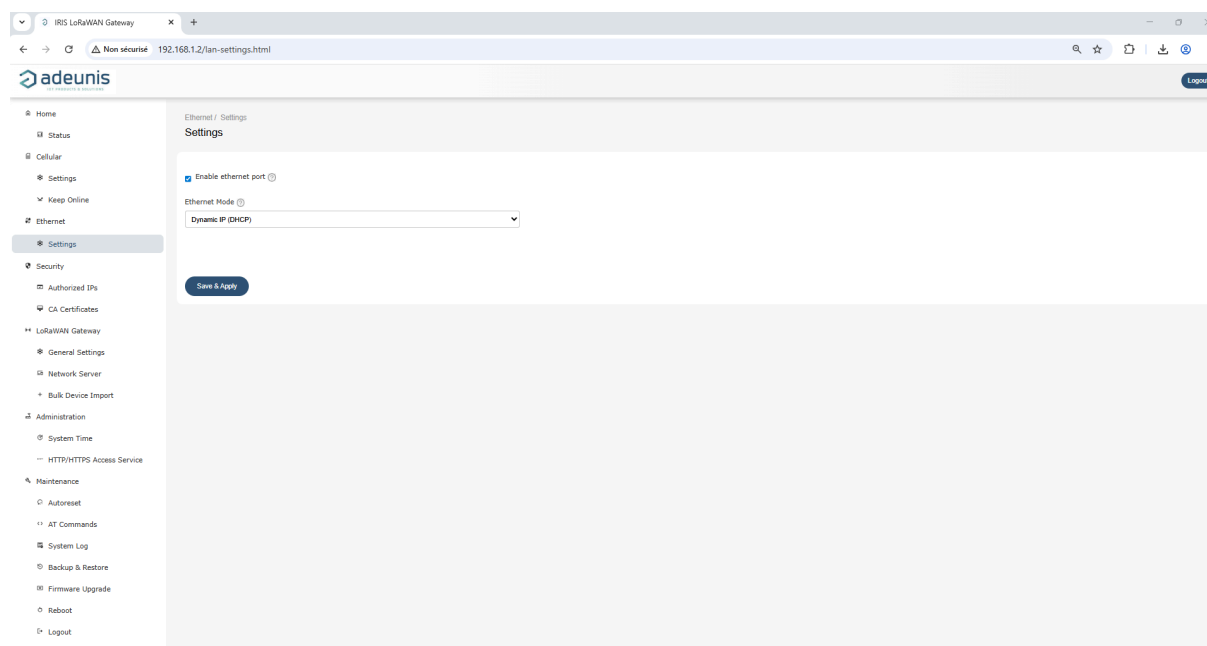
4.2.1. Interface Ethernet

Utilisez Ethernet pour la première configuration et pour les sites où la passerelle restera sur un LAN ou un VLAN géré par le client.

Décidez dès le départ avec le responsable du site si l'adressage est fourni par DHCP ou s'il doit être fixe.

Configuration d'adresse IP dynamique

Lorsque **DHCP** est disponible, l'activer est généralement l'option la plus sûre : la passerelle recevra son adresse IPv4, son masque, sa passerelle par défaut et ses serveurs DNS depuis le serveur DHCP.



Identifier l'adresse IP attribuée (DHCP)

Après avoir basculé **Ethernet** en **Dynamic (DHCP)** et appliqué le changement, la passerelle demande une adresse au serveur DHCP du réseau.

Pour connaître l'adresse IP attribuée :

- **Consulter la table des concessions DHCP du routeur / serveur DHCP**

Demandez à votre équipe IT de retrouver l'équipement à **partir de l'adresse MAC** de la passerelle (imprimée sur l'étiquette produit) ou à partir du **hostname** si le réseau en attribue un.

- **Découvrir l'équipement depuis le LAN**

Depuis un poste situé sur le **même sous-réseau**, identifiez la passerelle en vous appuyant sur la table ARP / voisins (correspondance IP ↔ MAC), ou lancez un scan réseau (ex. `arp`, `ip neigh`, `nmap`) afin de retrouver l'IP associée à l'adresse MAC de la passerelle.

Configuration d'adresse IP statique

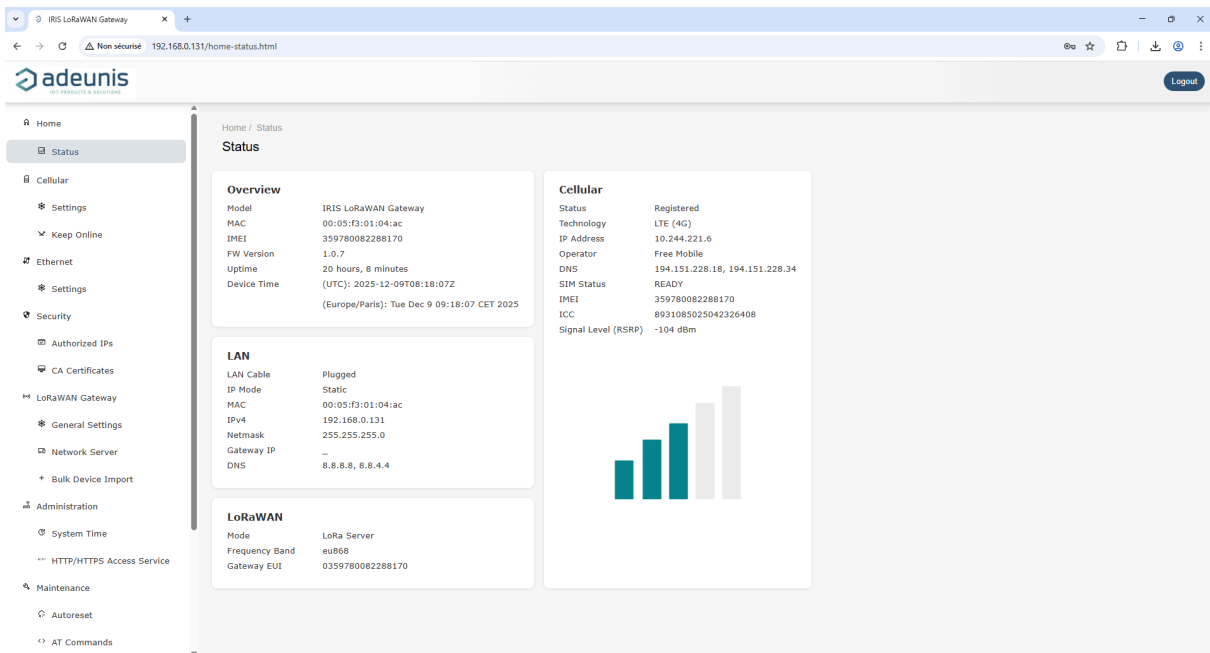
Si le site impose une **IP statique**, saisissez une adresse unique sur le VLAN, le **masque de sous réseau** correcte (par exemple `255.255.255.0` pour un /24) ainsi que l'**IP Gateway** permettant de router le trafic en dehors de ce sous-réseau.

Sans passerelle valide, le trafic LoRaWAN vers des serveurs externes ne sortira pas du LAN.

Renseignez au moins un résolveur **DNS** : les noms seront nécessaires plus tard pour NTP et pour Basics Station (WSS). Utilisez de préférence les résolveurs du client, sauf exigence particulière imposant des DNS publics.

The screenshot shows the 'Settings' page for the 'Ethernet' interface of the IRIS LoRaWAN Gateway. The page is accessed via a web browser at the URL '192.168.1.2/lan-settings.html'. The left sidebar contains a navigation menu with options like Home, Status, Cellular, Settings, Keep Online, Ethernet, Security, Authorized IPs, CA Certificates, LoRaWAN Gateway, General Settings, Network Server, Bulk Device Import, Administration, System Time, HTTP/HTTPS Access Service, Maintenance, Autoreboot, AT Commands, System Log, Backup & Restore, Firmware Upgrade, Reboot, and Logout. The main content area is titled 'Ethernet / Settings' and 'Settings'. It features a toggle for 'Enable ethernet port' which is turned on. Below this, the 'Ethernet Mode' is set to 'Static IP'. The configuration fields are as follows: IP Address is '192.168.1.2', IP Subnet Mask is '255.255.255.0', IP Gateway is empty, DNS 1 is '8.8.8.8', and DNS 2 is '8.8.4.4'. A 'Save & Apply' button is located at the bottom of the configuration section.

Lorsque vous appliquez de nouveaux paramètres Ethernet, l'interface web bascule sur la nouvelle IP : reconnectez votre navigateur sur cette adresse et vérifiez sur **Home** → **Status** que l'IPv4, le masque, la passerelle et les DNS sont exactement ceux validés avec l'équipe IT.



Si vous perdez la session à cause d'une erreur d'adressage, connectez votre ordinateur directement à la passerelle, définissez une IP temporaire dans le même sous-réseau, puis corrigez la configuration.

Référence rapide des paramètres

Paramètre (interface web)	Fonction	Valeur typique / exemple	Quand modifier	Validation / remarques
Enable Ethernet Port	Active l'interface Ethernet et applique les paramètres Ethernet. Désactivez cette option si vous ne souhaitez pas utiliser l'interface Ethernet.	Cochée	Activer pour la mise en service ou l'exploitation sur LAN	Status → LAN affiche "Plugged" et les informations de lien

Paramètre (interface web)	Fonction	Valeur typique / exemple	Quand modifier	Validation / remarques
Ethernet mode	Méthode d'adressage. Choix entre DHCP (adressage fourni par le LAN) et Static IP (valeurs à saisir manuellement).	DHCP ou Static IP	Selon la politique du site	Si DHCP : vérifier l'IP attribuée sur Status ; si Static : se reconnecter sur la nouvelle IP
IP Address	Adresse statique de la passerelle sur le LAN ; elle doit être unique sur ce sous-réseau.	192.168.10.42	Déploiements en IP statique	Doit être unique sur le VLAN ; à consigner pour le support
IP Subnet Mask	Définit la taille du réseau ; à régler selon le masque utilisé sur le VLAN.	255.255.255.0	Déploiements en IP statique	Un masque incorrect provoque des problèmes d'accessibilité au-delà du sous-réseau
IP Gateway	Routeur qui achemine le trafic hors du sous-réseau ; sans lui, les services LoRaWAN externes ne sont pas joignables.	192.168.10.1	Déploiements en IP statique	Indispensable pour accéder à un LNS / NTP externe
DNS 1 / DNS 2	Résolveurs de noms utilisés par la passerelle ; nécessaires pour NTP et Basics Station (WSS).	DNS du site ou 8.8.8.8 / 8.8.4.4	Déploiements en IP statique ou besoins DNS spécifiques	Requis pour les noms NTP et les endpoints WSS (Basics Station)

4.2.2. Interface cellulaire

Choisissez le cellulaire lorsque la passerelle doit fonctionner indépendamment du LAN du client, ou lorsque l'Ethernet n'est pas disponible.

Mettez l'équipement hors tension, insérez une carte SIM valide, puis remettez sous tension et ouvrez les paramètres cellulaires.



Avant d'activer le lien, insérez une carte SIM valide et récupérez auprès de votre opérateur les paramètres APN.

Configuration de l'interface cellulaire

L'**APN** (Access Point Name) est fourni par votre opérateur. Saisissez-le exactement tel qu'indiqué (certains APN privés sont stricts sur l'orthographe).

Si votre abonnement impose des identifiants, renseignez **Username** et **Password**, puis positionnez **Authentication** selon la méthode demandée par l'opérateur (le plus souvent **PAP** ou **CHAP** ; si rien n'est requis, laissez **None**).

Si la SIM est protégée par un code PIN, saisissez le **PIN** avec soin : plusieurs tentatives erronées bloquent la carte jusqu'à saisie du PUK selon la procédure de l'opérateur.

Le **Network selection** doit rester sur **Auto**, sauf raison spécifique de verrouiller une technologie (par exemple "4G-only").

Pour **DNS selection**, "Get DNS from Operator" convient dans la majorité des cas ; basculez vers "Selected DNS servers" uniquement si votre application nécessite des résolveurs que l'opérateur ne fournit pas. Dans ce cas, nous recommandons d'utiliser les DNS Google :

8.8.8.8 et 8.8.4.4 .

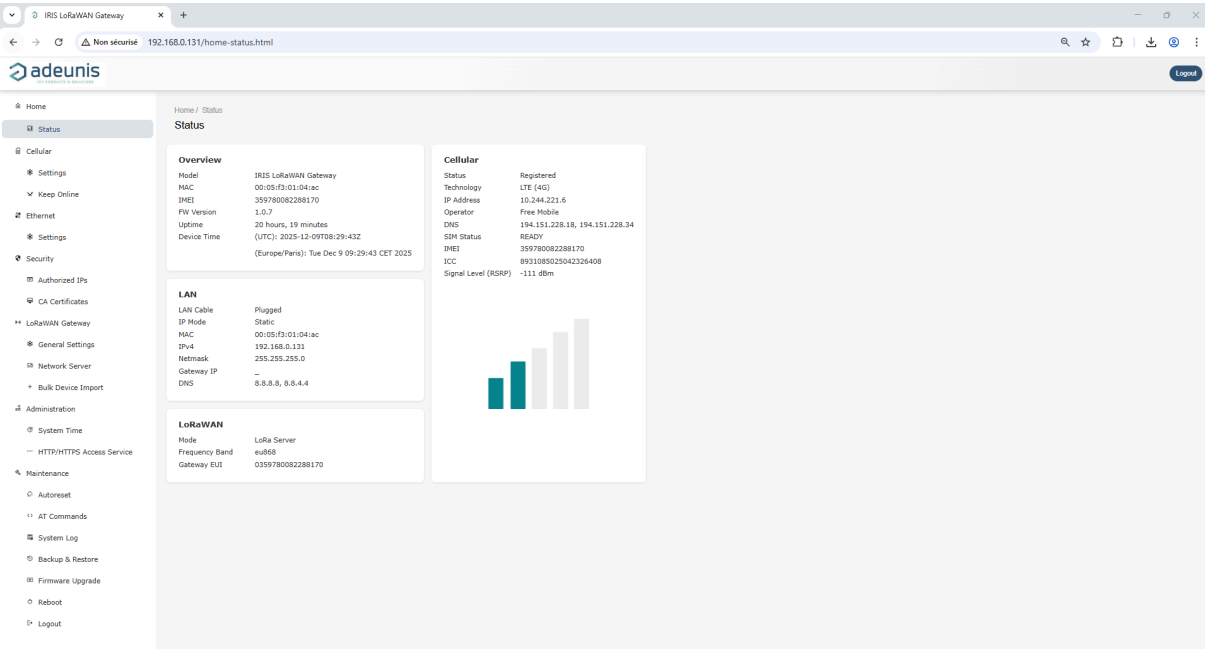
The screenshot shows the 'adeunis' web interface for a LoRaWAN Gateway. The left sidebar contains a navigation menu with options like Home, Status, Cellular, Settings, Security, LoRaWAN Gateway, Administration, and Maintenance. The main content area is titled 'Cellular / Settings' and 'Settings'. It features a toggle for 'Enable cellular connectivity'. Below this are input fields for 'APN' (containing 'mobioma.m2m'), 'Username', 'Password', 'PIN', 'Authentication' (set to 'None'), 'Network Selection' (set to 'Auto'), and 'DNS Selection' (set to 'Get DNS from Operator'). There is also a checkbox for 'Remote Webserver Management'. A 'Save & Apply' button is located at the bottom of the settings section.

Configuration de l'accès à distance au serveur Web

Si vous devez accéder à l'interface web via le réseau mobile, activez la gestion à distance du serveur web uniquement après avoir activé le protocole HTTPS, et uniquement si votre APN autorise les connexions entrantes.

Si vous n'avez pas besoin d'une administration à distance via le réseau cellulaire, laissez cette option désactivée afin de réduire les risques.

Après avoir enregistré vos modifications, consultez la page **Status** : le modem doit s'enregistrer sur le réseau, obtenir une adresse IP et signaler la qualité du signal (RSRP).



 **L'accès à distance à l'interface Web IRIS depuis l'extérieur du réseau local n'est pris en charge que via le réseau cellulaire, et uniquement lorsque la carte SIM/l'APN attribue une adresse IP statique publique routable à la passerelle.**
Si la carte SIM se trouve derrière un CGNAT ou utilise une adresse privée/dynamique, les connexions entrantes n'atteindront pas la passerelle et l'administration à distance ne sera pas possible.

Référence rapide des paramètres

Paramètre (interface web)	Fonction	Valeur typique / exemple	Quand modifier	Validation / remarques
Enable Cellular Connectivity	Lorsqu'elle est activée, le modem	Cochée	Utiliser le cellulaire comme	Status → Mobile affiche

Paramètre (interface web)	Fonction	Valeur typique / exemple	Quand modifier	Validation / remarques
	s'attache au réseau mobile et établit un contexte data via l'APN fourni.		connectivité amont active	"Registered" et une adresse IP
APN	APN fourni par l'opérateur	matouma.m2m / APN opérateur	Changement de SIM / opérateur	L'orthographe exacte est importante (APN privés parfois stricts)
Username / Password	Identifiants APN fournis par l'opérateur	vide si non requis	Si l'opérateur impose une authentification	À utiliser avec le bon mode Authentication
Authentication	Méthode d'authentification APN	None si non requis, PAP, ou CHAP	Selon les prérequis opérateur	Un mode incorrect empêche l'attachement / la data
PIN	Code de verrouillage SIM. À saisir uniquement si l'opérateur n'a pas désactivé la protection PIN à la livraison.	ex. 1234	Si la SIM est protégée par PIN	3 essais erronés bloquent la SIM ; PUK requis
Network selection	Politique de sélection radio	Auto, 4G, 3G, 2G	Rarement (demande opérateur)	Verrouiller une techno peut réduire la couverture, surtout en itinérance
DNS selection	Permet d'utiliser les DNS fournis par l'opérateur ou de définir des DNS spécifiques dans des cas particuliers	Get DNS from Operator	Si des DNS fixes sont requis	DNS manuels uniquement si nécessaire pour l'application
Remote webserver management	Exposition de l'interface web via cellulaire	Disabled (recommandé)	Activer uniquement avec HTTPS et si l'APN autorise l'accès entrant	Beaucoup d'APN utilisent le CGNAT → pas d'accessibilité entrante

4.2.3. Supervision de connectivité ("Keep Online")

Le watchdog est un mécanisme simple mais efficace pour améliorer la résilience de la passerelle en maintenant le lien **actif** en bon état. Il ping périodiquement une cible que vous définissez ; si la cible n'est pas joignable dans le délai (timeout) et pour le nombre de tentatives configuré, il réinitialise la connexion cellulaire et tente de rétablir le service.



Le watchdog ne bascule pas entre Ethernet et cellulaire : il ne fait que rétablir la connexion cellulaire.

Choisissez un **Ping server** stable et joignable depuis le réseau utilisé (par exemple un résolveur connu).

Le **Period** est l'intervalle entre contrôles, en minutes : trouvez le bon compromis entre réactivité et charge réseau.

Le **Timeout** correspond au temps d'attente avant de considérer une tentative comme échouée ; quelques secondes (ex. 5–10) conviennent à la plupart des réseaux.

Retries définit le nombre d'échecs consécutifs requis pour déclencher la récupération.

Retry period correspond au délai (en minutes) entre tentatives de récupération si la première n'aboutit pas.

The screenshot shows the 'Keep Online' configuration page in the IRIS LoRaWAN Gateway web interface. The sidebar on the left lists various system settings, with 'Keep Online' currently selected. The main panel displays configuration options for the cellular watchdog. The 'Enable ping keep-alive' checkbox is checked. Below it, there are input fields for 'Ping Server' (set to 8.8.8.8), 'Period' (set to 30 minutes), 'Timeout' (set to 5 seconds), 'Retries' (set to 1), and 'Retry Period' (set to 1 minute). A 'Save & Apply' button is located at the bottom of the configuration area.

Des périodes et des timeouts trop courts peuvent provoquer des réinitialisations inutiles sur des réseaux congestionnés ; des valeurs trop longues retardent la récupération. Démarrez avec des réglages modérés, puis vérifiez dans vos logs que le lien reste stable pendant les premières heures d'exploitation. Ajustez ensuite si vous observez soit des resets inutiles (réglage trop agressif), soit une récupération trop lente (réglage trop permissif).

Référence rapide des paramètres

Paramètre (interface web)	Fonction	Valeur typique / exemple	Quand modifier	Validation / remarques
Enable Ping Keep-Alive	Active le watchdog	Cochée pour sites non supervisés	À utiliser sur cellulaire pour auto-rétablir le lien data	Ne bascule pas vers Ethernet ; ne rétablit que le lien actif
Ping server	Hôte testé ; choisir une cible joignable depuis l'APN et autorisée par les pare-feu du chemin	Un résolveur connu	Si APN / pare-feu / routage change	Doit être joignable depuis l'APN utilisé
Period	Intervalle entre contrôles (1–1440 min)	30	Si trop/pas assez de récupérations	Trop court → faux resets ; trop long → récupération lente
Timeout	Attente par test (5–20 s)	5	Chemins à forte latence	Augmenter sur liens congestionnés/ éloignés
Retries	Nombre d'échecs avant récupération (0–9)	1	Réseaux bruités vs. besoin de réactivité	Plus élevé = moins de faux positifs
Retry period	Délai entre tentatives de récupération (1–1440 min)	1	Si "tempêtes" de récupération	Évite les resets rapprochés

Régler l'horloge avant de sécuriser la passerelle

La connectivité amont est opérationnelle. Avant d'activer la sécurité et les modes LoRaWAN, configurez l'heure système afin que l'horloge de l'équipement soit correcte. La

validation TLS, l'horodatage Syslog et les éléments de preuve de mise en service en dépendent.

Vous pouvez soit :

- Synchroniser automatiquement via **Serveurs NTP Time** (recommandé), ou
- **Configurer l'heure et la date manuellement** lorsqu'aucun service NTP n'est disponible.

4.2.4. Synchronisation de l'heure

Une heure exacte est un prérequis pour un déploiement stable. Les échanges TLS (par ex. Basics Station via **WSS**), la corrélation Syslog et les éléments de preuve de mise en service reposent sur l'horloge de la passerelle.

La page **System Time** permet de :

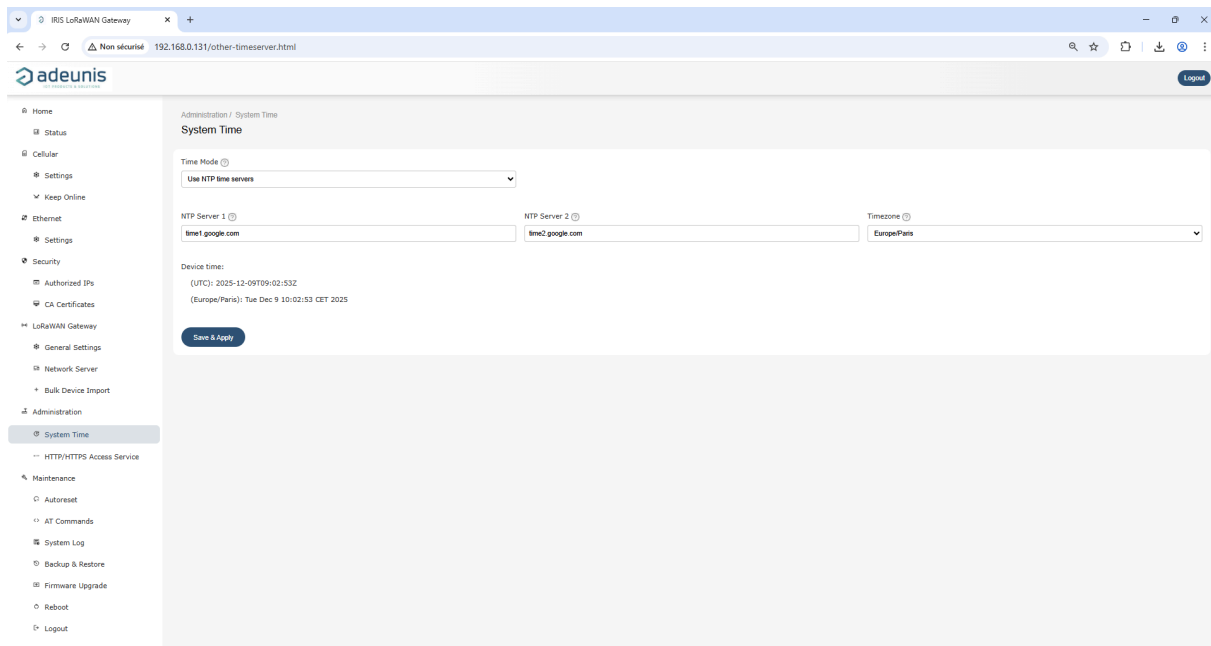
- Choisir le **Time Mode** (serveurs NTP ou configuration manuelle),
- Renseigner les serveurs NTP lorsque le mode NTP est sélectionné,
- Définir le **Timezone** local utilisé pour l'affichage et les logs.

Configuration NTP

Choisissez **Use NTP time servers** pour activer la synchronisation automatique.

Renseignez au moins **un serveur NTP fiable**, idéalement **deux** provenant d'infrastructures différentes (par ex. un NTP d'entreprise + un service public de secours). Les choix typiques sont le NTP interne du client (recommandé en LAN d'entreprise) ou des services publics reconnus tels que `time1.google.com` et `time2.google.com`.

Sélectionnez le **Timezone** du site (ex. *Europe/Paris*) afin que l'heure locale affichée sur Status et dans les exports de logs corresponde bien au fuseau horaire de l'installation.



Intervalle de synchronisation

La première synchronisation NTP est effectuée lors de la connexion initiale.

Ensuite, la synchronisation NTP est réalisée automatiquement toutes les 24 heures.

Exigences en matière de connectivité

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

Nécessite un **UDP/123** sortant et une résolution DNS (UDP/TCP 53) si vous utilisez des noms d'hôte

- **NTP d'entreprise ou d'opérateur**

Aucune connexion Internet requise ; seule la connectivité à ces serveurs via **UDP/123** est nécessaire.

- **APN privés**

L'accès à Internet est souvent bloqué ; demandez un NTP interne à l'opérateur ou utilisez un serveur d'entreprise accessible.

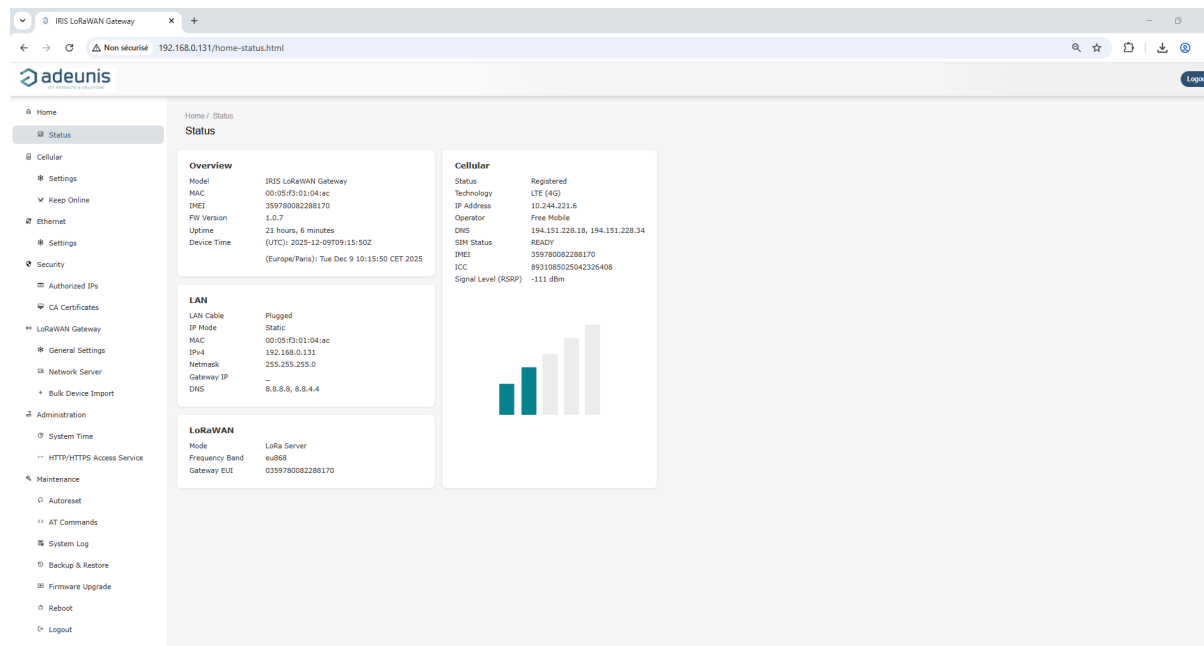
- **Restrictions DNS**

Si le DNS est filtré, utilisez les **adresses IP** statiques fournies par le service informatique.



Sur des APN privés ou des réseaux filtrés, privilégiez le **NTP interne** du client ou utilisez des **adresses IP** fournies par l'IT.

Après enregistrement, revenez sur **Home** → **Status** et vérifiez **Device Time** : l'heure UTC doit être à jour et la ligne d'heure locale doit refléter le timezone sélectionné.



Si l'heure ne se met pas à jour sous une minute : vérifiez que la connectivité amont active dispose d'un **DNS** fonctionnel (si vous avez utilisé des noms) et que l'accès sortant **UDP/123** vers les serveurs listés est autorisé par le pare-feu du site ou par l'APN.

Mode manuel

Choisissez **Set date/time manually** lorsque la passerelle ne peut joindre aucune source NTP.

Dans ce mode :

- Saisissez la **Date and Time** directement dans le champ prévu,
- Sélectionnez le **Timezone** approprié,
- Enregistrez la configuration pour appliquer l'heure manuelle.

Le mode manuel est destiné aux réseaux isolés, APN restreints, environnements de lab, ou mises en service temporaires lorsque NTP n'est pas disponible.

Notez que l'heure ne se corrigera pas automatiquement : mettez-la à jour manuellement si le déploiement dure suffisamment longtemps pour que la dérive devienne perceptible.



Si la date/l'heure est configurée manuellement, elle doit être mise à jour à chaque mise hors tension ou réinitialisation de l'équipement.

4.2.5. Validation et transfert

Une configuration réseau est considérée comme bonne lorsque :

1. La connectivité amont choisie affiche une IP valide sur **Home** → **Status**,
2. L'heure de l'équipement est synchronisée,
3. Et (si requis) l'interface web est joignable en **HTTPS** via ce même chemin.

Avant de quitter le site, exportez une sauvegarde de configuration, consignez l'adressage final et la méthode d'accès, documentez les serveurs NTP et le timezone dans votre rapport de mise en service, puis repassez l'adaptateur réseau de votre ordinateur en **DHCP** afin de ne pas rester bloqué sur les paramètres statiques temporaires lors de votre prochaine connexion.

Avant d'aller plus loin

Vous disposez désormais d'une liaison réseau opérationnelle (Ethernet ou cellulaire) et d'une heure correcte sur l'appareil.

Renforcez maintenant l'accès administratif. Commencez par imposer le protocole **HTTPS** pour l'interface Web, puis limitez l'exposition avec les **adresses IP autorisées** et enfin, chargez les certificats **CA Root** requis pour sécuriser les connexions sortantes.

4.3. Sécurité (contrôle d'accès et confiance)

Une fois la connectivité vérifiée, sécurisez la passerelle afin que votre première connexion LoRaWAN se déroule sans incident et que l'interface web ne reste pas exposée plus longtemps que nécessaire. Vous allez définir qui peut accéder aux services via le **Mobile WAN** et installer les **autorités de certification** (CA) auxquelles la passerelle fera confiance pour valider des serveurs sécurisés.

4.3.1. Accès à l'interface Web

La première étape consiste à protéger l'accès à l'interface web.

Activez **HTTPS** pour l'interface web afin que les identifiants et les sessions soient systématiquement chiffrés pendant le transport.

N'exposez l'interface au-delà d'un ordinateur directement connecté qu'une fois HTTPS actif, et uniquement en complément d'une liste d'adresses autorisées définie dans **Authorized IPs**.

Prérequis pour l'accès à distance (interface web)

L'accès à distance à l'interface web IRIS depuis l'extérieur du LAN local n'est supporté **que via la connectivité cellulaire**, et uniquement lorsque la SIM/APN attribue à la passerelle une **adresse IP statique publique** et routable.

Si la SIM est derrière du CGNAT ou utilise une adresse privée/dynamique, les connexions entrantes n'atteindront pas la passerelle : l'administration à distance n'est alors pas possible.

Paramètres d'identifiants et de ports

Définissez le **Username** et un **Password** robuste pour l'administration.

Conservez le **HTTPS port** à **443**, sauf contrainte spécifique (politique IT, port imposé, etc.). Réservez le **HTTP port** à la mise en service locale uniquement.

En production, accédez à l'interface via **https://** et bloquez le HTTP non chiffré au niveau du pare-feu du site ou du routeur amont. Si votre politique impose "no HTTP", coordonnez-vous avec l'IT afin de vérifier que le port 80 n'est pas accessible sur le chemin réseau vers la passerelle.

Activer HTTPS

Cochez **Enable HTTPS**.

The screenshot shows the 'HTTP/HTTPS Access Service' configuration page in the LoRaWAN Gateway administration interface. The page has a sidebar with navigation links like Home, Status, Cellular, Settings, Ethernet, Security, and Administration. The main content area contains the following fields and sections:

- HTTP port**: Input field with value 80.
- HTTPS port**: Input field with value 443.
- Enable HTTPS tool box**: A checkbox that is currently unchecked.
- Username**: Input field with value admin.
- Password**: Input field with masked characters.
- Confirm Password**: Input field with masked characters.
- Custom KEY and Certificate for HTTPS Webserver**: Two large text areas for pasting certificates and keys. The first area is labeled 'HTTPS Certificate' and the second is labeled 'HTTPS KEY'. Both contain sample PEM format text.
- Save & Apply**: A button at the bottom of the configuration section.

Certificat personnalisé pour l'interface web (recommandé)

Si les administrateurs doivent accéder à l'interface via le réseau cellulaire, installez un certificat serveur correspondant au nom d'hôte (hostname) que vous utiliserez pour joindre la passerelle.

- Collez le **HTTPS Certificate** complet (PEM) — incluez toute la chaîne si votre CA l'exige, avec les marqueurs `-----BEGIN CERTIFICATE-----` ... `-----END CERTIFICATE-----`.
- Collez le **HTTPS KEY** correspondant (PEM) — la clé privée associée (`PKCS#1` ou `PKCS#8`).
- Le **CN/SAN** du certificat doit correspondre au nom d'hôte utilisé dans l'URL (ex. `gw-iris-01.site.local`) ; sinon, le navigateur affichera un avertissement de non-correspondance.

- Protégez la clé privée et appliquez une rotation selon votre politique de sécurité.

Se reconnecter via l'URL HTTPS prévue

Un cadenas fermé sans avertissement confirme la cohérence certificat / nom d'hôte / horloge. Si le navigateur affiche encore un avertissement, vérifiez : l'heure de l'équipement (NTP), la correspondance hostname ↔ CN/SAN, la présence de la chaîne complète, et l'association correcte clé/certificat.

Référence rapide des paramètres

Paramètre (interface web)	Fonction	Valeur typique / exemple	Quand modifier	Validation / remarques
Enable HTTPS	Active l'accès chiffré à l'interface web	Cochée	Toujours en production	Se reconnecter en <code>https://...</code> ; vérifier le cadenas (aucun avertissement navigateur)
HTTPS port	Port TCP pour la configuration à distance via HTTPS	443	Uniquement si la politique IT impose un port non standard	Vérifier <code>https://<hôte>: <port></code> ; consigner le port pour l'exploitation
HTTP port	Port TCP pour la configuration à distance via HTTP non chiffré	80	À désactiver/bloquer en production	Privilégier HTTPS ; vérifier que HTTP n'est pas accessible sur le chemin prévu
Username	Identifiant administrateur pour l'accès à l'interface web	<code>admin</code> → modifier si la politique l'exige	Au premier paramétrage ou selon la politique	Tester la connexion ; stocker dans un coffre de mots de passe
Password / Re- Enter	Mot de passe administrateur	Phrase de passe robuste	Au premier paramétrage et lors des rotations	Vérifier la connexion après enregistrement ; appliquer la politique de rotation
HTTPS Certificate (PEM)	Certificat serveur (et chaîne)	PEM avec chaîne complète	Si exposition via LAN/VPN/APN	CN/SAN doit correspondre au

Paramètre (interface web)	Fonction	Valeur typique / exemple	Quand modifier	Validation / remarques
	présenté par l'interface			hostname ; inclure les marqueurs BEGIN/END
HTTPS KEY (PEM)	Clé privée correspondant au certificat serveur	Clé PEM (PKCS#1 / PKCS#8)	Lors de l'installation/rotation du certificat	Doit correspondre au certificat ; conserver la clé secrète ; rotation selon politique

Le protocole HTTPS est maintenant obligatoire. Passez à la section § 4.3.2 **Adresses IP autorisées** pour permettre uniquement aux adresses sources connues d'accéder aux services administratifs et LoRaWAN via le réseau WAN mobile.

4.3.2. Adresses IP autorisées (Mobile WAN allow-list)

Cette page met en place une **liste d'adresses autorisées** pour les services accessibles via l'interface **cellulaire / Mobile WAN**.

Pour chaque service, un sélecteur propose deux options :

- **ALLOW ANY IP** — aucune restriction (pratique uniquement pour la mise en service).
- **ALLOW ONLY AUTHORIZED IP** — n'autorise **que** les adresses sources renseignées dans **Authorized IP1-IP3**.

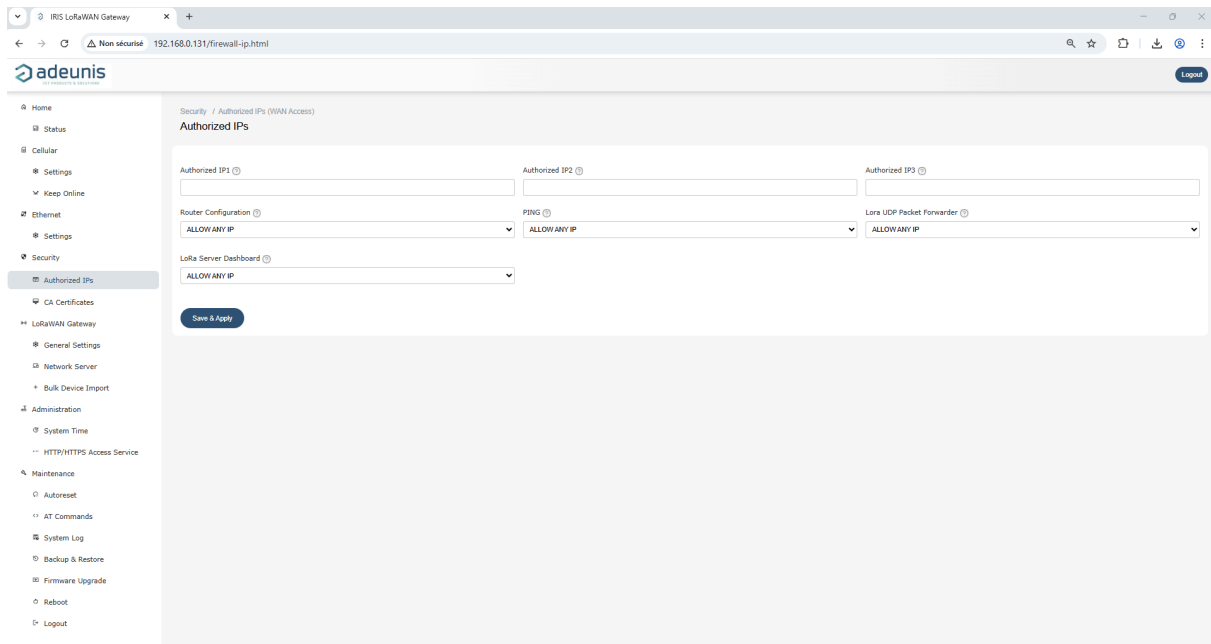
C'est votre première ligne de défense lorsque la passerelle est accessible en dehors d'un LAN privé. Sur Ethernet, privilégiez le pare-feu du client ; utilisez cette page pour maîtriser l'exposition via la connectivité cellulaire.



Conservez un accès Ethernet comme voie de secours pendant le réglage des règles Mobile WAN.

Réglages recommandés

Renseignez les trois champs **Authorized IP1 / IP2 / IP3** avec les **adresses publiques exactes** qui doivent pouvoir joindre la passerelle via le réseau cellulaire.



- **Remote Configuration.** Contrôle qui peut accéder à l'interface web via le réseau cellulaire. Commencez par imposer le protocole **HTTPS**, activez ensuite **l'accès distant à l'interface web**, puis renseignez **l'adresse IP publique** de votre équipe d'administration / NOC. Si vous n'avez pas besoin d'accès à l'interface web via cellulaire, désactivez **l'accès distant à l'interface web** ou positionnez **ALLOW ONLY AUTHORIZED IPs** et laissez la liste vide afin de bloquer effectivement ce service.
- **PING.** Contrôle les **réponses ICMP** (echo) via le Mobile WAN. Positionnez **ALLOW ONLY AUTHORIZED IPs** et laissez la liste vide, sauf si l'exploitation nécessite explicitement des réponses ICMP.
- **LoRa UDP Packet Forwarder.** Contrôle les downlinks UDP **entrants** depuis votre LNS vers la passerelle. Si vous utilisez le mode Packet Forwarder **UDP** via cellulaire, positionnez **ALLOW ONLY AUTHORIZED IPs** et assurez-vous que les IP de downlink du LNS figurent dans **Authorized IP1-3**. Si vous utilisez **Basics Station (WSS)**, ce sélecteur n'est pas utilisé par WSS.
- **LoRa Server Dashboard.** S'applique à la console du **serveur LoRaWAN intégré**. Positionnez **ALLOW ONLY AUTHORIZED IPs** ; ne renseignez une IP d'administration que si l'accès via cellulaire est réellement nécessaire, sinon laissez la liste vide pour bloquer l'accès.



NOTE 1

Les valeurs par défaut **ALLOW ANY IP** peuvent faciliter la mise en service, mais ne sont pas adaptées à une exploitation en production via cellulaire. Restreignez-les dès que le lien est opérationnel.

NOTE 2

Pour bloquer l'accès à un service via l'interface cellulaire / Mobile WAN, sélectionnez **ALLOW ONLY AUTHORIZED IPs** et laissez la liste vide.

Référence rapide des paramètres

Contrôle (interface web)	Recommandation en production (Mobile WAN)	Justification
Remote Configuration	ALLOW ONLY AUTHORIZED IPs	Limiter l'interface web aux administrateurs connus (ou bloquer via liste vide)
PING	ALLOW ONLY AUTHORIZED IPs (liste vide)	Désactiver les réponses ICMP sauf besoin explicite
LoRa UDP Packet Forwarder	ALLOW ONLY AUTHORIZED IPs (+ IP du LNS si UDP PF)	Les downlinks sont des flux UDP entrants
LoRa Server Dashboard	ALLOW ONLY AUTHORIZED IPs (liste vide si non utilisé)	Limiter l'accès à la console du serveur LoRaWAN intégré

4.3.3. CA Certificates – ancres de confiance pour les services distants sécurisés (MQTTs/HTTPs/Basics Station WSS)

Ce **référentiel de certificats** active TLS pour les connexions sortantes d'IRIS vers les **services applicatifs et réseau** :

- Brokers **MQTTs** (TCP **8883**)
- Webhooks / API **HTTPS** (TCP **443**)
- **Basics Station** en **WSS** vers votre LNS (TCP **443** ou le port spécifié par votre LNS)

En installant les **CA Root** appropriées, la passerelle peut valider la chaîne de certificats du serveur lors du handshake TLS et établir une session chiffrée et authentifiée.

Principe de validation

Lorsqu'IRIS se connecte, le serveur distant présente son **certificat serveur** (et éventuellement des certificats **intermédiaires**). IRIS vérifie que la chaîne s'ancre sur l'un des certificats **CA Root** chargés ici, et que le **nom d'hôte** configuré correspond au **CN/SAN** du certificat.

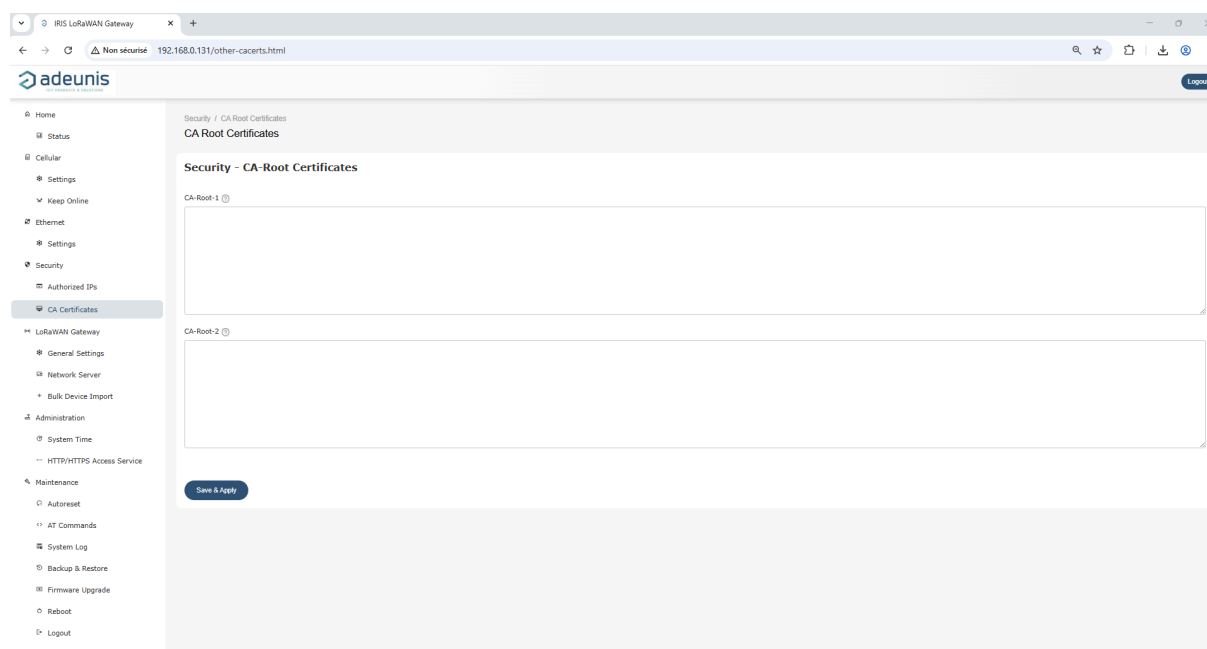
Que charger ?

1. Récupérez la chaîne CA auprès de votre fournisseur et vérifiez son empreinte (fingerprint) par un canal indépendant.
2. Collez les blocs PEM complets dans **CA-Root-1/2**, en incluant :

- `-----BEGIN CERTIFICATE-----`

...base64...

- `-----END CERTIFICATE-----`



3. Si la validation échoue, vérifiez : l'horloge, la correspondance CA vs certificat serveur, la correspondance hostname vs CN/SAN, et la présence éventuelle d'un proxy interceptant TLS.

Modèles de confiance pris en charge

IRIS prend en charge deux modèles de connexion :

- **Avec CA Root auto-signée (self-signed)**

Créez votre propre **CA Root** (auto-signée, comme toutes les racines), utilisez-la pour **signer** le certificat serveur de votre endpoint **MQTTs/HTTPS/WSS**, puis **chargez cette CA Root** dans IRIS. Configurez dans IRIS un **hostname** correspondant au **CN/SAN** du certificat serveur.

- **Avec certificat serveur signé par une CA**

Obtenez un certificat serveur auprès d'une CA publique ou d'entreprise (ex. Let's Encrypt). Assurez-vous que le serveur présente la **chaîne complète** (certificat serveur + intermédiaires). **Chargez la CA Root** correspondante (ex. **ISRG Root X1**) dans IRIS et configurez le **hostname** du service en conséquence.



Le firmware de la passerelle IRIS supporte jusqu'à deux entrées CA Root personnalisées au format PEM.

4.3.4. Validation et transfert

HTTPS est configuré, l'exposition via l'interface cellulaire est restreinte, et les CA Root sont chargées.

Effectuez les contrôles suivants pour valider la configuration de sécurité et constituer les éléments de preuve pour l'exploitation :

1. Ouvrez l'interface via **http://<gateway-ip>**. L'accès doit être bloqué par la politique du site, ou être immédiatement redirigé vers HTTPS si HTTPS est activé. Ouvrez ensuite **https://<gateway-hostname-or-ip>:<https-port>** et connectez-vous. Le navigateur doit afficher une **session sécurisée (cadenas) sans avertissement** lorsque vous utilisez un certificat personnalisé correspondant au hostname. Conservez une capture d'écran des détails du certificat (cadenas) ainsi que de la page **HTTP/HTTPS** (ports, "HTTPS enabled", empreinte / dates).
2. Testez la configuration Authorized IPs depuis une source **autorisée** (accès OK) et depuis une source **non autorisée** (accès bloqué). Documentez la liste d'adresses autorisées ; mettez-la à jour si le fournisseur LNS change d'IP.
3. Vérifiez que les blocs PEM sont bien présents, contrôlez la date d'expiration de chaque certificat et planifiez la rotation. Si votre mode LoRaWAN utilise **Basics Station (WSS)** ou **MQTTs/HTTPS**, vérifiez que le **hostname** configuré correspond au CN/SAN (valider avec l'administrateur LNS/broker en cas de doute). Conservez une capture de la page **CA Certificates** et notez pour chaque CA son **issuer** et sa **date d'expiration**.

Vous êtes prêt à vous connecter au réseau LoRaWAN

Votre passerelle est joignable, synchronisée, et sécurisée (HTTPS imposé, Authorized IPs appliquées, référentiel de certificats configuré).

L'étape suivante consiste à activer l'interface LoRaWAN. Dans le **Chapitre 5**, vous choisirez un mode de fonctionnement unique (Packet Forwarder en **UDP** ou **Basics Station/WSS**, ou le **serveur LoRaWAN intégré**), configurerez la bande régionale, complèterez les paramètres spécifiques au mode choisi, puis vérifierez le trafic avec un équipement réel.



Sauvegardez votre configuration avant de démarrer, puis appliquez les changements bloc par bloc et vérifiez systématiquement sur **Home** → **Status**.

5. CONFIGURATION LoRaWAN & MISE EN SERVICE

Ce chapitre décrit la mise en service de la passerelle sur votre réseau LoRaWAN, soit en transférant le trafic vers un serveur réseau LoRaWAN (LNS) externe (UDP Packet Forwarder ou Basics Station/WSS), soit en utilisant un serveur LoRaWAN intégré.

Avant de commencer, assurez-vous que :

- la connectivité amont est opérationnelle,
- l'heure système est correcte (NTP ou configuration manuelle),
- l'accès HTTPS et le référentiel de certificats CA sont configurés si vous utilisez des transports sécurisés.

Sauvegardez votre configuration avant d'appliquer des modifications et suivez la progression dans **Home** → **Status**.

Ayez à disposition les informations nécessaires : adresse/ports du LNS pour l'UDP, **URL WSS + CA correspondante** (et, le cas échéant, jeton/certificat client) pour Basics Station,

ou bien les profils/clefs des équipements si vous utilisez le serveur intégré.

5.1. Modes de fonctionnement

En LoRaWAN, la passerelle reçoit des trames radio émises par les équipements (end-devices) et les transmet à un serveur réseau LoRaWAN (LNS).

IRIS prend en charge les modes de fonctionnement suivants :

5.1.1. Packet Forwarder

La passerelle transmet les trames à un **serveur réseau externe**.

Deux implémentations sont disponibles :

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

Un pont uplink/downlink simple basé sur UDP, largement supporté par les plateformes LNS historiques.

- **Basics Station (WSS)**

Un transport moderne et sécurisé basé sur WebSockets (WSS recommandé).

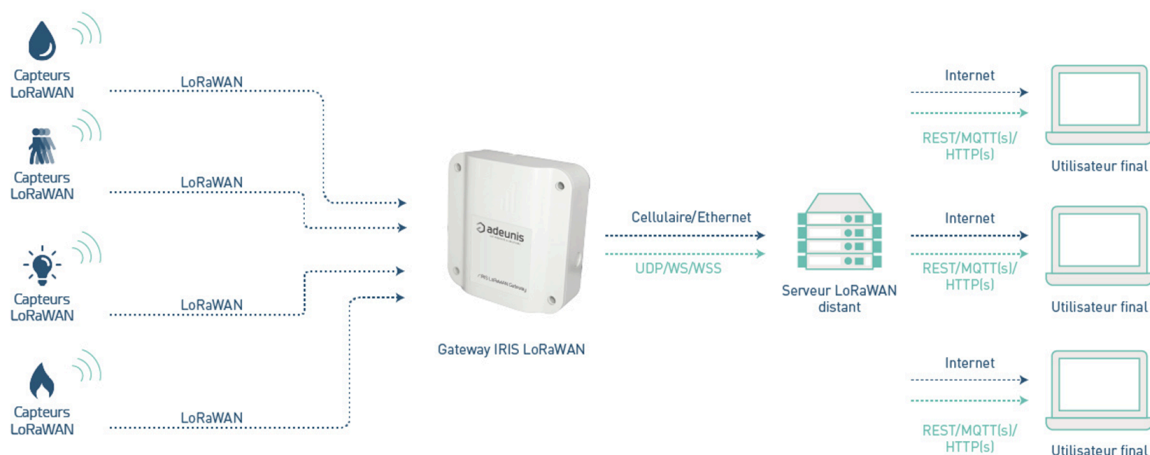
Basics Station nécessite une horloge correcte et un référentiel CA configuré afin d'établir des sessions TLS avec le LNS.

Bootstrap CUPS (optionnel)

Basics Station peut être provisionné dynamiquement via un serveur CUPS (Configuration and Update Server).

Le CUPS fournit à la passerelle l'URI du LNS, des identifiants mis à jour et les fichiers de configuration.

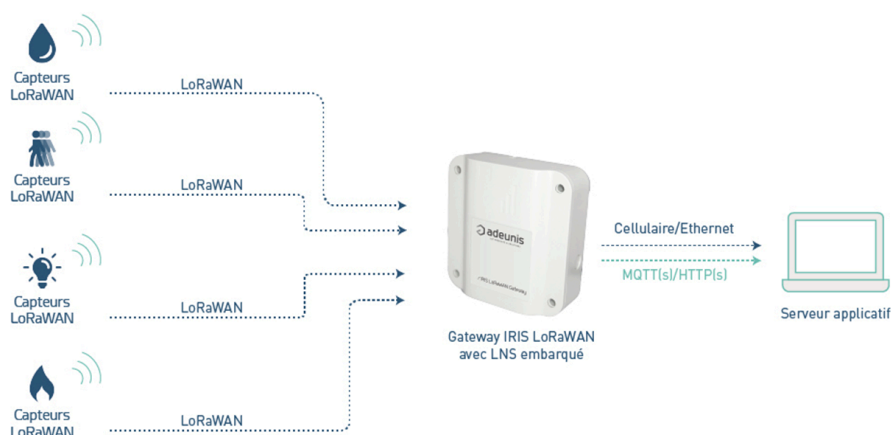
Le CUPS n'est pas un mode de transfert : il prépare la configuration d'exécution de Basics Station.



5.1.2. Serveur LoRaWAN embarqué (LNS)

La passerelle héberge localement le serveur réseau.

Choisissez ce mode si vous souhaitez gérer directement les équipements LoRaWAN depuis IRIS (registre d'équipements, profils, paramètres MAC et downlinks).



5.2. Sélectionner le mode de fonctionnement

1. Ouvrez **LoRaWAN** → **General Settings**
2. Cochez **Enable the LoRaWAN stack**
3. Puis sélectionnez l'un des modes suivants :
 - **Packet Forwarder (UDP)**

Pont Semtech UDP "classique" vers un LNS externe.

Nécessite les ports uplink/downlink du LNS et des IP joignables.

- **Packet Forwarder (Basics Station)**

Transfert moderne et sécurisé via WSS.

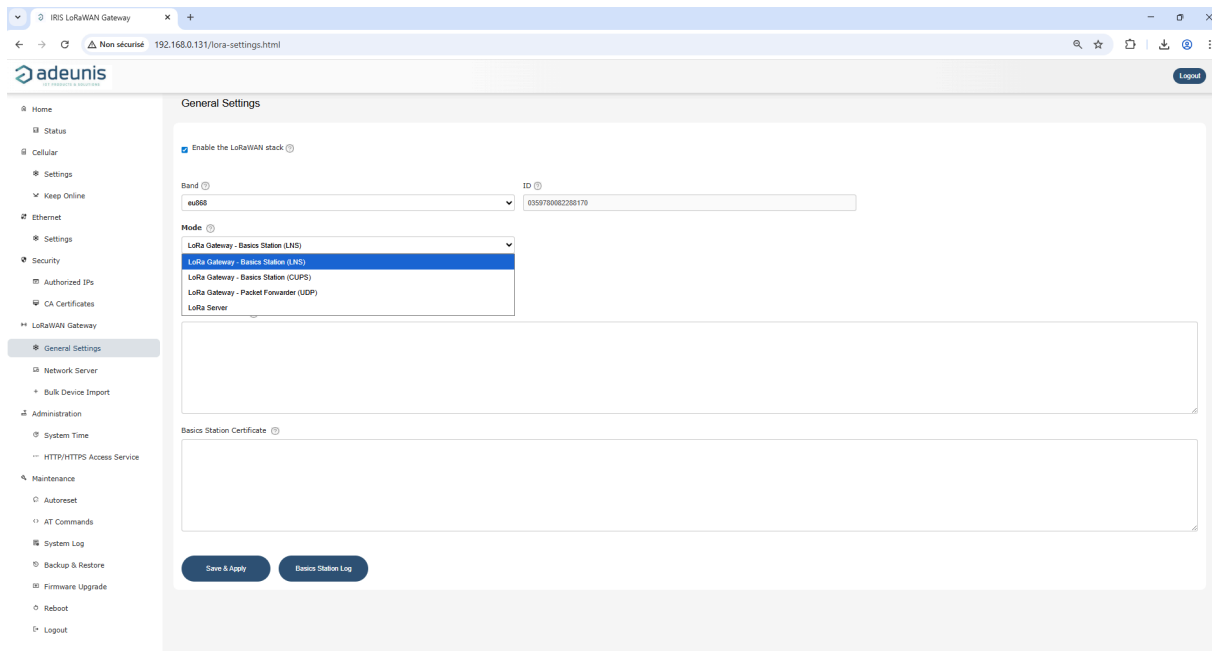
Nécessite une heure correcte, un référentiel CA configuré et l'URL WSS du LNS.

Si un serveur CUPS est fourni par votre opérateur, renseignez d'abord **CUPS Settings** avant de configurer les paramètres LNS.

- **LoRaWAN Server**

LNS interne hébergé sur IRIS (registre d'équipements, profils, planification des downlinks, décodage local optionnel).

The screenshot shows the 'General Settings' page for a LoRaWAN Gateway in the Adeunis web interface. The page is accessed via a browser at the URL 192.168.0.131/loras-settings.html. The interface includes a sidebar with navigation options like Home, Status, Cellular, Settings, Keep Online, Ethernet, Security, Authorized IPs, CA Certificates, General Settings (selected), Network Server, Bulk Device Import, Administration, System Time, HTTP/HTTPS Access Service, Maintenance, Autoreset, AT Commands, System Log, Backup & Restore, Firmware Upgrade, Reboot, and Logout. The main content area is titled 'General Settings' and contains various configuration fields. A checkbox 'Enable the LoRaWAN stack' is checked. Fields include Band (set to eu863), ID (035976082208170), Mode (set to LoRa Server), Keep Alive (10), Stat Interval (30), Push Timeout (100), Latitude, Longitude, Altitude, Net ID (000000), RX1 Delay (1), LoRa Server Dashboard Username (DEMO IRIS), and LoRa Server Dashboard Password (masked). There is also an option to 'Enable extra frequencies'. At the bottom, there are fields for MQTT Broker URL (set to tcp://adeunis-codex.com:1883), MQTT ID (IRISElia), MQTT Username (ades), MQTT Password (masked), MQTT QoS (0), and MQTT Key.



5.3. Définir la bande radio

Toujours dans **LoRaWAN** → **General Settings**, réglez **Band/Region** (par ex. **EU863-870 / EU868**).

Assurez-vous que la bande correspond au pays d'installation et que les antennes sont connectées / homologuées pour cette bande.

Les contraintes régionales (duty-cycle, puissance TX, canaux) sont appliquées par le LNS et les profils d'équipements. Une incohérence entraîne des joins en échec ou des trames ignorées.



Le firmware actuel ne prend en charge que la bande EU868.

En mode **LoRaWAN Server** uniquement, vous pouvez **Enable extra frequencies** et contraindre le **Minimum/Maximum Data Rate (DR0...DR5)** afin de correspondre à votre parc d'équipements et à votre plan radio. N'utilisez cette option que si vous maîtrisez le plan de canaux du site et les contraintes réglementaires.

1. Cochez **Enable Extra Frequencies**

Cette option active l'utilisation de canaux supplémentaires au-delà des 3 canaux EU868 obligatoires (868.1, 868.3 et 868.5 MHz).

Lorsque l'option est activée, le serveur utilise également l'un des 5 canaux optionnels 125 kHz : 867.1, 867.3, 867.5, 867.7 et 867.9 MHz.

2. Sélectionnez le débit minimum/maximum autorisé sur ces canaux supplémentaires.

DR0 est plus robuste mais plus lent ; DR5 est plus rapide mais moins robuste.

The screenshot shows the 'General Settings' page for a LoRaWAN Gateway. The interface includes a sidebar with navigation options like Home, Status, Cellular, Ethernet, Security, and Administration. The main content area is titled 'General Settings' and contains several sections:

- Enable the LoRaWAN stack:** A checkbox that is checked.
- Band:** A dropdown menu set to 'eu868'.
- Mode:** A dropdown menu set to 'LoRa Server'.
- Net ID:** A text field containing '000000'.
- MQTT Broker URL:** A text field containing 'tcp://adeunis-codex.com:1883'.
- MQTT ID:** A text field containing 'IRIS001'.
- MQTT Username:** A text field containing 'ades'.
- MQTT Password:** A text field with masked characters.
- MQTT QoS:** A dropdown menu set to '1'.
- Enable extra frequencies:** A checkbox that is checked.
- Minimum Data Rate:** A dropdown menu set to 'DR0'.
- Maximum Data Rate:** A dropdown menu set to 'DR5'.
- Re-Send data:** A dropdown menu set to 'Resend data using MQTT'.

DR	Facteur d'étalement / BW	Usage typique
DR0	SF12 / 125 kHz	Portée maximale, le plus lent
DR1	SF11 / 125 kHz	Longue portée
DR2	SF10 / 125 kHz	Rural / intérieur
DR3	SF9 / 125 kHz	Usage général
DR4	SF8 / 125 kHz	Portée plus courte
DR5	SF7 / 125 kHz	Portée courte, le plus rapide
DR6	SF7 / 250 kHz	Optionnel (downlink)
DR7	FSK 50 kbps	Optionnel

3. Cliquez sur "Save & Apply"

4. La passerelle lancera automatiquement une nouvelle procédure de join.



L'activation de fréquences supplémentaires augmente la capacité de la passerelle, limite le risque de collisions et améliore la répartition du duty-cycle. De nombreux profils restent en DR0-DR5. N'utilisez DR6/DR7 que si votre profil et votre réseau les autorisent.

5.4. Paramètres du Packet Forwarder UDP

En mode **Packet Forwarder (UDP)**, la passerelle IRIS transfère les données reçues des équipements LoRaWAN vers un serveur réseau LoRaWAN (LNS) externe via **UDP**.

Ce mode est particulièrement adapté lorsque le LNS est hébergé à l'extérieur et que la passerelle joue un rôle de passerelle de transfert (« bridge »), sans traitement supplémentaire.

Fonctionnalités :

- Intégration rapide avec les principaux LNS tiers, adaptée aux petits déploiements et aux Proof of Concept.
- Les données sont transférées via **UDP** pour une communication à faible latence.
- Pas de décodage local des payloads ni de traitement avancé des données sur la passerelle.

5.4.1. Informations nécessaires côté LNS

Avant de commencer, récupérez :

- le **nom d'hôte / IP du LNS** et les **ports UDP** (uplink/downlink) auprès de l'administrateur du LNS ;
- les éventuelles **règles de pare-feu du site** à appliquer pour autoriser l'UDP sortant (uplink) et l'UDP entrant (downlink), selon votre chemin réseau.

5.4.2. Configuration UDP

Allez dans **LoRaWAN** → **General Settings**

1. Sélectionnez **Packet Forwarder (UDP)**.
2. Renseignez **LNS host** et les **ports UDP Up/Down** exactement tels que fournis par votre LNS.
3. (Optionnel) Ajustez les paramètres de temporisation (keep-alive, stat interval, push timeout) selon les valeurs recommandées pour votre environnement :
 - **Keep Alive (s)** : heartbeat vers le LNS (typ. 10).
 - **Stat Interval (s)** : périodicité d'envoi de la télémétrie (typ. 30).
 - **Push Timeout (ms)** : seuil avant retransmission (typ. 100).

Un timeout trop court peut générer des retransmissions inutiles sur des réseaux congestionnés ; un timeout trop long retarde la détection des problèmes réseau. Commencez avec des réglages modérés (**100 ms est recommandé**) et vérifiez la stabilité du lien dans les premières heures suivant la mise en service. Ajustez si vous constatez soit

des retransmissions inutiles (réglage trop agressif), soit une détection trop lente (réglage trop permissif).

4. (Optionnel) Configurez **Latitude / Longitude / Altitude** (utile pour la cartographie et certaines statistiques côté LNS).

The screenshot shows the 'General Settings' page for a LoRaWAN Gateway. The left sidebar contains a navigation menu with options like Home, Status, Cellular, Settings, Keep Online, Ethernet, Security, Authorized IPs, CA Certificates, LoRaWAN Gateway, General Settings (selected), Network Server, Bulk Device Import, Administration, System Time, HTTP/HTTPS Access Service, Maintenance, Autorest, AT Commands, System Log, Backup & Restore, Firmware Upgrade, Reboot, and Logout. The main content area is titled 'General Settings' and contains a form with the following fields: 'Enable the LoRaWAN stack' (checked), 'Band' (dropdown set to 'eu868'), 'ID' (text field with '835076002289170'), 'Mode' (dropdown set to 'LoRa Gateway - Packet Forwarder (UDP)'), 'Keep Alive' (text field with '10'), 'Stat Interval' (text field with '30'), 'Push Timeout' (text field with '100'), 'Latitude' (text field with '45.26847824574859'), 'Longitude' (text field with '5.890621120285311'), 'Altitude' (text field with '1'), 'Server Address' (empty text field), 'UDP Upstream Port' (text field with '1700'), and 'UDP Downstream Port' (text field with '1700'). A 'Save & Apply' button is located at the bottom left of the form.

5. Cliquez sur **“Save & Apply”**.

Référence rapide des paramètres

Paramètre	Rôle	Valeur typique / exemple
Enable the LoRaWAN Stack	Active la pile LoRaWAN et les réglages associés	Activé
ID	Identifiant unique de la passerelle (EUI-64)	Lecture seule
Server address	Adresse du serveur LNS recevant les données et les paquets de statistiques	lns.example.com
Up port	Port du LNS pour les uplinks et les paquets de statistiques	1700
Down port	Port du LNS pour les downlinks	1700
Keep Alive (s)	Intervalle des messages heartbeat UDP vers le LNS pour maintenir la liaison	10
Stat Interval (s)	Intervalle d'envoi des statistiques passerelle	30

Paramètre	Rôle	Valeur typique / exemple
	(température, compteurs, RSSI moyen, etc.)	
Push Timeout (ms)	Temps maximal avant retransmission vers le LNS en cas d'erreur. Une valeur trop faible génère des transmissions inutiles	100
Latitude	Coordonnée latitude en degrés décimaux (optionnel)	45.2664
Longitude	Coordonnée longitude en degrés décimaux (optionnel)	5.8906
Altitude	Altitude en mètres au-dessus du niveau de la mer (optionnel)	1

5.4.3. Validation et transfert

Une configuration Packet Forwarder UDP est considérée correcte lorsque :

- Sur la page **Status** de la passerelle, la passerelle est indiquée comme **"connected"**.
- Dans la console du LNS, la passerelle apparaît **en ligne** et remonte des statistiques.
- Vous déclenchez un uplink de test depuis un équipement connu : le LNS doit afficher des trames reçues via votre passerelle.

Si vous ne voyez pas de trafic :

- Recontrôlez les règles de pare-feu du site.
- Recontrôlez précisément les numéros de ports Up/Down.
- Confirmez que la **bande / région** correspond à la configuration côté LNS.

5.5. Paramètres Basics Station (WS/WSS)

En mode **Basics Station**, la passerelle IRIS fonctionne comme une **station de base LoRaWAN** qui communique de manière sécurisée avec un serveur réseau via **WS/WSS (WebSocket / WebSocket Secure)**.

Ce mode est particulièrement adapté lorsque vous souhaitez un canal de communication **sécurisé et bidirectionnel** entre la passerelle et le LNS, et qu'une transmission fiable en temps réel est critique.

Fonctionnalités :

- Communication sécurisée avec le LNS via **WebSocket sécurisé (WSS)**.
- Particulièrement adapté aux environnements où la fiabilité et la réactivité de la transmission sont essentielles.

5.5.1. Informations nécessaires côté LNS

Avant de commencer, récupérez :

- l'**URL WSS + chemin (path)** fourni par votre LNS (par exemple `wss://lms.example.com/router`) ;
- un **token client** ou une **identité client (certificat/clé)** si votre LNS impose une authentification côté passerelle ;
- le **certificat CA racine** correspondant au certificat TLS du serveur distant ;
- une **heure correcte (NTP)** et la **résolution DNS** du nom d'hôte du LNS.

Si votre opérateur utilise CUPS, vous pouvez également recevoir :

- une **URL CUPS** ;
- une **clé CUPS** (identifiant JSON ou token) ;
- la **CA racine** utilisée pour signer le certificat du serveur CUPS ;
- et éventuellement un **certificat de passerelle**.

Dans ce cas, configurez **CUPS Settings**.

5.5.2. Configuration de Basics Station

Allez dans **LoRaWAN** → **General Settings**

1. Sélectionnez **Basics Station (LNS)**.
2. Renseignez l'URL du serveur "**Server URL**" exactement telle que fournie par votre LNS (schéma, hôte, port, **chemin**).
3. Si votre LNS requiert un **token**, collez-le dans **Basics Station KEY**.

Pour les déploiements en **mTLS**, l'authentification se fait via des **certificats** : chargez/sélectionnez les éléments nécessaires et vérifiez le référentiel de certificats CA.

4. Cliquez sur **Save & Apply**.

Référence rapide des paramètres

Paramètre	Rôle	Valeur typique
Enable the LoRaWAN Stack	Active la pile LoRaWAN et les réglages associés	Activé
ID	Identifiant unique de la passerelle (EUI-64)	Lecture seule
Server URL	Point d'accès WS/WSS + chemin. En environnement sécurisé, utilisez WSS (recommandé)	<code>wss://<host>:<port>/router</code> (TLS, recommandé) / <code>ws://<host>:<port>/router</code> (tests uniquement)
Basics Station key	Selon les déploiements, cette clé sert de token (envoyé dans l'en-tête d'autorisation ou dans l'URL). En mTLS , l'authentification se fait par certificats : laissez ce champ vide et utilisez les certificats	—



Si vous utilisez le mTLS (certificats), vérifiez que l'horloge (NTP) est correctement synchronisée.

5.5.3. Paramètres CUPS

Le CUPS (Configuration and Update Server) permet un provisionnement centralisé des passerelles Basics Station.

Utilisez CUPS lorsque :

- votre opérateur fournit un point d'accès CUPS ;
 - les URL ou identifiants du LNS sont renouvelés régulièrement ;
 - vous déployez des flottes importantes et souhaitez un bootstrap « zero-touch ».
-

Exigences réseau

CUPS s'appuie sur des connexions sortantes sécurisées en HTTPS :

- le trafic sortant **TCP 443** doit être autorisé ;
- la résolution DNS doit fonctionner si vous utilisez des noms de domaine ;
- l'heure système doit être correcte (NTP ou mode manuel) ;
- certains APN privés nécessitent un point d'accès CUPS interne fourni par l'opérateur.

Si le DNS est filtré, configurez le serveur CUPS via son IP et chargez la CA correspondante.

Configuration CUPS

Allez dans **LoRaWAN** → **General Settings**

1. Sélectionnez **Basics Station (CUPS)**.
2. Renseignez la **CUPS URL**.
3. Collez la **CUPS Key** fournie par l'opérateur.
4. Chargez le **Gateway Certificate** si requis.
5. Chargez le **CA Certificate** correspondant au serveur CUPS.

6. Sauvegardez et appliquez.

La passerelle lance immédiatement une séquence de bootstrap.

5.5.4. Validation et transfert

Une configuration Basics Station est considérée correcte lorsque :

- Sur la page **Status** de la passerelle, l'état est **"connected"**.
- Dans la console du LNS, la passerelle apparaît **en ligne** et remonte des statistiques.
- Un uplink de test depuis un équipement connu est visible dans le LNS, avec des trames arrivant via votre passerelle.

Si vous ne voyez pas de trafic :

- Recontrôlez que l'**heure de la passerelle** est correcte.
- Recontrôlez la présence du **certificat CA racine**.
- Vérifiez la correspondance du **nom d'hôte** avec le certificat (CN/SAN).
- Vérifiez le **chemin exact de l'URL WSS**.
- Confirmez que la **bande / région** correspond à la configuration côté LNS.



Basics Station utilise des connexions **TLS sortantes**. Les **Authorized IPs** (Mobile WAN) contrôlent l'exposition entrante (interface web, UDP PF), pas WSS. Assurez-vous que le pare-feu **autorise le trafic sortant** vers le point d'accès de votre LNS.

5.6. Paramètres du serveur réseau LoRaWAN intégré (LNS)

En mode **LNS intégré**, la passerelle IRIS fonctionne comme un **serveur réseau LoRaWAN complet** : la gestion des équipements, l'acheminement des données et les opérations réseau sont réalisés **localement** sur la passerelle.

Ce mode est particulièrement adapté si vous ne souhaitez pas dépendre d'un LNS externe et que vous voulez garder la maîtrise complète de votre réseau LoRaWAN.

Fonctionnalités :

- La passerelle devient elle-même le **serveur réseau LoRaWAN**.
- Gestion des équipements LoRaWAN (endpoints), du routage des données, de l'authentification des objets et des messages downlink.
- Prise en charge des downlinks multicast et du décodage local des payloads via le **Codec Manager**.
- Idéal pour des environnements isolés ou des réseaux privés.

Vous activez d'abord le **serveur** dans les paramètres LoRaWAN de l'**interface web**, puis vous finalisez la configuration dans le **LoRa Server Dashboard** (profils d'équipements, registre des équipements, applications, codec optionnel, multicast).

5.6.1. Activer le serveur LoRaWAN intégré

Allez dans **LoRaWAN** → **General Settings**

1. Sélectionnez **LoRa Server**.
2. Renseignez les métadonnées du site et les temporisations :
 - **Keep Alive (s)** : heartbeat vers le LNS (typ. 10).
 - **Stat Interval (s)** : périodicité de remontée de la télémétrie (typ. 30).
 - **Push Timeout (ms)** : seuil avant renvoi en cas d'erreur (typ. 100).

Un timeout trop court peut générer des renvois inutiles sur un réseau congestionné ; un timeout trop long retarde la détection des problèmes de connectivité. Commencez avec des valeurs modérées (100 ms est recommandé) puis vérifiez la stabilité durant les premières heures d'exploitation. Ajustez ensuite si vous observez soit des renvois inutiles (trop agressif), soit une reprise trop lente (trop permissif).

- **Latitude / Longitude / Altitude** (cartographie et statistiques côté LNS).
- Configurez **HTTP Port** (dashboard), **Net ID**, **RX1 Delay** (selon votre politique).
 - Définissez les identifiants **LoRa Server Dashboard Username/Password** (accès à la console du serveur LoRa).
 - (Optionnel) Activez **Enable extra frequencies** et choisissez **Minimum/Maximum Data Rate** selon votre plan de fréquences.

6. Cliquez sur **Save & Apply**.

Référence rapide des paramètres

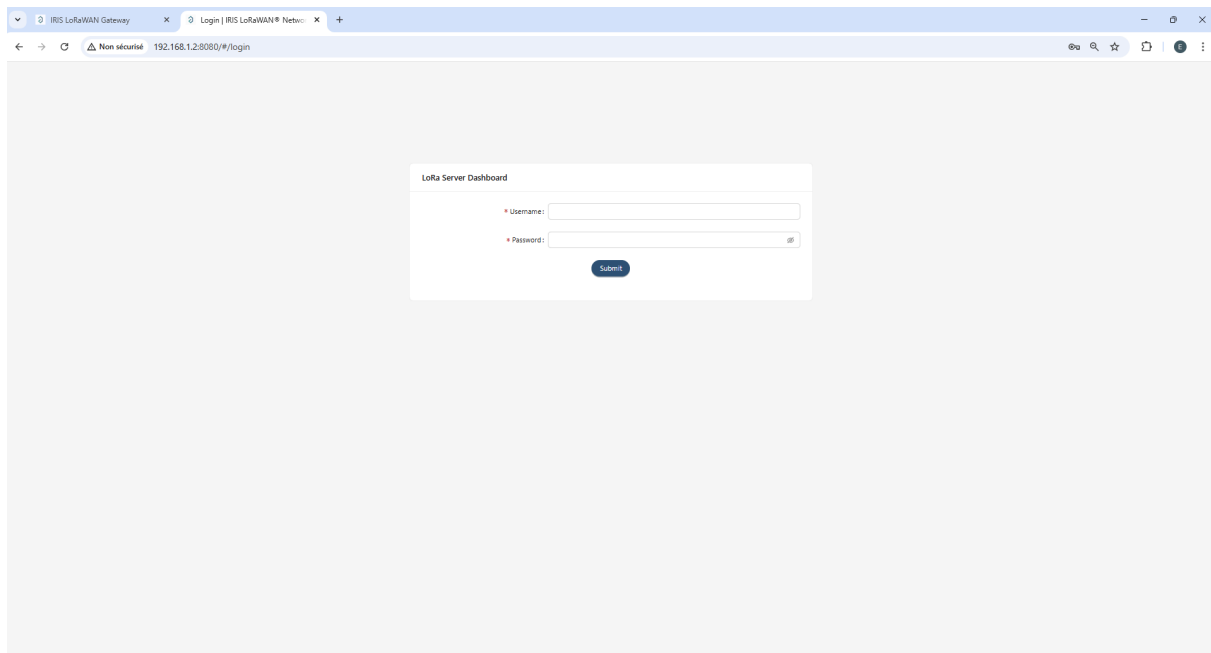
Paramètre	Rôle	Valeur typique
Enable the LoRaWAN Stack	Active la stack LoRaWAN et les réglages associés	Activé
ID	Identifiant unique de la passerelle (EUI-64)	Lecture seule
Keep Alive (s)	Intervalle entre messages heartbeat UDP vers le LNS	10
Stat Interval (s)	Intervalle d'envoi des statistiques passerelle (température, compteurs, RSSI moyen, etc.)	30
Push Timeout (ms)	Temps maximum avant renvoi des données en cas d'erreur. Une valeur trop faible génère des transmissions inutiles	100

Paramètre	Rôle	Valeur typique
Latitude	Coordonnée de latitude (degrés décimaux), optionnel	45.2664
Longitude	Coordonnée de longitude (degrés décimaux), optionnel	5.8906
Altitude	Altitude en mètres, optionnel	1
Net ID	Identifiant réseau LoRaWAN (3 octets hexadécimaux). Utilisé pour construire les DevAddr et pour le roaming. Pour un réseau privé, utiliser 000000. Modifier ce paramètre sur un réseau déjà opérationnel peut nécessiter de reprovisionner les équipements	000000
RX1 Delay (s)	Délai entre l'uplink (classe A) et l'ouverture de la fenêtre RX1 pour recevoir un downlink. Valeur standard : 1. Passez à 2-5 si le chemin réseau/serveur introduit une latence significative. Attention : descendre en dessous de 1 n'est pas conforme LoRaWAN	1
LoRa Server Dashboard Username	Identifiant pour accéder au LoRa Server Dashboard	
LoRa Server Dashboard Password	Mot de passe du LoRa Server Dashboard. Exigences : minimum 10 caractères, avec au moins 1 majuscule et 1 minuscule	

5.6.2. Accéder au serveur LoRaWAN

Une fois le serveur LoRaWAN intégré activé, ouvrez **LoRaWAN** → **Network Server** depuis l'interface web.

Connectez-vous avec les **identifiants du serveur LoRa** que vous venez de configurer.



5.6.3. Tableau de bord du serveur LoRaWAN

Après connexion au serveur LoRaWAN intégré, le tableau de bord s'ouvre dans un nouvel onglet et se compose de :

- une barre supérieure (champ de recherche, fil d'Ariane, sélecteur de tenant, menu utilisateur),
- une barre latérale gauche pour la navigation,
- une zone de travail principale qui change selon la vue sélectionnée.

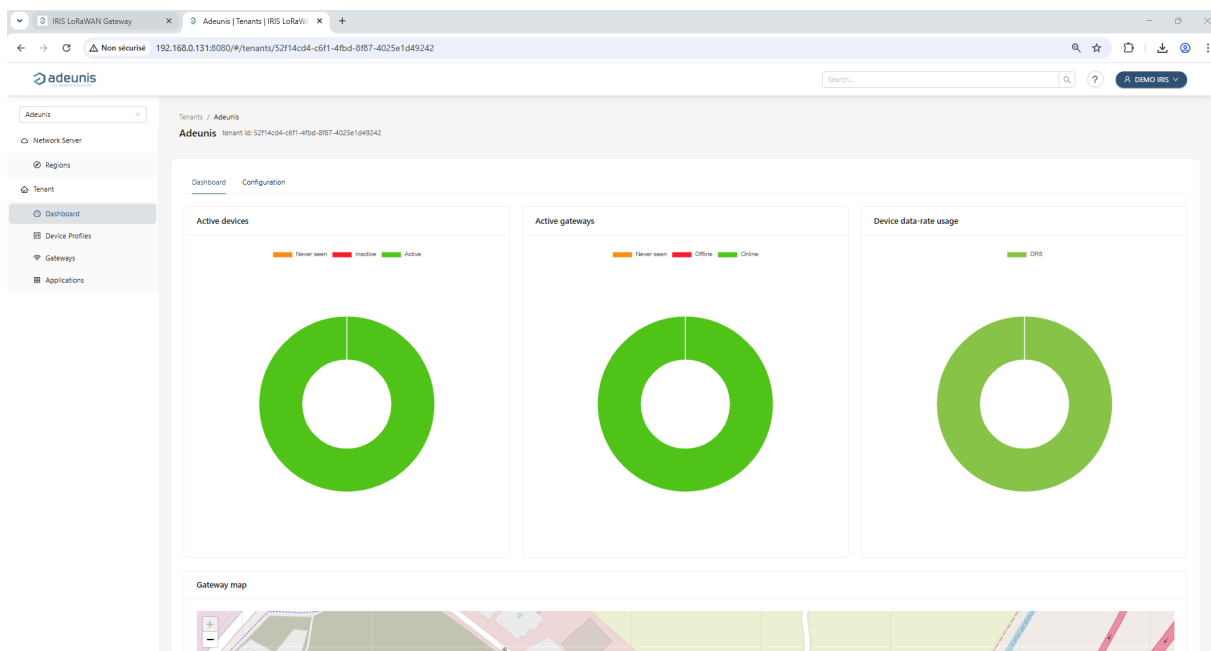


Tableau de bord (Dashboard) :

La vue par défaut fournit un instantané opérationnel pour le tenant sélectionné :

- **Donut "Active devices"** : Active / Inactive / Never seen.
 - **Donut "Active gateways"** : Online (stats récentes), Offline, Never seen.
 - **Device data-rate usage** : répartition des débits (DR) du tenant (utile pour valider l'ADR et la couverture).
 - **Gateway map** : passerelles positionnées sur la carte à partir des coordonnées configurées.
-

Navigation (barre latérale) :

- **Network Server → Regions** : liste la/les région(s) LoRaWAN activée(s) sur le serveur (EU868 sur cet équipement).
- **Tenant** : espace de travail isolé qui regroupe applications, équipements et passerelles. **Dashboard** présente l'état de santé ; **Configuration** regroupe les options de base du tenant.
- **Device profiles** : bibliothèque de profils (région, paramètres LoRaWAN/MAC, politique ADR, mode de join, classe, codec/mappings). IRIS fournit des profils préchargés que vous pouvez réutiliser ou dupliquer.
- **Gateways** : passerelles enregistrées pour ce tenant (statut, dernière activité, localisation).
- **Applications** : conteneurs logiques pour les équipements et l'acheminement des données ; c'est ici que vous ajoutez les équipements et configurez les intégrations.

5.6.4. Gérer un parc de passerelles

Cette page permet de gérer les passerelles LoRaWAN enregistrées dans le tenant lorsque le serveur réseau intégré est utilisé.

La passerelle IRIS qui exécute le LNS intégré est **pré-enregistrée automatiquement**. Elle représente la radio locale et **ne doit pas être supprimée**.

Ajoutez ensuite, si besoin, d'autres passerelles qui remontent leurs trames vers ce serveur via le **Packet Forwarder Semtech UDP**.

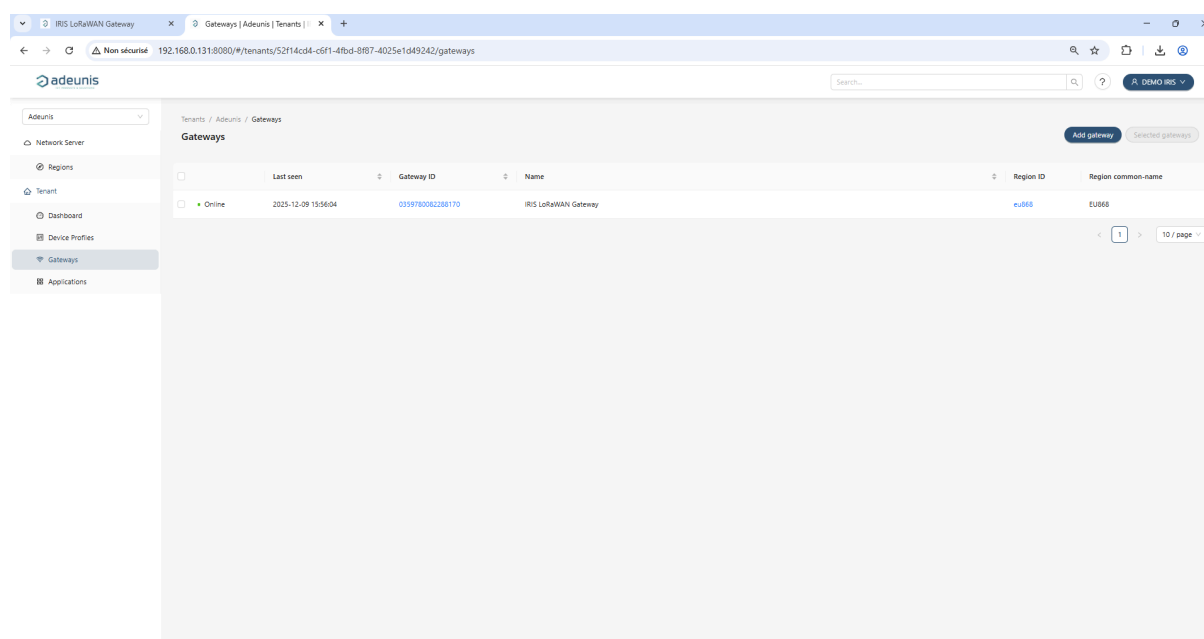
Liste de passerelles

La liste affiche une ligne par passerelle, avec une recherche et des actions groupées en haut.

Colonnes :

- **Last seen** (avec états Online/Offline/Never-seen).
- **Gateway ID** (EUI-64, cliquable).
- **Name**.
- **Region ID**.
- **Region common-name**.

La passerelle **IRIS** qui exécute le serveur LoRaWAN intégré apparaît **déjà** dans la liste. **Ne la supprimez pas**.



Cliquer sur **Gateway ID** ouvre la page de détails de la passerelle.

Ajouter une passerelle Packet Forwarder UDP externe

Allez dans **Tenant** → **Gateways** → **Add gateway**.

L'enregistrement d'une passerelle qui envoie ses trames vers ce serveur via UDP se fait en trois onglets :

1. Onglet : General

- **Name** (obligatoire) et **Description** (texte libre).

- **Gateway ID (EUI-64)** (obligatoire). Vous pouvez basculer l'ordre des octets **MSB/LSB** et utiliser l'icône d'**inversion** si l'EUI est fourni en LSB-first ; l'icône **copy** copie la valeur. **Cette valeur doit correspondre exactement à l'EUI configuré sur la passerelle physique.**
- **Stats interval (secs)** (obligatoire) : périodicité attendue des statistiques/heartbeats (typique **30 s**). Ce réglage **ne pousse rien** vers la passerelle ; il doit correspondre à l'intervalle configuré sur la passerelle. Des intervalles courts augmentent le trafic de supervision ; des intervalles longs retardent la détection Online/Offline.
- Cliquez sur **Submit**.

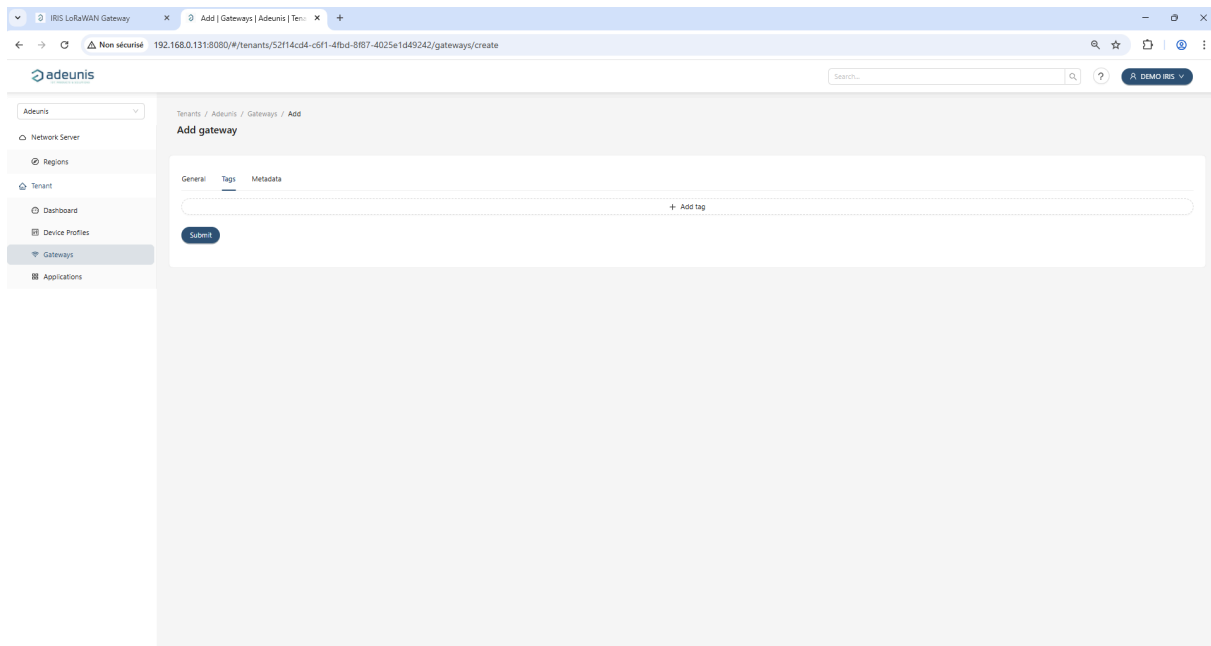
The screenshot shows the 'Add gateway' form in the Adeunis interface. The form is divided into three tabs: General, Tags, and Metadata. The General tab is selected, displaying the following fields:

- Name:** A text input field.
- Description:** A text input field.
- Gateway ID (EUI64):** A text input field with a dropdown menu set to 'MSB' and an 'inversion' icon.
- Stats interval (secs):** A text input field with the value '30'.
- Location:** A map area with a blue location pin and a 'Set to current location' button.

A 'Submit' button is located at the bottom left of the form.

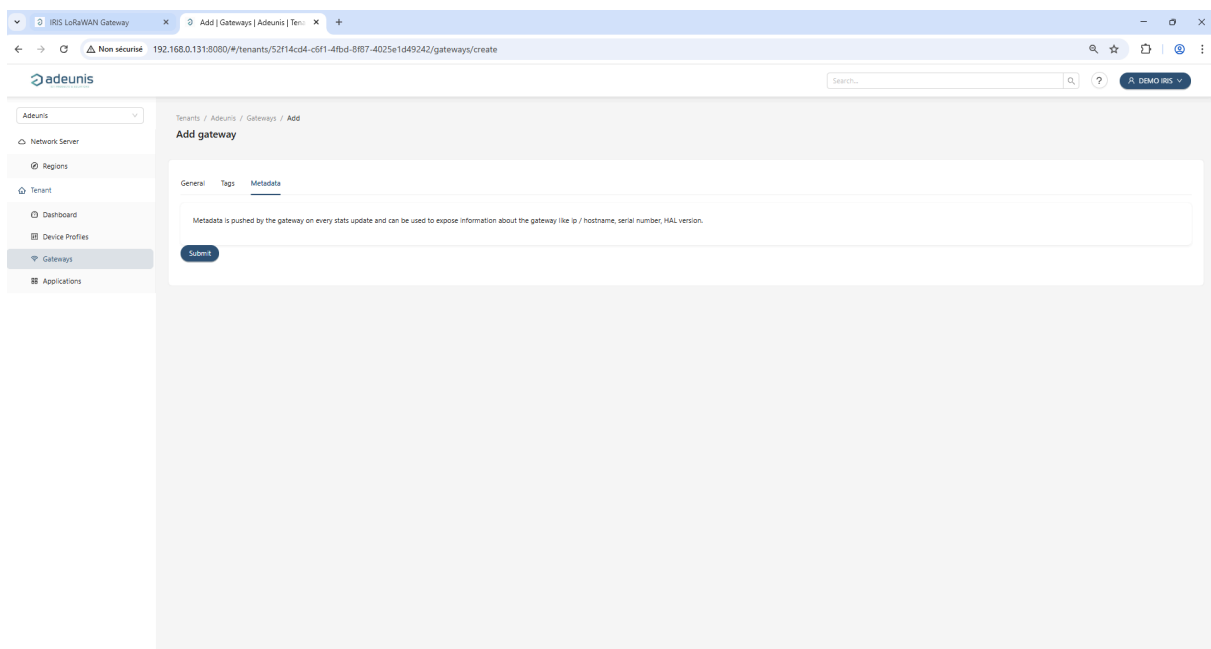
2. Onglet : Tags

Tags clé-valeur pour faciliter la recherche et certaines intégrations (ex. `site=BuildingA`, `backhaul=LTE`). Ils **n'influencent pas** le comportement radio.



3. Onglet : Metadata

Lecture seule. La passerelle envoie des métadonnées avec chaque heartbeat/stat ; le serveur les affiche et les associe aux événements.



Contrôles rapides (si une nouvelle passerelle reste en "Never seen")

- Le **gateway_ID** dans le JSON du packet forwarder correspond **exactement** au **Gateway ID (EUI64)** déclaré.

- Le `server_address` pointe bien vers l'**IP de l'IRIS** qui exécute le LNS intégré.
- Le port UDP **1700** (uplink & downlink) est autorisé de bout en bout.
- Les paramètres régionaux de la passerelle physique correspondent au déploiement (ex. **EU868**).

Gérer les passerelles existantes

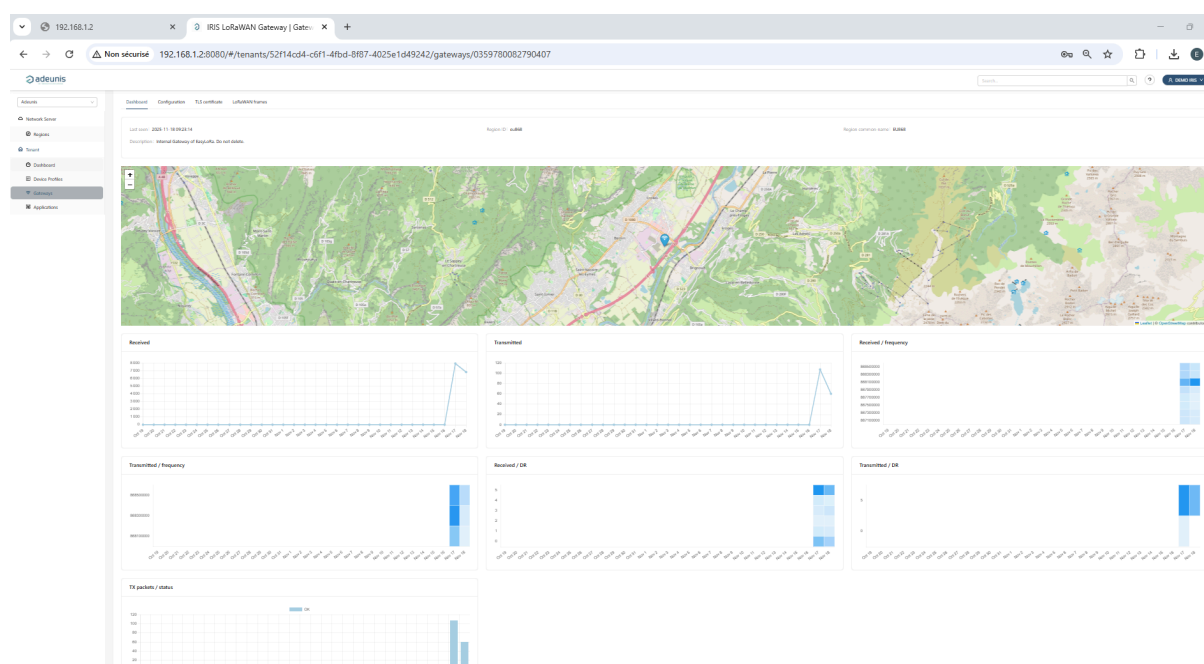
Cliquez sur un **Gateway ID** dans la liste pour ouvrir la page de détails.

L'en-tête affiche **Name** et **Gateway ID (EUI-64)** ainsi que **Delete gateway**.

Actions disponibles dans le détail d'une passerelle :

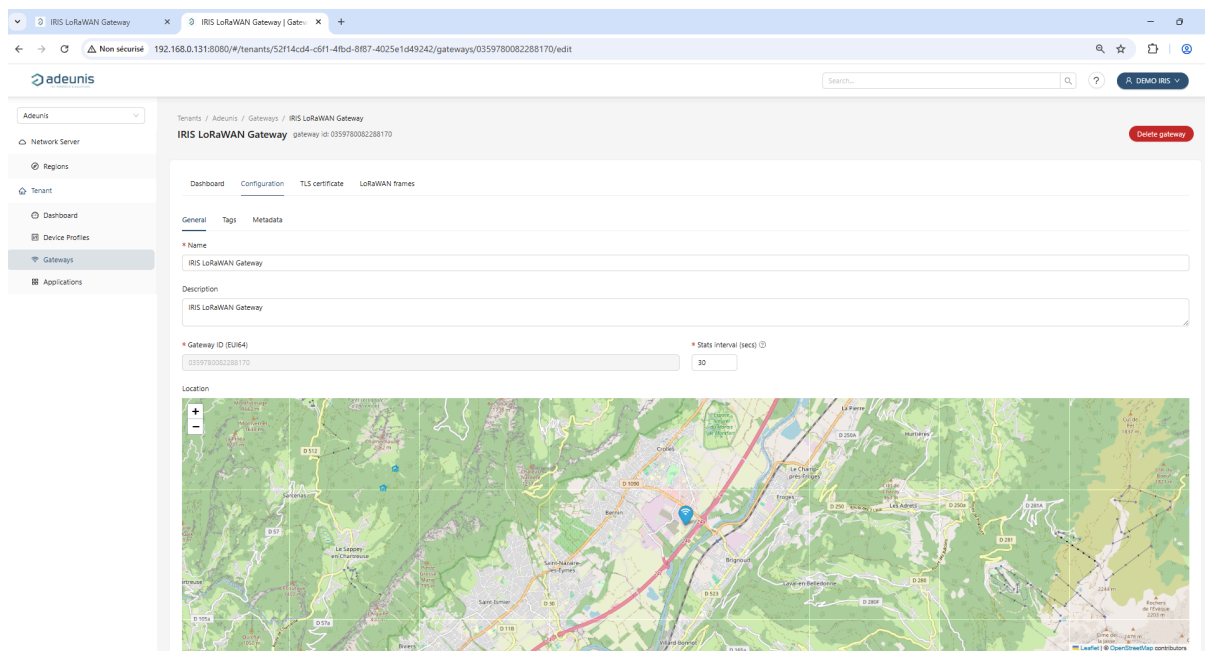
- **Onglet Dashboard**

Résumé opérationnel avec **carte** et graphiques (uplinks "Received", downlinks "Transmitted", distributions de fréquences et de DR, statut TX, etc.).



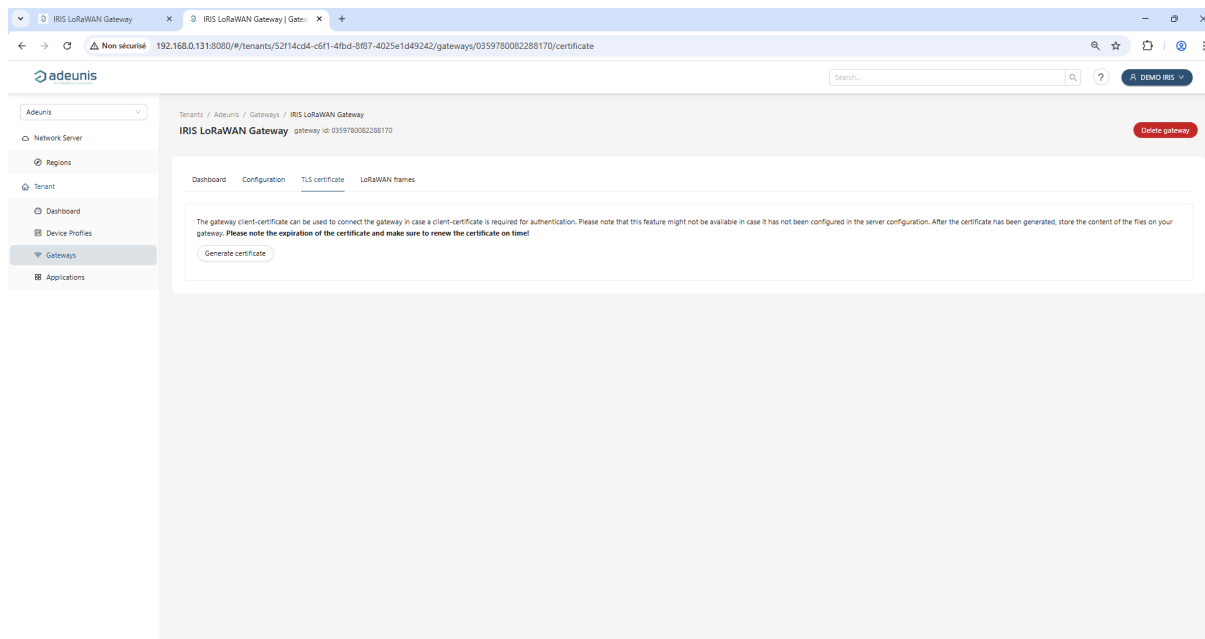
- **Onglet Configuration**

Modification du nom/de la description/de la région et de certains paramètres spécifiques.



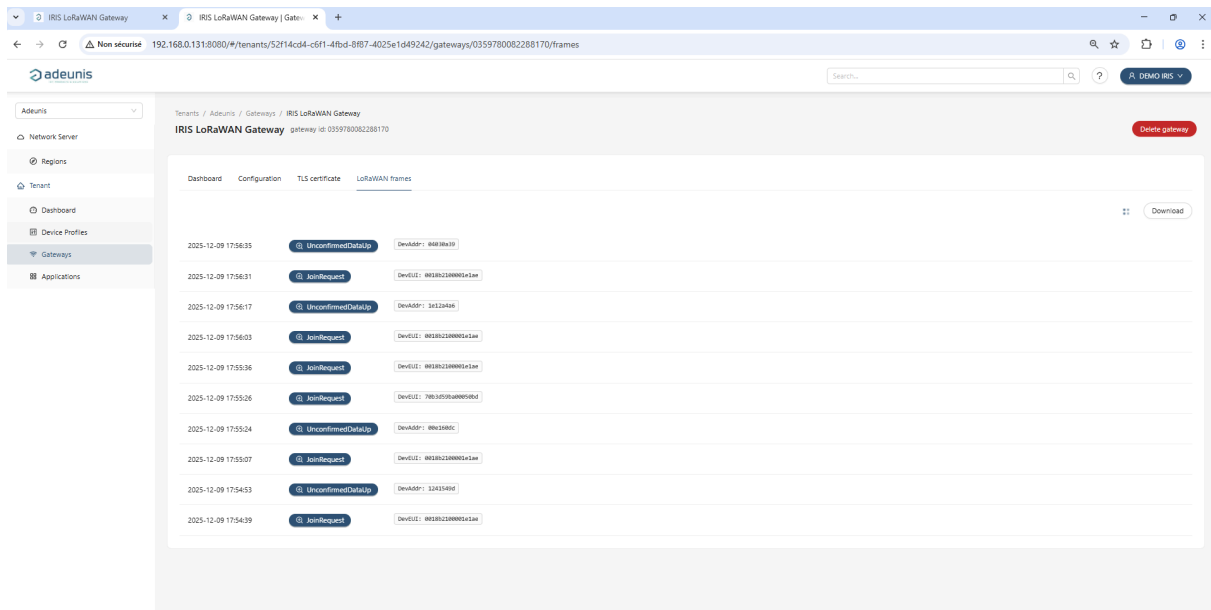
- **Onglet TLS Certificate : non pris en charge dans cette version**

Le serveur réseau intégré accepte uniquement des passerelles via **Semtech UDP Packet Forwarder**. **Basics Station (WS/WSS)** et l'**authentification par certificat client** ne sont pas **disponibles** à ce stade. Si l'onglet apparaît dans l'interface, il est informatif : ne pas l'utiliser.

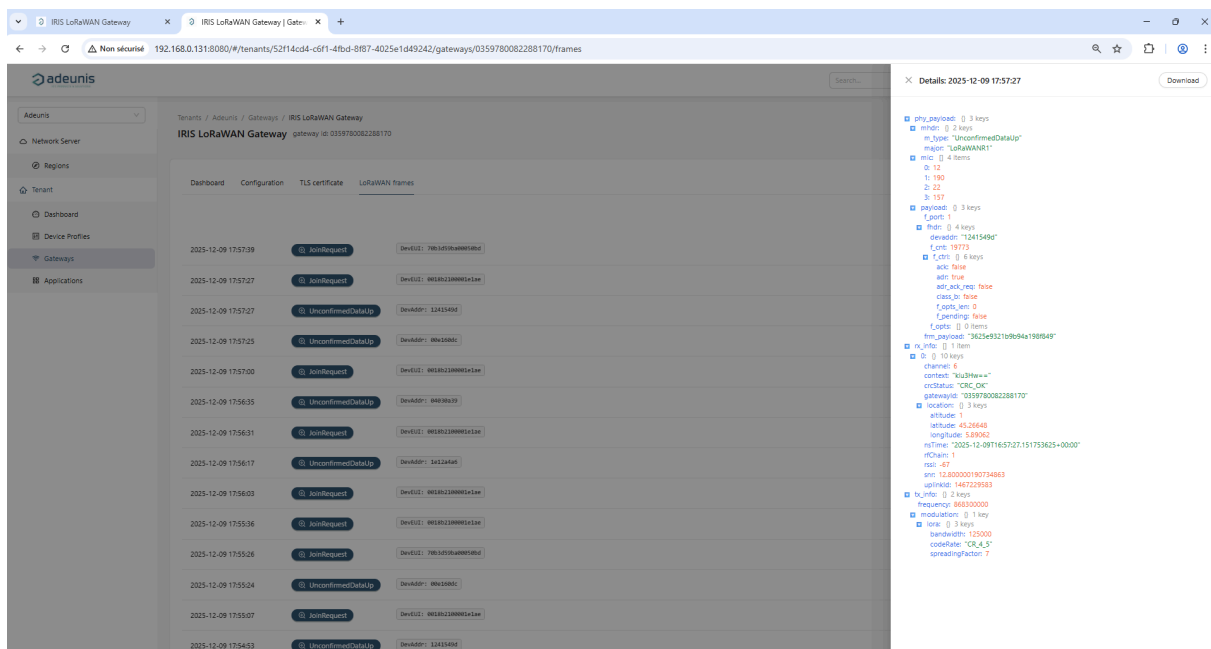


- **Onglet LoRaWAN frames**

Liste des trames RX/TX pour le diagnostic.



Cliquez sur une trame pour afficher les **détails complets** (MHDR, DevAddr, FCnt, DR, fréquence, MIC, etc.) et utilisez **Download** pour exporter la liste.



Une fois que vous avez vérifié que le tenant et la/les passerelle(s) sont enregistrés et en état correct, l'étape suivante est de **créer une Application**.

Une Application est l'espace qui regroupe vos profils d'équipements et vos équipements, et qui définit comment les données (décodées ou non) sont routées vers l'aval.

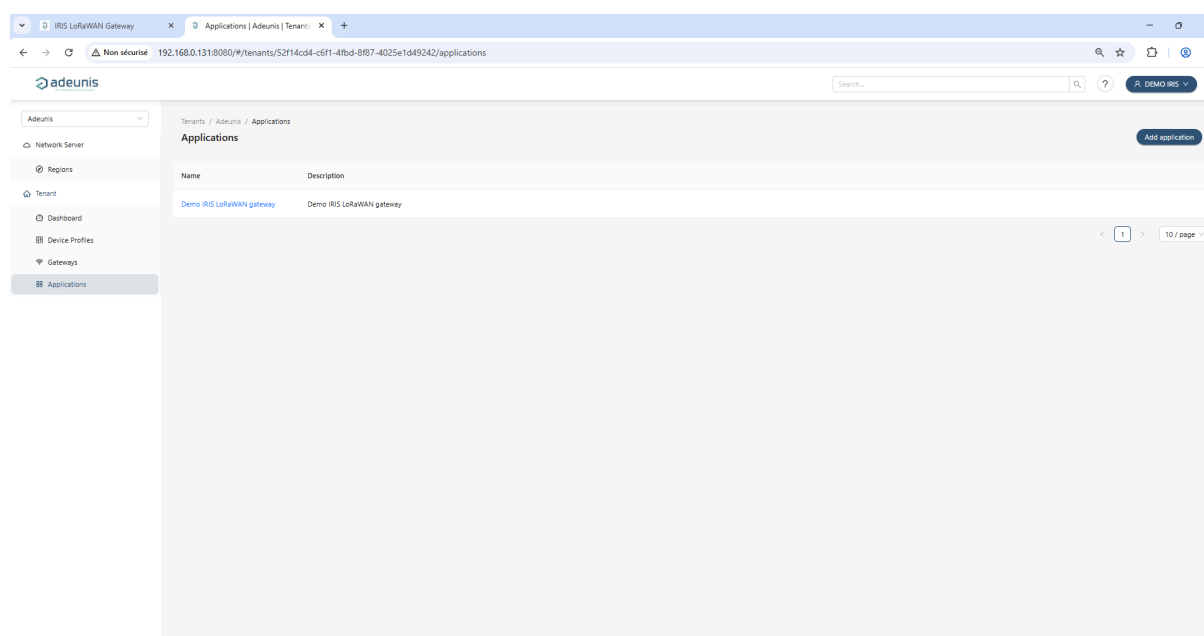
Créez une application par projet/site (ou domaine métier), puis ajoutez un **Device Profile** et enregistrez des **Devices** dans cette Application. Vous pourrez ensuite valider les joins, décoder les payloads et configurer l'intégration MQTT(s)/HTTP(s).

5.6.5. Gérer les applications

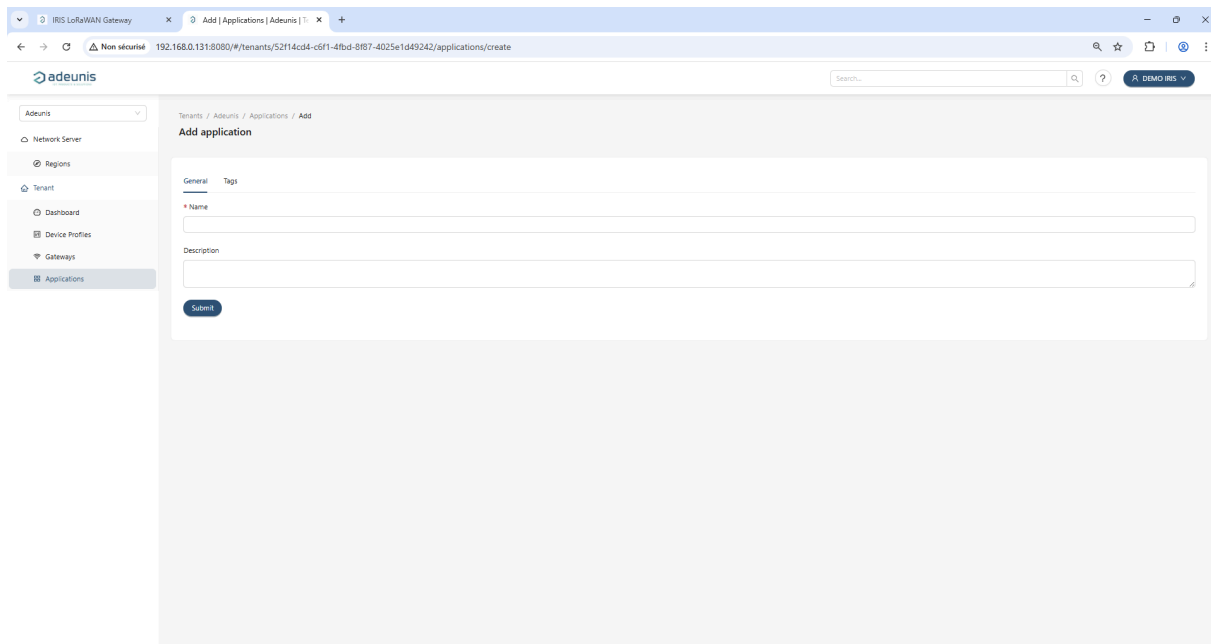
Une application regroupe des équipements LoRaWAN généralement par usage, localisation ou type, et achemine leurs données vers un même serveur.

Créer une nouvelle application

1. Dans le tableau de bord, allez dans **Applications** → **Add application**.



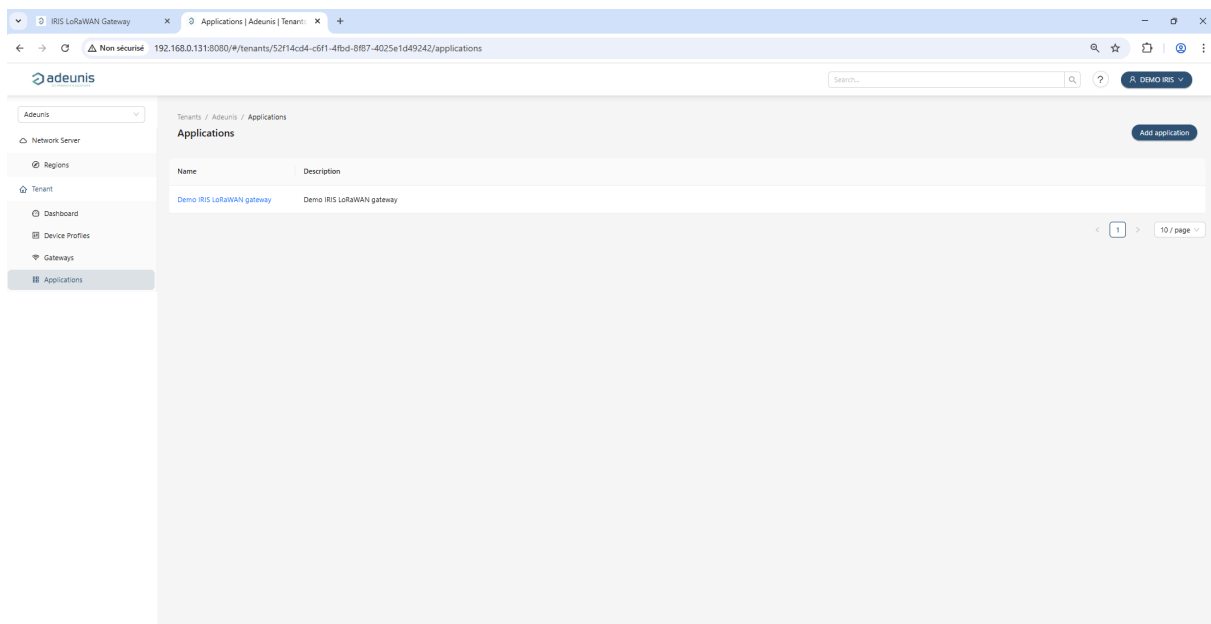
2. Renseignez **Name** et **Description** (ex. « Siège Social – Capteurs de température »).
3. (Optionnel) Ajoutez des **Tags** pour la recherche et les intégrations (ex. Bâtiment 1).



4. Créez l'application.

Gérer des applications existantes

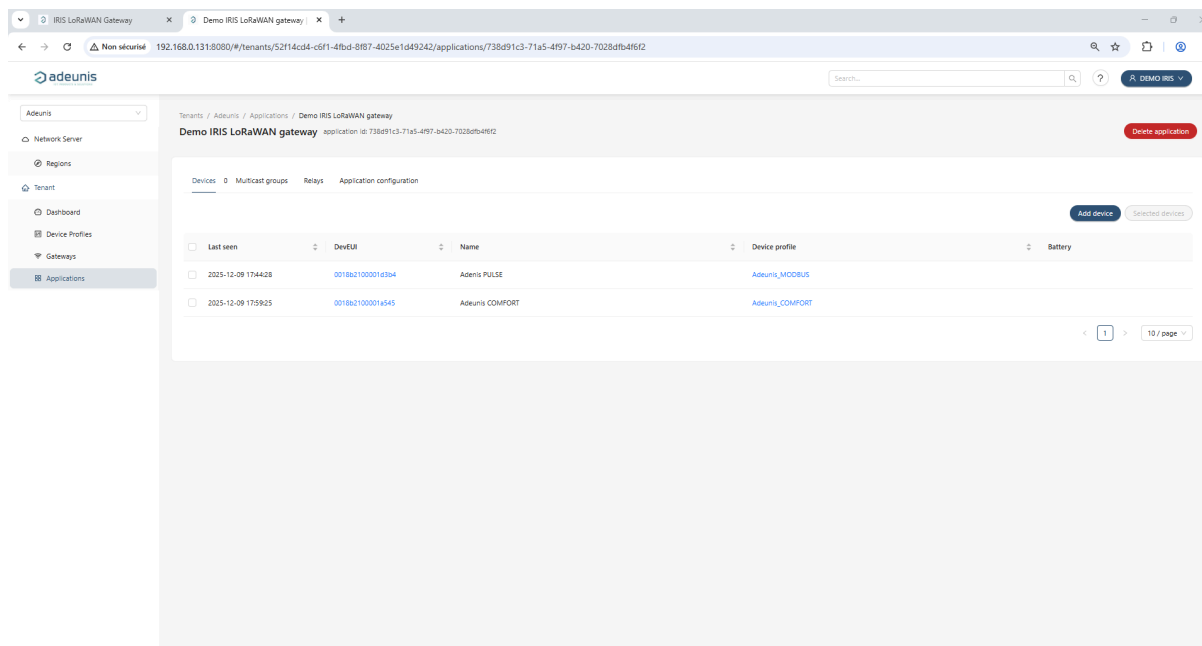
Une fois l'application créée, cliquez sur son nom dans **Tenant** → **Applications** pour ouvrir les **Application details**.



L'en-tête affiche le nom de l'application "**Application Name**" et son identifiant "**Application ID**"; le nom de l'application est utile lors d'un import en masse (CSV/JSON), car la colonne

`applicationName` doit référencer cette valeur.

Vous pouvez aussi supprimer l'application "**Delete application**" depuis cette page si nécessaire (cette action ne supprime pas les équipements présents dans d'autres applications).



Depuis les **Application details**, vous pouvez :

- Onglet **Devices** : consulter la liste des équipements associés (Last seen, DevEUI, Name, Device profile, Battery), **ajouter un équipement** (Add device) et utiliser des actions de masse via **Selected devices**.
- Onglet **Multicast groups** : créer et gérer des groupes multicast (Add multicast-group), affecter des équipements et planifier des downlinks multicast (Class-C, fréquence, DR, compteurs).
- Onglet **Relays** : gérer les nœuds relais et les équipements opérant via un relais.
- (Optionnel) Onglet **Application configuration** : ajuster des paramètres communs s'appliquant à tous les équipements de l'application.



La configuration de l'envoi des données vers un serveur applicatif via MQTT/s ou HTTP/s est détaillée dans le [chapitre suivant](#)

Une fois l'application créée, vous avez défini où vos équipements "vivent" et comment les données seront acheminées. L'étape suivante consiste à décrire à quoi ressemble chaque famille d'équipements sur le réseau. Créez un profil d'équipement **"Device Profile"** regroupant les spécifications LoRaWAN (région/MAC), les fenêtres RX, la politique ADR, le **codec** et la cartographie des mesures utilisée par votre famille de capteurs. Vous associerez ce profil lors de l'enregistrement des équipements.

5.6.6. Gérer les profils d'équipements (Device Profiles)

Un **profil d'équipement** décrit la manière dont une famille d'équipements communique sur le réseau : version LoRaWAN/MAC, classe LoRaWAN, méthode d'activation (OTAA/ABP), fenêtres RX, ADR et codec.

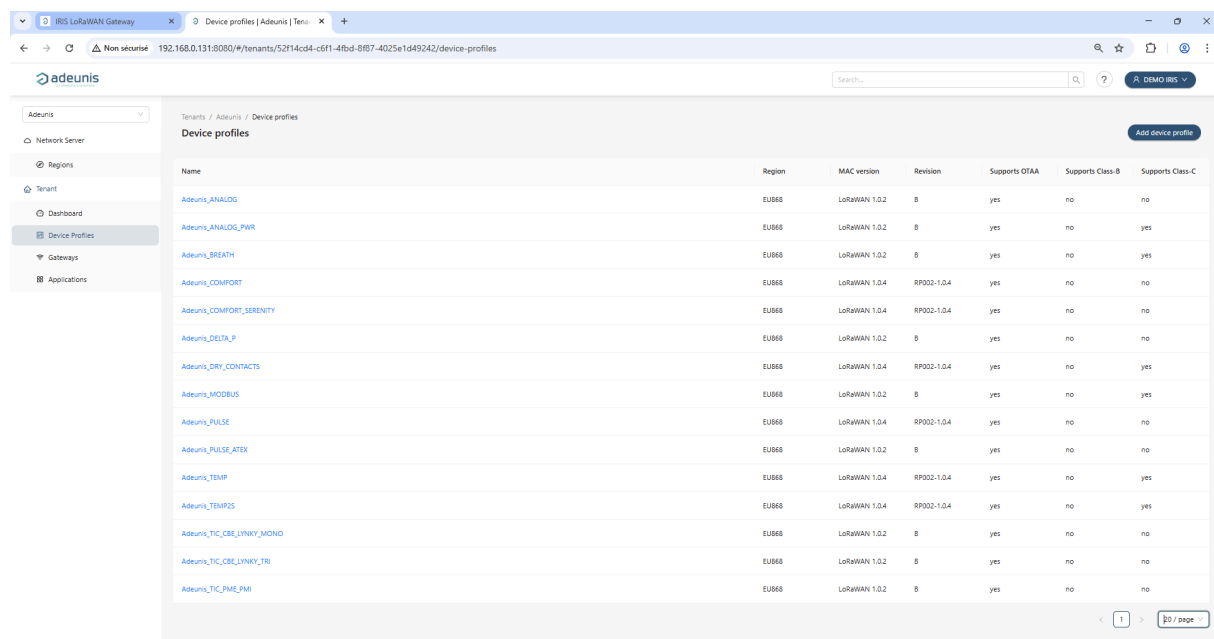
Tout capteur enregistré sur la passerelle doit être associé à un profil. Le serveur intégré s'en sert pour interpréter les uplinks, mettre en file les downlinks et afficher les mesures.

Ces informations proviennent de la documentation du fabricant et doivent correspondre au firmware du capteur.

Profils d'équipements pré-chargés

La passerelle IRIS est livrée avec des **profils préchargés pour les équipements Adeunis**.

Vous pouvez les utiliser tels quels ou les dupliquer comme modèles.



Name	Region	MAC version	Revision	Supports OTAA	Supports Class-B	Supports Class-C
Adeunis_ANALOG	EU868	LoRaWAN 1.0.2	8	yes	no	no
Adeunis_ANALOG_PRR	EU868	LoRaWAN 1.0.2	8	yes	no	yes
Adeunis_BREATH	EU868	LoRaWAN 1.0.2	8	yes	no	yes
Adeunis_COMFORT	EU868	LoRaWAN 1.0.4	RP002-1.0.4	yes	no	no
Adeunis_COMFORT_SERENITY	EU868	LoRaWAN 1.0.4	RP002-1.0.4	yes	no	no
Adeunis_DELTA_P	EU868	LoRaWAN 1.0.2	8	yes	no	no
Adeunis_DRY_CONTACTS	EU868	LoRaWAN 1.0.4	RP002-1.0.4	yes	no	yes
Adeunis_MODBUS	EU868	LoRaWAN 1.0.2	8	yes	no	yes
Adeunis_PULSE	EU868	LoRaWAN 1.0.4	RP002-1.0.4	yes	no	no
Adeunis_PULSE_ATEX	EU868	LoRaWAN 1.0.2	8	yes	no	no
Adeunis_TEMP	EU868	LoRaWAN 1.0.4	RP002-1.0.4	yes	no	yes
Adeunis_TEMP25	EU868	LoRaWAN 1.0.4	RP002-1.0.4	yes	no	yes
Adeunis_TIC_CBE_LYNKY_MONO	EU868	LoRaWAN 1.0.2	8	yes	no	no
Adeunis_TIC_CBE_LYNKY_TRI	EU868	LoRaWAN 1.0.2	8	yes	no	no
Adeunis_TIC_PME_PMI	EU868	LoRaWAN 1.0.2	8	yes	no	no

Créer un nouveau profil d'équipement

Pour d'autres fabricants, **créez un nouveau profil d'équipement** correspondant à chaque famille de capteurs déployée.

Pour en créer un :

1. Ouvrez le tableau de bord puis allez dans **Device profiles** → **Add device profile**.
2. Renseignez les 7 onglets décrits ci-dessous.
3. Puis cliquez sur **Submit**.

The screenshot shows the 'Add device profile' form in the Adeunis interface. The form is divided into several sections. The 'General' tab is selected, showing fields for Name, Description, Region (EU868), Region configuration, MAC version (LoRaWAN 1.0.3), Regional parameters version (A), ADR algorithm (Default ADR algorithm (LoRa only)), Flush queue on activate (checked), Allow roaming (unchecked), Expected uplink interval (secs) (1800), Device status request frequency (req/day) (1), and EUI Delay (secs) (0). A 'Submit' button is located at the bottom left of the form.

Onglet : General

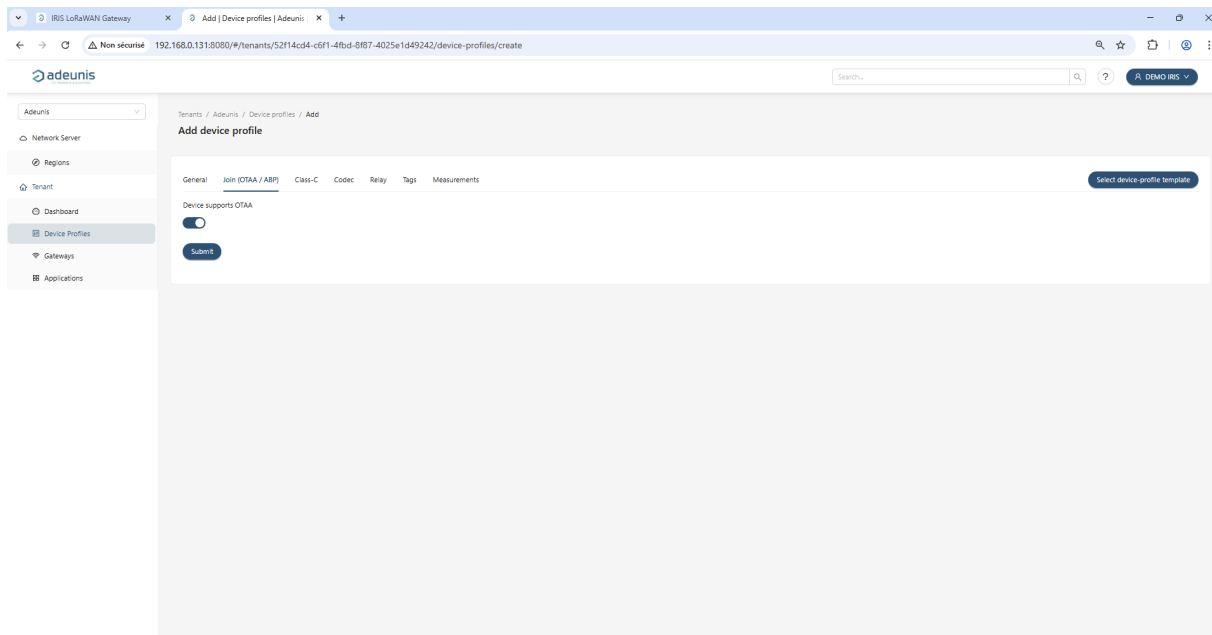
Cet onglet définit la base du profil pour un type d'équipement.

The screenshot shows the 'Add device profile' form in the Adeunis interface. The form is divided into several sections with tabs for General, Join (OTAA / ABP), Class-C, Codec, Relay, Tags, and Measurements. The General tab is active, showing fields for Name, Description, Region, MAC version, Region configuration, Regional parameters revision, ADR algorithm, Flush queue on activate, Allow roaming, Expected uplink interval, Device-status request frequency, and RX1 Delay. The form is designed for creating a new device profile, with a 'Submit' button at the bottom.

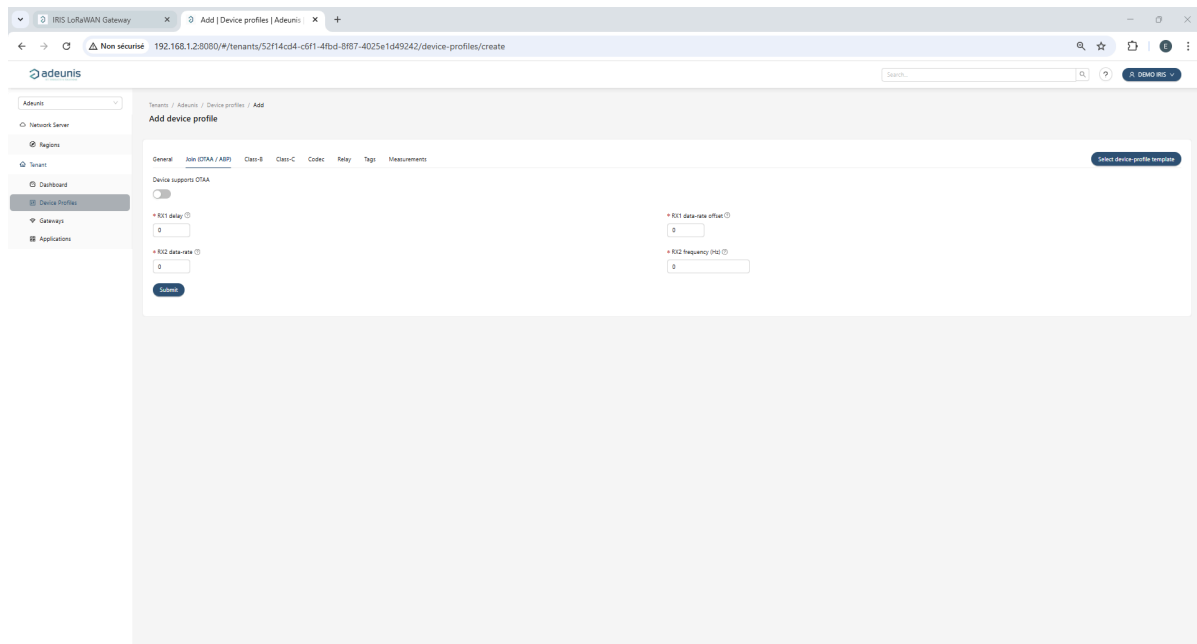
- Donnez au profil un nom **"Name"** clair et unique (ex. « Capteur de mouvement-PIR-EU868-ClassA-1.0.2 »)
- (Optionnel) Renseignez une **Description** pour contextualiser le profil
- **Region** : **EU868** (fixé pour IRIS).
- **MAC version** : version LoRaWAN utilisée par l'équipement (ex. 1.0.2, 1.0.3).
- **Region configuration / Regional parameters revision** : sélectionnez la révision correspondant à l'équipement (ex. *RP002-1.0.x / A*).
- **ADR algorithm** : conservez **Default ADR (LoRa only)** sauf besoin spécifique.
- **Flush queue on activate** : **On** recommandé (efface les downlinks obsolètes lorsqu'un équipement (re)join).
- **Allow roaming** : laissez **Off** sauf si vous opérez avec des accords de roaming.
- **Device-status request frequency (req/day)** : fréquence à laquelle le serveur demande un statut (batterie, marge). 0 = désactivé.
- **Expected uplink interval (sec)** : **important pour la vue santé/statut**. Renseignez un intervalle réaliste (ex. 3600 pour un capteur horaire) afin que le tableau de bord puisse signaler les uplinks manquants.

Onglet : Join

Cet onglet définit comment les équipements utilisant ce profil seront activés.



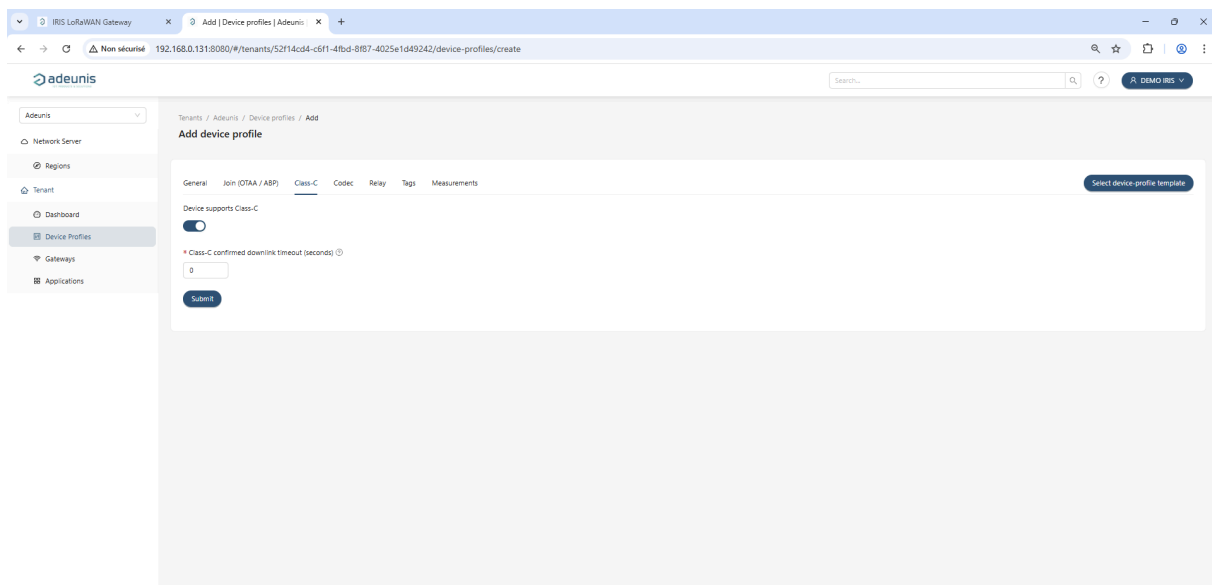
- **Device supports OTAA : On** pour OTAA (recommandé). **Off** bascule vers un comportement ABP.
- **OTAA Enabled :**
 - L'équipement s'active via un join sécurisé. Lors de la création de chaque équipement, les identifiants OTAA doivent être fournis.
 - Avantages : clés de session dynamiques, sécurité plus élevée, changements réseau et reprovisionnement plus simples.
- **ABP Enabled :**
 - Le profil utilise ABP. Lors de la création de l'équipement, des clés fixes doivent être renseignées.
 - Avantages : démarre sans procédure de join.
 - Inconvénients : moins sécurisé, clés non renouvelées automatiquement, plus sensible à une désynchronisation des compteurs de trames.



- **RX1 delay** : secondes avant l'ouverture de RX1. Laissez **0** pour utiliser les valeurs réseau par défaut, sauf exigence spécifique de l'équipement.
- **RX1 data-rate offset** : laissez **0** sauf indication du fabricant.
- **RX2 data-rate / RX2 frequency (Hz)** : laissez **0** pour utiliser les valeurs EU868 par défaut, ou définissez des valeurs explicites si l'équipement l'exige.

Onglet : Class-C (optionnel)

La classe C maintient les fenêtres de réception (RX) ouvertes presque en continu, en les fermant uniquement lors de la transmission uplink. C'est adapté aux actionneurs qui doivent recevoir des commandes à tout moment avec une faible latence, au prix d'une consommation plus élevée.

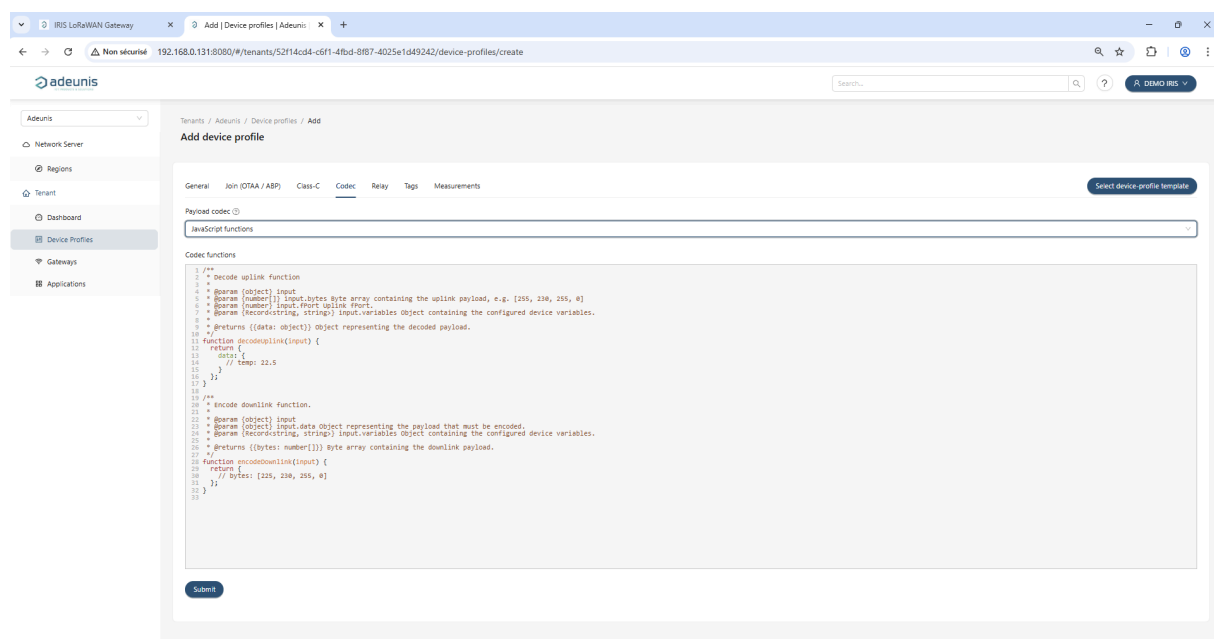


- **Device supports Class-C** : n'activez que pour des équipements alimentés et conçus pour la classe C.
- **Class-C confirmed downlink timeout (s)** : durée pendant laquelle le serveur attend l'ACK d'un downlink confirmé en classe C.

Onglet : Codec

Cet onglet définit comment le serveur interprète les octets reçus (uplinks) et, éventuellement, comment il génère des octets pour les transmissions (downlinks).

Si vous avez besoin de valeurs décodées dans le tableau de bord ou pour le routage, ajoutez un **payload codec**.



Choisissez comment les payloads sont décodés/encodés :

1. **None** : payloads bruts uniquement.

Le payload est conservé comme un tableau d'octets, avec une représentation en base64/Hex selon l'intégration.

Quand utiliser cette option :

- pour des tests initiaux,
- quand le serveur applicatif décode le payload indépendamment,
- pour des équipements aux formats propriétaires qui ne peuvent pas être décodés côté serveur.

2. **Cayenne LPP** : décodage conforme au standard LPP.

Le payload est décodé automatiquement selon le standard Cayenne Low Power Payload (LPP).

Quand utiliser cette option :

- si votre équipement utilise LPP.

3. **JavaScript functions** : permet d'écrire deux fonctions JavaScript :

- `decodeUplink(input)` → convertit des octets en JSON
- `encodeDownlink(input)` → convertit du JSON en octets

Quand utiliser cette option :

- pour des formats de payload propriétaires.



Conservez tous les décodeurs sous contrôle de version et notez l'association **profil** → **codec** dans votre dossier de site.

Onglet : Relay (avancé)

LoRaWAN prend en charge un mode Relay (répéteur intelligent) pour étendre la couverture sans installer une passerelle supplémentaire.

Un relais écoute des équipements à proximité et relaie leurs trames vers le réseau ; inversement, il peut délivrer des downlinks à ces équipements.

Cet onglet définit les paramètres des fonctionnalités **LoRaWAN Relay**.

Sauf si vous déployez des relais, **laissez tout désactivé**.

The screenshot shows the 'Add device profile' page in the Adeunis LoRaWAN Gateway web interface. The 'Relay' tab is selected, displaying various configuration options for relay functionality. The form includes sections for general settings, channel configuration, and rate limits. Key options include 'Relay enabled', 'Device is a Relay', and 'Only use Relay (end-device)'. There are also input fields for 'Default channel index', 'Second channel frequency (Hz)', 'Second channel data rate', 'Second channel ACK offset', 'CAD periodicity', 'End-device activation mode', 'Smart enable level', 'Back-off', and several limit bucket sizes and rates. A 'Submit' button is located at the bottom left of the form.

- **Device is a Relay** : activez uniquement pour de véritables équipements relais.

L'équipement agira comme intermédiaire entre d'autres end-devices et le réseau.

Il doit être placé là où la couverture vers la passerelle est bonne, et à proximité des équipements qui en dépendent.

- **Device is a Relay-capable end-device** : pour des équipements utilisant un chemin via relais.

Cette option doit être activée lorsque le profil concerne un équipement capable d'opérer via un relais au lieu de communiquer directement avec la passerelle.

L'équipement et le relais doivent partager une configuration compatible (paramètres régionaux, fenêtres RX, etc.).

- **Champs supplémentaires** (second channel, CAD periodicity, back-off, bucket sizes) : réglages fins du comportement relais ; conservez les valeurs par défaut si vous n'êtes pas sûr.

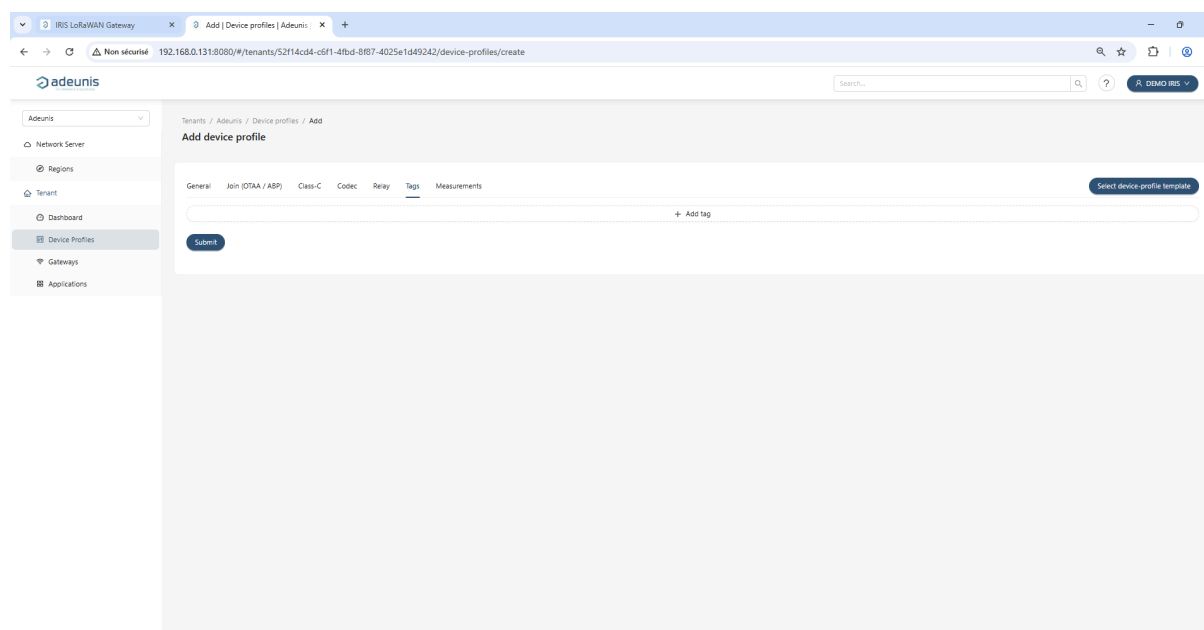
Onglet : Tags

Les tags sont des métadonnées clé-valeur.

Les tags définis dans un profil d'équipement s'appliquent à tous les équipements utilisant ce profil.

Ils sont utiles pour :

- la recherche : filtrer les équipements dans le tableau de bord par modèle, vertical, etc.
- le routage : les tags sont envoyés avec les événements équipements
- les tableaux de bord : regrouper par modèle, site, client, etc.

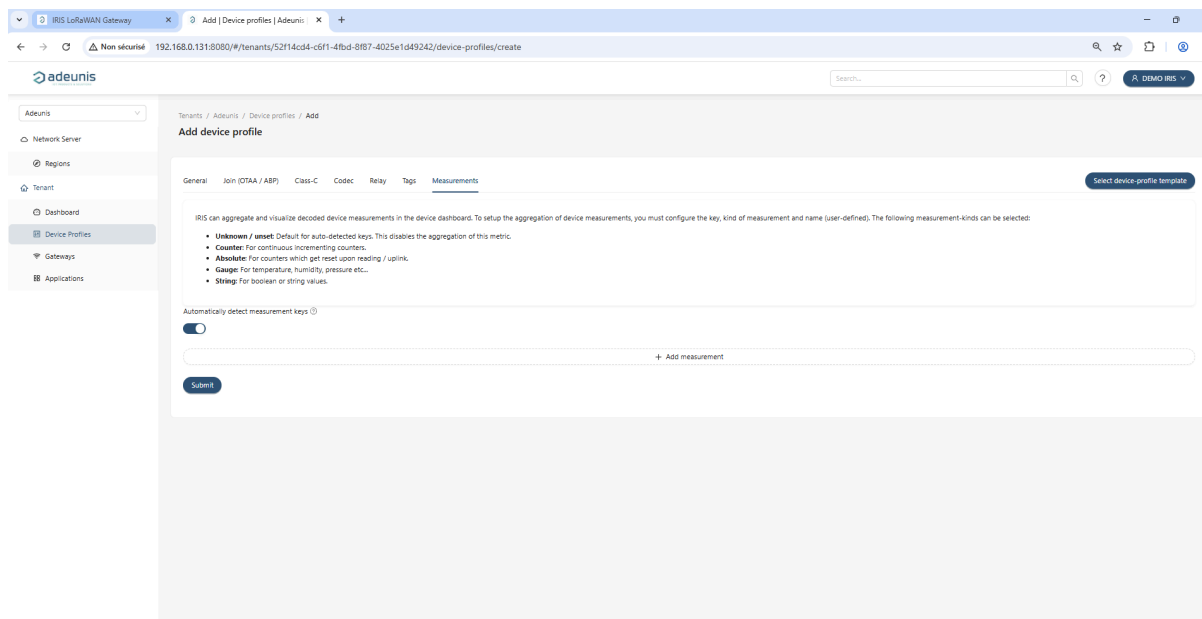


- Cliquez sur **Add Tag** pour créer des paires Key/Value

- Ajoutez autant de tags que nécessaire (ex. `site=BatA` , `scenario=energie`).

Onglet : Measurements

Cet onglet définit quelles clés décodées doivent être agrégées et comment elles sont interprétées et affichées dans les tableaux de bord et les requêtes.



- Les mesures sont lues à partir de l'objet `data` renvoyé par la fonction `decodeUplink()` lorsqu'un codec JavaScript est utilisé. Par exemple, si la fonction renvoie `{ data: { temperature: 21.7, batt: 3.92, pulses: 15 } }`, vous pouvez mapper `temperature`, `batt` et `pulses`.
- **Automatically detect measurement keys** : si activé, la passerelle IRIS "apprend" les clés vues dans les payloads décodés et les traite comme des métriques de type "Unknown". C'est pratique pour démarrer vite, mais nous recommandons de le désactiver et de définir les métriques manuellement pour éviter le bruit.
- **Manual entries** : ajoutez des lignes pour définir la Key, le Kind et le Name de chaque mesure d'intérêt.
 - **Measurement Key** : clé JSON exacte produite par votre codec (`temperature` , `kWh` , `state` , ...)
 - **Measurement Kind** : type de métrique (mode d'agrégation) – `Counter` (monotone), `Absolute` (remise à zéro), `Gauge` (ex. °C, %RH), ou `String`
 - **Measurement Name** (optionnel) : libellé "friendly" utilisé dans le tableau de bord (ex. « Ambient temperature »)

Si l'auto-détection est activée, vous pouvez quand même ajouter des lignes explicites pour les métriques critiques afin de contrôler leur type et leur libellé.

Types de mesures (kind)

Metric	Usage	Exemple
Unknown / Unset	Pas d'agrégation. Utile pour des valeurs que vous ne souhaitez pas grapher ou sommer	"Motion Sensor-PIR-EU868-ClassA-1.0.2"
Counter	Compteur cumulatif qui ne diminue jamais ; la plateforme calcule les incréments entre lectures	Compteurs d'impulsions, énergie
Absolute	Compteur remis à zéro après chaque uplink ou périodiquement ; la valeur absolue reportée est utilisée	Événements par message
Gauge	Mesures instantanées, agrégées en moyenne/min/max sur des intervalles	Température, humidité, pression, batterie, RSSI, etc.
String	Valeurs booléennes ou texte, non agrégées numériquement ; affichées comme dernière valeur connue	Statut, alarme



Gardez les clés de mesure strictement identiques à celles du codec (sensible à la casse).

Référence rapide des paramètres

Onglet General

Champ	Rôle	Valeur typique
Name / Description	Identifier le profil	"Motion Sensor-PIR-EU868-ClassA-1.0.2"
Region	Région radio	EU868
MAC version	Spécification LoRaWAN du device	1.0.2 ou 1.0.3
Region config / RP revision	Paramètres régionaux	RP002-1.0.x / A
ADR algorithm	Politique ADR	Default ADR (LoRa only)
Flush queue on activate	Évite l'envoi de downlinks obsolètes après un rejoin	On
Allow roaming	Roaming inter-NS	Off
Device-status request freq	Polling batterie/marge	0-1/jour

Champ	Rôle	Valeur typique
Expected uplink interval	Base de détection offline	ex. 3600 s

Onglet Join (OTAA/ABP)

Champ	Rôle	Note
Device supports OTAA	Méthode de join	On = OTAA (recommandé)
RX1 delay	Ouverture RX1 après join/uplink	0 = défaut serveur
RX1 DR offset	Offset data-rate RX1	0 si incertain
RX2 DR / Freq	Réglages RX2	0 = défaut serveur (EU868)

Onglet Class

Champ	Rôle	Note
Class-C support	RX continu	Équipements alimentés
C-confirmed downlink timeout	Attente ACK en Class-C	secondes

Onglet Codec

Option	Quand l'utiliser	Les clés en sortie pilotent...
None	Payload brut traité ailleurs	—
Cayenne LPP	Device en LPP	Mesures auto-mappées
JavaScript functions	Payloads custom	Tableau de bord & routage

Onglet Measurements

Champ	Rôle	Exemple
Auto-detect	Découvrir les clés vues dans <code>decodeUplink</code>	✓ pour démarrer vite
Key / Kind / Name	Mapping manuel & libellé	<code>temperature</code> / Gauge / "Room temp"

Bonnes pratiques

- Un profil par **famille d'équipements & ligne de firmware** ; dupliquez et ajustez lorsque le fabricant change les paramètres MAC/RP.
- Gardez **Expected uplink interval** réaliste : il sert de base à la vue "online/offline".
- Versionnez vos **codecs JavaScript** et testez-les avec des payloads d'exemple avant un déploiement massif.
- Ignorez l'onglet **Relay** sauf si vous déployez explicitement du LoRaWAN Relay.

Gérer les profils d'équipements existants

La page **Device profiles** liste tous les profils disponibles sur la passerelle.

Pour chaque ligne, vous verrez les principaux attributs utilisés par le serveur (ex. **Name**, **Region**, **LoRaWAN MAC version**, **Revision**, **Supports OTAA**, **Supports Class-B/C**).

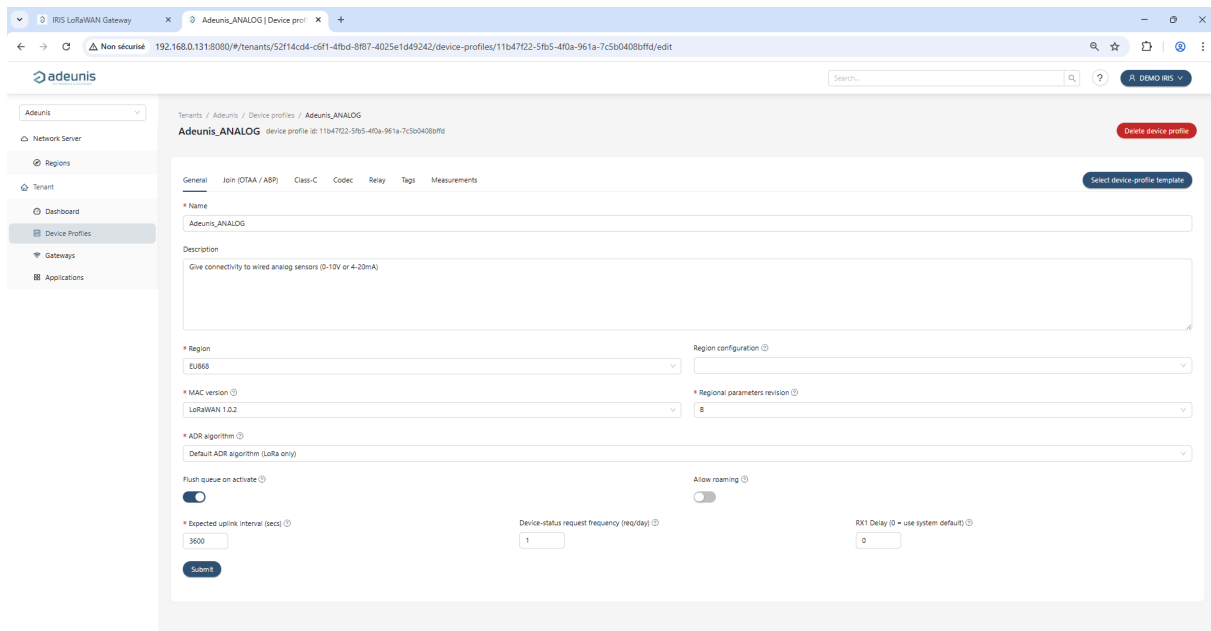
Utilisez la barre de recherche (en haut à droite) pour filtrer la liste, ou **Add device profile** pour créer un nouveau profil.

Name	Region	MAC version	Revision	Supports OTAA	Supports Class-B	Supports Class-C
Adeunis_ANALOG	EU868	LoRaWAN 1.0.2	8	yes	no	no
Adeunis_ANALOG_PWR	EU868	LoRaWAN 1.0.2	8	yes	no	yes
Adeunis_BREATH	EU868	LoRaWAN 1.0.2	8	yes	no	yes
Adeunis_COMFORT	EU868	LoRaWAN 1.0.4	RP002-1.0.4	yes	no	no
Adeunis_COMFORT_SERENITY	EU868	LoRaWAN 1.0.4	RP002-1.0.4	yes	no	no
Adeunis_DELTA_P	EU868	LoRaWAN 1.0.2	8	yes	no	no
Adeunis_DRY_CONTACTS	EU868	LoRaWAN 1.0.4	RP002-1.0.4	yes	no	yes
Adeunis_MODBUS	EU868	LoRaWAN 1.0.2	8	yes	no	yes
Adeunis_PULSE	EU868	LoRaWAN 1.0.4	RP002-1.0.4	yes	no	no
Adeunis_PULSE_ATEX	EU868	LoRaWAN 1.0.2	8	yes	no	no
Adeunis_TEMP	EU868	LoRaWAN 1.0.4	RP002-1.0.4	yes	no	yes
Adeunis_TEMP25	EU868	LoRaWAN 1.0.4	RP002-1.0.4	yes	no	yes
Adeunis_TIC_CSE_LYNKY_MONO	EU868	LoRaWAN 1.0.2	8	yes	no	no
Adeunis_TIC_CSE_LYNKY_TRI	EU868	LoRaWAN 1.0.2	8	yes	no	no
Adeunis_TIC_PME_PMI	EU868	LoRaWAN 1.0.2	8	yes	no	no

Cliquez sur un profil pour accéder à ses onglets de configuration (**General**, **Join (OTAA/ABP)**, **Class-C**, **Codec**, **Relay**, **Tags**, **Measurements**).

L'en-tête affiche le **Device Profile Name** et le **Device Profile ID** ; le **Profile Name** est requis lors d'un bulk import (CSV/JSON), car la colonne `deviceProfileName` doit référencer cette valeur.

Depuis cette page, vous pouvez aussi **éditer** les paramètres du profil ou **Delete device profile** si nécessaire (assurez-vous qu'aucun équipement actif ne dépend encore de ce profil avant suppression).



Une fois votre/vos **Application(s)** et **Device Profile(s)** en place, vous pouvez maintenant enregistrer les end-devices (OTAA ou ABP) dans le serveur LoRaWAN intégré.

5.6.7. Ajouter un capteur (Import unitaire et en masse)

Votre profil est prêt : vous pouvez maintenant enregistrer le matériel (les capteurs).

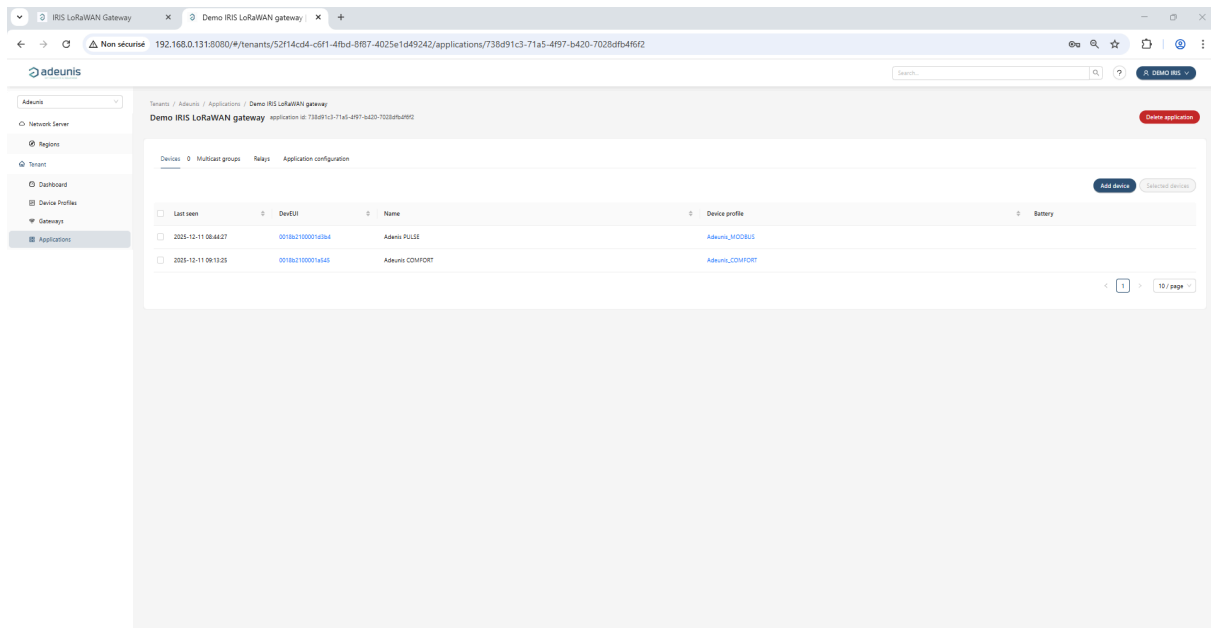
Dans **Create a device**, vous ajoutez chaque capteur dans l'application, vous sélectionnez un **Profil d'équipement "Device Profile"**, puis vous renseignez ses identifiants/clés (ex. DevEUI, JoinEUI/AppEUI, AppKey pour l'OTAA).

Vous pouvez ajouter les capteurs un par un ou les importer en masse : une fois enregistrés, ils peuvent rejoindre le réseau et vous commencerez à voir des trames en temps réel et des mesures décodées.

Ajouter un capteur (Import unitaire)

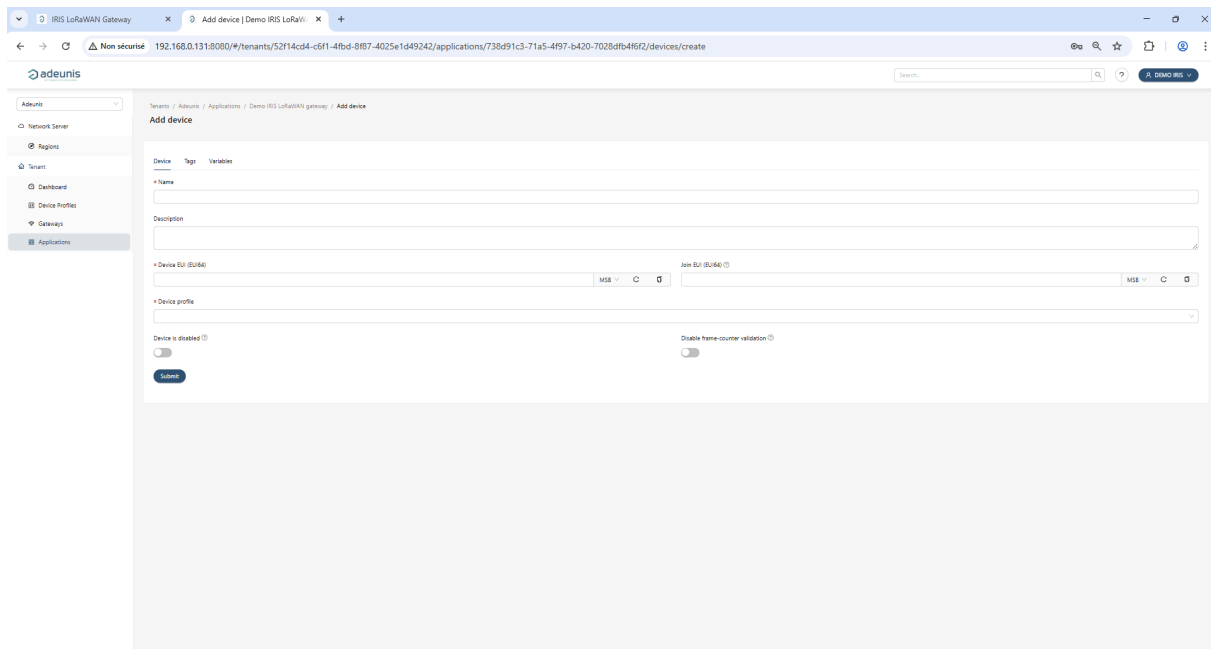
Pour ajouter un capteur,

1. Ouvrez le tableau de bord et allez dans **Applications** → **<votre application>** → **Devices** → **Add device**.



2. Renseignez l'onglet **Device** :

- **Name** : libellé lisible (site/salle/rôle du capteur).
- **Description** : contexte optionnel.
- **Device EUI (EUI64)** : 16 caractères hexadécimaux (8 octets). Utilisez le sélecteur **MSB/LSB** pour correspondre à l'étiquette du device ; **MSB** est le cas le plus courant.
- **JoinEUI (EUI64)** (alias AppEUI) : 16 hex, requis pour la plupart des devices OTAA. Respectez le sélecteur **MSB/LSB**.
- **Device profile** : sélectionnez le profil que vous avez créé (ex. *Adeunis_TEMP*).
- **Device is disabled** : laissez **off** pour un fonctionnement normal.
- **Disable frame-counter validation** : laissez **off** (n'activer que temporairement pour du dépannage ABP).



3. Cliquez sur **Submit to create the device**.

4. **Tags** (optionnel) : ajoutez des paires **key = value** (ex. **building=A** , **floor=2**). Les tags aident la recherche, le filtrage et les règles de routage.

5. **Variables** (optionnel) : ajoutez des paires **key = value** utilisées par votre **codec** ou vos intégrations (ex. **temp_unit=°C** , **pulse_factor=1.0**).

6. Renseigner les clés de join / session

- Ouvrez le device créé → **Keys (OTAA/ABP)** puis configurez :
 - **OTAA (LoRaWAN 1.0.x)** : **AppKey** (32 hex).
 - **OTAA (LoRaWAN 1.1.x)** : **NwkKey** et **AppKey** (32 hex chacun).
 - **ABP** : **DevAddr**, **NwkSKey** / **FNwkSIntKey** / **SNwkSIntKey** / **NwkSEncKey** et **AppSKey** selon votre device/profil.
- Enregistrez les clés.

7. Mise en service et vérification

- Démarrez le capteur et déclenchez un join / uplink.
- Dans **Applications** → **Devices** → **<device>** → **LoRaWAN frames**, vérifiez le **Join-Accept** (OTAA) et la réception des **uplinks**.
- Les graphiques du tableau de bord **"Dashboard"** se remplissent si vous avez configuré des mesure **"Measurements"** dans le profil d'équipement.

Référence rapide des paramètres

Paramètre	Rôle	Notes
Name	Identifiant "métier"	Texte libre
Description	Contexte	Optionnel
Device EUI (EUI64)	Identité unique du device	16 hex ; respecter MSB/LSB
JoinEUI (EUI64)	Périmètre de join (OTAA)	16 hex ; requis pour la plupart des devices OTAA
Device profile	Comportement radio/codec	Choisir le profil correspondant
Device is disabled	Verrouillage admin	Off = actif
Disable frame-counter validation	Contournement sécurité	Laisser off (test uniquement)
Tags	Métadonnées	Key/value
Variables	Paramètres codec/intégration	Key/value
Keys (OTAA/ABP)	Matériel de sécurité	À configurer après création



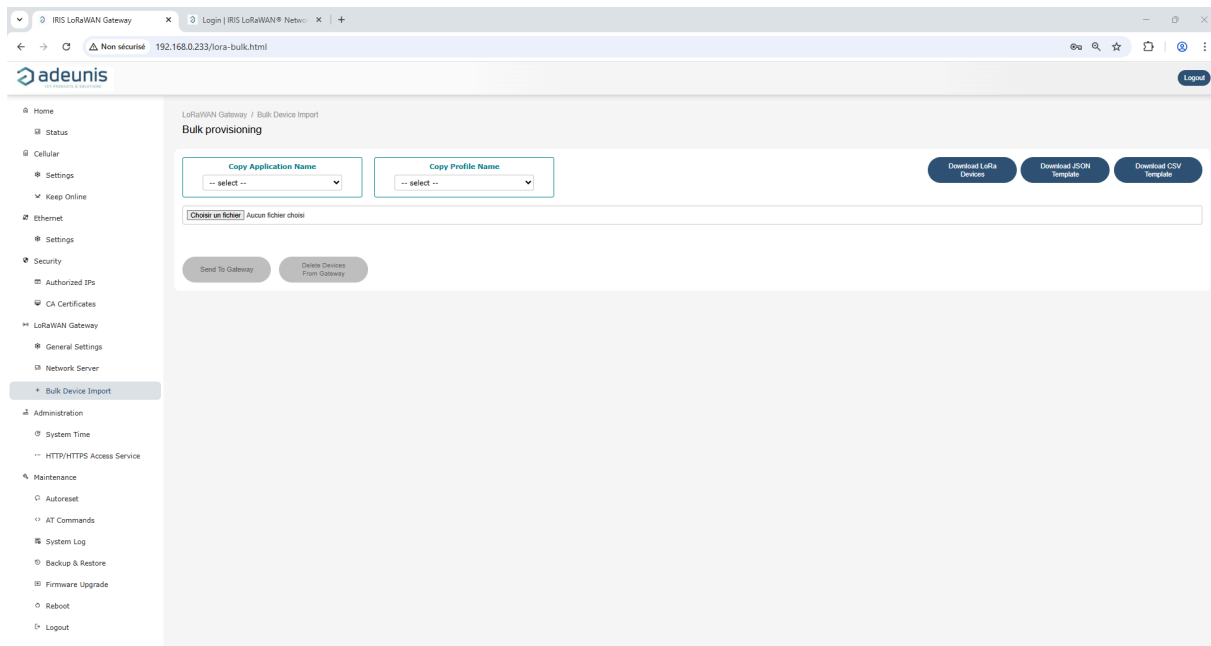
Si un équipement ne rejoint jamais, re-vérifiez : la bande (**EU868** uniquement avec ce firmware), la version MAC du profil, l'ordre MSB/LSB (présentation) des identifiants/clés, et **Authorized IPs / CA Certificates** si votre routage dépend de services sécurisés.

Un exemple est décrit dans **L'ANNEXE 3 ENREGISTRER UN CAPTEUR ADEUNIS COMFORT**

Ajouter plusieurs capteurs (Import en masse)

Cet outil permet d'importer ou de supprimer un grand nombre de capteurs en une seule opération via un fichier JSON ou CSV.

1. Ouvrez l'interface web de la passerelle et allez dans **LoRaWAN** → **Bulk Device Import**.



2. Cliquez sur **Download JSON template**

```
{
  "devices": [
    {
      "name": "Example Adeunis Breath Sensor",
      "description": "Sensor for measuring the level of fine particles and TVOCs",
      "devEui": "0018B210000BC44",
      "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
    }
  ]
}
```

ou sur **Download CSV template**

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	name	description	devEui	appKey	nwkKey	joinEui	deviceProfile	applicationName	isDisabled	skipFCntCheck			
2	Example Ade Sensor for m	0018B210000	384E786F39A54445BE9C279E0EF1E0E9	Adeunis_BRE	LoRaWAN	De	false	false					
3	Example Ade Sensor for m	0018B210000	D2DD78FF18DC47EFBF85EADCCB2C13C	Adeunis_COI	LoRaWAN	De	false	false					
4	Example Hur Sensor for m	B2903AD184	D2DD78FF58DC47EFBF85EADCCB2C13C	Brand_XYZ_F	LoRaWAN	De	false	false					
5	Light Sensor Sensor for m	C2903AD184	D2DD78FF58DC47EFBF85EADCCB2C13C	Brand_XYZ_L	LoRaWAN	De	false	false					
6	Motion Sensi Sensor for de	D2903AD184	D2DD78FF58 11223344556	D31D15AC45	Brand_XYZ_M	LoRaWAN	De	false	false				
7	Motion Sensi Sensor for de	D2903AD184	D2DD78FF58 11223344556	D31D15AC45	Brand_XYZ_M	LoRaWAN	De	false	false				
8	Pressure Ser Sensor for m	E2903AD184	D2DD78FF58DC47EFBF85EADCCB2C13C	Brand_XYZ_F	LoRaWAN	De	false	false					
9													
10													
11													
12													
13													
14													

3. Renseignez une ligne / un objet par device, avec :

- **name, description**
- **devEUI**
- **joinEUI** pour l'OTAA
- **app_key** (et **nwk_key** en 1.1) pour l'OTAA ; ou les clés de session ABP selon le cas
- **Device Profile Name**
- **Application Name**
- **Device disabled status**
- **Disable frame-counter status**

4. Importez le fichier.

L'interface affiche un aperçu des équipements listés dans le JSON ou le CSV.

5. Cliquez sur **SEND TO GATEWAY**.

Pour supprimer un lot précédemment importé, fournissez un fichier contenant la liste des **dev_eui** ciblés et cliquez sur **DELETE DEVICES FROM GATEWAY**.

Un exemple est décrit dans **L'ANNEXE 4 ENREGISTRER DES CAPTEURS EN MASSE**

Référence rapide des paramètres

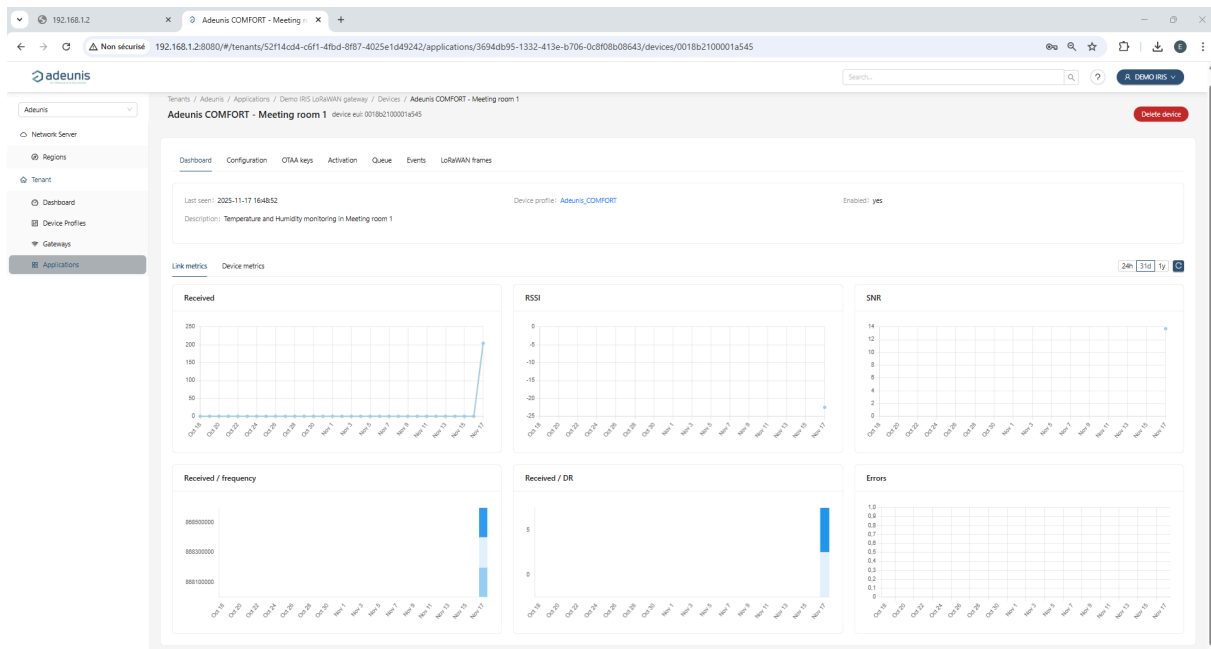
Élément	Rôle	Notes
Modèle JSON/CSV	Noms de colonnes/champs de référence	Télécharger depuis la page avant de préparer le fichier
Identifiants requis	<code>dev_eui</code> , <code>device_profile</code>	<code>join_eui</code> pour l'OTAA
Clés de sécurité	<code>app_key</code> (1.0.x), <code>app_key</code> + <code>nwk_key</code> (1.1)	32 hex chacune
Actions	SEND TO GATEWAY, DELETE DEVICES FROM GATEWAY	Importer ou supprimer



Commencez par un petit fichier pilote (2–3 devices) pour valider le template, puis importez la liste complète.

5.6.8. Visualiser les information détaillées d'un équipement

Cette vue centralise l'état, les métriques et les opérations d'un device. L'en-tête affiche le nom de l'équipement "**Device name**", le "**DevEUI**", un lien vers son profil "**Device profile**", et le bouton permettant de supprimer l'équipement "**Delete device**".



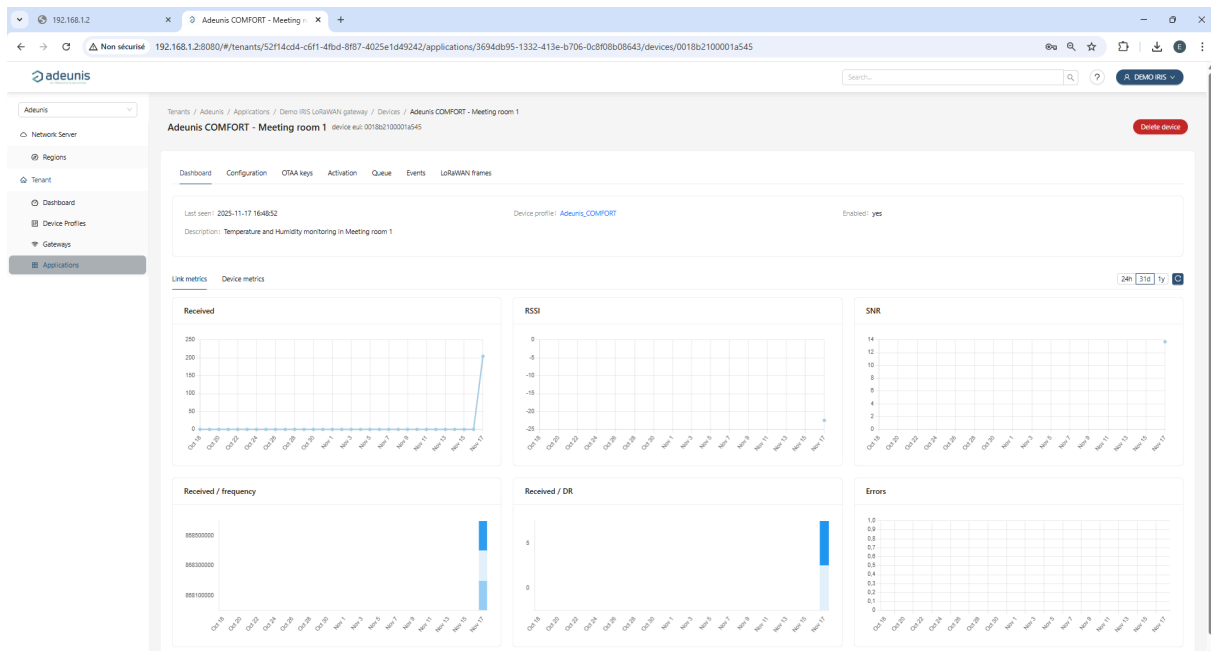
Onglet : Dashboard

- **Résumé (haut de page)**

Affiche l'heure de la dernière transmission "**Last seen**", le profil "**Device profile**" (cliquable), l'état "**Enabled**", et la "**Description**".

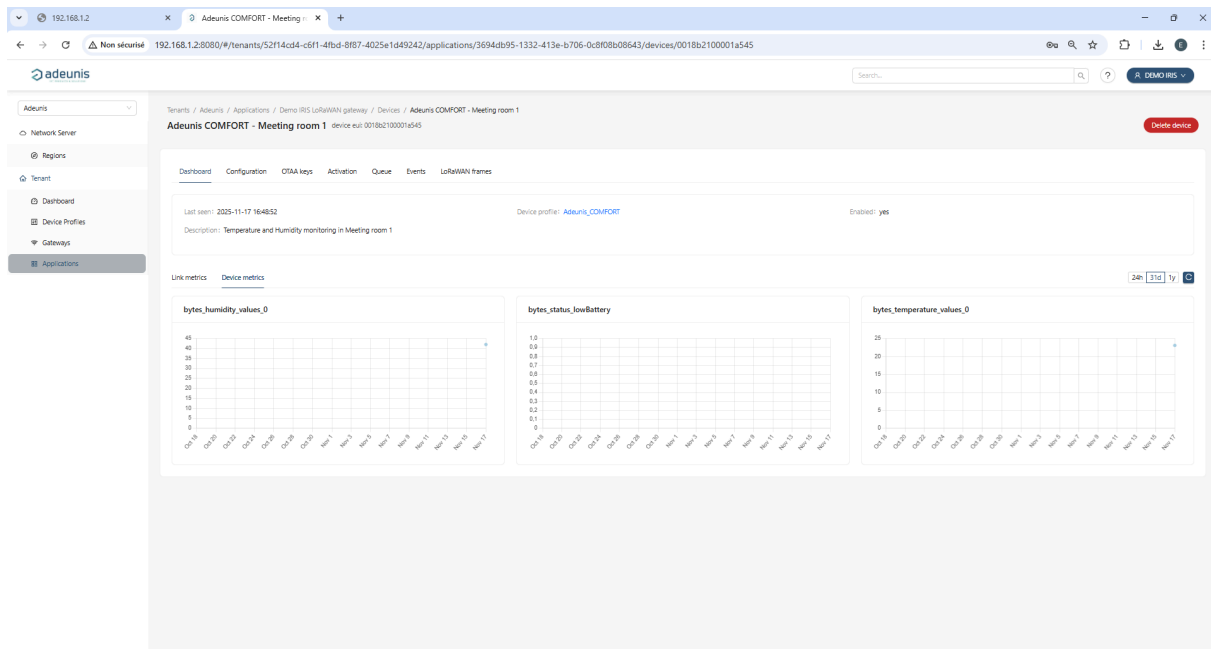
- **Métriques radio (Link metrics)**

Graphiques **Received** (uplinks), **RSSI** (dBm), **SNR** (dB), **Received / Frequency**, **Received / DR**, et **Errors** (taux d'erreurs downlink). À utiliser pour évaluer la couverture, l'ADR et la qualité de transmission.



• Métriques device (Device metrics)

Si un codec et des mesures **“Measurements”** sont définis dans le profil, les séries décodées (ex. température, humidité, batterie, impulsions) apparaissent ici.



Onglet : Configuration

Permet de modifier le nom **“Name”**, la description **“Description”**, le profil **“Device profile”** (changer le profil impacte région/version MAC/classes), ainsi que les **“Tags”** et les

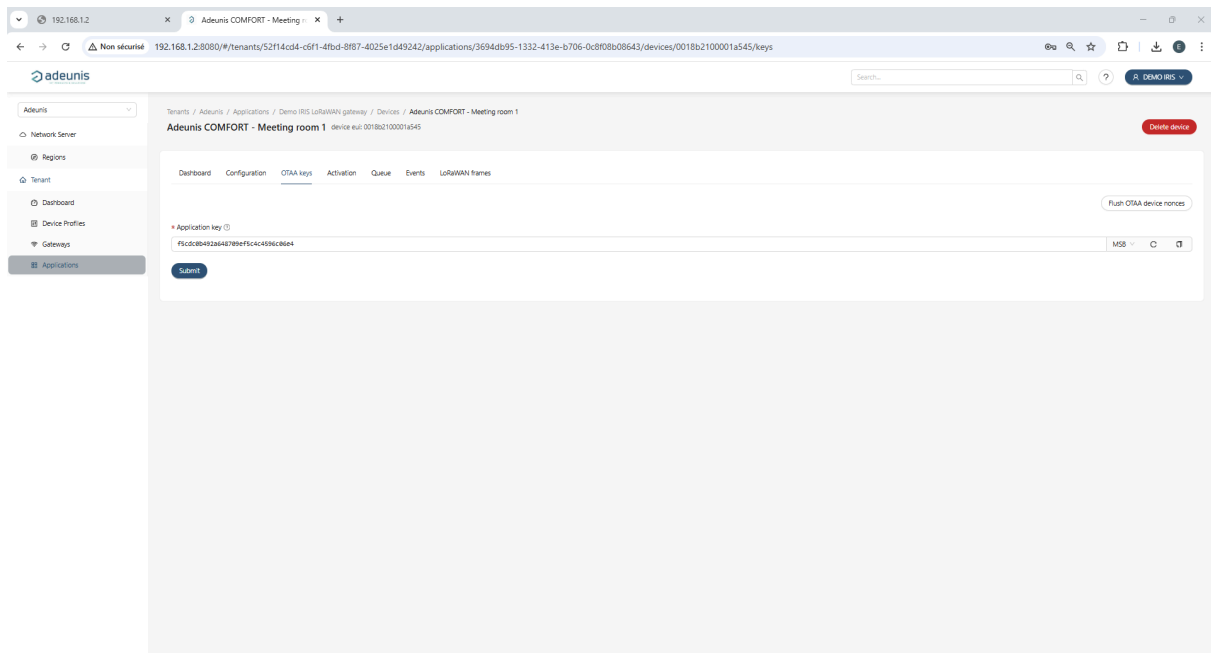
“**Variables**” d’un équipement. (DevEUI et JoinEUI apparaissent dans leurs zones respectives et peuvent être en lecture seule selon la méthode de création.)

The screenshot shows the Adeunis web interface. The browser address bar indicates the URL: 192.168.1.2:8080/#/tenants/52f14cd4-c6f1-4fbd-8f87-4025e1d49242/applications/3694db95-1332-413e-b706-0c8f08b08643/devices/0018b2100001a545/edit. The interface has a sidebar with navigation options: Regions, Tenant, Dashboard, Device Profiles, Gateways, and Applications. The main content area is titled 'Adeunis COMFORT - Meeting room 1' and contains a 'Delete device' button. Below the title are tabs for Dashboard, Configuration, OTAA keys, Activation, Queue, Events, and LoRaWAN frames. The 'Configuration' tab is selected, showing a form with the following fields: Name (Adeunis COMFORT - Meeting room 1), Description (Temperature and Humidity monitoring in Meeting room 1), Device EUI (EU864) (0018b2100001a545), Join EUI (EU864) (0018b2100001a545), Device profile (Adeunis_COMFORT), and a 'Device is disabled' toggle. A 'Submit' button is located at the bottom left of the form.

Onglet : OTAA keys

Pour les devices OTAA, permet de voir/modifier **JoinEUI/AppEUI** et **AppKey** (LoRaWAN 1.0.x) ou **NwkKey + AppKey** (LoRaWAN 1.1.x).

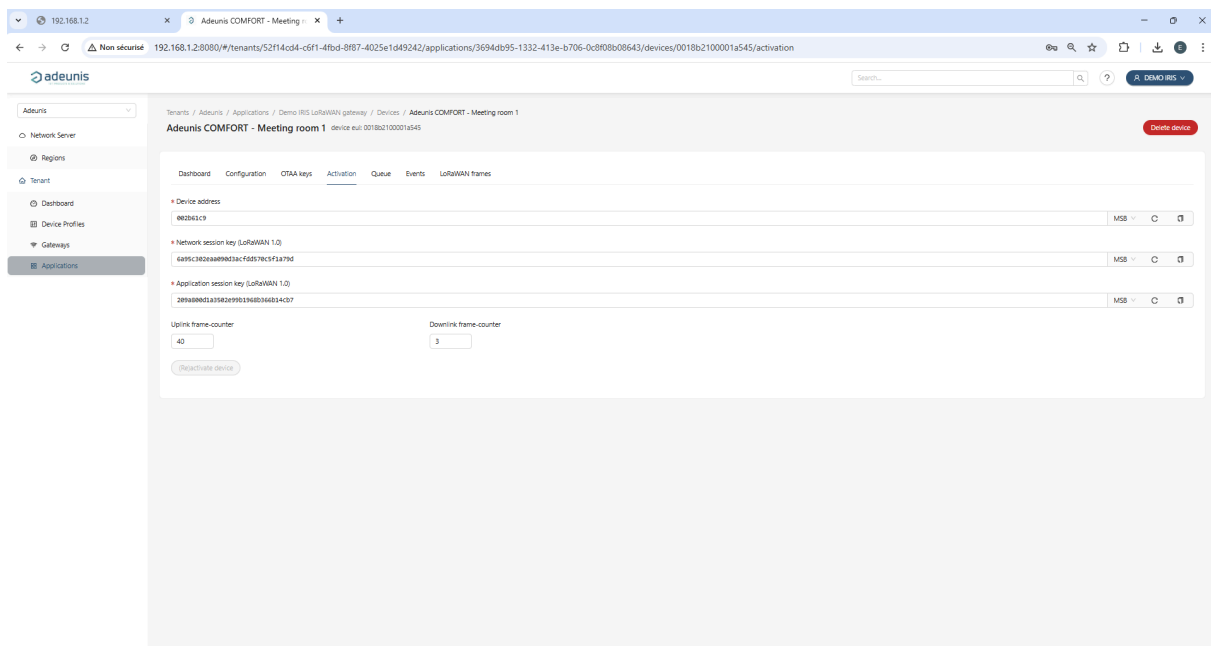
L’action “**Flush OTAA device nonces**” permet d’effacer les nonces stockés si un device a été réinitialisé et réutilise un DevNonce (fréquent sur certaines stacks 1.0.x), sinon les joins peuvent être rejetés comme “used DevNonce”.



Onglet : Activation

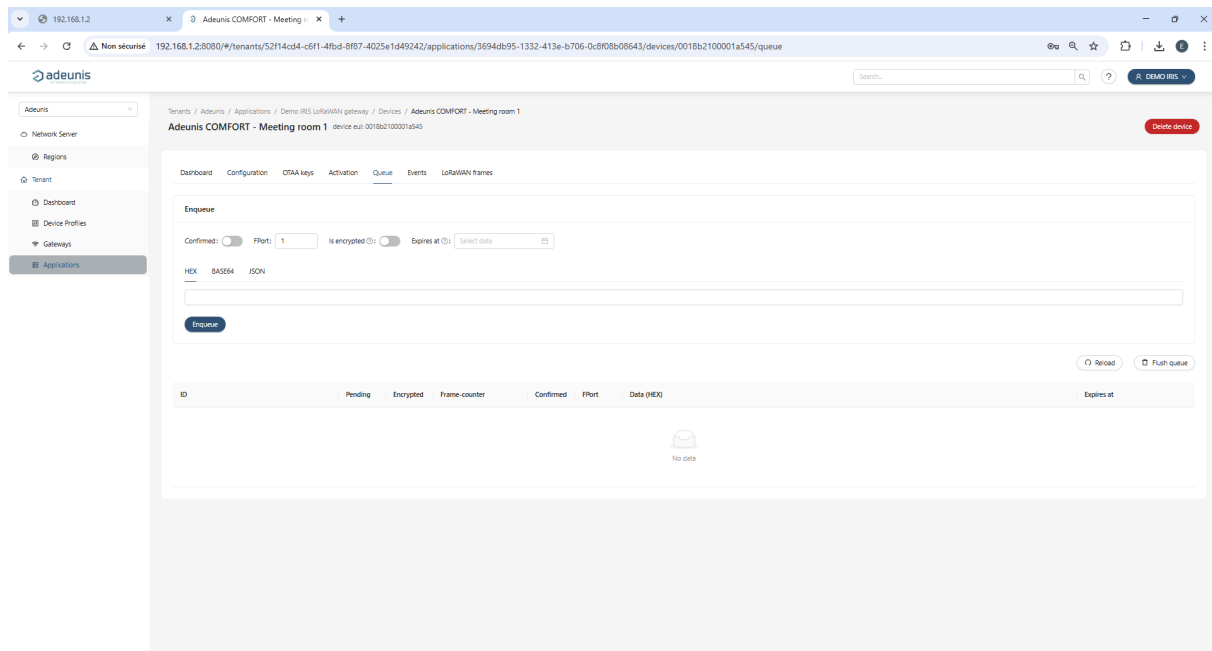
Affiche la session courante (**DevAddr**, **AppSKey**, **NwksKey** ou équivalents 1.1.x) et les compteurs **FCntUp/FCntDown**.

Vous pouvez (ré)activer manuellement des devices ABP ou effacer la session pour forcer un nouveau join OTAA.



Onglet : Queue

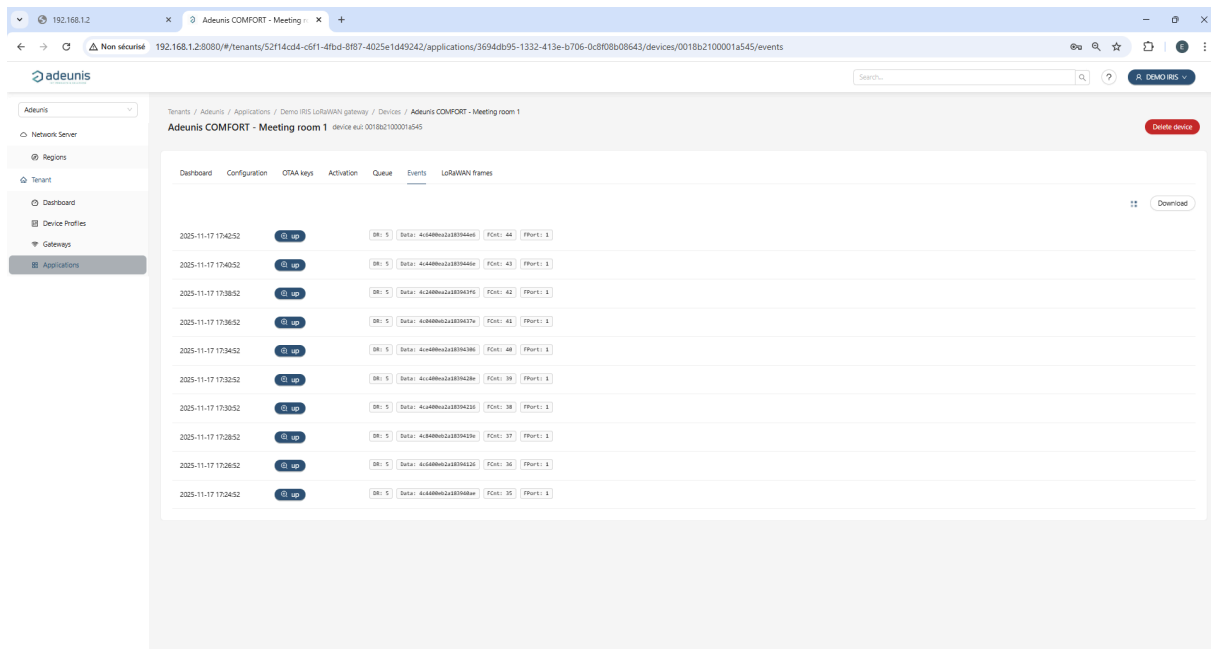
Éditeur pour composer et planifier des downlinks (device unitaire). Les messages sont conservés dans une file FIFO et envoyés lors de la prochaine fenêtre RX valide selon la classe (A/C).



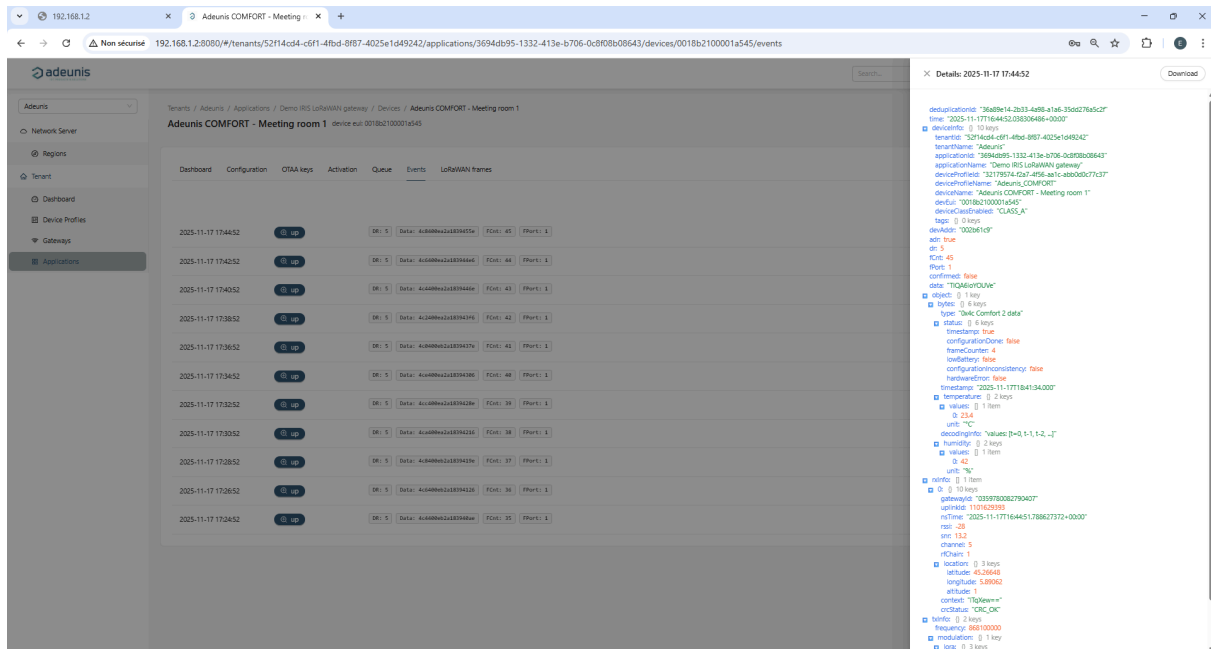
Pour la procédure pas-à-pas, voir la section [Envoyer un downlink vers un capteur](#).

Onglet : Events

Journal opérationnel : uplinks, downlinks, joins, ACK, messages d'état.



Utilisez **View details** pour inspecter fréquence, DR, fenêtre RX, RSSI/SNR, gateway, taille, MIC. La liste peut être **downloaded (JSON)** pour analyse ou support.



Onglet : LoRaWAN frames

Trames MAC/PHY brutes liées au device (fréquence, DR, RSSI/SNR, FCnt, FPort, flags).

Utile pour du diagnostic avancé ou pour vérifier le comportement réseau indépendamment des codecs.

Prérequis

L'équipement est déjà **provisionné** (OTAA : join effectué, ou ABP : activé) et apparaît connecté "**Online**" dans **Applications** → **Devices** → **[Device]**.

Un profil d'équipement "**Device profile**" est associé et (optionnellement) un codec "**payload codec**" est configuré si vous souhaitez utiliser le mode JSON.

En **Class A**, un **uplink est nécessaire** pour ouvrir RX1/RX2 : le downlink sera délivré **après le prochain uplink**.

En **Class C**, le serveur peut émettre dès que le duty-cycle de la passerelle le permet.

Downlink vers un équipement (Single-Device Downlink)

Utilisez un downlink pour envoyer une commande ou une configuration à un capteur spécifique (ex. changement de consigne, bascule de sortie, intervalle de remontée).

Sur IRIS, les downlinks sont planifiés par device depuis le serveur réseau embarqué et transmis lors de la prochaine fenêtre de réception valide, selon la classe LoRaWAN.

Allez dans **Applications** → **Devices** → **[Device]** → **Queue**.

Cette page permet de composer la payload, de choisir le port applicatif (FPort) et d'indiquer si le message doit être confirmé. Les éléments ajoutés apparaissent dans une liste FIFO et seront envoyés lors de la prochaine fenêtre RX disponible (Class A : après le prochain uplink ; Class C : dès que le duty-cycle le permet).

1. Composer le downlink

Dans **Queue**, renseignez les champs :

- **Confirmed**

Activez **ON** pour demander un ACK du device lors de son prochain uplink ; laissez **OFF** pour optimiser batterie et charge réseau. Si l'ACK n'est pas reçu, le serveur réessaie automatiquement.

- **FPort**

Utilisez **1-223** pour les payloads applicatives. **0** est réservé aux commandes MAC et ne doit pas être utilisé pour des données applicatives.

Is encrypted?

Laissez **OFF** en usage normal (le serveur chiffre avec les clés de session). Passez **ON** uniquement si vous fournissez un **FRMPayload déjà chiffré avec l'AppSKey**, à transmettre tel quel.

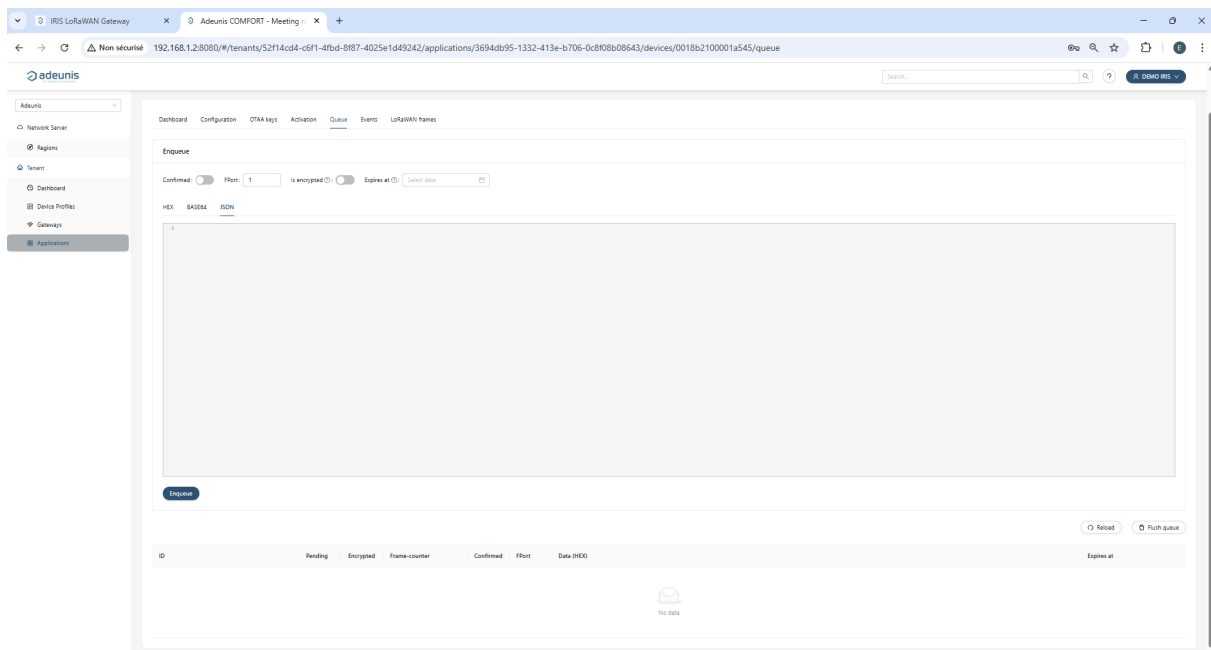
- **Expires at (optionnel)**

Définissez une durée de validité (TTL). Si le device ne reçoit pas le message avant cette date (ex. pas d'uplink d'un Class A), le serveur le supprime afin d'éviter une action obsolète.

- **Payload format**

Choisissez **HEX**, **BASE64** ou **JSON**.

- **HEX/BASE64** : collez les octets bruts à envoyer.
- **JSON** : fournissez un objet JSON si un codec est configuré dans le profil d'équipement ; le serveur appelle `encodeDownlink(input)` pour construire les octets avant mise en file.



2. Saisie de la payload

- **HEX/BASE64**

Exemple (PULSE Adeunis) : pour passer la période d'échantillonnage à 1 heure :

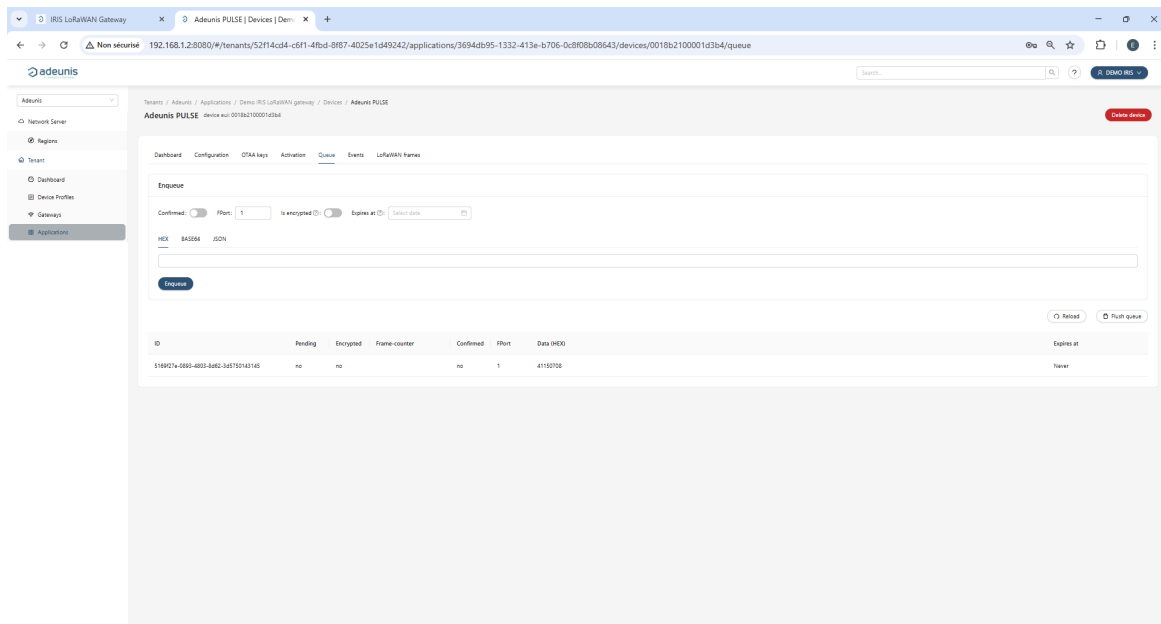
`41150708`

- **JSON**

Exemple avec un codec attendant une consigne : `{ "target": 22.5 }`

3. Mise en file d'attente

Cliquez sur **Enqueue**. L'élément apparaît dans la file avec les colonnes **Pending**, **Encrypted**, **Frame-counter**, **Confirmed**, **FPort**, **Data (HEX)** et **Expires at**.



Utilisez **Reload** pour rafraîchir la liste, ou **Flush queue** pour supprimer les éléments en attente.

5. Envoi et statut

- **Class A**: transmis en RX1/RX2 **après le prochain uplink** du device.
- **Class C**: transmis dès que possible (soumis au duty-cycle EU868).

Downlinks Multicast (optionnel, Class C)

Le multicast permet d'envoyer la même commande à plusieurs capteurs en une seule opération.

Tous les devices d'un groupe multicast partagent une **DevAddr multicast** et une paire de **clés de session multicast** ; les trames adressées au groupe sont reçues par chaque membre à l'écoute.

Par conception LoRaWAN, les trames multicast **ne sont pas acquittées (pas d'ACK)** : la validation se fait via la supervision des trames plutôt que par confirmation.

1. Créer un groupe Multicast

Allez dans **Applications** → **Multicast groups** → **Add Multicast group**.

Renseignez les champs :

- **Name** : libellé clair (ex. `Lighting_Floor1`).
- **Multicast Address (DevAddr)** : adresse groupe 4 octets / 8 hex.

- **mcNwkSKey / multicast network key** (LoRaWAN 1.0.x) : 16 octets hex ; **doit correspondre** aux devices.
- **mcAppSKey / multicast application key** : 16 octets hex ; **doit correspondre** aux devices.
- **Region** : **EU868** sur IRIS. Doit être cohérent avec devices et passerelle.
- **Data-Rate (DR)** : DR0...DR5 en EU868 (DR bas = plus de portée, DR haut = plus rapide/moins robuste).
- **Frequency (Hz)** : fréquence downlink du groupe (ex. **869525000** , **868100000**). Doit être légale en EU868 et cohérente avec le DR.
- **Downlink Frame-counter** : FCntDown du groupe (incrémentation automatique ; réinitialisation possible en cas de reprovisionnement).
- **Group type** : sélectionnez **Class-C**. (Class-B n'est pas utilisé dans ce guide.)
- **Class-C Scheduling Type (Class-C only)** : définit quand le downlink multicast est envoyé :
 - **Delay** : émission après un délai relatif (en secondes) à partir de la mise en file.
 - **GPS/Absolute time** : émission à une heure absolue (GPS/UTC). Assurez-vous que l'heure de la passerelle est correcte (NTP) avant utilisation.

The screenshot shows the 'Add multicast-group' form in the Adeunis web interface. The form is titled 'Add multicast-group' and is located under the 'Applications' menu. It contains several input fields and dropdowns for configuring a multicast group. The fields are: 'Multicast-group name' (text input), 'Multicast address' (16-character hex input with 'MSB' checkbox), 'Multicast network session key' (16-character hex input with 'MSB' checkbox), and 'Multicast application session key' (16-character hex input with 'MSB' checkbox). Below these are dropdowns for 'Region' (EU868), 'Data-rate' (0), 'Frame-counter' (0), 'Frequency (Hz)' (0), 'Group type' (Class-C), 'Class-B ping-slot periodicity' (Every second), and 'Class-C scheduling type' (Delay). A 'Submit' button is located at the bottom left of the form.

2. Ajouter des capteurs

Ouvrez le groupe créé et **ajoutez les capteurs**. Seuls les capteurs provisionnés avec la même DevAddr multicast et les mêmes clés recevront les trames ; des clés incohérentes empêchent la réception.



IRIS permet la création de groupes multicast **Class-C**.

3. Mettre en file d'attente un downlink Multicast

Allez dans **Applications** → **Multicast groups** → **[votre groupe]**.

Composez le downlink avec le même éditeur que pour un device unitaire :

- **Confirmed** : laissez **OFF** (pas d'ACK en multicast).
- **FPort** : **1...223** pour données applicatives ; **0** réservé MAC (ne pas utiliser pour l'applicatif).
- **Is encrypted?** : laissez **OFF** sauf si vous fournissez un FRMPayload déjà chiffré.
- **Expires at** : TTL optionnel.
- **Payload** : **HEX**, **BASE64**, ou **JSON** (si codec `encodeDownlink()` dans le device profile).

4. Cliquez sur **Enqueue**.

L'élément apparaît avec **Pending**, **Encrypted**, **Frame-counter**, **FPort**, **Data (HEX)** et **Expires at**.



Le multicast sur le serveur LoRaWAN embarqué est supporté en **Class-C**. Les devices Class A ne participent pas à un multicast coordonné car ils n'écoutent qu'en RX1/RX2 après leurs propres uplinks.

Référence rapide des paramètres

Champ	Où	Valeurs / Notes
Confirmed	Multicast group → Queue	OFF en multicast (pas d'ACK).
FPort	Multicast group → Queue	1...223 applicatif ; 0 = MAC (réservé).
Is encrypted?	Multicast group → Queue	OFF recommandé. ON seulement si payload pré-chiffré.
Expires at	Multicast group → Queue	TTL optionnel.
Payload format	Multicast group → Queue	HEX / BASE64 ou JSON (codec <code>encodeDownlink()</code>).

Champ	Où	Valeurs / Notes
Region	Multicast group	EU868 sur IRIS (cohérent devices/passerelles).
Data-Rate (DR)	Multicast group	EU868 DR0...DR5 .
Frequency (Hz)	Multicast group	Ex. 869525000 , 868100000 (légal & cohérent DR).
Class-C scheduling type	Multicast group	Delay / GPS/Absolute time (UTC). NTP requis.
Frame-counter	Multicast group	FCntDown (auto ; reset uniquement en reprovisionnement).

Validation

- **Onglet Events (device)** : recherchez **downlink scheduled** , **downlink acknowledged** , ou des erreurs (**frame-counter** , **no channel available** , **mic error**).
- **Onglet LoRaWAN frames** : inspectez PHYPayload, l'évolution de **fCnt** , **fPort** et la fenêtre RX utilisée.
- **Causes fréquentes d'échec**
 - Pas d'uplink récent (**Class A** n'ouvre pas RX).
 - Saturation du **duty-cycle** sur EU868 (délais possibles).
 - Mauvais **FPort** (0 utilisé).
 - Incohérence codec/JSON (le codec ne génère pas les octets attendus).
 - Désynchronisation des compteurs après reprovisionnement (n'utiliser **Disable frame-counter validation** que temporairement pour dépannage ABP).

Bonnes pratiques

- Gardez des **frames** aussi courtes que possible
- Planifiez les campagnes (notamment multicast) en période de faible trafic pour limiter les contraintes de **duty-cycle**.
- Renseignez **Expires at** pour éviter l'exécution de commandes obsolètes.
- Documentez chaque action multicast (qui / quand / quoi) dans votre journal d'exploitation pour la traçabilité.

5.6.10. Validation

Votre **serveur LoRaWAN embarqué** est opérationnel lorsque :

1. La **passerelle** apparaît **en ligne** dans le tableau de bord, avec la bande **EU868** et une localisation correcte.
2. Un profil d'équipement "**Device profile**" existe, avec un **codec** associé, et au moins une **Application** est créée.
3. Le(s) **capteur(s)/équipement(s)** a/ont rejoint (OTAA) et les **uplinks** affichent des valeurs **JSON décodées** (pas uniquement des trames brutes).
4. Un test de **downlink** aboutit (Classe A : délivré après le prochain uplink ; Classe C : immédiat).
5. Si utilisé, l'intégration **MQTT(S)/HTTP(S)** reçoit les trames attendues avec une configuration TLS correcte (CA racine installée sur IRIS).
6. L'**ADR** se stabilise dans les bornes de DR configurées et les paramètres **RX2** correspondent à la documentation du capteur/équipement.
7. Vous avez exporté une **sauvegarde de configuration** (IRIS → Backup/Factory) et consigné les identifiants du **dashboard** ainsi que le **NetID** dans le dossier site.

Routage des données vers votre applicatif

LoRaWAN est configuré et la passerelle est en ligne côté serveur réseau. L'étape suivante consiste à raccorder les **trames décodées** à votre application via **MQTT/s** ou **HTTP/s**, puis à réaliser la recette site pour valider la chaîne de bout en bout.

6. Intégration applicative & routage des données (MQTT/s & HTTP/s)

Ce chapitre explique comment envoyer les **données LoRaWAN décodées** à vos backends applicatifs.

IRIS peut **retransmettre** les uplinks issus du serveur LoRaWAN intégré vers un système externe via :

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

Si vous utilisez un **LNS externe** (UDP Packet Forwarder ou Basics Station), les intégrations se configurent généralement directement sur ce LNS ; ce chapitre est alors fourni **à titre de référence**.

Si vous utilisez le **serveur LoRaWAN intégré**, la passerelle envoie elle-même les données décodées vers votre application. Dans ce cas :

- Sélectionnez le mode d'intégration dans **LoRaWAN Gateway → General Settings → Re-send data using** (*Resend data using MQTT* ou *Resend data using HTTP*).
- Activez si besoin un script **JSON Transformer** pour adapter ou filtrer le JSON avant son envoi.

The screenshot shows the 'adeunis' web interface for the 'IRIS LoRaWAN Gateway'. The left sidebar contains a navigation menu with options like Home, Status, Cellular, Settings, Keep Online, Ethernet, Security, Authorized IPs, CA Certificates, LoRaWAN Gateway, General Settings (selected), Network Server, Bulk Device Import, Administration, System Time, HTTP/HTTPS Access Service, Maintenance, Autoreset, AT Commands, System Log, Backup & Restore, Firmware Upgrade, Reboot, and Logout. The main content area is titled 'General Settings' and includes a toggle for 'Enable extra frequencies'. It features dropdowns for 'Minimum Data Rate' (DRO) and 'Maximum Data Rate' (DRS). The 'Re-Send data' dropdown is set to 'Resend data using MQTT'. Other fields include 'MQTT ID' (IRISGW), 'MQTT Username' (adeun), 'MQTT Password' (masked), 'MQTT QoS' (0), and 'MQTT Key' (empty). There is also a 'MQTT Certificate' field. At the bottom, it shows 'MQTT connection status: Connected' and two buttons: 'Save & Apply' and 'JSON Transformer Script'.

Les recommandations ci-dessous se concentrent sur **ce que vous devez préparer, la sécurisation du transport, et la validation** de la livraison vers les systèmes du client.

6.1. Intégration MQTT/MQTTs

IRIS peut publier les uplinks LoRaWAN décodés vers un broker MQTT externe (port **1883** non chiffré pour des usages de laboratoire, ou **8883** avec TLS pour la production).

Lorsque le serveur LoRaWAN intégré est activé et que **Re-send data using MQTT** est sélectionné dans **LoRaWAN Gateway** → **General Settings**, chaque uplink décodé est transféré vers le broker configuré. Si le JSON Transformer est activé, le message MQTT contient le **JSON transformé** (ou la trame est ignorée si le script renvoie **"NULL"**).

Pré-requis

- **Hôte du broker** (FQDN) et **port** (1883 pour MQTT, 8883 pour MQTTS).
- **Identifiants** (nom d'utilisateur/mot de passe ou certificat client, selon la politique du broker).
- Politique de **QoS** (généralement **QoS 0** ou **QoS 1** pour une livraison fiable).
- **Modèle de confiance** :
 - **MQTT non sécurisé (1883)** : uniquement pour un réseau de labo/isolé.
 - **MQTTS 8883 avec certificat autosigné** : importer le **certificat serveur autosigné du broker** dans un emplacement CA-Root.
 - **MQTTS 8883 avec certificat signé par une CA** : importer la/les **CA racine/intermédiaire** émettrice(s).

The screenshot shows the 'General Settings' page for the LoRaWAN Gateway in the Adeunis web interface. The page is titled 'LoRaWAN Gateway' and 'General Settings'. It features a sidebar with navigation links: Home, Status, Cellular, Settings, Keep Online, Ethernet, Security, Authorized IPs, CA Certificates, LoRaWAN Gateway, General Settings (selected), Network Server, Bulk Device Import, Administration, System Time, HTTP/HTTPS Access Service, Maintenance, Autorest, AT Commands, System Log, Backup & Restore, Firmware Upgrade, Reboot, and Logout.

The main content area includes the following fields and sections:

- Enable extra frequencies** (checkbox, checked).
- Minimum Data Rate** (dropdown menu, set to DR0).
- Maximum Data Rate** (dropdown menu, set to DR5).
- Re-Send data** (dropdown menu, set to Re-send data using MQTT).
- MQTT Broker URL** (text input, set to http://adeunis-codexs.com:1883).
- MQTT ID** (text input, set to IREGW).
- MQTT Username** (text input, set to ades).
- MQTT Password** (password input, masked with asterisks).
- MQTT QoS** (dropdown menu, set to 0).
- MQTT Key** (text input, empty).
- MQTT Certificate** (text input, empty).
- Mqtt connection status:** Connected.
- Buttons:** Save & Apply, JSON Transformer Script.

Schéma de topic

Par défaut, IRIS publie les uplinks de chaque équipement sur :

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

<applicationID> est l'ID de l'application LoRa, et <deviceEUI> l'EUI de l'équipement.

Exemple

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

Si le JSON Transformer est activé, vous pouvez surcharger le topic MQTT dans le script. Dans ce cas, le broker reçoit le message sur le topic renvoyé par le script.

Format de données

Les messages sont au format JSON et incluent des horodatages, des identifiants, des compteurs de trame, des métriques RF et les champs décodés produits par votre codec. Votre application aval doit analyser ces champs directement, ou analyser le JSON transformé si vous utilisez le JSON Transformer.

```

{
  "deduplicationId": "8ca7b138-2534-4888-b4cc-9263454dbc7c",
  "time": "2025-09-29T18:05:35.723673117+00:00",
  "deviceInfo": {
    "tenantId": "52f14cd4-c6f1-4fbd-8f67-4825e1d49242",
    "tenantName": "Rebbyn",
    "applicationId": "58f6ce5d-21f5-443e-8891-843df288bc87",
    "applicationName": "LoRaWAN Devices",
    "deviceProfileId": "3ba319c7-43de-4818-a6cb-26a2698be53a",
    "deviceProfileName": "Aduv1s_BREATH",
    "deviceName": "Breath_Aduv1",
    "devEui": "8018b218898bc45",
    "deviceClassEnabled": "CLASS_B",
    "tags": {
    }
  },
  "devAddr": "8853c795",
  "adr": true,
  "dr": 0,
  "rfCnt": 09,
  "rfPort": 1,
  "confirmed": false,
  "data": "b8AAEgKCAIAAg=",
  "object": {
    "bytes": {
      "tvoc": {
        "unit": "pp/m3",
        "values": [
          10.0
        ]
      },
      "type": "Add Breath periodic data",
      "status": {
        "configurationDone": false,
        "lowBattery": false,
        "frameCounter": 3.0,
        "hardwareError": false,
        "configurationInconsistency": false,
        "sensorError": false
      },
      "decodingInfo": {
        "values": [
          "t=0, t=1, t=2, ..."
        ]
      },
      "pe1": {
        "values": [
          2.0
        ]
      },
      "unit": "pp/m3",
      "pe10": {
        "values": [
          2.0
        ]
      },
      "unit": "pp/m3",
      "pe25": {
        "unit": "pp/m3",
        "values": [
          2.0
        ]
      }
    }
  },
  "rxInfo": {
    {
      "gatewayId": "8359788882788588",
      "uplinkId": 182577581,
      "nsTime": "2025-09-29T18:05:35.437461763+00:00",
      "rssi": -53,
      "snr": 13.5,
      "channel": 5,
      "rfChain": 1,
      "location": {
        "latitude": 41.4838,
        "longitude": 2.8514,
        "altitude": 288.0
      },
      "context": "DMM-A=",
      "crcStatus": "CRC_OK"
    }
  },
  "txInfo": {
    {
      "frequency": 868100000,
      "modulation": {
        "lora": {
          "bandwidth": 125000,
          "spreadingFactor": 7,
          "codeRate": "CR_4_5"
        }
      }
    }
  },
  "regionConfigId": "eu868"
}

```

Référence rapide des paramètres

Paramètre	Rôle	Valeur typique / recommandation
URL / Port	Adresse du broker	<code>mqtt.example.com</code> / 8883 pour TLS
Client ID	Identifiant client MQTT utilisé	<code>iris-<site>-gw-<eui></code>

Paramètre	Rôle	Valeur typique / recommandation
	pour la connexion	
Auth	Username/password ou certificat client	Selon la politique du broker
QoS	Sémantique de livraison	0 ou 1 (à aligner avec l'application)
Certificat/Clé	Modèle de confiance	Voir §4.3.3 (autosigné vs signé par AC)
Re-send data using	Mode d'intégration depuis le serveur intégré	Resend data using MQTT
Topic	Chemin de routage	application//device//event/up
Données	Champs JSON	Horodatage, IDs, compteurs, métriques RF, valeurs décodées

Validation et transfert

Une intégration MQTT/s est considérée comme conforme lorsque :

1. **L'heure et le DNS** sont corrects.
2. La **session TLS** s'établit correctement vers le broker sur **8883** : la chaîne de certificats est validée par rapport aux CA importées, et le **nom d'hôte correspond au CN/SAN**.
3. Le broker confirme une **connexion réussie** avec le **Client ID** attendu et la méthode d'authentification prévue (user/pass ou certificat client).
4. Un **uplink de test** publié par la passerelle apparaît sur le **topic cible exact**.
5. La **structure JSON** correspond à l'attendu (horodatage, IDs, compteurs, métriques RF, champs décodés) et l'application l'analyse sans erreur.
6. Un workflow **downlink** (si applicable) peut être déclenché par l'application et atteint le LNS / l'équipement via le chemin normal.
7. Un **redémarrage de la passerelle** entraîne une **reconnexion automatique** dans la fenêtre attendue, avec le même Client ID et les abonnements en place.
8. La **posture de sécurité** est cohérente : TLS actif ; le référentiel de confiance ne contient que les CA nécessaires (ou le seul certificat serveur autosigné) ; toute exposition entrante via Mobile-WAN est restreinte via **Authorized IPs**.

6.2. Intégration HTTP/HTTPs

IRIS peut aussi pousser les uplinks décodés vers un serveur HTTP/HTTPS. C'est généralement utilisé pour intégrer des serveurs applicatifs qui n'exposent pas MQTT.

Lorsque le serveur LoRaWAN intégré est activé et que **Re-send data using HTTP** est sélectionné dans **LoRaWAN Gateway** → **General Settings**, la passerelle envoie une requête HTTP POST par uplink vers l'endpoint configuré. Si le JSON Transformer est activé, le corps de la requête correspond au **JSON transformé** (ou la requête n'est pas envoyée si le script renvoie **"NULL"**).

Pré-requis

- **URL de l'endpoint** (HTTP pour un labo, **HTTPS pour la production**).
- **Méthode** (POST).
- **En-têtes HTTP** (ex. **Authorization: Bearer <token>** , **Content-Type: application/json**).
- **Confiance TLS** si l'endpoint est en HTTPS.
- **Auth/ACL** côté application (token, liste d'IP autorisées, ou les deux).

The screenshot shows the 'General Settings' page for a LoRaWAN Gateway in the Adeunis web interface. The page is divided into a left sidebar with navigation links and a main content area with various configuration fields. The 'General Settings' section is active, showing fields for Band (eu868), ID (0359780602760275), Mode (LoRa Server), Keep Alive (10), Stat Interval (30), Push Timeout (100), Latitude, Longitude, Altitude, HTTP Port (8080), Net ID (000000), RX1 Delay (1), LoRa Server Dashboard Username (Nico), and LoRa Server Dashboard Password. There is a checkbox for 'Enable extra frequencies'. Below this, there are dropdowns for 'Minimum Data Rate' (DR0) and 'Maximum Data Rate' (DR5). The 'Re-Send data' dropdown is set to 'Resend data using HTTP'. At the bottom, there are fields for 'HTTP Server URL' (https://5b4429d5-2541-4531-9b33-9b6d706bce.mock.pstmn.io), 'HTTP Username', 'HTTP Password', 'HTTP Custom Header 1' (x-api-key: PMAN-6937d717cce96d00015d8fa-e070f96215af2d1197ba1c4fa28b43afcc), and 'HTTP Custom Header 1'. There are 'Save & Apply' and 'JSON Transformer Script' buttons at the bottom.

Paramètres recommandés

- POST d'un corps JSON avec les mêmes champs que pour MQTT (horodatage, IDs, compteurs, métriques RF, valeurs décodées), ou le JSON renvoyé par le Transformer.

Référence rapide des paramètres

Paramètre	Rôle	Valeur typique / recommandation
URL / Méthode	Où et comment livrer	<code>https://app.example.com/iot/ingest</code> / POST
En-têtes	Auth & type de contenu	<code>Authorization: Bearer ...</code> , <code>Content-Type: application/json</code>
TLS / CA	Modèle de confiance	CA racines selon §4.3.2
Données	Format du corps	JSON avec IDs, compteurs, métriques RF, valeurs décodées (ou JSON transformé)

Validation et transfert

Une intégration HTTP/s est considérée comme conforme lorsque :

1. **L'heure et le DNS** sont corrects.
2. La **session TLS** s'établit correctement vers l'endpoint sur **443** : la chaîne de certificats est validée par rapport aux CA importées, et le **nom d'hôte correspond au CN/SAN**.
3. L'endpoint **authentifie la requête** comme prévu (ex. `Authorization: Bearer ...`, mTLS, ou liste d'IP autorisées) et rejette les requêtes malformées/non autorisées.
4. Un **POST de test** renvoie un **2xx** avec une latence acceptable (définir une cible, ex. < 2 s sur LAN / < 5 s en cellulaire).
5. La structure JSON (après transformation si activée) respecte le contrat et l'application la traite sans erreur de mapping.
6. La **gestion d'erreur** est correcte : un **5xx** simulé ou une coupure amont déclenche le **retry/backoff configuré** côté passerelle ; les erreurs **4xx** ne sont pas retentées.
7. La **posture de sécurité** est cohérente : HTTPS en production ; le référentiel de confiance ne contient que les CA requises (ou un certificat serveur autosigné) ; l'exposition entrante via Mobile-WAN reste restreinte via **Authorized IPs**, tandis que la sortie vers l'endpoint applicatif est autorisée par le pare-feu.
8. Un **redémarrage de la passerelle** ne nécessite aucune action manuelle ; les POST suivants réussissent dès que le backhaul est opérationnel.

6.3. JSON Transformer

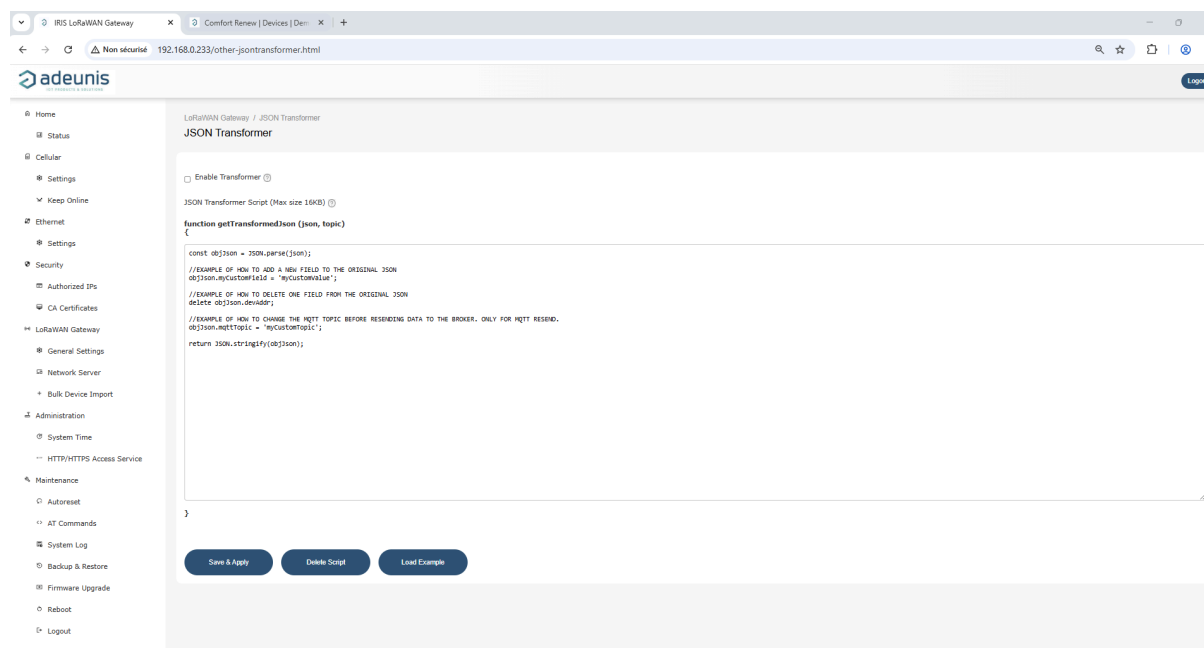
Le **JSON Transformer** permet d'adapter le format et le routage **sans modifier le LNS ni l'application** :

- supprimer des champs inutiles,
- renommer ou regrouper des valeurs,
- ajouter des champs personnalisés ou des tags,
- modifier (optionnellement) le topic MQTT,
- filtrer sélectivement des trames.

Le transformer est appliqué **après le décodage** par le serveur LoRaWAN intégré et **avant** l'envoi des données via MQTT ou HTTP.



Le script est optionnel : s'il est désactivé, le JSON d'origine produit par le serveur intégré est retransmis tel quel.



Utilisez le bouton **Load Example** de l'interface web comme point de départ, puis adaptez le script à votre propre structure JSON. Testez soigneusement toute modification via

l'intégration MQTT/HTTP et les logs avant un déploiement en production.

Signature de fonction

Vous devez fournir une fonction avec la signature suivante :

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

La fonction **doit retourner une chaîne** :

- une chaîne JSON → ces données sont envoyées via MQTT/HTTP ;
- la chaîne littérale `"NULL"` → la trame **n'est pas retransmise**.

Cas d'usage typiques

- **Réduction de la trame de données** : ne conserver qu'un sous-ensemble de champs nécessaires à l'application.
- **Mapping** : renommer/restructurer les champs pour correspondre à un schéma REST ou base de données existant.
- **Enrichissement** : ajouter des tags (site, groupe d'équipements, métadonnées statiques).
- **Filtrage sélectif** : ne retransmettre que certaines trames (selon équipement, port, application), en renvoyant `"NULL"` pour le reste.
- **Personnalisation de topic (MQTT)** : router différentes familles d'équipements vers des topics MQTT distincts.

Exemple de JSON standard

```
{ "deduplicationId": "441351a6-6153-494d-8b8c-460b5770c618", "time":  
"2025-12-02T08:29:38.637701176+00:00", "deviceInfo": { "tenantId":  
"52f14cd4-c6f1-4fbd-8f87-4025e1d49242", "tenantName": "Adeunis", "ap  
plicationId": "98f6ce6d-21f5-442e-8891-842df280bb87", "applicationNa
```

```

me": "LoRaWAN Devices", "deviceProfileId": "bbe319d7-43de-4010-a6cb-
26a2690be53a", "deviceProfileName": "Adeunis_BREATH", "deviceName":
"Breath_Jose", "devEui": "0018b2100000bc45", "deviceClassEnabled":
"CLASS_C", "tags": {} }, "adr": true, "dr": 5, "fCnt": 53, "fPort":
1, "confirmed": false, "data": "bSAA0gAGAAAYABQ==", "object": { "byte
s": { "type": "0x6d Breath periodic data", "tvoc": { "unit": "µg/m
3", "values": [ 58 ] }, "pm10": { "unit": "µg/m3", "values": [ 6 ]
}, "decodingInfo": "values: [t=0, t-1, t-2, ...]", "pm25": { "unit":
"µg/m3", "values": [ 6 ] }, "pm1": { "unit": "µg/m3", "values": [ 5
] }, "status": { "configurationInconsistency": false, "configuration
Done": false, "frameCounter": 1, "sensorError": false, "hardwareErro
r": false, "lowBattery": false } } }, "rxInfo": [ { "gatewayId": "03
59780082780580", "uplinkId": 2412397231, "nsTime": "2025-12-02T08:2
9:38.137058989+00:00", "rssi": -27, "snr": 13.5, "channel": 5, "rfCh
ain": 1, "location": {}, "context": "AteFLQ==", "crcStatus": "CRC_0
K" } ], "txInfo": { "frequency": 868100000, "modulation": { "loras":
{ "bandwidth": 125000, "spreadingFactor": 7, "codeRate": "CR_4_5" }
} }, "regionConfigId": "eu868" }

```

Exemple 1 – Ne conserver qu’un sous-ensemble de champs

Le script ci-dessous construit un JSON compact contenant quelques mesures et indicateurs d’état, ainsi que l’horodatage d’origine :

```

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.

Exemple 2 – Ne retransmettre qu'un seul équipement

Le script suivant retransmet les données **uniquement** pour l'équipement `0018b2100000bc45`. Les trames des autres équipements sont ignorées en renvoyant `"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);
}

```

Valider la chaîne complète

Le routage est configuré et sécurisé. Poursuivez avec **End-to-End Validation & Site Acceptance** afin de démontrer l'association de l'équipement, le décodage des uplinks et la

livraison **dans votre application** (ainsi qu'un downlink simple si applicable).

7. VALIDATION & RECETTE DE SITE

La mise en service est terminée lorsque vous pouvez démontrer un chemin de données propre, depuis un **capteur/équipement** jusqu'à l'**application**.

7.1. Statut & Identité

Commencez par **Home** → **Status** et vérifiez que la **passerelle** affiche une heure locale correcte, une connectivité IP saine (Ethernet ou Cellulaire) avec une adresse IP valide, et que la carte **LoRaWAN** indique le mode choisi, la bande régionale et le **Gateway EUI**.

Vérifiez que ce **Gateway EUI** correspond bien à celui enregistré sur votre LNS (ou visible dans le serveur embarqué).

7.2. Session Gateway ↔ LNS (selon le mode)

UDP Packet Forwarder

La passerelle apparaît **online** sur le LNS avec le bon plan de fréquences.

Assurez-vous que les pare-feux / **Authorized IPs** autorisent les **uplinks UDP sortants** et les **downlinks UDP entrants** depuis les IP du LNS que vous avez documentées.

Optionnellement, redémarrez la passerelle et vérifiez la réinscription automatique.

Basics Station (WSS)

La station apparaît **connectée** sur le LNS (router/session UP).

Confirmez que le nom d'hôte de l'URL **WSS** correspond au certificat serveur, que votre **CA Root** est installé, et qu'il n'y a pas d'erreur TLS.

Optionnellement, redémarrez et confirmez que la session se rétablit.

Serveur LoRaWAN embarqué

La console embarquée indique la passerelle **Up** ; l'**Application** et le **Device Profile** correspondent à la région.

7.3. Association (join) d'un équipement

Déclenchez un **join** depuis votre équipement OTAA.

Sur le LNS (ou la console embarquée), observez un **Join-request** suivi d'un **Join-accept** ; l'équipement apparaît **joined/activated**.

7.4. Uplink (RF vers application)

Envoyez un **uplink de test** depuis l'équipement.

Sur le LNS, vérifiez la réception de la trame avec des métriques radio plausibles (RSSI/SNR cohérents avec la proximité), puis confirmez que votre **décodeur côté application** (si applicable) traite les données sans erreur et que celles-ci atteignent l'intégration prévue (MQTT/HTTP) attendue par votre programme.

7.5. Downlink (réseau vers équipement)

Programmez un **downlink** vers l'équipement (non confirmé : OK ; utilisez **confirmed** si vous souhaitez un ACK).

- **Sites en UDP PF** : cela valide spécifiquement le chemin UDP **entrant** et votre politique **Authorized IPs** ; si vous retirez l'IP downlink du LNS de la liste d'autorisation, le downlink doit échouer ; réajoutez-la et retestez.
- **Basics Station (WSS)** : vérifiez que la station émet le downlink et que l'équipement le reçoit.

Une fois cette base validée, vous pouvez vous concentrer sur l'exploitation au quotidien. Le chapitre suivant explique comment sécuriser la configuration, conserver des journaux exploitables, maintenir le logiciel à jour et rendre la connectivité résiliente.

8. EXPLOITATION ET MAINTENANCE

L'exploitation en production consiste à éviter les surprises et à se rétablir rapidement quand elles surviennent. Votre objectif : une passerelle qui fonctionne discrètement, laisse une trace d'audit claire, et peut être restaurée en quelques minutes si quelque chose change en amont.

Commencez par mettre en place un **filet de sécurité**. Créez et archivez une **sauvegarde** de configuration à la fin de la mise en service et **avant chaque changement**. Un instantané à jour est le moyen le plus rapide de revenir en arrière après une erreur, ou de remplacer un matériel sans difficulté.

Ensuite, assurez la **visibilité**. Utilisez **Syslog** pour capturer les événements récents pour le diagnostic et, lorsque votre environnement le permet, exportez les logs vers votre collecteur central afin de conserver l'historique par site. Une heure exacte (NTP) est indispensable pour des journaux fiables : vérifiez-la à chaque relecture/export.

Ne procédez à des changements planifiés (comme les **mise à jour firmware**) qu'ensuite. Traitez chaque mise à jour comme une mini-release : choisissez une fenêtre de maintenance, vérifiez que vous disposez d'une sauvegarde récente, appliquez l'image, puis confirmez dans **Status** que l'heure, la connectivité IP et le transfert LoRaWAN sont sains. Notez la nouvelle version dans le dossier du site.

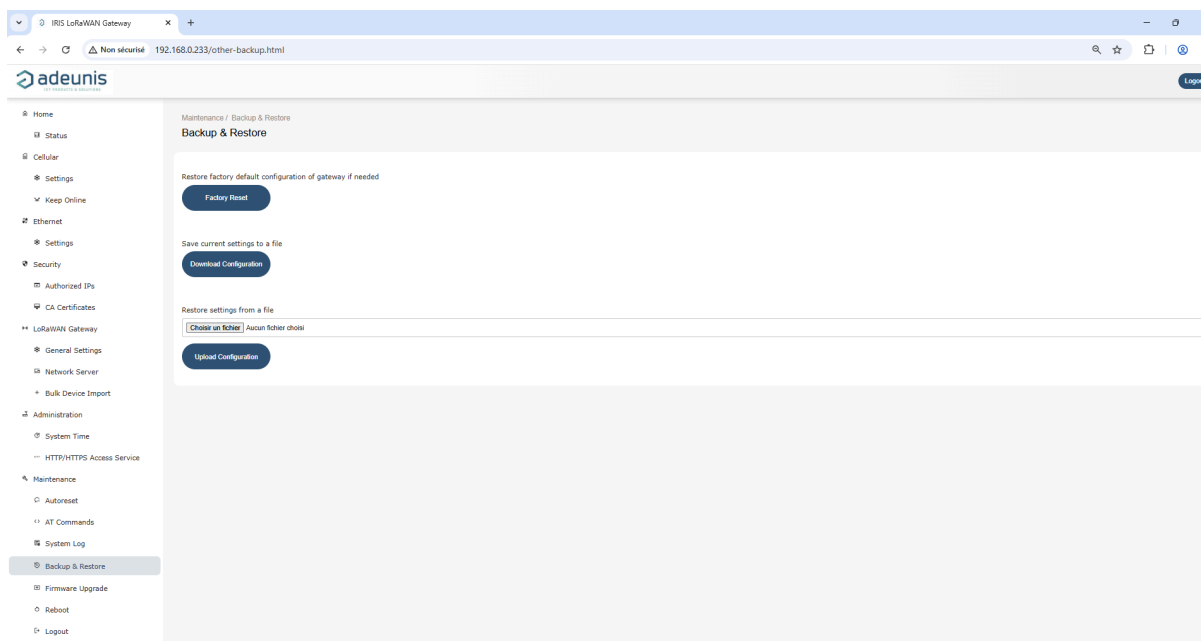
L'**Autoreset** est un outil de secours, pas un réglage par défaut. IRIS n'a pas besoin de redémarrages réguliers ; activez un redémarrage programmé seulement si votre politique d'exploitation l'exige ou si vous avez besoin d'un dernier recours sur des réseaux amont instables. Privilégiez la résolution des causes racines et appuyez-vous sur la surveillance de connectivité et le NTP pour la continuité.

En cas d'incident, utilisez les **AT Commands** pour un diagnostic ciblé du modem cellulaire et du logiciel IRIS, et gardez un **Reboot** propre pour des redémarrages contrôlés en maintenance. Appliquez une discipline de changement : **un seul changement à la fois, save & apply, vérification dans Status, et journalisation de l'action**. Ce rythme rend l'exploitation prévisible et le dépannage plus rapide.

8.1. Sauvegarde de configuration

Ce menu permet de sécuriser la configuration, d'effectuer des retours arrière rapides, ou de revenir aux paramètres usine.

- Cliquez sur **DOWNLOAD CONFIGURATION** pour exporter la configuration courante et stocker le fichier avec la documentation du site (à faire systématiquement **avant** une mise à jour firmware ou un changement majeur).
- Pour restaurer, sélectionnez l'archive puis **UPLOAD CONFIGURATION**. L'application IRIS réapplique les paramètres ; vérifiez l'accès réseau et le transfert LoRaWAN après restauration.
- **FACTORY SETTINGS** rétablit la configuration par défaut et efface les réglages personnalisés. À utiliser avec précaution, et uniquement après avoir exporté une sauvegarde récente. Un appui long sur le bouton "Function" réalise la même remise à zéro.





Après la mise en service initiale, exportez une sauvegarde de configuration et stockez-la avec les enregistrements du site. Refaire la même opération avant toute mise à jour firmware ou tout changement majeur.

8.2. Logs et Diagnostics

Utilisez les logs intégrés pour consulter les événements système et cellulaires récents directement dans le navigateur, ou exportez-les pour le support.

1. Vous verrez un journal roulant, incluant l'enregistrement cellulaire, les changements d'état de lien, et des notifications applicatives (ex. échantillons RSRP/RSRQ, attribution d'adresse IP).
2. Utilisez **REFRESH LOG** pour récupérer les dernières lignes, **DELETE LOG** pour effacer le buffer local, et **DOWNLOAD LOG** pour exporter un fichier .mtx à analyser ou à joindre à un ticket support.

The screenshot shows the 'System Log' page of the IRIS LoRaWAN Gateway. The page has a sidebar menu on the left with options like Home, Status, Cellular, Settings, Keep Online, Ethernet, Security, Authorized IPs, CA Certificates, LoRaWAN Gateway, General Settings, Network Server, Bulk Device Import, Administration, System Time, HTTP/HTTPS Access Service, Maintenance, Autreset, AT Commands, System Log, Backup & Restore, Firmware Upgrade, Reboot, and Logout. The main content area shows the 'System Log' with a title 'View and manage the device's system logs'. Below the title is a list of log entries with timestamps and details. At the bottom of the log list are three buttons: 'Refresh Log', 'Delete Log', and 'Download Log'.

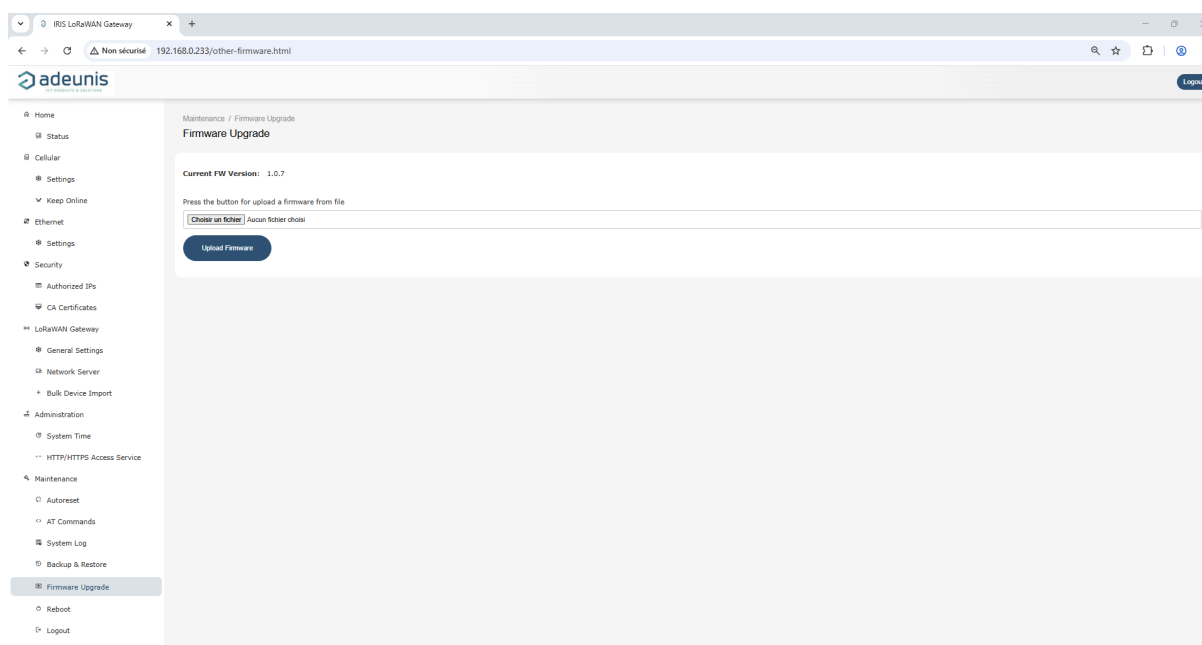


Assurez-vous que le NTP est configuré et synchronisé afin que les horodatages des logs soient cohérents avec votre flotte et vos systèmes backend ; des horloges décalées compliquent fortement la corrélation.

8.3. Mises à jour Firmware

Lorsqu'un nouveau firmware est fourni par l'équipe Adeunis, téléversez-le via l'interface web.

1. Vérifiez **Current FW Version** et comparez avec votre release note.
2. Cliquez sur **UPLOAD FIRMWARE**, sélectionnez l'image fournie, puis attendez la vérification et l'installation. Ne coupez **pas** l'alimentation pendant le processus.
3. La passerelle redémarre automatiquement une fois la mise à jour appliquée.



4. Après le redémarrage, confirmez la nouvelle version dans **Home** → **Status**, vérifiez la synchronisation de l'heure, puis assurez-vous que l'accès réseau et la configuration LoRaWAN sont toujours actifs.



Conservez une sauvegarde de configuration juste avant la mise à jour afin d'accélérer la reprise si nécessaire.

8.4. Autoreset

Programmez un redémarrage propre et automatique pendant une fenêtre de maintenance, ou déclenchez un redémarrage automatique lorsque l'équipement détecte des problèmes persistants de connectivité IP.

Utilisez cette fonction avec parcimonie : IRIS ne nécessite pas de redémarrages périodiques en fonctionnement normal. Préférez corriger les causes racines (alimentation, couverture radio, réseau amont) et utilisez **Keep Online** et le NTP pour une continuité de service.

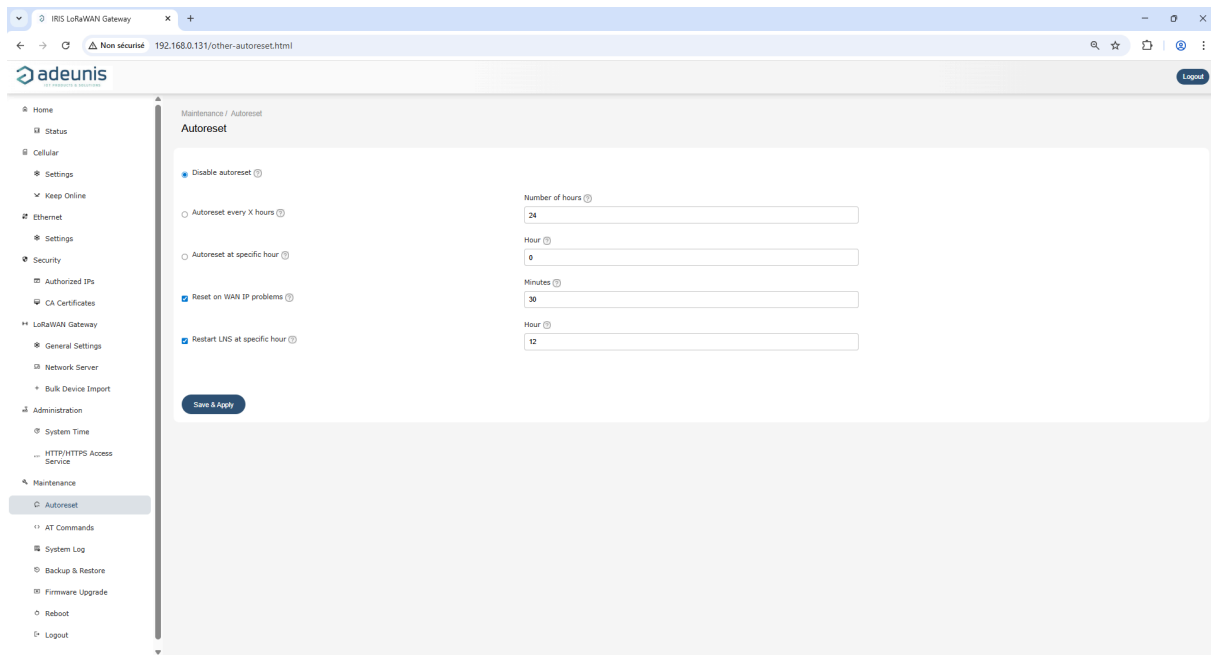
1. Choisissez l'un des trois modes :

- **Autoreset not enabled:** valeur recommandée par défaut.
- **Autoreset every X hours:** utile sur des sites distants qui bénéficient d'un "housekeeping" régulier.
- **Autoreset at specific hour:** redémarrage quotidien à une heure creuse (ex. 03:30 heure locale).

2. Si vous avez besoin d'un filet de sécurité pour des liens WAN bloqués, activez **Reset if IP problems**. Cette surveillance déclenche un redémarrage uniquement si la passerelle n'arrive pas à rétablir la connectivité par elle-même.

3. Si vous utilisez le serveur LoRaWAN embarqué, vous pouvez programmer un redémarrage périodique du serveur LoRaWAN en activant l'option **Restart LNS as specific hour**. Si vous avez plus de 100 capteurs connectés à la passerelle, nous recommandons de programmer un redémarrage périodique afin d'obtenir les meilleures performances.

Si vous utilisez le **serveur LoRaWAN embarqué**, vous pouvez programmer un redémarrage périodique du service en activant l'option **Restart LNS at a specific hour**. Au-delà de **100 capteurs** connectés à la passerelle, nous recommandons de planifier un redémarrage régulier afin de **maintenir des performances optimales**.



8.5. AT Commands

La console **AT Command** est une interface contrôlée pour interroger le module cellulaire et le logiciel IRIS.

Elle est destinée au diagnostic. Utilisez-la pour vérifier l'état d'enregistrement réseau, la qualité radio et le contexte data lorsque le lien cellulaire se comporte de manière inattendue.

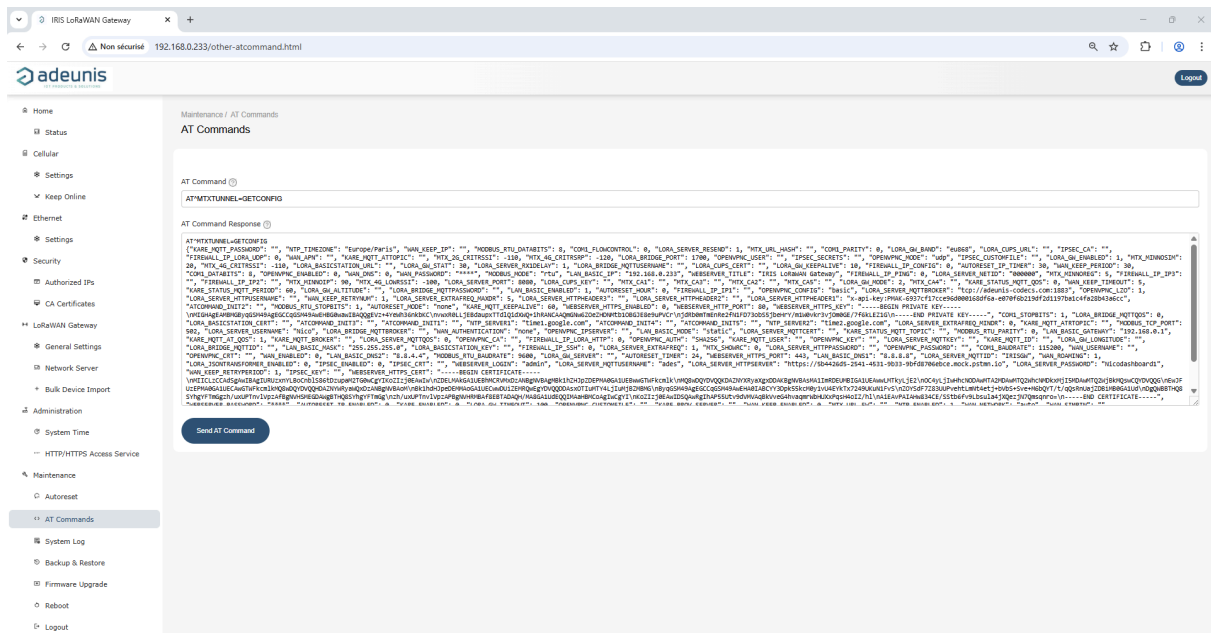
Gardez-la en lecture seule sauf si vous suivez une procédure précise fournie par le support.

Lors d'une investigation, récupérez la sortie AT avec horodatage ainsi que les dernières lignes de **Syslog**, puis joignez le tout à votre ticket.

8.5.1. Utiliser la console de manière sûre

1. Assurez-vous de disposer d'une **sauvegarde de configuration récente** et d'un **plan de retour arrière** clair.
2. Saisissez une commande dans **AT Command**.
3. Cliquez sur **SEND AT COMMAND**.
4. Lisez la réponse brute dans **AT Command Response**.
5. Appliquez **un seul changement à la fois**.

6. Si le comportement devient incohérent après un changement, **réappliquez les réglages via l'interface**, ou effectuez un **Reboot** contrôlé ; utilisez **Factory Settings** uniquement en dernier recours avec une sauvegarde disponible.



Dès que la vérification est terminée, quittez la console et revérifiez sur **Home** → **Status** que le modem est bien enregistré et dispose d'une adresse IP.



Utilisez la console AT principalement pour des diagnostics **en lecture seule**.
Avant toute commande modifiant l'état, contactez le support Adeunis et procédez sous guidance.

8.5.2. Commandes d'aide IRIS (logiciel)

Les commandes suivantes interrogent la couche applicative IRIS.

Commande	Objectif / Exemple de sortie
<code>AT+MTXTUNNEL=VERSION</code>	Retourne la version du logiciel IRIS (utile pour un ticket support).
<code>AT+MTXTUNNEL=GETTIME</code>	Retourne l'heure courante de la passerelle (UTC et fuseau local).
<code>AT+MTXTUNNEL=GETCONFIG</code>	Exporte la configuration IRIS courante (utile avant/après modifications).

Commande	Objectif / Exemple de sortie
<code>AT^MTXTUNNEL=GETPARAM,<KEY></code>	Lit un paramètre spécifique, ex. <code>AT^MTXTUNNEL=GETPARAM,NTP_SERVER1</code> .
<code>AT^MTXTUNNEL=GETIP</code>	Indique la dernière IP WAN attribuée.
<code>AT^MTXTUNNEL=REBOOT</code>	Déclenche un redémarrage applicatif contrôlé.

8.5.3. Vérifications courantes du modem Sierra

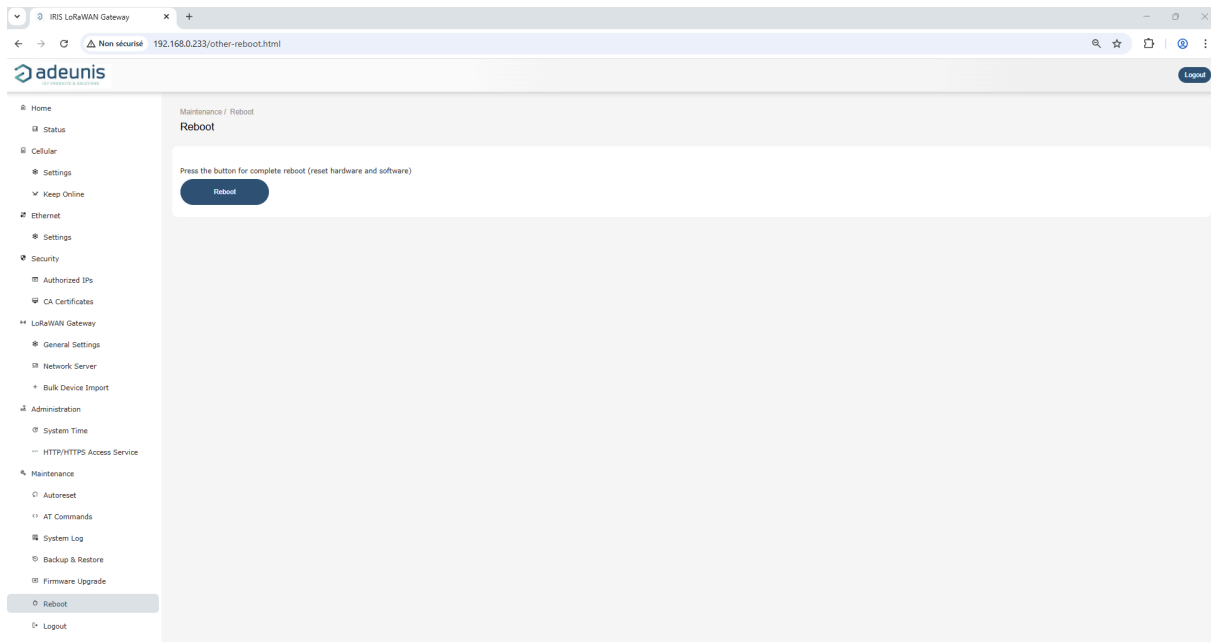
Ce sont des diagnostics standards pour évaluer l'enregistrement réseau et la qualité radio.

Ce que vous voulez vérifier	Exemple(s) de commande	Notes
Instantané qualité radio	<code>AT+CSQ</code>	Retourne RSSI (0–31) et BER. L'échelle d'interprétation est définie dans le guide.
Statut d'enregistrement LTE	<code>AT+CEREG?</code>	État d'enregistrement EPS selon 27.007.
État modem synthétique	<code>AT!GSTATUS?</code>	Cellule servante, RAT, température, etc. (contrôle rapide).
Métriques LTE détaillées	<code>AT!LTEINFO?</code>	EARFCN, bande, PCI, RSRP/RSRQ/SNR, TAC, Cell ID...
Contexte IP cellulaire	<code>AT+CGDCONT?</code> / <code>AT+CGPADDR</code> / <code>AT+CGCONTRDP</code>	Vérifier APN et IP attribuée.

8.6. Reboot

Utilisez cette fonction pour redémarrer le système de manière contrôlée sans modifier la configuration.

1. Cliquez sur **REBOOT** pour lancer la procédure de redémarrage (matériel & logiciel). La configuration est conservée, mais la synchronisation de l'heure peut être perdue si aucun serveur NTP n'est configuré et si l'horloge a été réglée manuellement.
2. La passerelle arrête proprement les services puis redémarre.



À utiliser lorsque le support demande un redémarrage propre pendant un dépannage.

8.7. Validation & contrôles de routine

Cette section propose une routine courte et répétable à exécuter après une fenêtre de maintenance (ou périodiquement) pour confirmer que la passerelle est saine et que le chemin de données LoRaWAN (uplink et downlink) fonctionne comme attendu.

8.7.1. Quand l'exécuter

- À la fin de la mise en service ou d'une fenêtre de maintenance.
- Après une **mise à jour firmware** ou un **changement sécurité/réseau** (HTTPS, Authorized IPs, NTP, APN, VLAN).
- **Trimestriellement** en contrôle préventif sur les sites en fonctionnement continu.

8.7.2. Procédure

1. Contrôle Status

- Ouvrez **Home** → **Status** et confirmez :
 - **Uptime** augmente ; **Device Time** est correct (NTP).
 - Le backhaul choisi (**Ethernet** ou **Cellular**) est **Up** avec une **IP** valide.

- Le mode/bande LoRaWAN sont corrects (si déjà configurés). Le **Gateway EUI** est celui enregistré sur votre LNS (ou visible dans le serveur embarqué).

2. Posture de sécurité

- Vérifiez que l'interface se charge en **HTTPS** ; le navigateur affiche un **cadenas** sans avertissement lorsqu'un certificat personnalisé est installé.
- **Authorized IPs** sur Mobile WAN : les sélecteurs sont positionnés sur **ALLOW ONLY AUTHORIZED IPs** (ou bloqué par une allow-list vide si vous ne souhaitez aucune exposition). Testez depuis une source **autorisée** puis **non autorisée** si l'accès Mobile WAN est dans le périmètre.

3. Heure & NTP

- Vérifiez que **NTP Time Servers** liste toujours des serveurs joignables ; le fuseau horaire correspond au site.
- Si vous utilisez des noms d'hôtes, validez que le **DNS** fonctionne sur le backhaul actif.

4. Surveillance de connectivité (sites cellulaires)

- Si applicable, vérifiez que la fonction **Keep Online** est configurée avec une cible ping stable et joignable.
- Vérifiez que période / timeout / retries sont cohérents et qu'il n'y a pas de "tempête" de récupération visible dans les logs.

5. État cellulaire (si utilisé)

- Si l'interface cellulaire est utilisée, ouvrez **Open AT Command** et exécutez **AT+CSQ** , **AT+CEREG?** , **AT!GSTATUS?** / **AT!LTEINFO?** pour un instantané du signal et de l'enregistrement.
- Recommandation : utilisez la console AT principalement en **lecture seule** ; contactez le support avant toute commande modifiant l'état.

5. Sauvegarde

- Exportez la **CONFIGURATION** et stockez-la avec l'**ID site**, la date et la version firmware.

7. Politique Autoreset

- Vérifiez que l'**Autoreset périodique** est aligné avec la politique du site (idéalement **Disabled** sauf exigence).

8. LoRaWAN

- Déclenchez un **join / uplink de test** depuis un équipement connu.
- Vérifiez les trames sur le LNS et (si applicable) un downlink de test pour les sites en UDP PF.

Checklist disponible en Annexe 5

Cette routine valide la **chaîne complète** : administration sécurisée → heure/bande correcte → session passerelle ↔ LNS → association (join) → uplink → downlink.

9. HISTORIQUE DU DOCUMENT

Version	Contenu
V 1.0	Création

ANNEXE 1 GLOSSAIRE & ACRONYMES

Terme / Acronyme	Nom détaillé	Définition	Où / pourquoi c'est important
2G / 3G / 4G (LTE Cat-1)	Réseaux cellulaires 2G/3G/4G	Générations de réseaux mobiles ; Cat-1 est une catégorie LTE couramment supportée pour le M2M.	Capacités et couverture de la liaison cellulaire (backhaul).
ABP	Activation By Personalization	Activation avec des clés de session fixes (pas de	Choix lors de la mise en service ; moins

Terme / Acronyme	Nom détaillé	Définition	Où / pourquoi c'est important
		procédure de join).	courant qu'OTAA.
ACK	Acknowledgement	Accusé de réception confirmant qu'une trame a été reçue (ex. downlink confirmé).	Vérifie une livraison fiable lors des tests.
ADR	Adaptive Data Rate	Le réseau optimise le débit et/ou la puissance RF pour l'équipement.	Impacte portée, temps d'antenne et autonomie.
APN	Access Point Name	Profil opérateur permettant au modem d'obtenir une connectivité IP.	Paramètre indispensable en configuration cellulaire.
AppKey / NwkKey	Application/Network Key	Clés racines OTAA utilisées pour dériver les clés de session lors du join.	Nécessaires pour enregistrer les équipements sur le LNS.
Application Server	—	Système applicatif qui consomme les données décodées et les intègre au SI/GTB.	Aboutissement de la chaîne de données LoRaWAN.
Authorized IPs	—	Liste blanche d'IP autorisées à accéder aux services via le WAN cellulaire.	Première barrière si l'interface web ou les downlinks UDP sont exposés via le cellulaire.
Autoreset	—	Redémarrage planifié ou récupération en dernier recours si l'IP ne revient pas.	Fiabilité en exploitation (jour 2) ; à utiliser avec parcimonie.
BASICS STATION (WSS)	—	Protocole LoRaWAN passerelle ↔ LNS via WebSockets (sécurisés) (WSS).	Alternative au Packet Forwarder UDP ; requiert confiance TLS (CA) et heure correcte.
CA (Root CA)	Certificate Authority	Ancre de confiance utilisée pour valider les certificats TLS des serveurs.	Requis pour WSS/MQTTs/HTTPs si des CA privées sont utilisées.
Cat-1	LTE Category 1	Profil de capacités modem LTE (débit/fonctions).	Capacité modem ; attentes de couverture.
CHAP / PAP	Challenge-Handshake / Password Auth	Méthodes d'authentification pour les identifiants APN.	À paramétrer selon l'opérateur pour l'attachement réseau.

Terme / Acronyme	Nom détaillé	Définition	Où / pourquoi c'est important
Class A / C	Classes LoRaWAN	A : très basse conso ; C : écoute quasi continue (plus favorable aux downlinks).	Impacte le timing des downlinks et la consommation.
CN / SAN	Common Name / Subject Alt Name	Champs du certificat qui doivent correspondre au nom d'hôte du serveur.	Évite les erreurs TLS en HTTPS/WSS.
Codec (Payload Decoder)	—	Logique (JavaScript ou intégrée) qui décode la trame en champs exploitables.	Valide la chaîne de données lors des tests d'uplink.
DevEUI	Device EUI-64	Identifiant unique global d'un équipement.	Nécessaire pour enregistrer les équipements sur le LNS.
DHCP	Dynamic Host Configuration Protocol	Attribue automatiquement IP/masque/passerelle/DNS.	Simplifie la mise en service Ethernet.
DNS	Domain Name System	Résout les noms (ex. NTP, WSS) en adresses IP.	Indispensable pour des serveurs NTP en nom de domaine et des URLs WSS.
Downlink	—	Message réseau → équipement.	Prouve le chemin entrant (notamment en UDP PF).
E2E	End-to-End	Chaîne complète de l'équipement (RF) jusqu'à l'application.	Réception de site et contrôles périodiques.
EARFCN	E-UTRA Absolute RF Channel Number	Indice de canal LTE (déduit bande et fréquence).	Diagnostics AT pour la RF cellulaire.
EUI-64	Extended Unique Identifier (64-bit)	Format 64 bits des identifiants passerelle/équipement.	Utilisé comme Gateway EUI / DevEUI.
Factory Settings	—	Restaure la configuration usine (efface la configuration).	À n'utiliser qu'après export d'une sauvegarde.
FCntUp / FCntDown	Frame Counters	Compteurs monotones des trames uplink/downlink.	Aide à détecter resets/rejeux ; utile pour valider un downlink.
Firmware	—	Image logicielle de la passerelle.	Mises à jour via Maintenance → Firmware.
Gateway EUI	—	Identifiant EUI-64 de la passerelle vu par le LNS.	Doit correspondre à l'enregistrement sur le

Terme / Acronyme	Nom détaillé	Définition	Où / pourquoi c'est important
			LNS.
HTTP / HTTPS	HyperText Transfer Protocol (Secure)	Accès navigateur à l'interface web ; HTTPS chiffre et authentifie.	HTTPS à imposer en production ; installer un certificat adapté.
Certificat / clé HTTPS (PEM)	—	Certificat serveur et clé privée au format PEM.	Nécessaire pour supprimer les avertissements navigateur en HTTPS.
IMEI	International Mobile Equipment Identity	Identifiant matériel du modem.	Visible dans Status ; utile pour les tickets support.
IP / Masque / Passerelle	—	Paramètres d'adressage IP.	Déploiements Ethernet en IP fixe et validation.
IP67	—	Étanche à la poussière et protégé contre l'immersion (courte durée) jusqu'à 1 m.	Indice de protection du boîtier.
Join (OTAA)	Over-The-Air Activation	L'équipement demande à joindre ; le LNS accepte et dérive les clés de session.	Première preuve fonctionnelle en mise en service.
JoinEUI (AppEUI)	Join/Application EUI	Identifiant utilisé pendant le join OTAA.	Doit correspondre à la configuration LNS/application.
LAN / VLAN	Local Area Network / Virtual LAN	Réseau local et segmentation réseau (VLAN).	Concerne les déploiements Ethernet chez le client.
LNS	LoRaWAN Network Server	Gère équipements, MAC, ADR, déduplication, downlinks.	Cible vers laquelle la passerelle relaie (ou serveur LoRaWAN embarqué).
LoRa	Long Range (couche RF)	Radio à étalement de spectre utilisée par LoRaWAN.	Couche physique entre équipement et passerelle.
LoRaWAN	—	Suite de protocoles au-dessus de LoRa (MAC + réseau).	La pile IoT déployée sur le site.
LTEINFO / GSTATUS	—	Diagnostics AT du modem Sierra (cellule, RSRP/RSRQ/SINR, bandes).	Photo rapide de l'état radio cellulaire.
MAC (Ethernet)	Media Access Control	Adresse matérielle de l'interface Ethernet.	Visible dans Status ; inventaire/IT.

Terme / Acronyme	Nom détaillé	Définition	Où / pourquoi c'est important
MAC Commands	Commandes MAC LoRaWAN	Messages de contrôle réseau (ex. ADR, LinkCheck).	Observables sur le LNS en diagnostic.
MQTT / MQTTs	Message Queue Telemetry Transport (secure)	Protocole pub/sub léger utilisé par certaines intégrations.	Utilisé par les intégrations du serveur LoRaWAN embarqué.
NAT	Network Address Translation	Traduction d'adresses privées → publiques.	Explique les limites d'accès entrant depuis Internet.
NOC	Network Operations Center	Équipe en charge de l'exploitation réseau.	Concernée par les listes d'autorisation et les tickets.
NTP	Network Time Protocol	Synchronise l'heure de l'équipement.	Requis pour TLS et des journaux cohérents.
OTAA	Over-The-Air Activation	Méthode d'activation sécurisée basée sur des clés racines.	Mode d'activation recommandé.
Packet Forwarder (UDP)	—	Protocole Semtech UDP (uplink/downlink) vers le LNS.	Simple et courant ; nécessite l'UDP entrant autorisé pour les downlinks.
PCI	Physical Cell ID	Identifiant de cellule LTE (couche physique).	Diagnostics AT (cellule servante/voisines).
PEM	Privacy-Enhanced Mail (format)	Format texte des certificats/clés (-----BEGIN CERTIFICATE-----).	Requis sur les pages HTTPS/WSS/CA.
PKCS#1 / PKCS#8	—	Encodages possibles des clés privées en PEM.	Formats de clé privée acceptés par l'interface web.
PIN / PUK	Personal ID / Unlock Key	Codes de sécurité SIM.	3 PIN erronés bloquent la SIM (déblocage via PUK).
PoE	Power over Ethernet	Alimentation via RJ45 (non supportée sur IRIS).	Clarifie les attentes d'alimentation.
PTP (non utilisé ici)	Precision Time Protocol	Alternative à NTP pour une synchronisation plus précise.	Non supporté ; utiliser NTP.
Reboot	—	Redémarrage contrôlé sans modifier la configuration.	À utiliser en maintenance ou en récupération.

Terme / Acronyme	Nom détaillé	Définition	Où / pourquoi c'est important
RSRP / RSRQ / SINR	Indicateurs LTE	Puissance, qualité et interférences (cellulaire).	Évaluer la qualité du lien cellulaire sur site.
SIM	Subscriber Identity Module	Carte opérateur fournissant le service cellulaire.	Indispensable pour un backhaul cellulaire.
SNR (LoRa)	Signal-to-Noise Ratio	Indicateur de qualité du lien radio LoRa.	Vérification de cohérence sur les trames uplink.
Static IP	—	Adressage IP fixe (vs DHCP).	Fréquent en réseau entreprise ; à coordonner avec l'IT.
Status Page	—	Tableau de bord en lecture seule.	Première page pour vérifier heure, IP, état backhaul et LoRaWAN.
Syslog	System Log	Journaux système/applicatifs (tampon) ; exportables/téléchargeables.	Preuves pour diagnostic / tickets support.
TAC	Tracking Area Code	Code de zone de poursuite LTE.	Diagnostics AT pour l'enregistrement réseau.
TLS 1.2	Transport Layer Security	Chiffrement/authentification pour HTTPS/WSS/MQTTs.	Référence sécurité ; nécessite heure correcte et CA.
Uplink	—	Message équipement → réseau.	Premier succès visible après join.
UDP / TCP	User/Transmission Control Protocol	Couches transport (UDP pour PF ; TCP pour HTTPS/WSS).	Pilote règles firewall et choix "Authorized IPs".
WSS / WS	(Secure) WebSocket	Canal TCP persistant (TLS) utilisé par Basics Station.	Requiert CA racine et heure correcte.
Watchdog ("Keep Online")	—	Ping d'une cible et récupération des sessions data cellulaires bloquées.	Améliore la résilience sur backhaul cellulaire.

ANNEXE 2 DEMARRAGE RAPIDE

Mettre un premier capteur en service, voir les uplinks et envoyer un downlink de test.

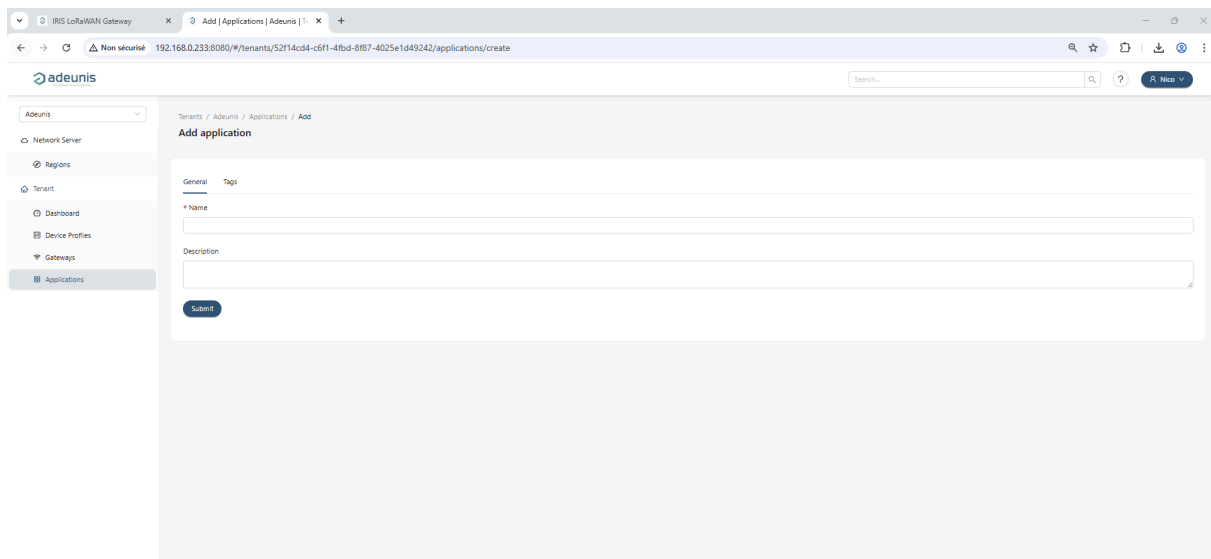
Prérequis

- La passerelle est connectée et apparaît en ligne **"Online"** dans **Tenant** → **Gateways**.
- Vous connaissez le **DevEUI**, **JoinEUI (AppEUI)** et **AppKey** du capteur.

Etapes

1. Créer une application

Aller dans **Tenant** → **Applications** → **Add application**. Donner un nom à votre application et enregistrer.

The screenshot shows a web browser window with the Adeunis interface. The address bar shows a URL starting with '192.168.0.233:8080/#/tenants/52f14cd4-c6f1-41bd-8f87-4025e1d49242/applications/create'. The left sidebar has a menu with 'Adeunis' at the top, followed by 'Network Server', 'Regions', 'Tenant', 'Dashboard', 'Device Profiles', 'Gateways', and 'Applications' (which is highlighted). The main content area is titled 'Add application' and has tabs for 'General' and 'Tags'. Under the 'General' tab, there is a 'Name' field, a 'Description' field, and a 'Submit' button at the bottom.

2. Créer/choisir un profil d'équipement

Aller dans **Tenant** → **Device Profiles** (ou utiliser un profil existant, e.g., *Adeunis_COMFORT*).

Vérifier **Region** = **EU868**, **LoRaWAN MAC** = **1.0.x**, et l'ADR selon besoin.

Name	Region	MAC version	Revision	Supports OTAA	Supports Class-B	Supports Class-C
Adeunis_ANALOG	EU868	LoRAWAN 1.0.2	B	yes	no	no
Adeunis_ANALOG_PWR	EU868	LoRAWAN 1.0.2	B	yes	no	yes
Adeunis_BREATH	EU868	LoRAWAN 1.0.2	B	yes	no	yes
Adeunis_COMFORT	EU868	LoRAWAN 1.0.4	RP002-1.0.4	yes	no	no
Adeunis_COMFORT_SERENITY	EU868	LoRAWAN 1.0.4	RP002-1.0.4	yes	no	no
Adeunis_DELTA_P	EU868	LoRAWAN 1.0.2	B	yes	no	no
Adeunis_DRY_CONTACTS	EU868	LoRAWAN 1.0.4	RP002-1.0.4	yes	no	yes
Adeunis_MOOBUS	EU868	LoRAWAN 1.0.2	B	yes	no	yes
Adeunis_PULSE	EU868	LoRAWAN 1.0.4	RP002-1.0.4	yes	no	no
Adeunis_PULSE_ATEX	EU868	LoRAWAN 1.0.2	B	yes	no	no
Adeunis_TEMP	EU868	LoRAWAN 1.0.4	RP002-1.0.4	yes	no	yes
Adeunis_TEMP2S	EU868	LoRAWAN 1.0.4	RP002-1.0.4	yes	no	yes
Adeunis_TTC_CBE_LYNKY_MONO	EU868	LoRAWAN 1.0.2	B	yes	no	no
Adeunis_TTC_CBE_LYNKY_TRI	EU868	LoRAWAN 1.0.2	B	yes	no	no
Adeunis_TTC_PHE_FMI	EU868	LoRAWAN 1.0.2	B	yes	no	no
FTD	EU868	LoRAWAN 1.0.2	B	yes	no	no

3. Enregistrer l'équipement (OTAA)

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

- Renseigner **Name/Description**.
- **DevEUI**, **JoinEUI** (AppEUI), **Device profile**.
- Dans **OTAA keys**, coller l'**AppKey**.
- Enregistrer.

Add device

Device | Tags | Variables

* Name

Description

* Device EUI (EU64) MSB C D

Join EUI (EU64) MSB C D

* Device profile

Device is disabled ☐

Disable frame-counter validation ☐

Submit

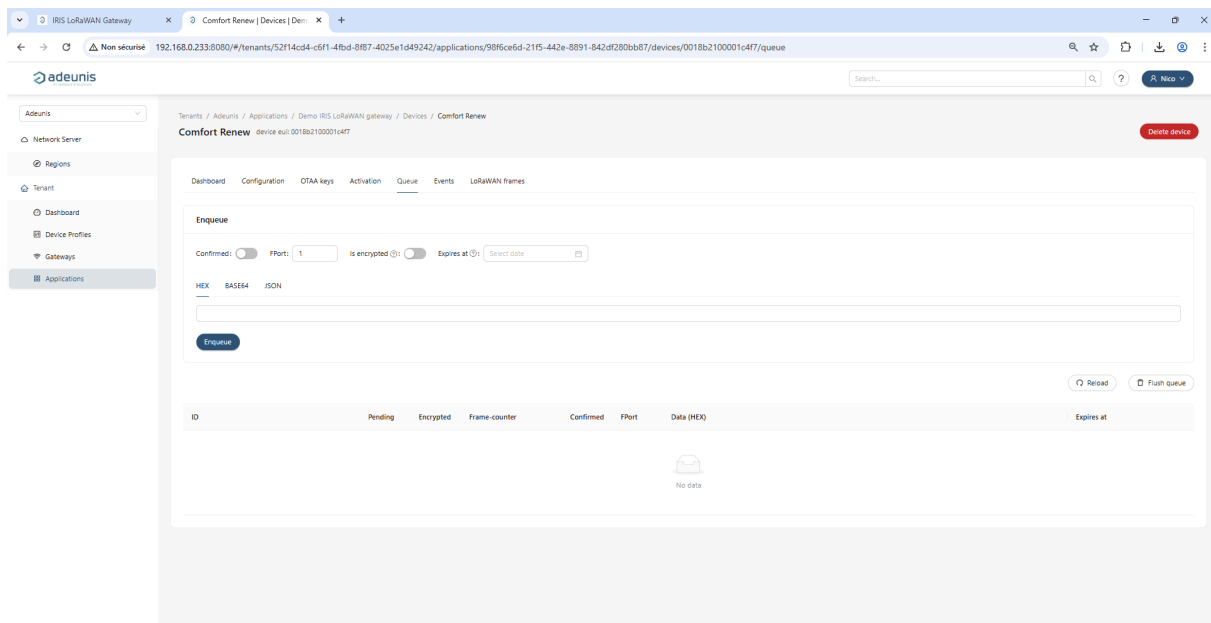
4. Démarrer / réinitialiser l'équipement et attendre un événement de Join

Vérifier **Device** → **LoRaWAN frames / Events** pour *JoinRequest/JoinAccept* et les premiers uplinks.

5. (Optionnel) Envoyer un downlink de test

Ouvrir **Device** → **Queue** : définir le **FPort** (≠0), coller la trame (HEX/Base64/JSON), choisir **Confirmed** si nécessaire, puis **Enqueue**.

Le downlink sera délivré à la prochaine fenêtre de réception (Class A) ou immédiatement (Class C)



ANNEXE 3 ENREGISTRER UN CAPTEUR ADEUNIS COMFORT

Cet exemple décrit comment enregistrer un équipement terminal **Adeunis COMFORT** (température & humidité indoor) dans l'interface du **serveur LoRaWAN embarqué**, en suivant le même déroulé que la section **5.6.7 Ajouter un capteur**.

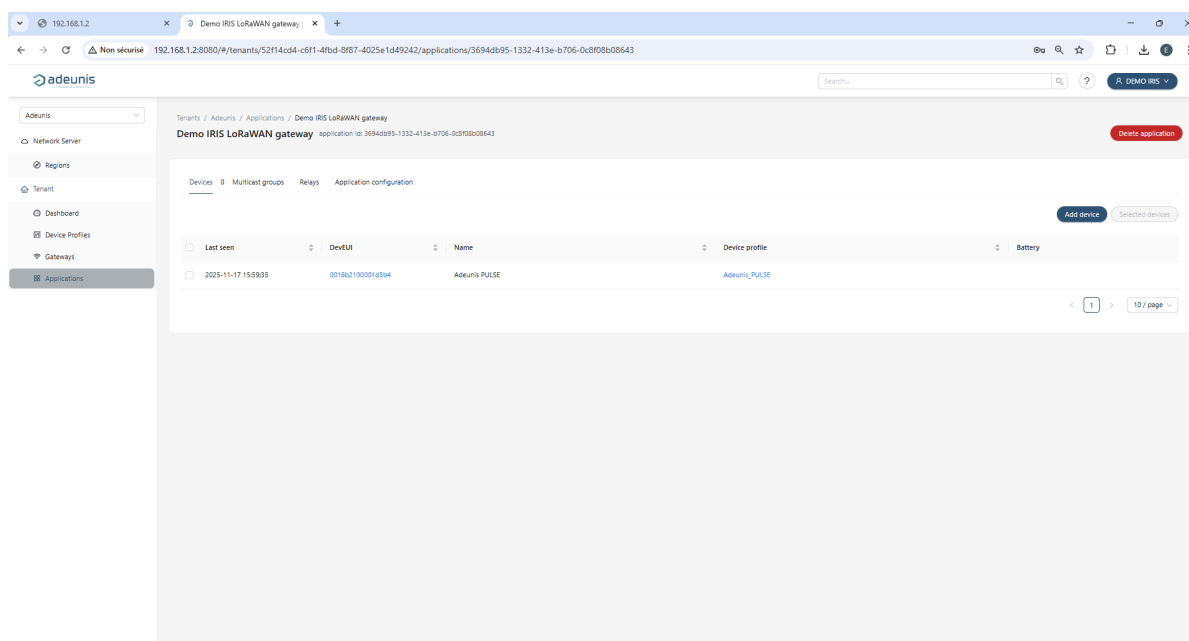
Prérequis

- Les identifiants (DevEUI, AppKey, JoinEUI/AppEUI) ont été fournis par le fabricant.
- Vous avez déjà créé une **Application**.
- Un **Device Profile** correspondant existe (par ex. `Adeunis_COMFORT`, EU868, bonne version LoRaWAN MAC / codec).

Etapes

1. Ouvrir le formulaire d'ajout

Aller dans **Tenant** → **Applications** → **your application** → **Devices** → **Clicker sur le bouton "Add device"**.



2. Renseigner l'onglet Device (exemples ci-dessous)

- **Name** : saisir le texte souhaité, ici : `Adeunis COMFORT – Meeting room 1`
- **Description** : saisir le texte souhaité, ici : `Temperature and Humidity monitoring in Meeting room 1`
- **Device EUI (EUI-64)** : fourni par le fabricant, ici : `001802100001a545`
- **JoinEUI (EUI-64 / AppEUI 1.0.x)** : fourni par le fabricant, ici : `0018025342544831`
- **Device profile** : sélectionner le profil correspondant, ici : `Adeunis_COMFORT`

Si le profil d'équipement n'existe pas il doit être créé.

- Laisser **Device is disabled** sur OFF et **Disable frame-counter validation** sur OFF pour un usage OTAA normal,
- Puis cliquer sur **“Submit”**

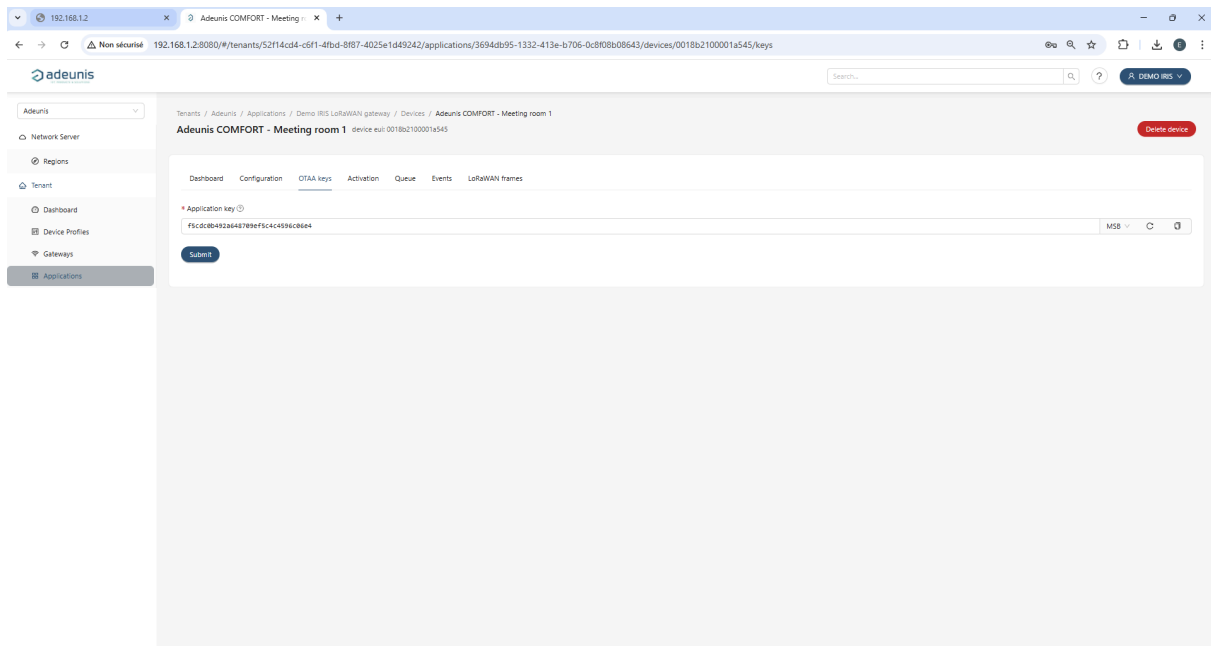
The screenshot shows the 'Add device' page in the Adeunis web application. The left sidebar contains navigation links: Network Server, Regions, Tenant, Dashboard, Device Profiles, Gateways, and Applications (which is highlighted). The main content area is titled 'Add device' and contains the following fields and controls:

- Name:** A text input field containing 'Adeunis COMFORT - Meeting room 1'.
- Description:** A text input field containing 'Temperature and Humidity monitoring in Meeting room 1'.
- Device EUI (EUI64):** A text input field containing '001B0210001A545'.
- Join EUI (EUI64):** A text input field containing '001B0210001A545'.
- Device profile:** A dropdown menu with 'Adeunis_COMFORT' selected.
- Device is disabled:** A toggle switch currently set to 'OFF'.
- Disable frame-counter validation:** A toggle switch currently set to 'OFF'.
- Submit:** A blue button at the bottom left of the form.

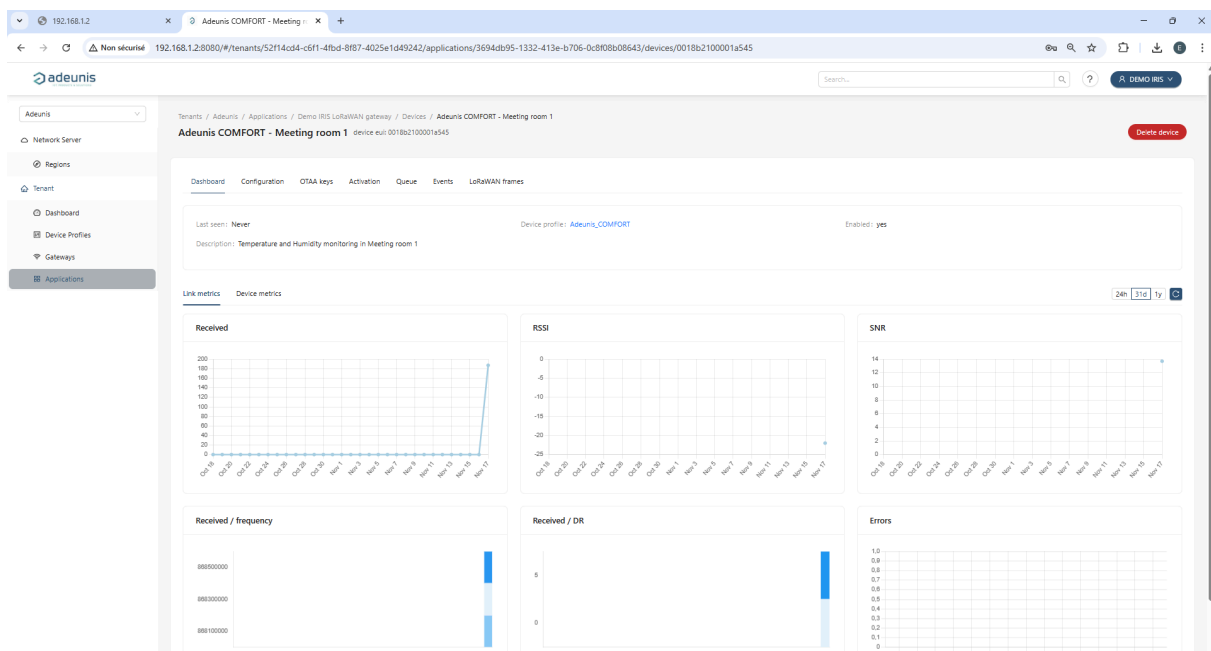
3. Renseigner les clés OTAA

L'onglet **OTAA keys** s'ouvre automatiquement : vous pouvez saisir le dernier identifiant, l'AppKey.

- **AppKey** : fourni par le fabricant, ici : `f5cdc0b492a648709ef5c4c4596c06e4`
(En OTAA LoRaWAN 1.0.x, seule l'AppKey est requise ; en 1.1, il faudrait aussi renseigner NwkKey.)
- Puis cliquer sur **“Submit”**



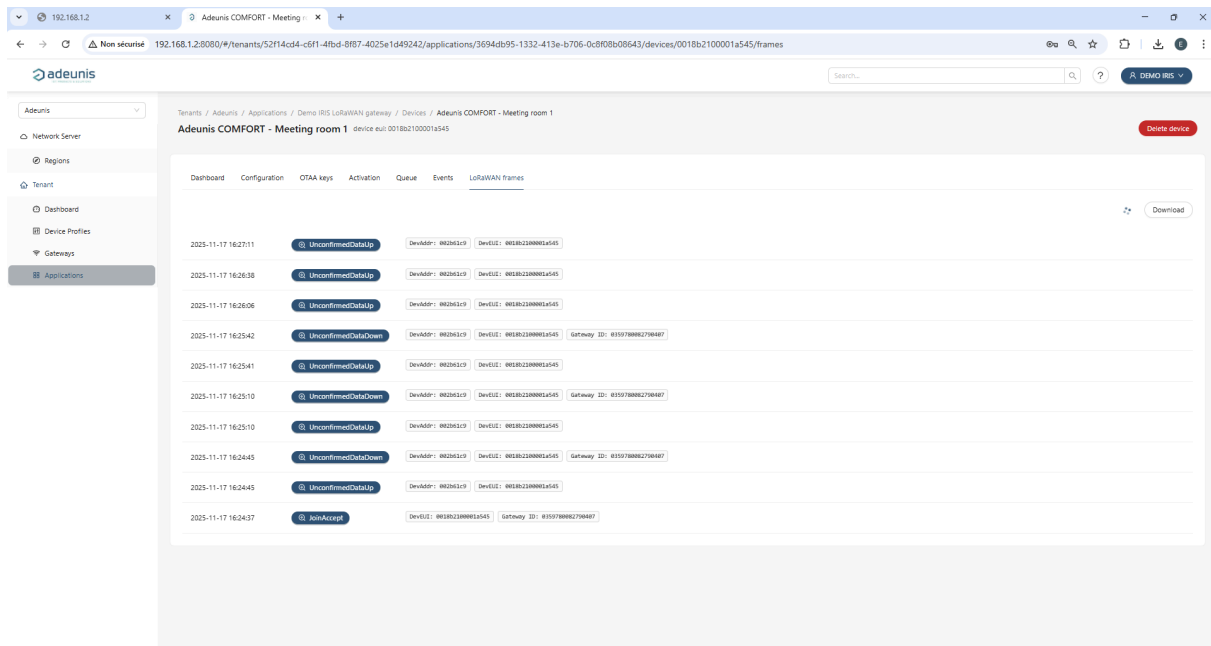
Le panneau d'information du nouvel équipement s'ouvre.



4. Mise en service & vérification

Démarrer le capteur pour lancer le processus de join.

Dans **Applications** → **Devices** → **your device** → **LoRaWAN frames**, vérifier un **Join-request/Join-accept**, puis des uplinks.



Vous pouvez aussi utiliser **Events / Frames** pour accéder aux informations radio et MAC détaillées.

ANNEXE 4 ENREGISTRER UN LOT DE CAPTEURS (CSV/JSON)

Cette annexe explique comment enregistrer de nombreux équipements LoRaWAN en une seule opération via l'outil **Bulk Device Import**. À utiliser lors d'un déploiement initial ou pour ajouter un lot de capteurs à une application existante. Cet exemple suit le même déroulé que la section **5.6.7 Ajouter plusieurs équipements**.

Prérequis

- Vous avez déjà créé l'**Application** qui contiendra ces équipements, et vous connaissez son **Application ID** (voir "Où les trouver" ci-dessous).
- Chaque équipement dispose de ses identifiants et clés (DevEUI, JoinEUI/AppEUI, AppKey ; et pour la 1.1, NwkKey). Ces éléments sont fournis par le fabricant.
- Un **Device Profile** existe pour chaque type d'équipement, et vous connaissez le **Device Profile Name** (voir "Où les trouver" ci-dessous).

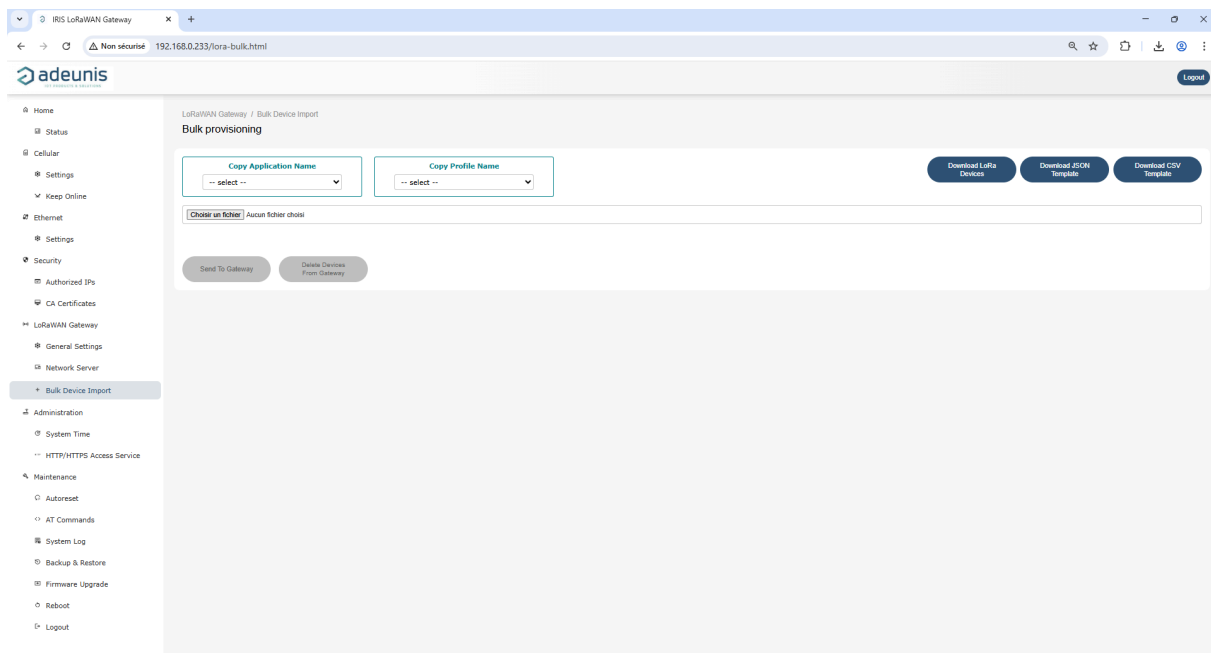
Où récupérer les IDs et clés avant de préparer le fichier CSV/JSON (guide rapide)

Champ (CSV/JSON)	Où le trouver	Remarques
devEui	Sur l'étiquette du produit ou la documentation fabricant.	Identifiant global EUI-64 fourni par le fabricant.
joinEui (a.k.a. AppEUI pour 1.0.x)	Documentation fabricant / étiquette produit.	Requis pour la plupart des équipements OTAA ; la 1.1 utilise JoinEUI, la 1.0.x utilise AppEUI.
appKey (OTAA 1.0.x)	Documentation fabricant / étiquette / fiche d'expédition.	32 hex ; ne jamais "deviner". En LoRaWAN 1.1, fournir aussi nwk_key .
nwkKey (OTAA 1.1)	Documentation fabricant.	Présent uniquement pour les équipements 1.1 ; si non fourni, c'est généralement un équipement 1.0.x.
applicationName	LoRa Server Dashboard → Tenant → Applications → cliquer sur l'application ; le Application Name apparaît dans l'en-tête.	À recopier dans la colonne applicationName lors de l'import en lot.
deviceProfileName	LoRa Server Dashboard → Tenant → Device Profiles → cliquer sur le profil ; le Device Profile Name apparaît dans l'en-tête.	À recopier dans deviceProfileName pour appliquer région/MAC/codec.
isDisabled	À votre choix (dans le modèle).	false en fonctionnement normal ; true pour bloquer tant que vous n'êtes pas prêt.
skipFCntCheck	À votre choix (dans le modèle).	Laisser false . À activer uniquement pour un dépannage ABP temporaire.

Etapes

1. Ouvrir l'outil d'import en lot

Dans l'interface web de la passerelle, aller dans **LoRaWAN** → **Bulk Device Import**.



2. Télécharger le modèle

Cliquer sur **Download JSON template** ou **Download CSV template**.

Toujours partir du modèle afin d'utiliser les noms de champs/colonnes attendus.

Dans cet exemple, nous utilisons le modèle CSV.

	A	B	C	D	E	F	G	H	I	J	K	L
1	name	description	devEui	appKey	nwkKey	joinEui	deviceProfile	applicationName	isDisabled	skipFCntCheck		
2	Example Ade Sensor for m	0018B210000	384E786F39A54445BE9C279E0EF1E0E9	Adeunis_BRE LoRaWAN De	false	false						
3	Example Ade Sensor for m	0018B210000	D2DD78FF18DC47EFBF85EADCCB2C13C	Adeunis_COI LoRaWAN De	false	false						
4	Example Hur Sensor for m	B2903AD184	D2DD78FF58DC47EFBFA5E B31D15AC45	Brand_XYZ_F LoRaWAN De	false	false						
5	Light Sensor Sensor for m	C2903AD184	D2DD78FF58DC47EFBFA5E C31D15AC45	Brand_XYZ_L LoRaWAN De	false	false						
6	Motion Sensi Sensor for d	E2903AD184	D2DD78FF58 11223344556 D31D15AC45	Brand_XYZ_N LoRaWAN De	false	false						
7	Motion Sensi Sensor for d	E2903AD184	D2DD78FF58 11223344556 D31D15AC45	Brand_XYZ_N LoRaWAN De	false	false						
8	Pressure Ser Sensor for m	E2903AD184	D2DD78FF58DC47EFBFA5E E31D15AC45	Brand_XYZ_F LoRaWAN De	false	false						
9												
10												
11												
12												
13												
14												
15												
16												

3. Préparer le fichier

Ici, nous voulons ajouter 2 capteurs à la passerelle.

Il faut donc renseigner **une ligne par équipement** avec :

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

- **app_key** (LoRaWAN 1.0.x) et **nwk_key** (à ajouter pour 1.1) en OTAA ; ou les **clés de session ABP** si applicable
- **device_profile_name** (Device Profile cible)
- **application_name** (Application cible)
- **device_disabled** (true/false)
- **disable_fcnt_check** (true/false)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	name	description	devEui	appKey	nwkKey	joinEui	deviceProfile	applicationName	isDisabled	skipFCntCheck						
2	Adeunis COMFORT	Monitoring of Temperature and Humidity	0018B210000F5CD00B492A648709EF5C	0018B253425	Adeunis_COI	Demo IRIS Lc	false	false	false	false						
3	Adeunis PULSE	Monitoring of Electricity consumption	0018B210000BED49159C025411C45E861	0018B250554	Adeunis_MO	Demo IRIS Lc	false	false	false	false						
4																
5																
6																
7																
8																
9																
10																
11																
12																
13																
14																
15																
16																
17																

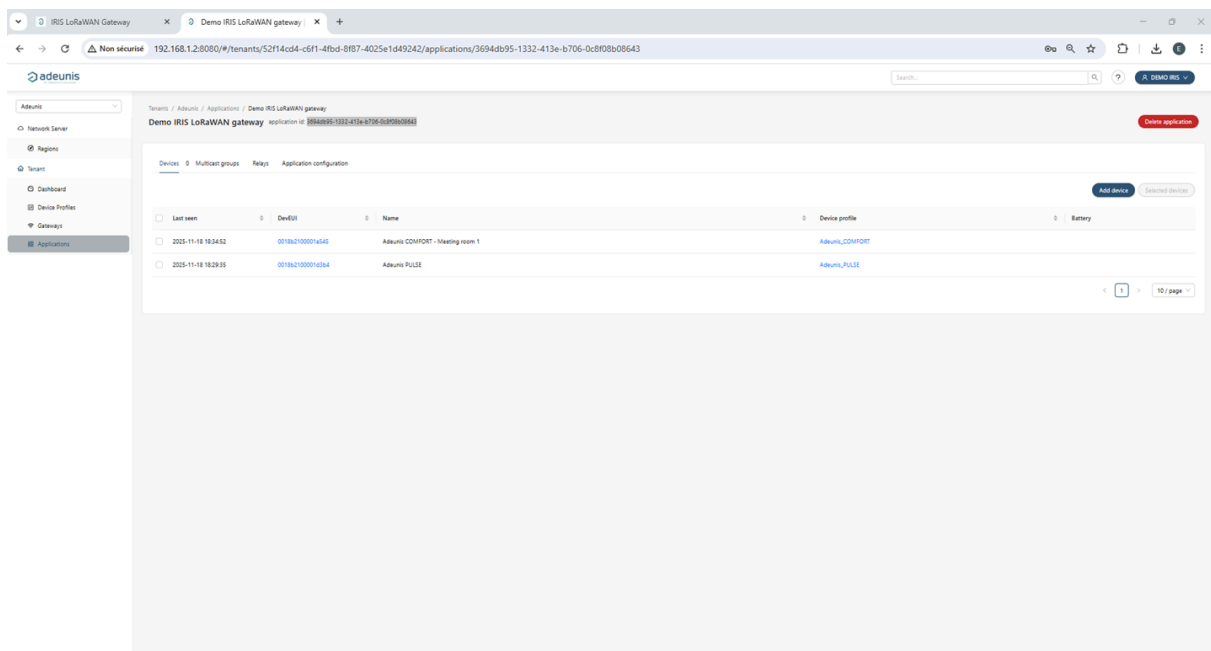
4. Import et execution

Importer le fichier dans **Bulk Device Import**, vérifier l'aperçu, puis choisir **SEND TO GATEWAY** pour créer les équipements listés.

DevEUI (EUI64)	Name	Profile name	Application name
0018B2100001A545	Adeunis COMFORT	Adeunis_COMFORT	Demo IRIS LoRaWAN gateway
0018B2100001D3B4	Adeunis PULSE	Adeunis_MODBUS	

5. Valider

Ouvrir le **LoRa Server dashboard** et aller dans **Tenant** → **Applications** → **Devices** pour confirmer que le lot a créé/mis à jour les équipements attendus.



ANNEXE 5 CHECKLIST DE MAINTENANCE

Cette checklist fournit une routine d'exploitation courte et répétable, à exécuter après une fenêtre de maintenance ou périodiquement, afin de confirmer que la passerelle est saine et que le chemin LoRaWAN (uplink et downlink) fonctionne comme attendu.

Quand l'exécuter

- À la fin de la mise en service (commissioning) ou d'une fenêtre de maintenance.
- Après une **mise à jour firmware** ou un **changement sécurité/réseau** (HTTPS, Authorized IPs, NTP, APN, VLAN).
- **Trimestriellement** en contrôle préventif sur les sites en exploitation longue durée.

Élément	Critères d'acceptation	Résultat	Preuve
Référence Status	Uptime ↑, heure correcte, connectivité amont (Ethernet/cellulaire) OK, IP présente,		Capture Status

Élément	Critères d'acceptation	Résultat	Preuve
	mode/bande/EUI corrects		
Sécurité	Interface web en https avec cadenas/sans avertissement ; Authorized IPs restrictifs ; CA racines présentes (WSS)		Captures (HTTP/HTTPS, Authorized IPs, page CA)
NTP	Serveurs joignables ; fuseau horaire correct		Page NTP + heure sur Status
Santé cellulaire	AT+CSQ , AT+CEREG? , AT!GSTATUS? / AT!LTEINFO? capturés		Sorties console AT
Connectivité LNS	Passerelle online (UDP PF) / Station connectée (WSS) / serveur LoRaWAN embarqué opérationnel		Capture LNS / console embarquée
Join	Join-request + Join-accept observés ; équipement activé		Vue événements équipement (LNS)
Uplink	Uplink de test reçu ; RSSI/SNR cohérents ; décodeur OK		Log de trames LNS
Downlink	Downlink transmis ; l'équipement le reçoit (ACK si confirmé)		Log downlink LNS / indication équipement
Logs	Syslog exporté ; pas d'erreurs critiques		Fichier de logs
Sauvegarde	Configuration exportée (nommée, archivée)		Fichier de configuration
Autoreset	Politique conforme aux règles du site		Capture / note
Reconnexion	Reboot → session PF/WSS restaurée automatiquement		Note courte / horodatage

Cette routine valide le **chemin complet** : admin sécurisé → heure/bande correctes → session passerelle ↔ LNS → join → uplink → downlink.

ANNEXE 6 MATRICE DE DEPANNAGE

Utilisez cette section pour diagnostiquer rapidement les problèmes courants.

Chaque ligne décrit le **symptôme**, les **causes les plus probables**, où **vérifier dans l'interface**, comment **diagnostiquer** et le **correctif**.

Passerelle ↔ serveur LoRaWAN embarqué

Symptôme	Cause(s) probable(s)	Où vérifier	Comment diagnostiquer	Correctif
La passerelle apparaît Offline	Pas d'alimentation / WAN ; l'UDP PF n'atteint pas le serveur LoRaWAN embarqué (pare-feu/NAT) ; mauvais Gateway ID (EUI64)	Liste Tenant → Gateways & Dashboard de la passerelle	Vérifier "Last seen" ; confirmer l'endpoint PF (UDP/1700 par défaut) et le Gateway ID configurés sur la passerelle	Restaurer le WAN ; ouvrir/rediriger UDP/1700 vers le serveur LoRaWAN embarqué ; corriger le Gateway ID (EUI64) ; assurer la synchro NTP
Passerelle Online mais aucun uplink	Décalage région/plan entre passerelle et capteurs ; problème d'antenne	Gateways → [gateway] → LoRaWAN frames	Chercher des trames rx entrantes et leurs fréquences ; comparer au plan du device profile	Aligner région/plan (EU868) ; vérifier antenne, placement, limites de duty-cycle
Onglet certificats TLS ambigu	Notre implémentation supporte uniquement UDP Packet Forwarder ; le TLS côté client n'est pas supporté	Gateways → [gateway] → TLS certificate	—	Ignorer l'onglet TLS pour le moment ; configurer la passerelle en UDP PF uniquement. Voir [Gateways (UDP Packet Forwarder)]

Enregistrement d'un capteur & Join (OTAA/ABP)

Symptôme	Cause(s) probable(s)	Où vérifier	Comment diagnostiquer	Correctif
L'équipement ne rejoint jamais (OTAA)	DevEUI / JoinEUI / AppKey incorrects ; équipement désactivé ;	Applications → [app] → Devices → [device] → Configuration /	Chercher JoinRequest / JoinAccept dans Events ; valider les clés	Corriger les clés ; vérifier que l'équipement est Enabled ; choisir un profil EU868 ;

Symptôme	Cause(s) probable(s)	Où vérifier	Comment diagnostiquer	Correctif
	mauvais device profile (région) ; nonces OTAA épuisés	OTAA keys / Events		Flush OTAA device nonces
Join OK, mais pas de données ensuite	Application envoie sur FPort=0 ; équipement en veille ; codec non sélectionné	Device → Events / LoRaWAN frames / Measurements	Vérifier UnconfirmedDataUp et le FPort ; vérifier l'apparition des champs décodés	Utiliser FPort ≠ 0 pour les données applicatives ; réveiller l'équipement ; associer le bon Codec
Downlink ABP bloqué ("frame-counter not valid")	Compteurs désynchronisés	Device → Activation	Comparer compteurs UL/DL	Réactiver avec les bons compteurs ou (temporairement) Disable frame-counter validation , puis rétablir. Voir [Device details]

Visibilité des uplinks (données absentes)

Symptôme	Cause(s) probable(s)	Où vérifier	Comment diagnostiquer	Correctif
Aucun uplink visible dans l'application	Équipement enregistré dans la mauvaise Application ; mauvais Device profile	Applications → [app] → Devices et Device → Frames	Vérifier que l'équipement est dans la bonne application ; observer les trames en direct	Déplacer l'équipement dans la bonne application ; appliquer le bon profil
ADR instable (DR très haut/bas)	Paramétrage ADR inadapté	Device profile → General	Vérifier l'algorithme ADR et la plage DR autorisée	Ajuster l'ADR ; restreindre la plage au besoin (EU868 DR0... DR5)
Champs décodés absents	Codec non associé / mapping incomplet	Device → Measurements / Codec	La trame brute est présente mais aucune série décodée	Associer le bon codec et vérifier le mapping

Downlinks (un capteur)

Symptôme	Cause(s) probable(s)	Où vérifier	Comment diagnostiquer	Correctif
Enqueued mais jamais délivré (Class A)	Aucun uplink ensuite ; expiration de la file avant l'uplink ; FPort=0	Device → Queue / Events / Frames	Vérifier Expires at dans Queue et la présence d'un uplink après	Déclencher un uplink (bouton/reset/rapport) ; augmenter l'expiration ; utiliser FPort ≠ 0 . Voir [Downlink — single device]
Délivré uniquement via RX2 (plus lent)	Mapping DR RX1 impossible	Device profile → General	Comparer DR uplink vs règles RX1=DR-1	Autoriser une fenêtre DR qui permette RX1, ou accepter la latence RX2
Downlink confirmé répété	Pas d'ACK ; duty-cycle passerelle	Device → Events	Répétitions de ConfirmedDataDown	Utiliser Unconfirmed si possible ; réduire la fréquence ; améliorer la marge radio

Downlinks Multicast

Symptôme	Cause(s) probable(s)	Où vérifier	Comment diagnostiquer	Correctif
La file multicast ne délivre jamais	Équipements en Class A (le multicast "immédiat" nécessite Class C) ; équipement non membre ; clés de groupe incorrectes	Application → Multicast groups et Device → Configuration	Vérifier appartenance au groupe, classe LoRaWAN, clés de groupe	Utiliser des équipements Class C ; ajouter les membres ; valider les clés de groupe ; voir [Downlink — multicast]
Seuls certains membres reçoivent	Différences RF ; classes mixtes ; duty-cycle	LoRaWAN frames par équipement	Comparer RSSI/SNR et DR	Uniformiser la classe ; choisir un DR adapté au groupe ; répéter en espaçant

Applications, Device-profiles, Import en lot

Symptôme	Cause(s) probable(s)	Où vérifier	Comment diagnostiquer	Correctif
Import en lot en échec / équipements dans la mauvaise application	applicationId manquant/incorrect ; nom de profil non conforme ; clés erronées	Tenant → Applications (copier Application ID depuis l'en-tête) et Tenant → Device Profiles (nom exact)	Vérifier en-têtes CSV/JSON et valeurs	Utiliser l' applicationId exact et le nom de profil exact ; vérifier format/longueur DevEUI/JoinEUI/AppKey . Voir [Batch device import]

Passerelles (UDP Packet Forwarder)

Symptôme	Cause(s) probable(s)	Où vérifier	Comment diagnostiquer	Correctif
Passerelle PF invisible	Non ajoutée dans l'UI ; mauvais Gateway ID (EUI64) ; UDP bloqué	Tenant → Gateways (Add gateway)	Vérifier config PF : IP LNS, UDP/1700, EUI	Ajouter la passerelle avec l'EUI exact ; ouvrir pare-feu/NAT ; pointer le PF vers le serveur LoRaWAN embarqué
Online mais aucune trame	Décalage région/plan ; problème d'antenne	Gateways → [gateway] → LoRaWAN frames	Pas de rx sur les canaux attendus	Aligner la région (EU868) ; vérifier antenne et placement. Voir [Gateways (UDP Packet Forwarder)]

MQTT / Intégration (si activée)

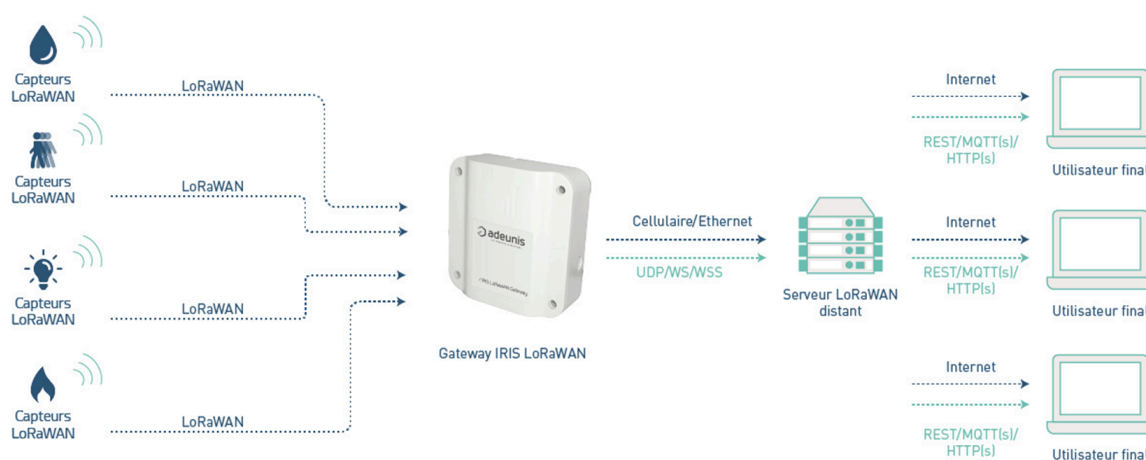
Symptôme	Cause(s) probable(s)	Où vérifier	Comment diagnostiquer	Correctif
Aucun message côté abonné	Mauvaise URL/identifiants/topic broker ; intégration désactivée	Application → Configuration (integration)	Vérifier l'état de connexion et le format de topic	Corriger broker et topic ; vérifier TLS si activé ; redémarrer le consommateur
Données reçues en base64/brutes	Décodeur non appliqué	Device → LoRaWAN frames / Measurements	La trame brute est visible mais pas de champs décodés	Décoder côté application ou activer/associer le bon codec

Performance radio

Symptôme	Cause(s) probable(s)	Où regarder (UI)	Diagnostic	Correctif
RSSI/SNR très faibles	Distance/obstacles ; antenne	Device → Dashboard → Link metrics	RSSI < -120 dBm ; SNR < -10 dB	Déplacer capteur/passerelle ; antenne externe ; réduire le DR
Pertes uplink élevées	Interférences ; duty-cycle	Gateway dashboard	"Trous" dans les  rx	Étalement des émissions ; vérifier canaux ; ADR

ANNEXE 7 CONNEXION D'IRIS À THE THINGS STACK AVEC LE PACKET FORWARDER LoRa Basics™ Station

Cette annexe décrit la procédure permettant de connecter la passerelle LoRaWAN **IRIS** à **The Things Stack** en utilisant le **packet forwarder LoRa Basics™ Station**.



Dans cette architecture, IRIS joue le rôle de **packet forwarder LoRaWAN** : la passerelle reçoit les trames radio LoRa émises par les équipements de terrain, puis les transmet de manière sécurisée via IP vers le serveur de réseau LoRaWAN de The Things Stack. Le décodage des données, la gestion des équipements et les intégrations applicatives sont ensuite assurés par The Things Stack.

IRIS prend en charge le mode **Packet Forwarder** en **UDP** ainsi qu'en **Basics Station**. Dans le cas de The Things Stack, **LoRa Basics™ Station constitue la méthode d'intégration recommandée**, car elle offre une communication WebSocket sécurisée, une authentification par jeton et une gestion centralisée du plan de fréquences.

Prérequis

Prérequis	Description
Passerelle IRIS prête à être configurée	La passerelle est alimentée, accessible via son interface web, et déjà configurée avec une

Prérequis	Description
	connectivité IP, une heure système correcte et un accès sécurisé.
Compte The Things Stack	Un compte utilisateur disposant des droits nécessaires pour enregistrer des passerelles et générer des clés API associées est disponible.
Gateway EUI	Le Gateway EUI peut être trouvé : • sur l'étiquette d'identification située à l'arrière du boîtier ; • dans l'interface web IRIS, sur la page Home → Status ; • ou dans LoRaWAN Gateway → General Settings → ID .
Plan de fréquences	La passerelle devra être enregistrée avec le plan de fréquences Europe 863-870 MHz / EU868 .
Accès réseau	La passerelle doit pouvoir joindre le point d'accès LNS de The Things Stack, généralement via <code>wss://<server-address>:8887</code> .



Le **Gateway EUI** est disponible dans l'interface web IRIS sous **LoRaWAN Gateway** → **General Settings** → **ID**. The Things Stack demande cet identifiant lors de l'enregistrement de la passerelle.

Procédure

1. Enregistrer la passerelle dans The Things Stack

Pour connecter une passerelle IRIS au LNS, il faut d'abord la déclarer dans The Things Stack.

- Connectez-vous à la console **The Things Stack** ;
- Ouvrez le menu **Gateways** ;
- Cliquez sur **+ Add new gateway** ou **+ Register Gateway** pour accéder à la page d'enregistrement.

Voir également les instructions générales : [Adding Gateways](#).

- Renseignez le champ **Gateway EUI** ;
- Cliquez sur **Confirm**.

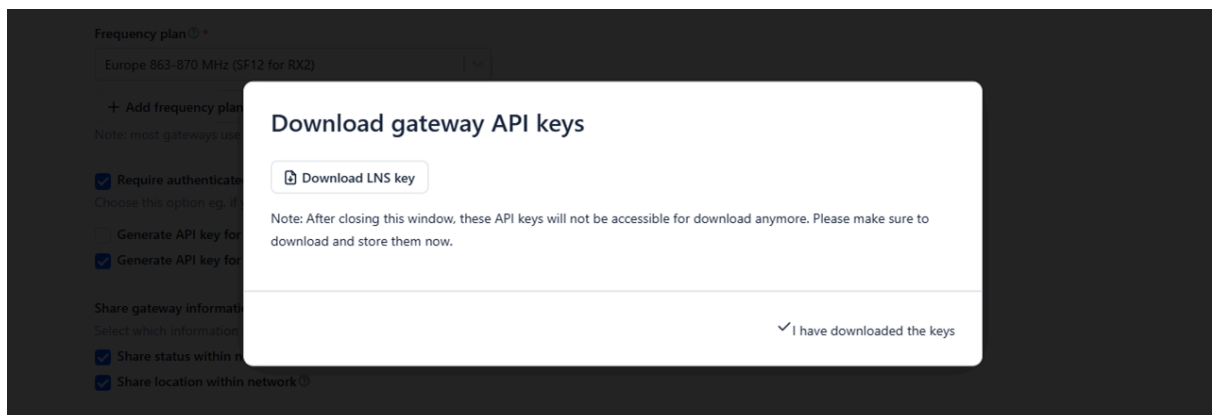
- Dans le formulaire d'enregistrement :
 - sélectionnez le plan de fréquences **Europe 863-870 MHz (SF12 for RX2)** ;
 - choisissez ensuite un **Gateway ID** ;
 - cochez la case **Require authenticated connection** ;
 - sélectionnez l'option **Generate API key for LNS**.
 - Les autres champs sont optionnels.
- Cliquez ensuite sur **Register Gateway** pour finaliser l'enregistrement.

Voir également les instructions générales : [Connecting LNS](#).

2. Télécharger la clé API LNS

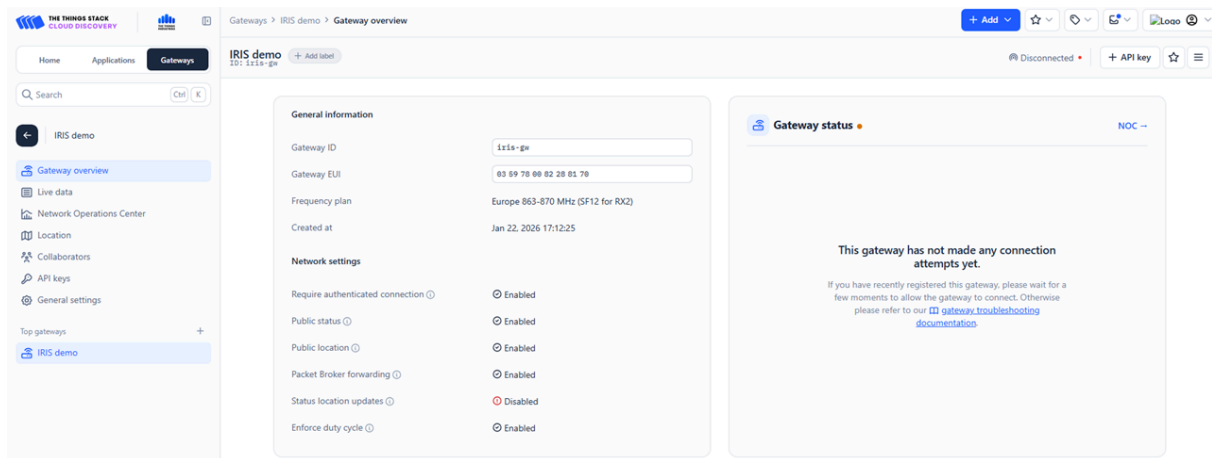
The Things Stack utilise une **clé API** pour authentifier la passerelle lorsqu'elle se connecte en **LoRa Basics™ Station LNS**.

- Un écran s'affiche avec un bouton permettant de télécharger la clé API qui vient d'être créée ;
- Cliquez sur **Download** ;
- Enregistrez cette clé dans un emplacement sûr, puis cliquez sur **I have downloaded the keys**.



Cette clé ne sera plus visible par la suite. En cas de perte, il faudra en générer une nouvelle et la remplacer dans la configuration de la passerelle.

Vous serez ensuite redirigé vers la page de synthèse de la passerelle nouvellement créée.



Une fois cette première configuration effectuée dans The Things Stack, vous pouvez poursuivre avec la configuration du transfert LoRa dans l'interface web de la passerelle.



Pour un premier accès à l'interface web IRIS, vous pouvez vous reporter au [guide utilisateur](#).

Avant de configurer le transfert LoRa, veuillez à paramétrer la [connectivité IP](#), l'[heure système](#) et la [sécurité](#).

Une fois ces éléments en place, la passerelle est prête à être configurée en packet forwarder LoRa.

3. Configurer IRIS en mode Basics™ Station LNS

- Ouvrez l'interface web IRIS ;
- Allez dans **LoRaWAN Gateway** → **General Settings** ;
- Cochez **Enable the LoRaWAN stack** ;
- Sélectionnez **LoRa Gateway - Semtech Basics™ Station** comme mode ;
- Dans le champ **Server Url** du [LNS](#), saisissez :

```
wss://<server-address>:8887
```

<server-address> correspond à l'adresse de votre déploiement The Things Stack.

Par exemple :

```
wss://eu1.cloud.thethings.network:8887
```

- Importez le [fichier de clé LNS](#) dans le champ **Basics™ Station KEY** ;
- Cliquez ensuite sur **Save & Apply** pour enregistrer la configuration.

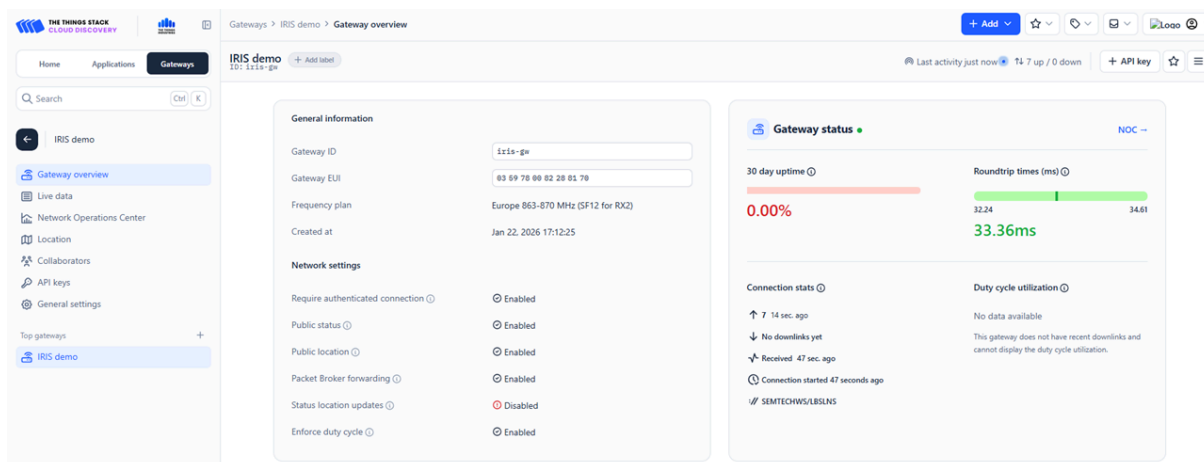
The screenshot shows the 'General Settings' page for a LoRaWAN Gateway. The left sidebar contains a navigation menu with options like Home, Status, Cellular, Settings, Keep Online, Ethernet, Security, Authorized IPs, CA Certificates, LoRaWAN Gateway, General Settings (selected), Administration, System Time, HTTP/HTTPS Access Service, Maintenance, Autoreset, AT Commands, System Log, Backup & Restore, Firmware Upgrade, Reboot, and Logout. The main content area is titled 'LoRaWAN Gateway / General Settings' and 'General Settings'. It includes a checkbox to 'Enable the LoRaWAN stack', a 'Band' dropdown set to 'eu868', an 'ID' input field with '835870000', a 'Mode' dropdown set to 'LoRa Gateway - Basic Station (LNS)', a 'Server URL' input field with 'vns.iadeunis.eu:1 cloud.thethingsindustries:8087', a 'Basic Station KEY' section with an 'Authorization: Bearer' token, and a 'Basic Station Certificate' section. At the bottom, there are 'Save & Apply' and 'Basic Station Log' buttons.

La configuration est désormais terminée : la passerelle devrait se connecter à The Things Stack en quelques secondes.

Validation

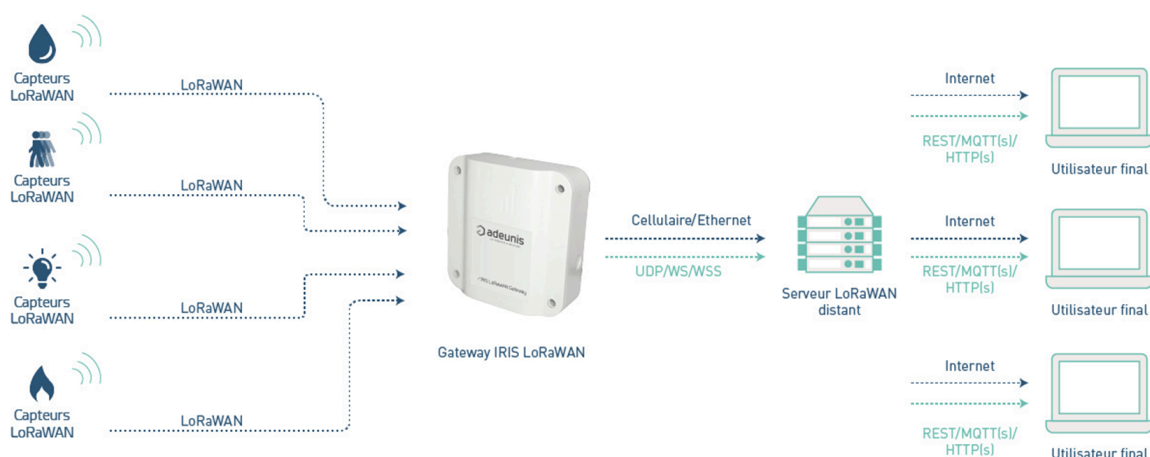
L'intégration est considérée comme valide lorsque :

1. la page **Home** → **Status** d'IRIS indique que la pile LoRaWAN est active ;
2. la passerelle apparaît comme **connected** dans The Things Stack ;
3. l'horodatage **Last seen** se met à jour régulièrement ;
4. la vue **Live data** de The Things Stack affiche les événements de connexion de la passerelle ;
5. un uplink LoRaWAN de test provenant d'un équipement connu remonte bien dans The Things Stack ;
6. un downlink de test peut être planifié puis transmis depuis The Things Stack vers l'équipement.



ANNEXE 8 CONNEXION D'IRIS À THE THINGS STACK AVEC LoRa Basics™ Station ET PROVISIONING CUPS

Cette annexe décrit la procédure permettant de connecter la passerelle LoRaWAN **IRIS** à **The Things Stack** en utilisant le **packet forwarder LoRa Basics™ Station avec provisioning CUPS**.



CUPS signifie **Configuration and Update Server**. Ce mécanisme est utilisé pour provisionner automatiquement la configuration Basics Station de la passerelle. Dans ce

mode, IRIS se connecte d'abord au point d'accès CUPS, récupère la configuration LNS nécessaire, puis établit ensuite la connexion LoRa Basics™ Station vers The Things Stack.

Dans cette architecture, IRIS joue le rôle de **packet forwarder LoRaWAN sécurisé** : la passerelle reçoit les trames radio LoRa émises par les équipements de terrain, puis les transmet via IP au serveur de réseau LoRaWAN de The Things Stack. La gestion des équipements, le décodage des données, les intégrations et le routage applicatif sont ensuite assurés dans The Things Stack.

L'utilisation de **CUPS** est particulièrement recommandée lorsque le provisionnement des passerelles doit être géré de manière centralisée, notamment dans le cadre de déploiements de flotte ou lorsque la configuration LNS et les identifiants d'accès peuvent évoluer dans le temps.

Prérequis

Prérequis	Description
Passerelle IRIS prête à être configurée	La passerelle est alimentée, accessible via son interface web, et déjà configurée avec une connectivité IP, une heure système correcte et un accès sécurisé.
Compte The Things Stack	Un compte utilisateur disposant des droits nécessaires pour enregistrer des passerelles et générer des clés API CUPS et LNS est disponible.
Gateway EUI	Le Gateway EUI peut être trouvé : • sur l'étiquette d'identification située à l'arrière du boîtier ; • dans l'interface web IRIS, sur la page Home → Status ; • ou dans LoRaWAN Gateway → General Settings → ID.
Plan de fréquences	La passerelle devra être enregistrée avec le plan de fréquences Europe 863-870 MHz / EU868 .
Source du certificat Root CA	Le certificat Root CA nécessaire à la validation TLS peut être téléchargé depuis la documentation The Things Stack ou fourni par l'administrateur d'une instance TTS privée.
Accès réseau	La passerelle doit pouvoir joindre le point d'accès CUPS, généralement via <code>https://<server-address>:443</code> , puis le point d'accès LNS après provisioning.



Le **Gateway EUI** est disponible dans l'interface web IRIS sous **LoRaWAN Gateway** → **General Settings** → **ID**. The Things Stack demande cet identifiant lors de l'enregistrement de la passerelle.

Procédure

1. Enregistrer la passerelle dans The Things Stack

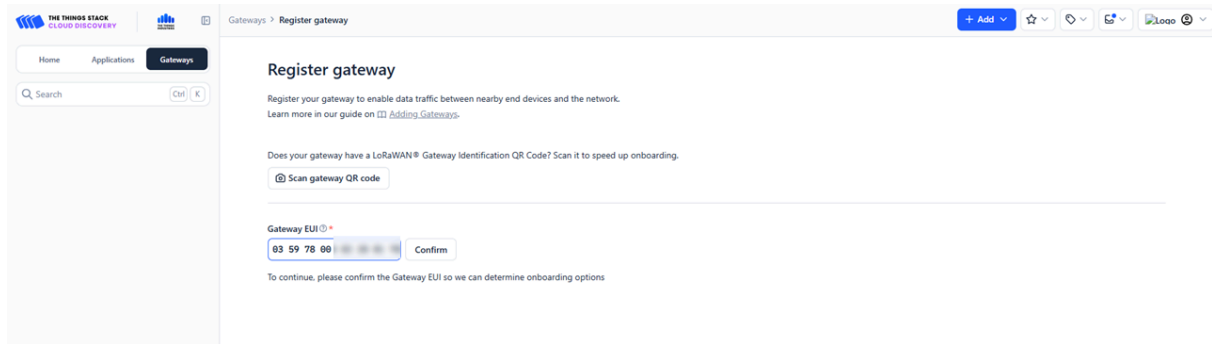
Pour connecter une passerelle IRIS au LNS, il faut d'abord la déclarer dans The Things Stack.

- Connectez-vous à la console **The Things Stack** ;
- Ouvrez le menu **Gateways** ;
- Cliquez sur **+ Add new gateway** ou **+ Register Gateway** pour accéder à la page d'enregistrement.

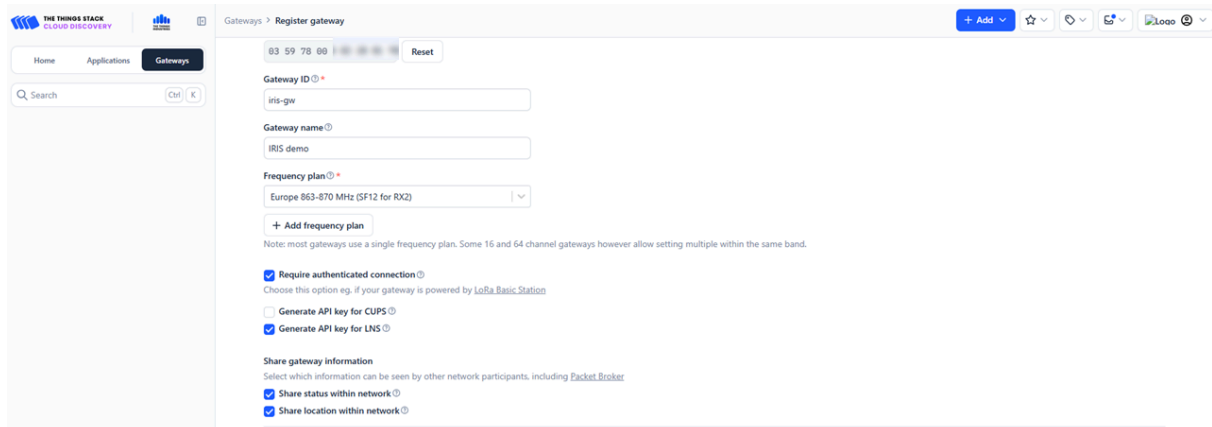
The screenshot shows the 'Register gateway' page in The Things Stack. The page has a sidebar with 'Home', 'Applications', and 'Gateways' (selected). The main content area is titled 'Register gateway' and includes instructions: 'Register your gateway to enable data traffic between nearby end devices and the network. Learn more in our guide on [Adding Gateways](#).' Below this, there is a section asking 'Does your gateway have a LoRaWAN® Gateway Identification QR Code? Scan it to speed up onboarding.' with a 'Scan gateway QR code' button. Further down, there is a 'Gateway EUI' input field with a red asterisk, a 'Continue without EUI' button, and a note: 'To continue, please confirm the Gateway EUI so we can determine onboarding options'.

Voir également les instructions générales : [Adding Gateways](#).

- Renseignez le champ **Gateway EUI** ;
- Cliquez sur **Confirm**.



- Dans le formulaire d'enregistrement :
 - sélectionnez le plan de fréquences **Europe 863-870 MHz (SF12 for RX2)** ;
 - choisissez ensuite un **Gateway ID** ;
 - cochez la case **Require authenticated connection** ;
 - sélectionnez les deux options suivantes :
 - **Generate API key for CUPS**
 - **Generate API key for LNS**
 - Les autres champs sont optionnels.
- Cliquez ensuite sur **Register Gateway** pour finaliser l'enregistrement.



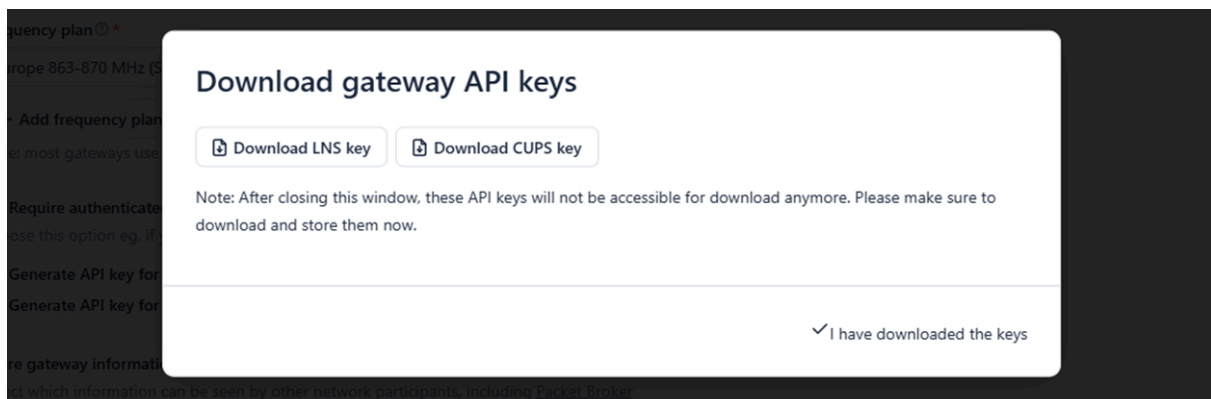
Voir également les instructions générales : [Connecting LNS](#).

2. Télécharger les clés API

CUPS et LNS utilisent deux clés API distinctes :

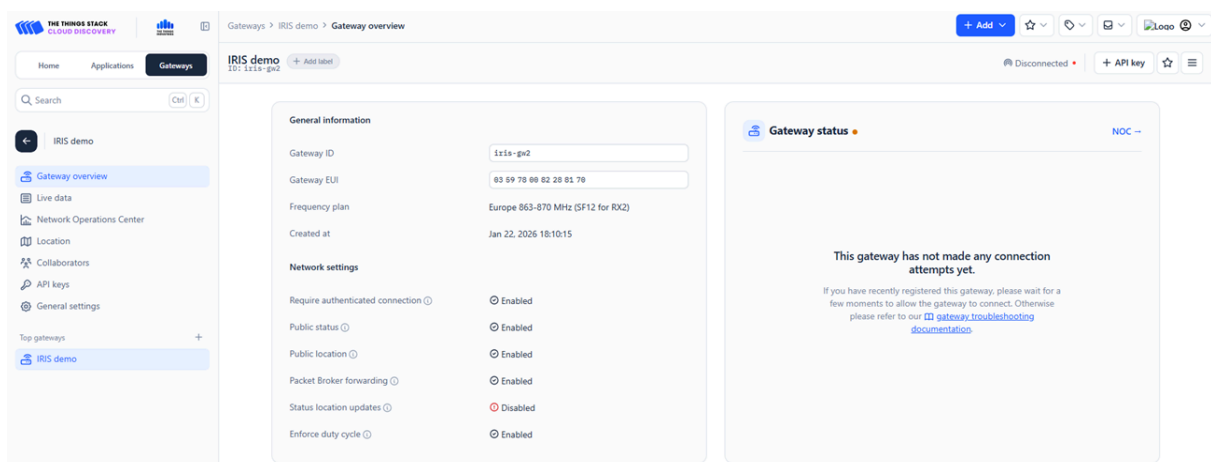
- la clé **CUPS** permet d'accéder aux informations de la passerelle, de modifier certains paramètres de base et de récupérer les secrets de provisioning ;
- la clé **LNS** permet l'échange du trafic entre la passerelle et le réseau LoRaWAN.

- Un écran s'affiche avec les boutons permettant de télécharger les clés API nouvellement créées ;
- Téléchargez la **clé API CUPS** ;
- Téléchargez la **clé API LNS** ;
- Enregistrez ces clés dans un emplacement sûr, puis cliquez sur **I have downloaded the keys**.



Les clés ne pourront plus être affichées par la suite. Si l'une d'elles est perdue, il faudra en générer une nouvelle puis mettre à jour la configuration de la passerelle.

Vous serez ensuite redirigé vers la page de synthèse de votre passerelle nouvellement créée.



Une fois cette première configuration effectuée dans The Things Stack, vous pouvez poursuivre avec la configuration du transfert LoRa dans l'interface web de la passerelle.



Pour un premier accès à l'interface web IRIS, vous pouvez vous reporter au [guide utilisateur](#).

Avant de configurer le transfert LoRa, veuillez à paramétrer la [connectivité IP](#), l'[heure système](#) et la [sécurité](#).

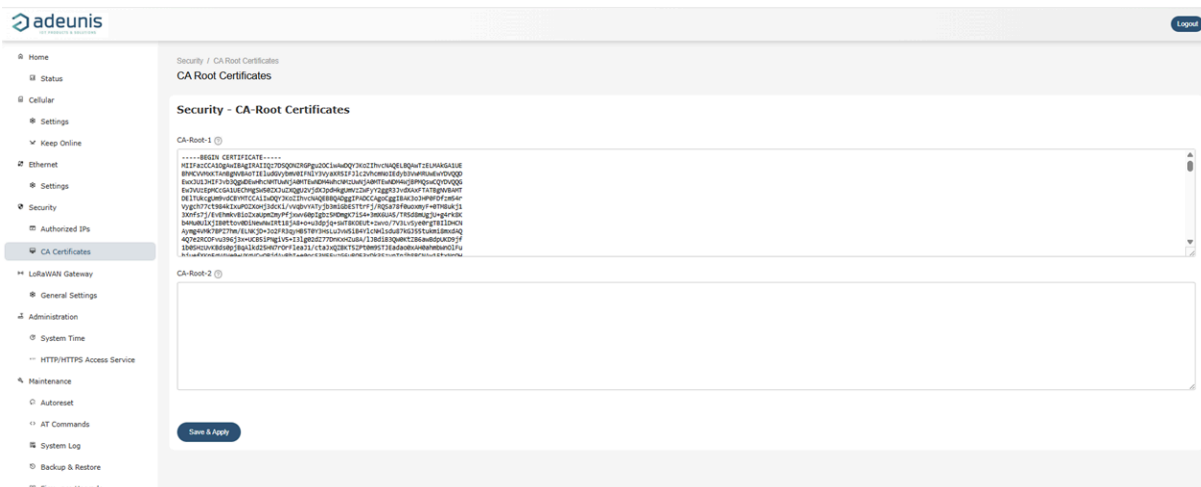
Une fois ces éléments en place, la passerelle est prête à être configurée en packet forwarder LoRa.

3. Importer les certificats racine dans IRIS

La passerelle doit faire confiance au certificat TLS présenté par le serveur CUPS.

Un fichier `.pem` contenant les certificats racine courants est disponible sur la page [Root Certificates Reference](#) de The Things Industries.

- Téléchargez le certificat **Root CA** depuis la documentation TTI ;
- Ouvrez l'interface web IRIS ;
- Allez dans **Security** → **CA Certificates** ;
- Importez le [certificat serveur CUPS](#) dans le champ **CA Root 1** ;
- Cliquez ensuite sur **Save & Apply** pour enregistrer la configuration.



4. Configurer IRIS en mode Basics™ Station (CUPS)

- Allez dans **LoRaWAN Gateway** → **General Settings** ;
- Cochez **Enable the LoRaWAN stack** ;
- Sélectionnez **LoRa Gateway – Semtech Basics™ Station (CUPS)** ;
- Dans le champ **Server URL** de [CUPS](#), saisissez :

`https://<server-address>:443`

Par exemple :

<https://eu1.cloud.thethings.network:443>

- Importez le fichier de clé CUPS dans le champ **Basics™ Station KEY** ;
- Cliquez ensuite sur **Save & Apply** pour enregistrer la configuration.

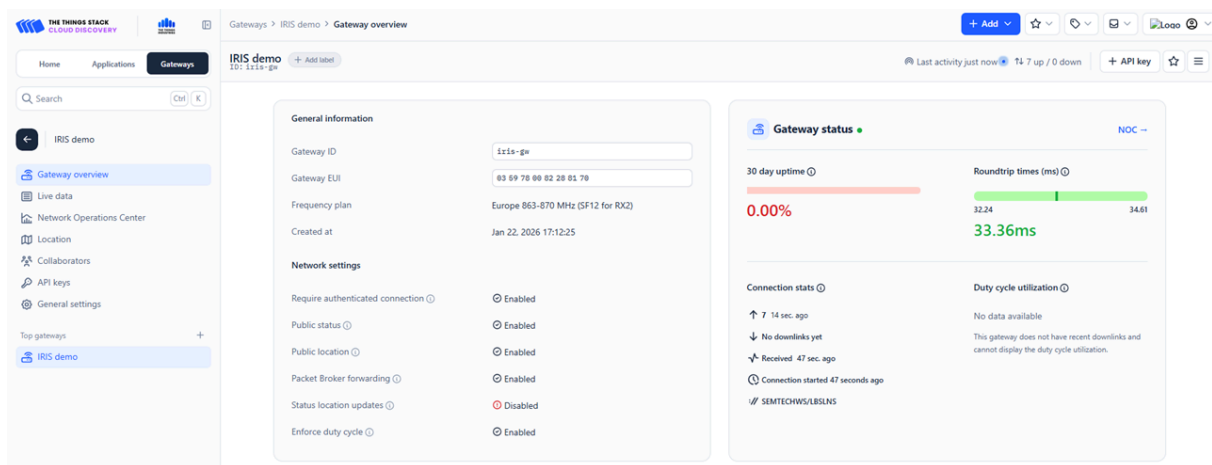
The screenshot shows the 'General Settings' page for a LoRaWAN Gateway in the Adeunis interface. The left sidebar contains a navigation menu with options like Home, Status, Cellular, Settings, Keep Online, Ethernet, Security, Authorized IPs, CA Certificates, LoRaWAN Gateway, General Settings (selected), Administration, System Time, HTTP/HTTPS Access Service, Maintenance, Autorest, AT Commands, System Log, Backup & Restore, Firmware Upgrade, Reboot, and Logout. The main content area is titled 'LoRaWAN Gateway / General Settings' and 'General Settings'. It includes a toggle for 'Enable the LoRaWAN stack', a 'Band' dropdown set to 'eu868', an 'ID' field with '03587000', a 'Mode' dropdown set to 'LoRa Gateway - Basics Station (CUPS)', a 'CUPS URI' field with 'adeunis.eu1.cloud.thethings.industries:443', and a 'CUPS KEY' field with a long alphanumeric string. There is also a 'CUPS Certificate' field. At the bottom, there are two buttons: 'Save & Apply' and 'Basics Station Log'.

Si la connexion CUPS aboutit correctement, la passerelle reçoit alors l'adresse du serveur LNS, les éléments de confiance nécessaires pour ce LNS ainsi que la clé LNS, puis se connecte automatiquement au serveur LNS.

Validation

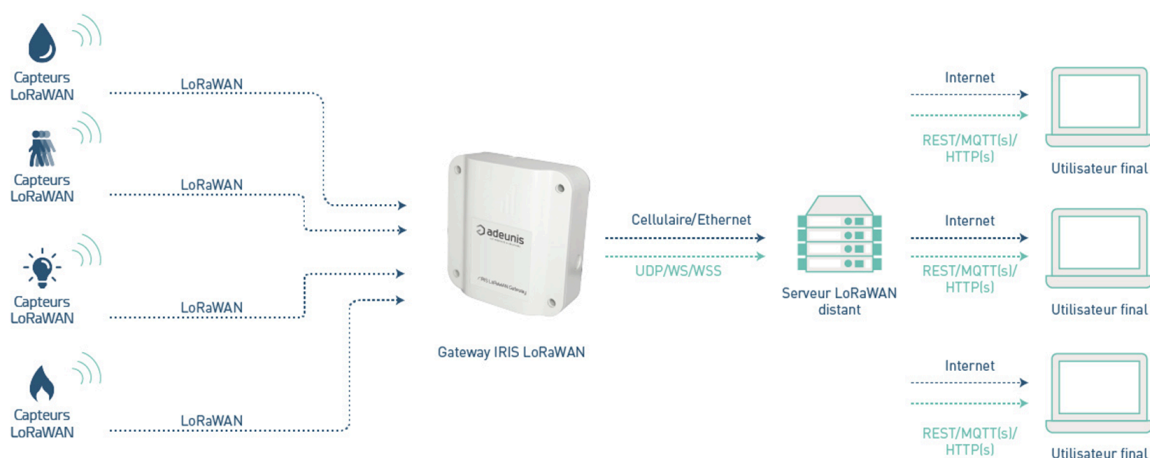
L'intégration est considérée comme valide lorsque :

1. IRIS se connecte correctement au point d'accès **CUPS** ;
2. The Things Stack transmet la configuration **LNS** à la passerelle ;
3. la passerelle se connecte ensuite au point d'accès **LNS** ;
4. l'état de la passerelle devient **connected** dans The Things Stack ;
5. l'horodatage **Last seen** se met à jour régulièrement ;
6. la page **Live data** affiche les événements liés à CUPS et au LNS ;
7. un uplink de test provenant d'un équipement remonte bien via la passerelle IRIS ;
8. un downlink peut être programmé depuis The Things Stack.



ANNEXE 9 CONNEXION D'IRIS À LORIENT AVEC LE PACKET FORWARDER LoRa Basics™ Station

Cette annexe décrit la procédure permettant de connecter la passerelle LoRaWAN **IRIS** au serveur de réseau **LORIENT** en utilisant le **packet forwarder LoRa Basics™ Station**.



Dans cette configuration, IRIS fonctionne comme un **packet forwarder LoRaWAN sécurisé**. La passerelle reçoit les trames radio LoRa émises par les équipements de terrain, puis les transmet via IP au serveur de réseau LoRaWAN de LORIENT. La gestion des équipements, l'exploitation du réseau, les downlinks et les intégrations applicatives sont ensuite pris en charge dans LORIENT.

IRIS prend en charge le mode **Packet Forwarder** en **UDP** ainsi qu'en **Basics Station**. Dans le cas de LORIoT, **LoRa Basics™ Station constitue la méthode d'intégration recommandée**, car elle permet d'établir une connexion LNS sécurisée via **TLS**.

Prérequis

Prérequis	Description
Passerelle IRIS prête à être configurée	La passerelle est alimentée, accessible via son interface web, et déjà configurée avec une connectivité IP, une heure système correcte et un accès sécurisé.
Ordinateur connecté au réseau de la passerelle	Un ordinateur connecté au même réseau que la passerelle IRIS est disponible pour accéder à l'interface web.
Compte LORIoT	Un compte LORIoT disposant des droits nécessaires pour créer ou configurer un réseau et ajouter des passerelles est disponible.
Réseau LORIoT	Un réseau LORIoT cible existe déjà, ou peut être créé avant l'enregistrement de la passerelle.
Adresse MAC Ethernet d'IRIS	L'adresse MAC Ethernet est disponible sur l'étiquette produit ou dans les informations d'état de la passerelle. Elle est demandée par LORIoT lors de l'enregistrement.
Gateway EUI d'IRIS	Le Gateway EUI peut être trouvé : • sur l'étiquette d'identification située à l'arrière du boîtier ; • dans l'interface web IRIS, sur la page Home → Status ; • ou dans LoRaWAN Gateway → General Settings → ID .
Plan de fréquences	La passerelle sera enregistrée avec le plan de fréquences EU863-870 / EU868 .
Accès réseau	La passerelle doit pouvoir joindre le point d'accès LNS de LORIoT en WSS/TLS , à l'aide de l'adresse serveur et du port fournis par la console LORIoT.



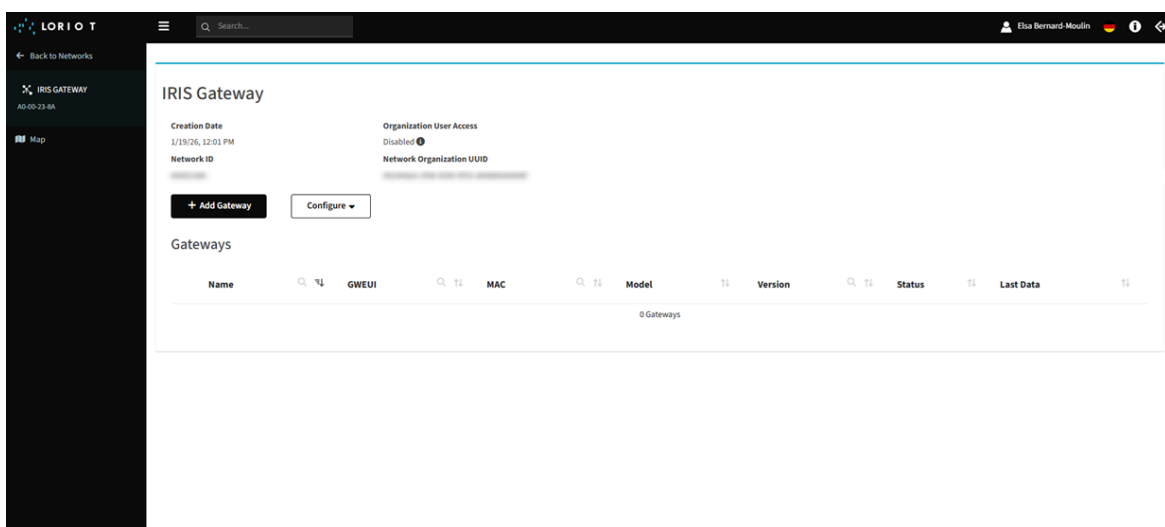
Le **Gateway EUI** est disponible dans l'interface web IRIS sous **LoRaWAN Gateway** → **General Settings** → **ID**. LORIoT utilise cet identifiant lors de l'enregistrement de la passerelle.

Procédure

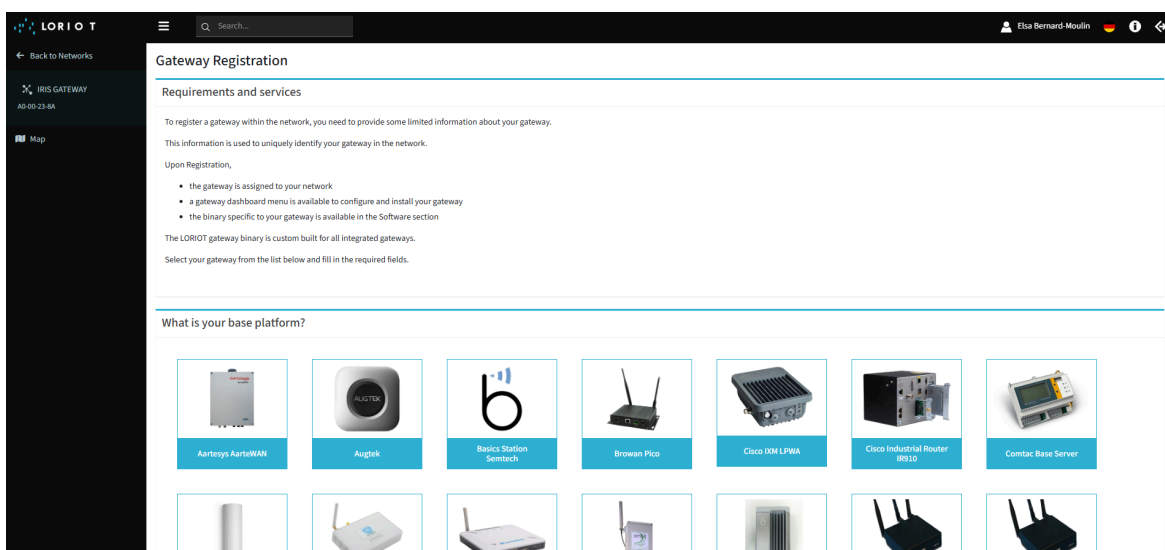
1. Ajouter la passerelle dans LORIoT

Pour connecter une passerelle IRIS au LNS, il faut d'abord l'ajouter dans LORIoT.

- Connectez-vous à la console **LORIoT** ;
- Créez un réseau cible ou ouvrez un réseau existant ;
- Cliquez sur **Add gateway**.



- Sur la page de sélection de la plateforme passerelle, choisissez **Basics Station Semtech**.



Poursuivez vers le formulaire d'enregistrement de la passerelle.

2. Renseigner les identifiants de la passerelle

Dans le formulaire d'enregistrement LORIoT :

- Saisissez l'**adresse MAC Ethernet** d'IRIS dans le champ `eth0 MAC address`.

L'adresse MAC Ethernet peut être trouvée :

- sur l'étiquette d'identification située à l'arrière du boîtier IRIS ;
- ou dans l'interface web IRIS, sur la page **Home** → **Status**.
- Saisissez ensuite le **Gateway EUI** d'IRIS.

Le Gateway EUI peut être trouvé :

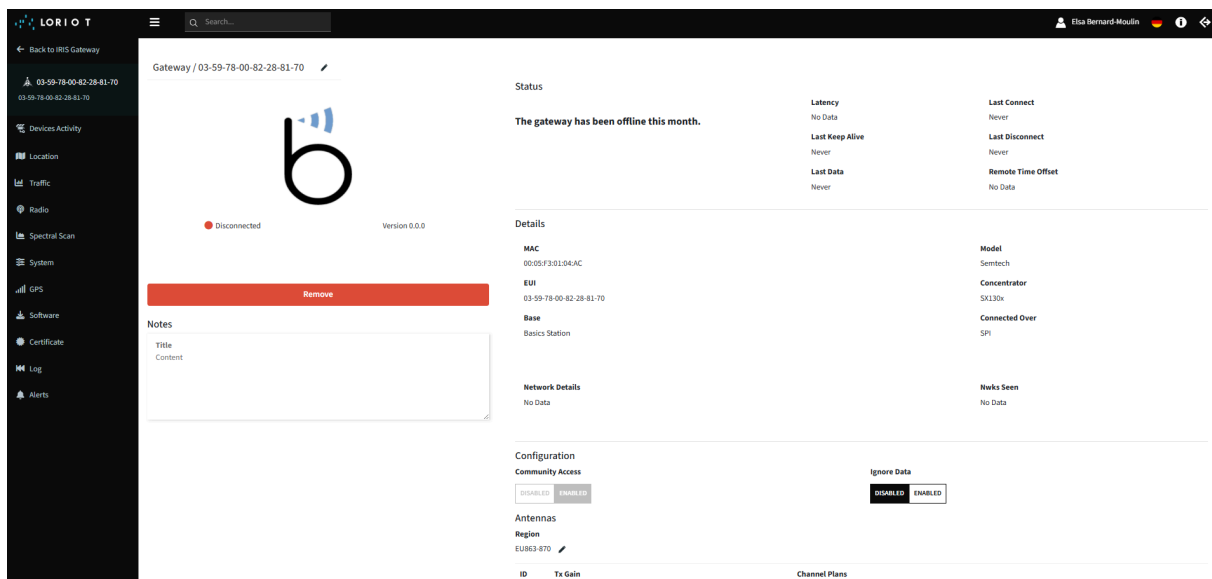
- dans l'interface web IRIS, sur la page **Home** → **Status** ;
- ou dans **LoRaWAN Gateway** → **General Settings** → **ID**.
- Finalisez l'enregistrement de la passerelle.

The screenshot shows the 'Gateway Registration' page in the LORIoT interface. The page has a dark sidebar on the left with navigation links like 'Back to Networks', 'MIS Gateway', and 'Help'. The main content area is titled 'Gateway Registration' and includes sections for 'Requirements and services', 'What is your base platform?' (with a 'Basics Station Semtech' option), 'MAC address of eth0 interface' (with a text input field and a 'Custom EUI (Optional)' button), and 'Gateway Location'.



Le Gateway EUI configuré dans LORIoT doit impérativement correspondre au Gateway EUI réellement utilisé par IRIS. En cas de non-correspondance, la passerelle peut sembler correctement enregistrée, mais le LNS ne pourra pas associer la connexion Basics Station entrante à la bonne passerelle.

Vous serez ensuite redirigé vers la page de synthèse de la passerelle nouvellement créée.



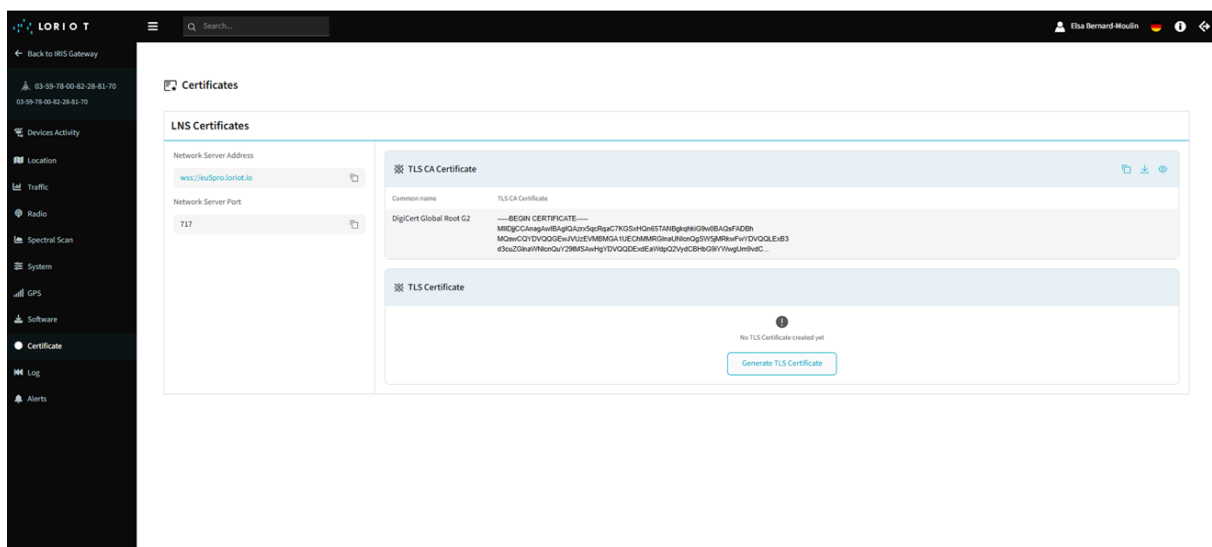
3. Récupérer les informations de connexion LNS dans LORIoT

Une fois la passerelle créée dans LORIoT :

- Ouvrez la page de la passerelle dans LORIoT ;
- Allez dans le menu **Certificate**.

Dans la section **LNS Certificates**, récupérez les informations suivantes :

- **Network Server Address ;**
- **Network Server Port ;**
- **TLS Certificate et TLS Private Key.**





Dans la page **Certificate** de LORIoT, l'**adresse du serveur réseau** et le **port du serveur réseau** sont affichés séparément. L'URL finale à saisir dans IRIS doit être construite à partir de ces deux informations.

Exemple :

Network Server Address: `wss://eu5pro.loriot.io`

Network Server Port: `717`

Server URL à saisir dans IRIS : `wss://eu5pro.loriot.io:717`

4. Générer le certificat TLS et la clé privée TLS

Toujours dans le menu **Certificate** de LORIoT :

- Cliquez sur **Generate TLS Certificate**.

LORIoT génère alors :

- un **TLS Certificate** ;
- une **TLS Private Key**.
- Copiez ou téléchargez immédiatement ces deux éléments ;
- Enregistrez-les dans un emplacement sûr avant de fermer la fenêtre.

Une fois la configuration de base réalisée dans LORIoT, vous pouvez poursuivre avec la configuration du transfert LoRa dans l'interface web de la passerelle.



Pour un premier accès à l'interface web IRIS, vous pouvez vous reporter au [guide utilisateur](#).

Avant de configurer le transfert LoRa, veillez à paramétrer la [connectivité IP](#), l'[heure système](#) et la [sécurité](#).

Une fois ces éléments en place, la passerelle est prête à être configurée en packet forwarder LoRa.

5. Configurer IRIS en mode Basics Station LNS

- Ouvrez l'interface web IRIS ;
- Allez dans **LoRaWAN Gateway** → **General Settings** ;
- Cochez **Enable the LoRaWAN stack** ;
- Sélectionnez la bande **eu868** ;

- Choisissez le mode **LoRa Gateway – Basics Station (LNS)** ;
- Dans le champ **Server URL**, saisissez l'URL LNS de LORIENT construite à partir de **Network Server Address** et **Network Server Port** récupérés dans LORIENT :

`wss://<loriot-network-server-address>:<port>`

Exemple: `wss://eu5pro.loriot.io:717`

The screenshot shows the 'General Settings' page for a LoRaWAN Gateway. The 'Enable the LoRaWAN stack' checkbox is checked. The 'Band' is set to 'eu868' and the 'ID' is empty. The 'Mode' is set to 'LoRa Gateway - Basics Station (LNS)'. The 'Server URL' is set to 'wss://eu5pro.loriot.io:717'. The 'Basics Station KEY' and 'Basics Station Certificate' fields are empty.

- Collez la **TLS Private Key** générée par LORIENT dans le champ **Basics Station KEY** ;
- Collez le **TLS Certificate** généré par LORIENT dans le champ **Basics Station Certificate** ;
- Cliquez ensuite sur **Save & Apply**.

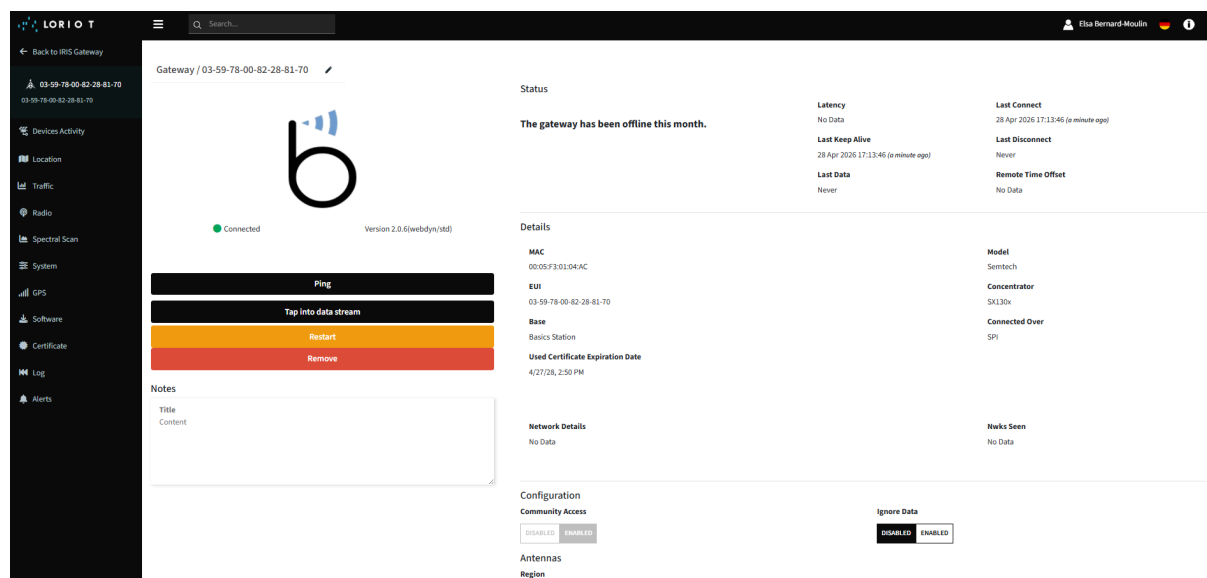
The screenshot shows the 'General Settings' page for a LoRaWAN Gateway. The 'Enable the LoRaWAN stack' checkbox is checked. The 'Band' is set to 'eu868' and the 'ID' is empty. The 'Mode' is set to 'LoRa Gateway - Basics Station (LNS)'. The 'Server URL' is set to 'wss://eu5pro.loriot.io:717'. The 'Basics Station KEY' and 'Basics Station Certificate' fields are filled with redacted text.

La configuration est désormais terminée : la passerelle devrait se connecter à LORIIOT en quelques secondes.

Validation

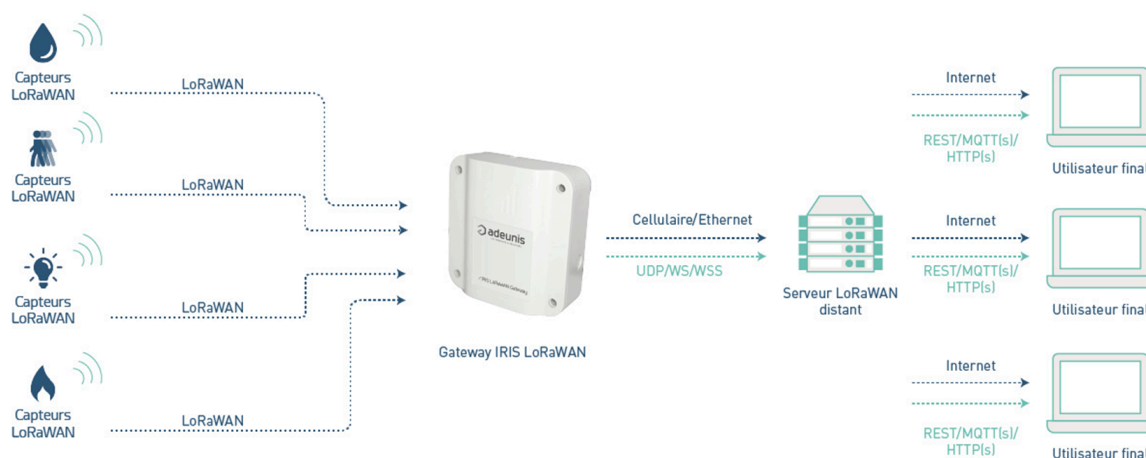
L'intégration est considérée comme valide lorsque :

1. la page **Home** → **Status** d'IRIS indique que la pile LoRaWAN est active ;
2. la passerelle IRIS se connecte bien au LNS LORIIOT ;
3. la page passerelle dans LORIIOT affiche l'état **Connected** ;
4. la page passerelle affiche des informations de connexion récentes telles que **Last Keep Alive** ou **Last Connect** ;
5. un uplink de test provenant d'un équipement LoRaWAN connu apparaît dans la console LORIIOT ;
6. un downlink peut être planifié depuis LORIIOT et transmis à travers la passerelle IRIS.



ANNEXE 10 CONNEXION D'IRIS À ACTIVITY THINGPARK AVEC LoRa Basics™ Station ET PROVISIONING CUPS

Cette annexe décrit la procédure permettant de connecter la passerelle LoRaWAN **IRIS** à **Actility ThingPark** en utilisant le **packet forwarder LoRa Basics™ Station avec provisioning CUPS**.



CUPS signifie **Configuration and Update Server**. Ce mécanisme sert à provisionner automatiquement la configuration Basics Station de la passerelle. Dans ce mode, IRIS se connecte d'abord au point d'accès CUPS, récupère la configuration LNS nécessaire, puis établit ensuite la connexion LoRa Basics™ Station vers Actility ThingPark.

Dans cette architecture, IRIS joue le rôle de **packet forwarder LoRaWAN sécurisé** : la passerelle reçoit les trames radio LoRa émises par les équipements de terrain, puis les transmet via IP au serveur Actility ThingPark. La gestion des équipements, le décodage des données, les intégrations et le routage applicatif sont ensuite pris en charge par ThingPark.

L'utilisation de **CUPS** est particulièrement recommandée lorsque le provisionnement des passerelles doit être géré de manière centralisée, notamment dans le cadre de déploiements de flotte ou lorsque la configuration LNS et les identifiants d'accès peuvent évoluer dans le temps.

Prérequis

Prérequis	Description
Passerelle IRIS prête à être configurée	La passerelle est alimentée, accessible via son interface web, et déjà configurée avec une

Prérequis	Description
	connectivité IP, une heure système correcte et un accès sécurisé.
Compte ThingPark	Un compte utilisateur disposant des droits nécessaires pour enregistrer des passerelles et générer les clés API CUPS/LNS est disponible.
Gateway EUI	Le Gateway EUI d'IRIS est disponible sur l'étiquette produit ou dans LoRaWAN Gateway → General Settings → ID .
Plan de fréquences	La passerelle devra être enregistrée avec le plan de fréquences Europe 863-870 MHz / EU868 .
Source du certificat Root CA	Le certificat Root CA nécessaire à la validation TLS peut être téléchargé depuis la documentation ThingPark ou fourni par l'administrateur d'une instance privée.
Accès réseau	La passerelle doit pouvoir joindre le point d'accès CUPS, généralement via <code>https://<server-address>:443</code> , puis le point d'accès LNS après provisioning.



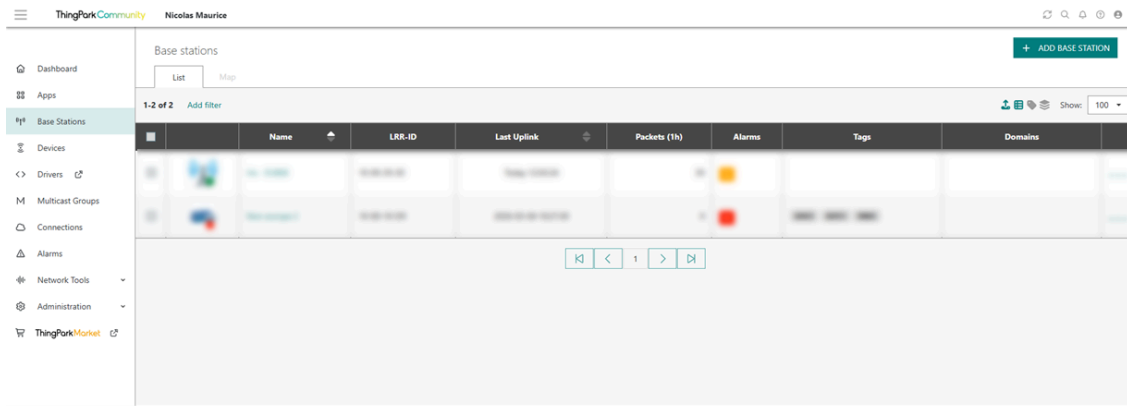
Le **Gateway EUI** est disponible dans l'interface web IRIS sous **LoRaWAN Gateway** → **General Settings** → **ID**. Actility ThingPark utilise cet identifiant lors de l'enregistrement de la passerelle.

Procédure

1. Enregistrer la passerelle dans ThingPark

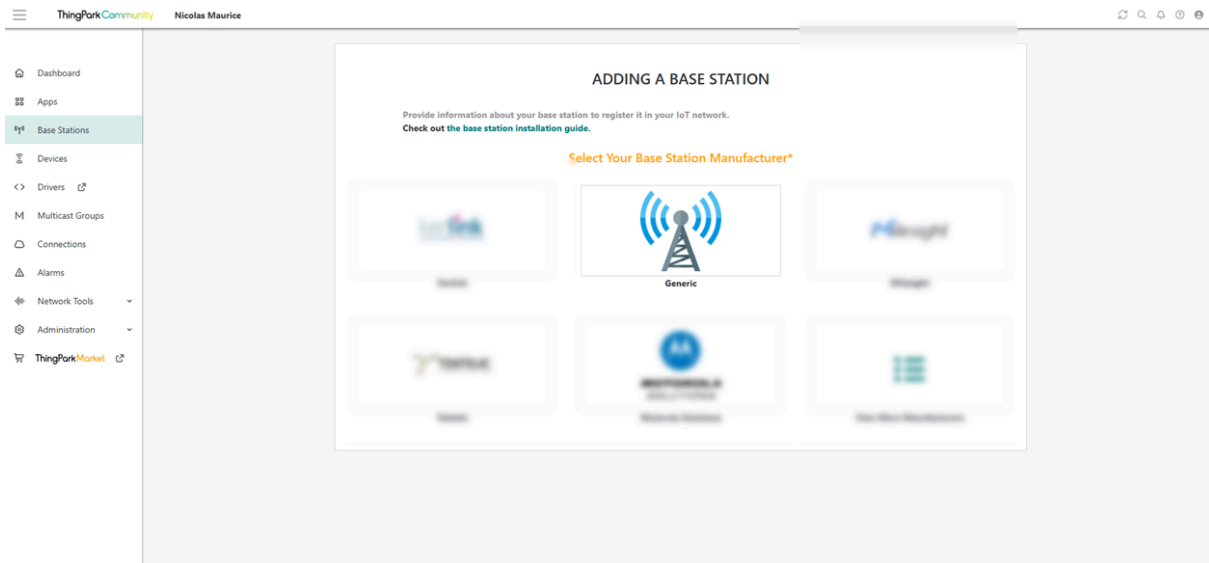
Pour connecter une passerelle IRIS au LNS, il faut d'abord l'ajouter dans ThingPark.

- Connectez-vous à **ThingPark** ;
- Dans le menu de gauche, ouvrez "**Passerelles**" ;
- Cliquez sur "**+ Ajouter une passerelle**" pour accéder à la page d'enregistrement.



Voir également les instructions générales : [Ajouter une passerelle.](#)

- Sélectionnez "**Generic**", car la passerelle IRIS n'apparaît pas encore dans la liste des fabricants.



- Dans le formulaire d'enregistrement :
 - sélectionnez **Basics Station packet forwarder** dans la liste des modèles ;
 - renseignez un **Nom** pour la passerelle ;
 - si nécessaire, sélectionnez le ou les **Domaine(s)** appropriés ;
 - renseignez ensuite le champ **LRR-UUID**.



Pour les passerelles utilisant **Basics Station packet forwarder**, ThingPark demande que le **LRR-UUID** soit construit selon le format suivant : **0016C0-
<GatewayID>**

Exemple :

Gateway EUI : **0359780082790571**

LRR-UUID : **0016C0-0359780082790571**

Le Gateway EUI peut être trouvé :

- sur l'étiquette d'identification située à l'arrière du boîtier ;
- dans l'interface web IRIS, sur la page **Home** → **Status** ;
- ou dans **LoRaWAN Gateway** → **General Settings** → **ID**.



Le Gateway EUI utilisé pour construire le **LRR-UUID** dans ThingPark doit correspondre exactement au Gateway EUI réellement utilisé par IRIS. Si cet identifiant est erroné, la passerelle pourra être provisionnée dans ThingPark, mais ne sera pas correctement associée lors de son démarrage via CUPS.

- Sélectionnez ensuite la **RF Region** appropriée :
 - pour une IRIS en EU868, utilisez **EU 863-870 MHz (8 channels)** ;
- Dans la section **Sécurité**, activez **Générer le certificat de la passerelle** ;
- Complétez, si besoin, les paramètres de **localisation** et les **alarmes** ;
- Validez enfin la création de la passerelle.

ThingPark Community Nicolas Maurice

Dashboard Apps Base Stations Devices Drivers Multicast Groups Connections Alarms Network Tools Administration ThingParkMarket

Enter Your Base Station Information*

Model* Basics Station packet forwarder eu868_a923_kr920_u915_a915_in865_ru864

This model uses the Basics Station packet forwarder. See the [user guide](#) for configuration details.

Name* IRIS ✓

Domains

LRR-UUID* 0016C0-359780082288170 ✓

RF Region* EU 863-870MHz (8 channels)

This 8-channels RF Region applies to any region where the use of the 863-870 MHz ISM radio spectrum is compliant with the ETSI EN300.220 standard.

Additional Information

Write here...

Security

☒ Generate base station certificate

2. Identifier l'URL CUPS correcte

Le guide officiel de configuration Basics Station de ThingPark définit le point d'accès **CUPS** selon la plateforme utilisée :

- **ThingPark Community:** <https://community.thingpark.io:443>
- **ThingPark Enterprise EU SaaS:** <https://thingparkenterprise.eu.actility.com:443>
- **ThingPark Enterprise AU SaaS:** <https://thingparkenterprise.au.actility.com:443>
- **ThingPark Enterprise US SaaS:** <https://thingparkenterprise.us.actility.com:443>
- **ThingPark self-hosted:** https://<HTTP_hostname>:443 en utilisant le nom d'hôte HTTP configuré sur la plateforme.

Une fois cette première configuration réalisée dans ThingPark, vous pouvez poursuivre avec la configuration du transfert LoRa dans l'interface web de la passerelle.



Pour un premier accès à l'interface web IRIS, vous pouvez vous reporter au guide utilisateur.

Avant de configurer le transfert LoRa, veuillez à paramétrer la connectivité IP, l'heure système et la sécurité.

Une fois ces éléments en place, la passerelle est prête à être configurée en packet forwarder LoRa.

3. Configurer IRIS en mode Basics Station (CUPS)

- Allez dans **LoRaWAN Gateway** → **General Settings** ;
- Cochez **Enable the LoRaWAN stack** ;
- Réglez la bande sur **eu868** ;
- Sélectionnez le mode **LoRa Gateway – Basics Station (CUPS)** ;
- Dans le champ **CUPS URL**, saisissez l'URL CUPS ThingPark identifiée à l'étape précédente.

The screenshot shows the 'General Settings' page for a LoRaWAN Gateway. The left sidebar contains a navigation menu with options like Home, Status, Cellular, Settings, Keep Online, Ethernet, Security, Authorized IPs, CA Certificates, LoRaWAN Gateway, Administration, System Time, HTTP/HTTPS Access Service, Maintenance, Autoreset, AT Commands, System Log, Backup & Restore, and Firmware Upgrade. The main content area is titled 'LoRaWAN Gateway / General Settings' and 'General Settings'. It includes a checkbox to 'Enable the LoRaWAN stack', a 'Band' dropdown set to 'eu868', an 'ID' field, a 'Mode' dropdown set to 'LoRa Gateway - Basics Station (CUPS)', a 'CUPS URI' field with the value 'https://community.thingspark.io:443', a 'CUPS KEY' field, and a 'CUPS Certificate' field. The 'CUPS KEY' and 'CUPS Certificate' fields are currently empty.

- Laissez le champ **CUPS KEY** vide pour le bootstrap initial, sauf si Actility vous fournit des identifiants spécifiques à votre tenant ;
- Laissez également le champ **CUPS Certificate** vide pour le bootstrap initial, sauf indication contraire explicite d'Actility ;
- Cliquez ensuite sur **Save & Apply**.

4. Importer l'ancre de confiance CUPS dans IRIS

- Ouvrez l'interface web ;
- Allez dans **Security** → **CA Certificates** ;
- Importez ou collez le certificat racine CUPS dans le champ **CA Root 1** ;
- Cliquez ensuite sur **Save & Apply**.

The screenshot shows the 'Security - CA Root Certificates' page. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Security / CA Root Certificates' and 'CA Root Certificates'. It shows two text areas for CA Root Certificates. The first area, labeled 'CA-Root-1', contains a large block of base64-encoded text. The second area, labeled 'CA-Root-2', is empty. A 'Save & Apply' button is visible at the bottom.

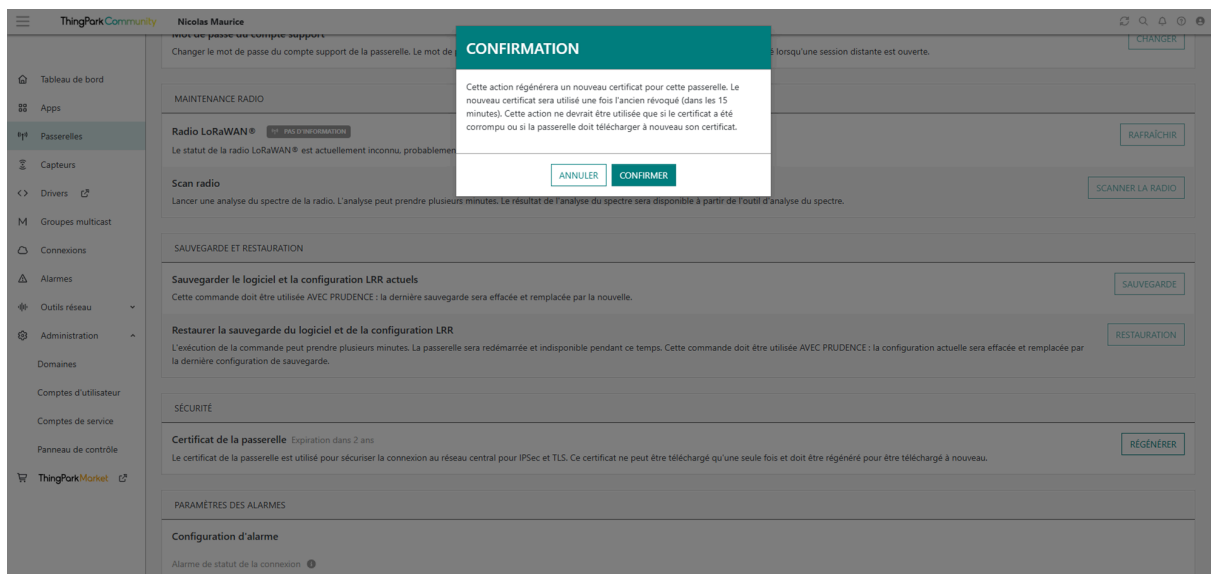
Pour **ThingPark Community** et les plateformes **SaaS régionales**, utilisez **Amazon Root CA 1** comme ancre de confiance.

Link direct: <https://www.amazontrust.com/repository/AmazonRootCA1.pem>

5. Générer le certificat X.509 de la passerelle

Une fois la passerelle IRIS configurée en mode **LoRa Gateway – Basics Station (CUPS)** et le certificat racine CUPS importé dans IRIS, revenez sur la fiche détaillée de la passerelle dans ThingPark.

- Connectez-vous à **ThingPark** ;
- Dans le menu de gauche, ouvrez **“Passerelles”** ;
- Cliquez sur la passerelle
- Dans le menu secondaire en haut de page cliquez sur **“Avancé”**
- Dans la section **“Sécurité”** cliquez sur **“Régénérer”** afin d'autoriser ThingPark à générer le certificat X.509 de la passerelle.



Si la connexion CUPS est établie avec succès, la passerelle reçoit alors l'adresse du serveur LNS, les éléments de confiance nécessaires pour ce LNS ainsi que la clé LNS, puis se connecte automatiquement au serveur LNS.

Validation

L'intégration est considérée comme valide lorsque :

1. la passerelle a bien été créée dans ThingPark ;

2. son état initial devient **Initialisation** ;
3. le certificat X.509 de la passerelle est généré depuis l'interface ThingPark ;
4. une fois la passerelle en ligne, ThingPark provisionne le certificat et l'état évolue vers **Connected**;
5. un uplink de test provenant d'un équipement LoRaWAN connu apparaît dans ThingPark ;
6. après redémarrage, la passerelle reste stable et se reconnecte automatiquement.

The screenshot displays the 'Basic View' configuration page for an 'IRIS' gateway in the ThingPark Community interface. The left sidebar shows navigation options like Dashboard, Apps, Base Stations, Devices, Drivers, Multicast Groups, Connections, Alarms, Network Tools, and Administration. The main content area is split into two columns. The left column, titled 'INFORMATION', contains various configuration fields: Name (set to 'IRIS'), Domains, Tags, Manufacturer (set to 'Generic'), Model (set to 'Basics Station packet forwarder'), LRR-ID (set to '10-00-38-4E'), LRR-UUID (set to '0016C0-359780082288170'), Packet Forwarder (set to 'Basics Station'), and RF Region (set to 'EU 863-870MHz (8 channels)'). A note indicates 'A new version is available'. The right column, titled 'STATUS', shows the current state of the gateway: Network Connection, LoRaWAN Radio Status, Clock Synchronization, Active alarms, Base Station Restart Time, Last Uplink, Last Downlink, Uplink Packets for the last hour, and Downlink Packets for the last hour. A map in the 'LOCATION' section shows the gateway's position.

Retour au sommaire

[Guide Utilisateur](#) | [IRIS WG0610-A01-ADE](#) | [LoRaWAN EU863-870](#)