INTERNET

Guide d'installation

Routeur I-NET 152



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

ALDEN

CE

Sommaire

Sommaire 2-3

Avertissements 4-7
Sécuriser l'accès de votre appareil : 5
Manipulation du produit 6
Mise à jour du I-NET 152 7

Informations de sécurité 8
Information de sécurité I-NET 152 8
- Exposition RF 8
- Conditions de fonctionnement 8
- Produits défectueux et endommagés 8
- Sécurité électrique 8

Installation 9-10
Configuration I-NET 152 9
- I-NET 152 Mesures spatiales et poids 9
- Mesures principales 9
- Vue avant 9
- Espace de montage 10
- Fixation 10

Configuration 11-14
- Description des interfaces 11
- Brochage de la prise d'alimentation 11
- Carte SIM I-NET 152 12
- Voyant d'alimentation 13
- Voyants du port Ethernet 13
- Voyants du réseau mobile 14
- LED d'indication de la force du signal mobile .. 14

Info pratiques 15-16
- Répéteur WiFi. 15
- Sélection 3G/4G 15
- Sélection manuelle de l'opérateur 15
- Mode Normal /Avancé 15
- Gestion réseau 15
- Installation rapide 15
- Première mise en service 16

Menu Statut 17-29
1. Menu Statut 17
1.1 Menu Statut > Aperçu 17
- Bouton Widget : Mobile 17
- Niveaux de signal 2G et 3G 18
- Niveaux de signal 4G et 5G 18
- Bouton Widget : Infos 18
- Ajout de widgets supplémentaires 18
- Widget latéral 19

1.2 Menu Statut > Système 20

1.3 Menu Statut > Réseau 21
1.3.1 Menu Statut > Réseau > Mobile 21
1.3.2 Menu Statut > Réseau> LAN 23
1.3.2 WiFi 24

1.4 Menu Statut > WiFi 24
1.4.1 Menu Statut > WiFi > Interfaces 24
- Interfaces WiFi 24
- Clients WiFi 24
1.4.2 Menu Statut > WiFi > ANALYSES DES CANAUX 24
- Répartition des canaux 24
- Scans 25
- Évaluation 25

1.5. Menu Statut > Données en temps réel 26
1.5.1 Menu Statut > Données en temps réel > Trafic 26
1.5.2 Menu Statut > Données en temps réel > Signal mobile 27
1.5.3 Menu Statut > Données en temps réel > ..... UTILISATION mobile 27
- Mesure de signaux 28
- Détermination des facteurs des valeurs de signal 28
- Avis de non-responsabilité 28
- 2G 28
- 3G 29
- 4G (LTE) 29

Menu Réseau 30-79
2. Menu Réseau 30
2.1 Menu Réseau > Mobile 30
2.1.1 Menu Réseau > Mobile > Général 30
- Gestion de la carte SIM 30
- Configuration APN de l'interface SIM 30
2.1.2 Menu Réseau > Mobile > connexion 31
- Reconnexion sur signal faible 31
2.1.3 Menu Réseau > Mobile > Limites 32
- Limites de données 32
- Limite SMS 33
2.1.4 Menu Réseau > Mobile > sélection du réseau 34
2.1.5 Menu Réseau > Mobile > utilitaires 36
- Gestion du code PIN de la carte SIM 36
- USSD 36
- Notification de verrouillage par code PIN/PUK . 37

2.2 Menu Réseau > WAN 38
- Paramétrage des interfaces 38
- CONFIGURATION interface 39
- Paramètres Généraux : Protocole statique 39
- Paramètres Généraux : Protocole DHCP 39
- Paramètres Généraux : Protocole DHCPV6 40
- Paramètres Généraux : Protocole PPPoE 40
- Paramètres Généraux : Protocole Mobile 41
- Paramètres IPv6 44
- Paramètres IPv6 : Protocole Statique 44
- Paramètres IPv6 : Protocole DHCPV6 45
- Paramètres IPv6 : Protocole PPPoE 45
- Paramètres avancés 46
- Paramètres avancés : protocole Statique 46
- Paramètres avancés : protocole DHCP 46
- Paramètres avancés : DHCPv6 47
- Paramètres avancés : PPPoE 48
- Paramètres avancés : Protocole mobile 49
- Paramètres physiques 49
- Paramètres du pare-feu 50

2.3 Menu Réseau > LAN 51
- CONFIGURATION interface 51
- Paramètres Généraux 51
- Paramètres IPV6 52
- Paramètres avancés 52
- Paramètres physiques 53
- Paramètres du pare-feu 53

Sommaire

2.4 Menu Réseau >WiFi..... 54
2.4.1 Menu Réseau >WiFi>SSiD 54
- Configuration générale 54
- Paramètres supplémentaires 55
- Sécurité WiFi 56
- Paramètres avancés..... 58
- Filtre MAC..... 59
- Scanner 2.4 GHz 59
- Multi AP 62
- Points d'accès 62
- QR Code WiFi 63
2.4.2 Menu Réseau >WiFi>BANDES..... 63
- Configuration générale 63
- Paramètres avancés..... 65
2.5 Menu Réseau > Gestion réseau 66
2.5.1 Menu Réseau > Gestion réseau > Multiwan66
- Réglage..... 67
- Interface 68
- Membre 69
- Politique 70
- Règle 71
2.6 Menu Réseau > DHCP 72
2.6.1 Menu Réseau > DHCP > Réglages du serveur 72
- IPv4 72
- Configuration générale DHCPv4 73
- Paramètres avancés DHCPv4 74
- IPv6 75
- Configuration DHCPv6 75
2.6.2 Menu Réseau > DHCP > Baux statique..... 77
2.7 Menu Réseau > DNS 78
2.7.1 Menu Réseau > DNS > Général 78
- Paramètres Généraux..... 78
- Paramètres avancés..... 79

Menu SERVICES..... 80-114
3 Menu SERVICES 80
3.1 Menu SERVICES > Services distants 80
3.1.1 Menu SERVICES > Services distants > RMS 80
- RMS : Paramètres du proxy 81
- RMS : Statut 81
3.2 Menu SERVICES > VPN 81
3.2.1 Menu SERVICES > VPN > IPSec 81
- IPSec : Configuration de Connexion..... 84
- IPSec : Paramètres généraux..... 84
- IPSec : Paramètres avancés..... 85
- IPSec : Configuration de proposition 87
3.2.2 Menu SERVICES > VPN > OpenVPN..... 89
- OpenVPN : Client 89
3.2.3 Menu SERVICES > VPN > WireGuard 99
- WireGuard : Paramètres généraux 99
- WireGuard : Paramètres avancés..... 100
- WireGuard : Pairs 100
- WireGuard : Paramètres généraux 101
- WireGuard : Paramètres avancés..... 101
3.2.4 Menu SERVICES > VPN > ZeroTier 102
3.3 Menu SERVICES >Hotspot 104
3.3.1 Menu SERVICES >Hotspot > Général 104
- Hotspot > Configuration point d'accès..... 105
3.3.2 Menu SERVICES >Hotspot >Utilisateurs locaux 110
3.3.3 Menu SERVICES >Hotspot > Page de destination 111
3.3.4 Menu SERVICES >Hotspot > Groupes d'utilisations 113
3.3.5 Menu SERVICES >Hotspot > Gestion des utilisateurs..... 114

Menu SYSTÈME.....115-123
4 Menu Système..... 115
4.1 Menu Système > administration..... 115
4.1.1 Menu Système > administration > Général ... 115
4.1.2 Menu Système > administration > Date et heure..... 117
4.1.3 Menu Système > administration > Paramètres utilisateur 117
- Changer le mot de passe..... 117
4.2 Menu Système > Maintenance..... 118
4.2.1 Menu Système > Maintenance > Sauvegarde/ Restauration 118
- Créer une sauvegarde 118
- Charger une sauvegarde 119
- Vérification de sécurité de sauvegarde 119
4.2.2 Menu Système > Maintenance > Réinitialiser les paramètres..... 119
- Créer la configuration par défaut de l'utilisateur.. 120
4.3 Menu Système > logiciel 120
4.3.1 Menu Système > logiciel > Mise à jour du logiciel..... 120
Mise à jour du logiciel..... 120
4.3.2 Menu Système > logiciel > paramètres fota 121
4.4 Menu Système > Assistant d'installation 121
4.4.1 Menu Système > Assistant d'installation > général 121
4.4.2 Menu Système > Assistant d'installation > mobile 122
4.4.3 Menu Système > Assistant d'installation > ... WiFi 123

Garantie ALDEN 124

Garantie..... 125

Bon de garantie 125

Avertissements

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Cet appareil répond aux exigences gouvernementales en matière d'exposition aux ondes radio. Cet appareil est conçu et fabriqué pour ne pas dépasser les limites d'émission pour l'exposition à l'énergie des radiofréquences (RF) fixées par les agences autorisées. Pour assurer la conformité avec les directives d'exposition RF, l'appareil doit être utilisé avec une distance minimale de 20 cm du corps d'une personne. Le non-respect de ces instructions peut entraîner une exposition aux RF dépassant les limites des directives pertinentes.
Les antennes externes utilisées avec le I-NET 152 doivent être installées pour fournir une distance de séparation d'au moins 20 cm de toutes les personnes et ne doivent pas être co-localisées ou utilisées en conjonction avec une autre antenne ou émetteur.

Avertissements

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

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

Sécuriser l'accès de votre appareil :

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

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

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

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

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





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

Avertissements

Manipulation du produit

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

Mise à jour du I-NET 152

Le routeur I-NET 152 dispose d'un système de mise à jour automatique et manuel du logiciel.

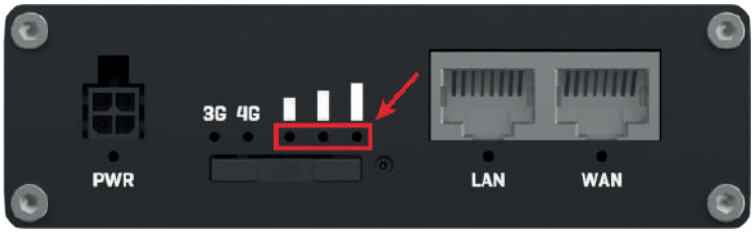
Des mises à jour du logiciel peuvent être effectuées automatiquement. Avant toute action sur l'appareil (coupure d'alimentation, redémarrage..), il convient de contrôler l'état des voyants et de s'assurer que le routeur ne soit pas dans une phase de mise à jour.

Pour mettre à jour le logiciel manuellement, se référer au chapitre "4.3.1 Menu Système > logiciel > Mise à jour du logiciel", page 120.

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.



- 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 152 HORS TENSION DURANT LA PHASE DE MISE A JOUR AU RISQUE DE RENDRE CELUI-CI DEFINITIVEMENT INUTILISABLE

Informations de sécurité I-NET 152

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 152 doivent être installées pour fournir une distance de séparation d'au moins 20 cm de toutes les personnes et ne doivent pas être co-localisées ou utilisées en conjonction avec une autre antenne ou émetteur.

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

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

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

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

Conditions de fonctionnement

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

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

Produits défectueux et endommagés

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

Sécurité électrique

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

Configuration I-NET 152

I-NET 152 Mesures spatiales et poids

Cette page contient des informations sur les mesures et le poids du routeur I-NET 152. 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

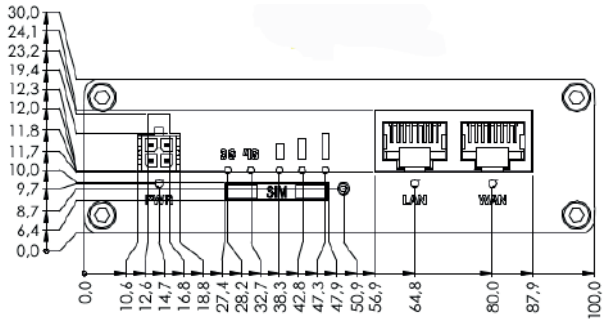
Dimensions L x H x P pour I-NET 152 :

Boîtier de l'appareil * :	100 x 30 x 85 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.

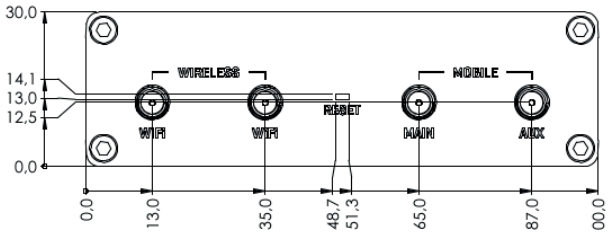
Vue avant

La figure ci-dessous illustre les mesures du I-NET 152 et de ses composants sur la face avant :



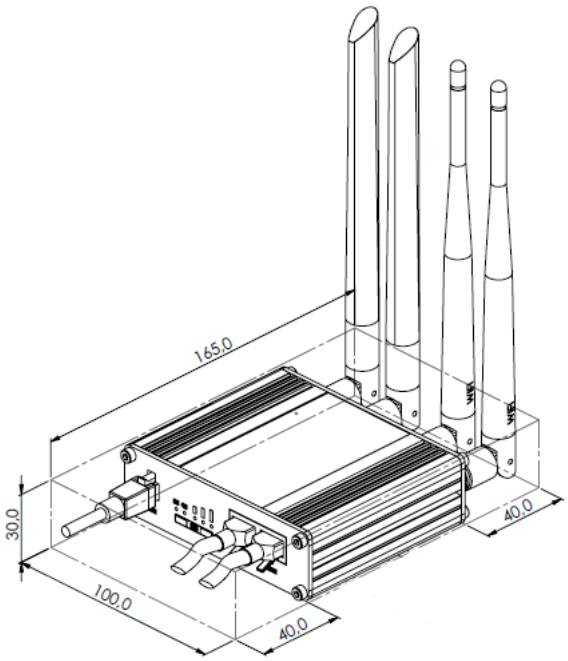
Vue arrière

La figure ci-dessous illustre les mesures du I-NET 152 et de ses composants sur la face arrière :



Espace de montage

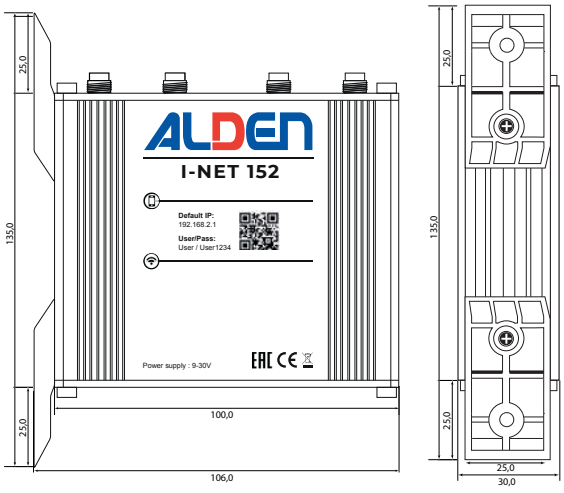
La figure ci-dessous représente le volume requis de l'appareil lorsque les câbles et les antennes sont connectés :



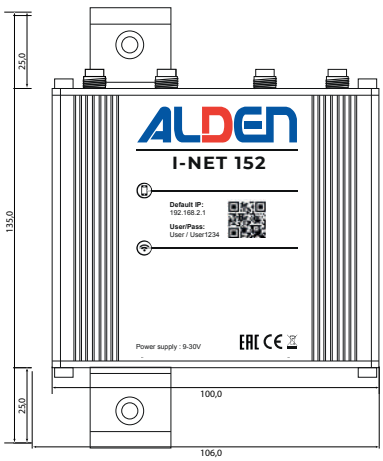
Fixation

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

Fixation verticale



Fixation horizontale

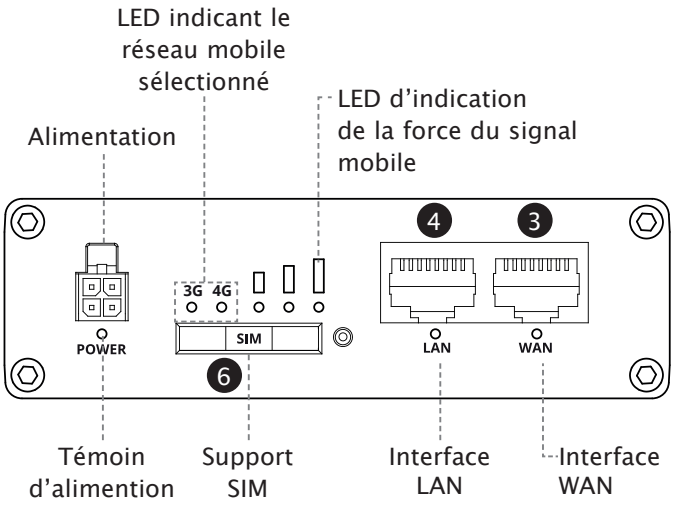


Il est à noter qu'il est possible de fixer le routeur verticalement et horizontalement. Visser les 2 supports à l'aide des 2 vis (fournies) dans le rail du routeur, prévu à cet effet.

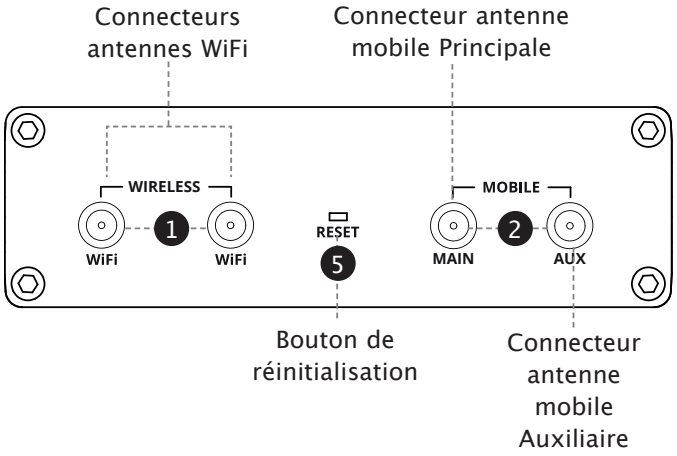
Description des interfaces

Le routeur I-NET 152 est doté de différentes interfaces et ports pour offrir un accès à internet optimal.

1. Interface WiFi via 2 connecteurs à l'arrière pour un accès sans fils à internet entre le routeur et un ordinateur ou une borne WiFi externe. L'interface WiFi permet l'accès à l'interface web utilisateur du routeur et à internet.
2. Interface mobile 4G avec 2 connecteurs pour connecter 2 antennes MIMO.
3. Un port WAN à l'avant pour un accès à internet grâce à un réseau filaire externe.
4. Un port LAN pour la connexion filaire d'un ordinateur au routeur I-NET 152.
5. Bouton Reset utilisé pour réinitialiser le routeur à ses réglages d'origine. Appuyer et maintenir le bouton 12 à 20 secondes à l'aide de l'aiguille fourni.
6. Lecteur carte SIM.

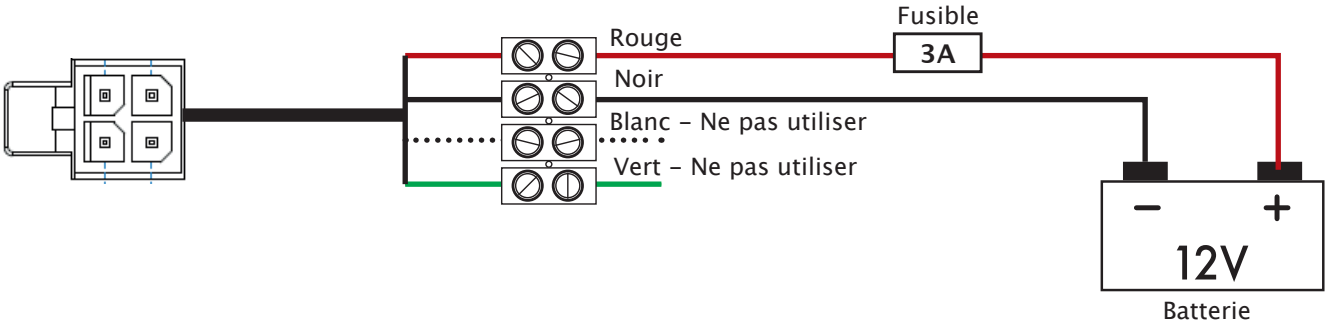


VUE AVANT

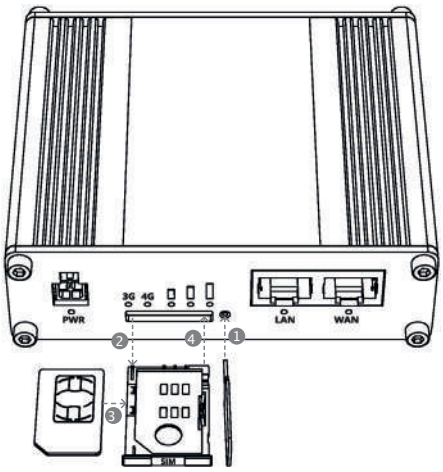


VUE ARRIÈRE

Brochage de la prise d'alimentation

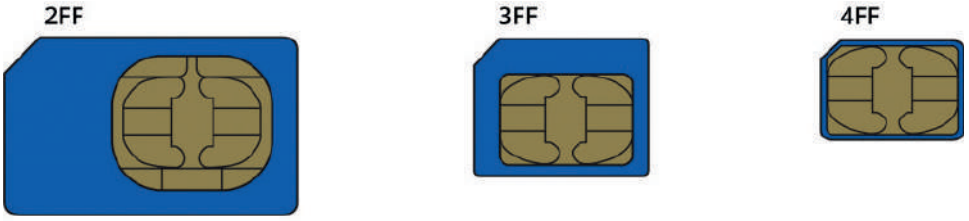


Carte SIM I-NET 152



1. Appuyez sur le bouton du support SIM avec l'aiguille SIM fournie.
2. Retirez le support SIM.
3. Insérez votre carte SIM dans le support SIM. Utiliser l'un des adaptateurs (fournis) si-besoin.
4. Insérer le support SIM dans le routeur.
5. Fixez les antennes Mobile 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.
7. Connectez-vous au SSID du réseau WiFi de l'appareil en scannant le QR code avec un smartphone ou en utilisant les infos à l'avant de l'appareil (ou sinon utilisez un câble Ethernet connecté à l'interface LAN).

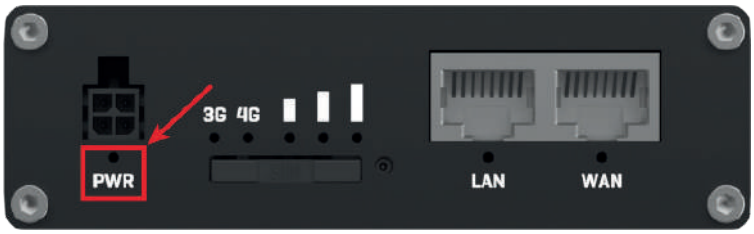
L'appareil est compatible avec les cartes de taille mini-SIM (2FF). Mais comme différents types de cartes SIM ont le même agencement de contacts, des cartes SIM plus petites peuvent également être utilisées avec le routeur, à condition qu'elles soient insérées dans un adaptateur de carte SIM 2FF. Une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

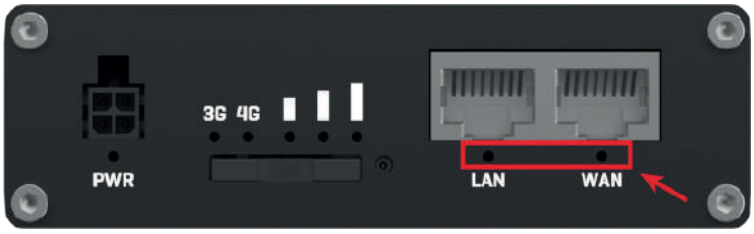


Il indique si l'appareil est sous tension ou non.

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

Voyants du port Ethernet

Les voyants du port Ethernet sont situés sur le panneau avant de l'appareil, sous chaque port Ethernet respectif.



Voyant allumé	Fonctionne comme une connexion 10/100 Mbps.
Voyant OFF	Aucun lien établi.
Voyant clignotant	Connexion établie et activité en cours sur ce port (Transfert de données).

Voyants du réseau mobile

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

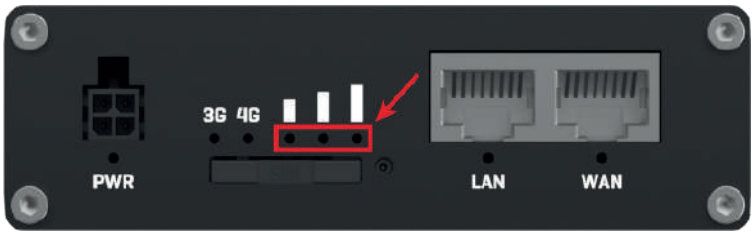


Ils affichent le type de connexion Internet actuellement actif.

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

LED d'indication de la force du signal mobile

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

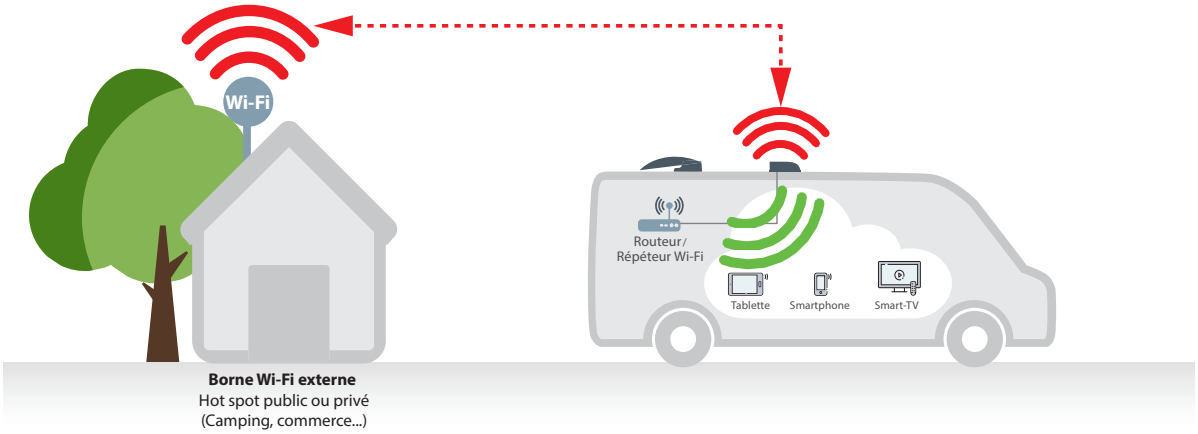


Le nombre de LED allumées représente une valeur de force de signal mobile (RSSI) différente en dBm.

0	≤ -111dBm
1	-110 dBm à -82 dBm
2	-81 dBm à -52 dBm
3	≥ -51dBm

Répéteur WiFi.

Le routeur I-NET 152 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 page 24 pour créer sont propre répéteur WiFi est ainsi économiser des données sur sa carte SIM.

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

Sélection 3G/4G

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

Se référer au chapitre "2.1.1 Menu Réseau > Mobile > Général", page 30 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 "2.1.4 Menu Réseau > Mobile > sélection du réseau", page 34 pour forcer la connexion sur un opérateur réseau de son choix.

Gestion réseau

L'objectif de ce module est de garantir à l'utilisateur un accès à internet si au moins l'une des interfaces est opérationnelle. Par défaut, le module de Gestion réseau est activé.

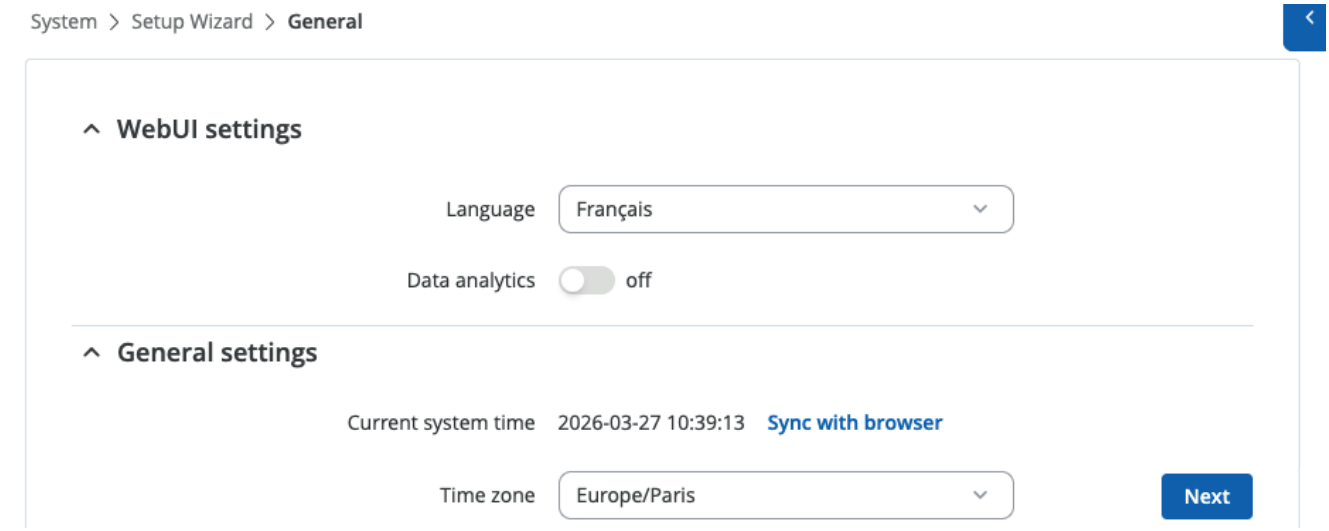
Se référer au chapitre "2.5 Menu Réseau > Gestion réseau", page 66.

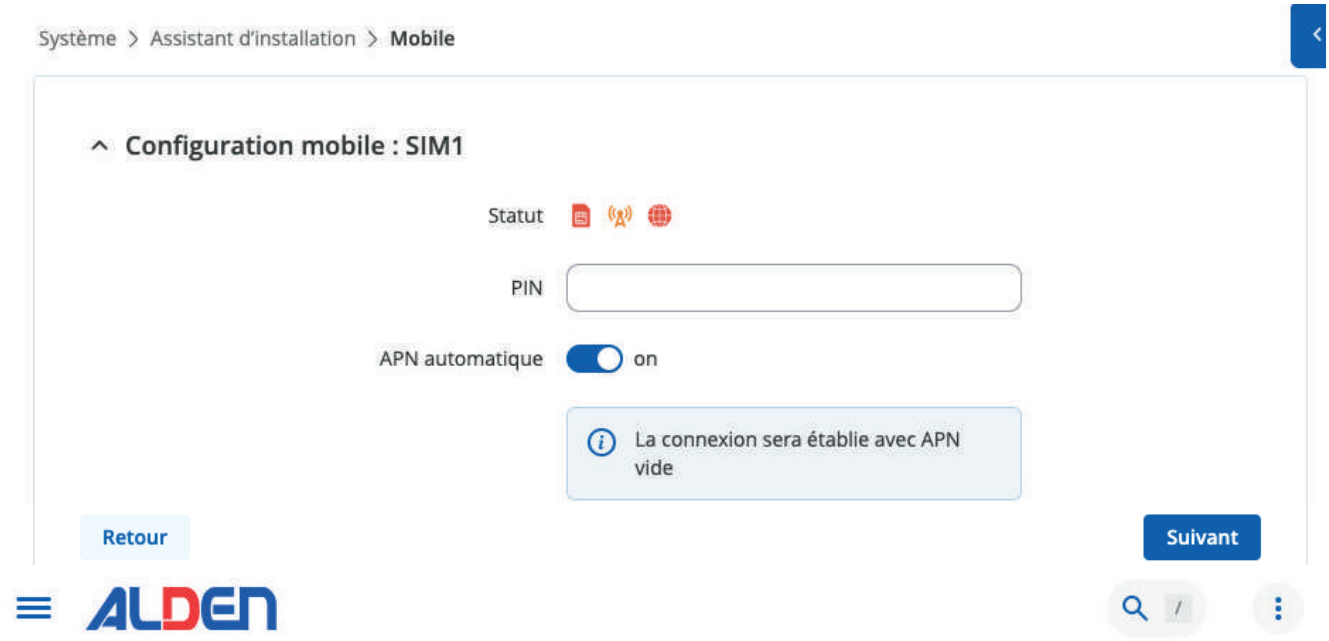
Installation rapide

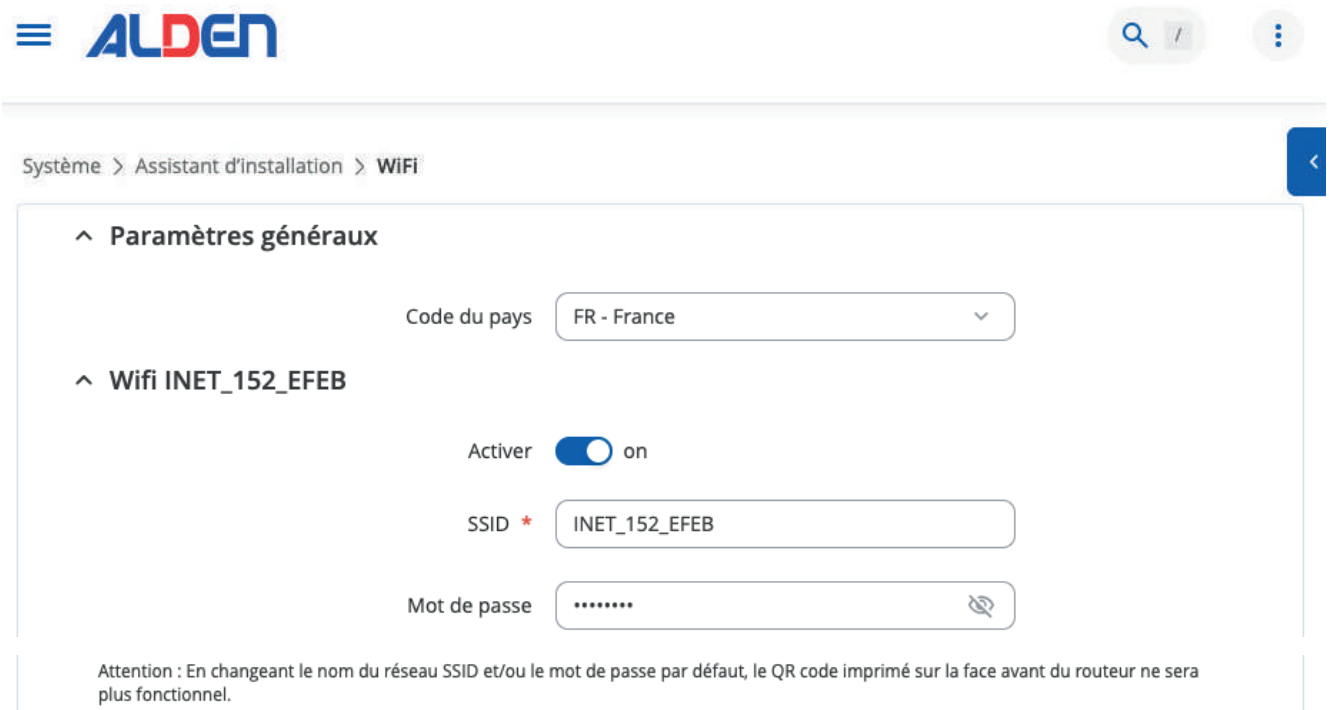
Lors de la première mise en service, vous êtes invités à saisir les principaux paramètres pour configurer votre routeur. Il est obligatoire de valider toutes les étapes de cette installation. Ne pas oublier de saisir le code PIN de votre carte SIM. En cas de doute sur un paramètre suggéré, valider la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

Première mise en service

Choix de la langue.



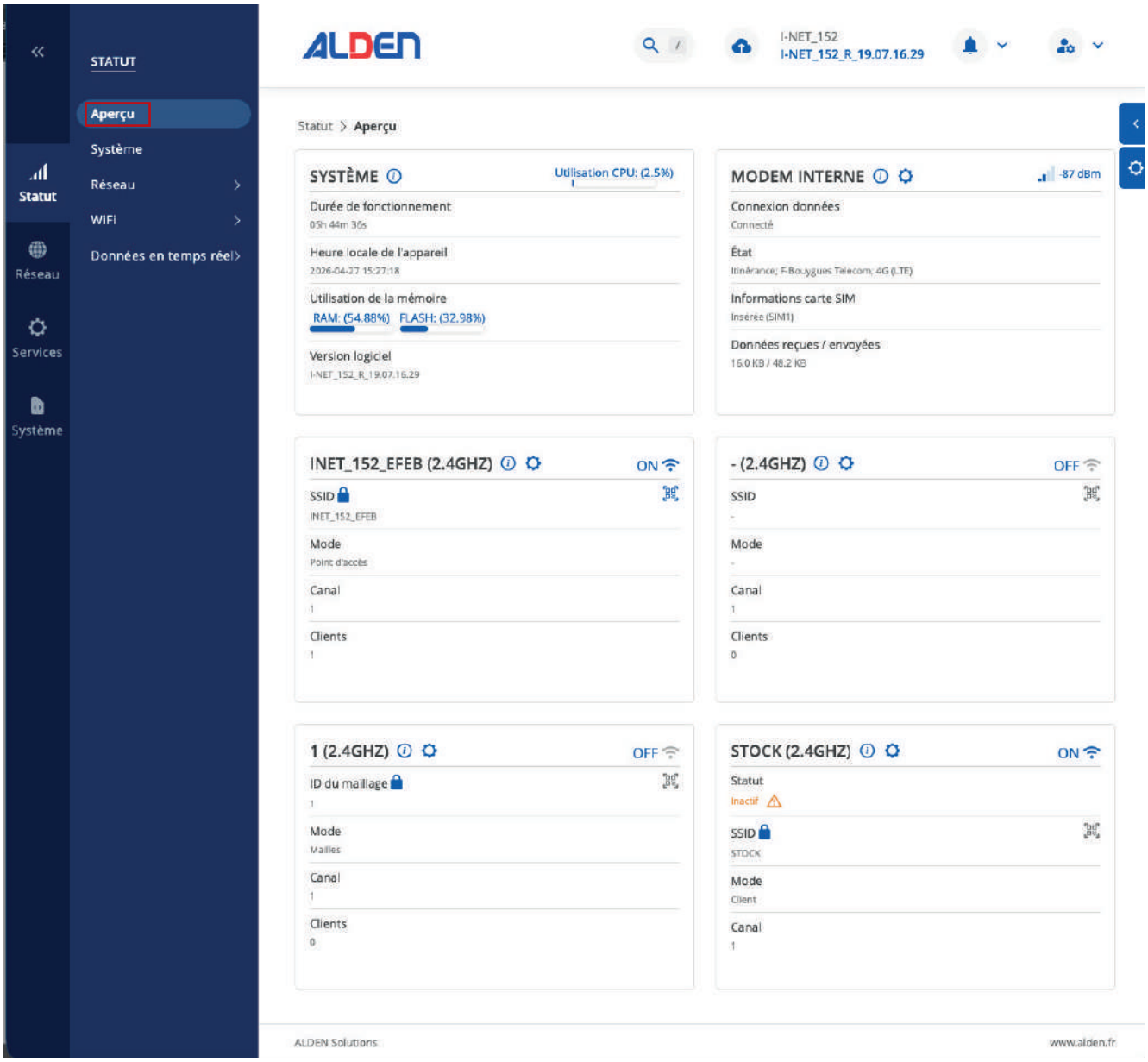




1. Menu STATUT

1.1 Menu STATUT > APERÇU

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



Bouton Widget : Mobile

Le widget Mobile 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 to -97
2	-96 to -52
3	≥ -51

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

Niveaux de signal 2G et 3G

RSSI	Force du signal	Description
>= -70dBm	Excellent	Signal fort permettant d'atteindre les meilleurs débits possibles
-70 dBm à -85 dBm	Bon	Signal fort avec de bons débits de données
-86 dBm à -100 dBm	Moyen	Utilisable, des débits rapides et fiables peuvent être atteints, mais des interruptions de connexion sont possibles
-100 dBm à -110 dBm	Faible	Les performances chuteront fortement
-110dBm	Très faible	La connexion peut être perdue

Niveaux de signal 4G et 5G

RSSI	Force du signal	Description
> -65dBm	Excellent	Signal fort avec des débits de données maximaux
-65 dBm à -75 dBm	Bon	Signal fort avec de bons débits de données
-75 dBm à -85 dBm	Moyen	Utilisable, des débits rapides et fiables peuvent être atteints, mais des interruptions de connexion sont possibles
-85 dBm à -95 dBm	Faible	Les performances chuteront fortement
<= -95dBm	Très faible	La connexion peut être perdue

Bouton Widget : Infos

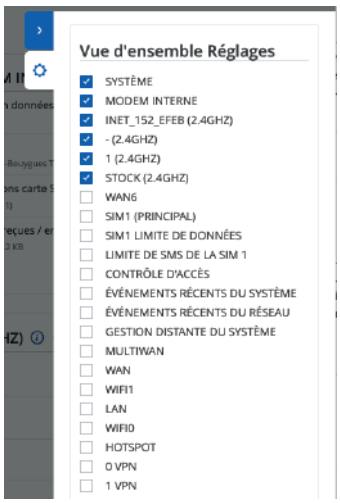
Le bouton Info (ⓘ) est situé à côté du nom de certains widgets. Cliquer sur le bouton Info redirige l'utilisateur vers une page d'état liée aux informations affichées par le widget. Par exemple, cliquer sur le bouton Info du



widget Système vers la page État

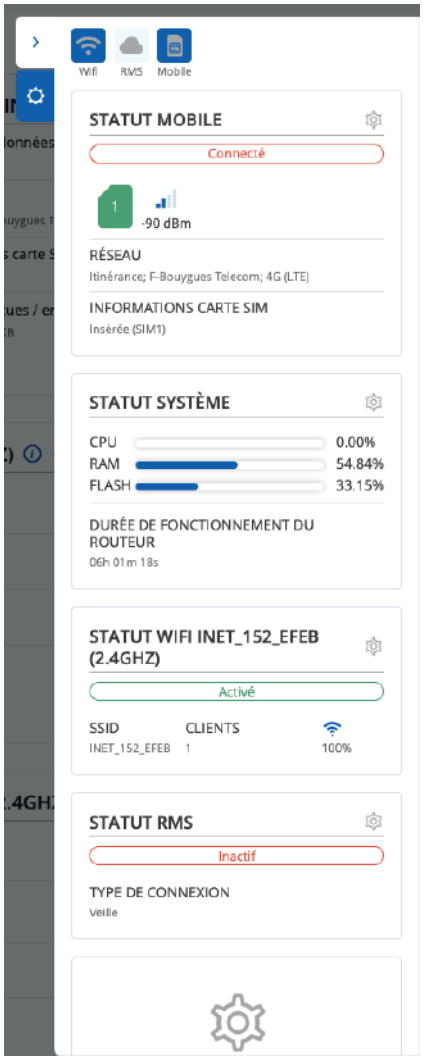
Ajout de widgets supplémentaires

La page Vue d'ensemble affiche un ensemble de widgets par défaut, mais il est possible d'en ajouter d'autres en cliquant sur le bouton Paramètres de la vue d'ensemble .



Widget latéral

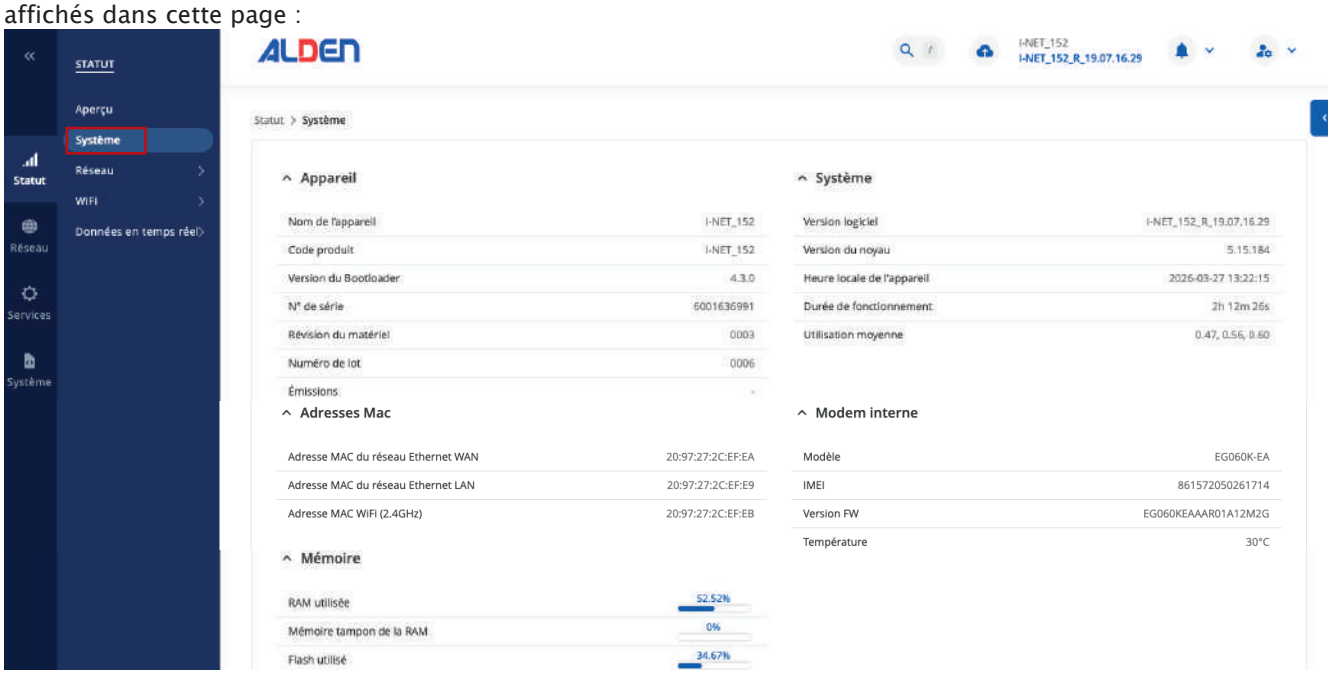
Le menu latéral permet d'activer/désactiver rapidement certaines fonctions du produit et de suivre l'état de certains services. L'affichage des états est paramétrable. L'image ci-dessous est commune à tous les produits. Chaque produit possède son propre menu latéral.



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 :



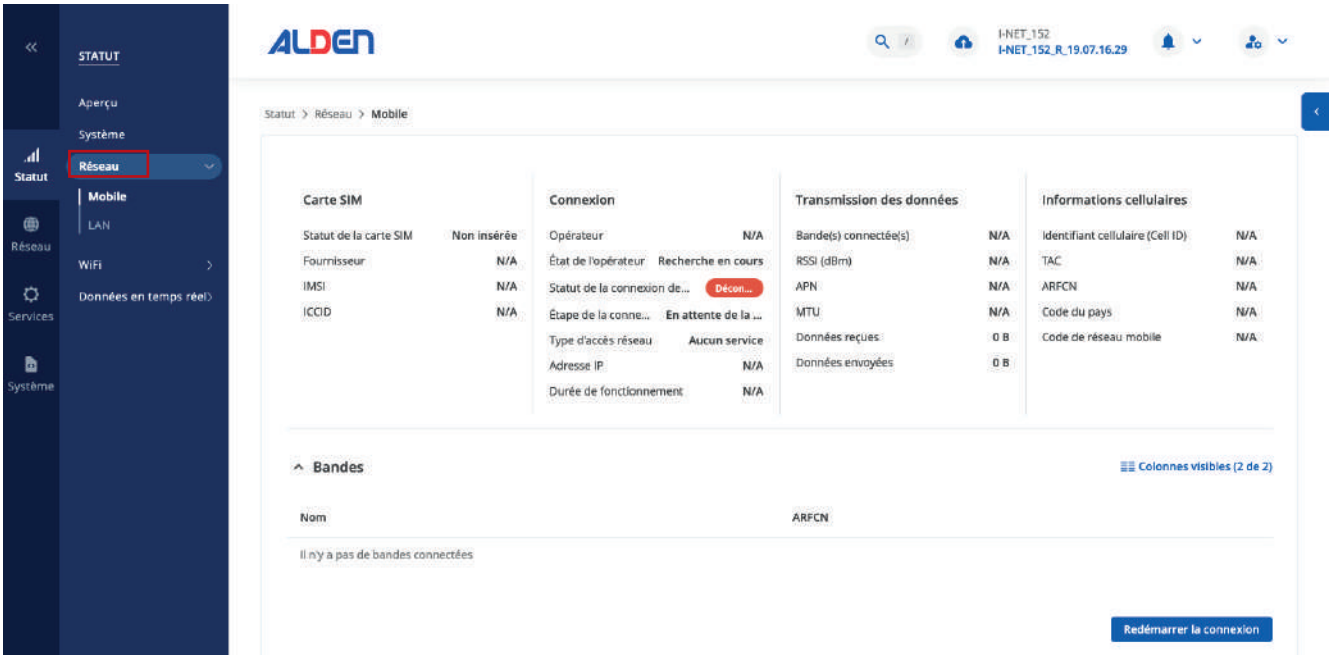
Nom de l'appareil	Le nom de cet appareil : I-NET_152
Code produit	Code de commande ; affiche sous quel code produit l'appareil a été fabriqué.
Version du Bootloader	Version du Bootloader actuellement utilisée par le dispositif. Un Bootloader est un programme qui charge le système d'exploitation.
N° de série	Un identifiant d'appareil unique à 10 chiffres.
Révision du matériel	Un nombre à 4 chiffres représentant la version du matériel.
Numéro de lot	Un numéro à 4 chiffres qui indique le lot de produit.
Émissions	Identifiant de la version matérielle
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 Services → Assistant de configuration – Général.
Durée de fonctionnement	Temps qui s'est écoulé depuis la dernière mise sous tension ou redémarrage de l'appareil.
Utilisation moyenne	Moyenne d'utilisation du CPU (en %) sur la dernière minute, 5 minutes et 15 minutes.
Adresse MAC du réseau Ethernet WAN	Adresse MAC de l'interface WAN.
Adresse MAC du réseau Ethernet LAN	Adresse MAC de l'interface LAN.
Adresse MAC WiFi (2,4 GHz)	Adresse MAC de l'interface WiFi 2,4 GHz.
Modèle	Numéro de modèle du modem à l'intérieur 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 réseaux GSM utilisent l'IMEI pour identifier les appareils dans leurs réseaux.
Version FW	Version du logiciel du modem à l'intérieur 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 :



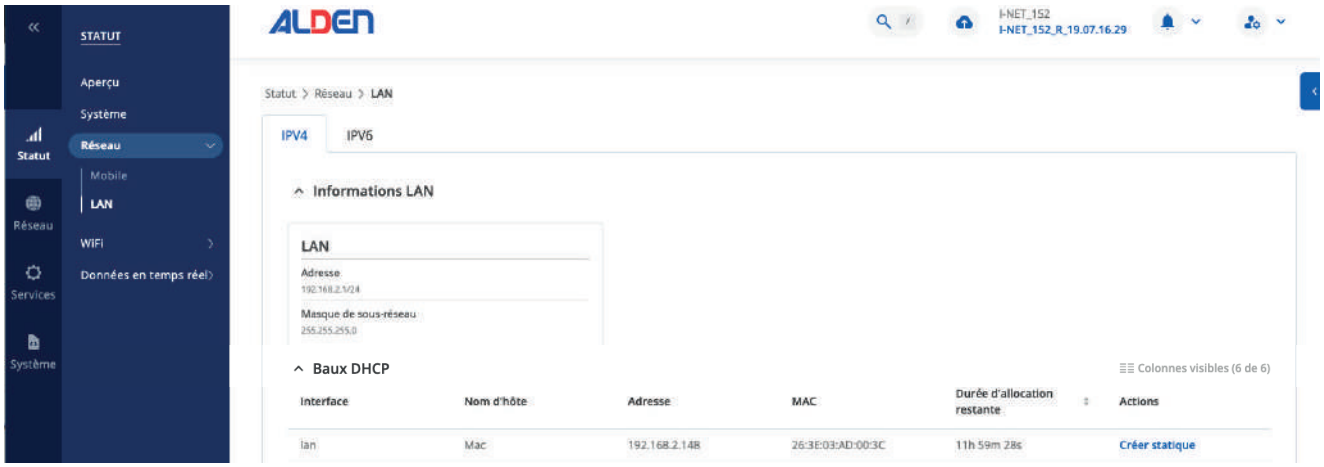
Statut de la carte SIM	L'état actuel de la carte SIM. Les valeurs possibles sont : • **Insérée** – La carte SIM est insérée et prête à être utilisée • **Non insérée** – La carte SIM n'est pas insérée • **Inconnu** – impossible d'obtenir la valeur d'état de la carte SIM. Problème de communication possible entre l'appareil et le modem
Fournisseur	Nom de l'opérateur 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 est 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 détecté l'enregistrement de l'appareil mobile. Valeurs possibles : • **Non enregistré** – l'appareil n'est pas enregistré auprès d'un réseau et ne recherche actuellement aucun nouvel opérateur. • **Enregistré** (domicile) – réseau domestique enregistré • **Recherche en cours** – appareil non enregistré sur un réseau, mais recherche actuellement un nouvel opérateur auquel s'enregistrer. • **Réseau refusé** – l'inscription au réseau a été refusée par l'opérateur • **Inconnu** – l'état de l'opérateur est actuellement inconnu • **Enregistré** (itinérance) – enregistré sur le réseau, conditions d'itinérance
Statut de la connexion des données	Indique si l'appareil dispose ou non d'une connexion de données mobiles.
Étape de la connexion	Afficher les étapes intermédiaires du processus d'établissement d'une connexion mobile.
Type d'accès réseau	Type de connexion mobile. Les valeurs possibles sont : • **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
Adresse IP	Adresse IP de l'interface mobile
Durée du fonctionnement	Disponibilité de la connexion mobile

MENU STATUT

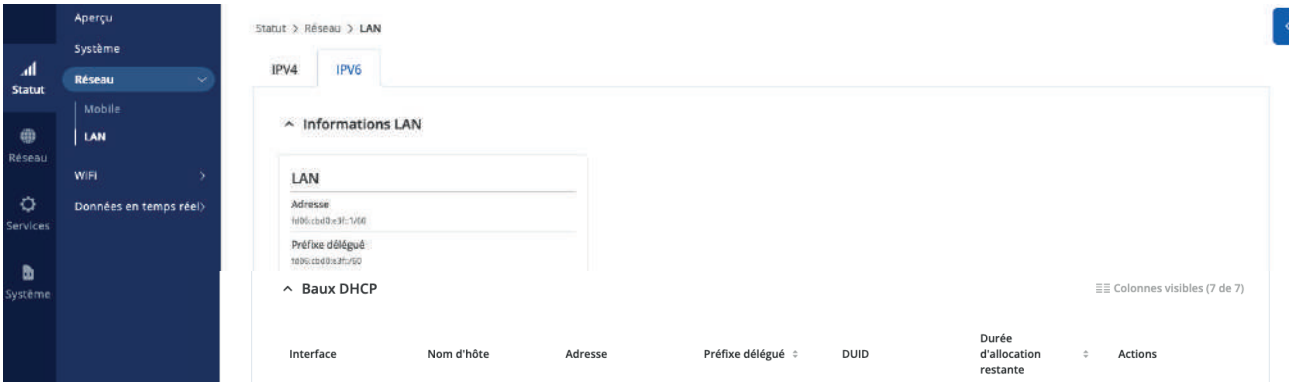
Bande(s) connectée(s)	Bande de fréquence mobile actuellement utilisée.
RSSI (dBm)	Indicateur calculé de la qualité globale de la connexion cellulaire. Les calculs sont effectués en fonction du type de réseau : • 4G : RSRP, RSRQ, SINR • 3G : RSCP, EC/IO
APN	Nom du point d'accès.
MTU	Unité de transmission maximale.
Données reçues	Quantité de données reçues via l'interface mobile
Données envoyées	Quantité de données transmises via l'interface mobile
Identifiant cellulaires(Cell ID)	L'identifiant de la cellule à laquelle le modem est actuellement connecté.
TAC	Le code de zone de suivi (TAC) est un identifiant numérique utilisé dans les réseaux LTE pour distinguer les différentes zones de suivi. Une zone de suivi est un groupe de cellules partageant la même identité à des fins de suivi et de localisation. Le TAC est un paramètre essentiel permettant à l'UE de déterminer sa position au sein du réseau LTE/5G.
ARFCN	Dans les réseaux cellulaires mobiles, un numéro de canal radiofréquence absolu (ARFCN) est un code qui spécifie une paire de porteuses radio physiques utilisées pour la transmission et la réception dans un système de radiocommunication mobile terrestre, une pour le signal de liaison montante et une pour le signal de liaison descendante.
Code Pays	Le code de pays mobile, 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 de 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) d'origine. Le MNC est attribué par l'autorité de régulation nationale.
Redémarrer la connexion	Permet de redémarrer le module Modem.

1.3.2 Menu STATUT > RÉSEAU> LAN

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



IPV4	
Adresse	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	
Interface	Interface qui a loué l'adresse
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 restante du bail	Durée restante du bail DHCP. Les titulaires de bail DHCP actifs tenteront de le renouveler après la moitié de sa durée restante.
Actions	Cette action réservera l'adresse IP actuellement attribuée à l'appareil.



IPV6	
Adresse	Adresse IP de l'interface LAN
Préfixe délégué	Le préfixe délégué est un sous-réseau plus petit attribué à un périphérique pour louer des adresses IPv6 à ses propres clients DHCPv6.
Baux DHCP	
Interface	Interface qui a loué l'adresse
Nom d'hôte	Nom d'hôte d'un client LAN
Adresse	Adresse IP d'un client LAN
Préfixe délégué	Le préfixe délégué est un sous-réseau plus petit attribué à un périphérique pour louer des adresses IPv6 à ses propres clients DHCPv6.
DUID	L'identifiant unique DHCP est utilisé par DHCPv6 pour identifier un appareil. Il est similaire à l'adresse MAC utilisée par DHCPv4.
Durée restante du bail	Durée restante du bail DHCP. Les titulaires de bail DHCP actifs tenteront de le renouveler après la moitié de sa durée restante.
Actions	Cette action réservera l'adresse IP actuellement attribuée à l'appareil dans Réseau -> Interfaces -> Baux statiques.

1.4 Menu STATUT > WIFI

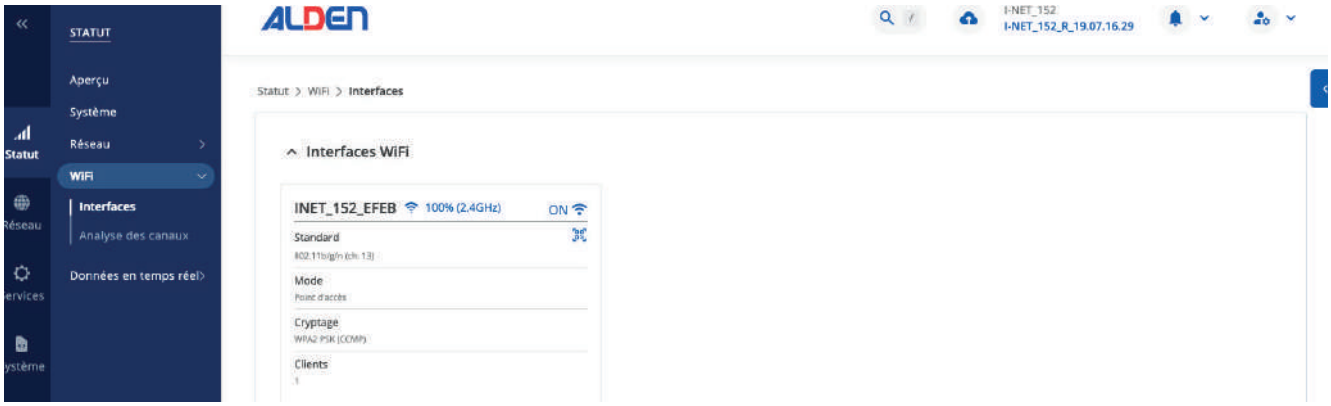
La page Sans fil contient des graphiques qui affichent en temps réel diverses variations des données sans fil. Ce chapitre du manuel d'utilisation présente un aperçu de la page WiFi pour le I-NET 152.

1.4.1 Menu STATUT > WIFI > INTERFACES

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

INTERFACES WIFI

La section Interfaces WiFi contient des widgets affichant l'état des interfaces sans fil de l'appareil.



CLIENTS WIFI

La section Clients WiFi affiche diverses informations sur toutes les sessions sans fil actives et permet d'expulser ou de bloquer les clients.



1.4.2 Menu STATUT > WIFI > ANALYSES DES CANAUX

La section « Analyse des canaux » affiche l'état de tous les réseaux sans fil disponibles à l'instant T.

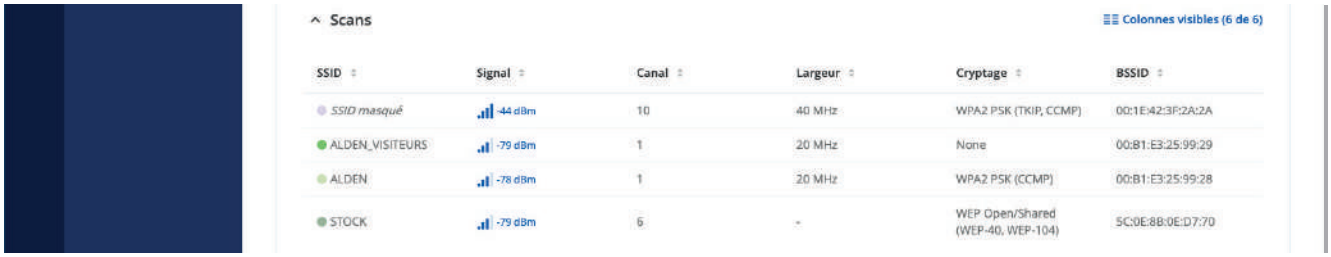
RÉPARTITION DES CANAUX

La section « Analyse des canaux » présente un diagramme interactif des bandes radio sujettes aux interférences, affichant en temps réel la répartition des canaux dans l'environnement. Pour lancer une analyse des interférences de canaux, appuyez sur le bouton « Effectuer un balayage».



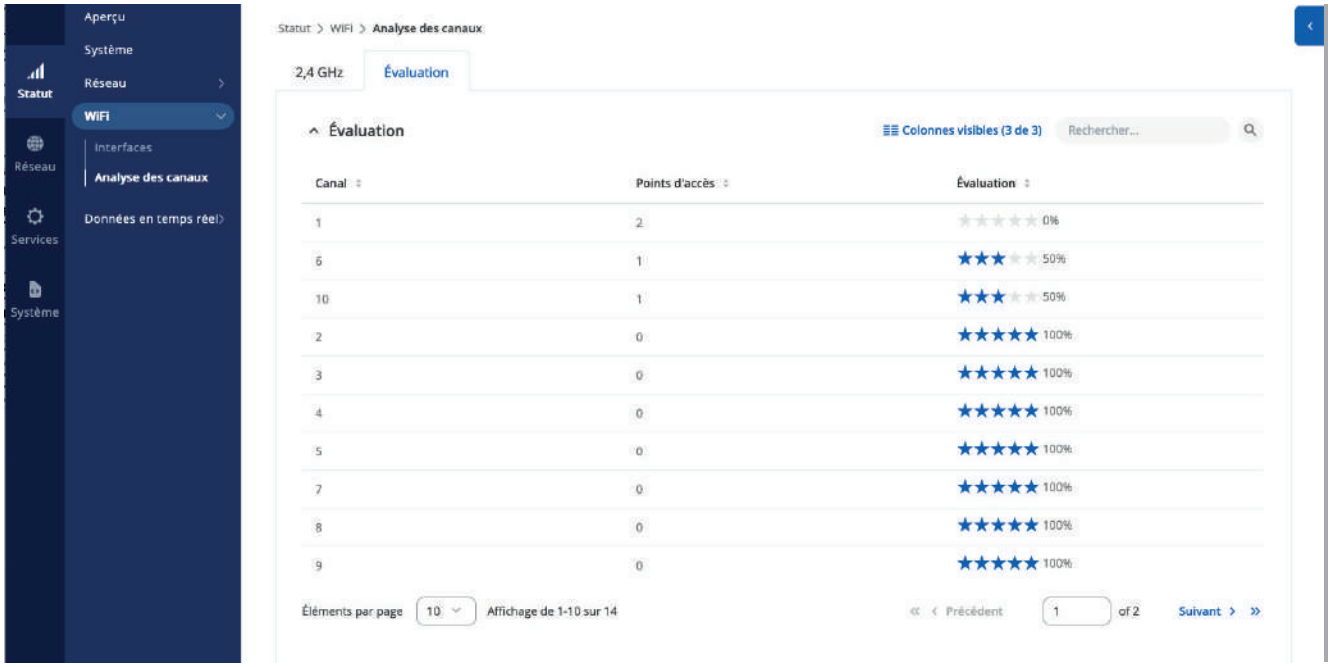
SCANS

La section «Scans» affiche le tableau des réseaux sans fil visibles. Ce tableau peut être trié par SSID, puissance du signal, canal, Largeur, Cryptage et BSSID. Exemple ci-dessous :



ÉVALUATION

L'onglet « Évaluation » indique la qualité de chaque canal des points d'accès sélectionnée. Moins il y a de bruit et de trafic sur le canal, meilleure est la qualité.



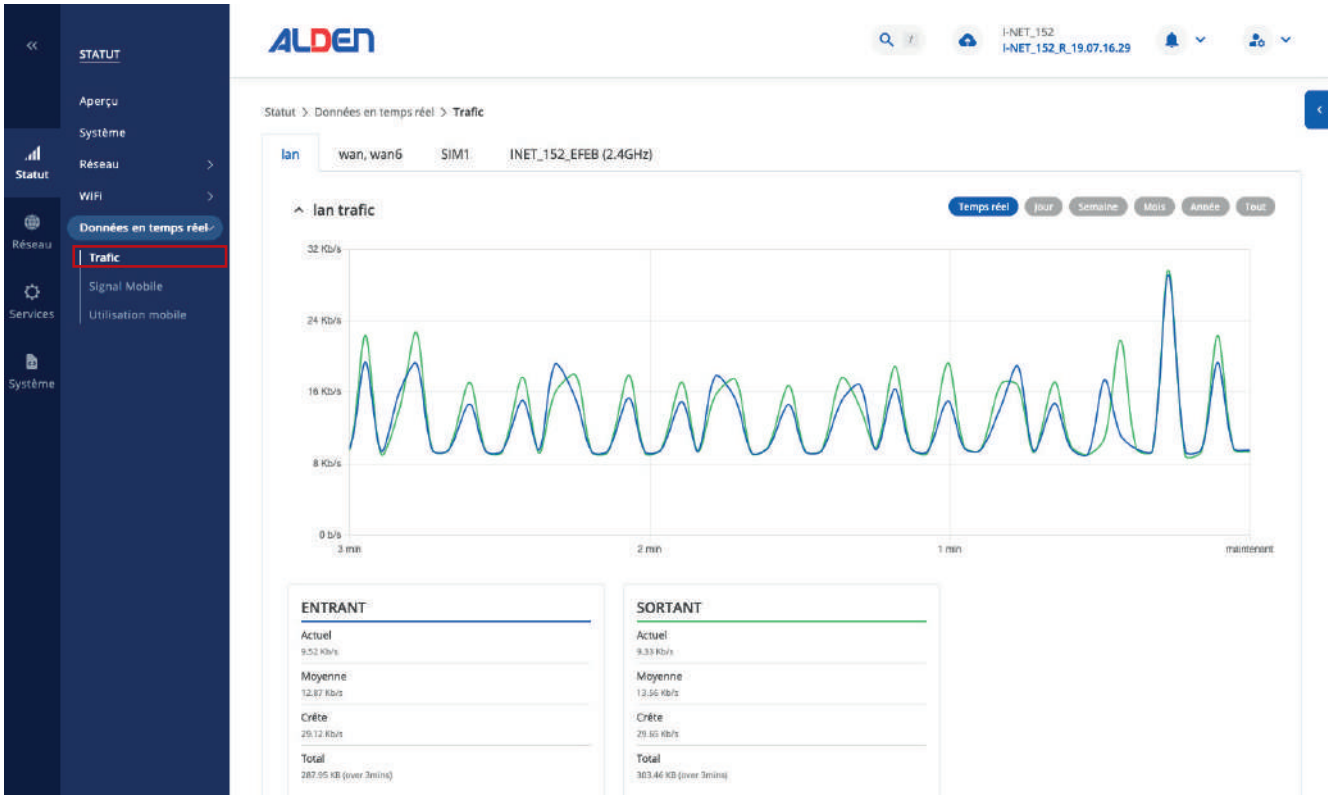
1.5. Menu STATUT > DONNÉES EN TEMPS RÉEL

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.

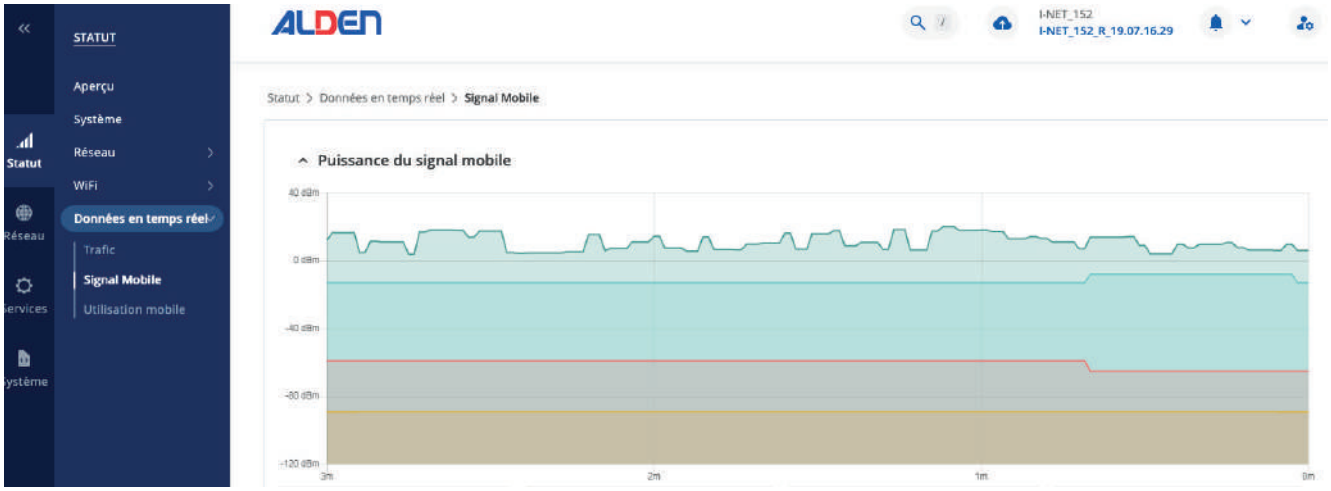
La figure ci-dessous est un exemple de graphique de trafic en temps réel pour la connexion LAN :



LAN	Affiche le trafic qui passe par la ou les interfaces réseau LAN.
WAN, WAN 6	Affiche le trafic passant par la connexion WAN filaire.
SIM1	Affiche le trafic passant par la connexion WAN mobile.
I-NET_152 XXX	Graphique cumulatif, qui englobe le LAN Ethernet câblé et WiFi.

1.5.2 Menu STATUT > DONNÉES EN TEMPS RÉEL > SIGNAL MOBILE

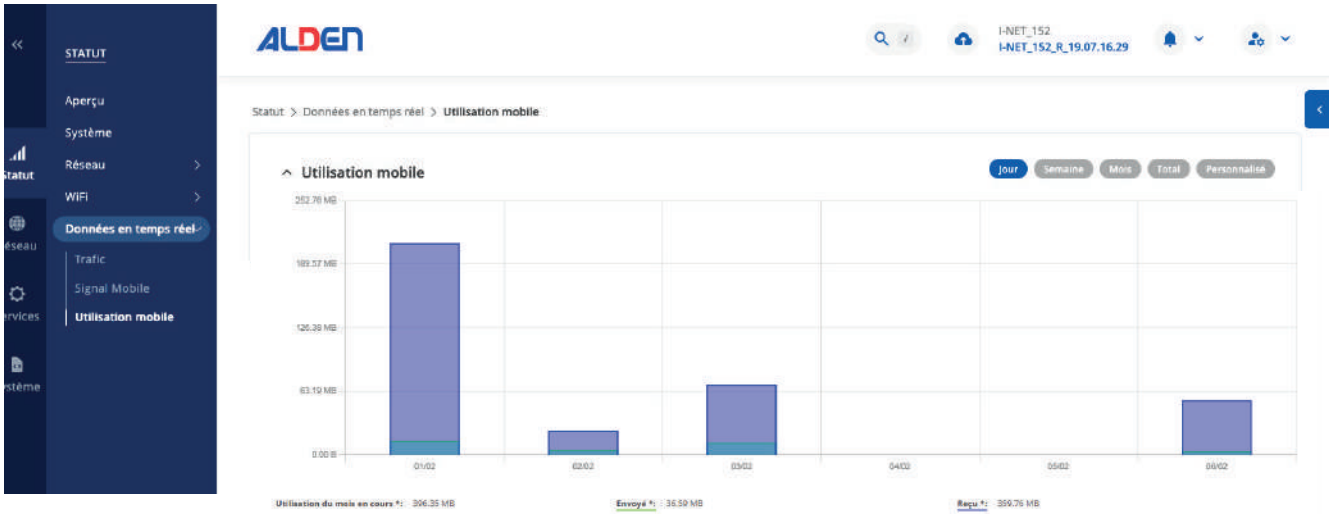
Le graphique Puissance du signal mobile affiche les variations de la valeur de l'intensité du signal cellulaire au fil du temps.



1.5.3 Menu STATUT > DONNÉES EN TEMPS RÉEL > UTILISATION MOBILE

La page « Utilisation mobile » contient des graphiques qui affichent les valeurs d'utilisation des données mobiles sur différentes périodes

Vous pouvez accéder à différentes pages pour afficher les valeurs d'utilisation des données mobiles sur différentes périodes



Mesure de signaux

Les niveaux du signal sont définies par différentes mesures, dépendant de différents modes de service. Les mesures sont les suivantes :

- RSSI
- RSRP
- RSRQ
- RSCP
- SINR
- EC/IO

Détermination des facteurs des valeurs de signal

Il existe de nombreux facteurs différents qui influencent la force et la qualité du signal :

- Charge sur le pylône émetteur
- Proximité de l'émetteur
- Signal passant par un répéteur cellulaire
- Signaux concurrents
- Barrières physiques (montagnes, bâtiments, trains, etc.)
- Météo

Par conséquent, des mesures telles que l'intensité du signal (RSSI) et la qualité du signal (EC/IO) n'intègrent pas tous les facteurs pertinents pour décrire la qualité de la connexion. Par exemple, vous pouvez avoir une excellente valeur RSSI de -51 dBm, mais la Tower Load (le nombre d'utilisateurs mobiles) à l'endroit où le routeur est connecté peut être très élevé. Dans ce cas, même si vous avez une bonne valeur de Force du signal, vous n'atteindrez peut-être pas les vitesses de données mobiles maximales.

Avis de non-responsabilité

- La force et la qualité du signal doivent être prises en compte pour une connexion de données cellulaire réussie.
- Les valeurs mesurées ou rapportées varient selon le modem, l'opérateur et l'environnement réseau.
- Il n'y a pas de réponse noir/blanc à ce qui constitue une connexion réussie.
- Bien que la force du signal puisse sembler adéquate, les vitesses de débit peuvent varier en fonction du nombre d'utilisateurs ou de pylônes émetteurs.

2G (GSM)

La puissance du signal 2G (GSM) est définie par une seule valeur : RSSI – Received Signal Strength Indicator ; RSSI est une valeur négative, plus proche de 0 est la valeur, plus le signal est fort.

RSSI	Force du signal	Description
>= -70dBm	Excellent	Signal fort avec des vitesses de données maximales
-70 dBm à -85 dBm	Bien	Signal fort avec de bonnes vitesses de données
-86 dBm à -100 dBm	Passable	Des vitesses de données passables mais utiles, rapides et fiables peuvent être atteintes, mais des données marginales avec des abandons sont possibles
< -100dBm	Pauvre	Les performances vont chuter drastiquement
-110dBm	Pas de signal	Coupure

3G (WCDMA, TDSCDMA, CDMA, EVDO, CDMA-EVDO)

Pour le mode de service 3G, il existe trois mesures pertinentes :

- RSSI – Indicateur de force du signal reçu. RSSI est une valeur négative, plus proche de 0 est la valeur, plus le signal est fort
- EC/IO – indique le rapport porteuse/interférence de la liaison descendante (qualité du signal). EC/IO est une valeur dBm négative. Plus les valeurs sont proche de 0, plus les signes sont forts.
- RSCP – indique la puissance du code du signal reçu

Les valeurs standard RSSI pour la 3G sont fondamentalement les mêmes que pour la 2G

RSSI	Force du signal	Description
>= -70dBm	Excellent	Signal fort avec des vitesses de données maximales
-70 dBm à -85 dBm	Bien	Signal fort avec de bonnes vitesses de données
-86 dBm à -100 dBm	Passable	Des vitesses de données passables mais utiles, rapides et fiables peuvent être atteintes, mais des données marginales avec des abandons sont possibles
< -100dBm	Pauvre	Les performances vont chuter drastiquement
-110dBm	Pas de signal	Coupure

EC/IO	Qualité du signal	Description
0 à -6	Excellent	Signal fort avec des vitesses de données maximales
-7 à -10	Bien	Signal fort avec de bonnes vitesses de données
-11 à -20	Passable à médiocre	Des vitesses de données fiables peuvent être atteintes, mais des données marginales avec des abandons sont possibles. Lorsque cette valeur se rapproche de -20, les performances chutent considérablement

4G (LTE)

Pour le mode service 4G, il existe quatre mesures pertinentes :

- RSSI – Indicateur de force du signal reçu. RSSI est une valeur négative, plus proche de 0 est la valeur, plus le signal est fort.
- SINR – Rapport signal sur bruit (un minimum de -20 dB SINR est nécessaire pour détecter RSRP/RSRQ). Indique la capacité de débit du canal. Comme son nom l'indique, SINR est la force du signal divisée par la force du bruit.

SINR	Force du signal	Description
>= 20 dB	Excellent	Signal fort avec des vitesses de données maximales
13 dB à 20 dB	Bien	Signal fort avec de bonnes vitesses de données
0 dB à 13 dB	Passable à médiocre	Des vitesses de données fiables peuvent être atteintes, mais des données marginales avec des abandons sont possibles. Lorsque cette valeur se rapproche de 0, les performances chutent considérablement
<= 0 dB	Pas de signal	Coupure

RSSI pour LTE est calculé à partir de plusieurs autres mesures liées au signal : RSSI = puissance large bande = bruit + puissance de la cellule de desserte + puissance du bruit. Par exemple, un modem 4G LTE peut signaler un RSSI de -68 dBm, mais : - SINR = -1,8 dB.

Dans ce cas, la qualité du signal est en fait très mauvaise. Cela peut être dû au fait que l'appareil est à une certaine distance de l'émetteur LTE. Il est également possible que quelque chose interfère avec le signal, comme un bâtiment ou d'autres obstacles entre l'appareil et le pylône.

RSSI	Force du signal	Description
> -65dBm	Excellent	Signal fort avec des vitesses de données maximales
-65 dBm à -75 dBm	Bien	Signal fort avec de bonnes vitesses de données
-75 dBm à -85 dBm	Passable	Des vitesses de données passables mais utiles, rapides et fiables peuvent être atteintes, mais des données marginales avec des abandons sont possibles
-85 dBm à -95 dBm	Pauvre	Les performances vont chuter drastiquement
<= -95dBm	Pas de signal	Coupure

2. Menu RÉSEAU

2.1 Menu RÉSEAU > MOBILE

La page Mobile permet de configurer les paramètres de connexion mobile.
Cette page du manuel fournit un aperçu de la page Mobile du routeur I-NET 152.

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.

Gestion de la carte SIM



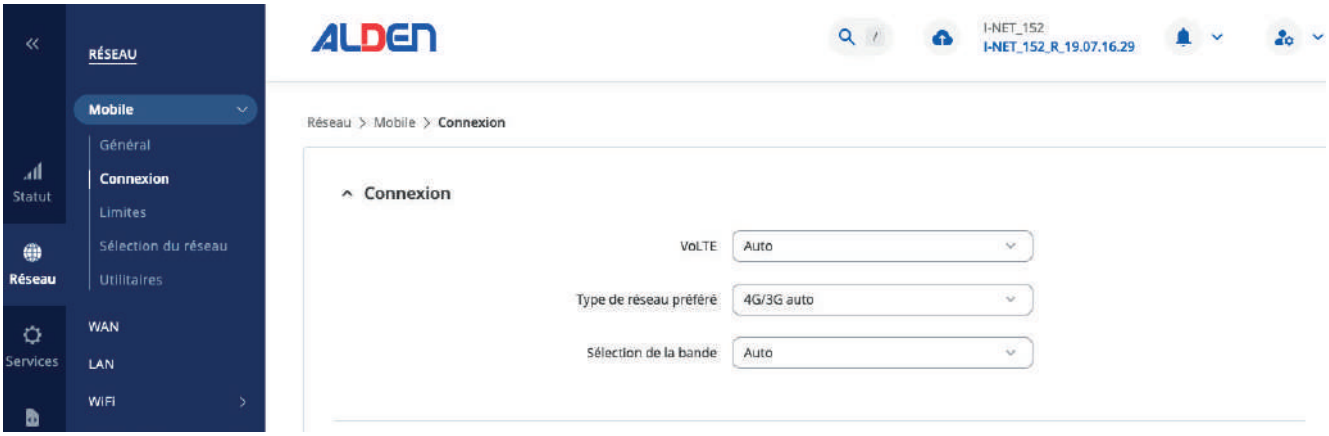
Refuser l'itinérance des données	Off | On ; Par défaut : Off	Refuse la connexion de données sur les conditions d'itinérance.
PIN	Par défaut : aucun	Le code PIN (Numéro d'Identification Personnel) d'une carte SIM est un mot de passe numérique secret permettant d'authentifier l'appareil auprès de la carte SIM. Ce code est composé uniquement de chiffres et peut comporter de 4 à 8 caractères. Le code PIN est enregistré dans la mémoire flash et n'est donc pas réinitialisé lors de la restauration des paramètres par défaut.

Configuration APN de l'interface SIM



Auto APN	Off | On Par défaut : On	La fonction Auto APN analyse une base de données APN 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, elle tente d'utiliser le suivant dans la base de données.
APN	Chaîne de caractères 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 l'utilisation d'un APN pour finaliser l'inscription au réseau. Dans d'autres cas, l'APN permet d'obtenir des paramètres spécifiques de l'opérateur (par exemple, une adresse IP publique), selon le contrat. Un identifiant de réseau APN ne peut pas commencer par les chaînes de caractères suivantes : • rac; • lac; • sgsn; • rnc; cela 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 pour authentifier les nouvelles connexions sur son réseau
Nom d'utilisateur	Chaîne de caractères Par défaut : vide	Nom d'utilisateur fourni par votre opérateur
Mot de passe	Chaîne de caractères Par défaut : vide	Mot de passe fourni par votre opérateur

2.1.2 Menu RÉSEAU > MOBILE > CONNEXION



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 préféré	4G/3G auto | 4G seulement | 3G seulement Par défaut : 4G/3G auto	Préférence de type de connexion réseau.
Sélection de la bande	Auto | Manuel Par défaut : Auto	Méthode de sélection de la bande de fréquence réseau. En mode automatique , l'appareil se connecte à la bande offrant les meilleures conditions de connectivité. En mode manuel, vous pouvez sélectionner manuellement les bandes que l'appareil utilisera. La sélection manuelle des bandes affiche uniquement leurs modes duplex pour les appareils compatibles 4G et 5G.
Bandes LTE	Liste des groupes Par défaut : vide	Bandes de fréquences prises en charge par le routeur I-NET152 et pouvant être sélectionnées dans la liste.
Bandes UMTS	Liste des groupes Par défaut : vide	Bandes de fréquences prises en charge par le routeur I-NET152 et pouvant être sélectionnées dans la liste.

Reconnexion sur signal faible

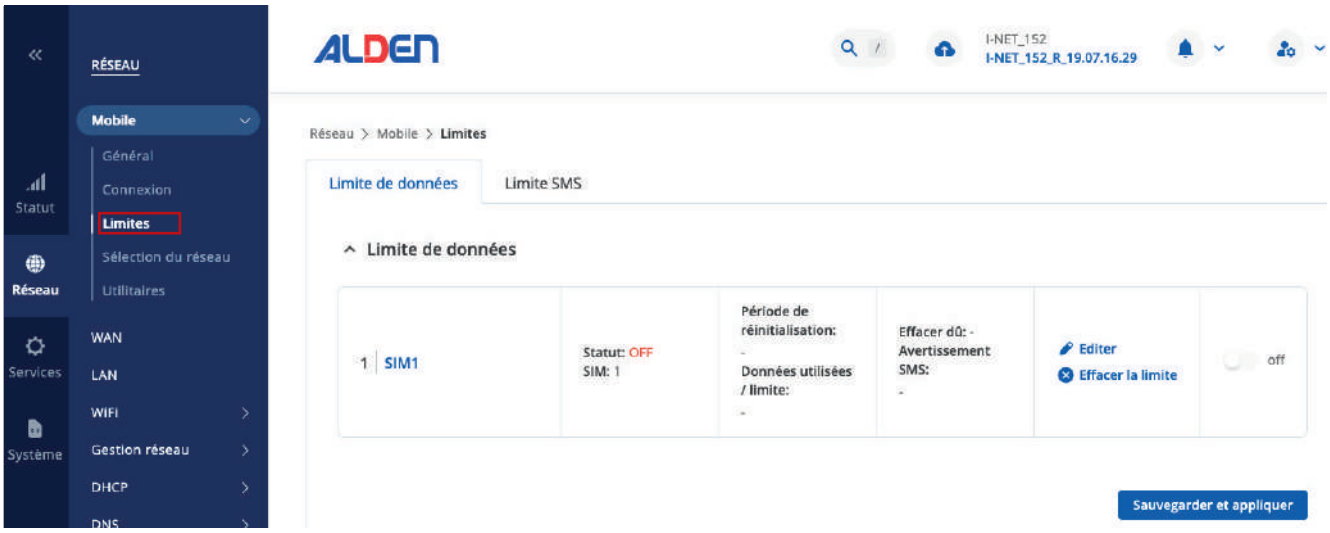


Activer	Off | On Par défaut : Off	Permet la reconnexion en cas de signal faible.
Seuil de réinitialisation	Entier [-120..-50] Par défaut :-90	Seuil de signal en dB pour la connexion. Lorsque le signal est inférieur à cette valeur, le modem réinitialise la connexion.
Délai de réinitialisation	Entier [15..65535] Par défaut : 600	Temps d'attente (en secondes) de l'appareil avant de tenter à nouveau de réinitialiser la connexion.

2.1.3 Menu RÉSEAU > MOBILE > LIMITES

Limites de données

La section « Limite de données » vous permet de définir une limite maximale de données utilisées pour votre carte SIM.



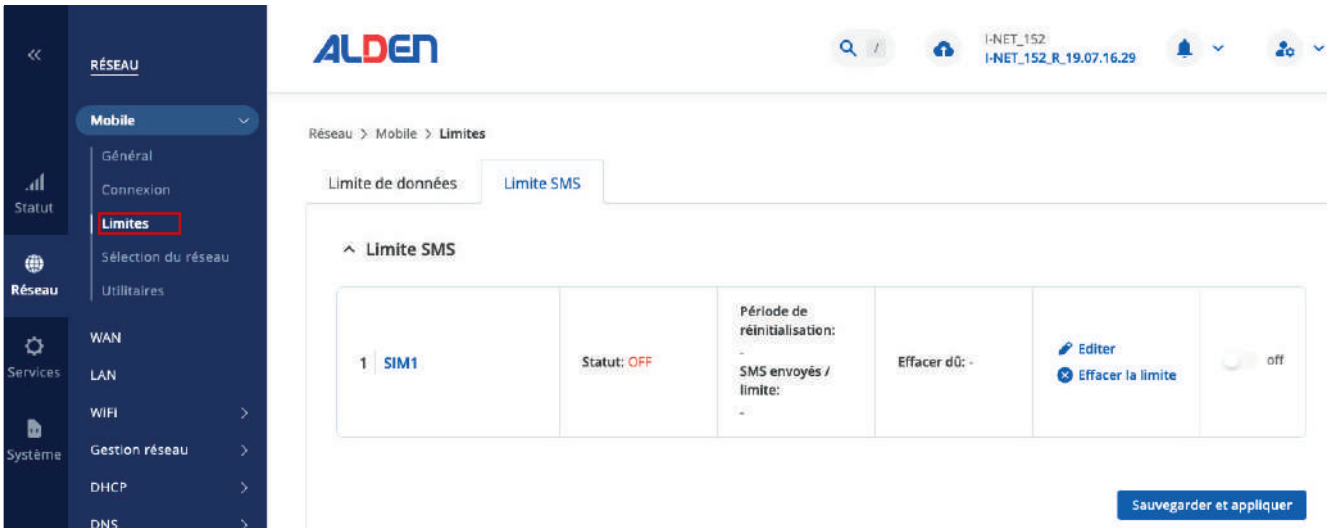
Pour configurer la limite de données, appuyez sur Editer.



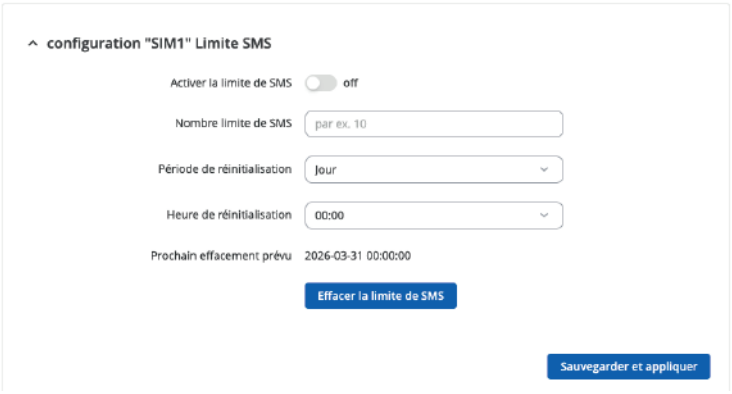
Activer la limitation de la connexion de données	Off | On Par défaut : Off	Désactive les données mobiles lorsque la limite pour la période en cours est atteinte.
Limite de données (MB)	Entier ; valeur Par défaut : aucun	Désactiver les données mobiles une fois la limite de Mo atteinte.
Période de réinitialisation	Jour | Semaine | Mois Par défaut : Jour	Intervalle de réinitialisation de la limite d'utilisation des données mobiles.
Heure de réinitialisation	0-23 / Lundi - Dimanche / 0-31 Valeur par défaut : 0	Indiquez l'heure (au format 24 heures) à laquelle la limite de données mobiles est réinitialisée.
Activer l'avertissement SMS	Off | On Par défaut : Off	Permet l'envoi d'un SMS d'avertissement lorsque la limite de données mobiles est atteinte.
Seuil d'avertissement	Entier ; valeur Par défaut : aucun	Un SMS d'avertissement est envoyé lorsque le seuil en Mo est atteint. Ce seuil ne peut pas dépasser la limite de données !
Numéro de téléphone	Entier ; valeur Par défaut : aucun	Un numéro de téléphone pour envoyer un SMS d'avertissement.
Activer la limite de débit	Off | On Par défaut : Off	Activer la limite de débitActive les règles de limitation de bande passante lorsque la limite de données indiquée est atteinte.
Limite de téléchargement	Par défaut : aucun	Limitation de bande passante de téléchargement en Kbps.
Limite de Chargement	Par défaut : aucun	Limitation de bande passante en upload en Kbps.
Supprimer les données collectées	- (bouton interactif)	Les données collectées pour cette interface seront effacées, mais seulement si l'interface est active.

Limite SMS

La section « Limite SMS » vous permet de définir une limite maximale de SMS envoyés pour votre carte SIM.



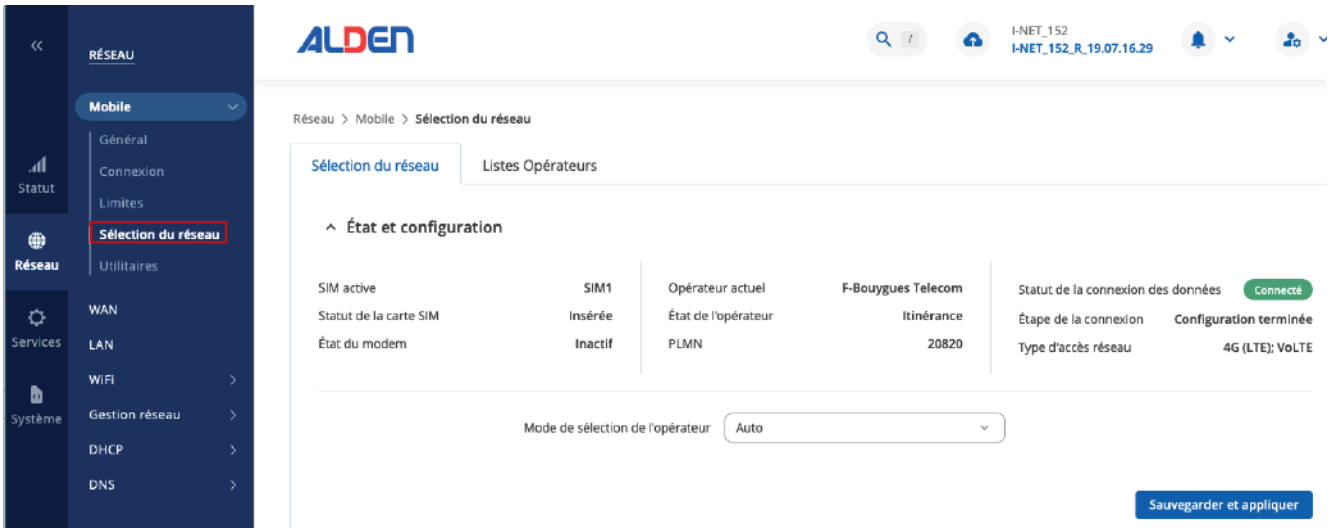
Pour configurer la limite de SMS, appuyez sur Editer.



Activer la limite de SMS	Off | On Par défaut : Off	Active ou désactive la limitation des SMS.
Nombre limite de SMS	Entier ; Par défaut : aucun	Définit la limite d'envoi de SMS, c'est-à-dire le nombre de SMS pouvant être envoyés depuis cette carte SIM pendant la période spécifiée.
Période de réinitialisation	Jour | Semaine | Mois Par défaut : Jour	Période pendant laquelle la limitation des SMS s'applique. Une fois cette période écoulée, le compteur de SMS sera réinitialisé.
Heure de réinitialisation	0–23 Par défaut : 0	Spécifiez l'heure (au format 24 heures) à laquelle la réinitialisation de la limite de SMS se produit
Limite de SMS effacée	- (bouton interactif)	Efface le compteur de limites de SMS pour la période sélectionnée.

2.1.4 Menu RÉSEAU > MOBILE > SÉLECTION DU RÉSEAU

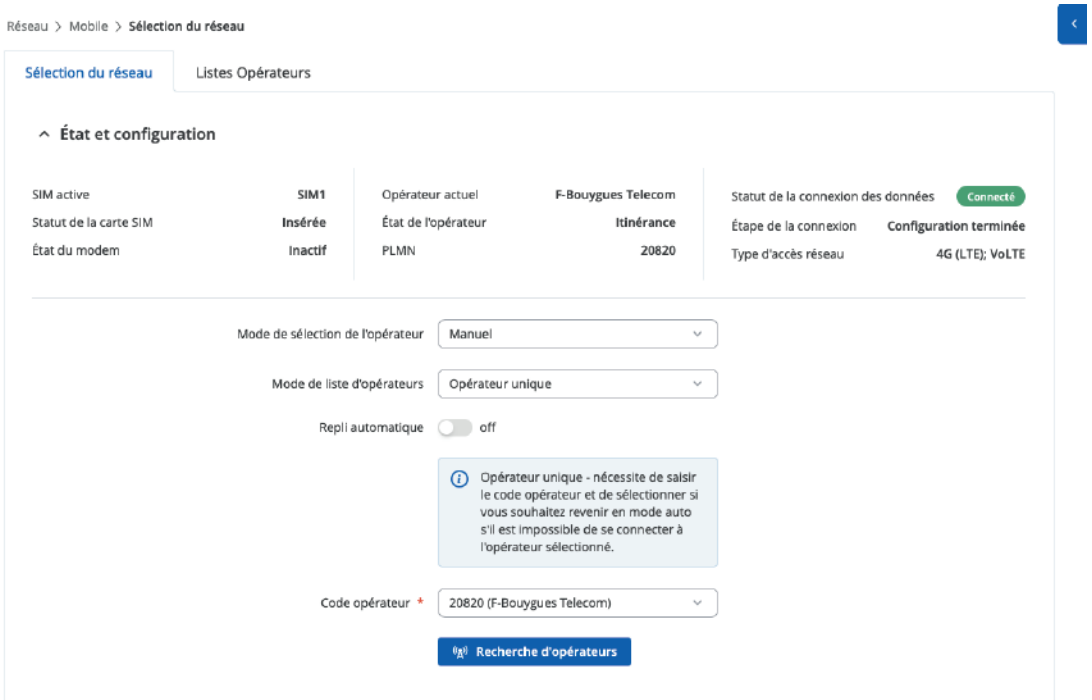
La section « Sélection du réseau » vous permet de rechercher et de gérer les opérateurs de réseaux mobiles auxquels la carte SIM de l'appareil peut se connecter.



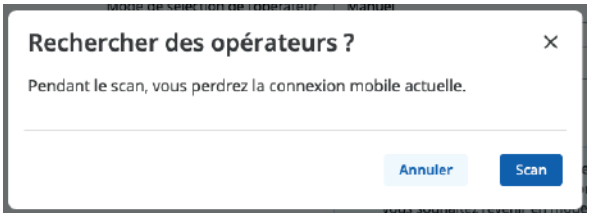
Mode de sélection de l'opérateur	Auto | Manuel Par défaut : Auto	Méthode de sélection de l'opérateur. • Mode Auto – sélectionne automatiquement l'opérateur. • Mode Manuel : vous devez sélectionner l'opérateur manuellement.

Sélection manuelle de l'opérateur

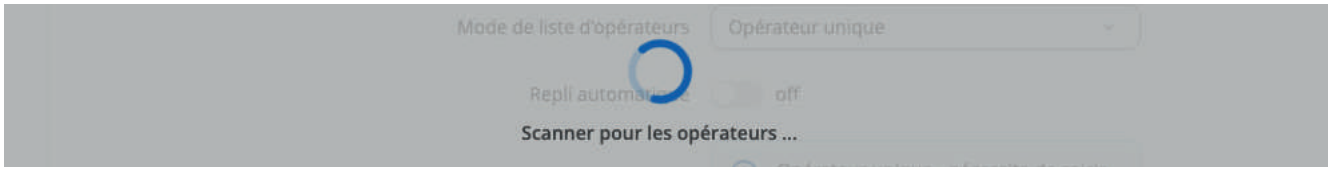
Pour sélectionner un opérateur manuellement, spécifiez le Mode de sélection de l'opérateur : Manuel et cliquez sur « Recherche d'opérateurs » .



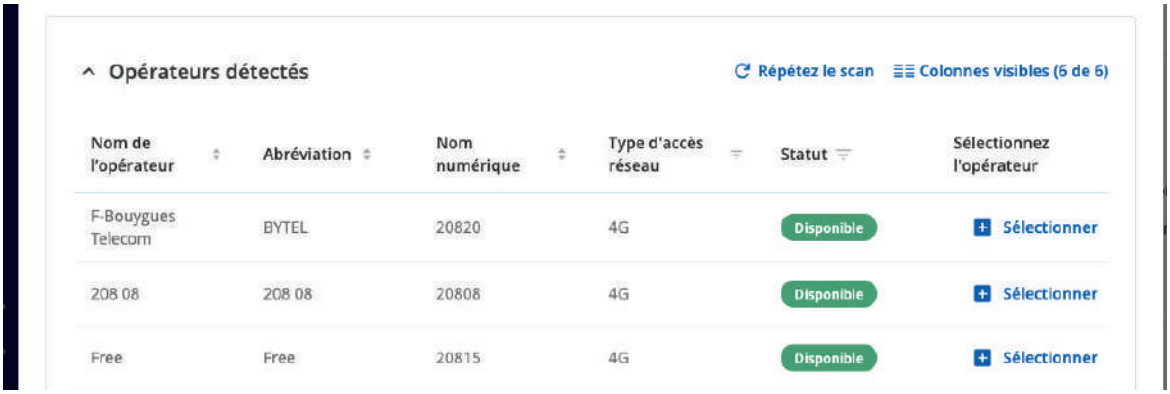
Une fenêtre contextuelle vous demandera confirmation. Cliquez sur « Scan » pour continuer.



Veuillez patienter jusqu'à la fin de l'analyse. Comme indiqué par le message à l'écran, cette opération peut prendre jusqu'à 3 minutes.



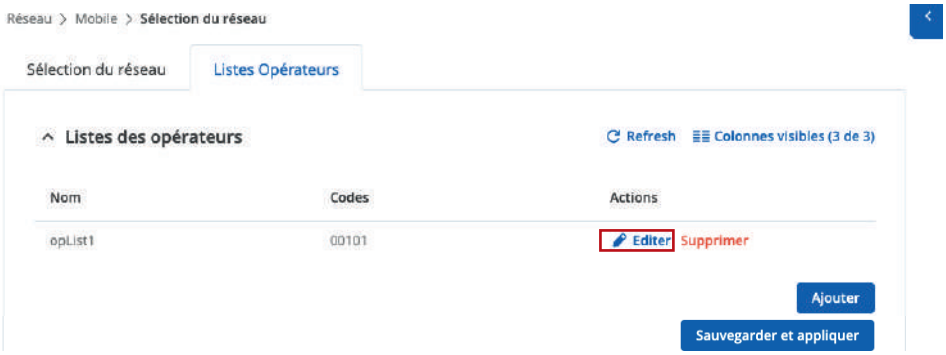
Une fois l'analyse terminée, vous verrez les résultats dans la section « Opérateurs détectés ».



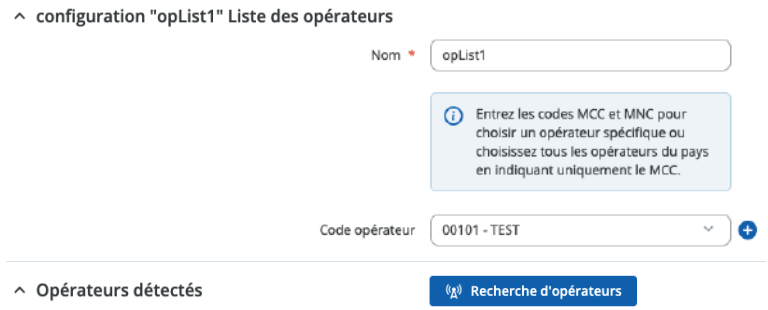
Pour verrouiller la carte SIM sur un seul opérateur, sélectionnez l'opérateur dans le champ « Sélectionnez l'opérateur » et cliquez sur « Sélectionner ».

Liste opérateurs

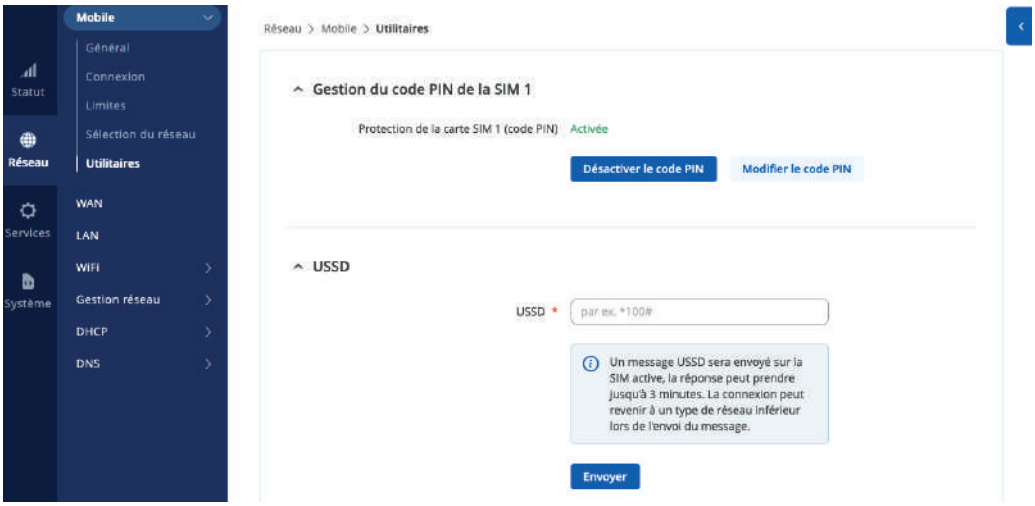
Cette section permet de créer des listes de codes d'opérateurs, qui peuvent ensuite être utilisées dans la section « Paramètres des opérateurs » pour les autoriser ou les bloquer. Un code d'opérateur se compose de deux parties : le code de pays mobile (MCC) et le code de réseau mobile (MNC).



En cliquant sur « Editer » dans une liste, vous serez redirigé vers une page de modification où vous pourrez saisir les codes d'opérateur pour cette liste.



2.1.5 Menu RÉSEAU > MOBILE > UTILITAIRES
GESTION DU CODE PIN DE LA CARTE SIM



Protection de la carte SIM 1 (code PIN)	Désactivé | Activé Par défaut : désactivé	Un code PIN correct est requis pour activer ou désactiver le verrouillage de la carte SIM. Une fois le verrouillage désactivé, vous n'aurez plus besoin de saisir de code PIN sur aucun appareil pour utiliser la carte SIM.
Modifier le code PIN	- (bouton interactif)	Ouvrez la fenêtre modale pour modifier le code PIN de la carte SIM

USSD

Le protocole USSD (Unstructured Supplementary Service Data) est un protocole de communication utilisé entre les appareils cellulaires et les opérateurs de réseaux mobiles. Il est généralement utilisé avec les cartes SIM prépayées pour activer ou désactiver certains services ou pour obtenir des informations auprès de l'opérateur.

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

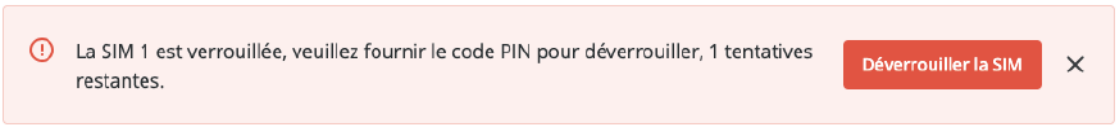


USSD	Chaîne de caractères Par défaut : aucun	Saisissez un code USSD (182 caractères maximum) à envoyer. Pour ce faire, cliquez sur le bouton « Envoyer » situé sous la zone de réponse.
Envoyer	- (bouton interactif)	Cliquez pour envoyer le message saisi dans le champ USSD.

Notification de verrouillage par code PIN/PUK

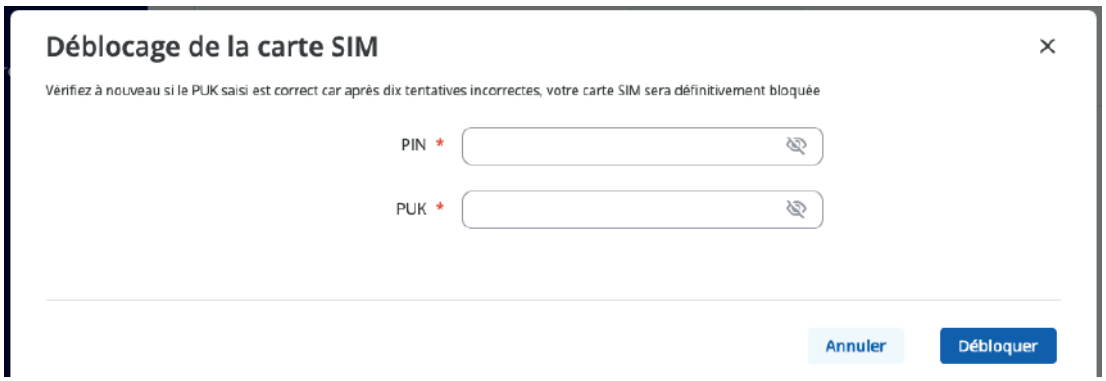
Si vous saisissez un code PIN/PUK invalide ou si vous insérez une carte SIM verrouillée/bloquée, un message s'affichera pour vous informer que la carte SIM est verrouillée ou bloquée. Cliquez sur « Déverrouiller la carte SIM ici » pour ouvrir la fenêtre modale où vous pourrez saisir les codes PIN/PUK de la carte SIM.

Message latéral indiquant que la carte SIM est verrouillée



Message annexe : la carte SIM est bloquée.



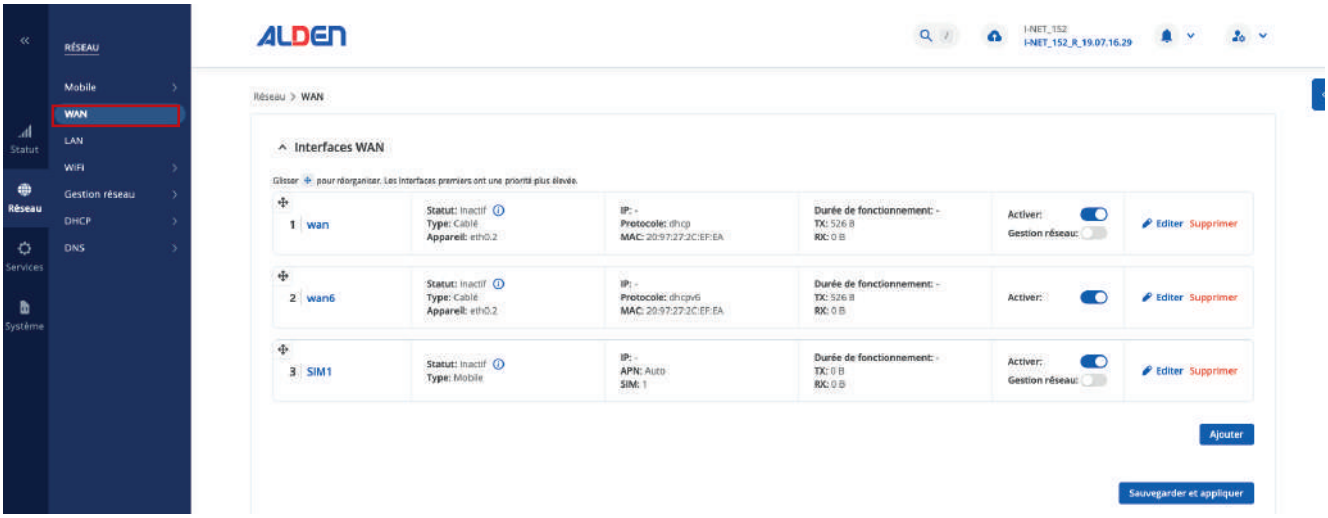


PIN	4 à 8 caractères numériques positifs (nombre positif) Par défaut : aucun	Le code PIN (numéro d'identification personnel) d'une carte SIM est un mot de passe numérique secret partagé entre un utilisateur et un système, permettant d'authentifier l'utilisateur. Ce code PIN est enregistré dans la mémoire flash et sera conservé même après la réinitialisation de l'appareil.
PUK	8 caractères numériques positifs (nombre positif) Par défaut : aucun	Le code PUK (Personal Unblocking Key) de votre carte SIM est un code à 8 chiffres. Il sert à débloquer votre carte SIM après avoir saisi un code PIN erroné à trois reprises.

2.2 Menu RÉSEAU > WAN

La page WAN est utilisée pour visualiser et configurer les interfaces réseau WAN. Ces dernières sont utilisées pour connecter l'appareil à différents réseaux externes.

La section WAN affiche les interfaces réseau actuellement disponibles sur cet appareil.



Vous pouvez activer ou désactiver les interfaces, modifier leur niveau de priorité* ou accéder à la page de configuration d'une interface.

* Modifier le niveau de priorité en faisant glisser et en déposant une interface vers une autre position. Le déplacement d'une interface modifie sa valeur métrique dans le fichier de configuration. Les interfaces qui sont plus hautes dans la liste ont une plus grande priorité.

Paramétrage des interfaces

Cette section fournit des informations sur la configuration de l'interface WAN. Par défaut, il existe deux types d'interfaces WAN sur l'appareil :

- WAN Ethernet
- Réseau étendu mobile

Chacun prend en charge différents types de protocoles et de configurations, qui sont décrits dans les sections ci-dessous.

	Statique	DHCP	DHCPv6	PPPoE	Mobile
WAN Ethernet	✓	✓	✓	✓	
Réseau étendu mobile					✓

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



CONFIGURATION INTERFACE

La section « Configuration interface» permet de configurer le protocole d'une interface ainsi que tous les paramètres associés. Si aucun protocole n'est sélectionné, tous les autres paramètres d'interface seront ignorés. Les sections suivantes diffèrent selon le protocole.

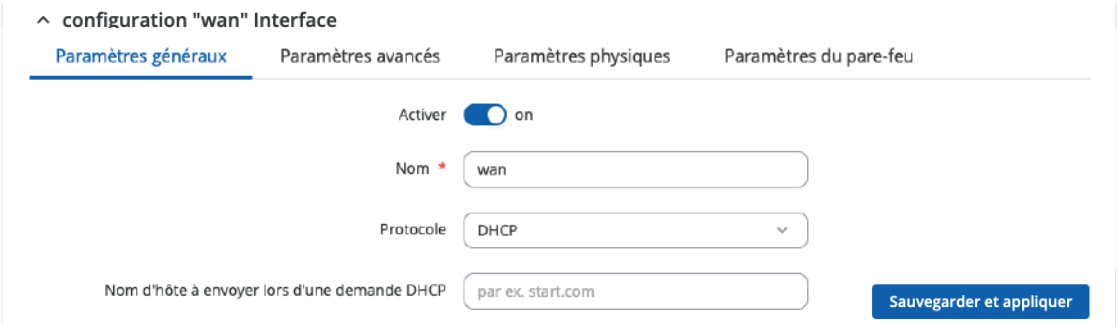
Paramètres Généraux : Protocole statique

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



Activer	Off | On Par défaut : On	Activer l'interface.
Adresse IPv4	ip4 Par défaut : aucun	L'interface d'adresse IPv4 de cette interface. Une adresse IP identifie un périphérique sur un réseau et lui permet de communiquer avec d'autres périphériques.
Masque de sous-réseau IPv4	Par défaut : 255.255.255.0	Le masque de sous-réseau IPv4 de cette interface. Un masque de sous-réseau sert à 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	ip4 Par défaut : aucun	Adresse de passerelle IPv4 utilisée par cette interface. La passerelle par défaut d'une interface est l'adresse par laquelle transite tout le trafic sortant.
Diffusion IPv4	ip4 Par défaut : aucun	Adresse de diffusion IPv4 utilisée par cette interface. Les diffusions IP sont utilisées par les clients BOOTP et DHCP pour trouver leurs serveurs respectifs et leur envoyer des requêtes.
Serveurs DNS	ip4 Par défaut : aucun	Adresses des serveurs DNS que cette interface utilisera. Si ce champ est laissé vide, les serveurs DNS sont attribués automatiquement.

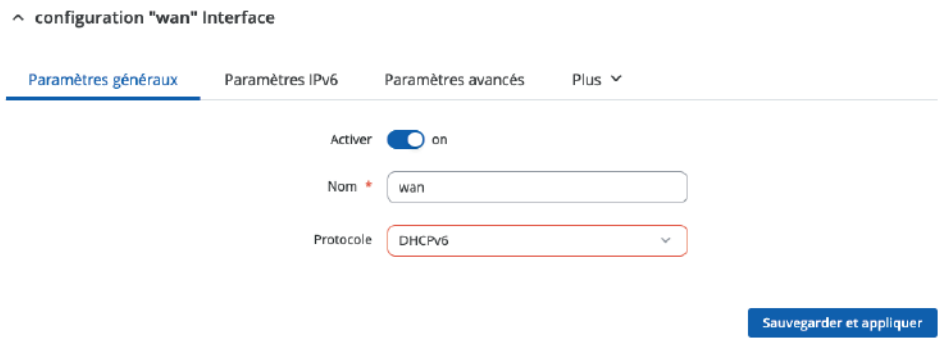
Paramètres Généraux : Protocole DHCP



Activer	Off | On Par défaut : On	Activer l'interface.
Nom d'hôte à envoyer lors dd'une demande DHCP	chaîne de caractères Par défaut : aucun	Nom d'hôte de cette interface utilisé pour identifier cette machine sur le serveur DHCP.

Paramètres Généraux : Protocole DHCPV6

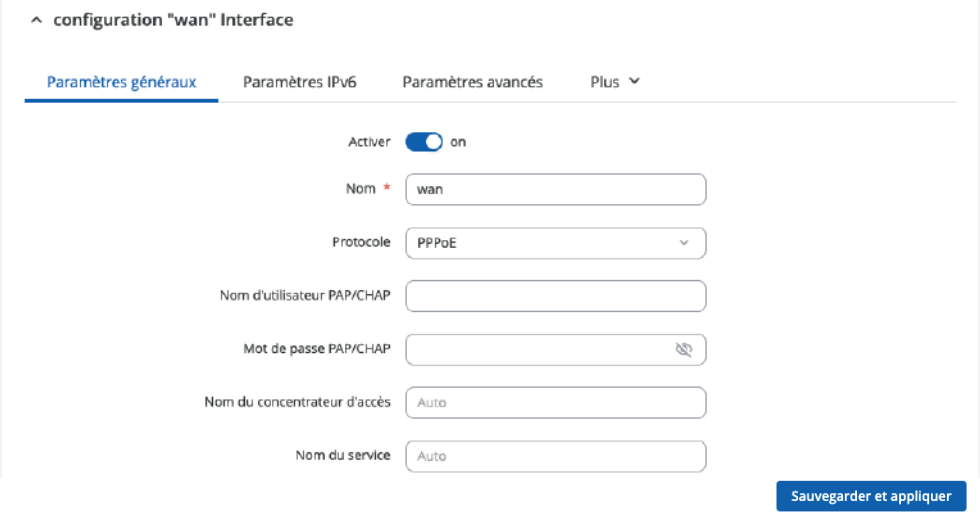
Le protocole DHCPv6 est utilisé pour configurer une interface IPv6 qui obtient automatiquement ses paramètres de configuration via un bail DHCP.



Activer	Off | On Par défaut : On	Activer l'interface.

Paramètres Généraux : Protocole PPPoE

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

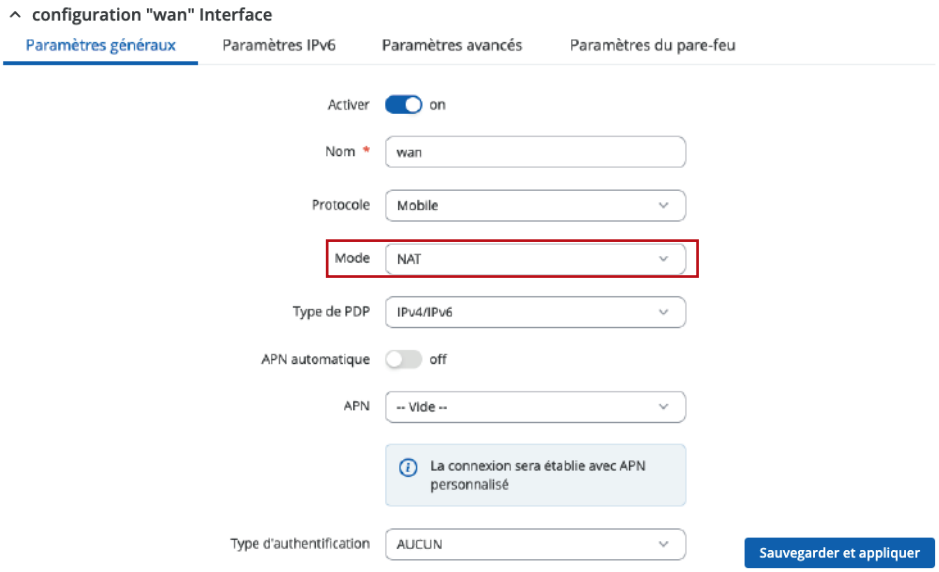


Activer	Off | On Par défaut : On	Activer l'interface.
Nom d'utilisateur PAP/CHAP	Chaîne de caractères Par défaut : aucun	Le nom d'utilisateur que vous utilisez pour vous connecter au réseau de votre opérateur.
Mot de passe PAP/ CHAP	Chaîne de caractères Par défaut : aucun	Le mot de passe que vous utilisez pour vous connecter au réseau de votre opérateur.
Nom du concentrateur d'accès	Chaîne de caractères Par défaut : aucun	Le concentrateur d'accès auquel se connecter. Les fournisseurs d'accès Internet utilisent des concentrateurs d'accès pour acheminer leurs connexions PPPoE. Généralement, les paramètres sont reçus automatiquement ; toutefois, dans certains cas, il est nécessaire de spécifier le nom du concentrateur d'accès. Laissez ce champ vide pour que les concentrateurs d'accès soient détectés automatiquement.
Nom du service	Chaîne de caractères Par défaut : aucun	Nom du service auquel se connecter. Laisser vide pour que le nom du service soit détecté automatiquement.

Paramètres Généraux : Protocole Mobile

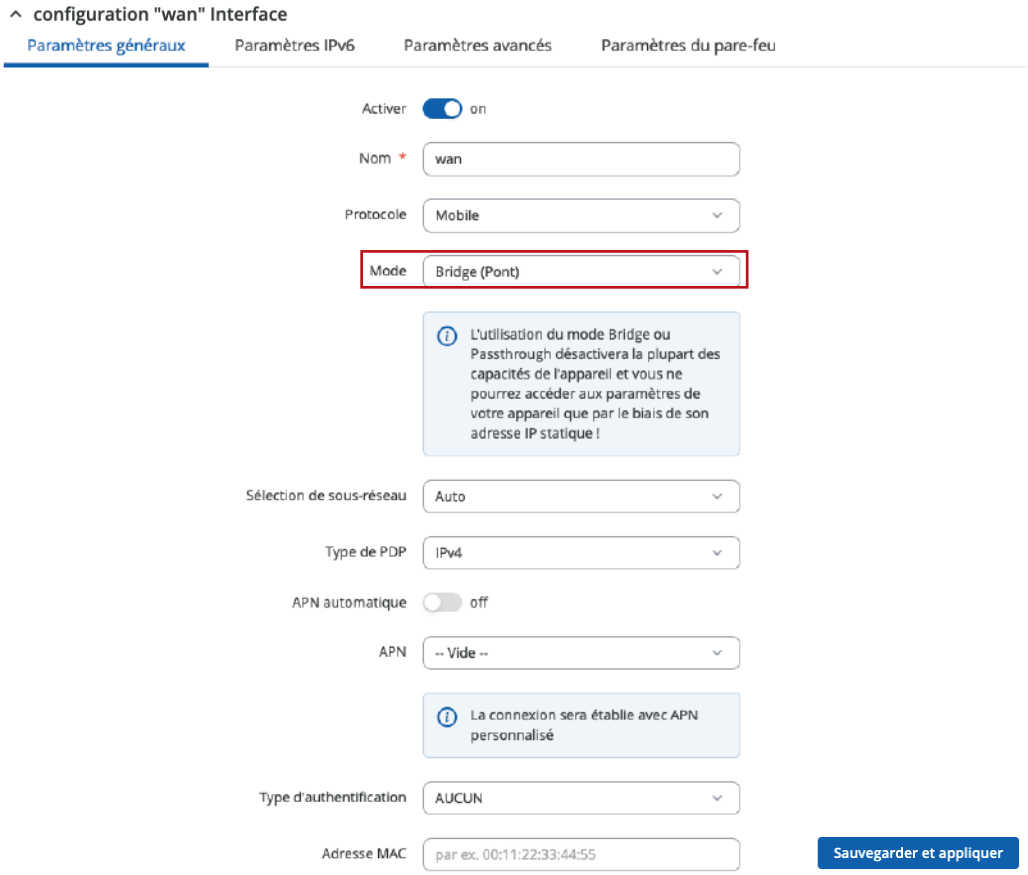
Le protocole mobile est utilisé pour configurer une interface permettant d'établir une connexion WAN mobile.

- **Mode : NAT**



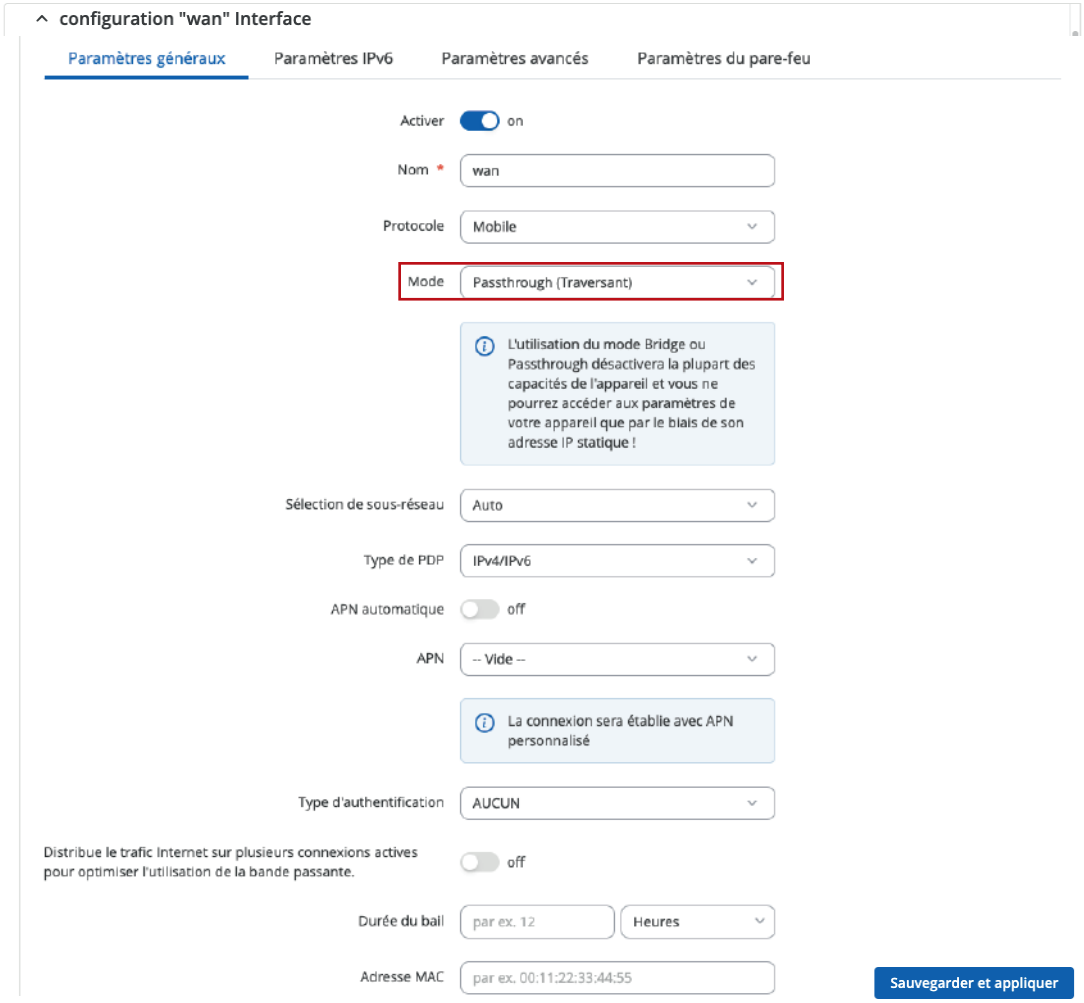
Mode	NAT | Bridge (Pont) | Passthrough Transparence) Par défaut : NAT	Mode de fonctionnement de la connexion mobile. • **NAT** – la connexion mobile utilise NAT (traduction d'adresse réseau). • **Bridge** – relie la connexion de données LTE au LAN. L'appareil attribue son adresse IP WAN à un autre appareil (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 152 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 152 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/IPv6	Spécifie quelles informations d'adresse seront demandées à l'opérateur.
APN automatique	Off | On; Par défaut : Off	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	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)**



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/IPv6	Spécifie quelle adresse sera demandée à l'opérateur.
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 / APN personnalisé	Chaîne; 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'identification	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)**



Sélection de sous-réseau	Auto | 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.
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, elle tente d'utiliser le suivant dans la base de données.
APN	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'identification	AUCUN | PAP | TYPE ; 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.

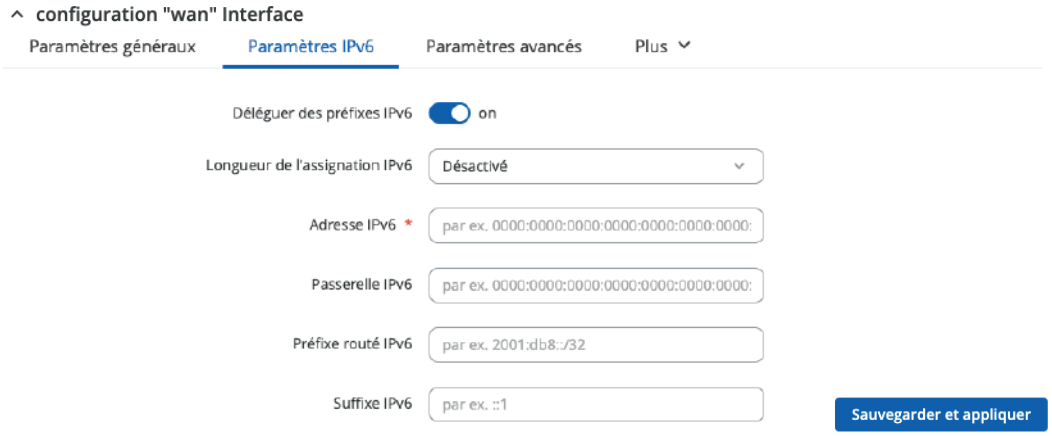
Désactiver DHCP	On | Off ; Par défaut : On	Désactive l'allocation dynamique des adresses client lorsqu'elle est désactivée
Durée du bail	Valeur ; Par défaut : 1	Heure d'expiration de l'adresse allouée. La valeur minimale pour les heures est 1, la valeur minimale pour les minutes est 2 et la valeur minimale 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 » permet de configurer certains paramètres d'interface plus spécifiques et moins fréquemment utilisés. Cette section diffère selon le protocole.

Paramètres IPv6 : Protocole Statique

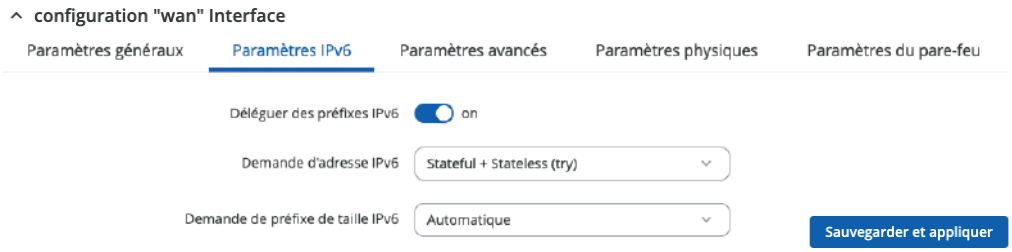
Les informations relatives aux paramètres généraux du protocole statique sont fournies dans le tableau ci-dessous.



Déléguer les préfixes IPv6	Off | On ; Par défaut : Off	Activer la délégation en aval des préfixes IPv6 disponibles sur cette interface.
Longueur de l'assignation IPv6	Désactivé | 64 | Personnalisé ; 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 maximale).
Adresse IPv6	Les adresses IPv6 avec ou sans masque de préfixe sont acceptées Par défaut : aucun.	Attribue une adresse IPv6 à cette interface. Notation CIDR : adresse/préfixe.
Passerelle IPv6	Les adresses IPv6 sont acceptées. 00:8a2e:0370:7334 Par défaut : aucun	Passerelle par défaut IPv6.
Préfixe routé IPv6	Par défaut : aucun	Préfixe public acheminé vers ce périphérique pour distribution aux clients. Les adresses IPv6 avec préfixe de masque sont acceptées, par exemple ::1/128
Suffixe IPv6	Par défaut : aucun	Optionnel. Valeurs autorisées : « eui64 », « random », valeur fixe comme « ::1 » ou « ::1:2 ». Lorsqu'un préfixe IPv6 (comme «a:b:c:d::») est reçu d'un serveur délégué, utilisez le suffixe (comme « ::1 ») pour former l'adresse IPv6 (« a:b:c:d::1 ») de l'interface.

Paramètres IPv6 : Protocole DHCPV6

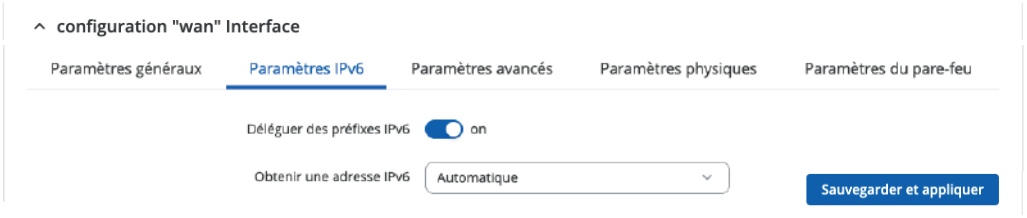
Les informations relatives aux paramètres généraux du protocole DHCPv6 sont fournies dans le tableau ci-dessous.



Déléguer les préfixes IPv6	Off | On Par défaut : On	Activer la délégation en aval des préfixes IPv6 disponibles sur cette interface.
Demande d'adresse IPv6	Stateful + Stateless | Stateful | Stateless uniquement Par défaut : Stateful + Stateless	Définit le comportement à adopter lors de la demande d'une adresse.
Préfixe IPv6 de longueur demandée	Entier [0.64] | Automatique | désactivé ; Par défaut : Automatique	Définit la manière dont la longueur du préfixe ULA IPv6 sera demandée. Si cette option est désactivée, l'interface obtiendra une seule adresse IPv6 sans sous-réseau pour le routage.

Paramètres IPv6 : Protocole PPPoE

Les informations relatives aux paramètres généraux du protocole PPPoE sont fournies dans le tableau ci-dessous.



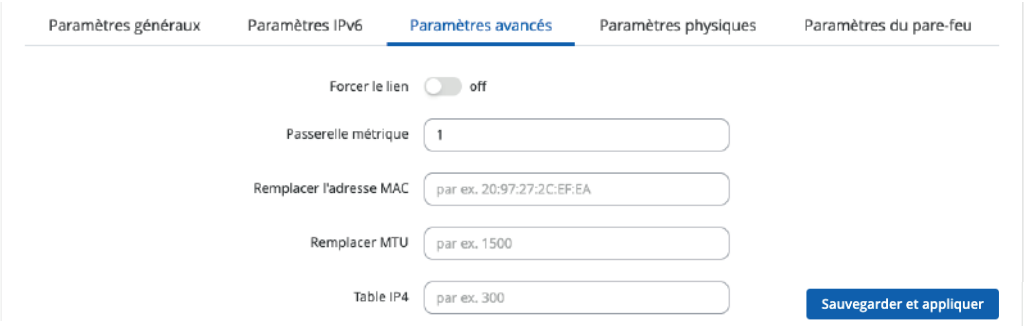
Déléguer les préfixes IPv6	Off | On Par défaut : On	Activer la délégation en aval des préfixes IPv6 disponibles sur cette interface.
Obtenir une adresse IPv6	Automatique | Désactivé | Manuel Par défaut : Automatique	Définit le comportement à adopter pour obtenir une adresse IPv6.

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

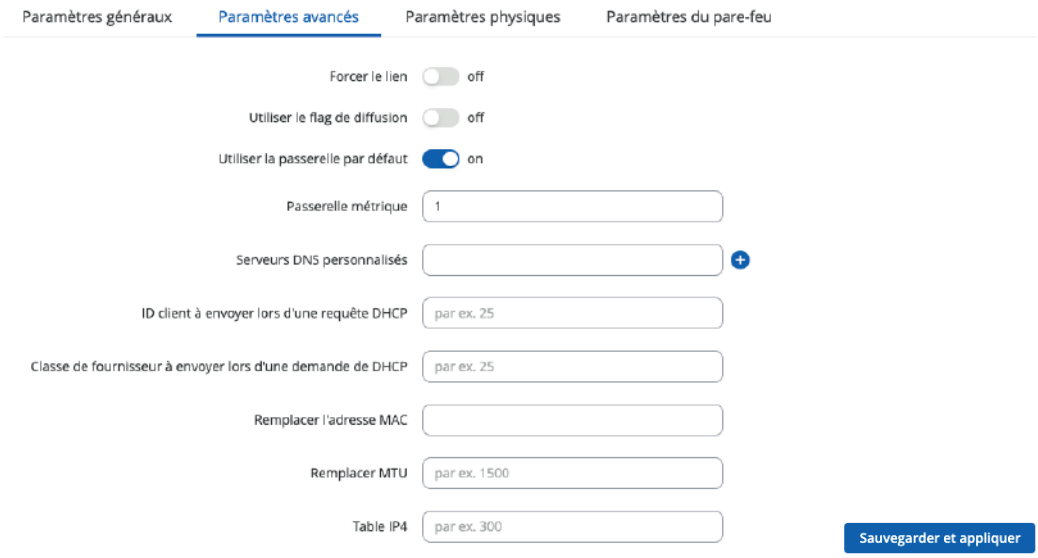
Les informations sur les paramètres avancés pour le protocole statique sont fournies dans le tableau ci-dessous.



Forcer le lien	Off | On Par défaut : Off	Indique si les paramètres d'interface (IP, route, passerelle) sont attribués à l'interface indépendamment de l'activité de la liaison ou seulement après que celle-ci soit devenue active.
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 maximale).
Remplacer l'adresse MAC	Mac Par défaut : aucun	Lorsqu'elle est activée, cette option utilise une adresse MAC définie par l'utilisateur pour l'interface au lieu de celle par défaut.
Remplacer l'unité de transmission maximale (MTU)	Entier [1..9200] Par défaut : aucun	Modifie la taille maximale des unités de transmission (MTU) autorisées pour les interfaces. Il s'agit de la taille maximale d'une unité de données de protocole (PDU) pouvant être transmise lors d'une seule transaction de couche réseau.
Tableau IP4	Par défaut : aucun	ID de la table de routage dans la page Tables de routage .

Paramètres avancés : protocole DHCP

Les informations relatives aux paramètres avancés du protocole DHCP sont fournies dans le tableau ci-dessous.

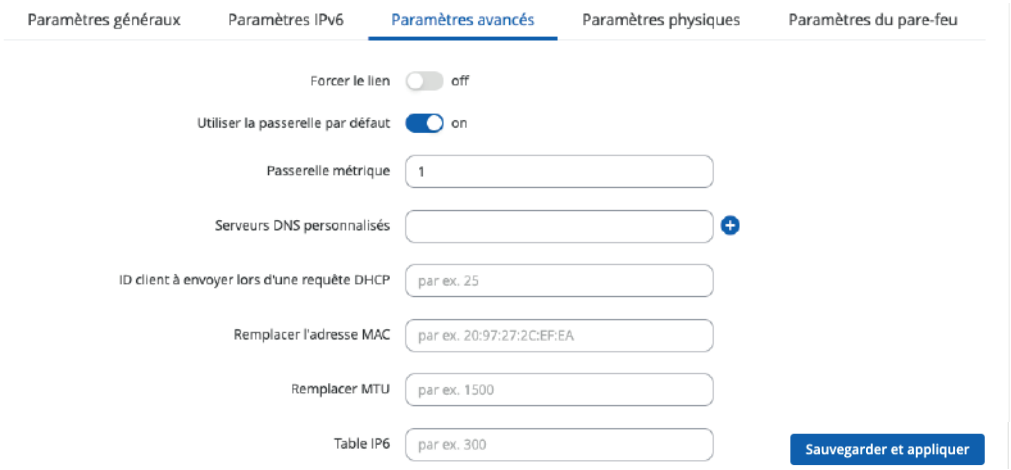


Forcer le lien	Off | On Par défaut : Off	Indique si les paramètres d'interface (IP, route, passerelle) sont attribués à l'interface indépendamment de l'activité de la liaison ou seulement après que celle-ci soit devenue active.
Utiliser le flag de diffusion	Off | On Par défaut : Off	Obligatoire pour certains fournisseurs d'accès Internet.
Utiliser la passerelle par défaut	Off | On Par défaut : On	Lorsqu'elle est cochée, cette option 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 maximale).
Serveurs DNS personnalisés	ip4 Par défaut : aucun	Spécifie les serveurs DNS personnalisés. Si ce champ est laissé vide, les serveurs DNS annoncés par le pair seront utilisés.
ID client à envoyer lors d'une requête DHCP	Chaîne de caractères Par défaut : aucun	Identifiant client qui sera envoyé lors de la demande d'un bail DHCP.
Classe de fournisseur à envoyer lors d'une demande de DHCP	chaîne de caractères Par défaut : aucun	Classe du fournisseur qui sera envoyée lors de la demande d'un bail DHCP.
Remplacer l'adresse MAC	Mac Par défaut : aucun	Lorsqu'elle est activée, cette option utilise une adresse MAC définie par l'utilisateur pour l'interface au lieu de celle par défaut.
Remplacer MTU	Entier [1..9200] Par défaut : aucun	Modifie la taille maximale des unités de transmission (MTU) autorisées pour les interfaces. Il s'agit de la taille maximale d'une unité de données de protocole (PDU) pouvant être transmise lors d'une seule transaction de couche réseau.
Tableau IP4	Par défaut : aucun	ID de la table de routage dans la page Tables de routage .

Paramètres avancés : DHCPv6

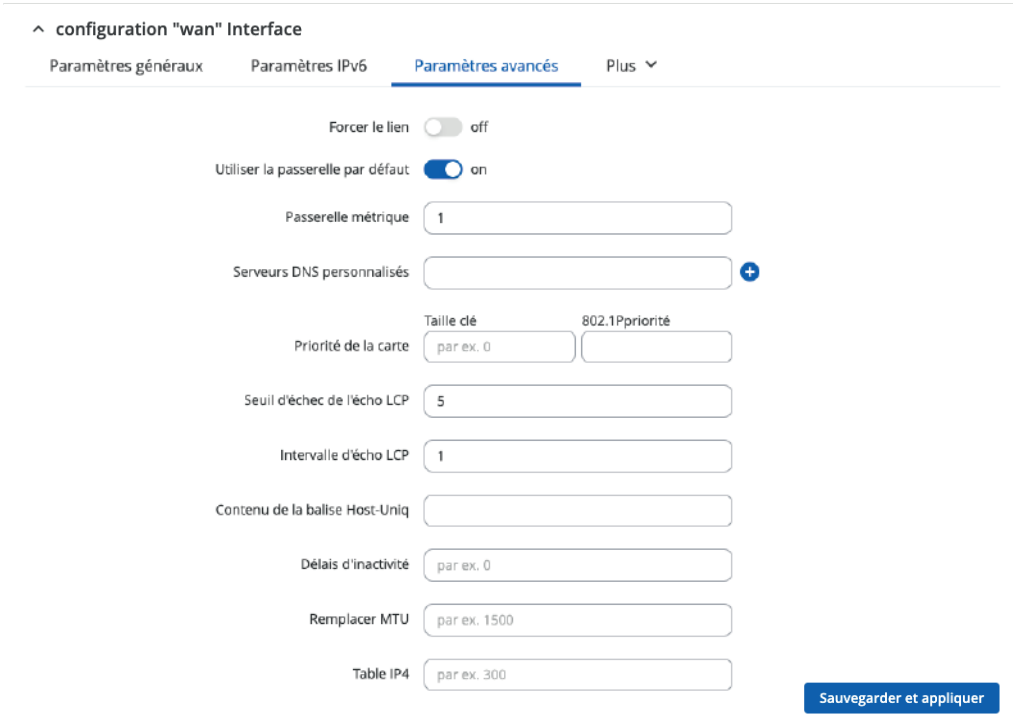
Les informations sur les paramètres avancés pour le protocole DHCPv6 sont fournies dans le tableau ci-dessous.



Forcer le lien	Off | On Par défaut : Off	Indique si les paramètres d'interface (IP, route, passerelle) sont attribués à l'interface indépendamment de l'activité de la liaison ou seulement après que celle-ci soit devenue active.
Utiliser la passerelle par défaut	Off | On Par défaut : On	Lorsqu'elle est cochée, cette option crée une route par défaut pour l'interface.
Passerelle métrique	Entier[0..4294967295] Par défaut : 2	La configuration génère par défaut une entrée dans la table de routage. Ce champ permet de modifier la métrique de cette entrée : plus la métrique est basse, plus la priorité est élevée.
Serveurs DNS personnalisés	Ip4 ; Par défaut : aucun	Spécifie les serveurs DNS personnalisés. Si ce champ est laissé vide, les serveurs DNS annoncés par le pair seront utilisés.
ID client à envoyer lors d'une requête DHCP	Chaîne de caractères Par défaut : aucun	Identifiant client qui sera envoyé lors de la demande d'un bail DHCP.
Remplacer l'adresse MAC	Par défaut : aucun	Lorsqu'elle est activée, cette option 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 autorisée de l'unité de transmission (MTU) de l'interface. Il s'agit de la taille maximale d'une unité de données de protocole (PDU) pouvant être transmise en une seule transaction de couche réseau.
Tableau IP6	Par défaut : aucun	ID de la table de routage dans la page Tables de routage .

Paramètres avancés : PPPoE

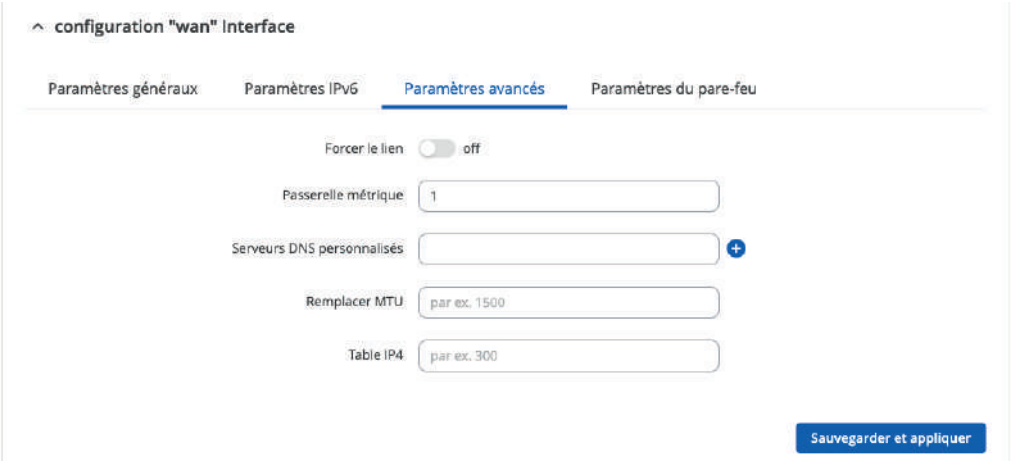
Les informations sur les paramètres avancés pour le protocole PPPoE sont fournies dans le tableau ci-dessous.



Forcer le lien	Off | On Par défaut : Off	Indique si les paramètres d'interface (IP, route, passerelle) sont attribués à l'interface indépendamment de l'activité de la liaison ou seulement après que celle-ci soit devenue active.
Utiliser la passerelle par défaut	Off | On Par défaut : On	Lorsqu'elle est cochée, cette option 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 faible, plus la priorité est élevée (0 pour la priorité la plus élevée).
Priorité de la carte	Par défaut : aucun	Carte la priorité de la priorité du noyau à 802.1p. Dans la plupart des cas, utilisez 0 pour la priorité du noyau car c'est la par défaut.
Seuil d'échec de l'écho LCP	Par défaut : aucun	Considère que le pair est hors service après un certain nombre d'échecs d'écho LCP. Laissez cette valeur à 0 pour ignorer les échecs.
Intervalle d'écho LCP	Par défaut : aucun	Envoie des requêtes d'écho LCP à l'intervalle spécifié en secondes. Cette fonction n'est effective qu'en présence d'un seuil de défaillance.
Contenu de la balise Host-Uniq	Par défaut : aucun	Laissez ce champ vide sauf si votre fournisseur d'accès Internet l'exige.
Délais d'inactivité	Par défaut : aucun	Fermer la connexion inactive après le nombre de secondes indiqué. Laisser à 0 pour maintenir la connexion.
Remplacer MTU	Par défaut : aucun	Unité de transmission maximale (MTU) - spécifie la taille maximale possible d'un paquet de données.
Tableau IP4	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.



Forcer le lien	Off | On ; Par défaut : Off	ndique si les paramètres d'interface (IP, route, passerelle) sont attribués à l'interface indépendamment de l'activité de la liaison ou seulement après que celle-ci soit devenue active.
Passerelle métrique	Par défaut : aucun	Une métrique spécifie la priorité de la passerelle. Plus la métrique est faible, 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 la MTU	Par défaut : aucun	Unité de transmission maximale (MTU) : spécifie la taille maximale d'un paquet de données. Si le champ « MTU de remplacement » est laissé vide, une MTU dynamique vide sera utilisée.
Table IP4	Par défaut : aucun	ID de la table de routage.

Paramètres physiques

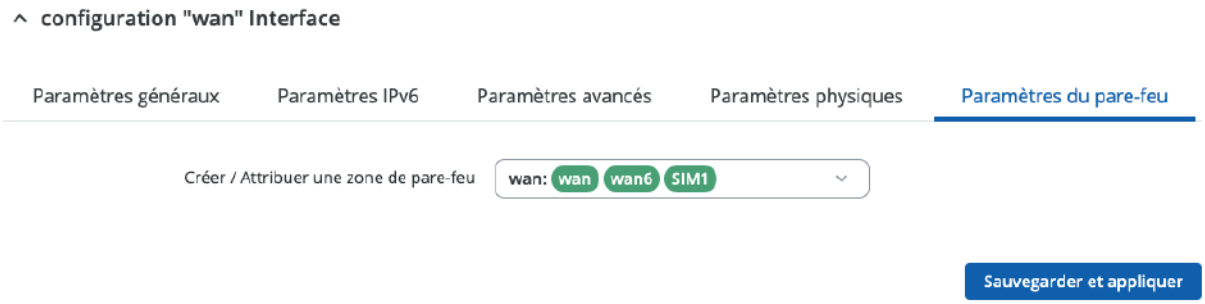
La section Paramètres physiques est utilisée pour créer des associations avec des interfaces physiques et des interfaces réseau de Bridge (pont).



Interfaces bridge (pont)	Off | On ; Par défaut : Off	Pont entre 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 : aucun	Lie cette interface réseau aux interfaces de périphériques physiques telles que les radios Ethernet ou WiFi.

Paramètres du pare-feu

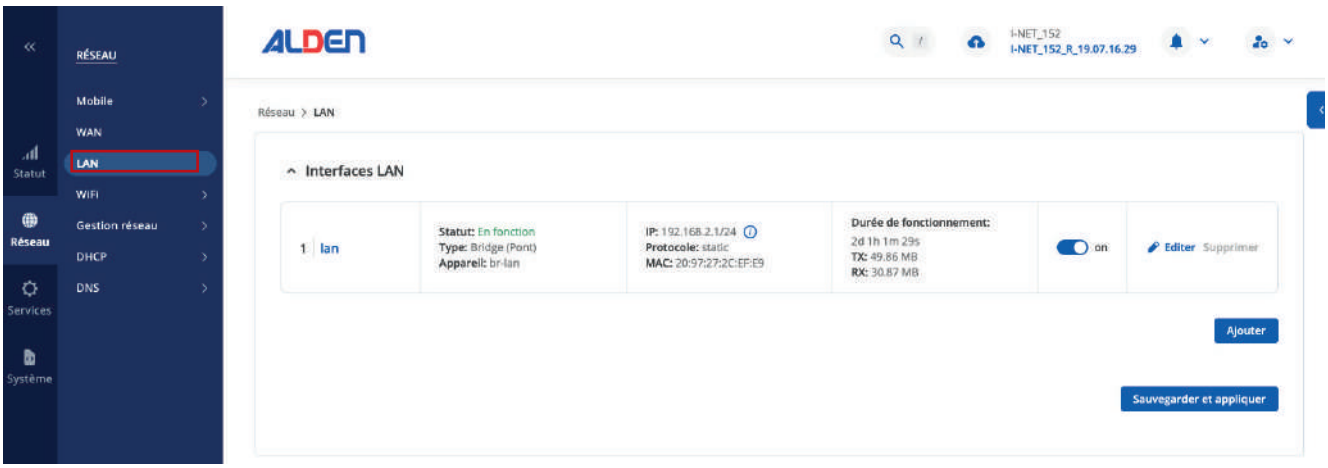
La section « Paramètres du pare-feu » permet de spécifier la zone de pare-feu à laquelle appartient cette interface, le cas échéant. L'attribution d'une interface à une zone peut simplifier la configuration des règles de pare-feu. Par exemple, au lieu de configurer des règles distinctes pour chaque interface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



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

La page LAN permet de créer et de configurer des interfaces de réseau local.
La section LAN affiche les interfaces réseau actuellement disponibles sur cet appareil.



Si vous passez votre souris sur ⓘ, les adresses d'attribution de préfixe IPv6 globales s'afficheront.

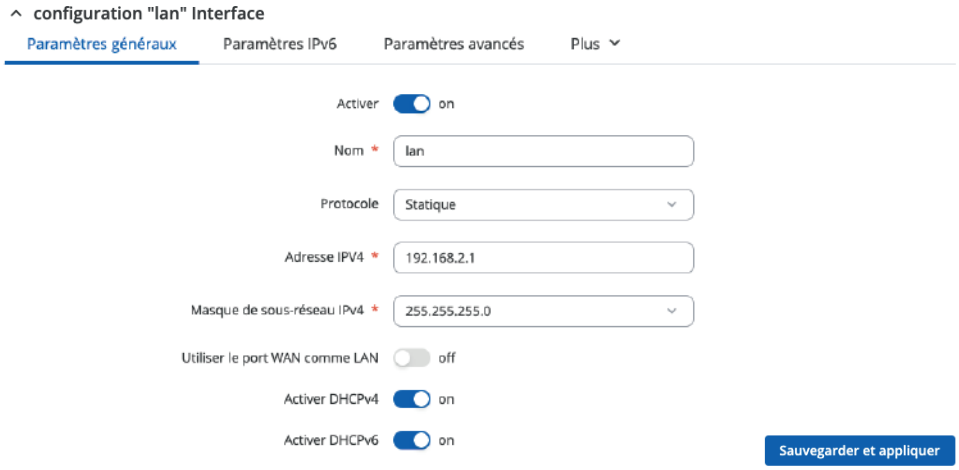


Pour créer des interfaces réseau supplémentaires, cliquez sur le bouton « Ajouter ».
Pour commencer la configuration d'une interface, cliquez sur le bouton « Editer » situé à droite de l'interface :

CONFIGURATION INTERFACE

Paramètres Généraux

La section Paramètres généraux permet de configurer les principaux paramètres du réseau local.

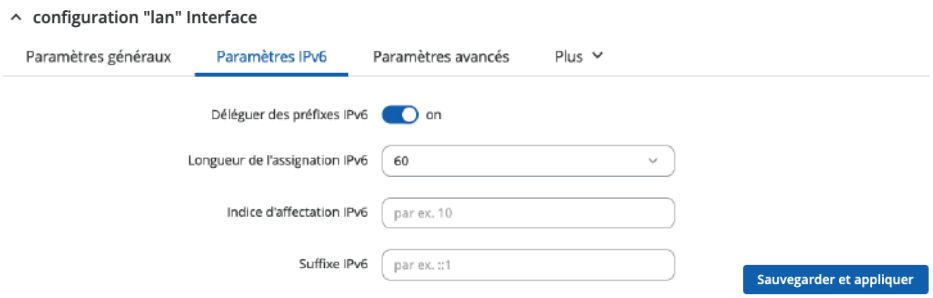


Activer	Off | On Par défaut : On	Activer l'interface
Nom	chaîne de caractère Par défaut : lan	Nom de l'interface.
Protocole	Statique | Aucun Par défaut : Statique	
Adresse IPv4	ip4 ; par défaut : 192.168.2.1	L'adresse de votre routeur sur le réseau

Masque de sous-réseau IPv4	Masque de sous-réseau Par défaut : 255.255.255.0	Le masque de sous-réseau IPv4 de cette interface. Un masque de sous-réseau sert à définir la « taille » d'un réseau en spécifiant quelle partie de l'adresse IP désigne le réseau et quelle partie désigne un périphérique.
Utiliser le port WAN comme port LAN	Off | On ; Par défaut : Off	Utiliser un port WAN comme un port LAN : vous perdrez la connexion WAN. / Utiliser un port LAN comme un port WAN : vous perdrez la connexion LAN.
Activer DHCPv4	Off | On ; Par défaut : On	Activer le serveur DHCPv4.
Activer DHCPv6	Off | On ; Par défaut : On	Activer le serveur DHCPv6.

Paramètres IPV6

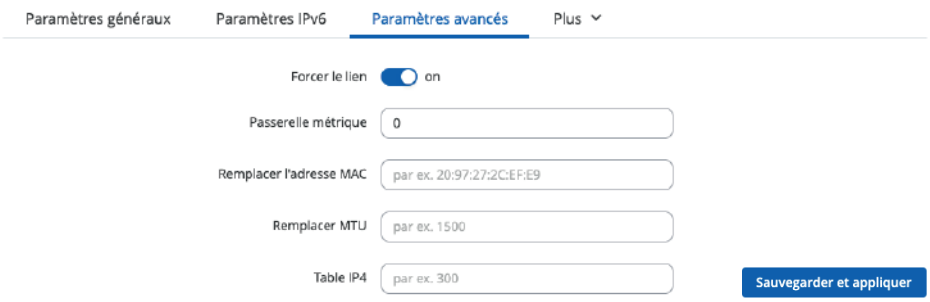
La section Paramètres généraux permet de configurer les principaux paramètres du réseau local.



Déléguer les préfixes IPv6	Off | On Par défaut : On	Activer la délégation en aval des préfixes IPv6 disponibles sur cette interface.
Longueur d'attribution IPv6	Désactivé | 64 | Personnalisé – entier [0..6] Par défaut : 60	Attribuez à cette interface une partie de la longueur donnée de chaque préfixe IPv6 public.
Conseil d'attribution d'adresse IPv6	Une chaîne hexadécimale de symboles (af, AF et 0-9) est acceptée ; Par défaut : aucun	Attribuez les parties de préfixe en utilisant cet ID de sous-préfixe hexadécimal pour cette interface.
Suffixe IPv6	Valeurs autorisées : « eui64 », « random », valeur fixe comme « ::1 » ou « ::1:2 » Par défaut : aucun	Optionnel. Valeurs autorisées : « eui64 », « random », valeur fixe comme « ::1 » ou « ::1:2 ». Lorsqu'un préfixe IPv6 (comme « a:b:c:d:: ») est reçu d'un serveur délégué, utilisez le suffixe (comme « ::1 ») pour former l'adresse IPv6 (« a:b:c:d::1 ») de l'interface.

Paramètres avancés

La section « Paramètres avancés » permet de configurer les paramètres avancés du réseau local.

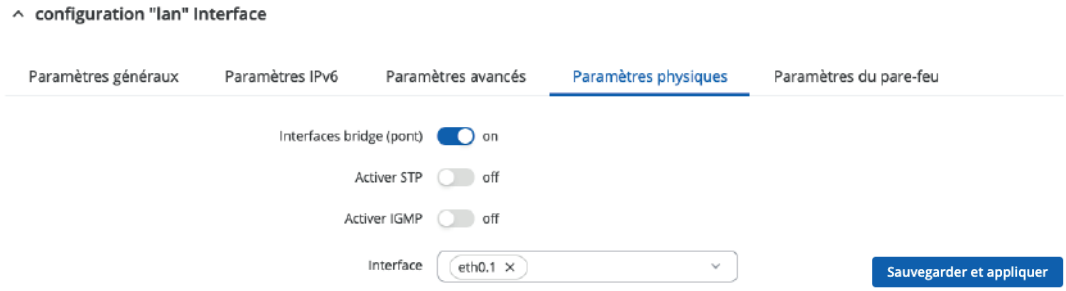


Forcer le lien	Off | On Par défaut : On	Définir les propriétés de l'interface indépendamment du support de liaison (si cette option est activée, les événements de détection de support n'invoquent pas les gestionnaires de branchement à chaud).

Utiliser la métrique de passerelle	Par défaut : aucun	La configuration génère par défaut une entrée dans la table de routage. Ce champ permet de modifier la métrique de cette entrée : plus la métrique est basse, plus la priorité est élevée.
Remplacer l'adresse MAC	Les adresses MAC composées de six groupes de deux chiffres hexadécimaux sont acceptées. Exemple : 00:23:45:67:89:AB Par défaut : aucun	Modifier l'adresse MAC de l'interface. Par exemple, votre FAI (Fournisseur d'Accès Internet) vous attribue une adresse IP statique et peut l'associer à l'adresse MAC de votre ordinateur (cette adresse IP ne fonctionnera donc qu'avec votre ordinateur, et non 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 celui-ci. Vous pouvez sélectionner l'adresse MAC d'un ordinateur actuellement connecté ou en utiliser une personnalisée. Lors de la modification de l'adresse MAC sur une interface LAN, veillez à éviter les conflits d'adresses MAC.
Remplacer l'unité de transmission maximale (MTU)	Entier [98..65535] Par défaut : aucun	Unité de transmission maximale (MTU) – spécifie la taille maximale possible d'un paquet de données.
Tableau IP4	Par défaut : aucun	L'adresse de votre routeur sur le réseau

Paramètres physiques

La section « Paramètres physiques » permet de configurer les paramètres avancés du réseau local.



interfaces bridge (pont)	Off | On Par défaut : On	Crée un pont via une ou plusieurs 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 l'écoute IGMP sur ce pont.
Interface	Interface(s) réseau ; Oar 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 » permet de configurer les paramètres du pare-feu du réseau local.



Créer/Attribuer une zone de pare-feu	Zone de pare-feu Par défaut : réseau local	Choisissez la zone de pare-feu à attribuer à cette interface. Sélectionnez « Non spécifié » pour supprimer l'interface de la zone associée ou définissez une nouvelle zone et rattachez-y l'interface.

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 152.

2.4.1 Menu RÉSEAU >WIFI>SSID

La section SSID est utilisée pour configurer vos points d'accès sans fil (AP) et vos clients sans fil (STA). Vous pouvez y accéder en cliquant sur le bouton « Editer ».

Définitions : Un point d'accès sans fils (AP) ou Hotpsot WiFi, est un réseau local sans fils créé par votre routeur I-NET152, auquel un appareil (ex : PC) vient se connecter pour un accéder à Internet.

Une station client sans fils (STA) est une interface créee par votre routeur I-NET152, utilisée pour se connecter à un autre point d'accès sans fils (exemple : une borne WiFi public).
Une station client sans fils est généralement créée pour obtenir un "répéteur WiFi" d'une borne WiFi public vers son propre réseau local WiFi.

Technologie WiFi

Les appareils I-NET 152 prennent en charge les technologies sans fil IEEE 802.11b/g/n et 802.11e_WMM.



Configuration générale

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



Activer	Off | On Par défaut : On	Active ou désactive l'interface WiFi.
Mode	Point d'accès | Client | Mailles | Multi AP Par défaut : Point d'accès	Définit le rôle de cette interface : **Point d'accès** pour fournir du WiFi à d'autres appareils. **Client** pour utiliser le WiFi d'autres appareils pour le WWAN et **Mailles** pour servir de passerelle de réseau maillé ou de nœud dans un réseau maillé.

Mode point d'accès

SSID	Le SSID d'usine est différent pour chaque appareil.	L'identificateur d'ensemble de services est un nom utilisé pour identifier un point d'accès et qui s'affiche lorsque le client tente de s'y connecter.
Mot de passe	Chaîne de caractères Par défaut : aucun	Phrase secrète personnalisée utilisée pour l'authentification (au moins 8 caractères). Une autre option consiste à utiliser l'icône , qui génère des mots de passe aléatoires.

Réseau	Par défaut : LAN	Choisissez le ou les réseaux que vous souhaitez connecter à cette interface sans fil ou remplissez le champ « +ajouter nouveau » pour définir un nouveau réseau.
Transition rapide 802.11r	Off | On Par défaut : Off	Permet une itinérance rapide entre les points d'accès appartenant au même domaine de mobilité

Mode Client

Reconnexion automatique	Off | On Par défaut : On	Permet la reconnexion automatique au point d'accès configuré en cas de perte de connexion.
SSID	Le SSID d'usine est différent pour chaque appareil	L'identificateur d'ensemble de services étendus est un nom utilisé pour identifier le point d'accès auquel le client se connectera.
BSSID	Adresse MAC Par défaut : aucun	Identifiant de l'ensemble de services de base.
Mot de passe	Chaîne de caractères Par défaut : aucun	Phrase secrète personnalisée utilisée pour l'authentification (au moins 8 caractères). Une autre option consiste à utiliser l'icône , qui génère des mots de passe aléatoires.
Réseau	Interfaces réseau Par défaut : Auto	Choisissez le réseau auquel vous souhaitez vous connecter à cette interface sans fil ou remplissez le champ Personnalisé pour définir un nouveau réseau (vous serez redirigé vers la page de configuration du réseau nouvellement créé).

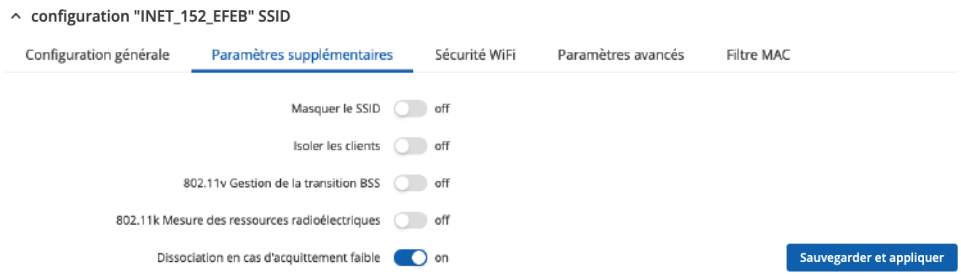
Mode Mailles

ID du maillage	entier ; valeur Par défaut : aucune	Identifiant du réseau maillé.
Mot de passe	Chaîne de caractères Par défaut : aucun	Phrase secrète personnalisée utilisée pour l'authentification (au moins 8 caractères). Une autre option consiste à utiliser l'icône , qui génère des mots de passe aléatoires.
Réseau	Interfaces réseau Par défaut : Auto	Choisissez le réseau auquel vous souhaitez vous connecter à cette interface sans fil ou remplissez le champ Personnalisé pour définir un nouveau réseau (vous serez redirigé vers la page de configuration du réseau nouvellement créé).

Mode Multi AP

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

Paramètres supplémentaires



Mode point d'accès

Masquer le SSID	Off | On Par défaut : Off	Masquer l'identifiant de l'ensemble de services
Isoler les clients	Off | On Par défaut : Off	Empêche la communication entre clients sur le même sous-réseau.
802.11v Gestion de la transition BSS	Off | On Par défaut : Off	Une suggestion (ou un conseil) donné à un client, que celui-ci peut choisir de suivre ou d'ignorer.

802.11k Mesure des ressources radioélectriques	Off | On Par défaut : Off	Permet aux appareils de rechercher rapidement les points d'accès à proximité disponibles en tant que cibles d'itinérance en créant une liste optimisée de canaux.
Dissociation en cas d'acquittement faible	Off | On Par défaut : On	Autoriser le mode AP à déconnecter les stations/clients en fonction d'un niveau d'accusé de réception faible.
Client et multi-AP		
Activer l'itinérance rapide	Off | On Par défaut : Off	Demande des analyses de base aux fins d'itinérance au sein d'un ESS.
Redirection du portail captif	Off | On Par défaut : Off	Également connu sous le nom de Travelmate. Permet la redirection vers un portail captif.
Mailles		
Rediriger le trafic des pairs en maillage	Off | On Par défaut : Off	Permet le transfert du trafic entre pairs du réseau maillé.
Seuil RSSI pour joindre	Par défaut : 0	0 = seuil RSSI non utilisé, 1 = ne pas modifier les paramètres par défaut du pilote.

Sécurité WiFi



Cryptage	Aucun chiffrement | WPA-PSK | WPA2-PSK | Mode mixte WPA-PSK/ WPA2-PSK | WPA3-SAE | Mode mixte WPA2-PSK/ WPA3-SAE | OWE | WPA-EAP | WPA2-EAP | Mode mixte WPA2-EAP/WPA3-EAP | WPA3-EAP Par défaut : WPA2-PSK	Le type de chiffrement utilisé sur cette interface sans fil. Cryptage sans fil opportuniste (OWE) – aucun mot de passe n'est requis et Tout le trafic sans fil est crypté (plus sûr qu'en l'absence de cryptage).
WPA-PSK, WPA2-PSK, mode mixte WPA-PSK/WPA2-PSK, WPA3-EAP		
Chiffrer	Auto | Forcer CCMP (AES) | Forcer TKIP | Forcer TKIP et CCMP (AES) ; par défaut : Auto	Un algorithme permettant d'effectuer un chiffrement ou un déchiffrement.
WPA-PSK, WPA2-PSK, mode mixte WPA-PSK/WPA2-PSK, WPA3-SAE, mode mixte WPA2-PSK/WPA3-SAE		
Mot de passe	Chaîne de caractères Par défaut : aucun	Phrase secrète personnalisée utilisée pour l'authentification (au moins 8 caractères). Une autre option consiste à utiliser l'icône « Dé », qui génère des mots de passe aléatoires.
WPA-EAP, WPA2-EAP, mode mixte WPA2-EAP/WPA3-EAP, WPA3-EAP		
Serveur d'authentification Radius	Chaîne de caractères Par défaut : aucun	Adresse IP du serveur d'authentification.
Radius-Authentication-Port	Chaîne de caractères Par défaut : aucun	Le port par défaut du serveur est le 1812.
Radius-Authentication-Secret	Chaîne de caractères Par défaut : aucun	Secret partagé du serveur.
Radius-Accounting-Serveur	Chaîne de caractères Par défaut : aucun	Adresse IP du serveur de comptabilité.

Radius-Comptabilité-Port	Chaîne de caractères Par défaut : aucun	Le port par défaut du serveur est le 1813.
Radius-Accounting-Secret	Chaîne de caractères Par défaut : aucun	Secret partagé du serveur.
Identifiant NAS	Chaîne de caractères Par défaut : aucun	Identifiant du serveur d'accès réseau.
Mode Maille : WPA3-SAE, sans chiffrement		
Mot de passe	Chaîne de caractères Par défaut : aucun	Phrase secrète personnalisée utilisée pour l'authentification (au moins 8 caractères). Une autre option consiste à utiliser l'icône , qui génère des mots de passe aléatoires.
Mode client : WPA-EAP, WPA2-EAP, mode mixte WPA2-EAP/WPA3-EAP, WPA3-EAP		
Méthode EAP	TLS | TTLS | PEAP | FAST ; par défaut : TLS	Identifiant du serveur d'accès réseau.
Utilisez le format PKCS#12	Off | On Par défaut : Off	Utilisez le format de fichier PKCS#12 pour le certificat client.
Fichier de certificat client PKCS#12	Off | On Par défaut : Off	Utilisez le format de fichier PKCS#12 pour le certificat client.
Phrase secrète PKCS#12	Chaîne de caractères Par défaut : aucun	Phrase secrète utilisée pour déchiffrer les certificats PKCS #12.
Fichiers de certificat de l'appareil	Off | On Par défaut : Off	Choisissez cette option si vous souhaitez sélectionner des fichiers de certificat depuis votre appareil.
Certificat CA	Fichier .crt Par défaut : aucun	Ce fichier peut contenir un ou plusieurs certificats d'autorité de certification (CA) de confiance. Si aucun certificat d'autorité de certification n'est inclus, le certificat du serveur ne sera pas vérifié. Cette situation est non sécurisée et il est impératif de toujours configurer un certificat d'autorité de certification de confiance lors de l'utilisation d'EAP-TLS/TTLS/PEAP/FAST.
Certificat client	Fichier .crt Par défaut : aucun	Un 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 essentiel dans de nombreux mécanismes d'authentification mutuelle, en garantissant l'identité du demandeur.
Clé privée	Fichier .key Par défaut : aucun	Fichier de clé client TLS.
Mot de passe de la clé privée	Chaîne de caractères Par défaut : aucun	Mot de passe de la clé privée.
Identité	EAP-GTC | EAP-MD5 | EAP-MSCHAPv2 | EAP-TLS | PAP | CHAP | MSCHAP | MSCHAPv2 ; Par défaut : EAP-GTC	Utilisé comme nom d'utilisateur pour l'authentification.
Fichiers de certificat internes de l'appareil	Off | On Par défaut : Off	Choisissez cette option si vous souhaitez sélectionner des fichiers de certificat depuis votre appareil.
Certificat CA interne	Fichier .crt Par défaut : aucun	Certificat CA interne.
Certificat du client interne	Fichier .crt Par défaut : aucun	Certificat du client interne.
Clé privée interne	Fichier .key Par défaut : aucun	Clé privée interne.
Mot de passe de la clé privée interne	Chaîne de caractères Par défaut : aucun	Mot de passe de la clé privée interne.

Identité	Chaîne de caractères Par défaut : aucun	Utilisé comme nom d'utilisateur pour l'authentification.
Identité anonyme	Chaîne de caractères Par défaut : aucun	Affiché comme nom d'utilisateur en dehors du tunnel chiffré. Non utilisé pour l'authentification.
Mot de passe	Chaîne de caractères Par défaut : aucun	Utilisé pour l'authentification.

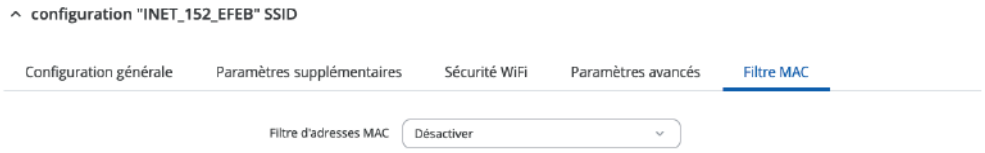
Paramètres avancés



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	Secondes ; Par défaut : aucun	Intervalle de message d'indication de trafic de livraison.
Intervalle de temps pour la recomposition des clés GTK	Secondes ; Par défaut : aucun	Période de temps entre les changements automatiques de la clé de groupe, que tous les appareils du réseau partagent.
Désactiver le pooling d'inactivité	Off | On; Par défaut : Off	La fonction d'interrogation en cas d'inactivité peut être désactivée pour déconnecter les stations en fonction du délai d'inactivité, de sorte 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	Secondes ; Par défaut : aucun	Limite d'inactivité de la station en secondes. Si une station/client n'envoie rien dans la 1ère trame temporelle, une trame de données vide lui est envoyée afin de vérifier si elle est toujours à portée. Si cette trame n'est pas acquittée, la station sera dissociée puis désauthentifiée.
Intervalle d'écoute maximal autorisé	Valeur ; Par défaut : aucun	L'association sera refusée si un client/poste tente de s'associer avec un intervalle d'écoute supérieur à cette valeur.
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	Le WiFi Multimedia (WMM), anciennement connu sous le nom de Wireless Multimedia Extensions (WME), est un sous-ensemble de la spécification WLAN 802.11e qui améliore la qualité de service (QoS) sur un réseau en priorisant les paquets de données selon quatre catégories.
Protection des trames de gestion 802.11w	Off | On; Par défaut : Off	Active la protection du cadre de gestion (MFP ou PMF). Par défaut, cette option est définie sur « Obligatoire » lors de l'utilisation du chiffrement WPA3.

Filtre MAC

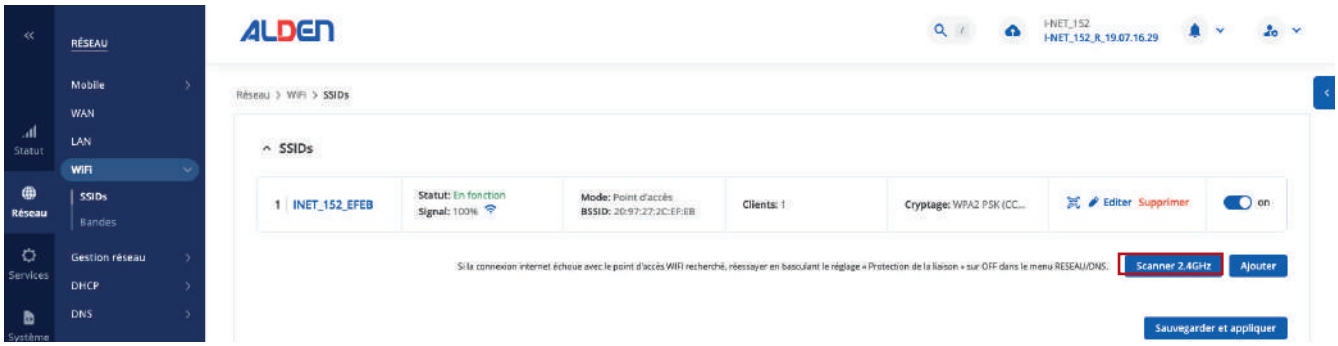
L' onglet Filtre MAC est utilisé pour configurer des règles qui autorisent ou excluent les appareils avec des adresses MAC spécifiées de se connecter à votre réseau WiFi. Cet onglet n'est visible que lorsque le mode d'interface sans fil est défini sur Point d'accès.



Filtre d'adresse MAC	Désactiver | N'autorise que la liste |Autoriser toutes les exceptions listées ; Par défaut : Désactiver	Définit le fonctionnement du filtre MAC. • N'autorise que la liste – autorise uniquement les appareils possédant les adresses MAC spécifiées à se connecter à votre point d'accès sans fil. • Autoriser toutes les exceptions listées – empêche les appareils ayant des adresses MAC spécifiques 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.
Retirer de la liste blanche	Off | On; Par défaut : Off	Permet la suppression de l'adresse MAC de la liste blanche lorsque l'appareil atteint le compteur de blocage d'adresses IP.

Scanner 2.4 GHz

Le I-NET152 peut également fonctionner comme client WiFi. La configuration en mode client est quasiment identique à celle du point d'accès, à ceci près que la plupart des options dépendent du point d'accès WiFi auquel le routeur se connecte. Les modifier peut entraîner une interruption de la connexion à ce routeur.



Pour commencer la configuration du client WiFi, cliquez d'abord sur le bouton « Scanner 2.4 GHz » pour analyser la zone environnante et tenter de vous connecter à un nouveau point d'accès sans fil.



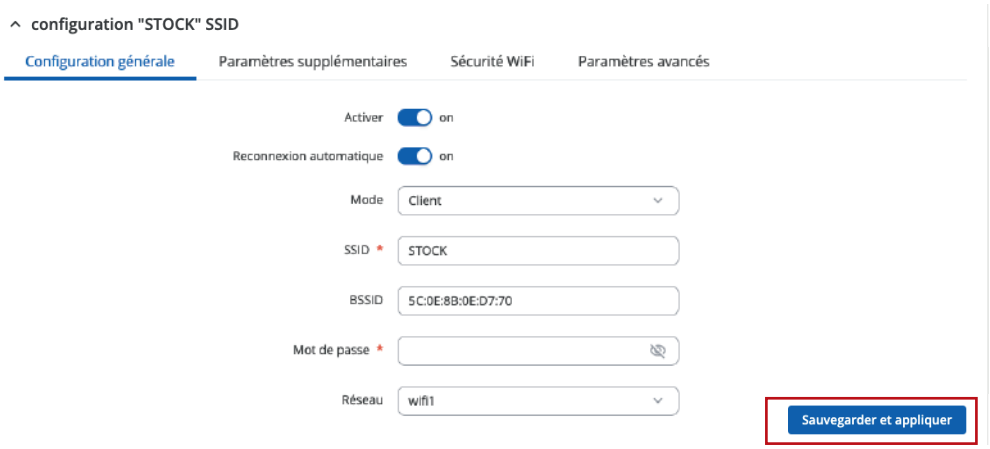
Vous serez ensuite redirigé vers la fenêtre ci-dessus, où vous verrez la liste des points d'accès WiFi disponibles dans la zone. Choisissez celui qui vous convient et appuyez sur le bouton « Rejoindre le réseau » situé à côté.

Vous serez à nouveau redirigé vers la fenêtre suivante, où vous devrez saisir votre mot de passe WiFi.



Mode Client

La fenêtre suivante qui s'ouvre est la Configuration générale. Il est généralement conseillé de ne pas modifier les valeurs affichées afin d'éviter les problèmes de connexion, car elles sont définies par le point d'accès. La seule différence avec les paramètres du point d'accès se trouve dans la section Configuration de l'interface → Configuration générale, où le mode est défini sur Client et le réseau associé à cette interface sans fil est wifi1 au lieu de LAN.



Cliquez sur Sauvegarder et appliquer et si votre configuration est correcte, le client sans fil sera fonctionnel.

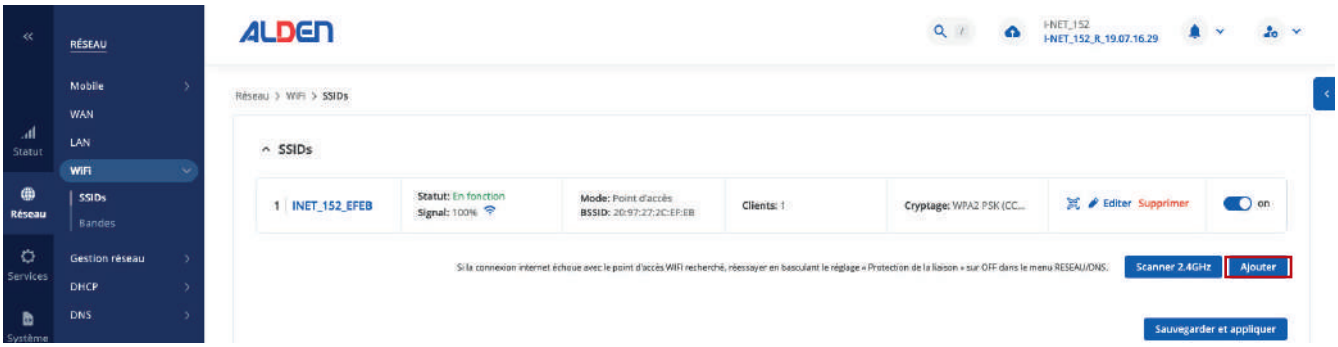
Mode maillage (ou MESH)

I-NET 152 peut également être configuré comme une passerelle maillée ou comme un nœud (routeur) se connectant à une passerelle maillée.

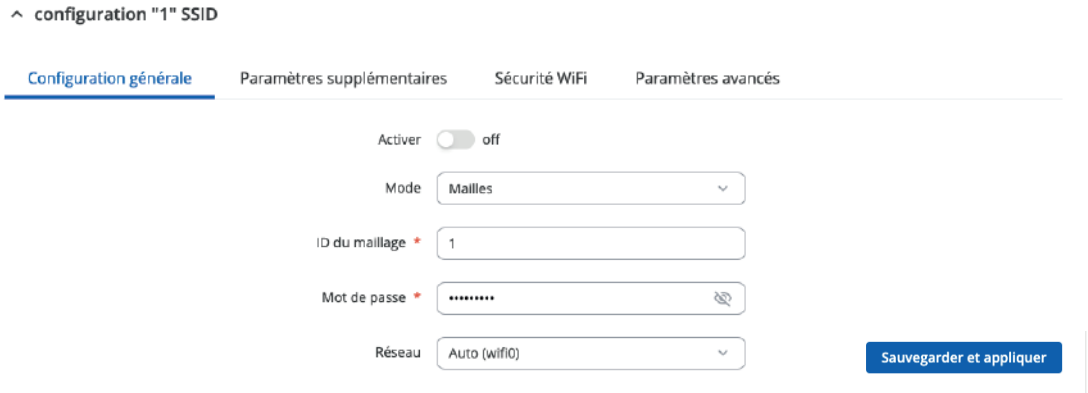
Lorsque I-NET 152 est configuré en tant que passerelle de maillage, il fournit un accès Internet à d'autres nœuds de maillage. Lorsqu'il est configuré en tant que nœud maillé, il agit comme un routeur maillé qui transfère le trafic vers et depuis la passerelle maillée. Les nœuds connectent également d'autres appareils sans fil au réseau, tels que des ordinateurs portables et des téléphones portables.

Lors de la configuration de I-NET 152 en tant que passerelle maillée, une connectivité Internet est requise.

Pour commencer, cliquez sur le bouton "Ajouter"



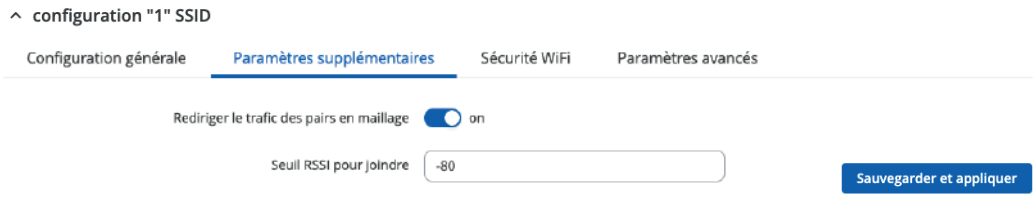
Dans l' onglet Configuration générale, sélectionnez le mode Maillé, définissez l'ID du maillage (ce numéro doit être le même dans tous les nœuds qui se connectent à ce réseau maillé sans fil) et sélectionnez le réseau souhaité qui sera attaché à l'interface. Cliquez sur Sauvegarder et appliquer.



Accédez ensuite à l' onglet Sécurité WiFi 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.



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 WiFi sera fonctionnelle.

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 WiFi de la passerelle. De plus, l'interface WAN doit être configurée en tant que client DHCP :



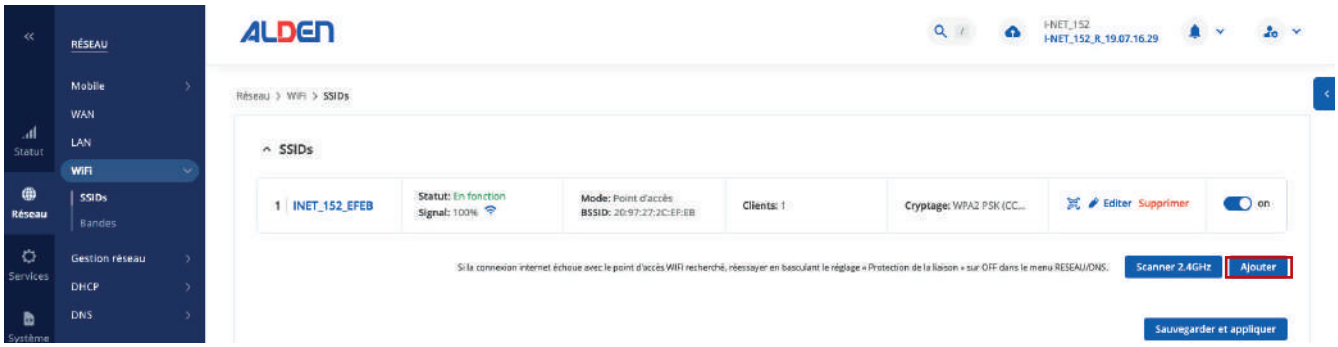
1. Accédez à l'interface utilisateur Web du routeur via le menu Réseau → WAN.
2. Appuyez sur le bouton d'édition situé à droite de l'interface WAN.
3. Changez le protocole en DHCP.

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

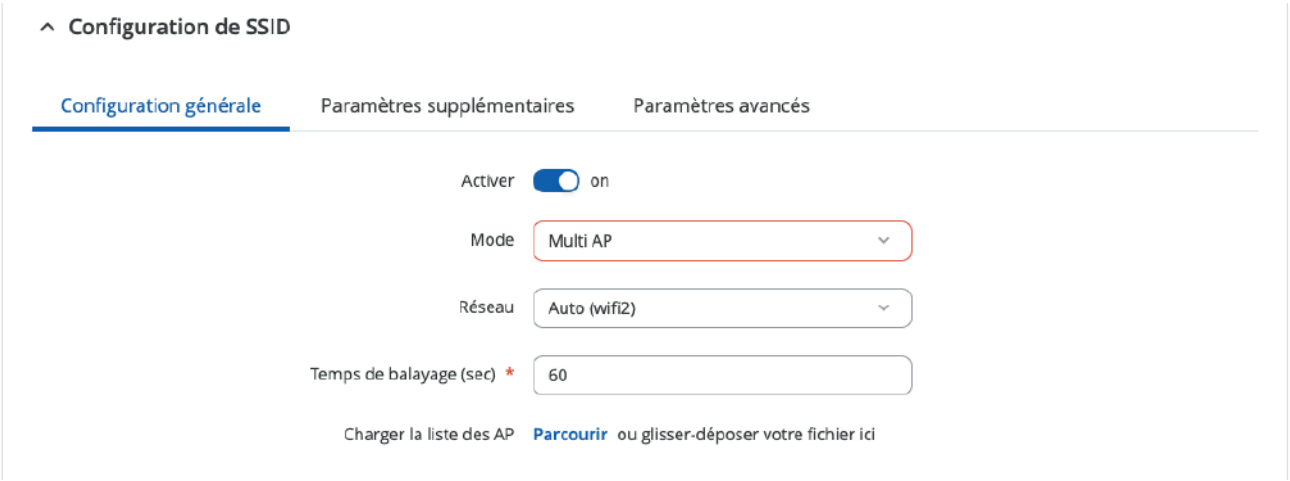
Multi AP

La fonction Multi AP permet de configurer l'accès à plusieurs points d'accès sans fil depuis une seule page. Pour créer une interface sans fil Multi AP, cliquez sur le bouton « Ajouter » situé sous l'interface sans fil dans la page Réseau → Sans fil.

IMPORTANT : le routeur I-NET 152 est doté d'un module intelligent vérifiant l'accessibilité à internet via les différentes interfaces. Si une interface WiFi créée devient inaccessible, le routeur bascule automatiquement sur la prochaine interface opérationnelle (WAN ou Mobile 4G).



Dans l'onglet Configuration générale, sélectionnez le mode Multi AP et choisissez le réseau à connecter à l'interface. Vous pouvez également définir la durée de l'analyse et importer un fichier contenant la liste des points d'accès.



Points d'accès

Vous pouvez configurer plusieurs points d'accès depuis cette page de l'interface Web ou importer un fichier contenant la liste des configurations. Ce fichier doit inclure les options et valeurs de configuration des points d'accès WiFi, définies au format option : valeur (par exemple, ssid : home_wifi). L'option SSID est obligatoire.



SSID	chaîne de caractères Par défaut : aucun	SSID d'un point d'accès.
Clé	chaîne de caractères Par défaut : aucun	Clé pré-partagée, une phrase secrète personnalisée utilisée pour l'authentification de l'utilisateur (d'au moins 8 caractères).
Activer	Off | On Par défaut : Off	Active ou désactive la configuration d'un point d'accès.
Supprimer	- (bouton interactif)	Supprime la configuration du point d'accès située à côté du bouton.

Les noms des options dans le fichier doivent être saisis en minuscules. Exemple de fichier de liste AP :
ssid : RUT_1
activer : 1
clé : 12345678
ssid : RUT_2
activer : 0
clé : 87654321
Une fois téléchargé, le contenu du fichier devrait apparaître dans la liste des points d'accès.

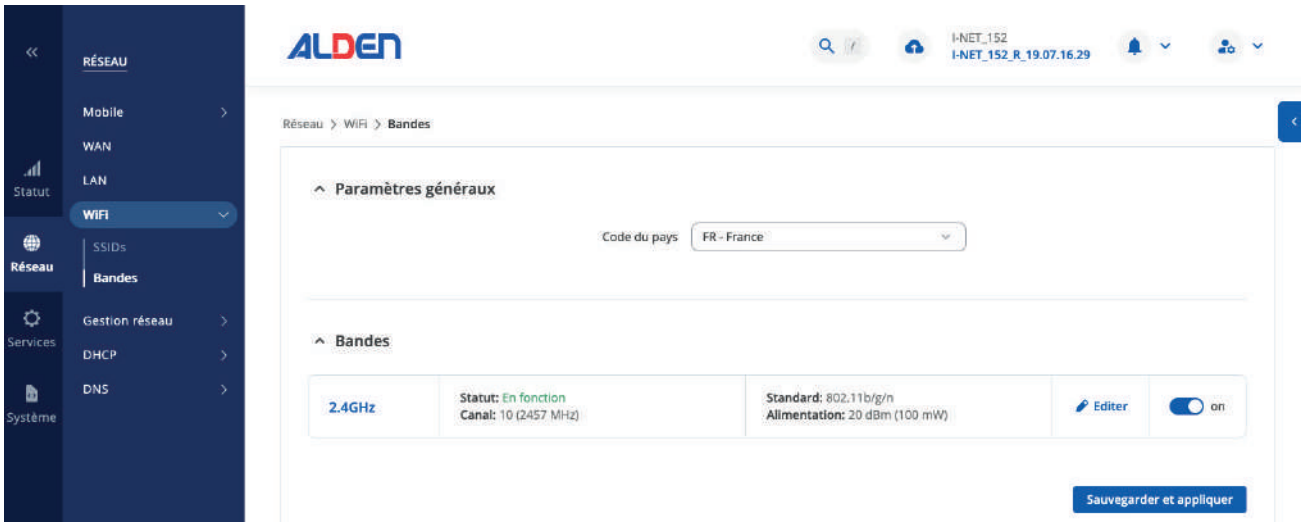
QR Code WiFi

Chaque interface WiFi possède un QR code spécifique contenant les informations SSID et mot de passe du réseau. Après avoir appuyé sur le bouton , un QR code s'affiche avec ces informations. Vous pouvez le télécharger en appuyant sur le bouton « Télécharger ». Si vous souhaitez uniquement un QR code sans informations supplémentaires, décochez la case « Inclure les identifiants ».



2.4.2 Menu RÉSEAU >WIFI>BANDES

La section Paramètres généraux permet de configurer le code pays, utilisé à des fins réglementaires (la puissance d'émission maximale et les fréquences de fonctionnement autorisées varient selon les zones), ainsi que les paramètres matériels WiFi. Vous pouvez modifier ces paramètres en cliquant sur le bouton « Modifier » situé à côté d'un périphérique sans fil (et non d'une interface) dans la page Réseau → WiFi → SSID.



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.



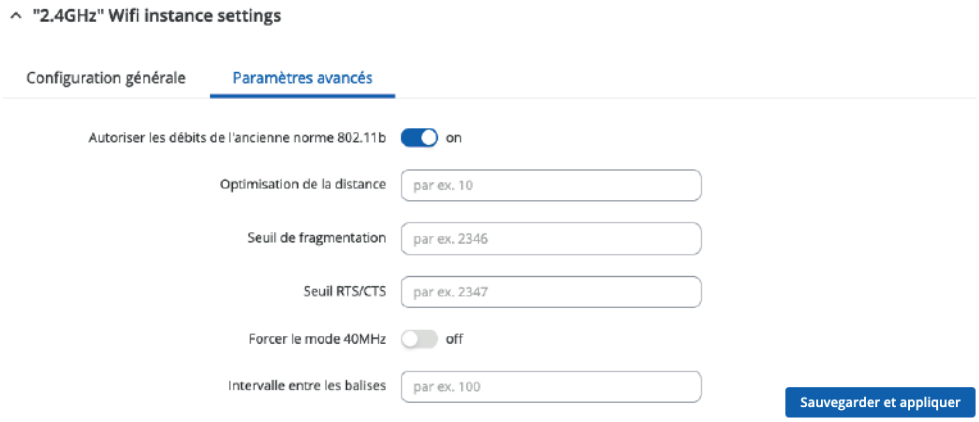
Activer	Off | On; Par défaut : On	Active ou désactive le périphérique WiFi.

Fréquence de fonctionnement (2,4 GHz)

Mode	N | Héritage; Par défaut : N	Wireless N (802.11n) prend en charge un taux de transfert théorique maximal de 300 Mbps avec 2 antennes. Il peut atteindre jusqu'à 450 Mbps avec 3 antennes. Bien que les vitesses typiques soient plus précises autour de 130 Mbps. Les anciennes normes incluent 802.11a, 802.11b et 802.11g.
Canal	automatique | 1 (2 412 MHz) | 2 (2 417 MHz) | 3 (2 422 MHz) | 4 (2427MHz) | 5 (2432MHz) | 6 (2437MHz) | 7 (2442MHz) | 8 (2447MHz) | 9 (2452MHz)| 10 (2457MHz) | 11 (2462 MHz); Par défaut : Automatique	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 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.
Largeur	20 MHz | 40 MHz ; Par défaut : 20 MHz	Une largeur de canal de 40 MHz lie 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 canaux sont encombrés de bruit et d'interférences. Dans les zones surpeuplées 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 il ne fonctionne pas aussi bien dans les zones surpeuplées.
Puissance d'émission	[5 %...100 %] ; Par défaut : 100 %	La puissance d'émission d'une radio de point d'accès est proportionnelle à sa portée effective – plus la puissance d'émission est élevée, plus un signal peut parcourir de distance et / ou plus il peut pénétrer efficacement dans des matériaux physiques tout en ayant des données résolues avec succès au destinataire.

Paramètres avancés

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



Fréquence de Fonctionnement (2,4 GHz)

Autoriser les débits de l'ancienne norme 802.11b	Off | On ; Par défaut : On	Activez cette option pour activer les connexions qui utilisent la norme 802.11b héritée.
Optimisation de la distance	Par défaut : aucun	HT Distance 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 fragment inférieur peut aider 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 de nœud caché. Il peut aider à résoudre les problèmes survenant lorsque plusieurs points d'accès se trouvent dans la même zone,
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 IEEE 802.11n-2009 !
Intervalle entre les balises	Par défaut : aucun	Intervalle de signal de balise en secondes.

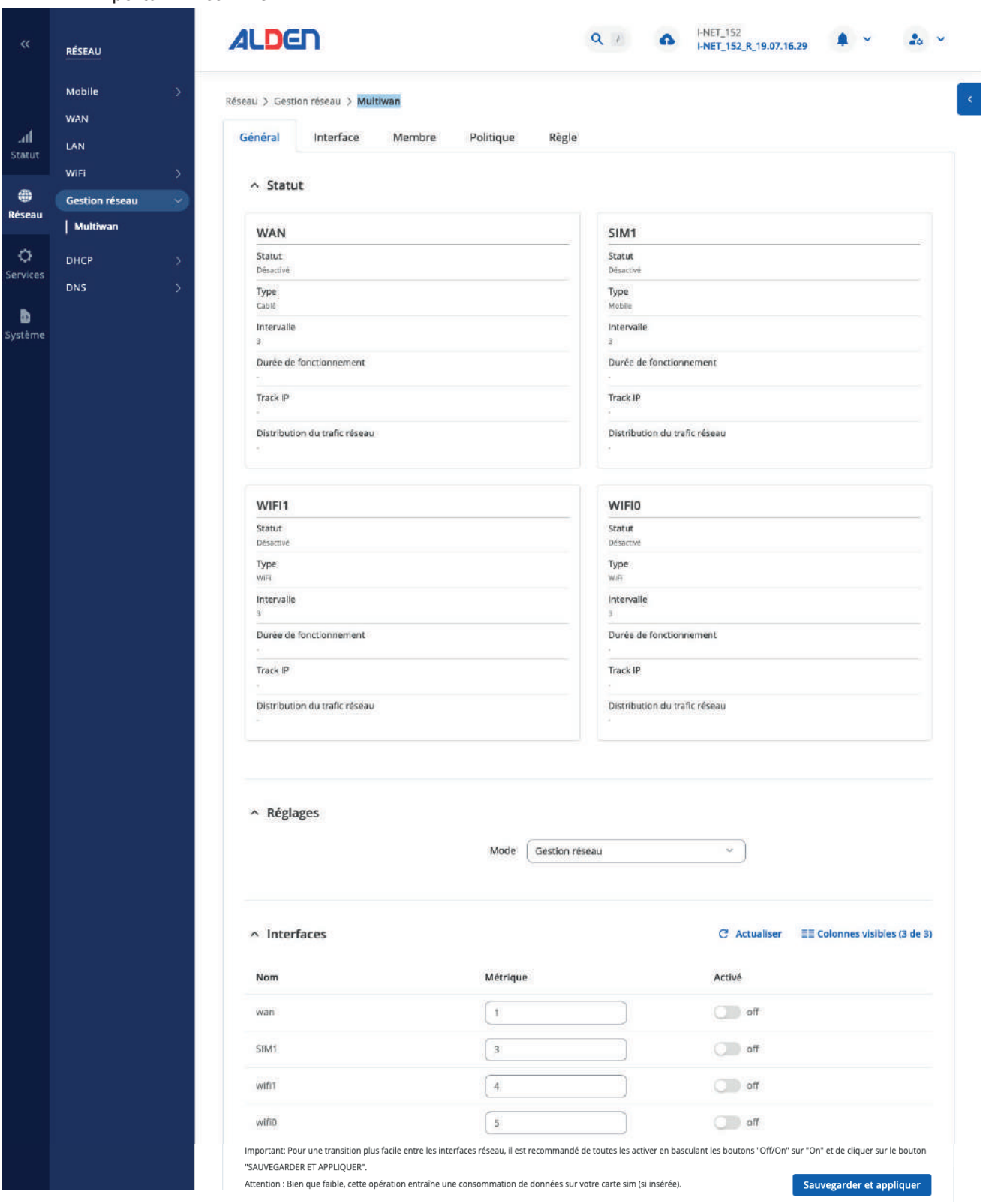
2.5 Menu RÉSEAU > GESTION RÉSEAU

2.5.1 Menu RÉSEAU > GESTION RÉSEAU > MULTIWAN

La fonction de Multiwan vous permet de sauvegarder votre connexion WAN principale en cas de panne.

Pour définir les priorités, il suffit de modifier les indicateurs d'interface dans la section « Interfaces », puis d'appuyer sur « Enregistrer et appliquer ».

Remarque : vous ne verrez aucune interface WAN câblée supplémentaire à moins que vous n'ayez configuré des ports LAN comme WAN.



Les interfaces présentant les métriques les plus élevées dans la liste sont prioritaires sur celles dont les métriques sont plus faibles. Autrement dit, l'appareil utilisera toujours l'interface WAN avec la métrique la plus élevée tant qu'elle est disponible. Si celle-ci devient indisponible, l'appareil utilisera l'interface avec la deuxième métrique la plus élevée, et ainsi de suite.

Veuillez noter que la modification des métriques d'une interface dans la liste ci-dessous modifie également sa position dans les pages suivantes :

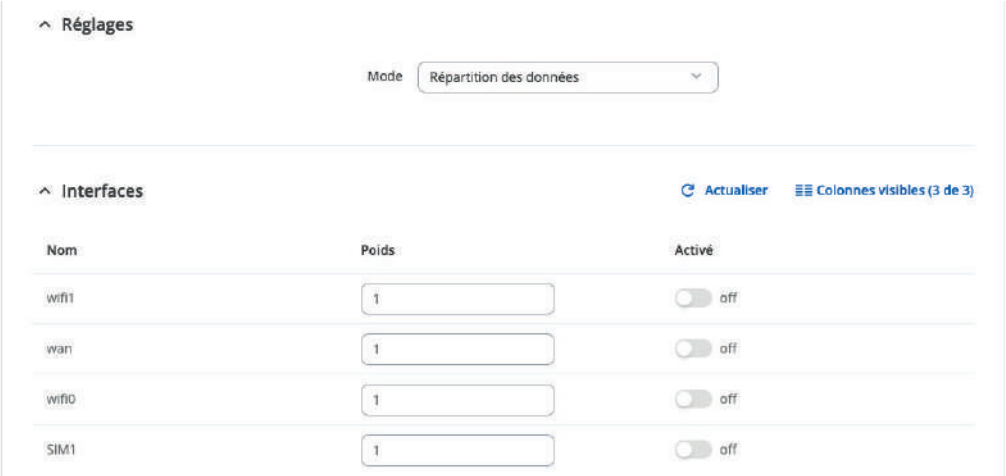
Réseau → WAN

RÉGLAGE

L'équilibrage de charge est une méthode de répartition du trafic entre plusieurs interfaces WAN. Il permet de répartir la charge de données entre différentes interfaces et d'améliorer la vitesse Internet globale pour plusieurs utilisateurs et connexions. Il est important de noter que l'équilibrage de charge n'augmente pas la vitesse d'une connexion individuelle . Par exemple, si vous téléchargez un fichier volumineux, l'utilisation de l'équilibrage de charge n'accélérera pas ce téléchargement.

Cependant, l'équilibrage de charge permet d'augmenter la vitesse de plusieurs connexions. Par exemple, dans un réseau WiFi, il utilise les ressources de plusieurs interfaces WAN pour gérer les nombreuses requêtes des différents clients.

L'équilibrage de charge et le basculement ne peuvent pas être utilisés simultanément. Si vous souhaitez sélectionner l'équilibrage de charge, vous pouvez le faire dans le menu déroulant situé dans la section «Réglages».



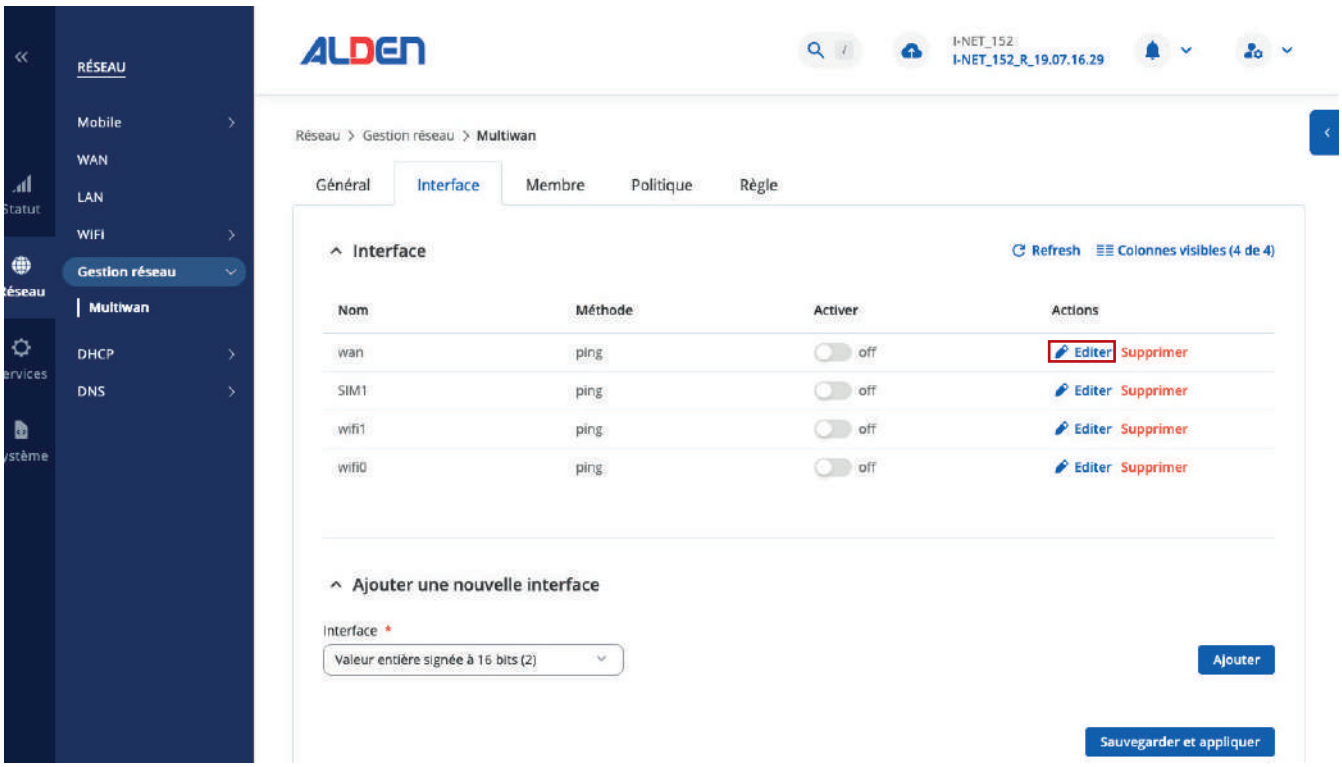
Lorsque l'équilibrage de charge est sélectionné, vous pouvez attribuer des pondérations aux interfaces WAN. Ces pondérations représentent le pourcentage de trafic qui transitera par chaque interface. Par exemple, si vous configurez l'interface comme suit :

- Poids du réseau étendu câblé : 3
- Poids du réseau étendu mobile : 2

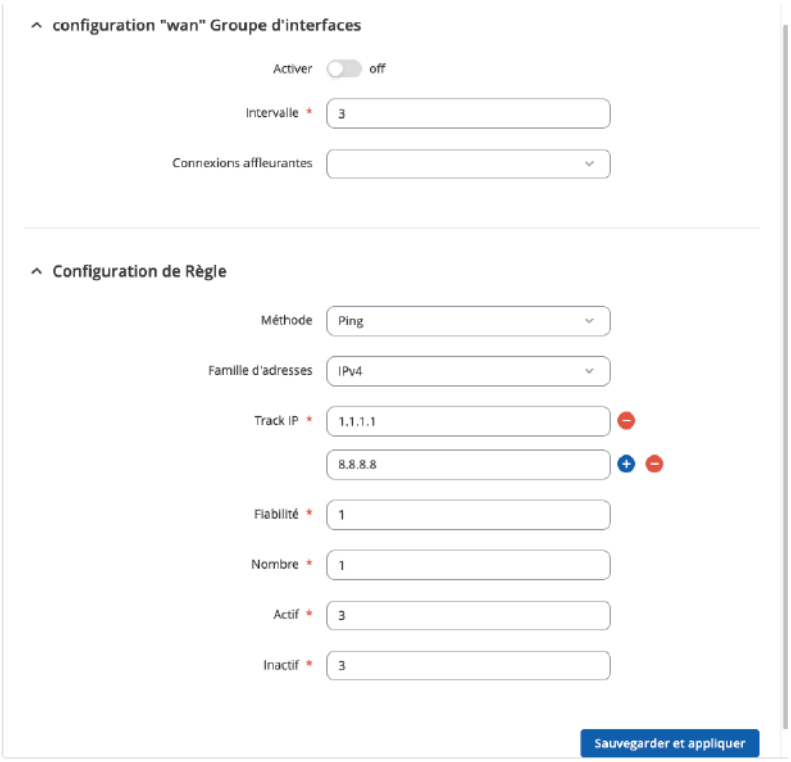
Environ 60 % (3/5) du trafic transiterait alors par l'interface WAN filaire et environ 40 % (2/5) par l'interface WAN mobile. Dans ce cas, si vous visionniez 100 vidéos différentes sur Internet, environ 60 seraient téléchargées via l'interface WAN filaire et les 40 autres via l'interface WAN mobile.

Interface

La page Interface permet de configurer la façon dont l'appareil détermine si une interface est en ligne ou hors ligne. Pour accéder à la configuration d'une interface, cliquez sur le bouton « Modifier » situé à côté de l'interface.



Vous devriez ensuite être redirigé vers la page de configuration de cette interface.



Activer	Off | On ; Par défaut : Off	Activer ou désactiver l'interface.
Intervalle	Entier [1..65000] ; Par défaut : 3	Nombre de secondes entre chaque test

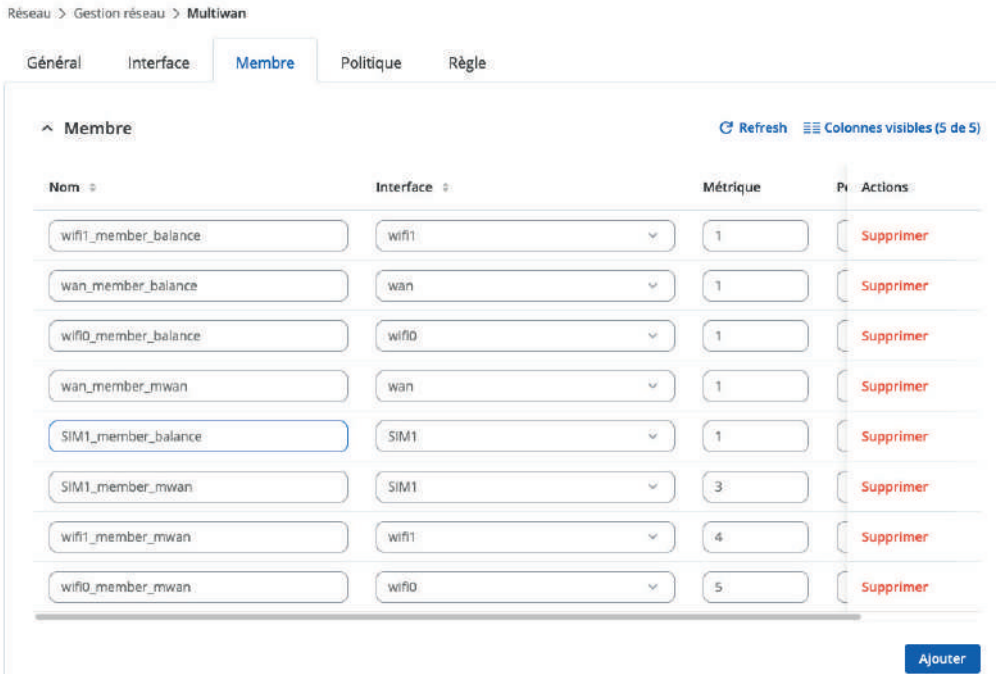
Connexions affleurantes	Connecté | Déconnecté | Interface active | Interface inactive Par défaut : aucun	Supprime les connexions établies après la survenue du scénario sélectionné afin de renouveler les priorités des interfaces configurées. • Connecté/Déconnecté – utilisé lorsque la connexion Internet apparaît/disparaît • Interface active/Interface inactive – utilisé lorsque le câble Internet est branché/débranché

Configuation de règle

Méthode	Ping | Wget Par défaut : Ping	Définit comment le contrôle d'intégrité sera effectué sur cette interface lors de la détermination de son état.
Famille d'adresses	IPv4 IPv6 Par défaut : IPv4	Famille de protocole spécifique gérée par cette interface.
Track IP	Adresse IP | nom d'hôte Par défaut : 1.1.1.1,8.8.8.8	Adresse(s) IP ou nom(s) d'hôte permettant de déterminer l'état d'une interface. En l'absence de réponse de l'un des hôtes spécifiés, l'interface est considérée comme « hors ligne ». Si cette valeur est manquante, l'interface est toujours considérée comme active.
Fiabilité	Entier [1..65000] ; Par défaut : 1	Nombre d'hôtes devant répondre pour que le test soit considéré comme réussi. Assurez-vous qu'au moins ce nombre d'hôtes est défini dans le champ « Adresse IP de suivi », sinon l'interface sera toujours considérée comme « Hors ligne ».
Nombre	Entier [1..65000] Par défaut : 1	Nombre de pings à envoyer à chaque hôte pour chaque test.
Actif	Entier [1..65000] Par défaut : 3	Nombre de tests réussis requis pour considérer une interface comme « en ligne ».
Inactif	Entier [1..65000] Par défaut : 3	Nombre de tests ayant échoué requis pour considérer une interface comme « hors ligne ».

Membre

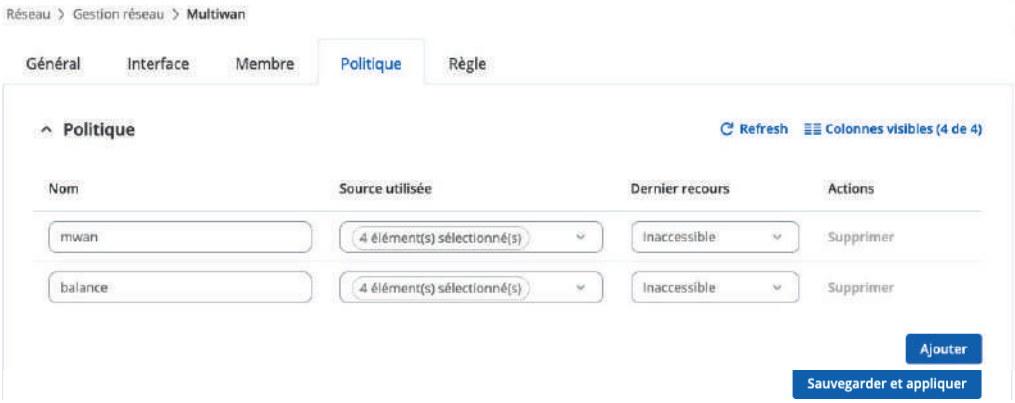
La page Membres permet de modifier/créer une liste de membres et de leur attribuer des interfaces. Vous pouvez également définir des indicateurs pour chaque utilisateur (utilisés pour le basculement) ou des pondérations pour chaque membre (utilisées pour l'équilibrage de charge).



Nom	Chaîne de caractères ; Par défaut : aucun	Nom du membre.
Interface	Nom de l'interface Par défaut : aucun	Liste des interfaces disponibles (variable selon le périphérique)
Métrique	Entier Par défaut : 1	Les membres d'une même politique ayant une métrique inférieure sont prioritaires sur ceux ayant une métrique supérieure. Les membres d'une même politique ayant la même métrique effectuent un équilibrage de charge.
Poids	Entier Par défaut : 1	Les valeurs de pondération représentent un pourcentage de la charge qui transitera par une interface. La valeur par défaut est 1 si elle n'est pas spécifiée.
Actions	–(bouton interactif) ; par défaut : Supprimer	Supprime un membre.

Politique

Une stratégie définit le comportement du périphérique lorsqu'une partie du trafic réseau correspond à la condition définie dans une règle de basculement/d'équilibrage de charge. Par défaut, deux stratégies sont configurées : l'une pour l'équilibrage de charge (balance) et l'autre pour le basculement (mwan). Vous pouvez créer des stratégies personnalisées utilisant différentes interfaces pour les scénarios de basculement et d'équilibrage de charge.



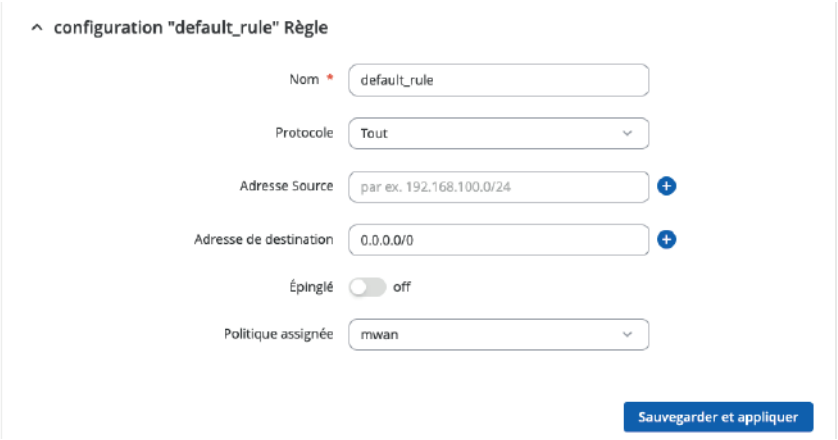
Source utilisée	Liste de la page des membres Par défaut : aucun	Membres affectés à la police d'assurance.
Dernier recours	Inaccessible | Trou noir | Par défaut Par défaut : Inaccessible	Déterminez le comportement de routage de secours si tous les membres WAN de la stratégie sont hors service. Variantes possibles : – Injoignable : Rejette tout le trafic. – Trou noir : Bloque tout le trafic. – Par défaut : utilise la table de routage principale.

Règle

Une règle d'équilibrage de charge/de basculement est un ensemble de conditions qui définissent un type de trafic réseau. Le trafic correspondant aux conditions définies dans la règle est traité conformément à la politique spécifiée.

Une règle par défaut est déjà configurée sur l'appareil. Vous pouvez ajouter d'autres règles en cliquant sur le bouton « Ajouter » ou personnaliser la règle existante en cliquant sur le bouton « Editer » situé à côté.





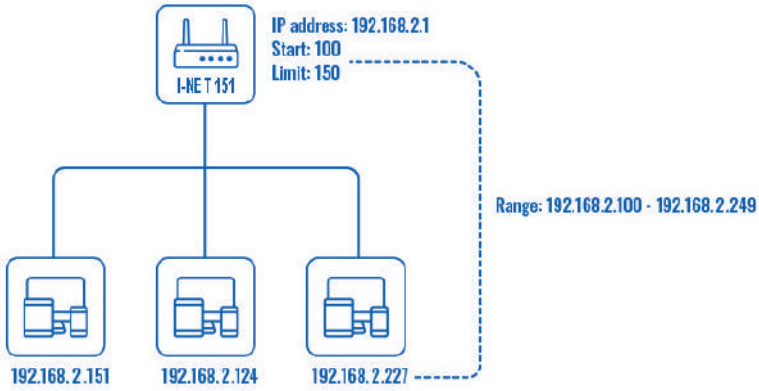
Nom	Chaîne de caractères Par défaut : defaut_rule	Nom de la règle.
Protocole	Tous | TCP | UDP | ICMP | ESP ; Par défaut : tous	Protocole correspondant à cette règle.
Adresse Source	Adresse IP/masque de sous-réseau ; Par défaut : aucun	Adresses IP sources devant correspondre à cette règle.
Adresse de destination	Adresse IP/masque de sous-réseau ; Par défaut : 0.0.0.0/0	Adresses IP de destination devant correspondre 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 pendant la période de délai d'expiration persistante utilisera la même interface WAN.
Délai d'attente persistant	Entier [1..1000000] Par défaut : aucune	Délai d'attente en secondes.
Politique assignée	mwan | balance | Inaccessible | Trou noir | Défaut Par défaut : nwan	Spécifie la politique appliquée au trafic de correspondance.

2.6 Menu RÉSEAU > DHCP

Les baux d'adresses IP statiques permettent de réserver des adresses IP spécifiques à des périphériques en les associant à leur adresse MAC. Ceci est utile pour les appareils fixes connectés au réseau et auxquels vous devez accéder fréquemment, comme une imprimante ou un téléphone IP.

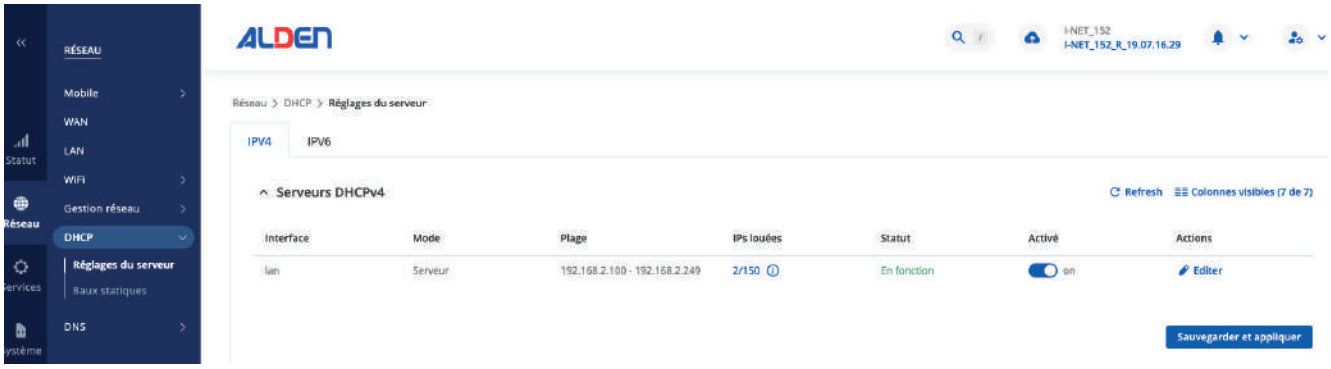
2.6.1 Menu RÉSEAU > DHCP > Réglages du serveur

Un serveur DHCP (Dynamic Host Configuration Protocol) est un service qui configure automatiquement les paramètres TCP/IP de tout appareil qui en fait la demande. Si vous connectez un appareil configuré pour obtenir une adresse IP automatiquement, le serveur DHCP lui attribuera une adresse IP parmi celles disponibles, et l'appareil pourra communiquer au sein du réseau privé.



IPV4

Pour modifier les paramètres DHCPv4 de l'interface LAN, cliquez sur le bouton « Editer ».



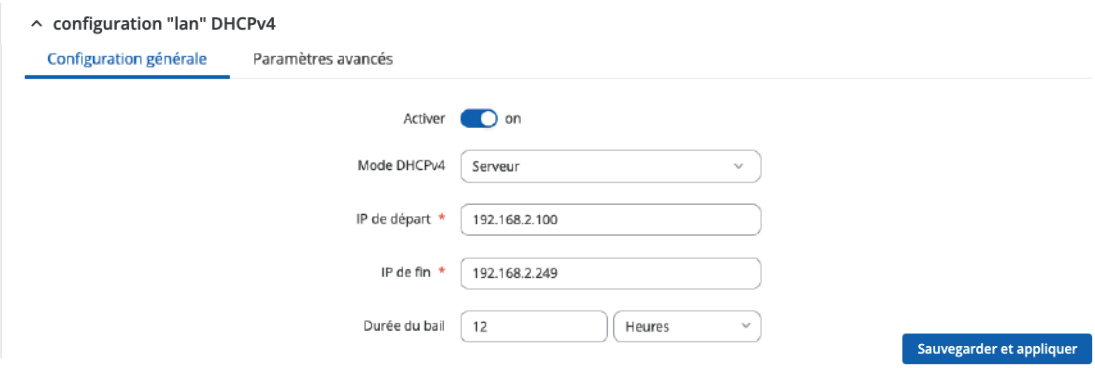
Remarque : `dnsmasq` ne loue pas d'adresses IPv4 se terminant par .0 et .255.

Le bouton d'information affiche le nombre de baux dynamiques et statiques :



CONFIGURATION GÉNÉRALE DHCPV4

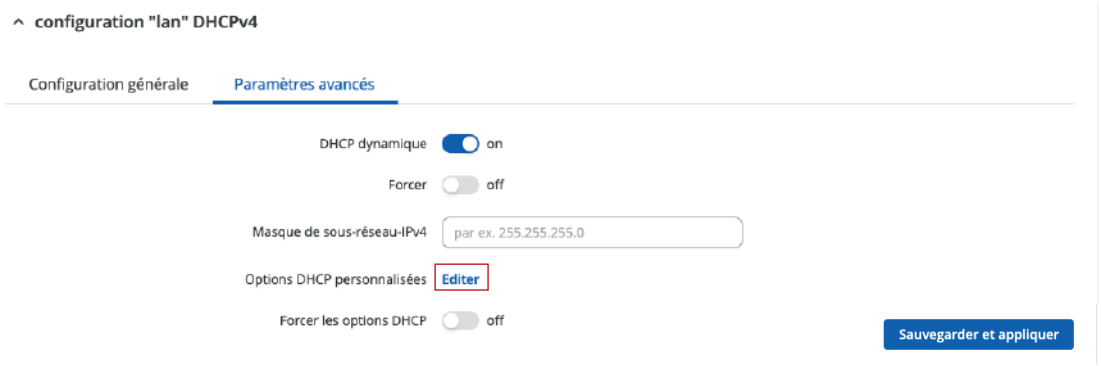
La section Configuration générale permet de configurer les principaux paramètres de fonctionnement du serveur DHCP.



Activer	Off | On ; Par défaut : Off	Active ou désactive le serveur DHCPv4.
Mode DHCPv4	Serveur | Relais Par défaut : Serveur	Spécifie le mode DHCPv4 • Variantes possibles : • Serveur : Ce périphérique sera utilisé pour gérer l'attribution des adresses IP. • Relais : Le serveur spécifié sera utilisé pour gérer l'attribution des adresses IP.
IP de départ	Entier [1..254] Par défaut : 100	Saisissez une adresse IP qui servira de point de départ à la plage d'adresses IP que le serveur DHCP utilisera pour attribuer les adresses IP.
IP de fin	Entier [1..254] Par défaut : 254	Saisissez une adresse IP qui servira de limite à la plage d'adresses IP que le DHCP utilisera pour attribuer les adresses IP.
Durée du bail	Entier [1..999999] | *infini * ; Par défaut : **12 entier [2..999999] ** ***entier [120..999999] ***	Un bail DHCP expire après la durée spécifiée dans ce champ et l'appareil qui l'utilisait devra en demander un nouveau. Toutefois, 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, l'appareil demandera au serveur DHCP de le renouveler toutes les 6 heures). La durée minimale pouvant être spécifiée est de 2 minutes. * L'option « Infini » permet de ne jamais faire expirer l'adresse DHCP ** Si l'unité sélectionnée est « Minutes ». *** Si l'unité sélectionnée est « Secondes ».
Serveur DHCP	Adresse IP Par défaut : aucun	Spécifie l'adresse IP du serveur DHCP, qui dirige toutes les requêtes vers ce serveur.
Activer l'option 82	Désactivé | activé ; Par défaut : désactivé	Active l'option d'informations de l'agent de relais DHCP utilisée pour fournir des informations supplémentaires sur l'emplacement du client DHCP.
Identification du circuit	Chaîne de caractères Par défaut : aucun	sous-option d'identification du circuit de l'agent relais.
ID distant	Chaîne de caractères Par défaut : aucun	sous-option d'identifiant distant de l'agent de relais.
Supprimer	-(bouton d'action)	Supprime le serveur DHCP.

PARAMÈTRES AVANCÉS DHCPV4

Consultez le tableau ci-dessous pour plus d'informations sur la section Paramètres avancés .



DHCP dynamique	Off | On ; Par défaut : On	Attribuer dynamiquement des adresses DHCP aux clients. Si cette option est désactivée, seuls les clients disposant d'un bail statique seront pris en charge.
Forcer	Off | On ; Par défaut : Off	Forcer le DHCP sur ce réseau même si un autre serveur est détecté.
Masque de sous-réseau IPv4	Masque de sous-réseau Par défaut : aucun	Modifiez le masque de sous-réseau envoyé aux clients. Normalement, il est calculé à partir du sous-réseau desservi.
Options DHCP personnalisées	-(bouton interactif)	Les options DHCP personnalisées sont des paires nombre/valeur permettant de configurer des fonctionnalités DHCP avancées. Elles ne configurent pas le DHCPv6 !
Forcer les options DHCP	Off | On ; Par défaut : Off	Forcer l'envoi des options DHCP même si elles ne sont pas demandées.

Options DHCP personnalisées

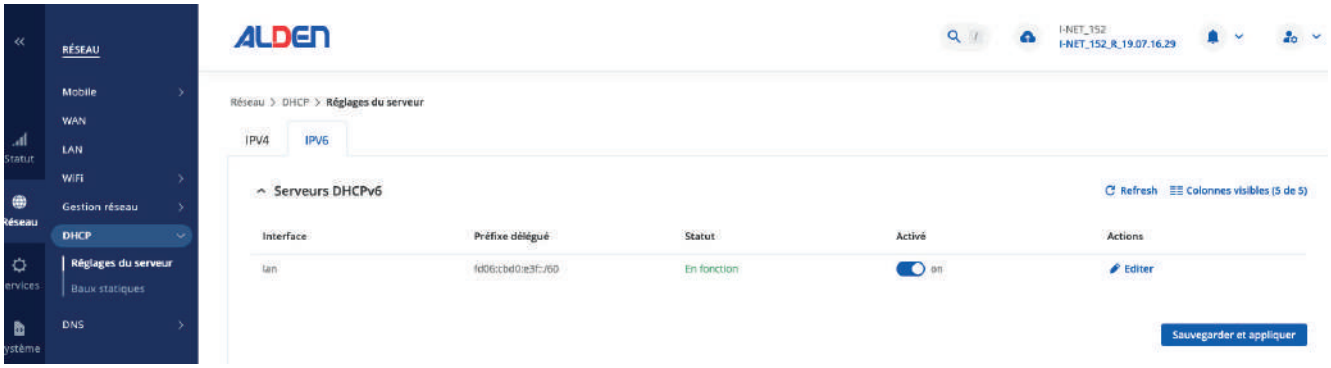
Les options DHCP personnalisées sont des paires numérique/valeur permettant de configurer des fonctionnalités DHCP avancées. Elles ne configurent pas le DHCPv6 ! La fenêtre modale des options DHCP permet d'ajouter, de supprimer et d'enregistrer plusieurs options.



Ajouter	-(bouton interactif)	Pour ajouter des options DHCP personnalisées.
Code d'option	Personnalisé | Décalage horaire (2) | Routeur (3) | DNS (6) | Nom de domaine (15) | Serveur NTP (42) | +Ajouter ; Par défaut : Décalage horaire (2)	Code d'option DHCP standardisé.
Valeur de l'option	entier ; Par défaut : aucune	Valeur qui sera attribuée à l'option sélectionnée.
Ne pas envoyer	Off | On ; Par défaut : Off	Empêcher l'envoi de cette valeur.

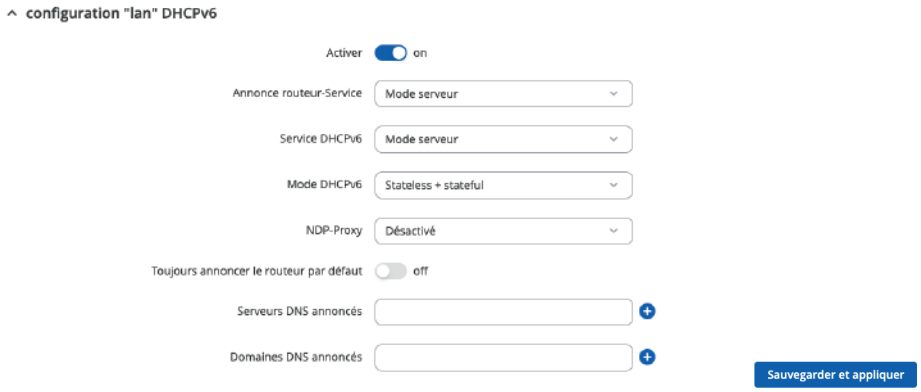
IPV6

Pour modifier les paramètres DHCPv6 de l'interface LAN, cliquez sur le bouton « Editer ».



CONFIGURATION DHCPV6

Consultez le tableau ci-dessous pour plus d'informations sur la section Paramètres avancés .

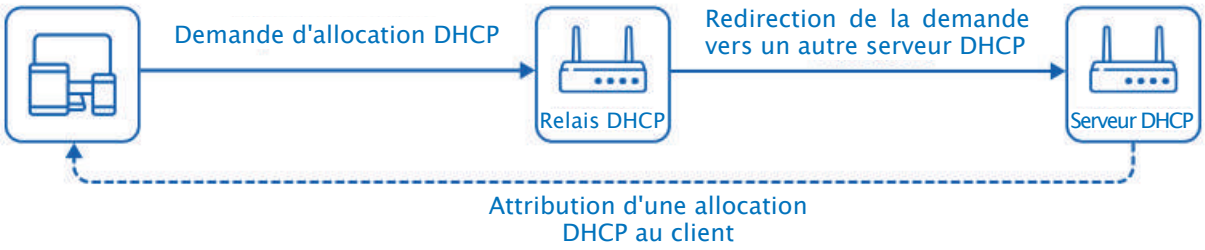


Activer	Off | On ; Par défaut : Off	Active ou désactive le serveur DHCPv6.
Annonce routeur-Service	Désactivé | Mode serveur | Mode relais | Mode hybride Par défaut : mode serveur	Variantes possibles : • Désactivé : Ne pas annoncer les appareils comme routeurs • Serveur : Annoncer cet appareil comme routeur • Relais : Annoncer l'interface parente comme routeur • Hybride : fonctionne normalement en mode « Relais » avec basculement automatique vers le mode « Serveur » en l'absence d'interface parent active.
Service DHCPv6	Désactivé | Mode serveur | Mode relais | Mode hybride Par défaut : mode serveur	Variantes possibles : Désactivé : Ne pas attribuer automatiquement d'adresses IPv6 Serveur : ce périphérique attribue des adresses IPv6 Relais : Transmet les requêtes d'attribution IPv6 entre les périphériques réseau et l'interface parente. Hybride : fonctionne normalement en mode « Relais » avec basculement automatique vers le mode « Serveur » en l'absence d'interface parent active.

Mode DHCPv6	Automatique | Préférer sans état | Préférer avec état Par défaut : Automatique	Configurez la manière dont les clients obtiendront des adresses IPv6. Variantes possibles : Privilégier le mode sans état : inciter le client à utiliser SLAAC (Stateless Address Autoconfiguration) pour obtenir une adresse IPv6. Certains périphériques peuvent ignorer cette option. Désactiver le service DHCPv6 pour imposer le mode sans état. Automatique : Le client utilisera sa méthode préférée pour obtenir une adresse IPv6. Privilégier le protocole avec état : le client doit utiliser DHCPv6 pour obtenir une adresse IPv6. Cette option peut être ignorée par certains appareils ne prenant pas en charge DHCPv6, comme Android.
NDP-Proxy	Désactivé | Mode relais | Mode hybride Par défaut : Désactivé	ariantes possibles : Désactivé : Ne pas faire transiter les paquets NDP par un proxy Relais : Transmet les paquets NDP entre les périphériques réseau et l'interface parente Hybride : fonctionne normalement en mode « Relais » avec basculement automatique en mode « Désactivé » en l'absence d'interface parent active.
Toujours annoncer le routeur par défaut	Off | On ; Par défaut : Off	S'annoncer comme routeur par défaut même si aucun préfixe public n'est disponible.
Serveur DNS annoncé	strin; Par défaut : aucun	Compléte les entrées de serveur DNS attribuées par DHCP avec celles spécifiées dans ce champ.
Domaines DNS annoncés	chaîne de caractères Par défaut : aucun	Domaine DNS attribué aux clients DHCP.

* Lorsqu'une interface est configurée pour agir comme relais DHCP, elle redirige tous les messages de requête DHCP reçus vers un autre serveur DHCP spécifié :

Remarque : les appareils dotés d'un module modem EG060K-EA prennent en charge le relais DHCP via une connexion mobile.



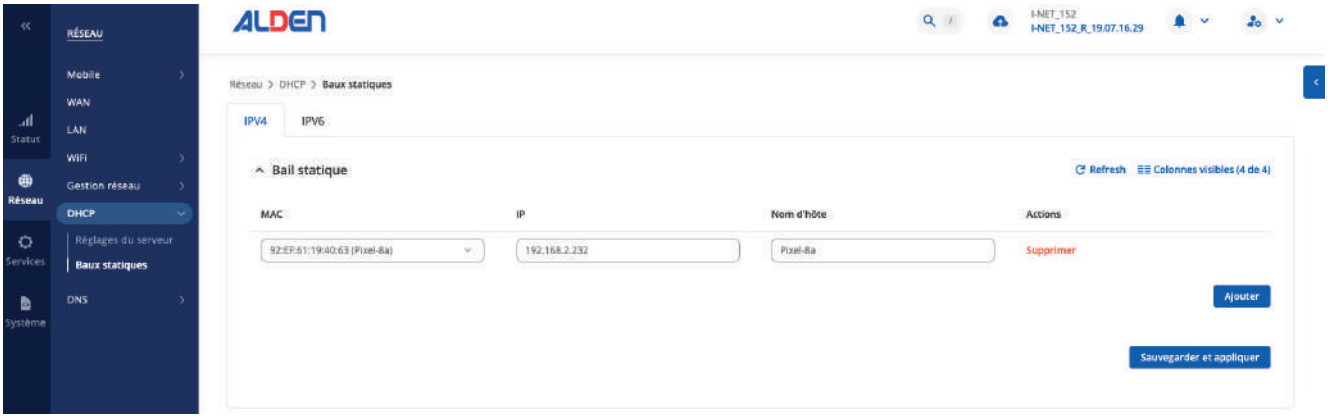
2.6.2 Menu RÉSEAU > DHCP > Baux statique

Les baux d'adresses IP statiques permettent de réserver des adresses IP spécifiques à des périphériques en les associant à leur adresse MAC. Ceci est utile pour les appareils fixes connectés au réseau et auxquels vous devez accéder fréquemment, comme une imprimante ou un téléphone IP.

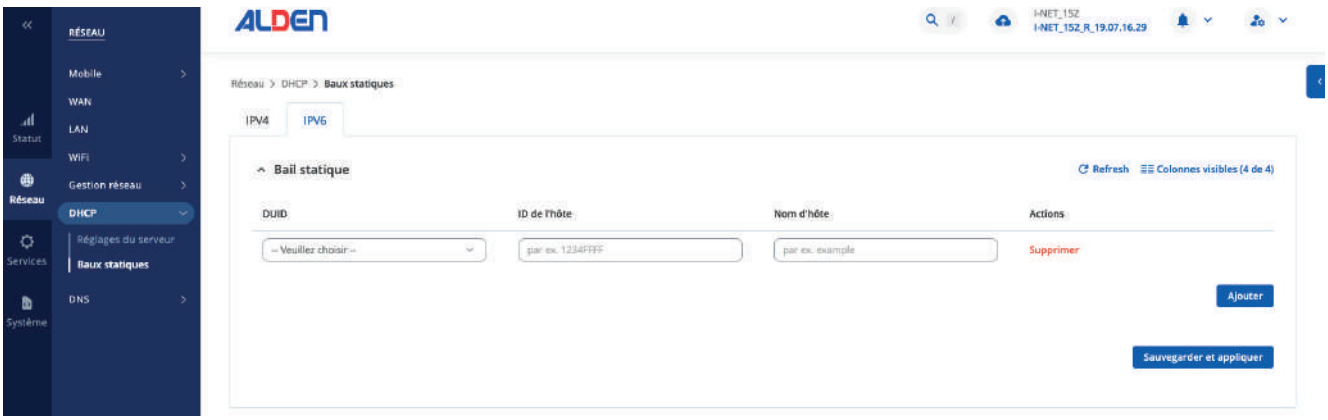
Cette page affiche les baux d'adresses IP statiques actuellement existants sur cet appareil.

Pour rendre la section du bail statique visible, définissez le protocole d'interface sur Statique .

La liste des baux statiques est vide par défaut. Pour ajouter un nouveau bail statique, cliquez sur le bouton «Ajouter».



MAC	Mac Par défaut : aucun	Adresse MAC d'un périphérique qui se connectera à cette interface réseau. Variantes possibles : Adresse MAC : 01:23:45:56:78:9a, Caractère générique : 01:23:45:56:*:*
IP	Adresse IP ; Par défaut : aucune	L'adresse IP qui sera réservée pour l'appareil spécifié.
Nom d'hôte	Chaîne de caractères Par défaut : aucun	Nom du bail statique.



DUID	DUID Par défaut : aucun	L'identifiant unique DHCP est utilisé par DHCPv6 pour identifier un appareil. Il est similaire à l'adresse MAC utilisée par DHCPv4.
ID de l'hôte	IPv6 Par défaut : aucun	Utilisé pour définir une adresse IPv6 statique. Pour l'obtenir à partir de l'adresse IPv6, supprimez le préfixe IPv6 et tous les points-virgules.
Nom d'hôte	Chaîne de caractères Par défaut : aucun	Nom du bail statique.

Après avoir cliqué sur « Sauvegarder et appliquer », les baux statiques seront enregistrés.

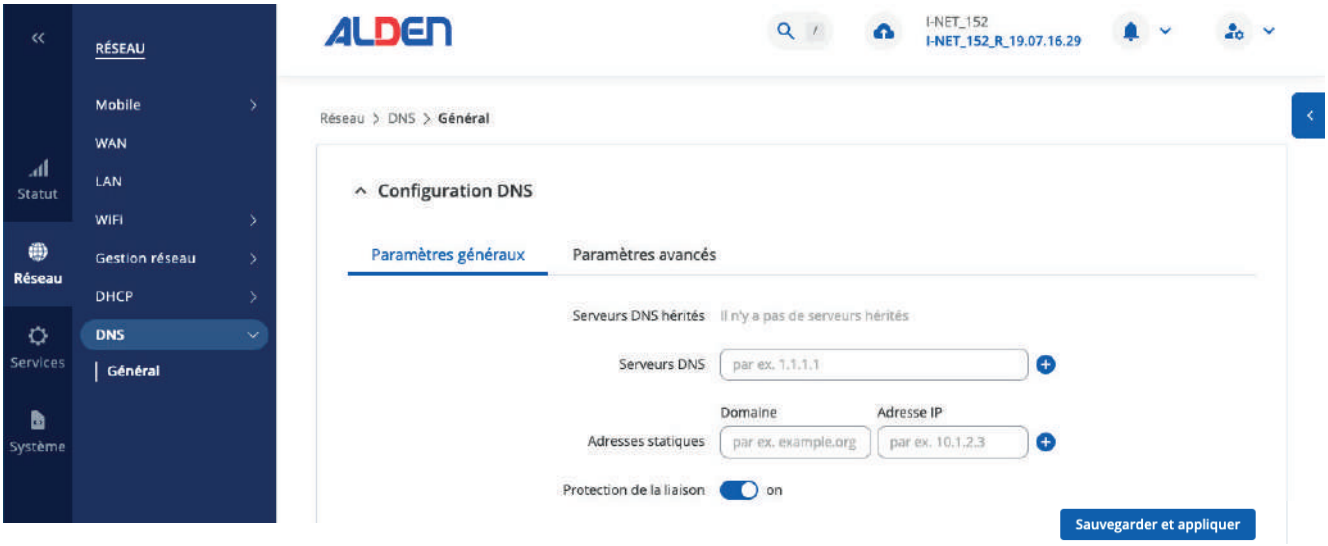
2.7 Menu RÉSEAU > DNS

La page DNS permet de configurer la manière dont l'appareil utilise ses propres serveurs DNS et les autres serveurs DNS.

2.7.1 Menu RÉSEAU > DNS > Général

Paramètres Généraux

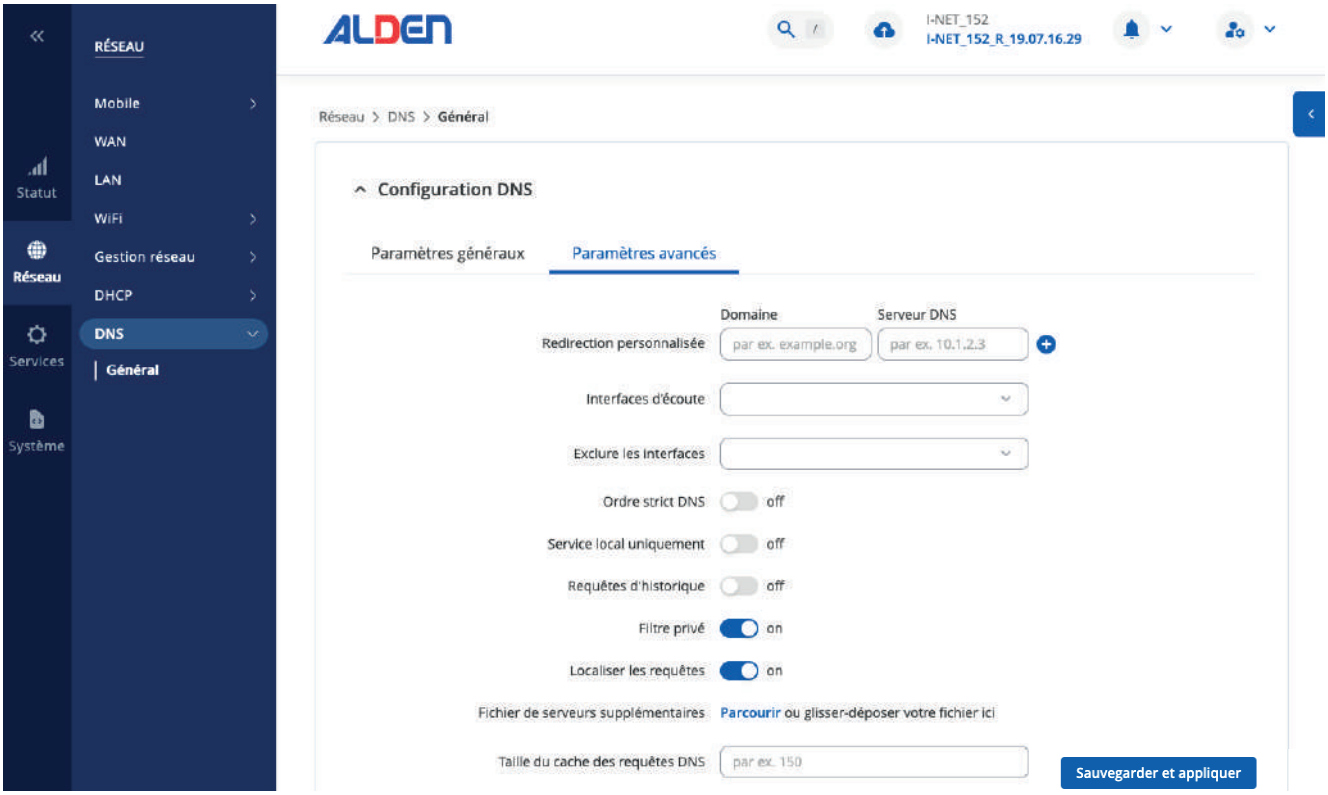
La section « Paramètres généraux » permet de configurer les principaux paramètres DNS.



Serveurs DNS hérités	Liste des serveurs hérités	Serveurs DNS hérités des interfaces WAN.
Serveurs DNS	Adresse IP (ip) Par défaut : aucun	Liste des serveurs DNS vers lesquels rediriger les requêtes. Spécifiez des serveurs complémentaires à ceux déjà installés.
Adresses statiques	Nom d'hôte (nom de domaine) | Adresse IP Par défaut : aucun	Liste des adresses IP des domaines interrogés.
Protection de la liaison	Off | On ; Par défaut : On	Ignore les réponses RFC1918 en amont. Lorsqu'elle est activée, l'appareil ne résout pas les noms de domaine des hôtes internes.

Paramètres avancés

La section Paramètres avancés permet de configurer certains paramètres DNS plus spécifiques. Consultez le tableau ci-dessous pour obtenir des informations sur chaque champ de configuration.



Redirection personnalisée	Domaine - Les noms de domaine sont acceptés (ex. : example.com). Le caractère générique (*) en début de domaine est également autorisé (ex. : *.example.com). | Serveur DNS - Adresse IP Par défaut : aucun.	Spécifiez le serveur pour un domaine. Ceci est destiné aux serveurs de noms privés.
Interfaces d'écoute	interface(s) réseau Par défaut : aucun	Limitez les requêtes DHCP et DNS à l'écoute sur ces interfaces, ainsi que sur l'interface de bouclage. Laissez ce champ vide pour écouter sur toutes les interfaces.
Exclure les interfaces	interface(s) réseau Par défaut : aucun	Empêcher l'écoute des requêtes DHCP et DNS sur ces interfaces. Laisser vide pour écouter sur toutes les interfaces.
Ordre strict DNS	Off | On ; Par défaut : On	Respecte l'ordre des serveurs DNS listés.
Service local uniquement	Off | On ; Par défaut : Off	Limiter le service DNS aux interfaces de sous-réseaux sur lesquelles nous fournissons le service DNS.
Requêtes d'historique	Off | On ; Par défaut : Off	Consigner les requêtes DNS reçues dans le journal système.
Filtre privé	Off | On ; Par défaut : On	Ne transmettez pas les requêtes de recherche inversée pour les réseaux locaux.
Localiser les requêtes	Off | On ; Par défaut : On	Localisez le nom d'hôte en fonction du sous-réseau demandeur si plusieurs adresses IP sont disponibles.
Fichier de serveurs supplémentaires	fichier texte Par défaut : aucun	Téléverse un fichier de serveurs DNS supplémentaire. Ce fichier peut contenir des lignes telles que « server=/domain/1.2.3.4 » ou « server=1.2.3.4 » pour les serveurs DNS spécifiques à un domaine ou les serveurs DNS en amont complets.
Taille du cache des requêtes DNS	entier [0..10000] Par défaut : aucun	Nombre d'entrées DNS mises en cache (maximum 10000, 0 signifie aucune mise en cache).

3 Menu SERVICES

3.1 Menu SERVICES > SERVICES DISTANTS

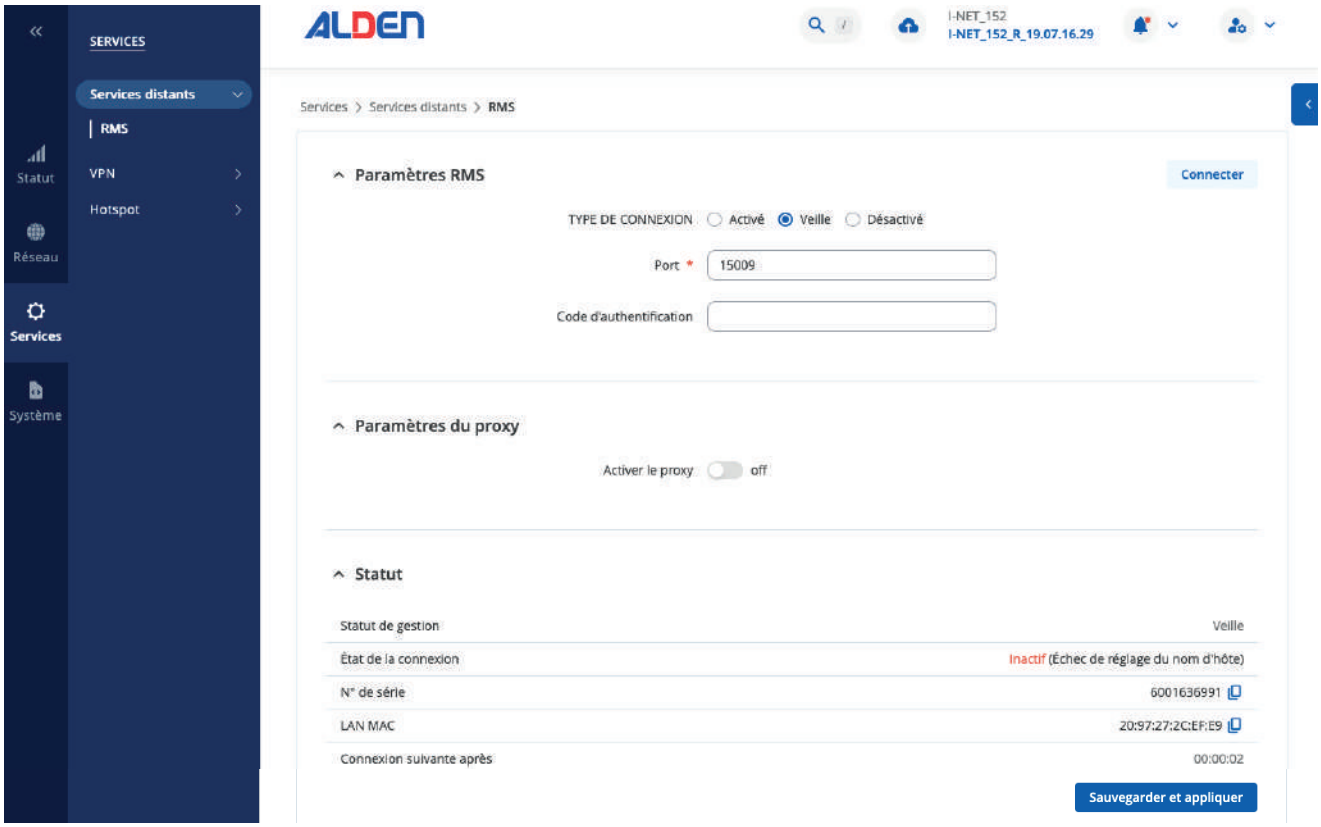
Le menu Services distants est utilisé pour configurer la manière dont l'appareil se connecte au système de gestion cloud, utilisé par le système de contrôle à distance.

3.1.1 Menu SERVICES > Services distants > RMS

I-NET 152 intègre une solution reliée à un cloud, utilisée pour des services de gestion à distance tel que les mises à 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 :



Type de connexion	Activé | Veille | Désactivé Par défaut : Activé	Définit comment l'appareil se connectera à RMS : • **Activé :** la fonctionnalité RMS est toujours active. En cas de déconnexion de RMS, l'appareil tentera de se reconnecter toutes les 2 à 5 minutes (toutes les 2 minutes la première heure, puis toutes les 5 minutes). Si l'appareil reste déconnecté de RMS pendant 14 jours, il passera en mode veille. Lors d'une tentative de connexion à RMS sans connexion Internet, le routeur tentera de rétablir la connexion toutes les 10 secondes. • **Veille :** l'appareil tente de se connecter au serveur de manière intermittente (toutes les 6 heures). Ceci permet de réduire le trafic réseau. L'utilisation de RMS ne nécessite aucune intervention de l'utilisateur. Dans le pire des cas, la connexion RMS sera établie 6 heures après l'ajout de l'appareil au service. • **Désactivé** – La fonctionnalité RMS est totalement désactivée ; par conséquent, aucune tentative de connexion n'est effectuée. Pour utiliser RMS, l'utilisateur doit activer le service sur son appareil.

Port	Entier [1..65535] Par défaut : 15009	Port du serveur RMS. Sauf si vous hébergez votre propre serveur RMS, il est conseillé de conserver la valeur par défaut.
Code d'authentification	Chaîne de caractères Par défaut : aucun	Code d'authentification fourni par RMS après l'ajout du périphérique.

RMS : Paramètres du proxy

Activer le proxy	Off | On ; Par défaut : Off	Activer la connexion RMS via un proxy.
*Adresse proxy	Noms de domaine ou adresses IP Par défaut : aucun	Spécifiez l'adresse du proxy.
*Port proxy SOCKS5	Entier [1..65535] Par défaut : 1080	Port du serveur proxy SOCKS5.
*Utiliser les identifiants	Off | On ; Par défaut : Off	Utilisez les identifiants pour la connexion proxy SOCKS5.
Nom d'utilisateur SOCKS5	Chaîne de caractères Par défaut : aucun	Spécifiez le nom d'utilisateur pour la connexion proxy SOCKS5.
Mot de passe SOCKS5	Chaîne de caractères Par défaut : aucun	Spécifiez le mot de passe pour la connexion proxy SOCKS5.

Le serveur RMS attend les connexions entrantes. L'appareil tentant de se connecter à intervalles réguliers, la connexion peut ne pas être instantanée après son ajout à RMS. Pendant la déconnexion, vous pouvez consulter le temps restant avant la prochaine tentative de connexion dans la section État.

RMS : Statut

Pour accélérer le processus en lançant une tentative de connexion immédiate, cliquez sur le bouton «Connecter». En cas d'échec ou d'état inconnu, vous pouvez tenter de vous reconnecter en cliquant sur le bouton «Reconnecter». Une fois l'appareil connecté, un bouton de réinitialisation apparaît. Utilisez-le pour déconnecter l'appareil du système RMS.

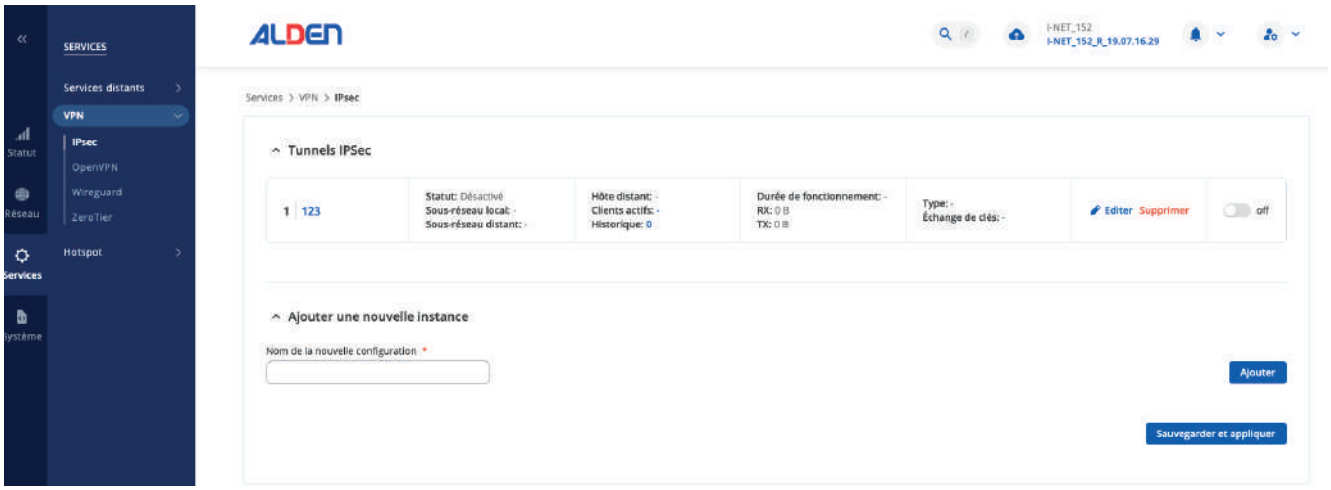
3.2 Menu SERVICES > VPN

Un réseau privé virtuel (VPN) est une méthode permettant de connecter plusieurs réseaux privés via Internet. Les VPN peuvent servir à atteindre de nombreux objectifs différents, mais voici quelques-uns de leurs principaux usages :

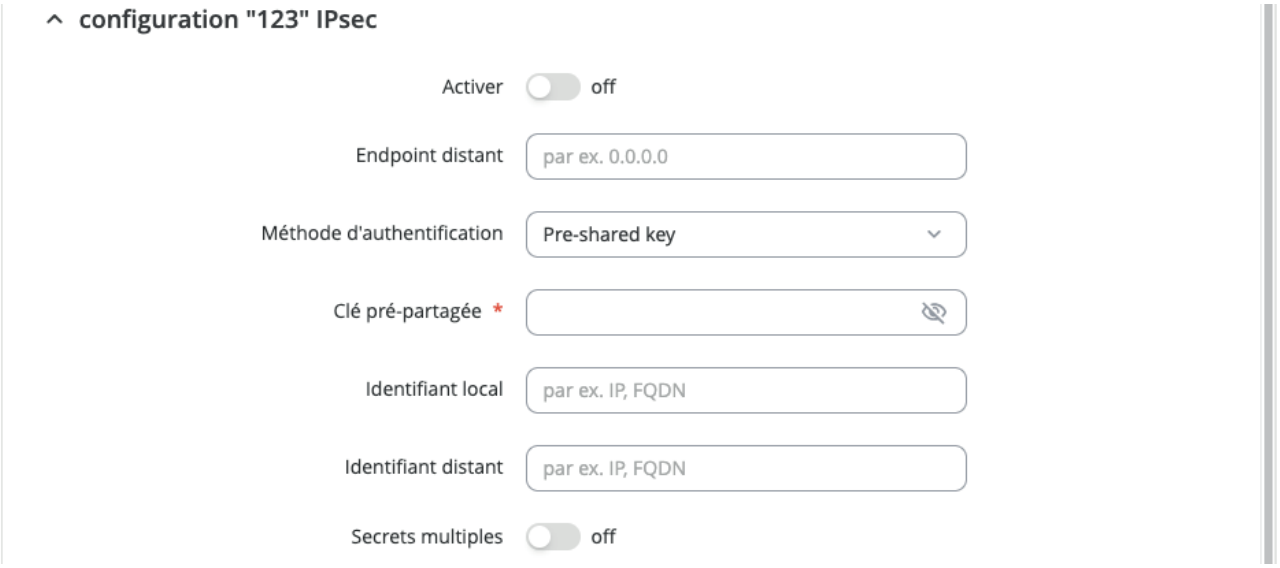
- accès entre réseaux privés distants ;
- chiffrement des données ;
- l'anonymat lors de la navigation sur Internet.

3.2.1 Menu SERVICES > VPN > IPSec

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



La section « Paramètres généraux » permet de configurer les principaux paramètres IPsec. Consultez la figure et le tableau ci-dessous pour plus d'informations sur les champs de configuration disponibles dans cette section.



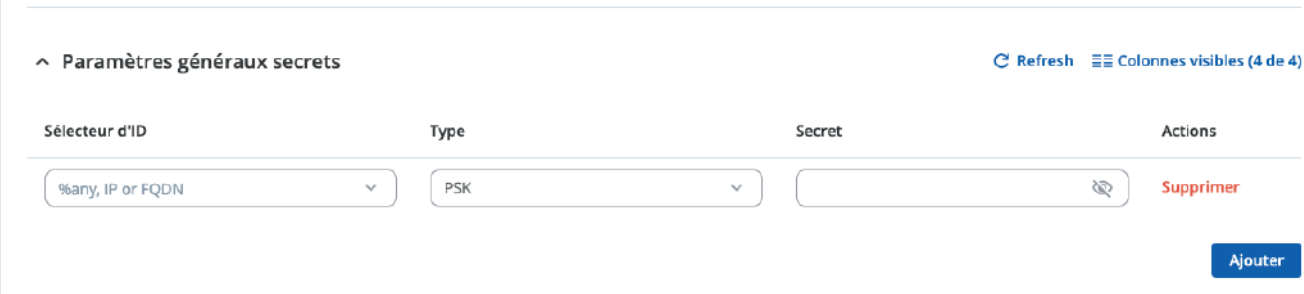
Activer	Off | On ; Par défaut : Off	Active ou désactive l'instance IPsec.
Endpoint distant	hôte | ip ; valeur par défaut : aucune	Les noms de domaine, les adresses IP (avec ou sans masque de réseau), les valeurs %any, %any4, %any6 sont acceptées (par exemple, 192.168.1.1 ou example.com).
Méthode d'authentification	Clé pré-partagée | X.509 | EAP | PKCS#12 ; Par défaut : Clé pré-partagée	Spécifiez la méthode d'authentification. Choisissez entre une clé pré-partagée et un certificat X.509.
PKCS#12 : conteneur PKCS12	-(bouton interactif)	Téléversez le fichier conteneur PKCS12.
PKCS#12 : phrase de déchiffrement PKCS12	Chaîne de caractères Par défaut : aucun	Phrase secrète pour déchiffrer un conteneur PKCS12.
Clé pré-partagée : Clé pré-partagée	Chaîne de caractères Par défaut : aucun	Un mot de passe partagé utilisé pour l'authentification entre les pairs IPsec avant l'établissement d'un canal sécurisé.
X.509 | EAP : Fichiers de certificat provenant de l'appareil	Off | On ; Par défaut : Off	Choisissez cette option si vous souhaitez sélectionner des fichiers de certificat depuis votre appareil. Les fichiers de certificat peuvent être générés ici.
X.509 | EAP : Stocker les clés dans le TPM	Off | On ; Par défaut : On	Si cette option est activée, la clé sera stockée dans l'espace de stockage sécurisé du TPM2, sous réserve de disponibilité. Remarque : cette option est uniquement disponible sur les appareils compatibles TPM et fonctionne avec IKEv2 (échange de clés).
X.509 | EAP : Clé	Fichier de clé privée Par défaut : aucun	Un fichier de clé privée.
X.509 | EAP : Phrase secrète de déchiffrement de la clé	Mot de passe pour les fichiers de clés privées Par défaut : aucun	Si le fichier de clé privée est chiffré, la phrase de passe doit être définie.
X.509 | EAP : Certificat local	Fichier .der Par défaut : aucun	Un fichier de certificat local.
X.509 | EAP : Certificat CA	Fichier .der Par défaut : aucun	Un fichier d'autorité de certification.

Identifiant local	Adresse IP | chaîne de caractères Par défaut : aucun	Définit la méthode d'identification de l'utilisateur (participant de gauche) lors de l'authentification. La longueur maximale de la valeur est de 255 caractères. IP – Adresse de protocole Internet. FQDN (nom de domaine pleinement qualifié) : identité définie par le nom de domaine complet d'un hôte (par exemple, quelquechose.quelquedomaine.com). Pris en charge uniquement par IKEv2.
Identifiant distant	Adresse IP | chaîne de caractères Par défaut : aucun	Définit la méthode d'identification du participant concerné lors de l'authentification. La longueur maximale de la valeur est de 255 caractères. • IP – Adresse de protocole Internet. • FQDN (nom de domaine pleinement qualifié) : identité définie par le nom de domaine complet d'un hôte (par exemple, quelquechose.quelquedomaine.com). Pris en charge uniquement par IKEv2.
Secrets multiples	Off | On ; Par défaut : Off	Activez cette option pour afficher la section « Paramètres secrets globaux » permettant de configurer plusieurs secrets.

Notes complémentaires :
Certains champs de configuration ne sont disponibles que lorsque certains autres paramètres sont sélectionnés. Le nom des paramètres est suivi d'un préfixe qui spécifie le type d'authentification sous lequel ils sont visibles. Différents codes couleur sont utilisés pour les différents préfixes :

- Orange pour la méthode d'authentification : clé pré-partagée
- Rouge pour la méthode d'authentification : X.509/EAP
- Bleu pour la méthode d'authentification : PKCS#12

Paramètres généraux Secrets
Cette section s'affiche lorsque l' option « Secrets multiples » est activée dans les paramètres généraux. Vous pouvez ajouter de nouvelles instances en appuyant sur Ajouter .



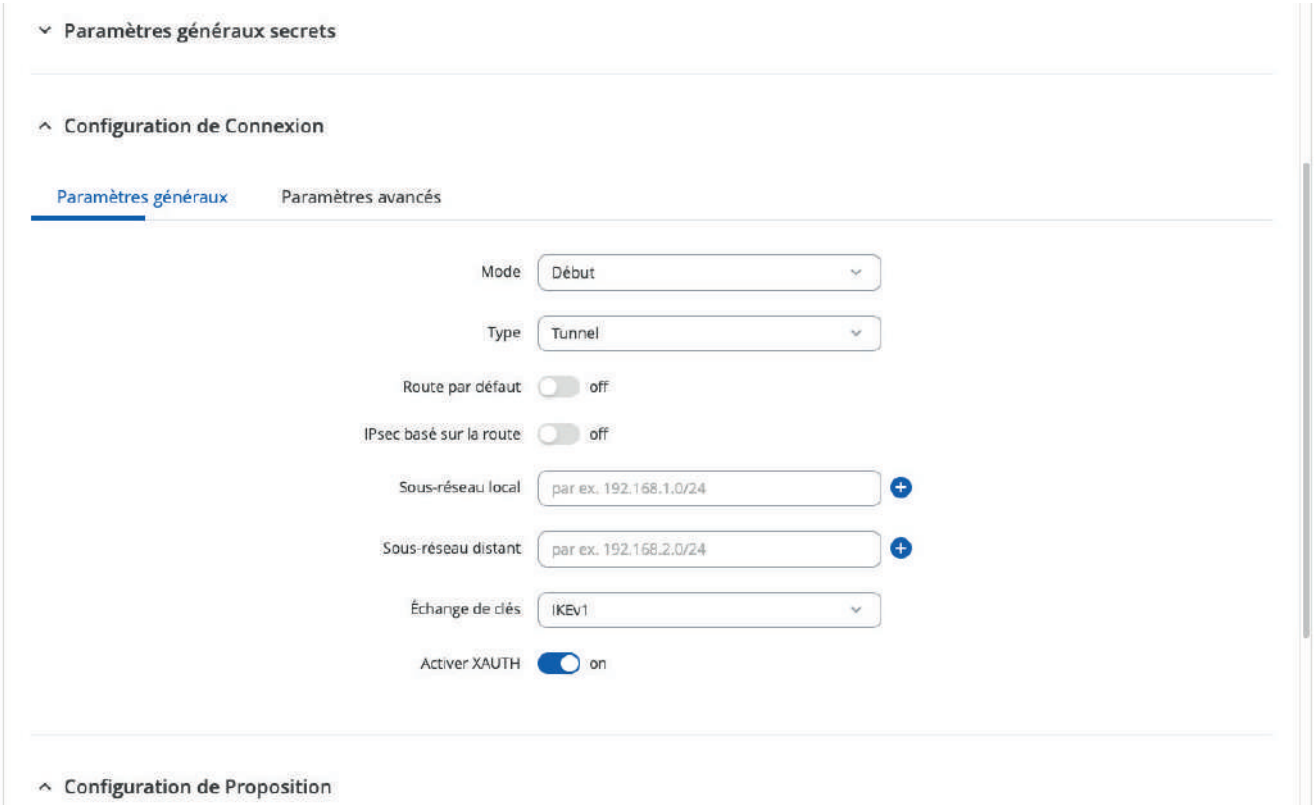
Sélecteur d'ID	%any, adresse IP ou nom de domaine complet Par défaut : aucun	Chaque secret peut être précédé d'une liste de sélecteurs d'identifiants optionnels. Un sélecteur peut être une adresse IP, un nom de domaine pleinement qualifié (FQDN), utilisateur@FQDN ou %any. Lors de l'utilisation d'IKEv1, utilisez une adresse IP. La longueur maximale d'une valeur est de 255 caractères. Remarque : IKEv1 ne prend en charge que les adresses IP comme sélecteurs d'identifiants.
Taper	PSK | XAUTH | EAP | RSA | PKCS#12 Par défaut : PSK	Assurez-vous d'activer l'option « Activer XAUTH » dans les paramètres de connexion si vous souhaitez utiliser des secrets de type XAUTH.
Secrète	chaîne de caractères Par défaut : aucun	Un mot de passe partagé (ou un fichier de clé EAP) pour l'authentification entre les pairs. La longueur minimale est de 5 caractères. Tous les caractères sont autorisés sauf `.

RSA | PKCS#12 : Secret	Fichier de clé privée ; Par défaut : aucun	Un fichier de clé privée.
RSA | PKCS#12 : Phrase secrète de déchiffrement de la clé	Mot de passe pour les fichiers de clés privées ; Par défaut : aucun	Si le fichier de clé privée est chiffré, la phrase de passe doit être définie.
Actes	-(bouton interactif)	Supprime le secret global.

IPSec : Configuration de Connexion

La section « Configuration de connexion » permet de configurer les principaux paramètres d'une connexion IPsec. Consultez la figure et le tableau ci-dessous pour plus d'informations sur les champs de configuration disponibles dans cette section.

IPSec : Paramètres généraux



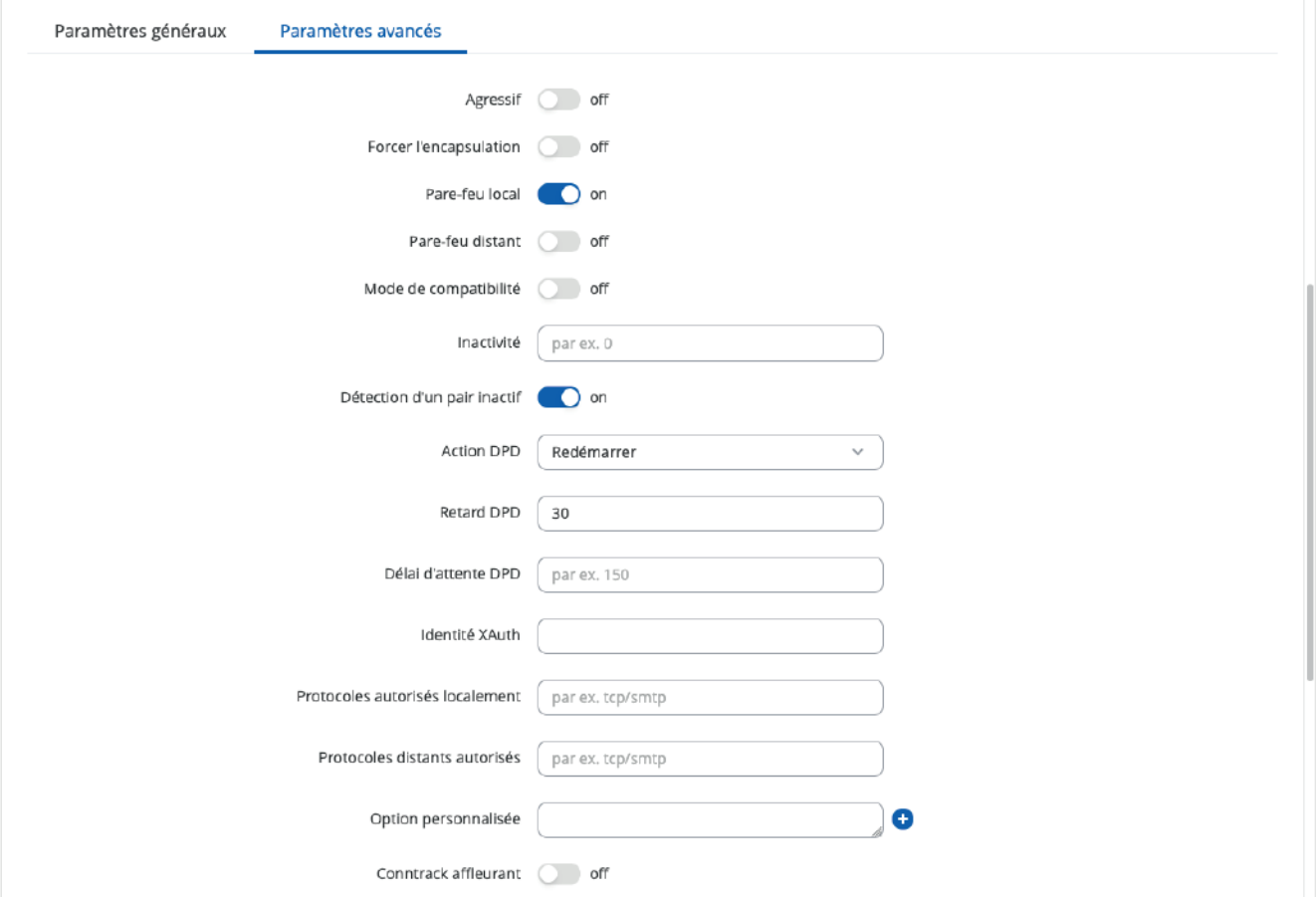
Mode	Démarrer | Ajouter | Itinéraire Par défaut : Démarrer	Spécifie l'opération qui sera effectuée automatiquement au démarrage d'IPSec.
Type	Tunnel | Transport Par défaut : Tunnel	Type de connexion. • Tunnel - protège les informations de routage interne en encapsulant l'intégralité du paquet IP (en-tête 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 tunnelage (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 : IPsec basé sur la route	Off | On ; Par défaut : Off	Un tunnel VPN IPsec a été créé entre deux points d'extrémité.
Tunnel : Adresse IP	Adresse IP Par défaut : aucune	Attribuer une adresse IP à l'interface XFRM.

Tunnel : MTU	Entier [68..9200] ; Par défaut : aucun	Définit la taille maximale de l'unité de transmission (MTU). Il s'agit de la taille maximale d'une unité de données de protocole (PDU) pouvant être transmise en une seule transaction de couche réseau.
Tunnel : Sous-réseau local	Adresse IP/masque de sous-réseau | Par défaut : aucun	Sous-réseau privé derrière le participant local (de gauche), exprimé sous la forme réseau/masque de sous-réseau. IKEv2 prend en charge plusieurs sous-réseaux, tandis qu'IKEv1 n'interprète que le premier.
Tunnel : Sous-réseau distant	Par défaut : aucun	Sous-réseau privé derrière le participant distant, exprimé sous la forme réseau/masque de sous-réseau. IKEv2 prend en charge plusieurs sous-réseaux, tandis qu'IKEv1 n'interprète que le premier.
Transport : Lier à	Par défaut : aucun	Liez-vous à une interface GRE ou L2TP pour créer une connexion GRE/L2TP sur IPsec.
Activer XAuth	Off | On ; Par défaut : Off	Active l'authentification étendue.

Notes complémentaires :

- Certains champs de configuration ne sont disponibles que lorsque certains autres paramètres sont sélectionnés. Le nom des paramètres est suivi d'un préfixe qui spécifie le type d'authentification sous lequel ils sont visibles. Différents codes couleur sont utilisés pour les différents préfixes :
- Rouge pour type : Tunnel
- Bleu pour le type : transport

IPSec : Paramètres avancés



Agressif	Off | On ; Par défaut : Off	Activez ou désactivez le mode agressif pour les connexions sortantes. Le mode agressif effectue moins d'échanges (4 messages au total) que le mode principal (6 messages au total) en stockant la plupart des données lors du premier échange. En mode agressif, les informations sont échangées avant l'établissement d'un canal sécurisé, ce qui le rend moins sécurisé mais plus rapide que le mode principal. Le mode agressif est disponible uniquement avec IKEv1 ; si IKEv2 est sélectionné, ce champ est masqué.
Forcer l'encapsulation	Off | On ; Par défaut : Off	Force l'encapsulation UDP pour les paquets ESP même si une situation « sans 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 : Off	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 disposant de plusieurs sous-réseaux.
Inactivité	Entier Par défaut : aucun	Définit l'intervalle de délai d'expiration après lequel une CHILD_SA est fermée si elle n'a envoyé ni reçu de trafic.
Détection d'un pair inactif	Off | On ; Par défaut : On	Fonction utilisée lors de l'échange de clés Internet (IKE) pour détecter un pair indisponible. Elle permet de réduire le trafic en minimisant le nombre de messages lorsque le pair distant est indisponible et sert de mécanisme de basculement.
Détection des pairs inactifs : Action DPD	Redémarrer | Maintenir | Effacer | Aucun Par défaut : Redémarrer	Contrôle l'utilisation du protocole de détection des pairs inactifs, dans lequel des messages de notification sont envoyés périodiquement afin de vérifier l'activité du pair IPsec.
Détection des pairs inactifs : Retard DPD	Entier Par défaut : aucun	La fréquence d'envoi des messages R_U_THERE ou des échanges INFORMATIONNELS au pair.
Détection de pair inactif : Délai d'attente DPD	Entier Par défaut : aucun	Définit l'intervalle de délai d'inactivité, après lequel toutes les connexions à un pair sont supprimées.
Identité XAuth	Chaîne de caractères Par défaut : aucun	L'identité/le nom d'utilisateur que le client utilise pour répondre à une requête XAuth. Si cette information n'est pas définie, l'identité IKEv1 sera utilisée comme identité XAuth.
Tunnel : IP source distant	Adresse IP Par défaut : aucun	L'adresse IP source interne à utiliser dans un tunnel pour le pair 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 adresse IP virtuelle.
Tunnel : DNS à distance	Adresse IP Par défaut : aucun	Liste des adresses de serveurs DNS à échanger comme attributs de configuration. Côté serveur, seules les adresses IPv4/IPv6 fixes sont autorisées et définissent les serveurs DNS attribués au client.
Protocoles autorisés localement	Chaîne de caractères Par défaut : aucun	Protocoles et ports autorisés sur la connexion, également appelés sélecteurs de ports. Définis sous la forme « protocole/port », par exemple : « 17/1701 », « 17/%any » ou « udp/l2f ».
Protocoles distants autorisés	Chaîne de caractères Par défaut : aucun	Protocoles et ports autorisés sur la connexion, également appelés sélecteurs de ports. Définis sous la forme « protocole/port », par exemple : « 17/1701 », « 17/%any » ou « udp/l2f ».
Option personnalisée	Chaîne de caractères Par défaut : aucun	Syntaxe : option = valeur. Les caractères suivants sont acceptés : a-z A-Z 0-9 =/_.:{}%\s-
Tunnel : Interfaces Passthrough (Traversant)w	Interfaces réseau Par défaut : aucun	Interfaces réseau à inclure dans le mode de transfert IPsec.

Tunnel : Sous-réseaux Passthrough (Traversant)	adresse IP/masque de sous-réseau Par défaut : aucune	Adresse/sous-réseau IPv4 ou IPv6.
Conntrack affleurant	Off | On ; Par défaut : Off	Vider le cache de conntrack une fois la connexion IPsec établie avec succès.

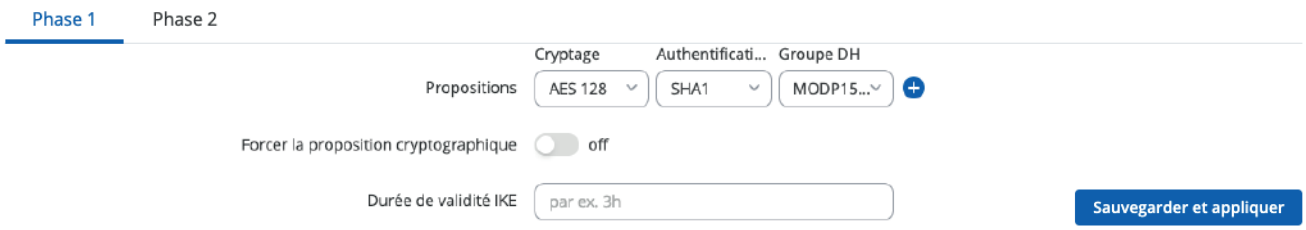
Notes complémentaires :
• Certains champs de configuration ne sont disponibles que lorsque certains autres paramètres sont sélectionnés. Le nom des paramètres est suivi d'un préfixe qui spécifie le type d'authentification sous lequel ils sont visibles. Différents codes couleur sont utilisés pour les différents préfixes :
• Rouge pour type : Tunnel
• Bleu pour la détection des pairs inactifs : activé

IPSec : Configuration de proposition

La section « Paramètres de la proposition » permet de configurer les paramètres des phases 1 et 2 d'IKE (Internet Key Exchange). IKE est un protocole utilisé pour établir des associations de sécurité (SA) pour la connexion IPsec. Ce processus est indispensable avant l'établissement de tout tunnel IPsec. Il se déroule en deux phases :

Phase	Mode	
Phase 1 • Établit un canal sécurisé entre pairs • Authentifie les pairs • Négocie la politique de l'Afrique du Sud • Partage des clés secrètes • Mise en place d'un tunnel sécurisé pour la phase 2	Mode principal (figure 1) • 6 paquets échangés • Identité protégée lors de l'échange	Mode agressif (figure 2) • 3 paquets échangés • Les informations d'identité échangées avant l'établissement d'un canal sécurisé
Phase 2 • Configure des SA IPsec correspondantes • Renégocie périodiquement les SA IPsec	Mode rapide • 3 paquets échangés • Paramètres IPsec SA (ESP/AH, SHA/MD5) établis • Ensemble à vie SA	

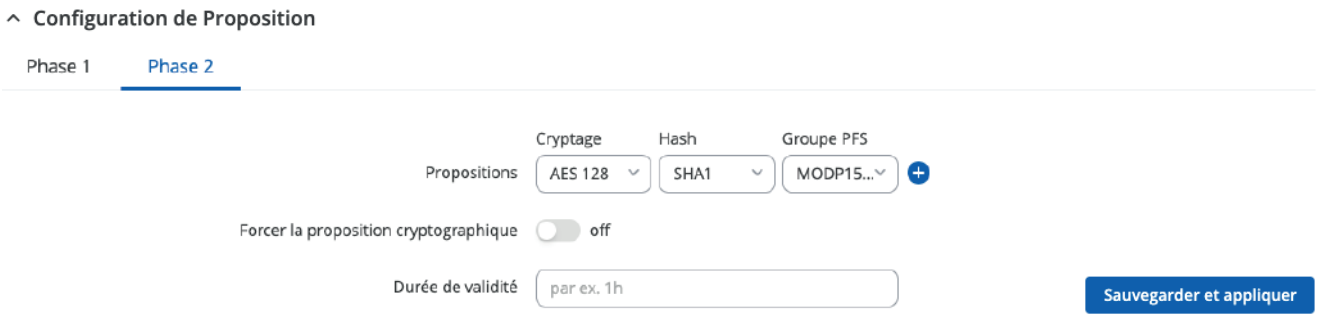
Phase 1



Algorithme de chiffrement	3DES | DES | AES 128 | AES 192 | AES 256 | AES 128 CTR | AES 192 CTR | AES 256 CTR | AES128 CCM8 | AES192 CCM8 | AES256 CCM8 | AES128 GCM8 | AES192 GCM8 | AES256 GCM8 | AES128 CCM12 | AES192 CCM12 | AES256 CCM12 | AES128 GCM12 | AES192 GCM12 | AES256 GCM12 | AES128 CCM16 | AES192 CCM16 | AES256 CCM16 | AES128 GCM16 | AES192 GCM16 | AES256 GCM16 | ChaCha20 Poly1305; Par défaut : AES 128	Algorithme utilisé pour le chiffrement des données.

Authentification	MD5 | SHA1 | SHA256 | SHA384 | SHA512 | AESXCBC ; Par défaut : SHA1	Algorithme utilisé pour l'échange d'informations d'authentification et de hachage.
Groupe DH	MODP768 | MODP1024 | MODP1536 | MODP2048 | MODP3072 | MODP4096 | MODP8192 | ECP192 | ECP224 | ECP256 | ECP384 | ECP521 | ECP224 BP | ECP256 BP | ECP384 BP | ECP512 BP | Curve25519 | Curve448 Par défaut : MODP1536	Le groupe Diffie-Hellman (DH) est utilisé lors de l'échange de clés. Plus le numéro de groupe est élevé, plus la sécurité est renforcée, mais le calcul de la clé est plus long et plus gourmand en ressources. Il doit correspondre à une autre connexion entrante pour établir IPSec.
Proposition de crypto-forcer	Off | On ; Par défaut : Off	Seules les propositions sélectionnées seront utilisées une fois activées.
Durée de validité IKE	Chaîne de caractères Par défaut : aucun	Durée de validité du canal de chiffrement d'une connexion (ISAKMP ou IKE SA) avant renégociation. Cette durée est exprimée en secondes. Les suffixes s, m, h et d précisent respectivement les unités suivantes : secondes, minutes, heures et jours.

Phase 2

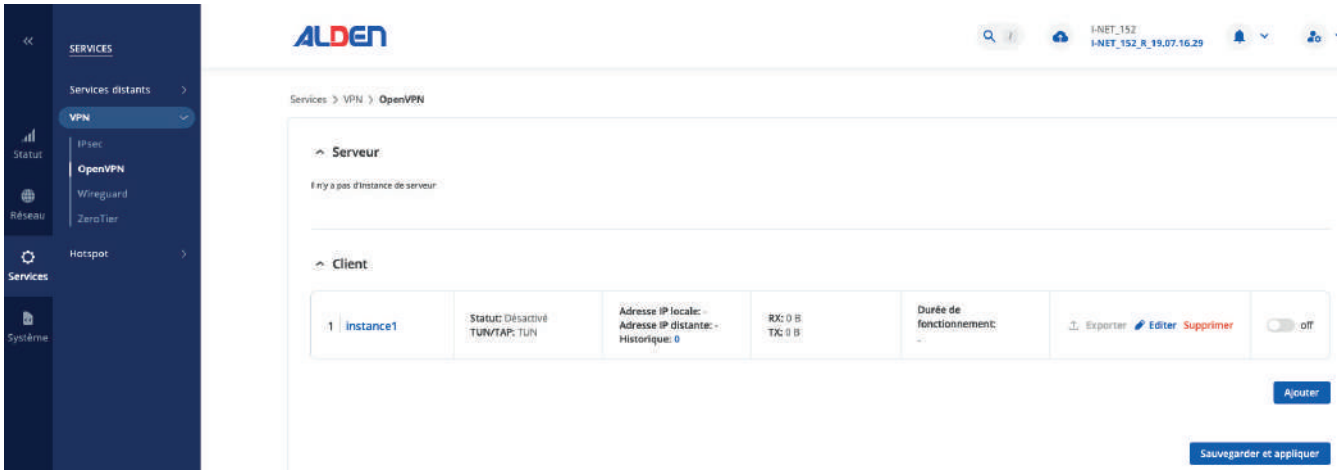


Cryptage	3DES | DES | AES 128 | AES 192 | AES 256 | AES 128 CTR | AES 192 CTR | AES 256 CTR | AES128 CCM8 | AES192 CCM8 | AES256 CCM8 | AES128 GCM8 | AES192 GCM8 | AES256 GCM8 | AES128 CCM12 | AES192 CCM12 | AES256 CCM12 | AES128 GCM12 | AES192 GCM12 | AES256 GCM12 | AES128 CCM16 | AES192 CCM16 | AES256 CCM16 | AES128 GCM16 | AES192 GCM16 | AES256 GCM16 | ChaCha20 Poly1305; Par défaut : AES 128	Algorithme utilisé pour le chiffrement des données.

Hash	MD5 | SHA1 | SHA256 | SHA384 | SHA512 ; par défaut : SHA1	Algorithme utilisé pour l'échange d'informations d'authentification et de hachage.
Groupe PFS	MODP768 | MODP1024 | MODP1536 | MODP2048 | MODP3072 | MODP4096 | MODP8192 | ECP192 | ECP224 | ECP256 | ECP384 | ECP521 | Pas de PFS Par défaut : MODP768	Le PFS (Perfect Forward Secrecy) doit correspondre à une autre connexion entrante pour établir IPSec.
Forcer la proposition cryptographique	Off | On ; Par défaut : Off	Seules les propositions sélectionnées seront utilisées une fois activées.
Durée de validité	chaîne de caractères Par défaut : aucun	Durée de validité du canal de chiffrement d'une connexion (ISAKMP ou IKE SA) avant renégociation. Cette durée est exprimée en secondes. Les suffixes s, m, h et d précisent respectivement les unités suivantes : secondes, minutes, heures et jours.

3.2.2 Menu SERVICES > VPN > OpenVPN

OpenVPN est un logiciel libre qui met en œuvre des techniques de réseau privé virtuel (VPN) pour créer des connexions sécurisées point à point ou site à site, en configuration routée ou pontée, et pour l'accès à distance. Il est souvent considéré comme le protocole VPN le plus universel grâce à sa flexibilité, sa prise en charge du protocole de sécurité SSL/TLS, ses multiples méthodes de chiffrement, ses nombreuses fonctionnalités réseau et sa compatibilité avec la plupart des systèmes d'exploitation.



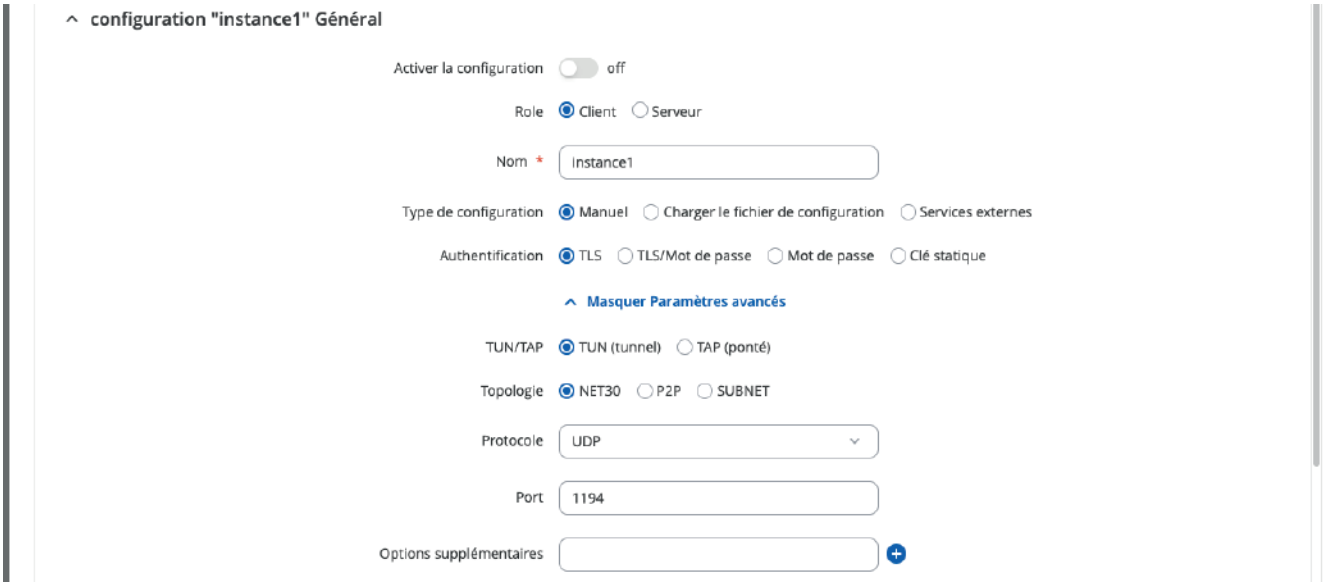
OpenVPN : Client

Un client OpenVPN est une entité qui initie une connexion à un serveur OpenVPN.

Exporter	-(bouton interactif)	Exporte la configuration de l'instance vers un fichier .ovpn.
Editer	-(bouton interactif)	Ouvre la fenêtre de configuration de l'instance.
Supprimer	-(bouton interactif)	Supprime une instance.

Client : Configuration Général

Pour commencer la configuration, cliquez sur le bouton « Editer », puis sélectionnez « Rôle : Client » . Consultez la figure et le tableau ci-dessous pour plus d'informations sur les champs de configuration du client OpenVPN :



Activer la configuration	Off | On ; Par défaut : Off	Activer la configuration actuelle.
Rôle	Client | Serveur Par défaut : Client	Choisissez un rôle pour l'instance OpenVPN.
Nom	Chaîne de caractères Par défaut : instance1	Nom de l'instance OpenVPN.
Type de configuration	Manuel | Téléverser un fichier de configuration | Services externes Par défaut : Manuel	Choisissez le type de configuration.
Fournisseurs VPN	ExpressVPN | NordVPN Par défaut : NordVPN	Représente une liste des fournisseurs de VPN disponibles.
Serveurs VPN	Royaume-Uni | États-Unis | Australie | Afrique du Sud | Personnalisé Par défaut : Royaume-Uni	Représente une liste des serveurs VPN disponibles.
Nom d'utilisateur	Chaîne de caractères Par défaut : aucun	Nom d'utilisateur utilisé pour l'authentification auprès du serveur VPN.
Mot de passe	chaîne de caractères Par défaut : aucun	Mot de passe utilisé pour l'authentification auprès du serveur VPN.
Activer l'analyse	Off | On ; Par défaut : Off	En activant l'analyse syntaxique, vous pourrez modifier la configuration ultérieurement.
Fichier de configuration OpenVPN	-(bouton interactif)	Téléverser la configuration OpenVPN. Attention ! Cette opération écrasera votre configuration actuelle.
Authentification	TLS | TLS/Mot de passe | Mot de passe | Clé statique Par défaut : TLS	Choisissez une méthode pour authentifier votre réseau OpenVPN.
TUN/TAP	TUN (tunnel) | TAP (pont) Par défaut : TUN (tunnel)	Type d'interface VPN virtuelle.
Topologie	NET30 | P2P | SUBNET (non affiché avec une clé statique) ; Par défaut : NET30	La topologie d'adressage virtuel détermine comment l'adressage IP et le routage sont gérés entre le serveur et les clients.

Protocole	UDP | TCP | UDP4 | TCP4 | UDP6 | TCP6 ; Par défaut : UDP	Protocole de transport utilisé pour la connexion. Remarque : UDP et TCP ne prennent pas en charge les connexions IPv6 ; utilisez plutôt UDP6 ou TCP6.
Port	entier [0..65535] ; Par défaut : 1194	Port TCP/UDP pour les points de terminaison locaux et distants. Assurez-vous que ce port est ouvert dans le pare-feu.
Options supplémentaires	chaîne de caractères Par défaut : aucune	Saisissez les options supplémentaires à ajouter à la configuration OpenVPN. Si une option est déjà utilisée, la nouvelle option sera prioritaire.

Client : Configuration de Réseau



Clé statique : adresse IP du point de terminaison du tunnel local	Adresse IP Par défaut : aucun	Adresse IP de l'interface réseau locale virtuelle.
Clé statique : adresse IP du point de terminaison du tunnel distant	Adresse IP Par défaut : aucun	Adresse IP de l'interface réseau distante virtuelle.
Hôte distant/adresse IP	Adresse IP Par défaut : aucun	Adresse IP ou nom de domaine du serveur OpenVPN.
Réseau distant	ip4 Par défaut : aucun	Adresse IP du réseau local distant.
TAP (ponté) : Pont	Réseau local | aucun Par défaut : réseau local	Attribuer une interface TAP à un pont.
Clé statique : Point de terminaison du tunnel local IPv6	Adresse IP Par défaut : aucun	Adresse IPv6 de l'interface réseau local virtuel.
Clé statique : Point de terminaison du tunnel distant IPv6	Adresse IP Par défaut : aucun	Adresse IPv6 de l'interface réseau distante virtuelle.
LZO	Aucun | Adaptatif | Oui | Non Par défaut : aucun	Utilisez la compression LZO rapide. Grâce à la compression LZO, votre connexion VPN générera moins de trafic réseau.
Résoudre la nouvelle tentative	Entier | infini Par défaut : infini	Essayez de résoudre le nom d'hôte du serveur pendant X secondes avant d'abandonner.
Restez en vie	Deux entiers séparés par un espace Par défaut : aucun	Essayez de maintenir la connexion active. Deux valeurs sont requises : ping_interval et ping_restart, par exemple : 10 120.

Client : Configuration de Sécurité



TLS/Mot de passe / Mot de passe : Nom d'utilisateur	Chaîne de caractères Par défaut : aucun	Nom d'utilisateur du client VPN.
TLS/Mot de passe / Mot de passe : Mot de passe	Chaîne de caractères Par défaut : aucun	Mot de passe du client VPN.
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 de chiffrement de paquets (chiffrement).
Chiffrements de données	dépend de l'authentification Par défaut : AES-256-CBC	Sélectionnez les algorithmes de chiffrement autorisés dans la liste ; ajoutez une valeur personnalisée si nécessaire.
Algorithme d'authentification	Aucun | MD5 | SHA1 | SHA256 | SHA384 | SHA512 Par défaut : SHA1	Type d'algorithme d'authentification HMAC.
TLS / TLS/Mot de passe / Mot de passe : Authentification HMAC supplémentaire	Aucune | Authentification uniquement (tls-auth) | Authentification uniquement (tls-auth) ; Par défaut : Aucun	Ajoutez une couche supplémentaire d'authentification HMAC au-dessus du canal de contrôle TLS pour vous protéger contre les attaques par déni de service (DoS).
TLS / TLS/Mot de passe / Mot de passe : direction de la clé HMAC	0 | 1 Par défaut : 1	La valeur de direction de la clé d'authentification HMAC est arbitraire et doit être opposée entre les parties communicantes (ou être totalement omise).

Client : Configuration de Certificats



TLS / TLS/Mot de passe / Mot de passe : Utiliser le format PKCS #12	Off | On ; Par défaut : Off	Utilisez le format de fichier d'archive PKCS #12 pour regrouper tous les membres d'une chaîne de confiance.
TLS / TLS/Mot de passe / Mot de passe : chaîne de certificats PKCS #12	-(bouton interactif)	Téléverse un fichier de chaîne de certificats PKCS #12.
TLS / TLS/Mot de passe / Mot de passe : phrase secrète PKCS #12	Chaîne de caractères Par défaut : aucun	Phrase secrète pour déchiffrer les certificats PKCS #12.
TLS / TLS/Mot de passe / Mot de passe : Fichiers de certificat de l'appareil	Off | On ; Par défaut : Off	Choisissez cette option si vous souhaitez sélectionner des fichiers de certificat depuis l'appareil.
TLS / TLS/Mot de passe / Mot de passe : Stocker la clé client dans le TPM	Off | On ; Par défaut : On	Si cette option est activée, la clé sera stockée dans la mémoire sécurisée du TPM2 si de l'espace est disponible. Remarque : cette option est uniquement disponible sur les appareils compatibles avec le TPM.
TLS / TLS/Mot de passe / Mot de passe : Autorité de certification	Fichier .ca ; Par défaut : aucun	Le certificat numérique vérifie la propriété d'une clé publique par le sujet nommé du certificat.
TLS / TLS/Mot de passe : Certificat client	Fichier .crt Par défaut : aucun	Identifier un client ou un utilisateur, authentifier le client auprès du serveur et établir précisément son identité.
TLS / TLS/Mot de passe : Clé client	Fichier .key Par défaut : aucun	Il a été généré dans le même but qu'un certificat client.
TLS / TLS/Mot de passe : Mot de passe de déchiffrement de la clé privée (facultatif)	Chaîne de caractères Par défaut : aucun	Déchiffrer la clé privée avec le mot de passe (facultatif).
Clé statique : Clé pré-partagée statique	Fichier .key Par défaut : aucun	Une clé pré-partagée (PSK) est un secret partagé qui a été préalablement échangé entre deux parties via un canal sécurisé avant d'être utilisé.

Notes complémentaires :

• Certains champs de configuration ne sont disponibles que lorsque certains autres paramètres sont sélectionnés.

Le nom des paramètres est suivi d'un préfixe qui spécifie le type d'authentification sous lequel ils sont visibles.

Différents codes couleur sont utilisés pour les différents préfixes :

- Rouge pour l'authentification : TLS
- Vert pour l'authentification : TLS/Mot de passe
- Violet pour l'authentification : clé statique
- Bleu pour l'authentification : Mot de passe
- Brun pour la configuration OpenVPN à partir du fichier

• 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.

OPEN VPN : Serveur

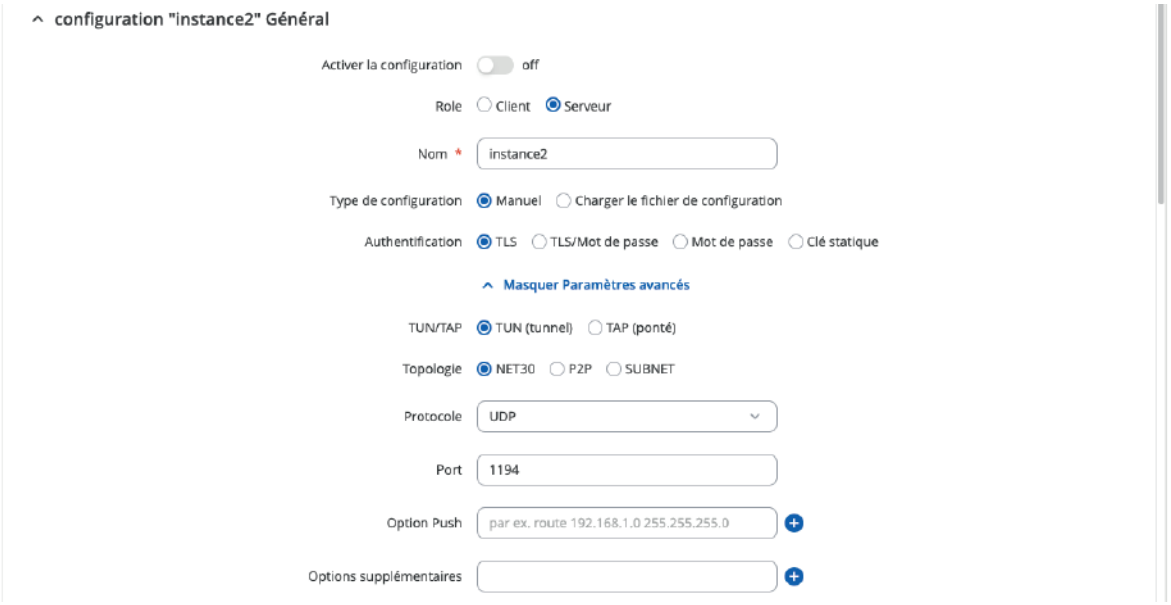
Un serveur OpenVPN est une entité qui attend les connexions entrantes des clients OpenVPN. Une seule instance de serveur OpenVPN peut être ajoutée.

Un serveur doit posséder une adresse IP publique pour être accessible depuis le réseau public (Internet).



Exporter	-(bouton interactif)	Exporte la configuration de l'instance vers un fichier .ovpn.
Editer	-(bouton interactif)	Ouvre la fenêtre de configuration de l'instance.
Supprimer	-(bouton interactif)	Supprime une instance.

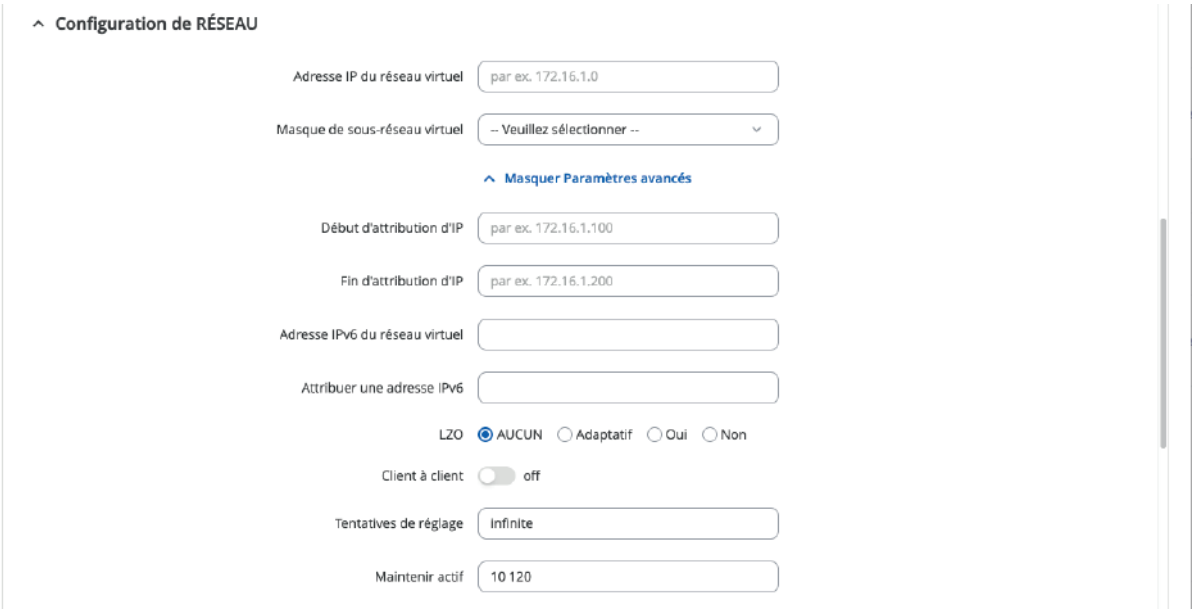
Serveur : Configuration Général



Activer la configuration	Off | On ; Par défaut : Off	Activer la configuration actuelle.
Rôle	Client | Serveur Par défaut : Serveur	Choisissez un rôle pour l'instance OpenVPN.
Nom	Chaîne de caractères Par défaut : instance1	Nom de l'instance OpenVPN.
Type de configuration	Manuel | Charger le fichier de configuration Par défaut : Manuel	Choisissez le type de configuration.
Activer l'analyse	Off | On ; Par défaut : Off	En activant l'analyse syntaxique, vous pourrez modifier la configuration ultérieurement.
fichier de configuration OpenVPN	-(bouton interactif)	Téléverser la configuration OpenVPN. Attention ! Cette opération écrasera votre configuration actuelle.
Authentification	TLS | TLS/Mot de passe | Mot de passe | Clé statique Par défaut : TLS	Choisissez une méthode pour authentifier votre réseau OpenVPN.
TUN/TAP	TUN (tunnel) | TAP (pont) Par défaut : TUN (tunnel)	Type d'interface VPN virtuelle.
Topologie	NET30 | P2P | SOUS-RÉSEAU (non affiché avec une clé statique) ; Par défaut : NET30	La topologie d'adressage virtuel détermine comment l'adressage IP et le routage sont gérés entre le serveur et les clients.

Protocole	UDP | TCP | UDP4 | TCP4 | UDP6 | TCP6 ; Par défaut : UDP	Protocole de transport utilisé pour la connexion. Remarque : UDP et TCP ne prennent pas en charge les connexions IPv6 ; utilisez plutôt UDP6 ou TCP6.
Port	Entier [0..65535] Par défaut : 1194	Port TCP/UDP pour les points de terminaison locaux et distants. Assurez-vous que ce port est ouvert dans le pare-feu.
Option Push (non affichée avec la touche statique)	Chaîne de caractères Par défaut : aucune	Renvoyer une option de configuration au client pour exécution à distance.
Options supplémentaires	Chaîne de caractères Par défaut : aucune	Saisissez les options supplémentaires à ajouter à la configuration OpenVPN. Si une option est déjà utilisée, la nouvelle option sera prioritaire.

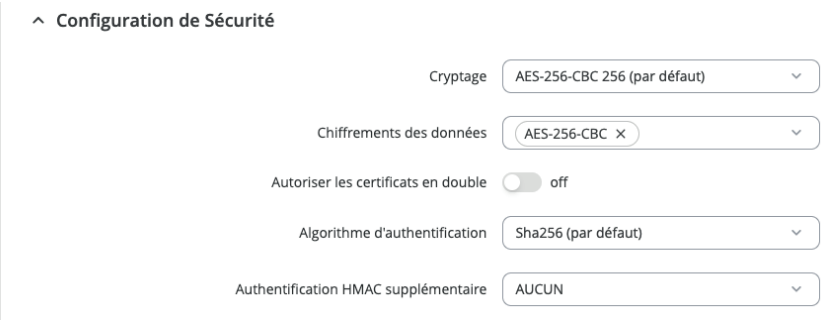
Serveur : Configuration de Réseau



TLS / TLS/Mot de passe / Mot de passe : Adresse IP du réseau virtuel	ip4 Par défaut : aucun	Adresse IP utilisée pour le réseau virtuel.
TLS / TLS/Mot de passe / Mot de passe : Masque de sous-réseau du réseau virtuel	masque de sous-réseau Par défaut : aucun	Masque de sous-réseau utilisé pour le réseau virtuel.
Clé statique : adresse IP du point de terminaison du tunnel local	adresse IP Par défaut : aucun	Adresse IP de l'interface réseau locale virtuelle.
Clé statique : adresse IP du point de terminaison du tunnel distant	adresse IP Par défaut : aucun	Adresse IP de l'interface réseau distante virtuelle.
TLS / TLS/Mot de passe / Mot de passe : Attribuer une adresse IP de début	IP Par défaut : aucun	Attribuer des adresses IP à partir d'un pool de sous-réseaux à allouer dynamiquement aux clients se connectant.
TLS / TLS/Mot de passe / Mot de passe : Attribuer l'adresse IP finale	IP Par défaut : aucun	Attribuer des adresses IP se terminant par un ensemble de sous-réseaux à allouer dynamiquement aux clients se connectant.
TLS / TLS/Mot de passe / Mot de passe : Adresse IPv6 du réseau virtuel	ip6 Par défaut : aucun	Adresse IPv6 utilisée pour le réseau virtuel.
TLS / TLS/Mot de passe / Mot de passe : Attribuer une adresse IPv6	ip6 Par défaut : aucun	Spécifiez un pool d'adresses IPv6 pour l'attribution dynamique aux clients.
Clé statique : Point de terminaison du tunnel local IPv6	Adresse IP Par défaut : aucun	Adresse IPv6 de l'interface réseau local virtuel.

Clé statique : Point de terminaison du tunnel distant IPv6	Adresse IP Par défaut : aucun	Adresse IPv6 de l'interface réseau distante virtuelle.
TAP (ponté) : Pont	Interface réseau local | aucune Par défaut : réseau local	Attribuer une interface TAP à un pont.
TAP (ponté) : Adresse IP de la passerelle	IPv4 Par défaut : aucun	Adresse IP et masque de sous-réseau de l'interface de pont sur le serveur VPN. Cette adresse est attribuée à l'interface TAP et annoncée aux clients VPN comme leur passerelle.
LZO	Aucun | Adaptatif | Oui | Non Par défaut : aucun	Utilisez la compression LZO rapide. Grâce à la compression LZO, votre connexion VPN générera moins de trafic réseau.
Client à client	Off | On ; Par défaut : Off	Autoriser le trafic client à client.
Tentatives de réglage	Entier | infini Par défaut : infini	Essayez de résoudre le nom d'hôte du serveur pendant X secondes avant d'abandonner.
Maintenir actif	Deux entiers séparés par un espace Par défaut : aucun	Essayez de maintenir la connexion active. Deux valeurs sont requises : ping_interval et ping_restart, par exemple : 10 120.

Serveur : Configuration de Sécurité



TLS/Mot de passe / Mot de passe : Noms d'utilisateur et mots de passe	-(bouton interactif)	Fichier contenant les identifiants et mots de passe permettant au serveur d'authentifier les clients. Chaque paire identifiant/mot de passe doit figurer sur une seule ligne et être séparée par un espace.
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 de chiffrement de paquets (chiffrement).

Chiffrements de données	dépend de l'authentification Par défaut : AES-256-CBC	Sélectionnez les algorithmes de chiffrement autorisés dans la liste ; ajoutez une valeur personnalisée si nécessaire.
TLS / TLS/Mot de passe / Mot de passe : Autoriser les certificats en double	Off | On ; Par défaut : Off	Tous les clients peuvent avoir les mêmes certificats.
Algorithme d'authentification	Aucun | MD5 | SHA1 | SHA256 | SHA384 | SHA512 Par défaut : SHA1	Type d'algorithme d'authentification HMAC.
TLS / TLS/Mot de passe / Mot de passe : Authentification HMAC supplémentaire	Aucune | Authentification uniquement (tls-auth) | Authentification uniquement (tls-auth) ; Par défaut : Aucune	Ajoutez une couche supplémentaire d'authentification HMAC au-dessus du canal de contrôle TLS pour vous protéger contre les attaques par déni de service (DoS).
TLS / TLS/Mot de passe / Mot de passe : direction de la clé HMAC	0 | 1 Par défaut : 1	La valeur de direction de la clé d'authentification HMAC est arbitraire et doit être opposée entre les parties communicantes (ou être totalement omise).

Serveur : Configuration de Certificats



TLS / TLS/Mot de passe / Mot de passe : Utiliser le format PKCS #12	Off | On ; Par défaut : Off	Utilisez le format de fichier d'archive PKCS #12 pour regrouper tous les membres d'une chaîne de confiance.
TLS / TLS/Mot de passe / Mot de passe : chaîne de certificats PKCS #12	-(bouton interactif)	Téléverse un fichier de chaîne de certificats PKCS #12.
TLS / TLS/Mot de passe / Mot de passe : Fichiers de certificat de l'appareil	Off | On ; Par défaut : Off	Choisissez cette option si vous souhaitez sélectionner des fichiers de certificat depuis l'appareil.
TLS / TLS/Mot de passe / Mot de passe : Stocker la clé du serveur dans le TPM	Off | On ; Par défaut : On	Si cette option est activée, la clé sera stockée dans la mémoire sécurisée du TPM2 si de l'espace est disponible. Remarque : cette option est uniquement disponible sur les appareils compatibles avec le TPM.
TLS / TLS/Mot de passe / Mot de passe : Autorité de certification	Fichier .ca Par défaut : aucun	Le certificat numérique vérifie la propriété d'une clé publique par le sujet nommé du certificat.
TLS / TLS/Mot de passe / Mot de passe : Certificat du serveur	Fichier .crt Par défaut : aucun	Les serveurs de certificats valident ou certifient les clés dans le cadre d'une infrastructure à clés publiques.

TLS / TLS/Mot de passe / Mot de passe : Clé du serveur	Fichier .key Par défaut : aucun	Il a été généré dans le même but que le certificat du serveur.
TLS / TLS/Mot de passe / Mot de passe : Paramètres Diffie-Hellman	Fichier .pem Par défaut : aucun	L'échange de clés Diffie-Hellman est une méthode spécifique d'échange de clés cryptographiques.
TLS / TLS/Mot de passe / Mot de passe : fichier CRL (facultatif)	Fichier .pem | Fichier .crl Par défaut : aucun	Révoquer un certificat signifie invalider un certificat précédemment signé afin qu'il ne puisse plus être utilisé à des fins d'authentification. Téléversez un fichier de révocation au format .pem.
TLS / TLS/Mot de passe / Mot de passe : phrase secrète PKCS #12	Chaîne de caractères Par défaut : aucun	Phrase secrète pour déchiffrer les certificats PKCS #12.
TLS / TLS/Mot de passe / Mot de passe : Mot de passe de déchiffrement de la clé privée (facultatif)	Chaîne de caractères Par défaut : aucun	Déchiffrer la clé privée avec le mot de passe (facultatif).
Clé statique : Clé pré-partagée statique	-(bouton interactif)	Une clé pré-partagée (PSK) est un secret partagé qui a été préalablement échangé entre deux parties via un canal sécurisé avant d'être utilisé.

Notes complémentaires :

- Certains champs de configuration ne sont disponibles que lorsque certains autres paramètres sont sélectionnés.

Le nom des paramètres est suivi d'un préfixe qui spécifie le type d'authentification sous lequel ils sont visibles.

Différents codes couleur sont utilisés pour les différents préfixes :

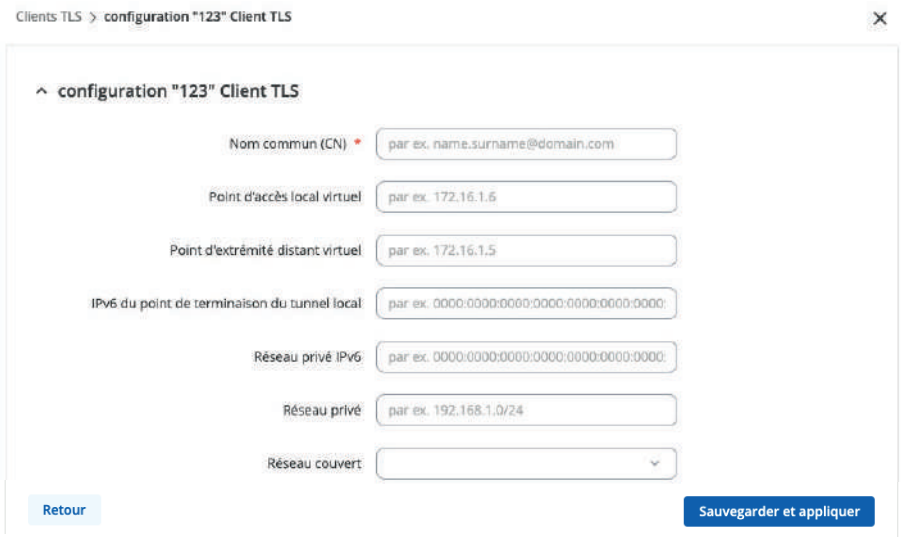
- Rouge pour l'authentification : TLS
- Vert pour l'authentification : TLS/Mot de passe
- Violet pour l'authentification : clé statique
- Bleu pour l'authentification : Mot de passe
- Brun pour la configuration OpenVPN à partir du fichier

- 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.

Clients TLS

Les clients TLS permettent de différencier les clients grâce à leurs noms communs (CN), qui figurent dans le fichier de certificat client. Ils peuvent être utilisés pour attribuer des adresses VPN spécifiques aux clients et les lier à leurs adresses LAN, permettant ainsi au serveur de savoir quel client possède quelle adresse IP LAN.

La section « Clients TLS » se trouve dans la fenêtre de configuration du serveur OpenVPN, à condition que ce dernier utilise l'authentification TLS ou TLS/mot de passe. Pour créer un client TLS, saisissez son nom dans le champ de texte situé sous l'onglet « Clients TLS », puis cliquez sur le bouton « Ajouter ». Consultez la figure et le tableau ci-dessous pour plus d'informations sur les champs de configuration des clients TLS.

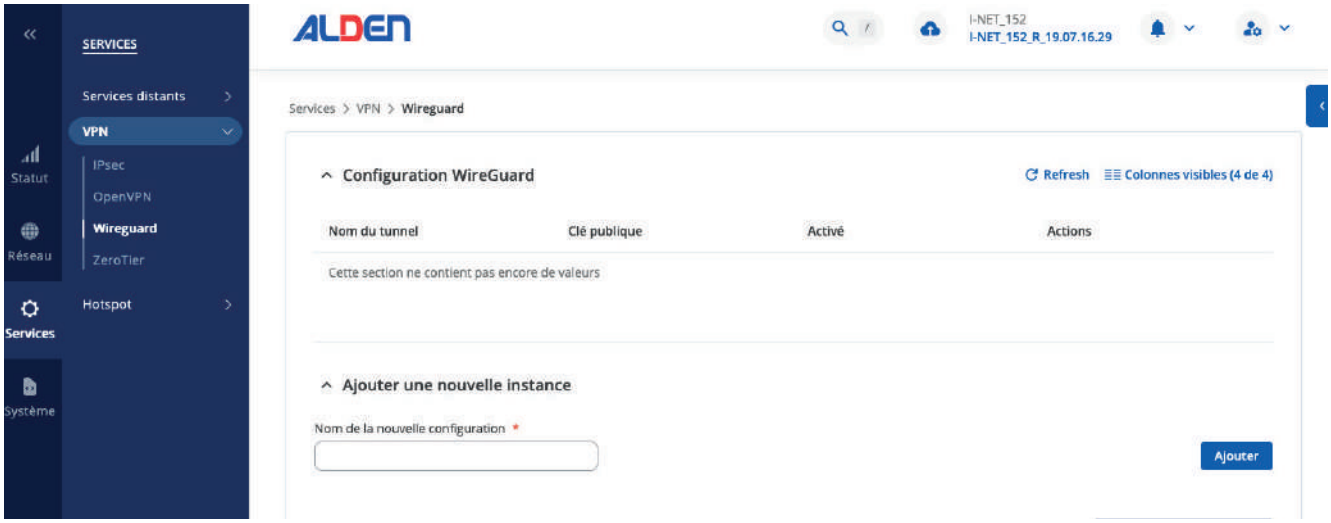


Nom commun (CN)	Chaîne de caractères Par défaut : aucun	Champ CN du certificat client (par exemple, nom.nom@domaine.com).
Point d'accès local virtuel	Adresse IP Par défaut : aucun	Adresse locale du client dans le réseau virtuel.
Point d'extrémité distant virtuel	Adresse IP Par défaut : aucun	Adresse distante du client dans le réseau virtuel.
IPv6 du point de terminaison du tunnel local	Adresse IP Par défaut : aucun	Adresse IPv6 de l'interface réseau local virtuel.
Réseau privé IPv6	Adresse IP Par défaut : aucun	Adresse IPv6 du réseau privé (LAN) du client.
Réseau privé	Adresse IP Par défaut : aucun	Adresse IP du réseau privé (LAN) du client.
Réseau couvert	Réseau() Par défaut : aucun	Sélectionne les réseaux qui doivent être accessibles à ce client.

3.2.3 Menu SERVICES > VPN > WireGuard

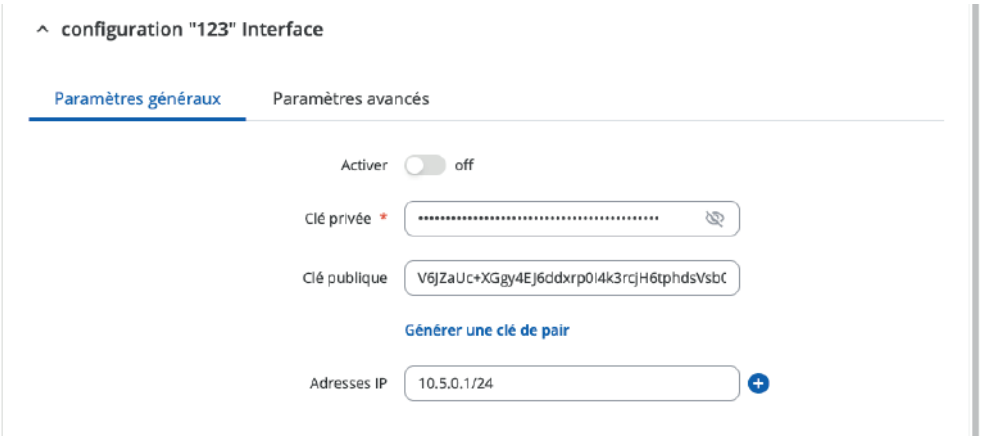
WireGuard est un VPN simple, rapide, léger et moderne qui utilise un chiffrement sécurisé et fiable. Il vise à être plus performant qu'OpenVPN. Conçu comme un VPN polyvalent, adapté à de nombreuses situations, WireGuard, bien qu'encore en développement, peut d'ores et déjà être considéré comme la solution VPN la plus sécurisée, la plus simple d'utilisation et la plus intuitive.

WireGuard fonctionne en ajoutant une interface faisant office de tunnel. Pour en créer une, saisissez son nom et cliquez sur le bouton Ajouter. Une nouvelle instance WireGuard sera alors créée et une fenêtre de configuration s'ouvrira.



WireGuard : Paramètres généraux

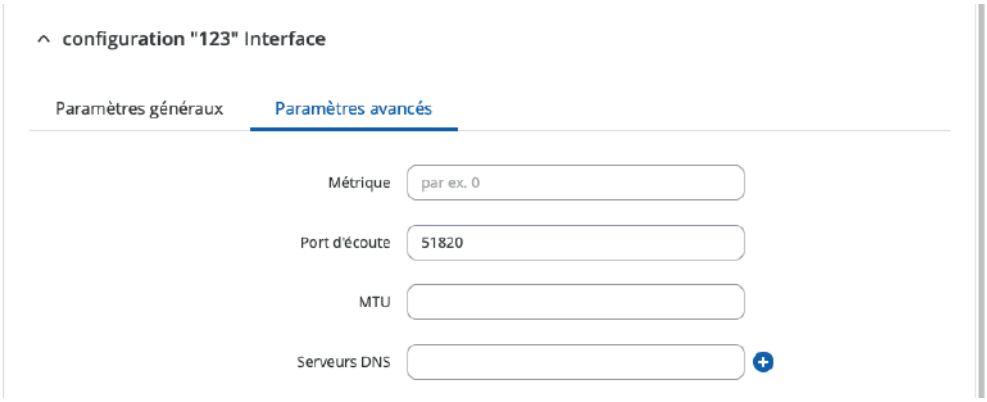
Cette section contient les paramètres généraux de l'instance WireGuard créée. Vous y trouverez ses clés publique et privée, que vous pourrez générer, ainsi que les adresses de port et IP pour la communication.



Activer	Off | On ; Par défaut : Off	Active ou désactive l'instance WireGuard.
Clé privée	Chaîne de caractères ; Par défaut : -	Clé privée utilisée pour l'authentification.
Clé publique	Chaîne de caractères ; Par défaut : -	Clé publique utilisée pour l'authentification.
Générer une clé de pair	-(bouton interactif)	Cliquez pour générer la clé publique et la clé privée.
Adresses IP	Adresse IP Par défaut : 10.5.0.1/24	Une seule adresse IP ou une liste d'adresses IP associées à des clés publiques dans cette instance.

WireGuard : Paramètres avancés

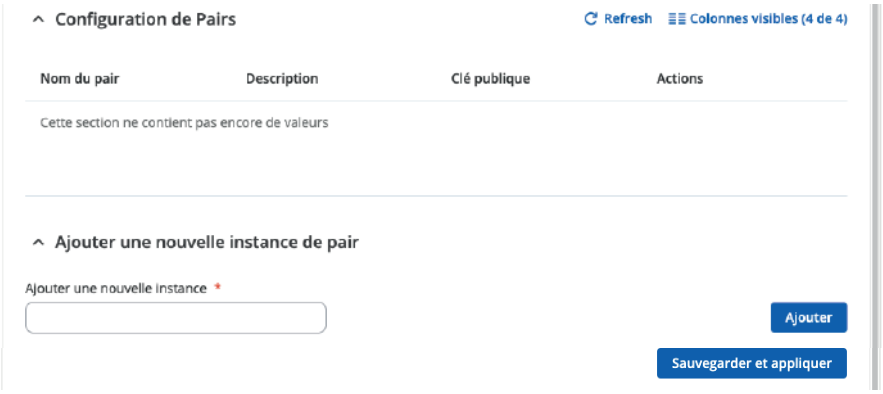
La section Paramètres avancés contient la configuration métrique et MTU pour cette interface WireGuard.



Métrique	entier positif Par défaut : aucun	Spécifiez (facultatif) la métrique pour cette interface de tunnel. Plus le nombre est bas, plus la priorité est élevée.
Port d'écoute	entier [1..65535] Par défaut : 51820	Obligatoire. Port UDP utilisé pour les paquets entrants et sortants.
MTU	Entier [68..9200] Par défaut : aucun	Unité de transmission maximale de l'interface tunnel. Plage : [68 à 9200]. Si elle n'est pas spécifiée, la MTU est automatiquement déterminée par la valeur MTU de l'interface physique.
Serveurs DNS	Adresse IP Par défaut : aucun	Serveur(s) DNS pour cette interface Wireguard.

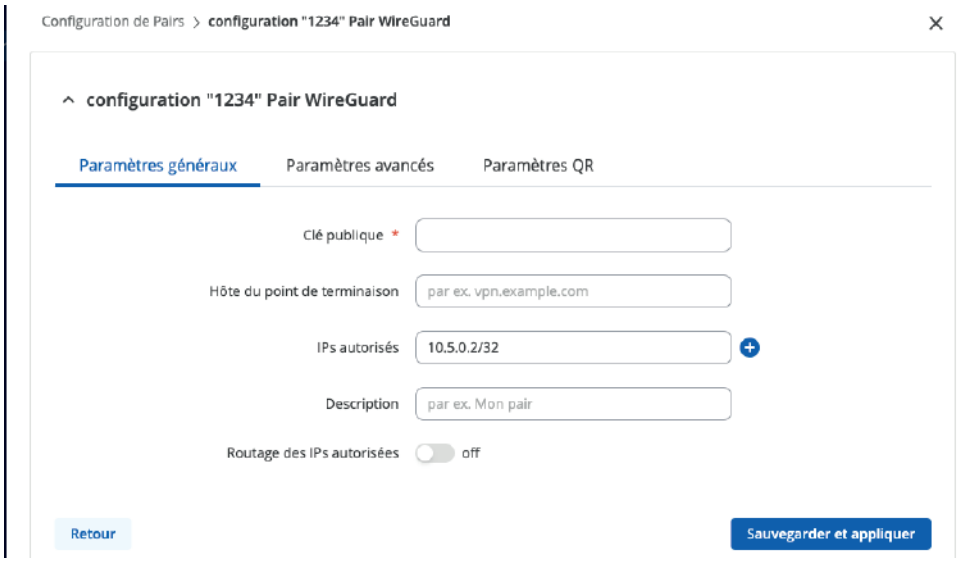
WireGuard : Pairs

La section « Pairs » permet de créer et de configurer tous les pairs de cette interface. Pour en créer un, saisissez son nom et cliquez sur le bouton « Ajouter » .



WireGuard : Paramètres généraux

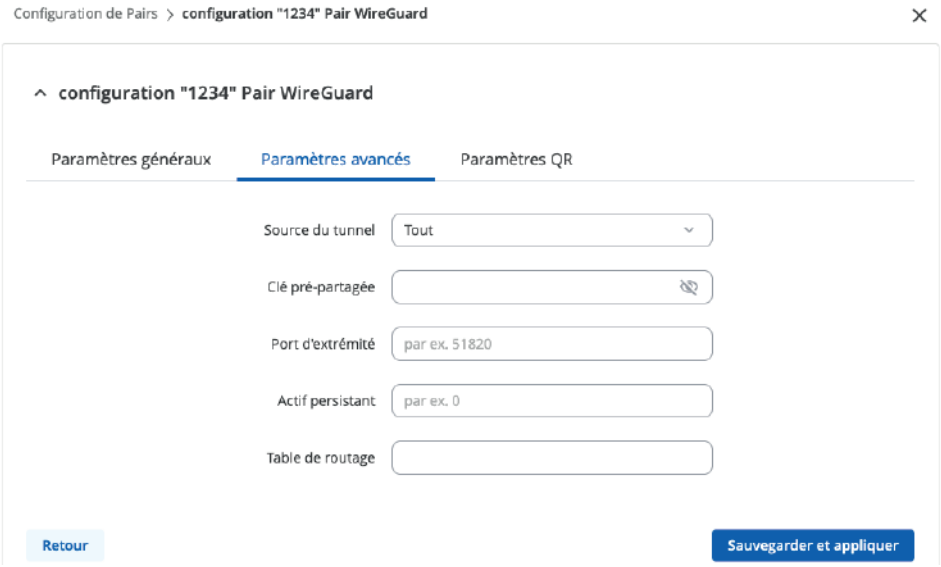
Dans la section Général de l'instance Peer, vous pouvez configurer les informations de base concernant le point de terminaison pour autoriser les communications.



Clé publique	Chaîne de caractères Par défaut : aucun	Clé publique du pair encodée en Base64.
Hôte de point de terminaison	Nom de domaine | adresse IP Par défaut : aucun	Hôte du pair. Les noms sont résolus avant l'activation de l'interface.
IPs autorisés	Adresse IP Par défaut : 10.5.0.2/32	Adresses IP et préfixes que ce pair est autorisé à utiliser à l'intérieur du tunnel. Il s'agit généralement des adresses IP du tunnel du pair et des réseaux que ce dernier achemine à travers ce tunnel.
Description	Chaîne de caractères Par défaut : aucun	Description du pair.
Routage des IPs autorisées	Off | On ; Par défaut : Off	Créer des routes pour les adresses IP autorisées pour ce pair.

WireGuard : Paramètres avancés

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

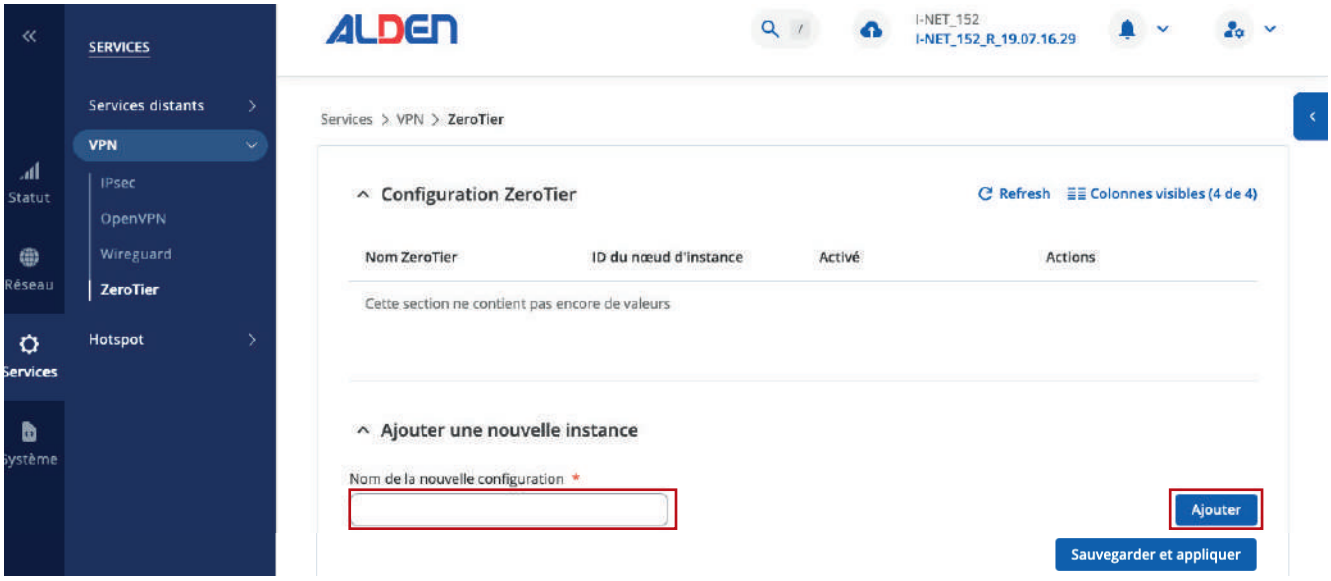


Source du tunnel	Tout | LAN | WAN | Mobile Par défaut : Tout	Interface à laquelle lier cette instance.
Mode source tunnel	Préférer | Persister Par défaut : Préférer	Choisissez si vous souhaitez conserver ou privilégier la connexion sur l'interface sélectionnée.
Clé pré-partagée	chaîne de caractères Par défaut : aucun	Clé pré-partagée encodée en Base64. Ajoute une couche supplémentaire de cryptographie symétrique pour une résistance post-quantique.
Port d'extrémité	entier [1..65535] Par défaut : aucun	Port de pair.
Actif persistant	entier [0..65535] Par défaut : aucun	Intervalle en secondes entre les messages de maintien de connexion. Par défaut : 0 (désactivé). Valeur recommandée si l'appareil se trouve derrière un NAT : 25. Plage : [0 à 65 535].
Table de routage	chaîne de caractères Par défaut : aucun	Définit la table de routage à utiliser pour ces routes homologues ; cette configuration n'est généralement pas nécessaire.

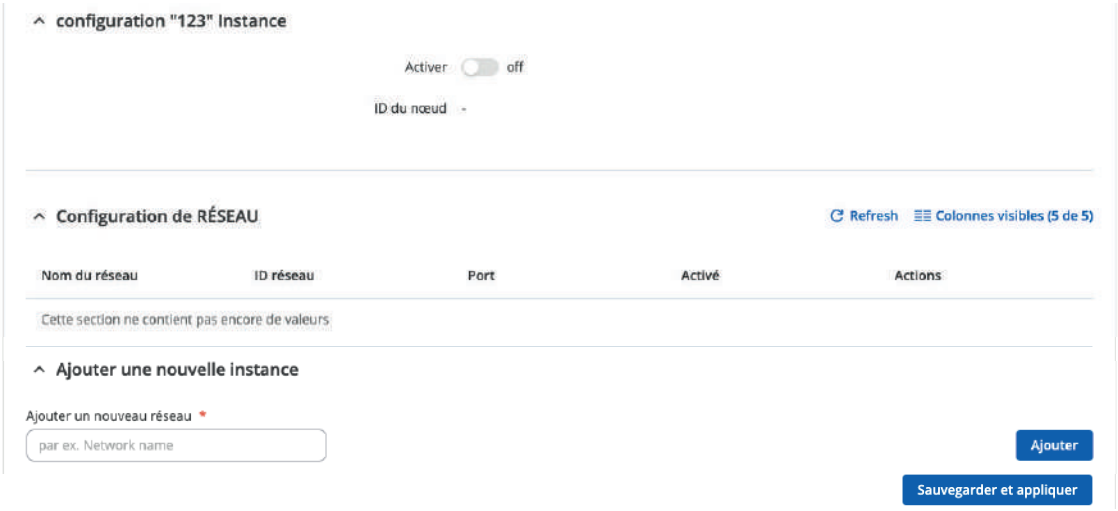
3.2.4 Menu SERVICES > VPN > ZeroTier

ZeroTier est un logiciel libre permettant d'établir une connexion VPN pair à pair (P2PVPN) entre différents appareils fonctionnant sous divers systèmes d'exploitation. Il offre également des fonctionnalités de gestion de réseau telles que le routage et la création de règles de pare-feu.

Pour créer une nouvelle instance ZeroTier, consultez la section Ajouter une nouvelle configuration ZeroTier ; saisissez un nom personnalisé et cliquez sur le bouton « Ajouter » :

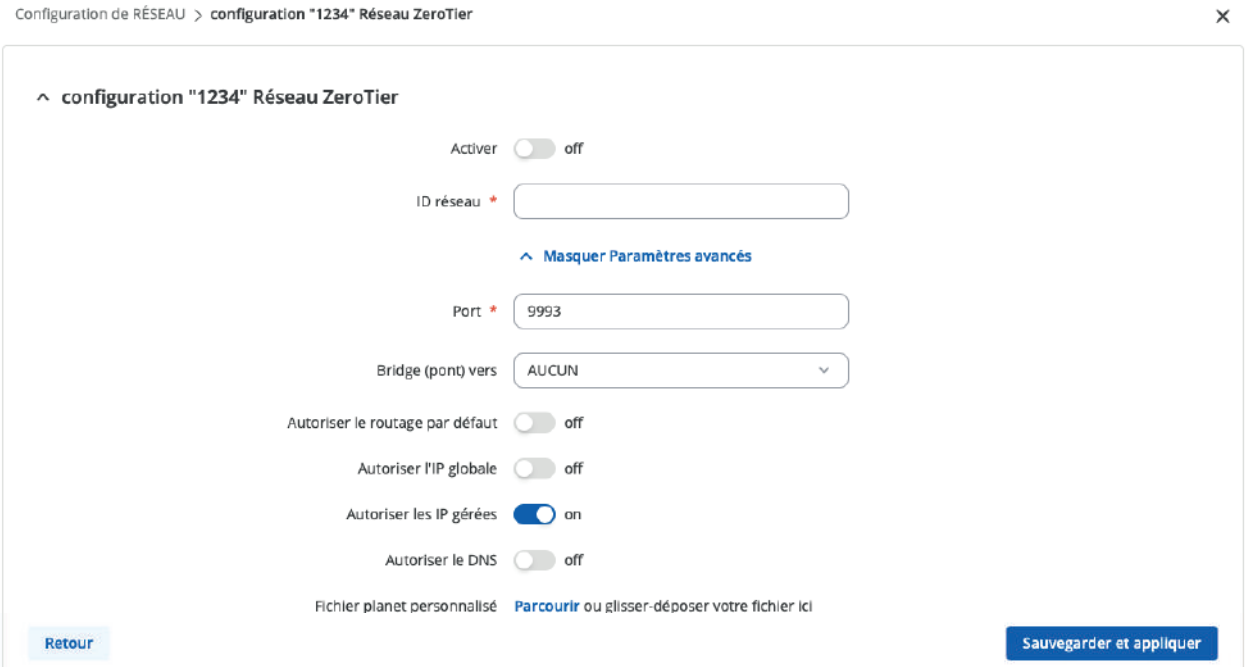


Vous devriez être redirigé vers la page de configuration de l'instance ZeroTier nouvellement ajoutée, qui devrait ressembler à ceci :



Activé	Off | On ; Par défaut : Off	Active ou désactive l'instance ZeroTier.

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



Activé	Off | On ; Par défaut : Off	Active ou désactive l'instance ZeroTier.
ID réseau	Chaîne hexadécimale Par défaut : aucun	Identifiant réseau ZeroTier. Connectez-vous à votre compte ZeroTier pour trouver l'identifiant réseau ZeroTier, qui devrait être une chaîne de caractères hexadécimaux.
Port	entier [0..65535] Par défaut : 9993	Port réseau ZeroTier.
Bridge (pont) vers	Aucun | LAN Par défaut : aucun	Spécifiez l'interface à laquelle cette instance ZeroTier doit être connectée.
Autoriser le routage par défaut	Off | On ; Par défaut : Off	Permet à ZeroTier de remplacer la route par défaut du système.
Autoriser l'IP globale	Off | On ; Par défaut : Off	Permet aux adresses IP et aux routes gérées par ZeroTier de chevaucher l'espace IP public.

Autoriser les IP gérées	Off | On ; Par défaut : On	Attribue des adresses IP et des routes gérées par ZeroTier.
Autoriser le DNS	Off | On ; Par défaut : Off	Applique les serveurs DNS configurés au niveau du contrôleur réseau.
Fichier planet personnalisé	-(bouton interactif)	Le fichier de planète personnalisé contient des racines définies par l'utilisateur, permettant l'utilisation de serveurs racines privés.

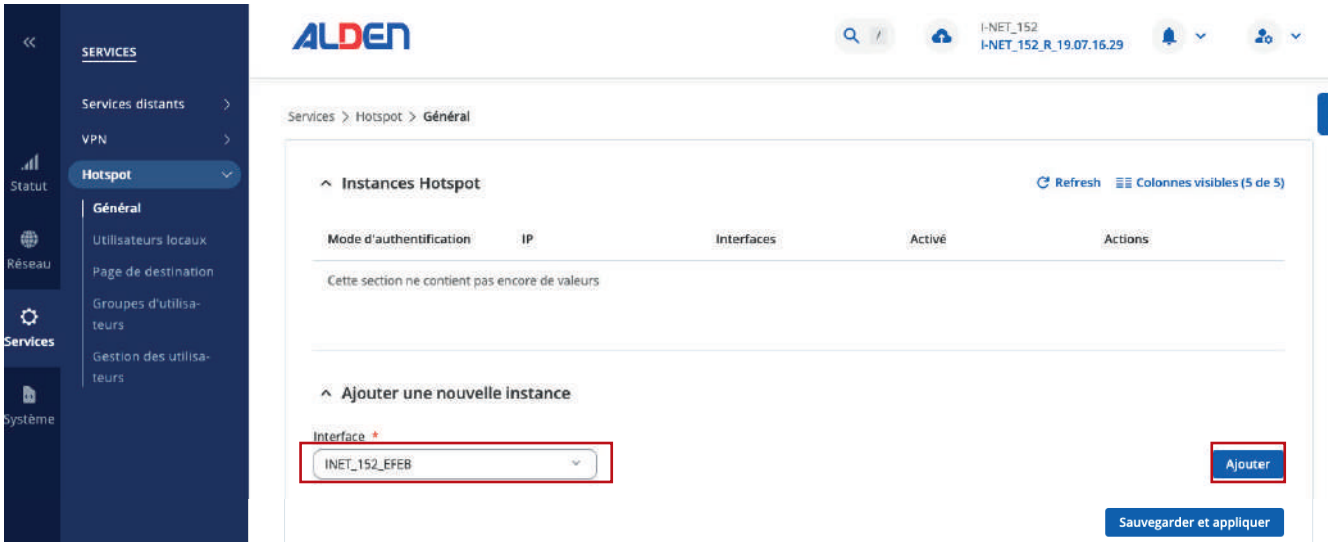
3.3 Menu SERVICES >HOTSPOT

Un point d'accès (Hotspot) est un service qui assure l'authentification, l'autorisation et la comptabilisation des connexions au réseau.

3.3.1 Menu SERVICES >HOTSPOT > Général

La section « Instances de point d'accès » affiche les principaux paramètres de votre point d'accès. Par défaut, aucune instance de point d'accès n'est installée sur l'appareil. Pour créer une nouvelle instance et commencer la configuration :

- Sélectionnez une « Interface » ;
- Cliquez sur le bouton « Ajouter » ;

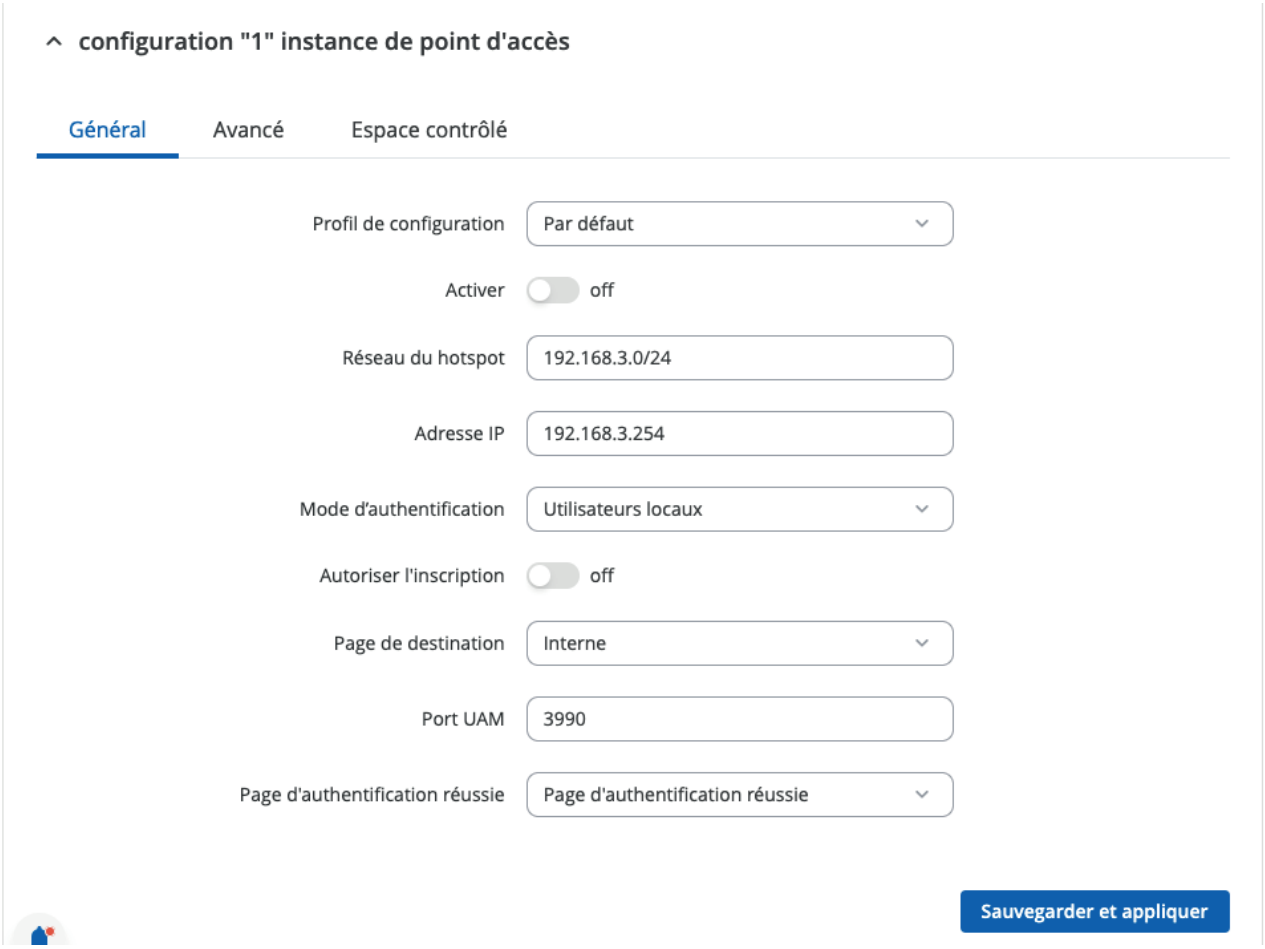


Une nouvelle fenêtre de configuration du point d'accès apparaîtra ensuite.

HOTSPOT > Configuration point d'accès

La fenêtre Point d'accès est l'endroit où se trouve 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 disponibles dans les Paramètres généraux.

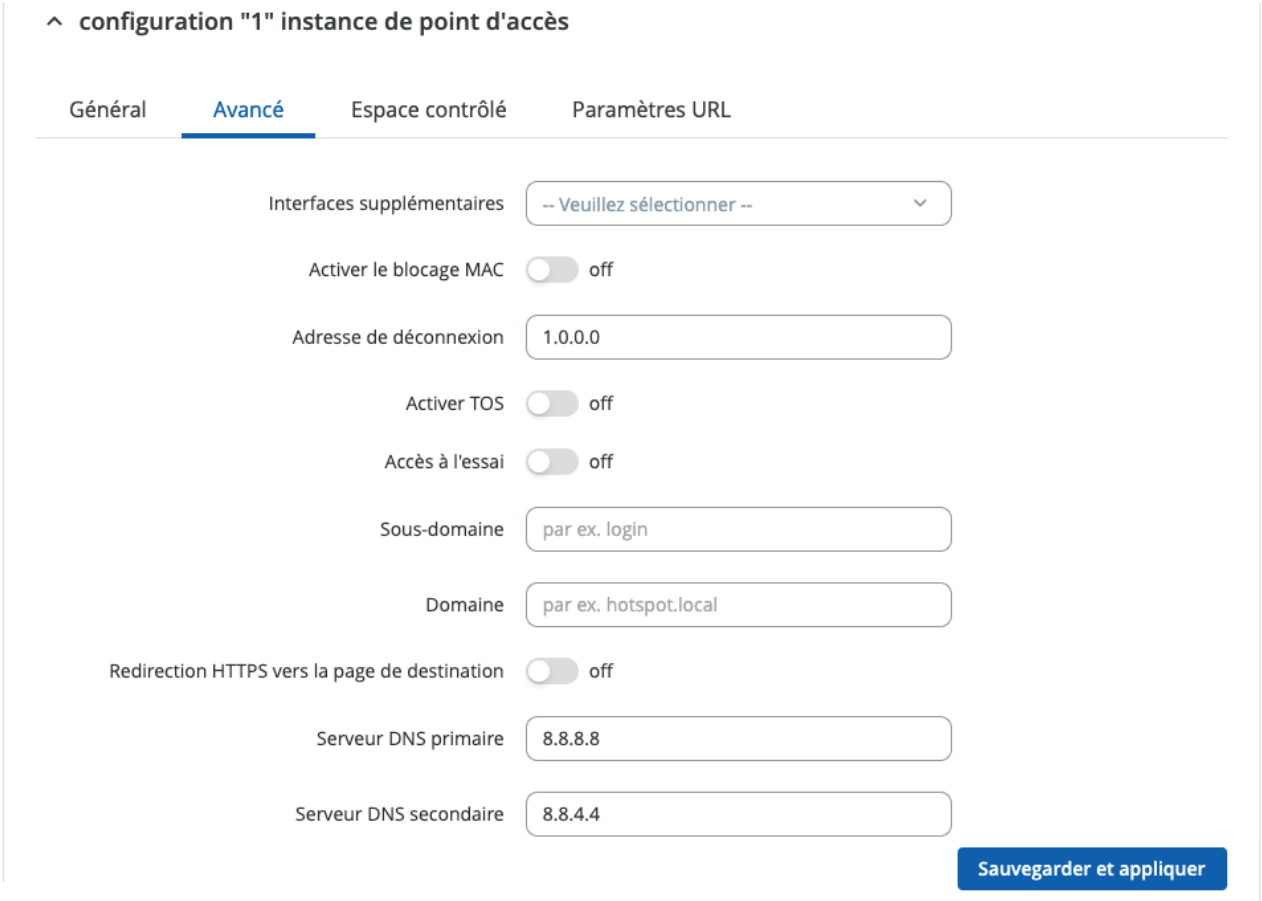
Général



Profil de configuration	Cloud4wi | Par défaut | Hotspotsystems | Portail violet 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	adresse IP/masque de sous-réseau Par défaut : 192.168.2.0/24	Adresse IP et sous-réseau du réseau Hotspot. Le masque de sous-réseau doit être compris entre 16 et 30.
Adresse IP	Adresse IP Par défaut : 192.168.2.254	Définit l'adresse IP de votre routeur Hotspot sur le réseau.
Mode d'authentification	Utilisateurs locaux | Radius | Authentification MAC | Authentification unique | Code OTP par SMS ; Par défaut : Utilisateurs locaux	Le mode d'authentification définit comment les utilisateurs se connecteront au point d'accès.
Utilisateurs locaux : Autoriser l'inscription	Off | On ; Par défaut : Off	Permet aux utilisateurs de s'inscrire au point d'accès via la page de destination.

Utilisateurs locaux : Temps d'expiration	Entier Par défaut : 0	Durée de validité des identifiants utilisateur. S'applique aux utilisateurs qui se sont inscrits via la page de destination.
Utilisateurs locaux : Groupe d'utilisateurs	Groupe d'utilisateurs ; Par défaut : par défaut	Le groupe d'utilisateurs auquel les utilisateurs se sont inscrits via la page de destination doit être affecté.
Radius / SMS OTP : Activer l'authentification MAC	Off | On ; Par défaut : Off	Activer l'authentification par adresse MAC.
Authentification MAC : mot de passe requis	Éteint | allumé Par défaut : éteint	Active l'exigence d'un mot de passe pour l'authentification MAC.
Authentification MAC : mot de passe d'authentification MAC	Chaîne de caractères Par défaut : aucune	Mot de passe pour l'authentification MAC.
Authentification MAC / Authentification unique / Code OTP par SMS : Groupe d'utilisateurs	Sélectionner Par défaut : par défaut	Spécifie le groupe d'utilisateurs créés dynamiquement.
SMS OTP : Autoriser les doublons de mots de passe	Off | On ; Par défaut : Off	Permet à plusieurs utilisateurs de se connecter avec le même mot de passe.
Code OTP par SMS : Durée de validité	Entier non signé Par défaut : 0	Durée d'expiration de l'utilisateur en secondes (0 signifie illimitée).
Page d'accueil	Interne | Externe Par défaut : Interne	Emplacement de la page d'accueil.
Port UAM	entier Par défaut : 3990	Port à lier pour l'authentification des clients.
Encodage du mot de passe	désactivé | activé Par défaut : aucun	Encodage du mot de passe avec défi.
Adresse de la page de destination	URL Par défaut : aucun	Adresse de la page de destination externe (http://www.example.com).
Secret UAM	Chaîne de caractères Par défaut : aucun	Secret partagé entre uamserver et hotspot.
Page d'authentification réussie	Page de succès | URL d'origine | Personnalisée Par défaut : Page de succès	Lieu de retour après authentification réussie.
URL personnalisée	URL Par défaut : aucun	L'adresse doit contenir le protocole (http://www.example.com).

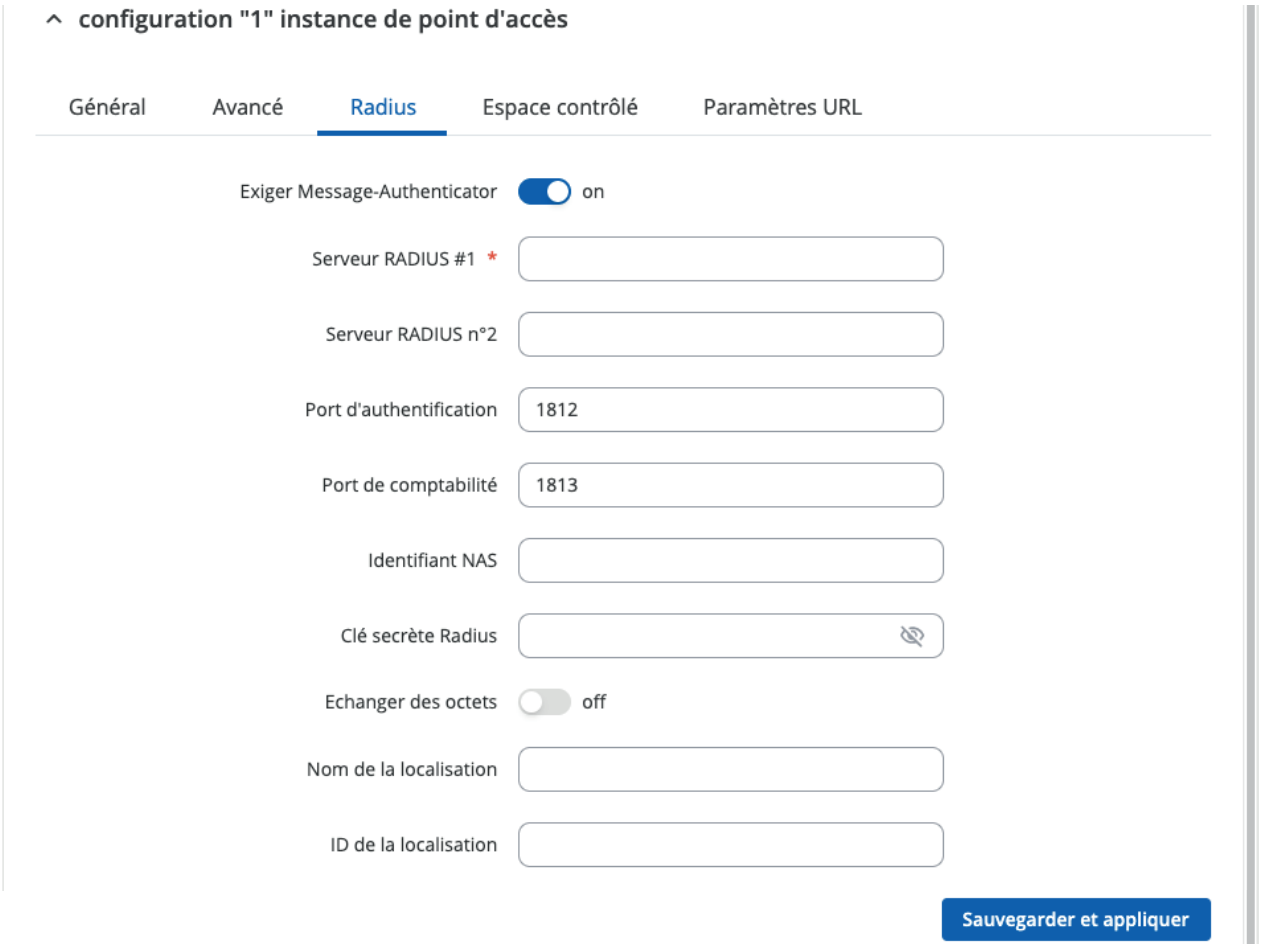
Avancé



Interfaces supplémentaires	Interfaces disponibles ; par défaut : aucune	Choisissez également les interfaces que vous souhaitez connecter à cette instance de point d'accès.
Activer le blocage MAC	Off | On ; Par défaut : Off	Bloque l'accès aux adresses MAC ayant atteint un certain nombre de tentatives de connexion infructueuses.
Adresse de déconnexion	Adresse IP ; par défaut : 1.0.0.0	Adresse IP permettant de déconnecter instantanément un client y accédant.
Protocole	HTTP | HTTPS ; par défaut : HTTP	Protocole à utiliser pour la page de destination.
Activer les conditions d'utilisation	Off | On ; Par défaut : Off	Active l'obligation d'accepter les conditions d'utilisation. L'appareil client ne pourra accéder à Internet qu'après avoir accepté ces conditions.
Accès d'essai	Off | On ; Par défaut : Off	Permet un accès Internet à titre d'essai pour un groupe spécifique.
Groupe	Groupe d'utilisateurs ; par défaut : par défaut	Spécifie le groupe d'utilisateurs à l'essai.
Sous-domaine	Chaîne de caractères ; valeur par défaut : aucune	Combiné avec un domaine pour créer un alias DNS pour l'adresse IP du point d'accès.
Domaine	Chaîne de caractères ; valeur par défaut : aucune	Combiné avec un sous-domaine pour créer un alias DNS pour l'adresse IP du point d'accès.
Redirection HTTPS vers la page de destination	Off | On ; Par défaut : Off	Rediriger les requêtes HTTPS initiales de pré-page d'accueil vers la page d'accueil du point d'accès.
Fichiers de certificat de l'appareil	Off | On ; Par défaut : Off	Indique 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 → Certificats .
Fichier de clé SSL	Fichier clé Par défaut : aucun	Télécharger/sélectionner la clé SSL.

Fichier de certificat SSL	Fichier de certificat Par défaut : aucun	Télécharger/sélectionner le certificat SSL.
Serveur DNS primaire	Adresse IP Par défaut : 8.8.8.8	Serveurs DNS supplémentaires qui seront utilisés par le point d'accès.
Serveur DNS secondaire	Adresse IP Par défaut : 8.8.4.4	Serveurs DNS supplémentaires qui seront utilisés par le point d'accès.

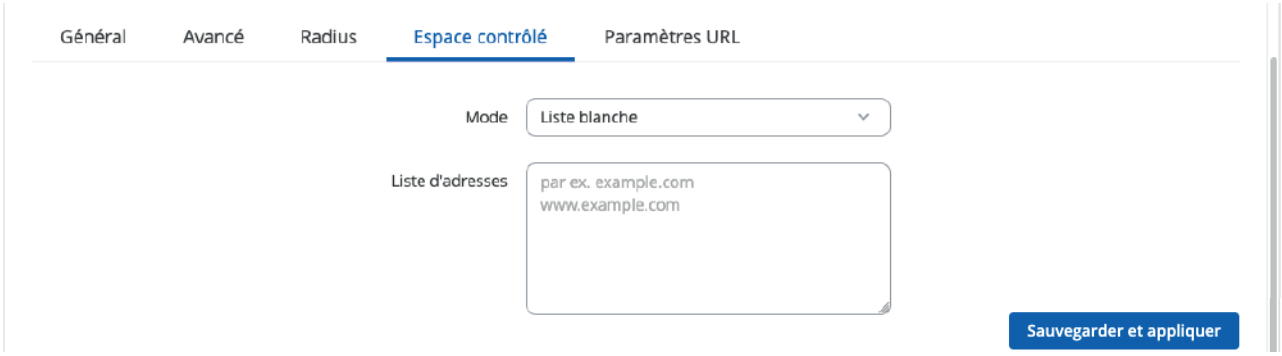
Radius



Exiger l'authentification par message	Off | On ; Par défaut : On	Exiger et valider l'attribut RADIUS Message-Authenticator dans les réponses Access-Request.
Serveur RADIUS n° 1	adresse IP Par défaut : aucun	L'adresse IP du serveur RADIUS n° 1 qui doit être utilisé pour authentifier vos clients sans fil.
Serveur RADIUS n° 2	adresse IP Par défaut : aucun	L'adresse IP du serveur RADIUS n° 2 qui doit être utilisé pour authentifier vos clients sans fil.
Port d'authentification	entier [0..65535] Par défaut : 1812	Port d'authentification du serveur RADIUS.
Port comptable	entier [0..65535] ; Par défaut : 1813	Port de comptabilité du serveur RADIUS.
Identifiant NAS	chaîne de caractères Par défaut : aucun	NAS-Identifier est l'un des attributs RADIUS de base.
Clé secrète Radius	chaîne de caractères Par défaut : aucun	La clé secrète est un mot de passe utilisé pour l'authentification auprès du serveur RADIUS.
Échanger les octets	Off | On ; Par défaut : Off	Inverse la signification des octets d'entrée et de sortie en ce qui concerne les attributs RADIUS.
Nom de la localisation	Chaîne de caractères Par défaut : aucun	Nom personnalisé pour votre point d'accès.
ID de localisation	Chaîne de caractères Par défaut : aucun	Identifiant de localisation personnalisé pour votre point d'accès.

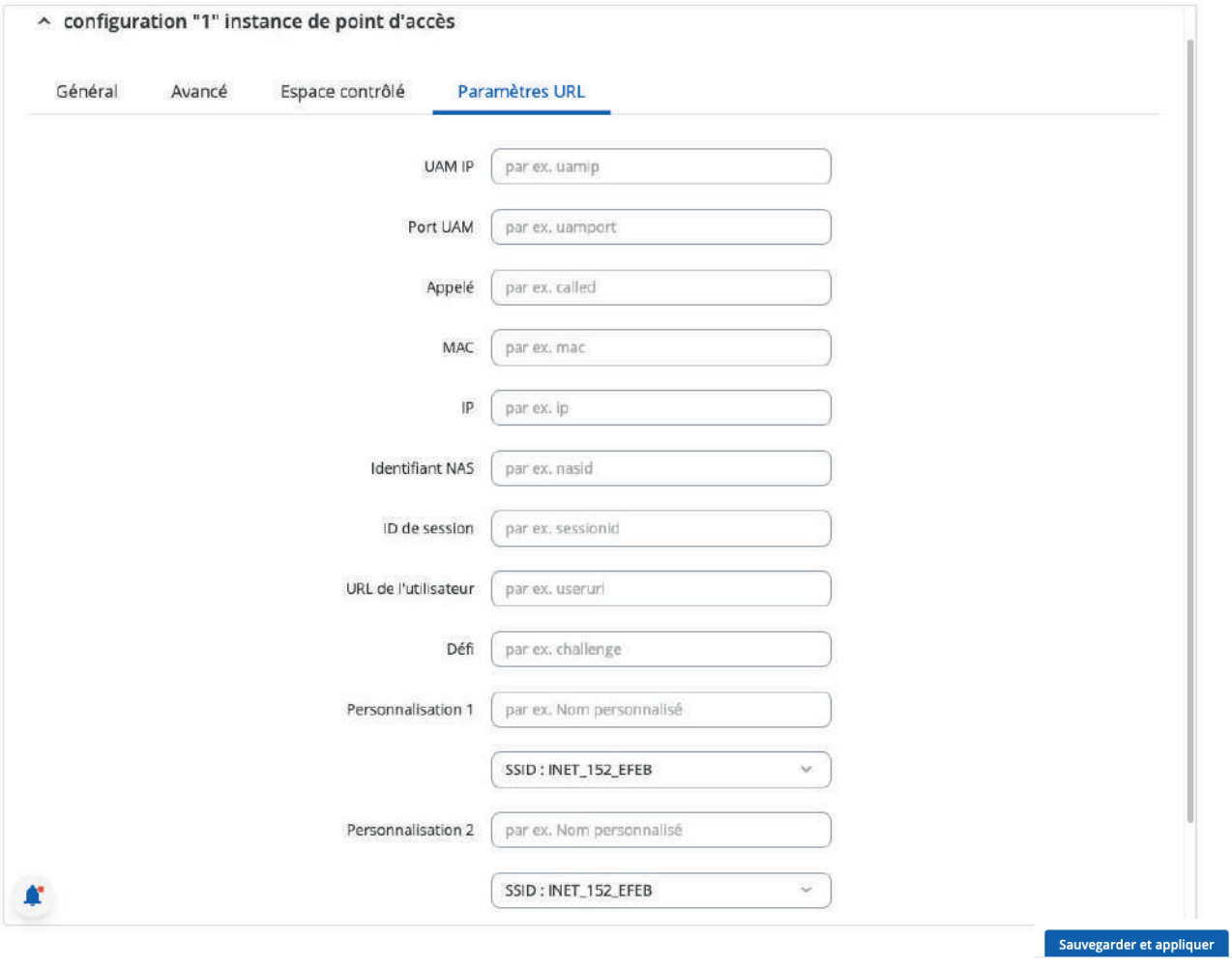
Espace controlé
Vous pouvez ajouter une liste d'adresses auxquelles les utilisateurs connectés au point d'accès pourront accéder sans authentification. Par défaut, cette liste est vide. Saisissez simplement les adresses dans le champ « Liste d'adresses ».

Le format de l'adresse est website.com (sans https://www).



Mode	Liste blanche | Liste noire Par défaut : Liste blanche	Sélectionnez le mode de blocage.
Liste d'adresses	Noms de domaine (un enregistrement par ligne) Par défaut : aucun	Liste des adresses auxquelles le client peut accéder sans authentification préalable. Une entrée par ligne. Voir l'espace réservé pour les formats acceptés. Certains domaines nécessitent la saisie des versions avec et sans « www » pour un blocage efficace.

Paramètres d'URL
La section des paramètres d'URL devient visible lorsque l'option « Page de destination externe » est sélectionnée dans la section « Paramètres généraux » .

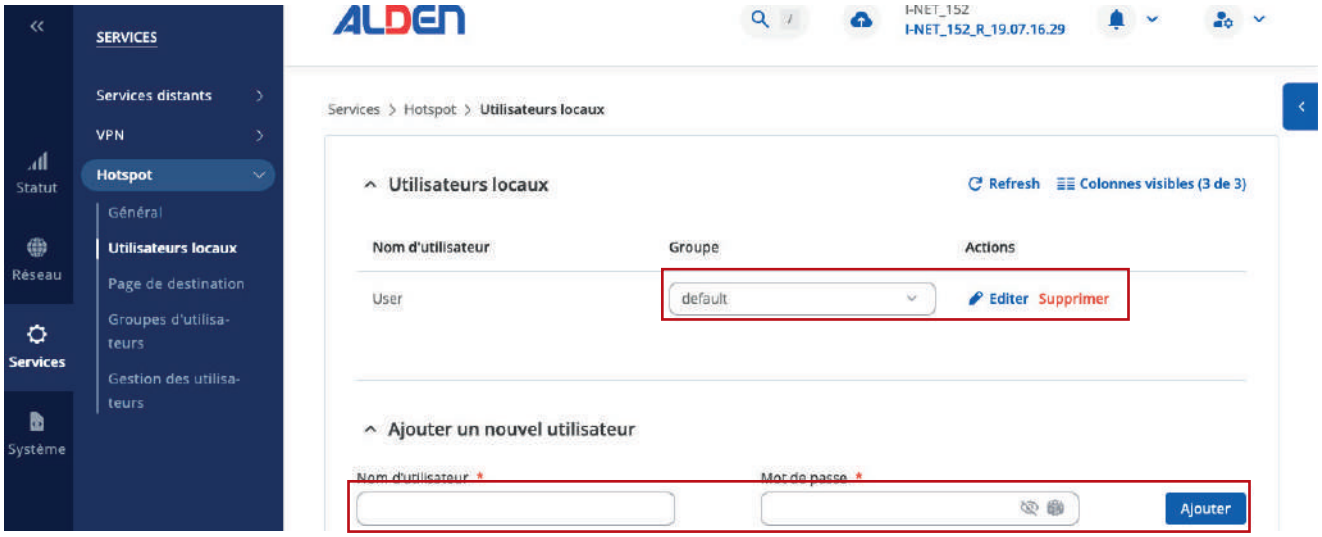


UAM IP	Chaîne de caractères Par défaut : aucun	Adresse IP de la passerelle du portail captif.
Port UAM	Chaîne de caractères Par défaut : aucun	Le port sur lequel le portail captif diffusera le contenu web.
Appelé	Chaîne de caractères Par défaut : aucun	L'adresse MAC de l'adresse IP de la passerelle du portail captif.
MAC	Chaîne de caractères Par défaut : aucun	L'adresse MAC du client tentant d'accéder à Internet.
IP	adresse IP par défaut : aucune	L'adresse IP du client qui tente d'accéder à Internet.
Identifiant NAS	Chaîne de caractères Par défaut : aucun	Identification du portail captif utilisé dans la requête RADIUS.
ID de session	Chaîne de caractères Par défaut : aucun	L'identifiant unique de la session.
URL de l'utilisateur	Chaîne de caractères Par défaut : aucun	L'URL à laquelle l'utilisateur a tenté d'accéder avant d'être redirigé vers les pages de l'URL du portail captif.
Défi	Chaîne de caractères Par défaut : aucun	Un défi à utiliser avec le mot de passe de l'utilisateur pour créer une phrase chiffrée permettant de se connecter.
Personnalisé 1	Chaîne de caractères Par défaut : aucun	Ajoutez un nom et une valeur personnalisés qui seront affichés dans les paramètres de l'URL.
-	SSID | Nom d'hôte | Version du firmware | --Personnalisé-- Par défaut : SSID	-
Personnalisé 2	Chaîne de caractères Par défaut : aucun	Ajoutez un nom et une valeur personnalisés qui seront affichés dans les paramètres de l'URL.
-	SSID | Nom d'hôte | Version du firmware | --Personnalisé-- Par défaut : SSID	-

3.3.2 Menu SERVICES >HOTSPOT >Utilisateurs locaux

La section « Utilisateurs locaux » permet de créer et de gérer les utilisateurs autorisés à se connecter au point d'accès. Les éléments qui composent la page « Utilisateurs locaux » sont expliqués dans la liste et la figure ci-dessous.

1. Saisir un nom d'utilisateur et un mot de passe, puis cliquer sur le bouton « Ajouter », crée 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'affecter cet utilisateur à un autre groupe.
4. Le bouton « Supprimer[X] » supprime un utilisateur.



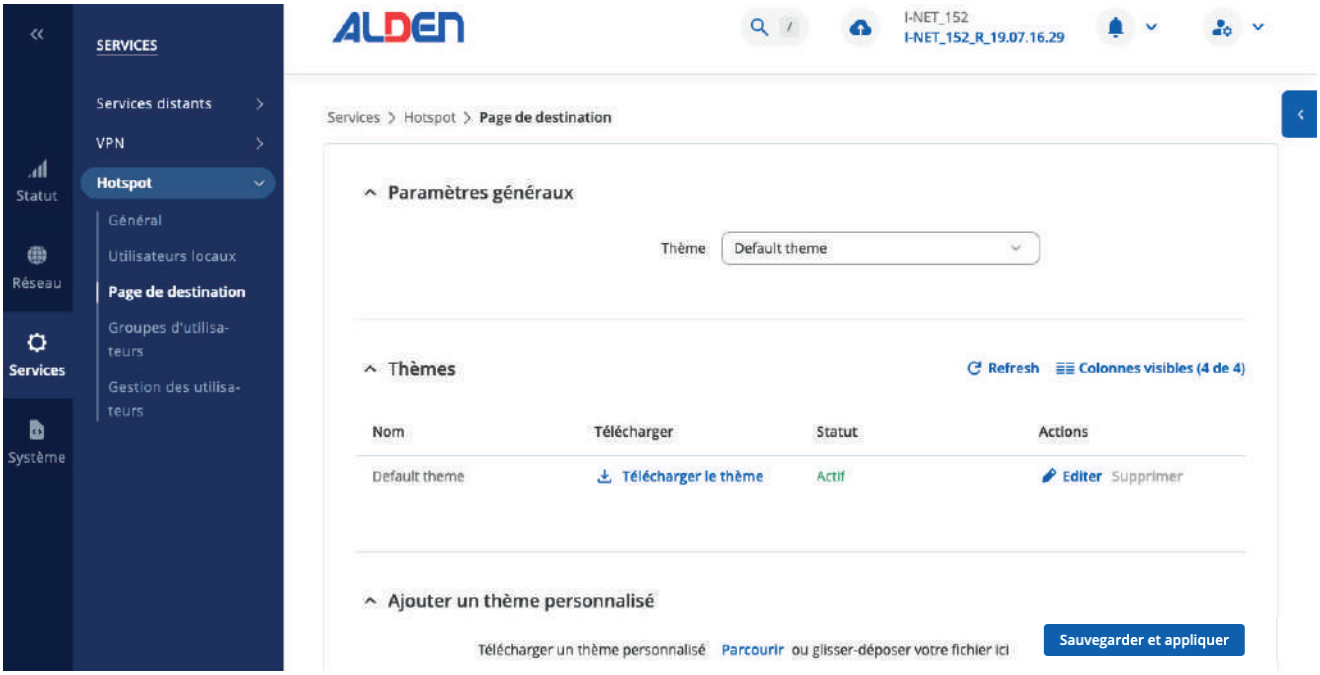
3.3.3 Menu SERVICES > HOTSPOT > Page de destination

Cette section sert à définir à quoi ressemblera la page de destination de votre point d'accès pour les utilisateurs qui se connectent.

Remarque : comme Hotspot prend en charge les utilisateurs non authentifiés, ces derniers utiliseront des adresses IP différentes. L'adresse IP sera incrémentée en fonction du préfixe fourni. Par exemple, si le réseau Hotspot est 192.168.2.0/24, le troisième octet sera incrémenté. Ainsi, l'adresse IP 192.168.2.254 deviendra 192.168.3.254. Si le réseau est 172.16.0.0/16, c'est le deuxième octet qui sera incrémenté. Ainsi, l'adresse IP 172.16.255.254 deviendra 172.17.255.254, et ainsi de suite. Après une authentification réussie, Hotspot utilisera le réseau configuré dans les paramètres généraux.

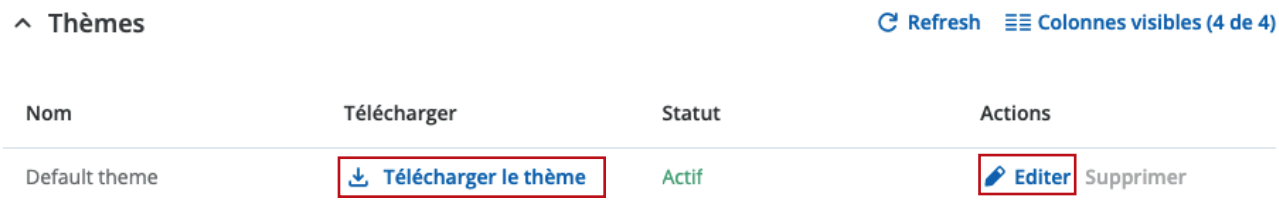
Paramètres généraux

La section Paramètres généraux vous permet de choisir le protocole d'authentification et le thème de la page d'accueil. Vous pouvez télécharger d'autres thèmes via le Gestionnaire de packages.



Thèmes

La section Thèmes affiche tous les thèmes disponibles pour les pages d'accueil. Pour télécharger un thème, cliquez sur le bouton « Télécharger ». Pour le modifier, cliquez sur le bouton « Editer » situé à côté.



Images

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



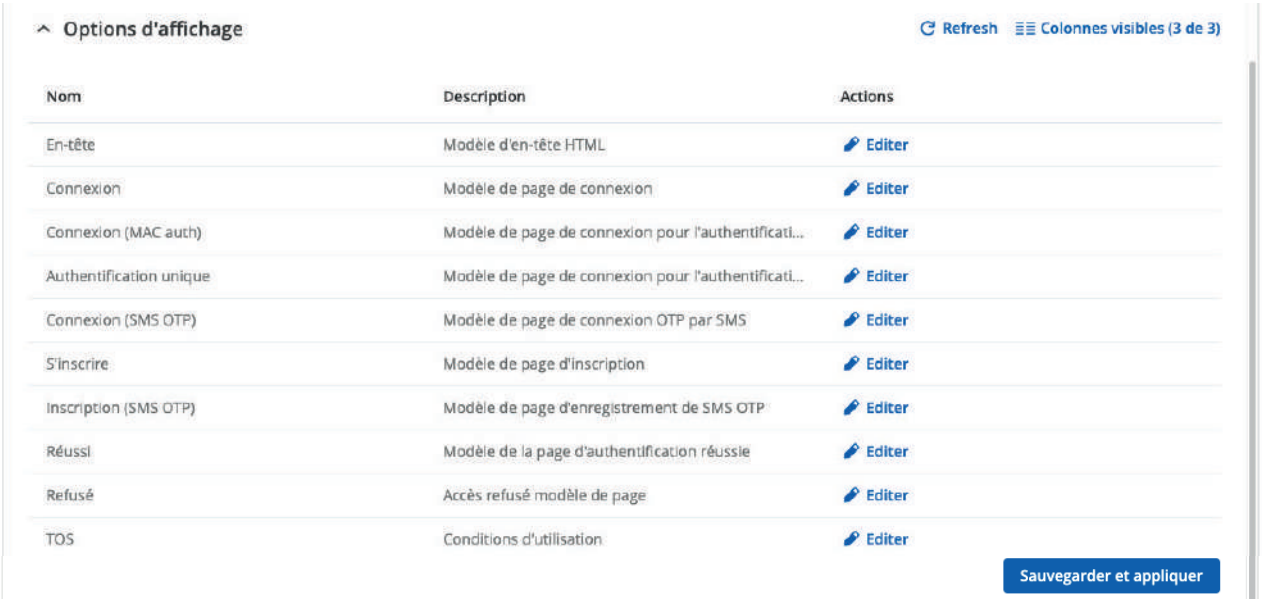
Paramètres de style

En cliquant sur le bouton « Modifier » situé à côté des paramètres de style, vous pouvez modifier l'apparence visuelle de votre page d'accueil à l'aide de la syntaxe CSS.



Afficher les paramètres

Dans les paramètres d'affichage, vous pouvez accéder aux modèles par défaut des différentes parties de la page d'accueil, les modifier et éditer leur code HTML.



Thème personnalisé

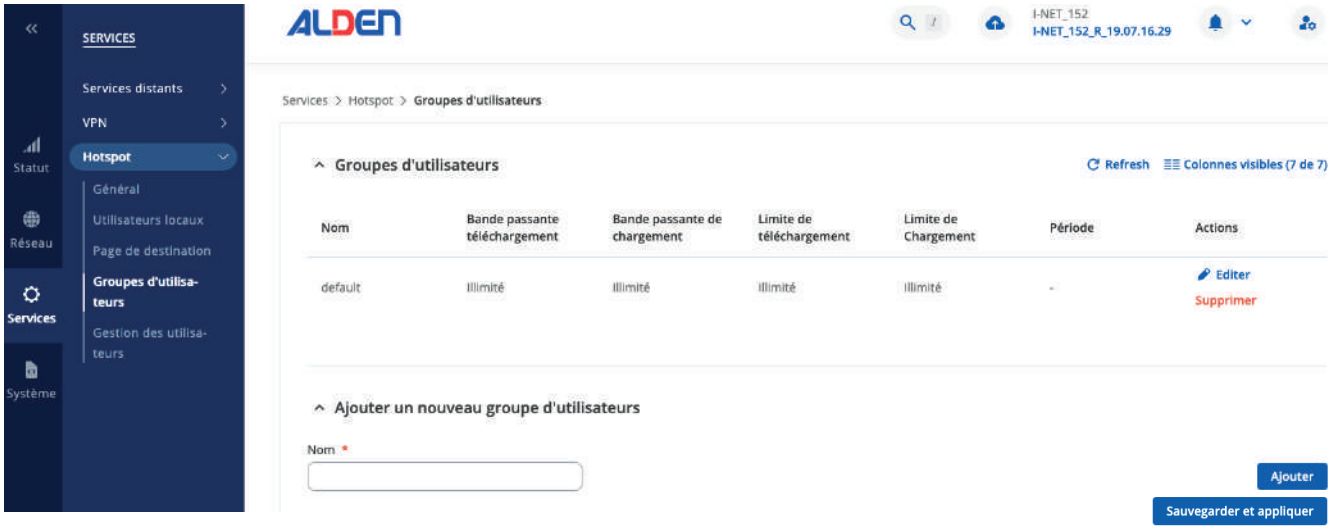
Pour utiliser un thème personnalisé, vous pouvez télécharger le thème par défaut et en modifier le contenu. Ensuite, utilisez le bouton « Parcourir » pour l'importer.



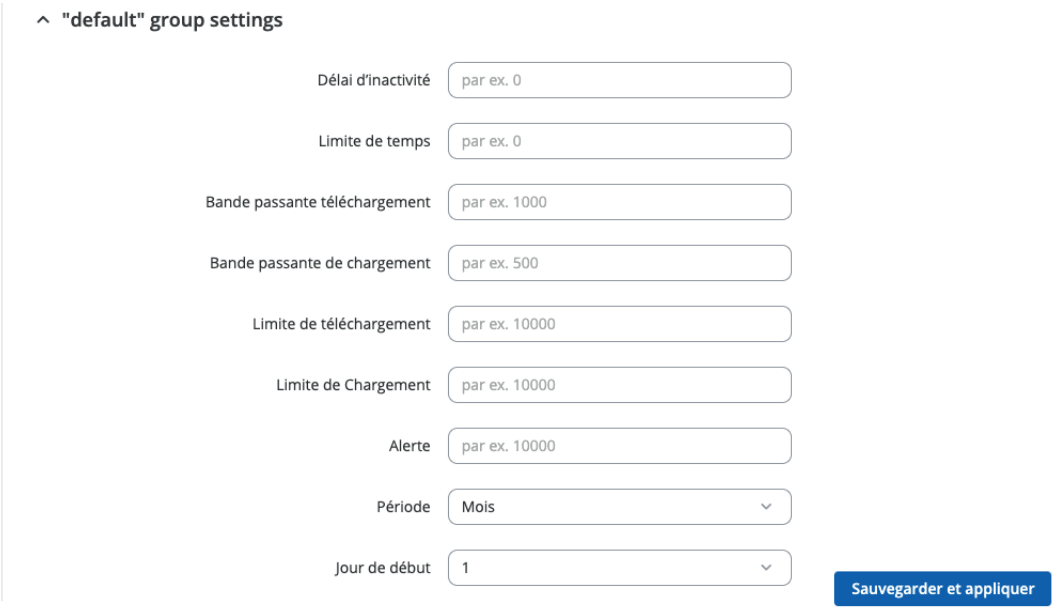
3.3.4 Menu SERVICES >HOTSPOT > Groupes d'utilisations

Les groupes d'utilisateurs permettent de définir des limites de connexion différentes pour chaque utilisateur. Un groupe nommé « default » est déjà créé et ne comporte aucune limitation par défaut. Vous pouvez

1. Créez un nouveau groupe en saisissant un nom personnalisé et en cliquant sur « Ajouter ».
2. ou configurez la règle existante en cliquant sur le bouton « Editer » situé à côté.



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

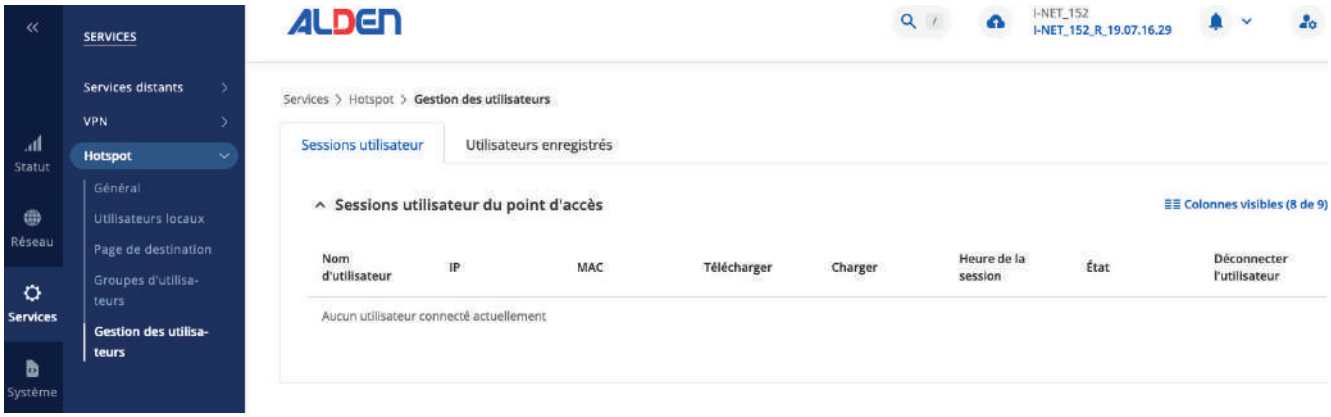


Délai d'inactivité	Entier Par défaut : aucun	Délai d'inactivité en secondes après lequel les utilisateurs inactifs sont automatiquement déconnectés du point d'accès. (0 signifie illimité.)
Limite de temps	Entier Par défaut : aucun	Désactive l'utilisateur du point d'accès WiFi une fois la limite de temps (en secondes) atteinte. (0 signifie illimité)
Bande passante de téléchargement	Entier Par défaut : aucun	Bande passante de téléchargement maximale autorisée pour les utilisateurs associés à ce modèle. La bande passante peut être spécifiée en Mbit/s.
Bande passante de chargement	Entier Par défaut : aucun	Bande passante maximale en envoi que les utilisateurs associés à ce modèle peuvent atteindre. La bande passante peut être spécifiée en Mbit/s.

Limite de téléchargement	Entier Par défaut : aucun	Limite de données reçues que les utilisateurs associés à ce modèle peuvent atteindre. Une fois cette limite atteinte, la connexion est interrompue. La limite de téléchargement est exprimée en Mo.
Limite de Chargement	Entier Par défaut : aucun	Limite de données envoyées que les utilisateurs associés à ce modèle peuvent atteindre. Une fois cette limite atteinte, la connexion est interrompue. La limite de chargement est exprimée en Mo.
Alerte	Entier Par défaut : aucun	Envoyer un SMS d'avertissement à l'utilisateur du point d'accès lorsque le seuil de téléchargement ou d'envoi de données (en Mo) est atteint. Fonctionne uniquement 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'applique. Une fois cette période écoulée, toutes les limites spécifiées sont réinitialisées.
Jour de début	entier [1..31] | Lundi.. Dimanche | entier [1..24] Par défaut : 1	Les options varient selon la période sélectionnée. Indique le jour du mois, de la semaine ou l'heure de la journée à laquelle les limites seront réinitialisées.

3.3.5 Menu SERVICES >HOTSPOT > Gestion des utilisateurs

L' onglet « Sessions utilisateur » affiche l'état et les statistiques de session des utilisateurs actuellement connectés. Vous pouvez également déconnecter un utilisateur en cliquant sur le bouton « Déconnexion » situé à côté de son nom.



L' onglet « Utilisateurs enregistrés » affiche les données des utilisateurs uniques qui se sont déjà inscrits au point d'accès.

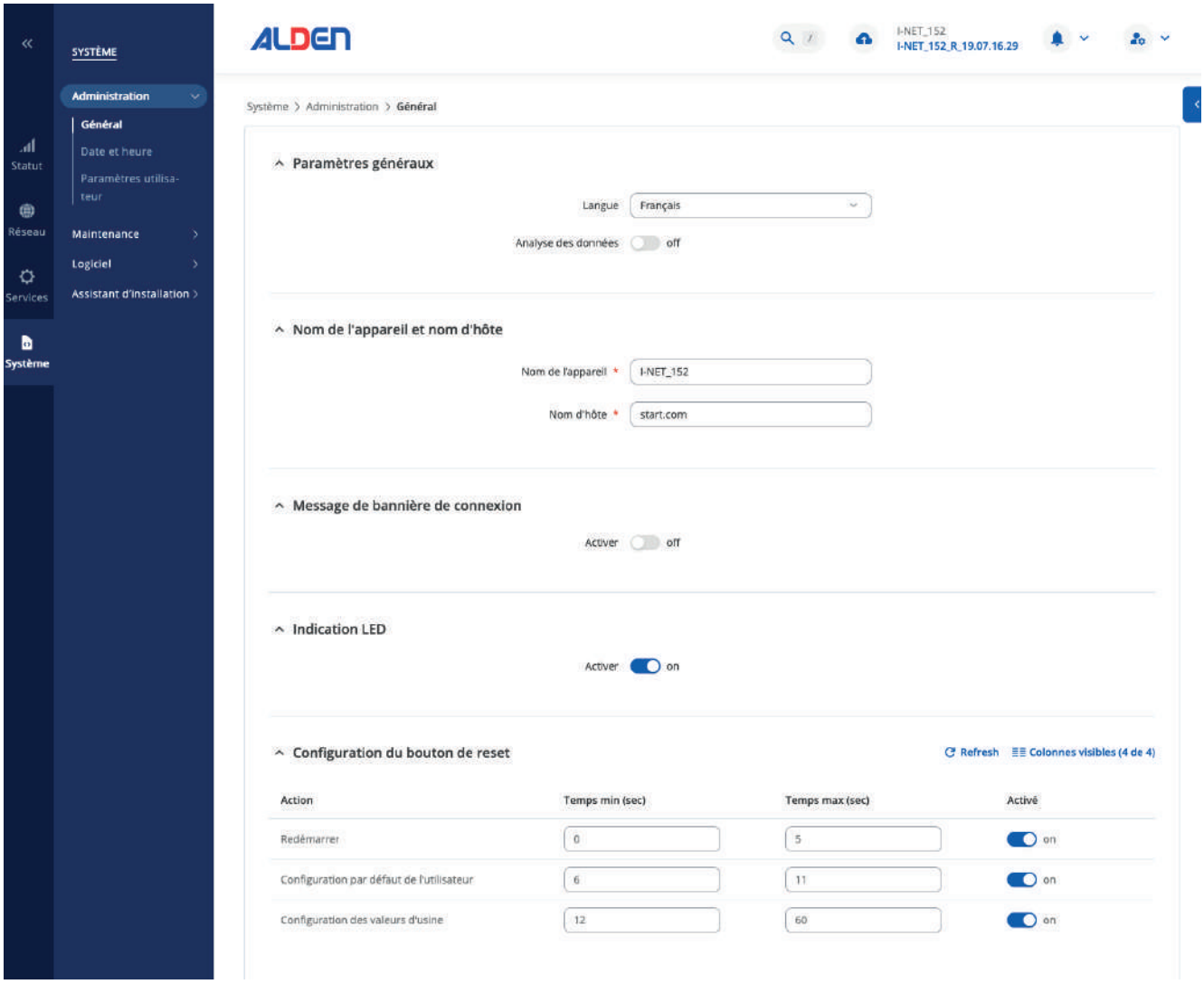


4 Menu SYSTÈME

4.1 Menu Système > ADMINISTRATION

4.1.1 Menu Système > ADMINISTRATION > GÉNÉRAL

La section Général permet de configurer certains paramètres de gestion du périphérique, comme sa dénomination. Pour plus d'informations sur la section Général, reportez-vous à la figure et au tableau ci-dessous.



Paramètres généraux

Langue	Anglais | Turc * | Espagnol * | Portugais * | Allemand * | Japonais * | Ukrainien * | Polonais * ; par défaut : anglais	Modifie la langue de l'interface Web du routeur. * Différents modules linguistiques peuvent être téléchargés séparément depuis la page Système → Gestionnaire de modules .
Analyse de données	Off | On ; Par défaut : On	Permet la collecte de données, utilisées pour améliorer la qualité et l'expérience utilisateur de nos produits. Cela inclut l'envoi d'informations concernant l'appareil et l'utilisation de l'interface web. Ces données sont collectées conformément à notre politique de confidentialité .

Nom du l'appareil et nom d'hôte

Nom de l'appareil	Chaîne de caractères Par défaut : I-NET_152	Nom du modèle de l'appareil.
Nom d'hôte	Chaîne de caractères Par défaut : start.com	Nom d'hôte du périphérique. Ce nom peut être utilisé pour communiquer avec d'autres hôtes du réseau local.

Message de bannière de connexion

Activer	Off | On ; Par défaut : Off	Ce message d'accueil s'affiche lors de la procédure de connexion. Il permet de s'assurer que tous les utilisateurs connaissent les règles et consignes à suivre avant d'accéder au système.
Titre du message	Chaîne de caractères Par défaut : Accès non autorisé interdit	Titre du message de la bannière de connexion.
Texte du message	Ce système est réservé à un usage autorisé. Toutes les activités sur ce système sont enregistrées et surveillées. En utilisant ce système, vous consentez à une telle surveillance. Un accès non autorisé ou une utilisation abusive peut entraîner des mesures disciplinaires, des sanctions civiles et pénales, ou les deux. Si vous n'êtes pas autorisé à utiliser ce système, déconnectez-vous immédiatement.	Texte du message de la bannière de connexion

Indication LED

Activer	Off | On ; Par défaut : On	Active/désactive l'indication par LED.

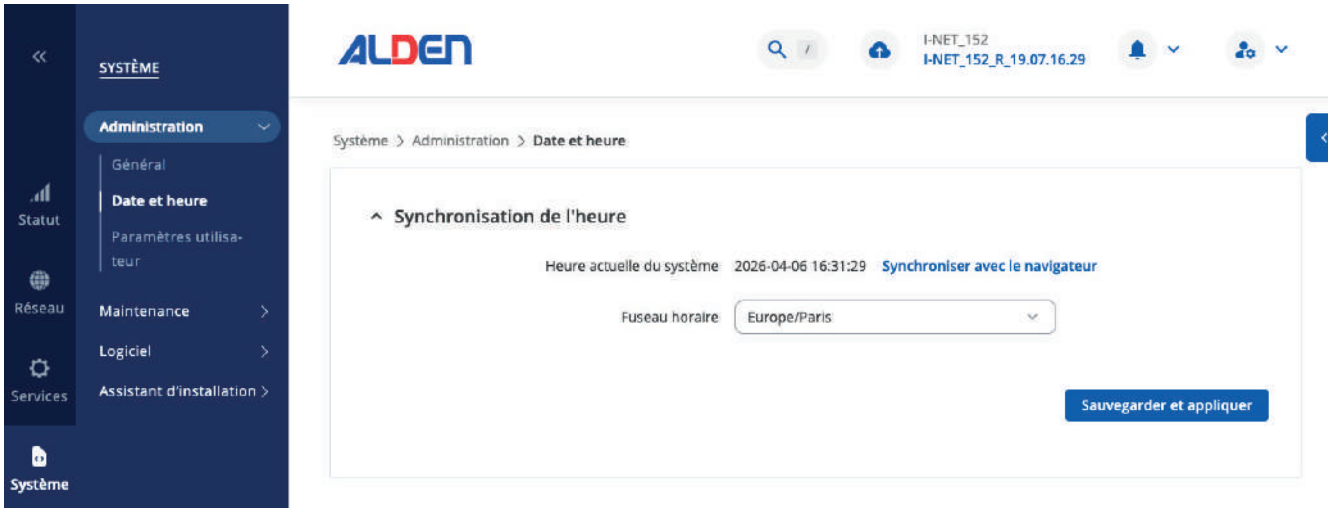
Configuration du bouton de réinitialisation

Temps min(sec)	Entier [0.60] Par défaut : aucun	Durée minimale (en secondes) pendant laquelle le bouton doit être maintenu enfoncé pour effectuer une action.
Temps max(sec)	Entier [1.60] ar 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

La section Synchronisation de l'heure vous permet de sélectionner le fuseau horaire et de synchroniser l'heure.

La figure ci-dessous est un exemple de la section Synchronisation de l'heure et le tableau ci-dessous fournit des informations sur les champs contenus dans cette section :

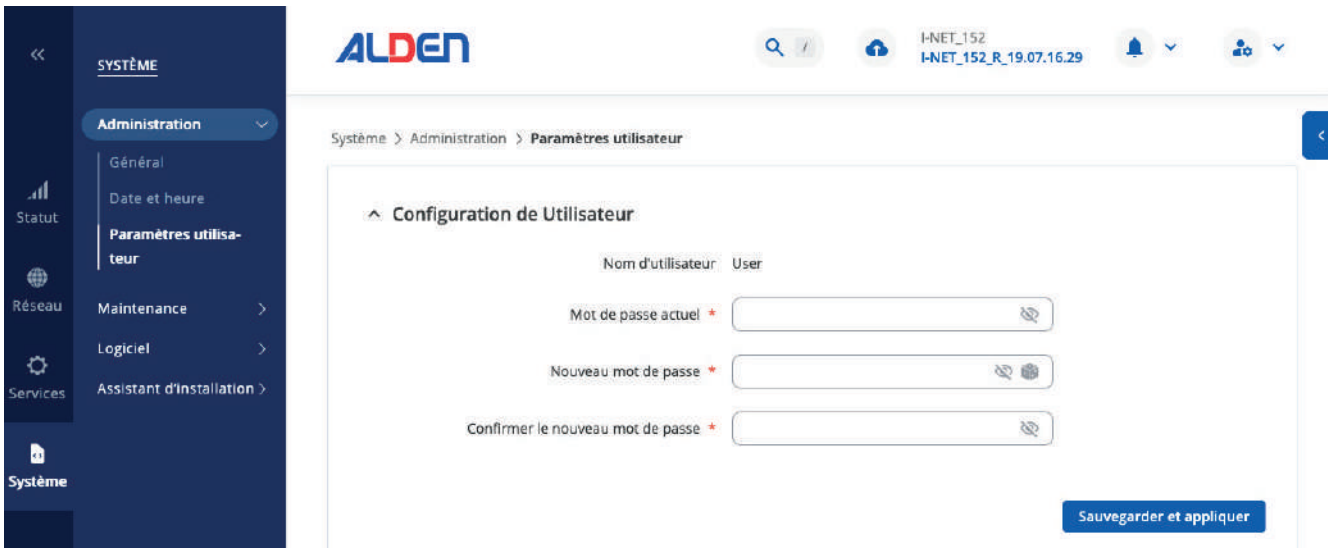


Heure système actuelle	Temps ; Par défaut : aucun	Heure locale actuelle de l'appareil.
Synchroniser avec le navigateur	-(bouton interactif)	Cliquez ici pour synchroniser l'heure et le fuseau horaire de votre appareil avec les navigateurs, si l'heure ou le fuseau horaire de votre appareil est incorrect.
Fuseau horaire	Fuseau horaire ; Par défaut : UTC	L'appareil synchronisera l'heure en fonction du fuseau horaire sélectionné.

4.1.3 Menu Système > ADMINISTRATION > PARAMÈTRES UTILISATEUR

CHANGER LE MOT DE PASSE

La section « Configuration utilisateur » permet de modifier le mot de passe de l'utilisateur actuel.



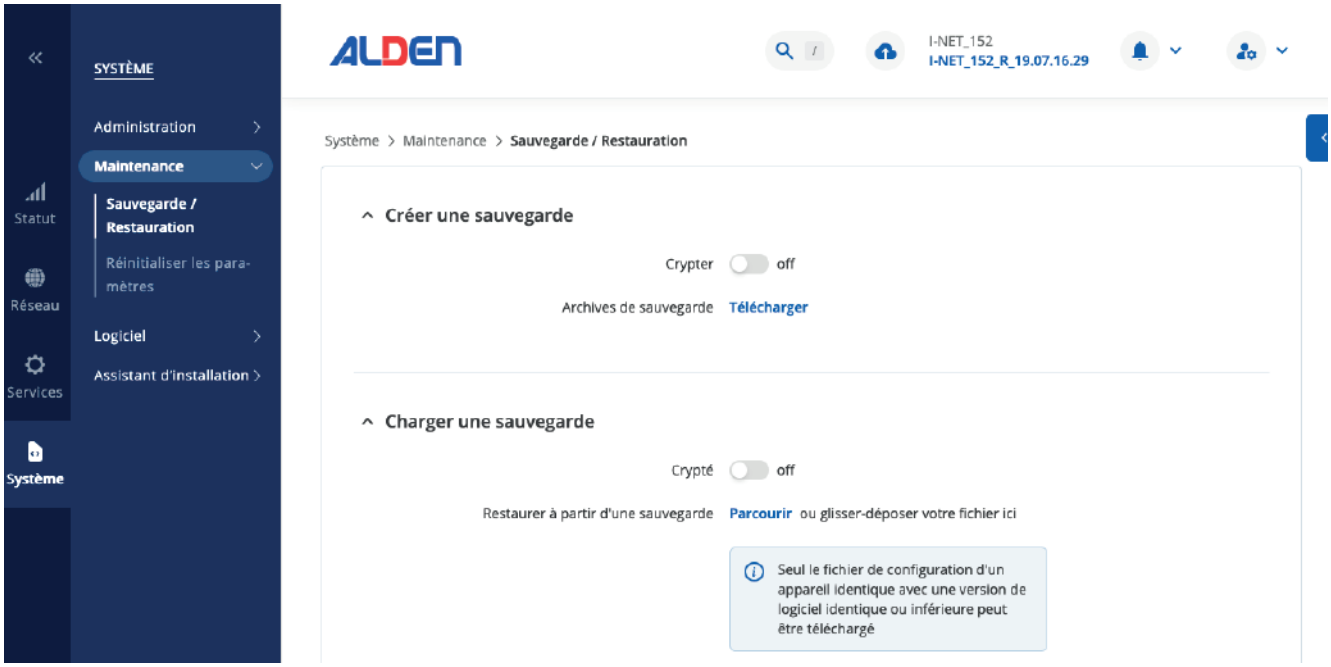
4.2 Menu Système > MAINTENANCE

4.2.1 Menu Système > MAINTENANCE > SAUVEGARDE/RESTAURATION

CRÉER UNE SAUVEGARDE

La section « Créer une sauvegarde » permet de générer et de télécharger un fichier contenant la configuration actuelle de l'appareil. Ce fichier de sauvegarde peut ensuite être importé sur le même appareil ou sur un autre appareil du même type (les références produits doivent correspondre).

Cette section contient les champs de somme de contrôle MD5 et SHA256 générés à partir du dernier fichier de sauvegarde téléchargé, l'option « Crypter » et le bouton « Télécharger » pour générer et télécharger le fichier de sauvegarde de la configuration de l'appareil.



Remarques importantes :

1. Le champ Mot de passe est obligatoire si le chiffrement est activé ; il apparaît alors uniquement si le mot de passe sert à chiffrer le fichier de sauvegarde. Il devra être fourni lors de l'extraction de l'archive ZIP formatée pour accéder au fichier TAR.

2. Le fichier de sauvegarde stocke le code PIN configuré sur la page mobile I-NET152, mais il ne sera restauré que si l'appareil n'a pas déjà de code PIN défini au moment du chargement du fichier de sauvegarde - le code PIN du fichier de sauvegarde ne sera défini que si l'appareil n'en a pas déjà un.

3. Si l'appareil n'est pas connecté à Internet lors du chargement d'un fichier de sauvegarde, les paquets logiciels installés via le Gestionnaire de paquets ne seront pas réinstallés . Vous pouvez ajouter manuellement les fichiers d'installation des paquets au fichier de sauvegarde ; un appareil I-NET152 les installera automatiquement lors du chargement du fichier de sauvegarde, même sans connexion Internet.

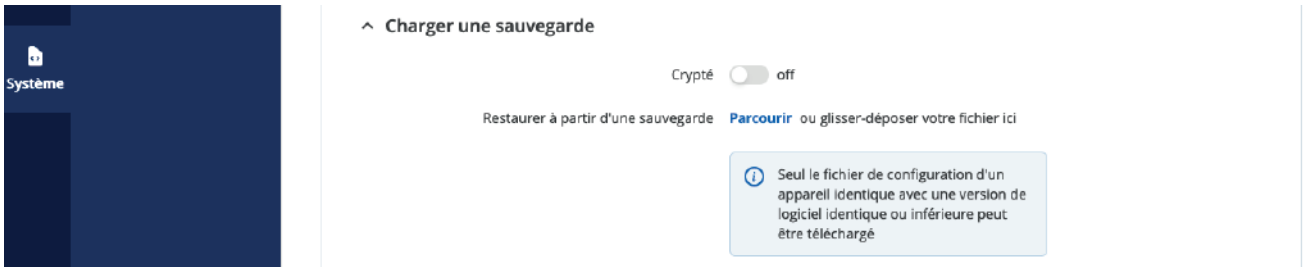
Pour intégrer un fichier de sauvegarde aux fichiers d'installation du package, suivez ces étapes :

- Téléchargez ici les fichiers d'installation du logiciel nécessaire.
- Télécharger 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

CHARGER UNE SAUVEGARDE

La section « Charger une sauvegarde » permet de télécharger un fichier de configuration provenant de cet appareil ou d'un autre appareil du même type.

Activez l'option « Crypté » si le fichier de sauvegarde était précédemment chiffré, puis cliquez sur le bouton « Parcourir » pour sélectionner un fichier de sauvegarde sur votre ordinateur et enfin sur le bouton « Télécharger l'archive » pour appliquer la configuration sélectionnée à cet appareil.



Remarques importantes

- Un mot de passe sera utilisé lors de l'extraction d'une archive 7z ou zip formatée pour accéder à un fichier tar.
- Les fichiers de sauvegarde ne peuvent être téléchargés que s'ils proviennent d'un appareil identique (code produit identique (vérifiable sur la page État → Système)) avec un firmware identique ou plus ancien.
- Il est important de noter que le fichier de sauvegarde modifie non seulement la configuration de l'appareil, mais aussi son mot de passe. Si vous ne connaissez pas le mot de passe du fichier de sauvegarde, il est conseillé de ne pas le télécharger avant de l'utiliser, car vous risquez de perdre l'accès à votre appareil.

VÉRIFICATION DE SÉCURITÉ DE SAUVEGARDE

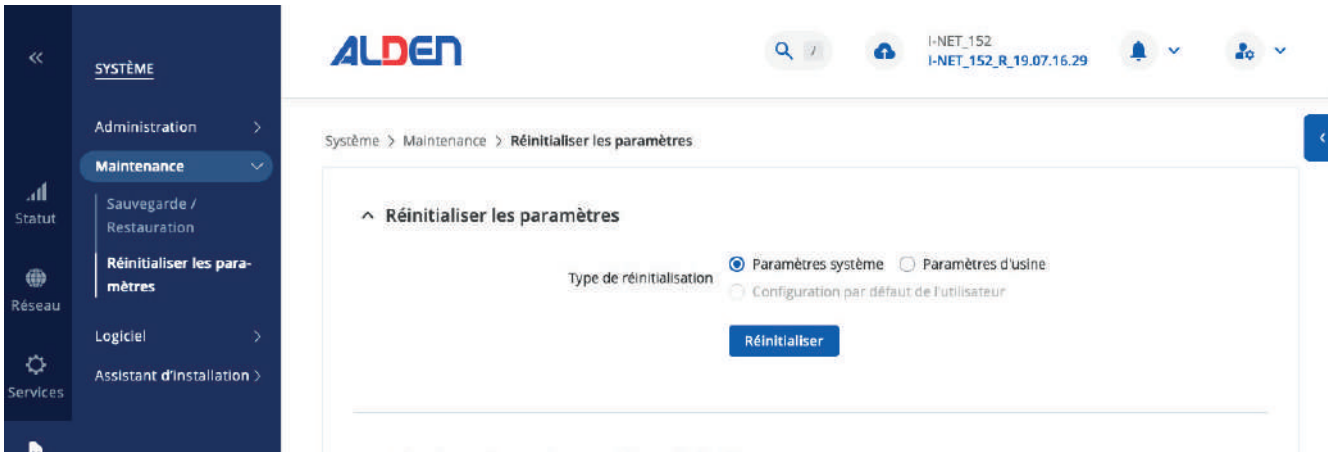
Après avoir importé un fichier de sauvegarde, votre appareil calculera et affichera sa somme de contrôle. Si ce fichier est le dernier téléchargé sur votre appareil, vous pourrez comparer cette somme de contrôle avec celles affichées dans la section « Créer une sauvegarde » afin de vérifier son intégrité.

Si tout est en ordre, cliquez sur « Procéder » pour restaurer la configuration à partir de la sauvegarde.

4.2.2 Menu Système > MAINTENANCE > RÉINITIALISER LES PARAMÈTRES

RÉINITIALISER LES PARAMÈTRES

La page de réinitialisation des paramètres permet de restaurer la configuration de l'appareil.

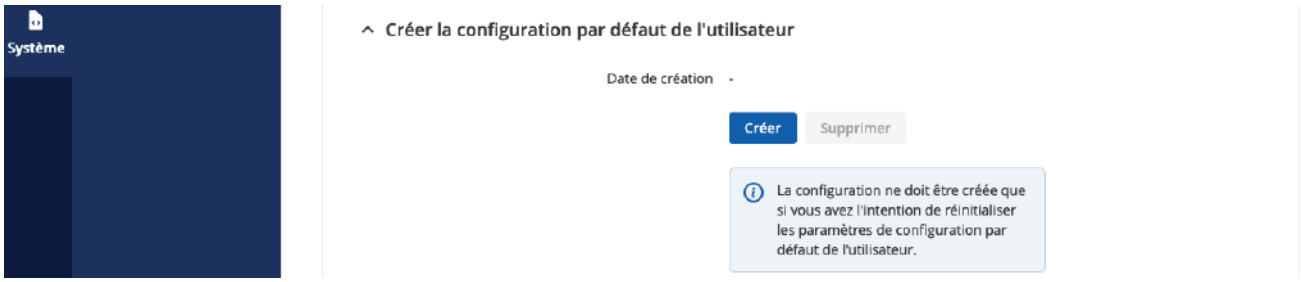


Paramètres système	-(sélection unique)	Réinitialise toute la configuration à l'exception des données RMS, de la base de données mdcollect, des journaux et du code PIN.
Paramètres d'usine	-(sélection unique)	Réinitialise l'appareil à sa configuration d'usine.
Configuration par défaut de l'utilisateur *	-(sélection unique)	Réinitialise l'appareil à sa configuration par défaut. * Ce bouton sera grisé jusqu'à ce que vous ayez créé une configuration par défaut pour

CRÉER LA CONFIGURATION PAR DÉFAUT DE L'UTILISATEUR

La section « Créer la configuration par défaut de l'utilisateur » permet de créer ou de supprimer un fichier contenant la configuration actuelle de l'appareil. Cette configuration par défaut peut ensuite être chargée depuis la page « Réinitialiser les paramètres » 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 appareil.

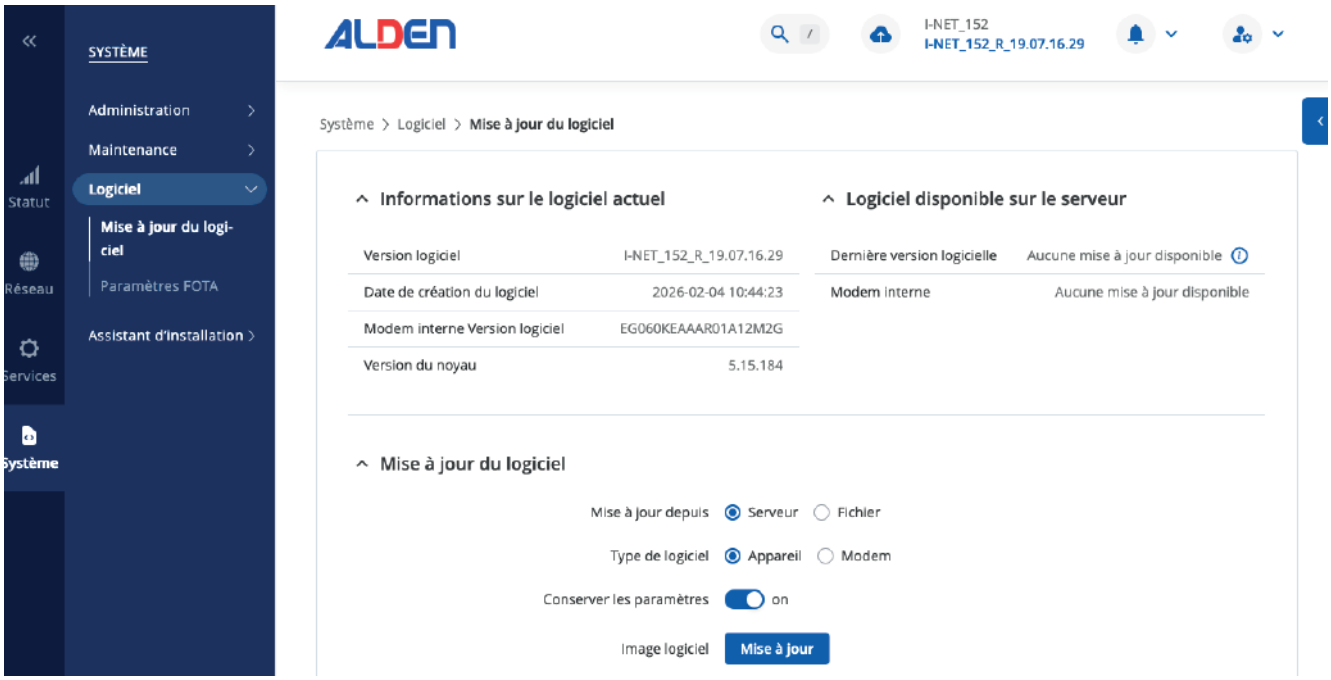


4.3 Menu Système > LOGICIEL

4.3.1 Menu Système > LOGICIEL > MISE À JOUR DU LOGICIEL

MISE À JOUR DU LOGICIEL

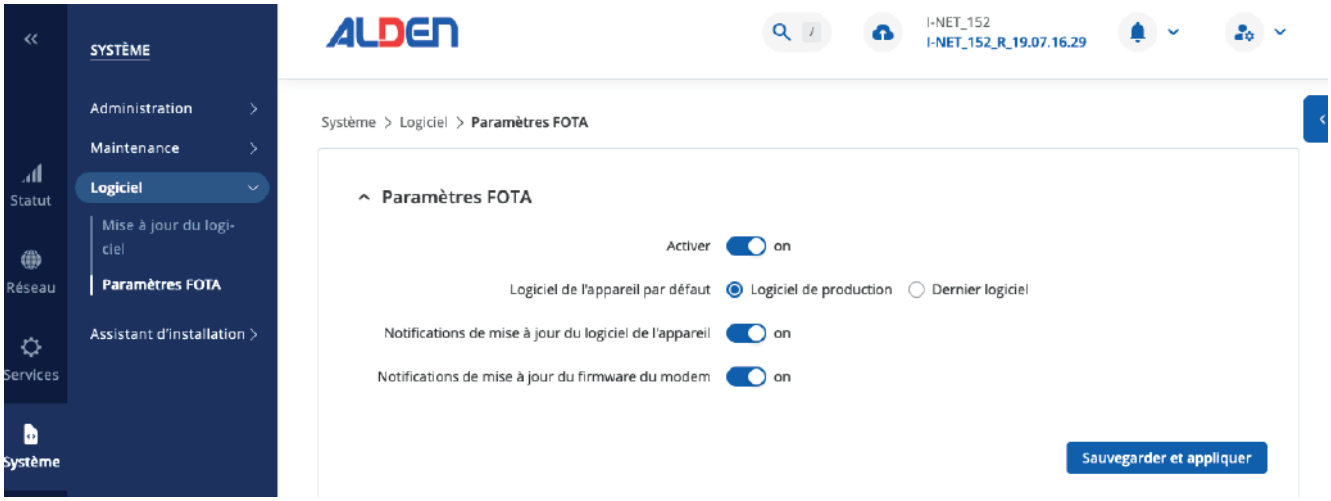
La page « Mise à jour du firmware » permet de mettre à jour le firmware de l'appareil/du modem. La mise à jour peut être effectuée soit depuis un serveur, soit à partir d'une image téléchargée depuis votre ordinateur.



Mise à jour depuis	Fichier | Serveur Par défaut : Serveur	Permet de sélectionner si le firmware sera téléchargé depuis le serveur ou chargé manuellement.
Type de logiciel	Appareil | Modem Par défaut : Appareil	Type de firmware à télécharger.
Conserver les paramètres	Off | On ; Par défaut : On	Garantit que tous les paramètres actuels de l'appareil seront conservés après la mise à jour du firmware.
Image logiciel	- (bouton interactif)	Cliquez ici pour parcourir votre ordinateur et rechercher un fichier image de firmware.

4.3.2 Menu Système > LOGICIEL > PARAMÈTRES FOTA

FOTA signifie « mise à jour du firmware par liaison radio » . Vous pouvez activer ou désactiver cette fonctionnalité ici.

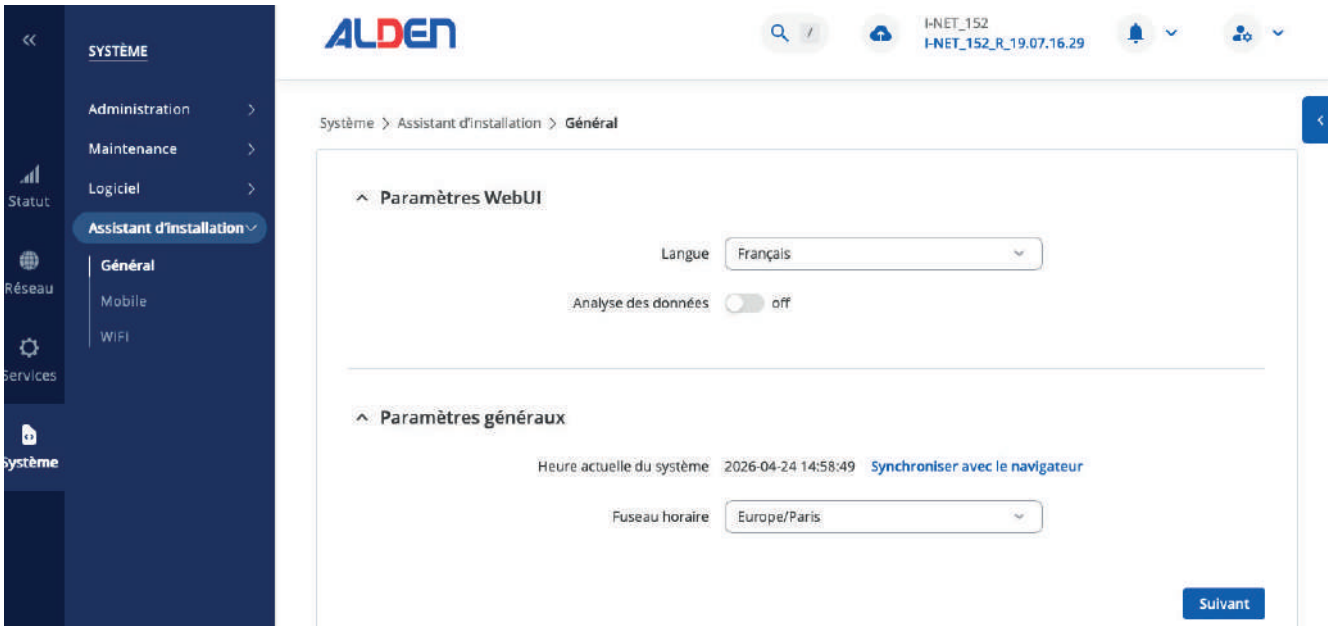


Activer	Off | On ; Par défaut : On	Active ou désactive le service FOTA.
Logiciel de l'appareil par défaut	Logiciel de production | Dernier logiciel Par défaut : Logiciel de production	Sélectionnez le type de firmware à mettre à jour.
notifications de mise à jour du micrologiciel de l'appareil	Off | On ; Par défaut : On	Active les notifications via l'interface Web lorsqu'une nouvelle version du firmware de l'appareil est disponible sur le serveur.
Notifications de mise à jour du micrologiciel du modem	Off | On ; Par défaut : On	Active les notifications via l'interface Web lorsqu'une nouvelle version du firmware du modem est disponible sur le serveur.

4.4 Menu Système > ASSISTANT D'INSTALLATION

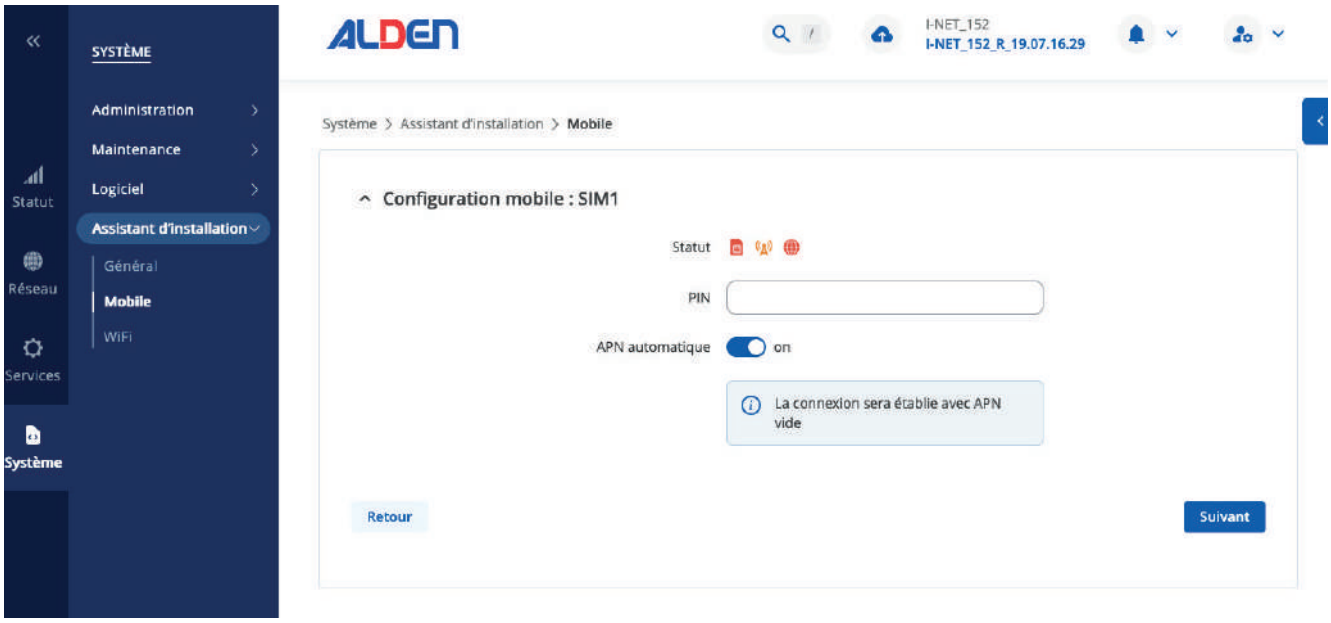
4.4.1 Menu Système > ASSISTANT D'INSTALLATION > GÉNÉRAL

La section Général permet de configurer l'heure, la langue et les paramètres du mode WebUI de l'appareil.



4.4.2 Menu Système > ASSISTANT D'INSTALLATION > MOBILE

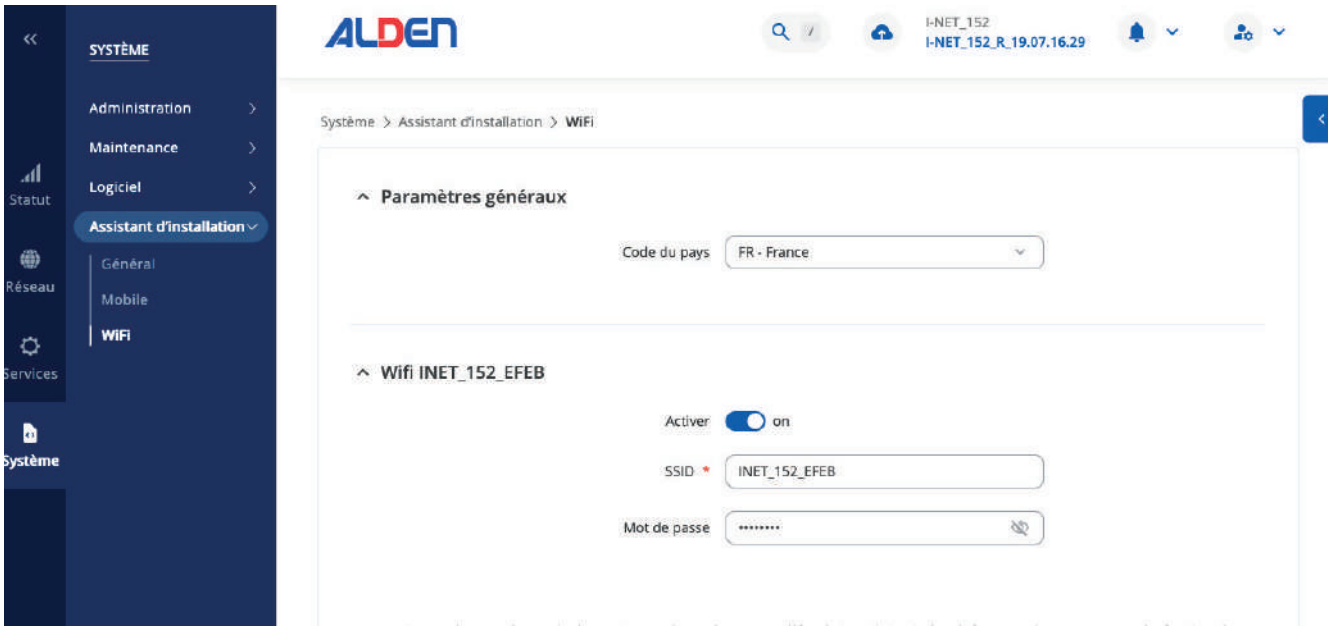
La section Mobile permet de configurer les paramètres de la carte SIM de l'appareil.



Statut	-(icônes interactives)	Affiche l'état de la connexion mobile.
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 la saisie de l'APN pour finaliser l'inscription au réseau. Dans d'autres cas, l'APN permet d'obtenir des paramètres spécifiques de l'opérateur (par exemple, une adresse IP publique), toujours selon le contrat. La fonction Auto APN analyse une base de données APN interne à 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, elle tente d'utiliser le suivant dans la base de données.
Off : APN	Suggestion de l'appareil | Personnalisé Par défaut : Suggestion de l'appareil	Choisissez entre un APN suggéré par l'appareil ou saisissez votre propre APN.
Personnalisé : APN personnalisé	Chaîne de caractères Par défaut : aucune	Identifiant de réseau APN personnalisé. Ne peut pas commencer par les chaînes suivantes : « rac », « lac », « sgsn » ou « rnc » ; ne peut pas se terminer par « .gprs » et ne peut pas prendre la valeur « * ».
Personnalisé : Type d'authentification	Aucun | PAP | CHAP Par défaut : Aucun	La méthode utilisée par votre opérateur pour authentifier les nouvelles connexions à son réseau. Si vous sélectionnez PAP, CHAP ou les deux, vous devrez saisir un nom d'utilisateur et un mot de passe.
Nom d'utilisateur	Chaîne de caractères Par défaut : aucun	Votre nom d'utilisateur, celui que vous utiliserez pour vous connecter au réseau de votre opérateur GSM.
Mot de passe	Chaîne de caractères Par défaut : aucun	Votre mot de passe, celui que vous utiliserez pour vous connecter au réseau de votre opérateur GSM.
ÉPINGLE	Chaîne de caractères Par défaut : aucun	Un mot de passe numérique long à 4 chiffres utilisé pour authentifier le mod

4.4.3 Menu Système > ASSISTANT D'INSTALLATION > WIFI

La section WiFi permet de configurer le point d'accès WiFi (AP) de l'appareil.



Activer	Off | On ; Par défaut : On	Active ou désactive le point d'accès WiFi.
SSID	Chaîne de caractères Par défaut : RUT_<4 derniers symboles de l'adresse MAC WiFi>	Chaîne d'identification (nom) du point d'accès. C'est ainsi que les appareils connectés le reconnaîtront.
Mot de passe	Chaîne de caractères Par défaut : unique à chaque appareil	Un mot de passe utilisé pour authentifier les utilisateurs à ce point d'accès.

Garantie ALDEN

La garantie ALDEN couvre :

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

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

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

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

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

Sont exclus de la garantie ALDEN :

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

Garantie

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

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

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

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

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

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

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

Bon de garantie

NOM, Prénom : .....

Adresse complète : .....

.....

Code postal : .....

Ville : .....

Concessionnaire : .....

Date d'achat : .....

Produit : .....

N° de série : .....

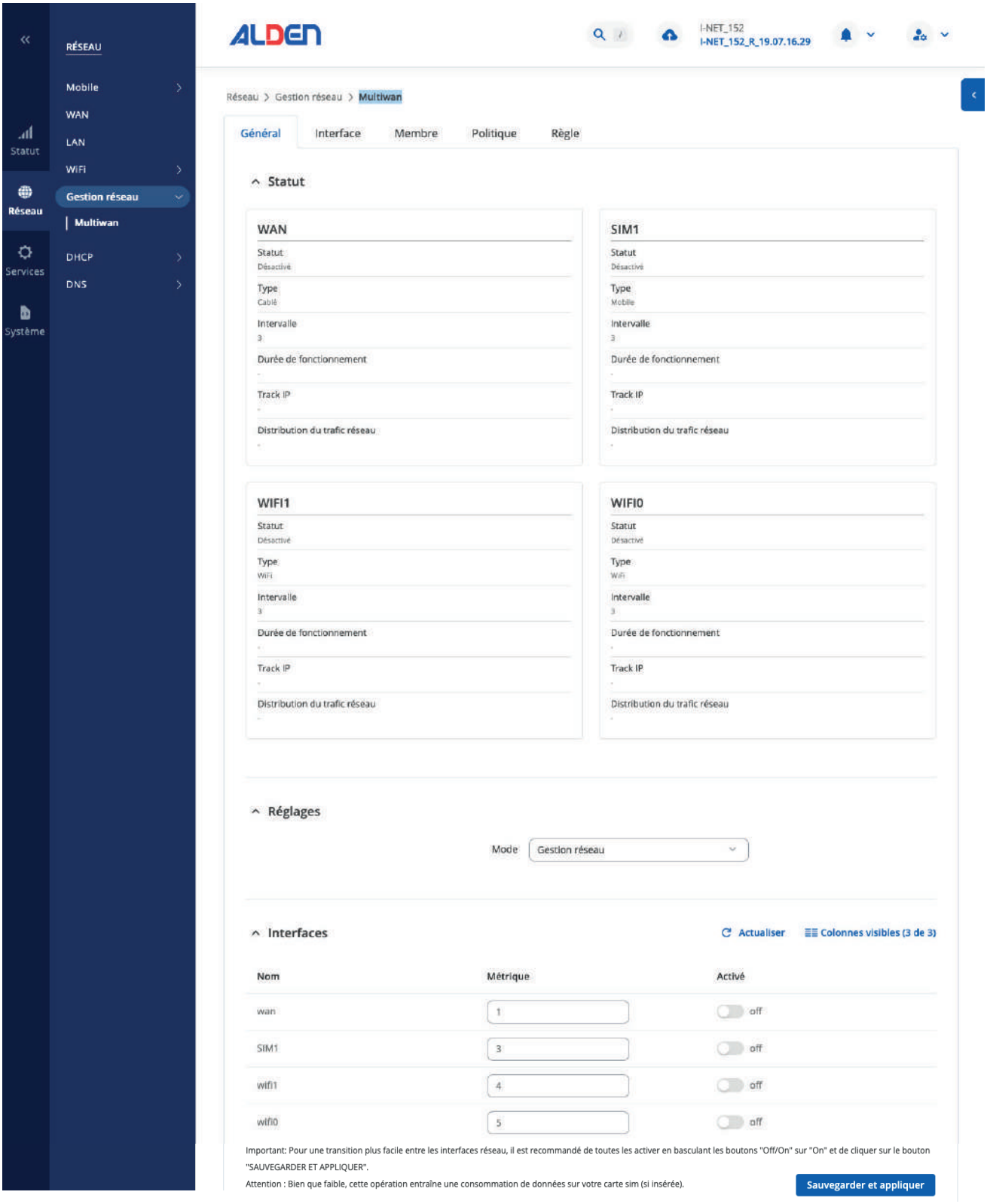
2.5 Menu RÉSEAU > GESTION RÉSEAU

2.5.1 Menu RÉSEAU > GESTION RÉSEAU > MULTIWAN

La fonction de Multiwan vous permet de sauvegarder votre connexion WAN principale en cas de panne.

Pour définir les priorités, il suffit de modifier les indicateurs d'interface dans la section « Interfaces », puis d'appuyer sur « Enregistrer et appliquer ».

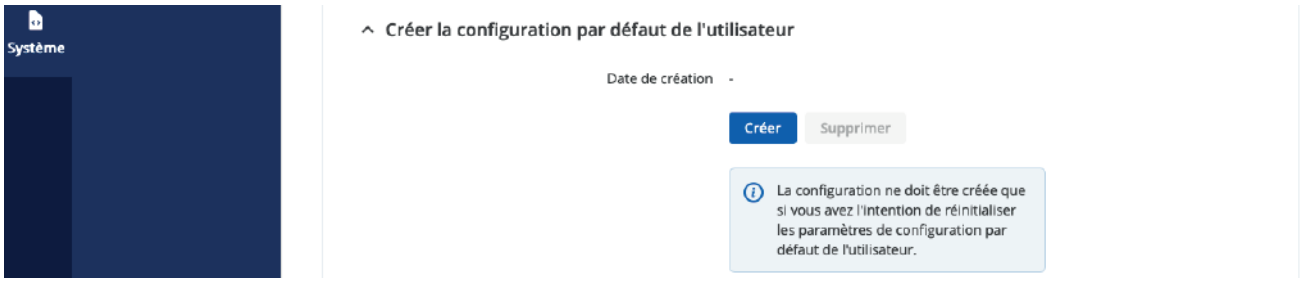
Remarque : vous ne verrez aucune interface WAN câblée supplémentaire à moins que vous n'ayez configuré des ports LAN comme WAN.



CRÉER LA CONFIGURATION PAR DÉFAUT DE L'UTILISATEUR

La section « Créer la configuration par défaut de l'utilisateur » permet de créer ou de supprimer un fichier contenant la configuration actuelle de l'appareil. Cette configuration par défaut peut ensuite être chargée depuis la page « Réinitialiser les paramètres » 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 appareil.

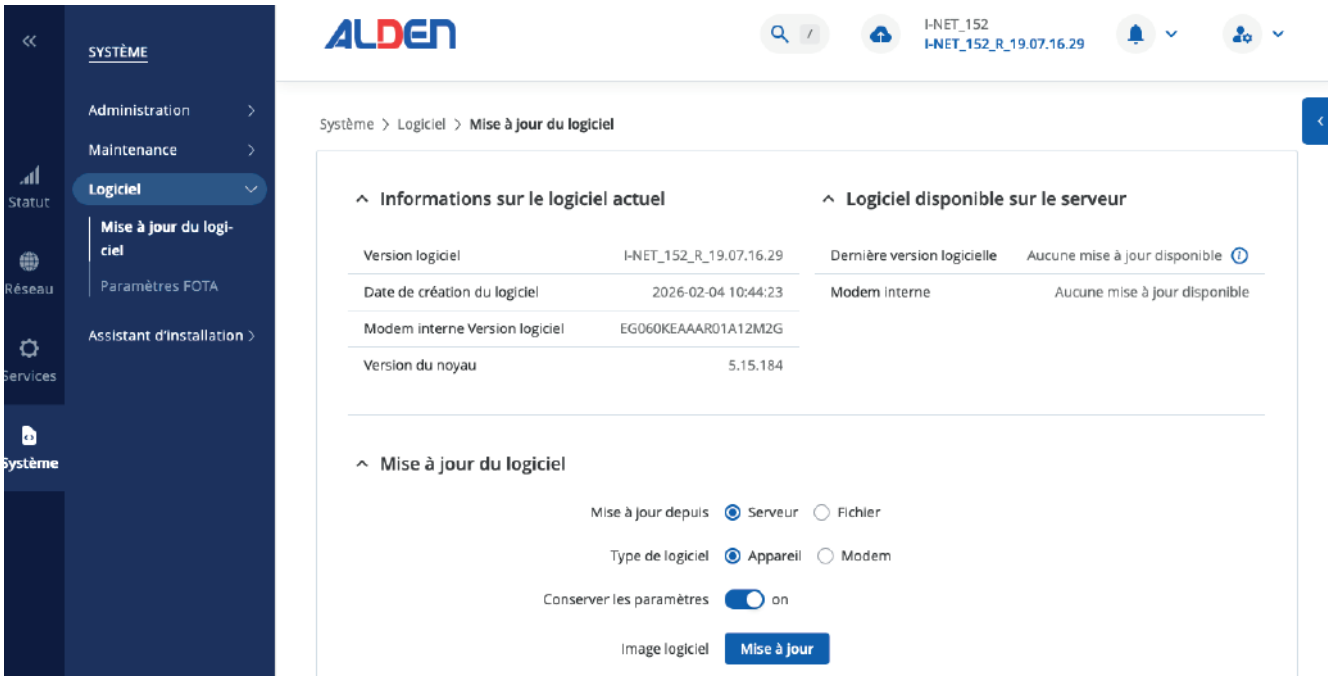


4.3 Menu Système > LOGICIEL

4.3.1 Menu Système > LOGICIEL > MISE À JOUR DU LOGICIEL

MISE À JOUR DU LOGICIEL

La page « Mise à jour du firmware » permet de mettre à jour le firmware de l'appareil/du modem. La mise à jour peut être effectuée soit depuis un serveur, soit à partir d'une image téléchargée depuis votre ordinateur.



Mise à jour depuis	Fichier | Serveur Par défaut : Serveur	Permet de sélectionner si le firmware sera téléchargé depuis le serveur ou chargé manuellement.
Type de logiciel	Appareil | Modem Par défaut : Appareil	Type de firmware à télécharger.
Conserver les paramètres	Off | On ; Par défaut : On	Garantit que tous les paramètres actuels de l'appareil seront conservés après la mise à jour du firmware.
Image logiciel	– (bouton interactif)	Cliquez ici pour parcourir votre ordinateur et rechercher un fichier image de firmware.