ALD-17552/1124

INTERNET

Guide d'installation - Aufbau-Anleitung - Start Guide

Routeur I-NET 512

Router I-NET 512

ALDEN

CE

Sommaire

Sommaire

Avertissements

La reproduction de tout ou partie de ce guide est interdite sans un accord écrit de la part d'ALDEN.

ALDEN attire une attention particulière sur les risques encourus en cas de montage non conforme.

La responsabilité d'ALDEN ne pourra être engagée en cas de montage non conforme aux règles de l'art et en particulier si l'installation est effectuée par un non-professionnel.

Le revendeur est réputé connaître les règles de l'art et s'y conformer. Il respectera tout particulièrement les règles en matière de choix d'emplacement, de branchement électrique, de collage, de vissage. Il s'engage, en vendant et en installant un produit ALDEN, à informer son client du mode d'emploi et éventuellement du mode d'installation et lui remettra les documents nécessaires. Il attirera l'attention du client sur tous les aspects concernant la sécurité. Il informera le client que le produit vendu ne devra pas être détourné de l'utilisation prévue. En outre, il attirera l'attention du client, s'il y a lieu, sur l'obligation de respecter les lois en vigueur dans le ou les pays d'utilisation.

Toute intervention effectuée sur le produit sans accord préalable de la part d'ALDEN entraîne la nullité de la garantie.

Le vendeur ainsi que le constructeur ne peuvent en aucun cas être tenus pour responsables en cas de modifications des modes d'émission ou des puissances d'émission. Les événements inconnus du vendeur et du constructeur ne peuvent pas donner lieu à une demande d'échange, de remboursement ou d'indemnité de quelque nature qu'elle soit. Les zones de réception sont données à titre indicatif.

ALDEN décline toute responsabilité de quelque nature qu'elle soit, en particulier pour tout accident ou incident en cas de non-observation des instructions données, tant au niveau de l'installation que de l'utilisation.

L'ouverture des différents éléments est strictement interdite. Aucun recours en garantie ne sera possible dans ce cas.

Pour toute intervention sur le circuit électrique, remplacement ou branchement de la batterie, il conviendra de retirer les fusibles des câbles d'alimentation des équipements satellites. Si le véhicule est équipé d'un panneau solaire, retirer également le fusible du régulateur de charge.

Il est impératif de tirer une alimentation séparée et équipée d'un fusible 3 Ampères directement depuis la batterie cellule pour alimenter le routeur.

Il est impératif de protéger les embouts des câbles avec du scotch papier durant l'installation.

Utilisez uniquement les pièces de rechange et les accessoires originaux ou des pièces recommandées par un revendeur spécialisé, faute de quoi la garantie sera annulée. Toute intervention sur l'appareil doit être effectuée par des techniciens qualifiés.

Ne pas ouvrir le couvercle de l'appareil sous peine de s'exposer à des chocs électriques et d'annuler la garantie. Ne confier l'entretien et la maintenance de l'appareil qu'à du personnel qualifié.

Lors du branchement des câbles, veiller à ce que l'appareil soit débranché. Attendre quelques secondes après l'arrêt de l'appareil avant de le déplacer ou de débrancher les câbles connectés.

Si l'appareil ne fonctionne pas correctement lorsque vous avez respecté strictement toutes les instructions de la présente notice, contactez votre revendeur.

Cet appareil répond aux exigences gouvernementales en matière d'exposition aux ondes radio. Cet appareil est conçu et fabriqué pour ne pas dépasser les limites d'émission pour l'exposition à l'énergie des radiofréquences (RF) fixées par les agences autorisées. Pour assurer la conformité avec les directives d'exposition RF, l'appareil doit être utilisé avec une distance minimale de 20 cm du corps d'une personne. Le non-respect de ces instructions peut entraîner une exposition aux RF dépassant les limites des directives pertinentes.
Les antennes externes utilisées avec le I-NET 512 doivent être installées pour fournir une distance de séparation d'au moins 20 cm de toutes les personnes et ne doivent pas être co-localisées ou utilisées en conjonction avec une autre antenne ou émetteur.

Avertissements

Tout gain d'antenne externe doit respecter les limites d'exposition RF et de puissance de sortie rayonnée maximale de la section de règle applicable.

● Le fait de procéder à l'installation implique l'acceptation des règles énoncées. ●

Sécuriser l'accès de votre appareil :

Conservez autant que l'usage le permet l'appareil près de vous. Changez régulièrement les codes d'accès (code PIN, mots de passes, etc..) de votre appareil.
Eteignez votre appareil lorsqu'il n'est pas utilisé ou pour éviter de capter des données sensibles.
Installer les mises à jour du logiciel.

Etre attentif à la gestion des données : soyez attentif aux données relatives à votre vie privée, notamment en désactivant le partage automatique des données, si vous associez l'appareil à des réseaux sociaux.
Effacer les données sur l'appareil avant de la mettre au rebut, de le vendre ou le remettre au service après-vente.
Dans le cas de la connexion à point d'accès (AP) WiFi, s'assurer que ce dernier soit sûr.

Dans le cadre de l'utilisation du produit, ALDEN ne peut être tenue responsable :
- Du contenu auquel l'utilisateur peut accéder dans le cadre de l'utilisation du produit.
- Des échanges de données réalisés entre l'utilisateur et quelconque plateforme que ce soit.
- Des actions de tiers pour collecter, utiliser, transmettre et divulguer vos informations ou données.
- De la consommation sur la quantité des données mobiles liées à la carte SIM donnant accès à un opérateur de réseau mobile.

ALDEN se réserve le droit de mettre à jour automatiquement le logiciel y compris les corrections de bogues et les mises à jour, l'interface utilisateur ou de la manière dont vous accédez au contenu, et d'autres modifications susceptibles d'ajouter, de modifier ou de supprimer des fonctionnalités et des caractéristiques. Vous reconnaissez que ces mises à jour peuvent se produire automatiquement à tout moment. Vous comprenez que ces mises à jour sont nécessaires pour maintenir la compatibilité avec d'autres mises à jour de nos produits et peuvent être nécessaires pour des raisons de sécurité. En utilisant notre service, vous acceptez par la présente de recevoir ces mises à jour.

MARQUAGE POUR L'EUROPE
Le marquage CE qui est attaché à ce produit signifie sa conformité aux directives Radio Equipment Directive 2014/53/CE, Low Voltage Directive 2014/35/EU et RoHS 2011/65/CE.

Directive DEEE (Union européenne et EEE uniquement).
Ce symbole indique que, conformément à la directive DEEE (2002/96/CE) et à la réglementation de votre pays, ce produit ne doit pas être jeté avec les ordures ménagères. Vous devez le déposer dans un lieu de ramassage prévu à cet effet, par exemple, un site de collecte officiel des équipements électriques et électroniques (EEE) en vue de leur recyclage ou un point d'échange de produits autorisé qui est accessible lorsque vous faites l'acquisition d'un nouveau produit du même type que l'ancien. Toute déviation par rapport à ces recommandations d'élimination de ce type de déchet peut avoir des effets négatifs sur l'environnement et la santé publique car ces produits EEE contiennent généralement des substances qui peuvent être dangereuses. Parallèlement, votre entière coopération à la bonne mise au rebut de ce produit favorisera une meilleure utilisation des ressources naturelles. Pour obtenir plus d'informations sur les points de collecte des équipements à recycler, contactez votre mairie, le service de collecte des déchets, le plan DEEE approuvé ou le service d'enlèvement des ordures ménagères. (EEE : Norvège, Islande et Liechtenstein)

Avertissements

Manipulation du produit

- Vous êtes seul responsable de l'utilisation que vous faites de votre appareil et des conséquences de son utilisation.
- L'utilisation de votre appareil est soumise à des mesures de sécurité destinées à protéger les utilisateurs et leur environnement.
- Traitez toujours votre appareil et ses accessoires avec soin et conservez-les dans un endroit propre et sans poussière.
- N'exposez pas votre appareil ou ses accessoires à des flammes.
- N'exposez pas votre appareil ou ses accessoires à des liquides, à l'humidité ou à une forte humidité.
- Ne laissez pas tomber, ne jetez pas ou n'essayez pas de plier votre appareil ou ses accessoires.
- N'utilisez pas de produits chimiques agressifs, de solvants de nettoyage ou d'aérosols pour nettoyer l'appareil ou ses accessoires.
- Ne peignez pas votre appareil ou ses accessoires.
- N'essayez pas de démonter votre appareil ou ses accessoires, seul le personnel est autorisé à le faire.
- N'utilisez pas votre appareil dans un environnement clos ou dans un endroit où la dissipation de la chaleur est mauvaise.
- Une utilisation prolongée dans un tel espace peut provoquer une chaleur excessive et augmenter la température ambiante, ce qui entraînera l'arrêt automatique de votre appareil ou la déconnexion de la connexion au réseau mobile pour votre sécurité. Pour utiliser à nouveau votre appareil normalement après un tel arrêt, refroidissez-le dans un endroit bien aéré avant de le rallumer.
- Veuillez vérifier les réglementations locales pour l'élimination des produits électroniques.
- N'utilisez pas l'appareil dans un endroit où la ventilation est restreinte.
- N'utilisez pas ou n'installez pas ce produit près de l'eau pour éviter tout risque d'incendie ou d'électrocution.
- Ne pas exposer l'équipement à la pluie ou à des zones humides.
- Disposez les câbles d'alimentation et Ethernet de manière à ce qu'ils ne soient pas susceptibles d'être piétinés ou d'être recouverts d'objets.
- Assurez-vous que la tension et le courant nominal de la source d'alimentation correspondent aux exigences de l'appareil. Ne connectez pas l'appareil à une source d'alimentation inappropriée.
- Ne laissez pas votre appareil et ses accessoires à la portée des jeunes enfants et ne les laissez pas jouer avec. Ils pourraient se blesser ou blesser d'autres personnes, ou endommager accidentellement l'appareil. Votre appareil contient de petites pièces avec des bords tranchants qui peuvent causer des blessures ou qui pourraient se détacher et créer un risque d'étouffement.
- Cet appareil, comme tout appareil sans fil, fonctionne à l'aide de signaux radio, qui ne peuvent garantir une connexion dans toutes les conditions. Par conséquent, vous ne devez jamais compter uniquement sur un appareil sans fil pour les communications d'urgence ou utiliser l'appareil dans des situations où l'interruption de la connectivité des données pourrait entraîner la mort, des blessures, des dommages matériels, la perte de données ou toute autre perte.
- L'appareil peut devenir chaud lors d'une utilisation normale.

Mise à jour du I-NET 512

Le routeur I-NET 512 dispose d'un système de mise à jour automatique et manuelle du logiciel.

Des mises à jour du logiciel peuvent être effectuées automatiquement. Avant toute action sur l'appareil (coupure d'alimentation, redémarrage..), il convient de contrôler l'état des voyants et de s'assurer que le routeur ne soit pas dans une phase de mise à jour.

Pour mettre à jour le logiciel manuellement, se référer au chapitre "4.3.1 Menu Système > Logiciel > Mise à jour du logiciel", page 104.

L'installation d'une mise à jour se traduit visuellement par 3 étapes comme décrit ci-dessous :

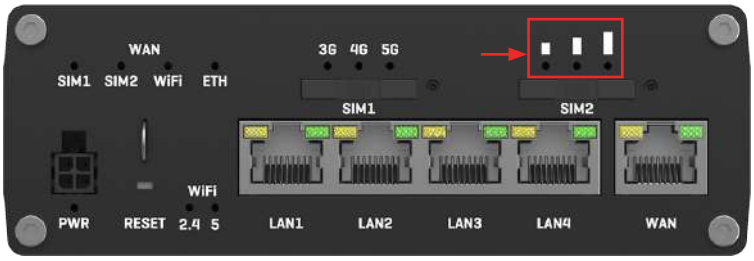
- Toutes les LED éteintes : Téléchargement du nouveau logiciel (durée : jusqu'à 30secondes)
- Clignotement des 3 LED l'une après l'autre : Installation du nouveau logiciel (durée : jusqu'à 90 secondes).

IMPORTANT : ne pas mettre l'appareil hors tension durant cette étape.

- Tout s'allume
- Clignotement simultané des LED : Redémarrage du routeur (durée : jusqu'à 2 minutes)

NOTE : Pendant la phase d'installation de la mise à jour, la connexion WiFi sera interrompue.

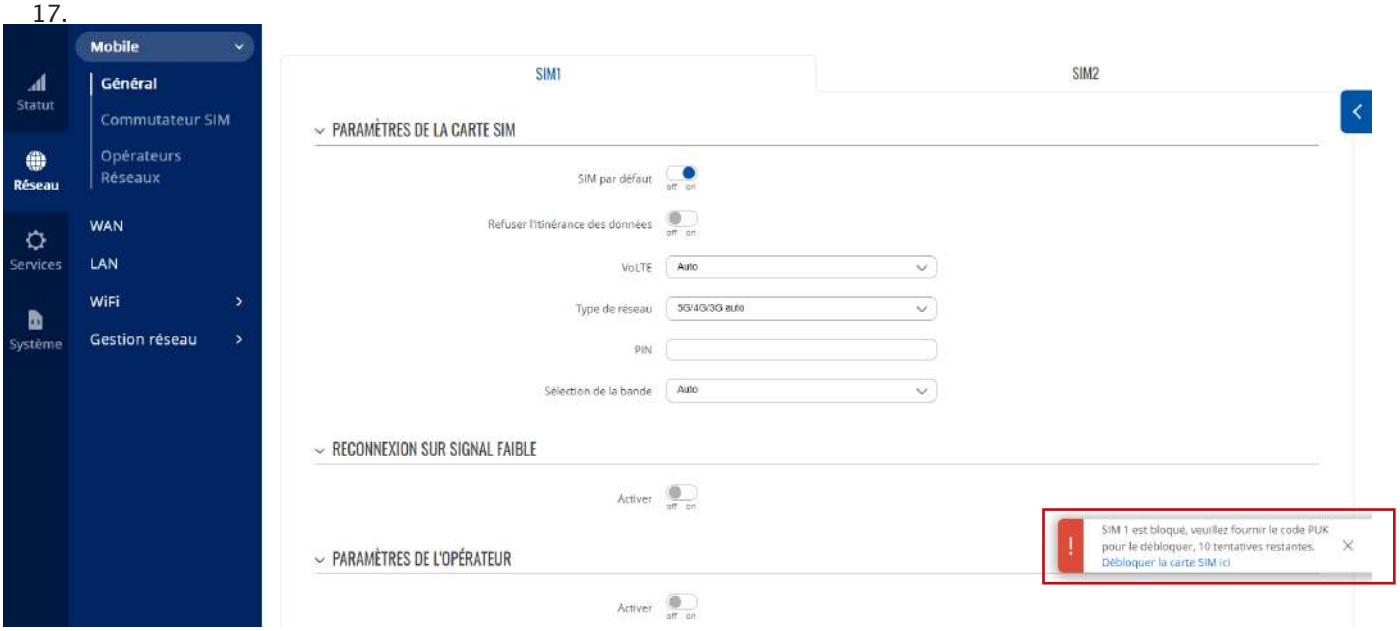
ATTENTION : NE PAS METTRE LE ROUTEUR I-NET 512 HORS TENSION DURANT LA PHASE DE MISE A JOUR AU RISQUE DE RENDRE CELUI-CI DEFINITIVEMENT INUTILISABLE



Code PUK

Le code PUK (Personal Unblocking Key) est un code de secours composé de 8 chiffres qui permet de débloquer votre SIM lorsque vous avez indiqué trois fois de suite un code PIN erroné.
Vous le trouverez sur le document accompagnement de votre carte SIM. Il peut également être communiqué par le service client de votre opérateur. Vous disposez de 10 essais pour entrer ce code PUK.

La saisie de ce code s'effectue en cliquant sur le message "Débloquer la carte SIM ici" dans la fenêtre pop-up qui s'affiche après la saisie de 3 codes PIN erronés dans le menu RESEAU - Mobile - Général. (se référer au chapitre "2.1.1 Menu Réseau > Mobile > Général", page 26).
Le code PUK peut aussi être saisi sur la ligne informations carte SIM sur la page "Déblocage carte SIM - code PUK", page 17.



Informations de sécurité I-NET 512

Exposition RF

Cet appareil répond aux exigences gouvernementales en matière d'exposition aux ondes radio. Cet appareil est conçu et fabriqué pour ne pas dépasser les limites d'émission pour l'exposition à l'énergie des radiofréquences (RF) fixées par les agences autorisées. Pour assurer la conformité avec les directives d'exposition RF, l'appareil doit être utilisé avec une distance minimale de 20 cm du corps d'une personne. Le non-respect de ces instructions peut entraîner une exposition aux RF dépassant les limites des directives pertinentes.
Les antennes externes utilisées avec le I-NET 512 doivent être installées pour fournir une distance de séparation d'au moins 20 cm de toutes les personnes et ne doivent pas être co-localisées ou utilisées en conjonction avec une autre antenne ou émetteur.

Tout gain d'antenne externe doit respecter les limites d'exposition RF et de puissance de sortie rayonnée maximale de la section de règle applicable.

Type d'antenne	Gamme de fréquences	Impédance	VSWR	Gain *	Radiation	Connecteur
Mobile	800~960MHz, 1710~2690MHz	50 Ω	≤ 3,0	≤ 4 dBi	omnidirectionnel	SMA mâle
WiFi	2,4 ~ 2,5 GHz, 5,10 ~ 5,95 GHz	50 Ω	2,5 maximum	≤ 3,5 dBi	omnidirectionnel	RP-SMA mâle

* Une antenne à gain plus élevé peut être connectée pour compenser l'atténuation du câble lorsqu'un câble est utilisé. L'utilisateur est responsable du respect des dispositions légales.

Puissance d'émission maximale	
WCDMA	24 dBm
LTE	23 dBm
WiFi	20 dBm

Conditions de fonctionnement

Température de fonctionnement : -40° à +75° C
Le taux d'humidité doit être compris entre 10 % et 90 % (sans condensation). N'utilisez l'appareil que dans des environnements secs.
Abrité de la lumière directe du soleil
A l'écart des sources de chaleur
A l'écart des substances corrosives, des sels et des gaz inflammables

ATTENTION : un fonctionnement en dehors de la plage autorisée peut réduire considérablement la durée de vie de l'appareil.

Produits défectueux et endommagés

- N'essayez pas de démonter l'appareil ou ses accessoires.
- Seul un personnel qualifié doit entretenir ou réparer l'appareil ou ses accessoires.
- Si votre appareil ou ses accessoires ont été immergés dans de l'eau, perforés ou soumis à une chute importante, ne les utilisez pas tant qu'ils n'ont pas été vérifiés dans un centre de service agréé.

Sécurité électrique

- N'utilisez que des accessoires approuvés.
- Ne pas connecter avec des produits ou accessoires incompatibles.

Configuration I-NET 512

I-NET 512 Mesures spatiales et poids

Cette page contient des informations sur les mesures et le poids du routeur I-NET 512. Les schémas fournis ici sont destinés à aider à déterminer la taille approximative de l'appareil avant l'installation.
Les figures présentées ci-dessous présentent les mesures de l'appareil sous plusieurs angles différents et de divers éléments (câbles, connecteurs, etc.) situés sur ou dépassant de l'appareil. Toutes les mesures sont spécifiées en millimètres (mm).

Mesures principales

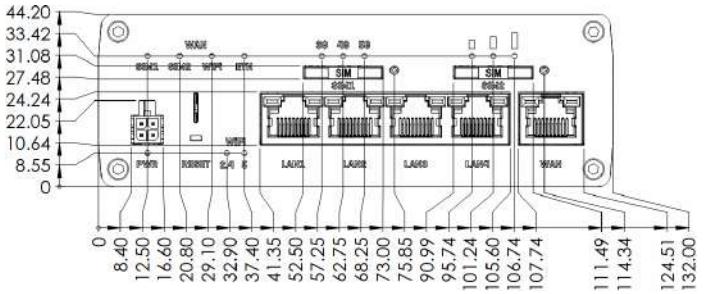
Dimensions L x H x P pour I-NET 512 :

Boîtier de l'appareil * :	132 x 44,2 x 95,1 mm
Boîte:	355 x 60 x 175 mm

* Les mesures du boîtier sont présentées sans connecteurs d'antenne, ni vis ; pour les mesures des autres éléments de l'appareil, consultez les sections ci-dessous.

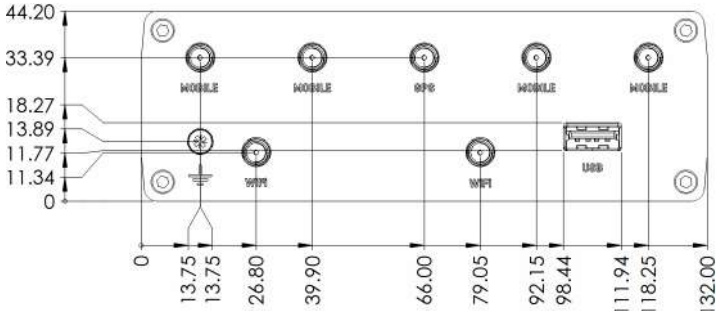
Vue avant

La figure ci-dessous illustre les mesures du I-NET 512 et de ses composants sur la face avant :



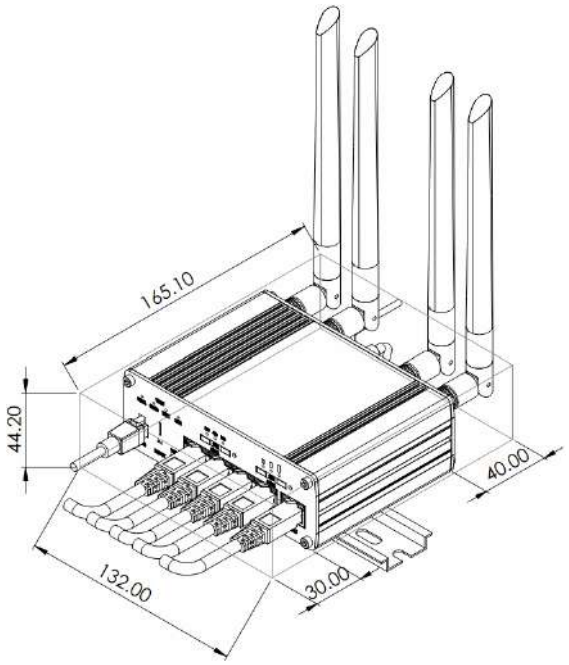
Vue arrière

La figure ci-dessous illustre les mesures du I-NET 512 et de ses composants sur la face arrière :



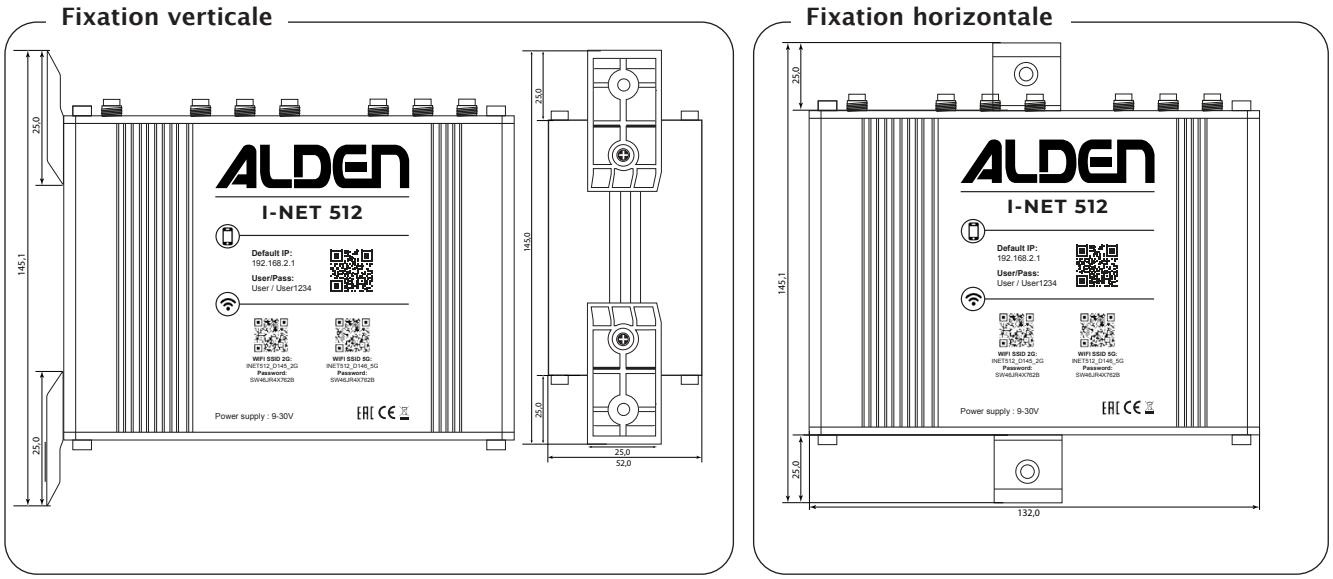
Espace de montage

La figure ci-dessous représente le volume requis de l'appareil lorsque les câbles et les antennes sont connectés :



Fixation

Les figures ci-dessous représente les dimensions de l'appareil avec ses supports de fixation :

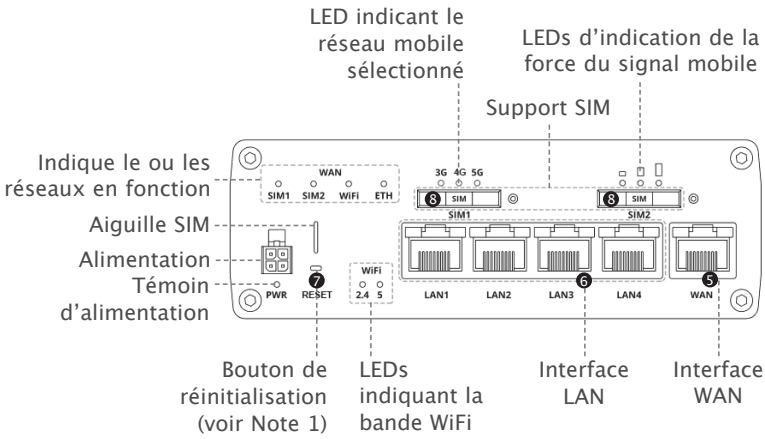


Il est à noter qu'il est possible de fixer le routeur verticalement et horizontalement. Visser les 2 supports à l'aide des 2 vis (fournies) dans le rail du routeur, prévu à cet effet.

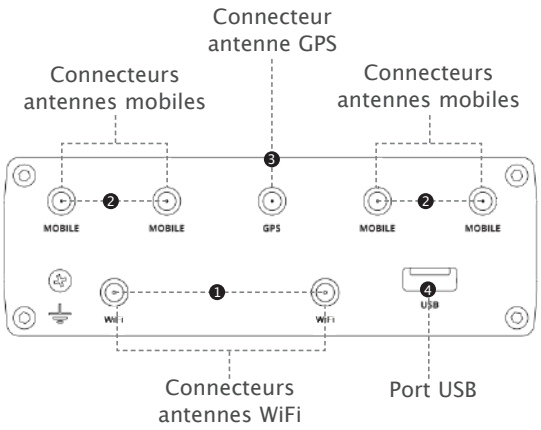
Description des interfaces

Le routeur I-NET 512 est doté de différentes interfaces et ports pour offrir un accès à internet optimal.

1. Interface WiFi via 2 connecteurs à l'arrière pour un accès sans fils à internet entre le routeur et un ordinateur ou une borne WiFi externe. L'interface WiFi permet l'accès à l'interface web utilisateur du routeur et à internet.
2. Interface mobile 5G/4G avec 4 connecteurs pour connecter 4 antennes MIMO.
3. Un connecteur GPS
4. Un port USB
5. Un port WAN à l'avant pour un accès à internet grâce à un réseau filaire externe.
6. 4 ports LAN pour la connexion filaire d'un ordinateur au routeur I-NET 512.
7. Bouton Reset utilisé pour réinitialiser le routeur à ses réglages d'origine. Appuyer et maintenir le bouton 12 à 60 secondes à l'aide de l'aiguille fourni.
8. 2 Lecteurs carte SIM.

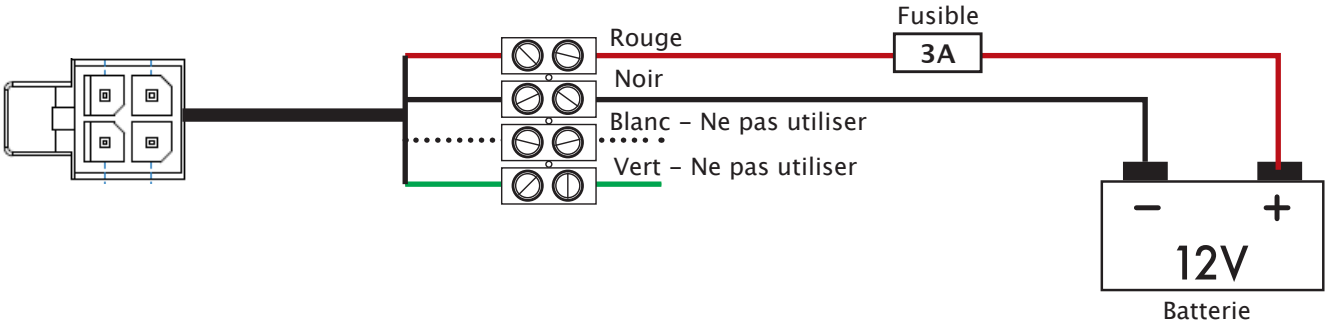


VUE AVANT

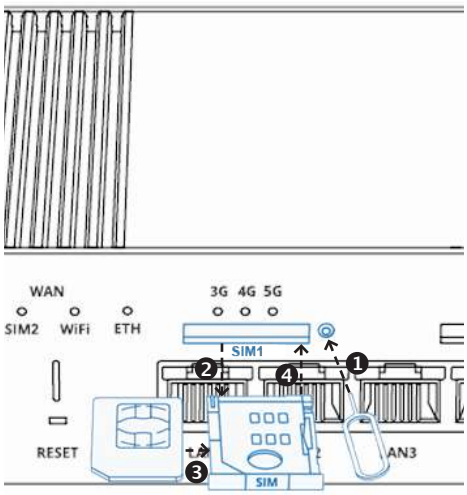


VUE ARRIÈRE

Brochage de la prise d'alimentation



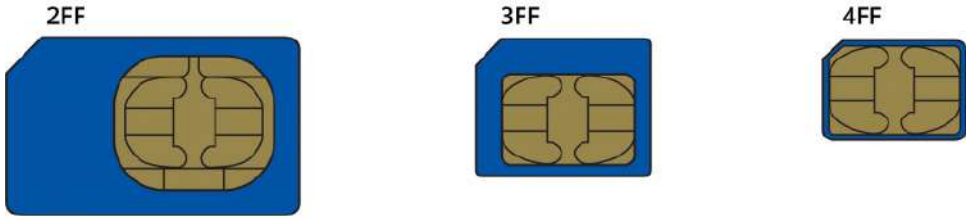
Carte SIM I-NET 512



1. Appuyez sur le bouton de l'un des deux supports SIM avec l'aiguille SIM fournie, SIM 1 de préférence.
2. Retirez le support SIM.
3. Insérez votre carte SIM dans le support SIM 1. Utiliser l'un des adaptateurs (fournis) si-besoin.
4. Insérer le support SIM 1 dans le routeur.
5. Fixez les antennes Mobiles et WiFi. Si fournie, préférez l'antenne extérieur I-NET aux antennes d'intérieur bâtons.
6. Connectez le cordon d'alimentation à la prise située à l'avant du routeur, coté domino :
   - Relier le fil noir (-) à la masse.
   - Relier le fil rouge (+) à la borne plus de la batterie. Le fils + doit être protégé par un fusible de 3A.

   Note : Ne pas connecter les fils vert et blanc.
7. Connectez-vous au SSID du réseau WiFi de l'appareil en scannant l'un des deux QR code avec un smartphone ou en utilisant les infos à l'avant de l'appareil. Pour la configuration avec un PC, préférer l'utilisation du câble Ethernet connecté à l'interface LAN.

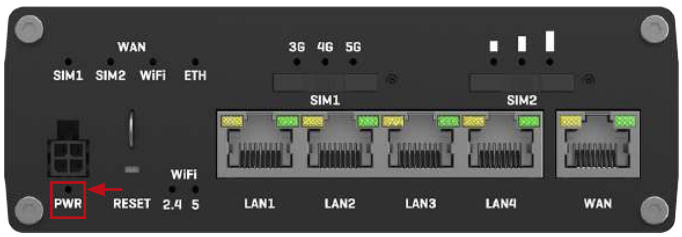
L'appareil est compatible avec les cartes de taille mini-SIM (2FF). Mais comme différents types de cartes SIM ont le même agencement de contacts, des cartes SIM plus petites peuvent également être utilisées avec le routeur, à condition qu'elles soient insérées dans un adaptateur de carte SIM 2FF. Une perspective de taille des types de cartes SIM les plus populaires peut être vue dans la figure ci-dessous :



Description des témoins lumineux

Voyant d'alimentation

Le voyant d'alimentation est situé dans le coin inférieur gauche du panneau avant, juste sous le connecteur d'alimentation.

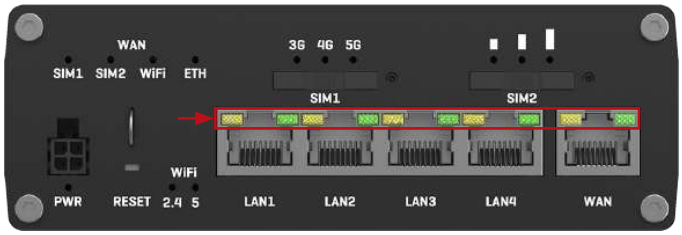


Il indique si l'appareil est sous tension ou non.

État	Description
LED allumée	L'appareil est sous tension.
LED éteinte	L'appareil n'est pas sous tension.

Voyants du port Ethernet

Il y a deux voyants situés en haut de chaque port Ethernet.

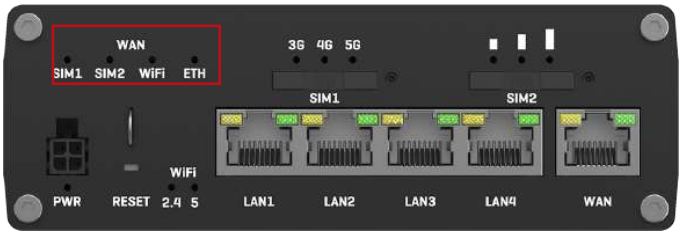


Ils fournissent des informations sur les états actuels des ports Ethernet. Chaque port possède deux voyants :
- Orange - Connexion 10/100 Mbps
- Vert : connexion 1 000 Mbit/s

État	Description
Voyant allumé	Une connexion de données sur le port est opérationnelle (câble branché, terminal visible, aucune donnée n'est transférée).
Voyant OFF	Aucune connexion de données sur le port n'est opérationnelle (pas de câble, mauvais câble ou périphérique final non visible pour une autre raison (telle qu'une carte réseau endommagée).
LED clignotante	Connexion établie et les données sont en cours de transfert via ce port.

Voyants du port WAN

Les voyants de type WAN sont situés en haut à droite du panneau avant.

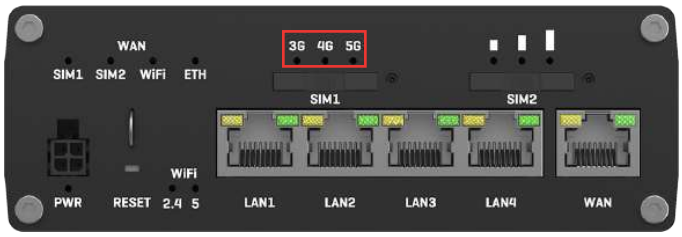


Ils indiquent quel type de connexion Internet est actuellement actif.

État	Description
Voyant SIM1 allumé	Une connexion de données mobiles sur SIM1 est active.
LED SIM1 éteinte	Une connexion de données mobiles sur SIM1 est inactive.
Voyant SIM2 allumé	Une connexion de données mobiles sur SIM2 est active.
LED SIM2 éteinte	Une connexion de données mobiles sur SIM2 est inactive.
LED WiFi allumée	Une connexion de données WiFi (WiFi WAN) est active.
LED WiFi éteinte	Une connexion de données WiFi (WiFi WAN) est inactive.
LED ETH allumée	Une connexion de données Ethernet (WAN filaire) est active.
LED ETH éteinte	Une connexion de données Ethernet (WAN filaire) est inactive.

Voyants du réseau mobile

Les voyants de type de réseau mobile sont situés près de l'emplacement de la carte SIM.

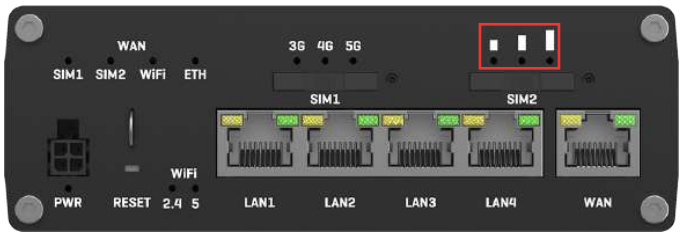


Ils affichent le type de connexion Internet actuellement actif.

Action	Description
Voyant 3G allumé, fixe	L'appareil est connecté à un réseau 3G.
Voyant 4G allumé, fixe	L'appareil est connecté à un réseau 4G.
Voyant 5G allumé, fixe	L'appareil est connecté à un réseau 5G via 5G SA.
LED 4G et 5G allumées	L'appareil est connecté via 5G NSA.
3G clignotant	L'appareil n'est pas connecté au réseau 3G.
4G clignotant	L'appareil n'est pas connecté au réseau 4G.
5G clignotant	L'appareil n'est pas connecté au réseau 5G.
Toutes les LED clignotent en même temps toutes les 500 ms	Pas de carte SIM ou code PIN incorrect.
Toutes les LED s'allument et s'éteignent dans une séquence, l'une après l'autre.	L'appareil tente de se connecter à un opérateur de réseau mobile.

LED d'indication de la force du signal mobile

Les LED d'indication de la force du signal mobile sont situées du dessus de la fente de la carte SIM.

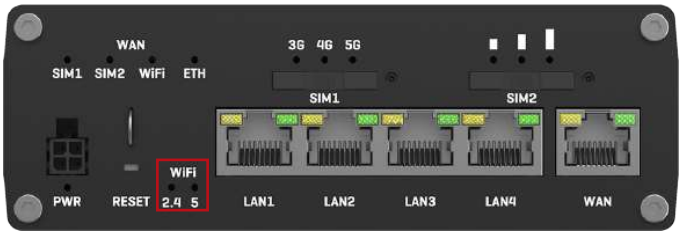


Le nombre de LED allumées représente une valeur de force de signal mobile (RSSI) différente en dBm.

Nombre de LED allumées	Valeur de force du signal
0	≤ -111dBm
1	-110 dBm à -82 dBm
2	-81 dBm à -52 dBm
3	≥ -51dBm

Voyants de la Bande WiFi

Les voyants de la bande WiFi sont situés en bas de la face avant de l'appareil, à gauche des ports Ethernet.

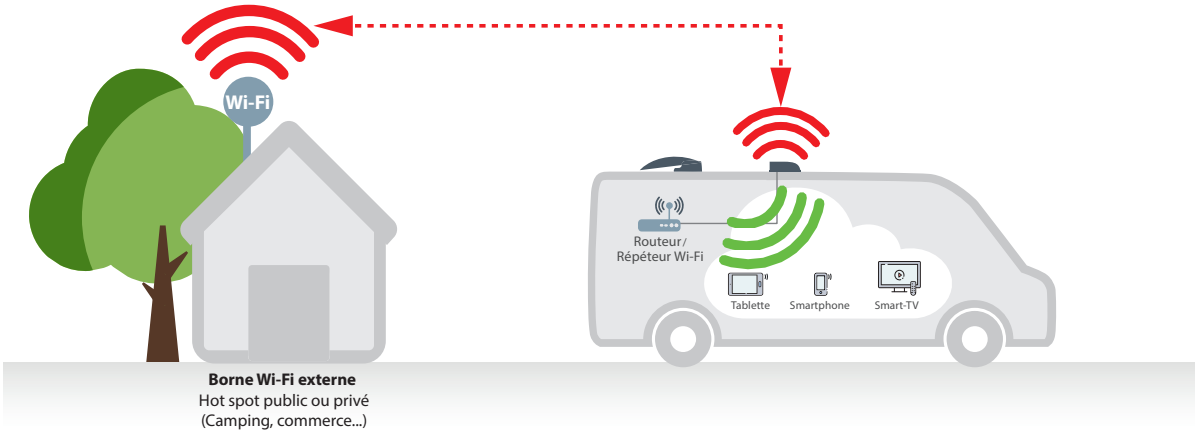


Ils indiquent si un point d'accès WiFi (AP) est actif sur une bande spécifique.

État	Description
2.4 LED allumée.	Au moins un point d'accès 2,4 GHz est en cours d'exécution.
2.4 LED éteinte	Aucun point d'accès 2,4 GHz n'est en cours d'exécution.
5 LED allumées	Au moins un point d'accès 5 GHz est en cours d'exécution.
5 LED éteintes	Aucun point d'accès 5 GHz n'est en cours d'exécution.

Répéteur WiFi.

Le routeur I-NET 512 offre la possibilité de se connecter à un réseau WiFi externe pour le rediffuser localement dans son véhicule, avec ses propres identifiants.



Suivre les instructions "Configuration du mode client", page 63 pour créer sont propre répéteur WiFi est ainsi économiser des données sur sa carte SIM.

NOTE : le réseau WiFi externe peut disposer de droits de connexion. Vérifier au préalable qu'il est possible de s'y connecter librement. A défaut, en demander la permission.

Sélection 5G/4G/3G

En fonction de la qualité du réseau 5G ou 4G, le routeur peut basculer automatiquement sur le réseau 3G. Si l'utilisation du réseau 5G ou 4G est un impératif, il est alors possible de le specifier dans le menu adéquat. Il suffit de basculer le réglage «Préférence réseau» sur «4G (LTE) uniquement» dans le menu Réseau-> Mobile-> Général-> Paramètres de la carte SIM. Ne pas oublier de cliquer sur le bouton «Sauvegarder et appliquer»

Se référer au chapitre "2.1.1 Menu Réseau > Mobile > Général", page 26 pour forcer l'utilisation d'un réseau 3G ou 4G.

Sélection manuelle de l'opérateur

Dans certains cas d'utilisations (Ex. à l'étranger), il peut être nécessaire de sélectionner manuellement l'opérateur mobile pour sa carte SIM.
Se référer au chapitre "2.1.3 Menu Réseau > Mobile > opérateurs réseaux", page 30 pour forcer la connexion sur un opérateur réseau de son choix.

Mode Normal /Avancé

L'interface utilisateur du routeur dispose de 2 modes : Normal et Avancé. Certaines fonctions ne sont accessible que si le mode sélectionné est le mode Avancé. Cliquer sur le bouton en haut à droite du logo ALDEN de la page WEB pour basculer du mode "Normal" au mode "Avancé".

Gestion réseau

L'objectif de ce module est de garantir à l'utilisateur un accès à internet si au moins l'une des interfaces est opérationnelle. Par défaut, le module de Gestion réseau est activé.
Se référer au chapitre "2.5 Menu Réseau > GESTION RÉSEAU", page 68.

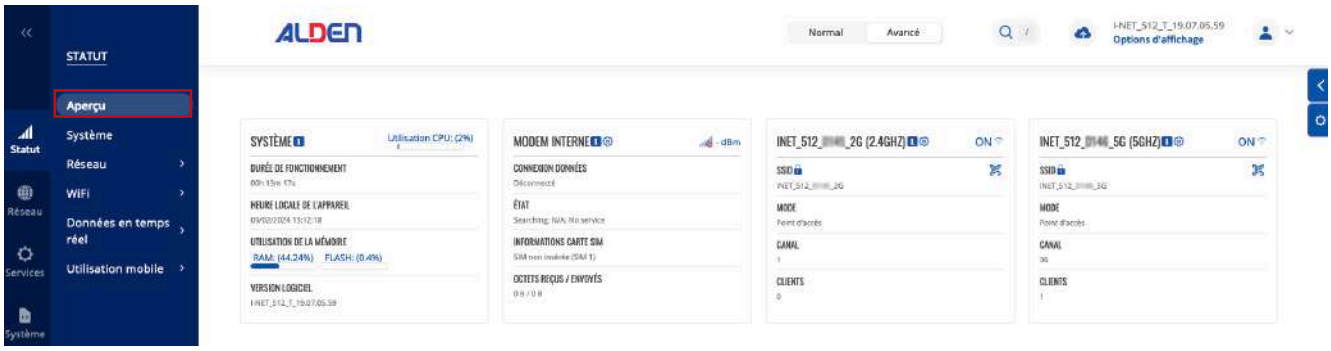
Installation rapide

Lors de la première mise en service, vous êtes invités à saisir les principaux paramètres pour configurer votre routeur. Il est obligatoire de valider toutes les étapes de cette installation. Ne pas oublier de saisir le code PIN de votre carte SIM. En cas de doute sur un paramètre suggéré, valider la suggestion affichée.

1. Menu STATUT

1.1 Menu STATUT > APERÇU

La page Présentation contient des widgets qui affichent l'état de divers systèmes liés à l'appareil :



Modem

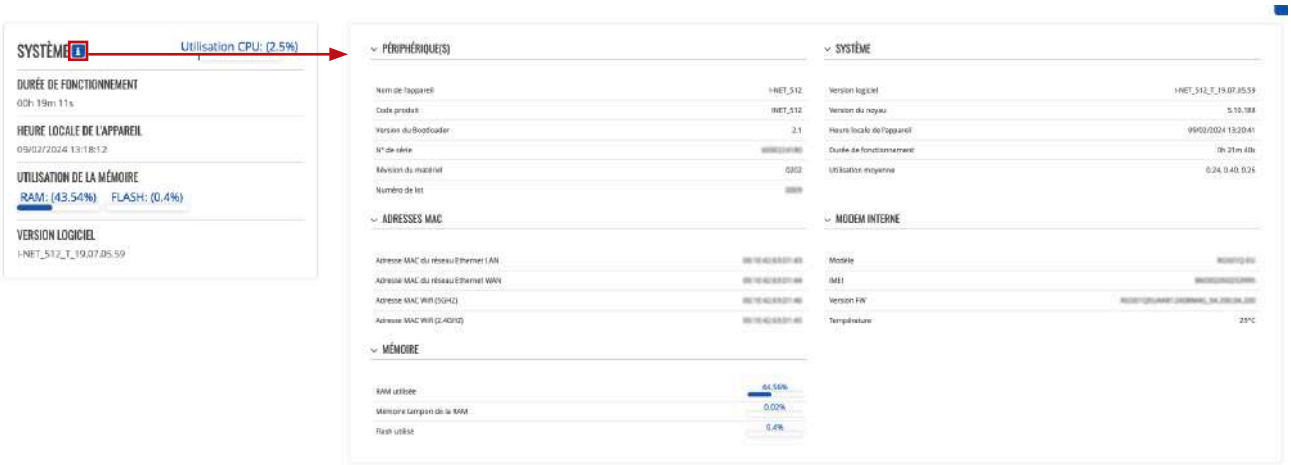
Le widget Modem affiche des informations relatives à la connexion mobile et à la puissance actuelle du signal (). Chaque barre pleine représente une valeur RSSI différente :

Barres	Valeur d'intensité du signal / RSSI (en dBm)
0	≤ -111
1	-110 à -97
2	-96 à -82
3	-81 à -67
4	-66 à -52
5	≥ -51

Le même principe de calcul s'applique aux LED d'intensité du signal situées sur votre appareil. Vous pouvez trouver plus d'informations sur les valeurs d'intensité du signal et les différentes mesures ci-dessous :

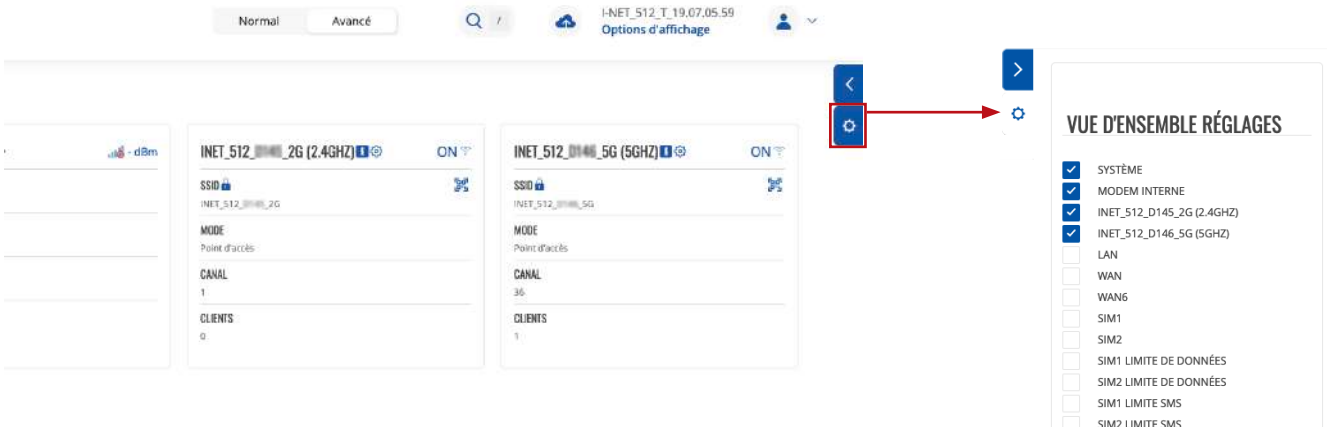
Bouton Widget : Infos

Le bouton Info () est situé à côté du nom de certains widgets. Cliquer sur le bouton Info redirige l'utilisateur vers une page d'état liée aux informations affichées par le widget. Par exemple, cliquer sur le bouton Info du widget Système redirigerait l'utilisateur vers la page Système



Ajout de plus de widgets

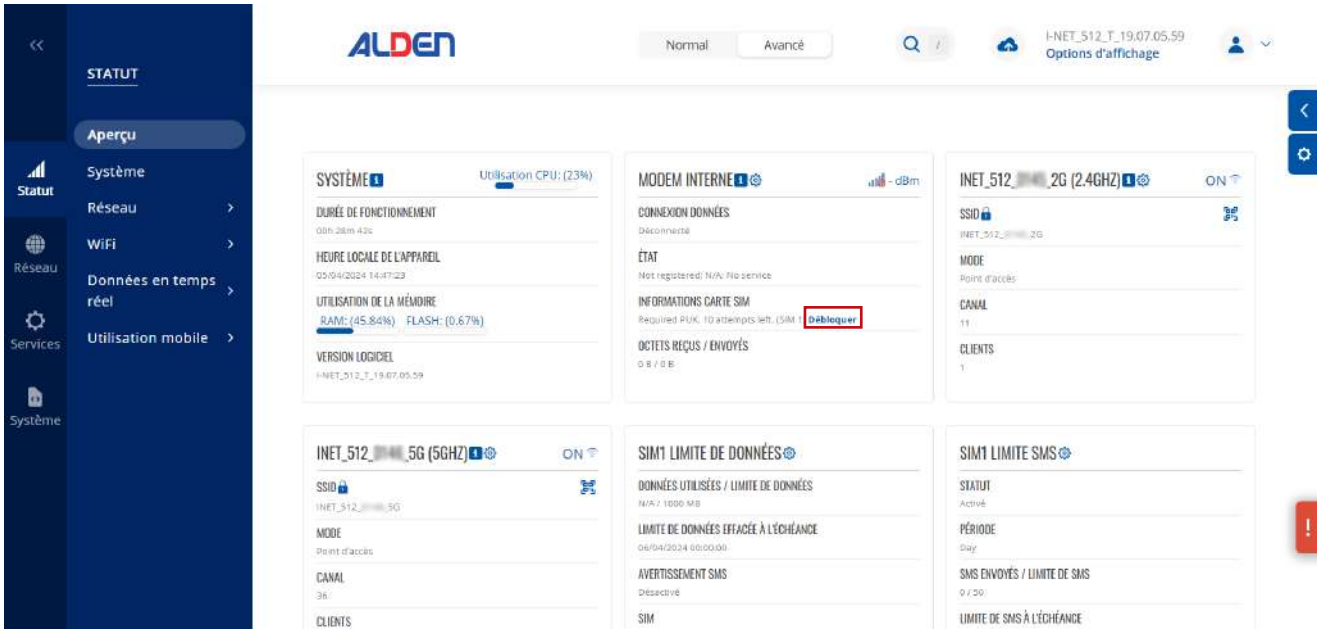
Un ensemble de widgets par défaut est affiché dans la page "Aperçu", mais d'autres peuvent être ajoutés en cliquant sur le bouton "Vue d'ensemble réglages" à droite de la page WEB. À partir de là, vous pouvez ajouter des widgets autres que ceux par défaut.



Déblocage carte SIM - code PUK

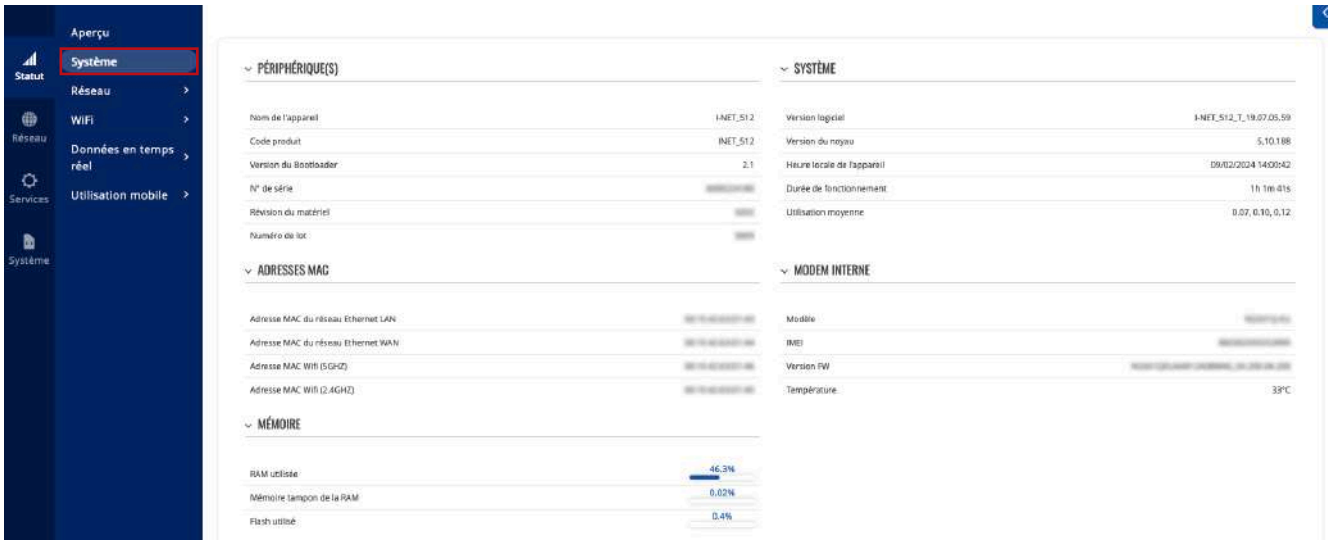
Le code PUK (Personal Unblocking Key) est un code de secours composé de 8 chiffres qui permet de débloquer votre SIM lorsque vous avez indiqué trois fois de suite un code PIN erroné.
Vous le trouverez sur le document accompagnement de votre carte SIM. Il peut également être communiqué par le service client de votre opérateur. Vous disposez de 10 essais pour entrer ce code PUK.

Le code PUK peut être saisi en cliquant sur le lien "Débloquer" afficher en bleu.



1.2 Menu STATUT > SYSTÈME

Le menu Système affiche des informations générales relatives au matériel, aux logiciels et à l'état de la mémoire de l'appareil.
La figure ci-dessous est un exemple de la page Système et le tableau fournit des informations sur les champs affichés dans cette page :



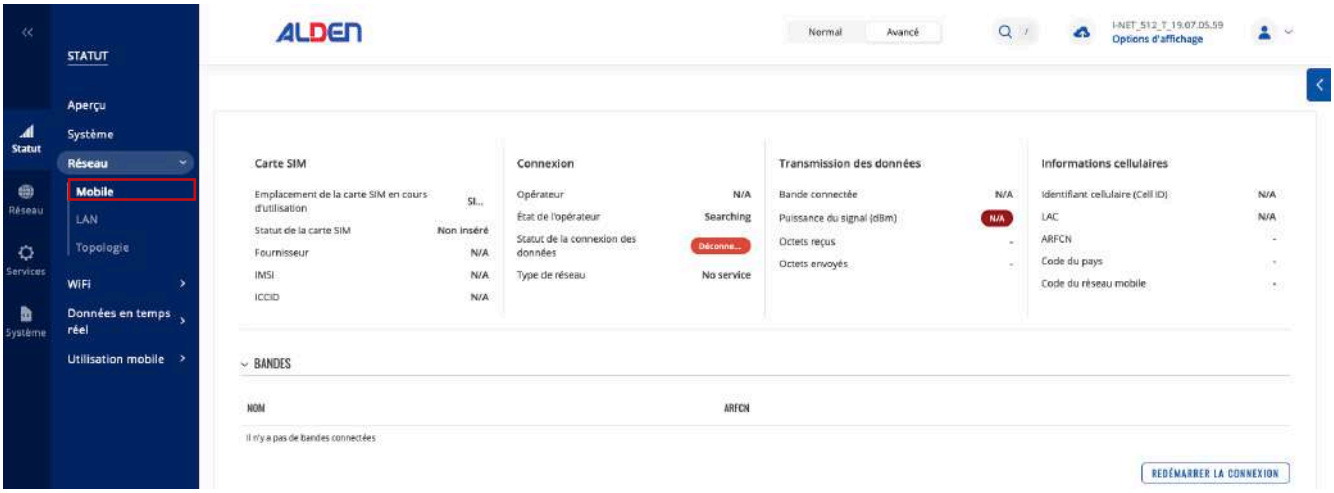
Champ	Description
Nom de l'appareil	Le nom de cet appareil : I-NET_512
Code produit	Alias, code de commande ; affiche sous quel code produit l'appareil a été fabriqué.
Version du Bootloader	Version du chargeur de démarrage actuellement utilisée par l'appareil. Un Bootloader est un programme qui charge le système d'exploitation.
Numéro de série	Identifiant d'appareil unique à 10 chiffres.
Révision du matériel	Nombre à 4 chiffres représentant la version de révision matérielle du routeur.
Numéro de lot	Numéro à 4 chiffres qui indique le lot de produit.
Version du logiciel	Version du logiciel actuellement utilisée par l'appareil. Le logiciel peut être mis à niveau à partir de la page Système → logiciel.
Version du noyau	Version du noyau actuellement utilisée par l'appareil. Un noyau est un programme informatique chargé de connecter le logiciel d'un appareil à son matériel.
Heure locale de l'appareil	Heure actuelle perçue par l'appareil. Les paramètres de temps peuvent être ajustés dans la page Système → Administration → Date et heure.
Durée de fonctionnement	Temps qui s'est écoulé depuis la dernière mise sous tension ou redémarrage de l'appareil.
Utilisation moyenne	Charge CPU moyenne (en %) sur la dernière minute, 5 minutes et 15 minutes.
Adresse MAC du réseau Ethernet LAN	Adresse MAC de l'interface LAN.
Adresse MAC du réseau Ethernet WAN	Adresse MAC de l'interface WAN.
Adresse MAC WiFi (5 GHz)	Adresse MAC de l'interface WiFi 5 GHz.
Adresse MAC WiFi (2,4 GHz)	Adresse MAC de l'interface WiFi 2,4 GHz.
Modèle	Numéro de modèle du modem de l'appareil.
IMEI	L'IMEI (International Mobile Equipment Identity) est un numéro unique à 15 chiffres décimaux utilisé pour identifier les modules mobiles. Les opérateurs de réseau GSM utilisent l'IMEI pour identifier les appareils dans leurs réseaux.
Version FW	Version du logiciel du modem de l'appareil.
Température	Température actuelle du modem.
RAM utilisée	Quantité de mémoire vive (RAM) actuellement utilisée par l'appareil.
Mémoire tampon de la RAM	Quantité de mémoire vive (RAM) utilisée par les données temporairement stockées avant de les déplacer vers un autre emplacement.
Flash utilisé	Quantité de mémoire Flash (stockage) actuellement utilisée par l'appareil.

1.3 Menu STATUT > RÉSEAU

La page Réseau contient des informations relatives à la mise en réseau de l'appareil.

1.3.1 Menu STATUT > RÉSEAU > MOBILE

L'onglet Mobile affiche des informations sur la connexion mobile. Ci-dessous un exemple de l'onglet Mobile :



Emplacement de la carte SIM en cours d'utilisation	Indique quel emplacement pour carte SIM est actuellement utilisé
Statut de la carte SIM	L'état actuel de la carte SIM. Les valeurs possibles sont : • Inséré – La carte SIM est insérée et prête à être utilisée • Non inséré – La carte SIM n'est pas insérée • Inconnu – impossible d'obtenir la valeur d'état de la carte SIM. Problème de communication possible entre l'appareil et le modem
Fournisseur	Nom de l'opérateur du réseau
IMSI	L'IMSI (identité internationale de l'abonné mobile) est un numéro unique à 15 chiffres décimaux (ou moins) utilisé pour identifier l'utilisateur d'un réseau cellulaire.
ICCID	ICCID de la carte SIM – un numéro de série unique utilisé pour identifier la puce SIM.
Opérateur	Nom de l'opérateur réseau.
État de l'opérateur	Indique si le réseau a actuellement enregistré l'appareil mobile. Précise l'état dans lequel le routeur est enregistré sur le réseau. Les valeurs possibles sont : • No registred – non enregistré sur un réseau, l'appareil ne recherche pas un nouvel opérateur auprès duquel s'enregistrer. • Registred (home) – enregistré sur un réseau domestique. • Searching – non enregistré sur un réseau, mais l'appareil recherche un nouvel opérateur auprès duquel s'enregistrer. • Denied – enregistrement au réseau refusé par l'opérateur • Unknow – l'état de l'opérateur est actuellement inconnu • Registred (Roaming) – enregistré sur le réseau, en conditions d'itinérance
Statut de la connexion de données	Indique si l'appareil dispose ou non d'une connexion de données mobiles.
Type de réseau	Type de réseau mobile. Les valeurs possibles sont : • 5G : 5G (NSA), 5G (SA) • 4G : 4G (LTE) • 3G : 3G (WCDMA), 3G (HSDPA), 3G (HSUPA), 3G (HSPA), 3G (HSPA+), 3G (DC-HSPA+), 3G (HSDPA+HSUPA), UMTS • N/A – impossible à déterminer pour le moment
Bande connectée	Bande de fréquence mobile actuellement utilisée.
Puissance du signal (dBm)	Indicateur de puissance du signal reçu (RSSI) mesuré en dBm. Les valeurs plus proches de 0 indiquent une meilleure force du signal
Octets reçus	Quantité de données reçues via l'interface mobile.
Octets envoyés	Quantité de données envoyées via l'interface mobile.

MENU STATUT

Identifiant cellulaire (Cell ID)	L'ID de la cellule à laquelle le modem est actuellement connecté.
LAC	L'indicatif régional de localisation, abrégé en LAC, est le numéro unique attribué à chaque zone de localisation au sein du réseau. La zone desservie d'un réseau d'accès radio cellulaire est généralement divisée en zones de localisation, constituées d'une ou plusieurs cellules radio.
ARFCN	Dans les réseaux cellulaires GSM, un numéro absolu de canal radiofréquence (ARFCN) est un code qui spécifie une paire de porteuses radio physiques utilisées pour la transmission et la réception dans un système radio mobile terrestre, une pour le signal de liaison montante et une pour le signal de liaison descendante.
Code du pays	Le Mobile Country Code, abrégé en MCC, est le code identifiant de manière unique le pays d'origine d'un (Glossaire : Opérateur de réseau mobile (MNO|opérateur de réseau mobile (MNO).
Code du réseau mobile	Le code de réseau mobile (MNC) est un numéro unique à deux ou trois chiffres utilisé pour identifier un réseau mobile terrestre public (PLMN) domestique. MNC est attribué par le régulateur national.
Redémarrer la connexion	Redémarrer la connexion du modem.

1.3.2 Menu STATUT > RÉSEAU> LAN

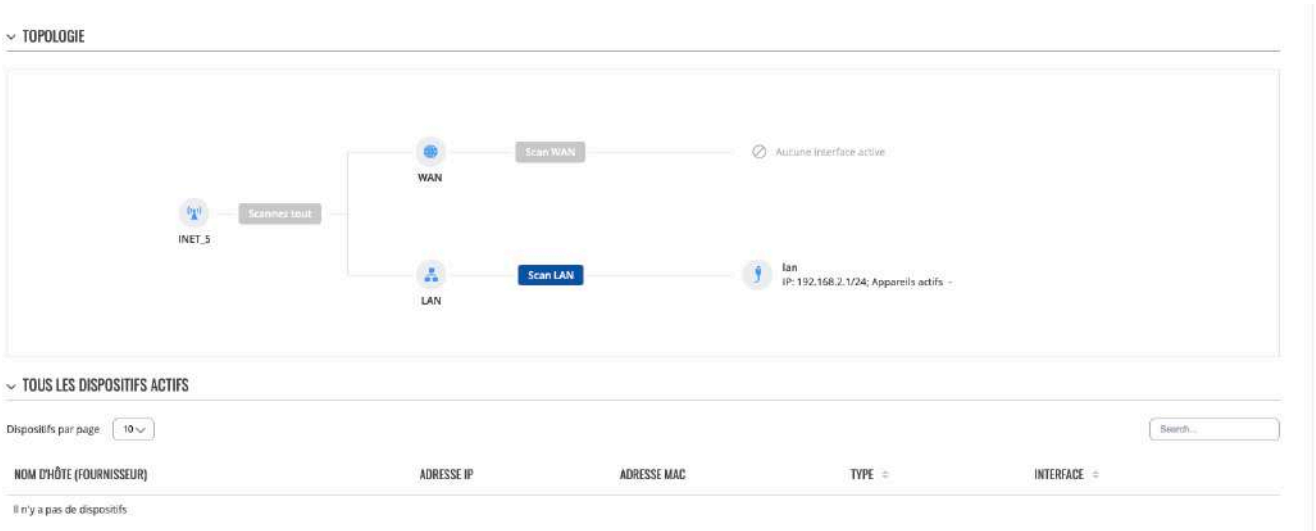
Cet onglet affiche des informations sur le(s) réseau(x) local(aux) de l'appareil.

Informations sur le réseau local	
Nom	Nom de l'interface LAN
Adresse IP	Adresse IP de l'interface LAN
Masque de sous-réseau	Masque de sous-réseau de l'interface LAN. Un masque de réseau indique la taille d'un réseau. Il indique quelle partie de l'adresse IP désigne le réseau et laquelle désigne l'appareil

Baux DHCP	
Nom d'hôte	Nom d'hôte d'un client LAN
Adresse IP	Adresse IP d'un client LAN
Adresse Mac	Adresse MAC d'un client LAN
Durée d'allocation restante	Durée de bail restante pour un client DHCP. Les titulaires de baux DHCP actifs tenteront de renouveler leurs baux DHCP une fois la moitié de la durée du bail écoulée.
Créer Statique	Cette action réservera l'adresse IP actuellement attribuée au périphérique dans Réseau -> Interfaces -> Baux statiques.

1.3.3 Menu STATUT > RÉSEAU> TOPOLOGIE

L' onglet Topologie permet d'analyser le WAN, le LAN ou les deux interfaces via l'analyse arp pour vérifier les périphériques connectés actifs. Après l'analyse, il indique combien de périphériques actifs ont été trouvés et sur quelle interface.



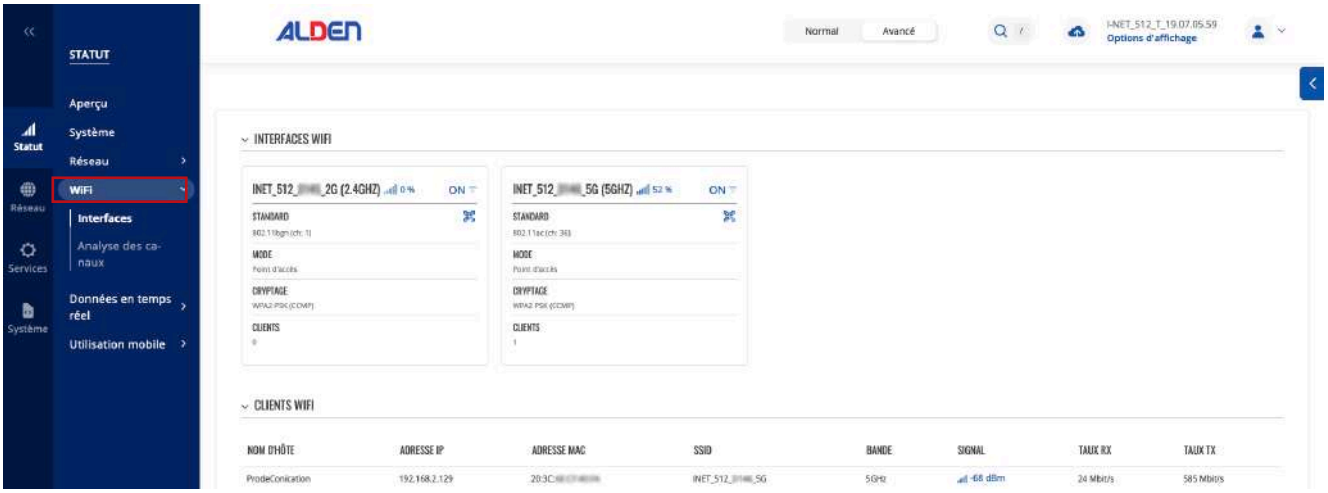
Champ	description
Nom d'hôte (fournisseur)	Nom d'hôte de l'appareil analysé
Adresse IP	Adresse IP de l'appareil analysé
Adresse Mac	Adresse MAC de l'appareil analysé
Type	Le type de connexion
Interface	L'interface à laquelle l'appareil scanné est connecté

1.4 Menu Statut > WiFi

La page Sans fil contient des graphiques qui affichent diverses modifications des données sans fil en temps réel.

1.4.1 Menu STATUT > WIFI > INTERFACE

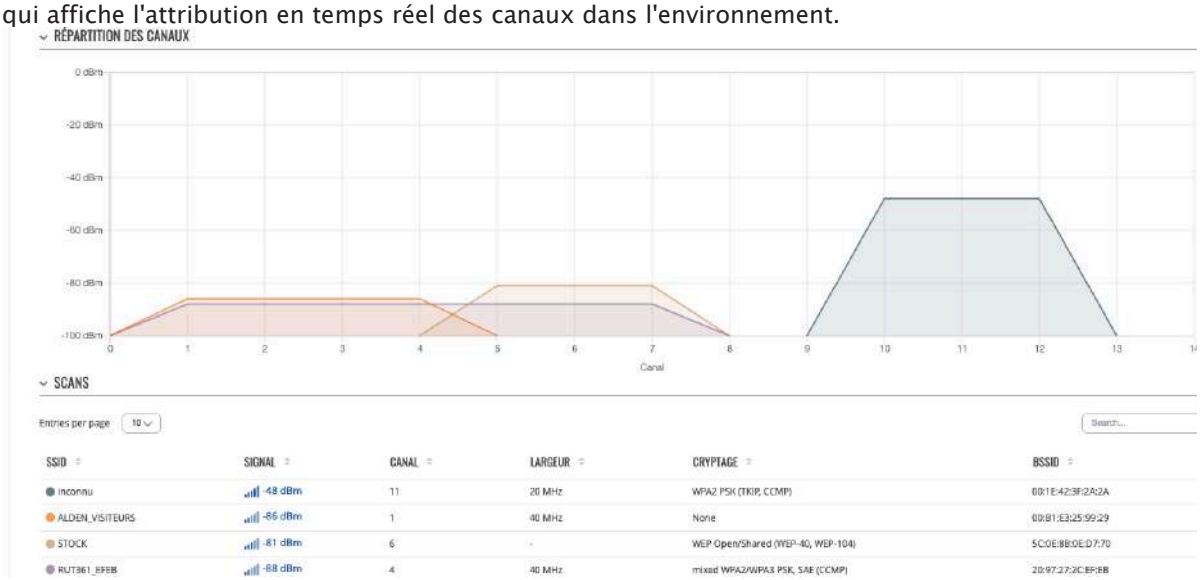
La page Interfaces affiche des informations sur toutes les interfaces sans fil et les clients connectés à l'appareil.



Champ	Description
Mode	Mode de connexion. Peut être un point d'accès (AP) ou un client. En mode AP, d'autres personnes peuvent se connecter à la connexion WiFi de ce routeur. En mode client, le routeur se connecte à d'autres réseaux WiFi.
Cryptage	Type de cryptage WiFi utilisé.
Nom d'hôte	Nom d'hôte de l'appareil.
Adresse IP	Affiche l'adresse IP allouée à l'appareil.
Adresse Mac	Adresse MAC (Media Access Control) de l'appareil.
SSID	Le SSID (Service Set Identifier) est le nom du réseau WiFi.
Bande	Fréquence utilisée.
Signal	Indicateur de force du signal reçu (RSSI). Force du signal mesurée en dBm.
Taux de réception	Taux auquel les paquets sont reçus de l'interface associée.
Taux d'émission	Débit auquel les paquets sont envoyés à l'interface associée.

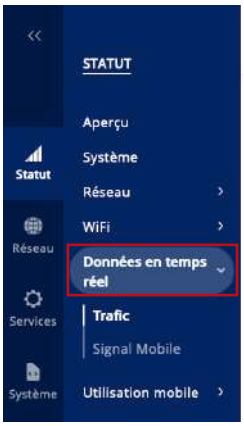
1.4.2 Menu STATUT > WIFI > ANALYSE DES CANAUX

La section "Répartition des canaux" montre un diagramme interactif des bandes radio d'interférence des canaux qui affiche l'attribution en temps réel des canaux dans l'environnement.



La section Scan affiche le tableau des réseaux sans fil visibles. Le tableau peut être trié par SSID, force du signal, canal, largeur, cryptage et adresse MAC (BSSID). Exemple ci-dessus.

1.5. Menu STATUT > DONNÉES EN TEMPS RÉEL



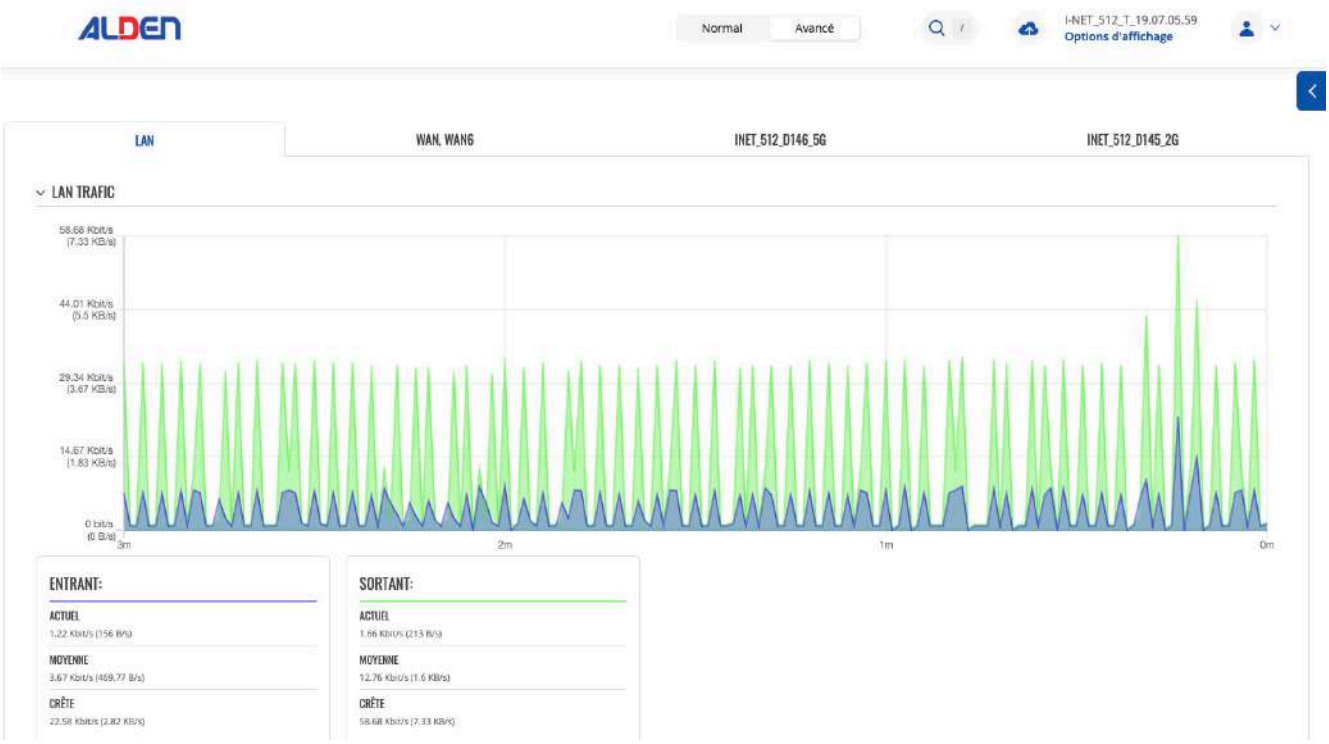
La page Données en temps réel contient divers graphiques qui affichent divers changements de données statistiques en temps réel.

1.5.1 Menu STATUT > DONNÉES EN TEMPS RÉEL > TRAFIC

Les graphiques de trafic en temps réel offrent aux utilisateurs la possibilité de surveiller le trafic entrant et sortant moyen sur une période de 3 minutes. Chaque nouvelle mesure est prise toutes les 3 secondes. Les graphiques se composent de deux graphiques codés par couleur : le graphique vert montre le trafic sortant, le graphique bleu montre le trafic entrant. Bien qu'elle ne soit pas représentée graphiquement, la page affiche également les pics de charge et les moyennes du trafic entrant et sortant.

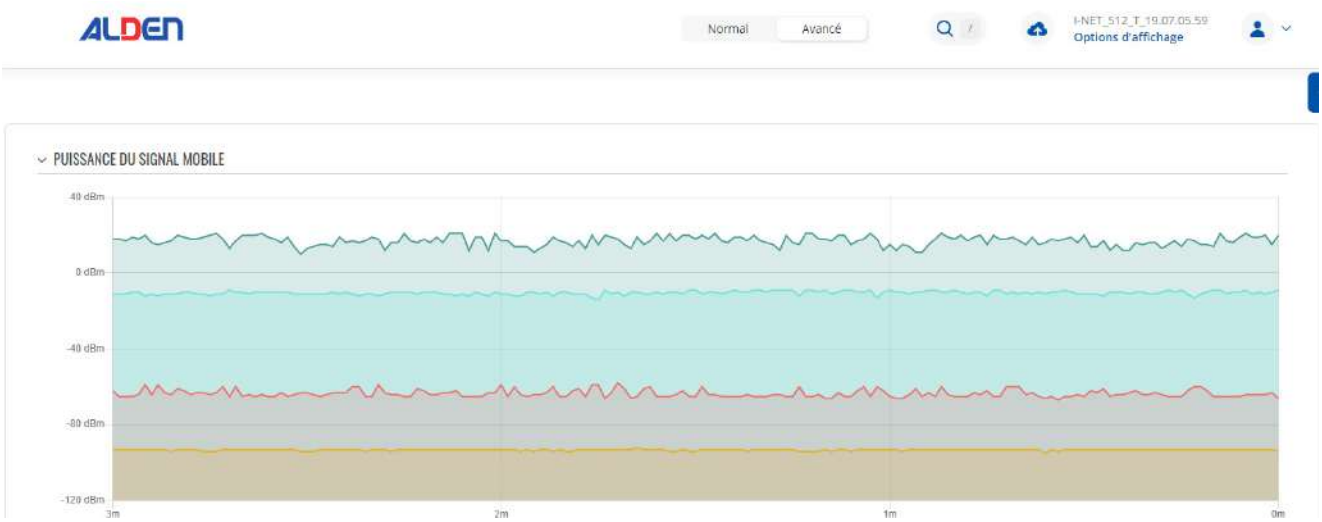
Graphique	Description
I-NET_512_XXXX_5G	Affiche le trafic qui passe par la connexion wifi 5G sous forme de graphique
I-NET_512_XXXX_2G	Affiche le trafic qui passe par la connexion wifi 2G sous forme de graphique
LAN	Affiche le trafic qui passe par la ou les interfaces réseau LAN sous forme de graphique
WAN, WAN6	Affiche le trafic qui passe par la connexion WAN filaire sous forme de graphique

La figure ci-dessous est un exemple de graphique de trafic en temps réel pour la connexion LAN :

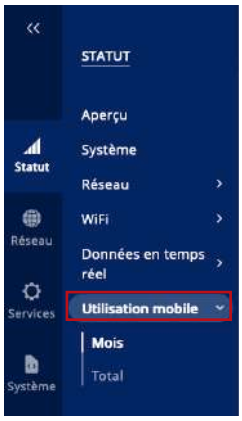


1.5.2 Menu STATUT > DONNÉES EN TEMPS RÉEL > SIGNAL MOBILE

Le graphique Puissance du signal mobile affiche les variations de la valeur de l'intensité du signal cellulaire au fil du temps.

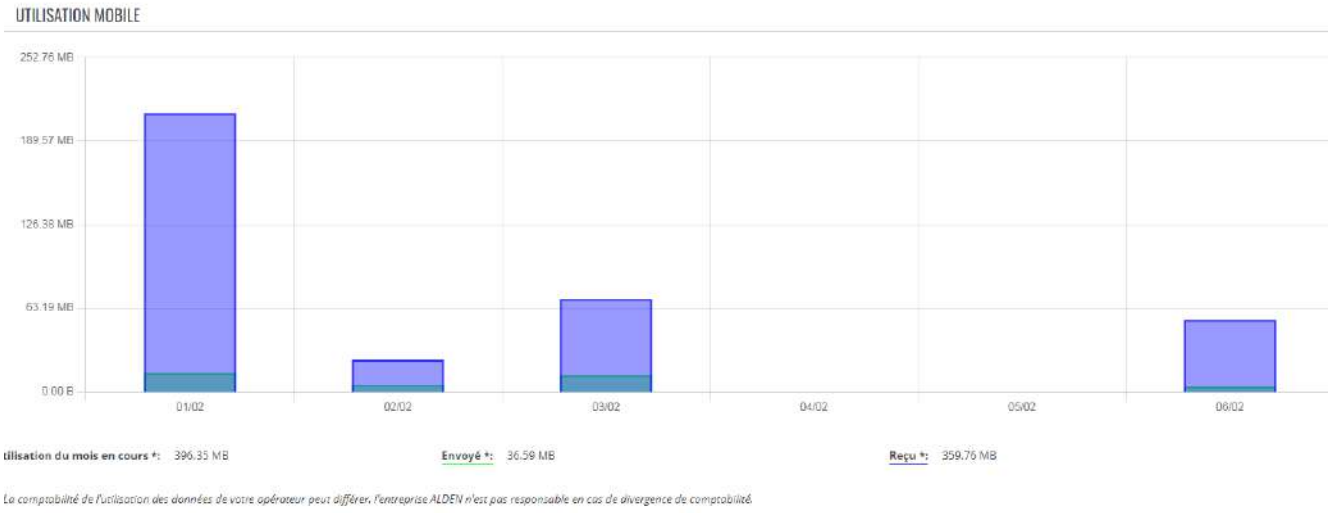


1.6 Menu STATUT > UTILISATION MOBILE

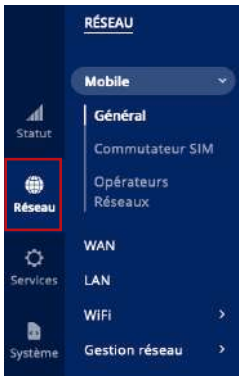


La page Utilisation mobile contient des graphiques qui affichent les valeurs d'utilisation des données mobiles sur différentes périodes et selon la carte SIM.
Vous pouvez accéder à différentes pages pour afficher les valeurs d'utilisation des données mobiles sur différentes périodes et selon la carte SIM.

Mois – valeurs mensuelles d'utilisation des données
Total – utilisation des données pour toute la période de surveillance



2. Menu RÉSEAU



Si vous rencontrez des difficultés pour trouver cette page ou certains des paramètres décrits ici sur l'interface Web de votre appareil, vous devez activer le mode «Avancé». Vous pouvez le faire en cliquant sur le bouton "Avancé", qui se trouve en haut au milieu de l'interface Web.

2.1 Menu RÉSEAU > MOBILE

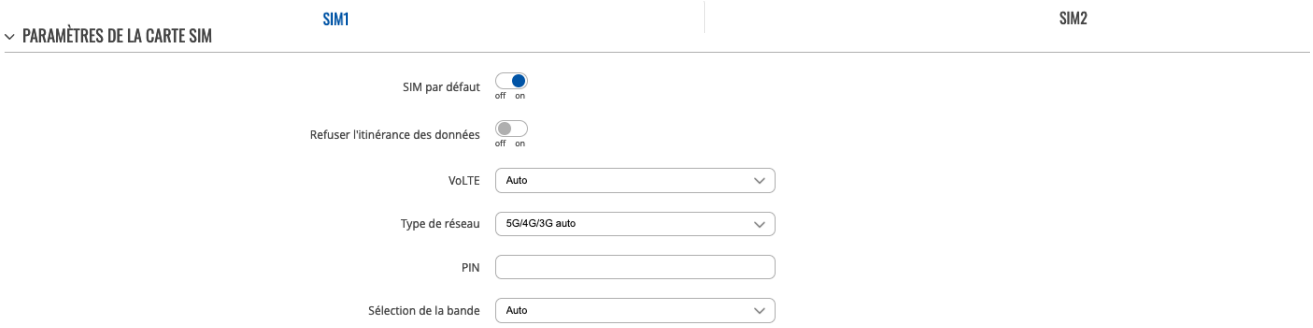
La page Mobile est utilisée pour configurer les paramètres de la connexion mobile.

2.1.1 Menu RÉSEAU > MOBILE > GÉNÉRAL

La section Général est utilisée pour configurer les paramètres de la carte SIM, ils définissent la façon dont l'appareil établira une connexion mobile.
Cette page du manuel fournit un aperçu de la page Mobile dans les appareils I-NET 512.

Paramètres de la carte SIM

La section Paramètres de la carte SIM est utilisée pour configurer les principaux paramètres de la carte SIM. Reportez-vous à la figure et au tableau ci-dessous pour plus d'informations sur les champs contenus dans cette section.
Si la carte SIM est bloqué suite à la saisie de 3 codes PIN erronés se référer "Code PUK", page 7



Carte SIM par défaut	Off | On ; Par défaut : On	Définit cet emplacement SIM comme emplacement par défaut.
Refuser l'itinérance des données	Off | On ; Par défaut : Off	Refuse la connexion de données sur les conditions d'itinérance.
VoLTE	Auto | On | Off ; Par défaut : Auto	Active la voix sur LTE, une technologie de paquets numériques qui utilise les réseaux 4G LTE pour acheminer le trafic vocal et transmettre des données.
Type de réseau	5G/4G/3G auto | 4G/3G auto | 4G seulement | 3G seulement ; Par défaut : 5G/4G/3G auto	Préférence de type de connexion réseau.
PIN	Par défaut : aucun	Le code PIN (numéro d'identification personnel) de la carte SIM est un mot de passe numérique secret utilisé pour authentifier l'appareil auprès de la carte SIM. Les codes PIN sont composés uniquement de chiffres, la longueur peut varier de 4 à 8 symboles. Le code PIN est enregistré dans la mémoire flash, il n'est donc pas réinitialisé lorsque les paramètres par défaut du routeur sont restaurés.
Sélection de la bande	Auto | Manuel Par défaut : Auto	Méthode de sélection de bande de fréquence réseau. Lorsqu'il est réglé sur Auto , l'appareil se connecte à la bande avec les meilleures conditions de connectivité, tandis que Manuel offre la possibilité de sélectionner manuellement les bandes que l'appareil sera obligé d'utiliser. La sélection manuelle des bandes affiche leurs modes duplex pour les appareils compatibles 4G et 5G uniquement.

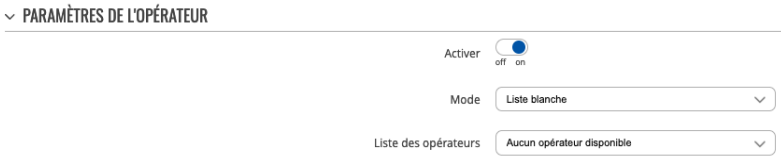
Reconnexion sur signal faible

La section Reconnexion du signal faible est utilisée pour configurer la réinitialisation de la connexion de l'opérateur du modem en fonction de la force du signal pour la carte SIM spécifiée.

Champ	Valeur	Description
Activer	Off | On; Par défaut : Off	Permet la reconnexion du signal faible.
Seuil de réinitialisation	Entier [-120..-50] ; Par défaut : aucun	Seuil de signal en dB pour la connexion. Lorsque le signal est inférieur à cette valeur, le modem réinitialise la connexion.
Délai de réinitialisation	Entier [15..65535] ; Par défaut : 600	Délais en secondes avant de tenter à nouveau de réinitialiser la connexion.

Paramètres de l'opérateur

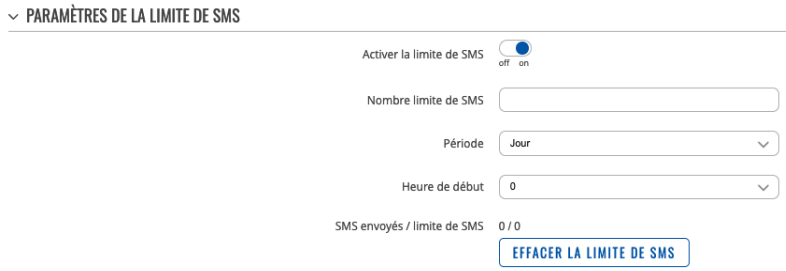
Ce menu n'est visible qu'en mode "Avancé", la section Paramètres de l'opérateur est utilisée pour configurer quels opérateurs peuvent être autorisés (liste blanche) ou bloqués (liste noire).



Champ	Valeur	Description
Activer	Off | On; Par défaut : Off	Active la liste blanche ou la liste noire pour la liste d'opérateurs spécifiée.
Mode	Liste blanche | liste noire ; Par défaut : liste blanche	Mode à appliquer pour la liste des opérateurs. • Liste blanche – n'autoriser que les opérateurs dans la liste • Liste noire – bloquer tous les opérateurs de la liste
Liste des opérateurs	Par défaut : aucun	Une liste d'opérateurs qui peut être configurée dans la page Liste des opérateurs.

Paramètres de limite de SMS

La section Paramètres de limite SMS vous offre la possibilité de configurer un plafond maximum de SMS envoyés pour votre carte SIM.



Champ	Valeur	Description
Activer la limite SMS	Off | On ; Par défaut : Off	Active ou désactive la limitation des SMS.
Nombre limite de SMS	Par défaut : aucun	Définit le plafond d'envoi de SMS, c'est-à-dire le nombre de SMS pouvant être envoyés depuis cette carte SIM pendant la période spécifiée.
Période	jour | semaine | Mois ; Par défaut : Jour	Période pendant laquelle la limitation des SMS doit s'appliquer. Une fois la période expirée, le compteur de limite de SMS sera réinitialisé.
Heure/jour de début	0-23 / lundi - dimanche / 0-31 ; Par défaut : 0	Heure de début du jour / jour de la semaine / jour du mois pour la période de limitation des SMS.
Effacer la limite de SMS	bouton interactif	Efface le compteur de limite de SMS pour la période sélectionnée.

USSD

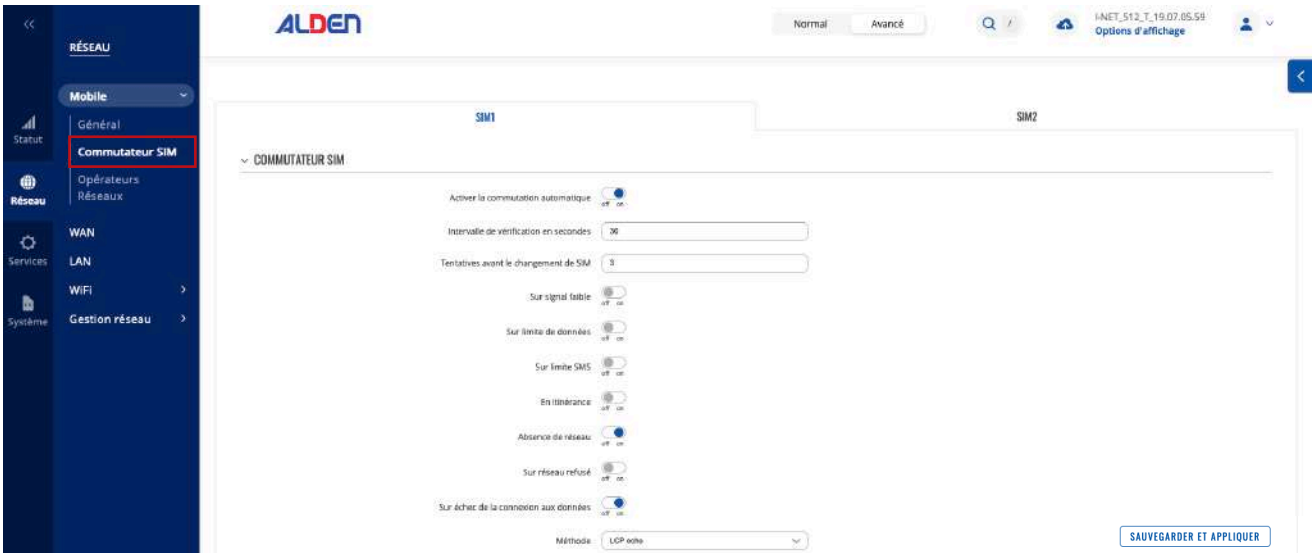
Les données de service supplémentaires non structurées (USSD) sont un protocole de communication utilisé dans la communication entre les appareils cellulaires et les opérateurs de réseaux mobiles. Il est généralement utilisé avec les cartes SIM prépayées pour activer/désactiver certains services ou pour obtenir des informations auprès d'un opérateur réseau.

Cette section offre la possibilité d'envoyer des messages USSD à l'opérateur mobile.

Champ	Valeur	Description
USSD	Par défaut : aucun	Saisissez un code USSD (jusqu'à 182 caractères) que vous souhaitez envoyer. Pour envoyer le code USSD saisi, cliquez sur le bouton « Envoyer » sous la zone de réponse.
Message de réponse	Par défaut : Pas encore de réponse	Affiche la réponse au dernier message USSD envoyé. La réception de la réponse peut prendre jusqu'à une minute.
Envoyer	bouton interactif	Cliquez pour envoyer le message saisi dans le champ USSD.

2.1.2 Menu RÉSEAU > MOBILE > COMMUTATEUR SIM

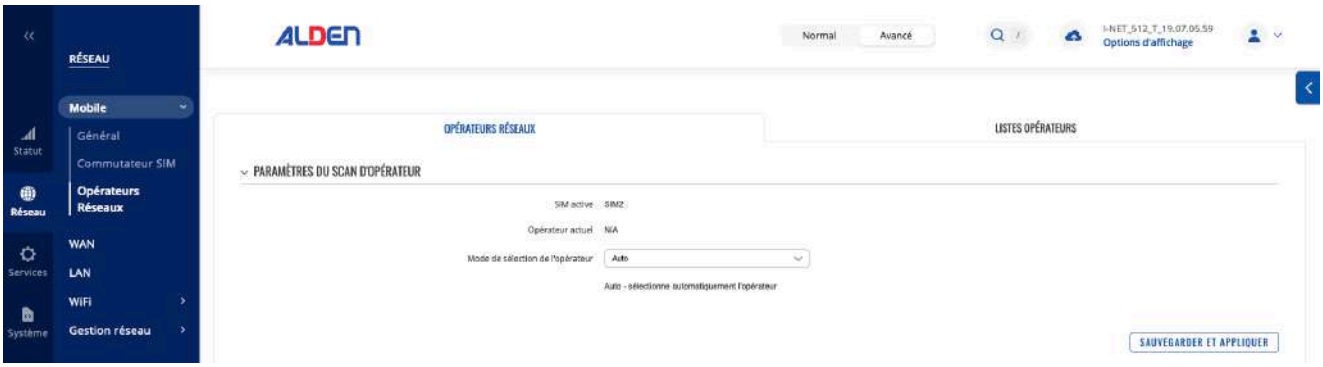
La page Commutateur SIM vous offre la possibilité de configurer les règles de commutation SIM, c'est-à-dire de définir les circonstances dans lesquelles l'appareil effectuera un basculement d'une carte SIM à une autre. Reportez-vous à la figure et au tableau ci-dessous pour plus d'informations.



Activer la commutation automatique	Off | On ; Par défaut : Off	Active ou désactive la commutation automatique de la carte SIM.
Intervalle de vérification en secondes	entier [3..3600] ; Par défaut : 30	Fréquence (en secondes) à laquelle l'appareil vérifiera les conditions du commutateur SIM. Si une telle condition existe, le routeur effectuera un changement de carte SIM, sinon il vérifiera à nouveau les mêmes conditions une fois le délai spécifié dans ce champ écoulé.
Tentatives avant le changement de carte SIM	entier [1..10] ; Par défaut : 3	Nombre de fois ou une condition sera vérifiée avant d'exécuter un changement SIM. Par exemple, si l'appareil est dans un état qui remplit au moins une condition de changement de carte SIM, l'appareil effectuera un certain nombre de vérifications supplémentaires spécifiées dans ce champ et effectuera un changement de carte SIM uniquement si la condition est remplie à chaque vérification.
Sur signal faible*	Off | On ; Par défaut : Off	Effectue un changement de carte SIM lorsque la force du signal descend en dessous d'un certain seuil.
*Puissance du signal (dBm)	Entier [-120..-50] ; Par défaut : -90	Valeur d'intensité du signal la plus basse (RSSI) en dBm en dessous de laquelle un changement de carte SIM doit se produire. Plus d'informations : RSSI
Sur limite de données	Off | On ; Par défaut : Off	Effectue un changement de carte SIM lorsque la limite de données mobiles pour cette carte SIM est atteinte. Vous pouvez configurer une limite de données mobiles dans les pages Réseau → WAN (mode WebUI de base) ou Réseau → Interfaces (mode WebUI avancé) en cliquant sur «Modifier» à côté de l'interface pour laquelle vous souhaitez limiter les données.
Sur limite des SMS	Off | On ; Par défaut : Off	Effectue un changement de carte SIM lorsque la limite de SMS pour cette carte SIM est atteinte. Vous pouvez configurer la limite de SMS sur la page Réseau → Mobile → Général .
En itinérance	Off | On ; Par défaut : Off	Effectue un changement de carte SIM lorsque des conditions d'itinérance sont détectées.
Absence de réseau	Off | On ; Par défaut : Off	Effectue un changement de carte SIM lorsqu'une connexion réseau n'est pas disponible.
Sur réseau refusé	Off | On ; Par défaut : Off	Effectue un changement de carte SIM lorsque l'accès à un réseau est refusé par un opérateur.
Sur échec de la connexion aux données	Off | On ; Par défaut : Off	Effectue un changement de carte SIM lorsque la connexion de données mobiles échoue. Les méthodes possibles de détermination des défaillances sont : - LCP Echo - Echo ICMP Si aucun écho n'est reçu, la connexion de données est considérée comme étant interrompue.

2.1.3 Menu RÉSEAU > MOBILE > OPÉRATEURS RÉSEAUX

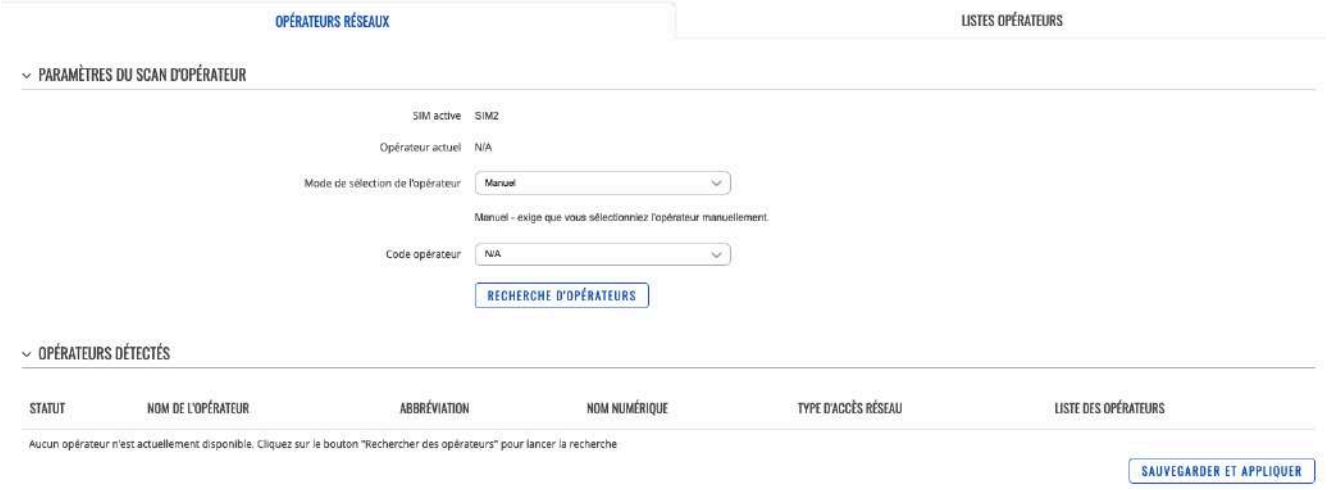
La page Opérateurs réseaux vous offre la possibilité de rechercher et de gérer les opérateurs de réseaux mobiles auxquels la carte SIM de l'appareil peut se connecter. La sélection de l'opérateur n'est disponible que pour la carte SIM principale. Afin de spécifier un opérateur pour l'autre carte SIM, celle-ci doit d'abord être sélectionnée comme SIM principale dans la section Paramètres de la carte SIM.



SIM active	SIM1 | SIM2 ; Par défaut : SIM 1	Affiche quelle carte SIM est actuellement active.
Opérateur actuel	Chaîne; Par défaut : aucun	Affiche le nom de l'opérateur auquel l'appareil est actuellement connecté.
Mode de sélection de l'opérateur	Automobile | Manuel | Manuel-Auto ; Par défaut : Auto	Méthode de sélection des opérateurs. • Auto : sélectionne automatiquement l'opérateur. • Manuel : vous oblige à sélectionner l'opérateur manuellement. • Manuel->Auto: vous invite à saisir le code d'un opérateur, mais si le routeur ne parvient pas à établir la connexion, il se connectera automatiquement au prochain opérateur disponible.

Sélection manuelle de l'opérateur

Pour sélectionner un opérateur manuellement, spécifiez "Mode de sélection de l'opérateur" : Manuel et cliquez sur "Recherche d'opérateurs"



Une fenêtre contextuelle vous demandera si vous êtes sûr. Cliquez sur « Scan » si vous souhaitez continuer. Attendez la fin de l'analyse.

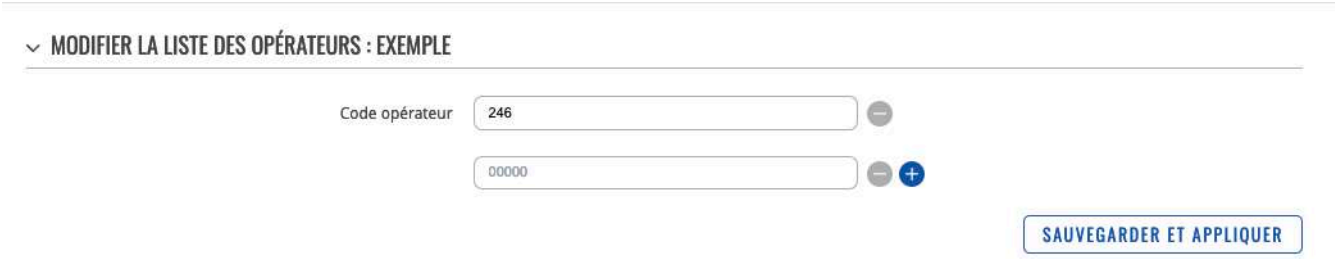
Comme l'indique le message à l'écran, le processus peut prendre jusqu'à 3 minutes.
Une fois l'analyse terminée, vous verrez les résultats dans les « Opérateurs disponibles ».

Afin de verrouiller la carte SIM pour l'utilisation d'un seul opérateur, sélectionnez l'opérateur dans le champ Code opérateur et cliquez sur « Sauvegarder et appliquer ».

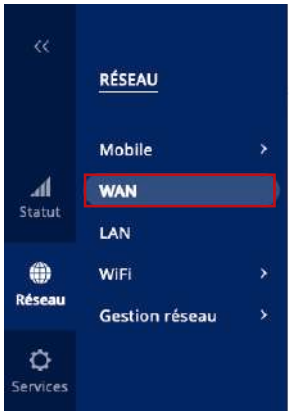
Liste des opérateurs

Cette section est utilisée pour créer des listes de codes d'opérateurs, qui peuvent ensuite être utilisées dans la section Paramètres de l'opérateur pour les mettre sur liste blanche ou sur liste noire. Le code de l'opérateur se compose de deux parties : le code de pays mobile (MCC) et le code de réseau mobile (MNC).

En cliquant sur Modifier sur une liste, vous serez redirigé vers la page d'édition dans laquelle vous pourrez saisir les codes d'opérateur pour cette liste.



2.2 Menu Réseau > WAN (Mode Avancé)



Certaine caractéristique ne sont disponible qu'en mode "Avancé."

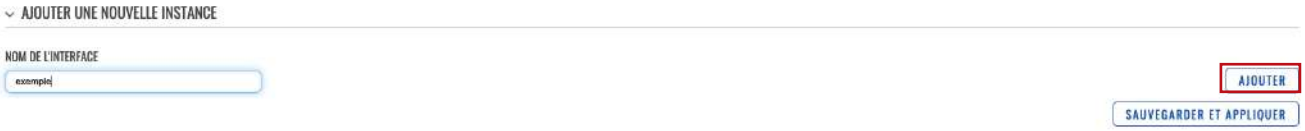
> ⚠ **Pour des raisons de stabilité de fonctionnement de votre routeur, il est fortement conseillé de ne pas modifier les paramètres de ce menu.**
> **Menu réservé aux utilisateurs avertis.**

Interfaces WAN

La section Interfaces Wan affiche les réseaux disponibles sur le routeur.

Ajouter une nouvelle instance

La section Ajouter une nouvelle instance est utilisée pour créer des interfaces réseau supplémentaires. Pour créer une nouvelle interface, entrez simplement un nom personnalisé pour celle-ci et cliquez sur le bouton "Ajouter".



Paramétrage des interfaces

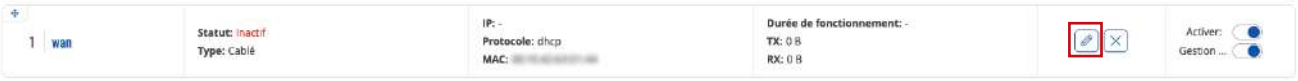
Cette section fournit des informations sur la configuration de l'interface réseau. Il existe deux principaux types d'interfaces sur l'appareil :

- Réseau étendu Ethernet
- Réseau étendu mobile

Différents types d'interfaces peuvent être configurés sous différents protocoles :

	Statique	DHCP	DHCPv6	PPPO	Mobile
Réseau étendu Ethernet	✓	✓	✓	✓	
Réseau étendu mobile					✓

Pour commencer à configurer une interface, cliquez sur le bouton "Modifier  " sur le côté droit de l'interface :

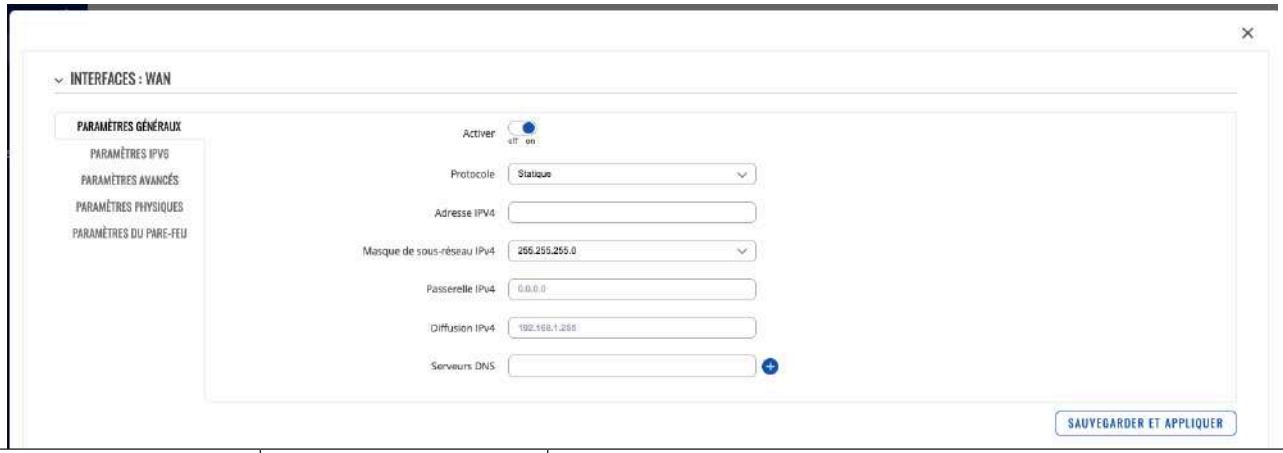


Réglages Généraux

La section Configuration générale est utilisée pour configurer le protocole d'une interface et tous les différents paramètres qui accompagnent chaque protocole. Si Aucun protocole est choisi, tous les autres paramètres d'interface seront ignorés. Les sections suivantes sont différentes pour chaque protocole.

Réglages Généraux : Statique

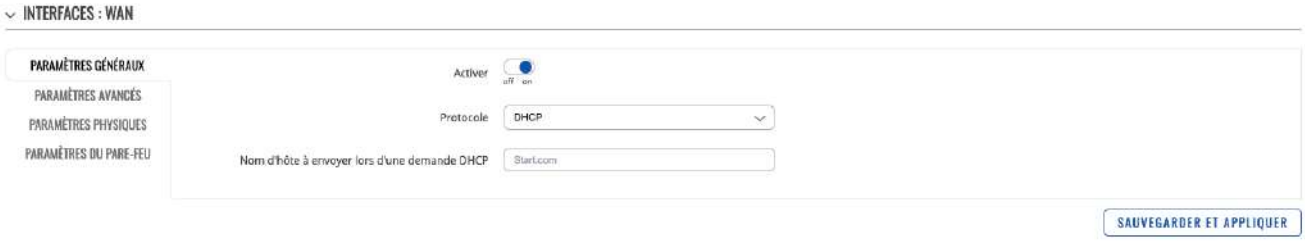
Le protocole Statique utilise une configuration manuelle prédéfinie au lieu d'obtenir automatiquement des paramètres via un bail DHCP.



Champ	Valeur	Description
Activer	Off | On; Par défaut : On	Activer l'interface.
Adresse IPv4	IPv4 ; Par défaut : 192.168.2.1	L'interface d'adresse IPv4 de cette interface. Une adresse IP identifie un appareil sur un réseau et lui permet de communiquer avec d'autres appareils.
Masque de sous-réseau IPv4	Masque de réseau ; Par défaut : 255.255.255.0	Le masque de sous-réseau IPv4 de cette interface. Un masque sous-réseau est utilisé pour définir la « taille » d'un réseau en spécifiant quelle partie de l'adresse IP désigne le réseau et quelle partie désigne un périphérique.
Passerelle IPv4	IPv4 ; Par défaut : aucun	L'adresse de la passerelle IPv4 utilisée par cette interface. La passerelle par défaut d'une interface est l'adresse par défaut par laquelle tout le trafic sortant est dirigé.
Diffusion IPv4	IPv4 ; Par défaut : aucun	L'adresse de diffusion IPv4 utilisée par cette interface. Les diffusions IP sont utilisées par les clients BOOTP et DHCP pour rechercher et envoyer des requêtes à leurs serveurs respectifs.
Serveurs DNS	IPv4 ; Par défaut : aucun	Adresses de serveur DNS que cette interface utilisera. Si laissé vide, les serveurs DNS sont attribués automatiquement. Pour voir quels serveurs DNS sont actuellement utilisés, vous pouvez vérifier le contenu du fichier /tmp/resolv.conf.auto.

Réglages Généraux : DHCP

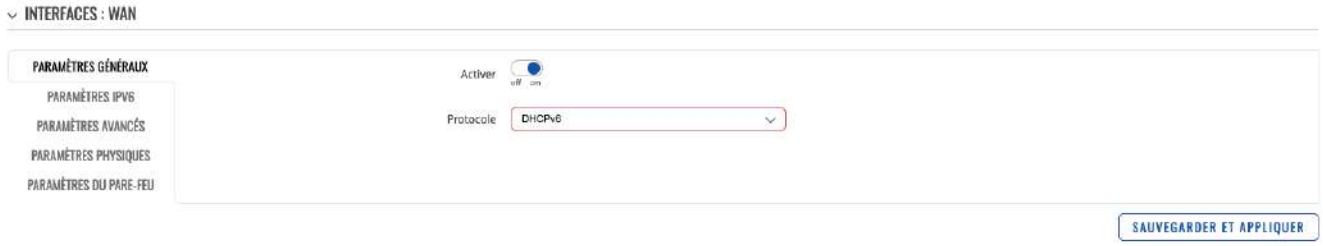
Le protocole DHCP permet de mettre en place une interface qui obtient automatiquement ses paramètres de configuration via un bail DHCP.



Champ	Valeur	Description
Activer	Off | On; Par défaut : On	Activer l'interface.
Nom d'hôte à envoyer lors de la demande DHCP	Chaîne de caractères; Par défaut : aucun	Nom d'hôte pour cette interface utilisée pour identifier cet appareil sur le serveur DHCP.

Réglages Généraux : DHCPv6

Le protocole DHCPv6 permet de mettre en place une interface IPv6 qui obtient automatiquement ses paramètres de configuration via un bail DHCP.



Champ	Valeur	Description
Activer	Off | On; Par défaut : On	Activer l'interface.

Réglages Généraux : PPPoE

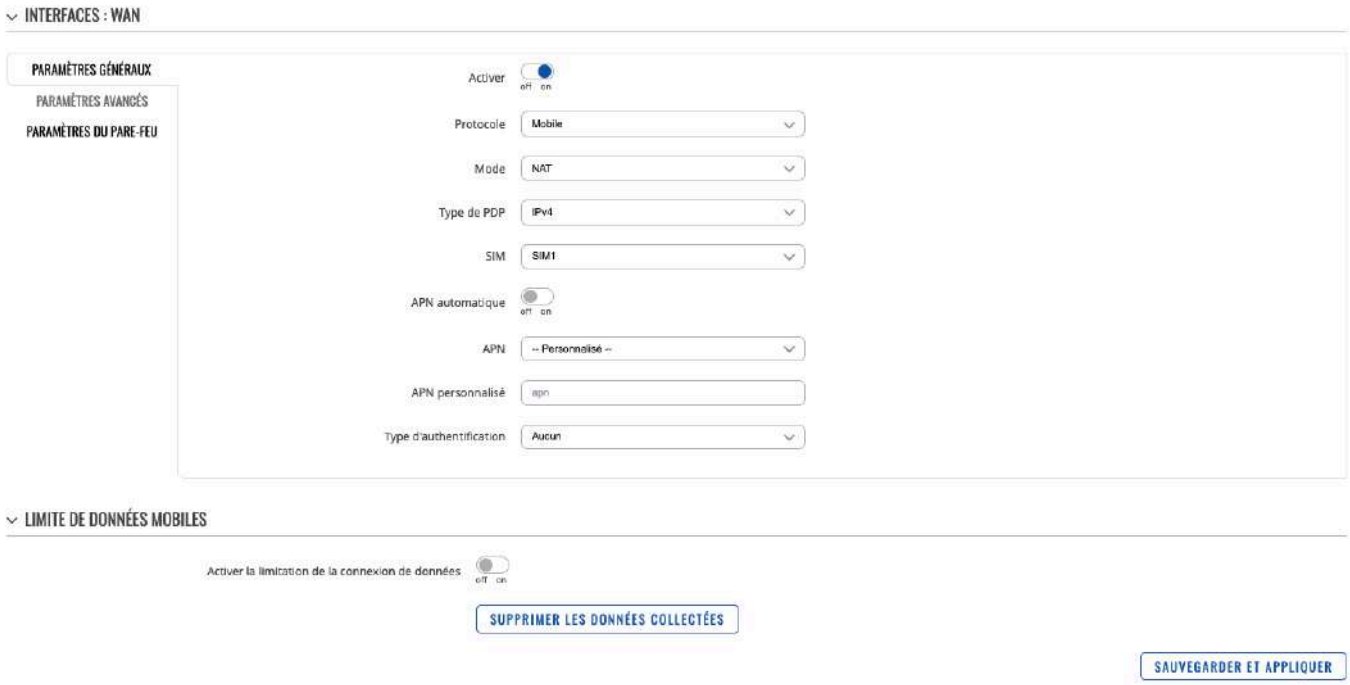
Le protocole PPPoE est utilisé pour établir une connexion PPP (Point-to-Point Protocol) sur le port Ethernet.

Champ	Valeur	Description
Activer	Off | On; Par défaut : On	Activer l'interface.
Nom d'utilisateur PAP/CHAP	Par défaut : aucun	Nom d'utilisateur utilisé dans l'authentification PAP/CHAP.
Mot de passe PAP/CHAP	Par défaut : aucun	Mot de passe utilisé dans l'authentification PAP/CHAP.
Concentrateur d'accès	Par défaut : aucun	Concentrateur d'accès auquel se connecter. Les FAI utilisaient des concentrateurs d'accès pour acheminer leurs connexions PPPoE. Généralement, les paramètres sont reçus automatiquement, mais dans certains cas, il est nécessaire de spécifier le nom d'un concentrateur d'accès. Laissez vide pour détecter automatiquement les concentrateurs d'accès.
Nom du service	Par défaut : aucun	Nom du service auquel se connecter. Laissez vide pour détecter automatiquement le nom du service.

Réglages Généraux : mobile

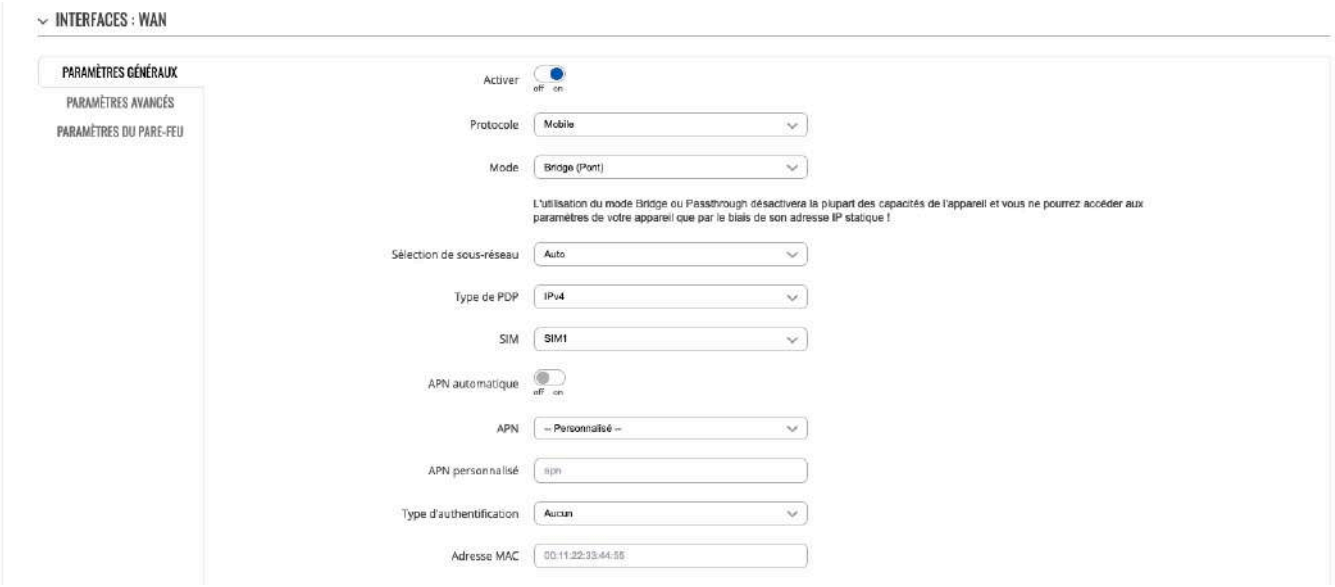
Le protocole Mobile est utilisé pour configurer une interface qui peut établir une connexion WAN mobile.

Mode : NAT



Champ	Valeur	Description
Mode	NAT | Bridge (pont) | Passthrough (traversant); Par défaut : NAT	Mode de fonctionnement de la connexion mobile. • **NAT** – la connexion mobile utilise NAT (traduction d'adresse réseau). • **Bridge** – relie la connexion de données LTE au LAN. L'appareil attribue son adresse IP WAN à un autre appareil (d'abord connecté au LAN ou spécifié avec une adresse MAC). L'utilisation du mode Bridge désactivera la plupart des fonctionnalités de l'appareil. • **Passthrough** – dans ce mode, le I-NET 512 partage son adresse IP WAN avec un seul périphérique LAN (d'abord connecté au LAN ou spécifié avec une adresse MAC). Le périphérique LAN obtiendra l'IP WAN de I-NET 512 au lieu de l'IP LAN. L'utilisation du mode Passthrough désactivera la plupart des fonctionnalités de l'appareil.
Type de PDP	IPv4 | IPv6 | IPv4/IPv6; Par défaut : IPv4	Spécifie quelle adresse sera demandée à l'opérateur.
SIM	SIM1 | SIM2 ; Par défaut : SIM1	Sélectionne quel emplacement SIM sera utilisé pour cette interface.
APN automatique	Off | On; Par défaut : On	La fonction APN automatique analyse une base de données APN Android interne et sélectionne un APN en fonction de l'opérateur et du pays de la carte SIM. Si le premier APN sélectionné automatiquement ne fonctionne pas, il tente d'utiliser le prochain APN existant de la base de données.
APN personnalisé	Par défaut : aucun	Un nom de point d'accès (APN) est une passerelle entre un réseau mobile GSM, GPRS, 3G ou 4G et un autre réseau informatique. Selon le contrat, certains opérateurs peuvent exiger que vous utilisiez un APN juste pour terminer l'enregistrement sur un réseau. Dans d'autres cas, APN est utilisé pour obtenir des paramètres spéciaux de l'opérateur (par exemple, une adresse IP publique) en fonction du contrat. Un identifiant de réseau APN ne peut pas commencer par l'une des chaînes suivantes : • rac; • lac; • sgn ; • rc; il ne peut pas se terminer par : •.gprs ; et il ne peut pas contenir le symbole astérisque (*).
Type d'authentification	Aucun | Pap | Chap; Par défaut : aucun	Méthode d'authentification utilisée par votre opérateur GSM pour authentifier les nouvelles connexions sur son réseau. Si vous sélectionnez PAP ou CHAP, vous devrez également saisir un nom d'utilisateur et un mot de passe.

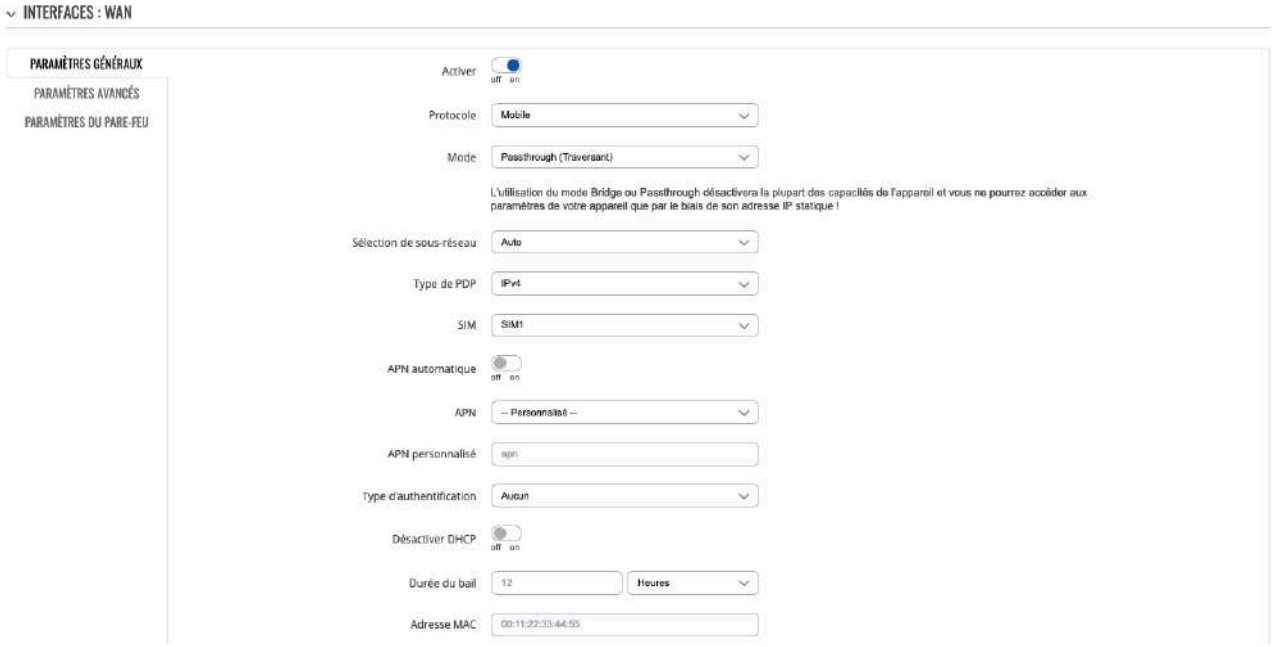
Mode : Bridge (Pont)



Champ	Valeur	Description
Mode	NAT | Bridge | Passthrough; Par défaut : NAT	• **NAT** – la connexion mobile utilise NAT (traduction d'adresse réseau). • **Bridge** – relie la connexion de données LTE au LAN. L'appareil attribue son adresse IP WAN à un autre appareil (d'abord connecté au LAN ou spécifié avec une adresse MAC). L'utilisation du mode Bridge désactivera la plupart des fonctionnalités de l'appareil. • **Passthrough** – dans ce mode, le I-NET 512 partage son adresse IP WAN avec un seul périphérique LAN (d'abord connecté au LAN ou spécifié avec une adresse MAC). Le périphérique LAN obtiendra l'IP WAN de I-NET 512 au lieu de l'IP LAN. L'utilisation du mode Passthrough désactivera la plupart des fonctionnalités de l'appareil.
Sélection de sous-réseau	Automatique | P2P ; Par défaut : Auto	Méthode de sélection de sous-réseau.
Type de PDP	IPv4 | IPv6 | IPv4/IPv6 ; Par défaut : IPv4	Spécifie quelle adresse sera demandée à l'opérateur.
SIM	SIM1 | SIM2 ; Par défaut : SIM1	Sélectionne quel emplacement SIM sera utilisé pour cette interface.
APN automatique	Off | on ; Par défaut : On	La fonction APN automatique analyse une base de données APN Android interne et sélectionne un APN en fonction de l'opérateur et du pays de la carte SIM. Si le premier APN sélectionné automatiquement ne fonctionne pas, il tente d'utiliser le prochain APN existant de la base de données.
APN personnalisé	Par défaut : aucun	Un nom de point d'accès (APN) est une passerelle entre un réseau mobile GSM, GPRS, 3G ou 4G et un autre réseau informatique. Selon le contrat, certains opérateurs peuvent exiger que vous utilisiez un APN juste pour terminer l'enregistrement sur un réseau. Dans d'autres cas, APN est utilisé pour obtenir des paramètres spéciaux de l'opérateur (par exemple, une adresse IP publique) en fonction du contrat. Un identifiant de réseau APN ne peut pas commencer par l'une des chaînes suivantes : • rac; • lac; • sgn ; • rc; il ne peut pas se terminer par : • gprs ; et il ne peut pas contenir le symbole astérisque (*).

Type d'authentification	Aucun | Pap | Chap; Par défaut : aucun	Méthode d'authentification utilisée par votre opérateur GSM pour authentifier les nouvelles connexions sur son réseau. Si vous sélectionnez PAP ou CHAP, vous devrez également saisir un nom d'utilisateur et un mot de passe.
Adresse Mac	Mac; Par défaut : aucun	Spécifie l'adresse MAC de l'appareil qui recevra l'adresse IP de l'interface mobile en mode Bridge ou Passthrough. Remarque : ce champ ne devient visible que lorsque vous utilisez le mode Bridge ou Passthrough.

Mode : Passthrough (traversant)



Champ	Valeur	Description
Mode	NAT | Bridge | Passthrough ; Par défaut : NAT	• **NAT** – la connexion mobile utilise NAT (traduction d'adresse réseau). • **Bridge** – relie la connexion de données LTE au LAN. L'appareil attribue son adresse IP WAN à un autre appareil (d'abord connecté au LAN ou spécifié avec une adresse MAC). L'utilisation du mode Bridge désactivera la plupart des fonctionnalités de l'appareil. • **Passthrough** – dans ce mode, le I-NET 512 partage son adresse IP WAN avec un seul périphérique LAN (d'abord connecté au LAN ou spécifié avec une adresse MAC). Le périphérique LAN obtiendra l'IP WAN de I-NET 512 au lieu de l'IP LAN. L'utilisation du mode Passthrough désactivera la plupart des fonctionnalités de l'appareil.
Sélection de sous-réseau	Automatique | P2P ; Par défaut : Auto	Méthode de sélection de sous-réseau.
Type de PDP	IPv4 | IPv6 | IPv4/IPv6 Par défaut : IPv4	Spécifie quelle adresse sera demandée à l'opérateur.
SIM	SIM1 | SIM2 ; Par défaut : SIM1	Sélectionne quel emplacement SIM sera utilisé pour cette interface.
APN automatique	Off | On ; Par défaut : On	La fonction Auto APN analyse une base de données APN Android interne et sélectionne un APN en fonction de l'opérateur et du pays de la carte SIM. Si le premier APN sélectionné automatiquement ne fonctionne pas, il tente d'utiliser le prochain APN existant dans la base de données.

APN personnalisé	Par défaut : aucun	Un nom de point d'accès (APN) est une passerelle entre un réseau mobile GSM, GPRS, 3G ou 4G et un autre réseau informatique. Selon le contrat, certains opérateurs peuvent exiger que vous utilisiez un APN juste pour terminer l'enregistrement sur un réseau. Dans d'autres cas, APN est utilisé pour obtenir des paramètres spéciaux de l'opérateur (par exemple, une adresse IP publique) en fonction du contrat. Un identifiant de réseau APN ne peut pas commencer par l'une des chaînes suivantes : • rac; • lac; • sgn ; • rc; il ne peut pas se terminer par : • gprs ; et il ne peut pas contenir le symbole astérisque (*).
Type d'authentification	Aucun | Pap | Chap ; Par défaut : Aucun	Méthode d'authentification utilisée par votre opérateur GSM pour authentifier les nouvelles connexions sur son réseau. Si vous sélectionnez PAP ou CHAP, vous devrez également saisir un nom d'utilisateur et un mot de passe.
Désactiver DHCP	Off | On; Par défaut : On	Désactive l'allocation dynamique des adresses client lorsqu'elle est désactivée
Durée du bail	Valeur ; Par défaut : 1	Heure d'expiration de l'adresse allouée. La valeur minimale pour les heures est 1, la valeur minimale pour les minutes est 2 et la valeur minimale pour les secondes est 120
Unités	Heures | minutes | Secondes ; Par défaut : Heures	Spécifie l'unité de mesure du temps
Adresse Mac	Mac ; Par défaut : aucun	Spécifie l'adresse MAC de l'appareil qui recevra l'adresse IP de l'interface mobile en mode Bridge ou Passthrough. Remarque : ce champ ne devient visible que lorsque vous utilisez le mode Bridge ou Passthrough.

Paramètres IPv6

La section Paramètres IPv6 est utilisée pour configurer certains des paramètres d'interface les plus spécifiques et les moins fréquemment utilisés. Cette section est différente pour chaque protocole.

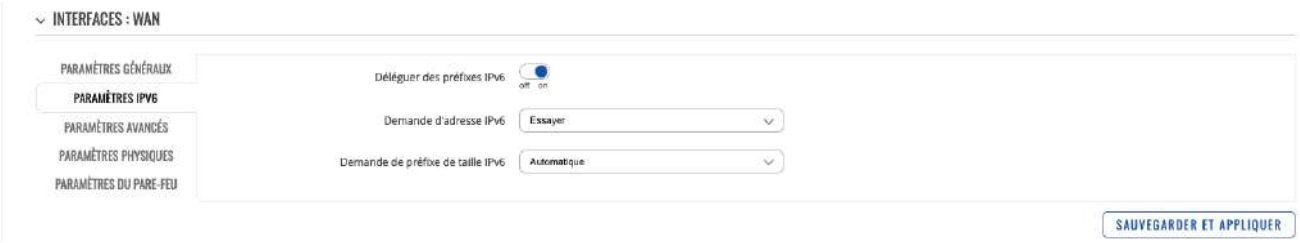
Paramètres IPv6 : protocole Statique

Les informations sur les paramètres avancés pour le protocole statique sont fournies dans le tableau ci-dessous.

Champ	Valeur	Description
Déléguer des préfixes IPv6	Off | On; Par défaut : On	Activez la délégation en aval des préfixes IPv6 disponibles sur cette interface.
Longueur de l'assignation IPv6	Désactivé | 64 ; Par défaut : Désactivé	Une métrique spécifie la priorité de la passerelle. Plus la métrique est basse, plus la priorité est élevée (0 pour la priorité la plus élevée).
Adresse IPv6	Les adresses IPv6 avec ou sans préfixe de masque sont acceptées ; ` Par défaut : aucun	Attribue une adresse IPv6 à cette interface. Notation CIDR : adresse/préfixe.
Passerelle IPv6	Les adresses IPv6 sont acceptées. Par défaut : aucun	Passerelle IPv6 par défaut. Par exemple ::0000:8a2e:0370:7334;
Préfixe routé IPv6	Les adresses IPv6 avec préfixe de masque sont acceptées. Par exemple ::1/128; Par défaut : aucun	Préfixe public acheminé vers cet appareil pour distribution aux clients.
Suffixe IPv6	Valeurs autorisées : "eui64", "random", valeur fixe comme "::1" ou "::1:2" ; Par défaut : aucun	Facultatif. Valeurs autorisées : 'eui64', 'random', valeur fixe comme '::1' ou '::1:2'. Lorsque le préfixe IPv6 (comme 'a:b:c:d::') est reçu d'un serveur délégant, utilisez le suffixe (comme '::1') pour former l'adresse IPv6 ('a:b:c:d: :1') pour l'interface.

Paramètres IPv6 : protocole DHCPv6

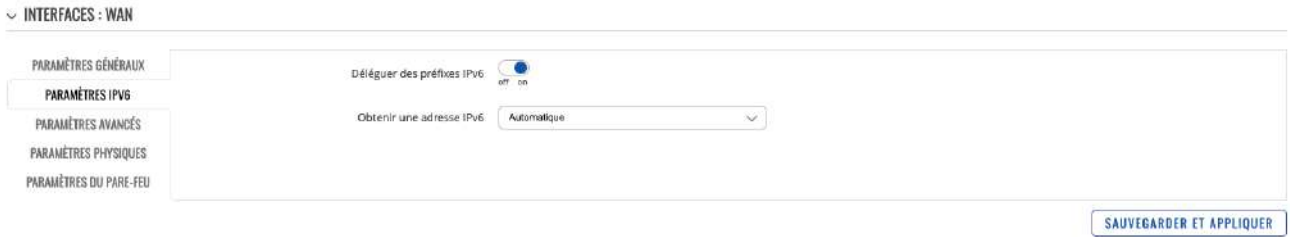
Les informations sur les paramètres avancés pour le protocole DHCPv6 sont fournies dans le tableau ci-dessous.



Champ	Valeur	Description
Déléguer les préfixes IPv6	Off | On; Par défaut : On	Activez la délégation en aval des préfixes IPv6 disponibles sur cette interface.
Demande d'adresse IPv6	Essayer | Forcer | Désactivé; Par défaut : Essayer	Définit le comportement de demande d'adresse.
Demande de préfixe de taille IPv6	48|52|56|60|64| Automatique | Désactivé ; Par défaut : Automatique	Définit comment cela demandera une longueur de préfixe ULA IPv6. Si elle est définie sur « désactivé », l'interface obtiendra une seule adresse IPv6 sans sous-réseau pour le routage.

Paramètres IPv6 : PPPoE

Les informations sur les paramètres avancés du protocole PPPoE sont fournies dans le tableau ci-dessous.



Champ	Valeur	Description
Déléguer les préfixes IPv6	Off | On; Par défaut : On	Activez la délégation en aval des préfixes IPv6 disponibles sur cette interface.
Obtenir une adresse IPv6	Automatique | Désactivé | Manuel; Par défaut : Automatique	Définit le comportement pour obtenir une adresse IPv6.

Paramètres avancés

La section Paramètres avancés est utilisée pour configurer certains des paramètres d'interface les plus spécifiques et les moins fréquemment utilisés. Cette section est différente pour chaque protocole.

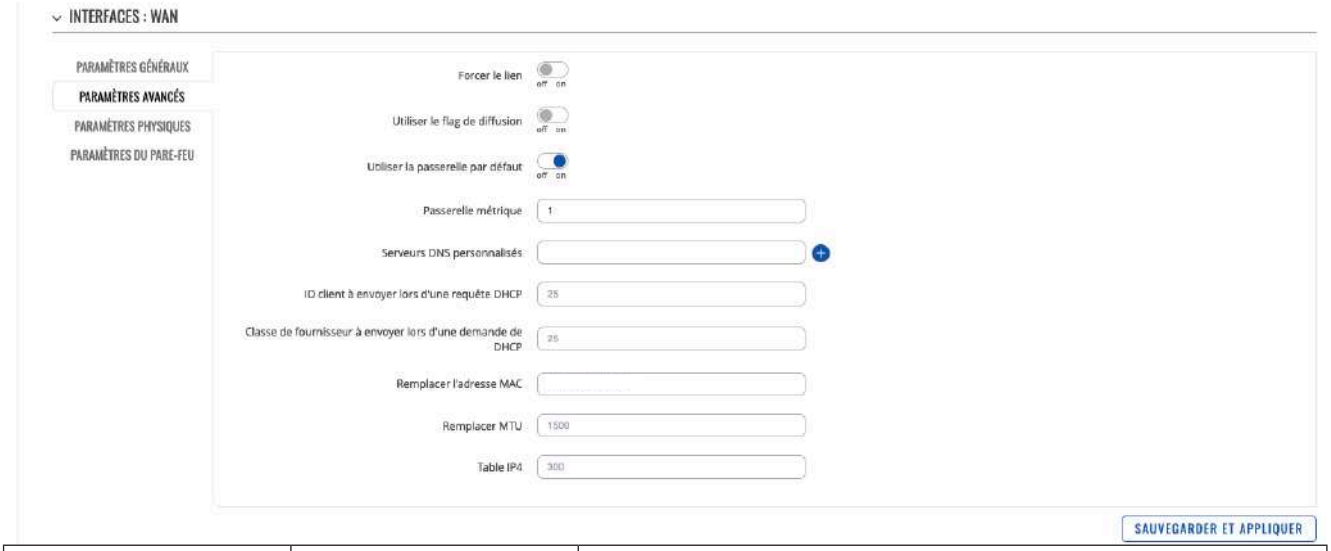
Paramètres avancés : protocole Statique

Les informations sur les paramètres avancés pour le protocole statique sont fournies dans le tableau ci-dessous.

Champ	Valeur	Description
Forcer le lien	Off | On ; Par défaut : On	Spécifie si les paramètres d'interface (IP, route, passerelle) sont attribués à l'interface indépendamment du lien actif ou seulement après que le lien soit devenu actif.
Passerelle métrique	Par défaut : 1	Une métrique spécifie la priorité de la passerelle. Plus la métrique est basse, plus la priorité est élevée (0 pour la priorité la plus élevée).
Remplacer l'adresse MAC	Par défaut : aucun	Lorsqu'il est défini, utilise une adresse MAC définie par l'utilisateur pour l'interface au lieu de celle par défaut.
Remplacer MTU	Valeur[1..9200] ; Par défaut : aucun	Modifie la taille maximale de l'unité de transmission (MTU) autorisée pour l'interface. Il s'agit de la plus grande taille d'unité de données de protocole (PDU) pouvant être transmise dans une seule transaction de couche réseau. • **Remarque :** Interface(s) : si le mtu est inférieur à 1 280, toutes les interfaces de la même interface physique ne prendront plus en charge IPv4. • **Remarque :** Interface(s) : si le mtu est inférieur à 576, toutes les interfaces de la même interface physique ne prendront plus en charge DHCP.
Table IPv4	Valeur [0..99999999] ; Par défaut : aucun	ID de la table de routage.

Paramètres avancés : protocole DHCP

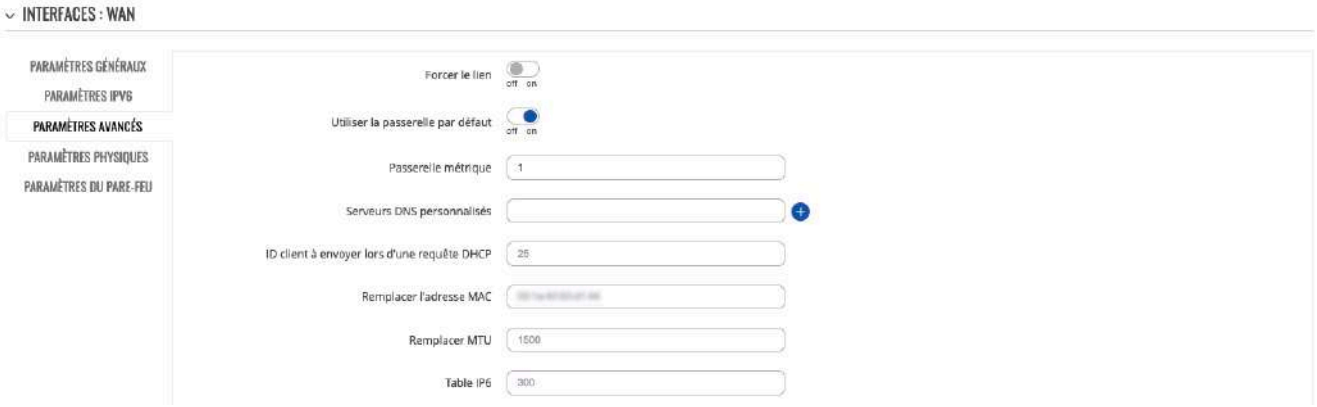
Les informations sur les paramètres avancés pour le protocole DHCP sont fournies dans le tableau ci-dessous.



Champ	Valeur	Description
Forcer le lien	Off | On; Par défaut : Off	Spécifie si les paramètres d'interface (IP, route, passerelle) sont attribués à l'interface indépendamment du lien actif ou seulement après que le lien soit devenu actif.
Utiliser le flag de diffusion	Off | On; Par défaut : Off	Obligatoire pour certains FAI. Par exemple, Charte avec DOCSIS 3.
Utiliser la passerelle par défaut	Off | On; Par défaut : On	Lorsqu'elle est cochée, crée une route par défaut pour l'interface.
Passerelle métrique	Par défaut : aucun	Une métrique spécifie la priorité de la passerelle. Plus la métrique est basse, plus la priorité est élevée (0 pour la priorité la plus élevée).
Serveurs DNS personnalisés	IPv4 ; Par défaut : aucun	Spécifie les serveurs DNS personnalisés. Si laissé vide, les serveurs DNS annoncés par les pairs sont utilisés.
ID client à envoyer lors d'une requête DHCP	Par défaut : aucun	ID client qui sera envoyé lors de la demande d'un bail DHCP.
Classe de fournisseur à envoyer lors d'une demande DHCP	Par défaut : aucun	Classe fournisseur qui sera envoyée lors de la demande d'un bail DHCP.
Remplacer l'adresse MAC	Par défaut : aucun	Lorsqu'il est défini, utilise une adresse MAC définie par l'utilisateur pour l'interface au lieu de celle par défaut.
Remplacer la MTU	Par défaut : aucun	Modifie la taille maximale de l'unité de transmission (MTU) autorisée pour l'interface. Il s'agit de la plus grande taille d'unité de données de protocole (PDU) pouvant être transmise dans une seule transaction de couche réseau. • **Remarque :** Interface(s) : si le mtu est inférieur à 1 280, toutes les interfaces de la même interface physique ne prendront plus en charge IPv4. • **Remarque :** Interface(s) : si le mtu est inférieur à 576, toutes les interfaces de la même interface physique ne prendront plus en charge DHCP.
Table IPv4	Par défaut : aucun	ID de la table de routage.

Paramètres avancés : Protocole DHCPv6

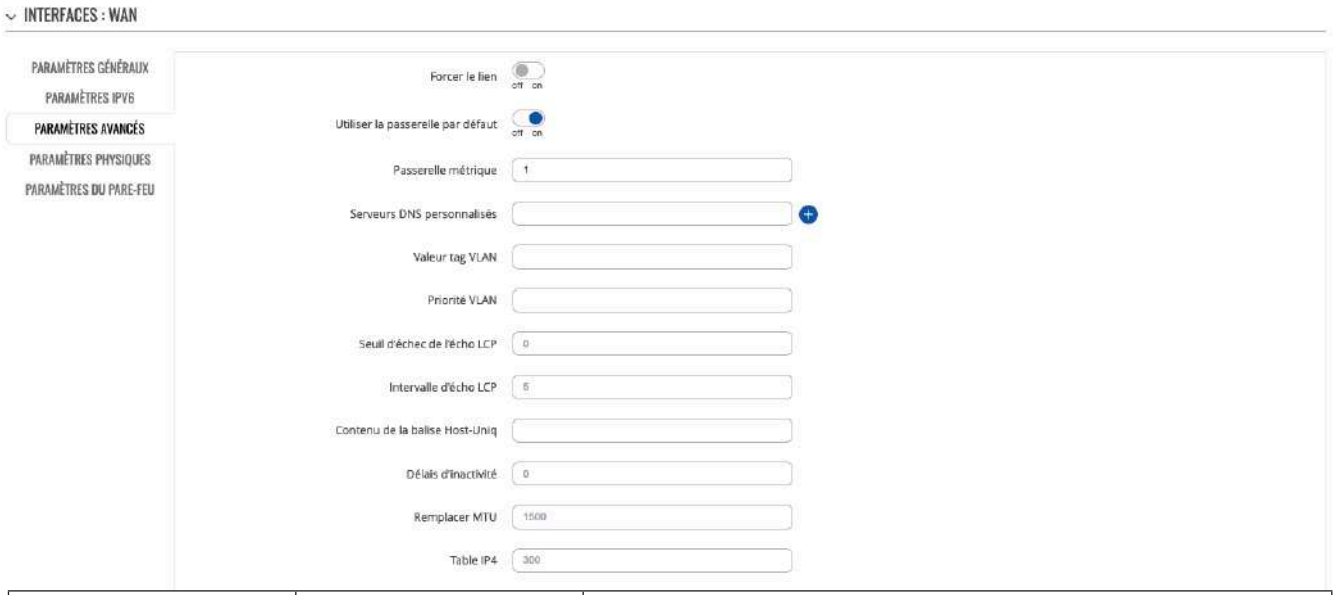
Les informations sur les paramètres avancés pour le protocole DHCPv6 sont fournies dans le tableau ci-dessous.



Champ	Valeur	Description
Forcer le lien	Off | On; Par défaut : Off	Spécifie si les paramètres d'interface (IP, route, passerelle) sont attribués à l'interface indépendamment du lien actif ou seulement après que le lien soit devenu actif.
Utiliser la passerelle par défaut	Off | On; Par défaut : On	Lorsqu'elle est cochée, crée une route par défaut pour l'interface.
Passerelle métrique	Par défaut : 1	Une métrique spécifie la priorité de la passerelle. Plus la métrique est basse, plus la priorité est élevée (0 pour la priorité la plus élevée).
Serveurs DNS personnalisés	Par défaut : aucun	Spécifie les serveurs DNS personnalisés. Si laissé vide, les serveurs DNS annoncés par les pairs sont utilisés
ID client à envoyer lors de la demande DHCP	Par défaut : aucun	ID client qui sera envoyé lors de la demande d'un bail DHCP.
Remplacer l'adresse MAC	Par défaut : aucun	Lorsqu'il est défini, utilise une adresse MAC définie par l'utilisateur pour l'interface au lieu de celle par défaut.
Remplacer MTU	Par défaut : aucun	Modifie la taille maximale de l'unité de transmission (MTU) autorisée pour l'interface. Il s'agit de la plus grande taille d'unité de données de protocole (PDU) pouvant être transmise dans une seule transaction de couche réseau. • **Remarque :** Interface(s) : si le mtu est inférieur à 1 280, toutes les interfaces de la même interface physique ne prendront plus en charge IPv4. • **Remarque :** Interface(s) : si le mtu est inférieur à 576, toutes les interfaces de la même interface physique ne prendront plus en charge DHCP.
Table IP6	Par défaut : aucun	ID de la table de routage.

Paramètres avancés : Protocole PPPoE

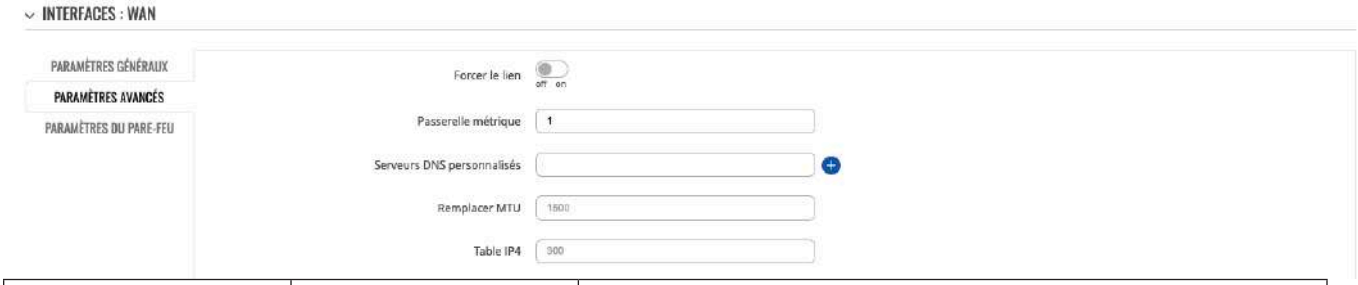
Les informations sur les paramètres avancés pour le protocole PPPoE sont fournies dans le tableau ci-dessous.



Champ	Valeur	Description
Forcer le lien	Off | On ; Par défaut : Off	Spécifie si les paramètres d'interface (IP, route, passerelle) sont attribués à l'interface indépendamment du lien actif ou seulement après que le lien est devenu actif.
Utiliser la passerelle par défaut	Off | On ; Par défaut : On	Lorsqu'elle est cochée, crée une route par défaut pour l'interface.
Passerelle métrique	Par défaut : aucun	Une métrique spécifie la priorité de la passerelle. Plus la métrique est basse, plus la priorité est élevée (0 pour la priorité la plus élevée).
Serveurs DNS personnalisés	Par défaut : aucun	Spécifie les serveurs DNS personnalisés. Si laissé vide, les serveurs DNS annoncés par les pairs sont utilisés.
Valeur de tag VLAN	Par défaut : aucun	Valeur de la balise VLAN.
Priorité VLAN	Par défaut : aucun	Priorité VLAN.
Seuil d'échec d'écho LCP	Par défaut : aucun	Suppose que l'homologue est désactivé après un certain nombre d'échecs d'écho LCP. Laissez-le à 0 pour ignorer les échecs.
Intervalle d'écho LCP	Par défaut : aucun	Envoie des requêtes d'écho LCP à l'intervalle donné en secondes. Cette fonction n'est efficace qu'en liaison avec le seuil de défaillance.
Contenu de la balise Host-Uniq	Par défaut : aucun	Laissez vide sauf si votre FAI l'exige.
Délais d'inactivité	Par défaut : aucun	Fermer la connexion inactive après le nombre de secondes indiqué. Laissez-le à 0 pour conserver la connexion.
Remplacer MTU	Par défaut : aucun	Unité de transmission maximale (MTU) - spécifie la plus grande taille possible d'un paquet de données.
Table IPv4	Par défaut : aucun	ID de la table de routage.

Paramètres avancés : Protocole mobile

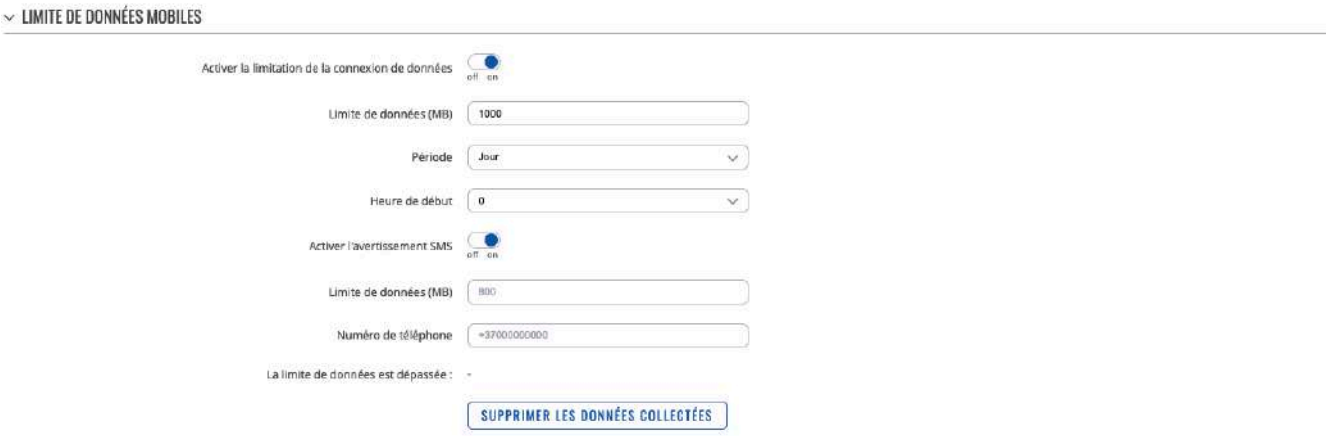
Les informations sur les paramètres avancés pour le protocole mobile sont fournies dans le tableau ci-dessous.



Champ	Valeur	Description
Forcer le lien	Off | On ; Par défaut : Off	Spécifie si les paramètres d'interface (IP, route, passerelle) sont attribués à l'interface indépendamment du lien actif ou seulement après que le lien soit devenu actif.
Passerelle métrique	Par défaut : aucun	Une métrique spécifie la priorité de la passerelle. Plus la métrique est basse, plus la priorité est élevée (0 pour la priorité la plus élevée).
Serveurs DNS personnalisés	Par défaut : aucun	Spécifie les serveurs DNS personnalisés. Si laissé vide, les serveurs DNS annoncés par les pairs sont utilisés.
Remplacer MTU	Par défaut : aucun	Unité de transmission maximale (MTU) – spécifie la plus grande taille possible d'un paquet de données. Si le champ Remplacer la MTU est laissé, une MTU dynamique vide sera utilisée.
Table IPv4	Par défaut : aucun	ID de la table de routage.

Paramètres avancés : Protocole mobile > Limite de données mobiles

Les informations sur les paramètres avancés pour le protocole mobile sont fournies dans le tableau ci-dessous.



Champ	Valeur	Description
Activer la limitation de la connexion de données	Off | On ; Par défaut : Off	Active ou désactive les limitations de données mobiles.
Limite de données (MB)	Par défaut : 1000	Quantité de données pouvant être téléchargées sur la période de temps spécifiée. Lorsque la limite est atteinte, l'appareil ne pourra plus établir de connexion de données jusqu'à ce que la période soit écoulée ou que la limite de données soit réinitialisée.
Période	Jour | Semaine | Mois; Par défaut : Jour	Période limite de données après laquelle le compteur de données est réinitialisé le jour de début spécifié .
Heure de début	Par défaut : heure 0	Active ou désactive l'avertissement SMS. Lorsqu'il est activé et configuré, envoie un message SMS à un numéro spécifié une fois que la carte SIM a utilisé une quantité spécifiée de données.
Activer l'avertissement SMS	Off | On ; Par défaut : Off	Active ou désactive l'avertissement SMS. Lorsqu'il est activé et configuré, envoie un message SMS à un numéro spécifié une fois que la carte SIM a utilisé une quantité spécifiée de données.

Limite de données* (MB)	Par défaut : aucun	La limite de données reçues avant d'envoyer un avertissement SMS. Après avoir atteint la quantité de données spécifiée dans ce champ, le routeur enverra un message d'avertissement SMS au numéro de téléphone spécifié.
Numéro de téléphone	Par défaut : aucun	Numéros de téléphone du destinataire.
La limite de données est dépassée	Par défaut : aucun	La limite de données reçues avant d'envoyer un avertissement SMS. Après avoir atteint la quantité de données spécifiée dans ce champ, le routeur enverra un message d'avertissement SMS au numéro de téléphone spécifié.

* La comptabilité d'utilisation des données de votre opérateur peut différer. ALDEN n'est pas responsable en cas d'écart comptable.

Paramètres physiques

La section Paramètres physiques est utilisée pour créer des associations avec des interfaces physiques et des interfaces réseau de Bridge (pont).

Champ	Valeur	Description
Interfaces Bridge	Off | On ; Par défaut : Off	Relie les interfaces physiques spécifiées dans cette configuration.
Activer STP	Off | On ; Par défaut : Off	Active ou désactive l'utilisation du protocole Spanning Tree (STP) pour cette interface. Remarque : ce champ devient visible lorsque 'Bridge interfaces' est activé.
Activer IGMP	Off | On ; Par défaut : Off	Active la surveillance IGMP sur ce Bridge. Remarque : ce champ devient visible lorsque 'Bridge interfaces' est activé et 'Protocol' est défini sur PPPoE.
Interface	Par défaut : Eth1	Lie cette interface réseau aux interfaces de périphériques physiques telles que les radios Ethernet ou WiFi.

Paramètres du pare-feu

La section Paramètres du pare-feu permet de spécifier à quelle zone de pare-feu appartient, le cas échéant, cette interface. L'attribution d'une interface à une zone peut faciliter la configuration des règles de pare-feu. Par exemple, au lieu de configurer des règles distinctes pour chaque interface WAN, vous pouvez ajouter toutes les interfaces WAN dans une seule zone de pare-feu et appliquer la règle à cette zone.

Champ	Valeur	Description
Créer / Attribuer une zone de pare-feu	Par défaut : aucun	Attribue cette interface à la zone de pare-feu spécifiée.

2.3 Menu Réseau > LAN

Le menu LAN n'est disponible qu'en mode "Avancé."

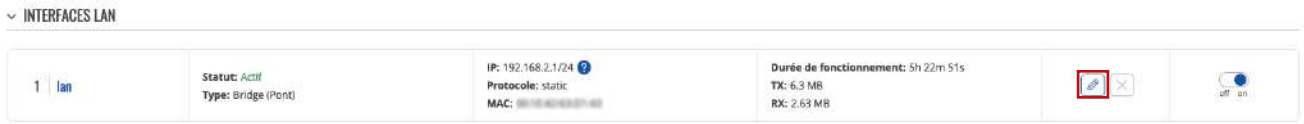
Interfaces LAN

La section Interfaces LAN affiche les réseaux disponibles sur le routeur.

Ajouter une nouvelle instance

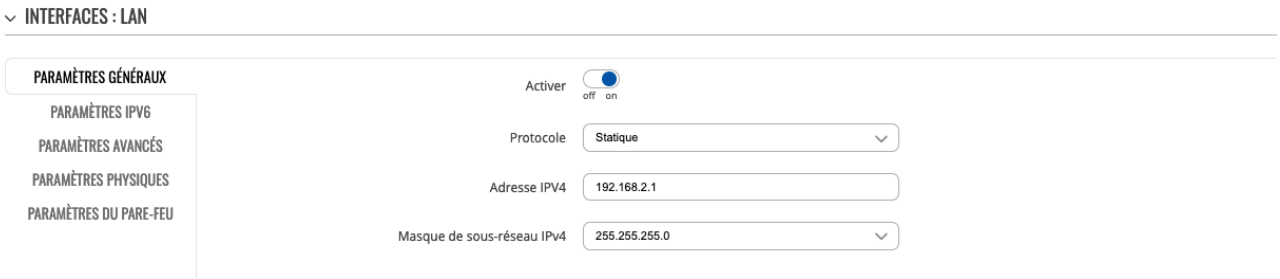
La section Ajouter une nouvelle instance est utilisée pour créer des interfaces réseau supplémentaires. Pour créer une nouvelle interface, entrez simplement un nom personnalisé pour celle-ci et cliquez sur le bouton "Ajouter".

Pour commencer à configurer une interface, cliquez sur le bouton « Modifier » sur le côté droit de l'interface :



Paramètres généraux

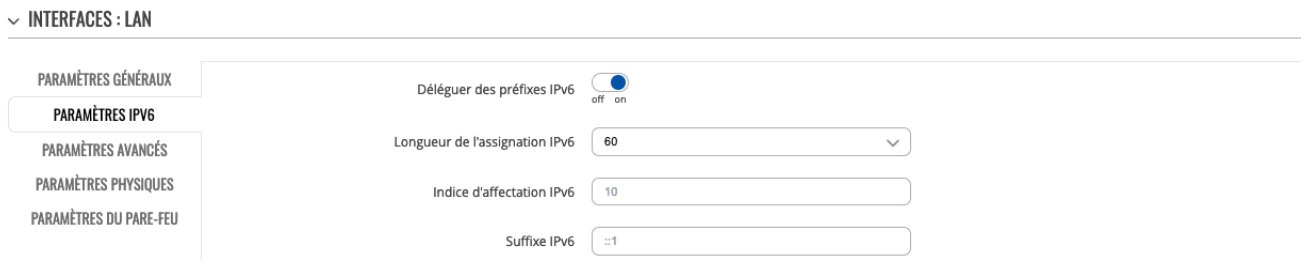
La section Paramètres généraux est utilisée pour configurer les principaux paramètres du LAN.



Champ	Valeur	Description
Activer	Off | On ; Par défaut : On	Attribue cette interface à la zone de pare-feu spécifiée.
Protocole	Statique | Aucun ; Par défaut : Statique	
Adresse IPV4	IP4 ; par défaut : 192.168.2.1	L'adresse de votre routeur sur le réseau
Masque de sous-réseau IPv4	Masque de réseau ; Par défaut : 255.255.255.0	Le masque de réseau IPv4 de cette interface. Un masque de réseau est utilisé pour définir la « taille » d'un réseau en spécifiant quelle partie de l'adresse IP désigne le réseau et quelle partie désigne un périphérique.

Paramètres IPV6

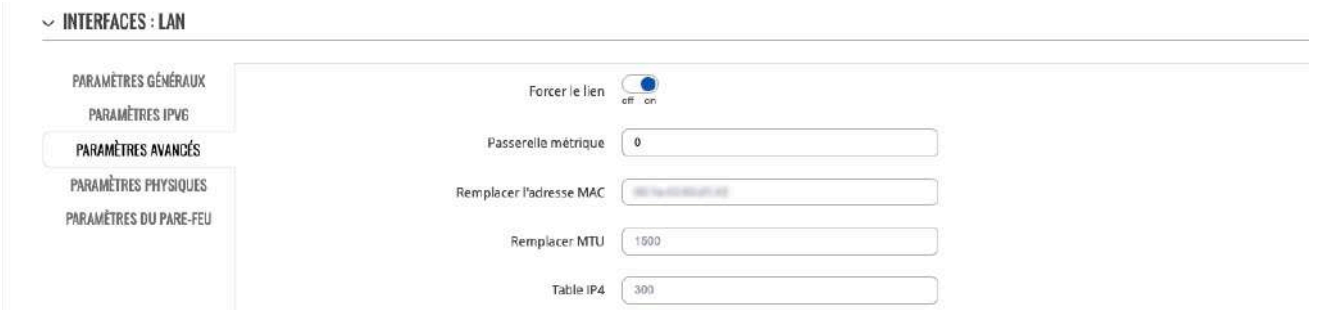
La section Paramètres IPV6 est utilisée pour configurer les paramètres IPv6 du LAN.



Champ	Valeur	Description
Déléguer les préfixes IPv6	Off | On ; Par défaut : On	Activez la délégation en aval des préfixes IPv6 disponibles sur cette interface.
Longueur d'assignation IPv6	Désactivé | 64 | Personnalisé – entier [0..6] ; par défaut : 64	Attribuez une partie d'une longueur donnée de chaque préfixe IPv6 public à cette interface.
Indice d'affectation IPv6	Par défaut : aucun	Attribuez des parties de préfixe à l'aide de cet ID de sous-préfixe hexadécimal pour cette interface.
Suffixe IPv6	Par défaut : aucun	Facultatif. Valeurs autorisées : 'eui64', 'random', valeur fixe comme '::1' ou '::1:2'. Lorsque le préfixe IPv6 (comme 'a:b:c:d::') est reçu d'un serveur délégant, utilisez le suffixe (comme '::1') pour former l'adresse IPv6 ('a:b:c:d: :1') pour l'interface.

Paramètres avancés

La section Paramètres avancés est utilisée pour configurer les paramètres avancés du LAN.

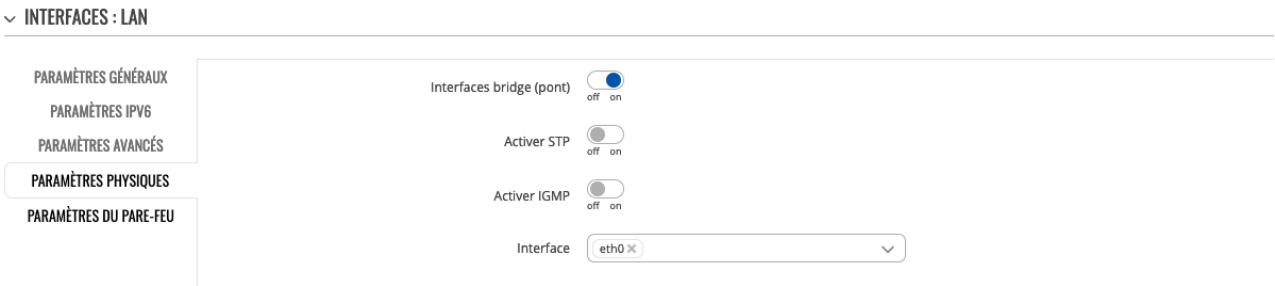


Champ	Valeur	Description
Force le lien	Off | On ; Par défaut : On	Définissez les propriétés de l'interface quel que soit le support de liaison (s'ils sont définis, les événements de détection de support n'appellent pas les gestionnaires de connexion à chaud).
Passerelle métrique	Par défaut : 0	La configuration génère par défaut une entrée de table de routage. Dans ce champ, vous pouvez modifier la métrique de cette entrée. Une métrique inférieure signifie une priorité plus élevée.
Remplacer l'adresse MAC	Par exemple 00:23:45:67:89:AB ; Par défaut : aucun	Remplacez l'adresse MAC de l'interface. Par exemple, votre FAI (fournisseur d'accès Internet) vous donne une adresse IP statique et il peut également la lier à l'adresse MAC de votre ordinateur (c'est-à-dire que cette IP ne fonctionnera qu'avec votre ordinateur mais pas avec votre routeur). Dans ce champ, vous pouvez sélectionner l'adresse MAC de votre ordinateur et faire croire à la passerelle qu'elle communique avec votre ordinateur. Vous pouvez sélectionner l'adresse MAC d'un ordinateur actuellement connecté ou en utiliser une personnalisée. Lorsque vous modifiez l'adresse MAC sur l'interface LAN, veillez à éviter les collisions d'adresses MAC.

Remplacer la MTU	Par défaut : aucun	Unité de transmission maximale (MTU) – spécifie la plus grande taille possible d'un paquet de données.
Table IP4	La valeur doit être un entier non signé valide ; Par défaut : aucun	Table de routage IPv4 pour les routes de cette interface.

Paramètres physiques

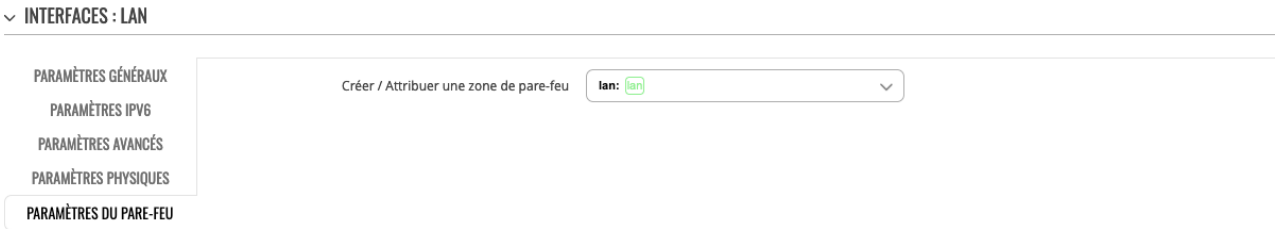
La section Paramètres physiques est utilisée pour configurer les paramètres physiques du LAN.



Champ	Valeur	Description
Interfaces bridge (pont)	Off | On ; Par défaut : On	Crée un pont sur les interfaces spécifiées.
Activer STP	Off | On ; Par défaut : Off	Active le protocole Spanning Tree sur ce pont.
Activer IGMP	Off | On ; Par défaut : Off	Active la surveillance IGMP sur ce pont.
Interface	Interfaces réseau); par défaut : interface physique LAN	Nom de l'interface physique à attribuer à cette section, liste des interfaces si le type pont est défini.

Paramètres du pare-feu

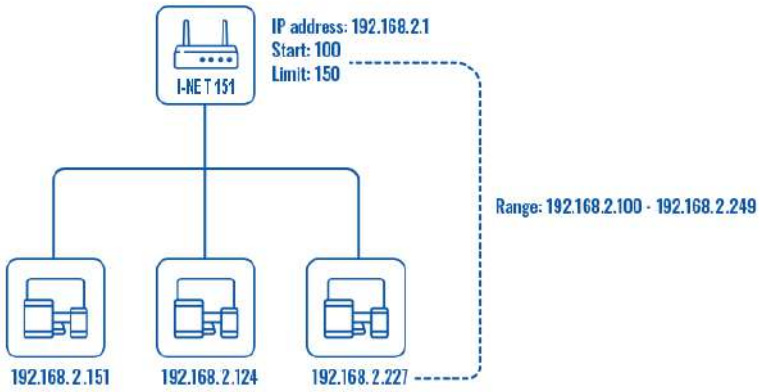
La section Paramètres du pare-feu est utilisée pour configurer les paramètres du pare-feu du LAN.



Champ	Valeur	Description
Créer/attribuer une zone de pare-feu	Non specifié | LAN | WAN ; Par défaut : LAN	Choisissez la zone pare-feu que vous souhaitez attribuer à cette interface. Sélectionnez « Non spécifié » pour supprimer l'interface de la zone associée ou définir une nouvelle zone et y attacher l'interface.

Serveur DHCP

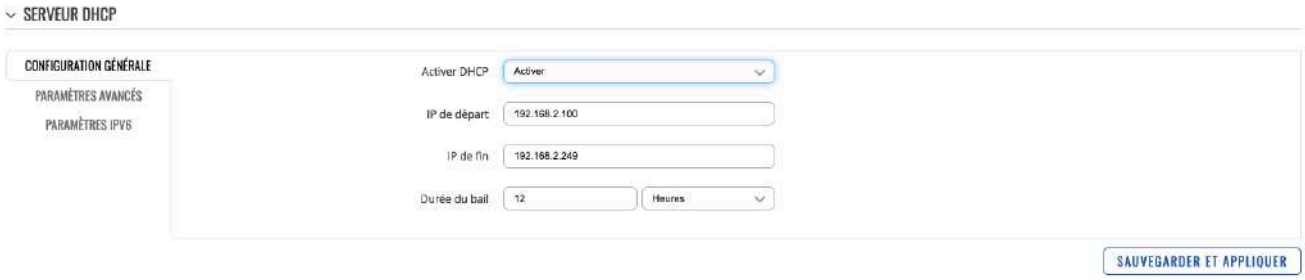
Un serveur DHCP (Dynamic Host Configuration Protocol) est un service qui peut configurer automatiquement les paramètres TCP/IP de tout appareil qui demande un tel service. Si vous connectez un appareil qui a été configuré pour obtenir une adresse IP automatiquement, le serveur DHCP allouera une adresse IP à partir du pool d'adresses



IP disponibles et l'appareil pourra communiquer au sein du réseau privé.
Pour rendre la section DHCP Server visible, définissez le protocole d'interface sur Static.

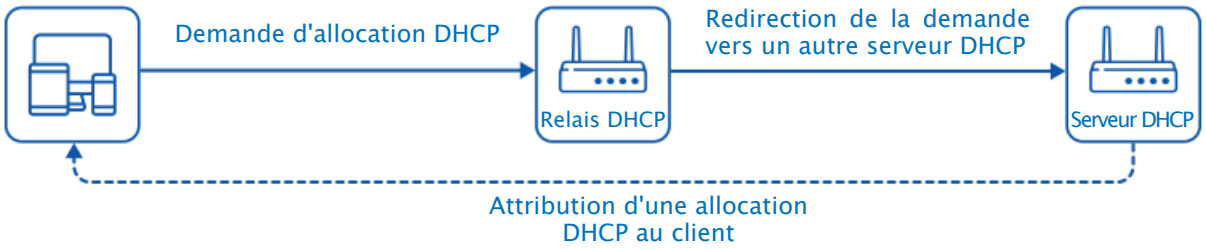
Serveur DHCP : configuration générale

La section configuration générale permet de configurer les principaux paramètres de fonctionnement du serveur DHCP.



Champ	Valeur	Description
Activer DHCP	Activer | Désactiver | Relais DHCP* ; Par défaut : Activer	Active ou désactive le serveur DHCP ou active le relais DHCP *. Si DHCP Relais* est sélectionné, vous serez invité à saisir l'adresse IP d'un autre serveur DHCP de votre réseau local. Dans ce cas, chaque fois qu'une nouvelle machine se connecte à ce périphérique, elle redirige toutes les requêtes DHCP vers le serveur DHCP spécifié.
IP de départ	Par défaut : 100	La valeur de l'adresse IP de départ. Par exemple, si l'adresse IP LAN de votre appareil est 192.168.2.1 et que votre masque de sous-réseau est 255.255.255.0, cela signifie que dans votre réseau, une adresse IP valide doit être comprise entre [192.168.2.0..192.168.2.254] (192.168.2.255 est une adresse spéciale indisponible). Si la valeur Start est définie sur 100, le serveur DHCP ne louera que les adresses à partir de 192.168.2. 100
IP de fin	Par défaut : 254	La valeur de l'adresse IP de départ. Par exemple, si l'adresse IP LAN de votre appareil est 192.168.2.1 et que votre masque de sous-réseau est 255.255.255.0, cela signifie que dans votre réseau, une adresse IP valide doit être comprise entre [192.168.2.0..192.168.2.254] (192.168.2.255 est une adresse spéciale indisponible). Si la valeur Start est définie sur 100, le serveur DHCP ne louera que les adresses à partir de 192.168.2. 100

Durée du bail	Par défaut : 12	Un bail DHCP expirera après la durée spécifiée dans ce champ et l'appareil qui utilisait le bail devra en demander un nouveau. Cependant, si l'appareil reste connecté, son bail sera renouvelé après la moitié de la durée spécifiée (par exemple, si la durée du bail est de 12 heures, toutes les 6 heures, l'appareil demandera au serveur DHCP de renouveler son bail). La durée minimale pouvant être spécifiée est de 2 minutes. * Si les unités sélectionnées sont les minutes. ** Si les unités sélectionnées sont les secondes.
Unités	Heures | minutes | secondes | Infini Par défaut : Heures	Unités de mesure de la durée du bail.



Serveur DHCP : paramètres avancés

Reportez-vous au tableau ci-dessous pour plus d'informations sur la section Paramètres avancés.

Champ	Valeur	Description
DHCP dynamique	Off | On ; Par défaut : On	Active l'allocation dynamique des adresses client. Si cette option est désactivée, seuls les clients qui ont des baux IP statiques seront servis.
Forcer	Off| On ; Par défaut : Off	La fonction de forçage DHCP garantit que l'appareil démarrera toujours son serveur DHCP, même s'il existe un autre serveur DHCP déjà en cours d'exécution sur son réseau. Par défaut, le serveur DHCP de l'appareil ne démarre pas lorsqu'il est connecté à un segment de réseau qui dispose déjà d'un serveur DHCP fonctionnel.
Masque de sous-réseau IPv4	Masque de réseau ; Par défaut : aucun	Envoie un masque de sous-réseau différent du masque de réseau LAN aux clients DHCP.
Option DHCP personnalisées	EDITER- (bouton interactif)	Ouvre la fenêtre d'édition des options DHCP.
Forcer les options DHCP	Off | On ; Par défaut : Off	Si activé, les options DHCP seront envoyées même si elles ne sont pas demandées.

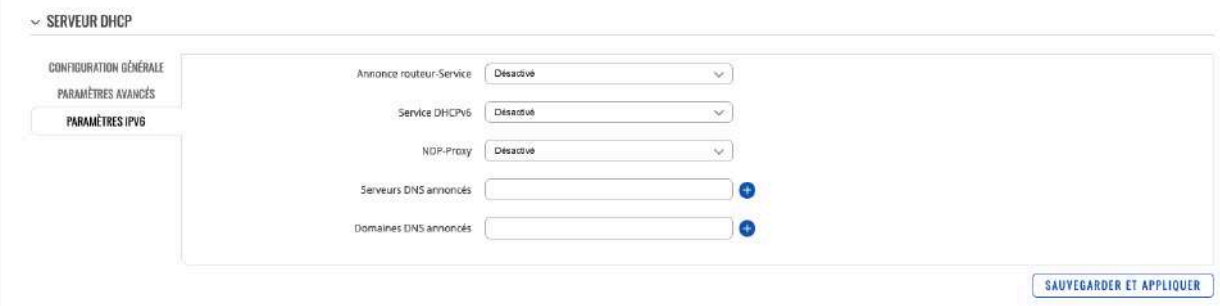
Options DHCP personnalisées

Les options DHCP personnalisées sont des paires de nombres et de valeurs utilisées pour configurer la fonctionnalité DHCP avancée. Il ne configure pas DHCP ipv6. Le modal des options DHCP est utilisé pour «Ajouter», «Supprimer», «Enregistrer» plusieurs options.

Champ	Valeur	Description
Code des options	Personnalisé | Décalage temporel (2) | Routeur (3) | DNS (6) | Champs(15) | serveur NTP (42); Par défaut : Décalage temporel (2)	Code d'option DHCP standardisé.
Valeur d'option	Personnalisé | Décalage temporel (2) – entier | Routeur (3) – IPv4 | DNS (6) – IPv4 | Champs(15) – chaîne | Serveur NTP (43) – IPv4 ; Par défaut : vide	Valeur qui sera définie pour l'option sélectionnée.

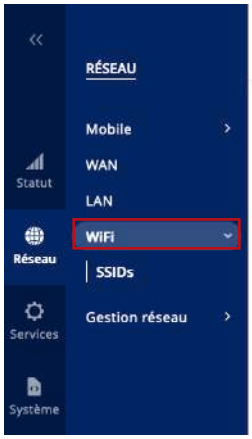
Serveur DHCP : paramètres IPv6

Reportez-vous au tableau ci-dessous pour plus d'informations sur la section Paramètres IPv6.



Champ	Valeur	Description
Annonce routeur-service	Désactivé | Mode relais | Mode serveur | Mode hybride ; Par défaut : Désactivé	Spécifie si les publicités du routeur doivent être activées (mode serveur), relayées ou désactivées.
Service DHCPv6	Désactivé | Mode relais | Mode serveur | Mode hybride ; Par défaut : Désactivé	Spécifie si le serveur DHCPv6 doit être activé (serveur), relayé (relais) ou désactivé (désactivé).
NDP-Proxy	Désactivé | Mode relais | Mode hybride ; Par défaut : Désactivé	Spécifie si NDP doit être relayé ou désactivé.
Serveurs DNS annoncés	Par défaut : aucun	Complète les entrées du serveur DNS attribuées par DHCP avec celles spécifiées dans ce champ.
Domaines DNS annoncés	Par défaut : aucun	Domaine DNS distribué aux clients DHCP.

2.4 Menu RÉSEAU >WiFi



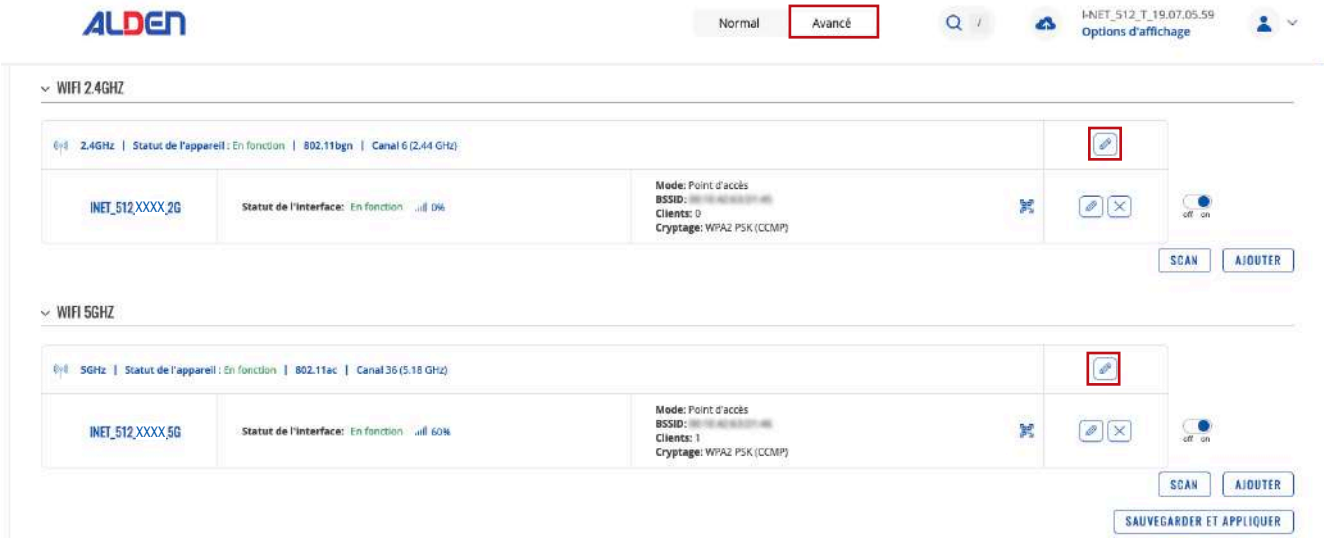
La section WiFi de l'onglet Réseau est utilisée pour gérer et configurer les points d'accès WiFi et les stations WiFi (clients). Ce chapitre du manuel de l'utilisateur donne un aperçu de la section WiFi pour les appareils I-NET 512.

Si vous rencontrez des difficultés pour trouver cette page ou certains des paramètres décrits ici sur l'interface Web de votre appareil, vous devez activer le mode «Avancé». Vous pouvez le faire en cliquant sur le bouton "Normal" sous "Mode", qui se trouve en haut de l'interface Web.

Technologie WiFi
Les appareils I-NET 512 prennent en charge IEEE 802.11ac (WiFi 5) avec des taux de transmission de données allant jusqu'à 867 Mbps (double bande, MU-MIMO), transition rapide 802.11r.

SSID

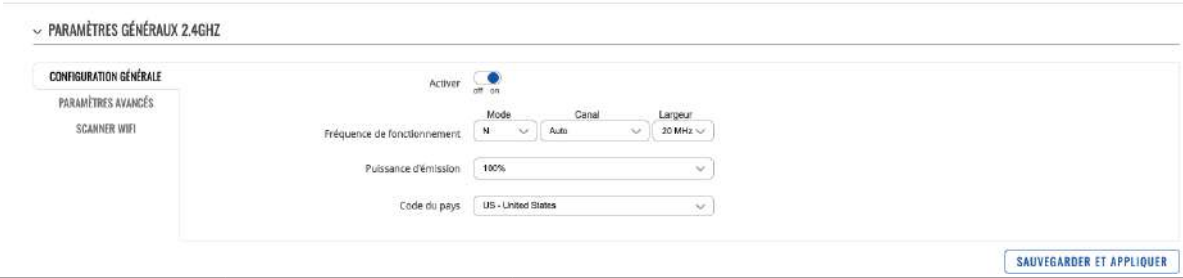
La section SSID est utilisée pour configurer vos points d'accès sans fil (AP) et vos clients sans fil (STA).



Ci-dessus se trouve un aperçu de la fenêtre Présentation du SSIDS. Il affiche les points d'accès et les stations actifs. Ici vous pouvez activer ou désactiver vos interfaces WiFi, les supprimer ou commencer la configuration en cliquant sur le Bouton Modifier sur le côté droit de l'interface. Vous pouvez également configurer vos appareils WiFi en cliquant sur le bouton Modifier sur le côté droit de chaque en-tête de tableau. Pour configurer votre appareil sans fil en tant que client, appuyez sur le bouton Scan pour scanner la zone environnante et tenter de vous connecter à un nouveau point d'accès sans fil.

Configuration générale

La section Configuration générale est utilisée pour activer ou désactiver un périphérique WiFi, sélectionner la fréquence de fonctionnement (mode et canal WiFi), transmettre la puissance et définir un code de pays.
Un canal WiFi sans fil de 2,4 GHz nécessite une bande de signalisation d'environ 22 MHz de large, les fréquences des canaux voisins se chevauchent considérablement. Choisissez un canal WiFi en fonction de l'activité des autres canaux. Vous pouvez télécharger une application d'analyse WiFi gratuite sur votre téléphone, ordinateur portable ou autre appareil WiFi et vérifier quel canal est le moins peuplé.
De nombreux réseaux domestiques utilisent des routeurs qui fonctionnent par défaut sur le canal 6 sur la bande 2,4 GHz. Les réseaux domestiques WiFi voisins qui fonctionnent sur le même canal génèrent des interférences radio qui peuvent entraîner des ralentissements importants des performances du réseau pour les utilisateurs. La reconfiguration d'un réseau pour qu'il s'exécute sur un canal sans fil différent permet de minimiser ces ralentissements. Par conséquent, choisissez un canal sans autres points d'accès actifs et de préférence un canal qui n'a pas de point d'accès actif sur deux canaux adjacents de chaque côté également. Dans le doute, définissez le champ "Canal" sur Auto et l'appareil sélectionnera automatiquement le canal le moins occupé de votre emplacement.



Champ	Valeur	Description
Activer	Off | On ; Par défaut : On	Active ou désactive le périphérique sans fil.
Fréquence de fonctionnement (2,4 GHz)		
Mode	N | Ancienne version ; Par défaut : N	Le Wireless N (802.11n) prend en charge un taux de transfert théorique maximum de 300 Mbps avec 2 antennes. Il peut atteindre jusqu'à 450 Mbps avec 3 antennes. Bien que les vitesses typiques soient plus précisément d'environ 130 Mbps. Les normes existantes incluent 802.11a, 802.11b et 802.11g.
Canal	Auto | 1 (2 412 MHz) | 2 (2 417 MHz) | 3 (2 422 MHz) | 4 (2 427 MHz) | 5 (2 432 MHz) | 6 (2 437 MHz) | 7 (2 442 MHz) | 8 (2 447 MHz) | 9 (2 452 MHz) | 10 (2 457 MHz) | 11 (2 462 MHz); Par défaut : Auto	Un canal WiFi sans fil de 2,4 GHz nécessite une bande de signalisation d'environ 22 MHz de large, les fréquences radio des numéros de canaux voisins se chevauchent considérablement. Par conséquent, choisissez un canal sans autre point d'accès actif et de préférence un canal qui n'a pas de point d'accès actif sur deux canaux adjacents de chaque côté également.
Largeur	20 MHz | 40 MHz ; Par défaut : 20 MHz	Une largeur de canal de 40 MHz relie deux canaux de 20 MHz ensemble, formant une largeur de canal de 40 MHz ; par conséquent, il permet une plus grande vitesse et des taux de transfert plus rapides. Mais pas si ces chaînes sont saturées de bruit et d'interférences. Dans les zones très fréquentées avec beaucoup de bruit de fréquence et d'interférences, un seul canal de 20 MHz sera plus stable. La largeur de canal de 40 MHz permet une plus grande vitesse et des taux de transfert plus rapides, mais elle ne fonctionne pas aussi bien dans les zones très fréquentées.

Fréquence de fonctionnement (5 GHz)		
Mode	N | CA ; Par défaut : CA	Choisissez entre les normes 802.11n et 802.11ac.
Canal	Auto | 36 (5 180 MHz) | 40(5 200 MHz) | 44 (5 220 MHz) | 48 (5 240 MHz) | 52 (5 260 MHz) | 56 (5 280 MHz) | 60 (5 300 MHz) | 64 (5 320 MHz) | 68 (5 340 MHz) | 72 (5 360 MHz) | 76 (5 380 MHz) | 80(5 400 MHz) | 84 (5 420 MHz) | 88 (5 440 MHz) | 92 (5 460 MHz) | 96 (5 480 MHz) | 100(5 500 MHz) | 104 (5 520 MHz) | 108 (5 540 MHz) | 112 (5 560 MHz) | 116 (5 580 MHz) | 120 (5 600 MHz) | 124 (5 620 MHz) | 128(5640 MHz) | 132 (5 660 MHz) | 136 (5 680 MHz) | 140(5 700 MHz) | 144 (5 720 MHz) | 149 (5 745 MHz) | 153 (5 765 MHz) |157 (5 785 MHz) | 161 (5 805 MHz) | 165 (5 825 MHz) ; Par défaut : 36 (5 180 MHz)	Un canal WiFi sans fil de 5 GHz nécessite également une bande de signalisation d'environ 22 MHz de large, mais comme son canal de 20 MHz chevauche moins les canaux voisins, il est néanmoins recommandé de choisir un canal sans autre point d'accès actif et de préférence un qui n'a pas non plus de point d'accès actif sur deux canaux adjacents de chaque côté.
Largeur	20 MHz | 40 MHz | 80 MHz ; Par défaut : 80 MHz	Une largeur de canal de 40 MHz relie deux canaux de 20 MHz ensemble, formant une largeur de canal de 40 MHz, un canal de 8 MHz relie quatre canaux de 20 MHz ; par conséquent, il permet une plus grande vitesse et des taux de transfert plus rapides. Mais pas si ces chaînes sont saturées de bruit et d'interférences. Dans les zones très fréquentées avec beaucoup de bruit de fréquence et d'interférences, un seul canal de 20 MHz sera plus stable. Un canal de largeur 80 MHz est plus rapide que 40 MHz, ce qui est plus rapide que 20 MHz, mais il ne fonctionne pas aussi bien dans les zones très fréquentées.

Puissance de transmission	[5 %...100 %] ; Par défaut : 100 %	La puissance de transmission d'un point d'accès radio est proportionnelle à sa portée effective : plus la puissance de transmission est élevée, plus un signal peut parcourir de distance et/ou plus il peut pénétrer efficacement de matériaux physiques tout en permettant une résolution réussie des données au niveau du point d'accès. destinataire.
Code du pays	Par défaut : US – United States	Codes pays SO/IEC 3166 alpha2 tels que définis dans la norme ISO 3166-1.

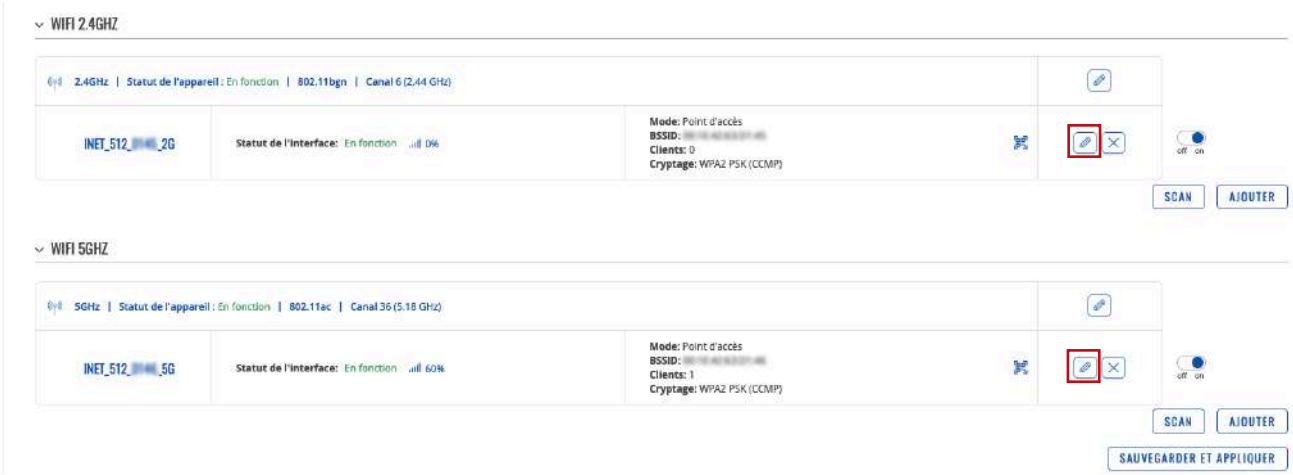
Paramètres avancés

La section Paramètres avancés est utilisée pour configurer le fonctionnement du point d'accès sans fil d'un point de vue matériel.

Champ	Valeur	Description
Fréquence de fonctionnement (2,4 GHz)		
Autoriser les débits de l'ancienne norme 802.11b	Off | On ; Par défaut : On	Activez-le pour activer les connexions qui utilisent l'ancienne norme 802.11b.
Optimisation de la distance	Par défaut : aucun	HT Distance jusqu'au membre du réseau le plus éloigné en mètres.
Seuil de fragmentation	Par défaut : aucun	La plus petite taille de paquet pouvant être fragmentée et transmise par plusieurs trames. Dans les zones où les interférences posent problème, la définition d'un seuil de fragmentation plus faible pourrait contribuer à réduire la probabilité d'échec des transferts de paquets, augmentant ainsi la vitesse.
Seuil RTS/CTS	Par défaut : aucun	RTS/CTS (Request to Send/Clear to Send) sont des mécanismes utilisés pour réduire les collisions de trames introduites par le problème des nœuds cachés. Cela peut aider à résoudre les problèmes qui surviennent lorsque plusieurs points d'accès se trouvent dans la même zone, en concurrence
Forcer le mode 40 MHz	Off | On ; Par défaut : Off	Utilisez toujours les canaux 40 MHz même si le canal secondaire se chevauche. L'utilisation de cette option n'est pas conforme à la norme IEEE 802.11n-2009 !
Intervalle entre les balises	Par défaut : aucun	Intervalle du signal de balise en secondes.
Fréquence de fonctionnement (5 GHz)		
Optimisation de la distance	Par défaut : aucun	HT Distance jusqu'au membre du réseau le plus éloigné en mètres.
Seuil de fragmentation	Par défaut : aucun	La plus petite taille de paquet pouvant être fragmentée et transmise par plusieurs trames. Dans les zones où les interférences posent problème, la définition d'un seuil de fragmentation plus faible pourrait contribuer à réduire la probabilité d'échec des transferts de paquets, augmentant ainsi la vitesse.
Seuil RTS/CTS	Par défaut : aucun	RTS/CTS (Request to Send/Clear to Send) sont des mécanismes utilisés pour réduire les collisions de trames introduites par le problème des nœuds cachés. Cela peut aider à résoudre les problèmes qui surviennent lorsque plusieurs points d'accès se trouvent dans la même zone, en concurrence
Forcer le mode 40 MHz	Off | On ; Par défaut : Off	Utilisez toujours les canaux 40 MHz même si le canal secondaire se chevauche. L'utilisation de cette option n'est pas conforme à la norme IEEE 802.11n-2009 !
Intervalle entre les balises	Par défaut : aucun	Intervalle du signal de balise en secondes.
ACS exclut DFS	Off | On ; Par défaut : Off	Activez cette option pour exclure les chaînes DFS de la sélection automatique des chaînes.

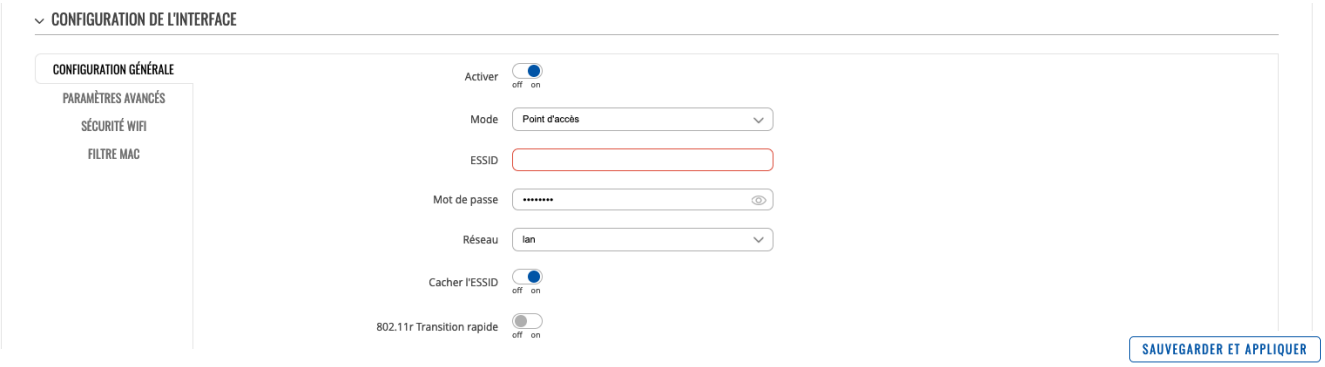
Configuration des interfaces

La section Configuration de l'interface est utilisée pour configurer les paramètres des points d'accès ou des clients sans fil. Vous pouvez trouver cette section en cliquant sur le bouton « Modifier » à côté d'un périphérique sans fil dans la page Réseau → WiFi → SSID :



Configuration générale

L' onglet Configuration générale contient les options de base pour l'ESSID et l'interface réseau.



Champ	Valeur	Description
Activer	Off | On ; Par défaut : On	Active ou désactive l'interface WiFi.
Mode	Client | Point d'accès | Maille | Multi-AP ; Par défaut : point d'accès	Définit le rôle que jouera cette interface, point d'accès pour fournir le WiFi à d'autres appareils, client pour utiliser d'autres appareils WiFi pour WWAN et Mesh pour agir comme passerelle de réseau maillé ou nœud dans un réseau maillé.

Mode point d'accès

ESSID	L'ESSID d'usine est différent pour chaque appareil ; Par défaut : aucun	L'identifiant d'ensemble de services étendu est un nom utilisé pour identifier le point d'accès qui s'affiche lorsque le client tente de s'y connecter.
Mot de passe	Par défaut : aucun	Phrase secrète personnalisée utilisée pour l'authentification (au moins 8 caractères).
Réseau	Auto (wifi0) lan | wan | wan6 | SIM1 | SIM2 Par défaut : lan	Choisissez le(s) réseau(s) que vous souhaitez connecter à cette interface sans fil ou remplissez le champ de création pour définir un nouveau réseau.
Cacher l'ESSID	Off | On ; Par défaut : Off	Masquer l'identifiant d'ensemble de services étendu.
802.11r Transition rapide	Off | On ; Par défaut : Off	Permet une itinérance rapide entre les points d'accès appartenant au même domaine de mobilité

Mode client

ESSID	L'ESSID d'usine est différent pour chaque appareil ; Par défaut : aucun	L'identifiant d'ensemble de services étendu est un nom utilisé pour identifier le point d'accès auquel le client se connectera.
BSSID	Adresse Mac; Par défaut : aucun	Identificateur d'ensemble de services de base.
Mot de passe	Par défaut : aucun	Phrase secrète personnalisée utilisée pour l'authentification (au moins 8 caractères).
Réseau	Par défaut : Auto	Choisissez le réseau que vous souhaitez connecter à cette interface sans fil ou remplissez le champ Personnalisé pour définir un nouveau réseau (vous serez redirigé vers la page de configuration réseau nouvellement créée).

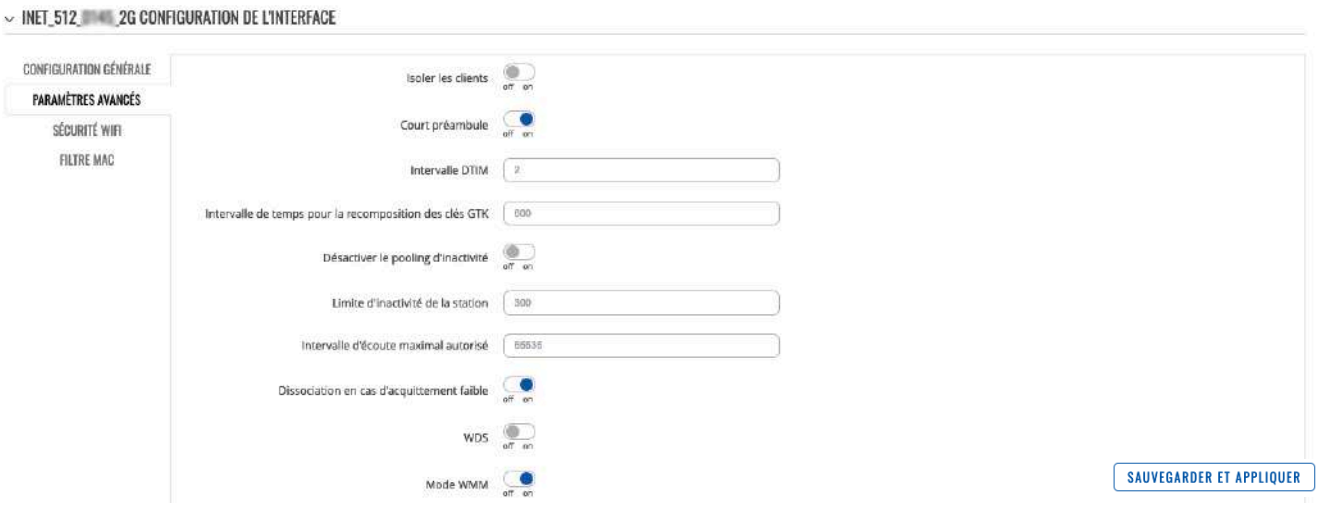
Mode mailles

ID de maillage	Par défaut : aucun	Identifiant du réseau maillé.
Mot de passe	Par défaut : aucun	Phrase secrète personnalisée utilisée pour l'authentification (au moins 8 caractères).
Réseau	Par défaut : Auto	Choisissez le réseau que vous souhaitez connecter à cette interface sans fil ou remplissez le champ Personnalisé pour définir un nouveau réseau (vous serez redirigé vers la page de configuration réseau nouvellement créée).

Multi-AP

Réseau	Par défaut : Auto	Choisissez le réseau que vous souhaitez connecter à cette interface sans fil ou remplissez le champ Personnalisé pour définir un nouveau réseau (vous serez redirigé vers la page de configuration réseau nouvellement créée).
Temps de balayage (sec)	Par défaut : 60	Temps entre les analyses des points d'accès disponibles (minimum 30 secondes)
Charger la liste des AP	Parcourir - (bouton interactif)	Télécharge une liste de configurations de points d'accès.

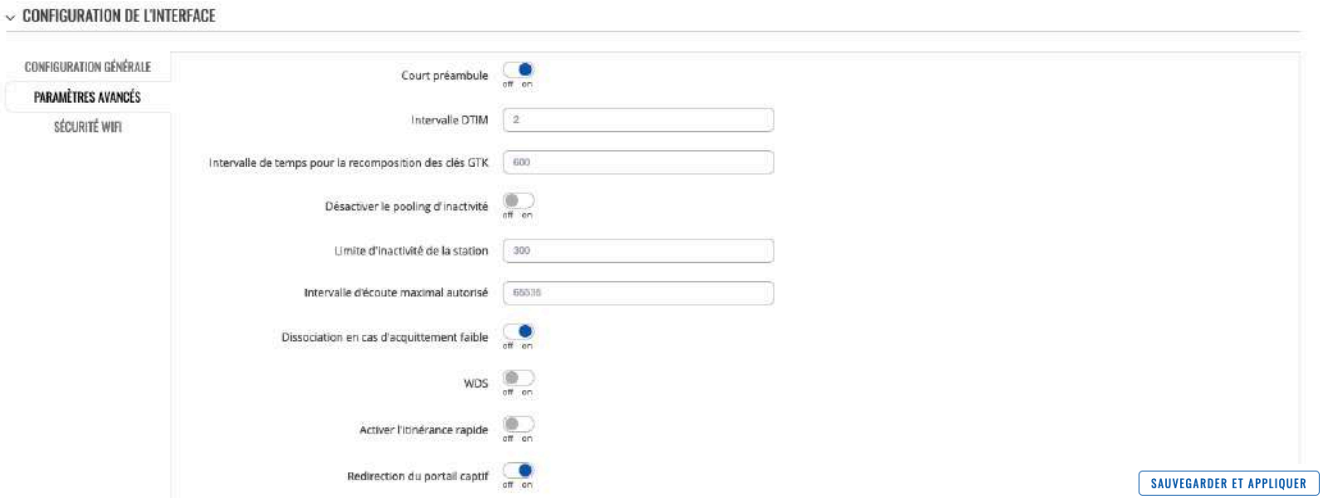
Paramètres avancés : Mode points d'accès



Champ	Valeur	Description
Isoler les clients	Off | On ; Par défaut : Off	Empêche la communication client à client sur le même sous-réseau.
Court préambule	Off | On ; Par défaut : On	Utilise un préambule court, il utilise des chaînes de données plus courtes qui ajoutent moins de données pour transmettre le contrôle de redondance des erreurs, ce qui signifie qu'il est beaucoup plus rapide.
Intervalle DTIM	Par défaut : aucun	Intervalle des messages d'indication du trafic de livraison.

Intervalle de temps pour la recomposition des clés GTK	Par défaut : aucun	Période de temps entre les modifications automatiques de la clé de groupe, partagée par tous les appareils du réseau.
Désactiver le pooling d'inactivité	Off | On ; Par défaut : Off	L'interrogation d'inactivité peut être désactivée pour déconnecter les stations en fonction du délai d'inactivité afin que les stations inactives soient plus susceptibles d'être déconnectées même si elles sont toujours à portée du point d'accès.
Limite d'inactivité de la station	Par défaut : aucun	Limite d'inactivité de la station en secondes. Si une station/client n'envoie rien dans le premier intervalle de temps, une trame de données vide lui est envoyée afin de vérifier si elle est toujours à portée. Si cette trame n'est pas acquittée, la station sera dissociée puis désauthentifiée.
Intervalle d'écoute maximal autorisé	Par défaut : aucun	L'association sera refusée si un client/station tente de s'associer avec un intervalle d'écoute supérieur à cette valeur.
Dissociation en cas d'acquittement faible	Off | On ; Par défaut : On	Autoriser le mode AP à déconnecter les stations/clients en fonction d'une condition d'accusé de réception faible.
WDS	Off | On ; Par défaut : Off	Un système de distribution sans fil (WDS) est un système qui permet l'interconnexion sans fil des points d'accès (AP) dans un réseau.
Mode WMM	Off | On ; Par défaut : On	WiFi Multimedia (WMM), anciennement connu sous le nom d'extensions multimédia sans fil (WME), est un sous-ensemble de la spécification LAN sans fil (WLAN) 802.11e qui améliore la qualité de service (QoS) sur un réseau en hiérarchisant les paquets de données selon quatre catégories.

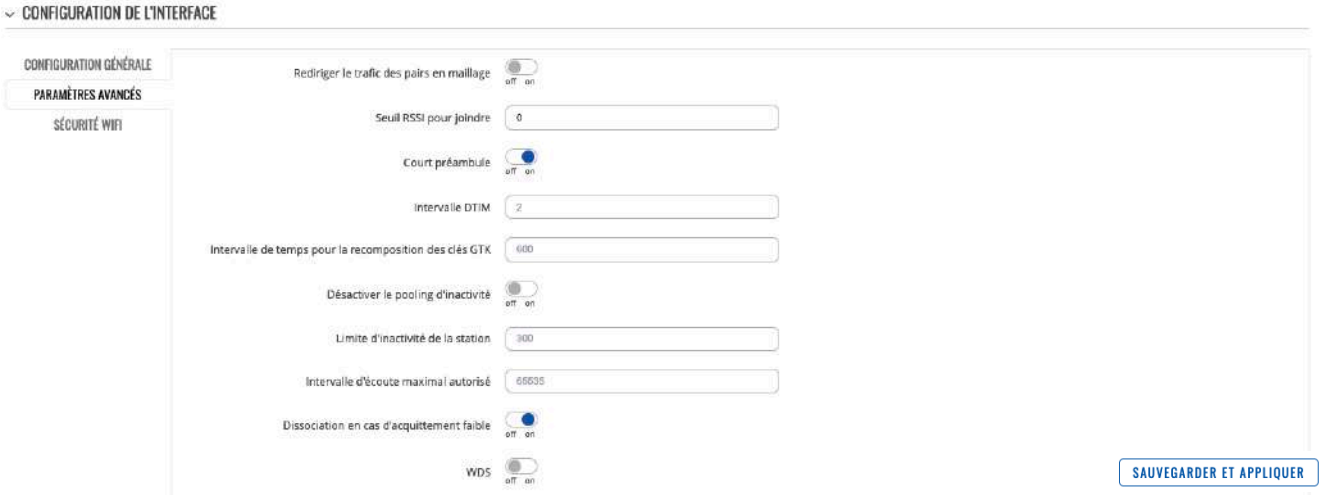
Paramètres avancés : Mode Client et Multi AP



Champ	Valeur	Description
Court préambule	Off | On ; Par défaut : On	Utilise un préambule court, il utilise des chaînes de données plus courtes qui ajoutent moins de données pour transmettre le contrôle de redondance des erreurs, ce qui signifie qu'il est beaucoup plus rapide.
Intervalle DTIM	Par défaut : aucun	Intervalle des messages d'indication du trafic de livraison.
Intervalle de temps pour la recomposition des clés GTK	Par défaut : aucun	Période de temps entre les modifications automatiques de la clé de groupe, partagée par tous les appareils du réseau.
Désactiver le pooling d'inactivité	Off | On ; Par défaut : Off	L'interrogation d'inactivité peut être désactivée pour déconnecter les stations en fonction du délai d'inactivité afin que les stations inactives soient plus susceptibles d'être déconnectées même si elles sont toujours à portée du point d'accès.

Limite d'inactivité de la station	Par défaut : aucun	Limite d'inactivité de la station en secondes. Si une station/client n'envoie rien dans le premier intervalle de temps, une trame de données vide lui est envoyée afin de vérifier si elle est toujours à portée. Si cette trame n'est pas acquittée, la station sera dissociée puis désauthentifiée.
Intervalle d'écoute maximal autorisé	Par défaut : aucun	L'association sera refusée si un client/station tente de s'associer avec un intervalle d'écoute supérieur à cette valeur.
Dissociation en cas d'acquittement faible	Off | On ; Par défaut : On	Autoriser le mode AP à déconnecter les stations/clients en fonction d'une condition d'accusé de réception faible.
WDS	Off | On ; Par défaut : Off	Un système de distribution sans fil (WDS) est un système qui permet l'interconnexion sans fil des points d'accès (AP) dans un réseau.
Activer l'itinérance rapide	Off | On ; Par défaut : Off	Demande des analyses en arrière-plan à des fins d'itinérance au sein d'un ESS.
Redirection du portail captif	Off | On ; Par défaut : On	

Paramètres avancés : Mode Mailles



Champ	Valeur	Description
Rediriger le trafic des pairs en maillage	Off | On ; Par défaut : Off	
Seuil RSSI pour joindre	Par défaut : aucun	0 = ne pas utiliser le seuil RSSI, 1 = ne pas modifier les paramètres par défaut du pilote.
Court préambule	Off | On ; Par défaut : On	Utilise un préambule court, il utilise des chaînes de données plus courtes qui ajoutent moins de données pour transmettre le contrôle de redondance des erreurs, ce qui signifie qu'il est beaucoup plus rapide.
Intervalle DTIM	Par défaut : aucun	Intervalle des messages d'indication du trafic de livraison.
Intervalle de temps pour la recomposition des clés GTK	Par défaut : aucun	Période de temps entre les modifications automatiques de la clé de groupe, partagée par tous les appareils du réseau.
Désactiver le pooling d'inactivité	Off | On ; Par défaut : Off	L'interrogation d'inactivité peut être désactivée pour déconnecter les stations en fonction du délai d'inactivité afin que les stations inactives soient plus susceptibles d'être déconnectées même si elles sont toujours à portée du point d'accès.
Limite d'inactivité de la station	Par défaut : aucun	Limite d'inactivité de la station en secondes. Si une station/client n'envoie rien dans le premier intervalle de temps, une trame de données vide lui est envoyée afin de vérifier si elle est toujours à portée. Si cette trame n'est pas acquittée, la station sera dissociée puis désauthentifiée.
Intervalle d'écoute maximal autorisé	Par défaut : aucun	L'association sera refusée si un client/station tente de s'associer avec un intervalle d'écoute supérieur à cette valeur.
Dissociation en cas d'acquittement faible	Off | On ; Par défaut : On	Autoriser le mode AP à déconnecter les stations/clients en fonction d'une condition d'accusé de réception faible.
WDS	Off | On ; Par défaut : Off	Un système de distribution sans fil (WDS) est un système qui permet l'interconnexion sans fil des points d'accès (AP) dans un réseau.

Sécurité WiFi

Champ	Valeur	Description
Cryptage	Pas de cryptage | WPA-PSK | WPA2-PSK | Mode mixte WPA-PSK/ WPA2-PSK | WPA3-SAE | Mode mixte WPA2-PSK/ WPA3-SAE | WPA-EAP | WPA2-EAP | DEVOIR | Mode mixte WPA2-EAP/ WPA3-EAP | WPA3-EAP ; Par défaut : WPA2-PSK	Le type de cryptage utilisé sur cette interface sans fil.
Avec tous les cryptages		
Chiffrer	Automobile | Force CCMP (AES) | Forcer TKIP | Forcer TKIP et CCMP (AES) ; Par défaut : Auto	Un algorithme pour effectuer le cryptage ou le déchiffrement.
Mode mixte WPA3-SAE, WPA2-PSK/WPA3-SAE		
Mot de passe	Par défaut : aucun	Une phrase secrète personnalisée utilisée pour l'authentification (au moins 8 caractères).
WPA-EAP, WPA2-EAP, mode mixte WPA2-EAP/WPA3-EAP, WPA3-EAP		
Serveur d'authentification Radius	Par défaut : aucun	Adresse IP du serveur d'authentification.
Radius-Authentication-Port	Par défaut : aucun	Le port par défaut du serveur est 1812.
Radius-Authentication-Secret	Par défaut : aucun	Secret partagé du serveur.
Radius-Accounting-Serveur	Par défaut : aucun	Adresse IP du serveur de comptabilité.
Radius-Comptabilité-Port	Par défaut : aucun	Le port par défaut du serveur est 1813.
Radius-Accounting-Secret	Par défaut : aucun	Secret partagé du serveur.
Identifiant NAS	Par défaut : aucun	Identifiant du serveur d'accès au réseau.

Filtre MAC

Champ	Valeur	Description
Filtre d'adresse MAC	Désactiver | N'autoriser que la liste | Autoriser toutes les exceptions listées ; Par défaut : Désactiver	Définit comment le filtre MAC doit fonctionner. • Autoriser uniquement la liste : autorise uniquement les appareils dotés d'adresses MAC spécifiées à se connecter à votre point d'accès sans fil. • Autoriser tous sauf ceux répertoriés : empêche les appareils dotés d'adresses MAC spécifiées de se connecter à votre point d'accès sans fil.
Liste MAC	MAC; Par défaut : aucun	Liste des adresses MAC à inclure ou à exclure de la connexion à votre point d'accès sans fil.
Supprimer de la liste blanche	désactivé | sur; par défaut : désactivé	Permet la suppression du MAC de la liste blanche lorsque l'appareil atteint le compteur de blocage IP.

Mode client

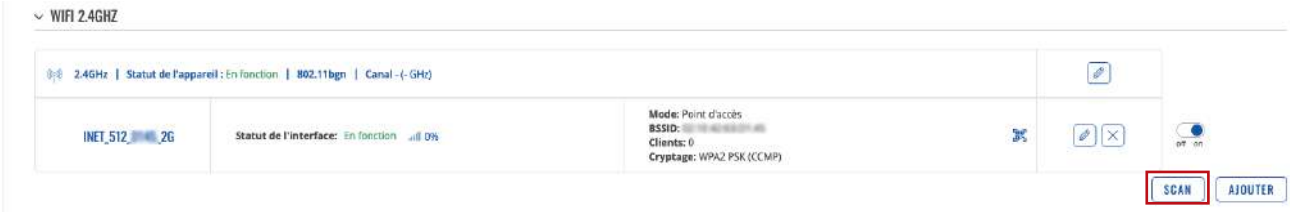
Un mode client sans fil (STA) est une interface créée par le routeur, utilisée pour se connecter à un point d'accès sans fils. (Ex: borne WiFi public)
Créer une station client est particulièrement utile pour économiser du forfait de données sur sa carte SIM à condition qu'un point d'accès WiFi public soit disponible.

NOTE : L'ajout d'une interface WiFi en mode client la rend automatiquement prioritaire sur toutes les autres interfaces (WAN et Mobile 4G). Ce mode est à utiliser lorsque l'on souhaite créer un répéteur Wi-Fi entre un point d'accès public et son pc, tablette, téléphone ou tout autre appareil connecté.

IMPORTANT : Le routeur I-NET 512 est doté d'un module intelligent scrutant l'accessibilité à Internet. Si l'interface Wi-Fi ajoutée devient inaccessible, le routeur bascule automatiquement à la prochaine connexion Internet disponible (WAN ou Mobile 5G).

Configuration du mode client

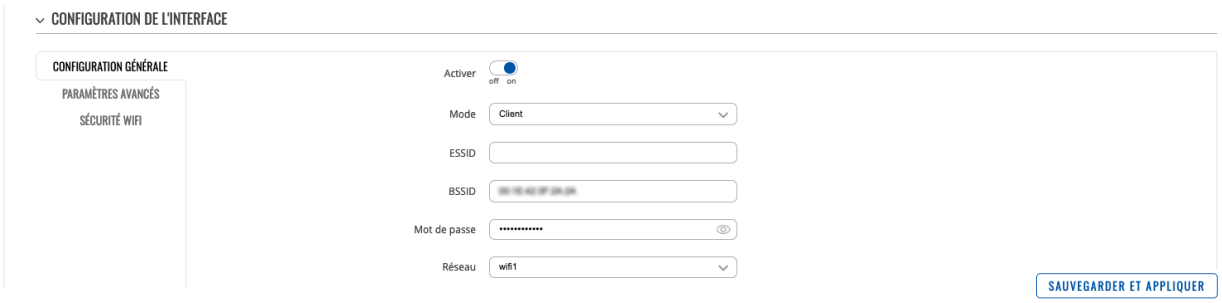
Cliquez sur le bouton "SCAN" pour analyser les réseaux WiFi présents dans la zone environnante.



La liste des points d'accès Wi-Fi disponibles s'affiche.
Cliquer sur le bouton « Rejoindre le réseau » du point d'accès Wi-Fi que vous souhaitez utiliser.

Vous devrez ensuite saisir le mot de passe WPA du point d'accès auquel vous souhaitez vous connecter. Nommez votre réseau (ce sera le nom de votre interface WAN Wi-Fi) et attribuez une zone de pare-feu (il est recommandé de conserver la zone attribuée par défaut).

S'ouvrira ensuite la fenêtre Configuration de l'interface. Les valeurs ici sont dictées par le point d'accès. Elles doivent rester inchangées afin d'éviter les problèmes de connexion.

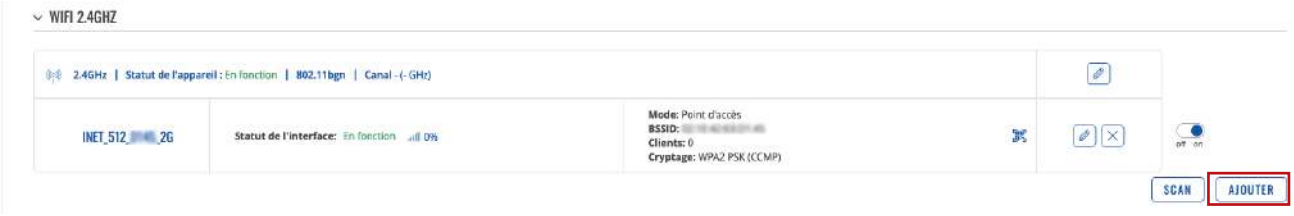


Validez en cliquant sur "Sauvegarder et appliquer" pour valider la configuration du mode client et ainsi se connecter au point d'accès public.

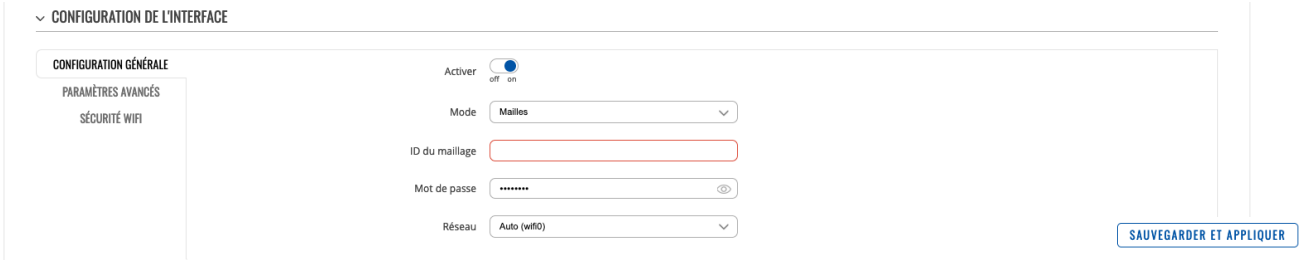
IMPORTANT : la configuration du mode client terminée, le réseau Wi-Fi du routeur est automatiquement réinitialisé. La connexion avec ce dernier est alors interrompu. Patienter durant cette opération qui peut durer jusqu'à 2 minutes. En fonction du navigateur Web utilisé, il peut être nécessaire de rafraîchir votre page WEB pour accéder à nouveau à l'interface WEB du routeur.

Mode maillage (ou MESH)

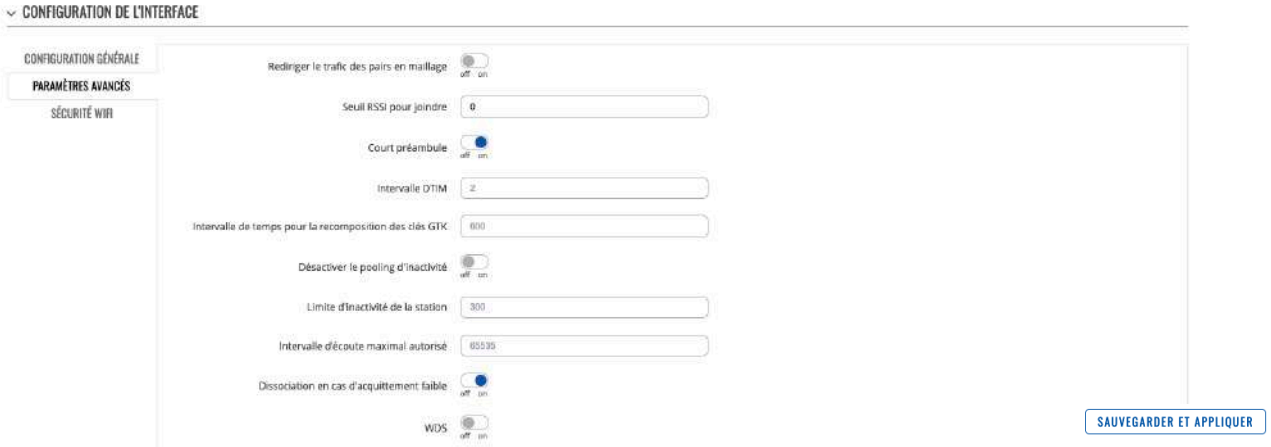
I-NET 512 peut également être configuré comme une passerelle maillée ou comme un nœud (routeur) se connectant à une passerelle maillée.
Lorsque I-NET 512 est configuré en tant que passerelle de maillage, il fournit un accès Internet à d'autres nœuds de maillage. Lorsqu'il est configuré en tant que nœud maillé, il agit comme un routeur maillé qui transfère le trafic vers et depuis la passerelle maillée. Les nœuds connectent également d'autres appareils sans fil au réseau, tels que des ordinateurs portables et des téléphones portables.
Lors de la configuration de I-NET 512 en tant que passerelle maillée, une connectivité Internet est requise.
Pour commencer, cliquez sur le bouton "Ajouter"



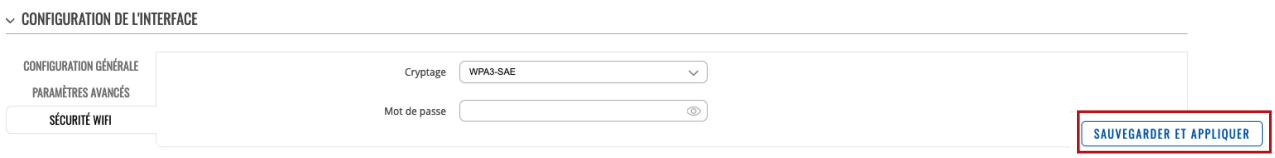
Dans l' onglet Configuration générale, sélectionnez le mode Maillé, définissez l'ID du maillage (ce numéro doit être le même dans tous les nœuds qui se connectent à ce réseau maillé sans fil) et sélectionnez le réseau souhaité qui sera attaché à l'interface. Cliquez sur Sauvegarder et appliquer.



Enfin, dans l'onglet Paramètres avancés, activez "**Rediriger le trafic des pairs en maillage**" et définissez le "Seuil RSSI pour joindre à -80". Laissez le reste tel qu'il est défini par défaut. Cliquez sur Enregistrer et appliquer. Si la configuration a été correctement effectuée la passerelle de maillage Wi-Fi sera fonctionnelle.



Accédez ensuite à l' onglet Sécurité Wi-Fi et sélectionnez le cryptage WPA3-SAE pour ajouter une couche d'authentification. Le mot de passe doit être le même dans tous les appareils du réseau maillé.



Nœud de maillage

Le nœud de maillage est configuré de la même manière que la passerelle de maillage. Le nœud doit correspondre à la configuration de l'interface de maillage Wi-Fi de la passerelle. De plus, l'interface LAN doit être configurée en tant que client DHCP :

1. Accédez à l'interface utilisateur Web du routeur via le menu Réseau → Interfaces.
2. Cliquez sur l'icône à droite de l'interface WAN.

3. Changez le protocole en DHCP.

Cliquez sur "**Sauvegarder et appliquer**". Si la configuration a été correctement effectuée, le mode de maillage sera fonctionnel.

Points d'accès multiples

Introduction:

La fonction "Multi AP" permet d'adresser un ensemble de réseaux Wi-Fi, regroupé sous une seule interface. Pour créer une interface sans fil Multi AP, cliquez sur le bouton « Ajouter » ci-dessous de l'interface sans fil.

Le routeur analyse en continu l'ensemble des réseaux Wi-Fi qui ont été renseignés, sélectionne le plus performant pour le mettre à disposition de l'utilisateur.
Comme pour la fonction "Service client", une interface Wi-Fi "Multi AP" est prioritaire sur les interface WAN et Mobile dans la liste des interfaces.
Cette fonction peut etre utilisée lorsque l'on souhaite créer un répéteur Wi-Fi entre son ordinateur n'importe quel réseau Wi-Fi renseigné dans le liste de la fonction "Muli AP", sans avoir à se soucier de l'état des différents réseaux Wi-Fi.

IMPORTANT : le routeur I-NET 512 est doté d'un module intelligent vérifiant l'accessibilité à internet via les différentes interfaces. Si une interface Wi-Fi créée devient inaccessible, le routeur bascule automatiquement sur la prochaine interface opérationnelle (WAN ou Mobile).

Paramètres généraux

Dans la section Paramètres généraux, activer la fonction Multi AP. Vous pouvez modifier la périodicité d'analyse de disponibilité des points d'accès Wi-Fi publics.

Champ	Valeur	Description
Activer	Off | On; Par défaut : Off	Active ou désactive la configuration Multi-AP d'accès.
Mode	Client | Point d'accès | Maille | Multi-AP ; Par défaut : Multi-AP	Définit le rôle que jouera cette interface, point d'accès pour fournir le WiFi à d'autres appareils, client pour utiliser d'autres appareils WiFi pour WWAN et Mesh pour agir comme passerelle de réseau maillé ou nœud dans un réseau maillé.
Temps de balayage (sec)	Par défaut : 60	Période (en secondes) de l'analyses de disponibilité des points d'accès Wi-Fi.
Charger la liste des AP	- (bouton interactif)	Télécharge une liste de configurations de points d'accès.

Points d'accès

Dans la section Point d'accès, saisir les différents point d'accès Wi-Fi public auquels vous souhaitez vous raccorder. Pour chaque point d'accès, cliquer sur le bouton AJOUTER et saisir identifiant (SSID) et mot de passe. A la fin de la saisie, cliquer le bouton SAUVEGARGER et APPLIQUER.

NOTE : Ne pas oublier d'activer chaque point d'accès en glissant le bouton de droite sur On.

Champ	Valeur	Description
SSID	Chaîne de caractères ; Par défaut : aucun	SSID d'un point d'accès.
Mot de passe	Chaîne de caractères ; Par défaut : aucun	Mot de passe, utilisé pour l'authentification de l'utilisateur (au moins 8 caractères).
Activer	Off | On; Par défaut : Off	Active ou désactive un point d'accès.
Supprimer	- (bouton interactif)	Supprime le point d'accès de la liste.

Il est possible de télécharger une liste de point d'accès renseignée dans un fichier, à l'aide du bouton RECHERCHER. Ci-dessous un exemple de format du fichier à saisir:
identifiant de connexion : INET_1
activer : 1
clé : 12345678
ssid : INET_2
activer : 0
clé : 87654321

NOTE : pour supprimer une interface "Multi AP" dans le menu WIFI, basculer en mode "Avancé" et cliquer sur le bouton avec la croix correspondant.

QR Codes WiFi

Chaque interface WiFi possède un QR code spécialement conçu qui contient des informations sur le SSID et le mot de passe du réseau WiFi. Après avoir appuyé sur le bouton de QR code WiFi manuel un QR code s'affiche avec le SSID et le mot de passe du réseau, que vous pouvez le télécharger localement en appuyant sur le bouton « Download QR code». Si vous souhaitez uniquement un code QR sans informations supplémentaires, décochez la case « Inclure les références ».

2.5 Menu Réseau > GESTION RÉSEAU

Le menu GESTION RÉSEAU permet de piloter les différentes interfaces réseaux du routeur à l'aide de modules distincts : **Gestion réseau** et **Répartition des données**.

Gestion réseau.

Le module **Gestion réseau** est un module intelligent vérifiant l'accessibilité à internet en continue sur les différentes interfaces présentes dans le tableau ci-dessous. Pour se faire, sur chaque interface réseau, une requête est envoyée à intervalle de temps régulier sur Internet dans l'attente d'une réponse.
Les interfaces réseau dont l'accessibilité à internet est opérationnelle sont renseignées avec le statut "En ligne". Dans le cas contraire, elle sont renseignées avec le statut "Interface arrêtée".

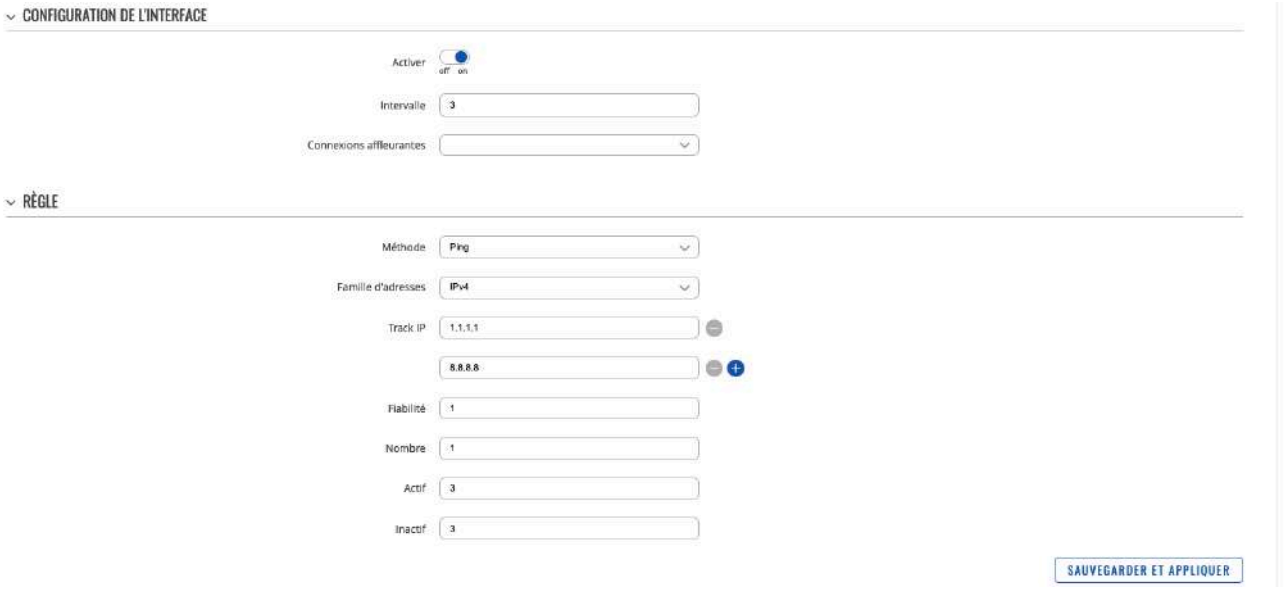
L'interface réseau utilisée pour vous donner l'accès à internet sera la première de la liste dont le statut est "En ligne".

Les interfaces réseaux sont classées dans un ordre de priorité définie dans la colonne de gauche. Celle dont le niveau de priorité est le plus élevé est celle située sur la première ligne du tableau.
Si besoin, il est possible de modifier le niveau de priorité de chaque interface réseau en cliquant et déplaçant le curseur de votre souris sur la croix, tout à gauche de chaque ligne.

Configuration de l'interface.

Un menu de configuration d'interface est utilisée pour configurer la façon dont le périphérique déterminera si une interface est en ligne ou hors ligne. Pour accéder à une page de configuration d'interface, cliquez sur le bouton "Modifier" à côté d'une interface.

Vous serez ensuite redirigé vers la page de configuration de cette interface.

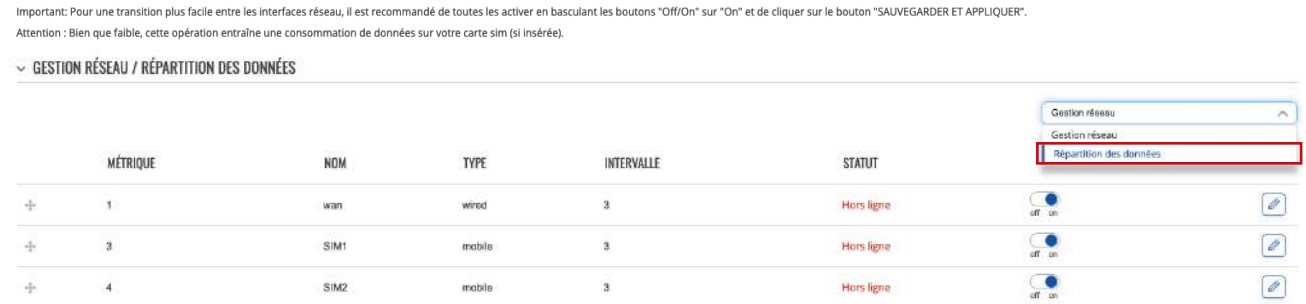


Champ	Valeur	Description
Activer	Off | On; Par défaut : On	Activez ou désactivez l'interface.
Intervalle	Par défaut : 3	Nombre de secondes entre chaque test
Connexions affleurantes	Connecté | Déconnecté : Par défaut : aucun	Vide les connexions établies après le scénario
Méthode	Par défaut : Ping	Définit comment la vérification de l'état sera effectuée sur cette interface lors de la détermination de son état.
Famille d'adresses	IPv4 | IPv6 Par défaut : IPV4	
Track IP	Par défaut : 1.1.1.1,8.8.8.8	Adresse(s) IP ou nom(s) d'hôte qui seront utilisés pour déterminer l'état d'une interface. Si l'appareil ne reçoit aucune réponse de l'un des hôtes spécifiés, l'interface sera considérée comme « hors ligne ». Si cette valeur est manquante, l'interface sera toujours considérée comme active.
Fiabilité	Par défaut : 1	Nombre d'hôtes qui doivent répondre pour que le test soit considéré comme réussi. Assurez-vous qu'il y a au moins ce nombre d'hôtes définis dans le champ 'Track IP', sinon l'interface sera toujours considérée comme 'Offline'.
Nombre	Par défaut : 1	Nombre de pings à envoyer à chaque hôte avec chaque test.
Actif	Par défaut : 3	Nombre de tests réussis requis pour considérer une interface comme 'En ligne'.
Inactif	Par défaut : 3	Nombre de tests échoués requis pour considérer une interface comme "Hors ligne".

Répartition des données

La répartition des données est un module de répartition du trafic entre plusieurs interfaces. La répartition des données peut être utilisée pour partager la charge de données entre différentes interfaces et augmenter le débit internet pour plusieurs utilisateurs et connexions. La charge n'augmente pas la vitesse pour une seule connexion. Cependant, l'équilibrage de données peut être utilisé pour augmenter la vitesse de plusieurs connexions.

NOTE : La répartition des données et la gestion réseau ne peuvent pas être utilisés en même temps. Si vous souhaitez sélectionner le module de Répartition des données, cliquer sur le menu déroulant situé dans le coin supérieur droit de la page :



Vous trouverez ci-dessous un exemple de la page Répartition des données.

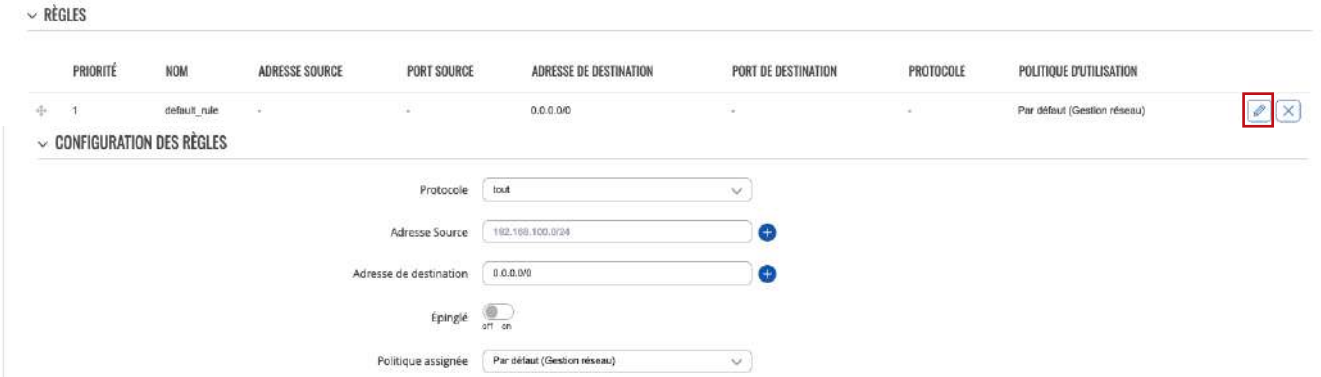
Lorsque la répartition des données est sélectionnée, vous pouvez attribuer des valeurs de ratios aux différentes interfaces. La valeur du ratio représente un pourcentage de la charge de trafic qui passera par une interface. Exemple, si vous configurez la colonne ratio comme ceci :

- Rapport WAN filaire : 3
- Rapport WAN mobile : 2

Environ 60 % (3/5) du trafic passerait par l'interface WAN filaire et environ 40 % (2/5) passerait par le WAN mobile. Dans ce cas, si vous lisiez 100 vidéos différentes sur Internet, environ 60 seraient lues via le WAN filaire et les 40 autres seraient lues via le WAN mobile.

Règles

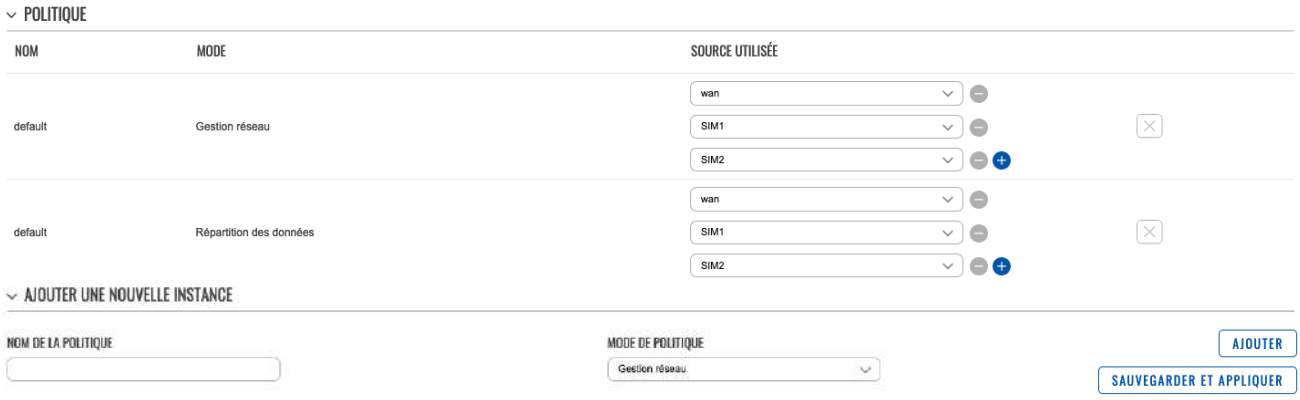
Une règle d'équilibrage de charge/de basculement est un ensemble de conditions qui définissent un certain type de trafic réseau.
Une règle par défaut est présente sur l'appareil. Vous pouvez ajouter plus de règles avec le bouton « Ajouter » ou vous pouvez personnaliser la règle existante en cliquant sur le bouton « Modifier » à côté :



Champ	Valeur	Description
Protocole	Tout | TCP | UDP | ICMP | ESP ; Par défaut : Tout	Protocole pour correspondre à cette règle.
Adresse source	IP/masque de réseau ; Par défaut : aucun	Adresses IP source pour correspondre à cette règle.
Adresse de destination	IP/masque de réseau ; Par défaut : 0.0.0.0/0	Adresses IP de destination correspondant à cette règle.
Épinglé	Off | On ; Par défaut : Off	Si cette option est activée, le trafic provenant de la même adresse IP source qui correspondait précédemment à cette règle dans le délai d'attente persistant utilisera la même interface WAN.
Délai d'attente	Valeur [1..1000000] ; Par défaut : aucun	Délai d'attente en secondes.
Politique assignée	Par défaut (Gestion réseau) | Par défaut (Répartition des données) | Inaccessible (Rejet) | Trou noir (saut) | Défaut (utiliser la table de routage principale) Par défaut : Par défaut (Gestion réseau)	Sélectionne la politique à appliquer au trafic qui correspond aux conditions de cette règle. Vous pouvez créer des politiques personnalisées de répartition des données/de gestion réseau dans la section ci-dessous.

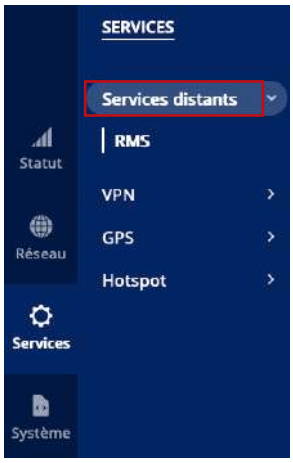
Politique

Une politique dicte ce que l'appareil doit faire lorsqu'une partie du trafic réseau correspond à la condition définie dans une règle de répartition des données/de gestion réseau. Vous pouvez créer des politiques personnalisées qui utilisent différentes interfaces pour la répartition des données/de gestion réseau.



Champ	Valeur	Description
Source utilisée	wan | SIM1 | SIM2 ; Par défaut : WAN	Pour qu'une interface réseau puisse être utilisée dans mwan3, elle doit être définie en tant que membre, qui peut ensuite être utilisée dans les stratégies.

3. Menu SERVICES



3.1 Menu SERVICES > SERVICES DISTANTS

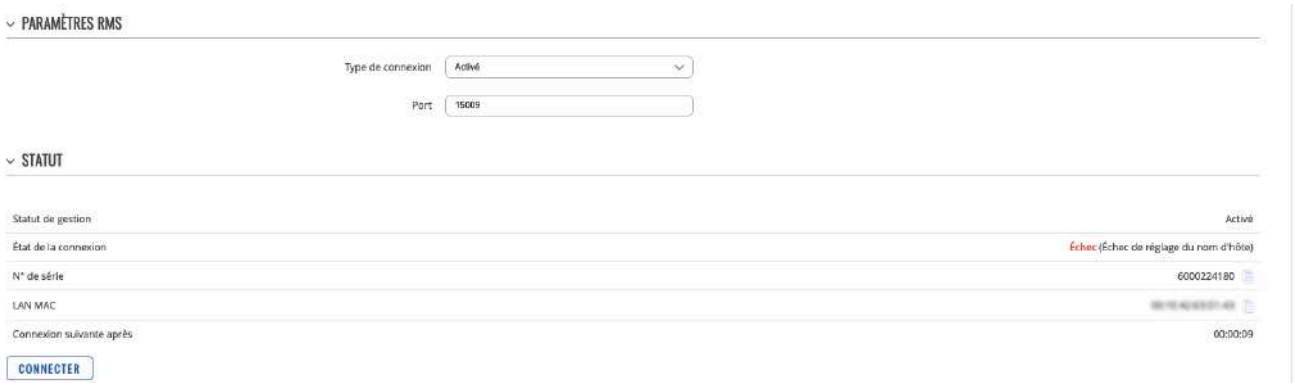
Le menu Services distants est utilisé pour configurer la manière dont l'appareil se connecte au système de Services distants, utilisé par le système de contrôle à distance.

3.1.1 Menu SERVICES > SERVICES DISTANTS > RMS

I-NET-512 intègre une solution reliée à un cloud, utilisée pour des services de gestion à distance tel que les mises à jour ou la maintenance**. Afin de garantir le bon fonctionnement de l'accès distant, les paramètres de ce menu ne doivent pas être modifiés.

**Services proposés par ALDEN sous conditions.

La figure ci-dessous est une capture d'écran de la section RMS :



Champ	Valeur	Description
Type de connexion	Par défaut : Activé	Définit comment l'appareil se connectera : • Activé – l'appareil tente de se connecter toutes les 2 à 5 minutes (toutes les 2 minutes la première heure, puis toutes les 5 minutes). S'il ne peut pas se connecter pendant 14 jours, il entrera en mode veille. • Veille – l'appareil tente de se connecter toutes les 6 heures. • Désactivé – La fonctionnalité est désactivée.
Port	Par défaut : 15009	Numéro de port pour la connexion., laissez le port par défaut (15009).

Le serveur RMS attend les connexions entrantes. Étant donné que l'appareil tente de se connecter à un intervalle fixe, il se peut qu'il ne se connecte pas instantanément. Pendant qu'il est déconnecté, vous pouvez vérifier la durée restante jusqu'à la prochaine tentative de connexion dans la section État :

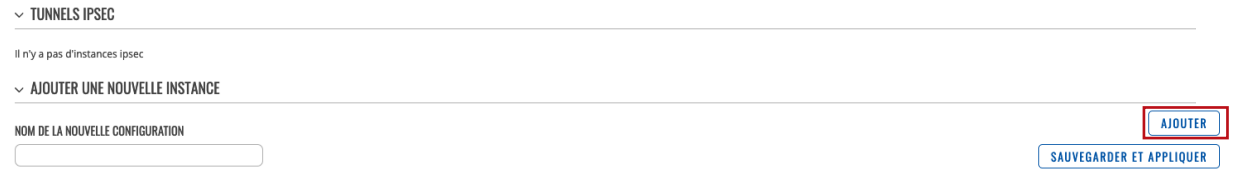
3.2 Menu SERVICES > VPN

Un réseau privé virtuel (VPN) est une méthode permettant de connecter plusieurs réseaux privés sur Internet. Les VPN peuvent servir à atteindre de nombreux objectifs différents, mais certains de leurs objectifs principaux sont les suivants :

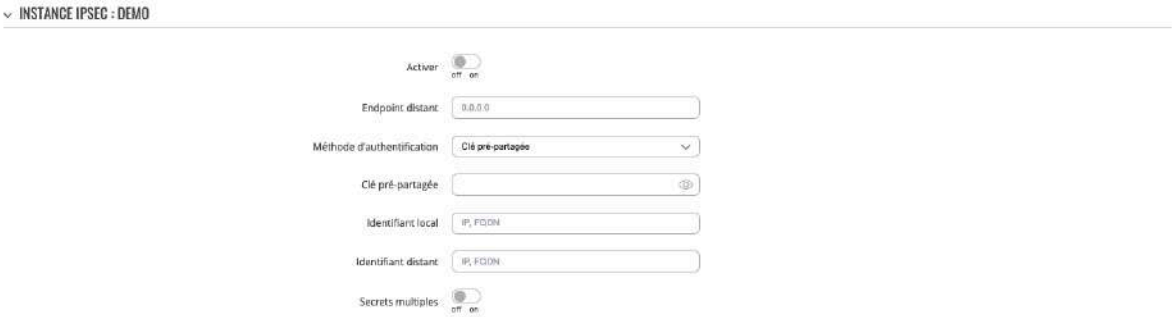
- accès entre réseaux privés distants ;
- cryptage des données ;
- l'anonymat lors de la navigation sur Internet.

3.2.1 Menu SERVICES > VPN > IPSEC

Pour créer une nouvelle instance IPsec, accédez à la section Services → VPN → IPsec , entrez un nom personnalisé et cliquez sur le bouton « Ajouter ». Une instance IPsec portant le nom donné apparaîtra dans la liste « Configuration IPsec ».



La section des paramètres généraux permet de configurer les principaux paramètres IPsec. Reportez-vous à la figure et au tableau ci-dessous pour plus d'informations sur les champs de configuration situés dans la section des paramètres généraux.



Champ	Valeur	Description
Activer	Off | On; Par défaut : Off	Active ou désactive l'instance IPsec.
Endpoint distant	Hôte | adresse IP ; par défaut : aucun	Adresse IP ou nom d'hôte de l'instance IPsec distante.
Méthode d'authentification	Clé pré-partagée | X.509 | EAP ; par défaut : clé pré-partagée	Spécifiez la méthode d'authentification. Choisissez entre la clé pré-partagée et les certificats X.509.
Clé pré-partagée : Clé pré-partagée	Par défaut : aucun	Mot de passe partagé utilisé pour l'authentification entre les homologues IPsec avant l'établissement d'un canal sécurisé.
X.509 | EAP : Clé	Un fichier de clé privée ; Par défaut : aucun	Un fichier de clé privée.
X.509 | EAP : Phrase secrète de décryptage de clé	Un mot de passe pour les fichiers de clé privée ; Par défaut : aucun	Si le fichier de clé privée est chiffré, la phrase secrète doit être définie.
X.509 | EAP : Certificat local	Fichier .der ; Par défaut : aucun	Fichier de certificat local.
X.509 | EAP : Certificat CA	Fichier .der ; Par défaut : aucun	Fichier d'autorité de certification.

Identifiant local	Adresse IP | chaîne; par défaut : aucun	Définit comment l'utilisateur (participant de gauche) sera identifié lors de l'authentification. • IP – Adresse de protocole Internet. • FQDN – identité définie par un Champscomplet. Il s'agit du Champscomplet d'un hôte (par exemple, quelque chose.somedomain.com). Uniquement pris en charge avec IKEv2.
Identifiant distant	Adresse IP | chaîne; par défaut : aucun	Définit comment le bon participant sera identifié lors de l'authentification. • IP – Adresse de protocole Internet. • FQDN – identité définie par un Champscomplet. Il s'agit du Champscomplet d'un hôte (par exemple, quelque chose.somedomain.com). Uniquement pris en charge avec IKEv2.
Secrets Multiples	Off | On; Par défaut : Off	Activez pour afficher la section Paramètres de secret global pour configurer plusieurs secrets.

Notes complémentaires :

Certains champs de configuration deviennent disponibles uniquement lorsque certains autres paramètres sont sélectionnés. Les noms des paramètres sont suivis d'un préfixe qui précise le type d'authentification sous lequel ils deviennent visibles. Différents codes couleurs sont utilisés pour différents préfixes :

- Vert pour la méthode d'authentification : clé pré-partagée
- Rouge foncé pour la méthode d'authentification : X.509/EAP

Paramètres généraux secrets

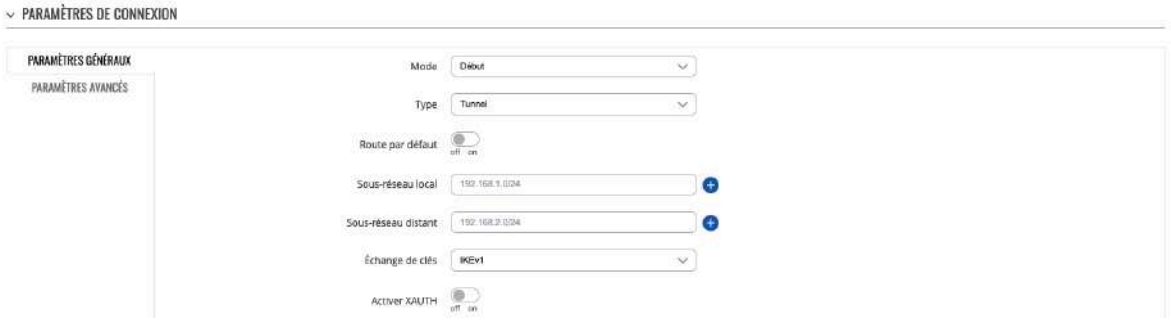
Cette section s'affiche lorsque Secrets multiples sont activés dans les paramètres généraux. Vous pouvez ajouter de nouvelles instances en appuyant sur Ajouter.

Champ	Valeur	Description
Sélecteur d'identification	%any, IP ou FQDN ; Par défaut : aucun	Chaque secret peut être précédé d'une liste de sélecteurs d'ID facultatifs. Un sélecteur est une adresse IP, un Champscomplet, un utilisateur@FQDN ou %any. Lorsque vous utilisez IKEv1, utilisez l'adresse IP. REMARQUE : IKEv1 prend uniquement en charge le sélecteur d'ID d'adresse IP.
Type	PSK | XAUTH | PAE | RSA | PKCS#12 ; Par défaut : PSK	Type de secret IPSec. REMARQUE : les secrets XAUTH sont uniquement IKEv1.
Secret	Par défaut : aucun	Mot de passe partagé pour s'authentifier entre les pairs. La longueur minimale est de 5 symboles. Tous les caractères sont autorisés sauf '.
RSA | PKCS#12 : Secret	Fichier de clé privée ; Par défaut : aucun	Fichier de clé privée.
RSA | PKCS#12 : Phrase secrète de déchiffrement de clé	Un mot de passe pour les fichiers de clé privée ; Par défaut : aucun	Si le fichier de clé privée est chiffré, la phrase secrète doit être définie.

Instance IPsec : paramètres de connexion

La section des paramètres de connexion permet de configurer les principaux paramètres d'une connexion IPsec. Reportez-vous à la figure et au tableau ci-dessous pour plus d'informations sur les champs de configuration situés dans la section des paramètres de connexion.

Paramètres généraux

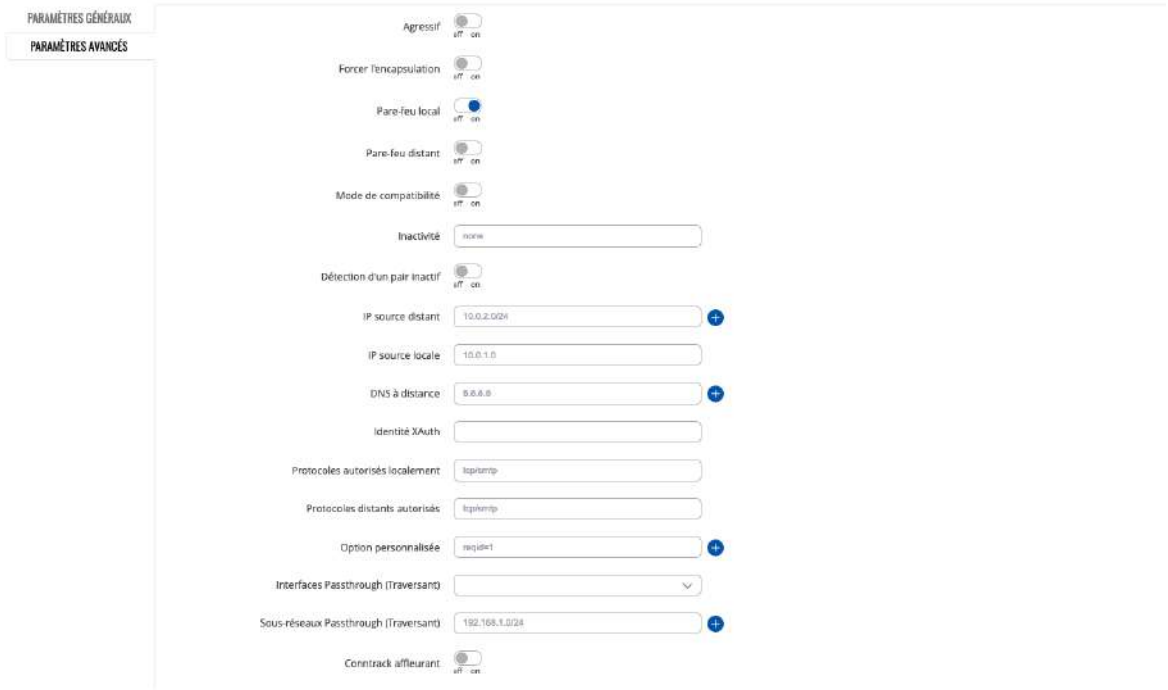


Champ	Valeur	Description
Mode	Début | Ajouter | Routage ; Par défaut : Début	Spécifie quelle opération sera effectuée automatiquement au démarrage d'IPSec.
Type	Tunnel | Transport ; Par défaut : Type	Type de connexion. • Tunnel : protège les informations de routage interne en encapsulant l'intégralité du paquet IP (en-tête IP et charge utile) ; couramment utilisé dans les connexions VPN de site à site ; prend en charge la traversée NAT. • Transport : encapsule uniquement les données utiles IP ; utilisé dans les connexions VPN client-site ; ne prend pas en charge la traversée NAT ; généralement implémenté avec d'autres protocoles de tunneling (par exemple, L2TP).
Tunnel : route par défaut	Off | On; Par défaut : Off	Activez cette option pour acheminer tout le trafic via le tunnel IPSec.
Tunnel : sous-réseau local	IP/masque de réseau | Par défaut : aucun	Adresse IP locale et masque de sous-réseau utilisés pour déterminer quelle partie du réseau est accessible dans le réseau VPN. Plage du masque de réseau [0..32]. Si elle est laissée vide, l'adresse IP sera sélectionnée automatiquement.
Tunnel : sous-réseau distant	IP/masque de réseau ; Par défaut : aucun	Adresse IP du réseau distant et masque de sous-réseau utilisés pour déterminer quelle partie du réseau est accessible dans le réseau VPN. Plage du masque de réseau [0..32]. Cette valeur doit différer de l'adresse IP LAN de l'appareil.
Transport : Lier à	Interface GRE ; Interface L2TP ; Par défaut : aucun	Liez-vous à l'interface GRE ou L2TP pour créer GRE/L2TP sur IPsec.
Échange de clés	IKEv1 | IKEv2 ; Par défaut : IKEv1	Version Internet Key Exchange (IKE) utilisée pour l'échange de clés. • IKEv1 – plus couramment utilisé mais contient des problèmes connus, par exemple liés au NAT. • IKEv2 – version mise à jour avec des fonctionnalités accrues et améliorées, telles que la prise en charge NAT intégrée, le multihébergement pris en charge, les modes d'échange obsolètes (n'utilise pas le mode principal ou agressif ; seulement 4 messages requis pour établir une connexion).
Activer XAuth	Off | On; Par défaut : Off	Active l'authentification étendue.

Notes complémentaires :
Certains champs de configuration deviennent disponibles uniquement lorsque certains autres paramètres sont sélectionnés. Les noms des paramètres sont suivis d'un préfixe qui précise le type d'authentification sous lequel ils deviennent visibles. Différents codes couleurs sont utilisés pour différents préfixes :

- Rouge pour le type : Tunnel
- Bleu pour le type : Transport

Paramètres avancés

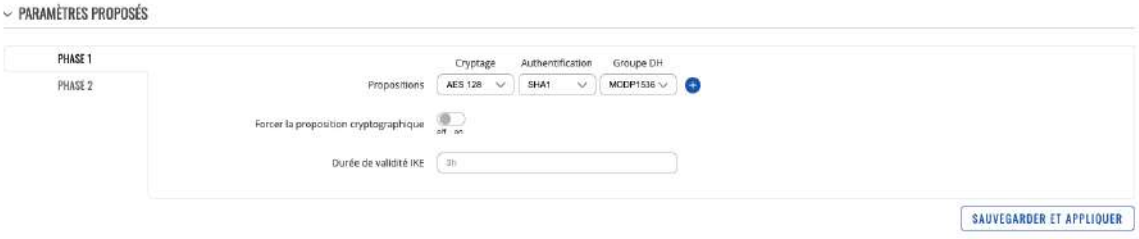


Champ	Valeur	Description
Agressif	Off | On ; Par défaut : Off	Activez ou désactivez le mode agressif pour les connexions sortantes. Le mode agressif effectue moins d'échanges (un total de 4 messages) que le mode principal (un total de 6 messages) en stockant la plupart des données dans le premier échange. En mode agressif, les informations sont échangées avant qu'il n'existe un canal sécurisé, ce qui le rend moins sécurisé mais plus rapide que le mode principal.
Forcer l'encapsulation	Off | On ; Par défaut : Off	Force l'encapsulation UDP pour les paquets ESP même si une situation « pas de NAT » est détectée.
Pare-feu local	Off | On ; Par défaut : On	Ajoute les règles de pare-feu nécessaires pour autoriser le trafic de cette instance IPsec sur cet appareil.
Pare-feu distant	Off | On ; Par défaut : On	Ajoute les règles de pare-feu nécessaires pour autoriser le trafic provenant de l'instance IPsec opposée sur cet appareil.
Mode de compatibilité	Off | On ; Par défaut : Off	Active le mode de compatibilité pour faciliter la gestion d'un homologue distant tiers avec plusieurs sous-réseaux.
Inactivité	Par défaut : aucun	Définit un intervalle de délai d'attente, après lequel un CHILD_SA est fermé s'il n'a envoyé ou reçu aucun trafic.
Détection d'un pair inactif	Off | On ; Par défaut : Off	Fonction utilisée lors de l'échange de clés Internet (IKE) pour détecter un homologue « mort ». Il réduisait le trafic en minimisant le nombre de messages lorsque l'homologue opposé n'était pas disponible et servait de mécanisme de basculement.

Détection d'un pair inactif : action DPD	Redémarrer | En attente | Effacer | Aucun; Par défaut : Redémarrer	Contrôle l'utilisation du protocole Dead Peer Detection où des messages de notification sont périodiquement envoyés afin de vérifier la vivacité du homologue IPsec.
Détection d'un pair inactif : Retard DPD	Par défaut : aucun	Fréquence d'envoi de messages R_U_THERE ou d'échanges INFORMATIONNELS à un homologue.
Détection d'un pair inactif : expiration du délai DPD	Par défaut : aucun	Définit l'intervalle de délai d'attente après lequel toutes les connexions à un homologue sont supprimées en cas d'inactivité.
Identité XAuth	Par défaut : aucun	L'identité/nom d'utilisateur que le client utilise pour répondre à une requête XAuth. Si elle n'est pas définie, l'identité IKEv1 sera utilisée comme identité XAuth.
Tunnel : IP source distante	Adresse IP ; Par défaut : aucun	L'adresse IP source interne à utiliser dans un tunnel pour le homologue distant (droit).
Tunnel : IP source locale	Adresse IP ; Par défaut : aucun	L'adresse IP source interne (à gauche) à utiliser dans un tunnel, également appelée IP virtuelle.
Tunnel : DNS à distance	Adresse IP ; Par défaut : aucun	Liste des adresses de serveurs DNS à échanger comme attributs de configuration. Sur le répondeur, seules les adresses IPv4/IPv6 fixes sont autorisées et définissent les serveurs DNS attribués au client.
Protocoles autorisés localement	Par défaut : aucun	Protocoles et ports autorisés sur la connexion, également appelés sélecteurs de ports. Définit sous forme de « protocole/port », par exemple : « 17/1701 » ou « 17/%any » ou « udp/l2f ».
Protocoles distants autorisés	Par défaut : aucun	Protocoles et ports autorisés sur la connexion, également appelés sélecteurs de ports. Définit sous forme de « protocole/port », par exemple : « 17/1701 » ou « 17/%any » ou « udp/l2f ».
Option personnalisée	Par défaut : aucun	Ajoutez des paramètres de connexion personnalisés.
Interfaces Passthrough (Traversant)	Adresse IP ; Par défaut : aucun	L'adresse IP source interne (à gauche) à utiliser dans un tunnel, également appelée IP virtuelle.
Tunnel : interfaces de passage	Interfaces réseau; Par défaut : aucun	Interfaces réseau à inclure dans IPsec Passthrough.
Tunnel : Sous-réseaux Passthrough (Traversant)	IP/masque de réseau ; Par défaut : aucun	Réseaux à inclure dans IPsec Passthr

Notes complémentaires :

• Certains champs de configuration deviennent disponibles uniquement lorsque certains autres paramètres sont sélectionnés. Les noms des paramètres sont suivis d'un préfixe qui précise le type d'authentification sous lequel ils deviennent visibles. Différents codes couleurs sont utilisés pour différents préfixes :
• Rouge pour le type : Tunnel
• Bleu pour la Détection d'un pair inactif : activé



3.2.2 Menu SERVICES > VPN > OPENVPN

OPENVPN > Serveur

OpenVPN est une application logicielle open-source qui met en œuvre des techniques de réseau privé virtuel (VPN) pour créer des connexions sécurisées de point à point ou de site à site dans des configurations routées ou pontées ainsi que des installations d'accès distant. Il est souvent considéré comme le protocole VPN le plus universel en raison de sa flexibilité, de son support de la sécurité SSL/TLS, de ses multiples méthodes de chiffrement, de ses nombreuses fonctionnalités réseau et de sa compatibilité avec la plupart des plates-formes OS.

Champ	Valeur	Description
Activer	Off | On ; Par défaut : Off	Active ou désactive l'instance OpenVPN.
Activer la configuration d'OpenVPN à partir d'un fichier	Off | On ; Par défaut : Off	Active ou désactive la configuration OpenVPN personnalisée à partir d'un fichier.

TUN/TAP	TUN (tunnel) | TAP (ponté); Par défaut : TUN (tunnel)	Type de périphérique réseau virtuel. TUN – un lien IP virtuel point à point qui fonctionne au niveau réseau (couche OSI 3), utilisé lorsque le routage est nécessaire. TAP – un adaptateur Ethernet virtuel (commutateur) qui fonctionne au niveau liaison de données (couche OSI 2), utilisé lorsque le pontage est nécessaire.
Protocole	UDP | TCP | UDP6 | TCP6; Par défaut : UDP	UDP (User Datagram Protocol) – Protocole de transfert utilisé par la connexion OpenVPN. Transmission Control Protocol (TCP) – Protocole le plus couramment utilisé dans la suite de protocoles Internet (IP). Il garantit que le destinataire recevra les paquets dans l'ordre où ils ont été envoyés en les numérotant, en analysant les messages de réponse, en vérifiant les erreurs et en les renvoyant en cas de problème. Il doit être utilisé lorsque la fiabilité est cruciale (par exemple, le transfert de fichiers). User Datagram Protocol (UDP) – Les paquets sont envoyés au destinataire sans vérification d'erreur ni contrôle qualité aller-retour, ce qui signifie que lorsque des paquets sont perdus, ils sont perdus pour toujours. Cela le rend moins fiable mais plus rapide que TCP ; par conséquent, il doit être utilisé lorsque la vitesse de transfert est cruciale (par exemple, le streaming vidéo, les appels en direct).
Port	Par défaut : 1194	Numéro de port TCP/UDP utilisé pour la connexion. Assurez-vous qu'il correspond au numéro de port spécifié du côté du serveur. REMARQUE : le trafic sur le port sélectionné sera automatiquement autorisé dans les règles du pare-feu de l'appareil.
LZO	Oui | Non | Aucun ; Par défaut : Aucun	Active ou désactive la compression de données LZO.
Authentication	Clé statique | TLS | TLS/Mot de passe | Mot de passe ; Par défaut : TLS	Mode d'authentification, utilisé pour sécuriser les sessions de données. La clé statique est une clé secrète utilisée pour l'authentification serveur-client. Le mode d'authentification TLS utilise des certificats de type X.509 : Autorité de Certification (AC) Certificat client Clé client Tous les certificats mentionnés peuvent être générés à l'aide des utilitaires OpenVPN ou Open SSL sur n'importe quel type de machine hôte. L'un des utilitaires les plus populaires utilisés à cette fin s'appelle Easy-RSA. TLS/Mot de passe utilise à la fois TLS et l'authentification par nom d'utilisateur/mot de passe.

Cryptage	DES-CBC 64 | RC2-CBC 128 | DES-EDE-CBC 128 | DES-EDE3-CBC 192 | DESX-CBC 192 | BF-CBC 128 | RC2-40-CBC 40 | CAST5-CBC 128 | RC2-64CBC 64 | AES-128-CBC 128 | AES-128-CFB 128 | AES-128-CFB1 128 | AES-128-CFB8 128 | AES-128-OFB 128 | AES-128-GCM 128 | AES-192-CBC 192 | AES-192-CFB 192 | AES-192-CFB1 192 | AES-192-CFB8 192 | AES-192-OFB 192 | AES-192-GCM 192 | AES-256-CBC 256 | AES-256-CFB 256 | AES-256-CFB1 256 | AES-256-CFB8 256 | AES-256-OFB 256 | AES-256-GCM 256 | none; default: AES-256-CBC 256	Algorithme utilisé pour le chiffrement des paquets.
Clé statique : IP de l'extrémité du tunnel local	Par défaut : Aucun	Adresse IP de l'interface réseau OpenVPN locale.
Clé statique : IP endpoint du tunnel distant	Par défaut : Aucun	Adresse IP de l'interface réseau OpenVPN distante (client).
Clé statique : Adresse IP du réseau distant	Par défaut : Aucun	Adresse IP LAN du réseau distant (client).
Clé statique : Masque de sous-réseau distant	Personnalisé | 255.255.255.0 | 255.255.0.0 | 255.0.0.0 Par défaut : Aucun	Masque de sous-réseau IP LAN du réseau distant (client).
Clé statique : Authentifizierungsalgorithmus	MD5 | SHA1 (Par défaut) | SHA256 | SHA384 | SHA512 Par défaut : Aucun	Algorithme utilisé pour l'échange d'informations d'authentification et de hachage.
TLS | TLS/Mot de passe | Mot de passe : Chiffrement TLS	Tout | DHE+RSA | Personnalisé ; Par défaut : tout	Algorithme de chiffrement des paquets.
TLS | TLS/Mot de passe | Mot de passe : Client à client	Off | On ; Par défaut : Off	Permet aux clients OpenVPN de communiquer entre eux sur le réseau VPN.
TLS | TLS/Mot de passe | Mot de passe : Maintenir actif	Deux entiers séparés par un espace ; Par défaut : Aucun	Définit deux intervalles de temps : le premier est utilisé pour envoyer périodiquement des requêtes ICMP au serveur OpenVPN, le deuxième définit une fenêtre temporelle, qui est utilisée pour redémarrer le service OpenVPN si aucune réponse ICMP n'est reçue pendant la tranche horaire spécifiée. Lorsque cette valeur est spécifiée sur le serveur OpenVPN, elle remplace les valeurs de 'Maintenir actif' définies sur les instances clienteles. Exemple : 10 120

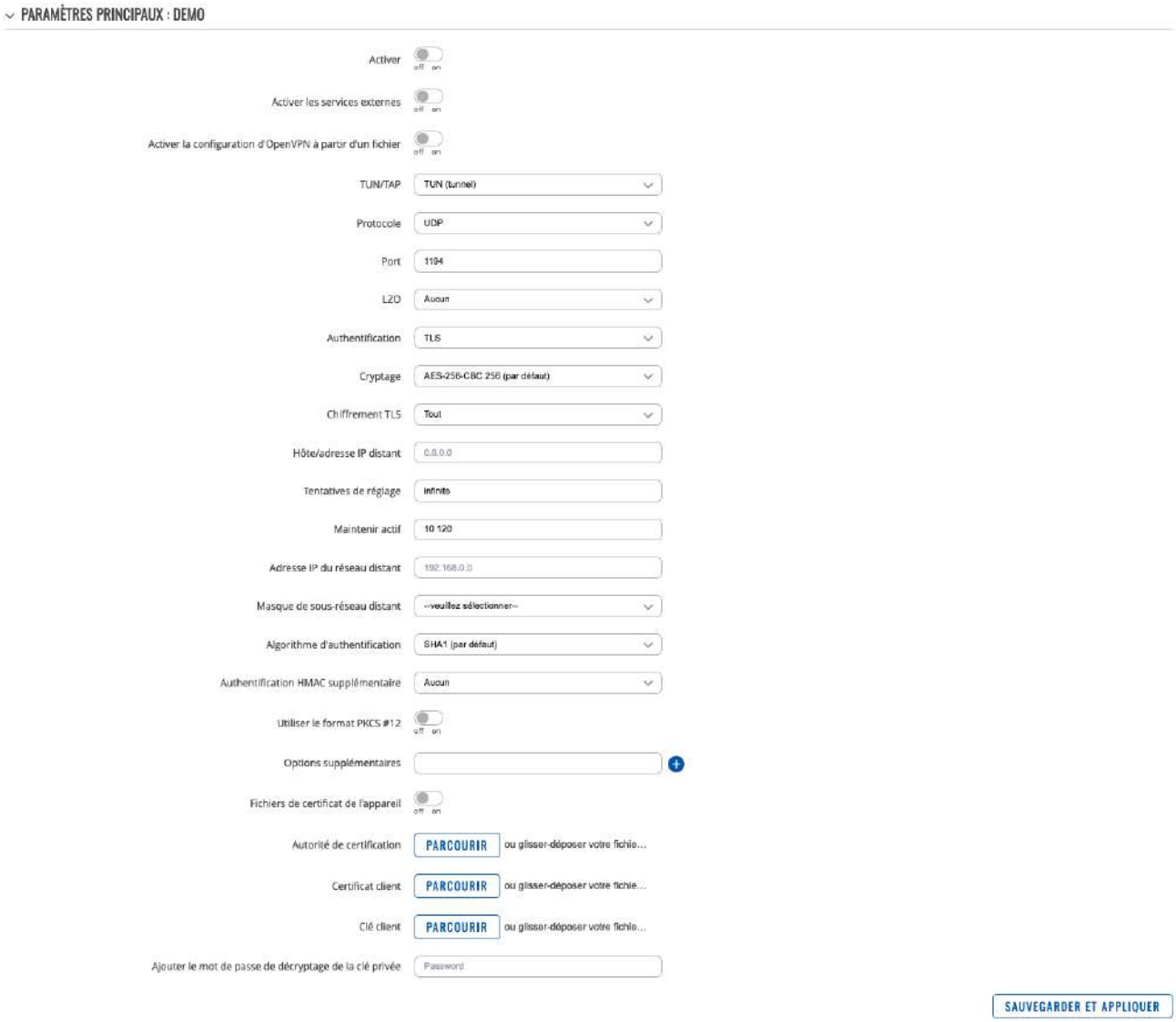
TLS | TLS/Mot de passe | Mot de passe : Adresse IP du réseau virtuel	Par défaut : Aucun	Adresse IPv4 du réseau OpenVPN.
TLS | TLS/Mot de passe | Mot de passe : Masque de sous-réseau virtuel	Personnalisé | 255.255.255.0 | 255.255.0.0 | 255.0.0.0 Par défaut : Aucun	Masque de sous-réseau du réseau OpenVPN.
TLS | TLS/Mot de passe | Mot de passe : Option Push	OpenVPN options; Par défaut : Aucun	Les options de poussée (Push options) sont une manière de "pousser" des routes et d'autres options supplémentaires d'OpenVPN aux clients connectés.
TLS | TLS/Mot de passe | Mot de passe : Autoriser les certificats en double	Off | On ; Par défaut : Off	Activée, elle permet à plusieurs clients de se connecter en utilisant les mêmes certificats.
TLS | Mot de passe : Noms d'utilisateurs et mots de passe	Bouton interactif – Parcourir	Nom d'utilisateur utilisé pour l'authentification auprès de ce serveur OpenVPN.
TLS | Mot de passe : Mot de passe	Par défaut : Aucun	Mot de passe utilisé pour l'authentification auprès de ce serveur OpenVPN.
Clé statique: Clé pré-partagée statique	Bouton interactif – Parcourir	Télécharge un fichier de clé secrète utilisé pour l'authentification serveur-client.
TLS | TLS/Mot de passe | Mot de passe : Autorité de certification	Bouton interactif – Parcourir	Une autorité de certification est une entité qui délivre des certificats numériques. Un certificat numérique certifie la propriété d'une clé publique par le sujet nommé dans le certificat.
TLS | TLS/Mot de passe | Mot de passe : Certificat du serveur	Bouton interactif – Parcourir	Un type de certificat numérique utilisé pour identifier le serveur OpenVPN.
TLS | TLS/Mot de passe | Mot de passe : Clé du serveur	Bouton interactif – Parcourir	Authentifie les clients auprès du serveur.
TLS | TLS/Mot de passe | Mot de passe :Paramètres Diffie Hellman	Bouton interactif – Parcourir	Les paramètres DH définissent la manière dont OpenSSL effectue l'échange de clés Diffie-Hellman (DH).
TLS | TLS/Mot de passe | Mot de passe : Fichier CRL (facultatif)	Bouton interactif – Parcourir	Un fichier de liste de révocation de certificats (CRL) est une liste de certificats qui ont été révoqués par l'autorité de certification (CA). Il indique quels certificats ne sont plus acceptés par la CA et, par conséquent, ne peuvent pas être authentifiés auprès du serveur.

Certain champs de configuration deviennent disponibles uniquement lorsque certains autres paramètres sont sélectionnés. Les noms des paramètres sont suivis d'un préfixe qui spécifie le type d'authentification sous lequel ils deviennent visibles. Différents codes couleur sont utilisés pour différents préfixes.

Après avoir modifié l'un des paramètres, n'oubliez pas de cliquer sur le bouton Enregistrer et Appliquer situé en bas à droite de la page.

OPENVPN > Client

Un client OpenVPN est une entité qui initie une connexion à un serveur OpenVPN. Pour créer une nouvelle instance client, allez dans la section Services → VPN → OpenVPN, sélectionnez le rôle : Client, saisissez un nom personnalisé et cliquez sur le bouton 'Ajouter'. Une instance client OpenVPN avec le nom donné apparaîtra dans la liste "Configuration OpenVPN".
Pour commencer la configuration, cliquez sur le bouton qui ressemble à un crayon à côté de l'instance client. Référez-vous à la figure et au tableau ci-dessous pour des informations sur les champs de configuration du client OpenVPN :



Champ	Valeur	Description
Activer	Off | On ; Par défaut : Off	Active ou désactive l'instance OpenVPN.
Activer les services externes	Off | On ; Par défaut : Off	Active ou désactive les services externes OpenVPN.
Fournisseurs VPN	Express VPN | Nord VPN ; Par défaut : Nord VPN	Représente une liste de fournisseurs de VPN disponibles
Serveurs VPN	Royaume-Uni | USA | Australie | Afrique du Sud | Personnalisé ; Par défaut : Royaume-Uni	Représente une liste de serveurs VPN disponibles.
Nom d'utilisateur	Par défaut : Aucun	Nom d'utilisateur utilisé pour l'authentification auprès du serveur VPN.

Mot de passe	Par défaut : Aucun	Mot de passe utilisé pour l'authentification auprès du serveur VPN.
Activer la configuration d'OpenVPN à partir d'un fichier	Off | On ; Par défaut : Off	Active ou désactive la configuration personnalisée d'OpenVPN à partir d'un fichier.
Fichier de configuration OpenVPN	Bouton interactif – Parcourir	Télécharger la configuration OpenVPN. Attention ! Cela écrasera votre configuration actuelle.
Upload OpenVPN authentications files	Off | On ; Par défaut : Off	Téléchargez les fichiers d'authentification OpenVPN, qui seront automatiquement inclus dans la configuration.
TUN/TAP	TUN (tunnel) | TAP (Ponté); Par défaut : TUN (tunnel)	Type de dispositif réseau virtuel. TUN – un lien IP virtuel point-à-point qui fonctionne au niveau réseau (couche OSI 3), utilisé lorsque le routage est nécessaire. TAP – un adaptateur Ethernet virtuel (commutateur) qui fonctionne au niveau liaison de données (couche OSI 2), utilisé lorsque le pontage est nécessaire.
Protocole	UDP | TCP | UDP6 | TCP6; Par défaut : UDP	Protocole de transfert utilisé par la connexion OpenVPN. Protocole de contrôle de transmission (TCP) – le protocole le plus couramment utilisé dans la suite de protocoles Internet (IP). Il garantit que le destinataire recevra les paquets dans l'ordre où ils ont été envoyés en les numérotant, en analysant les messages de réponse, en vérifiant les erreurs et en les renvoyant en cas de problème. Il devrait être utilisé lorsque la fiabilité est cruciale (par exemple, dans le transfert de fichiers). Protocole de datagramme utilisateur (UDP) – les paquets sont envoyés au destinataire sans vérification d'erreur ou de contrôle de qualité en aller-retour, ce qui signifie que lorsque des paquets sont perdus, ils sont perdus pour toujours. Cela le rend moins fiable mais plus rapide que TCP ; par conséquent, il devrait être utilisé lorsque la vitesse de transfert est cruciale (par exemple, dans la diffusion vidéo, les appels en direct).
Port	Par défaut : 1194	Numéro de port TCP/UDP utilisé pour la connexion. Assurez-vous qu'il correspond au numéro de port spécifié du côté du serveur. REMARQUE : le trafic sur le port sélectionné sera automatiquement autorisé dans les règles du pare-feu de l'appareil.
LZO	Oui | Non | Aucun ; Par défaut : Aucun	Active ou désactive la compression de données LZO.

Authentication	Clé statique | TLS | TLS/Mot de passe | Mot de passe ; Par défaut : TLS	Mode d'authentification, utilisé pour sécuriser les sessions de données. • La clé statique est une clé secrète utilisée pour l'authentification serveur-client. • Le mode d'authentification TLS utilise des certificats de type X.509 : – Autorité de certification (CA) – Certificat client – Clé client Tous les certificats mentionnés peuvent être générés à l'aide des utilitaires OpenVPN ou Open SSL sur n'importe quel type de machine hôte. L'un des utilitaires les plus populaires utilisés à cette fin est appelé Easy-RSA. – Le **mot de passe** est une authentification simple basée sur un nom d'utilisateur et un mot de passe où le propriétaire du serveur OpenVPN fournit les données de connexion. – **TLS/Mot de passe** utilise à la fois TLS et l'authentification par nom d'utilisateur/mot de passe.
Cryptage	DES-CBC 64 | RC2-CBC 128 | DES-EDE-CBC 128 | DES-EDE3-CBC 192 | DESX-CBC 192 | BF-CBC 128 | RC2-40-CBC 40 | CAST5-CBC 128 | RC2-64CBC 64 | AES-128-CBC 128 | AES-128-CFB 128 | AES-128-CFB1 128 | AES-128-CFB8 128 | AES-128-OFB 128 | AES-128-GCM 128 | AES-192-CBC 192 | AES-192-CFB 192 | AES-192-CFB1 192 | AES-192-CFB8 192 | AES-192-OFB 192 | AES-192-GCM 192 | AES-256-CBC 256 | AES-256-CFB 256 | AES-256-CFB1 256 | AES-256-CFB8 256 | AES-256-OFB 256 | AES-256-GCM 256 | aucun ; Par défaut : AES-256-CBC 256	Algorithme utilisé pour le chiffrement des paquets.
TLS | TLS/Mot de passe : Chiffrement TLS	Tout | DHE+RSA | Personnalisé ; Par défaut : tout	Algorithme de chiffrement des paquets.
TLS | TLS/Mot de passe : Chiffrement TLS autorisés	Par défaut : Aucun	Liste des algorithmes de chiffrement TLS acceptés par cette connexion.
Hôte/adresse IP distant	Par défaut : Aucun	Adresse IP ou nom d'hôte d'un serveur OpenVPN.
Tentatives de réglage	Infinite; Par défaut : infinite	En cas d'échec de la résolution du nom d'hôte du serveur, ce champ indique la durée (en secondes) avant de réessayer la résolution. Spécifiez "infinite" pour réessayer indéfiniment.

Maintenir actif	Deux entiers séparés par un espace ; Par défaut : Aucun	Définit deux intervalles de temps : le premier est utilisé pour envoyer périodiquement des requêtes ICMP au serveur OpenVPN, le second définit une fenêtre de temps, qui est utilisée pour redémarrer le service OpenVPN si aucune réponse ICMP n'est reçue pendant la tranche de temps spécifiée. Lorsque cette valeur est spécifiée sur le serveur OpenVPN, elle remplace les valeurs de "Maintenir actif" définies sur les instances clientes. Exemple : 10 120
Clé statique : IP de l'extrémité du tunnel local	Par défaut : Aucun	Adresse IP de l'interface réseau OpenVPN locale.
Clé statique : IP endpoint du tunnel distant	Par défaut : Aucun	Adresse IP de l'interface réseau OpenVPN distante (client).
Adresse IP du réseau distant	Par défaut : Aucun	Adresse IP LAN du réseau distant (client).
Masque de sous-réseau distant	Personnalisé | 255.255.255.0 | 255.255.0.0 | 255.0.0.0 Par défaut : Aucun	Masque de sous-réseau IP LAN du réseau distant (client).
Algorithme d'authentification	MD5 | SHA1 (Par défaut) | SHA256 | SHA384 | SHA512 Par défaut : Aucun	Algorithme utilisé pour l'échange d'informations d'authentification et de hachage.
TLS | TLS/Mot de passe | Mot de passe : Authentification HMAC supplémentaire	Off | On ; Par défaut : Off	Couche supplémentaire d'authentification HMAC au-dessus du canal de contrôle TLS pour se protéger contre les attaques par déni de service (DoS).
TLS | TLS/Mot de passe | Mot de passe : Clé d'authentification HMAC	Bouton interactif – Parcourir	Télécharge un fichier de clé d'authentification HMAC.
TLS | TLS/Mot de passe | Mot de passe : Direction de la clé HMAC	0 | 1 | aucun ; Par défaut : 1	La valeur du paramètre de direction de clé doit être complémentaire des deux côtés (client et serveur) de la connexion. Si un côté utilise 0, l'autre côté doit utiliser 1, ou les deux côtés doivent omettre le paramètre entièrement.
Utiliser le format PKCS #12	Off | On ; Par défaut : Off	Activer ou désactiver le format PKCS #12.
TLS/Mot de passe | Mot de passe : Nom d'utilisateur	Par défaut : Aucun	Nom d'utilisateur utilisé pour l'authentification auprès du serveur OpenVPN.
TLS/Mot de passe | Mot de passe : Mot de passe	Par défaut : Aucun	Mot de passe utilisé pour l'authentification auprès du serveur OpenVPN.
Options supplémentaires	Par défaut : Aucun	Options supplémentaires OpenVPN à utiliser par l'instance OpenVPN.
TLS | TLS/Mot de passe | Mot de passe : Fichiers de certificat de l'appareil	Off | On ; Par défaut : Off	Activez cette option si vous souhaitez sélectionner les fichiers de certificat générés à partir du périphérique.
TLS | TLS/Mot de passe | Mot de passe : Autorité de certification	Bouton interactif – Parcourir	L'autorité de certification est une entité qui délivre des certificats numériques. Un certificat numérique atteste la propriété d'une clé publique par le sujet nommé dans le certificat.
TLS | TLS/Mot de passe : Certificat client	Bouton interactif – Parcourir	Le certificat client est un type de certificat numérique utilisé par les systèmes clients pour effectuer des requêtes authentifiées auprès d'un serveur distant. Les certificats clients jouent un rôle clé dans de nombreux designs d'authentification mutuelle, fournissant des garanties solides quant à l'identité du demandeur.

TLS | TLS/Mot de passe : Clé client	Bouton interactif – Parcourir	Authentifie le client auprès du serveur et établit précisément qui il est.
TLS | TLS/Mot de passe : Ajouter le mot de passe de décryptage de la clé privée	Par défaut : Aucun	Mot de passe utilisé pour décrypter la clé privée du serveur. À utiliser uniquement si le fichier .key du serveur est crypté avec un mot de passe.
Clé statique : Clé pré-partagée statique	Bouton interactif – Parcourir	Télécharge un fichier de clé secrète utilisé pour l'authentification entre le serveur et le client.

Certain champs de configuration deviennent disponibles uniquement lorsque certains autres paramètres sont sélectionnés. Les noms des paramètres sont suivis d'un préfixe qui spécifie le type d'authentification sous lequel ils deviennent visibles. Différents codes couleur sont utilisés pour différents préfixes.

Après avoir modifié l'un des paramètres, n'oubliez pas de cliquer sur le bouton Enregistrer et Appliquer situé en bas à droite de la page.

3.2.3 Menu SERVICES > VPN > WireGuard

WireGuard est un VPN simple, rapide, léger et moderne qui utilise une cryptographie sécurisée et éprouvée. Il vise à être plus performant qu'OpenVPN. WireGuard est conçu comme un VPN polyvalent, adapté à de nombreuses situations différentes, et bien qu'il soit actuellement en développement intensif, il pourrait déjà être considéré comme la solution VPN la plus sécurisée, la plus facile à utiliser et la plus simple.

WireGuard fonctionne en ajoutant une interface qui agit comme un tunnel. Pour en créer un, entrez son nom et cliquez sur le bouton Ajouter. Cela devrait ajouter une nouvelle instance de Wireguard et ouvrir une fenêtre de configuration.

Interface WireGuard > Configuration générale

Cette section contient les paramètres généraux de l'instance WireGuard créée. Vous pouvez y trouver ses clés publique et privée et les générer, spécifier le port et les adresses IP pour la communication.

Champ	Valeur	Description
Activer	Off | On ; Par défaut : Off	Active ou désactive l'instance WireGuard.
Clé privée	Par défaut : Aucun	Clé privée utilisée dans l'authentification.
Clé publique	Par défaut : Aucun	Clé publique utilisée dans l'authentification.
Générer une clé de pair	Bouton interactif – Générer	Cliquez pour générer la clé publique et la clé privée.
Adresses IP	Par défaut : Aucun	Une adresse IP unique ou une liste d'adresses IP pour cette instance associée à des clés publiques.

Interface WireGuard > Paramètres avancés

La section des paramètres avancés contient la configuration des métriques et de l'unité de transmission maximale (MTU) pour cette interface WireGuard.

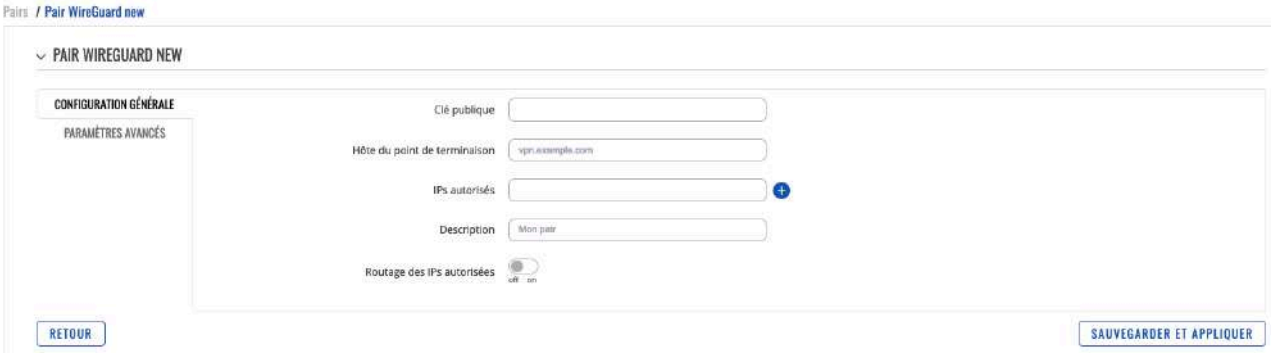
Champ	Valeur	Description
Métrique	Par défaut : Aucun	Spécifiez la métrique pour cette interface de tunnel. Un nombre plus bas signifie une priorité plus élevée.
MTU	Par défaut : Aucun	Unité de transmission maximale pour cette interface de tunnel.
Serveurs DNS	Par défaut : Aucun	Serveur(s) DNS pour cette interface WireGuard.

Interface WireGuard > Pairs

La section "Pairs" est utilisée pour créer et configurer tous les pairs pour cette interface. Pour en créer un, saisissez son nom et cliquez sur le bouton "Ajouter". Pour le configurer, cliquez sur le bouton "Modifier"

Pairs > Configuration générale

Dans la section "Configuration Général" de l'instance "Pairs", vous pouvez configurer des informations de base sur le point de terminaison pour permettre les communications.



Champ	Valeur	Description
Clé publique	Par défaut : Aucun	Clé publique du point de terminaison.
IPs autorisés	Par défaut : Aucun	Une seule adresse IP ou une liste d'adresses IP qui sont autorisées à communiquer avec ce pair.
Description	Par défaut : Aucun	Description du pair.
Routage des IPs autorisées	Off | On ; Par défaut : Off	Activer pour créer des routes pour les adresses IP autorisées pour ce pair.

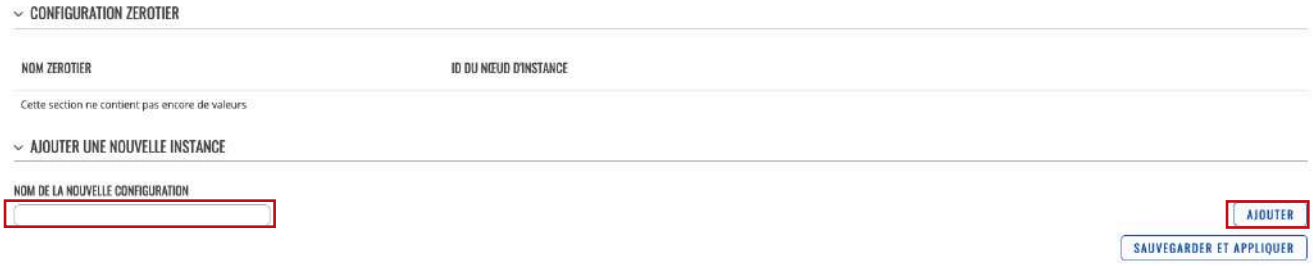
Pairs > Paramètres avancés

Dans la section "Paramètres avancés" de l'instance "Pairs", vous pouvez configurer des paramètres supplémentaires tels que sa description, l'hôte et le port du point de terminaison, la clé pré-partagée, et d'autres. Voir plus d'informations ci-dessous.

Champ	Valeur	Description
Clé pré-partagée	Par défaut : Aucun	Clé pré-partagée encodée en Base64. Ajoute une couche supplémentaire de cryptographie à clé symétrique pour une résistance post-quantique.
Port d'extrémité	Par défaut : Aucun	Spécifiez le port auquel se connecter au point de terminaison distant. Il sera défini sur 51820 s'il est laissé vide.
Actif persistant	Par défaut : Aucun	Adresse IP ou URL du point de terminaison distant.
Table de routage	Par défaut : Aucun	Activer pour créer des routes pour les adresses IP autorisées pour ce pair.

3.2.4 Menu SERVICES > VPN > ZeroTier

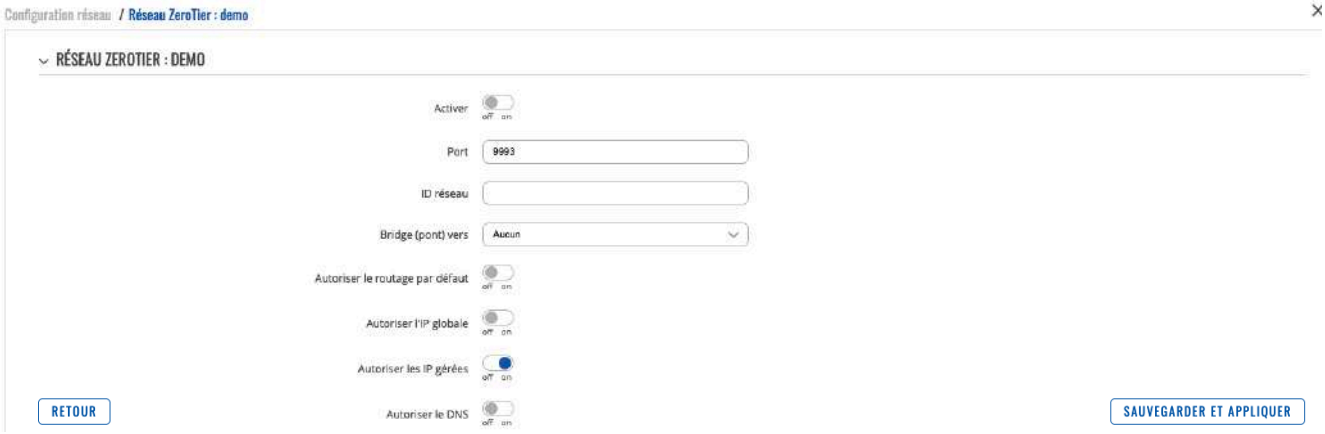
ZeroTier One est un logiciel open source qui peut établir une connexion VPN peer-to-peer (P2PVPN) entre différents appareils exécutant différents systèmes d'exploitation. Il offre également des possibilités de gestion de réseau telles que le routage et la création de règles de pare-feu.
Pour créer une nouvelle instance ZeroTier, recherchez la section "Ajouter une nouvelle instance"; saisissez un nom personnalisé et cliquez sur le bouton 'Ajouter'.



Vous devriez être redirigé vers la page de configuration de la nouvelle instance ZeroTier qui devrait ressembler à ceci :

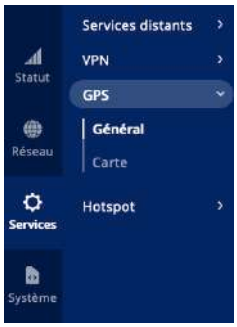
Champ	Valeur	Description
Activer	Off | On ; Par défaut : Off	Active ou désactive l'instance ZeroTier.

L'instance de configuration du réseau ZeroTier devrait ressembler à ceci :



Champ	Valeur	Description
Activer	Off | On ; Par défaut : Off	Active ou désactive l'instance ZeroTier.
Port	Integer [0..65535]; default: 9993	
ID réseau	Par défaut : Aucun	ID du réseau ZeroTier. Connectez-vous à votre compte ZeroTier pour localiser l'ID du réseau ZeroTier, qui devrait être une chaîne de caractères hexadécimaux.

Bridge (pont) vers	Aucun | LAN Par défaut : Aucun	Spécifiez à quelle interface cette instance ZeroTier doit être pontée.
Autoriser le routage par défaut	Off | On ; Par défaut : Off	Autorise ZeroTier à remplacer la route par défaut du système.
Autoriser l'IP globale	Off | On ; Par défaut : Off	Autorise les adresses IP et les routes gérées par ZeroTier à chevaucher l'espace IP public.
Autoriser les IP gérées	Off | On ; Par défaut : On	Attribue les adresses IP et les routes gérées par ZeroTier
Autoriser le DNS	Off | On ; Par défaut : Off	Applique les serveurs DNS qui sont définis au niveau du contrôleur réseau.



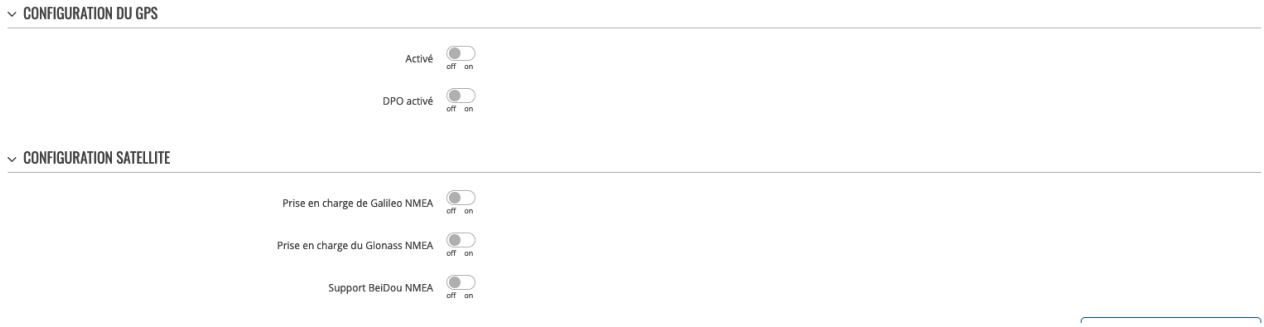
3.3 Menu SERVICES > GPS

Le système de positionnement global (GPS) est un système de radionavigation spatial. Cette page est un aperçu du service GPS.

3.3.1 Menu SERVICES > GPS > Général

Le Général est utilisé pour activer le service GPS et la prise en charge de différents types de satellites. Une fois que vous avez activé le GPS, vous pouvez consulter la page Carte afin de voir si l'appareil a obtenu une position GPS. Il est très important de fixer l'antenne GPS sur l'appareil et de la placer à l'extérieur (pas à l'intérieur d'un bâtiment). Autrement, l'appareil ne sera pas susceptible d'obtenir une position GPS.

La figure ci-dessous est un exemple de la page Général et le tableau ci-dessous fournit des informations sur les champs contenus dans cette page :

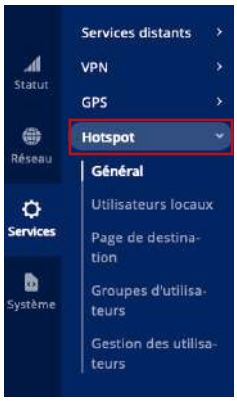


Champ	Valeur	Description
Activé	Off | On; Par défaut : Off	Active ou désactive le service GPS.
DPO activé	Off | On; Par défaut : Off	Activer l'optimisation dynamique de l'alimentation (nécessite le redémarrage du modem). Cette fonction n'est pas prise en charge sur les appareils équipés de modems Meig ou de modem Quectel BG95
Prise en charge Galileo NMEA *	Off | On; Par défaut : Off	Active ou désactive la prise en charge des satellites Galileo.
Prise en charge Glonass NMEA *	Off | On; Par défaut : Off	Active ou désactive la prise en charge des satellites Glonass.
Prise en charge BeiDou NMEA *	Off | On; Par défaut : Off	Active ou désactive la prise en charge des satellites BeiDou.

* La modification de ces options nécessite un redémarrage du modem. Par conséquent, si vous modifiez ces options et les enregistrez, l'appareil perdra la connectivité cellulaire pendant environ 30 secondes.

3.3.2 Menu SERVICES > GPS > Carte

La page Carte affiche les coordonnées et la position actuelles de l'appareil sur la carte. Pour voir l'emplacement de l'appareil sur la carte, assurez-vous de fixer l'antenne GPS sur l'appareil et d'activer le GPS sur la page Général .
La figure ci-dessous est un exemple de la page Carte :



3.4 Menu SERVICES > HOTSPOT

Un Hotspot est un service qui fournit l'authentification, l'autorisation et la comptabilité d'un réseau.

3.4.1 Menu SERVICES > HOTSPOT > Général

Instances HOTSPOT

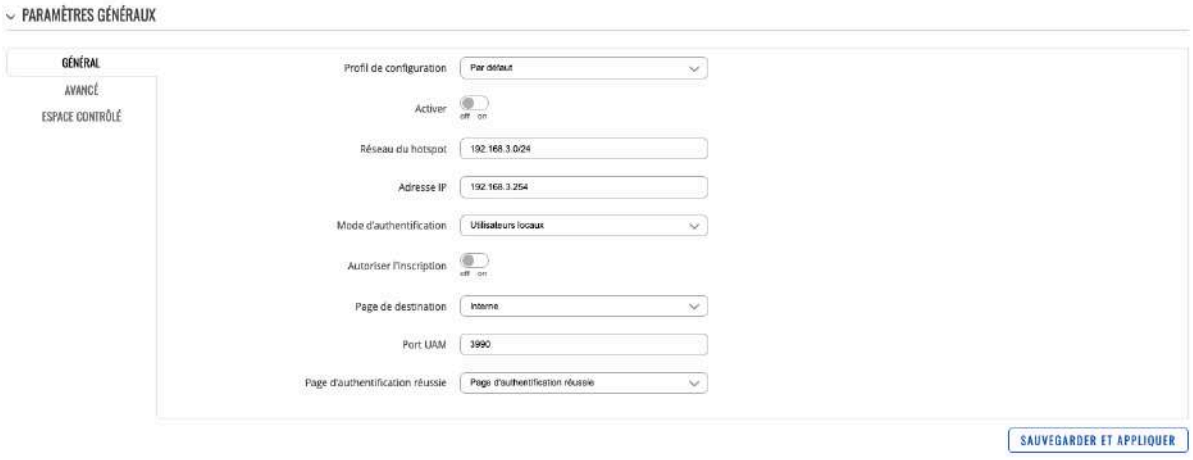
La section Instances Hotspot affiche les principaux paramètres de votre Hotspot. Par défaut, une instance Hotspot n'existe pas sur l'appareil. Pour créer une nouvelle instance et commencer la configuration :

1. Sélectionnez une « Interface » ;
2. Cliquez sur le bouton « Ajouter » ;

Après cela, une nouvelle fenêtre de configuration du Hotspot apparaîtra.

Paramètres généraux : mode général

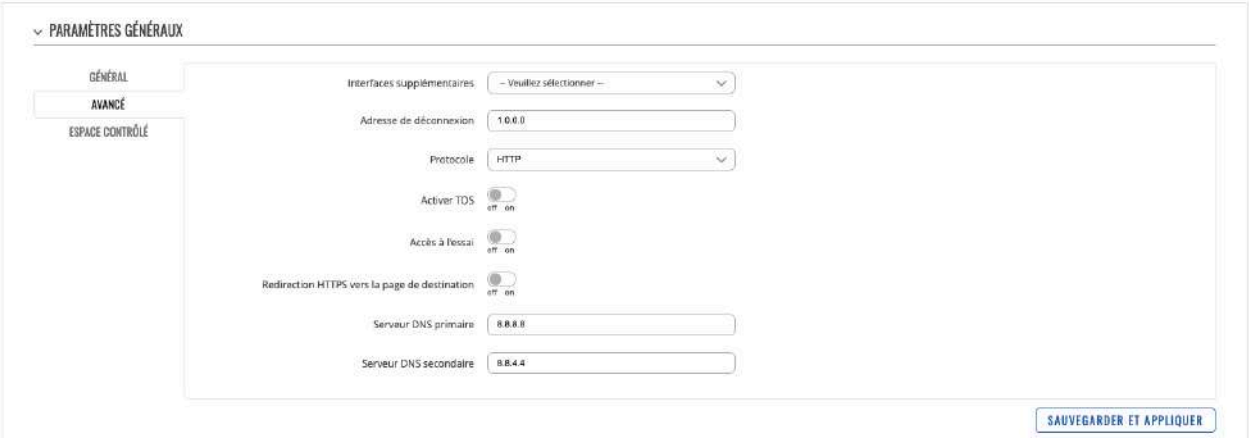
La fenêtre Paramètres généraux est l'endroit où s'effectue la majeure partie de la configuration du point d'accès. Consultez les sous-sections ci-dessous pour obtenir des informations sur les champs de configuration trouvés dans les sections Paramètres généraux.



Champ	Valeur	Description
Profil de configuration	Cloud4wi | Par défaut | Systèmes de hotspot ; Par défaut : Par défaut	Préconfigure les paramètres du point d'accès en fonction du fournisseur de services sélectionné.
Activer	Off | On; Par défaut : On	Active ou désactive l'instance Hotspot.

Réseau du hotspot	IP/masque de réseau ; Par défaut : 192.168.3.0/24	Adresse IP et sous-réseau du réseau Hotspot.
Adresse IP	Adresse IP ; Par défaut : 192.168.3.254	Définit l'adresse IP de votre routeur Hotspot en réseau.
Mode d'authentification	Utilisateurs locaux | Radius | SMS OTP ; Par défaut : utilisateurs locaux	Le mode d'authentification définit la manière dont les utilisateurs se connecteront au Hotspot.
Autoriser l'inscription	Off | On; Par défaut : Off	Permet aux utilisateurs de s'inscrire au hotspot via la page de destination.
Temps d'expiration	Entier; Par défaut : 0	Délai d'expiration des identifiants utilisateur. S'applique aux utilisateurs qui se sont inscrits via la page de destination.
Groupe d'utilisateurs	Groupe d'utilisateurs ; Par défaut : par défaut	Groupe d'utilisateurs auquel les utilisateurs se sont inscrits via la page de destination doivent être attribués.
Page de destination	Interne | Externe ; Par défaut : Interne	Si une page de destination externe est choisie, une nouvelle section apparaîtra pour saisir l'adresse du site Web, par exemple http://www.example.com
Port UAM	Par défaut : 3990	Port à lier pour authentifier les clients.
Secret UAM	Par défaut : aucun	Secret partagé entre uamserver et hotspot.
Page d'authentification réussie	Page d'authentification réussie | URL d'origine | Personnalisé ; Par défaut : Page d'authentification réussie	Emplacement vers lequel revenir après une authentification réussie.

Paramètres généraux : mode avancé

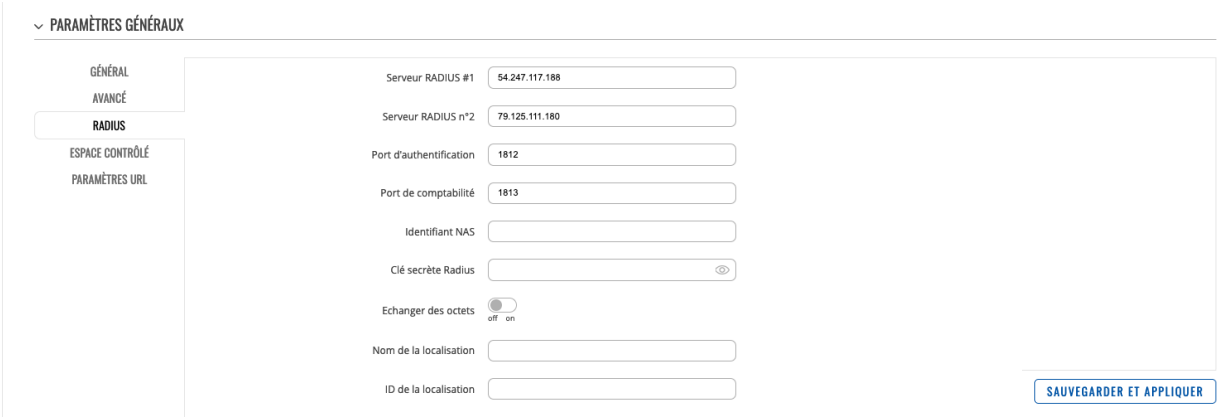


Champ	Valeur	Description
Interfaces supplémentaires	Interfaces disponibles ; Par défaut : aucun	Affiche les interfaces supplémentaires qui peuvent être attachées à l'instance de point d'accès.
Adresse de déconnexion	Adresse IP ; Par défaut : 1.0.0.0	Une adresse qui peut être utilisée par les utilisateurs pour se déconnecter de la session Hotspot.
Protocole	HTTP | HTTPS ; Par défaut : HTTP	Protocole à utiliser pour la page de destination.

Activer TOS	Off | On ; Par défaut : Off	Active les exigences de conditions de service (ToS). L'appareil client ne pourra accéder à Internet qu'après avoir accepté les ToS.
Accès à l'essai	Off | On ; Par défaut : Off	Permet un accès Internet d'essai pour un groupe spécifique.
Accès essai : Groupe	Groupe d'utilisateurs ; Par défaut : par défaut	Specifie le groupe d'utilisateurs d'essai.
Redirection HTTPS vers la page de destination	Off | On; Par défaut : Off	Redirigez les requêtes HTTPS initiales de la page de destination préalable vers la page de destination du point d'accès.
Fichiers de certificat de l'appareil	Off | On; Par défaut : Off	Spécifié s'il faut télécharger les fichiers de clé et de certificat depuis l'ordinateur ou utiliser les fichiers générés sur cet appareil via la page Système → Administration.
Fichier de clé SSL	Fichier clé; Par défaut : aucun	Téléchargez/sélectionnez la clé SSL.
Fichier de certificat SSL	Fichier de certificat ; Par défaut : aucun	Téléchargez/sélectionnez le certificat SSL.
Serveur DNS primaire	Adresse IP ; Par défaut : 8.8.8.8	Serveurs DNS supplémentaires qui doivent être utilisés par le Hotspot.
Serveur DNS secondaire	Adresse IP ; Par défaut : 8.8.4.4	Serveurs DNS supplémentaires qui doivent être utilisés par le Hotspot.

Paramètres généraux : mode radius

Le mode d'authentification Radius utilise un serveur RADIUS externe, auquel vous devez fournir une adresse, au lieu d'utiliser l'authentification locale du routeur. Cette section est visible quand le profil Cloud4wi ou Systèmes de hotspot est séléctionné dans le Profil de configuration dans le menu Général.



Champ	Valeur	Description
Serveur RADIUS #1	ip; Par défaut : aucun	L'adresse IP du serveur RADIUS n°1 à utiliser pour authentifier vos clients sans fil.
Serveur RADIUS n°2	ip; Par défaut : aucun	L'adresse IP du serveur RADIUS n°2 à utiliser pour authentifier vos clients sans fil.
Port d'authentification	Par défaut : 1812	Le port d'authentification du serveur RADIUS.
Port de comptabilité	Par défaut : 1813	Le port de comptabilité du serveur RADIUS.
Identifiant NAS	Par défaut : aucun	NAS-Identifier" est l'un des attributs RADIUS de base.

Clé secrète Radius	Par défaut :aucun	La clé secrète est un mot de passe utilisé pour l'authentification avec le serveur RADIUS.
Echanger des octets	Off | On; Par défaut : Off	Échange le sens des octets d'entrée et de sortie en ce qui concerne les attributs RADIUS.
Nom de la localisation	Par défaut : aucun	Nom personnalisé de l'emplacement pour votre hotspot.
ID de la localisation	Par défaut : aucun	Identifiant personnalisé de l'emplacement pour votre hotspot.

Paramètres généraux : Espace contrôlé

Vous pouvez ajouter une liste d'adresses auxquelles les utilisateurs connectés au hotspot pourront accéder sans aucune authentification. Par défaut, cette liste est vide. Il vous suffit d'écrire les adresses dans la liste d'adresses

Paramètres généraux : Paramètres URL

La section des Paramètres d'URL devient visible lorsque le Profil de configuration: Cloud4wi ou Systèmes de hotspot est sélectionné dans la section des paramètres généraux.

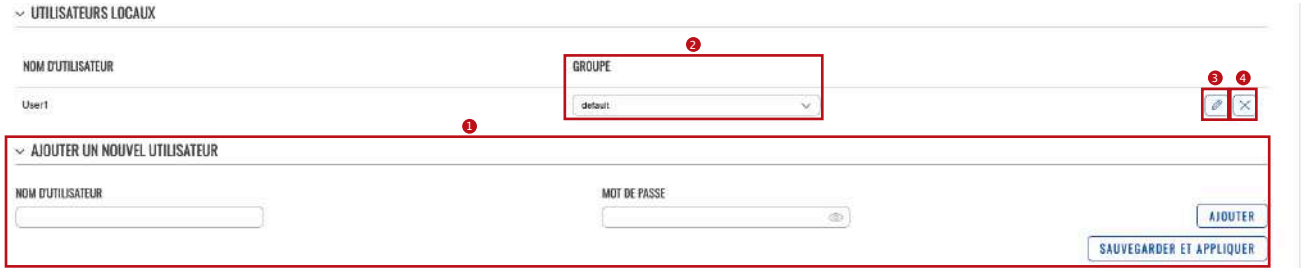
Champ	Valeur	Description
UAM IP	Par défaut : aucun	L'adresse IP de la passerelle du portail captif.
Port UAM	Par défaut : aucun	Le port sur lequel le portail captif servira le contenu web.
Appelé	Par défaut : aucun	L'adresse MAC de l'adresse IP de la passerelle du portail captif.
MAC	Par défaut : aucun	L'adresse MAC du client qui tente d'accéder à Internet.
IP	Par défaut : aucun	Identification pour le portail captif utilisé dans la requête RADIUS
Identifiant NAS	Par défaut : aucun	Identification pour le portail captif utilisé dans la requête RADIUS
Id session	Par défaut : aucun	L'identifiant unique de la session.
URL de l'utilisateur	Par défaut : aucun	L'URL que l'utilisateur a tenté d'accéder avant d'être redirigé vers les pages d'URL du portail captif.

Défi	Par défaut : aucun	Défi qui devrait être utilisé avec le mot de passe de l'utilisateur pour créer une phrase chiffrée utilisée pour se connecter.
Personnalisation 1	Par défaut : aucun	Ajoutez un nom personnalisé et une valeur personnalisée qui seront affichés dans les paramètres d'URL.
–	SSID | Nom d'hôte | Version FW ; Par défaut : SSID	–
Personnalisation 2	Par défaut : aucun	Ajoutez un nom personnalisé et une valeur personnalisée qui seront affichés dans les paramètres d'URL.
–	SSID | Nom d'hôte | Version FW ; Par défaut : SSID	–

3.4.2 Menu SERVICES > HOTSPOT > Utilisateurs locaux

La section des Utilisateurs Locaux est utilisée pour créer et gérer les utilisateurs qui peuvent se connecter au hotspot. Les éléments de la page des Utilisateurs Locaux sont expliqués dans la liste et l'image ci-dessous :

1. En entrant un nom d'utilisateur, un mot de passe et en cliquant sur le bouton 'Ajouter', vous créez un nouvel utilisateur.
2. Le menu déroulant 'Groupe' permet d'assigner un utilisateur à un autre groupe.
3. Le bouton 'Modifier' vous permet de changer le mot de passe d'un utilisateur ou d'assigner l'utilisateur à un autre groupe.
4. Le bouton 'Supprimer[X]' supprime un utilisateur.



3.4.3 Menu SERVICES > HOTSPOT > Page de destination

Thèmes

La section "Thèmes" affiche tous les thèmes de la page de destination disponibles. Pour télécharger un thème, cliquez sur le bouton "Télécharger", et pour modifier un thème, cliquez sur le bouton "Modifier" à côté de celui-ci.

Thèmes : images

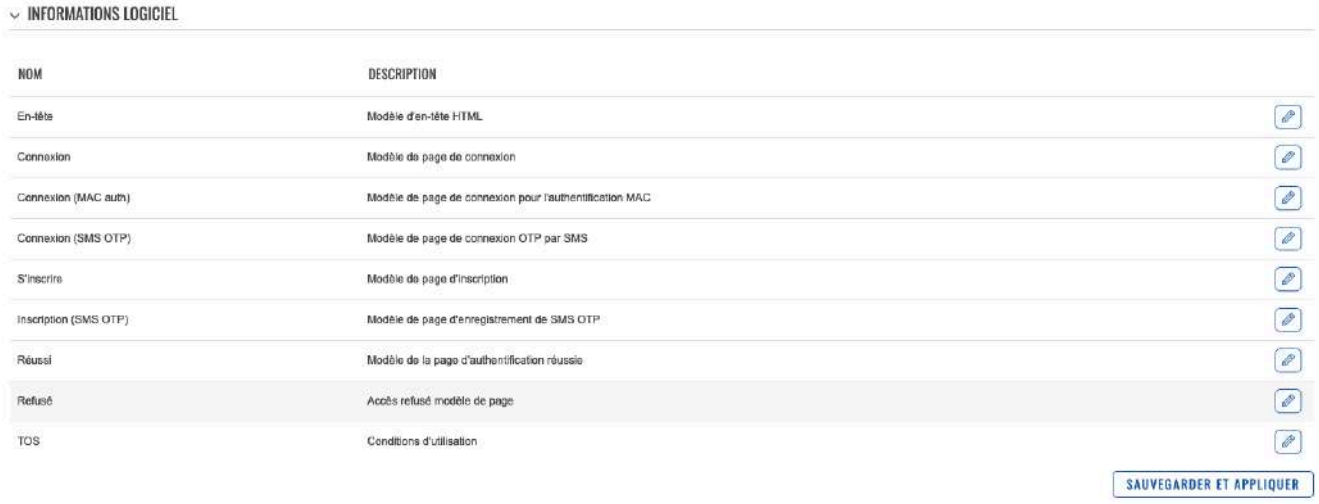
La section "Images" vous permet de télécharger des images personnalisées pour différents objets.

Thèmes : Paramètres de style

En appuyant sur le bouton "Modifier" à côté des paramètres de style, vous permet de modifier l'apparence visuelle de votre page d'atterrissage en utilisant la syntaxe CSS.

Thèmes : Informations logiciel

Dans les Informations logiciel, vous pouvez accéder et modifier les modèles par défaut pour différentes parties de la Page de destination et éditer leur code HTML.



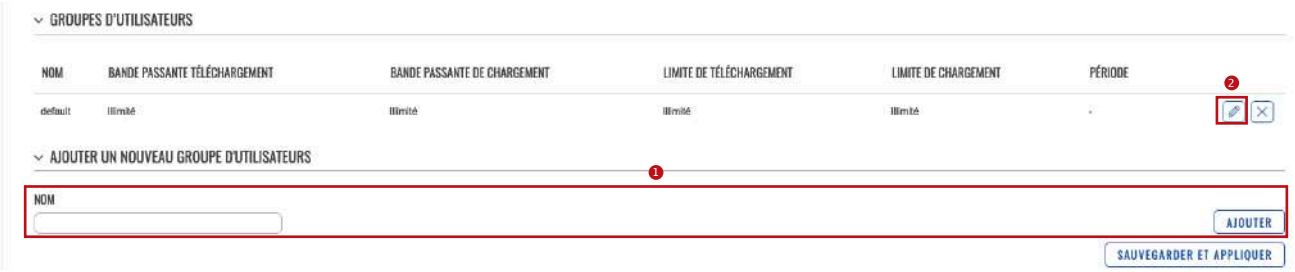
Ajouter un thème personnalisé

Pour utiliser un thème personnalisé, vous pouvez télécharger le thème par défaut et modifier son contenu. Ensuite, utilisez le bouton Parcourir pour le télécharger.

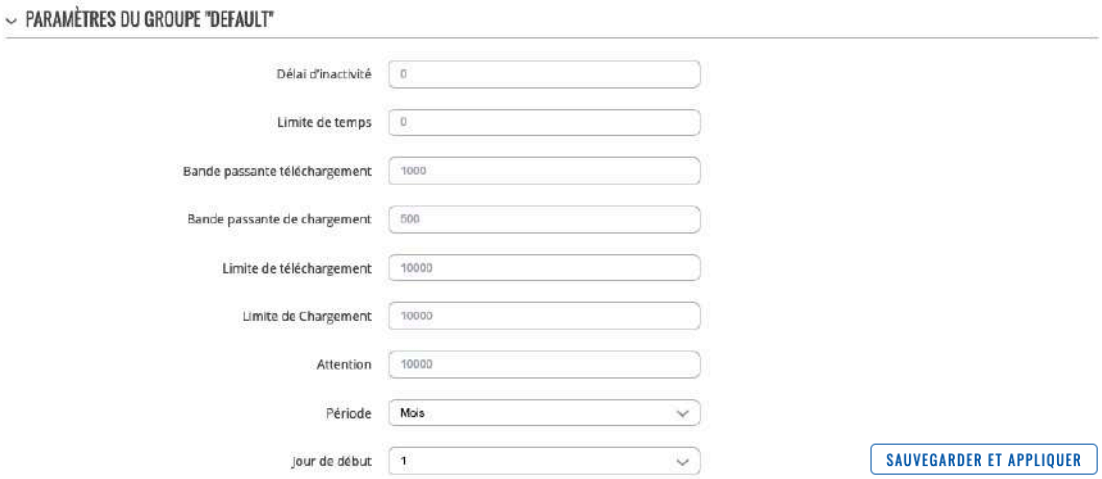
3.4.4 Menu SERVICES > HOTSPOT > Groupes d'utilisateurs

Pour utiliser un thème personnalisé, vous pouvez télécharger le thème par défaut et modifier son contenu. Ensuite, utilisez le bouton de Parcourir pour le télécharger.

1) Créez un nouveau groupe en entrant un nom personnalisé, puis en cliquant sur 'Ajouter'.
2) Ou configurez la règle existante en cliquant sur le bouton 'Modifier' à côté de celle-ci.



La page des paramètres d'un groupe ressemblera à ceci :

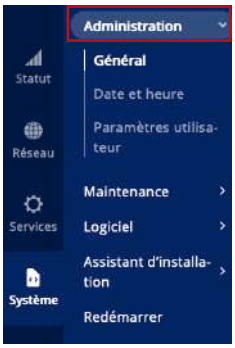


Champ	Valeur	Description
Délai d'inactivité	Par défaut : aucun	Un délai en secondes après lequel les utilisateurs inactifs sont automatiquement déconnectés du Hotspot. (0 signifie illimité.)
Limite de temps	Par défaut : aucun	Désactive l'utilisateur du hotspot après que le délai en secondes soit atteint. (0, signifiant illimité)
Bande passante téléchargement	Par défaut : aucun	La bande passante de téléchargement maximale que les utilisateurs assignés à ce modèle peuvent atteindre. La bande passante peut être spécifiée en Mbit/s.
Bande passante de chargement	Par défaut : aucun	La bande passante de téléversement maximale que les utilisateurs assignés à ce modèle peuvent atteindre. La bande passante peut être spécifiée en Mbit/s.
Limite de téléchargement	Par défaut : aucun	Une limite de données reçues que les utilisateurs assignés à ce modèle peuvent atteindre. Après que la limite de données soit atteinte, l'utilisateur perdra la connexion de données. La limite de téléchargement est spécifiée en Mo.
Limite de Chargement	Par défaut : aucun	Une limite de données envoyées que les utilisateurs assignés à ce modèle peuvent atteindre. Après que la limite de données soit atteinte, l'utilisateur perdra la connexion de données. La limite de téléversement est spécifiée en Mo.
Attention	Par défaut : aucun	Envoyer un avertissement par SMS à l'utilisateur du hotspot après que la valeur d'avertissement de téléchargement ou de téléversement de données en Mo soit atteinte. Ne fonctionne qu'avec l'authentification par SMS OTP.
Période	Mois | Semaine | Jour ; Par défaut : Mois	Le début de la période pendant laquelle la restriction spécifiée dans cette section s'appliquera. Une fois la période terminée, toutes les limites spécifiées sont réinitialisées.
Jour de début	Par défaut : 1	Les choix changent en fonction de ce qui a été choisi pour "Période". Spécifie le jour du mois, de la semaine ou de l'heure du jour où les limites seront réinitialisées.

3.4.5 Menu SERVICES > HOTSPOT > Gestion des utilisateurs

L'onglet Utilisateurs actuels affiche le statut et les statistiques de session des utilisateurs actuellement connectés. Vous pouvez également "expulser" (déconnecter) un utilisateur en cliquant sur le bouton 'Déconnexion' à côté de son nom.

L'onglet Utilisateurs enregistrés affiche les données des utilisateurs uniques qui se sont déjà enregistrés sur le hotspot.



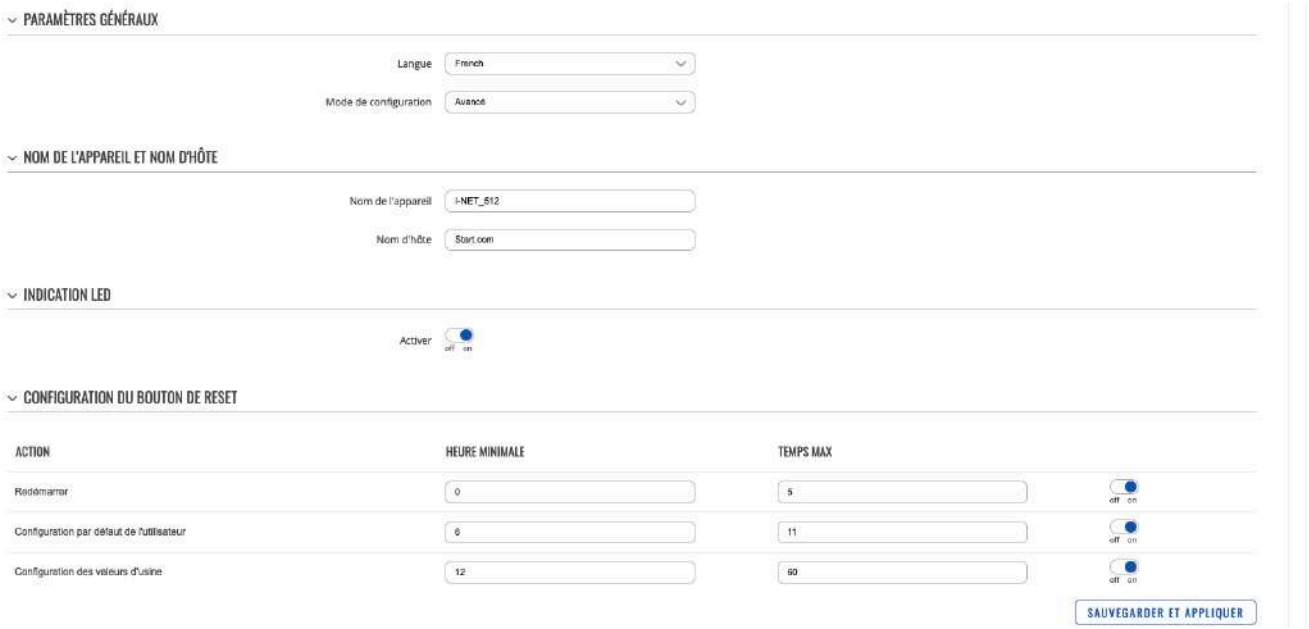
4 Menu Système

Un Hotspot est un service qui fournit l'authentification, l'autorisation et la comptabilité d'un réseau.

4.1 Menu Système > Administration

4.1.1 Menu Système > Administration > Général

La section Général est utilisée pour configurer certains paramètres de gestion de l'appareil, tels que le changement du nom de l'appareil. Pour plus d'informations sur la section Général, veuillez vous référer à la figure et au tableau ci-dessous.



Champ	Valeur	Description
Paramètres généraux		
Langue	English | French | German ; Par défaut : French	Modifie la langue de l'interface utilisateur Web du routeur.
Mode de configuration	Normal | Avancé ; Par défaut : Normal	Le mode détermine quelles options et configurations sont affichées. En mode Basique, seules les configurations essentielles sont affichées. En mode Avancé, il y a une plus grande liberté pour configurer et accéder à davantage d'options.
Nom de l'appareil et nom d'hôte		
Nom de l'appareil	Par défaut : I-NET_512	Nom du modèle de l'appareil.
Nom d'hôte	Par défaut : Start.com	Nom d'hôte de l'appareil. Ceci peut être utilisé pour la communication avec d'autres hôtes du réseau local (LAN).
Indication LED		
Activer	Off | On; Par défaut : On	Gère les voyants d'indication de la force du signal et du statut de la connexion.
Configuration du bouton de reset		
Heure minimale	Par défaut : aucun	Durée minimale (en secondes) pendant laquelle le bouton doit être maintenu enfoncé pour effectuer une action.
Temps max	Par défaut : aucun	Durée maximale (en secondes) pendant laquelle le bouton peut être maintenu enfoncé pour effectuer une action, après quoi aucune action ne sera effectuée.

4.1.2 Menu Système > Administration > Date et heure

Le protocole Network Time Protocol (NTP) est un protocole de réseau utilisé pour la synchronisation des horloges entre les systèmes informatiques via des réseaux de données à commutation de paquets, à latence variable.

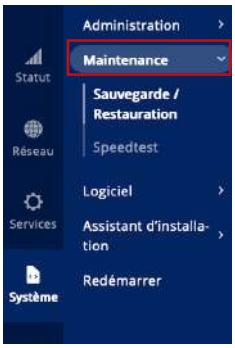
Général

La section de synchronisation horaire vous permet de sélectionner le fuseau horaire, d'activer la synchronisation GPS et de synchroniser l'heure.

Champ	Valeur	Description
Heure actuelle du système	Par défaut : aucun	L'heure locale actuelle de l'appareil.
Synchroniser avec le navigateur	Bouton interactif	Cliquez pour synchroniser l'heure de l'appareil et le fuseau horaire avec les navigateurs, si l'heure ou le fuseau horaire de votre appareil ne sont pas corrects.
Fuseau horaire	Par défaut : UTC	L'appareil synchronisera l'heure en fonction du fuseau horaire sélectionné.
Synchronisation GPS	Off | On; Par défaut : Off	Active la synchronisation périodique de l'heure pour le système en utilisant le module GPS, ce qui ne nécessite pas de connexion Internet.

4.1.3 Menu Système > Administration > Paramètres utilisateur

La section Paramètres utilisateur est utilisée pour changer le mot de passe de l'utilisateur actuel.



4.2 Menu Système > Maintenance

4.2.1 Menu Système > Maintenance > Sauvegarde / Restauration

La page Sauvegarde est utilisée pour générer des fichiers de sauvegarde de configuration ou télécharger des fichiers de sauvegarde existants vers l'appareil.

Créer une configuration par défaut

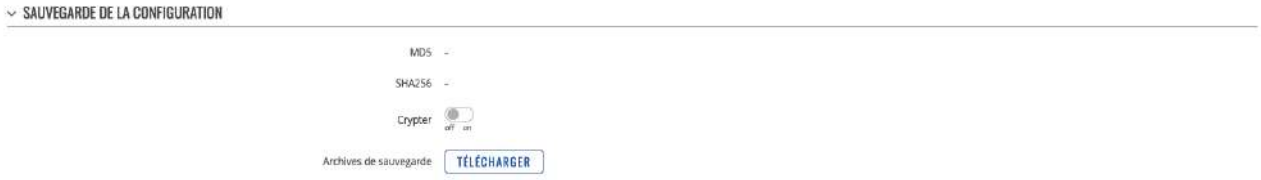
La section Créer une configuration par défaut est utilisée pour créer ou supprimer un fichier qui stocke la configuration actuelle du dispositif. La configuration par défaut peut ensuite être chargée ultérieurement dans la page Administration ou via le bouton de réinitialisation.

Cliquez sur le bouton "Créer" pour générer un fichier de configuration par défaut à partir de la configuration actuelle de votre dispositif.

Sauvegarde de la configuration

La section de sauvegarde de la configuration est utilisée pour générer et télécharger un fichier qui stocke la configuration actuelle du dispositif. Le fichier de sauvegarde peut ensuite être téléchargé vers le même dispositif ou un autre dispositif du même type (les codes produits doivent correspondre).

Cette section contient des champs de contrôle de somme de contrôle MD5 et SHA256 générés à partir du dernier fichier de sauvegarde téléchargé, une option de chiffrement et le bouton de téléchargement pour générer et télécharger le fichier de sauvegarde de la configuration du dispositif.



Notes importantes :

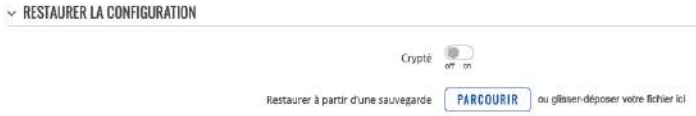
1) Le champ du mot de passe est requis si le chiffrement est activé, c'est à ce moment que le champ apparaît. Si le chiffrement est activé, mais que le routeur n'a pas le paquet 7-zip installé, une fenêtre contextuelle devrait apparaître pour inviter l'utilisateur à télécharger le paquet depuis le Gestionnaire de paquets. Le mot de passe qui sera utilisé pour chiffrer le fichier de sauvegarde devra être fourni lors de l'extraction de l'archive 7z formatée pour accéder au fichier tar.
2) Le fichier de sauvegarde stocke le code PIN configuré dans la page Mobile du I-NET 512, mais il ne sera restauré que si le dispositif n'a pas déjà de code PIN défini lorsque le fichier de sauvegarde est téléchargé - le code PIN du fichier de sauvegarde sera défini uniquement si le dispositif n'en a pas déjà un défini.
3) Si le dispositif n'a pas de connexion Internet lors du chargement d'un fichier de sauvegarde, il ne réinstallera pas les paquets logiciels installés depuis le Gestionnaire de paquets. Vous pouvez ajouter manuellement les fichiers d'installation des paquets au fichier de sauvegarde, un dispositif I-NET 512 les installera automatiquement lorsque vous chargerez le fichier de sauvegarde même sans connexion de données.

Pour intégrer un fichier de sauvegarde avec des fichiers d'installation de paquets, suivez ces étapes :
- Téléchargez les fichiers d'installation de paquets logiciels nécessaires à partir d'ici.
- Téléchargez un fichier de sauvegarde.
- Ouvrez le fichier de sauvegarde et créez un nouveau dossier appelé backup_packages dans le répertoire /etc.
- Ajoutez les fichiers de paquet nécessaires à /etc/backup_packages.
- Assurez-vous que les fichiers dans /etc/backup_packages sont entièrement extraits avec les extensions *.ipk.

Restaurer la configuration

La section Restaurer la configuration est utilisée pour télécharger un fichier de configuration qui a été pris de cet appareil ou d'un autre appareil du même type.

Activez "Crypté" si le fichier de sauvegarde était précédemment crypté, puis cliquez sur le bouton "Parcourir" pour sélectionner un fichier de sauvegarde depuis votre ordinateur. Enfin, cliquez sur le bouton "Charger l'archive" pour appliquer la configuration sélectionnée sur cet appareil.



Restaurer les paramètres par défaut

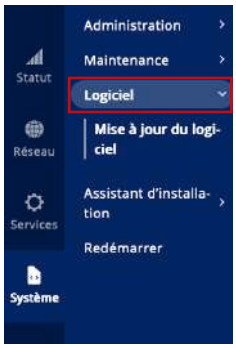
La section Restaurer les paramètres par défaut est utilisée pour restaurer la configuration par défaut de l'appareil.

Champ	Valeur	Description
Restaurer les paramètres d'usine	Bouton interactif	Restaure l'appareil aux paramètres par défaut.
Restaurer les valeurs utilisateur par défaut*	Bouton interactif	Restaure l'appareil à la configuration personnalisée définie par l'utilisateur.

* Vous ne verrez pas ce bouton tant que vous n'aurez pas créé une configuration par défaut de l'utilisateur.

4.2.2 Menu Système > Maintenance > Speedtest

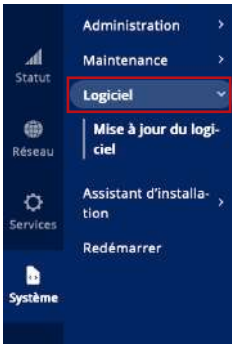
Ce compteur de vitesse du trafic réseau vous indiquera quelle est votre vitesse de téléchargement et de téléversement en Mbps.



4.3 Menu Système > Logiciel

4.3.1 Menu Système > Logiciel > Mise à jour du logiciel

Champ	Valeur	Description
Mise à jour depuis	Fichier | Serveur : Par défaut : File	Source de l'image du micrologiciel. Peut être téléchargée depuis FOTA (serveur) ou téléversée depuis un ordinateur (fichier).
Conserver les paramètres	Off | On; Par défaut : Off	Garantit que tous les paramètres actuels de l'appareil seront conservés après la mise à niveau du micrologiciel.
Image	Bouton interactif	Cliquez pour parcourir votre ordinateur à la recherche d'un fichier d'image de micrologiciel.



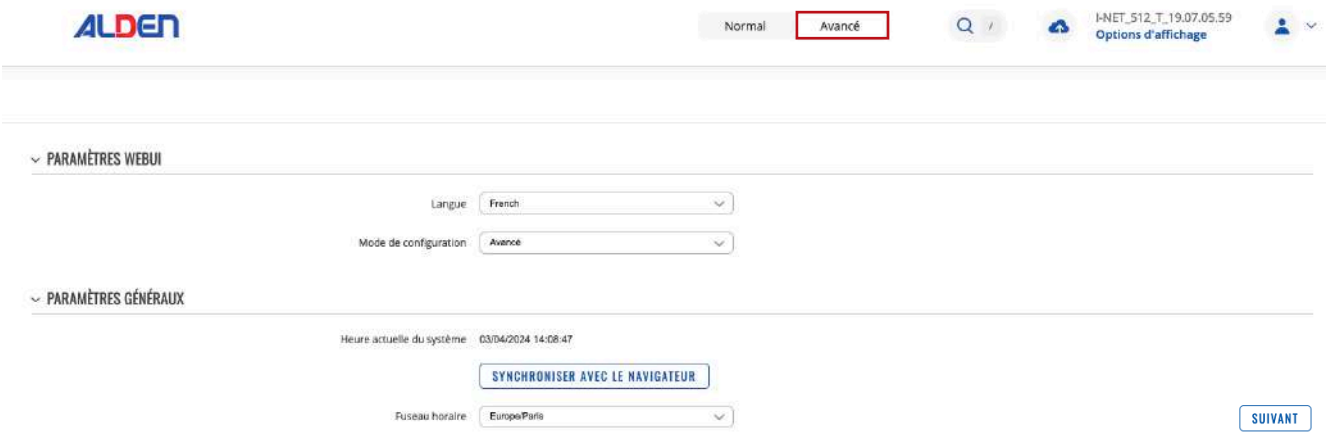
4.4 Menu Système > Assistant d'installation

4.4.1 Menu Système > Assistant d'installation > Général

La section Général est utilisée pour configurer l'heure de l'appareil, la langue et les paramètres du mode d'interface utilisateur Web (WebUI).

Si vous préférez définir ultérieurement les paramètres du fuseau horaire de l'appareil, vous pouvez le faire via la page Administration → NTP.

Si vous rencontrez des difficultés à trouver cette page ou certains des paramètres décrits ici sur l'interface utilisateur Web de votre appareil, vous devriez activer le mode "Interface utilisateur Web avancée". Vous pouvez le faire en cliquant sur le bouton "Avancé", situé en haut de l'interface utilisateur Web.

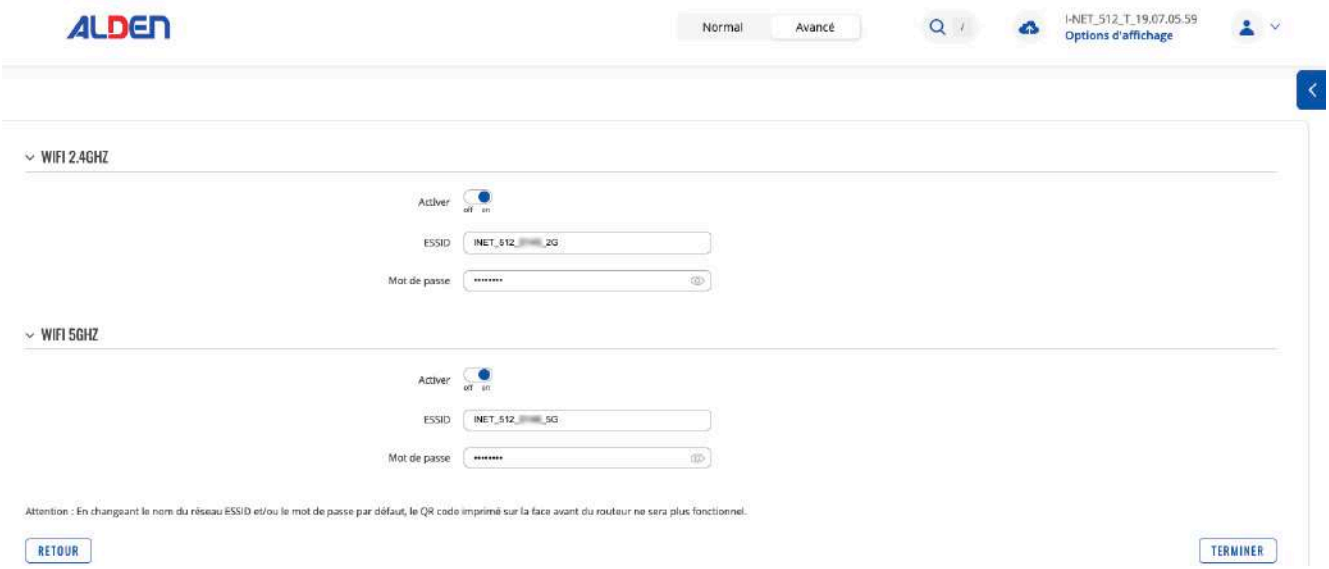


4.4.2 Menu Système > Assistant d'installation > Mobile

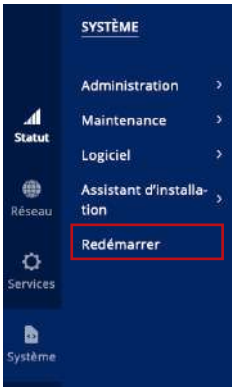
La section Mobile est utilisée pour configurer les paramètres de la carte SIM de l'appareil.

Champ	Valeur	Description
Auto APN	Off | On; Par défaut : On	Un Nom de Point d'Accès (APN) est une passerelle entre un réseau mobile GSM, GPRS, 3G ou 4G et un autre réseau informatique. Selon le contrat, certains opérateurs peuvent exiger que vous saisissiez l'APN juste pour finaliser l'inscription à un réseau. Dans d'autres cas, un APN est utilisé pour obtenir des paramètres spéciaux de l'opérateur (par exemple, une adresse IP publique) en fonction du contrat. L'APN automatique analyse une base de données interne d'APN Android et sélectionne un APN en fonction de l'opérateur et du pays de la carte SIM. Si le premier APN sélectionné automatiquement ne fonctionne pas, il tente d'utiliser le prochain APN existant de la base de données.
Off: APN	Par défaut : Personnalisé	Sélectionnez entre un APN suggéré par l'appareil ou saisissez votre APN personnalisé.
Personnalisé : APN personnalisé	Par défaut : aucun	Identifiant de réseau APN personnalisé. Ne peut pas commencer par l'une des chaînes suivantes : "rac", "lac", "sgsn" ou "rnc"; il ne peut pas se terminer par ".gprs" et il ne peut pas prendre la valeur "*".
Personnalisé : Type d'authentification	Aucun | PAP | CHAP; Par défaut : aucun	La méthode que votre opérateur utilise pour authentifier de nouvelles connexions sur son réseau. Si vous sélectionnez PAP, CHAP ou les deux, vous devrez entrer un nom d'utilisateur et un mot de passe.
PIN	Par défaut : aucun	Un mot de passe numérique à 4 chiffres utilisé pour authentifier le modem à la carte SIM.

4.4.3 Menu Système > Assistant d'installation > WiFi



Champ	Valeur	Description
Activer	Off | On; Par défaut : On	Active ou désactive le point d'accès Wi-Fi.
ESSID	Par défaut : INET_512_	Un nom d'identification pour le point d'accès. C'est ainsi que le point d'accès sera vu par les appareils connectés.
Mot de passe	Par défaut : unique à chaque appareil	Un mot de passe utilisé pour authentifier les utilisateurs sur ce point d'accès.



4.5 Menu Système > Redémarrer

Cliquez sur le bouton "Redémarrer" si vous souhaitez redémarrer l'appareil.

Garantie ALDEN

La garantie ALDEN couvre :

Les garanties pour vice de fabrication sont accordées à partir de la date de facturation à l'acheteur sous réserve de renvoi du bon de garantie. À défaut de retour, cette garantie sera limitée dans le temps. Pour pouvoir bénéficier de la garantie des produits, il convient impérativement de conserver la facture d'achat du dit produit.

Attention : Toute intervention sans accord écrit de la part de la SAS ALDEN entraîne de plein droit la nullité de la garantie. Le client et l'acheteur ne pourront prétendre à aucune indemnité de quelque nature qu'elle soit pour démontage, remontage ou privation d'usage inférieur à 30 jours. La SAS ALDEN ne peut être tenue pour responsable d'incidents ou de dommages quels qu'ils soient en cas de montage non conforme aux recommandations de la SAS ALDEN. Il est rappelé que toute installation électrique doit être protégée par un fusible adéquat.

De manière générale, les montages doivent être effectués dans les règles de l'art. L'installateur et l'utilisateur sont réputés connaître les réglementations et lois. L'installateur et l'utilisateur doivent se tenir informés des règles de montage. L'installateur et l'utilisateur ne pourront prétendre à aucune indemnité ou garantie en cas de non-observation de ces règles.

Toutefois, en tout état de cause, vous bénéficiez des dispositions de la garantie légale notamment celles relatives à la garantie des vices cachés.

Attention : L'application des garanties ainsi qu'un retour éventuel sont subordonnés à accord préalable de la SAS ALDEN. Les retours éventuels se font en Franco et sont à la charge des expéditeurs (client, pour le retour ALDEN ; ALDEN, pour le retour client). En cas de demande de renvoi en Express ou en ChronoPost, les frais de retour client sont à la charge de celui-ci.

Sont exclus de la garantie ALDEN :

- le remplacement des consommables et pièces d'usure ;
- l'utilisation anormale ou non conforme des produits. Nous vous invitons à cet égard à consulter attentivement la notice d'emploi fournie avec les produits ;
- les pannes liées aux accessoires ou dues à un mauvais montage ;
- les défauts et leurs conséquences dus à l'intervention d'un réparateur non agréé par la SAS ALDEN ;
- les défauts et leurs conséquences liés à l'utilisation non conforme à l'usage pour lequel le produit est destiné ;
- les défauts et leurs conséquences liés à toute cause extérieure.

Garantie

ALDEN recommande de s'adresser aux professionnels pour tout montage.

En cas d'installation personnelle, l'acheteur fera sienne les responsabilités affairant à la sécurité.

L'acheteur est dans ce cas réputé avoir les compétences nécessaires. Il s'engage à respecter les règles usuelles qu'appliquent les professionnels. Il veillera à respecter les lois en vigueur dans le pays d'utilisation. Il ne déviera pas le produit de l'utilisation prévue.

Garantie :
L'acheteur prendra contact avec son revendeur en cas de dysfonctionnement.

ATTENTION :
La garantie sera caduque en cas d'intervention sans accord de la part d'ALDEN.

Complétez puis renvoyez ce bon accompagné d'une photocopie de la facture à l'adresse suivante :

ALDEN – Z.A. du Hairy – 67230 HUTTENHEIM.

Bon de garantie

NOM, Prénom : .....

Adresse complète : .....

.....

Code postal : .....

Ville : .....

Concessionnaire : .....

Date d'achat : .....

Produit : .....

N° de série : .....

Inhaltsverzeichnis

Inhaltsverzeichnis

Warnhinweise

Die Vervielfältigung dieser Anleitung oder von Teilen davon ist ohne schriftliche Genehmigung von ALDEN untersagt. ALDEN weist besonders auf die Gefahren hin, die bei unsachgemäßer Montage entstehen können.

ALDEN kann nicht haftbar gemacht werden, wenn die Montage nicht den Regeln der Technik entspricht, insbesondere wenn die Installation von einem Nichtfachmann durchgeführt wird.

Es wird davon ausgegangen, dass der Händler die Regeln der Technik kennt und sich an diese hält. Er wird insbesondere die Regeln für die Wahl des Standorts, den elektrischen Anschluss, das Kleben und Verschrauben beachten. Er verpflichtet sich, beim Verkauf und bei der Installation eines ALDEN-Produkts seinen Kunden über die Gebrauchsanweisung und gegebenenfalls über die Installationsanweisung zu informieren und übergibt ihm die erforderlichen Unterlagen. Er wird den Kunden auf alle sicherheitsrelevanten Aspekte aufmerksam machen. Er wird den Kunden darüber informieren, dass das verkaufte Produkt nicht zweckentfremdet werden darf. Außerdem wird er den Kunden gegebenenfalls auf die Verpflichtung hinweisen, die geltenden Gesetze des Landes oder der Länder, in denen das Produkt verwendet wird, einzuhalten.

Jedes Produkt mit elektronischen Elementen muss vor Unterspannungen (unter 10,5 Volt) und Überspannungen (über 15 Volt) geschützt werden.

Jeder Eingriff am Produkt, der ohne vorherige Zustimmung von ALDEN vorgenommen wird, führt zum Erlöschen der Garantie.

Der Verkäufer sowie der Hersteller können in keinem Fall für Änderungen der Emissionsarten oder der Sendeleistungen haftbar gemacht werden. Ereignisse, die dem Verkäufer und dem Hersteller nicht bekannt sind, können keinen Anspruch auf Umtausch, Rückerstattung oder Entschädigung jeglicher Art begründen. Die Angaben zu den Empfangsgebieten sind unverbindlich.

ALDEN lehnt jede Haftung jeglicher Art ab, insbesondere für Unfälle oder Zwischenfälle bei Nichtbeachtung der gegebenen Anweisungen, sowohl bei der Installation als auch bei der Verwendung.

Das Öffnen der einzelnen Komponenten ist strengstens untersagt. In diesem Fall können keine Garantieansprüche geltend gemacht werden.

Bei Eingriffen in den Stromkreis, beim Austausch oder Anschließen der Batterie müssen die Sicherungen in den Versorgungskabeln der Satellitengeräte entfernt werden. Wenn das Fahrzeug mit einem Solarmodul ausgestattet ist, muss auch die Sicherung des Ladereglers entfernt werden.

Es ist unbedingt erforderlich, eine separate, mit 5 Ampere abgesicherte Stromversorgung direkt von der Aufbaubatterie zu verlegen, um die Geräte mit Strom zu versorgen.

Die Kabelenden müssen während der Installation unbedingt gegen Kurzschlüsse geschützt werden.

Verwenden Sie nur Originalersatzteile und Zubehör oder von einem Fachhändler empfohlene Teile, da sonst die Garantie erlischt. Alle Arbeiten an dem Gerät dürfen nur von qualifizierten Technikern durchgeführt werden.

Öffnen Sie nicht das Gehäuse des Geräts, da dies zu Stromschlägen führen kann und die Garantie erlischt. Lassen Sie das Gerät nur von qualifiziertem Personal warten und instand halten.

Achten Sie beim Anschließen der Kabel darauf, dass das Gerät vom Stromnetz getrennt ist. Warten Sie nach dem Ausschalten des Geräts einige Sekunden, bevor Sie angeschlossene Kabel abziehen.

Verwenden Sie nur Kabel und Verlängerungskabel, die mit der Leistungsaufnahme des Geräts kompatibel sind.

Wenn das Gerät nicht richtig funktioniert, obwohl Sie alle Anweisungen in dieser Anleitung strikt befolgt haben, wenden Sie sich an Ihren Händler.

Dieses Gerät erfüllt die staatlichen Anforderungen für die Belastung durch Funkwellen. Dieses Gerät wurde so konzipiert und hergestellt, dass es die von den autorisierten Behörden festgelegten Emissionsgrenzwerte für die Belastung durch Radiofrequenzen (RF) nicht überschreitet. Um die Einhaltung der Richtlinien für die RF-Belastung

zu gewährleisten, muss das Gerät mit einem Mindestabstand von 20 cm zum Körper einer Person betrieben werden. Die Nichtbeachtung dieser Anweisungen kann zu einer HF-Belastung führen, die die Grenzwerte der relevanten Richtlinien überschreitet.
Externe Antennen, die mit dem I-NET 512 verwendet werden, müssen so installiert werden, dass sie einen Trennungsabstand von mindestens 20 cm zu allen Personen bieten, und dürfen nicht gemeinsam mit einer anderen Antenne oder einem anderen Sender platziert oder verwendet werden.
Jeder externe Antennenverstärkung muss die Grenzwerte für die HF-Exposition und die maximale abgestrahlte Ausgangsleistung des zutreffenden Regelabschnitts einhalten.

- Mit der Durchführung der Installation akzeptieren Sie die aufgeführten Richtlinien. -

Schützen Sie den Zugriff auf Ihr Gerät :

Montieren Sie den Router an einem Sicheren Ort und schützen Sie diesen vor unautorisierten Personen. Ändern Sie regelmäßig die Zugangscodes (PIN-Code, Passwörter usw.) Ihres Geräts. Schalten Sie Ihr Gerät aus, wenn es nicht benutzt wird oder um zu verhindern, dass sensible Daten abgefangen werden. Installieren Sie Software-Updates wenn diese zur Verfügung stehen.

Achten Sie auf den Umgang mit Daten: Achten Sie auf Daten, die Ihre Privatsphäre betreffen, z. B. indem Sie die automatische Datenfreigabe deaktivieren, wenn Sie das Gerät mit sozialen Netzwerken verknüpfen.
Löschen Sie die Daten auf dem Gerät, bevor Sie es entsorgen, verkaufen oder zum Kundendienst geben.
Achten Sie bei der Verbindung mit einem Wi-Fi Access Point (AP) darauf, dass dieser sicher ist.

Im Zusammenhang mit der Nutzung des Produkts ist ALDEN nicht verantwortlich für :
- Für die Inhalte, auf die der Nutzer im Rahmen der Nutzung des Produkts zugreifen kann.
- Für den Datenaustausch zwischen dem Nutzer und einer beliebigen Plattform.
- Für die Handlungen Dritter, die Ihre Informationen oder Daten sammeln, verwenden, übertragen und offenlegen.
- Der Verbrauch und die Menge der mobilen Daten, die mit der SIM-Karte verbunden sind, die den Zugang zu einem Mobilfunknetzbetreiber ermöglicht.

ALDEN behält sich das Recht vor, die Software automatisch zu aktualisieren, einschließlich Fehlerbehebungen und Updates, der Benutzeroberfläche oder der Art und Weise, wie Sie auf Inhalte zugreifen, sowie anderer Änderungen, die Funktionen und Merkmale hinzufügen, ändern oder entfernen können. Sie erkennen an, dass diese Aktualisierungen jederzeit automatisch erfolgen können. Sie verstehen, dass diese Aktualisierungen notwendig sind, um die Kompatibilität mit anderen Aktualisierungen unserer Produkte aufrechtzuerhalten, und aus Sicherheitsgründen notwendig sein können. Durch die Nutzung unseres Dienstes erklären Sie sich hiermit einverstanden, diese Updates zu erhalten.

KENNZEICHNUNG FÜR EUROPA
Das CE-Zeichen, das an diesem Produkt angebracht ist, bedeutet, dass es die Richtlinien Radio Equipment Directive 2014/53/EU, Low **Voltage Directive 2014/35/EU und RoHS 2011/65/EU erfüllt.**

Die WEEE-Richtlinie (nur Europäische Union und EWR).
Dieses Symbol weist darauf hin, dass dieses Produkt gemäß der WEEE-Richtlinie (2002/96/EG) und den Vorschriften Ihres Landes nicht mit dem Hausmüll entsorgt werden darf. Sie müssen es an einer dafür vorgesehenen Sammelstelle abgeben, z. B. an einer offiziellen Sammelstelle für elektrische und elektronische Geräte (EEE) zum Recycling oder an einer autorisierten Produkttauschstelle, die zugänglich ist, wenn Sie ein neues Produkt desselben Typs wie das alte erwerben. Jede Abweichung von diesen Empfehlungen zur Entsorgung dieser Art von Abfall kann negative Auswirkungen auf die Umwelt und die öffentliche Gesundheit haben, da diese EEEProdukte in der Regel Stoffe enthalten, die gefährlich sein können. Gleichzeitig wird Ihre volle Kooperation bei der ordnungsgemäßen Entsorgung dieses Produkts eine bessere Nutzung der natürlichen Ressourcen fördern. So erhalten Sie weitere Informationen über Sammelstellen für zu recycelnde Geräte erhalten Sie bei Ihrer Stadtverwaltung, der Müllabfuhr, dem genehmigten WEEE-Plan oder der Müllabfuhr. (EWR: Norwegen, Island und Liechtenstein)

Produkthandhabung

- Sie allein sind dafür verantwortlich, wie Sie Ihr Gerät verwenden, und für alle Folgen seiner Verwendung.
- Die Verwendung Ihres Geräts unterliegt Sicherheitsmaßnahmen zum Schutz der Benutzer und ihrer Umgebung.
- Behandeln Sie Ihr Gerät und sein Zubehör stets pfleglich und bewahren Sie es an einem sauberen und staubfreien Ort auf.
- Setzen Sie Ihr Gerät oder sein Zubehör nicht offenen Flammen oder brennenden Tabakprodukten aus.
- Setzen Sie Ihr Gerät oder sein Zubehör keiner Flüssigkeit, Nässe oder hoher Luftfeuchtigkeit aus.
- Lassen Sie Ihr Gerät oder sein Zubehör nicht fallen, werfen Sie es nicht und versuchen Sie nicht, es zu biegen.
- Verwenden Sie keine aggressiven Chemikalien, Reinigungslösungen oder Sprays, um das Gerät oder sein Zubehör zu reinigen.
- Lackieren Sie Ihr Gerät oder sein Zubehör nicht.
- Versuchen Sie nicht, Ihr Gerät oder sein Zubehör zu zerlegen, dies darf nur von autorisiertem Personal durchgeführt werden.
- Verwenden Sie Ihr Gerät nicht in einer geschlossenen Umgebung oder an Orten mit schlechter Wärmeableitung.
- Eine längere Verwendung in einem solchen Raum kann übermäßige Hitze verursachen und die Umgebungstemperatur erhöhen, was zu Ihrer Sicherheit zum automatischen Herunterfahren Ihres Geräts oder zum Trennen der Mobilfunknetzverbindung führt. Um Ihr Gerät nach einer solchen Abschaltung wieder normal zu verwenden, kühlen Sie es an einem gut belüfteten Ort ab, bevor Sie es einschalten.
- Bitte überprüfen Sie die örtlichen Vorschriften zur Entsorgung elektronischer Produkte.
- Betreiben Sie das Gerät nicht an Orten mit eingeschränkter Belüftung.
- Verwenden oder installieren Sie dieses Produkt nicht in der Nähe von Wasser, um Brand- oder Stromschlaggefahr zu vermeiden.
- Vermeiden Sie es, das Gerät Regen oder feuchten Bereichen auszusetzen.
- Ordnen Sie Strom- und Netzwerkkabel so an, dass niemand darauf treten oder Gegenstände darauf ablegen können.
- Stellen Sie sicher, dass Spannung und Nennstrom der Stromquelle den Anforderungen des Geräts entsprechen. Schließen Sie das Gerät nicht an eine ungeeignete Stromquelle an.
- Lassen Sie Ihr Gerät und sein Zubehör nicht in Reichweite von kleinen Kindern und lassen Sie sie nicht damit spielen. Sie könnten sich selbst oder andere verletzen oder das Gerät versehentlich beschädigen. Ihr Gerät enthält Kleinteile mit scharfen Kanten, die Verletzungen verursachen oder sich lösen und eine Erstickungsgefahr darstellen können.
- Dieses Gerät arbeitet wie jedes drahtlose Gerät mit Funksignalen, die eine Verbindung nicht unter allen Bedingungen garantieren können. Daher dürfen Sie sich für die Notfallkommunikation niemals ausschließlich auf ein drahtloses Gerät verlassen oder das Gerät anderweitig in Situationen verwenden, in denen die Unterbrechung der Datenkonnektivität zu Tod, Körperverletzung, Sachschäden, Datenverlust oder anderen Verlusten führen könnte.
- Das Gerät kann während des normalen Gebrauchs warm werden.

Aktualisierung des I-NET 512

Der I-NET 512-Router verfügt über automatische und manuelle Softwareaktualisierungen. Software-Updates können automatisch durchgeführt werden. Vor jeder Aktion am Gerät (Unterbrechung der Stromversorgung, Neustart..) sollten Sie den Status der LEDs überprüfen und sicherstellen, dass sich der Router nicht in einer Update-Phase befindet.

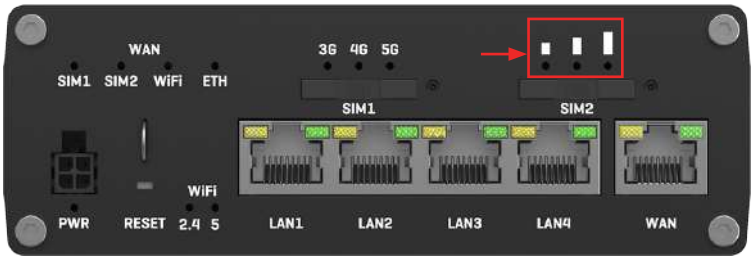
Um die Software manuell zu aktualisieren, lesen Sie bitte das Kapitel ""4.3.1 Menü System > Firmware > Firmware aktualisieren", page 211.

Die Installation eines Updates äußert sich visuell in 3 Schritten, wie unten beschrieben:

- Alle LEDs ausgeschaltet : Herunterladen der neuen Software (Dauer: bis zu 30 Sekunden).
- Alle 3 LEDs blinken nacheinander: Installation der neuen Software (Dauer: bis zu 90 Sekunden).
WICHTIG : Schalten Sie das Gerät während dieses Schrittes nicht aus.
- Gleichzeitiges Blinken der LEDs: Neustart des Routers (Dauer: bis zu 2 Minuten)

HINWEIS : Während der Installationsphase des Updates wird die Wi-Fi-Verbindung unterbrochen.

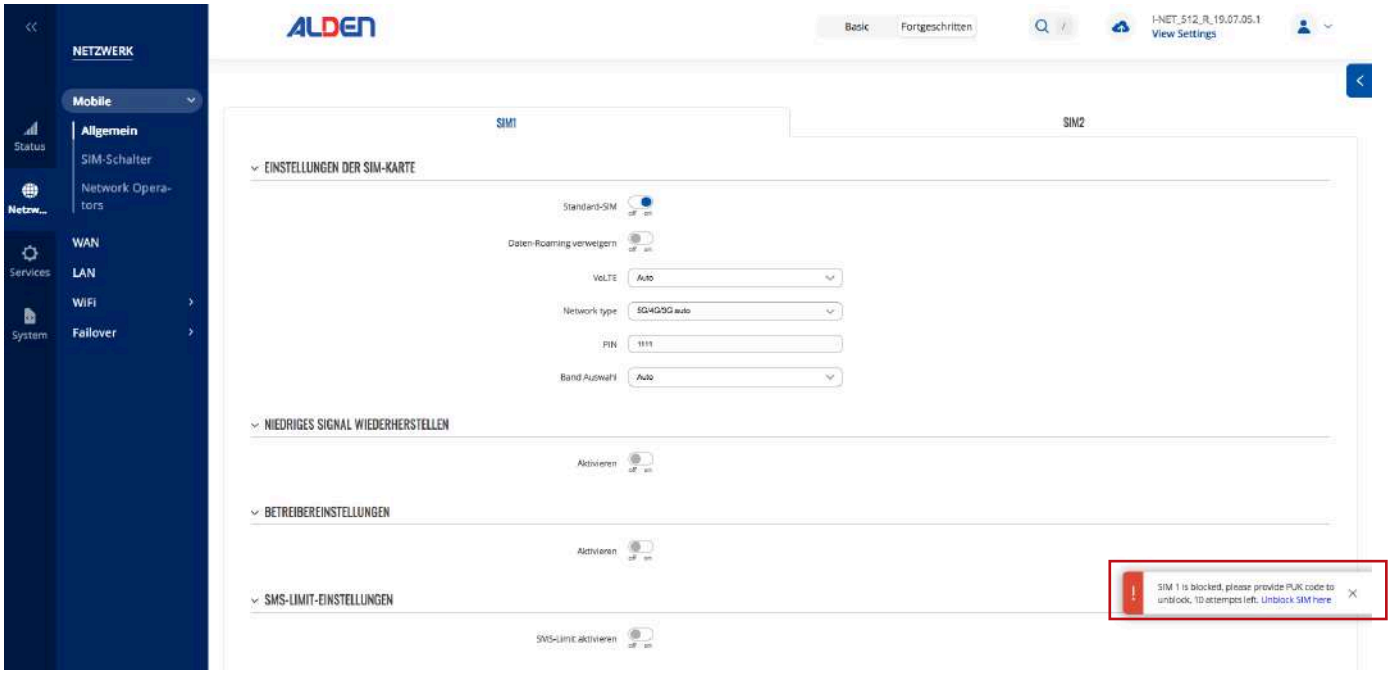
ACHTUNG : SCHALTEN SIE DEN I-NET 512 ROUTER WÄHREND DER UPDATEPHASE NICHT AUS, DA DIESER SONST EINEN DAUERHAFTEN SCHADEN ERLEIDEN UND UNBRAUCHBAR WERDEN KÖNNTE.



PUK-Code

Der PUK (Personal Unblocking Key) ist ein 8-stelliger Notfallcode, der verwendet wird, um Ihre SIM-Karte zu entsperren, nachdem Sie dreimal hintereinander einen falschen PIN-Code eingegeben haben. Sie finden diesen Code auf dem Begleitdokument Ihrer SIM-Karte. Alternativ kann er auch vom Kundenservice Ihres Mobilfunkanbieters bereitgestellt werden. Sie haben 10 Versuche, um den PUK-Code einzugeben.

Die Eingabe des PUK-Codes erfolgt durch Klicken auf die Nachricht "Débloquer la carte SIM ici" (SIM-Karte hier entsperren) in dem Pop-up-Fenster, das angezeigt wird, nachdem dreimal ein falscher PIN-Code im Menü NETZWERK - Mobile - Allgemein eingegeben wurde. (siehe Kapitel "2.1.1 Menü Netzwerk > Mobile > Allgemein", page 133). Der PUK-Code kann auch in der Zeile "Infos zur SIM-Karte" eingegeben werden - auf der Seite 17 "SIM-Karte entsperren - PUK-Code.



I-NET 512 - Sicherheitsinformationen

HF-Exposition

Dieses Gerät erfüllt die Anforderungen der Regierung für die Belastung durch Funkwellen. Dieses Gerät wurde so konzipiert und hergestellt, dass es die von den autorisierten Behörden festgelegten Emissionsgrenzwerte für die Exposition gegenüber Hochfrequenzenergie (RF) nicht überschreitet. Um die Einhaltung der Richtlinien zur HF-Exposition zu gewährleisten, muss das Gerät mit einem Mindestabstand von 20 cm zum Körper einer Person verwendet werden. Die Nichtbeachtung dieser Anweisungen kann dazu führen, dass Ihre HF-Exposition die entsprechenden Richtliniengrenzwerte überschreitet.
Externe Antennen, die mit I-NET 512 verwendet werden, müssen so installiert werden, dass ein Mindestabstand von 20 cm zu allen Personen eingehalten wird, und dürfen nicht zusammen mit anderen Antennen oder Sendern aufgestellt oder betrieben werden.
Jede externe Antennenverstärkung muss die Grenzwerte für die HF-Belastung und die maximale abgestrahlte Ausgangsleistung des anwendbaren Regelabschnitts erfüllen.

Antennentyp	Frequenzbereich	Impedanz	VSWR	Verstärkung*	Strahlung	Verbinder
Handy, Mobiltelefon	800~960MHz, 1710~2690MHz	50 Ω	≤ 3,0	≤ 4 dBi	omnidirektional	SMA-männlich
W-Lan	2,4 ~ 2,5 GHz, 5,10 ~ 5,95 GHz	50 Ω	2,5 max	≤ 3,5 dBi	omnidirektional	RP-SMA-männlich

* Eine Antenne mit höherem Gewinn kann angeschlossen werden, um die Kabeldämpfung zu kompensieren, wenn ein Kabel verwendet wird. Der Nutzer ist für die Einhaltung der gesetzlichen Vorschriften verantwortlich.

Maximale Sendeleistung	
WCDMA	24 dBm
LTE	23 dBm
W-Lan	20 dBm

Betriebsbedingungen

- Betriebstemperatur: -40° bis +75° Celsius
- Die Luftfeuchtigkeit sollte im Bereich von 10 % bis 90 % liegen (nicht kondensierend). Verwenden Sie das Gerät nur in trockener Umgebung.
- Außerhalb direkter Sonneneinstrahlung
- Außerhalb von Wärmequellen
- Abseits von ätzenden Stoffen, Salzen und brennbaren Gasen

ACHTUNG: Der Betrieb außerhalb des zulässigen Bereichs kann die Lebensdauer des Geräts erheblich verkürzen

Fehlerhafte und beschädigte Produkte

- Versuchen Sie nicht, das Gerät oder sein Zubehör zu zerlegen.
- Nur qualifiziertes Personal darf das Gerät oder sein Zubehör warten oder reparieren.
- Wenn Ihr Gerät oder sein Zubehör in Wasser getaucht, durchstochen oder einem schweren Sturz ausgesetzt wurden, verwenden Sie es nicht, bis es von einem autorisierten Servicecenter überprüft wurde.

Elektrische Sicherheit

- Verwenden Sie nur zugelassenes Zubehör.
- Nicht mit inkompatiblen Produkten oder Zubehör verbinden.

Konfiguration I-NET 512

I-NET 512 Abmessungen & Gewicht

Diese Seite enthält Abmessungen- und Gewichtsinformationen. Die hier bereitgestellten Zeichnungen sollen helfen, die Größe des Geräts vor der Installation abzuschätzen.

Die unten dargestellten Abbildungen zeigen die Abmessungen des Geräts aus verschiedenen Blickwinkeln und von verschiedenen Elementen (Kabel, Anschlüsse usw.), die sich am Gerät befinden oder aus ihm herausragen. Alle Maße sind in Millimeter (mm) angegeben.

Allgemeine Abmessungen

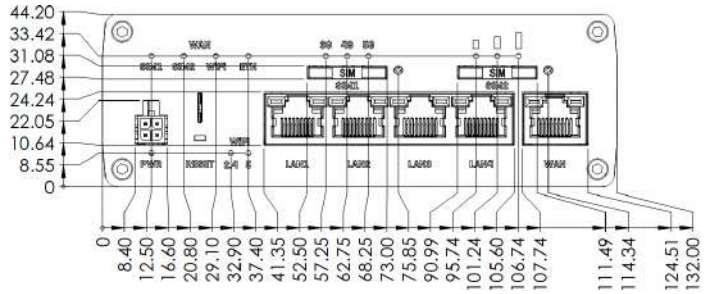
Maße B x H x T für I-NET 512:

- Gerätegehäuse *: 132 x 44,2 x 95,1 mm
- Verpackung: 355 x 60 x 175 mm

* Gehäusemaße sind ohne Antennenstecker und Schrauben dargestellt; Informationen zu Maßen anderer Geräteelemente finden Sie in den folgenden Abschnitten.

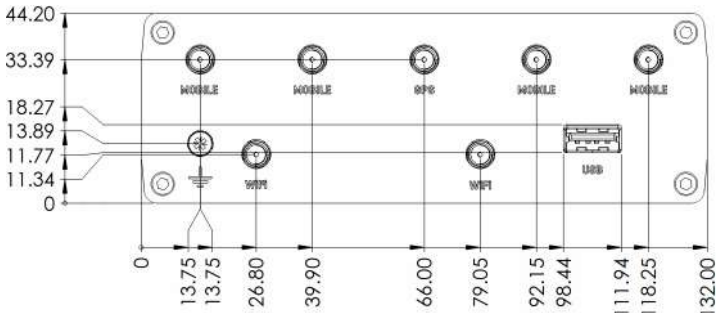
Ansicht von vorne

Die folgende Abbildung zeigt die Messungen des I-NET 512 und seiner Komponenten auf der Vorderseite :



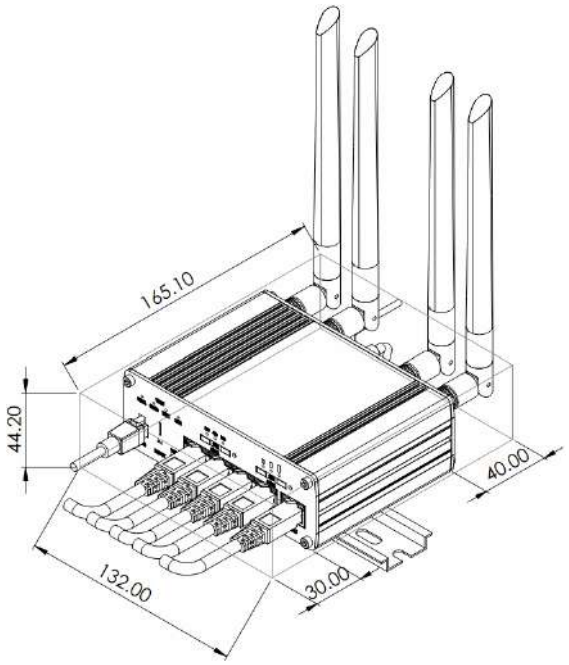
Rückansicht

Die folgende Abbildung zeigt die Abmessungen des I-NET 512 und seiner Komponenten auf der Rückseite :



Anforderungen an den Montageplatz

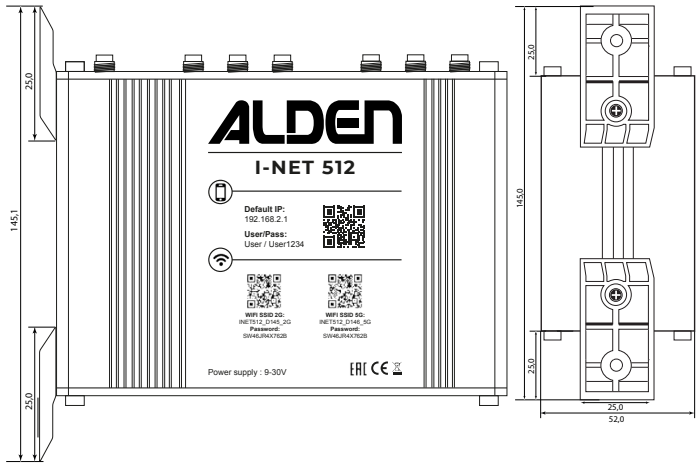
Die folgende Abbildung zeigt ungefähr die Abmessungen des Geräts mit angeschlossenen Kabeln und Antennen:



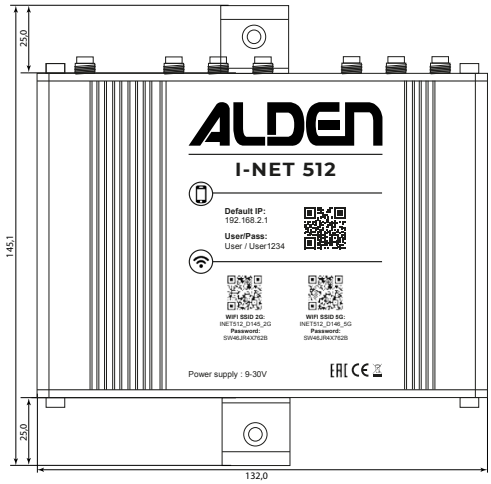
Befestigung

Die folgenden Abbildungen zeigen die Abmessungen des Geräts mit seinen Halterungen:

Vertikale Befestigung



Horizontale Befestigung

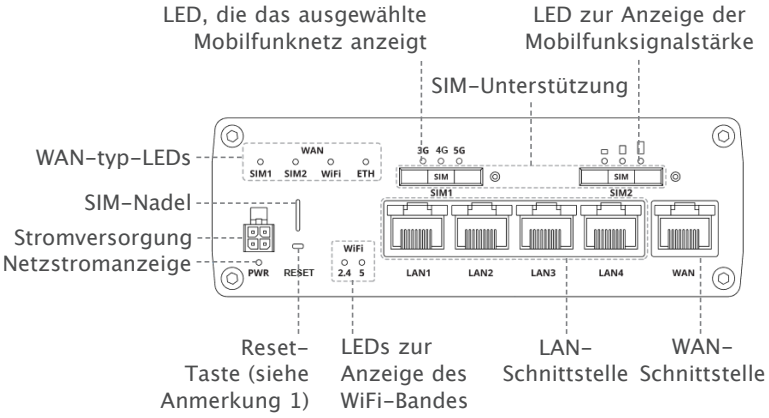


Beachten Sie, dass Sie den Router sowohl vertikal als auch horizontal befestigen können. Schrauben Sie die beiden Halterungen mithilfe der beiden Schrauben in die dafür vorgesehene Schiene des Routers.

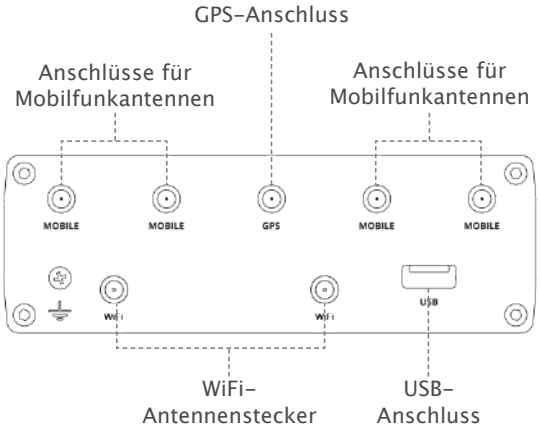
Beschreibung der Schnittstellen

Der I-NET-Router 512 verfügt über verschiedene Schnittstellen und Ports, um einen optimalen Internetzugang zu ermöglichen.

1. WiFi-Schnittstelle über 2 Anschlüsse auf der Rückseite für drahtlosen Internetzugang zwischen dem Router und einem Computer oder einem externen WiFi-Access-Point. Die WiFi-Schnittstelle ermöglicht den Zugriff auf die Web-Benutzeroberfläche des Routers und das Internet.
2. Mobile 5G/4G-Schnittstelle mit 4 Anschlüssen für den Anschluss von 4 MIMO-Antennen.
3. Ein GPS-Anschluss.
4. Ein USB-Anschluss
5. Ein WAN-Anschluss an der Vorderseite für den Zugang zum Internet über ein externes kabelgebundenes Netzwerk.
6. 4 LAN-Anschlüsse für die kabelgebundene Verbindung eines Computers mit dem Router I-NET 512.
7. Reset-Taste zum Zurücksetzen des Routers auf die Werkseinstellungen. Drücken und halten Sie die Taste 12 bis 60 Sekunden lang mit der mitgelieferten Nadel.
8. 2 SIM-Kartenleser.

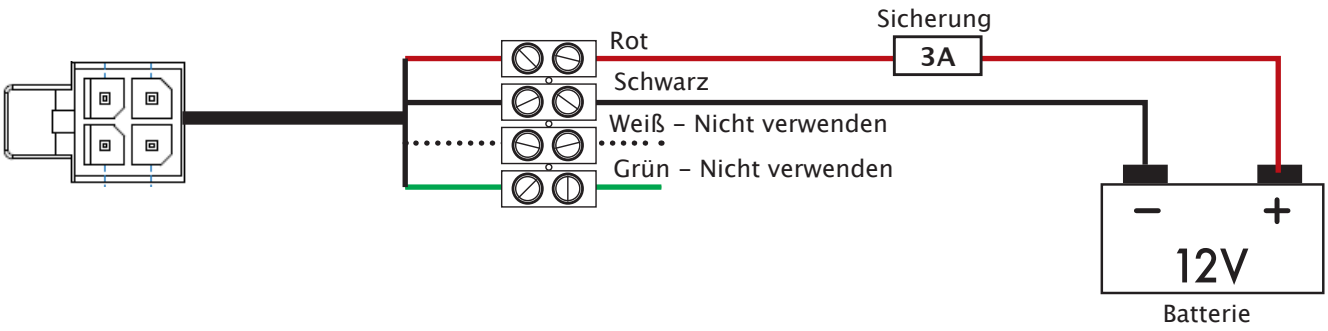


VORDERSEITE

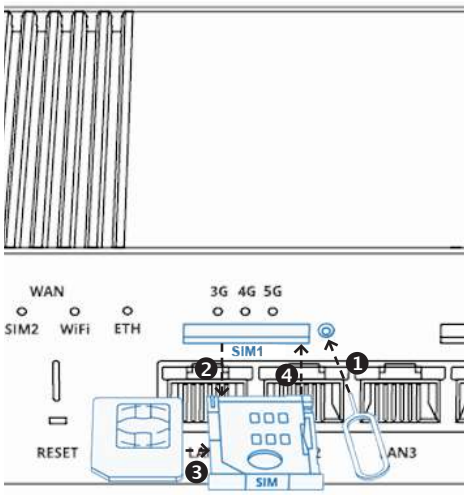


RÜCKSEITE

Pinbelegung des Netzstecker



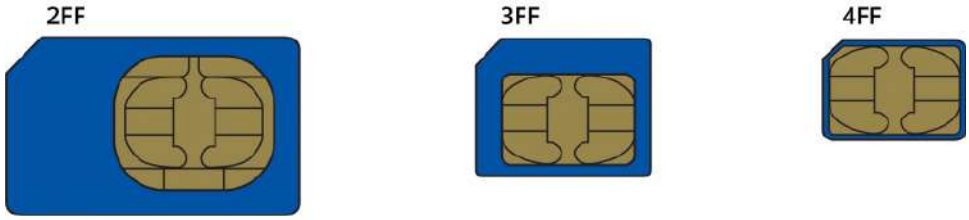
SIM-Karte I-NET 512



1. Drücken Sie auf die Taste an einem der beiden SIM-Kartenhalter mit der mitgelieferten SIM-Nadel, vorzugsweise SIM 1.
2. Nehmen Sie den SIM-Halter heraus.
3. Legen Sie Ihre SIM-Karte in den SIM-Steckplatz 1 ein. Verwenden Sie bei Bedarf einen der mitgelieferten Adapter.
4. Setzen Sie den SIM-Halter in den Router ein.
5. Befestigen Sie die Mobilfunk- und WiFi-Antennen. Sofern vorhanden, ziehen Sie die I-NET Außenantenne der Zimmerantennen vor.
6. Schließen Sie das 12-Volt-Kabel an die Buchse an der Vorderseite des Routers an :
   - Verbinden Sie den schwarzen Draht (-) mit der Masse.
   - Verbinden Sie den roten Draht (+) mit dem Pluspol der Batterie. Der + Draht muss mit einer 3A Sicherung abgesichert sein.

   Hinweis: Die grünen und weißen Drähte dürfen nicht verbunden werden.
7. Verbinden Sie sich mit der SSID des WiFi-Netzwerks des Geräts, indem Sie einen der beiden QR-Codes mit einem Smartphone scannen oder die Informationen auf der Vorderseite des Geräts verwenden. Für die Konfiguration mit einem PC bevorzugen Sie die Verwendung eines Ethernet-Kabels, das mit der LAN-Schnittstelle verbunden ist.

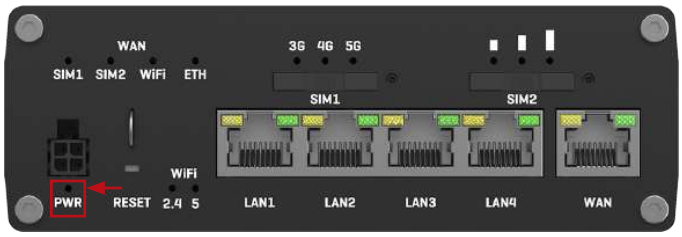
Das Gerät ist kompatibel mit Mini-SIM-Karten (2FF). Da jedoch verschiedene SIM-Kartentypen das gleiche Kontaktlayout haben, können auch kleinere SIM-Karten mit dem Router verwendet werden, sofern sie in einen 2FF-SIM-Kartenadapter eingesetzt werden. Eine Größenübersicht der gängigsten SIM-Kartentypen ist in der Abbildung unten zu sehen:



Beschreibung der Kontrolleuchten

Power LED

Die Power-LED befindet sich in der unteren linken Ecke der Vorderseite, direkt unter dem Stromanschluss.

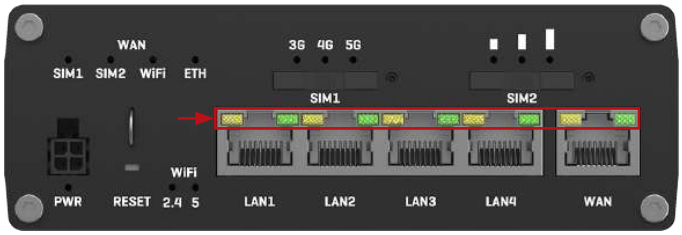


Es zeigt an, ob das Gerät eingeschaltet ist oder nicht.

Zustand	Beschreibung
LED eingeschaltet	Gerät ist eingeschaltet.
LED ausgeschaltet	Gerät ist nicht eingeschaltet.

Ethernet-Port-LEDs

Oben an jedem Ethernet-Port befinden sich zwei LEDs .

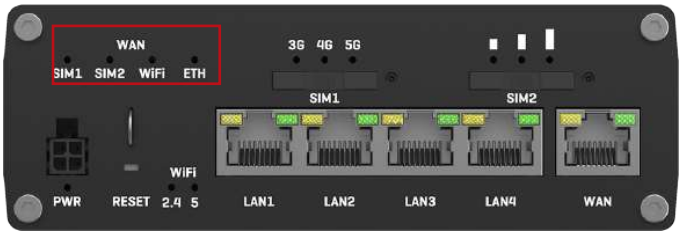


Sie geben Auskunft über die aktuellen Zustände der Ethernet-Ports. Jeder Port verfügt über zwei LEDs:
Orange – 10/100 Mbit/s-Verbindung
Grün – 1000 Mbit/s-Verbindung

Zustand	Beschreibung
LED an	Eine Datenverbindung am Port ist betriebsbereit (Kabel eingesteckt, Endgerät sichtbar, es werden keine Daten übertragen).
LED aus	Keine Datenverbindung am Port ist funktionsfähig (kein Kabel, defektes Kabel oder Endgerät aus einem anderen Grund nicht sichtbar (z. B. beschädigte Netzwerkkarte).
LED blinkt	Verbindung hergestellt und Daten werden über diesen Port übertragen.

WAN LEDs

Die WAN-LEDs befinden sich oben links auf der Vorderseite.

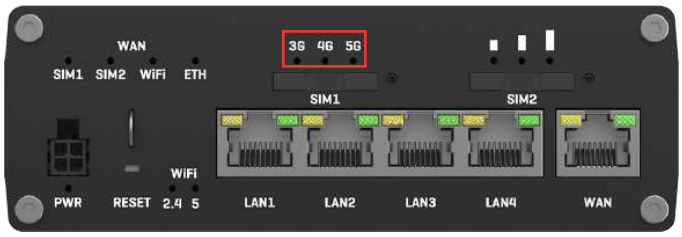


Sie zeigen an, welche Art von Internetverbindung gerade aktiv ist.

Zustand	Beschreibung
SIM1-LED leuchtet	Eine mobile Datenverbindung auf SIM1 ist aktiv.
SIM1-LED aus	Eine mobile Datenverbindung auf SIM1 ist inaktiv.
SIM2-LED leuchtet	Eine mobile Datenverbindung auf SIM2 ist aktiv.
SIM2-LED aus	Eine mobile Datenverbindung auf SIM2 ist inaktiv.
WLAN-LED leuchtet	Eine WLAN-Datenverbindung (WiFi WAN) ist aktiv.
WLAN-LED aus	Eine WLAN-Datenverbindung (WiFi WAN) ist inaktiv.
ETH LED an	Eine Ethernet-Datenverbindung (kabelgebundenes WAN) ist aktiv.
ETH-LED aus	Eine Ethernet-Datenverbindung (kabelgebundenes WAN) ist inaktiv.

LEDs für Mobilfunknetze

Die Mobilfunknetztyp-LEDs befinden sich oberhalb des SIM-Kartensteckplatzes.

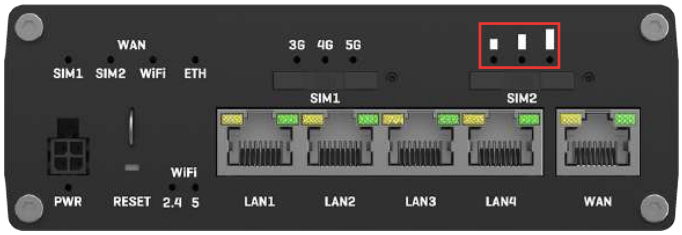


Sie zeigen an, welche Art von Internetverbindung gerade aktiv ist.

Aktion	Beschreibung
3G-LED leuchtet	Das Gerät ist mit einem 3G-Netzwerk verbunden.
4G-LED leuchtet	Das Gerät ist mit einem 4G-Netzwerk verbunden.
5G-LED leuchtet	Das Gerät ist über 5G SA mit einem 5G-Netzwerk verbunden.
4G- und 5G-LEDs leuchten	Das Gerät ist über 5G NSA verbunden.
3G blinkt	Das Gerät ist mit einem 3G-Netzwerk verbunden, hat aber keine IP-Adresse erhalten.
4G blinkt	Das Gerät ist mit einem 4G-Netzwerk verbunden, hat aber keine IP-Adresse erhalten.
5G blinkt	Das Gerät ist mit einem 5G-Netzwerk verbunden, hat aber keine IP-Adresse erhalten.
Alle LEDs blinken alle 500 ms gleichzeitig	Keine SIM-Karte oder falsche PIN.
Alle LEDs schalten sich nacheinander ein und aus	Das Gerät versucht, eine Verbindung zu einem Mobilfunknetzbetreiber herzustellen.

LEDs zur Anzeige der Mobilfunksignalstärke

Die LEDs zur Anzeige der Mobilfunksignalstärke befinden sich oberhalb des SIM2-Kartensteckplatzes.

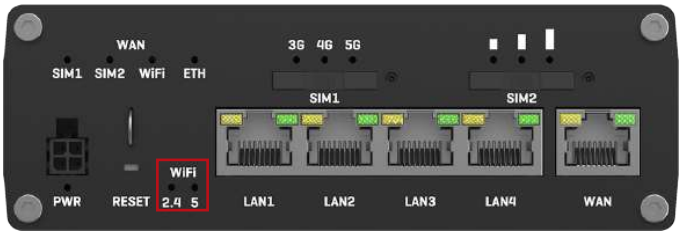


Die Anzahl der leuchtenden LEDs stellt einen unterschiedlichen RSSI -Wert (Mobile Signal Strength) in dBm dar.

Anzahl der leuchtenden LEDs	Wert der Signalstärke
0	≤ -111dBm
1	-110 dBm à -82 dBm
2	-81 dBm à -52 dBm
3	≥ -51dBm

WiFi-Band-LEDs

Die WLAN-Band-LEDs befinden sich unten an der Vorderseite des Geräts, links neben den Ethernet-Anschlüssen.

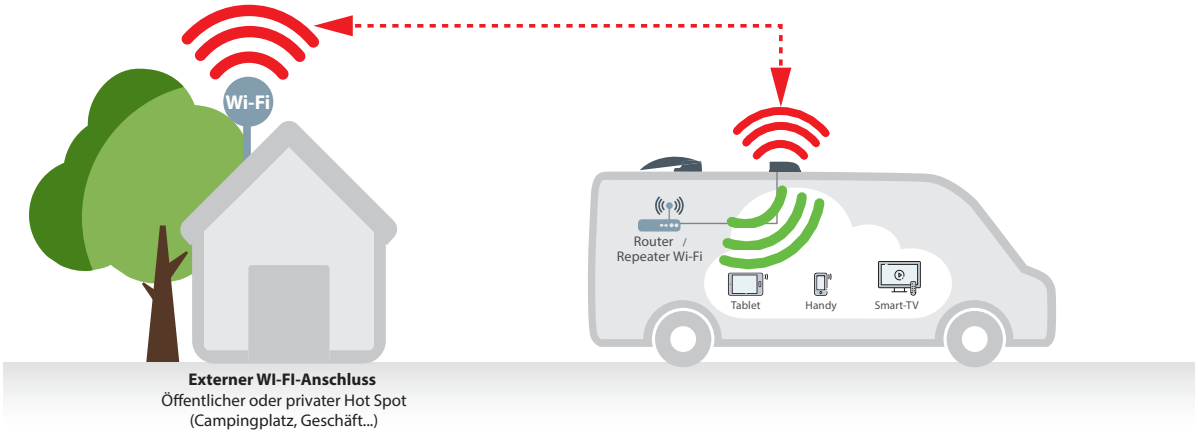


Sie zeigen an, ob ein WLAN Access Point (AP) auf einem bestimmten Band aktiv ist.

Zustand	Beschreibung
2.4 LED eingeschaltet.	Mindestens ein 2,4-GHz-Access Point läuft.
2.4 LED ausgeschaltet	Es sind keine 2,4-GHz-Access Points in Betrieb.
5 LED leuchtet	Mindestens ein 5-GHz-Access Point läuft.
5 LED ausgeschaltet	Es sind keine 5-GHz-Access Points in Betrieb.

Wi-Fi-Repeater

Der I-NET-Router 512 bietet die Möglichkeit, sich mit einem externen Wi-Fi-Netzwerk zu verbinden, um es lokal im Fahrzeug weiterzugeben, wodurch ein Wi-Fi-Repeater geschaffen werden kann.



Folgen Sie der "Konfiguration des Client-Modus", page 170, um Ihren eigenen Wi-Fi-Repeater (Clientstation) zu erstellen und so Datenvolumen auf Ihrer SIM-Karte zu sparen.

HINWEIS: Das externe WI-FI Netzwerk (Hot Spot) verfügt möglicherweise über Verbindungsrechte. Vergewissern Sie sich vorab, dass Sie sich kostenlos einloggen können. Falls dies nicht möglich ist, bitten Sie um Erlaubnis.

5G/4G/3G-Auswahl

Abhängig von der Qualität des 5G- oder 4G-Netzwerks kann der Router automatisch auf das 3G-Netzwerk umschalten. Wenn die Nutzung des 5G- oder 4G-Netzwerks zwingend erforderlich ist, kann dies im entsprechenden Menü festgelegt werden. Stellen Sie einfach die Einstellung „Network type“ im Menü Netzwerk-> Mobile-> Allgemein-> SIM-Karteneinstellungen auf „Nur 4G (LTE)“ um. Vergessen Sie nicht, auf die Schaltfläche „Speichern und übernehmen“ zu klicken.

Siehe Kapitel „2.1.1 Menü Netzwerk > Mobile > Allgemein“, S. 26, um die Verwendung eines 3G oder 4G-Netz zu verwenden

Manuelle Auswahl des Netzbetreiber

In bestimmten Anwendungsfällen (z. B. im Ausland) kann es notwendig sein, den Mobilfunkanbieter für ihre SIM-Karte manuell auszuwählen.
Siehe Kapitel ""2.1.3 Menü Netzwerk > MOBILE > Network Operators", page 137, um die Verwendung eines 3G- oder 4G-Netzes zu erzwingen.

Benutzeroberfläche Normal /Erweitert

Die Benutzeroberfläche des Routers verfügt über zwei Modi: Normal und Erweitert. Einige Funktionen sind nur zugänglich, wenn der Modus "Fortgeschritten" ausgewählt ist. Klicken Sie auf die Schaltfläche in der oberen rechten Ecke der Router WEB-Oberfläche, um vom Modus "Basic" in den Modus "Fortgeschritten" zu wechseln.

Netzwerkmanagement

Der Zweck dieses Moduls ist es, dem Benutzer einen Internetzugang zu garantieren, wenn mindestens eine der Schnittstellen funktionsfähig ist. Standardmäßig ist das Modul Netzwerkverwaltung aktiviert.
Siehe Kapitel "2.5 Menü Netzwerk > Failover 175", page 110.

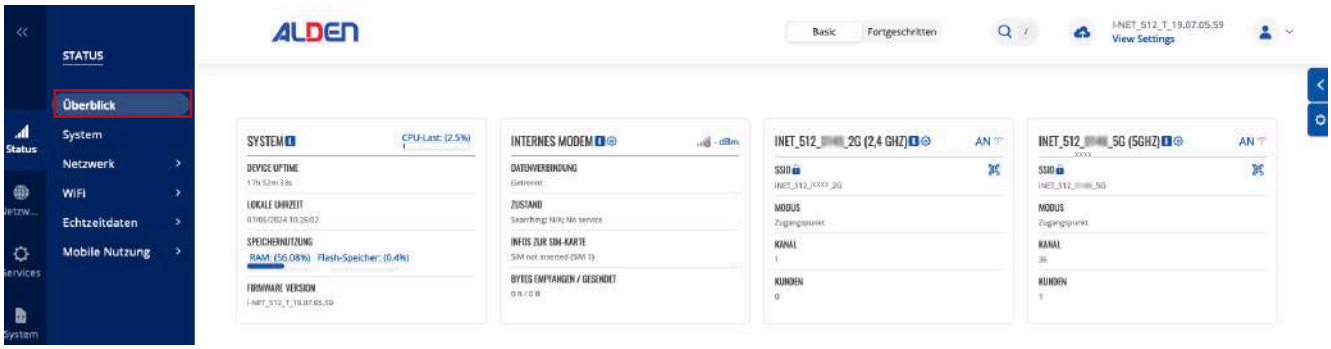
Schnelle Installation

Bei der ersten Inbetriebnahme werden Sie aufgefordert, die wichtigsten Parameter einzugeben, um Ihren Router einzurichten. Es ist Pflicht, alle Schritte dieser Einrichtung zu bestätigen. Vergessen Sie nicht, den PIN-Code Ihrer SIM-Karte einzugeben. Wenn Sie sich bei einem vorgeschlagenen Parameter nicht sicher sind, bestätigen Sie den angezeigten Vorschlag.

1. Menü - STATUS

1.1. Menü - STATUS > ÜBERBLICK

Die Übersichtsseite enthält Widgets, die den Status verschiedener Systeme im Zusammenhang mit dem Gerät anzeigen. Die folgende Abbildung ist ein Beispiel für die Übersichtsseite:



Modem Widget

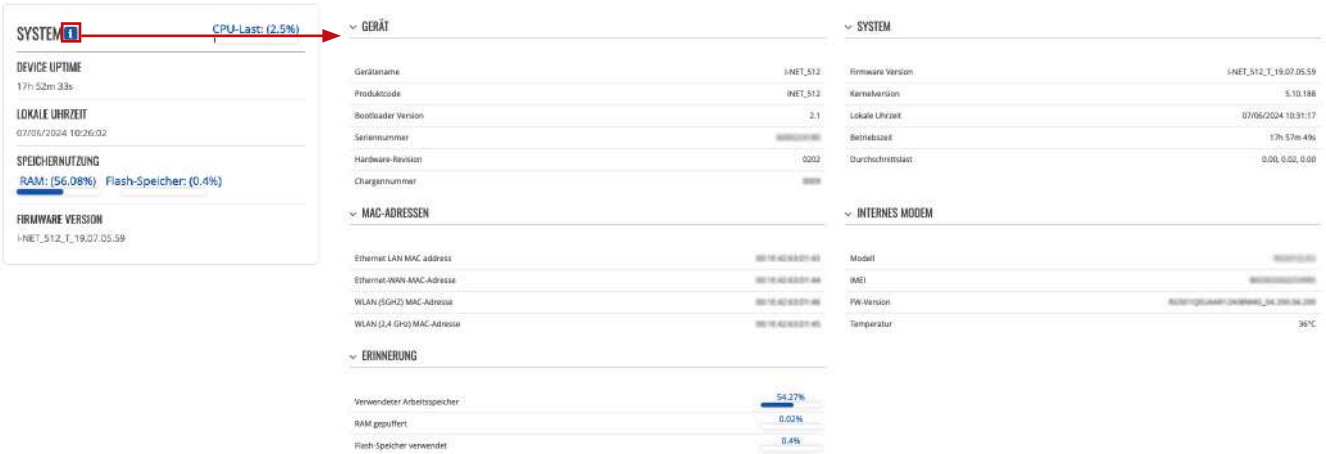
Das Modem- Widget zeigt Informationen zur Mobilfunkverbindung und zur aktuellen Signalstärke an ( ). Jeder gefüllte Balken repräsentiert einen anderen RSSI-Wert:

Riegel	Signalstärkewert / RSSI (in dBm)
0	≤ -111
1	-110 bis -97
2	-96 bis -52
3	≥ -51

Das gleiche Berechnungsprinzip gilt für die Signalstärke-LEDs an Ihrem Gerät. Weitere Informationen zu Signalstärkewerten und verschiedenen Messungen finden Sie hier.

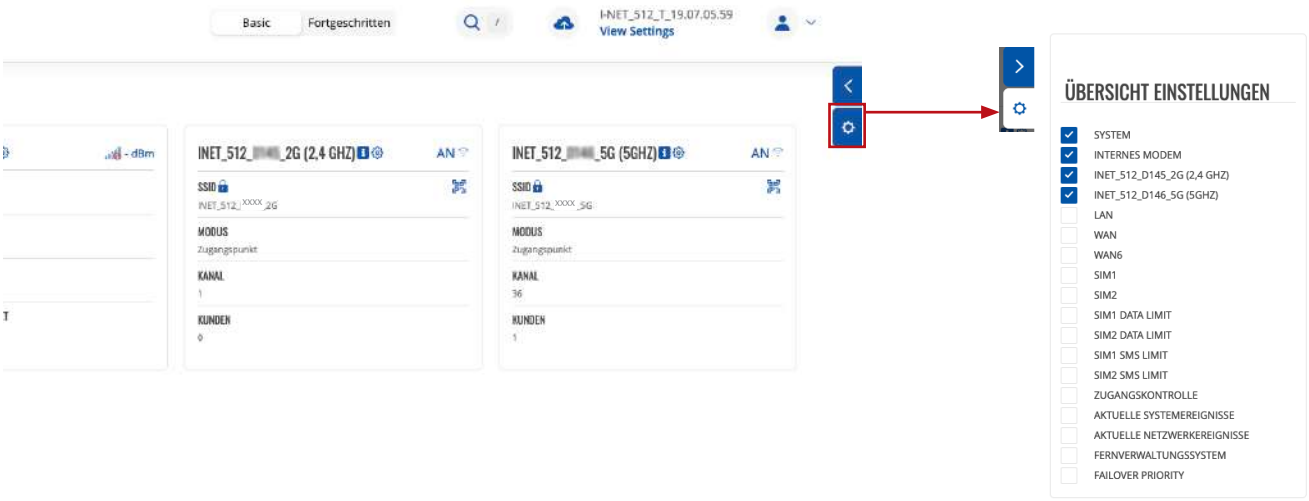
Widget Info-Button

Die Info- Schaltfläche ( ) befindet sich neben dem Namen einiger Widgets. Durch Klicken auf die Info-Schaltfläche wird der Benutzer zu einer Statusseite weitergeleitet, die sich auf die angezeigten Informationen des Widgets bezieht. Wenn Sie beispielsweise auf die Schaltfläche Info im System-Widget klicken, wird der Benutzer auf die Seite Status → System weitergeleitet



Hinzufügen von mehr Widgets

Eine Reihe von Standard-Widgets wird auf der Seite "Übersicht" angezeigt, aber weitere können hinzugefügt werden, indem Sie auf die Schaltfläche ⚙ "Übersicht Einstellungen" rechts auf der Webseite klicken. Von dort aus können Sie andere Widgets als die Standard-Widgets hinzufügen.

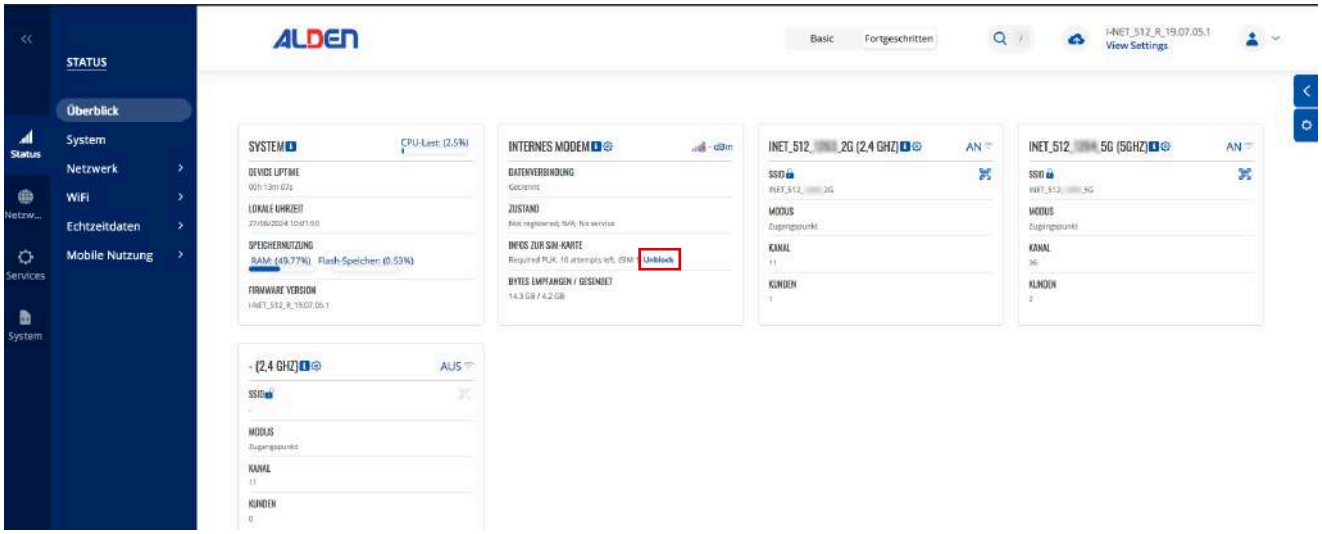


SIM-Karte entsperren - PUK-Code

Der PUK-Code (Personal Unblocking Key) ist ein aus 8 Ziffern bestehender Notfallcode, mit dem Sie Ihre SIM entsperren können, wenn Sie dreimal hintereinander einen falschen PIN-Code angegeben haben.

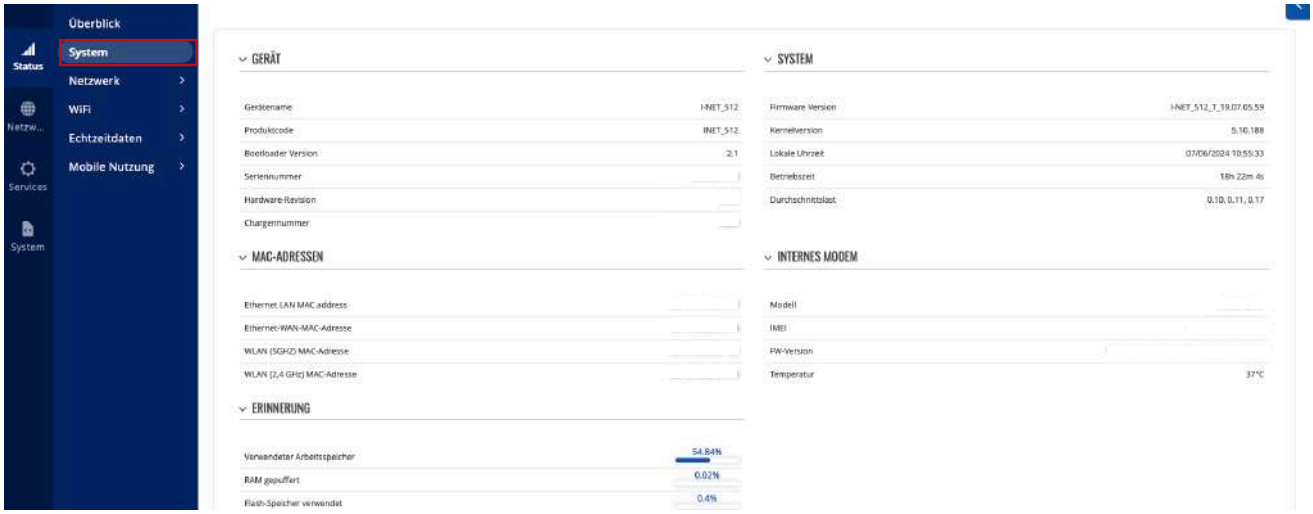
Sie finden ihn auf dem Begleitdokument Ihrer SIM-Karte. Sie kann Ihnen auch vom Kundenservice Ihres Mobilfunkanbieters mitgeteilt werden. Sie haben 10 Versuche, diesen PUK-Code einzugeben.

Der PUK-Code kann eingegeben werden, indem Sie auf den blau angezeigten Link "Unblock" klicken.



1.2 Menü STATUS > SYSTEM

Auf der Systemseite werden allgemeine Informationen zur Hardware, Software und zum Speicherstatus des Geräts angezeigt. Dieses Kapitel des Benutzerhandbuchs bietet einen Überblick über die Systemseite des I-NET 512.
Die folgende Abbildung ist ein Beispiel der Systemseite und die folgende Tabelle enthält Informationen zu den Feldern, die auf dieser Seite angezeigt werden:



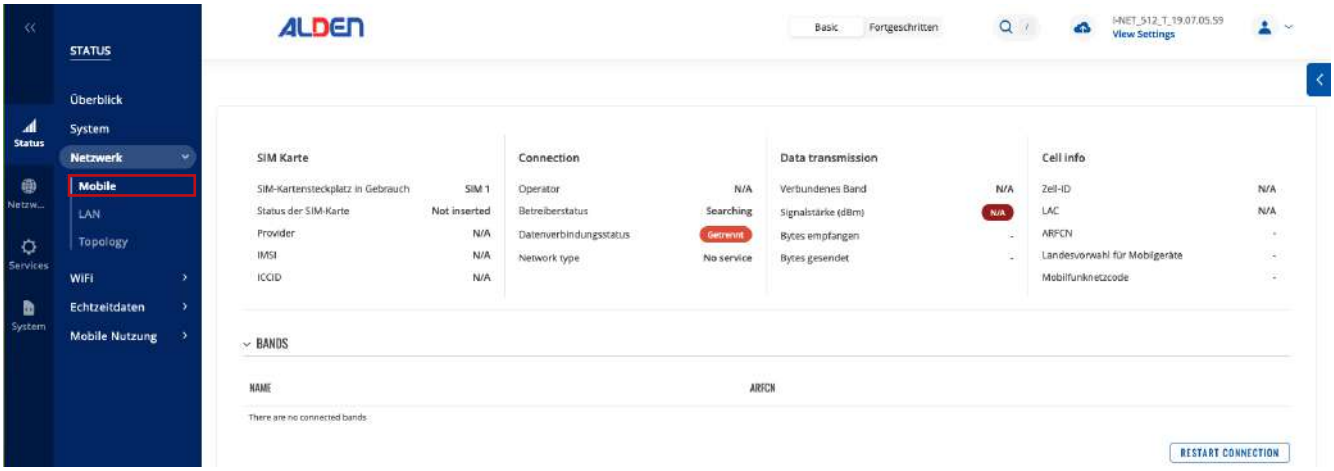
Feldname	Beschreibung
Gerätename	Name des Geräts.
Produktcode	Auch bekannt als Bestellcode; zeigt an, unter welchem Produktcode das Gerät hergestellt wurde. Unterschiedliche Produktcodes weisen auf unterschiedliche Versionen des Gesamtprodukts hin. Beispielsweise können Geräte mit unterschiedlichen Produktcodes unterschiedliche LTE-Bänder unterstützen, mit unterschiedlichem Zubehör, unterschiedlicher Firmware usw. geliefert werden.
Bootloader Version	Aktuell vom Gerät verwendete Bootloader-Version. Ein Bootloader ist ein Programm, das das Betriebssystem lädt.
Seriennummer	Eine eindeutige 10-stellige Gerätekennung. Diese ist erforderlich, wenn das Gerät mit dem Remote Management System (RMS) verbunden wird. Das Gerät kann über die Seite Dienstleistungen → Cloud-Lösungen → RMS zu RMS hinzugefügt werden.
Hardware-Revision	Eine 4-stellige Nummer, die die Hardwareversion des Routers darstellt.
Chargennummer	Eine 4-stellige Nummer, die die Materialcharge angibt.
Firmware Version	Aktuell vom Gerät verwendete Firmware-Version. Die Firmware kann auf der Seite System → Firmware aktualisiert werden.
Kernelversion	Aktuell vom Gerät verwendete Kernel-Version. Ein Kernel ist ein Computerprogramm, das für die Verbindung der Software eines Geräts mit seiner Hardware verantwortlich ist.
Lokale Uhrzeit	Aktuelle Zeit, wie sie vom Gerät wahrgenommen wird. Die Zeiteinstellungen können auf der Seite System → Setup-Assistent eingestellt werden.
Betriebszeit	Zeit, die vergangen ist, seitdem das Gerät zuletzt eingeschaltet oder neu gestartet wurde.
Durchschnittslast	Durchschnittliche CPU-Auslastung (in %) über die letzte Minute, 5 Minuten und 15 Minuten.
Ethernet LAN MAC address	MAC-Adresse der LAN-Schnittstelle.
Ethernet-WAN-MAC-Adresse	MAC-Adresse der WAN-Schnittstelle.
WLAN (5GHZ) MAC-Adresse	MAC-Adresse der 5-GHz-Funkschnittstelle.
WLAN (2,4 GHz) MAC-Adresse	MAC-Adresse der 2,4-GHz-Funkschnittstelle.
Modell	Modellnummer des Modems im Gerät.
IMEI	Die IMEI (International Mobile Equipment Identity) ist eine eindeutige Nummer mit 15 Dezimalziffern, die zur Identifizierung mobiler Module verwendet wird. GSM-Netzbetreiber verwenden die IMEI, um Geräte in ihren Netzen zu identifizieren.
FW-Version	Firmware-Version des Modems im Gerät.
Temperatur	Aktuelle Temperatur des Modems.
Verwendeter Arbeitsspeicher	Größe des Direktzugriffsspeichers (RAM), der von temporär gespeicherten Daten verwendet wird, bevor sie an einen anderen Ort verschoben werden.
RAM gepuffert	Menge der über die mobile Schnittstelle empfangenen Daten.
Flash-Speicher verwendet	Menge der über die mobile Schnittstelle gesendeten Daten.

1.3 Menü STATUS > NETZWERK

Die Seite Netzwerk enthält Informationen über die Vernetzung des Geräts. Dieses Kapitel gibt einen Überblick über die Netzwerkseite in I-NET 512 Geräten.

1.3.1 Menü STATUS > NETZWERK > MOBILE

Auf der Registerkarte Mobile werden Informationen zur mobilen Verbindung angezeigt. Die folgende Abbildung ist ein Beispiel für die Registerkarte „Mobile“:



SIM-Kartensteckplatz in Gebrauch	Zeigt an, welcher SIM-Kartensteckplatz derzeit verwendet wird
Status der SIM-Karte	Der aktuelle Status der SIM-Karte. Mögliche Werte sind: • Inserted/**Eingelegt** – Die SIM-Karte ist eingelegt und einsatzbereit • Not inserted/**Nicht eingelegt** – SIM-Karte ist nicht eingelegt • Unknown/**Unbekannt** – Statuswert der SIM-Karte konnte nicht ermittelt werden. Mögliches Kommunikationsproblem zwischen dem Gerät und dem Modem
Provider	Name des Netzbetreibers
IMSI	Die IMSI (International Mobile Subscriber Identity) ist eine eindeutige Nummer mit 15 Dezimalstellen (oder weniger), die zur Identifizierung des Benutzers eines Mobilfunknetzes verwendet wird
ICCID	ICCID der SIM-Karte – eine eindeutige Seriennummer zur Identifizierung des SIM-Chips
Operator	Name des Netzbetreibers
Betreiberstatus	Zeigt an, ob das Netzwerk aktuell die Registrierung des Mobilgeräts angezeigt hat. Mögliche Werte sind: • **No registred** – nicht bei einem Netzwerk registriert und das Gerät sucht derzeit nicht nach einem neuen Betreiber, bei dem es sich registrieren kann • **Registred** (Heim) – registriert, Heimnetzwerk • **Searching** – nicht bei einem Netzwerk registriert, aber das Gerät sucht derzeit nach einem neuen Betreiber, bei dem es sich registrieren kann • **Denied** – Registrierung im Netzwerk vom Betreiber verweigert • **Unknow** – Der Betreiberstatus ist derzeit unbekannt • **Registred** (Roaming) – im Netzwerk registriert, Roaming-Bedingungen
Datenverbindungsstatus	Gibt an, ob das Gerät über eine mobile Datenverbindung verfügt oder nicht.
Network type	Zeigen Sie Zwischenstadien beim Aufbau einer Mobilfunkverbindung an.
Verbundenes Band	Derzeit verwendetes Mobilfunkfrequenzband.
Signalstärke (dBm)	Indikator für die empfangene Signalstärke (RSSI), gemessen in dBm. Werte näher bei 0 weisen auf eine bessere Signalstärke hin
Bytes empfangen	Über die mobile Schnittstelle empfangene Datenmenge
Bytes gesendet	Menge der über die mobile Schnittstelle gesendeten Daten
Zell-ID	Die ID der Zelle, mit der das Modem derzeit verbunden ist
LAC	LAC Der Location Area Code, abgekürzt LAC, ist die eindeutige Nummer, die jedem Standortbereich innerhalb des Netzwerks zugewiesen wird. Der versorgte Bereich eines Mobilfunkzugangsnetzes ist üblicherweise in Standortbereiche unterteilt, die aus einer oder mehreren Funkzellen GSM/3G bestehen

ARFCN	In Mobilfunknetzen ist eine absolute Funkfrequenzkanalnummer (ARFCN) ein Code, der ein Paar physischer Funkträger angibt, die zum Senden und Empfangen in einem Landmobilfunksystem verwendet werden, einer für das Uplink-Signal und einer für das Downlink-Signal.
Landesvorwahl für Mobilgeräte	Der Mobile Country Code, abgekürzt MCC, ist der Code, der das Heimatland eines Mobilfunknetzbetreibers (MNO) eindeutig identifiziert.
Mobilfunknetzcode	Der Mobile Network Code (MNC) ist eine eindeutige zwei- oder dreistellige Nummer, die zur Identifizierung eines heimischen Public Land Mobile Network (PLMN) verwendet wird. MNC wird von der nationalen Regulierungsbehörde zugewiesen.
Restart connection	Starten Sie die Modemverbindung neu.

1.3.2 Menü STATUS > NETZWERK > LAN

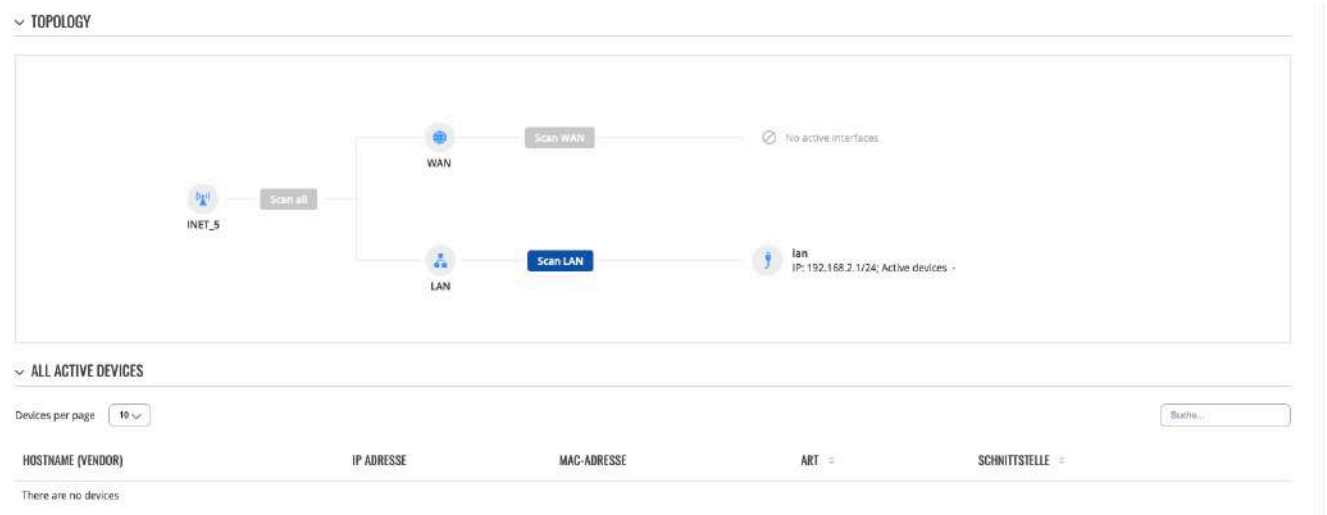
Dieser Tab zeigt Informationen über das/die lokale(n) Netzwerk(e) des Geräts an.

LAN-Informationen	
Name	Name der LAN-Schnittstelle
IP Adresse	IP-Adresse der LAN-Schnittstelle
Netzmaske	Netzmaske der LAN-Schnittstelle. Eine Netzmaske gibt gewissermaßen die Größe eines Netzwerks an. Mit anderen Worten: Es gibt an, welcher Teil der IP-Adresse das Netzwerk und welcher das Gerät bezeichnet

DHCP-Leases	
Hostname	Hostname eines LAN-Clients
IP Adresse	IP-Adresse eines LAN-Clients
MAC-Adresse	MAC-Adresse eines LAN-Clients
Verbleibende lease time	Der Mobile Network Code (MNC) ist eine einzigartige zwei- oder dreistellige Nummer, die zur Identifizierung eines nationalen öffentlichen Mobilfunknetzes (PLMN) verwendet wird. Der MNC wird von der nationalen Regulierungsbehörde vergeben.

1.3.3 Menü STATUS > NETZWERK > TOPOLOGY

Die Registerkarte „Topologie“ ermöglicht das Scannen von WAN, LAN oder beiden Schnittstellen per ARP-Scan, um aktiv verbundene Geräte zu überprüfen. Nach dem Scan wird angezeigt, wie viele aktive Geräte gefunden wurden und an welcher Schnittstelle.



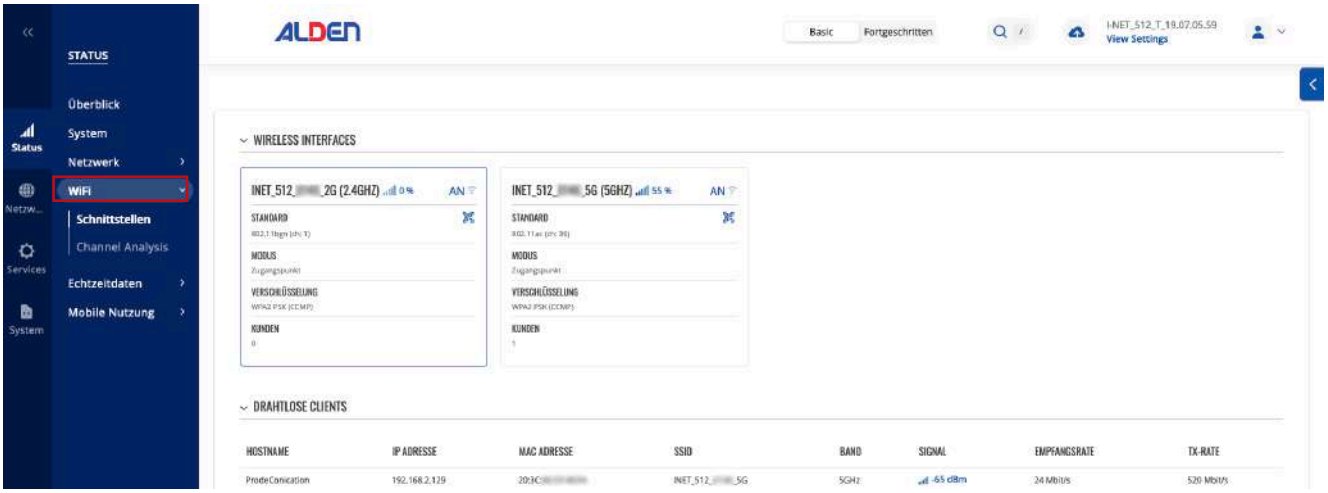
Feldname	Beschreibung
Hostname (Vendor)	Hostname des gescannten Geräts
IP Adresse	IP-Adresse des gescannten Geräts
MAC-Adresse	MAC-Adresse des gescannten Geräts
Art	Die Art der Verbindung
Schnittstelle	Die Schnittstelle, mit der das gescannte Gerät verbunden ist

1.4 Menü STATUS > WiFi

Die Seite "Wireless" enthält Diagramme, die verschiedene Echtzeitänderungen der drahtlosen Daten anzeigen.

1.4.1 Menü STATUS > WiFi > SCHNITTSTELLEN

Die Seite "Interfaces" zeigt Informationen zu allen drahtlosen Schnittstellen und den mit dem Gerät verbundenen Clients an.



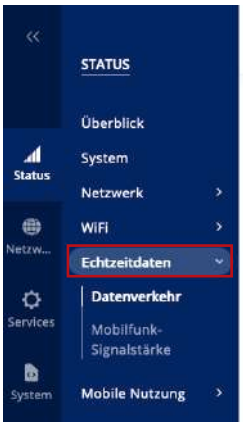
Feldname	Beschreibung
Modus	Verbindungsmodus. Kann ein Zugangspunkt (AP) oder ein Client sein. Im AP-Modus können sich andere Personen mit dem WiFi dieses Routers verbinden. Im Client-Modus verbindet sich der Router mit anderen WiFi-Netzwerken.
Verschlüsselung	Verwendeter WiFi-Verschlüsselungstyp.
Hostname	Hostname des Geräts.
IP Adresse	Zeigt die dem Gerät zugewiesene IP-Adresse an.
Mac Adresse	MAC-Adresse (Media Access Control) des Geräts.
SSID	Die SSID (Service Set Identifier) ist der Name des WiFi-Netzwerks.
Band	Verwendete Frequenz.
Signal	Empfangssignalstärkeanzeige (RSSI). Signalstärke gemessen in dBm.
Empfangsrate	Rate, mit dem Pakete von der verbundenen Schnittstelle empfangen werden.
TX-Rate	Übertragungsrate, mit der Pakete an die verbundene Schnittstelle gesendet werden.

1.4.2 Menü STATUS > WiFi > CHANNEL ANALYSIS

Der Abschnitt "Kanalzuweisung" zeigt ein interaktives Diagramm der Kanalstörungsfunkbänder, das die Kanalzuweisung in Echtzeit in der Umgebung anzeigt.

Im Abschnitt Scan wird eine Tabelle mit den sichtbaren Drahtlosnetzwerken angezeigt. Die Tabelle kann nach SSID, Signalstärke, Kanal, Breite, Verschlüsselung und MAC-Adresse (BSSID) sortiert werden. Beispiel oben.

1.5 Menü STATUS > ECHTZEITDATEN >



Die Seite „Echtzeitdaten“ enthält verschiedene Diagramme, die verschiedene statistische Datenänderungen in Echtzeit anzeigen.

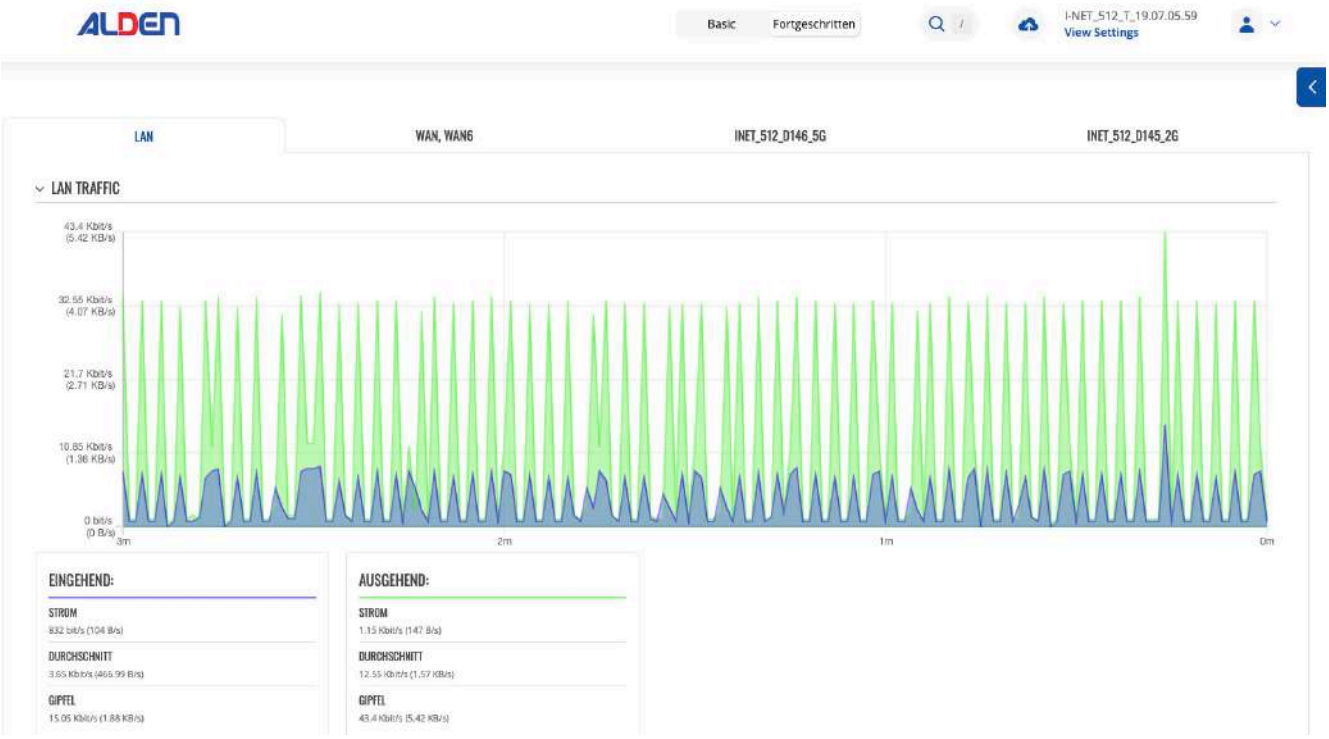
Dieses Kapitel des Benutzerhandbuchs bietet einen Überblick über die Seite „Echtzeitdaten“ für das I-NET 512.

1.5.1 Menü STATUS > ECHTZEITDATEN > DATENVERKEHR

Die Echtzeit-Transferdiagramme bieten Benutzern die Möglichkeit, den durchschnittlichen eingehenden und ausgehenden Datenverkehr über einen Zeitraum von 3 Minuten zu überwachen. Jede neue Messung wird alle 3 Sekunden durchgeführt. Die Diagramme bestehen aus zwei farbcodierten Diagrammen: Das grüne Diagramm zeigt den ausgehenden Datenverkehr, das blaue Diagramm den eingehenden Datenverkehr. Obwohl nicht grafisch dargestellt, zeigt die Seite auch Spitzenlasten und Durchschnittswerte des ein- und ausgehenden Datenverkehrs an.

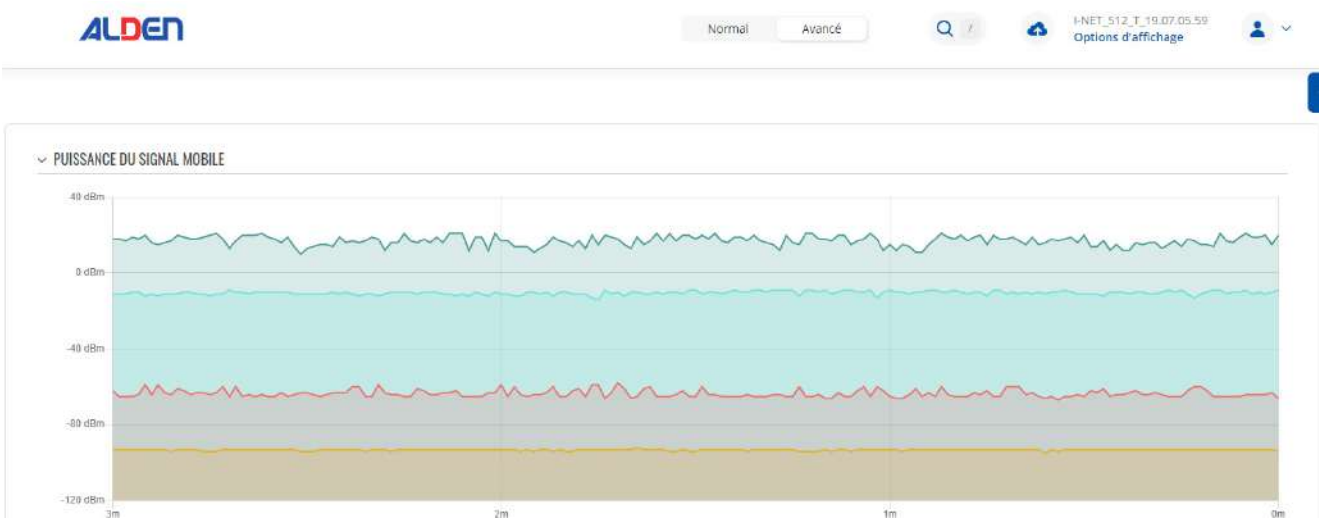
Graph	Beschreibung
I-NET_512_XXXX_5G	Zeigt den Datenverkehr, der über die WLAN-Verbindung läuft, in Diagrammform an
I-NET_512_XXXX_2G	Zeigt den Datenverkehr, der über die WLAN-Verbindung läuft, in Diagrammform an
LAN	Zeigt den Datenverkehr, der über die LAN-Netzwerkschnittstelle(n) läuft, in Diagrammform an
WAN, WAN6	Zeigt den Datenverkehr, der über die kabelgebundene WAN-Verbindung läuft, in Diagrammform an

Die folgende Abbildung ist ein Beispiel für das Echtzeit-Transferdiagramm für die LAN-Verbindung:

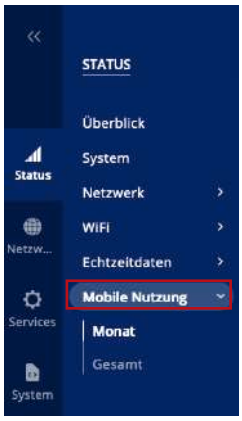


1.5.2 Menü STATUS > ECHTZEITDATEN > MOBILFUNK-SIGNALSTÄRKE

Das Diagramm Mobilfunk-Signalstärke zeigt die Veränderung des Wertes für die Stärke des Zellsignals im Laufe der Zeit an.



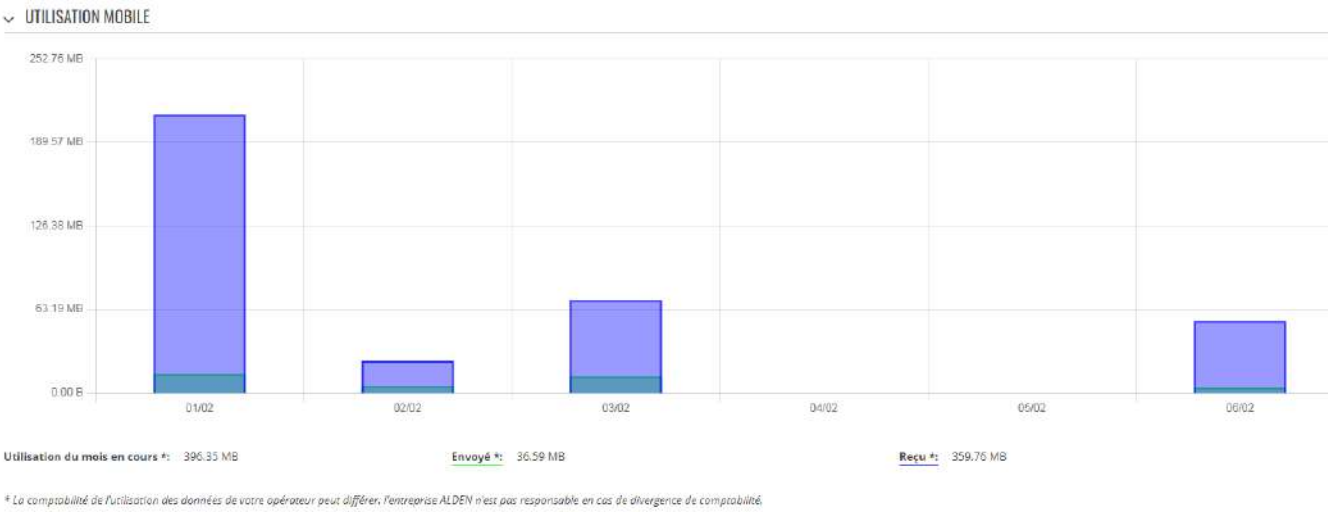
1.6 Menü STATUS > MOBILE NUTZUNG



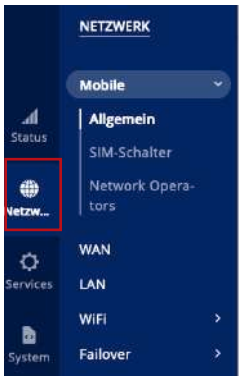
Die Seite Mobile Nutzung enthält Diagramme, die mobile Datennutzungswerte über verschiedene Zeiträume anzeigen.

Sie können verschiedene Seiten aufrufen, um die Werte der mobilen Datennutzung über verschiedene Zeiträume anzuzeigen.

Monat – monatliche Datennutzungswerte
Gesamt – Datenverbrauch für den gesamten Überwachungszeitraum



2. Menü NETZWERK



Wenn Sie Probleme haben, diese Seite oder einige der hier beschriebenen Parameter auf der WebUI Ihres Geräts zu finden, sollten Sie den Modus „Fortgeschrittene WebUI“ aktivieren. Sie können dies tun, indem Sie auf die Schaltfläche „Basic“ unter „Modus“ klicken, die sich in der oberen rechten Ecke der WebUI befindet.

2.1 Menü NETZWERK > MOBILE

Die Seite Mobile wird verwendet, um mobile Verbindungseinstellungen zu konfigurieren.

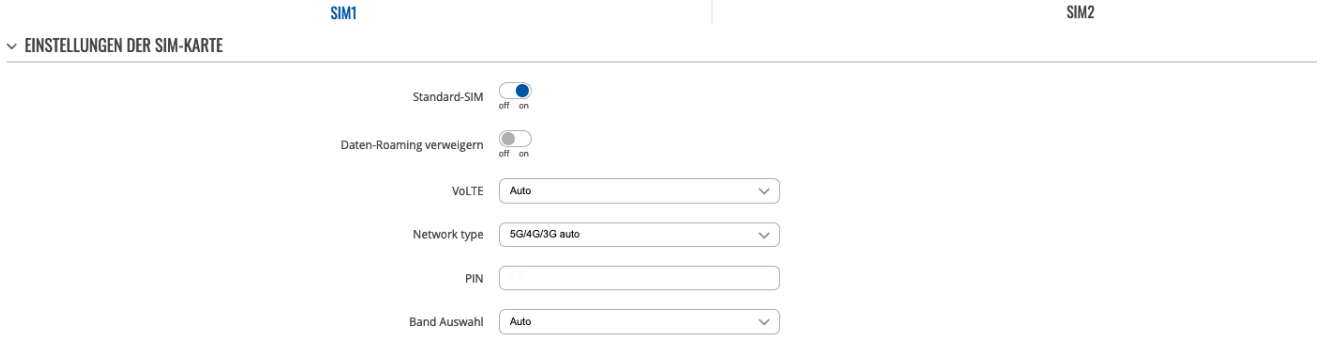
2.1.1 Menü NETZWERK > MOBILE > ALLGEMEIN

Der Abschnitt Allgemein wird verwendet, um SIM-Kartenparameter zu konfigurieren, die definieren, wie das Gerät eine mobile Verbindung herstellt.
Diese Seite des Handbuchs bietet einen Überblick über die Seite Mobile in I-NET 512-Geräten.

Einstellungen der SIM-Karte

Der Abschnitt SIM-Karteneinstellungen wird verwendet, um die wichtigsten Parameter der SIM-Karte zu konfigurieren. Informationen zu den in diesem Abschnitt enthaltenen Feldern finden Sie in der folgenden Abbildung und Tabelle.

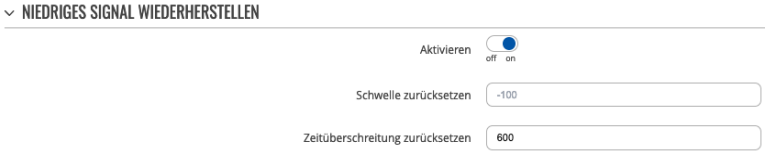
Wenn die SIM-Karte nach der Eingabe von 3 falschen PIN-Codes gesperrt ist, siehe"PUK-Code", page 114



Standard-SIM	Off | On ; Standard : On	Legt diesen SIM-Steckplatz als Standard fest.
Daten-Roaming verweigern	Off | On ; Standard : Off	Verweigert die Datenverbindung unter Roaming-Bedingungen.
VoLTE	Auto | An | Aus ; Standard : Auto	Ermöglicht Voice over LTE, eine digitale Pakettechnologie, die 4G LTE-Netzwerke nutzt, um Sprachverkehr weiterzuleiten und Daten zu übertragen.
Network type	5G/4G/3G auto | 4G/3G auto | 4G only | 3G only ; Standard : 5G/4G/3G auto	Präferenz für den Netzwerkverbindungstyp.
PIN	Standard : keine	Die PIN (Personal Identification Number) der SIM-Karte ist ein geheimes numerisches Passwort, das verwendet wird, um das Gerät gegenüber der SIM-Karte zu authentifizieren. PIN-Codes bestehen nur aus Zahlen und können zwischen 4 und 8 Zeichen lang sein. Die PIN-Nummer wird im Flash- Speicher gespeichert und wird daher nicht zurückgesetzt, wenn die Standardeinstellungen wiederhergestellt werden.
Band Auswahl	Auto | Manuell Standard : Auto	Methode zur Auswahl des Netzwerkfrequenzbands. Bei der Einstellung „ Auto“ verbindet sich das Gerät mit dem Band mit den besten Konnektivitätsbedingungen, während „Manuell“ die Möglichkeit bietet, manuell die Bänder auszuwählen, die das Gerät verwenden muss. Bei der manuellen Auswahl von Bändern werden deren Duplexmodi nur für 4G- und 5G-fähige Geräte angezeigt.

Niedriges Signal erneut verbinden

Der Abschnitt „Niedriges Signal erneut verbinden“ wird verwendet, um das Zurücksetzen der Modembetreiberverbindung basierend auf der Signalstärke für die angegebene SIM-Karte zu konfigurieren.



Feld	Wert	Beschreibung
Aktivieren	Off | On; Standard : Off	Ermöglicht die Wiederverbindung bei niedrigem Signal.
Schwelle zurücksetzen	Ganzzahl [-120..-50] ; Standard : keine	Signalschwelle in dB für die Verbindung. Wenn das Signal unter diesem Wert liegt, setzt das Modem die Verbindung zurück.
Zeitüberschreitung zurücksetzen	Ganzzahl [15..65535] ; Standard : 600	Zeit in Sekunden, die das Gerät wartet, bevor es erneut versucht, die Verbindung zurückzusetzen.

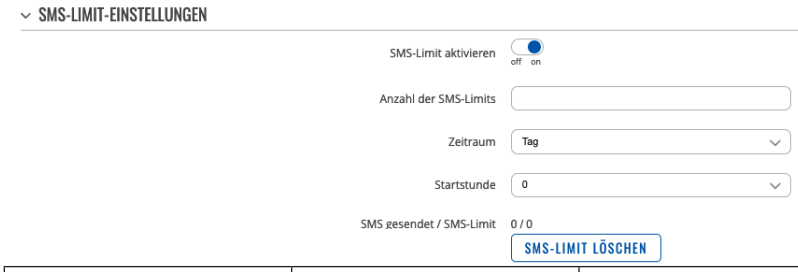
Betreibereinstellungen

Im Abschnitt Betreibereinstellungen wird konfiguriert, welche Betreiber zugelassen (Whitelist) oder blockiert (Blacklist) werden können.

Feld	Wert	Beschreibung
Aktivieren	Off | On; Standard : Off	Aktiviert Whitelist oder Blacklist für die angegebene Betreiberliste.
Modus	Weiße Liste | Schwarze Liste; Standard: Weiße Liste	Modus, der für die Bedienerliste angewendet werden soll. • Weiße Liste – nur Betreiber in der Liste zulassen • Schwarze Liste – Sperren Sie alle Betreiber in der Liste
Betreiberliste	Betreiberliste; Standard: keine	Eine Liste von Betreiber, die auf der Seite Betreiber List konfiguriert werden können.

SMS-Limit-Einstellungen

Der Abschnitt SMS-Limit-Einstellungen bietet Ihnen die Möglichkeit, eine Obergrenze für gesendete SMS-Nachrichten für Ihre SIM-Karte einzurichten.

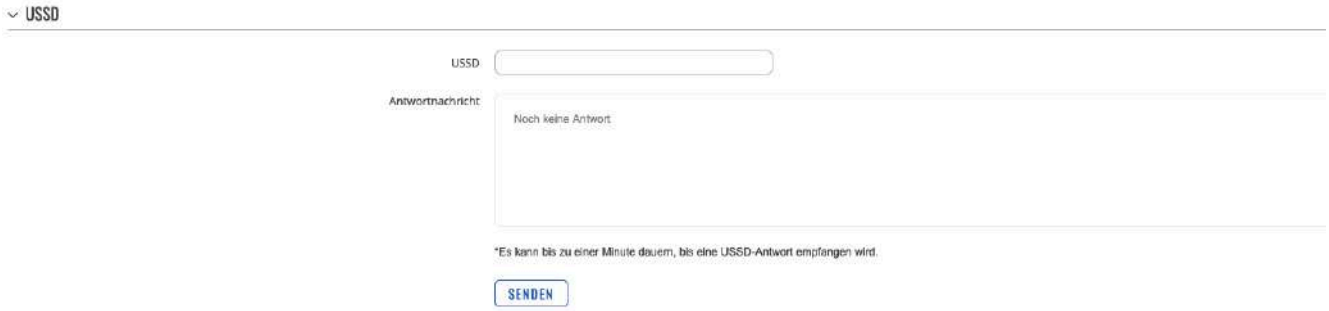


Feld	Wert	Beschreibung
SMS-Limit aktivieren	Off | On ; Standard : Off	Schaltet die SMS-Begrenzung ein oder aus.
Anzahl der SMS-Limits	Ganzzahl; Standard: keine	Legt das SMS-Sendelimit fest, d.h. wie viele SMS-Nachrichten können von dieser SIM-Karte während des angegebenen Zeitraums gesendet werden.
Zeitraum	Tag | Woche | Monat; Standard: Tag	Zeitraum, für den die SMS-Begrenzung gelten soll. Nach Ablauf des Zeitraums wird der SMS- Limit-Zähler zurückgesetzt.
Startstunde	0-23 / Montag - Sonntag / 0-31; Standard: 0	Startzeit des Tages / Wochentags / Monatstags für SMS-Beschränkungszeitraum.
SMS gesendet / SMS-Limit	Interaktive Schaltfläche	Löscht den SMS-Limit-Zähler für den ausgewählten Zeitraum.

USSD

Unstrukturierte Zusatzdienstdaten (Unstructured Supplementary Service Data, USSD) ist ein Kommunikationsprotokoll, das bei der Kommunikation zwischen zellularen Geräten und Mobilfunknetzbetreibern verwendet wird. Es wird normalerweise bei Prepaid-SIM-Karten verwendet, um bestimmte Dienste zu aktivieren/deaktivieren oder um Informationen von einem Netzbetreiber zu erhalten.

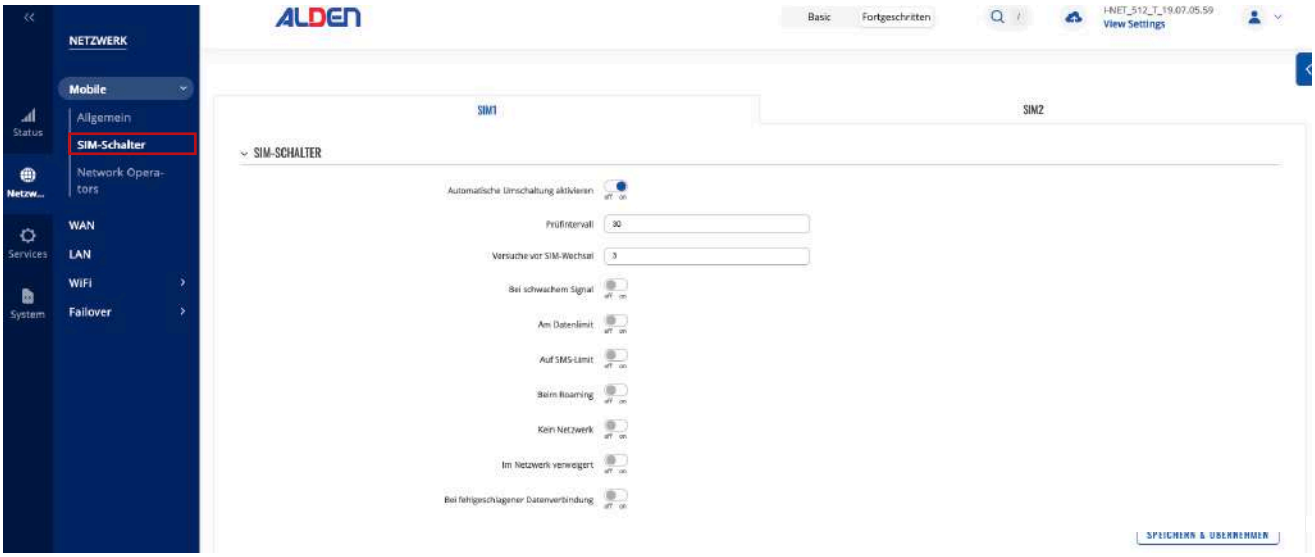
Dieser Abschnitt bietet die Möglichkeit, USSD-Nachrichten an den Mobilfunkbetreiber zu senden.



Feld	Wert	Beschreibung
USSD	Standard : Keine	Geben Sie einen USSD-Code (bis zu 182 Zeichen) ein, den Sie senden möchten. Um den eingegebenen USSD-Code zu senden, klicken Sie auf die Schaltfläche „Senden“ unter dem Antwortfeld.
Antwortnachricht	Standard : Noch keine Antwort	Zeigt die Antwort auf die zuletzt gesendete USSD-Nachricht an. Der Erhalt der Antwort kann bis zu einer Minute dauern.
Senden	Interaktive Schaltfläche	Klicken Sie, um die im USSD-Feld eingegebene Nachricht zu senden.

2.1.2 Menü NETZWERK > MOBILE > SIM-SCHALTER

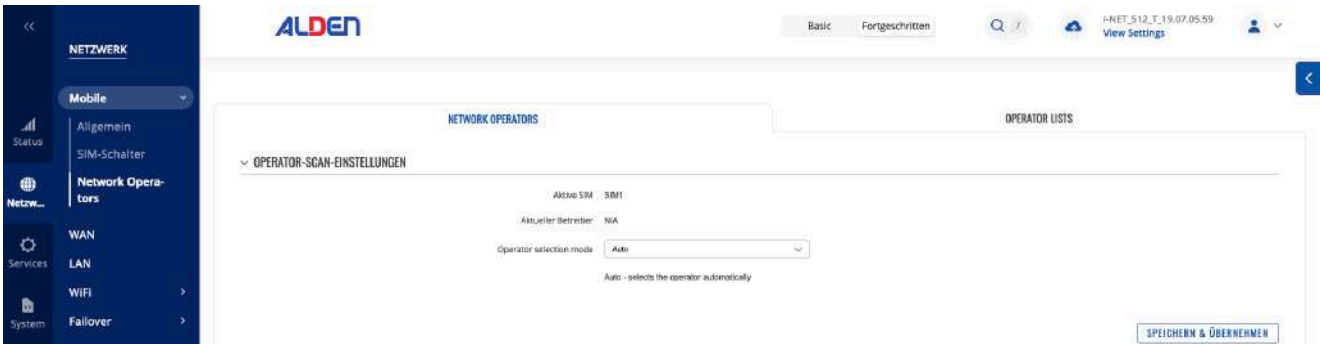
Im Abschnitt „SIM-Schalter“ haben Sie die Möglichkeit, Regeln für den SIM-Wechsel zu konfigurieren, d. h. Bedingungen festzulegen, unter denen das Gerät von einer SIM-Karte auf eine andere umschaltet. Weitere Informationen finden Sie in der Abbildung und Tabelle unten.



Automatische Umschaltung aktivieren	Off | On ; Standard : Off	Schaltet die automatische SIM-Umschaltung ein oder aus.
Prüfintervall	Ganzzahl [3..3600] ; Standard : 30	Die Häufigkeit (in Sekunden), mit der das Gerät die SIM-Wechselbedingungen überprüft. Wenn eine solche Bedingung vorliegt, führt der Router einen SIM-Wechsel durch. Wenn nicht, prüft er erneut, ob die gleichen Bedingungen vorliegen, nachdem die in diesem Feld angegebene Zeitspanne verstrichen ist.
Versuche vor SIM-Wechsel	Ganzzahl [1..10] ; Standard : 3	Wie oft eine Bedingung überprüft wird, bevor ein SIM-Wechsel ausgeführt wird. Wenn sich das Gerät beispielsweise in einem Zustand befindet, der mindestens eine SIM-Wechselbedingung erfüllt, führt das Gerät eine Reihe zusätzlicher Prüfungen durch, die in diesem Feld angegeben sind, und führt nur dann einen SIM-Wechsel durch, wenn die Bedingung bei jeder Prüfung erfüllt ist.
Bei schwachem Signal*	Off | On ; Standard : Off	Führt einen SIM-Wechsel durch, wenn die Signalstärke unter einen bestimmten Schwellenwert fällt.
*Signalstärke (dBm)	Entier [-120..-50] ; Standard : -59	Niedrigster Signalstärkewert (RSSI) in dBm, unterhalb dessen ein Wechsel der SIM-Karte erfolgen sollte. Weitere Informationen: RSSI
Am Datenlimit	Off | On ; Standard : Off	Führt einen SIM-Wechsel durch, wenn das mobile Datenlimit für diese SIM-Karte erreicht ist. Sie können auf den Seiten Netzwerk → WAN (einfacher WebUI-Modus) oder Netzwerk → Schnittstellen (erweiterter WebUI-Modus) ein mobiles Datenlimit einrichten, indem Sie neben der Schnittstelle, für die Sie die Daten beschränken möchten, auf „Bearbeiten“ klicken.
Auf SMS-Limit	Off | On ; Standard : Off	Führt einen SIM-Wechsel durch, wenn das SMS-Limit für diese SIM-Karte erreicht ist. Sie können das SMS-Limit auf der Seite Netzwerk → Mobil → Allgemein einrichten .
Beim Roaming	Off | On ; Standard : Off	Führt einen SIM-Wechsel durch, wenn Roaming-Bedingungen erkannt werden.
Kein Netzwerk	Off | On ; Standard : Off	Führt einen SIM-Wechsel durch, wenn keine Netzwerkverbindung verfügbar ist.
Im Netzwerk verweigert	Off | On ; Standard : Off	Führt einen SIM-Wechsel durch, wenn der Zugriff auf ein Netzwerk von einem Betreiber verweigert wird.
Bei fehlgeschlagener Datenverbindung	Off | On ; Standard : Off	Führt einen SIM-Wechsel durch, wenn die mobile Datenverbindung fehlschlägt. Mögliche Methoden zur Fehlerermittlung sind: LCP-Echo ICMP-Echo Wenn kein Echo empfangen wird, gilt die Datenverbindung als unterbrochen.

2.1.3 Menü NETZWERK > MOBILE > NETWORK OPERATORS

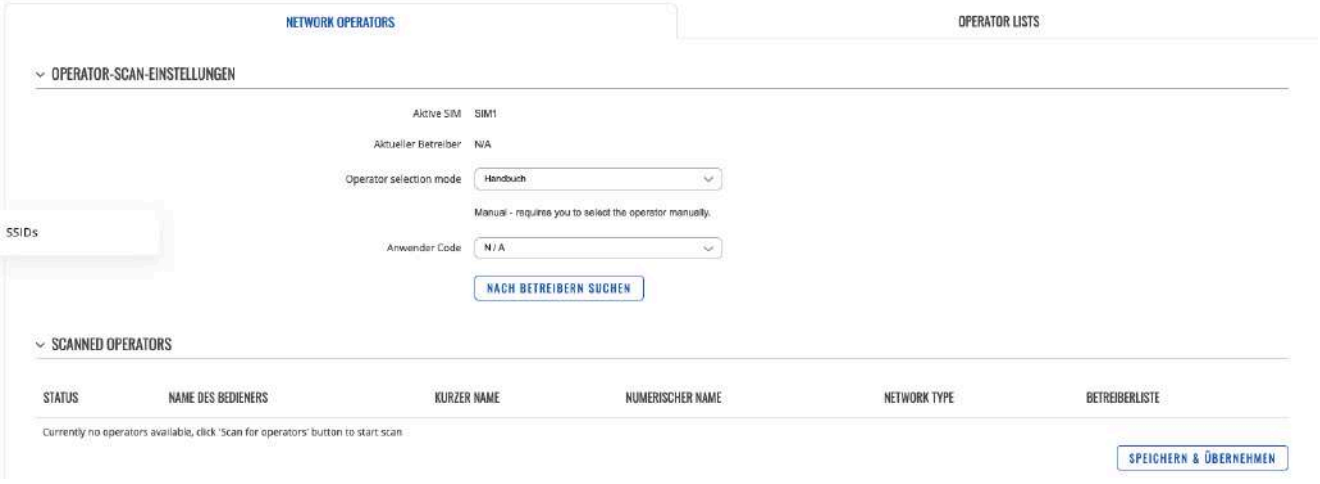
Im Bereich Netzbetreiber haben Sie die Möglichkeit, nach Mobilfunknetzbetreibern zu suchen und diese zu verwalten, mit denen sich die SIM-Karte des Geräts verbinden kann. Die Betreiberauswahl ist nur für die primäre SIM-Karte verfügbar. Um einen Betreiber für die andere SIM-Karte festzulegen, muss diese zunächst im Abschnitt „SIM-Karteneinstellungen“ als primäre SIM-Karte ausgewählt werden .



Aktive SIM	SIM1 | SIM2 ; Standard : SIM 1	Zeigt an, welche SIM-Karte derzeit aktiv ist.
Aktueller Betreiber	Standard : Keine	Zeigt den Namen des Betreibers an, mit dem das Gerät derzeit verbunden ist.
Operator selection mode	Auto | Manuell | Manuell-Automatik ; Standard : Auto	Methode zur Betreiberauswahl. • Auto : Wählt den Operator automatisch aus. • Manuell : Sie müssen den Operator manuell auswählen. (Mehr zu dieser Auswahl weiter unten .) • Manuell-Automatik : Fordert Sie auf, den Code eines Betreibers einzugeben. Wenn der Router die Verbindung jedoch nicht herstellen kann, stellt er automatisch eine Verbindung zum nächsten verfügbaren Betreiber her.

Manuelle Auswahl des Bedieners

Um einen Operator manuell auszuwählen, geben Sie den Verbindungsmodus „Manuell“ an und klicken Sie auf „Nach Operatoren suchen“ .



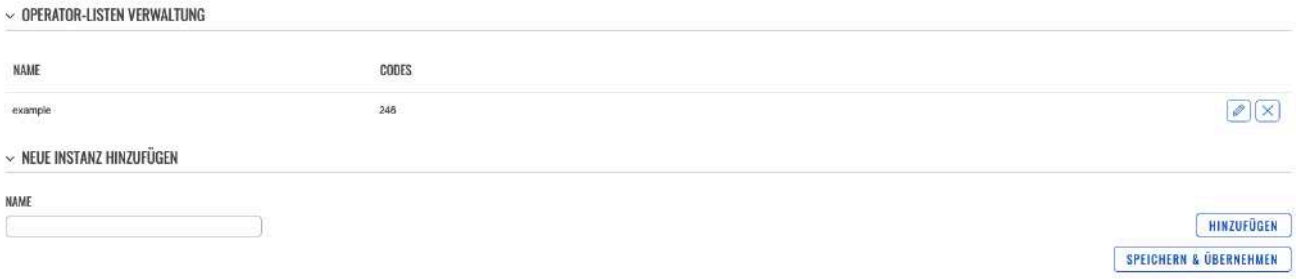
Es erscheint ein Popup-Fenster, in dem Sie gefragt werden, ob Sie sicher sind. Klicken Sie auf „Suchen“, wenn Sie fortfahren möchten.

Sobald der Scan abgeschlossen ist, werden die Ergebnisse unter „Scanned Operators/Verfügbare Operatoren“ angezeigt.

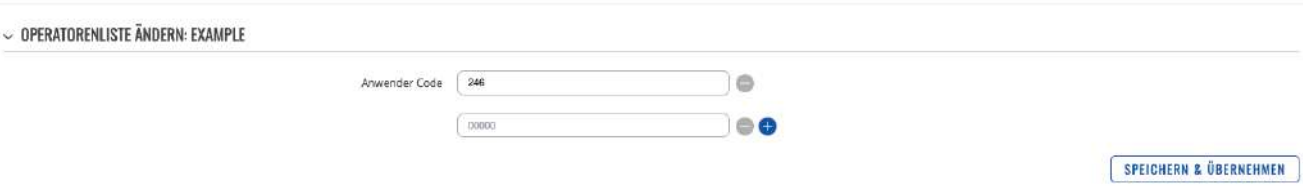
Um die SIM-Karte für die Verwendung eines einzelnen Betreibers zuzuweisen, wählen Sie im Feld „Betreiberliste“ den Betreiber aus und klicken Sie auf „Speichern & übernehmen“.

Operator Lists

In diesem Abschnitt werden Listen mit Betreibercodes erstellt, die dann im Abschnitt „Betreibereinstellungen“ verwendet werden können , um sie auf die Whitelist oder Blacklist zu setzen. Der Betreibercode besteht aus zwei Teilen: Mobile Country Code (MCC) und Mobile Network Code (MNC).



Wenn Sie  in einer Liste auf „Bearbeiten“ klicken, werden Sie zur Bearbeitungsseite weitergeleitet, auf der Sie Betreibercodes für diese Liste eingeben können.



2.2 Menü Netzwerk > WAN (Modus Fortgeschritten)

Das WAN INTERFACES-Menü ist nur im Fortgeschrittenen-Modus verfügbar.

Aus Gründen der Betriebsstabilität Ihres Routers wird dringend empfohlen, die Einstellungen dieses Menüs nicht zu ändern.
Dieses Menü ist für erfahrene Benutzer reserviert.

WAN-Schnittstellen

Im Abschnitt Wan-Schnittstellen werden die auf dem Router verfügbaren Netzwerke angezeigt.

Neue Instanz hinzufügen

Der Abschnitt "Neue Instanz hinzufügen" wird verwendet, um zusätzliche Netzwerkschnittstellen zu erstellen. Um eine neue Schnittstelle zu erstellen, geben Sie einfach einen benutzerdefinierten Namen dafür ein und klicken Sie auf die Schaltfläche "Hinzufügen".

Konfiguration der Schnittstellen

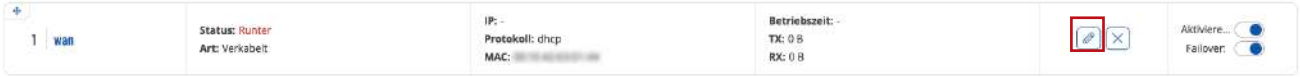
Dieser Abschnitt enthält Informationen zur Konfiguration der Netzwerkschnittstelle. Es gibt zwei Haupttypen von Schnittstellen auf dem Gerät:

- Ethernet-WAN
- Mobilfunk-WAN

Verschiedene Schnittstellentypen können unter verschiedenen Protokollen konfiguriert werden:

	Statisch	DHCP	DHCPv6	PPPoE	Mobile
Ethernet-WAN	✓	✓	✓	✓	
Mobilfunk-WAN					✓

Um mit der Konfiguration einer Schnittstelle zu beginnen, klicken Sie auf die Schaltfläche "Bearbeiten  " auf der rechten Seite der Schnittstelle:

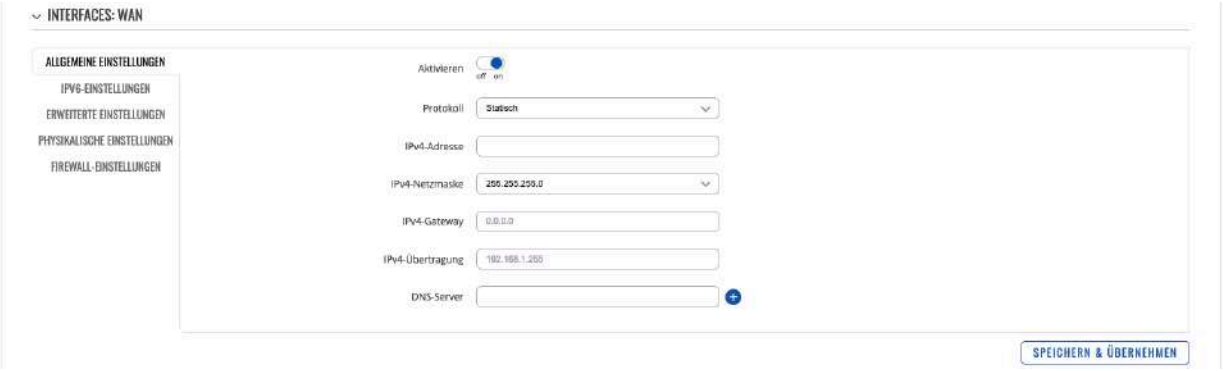


Allgemeine Einstellungen

Der Abschnitt Allgemeine Konfiguration wird verwendet, um das Protokoll einer Schnittstelle und alle verschiedenen Parameter zu konfigurieren, die zu jedem Protokoll gehören. Wenn Kein Protokoll ausgewählt ist, werden alle anderen Schnittstellenparameter ignoriert. Die folgenden Abschnitte unterscheiden sich je nach Protokoll.

Allgemeine Einstellungen : Statisch

Das statische Protokoll verwendet eine vordefinierte manuelle Konfiguration anstelle der automatischen Parametererfassung über ein DHCP-Lease.



Feld	Wert	Beschreibung
Aktivieren	Off | On; Standard : On	Schnittstelle aktivieren.
IPv4-Adresse	IPv4 ; Standard :192.168.2.1	Die IPv4-Adresse dieser Schnittstelle. Eine IP-Adresse identifiziert ein Gerät in einem Netzwerk und ermöglicht ihm die Kommunikation mit anderen Geräten.
IPv4-Netzmaske	Netzmaske; Standard : 255.255.255.0	Die IPv4-Subnetzmaske dieser Schnittstelle. Eine Subnetzmaske wird verwendet, um die "Größe" eines Netzwerks zu definieren, indem festgelegt wird, welcher Teil der IP-Adresse das Netzwerk und welcher Teil ein Gerät bezeichnet.
IPv4-Gateway	IPv4 ; Standard : Keine	Die IPv4-Gateway-Adresse, die von dieser Schnittstelle verwendet wird. Das Standardgateway einer Schnittstelle ist die Standardadresse, über die der gesamte ausgehende Datenverkehr geleitet wird.
IPv4-Übertragung	IPv4 ; Standard : Keine	Die IPv4-Broadcast-Adresse, die von dieser Schnittstelle verwendet wird. IP-Broadcasts werden von BOOTP- und DHCP-Clients verwendet, um ihre jeweiligen Server zu suchen und Anfragen zu senden.
DNS-Server	IPv4 ; Standard : Keine	DNS-Server-Adressen, die von dieser Schnittstelle verwendet werden. Wenn dieses Feld leer gelassen wird, werden die DNS-Server automatisch zugewiesen. Um zu überprüfen, welche DNS-Server derzeit verwendet werden, können Sie den Inhalt der Datei /tmp/resolv.conf.auto prüfen.

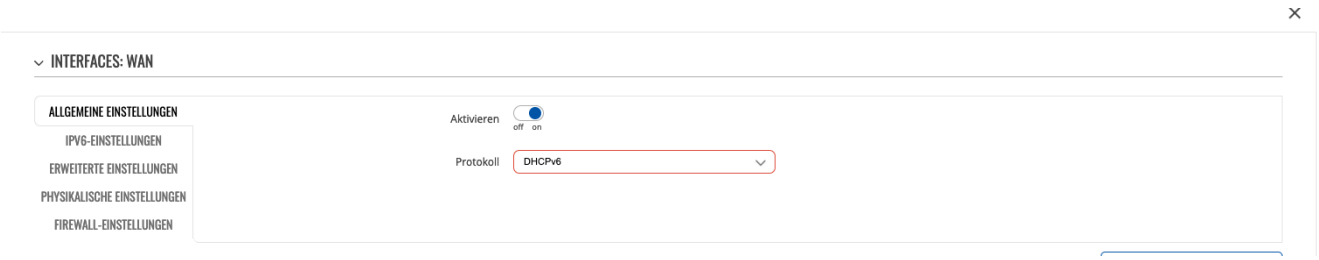
Allgemeine Einstellungen : DHCP

Das DHCP-Protokoll ermöglicht es, eine Schnittstelle einzurichten, die automatisch ihre Konfigurationsparameter über ein DHCP-Lease erhält.

Feld	Wert	Beschreibung
Aktivieren	Off | On; Standard : On	Schnittstelle aktivieren.
Hostname, der gesendet werden soll, wenn DHCP angefordert wird	Zeichenkette; Standard : Keine	Hostname für diese Schnittstelle, der verwendet wird, um dieses Gerät auf dem DHCP-Server zu identifizieren.

Allgemeine Einstellungen : DHCPv6

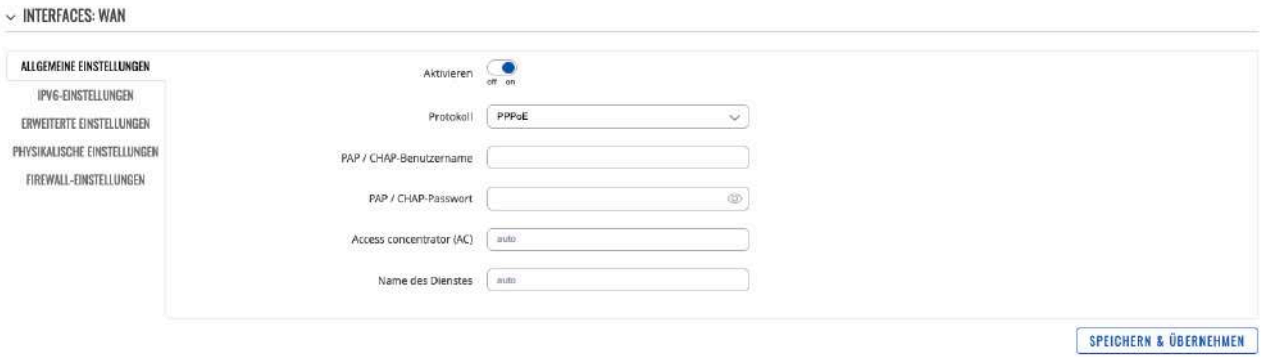
Das DHCPv6-Protokoll ermöglicht es, eine IPv6-Schnittstelle einzurichten, die automatisch ihre Konfigurationsparameter über ein DHCPv6-Lease erhält.



Feld	Wert	Beschreibung
Aktivieren	Off | On; Standard : On	Schnittstelle aktivieren.

Allgemeine Einstellungen : PPPoE

Das PPPoE-Protokoll wird verwendet, um eine PPP (Point-to-Point Protocol)-Verbindung über den Ethernet-Port herzustellen.

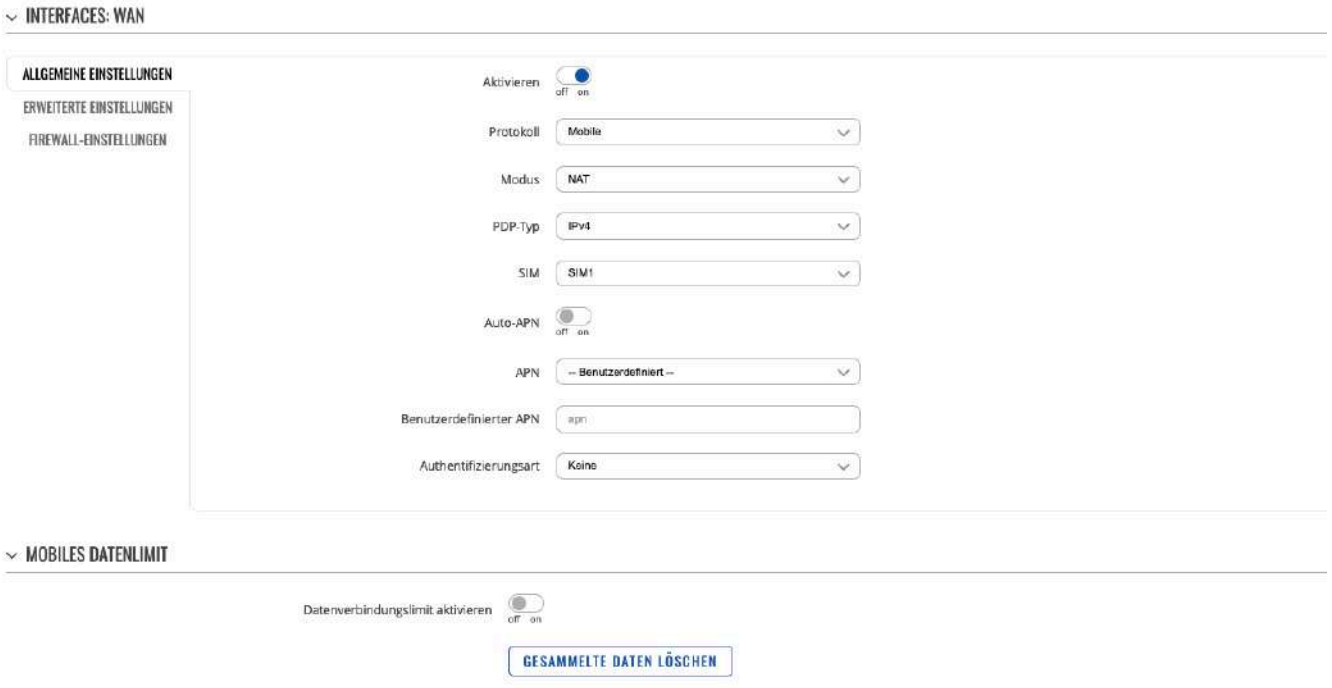


Feld	Wert	Beschreibung
Aktivieren	Off | On; Standard : On	Schnittstelle aktivieren.
PAP / CHAP-Benutzername	Standard : Keine	Benutzername für die PAP/CHAP-Authentifizierung.
PAP / CHAP-Passwort	Standard : Keine	Passwort für die PAP/CHAP-Authentifizierung.
Access concentrator (AC)	Standard : Keine	Zugangskonzentrator, mit dem verbunden werden soll. Internetanbieter verwenden Zugangskonzentratoren zur Weiterleitung ihrer PPPoE-Verbindungen. Normalerweise werden die Einstellungen automatisch empfangen, aber in einigen Fällen ist es erforderlich, den Namen eines Zugangskonzentrators anzugeben. Leer lassen, um Zugangskonzentratoren automatisch zu erkennen.
Name des Dienstes	Standard : Keine	Name des Dienstes, mit dem verbunden werden soll. Leer lassen, um den Dienstnamen automatisch zu erkennen.

Allgemeine Einstellungen : mobile

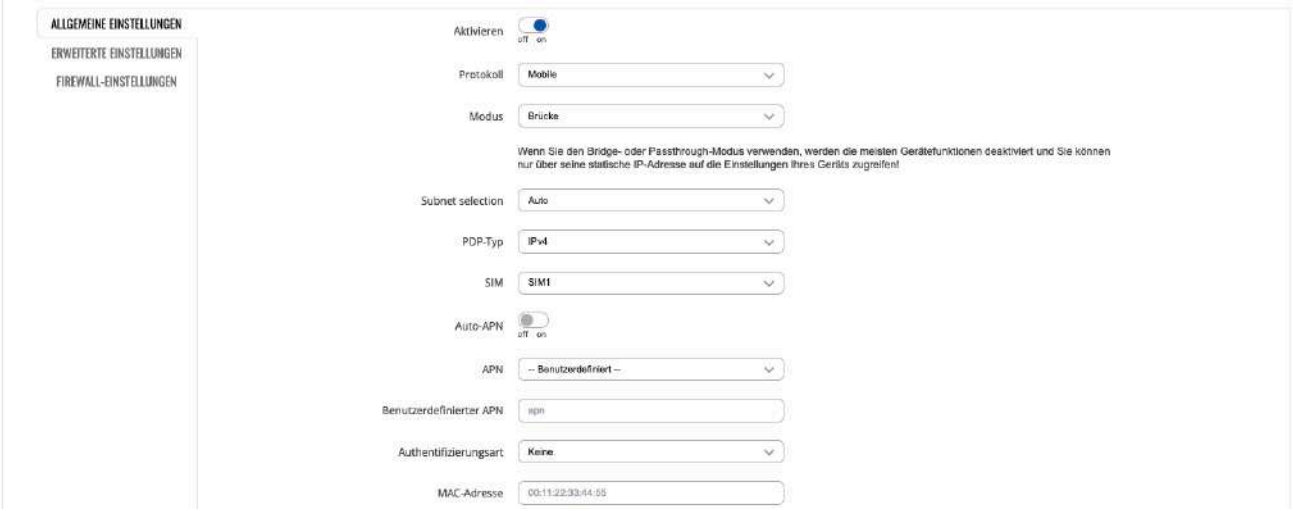
Das Mobile-Protokoll wird verwendet, um eine Schnittstelle zu konfigurieren, die eine mobile WAN-Verbindung herstellen kann.

Modus : NAT



Feld	Wert	Beschreibung
Aktivieren	NAT | Brücke | Passthrough; Standard : NAT	Betriebsmodus der mobilen Verbindung: • **NAT** – Die mobile Verbindung verwendet NAT (Network Address Translation). • **Bridge** – Verbindet die LTE-Datenverbindung mit dem LAN. Das Gerät weist seine WAN-IP-Adresse einem anderen Gerät zu (zuerst mit dem LAN verbunden oder durch Angabe einer MAC-Adresse). Die Verwendung des Bridge-Modus deaktiviert die meisten Funktionen des Geräts. • **Passthrough** – In diesem Modus teilt das I-NET 512 seine WAN-IP-Adresse mit einem einzelnen LAN-Gerät (zuerst mit dem LAN verbunden oder durch Angabe einer MAC-Adresse). Das LAN-Gerät erhält die WAN-IP des I-NET 512 anstelle der LAN-IP. Die Verwendung des Passthrough-Modus deaktiviert die meisten Funktionen des Geräts.
PDP-Typ	IPv4 | IPv6 | IPv4/IPv6; Standard : IPv4	Geben Sie an, welche Adresse beim Betreiber angefordert wird.
SIM	SIM1 | SIM2 ; Standard : SIM1	Wählen Sie aus, welcher SIM-Steckplatz für diese Schnittstelle verwendet werden soll.
Auto-APN	Off | On; Standard : On	Die automatische APN-Funktion durchsucht eine interne Android-APN-Datenbank und wählt einen APN basierend auf dem Mobilfunkanbieter und dem Land der SIM-Karte aus. Wenn der zuerst ausgewählte APN nicht funktioniert, versucht das System, den nächsten vorhandenen APN in der Datenbank zu verwenden.
Benutzerdefinierter APN	Standard : Keine	Ein Access Point Name (APN) ist ein Gateway zwischen einem mobilen Netzwerk (GSM, GPRS, 3G oder 4G) und einem anderen Computernetzwerk. Je nach Vertrag können einige Betreiber verlangen, dass Sie einen bestimmten APN verwenden, um sich im Netzwerk anzumelden. In anderen Fällen wird der APN verwendet, um spezielle Einstellungen vom Betreiber zu erhalten (zum Beispiel eine öffentliche IP-Adresse), je nach Vertrag. Ein APN-Netzwerk-Identifier darf nicht mit einer der folgenden Zeichenketten beginnen: • rac; • lac; • sgn; • rc; Er darf nicht mit • gprs enden und darf das Asterisk (*)-Symbol nicht enthalten.
Authentifizierungsart	Keine | Pap | Chap; Standard : Keine	Authentifizierungsmethode, die Ihr GSM-Betreiber verwendet, um neue Verbindungen in seinem Netzwerk zu authentifizieren. Wenn Sie PAP oder CHAP auswählen, müssen Sie auch einen Benutzernamen und ein Passwort eingeben.

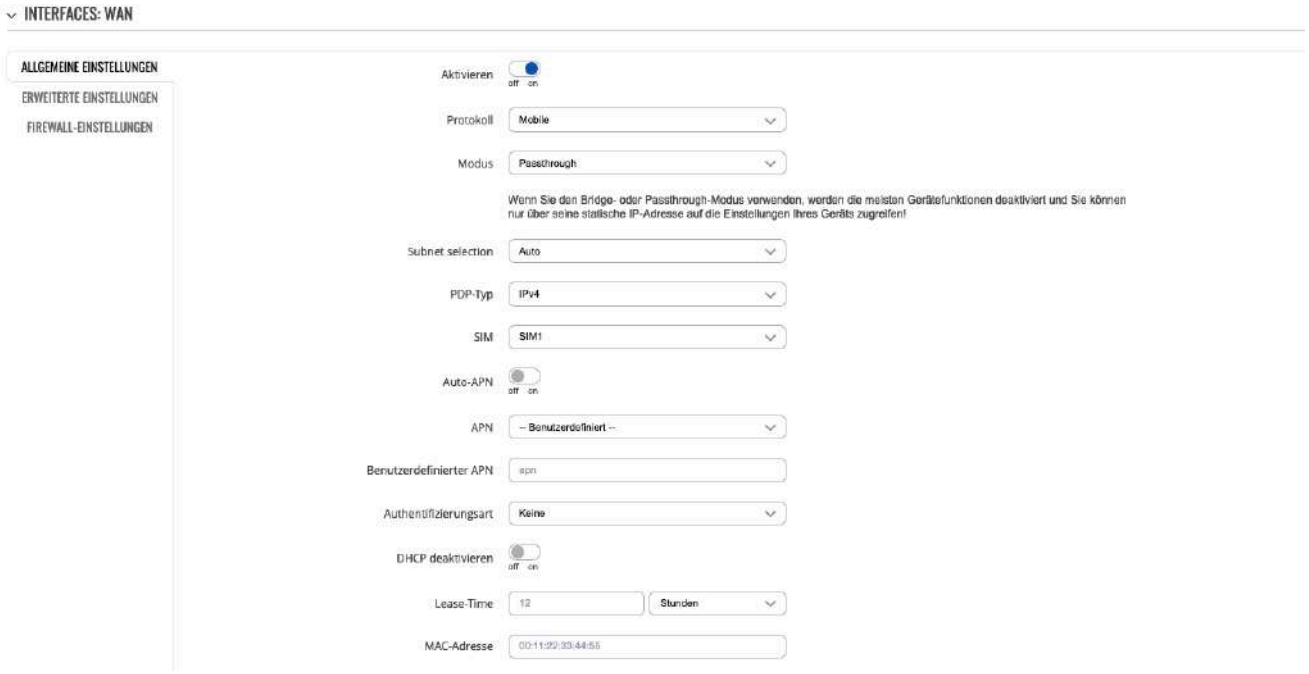
Modus : Brücke



Feld	Wert	Beschreibung
Modus	NAT | Brücke | Passthrough; Standard : Brücke	• **NAT** – Die mobile Verbindung verwendet NAT (Network Address Translation). • **Bridge** – Verbindet die LTE-Datenverbindung mit dem LAN. Das Gerät weist seine WAN-IP-Adresse einem anderen Gerät zu (zuerst mit dem LAN verbunden oder durch Angabe einer MAC-Adresse). Die Verwendung des Bridge-Modus deaktiviert die meisten Funktionen des Geräts. • **Passthrough** – In diesem Modus teilt das I-NET 512 seine WAN-IP-Adresse mit einem einzelnen LAN-Gerät (zuerst mit dem LAN verbunden oder durch Angabe einer MAC-Adresse). Das LAN-Gerät erhält die WAN-IP des I-NET 512 anstelle der LAN-IP. Die Verwendung des Passthrough-Modus deaktiviert die meisten Funktionen des Geräts.
Subnet selection	Auto | P2P ; Standard : Auto	Subnetzauswahlmethode.
PDP-Typ	IPv4 | IPv6 | IPv4/IPv6 ; Standard : IPv4	Geben Sie an, welche Adresse beim Betreiber angefragt werden soll.
SIM	SIM1 | SIM2 ; Standard : SIM1	Wählen Sie aus, welcher SIM-Steckplatz für diese Schnittstelle verwendet werden soll.
Auto-APN	Off | on ; Standard : On	Die automatische APN-Funktion analysiert eine interne Android-APN-Datenbank und wählt einen APN basierend auf dem Mobilfunkanbieter und dem Land der SIM-Karte aus. Wenn der zuerst automatisch ausgewählte APN nicht funktioniert, versucht das System, den nächsten vorhandenen APN aus der Datenbank zu verwenden.
Benutzerdefinierter APN	Standard : Keine	Ein Access Point Name (APN) ist ein Gateway zwischen einem mobilen Netzwerk (GSM, GPRS, 3G oder 4G) und einem anderen Computernetzwerk. Je nach Vertrag können einige Betreiber verlangen, dass Sie einen bestimmten APN verwenden, um sich im Netzwerk anzumelden. In anderen Fällen wird der APN verwendet, um spezielle Einstellungen vom Betreiber zu erhalten (zum Beispiel eine öffentliche IP-Adresse), je nach Vertrag. Ein APN-Netzwerk-Identifier darf nicht mit einer der folgenden Zeichenketten beginnen: • rac; • lac; • sgn; • rc; Er darf nicht mit • gprs enden und darf das Asterisk (*)-Symbol nicht enthalten.

Authentifizierungsart	Keine | Pap | Chap; Standard : Keine	Authentifizierungsmethode, die Ihr GSM-Betreiber verwendet, um neue Verbindungen in seinem Netzwerk zu authentifizieren. Wenn Sie PAP oder CHAP auswählen, müssen Sie auch einen Benutzernamen und ein Passwort eingeben.
MAC-Adresse	Mac; Standard : Keine	Geben Sie die MAC-Adresse des Geräts an, das die IP-Adresse der mobilen Schnittstelle im Bridge- oder Passthrough-Modus erhalten soll.

Modus : Passthrough



Feld	Wert	Beschreibung
Modus	NAT | Bridge | Passthrough ; Standard : NAT	• NAT – Die mobile Verbindung verwendet NAT (Network Address Translation). • Bridge – Verbindet die LTE-Datenverbindung mit dem LAN. Das Gerät weist seine WAN-IP-Adresse einem anderen Gerät zu (zuerst mit dem LAN verbunden oder durch Angabe einer MAC-Adresse). Die Verwendung des Bridge-Modus deaktiviert die meisten Funktionen des Geräts. • Passthrough – In diesem Modus teilt das I-NET 512 seine WAN-IP-Adresse mit einem einzelnen LAN-Gerät (zuerst mit dem LAN verbunden oder durch Angabe einer MAC-Adresse). Das LAN-Gerät erhält die WAN-IP des I-NET 512 anstelle der LAN-IP. Die Verwendung des Passthrough-Modus deaktiviert die meisten Funktionen des Geräts.
Subnet selection	Auto | P2P ; Standard : Auto	Subnetzauswahlmethode.
PDP-Typ	IPv4 | IPv6 | IPv4/IPv6 Standard : IPv4	Geben Sie an, welche Adresse beim Betreiber angefordert werden soll.
Auto-APN	Off | On ; Standard : On	Die Auto-APN-Funktion analysiert eine interne Android-APN-Datenbank und wählt einen APN basierend auf dem Betreiber und dem Land der SIM-Karte aus. Wenn der erste automatisch ausgewählte APN nicht funktioniert, versucht sie, den nächsten in der Datenbank vorhandenen APN zu verwenden.

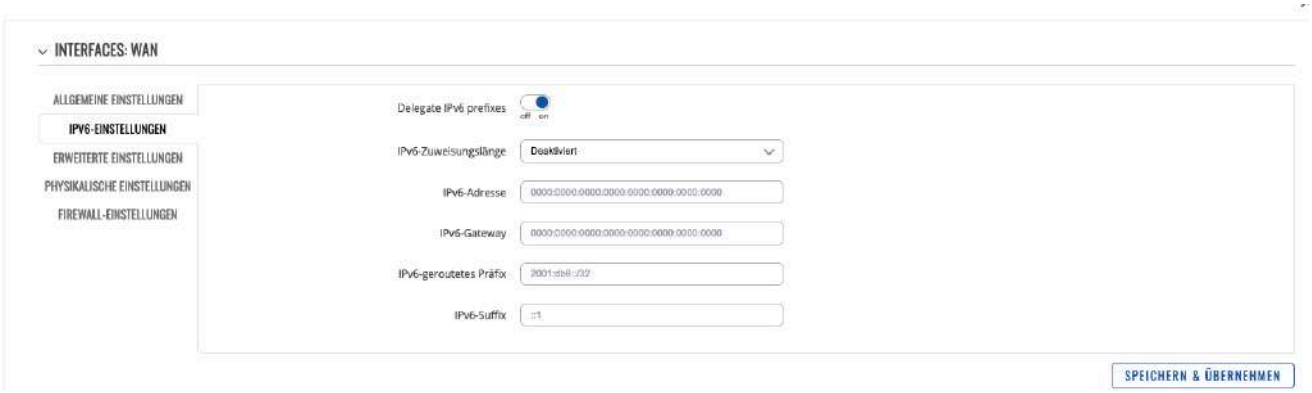
Benutzerdefinierter APN	Standard : keine	Ein Access Point Name (APN) ist ein Gateway zwischen einem mobilen Netzwerk (GSM, GPRS, 3G oder 4G) und einem anderen Computernetzwerk. Je nach Vertrag können einige Betreiber verlangen, dass Sie einen bestimmten APN verwenden, um sich im Netzwerk anzumelden. In anderen Fällen wird der APN verwendet, um spezielle Einstellungen vom Betreiber zu erhalten (zum Beispiel eine öffentliche IP-Adresse), je nach Vertrag. Ein APN-Netzwerk-Identifier darf nicht mit einer der folgenden Zeichenketten beginnen: • rac; • lac; • sgn; • rc; Er darf nicht mit ".gprs" enden und darf das Asterisk (*)-Symbol nicht enthalten.
Authentifizierungsart	Keine | Pap | Chap ; Standard : Keine	Méthode zur Authentifizierung, die von Ihrem GSM-Betreiber verwendet wird, um neue Verbindungen in seinem Netzwerk zu authentifizieren. Wenn Sie PAP oder CHAP auswählen, müssen Sie auch einen Benutzernamen und ein Passwort eingeben.
DHCP deaktivieren	Off | On; Standard : On	Deaktiviert die dynamische Zuweisung von Client-Adressen, wenn sie deaktiviert ist.
Lease-Time	Wert ; Standard : keine	Ablaufzeit der zugewiesenen Adresse. Der Mindestwert für Stunden beträgt 1, der Mindestwert für Minuten beträgt 2 und der Mindestwert für Sekunden beträgt 120.
Einheiten	Stunden | Minuten | Sekunden ; Standard : Stunden	Gibt die Zeiteinheit an.
MAC-Adresse	Mac ; Standard : keine	Gibt die MAC-Adresse des Geräts an, das die IP-Adresse der mobilen Schnittstelle im Bridge- oder Passthrough-Modus erhalten wird. Hinweis: Dieses Feld wird nur sichtbar, wenn Sie den Bridge- oder Passthrough-Modus verwenden.

IPv6-Einstellungen

Die IPv6-Einstellungensektion wird verwendet, um einige der spezifischeren und weniger häufig verwendeten Schnittstellenparameter zu konfigurieren. Diese Sektion ist für jedes Protokoll unterschiedlich.

IPv6-Einstellungen: Statisches Protokoll

Die Informationen zu den erweiterten Einstellungen für das statische Protokoll sind in der untenstehenden Tabelle aufgeführt.



Feld	Wert	Beschreibung
Delegate IPv6 prefixes	Off | On; Standard : On	Aktivieren Sie die Delegation der verfügbaren IPv6-Präfixe für dieses Interface.
IPv6-Zuweisungslänge	Deaktiviert | 64 ; Standard : Deaktiviert	Ein Metrik-Wert gibt die Priorität des Gateways an. Je niedriger die Metrik, desto höher die Priorität (0 für die höchste Priorität).
IPv6-Adresse	IPv6-Adressen mit oder ohne Maskenpräfix werden akzeptiert ; Standard : keine	Weisen Sie dieser Schnittstelle eine IPv6-Adresse zu. CIDR-Notation: Adresse/Präfix.
IPv6-Gateway	IPv6-Adressen sind akzeptiert. Standard : keine	Standard-Gateway für IPv6. Zum Beispiel ::0000:8a2e:0370:7334;
IPv6-geroutetes Präfix	IPv6-Adressen mit Maskenpräfix werden akzeptiert. Zum Beispiel ::1/128; Standard : keine	Öffentlicher Präfix zur Weiterleitung an dieses Gerät zwecks Verteilung an Kunden.
IPv6-Suffix	Erlaubte Werte: 'eui64', 'random', fester Wert wie '::1' oder '::1:2'; Standard : keine	Optional. Erlaubte Werte: 'eui64', 'random', fester Wert wie '::1' oder '::1:2'. Wenn ein IPv6-Präfix (z. B. 'a:b:c:d::') von einem Delegierungsserver empfangen wird, verwenden Sie den Suffix (z. B. '::1'), um die IPv6-Adresse ('a:b:c:d::1') für die Schnittstelle zu bilden.

IPv6-Einstellungen: DHCPv6 Protokoll

Die Informationen zu den erweiterten Einstellungen für das DHCPv6-Protokoll sind in der folgenden Tabelle aufgeführt.

Feld	Wert	Beschreibung
Delegate IPv6 prefixes	Off | On; Standard : On	Aktivieren Sie die Delegation der verfügbaren IPv6-Präfixe für dieses Interface.
IPv6-Adresse anfordern	Try | Force | Deaktiviert ; Standard : try	Legt das Verhalten der Adressanforderung fest.
IPv6-Präfix der Länge anfordern	48|52|56|60|64| Automatisch | Deaktiviert ; Standard : Automatisch	Legt fest, wie die Länge des ULA IPv6-Präfixes angefordert wird. Wenn auf "deaktiviert" gesetzt, erhält die Schnittstelle eine einzelne IPv6-Adresse ohne Subnetz für die Weiterleitung.

IPv6-Einstellungen: PPPoE Protokoll

Die Informationen zu den erweiterten Einstellungen des PPPoE-Protokolls sind in der untenstehenden Tabelle aufgeführt.

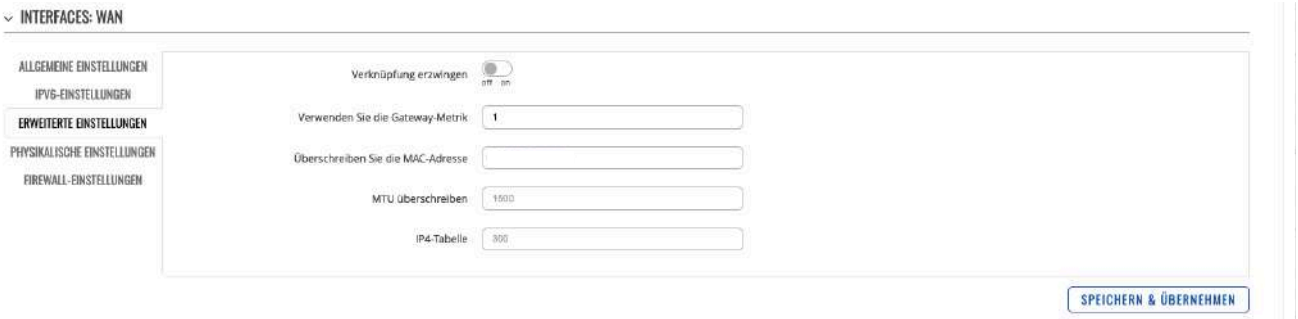
Feld	Wert	Beschreibung
Delegate IPv6 prefixes	Off | On; Standard : On	Aktivieren Sie die Delegation der verfügbaren IPv6-Präfixe für dieses Interface.
IPv6-Adresse beziehen	Automatisch | Deaktiviert | Handbuch/Manuell ; Standard : Automatisch	Legt das Verhalten zur Erlangung einer IPv6-Adresse fest.

Erweiterte Einstellungen

Die Sektion "Erweiterte Einstellungen" wird verwendet, um einige der spezifischsten und weniger häufig verwendeten Schnittstellenparameter zu konfigurieren. Diese Sektion variiert je nach Protokoll.

Erweiterte Einstellungen: Statisches Protokoll

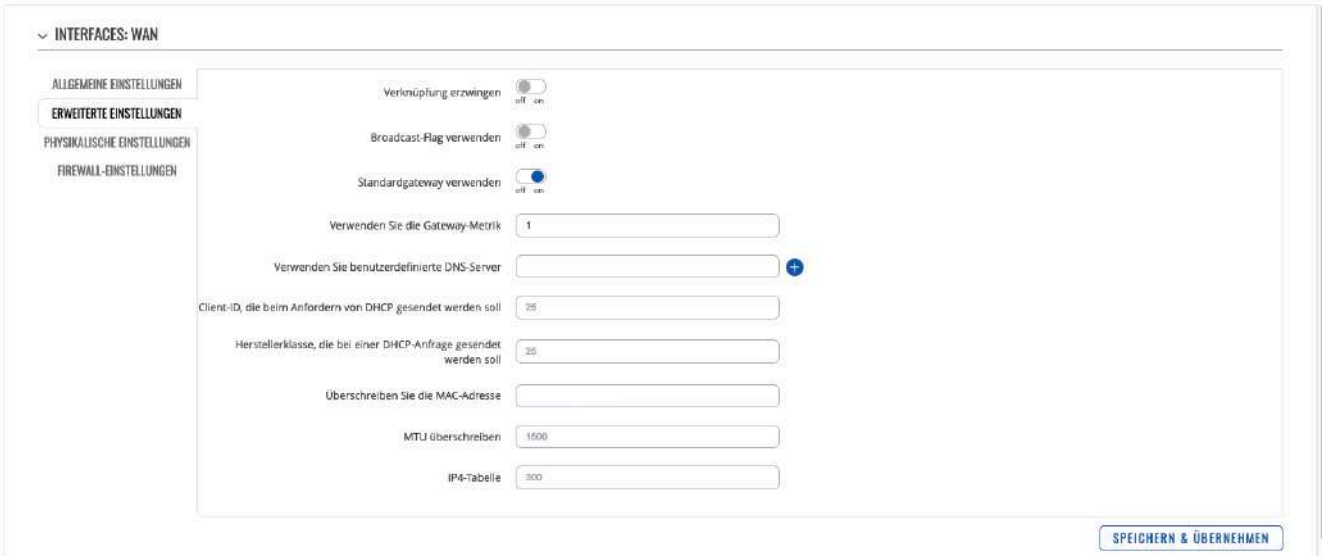
Die Informationen zu den erweiterten Einstellungen für das statische Protokoll sind in der untenstehenden Tabelle aufgeführt.



Feld	Wert	Beschreibung
Verknüpfung erzwingen	Off | On ; Standard : On	Spezifiziert, ob die Schnittstellenparameter (IP, Route, Gateway) unabhängig vom aktiven Link der Schnittstelle zugewiesen werden oder nur nachdem der Link aktiv geworden ist.
Verwenden Sie die Gateway-Metrik	Standard : 5	Ein Metrik-Wert gibt die Priorität des Gateways an. Je niedriger die Metrik, desto höher die Priorität (0 für die höchste Priorität).
Überschreiben Sie die MAC-Adresse	Standard : keine	Wenn festgelegt, verwendet die Schnittstelle anstelle der Standard-MAC-Adresse eine vom Benutzer festgelegte MAC-Adresse.
MTU überschreiben	Standard : keine	Ändert die maximale zulässige Übertragungseinheit (MTU) für die Schnittstelle. Dies ist die größte Größe der Protokolldateneinheit (PDU), die in einer einzelnen Netzwerkschichttransaktion übertragen werden kann. • **Hinweis :** Schnittstelle(n): Wenn die MTU kleiner als 1280 ist, unterstützen alle Schnittstellen derselben physischen Schnittstelle IPv4 nicht mehr. • **Hinweis :** Schnittstelle(n): Wenn die MTU kleiner als 576 ist, unterstützen alle Schnittstellen derselben physischen Schnittstelle kein DHCP mehr.
IP4-Tabelle	Standard : keine	Routentabellen-ID

Erweiterte Einstellungen: DHCP-Protokoll

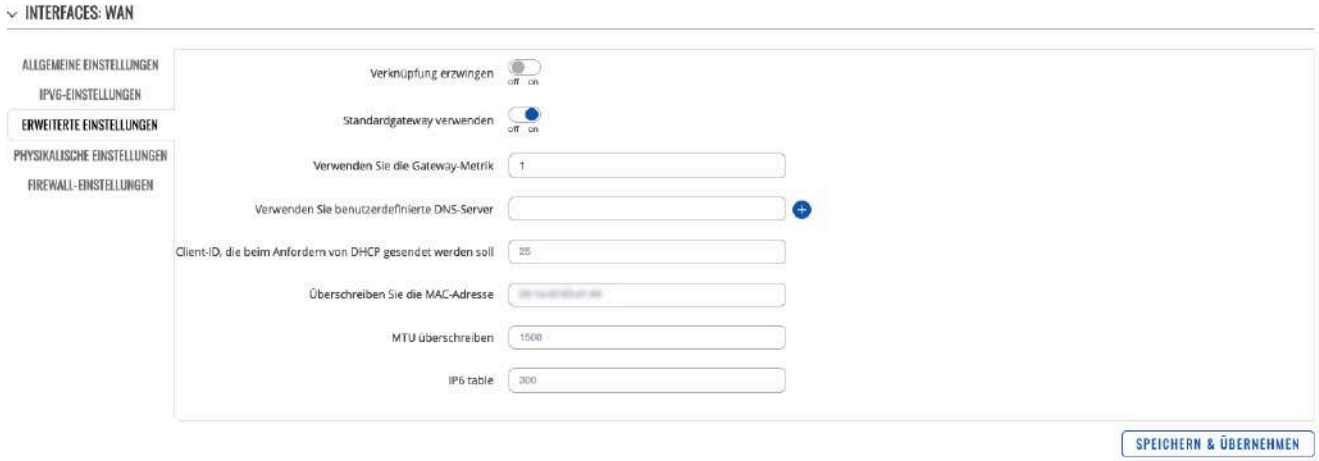
Die Informationen zu den erweiterten Einstellungen für das DHCP-Protokoll sind in der untenstehenden Tabelle aufgeführt.



Feld	Wert	Beschreibung
Verknüpfung erzwingen	Off | On; Standard : Off	Spezifiziert, ob die Schnittstellenparameter (IP, Route, Gateway) unabhängig vom aktiven Link der Schnittstelle zugewiesen werden oder nur nachdem der Link aktiv geworden ist.
Broadcast-Flag verwenden	Off | On; Standard : Off	Für einige ISPs obligatorisch. Zum Beispiel, Vertrag mit DOCSIS 3.
Standardgateway verwenden	Off | On; Standard : On	Wenn aktiviert, erstellt eine Standardroute für die Schnittstelle.
Verwenden Sie die Gateway-Metrik	Standard : keine	Ein Metrik-Wert gibt die Priorität des Gateways an. Je niedriger die Metrik, desto höher die Priorität (0 für die höchste Priorität).
Verwenden Sie benutzerdefinierte DNS-Server	IPv4 ; Standard : 5	Legt benutzerdefinierte DNS-Server fest. Wenn leer gelassen, werden die DNS-Server verwendet, die von den Peers angekündigt wurden.
Client-ID, die beim Anfordern von DHCP gesendet werden soll	Standard : keine	Client-ID, die bei der DHCP-Lease-Anfrage gesendet wird.
Herstellerklasse, die bei einer DHCP-Anfrage gesendet werden soll	Standard : keine	Anbieterklasse, die bei der DHCP-Lease-Anfrage gesendet wird.
Überschreiben Sie die MAC-Adresse	Standard : keine	Wenn festgelegt, verwendet die Schnittstelle eine vom Benutzer definierte MAC-Adresse anstelle der Standard-MAC-Adresse.
MTU überschreiben	Standard : keine	Ändert die maximale zulässige Übertragungseinheit (MTU) für die Schnittstelle. Dies ist die größte Größe der Protokolldateneinheit (PDU), die in einer einzelnen Netzwerkschichttransaktion übertragen werden kann. • **Hinweis :** Schnittstelle(n): Wenn die MTU kleiner als 1280 ist, unterstützen alle Schnittstellen derselben physischen Schnittstelle IPv4 nicht mehr. • **Hinweis :** Schnittstelle(n): Wenn die MTU kleiner als 576 ist, unterstützen alle Schnittstellen derselben physischen Schnittstelle kein DHCP mehr.
IP4-Tabelle	Standard : keine	Routentabellen-ID

Erweiterte Einstellungen: DHCPv6-Protokoll

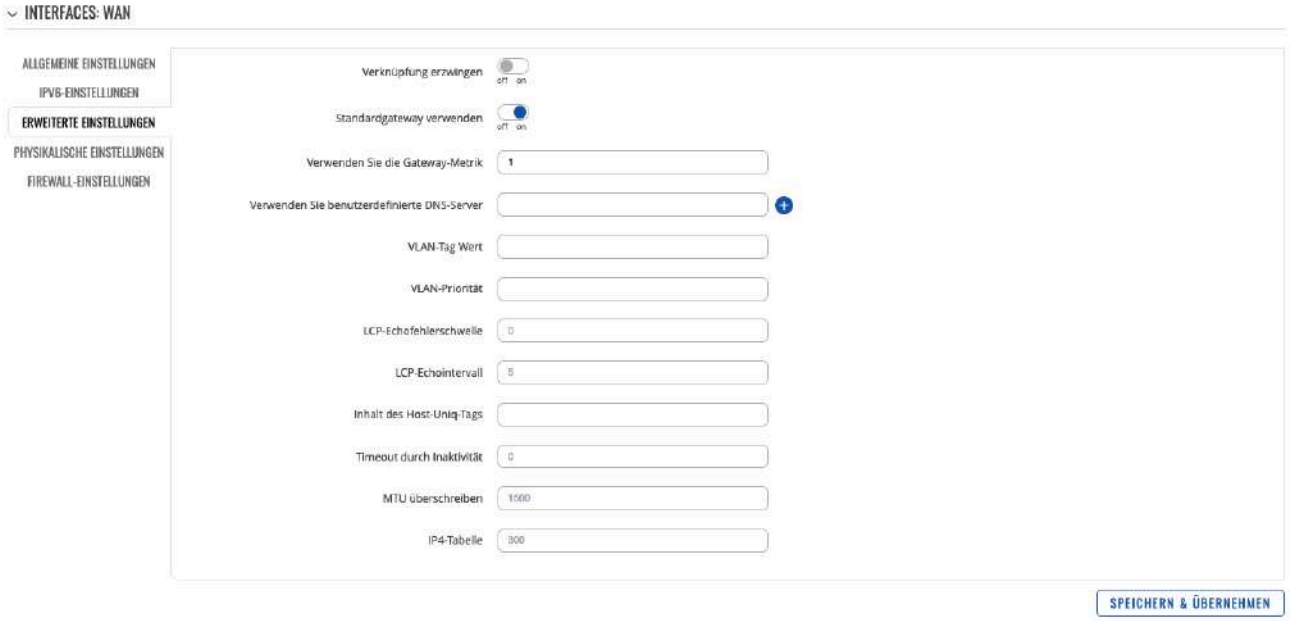
Die Informationen zu den erweiterten Einstellungen für das DHCPv6-Protokoll sind in der untenstehenden Tabelle aufgeführt.



Feld	Wert	Beschreibung
Verknüpfung erzwingen	Off | On; Standard : Off	Spezifiziert, ob die Schnittstellenparameter (IP, Route, Gateway) unabhängig vom aktiven Link der Schnittstelle zugewiesen werden oder nur nachdem der Link aktiv geworden ist.
Standardgateway verwenden	Off | On; Standard : On	Wenn aktiviert, erstellt eine Standardroute für die Schnittstelle.
Verwenden Sie die Gateway-Metrik	Standard : 5	Ein Metrik-Wert gibt die Priorität des Gateways an. Je niedriger die Metrik, desto höher die Priorität (0 für die höchste Priorität).
Verwenden Sie benutzerdefinierte DNS-Server	Standard : keine	Legt benutzerdefinierte DNS-Server fest. Wenn leer gelassen, werden die DNS-Server verwendet, die von den Peers angekündigt wurden.
Client-ID, die beim Anfordern von DHCP gesendet werden soll	Standard : keine	Client-ID, die bei der DHCP-Lease-Anfrage gesendet wird.
Überschreiben Sie die MAC-Adresse	Standard : keine	Wenn festgelegt, verwendet die Schnittstelle eine vom Benutzer definierte MAC-Adresse anstelle der Standard-MAC-Adresse.
MTU überschreiben	Standard : keine	"Ändert die maximale zulässige Übertragungseinheit (MTU) für die Schnittstelle. Dies ist die größte Größe der Protokolldateneinheit (PDU), die in einer einzelnen Netzwerkschichttransaktion übertragen werden kann. • **Hinweis:** Schnittstelle(n): Wenn die MTU kleiner als 1280 ist, unterstützen alle Schnittstellen derselben physischen Schnittstelle IPv4 nicht mehr. • **Hinweis:** Schnittstelle(n): Wenn die MTU kleiner als 576 ist, unterstützen alle Schnittstellen derselben physischen Schnittstelle kein DHCP mehr."
IP6 table	Standard : keine	Routentabellen-ID

Erweiterte Einstellungen: PPPoE-Protokoll

Die Informationen zu den erweiterten Einstellungen für das PPPoE-Protokoll sind in der untenstehenden Tabelle aufgeführt."



Feld	Wert	Beschreibung
Verknüpfung erzwingen	Off | On ; Standard : Off	Legt fest, ob die Schnittstellenparameter (IP, Route, Gateway) der Schnittstelle unabhängig vom aktiven Link zugewiesen werden sollen oder erst nachdem der Link aktiv geworden ist.
Standardgateway verwenden	Off | On ; Standard : On	Wenn aktiviert, erstellt eine Standardroute für die Schnittstelle.
Verwenden Sie die Gateway-Metrik	Standard : 5	Eine Metrik gibt die Priorität des Gateways an. Je niedriger die Metrik, desto höher die Priorität (0 für die höchste Priorität).
Verwenden Sie benutzerdefinierte DNS-Server	Standard : keine	Legt benutzerdefinierte DNS-Server fest. Wenn leer gelassen, werden die DNS-Server verwendet, die von den Peers angekündigt wurden.
VLAN-Tag Wert	Standard : keine	Wert des VLAN-Tags
VLAN-Priorität	Standard : keine	VLAN-Priorität
LCP-Echofehlerschwelle	Standard : keine	Annahme, dass der Gegenüber nach einer bestimmten Anzahl von LCP Echo-Fehlern deaktiviert wird. Setzen Sie den Wert auf 0, um Fehler zu ignorieren.
LCP-Echointervall	Standard : keine	Sendet LCP Echo-Anfragen in Intervallen von Sekunden. Diese Funktion ist nur in Verbindung mit der Ausfallgrenze wirksam.
Inhalt des Host-Uniq-Tags	Standard : keine	Lassen Sie es leer, es sei denn, Ihr Internetdienstanbieter verlangt es.
Timeout durch Inaktivität	Standard : keine	Schließen Sie die inaktive Verbindung nach der angegebenen Anzahl von Sekunden. Lassen Sie den Wert auf 0, um die Verbindung zu behalten.
MTU überschreiben	Standard : keine	Maximale Übertragungseinheit (MTU) – gibt die größtmögliche Paketgröße an.
IP4-Tabelle	Standard : keine	Routentabellen-ID

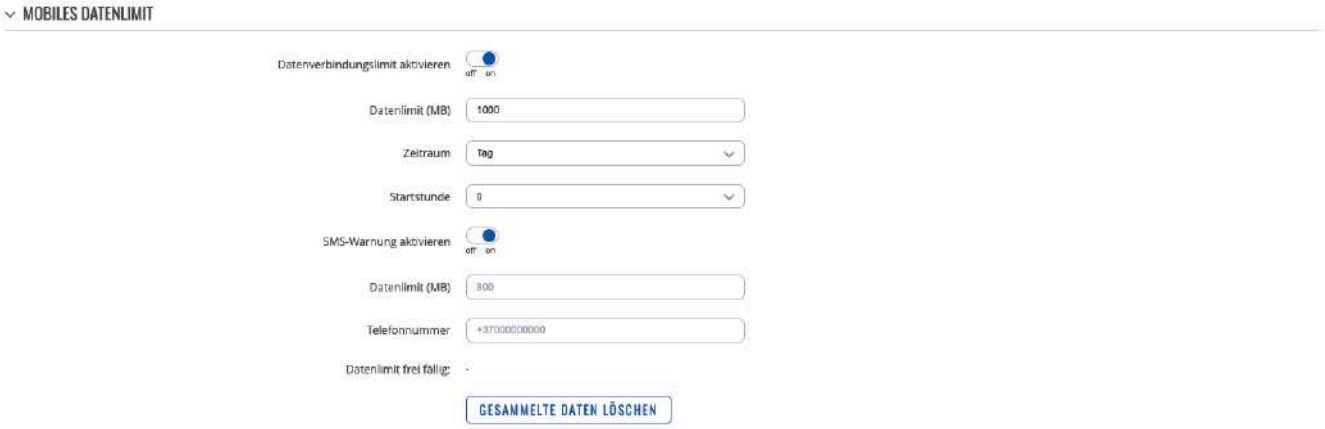
Erweiterte Einstellungen: Mobiles Protokoll

Die Informationen zu den erweiterten Einstellungen für das mobile Protokoll sind in der untenstehenden Tabelle enthalten.

Feld	Wert	Beschreibung
Verknüpfung erzwingen	Off | On ; Standard : Off	Spezifiziert, ob die Interface-Einstellungen (IP-Adresse, Route, Gateway) unabhängig vom aktiven Link zugewiesen werden oder erst nachdem der Link aktiv geworden ist.
Verwenden Sie die Gateway-Metrik	Standard : 5	Ein Metrikwert spezifiziert die Priorität des Gateways. Je niedriger die Metrik ist, desto höher ist die Priorität (0 für die höchste Priorität).
Verwenden Sie benutzerdefinierte DNS-Server	Standard : keine	Gibt benutzerdefinierte DNS-Server an. Wenn leer gelassen, werden die DNS-Server verwendet, die von den Peers bekannt gegeben wurden.
MTU überschreiben	Standard : keine	Maximale Übertragungseinheit (MTU) - gibt die größtmögliche Größe eines Datenpakets an. Wenn das Feld 'MTU ersetzen' leer gelassen wird, wird eine dynamische MTU verwendet.
IP4-Tabelle	Standard : keine	Routentabellen-ID

Erweiterte Einstellungen: Mobiles Protokoll > Mobile Datenbegrenzung

Die Informationen zu den erweiterten Einstellungen für das mobile Protokoll sind in der untenstehenden Tabelle enthalten.



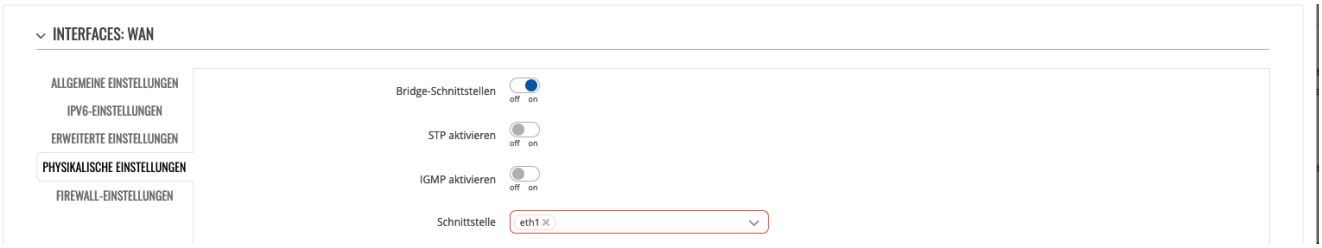
Feld	Wert	Beschreibung
Datenverbindungslimit aktivieren	Off | On ; Standard : Off	Aktiviert oder deaktiviert die Begrenzung der mobilen Daten
Datenlimit (MB)	Standard : 1000	Menge der Daten, die innerhalb des angegebenen Zeitraums heruntergeladen werden können. Wenn das Limit erreicht ist, kann das Gerät keine Datenverbindung mehr herstellen, bis der Zeitraum abgelaufen ist oder das Datenlimit zurückgesetzt wird.
Zeitraum	Tag | Woche | Monat ; Standard : Tag	Zeitraum für das Datenlimit, nach dem der Datenzähler am angegebenen Starttag zurückgesetzt wird.
Startzeit	Standard : Zeit 0	Aktiviert oder deaktiviert die SMS-Benachrichtigung. Wenn aktiviert und konfiguriert, sendet eine SMS-Nachricht an eine spezifizierte Nummer, sobald die SIM-Karte eine bestimmte Menge an Daten verwendet hat.

SMS-Warnung aktivieren	Off | On ; Standard : Off	Aktiviert oder deaktiviert die SMS-Benachrichtigung. Wenn aktiviert und konfiguriert, wird eine SMS an eine spezifizierte Nummer gesendet, sobald die SIM-Karte eine bestimmte Menge an Daten verwendet hat.
Datenlimit (MB)	Standard : keine	Die Grenze für empfangene Daten, bevor eine SMS-Benachrichtigung gesendet wird. Nach Erreichen der in diesem Feld angegebenen Datenmenge sendet der Router eine SMS-Warnung an die angegebene Telefonnummer.
Telefonnummer	Standard : keine	Telefonnummern des Empfängers.
Datenlimit frei fällig:	Standard : keine	Die Grenze für empfangene Daten, bevor eine SMS-Warnung gesendet wird. Nach Erreichen der in diesem Feld angegebenen Datenmenge sendet der Router eine SMS-Warnung an die angegebene Telefonnummer.

* Die Buchhaltung für die Nutzung der Daten Ihres Netzbetreibers kann abweichen. ALDEN ist nicht verantwortlich für Abweichungen in der Buchhaltung.

Physikalische Einstellungen

Der Abschnitt 'Physikalische Einstellungen' wird verwendet, um Verknüpfungen mit physischen Schnittstellen und Netzwerk-Bridge-Schnittstellen zu erstellen.



Feld	Wert	Beschreibung
Bridge-Schnittstellen	Off | On ; Standard : Off	Verbindet die in dieser Konfiguration angegebenen physischen Schnittstellen.
STP aktivieren	Off | On ; Standard : Off	Aktiviert oder deaktiviert die Verwendung des Spanning Tree Protokolls (STP) für dieses Interface. Hinweis: Dieses Feld wird sichtbar, wenn 'Bridge-Schnittstellen' aktiviert ist.
IGMP aktivieren	Off | On ; Standard : Off	Aktiviere die Überwachung von IGMP auf diesem Bridge. Hinweis: Dieses Feld wird sichtbar, wenn 'Bridge-Schnittstellen' aktiviert ist und das 'Protokoll' auf PPPoE festgelegt ist.
Schnittstelle	Standard : keine	Verbindet diese Netzwerkschnittstelle mit physischen Geräteschnittstellen wie Ethernet- oder WLAN-Radios.

Firewall-Einstellungen

Der Abschnitt Firewall-Einstellungen ermöglicht es Ihnen festzulegen, zu welcher Firewall-Zone diese Schnittstelle gehört, falls zutreffend. Die Zuordnung einer Schnittstelle zu einer Zone kann die Konfiguration von Firewall-Regeln erleichtern. Zum Beispiel können Sie anstatt separate Regeln für jede WAN-Schnittstelle zu konfigurieren, alle WAN-Schnittstellen einer einzigen Firewall-Zone hinzufügen und die Regel auf diese Zone anwenden.

Feld	Wert	Beschreibung
Firewall-Zone erstellen / zuweisen	Standard : keine	Weist diese Schnittstelle der angegebenen Firewall-Zone zu.

2.3 Menü Netzwerk > LAN

Das LAN-Menü ist nur im 'Erweiterten' Modus verfügbar.

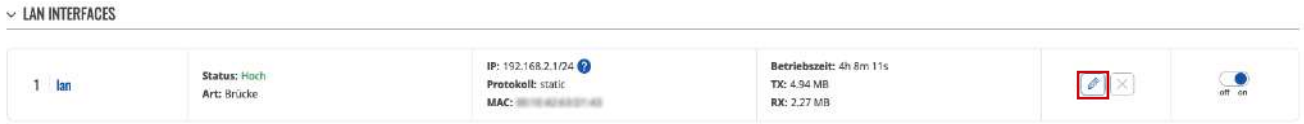
LAN-Schnittstellen

Der Abschnitt LAN-Schnittstellen zeigt die verfügbaren Netzwerke auf dem Router an.

Neue Instanz hinzufügen

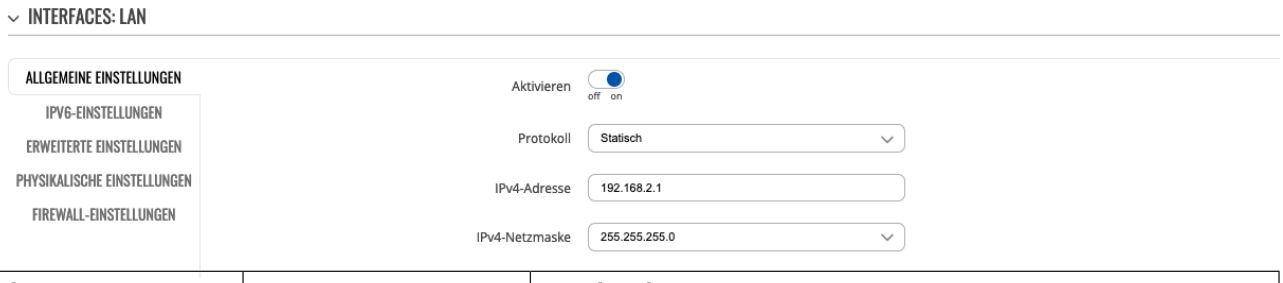
Der Abschnitt 'Neue Instanz hinzufügen' wird verwendet, um zusätzliche Netzwerkschnittstellen zu erstellen. Um eine neue Schnittstelle zu erstellen, geben Sie einfach einen benutzerdefinierten Namen dafür ein und klicken Sie auf die Schaltfläche 'Hinzufügen'.

Um mit der Konfiguration einer Schnittstelle zu beginnen, klicken Sie auf die Schaltfläche 'Bearbeiten' auf der rechten Seite der Schnittstelle.



Allgemeine Einstellungen

Der Abschnitt 'Allgemeine Einstellungen' wird verwendet, um die Hauptparameter des LAN zu konfigurieren.



Feld	Wert	Beschreibung
Aktivieren	Off | On ; Standard : On	Weist dieser Schnittstelle die angegebene Firewall-Zone zu.
Protokoll	Statisch | Keine ; Standard : Statisch	
IPv4-Adresse	IP4 ; Standard : 192.168.2.1	Die Adresse Ihres Routers im Netzwerk.
IPv4-Netzmaske	Netzmaske ; Standard : 255.255.255.0	Die IPv4-Netzwerkmaske dieser Schnittstelle. Eine Netzwerkmaske wird verwendet, um die 'Größe' eines Netzwerks zu definieren, indem angegeben wird, welcher Teil der IP-Adresse das Netzwerk und welcher Teil ein Gerät bezeichnet.

IPv6-Einstellungen

Der Abschnitt IPv6-Einstellungen wird verwendet, um die IPv6-Parameter des LAN zu konfigurieren.

Feld	Wert	Beschreibung
Delegate IPv6 prefixes	Off | On ; Standard : On	Aktivieren Sie die Weitergabe der verfügbaren IPv6-Präfixe auf dieser Schnittstelle.
IPv6-Zuweisungslänge	Deaktiviert | 64 | Benutzerdefiniert - ganzzahlig [0..6] ; Standard : 60	Weisen Sie dieser Schnittstelle einen Teil einer bestimmten Länge jedes öffentlichen IPv6-Präfixes zu.
Hinweis zur IPv6-Zuweisung	Standard : keine	Weisen Sie dieser Schnittstelle Teile des Präfixes unter Verwendung dieser hexadezimalen Sub-Präfix-ID zu.
IPv6-Suffix	Standard : keine	Optional. Zulässige Werte: 'eui64', 'random', fester Wert wie '::1' oder '::1:2'. Wenn das IPv6-Präfix (z. B. 'a:b:c:d::') von einem delegierenden Server empfangen wird, verwenden Sie das Suffix (z. B. '::1'), um die IPv6-Adresse ('a:b:c:d::1') für die Schnittstelle zu bilden.

Erweiterte Einstellungen

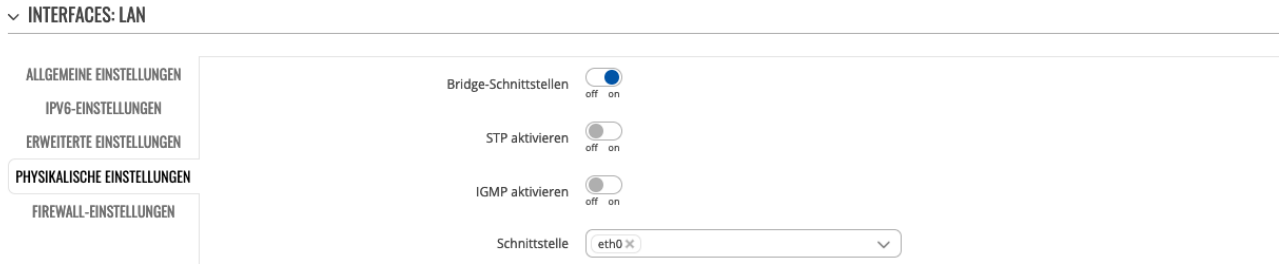
Der Abschnitt Erweiterte Einstellungen wird verwendet, um die fortgeschrittenen Einstellungen des LAN zu konfigurieren.

Feld	Wert	Beschreibung
Verknüpfung erzwingen	Off | On ; Standard : On	Legen Sie die Eigenschaften der Schnittstelle unabhängig vom Verbindungstyp fest (wenn definiert, rufen die Ereignisse zur Erkennung der Verbindung keine Hotplug-Handler auf).
Verwenden Sie die Gateway-Metrik	Standard : 0	Die Konfiguration generiert standardmäßig einen Routingtabelleneintrag. In diesem Feld können Sie die Metrik dieses Eintrags ändern. Eine niedrigere Metrik bedeutet eine höhere Priorität.
Überschreiben Sie die MAC-adresse	Zum Beispiel 00:23:45:67:89:AB ; Standard : keine	Ersetzen Sie die MAC-Adresse der Schnittstelle. Zum Beispiel kann Ihnen Ihr Internetdienstanbieter eine statische IP-Adresse geben und sie möglicherweise auch mit der MAC-Adresse Ihres Computers verknüpfen (dh diese IP funktioniert nur mit Ihrem Computer, nicht mit Ihrem Router). In diesem Feld können Sie die MAC-Adresse Ihres Computers auswählen und der Gateway vortäuschen, dass er mit Ihrem Computer kommuniziert. Sie können die MAC-Adresse eines derzeit verbundenen Computers auswählen oder eine benutzerdefinierte verwenden. Wenn Sie die MAC-Adresse auf der LAN-Schnittstelle ändern, achten Sie darauf, Kollisionen mit anderen MAC-Adressen zu vermeiden.

MTU überschreiben	Standard : keine	Maximale Übertragungseinheit (MTU) – gibt die maximale Größe eines Datenpakets an.
IP4-Tabelle	Der Wert muss eine gültige nicht signierte Ganzzahl sein. ; Standard : keine	IPv4-Routingtabelle für Routen dieser Schnittstelle.

Physikalische Einstellungen

Der Abschnitt 'Physikalische Einstellungen' wird verwendet, um die physischen Einstellungen des LAN zu konfigurieren.



Feld	Wert	Beschreibung
Bridge-Schnittstellen	Off | On ; Standard : On	Erstelle eine Bridge über die angegebenen Schnittstellen.
STP aktivieren	Off | On ; Standard : Off	Aktiviere das Spanning Tree Protokoll auf dieser Bridge.
IGMP aktivieren	Off | On ; Standard : Off	Aktiviere die IGMP-Überwachung auf dieser Bridge.
Schnittstelle	Netzwerkschnittstellen; Standard: physische LAN-Schnittstelle	Name der physischen Schnittstelle, die diesem Abschnitt zugewiesen werden soll; Liste der Schnittstellen, wenn der Brückentyp festgelegt ist.

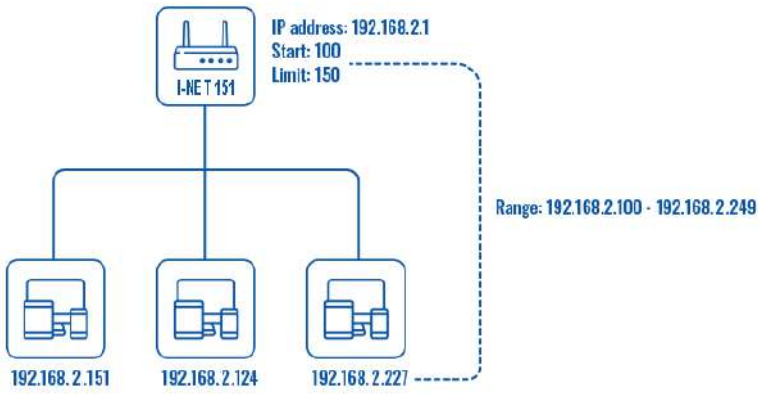
Firewall-Einstellungen

Der Abschnitt Firewall-Einstellungen wird verwendet, um die Firewall-Einstellungen des LAN zu konfigurieren.

Feld	Wert	Beschreibung
Firewall-Zone erstellen / zuweisen	Nicht spezifiziert | LAN | WAN ; Standard : LAN	Wählen Sie die Firewall-Zone aus, die Sie dieser Schnittstelle zuweisen möchten. Wählen Sie 'Nicht spezifiziert', um die Schnittstelle aus der zugeordneten Zone zu entfernen oder definieren Sie eine neue Zone und ordnen Sie die Schnittstelle dieser zu.

DHCP-Server

Ein DHCP-Server (Dynamic Host Configuration Protocol) ist ein Dienst, der automatisch die TCP/IP-Einstellungen für jedes Gerät konfigurieren kann, das einen solchen Dienst anfordert. Wenn Sie ein Gerät anschließen, das so konfiguriert ist, automatisch eine IP-Adresse zu erhalten, wird der DHCP-Server eine IP-Adresse aus dem verfügbaren IP-Adresspool zuweisen, und das Gerät kann innerhalb des privaten Netzwerks kommunizieren.
Um den Abschnitt DHCP-Server sichtbar zu machen, stellen Sie das Schnittstellenprotokoll auf Statisch ein.

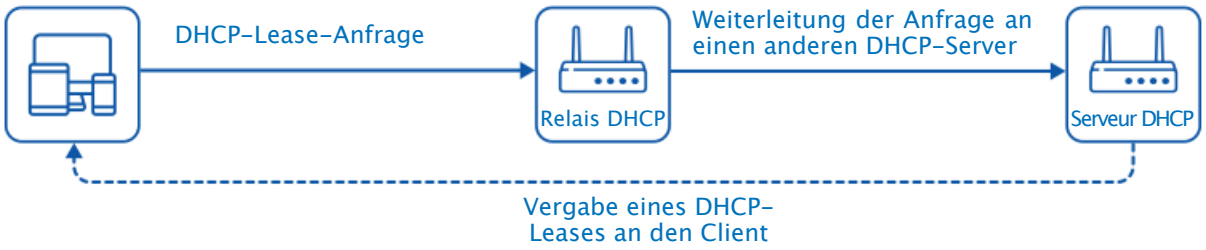


DHCP-Server: Allgemeine Konfiguration

Der Abschnitt 'Allgemeine Konfiguration' ermöglicht die Konfiguration der wichtigsten Betriebsparameter des DHCP-Servers.

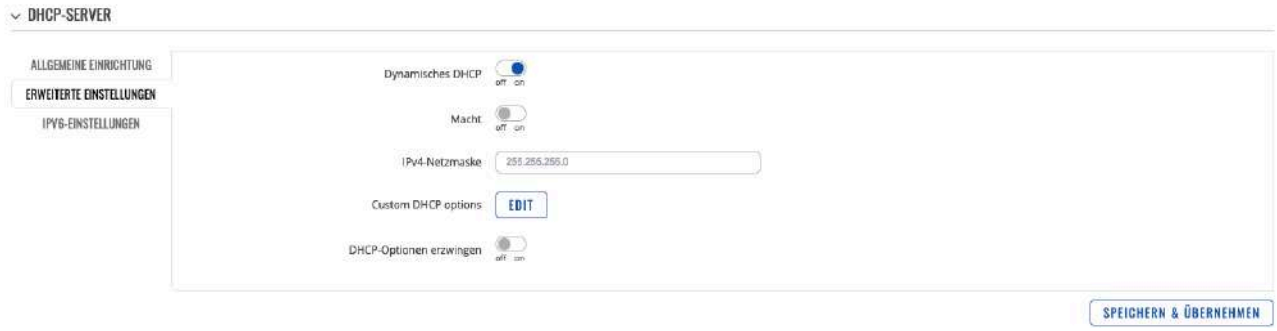
Feld	Wert	Beschreibung
DHCP aktivieren	Aktivieren | Deaktivieren | Relais ; Standard : Aktivieren	Aktiviert oder deaktiviert den DHCP-Server oder aktiviert den DHCP-Relay*. Wenn DHCP-Relay* ausgewählt ist, werden Sie aufgefordert, die IP-Adresse eines anderen DHCP-Servers in Ihrem lokalen Netzwerk einzugeben. In diesem Fall leitet das Gerät alle DHCP-Anfragen an den angegebenen DHCP-Server weiter, wenn eine neue Maschine angeschlossen wird.
Start-IP	Standard : 100	Der Startwert der IP-Adresse. Zum Beispiel, wenn die LAN-IP-Adresse Ihres Geräts 192.168.1.1 ist und Ihr Subnetzmaske 255.255.255.0 ist, bedeutet dies, dass in Ihrem Netzwerk eine gültige IP-Adresse im Bereich [192.168.1.0..192.168.1.254] liegen muss (192.168.1.255 ist eine spezielle nicht verfügbare Adresse). Wenn der Startwert auf 100 gesetzt ist, wird der DHCP-Server nur Adressen ab 192.168.1.100 vergeben.
End-IP	Standard : 249	Der Startwert der IP-Adresse. Zum Beispiel, wenn die LAN-IP-Adresse Ihres Geräts 192.168.1.1 ist und Ihre Subnetzmaske 255.255.255.0 beträgt, bedeutet dies, dass in Ihrem Netzwerk gültige IP-Adressen im Bereich von [192.168.1.0 bis 192.168.1.254] liegen müssen (192.168.1.255 ist eine spezielle, nicht verfügbare Adresse). Wenn der Startwert auf 100 festgelegt ist, vergibt der DHCP-Server nur Adressen ab 192.168.1.100.

Lease-Time	Standard : 12	Ein DHCP-Lease läuft nach der in diesem Feld angegebenen Zeit ab, und das Gerät, das das Lease verwendet hat, muss ein neues anfordern. Wenn das Gerät jedoch weiterhin verbunden bleibt, wird sein Lease nach der Hälfte der angegebenen Zeit erneuert (zum Beispiel, wenn die Lease-Zeit 12 Stunden beträgt, wird alle 6 Stunden der DHCP-Server gebeten, das Lease zu erneuern). Die kürzeste Zeit, die angegeben werden kann, beträgt 2 Minuten. * Wenn die ausgewählten Einheiten Minuten sind. ** Wenn die ausgewählten Einheiten Sekunden sind.
Einheiten	Stunden | Minuten | Sekunden | Infinite Standard : Stunden	Einheit(en) für die Lease-Dauer.



DHCP-Server: Erweiterte Einstellungen

Siehe die Tabelle unten für weitere Informationen zu den erweiterten Einstellungen.



Feld	Wert	Beschreibung
Dynamisches DHCP	Off | On ; Standard : On	Aktiviere die dynamische Zuweisung von Client-IP-Adressen. Wenn diese Option deaktiviert ist, werden nur Clients mit statischen IP-Leases bedient.
Macht	Off| On ; Standard : Off	Die DHCP-Force-Funktion stellt sicher, dass das Gerät seinen DHCP-Server immer startet, auch wenn bereits ein anderer DHCP-Server im Netzwerk aktiv ist. Standardmäßig startet der DHCP-Server des Geräts nicht, wenn es mit einem Netzwerksegment verbunden ist, das bereits über einen funktionierenden DHCP-Server verfügt.
IPv4-Netzmaske	Netzwerkmaske; Standard: keine	Sendet an DHCP-Clients eine Subnetzmaske, die sich vom LAN-Netzwerkmaske unterscheidet.
Custom DHCP options	EDITIEREN" (interaktive Schaltfläche)	Öffnet das Fenster zur Bearbeitung der DHCP-Optionen."
DHCP-Optionen erzwingen	Off | On ; Standard : Off	Wenn aktiviert, werden DHCP-Optionen gesendet, auch wenn sie nicht angefordert werden.

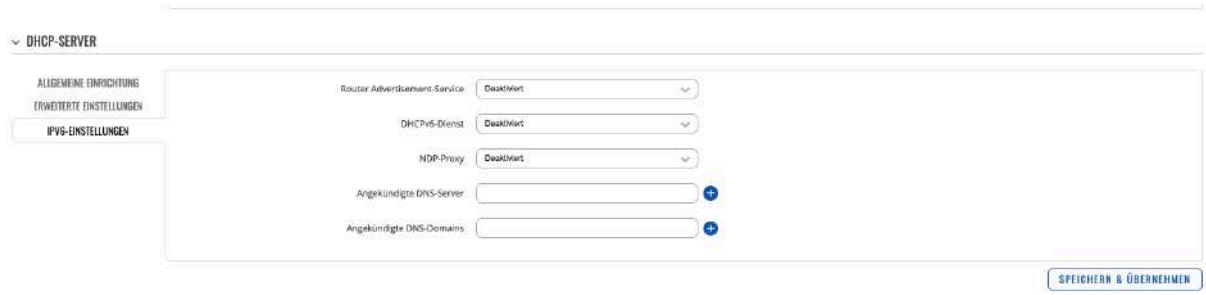
Benutzerdefinierte DHCP-Optionen

Benutzerdefinierte DHCP-Optionen sind Paare aus Zahlen und Werten, die zur Konfiguration erweiterter DHCP-Funktionen verwendet werden. Dies konfiguriert kein DHCP IPv6! Das Modalfenster für DHCP-Optionen wird verwendet, um 'Hinzufügen', 'Löschen', 'Speichern' mehrerer Optionen durchzuführen.

Feld	Wert	Beschreibung
Option code	Benutzerdefiniert | Time offset (2) | Router (3) | DNS (6) | Domain name (15) | NTP serveur (42); Standard:Time offset (2)	Standardisierter DHCP-Optionscode.
Option value	Standard : keine	Wert, der für die ausgewählte Option festgelegt wird.

DHCP-Server : IPv6-Einstellungen

In der folgenden Tabelle finden Sie weitere Informationen zum Abschnitt IPv6-Einstellungen.



Feld	Wert	Beschreibung
Router Advertisement-Service	Deaktiviert | Relaismodus | Servermodus | Hybridmodus ; Standard : Deaktiviert	Legt fest, ob die Router-Werbungen aktiviert (Servermodus), weitergeleitet oder deaktiviert werden sollen.
DHCPv6-Dienst	Deaktiviert | Relaismodus | Servermodus | Hybridmodus ; Standard : Deaktiviert	Legt fest, ob der DHCPv6-Server aktiviert (Server), weitergeleitet (Relais) oder deaktiviert (Deaktiviert) werden soll.
NDP-Proxy	Deaktiviert | Relaismodus | Hybridmodus ; Standard : Deaktiviert	Legt fest, ob NDP weitergeleitet oder deaktiviert werden soll.
Angekündigte DNS-Server	Standard : keine	Vervollständigt die vom DHCP zugewiesenen DNS-Servereinträge mit denen, die in diesem Feld angegeben sind.
Angekündigte DNS-Domains	Standard : keine	DNS-Domäne, die an DHCP-Clients verteilt wird.

2.4 Menü Netzwerk > WiFi

Die WLAN-Sektion im Netzwerk-Tab wird verwendet, um WLAN-Zugangspunkte und WLAN-Stationen (Clients) zu verwalten und zu konfigurieren.

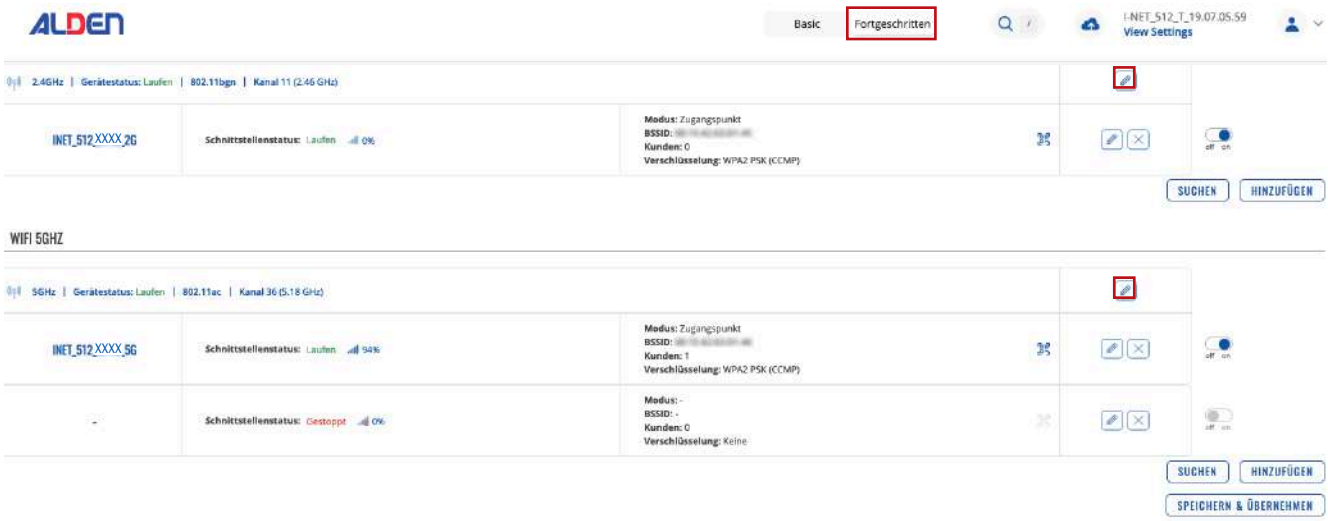
Wenn Sie Schwierigkeiten haben, diese Seite oder einige der hier beschriebenen Einstellungen auf der Web-Oberfläche Ihres Geräts zu finden, sollten Sie den "Erweiterten Modus" aktivieren. Dies können Sie tun, indem Sie auf die Schaltfläche "Normal" unter "Modus" oben auf der Web-Oberfläche klicken.

WiFi-Technologie

Die I-NET 512 Geräte unterstützen IEEE 802.11ac (WiFi 5) mit Datenübertragungsraten von bis zu 867 Mbps (Dual-Band, MU-MIMO), schneller Übergang 802.11r.

SSID

Der SSID-Abschnitt wird verwendet, um Ihre drahtlosen Zugangspunkte (AP) und drahtlosen Clients (STA) zu konfigurieren.



Oben befindet sich eine Übersicht des SSID-Präsentationsfensters. Es zeigt aktive Zugangspunkte und Stationen an. Hier können Sie Ihre WiFi-Schnittstellen aktivieren oder deaktivieren, sie löschen oder die Konfiguration starten, indem Sie auf die Schaltfläche "Bearbeiten" auf der rechten Seite der Schnittstelle klicken. Sie können auch Ihre WiFi-Geräte konfigurieren, indem Sie auf die Schaltfläche "Bearbeiten" auf der rechten Seite jeder Tabellenüberschrift klicken. Um Ihr drahtloses Gerät als Client zu konfigurieren, drücken Sie die "Scan"-Taste, um die Umgebung zu scannen und versuchen, sich mit einem neuen drahtlosen Zugangspunkt zu verbinden.

Allgemeine Konfiguration

Der Abschnitt Allgemeine Konfiguration wird verwendet, um ein WiFi-Gerät zu aktivieren oder zu deaktivieren, die Betriebsfrequenz auszuwählen (WiFi-Modus und -Kanal), die Sendeleistung einzustellen und ein Ländercode festzulegen.

Ein drahtloses WiFi-Signal im 2,4-GHz-Bereich benötigt etwa 22 MHz Bandbreite, und die Frequenzen der benachbarten Kanäle überlappen sich erheblich. Wählen Sie einen WiFi-Kanal basierend auf der Aktivität anderer Kanäle aus. Sie können eine kostenlose WiFi-Analyse-App auf Ihrem Telefon, Laptop oder einem anderen WiFi-fähigen Gerät installieren und überprüfen, welcher Kanal am wenigsten belegt ist.

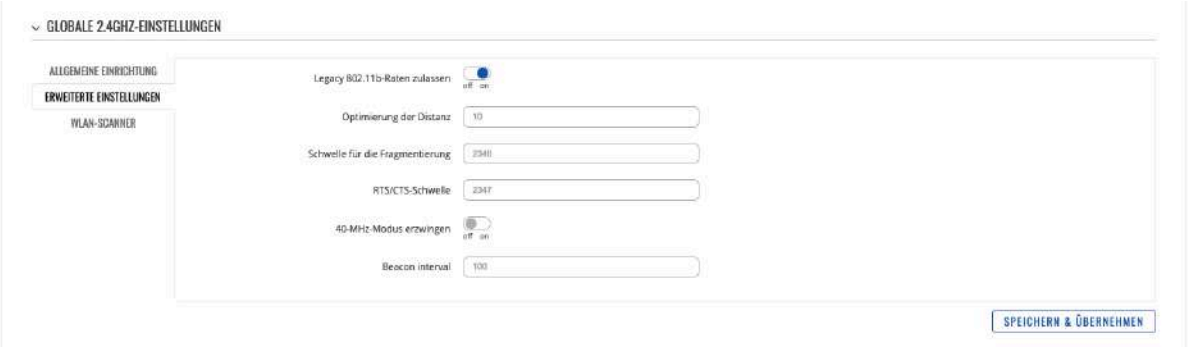
Viele Heimnetzwerke verwenden Router, die standardmäßig auf Kanal 6 im 2,4-GHz-Band betrieben werden. Nachbars WLAN-Netzwerke, die auf dem gleichen Kanal arbeiten, erzeugen Funkinterferenzen, die zu erheblichen Netzwerkperformance-Einbußen für die Benutzer führen können. Das Umstellen eines Netzwerks auf einen anderen drahtlosen Kanal kann diese Einbußen minimieren. Daher wählen Sie einen Kanal ohne andere aktive Zugangspunkte und idealerweise einen Kanal, der auf beiden Seiten keine aktiven Zugangspunkte auf zwei benachbarten Kanälen hat. Bei Unsicherheit stellen Sie das "Kanal"-Feld auf Auto ein, und das Gerät wählt automatisch den am wenigsten belegten Kanal an Ihrem Standort aus.

Feld	Wert	Beschreibung
Aktivieren	Off | On ; Standard : On	Schaltet das drahtlose Gerät ein oder aus.
Betriebsfrequenz (2,4 GHz)		
Modus	N | Legacy; Standard : N	Das Wireless N (802.11n) unterstützt eine theoretische maximale Übertragungsrate von 300 Mbps mit 2 Antennen. Mit 3 Antennen kann es bis zu 450 Mbps erreichen. Die typischen Geschwindigkeiten liegen jedoch eher bei etwa 130 Mbps. Die bestehenden Standards umfassen 802.11a, 802.11b und 802.11g.
Kanal	Auto | 1 (2 412 MHz) | 2 (2 417 MHz) | 3 (2 422 MHz) | 4 (2 427 MHz) | 5 (2 432 MHz) | 6 (2 437 MHz) | 7 (2 442 MHz) | 8 (2 447 MHz) | 9 (2 452 MHz) | 10 (2 457 MHz) | 11 (2 462 MHz); Standard : Auto	Ein 2,4-GHz-WiFi-Kanal benötigt eine Signalisierungsband-breite von etwa 22 MHz, wodurch sich die Funkfrequenzen benachbarter Kanäle erheblich überlappen. Wählen Sie daher einen Kanal ohne anderen aktiven Zugangspunkt und vorzugsweise einen Kanal, der auch auf beiden angrenzenden Kanälen keinen aktiven Zugangspunkt hat.
Breite	20 MHz | 40 MHz ; Standard : 20 MHz	Eine Kanalbreite von 40 MHz verbindet zwei 20-MHz-Kanäle und bildet so eine 40-MHz-Kanalbreite; dies ermöglicht höhere Geschwindigkeiten und schnellere Übertragungsraten. Allerdings nicht, wenn diese Kanäle durch Rauschen und Störungen überlastet sind. In stark frequentierten Bereichen mit viel Frequenzrauschen und Störungen ist ein einzelner 20-MHz-Kanal stabiler. Die 40-MHz-Kanalbreite ermöglicht höhere Geschwindigkeiten und schnellere Übertragungsraten, funktioniert jedoch in stark frequentierten Bereichen nicht so gut.
Betriebsfrequenz (5 GHz)		
Modus	N | CA ; Standard : CA	Wählen Sie zwischen den Standards 802.11n und 802.11ac.

Kanal	Auto | 36 (5 180 MHz) | 40(5 200 MHz) | 44 (5 220 MHz) | 48 (5 240 MHz) | 52 (5 260 MHz) | 56 (5 280 MHz) | 60 (5 300 MHz) | 64 (5 320 MHz) | 68 (5 340 MHz) | 72 (5 360 MHz) | 76 (5 380 MHz) | 80(5 400 MHz) | 84 (5 420 MHz) | 88 (5 440 MHz) | 92 (5 460 MHz) | 96 (5 480 MHz) | 100(5 500 MHz) | 104 (5 520 MHz) | 108 (5 540 MHz) | 112 (5 560 MHz) | 116 (5 580 MHz) | 120 (5 600 MHz) | 124 (5 620 MHz) | 128(5640 MHz) | 132 (5 660 MHz) | 136 (5 680 MHz) | 140(5 700 MHz) | 144 (5 720 MHz) | 149 (5 745 MHz) | 153 (5 765 MHz) |157 (5 785 MHz) | 161 (5 805 MHz) | 165 (5 825 MHz) ; Standard : 36 (5 180 MHz)	Ein 5-GHz-WiFi-Kanal benötigt ebenfalls eine Signalisierungsbandbreite von etwa 22 MHz, aber da sein 20-MHz-Kanal die benachbarten Kanäle weniger überlappt, wird dennoch empfohlen, einen Kanal ohne anderen aktiven Zugangspunkt zu wählen und vorzugsweise einen, der auch auf beiden angrenzenden Kanälen keinen aktiven Zugangspunkt hat.
Breite	20 MHz | 40 MHz | 80 MHz ; Standard : 80 MHz	Eine Kanalbreite von 40 MHz verbindet zwei 20-MHz-Kanäle und bildet so eine 40-MHz-Kanalbreite, während eine Kanalbreite von 80 MHz vier 20-MHz-Kanäle verbindet. Dies ermöglicht höhere Geschwindigkeiten und schnellere Übertragungsraten. Allerdings nicht, wenn diese Kanäle durch Rauschen und Störungen überlastet sind. In stark frequentierten Bereichen mit viel Frequenzrauschen und Störungen ist ein einzelner 20-MHz-Kanal stabiler. Ein 80-MHz-Kanal ist schneller als ein 40-MHz-Kanal, der wiederum schneller ist als ein 20-MHz-Kanal, aber in stark frequentierten Bereichen funktioniert er nicht so gut.
Sendeleistung	[5 %...100 %] ; Standard : 100 %	Die Sendeleistung eines Funkzugangspunkts ist proportional zu seiner effektiven Reichweite: Je höher die Sendeleistung, desto weiter kann ein Signal übertragen werden und/oder desto besser kann es physische Materialien durchdringen, während eine erfolgreiche Datenübertragung zum Empfänger-Zugangspunkt ermöglicht wird.
Ländercode	Standard : US - United States	ISO 3166-1 Alpha-2 Ländercodes gemäß der Norm ISO 3166-1.

Erweiterten Einstellungen

Die "Erweiterten Einstellungen" werden verwendet, um den Betrieb des drahtlosen Zugangspunkts hardwareseitig zu konfigurieren.



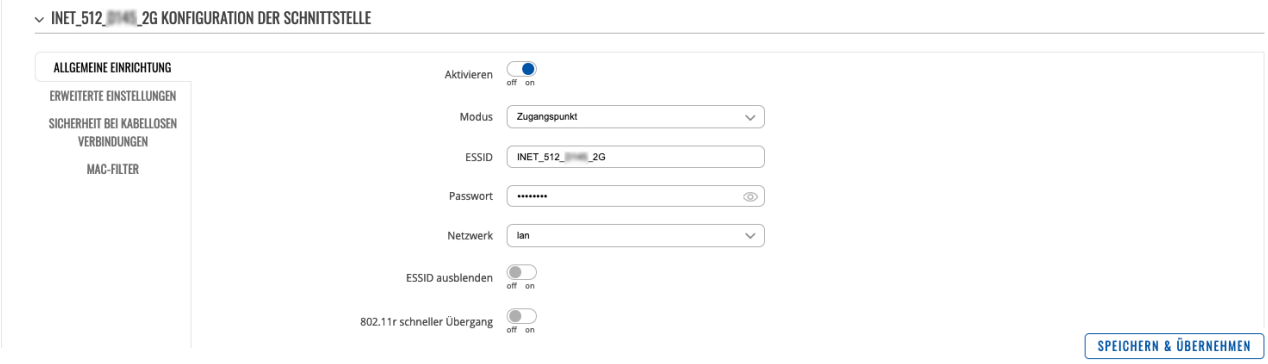
Feld	Wert	Beschreibung
Betriebsfrequenz (2,4 GHz)		
Legacy 802.11b-Raten zulassen	Off | On ; Standard : On	Activieren Sie es, um Verbindungen zu ermöglichen, die den älteren Standard 802.11b nutzen.
Optimierung der Distanz	Standard : keine	HT Entfernung zum am weitesten entfernten Netzmitglied in Metern
Schwelle für die Fragmentierung	Standard : keine	Die kleinste Paketgröße, die fragmentiert und über mehrere Frames übertragen werden kann. In Gebieten mit Interferenzen kann das Festlegen einer niedrigeren Fragmentierungsschwelle dazu beitragen, die Wahrscheinlichkeit von Paketübertragungs-fehlern zu verringern und somit die Geschwindigkeit zu erhöhen.
RTS/CTS-Schwelle	Standard : keine	RTS/CTS (Request to Send/Clear to Send) sind Mechanismen, die zur Reduzierung von Kollisionen bei Rahmen dienen, die durch das Problem verborgener Knoten eingeführt werden. Dies kann dazu beitragen, Probleme zu lösen, die auftreten, wenn mehrere Zugangspunkte in derselben Zone miteinander konkurrieren.
40-MHz-Modus erzwingen	Off | On ; Standard : Off	Verwenden Sie immer 40-MHz-Kanäle, auch wenn der sekundäre Kanal überlappt. Die Verwendung dieser Option entspricht nicht dem Standard IEEE 802.11n-2009!
Beacon interval	Standard : keine	Beacon interval in Sekunden.
Betriebsfrequenz (5 GHz)		
Optimierung der Distanz	Standard : keine	HT-Distanz zum am weitesten entfernten Netzwerkmitglied in Metern.
Schwelle für die Fragmentierung	Standard : keine	Die kleinste Paketgröße, die fragmentiert und über mehrere Frames übertragen werden kann. In Gebieten mit Interferenzen kann das Festlegen einer niedrigeren Fragmentierungsschwelle dazu beitragen, die Wahrscheinlichkeit von Paketübertragungs-fehlern zu verringern und somit die Geschwindigkeit zu erhöhen.
RTS/CTS-Schwelle	Standard : keine	RTS/CTS (Request to Send/Clear to Send) sind Mechanismen, die dazu dienen, Kollisionen von Frames zu reduzieren, die durch das Problem der versteckten Knoten verursacht werden. Dies kann helfen, Probleme zu lösen, die auftreten, wenn mehrere Zugangspunkte in derselben Zone konkurrieren.
40-MHz-Modus erzwingen	Off | On ; Standard : Off	Verwenden Sie immer 40-MHz-Kanäle, auch wenn der sekundäre Kanal überlappt. Die Verwendung dieser Option entspricht nicht dem Standard IEEE 802.11n-2009!
Beacon interval	Standard : keine	Intervall des Beacon-Signals in Sekunden.
ACS schließt DFS aus	Off | On ; Standard : Off	Aktivieren Sie diese Option, um DFS-Kanäle von der automatischen Kanalauswahl auszuschließen.

Interface-Konfiguration

Der Abschnitt Interface-Konfiguration wird verwendet, um die Einstellungen für Access Points oder drahtlose Clients zu konfigurieren. Sie finden diesen Abschnitt, indem Sie auf die Schaltfläche 'Bearbeiten' neben einem drahtlosen Gerät auf der Seite Netzwerk → WiFi → SSID klicken."

Allgemeine Konfiguration

Das Register Allgemeine Konfiguration enthält grundlegende Optionen für die ESSID und die Netzwerkschnittstelle.



Feld	Wert	Beschreibung
Aktivieren	Off | On ; Standard : On	Aktivieren oder deaktivieren Sie die WiFi-Schnittstelle.
Modus	Klient | Zugangspunkt | Mesh/Gittergewebe | Multi-AP ; Standard : Zugangspunkt	Legt die Rolle dieser Schnittstelle fest: Access Point zur Bereitstellung von WiFi für andere Geräte, Client zur Nutzung anderer WiFi-Geräte für WWAN und Mesh zur Funktion als Gateway oder Knotenpunkt in einem Mesh-Netzwerk.
Zugangspunkt Modus		
ESSID	Die Werkseinstellung für die ESSID ist für jedes Gerät unterschiedlich ; Standard : keine	Die Extended Service Set Identifier (ESSID) ist ein Name, der verwendet wird, um den Access Point zu identifizieren, der angezeigt wird, wenn ein Client versucht, sich damit zu verbinden.
Passwort	Standard : keine	Benutzerdefinierter geheimer Satz zur Authentifizierung (mindestens 8 Zeichen).
Netzwerk	Kein Netzwerk | Auto (wifi0) | lan | wan | wan6 | SIM1 | SIM2 Standard : lan	Wählen Sie das/die Netzwerk(e) aus, mit dem/denen Sie diese drahtlose Schnittstelle verbinden möchten, oder füllen Sie das Erstellungsfeld aus, um ein neues Netzwerk zu definieren.
ESSID ausblenden	Off | On ; Standard : Off	Extended Service Set Identifier (ESSID) verbergen.

802.11r schneller Übergang	Off | On ; Standard : Off	Ermöglicht schnelles Roaming zwischen Zugangspunkten im selben Mobilitätsdomänenbereich.
ACS exclut DFS	Off | On ; Standard : Off	Aktivieren Sie diese Option, um DFS-Kanäle von der automatischen Kanalauswahl auszuschließen.

Klient Modus

ESSID	Die Werkseinstellung für die ESSID ist für jedes Gerät unterschiedlich ; Standard : keine	Die Extended Service Set Identifier (ESSID) ist ein Name, der verwendet wird, um den Access Point zu identifizieren, mit dem sich der Client verbinden wird.
BSSID	Standard : keine	Basisdienst-Set-Identifier.
Passwort	Standard : keine	Benutzerdefinierter geheimer Satz zur Authentifizierung (mindestens 8 Zeichen).
Netzwerk	Standard : Auto	Wählen Sie das Netzwerk aus, mit dem Sie diese drahtlose Schnittstelle verbinden möchten, oder füllen Sie das Feld für eine benutzerdefinierte Definition eines neuen Netzwerks aus (Sie werden zur neu erstellten Netzwerkkonfigurationsseite weitergeleitet).

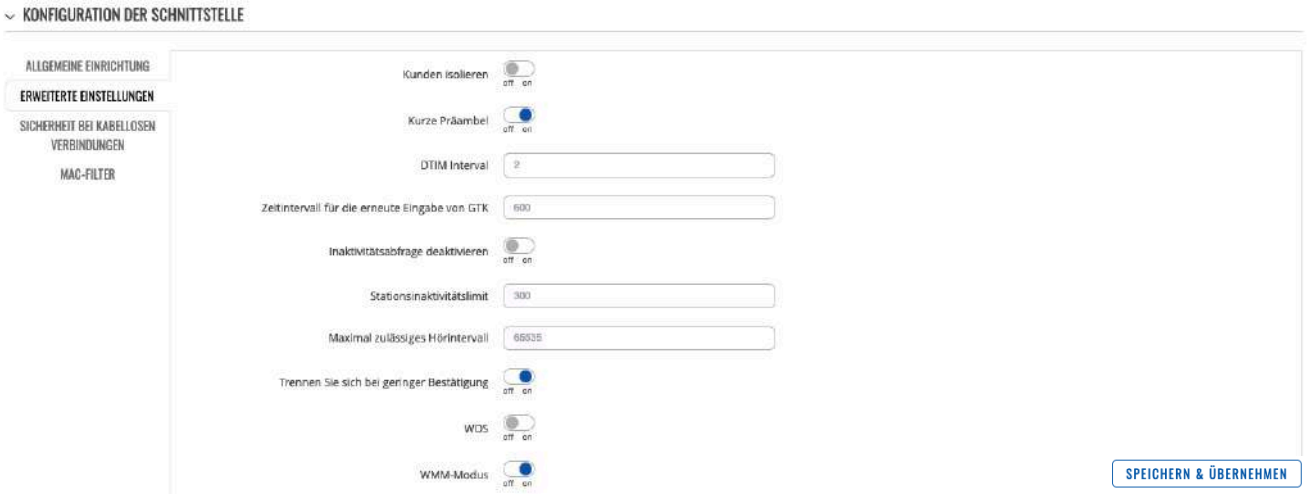
Gittergewebe Modus

Mesh ID	Standard : keine	Mesh-Netzwerk-ID.
Passwort	Standard : keine	Benutzerdefinierter geheimer Satz zur Authentifizierung (mindestens 8 Zeichen).
Netzwerk	Standard : Auto	Wählen Sie das Netzwerk aus, das Sie mit dieser drahtlosen Schnittstelle verbinden möchten, oder füllen Sie das Feld für eine benutzerdefinierte Definition eines neuen Netzwerks aus (Sie werden zur neu erstellten Netzwerkkonfigurationsseite weitergeleitet).

Multi-AP Modus

Netzwerk	Standard : Auto	Wählen Sie das Netzwerk aus, das Sie mit dieser drahtlosen Schnittstelle verbinden möchten, oder geben Sie im benutzerdefinierten Feld ein neues Netzwerk ein (Sie werden zur neu erstellten Netzwerkkonfigurationsseite weitergeleitet).
Scanzeit (Sek.)	Standard : 60	Zeit zwischen den Scans verfügbarer Access Points (mindestens 30 Sekunden).
AP-Liste hochladen	Durchsuche - (interaktiver Button)	Lade eine Liste von Access Point Konfigurationen herunter.

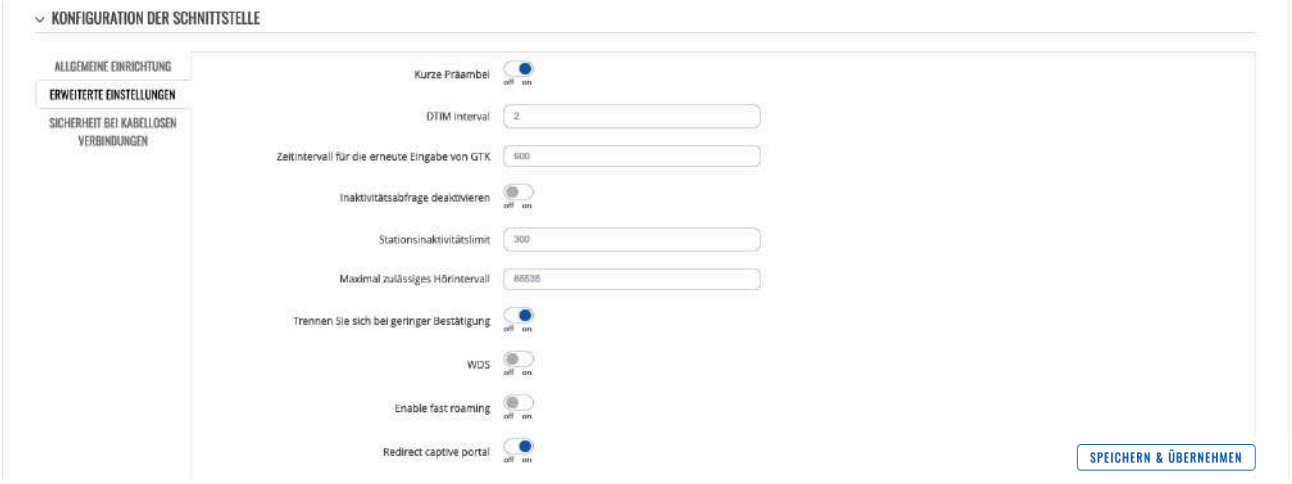
Erweiterte Einstellungen : Zugangspunktmodus



Feld	Wert	Beschreibung
Kunden isolieren	Off | On ; Standard : Off	Verhindert die Kommunikation zwischen Clientgeräten im gleichen Subnetz.

Kurze Präambel	Off | On ; Standard : On	Verwendet ein kurzes Präambel, das kürzere Datensignale nutzt und weniger Daten für die Fehlererkennung hinzufügt, was bedeutet, dass es wesentlich schneller ist.
DTIM Interval	Standard : keine	Intervalle des Nachrichtenverkehrsindikators für die Zustellung.
Zeitintervalle für die Neubildung der GTK-Schlüssel.	Standard : keine	Zeitintervall zwischen automatischen Änderungen des Gruppenschlüssels, der von allen Geräten im Netzwerk gemeinsam genutzt wird.
Inaktivitätsabfrage deaktivieren	Off | On ; Standard : Off	Die Inaktivitätsabfrage kann deaktiviert werden, um Stationen basierend auf der Inaktivitätszeit zu trennen, wodurch inaktive Stationen wahrscheinlicher vom Netzwerk getrennt werden, auch wenn sie sich noch in Reichweite des Access Points befinden.
Stationsinaktivitätslimit	Standard : keine	Inaktivitätsgrenze der Station in Sekunden. Wenn eine Station/Klient in einem bestimmten Zeitraum nichts sendet, wird ein leeres Datenrahmen an sie gesendet, um zu überprüfen, ob sie noch in Reichweite ist. Wenn dieser Rahmen nicht bestätigt wird, wird die Station zuerst getrennt und dann deauthentifiziert.
Maximal zulässiges Hörintervall	Standard : keine	Die Verbindung wird abgelehnt, wenn ein Client/Station versucht, sich mit einem höheren Hearbeat-Intervall als diesem Wert zu verbinden.
Trennen Sie sich bei geringer Bestätigung	Off | On ; Standard : On	Erlauben Sie dem Access Point Modus, Stationen/Klienten basierend auf schwachen ACK-Bedingungen zu trennen.
WDS	Off | On ; Standard : Off	Ein Wireless Distribution System (WDS) ist ein System, das die drahtlose Interkonnektivität von Access Points (APs) in einem Netzwerk ermöglicht.
WMM-Modus	Off | On ; Standard : On	WiFi Multimedia (WMM), früher bekannt als Wireless Multimedia Extensions (WME), ist ein Subset der drahtlosen LAN-Spezifikation (WLAN) 802.11e, das die Quality of Service (QoS) in einem Netzwerk verbessert, indem es Datenpakete nach vier Kategorien priorisiert.

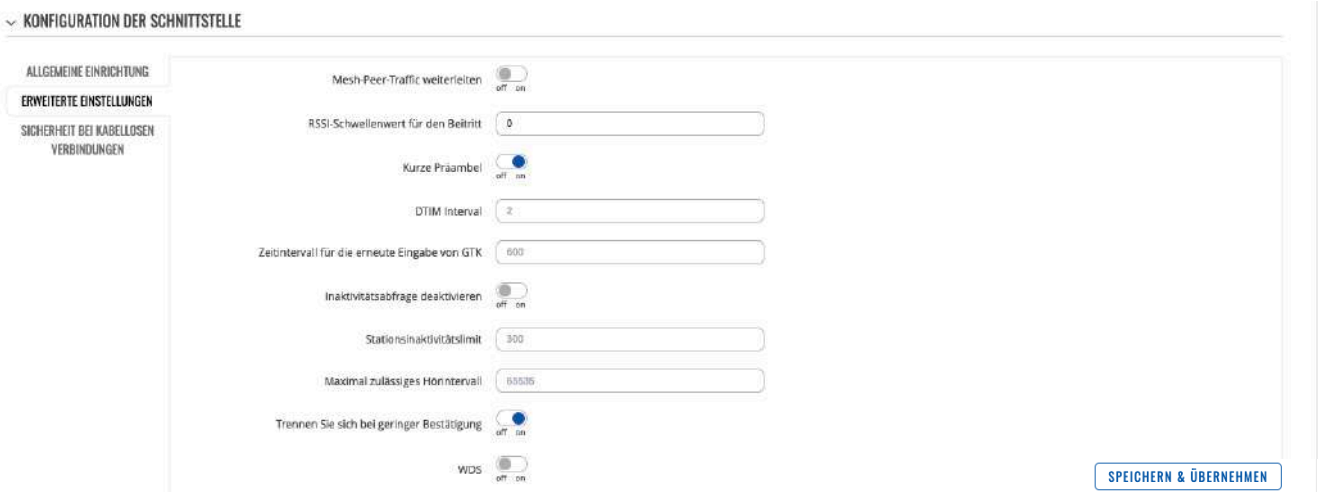
Erweiterte Einstellungen: Client-Modus und Multi-AP.



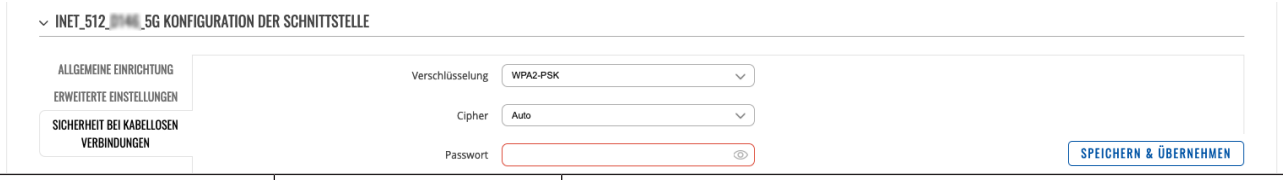
Feld	Wert	Beschreibung
Kurze Präambel	Off | On ; Standard : On	Verwende einen kurzen Präambel, der kürzere Datensequenzen nutzt, die weniger Daten zur Übertragung der Fehlerkontrollredundanz hinzufügen, was bedeutet, dass es viel schneller ist.
DTIM Interval	Standard : keine	Intervalle der Lieferverkehrsindikationsmeldungen.
Zeitintervall für die erneute Eingabe von GTK	Standard : keine	Zeitintervall zwischen automatischen Änderungen des Gruppenschlüssels, der von allen Geräten im Netzwerk gemeinsam genutzt wird."
Inaktivitätsabfrage deaktivieren	Off | On ; Standard : Off	Die Inaktivitätsabfrage kann deaktiviert werden, um Stationen basierend auf ihrer Inaktivitätszeit zu trennen, sodass inaktive Stationen eher getrennt werden, auch wenn sie sich noch in Reichweite des Zugriffspunkts befinden.

Stationsinaktivitätslimit	Standard : keine	Station-Inaktivitätslimit in Sekunden. Wenn eine Station/Client während des ersten Zeitintervalls nichts sendet, wird ihr ein leeres Datenrahmen gesendet, um zu überprüfen, ob sie noch in Reichweite ist. Wenn dieser Rahmen nicht bestätigt wird, wird die Station getrennt und dann deauthentifiziert.
Maximal zulässiges Hörintervall	Standard : keine	Die Assoziation wird abgelehnt, wenn ein Client/Station versucht, sich mit einem höheren Hear-Interval als diesem Wert zu verbinden.
Trennen Sie sich bei geringer Bestätigung	Off | On ; Standard : On	Erlaube dem AP-Modus, Stationen/Clients basierend auf einer schwachen Acknowledgment-Bedingung zu trennen.
WDS	Off | On ; Standard : Off	Ein Wireless Distribution System (WDS) ist ein System, das die drahtlose Interkonnektivität von Zugriffspunkten (APs) in einem Netzwerk ermöglicht.
Enable fast roaming	Off | On ; Standard : Off	Hintergrundanalysen für Roaming-Zwecke innerhalb eines ESS anfordern.
Redirect captive portal	Off | On ; Standard : On	

Erweiterte Einstellungen: Mesh-Modus

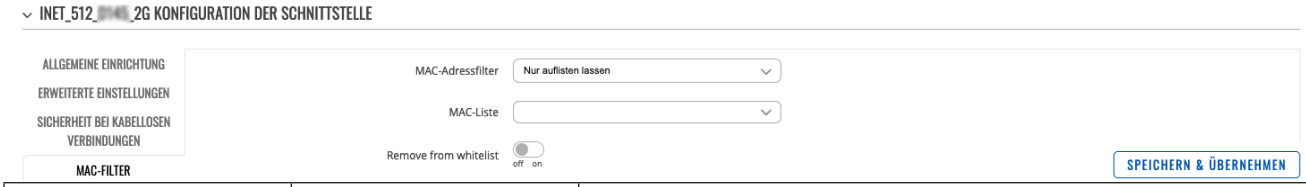


Feld	Wert	Beschreibung
Mesh-Peer-Traffic weiterleiten	Off | On ; Standard : Off	
RSSI-Schwellenwert für den Beitritt	Standard : keine	0 = RSSI-Schwelle nicht verwenden, 1 = Standardtreibereinstellungen nicht ändern.
Kurze Präambel	Off | On ; Standard : On	Verwenden Sie einen kurzen Präambel, der kürzere Datensequenzen verwendet, die weniger Daten zur Übertragung der Fehlerkontrollredundanz hinzufügen, wodurch die Übertragung wesentlich schneller erfolgt.
DTIM Interval	Standard : keine	Intervalle für die Lieferverkehrsindikationsmeldungen
Zeitintervall für die erneute Eingabe von GTK	Standard : keine	Zeitintervall zwischen automatischen Änderungen des Gruppenschlüssels, der von allen Geräten im Netzwerk gemeinsam genutzt wird.
Inaktivitätsabfrage deaktivieren	Off | On ; Standard : Off	Die Inaktivitätsabfrage kann deaktiviert werden, um Stationen basierend auf ihrer Inaktivitätszeit zu trennen, so dass inaktive Stationen wahrscheinlicher getrennt werden, auch wenn sie sich noch in Reichweite des Zugriffspunkts befinden.
Stationsinaktivitätslimit	Standard : keine	Inaktivitätslimit der Station in Sekunden. Wenn eine Station/Client während des ersten Zeitintervalls nichts sendet, wird ihr ein leerer Datenrahmen gesendet, um zu überprüfen, ob sie noch in Reichweite ist. Wenn dieser Rahmen nicht quittiert wird, wird die Station zuerst dissoziiert und dann deauthentifiziert.
Maximal zulässiges Hörintervall	Standard : keine	Die Assoziation wird abgelehnt, wenn ein Client/Station versucht, sich mit einem höheren Hear-Interval als diesem Wert zu verbinden.
Trennen Sie sich bei geringer Bestätigung	Off | On ; Standard : On	Erlaube dem AP-Modus, Stationen/Clients basierend auf einer schwachen Empfangsbestätigungsbedingung zu trennen.
WDS	Off | On ; Standard : Off	Ein Wireless Distribution System (WDS) ist ein System, das die drahtlose Interkonnektivität von Zugriffspunkten (AP) in einem Netzwerk ermöglicht.



Feld	Wert	Beschreibung
Verschlüsselung	Verschlüsselung | WPA-PSK | WPA2-PSK | Mode mixte WPA-PSK/ WPA2-PSK | WPA3-SAE | Mode mixte WPA2-PSK/ WPA3-SAE | WPA-EAP | WPA2-EAP | DEVOIR | Mode mixte WPA2-EAP/ WPA3-EAP | WPA3-EAP ; Standard : WPA2-PSK	Die Art der Verschlüsselung, die auf dieser drahtlosen Schnittstelle verwendet wird.
Mit allen Verschlüsselungen		
Cipher	Auto | CCMP (AES) erzwingen | TKIP erzwingen | TKIP und CCMP (AES) erzwingen Standard : Auto	Ein Algorithmus zur Verschlüsselung oder Entschlüsselung.
Mixed Mode WPA3-SAE, WPA2-PSK/WPA3-SAE.		
Passwort	Standard : keine	Ein persönlicher geheimer Satz zur Authentifizierung (mindestens 8 Zeichen).
WPA-EAP, WPA2-EAP, gemischter Modus WPA2-EAP/WPA3-EAP, WPA3-EAP.		
Radius-Authentifizierungsserver	Standard : keine	IP-Adresse des Authentifizierungsservers.
Radius-Authentifizierungs-Port	Standard : keine	Der Standardport des Servers ist 1812.
Radius-Authentifizierungs-Geheimnis	Standard : keine	Gemeinsames Geheimnis des Servers.
Radius-Accounting-Server	Standard : keine	IP-Adresse des Abrechnungsservers.
Radius-Accounting-Port	Standard : keine	Der Standardport des Servers ist 1813.
Radius-Accounting-Geheimnis	Standard : keine	Gemeinsames Geheimnis des Servers.
NAS id	Standard : keine	Netzwerkzugangsserver-Identifikator.

MAC-Filter



Feld	Wert	Beschreibung
MAC-Adressfilter	Deaktivieren | Nur auflisten lassen | Remove from whitelist ; Standard : Deaktivieren	Definiert, wie der MAC-Filter funktionieren soll. • Nur die Liste zulassen: Erlaubt nur Geräten mit den angegebenen MAC-Adressen, sich mit Ihrem drahtlosen Zugangspunkt zu verbinden. • Alle außer den aufgeführten zulassen: Verhindert, dass sich Geräte mit den angegebenen MAC-Adressen mit Ihrem drahtlosen Zugangspunkt verbinden.
MAC-Liste	MAC; Standard : keine	Liste der MAC-Adressen, die in die Verbindung zu Ihrem drahtlosen Zugangspunkt einbezogen oder davon ausgeschlossen werden sollen.
Remove from whitelist	Off | On ; Standard : Off	Erlaubt das Entfernen der MAC-Adresse aus der Whitelist, wenn das Gerät den IP-Blockierungszähler erreicht.

Client-Modus

Ein drahtloser Client-Modus (STA) ist eine vom Router erstellte Schnittstelle, die zur Verbindung mit einem drahtlosen Zugangspunkt verwendet wird. (Beispiel: öffentliches WLAN)

Das Erstellen einer Client-Station ist besonders nützlich, um Datenvolumen auf Ihrer SIM-Karte zu sparen, sofern ein öffentlicher WLAN-Zugangspunkt verfügbar ist.

HINWEIS: Das Hinzufügen einer WiFi-Schnittstelle im Client-Modus macht diese automatisch zur Priorität gegenüber allen anderen Schnittstellen (WAN und Mobile 4G). Dieser Modus sollte verwendet werden, wenn man einen Wi-Fi-Repeater zwischen einem öffentlichen Zugangspunkt und seinem PC, Tablet, Telefon oder einem anderen verbundenen Gerät erstellen möchte.

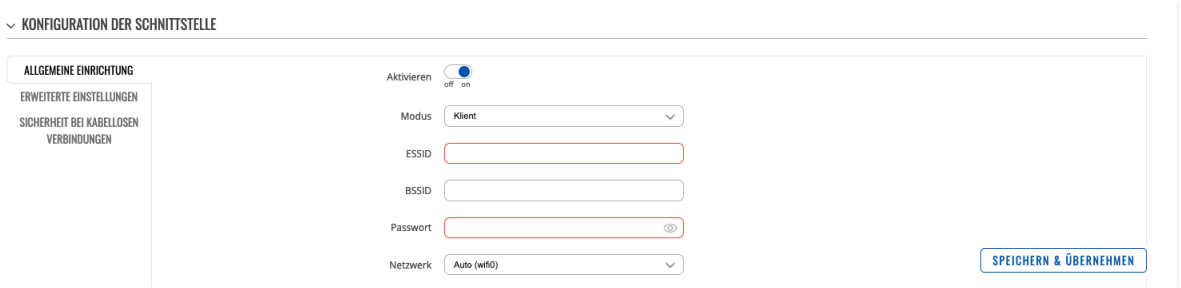
WICHTIG: Der I-NET 512-Router ist mit einem intelligenten Modul ausgestattet, das die Internetzugänglichkeit überwacht. Wenn die hinzugefügte Wi-Fi-Schnittstelle nicht mehr zugänglich ist, wechselt der Router automatisch zur nächsten verfügbaren Internetverbindung (WAN oder Mobile 4G).

Konfiguration des Client-Modus

Klicken Sie auf die Schaltfläche „SCAN“, um die in der Umgebung vorhandenen WiFi-Netzwerke zu analysieren.

Die Liste der verfügbaren WiFi-Zugangspunkte wird angezeigt.
Klicken Sie auf die Schaltfläche „Netzwerk beitreten“ des WiFi-Zugangspunkts, den Sie verwenden möchten.
Anschließend müssen Sie das WPA-Passwort des Zugangspunkts eingeben, mit dem Sie sich verbinden möchten.
Benennen Sie Ihr Netzwerk (dies wird der Name Ihrer WAN-WiFi-Schnittstelle sein) und weisen Sie eine Firewall-Zone zu (es wird empfohlen, die standardmäßig zugewiesene Zone beizubehalten).

Anschließend wird das Fenster Schnittstellenkonfiguration geöffnet. Die Werte hier werden durch den Zugangspunkt vorgegeben. Sie sollten unverändert bleiben, um Verbindungsprobleme zu vermeiden.



Klicken Sie auf 'Speichern und Anwenden', um die Konfiguration des Client-Modus zu bestätigen und sich mit dem öffentlichen Zugangspunkt zu verbinden.

WICHTIG: Nach Abschluss der Konfiguration des Client-Modus wird das Wi-Fi-Netzwerk des Routers automatisch neu gestartet. Die Verbindung mit diesem wird dann unterbrochen. Warten Sie während dieses Vorgangs, der bis zu 2 Minuten dauern kann. Abhängig vom verwendeten Webbrowser kann es erforderlich sein, Ihre Webseite zu aktualisieren, um erneut auf die Weboberfläche des Routers zuzugreifen.

Modus Gittergewebe (oder MESH)

I-NET 512 kann auch als Mesh-Gateway oder als Knoten (Router) konfiguriert werden, der sich mit einem Mesh-Gateway verbindet.

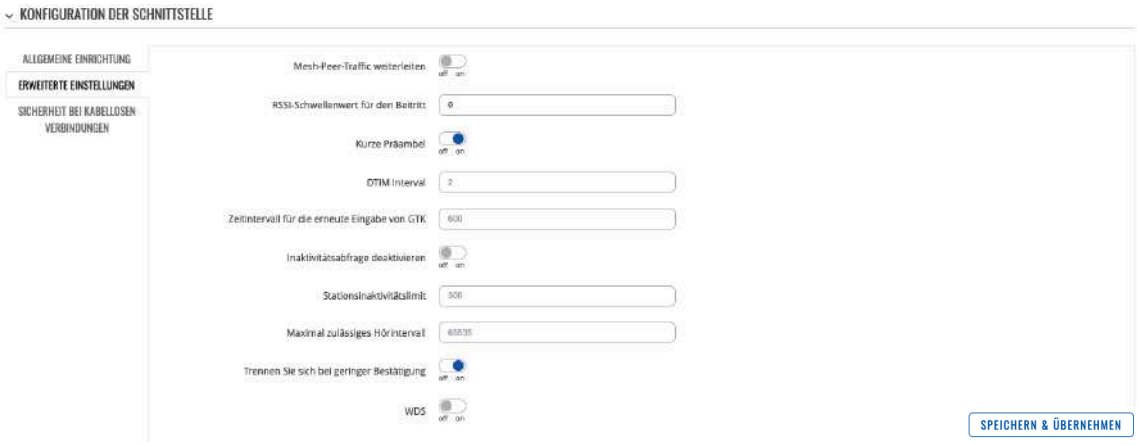
Wenn I-NET 512 als Mesh-Gateway konfiguriert ist, stellt es anderen Mesh-Knoten Internetzugang zur Verfügung. Wenn es als Mesh-Knoten konfiguriert ist, fungiert es als Mesh-Router, der den Datenverkehr zu und von dem Mesh-Gateway weiterleitet. Die Knoten verbinden auch andere drahtlose Geräte mit dem Netzwerk, wie Laptops und Mobiltelefone.

Bei der Konfiguration von I-NET 512 als Mesh-Gateway ist eine Internetverbindung erforderlich.

Um zu beginnen, klicken Sie auf die Schaltfläche "Hinzufügen"

"Im Reiter Allgemeine Konfiguration wählen Sie den Mesh-Modus, legen Sie die Mesh-ID fest (diese Nummer muss bei allen Knoten, die sich mit diesem drahtlosen Mesh-Netzwerk verbinden, gleich sein) und wählen Sie das gewünschte Netzwerk, das an die Schnittstelle angehängt wird. Klicken Sie auf Speichern und Anwenden."

Gehen Sie schließlich zum Reiter Erweiterte Einstellungen, aktivieren Sie 'Peer-Traffic im Mesh weiterleiten' und setzen Sie den 'RSSI-Schwellenwert zum Verbinden' auf -80. Lassen Sie den Rest auf den Standardwerten. Klicken Sie auf Speichern und Anwenden. Wenn die Konfiguration korrekt durchgeführt wurde, wird das Wi-Fi-Mesh-Gateway funktionieren.



Gehen Sie dann zum Reiter Wi-Fi-Sicherheit und wählen Sie die Verschlüsselung WPA3-SAE, um eine zusätzliche Authentifizierungsebene hinzuzufügen. Das Passwort muss bei allen Geräten im Mesh-Netzwerk gleich sein.

Mesh-Knoten

Der Mesh-Knoten wird genauso konfiguriert wie das Mesh-Gateway. Der Knoten muss der Konfiguration der Wi-Fi-Mesh-Schnittstelle des Gateways entsprechen. Außerdem muss die LAN-Schnittstelle als DHCP-Client konfiguriert werden:

1. Greifen Sie über das Menü Netzwerk → Schnittstellen auf die Web-Oberfläche des Routers zu.
2. Klicken Sie auf das Symbol rechts neben der WAN-Schnittstelle.

3. Ändern Sie das Protokoll auf DHCP

Klicken Sie auf 'Speichern und anwenden'. Wenn die Konfiguration korrekt durchgeführt wurde, wird der Mesh-Modus funktionsfähig sein.

Mehrere Zugangspunkte

Einführung:

Die Funktion "Multi AP" ermöglicht die Verwaltung einer Gruppe von Wi-Fi-Netzwerken unter einer einzigen Schnittstelle. Um eine Multi-AP-Wireless-Schnittstelle zu erstellen, klicken Sie auf die Schaltfläche "Hinzufügen" unten

auf der drahtlosen Oberfläche.
Der Router überwacht kontinuierlich alle angegebenen Wi-Fi-Netzwerke und wählt das leistungsfähigste Netzwerk aus, um es dem Benutzer zur Verfügung zu stellen.
Ähnlich wie bei der "Client-Service"-Funktion hat eine "Multi AP" Wi-Fi-Schnittstelle Vorrang vor WAN- und Mobile-4G-Schnittstellen in der Schnittstellenliste.
Diese Funktion kann genutzt werden, um einen Wi-Fi-Repeater zwischen Ihrem Computer und einem beliebigen Wi-Fi-Netzwerk aus der Liste der "Multi AP" Funktion zu erstellen, ohne sich um den Zustand der verschiedenen Wi-Fi-Netzwerke kümmern zu müssen.

WICHTIG: Der Router I-NET 512 ist mit einem intelligenten Modul ausgestattet, das die Internetzugänglichkeit über verschiedene Schnittstellen überprüft. Wenn eine erstellte Wi-Fi-Schnittstelle nicht erreichbar ist, wechselt der Router automatisch zur nächsten betriebsbereiten Schnittstelle (WAN oder Mobile 4G).

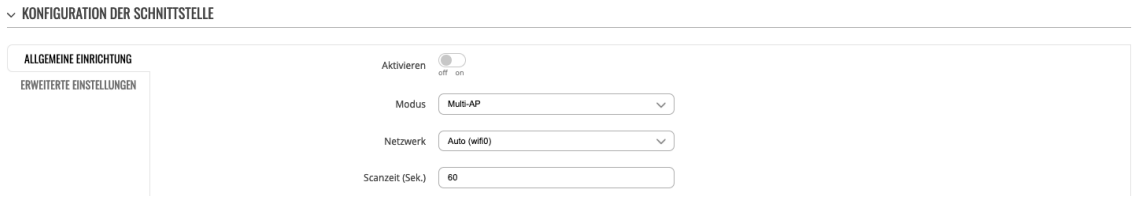
Allgemeine Einstellungen

Aktivieren Sie in der Rubrik "Allgemeine Einstellungen" die Funktion "Multi AP". Sie können die Häufigkeit der Überprüfung der Verfügbarkeit öffentlicher Wi-Fi-Zugangspunkte ändern.

Feld	Wert	Beschreibung
Aktivieren	Off | On; Standard : Off	Aktivieren oder Deaktivieren der Multi-AP-Konfiguration.
Modus	Klient | Zugangspunkt | Mesh/Gittergewebe | Multi-AP ; Standard : Multi-AP	Festlegen der Rolle dieser Schnittstelle: Access Point, um Wi-Fi für andere Geräte bereitzustellen; Client, um Wi-Fi von anderen Geräten für WWAN zu nutzen; Mesh, um als Gateway oder Knoten in einem Mesh-Netzwerk zu fungieren.
Scanzeit (Sek.)	Standard : 60	Intervall (in Sekunden) für die Verfügbarkeitsprüfung von Wi-Fi-Zugangspunkten.
AP-Liste hochladen	(interaktive Schaltfläche)	Herunterladen einer Liste von Wi-Fi-Konfigurationen.

Zugangspunkte

In der Rubrik "Zugangspunkte" geben Sie die verschiedenen öffentlichen Wi-Fi-Zugangspunkte ein, mit denen Sie sich verbinden möchten. Klicken Sie für jeden Zugangspunkt auf die Schaltfläche HINZUFÜGEN und geben Sie die SSID und das Passwort ein. Nachdem Sie alle Informationen eingegeben haben, klicken Sie auf die Schaltfläche SPEICHERN und ANWENDEN.
Hinweis: Vergessen Sie nicht, jeden Zugangspunkt zu aktivieren, indem Sie den Schalter auf der rechten Seite auf "Ein" setzen.



Feld	Wert	Beschreibung
SSID	Standard : keine	SSID eines Zugangspunkts
Mot de passe	Standard : keine	Passwort, das zur Authentifizierung des Benutzers verwendet wird (mindestens 8 Zeichen)
Activer	Off | On; Standard : Off	Aktiviert oder deaktiviert einen Zugangspunkt
Supprimer	(interaktive Schaltfläche)	Entfernt den Zugangspunkt aus der Liste

Es ist möglich, eine Liste von Zugangspunkten aus einer Datei hochzuladen, indem Sie die Schaltfläche DURCHSUCHEN verwenden. Hier ist ein Beispiel für das Dateiformat:
Verbindungskennung: INET_1
Aktivieren: 1
Schlüssel: 12345678
SSID: INET_2
Aktivieren: 0
Schlüssel: 87654321

HINWEIS : Um eine 'Multi AP'-Schnittstelle im WLAN-Menü zu löschen, wechseln Sie in den 'Erweiterten' Modus und klicken Sie auf die Schaltfläche mit dem entsprechenden Kreuz.

WiFi QR-Codes

Jede WiFi-Schnittstelle verfügt über einen speziell gestalteten QR-Code, der Informationen zur SSID und zum Passwort des WiFi-Netzwerks enthält. Nachdem Sie auf die Schaltfläche für den manuellen WiFi-QR-Code gedrückt haben, wird ein QR-Code mit der SSID und dem Passwort des Netzwerks angezeigt, den Sie lokal herunterladen können, indem Sie auf die Schaltfläche „QR-Code herunterladen“ klicken. Wenn Sie nur einen QR-Code ohne zusätzliche Informationen wünschen, deaktivieren Sie das Kontrollkästchen „Referenzen einschließen.

2.5 MENÜ NETZWERK > FAILOVER

Das MENÜ NETZWERKVERWALTUNG ermöglicht die Steuerung der verschiedenen Netzwerkschnittstellen des Routers mit Hilfe von separaten Modulen: Netzwerkverwaltung und Datenverteilung.

Netzwerkverwaltung:

Das Modul Netzwerkverwaltung ist ein intelligentes Modul, das kontinuierlich die Internetzugänglichkeit über die verschiedenen Schnittstellen im unten stehenden Tabellenformat überprüft. Dazu sendet es auf jeder Netzwerkschnittstelle in regelmäßigen Abständen eine Anfrage ins Internet und wartet auf eine Antwort.

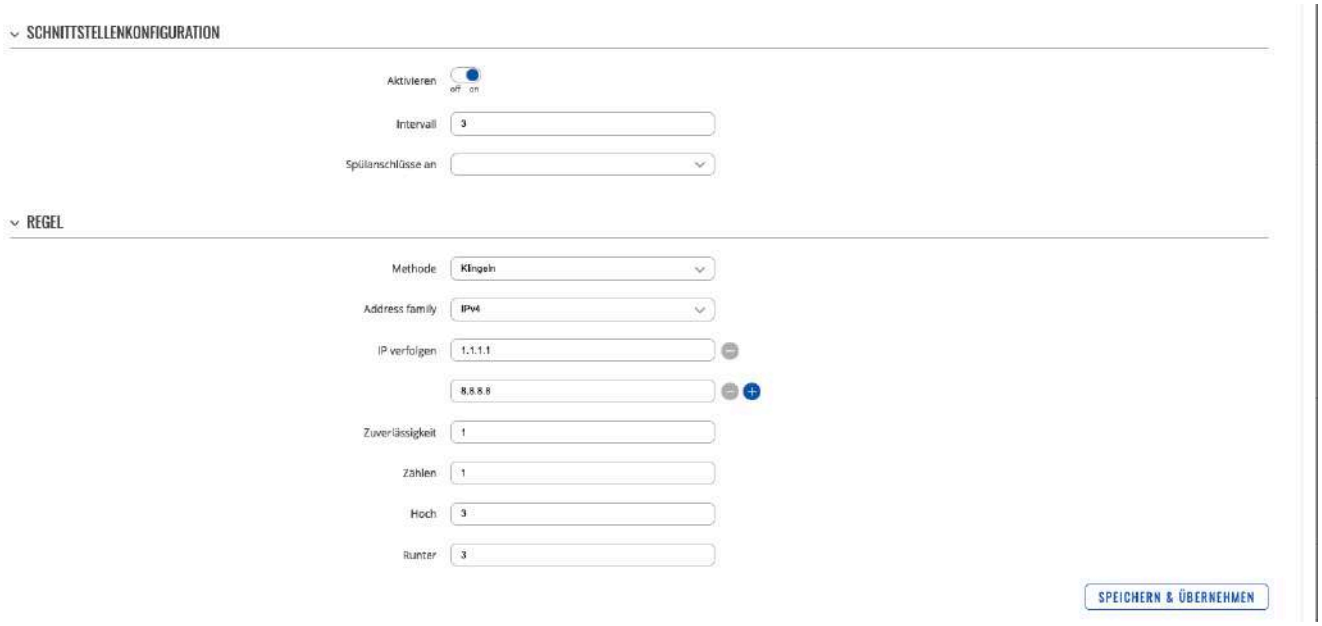
Die Netzwerkschnittstelle, die für den Internetzugang verwendet wird, ist diejenige, deren Status "Online" ist und die sich an erster Stelle in der Liste befindet.

Die Netzwerkschnittstellen sind nach einer festgelegten Prioritätsreihenfolge in der linken Spalte sortiert. Die Schnittstelle mit der höchsten Priorität befindet sich auf der ersten Zeile der Tabelle. Bei Bedarf können Sie die Priorität jeder Netzwerkschnittstelle ändern, indem Sie den Cursor auf das Kreuz ganz links jeder Zeile bewegen und klicken.

Konfiguration der Schnittstelle:

Ein Interface-Konfigurationsmenü wird verwendet, um festzulegen, wie das Gerät bestimmt, ob eine Schnittstelle online oder offline ist. Um zu einer Interface-Konfigurationsseite zu gelangen, klicken Sie auf die Schaltfläche "Bearbeiten" neben einer Schnittstelle.

Daraufhin werden Sie zur Konfigurationsseite dieser Schnittstelle weitergeleitet.

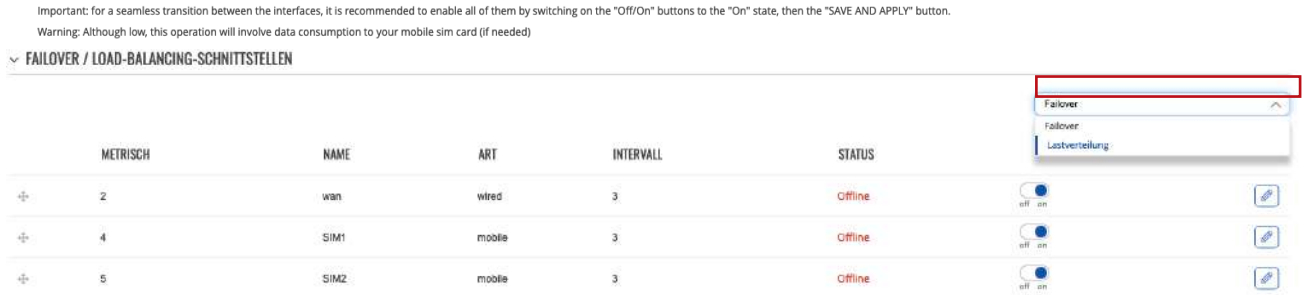


Feld	Wert	Beschreibung
Aktivieren	Off | On; Standard : On	Schnittstelle aktivieren/deaktivieren
Intervall	Standard : 3	Sekundenanzahl zwischen den einzelnen Prüfungen
Verbindungen leeren	Verbunden | Getrennt : Standard : keine	Leert die nachdem Szenario hergestellten Verbindungen
Methode	Standard : Klingeln	Legt fest, wie die Statusprüfung bei dieser Schnittstelle durchgeführt wird, wenn ihr Status ermittelt wird.
Address family	IPv4 | IPv6 Standard : IPV4	
IP verfolgen	Standard : 1.1.1.1,8.8.8.8	IP-Adresse(n) oder Hostname(n), die verwendet werden, um den Status einer Schnittstelle zu bestimmen. Wenn das Gerät keine Antwort von einem der angegebenen Hosts erhält, wird die Schnittstelle als „offline“ betrachtet. Wenn dieser Wert fehlt, wird die Schnittstelle immer noch als aktiv betrachtet.
Zuverlässigkeit	Standard : 1	Anzahl der Hosts, die antworten müssen, damit der Test als bestanden gilt. Stellen Sie sicher, dass es mindestens diese Anzahl von Hosts gibt, die im Feld „Track IP“ definiert sind, sonst wird die Schnittstelle immer als „Offline“ betrachtet.
Zählen	Standard : 1	Anzahl der Pings, die mit jedem Test an jeden Host gesendet werden sollen.
Hoch	Standard : 3	Anzahl der erfolgreichen Tests, die erforderlich sind, um eine Schnittstelle als 'Online' zu betrachten.
Runter	Standard : 3	Anzahl der fehlgeschlagenen Tests, die erforderlich sind, um eine Schnittstelle als „Offline“ zu betrachten.

Datenverteilung:

Die Datenverteilung ist ein Modul zur Verteilung des Datenverkehrs zwischen mehreren Schnittstellen. Mit der Datenverteilung können Datenlasten zwischen verschiedenen Schnittstellen geteilt werden, um die Internetgeschwindigkeit für mehrere Benutzer und Verbindungen zu erhöhen. Die Datenlast erhöht jedoch nicht die Geschwindigkeit für eine einzelne Verbindung.Die Datenverteilung kann jedoch verwendet werden, um die Geschwindigkeit mehrerer Verbindungen zu erhöhen.

HINWEIS: Datenverteilung und Netzwerkverwaltung können nicht gleichzeitig verwendet werden. Wenn Sie das Datenverteilungsmodul auswählen möchten, klicken Sie auf das Dropdown-Menü in der oberen rechten Ecke der Seite:



Nachfolgend finden Sie ein Beispiel für die Datenverteilungsseite.

Wenn die Datenverteilung ausgewählt ist, können Sie verschiedenen Schnittstellen Prozentwerte zuweisen. Der Prozentsatz repräsentiert den Anteil des Datenverkehrs, der über eine Schnittstelle läuft.

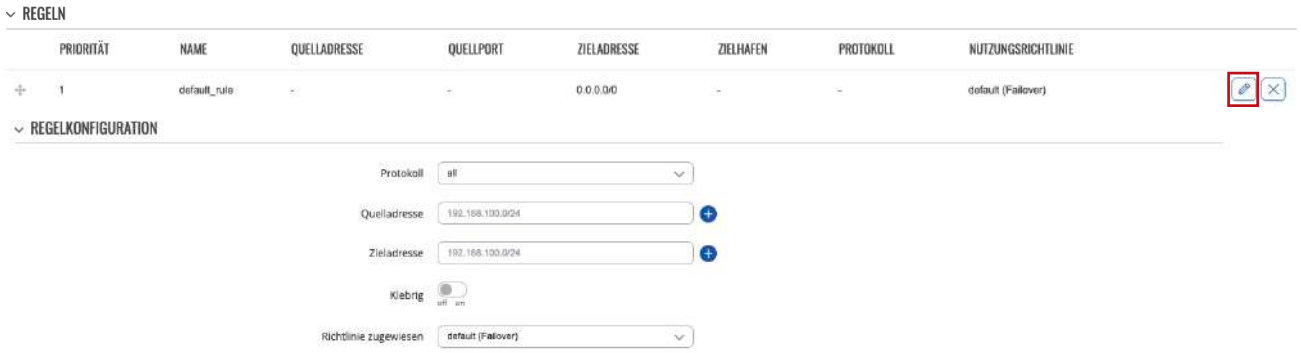
Beispiel: Wenn Sie die Ratio wie folgt konfigurieren:

- Verkabeltes WAN-Verhältnis: 3
- Mobiles WAN-Verhältnis: 2

Etwa 60 % (3/5) des Datenverkehrs würde über die verkabelte WAN-Schnittstelle und etwa 40 % (2/5) über die mobile WAN-Schnittstelle laufen. In diesem Fall würden von 100 verschiedenen Videos, die Sie im Internet anschauen, etwa 60 über die verkabelte WAN-Schnittstelle und die restlichen 40 über die mobile WAN-Schnittstelle gestreamt.

Regeln

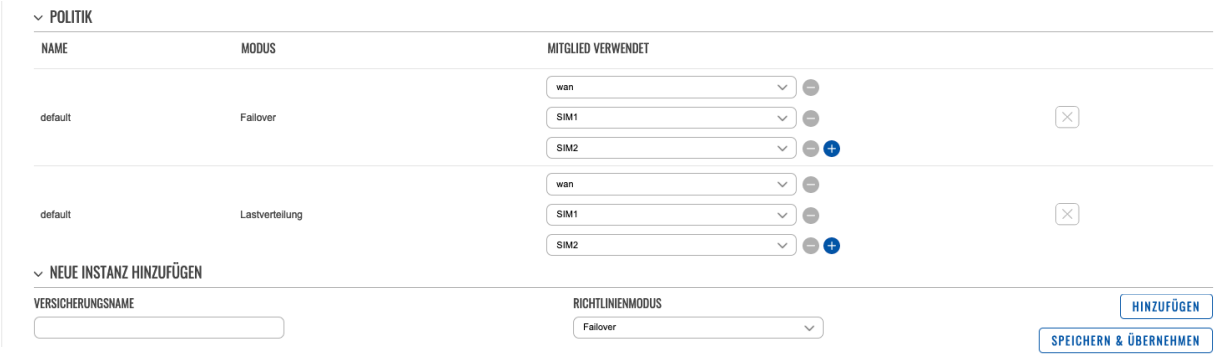
Eine Regel zur Lastverteilung/failover ist eine Reihe von Bedingungen, die eine bestimmte Art von Netzwerkverkehr definieren.
Auf dem Gerät ist eine Standardregel vorhanden. Sie können weitere Regeln hinzufügen, indem Sie auf die Schaltfläche „Hinzufügen“ klicken, oder Sie können die vorhandene Regel anpassen, indem Sie auf die Schaltfläche „Bearbeiten“ daneben klicken:



Feld	Wert	Beschreibung
Protokoll	All | TCP | UDP | ICMP | ESP ; Standard : All	Protokoll, das dieser Regel entspricht.
Quelladresse	IP/Netzmaske ; Standard : keine	Quell-IP-Adressen, die dieser Regel entsprechen.
Zieladresse	IP/Netzmaske; Standard : 0.0.0.0/0	Ziel-IP-Adressen, die dieser Regel entsprechen.
Klebrig	Off | On ; Standard : Off	Wenn diese Option aktiviert ist, wird der Datenverkehr von derselben Quell-IP-Adresse, der zuvor dieser Regel innerhalb der persistenten Wartezeit entsprochen hat, dieselbe WAN-Schnittstelle verwenden.
Sticky-Timeout	Valeur [1..1000000] ; Standard : keine	Wartezeit in Sekunden.
Richtlinie zugewiesen	Default (Failover) | default (Lastverteilung) | Nicht erreichbar (Ablehnen) | Schwarzes Loch (Tropfen) | Standard (Hauptroutingtabelle verwenden) Standard : default (Failover)	Wählen Sie die Richtlinie aus, die auf den Datenverkehr angewendet werden soll, der den Bedingungen dieser Regel entspricht. Sie können benutzerdefinierte Richtlinien zur Datenverteilung/zum Netzwerkmanagement im unten stehenden Abschnitt erstellen.

Politik

Eine Politik legt fest, was das Gerät tun soll, wenn ein Teil des Netzwerkverkehrs der in einer Regel zur Datenverteilung/zum Netzwerkmanagement definierten Bedingung entspricht. Sie können benutzerdefinierte Richtlinien erstellen, die verschiedene Schnittstellen für die Datenverteilung/das Netzwerkmanagement verwenden.



Feld	Wert	Beschreibung
Mitglied verwendet	wan | SIM1 | SIM2 ; Standard : WAN	Damit eine Netzwerkschnittstelle in mwan3 verwendet werden kann, muss sie als Mitglied definiert werden, das dann in den Richtlinien verwendet werden kann.

3. Menü SERVICES

3.1 Menü SERVICES > CLOUD-LÖSUNGEN

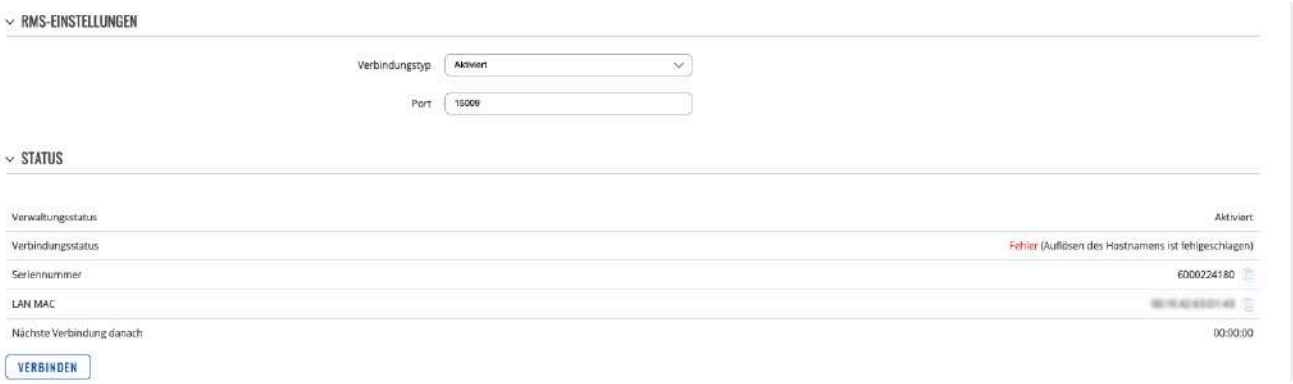
Das Remote-Services-Menü wird verwendet, um zu konfigurieren, wie das Gerät mit dem Remote-Services-System verbunden ist, das vom Fernsteuerungssystem verwendet wird.

3.1.1 Menu SERVICES > CLOUD-LÖSUNGEN > RMS

I-NET-512 integriert eine cloudbasierte Lösung, die für Remote-Management-Dienste wie Updates oder Wartung verwendet wird. Um einen ordnungsgemäßen Betrieb des Fernzugriffs sicherzustellen, sollten die Einstellungen in diesem Menü nicht geändert werden."

**Dienstleistungen, die von ALDEN unter Bedingungen angeboten werden.

In der Abbildung unten handelt es sich um einen Screenshot des RMS-Bereichs



Feld	Wert	Beschreibung
Verbindungstyp	Standard : Aktiviert	Legt fest, wie das Gerät eine Verbindung herstellt: • Aktiviert – Das Gerät versucht alle 2 bis 5 Minuten eine Verbindung herzustellen (alle 2 Minuten in der ersten Stunde, dann alle 5 Minuten). Wenn es sich 14 Tage lang nicht verbinden kann, wechselt es in den Schlafmodus. • Schlafmodus – Das Gerät versucht alle 6 Stunden eine Verbindung herzustellen. • Deaktiviert – Die Funktion ist deaktiviert.
Port	Standard : 15009	Portnummer für die Verbindung, lassen Sie den Standardport (15009) stehen.

Der RMS-Server wartet auf eingehende Verbindungen. Da das Gerät in regelmäßigen Abständen versucht, eine Verbindung herzustellen, kann es nicht sofort verbunden sein. Während es getrennt ist, können Sie die verbleibende Zeit bis zum nächsten Verbindungsversuch im Abschnitt Status überprüfen.

3.2 Menü SERVICES > VPN

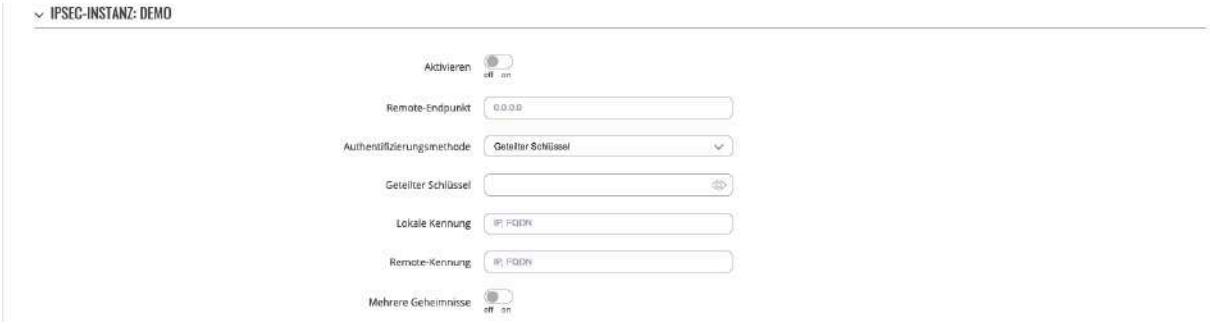
Ein Virtual Private Network (VPN) ist eine Methode, um mehrere private Netzwerke über das Internet zu verbinden. VPNs können dazu dienen, verschiedene Ziele zu erreichen, aber einige ihrer Hauptziele sind:

- Zugang zwischen entfernten privaten Netzwerken;
- Verschlüsselung von Daten;
- Anonymität beim Surfen im Internet.

3.2.1 Menü SERVICES VPN > IPSEC

Um eine neue IPsec-Instanz zu erstellen, gehen Sie zu Abschnitt Dienste → VPN → IPsec, geben Sie einen benutzerdefinierten Namen ein und klicken Sie auf die Schaltfläche „Hinzufügen“. Eine IPsec-Instanz mit dem angegebenen Namen wird in der Liste „IPsec-Konfiguration“ angezeigt.

Der Abschnitt der allgemeinen Einstellungen ermöglicht die Konfiguration der wichtigsten IPsec-Parameter. Beziehen Sie sich auf die Abbildung und die Tabelle unten für weitere Informationen zu den Konfigurationsfeldern, die sich im Abschnitt der allgemeinen Einstellungen befinden.



Feld	Wert	Beschreibung
Aktivieren	Off | On; Standard : Off	Aktiviert oder deaktiviert die IPsec-Instanz.
Remote-Endpunkt	Host | IP-Adresse ; Standard : keine	IP-Adresse oder Hostname der entfernten IPsec-Instanz.
Authentifizierungsmethode	Geteilter Schlüssel | X.509 | EAP ; Standard : Geteilter Schlüssel	Geben Sie die Authentifizierungsmethode an. Wählen Sie zwischen dem vorab geteilten Schlüssel und X.509-Zertifikaten.
Geteilter Schlüssel : Geteilter Schlüssel	Standard : keine	Gemeinsam genutztes Passwort, das zur Authentifizierung zwischen den IPsec-Peers vor der Einrichtung eines sicheren Kanals verwendet wird.
X.509 | EAP : Schlüssel	Eine Datei mit einem privaten Schlüssel; Standard: keine	Eine Datei mit einem privaten Schlüssel.
X.509 | EAP : Key decryption passphrase	Ein Passwort für die Dateien mit privaten Schlüsseln; Standard: keine	Falls die Datei mit dem privaten Schlüssel verschlüsselt ist, muss die Passphrase festgelegt werden.
X.509 | EAP : Lokales Zertifikat	.der-Datei ; Standard : keine	Lokale Zertifikatsdatei.

X.509 | EAP : CA-Zertifikat	.der-Datei ; Standard : keine	Zertifizierungsstellen-Zertifikatdatei.
Lokale Kennung	IP-Adresse | Zeichenkette; Standard : keine	Definiert, wie der Benutzer (Teilnehmer auf der linken Seite) bei der Authentifizierung identifiziert wird. • IP: Internet Protocol-Adresse. • FQDN: Vollqualifizierter Domänenname. Dies ist der vollständige Domänenname eines Hosts (z. B. something.somedomain.com). Nur mit IKEv2 unterstützt.
Remote-Kennung	IP-Adresse | Zeichenkette; Standard : keine	Definiert, wie der richtige Teilnehmer bei der Authentifizierung identifiziert wird: • IP: Internet-Protokoll-Adresse. • FQDN: Identität durch einen vollständigen Domainnamen definiert. Dies ist der vollständige Domainname eines Hosts (zum Beispiel etwas. somedomain.com). Unterstützt nur mit IKEv2.
Globale Kennung	Off | On; Standard : Off	Aktiviert den Abschnitt Einstellungen für globale Kennung , um mehrere Kennungen einzurichten

Zusätzliche Hinweise:
Einige Konfigurationsfelder stehen nur zur Verfügung, wenn bestimmte andere Parameter ausgewählt sind. Die Namen der Parameter werden von einem Präfix begleitet, das angibt, unter welcher Art der Authentifizierung sie sichtbar werden. Unterschiedliche Farbcodes werden für verschiedene Präfixe verwendet:
• Grün für die Authentifizierungsmethode: Pre-Shared Key
• Dunkelrot für die Authentifizierungsmethode: X.509/EAP

Allgemeine geheime Einstellungen

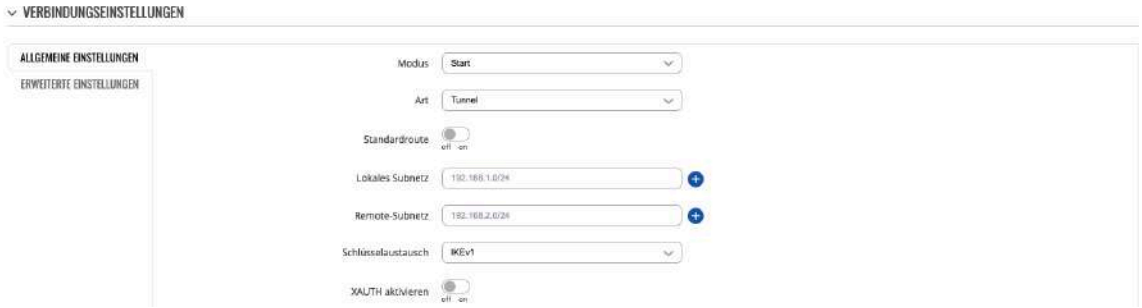
Dieser Abschnitt wird angezeigt, wenn Mehrfachgeheimnisse in den allgemeinen Einstellungen aktiviert sind. Sie können neue Instanzen hinzufügen, indem Sie auf 'Hinzufügen' klicken.

Feld	Wert	Beschreibung
ID-Selektor	%any, IP ou FQDN ; Standard : keine	Jedes Geheimnis kann von einer optionalen Liste von ID-Selektoren begleitet werden. Ein Selektor kann eine IP-Adresse, eine vollständige Domäne, ein Benutzer@ FQDN oder %any sein. Bei der Verwendung von IKEv1 verwenden Sie die IP-Adresse. HINWEIS: IKEv1 unterstützt nur den ID-Selektor für IP-Adressen.
Art	PSK | XAUTH | PAE | RSA ; Standard : PSK	Typ des IPSec-Geheimnisses. HINWEIS: XAUTH-Geheimnisse sind nur für IKEv1.
Geheimnis	Standard : keine	Gemeinsames Passwort zur Authentifizierung zwischen Peers. Die minimale Länge beträgt 5 Zeichen. Alle Zeichen sind erlaubt außer
RSA : Geheimnis	Private-Schlüssel-Datei; Standard : keine	Private Schlüsseldatei.
RSA : Key decryption passphrase	Passphrase ; Standard : keine	Wenn die private Schlüsseldatei verschlüsselt ist, muss das Passwort festgelegt werden.

IPsec-Instanz: Verbindungseinstellungen

Der Abschnitt der Verbindungseinstellungen ermöglicht die Konfiguration der wichtigsten Parameter einer IPsec-Verbindung. Bitte beziehen Sie sich auf die Abbildung und die nachstehende Tabelle für weitere Informationen zu den Konfigurationsfeldern im Abschnitt der Verbindungseinstellungen.

Allgemeine Einstellungen



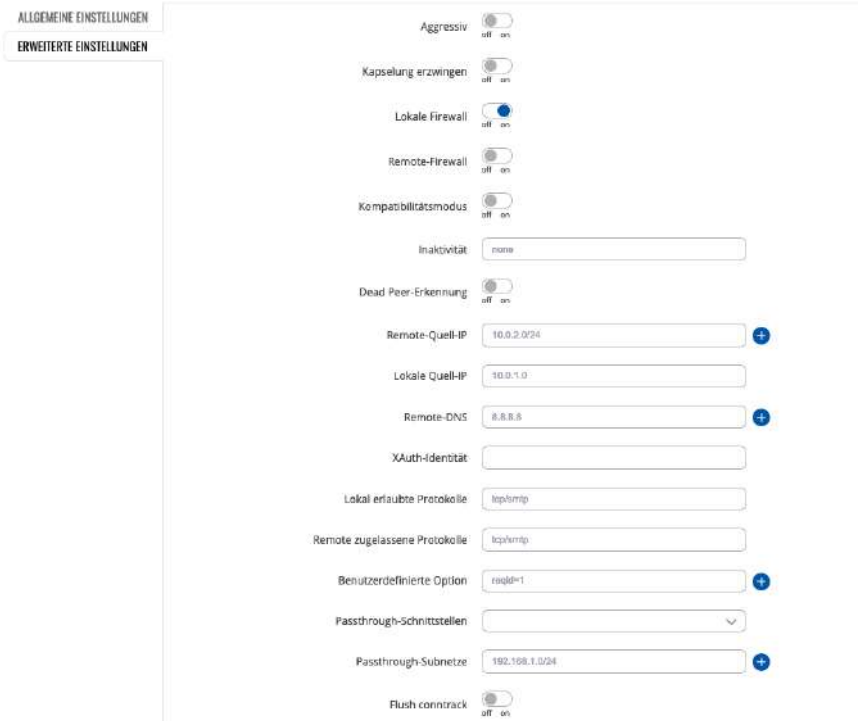
Feld	Wert	Beschreibung
Modus	Start | Hinzufügen | Route ; Standard : Start	Legt fest, welche Operation automatisch beim Start von IPSec durchgeführt wird.
Art	Tunnel | Transport ; Standard : Art	Verbindungstyp: • Tunnel: Schützt interne Routing-Informationen, indem das gesamte IP-Paket (IP-Header und Nutzlast) eingekapselt wird. Häufig verwendet bei standortübergreifenden VPN-Verbindungen; unterstützt NAT-Traversal. • Transport: Kapselt nur die IP-Nutzdaten ein. Wird bei VPN-Verbindungen Client-zu-Site verwendet; unterstützt kein NAT-Traversal; üblicherweise implementiert mit anderen Tunneling-Protokollen (z. B. L2TP).
Tunnel : Standardroute	Off | On; Standard : Off	Aktivieren Sie diese Option, um den gesamten Datenverkehr über den IPSec-Tunnel zu leiten.
Tunnel : Lokales Subnetz	Standard : keine	Lokale IP-Adresse und Subnetzmaske, die verwendet werden, um festzulegen, welcher Teil des Netzwerks im VPN-Netzwerk zugänglich ist. Der Netzwerkmaskenbereich liegt zwischen [0..32]. Wenn dieses Feld leer gelassen wird, wird die IP-Adresse automatisch ausgewählt.
Tunnel : Remote-Subnetz	Standard : keine	IP-Adresse des entfernten Netzwerks und Subnetzmaske, die verwendet werden, um festzulegen, welcher Teil des Netzwerks im VPN zugänglich ist. Der Bereich der Netzwerkmasken liegt zwischen [0..32]. Diese Adresse muss sich von der LAN-IP-Adresse des Geräts unterscheiden.
Transport : Zu binden	Standard : keine	Verbinden Sie sich mit der GRE- oder L2TP-Schnittstelle, um GRE/L2TP über IPSec zu erstellen.
Schlüsselaustausch	IKEv1 | IKEv2 ; Standard : IKEv1	Internet Key Exchange (IKE) Version für den Schlüsselaustausch: • IKEv1 – häufiger verwendet, aber bekannt für Probleme wie NAT-Traversal. • IKEv2 – aktualisierte Version mit erweiterten und verbesserten Funktionen wie integrierte NAT-Unterstützung, Unterstützung für Multi-Hosting, Verzicht auf veraltete Austauschmodi (kein Main oder Aggressive Mode; nur 4 Nachrichten zum Aufbau einer Verbindung erforderlich).
XAUTH aktivieren	Off | On; Standard : Off	Aktiviere erweiterte Authentifizierung.

Hinweise:

Einige Konfigurationsfelder sind nur verfügbar, wenn bestimmte andere Einstellungen ausgewählt sind. Die Parameter werden von einem Präfix begleitet, das den Authentifizierungstyp angibt, unter dem sie sichtbar werden. Unterschiedliche Farbcodes werden für unterschiedliche Präfixe verwendet:

- Rot für Typ: Tunnel
- Blau für Typ: Transport

Erweiterte Einstellungen

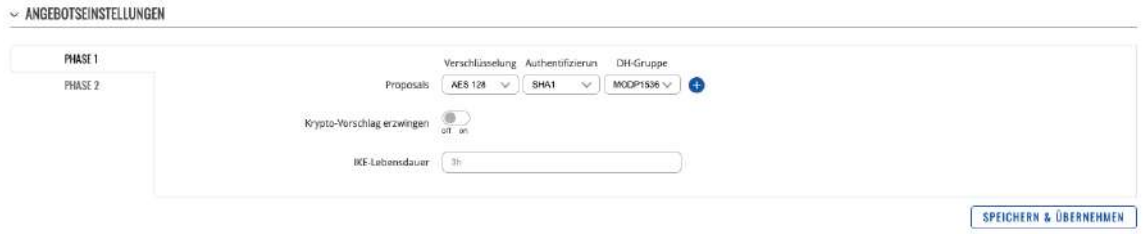


Feld	Wert	Beschreibung
Aggressiv	Off | On ; Standard : Off	Aktivieren oder deaktivieren Sie den aggressiven Modus für ausgehende Verbindungen. Der aggressive Modus führt weniger Austauschvorgänge (insgesamt 4 Nachrichten) durch als der Hauptmodus (insgesamt 6 Nachrichten), indem er die meisten Daten im ersten Austauschvorgang speichert. Im aggressiven Modus werden die Informationen ausgetauscht, bevor es einen sicheren Kanal gibt, wodurch er weniger sicher, aber schneller als der Hauptmodus ist.
Kapselung erzwingen	Off | On ; Standard : Off	Erzwingt die UDP-Kapselung für ESP-Pakete, selbst wenn eine "Kein NAT"-Situation erkannt wird.
Lokale Firewall	Off | On ; Standard : On	Fügt die notwendigen Firewallregeln hinzu, um den Datenverkehr dieser IPsec-Instanz auf diesem Gerät zuzulassen.
Remote-Firewall	Off | On ; Standard : On	Fügt die notwendigen Firewallregeln hinzu, um den Datenverkehr von der gegnerischen IPsec-Instanz auf diesem Gerät zuzulassen.
Kompatibilitätsmodus	Off | On ; Standard : Off	Aktiviert den Kompatibilitätsmodus, um die Verwaltung eines entfernten Peers eines Drittanbieters mit mehreren Subnetzen zu erleichtern.
Inaktivität	Standard : keine	Legt ein Timeout-Intervall fest, nach dem eine CHILD_ SA geschlossen wird, wenn sie keinen Datenverkehr gesendet oder empfangen hat.
Dead Peer-Erkennung	Off | On ; Standard : Off	Funktion, die beim Internet Key Exchange (IKE) verwendet wurde, um einen "toten" Peer zu erkennen. Sie reduzierte den Datenverkehr, indem sie die Anzahl der Nachrichten minimierte, wenn der gegenüberliegende Peer nicht verfügbar war, und diente als Ausfallsicherungsmechanismus.

Dead Peer-Erkennung : action DPD	Neustart | Halt | einverstanden | Keine; Standard : Neustart	Steuerung der Verwendung von Dead Peer Detection (DPD), bei der periodisch Benachrichtigungsnachrichten gesendet werden, um die Verfügbarkeit des IPsec-Peer zu überprüfen.
Dead Peer-Erkennung : DPD-Verzögerung	Standard : keine	Frequenz zum Senden von R_U_THERE-Nachrichten oder INFORMATIONAL-Austauschen an einen Peer.
Dead Peer-Erkennung : DPD-Zeitüberschreitung	Standard : keine	Legt das Timeout-Intervall fest, nach dem alle Verbindungen zu einem Peer aufgrund von Inaktivität gelöscht werden.
XAuth-Identität	Standard : keine	Der Benutzername, den der Client verwendet, um auf eine XAuth-Anfrage zu antworten. Wenn nicht festgelegt, wird die IKEv1-Identität als XAuth-Identität verwendet.
Tunnel : Remote-Quell-IP	Adresse IP ; Standard : keine	Die interne Quell-IP-Adresse, die in einem Tunnel für den entfernten Peer verwendet werden soll (Rechts).
Tunnel : Lokale Quell-IP	Adresse IP ; Standard : keine	Die interne Quell-IP-Adresse (links), die in einem Tunnel verwendet werden soll, auch als virtuelle IP bezeichnet.
Tunnel : Remote-DNS	Adresse IP ; Standard : keine	Liste der DNS-Serveradressen zum Austausch als Konfigurationsattribute. Auf dem Responder sind nur feste IPv4/IPv6-Adressen erlaubt und definieren die DNS-Server, die dem Client zugewiesen sind.
Lokal erlaubte Protokolle	Standard : keine	Zulässige Protokolle und Ports für die Verbindung, auch als Port-Selektoren bekannt. Werden definiert in Form von 'Protokoll/Port', z. B. '17/1701' oder '17/%any' oder 'udp/l2f'.
Remote zugelassene Protokolle	Standard : keine	Zugelassene Protokolle und Ports für die Verbindung, auch als Port-Selektoren bekannt. Werden in Form von 'Protokoll/Port' definiert, z. B. '17/1701' oder '17/%any' oder 'udp/l2f'.
Benutzerdefinierte Option	Standard : keine	Fügen Sie benutzerdefinierte Verbindungseinstellungen hinzu.
Interfaces Passthrough (Traversant)	Adresse IP ; Standard : keine	Die interne Quell-IP-Adresse (links), die in einem Tunnel verwendet werden soll, auch als virtuelle IP bezeichnet.
Tunnel :Passthrough-Schnittstellen	Netzwerkschnittstellen; Standard : keine	Netzwerkschnittstellen, die in IPsec Passthrough einbezogen werden sollen.
Tunnel : Passthrough-Subnetze	IP/Netzmaske ; Standard : keine	Netzwerke, die in IPsec Passthrough einbezogen werden sollen.

Zusätzliche Hinweise:

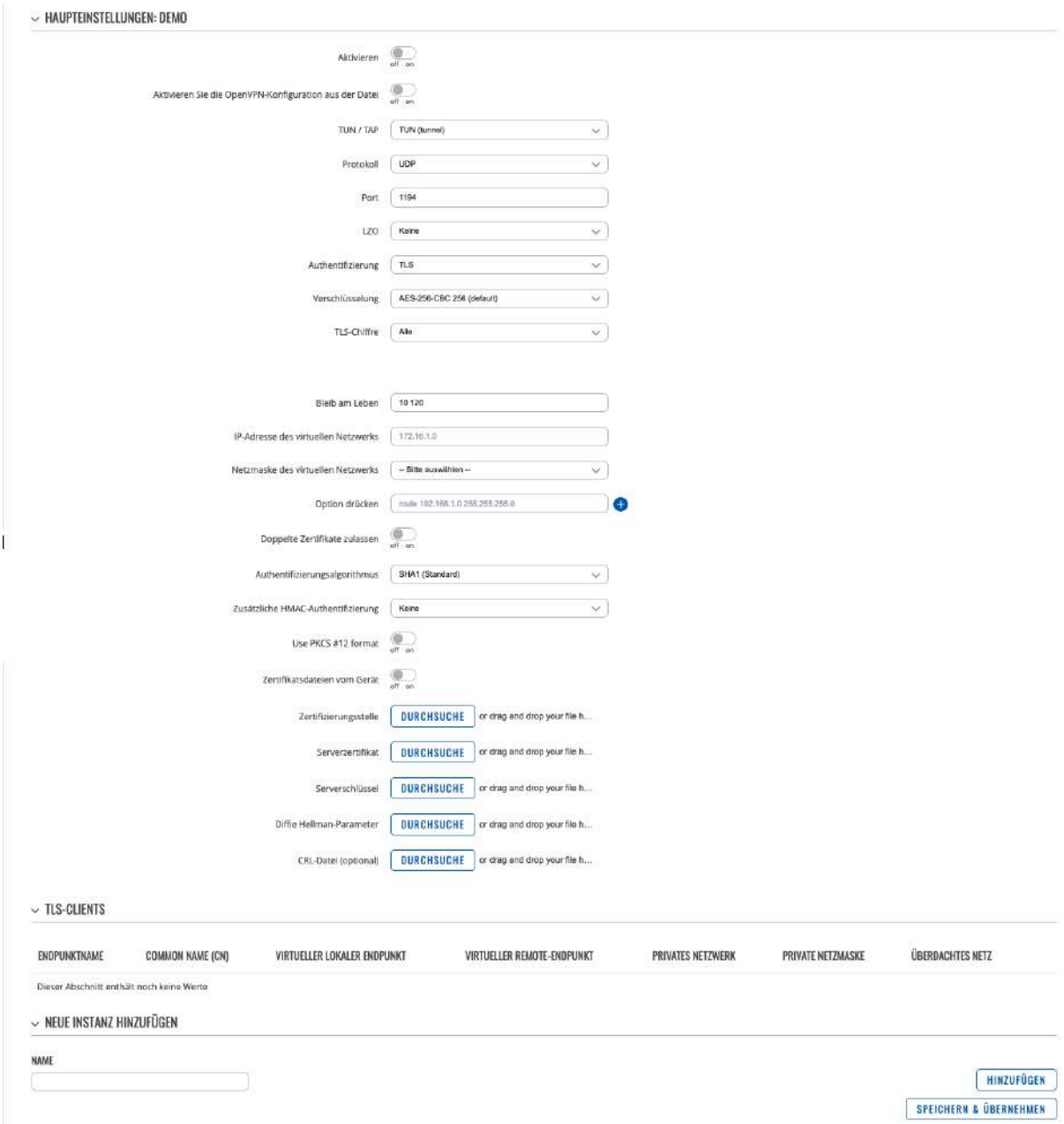
- Einige Konfigurationsfelder werden nur verfügbar, wenn bestimmte andere Einstellungen ausgewählt sind. Die Parameter werden von einem Präfix begleitet, das den Authentifizierungstyp angibt, unter dem sie sichtbar werden. Unterschiedliche Farbcodes werden für verschiedene Präfixe verwendet:
- Rot für den Typ: Tunnel
- Blau für die Aktivierung der Dead Peer Detection



3.2.2 Menü SERVICES VPN > OPENVPN

OPENVPN > Server

OpenVPN ist eine Open-Source-Softwareanwendung, die VPN-Techniken (Virtual Private Network) einsetzt, um sichere Punkt-zu-Punkt- oder Standort-zu-Standort-Verbindungen in gerouteten oder überbrückten Konfigurationen sowie Installationen für den Fernzugriff herzustellen. Es wird häufig als das universellste VPN-Protokoll angesehen, da es flexibel ist, die SSL/TLS-Sicherheit unterstützt, mehrere Verschlüsselungsmethoden bietet, zahlreiche Netzwerkfunktionen enthält und mit den meisten OS-Plattformen kompatibel ist.



Feld	Wert	Beschreibung
Aktivieren	Off | On ; Standard : Off	Schaltet die OpenVPN-Instanz ein oder aus.
Aktivieren Sie die OpenVPN-Konfiguration aus der Datei	Off | On ; Standard : Off	Aktiviert oder deaktiviert die benutzerdefinierte OpenVPN-Konfiguration aus einer Datei.

TUN/TAP	TUN (tunnel) | TAP (ponté); Standard : TUN (tunnel)	Virtueller Netzwerktyp: TUN – Eine virtuelle Punkt-zu-Punkt-IP-Verbindung, die auf der Netzwerkschicht (OSI-Schicht 3) arbeitet und verwendet wird, wenn Routing erforderlich ist. TAP – Ein virtueller Ethernet-Adapter (Switch), der auf der Datenverbindungsschicht (OSI-Schicht 2) arbeitet und verwendet wird, wenn Bridging erforderlich ist.
Protokoll	UDP | TCP | UDP6 | TCP6; Standard : UDP	**UDP** (User Datagram Protocol) – Übertragungsprotokoll, das von der OpenVPN-Verbindung verwendet wird. **Transmission Control Protocol** (TCP) – Das am häufigsten verwendete Protokoll im Internet-Protokoll-Stack (IP). Es stellt sicher, dass der Empfänger die Pakete in der Reihenfolge erhält, in der sie gesendet wurden, indem es sie nummeriert, Antwortnachrichten analysiert, Fehler überprüft und die Pakete bei Problemen erneut sendet. Es sollte verwendet werden, wenn Zuverlässigkeit entscheidend ist (z. B. bei der Dateiübertragung). **User Datagram Protocol** (UDP) – Die Pakete werden an den Empfänger gesendet, ohne Fehlerüberprüfung oder Rückkontrolle, was bedeutet, dass verlorene Pakete für immer verloren sind. Dies macht es weniger zuverlässig, aber schneller als TCP; daher sollte es verwendet werden, wenn die Übertragungsgeschwindigkeit entscheidend ist (z. B. beim Video-Streaming, bei Live-Anrufen).
Port	Standard : 1194	TCP/UDP-Portnummer – Die für die Verbindung verwendete Portnummer. Stellen Sie sicher, dass sie mit der auf der Serverseite angegebenen Portnummer übereinstimmt. **HINWEIS:** Der Datenverkehr auf dem ausgewählten Port wird automatisch in den Firewall-Regeln des Geräts zugelassen.
LZO	Ja | Nein | keine ; Standard : Keine	Aktiviert oder deaktiviert die LZO-Datenkomprimierung.
Authentifizierung	Statischer Schlüssel | TLS | TLS/Passwort | Passwort ; Standard : TLS	Authentifizierungsmodus, der zur Sicherung der Datensitzungen verwendet wird. Der statische Schlüssel ist ein geheimer Schlüssel, der zur Authentifizierung zwischen Server und Client verwendet wird. Der TLS-Authentifizierungsmodus verwendet X.509-Zertifikate: • Zertifizierungsstelle (CA) • Client-Zertifikat • Client-Schlüssel Alle genannten Zertifikate können mithilfe der OpenVPN- oder OpenSSL-Dienstprogramme auf jedem Host-Typ erstellt werden. Eines der beliebtesten Dienstprogramme zu diesem Zweck heißt Easy-RSA. TLS/Passwort verwendet sowohl TLS als auch die Authentifizierung mit Benutzername und Passwort.

Verschlüsselung	DES-CBC 64 | RC2-CBC 128 | DES-EDE-CBC 128 | DES-EDE3-CBC 192 | DESX-CBC 192 | BF-CBC 128 | RC2-40-CBC 40 | CAST5-CBC 128 | RC2-64CBC 64 | AES-128-CBC 128 | AES-128-CFB 128 | AES-128-CFB1 128 | AES-128-CFB8 128 | AES-128-OFB 128 | AES-128-GCM 128 | AES-192-CBC 192 | AES-192-CFB 192 | AES-192-CFB1 192 | AES-192-CFB8 192 | AES-192-OFB 192 | AES-192-GCM 192 | AES-256-CBC 256 | AES-256-CFB 256 | AES-256-CFB1 256 | AES-256-CFB8 256 | AES-256-OFB 256 | AES-256-GCM 256 | none; default: AES-256-CBC 256	Algorithmus, der zur Verschlüsselung der Pakete verwendet wird.
Statischer Schlüssel : IP des Lokalen-Tunnelendpunkts	Standard : Keine	IP-Adresse der lokalen OpenVPN-Netzwerkschnittstelle.
Statischer Schlüssel : IP des Remote-Tunnelendpunkts	Standard : Keine	IP-Adresse der entfernten OpenVPN-Netzwerkschnittstelle (Client).
Statischer Schlüssel : Remote-Netzwerk-IP-Adresse	Standard : Keine	LAN-IP-Adresse des entfernten Netzwerks (Client).
Statischer Schlüssel : Remote-Netzwerknetzmaske	Personnalisé | 255.255.255.0 | 255.255.0.0 | 255.0.0.0 Standard : Keine	Maske des IP-Subnetzes des LANs des entfernten Netzwerks (Clients).
Statischer Schlüssel : Authentifizierungsalgorithmus	MD5 | SHA1 (Par défaut) | SHA256 | SHA384 | SHA512 Standard : Keine	Algorithmus verwendet für den Austausch von Authentifizierungs- und Hash-Informationen.
TLS | TLS/Passwort | Passwort : TLS-Chiffre	Alle | DHE+RSA | Benutzerdefiniert ; Standard : Alle	Verschlüsselungsalgorithmus für Pakete.
TLS | TLS/Passwort | Passwort : Kunde zu Kunde	Off | On ; Standard : Off	Clients von OpenVPN können miteinander im VPN-Netzwerk kommunizieren.
TLS | TLS/Passwort | Passwort : Aktiv halten	Zwei Ganzzahlen, getrennt durch ein Leerzeichen ; Standard : Keine	Definiert zwei Zeitintervalle: Das erste wird verwendet, um periodisch ICMP-Anfragen an den OpenVPN-Server zu senden. Das zweite definiert ein Zeitfenster, das verwendet wird, um den OpenVPN-Dienst neu zu starten, falls innerhalb des angegebenen Zeitrahmens keine ICMP-Antwort empfangen wird. Wenn dieser Wert auf dem OpenVPN-Server spezifiziert ist, ersetzt er die 'Aktiv halten'-Werte, die auf den Client-Instanzen festgelegt sind. Beispiel: 10 120

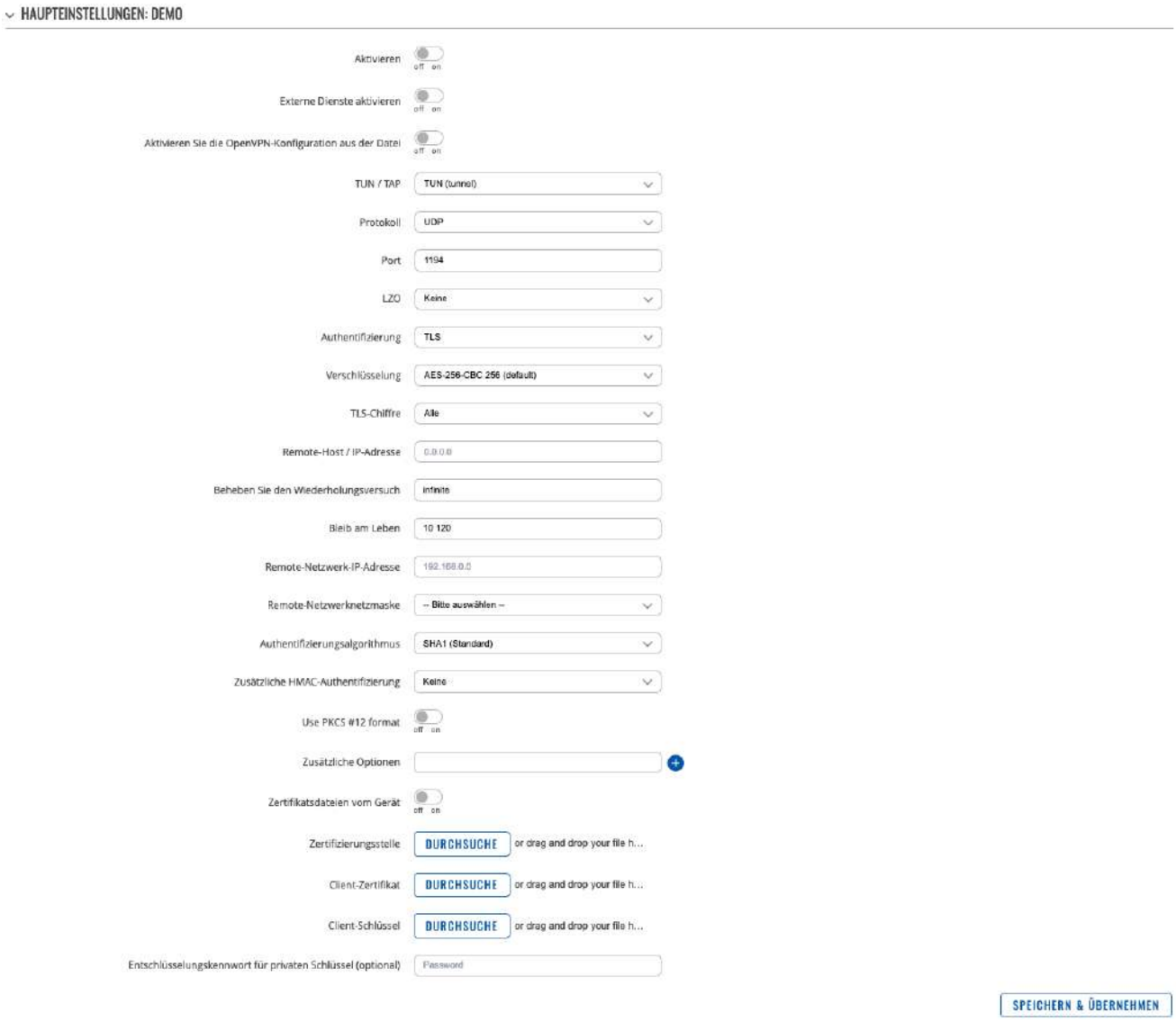
TLS | TLS/Passwort | Password : IP-Adresse des virtuellen Netzwerks	Standard : Keine	IPv4-Adresse des OpenVPN-Netzwerks.
TLS | TLS/Passwort | Passwort : Netzmaske des virtuellen Netzwerks	Benutzerdefiniert | 255.255.255.0 | 255.255.0.0 | 255.0.0.0 Standard : Keine	Subnetzmaske des OpenVPN-Netzwerks.
TLS | TLS/Passwort | Passwort : Option drücken	OpenVPN options; Standard : Keine	Die Push-Optionen sind eine Methode, um Routen und andere zusätzliche Optionen von OpenVPN an verbundene Clients "zu pushen" oder zu übertragen.
TLS | TLS/Passwort | Passwort : Doppelte Zertifikate zulassen	Off | On ; Standard : Off	Aktiviert erlaubt sie mehreren Clients, sich mit denselben Zertifikaten anzumelden.
TLS/Passwort : Benutzernamen und Passwörter	Interaktive Schaltfläche - Durchsuche	Benutzername, der für die Authentifizierung bei diesem OpenVPN-Server verwendet wird.
TLS | Passwort : Passwort	Standard : Keine	Das Passwort, das für die Authentifizierung bei diesem OpenVPN-Server verwendet wird.
Statischer Schlüssel : Statischer Pre-Shared Key	Interaktive Schaltfläche - Durchsuche	Lädt eine Datei mit einem geheimen Schlüssel hoch, der für die Server-Client-Authentifizierung verwendet wird.
TLS | TLS/Password | Password : Zertifizierungsstelle	Interaktive Schaltfläche - Durchsuche	Eine Zertifizierungsstelle ist eine Einrichtung, die digitale Zertifikate ausstellt. Ein digitales Zertifikat bescheinigt die Inhaberschaft eines öffentlichen Schlüssels durch die im Zertifikat genannte Person.
TLS | TLS/Password | Password : Serverzertifikat	Interaktive Schaltfläche - Durchsuche	Ein Typ des digitalen Zertifikats, das zur Identifizierung des OpenVPN-Servers verwendet wird.
TLS | TLS/Password | Password : Serverschlüssel	Interaktive Schaltfläche - Durchsuche	Authentifiziert Clients gegenüber dem Server.
TLS | TLS/Password | Password : Diffie Hellman-Parameter	Interaktive Schaltfläche - Durchsuche	Die DH-Einstellungen legen fest, wie OpenSSL den Diffie-Hellman-Schlüsselaustausch (DH) durchführt.
TLS | TLS/Password | Password : CRL-Datei (optional)	Interaktive Schaltfläche - Durchsuche	Eine CRL-Datei (Certificate Revocation List) ist eine Liste von Zertifikaten, die von der Zertifizierungsstelle (CA) widerrufen wurden. Sie gibt an, welche Zertifikate von der CA nicht mehr akzeptiert werden und daher nicht gegenüber dem Server authentifiziert werden können.

Nachdem bestimmte Parameter ausgewählt wurden, werden bestimmte Konfigurationsfelder verfügbar. Diese Parameter sind mit einem Präfix versehen, das angibt, unter welcher Art von Authentifizierung sie sichtbar werden. Verschiedene Farbcodes werden für unterschiedliche Präfixe verwendet.

Nach der Änderung eines Parameters vergessen Sie nicht, auf die Schaltfläche "Speichern und Anwenden" unten rechts auf der Seite zu klicken.

OPENVPN > Klient

Ein OpenVPN-Client ist eine Entität, die eine Verbindung zu einem OpenVPN-Server herstellt. Um eine neue Client-Instanz zu erstellen, gehen Sie zu "Services" → "VPN" → "OpenVPN", wählen Sie die Rolle: Client, geben Sie einen benutzerdefinierten Namen ein und klicken Sie auf die Schaltfläche "Hinzufügen". Eine OpenVPN-Client-Instanz mit dem angegebenen Namen wird in der Liste "OpenVPN-Konfiguration" angezeigt.
Um mit der Konfiguration zu beginnen, klicken Sie auf die Schaltfläche neben der Client-Instanz, die einem Bleistift ähnelt. Verweisen Sie auf die Abbildung und die Tabelle unten für Informationen zu den Konfigurationsfeldern des OpenVPN-Clients.



Feld	Wert	Beschreibung
Aktivieren	Off | On ; Standard : Off	Aktiviert oder deaktiviert die OpenVPN-Instanz.
Externe Dienste aktivieren	Off | On ; Standard : Off	Aktiviert oder deaktiviert die externen OpenVPN-Dienste.
VPN-Anbieter	Express VPN | Nord VPN ; Standard : Nord VPN	Stellt eine Liste verfügbarer VPN-Anbieter dar.
VPN-Server	Vereinigtes Königreich | Vereinigte Staaten von Amerika | Australien | Südafrika | Benutzerdefiniert ; Standard : Vereinigtes Königreich	Stellt eine Liste verfügbarer VPN-Server dar.

Benutzer	Standard : Keine	Benutzername, der zur Authentifizierung beim VPN-Server verwendet wird.
Passwort	Standard : Keine	Passwort, das zur Authentifizierung beim VPN-Server verwendet wird.
Aktivieren Sie die OpenVPN-Konfiguration aus der Datei	Off | On ; Standard : Off	Aktiviert oder deaktiviert die benutzerdefinierte OpenVPN-Konfiguration aus einer Datei.
OpenVPN-Konfigurationsdatei	Interaktive Schaltfläche – Durchsuche	Laden Sie die OpenVPN-Konfiguration herunter. Achtung! Dadurch wird Ihre aktuelle Konfiguration überschrieben.
Laden Sie OpenVPN-Authentifizierungsdateien hoch	Off | On ; Standard : Off	Laden Sie die OpenVPN-Authentifizierungsdateien herunter, die automatisch in die Konfiguration aufgenommen werden.
TUN/TAP	TUN (tunnel) | TAP (Ponté); Standard : TUN (tunnel)	Typ des virtuellen Netzwerkgeräts. TUN – eine virtuelle Punkt-zu-Punkt-IP-Verbindung, die auf der Netzwerkschicht (OSI-Schicht 3) arbeitet und verwendet wird, wenn Routing erforderlich ist. TAP – ein virtueller Ethernet-Adapter (Switch), der auf der Datenverbindungsschicht (OSI-Schicht 2) arbeitet und verwendet wird, wenn Bridging erforderlich ist.
Protokoll	UDP | TCP | UDP6 | TCP6; Standard : UDP	Protokoll für die Verbindung verwendet von OpenVPN: • Transmission Control Protocol (TCP) – Das am häufigsten verwendete Protokoll in der Internet-Protokoll-Suite (IP). Es gewährleistet, dass der Empfänger die Pakete in der Reihenfolge erhält, in der sie gesendet wurden, indem es sie nummeriert, Antwortnachrichten analysiert, Fehler überprüft und sie bei Bedarf erneut sendet. Es sollte verwendet werden, wenn Zuverlässigkeit entscheidend ist, zum Beispiel beim Dateitransfer. • User Datagram Protocol (UDP) – Pakete werden ohne Überprüfung auf Fehler oder Qualitätskontrolle hin und zurück gesendet, was bedeutet, dass verlorene Pakete für immer verloren sind. Dies macht es weniger zuverlässig, aber schneller als TCP; daher sollte es verwendet werden, wenn die Übertragungsgeschwindigkeit entscheidend ist, zum Beispiel bei Video-Streaming oder Live-Anrufen.
Port	Standard : 1194	Die Nummer des TCP/UDP-Ports, der für die Verbindung verwendet wird. Stellen Sie sicher, dass sie mit der auf der Serverseite angegebenen Portnummer übereinstimmt. HINWEIS: Der Datenverkehr auf dem ausgewählten Port wird in den Firewall-Regeln des Geräts automatisch zugelassen.
LZO	Ja | Nein | Keine ; Standard : Keine	Aktiviert oder deaktiviert die LZO-Datenkomprimierung.

Authentifizierung	Statischer Schlüssel | TLS | TLS/Passwort | Passwort ; Standard : TLS	Authentifizierungsmodus, der zur Sicherung von Datensitzungen verwendet wird. • Der statische Schlüssel ist ein geheimer Schlüssel, der für die Server-Client-Authentifizierung verwendet wird. • Der TLS-Authentifizierungsmodus verwendet Zertifikate vom Typ X.509 : - Zertifizierungsstelle (CA) - Client-Zertifikat - Client-Schlüssel Alle genannten Zertifikate können mithilfe der Dienstprogramme OpenVPN oder Open SSL auf jedem beliebigen Host-Rechner erzeugt werden. Eines der beliebtesten Dienstprogramme, das für diesen Zweck verwendet wird, heißt Easy-RSA. - **Passwort** ist eine einfache Authentifizierung, die auf einem Benutzernamen und einem Passwort basiert, bei der der Besitzer des OpenVPN-Servers die Verbindungsdaten bereitstellt. - **TLS/Passwort** verwendet sowohl TLS als auch die Authentifizierung über Benutzername/Passwort.
Verschlüsselung	DES-CBC 64 | RC2-CBC 128 | DES-EDE-CBC 128 | DES-EDE3-CBC 192 | DESX-CBC 192 | BF-CBC 128 | RC2-40-CBC 40 | CAST5-CBC 128 | RC2-64CBC 64 | AES-128-CBC 128 | AES-128-CFB 128 | AES-128-CFB1 128 | AES-128-CFB8 128 | AES-128-OFB 128 | AES-128-GCM 128 | AES-192-CBC 192 | AES-192-CFB 192 | AES-192-CFB1 192 | AES-192-CFB8 192 | AES-192-OFB 192 | AES-192-GCM 192 | AES-256-CBC 256 | AES-256-CFB 256 | AES-256-CFB1 256 | AES-256-CFB8 256 | AES-256-OFB 256 | AES-256-GCM 256 | Keine ; Standard : AES-256-CBC 256	Algorithmus, der zur Verschlüsselung von Paketen verwendet wird.
TLS | TLS/Passwort : TLS-Chiffre	Alle | DHE+RSA | Benutzerdefiniert ; Standard : Alle	Algorithmus zur Verschlüsselung von Paketen.
TLS | TLS/Passwort : Zulässige TLS-Chiffren	Standard : Keine	Liste der TLS-Verschlüsselungsalgorithmen, die von dieser Verbindung akzeptiert werden.
Remote-Host / IP-Adresse	Standard : Keine	IP-Adresse oder Hostname eines OpenVPN-Servers.

Beheben Sie den Wiederholungsversuch	Unendlich; Standard : Unendlich	Wenn die Auflösung des Hostnamens des Servers fehlschlägt, gibt dieses Feld an, wie lange (in Sekunden) es dauert, bis die Auflösung erneut versucht wird. Geben Sie "unendlich" an, um es auf unbestimmte Zeit erneut zu versuchen.
Aktiv halten	Zwei ganze Zahlen, die durch ein Leerzeichen getrennt sind ; Standard : Keine	Legt zwei Zeitintervalle fest: Das erste wird verwendet, um periodisch ICMP-Anfragen an den OpenVPN-Server zu senden, das zweite legt ein Zeitfenster fest, das verwendet wird, um den OpenVPN-Dienst neu zu starten, wenn während des angegebenen Zeitfensters keine ICMP-Antwort empfangen wird. Wenn dieser Wert auf dem OpenVPN-Server angegeben wird, überschreibt er die Werte für "Aktiv halten", die auf den Clientinstanzen eingestellt sind. Beispiel: 10 120
Statischer Schlüssel : IP des Lokalen-Tunnelendpunkts	Standard : Keine	P-Adresse der lokalen OpenVPN-Netzwerkschnittstelle.
Statischer Schlüssel : IP des Remote-Tunnelendpunkts	Standard : Keine	IP-Adresse der entfernten OpenVPN-Netzwerkschnittstelle (Client).
Remote-Netzwerk-IP-Adresse	Standard : Keine	LAN-IP-Adresse des entfernten Netzwerks (Client).
Remote-Netzwerknetzmaske	Benutzerdefiniert | 255.255.255.0 | 255.255.0.0 | 255.0.0.0 Standard : Keine	IP-Subnetzmaske LAN des entfernten Netzwerks (Client).
Authentifizierungsalgorithmus	MD5 | SHA1 (Standard) | SHA256 | SHA384 | SHA512 Standard : Keine	Algorithmus, der für den Austausch von Authentifizierungs- und Hash-Informationen verwendet wird.
TLS | TLS/Passwort | Passwort : Zusätzliche HMAC-Authentifizierung	Nur Authentifizierung (tls-auth) | Authentifizierung und Verschlüsselung (tls-crypt) ; Standard : Keine	Zusätzliche Schicht der HMAC-Authentifizierung über dem TLS-Kontrollkanal zum Schutz vor Denial-of-Service-Angriffen (DoS).
TLS | TLS/Passwort | Passwort : HMAC-Schlüssel	Interaktive Schaltfläche - Durchsuche	Lädt eine Datei mit dem HMAC-Authentifizierungsschlüssel hoch.
TLS | TLS/Passwort | Passwort : Direction de la clé HMAC	0 | 1 | Keine ; Standard : 1	Der Wert des Parameters für die Schlüsselrichtung muss auf beiden Seiten (Client und Server) der Verbindung komplementär sein. Wenn eine Seite 0 verwendet, muss die andere Seite 1 verwenden, oder beide Seiten müssen den Parameter ganz weglassen.
TLS | TLS/Passwort | Passwort : Use PKCS #12 format	Off | On ; Standard : Off	Aktiviert oder deaktiviert das PKCS #12-Format.
TLS/Passwort | Passwort : Benutzer	Standard : Keine	Benutzername, der für die Authentifizierung beim OpenVPN-Server verwendet wird.
TLS/Passwort | Passwort : Passwort	Standard : Keine	Passwort, das für die Authentifizierung beim OpenVPN-Server verwendet wird.
Zusätzliche Optionen	Standard : Keine	Zusätzliche OpenVPN-Optionen, die von der OpenVPN-Instanz verwendet werden sollen.
TLS | TLS/Passwort | Passwort : Zertifikatsdateien vom Gerät	Off | On ; Standard : Off	Aktivieren Sie diese Option, wenn Sie die vom Gerät erzeugten Zertifikatsdateien auswählen möchten.

TLS | TLS/Passwort | Passwort : Zertifizierungsstelle	Interaktive Schaltfläche – Durchsuche	Eine Zertifizierungsstelle ist eine Einrichtung, die digitale Zertifikate ausstellt. Ein digitales Zertifikat bescheinigt den Besitz eines öffentlichen Schlüssels durch die im Zertifikat genannte Person.
TLS | TLS/Password : Client-Zertifikat	Interaktive Schaltfläche – Durchsuche	Ein Client-Zertifikat ist eine Art digitales Zertifikat, das von Client-Systemen verwendet wird, um authentifizierte Anfragen an einen Remote-Server zu stellen. Client-Zertifikate spielen eine Schlüsselrolle in vielen Designs zur gegenseitigen Authentifizierung und bieten solide Garantien für die Identität des Antragstellers.
TLS | TLS/Password : Client-Schlüssel	Interaktive Schaltfläche – Durchsuche	Authentifiziert den Client gegenüber dem Server und stellt genau fest, wer er ist.
TLS | TLS/Password : Entschlüsselungskennwort für privaten Schlüssel (optional)	Standard : Keine	Passwort, das zum Entschlüsseln des privaten Schlüssels des Servers verwendet wird. Nur zu verwenden, wenn die .key-Datei des Servers mit einem Passwort verschlüsselt ist.
Statischer Schlüssel : Statischer Pre-Shared Key	Interaktive Schaltfläche – Durchsuche	Lädt eine Datei mit einem geheimen Schlüssel hoch, der für die Authentifizierung zwischen Server und Client verwendet wird.

Bestimmte Konfigurationsfelder werden nur sichtbar, wenn bestimmte andere Einstellungen ausgewählt werden. Den Namen der Einstellungen wird ein Präfix angehängt, das den Authentifizierungstyp angibt, unter dem sie sichtbar sind. Für verschiedene Präfixe werden unterschiedliche Farbcodes verwendet.

Wenn Sie eine der Einstellungen geändert haben, vergessen Sie nicht, auf die Schaltfläche Speichern und Anwenden unten rechts auf der Seite zu klicken.

3.2.3 Menü SERVICES VPN > WireGuard

WireGuard ist ein einfaches, schnelles, leichtes und modernes VPN, das eine sichere und bewährte Kryptografie verwendet. Es zielt darauf ab, besser als OpenVPN zu sein. WireGuard ist als vielseitiges VPN konzipiert, das sich für viele verschiedene Situationen eignet, und obwohl es derzeit intensiv weiterentwickelt wird, könnte es bereits als die sicherste, benutzerfreundlichste und einfachste VPN-Lösung angesehen werden.

WireGuard funktioniert, indem es eine Schnittstelle hinzufügt, die als Tunnel fungiert. Um einen solchen zu erstellen, geben Sie seinen Namen ein und klicken Sie auf die Schaltfläche Hinzufügen. Dies sollte eine neue Instanz von Wireguard hinzufügen und ein Konfigurationsfenster öffnen.

WireGuard-Schnittstelle > Allgemeine Einrichtung

Dieser Abschnitt enthält die allgemeinen Einstellungen für die erstellte WireGuard-Instanz. Hier finden Sie seine öffentlichen und privaten Schlüssel und können diese generieren, den Port und die IP-Adressen für die Kommunikation angeben.

Feld	Wert	Beschreibung
Aktivieren	Off | On ; Standard : Off	Aktiviert oder deaktiviert die WireGuard-Instanz.
Privat Schlüssel	Standard : keine	Privater Schlüssel, der bei der Authentifizierung verwendet wird.
Öffentlicher Schlüssel	Standard : keine	Öffentlicher Schlüssel, der bei der Authentifizierung verwendet wird.
Schlüsselpaar erzeugen	Interaktive Schaltfläche – Generieren	Klicken Sie, um den öffentlichen und den privaten Schlüssel zu generieren.
IP-Adressen	Standard : keine	Eine eindeutige IP-Adresse oder eine Liste von IP-Adressen für diese Instanz, die mit öffentlichen Schlüsseln verknüpft ist.

WireGuard-Schnittstelle > Erweiterte Einstellungen

Der Abschnitt "Erweiterte Einstellungen" enthält die Konfiguration der Metriken und der maximalen Übertragungseinheit (MTU) für diese WireGuard-Schnittstelle.

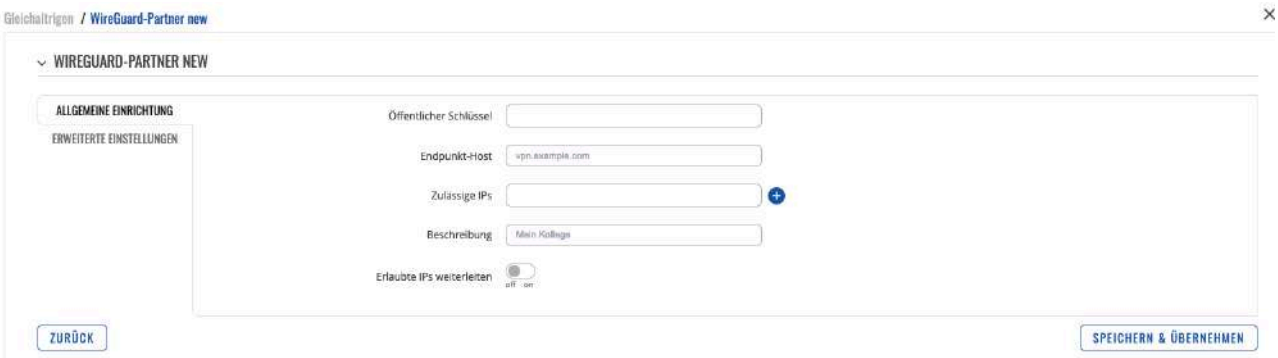
Feld	Wert	Beschreibung
Metrisch	Standard : Keine	Geben Sie die Metrik für diese Tunnelschnittstelle an. Eine niedrigere Zahl bedeutet eine höhere Priorität.
MTU	Standard : Keine	Maximale Übertragungseinheit für diese Tunnelschnittstelle.
DNS-Server	Standard : Keine	DNS-Server(n) für diese WireGuard-Schnittstelle.

WireGuard-Schnittstelle > Peer / Gegenstelle

Der Abschnitt "Peer / Gegenstelle" wird verwendet, um alle Peers für diese Schnittstelle zu erstellen und einzurichten. Um einen zu erstellen, geben Sie seinen Namen ein und klicken Sie auf die Schaltfläche "Hinzufügen". Um ihn zu konfigurieren, klicken Sie auf die Schaltfläche "Bearbeiten".

Peer / Gegenstelle > Allgemeine Einrichtung

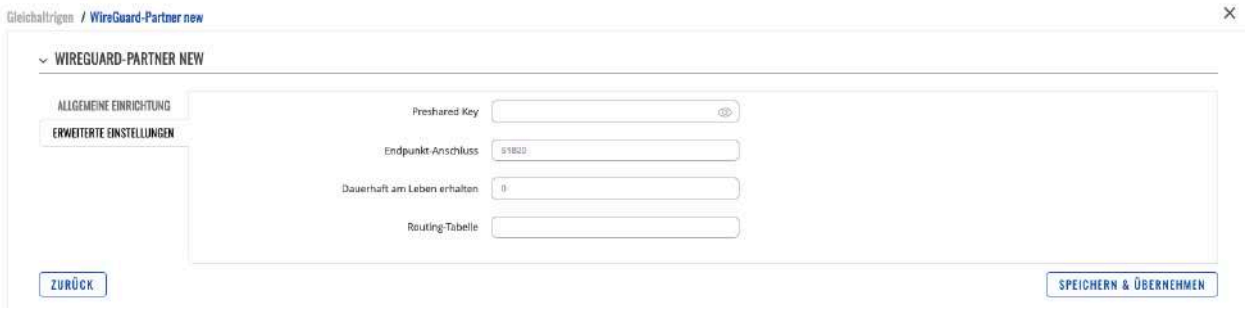
Im Abschnitt "Allgemeine Konfiguration" der Instanz "Peer / Gegenstelle" können Sie grundlegende Informationen über den Endpunkt konfigurieren, um die Kommunikation zu ermöglichen.



Feld	Wert	Beschreibung
Öffentlicher Schlüssel	Standard : Keine	Öffentlicher Schlüssel des Endpunkts.
Zulässige IPs	Standard : Keine	Eine einzelne IP-Adresse oder eine Liste von IP-Adressen, die mit diesem Peer kommunizieren dürfen.
Beschreibung	Standard : Keine	Beschreibung des Peer / Gegenstelle
Erlaubte IPs weiterleiten	Off | On ; Standard : Off	Aktivieren, um Routen für die IP-Adressen zu erstellen, die für dieses Peer zugelassen sind.

Peer / Gegenstelle > Erweiterte Einstellungen

Im Abschnitt "Erweiterte Einstellungen" der Instanz "Peer/Gegenstelle" können Sie zusätzliche Einstellungen konfigurieren, wie z. B. ihre Beschreibung, den Host und Port des Endpunkts, den Pre-Shared Key und andere. Weitere Informationen finden Sie weiter unten.



Feld	Wert	Beschreibung
Preshared Key	Standard : Keine	Pre-Shared Key, der mit Base64 kodiert ist. Fügt eine zusätzliche Ebene der Kryptografie mit symmetrischem Schlüssel für Post-Quantum-Resistenz hinzu.
Endpunkt-Anschluss	Standard : Keine	Geben Sie den Port an, mit dem eine Verbindung zum entfernten Endpunkt hergestellt werden soll. Er wird auf 51820 gesetzt, wenn er leer gelassen wird.
Dauerhaft am Leben erhalten	Standard : Keine	IP-Adresse oder URL des entfernten Endpunkts.
Routing-Tabelle	Standard : Keine	Aktivieren, um Routen für die IP-Adressen zu erstellen, die für dieses Peer zugelassen sind.

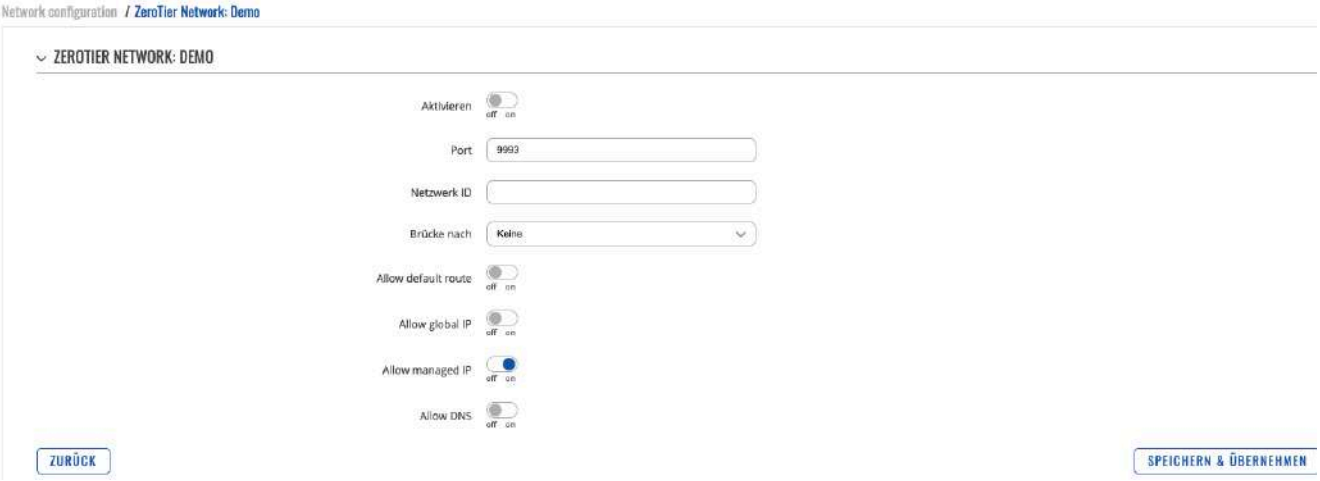
3.2.4 Menü SERVICES VPN > ZeroTier

ZeroTier One ist eine Open-Source-Software, die eine Peer-to-Peer-VPN-Verbindung (P2PVPN) zwischen verschiedenen Geräten, auf denen unterschiedliche Betriebssysteme laufen, herstellen kann. Außerdem bietet sie Möglichkeiten zur Netzwerkverwaltung wie Routing und das Erstellen von Firewall-Regeln.
Um eine neue ZeroTier-Instanz zu erstellen, suchen Sie den Abschnitt "Neue ZeroTier-Konfiguration hinzufügen", geben Sie einen benutzerdefinierten Namen ein und klicken Sie auf die Schaltfläche "Hinzufügen".

Sie sollten zur Konfigurationsseite der neuen ZeroTier-Instanz weitergeleitet werden, die wie folgt aussehen sollte:

Feld	Wert	Beschreibung
Aktivieren	Off | On ; Standard : Off	Aktiviert oder deaktiviert die ZeroTier-Instanz.

Die Konfigurationsinstanz des ZeroTier-Netzwerks sollte wie folgt aussehen:



Feld	Wert	Beschreibung
Aktivieren	Off | On ; Standard : Off	Aktiviert oder deaktiviert die ZeroTier-Instanz.
Port	Standard : 9993	

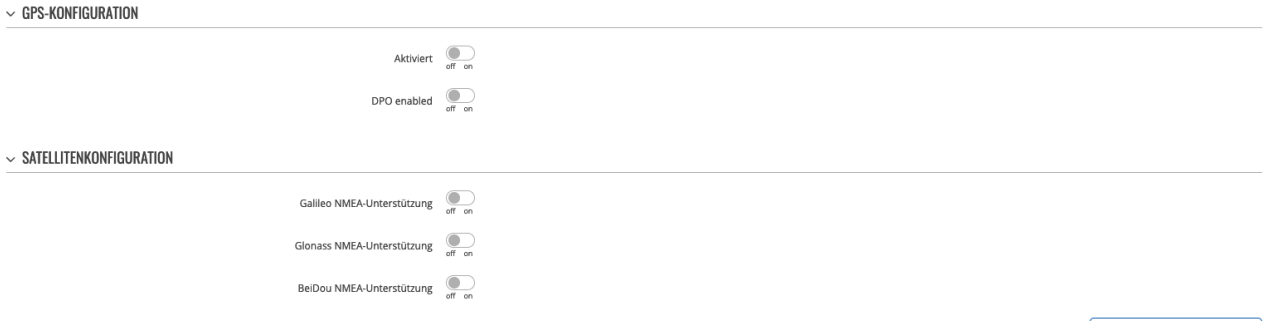
Netzwerk ID	Standard : Keine	ID des ZeroTier-Netzwerks. Melden Sie sich bei Ihrem ZeroTier-Konto an, um die ZeroTier-Netzwerk-ID zu finden, die aus einer hexadezimalen Zeichenfolge bestehen sollte.
Brücke nach	Keine | LAN Standard : Keine	Geben Sie an, an welcher Schnittstelle diese ZeroTier-Instanz überbrückt werden soll.
Allow default route	Off | On ; Standard : Off	Erlaubt ZeroTier, die Standardroute des Systems zu überschreiben.
Allow global IP	Off | On ; Standard : Off	Erlaubt von ZeroTier verwalteten IP-Adressen und Routen, sich mit dem öffentlichen IP-Raum zu überschneiden.
Allow managed IP	Off | On ; Standard : On	Weist IP-Adressen und Routen zu, die von ZeroTier verwaltet werden.
Allow DNS	Off | On ; Standard : Off	Wendet die DNS-Server an, die auf der Ebene des Netzwerkcontrollers eingestellt sind.

3.3 Menü SERVICES > GEOGRAPHISCHES POSITIONIERUNGS SYSTEM

Das Global Positioning System (GPS) ist ein weltraumgestütztes Funknavigationssystem. Diese Seite ist eine Übersicht über den GPS-Dienst.

3.3.1 Menü SERVICES > GEOGRAPHISCHES POSITIONIERUNGS SYSTEM > Allgemein

General wird verwendet, um den GPS-Dienst und die Unterstützung für verschiedene Satellitentypen zu aktivieren. Sobald Sie GPS aktiviert haben, können Sie auf der Kartenseite nachsehen, ob das Gerät eine GPS-Position ermittelt hat. Es ist sehr wichtig, dass Sie die GPS-Antenne am Gerät befestigen und sie im Freien (nicht in einem Gebäude) aufstellen. Andernfalls ist es unwahrscheinlich, dass das Gerät eine GPS-Position ermittelt.
Die folgende Abbildung ist ein Beispiel für die Seite Allgemein und die folgende Tabelle enthält Informationen zu



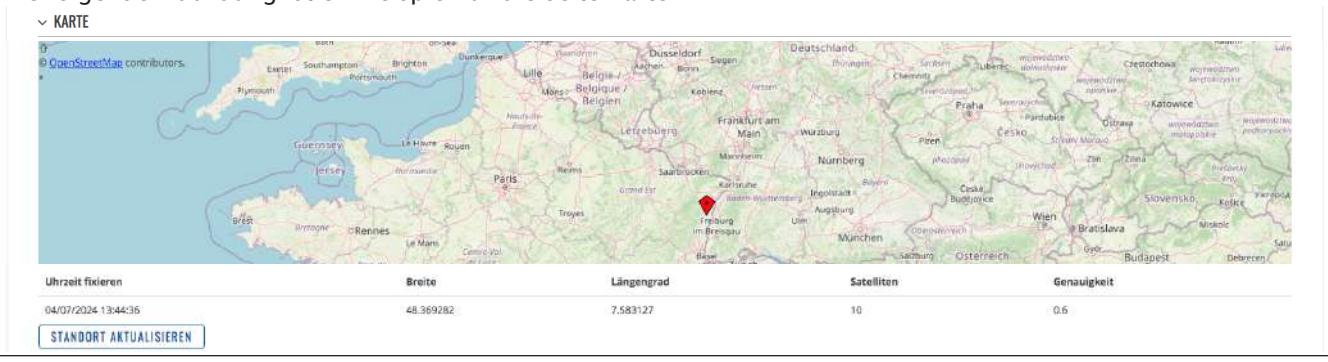
den Feldern, die auf dieser Seite enthalten sind:

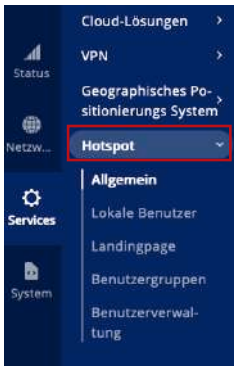
Feld	Wert	Beschreibung
Aktiviert	Off | On; Standard : Off	Schaltet den GPS-Dienst ein oder aus.
DPO enabled	Off | On; Standard : Off	Aktivieren Sie die dynamische Stromoptimierung (erfordert einen Neustart des Modems). Diese Funktion wird bei Geräten mit Meig-Modem oder Quectel-Modem BG95 nicht unterstützt.
Galileo NMEA-Unterstützung	Off | On; Standard : Off	Aktiviert oder deaktiviert die Unterstützung für Galileo-Satelliten.
Glonass NMEA-Unterstützung*	Off | On; Standard : Off	Schaltet die Unterstützung für Glonass-Satelliten ein oder aus.
BeiDou NMEA-Unterstützung*	Off | On; Standard : Off	Aktiviert oder deaktiviert die Unterstützung für BeiDou-Satelliten.

* Das Ändern dieser Optionen erfordert einen Neustart des Modems. Wenn Sie diese Optionen ändern und speichern, verliert das Gerät daher für etwa 30 Sekunden die Zellkonnektivität.

3.3.2 Menü SERVICES > GEOGRAPHISCHES POSITIONIERUNGS SYSTEM > Karte

Auf der Kartenseite werden die aktuellen Koordinaten und der Standort des Geräts auf der Karte angezeigt. Um die Position des Geräts auf der Karte zu sehen, stellen Sie sicher, dass die GPS-Antenne am Gerät angebracht ist und aktivieren Sie GPS auf der Seite Allgemein .
Die folgende Abbildung ist ein Beispiel für die Seite Karte :





3.4 Menü SERVICES > HOTSPOT

Ein Hotspot ist ein Dienst, der die Authentifizierung, Autorisierung und Abrechnung eines Netzwerks bereitstellt.

3.4.1 Menü SERVICES > HOTSPOT > Allgemein

HOTSPOT-Instanzen

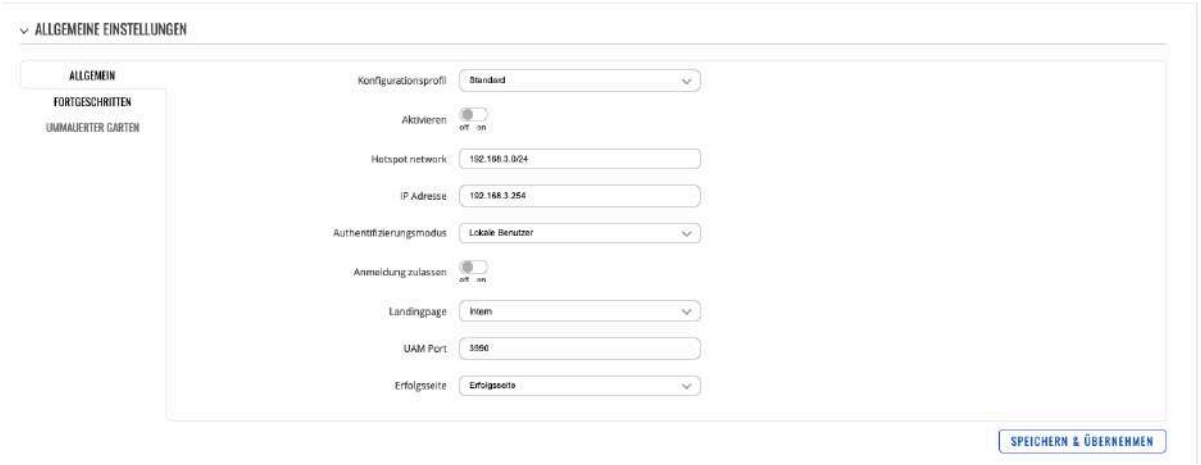
Im Abschnitt Hotspot-Instanzen werden die wichtigsten Einstellungen für Ihren Hotspot angezeigt. Standardmäßig ist auf dem Gerät keine Hotspot-Instanz vorhanden. So erstellen Sie eine neue Instanz und beginnen mit der Konfiguration :

1. Wählen Sie eine "Schnittstelle" ;
2. Klicken Sie auf die Schaltfläche "Hinzufügen";

Danach erscheint ein neues Fenster zum Einrichten des Hotspots.

Allgemeine Einstellungen: Allgemeiner Modus

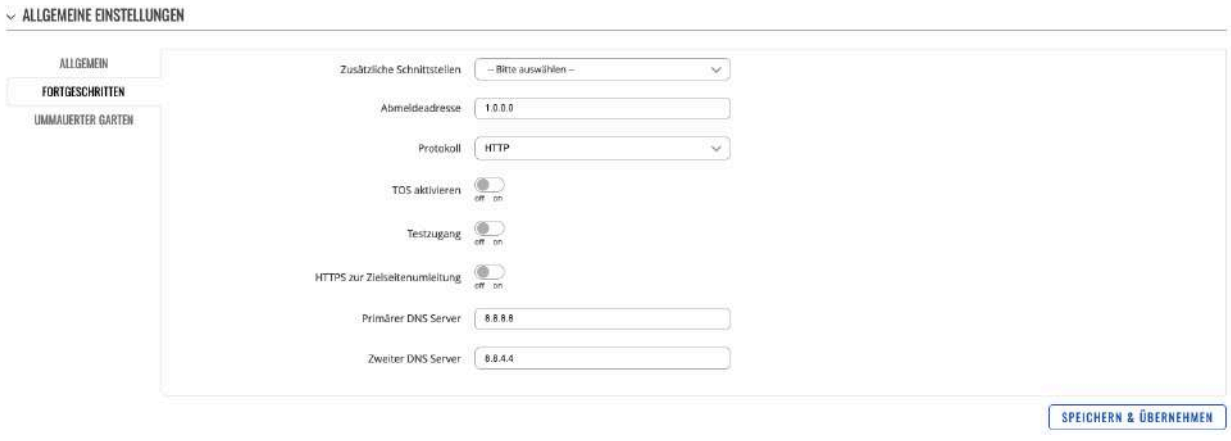
Im Fenster Allgemeine Einstellungen wird der größte Teil der Konfiguration des Zugangspunkts vorgenommen. In den folgenden Unterabschnitten finden Sie Informationen zu den Konfigurationsfeldern, die in den Abschnitten Allgemeine Einstellungen zu finden sind.



Feld	Wert	Beschreibung
Konfigurationsprofil	Cloud4wi | Standard | Hotspot systems ; Standard : Standard	Konfiguriert die Einstellungen des Zugangspunkts entsprechend dem ausgewählten Dienstanbieter vor.
Aktivieren	Off | On; Standard : On	Aktiviert oder deaktiviert die Hotspot-Instanz.

Hotspot network	IP/Netzmaske ; Standard : 192.168.3.0/24	IP-Adresse und Subnetz des Hotspot-Netzwerks.
IP Adresse	Adresse IP ; Standard : 192.168.3.254	Stellt die IP-Adresse Ihres vernetzten Hotspot-Routers ein.
Authentifizierungsmodus	Lokale Benutzer | Radius | SMS OTP ; Standard : Lokale Benutzer	Der Authentifizierungsmodus legt fest, wie sich die Nutzer mit dem Hotspot verbinden.
Anmeldung zulassen	Off | On; Standard : Off	Ermöglicht es Nutzern, sich über die Zielseite für den Hotspot zu registrieren.
Ablaufzeit	Entier; Standard : 0	Zeitlimit für den Ablauf von Benutzerkennungen. Gilt für Nutzer, die sich über die Zielseite angemeldet haben.
Benutzergruppe	Default ; Standard : Default	Benutzergruppe, der die Benutzer, die sich über die Zielseite angemeldet haben, zugewiesen werden sollen.
Landingpage	Interne | Externe ; Standard : Interne	Wenn eine externe Zielseite ausgewählt wird, erscheint ein neuer Abschnitt, in dem die Adresse der Website eingegeben werden kann, z. B. http://www.example.com
UAM Port	Standard : 3990	Port, der zur Authentifizierung von Clients verlinkt werden soll.
UAM - Geheimnis	Standard : Keine	Gemeinsames Geheimnis zwischen uamserver und hotspot.
Erfolgsseite	Erfolgsseite | Ursprüngliche URL | Benutzerdefiniert ; Standard : Erfolgsseite	Ort, zu dem nach einer erfolgreichen Authentifizierung zurückgekehrt werden soll.

Allgemeine Einstellungen: Erweiterter Modus

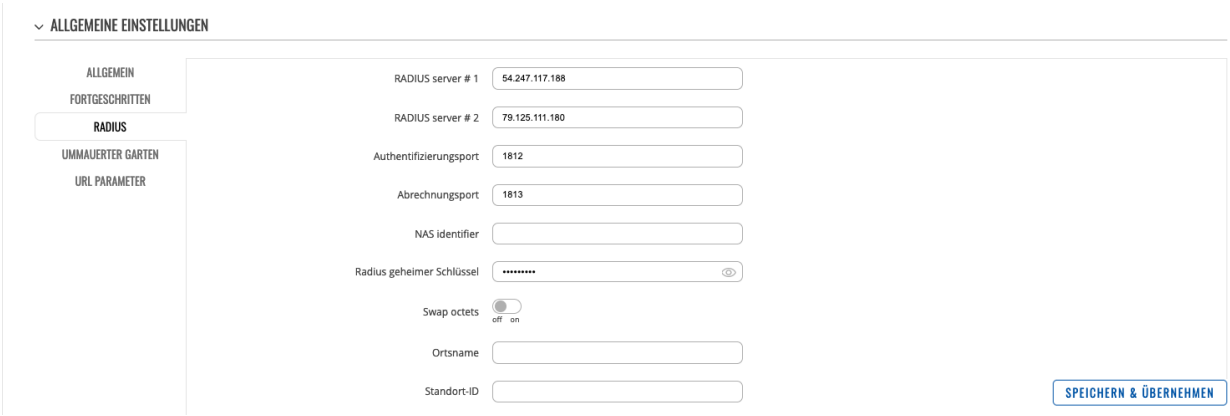


Feld	Wert	Beschreibung
Zusätzliche Schnittstellen	Verfügbare Schnittstellen ; Standard : Keine	Zeigt zusätzliche Schnittstellen an, die an die Instanz des Zugangspunkts angehängt werden können.
Abmeldeadresse	Adresse IP ; Standard : 1.0.0.0	Eine Adresse, die von Nutzern verwendet werden kann, um sich von der Hotspot-Sitzung abzumelden.
Protokoll	HTTP | HTTPS ; Standard : HTTP	Das Protokoll, das für die Zielseite verwendet werden soll.
TOS aktivieren	Off | On; Standard : Off	Aktiviert die Anforderungen an die Dienstbedingungen (ToS). Das Clientgerät kann erst dann auf das Internet zugreifen, wenn es die ToS akzeptiert hat.

Testzugang	Off | On ; Standard : Off	Ermöglicht einen Testzugang zum Internet für eine bestimmte Gruppe.
Testzugang : Gruppe	Groupe d'utilisateurs ; Standard :Default	Gibt die Testbenutzergruppe an.
HTTPS zur Zielseitenumleitung	Off | On; Standard : Off	Leiten Sie die anfänglichen HTTPS-Anfragen von der vorherigen Zielseite auf die Zielseite des Zugangspunkts um.
Zertifikatsdateien vom Gerät	Off | On; Standard : Off	Angegeben, ob die Schlüssel- und Zertifikatsdateien vom Computer heruntergeladen werden sollen oder die auf diesem Gerät über die Seite System → Verwaltung erzeugten Dateien verwendet werden sollen.
SSL Schlüsseldatei	Fichier clé; Standard : Keine	Laden Sie den SSL-Schlüssel hoch/wählen Sie ihn aus.
SSL Zertifikatsdatei	Fichier de certificat ; Standard : Keine	Laden Sie das SSL-Zertifikat herunter bzw. wählen Sie es aus.
Primärer DNS Server	Adresse IP ; Standard : 8.8.8.8	Zusätzliche DNS-Server, die vom Hotspot verwendet werden sollen.
Zweiter DNS Server	Adresse IP ; Standard : 8.8.4.4	Zusätzliche DNS-Server, die vom Hotspot verwendet werden sollen.

Allgemeine Einstellungen: Radius-Modus

Der Radius-Authentifizierungsmodus verwendet einen externen RADIUS-Server, dem Sie eine Adresse angeben müssen, anstatt die lokale Authentifizierung des Routers zu verwenden. Dieser Abschnitt ist sichtbar, wenn das Cloud4wi- oder Hotspot-Systemprofil im Konfigurationsprofil im Allgemeinen Menü ausgewählt ist.



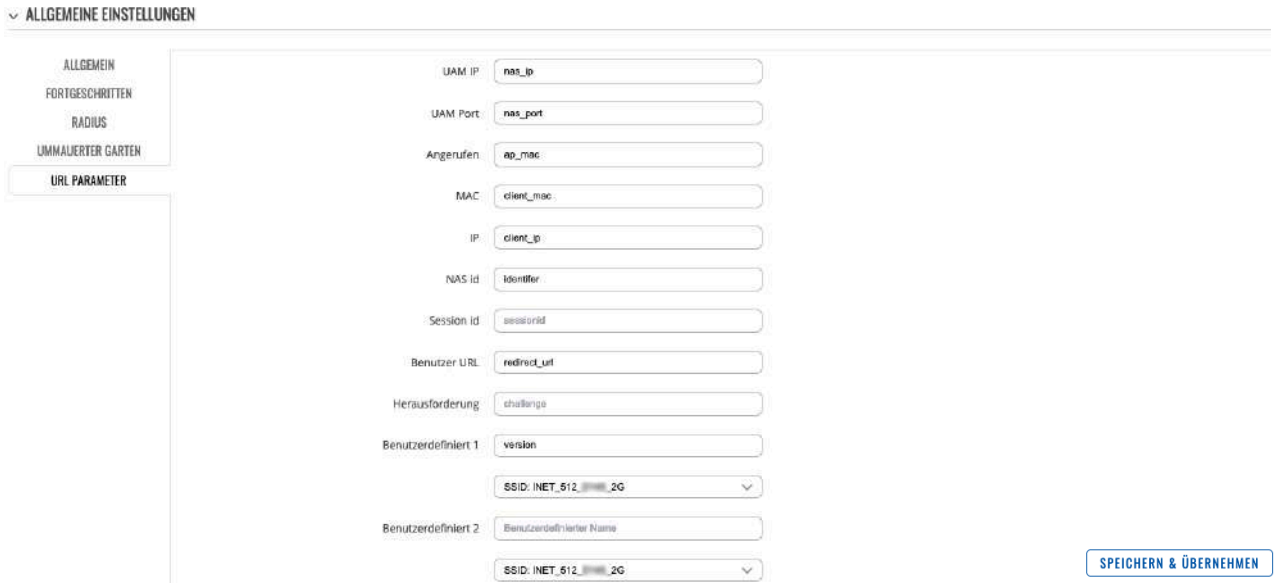
Feld	Wert	Beschreibung
RADIUS server # 1	ip; Standard : Keine	Die IP-Adresse des RADIUS-Servers Nr. 1, den Sie zur Authentifizierung Ihrer drahtlosen Clients verwenden sollen.
RADIUS server # 2	ip; Standard : Keine	Die IP-Adresse des RADIUS-Servers Nr. 2, den Sie zur Authentifizierung Ihrer drahtlosen Clients verwenden sollen.
Authentifizierungsport	Standard : 1812	Der Authentifizierungsport des RADIUS-Servers.
Abrechnungsport	Standard : 1813	Der Buchhaltungsport des RADIUS-Servers.
NAS identifier	Standard : Keine	NAS-Identifier" ist eines der grundlegenden RADIUS-Attribute.
Radius geheimer Schlüssel	Standard : Keine	Der geheime Schlüssel ist ein Passwort, das für die Authentifizierung beim RADIUS-Server verwendet wird.
Swap octets	Off | On; Standard : Off	Tauscht die Bedeutung der Eingabe- und Ausgabebytes in Bezug auf RADIUS-Attribute aus.
Ortsname	Standard : Keine	Individueller Name des Standorts für Ihren Hotspot.
Standort-ID	Standard : Keine	Benutzerdefinierte Standortkennung für Ihren Hotspot.

Allgemeine Einstellungen : Ummauerter Garten

Sie können eine Liste von Adressen hinzufügen, auf die mit dem Hotspot verbundene Nutzer ohne jegliche Authentifizierung zugreifen können. Standardmäßig ist diese Liste leer. Schreiben Sie einfach die Adressen in die Adressliste

Allgemeine Einstellungen : URL-Parameter

Der Abschnitt URL-Parameter wird sichtbar, wenn im Abschnitt Allgemeine Einstellungen das Konfigurationsprofil: Cloud4wi oder Hotspot-Systeme ausgewählt wurde.



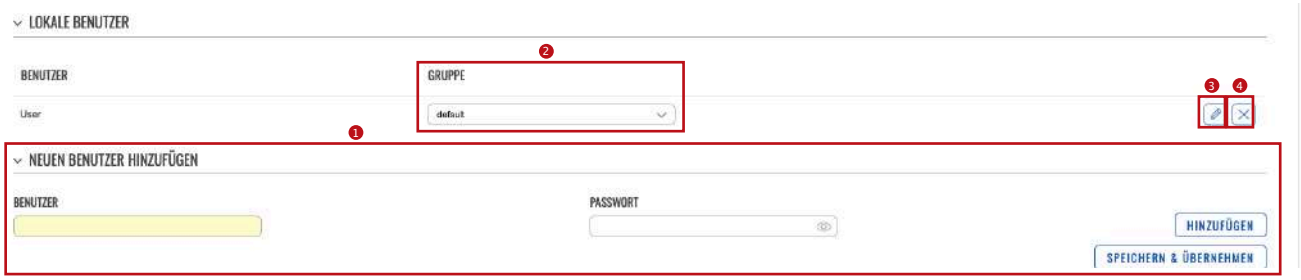
Feld	Wert	Beschreibung
UAM IP	Standard : Keine	Die IP-Adresse des Gateways des Captive Portals.
UAM Port	Standard : Keine	Der Port, auf dem das Captive Portal die Webinhalte bedient.
Angerufen	Standard : Keine	Die MAC-Adresse der IP-Adresse des Gateways des Captive Portals.
MAC	Standard : Keine	Die MAC-Adresse des Clients, der versucht, auf das Internet zuzugreifen.
IP	Standard : Keine	Identifikation für das in der RADIUS-Abfrage verwendete Captive Portal
NAS id	Standard : Keine	Identifikation für das in der RADIUS-Abfrage verwendete Captive Portal
Session id	Standard : Keine	Die eindeutige Kennung der Sitzung.
Benutzer URL	Standard : Keine	Die URL, auf die der Nutzer versucht hat zuzugreifen, bevor er auf die URL-Seiten des Captive Portals weitergeleitet wurde.
Herausforderung	Standard : Keine	Herausforderung, die zusammen mit dem Passwort des Benutzers verwendet werden sollte, um eine verschlüsselte Phrase zu erstellen, die zum Einloggen verwendet wird.

Benutzerdefiniert 1	Standard : Keine	Fügen Sie einen benutzerdefinierten Namen und einen benutzerdefinierten Wert hinzu, die in den URL-Parametern angezeigt werden.
–	SSID | Hostname | FW-Version ; Standard : SSID	–
Benutzerdefiniert 2	Standard : Keine	Fügen Sie einen benutzerdefinierten Namen und einen benutzerdefinierten Wert hinzu, die in den URL-Parametern angezeigt werden.
–	SSID | Hostname | FW-Version ; Standard : SSID	–

3.4.2 Menü SERVICES > HOTSPOT > Lokale Benutzer

Der Abschnitt Lokale Benutzer wird verwendet, um Benutzer zu erstellen und zu verwalten, die sich mit dem Hotspot verbinden können. Die Elemente der Seite Lokale Benutzer werden in der folgenden Liste und Abbildung erklärt:

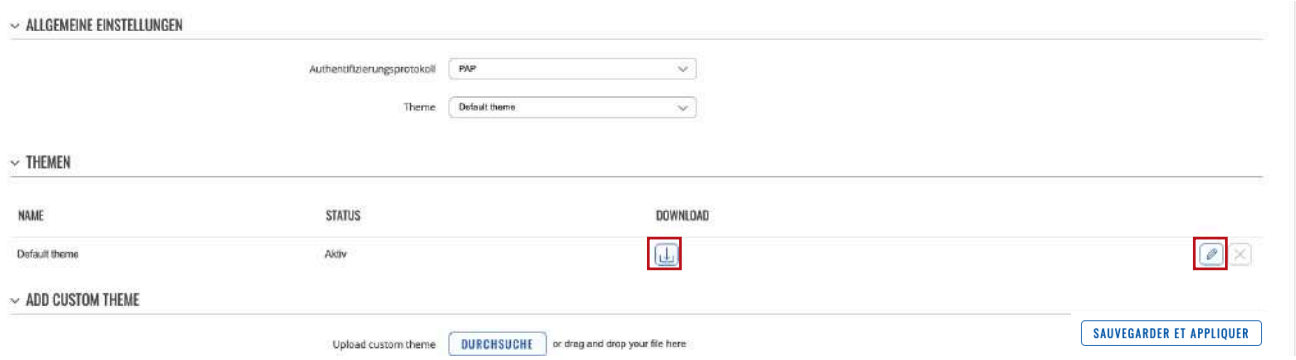
1. Durch Eingabe eines Benutzernamens, eines Passworts und Klicken auf die Schaltfläche 'Hinzufügen' erstellen Sie einen neuen Benutzer.
2. Das Dropdown-Menü 'Gruppe' ermöglicht es, einen Benutzer einer anderen Gruppe zuzuweisen.
3. Die Schaltfläche 'Bearbeiten' ermöglicht es Ihnen, das Passwort eines Benutzers zu ändern oder den Benutzer einer anderen Gruppe zuzuweisen.
4. Die Schaltfläche 'Löschen[X]' löscht einen Benutzer.



3.4.3 Menü SERVICES > HOTSPOT > Allgemeine Einstellungen

Themen

Im Abschnitt "Themen" werden alle verfügbaren Designs der Zielseite angezeigt. Um ein Thema herunterzuladen, klicken Sie auf die Schaltfläche "Download". Um ein Thema zu bearbeiten, klicken Sie auf die Schaltfläche "Bearbeiten" neben dem Themen.



Themen : Bilder

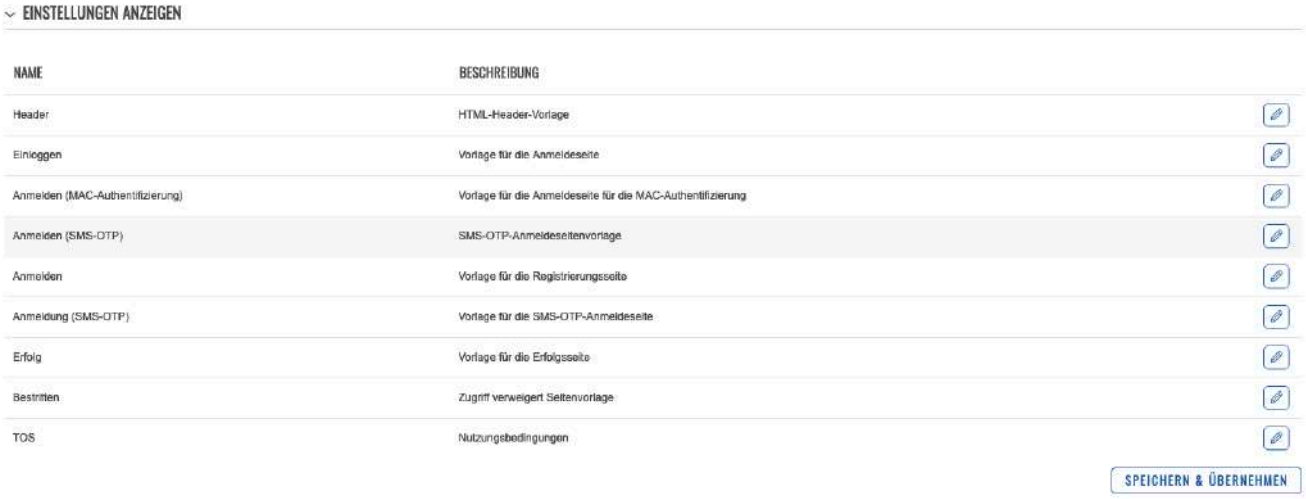
Der Abschnitt 'Bilder' ermöglicht es Ihnen, benutzerdefinierte Bilder für verschiedene Objekte hochzuladen.

Themen : Stileinstellungen

Wenn Sie auf die Schaltfläche "Bearbeiten" neben den Stileinstellungen klicken, können Sie das visuelle Erscheinungsbild Ihrer Landingpage mithilfe der CSS-Syntax ändern.

Themen : Einstellungen anzeigen

In den Softwareinformationen können Sie auf die Standardvorlagen für verschiedene Teile der Zielseite zugreifen und deren HTML-Code bearbeiten.



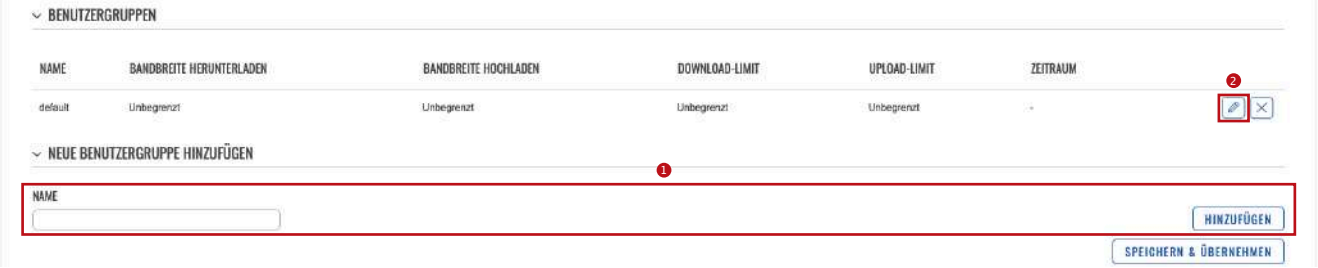
Ein eigenes Thema hinzufügen

Um ein benutzerdefiniertes Design zu verwenden, können Sie das Standarddesign herunterladen und seinen Inhalt bearbeiten. Verwenden Sie dann die Schaltfläche Durchsuchen, um es herunterzuladen.

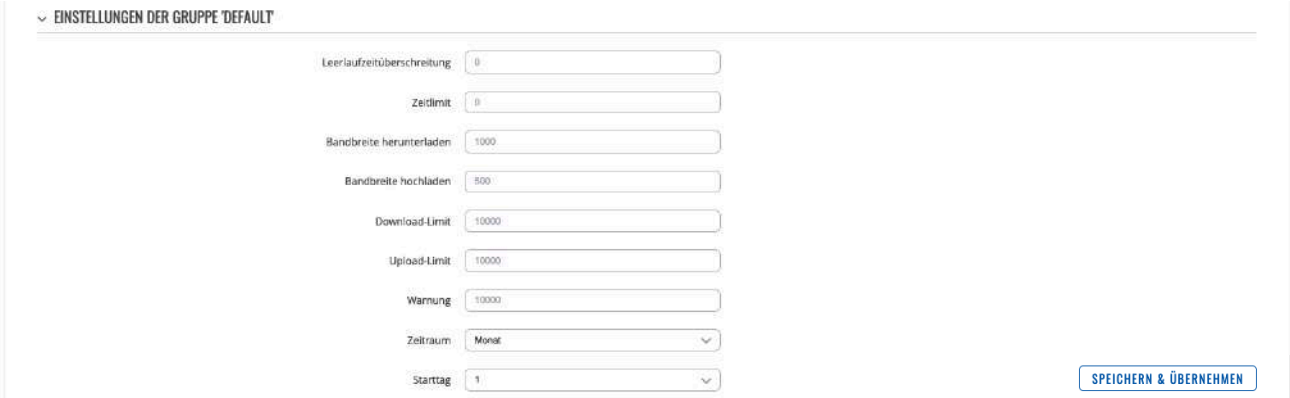
3.4.4 Menü SERVICES > HOTSPOT > Benutzergruppen

Um ein benutzerdefiniertes Design zu verwenden, können Sie das Standarddesign herunterladen und seinen Inhalt bearbeiten. Verwenden Sie dann die Schaltfläche Durchsuchen, um es herunterzuladen.

1) Erstellen Sie eine neue Gruppe, indem Sie einen benutzerdefinierten Namen eingeben und dann auf 'Hinzufügen' klicken.
2) Oder konfigurieren Sie die bestehende Regel, indem Sie auf die Schaltfläche 'Bearbeiten' neben der Regel klicken.



Die Seite mit den Einstellungen einer Gruppe wird wie folgt aussehen:

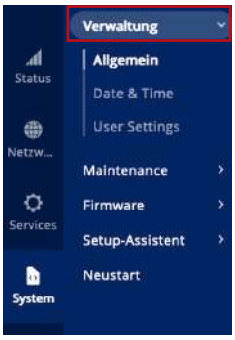


Feld	Wert	Beschreibung
Leerlaufzeitüberschreitung	Standard : Keine	Eine Zeitspanne in Sekunden, nach der inaktive Benutzer automatisch vom Hotspot getrennt werden. (0 bedeutet unbegrenzt.)
Zeitlimit	Standard : Keine	Deaktiviert den Benutzer des Hotspots, nachdem die Zeitspanne in Sekunden erreicht ist. (0 bedeutet unbegrenzt.)
Bandbreite herunterladen	Standard : Keine	Die maximale Download-Bandbreite, die Benutzer, die diesem Modell zugewiesen sind, erreichen können. Die Bandbreite kann in Mbit/s angegeben werden.
Bandbreite hochladen	Standard : Keine	Die maximale Upload-Bandbreite, die Benutzer, die diesem Modell zugewiesen sind, erreichen können. Die Bandbreite kann in Mbit/s angegeben werden.
Download-Limit	Standard : Keine	Ein Datenempfangslimit, das Benutzer, die diesem Modell zugewiesen sind, erreichen können. Nachdem das Datenlimit erreicht ist, verliert der Benutzer die Datenverbindung. Das Download-Limit wird in MB angegeben.
Upload-Limit	Standard : Keine	Ein Limit für gesendete Daten, das die dieser Vorlage zugewiesenen Nutzer erreichen können. Nachdem das Datenlimit erreicht wurde, verliert der Nutzer die Datenverbindung. Das Upload-Limit wird in MB angegeben.
Warnung	Standard : Keine	Senden Sie eine SMS-Warnung an den Benutzer des Hotspots, nachdem der Warnwert für Daten-Download oder -Upload in MB erreicht wurde. Funktioniert nur mit der SMS-OTP-Authentifizierung.
Zeitraum	Monat | Monat | Tag ; Standard : Monat	Der Beginn des Zeitraums, in dem die in diesem Abschnitt angegebene Beschränkung gelten soll. Sobald der Zeitraum abgelaufen ist, werden alle angegebenen Beschränkungen zurückgesetzt.
Startstunde	Standard : 1	Die Auswahl ändert sich je nachdem, was für "Zeitraum" ausgewählt wurde. Gibt den Tag des Monats, der Woche oder der Tageszeit an, an dem die Limits zurückgesetzt werden.

3.4.5 Menü SERVICES > HOTSPOT > Benutzerverwaltung

Die Registerkarte Aktuelle Benutzer zeigt den Status und die Sitzungsstatistiken der aktuell angemeldeten Benutzer an. Sie können einen Nutzer auch "rauswerfen" (abmelden), indem Sie auf die Schaltfläche 'Abmelden' neben seinem Namen klicken.

Der Reiter Registrierte Nutzer zeigt die Daten von eindeutigen Nutzern an, die sich bereits am Hotspot registriert haben.



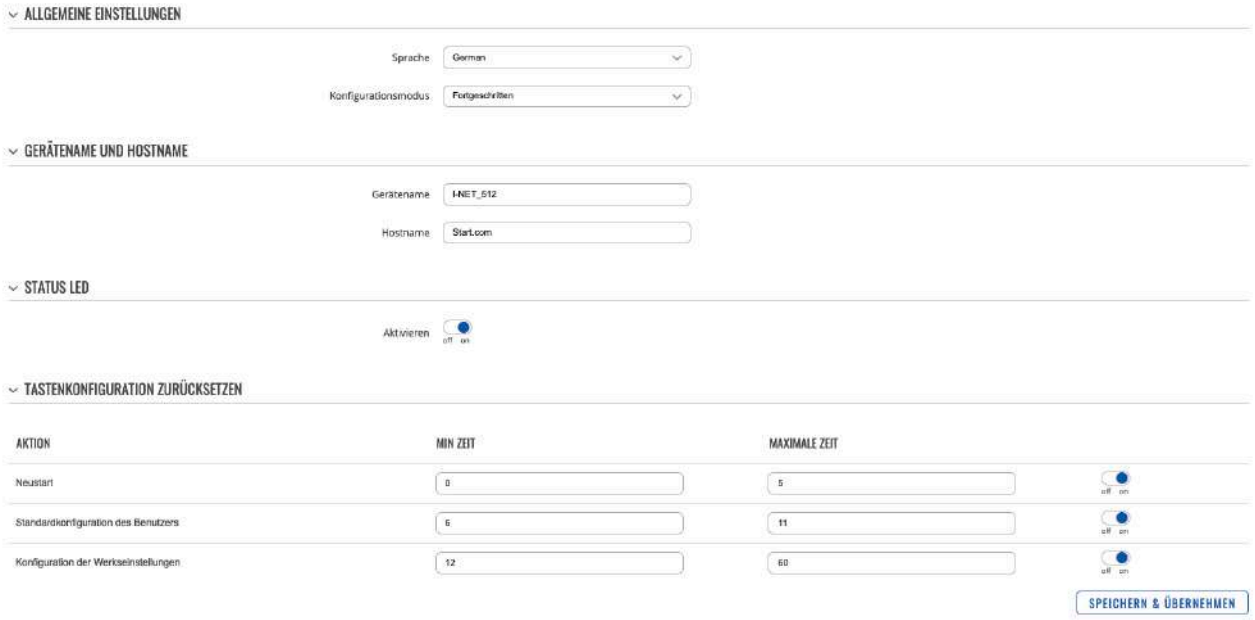
4 Menü System

Ein Hotspot ist ein Dienst, der die Authentifizierung, Autorisierung und Abrechnung eines Netzwerks bereitstellt.

4.1 Menü System > Verwaltung

4.1.1 Menü System > Verwaltung > Allgemein

Der Abschnitt Allgemein wird verwendet, um einige Einstellungen zur Verwaltung des Geräts vorzunehmen, wie z. B. das Ändern des Namens des Geräts. Weitere Informationen zum Abschnitt Allgemein finden Sie in der Abbildung und der Tabelle unten.



Feld	Wert	Beschreibung
Allgemeine Einstellungen		
Sprache	English | French | German ; Standard : French	Ändert die Sprache der Web-Benutzeroberfläche des Routers.
Konfigurationsmodus	Basic | Fortgeschritten ; Standard : Basic	Der Modus bestimmt, welche Optionen und Konfigurationen angezeigt werden. Im Basic-Modus werden nur die wichtigsten Konfigurationen angezeigt. Im Modus Erweitert gibt es mehr Freiheit bei der Konfiguration und dem Zugriff auf mehr Optionen.
Gerätename und Hostname		
Gerätename	Standard : I-NET_512	Modellname des Geräts.
Hostname	Standard : Start.com	Der Hostname des Geräts. Dies kann für die Kommunikation mit anderen Hosts im lokalen Netzwerk (LAN) verwendet werden.
Indication LED		
Aktivieren	Off | On; Standard : On	Verwaltet die LEDs zur Anzeige der Signalstärke und des Verbindungsstatus.
Tastenkonfiguration zurücksetzen		
Min Zeit	Standard : keine	Mindestzeit (in Sekunden), die die Taste gedrückt gehalten werden muss, um eine Aktion auszuführen.
Maximale Zeit	Standard : keine	Maximale Zeit (in Sekunden), die die Taste gedrückt gehalten werden kann, um eine Aktion auszuführen, danach wird keine Aktion mehr ausgeführt.

4.1.2 Menü System > Verwaltung > Date & Time

Das Network Time Protocol (NTP) ist ein Netzwerkprotokoll, das zur Synchronisierung von Uhren zwischen Computersystemen über paketvermittelte Datennetze mit variabler Latenz verwendet wird.

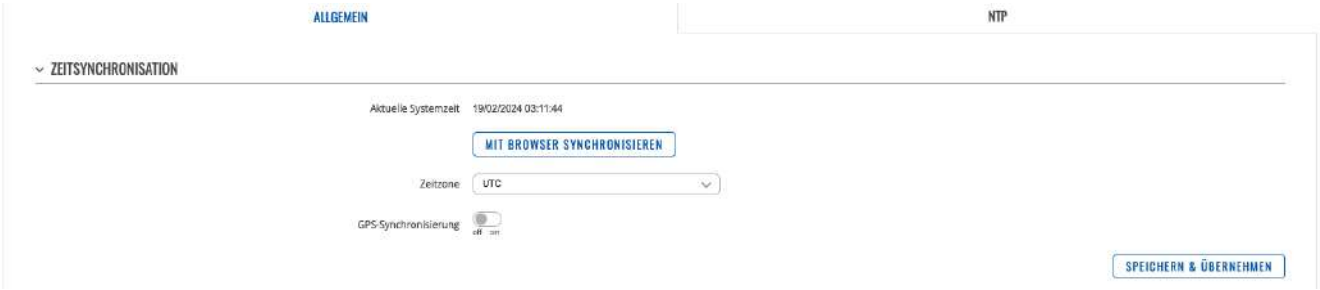
General

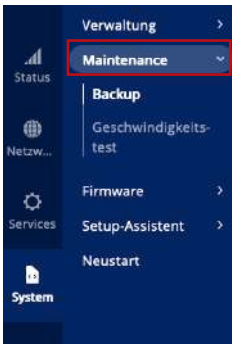
Im Abschnitt zur Zeitsynchronisierung können Sie die Zeitzone auswählen, die GPS-Synchronisierung aktivieren und die Uhrzeit synchronisieren.

Feld	Wert	Beschreibung
Aktuelle Systemzeit	Standard : Keine	Die aktuelle Ortszeit des Geräts.
Mit browser synchronisieren	Interaktive Schaltfläche	Klicken Sie, um die Uhrzeit des Geräts und die Zeitzone mit den Browsern zu synchronisieren, wenn die Uhrzeit oder die Zeitzone Ihres Geräts nicht korrekt sind.
Zeitzone	Standard : UTC	Das Gerät wird die Uhrzeit entsprechend der ausgewählten Zeitzone synchronisieren.
GPS-Synchronisierung	Off | On; Standard : Off	Aktiviert die regelmäßige Zeitsynchronisation für das System mithilfe des GPS-Moduls, wofür keine Internetverbindung erforderlich ist.

4.1.3 Menü System > Verwaltung > User Settings

Der Abschnitt Benutzereinstellungen wird verwendet, um das Passwort des aktuellen Benutzers zu ändern.





4.2 Menü System > Maintenance

4.2.1 Menü System > Maintenance> Backup

Die Seite Sicherung wird verwendet, um Sicherungsdateien für die Konfiguration zu erstellen oder vorhandene Sicherungsdateien auf das Gerät herunterzuladen.

Standardkonfiguration erstellen

Der Abschnitt Standardkonfiguration erstellen wird verwendet, um eine Datei zu erstellen oder zu löschen, die die aktuelle Konfiguration des Geräts speichert. Die Standardkonfiguration kann dann zu einem späteren Zeitpunkt auf der Seite Verwaltung oder über die Schaltfläche Zurücksetzen geladen werden.

Klicken Sie auf die Schaltfläche "Erstellen", um eine Standardkonfigurationsdatei aus der aktuellen Konfiguration Ihres Geräts zu erzeugen.

Backup-Konfiguration

Der Abschnitt zum Sichern der Konfiguration wird verwendet, um eine Datei zu erzeugen und herunterzuladen, die die aktuelle Konfiguration des Geräts speichert. Die Sicherungsdatei kann dann auf das gleiche Gerät oder ein anderes Gerät des gleichen Typs hochgeladen werden (die Produktcodes müssen übereinstimmen).

Dieser Abschnitt enthält Prüffelder für MD5- und SHA256-Prüfsummen, die aus der zuletzt heruntergeladenen Sicherungsdatei generiert werden, eine Verschlüsselungsoption und die Schaltfläche zum Herunterladen, um die Sicherungsdatei der Gerätekonfiguration zu generieren und herunterzuladen.
Wichtige Hinweise:

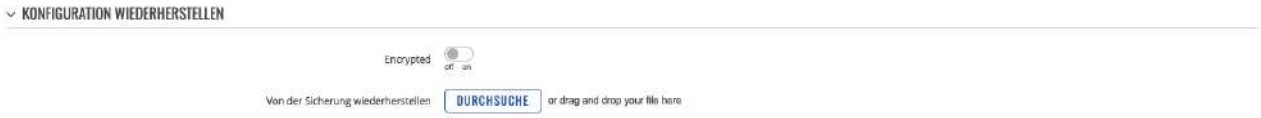
1) Das Passwortfeld ist erforderlich, wenn die Verschlüsselung aktiviert ist, dann erscheint das Feld. Wenn die Verschlüsselung aktiviert ist, aber der Router das Paket 7-zip nicht installiert hat, sollte ein Popup-Fenster erscheinen, das den Benutzer auffordert, das Paket aus dem Paketmanager herunterzuladen. Das Passwort, das zur Verschlüsselung der Sicherungsdatei verwendet wird, muss beim Entpacken des formatierten 7z-Archivs angegeben werden, um auf die tar-Datei zuzugreifen.
2) Die Sicherungsdatei speichert die auf der Mobilseite des I-NET 512 konfigurierte PIN, wird aber nur dann wiederhergestellt, wenn das Gerät beim Herunterladen der Sicherungsdatei nicht bereits eine PIN eingestellt hat - die PIN der Sicherungsdatei wird nur dann eingestellt, wenn das Gerät nicht bereits eine PIN eingestellt hat.
3) Wenn das Gerät beim Hochladen einer Sicherungsdatei keine Internetverbindung hat, wird es die vom Paketmanager installierten Softwarepakete nicht neu installieren. Sie können die Installationsdateien der Pakete manuell zur Sicherungsdatei hinzufügen, ein I-NET 512-Gerät wird sie automatisch installieren, wenn Sie die Sicherungsdatei laden, auch wenn keine Datenverbindung besteht.

Um eine Sicherungsdatei mit Paketinstallationsdateien einzubinden, gehen Sie wie folgt vor:
- Laden Sie die erforderlichen Softwarepaket-Installationsdateien von hier herunter.
- Laden Sie eine Sicherungsdatei herunter.
- Öffnen Sie die Sicherungsdatei und erstellen Sie einen neuen Ordner namens backup_packages im Verzeichnis /etc.
- Fügen Sie die benötigten Paketdateien zu /etc/backup_packages hinzu.
- Stellen Sie sicher, dass die Dateien in /etc/backup_packages vollständig mit den Erweiterungen *.ipk extrahiert werden.

Konfiguration wiederherstellen

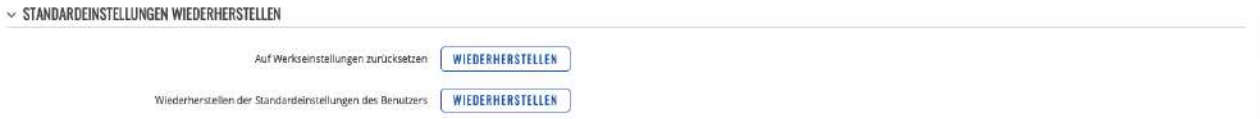
Der Abschnitt Konfiguration wiederherstellen wird verwendet, um eine Konfigurationsdatei herunterzuladen, die von diesem Gerät oder einem anderen Gerät desselben Typs genommen wurde.

Aktivieren Sie "Verschlüsselt", wenn die Sicherungsdatei zuvor verschlüsselt war, und klicken Sie dann auf die Schaltfläche "Durchsuchen", um eine Sicherungsdatei von Ihrem Computer auszuwählen. Klicken Sie schließlich auf die Schaltfläche "Archiv laden", um die ausgewählte Konfiguration auf diesem Gerät anzuwenden.



Standardeinstellungen wiederherstellen

Der Abschnitt Standardeinstellungen wiederherstellen wird verwendet, um die Standardeinstellungen des Geräts wiederherzustellen.

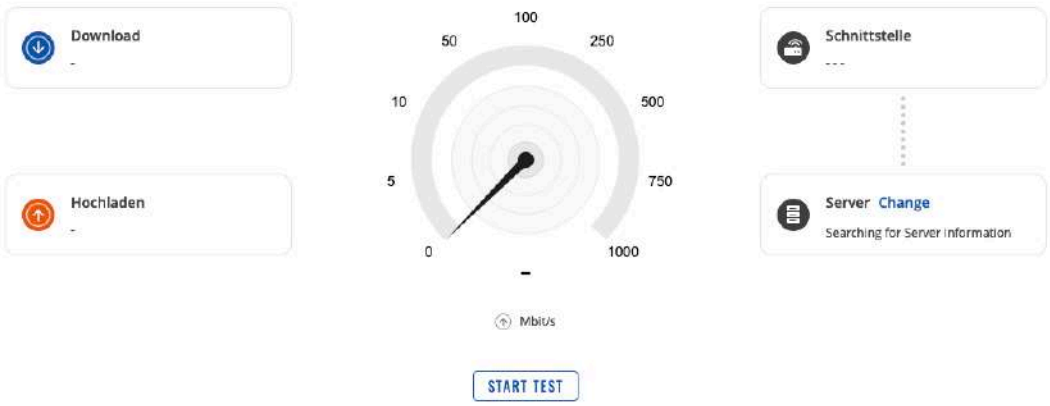


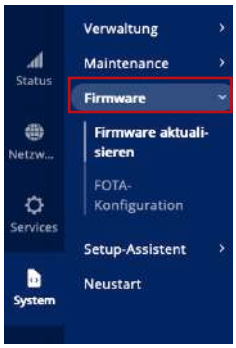
Feld	Wert	Beschreibung
Auf Werkseinstellungen zurücksetzen	Interaktive Schaltfläche	Stellt das Gerät auf die Standardeinstellungen zurück.
Wiederherstellen der Standardeinstellungen des Benutzers	Interaktive Schaltfläche	Stellt das Gerät auf die benutzerdefinierte Konfiguration zurück, die vom Benutzer festgelegt wurde.

* Sie werden diese Schaltfläche erst sehen, wenn Sie eine Standardkonfiguration des Benutzers erstellt haben.

4.2.2 Menü System > Maintenance > Geschwindigkeitstest

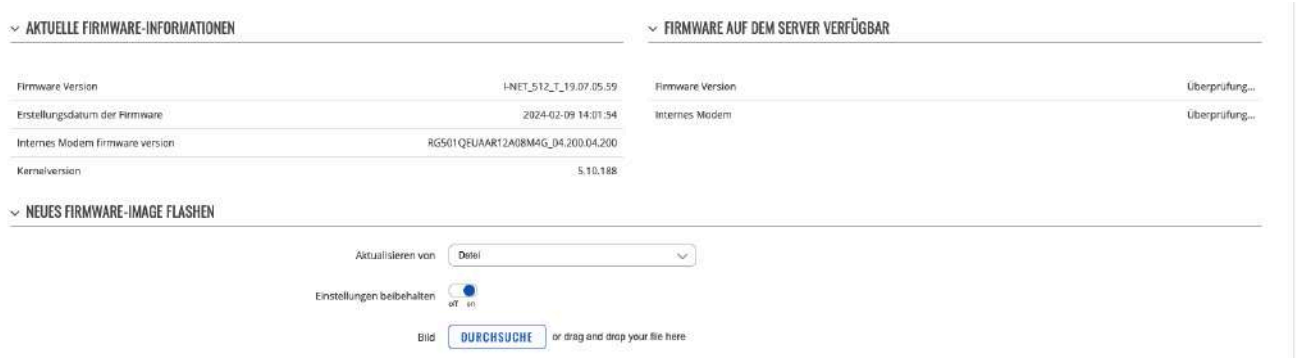
Dieser Geschwindigkeitsmesser für den Netzwerkverkehr zeigt Ihnen an, wie hoch Ihre Download- und Upload-Geschwindigkeit in Mbps ist.





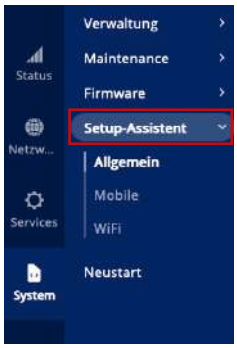
4.3 Menü System > Firmware

4.3.1 Menü System > Firmware > Firmware aktualisieren



Feld	Wert	Beschreibung
Aktualisieren von	Datei | Server : Standard : Datei	Quelle für das Bild der Firmware. Kann von FOTA heruntergeladen (Server) oder von einem Computer hochgeladen (Datei) werden.
Einstellungen beibehalten	Off | On; Standard : Off	Stellt sicher, dass alle aktuellen Einstellungen des Geräts nach der Aktualisierung der Firmware beibehalten werden.
Bild	Interaktive Schaltfläche	Klicken Sie, um Ihren Computer nach einer Firmware-Imagedatei zu durchsuchen.

SUIVANT



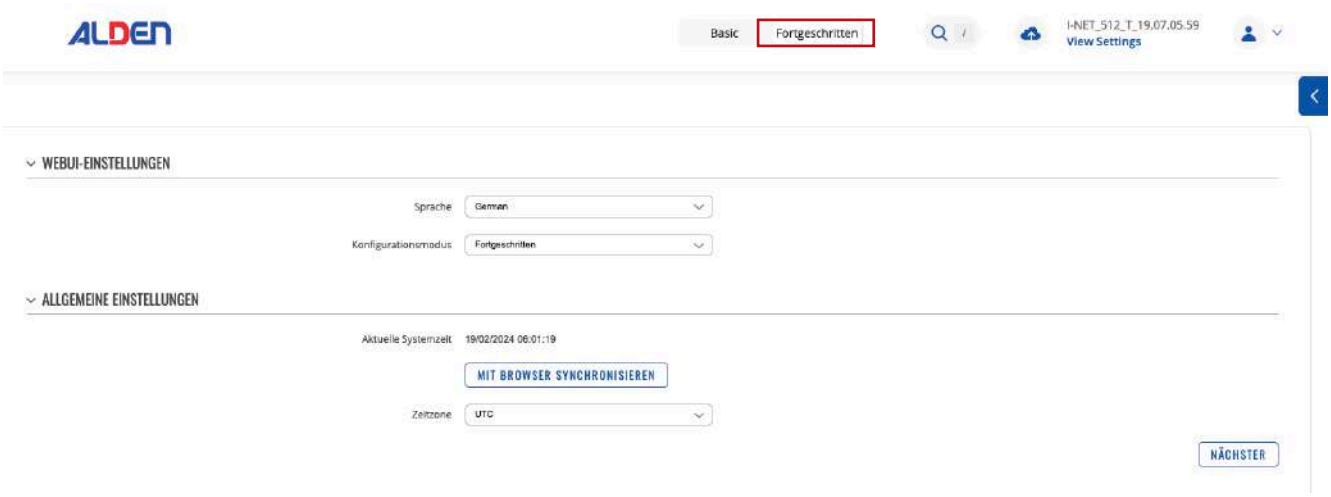
4.4 Menü System > Setup-Assistent

4.4.1 Menü System > Setup-Assistent > Allgemein

Der Abschnitt Allgemein wird verwendet, um die Uhrzeit des Geräts, die Sprache und die Einstellungen für den WebUI-Modus (Web User Interface) zu konfigurieren.

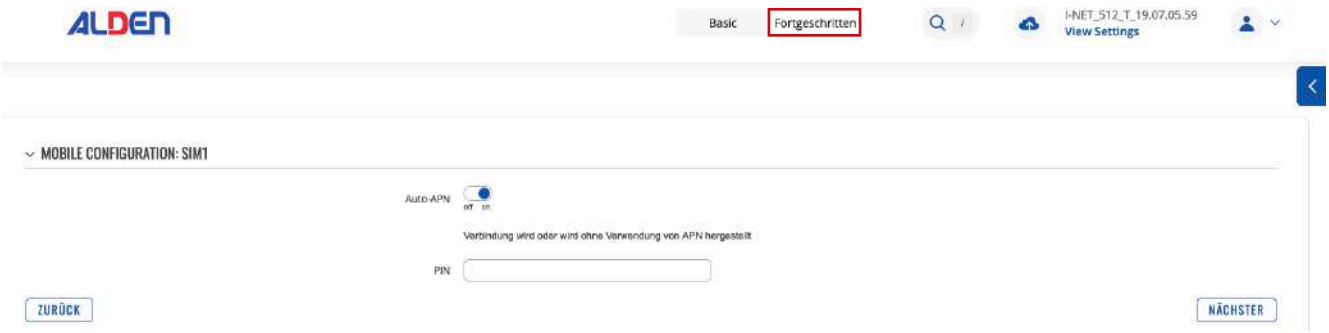
Wenn Sie es vorziehen, die Einstellungen für die Zeitzone des Geräts später festzulegen, können Sie dies über die Seite Verwaltung → NTP tun.

Wenn Sie Schwierigkeiten haben, diese Seite oder einige der hier beschriebenen Einstellungen auf der Web-Benutzeroberfläche Ihres Geräts zu finden, sollten Sie den Modus "Erweiterte Web-Benutzeroberfläche" aktivieren. Dies können Sie tun, indem Sie auf die Schaltfläche "Erweitert" klicken, die sich oben auf der Web-Benutzeroberfläche befindet.



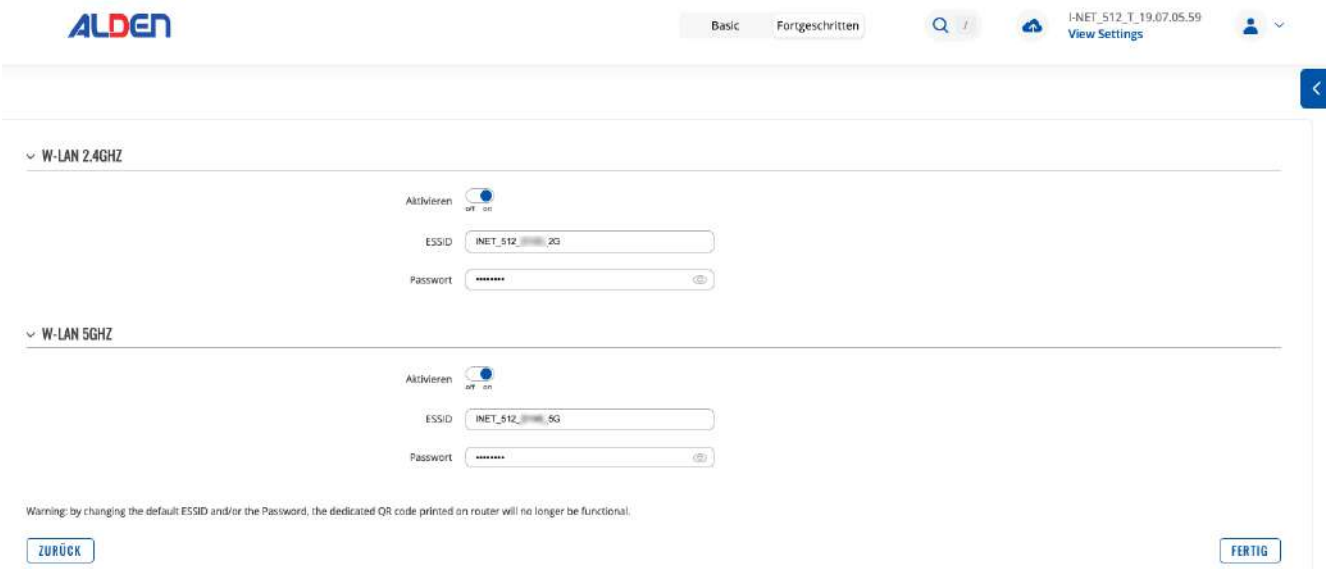
4.4.2 Menü System > Setup-Assistent > Mobile

Der Abschnitt Mobil wird verwendet, um die Einstellungen für die SIM-Karte des Geräts zu konfigurieren.

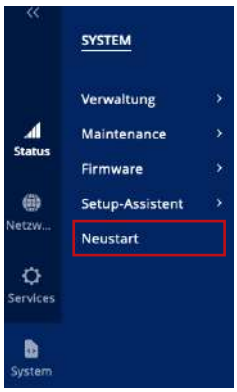


Feld	Wert	Beschreibung
Auto-APN	Off | On; Standard : On	Ein Access Point Name (APN) ist ein Gateway zwischen einem GSM-, GPRS-, 3G- oder 4G-Mobilfunknetz und einem anderen Computernetz. Je nach Vertrag kann es sein, dass einige Betreiber verlangen, dass Sie den APN nur eingeben, um die Anmeldung in einem Netz abzuschließen. In anderen Fällen wird ein APN verwendet, um je nach Vertrag spezielle Einstellungen vom Betreiber zu erhalten (z. B. eine öffentliche IP-Adresse). Der automatische APN durchsucht eine interne Android-APN-Datenbank und wählt einen APN auf der Grundlage des Netzbetreibers und des Landes der SIM-Karte aus. Wenn der erste automatisch ausgewählte APN nicht funktioniert, versucht er, den nächsten vorhandenen APN aus der Datenbank zu verwenden.
Off: APN	Standard : Benutzerdefiniert	Wählen Sie zwischen einem vom Gerät vorgeschlagenen APN oder geben Sie Ihren eigenen APN ein.
Benutzerdefiniert : Benutzerdefinierter APN	Standard : Keine	Eine benutzerdefinierte APN-Netzwerkkennung. Darf nicht mit einer der folgenden Zeichenfolgen beginnen: "rac", "lac", "sgsn" oder "rnc", darf nicht mit ".gprs" enden und darf nicht den Wert "*" annehmen.
Benutzerdefiniert : Authentifizierungsart	Keine | PAP | CHAP; Standard : Keine	Die Methode, die Ihr Netzbetreiber verwendet, um neue Verbindungen in seinem Netzwerk zu authentifizieren. Wenn Sie PAP, CHAP oder beides wählen, müssen Sie einen Benutzernamen und ein Passwort eingeben.
PIN	Standard : Keine	Ein vierstelliges numerisches Passwort, das zur Authentifizierung des Modems an der SIM-Karte verwendet wird.

4.4.3 Menü System > Setup-Assistent > WiFi



Feld	Wert	Beschreibung
Aktivieren	Off | On; Standard : On	Aktiviert oder deaktiviert den Wi-Fi-Zugangspunkt.
ESSID	Standard : INET_512_	Ein Identifikationsname für den Zugangspunkt. So wird der Zugangspunkt von den verbundenen Geräten gesehen.
Passwort	Standard : einzigartig für jedes Gerät	Ein Passwort, das zur Authentifizierung der Benutzer an diesem Zugangspunkt verwendet wird.



4.5 Menü System > Neustart

Klicken Sie auf die Schaltfläche "Neustart", wenn Sie das Gerät neu starten möchten.

ALDEN-Garantie

Die ALDEN-Garantie umfasst :

Garantien für Herstellungsfehler werden ab dem Datum der Rechnungsstellung an den Käufer gewährt, sofern der Garantieschein zurückgeschickt wird. Erfolgt keine Rücksendung, ist diese Garantie zeitlich begrenzt. Um die Produktgarantie in Anspruch nehmen zu können, müssen Sie unbedingt die Kaufrechnung für das besagte Produkt aufbewahren.

Achtung: Jeder Eingriff ohne schriftliche Zustimmung der SAS ALDEN führt von Rechts wegen zur Ungültigkeit der Garantie. Der Kunde und der Käufer haben keinen Anspruch auf eine wie auch immer geartete Entschädigung für Demontage, Wiedermontage oder Nutzungsausfall von weniger als 30 Tagen. Die SAS ALDEN kann nicht für Zwischenfälle oder Schäden jeglicher Art haftbar gemacht werden, wenn die Montage nicht den Empfehlungen der SAS ALDEN entspricht. Es wird darauf hingewiesen, dass jede elektrische Installation durch eine angemessene Sicherung geschützt werden muss

Generell muss die Montage nach den Regeln der Kunst durchgeführt werden. Es wird davon ausgegangen, dass der Installateur und der Nutzer die Vorschriften und Gesetze kennen. Der Installateur und der Nutzer müssen sich über die Montagevorschriften auf dem Laufenden halten. Der Installateur und der Nutzer haben keinen Anspruch auf Entschädigung oder Garantie, wenn diese Regeln nicht beachtet werden.

Sie profitieren jedoch in jedem Fall von den gesetzlichen Garantiebestimmungen, insbesondere von denjenigen, die sich auf die Garantie für versteckte Mängel beziehen.

Achtung: Die Anwendung von Garantien sowie eine eventuelle Rücksendung bedürfen der vorherigen Zustimmung der SAS ALDEN. Eventuelle Rücksendungen erfolgen franko und gehen zu Lasten der Absender (Kunde, für die Rücksendung ALDEN; ALDEN, für die Rücksendung Kunde). Im Falle eines Antrags auf Rücksendung per Express oder ChronoPost gehen die Kosten für die Kundenrücksendung zu Lasten des Kunden.

Von der ALDEN Garantie ausgeschlossen sind:

- der Ersatz von Verbrauchsmaterialien und Verschleißteilen ;

- die anormale oder nicht bestimmungsgemäße Verwendung der Produkte. Wir empfehlen Ihnen in diesem Zusammenhang, die mit den Produkten gelieferte Gebrauchsanweisung aufmerksam zu lesen;

- Störungen, die mit dem Zubehör zusammenhängen oder auf eine falsche Montage zurückzuführen sind ;

- Defekte und deren Folgen, die auf den Eingriff einer nicht von der SAS ALDEN autorisierten Reparaturwerkstatt zurückzuführen sind;

- Mängel und deren Folgen, die auf eine nicht bestimmungsgemäße Verwendung des Produkts zurückzuführen sind;

- Mängel und ihre Folgen im Zusammenhang mit jeglichen äußeren Ursachen.

Garantie

ALDEN empfiehlt, sich bei der Montage an Fachleute zu wenden.

Im Falle einer Eigeninstallation übernimmt der Käufer die Verantwortung für die Sicherheit.

In diesem Fall wird davon ausgegangen, dass der Käufer über die erforderlichen Fähigkeiten verfügt. Er verpflichtet sich, die üblichen Regeln einzuhalten, die von Fachleuten angewendet werden. Er wird sicherstellen, dass er die im Land der Nutzung geltenden Gesetze einhält. Er wird das Produkt nicht vom vorgesehenen Verwendungszweck abbringen.

Garantie :
Der Käufer wird sich im Falle einer Fehlfunktion mit seinem Händler in Verbindung setzen.

ACHTUNG:
Die Garantie verfällt, wenn ein Eingriff ohne Zustimmung von ALDEN vorgenommen wird.