DOCUMENTATION 7.00

Manuel d'utilisation NXS-9700

Documentation

FRANÇAIS · SMSEAGLE

Ce document a été traduit automatiquement (IA) et peut contenir des erreurs.

Table of contents

Couverture . . . 9

Informations sur la licence du logiciel SMSEagle . . . 10

Contenu de la boîte . . . 19

Assistant de configuration . . . 21

- Étape 1 : Langue et heure . . . 21
- Étape 2 : Compte administrateur . . . 21
- Étape 3 : Notifications . . . 22
- Étape 4 : Modems . . . 23

Connecteurs, ports et LED . . . 24

Aperçu de l'interface Web . . . 26

- Connexion . . . 26
- Disposition de l'interface . . . 27
- Tableau de bord . . . 27
  - Needs your attention . . . 28
  - Traffic . . . 29
  - Unread messages . . . 29
  - Système . . . 29
  - Derniers messages et appels . . . 30
  - Modems . . . 30
- Actions rapides . . . 31
- Paramètres du compte personnel . . . 31
  - Données personnelles . . . 32
  - Mot de passe . . . 32
  - Sécurité . . . 33

Messages . . . 34

- SMS (Conversations) . . . 34
  - Composition d'un message . . . 35
- Dossiers . . . 36
- Groupes de messages . . . 37
- File d'attente d'escalade . . . 38
- Appels . . . 39
  - Historique . . . 39
- WhatsApp . . . 40
- Signal . . . 42
- Emails . . . 43
- Modèles de message . . . 43

Carnet d'adresses . . . 44

- Contacts . . . 44
- Groupes . . . 44
  - Groupes d'escalade . . . 45

Équipes . . . 47
Avant de commencer . . . 47
Étape 1 : Ouvrir la page Équipes . . . 47
Étape 2 : Créer une équipe . . . 47
Étape 3 : Assigner des contacts à l'équipe . . . 48
Étape 4 : Choisir ce qui se passe en dehors des heures d'équipe . . . 48
Automatisation . . . 49
Email vers SMS . . . 49
Où la trouver . . . 49
Étape 1 : Comprendre le format de l'adresse destinataire . . . 49
Étape 2 : Créer une nouvelle règle . . . 50
Étape 3 : Ajouter des conditions de filtrage (facultatif) . . . 51
Étape 4 : Gérer les règles existantes . . . 52
Collecteur d'e-mails vers SMS . . . 52
Où la trouver . . . 52
Création d'une règle . . . 53
SMS vers E-mail . . . 53
Ce que fait cette fonctionnalité . . . 53
Avant de commencer . . . 53
Étape 1 : Ouvrir la page SMS vers E-mail . . . 53
Étape 2 : Créer une règle . . . 54
SMS Forward . . . 55
Ce que fait cette fonctionnalité . . . 55
Avant de commencer . . . 55
Étape 1 : Ouvrir la page SMS Forward . . . 56
Étape 2 : Créer une règle . . . 56
Fonctionnement du transfert . . . 58
Réponses automatiques . . . 58
Ce que fait cette fonctionnalité . . . 58
Avant de commencer . . . 59
Étape 1 : Ouvrez la page Réponses automatiques . . . 59
Étape 2 : Créer une règle . . . 59
Étape 3 : Définissez la limite d'envoi . . . 60
Comment fonctionne la correspondance . . . 60
SMS périodique . . . 61
Ce que fait cette fonctionnalité . . . 61
Avant de commencer . . . 61
Étape 1 : Ouvrez la page SMS périodique . . . 61
Étape 2 : Créer une règle . . . 61
Abonnements . . . 63
Ce que fait cette fonctionnalité . . . 63
Avant de commencer . . . 63
Étape 1 : Ouvrir la page Abonnements . . . 64
Étape 2 : Créer une règle . . . 64
Comment fonctionne la correspondance . . . 64
Ce qui se passe quand quelqu'un s'abonne . . . 65
Liste d'autorisation / d'interdiction . . . 65

Ce que fait cette fonctionnalité . . . 65
Avant de commencer . . . 66
Étape 1 : Ouvrir la page Liste d'autorisation / d'interdiction . . . 66
Étape 2 : Choisir le mode actif . . . 66
Étape 3 : Ajouter un numéro . . . 66
Étape 4 : Importer une liste à partir d'un CSV . . . 67
Étape 5 : Configurer le mot STOP (optionnel) . . . 67
Fonctionnement du filtrage . . . 68
Workflows . . . 68
Où la trouver . . . 69
Étape 1 : Créer un workflow et choisir un déclencheur . . . 69
Étape 2 : Ajouter des groupes de conditions (optionnel) . . . 69
Étape 3 : Ajouter des actions . . . 69
Webhooks . . . 69
Ce que fait cette fonctionnalité . . . 69
Avant de commencer . . . 70
Étape 1 : Ouvrir la page Webhooks . . . 70
Étape 2 : Créer une règle . . . 70
Étape 3 : Configuration de base . . . 71
Étape 4 : Conditions de déclenchement . . . 73
Étape 5 : Paramètres de sécurité . . . 74
Étape 6 : Définir l'intervalle de nouvelle tentative . . . 74
Comportement des webhooks . . . 75
MQTT . . . 75
Ce que fait cette fonctionnalité . . . 75
Avant de commencer . . . 76
Partie 1 : S'abonner (MQTT vers SMS) . . . 76
Partie 2 : Publish (SMS dans MQTT) . . . 77
Règles de la boîte de réception . . . 79
Où la trouver . . . 79
Configuration d'une règle de boîte de réception . . . 80
Nettoyage des dossiers . . . 80
Où la trouver . . . 80
Configuration d'une règle de nettoyage . . . 80
Rapports et statistiques . . . 81
Rapports . . . 81
Rapports périodiques . . . 82
Statistiques . . . 83
Statistiques périodiques . . . 84
Surveillance . . . 85
Moniteur réseau . . . 85
À quoi sert cette fonctionnalité . . . 85
Avant de commencer . . . 85
Partie 1 : Tâches . . . 86
Partie 2 : Rapports . . . 91
Partie 3 : Traps SNMP . . . 92

Comportement du Network Monitor . . . 94
Entrée/Sortie numérique . . . 95
À quoi sert cette fonctionnalité . . . 95
Avant de commencer . . . 95
Hardware: ports, logic levels and wiring . . . 96
Où le trouver . . . 99
Partie 1 : Règles d'entrée (signal d'entrée vers SMS) . . . 100
Partie 2 : Règles de sortie (SMS vers signal de sortie) . . . 103
Partie 3 : Broches internes . . . 106
Partie 4 : Broches externes . . . 106
Fonctionnement des règles Digital I/O . . . 108
Capteurs de température et d'humidité . . . 108
À quoi sert cette fonctionnalité . . . 108
Avant de commencer . . . 109
Où le trouver . . . 109
Partie 1 : Ajouter et nommer les capteurs . . . 110
Partie 2 : Règles d'alarme . . . 112
Partie 3 : Lectures et rapports . . . 114
Comment cela fonctionne . . . 116
Paramètres . . . 117
Paramètres du compte . . . 117
Comment configurer l'authentification multifacteur (MFA) . . . 117
SMS / MMS . . . 118
Messages . . . 118
Modems . . . 119
Multimodem . . . 119
MMS . . . 120
Appels . . . 122
Modèles locaux TTS . . . 122
Modèles TTS en ligne (ElevenLabs) . . . 124
Appels entrants . . . 126
Renvoi d'appel . . . 126
WhatsApp . . . 126
Ce que cette fonction fait . . . 126
Avant de commencer . . . 127
Étape 1 : Ouvrir les paramètres WhatsApp . . . 127
Étape 2 : Activer le service . . . 127
Étape 3 : Lier votre téléphone . . . 127
Étape 4 : Décider ce qui se passe pour les destinataires non WhatsApp . . . 128
Étape 5 : Maintenir le service à jour . . . 128
Déliaison et désactivation . . . 128
Bon à savoir . . . 129
Signal . . . 129
Ce que cette fonction fait . . . 129
Avant de commencer . . . 130
Étape 1 : Ouvrir les paramètres Signal . . . 130
Étape 2 : Activer le service . . . 130

Étape 3 : Enregistrer un numéro de téléphone . . . 130
Étape 4 : Vérifier le numéro . . . 131
Étape 5 : Maintenir le service à jour . . . 131
Suppression du numéro . . . 132
Bon à savoir . . . 132
Email . . . 133
Email vers SMS . . . 133
Email to SMS Poller . . . 134
Configuration SMTP . . . 136
Alertes email . . . 136
SMPP . . . 137
Détails de la connexion . . . 138
Activation de SMPP . . . 138
MQTT . . . 139
Réseau . . . 140
Paramètres IP . . . 140
SSL . . . 141
Basculement . . . 141
SNMP . . . 142
Données mobiles . . . 147
Application . . . 148
Régional . . . 148
Sécurité . . . 148
Accès et visibilité . . . 148
API et intégrations . . . 149
LDAP . . . 149
Ce que cette fonction fait . . . 149
Avant de commencer . . . 150
Étape 1 : Ouvrir la page LDAP . . . 150
Étape 2 : Activer l'intégration . . . 150
Étape 3 : Connexion . . . 151
Étape 4 : Structure du répertoire . . . 151
Étape 5 : Attributs et sécurité . . . 152
Étape 6 : Synchronisation et accès . . . 152
Étape 7 : Enregistrer et tester . . . 154
Date / Heure . . . 155

Système . . . 156
Utilisateurs . . . 156
Informations système . . . 156
Journaux . . . 157
Mises à jour . . . 157
Correctifs . . . 157
Sauvegarde / Restauration . . . 157
Redémarrage . . . 157
Avancé . . . 158

Intégration API et développeur . . . 159
Référence API . . . 159
Clés API . . . 159
Clés API v2 . . . 159
Clés API v1 . . . 160
Créer une clé . . . 160
Quels utilisateurs ont accès à l'API . . . 161
Accès aux ressources d'autres utilisateurs . . . 162

Plugins et intégrations . . . 163

Avancé . . . 164
Connexion directe à la base de données SMSEagle . . . 164
Injection d'un SMS court via SQL . . . 164
Injection d'un SMS long via SQL . . . 165
Scripts de nettoyage de base de données . . . 167
Transfert des journaux vers un serveur externe . . . 167

Dépannage . . . 169
Vérification des LED . . . 169
Vérification des informations de l'appareil . . . 170
Journaux de l'appareil . . . 170
Lorsque l'appareil n'est pas joignable . . . 170
Restauration des paramètres d'usine . . . 170
Hardware Rev.5 et ultérieure . . . 171
Hardware Rev.3–Rev.4 . . . 171
Service et réparation . . . 172
Garantie . . . 172
Service . . . 172

Spécifications techniques et informations de sécurité . . . 173
Spécification technique . . . 173
Spécification matérielle . . . 173
Alimentation électrique . . . 176
Antenne . . . 176
Débit d'émission/réception . . . 177
Plateforme logicielle . . . 177
Informations importantes de sécurité . . . 177

Déclarations réglementaires . . . 179
Déclaration de conformité UE . . . 179
Déclaration de conformité FCC . . . 179
Déclaration de conformité du fournisseur FCC . . . 180
Déclaration réglementaire canadienne (ISDE) . . . 180
Avis de conformité à la réglementation d'Industrie Canada . . . 181
Déclaration de conformité du Royaume-Uni . . . 181
Limites d'exposition aux radiofréquences . . . 181
Informations sur l'élimination et le recyclage . . . 181

Union européenne — Informations sur l’élimination 181
Pour l’élimination dans les pays en dehors de l’Union européenne 182
Informationen gemäß § 4 Absatz 4 Elektrogesetz (DE) 182
Informations relatives à l’enlèvement sûr des piles ou des accumulateurs 182
Directive relative à la restriction de l’utilisation de certaines substances dangereuses (RoHS) 183
RoHS de l’Union européenne 183

Couverture

Bienvenue dans le Manuel de l'Utilisateur NXS-9700 !

Le NXS-9700 est une passerelle SMS matérielle avec un modem intégré et votre propre carte SIM, ce qui permet à vos messages d'être envoyés directement sur le réseau mobile depuis votre propre infrastructure, sans aucun fournisseur SMS tiers entre les deux.

Ce manuel est la référence complète pour l'appareil et s'applique à toutes les variantes NXS-9700 ; lorsque le comportement dépend du type de modem ou de la révision matérielle, la section concernée est marquée d'un badge. Si votre appareil est encore dans sa boîte, commencez par Contenu de la boîte puis exécutez l"Assistant de configuration. Sinon, utilisez la navigation de gauche ou la barre de recherche pour accéder directement au sujet dont vous avez besoin.

Les matériaux utilisés dans cette publication sont protégeables par le droit d'auteur et ne peuvent pas être dupliqués, copiés ou utilisés sans le consentement préalable du titulaire des droits d'auteur. Les spécifications techniques et les informations contenues dans ce document sont sujettes à modification sans avis préalable.

Informations sur la licence du logiciel SMSEagle

IMPORTANT – À LIRE AVANT TOUTE UTILISATION!

CONTRAT DE LICENCE UTILISATEUR FINAL DU LOGICIEL SMSEAGLE

Le présent Contrat de Licence Utilisateur Final (le « **Contrat** » ou la « **Licence** » ou le « **CLUF** ») sera considéré comme un accord juridiquement contraignant entre vous (une personne physique ou une entité, ci-après désigné « **Titulaire de la licence** » ou « **Vous** » ou « **Votre** ») et Proximus Sp. z o.o., ul. Piątkowska 163, Poznań, Pologne, code postal 60-650 (ci-après « **PROXIMUS** ») pour l'utilisation du logiciel préinstallé sur un appareil SMSEagle (c'est-à-dire le logiciel qui est installé et livré avec cet appareil), lequel peut inclure la documentation imprimée associée et tout autre composant et/ou module logiciel, y compris, mais sans s'y limiter, les pilotes requis (le « **Logiciel SMSEagle** »). D'autres aspects du Logiciel SMSEagle peuvent également inclure, sans s'y limiter, les mises à jour logicielles et toutes les mises à niveau que PROXIMUS pourrait vous fournir ou mettre à votre disposition, ou que vous obtenez après avoir acquis l'appareil SMSEagle, à condition que ces éléments ne soient pas accompagnés d'un contrat de licence distinct ou de conditions d'utilisation distinctes.

EN ACCEPTANT CES CONDITIONS DANS L'INTERFACE UTILISATEUR GRAPHIQUE (GUI) DE L'APPAREIL SMSEAGLE, EN UTILISANT L'APPAREIL SMSEAGLE, OU EN METTANT À JOUR OU EN METTANT À NIVEAU LE LOGICIEL SMSEAGLE, VOUS ACCEPTEZ D'ÊTRE LÉGALEMENT LIÉ PAR LES CONDITIONS DU PRÉSENT CONTRAT DE LICENCE. SI VOUS N'ACCEPTEZ PAS D'ÊTRE LIÉ PAR LES CONDITIONS DE CE CLUF, N'UTILISEZ PAS L'APPAREIL SMSEAGLE ET VOUS POUVEZ CHOISIR DE RETOURNER RAPIDEMENT L'APPAREIL POUR UN REMBOURSEMENT DE SON PRIX D'ACHAT EN CONTACTANT PROXIMUS À L'ADRESSE CI-DESSUS. La version actuelle de ce CLUF vous est mise à disposition avant l'achat sur www.smseagle.eu et est présentée dans l'interface GUI de l'appareil SMSEagle lors de la configuration initiale et après toute modification substantielle de ses conditions. Votre acceptation dans l'interface GUI (y compris la date, la version et l'identifiant de l'appareil) est enregistrée localement dans la base de données de l'appareil SMSEagle. Si vous n'acceptez pas les conditions dans l'interface GUI, le Logiciel SMSEagle ne sera pas activé pour utilisation.

LE LOGICIEL SMSEAGLE EST PROTÉGÉ PAR LES LOIS SUR LE DROIT D'AUTEUR, AINSI QUE PAR TOUTE AUTRE LOI PERTINENTE EN MATIÈRE DE PROPRIÉTÉ INTELLECTUELLE. LE LOGICIEL SMSEAGLE EST CONCÉDÉ SOUS LICENCE ET NON VENDU. TOUS LES DROITS, Y COMPRIS LES DROITS D'AUTEUR SUR LE LOGICIEL SMSEAGLE, DEMEURENT LA PROPRIÉTÉ EXCLUSIVE DE PROXIMUS. DE PLUS, COMME INDIQUÉ CI-DESSOUS, LE LOGICIEL SMSEAGLE INCLUT CERTAINS MODULES DÉVELOPPÉS PAR DES TIERS, QUI VOUS SONT SOUS-LICENCIÉS PAR LES PRÉSENTES SELON LES CONDITIONS AUTORISÉES PAR LE DÉVELOPPEUR.

Ce CLUF vous confère des droits légaux spécifiques, et vous pouvez également disposer d'autres droits légaux, qui varient d'une juridiction à l'autre. Les avertissements, exclusions et limitations de responsabilité prévus dans ce CLUF ne s'appliqueront que dans la mesure où la loi applicable ne l'interdit pas. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites ou l'exclusion ou la limitation des dommages accessoires ou consécutifs ou d'autres droits, auquel cas

ces dispositions du présent CLUF pourraient ne pas s'appliquer à vous. Toutefois, cela ne porte pas atteinte à l'applicabilité et à l'exécutabilité de toutes les autres dispositions du CLUF.

1. **DÉFINITIONS ET INTERPRÉTATIONS**
    1. « Contrat » ou « Licence » ou « CLUF » désigne le présent Contrat de Licence Utilisateur Final.
    2. « Titulaire de la licence » ou « Vous » ou « Votre » vous désigne, la personne physique ou l'entité commerciale acquérant un appareil SMSEagle sur lequel le Logiciel SMSEagle a été installé.
    3. « Propriété Intellectuelle » désigne les droits actuels et futurs à l'échelle mondiale en vertu du droit d'auteur, du droit des brevets, du droit des secrets commerciaux, du droit des marques, du droit moral et d'autres droits similaires.
    4. « Mise à jour » désigne la maintenance ou une correction d'une version du Logiciel SMSEagle, y compris, sans s'y limiter, un correctif urgent, un patch ou une amélioration, dont aucun ne fonctionne comme un service autonome ou un autre progiciel et qui n'entraînent pas de coût supplémentaire pour un Titulaire de licence existant.
    5. « Mise à niveau » désigne une version majeure et autonome du Logiciel SMSEagle, qui peut inclure des applications, fonctionnalités ou fonctions supplémentaires.
    6. Une référence à une « personne » inclut une personne physique, un organisme constitué en société ou non constitué en société (qu'il ait ou non une personnalité juridique distincte) et les représentants légaux et personnels de cette personne, ses successeurs et ayants droit autorisés.
    7. Les mots au singulier incluent le pluriel et vice versa.
    8. Une référence à une loi, une disposition légale ou une législation subordonnée est une référence à celle-ci telle qu'en vigueur à tout moment, en tenant compte de tout amendement ou de toute réadoption, et inclut toute loi, disposition légale ou législation subordonnée qu'elle modifie ou réadopte ; étant entendu que, entre les Parties, aucun tel amendement ou réadoption ne s'appliquera aux fins du présent Contrat dans la mesure où il imposerait une obligation, une responsabilité ou une restriction nouvelle ou étendue, ou affecterait autrement de manière défavorable les droits, de l'une quelconque des Parties.
    1. Une référence à un écrit ou à une communication écrite inclut le courrier électronique.
    2. Toute obligation dans ce Contrat imposant à une personne de ne pas faire quelque chose inclut l'obligation de ne pas accepter ou permettre que cette chose soit faite.
    3. Toute expression introduite par les termes « incluant », « inclure », « en particulier » ou toute expression similaire sera interprétée comme illustrative et ne limitera pas le sens des termes qui la précèdent.
    4. Les références aux articles, sections ou clauses renvoient aux articles, sections et clauses du présent Contrat.
    5. « Nous » et « Notre » désignent Proximus Sp. z o.o. (« PROXIMUS »).

6. Les « Parties » au présent Contrat sont Vous et Proximus Sp. z o.o. (« PROXIMUS »).
7. « Collecter » désigne la transmission de données hors de l'appareil d'une manière permettant à PROXIMUS ou à tout partenaire tiers d'y accéder.

2. **OCTROI DE LICENCE**
    1. PROXIMUS vous accorde une licence non exclusive pour l'utilisation du Logiciel SMSEagle sur l'appareil SMSEagle sur lequel il a été préinstallé, ainsi que pour l'installation des Mises à jour et des Mises à niveau, sous réserve des termes et conditions énoncés dans les présentes :

1. **Utilisation.** PROXIMUS vous accorde le droit d'utiliser une seule instance du Logiciel SMSEagle sur l'appareil SMSEagle que vous avez acquis. Toute utilisation sur un autre appareil ou ordinateur est interdite.
2. **Copie de sauvegarde.** Vous pouvez conserver une seule copie de la version actuelle du Logiciel SMSEagle pour votre appareil SMSEagle, dans la mesure où cela peut être nécessaire à des fins de sauvegarde.
    1. En outre, ce CLUF couvrira également toutes les Mises à jour et Mises à niveau logicielles fournies par PROXIMUS qui remplaceraient, écraseraient et/ou compléteraient la version originale installée du Logiciel SMSEagle, sauf si ces autres Mises à jour et Mises à niveau sont couvertes par une licence distincte, auquel cas les termes de cette licence prévaudront.

1. **PROPRIÉTÉ INTELLECTUELLE**
    1. **LOGICIEL SMSEAGLE PROTÉGÉ**. Le Logiciel SMSEagle est protégé par le droit d'auteur et d'autres lois et traités relatifs à la Propriété Intellectuelle.
    2. **RESTRICTIONS D'UTILISATION**. En tant que Titulaire de licence, Vous ne pouvez pas : (a) Utiliser le Logiciel SMSEagle sur plus d'un appareil à la fois, sans achat préalable d'appareils supplémentaires ; (b) Partager ou mettre à disposition de toute autre manière le Logiciel SMSEagle, de quelque façon que ce soit, à un tiers ; (c) Modifier, adapter, créer des œuvres dérivées ou traduire toute partie du Logiciel SMSEagle autre que ce qui peut être utilisé dans Votre appareil SMSEagle conformément à cette Licence ; (d) Faire de l'ingénierie inverse, décompiler ou désassembler le Logiciel SMSEagle, ni tenter de localiser ou d'obtenir son code source (sauf dans la mesure où de tels actes sont autorisés par les dispositions impératives du droit applicable, y compris l'Article 6 de la Directive 2009/24/CE relative à la décompilation aux fins d'interopérabilité avec d'autres programmes) ; (e) Tenter de modifier ou de supprimer toute marque, droit d'auteur ou autre mention de propriété contenue dans le Logiciel SMSEagle ; ou (f) Utiliser le Logiciel SMSEagle de toute manière non stipulée dans ce CLUF ou dans la documentation accompagnant l'appareil SMSEagle sur lequel il était préinstallé.
    3. **MISES À JOUR/MISES À NIVEAU**. PROXIMUS peut juger approprié de mettre à disposition des Mises à jour ou des Mises à niveau du Logiciel SMSEagle. Vous pouvez initier le processus d'installation de toute Mise à jour ou Mise à niveau, par exemple en cliquant sur un bouton « Check for software updates now » dans l'interface web de

l'appareil SMSEagle. Alternativement (lorsque l'appareil n'a pas d'accès Internet), Vous pouvez obtenir un package de Mise à jour ou de Mise à niveau auprès du support SMSEagle à l'adresse https://support.smseagle.eu, à installer ultérieurement sur l'appareil SMSEagle. Il appartiendra à la seule discrétion de PROXIMUS de conditionner la mise à disposition desdites Mises à jour ou Mises à niveau à Votre acceptation d'un autre CLUF ou à l'exécution d'un autre accord distinct. En décidant d'installer et d'utiliser ces Mises à jour ou Mises à niveau, Vous acceptez d'être soumis à toutes les licences, termes et conditions applicables de ce CLUF et/ou de tout autre accord. PROXIMUS s'engage à fournir des Mises à jour de sécurité pour le Logiciel SMSEagle pendant une période minimale de cinq (5) ans à compter de la date de première vente du modèle d'appareil SMSEagle concerné (la « Période de Mise à jour »). Après l'expiration de la Période de Mise à jour, PROXIMUS peut, à sa seule discrétion, continuer à fournir des Mises à jour ou des Mises à niveau, mais n'y sera pas obligé. PROXIMUS annoncera la date de Fin de vie de chaque modèle d'appareil SMSEagle sur son site web au plus tard douze (12) mois avant cette date. Cet engagement s'entend sans préjudice de toute période de support plus longue qui pourrait être exigée par des dispositions impératives du droit applicable, y compris le Cyber Resilience Act et la Directive NIS2.

2. **EXCLUSION DE GARANTIE**

PROXIMUS déploiera des efforts raisonnables conformes aux normes de développement logiciel en vigueur pour maintenir le Logiciel SMSEagle d'une manière qui minimise les erreurs et les interruptions.

TOUTEFOIS, PROXIMUS NE GARANTIT NI QUE L'UTILISATION DU LOGICIEL SMSEAGLE SERA ININTERROMPUE OU EXEMPTE D'ERREURS ; NI NE FAIT AUCUNE GARANTIE QUANT AUX RÉSULTATS QUI POURRAIENT ÊTRE OBTENUS DE L'UTILISATION DU LOGICIEL SMSEAGLE.

DANS TOUTE LA MESURE PERMISE PAR LE DROIT APPLICABLE, SAUF DISPOSITION EXPRESSE CONTRAIRE AUX PRÉSENTES ET NONOBSTANT TOUTE DISPOSITION CONTRAIRE, NI PROXIMUS NI AUCUN DE SES DIRIGEANTS, ADMINISTRATEURS, FILIALES, AFFILIÉS, REVENDEURS AGRÉÉS OU EMPLOYÉS NE DONNE AUCUNE AUTRE GARANTIE DE QUELQUE NATURE QUE CE SOIT, EXPRESSE, IMPLICITE, LÉGALE OU AUTRE, Y COMPRIS, MAIS SANS S'Y LIMITER, LES GARANTIES DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER ET DE NON-CONTREFAÇON.

1. **LIMITATION DE RESPONSABILITÉ**

    1. La responsabilité de PROXIMUS en lien avec toute réclamation causée par, liée à, ou résultant de l'utilisation du Logiciel SMSEagle, ou la somme de ces réclamations, ne dépassera jamais le coût de l'appareil SMSEagle au titre duquel le dommage est survenu, sauf si une telle limitation de responsabilité n'est pas autorisée en vertu du droit polonais applicable.
    2. PROXIMUS ne sera pas responsable envers le Titulaire de licence des pertes indirectes ou consécutives, y compris la perte de profits de toute nature et la perte de clients, de ventes, de marge, de production, d'image, de données ou de configuration, étant

précisé que l'exclusion ci-dessus ne s'applique pas aux dommages causés intentionnellement par PROXIMUS.

3. PROXIMUS ne sera pas responsable, en particulier, de : (i) la perte de données ou de configuration ; (ii) la perte de profits du Titulaire de licence ; (iii) les dommages indirects ou consécutifs ; (iv) les actions de tiers.
4. En ce qui concerne la responsabilité de PROXIMUS pour toute réclamation de l'utilisateur final, la responsabilité de PROXIMUS est limitée uniquement aux situations où le dommage résulte d'une action ou d'une omission directe de PROXIMUS, et uniquement au coût de l'appareil SMSEagle au titre duquel le dommage est survenu, sauf si une telle limitation de responsabilité n'est pas autorisée en vertu du droit polonais applicable.
5. Les dispositions de cette section ne s'appliquent pas aux Titulaires de licence qui sont des consommateurs ou des entrepreneurs individuels au sens du droit polonais, dans la mesure où les limitations prévues ici sont interdites par des dispositions impératives de protection des consommateurs.

2. **OPEN SOURCE**

Certains modules logiciels du Logiciel PROXIMUS sont soumis à des licences « open source » ou de « logiciel libre » (« Logiciel Open Source »). Une partie du Logiciel Open Source appartient à des tiers. Ce Logiciel Open Source n'est pas soumis aux termes et conditions du présent Accord. Au lieu de cela, chaque élément de Logiciel Open Source est licencié selon les termes de la licence utilisateur final qui l'accompagne. Rien dans le présent Accord ne limite Vos droits, ni ne Vous accorde des droits qui l'emporteraient sur les termes et conditions de toute licence utilisateur final applicable au Logiciel Open Source. Les licences Open Source applicables incluent : la Licence MIT ; la GNU General Public License v. 2.0 ; la GNU Lesser General Public License v. 2.1 ; la Licence BSD-3 Clause ; la Licence Apache 2.0. Si une licence particulière de Logiciel Open Source l'exige, PROXIMUS met à disposition ce Logiciel Open Source, ainsi que Nos modifications apportées à celui-ci, sur demande écrite adressée à Nous à l'adresse e-mail ou postale.

1. **UTILISATEURS FINAUX DU GOUVERNEMENT DES ÉTATS-UNIS**

Le Logiciel SMSEagle est concédé sous licence au Gouvernement des États-Unis avec DROITS RESTREINTS. L'utilisation, la duplication ou la divulgation par le Gouvernement des États-Unis seront soumises aux restrictions conformément à la clause DFARS 252.227-7013 relative aux Données techniques et Logiciels informatiques, et à la clause 48 CFR 52.227-19 relative aux Logiciels informatiques commerciaux, selon le cas.

1. **CONFIDENTIALITÉ DES DONNÉES**

1. **DÉCLARATION DE COLLECTE DE DONNÉES**. PROXIMUS ne collecte AUCUNE donnée avec laquelle Vous travaillez lorsque Vous utilisez l'appareil SMSEagle. Nous ne pouvons voir ni collecter aucune donnée enregistrée sur l'appareil SMSEagle, car nous n'avons aucun accès à Votre appareil. Toutefois, dans le cadre de la fourniture du Logiciel SMSEagle et du support associé, PROXIMUS peut traiter certaines données personnelles du Titulaire de licence (ou, lorsque le Titulaire de licence est une entité,

de ses représentants autorisés et utilisateurs finaux). Les informations suivantes sont fournies conformément à l'Article 13 du Règlement (UE) 2016/679 (RGPD) :

2. Responsable du traitement : Proximus Sp. z o.o., ul. Piątkowska 163, 60-650 Poznań, Pologne ; E-mail : odo@smseagle.eu.
3. Catégories de données personnelles traitées : (a) données d'enregistrement et de licence (nom de l'entreprise, personne de contact, e-mail, numéro de série de l'appareil) ; (b) télémétrie de Mise à jour/Mise à niveau strictement limitée à la version du logiciel, au modèle d'appareil, au numéro de série de l'appareil, à l'adresse IP, le cas échéant. Les données personnelles traitées dans le cadre de la fourniture du support technique sont régies par une Politique de Services de Support Technique distincte, disponible sur le site web de Proximus : www.smseagle.eu.
4. Finalités et bases légales du traitement : (a) exécution du présent CLUF et fourniture des Mises à jour et Mises à niveau - Article 6(1)(b) RGPD ; (b) respect des obligations légales (fiscales, comptables) - Article 6(1)(c) RGPD ; (c) intérêts légitimes de PROXIMUS visant à améliorer le Logiciel SMSEagle et à se défendre contre d'éventuelles réclamations - Article 6(1)(f) RGPD.
5. Destinataires des données personnelles : employés et sous-traitants autorisés de PROXIMUS tenus à la confidentialité, fournisseurs de services informatiques (hébergement, e-mail, gestion des tickets) agissant en tant que sous-traitants au sens de l'Article 28 du RGPD, et autorités publiques compétentes lorsque la loi l'exige.
6. Transferts vers des pays tiers : les données personnelles sont traitées principalement au sein de l'Espace économique européen. Lorsque des transferts vers des pays tiers ont lieu (par exemple, l'utilisation de certains fournisseurs informatiques), ils s'effectuent sur la base d'une décision d'adéquation ou de garanties appropriées telles que les Clauses Contractuelles Types de l'UE.
7. Durée de conservation : données d'enregistrement et de licence – pendant la durée du présent CLUF et pendant la période requise par le droit applicable (notamment le droit fiscal et comptable, généralement 5 ans) ; données traitées sur la base d'intérêts légitimes – jusqu'à ce qu'une objection effective soit soulevée ou que l'intérêt légitime cesse.
8. Droits des personnes concernées : le Titulaire de licence a le droit d'accéder à ses données personnelles, de les rectifier, de les effacer, d'en limiter le traitement et d'en obtenir la portabilité, ainsi que le droit de s'opposer au traitement fondé sur des intérêts légitimes.
9. Droit d'introduire une réclamation : le Titulaire de licence a le droit d'introduire une réclamation auprès du Président de l'Office de Protection des Données Personnelles (Prezes Urzędu Ochrony Danych Osobowych), ul. Stawki 2, 00-193 Varsovie, Pologne.
10. Prise de décision automatisée : PROXIMUS ne procède à aucune prise de décision automatisée, y compris de profilage, au sens de l'Article 22 du RGPD, en lien avec le présent CLUF.
11. La fourniture de données personnelles est volontaire mais nécessaire à la conclusion et à l'exécution du présent CLUF ainsi qu'à la fourniture des services de support. De

plus amples détails, y compris toute mise à jour de ces informations, sont disponibles dans la Politique de Confidentialité à l'adresse https://www.smseagle.eu/privacy-policy/.

2. **RÉSILIATION**

    1. PROXIMUS se réserve le droit de résilier ce CLUF avec effet immédiat en cas de : (i) violation substantielle par le Titulaire de licence des restrictions de licence énoncées dans la section « Restrictions d'utilisation » ; (ii) reproduction, distribution ou modification non autorisée du Logiciel SMSEagle ; ou (iii) contournement ou altération de toute mesure de protection technique.
    2. PROXIMUS et un Titulaire de licence ayant acquis l'appareil SMSEagle directement auprès de PROXIMUS peuvent résilier ce CLUF avec un préavis écrit d'au moins trente (30) jours.
    3. Sous réserve des lois impératives sur la protection des consommateurs, si PROXIMUS résilie ce CLUF pour les raisons énumérées à la section 9.01. ci-dessus, le Titulaire de licence n'aura droit à aucun remboursement du prix d'achat de l'appareil SMSEagle ni des frais payés en lien avec le Logiciel SMSEagle.
    4. Dès la résiliation de ce CLUF, le Titulaire de licence doit cesser toute utilisation du Logiciel SMSEagle et rendre inutilisables toutes les copies de sauvegarde qu'il détient. Les sections « Propriété intellectuelle », « Exclusion de garantie », « Limitation de responsabilité et recours », « Confidentialité des données », « Droit applicable » et « Règlement des litiges » demeureront en vigueur après la résiliation.
    5. Si le Titulaire de licence a acheté l'appareil SMSEagle auprès d'un revendeur ou d'un partenaire agréé, les règles relatives aux retours, annulations et remboursements de l'appareil SMSEagle sont précisées sur la facture ou dans toute autre documentation commerciale fournie par ce revendeur ou partenaire agréé.
    6. Ce CLUF est fourni indépendamment de toute garantie matérielle applicable à l'appareil SMSEagle. L'expiration ou la résiliation de ce CLUF n'affecte pas la validité ni la durée de la garantie matérielle attachée à l'appareil SMSEagle, et les termes de cette garantie matérielle ne limitent pas les droits du Titulaire de licence en vertu du présent CLUF.

3. **DISPOSITIONS DIVERSES**

    1. **SUCCESSEURS ET AYANTS DROIT**. Le présent CLUF, dans son intégralité, engagera juridiquement et bénéficiera à PROXIMUS et à Vous-même, ainsi qu'à nos successeurs et ayants droit respectifs autorisés.
    2. **DIVISIBILITÉ**. Si une disposition du présent Contrat est jugée illégale, invalide ou inapplicable par un tribunal compétent, les autres dispositions n'en seront pas affectées.
    3. **RENONCIATION**. Le fait de renoncer à faire valoir une violation ou de ne pas appliquer l'une des dispositions contenues dans le présent document ne saurait être interprété comme une renonciation future à ces conditions ni comme une renonciation à toute autre disposition du présent CLUF.

4. **MODIFICATIONS**. Toute renonciation, tout complément, toute modification ou tout amendement apporté à une disposition du présent CLUF ne sera valable que s'il est effectué par écrit et signé par PROXIMUS.
5. **DROIT APPLICABLE**. Pour les questions non réglées par le présent document, les dispositions du Code civil polonais s'appliquent, ainsi que les dispositions de la loi polonaise sur le droit d'auteur du 4 février 1994 (Journal officiel 1994, n° 24, point 83). Le présent Contrat est régi à tous égards par les lois de la République de Pologne.
6. **RÈGLEMENT DES LITIGES**. Tout litige découlant du présent Contrat ou en lien avec celui-ci sera soumis à la compétence exclusive des tribunaux de droit commun compétents pour le siège social de PROXIMUS à Poznań, en Pologne. Cette disposition ne s'applique pas aux Titulaires de licence qui sont des consommateurs ou des entrepreneurs individuels au sens du droit polonais, qui conservent le droit d'engager une procédure devant le tribunal compétent en vertu des dispositions légales impératives applicables.
7. **CESSIONS**. Vous avez le droit de transférer le Logiciel SMSEagle à un tiers uniquement conjointement avec le transfert définitif de la propriété de l'appareil SMSEagle sur lequel il était préinstallé. Dans ce cas, le cessionnaire est tenu d'accepter le présent CLUF dans sa forme actuelle avant toute utilisation du Logiciel SMSEagle, et Vous devez rendre inutilisables toutes les copies de sauvegarde ou autres copies du Logiciel SMSEagle que Vous détenez au moment du transfert. Cette disposition ne porte pas atteinte à la doctrine de l'épuisement des droits en vertu de l'article 4(2) de la Directive 2009/24/CE ni à tout droit impératif du Titulaire de licence en vertu du droit de l'UE.
8. **VALIDITÉ ET CARACTÈRE OBLIGATOIRE**. Le présent Contrat constitue une obligation valable et juridiquement contraignante pour les Parties, opposable à celles-ci conformément à ses termes, sous réserve, à tous égards, des effets de la faillite, de l'insolvabilité, de la fraude, de la réorganisation, du moratoire et des autres lois relatives ou affectant de manière générale les droits des créanciers, ainsi que des principes généraux d'équité.
9. **EFFET DU TITRE ET DES INTITULÉS**. Le titre du Contrat ainsi que les intitulés des Sections et des Clauses sont inclus par souci de commodité et n'affectent en rien le sens du Contrat ou de la Section concernée.
10. **FORCE MAJEURE**. Sauf en ce qui concerne les obligations de paiement, si l'une des Parties est empêchée d'exécuter ou est incapable d'exécuter l'une de ses obligations en vertu du présent Contrat en raison de causes échappant au contrôle raisonnable de la Partie invoquant cette disposition, y compris, mais sans s'y limiter, les catastrophes naturelles, les actes des autorités civiles ou militaires, les émeutes ou la désobéissance civile, les guerres, les grèves ou les conflits du travail (chacun constituant un « **Cas de Force Majeure** »), l'exécution par cette Partie sera excusée et le délai d'exécution sera prolongé en conséquence, à condition que la Partie prenne rapidement toutes les mesures raisonnablement nécessaires pour reprendre l'exécution complète.

4. **PROTECTION DES CONSOMMATEURS ET DES TRAVAILLEURS INDEPENDANTS**

Les dispositions du présent CLUF ne portent pas préjudice aux dispositions relatives à la protection des consommateurs et à la protection des travailleurs indépendants si Vous êtes une personne physique qui achète l'appareil et concluez ce CLUF sans lien direct avec son activité commerciale ou professionnelle ou dans le cas d'un travailleur indépendant personne physique – sans lien direct avec son activité professionnelle (appliqué au CLUF conclu à partir du 1er janvier 2021). Si une disposition du présent CLUF est incompatible avec les lois obligatoires de protection des consommateurs ou des travailleurs indépendants, la disposition n'engage pas le consommateur/le travailleur indépendant et la disposition de la loi d'application commune la plus proche de cette disposition s'appliquera.

1. **COORDONNÉES**

Si vous avez des questions concernant ce CLUF, veuillez contacter PROXIMUS à :

Proximus Sp. z o.o.
Ul. Piątkowska 163
60-650 Poznań
Poland | Europe
tel. + 48 61 6713 413
https://www.smseagle.eu

Contenu de la boîte



SMSEagle déballé

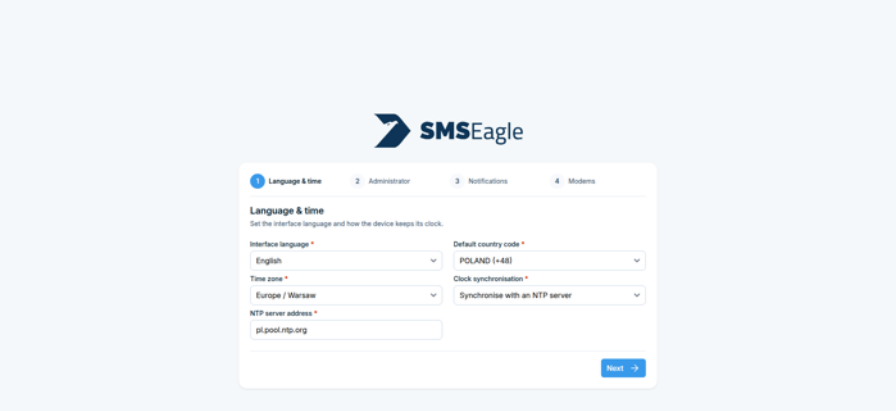
Votre boîte SMSEagle contient :

- Passerelle SMS matérielle SMSEagle
- Antenne omnidirectionnelle externe (avec pied magnétique) NXS-9700-3G NXS-9700-4G

- 2x Antennes MIMO externes (avec pied magnétique/adhésif) NXS-9700-5G
- Alimentation AC/DC (tension d'entrée : 100-240V)
- Guide de démarrage rapide
- Carte de garantie

Assistant de configuration

Lors de votre première connexion à un appareil SMSEagle fraîchement configuré, un assistant de configuration vous guide à travers les paramètres nécessaires avant que la passerelle ne soit active. L'assistant comporte quatre étapes ; vous ne pouvez pas accéder au reste de l'interface Web tant qu'il n'est pas terminé.

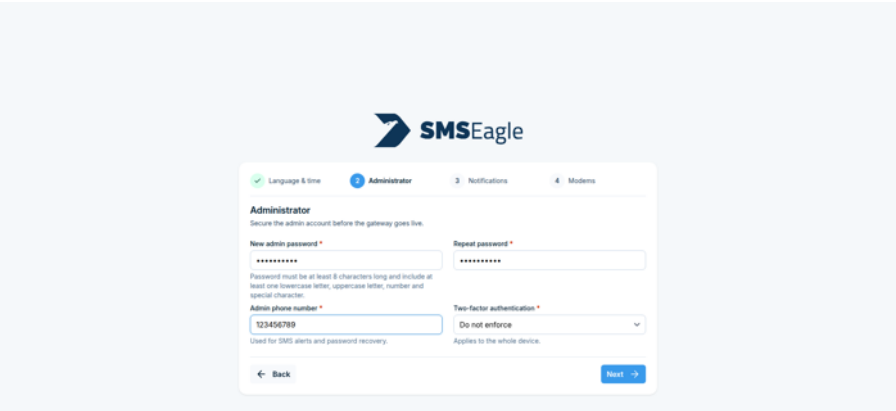


Étape 1 : Langue et heure

Étape 1 : Langue et heure

Définissez la langue de l'interface, le code pays par défaut (utilisé lorsqu'un numéro de téléphone est entré sans celui-ci), le fuseau horaire de l'appareil et la synchronisation de l'horloge. Si vous choisissez **Synchroniser avec un serveur NTP**, entrez également l'"**adresse du serveur NTP**.

Étape 2 : Compte administrateur



Étape 2 : Compte administrateur

Sécurisez le compte administrateur avant que la passerelle ne soit active :

Champ	Description
Nouveau mot de passe administrateur / Répéter le mot de passe	Doit contenir au moins 8 caractères et inclure une lettre minuscule, une lettre majuscule, un chiffre et un caractère spécial
Numéro de téléphone administrateur	Utilisé pour les alertes SMS et la récupération de mot de passe
Authentification multifacteur	Ne pas appliquer, Appliquer à tous les utilisateurs, ou Appliquer aux nouveaux utilisateurs - s'applique à tout l'appareil, voir Authentification multifacteur (MFA)

La modification du mot de passe administrateur ici vous déconnecte ; reconnectez-vous avec le nouveau mot de passe pour continuer l'assistant.

Étape 3 : Notifications

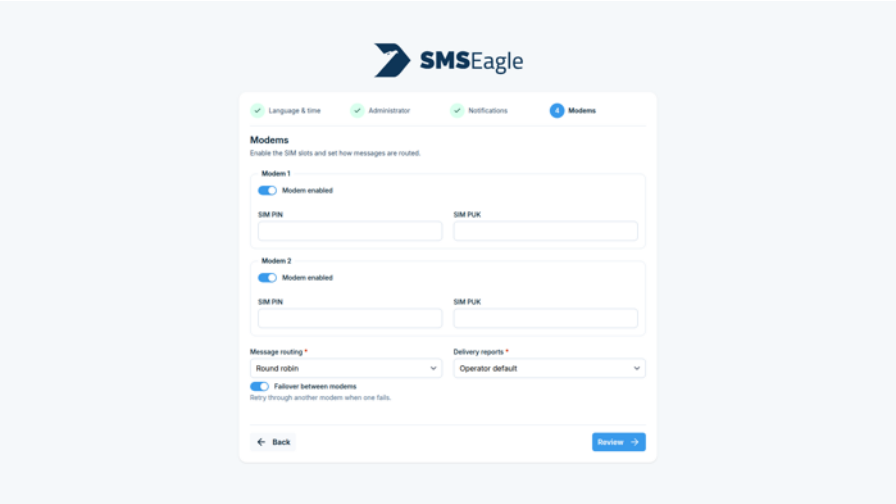


Étape 3 : Notifications

Choisissez ce que l'appareil doit vous communiquer :

- Vérifier automatiquement les mises à jour logicielles et, éventuellement, notifier l'administrateur par SMS lorsqu'une nouvelle version est disponible
- Vérifier automatiquement la validité du support et, éventuellement, notifier l'administrateur par SMS lorsque le support est sur le point d'expirer

Étape 4 : Modems



Étape 4 : Modems

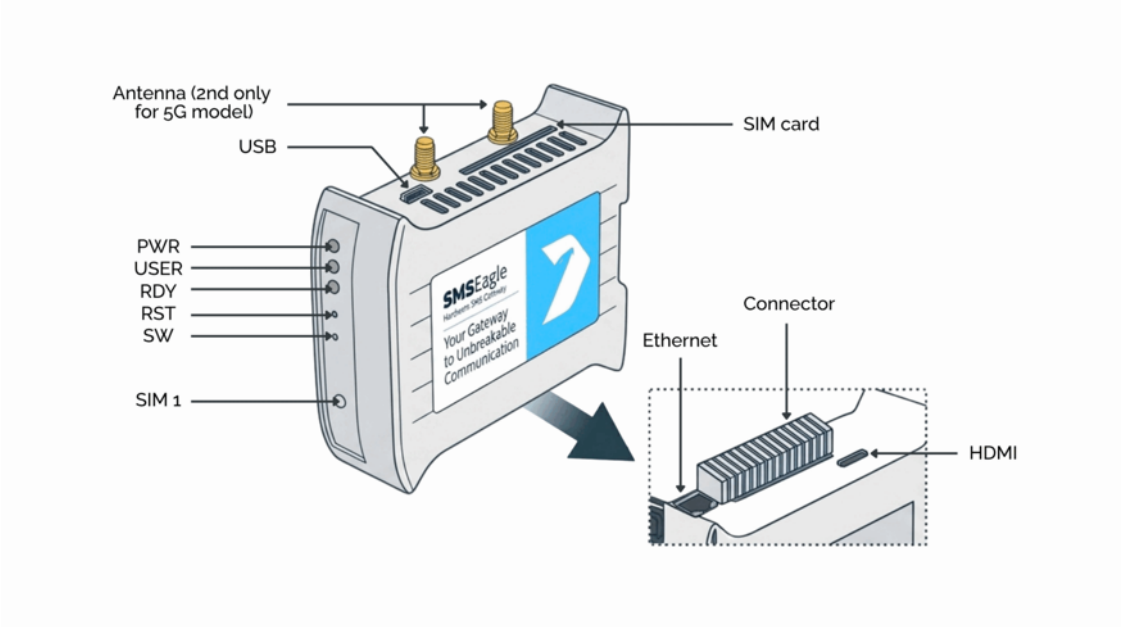
Pour le modem intégré, activez-le et, si nécessaire, entrez son **PIN SIM** et **PUK SIM**. Définissez ensuite :

- **Rapports de livraison** - Valeur par défaut de l'opérateur, Toujours demander, ou Ne jamais demander

Le NXS-9700 est livré avec un seul modem intégré, donc le routage des messages entre modems et les paramètres de basculement (disponibles sur les produits SMSEagle multi-modems) ne s'appliquent pas ici.

Vérifiez vos paramètres et terminez l'assistant pour accéder au tableau de bord normal.

Connecteurs, ports et LED



Connecteurs, ports et LED

Élément	Étiquette	Description
VCC Rev.3 Rev.4	VCC	Connecteur d'alimentation
Connecteur à 12 pôles	–	4x entrées numériques, 4x sorties numériques, 1× 1Wire, 1× 5V, 2x GND
Emplacement pour carte SIM	SIM	Emplacement pour carte SIM
Port HDMI	HDMI	Port HDMI (à des fins de débogage uniquement)
Port USB	USB	Port USB (à des fins de débogage uniquement)
Port Ethernet	ETH	Port Ethernet RJ45
Antenne	ANT	Prise d'antenne Deuxième prise, pour MIMO NXS-9700-5G
LED d'alimentation	PWR	LED indiquant la mise sous tension
User LED	USER	LED pour un usage applicatif utilisateur
LEDs SIM1,2	Modem 1,2 (optionnel)	Indicateur LED de l'état du modem
Ready LED	RDY	Indication LED de l'état de l'appareil
Reset	RST	Bouton pour redémarrer l'appareil
User Switch	SW	Bouton pour restaurer les paramètres d'usine

Aperçu de l'interface Web

Ce chapitre propose un tour rapide de l'interface Web de SMSEagle elle-même, avant les fonctionnalités individuelles couvertes dans le reste de ce manuel.

Connexion

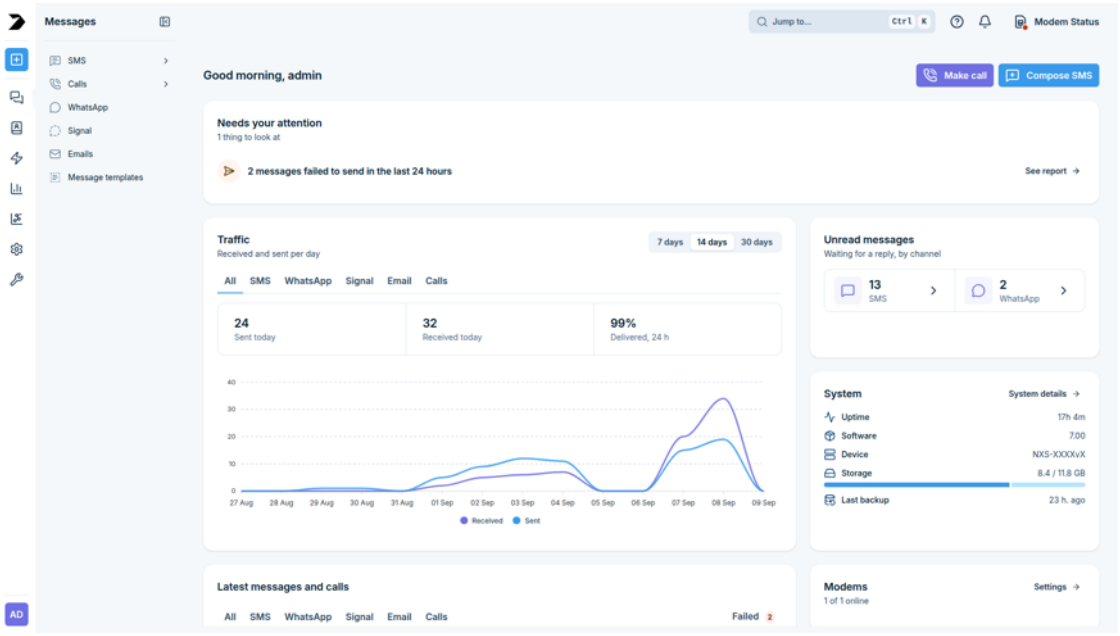


La page de connexion

Ouvrez l'adresse IP ou le nom d'hôte du dispositif dans un navigateur et connectez-vous avec vos identifiants. Si l'authentification multifacteur a été appliquée au niveau du dispositif (voir MFA), on vous demandera également un code à usage unique.

- **Authentication type** décide où les identifiants sont vérifiés : **Local (par défaut)** par rapport à la liste des utilisateurs du dispositif, ou **LDAP** par rapport à un serveur d'annuaire, qu'un administrateur configure d'abord sous LDAP.
- **Forgot password?** envoie les instructions de récupération au numéro de téléphone du compte par SMS. Identifiez-vous avec votre nom d'utilisateur ou ce numéro de téléphone.
- Le sélecteur en bas à droite définit la langue de la page de connexion. La langue de l'interface après connexion provient de votre propre compte, voir Personal account settings.

Disposition de l’interface

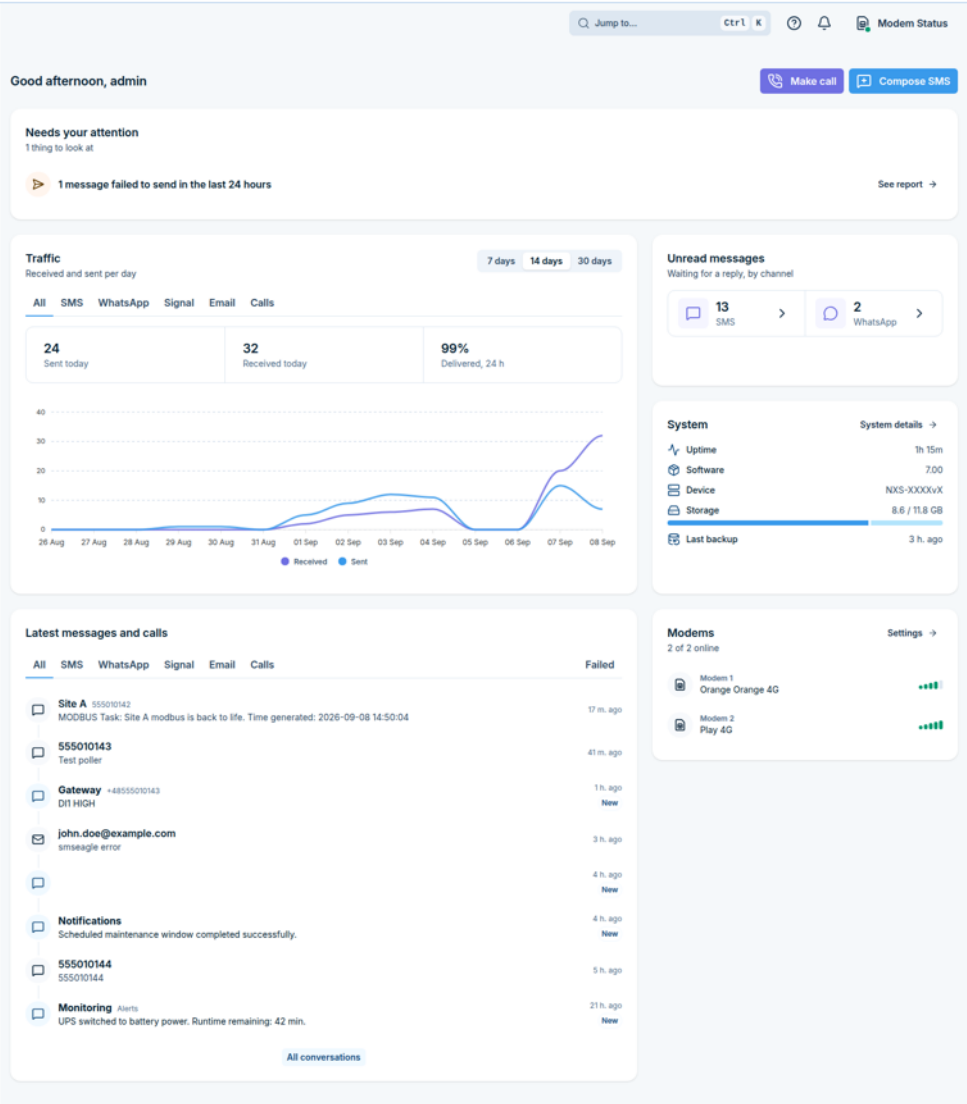


Navigation de gauche développée au-dessus de la zone de contenu principal, avec la barre supérieure au-dessus

- **Left navigation** - une barre d’icônes donnant accès à Messages, Phonebook, Automation, Reports, Monitoring, Settings et System. Survoler une icône nomme la section ; cliquer dessus développe un panneau listant les pages de cette section par nom, comme **Messages** ci-dessus. Le bouton dans l’en-tête du panneau le ferme à nouveau.
- **Top bar** - la recherche **Jump to...** (`Ctrl K`) vous permet d’accéder directement à n’importe quelle page par son nom au lieu de naviguer dans le menu ; elle affiche également les notifications, l’aide et l’indicateur d’état du modem.
- **Main content area** - la page de la section actuellement sélectionnée.

Tableau de bord

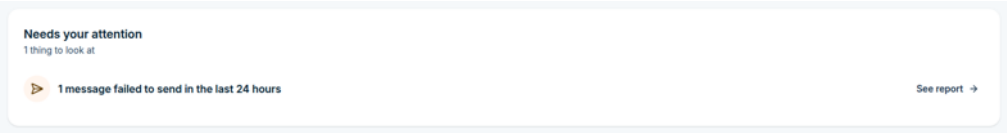
Le Tableau de bord est la page d’accueil après connexion. Il s’ouvre avec un message de bienvenue et les boutons d’action rapide, suivi de cartes résumant ce qui nécessite une intervention, le trafic des messages, les conversations sans réponse, la santé du dispositif, l’activité récente et l’état des modems.



Le Tableau de bord

Needs your attention

Collecte les éléments nécessitant une intervention immédiate, avec le nombre d'entre eux sous le titre de la carte et combien d'entre eux sont critiques. Chaque entrée renvoie à la page où vous pouvez le gérer, donc un message bloqué dans la boîte d'envoi renvoie au dossier de la boîte d'envoi, et une entrée de non-livraison renvoie à Reports & Statistics.



Needs your attention

Traffic

Messages reçus et envoyés par jour. Les onglets limitent la carte à un seul canal (SMS, WhatsApp, Signal, Email ou Calls), et les boutons **7 days** / **14 days** / **30 days** définissent la plage du graphique ci-dessous. Trois compteurs se trouvent au-dessus du graphique :

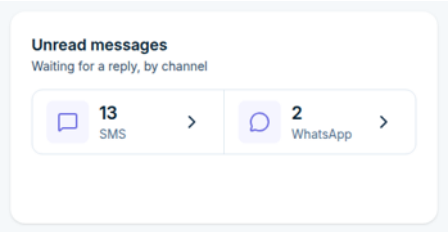
- **Sent today** - messages envoyés depuis minuit
- **Received today** - messages reçus depuis minuit
- **Delivered, 24 h** - part des messages envoyés au cours des dernières 24 heures qui ont été confirmés comme livrés



Traffic

Unread messages

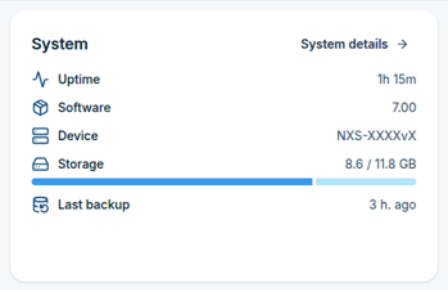
Conversations en attente d'une réponse, comptabilisées par canal. Chaque tuile ouvre la liste de conversations de ce canal, voir Messages.



Unread messages

Système

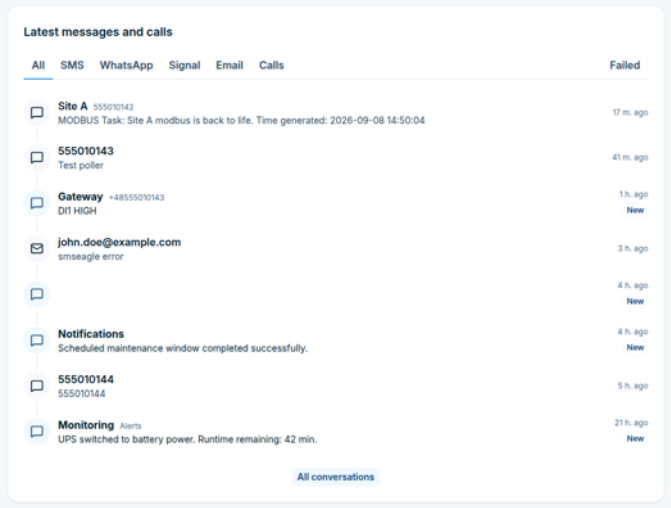
État du système en un coup d'œil : temps de fonctionnement, version du logiciel, type d'appareil, stockage utilisé sur le total, et date de la dernière sauvegarde. **Détails système** ouvre la section Système.



Système

Derniers messages et appels

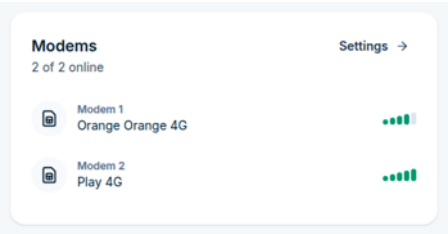
Le trafic le plus récent sur tous les canaux, les plus récents en premier, avec l’expéditeur, le début du message et son heure d’arrivée. Les onglets limitent la liste à un canal, et **Échoué** affiche ce qui n’a pas été envoyé. Tout message non lu est marqué **Nouveau**. **Toutes les conversations** ouvre la liste complète dans Messages.



Derniers messages et appels

Modems

Nombre de modems en ligne sur ceux installés, et pour chacun le réseau auquel il est enregistré, la technologie radio et la puissance du signal. **Settings** ouvre la configuration des modems, voir Settings.



Modems

Actions rapides

Deux boutons dans le coin supérieur droit du Tableau de bord.



Actions rapides

Tous deux ouvrent le même dialogue **Compose**, sur un onglet différent :

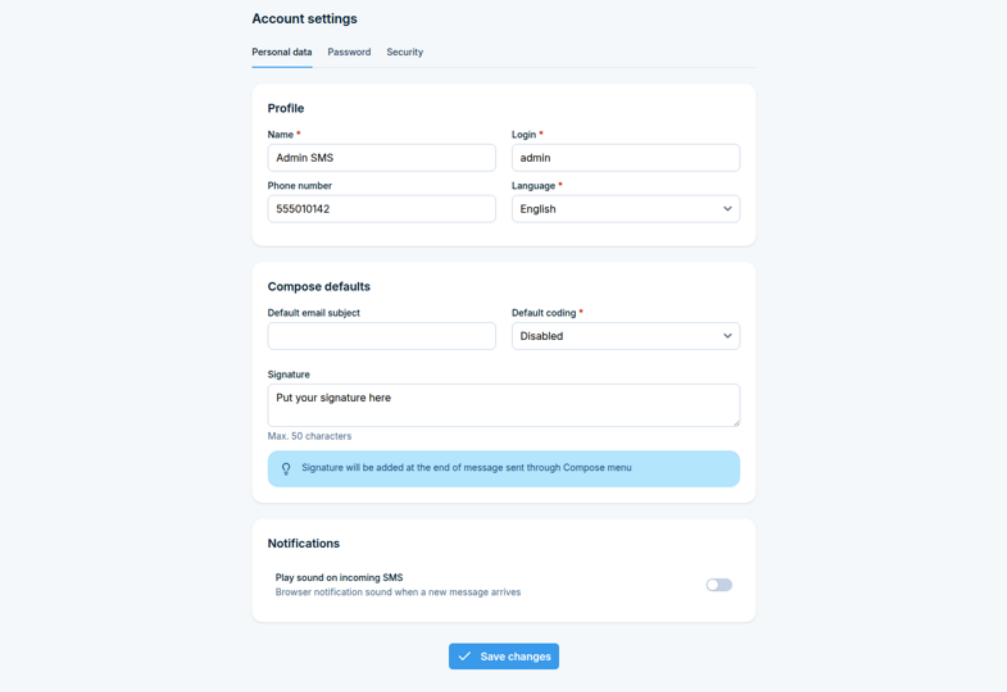
- **Composer SMS** l'ouvre sur l'onglet **Message** - choisissez le type de message (SMS, Flash SMS, MMS, Code USSD, Signal, WhatsApp, Courrier), les destinataires (depuis le Carnet d'adresses, saisis manuellement ou à partir d'un fichier CSV), la date d'envoi et le message lui-même. Un modèle enregistré peut être utilisé à la place de taper le texte, voir Messages.
- **Passer un appel** l'ouvre sur l'onglet **Appel** - choisissez le type d'appel (sonnerie uniquement, synthèse vocale, un fichier audio), les destinataires et la date de l'appel, voir Messages.

Un canal qui n'est pas configuré sur cet appareil est grisé dans la liste des types de messages.

Paramètres du compte personnel

Cliquez sur votre avatar (bas-gauche) et choisissez **Paramètres du compte** pour gérer votre propre compte, sous trois onglets.

Données personnelles

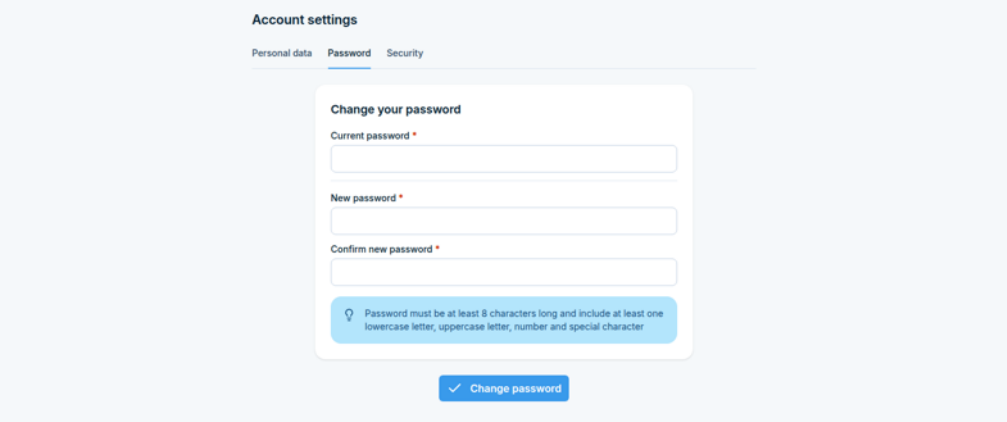


Paramètres du compte > Données personnelles

- **Profil** - nom, identifiant de connexion, numéro de téléphone et langue de l'interface pour votre propre compte
- **Paramètres par défaut de composition** - l'objet du courrier par défaut, le codage SMS par défaut et une signature de jusqu'à 50 caractères, ajoutée aux messages envoyés depuis Compose
- **Notifications** - si le navigateur joue un son à l'arrivée d'un nouveau message

Enregistrer les modifications applique l'onglet entier à la fois.

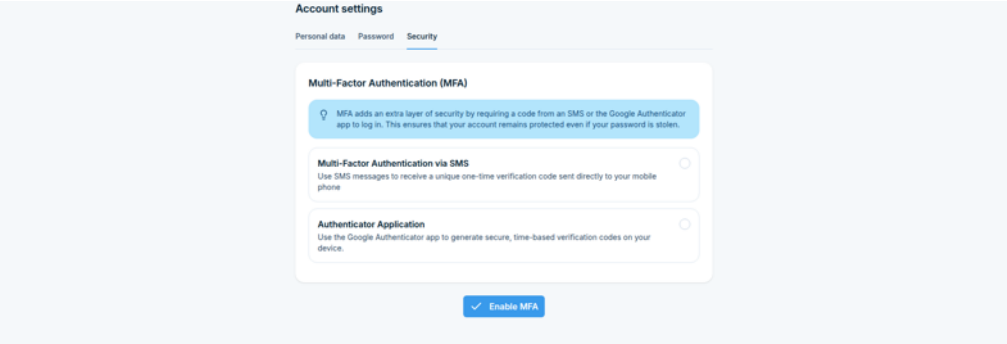
Mot de passe



Paramètres du compte > Mot de passe

Modifiez votre propre mot de passe en entrant le mot de passe actuel et le nouveau deux fois. Le nouveau mot de passe doit être long d’au moins 8 caractères et contenir une lettre minuscule, une lettre majuscule, un chiffre et un caractère spécial.

Sécurité



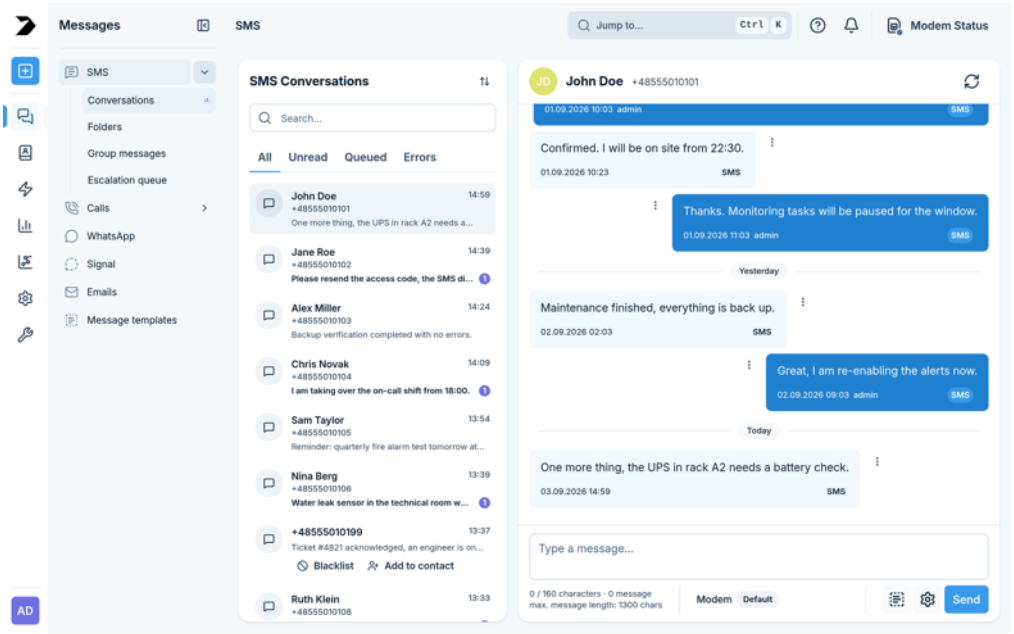
Paramètres de compte > Sécurité

Configurez votre propre authentification multifacteur, soit par SMS soit avec une application authenticator. La procédure complète, y compris l’activation obligatoire de MFA au niveau du dispositif, se trouve dans MFA.

Messages

Ce chapitre couvre la section **Messages** de l'interface web - où vous lisez, composez et gérez les conversations de chaque canal. La configuration d'un canal (activer WhatsApp, connecter SMTP, configurer des modems) est couverte séparément dans Paramètres ; ce chapitre concerne l'utilisation quotidienne d'un canal.

SMS (Conversations)

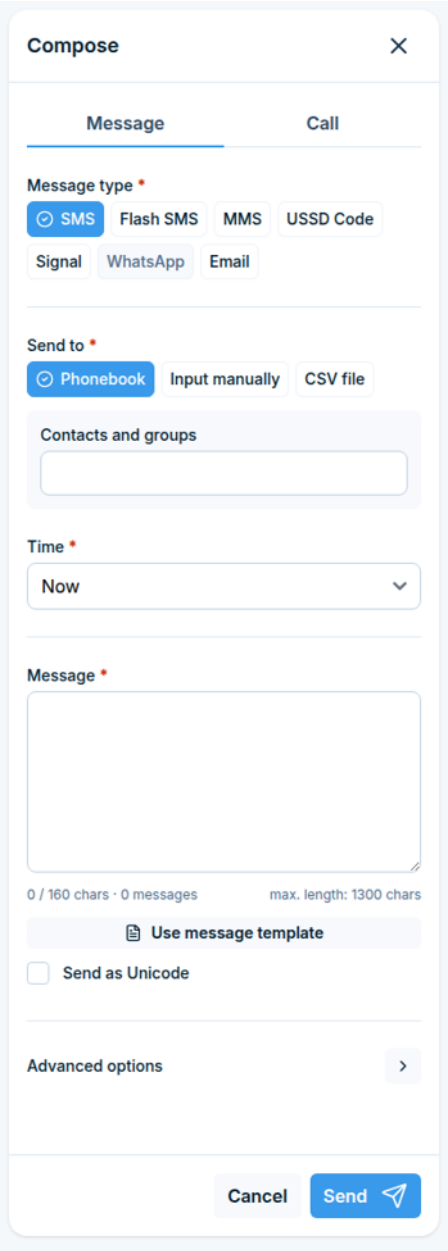


SMS Conversations, avec un fil ouvert

Messages > SMS > Conversations (`/messages/sms/`) est la boîte de réception SMS/MMS principale : un fil par numéro de téléphone, les plus récents en premier.

- Filtrez avec les onglets **All**, **Unread**, **Queued** et **Errors**.
- Ouvrez un fil pour lire l'historique complet et répondre à partir de la boîte en bas.
- Les pièces jointes MMS (images, fichiers) apparaissent en ligne dans le fil une fois qu'un modem a MMS configuré - voir MMS dans Paramètres.
- Composez un nouveau message avec le bouton **+** en haut du rail gauche, ou l'action rapide **Compose** sur le Tableau de bord.

Composition d'un message



Le dialogue Compose

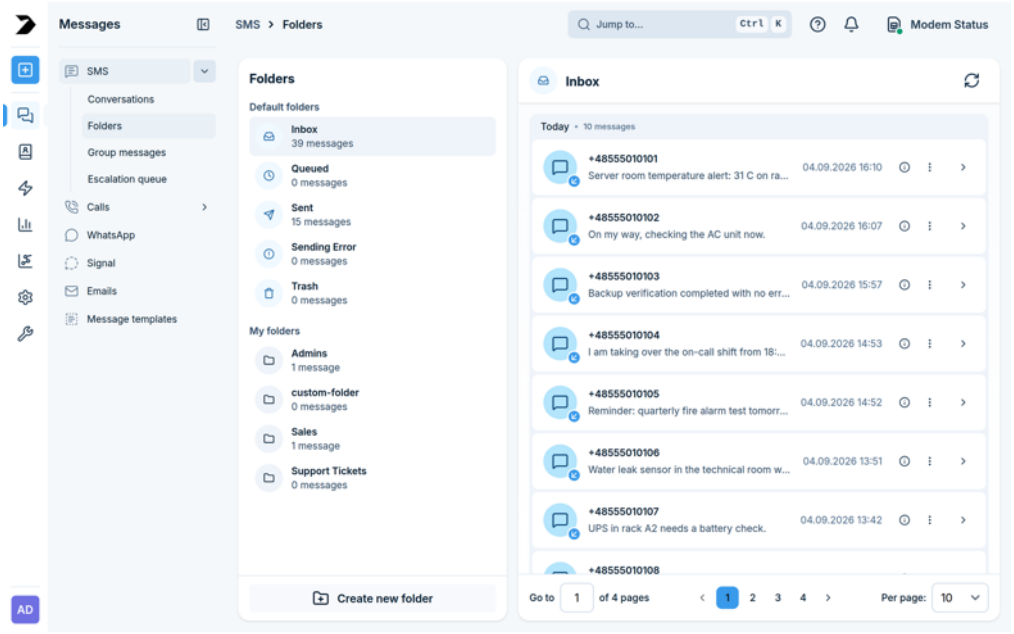
Compose s'ouvre comme un panneau sur la droite, avec un onglet **Message** et un onglet **Call**. L'onglet Message contient :

- **Message type** - SMS, Flash SMS, MMS, USSD Code, Signal, WhatsApp ou Email. Un canal non configuré sur cet appareil est grisé, voir Paramètres.
- **Send to** - choisissez les destinataires dans le **Phonebook** (contacts et groupes), entrez-les avec **Input manually**, ou téléchargez un fichier **CSV**.
- **Time** - envoyer **Now**, **At date and time**, **After delay** ou **Between hours**.
- **Message** - le texte, avec un compteur en direct des caractères et du nombre de parties SMS qu'ils représentent. **Use message template** le remplit à partir d'un modèle enregistré, et **Send as Unicode** change l'encodage pour les caractères non-GSM.

- **Advanced options** - paramètres supplémentaires par message.

Send met le message en file d'attente ; le fil apparaît immédiatement dans Conversations.

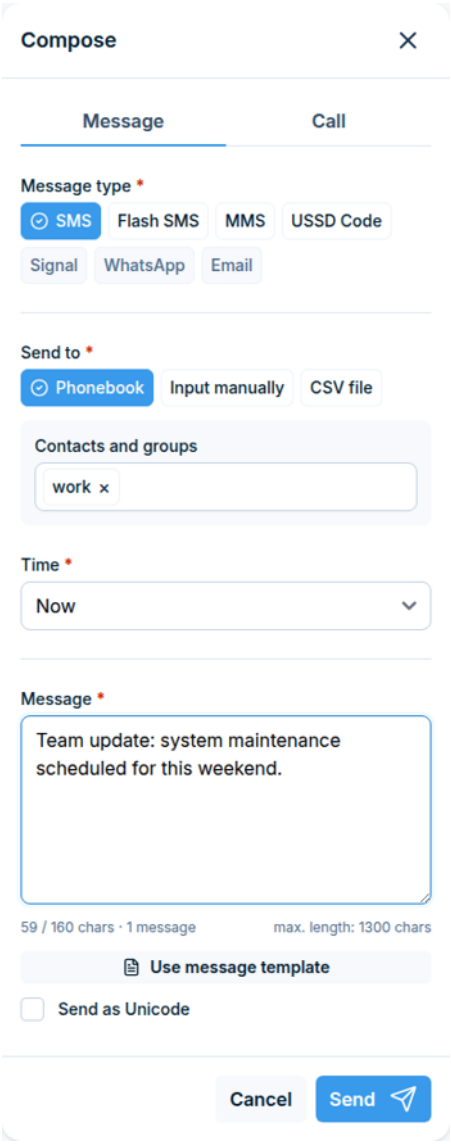
Dossiers



Dossiers

Messages > SMS > Folders (`/messages/sms/folders/`) liste les dossiers par défaut (Inbox, Queued, Sent, Sending Error, Trash) aux côtés de tout dossier personnalisé que vous avez créé sous **My folders**. Chaque dossier affiche le nombre de messages qu'il contient. Cliquez sur **Create new folder** pour ajouter le vôtre - utile avec les Inbox Rules pour trier automatiquement les messages entrants, et Cleanup Folders pour les élaguer automatiquement.

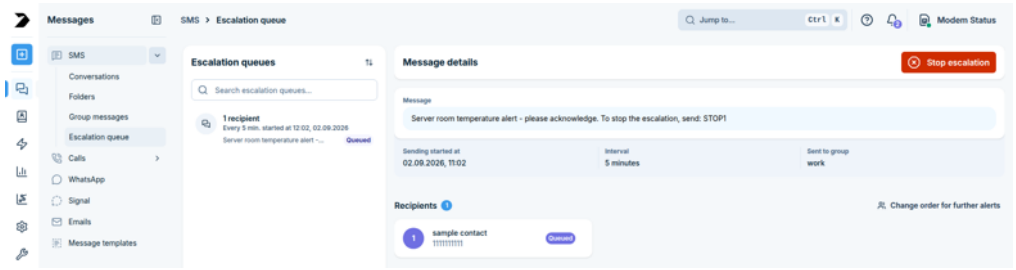
Groupes de messages



Composition d'un message à un groupe Phonebook

Messages > SMS > Group messages (`/messages/sms/groups/`) liste les conversations que vous avez initiées en envoyant à un groupe Phonebook plutôt qu'à un numéro individuel - une entrée par envoi de groupe, pour que vous puissiez examiner qui un message de groupe a été envoyé sans fouiller dans les fils individuels.

File d’attente d’escalade



File d’attente d’escalade

Messages > SMS > Escalation queue (`/messages/sms/escalation/`) affiche chaque escalade actuellement en cours - un message envoyé à un groupe d’escalade qui progresse toujours dans la liste de contacts. La configuration d’un groupe d’escalade lui-même est couverte dans Phonebook ; cette page est l’endroit où vous regardez et contrôlez un qui est déjà en cours.

Chaque escalade en cours est listée avec son message, son heure de début et son intervalle. En ouvrir une affiche les **Détails du message** : le texte du message, l’heure de début, l’intervalle, le groupe cible et chaque destinataire avec un statut de **Livré**, **Envoi en cours**, **En attente** ou **Erreur d’envoi**.

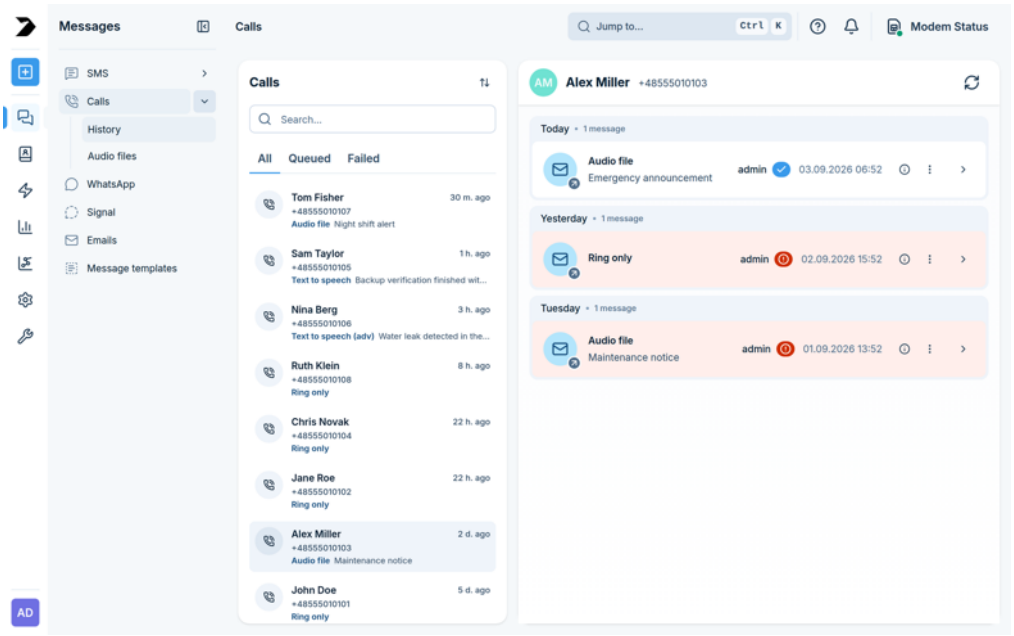
À partir de cette vue, vous pouvez :

- **Modifier l’ordre pour les prochaines alertes** - réorganiser les personnes qui n’ont pas encore été contactées.
- **Arrêter l’escalade** - annuler l’escalade entière immédiatement ; personne d’autre sur la liste n’est contacté.

Une escalade se termine également automatiquement lorsqu’un destinataire renvoie le mot d’arrêt du groupe, ou une fois que la dernière personne de la liste a été contactée.

Appels

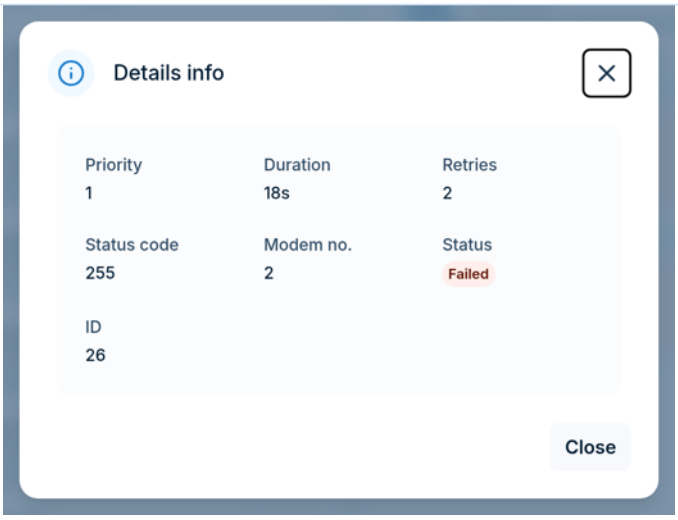
Historique



Historique des appels

Messages > Appels > Historique (`/messages/calls/`) répertorie chaque appel effectué par l'appareil, regroupés par numéro de téléphone, le plus récent en premier.

- Les onglets **Tous**, **En attente** et **Échoués** affinent la liste.
- La boîte de recherche trouve des appels par numéro, par nom de contact ou par le texte qui a été lu à haute voix.
- L'ouverture d'un appel affiche ses détails : priorité, durée, nombre de tentatives, code de statut, numéro de modem et ID. Le code de statut est ce qu'il faut citer lorsque vous contactez le support à propos d'un appel ayant échoué.
- Supprimez un seul appel ou sélectionnez-en plusieurs et supprimez-les ensemble.

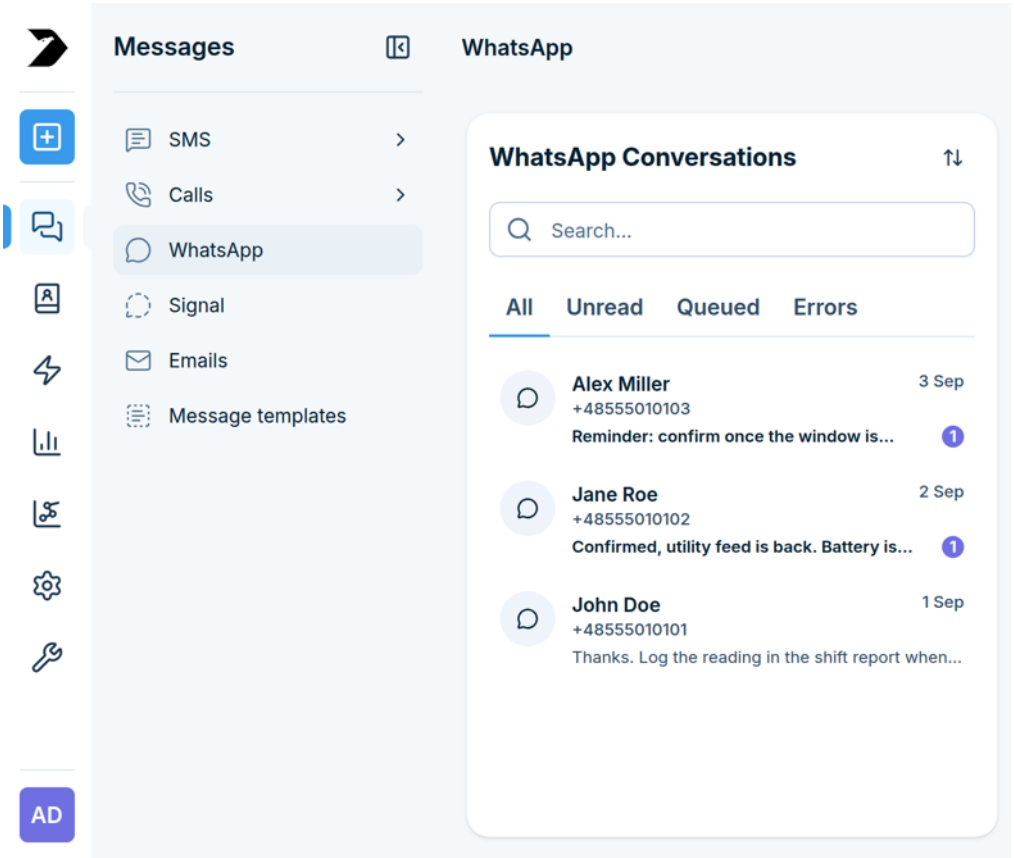


Détails d'appel

Les appels sont mis en file d'attente comme les messages : un programmé pour plus tard ou retenu par la priorité reste dans cette liste comme **En attente** jusqu'à ce qu'il soit effectué. La création d'un appel (types d'appels, modèles de voix et le panneau Composer

Appel) est couverte dans Appels sous Paramètres.

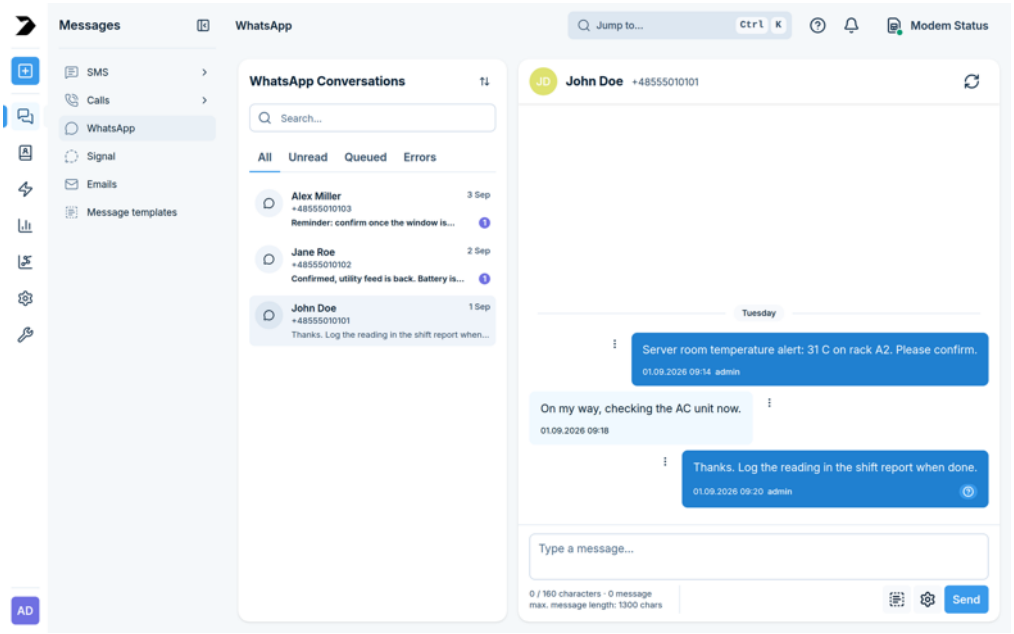
WhatsApp



Conversations WhatsApp

Messages > WhatsApp (`/messages/whatsapp/`) répertorie les conversations WhatsApp, une par numéro, la plus récente en premier, une fois que le canal a été lié sous Paramètres.

- Filtrez avec les onglets **All**, **Unread**, **Queued** et **Errors**.
- Recherchez et triez les conversations par date ou numéro de téléphone.
- Ouvrez une conversation et répondez directement à partir de la boîte en bas (maximum 1300 caractères).
- Supprimez une seule conversation ou sélectionnez-en plusieurs et supprimez-les ensemble.

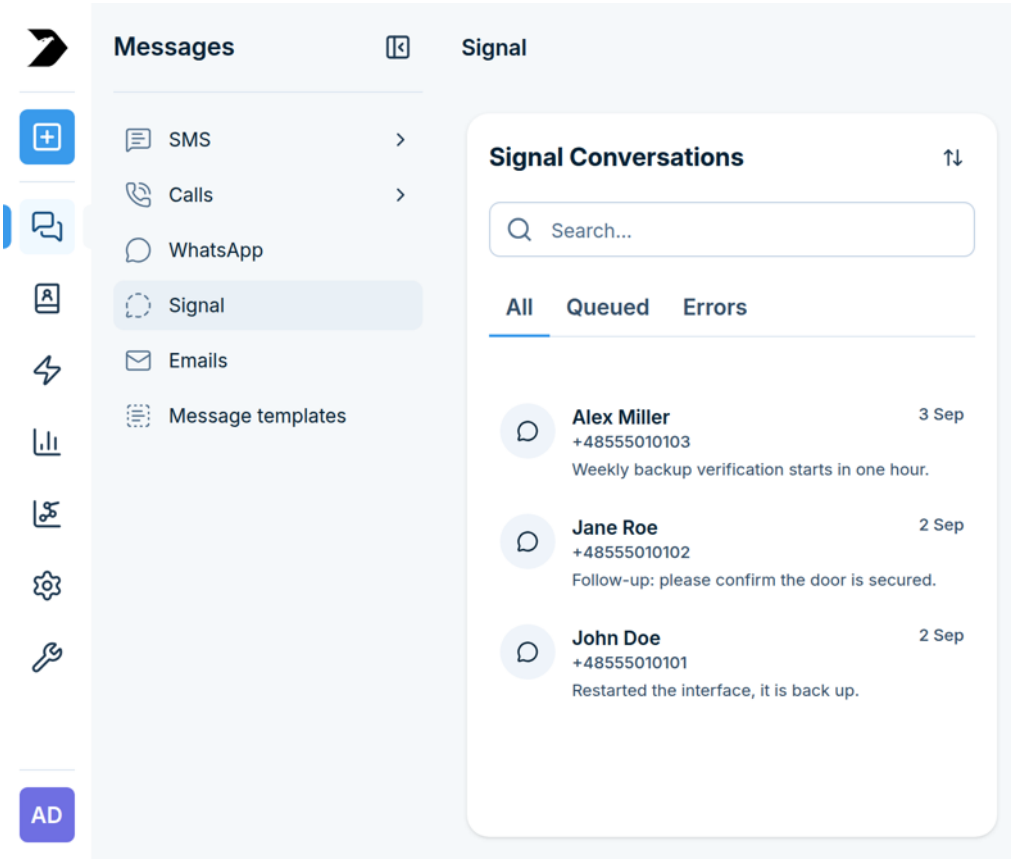


Une conversation WhatsApp ouverte

Si WhatsApp n'a pas encore été configuré, cette page affiche un avis avec un bouton qui vous amène directement aux paramètres WhatsApp. Pour envoyer un nouveau message WhatsApp, ouvrez **Composer**, cochez **WhatsApp** comme type de message et écrivez comme d'habitude.

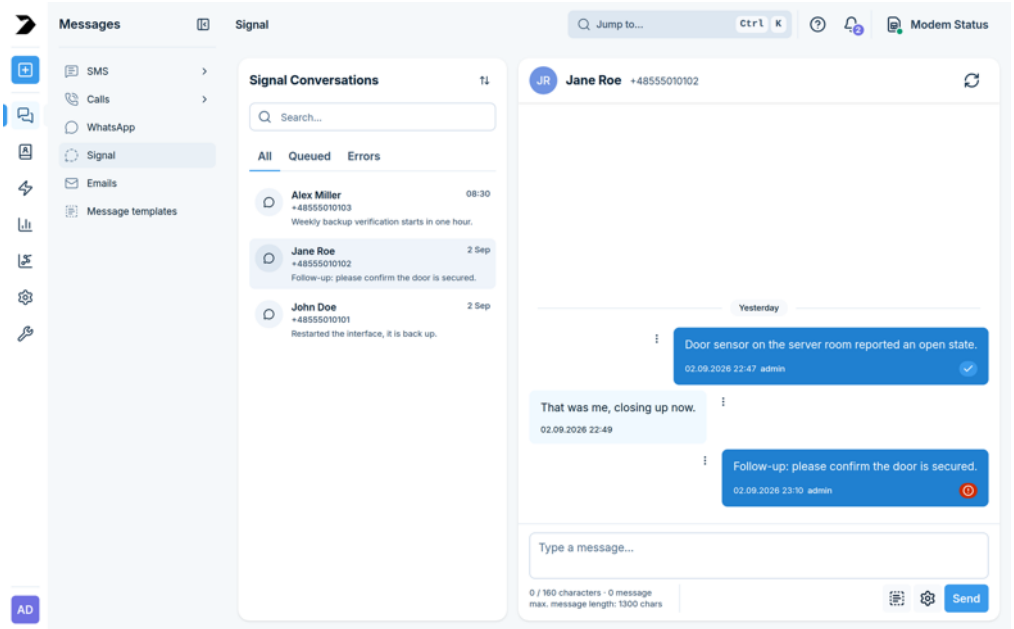
Seuls les messages reçus après que l'appareil a été lié apparaissent ici.

Signal



Conversations Signal

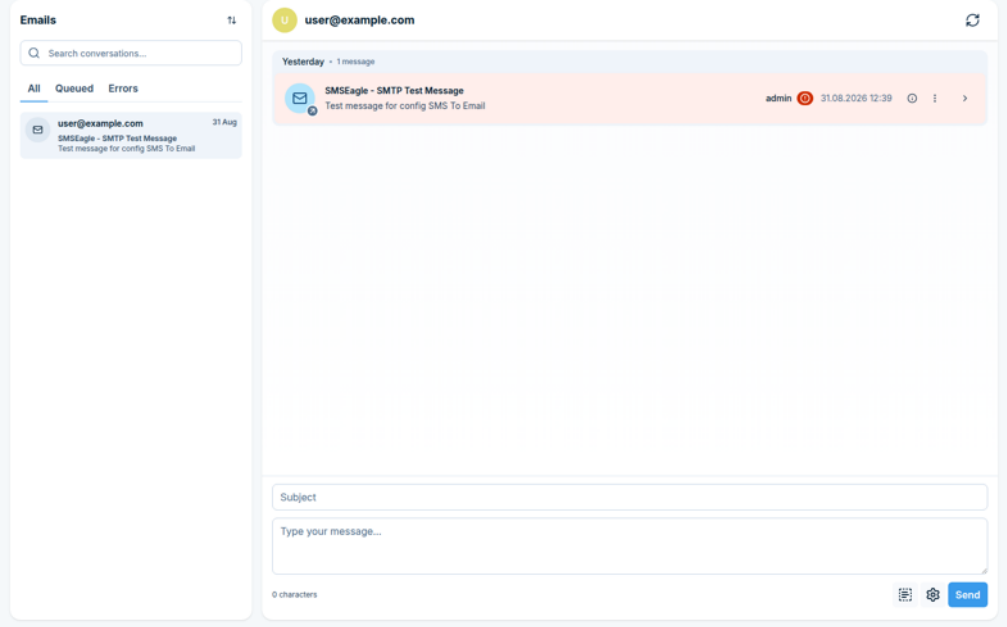
Messages > Signal (`/messages/signal/`) fonctionne de la même manière que WhatsApp ci-dessus, une fois qu'un numéro a été enregistré dans Paramètres : une conversation par numéro, les filtres **Tous / En attente / Erreurs**, et réponse depuis la zone en bas (1300 caractères maximum). Signal n'a pas d'onglet **Non lus**.



Une conversation Signal ouverte

Pour envoyer un nouveau message Signal, ouvrez **Compose**, cochez **Signal** comme type de message, et écrivez comme d'habitude. Seuls les messages reçus après l'activation du service apparaissent ici.

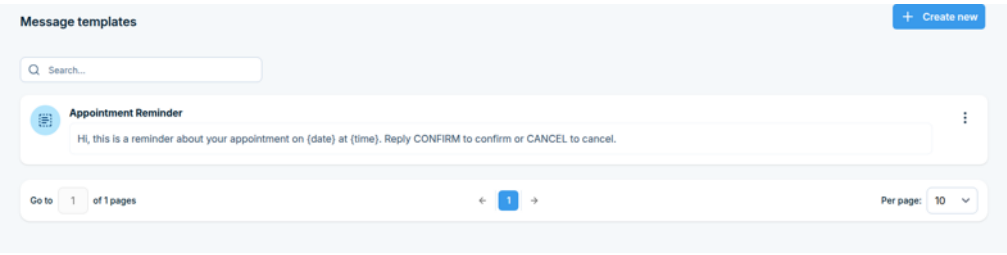
Emails



Conversations emails

Messages > Emails (`/messages/email/`) répertorie les conversations par email, un fil de discussion par adresse, les plus récentes en premier, avec les filtres **Tous**, **En attente** et **Erreurs** - la même vue de style conversation que SMS, WhatsApp et Signal, pour les mails envoyés ou reçus via SMS vers Email et Email vers SMS.

Modèles de message



Modèles de message

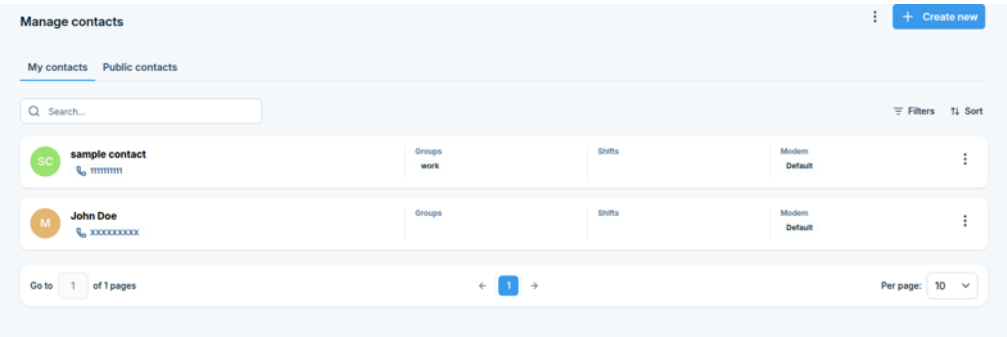
Messages > Message templates (`/messages/templates/`) stocke du texte de message réutilisable pour Compose, afin que les messages fréquents n'aient pas besoin d'être retapés à chaque fois.

Cliquez sur **Create new**, donnez au modèle un **Template name**, et écrivez le **Message content**. Les modèles enregistrés peuvent ensuite être sélectionnés dans Compose au lieu de taper le message de zéro.

Carnet d'adresses

Le carnet d'adresses est l'endroit où vous conservez les contacts et les groupes auxquels vous envoyez des messages ou desquels vous recevez des messages.

Contacts



Liste des contacts du carnet d'adresses

Carnet d'adresses > Contacts (`/phonebook/contacts`). Cliquez sur **Create new** pour ajouter un contact. La liste des contacts est divisée en deux onglets :

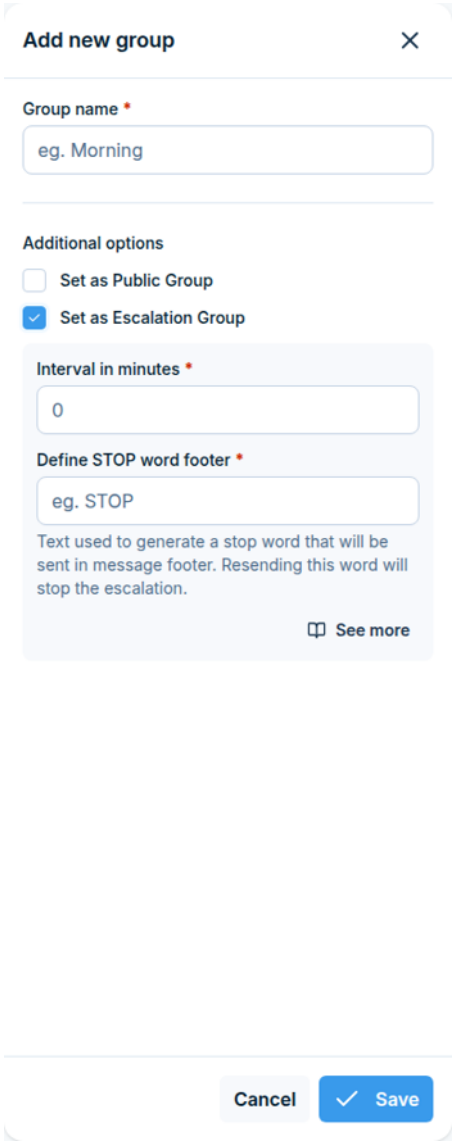
- **My contacts** - contacts visibles et utilisables uniquement par vous.
- **Public contacts** - contacts partagés avec d'autres utilisateurs de l'appareil (nécessaire, par exemple, pour qu'un contact public puisse être adressé par nom à partir d'Email vers SMS).

Chaque contact peut appartenir à un ou plusieurs **Groups**, se voir assigner un **Shift** (voir Shifts ci-dessous), et être épinglé à un **Modem** spécifique pour les messages sortants. Utilisez **Filters** et **Sort** pour trouver un contact dans un grand carnet d'adresses.

Groupes

Carnet d'adresses > Groups (`/phonebook/groups`). Les groupes vous permettent d'adresser un ensemble complet de contacts à la fois (par exemple à partir de Compose SMS, ou comme cible d'une règle d'automatisation) au lieu de sélectionner chaque contact individuellement. Cliquez sur **Add new**, donnez un **Name** au groupe, et cochez **Set as Public Group** si d'autres utilisateurs, des règles d'automatisation ou l'API doivent pouvoir envoyer des messages à ce groupe.

Groupes d’escalade



Options de groupe d’escalade dans la boîte de dialogue « Ajouter un nouveau groupe »

Un groupe d’escalade alerte les gens **l’un après l’autre, pas tous à la fois**, jusqu’à ce que quelqu’un confirme qu’il gère le problème - mettez vos personnes d’astreinte dans un groupe dans un ordre choisi, définissez un intervalle, et quand vous envoyez un message au groupe, la première personne le reçoit immédiatement, la deuxième le reçoit si personne n’arrête l’escalade, et ainsi de suite jusqu’au bas de la liste. Le suivi et le contrôle d’une escalade en cours se font dans Escalation queue sous Messages ; cette section est l’endroit où vous le configurez.

Étape 1 : Créer le groupe d’escalade

1. Cliquez sur **Add new**. Un panneau latéral s’ouvre.
2. Remplissez **Name**, par exemple `Night on-call`.
3. Cochez **Escalation group**. Deux champs supplémentaires apparaissent.
4. Remplissez **Escalation interval (minutes)** : combien de temps attendre avant d’alerter la personne suivante. Les valeurs autorisées sont de 1 à 999.

5. Remplissez **Escalation stop word** : le mot que les destinataires renvoient par texto pour arrêter l'escalade.
    - Maximum 8 caractères.
    - Lettres uniquement, pas de chiffres, d'espaces ou de ponctuation.
    - Il doit être unique - chaque groupe d'escalade a besoin de son propre mot d'arrêt.
6. Cliquez sur **Save**.

    Cochez également **Set as Public Group** si d'autres utilisateurs de l'appareil, des règles d'automatisation ou l'API doivent pouvoir envoyer des messages à ce groupe.

Étape 2 : Ajouter des personnes et définir leur ordre

1. Sur la page **Groups**, trouvez votre groupe d'escalade et ouvrez **Manage contacts**.
2. Ajoutez les contacts qui doivent être alertés.
3. Mettez-les dans le bon ordre en **faisant glisser les cartes** vers le haut et vers le bas. La personne au sommet est contactée en premier - c'est exactement l'ordre dans lequel les alertes sont envoyées.

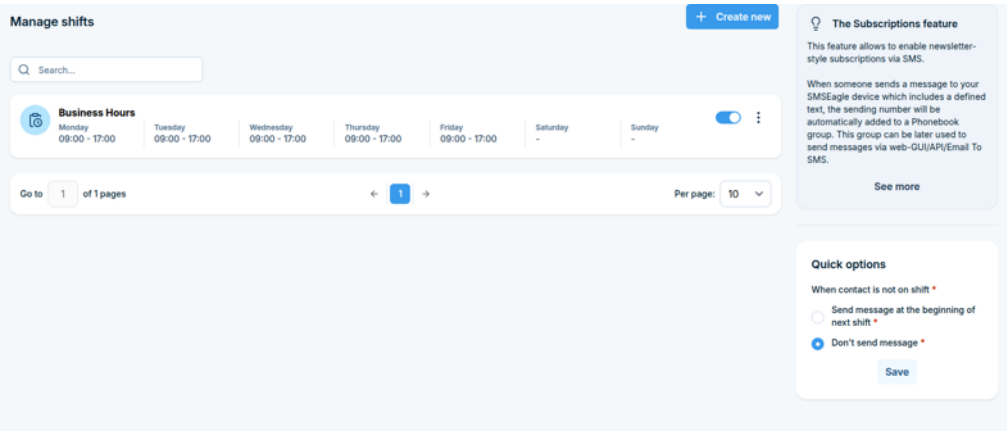
Étape 3 : Déclencher une escalade

Envoyez un message au groupe de la même manière que tout autre message, depuis **Compose**. SMSEagle ajoute alors une ligne indiquant au destinataire ce qu'il doit renvoyer par SMS pour arrêter l'escalade (sous la forme `To stop the escalation, send: <stop word><number>`), envoie le message au premier contact immédiatement, et programme le même message pour les contacts suivants, espacés selon l'intervalle que vous avez défini.

> **Indiquez exactement à vos destinataires ce qu'ils doivent répondre.** Le nombre après le mot d'arrêt identifie cette escalade particulière, de sorte que la réponse doit contenir la totalité, par exemple `ACK17`, correspondant exactement - le mot d'arrêt **et** le nombre joints sans espace, avec la même casse, et rien d'autre dans le message. Seul un membre du groupe d'escalade peut l'arrêter ; une réponse d'un numéro non lié est ignorée.

Vous pouvez également déclencher un groupe d'escalade depuis l'API, depuis Email vers SMS, ou depuis n'importe quelle règle d'automatisation qui envoie à un groupe.

Équipes



Aperçu de la gestion des équipes

Les équipes décrivent **quand une personne est en service**. Une fois que vous assignez une équipe à un contact, SMSEagle vérifie l'équipe avant d'envoyer un message à ce contact : si un message est adressé à un contact qui est actuellement en dehors de ses heures d'équipe, SMSEagle soit conserve le message et le remet au début de son équipe suivante, soit ne l'envoie pas du tout - vous choisissez (voir Étape 4 ci-dessous).

Utilisation typique : un planning de permanence, où l'équipe de nuit ne doit pas être réveillée par des alertes destinées à l'équipe de jour.

> **À savoir :** un contact avec **aucune équipe assignée** est toujours considéré comme disponible. Les équipes ne restreignent que les contacts auxquels vous les assignez.

Avant de commencer

- Vous avez besoin d'au moins un contact dans le Carnet (**Phonebook > Contacts**).
- Assurez-vous que l'horloge de l'appareil et le fuseau horaire sont corrects, car les heures d'équipe sont comparées à l'heure de l'appareil. Vérifiez cela dans **Settings > Date/Time**.

Étape 1 : Ouvrir la page Équipes

Phonebook > Shifts (`/phonebook/shifts`) répertorie les équipes que vous avez déjà créées, avec une boîte **Quick options** sur la droite.

Étape 2 : Créer une équipe

1. Cliquez sur **Create new** dans le coin supérieur droit. Un panneau latéral s'ouvre.
2. Remplissez **Name**, par exemple `Night shift` ou `Weekend duty`.
3. Laissez **Enabled** coché pour que l'équipe commence à fonctionner immédiatement. Décochez-le pour préparer l'équipe maintenant et l'activer plus tard.
4. Sous **Active from - to**, définissez les heures pour chaque jour de la semaine : entrez une heure **From** et une heure **To** pour chaque jour où la personne est en service, et laissez un jour vide si elle ne l'est pas.

5. Cliquez sur **Save**.

Règles pour les heures d’équipe

- **From** doit être antérieur à **To** le même jour.
- **From** et **To** doivent tous deux être remplis, ou tous deux laissés vides. Un jour partiellement rempli est rejeté avec un message d’erreur.
- Au moins un jour doit avoir des heures définies.

> **Équipes de nuit :** une équipe qui traverse minuit (par exemple 22:00 à 06:00) doit être saisie en deux entrées : `22:00 - 23:59` le premier jour et `00:00 - 06:00` le jour suivant.

Étape 3 : Assigner des contacts à l’équipe

Vous pouvez faire cela des deux côtés.

À partir de l’équipe : sur la page **Shifts**, trouvez votre équipe, ouvrez ses actions, et choisissez **Manage contacts**.

À partir du contact : allez à **Phonebook > Contacts**, sélectionnez un ou plusieurs contacts à l’aide de leurs cases à cocher, choisissez **Edit shifts**, sélectionnez les équipes à assigner, et cliquez sur **Assign shifts**.

Étape 4 : Choisir ce qui se passe en dehors des heures d’équipe

La zone **Quick options** à droite de la page Shifts contient **When contact is not on shift** :

Option	Résultat
Send message at the beginning of next shift	Le message attend dans la file d’attente et est livré automatiquement au début de la prochaine plage horaire du contact.
Don’t send message	Le message n’est pas envoyé à ce contact. Il est enregistré comme non livré.

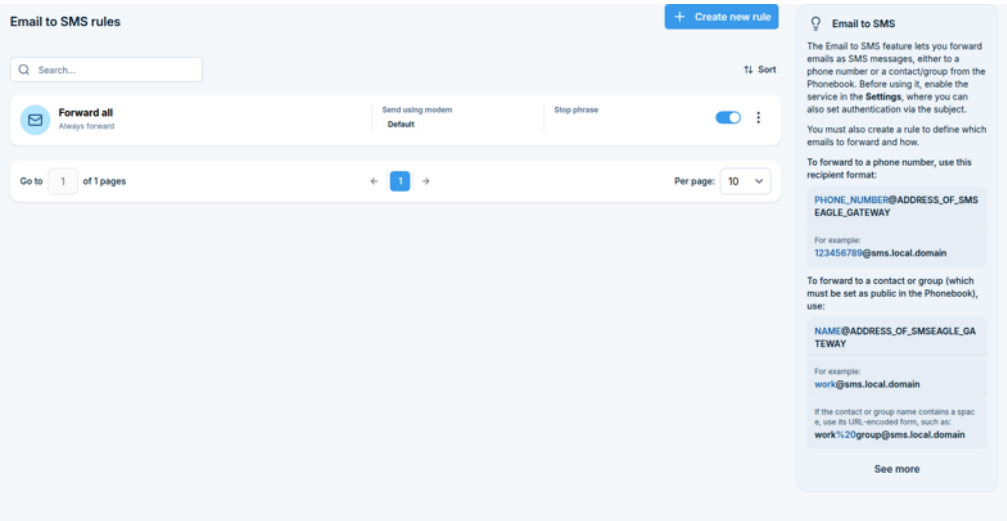
Choisissez l’option que vous souhaitez et cliquez sur **Save**.

> Ce paramètre est **global**. Il s’applique à toutes les plages horaires et à tous les contacts de l’appareil, pas seulement à la plage horaire que vous consulez actuellement.

Automatisation

Ce chapitre couvre la section **Automatisation** de l'interface web, dans le même ordre que celui des règles qui y apparaissent.

Email vers SMS



Règles Email vers SMS

La fonctionnalité Email vers SMS vous permet de transférer les emails reçus sous forme de messages SMS, soit vers un numéro de téléphone, soit vers un contact/groupe de votre Carnet d'adresses.

Où la trouver

Cette fonctionnalité est répartie en deux endroits dans l'interface web :

- **Automatisation > Email > Email vers SMS** (`/automation/email-to-sms`) est l'endroit où vous créez et gérez les règles de transfert.
- **Paramètres > Canaux > Email > Email vers SMS** (`/settings/email/email-to-sms`) est l'endroit où vous activez le service et configurez la conversion des emails en messages - voir Email vers SMS dans Paramètres.

Étape 1 : Comprendre le format de l'adresse destinataire

Les emails doivent être envoyés à une adresse au format spécial pour que SMSEagle sache où livrer le message.

Pour transférer vers un numéro de téléphone :

```
PHONE_NUMBER@ADDRESS_OF_SMSEAGLE_GATEWAY
```

Par exemple : `999888777@gateway.smseagle.eu`

Pour transférer vers un contact ou groupe du Carnet d'adresses (le contact ou groupe doit être défini comme **public**) :

```
NAME@ADDRESS_OF_SMSEAGLE_GATEWAY
```

Par exemple : `work@gateway.smseagle.eu`

Si le nom du contact ou du groupe contient un espace, utilisez sa forme encodée pour les URL : `work%20group@gateway.smseagle.eu`

Au lieu de l'adresse IP de la passerelle, vous pouvez utiliser un Nom de Domaine Pleinement Qualifié, défini sous **Paramètres > Canaux > Email > Email vers SMS > Paramètres avancés > Nom d'hôte FQDN**. Si **Utiliser les contacts LDAP** y est activé, le même format `NAME@GATEWAY` résout également les contacts et groupes définis dans LDAP / Active Directory.

Par défaut, le corps de l'email devient le texte du SMS. Cela dépend du paramètre **Que faire avec le sujet de l'email** dans Paramètres : le sujet peut être ignoré, ajouté au début du texte du message, utilisé pour l'authentification, ou envoyé à la place du corps.

Étape 2 : Créer une nouvelle règle

Accédez à **Automatisation > Email > Email vers SMS** et cliquez sur **Créer une nouvelle règle**. Un panneau intitulé Ajouter une règle Email vers SMS s'ouvre à droite.

Champ	Description
Nom de la règle *	Un nom pour identifier la règle (obligatoire, 100 caractères maximum)
Transférer pour *	Toujours envoyer transfère chaque email reçu correspondant au format d'adresse. Expéditeur spécifié / message contient ajoute des conditions de filtrage, voir Étape 3.
Phrase d'arrêt	Le texte commençant à partir de cette phrase sera supprimé du message (sensible à la casse)
Priorité	Priorité d'envoi de 0 à 5. Les messages avec une priorité plus élevée sont traités en premier.
Appel après envoi du SMS	Non, Sonnerie uniquement, Oui - synthèse vocale, ou Oui - synthèse vocale (avancée). Les options disponibles dépendent de la voix et des capacités TTS de votre appareil.
Modèle de voix	Voix utilisée pour l'appel de synthèse vocale. Affichée uniquement pour les appareils prenant en charge la synthèse vocale avancée, et uniquement après sélection de Oui - synthèse vocale (avancée).
Forcer la conversion en UTF-8	Force la conversion du texte du message en UTF-8
Supprimer l'historique de la conversation	Supprime l'historique cité de la conversation par email du texte du message

Cliquez sur **Save** pour créer la règle, ou **Cancel** pour l'annuler.

Étape 3 : Ajouter des conditions de filtrage (facultatif)

Si vous sélectionnez **Specified sender / message contains** sous Forward for, trois conditions indépendantes deviennent disponibles, chacune avec sa propre case à cocher et son champ de texte :

- **When incoming email address contains** filtre par l'adresse email de l'expéditeur
- **When incoming messages subject contains** filtre par la ligne d'objet de l'email
- **When incoming message content contains** filtre par le corps du message email

Le commutateur **Case sensitive** s'applique à toutes les conditions activées.

Vous pouvez activer une, deux ou les trois conditions. La règle ne se déclenche que lorsque **toutes** les conditions activées sont remplies.

Étape 4 : Gérer les règles existantes

Chaque règle apparaît sous forme de carte dans la liste Email to SMS, affichant :

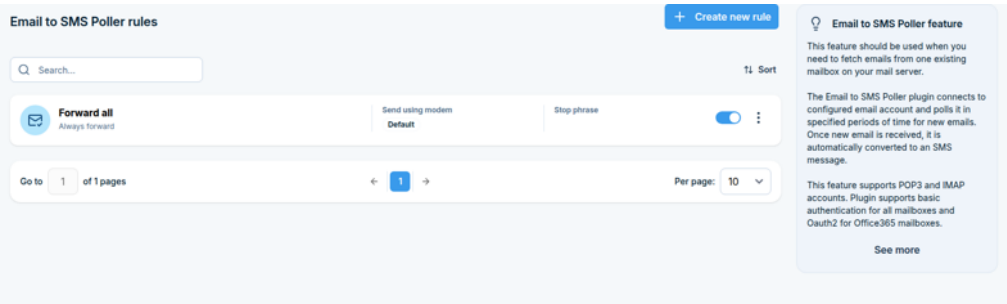
- le nom de la règle
- la condition de transfert, par exemple Forward when incoming: email address contains: ..., ou Always forward lorsqu'aucune condition n'est définie
- le modem utilisé pour l'envoi
- la phrase d'arrêt configurée
- un commutateur activé/désactivé pour activer ou désactiver la règle sans la supprimer
- un menu ⋮ avec **Edit** et **Delete**

Contrôles supplémentaires sur la liste :

- **Search** filtre les règles par nom.
- La sélection des cases à cocher des règles révèle les actions en masse : **Enable / Disable** et **Delete**.
- Les contrôles de pagination au bas vous permettent d'accéder à une page et de modifier le nombre de règles affichées par page.

Le panneau d'aide de droite explique les formats d'adresse des destinataires, avec un bouton **See more** qui renvoie à la page de la fonctionnalité sur smseagle.eu.

Collecteur d'e-mails vers SMS



Règles du sondeur Email vers SMS

Le collecteur d'e-mails vers SMS vérifie périodiquement une boîte aux lettres externe via POP3, IMAP ou IMAP avec OAuth2 (Microsoft 365 / Outlook), et convertit les e-mails qu'il y trouve en messages SMS selon les règles du collecteur d'e-mails vers SMS. Contrairement à E-mail vers SMS (qui exécute son propre serveur de messagerie et reçoit les e-mails activement), le collecteur accède à une boîte aux lettres existante que vous possédez déjà.

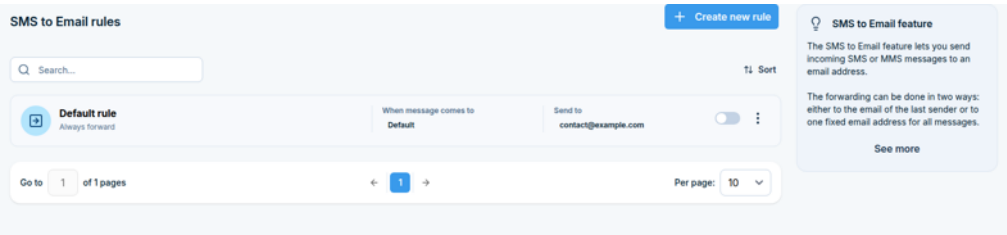
Où la trouver

Automation > Email > Email to SMS Poller (`/automation/email-to-sms-poller/`) est l'endroit où vous créez et gérez les règles. L'activation du service et la connexion de la boîte aux lettres (POP3, IMAP ou IMAP + OAuth2 pour Microsoft 365) se font dans Email to SMS Poller des paramètres.

Création d'une règle

Cliquez sur **Create new rule**. Les règles ici fonctionnent de la même manière que les règles Email to SMS - nommez la règle, choisissez si elle redirige tous les e-mails interrogés ou uniquement ceux correspondant aux conditions d'expéditeur/sujet/contenu, et définissez les mêmes options par règle (modem, phrase d'arrêt, priorité, appel après envoi).

SMS vers E-mail



Règles SMS vers E-mail

Ce que fait cette fonctionnalité

SMS vers E-mail redirige les messages SMS et MMS **entrants** vers une adresse e-mail, afin que vous puissiez les lire dans votre boîte aux lettres au lieu de vous connecter à SMSEagle.

Vous créez des règles qui décident quels messages sont redirigés et où ils vont. Une règle peut tout rediriger, ou uniquement les messages de certains expéditeurs, ou uniquement les messages contenant une certaine phrase.

Utilisations typiques : redirection des réponses du personnel sur le terrain vers une boîte aux lettres d'assistance partagée, ou archivage des confirmations d'alertes dans la boîte de réception e-mail d'un système de ticketing.

Avant de commencer

SMSEagle a besoin d'une configuration de serveur de messagerie fonctionnelle pour envoyer les e-mails. Allez dans **Settings > Channels > Email > SMTP Configuration** et assurez-vous qu'elle est remplie et testée - consultez SMTP Configuration. Sans cela, les règles correspondront mais aucun e-mail n'arrivera.

Si vous souhaitez effectuer une redirection en fonction des contacts ou des groupes de l'expéditeur, ces contacts et groupes doivent être marqués comme **Public** dans l'"Annuaire.

Étape 1 : Ouvrir la page SMS vers E-mail

Dans la barre latérale, allez dans **Automation > Email > SMS to Email**.

Étape 2 : Créer une règle

Cliquez sur **Create new rule** dans le coin supérieur droit. Un panneau latéral s'ouvre.

Nommer la règle

Dans **Rule name**, tapez quelque chose de descriptif, par exemple `Forward all to support`. Maximum 100 caractères.

Décider quels messages rediriger

Choisissez **Forward for** :

Option	Ce que cela signifie
Always forward	Chaque SMS et MMS entrant est redirigé.
Specified sender / message	Seuls les messages correspondant aux conditions que vous définissez ci-dessous sont transférés.

Si vous avez choisi **Expéditeur/message spécifié**, deux conditions deviennent disponibles. Vous pouvez en utiliser une ou les deux. Lorsque vous utilisez les deux, un message doit satisfaire **les deux** pour être transféré.

Lorsqu'un SMS entrant provient de Cochez cette case et sélectionnez les contacts ou groupes dont les messages doivent être transférés. Commencez à taper pour effectuer une recherche. Seuls les contacts et groupes **publics** peuvent être sélectionnés ici.

Lorsque le texte d'un SMS entrant contient Cochez cette case et tapez la phrase à rechercher, par exemple `URGENT`. La phrase peut apparaître n'importe où dans le texte du message. Cochez **Respecter la casse** si `urgent` et `URGENT` doivent être traités comme différents.

Choisissez l'adresse e-mail de destination

Choisissez **Type de transfert d'e-mail**:

Option	Ce que cela signifie
Vers une adresse e-mail fixe	Chaque message correspondant est envoyé à l'adresse unique que vous entrez dans **Transférer vers l'adresse e-mail**.
Vers l'e-mail du dernier utilisateur ayant envoyé	Le message est renvoyé à l'adresse e-mail de la personne qui a envoyé le dernier SMS à ce numéro de téléphone via SMSEagle. Cela ferme la boucle d'une conversation e-mail vers SMS. Entrez une **Adresse e-mail par défaut** comme secours, utilisée lorsqu'aucun dernier expéditeur n'est enregistré.

Définir l'objet de l'e-mail

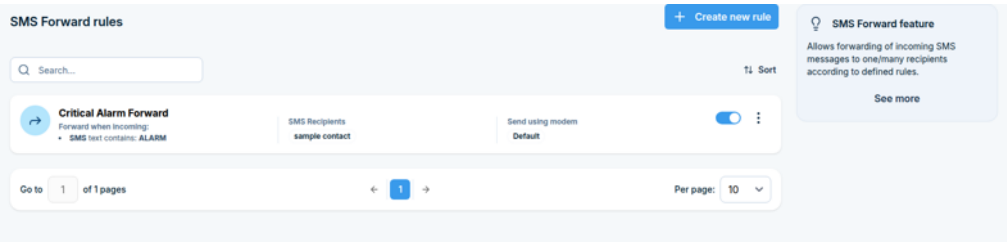
Email subject contrôle la ligne d'objet de l'e-mail transféré. Vous pouvez utiliser des espaces réservés, qui sont remplacés par des valeurs réelles lors de l'envoi de l'e-mail:

Espace réservé	Remplacé par
`{SENDER}`	Le numéro de téléphone à partir duquel le SMS provient
`{WORDS,X}`	Les premiers X mots du texte du message
`{CHARS,X}`	Les premiers X caractères du texte du message

Exemple: `SMS from {SENDER}: {WORDS,5}` produit un objet comme `SMS from +48111222333: Server room temperature alarm triggered`. Maximum 150 caractères.

Cliquez sur **Save**. La règle commence à fonctionner immédiatement sur les nouveaux messages reçus.

SMS Forward



Dialogue Ajouter une règle de transfert

Ce que fait cette fonctionnalité

SMS Forward transmet **les messages SMS entrants à d'autres personnes**. Lorsqu'un message arrive, SMSEagle l'envoie à nouveau aux destinataires que vous choisissez.

Vous pouvez transférer le message exactement tel qu'il est arrivé, ou le remplacer par votre propre texte. Vous pouvez également ajouter un appel vocal au-dessus du SMS transféré, afin qu'une alerte ne puisse pas être ignorée.

Utilisations typiques: envoi de messages d'alarme d'une machine à toute l'équipe de garde, transmission de messages d'un numéro partagé à la personne actuellement de service, ou conversion d'un court code machine en une phrase lisible pour l'équipe.

Avant de commencer

- Les contacts et groupes vers lesquels vous transférez **vers** doivent exister dans l'"Annuaire. Les contacts et groupes utilisés comme destinataires de transfert ou comme conditions d'expéditeur doivent être marqués comme **Public**.

- Décidez si les destinataires ont besoin du libellé original ou d'un message réécrit.

Étape 1 : Ouvrir la page SMS Forward

Dans la barre latérale, allez à **Automation > SMS > SMS Forward**.

Étape 2 : Créer une règle

Cliquez sur **Create new rule** dans le coin supérieur droit. Un panneau latéral s'ouvre.

Nommez la règle et définissez sa priorité

Rule name Un nom descriptif, par exemple `Alarms to on-call team`. 100 caractères maximum.

Priority Un nombre de 0 à 9. Les messages générés par une règle de priorité plus élevée sont mis en file d'attente pour l'envoi plus tôt que les messages d'une règle de priorité plus basse. Laissez la valeur par défaut à moins que vous ayez des règles urgentes qui doivent avoir la priorité sur les envois en masse.

Décider quels messages rediriger

Choisissez **Forward for** :

Option	Ce que cela signifie
All incoming messages	Chaque SMS entrant est transmis.
Specified sender / message	Seuls les messages correspondant aux conditions que vous définissez ci-dessous sont transférés.

Si vous avez choisi **Expéditeur/message spécifié**, deux conditions deviennent disponibles. Vous pouvez en utiliser une ou les deux. Lorsque vous utilisez les deux, un message doit satisfaire **les deux** pour être transféré.

When incoming SMS comes from Cochez cette option et sélectionnez les contacts ou groupes d'expéditeurs dans **Sender contacts**. Seuls les contacts et groupes **publics** peuvent être sélectionnés ici.

When incoming SMS text contains Cochez cette option et tapez la phrase dans **Text fragment**, par exemple `ALARM`. La phrase peut apparaître n'importe où dans le message. Cochez **Case sensitive** si `alarm` et `ALARM` doivent être traités comme différents.

Choisissez ce que dit le message transmis

Utilisez **Message content** :

Option A : Message original

Les destinataires reçoivent le texte entrant inchangé. Un choix supplémentaire apparaît, **Message header** :

Option	Résultat
Don’t include	Seul le texte original est transmis.
Include sender	Le numéro de téléphone de l’expéditeur original est ajouté au message transmis, afin que les destinataires sachent d’où il provient.

Option B : Texte personnalisé

Les destinataires reçoivent votre propre texte à la place de l’original. Tapez-le dans **Custom message** (500 caractères maximum). Vous pouvez incorporer des parties du message original avec des espaces réservés :

Espace réservé	Remplacé par
`{SENDER}`	Le numéro de téléphone à partir duquel le SMS provient
`{MESSAGE}`	Le texte complet du message original

Exemple : `Alarm from {SENDER}. Details: {MESSAGE}` envoie une phrase lisible construite autour du texte brut de la machine.

Choisissez les destinataires

Dans **Forward to**, sélectionnez les contacts ou groupes qui doivent recevoir le message. Commencez à taper pour effectuer une recherche. Ce champ est obligatoire ; une règle ne peut pas être enregistrée sans au moins un destinataire.

Optionnellement, ajouter un appel téléphonique

Call after sending SMS fait que l’appareil effectue également un appel vocal aux mêmes destinataires. Les options disponibles dépendent de votre modèle d’appareil :

Option	Ce qui se passe
No	Aucun appel n’est effectué. C’est la valeur par défaut.
Sonnerie uniquement	L’appareil appelle le destinataire et raccrocche. Aucun message audio n’est lu.
Oui - synthèse vocale	L’appareil appelle et lit le texte du message.
Oui - synthèse vocale (avancée)	Identique à ce qui précède, avec une voix sélectionnable plus naturelle. Choisissez la voix dans le champ **Voice model** qui apparaît.

Si votre appareil ne supporte pas les appels vocaux, seul **No** est disponible.

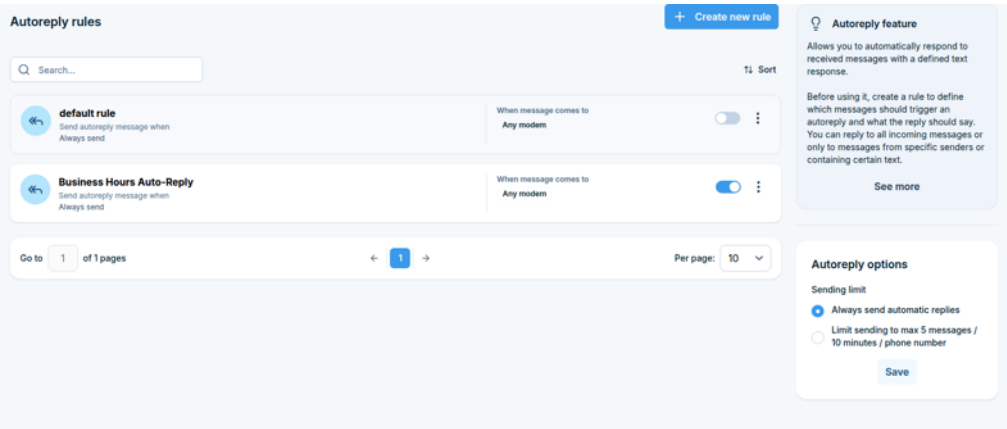
Cliquez sur **Save**. La règle commence à fonctionner immédiatement sur les nouveaux messages reçus.

Fonctionnement du transfert

- La condition de texte est une correspondance **contains**, et non une correspondance exacte. Une règle recherchant `ALARM` transfère un message disant `ROOM 4 ALARM triggered`.
- Si plusieurs règles correspondent au même message entrant, **chacune d'elles** transfère séparément, de sorte que les destinataires peuvent recevoir plus d'un SMS. Maintenez les conditions distinctes pour éviter les doublons.
- Les règles s'appliquent uniquement aux messages arrivant après la création et l'activation de la règle. Elles ne traitent pas les messages déjà dans la boîte de réception.
- Les destinataires peuvent toujours être ignorés pour leurs propres raisons : **Vacation mode** sur le contact, un quart de travail actuellement en dehors de ses heures (voir Shifts), ou le numéro se trouvant sur la liste de refus.

  Évitez les boucles de transfert. Ne transférez pas les messages vers un numéro qui transfère lui-même en retour vers votre appareil. Deux appareils se pointant l'un l'autre continueront à s'envoyer des messages mutuellement.

Réponses automatiques



Règles de réponse automatique et options de limite d'envoi

Ce que fait cette fonctionnalité

Les réponses automatiques envoient une **réponse textuelle automatique aux messages SMS entrants**.

Vous créez des règles qui décident quels messages entrants reçoivent une réponse et ce que dit la réponse. Une règle peut répondre à tout, ou seulement aux messages de certains expéditeurs, ou seulement aux messages contenant une certaine phrase.

Usages typiques : confirmer la réception d'une demande de commande, indiquer aux gens que le numéro est sans surveillance la nuit, ou répondre à un mot-clé avec des informations fixes telles que les heures d'ouverture.

Avant de commencer

- L'appareil doit être capable d'envoyer des SMS. Vérifiez qu'au moins un modem est connecté et enregistré sur le réseau.
- Si vous souhaitez répondre uniquement à des expéditeurs spécifiques, ces contacts et groupes doivent être marqués comme **Public** dans l'"Annuaire.

Étape 1 : Ouvrez la page Réponses automatiques

Dans la barre latérale, allez à **Automation > SMS > Autoreplies**.

Sur le côté droit de la page se trouve une boîte **Autoreply options**. Elle contient un paramètre qui s'applique à toutes les règles, décrit à l'"Étape 3.

Étape 2 : Créer une règle

Cliquez sur **Create new rule** dans le coin supérieur droit. Un panneau latéral s'ouvre.

Nommer la règle

Dans **Rule name**, tapez quelque chose de descriptif, par exemple `Out of hours reply`. Maximum 100 caractères.

Décidez quels messages auxquels répondre

Choisissez **Send autoreply for** :

Option	Ce que cela signifie
All incoming messages	Chaque SMS entrant reçoit la réponse.
Specified sender / message	Seuls les messages correspondant aux conditions que vous définissez ci-dessous reçoivent une réponse.

Si vous avez choisi **Specified sender / message**, deux conditions deviennent disponibles. Vous pouvez en utiliser une ou les deux. Quand vous en utilisez les deux, un message doit satisfaire **les deux** pour recevoir une réponse.

Quand un SMS entrant provient de Cochez cette option et sélectionnez les contacts ou groupes qui doivent recevoir une réponse. Commencez à taper pour rechercher. Seuls les contacts et groupes **publics** peuvent être sélectionnés ici.

Quand le texte du SMS entrant contient Cochez cette option et tapez la phrase à rechercher, par exemple `PRICE`. La phrase peut apparaître n'importe où dans le texte du message. Cochez **Sensible à la casse** si `price` et `PRICE` doivent être traités comme différents.

Rédigez la réponse

Message de réponse automatique Le texte qui est renvoyé. Maximum 2000 caractères. Le même texte est envoyé à tous ceux qui déclenchent cette règle, gardez-le donc général.

Envoyer en Unicode Cochez cette option si la réponse contient des caractères en dehors de l'alphabet GSM standard, comme des lettres polonaises, allemandes ou cyrilliques. Les messages Unicode contiennent moins de caractères par partie SMS.

Cliquez sur **Save**. La règle commence à fonctionner immédiatement sur les nouveaux messages reçus.

Étape 3 : Définissez la limite d'envoi

La boîte **Options de réponse automatique** à droite de la page contrôle la fréquence à laquelle l'appareil accepte de répondre automatiquement au même numéro de téléphone :

Option	Résultat
Toujours envoyer des réponses automatiques	Chaque message correspondant reçoit une réponse, peu importe le nombre reçu.
Limiter l'envoi à 5 messages max / 10 minutes / numéro de téléphone	Au maximum 5 réponses automatiques sont envoyées au même numéro de téléphone en 10 minutes. Les messages supplémentaires de ce numéro ne reçoivent pas de réponse jusqu'à ce que la fenêtre de temps passe.

Choisissez l'option souhaitée et cliquez sur **Save**.

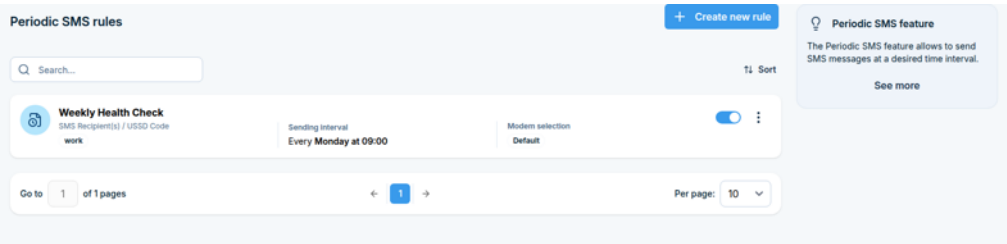
> **Il est vivement recommandé d'utiliser la limite.** Sans elle, deux appareils qui répondent tous les deux automatiquement peuvent finir par se répondre mutuellement en boucle, ce qui épuise rapidement les crédits SMS. La limite est la protection contre cela.

Ce paramètre est **global**. Il s'applique à chaque règle de réponse automatique sur l'appareil.

Comment fonctionne la correspondance

- La condition de texte est une correspondance **contient**, pas une correspondance exacte. Une règle recherchant `PRICE` répond à un message disant `what is the PRICE of item 5`.
- Si plusieurs règles correspondent au même message entrant, **chacune** d'elles envoie sa propre réponse, ainsi l'expéditeur peut recevoir plus d'un SMS. Gardez les conditions distinctes si vous ne souhaitez qu'une seule réponse.
- Les règles s'appliquent uniquement aux messages arrivant après la création et l'activation de la règle. Elles ne traitent pas les messages déjà dans la boîte de réception.

SMS périodique



Ajouter un dialogue de règle SMS périodique

Ce que fait cette fonctionnalité

SMS périodique envoie un message **automatiquement selon un calendrier répétitif**, sans que personne n'ait à cliquer sur Envoyer. Vous créez une règle une fois, et SMSEagle continue à l'envoyer toutes les heures, tous les jours, chaque semaine, chaque mois ou chaque année.

Vous pouvez planifier deux choses :

- un **SMS** vers des numéros de téléphone ou un groupe du répertoire téléphonique, éventuellement suivi d'un appel téléphonique,
- un **code USSD** envoyé à votre opérateur mobile (par exemple pour vérifier le solde prépayé de la carte SIM).

Utilisations courantes : un message quotidien « système actif », un rappel hebdomadaire à une équipe d'astreinte, une vérification mensuelle du solde sur une carte SIM prépayée.

Avant de commencer

- Si vous souhaitez envoyer à un groupe, le groupe doit exister dans **Phonebook > Groups** et être marqué comme **Public**. Les groupes privés ne peuvent pas être sélectionnés ici.
- Assurez-vous que l'horloge et le fuseau horaire de l'appareil sont corrects, car le calendrier suit l'heure de l'appareil. Vérifiez ceci dans **Settings > Date/Time**.

Étape 1 : Ouvrez la page SMS périodique

Dans la barre latérale, allez à **Automation > SMS > Periodic SMS**. Vous verrez la liste des règles que vous avez déjà.

Étape 2 : Créer une règle

Cliquez sur **Create new rule** dans le coin supérieur droit. Un panneau latéral s'ouvre.

Nommer la règle

Dans **Rule name**, tapez quelque chose que vous reconnaîtrez plus tard, par exemple `Daily heartbeat` ou `Monthly SIM balance`. Maximum 100 caractères.

Définir la planification

Choisissez un **Sending interval**. Les champs ci-dessous le sélecteur changent selon votre choix :

Intervalle	Ce que vous définissez	Exemple
Horaire	**À la minute** (par étapes de 5 minutes)	`15` envoie à 00:15, 01:15, 02:15 et ainsi de suite
Quotidienne	**À l'heure**	`07:30` envoie chaque matin à 07:30
Hebdomadaire	**Au jour de la semaine** et **À l'heure**	`Monday + 08:00` envoie chaque lundi matin
Mensuelle	**Au jour du mois** et **À l'heure**	`1 + 09:00` envoie le premier jour de chaque mois
Annuelle	**Au mois - jour** (format `mm-dd`) et **À l'heure**	`12-24 + 10:00` envoie chaque 24 décembre

> **Jours inexistants :** si vous planifiez quelque chose pour le jour 31 de chaque mois, le message ne sera pas envoyé dans les mois plus courts. Utilisez le jour 28 ou antérieur si le message doit être envoyé chaque mois.

Choisir ce qui envoyer

Utilisez le commutateur **Message type** en haut de cette section :

Option A : SMS

1. Tapez le texte dans **SMS Text** (maximum 2000 caractères).
2. Cochez **Send as Unicode** si le texte contient des caractères en dehors de l'alphabet GSM standard, tels que les lettres polonaises, allemandes ou cyrilliques. Notez que les messages Unicode contiennent moins de caractères par partie SMS.
3. Sous **Send to**, choisissez où le message va :
   - **Public groups** - commencez à taper le nom d'un groupe et sélectionnez-le dans la liste. Vous pouvez ajouter plusieurs groupes.
   - **Input manually** - tapez les numéros de téléphone. Séparez plusieurs numéros par des virgules, par exemple `+48111222333,+48444555666`.

   Vous devez remplir l'un des deux, sinon la règle ne peut pas être enregistrée.

Option B : Code USSD

Tapez le code dans **Code USSD**, par exemple `*100#`. La réponse de l'opérateur arrive comme un message entrant dans votre boîte de réception.

> Les codes USSD sont envoyés via le modem à votre opérateur mobile. Les codes disponibles dépendent de l'opérateur, pas de SMSEagle.

Optionnellement, ajouter un appel téléphonique

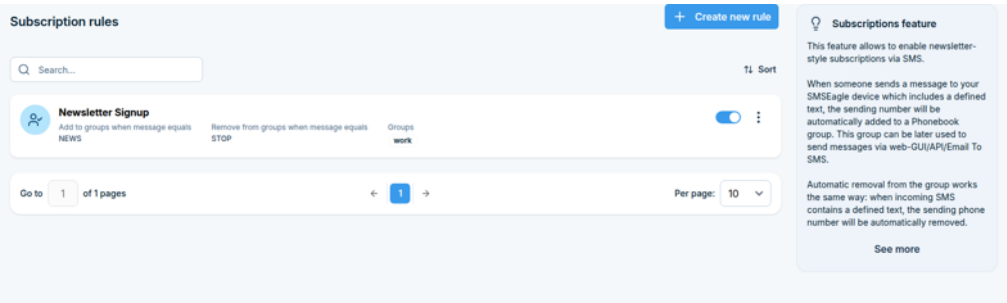
Appel après envoi du SMS fait également passer un appel vocal de l'appareil aux mêmes destinataires, ce qui est utile pour les alertes qui ne doivent pas être manquées. Les options disponibles dépendent du modèle de votre appareil :

Option	Ce qui se passe
No	Aucun appel n'est effectué. C'est la valeur par défaut.
Sonnerie uniquement	L'appareil appelle le destinataire et raccrocche. Aucun message audio n'est lu.
Oui - synthèse vocale	L'appareil appelle et lit le texte du message.
Oui - synthèse vocale (avancée)	Identique à ce qui précède, avec une voix sélectionnable plus naturelle. Choisissez la voix dans le champ **Voice model** qui apparaît.

Si votre appareil ne supporte pas les appels vocaux, seul **No** est disponible.

Cliquez sur **Save**. La règle apparaît dans la liste et commence à s'exécuter à son heure programmée suivante.

Abonnements



Règles d'abonnement

Ce que fait cette fonctionnalité

Les abonnements permettent aux gens de **rejoindre et de quitter un groupe du répertoire en envoyant un SMS**, de la même manière qu'une inscription à une newsletter.

Vous définissez deux mots-clés : un qui ajoute l'expéditeur à un groupe, et un qui l'en retire. Quand quelqu'un envoie un SMS à votre numéro SMSEagle avec l'un de ces mots-clés, son numéro de téléphone est automatiquement ajouté ou retiré du groupe. Vous pouvez ensuite envoyer des messages à ce groupe à partir de Compose, de l'API ou du courrier électronique vers SMS.

Usages typiques : une liste d'alerte publique à laquelle les résidents peuvent s'inscrire, ou une liste de notifications de quart de travail à laquelle le personnel peut s'inscrire lui-même sans intervention d'un administrateur.

Avant de commencer

Créez le groupe auquel les gens s'abonneront :

1. Allez à **Phonebook > Groups**.
2. Cliquez sur **Add new**, donnez un nom au groupe et cochez **Set as Public Group**.
3. Cliquez sur **Save**.

Seuls les groupes **publics** peuvent être utilisés dans une règle d'abonnement.

Vous devez également indiquer à vos utilisateurs quel numéro envoyer et quel mot-clé envoyer. SMSEagle ne le fait pas savoir automatiquement.

Étape 1 : Ouvrir la page Abonnements

Dans la barre latérale, allez à **Automation > SMS > Subscriptions**.

Étape 2 : Créer une règle

Cliquez sur **Create new rule** dans le coin supérieur droit. Un panneau latéral s'ouvre. Remplissez les champs :

Rule name Quelque chose que vous reconnaîtrez, par exemple `Flood alerts opt-in`. Maximum 100 caractères.

Groups Commencez à taper et sélectionnez un ou plusieurs groupes. Les abonnés sont ajoutés à, ou retirés de, **tous** les groupes répertoriés ici. Seuls les groupes publics peuvent être sélectionnés.

Ajouter le numéro de téléphone aux groupes, quand le message entrant est égal à Le mot-clé qui abonne quelqu'un, par exemple `JOIN` ou `START ALERTS`. Le mot-clé doit être unique à la règle d'abonnement.

Remove phone number from groups, when incoming message equals Le mot-clé qui désabonne quelqu'un, par exemple `STOP` ou `LEAVE`.

Case sensitive Laissez cette case décochée pour que `join`, `Join` et `JOIN` fonctionnent tous. Cochez-la uniquement si vous avez besoin que le mot-clé corresponde exactement tel que tapé.

Cliquez sur **Save**.

Comment fonctionne la correspondance

C'est le détail le plus important à communiquer à vos utilisateurs :

> Le message entrant complet doit être **exactement** le mot-clé. Rien d'autre ne peut être dans le message.

Le mot-clé est `JOIN`	Résultat
L'utilisateur envoie `JOIN`	Abonné
L'utilisateur envoie `join`	Abonné (sauf si **Case sensitive** est coché)
L'utilisateur envoie `Please JOIN me`	Rien ne se passe
L'utilisateur envoie `JOIN ALERTS`	Rien ne se passe

Pour cette raison, conservez les mots-clés courts et faciles à taper, et demandez à vos utilisateurs d'envoyer uniquement le mot-clé.

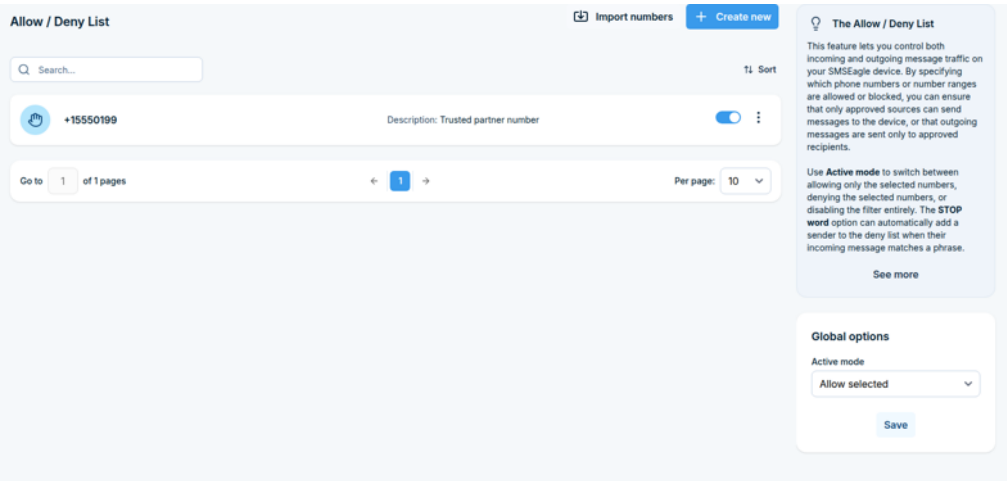
Ce qui se passe quand quelqu'un s'abonne

- Si le numéro de téléphone de l'expéditeur **est déjà dans l'Annuaire**, ce contact existant est ajouté au groupe.
- Si le numéro **n'est pas dans l'Annuaire**, SMSEagle crée automatiquement un nouveau contact. Le contact est nommé d'après la règle et le numéro de téléphone, par exemple `Flood alerts opt-in +48111222333`, et il est créé en tant que contact privé.

Quand quelqu'un se désabonne, il est supprimé du groupe, mais le contact lui-même est conservé dans l'Annuaire.

Vous pouvez consulter à tout moment qui s'est abonné : allez à **Phonebook > Groups**, trouvez le groupe et ouvrez **Manage contacts**.

Liste d'autorisation / d'interdiction



Options globales de la liste d'autorisation / d'interdiction

Ce que fait cette fonctionnalité

La liste d'autorisation / d'interdiction filtre le trafic SMS sur votre appareil par numéro de téléphone.

Vous conservez une liste de numéros et choisissez comment l'appareil la traite :

Mode actif	Ce qui se passe
Allow selected	Seuls les numéros de la liste sont acceptés. Tout le reste est ignoré.
Deny selected	Les numéros de la liste sont ignorés. Tout le reste est accepté.
Disabled	Aucun filtrage du tout. La liste est conservée mais non utilisée.

Usages typiques : bloquer un numéro qui ne cesse de bombarder l'appareil (Deny), ou verrouiller une passerelle de sorte que seuls vos propres systèmes d'alarme puissent communiquer avec elle (Allow).

Il y a aussi une option **STOP word** qui ajoute automatiquement un expéditeur à la liste quand son message correspond à une phrase que vous définissez. C'est ce qui fait fonctionner un mot-clé de désabonnement tel que `STOP`.

Avant de commencer

Décidez dans quel sens vous voulez travailler. **Allow selected** et **Deny selected** utilisent deux listes séparées, les règles que vous ajoutez dans un mode ne sont donc pas visibles dans l'autre. Le changement de mode change toute la liste, il ne l'inverse pas.

Étape 1 : Ouvrir la page Liste d'autorisation / d'interdiction

Dans la barre latérale, allez à **Automation > General > Allow / Deny List**.

Sur le côté droit se trouve une boîte **Global options** contenant le paramètre **Active mode** et la configuration **STOP word**. Les deux sont décrits ci-dessous.

Étape 2 : Choisir le mode actif

Dans la boîte **Options globales**, définissez **Mode actif** sur **Autoriser la sélection**, **Refuser la sélection** ou **Désactivé**, puis cliquez sur **Enregistrer**. La page se recharge en affichant la liste correspondant au mode que vous avez choisi.

> Lorsque le mode est **Désactivé**, la page affiche un avis « Filtrage désactivé » au lieu de la liste, et les règles ne peuvent pas être ajoutées ou modifiées. Basculez vers **Autoriser la sélection** ou **Refuser la sélection** pour les gérer à nouveau.

Étape 3 : Ajouter un numéro

Cliquez sur **Create new** dans le coin supérieur droit. Un panneau latéral s'ouvre.

Phone number Le numéro auquel cette règle s'applique. Maximum 15 caractères. Seuls les chiffres, `+` et `*` sont autorisés, et l'entrée doit contenir au moins un chiffre.

Vous pouvez faire correspondre une plage entière de numéros en utilisant * comme caractère générique, qui représente n'importe quels caractères :

Modèle	Correspondances
`NUMBER`	Exactement ce numéro
`*NUMBER`	Tout numéro se terminant par celui-ci
`NUMBER*`	Tout numéro commençant par celui-ci
`*NUMBER*`	Tout numéro le contenant

Par exemple, `48512*` couvre tous les numéros commençant par `48512`, et `*12345678` correspond au même abonné quel que soit le format du préfixe pays qui arrive.

Description Une brève note expliquant pourquoi le numéro est sur la liste, par exemple `Spam` ou `Panneau d'alarme, siège social`. Obligatoire, maximum 255 caractères.

Cliquez sur **Save**.

Étape 4 : Importer une liste à partir d'un CSV

Si vous avez déjà les numéros dans une feuille de calcul, cliquez sur **Import rules** dans le coin supérieur droit au lieu de les ajouter un par un.

1. Préparez un fichier CSV encodé en UTF-8 avec exactement deux colonnes, intitulées **Number** et **Reason**.
2. Cliquez sur **Import rules**, déposez le fichier dans la zone de téléchargement ou cliquez dessus pour parcourir.
3. Cliquez sur **Import**.

Les numéros sont ajoutés à la liste actuellement active.

Étape 5 : Configurer le mot STOP (optionnel)

Le mot STOP ajoute automatiquement les expéditeurs à la liste, permettant aux personnes de refuser en envoyant un mot-clé par SMS.

Dans la boîte **Options globales**, cliquez sur **Edit config** à côté de **STOP word**. Un panneau latéral s'ouvre. Choisissez **Ajouter automatiquement le numéro à la liste quand** :

Option	Ce que cela signifie
Never	Le mot STOP est désactivé. Les numéros ne sont ajoutés que manuellement ou par importation.
Incoming message equals to…	Le message entier doit être exactement la phrase que vous tapez.
Le message entrant contient…	La phrase peut apparaître n'importe où dans le message.

Si vous choisissez l'une des deux options de correspondance, deux champs supplémentaires apparaissent :

- La phrase elle-même, maximum 160 caractères, par exemple `STOP`.
- **Message de réponse automatique**, maximum 160 caractères. Ce texte est envoyé au numéro après son ajout à la liste. Laissez vide si vous ne souhaitez pas confirmer le refus.

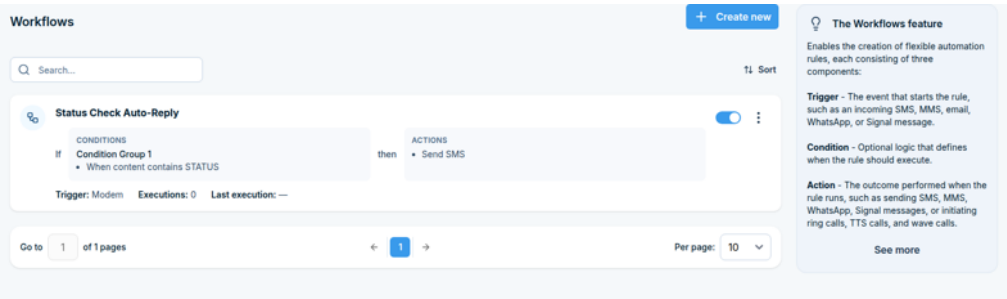
Cliquez sur **Save**. Le résumé dans la boîte **Global options** affiche maintenant la condition active et le texte de la réponse automatique.

> **Utilisez « equals » plutôt que « contains » pour les mots-clés de refus.** Avec **contains**, un message ordinaire tel que `please stop sending the night reports` supprimerait également l'expéditeur.

Fonctionnement du filtrage

- Le filtre s'applique aux messages arrivant après la création et l'activation de la règle. Il ne retraite pas les messages déjà dans la boîte de réception.
- Une règle désactivée est complètement ignorée, quel que soit le mode actif.
- **Allow selected** et **Deny selected** conservent des listes séparées. Si vous changez le mode et que la page semble vide, vous regardez l'autre liste, rien n'a été supprimé.
- Le paramètre de mot STOP est **global** : il s'applique à la liste actuellement active.

Workflows



Aperçu des workflows

Les workflows vous permettent de créer des règles d'automatisation flexibles sans avoir besoin d'une intégration séparée pour chaque combinaison de déclencheur et d'action. Chaque workflow comprend trois parties :

- **Trigger** - l'événement qui démarre la règle : un message SMS, MMS, e-mail, WhatsApp ou Signal entrant (ou un événement de livraison/envoi/erreur d'envoi du modem).
- **Condition** - logique optionnelle qui détermine si la règle doit s'exécuter pour un événement donné.
- **Action** - ce qui se passe quand la règle s'exécute : envoi d'un message SMS, MMS, WhatsApp ou Signal, ou lancement d'un appel ring, d'un appel TTS ou d'un appel wave.

Où la trouver

Automation > General > Workflows (`/automation/workflows/`).

Étape 1 : Créer un workflow et choisir un déclencheur

Cliquez sur **Create new**, donnez un **Name** au workflow et choisissez un **Trigger** : Modem, Email, Signal, WhatsApp, Modem (delivered), Modem (sent), ou Modem (sending error).

Étape 2 : Ajouter des groupes de conditions (optionnel)

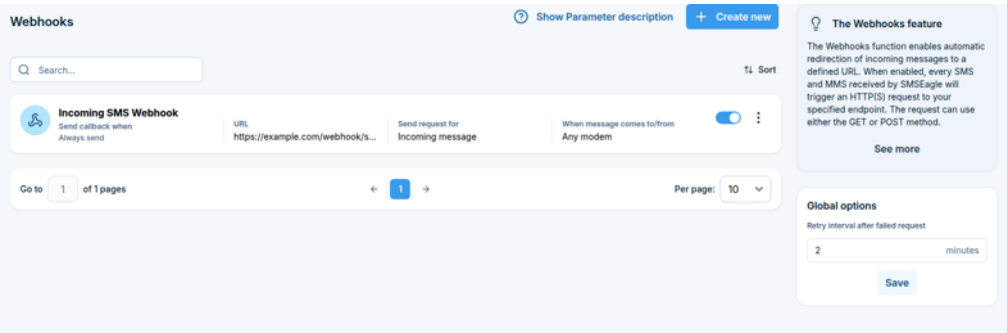
Sous **Condition groups**, cliquez sur **Add group** pour ajouter une ou plusieurs conditions que l'événement entrant doit respecter avant l'exécution du workflow. Laissez vide si le workflow doit s'exécuter pour chaque événement correspondant au déclencheur.

Étape 3 : Ajouter des actions

Sous **Actions**, cliquez sur **Add action** pour définir ce que fait le workflow quand il s'exécute - par exemple envoyer une réponse, transférer le message vers un autre canal ou passer un appel.

Cliquez sur **Save workflow** pour l'activer.

Webhooks



Aperçu des webhooks

Ce que fait cette fonctionnalité

Un webhook fait appeler **votre** système par SMSEagle. Chaque fois que quelque chose se produit sur l'appareil (un message arrive, un message est envoyé, un accusé de livraison revient, un appel entre), l'appareil envoie une requête HTTP(S) à une URL de votre choix, en incluant les détails en tant que paramètres.

C'est ainsi que vous poussez le trafic SMS dans un système de tickets, un CRM, un chatbot ou votre propre application sans interroger l'API.

Deux intégrations bénéficient d'un support dédié :

Méthode	À quoi ça sert
POST (3CX)	Pousser des messages dans un système téléphonique 3CX.
POST (Zabbix)	Accuser réception des événements Zabbix par SMS, pour qu'un ingénieur puisse répondre `ACK 12345` pour fermer une alerte.

Avant de commencer

- Vous avez besoin de l'URL qui recevra les requêtes, accessible depuis l'appareil. Les adresses locales et privées sont rejetées.
- Votre endpoint doit répondre avec HTTP **200 OK**, ou avec les codes de statut que vous configurez dans la règle.
- Pour Zabbix, vous avez besoin soit d'un jeton API (Zabbix 6.4 et plus récent), soit d'un nom d'utilisateur et d'un mot de passe.

Étape 1 : Ouvrir la page Webhooks

Dans la barre latérale, allez à **Automation > General > Webhooks**.

Chaque règle affiche son URL et ce qui la déclenche. Chaque règle dispose d'un commutateur pour l'"**activer ou la désactiver**, d'une action **Edit** et d'une action **Delete**.

La boîte **Global options** sur la droite contient un paramètre qui s'applique à toutes les règles, décrit dans Étape 6.

Étape 2 : Créer une règle

Cliquez sur **Create new** dans le coin supérieur droit. Le formulaire webhook s'ouvre en tant que page complète avec trois sections.

Étape 3 : Configuration de base

Champ	Ce qu'il faut entrer
Rule name	Un nom descriptif, maximum 100 caractères.
URL	L'adresse à appeler, maximum 300 caractères, par exemple `https://example.com/webhook`.
URL method	**GET**, **POST**, **POST (3CX)** ou **POST (Zabbix)**.
Content type	Seulement pour **POST** simple : **FormData** ou **JSON**.
To (3CX)	Seulement pour **POST (3CX)** : la destination dans votre système 3CX.

Cliquez sur **Test connection** à côté de l'URL pour envoyer une requête d'exemple immédiatement. Le résultat s'affiche sous le champ et vous indique le statut HTTP reçu, ce qui vous permet de confirmer que le point de terminaison fonctionne avant d'enregistrer.

Pour **GET** et **POST**, un exemple de la chaîne de requête s'affiche sous les champs, ce qui vous permet de voir exactement ce que votre point de terminaison recevra.

Contenu de la requête

La requête que votre point de terminaison reçoit contient les détails de l'événement en tant que paramètres. Certains sont envoyés pour chaque événement, d'autres uniquement pour les messages ou uniquement pour les appels.

Toujours envoyé

Paramètre	Contenu
`sender`	Numéro de l'expéditeur.
`timestamp`	Moment où SMSEagle a reçu ou envoyé le message, au format `YYYYmmddHHiiss`, par exemple `20140531092257`.
`msgid`	L'identifiant du message SMSEagle.
`modemno`	Le modem sur lequel le message entrant a été reçu, ou celui à partir duquel le message a été envoyé.
`apikey`	La clé API de votre service, si vous en avez défini une dans les **Security settings**. Facultatif.

Envoyé uniquement pour SMS et MMS

Paramètre	Contenu
`text`	Contenu du message SMS.
`text_binary`	Contenu binaire du message SMS.
`status`	Statut du message.
`oid`	Valeur de l'identifiant OID assigné à un message sortant avec un numéro de téléphone correspondant. Facultatif.
`attachments`	Pièces jointes MMS, par exemple `[0 => [name => image.png, content-type => image/png, content => wfFWgwOlgBRwdWvsvs=]]`. **POST only**, car une chaîne de requête GET ne peut pas contenir de données de fichier. Facultatif.

Envoyé uniquement pour les appels vocaux entrants

Paramètre	Contenu
`status`	Statut de l'appel entrant : `accepted`, `rejected` ou `ignored`.

Une règle se déclenche pour un seul type d'événement, donc une requête ne contient que les paramètres de ce type. Une règle avec le déclencheur **Incoming call**, par exemple, n'envoie jamais `text` ou `attachments`.

Quelle que soit la méthode, SMSEagle attend que votre endpoint réponde avec **200 [OK]**, sauf si vous l'élargissez avec **Expected HTTP Status Code(s)** dans les Paramètres de sécurité.

Le lien **Show Parameter description** sur la page des règles ouvre cette même liste dans l'application, ainsi qu'un exemple de requête GET :

```
?
sender=48601123123&timestamp=20140531092257&msgid=431&modemno=1&text=This+is+an+incoming+message
```

Personnalisation des noms de paramètres

Par défaut, la requête utilise les noms de paramètres SMSEagle énumérés ci-dessus. Si votre endpoint en attend d'autres, cochez **Customize parameter names** et tapez votre propre nom à côté de chaque paramètre que vous souhaitez renommer. Tous les paramètres des trois tableaux peuvent être renommés ; ceux que vous laissez vides conservent leur nom par défaut.

Le renommage modifie uniquement le **nom** du paramètre dans la requête, jamais sa valeur ou le moment où il est envoyé.

Étape 4 : Conditions de déclenchement

Send request for décide quel événement déclenche le webhook :

Option	Se déclenche quand
Incoming message	Un SMS ou MMS arrive.
Sent message	Un message sortant a été envoyé.
Delivery report	Un rapport de livraison revient.
Sending error	Un message sortant a échoué.
Incoming call	Un appel arrive.

Send request when affine davantage :

Option	Ce que cela signifie
Always	Chaque événement du type choisi déclenche le webhook.
For specified senders / when text contains	Seuls les événements correspondant aux conditions ci-dessous le déclenchent.

Si vous avez choisi la deuxième option, deux conditions deviennent disponibles. Vous pouvez en utiliser une ou les deux, et un événement doit satisfaire chaque condition que vous activez.

When incoming SMS comes from Cochez cette case et sélectionnez les contacts ou groupes. Seuls les contacts et groupes publics sont acceptés.

When incoming SMS text contains Cochez cette case et tapez la phrase. Cochez **Case sensitive** si la casse des majuscules et minuscules doit être traitée comme différente. Cette condition n'est pas disponible pour le déclencheur **Incoming call**, car un appel n'a pas de texte.

Étape 5 : Paramètres de sécurité

Champ	Fonction
API key of your service	Une clé optionnelle envoyée avec la requête, pour que votre endpoint puisse vérifier que l'appel provient vraiment de votre appareil.
Code(s) de statut HTTP attendu(s)	Quelles réponses comptent comme un succès. Un ou plusieurs codes à trois chiffres séparés par des virgules, par exemple `200,201,202`. La valeur par défaut est `200`, maximum 20 caractères.
Accepter un certificat SSL auto-signé	Accepter un certificat qui n'est pas signé par une autorité publique.
Vérifier le pair	Vérifier le certificat du serveur.
Vérifier le nom du pair	Vérifier que le certificat correspond au nom d'hôte.

Tout ce qui ne correspond pas aux codes de statut attendus compte comme une requête échouée et est réessayé selon l'intervalle de nouvelle tentative global.

Règles Zabbix

Si vous avez choisi **POST (Zabbix)** comme méthode, des champs supplémentaires apparaissent :

- **Action Zabbix** - **Acknowledge (ACK)**, **Unacknowledge (NOACK)** ou les deux. Le panneau affiche le format SMS que l'appareil attendra, par exemple `ACK 12345 Problem resolved`.
- **Type d'authentification** - **Token API** (Zabbix 6.4 et plus récent, recommandé) ou **Login/Password** pour les versions plus anciennes. Avec un token vous l'entrez dans le champ Clé API ; avec une connexion vous entrez **Nom d'utilisateur Zabbix** et **Mot de passe Zabbix**.
- **Valeurs de test** - un **Event ID** et un **Message** utilisés uniquement par **Test connection**, jamais enregistrés.

Cliquez sur **Save webhook**.

Étape 6 : Définir l'intervalle de nouvelle tentative

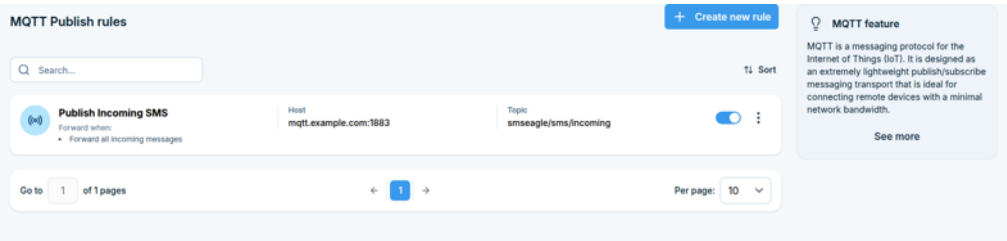
La boîte **Global options** sur la page des règles contient **Retry interval after failed request**, en minutes. Quand une requête échoue, l'appareil attend ce laps de temps avant de réessayer.

Entrez un nombre entier de minutes et cliquez sur **Save**. Le paramètre est **global** : il s'applique à chaque règle webhook sur l'appareil.

Comportement des webhooks

- Les règles s'appliquent aux événements qui se produisent après la création et l'activation de la règle. Elles ne rejouent pas les messages passés.
- La condition de texte est une correspondance **contains**, pas une correspondance exacte.
- Si plusieurs règles correspondent au même événement, **chacune d'elles** envoie sa propre requête, ainsi un message peut atteindre plusieurs endpoints.
- Une requête compte comme réussie uniquement si le statut de la réponse est l'un des **Code(s) de statut HTTP attendu(s)**. Tout ce qui est différent, y compris l'absence de réponse, est un échec et est réessayé.
- **Test connection** envoie un exemple de charge utile, pas un vrai message, donc il est sûr de l'exécuter contre un endpoint de production qui ne fait que consigner.

MQTT



Règles de publication MQTT

Ce que fait cette fonctionnalité

MQTT est le protocole de messagerie utilisé par la plupart des appareils IoT, des capteurs et des systèmes d'automatisation de bâtiments. Les appareils envoient des messages courts à un **broker**, chacun étiqueté avec une **rubrique** telle que `building/boiler/temperature`. Quiconque connecté au broker peut écouter les rubriques qui l'intéressent.

SMSEagle se tient des deux côtés de cette conversation :

Type de règle	Direction	Fonction
S'abonner	MQTT vers SMS	Écoute un courtier et convertit les messages MQTT entrants en messages SMS envoyés à vos utilisateurs.
Publier	SMS vers MQTT	Prend les messages SMS entrants et les publie sur un courtier, afin que votre système IoT puisse y réagir.

Utilisations typiques : convertir une alarme de capteur en SMS pour l'équipe de maintenance (S'abonner), ou permettre à un technicien d'envoyer un message texte qui est capté par le système d'automatisation (Publier).

Les deux types de règles sont configurés séparément et ne dépendent pas l'un de l'autre. Utilisez celui dont vous avez besoin.

Avant de commencer

Vous avez besoin des détails de connexion de votre courtier MQTT : adresse d'hôte, port et nom d'utilisateur et mot de passe si le courtier les exige - configurés une seule fois sous MQTT dans Paramètres, avant de rédiger des règles S'abonner ici.

Pour les règles **S'abonner**, vous avez également besoin de la liste des rubriques à écouter (également définie dans Paramètres). Pour les règles **Publier**, vous avez besoin de la rubrique sur laquelle publier (définie par règle, ci-dessous).

Partie 1 : S'abonner (MQTT vers SMS)

Les règles S'abonner convertissent les messages MQTT entrants en SMS, une fois que la connexion du courtier elle-même est configurée sous Paramètres.

Étape 1 : Ouvrir la page des règles S'abonner

Dans la barre latérale, allez à **Automation > General > MQTT**, puis choisissez **Subscribe**.

Étape 2 : Créer une règle S'abonner

Cliquez sur **Create new rule** dans le coin supérieur droit. Un panneau latéral s'ouvre.

Nommer la règle

Dans **Rule name**, tapez quelque chose de descriptif, par exemple `Boiler alarm to maintenance`. Maximum 100 caractères.

Décidez quels messages MQTT traiter

Choisissez **Forward for** :

Option	Ce que cela signifie
Any message	Chaque message MQTT reçu par l'appareil déclenche cette règle.
Specified topic / message	Seuls les messages correspondant aux conditions que vous définissez ci-dessous la déclenchent.

Si vous avez choisi **Specified topic / message**, deux conditions deviennent disponibles. Vous pouvez en utiliser une ou les deux. Lorsque vous en utilisez les deux, un message doit satisfaire **les deux**.

When incoming message has topic Cochez cette case et tapez la rubrique dans **Topic**, par exemple `building/boiler`.

When incoming message contains Cochez cette case et tapez la phrase dans **Message phrase**, par exemple `ALARM`. Cochez **Case sensitive** si `alarm` et `ALARM` doivent être traités comme différents.

Choisissez les destinataires

Dans **Forward to**, sélectionnez les contacts ou groupes qui doivent recevoir le SMS. Seuls les contacts et groupes **publics** peuvent être sélectionnés ici. Ce champ est obligatoire.

Rédiger le texte du SMS

Message format contrôle ce que le SMS dit. Vous le construisez à partir du message MQTT en utilisant des espaces réservés :

Espace réservé	Remplacé par
`{TOPIC}`	Le sujet sur lequel le message MQTT est arrivé
`{MESSAGE}`	Le contenu du message MQTT

La valeur par défaut est `{TOPIC}: {MESSAGE}`, qui génère un SMS comme `building/boiler/temperature: 94`. Vous pouvez aussi composer votre propre phrase autour d'eux, par exemple `Boiler warning on {TOPIC}, value {MESSAGE}`.

Cochez **Send as Unicode** si le texte contient des caractères en dehors de l'alphabet GSM standard, comme des lettres polonaises, allemandes ou cyrilliques.

Options avancées

Cliquez sur **Advanced options** pour développer cette section. Vous n'en avez pas besoin pour une configuration de base.

- **Call after sending SMS** - place aussi un appel vocal aux mêmes destinataires. Les options sont **No**, **Ring only**, **Yes - text to speech** et **Yes - text to speech (advanced)**, selon ce que supporte le modèle de votre appareil. Avec l'option avancée, vous sélectionnez aussi un **Voice model**.

Cliquez sur **Save**. La règle commence à fonctionner sur les messages MQTT reçus à partir de ce moment.

Comment fonctionne la correspondance d'abonnement

- La condition **Topic** est une correspondance **contains** et ignore la casse. Une règle avec le sujet `boiler` correspond aussi à `building/boiler/temperature`.
- La case à cocher **Case sensitive** s'applique uniquement à la phrase du message, jamais au sujet.
- Si plusieurs règles d'abonnement correspondent au même message MQTT, **chacune** d'elles envoie son propre SMS.

Partie 2 : Publish (SMS dans MQTT)

Les règles Publish n'utilisent **pas** les paramètres du service MQTT sous Settings. Chaque règle porte sa propre connexion au courtier, donc différentes règles peuvent publier sur des courtiers différents.

Étape 1 : Ouvrir la page des règles Publish

Dans la barre latérale, allez à **Automation > General > MQTT**, puis choisissez **Publish**.

Étape 2 : Créer une règle Publish

Cliquez sur **Create new rule** dans le coin supérieur droit. Un panneau latéral s'ouvre.

Nommer la règle

Dans **Rule name**, tapez quelque chose de descriptif, par exemple `Technician commands to automation`. Maximum 100 caractères.

Décidez quels messages SMS publier

Choisissez **Forward for** :

Option	Ce que cela signifie
Any message	Chaque SMS entrant est publié sur le courtier.
Specified sender / message	Seuls les messages correspondant aux conditions que vous définissez ci-dessous sont publiés.

Si vous avez choisi **Specified sender / message**, les conditions ci-dessous deviennent disponibles. Vous pouvez les combiner, et un message doit alors satisfaire tous ceux que vous activez.

When incoming SMS comes from Cochez cette case et sélectionnez les contacts ou groupes d'expéditeurs. Seuls les contacts et groupes **public** peuvent être sélectionnés ici.

When incoming SMS text contains Cochez cette case et tapez la phrase dans **Text fragment**. Cochez **Case sensitive** si la casse doit être traitée différemment.

> Restreindre une règle Publish par expéditeur est une précaution judicieuse. Sans une condition d'expéditeur, n'importe qui connaissant votre numéro peut injecter du contenu dans votre système IoT.

Entrez la connexion au courtier

Remplissez le courtier sur lequel cette règle publie :

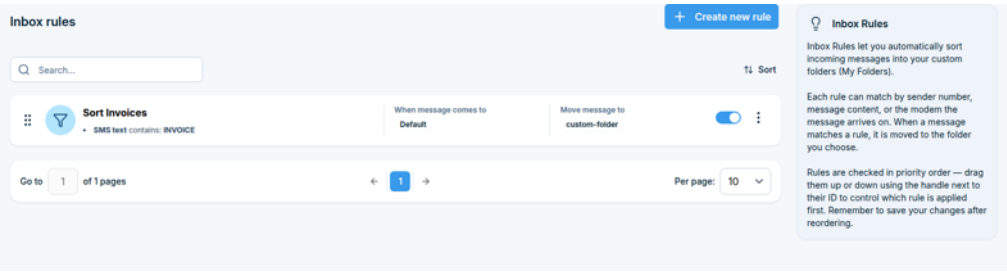
Champ	Ce qu'il faut entrer
Host	L'adresse du courtier, par exemple `test.host.io`
Port	Le port du courtier, par exemple 1883. La plage autorisée est de 1 à 65535.
Nom d'utilisateur	L'utilisateur du courtier, si requis. Laissez vide pour un courtier ouvert.
Mot de passe	Le mot de passe du courtier, si requis.
Sujet	Le sujet sur lequel publier, par exemple `smseagle/incoming`
TLS/SSL	Activez si le courtier utilise une connexion chiffrée.
Vérification du certificat TLS	Laissez activé sauf si le courtier utilise un certificat auto-signé que l'appareil ne peut pas valider.

Cliquez sur **Save**. Les messages SMS entrants qui correspondent à la règle sont maintenant publiés.

Comment fonctionne la correspondance Publish

- La condition de texte est une correspondance **contains**, pas une correspondance exacte.
- Si plusieurs règles Publish correspondent au même SMS, **chacune d'elles** publie, de sorte que le message peut atterrir sur plusieurs courtiers ou sujets.
- Les règles s'appliquent uniquement aux messages arrivant après la création et l'activation de la règle. Elles ne traitent pas les messages déjà dans la boîte de réception.

Règles de la boîte de réception



Aperçu des règles de la boîte de réception

Les règles de la boîte de réception trient automatiquement les messages entrants dans vos dossiers personnalisés (Mes dossiers), au lieu de tout laisser dans la boîte de réception principale.

Où la trouver

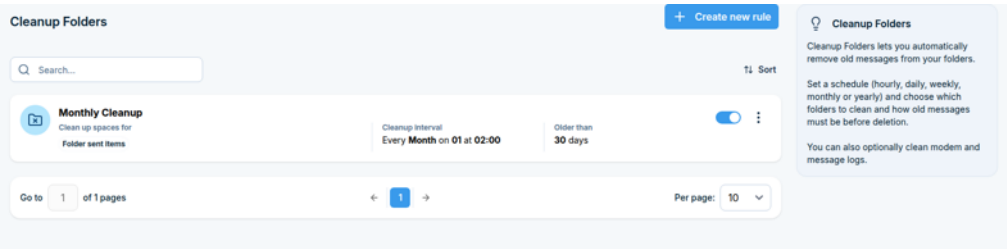
Automation > Folders > Inbox Rules (`/automation/inbox-rules/`).

Configuration d’une règle de boîte de réception

Cliquez sur **Create new rule**. Chaque règle peut correspondre par numéro d’expéditeur, contenu du message ou modem sur lequel le message est arrivé ; un message correspondant à la règle est déplacé vers le dossier que vous choisissez.

Les règles sont vérifiées par ordre de priorité. Faites glisser une règle vers le haut ou vers le bas à l’aide de la poignée à côté de son ID pour contrôler quelle règle est appliquée en premier, et n’oubliez pas d’enregistrer vos modifications après réorganisation.

Nettoyage des dossiers



Aperçu du nettoyage des dossiers

Le nettoyage des dossiers supprime automatiquement les anciens messages de vos dossiers, afin qu’ils ne s’accumulent pas indéfiniment.

Où la trouver

Automation > Folders > Cleanup Folders (`/automation/cleanup-folders/`).

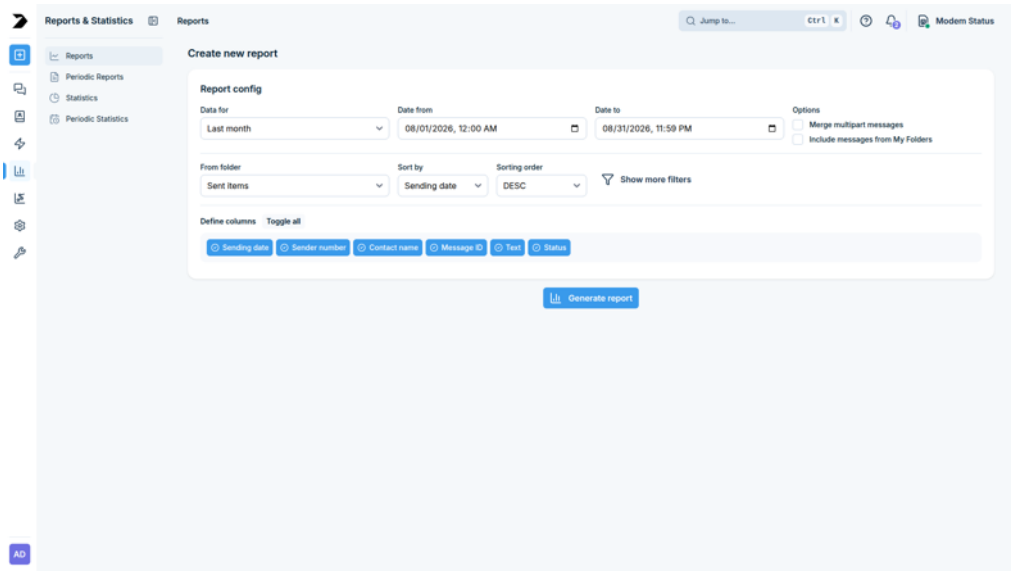
Configuration d’une règle de nettoyage

Cliquez sur **Create new rule**, puis définissez un calendrier (horaire, quotidien, hebdomadaire, mensuel ou annuel), choisissez les dossiers à nettoyer et l’ancienneté d’un message avant sa suppression. Vous pouvez également nettoyer les journaux des modems et des messages selon le même calendrier.

Rapports et statistiques

Ce chapitre couvre la section **Rapports et statistiques** de l'interface web - exporter les données de messages sous forme de rapport ponctuel ou planifier des rapports à envoyer automatiquement par e-mail.

Rapports



Créer un rapport

Rapports et statistiques > Rapports (`/reports/`) crée un rapport ponctuel de l'historique de vos messages.

Sous **Config du rapport**, choisissez la plage horaire avec **Données pour** (une plage prédéfinie telle que Aujourd'hui, 7 derniers jours ou Ce mois, ou **Plage personnalisée** avec les champs *Date du / Date au explicites).

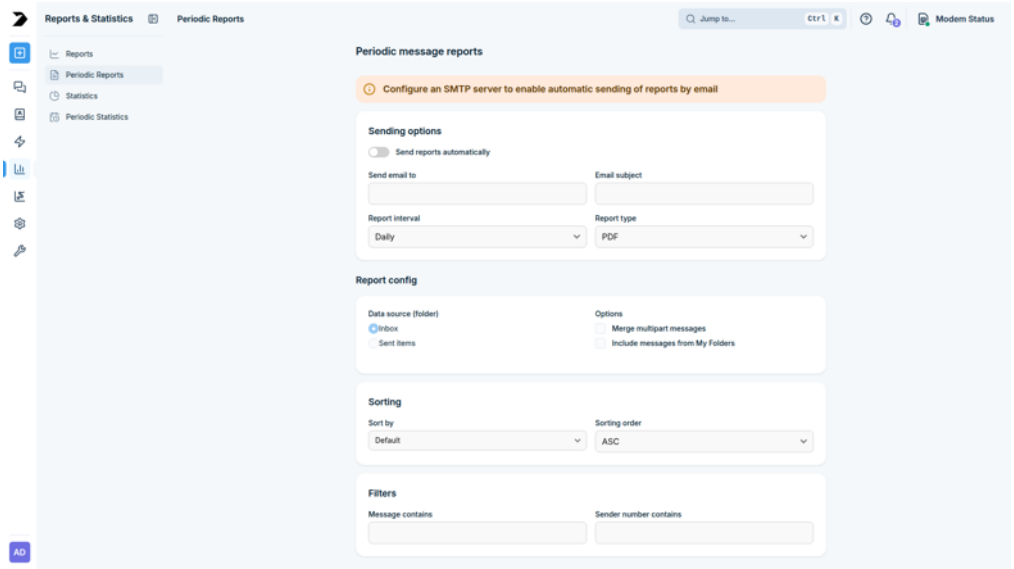
Sous **Options** :

Option	Ce qu'elle fait
Fusionner les messages en plusieurs parties	Combine un long SMS divisé en plusieurs parties en une seule ligne.
Inclure les messages de Mes dossiers	Inclut également les messages qui ont été déplacés dans un dossier personnalisé.
À partir du dossier	Dossier à inclure dans le rapport : **Éléments envoyés**, **Boîte de réception** ou **Boîte d'envoi**.
Trier par / **Ordre de tri**	Colonne à trier (date d'envoi, numéro de l'expéditeur, nom du contact, ID du message, texte ou statut) et direction (ASC/DESC).

Cliquez sur **Afficher plus de filtres** pour un filtrage supplémentaire, et utilisez **Définir les colonnes** pour choisir quelles colonnes apparaissent dans le rapport généré - **Tout basculer** sélectionne ou désactive toutes les colonnes à la fois.

Cliquez sur **Générer un rapport** pour le produire.

Rapports périodiques



Rapports de messages périodiques

Rapports et statistiques > Rapports périodiques (`/reports/periodic-reports`) planifie la génération et l'envoi automatique d'un rapport par e-mail de manière récurrente, au lieu de l'exécuter manuellement à chaque fois.

Cela nécessite une Configuration SMTP fonctionnelle - la page affiche un rappel pour en configurer une si elle est manquante.

Sous **Options d'envoi**, activez **Envoyer les rapports automatiquement** et remplissez :

Champ	Ce qu'elle fait
Envoyer le message à	L'adresse destinataire du rapport généré.
Sujet du message	La ligne d'objet de l'e-mail.
Intervalle de rapport	**Quotidien**, **Hebdomadaire** ou **Mensuel**.
Type de rapport	**PDF** ou **CSV**.

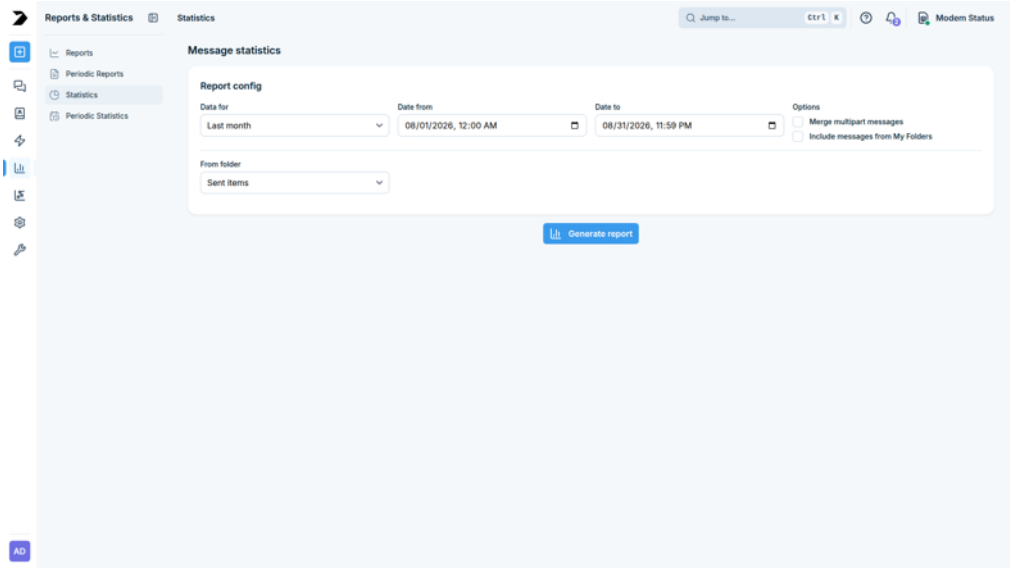
Sous **Report config**, choisissez la **Data source (folder)** (**Inbox** ou **Sent items**), les mêmes options **Merge multipart messages** / **Include messages from My Folders** qu'un rapport unique, et **Sorting** (champ de tri et ordre ASC/DESC).

Sous **Filters**, affinez le rapport avec **Message contains** et/ou **Sender number contains**.

Sous **Output**, utilisez **Select table columns** (avec un raccourci **Toggle all**) pour choisir les colonnes que le fichier généré inclut : date de réception, numéro de l'expéditeur, nom du contact, numéro du centre SMS, ID du message, texte, statut de lecture et ID du modem.

Cliquez sur **Save configuration**.

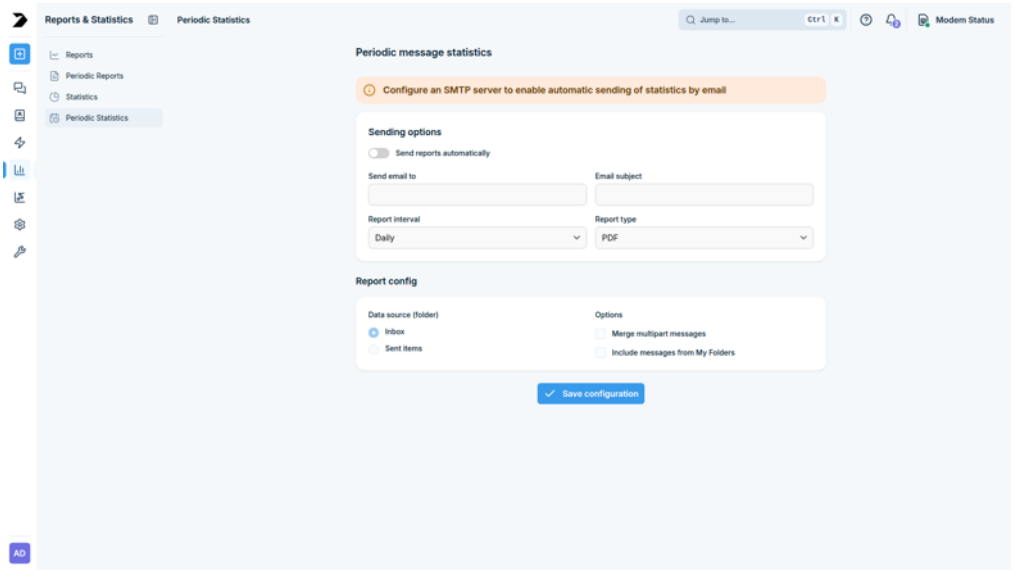
Statistiques



Statistiques des messages

Reports & Statistics > Statistics (`/reports/statistics`) fonctionne de la même manière que Reports ci-dessus - le même sélecteur de plage de temps **Data for** et les mêmes options **Merge multipart messages** / **Include messages from My Folders** / **From folder** - mais produit des statistiques de trafic agrégées au lieu d'une exportation une ligne par message. Cliquez sur **Generate report** pour la générer.

Statistiques périodiques



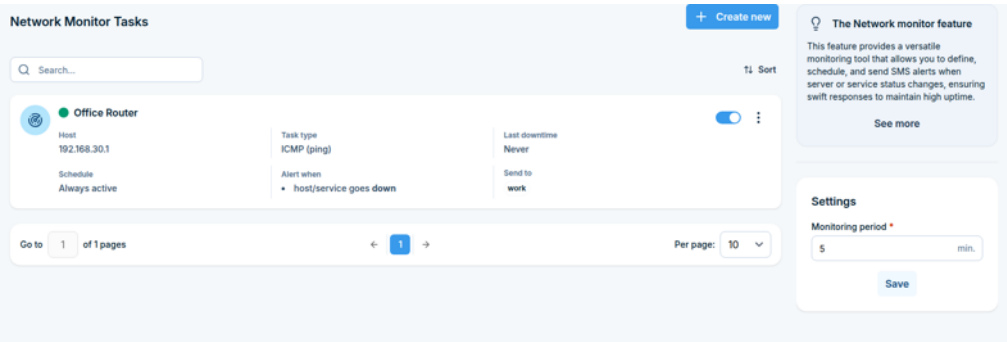
Statistiques de messages périodiques

Reports & Statistics > Periodic Statistics (`/reports/periodic-statistics`) planifie la génération automatique du rapport de statistiques ci-dessus et l'envoi par e-mail, de la même manière que Periodic Reports le fait pour l'exportation une ligne par message : il nécessite une SMTP Configuration fonctionnelle, et offre les mêmes **Sending options** (destinataire, objet, intervalle **Daily / Weekly / Monthly**, type de rapport **PDF / CSV**) plus une section **Report config** (dossier source de données, fusion des messages multipartites, inclusion de My Folders). Cliquez sur **Save configuration**.

Surveillance

Ce chapitre couvre la section **Surveillance** de l'interface web : vérification des hôtes et services externes, lecture des entrées/sorties numériques et des capteurs physiques.

Moniteur réseau



Présentation du Moniteur réseau

À quoi sert cette fonctionnalité

Le Moniteur réseau transforme votre SMSEagle en petite station de surveillance. Il vérifie les serveurs, appareils et services selon un calendrier et envoie un SMS quand quelque chose cesse de répondre, revient en ligne ou signale une valeur en dehors de la plage attendue.

Il se compose de trois parties :

Page	À quoi elle sert
Tasks	Les règles de surveillance : ce à vérifier, la fréquence, les personnes à alerter.
Reports	Un historique des indisponibilités, filtré par plage de dates et tâche, exportable en CSV.
SNMP Traps	Des règles qui transforment les traps SNMP envoyés vers l'appareil en messages SMS.

Utilisations typiques : alerte de l'ingénieur de garde quand un serveur de production cesse de répondre aux pings, avertissement concernant une lecture de température d'un capteur SNMP, ou renvoi d'un trap UPS vers un téléphone.

Avant de commencer

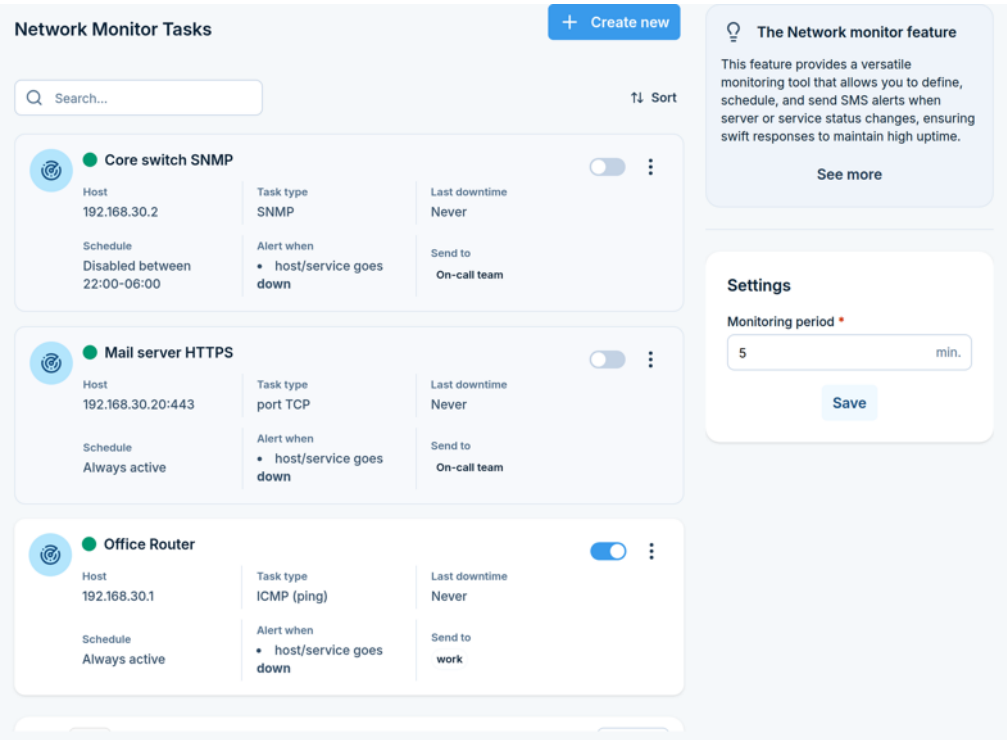
- L'appareil doit être capable de joindre les hôtes que vous souhaitez surveiller. Vérifiez d'abord les paramètres réseau sous **Settings > Network**.

- Les destinataires doivent être marqués comme **Public** dans le Carnet d'adresses si vous souhaitez alerter un groupe. Sinon, vous pouvez taper des numéros de téléphone simples dans la tâche.
- Pour les vérifications SNMP, vous avez besoin de la chaîne de communauté et de l'identifiant d'objet (OID) que vous souhaitez lire. Pour les vérifications Modbus, vous avez besoin de l'ID d'unité, du registre et du code de fonction.

Partie 1 : Tâches

Étape 1 : Ouvrir la page Tâches

Dans la barre latérale, accédez à **Monitoring > Network Monitoring > Tasks**.



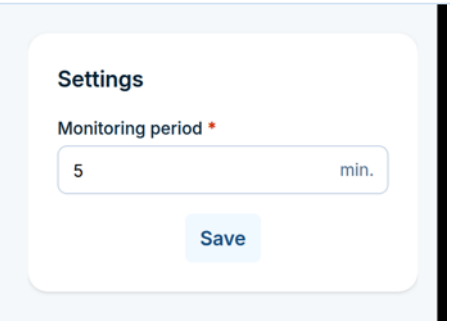
Tâches du Moniteur réseau

Chaque tâche de la liste affiche son hôte, son calendrier, le type de tâche, ce qu'elle alerte, quand elle a été dernièrement indisponible et qui elle notifie. Un marqueur vert ou rouge indique si l'hôte répond actuellement.

Étape 2 : Définir la période de surveillance

La boîte **Settings** à droite de la page Tâches contient un paramètre qui s'applique à **toutes** les tâches : **Monitoring period**, en minutes. C'est la fréquence à laquelle l'appareil exécute les vérifications.

Entrez une valeur et cliquez sur **Save**.



Période de surveillance

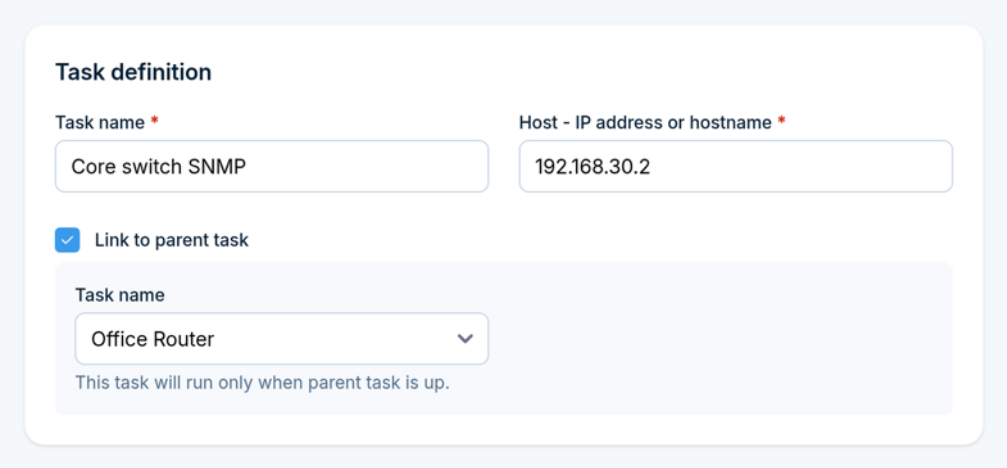
Étape 3 : Créer une tâche

Cliquez sur **Créer nouveau** dans le coin supérieur droit. Le formulaire de tâche s'ouvre en tant que page complète, divisée en cinq sections.

Définition de la tâche

Champ	Ce qu'il faut entrer
Nom de la tâche	Un nom descriptif, maximum 100 caractères, par exemple `Serveur de messagerie`.
Hôte - Adresse IP ou nom d'hôte	Ce à vérifier, par exemple `192.168.1.10` ou `mail.example.com`.
Lien vers la tâche parente	Cochez cette case pour rendre la tâche dépendante d'une autre.
Nom de la tâche (parent)	Affiché une fois la case cochée : la tâche dont celle-ci dépend.

Une tâche liée **s'exécute uniquement tandis que sa tâche parente est active**. Utilisez-la pour éviter les tempêtes d'alertes : si le routeur en face de dix serveurs s'arrête, seule la tâche du routeur génère une alerte, et les dix tâches des serveurs restent silencieuses.



Définition de la tâche

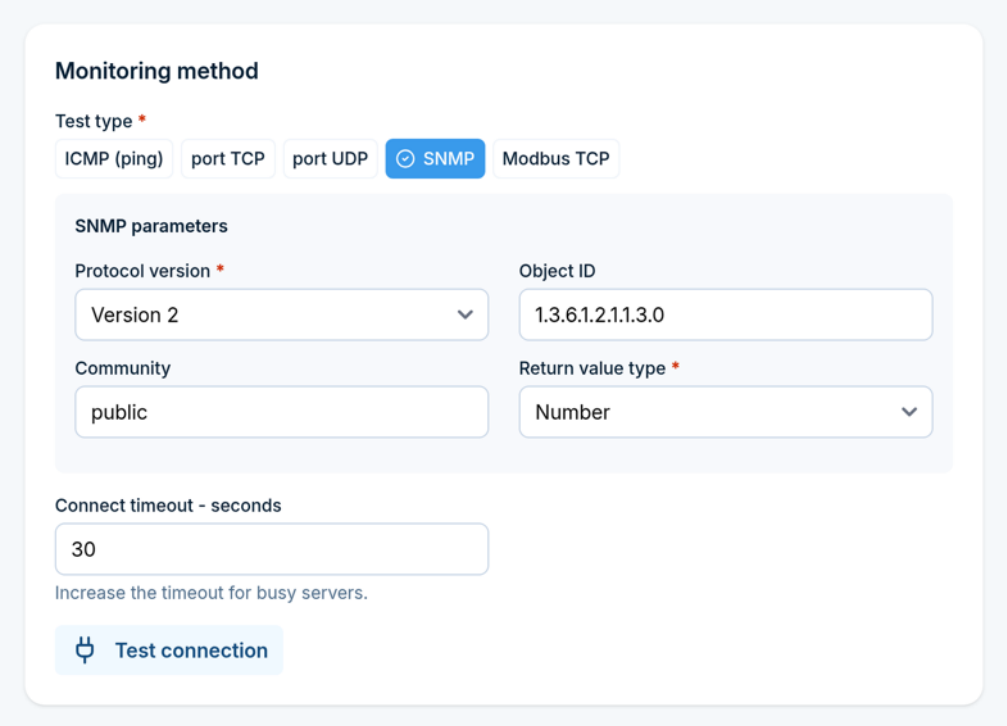
Méthode de surveillance

Choisissez le **Type de test**, puis remplissez les paramètres qui apparaissent pour celui-ci :

Type de test	Paramètres
ICMP (ping)	**Nombre de demandes** - combien de pings envoyer par vérification.
Port TCP	**Port** - le port TCP qui doit accepter une connexion.
Port UDP	**Port** - le port UDP à tester.
SNMP	**Version du protocole** (1 ou 2), **ID d'objet**, **Communauté**, **Type de valeur de retour** (Nombre ou Chaîne).
Modbus TCP	**Port**, **Identifiant unité**, **Registre**, **Code de fonction** (Lire les bobines, Lire les entrées discrètes, Lire les registres de maintien, Lire les registres d'entrée).

Délai de connexion - secondes s'applique à chaque type de test. Augmentez-le pour les serveurs occupés qui répondent lentement ; la valeur par défaut est 30 secondes.

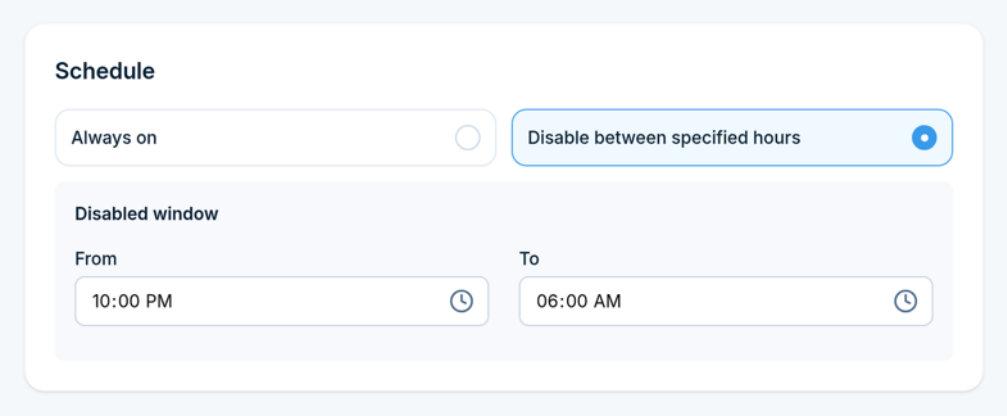
Cliquez sur **Test connection** pour essayer la vérification immédiatement. Le résultat s'affiche à côté du bouton, ce qui vous permet de confirmer que l'hôte répond avant d'enregistrer la tâche.



Méthode de surveillance

Calendrier

Choisissez **Always on** si la tâche doit s'exécuter 24 heures sur 24, ou **Disable between specified hours** et définissez **From** et **To** pour créer une fenêtre silencieuse, par exemple pendant une sauvegarde nocturne qui met toujours le service hors ligne.



Calendrier

Déclencheurs d'alerte

Choisissez d'abord qui reçoit l'alerte :

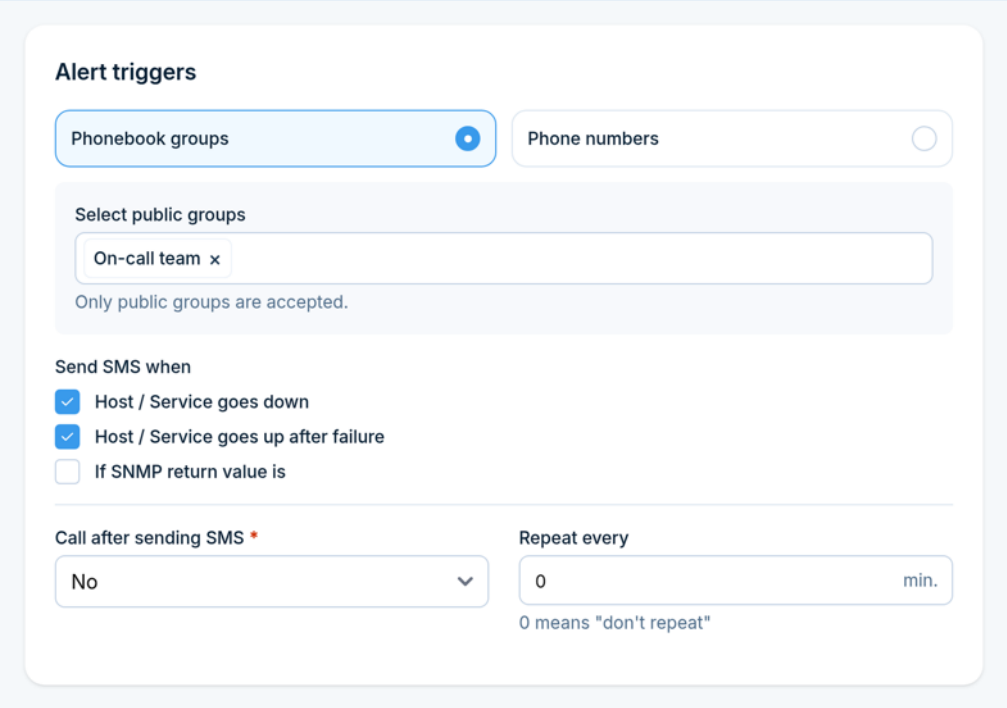
Option	Ce qu'il faut entrer
Phonebook groups	Sélectionnez les groupes publics. Seuls les groupes publics sont acceptés.
Phone numbers	Tapez les numéros directement, séparés par des virgules. Maximum 100 caractères au total.

Ensuite, cochez au moins une condition **Send SMS when**. Sans cela, la tâche ne peut pas être enregistrée :

- **Host / Service goes down**
- **Host / Service goes up after failure**
- **If SNMP return value is** - uniquement pour les tâches SNMP. Choisissez un **Operator** (Equal to, Not equal to, Greater than, Less than, Contains, Does not contain) et une **Value**.
- **If Modbus return value is** - uniquement pour les tâches Modbus, avec les mêmes champs d'opérateur et de valeur.

Deux autres paramètres ferment la section :

- **Call after sending SMS** - placer également un appel vocal. Les options sont **No**, **Ring only**, **Yes - text to speech** et **Yes - text to speech (advanced)**, selon le modèle de votre appareil. Avec l'option avancée, vous choisissez également un **Voice model**.
- **Repeat every** - renvoyer l'alerte toutes les X minutes pendant que le problème persiste. `0` signifie l'envoyer une fois et rester silencieux.



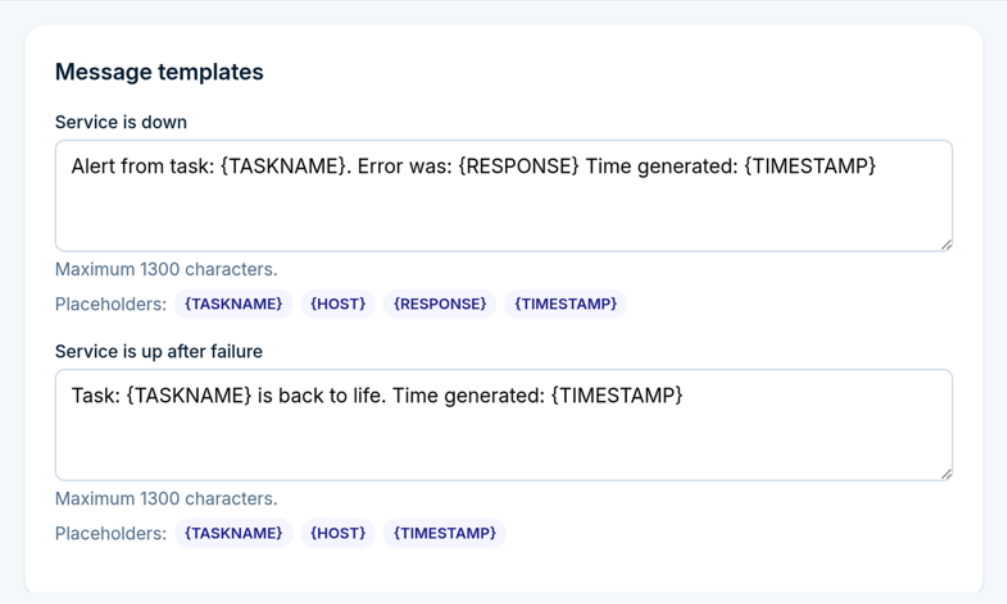
Déclencheurs d'alerte

Modèles de message

Écrivez le texte de chaque alerte que vous avez activée. Chaque message peut contenir jusqu'à 1300 caractères et peut utiliser des espaces réservés :

Message	Espaces réservés disponibles
Service is down	`{TASKNAME}`, `{HOST}`, `{RESPONSE}`, `{TIMESTAMP}`
Service is up after failure	`{TASKNAME}`, `{HOST}`, `{TIMESTAMP}`
Texte SMS (SNMP)	`{TASKNAME}`, `{VALUE}`, `{TIMESTAMP}`
Texte SMS (Modbus)	`{TASKNAME}`, `{VALUE}`, `{TIMESTAMP}`

Par exemple, `DOWN: {TASKNAME} ({HOST}) at {TIMESTAMP}` produit un message indiquant ce qui a échoué, où et quand.



Modèles de message

Cliquez sur **Create task**. La tâche commence à être vérifiée à la prochaine exécution de surveillance.

Partie 2 : Rapports

Allez sur **Monitoring > Network Monitoring > Reports**.

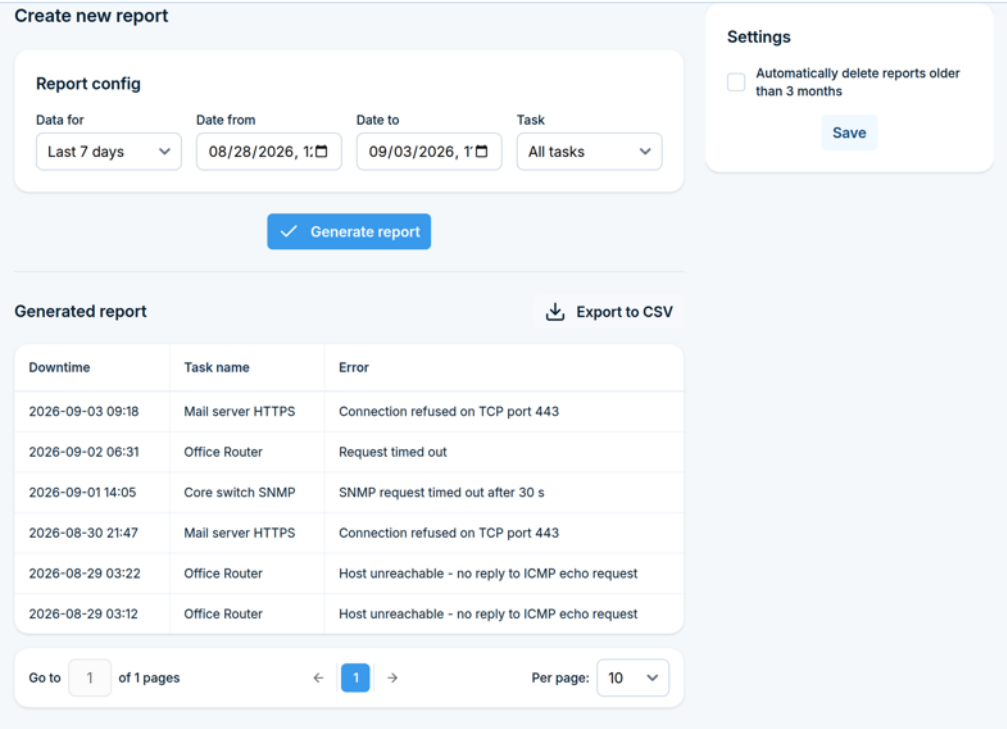
Générer un rapport

Dans la boîte **Report config**, choisissez :

Champ	À quoi elle sert
Data for	Une plage de dates prédéfinie. En en choisir une remplit les dates ci-dessous.
Date from / **Date to**	La plage exacte. La modification de ces champs bascule **Data for** sur une plage personnalisée.
Task	Une seule tâche, ou **All tasks**.

Cliquez sur **Generate report**. Les résultats apparaissent ci-dessous, énumérant le temps d'arrêt, le nom de la tâche et l'erreur enregistrée pour chaque incident.

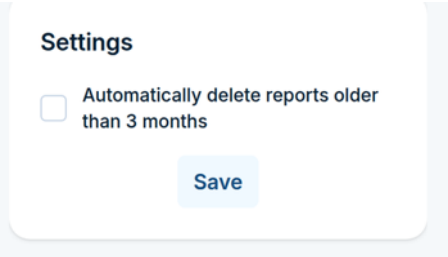
Cliquez sur **Export to CSV** au-dessus des résultats pour les télécharger.



Rapport généré

Rétention des rapports

La boîte à droite contient une option, **Automatically delete reports older than 3 months**. Activez-la pour empêcher l'historique des rapports de croître indéfiniment, puis cliquez sur **Save**.



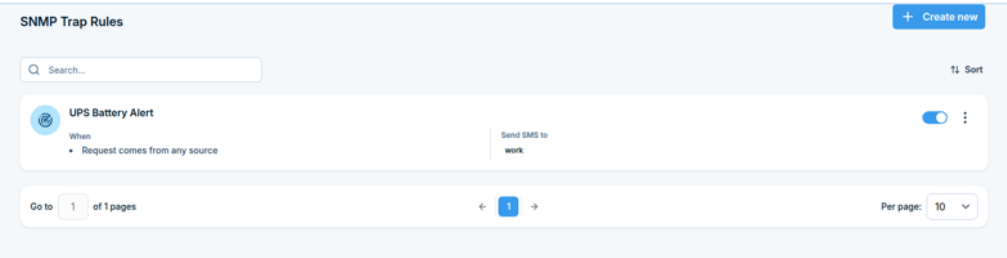
Rétention des rapports

Partie 3 : Traps SNMP

Les tâches interrogent les appareils. Les règles de trap SNMP fonctionnent différemment : un autre appareil envoie un trap **vers** le SMSEagle, et la règle le transforme en SMS.

Étape 1 : Ouvrir la page SNMP Traps

Allez sur **Monitoring > Network Monitoring > SNMP Traps**.



Règles SNMP Trap

Étape 2 : Créer une règle

Cliquez sur **Create new** dans le coin supérieur droit. Un panneau latéral s'ouvre.

Nommez la règle

Dans **Rule name**, tapez quelque chose de descriptif, par exemple `UPS battery trap`. Maximum 100 caractères.

Décidez des traps à traiter

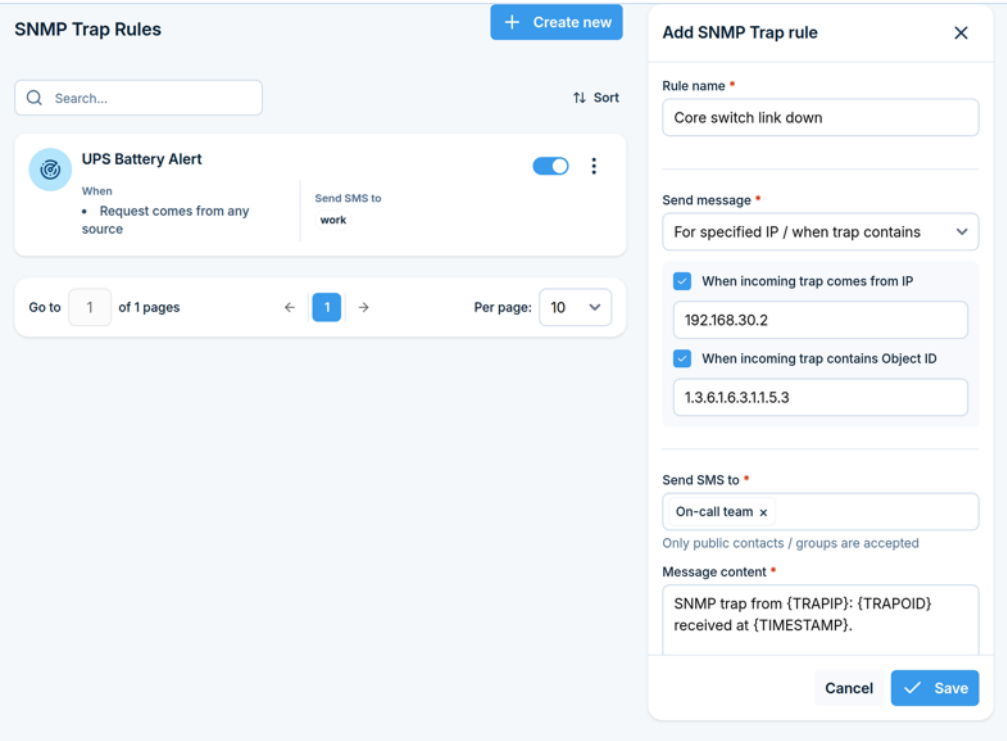
Choisissez **Send message** :

Option	Signification
Always send	Chaque trap reçu par l'appareil déclenche cette règle.
For specified IP / when trap contains	Seuls les traps correspondant aux conditions ci-dessous la déclenchent.

Si vous avez choisi la deuxième option, deux conditions deviennent disponibles. Vous pouvez en utiliser une ou les deux, et un trap doit satisfaire à chaque condition que vous activez.

When incoming trap comes from IP Cochez cette case et tapez l'adresse IP de l'appareil émetteur.

When incoming trap contains Object ID Cochez cette case et tapez l'OID qui doit être présent dans le trap.



Une règle SNMP trap avec conditions

Choisissez les destinataires et rédigez le message

Send SMS to - sélectionnez les contacts ou groupes. Seuls les contacts et groupes **public** sont acceptés.

Message content - le texte à envoyer, maximum 1300 caractères. Vous pouvez utiliser ces espaces réservés :

Espace réservé	Remplacé par
`{TASKNAME}`	Le nom de la règle
`{IP}`	L'adresse IP d'où provient le trap
`{TRAP}`	Le contenu du trap

Paramètres optionnels

- **Call after sending SMS** - placer également un appel vocal, avec les mêmes options que dans les tâches.

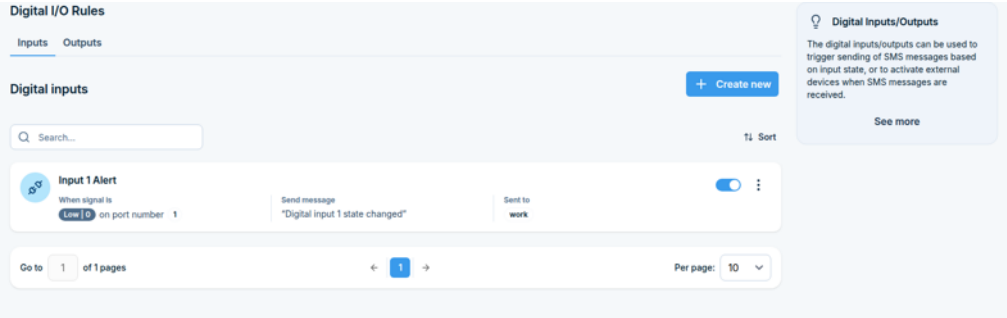
Cliquez sur **Save**. La règle s'applique aux traps reçus à partir de maintenant.

Comportement du Network Monitor

- Les tâches sont vérifiées sur la **Monitoring period** partagée, donc une tâche ne peut pas alerter plus rapidement que cet intervalle ne le permet.

- Une alerte « down » est envoyée une seule fois quand l'état change, puis répétée uniquement si vous définissez **Repeat every**.
- Une tâche liée à un parent est entièrement ignorée tandis que le parent est down, donc ses propres alertes restent silencieuses jusqu'à la récupération du parent.
- Si plusieurs règles de trap SNMP correspondent au même trap, **chacune** d'elles envoie son propre SMS.

Entrée/Sortie numérique



Aperçu entrée/sortie numérique

À quoi sert cette fonctionnalité

Les entrées et sorties numériques sont le connecteur physique sur l'appareil qui permet à SMSEagle de communiquer avec le monde en dehors du réseau :

Direction	À quoi elle sert
Entrée	Un changement de tension sur un port d'entrée (un contact de porte se ferme, un relais d'alarme se déclenche, un onduleur signalant une panne) fait envoyer un SMS par l'appareil.
Sortie	Un SMS entrant fait commuter un port de sortie par l'appareil vers on ou off, de sorte qu'il peut activer une sirène, ouvrir un portail ou réinitialiser une machine.

Vous configurez ceci avec des **rules**. Une règle Input dit « quand le port 2 passe high, envoyer un SMS à l'équipe de maintenance ». Une règle Output dit « quand un SMS contenant OPEN arrive, mettre le port 1 high pendant 5 secondes ».

À côté des règles, il y a deux pages qui affichent les ports eux-mêmes : **Internal pins** (les ports intégrés à l'appareil) et **External pins** (ports supplémentaires ajoutés via un module io-bridge).

Avant de commencer

- Vérifiez combien de ports d'entrée et de sortie votre modèle d'appareil possède, et connectez votre équipement à ces ports. Les listes de ports dans les formulaires de règles

sont construites à partir du modèle de votre appareil, donc elles ne proposent que les ports qui existent physiquement.

- L'appareil doit être capable d'envoyer des SMS. Vérifiez qu'au moins un modem est connecté et enregistré sur le réseau.
- Les destinataires des règles Input doivent être marqués comme **Public** dans le Phonebook.

Hardware: ports, logic levels and wiring

The digital inputs (DI) and digital outputs (DO) are located on the 12-pole I/O connector of the device, together with the 1-Wire, +5V and GND terminals. See Connectors, Ports and LEDs for the connector location.

Number of ports

Port type	Number of ports
Digital inputs (DI)	4
Digital outputs (DO)	4

The 12-pole connector carries: 4x digital input, 4x digital output, 1× 1-Wire, 1x +5V and 2x GND.

Logic levels

The logical states shown in the web interface (rule forms, **Internal pins** page) map to the following voltages on the terminals:

Logical state	Voltage on the terminal
0 (Low)	+5 V
1 (High)	0 V

> **The logic is inverted.** Logical **1 (High)** corresponds to **0 V** on the terminal. An unconnected input is pulled up to about 5 V, so it reads **0 (Low)** on the **Internal pins** page.

With a contact wired between an input and GND (as in the examples below):

Contact state	Voltage on DI	Logical state
Open	3 to 5 V	0 (Low)
Closed	0 V	1 (High)

NO and NC contacts (normally open / normally closed)

Most sensors, alarm panels, door contacts and relays offer a **NO** (normally open) or **NC** (normally closed) contact, often both. The contact type decides which value to choose in **When input signal**:

Contact type	Normal state	On alarm	Choose in When input signal
NO (normally open)	Open	Closes	**1 (High)**
NC (normally closed)	Closed	Opens	**0 (Low)**

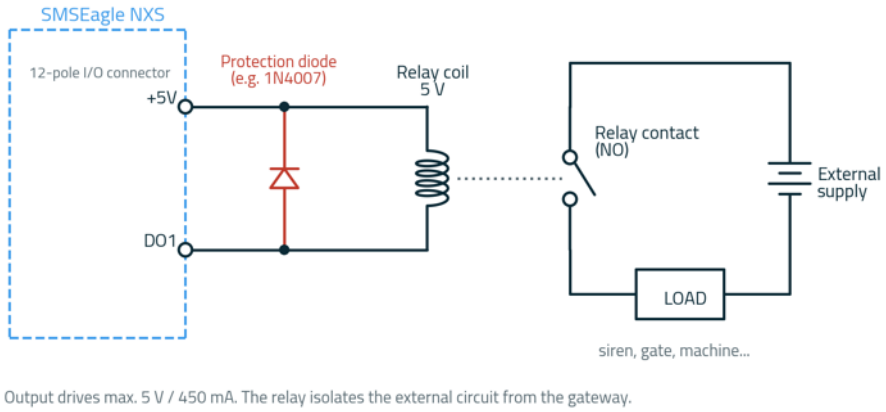
> **Prefer NC contacts for alarm circuits.** With an NC contact, a cut or disconnected cable opens the circuit in the same way as a real alarm, so a wiring fault also triggers an SMS. With an NO contact, a broken cable goes unnoticed.

Using digital outputs

A digital output can directly drive an external circuit with a voltage **not exceeding 5 V** and a current of **max. 450 mA**.

The safest way to control external equipment is through an intermediary **relay with a protection diode**. The relay keeps the external circuit (which may run at a different voltage) separated from the gateway, and the relay contacts can switch loads well above the limits of the output itself.

Use the relay **NO** (normally open) contact if the load should be switched **on** when the coil is energized, for example to start a siren or open a gate. Use the **NC** (normally closed) contact if the load should be switched **off**, for example to cut power to a device for a remote reset. Many relays have a changeover contact (COM, NO, NC) that offers both.



Digital output: example of use with an external relay (NO contact)

> **Always fit a protection diode across the relay coil.** When the current through a coil is switched off, the coil produces a high reverse voltage spike. The diode (for example 1N4007), connected in reverse direction across the coil terminals, gives this current a safe path and protects the output from damage. Some relay manufacturers offer relays with the diode already built in.

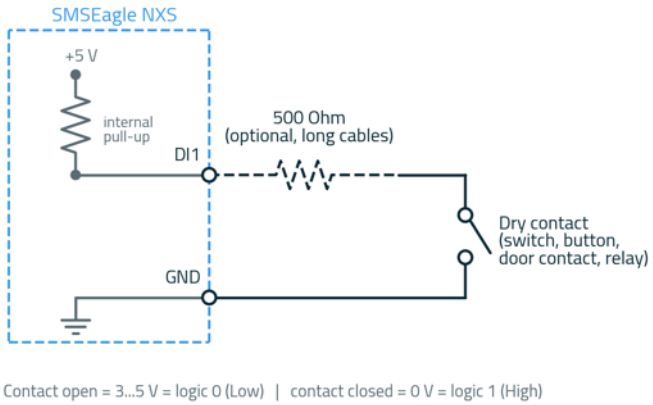
Using digital inputs

The digital inputs have **internal pull-up resistors**. A pull-up gives an input a defined state when nothing is connected to it, so that it does not float and trigger by accident. On an unconnected input you will measure **3 to 5 V**.

To change the state of an input, connect it to **GND**: through a potential-free contact, an open collector output, or a relay. Do not apply an external voltage to the inputs.

Dry contact, NO or NC (simplest connection)

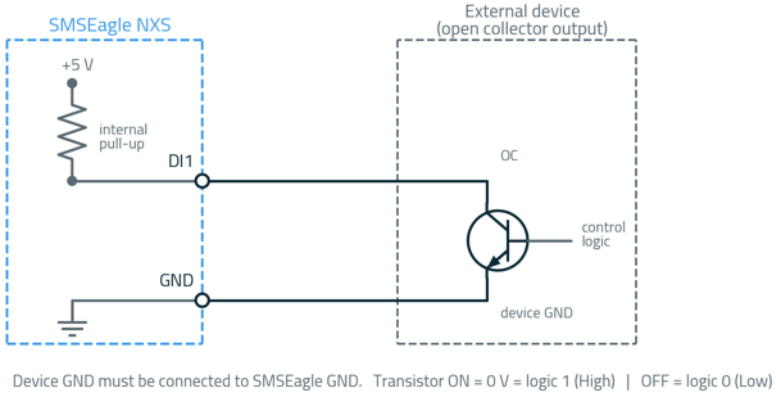
Connect a potential-free (dry) contact between the input and GND: a switch, push button, door or window contact, PIR detector output, alarm panel output or relay contact. Both **NO** (normally open) and **NC** (normally closed) contacts can be used; set **When input signal** according to the table in NO and NC contacts. If the cable to the contact is long, add an optional **500 Ohm** resistor in series with the input.



Digital input: dry contact (NO or NC). The 500 Ohm resistor is optional, for long cables

Device with an open collector output

Connect the open collector output of the device to the input, and the GND of the device to the GND of SMSEagle. A common ground is required. When the output transistor is switched on, it pulls the input to 0 V.



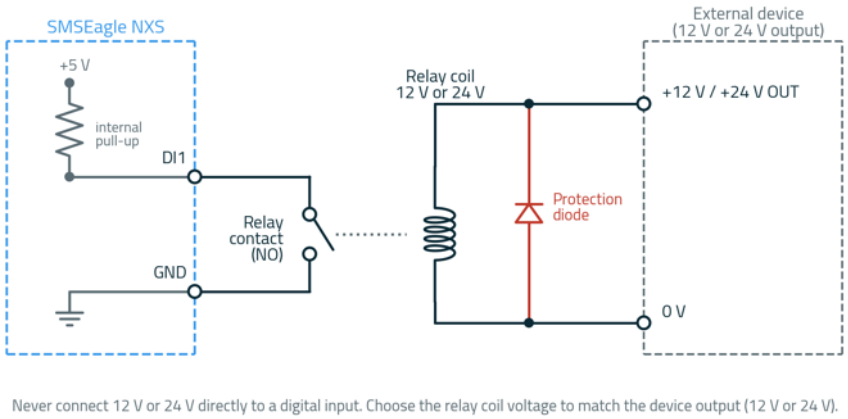
Digital input: connection with a device with an open collector output

Device with a 12 V or 24 V output

A 12 V or 24 V signal must **never** be connected directly to a digital input. Use the output of the device to drive the coil of an intermediary relay (with a protection diode), and connect the relay

contact between the input and GND. Choose a relay with a coil voltage matching the output of the device: **12 V** coil for a 12 V output, **24 V** coil for a 24 V output. An optocoupler module rated for the same voltage can be used in the same way. This keeps the 12 V or 24 V circuit fully separated from the gateway.

The example uses the relay **NO** (normally open) contact: when the device output is active, the contact closes and the input reads **1 (High)**. If you wire the **NC** (normally closed) contact instead, the logic is reversed: an active output opens the contact and the input reads **0 (Low)**.

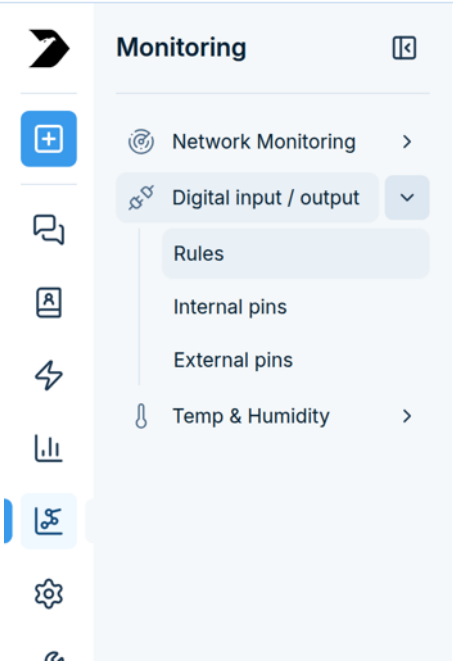


Digital input: connection with a device with a 12 V or 24 V output

Où le trouver

Dans la barre latérale, allez à **Monitoring > Digital input / output**. Il a trois pages :

Page	À quoi ça sert
Rules	Créez les règles Input et Output. C'est là que vous passez la plupart de votre temps.
Internal pins	Consultez l'état en direct des ports intégrés et activez ou désactivez le service.
External pins	Définissez et contrôlez les ports supplémentaires fournis par un module io-bridge.

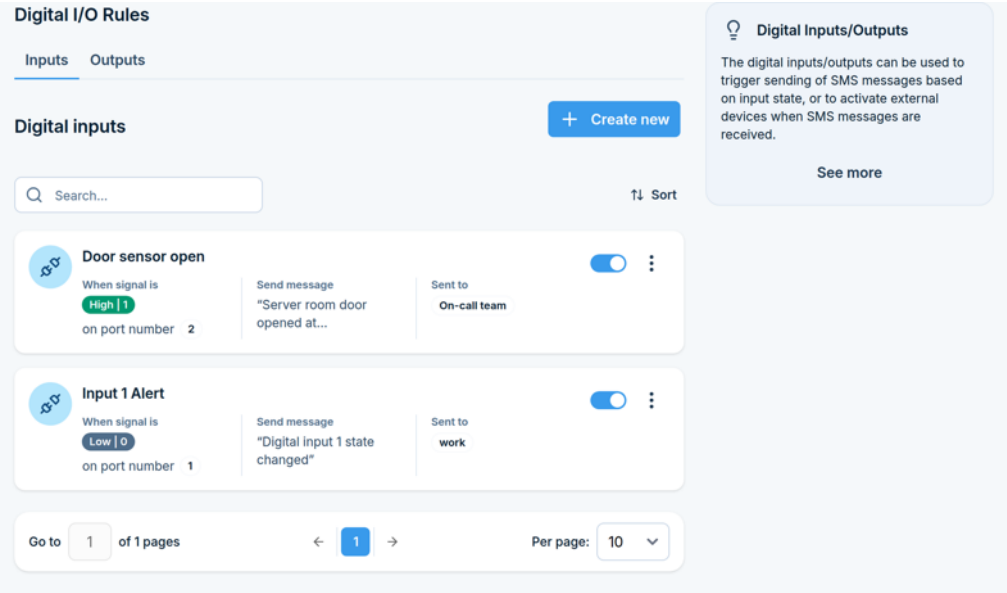


Où trouver les pages Digital I/O

Partie 1 : Règles d'entrée (signal d'entrée vers SMS)

Étape 1 : Ouvrir la page des règles

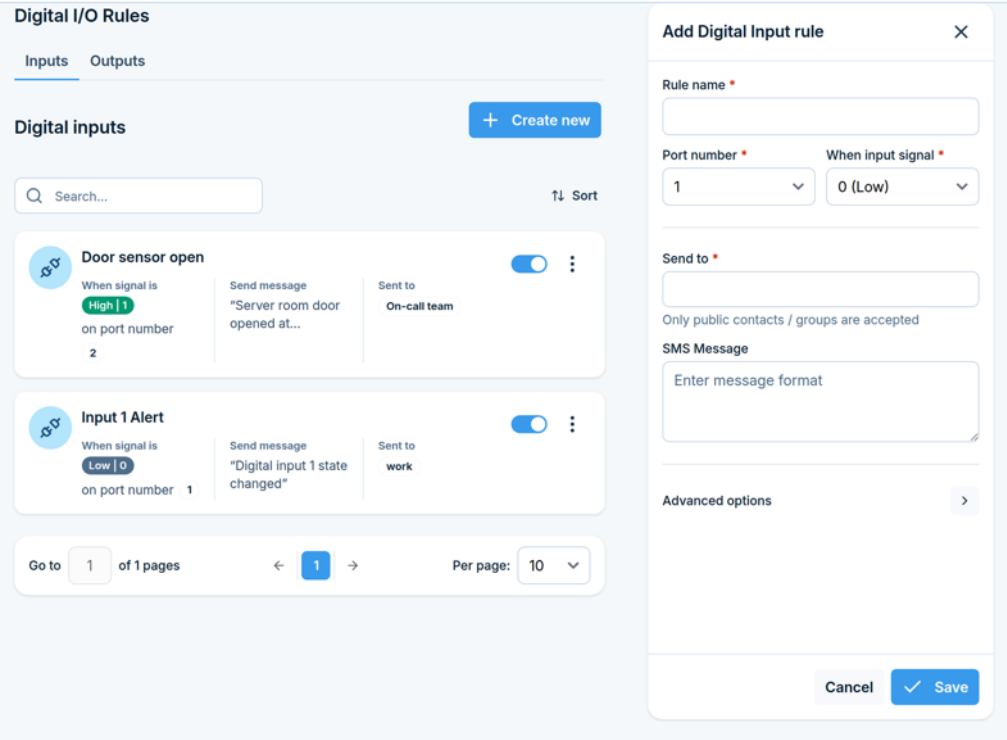
Allez à **Monitoring > Digital input / output > Rules** et assurez-vous que l'onglet **Inputs** est sélectionné.



Règles d'entrée numérique

Étape 2 : Créer une règle d'entrée

Cliquez sur **Create new** dans le coin supérieur droit. Un panneau latéral s'ouvre.



Une nouvelle règle d'entrée numérique

Nommez la règle

Dans **Rule name**, tapez quelque chose de descriptif, par exemple `Server room door opened`. Maximum 100 caractères.

Choisir le port et le signal

Champ	Ce qu'il faut entrer
Port number	Le port d'entrée sur lequel l'équipement est câblé. Les ports externes (io-bridge) apparaissent dans la liste marqués `(Ext)`.
When input signal	`0 (Low)` ou `1 (High)`. C'est l'état qui déclenche la règle.

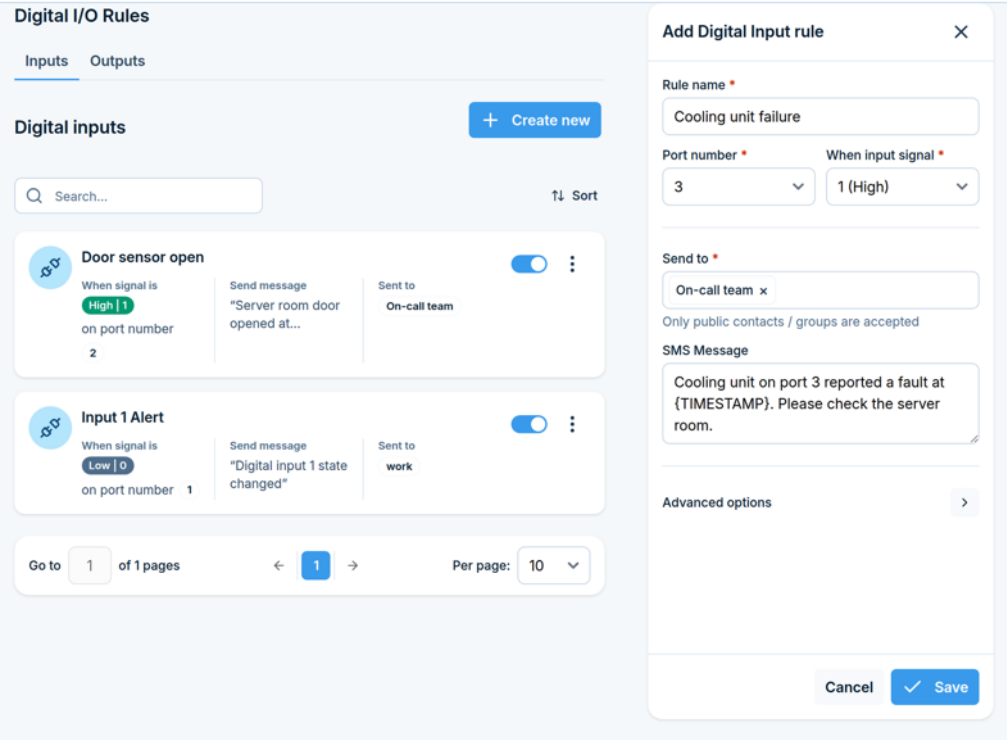
Pick the value that represents the alarm condition on your equipment. A **NO** (normally open) contact that closes on alarm needs **1 (High)**; a **NC** (normally closed) contact that opens on alarm needs **0 (Low)**. See NO and NC contacts for details.

Choisir les destinataires

Dans **Send to**, sélectionnez les contacts ou groupes qui doivent recevoir l'SMS. Seuls les contacts et groupes **publics** peuvent être sélectionnés ici. Ce champ est obligatoire.

Écrire le texte SMS

SMS Message est le texte qui est envoyé quand la règle se déclenche. Maximum 1000 caractères. Le même texte est envoyé à chaque destinataire, donc incluez le nom du lieu ou de la machine, par exemple `ALARM: server room door opened`.

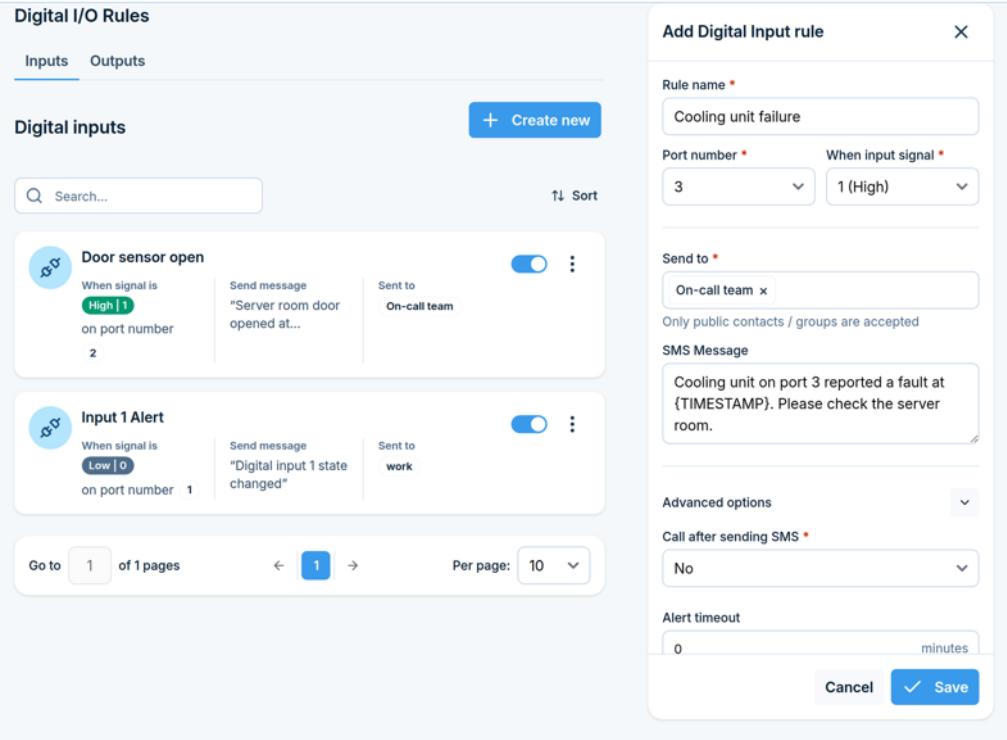


Une règle d'entrée complétée

Options avancées

Cliquez sur **Advanced options** pour développer cette section. Vous n'en avez pas besoin pour une configuration de base.

- **Call after sending SMS** - placer également un appel vocal aux mêmes destinataires. Les options sont **No**, **Ring**, **Text-to-speech (TTS)** et **Text-to-speech (advanced)**, selon le modèle d'appareil que vous possédez. Avec l'option avancée, vous choisissez également un **Voice model**.
- **Alert timeout** - le nombre de minutes qui doivent s'écouler avant que la même règle puisse à nouveau déclencher une alerte. `0` signifie pas de limite, donc chaque changement de signal envoie un SMS.



Options avancées de règle d'entrée

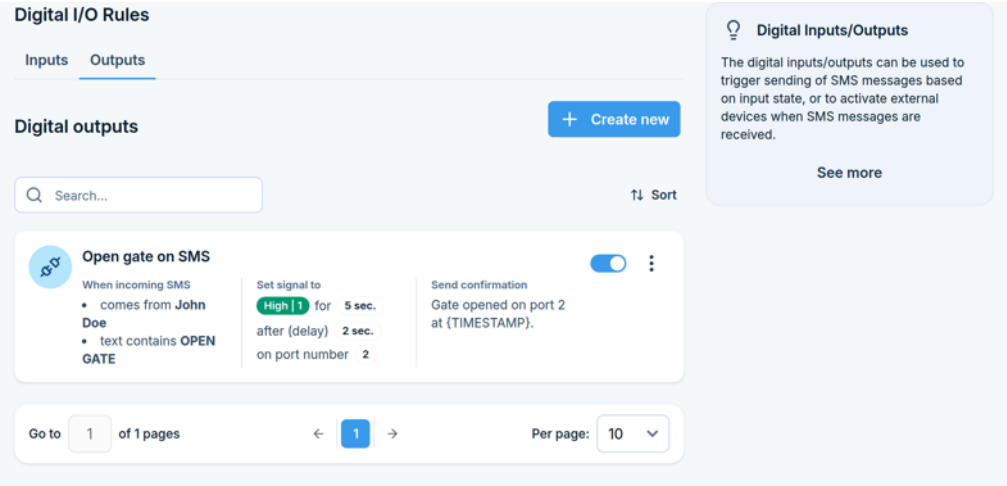
Définissez un délai d'alerte pour les entrées bruyantes. Un contact qui vibre, ou un équipement qui se déclenche à plusieurs reprises, peut produire une rafale de messages. Un délai de quelques minutes permet de ne envoyer qu'un seul SMS par événement réel.

Cliquez sur **Save**. La règle commence à fonctionner sur les changements de signal à partir de maintenant.

Partie 2 : Règles de sortie (SMS vers signal de sortie)

Étape 1 : Ouvrir la page des règles

Allez à **Monitoring > Digital input / output > Rules** et choisissez l'onglet **Outputs**.



Règles de sortie numérique

Étape 2 : Créer une règle Output

Cliquez sur **Create new** dans le coin supérieur droit. Un panneau latéral s'ouvre.

Nommez la règle et choisissez le port

Dans **Rule name**, tapez quelque chose de descriptif, par exemple `Open gate on SMS`. Maximum 100 caractères. Dans **Port number**, choisissez le port de sortie auquel votre équipement est connecté. Les ports externes (io-bridge) apparaissent marqués `(Ext)`.

Décidez quels messages SMS déclenchent la règle

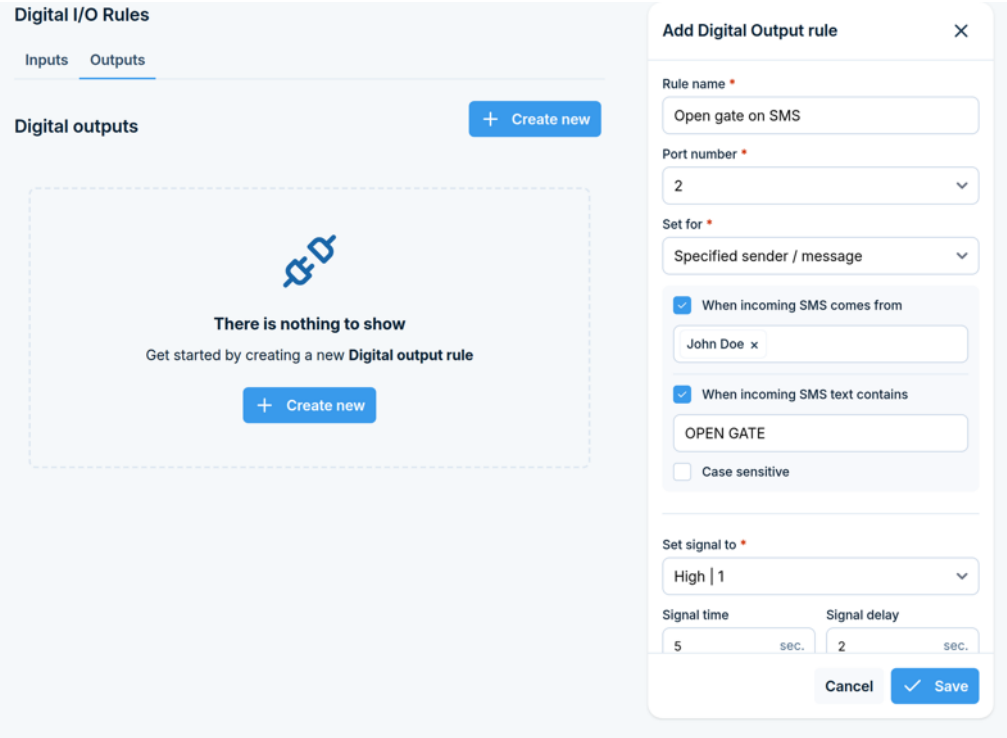
Choisissez **Set for** :

Option	Signification
All incoming messages	Chaque SMS entrant bascule la sortie.
Specified sender / message	Seuls les messages correspondant aux conditions que vous définissez ci-dessous la basculent.

Si vous avez choisi **Specified sender / message**, deux conditions deviennent disponibles. Vous pouvez en utiliser une ou les deux. Lorsque vous en utilisez deux, un message doit satisfaire **les deux**.

When incoming SMS comes from Cochez cette option et sélectionnez les contacts ou groupes d'expéditeurs.

When incoming SMS text contains Cochez cette option et tapez la phrase dans **Text**, par exemple `OPEN`. Cochez **Case sensitive** si `open` et `OPEN` doivent être traités comme différents.



Conditions de la règle de sortie

Restrict output rules by sender. Une règle de sortie bascule des équipements physiques. Sans condition d'expéditeur, toute personne connaissant votre numéro peut les utiliser.

Décidez ce que la sortie fait

Champ	Signification
Set signal to	`Low` | `0` ou `High` | `1`. L'état dans lequel le port est basculé.
Signal time	Le nombre de secondes pendant lesquelles le port reste dans cet état avant de revenir. `0` signifie qu'il y reste indéfiniment.
Signal delay	Le nombre de secondes à attendre après l'arrivée du SMS avant de basculer le port.

Options avancées

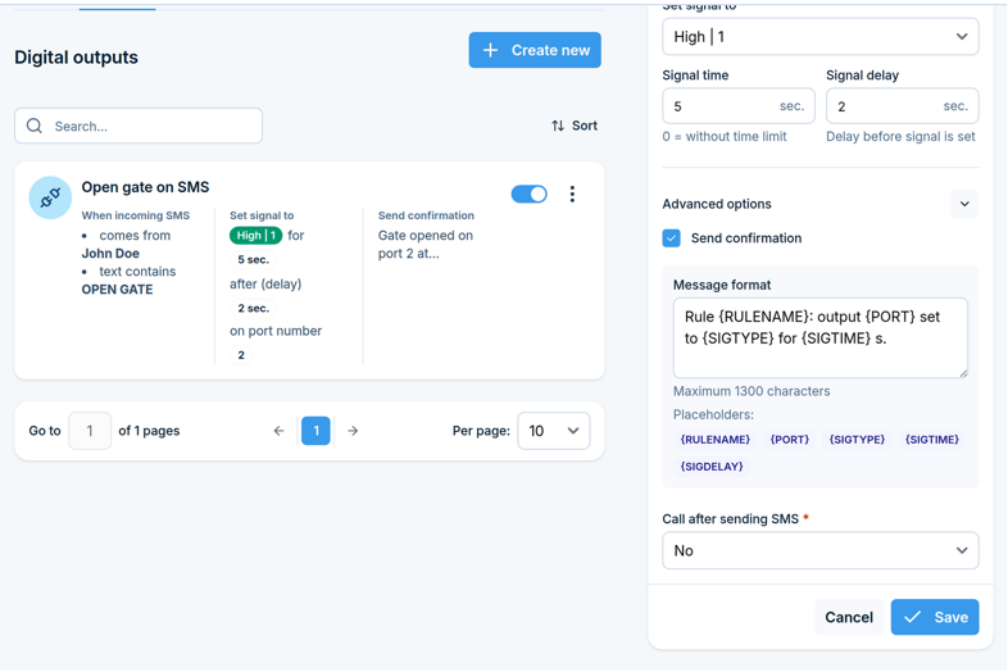
Cliquez sur **Advanced options** pour développer cette section.

Send confirmation Cochez cette option pour envoyer un SMS en retour à l'expéditeur après que la sortie a été basculée. Le champ **Message format** apparaît, maximum 1300 caractères. Vous pouvez construire le texte à partir d'espaces réservés :

Espace réservé	Remplacé par
`{RULENAME}`	Le nom de la règle qui s'est déclenchée
`{PORT}`	Le numéro du port de sortie
`{SIGTYPE}`	Le signal auquel le port a été configuré
`{SIGTIME}`	La durée du signal en secondes
`{SIGDELAY}`	Le délai du signal en secondes

Par exemple, `{RULENAME}: port {PORT} set to {SIGTYPE} for {SIGTIME}s` produit une confirmation claire pour la personne qui a envoyé la commande.

Appel après envoi du SMS Effectuez également un appel vocal, exactement comme décrit pour les règles d'entrée ci-dessus.



Message de confirmation de la règle de sortie

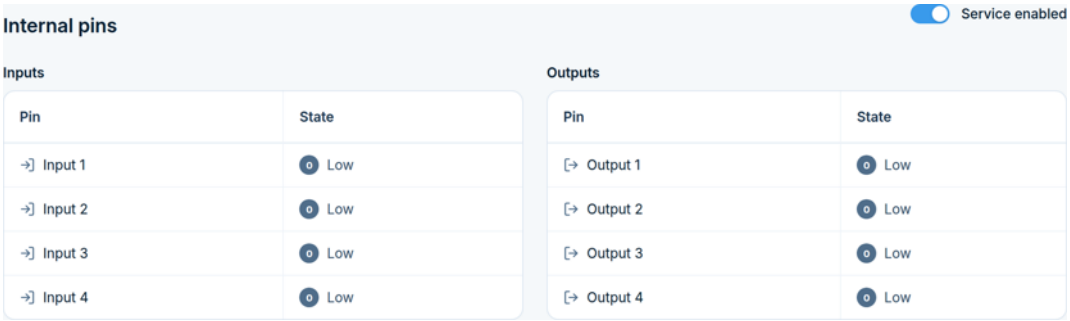
Cliquez sur **Save**. La règle commence à fonctionner sur les messages reçus à partir de maintenant.

Partie 3 : Broches internes

Allez à **Monitoring > Digital input / output > Internal pins**.

La page affiche deux tableaux, **Inputs** et **Outputs**, listant chaque port intégré avec son état actuel (`0` Low ou `1` High). Il s'agit d'une lecture directe du matériel, utile pour vérifier votre câblage avant d'écrire une règle.

En haut de la page se trouve un commutateur **Service enabled**. Il démarre et arrête le service qui lit et commande les ports intégrés. **Lorsqu'il est désactivé, les règles d'entrée et de sortie sur les ports internes ne fonctionnent pas.**



Broches internes avec le service en cours d'exécution. Chaque port ici affiche `0` Low car rien n'y est connecté

Partie 4 : Broches externes

Les broches externes sont des ports supplémentaires fournis par un module io-bridge connecté à l'appareil.

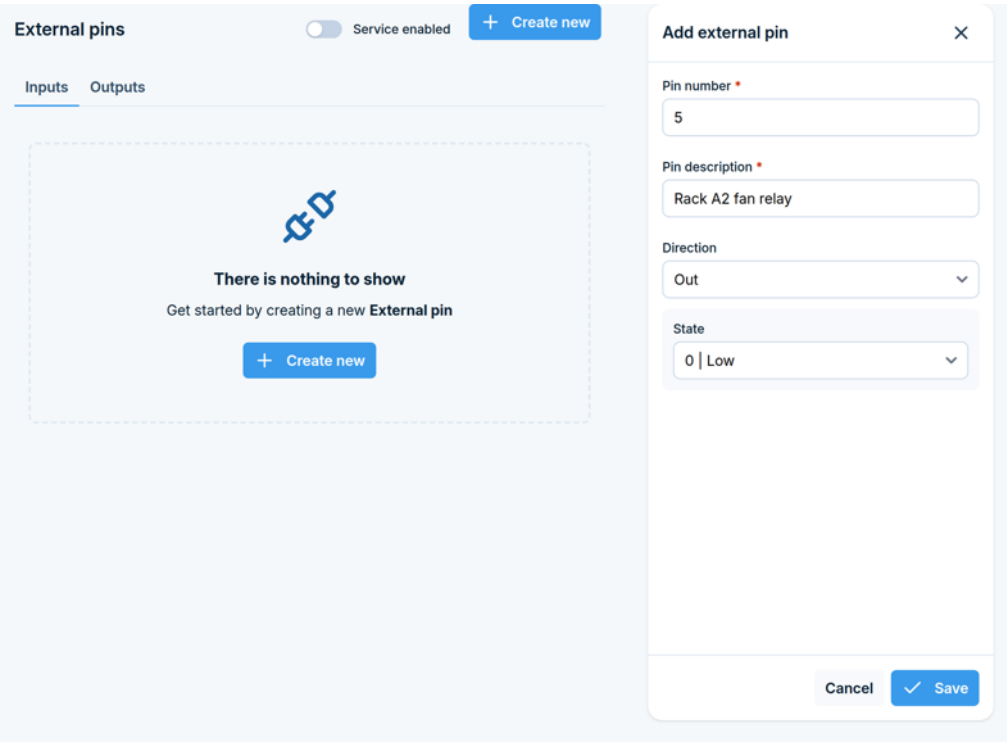
Allez à **Monitoring > Digital input / output > External pins**. La page a un onglet **Inputs** et un onglet **Outputs**, plus un commutateur **Service enabled** qui démarre et arrête le service io-bridge.

Ajouter une broche externe

Cliquez sur **Create new**. Un panneau latéral s'ouvre.

Champ	Ce qu'il faut entrer
Pin number	Le numéro du port sur le module io-bridge, par exemple 1. Chaque numéro ne peut être configuré qu'une seule fois.
Pin description	Un nom court, maximum 64 caractères. Seules les lettres, les chiffres et les espaces sont autorisés.
Direction	**In** pour un port que vous lisez, **Out** pour un port que vous commandez.
State	Affiché uniquement pour les broches **Out** : l'état initial du port, `1 | High` ou `0 | Low`.

Cliquez sur **Save**.



Ajout d'une broche externe

Utiliser les broches

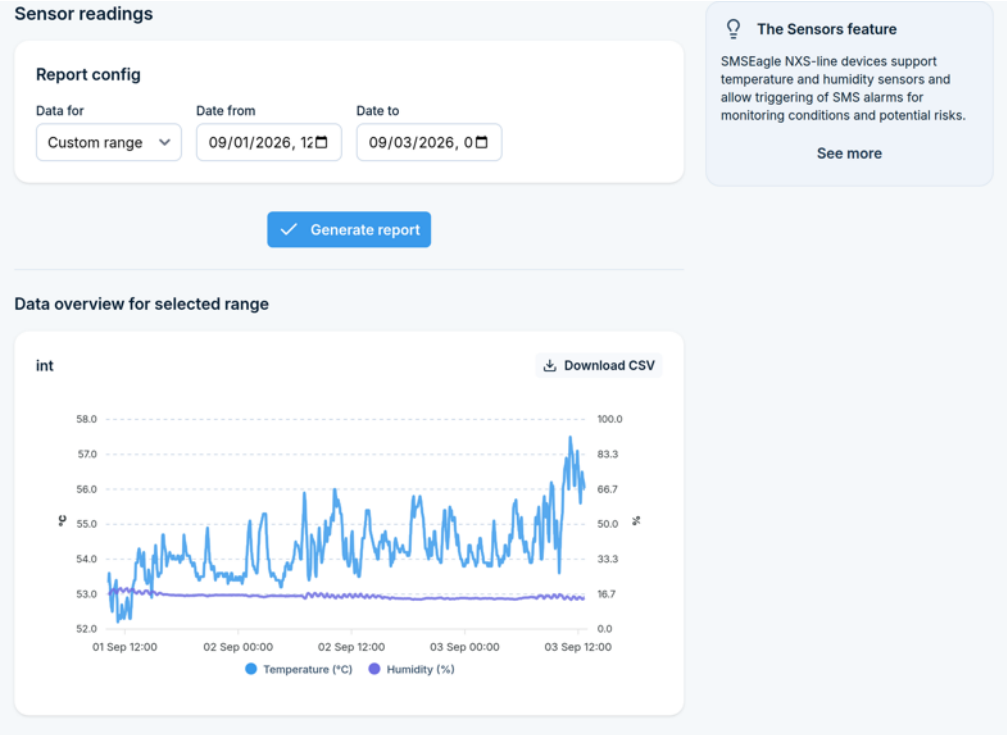
- Sous l'onglet **Outputs**, vous pouvez basculer directement l'état d'une broche à partir de la liste.
- Sous l'onglet **Inputs**, l'état est en lecture seule, car la valeur est déterminée par ce qui est connecté à la broche.

- Une fois définies, les broches externes apparaissent également dans les listes **Port number** des règles Input et Output, marquées `(Ext)`, de sorte que les règles peuvent les utiliser exactement comme les ports intégrés.

Fonctionnement des règles Digital I/O

- Les règles ne s'activent que sur les événements survenant après la création et l'activation de la règle. Utilisez le commutateur en regard d'une règle pour la suspendre sans la supprimer.
- Si plusieurs règles correspondent au même événement, **chacune** d'elles s'exécute, de sorte qu'un signal d'entrée peut envoyer plusieurs messages et un SMS peut basculer plusieurs ports.
- La condition de texte sur les règles Output est une correspondance **contient**, pas une correspondance exacte.
- Les règles qui utilisent des ports internes ont besoin du service **Internal pins** activé ; les règles qui utilisent des ports `(Ext)` ont besoin du service **External pins** activé.

Capteurs de température et d'humidité



Aperçu des capteurs de température et d'humidité

À quoi sert cette fonctionnalité

Les appareils SMSEagle série NXS supportent les capteurs de température et d'humidité connectés à l'appareil. Une fois qu'un capteur est connecté, l'appareil le lit selon un calendrier, conserve un historique des relevés et peut envoyer un SMS lorsqu'une valeur dépasse un seuil que vous définissez.

La fonctionnalité comporte trois pages :

Page	À quoi ça sert
Reading	Graphiques des valeurs enregistrées, avec téléchargement CSV.
Alarms	Les règles qui transforment un relevé en SMS.
Sensor settings	La liste des capteurs connectés, leurs noms et la fréquence de lecture.

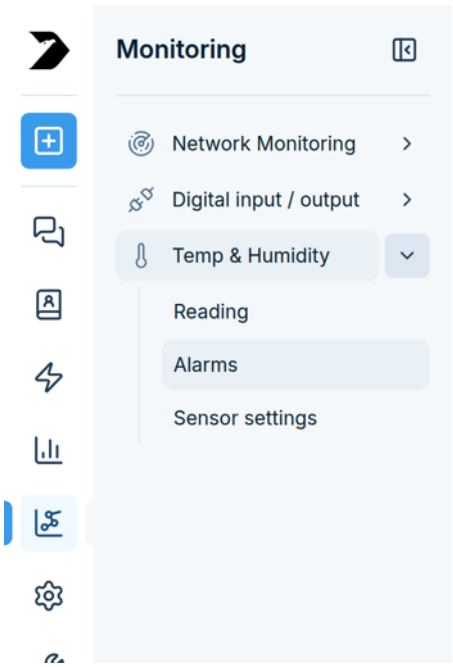
Utilisations courantes : surveiller une salle serveur, un entrepôt frigorifique ou une armoire technique, et envoyer un SMS à la personne d'astreinte lorsque la température ou l'humidité devient excessive.

Avant de commencer

- Connectez le capteur à l'appareil avant de configurer quoi que ce soit. L'appareil trouve les capteurs en scannant le matériel, de sorte qu'un capteur débranché ne peut pas être configuré.
- Les destinataires des règles d'alarme doivent être marqués comme **Public** dans le Phonebook.

Où le trouver

Dans la barre latérale, accédez à **Monitoring > Temp & Humidity**. Les trois pages énumérées ci-dessus apparaissent sous celle-ci.



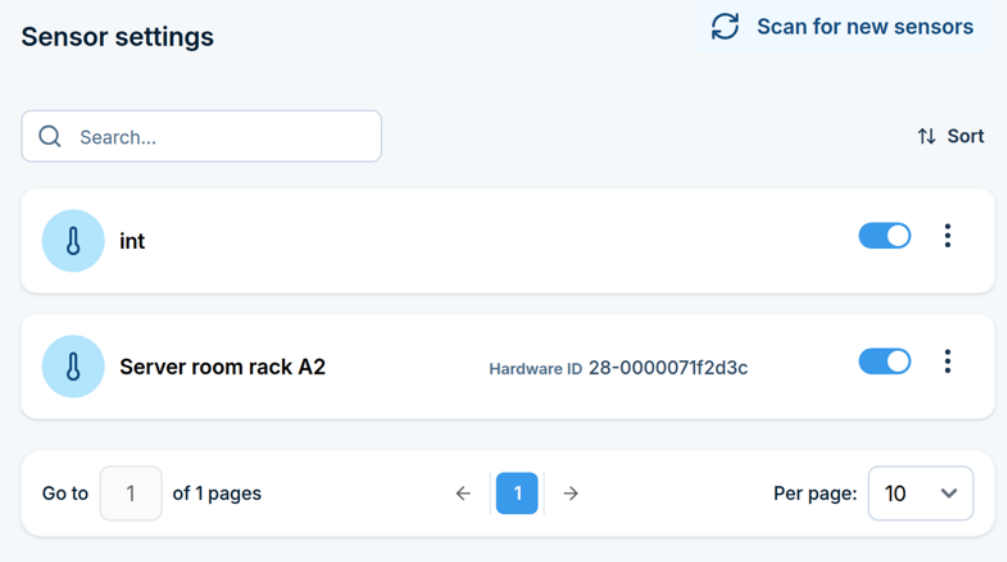
Où trouver les pages des capteurs

Partie 1 : Ajouter et nommer les capteurs

Étape 1 : Analyser les capteurs

Allez à **Monitoring > Temp & Humidity > Sensor settings** et cliquez sur **Scan for new sensors** dans le coin supérieur droit.

L'appareil vérifie ses entrées et ajoute tout ce qu'il trouve. La page indique soit que de nouveaux capteurs ont été ajoutés, soit qu'aucun n'a été trouvé.



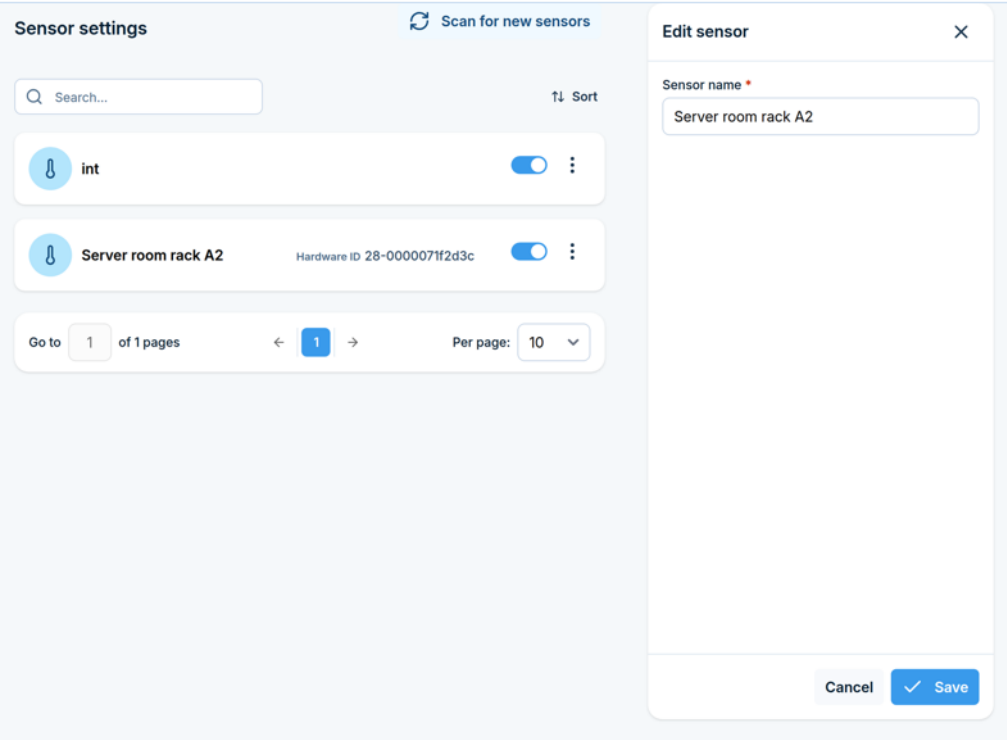
Sensor settings

Chaque capteur de la liste affiche son **Sensor name** et son **Hardware ID**. L'Hardware ID est la façon dont l'appareil identifie le capteur physique ; il n'est pas modifiable.

Étape 2 : Donner aux capteurs des noms significatifs

Un capteur fraîchement détecté n'est pas nommé d'après le lieu qu'il surveille, renommez-le donc : cliquez sur **Edit** à côté d'un capteur et tapez un **Sensor name**, maximum 255 caractères, par exemple `Server room rack A`.

Ce nom apparaît sur les graphiques, dans les règles d'alarme et dans l'export CSV, il vaut donc la peine de le faire avant de créer des règles.



Renommage d'un capteur

Étape 3 : Gérer la liste

Chaque capteur possède :

- un commutateur pour l'"**activer ou le désactiver**, ce qui arrête sa lecture sans le supprimer,
- une action **Edit** pour le nom,
- une action **Delete**.

Vous pouvez également cocher plusieurs capteurs et les activer, les désactiver ou les supprimer ensemble.

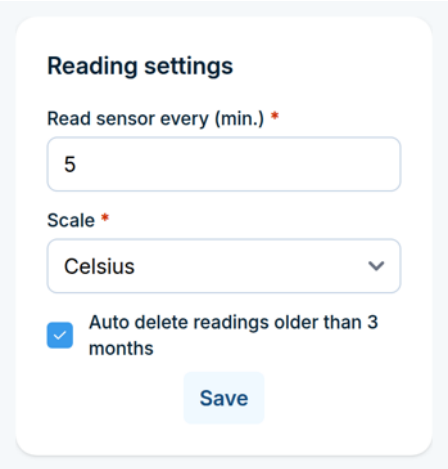
> Le **capteur interne ne peut pas être supprimé**. Les appareils dotés d'un capteur intégré le conservent toujours dans la liste ; désactivez-le si vous ne voulez pas ses lectures.

Étape 4 : Définir les paramètres de lecture

La boîte **Reading settings** à droite de la page Sensor settings contrôle la façon dont les capteurs sont lus. Ces paramètres sont **globaux**, ils s'appliquent à chaque capteur :

Champ	À quoi elle sert
Read sensor every (min.)	Fréquence de lecture des capteurs, de 1 à 59 minutes.
Scale	**Celsius** ou **Fahrenheit**. S'applique aux graphiques, aux alarmes et à l'export.
Auto delete readings older than 3 months	Empêche l'historique de lecture de croître indéfiniment.

Cliquez sur **Save**.

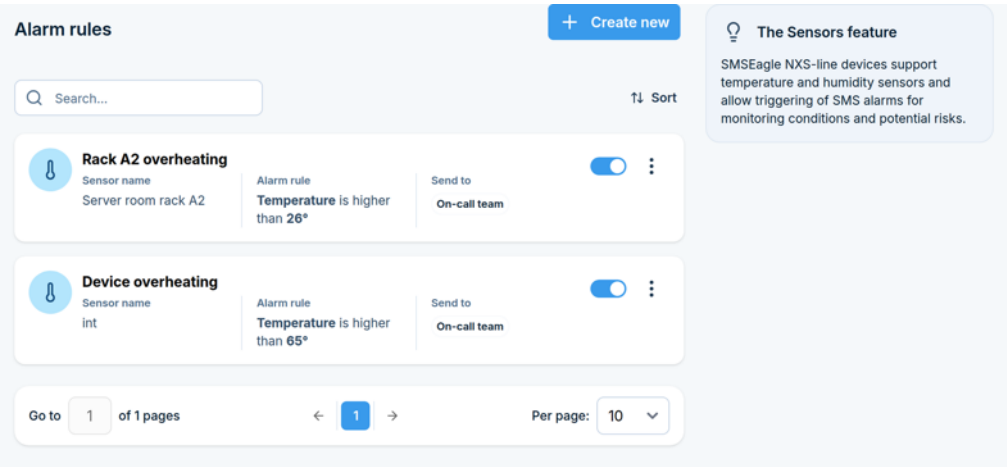


Reading settings

Partie 2 : Règles d'alarme

Étape 1 : Ouvrir la page Alarmes

Allez à **Monitoring > Temp & Humidity > Alarms**.



Règles d'alarme

Étape 2 : Créer une règle

Cliquez sur **Create new** dans le coin supérieur droit. Un panneau latéral s'ouvre.

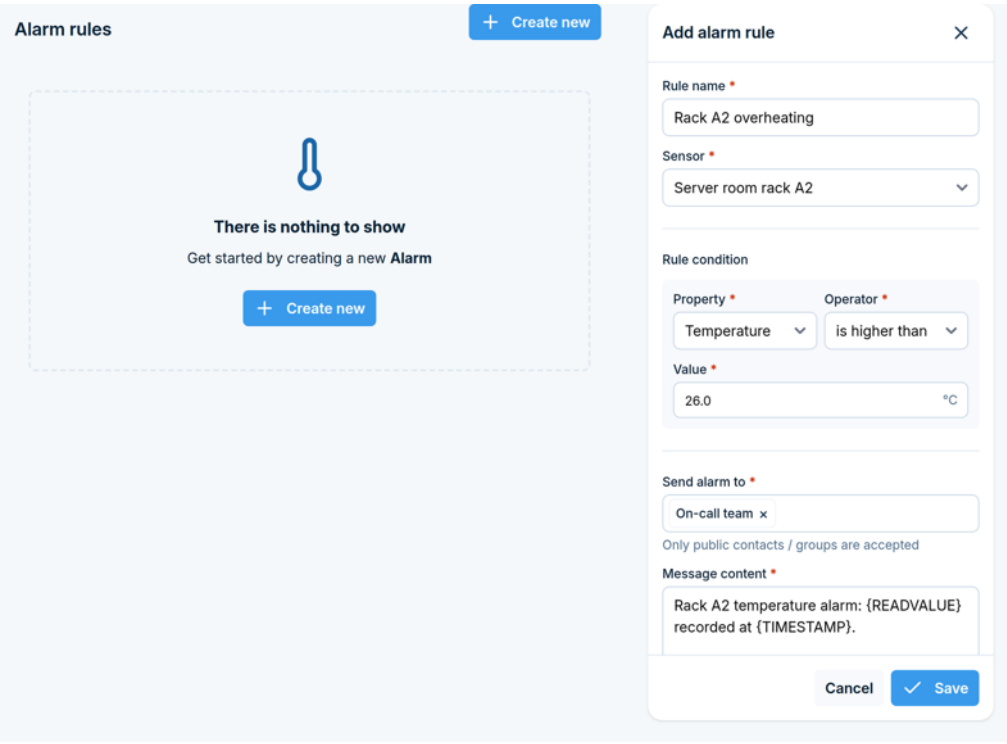
Nommez la règle

Dans **Rule name**, tapez quelque chose de descriptif, par exemple `Server room too warm`. Maximum 100 caractères.

Définir la condition

Champ	Ce qu'il faut choisir
Sensor	Le capteur que la règle surveille.
Property	**Temperature** ou **Humidity**.
Operator	**is higher than** ou **is lower than**.
Value	Le seuil, avec une décimale, par exemple `27.5`.

Le seuil de température est lu dans l'"**Scale** que vous avez défini dans les paramètres de lecture. Une règle écrite pour Celsius signifie quelque chose de différent après avoir basculé l'appareil en Fahrenheit. Vérifiez vos règles si vous changez l'échelle.



Création d'une règle d'alarme

Choisir les destinataires

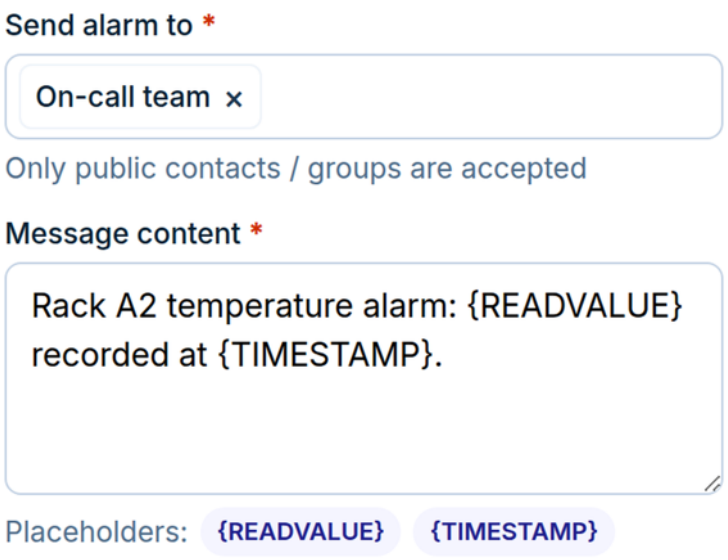
Dans **Send alarm to**, sélectionnez les contacts ou les groupes. Seuls les contacts et groupes **public** peuvent être sélectionnés ici. Ce champ est obligatoire.

Rédiger le message

Message content est le SMS qui est envoyé, maximum 2000 caractères. Vous pouvez le construire à partir d'espaces réservés :

Espace réservé	Remplacé par
`{READVALUE}`	La valeur qui a déclenché l'alarme
`{TIMESTAMP}`	Quand la lecture a été effectuée

Par exemple, `ALARM: server room at {READVALUE} ({TIMESTAMP})` produit un message qui dit ce qui a été mesuré et quand, sans que quiconque ait besoin d'ouvrir l'interface.



Les badges en dessous du champ insèrent un espace réservé au curseur

Cliquez sur **Save**. La règle est vérifiée à chaque lecture à partir de maintenant.

Partie 3 : Lectures et rapports

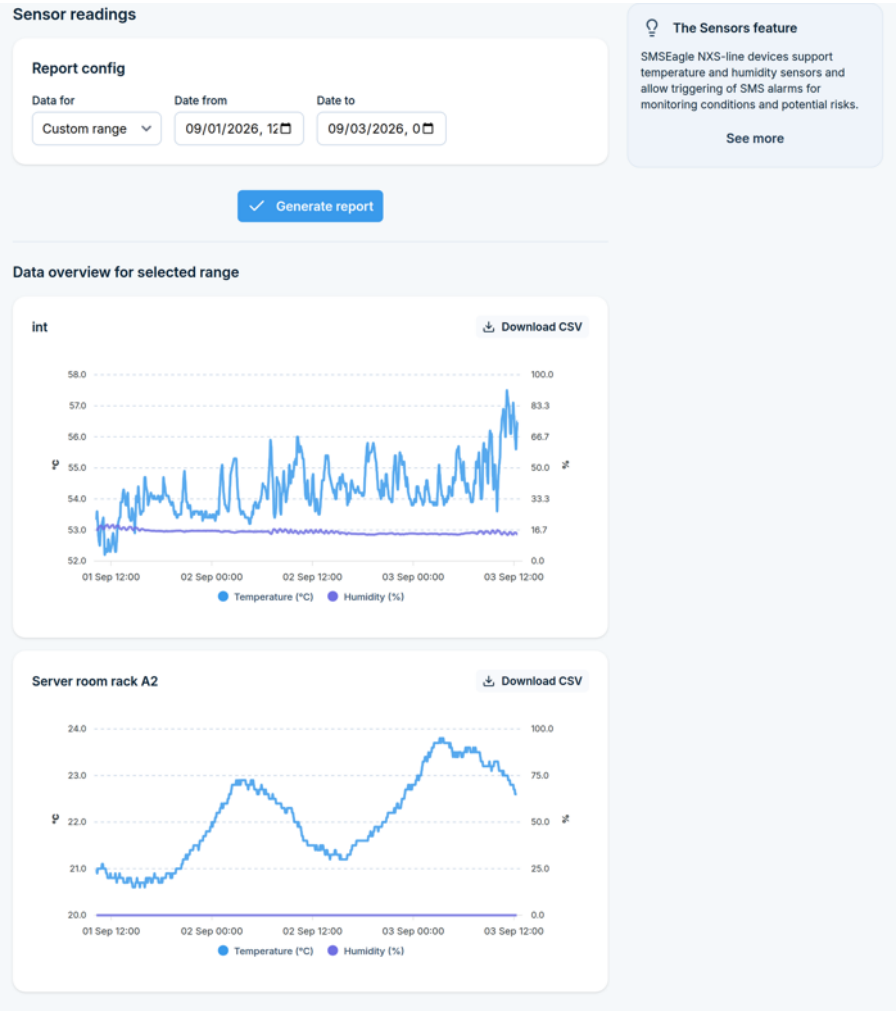
Allez à **Monitoring > Temp & Humidity > Reading**.

Dans la boîte **Report config**, choisissez :

Champ	À quoi elle sert
Data for	Une plage de dates prédéfinie. En en choisir une remplit les dates ci-dessous.
Date from / **Date to**	La plage exacte. La modification de ces champs bascule **Data for** sur une plage personnalisée.

Cliquez sur **Generate report**. Ci-dessous, sous **Data overview for selected range**, vous obtenez un graphique par capteur, traçant sa température et son humidité sur la période.

Chaque graphique dispose d'un bouton **Download CSV**, qui exporte les lectures de ce capteur pour la plage sélectionnée.



Lectures de capteur

Si la page indique **No sensors found**, aucun capteur n'a été détecté pour le moment. Connectez-en un et exécutez **Scan for new sensors** sur la page Paramètres des capteurs.

Comment cela fonctionne

- Les alarmes sont évaluées au moment où une lecture est effectuée, le temps de réaction dépend donc de **Read sensor every**. Un intervalle de 15 minutes signifie qu'une alarme peut être jusqu'à 15 minutes en retard.
- Un capteur désactivé n'est pas lu du tout, donc les règles d'alarme pointant vers celui-ci restent silencieuses.
- Si plusieurs règles correspondent à la même lecture, **chacune** d'elles envoie son propre SMS.

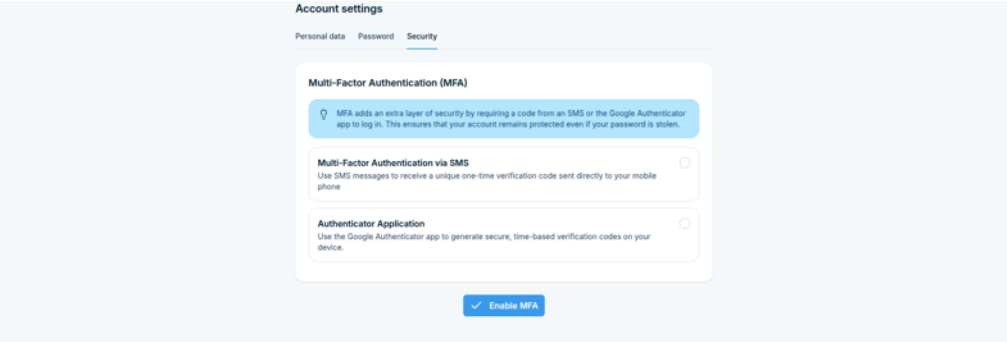
Paramètres

Ce chapitre couvre la section **Paramètres** de l'interface web, en suivant le même menu de deuxième niveau que vous voyez dans la barre latérale.

Paramètres du compte

Cliquez sur votre avatar (en bas à gauche) et choisissez **Account settings** pour gérer votre compte, réparti sur trois onglets : **Personal data** (nom, identifiant, numéro de téléphone, langue de l'interface, paramètres par défaut de composition, son de notification), **Password** et **Security** - voir Web Interface Overview pour la disposition complète des onglets.

Comment configurer l'authentification multifacteur (MFA)



Configuration MFA sous Paramètres du compte > Sécurité

MFA ajoute une couche de sécurité supplémentaire en exigeant un code à usage unique, en plus du mot de passe, pour se connecter. Cela protège le compte même si le mot de passe est volé.

Où le trouver

- **Par utilisateur** : **Account settings > Security** (`/settings/account/security`), pour votre compte.
- **À l'échelle de l'appareil** : l'option **Two-factor authentication** à l'étape Administrateur de l'"Assistant de configuration, et lors de la création ou de la modification d'un utilisateur sous **System > Users**.

Étape 1 : Choisir une méthode MFA

Sous **Account settings > Security**, choisissez l'une des options suivantes :

- **Multi-Factor Authentication via SMS** - un code de vérification à usage unique est envoyé à votre téléphone mobile par SMS à chaque connexion.
- **Authenticator Application** - des codes basés sur le temps sont générés par une application telle que Google Authenticator.

Cliquez sur **Enable MFA** et suivez les étapes à l'écran pour confirmer la méthode choisie.

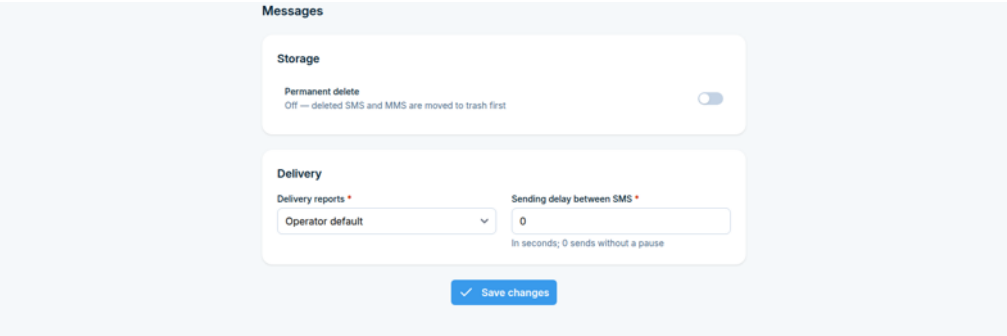
Étape 2 : Appliquer MFA à l'échelle de l'appareil (facultatif)

Un administrateur peut exiger MFA pour chaque compte au lieu de le laisser facultatif par utilisateur. Dans **Administrator** de l'assistant d'installation (ou par utilisateur sous **System > Users**), définissez **Two-factor authentication** sur :

- **Do not enforce** - chaque utilisateur décide individuellement s'il doit activer MFA.
- **Enforce for all users** - chaque utilisateur existant et nouveau doit configurer MFA.
- **Enforce for new users** - MFA est obligatoire uniquement pour les comptes créés à partir de maintenant.

SMS / MMS

Messages



Paramètres des messages sous SMS / MMS

Settings > SMS / MMS > Messages (`/settings/sms-mms/messages/`) regroupe le comportement général du pipeline de stockage et de livraison des SMS/MMS.

Stockage

Permanent delete - désactivé par défaut, donc les SMS et MMS supprimés sont d'abord déplacés vers la Corbeille au lieu d'être supprimés immédiatement.

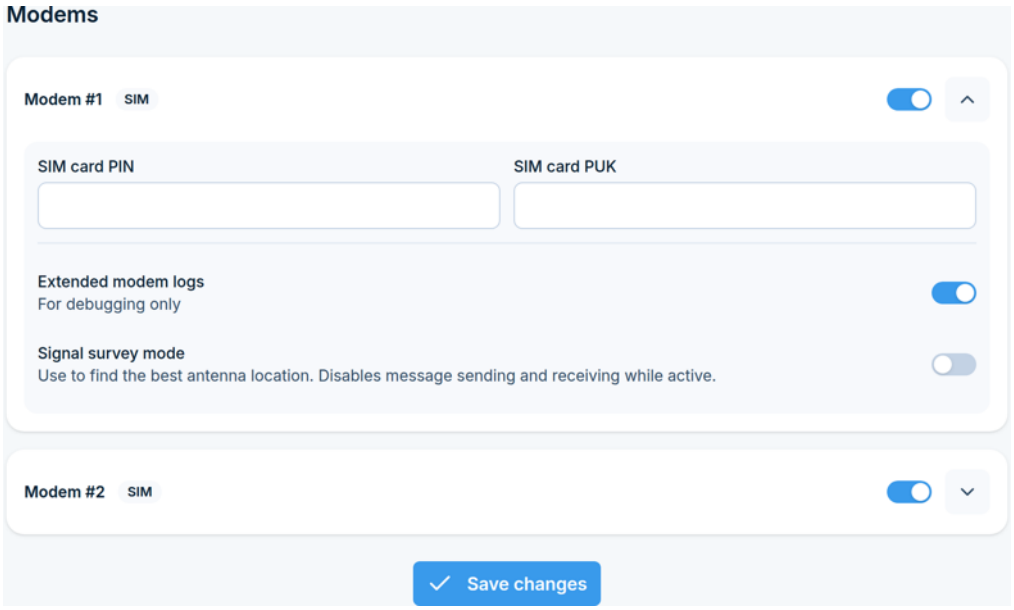
Livraison

Les rapports de livraison vous permettent de déterminer si un SMS envoyé a vraiment atteint le téléphone du destinataire.

- **Rapports de livraison** - Paramètre par défaut de l'opérateur (utiliser le comportement par défaut appliqué par votre opérateur mobile), Toujours demander, ou Ne jamais demander. Également proposé lors de l'"Assistant de configuration.
- **Délai d'envoi entre les SMS** - une pause, en secondes, insérée entre les SMS sortants consécutifs. `0` envoie sans pause.

Quand un rapport de livraison est demandé, SMSEagle met à jour le statut du message dans Éléments envoyés / Boîte d'envoi dès que le réseau confirme la livraison (ou signale un échec), et le rapport devient visible dans les détails du message.

Modems



Paramètres Modems, avec la section du premier modem développée. NXS-9700 répertorie une section modem

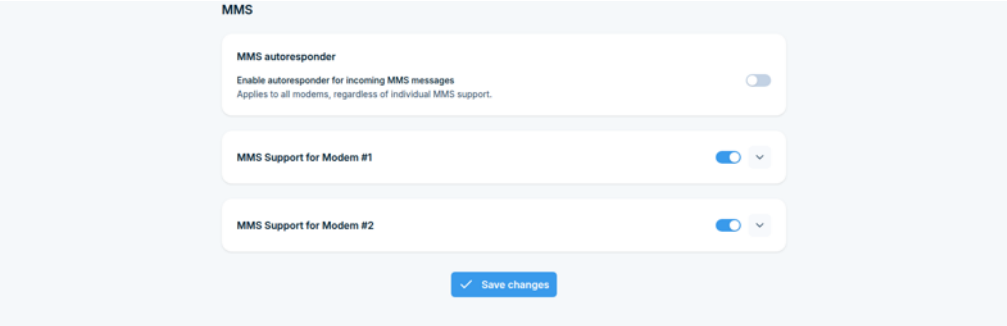
Paramètres > SMS / MMS > Modems (`/settings/sms-mms/modems/`) répertorie le modem intégré (Modem #1) avec un commutateur pour activer sa SIM. Le développement de la section d'un modem révèle quatre paramètres :

- **PIN de la carte SIM** et **PUK de la carte SIM** - uniquement nécessaires si la carte les demande. Les deux mêmes champs sont proposés lors de l'"Assistant de configuration.
- **Journaux modem étendus** - enregistrement modem détaillé, pour le débogage uniquement.
- **Mode d'enquête de signal** - l'utiliser pour trouver le meilleur emplacement d'antenne. Il **désactive l'envoi et la réception de messages** tant qu'il est actif, donc désactivez-le quand vous avez terminé.

Multimodem

NXS-9700 est livré avec un seul modem intégré, donc la stratégie de sélection des modems et les paramètres de basculement des modems ne s'appliquent pas - tout le trafic SMS/MMS passe par le seul modem intégré. Les produits SMSEagle multimodems (NXS-9750, NXS-9850, MHD-8100) exposent cette page sous **Paramètres > SMS / MMS > Multimodem**, avec une stratégie de sélection (Alternance circulaire, SIM 1/SIM 2 comme modem maître) et un mécanisme de basculement modem entre leurs modems intégrés.

MMS



Paramètres MMS, affichés ici sur un appareil à deux modems. NXS-9700 répertorie une section modem

Ce que cette fonction fait

MMS permet à l'appareil d'envoyer et de recevoir des **messages multimédias** : un texte avec des images ou d'autres fichiers joints, plutôt que du SMS brut.

Contrairement aux SMS, les MMS ne circulent pas sur le canal GSM brut. Ils passent par le réseau de données de l'opérateur vers un centre MMS, donc chaque carte SIM a besoin de son propre ensemble de paramètres de connexion (APN, MMSC et éventuellement un proxy). Dans SMSEagle, ces paramètres sont définis **par modem**, sous **Paramètres > Canaux > SMS / MMS > MMS**.

Le même écran contient également le **répondeur automatique MMS**, qui envoie une réponse automatique à chaque MMS entrant.

Avant de commencer

- Vous avez besoin des paramètres MMS pour chaque carte SIM auprès de son opérateur : **APN**, adresse **MMSC** et un **proxy** avec **port** si l'opérateur en utilise un. Certains opérateurs exigent également un nom d'utilisateur et un mot de passe.
- La SIM doit avoir MMS activé sur le forfait. Une SIM qui peut envoyer des SMS mais n'a pas de service de données ou MMS échouera peu importe comment les paramètres sont remplis.
- De nombreux profils d'opérateurs sont déjà connus de l'appareil, alors essayez **Lire les paramètres APN** avant de chercher les valeurs vous-même.

Étape 1 : Ouvrir la page MMS

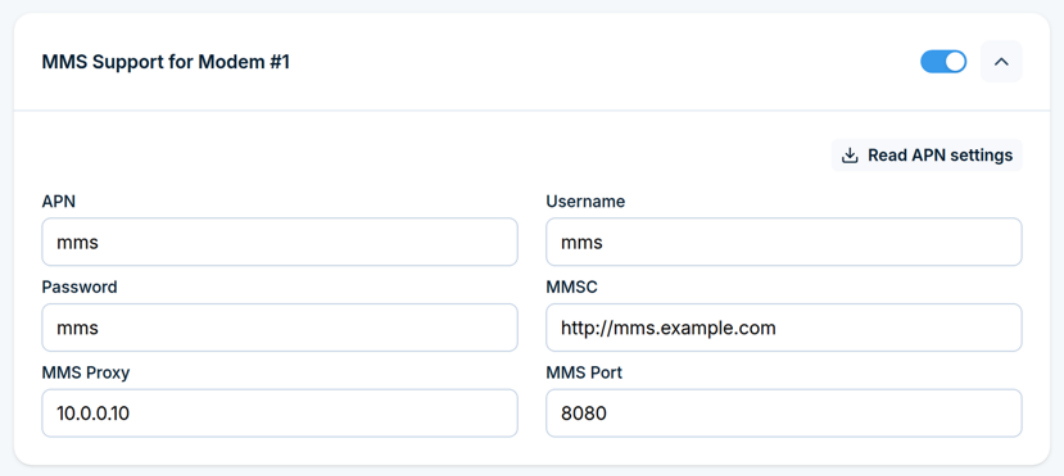
Dans la barre latérale, allez à **Paramètres > Canaux > SMS / MMS > MMS**.

La page MMS affiche la boîte du **répondeur automatique MMS** en haut, puis une section dépliable par modem. NXS-9700 a un seul modem intégré, donc il y a une section, titrée **Support MMS pour Modem #1**.

Étape 2 : Activer MMS sur un modem

La section du modem a un commutateur à côté de son en-tête. Activez-le si la SIM doit gérer les MMS.

Ensuite, cliquez sur la flèche à droite de l'en-tête pour développer la section et remplissez les paramètres de connexion.



Une section modem développée, avec **Lire les paramètres APN** au-dessus des champs

Étape 3 : Remplir les paramètres de connexion

Le chemin le plus rapide est le bouton **Lire les paramètres APN** en haut de la section développée. Il recherche une configuration correspondante pour la carte SIM actuellement dans ce modem et remplit les champs pour vous. Si aucune correspondance n'est trouvée, SMSEagle le signale et vous entrez les valeurs manuellement.

Champ	Quoi entrer
APN	Le nom du point d'accès de l'opérateur, par exemple `internet`.
Nom d'utilisateur	L'utilisateur APN, si l'opérateur en demande un. Laissez vide sinon.
Mot de passe	Le mot de passe APN, s'il est requis.
MMSC	L'adresse du centre MMS de l'opérateur, par exemple `http://mms.example.com`.
Proxy MMS	L'adresse du proxy, si l'opérateur en utilise un. Laissez vide sinon.
Port MMS	Le port du proxy. Nécessaire uniquement avec un proxy.

Toutes ces valeurs appartiennent à la carte SIM de ce modem, elles proviennent donc de l'opérateur de cette carte SIM. Laissez **Proxy MMS** et **Port MMS** vides sauf si l'opérateur utilise réellement un proxy.

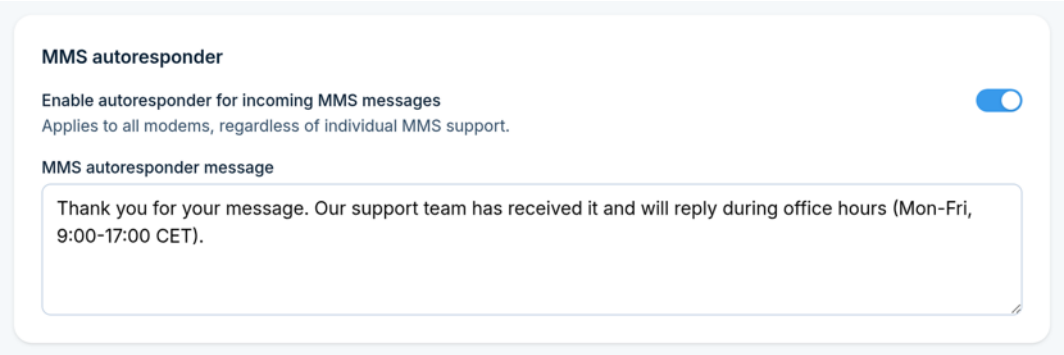
Étape 4 : Configurer le répondeur automatique (optionnel)

La boîte **Répondeur automatique MMS** en haut de la page MMS envoie une réponse automatique chaque fois qu'un MMS arrive.

1. Activez **Activer le répondeur automatique pour les messages MMS entrants**.

2. Tapez la réponse dans **Message du répondeur automatique MMS**.

Le répondeur **s'applique à tous les modems, indépendamment du support MMS individuel**. C'est un paramètre global unique, pas un paramètre par modem, et il existe un texte de réponse unique partagé par tous les MMS entrants, donc gardez la formulation générale.



Le répondeur, activé avec un exemple de réponse

Étape 5 : Enregistrer et redémarrer

Cliquez sur **Enregistrer les modifications**.

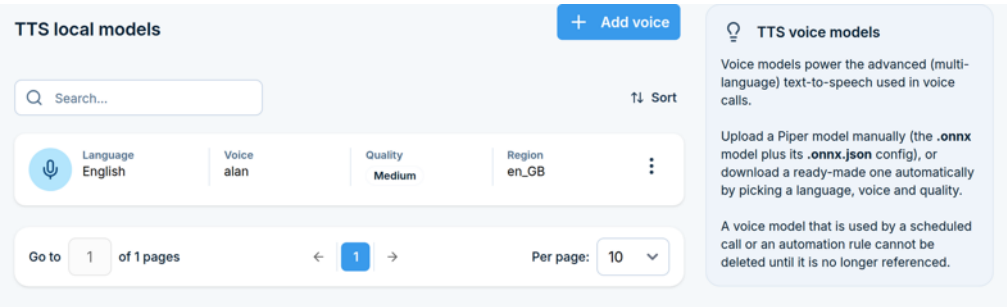
> **Un redémarrage est nécessaire.** Après l'enregistrement, SMSEagle vous demande de redémarrer l'appareil pour que les modifications MMS prennent effet. Jusqu'à ce que vous le fassiez, les nouveaux paramètres sont stockés mais pas encore en utilisation.

Appels

Modèles locaux TTS

Les modèles de voix locaux alimentent **Texte vers parole - avancé**. Ils s'exécutent sur l'appareil, donc aucune connexion Internet n'est nécessaire une fois qu'un modèle est installé.

Allez à **Settings > Channels > Calls > TTS local models**. La page liste les modèles installés avec leur langue, région et qualité.



Modèles locaux TTS

Ajouter un modèle

Cliquez sur **Add voice** dans le coin supérieur droit. Le panneau offre deux façons de le faire.

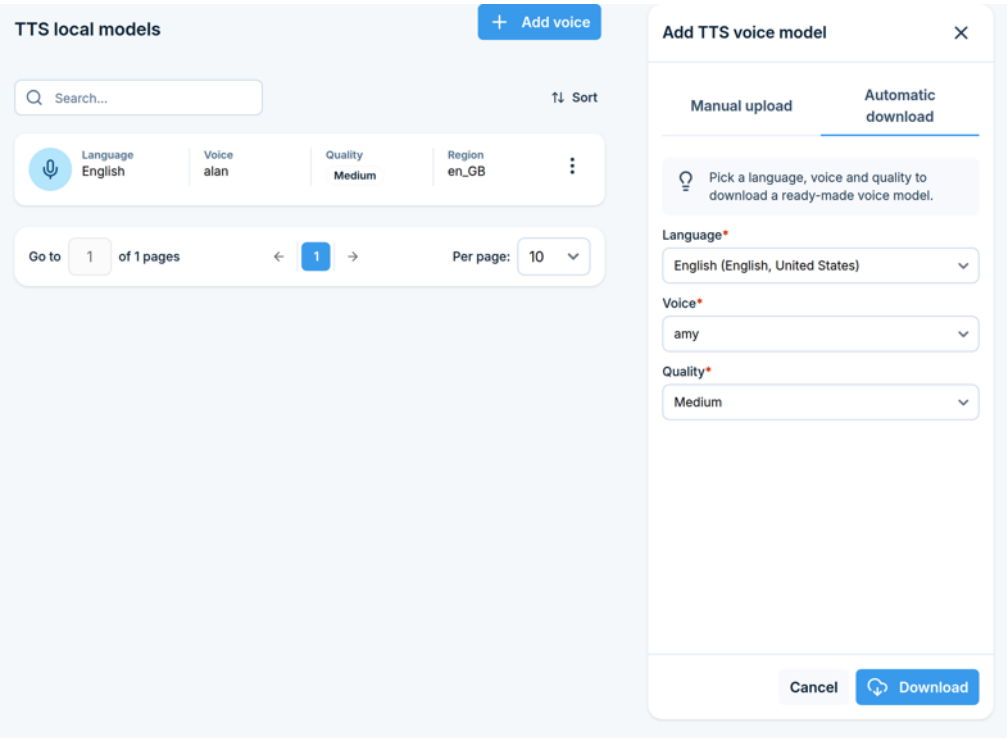
Téléchargement automatique (le moyen facile)

Sur l'onglet **Automatic download**, choisissez dans l'ordre :

1. **Language**
2. **Voice**
3. **Quality** - **Very low**, **Low**, **Medium** ou **High**

Cliquez sur **Download**. Une barre de progression affiche le téléchargement, et le modèle apparaît dans la liste lorsqu'il se termine.

Une qualité plus élevée signifie une voix plus naturelle mais un fichier plus volumineux et une synthèse légèrement plus lente. **Medium** est une bonne valeur par défaut.



Téléchargement d'un modèle de voix préconfectionné

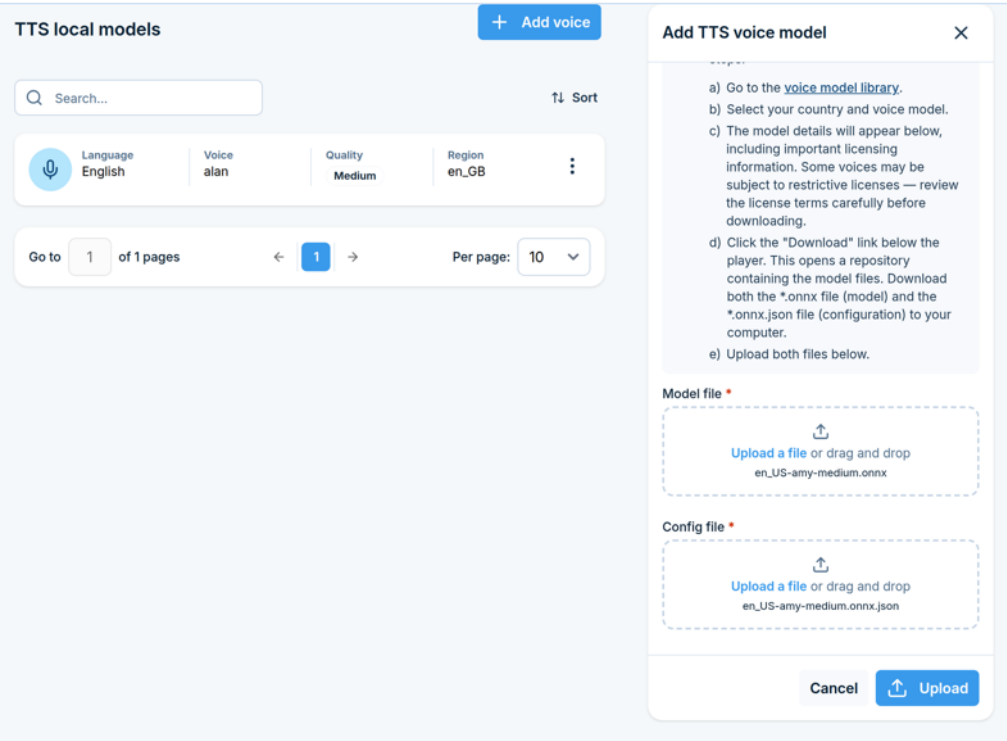
> Si le panneau affiche « Voice list unavailable », l'appareil n'a pas pu accéder au catalogue de voix en ligne. Vérifiez les paramètres réseau et réessayez plus tard, ou utilisez le téléchargement manuel à la place.

Téléchargement manuel

Sur l'onglet **Manual upload**, vous fournissez vous-même un modèle de voix :

1. **Model file (.onnx)** - le modèle lui-même.
2. **Config file (.onnx.json)** - son fichier de configuration correspondant.

Les deux fichiers sont obligatoires et doivent être associés. Cliquez sur **Upload**.



Téléchargement manuel d'un modèle Piper

Supprimer un modèle

Utilisez l'action **Delete** à côté d'un modèle, ou cochez plusieurs et supprimez-les ensemble.

Un modèle qui est encore référencé quelque part ne peut pas être supprimé. Le message vous indique où il est utilisé, par exemple dans un appel programmé, une règle Email vers SMS, une action d'entrée ou de sortie numérique, ou une tâche de surveillance du réseau. Modifiez ou supprimez d'abord cette référence, puis supprimez le modèle.

Modèles TTS en ligne (ElevenLabs)

Les modèles en ligne produisent la parole la plus naturelle, mais ils utilisent l'API ElevenLabs, ils nécessitent donc un compte ElevenLabs et une connexion Internet.

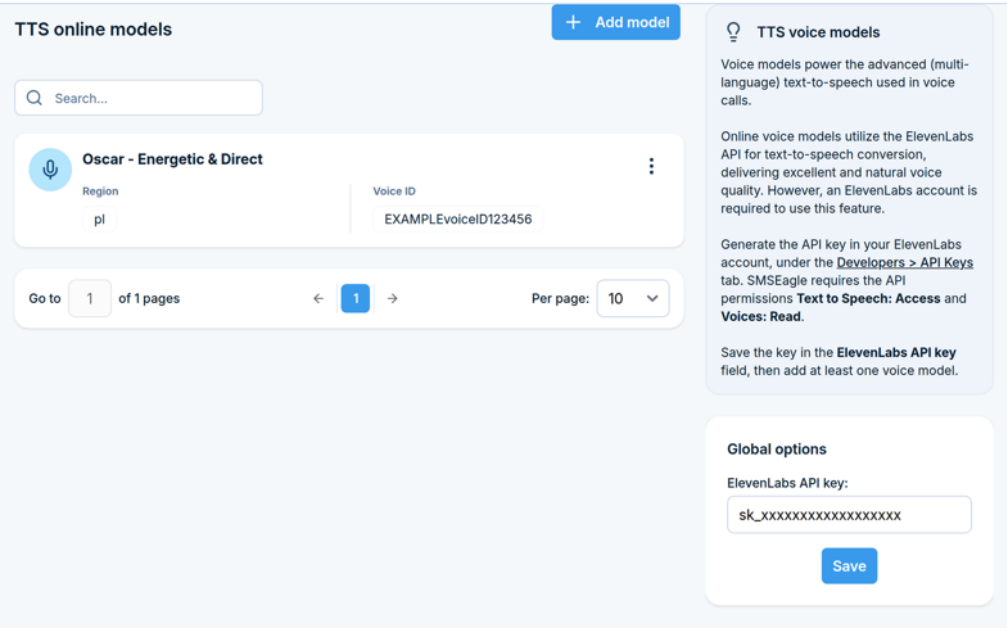
Allez à **Settings > Channels > Calls > TTS online models**.

Étape 1 : Préparez le compte ElevenLabs

Dans votre compte ElevenLabs :

1. Allez dans **Développeurs > Clés API** et générez une clé API.
2. Donnez à la clé les permissions **Text to Speech: Access** et **Voices: Read**, puis enregistrez.
3. Allez dans l'onglet **Voices**, choisissez la voix que vous voulez et ajoutez-la à votre compte.
4. Ouvrez **My Voices** et copiez l'"**ID de voix** de cette voix.

La page a un bouton qui vous amène directement aux paramètres ElevenLabs.



Modèles TTS en ligne

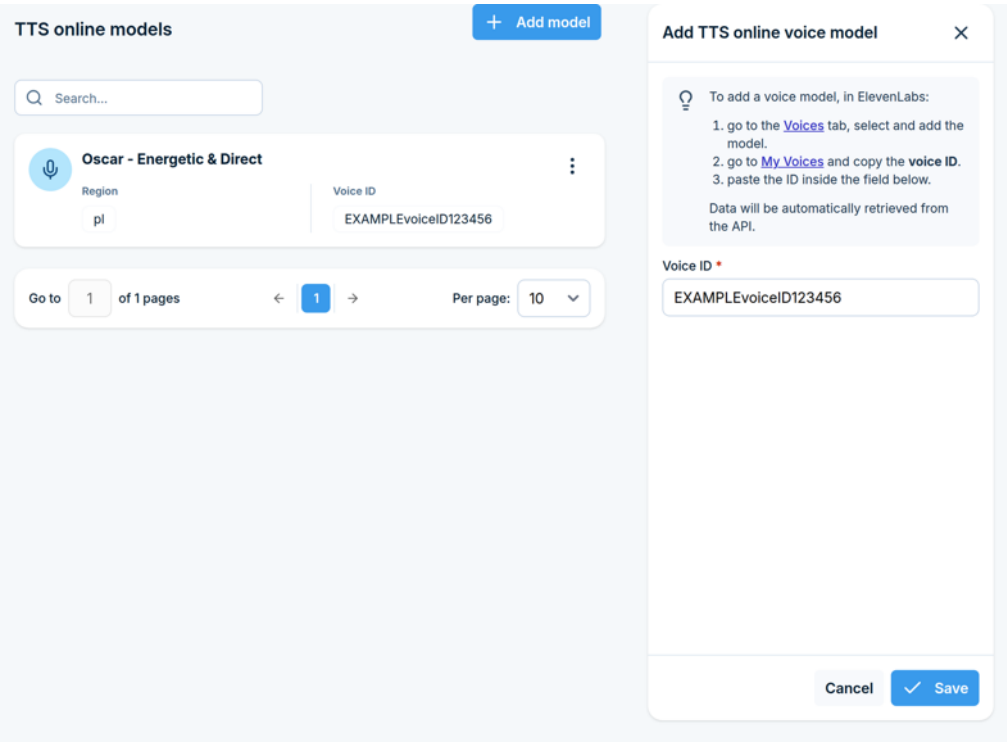
Étape 2 : Enregistrez la clé API

Dans la boîte **Global options** sur la droite, collez la clé dans **ElevenLabs API key** et cliquez sur **Save**.

Étape 3 : Ajoutez un modèle de voix

Cliquez sur **Add model** dans le coin supérieur droit, collez l'**ID de voix** que vous avez copié et cliquez sur **Save**.

Le reste des données du modèle (nom, langue, région) sont récupérés automatiquement depuis l'API et affichés dans la liste.



Ajout d'un modèle de voix ElevenLabs

Les modèles peuvent être modifiés (pour pointer vers un ID de voix différent) ou supprimés de la liste, individuellement ou en masse.

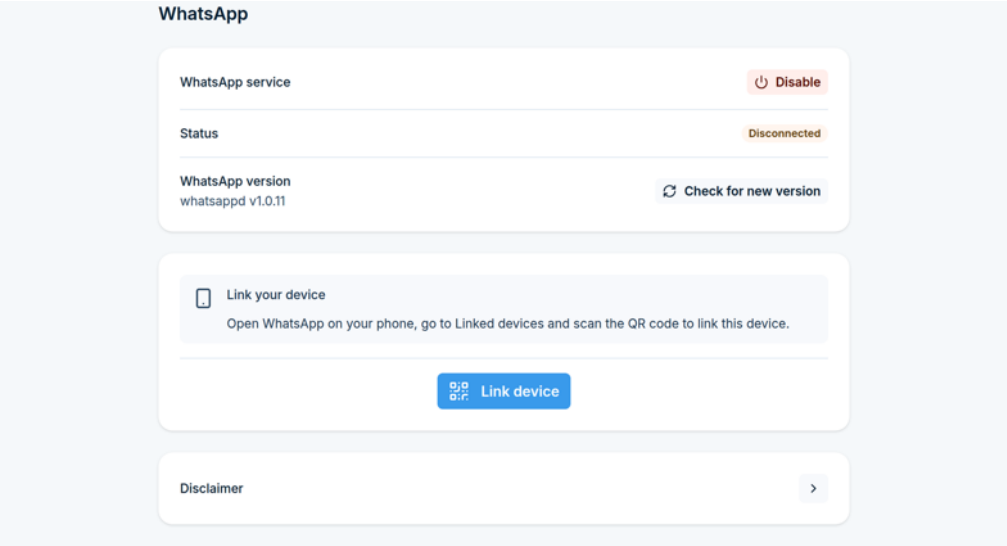
Appels entrants

Settings > Channels > Calls > Incoming calls (`/settings/calls/incoming-calls`) définit, par modem, comment un appel vocal entrant est traité : **Always accept**, **Always reject**, ou **Ignore**.

Renvoi d'appel

Settings > Channels > Calls > Call forward (`/settings/calls/call-forward`) gère les codes de renvoi d'appel par modem. Tous les opérateurs réseau ne supportent pas les codes de renvoi - vérifiez auprès de votre opérateur avant de compter sur cette fonctionnalité.

WhatsApp



Paramètres WhatsApp et liaison d'appareil

Ce que cette fonction fait

Le support WhatsApp permet à votre SMSEagle d'envoyer et de recevoir des **messages WhatsApp** en plus des SMS. L'appareil est lié à un compte WhatsApp de la même manière qu'une session de bureau ou de navigateur : vous scannez un code QR avec le téléphone qui possède le compte.

Une fois liée, WhatsApp devient un autre canal que vous pouvez choisir lors de la composition d'un message, avec sa propre vue de conversation. Il y a aussi une option **fallback**, qui envoie un SMS ou MMS à la place chaque fois qu'un destinataire n'a pas WhatsApp.

Utilisations typiques : atteindre les personnes qui utilisent WhatsApp, envoyer des notifications plus longues sans les diviser en plusieurs parties SMS, ou réduire le coût des messages vers les destinataires à l'étranger.

La configuration se fait en deux étapes : d'abord vous activez le service et liez un appareil (**Settings > Channels > WhatsApp**), puis vous utilisez le canal (**Messages > WhatsApp**, ou la fenêtre Compose).

Avant de commencer

- WhatsApp est disponible sur certains modèles d'appareil uniquement. Si **Settings > Channels > WhatsApp** n'est pas dans votre barre latérale, votre appareil ne le supporte pas.
- Vous avez besoin d'un téléphone avec un compte WhatsApp actif, en main, pour scanner le code QR.
- L'appareil doit pouvoir accéder à Internet. Les messages WhatsApp voyagent via la connexion réseau, pas via le modem.

  Le compte lié est un vrai compte WhatsApp. Tout ce que la passerelle envoie semble provenir de ce compte, et les messages qui lui sont envoyés apparaissent dans SMSEagle.

Étape 1 : Ouvrir les paramètres WhatsApp

Dans la barre latérale, allez à **Paramètres > Canaux > WhatsApp**.

La zone **Connexion** affiche la **version WhatsApp** installée et le **Statut** actuel. Sur un appareil neuf, le statut est **Désactivé** et un avertissement explique que le service doit être activé avant qu'un appareil puisse être lié.

Étape 2 : Activer le service

Cliquez sur **Activer** en bas de la page. Le statut change en **Déconnecté**, ce qui signifie que le service fonctionne mais qu'aucun compte n'est encore lié. C'est l'état montré dans la figure au début de cette section, avec le bouton **Lier un appareil** qui attend sous la zone Connexion.

Étape 3 : Lier votre téléphone

1. Cliquez sur **Lier un appareil**. Un code QR apparaît à l'écran.
2. Sur votre téléphone, ouvrez **WhatsApp**, allez à **Appareils liés** et choisissez de lier un nouvel appareil.
3. Pointez le téléphone vers le code QR affiché à l'écran.

Pendant que le code s'affiche, la page continue de vérifier s'il a été scanné et rafraîchit le code automatiquement. Lorsque le téléphone confirme, le statut change en **Connecté**.

> **Le code QR n'attend pas indéfiniment.** Si aucun appareil ne le scanne dans un court laps de temps, la liaison est annulée et la page revient à **Déconnecté**. Ayez le téléphone ouvert sur l'écran **Appareils liés** avant de cliquer sur **Lier un appareil**, et cliquez simplement à nouveau si le code expire.

Vous pouvez également arrêter le processus avec **Annuler la liaison**.

Étape 4 : Décider ce qui se passe pour les destinataires non WhatsApp

Une fois que le statut est **Connecté**, une zone **Secours** apparaît avec un commutateur :

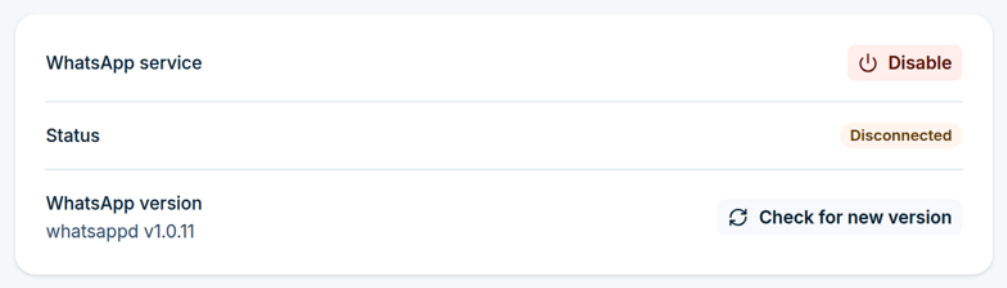
Basculer vers SMS/MMS Quand il est activé, un message adressé à un numéro qui n'est pas enregistré sur WhatsApp est envoyé en SMS ou MMS au lieu d'échouer. Quand il est désactivé, un tel message n'est simplement pas livré.

Le commutateur est enregistré dès que vous le basculez, il n'y a pas de bouton d'enregistrement séparé.

Étape 5 : Maintenir le service à jour

La zone **Connexion** dispose d'un bouton **Vérifier la nouvelle version**. Cliquez dessus pour demander si une version WhatsApp plus récente est disponible :

Résultat	Ce qu'il faut faire
Aucune nouvelle version trouvée	Rien. Vous êtes à jour.
Une nouvelle version est disponible	Le bouton se transforme en **Mettre à jour maintenant**, qui vous amène à la page de correctif où la mise à jour peut être installée.
Impossible de récupérer la dernière version	L'appareil n'a pas pu atteindre le serveur de mise à jour. Vérifiez les paramètres réseau et réessayez plus tard.



La zone Connexion, avec **Vérifier la nouvelle version** à côté de la version installée

Déliaison et désactivation

Deux boutons en bas de la page des paramètres font des choses différentes :

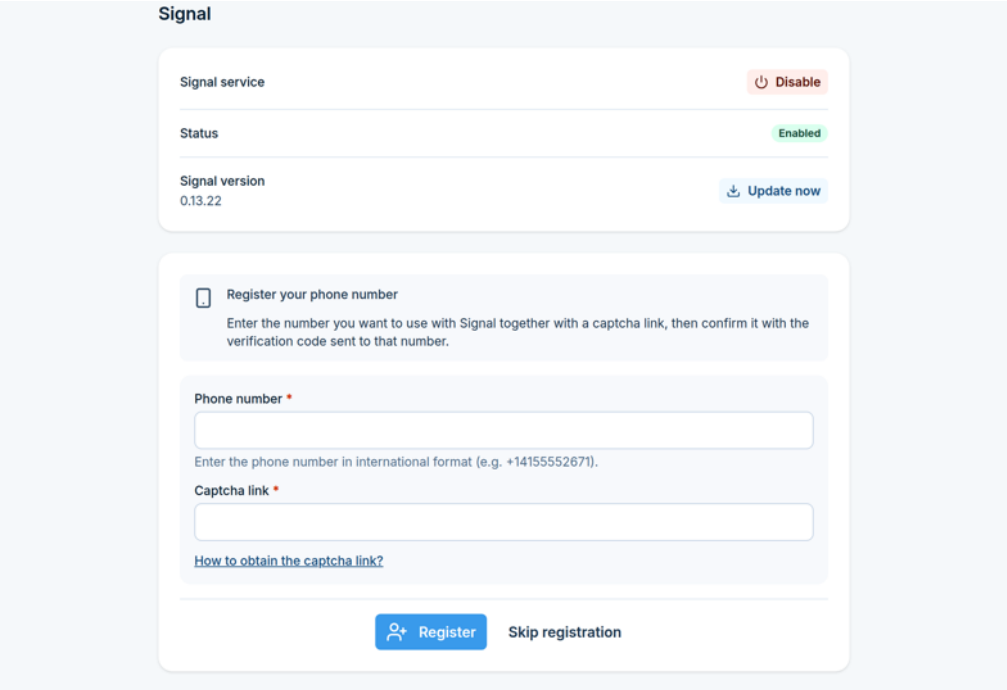
Bouton	Ce qu'il fait
Unlink device	Déconnecte le compte. Le service continue de fonctionner, la page revient à **Disconnected** et vous pouvez lier un autre compte. **Fall back to SMS/MMS** est désactivé en même temps.
Disable	Arrête complètement le service WhatsApp. Le canal disparaît de la fenêtre de composition.

Vous pouvez aussi vous délier depuis le téléphone, dans **WhatsApp > Linked devices**. La page affiche alors **Disconnected** à son prochain rafraîchissement.

Bon à savoir

- Les messages WhatsApp utilisent la connexion réseau, ils ne consomment donc pas de crédit SIM et ne dépendent pas de la couverture GSM. L'option **Fall back to SMS/MMS** en est l'exception : ces messages de secours passent par le modem.
- Le lien est stocké sur l'appareil. La restauration d'une sauvegarde sur un matériel différent, ou un déliaison depuis le téléphone, nécessite de scanner un nouveau code QR.
- Seuls les messages reçus après la liaison de l'appareil apparaissent dans la liste de conversation.

Signal



Paramètres du service Signal

Ce que cette fonction fait

Le support Signal permet à votre SMSEagle d'envoyer et de recevoir des **messages Signal** en plus des SMS. L'appareil s'enregistre auprès du réseau Signal en utilisant un numéro de téléphone, et à partir de là Signal devient un autre canal que vous pouvez choisir lors de la composition d'un message, avec sa propre vue de conversation.

Utilisations typiques : atteindre les personnes qui préfèrent Signal aux SMS, ou envoyer des alertes aux destinataires qui sont à l'étranger et qui entraîneraient autrement des frais d'itinérance.

La mise en place se fait en deux étapes : d'abord vous activez le service et enregistrez un numéro (**Settings > Channels > Signal**), puis vous utilisez le canal (**Messages > Signal**, ou la fenêtre de composition).

Avant de commencer

- Signal n'est disponible que sur certains modèles d'appareil. Si **Settings > Channels > Signal** ne figure pas dans votre barre latérale, votre appareil ne le supporte pas.
- Vous avez besoin d'un numéro de téléphone qui peut recevoir un code de vérification, et il ne doit pas déjà être enregistré auprès de Signal sur un autre appareil.
- L'enregistrement nécessite un **lien captcha**, que vous générez dans un navigateur. Gardez le lien à portée de main avant de commencer ; il expire rapidement.

Étape 1 : Ouvrir les paramètres Signal

Dans la barre latérale, allez à **Settings > Channels > Signal**.

La boîte **Service** en haut affiche la **version Signal** installée et le **statut** actuel. Sur un appareil neuf, le statut est **Disabled** et un avertissement explique que le service doit être activé avant qu'un numéro puisse être enregistré.

Étape 2 : Activer le service

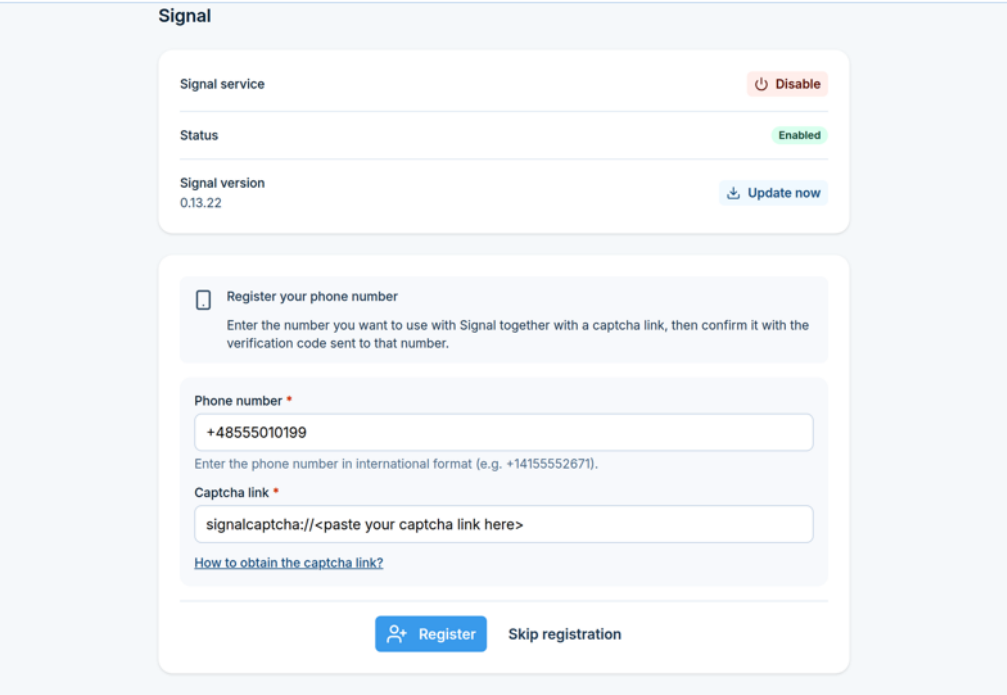
Cliquez sur **Enable** en bas de la page. Le statut passe à **Enabled** et le formulaire d'enregistrement apparaît, comme dans la figure au début de cette section.

Étape 3 : Enregistrer un numéro de téléphone

Dans la boîte **Register a phone number** :

1. Dans **Phone number**, tapez le numéro au format international, par exemple `+14155552671`.
2. Dans **Captcha link**, collez le lien captcha. Le lien **How to obtain the captcha link?** sous le champ ouvre des instructions étape par étape dans un nouvel onglet.
3. Cliquez sur **Register**.

Signal envoie alors un code de vérification au numéro.



Enregistrement d'un numéro de téléphone

Avez-vous déjà enregistré ce numéro récemment ? Cliquez sur **Skip registration** à la place. Le formulaire accède directement à l'étape de vérification, où vous pouvez entrer un code que vous avez déjà reçu.

Étape 4 : Vérifier le numéro

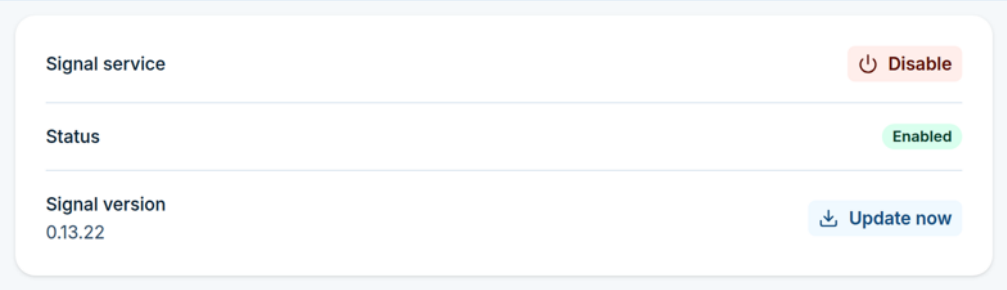
Le formulaire demande maintenant le **Verification code**. Tapez le code que vous avez reçu et cliquez sur **Verify**.

En cas de succès, la page indique que Signal est connecté et affiche la boîte **Registered number**.

Étape 5 : Maintenir le service à jour

La boîte **Service** dispose d'un bouton **Check for new version**. Cliquez dessus pour demander si une version plus récente de Signal est disponible :

Résultat	Ce qu'il faut faire
Aucune nouvelle version trouvée	Rien. Vous êtes à jour.
Une nouvelle version est disponible	Le bouton se transforme en **Mettre à jour maintenant**, qui vous amène à la page de correctif où la mise à jour peut être installée.
Impossible de récupérer la dernière version	L'appareil n'a pas pu atteindre le serveur de mise à jour. Vérifiez les paramètres réseau et réessayez plus tard.

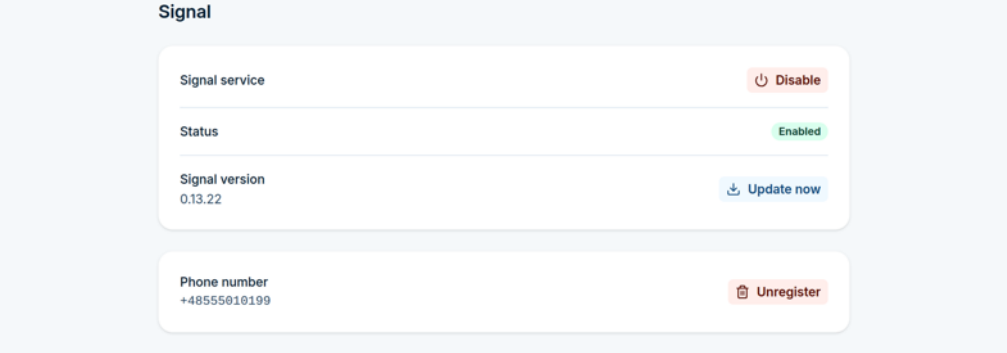


La boîte Service. Une vérification a déjà trouvé une version plus récente, le bouton indique donc **Update now**

Suppression du numéro

Pour désenregistrer l'appareil de Signal, retournez à **Settings > Channels > Signal** et cliquez sur **Unregister** dans la boîte **Registered number**. Le numéro est libéré et la page revient au formulaire d'enregistrement.

Pour désactiver le canal sans désenregistrer, cliquez sur **Disable** en bas de la page. Le service s'arrête et Signal disparaît de la fenêtre Compose, mais l'enregistrement est conservé, donc l'activation n'exige pas une nouvelle vérification.



Un numéro Signal enregistré

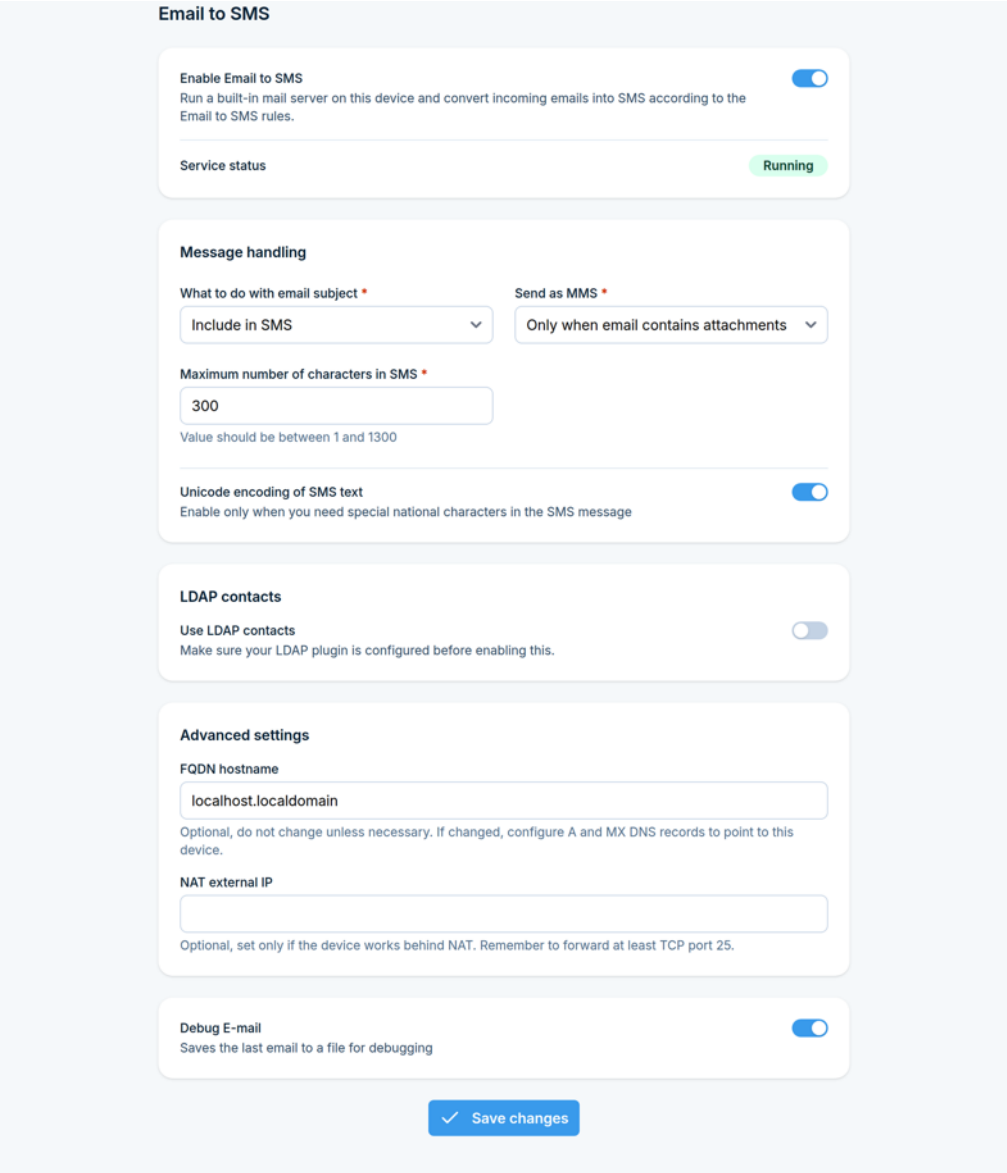
Bon à savoir

- Les messages Signal sont envoyés sur la connexion réseau, pas via le modem, ils n'utilisent donc pas le crédit SIM et ne dépendent pas de la couverture GSM.
- L'enregistrement se trouve sur l'appareil. La restauration d'une sauvegarde sur un matériel différent, ou la suppression du numéro, nécessite un nouvel enregistrement.
- Seuls les messages reçus après l'activation du service apparaissent dans la liste de conversation.

Email

Email vers SMS

Paramètres > Canaux > Email > Email vers SMS (`/settings/email/email-to-sms`) démarre un serveur de messagerie intégré sur l'appareil et convertit les emails entrants en SMS, selon les règles que vous définissez sous Email vers SMS dans Automation.



Paramètres Email vers SMS

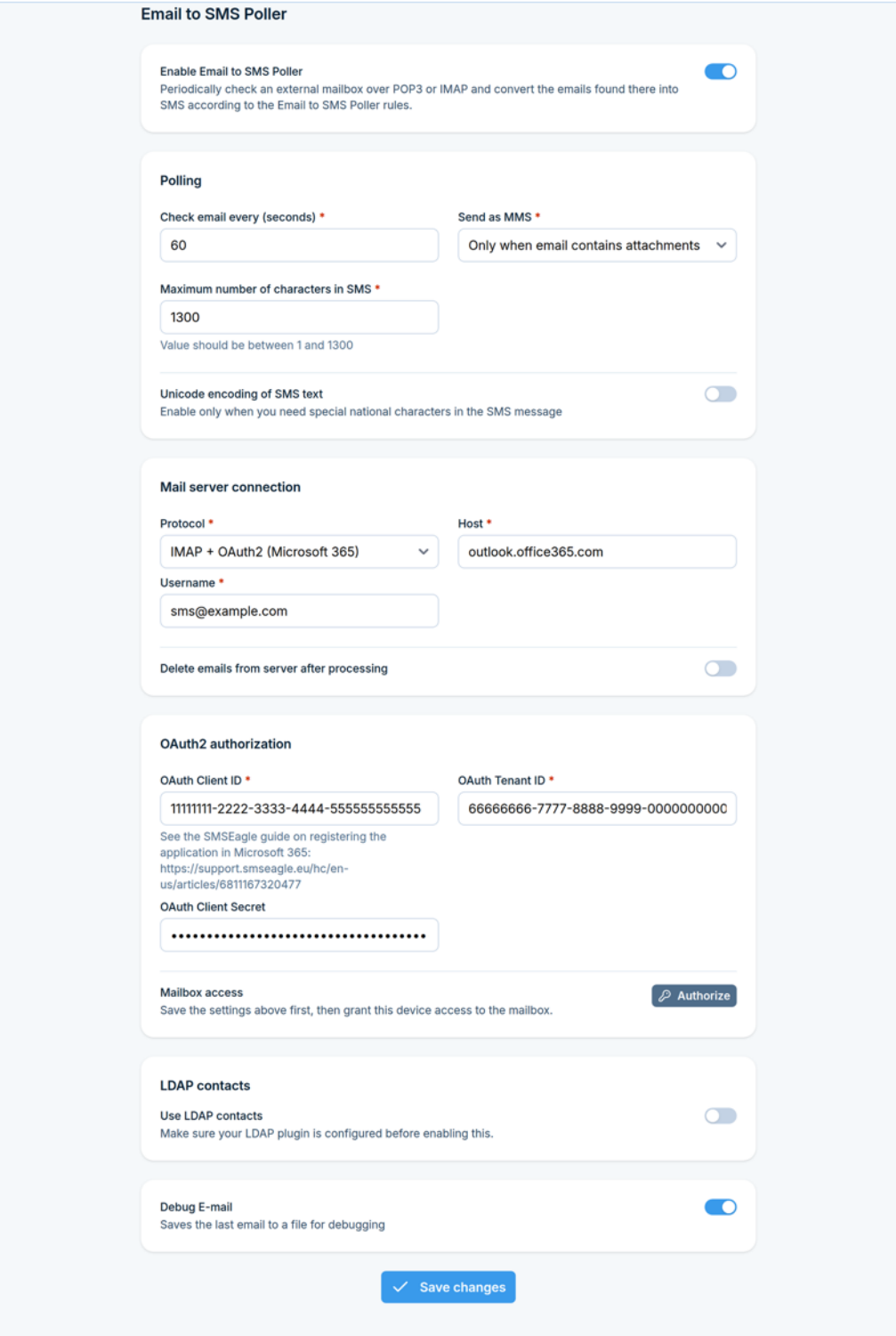
Activez **Enable Email to SMS** pour démarrer le serveur de messagerie. **Service status** indique s'il est **Running** ou **Stopped**. Le reste de la page détermine comment un email devient un SMS :

- **What to do with email subject** - **Ignore** le, **Include in SMS**, **Use for authentication**, ou **Send only subject without email body**.
- **Send as MMS** - **Never**, **Always**, ou **Only when email contains attachments**.
- **Maximum number of characters in SMS** - de 1 à 1300.

- **Unicode encoding of SMS text** - activez-le uniquement lorsque les messages ont besoin de caractères nationaux que l'alphabet SMS standard ne contient pas.
- **Use LDAP contacts** - permet à la partie destinataire de l'adresse de nommer un contact ou un groupe d'annuaire. Configurez d'abord LDAP.
- **FQDN hostname** (sous **Advanced settings**) - nom de domaine optionnel à utiliser dans les adresses des destinataires à la place de l'adresse IP de l'appareil. Si vous le modifiez, pointez les enregistrements DNS A et MX pour ce nom vers l'appareil.
- **NAT external IP** - définez-le uniquement lorsque l'appareil se trouve derrière un NAT, et transférez au moins le port TCP 25 vers l'appareil.
- **Debug E-mail** - enregistre le dernier email reçu dans un fichier pour dépannage.

Email to SMS Poller

Paramètres > Canaux > Email > Email vers SMS Poller (`/settings/email/email-to-sms-poller`) connecte l'appareil à une boîte aux lettres existante, la vérifie à intervalle fixe, et convertit les emails trouvés en SMS selon les règles sous Email vers SMS Poller dans Automation. Contrairement à Email vers SMS, aucun email ne doit être livré à l'appareil lui-même.



Paramètres Email vers SMS Poller, connectés à une boîte aux lettres Microsoft 365

Activez **Enable Email to SMS Poller**. Le formulaire ci-dessous a ces parties :

Polling

- **Check email every (seconds)** - fréquence de vérification de la boîte aux lettres.
- **Send as MMS**, **Maximum number of characters in SMS** et **Unicode encoding of SMS text** - même signification que pour Email vers SMS.

Mail server connection

- **Protocol** - **POP3**, **IMAP**, ou **IMAP + OAuth2 (Microsoft 365)**.
- **Host** et **Username** de la boîte aux lettres.
- Avec **POP3** et **IMAP** uniquement : **Port**, **Password** et **Use TLS/SSL encryption**. La page liste les ports standard : POP3 110, POP3 avec TLS/SSL 995, IMAP 143, IMAP avec TLS/SSL 993.
- **Delete emails from server after processing** - supprime chaque email de la boîte aux lettres une fois qu'il a été traité. Laissez-le désactivé pour garder la boîte aux lettres intacte.

OAuth2 authorization (uniquement avec **IMAP + OAuth2 (Microsoft 365)**)

- **OAuth Client ID**, **OAuth Tenant ID** et **OAuth Client Secret** de l'application enregistrée dans Microsoft 365. Consultez le guide SMSEagle sur l'enregistrement de l'application dans Microsoft 365.
- Enregistrez d'abord les paramètres, puis cliquez sur **Authorize** sous **Mailbox access** et accordez à l'appareil l'accès à la boîte aux lettres.

Use LDAP contacts et **Debug E-mail** fonctionnent comme pour Email vers SMS.

Pour POP3 et IMAP, la page a aussi un bouton **Test connection**. Enregistrez les paramètres avant de l'utiliser. Certains fournisseurs de messagerie bloquent les connexions de test IMAP selon leurs paramètres de sécurité par défaut, donc un test échoué ne signifie pas toujours que les paramètres sont incorrects.

Configuration SMTP

Settings > Channels > Email > SMTP Configuration (`/settings/email/smtp`) gère une liste de présets de serveur SMTP réutilisables et en assigne un à chaque fonction qui envoie des emails sortants :

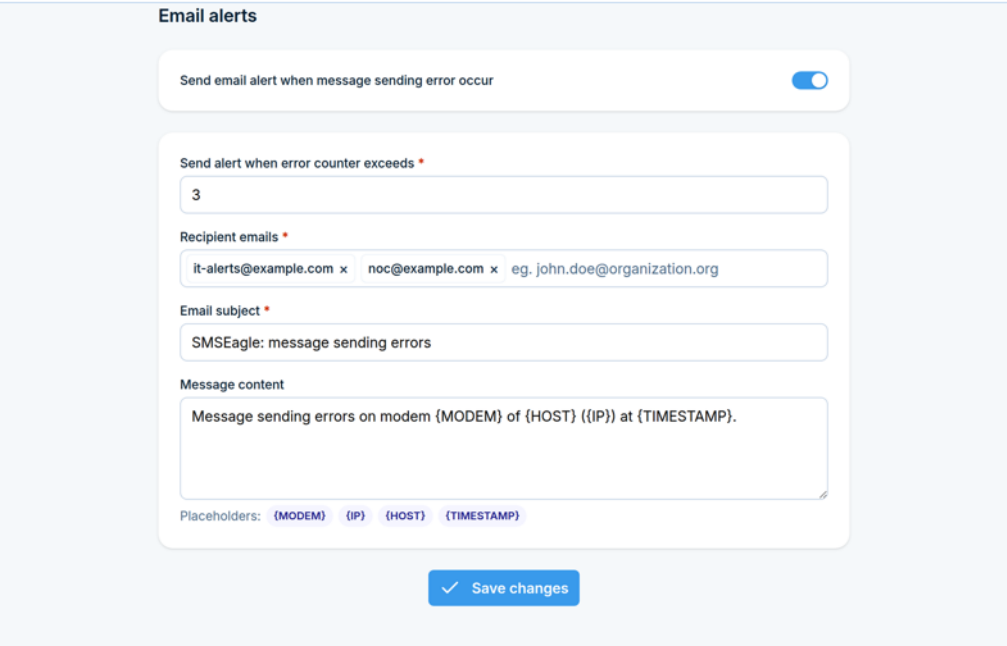
- **Compose menu**, **APIv2**, **SMS to Email**, **Alerts**, **Reporting module**, **Workflows**

Chacun peut être défini sur **None** ou sur l'un de vos présets enregistrés. Annuler l'assignation d'un préset à une fonction désactive la configuration email existante de cette fonction.

Cliquez sur **Create new** sous **Configuration presets** pour ajouter un serveur SMTP (host, port, encryption, sender address, credentials) ; les présets peuvent ensuite être sélectionnés dans la liste déroulante pour l'une des fonctions ci-dessus.

Alertes email

Paramètres > Canaux > Email > Email alerts (`/settings/email/alerts`) envoie une alerte par email lorsque les messages sortants continuent d'échouer à l'envoi. Il nécessite un préréglage SMTP assigné à **Alerts** sous Configuration SMTP.



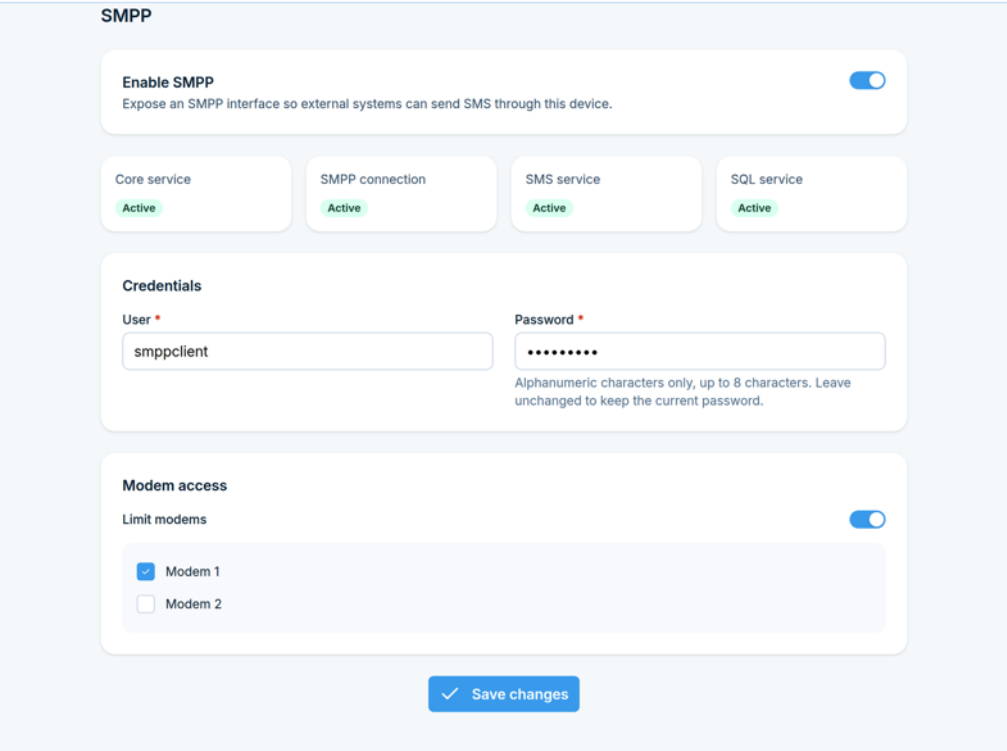
Paramètres d'alertes e-mail

Activez **Send email alert when message sending error occur**, puis configurez :

- **Send alert when error counter exceeds** - nombre d'erreurs d'envoi comptabilisées avant l'envoi de l'alerte. Une valeur supérieure à 2 évite les alertes causées par une défaillance temporaire unique.
- **Recipient emails** - une ou plusieurs adresses.
- **Email subject** et **Message content** - le texte de l'alerte. Les espaces réservés **{MODEM}** (le modem qui a déclenché l'alerte), **{IP}** (l'adresse IP de l'appareil), **{HOST}** (son nom d'hôte) et **{TIMESTAMP}** (quand l'erreur a été détectée) sont remplacés par des valeurs réelles. Cliquez sur un espace réservé sous le champ de message pour l'insérer.

SMPP

Settings > Channels > SMPP (`/settings/smpp/`) active le serveur SMPP intégré de l'appareil. Une application externe agissant en tant que client SMPP peut ensuite soumettre des SMS via les modems de l'appareil et recevoir les SMS entrants et les accusés de réception sur la même connexion.



Paramètres SMPP, présentés ici sur un appareil à deux modems. NXS-9700 en répertorie un

Détails de la connexion

Paramètre	Valeur
Protocole	SMPP 3.4
Port	TCP 2770
Client vers SMSEagle	SMS à envoyer via les modems de l'appareil
SMSEagle vers client	SMS entrants et accusés de réception

Le client SMPP se lie avec l'"**User** et le **Password** définis sur cette page, en tant que `system_id` et `password`.

Les SMS entrants et les accusés de réception sont mis en file d'attente sur l'appareil tant qu'aucun client SMPP n'est connecté. Dès qu'un client se lie, SMSEagle remet tout ce qui se trouve dans cette file d'attente, le client doit donc être prêt à recevoir et à accuser réception des messages `deliver_sm` dès qu'il se lie.

Activation de SMPP

1. Activez **Enable SMPP**. Les cartes d'état du service, **Credentials** et **Modem access** apparaissent.

2. Sous **Credentials**, configurez l"**User** et le **Password** avec lesquels le client SMPP se liera. Le mot de passe ne peut contenir que des lettres et des chiffres, jusqu'à 8 caractères. Si un mot de passe est déjà stocké, laissez le champ tel quel pour le conserver.
3. Laissez **Limit modems** sous **Modem access** désactivé. NXS-9700 disposant d'un modem intégré unique, tout le trafic SMPP l'utilise de toute façon.
4. Cliquez sur **Enregistrer les modifications**.

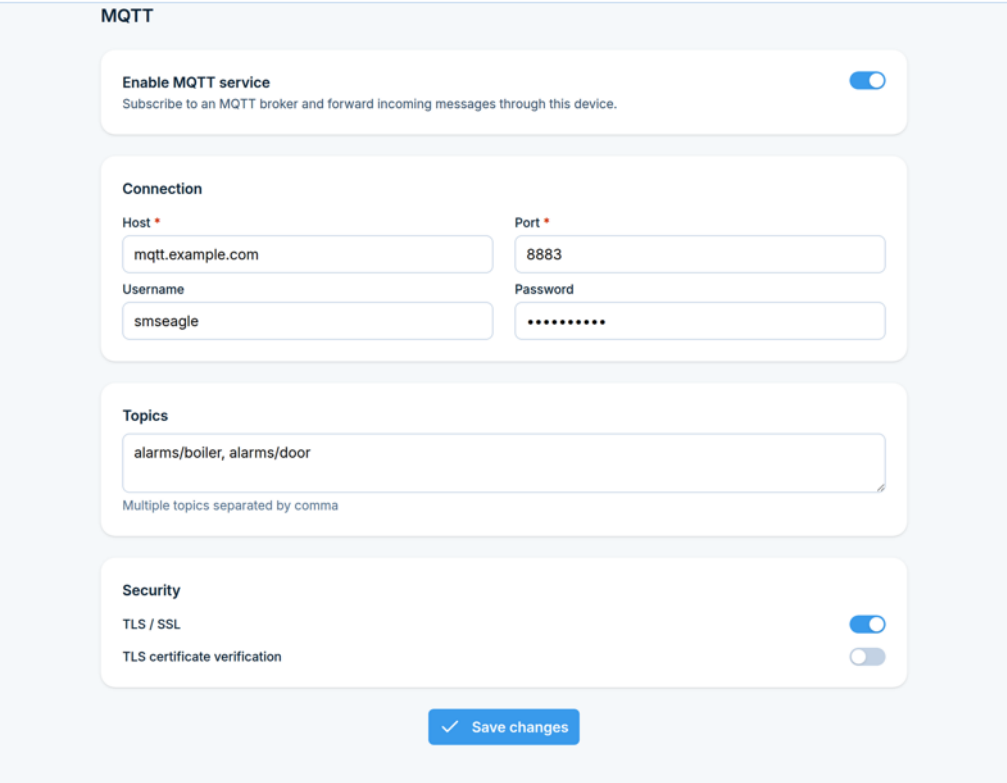
   Un redémarrage est nécessaire. Après l'enregistrement, SMSEagle vous demande de redémarrer l'appareil pour que les modifications SMPP prennent effet. Jusqu'à ce que vous le fassiez, les nouveaux paramètres sont stockés mais pas encore en usage. Utilisez **System > Restart** quand vous êtes prêt.

Après le redémarrage, les quatre cartes d'état (**Core service**, **SMPP connection**, **SMS service**, **SQL service**) indiquent si chaque partie du serveur SMPP fonctionne. Les quatre doivent afficher **Active** pour que les clients SMPP puissent se connecter et échanger des messages.

La première fois que vous activez SMPP, SMSEagle crée également un utilisateur interne pour le trafic SMPP, avec sa propre clé API répertoriée sous **Settings > API v2 keys**, et les règles internes qui transmettent les SMS entrants et les accusés de réception au client SMPP. Ne les révoquez ou ne les modifiez pas. La désactivation de SMPP supprime à nouveau l'utilisateur et les règles.

MQTT

Settings > Channels > MQTT (`/settings/mqtt/`) connecte l'appareil au courtier MQTT qu'il écoute. Les règles Subscribe sous MQTT dans Automation, qui transforment les messages MQTT en SMS, utilisent cette connexion. Les règles Publish ne le font pas : chacune d'elles désigne son propre courtier.



Paramètres de connexion au courtier MQTT

Activez **Enable MQTT service**, puis configurez :

- **Host** et **Port** du courtier (tous deux obligatoires).
- **Username** et **Password**, si le courtier les exige.
- **Topics** - les sujets auxquels l'appareil s'abonne, séparés par des virgules.
- **TLS / SSL** - chiffre la connexion au courtier. La **TLS certificate verification** vérifie également le certificat du courtier, laissez-la désactivée uniquement pour un courtier avec un certificat auto-signé.

Cliquez sur **Enregistrer les modifications**.

> **Un redémarrage est nécessaire.** Après l'enregistrement, SMSEagle vous demande de redémarrer l'appareil pour que les modifications MQTT prennent effet. Jusqu'à ce que vous le fassiez, les nouveaux paramètres sont stockés mais pas encore en usage. Utilisez **System > Restart** quand vous êtes prêt.

Réseau

Paramètres IP

Paramètres > Paramètres globaux > Réseau > Paramètres IP (`/settings/network/ip`) affiche l'"**adresse MAC** de l'appareil (lecture seule) et vous permet de configurer :

- **Get IP address from DHCP** - activez DHCP ou désactivez-le pour définir une adresse IP statique.

- **Hostname**
- **Use proxy** - acheminez les connexions sortantes de l'appareil via un proxy HTTP.
- **IP address restriction** - **Allow**, **Deny**, ou **Disabled**, avec une liste d'adresses IP à laquelle la règle s'applique. Lorsque la restriction est active, tous les ports sauf le 22 (SSH) sont bloqués pour tous les accès ne figurant pas sur la liste.

  Soyez prudent avec la restriction d'adresse IP. Une liste d'autorisation mal configurée peut vous verrouiller hors de l'interface web depuis votre propre machine. Ajoutez d'abord votre adresse IP actuelle (la page propose un raccourci **Add your IP address**) avant d'enregistrer.

SSL

Paramètres > Paramètres globaux > Réseau > SSL (`/settings/network/ssl`) vous permet de remplacer le certificat auto-signé par défaut de l'appareil par le vôtre : téléchargez un **Certificate**, sa **Private key**, et optionnellement un **Root CA certificate** et **Full chain**. Un interrupteur séparé, **Forward HTTP to HTTPS**, redirige les requêtes HTTP simples vers HTTPS.

Basculement

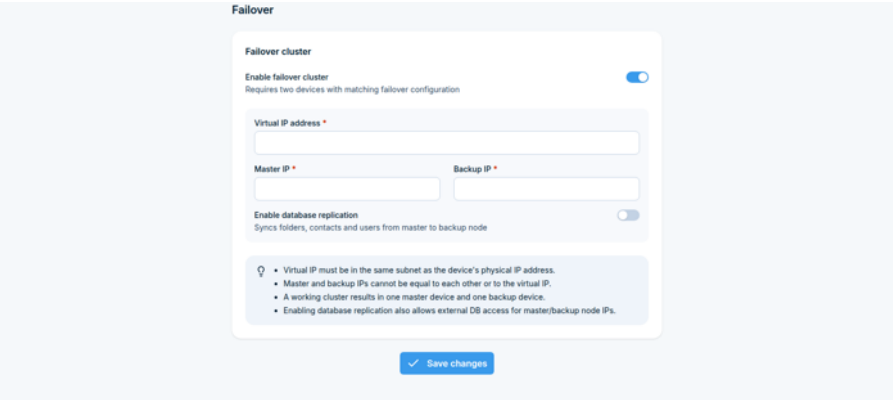
Le cluster de basculement fournit une haute disponibilité au niveau de l'appareil : un deuxième appareil SMSEagle se tient prêt en tant que sauvegarde, prêt à prendre le relais si l'appareil maître cesse de répondre.

Où le trouver

Paramètres > Paramètres globaux > Réseau > Failover (`/settings/network/failover`).

Activation du cluster de basculement

Activez **Enable failover cluster**. Cela nécessite deux appareils avec une configuration de basculement identique, l'un agissant comme maître et l'autre comme sauvegarde.



Paramètres du cluster de basculement

Définissez les mêmes valeurs sur les deux appareils :

- **Virtual IP address** - l'adresse à laquelle vos utilisateurs et intégrations se connectent.

- **Master IP** et **Backup IP** - les adresses IP physiques des deux appareils. Chaque appareil adopte son rôle en fonction de sa propre adresse : celui dont l'IP correspond à **Master IP** devient le maître, celui qui correspond à **Backup IP** devient la sauvegarde. L'un des deux doit donc être l'adresse de l'appareil que vous configurez.
- **Enable database replication** - copie les dossiers, les contacts et les utilisateurs du nœud maître vers le nœud de sauvegarde (voir ci-dessous).

Cliquez sur **Enregistrer les modifications**.

> **Un redémarrage est nécessaire.** Après l'enregistrement, SMSEagle vous demande de redémarrer l'appareil pour que les modifications de basculement prennent effet. Jusqu'à ce que vous le fassiez, les nouveaux paramètres sont stockés mais pas encore en usage. Utilisez **System > Restart** quand vous êtes prêt.

Rôles maître/sauvegarde et adresse IP virtuelle

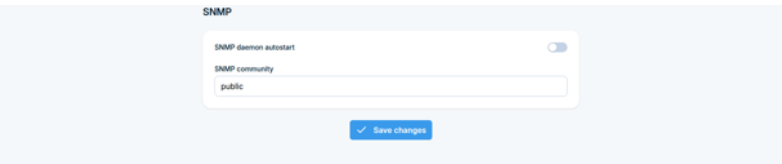
Le cluster est accessible via une seule **adresse IP virtuelle**, qui pointe toujours vers l'appareil actuellement actif :

- L'adresse IP virtuelle doit être sur le même sous-réseau que l'adresse IP physique propre de chaque appareil.
- L'adresse IP maître, l'adresse IP de sauvegarde et l'adresse IP virtuelle doivent toutes être différentes les unes des autres.
- Un cluster fonctionnant a toujours exactement un appareil maître et un appareil de sauvegarde à un moment donné ; si le maître cesse de répondre, la sauvegarde reprend l'adresse IP virtuelle.

Réplication de base de données et accès externe

L'activation du cluster de basculement active également la réplication de base de données entre le maître et la sauvegarde, de sorte que l'appareil de sauvegarde dispose d'une copie à jour des messages, des contacts et des paramètres s'il doit prendre le relais. Ce même paramètre permet également l'accès externe à la base de données pour les adresses IP du nœud maître et de sauvegarde spécifiquement, ce qui est nécessaire pour que la réplication fonctionne.

SNMP



Paramètres de l'agent SNMP

L'agent SNMP permet aux outils externes (un NMS, un navigateur MIB ou un simple appel `snmpget`/`snmpwalk`) d'interroger SMSEagle pour ses propres métriques - force du signal, nom du réseau, nombre de messages dans les dossiers, uptime du système, et bien d'autres. C'est la direction opposée aux traps SNMP : l'agent est interrogé par un outil externe, plutôt que SMSEagle poussant une alerte vers un.

Où le trouver

Paramètres > Paramètres globaux > Réseau > SNMP (`/settings/network/snmp`).

Configuration de l'agent SNMP

Activez **SNMP daemon autostart** pour que l'agent démarre automatiquement avec le périphérique, et définissez la chaîne **SNMP community** utilisée pour authentifier les demandes de lecture.

Une fois activé, les paramètres d'extension de SMSEagle (force du signal, nom du réseau, compteurs de dossiers, uptime, et autres) peuvent être lus à partir de l'arborescence MIB du périphérique en utilisant tout outil SNMP standard, par exemple `snmpget`/`snmpwalk` de NET-SNMP ou un navigateur MIB graphique.

Métriques disponibles

En plus des métriques standard de l'hôte Linux, SMSEagle publie ses propres métriques via NET-SNMP-EXTEND-MIB. Chacune peut être lue par son OID, ou par nom comme `NET-SNMP-EXTEND-MIB::nsExtendOutputFull."<metric name>"`.

Les métriques qui décrivent un modem se terminent par le numéro du modem. Le NXS-9700 dispose d'un modem, donc ces métriques se terminent par `1`. Une métrique retourne `-1` quand sa valeur ne peut pas être lue, par exemple quand le modem est éteint ou que le capteur de température n'est pas activé.

Métrique	Retourne
`GSM_Signal1`	Force du signal du modem, en pourcentage (0-100).
`GSM_NetName1`	Nom du réseau mobile auquel le modem est enregistré.
`GSM_ModemState1`	`on` ou `off` : indique si le modem est activé sous Modems.
`SIM_State1`	État de la carte SIM tel que signalé par le modem : `READY` quand la SIM est prête, sinon l'état propre du modem comme `SIM PIN` ou `SIM PUK`, ou une erreur comme `NOSIM`.
`SIM_RegState1`	Enregistrement réseau : `Registered Home`, `Registered Roaming`, `Searching`, `Not Registered`, `Denied`, `Registered Emergency`, `Unknown` ou `Unset`.
`SMSCountIn1`	SMS reçus par le modem aujourd'hui, depuis minuit.
`SMSCountOut1`	SMS envoyés par le modem aujourd'hui, depuis minuit.
`FolderInbox_Total`	Messages **non lus** dans la Inbox. Un message multi-parties compte une seule fois.
`FolderOutbox_Total`	Messages en attente dans la Outbox, la file d'envoi.
`FolderSent_Last24H`	Messages envoyés au cours des 24 dernières heures. Chaque partie d'un message multi-parties est comptée séparément.
`FolderSent_Last1M`	Messages envoyés au cours du dernier mois, comptés de la même façon.
`FolderSent_Last24HSendErr`	Messages dont l'envoi a échoué au cours des 24 dernières heures, parce que le modem n'a pas pu les envoyer ou que le réseau les a rejetés.
`Temp`	Température du capteur 1, en °C. Même valeur que `Temp1`.
`Temp1`	Température des capteurs 1 à 4 (`Temp1` à `Temp4`), en °C, dans la numérotation des capteurs de température et d'humidité. L'OID ci-dessous est pour `Temp1`.
`Humidity`	Humidité du capteur 1, en %.

Métrique	OID
GSM_Signal1	.1.3.6.1.4.1.8072.1.3.2.3.1.2.11.71.83.77.95.83.105.103.110.97.108.49
GSM_NetName1	.1.3.6.1.4.1.8072.1.3.2.3.1.2.12.71.83.77.95.78.101.116.78.97.109.101.49
GSM_ModemState1	.1.3.6.1.4.1.8072.1.3.2.3.1.2.15.71.83.77.95.77.111.100.101.109.83.116.9
SIM_State1	.1.3.6.1.4.1.8072.1.3.2.3.1.2.10.83.73.77.95.83.116.97.116.101.49
SIM_RegState1	.1.3.6.1.4.1.8072.1.3.2.3.1.2.13.83.73.77.95.82.101.103.83.116.97.116.10
SMSCountIn1	.1.3.6.1.4.1.8072.1.3.2.3.1.2.11.83.77.83.67.111.117.110.116.73.110.49
SMSCountOut1	.1.3.6.1.4.1.8072.1.3.2.3.1.2.12.83.77.83.67.111.117.110.116.79.117.116.
FolderInbox_Total	.1.3.6.1.4.1.8072.1.3.2.3.1.2.17.70.111.108.100.101.114.73.110.98.111.12
FolderOutbox_Total	.1.3.6.1.4.1.8072.1.3.2.3.1.2.18.70.111.108.100.101.114.79.117.116.98.11
FolderSent_Last24H	.1.3.6.1.4.1.8072.1.3.2.3.1.2.18.70.111.108.100.101.114.83.101.110.116.9
FolderSent_Last1M	.1.3.6.1.4.1.8072.1.3.2.3.1.2.17.70.111.108.100.101.114.83.101.110.116.9
FolderSent_Last24HSendErr	.1.3.6.1.4.1.8072.1.3.2.3.1.2.25.70.111.108.100.101.114.83.101.110.116.95
Temp	.1.3.6.1.4.1.8072.1.3.2.3.1.2.4.84.101.109.112
Temp1	.1.3.6.1.4.1.8072.1.3.2.3.1.2.5.84.101.109.112.49
Humidity	.1.3.6.1.4.1.8072.1.3.2.3.1.2.8.72.117.109.105.100.105.116.121

L'OID de toute métrique est `.1.3.6.1.4.1.8072.1.3.2.3.1.2`, suivi du nombre de caractères du nom de la métrique et du code ASCII de chaque caractère. Le dernier numéro de l'OID d'une métrique de modem est 48 plus le numéro du modem, ce qui est pourquoi les métriques du modem ci-dessus se terminent par `.49`.

Si votre outil SNMP ne connaît pas les noms NET-SNMP-EXTEND-MIB, chargez le fichier de définition MIB.

Lecture des métriques

Remplacez `public` par votre **communauté SNMP** et `192.0.2.10` par l'adresse IP de l'appareil.

Lire une métrique par OID :

```
snmpget -v 2c -c public 192.0.2.10 .
1.3.6.1.4.1.8072.1.3.2.3.1.2.11.71.83.77.95.83.105.103.110.97.108.49
```

```
NET-SNMP-EXTEND-MIB::nsExtendOutputFull."GSM_Signal1" = STRING: 77
```

Lire une métrique par nom :

```
snmpget -v 2c -c public 192.0.2.10 'NET-SNMP-EXTEND-
MIB::nsExtendOutputFull."FolderOutbox_Total"'
```

```
NET-SNMP-EXTEND-MIB::nsExtendOutputFull."FolderOutbox_Total" = STRING: 0
```

Lister toutes les métriques SMSEagle à la fois :

```
snmpwalk -v 2c -c public 192.0.2.10 .1.3.6.1.4.1.8072.1.3.2.3.1.2
```

Ce qui peut être lu depuis le réseau

Les requêtes en provenance de l'appareil lui-même (`localhost`) voient l'ensemble de l'arborescence MIB. Les requêtes en provenance d'autres hôtes voient une partie restreinte : les métriques SMSEagle ci-dessus, et dans les MIB standards le groupe système (y compris le temps de disponibilité), les interfaces réseau, le stockage, les processeurs, la mémoire, la charge et l'utilisation du processeur. La liste des processus et autres détails ne sont pas exposés au réseau.

La même **communauté SNMP** s'applique à la fois. Après l'avoir modifiée, redémarrez l'appareil pour que la nouvelle valeur prenne effet.

Utilisation de SNMP v3

La page configure SNMP v1/v2c. Pour SNMP v3 avec authentification et chiffrement, utilisez le script `snmpv3` via SSH :

1. Connectez-vous à l'appareil via SSH en tant que `root`.
2. Accédez au répertoire SMSEagle :

```
cd /mnt/nand-user/smseagle/
```

3. Ajoutez un utilisateur SNMP v3 en lecture seule. Il utilise SHA pour l'authentification et AES pour le chiffrement. Les deux mots de passe doivent comporter au moins 8 caractères.

   ```
   ./snmpv3 add USERNAME AUTH_PASSWORD ENCRYPTION_PASSWORD
   ```

4. Optionnellement, désactivez l'accès SNMP v1/v2c afin que seuls les utilisateurs SNMP v3 puissent lire l'agent :

   ```
   ./snmpv3 disablev2
   ```

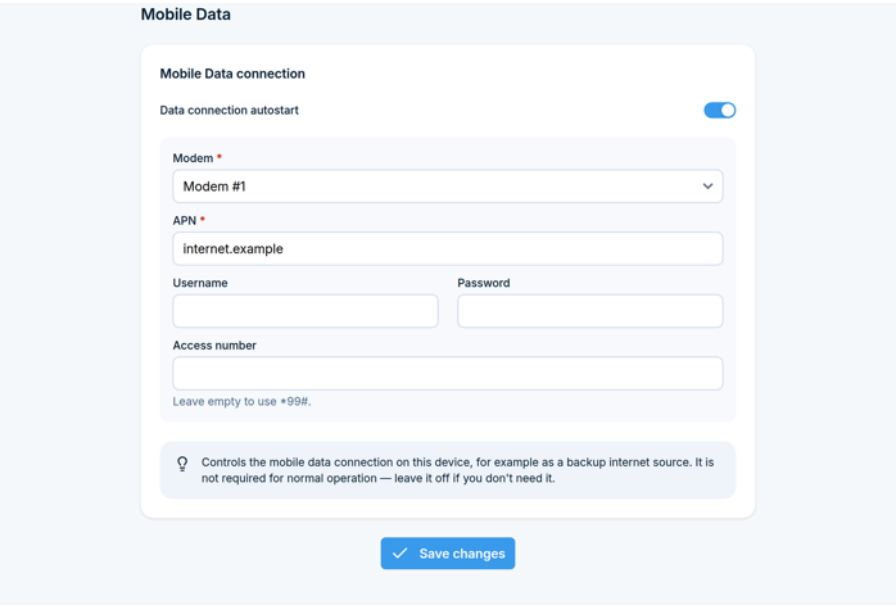
   `./snmpv3 enablev2` le réactive, et `./snmpv3 del USERNAME` supprime l'utilisateur.

Le script redémarre l'agent SNMP lui-même. Une requête v3 ressemble alors à ceci :

```
snmpget -v 3 -l authPriv -u USERNAME -a SHA -A AUTH_PASSWORD -x AES -X
ENCRYPTION_PASSWORD 192.0.2.10 .
1.3.6.1.4.1.8072.1.3.2.3.1.2.11.71.83.77.95.83.105.103.110.97.108.49
```

Données mobiles

Settings > Global settings > Network > Mobile Data (`/settings/network/mobile-data`) contrôle une connexion de données mobiles via l'un des modems de l'appareil, par exemple comme source Internet de secours. Elle n'est pas requise pour envoyer ou recevoir des SMS. Laissez-la désactivée si vous n'en avez pas besoin.



Paramètres Mobile Data, affichés ici sur un appareil à deux modems. NXS-9700 n'a pas de champ **Modem**

Activez **Data connection autostart**, puis définissez :

- **APN** de l'opérateur de la SIM (obligatoire), et **Username** et **Password** si l'opérateur les exige.
- **Access number** - laissez-le vide pour utiliser `*99#`.

Cliquez sur **Enregistrer les modifications**.

> **Un redémarrage est nécessaire.** Après l'enregistrement, SMSEagle vous demande de redémarrer l'appareil pour que les modifications des données mobiles prennent effet. Jusqu'à ce que vous le fassiez, les nouveaux paramètres sont stockés mais pas encore utilisés. Utilisez **System > Restart** lorsque vous êtes prêt.

Application

Paramètres > Paramètres globaux > Application (`/settings/application/`) contient un comportement à l'échelle du périphérique qui ne s'inscrit pas dans un seul canal ou fonctionnalité, regroupé en quatre sections :

Régional

Langue (par défaut sur l'appareil) et **Indicatif téléphonique du pays** (utilisé lorsqu'un numéro de téléphone est entré sans lui).

Sécurité

- **Forcer l'authentification multifacteur** - Pour tous les utilisateurs, Pour les nouveaux utilisateurs, ou Ne pas forcer (même effet que le paramètre d'authentification multifacteur à l'échelle du périphérique de l'assistant, voir MFA).
- **Vérification de la complexité du mot de passe** - exiger les règles de mot de passe (longueur, casse mixte, chiffre, caractère spécial) pour chaque utilisateur.
- **Accès à la base de données pour les applications externes** - active l'accès PostgreSQL direct pour les applications externes, désactivé par défaut. Les détails complets de la connexion et les exemples SQL sont traités séparément dans Avancé, car c'est un sujet de power-user en soi.

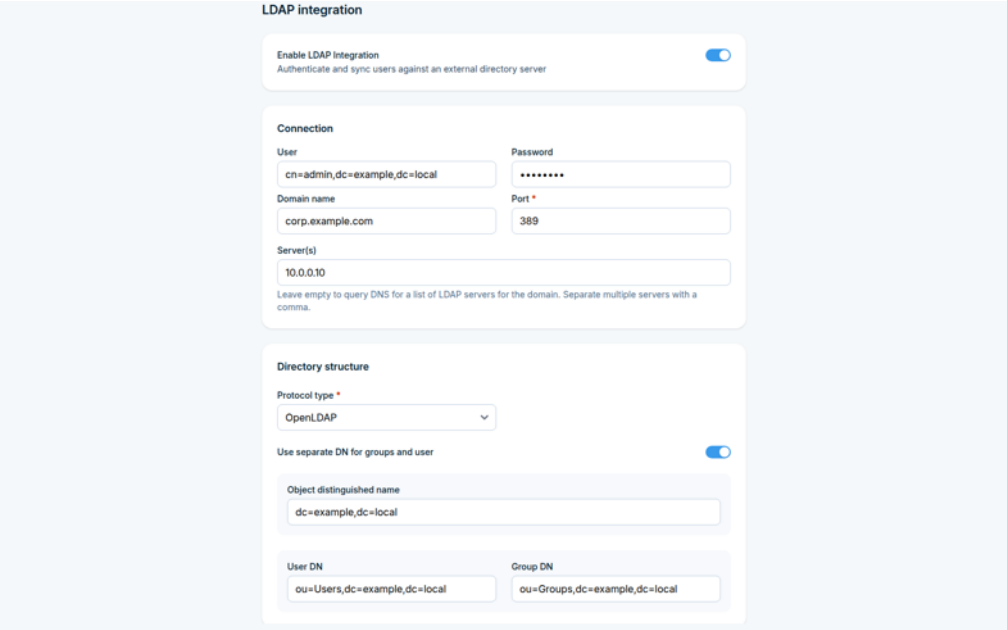
Accès et visibilité

- **Visibilité du contenu de la boîte de réception** - Pour tous les utilisateurs, Uniquement pour les administrateurs, ou Uniquement les messages des modems assignés à l'utilisateur (les modems sont assignés par utilisateur dans **Système > Utilisateurs**).
- **Visibilité du contenu de la boîte de réception e-mail** - Pour tous les utilisateurs ou Uniquement pour les administrateurs.
- **Module de rapports accessible pour** - Tous les utilisateurs ou Uniquement les administrateurs.

API et intégrations

- **Enregistrer les journaux API** - enregistre chaque appel API v1 et v2 (méthode, chemin et paramètres) dans `/var/log/smseagle/api.log`. Les jetons d'accès sont masqués et le texte des messages est omis. Le fichier n'est pas affiché dans le navigateur de journaux sous **System > Logs**, mais **Download logs** sur cette page l'inclut. Activez-le lors de la configuration ou du débogage d'une intégration.
- **Transférer les messages 3CX en Unicode** - les messages que 3CX envoie à SMSEagle via le point de terminaison 3CX de l'API v2 sont envoyés en tant que SMS Unicode au lieu de l'alphabet SMS standard. Activez cette option lorsque les utilisateurs de 3CX envoient des caractères nationaux.

LDAP



Paramètres d'intégration LDAP

Ce que cette fonction fait

L'intégration LDAP connecte SMSEagle à l'annuaire de votre entreprise, tel qu'Active Directory ou OpenLDAP. Elle effectue deux tâches distinctes, et vous pouvez utiliser l'une ou l'autre ou les deux :

Tâche	Ce qu'il vous donne
Contacts	Le Carnet d'adresses est alimenté à partir du répertoire, vous pouvez donc envoyer des messages aux mêmes personnes et groupes que votre entreprise gère déjà, sans taper les numéros deux fois.
Authentification	Les utilisateurs se connectent à SMSEagle avec leur compte de répertoire, et leur niveau de permission est déterminé par l'appartenance à leur groupe de répertoire.

Utilisations typiques : maintenir le Carnet d'adresses en sync avec les changements de personnel automatiquement, et permettre aux utilisateurs d'utiliser leur mot de passe d'entreprise existant au lieu d'un mot de passe SMSEagle séparé.

Avant de commencer

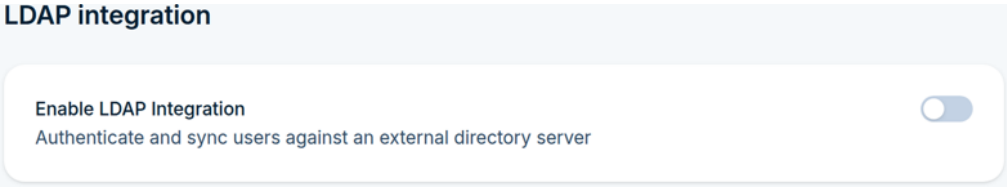
Collectez ces informations auprès de celui qui administre le répertoire :

- Le **nom de domaine** et le **port** (389 pour LDAP simple, généralement 636 avec SSL).
- Un **compte de service** (utilisateur et mot de passe) autorisé à lire le répertoire.
- Le **nom unique** de la branche contenant vos utilisateurs, par exemple `ou=Users,dc=company,dc=local`, et la branche contenant les groupes si elle est différente.
- Quel **attribut** contient le numéro de téléphone auquel vous voulez envoyer des messages.
- Si vous voulez l'authentification par répertoire : les noms des groupes dont les membres doivent devenir administrateurs SMSEagle et utilisateurs réguliers.

Étape 1 : Ouvrir la page LDAP

Dans la barre latérale, allez à **Settings > Global settings > LDAP**.

La page commence par un seul bouton, **Enable LDAP Integration**. Tant que vous ne l'activez pas, rien d'autre n'est affiché.



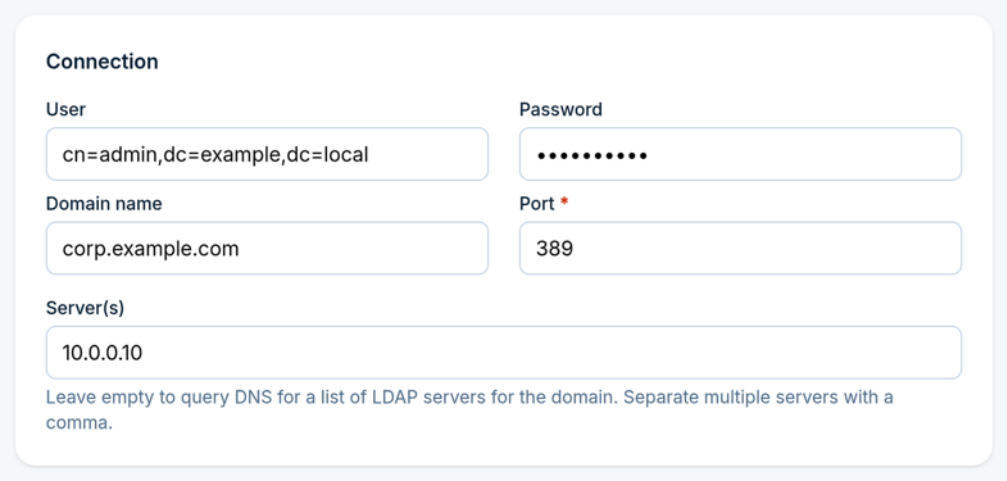
Avec l'intégration désactivée, la page ne montre que le bouton

Étape 2 : Activer l'intégration

Activez **Enable LDAP Integration**. Quatre sections apparaissent : **Connection**, **Directory structure**, **Attributes and security** et **Sync and access**.

Étape 3 : Connexion

Champ	Quoi entrer
User	Le compte de service utilisé pour lire le répertoire.
Mot de passe	Son mot de passe. Le champ s'affiche vide quand vous revenez à la page ; laissez-le vide pour conserver le mot de passe stocké.
Domain name	Le domaine du répertoire, par exemple `company.local`.
Port	389 pour LDAP simple, 636 pour LDAP sur SSL. Obligatoire.
Server(s)	Serveurs spécifiques, séparés par des virgules, par exemple `ldap1.company.local, ldap2.company.local`. Laissez vide pour laisser l'appareil chercher les serveurs dans le DNS pour le domaine.



Section Connection, remplie avec des valeurs d'exemple

Étape 4 : Structure du répertoire

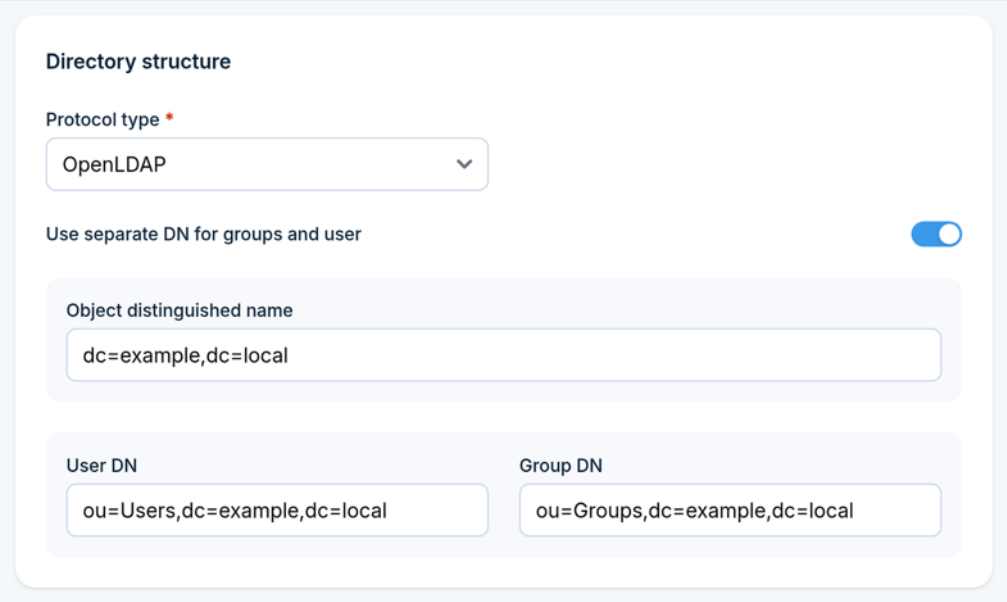
Type de protocole Choisissez **Active Directory** ou **OpenLDAP**, en correspondance avec votre serveur.

Utiliser un DN séparé pour les groupes et les utilisateurs Laissez-le désactivé si les utilisateurs et les groupes se trouvent sous la même branche. Un seul champ est alors affiché :

- **Object distinguished name**, par exemple `ou=Users,dc=smseagle,dc=local`.

Activez-le s'ils se trouvent dans des branches différentes. **Object distinguished name** reste, et deux autres champs apparaissent ci-dessous :

- **User DN**, par exemple `ou=Users,dc=smseagle,dc=local`
- **Group DN**, par exemple `ou=Groups,dc=smseagle,dc=local`



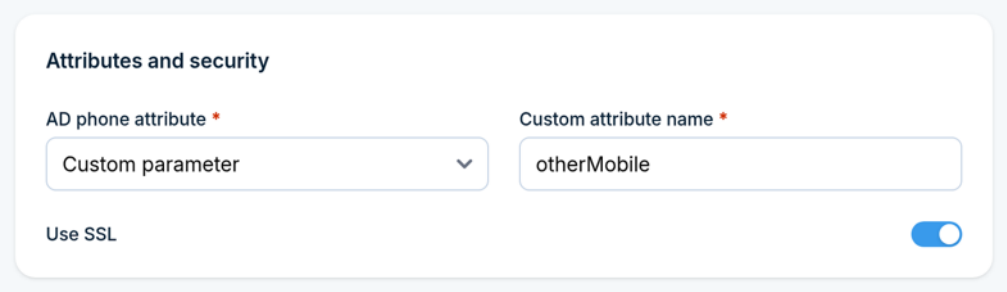
Structure de répertoire avec DNs séparés activés

Étape 5 : Attributs et sécurité

Attribut téléphone AD Quel attribut de répertoire contient le numéro que SMSEagle doit utiliser : **Telephone number**, **Mobile number**, **Home number**, **Pager number**, **Fax number**, **IP phone number**, ou **Custom parameter**.

Choisir **Custom parameter** révèle **Custom attribute name**, où vous tapez l'attribut vous-même, par exemple `otherMobile`. Seuls les noms d'attribut simples sont acceptés ; la ponctuation telle que `< > / \ : ; , . + ' " & =` est rejetée.

Use SSL Activez-le pour chiffrer la connexion au répertoire. N'oubliez pas de définir le **Port** correspondant dans la section Connection.



Attributs et sécurité, avec **Custom parameter** sélectionné et SSL activé

Étape 6 : Synchronisation et accès

Contacts and group fetch method

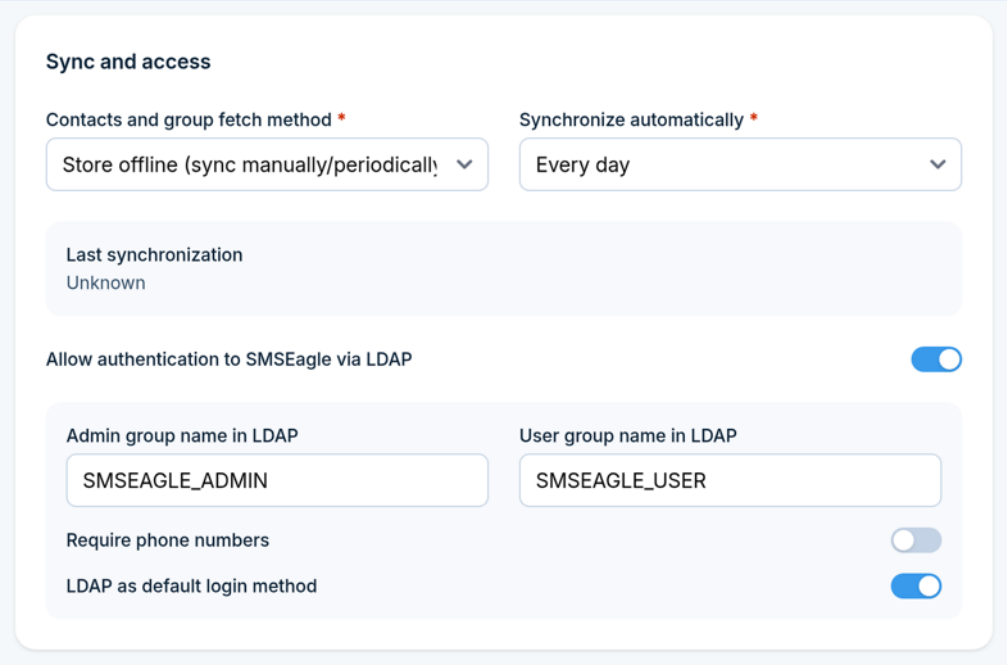
Option	Ce qui se passe
Fetch from LDAP server	Les contacts et les groupes sont lus dans le répertoire chaque fois qu'ils sont nécessaires. Toujours à jour, mais chaque recherche dépend de la disponibilité du répertoire.
Store offline (sync manually/periodically)	Une copie est conservée sur l'appareil. La messagerie continue de fonctionner quand le répertoire est inaccessible, au prix d'une légère obsolescence de la copie.

Si vous avez choisi **Store offline**, **Synchronize automatically** apparaît : **Never**, **Every hour**, **Every day**, **Every week** ou **Every month**. **Never** signifie que la copie n'est actualisée que lorsque vous déclenchez vous-même une synchronisation.

Last synchronization sous la méthode de récupération est en lecture seule et indique quand la copie hors ligne a été actualisée pour la dernière fois. Il affiche Unknown jusqu'à ce que la première synchronisation s'exécute.

Allow authentication to SMSEagle via LDAP Activez-le pour permettre aux utilisateurs de se connecter avec leur compte de répertoire. Quatre champs supplémentaires apparaissent :

- **Admin group name in LDAP** - les membres de ce groupe se connectent en tant qu'administrateurs.
- **User group name in LDAP** - les membres de ce groupe se connectent en tant qu'utilisateurs réguliers.
- **Require phone numbers** - seuls les comptes de répertoire qui ont un numéro dans l'attribut téléphone choisi peuvent se connecter. Désactivé par défaut.
- **LDAP as default login method** - présélectionne LDAP au lieu de Local dans le type d'authentification du formulaire de connexion, de sorte que les utilisateurs du répertoire n'ont pas à le modifier à chaque fois.



Synchronisation et accès, avec stockage hors ligne et connexion à l'annuaire activée

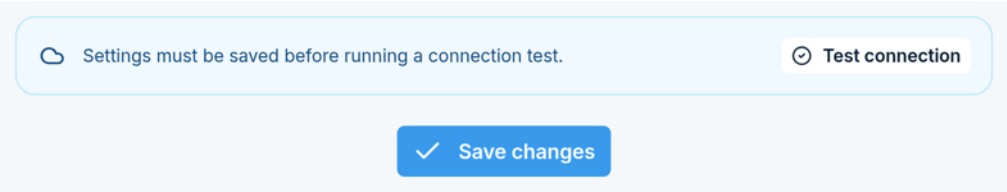
Vérifiez les noms de groupe avant de les utiliser. Un membre d'aucun groupe ne peut pas se connecter, et une faute de frappe dans le nom du groupe administrateur n'est remarquée que lorsque personne ne peut administrer l'appareil. Maintenez au moins un compte administrateur SMSEagle local actif jusqu'à ce que vous ayez vérifié la connexion à l'annuaire.

Étape 7 : Enregistrer et tester

Cliquez sur **Save changes** au bas de la page.

Cliquez ensuite sur **Test connection**. L'appareil se connecte à l'annuaire avec les paramètres que vous venez d'enregistrer et signale soit que la connexion a été établie, soit ce qui s'est mal passé.

Enregistrez d'abord, puis testez. Le test utilise les paramètres stockés, et non ce qui est actuellement affiché à l'écran, donc tester avant d'enregistrer vérifie la configuration précédente. La note à côté du bouton le dit également.



Le panneau de test répète la règle : enregistrez d'abord, puis testez

Date / Heure

Settings > Global settings > Date / Time (`/settings/datetime/`) affiche la date et l'heure système actuelles (lecture seule) et vous permet de définir :

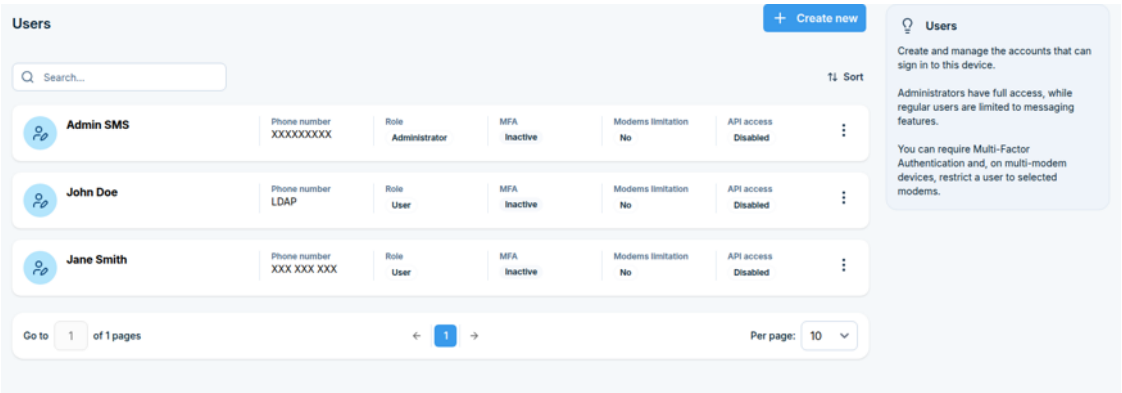
- **Time zone**
- **NTP time synchronization** - lorsqu'elle est activée, révèle **NTP server address**. Également proposée lors de l'"Assistant de configuration.

Système

Ce chapitre couvre la section **Système** de l'interface web : gestion des comptes utilisateur et de l'appareil lui-même.

Utilisateurs

Système > Utilisateurs (`/system/users/`) est l'endroit où vous créez et gérez les comptes qui peuvent se connecter à l'appareil. Les administrateurs ont un accès complet, tandis que les utilisateurs réguliers sont limités aux fonctionnalités de messagerie.



Utilisateurs, dans la section Système du menu

Pour chaque utilisateur, vous pouvez définir son **Niveau d'accès** (Administrateur ou Utilisateur) et exiger l'"Authentification Multi-Facteurs. L'accès API (voir Intégration API et Développeur) est également accordé par utilisateur à partir d'ici.

Informations système

Système > Informations système (`/system/info/`) affiche des informations en lecture seule sur l'appareil et ses modems :

- Type d'appareil, version du logiciel SMSEagle, numéro de série (adresse MAC), version du logiciel modem et version du schéma de base de données
- Utilisation de l'"**espace disque**, avec une notification SMS facultative à l'administrateur principal lorsque l'utilisation dépasse un seuil que vous définissez
- Détails par modem : force du signal, nom du réseau, statut de la carte SIM et statut d'enregistrement, IMEI et IMSI de la carte SIM

Journaux

System > Logs (`/system/logs/`) vous permet de parcourir et de rechercher les journaux du dispositif, regroupés en journaux par modem et journaux système (Base de données, Système, Application, Message). Utilisez **Search by phrase** pour filtrer, ou **Download logs** pour les enregistrer pour le support. Les journaux peuvent également être transférés vers un serveur syslog externe pour une collecte centralisée, voir Forwarding logs to an external server.

Mises à jour

Système > Mises à jour (`/system/updates/`) affiche la version du logiciel installée et vous permet de vérifier les mises à jour manuellement ou automatiquement ; vous pouvez également demander à l'appareil de notifier l'administrateur par SMS lorsqu'une nouvelle version est disponible. La même page affiche la validité de votre support technique et vous permet de vérifier cela aussi automatiquement.

Correctifs

Système > Correctifs (`/system/patches/`) installe un correctif ciblé ou un composant supplémentaire fourni par le support SMSEagle : entrez un **code de correctif** pour le télécharger et l'installer directement, ou téléchargez un **fichier de correctif** (un fichier `.bin`, jusqu'à 100 Mo) fourni par le support.

Sauvegarde / Restauration

Système > Sauvegarde / Restauration (`/system/backup/`) couvre les deux directions :

- **Sauvegardes manuelles** - créez une sauvegarde de la base de données et des paramètres de l'appareil à la demande.
- **Sauvegardes automatiques** - activez les sauvegardes planifiées sur un serveur SFTP/FTP(S), avec nettoyage des anciennes versions de sauvegarde.
- **Restaurer les données** - restaurez la base de données à partir d'un fichier de sauvegarde.

Redémarrage

Système > Redémarrage (`/system/restart/`) redémarre l'appareil à la demande - l'envoi et la réception sont indisponibles jusqu'à son retour en ligne - ou vous permet d'activer un redémarrage planifié sur une base récurrente.

Avancé

L’accès direct à la base de données et d’autres sujets pour utilisateurs avancés, hors des sentiers battus, ont leur propre chapitre : voir Avancé.

Intégration API et développeur

SMSEagle offre une puissante API REST intégrée. L'API est dédiée à l'intégration de SMSEagle avec tout système externe ou application.

Référence API

SMSEagle propose deux versions d'API :

- **API v2 - recommandée, utilisez-la pour chaque nouvelle intégration.** Une API RESTful moderne basée sur la spécification OpenAPI 3.0. Référence API v2
- **API v1 - l'API héritée, conservée uniquement pour la compatibilité descendante.** Une simple API HTTP et JSON-RPC. Elle fonctionne toujours et reste supportée, mais ne reçoit pas de nouvelles fonctionnalités - ne développez pas de nouvelles intégrations avec elle. Référence API v1

En raison de l'étendue du contenu de la documentation API, elle est maintenue comme un document séparé. Suivez les liens ci-dessus pour la spécification complète de chaque API.

Clés API

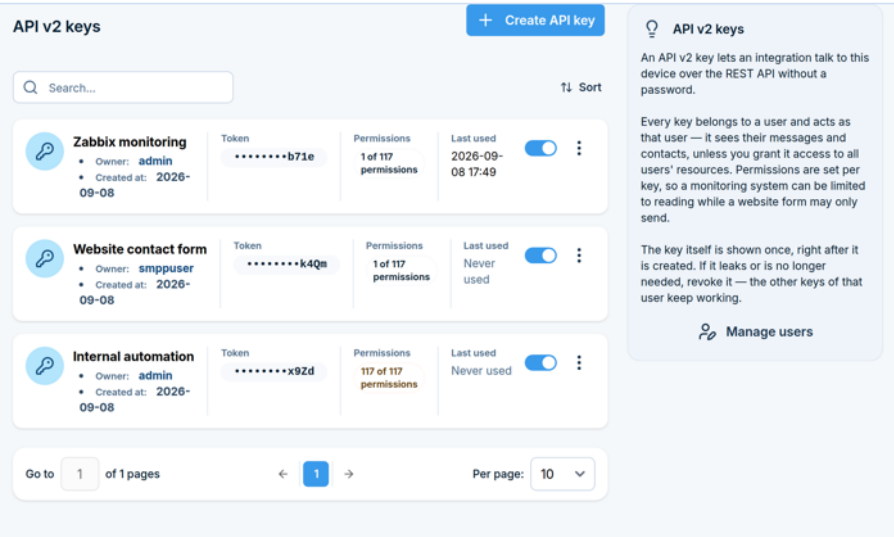
Une intégration s'authentifie avec une **clé API** au lieu d'un mot de passe utilisateur. Les clés sont conservées séparément pour chaque version d'API, sur deux pages :

- **Settings > API > API v2** (`/settings/api/v2`)
- **Settings > API > API v1** (`/settings/api/v1`)

Une clé appartient toujours à un utilisateur et agit comme cet utilisateur, elle voit donc les messages et les contacts de cet utilisateur. Les permissions sont accordées par clé, ce qui vous permet de limiter un système de surveillance à la lecture tandis qu'un formulaire web peut uniquement envoyer.

Clés API v2

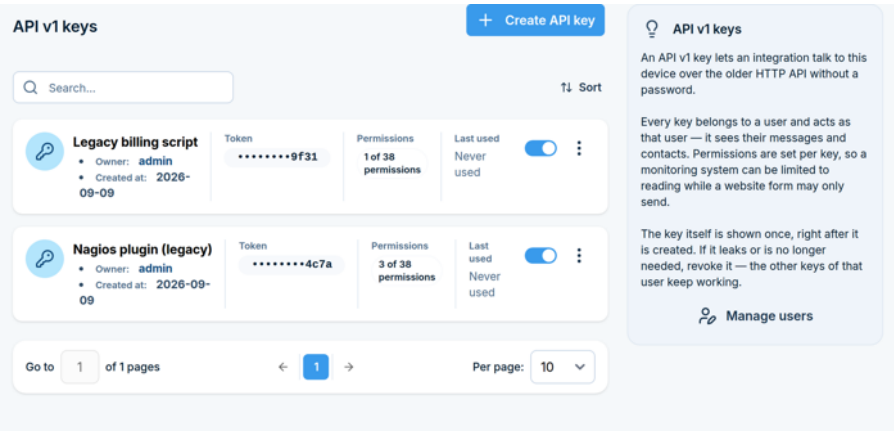
C'est la page à utiliser pour une nouvelle intégration.



Clés API v2

Clés API v1

API v1 est l'API héritée. Créez une clé v1 uniquement pour une intégration existante qui ne peut pas être migrée vers v2 - pour tout nouveau développement, créez plutôt une clé API v2.



Clés API v1

Créer une clé

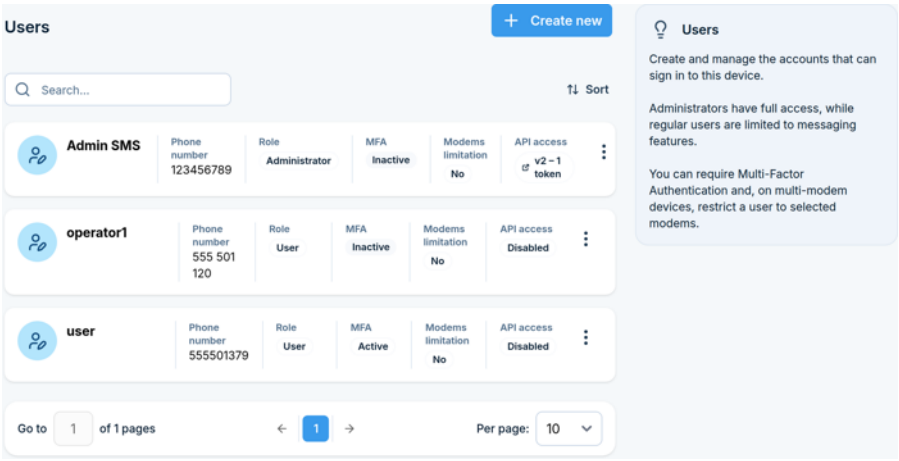
Create API key ouvre le formulaire de la version d'API de la page sur laquelle vous vous trouvez :

Champ	Ce qu'il fait
Key name	La façon dont vous reconnaîtrez cette intégration plus tard, par exemple Zabbix ou Website form.
Owner	L'utilisateur en tant que lequel la clé agit. La clé voit les messages et les contacts de cet utilisateur.
Key enabled	Une clé désactivée est refusée par l'API sans être supprimée, ce qui désactive une intégration sans perdre sa configuration.
Access to all users" resources	API v2 uniquement. Permet à la clé de lire et de modifier les ressources appartenant à d'autres utilisateurs (voir ci-dessous).
Autorisations	Seules les méthodes que vous activez peuvent être appelées avec cette clé.

La clé elle-même n'est affichée qu'une seule fois, immédiatement après sa création. Copiez-la et stockez-la en lieu sûr. Si vous la perdez, révoquez cette clé et créez-en une nouvelle - les autres clés du même utilisateur continueront de fonctionner.

Quels utilisateurs ont accès à l'API

System > Users affiche, par utilisateur, le nombre de clés API que l'utilisateur possède et pour quelle version d'API. Le badge renvoie directement à la page des clés correspondante.



Accès API, affiché par utilisateur dans la liste des utilisateurs

Accès aux ressources d’autres utilisateurs

Les deux versions d’API diffèrent dans la façon dont une clé API peut voir les données des autres utilisateurs :

- En **API v1**, une clé a accès par défaut aux ressources de tous les autres utilisateurs - contacts du carnet d’adresses, groupes, et ainsi de suite.
- En **API v2**, l’accès est plus granulaire : une clé n’a accès par défaut qu’aux ressources qu’elle a elle-même créées. Pour permettre l’accès aux ressources de tous les autres utilisateurs, activez **Access to all users” resources** sur la clé.

Plugins et intégrations

SMSEagle peut être intégré à des logiciels externes tels que les systèmes de surveillance réseau, les systèmes d'authentification et bien d'autres. La plupart des intégrations utilisent l'une des deux méthodes suivantes :

- **API** - le système externe envoie et reçoit des messages via l'API REST de SMSEagle. C'est la méthode la plus flexible et elle donne accès à toutes les fonctions de l'appareil. Voir API and Developer Integration.
- **Email to SMS** - le système externe envoie un email ordinaire et SMSEagle le convertit en SMS. Aucun codage n'est nécessaire, donc cela fonctionne avec n'importe quel logiciel capable d'envoyer des notifications par email. Voir Email to SMS.

Selon votre environnement, vous pouvez également utiliser MQTT ou SMPP.

Pour de nombreux systèmes populaires, vous n'avez pas besoin de construire vous-même l'intégration. SMSEagle fournit des plugins prêts à l'emploi et des manuels d'intégration étape par étape, et la liste s'agrandit constamment. Pour une liste complète et à jour, allez à : https://www.smseagle.eu/integration-plugins/

Avancé

Ce chapitre couvre des sujets avancés qui contournent l'interface web normale plutôt que de la traverser : accès direct à la base de données et SQL, et scripts de nettoyage de base de données en ligne de commande. La plupart des utilisateurs n'auront jamais besoin de ce chapitre.

Connexion directe à la base de données SMSEagle

La base de données de SMSEagle s'exécute sur PostgreSQL. Vous pouvez y accéder directement pour lire ou écrire des messages SMS via des requêtes SQL, au lieu de passer par l'interface web ou l'API.

L'accès à la base de données pour les applications externes est **désactivé par défaut**. Activez-le sous **Settings > Global settings > Application > Access to DB for external applications**.

Une fois activé, connectez-vous à la base de données depuis une application externe en utilisant :

- Host : l'adresse IP de l'appareil
- Database name: `smseagle`
- User: `smseagleuser`
- Password: `postgreeagle`

Injection d'un SMS court via SQL

Un message texte court (jusqu'à 160 caractères) :

```
INSERT INTO outbox (
    DestinationNumber,
    TextDecoded,
    CreatorID,
    Coding,
    Class,
    SenderID
) VALUES (
    '1234567',
    'This is a SQL test message',
    'Program',
    'Default_No_Compression',
    -1,
    'smseagle1'
);
INSERT INTO user_outbox (
    id_outbox,
    id_user
) SELECT CURRVAL(pg_get_serial_sequence('outbox','ID')), 1;
```

Le message ci-dessus appartient à l'utilisateur avec `id_user` 1 (l'utilisateur `admin` par défaut) - les valeurs `id_user` des autres utilisateurs se trouvent dans la table `public."user"`. Le champ `SenderID` identifie quel modem envoie le message : `smseagle1` pour le modem 1, `smseagle2` pour le modem 2.

Injection d'un SMS long via SQL

Les messages multipièces ont également besoin d'un en-tête UDH, stocké sous forme de chaîne hexadécimale dans le champ `UDH`. À moins d'avoir une raison spécifique de le faire manuellement, utilisez l'API à la place (voir API and Developer Integration).

Pour un message texte long, l'UDH commence par `050003`, suivi d'un octet utilisé comme référence de message (n'importe quelle valeur hexadécimale, mais différente pour chaque message - `D3` ci-dessous), un octet pour le nombre total de parties (`02` ci-dessous, unique par message envoyé au même numéro), et un octet pour le numéro de la partie actuelle (`01` pour la première partie, `02` pour la deuxième, et ainsi de suite).

Un message long en deux parties ressemble à ceci :

```
INSERT INTO outbox (
    "DestinationNumber",
    "CreatorID",
    "MultiPart",
    "UDH",
    "TextDecoded",
    "Coding",
    "Class",
    "SenderID"
) VALUES (
    '1234567',
    'Program',
    'true',
    '050003D30201',
    'Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor
incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, qui',
    'Default_No_Compression',
    -1,
    'smseagle1'
)
INSERT INTO outbox_multipart (
    "ID",
    "SequencePosition",
    "UDH",
    "TextDecoded",
    "Coding",
    "Class"
) SELECT
    CURRVAL(pg_get_serial_sequence('outbox','ID')),
    2,
    '050003D30202',
    's nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo
consequat.',
    'Default_No_Compression',
    -1;
INSERT INTO user_outbox (
    id_outbox,
    id_user
) SELECT
    CURRVAL(pg_get_serial_sequence('outbox','ID')),
    1;
```

L'ajout d'un UDH réduit l'espace disponible pour le texte - l'exemple ci-dessus permet seulement 153 caractères par partie de message.

Scripts de nettoyage de base de données

Quelques scripts sont disponibles pour supprimer des messages SMS de la base de données via la CLI Linux, situés à `/mnt/nand-user/scripts/` :

Script	Utilisation	Objectif
`db_delete`	`./db_delete YYYYMMDDhhmm`	Supprimer les SMS de la Inbox et des SentItems plus anciens que la date donnée
`db_delete_7days`	`./db_delete_7days`	Supprimer les SMS de la Inbox et des SentItems plus anciens que 7 jours
`db_delete_allfolders`	`./db_delete_allfolders`	Nettoie les dossiers Inbox, SentItems et Outbox - conçu pour s'exécuter périodiquement via cron
`db_delete_select`	`./db_delete_select {inbox|outbox|sentitems|trash}`	Supprime les SMS d'un dossier choisi

Ajouter un script à cron : créez un fichier sous `/etc/cron.d/` (par exemple `db_cleaner`) avec un contenu tel que :

```
0 0 1 * * root /mnt/nand-user/scripts/db_delete_allfolders
```

Cet exemple exécute le script de nettoyage le 1er de chaque mois.

Transfert des journaux vers un serveur externe

SMSEagle écrit ses journaux via rsyslog. Pour envoyer une copie vers un serveur syslog central, ajoutez une règle de transfert via SSH. Il n'y a pas de paramètre pour cela dans l'interface web.

1. Connectez-vous au dispositif via SSH en tant que `root`.
2. Créez le fichier `/etc/rsyslog.d/005-remote.conf` avec cette règle, en remplaçant l'adresse, le port et le protocole par ceux de votre serveur :

```
*.* action(type="omfwd" target="192.0.2.250" port="514" protocol="udp"
           action.resumeRetryCount="10"
           queue.type="linkedList" queue.size="10000")
```

   - `target` - Adresse IP ou nom d'hôte du serveur syslog.

- `port` - port sur lequel le serveur écoute, généralement `514`.
- `protocol` - `udp` ou `tcp`.
- Les paramètres de file d'attente conservent jusqu'à 10000 messages sur le dispositif lorsque le serveur est inaccessible, et les envoient une fois qu'il est de retour.

3. Vérifiez la configuration, puis redémarrez rsyslog :

```
rsyslogd -N1
systemctl restart rsyslog
```

Conservez le nom du fichier. Les propres journaux de SMSEagle (Application, API, Message, ainsi que les services de messagerie, appel, Signal et WhatsApp) sont écrits par des règles dans `/etc/rsyslog.d/010-*.conf` à `018-*.conf`, et chacune de ces règles arrête le traitement ultérieur de ses messages. Une règle de transfert placée après celles-ci, par exemple à la fin de `/etc/rsyslog.conf`, ne transfère que les journaux système. Le préfixe `005-` fait que rsyslog lit la règle de transfert en premier, de sorte que chaque message est transféré.

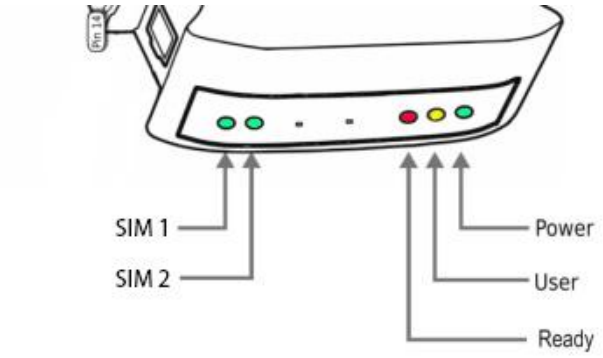
Pour chiffrer le trafic des journaux avec TLS, consultez le guide rsyslog Encrypting Syslog Traffic with TLS.

Dépannage

Pour vous assurer que l'appareil fonctionne correctement, suivez les trois étapes:

1. Vérification des LED
2. Vérification des informations de l'appareil (Informations système)
3. Vérification des journaux de l'appareil (description ci-dessous)

Vérification des LED



Emplacements des LED

Le fonctionnement normal de l'appareil est signalé par les LED comme suit:

LED	Fonctionnement correct
Power (PWR)	Allumée en continu
User	Clignote pendant la lecture/écriture sur la clé USB
Ready (RDY)	Clignotement
SIM1 NXS-9700-3G	Clignotement lent en mode veille, Clignotement rapide lorsque le modem 1 est utilisé
SIM2 NXS-9700-3G	Non utilisée

Vérification des informations de l'appareil

Les informations de l'appareil (type d'appareil, version du logiciel, IMEI du modem, IMSI, force du signal réseau, nom du réseau) se trouvent sous **System > System info**. Voir System.

Journaux de l'appareil

Sous **System > Logs** vous pouvez trouver les dernières lignes des journaux de l'appareil: journal du modem, journal de la base de données et journal système. En cas de problème avec l'appareil, ces journaux constituent une source précieuse d'informations de dépannage.

Les journaux étendus de l'appareil peuvent être téléchargés via le bouton **Download logs** sur la même page. Voir System.

Lorsque l'appareil n'est pas joignable

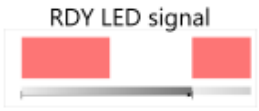
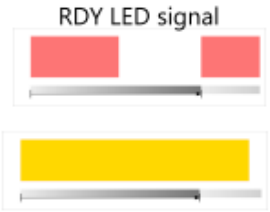
1. Vérifiez que l'appareil est correctement connecté au réseau. Vérifiez l'état des LED de la prise RJ45.
2. Si l'appareil ne répond pas en raison d'un dysfonctionnement ou de paramètres utilisateur incorrects, redémarrez l'appareil en débranchant et en rebranchant la source d'alimentation (ou en appuyant sur l'interrupteur de réinitialisation).
3. Si vous ne pouvez toujours pas vous connecter à l'appareil, il est possible de restaurer les paramètres d'adresse IP d'usine en utilisant le bouton SW.

Restauration des paramètres d'usine

La fonction Réinitialiser aux paramètres par défaut vous permet de restaurer rapidement l'appareil à sa configuration d'usine d'origine.

> **Avertissement**
>
> La restauration des paramètres d'usine supprime définitivement la configuration utilisateur actuelle. Assurez-vous que tous les paramètres ou données nécessaires sont sauvegardés avant de continuer.

Pour lancer la réinitialisation, appuyez sur le bouton SW et maintenez-le enfoncé pendant 10 secondes. L'appareil passera en mode de récupération.

Signalisation LED	Actions UTILISATEUR	Réaction du système
	1. **When the device is ready to operate**	–
–	2. **Press and hold SW button for 10 seconds**	Restore service est en compte à rebours.
	3. **Release SW button after 10 seconds.** User LED will begin to blink.	Le système lit les paramètres d'usine. Les paramètres d'usine sont appliqués à l'appareil.
	4. **Wait until system reboots.** Default settings are restored.	Le système se prépare à redémarrer.

Hardware Rev.5 et ultérieure

Rev.5

Le processus utilise une partition de récupération dédiée en lecture seule, garantissant que l'image de restauration reste intacte et n'est pas affectée par le fonctionnement normal de l'appareil. Une fois le mode de récupération activé, un seul bip court lance un compte à rebours de 10s. Un deuxième bip court confirme le début du processus de restauration. L'ensemble du processus prend généralement quelques minutes.

Une fois l'opération réussie, l'appareil signale avec trois bips courts, suivis d'un compte à rebours de 10s avant de redémarrer automatiquement. Si l'opération est annulée pendant le compte à rebours, deux bips courts sont émis. En cas d'erreur de restauration, l'appareil émet un bip long suivi de deux bips courts, puis bascule vers un shell de service pour les diagnostics.

Hardware Rev.3–Rev.4

Rev.3 Rev.4

La fonction de réinitialisation restaure uniquement les paramètres suivants à leurs valeurs par défaut : paramètres IP, paramètres de fuseau horaire, contenu de la base de données et utilisateurs/mots de passe du système d'exploitation Linux.

Service et réparation

Garantie

Votre SMSEagle est fourni avec une couverture standard de 2 ans d'assistance technique et de garantie de réparation matérielle. La garantie standard peut être prolongée lors de l'achat de l'appareil à une couverture de 3 ans (vérifiez vos conditions d'achat). Pour des informations détaillées sur les conditions de garantie, consultez la carte de garantie fournie avec votre appareil ou suivez le lien : www.smseagle.eu/downloads

Service

Avant de contacter l'équipe d'assistance, assurez-vous d'avoir lu la section Dépannage de ce manuel. Plus d'informations et de conseils utiles sur la configuration de l'appareil SMSEagle peuvent également être trouvés dans notre base de connaissances en ligne, à la même adresse que le portail d'assistance ci-dessous.

L'équipe d'assistance SMSEagle est disponible par e-mail ou téléphone.

Portail d'assistance et base de connaissances : https://support.smseagle.eu

E-mail : support@smseagle.eu

Téléphone : + 48 61 6713 413

Le service d'assistance est fourni par : Proximus Sp. z o.o. ul. Piątkowska 163, 60-650 Poznan, Poland

Lorsque vous contactez l'équipe d'assistance, préparez-vous à fournir les informations suivantes :

Journaux système

Accédez à **System > Logs > Download logs**. Fournissez le package de journal à l'équipe d'assistance si demandé.

Adresse MAC

Chaque appareil SMSEagle a une adresse MAC unique. Elle est imprimée sur le corps de l'appareil ou se trouve sous **System > System info**.

Spécifications techniques et informations de sécurité

Spécification technique

Spécification matérielle

- Type de processeur :
  - hardware Rev.5, Rev.4: Broadcom BCM2711 1.5 GHz quad-core Cortex-A72 (ARM v8) 64-bit
  - hardware Rev.3: Broadcom BCM2837 1.2 GHz quad-core ARM Cortex-A53 (64-bit)
- Mémoire opérationnelle (RAM) :
  - hardware Rev.5, Rev.4: 2GB LPDDR4
  - hardware Rev.3: 1GB LPDDR2 @ 900 MHz
- Stockage eMMC
  - hardware Rev.5, Rev.4: 16GB
  - hardware Rev.3: 4GB
- Interface réseau : Ethernet (1xRJ45) : Gigabit Ethernet 10/100/1000 TX
- 1x port HDMI à des fins de débogage
- Autres ports externes : 4x DI, 4x DO, 1× 1Wire, 2x USB 2.0 (max. 300mA)
- Types de ports d'entrée/sortie numérique : type DI « résistance de tirage », type DO « collecteur ouvert »
- Horloge RTC : RTC 240B SRAM, Watchdog timer
- Capteur interne d'humidité et de température : Précision ± 0,5 °C, ±2 %RH
- Consommation d'énergie :
  - hardware Rev.5, Rev.4: max 25W
  - hardware Rev.3: max 12W
- Niveau sonore : Sans ventilateur
- Dimensions : (largeur x profondeur x hauteur) 45 × 120 × 101 mm
- Poids : 350g
- Boîtier : ABS, installation sur rail DIN
- Paramètres de fonctionnement :
  - Température de fonctionnement : 0 ~ 40°C

    - Humidité : 8 ~ 90% RH (pas de condensation)
- Modem interne

Device type NXS-9700-5G Rev.5

- Bandes de fréquences : 5G NR, LTE.
- 5G NR 3GPP Release 17 RedCap SA, Sub-6 GHz
- 5G NR SA : n1/ 2/ 3/ 5/ 7/ 8/ 12/ 13/ 14/ 18/ 20/ 25/ 26/ 28/ 30/ 38/ 40/ 41/ 48/ 66/ 70/ 71/ 77/ 78/ 79
- LTE FDD : B1/ 2/ 3/ 4/ 5/ 7/ 8/ 12/ 13/ 14/ 17/ 18/ 19/ 20/ 25/ 26/ 28/ 30/ 66/ 70/ 71
- LTE TDD : B34/ 38/ 39/ 40/ 41/ 42/ 43/ 48
- Débits de données (Max)
    - 5G SA Sub-6 : 223 Mbps (DL)/ 123 Mbps (UL)
    - LTE : 195 Mbps (DL)/ 105 Mbps (UL)
- Puissance de sortie (Nominale) :
    - Classe 3 (23dBm±2dB) pour les bandes 5G NR
    - Classe 2 (26dBm+2/-3dB) pour les bandes 5G NR HPUE (n38/n40/n41/n77/n78/n79)
    - Classe 3 (23dBm±2dB) pour les bandes LTE
    - Classe 2 (26dBm±2dB) pour les bandes LTE HPUE (B38/B40/B41/B42/B43)

Type de périphérique NXS-9700-5G Rev.4

- Bandes de fréquences : 5G NR, LTE, UMTS.
- 5G NR 3GPP Release 15 NSA/SA, Sub-6 GHz
- 5G NR NSA/SA : n1/n2/n3/n5/n7/n8/n12/n20/n25/n28/n38/n40/n41/ /n66/n71/n77/n78/n79
- LTE DL Cat 16/ UL Cat 18
- LTE FDD : B1/B2/B3/B4/B5/B7/B8/B12(B17)/B13/B14/B18/B19/B20/B25/B26/B28/B29/B30/B32/B66/B71
- LTE TDD : B34/B38/B39/B40/B41/B42/B43/B48
- WCDMA : B1/B2/B3/B4/B5/B6/B8/B19
- Puissance de sortie (Nominale) :
    - Classe 3 (23dBm±2dB) pour les bandes 5G NR
    - Classe 2 (26dBm±2dB) pour les bandes 5G NR HPUE (n41/n77)
    - Classe 3 (23dBm±2dB) pour les bandes LTE
    - Classe 2 (26dBm±2dB) pour les bandes LTE HPUE (B38/B41)
    - Classe 3 (24dBm+1/-3dB) pour les bandes WCDMA

Type de périphérique NXS-9700-4G Rev.4

- Bandes de fréquences : LTE, UMTS. GSM optionnel.
- LTE FDD : B1/B2/B3/B4/B5/B7/B8/B12/B13/B18/B19/B20/B25/B26/B28
- LTE TDD : B38/B39/B40/B41
- UMTS : B1/B2/B4/B5/B6/B8/B19
- GSM : B2/B3/B5/B8 (optionnel)
- Puissance de sortie (Nominale) :
  - Classe 3 (23dBm±2dB) pour bandes LTE-FDD, LTE-TDD
  - Classe 3 (24dBm+1/-3dB) pour les bandes WCDMA
  - Classe 4 (33dBm±2dB) pour GSM850, EGSM900
  - Classe 1 (30dBm±2dB) pour DCS1800, PCS1900
  - Classe E2 (27dBm±3dB) pour GSM850 8-PSK, EGSM900 8-PSK
  - Classe E2 (26dBm±3dB) pour DCS1800 8-PSK, PCS1900 8-PSK

Type de dispositif NXS-9700-4G Rev.3

- Bande de fréquences : UMTS, LTE
- Bandes LTE : LTE FDD : 1-5, 7, 8, 12, 13, 17, 20, 25, 26, 28, 29, 30 (réception uniquement), 66 LTE TDD : 38, 40, 41
- Bandes 3G : 1, 2, 4, 5, 8
- Puissance de sortie :
  - Classe 3 (0,2 W, 23 dBm) @ LTE
  - Classe 3 (0,25 W, 23 dBm) @ 3G

Type de dispositif NXS-9700-3G Rev.3

- Bande de fréquences : GSM, UMTS
- GSM/GPRS quadri-bande 850/900/1800/1900 MHz
- UMTS 800/850/900/AWS 1700/1900/2100 MHz
- Puissance de sortie (Nominale) :
  - E-GSM 900 : Classe 4, DCS 1800 : Classe 1
  - EDGE 900 : Classe E2, EDGE 1800 : Classe E2
  - FDD I : Classe 3, FDD VIII : Classe 3
- Norme de carte SIM : mini
- Connecteur d’antenne : SMA
- Pays d’origine : Union européenne (Pologne)

Alimentation électrique

- matériel Rev.5, Rev.4 :
  - Bloc d'alimentation externe avec circuit de sortie évalué ES1 (12Vcc ; min. 3,3A), PS2 (LPS – Limited Power Source). Entrée de ligne CA :
    - Plages de tension : 100–240V courant alternatif (CA)
    - Fréquence : 50–60Hz monophasé
    - Type de fiche CC : 5,5/2,5
  - Source d'alimentation alternative : PoE+ (IEEE 802.3at Type 2). Circuit fourni avec PoE+ : évalué ES1 (50-57Vcc ; 30W), PS2 (LPS – Limited Power Source)
- matériel Rev.3 :
  - Alimentation électrique externe avec circuit de sortie évalué ES1 (12Vdc ; min, 1A), PS2 (LPS – Limited Power Source). Entrée ligne AC :
    - Plages de tension : 100–240V courant alternatif (CA)
    - Fréquence : 50–60Hz monophasé
    - Type de fiche CC : 5,5/2,5

Antenne

- Type de dispositif NXS-9700-5G Rev.5 :
  - 2x antennes omnidirectionnelles 2,5dBi avec pied magnétique
  - Bande de fréquence : 4GLTE, 5GNR
  - Longueur de câble 2m
  - Type de connecteur : SMA
  - Impédance : 50 Ohm
  - Dimensions Ø 31 × 109 mm
- Type de dispositif NXS-9700-5G Rev.4 :
  - 2x antennes MIMO omnidirectionnelles 2,5dBi avec pied magnétique/adhésif
  - Bande de fréquence : UMTS, LTE, 5GNR
  - Longueur de câble 2m
  - Type de connecteur : SMA
  - Impédance : 50 Ohm
- Type de dispositif NXS-9700-4G :
  - Antenne omnidirectionnelle 2dBi avec pied magnétique
  - Bande de fréquences : UMTS, LTE
  - Longueur de câble 3m
  - Type de connecteur : SMA

    - Impédance : 50 Ohm
- Type de dispositif NXS-9700-3G :
    - Antenne omnidirectionnelle 3dBi avec pied magnétique
    - Bande de fréquences : GSM, UMTS
    - Longueur de câble 3m
    - Type de connecteur : SMA
    - Impédance : 50 Ohm

Débit d'émission/réception

- Taux de transmission entrant : jusqu'à 30 SMS/min
- Taux de transmission sortant : jusqu'à 30 SMS/min

Plateforme logicielle

- Système d'exploitation : Linux
    - matériel Rev. 5 : noyau 6.12
    - matériel Rev. 4 : noyau 5.1x
    - matériel Rev. 3 : noyau 4.14
- serveur web Apache2 intégré
- serveur de base de données PostgreSQL intégré
- serveur de courrier Postfix intégré
- agent SNMP intégré
- client NTP intégré
- service de basculement intégré (cluster HA)
- mécanisme de surveillance pour modem 3G/4G/5G
- interface web moderne et réactive
- liste des ports TCP/UDP ouverts dans la configuration par défaut :
    - TCP : 22 (SSH), 80 (HTTP), 443 (HTTPS), 5432 (PostgreSQL avec restriction d'accès à localhost uniquement)
    - UDP : 68 (client DHCP), 323 (client NTP)

Informations importantes de sécurité

Ce chapitre fournit des informations importantes concernant les procédures de sécurité. Pour votre sécurité et celle de votre équipement, suivez ces règles de manipulation de votre appareil.

Avertissement

Le stockage ou l'utilisation incorrecte de votre appareil peut annuler la garantie du fabricant. Le non-respect de ces consignes de sécurité pourrait entraîner un incendie, une électrocution ou d'autres blessures ou dommages.

Prenez toujours les précautions suivantes.

Débranchez la fiche d'alimentation de la source d'alimentation secteur ou si l'une des conditions suivantes existe :

- le cordon ou la fiche d'alimentation devient effiloché ou endommagé autrement
- vous renversez quelque chose dans le boîtier
- l'appareil est exposé à la pluie ou à toute autre humidité excessive
- l'appareil a été tombé ou le boîtier a été endommagé autrement

Assurez-vous que l'utilisation de ce produit est autorisée dans votre pays et dans l'environnement requis. Comme pour tout autre équipement de télécommunication, l'utilisation de ce produit peut être dangereuse et doit être évitée dans les zones suivantes : où il peut interférer avec d'autres appareils électroniques situés à proximité dans des environnements tels que les hôpitaux, les aéroports, les avions, etc. ; où il existe un risque d'explosion tel que les stations-essence, les raffineries de pétrole, etc.

Il est de la responsabilité de l'utilisateur de respecter la réglementation du pays et la réglementation spécifique à l'environnement.

Ne démontez pas le produit ; toute trace de manipulation compromettrait la validité de la garantie.

Chaque appareil doit être équipé d'une antenne appropriée ayant des caractéristiques spécifiques. L'antenne doit être installée avec soin afin d'éviter toute interférence avec d'autres appareils électroniques et doit être installée en garantissant une distance minimale de 30 cm (12 pouces) par rapport au corps. Si cette exigence ne peut pas être satisfaite, l'intégrateur système doit évaluer le produit final par rapport à la réglementation SAR.

CLAUSE DE NON-RESPONSABILITÉ : Le fabricant n'est pas responsable de tout dommage causé par une installation inappropriée, le non-respect des conditions techniques appropriées ou l'utilisation d'un produit à des fins contraires à sa destination.

Déclarations réglementaires

Déclaration de conformité UE

Par les présentes, Proximus Sp. z o.o., propriétaire de la marque SMSEagle, déclare que l'équipement radio de type SMSEagle NXS-9700-3G, NXS-9700-4G, NXS-9700-5G est conforme à la Directive 2014/53/UE.

Le texte complet de la déclaration de conformité UE est disponible à l'adresse Internet suivante : www.smseagle.eu/certification

Déclaration de conformité FCC

Cet appareil est conforme à la partie 15 des règles FCC. L'utilisation est soumise aux deux conditions suivantes :

(1) Cet appareil ne doit pas causer d'interférences nuisibles, et

(2) cet appareil doit accepter toute interférence reçue, y compris les interférences susceptibles de causer un fonctionnement indésirable.

Note :

Cet équipement a été testé et jugé conforme aux limites pour un appareil de classe B, conformément à la partie 15 des règles FCC. Ces limites sont conçues pour fournir une protection raisonnable contre les interférences nuisibles dans un environnement commercial/professionnel non résidentiel. Cependant, il n'y a aucune garantie que des interférences ne se produiront pas dans une installation particulière. Si cet équipement cause des interférences nuisibles à la réception radio ou télévisée, ce qui peut être déterminé en éteignant et rallumant l'équipement, l'utilisateur est invité à essayer de corriger l'interférence par une ou plusieurs des mesures suivantes :

- Réorienter ou relocaliser l'antenne de réception
- Augmenter la séparation entre l'équipement et le récepteur
- Connecter l'équipement à une prise de courant sur un circuit différent de celui du récepteur
- Consulter le revendeur ou un technicien radio/TV expérimenté pour obtenir de l'aide

Important :

Cet équipement génère, utilise et peut rayonner de l'énergie radiofréquence et, s'il n'est pas installé et utilisé conformément au manuel d'instructions du fabricant, peut causer des interférences nuisibles avec les communications radio. L'utilisation de cet équipement dans une zone résidentielle risque de causer des interférences nuisibles, auquel cas vous serez tenu de corriger l'interférence à vos propres frais. Les règles FCC prévoient que les modifications ou les changements non expressément approuvés par SMSEagle™ pourraient invalider votre autorisation

à utiliser cet équipement. Ce produit a démontré la conformité EMC dans des conditions qui comprenaient l'utilisation d'appareils périphériques conformes (antennes) et de câbles blindés entre les composants du système. Il est important que vous utilisiez des appareils périphériques conformes et des câbles blindés entre les composants du système pour réduire la possibilité d'interférences avec les radios, les téléviseurs et autres appareils électroniques.

Déclaration de conformité du fournisseur FCC



Cette Déclaration de conformité du fournisseur est par les présentes émise conformément au Chapitre 1, Sous-partie A, Partie 2 du Titre 47 du Code des réglementations fédérales par :

Proximus Sp. z o.o.
ul. Piatkowska 163
60-650 Poznan, Poland

Le produit NXS-9700-4G, NXS-9700-5G est conforme aux exigences applicables de la Partie 15B de la Règle FCC pour les classes d'équipement correspondantes de Radiateurs non intentionnels.

PARTIE RESPONSABLE située aux États-Unis :

Testing Partners LLC

18200 SR 306

Chagrin Falls, OH 44023

info@testingpartners.com

La partie responsable garantit que chaque unité d'équipement commercialisée en vertu de cette Déclaration de conformité sera identique à l'unité testée et jugée acceptable selon les normes et que les dossiers entretenus par la partie responsable continuent à refléter que l'équipement produit en vertu de cette Déclaration de conformité du fournisseur continue de se conformer dans les limites de la variation qui peut être attendue en raison de la production en quantité et des tests sur une base statistique.

Déclaration réglementaire canadienne (ISDE)

Cet appareil est conforme aux norme(s) RSS exemptes de licence d'Industrie Canada. L'utilisation est soumise aux deux conditions suivantes :

(1) cet appareil ne doit pas causer d'interférence, et

(2) cet appareil doit accepter toute interférence, y compris l'interférence qui peut causer un fonctionnement indésirable de l'appareil.

Cet appareil numérique de classe B respecte les exigences du Règlement canadien sur le matériel brouilleur.

CAN ICES-3 (B)/NMB-3(B)

Avis de conformité à la réglementation d'Industrie Canada

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

(1) l'appareil ne doit pas produire de brouillage,

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Cet appareil numérique de classe B répond aux exigences du Règlement sur le matériel brouilleur du Canada.

CAN ICES-3 (B)/NMB-3(B)

Déclaration de conformité du Royaume-Uni

Par la présente, Proximus Sp. z o.o., propriétaire de la marque SMSEagle, déclare que l'équipement radio de type SMSEagle NXS-9700-3G, NXS-9700-4G, NXS-9700-5G est conforme à la Radio Equipment Regulations 2017.

Le texte complet de la déclaration de conformité UE est disponible à l'adresse Internet suivante : www.smseagle.eu/certification

Limites d'exposition aux radiofréquences

Cet appareil est conforme aux limites d'exposition aux radiations établies pour un environnement non contrôlé. Afin d'éviter le risque de dépasser les limites d'exposition aux radiofréquences, la proximité humaine à l'antenne ne doit pas être inférieure à 30 cm (12 pouces) pendant le fonctionnement normal.

Informations sur l'élimination et le recyclage

Votre appareil SMSEagle contient une batterie au lithium pour la sauvegarde de l'horloge temps réel. Éliminez l'appareil et/ou la batterie conformément aux lois et directives environnementales locales.

Union européenne — Informations sur l'élimination



Le symbole ci-dessus signifie que selon les lois et réglementations locales, votre produit doit être éliminé séparément des déchets ménagers. Lorsque ce produit arrive en fin de vie, apportez-le à

un point de collecte désigné par les autorités locales. La collecte séparée et le recyclage de votre produit au moment de l'élimination contribueront à préserver les ressources naturelles et à garantir qu'il est recyclé d'une manière qui protège la santé humaine et l'environnement.

Pour l'élimination dans les pays en dehors de l'Union européenne

Ce symbole n'est valable que dans l'Union européenne (UE). Si vous souhaitez vous débarrasser de ce produit, veuillez contacter vos autorités locales ou votre revendeur et demander la méthode d'élimination appropriée.

Informationen gemäß § 4 Absatz 4 Elektrogesetz (DE)

Folgende Batterien bzw. Akkumulatoren sind in diesem Elektrogerät enthalten

Matériel informatique	Type de batterie	Système chimique
Rev.4 Rev.5	CR1216	Lithium
Rev.3	CR1632	Lithium

Informations relatives à l'enlèvement sûr des piles ou des accumulateurs

Hardware Rev.4-5

Rev.4 Rev.5

- Ouvrez la paroi latérale transparente
- Soulevez le clapet situé sur le bord latéral à l'aide d'un tournevis. Retirez le clapet
- Retirez avec précaution la batterie du support situé sur le côté gauche
- La batterie et l'appareil peuvent maintenant être éliminés séparément

Hardware Rev.3

Rev.3

- Retirez le verrou DIN rouge en insérant un tournevis à fente sous la partie inférieure du verrou. Soulevez le verrou situé sous le clapet DIN retiré.
- Retirez le compartiment à cartes SIM
- Utilisez un tournevis à fente pour soulever les quatre verrous situés aux coins de l'appareil.
- Ouvrez le boîtier. La batterie se trouve sur la deuxième plaque. Retirez la batterie
- La batterie ou l'accumulateur et l'appareil peuvent maintenant être éliminés séparément

Directive relative à la restriction de l'utilisation de certaines substances dangereuses (RoHS)

RoHS de l'Union européenne

Les appareils SMSEagle vendus dans l'Union européenne, à partir du 3 janvier 2013, satisfont aux exigences de la directive 2015/863 relative à la restriction de l'utilisation de certaines substances dangereuses dans les équipements électriques et électroniques (« RoHS 3 »).