

Guide d'installation

Routeur I-NET 512

Router I-NET 512



Modèles déposés – Photos non contractuelles – Document établi sous réserve de modifications techniques

Sommaire.....2-3

Avertissements.....4-7

- Sécuriser l'accès de votre appareil :.....5
- Manipulation du produit.....6
- Mise à jour du I-NET 5127
- Code PUK.....7

Information de sécurité I-NET 5128

- Informations de sécurité I-NET 512.....8
- Exposition RF.....8
- Conditions de fonctionnement8
- Produits défectueux et endommagés8
- Sécurité électrique8

Installation..... 09-11

- Configuration I-NET 512.....9
- I-NET 512 Mesures spatiales et poids9
- Mesures principales9
- Vue avant.....9
- Vue arrière.....9
- Espace de montage10
- Fixation10

Configuration 11-14

- Description des interfaces.....11
- Brochage de la prise d'alimentation.....11
- Carte SIM I-NET 51212
- Voyant d'alimentation13
- Voyants du port Ethernet13
- Voyants du port WAN13
- Voyants du réseau mobile14
- LED d'indication de la force du signal mobile ...14
- Voyants de la Bande WiFi.....14
- Info pratiques15
- Répéteur WiFi.....15
- Sélection 5G/4G/3G.....15
- Sélection manuelle de l'opérateur.....15
- Mode Normal /Avancé.....15
- Gestion réseau15
- Installation rapide15

Menu Statut 16-25

- 1. Menu Statut16
 - 1.1 Menu Statut > Aperçu16
 - Modem16
 - Bouton Widget : Infos.....16
 - Ajout de plus de widgets.....17
 - Déblocage carte SIM – code PUK.....17
 - 1.2 Menu Statut > Système18
 - 1.3 Menu Statut > Réseau19
 - 1.3.1 Menu Statut > Réseau > Mobile19
 - 1.3.2 Menu Statut > Réseau> LAN21
 - 1.3.3 Menu Statut > Réseau> Topologie21
 - 1.3.2 WiFi22

- 1.4 Menu Statut > WiFi22
 - 1.4.1 Menu Statut > WiFi > Interface.....22
 - 1.4.2 Menu Statut > WiFi > Analyse des canaux22
- 1.5. Menu Statut > Données en temps réel23
 - 1.5.1 Menu Statut > Données en temps réel > Trafic23
 - 1.5.2 Menu Statut > Données en temps réel > Signal mobile24
- 1.6 Menu Statut > UTILISATION MOBILE25

Menu Réseau..... 26-70

- 2. Menu Réseau26
 - 2.1 Menu Réseau > Mobile.....26
 - 2.1.1 Menu Réseau > Mobile > Général26
 - Paramètres de la carte SIM26
 - Reconnexion sur signal faible.....27
 - Paramètres de l'opérateur27
 - Paramètres de limite de SMS27
 - USSD28
 - 2.1.2 Menu Réseau > Mobile > Commutateur SIM29
 - 2.1.3 Menu Réseau > Mobile > opérateurs réseaux30
 - Sélection manuelle de l'opérateur.....30
 - Liste des opérateurs31
 - 2.2 Menu Réseau > WAN (Mode Avancé)32
 - Interfaces WAN.....32
 - Ajouter une nouvelle instance32
 - Paramétrage des interfaces32
 - Réglages Généraux33
 - Réglages Généraux : Statique.....33
 - Réglages Généraux : DHCP.....34
 - Réglages Généraux : DHCPv634
 - Réglages Généraux : PPPoE35
 - Réglages Généraux : mobile.....35
 - Mode : NAT.....35
 - Mode : Bridge (Pont).....37
 - Mode : Passthrough (traversant)38
 - Paramètres IPv640
 - Paramètres IPv6 : protocole Statique40
 - Paramètres IPv6 : protocole DHCPv6.....41
 - Paramètres IPv6 : PPPoE41
 - Paramètres avancés.....42
 - Paramètres avancés : protocole Statique.....42
 - Paramètres avancés : protocole DHCP43
 - Paramètres avancés : Protocole DHCPv644
 - Paramètres avancés : Protocole PPPoE45
 - Paramètres avancés : Protocole mobile.....46
 - Paramètres avancés : Protocole mobile > Limite de données mobiles46
 - Paramètres physiques47
 - Paramètres du pare-feu47
 - 2.3 Menu Réseau > LAN48
 - Interfaces LAN.....48
 - Ajouter une nouvelle instance48
 - Paramètres généraux48

- Paramètres IPV6	49
- Paramètres avancés.....	49
- Paramètres physiques	50
- Paramètres du pare-feu	50
- Serveur DHCP.....	51
- Serveur DHCP : configuration générale	51
- Serveur DHCP : paramètres avancés	52
- Options DHCP personnalisées	53
- Serveur DHCP : paramètres IPv6	53
2.4 Menu Réseau > WiFi.....	54
- SSID	54
- Configuration générale	55
- Paramètres avancés.....	57
- Configuration des interfaces	58
- Configuration générale	58
- Paramètres avancés : Mode points d'accès	59
- Paramètres avancés : Mode Client et Multi AP...60	
- Paramètres avancés : Mode Mailles.....	61
- Sécurité WiFi	62
- Filtre MAC	62
- Mode client	63
- Configuration du mode client.....	63
- Mode maillage (ou MESH)	64
- Nœud de maillage.....	65
- Points d'accès multiples	65
- Paramètres généraux	66
- Points d'accès	66
- QR Codes WiFi.....	67
2.5 Menu Réseau > GESTION RÉSEAU	68
- Configuration de l'interface.....	68
- Répartition des données.....	69
- Règles.....	70
- Politique	70

Menu Services 71-99

3. Menu SERVICES	71
3.1 Menu SERVICES > Services distants	71
3.1.1 Menu SERVICES > Services distants > RMS71	71
3.2 Menu SERVICES > VPN.....	72
3.2.1 Menu SERVICES > VPN > IPSEC.....	72
- Paramètres généraux secrets	73
- Instance IPsec : paramètres de connexion	74
- Paramètres généraux	74
- Paramètres avancés.....	75
- Notes complémentaires :.....	76
3.2.2 Menu SERVICES > VPN > OPENVPN.....	77
- OPENVPN > Serveur	77
- OPENVPN > Client	81
3.2.3 Menu SERVICES > VPN > WireGuard	86
- Interface WireGuard > Configuration générale.....	86
- Interface WireGuard > Paramètres avancés.....	87
- Interface WireGuard > Pairs.....	87
- Pairs > Configuration générale.....	87
- Pairs > Paramètres avancés.....	88
3.2.4 Menu SERVICES > VPN > ZeroTier	89
3.3 Menu SERVICES > GPS.....	91
3.3.1 Menu SERVICES > GPS > Général.....	91

3.3.2 Menu SERVICES > GPS > Carte	91
3.4 Menu SERVICES > Hotspot	92
3.4.1 Menu SERVICES > Hotspot > Général	92
- Instances HOTSPOT.....	92
3.4.2 Menu SERVICES > Hotspot > Utilisateurs locaux	96
3.4.3 Menu SERVICES > Hotspot > Page de destination	96
- Thèmes.....	96
- Thèmes : images.....	97
- Thèmes : Paramètres de style.....	97
- Thèmes : Informations logiciel	97
- Ajouter un thème personnalisé	97
3.4.4 Menu SERVICES > Hotspot > Groupes d'utilisateurs	98
3.4.5 Menu SERVICES > Hotspot > Gestion des utilisateurs.....	99

Menu Système 100-106

4 Menu Système.....	100
4.1 Menu Système > Administration	100
4.1.1 Menu Système > Administration > Général	100
4.1.2 Menu Système > Administration > Date et heure.....	101
- Général.....	101
4.1.3 Menu Système > Administration > Paramètres utilisateur	101
4.2 Menu Système > Maintenance.....	102
4.2.1 Menu Système > Maintenance > Sauvegarde / Restauration.....	102
- Créer une configuration par défaut	102
- Sauvegarde de la configuration	102
- Restaurer la configuration	103
- Restaurer les paramètres par défaut.....	103
4.2.2 Menu Système > Maintenance > Speedtest	103
4.3 Menu Système > Logiciel	104
4.3.1 Menu Système > Logiciel > Mise à jour du logiciel.....	104
4.4 Menu Système > Assistant d'installation	104
4.4.1 Menu Système > Assistant d'installation > Général.....	104
4.4.2 Menu Système > Assistant d'installation > Mobile	105
4.4.3 Menu Système > Assistant d'installation > WiFi	106
4.5 Menu Système > Redémarrer	106

Garantie ALDEN 107

Garantie..... 108

Bon de garantie 108

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.

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 quelque 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)

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 :

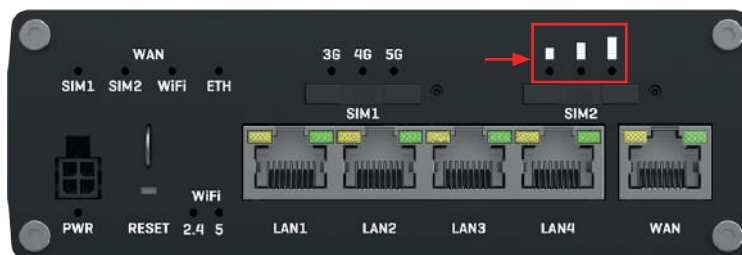
- Toutes les LED éteintes : Téléchargement du nouveau logiciel (durée : jusqu'à 30secondes)
- Clignotement des 3 LED l'une après l'autre : Installation du nouveau logiciel (durée : jusqu'à 90 secondes).

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



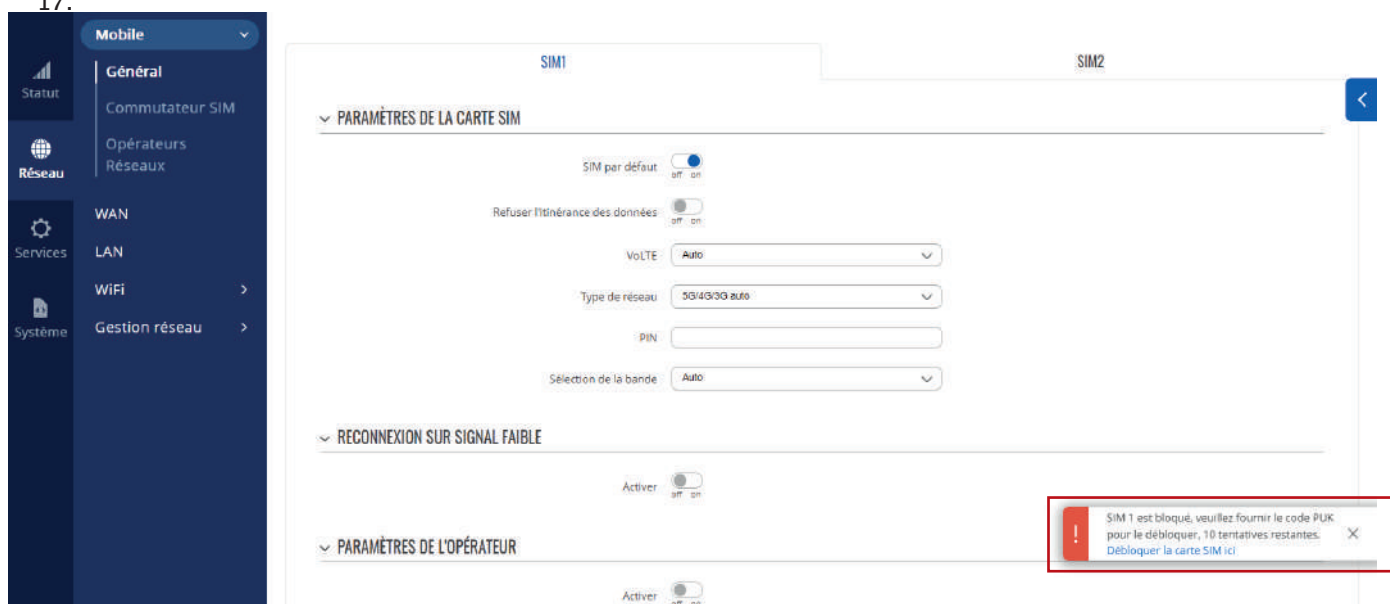
Code PUK

Le code PUK (Personal Unblocking Key) est un code de secours composé de 8 chiffres qui permet de débloquent 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 +40° 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 :

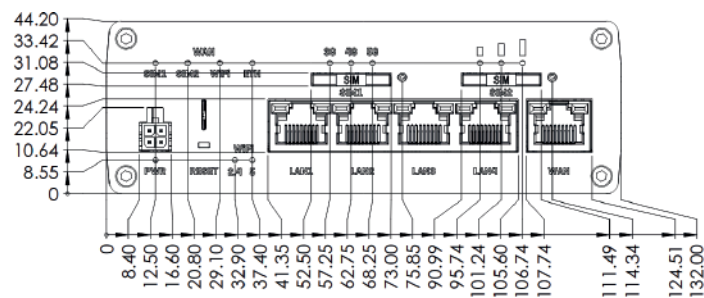
Boîtier de l'appareil * : 132 x 44,2 x 95,1 mm

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.

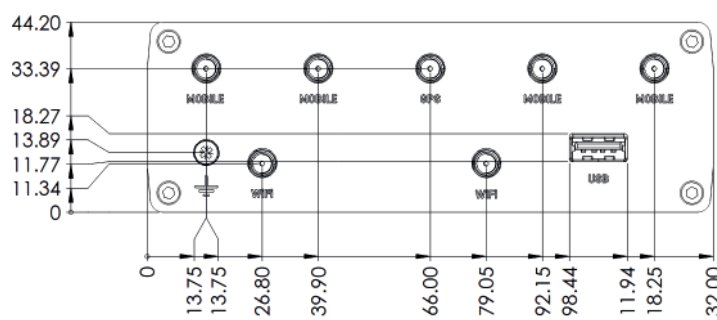
Vue avant

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



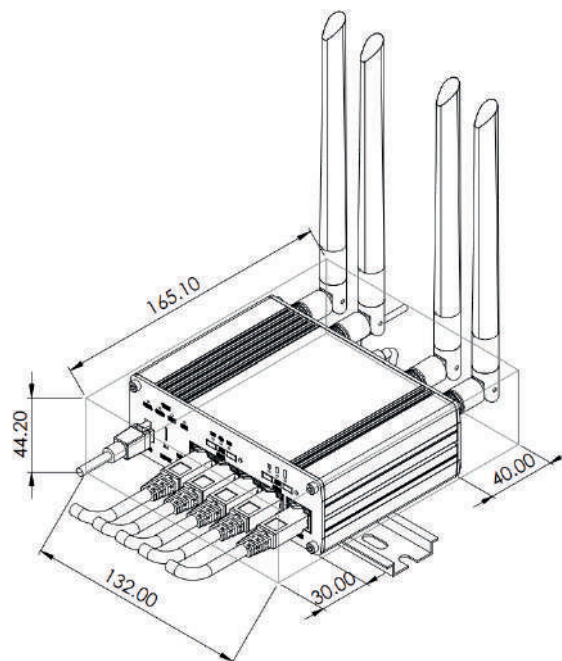
Vue arrière

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



Espace de montage

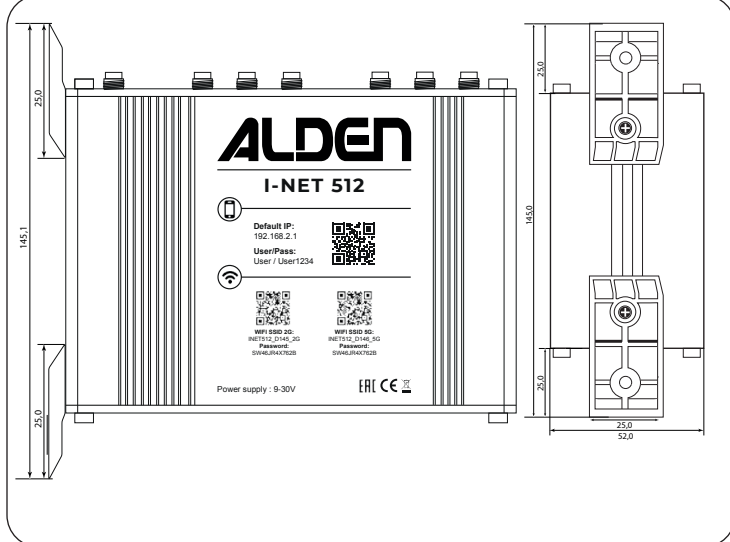
La figure ci-dessous représente le volume requis de l'appareil lorsque les câbles et les antennes sont connectés :



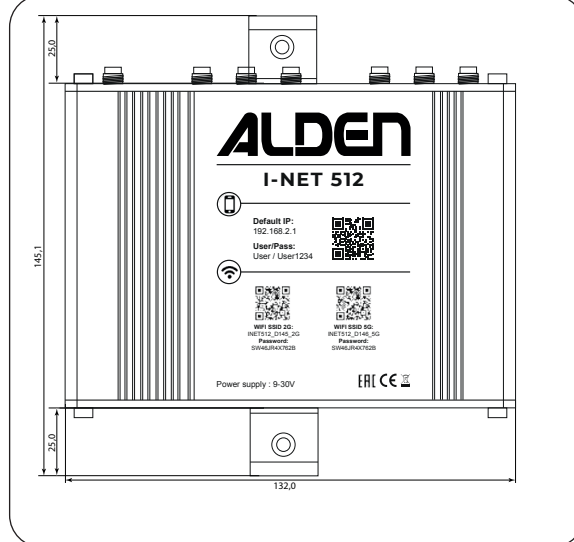
Fixation

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

Fixation verticale



Fixation horizontale

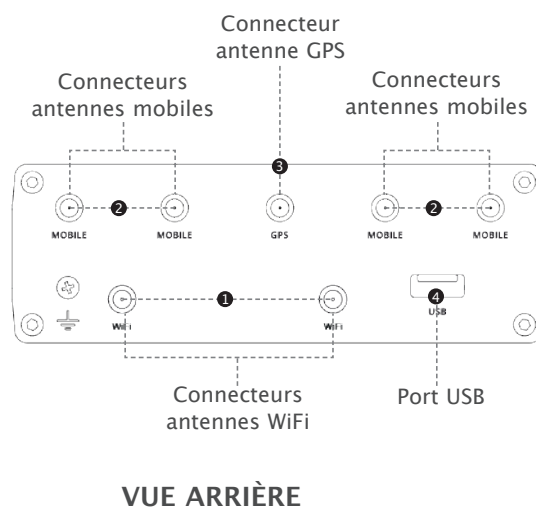
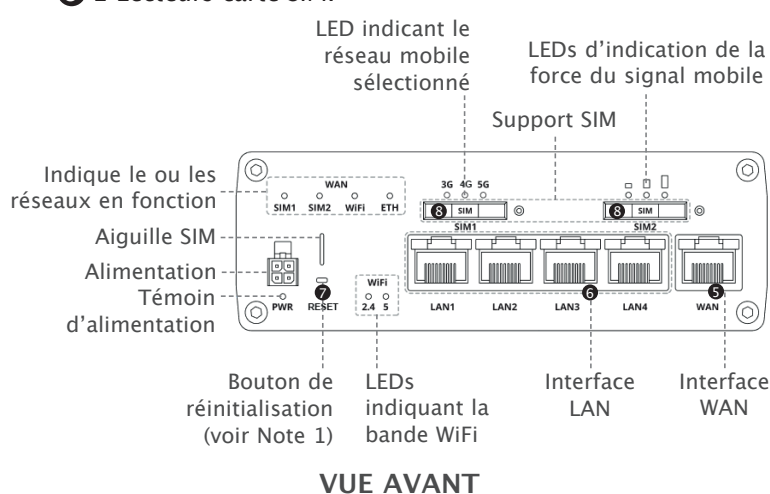


Il est à noter qu'il est possible de fixer le routeur verticalement et horizontalement. Visser les 2 supports à l'aide des 2 vis (fournies) dans le rail du routeur, prévu à cet effet.

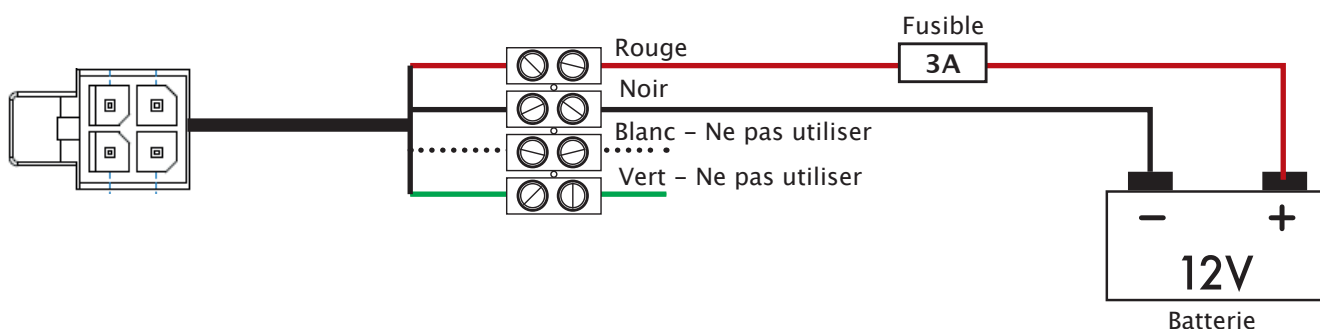
Description des interfaces

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

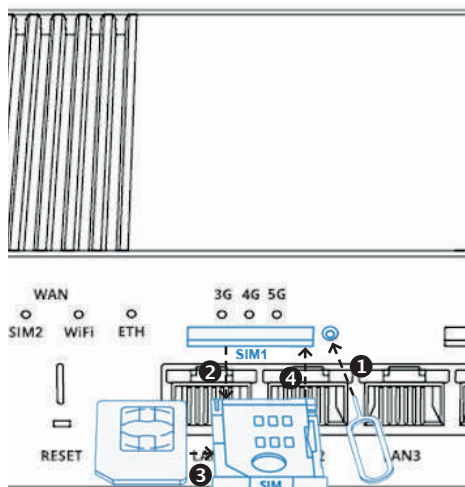
- ❶ Interface WiFi via 2 connecteurs à l'arrière pour un accès sans fils à internet entre le routeur et un ordinateur ou une borne WiFi externe. L'interface WiFi permet l'accès à l'interface web utilisateur du routeur et à internet.
- ❷ Interface mobile 5G/4G avec 4 connecteurs pour connecter 4 antennes MIMO.
- ❸ Un connecteur GPS
- ❹ Un port USB
- ❺ Un port WAN à l'avant pour un accès à internet grâce à un réseau filaire externe.
- ❻ 4 ports LAN pour la connexion filaire d'un ordinateur au routeur I-NET 512.
- ❼ 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.
- ❽ 2 Lecteurs carte SIM.



Brochage de la prise d'alimentation

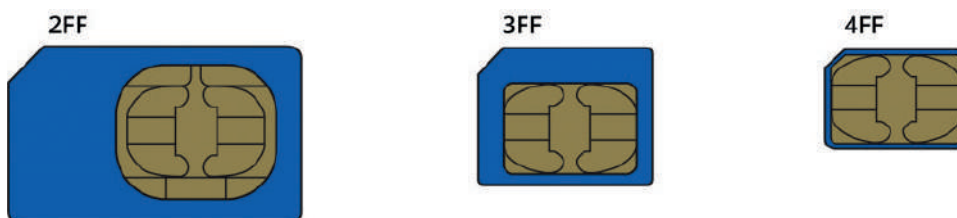


Carte SIM I-NET 512



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.

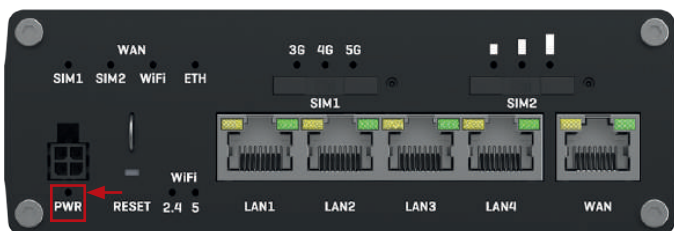
L'appareil est compatible avec les cartes de taille mini-SIM (2FF). Mais comme différents types de cartes SIM ont le même agencement de contacts, des cartes SIM plus petites peuvent également être utilisées avec le routeur, à condition qu'elles soient insérées dans un adaptateur de carte SIM 2FF. Une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

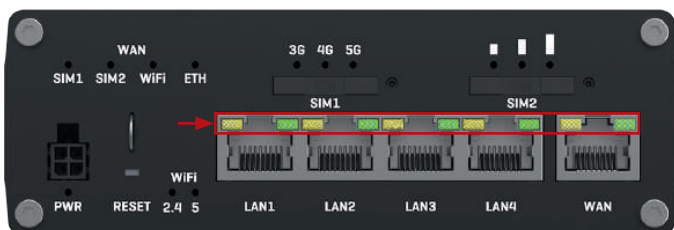


Il indique si l'appareil est sous tension ou non.

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.



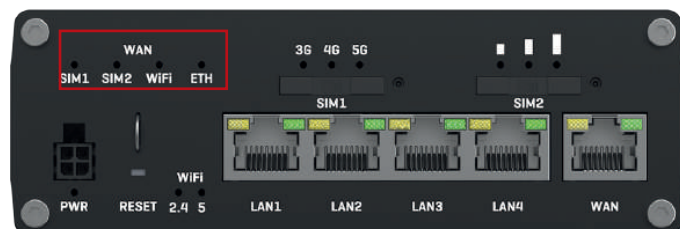
Ils fournissent des informations sur les états actuels des ports Ethernet. Chaque port possède deux voyants :

- 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.

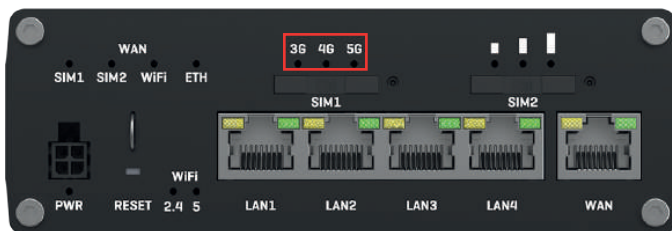


Ils indiquent quel type de connexion Internet est actuellement actif.

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.

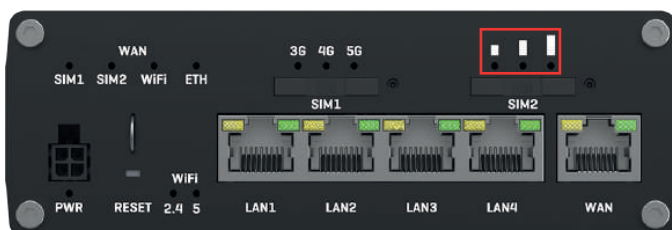


Ils affichent le type de connexion Internet actuellement actif.

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 au-dessus de la fente de la carte SIM.

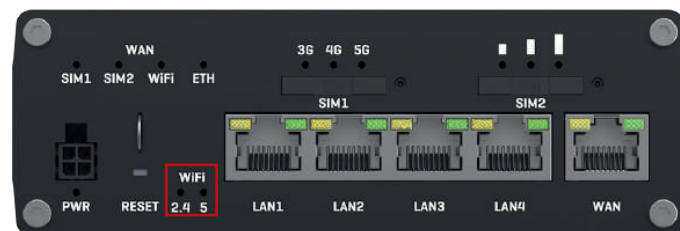


Le nombre de LED allumées représente une valeur de force de signal mobile (RSSI) différente en dBm.

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

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.

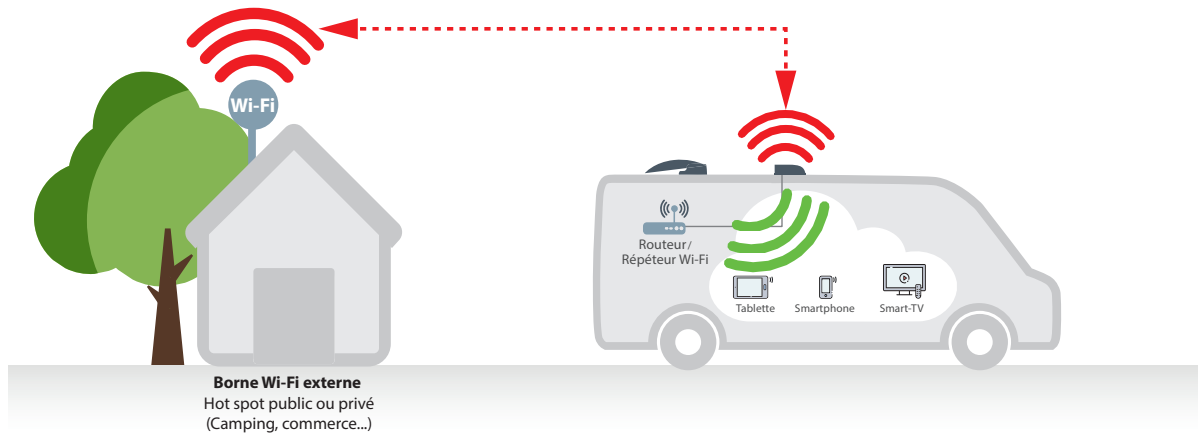


Ils indiquent si un point d'accès WiFi (AP) est actif sur une bande spécifique.

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 son propre répéteur WiFi et 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 spécifier 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

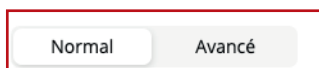
Dans certains cas d'utilisations (Ex. à l'étranger), il peut être nécessaire de sélectionner manuellement l'opérateur mobile pour sa carte SIM.

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 accessibles 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



I-NET_512_T_19.07.05.59
Options d'affichage



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.

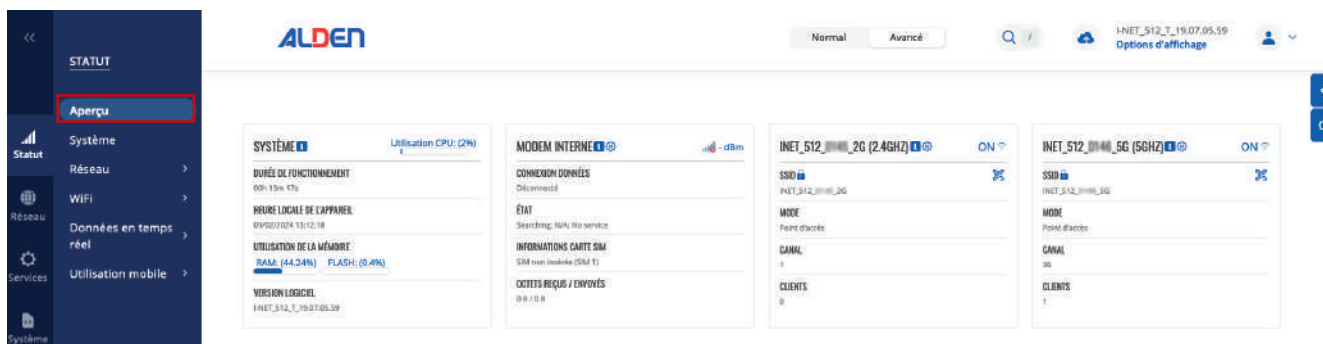
Installation rapide

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 :



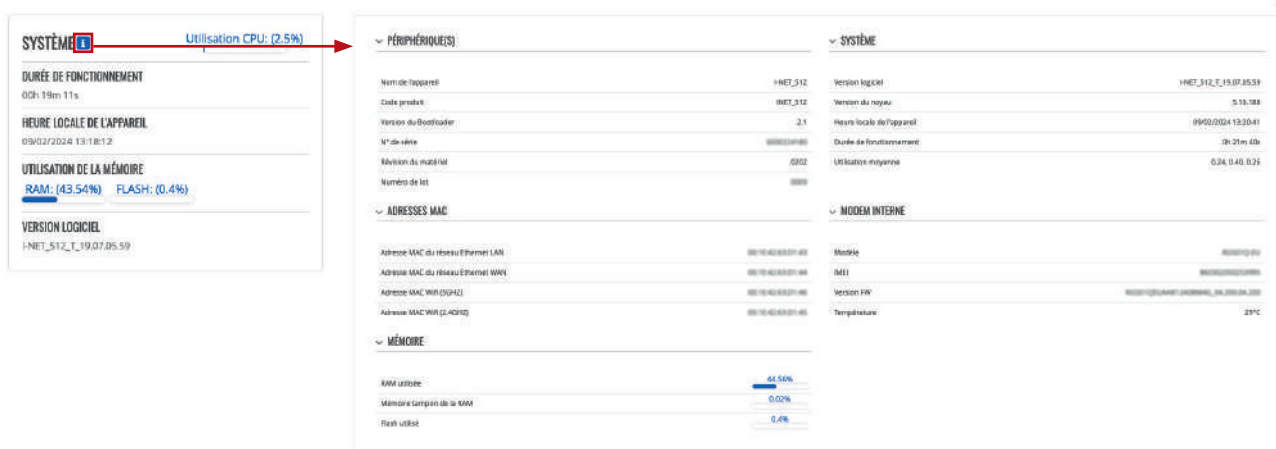
Modem

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

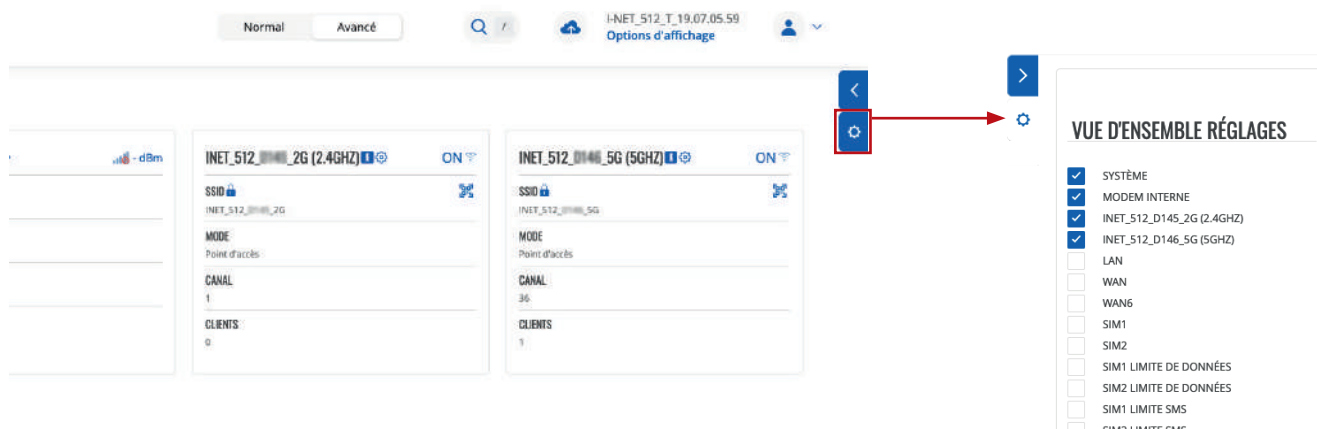
Bouton Widget : Infos

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.

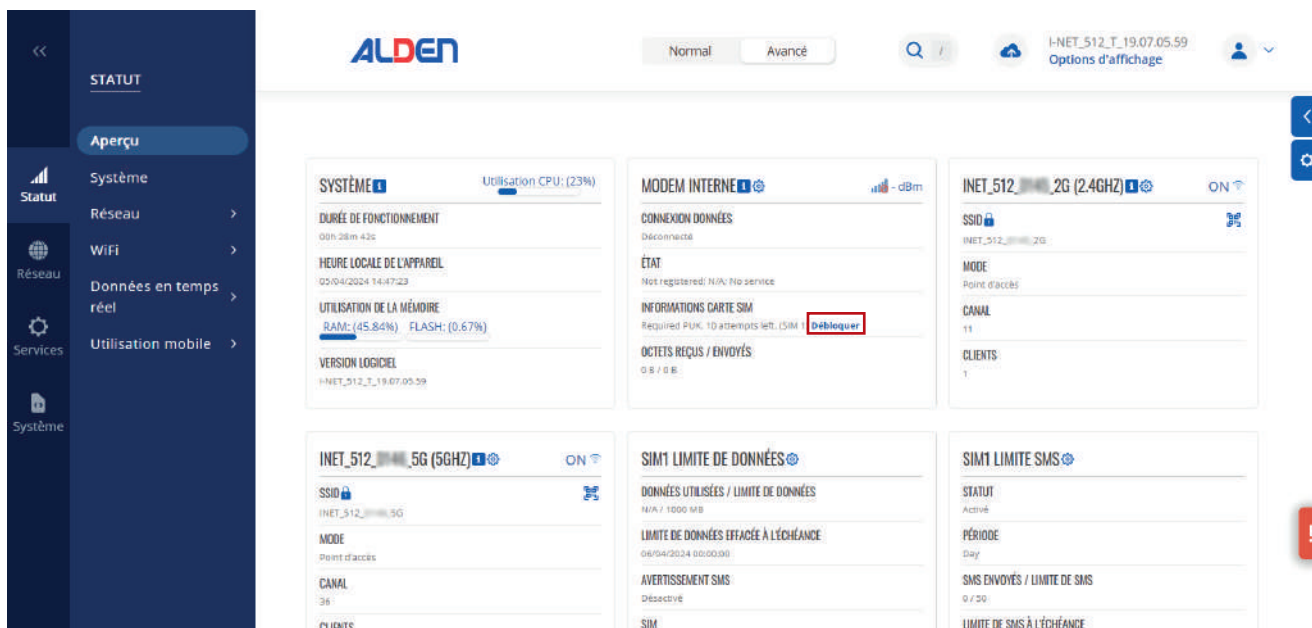


Débloquer carte SIM - code PUK

Le code PUK (Personal Unblocking Key) est un code de secours composé de 8 chiffres qui permet de débloquent 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.

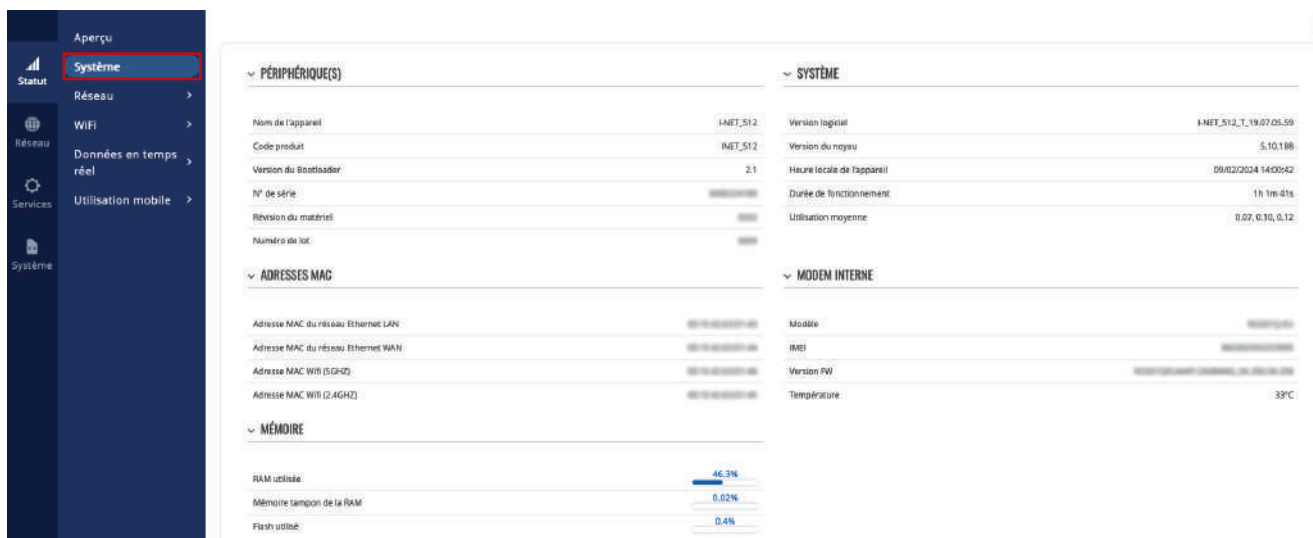
Le code PUK peut être saisi en cliquant sur le lien "Débloquer" affiché en bleu.



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 :



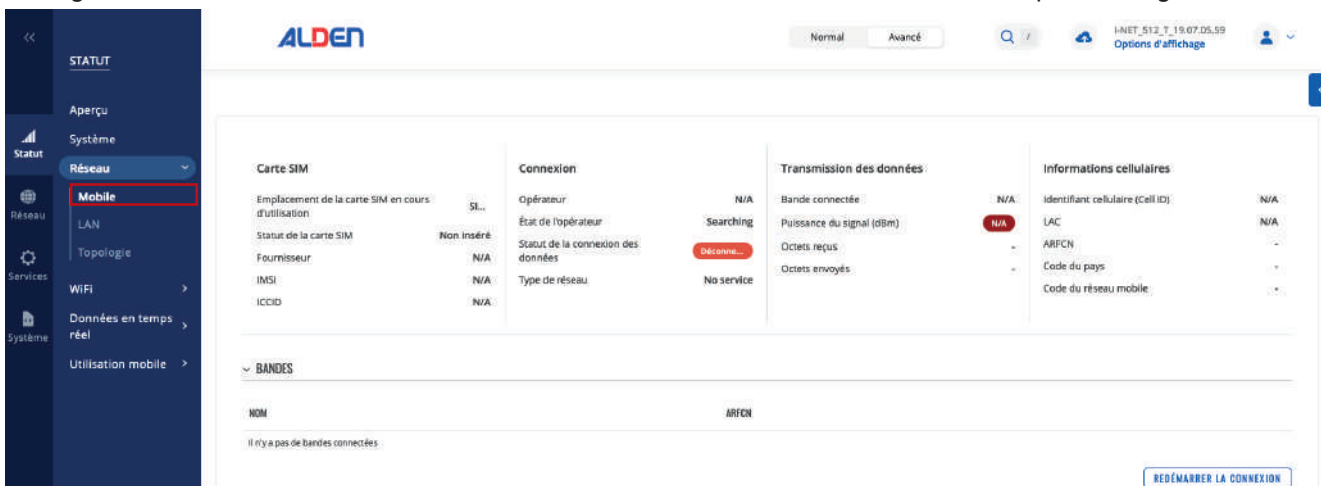
Champ	Description
Nom de l'appareil	Le nom de cet appareil : I-NET_512
Code produit	Alias, code de commande ; affiche sous quel code produit l'appareil a été fabriqué.
Version du Bootloader	Version du chargeur de démarrage actuellement utilisée par l'appareil. Un Bootloader est un programme qui charge 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.

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 LAN			
NOM	ADRESSE IP	MASQUE DE SOUS-RÉSEAU	
lan	192.168.2.1	255.255.255.0	
BAUX DHCP			
NOM D'HÔTE	ADRESSE IP	ADRESSE MAC	DURÉE D'ALLOCATION RESTANTE
ProdeConlicon	192.168.2.129	20:3C:9E:07:40:0A	09:37:09

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.

▼ TOPOLOGIE

▼ TOUS LES DISPOSITIFS ACTIFS

Dispositifs par page: 10 ▼

Search...

NOM D'HÔTE (FOURNISSEUR)	ADRESSE IP	ADRESSE MAC	TYPE	INTERFACE
Il n'y a pas de dispositifs				

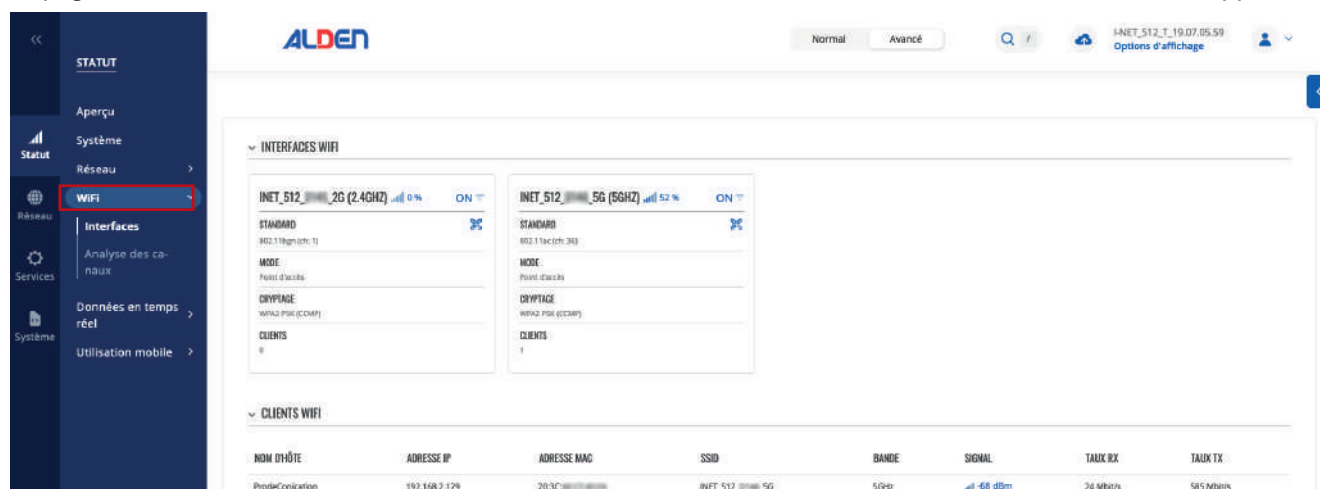
Champ	description
Nom d'hôte (fournisseur)	Nom d'hôte de l'appareil analysé
Adresse IP	Adresse IP de l'appareil analysé
Adresse Mac	Adresse MAC de l'appareil analysé
Type	Le type de connexion
Interface	L'interface à laquelle l'appareil scanné est connecté

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

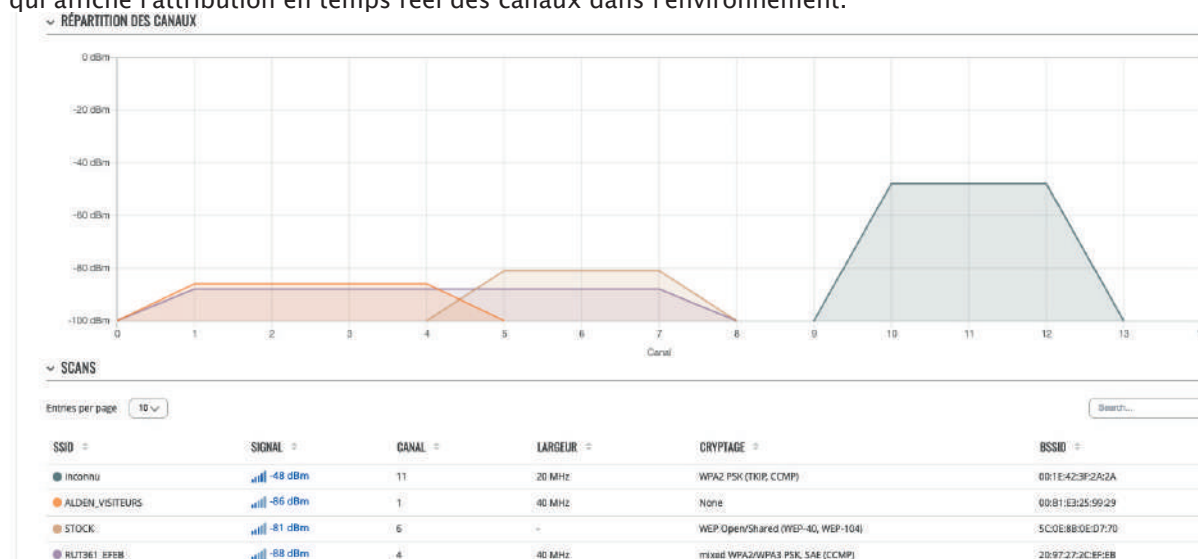
La page Interfaces affiche des informations sur toutes les interfaces sans fil et les clients connectés à l'appareil.



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.

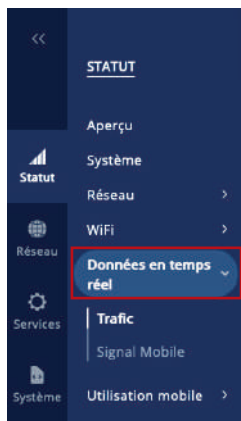
1.4.2 Menu STATUT > WIFI > ANALYSE DES CANAUX

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



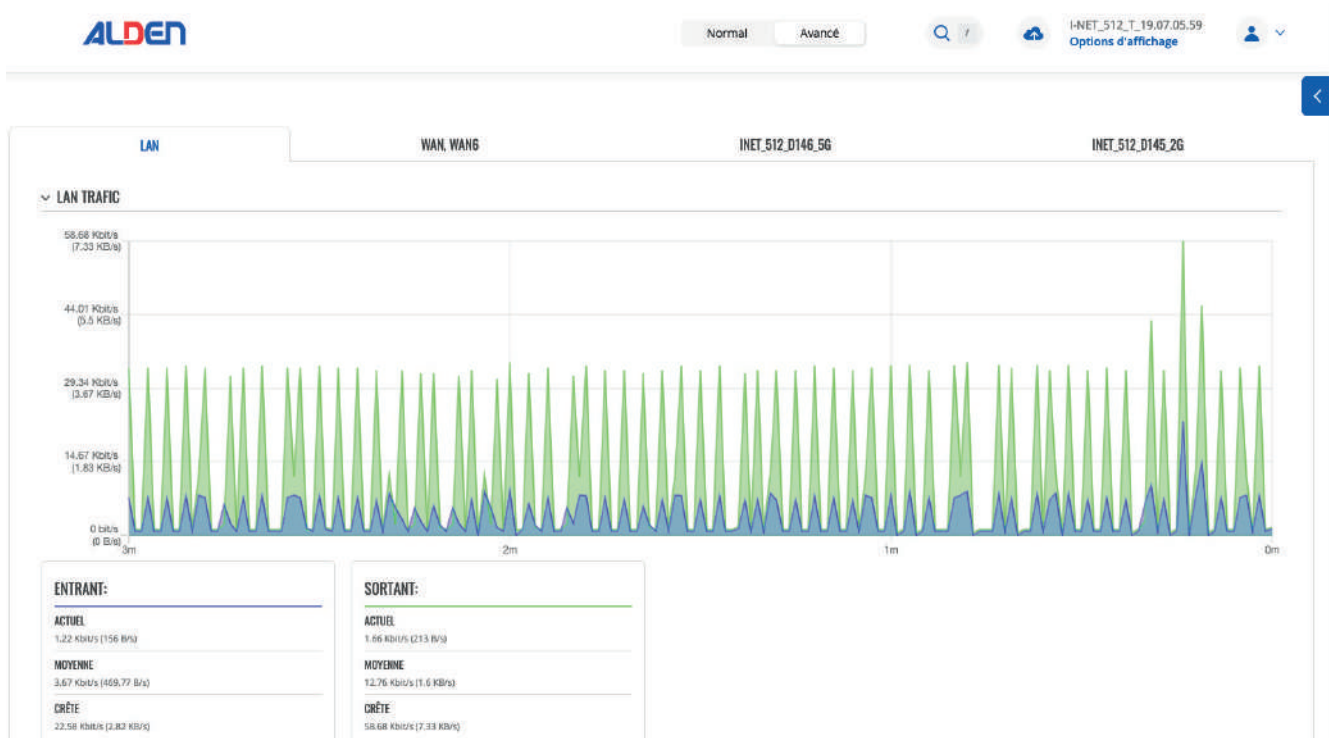
La page Données en temps réel contient divers graphiques qui affichent divers changements de données statistiques en temps réel.

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.

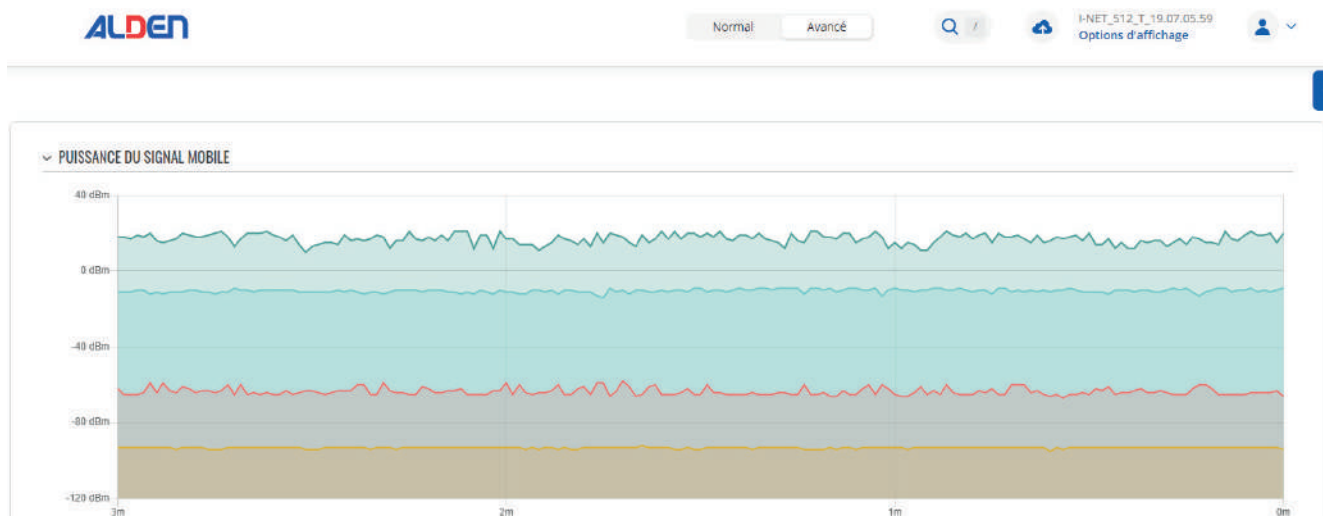
Graphique	Description
I-NET_512_XXXX_5G	Affiche le trafic qui passe par la connexion wifi 5G sous forme de graphique
I-NET_512_XXXX_2G	Affiche le trafic qui passe par la connexion wifi 2G sous forme de graphique
LAN	Affiche le trafic qui passe par la ou les interfaces réseau LAN sous forme de graphique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

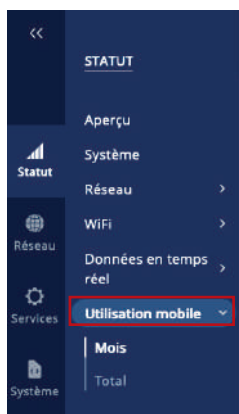


1.5.2 Menu STATUT > DONNÉES EN TEMPS RÉEL > SIGNAL MOBILE

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



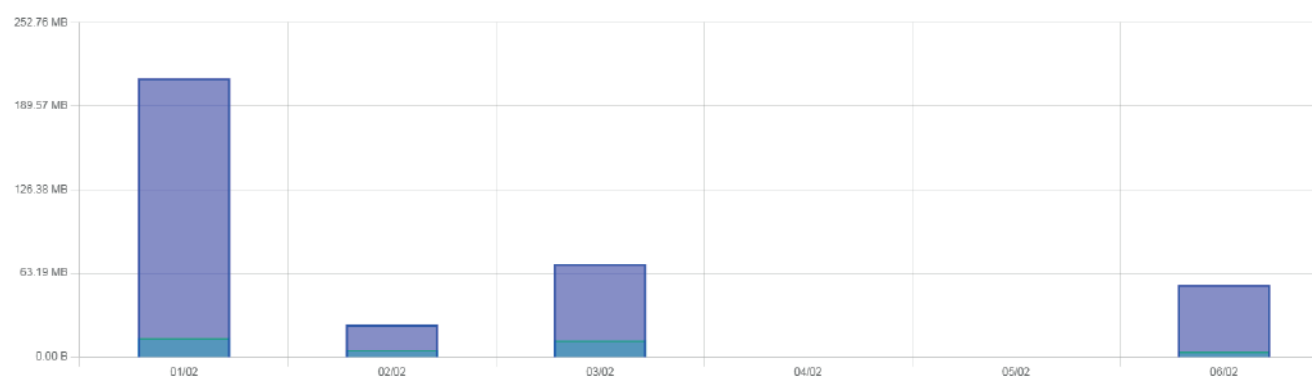
La page Utilisation mobile contient des graphiques qui affichent les valeurs d'utilisation des données mobiles sur différentes périodes et selon la carte SIM.

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

UTILISATION MOBILE



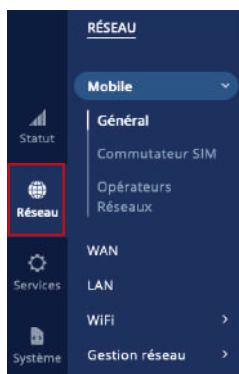
Utilisation du mois en cours *: 396.35 MB

Envoyé *: 36.59 MB

Reçu *: 359.76 MB

La comptabilité de l'utilisation des données de votre opérateur peut différer, l'entreprise ALDEN n'est pas responsable en cas de divergence de comptabilité.

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

~ PARAMÈTRES DE LA CARTE SIM
SIM1
SIM2

SIM par défaut ☒ on

Refuser l'itinérance des données ☐ off

VoLTE

Type de réseau

PIN

Sélection de la bande

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.

RECONNEXION SUR SIGNAL FAIBLE

Activer ☒

Seuil de réinitialisation -100

Délai de réinitialisation 600

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).

PARAMÈTRES DE L'OPÉRATEUR

Activer ☒

Mode Liste blanche

Liste des opérateurs Aucun opérateur disponible

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.

PARAMÈTRES DE LA LIMITE DE SMS

Activer la limite de SMS ☒

Nombre limite de SMS

Période Jour

Heure de début 0

SMS envoyés / limite de SMS 0 / 0

EFFACER LA LIMITE DE SMS

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.

▼ USSD

USSD:

Message de réponse:

Pas encore de réponse

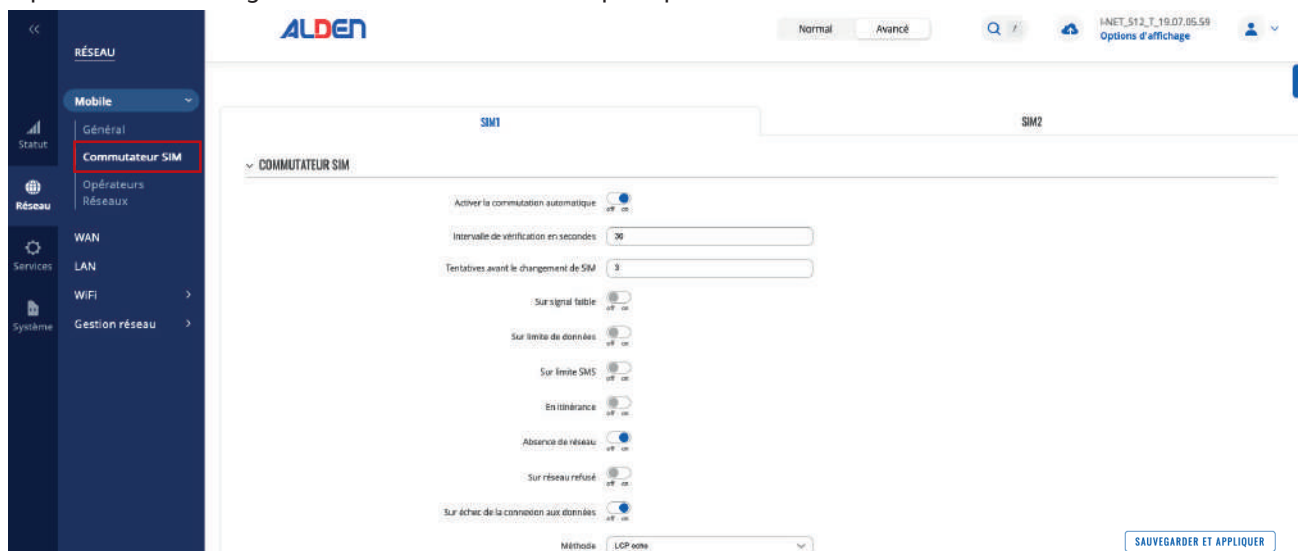
*La réception d'une réponse USSD peut prendre jusqu'à une minute.

ENVOYER

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 ».

✓ OPÉRATEURS DISPONIBLES

STATUT	NOM DE L'OPÉRATEUR	ABBREVIATION	NOM NUMÉRIQUE	TYPE D'ACCÈS RÉSEAU
Disponible	F SFR	SFR	20810	3G/4G
Interdit	Free	Free	20815	3G/4G
Interdit	Orange F	Orange	20801	3G/4G
Interdit	208 16	208 16	20816	4G
Interdit	F-Bouygues Telecom	BYTEL	20820	3G/4G

SAUVEGARDER ET APPLIQUER

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).

OPÉRATEURS RÉSEAUX

LISTES OPÉRATEURS

✓ GESTION DES LISTES D'OPÉRATEURS

NOM

CODES

Exemple

246

✎ ✕

✓ AJOUTER UNE NOUVELLE INSTANCE

NOM

AJOUTER

SAUVEGARDER ET APPLIQUER

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.

✓ MODIFIER LA LISTE DES OPÉRATEURS : EXEMPLE

Code opérateur

246

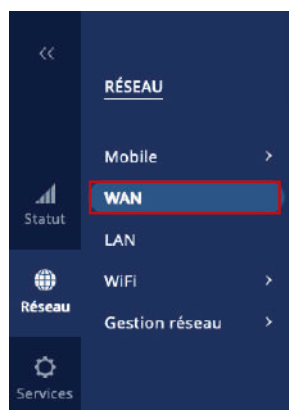
−

00000

− +

SAUVEGARDER ET APPLIQUER

2.2 Menu Réseau > WAN (Mode Avancé)



Certaines caractéristiques ne sont disponibles qu'en mode "Avancé."



Interfaces WAN

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

INTERFACES WAN					
1	wan	Statut: Inactif Type: Câblé	IP: - Protocole: dhcp MAC: 00:00:00:00:00:00	Durée de fonctionnement: - TX: 0 B RX: 0 B	Activer: ☐ Gestion: ☐
2	wan6	Statut: Inactif Type: Câblé	IP: - Protocole: dhcpv6 MAC: 00:00:00:00:00:00	Durée de fonctionnement: - TX: 0 B RX: 0 B	Activer: ☐
3	SIM1	Statut: Inactif Type: Mobile	IP: - APN: Auto SIM: 1	Durée de fonctionnement: - TX: 0 B RX: 0 B	Activer: ☐ Gestion: ☐
4	SIM2	Statut: Inactif Type: Mobile	IP: - APN: Auto SIM: 2	Durée de fonctionnement: - TX: 0 B RX: 0 B	Activer: ☐ Gestion: ☐

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".

▼ AJOUTER UNE NOUVELLE INSTANCE

NOM DE L'INTERFACE

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 :

1	wan	Statut: Inactif Type: Câblé	IP: - Protocole: dhcp MAC: 00:00:00:00:00:00	Durée de fonctionnement: - TX: 0 B RX: 0 B	 	Activer: ☐ Gestion: ☐
---	-----	--------------------------------	--	--	---	--

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.

INTERFACES : WAN

PARAMÈTRES GÉNÉRAUX
PARAMÈTRES AVANCÉS
PARAMÈTRES PHYSIQUES
PARAMÈTRES DU PARE-FEU

Activer ☒

Protocole DHCP

Nom d'hôte à envoyer lors d'une demande DHCP StarLcom

SAUVEGARDER ET APPLIQUER

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.

INTERFACES : WAN

PARAMÈTRES GÉNÉRAUX
PARAMÈTRES IPV6
PARAMÈTRES AVANCÉS
PARAMÈTRES PHYSIQUES
PARAMÈTRES DU PARE-FEU

Activer ☒

Protocole DHCPv6

SAUVEGARDER ET APPLIQUER

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.

INTERFACES : WAN

PARAMÈTRES GÉNÉRAUX
PARAMÈTRES IPV6
PARAMÈTRES AVANCÉS
PARAMÈTRES PHYSIQUES
PARAMÈTRES DU PARE-FEU

Activer ☒

Protocole PPPoE

Nom d'utilisateur PAP/CHAP

Mot de passe PAP/CHAP

Concentrateur d'accès auto

Nom du service auto

SAUVEGARDER ET APPLIQUER

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

INTERFACES : WAN

PARAMÈTRES GÉNÉRAUX
PARAMÈTRES AVANCÉS
PARAMÈTRES DU PARE-FEU

Activer ☒

Protocole Mobile

Mode NAT

Type de PDP IPv4

SIM SIM1

APN automatique ☒

APN -- Personnalisé --

APN personnalisé

Type d'authentification Aucun

LIMITE DE DONNÉES MOBILES

Activer la limitation de la connexion de données ☐

SUPPRIMER LES DONNÉES COLLECTÉES

SAUVEGARDER ET APPLIQUER

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)

INTERFACES : WAN

PARAMÈTRES GÉNÉRAUX
PARAMÈTRES AVANCÉS
PARAMÈTRES DU PARE-FEU

Activer ☒
Protocole Mobile
Mode Bridge (Pont)

L'utilisation du mode Bridge ou Passthrough désactivera la plupart des capacités de l'appareil et vous ne pourrez accéder aux paramètres de votre appareil que par le biais de son adresse IP statique !

Sélection de sous-réseau Auto
Type de PDP IPv4
SIM SIM1
APN automatique ☒
APN -- Personnalisé --
APN personnalisé apn
Type d'authentification Aucun
Adresse MAC 00:11:22:33:44:55

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)

INTERFACES : WAN

PARAMÈTRES GÉNÉRAUX
PARAMÈTRES AVANCÉS
PARAMÈTRES DU PARE-FEU

Activer ☒

Protocole Mobile

Mode Passthrough (Traversant)

L'utilisation du mode Bridge ou Passthrough désactivera la plupart des capacités de l'appareil et vous ne pourrez accéder aux paramètres de votre appareil que par le biais de son adresse IP statique !

Sélection de sous-réseau Auto

Type de PDP IPv4

SIM SIM1

APN automatique ☒

APN -- Personnalisé --

APN personnalisé apn

Type d'authentification Aucun

Désactiver DHCP ☒

Durée du bail 12 Heures

Adresse MAC 00:11:22:33:44:55

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.

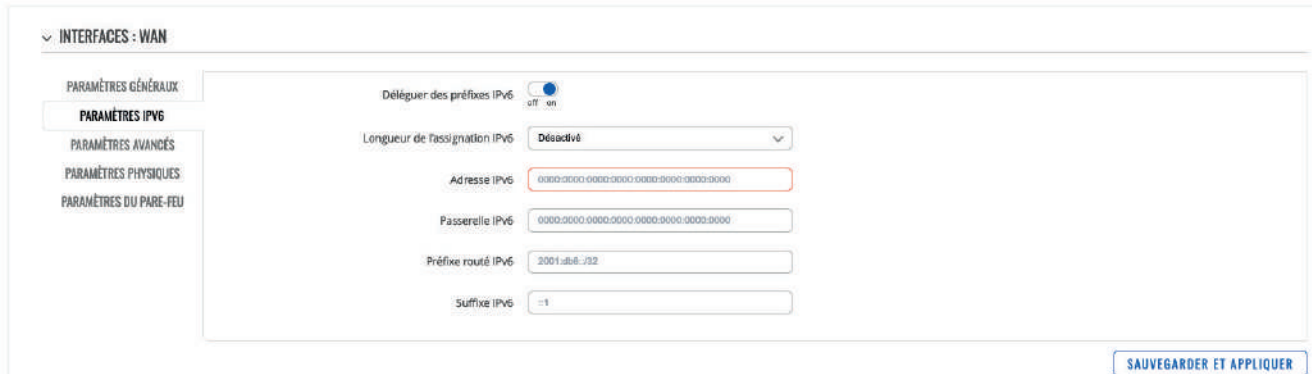
APN personnalisé	Par défaut : aucun	Un nom de point d'accès (APN) est une passerelle entre un réseau mobile GSM, GPRS, 3G ou 4G et un autre réseau informatique. Selon le contrat, certains opérateurs peuvent exiger que vous utilisiez un APN juste pour terminer l'enregistrement sur un réseau. Dans d'autres 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.

INTERFACES : WAN

PARAMÈTRES GÉNÉRAUX

PARAMÈTRES IPv6

PARAMÈTRES AVANCÉS

PARAMÈTRES PHYSIQUES

PARAMÈTRES DU PARE-FEU

Déléguer des préfixes IPv6: ☒ Off ☐ On

Demande d'adresse IPv6:

Demande de préfixe de taille IPv6:

SAUVEGARDER ET APPLIQUER

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.

INTERFACES : WAN

PARAMÈTRES GÉNÉRAUX

PARAMÈTRES IPv6

PARAMÈTRES AVANCÉS

PARAMÈTRES PHYSIQUES

PARAMÈTRES DU PARE-FEU

Déléguer des préfixes IPv6: ☒ Off ☐ On

Obtenir une adresse IPv6:

SAUVEGARDER ET APPLIQUER

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.

INTERFACES : WAN

PARAMÈTRES GÉNÉRAUX
PARAMÈTRES IPV6
PARAMÈTRES AVANCÉS
PARAMÈTRES PHYSIQUES
PARAMÈTRES DU PARE-FEU

Forcer le lien: ☒ off ☐ on
Passerelle métrique:
Remplacer l'adresse MAC:
Remplacer MTU:
Table IPv4:

SAUVEGARDER ET APPLIQUER

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.

INTERFACES : WAN

PARAMÈTRES GÉNÉRAUX

PARAMÈTRES AVANCÉS

PARAMÈTRES PHYSIQUES

PARAMÈTRES DU PARE-FEU

Forcer le lien ☐ Off ☐ On

Utiliser le flag de diffusion ☐ Off ☐ On

Utiliser la passerelle par défaut ☐ Off ☒ On

Passerelle métrique

Serveurs DNS personnalisés

ID client à envoyer lors d'une requête DHCP

Classe de fournisseur à envoyer lors d'une demande de DHCP

Remplacer l'adresse MAC

Remplacer MTU

Table IPv4

SAUVEGARDER ET APPLIQUER

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.

INTERFACES : WAN

PARAMÈTRES GÉNÉRAUX
PARAMÈTRES IPV6
PARAMÈTRES AVANCÉS
PARAMÈTRES PHYSIQUES
PARAMÈTRES DU PARE-FEU

Forcer le lien ☐

Utiliser la passerelle par défaut ☒

Passerelle métrique

Serveurs DNS personnalisés

ID client à envoyer lors d'une requête DHCP

Remplacer l'adresse MAC

Remplacer MTU

Table IPv6

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 IPv6	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.

✓ INTERFACES : WAN

PARAMÈTRES GÉNÉRAUX
PARAMÈTRES IPV6
PARAMÈTRES AVANCÉS
PARAMÈTRES PHYSIQUES
PARAMÈTRES DU PARE-FEU

Forcer le lien ☐ off ☒ on

Utiliser la passerelle par défaut ☐ off ☒ on

Passerelle métrique

Serveurs DNS personnalisés

Valeur tag VLAN

Priorité VLAN

Seuil d'échec de l'écho LCP

Intervalle d'écho LCP

Contenu de la balise Host-Uniq

Délais d'inactivité

Remplacer MTU

Table IP4

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.

INTERFACES : WAN

PARAMÈTRES GÉNÉRAUX
PARAMÈTRES AVANCÉS
PARAMÈTRES DU PARE-FEU

Forcer le lien ☐ off ☒ on
Passerelle métrique:
Serveurs DNS personnalisés: +
Remplacer MTU:
Table IPv4:

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.

LIMITE DE DONNÉES MOBILES

Activer la limitation de la connexion de données ☐ off ☒ on
Limite de données (MB)
Période
Heure de début
Activer l'avertissement SMS ☐ off ☒ on
Limite de données (MB)
Numéro de téléphone
La limite de données est dépassée : -
[SUPPRIMER LES DONNÉES COLLECTÉES](#)

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).

INTERFACES : WAN

PARAMÈTRES GÉNÉRAUX

PARAMÈTRES IPV6

PARAMÈTRES AVANCÉS

PARAMÈTRES PHYSIQUES

PARAMÈTRES DU PARE-FEU

Interfaces bridge (pont) ☒

Activer STP ☐

Activer IGMP ☐

Interface

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.

INTERFACES : WAN

PARAMÈTRES GÉNÉRAUX

PARAMÈTRES IPV6

PARAMÈTRES AVANCÉS

PARAMÈTRES PHYSIQUES

PARAMÈTRES DU PARE-FEU

Créer / Attribuer une zone de pare-feu

wan

wan0

SIM1

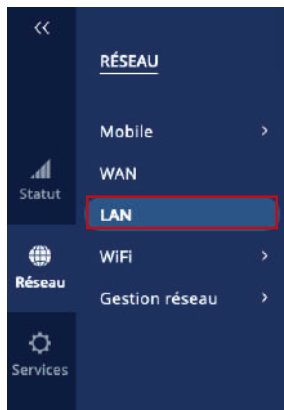
SIM2

Exemple

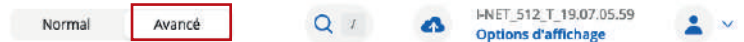
SAUVEGARDER ET APPLIQUER

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".

INTERFACES LAN

1 lan	Statut: Actif Type: Bridge (Pont)	IP: 192.168.2.1/24 Protocole: static MAC: 88:77:42:63:00:00	Durée de fonctionnement: 5h 22m 51s TX: 6.3 MB RX: 2.63 MB	 	
---------	--------------------------------------	---	--	---	---

AJOUTER UNE NOUVELLE INSTANCE

NOM DE L'INTERFACE

AJOUTER

SAUVEGARDER ET APPLIQUER

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

INTERFACES LAN

1 lan	Statut: Actif Type: Bridge (Pont)	IP: 192.168.2.1/24 Protocole: static MAC: 88:77:42:63:00:00	Durée de fonctionnement: 5h 22m 51s TX: 6.3 MB RX: 2.63 MB	 	
---------	--------------------------------------	---	--	---	---

Paramètres généraux

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

INTERFACES : LAN

PARAMÈTRES GÉNÉRAUX

PARAMÈTRES IPV6

PARAMÈTRES AVANCÉS

PARAMÈTRES PHYSIQUES

PARAMÈTRES DU PARE-FEU

Activer 

Protocole Statique

Adresse IPV4 192.168.2.1

Masque de sous-réseau IPV4 255.255.255.0

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.

INTERFACES : LAN

PARAMÈTRES GÉNÉRAUX

PARAMÈTRES IPV6

PARAMÈTRES AVANCÉS

PARAMÈTRES PHYSIQUES

PARAMÈTRES DU PARE-FEU

Déléguer des préfixes IPV6 ☒

Longueur de l'assignation IPV6

Indice d'affectation IPV6

Suffixe IPV6

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 déléguant, 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.

INTERFACES : LAN

PARAMÈTRES GÉNÉRAUX

PARAMÈTRES IPV6

PARAMÈTRES AVANCÉS

PARAMÈTRES PHYSIQUES

PARAMÈTRES DU PARE-FEU

Forcer le lien ☒

Passerelle métrique

Remplacer l'adresse MAC

Remplacer MTU

Table IP4

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.

INTERFACES : LAN

PARAMÈTRES GÉNÉRAUX
PARAMÈTRES IPV6
PARAMÈTRES AVANCÉS
PARAMÈTRES PHYSIQUES
PARAMÈTRES DU PARE-FEU

Interfaces bridge (pont) ☒

Activer STP ☐

Activer IGMP ☐

Interface

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.

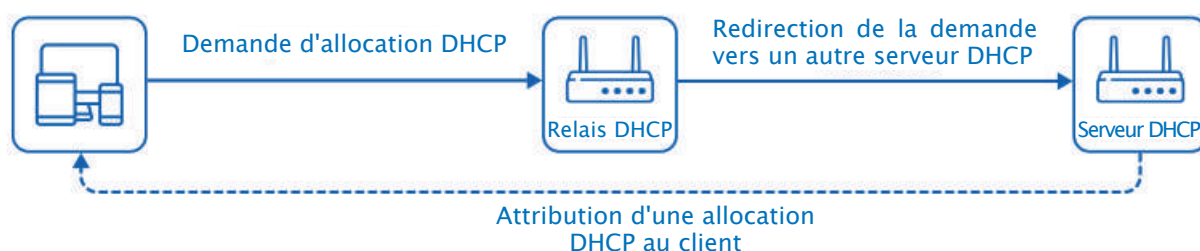
INTERFACES : LAN

PARAMÈTRES GÉNÉRAUX
PARAMÈTRES IPV6
PARAMÈTRES AVANCÉS
PARAMÈTRES PHYSIQUES
PARAMÈTRES DU PARE-FEU

Créer / Attribuer une zone de pare-feu

Champ	Valeur	Description
Créer/attribuer une zone de pare-feu	Non spécifié 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.

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.

✓ SERVEUR DHCP

CONFIGURATION GÉNÉRALE

PARAMÈTRES AVANCÉS

PARAMÈTRES IPV6

DHCP dynamique ☒

Forcer ☐

Masque de sous-réseau-IPv4

Options DHCP personnalisées [EDITER](#)

Forcer les options DHCP ☐

SAUVEGARDER ET APPLIQUER

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.

Interfaces : lan / Options DHCP

Options DHCP

CODE D'OPTION

Délaiage temporel (2)

VALEUR DE L'OPTION

AJOUTER

SAUVEGARDER

Champ	Valeur	Description
Code des options	Personnalisé Délaiage temporel (2) Routeur (3) DNS (6) Champs(15) serveur NTP (42); Par défaut : Délaiage temporel (2)	Code d'option DHCP standardisé.
Valeur d'option	Personnalisé Délaiage 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.

✓ SERVEUR DHCP

CONFIGURATION GÉNÉRALE

PARAMÈTRES AVANCÉS

PARAMÈTRES IPV6

Annonce routeur-Service: Désactivé

Service DHCPv6: Désactivé

NDP-Proxy: Désactivé

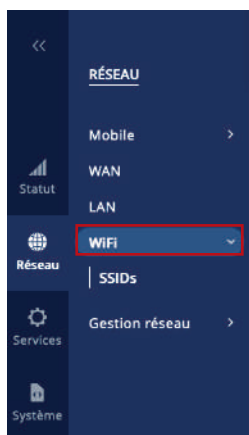
Serveurs DNS annoncés

Domaines DNS annoncés

SAUVEGARDER ET APPLIQUER

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.

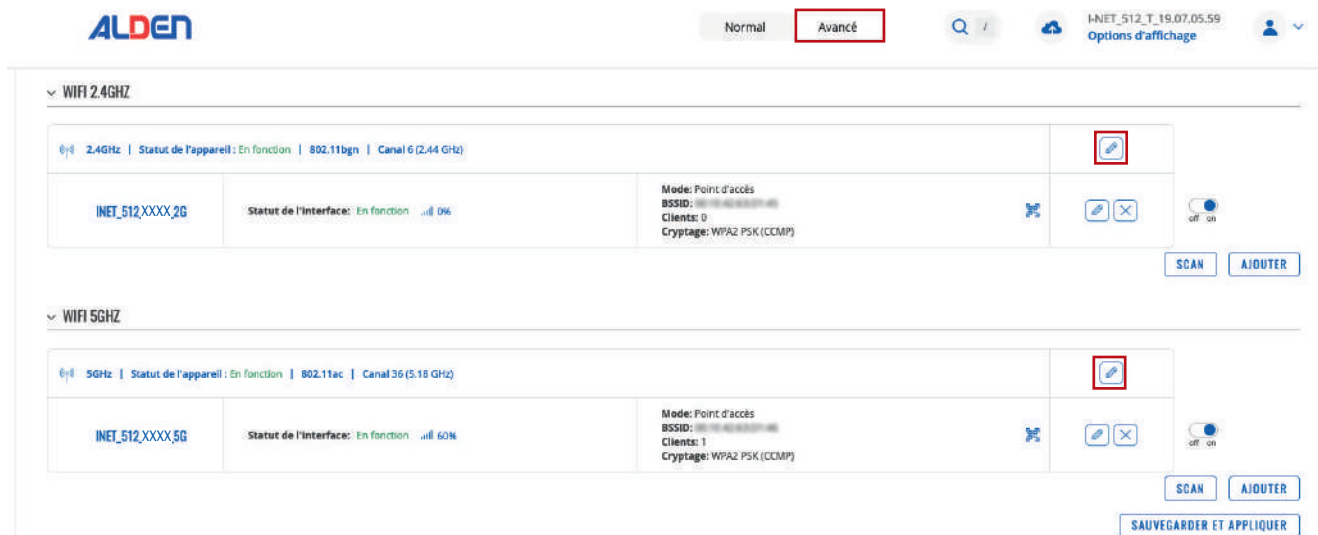
Si vous rencontrez des difficultés pour trouver cette page ou certains des paramètres décrits ici sur l'interface Web de votre appareil, vous devez activer le mode «Avancé». Vous pouvez le faire en cliquant sur le bouton "Normal" sous "Mode", qui se trouve en haut de l'interface Web.

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.

PARAMÈTRES GÉNÉRAUX 2.4GHZ

CONFIGURATION GÉNÉRALE

PARAMÈTRES AVANCÉS

SCANNER WIFI

Activer ☒

Fréquence de fonctionnement

Mode

Canal

Largeur

N

Auto

20 MHz

Puissance d'émission

100%

Code du pays

US - United States

SAUVEGARDER ET APPLIQUER

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 :

WIFI 2.4GHZ

Fréq.	Statut de l'appareil	Mode	Actions
2.4GHz	En fonction	802.11bgn	Canal 6 (2.44 GHz)
INET_512_2G	Statut de l'interface: En fonction 0%	Mode: Point d'accès BSSID: [redacted] Clients: 0 Cryptage: WPA2 PSK (CCMP)	[Modifier] [Supprimer]

WIFI 5GHZ

Fréq.	Statut de l'appareil	Mode	Actions
5GHz	En fonction	802.11ac	Canal 36 (5.18 GHz)
INET_512_5G	Statut de l'interface: En fonction 60%	Mode: Point d'accès BSSID: [redacted] Clients: 1 Cryptage: WPA2 PSK (CCMP)	[Modifier] [Supprimer]

SCAN AJOUTER

SAUVEGARDER ET APPLIQUER

Configuration générale

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

CONFIGURATION DE L'INTERFACE

CONFIGURATION GÉNÉRALE

PARAMÈTRES AVANCÉS

SÉCURITÉ WIFI

FILTRE MAC

Activer ☒

Mode: Point d'accès

ESSID: [redacted]

Mot de passe: [redacted]

Réseau: lan

Cacher l'ESSID ☒

802.11r Transition rapide ☐

SAUVEGARDER ET APPLIQUER

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

INET_512_2G CONFIGURATION DE L'INTERFACE

CONFIGURATION GÉNÉRALE

PARAMÈTRES AVANCÉS

SÉCURITÉ WIFI

FILTRE MAC

Isoler les clients

Court préambule

Intervalle DTIM

Intervalle de temps pour la recombinaison des clés GTK

Désactiver le pooling d'inactivité

Limite d'inactivité de la station

Intervalle d'écoute maximal autorisé

Dissociation en cas d'acquiescement faible

WDS

Mode WMM

SAUVEGARDER ET APPLIQUER

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 recombinaison 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 désauthenticée.
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'acquiescement 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

✓ CONFIGURATION DE L'INTERFACE

CONFIGURATION GÉNÉRALE

PARAMÈTRES AVANCÉS

SÉCURITÉ WIFI

Court préambule ☒

Intervalle DTIM

Intervalle de temps pour la recombinaison des clés GTK

Désactiver le pooling d'inactivité ☐

Limite d'inactivité de la station

Intervalle d'écoute maximal autorisé

Dissociation en cas d'acquiescement faible ☒

WDS ☐

Activer l'itinérance rapide ☐

Redirection du portail captif ☒

SAUVEGARDER ET APPLIQUER

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 recombinaison 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 désauthenticée.
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'acquiescement 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

CONFIGURATION DE L'INTERFACE

CONFIGURATION GÉNÉRALE

PARAMÈTRES AVANCÉS

SÉCURITÉ WIFI

Rediriger le trafic des pairs en maillage

Seuil RSSI pour joindre

Court préambule

Intervalle DTIM

Intervalle de temps pour la recombinaison des clés GTK

Désactiver le pooling d'inactivité

Limite d'inactivité de la station

Intervalle d'écoute maximal autorisé

Dissociation en cas d'acquiescement faible

WDS

SAUVEGARDER ET APPLIQUER

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 recombinaison 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 désauthenticée.
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'acquiescement 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

INET_512_XXXX_2G CONFIGURATION DE L'INTERFACE

CONFIGURATION GÉNÉRALE	Cryptage	WPA2-PSK
PARAMÈTRES AVANCÉS	Chiffrer	Auto
SÉCURITÉ WIFI	Mot de passe	*****
FILTRE MAC		

SAUVEGARDER ET APPLIQUER

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

INET_512_XXXX_2G CONFIGURATION DE L'INTERFACE

CONFIGURATION GÉNÉRALE	Filtre d'adresses MAC	Désactiver
PARAMÈTRES AVANCÉS		
SÉCURITÉ WIFI		
FILTRE MAC		

SAUVEGARDER ET APPLIQUER

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.

✓ RÉSULTATS DU SCAN WIFI

Signal	SSID	Canal	Mode	BSSID	Cryptage	
44 %		11	Master	88:7E:42:3F:2A:2A	WPA2 PSK (TKIP, CCMP)	REJOINDRE LE RÉSEAU

[RÉPÉTEZ LE SCAN](#)

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)

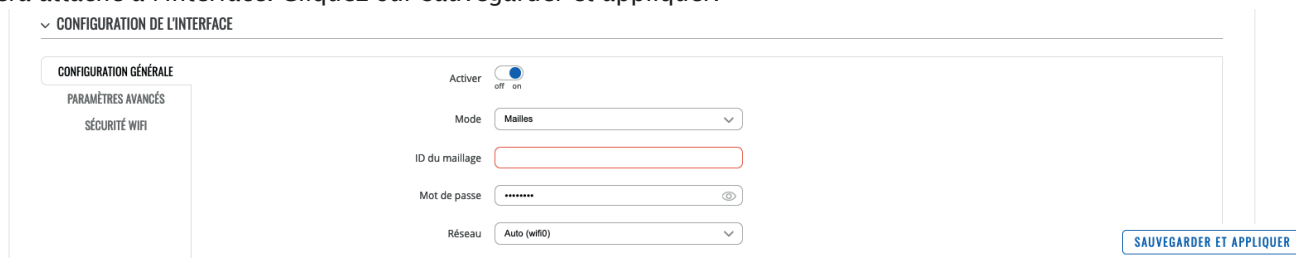
I-NET 512 peut également être configuré comme une passerelle maillée ou comme un nœud (routeur) se connectant à une passerelle maillée.

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.

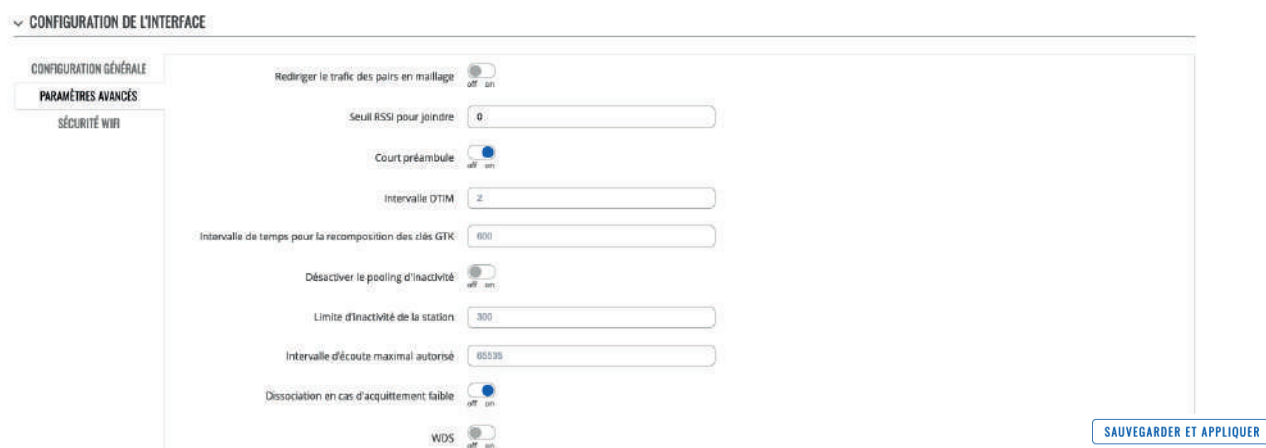
Lors de la configuration de I-NET 512 en tant que passerelle maillée, une connectivité Internet est requise. Pour commencer, cliquez sur le bouton "Ajouter"



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.

INTERFACES WAN

1 wan	Statut: Inactif Type: Câblé	IP: - Protocole: dhcp MAC: 88:88:88:88:88:88	Durée de fonctionnement: - TX: 0 B RX: 0 B	 	Activer: ☒ Gestion: ☒
-------	---	--	--	---	--

3. Changez le protocole en DHCP.

INTERFACES : WAN

PARAMÈTRES GÉNÉRAUX

PARAMÈTRES AVANCÉS

PARAMÈTRES PHYSIQUES

PARAMÈTRES DU PARE-FEU

Activer: ☒

Protocole: DHCP

Nom d'hôte à envoyer lors d'une demande DHCP: Start.com

SAUVEGARDER ET APPLIQUER

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.

2.4GHz Statut de l'appareil: En fonction 802.11bgn Canal: 4 (GHz)		
INET_512_2G	Statut de l'interface: En fonction 0%	Mode: Point d'accès BSSID: 88:88:88:88:88:88 Clients: 0 Cryptage: WPA2 PSK (CCMP)
		SCAN AJOUTER

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 être utilisée lorsque l'on souhaite créer un répéteur Wi-Fi entre son ordinateur n'importe quel réseau Wi-Fi renseigné dans la liste de la fonction "Multi 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.

CONFIGURATION DE L'INTERFACE

CONFIGURATION GÉNÉRALE

PARAMÈTRES AVANCÉS

Activer ☐

Mode

Réseau

Temps de balayage (sec)

Charger la liste des AP ou glisser-déposer votre fichier ici

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 auxquels 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.

POINTS D'ACCÈS

SSID

MOT DE PASSE

☐

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

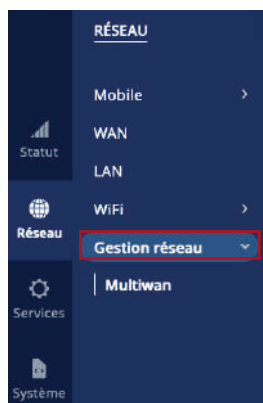
NOTE : pour supprimer une interface "Multi AP" dans le menu WIFI, basculer en mode "Avancé" et cliquer sur le bouton avec la croix correspondant.

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.

Gestion réseau

	MÉTRIQUE	NOM	TYPE	INTERVALLE	STATUT		
+	1	wan	wired	3	Hors ligne	off on	
+	3	SIM1	mobile	3	Hors ligne	off on	
+	4	SIM2	mobile	3	Hors ligne	off on	

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.

GESTION RÉSEAU / RÉPARTITION DES DONNÉES

Gestion réseau

	MÉTRIQUE	NOM	TYPE	INTERVALLE	STATUT	
	1	wan	wired	3	Hors ligne	off on

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

▼ CONFIGURATION DE L'INTERFACE

Activer ☒ off on

Intervalle

Connexions affleurantes

▼ RÉGLE

Méthode

Famille d'adresses

Track IP

Fiabilité

Nombre

Actif

Inactif

SAUVEGARDER ET APPLIQUER

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 :

Important: Pour une transition plus facile entre les interfaces réseau, il est recommandé de toutes les activer en basculant les boutons "Off/On" sur "On" et de cliquer sur le bouton "SAUVEGARDER ET APPLIQUER".

Attention : Bien que faible, cette opération entraîne une consommation de données sur votre carte sim (si insérée).

▼ GESTION RÉSEAU / RÉPARTITION DES DONNÉES

MÉTRIQUE	NOM	TYPE	INTERVALLE	STATUT	
1	wan	wired	3	Hors ligne	☐ off ☒ on
3	SIM1	mobile	3	Hors ligne	☐ off ☒ on
4	SIM2	mobile	3	Hors ligne	☐ off ☒ on

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

▼ GESTION RÉSEAU / RÉPARTITION DES DONNÉES

GROUPES	NOM	TYPE	INTERVALLE	STATUT	RATIO
1	wan	wired	3	Hors ligne	☐ off ☒ on 1
1	SIM1	mobile	3	Hors ligne	☐ off ☒ on 1

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 :

▼ RÈGLES

PRIORITÉ	NOM	ADRESSE SOURCE	PORT SOURCE	ADRESSE DE DESTINATION	PORT DE DESTINATION	PROTOCOLE	POLITIQUE D'UTILISATION
1	default_rule	-	-	0.0.0.0/0	-	-	Par défaut (Gestion réseau)

✎ ✕

▼ CONFIGURATION DES RÈGLES

Protocole :

Adresse Source : +

Adresse de destination : +

Épinglé : ☐ Off ☐ On

Politique assignée :

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.

▼ POLITIQUE

NOM	MODE	SOURCE UTILISÉE
default	Gestion réseau	wan - SIM1 - SIM2 +
default	Répartition des données	wan - SIM1 - SIM2 +

✕ ✕

▼ AJOUTER UNE NOUVELLE INSTANCE

NOM DE LA POLITIQUE :

MODE DE POLITIQUE :

AJOUTER

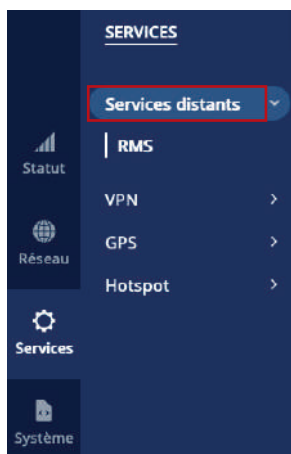
SAUVEGARDER ET APPLIQUER

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 :

✓ PARAMÈTRES RMS

Type de connexion:

Port:

✓ STATUT

Statut de gestion: Activé

État de la connexion: Échec (Échec de réglage du nom d'hôte)

N° de série: 6000224180

LAN MAC: 88-1E-4D-83-87-4B

Connexion suivante après: 00:00:09

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 :

✓ STATUT

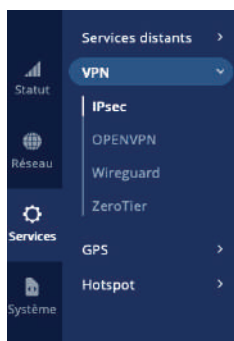
Statut de gestion: Activé

État de la connexion: Échec (Échec de réglage du nom d'hôte)

N° de série: 6000224180

LAN MAC: 88-1E-4D-83-87-4B

Connexion suivante après: 00:00:09



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 ».

▼ TUNNELS IPSEC

Il n'y a pas d'instances ipsec

▼ AJOUTER UNE NOUVELLE INSTANCE

NOM DE LA NOUVELLE CONFIGURATION

AJOUTER

SAUVEGARDER ET APPLIQUER

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.

▼ INSTANCE IPSEC : DEMO

Activer ☐

Endpoint distant:

Méthode d'authentification:

Clé pré-partagée:

Identifiant local:

Identifiant distant:

Secrets multiples ☐

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.

~ PARAMÈTRES GÉNÉRAUX SECRETS

SÉLECTEUR D'ID

TYPE

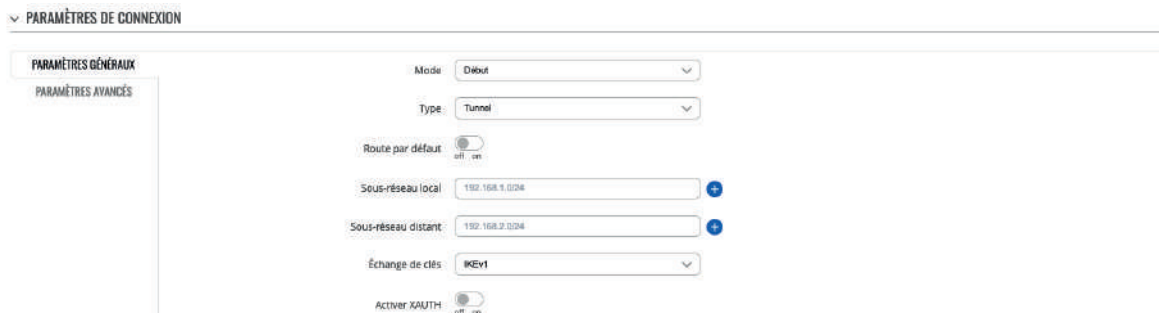
SECRET

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 Routeage ; 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 : Liez 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/I2f ».
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/I2f ».
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 Passth

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

PARAMÈTRES PROPOSÉS

PHASE 1

PHASE 2

Propositions

Cryptage

AES 128

Authentification

SHA1

Groupe DH

MODP1536

Forcer la proposition cryptographique

☐

off on

Durée de validité IKE

3h

SAUVEGARDER ET APPLIQUER

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.

PARAMÈTRES PRINCIPAUX : DEMO

Activer ☐

Activer la configuration d'OpenVPN à partir d'un fichier ☐

TUN/TAP

Protocole

Port

LZO

Authentification

Cryptage

Chiffrement TLS

Client à client ☐

Maintenir actif

Adresse IP du réseau virtuel

Masque de sous-réseau virtuel

Option Push

Autoriser les certificats en double ☐

Algorithme d'authentification

Authentification HMAC supplémentaire

Utiliser le format PKCS #12 ☐

Fichiers de certificat de l'appareil ☐

Autorité de certification ou glisser-déposer votre fichier...

Certificat du serveur ou glisser-déposer votre fichier...

Clé du serveur ou glisser-déposer votre fichier...

Paramètres Diffie-Hellman ou glisser-déposer votre fichier...

Fichier CRL (facultatif) ou glisser-déposer votre fichier...

CLIENTS TLS

NOM DU POINT DE TERMINAISON	NOM COMMUN (CN)	POINT D'ACCÈS LOCAL VIRTUEL	POINT D'EXTRÉMITÉ DISTANT VIRTUEL	RÉSEAU PRIVÉ	MASQUE DE SOUS-RÉSEAU PRIVÉ	RÉSEAU COUVERT
-----------------------------	-----------------	-----------------------------	-----------------------------------	--------------	-----------------------------	----------------

Cette section ne contient pas encore de valeurs

AJOUTER UNE NOUVELLE INSTANCE

NOM

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 clientes. 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 :

PARAMÈTRES PRINCIPAUX : DEMO

Activer ☐

Activer les services externes ☐

Activer la configuration d'OpenVPN à partir d'un fichier ☐

TUN/TAP

Protocole

Port

LZO

Authentification

Cryptage

Chiffrement TLS

Hôte/adresse IP distant

Tentatives de réglage

Maintenir actif

Adresse IP du réseau distant

Masque de sous-réseau distant

Algorithme d'authentification

Authentification HMAC supplémentaire

Utiliser le format PKCS #12 ☐

Options supplémentaires

Fichiers de certificat de l'appareil ☐

Autorité de certification ou glisser-déposer votre fichier...

Certificat client ou glisser-déposer votre fichier...

Clé client ou glisser-déposer votre fichier...

Ajouter le mot de passe de décryptage de la clé privée

SAUVEGARDER ET APPLIQUER

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.

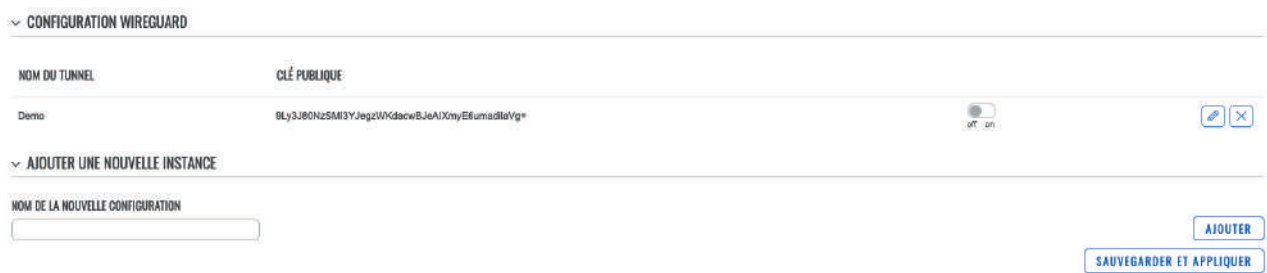
Certain champs de configuration deviennent disponibles uniquement lorsque certains autres paramètres sont sélectionnés. Les noms des paramètres sont suivis d'un préfixe qui spécifie le type d'authentification sous lequel ils deviennent visibles. Différents codes couleur sont utilisés pour différents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

✓ INTERFACE WIREGUARD : DEMO

CONFIGURATION GÉNÉRALE

PARAMÈTRES AVANCÉS

Métrique

0

Port d'écoute

51820

MTU

Serveurs DNS

+

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

NOM DU PAIR	DESCRIPTION	CLÉ PUBLIQUE
new		

+

✕

✓ AJOUTER UNE NOUVELLE INSTANCE

AJOUTER UNE NOUVELLE INSTANCE

AJOUTER

SAUVEGARDER ET APPLIQUER

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.

Pairs / Pair WireGuard new

PAIR WIREGUARD NEW

CONFIGURATION GÉNÉRALE

PARAMÈTRES AVANCÉS

Clé publique

Hôte du point de terminaison

vpn.example.com

IPs autorisés

+

Description

Mon pair

Routage des IPs autorisées

off on

RETOUR

SAUVEGARDER ET APPLIQUER

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.

Pairs / Pair WireGuard new

PAIR WIREGUARD NEW

CONFIGURATION GÉNÉRALE

PARAMÈTRES AVANCÉS

Clé pré-partagée

Port d'extrémité

Actif persistant

Table de routage

RETOUR

SAUVEGARDER ET APPLIQUER

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'.

~ CONFIGURATION ZEROTIER

NOM ZEROTIER

ID DU NŒUD D'INSTANCE

Cette section ne contient pas encore de valeurs

~ AJOUTER UNE NOUVELLE INSTANCE

NOM DE LA NOUVELLE CONFIGURATION

AJOUTER

SAUVEGARDER ET APPLIQUER

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

~ PARAMÈTRES DE L'INSTANCE : DEMO

Activer ☐

ID du nœud -

~ CONFIGURATION RÉSEAU

NOM DU RÉSEAU

ID RÉSEAU

PORT

Cette section ne contient pas encore de valeurs

~ AJOUTER UNE NOUVELLE INSTANCE

AJOUTER UN NOUVEAU RÉSEAU

Network name

AJOUTER

SAUVEGARDER ET APPLIQUER

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 :

Configuration réseau / Réseau ZeroTier : demo

✕

~ RÉSEAU ZEROTIER : DEMO

Activer ☐

Port 9993

ID réseau

Bridge (pont) vers Aucun

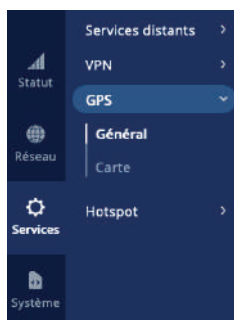
Autoriser le routage par défaut ☐Autoriser l'IP globale ☐Autoriser les IP gérées ☐Autoriser le DNS ☐

RETOUR

SAUVEGARDER ET APPLIQUER

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 hexadécimale.

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

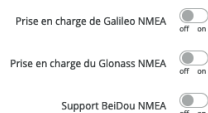
Le Général est utilisé pour activer le service GPS et la prise en charge de différents types de satellites. Une fois que vous avez activé le GPS, vous pouvez consulter la page Carte afin de voir si l'appareil a obtenu une position GPS. Il est très important de fixer l'antenne GPS sur l'appareil et de 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 :

CONFIGURATION DU GPS



CONFIGURATION SATELLITE

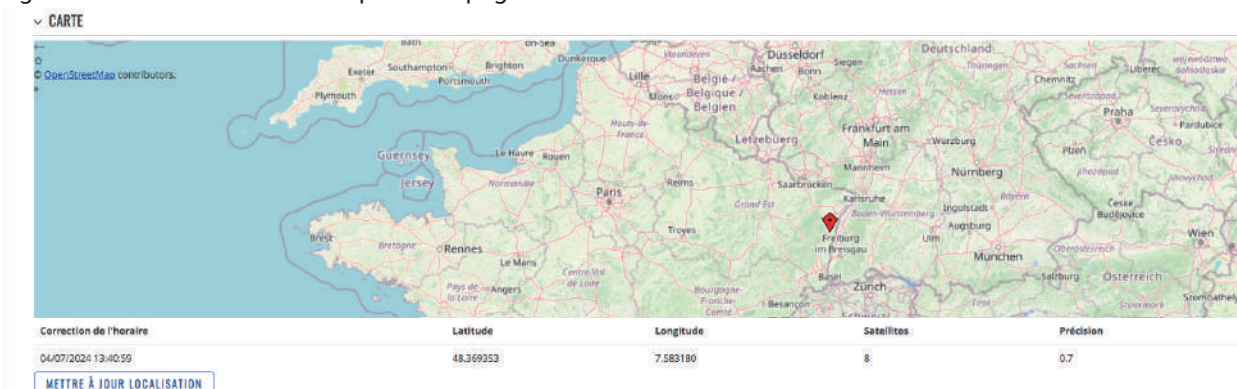


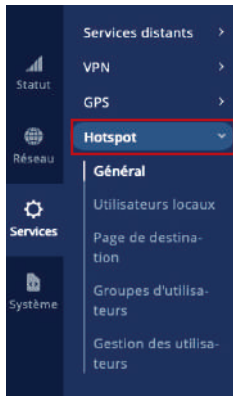
Champ	Valeur	Description
Activé	Off On; Par défaut : Off	Active ou désactive le service GPS.
DPO activé	Off On; Par défaut : Off	Activer l'optimisation dynamique de l'alimentation (nécessite le redémarrage du modem). Cette fonction n'est pas prise en charge sur les appareils équipés de modems Meig ou 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 » ;

The screenshot shows the 'INSTANCES HOTSPOT' section. It contains a table with the following data:

MODE D'AUTHENTIFICATION	IP	INTERFACES	
Utilisateurs locaux	192.168.3.254	lan	☐ ☐

Below the table is a section 'AJOUTER UNE NOUVELLE INSTANCE'. It includes a dropdown menu for 'INTERFACE' with the value 'INET_512_99 (wan1)' selected. To the right of the dropdown is a red box with the number '2' and an 'AJOUTER' button. At the bottom right is a 'SAUVEGARDER ET APPLIQUER' button.

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.

The screenshot shows the 'PARAMÈTRES GÉNÉRAUX' configuration window. It has a sidebar with 'GÉNÉRAL', 'AVANCÉ', and 'ESPACE CONTRÔLÉ'. The main area contains the following fields:

- Profil de configuration: Par défaut
- Activer: ☐ (off/on)
- Réseau du hotspot: 192.168.3.0/24
- Adresse IP: 192.168.3.254
- Mode d'authentification: Utilisateurs locaux
- Autoriser l'inscription: ☐ (off/on)
- Page de destination: Interm.
- Port UAM: 3990
- Page d'authentification réussie: Page d'authentification réussie

At the bottom right is a 'SAUVEGARDER ET APPLIQUER' button.

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

PARAMÈTRES GÉNÉRAUX

GÉNÉRAL

AVANCÉ

ESPACE CONTRÔLÉ

Interfaces supplémentaires

— Veuillez sélectionner —

Adresse de déconnexion

1.0.0.0

Protocole

HTTP

Activer TOS

off on

Accès à l'essai

off on

Redirection HTTPS vers la page de destination

off on

Serveur DNS primaire

8.8.8.8

Serveur DNS secondaire

8.8.4.4

SAUVEGARDER ET APPLIQUER

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	Spécifie 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 sélectionné dans le Profil de configuration dans le menu Général.

PARAMÈTRES GÉNÉRAUX

GÉNÉRAL

AVANCÉ

RADIUS

ESPACE CONTRÔLÉ

PARAMÈTRES URL

Serveur RADIUS #1

54.247.117.188

Serveur RADIUS n°2

79.125.111.180

Port d'authentification

1812

Port de comptabilité

1813

Identifiant NAS

Clé secrète Radius

Echanger des octets

off on

Nom de la localisation

ID de la localisation

SAUVEGARDER ET APPLIQUER

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-Identifiant" 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

GÉNÉRAL

AVANCÉ

RADIUS

ESPACE CONTRÔLÉ

PARAMÈTRES URL

Liste d'adresses

cloud4wi.com
facebook.com
facebook.net
flickr.com
icdn.com

SAUVEGARDER ET APPLIQUER

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.

PARAMÈTRES GÉNÉRAUX

GÉNÉRAL

AVANCÉ

RADIUS

ESPACE CONTRÔLÉ

PARAMÈTRES URL

UAM IP

nas_ip

Port UAM

nas_port

Appelé

ap_mac

MAC

client_mac

IP

client_ip

Identifiant NAS

identifier

Id session

sessionid

URL de l'utilisateur

redirect_url

Défi

challenge

Personnalisation 1

version

SSID : INET_512_2G

Personnalisation 2

Nom personnalisé

SSID : INET_512_2G

SAUVEGARDER ET APPLIQUER

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.

IMAGES

NOM	IMAGE	EMPLACEMENT DU FICHIER
Logo	logo.svg (3.2 KB)	<%=logo%>
Favicon	favicon.png (14.7 KB)	<%=favicon%>
Background	background.jpg (241.2 KB)	<%=background%>
Loading	PARCOURIR ou glisser-déposer votre fichier...	<%=loading%>

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.

PARAMÈTRES DE STYLE

NOM	DESCRIPTION	
Style	Le fichier contient toutes les règles de style 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.

INFORMATIONS LOGICIEL

NOM	DESCRIPTION	
En-tête	Modèle d'en-tête HTML	
Connexion	Modèle de page de connexion	
Connexion (MAC auth)	Modèle de page de connexion pour l'authentification MAC	
Connexion (SMS OTP)	Modèle de page de connexion OTP par SMS	
S'inscrire	Modèle de page d'inscription	
Inscription (SMS OTP)	Modèle de page d'enregistrement de SMS OTP	
Réussi	Modèle de la page d'authentification réussie	
Refusé	Accès refusé modèle de page	
TOS	Conditions d'utilisation	

SAUVEGARDER ET APPLIQUER

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.

THÈMES

NOM	STATUT	TÉLÉCHARGER	
Default theme	Actif		

▼ AJOUTER UN THÈME PERSONNALISÉ

Télécharger un thème personnalisé

PARCOURIR

 ou glisser-déposer votre fichier ici

SAUVEGARDER ET APPLIQUER

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.

▼ GROUPES D'UTILISATEURS

NOM	BANDE PASSANTE TÉLÉCHARGEMENT	BANDE PASSANTE DE CHARGEMENT	LIMITE DE TÉLÉCHARGEMENT	LIMITE DE CHARGEMENT	PÉRIODE	
default	illimité	illimité	illimité	illimité	-	2 ✎ ✕

▼ AJOUTER UN NOUVEAU GROUPE D'UTILISATEURS

1

NOM

AJOUTER

SAUVEGARDER ET APPLIQUER

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

▼ PARAMÈTRES DU GROUPE "DEFAULT"

Délai d'inactivité

0

Limite de temps

0

Bande passante téléchargement

1000

Bande passante de chargement

500

Limite de téléchargement

10000

Limite de Chargement

10000

Attention

10000

Période

Mois

jour de début

1

SAUVEGARDER ET APPLIQUER

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.

UTILISATEURS ACTUELS

UTILISATEURS ENREGISTRÉS

UTILISATEURS ACTUELS DU HOTSPOT

Nom d'utilisateur	IP	MAC	Télécharger	Charger	Heure de la session	Heure de début	Déconnecter l'utilisateur
Aucun utilisateur connecté actuellement							

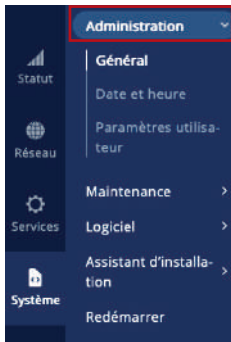
L'onglet Utilisateurs enregistrés affiche les données des utilisateurs uniques qui se sont déjà enregistrés sur le hotspot.

UTILISATEURS ACTUELS

UTILISATEURS ENREGISTRÉS

~ UTILISATEURS DE HOTSPOTS ENREGISTRÉS

Email	Temps d'expiration	Liste de numéros de téléphone sur liste blanche	Date d'inscription	Supprimer l'utilisateur
Aucun utilisateur enregistré				



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.

▼ PARAMÈTRES GÉNÉRAUX

Langue:

Mode de configuration:

▼ NOM DE L'APPAREIL ET NOM D'HÔTE

Nom de l'appareil:

Nom d'hôte:

▼ INDICATION LED

Activer: ☐

▼ CONFIGURATION DU BOUTON DE RESET

ACTION	HEURE MINIMALE	TEMPS MAX	
Redémarrer	0	5	☐
Configuration par défaut de l'utilisateur	6	11	☐
Configuration des valeurs d'usine	12	99	☐

[SAUVEGARDER ET APPLIQUER](#)

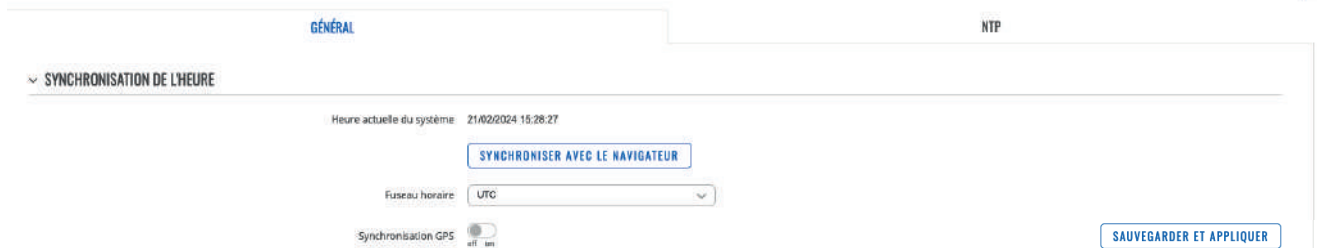
Champ	Valeur	Description
Paramètres généraux		
Langue	English French German ; Par défaut : French	Modifie la langue de l'interface utilisateur Web du routeur.
Mode de configuration	Normal Avancé ; Par défaut : Normal	Le mode détermine quelles options et configurations sont affichées. En mode Basique, 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.

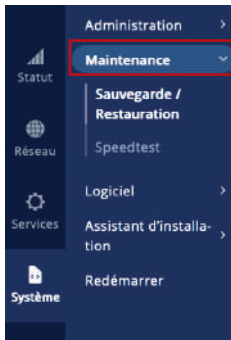


Champ	Valeur	Description
Heure actuelle du système	Par défaut : aucun	L'heure locale actuelle de l'appareil.
Synchroniser avec le navigateur	Bouton interactif	Cliquez pour synchroniser l'heure de l'appareil et le fuseau horaire avec les navigateurs, si l'heure ou le fuseau horaire de votre appareil ne 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.

✓ CRÉER UNE CONFIGURATION PAR DÉFAUT



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.

✓ SAUVEGARDE DE LA CONFIGURATION



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 LA CONFIGURATION



Restaurer les paramètres par défaut

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

RESTAURER LES PARAMÈTRES PAR DÉFAUT



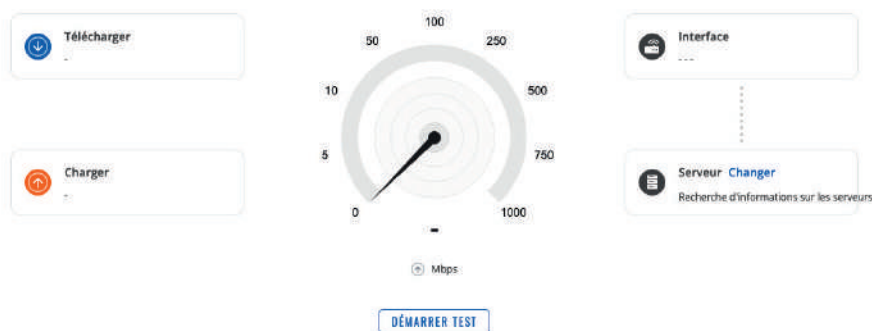
Champ	Valeur	Description
Restaurer les paramètres d'usine	Bouton interactif	Restaure l'appareil aux paramètres par défaut.
Restaurer les valeurs utilisateur par défaut*	Bouton interactif	Restaure l'appareil à la configuration personnalisée définie par l'utilisateur.

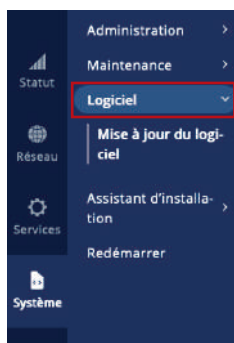
* Vous ne verrez pas ce bouton tant que vous n'aurez pas créé une configuration par défaut de l'utilisateur.

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.

SPEEDTEST





4.3 Menu Système > Logiciel

4.3.1 Menu Système > Logiciel > Mise à jour du logiciel

INFORMATIONS SUR LE LOGICIEL ACTUEL

Version logiciel	I-NET_512_T_19.07.05.59
Date de création du logiciel	2024-02-09 15:01:54
Version logiciel du modem	RG501QEUAR12A0BM4G_04.200.04.200
Version du noyau	5.10.188

LOGICIEL DISPONIBLE SUR LE SERVEUR

Version logiciel	Aucune mise à jour disponible
Modem interne	Aucune mise à jour disponible

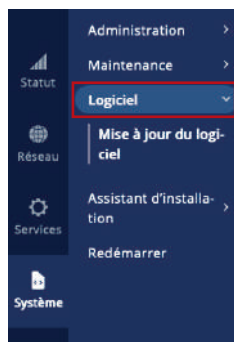
MISE À JOUR DU LOGICIEL

Mise à jour depuis Fichier

Conserver les paramètres off on

Image PARCOURIR ou glissez-déposez votre fichier ici

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.

ALDEN

Normal Avancé

I-NET_512_T_19.07.05.59
Options d'affichage

PARAMÈTRES WEBUI

Langue French

Mode de configuration Avancé

PARAMÈTRES GÉNÉRAUX

Heure actuelle du système 03/04/2024 14:08:47

SYNCHRONISER AVEC LE NAVIGATEUR

Fuseau horaire Europe/Paris

SUIVANT

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

ALDEN

Normal Avancé

WIFI 2.4GHZ

Activer ☐ Off ☒ On

ESSID: INET_512_2G

Mot de passe: [masked]

WIFI 5GHZ

Activer ☐ Off ☒ On

ESSID: INET_512_5G

Mot de passe: [masked]

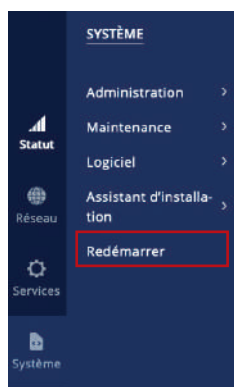
Attention : En changeant le nom du réseau ESSID et/ou le mot de passe par défaut, le QR code imprimé sur la face avant du routeur ne sera plus fonctionnel.

RETOUR TERMINER

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.



REDÉMARRER LE ROUTEUR ?

Pendant le redémarrage, l'appareil ne sera pas joignable pendant 1 à 2 minutes.

REDÉMARRER ANNULER

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.

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

En cas d'installation personnelle, l'acheteur fera sienne les responsabilités affaissant 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 déviara 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 :



SAT



TV



INTERNET



SOLAR



ENERGIE

www.alden.fr