DOCUMENTATION 7.00

MHD-8100 User's Manual

Documentation

ENGLISH · SMSEAGLE

Table of contents

Cover . . . 8

SMSEagle Software Licensing Information . . . 9

What's In The Box . . . 17

Configuration Wizard . . . 18

- Step 1: Language & time . . . 18
- Step 2: Administrator account . . . 18
- Step 3: Notifications . . . 19
- Step 4: Modems . . . 20

Connectors, Ports and LEDs . . . 21

- Front Panel . . . 22
- Back Panel . . . 22
- Display . . . 22

Web Interface Overview . . . 26

- Signing in . . . 26
- Interface layout . . . 27
- Dashboard . . . 27
  - Needs your attention . . . 28
  - Traffic . . . 29
  - Unread messages . . . 29
  - System . . . 29
  - Latest messages and calls . . . 30
  - Modems . . . 30
- Quick actions . . . 31
- Personal account settings . . . 31
  - Personal data . . . 31
  - Password . . . 32
  - Security . . . 32

Messages . . . 33

- SMS (Conversations) . . . 33
  - Composing a message . . . 34
- Folders . . . 35
- Group messages . . . 36
- Escalation queue . . . 37
- Calls . . . 38
  - History . . . 38
- WhatsApp . . . 39
- Signal . . . 41
- Emails . . . 42
- Message templates . . . 42

Phonebook . . . 43
Contacts . . . 43
Groups . . . 43
Escalation groups . . . 44
Shifts . . . 46
Before you start . . . 46
Step 1: Open the Shifts page . . . 46
Step 2: Create a shift . . . 46
Step 3: Assign contacts to the shift . . . 47
Step 4: Choose what happens outside shift hours . . . 47

Automation . . . 48
Email to SMS . . . 48
Where to find it . . . 48
Step 1: Understand the recipient address format . . . 48
Step 2: Create a new rule . . . 49
Step 3: Add filtering conditions (optional) . . . 50
Step 4: Manage existing rules . . . 50
Email to SMS Poller . . . 51
Where to find it . . . 51
Creating a rule . . . 51
SMS to Email . . . 52
What this feature does . . . 52
Before you start . . . 52
Step 1: Open the SMS to Email page . . . 52
Step 2: Create a rule . . . 52
SMS Forward . . . 54
What this feature does . . . 54
Before you start . . . 54
Step 1: Open the SMS Forward page . . . 54
Step 2: Create a rule . . . 54
How forwarding works . . . 56
Autoreplies . . . 57
What this feature does . . . 57
Before you start . . . 57
Step 1: Open the Autoreplies page . . . 57
Step 2: Create a rule . . . 57
Step 3: Set the sending limit . . . 58
How matching works . . . 59
Periodic SMS . . . 59
What this feature does . . . 59
Before you start . . . 60
Step 1: Open the Periodic SMS page . . . 60
Step 2: Create a rule . . . 60
Subscriptions . . . 62
What this feature does . . . 62
Before you start . . . 62

Step 1: Open the Subscriptions page . . . 62
Step 2: Create a rule . . . 62
How matching works . . . 63
What happens when somebody subscribes . . . 63
Allow / Deny List . . . 64
What this feature does . . . 64
Before you start . . . 64
Step 1: Open the Allow / Deny List page . . . 64
Step 2: Choose the active mode . . . 65
Step 3: Add a number . . . 65
Step 4: Import a list from CSV . . . 65
Step 5: Configure the STOP word (optional) . . . 66
How filtering works . . . 66
Workflows . . . 67
Where to find it . . . 67
Step 1: Create a workflow and pick a trigger . . . 67
Step 2: Add condition groups (optional) . . . 67
Step 3: Add actions . . . 67
Webhooks . . . 68
What this feature does . . . 68
Before you start . . . 68
Step 1: Open the Webhooks page . . . 68
Step 2: Create a rule . . . 69
Step 3: Basic configuration . . . 69
Step 4: Trigger conditions . . . 71
Step 5: Security settings . . . 72
Step 6: Set the retry interval . . . 72
How webhooks behave . . . 72
MQTT . . . 73
What this feature does . . . 73
Before you start . . . 73
Part 1: Subscribe (MQTT into SMS) . . . 74
Part 2: Publish (SMS into MQTT) . . . 75
Inbox Rules . . . 77
Where to find it . . . 77
Configuring an inbox rule . . . 77
Cleanup Folders . . . 77
Where to find it . . . 78
Configuring a cleanup rule . . . 78
Reports & Statistics . . . 79
Reports . . . 79
Periodic Reports . . . 80
Statistics . . . 81
Periodic Statistics . . . 82
Monitoring . . . 83
Network Monitor . . . 83

What this feature does . . . 83
Before you start . . . 83
Part 1: Tasks . . . 84
Part 2: Reports . . . 89
Part 3: SNMP Traps . . . 90
How Network Monitor behaves . . . 92
Digital Input / Output . . . 93
What this feature does . . . 93
Before you start . . . 93
Where to find it . . . 94
Part 1: Input rules (input signal into SMS) . . . 94
Part 2: Output rules (SMS into output signal) . . . 97
Part 3: External pins . . . 100
How Digital I/O rules behave . . . 102
Settings . . . 103
Account settings . . . 103
How to configure Multi-Factor Authentication (MFA) . . . 103
SMS / MMS . . . 104
Messages . . . 104
Modems . . . 105
Multimodem . . . 105
MMS . . . 108
Calls . . . 111
TTS local models . . . 111
TTS online models (ElevenLabs) . . . 113
Incoming calls . . . 115
Call forward . . . 115
WhatsApp . . . 115
What this feature does . . . 115
Before you start . . . 115
Step 1: Open the WhatsApp settings . . . 116
Step 2: Enable the service . . . 116
Step 3: Link your phone . . . 116
Step 4: Decide what happens to non-WhatsApp recipients . . . 116
Step 5: Keep the service up to date . . . 117
Unlinking and switching off . . . 117
Good to know . . . 117
Signal . . . 118
What this feature does . . . 118
Before you start . . . 118
Step 1: Open the Signal settings . . . 119
Step 2: Enable the service . . . 119
Step 3: Register a phone number . . . 119
Step 4: Verify the number . . . 120
Step 5: Keep the service up to date . . . 120
Removing the number . . . 120
Good to know . . . 121

Email . . . 121
Email to SMS . . . 121
Email to SMS Poller . . . 123
SMTP Configuration . . . 125
Email alerts . . . 125
SMPP . . . 126
Connection details . . . 127
Turning SMPP on . . . 127
MQTT . . . 128
Network . . . 129
IP Settings . . . 129
SSL . . . 129
Failover . . . 129
SNMP . . . 131
Mobile Data . . . 135
Application . . . 136
Regional . . . 136
Security . . . 136
Access and visibility . . . 136
API and integrations . . . 136
LDAP . . . 137
What this feature does . . . 137
Before you start . . . 137
Step 1: Open the LDAP page . . . 138
Step 2: Enable the integration . . . 138
Step 3: Connection . . . 138
Step 4: Directory structure . . . 139
Step 5: Attributes and security . . . 140
Step 6: Sync and access . . . 140
Step 7: Save and test . . . 141
Date / Time . . . 142

System . . . 143
Users . . . 143
System info . . . 143
Logs . . . 144
Updates . . . 144
Patches . . . 144
Backup / Restore . . . 144
Restart . . . 144
Advanced . . . 144

API and Developer Integration . . . 145
API Reference . . . 145
API keys . . . 145
API v2 keys . . . 145
API v1 keys . . . 146
Creating a key . . . 146

Which users have API access . . . 147
Access to resources of other users . . . 147

Plugins and integrations . . . 148

Advanced . . . 149
Connecting directly to the SMSEagle database . . . 149
Injecting a short SMS using SQL . . . 149
Injecting a long SMS using SQL . . . 150
Database cleaning scripts . . . 152
Forwarding logs to an external server . . . 152

Troubleshooting . . . 154
Verification of LEDs . . . 154
Checking the device information . . . 154
Device logs . . . 154
When the device is not reachable . . . 155
Restoring factory defaults . . . 155
Service & Repair . . . 155
Warranty . . . 155
Service . . . 156

Tech Specs & Safety Information . . . 157
Technical Specification . . . 157
Hardware Specification . . . 157
Power Supply . . . 158
Antenna . . . 158
Sending/Receiving Throughput . . . 158
Software Platform . . . 158
Important Safety Information . . . 159

Regulatory Statements . . . 161
EU Declaration of Conformity . . . 161
FCC Compliance Statement . . . 161
FCC Supplier's Declaration of Conformity . . . 162
Canadian Regulatory Statement (ISED) . . . 162
Avis de conformité à la réglementation d'Industrie Canada . . . 163
UK Declaration of Conformity . . . 163
RF Exposure Limits . . . 163
Disposal and Recycling Information . . . 163
For disposal in countries outside of the European Union . . . 164
Information gemäß § 4 Absatz 4 Elektrogesetz (DE) . . . 164
Angaben zur sicheren Entnahme der Batterien oder der Akkumulatoren . . . 164
Restriction of Hazardous Substances Directive (RoHS) . . . 164
European Union RoHS . . . 164

Cover

Welcome to the MHD-8100 User's Manual!

The MHD-8100 is a hardware SMS gateway with eight built-in modems and your own SIM cards, so your messages go out over the mobile network directly from your own infrastructure, with no third-party SMS provider in between.

This manual is the complete reference for the device and applies to all MHD-8100 variants; where behaviour depends on the modem type or the hardware revision, the relevant section is marked with a badge. If your device is still in its box, start with What's In The Box and then run the Configuration Wizard. Otherwise, use the navigation on the left or the search box to go straight to the topic you need.

The materials used in this publication are copyright and are not to be duplicated, copied, or used without the prior consent of the copyright holder. Technical specifications and information in this document is subject to change without prior notice being given.

SMSEagle Software Licensing Information

IMPORTANT – READ BEFORE OPERATING

SMSEAGLE SOFTWARE END USER LICENSE AGREEMENT

The herein contained End User License Agreement (the "**Agreement**" or "**License**" or "**EULA**") shall be considered a legally binding agreement between you (an individual or an entity, hereinafter "**Licensee**" or "**You**" or "**Your**") and Proximus Sp. z o.o., ul. Piątkowska 163, Poznań, Poland, zip code 60-650 (hereinafter "**PROXIMUS**") for the use of the software preinstalled on a SMSEagle device (i.e. software which is installed and delivered together with this device), which may include related printed material and any other components and/or software modules, including but not limited to required drivers (the "**SMSEagle Software**"). Other aspects of the SMSEagle Software may also include, but not limited to software updates and any upgrades that PROXIMUS may supply to You or make available to You, or that You obtain after acquiring the SMSEagle device, and as such that said items are not accompanied by a separate license agreement or terms of use.

BY ACCEPTING THESE TERMS IN THE SMSEAGLE DEVICE'S GRAPHICAL USER INTERFACE (GUI), BY YOUR USING THE SMSEAGLE DEVICE, OR UPDATING OR UPGRADING THE SMSEAGLE SOFTWARE, YOU AGREE TO BE LEGALLY BOUND BY THE HEREIN-CONTAINED TERMS OF THIS LICENSE AGREEMENT. IF YOU DO NOT AGREE TO BE BOUND BY THE TERMS OF THIS EULA, DO NOT USE THE SMSEAGLE DEVICE AND YOU MAY CHOOSE TO PROMPTLY RETURN THE DEVICE FOR A REFUND OF ITS PURCHASE PRICE BY CONTACTING PROXIMUS AT THE ADDRESS ABOVE. The current version of this EULA is made available to You prior to purchase on www.smseagle.eu and is presented in the SMSEagle device's GUI during initial setup and after any material change to its terms. Your acceptance in the GUI (including the date, version, and device identifier) is recorded locally in the SMSEagle device's database. If You do not accept the terms in the GUI, the SMSEagle Software will not be activated for use.

THE SMSEAGLE SOFTWARE IS PROTECTED BY COPYRIGHT LAWS, AS WELL AS ANY OTHER RELEVANT INTELLECTUAL PROPERTY LAWS. THE SMSEAGLE SOFTWARE IS LICENSED AND NOT SOLD. ALL RIGHTS INCLUDING COPYRIGHTS TO SMSEAGLE SOFTWARE REMAIN THE SOLE OWNERSHIP OF PROXIMUS, ADDITIONALLY AS STATED BELOW, THE SMSEAGLE SOFTWARE INCLUDES SOME MODULES DEVELOPED BY OTHERS, WHICH ARE SUBLICENSED TO YOU HEREBY ACCORDING TO TERMS PERMITTED BY THE DEVELOPER.

This EULA gives you specific legal rights, and you may also have other legal rights in addition, which vary from jurisdiction to jurisdiction. The disclaimers, exclusions, and limitations of liability under this EULA will not apply only to the extent prohibited by applicable law. Some jurisdictions do not allow the exclusion of implied warranties or the exclusion or limitation of incidental or consequential damages or other rights, so in that case those provisions of this EULA may not apply to you. However, it does not prejudice the executability and applicability of all other provisions of EULA.

1. **DEFINITIONS AND INTERPRETATIONS**
    1. "Agreement" or "License" or "EULA" shall mean this End User License Agreement.

2. “Licensee” or “You” or “Your” refers to you, the individual or business entity acquiring a SMSEagle device on which the SMSEagle Software has been installed.
3. “Intellectual Property” means current and future worldwide rights under copyright law, patent law, trade secret law, trademark law, moral rights law, and other similar rights.
4. “Update” means maintenance of, or a fix to, a version of SMSEagle Software, including, but not limited to a hot fix, patch, or enhancement, none of which function as a standalone service or other software package and which do not have an additional cost for an existing Licensee.
5. “Upgrade” means a major, standalone version of SMSEagle Software, which may include additional applications, features, or functionality.
6. A reference to “person” includes a natural person, corporate or unincorporated body (whether or not having separate legal personality) and that person’s legal and personal representatives, successors and permitted assigns.
7. Words in the singular shall include the plural and vice versa.
8. A reference to a statute, statutory provision or subordinate legislation is a reference to it as it is in force from time to time, taking account of any amendment or reenactment and includes any statute, statutory provision or subordinate legislation which it amends or re-enacts; provided that, as between the Parties, no such amendment or re-enactment shall apply for the purposes of this Agreement to the extent that it would impose any new or extended obligation, liability or restriction on, or otherwise adversely affect the rights of, any Party.

1. A reference to writing or written includes e-mail.
2. Any obligation in this Agreement on a person not to do something includes an obligation to not agree or allow that thing to be done.
3. Any phrase introduced by the terms “including”, “include”, “in particular” or any similar expression shall be construed as illustrative and shall not limit the sense of the words preceding those terms.
4. References to articles, sections, or clauses are to the articles, sections, and clauses of this Agreement.
5. “We”, “Us”, and “Our” refer to Proximus Sp. z o.o. (“PROXIMUS”).
6. The “Parties” to this Agreement are You and Proximus Sp. z o.o. (“PROXIMUS”).
7. “Collect” refers to transmitting data off the device in a way that allows PROXIMUS or any third-party partners to access it.

2. **LICENSE GRANT**

1. PROXIMUS grants to You a non-exclusive license for the use of the SMSEagle Software on the SMSEagle device on which it was preinstalled and installation of Updates and Upgrades subject to the terms and conditions set forth herein:

1. **Use.** PROXIMUS grants You the right to use a single instance of the SMSEagle Software on the SMSEagle device you have acquired. Use on any other device or computer is prohibited.

2. **Backup Copy.** You may retain a single copy of the current version of SMSEagle Software for Your SMSEagle device as may be necessary for backup purposes.
    1. Furthermore, this EULA shall also cover any and all software Updates and Upgrades provided by PROXIMUS that would replace, overwrite and/or supplement the original installed version of the SMSEagle Software, unless those other Updates and Upgrades are covered by a separate license, in which case the terms of that license will govern.

1. **INTELLECTUAL PROPERTY**
    1. **PROTECTED SMSEAGLE SOFTWARE**. The SMSEagle Software is protected by copyright and other Intellectual Property laws and treaties.
    2. **RESTRICTIONS ON USE**. As a Licensee, You may not: (a) Make use of the SMSEagle Software on more than one device at a time, without prior purchase of additional devices; (b) Share or otherwise make available the SMSEagle Software, in any manner whatsoever, to any third party (c) Modify, adapt, create derivative works from or translate any part of the SMSEagle Software other than what may be used within Your SMSEagle device in accordance with this License; (d) Reverse engineer, decompile or disassemble the SMSEagle Software, nor attempt to locate or obtain its source code (except to the extent such acts are permitted by mandatory provisions of applicable law, including Article 6 of Directive 2009/24/EC on decompilation for the purpose of achieving interoperability with other programs); (e) Attempt to alter or remove any trademark, copyright or other proprietary notice contained within the SMSEagle Software; or (f) Make use of SMSEagle Software in any manner not stipulated within this EULA or the documentation accompanying the SMSEagle device on which it was preinstalled.
    3. **UPDATES/UPGRADES**. PROXIMUS may find it appropriate to make available Updates or Upgrades to the SMSEagle Software. You may initiate the process for installing any Update or Upgrade such as by clicking a button “Check for software updates now” in the SMSEagle device’s web interface. Alternatively (when the device has no Internet access) You may obtain an Update or Upgrade package from SMSEagle support at https://support.smseagle.eu to be later installed on the SMSEagle device. It shall be at the sole discretion of PROXIMUS to make conditional releases of said Updates or Upgrades to You upon Your acceptance of another EULA or execution of another separate agreement. Deciding to install and make use of these Updates or Upgrades, You agree to be subject to all applicable license, terms and conditions of this EULA and/or any other agreement. PROXIMUS undertakes to provide security Updates for the SMSEagle Software for a minimum period of five (5) years from the date of first sale of the relevant SMSEagle device model (the “Update Period”). Following expiry of the Update Period, PROXIMUS may, at its sole discretion, continue to provide Updates or Upgrades, but shall not be obliged to do so. PROXIMUS shall announce the End-of-Life date of each SMSEagle device model on its website no later than twelve (12) months before that date. This commitment is without prejudice to any longer support period that may be required by mandatory provisions of applicable law, including the Cyber Resilience Act and the NIS2 Directive.

2. **DISCLAIMER OF WARRANTY**

PROXIMUS shall use reasonable efforts consistent with prevailing software development standards to maintain SMSEagle Software in a manner which minimizes errors and interruptions.

HOWEVER, PROXIMUS NEITHER WARRANT THAT THE USE OF SMSEAGLE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE; NOR MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM USE OF SMSEAGLE SOFTWARE.

TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT AS EXPRESSLY PROVIDED HEREIN AND NOTWITHSTANDING ANYTHING TO THE CONTRARY, NEITHER PROXIMUS NOR ANY OFFICER, DIRECTOR, SUBSIDIARY, AFFILIATE, AUTHORIZED RESELLER, OR EMPLOYEE THEREOF, MAKES ANY OTHER WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE, AND NONINFRINGEMENT.

1. **LIMITATION OF LIABILITY**
    1. PROXIMUS's liability in connection with any claim caused by, related to, or arising from the use of the SMSEagle Software, or the sum of such claims, shall never exceed the cost of the SMSEagle device in respect of which the damage occurred, unless such limitation of liability is not permitted under applicable Polish law.
    2. PROXIMUS shall not be liable to the Licensee for any indirect or consequential losses, including loss of profits of any kind and loss of customers, sales, margin, production, image, data or configuration, provided that the above exclusion does not apply to damage caused by PROXIMUS willfully (intentionally).
    3. PROXIMUS shall not be liable in particular for: (i) loss of data or configuration; (ii) lost profits of the Licensee; (iii) indirect or consequential damages; (iv) actions of third parties.
    4. With regard to PROXIMUS's liability for any claims by the end user, PROXIMUS's liability is limited only to situations where the damage is the result of a direct action or omission by PROXIMUS and only to the cost of the SMSEagle device in respect of which the damage occurred, unless such limitation of liability is not permitted under applicable Polish law.
    5. The provisions of this section do not apply to Licensees who are consumers or individual entrepreneurs within the meaning of Polish law, to the extent the limitations herein are prohibited by mandatory consumer protection provisions.
2. **OPEN SOURCE**

Certain software modules in the PROXIMUS Software are subject to "open source" or "free software" licenses ("Open Source Software"). Some of the Open Source Software is owned by third parties. Such Open Source Software is not subject to the terms and conditions of this Agreement. Instead, each item of Open Source Software is licensed under the terms of the end user license that accompanies such Open Source Software. Nothing in this Agreement limits your rights under, or grants you rights that supersede, the terms and conditions of any applicable end user license for the Open Source Software. Applicable Open Source licenses include the: MIT License; GNU General Public License v. 2.0; GNU Lesser General Public License v. 2.1; BSD-3 Clause License; Apache License 2.0. If required by any license for particular Open Source Software, PROXIMUS

makes such Open Source Software, and Our modifications to that Open Source Software, available by written request to Us at the email or mailing address.

1. **U.S. GOVERNMENT END USERS**

The SMSEagle Software is licensed to the U.S. Government with RESTRICTED RIGHTS. The use, duplication of, or the disclosure thereof by the U.S. Government, shall be subject to restrictions in accordance with DFARS 252.227-7013 of the Technical Data and Computer Software clause, and 48 CFR 52.227-19 of the Commercial Computer Software clause, as applicable.

1. **DATA PRIVACY**
    1. **DATA COLLECTION STATEMENT**. PROXIMUS does NOT collect ANY data you are working with when You use SMSEagle device. We could not see or collect any data saved on SMSEagle device, because we do not have any access to Your device. In the course of providing the SMSEagle Software and related support, however, PROXIMUS may process certain personal data of the Licensee (or, where the Licensee is an entity, its authorised representatives and end users). The following information is provided pursuant to Article 13 of Regulation (EU) 2016/679 (GDPR):
    2. Controller: Proximus Sp. z o.o., ul. Piątkowska 163, 60-650 Poznań, Poland; Email: odo@smseagle.eu.
    3. Categories of personal data processed: (a) registration and licensing data (company name, contact person, email, device serial number); (b) Update/Upgrade telemetry strictly limited to software version, device model, device serial number, IP address, where applicable. Personal data processed in connection with the provision of technical support is governed by a separate Technical Support Services Policy available at the Proximus website: www.smseagle.eu.
    4. Purposes and legal bases of processing: (a) performance of this EULA and provision of Updates and Upgrades - Article 6(1)(b) GDPR; (b) compliance with legal obligations (tax, accounting) - Article 6(1)(c) GDPR; (c) legitimate interests of PROXIMUS in improving the SMSEagle Software and defending against claims - Article 6(1)(f) GDPR.
    5. Recipients of personal data: authorised employees and contractors of PROXIMUS bound by confidentiality, IT service providers (hosting, email, ticketing) acting as processors under Article 28 GDPR, and competent public authorities where required by law.
    6. Transfers to third countries: personal data is processed primarily within the European Economic Area. Where transfers to third countries occur (e.g. use of certain IT providers), they take place on the basis of an adequacy decision or appropriate safeguards such as the EU Standard Contractual Clauses.
    7. Retention period: registration and licensing data – for the term of this EULA and for the period required by applicable law (in particular tax and accounting law, typically 5 years); data processed on the basis of legitimate interests – until an effective objection is raised or the legitimate interest ceases.

8. Rights of data subjects: the Licensee has the right to access, rectification, erasure, restriction of processing and data portability of their personal data, as well as the right to object to processing based on legitimate interests.
9. Right to lodge a complaint: the Licensee has the right to lodge a complaint with the President of the Personal Data Protection Office (Prezes Urzędu Ochrony Danych Osobowych), ul. Stawki 2, 00-193 Warsaw, Poland.
10. Automated decision-making: PROXIMUS does not carry out automated decision-making, including profiling, within the meaning of Article 22 GDPR in connection with this EULA.
11. Provision of personal data is voluntary but necessary for the conclusion and performance of this EULA and for the provision of support services. Further details, including any updates to this information, are available in the Privacy Policy at https://www.smseagle.eu/privacy-policy/.

2. **TERMINATION**
    1. PROXIMUS reserves the right to terminate this EULA with immediate effect in the event of: (i) a material breach by the Licensee of the license restrictions set out in Section “Restrictions on Use”; (ii) unauthorised reproduction, distribution or modification of the SMSEagle Software; or (iii) circumvention or tampering with any technical protection measures.
    2. PROXIMUS and a Licensee who acquired the SMSEagle device directly from PROXIMUS may terminate this EULA with at least thirty (30) days’ written notice.
    3. Subject to mandatory consumer protection laws, if PROXIMUS terminates this EULA for the reasons listed in section 9.01. above, the Licensee shall not be entitled to a refund of the purchase price of the SMSEagle device or of any fees paid in connection with the SMSEagle Software.
    4. Upon termination of this EULA, the Licensee shall cease all use of the SMSEagle Software and make any backup copies held unusable. Sections “Intellectual Property”, “Disclaimer of Warranty”, “Limitation of Liability and Remedies”, “Data Privacy”, “Governing Law” and “Dispute Resolution” shall survive termination.
    5. If the Licensee purchased the SMSEagle device from a reseller or authorized partner, the rules for returns, cancellations, and refunds of the SMSEagle device are specified on the invoice or in other sales documentation provided by that reseller or authorized partner.
    6. This EULA is provided independently of a hardware warranty applicable to the SMSEagle device. The expiration or termination of this EULA does not affect the validity and duration of the hardware warranty assigned to the SMSEagle device, nor do the terms of the hardware warranty limit the Licensee’s rights under this EULA.
3. **MISCELLANEOUS**
    1. **SUCCESSORS AND ASSIGNS**. This EULA, in its entirety, shall be legally binding upon and inure to the benefit of PROXIMUS and You, our respective successors and permitted assigns.

2. **SEVERABILITY**. If any provision of this Agreement is held to be illegal, invalid or unenforceable by a tribunal of competent jurisdiction, the remaining provisions shall not be affected.
3. **WAIVER**. If there is any waiver of any breach or failure to enforce any of the provisions contained herein, it shall not be deemed as a future waiver of said terms or a waiver of any other provision of this EULA.
4. **AMENDMENTS**. Any waiver, supplementation, modification or amendment to any provision of this EULA, shall be effective only when done so in writing and signed off by PROXIMUS.
5. **GOVERNING LAW**. In matters not regulated herein the provisions of the Polish Civil Code shall apply and provisions of Polish Copyright Act, 4th February 1994 (Journal of Laws 1994, No. 24, item 83). This Agreement shall be governed in all respects by the laws of the Republic of Poland.
6. **DISPUTE RESOLUTION**. Any disputes arising out of or in connection with this Agreement shall be submitted to the exclusive jurisdiction of the common courts competent for the registered seat of PROXIMUS in Poznań, Poland. This provision shall not apply to Licensees who are consumers or individual entrepreneurs within the meaning of Polish law, who retain the right to bring proceedings before the court competent under applicable mandatory provisions of law.
7. **ASSIGNMENTS**. You have the right to transfer the SMSEagle Software to a third party only together with the permanent transfer of ownership of the SMSEagle device on which it was preinstalled. In such case, the transferee is obliged to accept this EULA in its current form prior to use of the SMSEagle Software, and You shall make any backup or other copies of the SMSEagle Software held by You unusable at the time of transfer. This provision is without prejudice to the doctrine of exhaustion of rights under Article 4(2) of Directive 2009/24/EC and any mandatory rights of the Licensee under EU law.
8. **VALID AND BINDING**. This Agreement constitutes a valid and legally binding obligation of the Parties, enforceable against the Parties in accordance with its terms, subject in all respects to the effects of bankruptcy, insolvency, fraudulent conveyance, reorganization, moratorium and other laws relating to or affecting creditors' rights generally and general equitable principles.
9. **EFFECT OF TITLE AND HEADINGS**. The title of the Agreement and the headings of Sections, and Clauses are included for convenience and shall not affect the meaning of the Agreement or the Section.
10. **FORCE MAJEURE**. Except for payment obligations, if either Party is prevented from performing or is unable to perform any of its obligations under this Agreement due to causes beyond the reasonable control of the Party invoking this provision, including but not limited to acts of God, acts of civil or military authorities, riots or civil disobedience, wars, strikes or labor disputes (each, a "**Force Majeure Event**"), such Party's performance shall be excused and the time for performance shall be extended accordingly provided that the Party promptly takes all reasonably necessary steps to resume full performance.

4. **CONSUMER AND INDIVIDUAL ENTREPRENEUR PROTECTION**

The provisions of this EULA do not prejudice the provisions on consumer protections and entrepreneur protection if You are a natural person who buys the device and conclude this EULA not connected directly with its business or professional activity or in case of entrepreneur being a natural person – not connected directly with its professional activity (applied to the EULA concluded from January 1st, 2021). If any provision of this EULA is inconsistent with mandatory consumer or individual entrepreneur's protection laws, the provision does not bind the consumer/ individual entrepreneur and the provision of commonly binding law closest to that provision shall apply.

1. **CONTACT INFORMATION**

If you have questions regarding this EULA, please contact PROXIMUS at:

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

What's In The Box



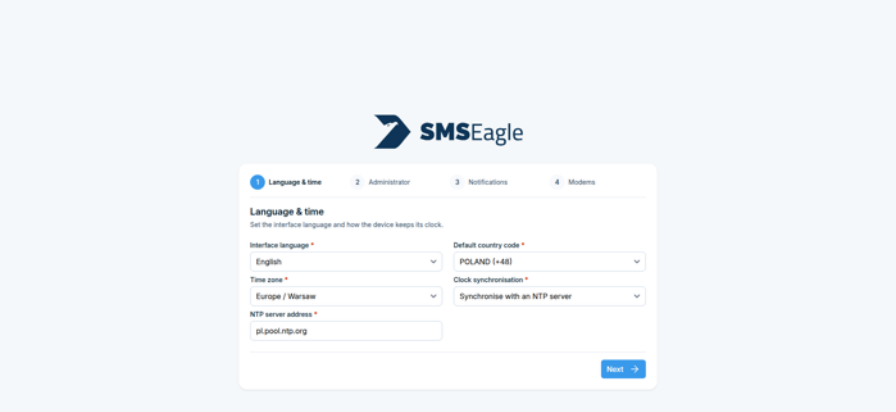
SMSEagle box contents

Your SMSEagle box contains:

- SMSEagle hardware SMS gateway
- 8x External omnidirectional antenna
- AC power cable
- Rack mounting brackets
- Quick start guide

Configuration Wizard

The first time you sign in to a freshly set-up SMSEagle device, a configuration wizard walks you through the settings needed before the gateway goes live. The wizard has four steps; you cannot access the rest of the web interface until it is completed.

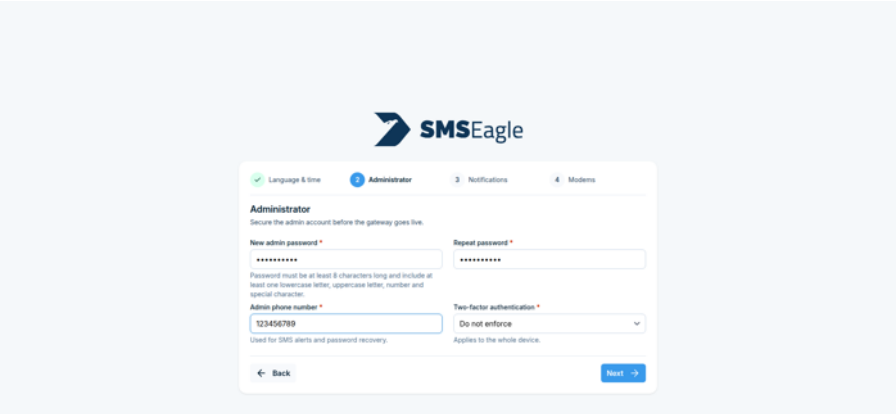


Step 1: Language & time

Step 1: Language & time

Set the interface language, the default country code (used when a phone number is entered without one), the device time zone, and clock synchronization. If you choose **Synchronise with an NTP server**, also enter the **NTP server address**.

Step 2: Administrator account



Step 2: Administrator account

Secure the admin account before the gateway goes live:

Field	Description
New admin password / Repeat password	Must be at least 8 characters long and include a lowercase letter, an uppercase letter, a number, and a special character
Admin phone number	Used for SMS alerts and password recovery
Two-factor authentication	Do not enforce, Enforce for all users, or Enforce for new users - applies to the whole device, see Multi-Factor Authentication (MFA)

Changing the admin password here signs you out; sign back in with the new password to continue the wizard.

Step 3: Notifications

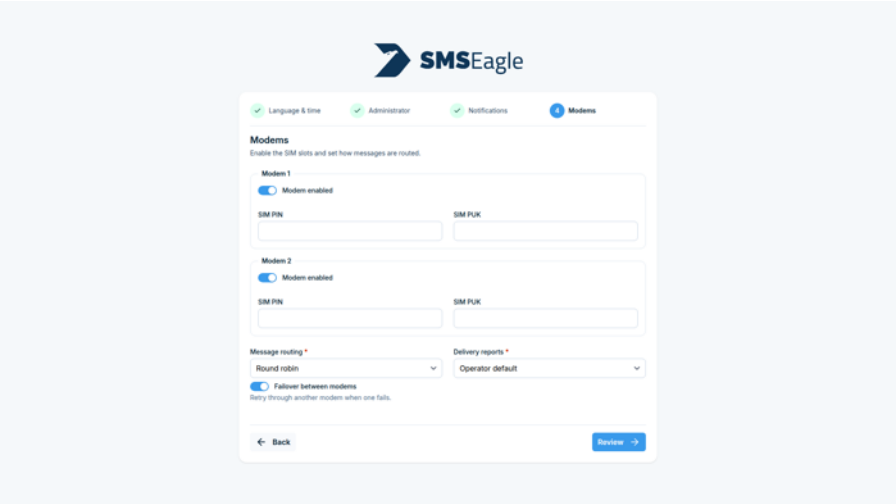


Step 3: Notifications

Choose what the device should tell you about:

- Automatically check for software updates, and optionally notify the admin by SMS when a new version is available
- Automatically check for support validity, and optionally notify the admin by SMS when support is about to expire

Step 4: Modems



Step 4: Modems

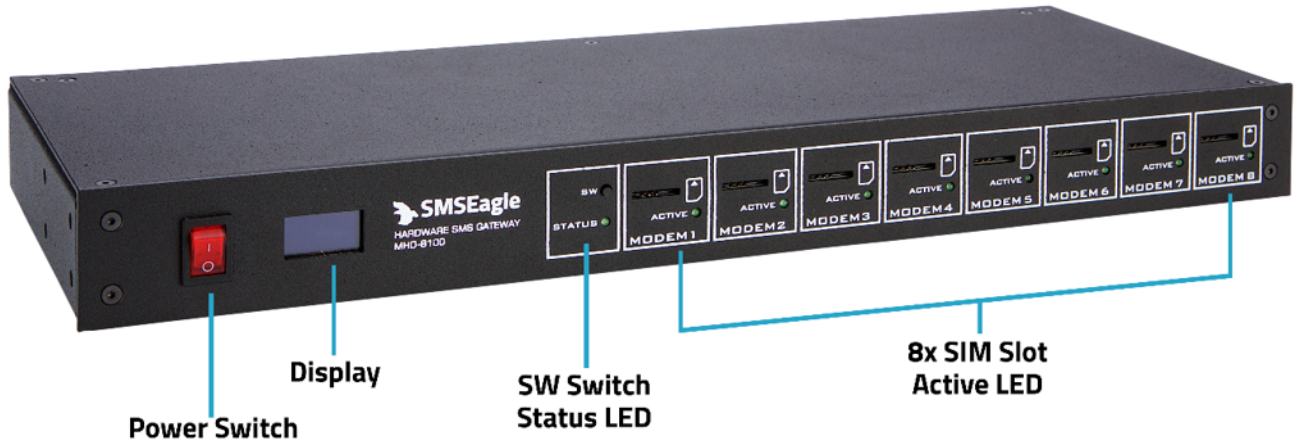
For each built-in modem (Modem 1, Modem 2 on multi-modem devices), enable it and, if required, enter its **SIM PIN** and **SIM PUK**. Then set:

- **Message routing** - Round robin, SIM 1 as master, or SIM 2 as master (see Multimodem selection strategy)
- **Delivery reports** - Operator default, Always request, or Never request
- **Failover between modems** - retry through the other modem when one fails

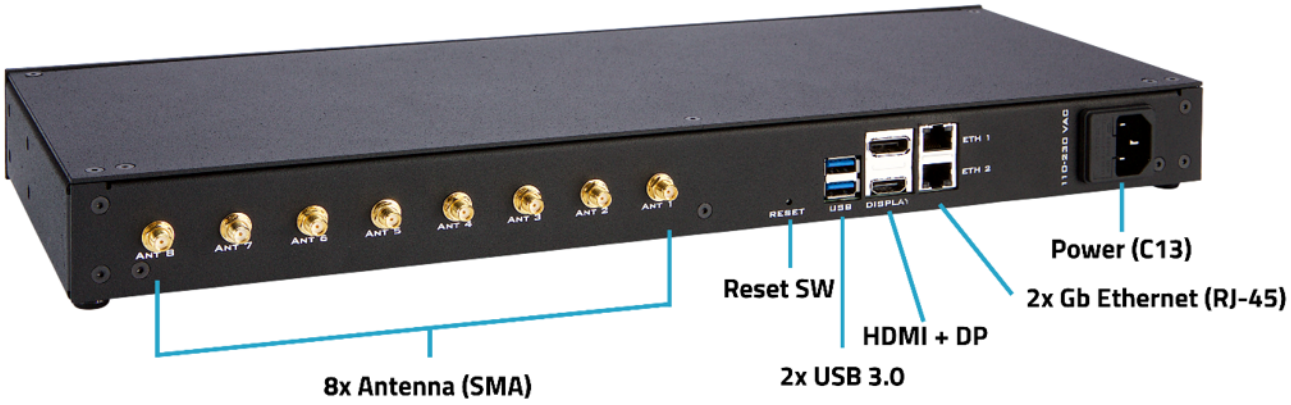
Review your settings and finish the wizard to reach the normal dashboard.

Connectors, Ports and LEDs

Front Panel



Back Panel



Front Panel

Element	Label	Description
Power switch	-	Power switch to turn on/off the device
Display	-	Display screen
User Switch	SW	Switch to toggle information on the display, restore settings to factory defaults
Status LED	STATUS	LED indicating device status
SIM slot	-	8x SIM slot - mini size
SIM Active LED	ACTIVE	8x LED indicator for modem status

Back Panel

Element	Label	Description
Antenna	ANT1-8	Antenna socket (SMA)
Reset	RESET	Switch for rebooting the device
USB	USB	2x USB 3.0 port
Display ports	DISPLAY	HDMI & Display Port (for debugging purposes only)
Ethernet ports	ETH1-2	Gigabit Ethernet RJ45 ports
Power socket	110-230VAC	Power socket

Display

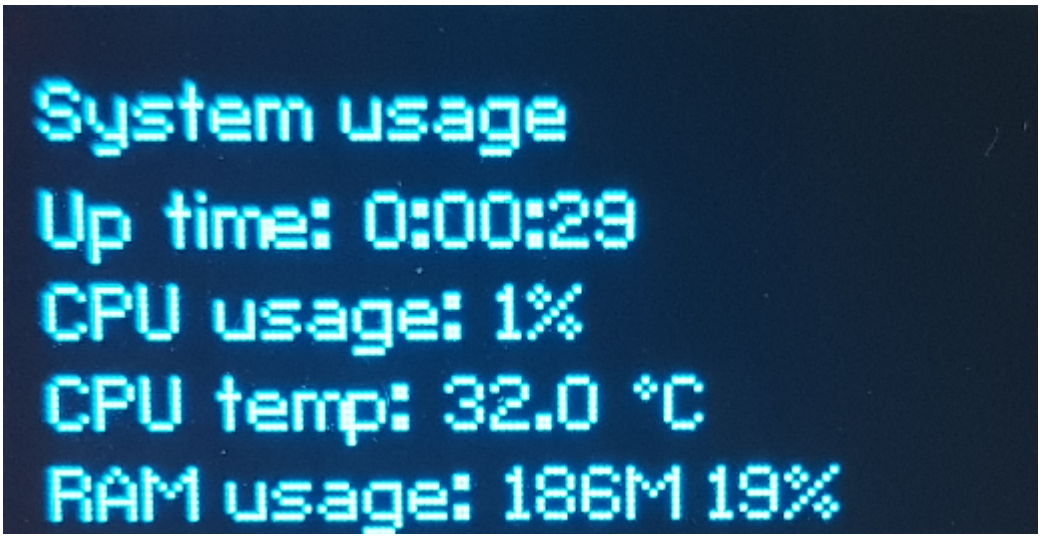
MHD-8100 has a built-in display with 5 screens, each showing different information. Press the **SW** switch to cycle through screens.

Screen 1: SMSEagle Logo

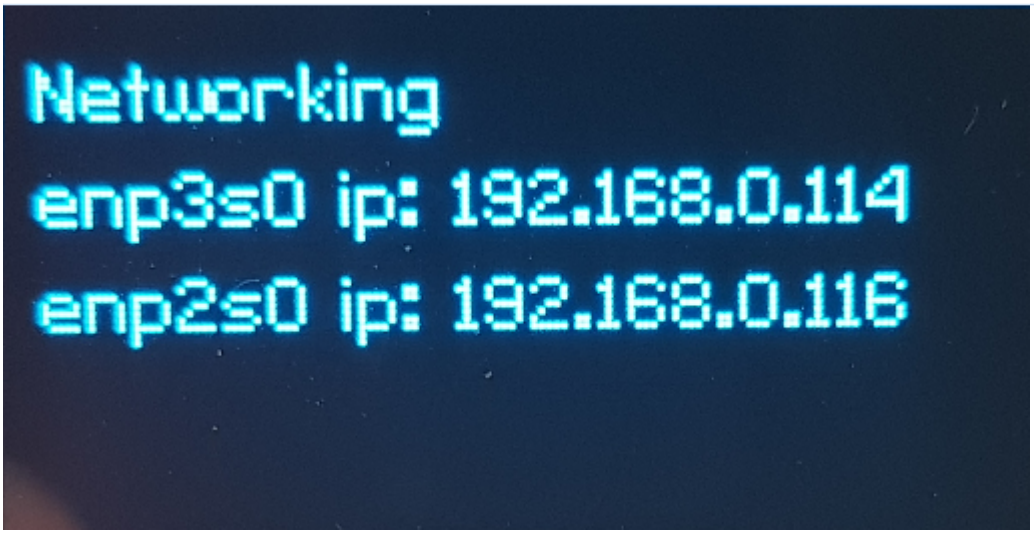


Screen 2: System Usage

1. Device power on time
2. CPU usage in %
3. CPU temperature in Celsius
4. RAM usage in MB and %

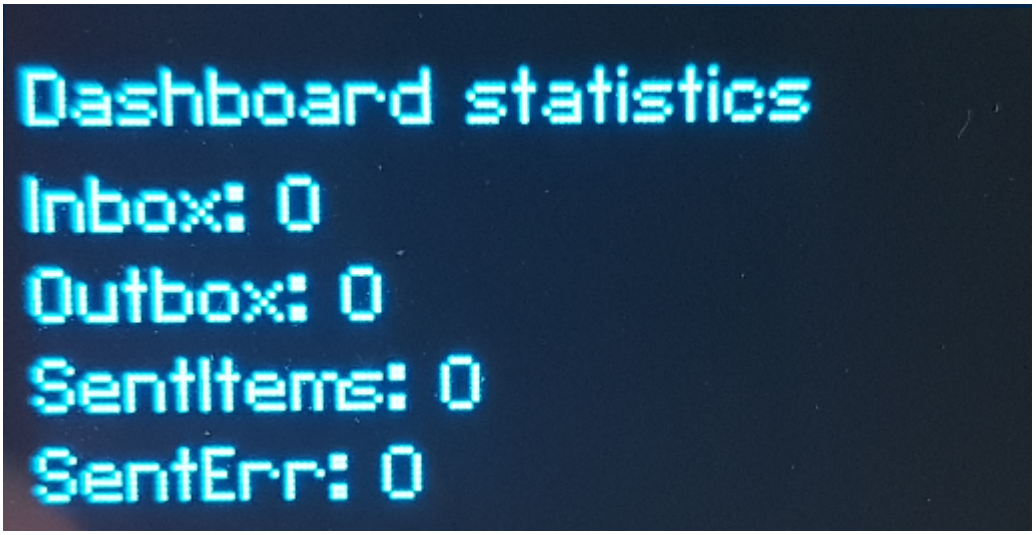


Screen 3: Networking IP list

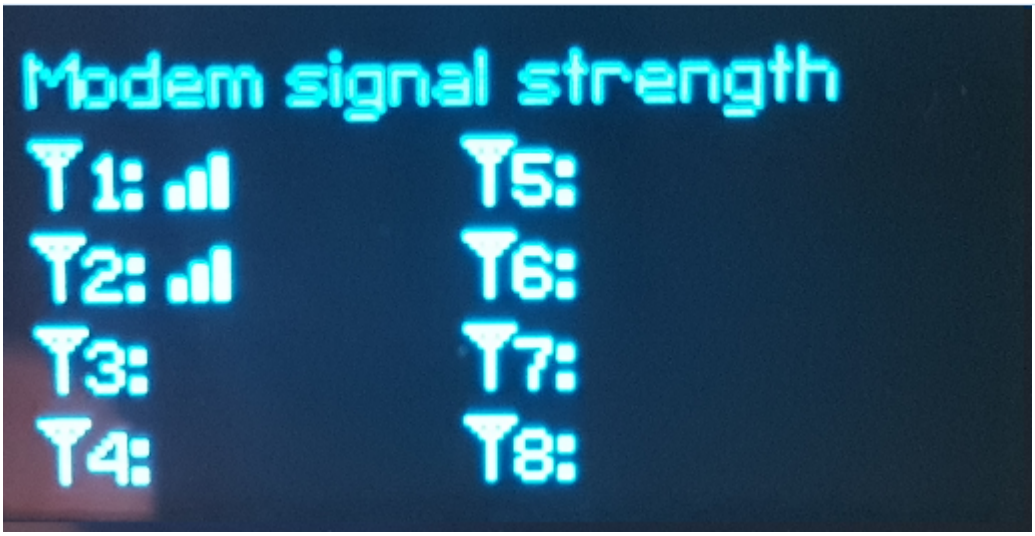


Screen 4: Dashboard Statistics - counts for:

1. Inbox
2. Outbox
3. Sent Items
4. Sent Errors



Screen 5: Modem signal strength for all 8 modems



Automatic power saving: the display turns off after 5 minutes of inactivity (no SW button press). Press the SW button to wake it up again.

Web Interface Overview

This chapter is a quick tour of the SMSEagle web interface itself, before the individual features covered in the rest of this manual.

Signing in

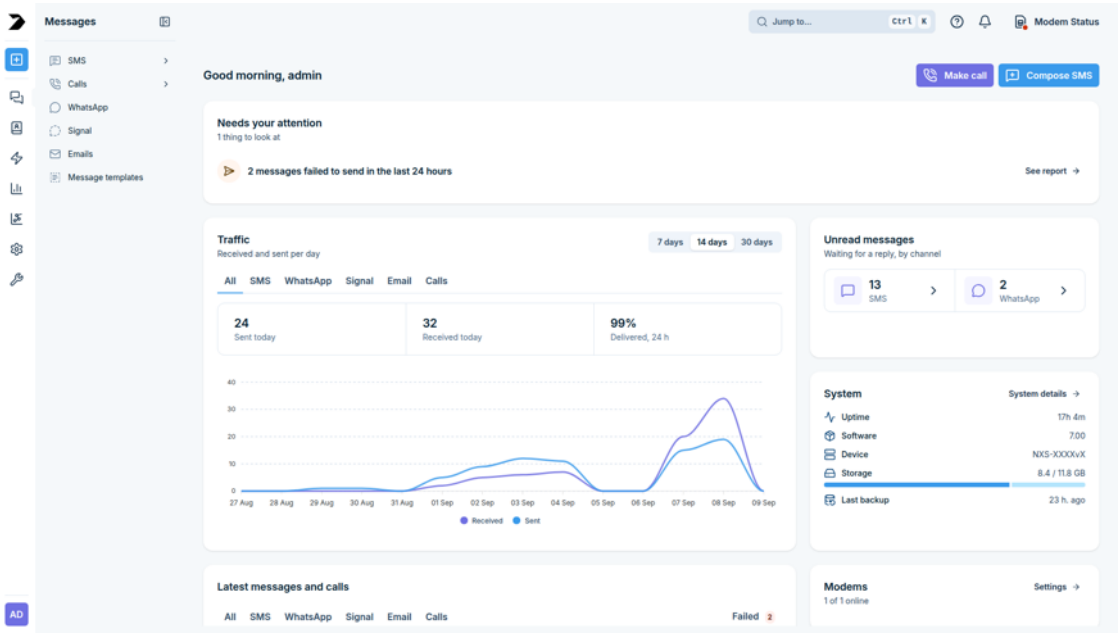


The sign-in page

Open the device's IP address or hostname in a browser and sign in with your login and password. If Multi-Factor Authentication has been enforced device-wide (see MFA), you will also be asked for a one-time code.

- **Authentication type** decides where the credentials are checked: **Local (default)** against the device's own user list, or **LDAP** against a directory server, which an administrator configures first under LDAP.
- **Forgot password?** sends recovery instructions to the phone number on the account by SMS. Identify yourself there with either your username or that phone number.
- The selector in the bottom-right corner sets the language of the sign-in page. The language of the interface after signing in comes from your own account, see Personal account settings.

Interface layout

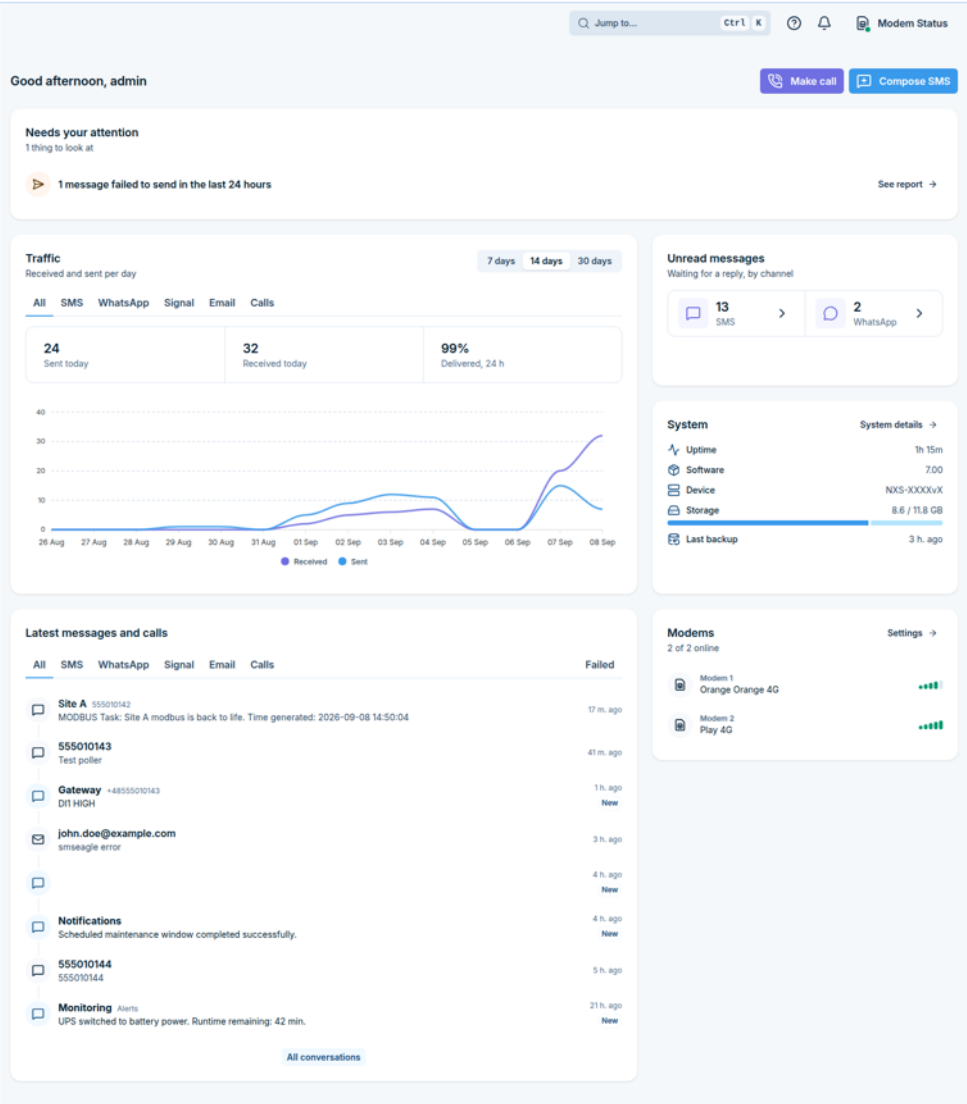


Left navigation expanded over the main content area, with the top bar above it

- **Left navigation** - an icon rail giving access to Messages, Phonebook, Automation, Reports, Monitoring, Settings, and System. Hovering an icon names the section; clicking it expands a panel listing that section's pages by name, as **Messages** is above. The button in the panel's own header closes it again.
- **Top bar** - the **Jump to...** search (`Ctrl K`) lets you jump straight to any page by name instead of navigating the menu; it also shows notifications, help, and the modem status indicator.
- **Main content area** - the page for whatever section is currently selected.

Dashboard

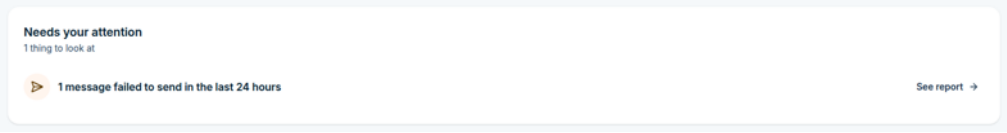
The Dashboard is the landing page after signing in. It opens with a greeting and the quick-action buttons, followed by cards that summarise what needs acting on, message traffic, unanswered conversations, device health, recent activity, and modem state.



The Dashboard

Needs your attention

Collects the items worth acting on right now, with the number of them under the card title and how many of those are critical. Each entry links to the page where you can deal with it, so a message stuck in the outbox links to the outbox folder, and a failed-delivery entry links to Reports & Statistics.



Needs your attention

Traffic

Received and sent messages per day. The tabs narrow the card to a single channel (SMS, WhatsApp, Signal, Email, or Calls), and the **7 days** / **14 days** / **30 days** buttons set the range of the chart below. Three counters sit above the chart:

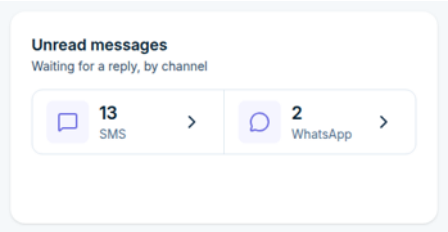
- **Sent today** - messages sent since midnight
- **Received today** - messages received since midnight
- **Delivered, 24 h** - share of the messages sent in the last 24 hours that have been confirmed as delivered



Traffic

Unread messages

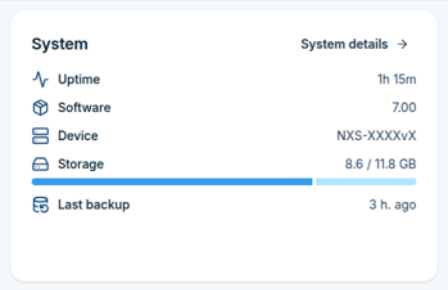
Conversations still waiting for a reply, counted per channel. Each tile opens that channel's conversation list, see Messages.



Unread messages

System

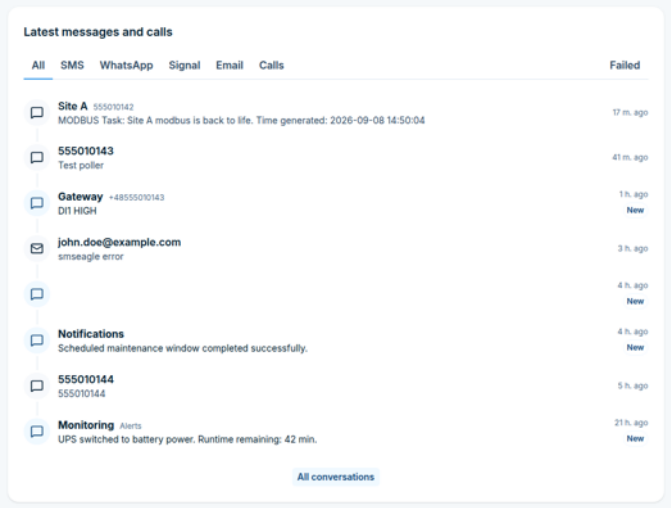
Device health at a glance: uptime, software version, device type, storage used out of total, and how long ago the last backup ran. **System details** opens the System section.



System

Latest messages and calls

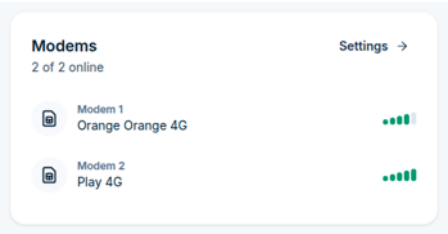
The most recent traffic across all channels, newest first, with the sender, the beginning of the message, and how long ago it arrived. The tabs limit the list to one channel, and **Failed** lists what did not go out. Anything still unread is marked **New**. **All conversations** opens the full list in Messages.



Latest messages and calls

Modems

How many modems are online out of those installed, and for each one the network it is registered to, the radio technology, and the signal strength. **Settings** opens the modem configuration, see Settings.



Modems

Quick actions

Two buttons in the top-right corner of the Dashboard.



Quick actions

Both open the same **Compose** dialog, on a different tab:

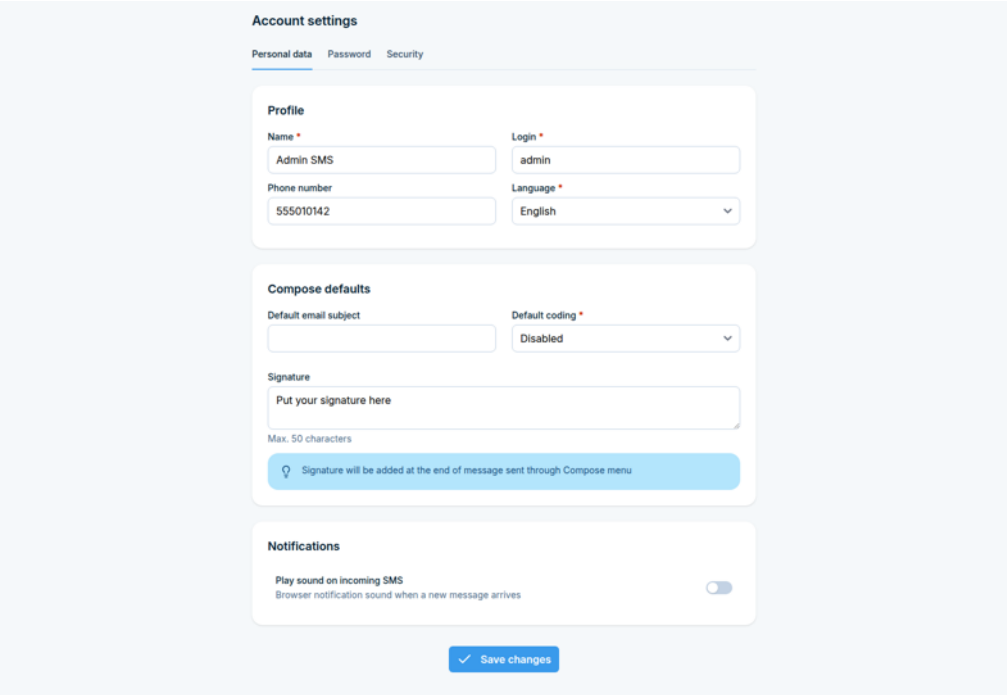
- **Compose SMS** opens it on the **Message** tab - pick the message type (SMS, Flash SMS, MMS, USSD Code, Signal, WhatsApp, Email), the recipients (from the Phonebook, typed in manually, or from a CSV file), when to send, and the message itself. A saved template can be used instead of typing the text, see Messages.
- **Make call** opens it on the **Call** tab - pick the call type (ring only, text to speech, an audio file), the recipients, and when to place the call, see Messages.

A channel that is not configured on this device is greyed out in the message type list.

Personal account settings

Click your avatar (bottom-left) and choose **Account settings** to manage your own account, under three tabs.

Personal data



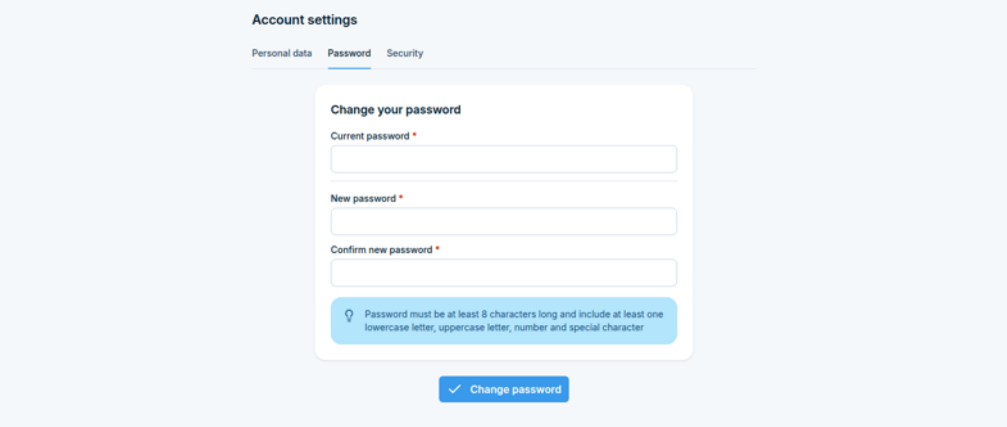
Account settings > Personal data

- **Profile** - name, login, phone number, and the interface language for your own account

- **Compose defaults** - the default email subject, the default SMS coding, and a signature of up to 50 characters, appended to messages sent from Compose
- **Notifications** - whether the browser plays a sound when a new message arrives

Save changes applies the whole tab at once.

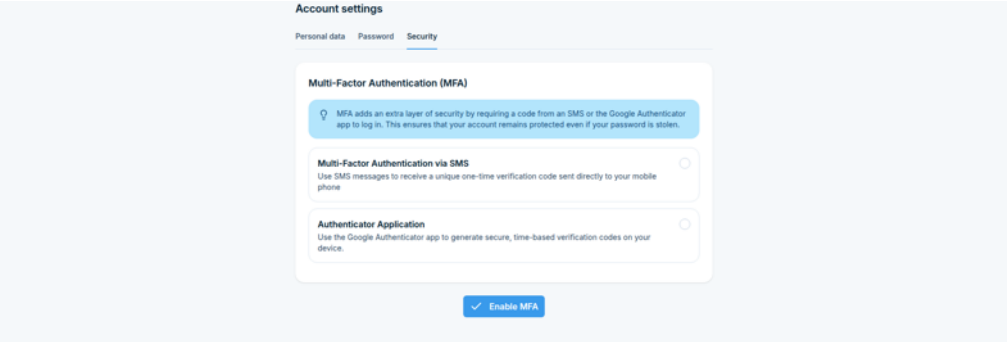
Password



Account settings > Password

Change your own password by entering the current one and the new one twice. The new password must be at least 8 characters long and contain a lowercase letter, an uppercase letter, a number, and a special character.

Security



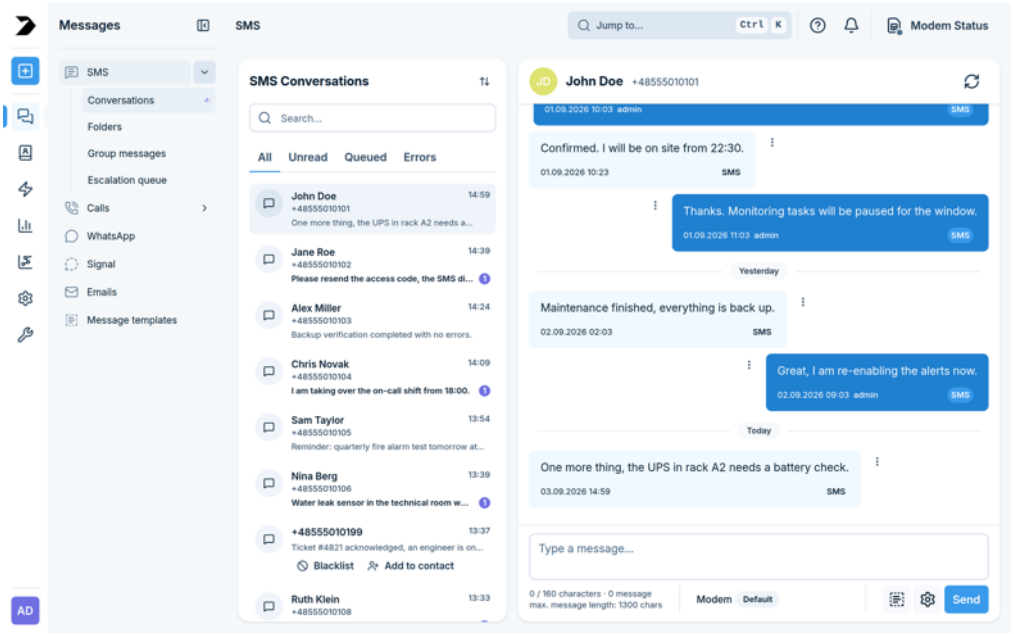
Account settings > Security

Configure your own Multi-Factor Authentication, either by SMS or with an authenticator application. The full walkthrough, including enforcing MFA device-wide, is in MFA.

Messages

This chapter covers the **Messages** section of the web interface - where you read, compose, and manage every channel's conversations. Configuring a channel (enabling WhatsApp, connecting SMTP, setting up modems) is covered separately in Settings; this chapter is about using a channel day to day.

SMS (Conversations)

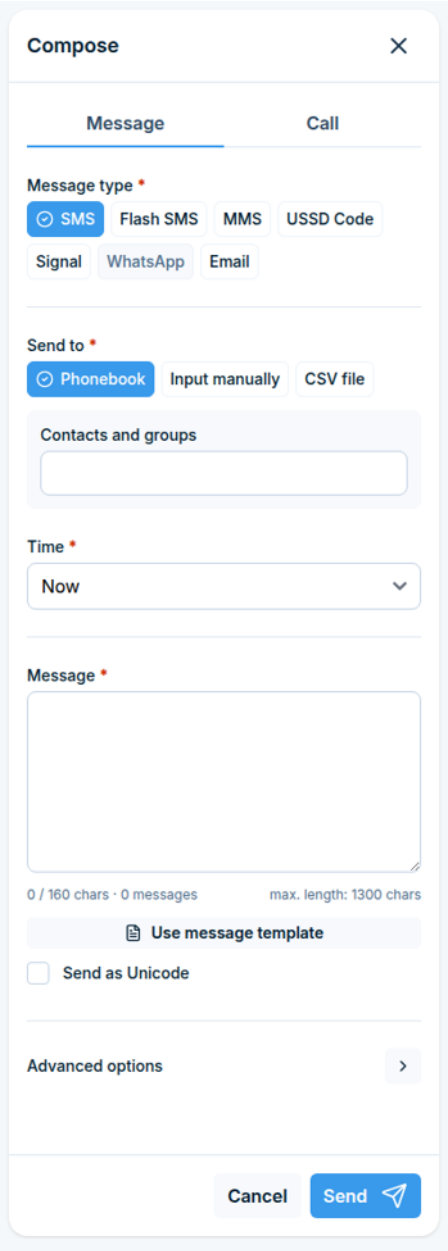


SMS Conversations, with a thread open

Messages > SMS > Conversations (`/messages/sms/`) is the main SMS/MMS inbox: one thread per phone number, newest first.

- Filter with the **All**, **Unread**, **Queued**, and **Errors** tabs.
- Open a thread to read the full history and reply from the box at the bottom.
- MMS attachments (images, files) appear inline in the thread once a modem has MMS configured - see MMS in Settings.
- Compose a new message with the **+** button at the top of the left rail, or the **Compose** quick action on the Dashboard.

Composing a message



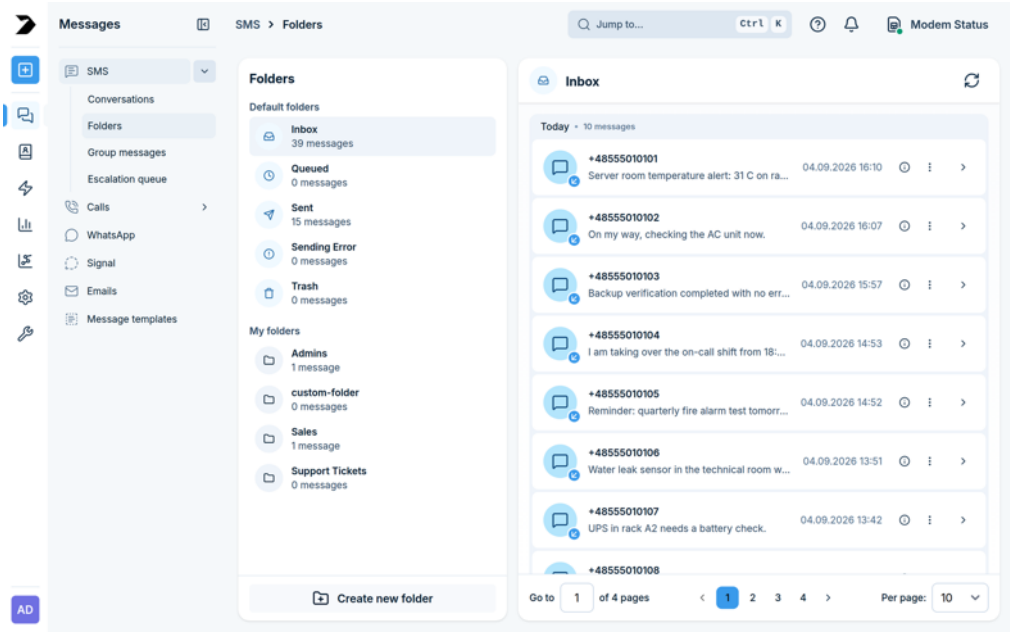
The Compose dialog

Compose opens as a panel on the right, with a **Message** and a **Call** tab. The Message tab holds:

- **Message type** - SMS, Flash SMS, MMS, USSD Code, Signal, WhatsApp, or Email. A channel that is not configured on this device is greyed out, see Settings.
- **Send to** - pick recipients from the **Phonebook** (contacts and groups), enter them with **Input manually**, or upload a **CSV file**.
- **Time** - send **Now**, **At date and time**, **After delay**, or **Between hours**.
- **Message** - the text, with a live counter of characters and of how many SMS parts they add up to. **Use message template** fills it from a saved template, and **Send as Unicode** switches the encoding for non-GSM characters.
- **Advanced options** - further per-message settings.

Send queues the message; the thread appears in Conversations straight away.

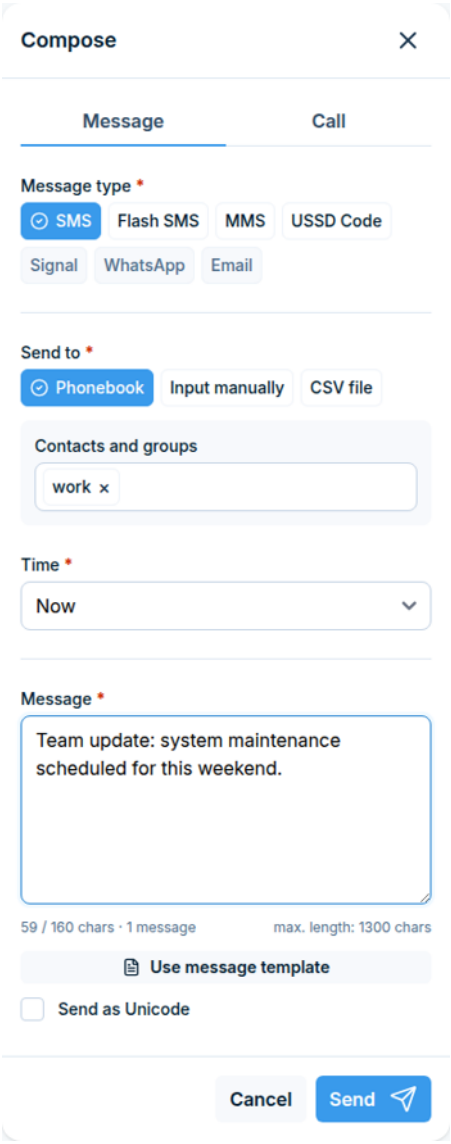
Folders



Folders

Messages > SMS > Folders (`/messages/sms/folders/`) lists the default folders (Inbox, Queued, Sent, Sending Error, Trash) alongside any custom folders you created under **My folders**. Each folder shows how many messages it holds. Click **Create new folder** to add your own - useful together with Inbox Rules to automatically sort incoming messages, and Cleanup Folders to prune them automatically.

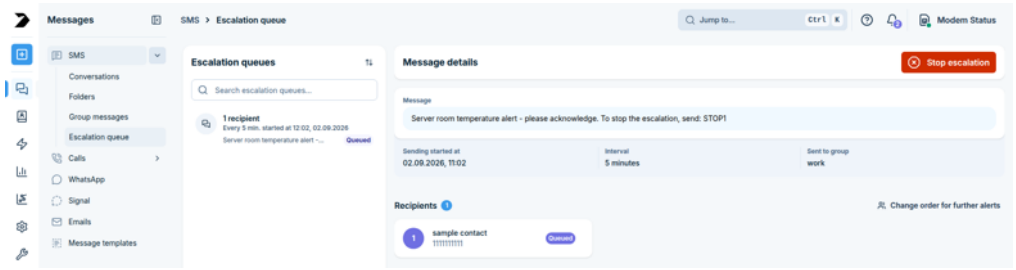
Group messages



Composing a message to a Phonebook group

Messages > SMS > Group messages (`/messages/sms/groups/`) lists conversations you started by sending to a Phonebook group rather than an individual number - one entry per group send, so you can review who a group message went to without digging through individual threads.

Escalation queue



Escalation queue

Messages > SMS > Escalation queue (`/messages/sms/escalation/`) shows every currently running escalation - a message sent to an escalation group that is still working its way down the contact list. Setting up an escalation group itself is covered in Phonebook; this page is where you watch and control one that is already in progress.

Each running escalation is listed with its message, when it started, and its interval. Opening one shows **Message details**: the message text, start time, interval, target group, and each recipient with a status of **Delivered**, **Sending**, **Queued**, or **Sending error**.

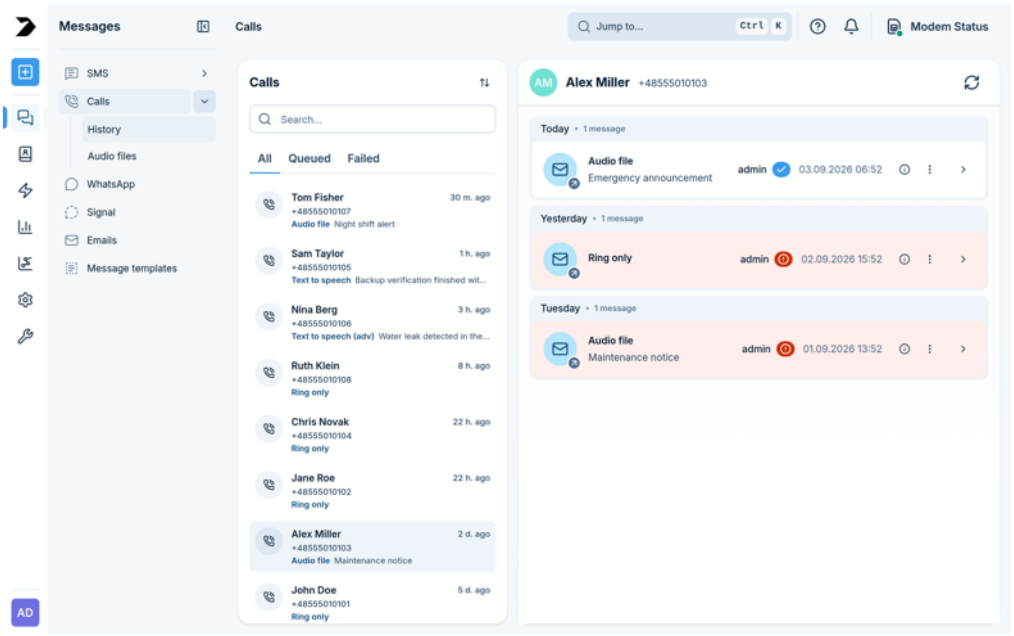
From this view you can:

- **Change order for further alerts** - reorder the people who have not been contacted yet.
- **Stop escalation** - cancel the whole escalation immediately; nobody else on the list is contacted.

An escalation also ends on its own when a recipient texts back the group's stop word, or once the last person on the list has been contacted.

Calls

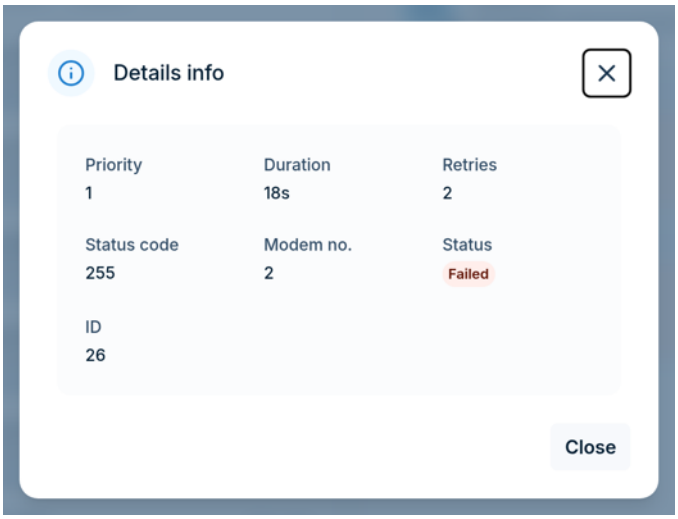
History



Calls history

Messages > Calls > History (`/messages/calls/`) lists every call the device has placed, grouped by phone number, newest first.

- The **All**, **Queued**, and **Failed** tabs narrow the list down.
- The search box finds calls by number, by contact name, or by the text that was read out.
- Opening a call shows its details: priority, duration, retries, status code, modem number, and ID. The status code is what to quote when asking support about a failed call.
- Delete a single call, or select several and delete them together.

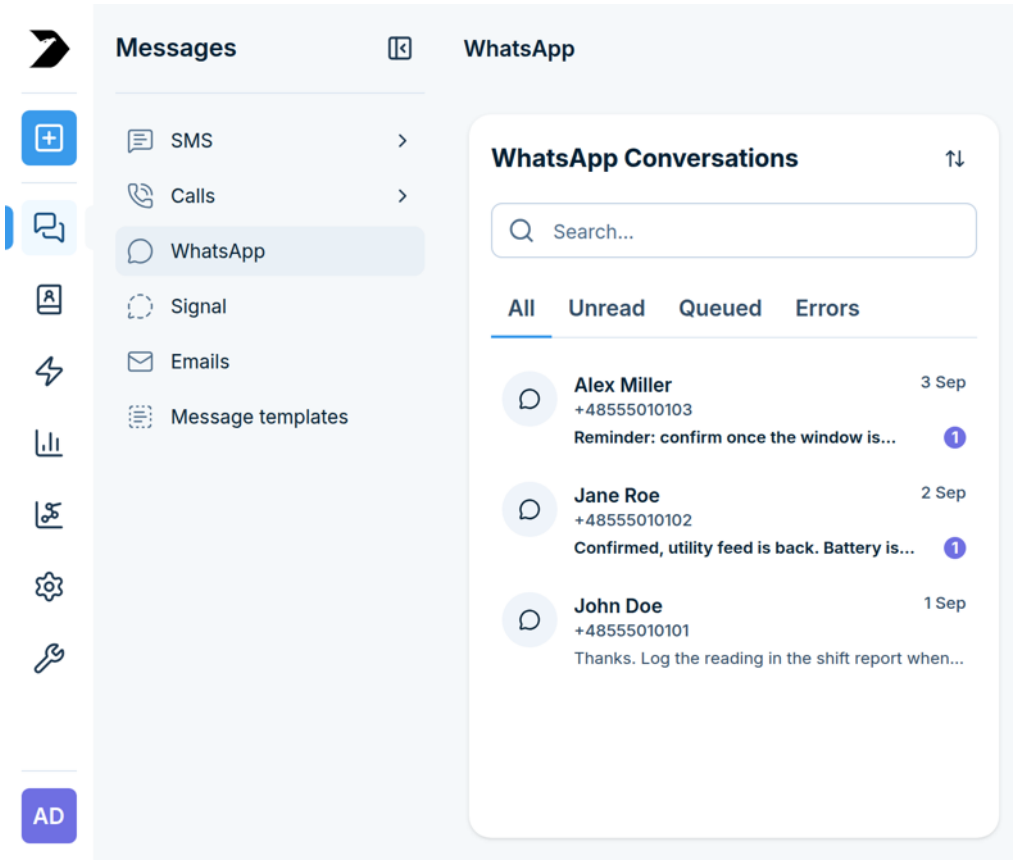


Call details

Calls are queued like messages: one scheduled for later, or held back by priority, stays in this list as **Queued** until it is placed. Placing a call (call types, voice models, and the Compose

Call panel) is covered in Calls under Settings.

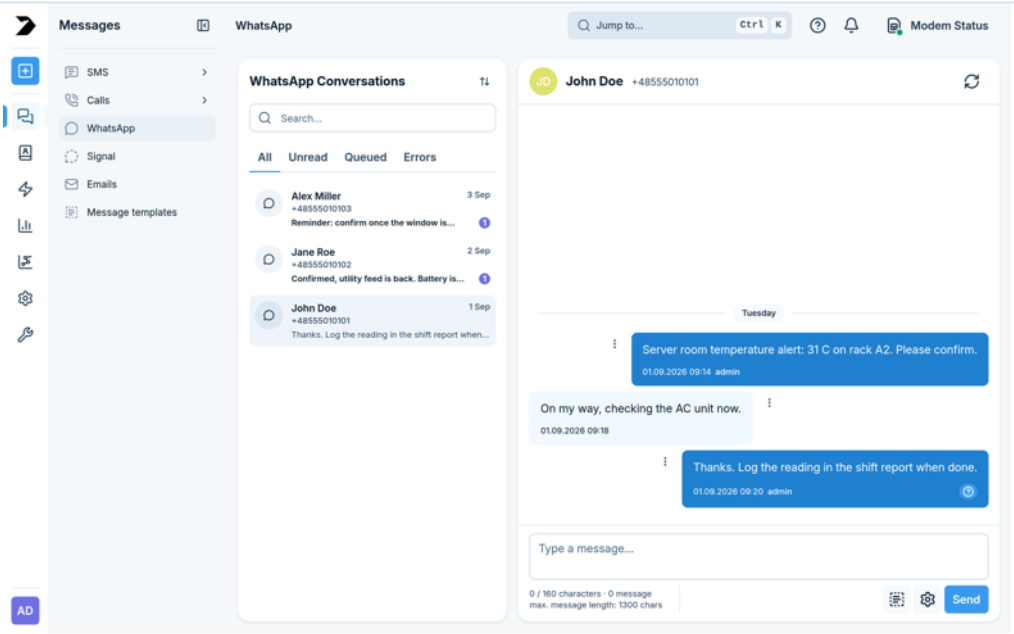
WhatsApp



WhatsApp conversations

Messages > WhatsApp (`/messages/whatsapp/`) lists WhatsApp conversations, one per number, newest first, once the channel has been linked under Settings.

- Filter with the **All**, **Unread**, **Queued**, and **Errors** tabs.
- Search and sort conversations by date or phone number.
- Open a conversation and reply directly from the box at the bottom (maximum 1300 characters).
- Delete a single conversation, or select several and delete them together.

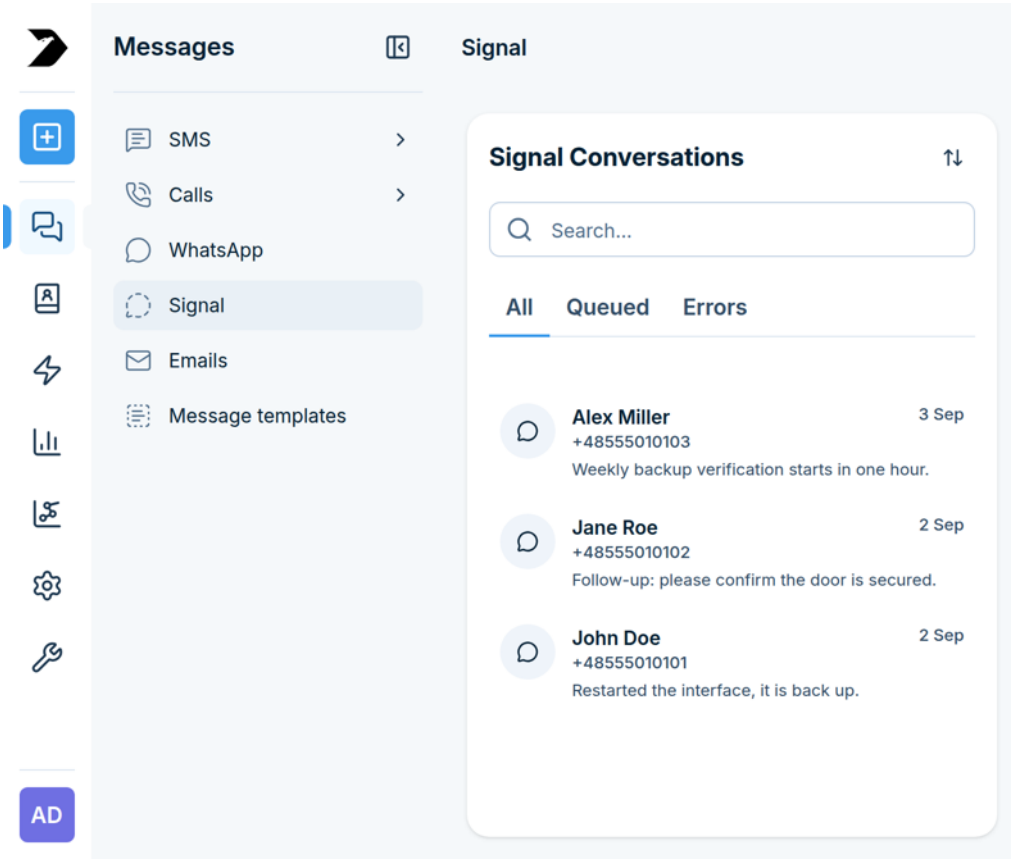


An open WhatsApp conversation

If WhatsApp has not been configured yet, this page shows a notice with a button that takes you straight to the WhatsApp settings. To send a new WhatsApp message, open **Compose**, tick **WhatsApp** as the message type, and write as usual.

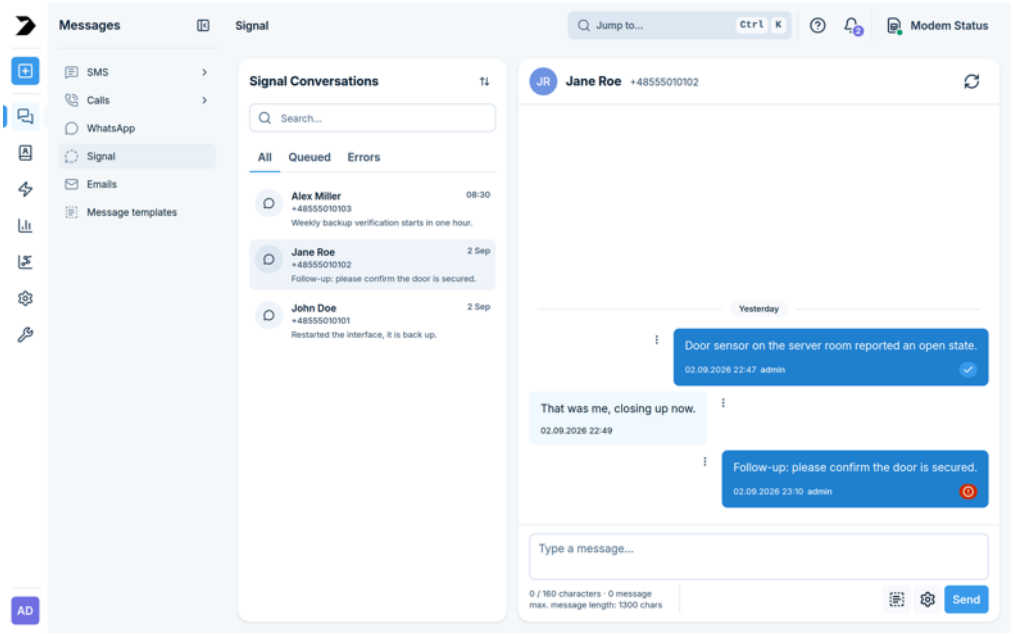
Only messages received after the device was linked appear here.

Signal



Signal conversations

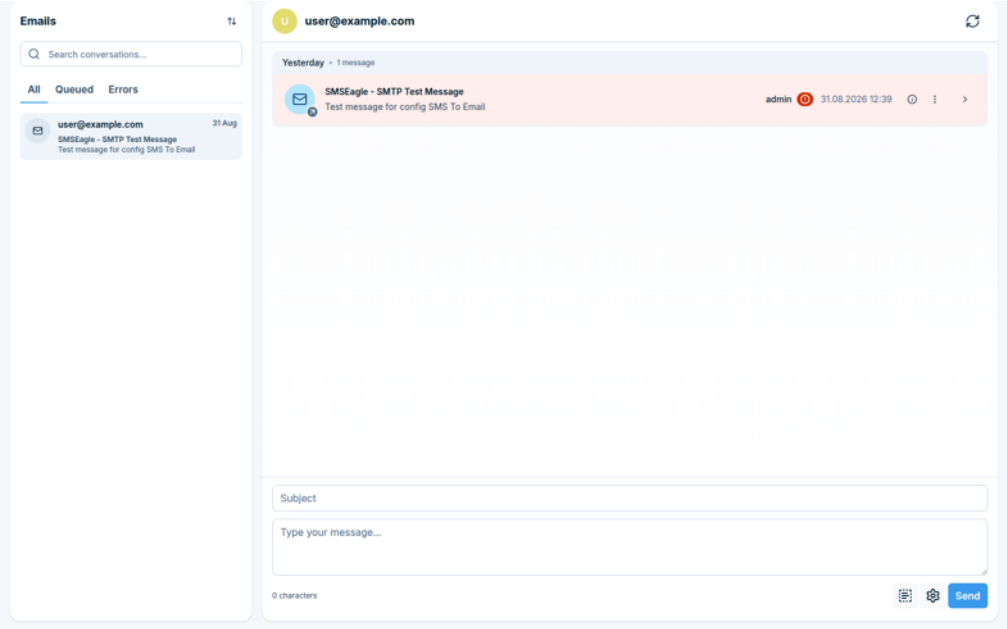
Messages > Signal (`/messages/signal/`) works the same way as WhatsApp above, once a number has been registered under Settings: one conversation per number, the **All / Queued / Errors** filters, and reply from the box at the bottom (maximum 1300 characters). Signal has no **Unread** tab.



An open Signal conversation

To send a new Signal message, open **Compose**, tick **Signal** as the message type, and write as usual. Only messages received after the service was enabled appear here.

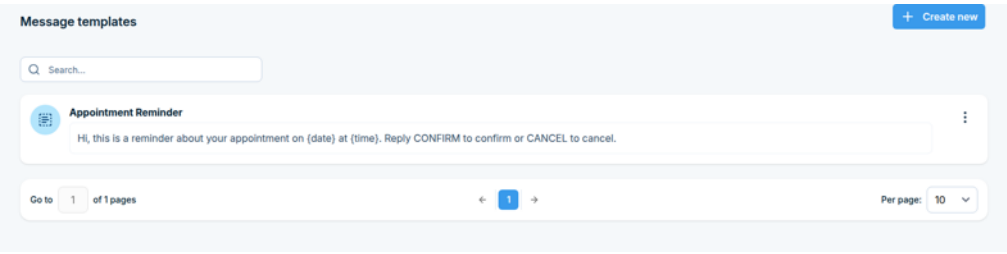
Emails



Emails conversations

Messages > Emails (`/messages/email/`) lists email conversations, one thread per address, newest first, with **All**, **Queued**, and **Errors** filters - the same conversation-style view as SMS, WhatsApp, and Signal, for mail sent or received through SMS to Email and Email to SMS.

Message templates



Message templates

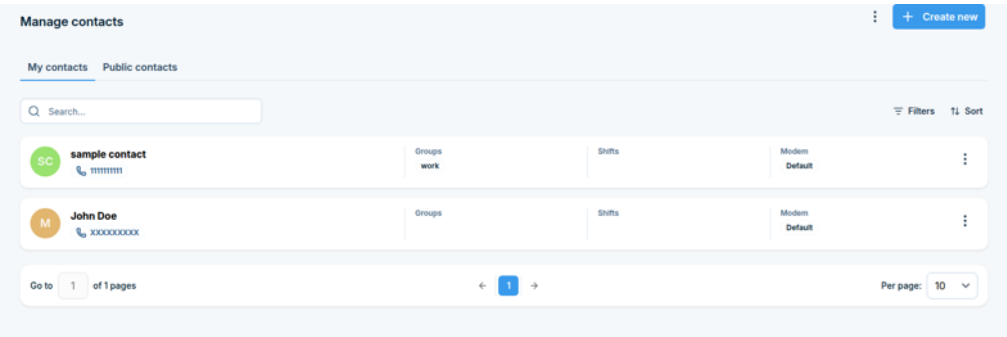
Messages > Message templates (`/messages/templates/`) stores reusable message text for Compose, so frequent messages don't need retyping every time.

Click **Create new**, give the template a **Template name**, and write the **Message content**. Saved templates can then be picked from Compose instead of typing the message from scratch.

Phonebook

The Phonebook is where you keep the contacts and groups you send messages to or receive messages from.

Contacts



Phonebook contacts list

Phonebook > Contacts (`/phonebook/contacts`). Click **Create new** to add a contact. The contacts list is split into two tabs:

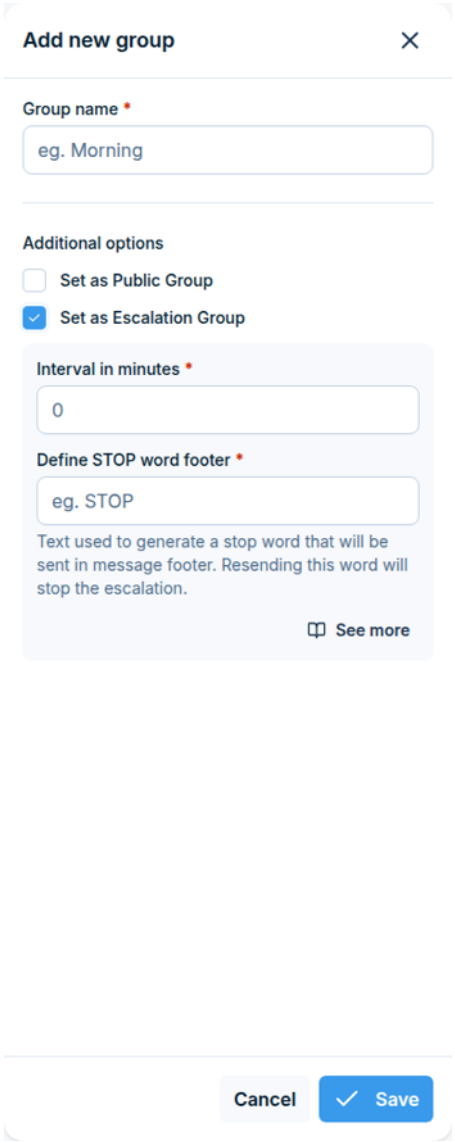
- **My contacts** - contacts only you can see and use.
- **Public contacts** - contacts shared with other users of the device (needed, for example, so a public contact can be addressed by name from Email to SMS).

Each contact can belong to one or more **Groups**, be assigned a **Shift** (see Shifts below), and be pinned to a specific **Modem** for outgoing messages. Use **Filters** and **Sort** to find a contact in a large phonebook.

Groups

Phonebook > Groups (`/phonebook/groups`). Groups let you address a whole set of contacts at once (for example from Compose SMS, or as the target of an automation rule) instead of picking each contact individually. Click **Add new**, give the group a **Name**, and tick **Set as Public Group** if other users, automation rules, or the API should be able to send to it.

Escalation groups



Escalation group options in the “Add new group” dialog

An escalation group alerts people **one after another, not all at once**, until somebody confirms they are handling the problem - put your on-call people into a group in a chosen order, set an interval, and when you send a message to the group the first person gets it immediately, the second gets it if nobody stops the escalation, and so on down the list. Watching and controlling a running escalation happens in Escalation queue under Messages; this section is where you set one up.

Step 1: Create the escalation group

1. Click **Add new**. A side panel opens.
2. Fill in **Name**, for example `Night on-call`.
3. Tick **Escalation group**. Two extra fields appear.
4. Fill in **Escalation interval (minutes)**: how long to wait before alerting the next person. Allowed values are 1 to 999.

5. Fill in **Escalation stop word**: the word recipients text back to stop the escalation.
    - Maximum 8 characters.
    - Letters only, no digits, spaces, or punctuation.
    - It must be unique - each escalation group needs its own stop word.
6. Click **Save**.

> Tick **Set as Public Group** as well if other users of the device, automation rules, or the API should be able to send to this group.

Step 2: Add people and set their order

1. On the **Groups** page, find your escalation group and open **Manage contacts**.
2. Add the contacts who should be alerted.
3. Put them in the right order by **dragging the cards** up and down. The person at the top is contacted first - this is exactly the order in which alerts are sent.

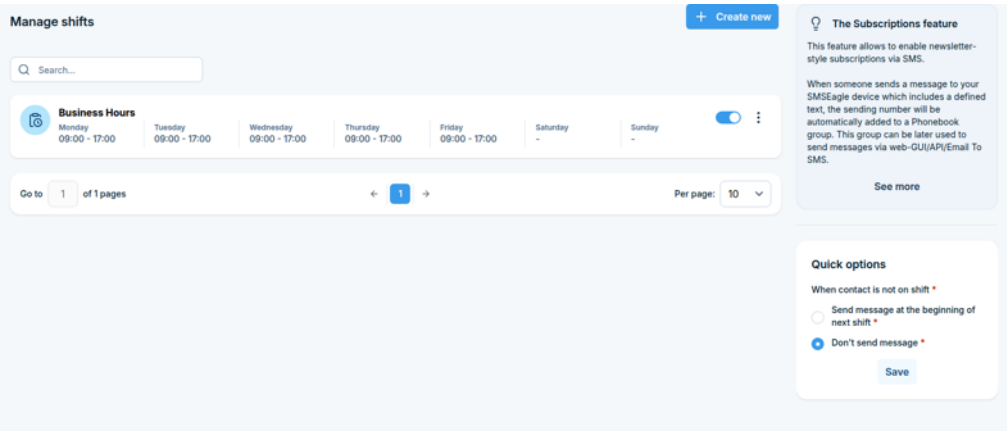
Step 3: Trigger an escalation

Send a message to the group the same way you send any other message, from **Compose**. SMSEagle then appends a line telling the recipient what to text back to stop the escalation (in the form `To stop the escalation, send: <stop word><number>`), sends the message to the first contact right away, and schedules the same message for the next contacts, spaced out by the interval you set.

> **Tell your recipients exactly what to reply.** The number after the stop word identifies this particular escalation, so the reply must contain the whole thing, for example `ACK17`, matching exactly - the stop word **and** the number joined with no space, the same upper and lower case, and nothing else in the message. Only somebody who is a member of the escalation group can stop it; a reply from an unrelated number is ignored.

You can also trigger an escalation group from the API, from Email to SMS, or from any automation rule that sends to a group.

Shifts



Shift management overview

Shifts describe **when a person is on duty**. Once you assign a shift to a contact, SMSEagle checks the shift before sending them a message: if a message is addressed to a contact who is currently outside their shift hours, SMSEagle either holds the message and delivers it at the start of their next shift, or does not send it at all - you choose which (see Step 4 below).

Typical use: an on-call rota, where the night shift should not be woken up by alerts meant for the day shift.

> **Good to know:** a contact with **no shift assigned** is always considered available. Shifts only restrict the contacts you assign them to.

Before you start

- You need at least one contact in the Phonebook (**Phonebook > Contacts**).
- Make sure the device clock and time zone are correct, because shift hours are compared against the device time. Check this in **Settings > Date/Time**.

Step 1: Open the Shifts page

Phonebook > Shifts (`/phonebook/shifts`) lists the shifts you have already created, with a **Quick options** box on the right.

Step 2: Create a shift

1. Click **Create new** in the top right corner. A side panel opens.
2. Fill in **Name**, for example `Night shift` or `Weekend duty`.
3. Leave **Enabled** ticked so the shift starts working right away. Untick it to prepare the shift now and activate it later.
4. Under **Active from - to**, set the hours for each day of the week: enter a **From** and a **To** time for every day the person is on duty, and leave a day empty if they are not.
5. Click **Save**.

Rules for shift hours

- **From** must be earlier than **To** on the same day.
- Both **From** and **To** must be filled in, or both left empty. A half-filled day is rejected with an error message.
- At least one day must have hours set.

> **Overnight shifts:** a shift that crosses midnight (for example 22:00 to 06:00) has to be entered as two entries: `22:00 - 23:59` on the first day and `00:00 - 06:00` on the next day.

Step 3: Assign contacts to the shift

You can do this from either side.

From the shift: on the **Shifts** page, find your shift, open its actions, and choose **Manage contacts**.

From the contact: go to **Phonebook > Contacts**, select one or more contacts using their checkboxes, choose **Edit shifts**, pick the shifts to assign, and click **Assign shifts**.

Step 4: Choose what happens outside shift hours

The **Quick options** box on the right of the Shifts page holds **When contact is not on shift**:

Option	Result
Send message at the beginning of next shift	The message waits in the queue and is delivered automatically when the contact's next shift starts.
Don't send message	The message is not sent to that contact. It is recorded as not delivered.

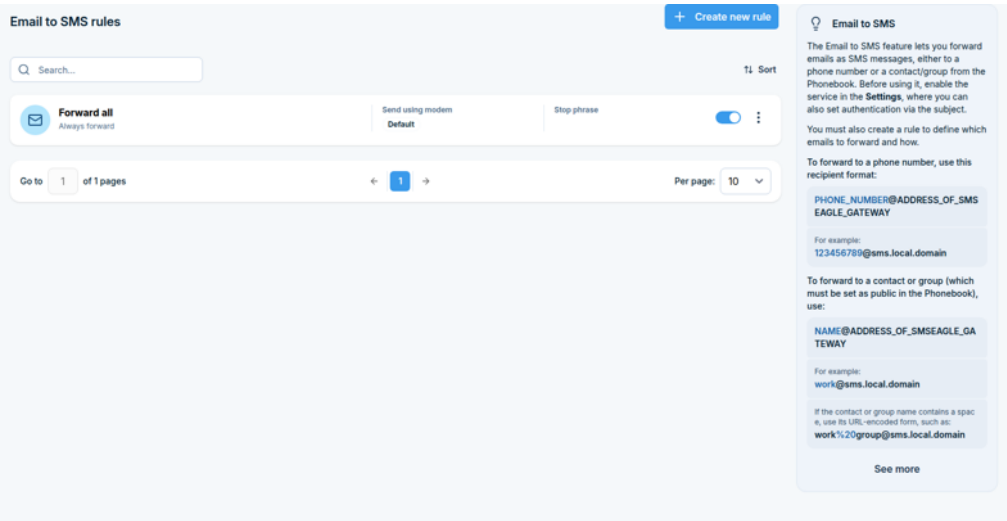
Pick the option you want and click **Save**.

> This setting is **global**. It applies to every shift and every contact on the device, not just the shift you are currently looking at.

Automation

This chapter covers the **Automation** section of the web interface, in the same order the rules appear there.

Email to SMS



Email to SMS rules

The Email to SMS feature lets you forward incoming emails as SMS messages, either to a phone number or to a contact/group from your Phonebook.

Where to find it

The feature is split across two places in the WebGUI:

- **Automation > Email > Email to SMS** (`/automation/email-to-sms`) is where you create and manage forwarding rules.
- **Settings > Channels > Email > Email to SMS** (`/settings/email/email-to-sms`) is where you enable the service and configure how emails are converted to messages - see Email to SMS in Settings.

Step 1: Understand the recipient address format

Emails must be sent to a specially formatted address so SMSEagle knows where to deliver the message.

To forward to a phone number:

```
PHONE_NUMBER@ADDRESS_OF_SMSEAGLE_GATEWAY
```

For example: `999888777@gateway.smseagle.eu`

To forward to a contact or group from the Phonebook (the contact or group must be set as **public**):

```
NAME@ADDRESS_OF_SMSEAGLE_GATEWAY
```

For example: `work@gateway.smseagle.eu`

If the contact or group name contains a space, use its URL-encoded form: `work%20group@gateway.smseagle.eu`

Instead of the gateway IP address you can use a Fully Qualified Domain Name, set under **Settings > Channels > Email > Email to SMS > Advanced settings > FQDN hostname**. If **Use LDAP contacts** is enabled there, the same `NAME@GATEWAY` format also resolves contacts and groups defined in LDAP / Active Directory.

By default the body of the email becomes the text of the SMS. This depends on the **What to do with email subject** setting in Settings: the subject can be ignored, prepended to the message text, used for authentication, or sent instead of the body.

Step 2: Create a new rule

Go to **Automation > Email > Email to SMS** and click **Create new rule**. A panel titled Add Email to SMS rule opens on the right.

Field	Description
Rule name *	A name to identify the rule (required, max 100 characters)
Forward for *	Always send forwards every incoming email that matches the address format. Specified sender / message contains adds filtering conditions, see Step 3.
Send using modem	Which modem sends the SMS. Default is Default. Shown only on devices with more than one modem.
Stop phrase	Text starting from this phrase will be removed from the message (case sensitive)
Priority	Sending priority from 0 to 5. Messages with higher priority are processed first.
Call after sending SMS	No, Ring only, Yes - text to speech, or Yes - text to speech (advanced). The available options depend on the voice and TTS capabilities of your device.
Voice model	Voice used for the text-to-speech call. Shown only for devices supporting advanced TTS, and only after selecting Yes - text to speech (advanced).
Force converting to UTF-8	Forces conversion of the message text to UTF-8
Remove conversation history	Strips quoted history of the email conversation from the message text

Click **Save** to create the rule, or **Cancel** to discard it.

Step 3: Add filtering conditions (optional)

If you select **Specified sender / message contains** under Forward for, three independent conditions become available, each with its own checkbox and text field:

- **When incoming email address contains** filters by the sender's email address
- **When incoming messages subject contains** filters by the email subject line
- **When incoming message content contains** filters by the email body text

The **Case sensitive** switch applies to all enabled conditions.

You may enable one, two, or all three conditions. The rule triggers only when **all** enabled conditions are met.

Step 4: Manage existing rules

Each rule appears as a card in the Email to SMS list, showing:

- the rule name

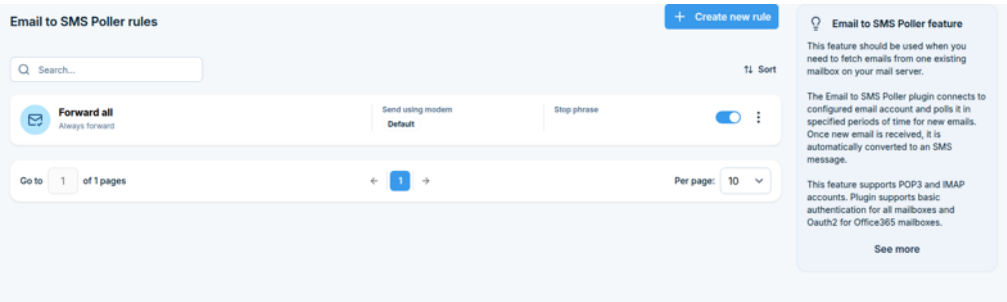
- the forwarding condition, for example Forward when incoming: email address contains: ..., or Always forward when no condition is set
- the modem used to send
- the configured stop phrase
- an on/off toggle to enable or disable the rule without deleting it
- a ⋮ menu with **Edit** and **Delete**

Additional controls on the list:

- **Search** filters rules by name.
- Selecting rule checkboxes reveals bulk actions: **Enable / Disable** and **Delete**.
- The pagination controls at the bottom let you jump to a page and change how many rules are shown per page.

The right-hand help panel explains the recipient address formats, with a **See more** button linking to the feature page on smseagle.eu.

Email to SMS Poller



Email to SMS Poller rules

Email to SMS Poller periodically checks an external mailbox over POP3, IMAP, or IMAP with OAuth2 (Microsoft 365 / Outlook), and converts the emails it finds there into SMS messages according to the Email to SMS Poller rules. Unlike Email to SMS (which runs its own mail server and receives mail actively), the Poller reaches out to an existing mailbox you already have.

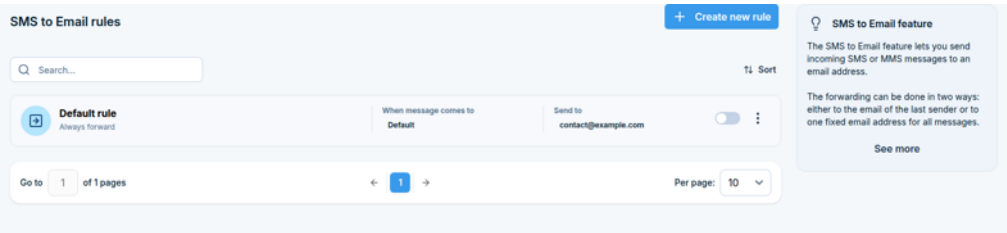
Where to find it

Automation > Email > Email to SMS Poller (`/automation/email-to-sms-poller/`) is where you create and manage rules. Enabling the service and connecting the mailbox (POP3, IMAP, or IMAP + OAuth2 for Microsoft 365) happens under Email to SMS Poller in Settings.

Creating a rule

Click **Create new rule**. Rules here work the same way as Email to SMS rules - name the rule, choose whether it forwards every polled email or only ones matching sender/subject/ content conditions, and set the same per-rule options (modem, stop phrase, priority, call after sending).

SMS to Email



SMS to Email rules

What this feature does

SMS to Email forwards **incoming** SMS and MMS messages to an email address, so you can read them in your mailbox instead of logging in to SMSEagle.

You create rules that decide which messages get forwarded and where they go. A rule can forward everything, or only messages from certain senders, or only messages containing a certain phrase.

Typical uses: forwarding replies from field staff to a shared support mailbox, or archiving alert confirmations into a ticketing system's email inbox.

Before you start

SMSEagle needs a working mail server configuration to send the emails. Go to **Settings > Channels > Email > SMTP Configuration** and make sure it is filled in and tested - see SMTP Configuration. Without it, rules will match but no email will arrive.

If you want to forward based on sender contacts or groups, those contacts and groups must be marked as **Public** in the Phonebook.

Step 1: Open the SMS to Email page

In the sidebar, go to **Automation > Email > SMS to Email**.

Step 2: Create a rule

Click **Create new rule** in the top right corner. A side panel opens.

Name the rule

In **Rule name**, type something descriptive, for example `Forward all to support`. Maximum 100 characters.

Decide which messages to forward

Choose **Forward for**:

Option	What it means
Always forward	Every incoming SMS and MMS is forwarded.
Specified sender / message	Only messages matching the conditions you set below are forwarded.

If you chose **Specified sender / message**, two conditions become available. You can use one or both. When you use both, a message must satisfy **both** to be forwarded.

When incoming SMS comes from Tick this and select the contacts or groups whose messages should be forwarded. Start typing to search. Only **public** contacts and groups can be selected here.

When incoming SMS text contains Tick this and type the phrase to look for, for example `URGENT`. The phrase can appear anywhere in the message text. Tick **Case sensitive** if `urgent` and `URGENT` should be treated as different.

Limit the rule to one modem (multi-modem devices only)

If your device has more than one modem, a **When message comes to** field appears. Leave it on **Any modem**, or pick a specific modem so the rule only applies to messages arriving on that SIM card. On single-modem devices this field is not shown.

Choose the destination email address

Choose **Type of email forwarding**:

Option	What it means
To fixed email address	Every matching message goes to the one address you enter in **Forward to email address**.
To email of last sending user	The message goes back to the email address of the person who last sent an SMS to that phone number through SMSEagle. This closes the loop on an email-to-SMS conversation. Enter a **Default email address** as a fallback, used when there is no last sender on record.

Set the email subject

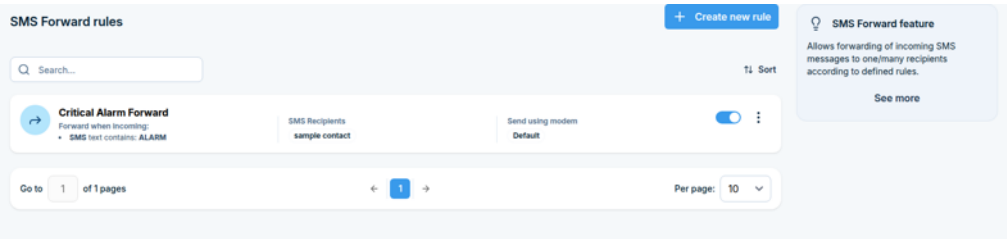
Email subject controls the subject line of the forwarded email. You can use placeholders, which are replaced with real values when the email is sent:

Placeholder	Replaced with
`{SENDER}`	The phone number the SMS came from
`{WORDS,X}`	The first X words of the message text
`{CHARS,X}`	The first X characters of the message text

Example: `SMS from {SENDER}: {WORDS,5}` produces a subject like `SMS from +48111222333: Server room temperature alarm triggered`. Maximum 150 characters.

Click **Save**. The rule starts working immediately on newly received messages.

SMS Forward



Add forwarding rule dialog

What this feature does

SMS Forward passes **incoming SMS messages on to other people**. When a message arrives, SMSEagle sends it out again to the recipients you choose.

You can forward the message exactly as it came in, or replace it with your own text. You can also add a voice call on top of the forwarded SMS, so an alert cannot be slept through.

Typical uses: sending alarm messages from a machine to the whole on-call team, passing messages from a shared number to the person currently on duty, or turning a short machine code into a readable sentence for the team.

Before you start

- The contacts and groups you forward **to** must exist in the Phonebook. Contacts and groups used as forwarding recipients or as sender conditions have to be marked as **Public**.
- Decide whether the recipients need the original wording or a rewritten message.

Step 1: Open the SMS Forward page

In the sidebar, go to **Automation > SMS > SMS Forward**.

Step 2: Create a rule

Click **Create new rule** in the top right corner. A side panel opens.

Name the rule and set its priority

Rule name Something descriptive, for example `Alarms to on-call team`. Maximum 100 characters.

Priority A number from 0 to 9. Messages produced by a higher-priority rule are queued for sending earlier than messages from a lower-priority rule. Leave it at the default unless you have urgent rules that must overtake bulk ones.

Decide which messages to forward

Choose **Forward for**:

Option	What it means
All incoming messages	Every incoming SMS is forwarded.
Specified sender / message	Only messages matching the conditions you set below are forwarded.

If you chose **Specified sender / message**, two conditions become available. You can use one or both. When you use both, a message must satisfy **both** to be forwarded.

When incoming SMS comes from Tick this and select the sender contacts or groups in **Sender contacts**. Only **public** contacts and groups can be selected here.

When incoming SMS text contains Tick this and type the phrase in **Text fragment**, for example `ALARM`. The phrase can appear anywhere in the message. Tick **Case sensitive** if `alarm` and `ALARM` should be treated as different.

Limit the rule to one modem (multi-modem devices only)

If your device has more than one modem, a **When messages comes to** field appears. Leave it on the default, or pick a specific modem so the rule only applies to messages arriving on that SIM card. On single-modem devices this field is not shown.

Choose what the forwarded message says

Use **Message content**:

Option A: Original message

The recipients get the incoming text unchanged. One extra choice appears, **Message header**:

Option	Result
Don't include	Only the original text is forwarded.
Include sender	The phone number of the original sender is added to the forwarded message, so recipients know where it came from.

Option B: Custom text

The recipients get your own text instead of the original. Type it in **Custom message** (maximum 500 characters). You can pull pieces of the original message in with placeholders:

Placeholder	Replaced with
`{SENDER}`	The phone number the SMS came from
`{MESSAGE}`	The full text of the original message

Example: `Alarm from {SENDER}. Details: {MESSAGE}` sends a readable sentence built around the raw machine text.

Choose the recipients

In **Forward to**, select the contacts or groups that should receive the message. Start typing to search. This field is required, a rule cannot be saved without at least one recipient.

Optionally add a phone call

Call after sending SMS makes the device also place a voice call to the same recipients. The available options depend on your device model:

Option	What happens
No	No call is made. This is the default.
Ring only	The device rings the recipient and hangs up. No audio is played.
Yes - text to speech	The device calls and reads out the message text.
Yes - text to speech (advanced)	Same as above, using a selectable, more natural voice. Choose the voice in the **Voice model** field that appears.

If your device does not support voice calls, only **No** is available.

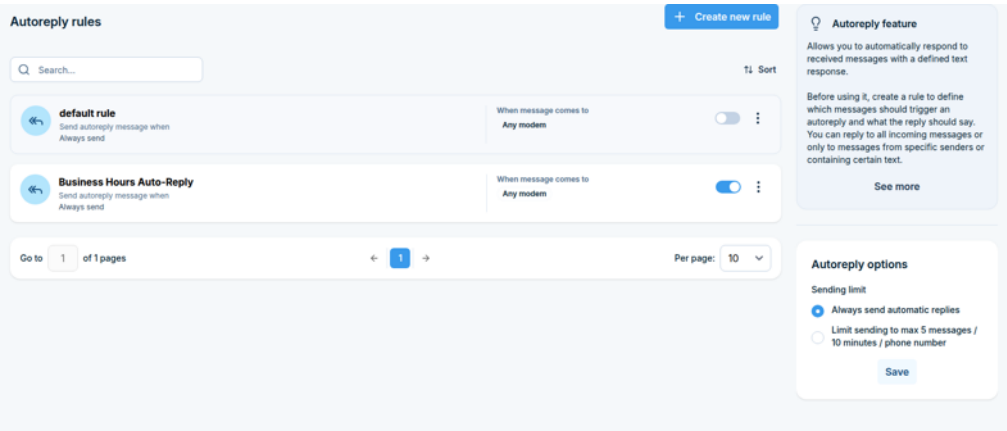
Click **Save**. The rule starts working immediately on newly received messages.

How forwarding works

- The text condition is a **contains** match, not an exact match. A rule looking for `ALARM` forwards a message saying `ROOM 4 ALARM triggered`.
- If several rules match the same incoming message, **each** of them forwards separately, so recipients can receive more than one SMS. Keep the conditions distinct to avoid duplicates.
- Rules apply only to messages arriving after the rule was created and enabled. They do not process messages already in the inbox.
- Recipients can still be skipped for their own reasons: **Vacation mode** on the contact, a shift that is currently outside its hours (see Shifts), or the number being on the deny list.

Avoid forwarding loops. Do not forward messages to a number that itself forwards back to your device. Two devices pointing at each other will keep sending messages back and forth.

Autoreplies



Autoreply rules and sending limit options

What this feature does

Autoreplies sends an **automatic text answer to incoming SMS messages**.

You create rules that decide which incoming messages get an answer and what the answer says. A rule can reply to everything, or only to messages from certain senders, or only to messages containing a certain phrase.

Typical uses: confirming that an order request was received, telling people that the number is unattended at night, or answering a keyword with fixed information such as opening hours.

Before you start

- The device must be able to send SMS. Check that at least one modem is connected and registered on the network.
- If you want to reply only to specific senders, those contacts and groups must be marked as **Public** in the Phonebook.

Step 1: Open the Autoreplies page

In the sidebar, go to **Automation > SMS > Autoreplies**.

On the right side of the page there is an **Autoreply options** box. It holds one setting that applies to all rules, described in Step 3.

Step 2: Create a rule

Click **Create new rule** in the top right corner. A side panel opens.

Name the rule

In **Rule name**, type something descriptive, for example `Out of hours reply`. Maximum 100 characters.

Decide which messages to answer

Choose **Send autoreply for**:

Option	What it means
All incoming messages	Every incoming SMS gets the reply.
Specified sender / message	Only messages matching the conditions you set below get a reply.

If you chose **Specified sender / message**, two conditions become available. You can use one or both. When you use both, a message must satisfy **both** to get a reply.

When incoming SMS comes from Tick this and select the contacts or groups that should get a reply. Start typing to search. Only **public** contacts and groups can be selected here.

When incoming SMS text contains Tick this and type the phrase to look for, for example `PRICE`. The phrase can appear anywhere in the message text. Tick **Case sensitive** if `price` and `PRICE` should be treated as different.

Limit the rule to one modem (multi-modem devices only)

If your device has more than one modem, a **When messages comes to** field appears. Leave it on **Any modem**, or pick a specific modem so the rule only replies to messages arriving on that SIM card. On single-modem devices this field is not shown.

Write the reply

Autoreply message The text that is sent back. Maximum 2000 characters. The same text goes to everyone who triggers this rule, so keep it general.

Send as Unicode Tick this if the reply contains characters outside the standard GSM alphabet, such as Polish, German or Cyrillic letters. Unicode messages fit fewer characters per SMS part.

Click **Save**. The rule starts working immediately on newly received messages.

Step 3: Set the sending limit

The **Autoreply options** box on the right of the page controls how often the device is willing to auto-answer the same phone number:

Option	Result
Always send automatic replies	Every matching message gets a reply, no matter how many arrive.
Limit sending to max 5 messages / 10 minutes / phone number	At most 5 automatic replies go to the same phone number within 10 minutes. Further messages from that number are not answered until the window passes.

Pick the option you want and click **Save**.

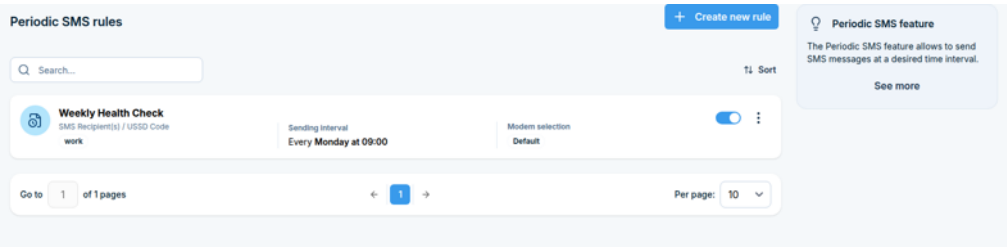
> **It's highly recommended to use the limit.** Without it, two devices that both auto-reply can end up answering each other in a loop, which burns through SMS credits quickly. The limit is the safeguard against that.

This setting is **global**. It applies to every autoreply rule on the device.

How matching works

- The text condition is a **contains** match, not an exact match. A rule looking for `PRICE` answers a message saying `what is the PRICE of item 5`.
- If several rules match the same incoming message, **each** of them sends its own reply, so the sender can receive more than one SMS. Keep the conditions distinct if you only want one answer.
- Rules apply only to messages arriving after the rule was created and enabled. They do not process messages already in the inbox.

Periodic SMS



Add Periodic SMS rule dialog

What this feature does

Periodic SMS sends a message **automatically on a repeating schedule**, without anyone having to click Send. You create a rule once, and SMSEagle keeps sending it every hour, day, week, month or year.

You can schedule two things:

- an **SMS** to phone numbers or to a Phonebook group, optionally followed by a phone call,

- a **USSD code** sent to your mobile operator (for example to check the prepaid balance of the SIM card).

Typical uses: a daily “system alive” message, a weekly reminder to a duty team, a monthly balance check on a prepaid SIM.

Before you start

- If you want to send to a group, the group must exist in **Phonebook > Groups** and be marked as **Public**. Private groups cannot be selected here.
- Make sure the device clock and time zone are correct, because the schedule follows device time. Check this in **Settings > Date/Time**.

Step 1: Open the Periodic SMS page

In the sidebar, go to **Automation > SMS > Periodic SMS**. You will see the list of rules you already have.

Step 2: Create a rule

Click **Create new rule** in the top right corner. A side panel opens.

Name the rule

In **Rule name**, type something you will recognise later, for example `Daily heartbeat` or `Monthly SIM balance`. Maximum 100 characters.

Set the schedule

Choose a **Sending interval**. The fields below the selector change depending on what you pick:

Interval	What you set	Example
Hourly	**At minute** (in 5-minute steps)	`15` sends at 00:15, 01:15, 02:15 and so on
Daily	**At time**	`07:30` sends every morning at 07:30
Weekly	**At week day** and **At time**	`Monday` + `08:00` sends every Monday morning
Monthly	**At day of month** and **At time**	`1` + `09:00` sends on the first day of each month
Annually	**At month - day** (format `mm-dd`) and **At time**	`12-24` + `10:00` sends every 24 December

> **Days that do not exist:** if you schedule something for day 31 of every month, it will not be sent in months that are shorter. Use day 28 or earlier if the message must go out every month.

Choose the modem (multi-modem devices only)

If your device has more than one modem, a **Modem selection** field appears. Leave it on the default to let SMSEagle choose, or pick a specific modem if the message has to go through a particular SIM card. On single-modem devices this field is not shown.

Choose what to send

Use the **Message type** switch at the top of this section:

Option A: SMS

1. Type the text in **SMS Text** (maximum 2000 characters).
2. Tick **Send as Unicode** if the text contains characters outside the standard GSM alphabet, such as Polish, German or Cyrillic letters. Note that Unicode messages fit fewer characters per SMS part.
3. Under **Send to**, choose where the message goes:
    - **Public groups** - start typing a group name and pick it from the list. You can add several groups.
    - **Input manually** - type the phone numbers. Separate multiple numbers with commas, for example `+48111222333,+48444555666`.

    You must fill in one of the two, otherwise the rule cannot be saved.

Option B: USSD Code

Type the code in **USSD code**, for example `*100#`. The reply from the operator arrives as an incoming message in your inbox.

> USSD codes are sent through the modem to your mobile operator. The available codes depend on the operator, not on SMSEagle.

Optionally add a phone call

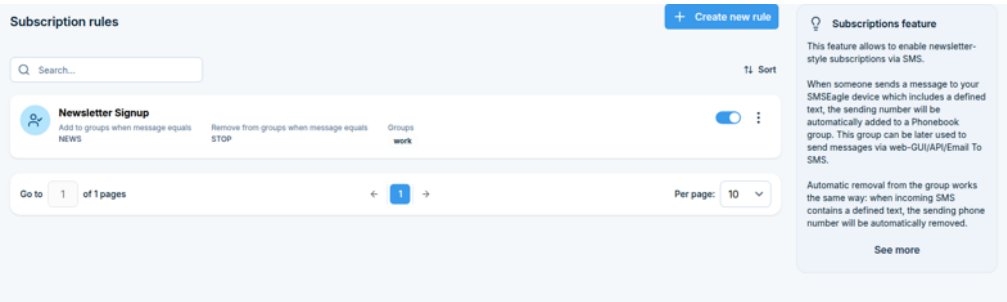
Call after sending SMS makes the device also place a voice call to the same recipients, which is useful for alerts that must not be missed. The available options depend on your device model:

Option	What happens
No	No call is made. This is the default.
Ring only	The device rings the recipient and hangs up. No audio is played.
Yes - text to speech	The device calls and reads out the message text.
Yes - text to speech (advanced)	Same as above, using a selectable, more natural voice. Choose the voice in the **Voice model** field that appears.

If your device does not support voice calls, only **No** is available.

Click **Save**. The rule appears in the list and starts running at its next scheduled time.

Subscriptions



Subscription rules

What this feature does

Subscriptions let people **join and leave a Phonebook group by sending an SMS**, the same way a newsletter opt-in works.

You define two keywords: one that adds the sender to a group, and one that removes them. When somebody texts your SMSEagle number with one of those keywords, their phone number is added to or removed from the group automatically. You can then send messages to that group from Compose, the API or Email to SMS.

Typical uses: a public alert list that residents can opt into, or a shift notification list that staff can join themselves without an administrator.

Before you start

Create the group that people will subscribe to:

1. Go to **Phonebook > Groups**.
2. Click **Add new**, give the group a name and tick **Set as Public Group**.
3. Click **Save**.

Only **public** groups can be used in a subscription rule.

You also need to tell your users which number to text and which keyword to send. SMSEagle does not advertise this automatically.

Step 1: Open the Subscriptions page

In the sidebar, go to **Automation > SMS > Subscriptions**.

Step 2: Create a rule

Click **Create new rule** in the top right corner. A side panel opens. Fill in the fields:

Rule name Something you will recognise, for example `Flood alerts opt-in`. Maximum 100 characters.

Groups Start typing and select one or more groups. Subscribers are added to, or removed from, **all** the groups listed here. Only public groups can be selected.

Add phone number to groups, when incoming message equals The keyword that subscribes somebody, for example `JOIN` or `START ALERTS`. The keyword must be unique to the subscription rule.

Remove phone number from groups, when incoming message equals The keyword that unsubscribes somebody, for example `STOP` or `LEAVE`.

Case sensitive Leave this unticked so that `join`, `Join` and `JOIN` all work. Tick it only if you need the keyword to match exactly as typed.

Click **Save**.

How matching works

This is the most important detail to communicate to your users:

> The whole incoming message must be **exactly** the keyword. Nothing else may be in the message.

Keyword is `JOIN`	Result
User texts `JOIN`	Subscribed
User texts `join`	Subscribed (unless **Case sensitive** is ticked)
User texts `Please JOIN me`	Nothing happens
User texts `JOIN ALERTS`	Nothing happens

Because of this, keep keywords short and easy to type, and tell your users to send only the keyword.

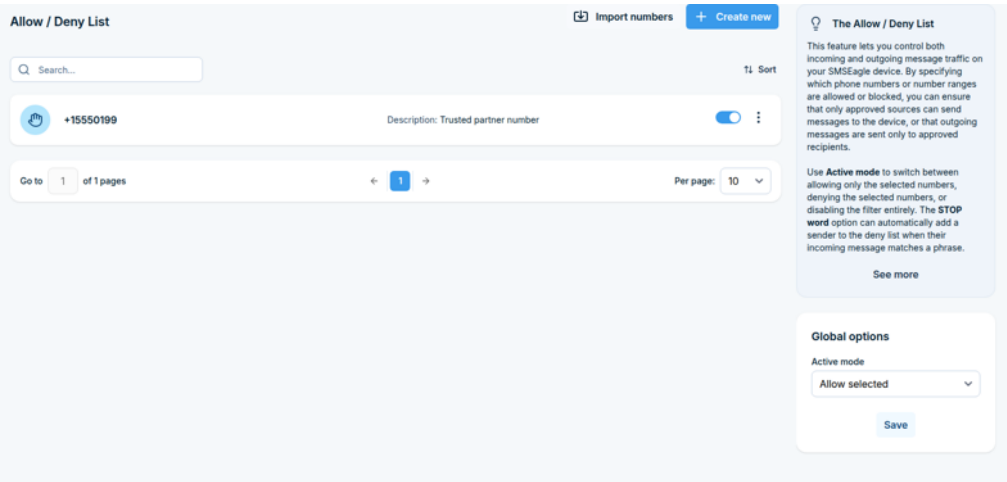
What happens when somebody subscribes

- If the sender's phone number is **already in the Phonebook**, that existing contact is added to the group.
- If the number is **not in the Phonebook**, SMSEagle creates a new contact for it automatically. The contact is named after the rule plus the phone number, for example `Flood alerts opt-in +48111222333`, and it is created as a private contact.

When somebody unsubscribes, they are removed from the group, but the contact itself is kept in the Phonebook.

You can review who has joined at any time: go to **Phonebook > Groups**, find the group and open **Manage contacts**.

Allow / Deny List



Allow / Deny List global options

What this feature does

The Allow / Deny List filters SMS traffic on your device by phone number.

You keep a list of numbers and choose how the device treats it:

Active mode	What happens
Allow selected	Only the numbers on the list are accepted. Everything else is ignored.
Deny selected	The numbers on the list are ignored. Everything else is accepted.
Disabled	No filtering at all. The list is kept but not used.

Typical uses: blocking a number that keeps spamming the device (Deny), or locking a gateway down so that only your own alarm systems can talk to it (Allow).

There is also a **STOP word** option, which adds a sender to the list automatically when their message matches a phrase you define. That is what makes an opt-out keyword such as `STOP` work.

Before you start

Decide which way round you want to work. **Allow selected** and **Deny selected** use two separate lists, so the rules you add in one mode are not visible in the other. Switching the mode switches the whole list, it does not invert it.

Step 1: Open the Allow / Deny List page

In the sidebar, go to **Automation > General > Allow / Deny List**.

On the right side there is a **Global options** box holding the **Active mode** setting and the **STOP word** configuration. Both are described below.

Step 2: Choose the active mode

In the **Global options** box, set **Active mode** to **Allow selected**, **Deny selected** or **Disabled**, then click **Save**. The page reloads showing the list that belongs to the mode you picked.

> While the mode is **Disabled**, the page shows a “Filtering is disabled” notice instead of the list, and rules cannot be added or edited. Switch to **Allow selected** or **Deny selected** to manage them again.

Step 3: Add a number

Click **Create new** in the top right corner. A side panel opens.

Phone number The number this rule applies to. Maximum 15 characters. Only digits, `+` and `*` are allowed, and the entry must contain at least one digit.

You can match a whole range of numbers by using `*` as a wildcard, which stands for any characters:

Pattern	Matches
`NUMBER`	Exactly that number
`*NUMBER`	Any number ending with it
`NUMBER*`	Any number starting with it
`*NUMBER*`	Any number containing it

For example, `48512*` covers every number starting with `48512`, and `*12345678` matches the same subscriber no matter which country prefix format arrives.

Description A short note explaining why the number is on the list, for example `Spam` or `Alarm panel, HQ`. Required, maximum 255 characters.

Click **Save**.

Step 4: Import a list from CSV

If you already have the numbers in a spreadsheet, click **Import rules** in the top right corner instead of adding them one by one.

1. Prepare a UTF-8 encoded CSV file with exactly two columns, headed **Number** and **Reason**.
2. Click **Import rules**, drop the file into the upload area or click it to browse.
3. Click **Import**.

The numbers are added to the list that is currently active.

Step 5: Configure the STOP word (optional)

The STOP word adds senders to the list automatically, so people can opt out by texting a keyword.

In the **Global options** box, click **Edit config** next to **STOP word**. A side panel opens. Choose **Auto add number to list when**:

Option	What it means
Never	The STOP word is off. Numbers are only added by hand or by import.
Incoming message equals to…	The whole message must be exactly the phrase you type.
Incoming message contains to…	The phrase may appear anywhere in the message.

If you pick one of the two matching options, two more fields appear:

- The phrase itself, maximum 160 characters, for example `STOP`.
- **Autoreply message**, maximum 160 characters. This text is sent back to the number after it has been added to the list. Leave it empty if you do not want to confirm the opt-out.

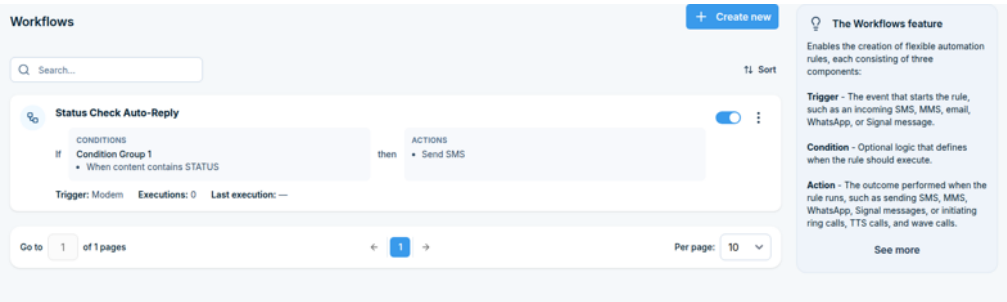
Click **Save**. The summary in the **Global options** box now shows the active condition and the autoreply text.

> **Use "equals" rather than "contains" for opt-out keywords.** With **contains**, an ordinary message such as `please stop sending the night reports` would also remove the sender.

How filtering works

- The filter is applied to messages arriving after the rule was created and enabled. It does not reprocess messages already in the inbox.
- A disabled rule is ignored completely, whichever mode is active.
- **Allow selected** and **Deny selected** keep separate lists. If you switch the mode and the page looks empty, you are looking at the other list, nothing has been deleted.
- The STOP word setting is **global**: it applies to the list that is currently active.

Workflows



Workflows overview

Workflows let you build flexible automation rules without needing a separate integration for every combination of trigger and action. Each workflow consists of three parts:

- **Trigger** - the event that starts the rule: an incoming SMS, MMS, email, WhatsApp, or Signal message (or a modem delivery/sent/sending-error event).
- **Condition** - optional logic that decides whether the rule should run for a given event.
- **Action** - what happens when the rule runs: sending an SMS, MMS, WhatsApp, or Signal message, or initiating a ring call, TTS call, or wave call.

Where to find it

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

Step 1: Create a workflow and pick a trigger

Click **Create new**, give the workflow a **Name**, and choose a **Trigger**: Modem, Email, Signal, WhatsApp, Modem (delivered), Modem (sent), or Modem (sending error).

Step 2: Add condition groups (optional)

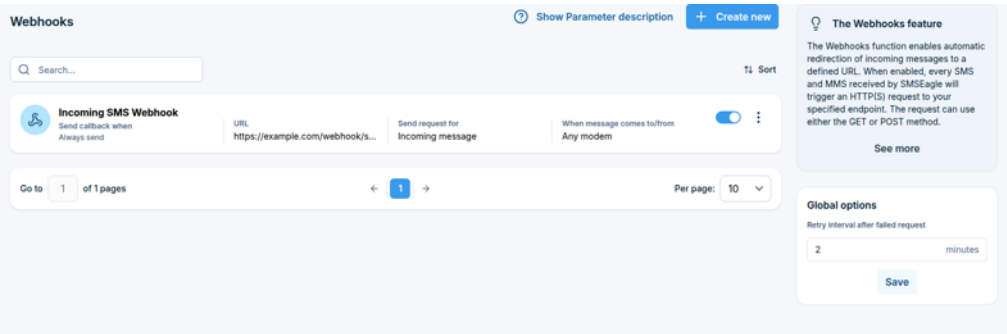
Under **Condition groups**, click **Add group** to add one or more conditions the incoming event must match before the workflow runs. Leave this empty if the workflow should run for every event matching the trigger.

Step 3: Add actions

Under **Actions**, click **Add action** to define what the workflow does when it runs - for example sending a reply, forwarding the message to another channel, or placing a call.

Click **Save workflow** to activate it.

Webhooks



Webhooks overview

What this feature does

A webhook makes SMSEagle call **your** system. Whenever something happens on the device (a message arrives, a message is sent, a delivery report comes back, a call comes in), the device sends an HTTP(S) request to a URL you choose, carrying the details as parameters.

That is how you push SMS traffic into a ticketing system, a CRM, a chat bot or your own application without polling the API.

Two integrations get dedicated support:

Method	What it is for
POST (3CX)	Pushing messages into a 3CX phone system.
POST (Zabbix)	Acknowledging Zabbix events by SMS, so an engineer can reply `ACK 12345` to close an alert.

Before you start

- You need the URL that will receive the requests, reachable from the device. Local and private addresses are rejected.
- Your endpoint should answer with HTTP **200 OK**, or with whichever status codes you configure in the rule.
- For Zabbix you need either an API token (Zabbix 6.4 and newer) or a username and password.

Step 1: Open the Webhooks page

In the sidebar, go to **Automation > General > Webhooks**.

Each rule shows its URL, what it fires for and, on multi-modem devices, which modem it is limited to. Every rule has a switch to **enable or disable** it, an **Edit** action and a **Delete** action.

The **Global options** box on the right holds one setting that applies to all rules, described in Step 6.

Step 2: Create a rule

Click **Create new** in the top right corner. The webhook form opens as a full page with three sections.

Step 3: Basic configuration

Field	What to enter
Rule name	A descriptive name, maximum 100 characters.
URL	The address to call, maximum 300 characters, for example `https://example.com/webhook`.
URL method	**GET**, **POST**, **POST (3CX)** or **POST (Zabbix)**.
Content type	Only for plain **POST**: **FormData** or **JSON**.
To (3CX)	Only for **POST (3CX)**: the destination in your 3CX system.

Click **Test connection** next to the URL to send a sample request straight away. The result appears below the field and tells you the HTTP status that came back, so you can confirm the endpoint works before saving.

For **GET** and **POST**, an example of the request string is shown under the fields, so you can see exactly what your endpoint will receive.

What the request contains

The request your endpoint receives carries the event details as parameters. Some are sent for every event, others only for messages or only for calls.

Always sent

Parameter	What it carries
`sender`	Sender number.
`timestamp`	When SMSEagle received or sent the message, as `YYYYmmddHHiiss`, for example `20140531092257`.
`msgid`	The SMSEagle message id.
`modemno`	The modem the incoming message was received on, or the one the message was sent from.
`apikey`	The API key of your service, if you set one in the **Security settings**. Optional.

Sent for SMS and MMS only

Parameter	What it carries
`text`	Content of the SMS message.
`text_binary`	Binary content of the SMS message.
`status`	Message status.
`oid`	Value of the OID identifier assigned to an outgoing message with a matching phone number. Optional.
`attachments`	MMS attachments, for example `[0 => [name => image.png, content-type => image/png, content => wfFWgwOlgBRwdWvsvs=]]`. **POST only**, since a GET query string cannot carry file data. Optional.

Sent for incoming voice calls only

Parameter	What it carries
`status`	Status of the incoming call: `accepted`, `rejected` or `ignored`.

A rule fires for one event type, so a request only ever carries the parameters of that type. A rule with the **Incoming call** trigger, for instance, never sends `text` or `attachments`.

Whatever the method, SMSEagle expects your endpoint to answer with **200 [OK]**, unless you widen that with **Expected HTTP Status Code(s)** in the Security settings.

The **Show Parameter description** link on the rules page opens this same list inside the application, together with a sample GET request:

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

Customising parameter names

By default the request uses the SMSEagle parameter names listed above. If your endpoint expects different ones, tick **Customize parameter names** and type your own name next to each parameter you want renamed. Every parameter in the three tables can be renamed; the ones you leave empty keep their default name.

Renaming changes only the parameter **name** in the request, never its value or when it is sent.

Step 4: Trigger conditions

Send request for decides which event fires the webhook:

Option	Fires when
Incoming message	An SMS or MMS arrives.
Sent message	An outgoing message has been sent.
Delivery report	A delivery report comes back.
Sending error	An outgoing message failed.
Incoming call	A call comes in.

Send request when narrows it down further:

Option	What it means
Always	Every event of the chosen type fires the webhook.
For specified senders / when text contains	Only events matching the conditions below fire it.

If you chose the second option, two conditions become available. You can use one or both, and an event must satisfy every condition you enable.

When incoming SMS comes from Tick this and select the contacts or groups. Only public contacts and groups are accepted.

When incoming SMS text contains Tick this and type the phrase. Tick **Case sensitive** if upper and lower case should be treated as different. This condition is not available for the **Incoming call** trigger, since a call has no text.

On multi-modem devices, **When message comes to/from** limits the rule to a single modem. Leave it on **Any modem** otherwise.

Step 5: Security settings

Field	What it does
API key of your service	An optional key sent with the request, so your endpoint can verify that the call really comes from your device.
Expected HTTP Status Code(s)	Which responses count as success. One or more three-digit codes separated by commas, for example `200,201,202`. Default is `200`, maximum 20 characters.
Allow self-signed SSL certificate	Accept a certificate that is not signed by a public authority.
Verify peer	Check the server's certificate.
Verify peer name	Check that the certificate matches the host name.

Anything that does not match the expected status codes counts as a failed request, and is retried according to the global retry interval.

Zabbix rules

If you picked **POST (Zabbix)** as the method, extra fields appear:

- **Zabbix action** - **Acknowledge (ACK)**, **Unacknowledge (NOACK)** or both. The panel shows the SMS format the device will expect, for example `ACK 12345 Problem resolved`.
- **Auth type** - **API Token** (Zabbix 6.4 and newer, recommended) or **Login/Password** for older versions. With a token you enter it in the API key field; with login you enter **Zabbix username** and **Zabbix password**.
- **Test values** - an **Event ID** and **Message** used only by **Test connection**, never saved.

Click **Save webhook**.

Step 6: Set the retry interval

The **Global options** box on the rules page holds **Retry interval after failed request**, in minutes. When a request fails, the device waits this long before trying again.

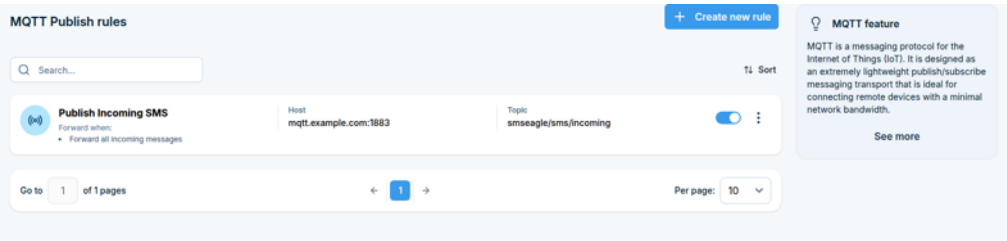
Enter a whole number of minutes and click **Save**. The setting is **global**: it applies to every webhook rule on the device.

How webhooks behave

- Rules apply to events happening after the rule was created and enabled. They do not replay past messages.

- The text condition is a **contains** match, not an exact match.
- If several rules match the same event, **each** of them sends its own request, so one message can reach several endpoints.
- A request counts as successful only if the response status is one of the **Expected HTTP Status Code(s)**. Anything else, including no response at all, is a failure and is retried.
- **Test connection** sends a sample payload, not a real message, so it is safe to run against a production endpoint that only logs.

MQTT



MQTT Publish rules

What this feature does

MQTT is the messaging protocol used by most IoT devices, sensors and building automation systems. Devices send short messages to a **broker**, each tagged with a **topic** such as `building/boiler/temperature`. Anyone connected to the broker can listen to the topics they care about.

SMSEagle sits on both sides of that conversation:

Rule type	Direction	What it does
Subscribe	MQTT into SMS	Listens to a broker and turns incoming MQTT messages into SMS messages sent to your people.
Publish	SMS into MQTT	Takes incoming SMS messages and publishes them to a broker, so your IoT system can react to them.

Typical uses: turning a sensor alarm into an SMS to the maintenance team (Subscribe), or letting a technician text a command that is picked up by the automation system (Publish).

The two rule types are configured separately and do not depend on each other. Use whichever you need.

Before you start

You need the connection details of your MQTT broker: host address, port, and a username and password if the broker requires them - configured once under MQTT in Settings, before writing Subscribe rules here.

For **Subscribe** rules you also need the list of topics to listen to (also set in Settings). For **Publish** rules you need the topic to publish into (set per rule, below).

Part 1: Subscribe (MQTT into SMS)

Subscribe rules turn incoming MQTT messages into SMS, once the broker connection itself is configured under Settings.

Step 1: Open the Subscribe rules page

In the sidebar, go to **Automation > General > MQTT**, then choose **Subscribe**.

Step 2: Create a Subscribe rule

Click **Create new rule** in the top right corner. A side panel opens.

Name the rule

In **Rule name**, type something descriptive, for example `Boiler alarm to maintenance`. Maximum 100 characters.

Decide which MQTT messages to act on

Choose **Forward for**:

Option	What it means
Any message	Every MQTT message the device receives triggers this rule.
Specified topic / message	Only messages matching the conditions you set below trigger it.

If you chose **Specified topic / message**, two conditions become available. You can use one or both. When you use both, a message must satisfy **both**.

When incoming message has topic Tick this and type the topic in **Topic**, for example `building/boiler`.

When incoming message contains Tick this and type the phrase in **Message phrase**, for example `ALARM`. Tick **Case sensitive** if `alarm` and `ALARM` should be treated as different.

Choose the recipients

In **Forward to**, select the contacts or groups that should receive the SMS. Only **public** contacts and groups can be selected here. This field is required.

Write the SMS text

Message format controls what the SMS says. You build it from the MQTT message using placeholders:

Placeholder	Replaced with
`{TOPIC}`	The topic the MQTT message arrived on
`{MESSAGE}`	The content of the MQTT message

The default is `{TOPIC}: {MESSAGE}`, which produces an SMS like `building/boiler/temperature: 94`. You can also write your own sentence around them, for example `Boiler warning on {TOPIC}, value {MESSAGE}`.

Tick **Send as Unicode** if the text contains characters outside the standard GSM alphabet, such as Polish, German or Cyrillic letters.

Advanced options

Click **Advanced options** to expand this section. You do not need it for a basic setup.

- **Modem** (multi-modem devices only) - send the SMS through a specific SIM card instead of the default.
- **Call after sending SMS** - also place a voice call to the same recipients. Options are **No**, **Ring only**, **Yes - text to speech** and **Yes - text to speech (advanced)**, depending on what your device model supports. With the advanced option you also pick a **Voice model**.

Click **Save**. The rule starts working on MQTT messages received from now on.

How Subscribe matching works

- The **Topic** condition is a **contains** match and ignores upper and lower case. A rule with topic `boiler` also matches `building/boiler/temperature`.
- The **Case sensitive** checkbox applies to the message phrase only, never to the topic.
- If several Subscribe rules match the same MQTT message, **each** of them sends its own SMS.

Part 2: Publish (SMS into MQTT)

Publish rules do **not** use the MQTT service settings under Settings. Each rule carries its own broker connection, so different rules can publish to different brokers.

Step 1: Open the Publish rules page

In the sidebar, go to **Automation > General > MQTT**, then choose **Publish**.

Step 2: Create a Publish rule

Click **Create new rule** in the top right corner. A side panel opens.

Name the rule

In **Rule name**, type something descriptive, for example `Technician commands to automation`. Maximum 100 characters.

Decide which SMS messages to publish

Choose **Forward for**:

Option	What it means
Any message	Every incoming SMS is published to the broker.
Specified sender / message	Only messages matching the conditions you set below are published.

If you chose **Specified sender / message**, the conditions below become available. You can combine them, and a message then has to satisfy all of the ones you enable.

When incoming SMS comes from Tick this and select the sender contacts or groups. Only **public** contacts and groups can be selected here.

When incoming SMS text contains Tick this and type the phrase in **Text fragment**. Tick **Case sensitive** if upper and lower case should be treated as different.

When messages comes to (multi-modem devices only) Leave on **Any modem**, or pick a specific modem so only messages arriving on that SIM card are published.

> Restricting a Publish rule by sender is a sensible precaution. Without a sender condition, anybody who knows your number can push content into your IoT system.

Enter the broker connection

Fill in the broker this rule publishes to:

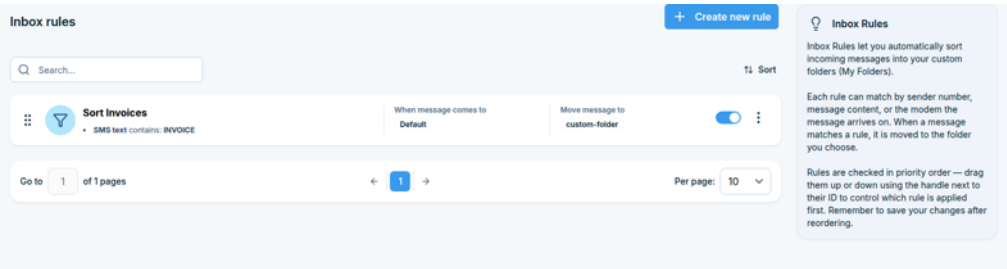
Field	What to enter
Host	The broker address, for example `test.host.io`
Port	The broker port, for example 1883. Allowed range is 1 to 65535.
Username	The broker user, if required. Leave empty for an open broker.
Password	The broker password, if required.
Topic	The topic to publish into, for example `smseagle/incoming`
TLS/SSL	Turn on if the broker uses an encrypted connection.
TLS certificate verification	Leave on unless the broker uses a self-signed certificate the device cannot validate.

Click **Save**. Incoming SMS messages that match the rule are published from now on.

How Publish matching works

- The text condition is a **contains** match, not an exact match.
- If several Publish rules match the same SMS, **each** of them publishes, so the message can land on more than one broker or topic.
- Rules apply only to messages arriving after the rule was created and enabled. They do not process messages already in the inbox.

Inbox Rules



Inbox Rules overview

Inbox Rules automatically sort incoming messages into your custom folders (My Folders), instead of leaving everything in the main Inbox.

Where to find it

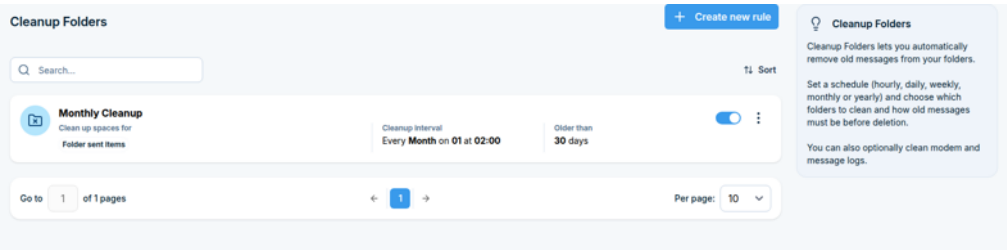
Automation > Folders > Inbox Rules (`/automation/inbox-rules/`).

Configuring an inbox rule

Click **Create new rule**. Each rule can match by sender number, message content, or the modem the message arrived on; a message matching the rule is moved to the folder you choose.

Rules are checked in priority order. Drag a rule up or down using the handle next to its ID to control which rule is applied first, and remember to save your changes after reordering.

Cleanup Folders



Cleanup Folders overview

Cleanup Folders automatically removes old messages from your folders, so they do not accumulate indefinitely.

Where to find it

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

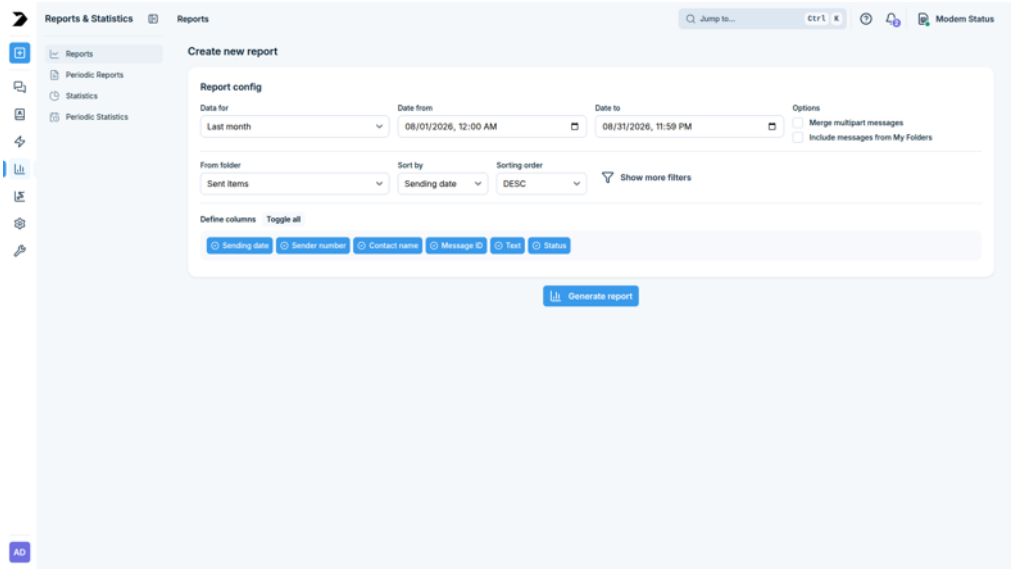
Configuring a cleanup rule

Click **Create new rule**, then set a schedule (hourly, daily, weekly, monthly, or yearly), choose which folders to clean, and how old a message must be before it is deleted. You can also optionally clean modem and message logs on the same schedule.

Reports & Statistics

This chapter covers the **Reports & Statistics** section of the web interface - exporting message data as a one-off report, or scheduling reports to be emailed automatically.

Reports



Create new report

Reports & Statistics > Reports (`/reports/`) builds a one-off report of your message history.

Under **Report config**, choose the time range with **Data for** (a ready-made range such as Today, Last 7 days, or This month, or **Custom range** with explicit **Date from** / **Date to** fields).

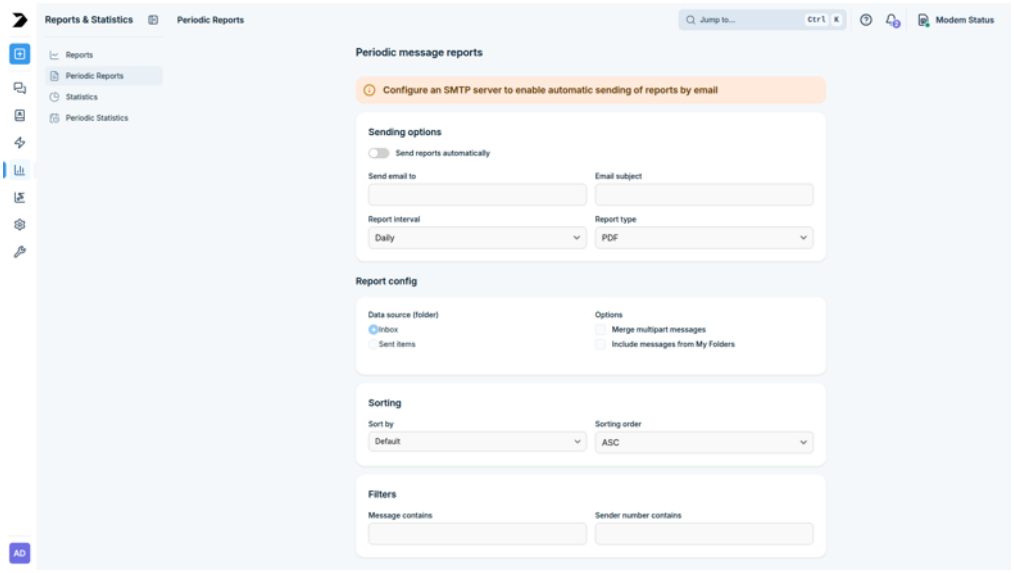
Under **Options**:

Option	What it does
Merge multipart messages	Combines a long SMS split into several parts back into one row.
Include messages from My Folders	Also includes messages that were moved into a custom folder.
From folder	Which folder to report on: **Sent items**, **Inbox**, or **Outbox**.
Sort by / **Sorting order**	Column to sort by (sending date, sender number, contact name, message ID, text, or status) and direction (ASC/DESC).

Click **Show more filters** for additional filtering, and use **Define columns** to choose which columns appear in the generated report - **Toggle all** selects or clears every column at once.

Click **Generate report** to produce it.

Periodic Reports



Periodic message reports

Reports & Statistics > Periodic Reports (`/reports/periodic-reports`) schedules a report to be generated and emailed automatically on a recurring basis, instead of running one by hand each time.

This requires a working SMTP Configuration - the page shows a reminder to configure one if it is missing.

Under **Sending options**, turn on **Send reports automatically** and fill in:

Field	What it does
Send email to	The recipient address for the generated report.
Email subject	The subject line of the email.
Report interval	**Daily**, **Weekly**, or **Monthly**.
Report type	**PDF** or **CSV**.

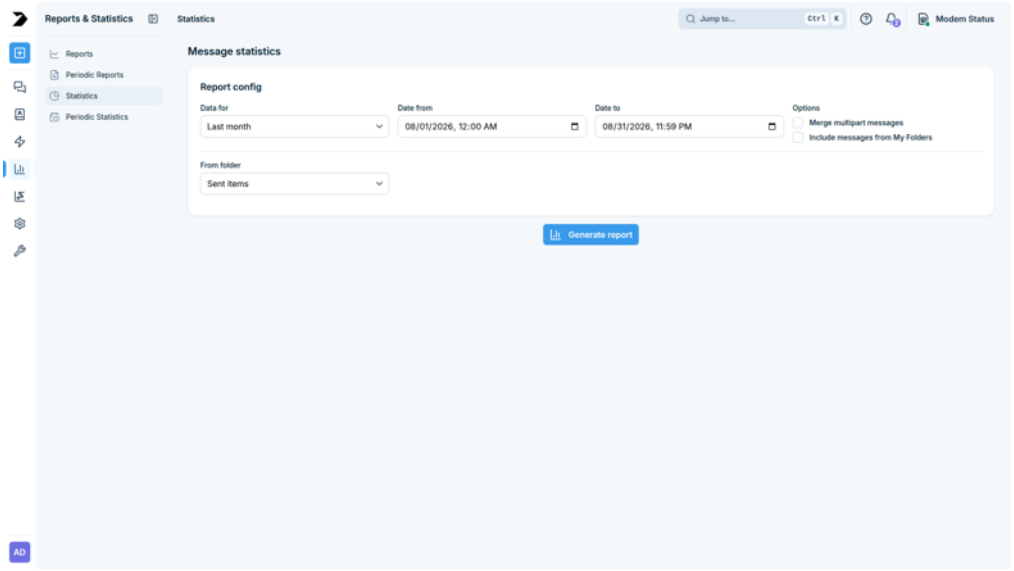
Under **Report config**, choose the **Data source (folder)** (**Inbox** or **Sent items**), the same **Merge multipart messages** / **Include messages from My Folders** options as a one-off report, and **Sorting** (sort field and ASC/DESC order).

Under **Filters**, narrow the report down with **Message contains** and/or **Sender number contains**.

Under **Output**, use **Select table columns** (with a **Toggle all** shortcut) to choose which columns the generated file includes: receiving date, sender number, contact name, SMS Center Number, message ID, text, read status, and modem ID.

Click **Save configuration**.

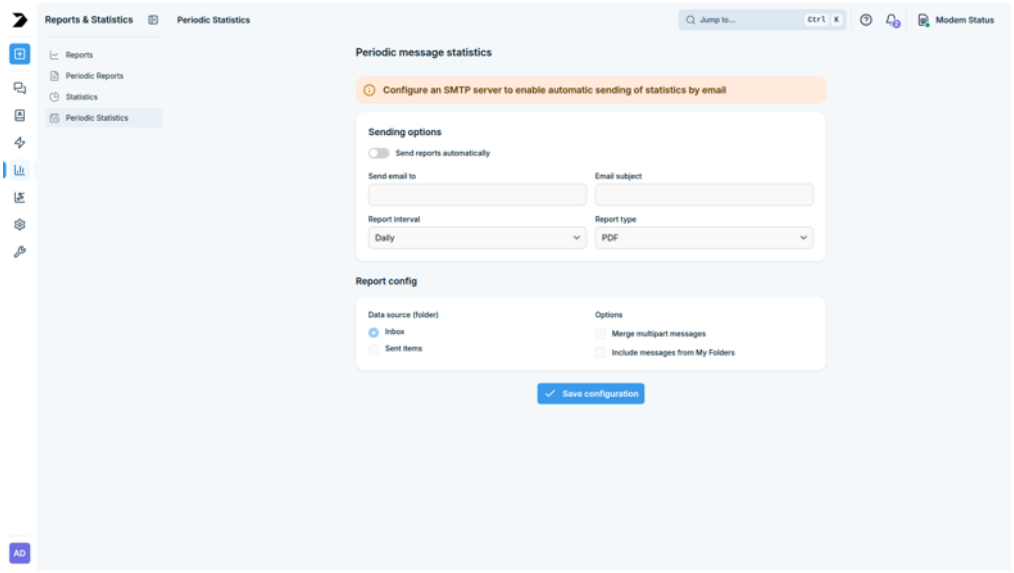
Statistics



Message statistics

Reports & Statistics > Statistics (`/reports/statistics`) works the same way as Reports above - the same **Data for** time-range picker and **Merge multipart messages** / **Include messages from My Folders** / **From folder** options - but produces aggregate traffic statistics instead of a row-per-message export. Click **Generate report** to produce it.

Periodic Statistics



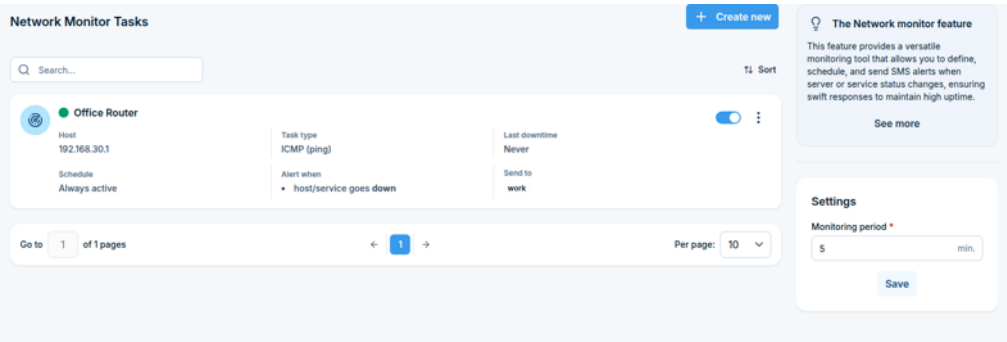
Periodic message statistics

Reports & Statistics > Periodic Statistics (`/reports/periodic-statistics`) schedules the statistics report above to be generated and emailed automatically, the same way Periodic Reports does for the row-per-message export: it needs a working SMTP Configuration, and offers the same **Sending options** (recipient, subject, **Daily / Weekly / Monthly** interval, **PDF / CSV** report type) plus a **Report config** section (data source folder, merge multipart messages, include My Folders). Click **Save configuration**.

Monitoring

This chapter covers the **Monitoring** section of the web interface: checking external hosts and services, and reading digital I/O.

Network Monitor



Network Monitor overview

What this feature does

Network Monitor turns your SMSEagle into a small monitoring station. It checks servers, devices and services on a schedule and sends an SMS when something stops responding, comes back, or reports a value outside the range you expect.

It has three parts:

Page	What it does
Tasks	The monitoring rules: what to check, how often, who to alert.
Reports	A history of downtime, filtered by date range and task, exportable to CSV.
SNMP Traps	Rules that turn SNMP traps sent to the device into SMS messages.

Typical uses: alerting the on-call engineer when a production server stops answering pings, warning about a temperature reading from an SNMP sensor, or forwarding a UPS trap to a phone.

Before you start

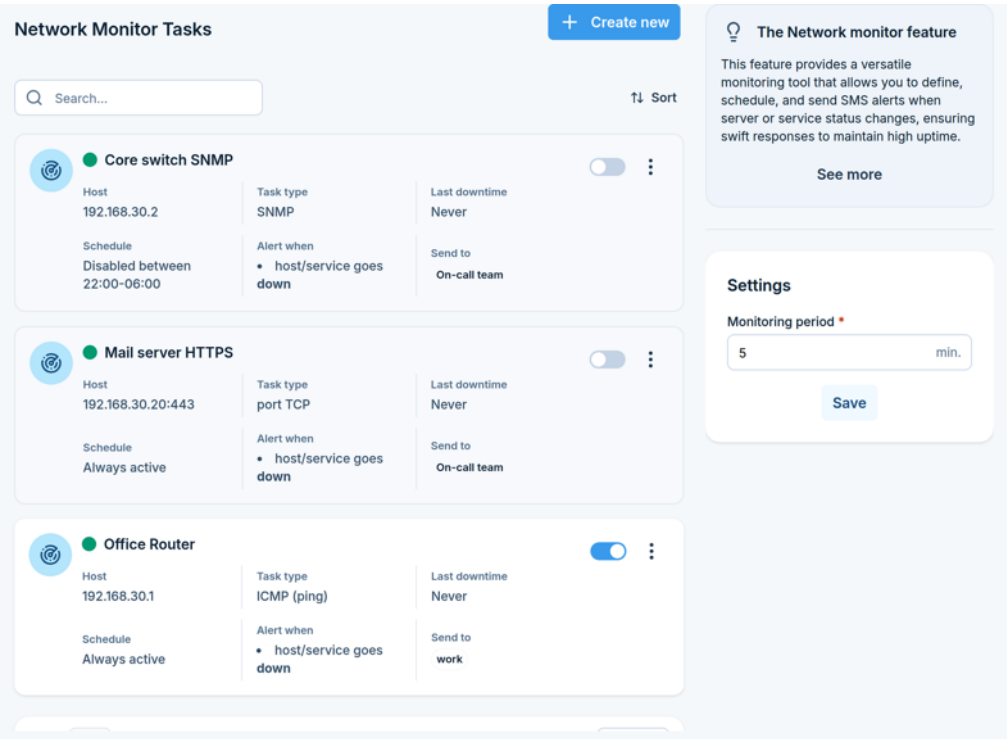
- The device must be able to reach the hosts you want to monitor. Check the network settings under **Settings > Network** first.

- Recipients must be marked as **Public** in the Phonebook if you want to alert a group. Otherwise you can type plain phone numbers into the task.
- For SNMP checks you need the community string and the Object ID (OID) you want to read. For Modbus checks you need the unit ID, the register and the function code.

Part 1: Tasks

Step 1: Open the Tasks page

In the sidebar, go to **Monitoring > Network Monitoring > Tasks**.



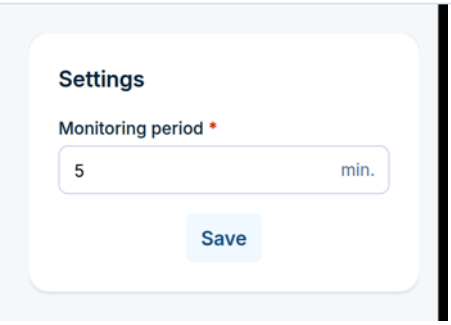
Network Monitor tasks

Each task in the list shows its host, schedule, task type, what it alerts on, when it was last down and who it notifies. A green or red marker tells you whether the host is currently responding.

Step 2: Set the monitoring period

The **Settings** box on the right of the Tasks page holds one setting that applies to **all** tasks: **Monitoring period**, in minutes. This is how often the device runs the checks.

Enter a value and click **Save**.



Monitoring period

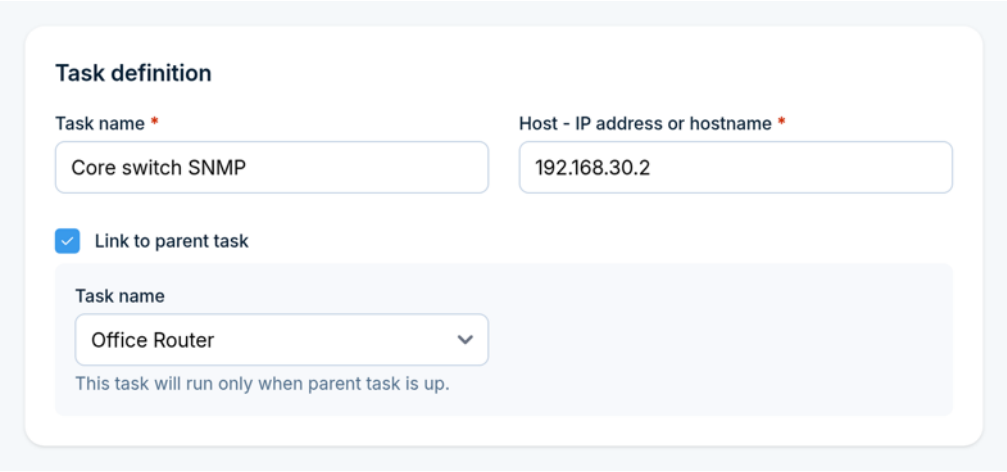
Step 3: Create a task

Click **Create new** in the top right corner. The task form opens as a full page, divided into five sections.

Task definition

Field	What to enter
Task name	A descriptive name, maximum 100 characters, for example `Mail server`.
Host - IP address or hostname	What to check, for example `192.168.1.10` or `mail.example.com`.
Link to parent task	Tick this to make the task depend on another one.
Task name (parent)	Shown once the checkbox is ticked: the task this one depends on.

A linked task **runs only while its parent task is up**. Use it to avoid alert storms: if the router in front of ten servers goes down, only the router task alerts, and the ten server tasks stay quiet.



Task definition

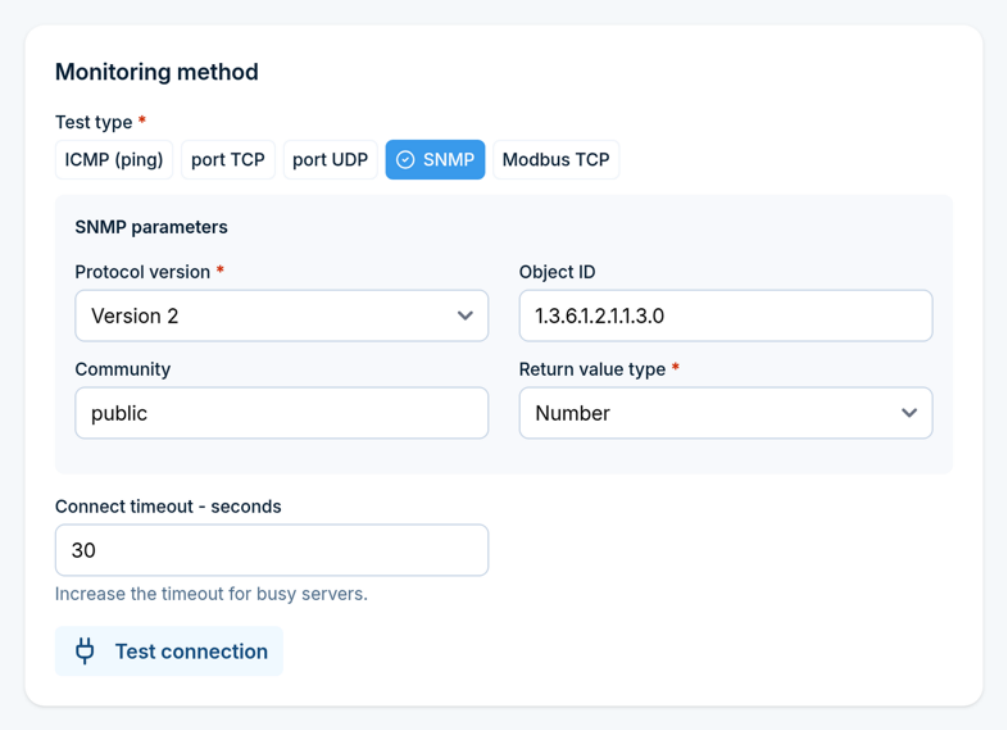
Monitoring method

Pick the **Test type**, then fill in the parameters that appear for it:

Test type	Parameters
ICMP (ping)	**Number of requests** - how many pings to send per check.
port TCP	**Port** - the TCP port that must accept a connection.
port UDP	**Port** - the UDP port to probe.
SNMP	**Protocol version** (1 or 2), **Object ID**, **Community**, **Return value type** (Number or String).
Modbus TCP	**Port**, **Unit ID**, **Register**, **Function code** (Read coils, Read Discrete Inputs, Read Holding Registers, Read Input Registers).

Connect timeout - seconds applies to every test type. Increase it for busy servers that answer slowly; the default is 30 seconds.

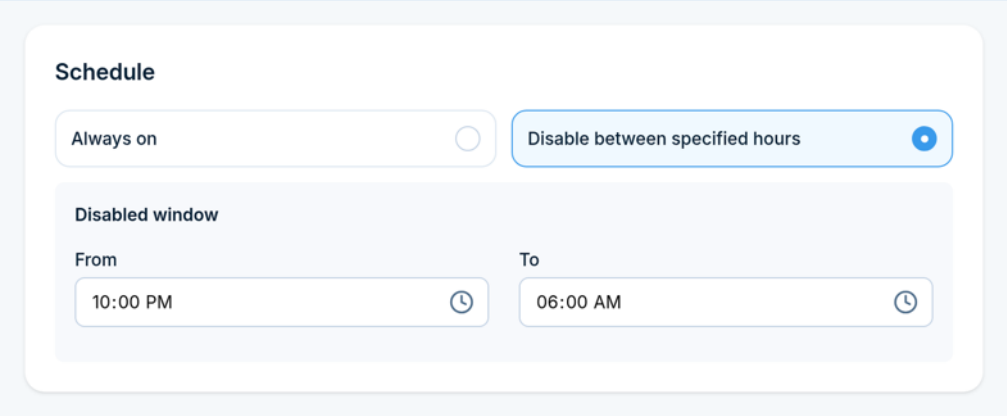
Click **Test connection** to try the check straight away. The result appears next to the button, so you can confirm the host answers before you save the task.



Monitoring method

Schedule

Choose **Always on** if the task should run around the clock, or **Disable between specified hours** and set **From** and **To** to create a quiet window, for example during a nightly backup that always takes the service offline.



Schedule

Alert triggers

First choose who gets the alert:

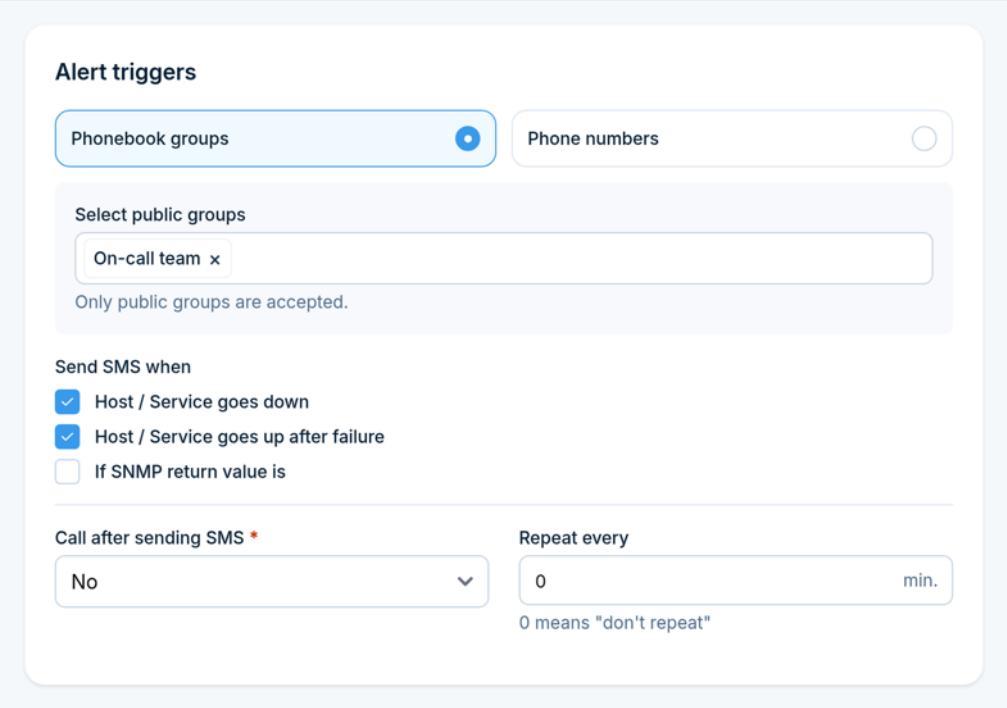
Option	What to enter
Phonebook groups	Select public groups. Only public groups are accepted.
Phone numbers	Type the numbers directly, separated by commas. Maximum 100 characters in total.

Then tick at least one **Send SMS when** condition. Without one the task cannot be saved:

- **Host / Service goes down**
- **Host / Service goes up after failure**
- **If SNMP return value is** - only for SNMP tasks. Pick an **Operator** (Equal to, Not equal to, Greater than, Less than, Contains, Does not contain) and a **Value**.
- **If Modbus return value is** - only for Modbus tasks, with the same operator and value fields.

Two more settings close the section:

- **Call after sending SMS** - also place a voice call. Options are **No**, **Ring only**, **Yes - text to speech** and **Yes - text to speech (advanced)**, depending on your device model. With the advanced option you also pick a **Voice model**.
- **Repeat every** - resend the alert every X minutes while the problem lasts. `0` means send it once and stay quiet.



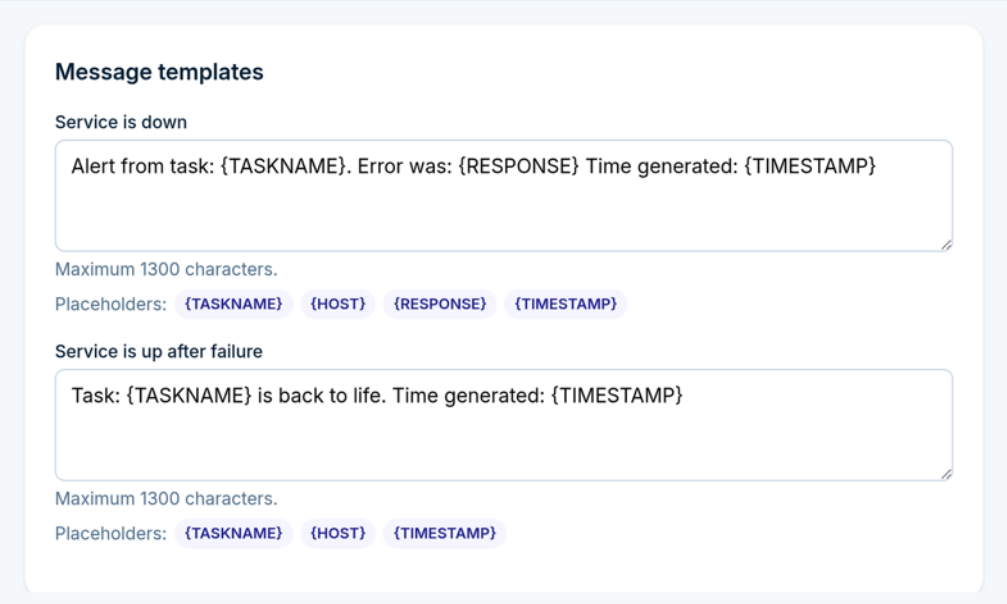
Alert triggers

Message templates

Write the text for each alert you enabled. Each message may be up to 1300 characters and can use placeholders:

Message	Placeholders available
Service is down	`{TASKNAME}`, `{HOST}`, `{RESPONSE}`, `{TIMESTAMP}`
Service is up after failure	`{TASKNAME}`, `{HOST}`, `{TIMESTAMP}`
SMS Text (SNMP)	`{TASKNAME}`, `{VALUE}`, `{TIMESTAMP}`
SMS Text (Modbus)	`{TASKNAME}`, `{VALUE}`, `{TIMESTAMP}`

For example, `DOWN: {TASKNAME} ({HOST}) at {TIMESTAMP}` produces a message that says what failed, where and when.



Message templates

Click **Create task**. The task starts being checked at the next monitoring run.

Part 2: Reports

Go to **Monitoring > Network Monitoring > Reports**.

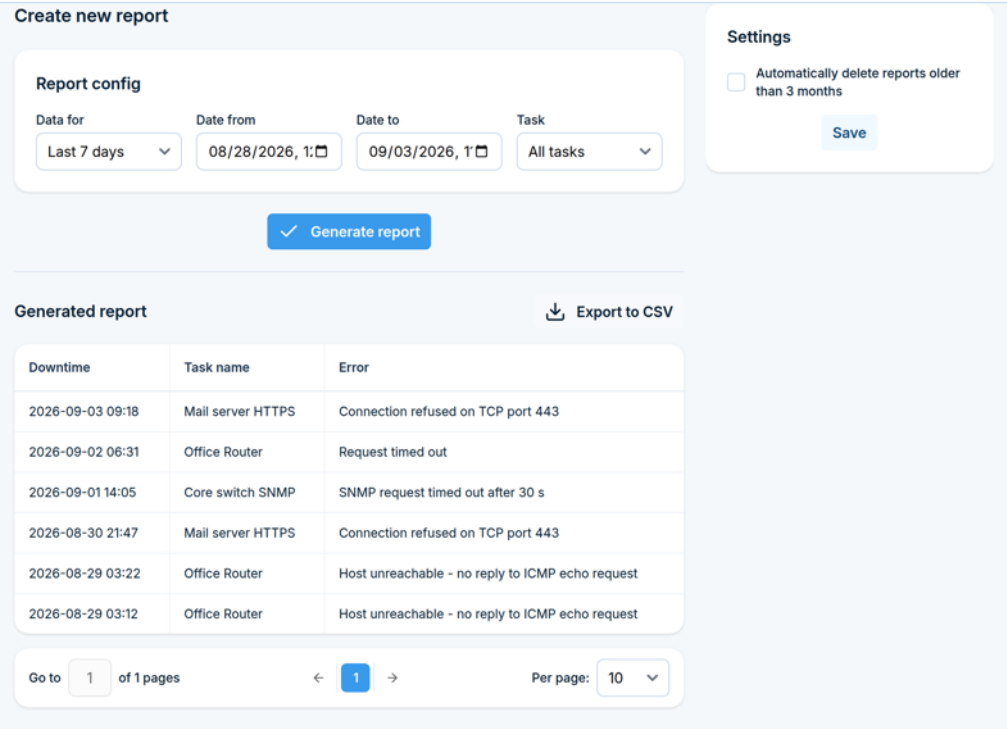
Generate a report

In the **Report config** box choose:

Field	What it does
Data for	A ready-made date range. Choosing one fills in the dates below.
Date from / **Date to**	The exact range. Editing these switches **Data for** to a custom range.
Task	A single task, or **All tasks**.

Click **Generate report**. The results appear below, listing the downtime, the task name and the error recorded for each incident.

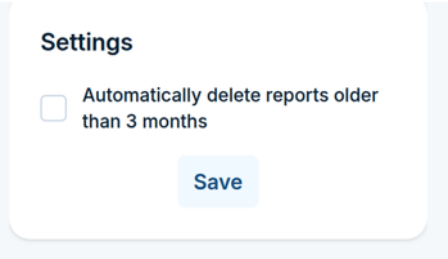
Click **Export to CSV** above the results to download them.



Generated report

Report retention

The box on the right holds one option, **Automatically delete reports older than 3 months**. Turn it on to stop the report history from growing indefinitely, then click **Save**.



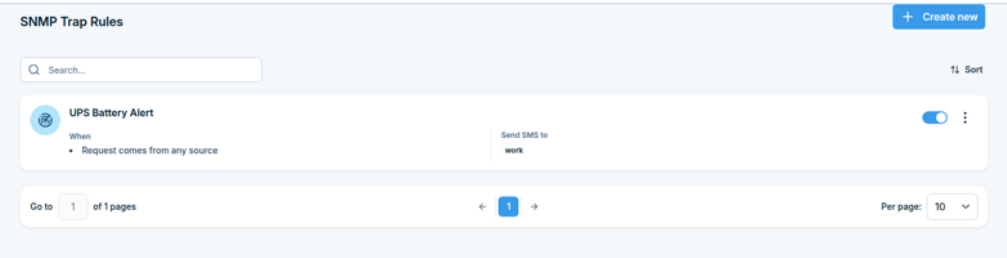
Report retention

Part 3: SNMP Traps

Tasks reach out and check things. SNMP trap rules work the other way round: another device sends a trap **to** the SMSEagle, and the rule turns it into an SMS.

Step 1: Open the SNMP Traps page

Go to **Monitoring > Network Monitoring > SNMP Traps**.



SNMP Trap Rules

Step 2: Create a rule

Click **Create new** in the top right corner. A side panel opens.

Name the rule

In **Rule name**, type something descriptive, for example `UPS battery trap`. Maximum 100 characters.

Decide which traps to act on

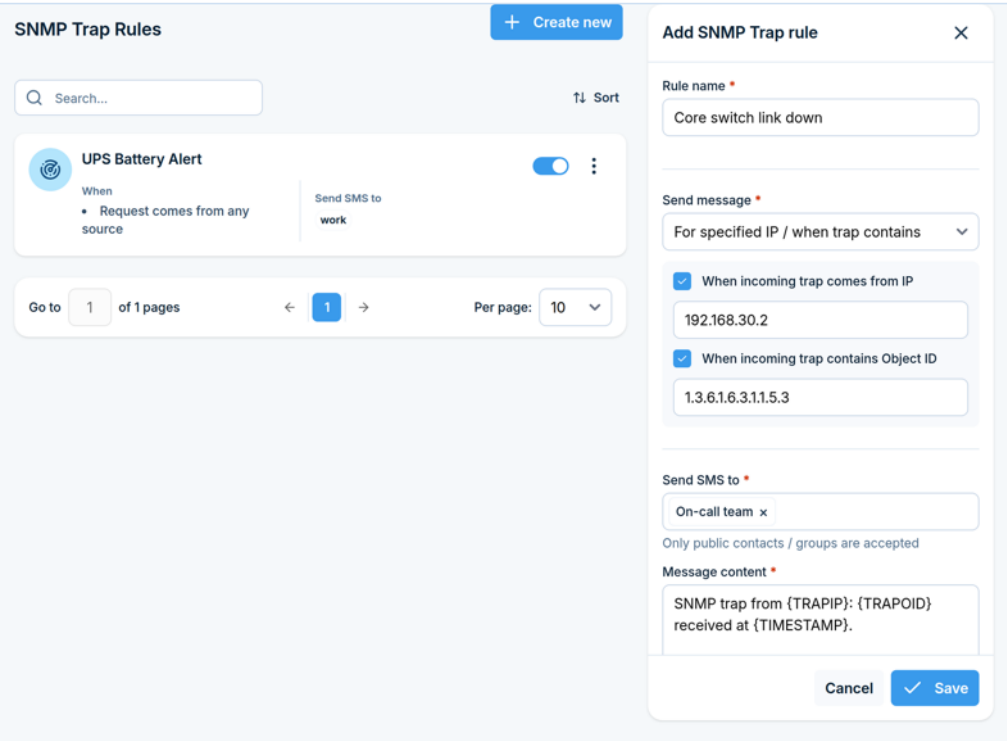
Choose **Send message**:

Option	What it means
Always send	Every trap the device receives triggers this rule.
For specified IP / when trap contains	Only traps matching the conditions below trigger it.

If you chose the second option, two conditions become available. You can use one or both, and a trap must satisfy every condition you enable.

When incoming trap comes from IP Tick this and type the IP address of the sending device.

When incoming trap contains Object ID Tick this and type the OID that must be present in the trap.



An SNMP trap rule with conditions

Choose the recipients and write the message

Send SMS to - select the contacts or groups. Only **public** contacts and groups are accepted.

Message content - the text to send, maximum 1300 characters. You can use these placeholders:

Placeholder	Replaced with
`{TASKNAME}`	The name of the rule
`{IP}`	The IP address the trap came from
`{TRAP}`	The content of the trap

Optional settings

- **Modem** (multi-modem devices only) - send through a specific SIM card instead of the default.
- **Call after sending SMS** - also place a voice call, with the same options as in tasks.

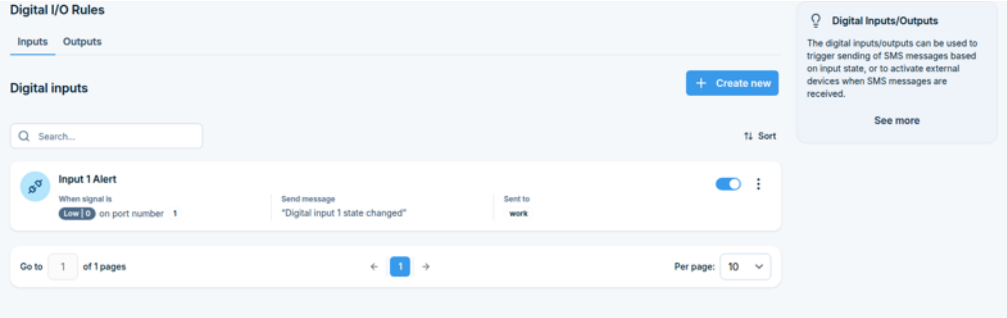
Click **Save**. The rule applies to traps received from now on.

How Network Monitor behaves

- Tasks are checked on the shared **Monitoring period**, so a task cannot alert faster than that interval allows.

- A “down” alert is sent once when the state changes, and then repeated only if you set **Repeat every**.
- A task linked to a parent is skipped entirely while the parent is down, so its own alerts stay silent until the parent recovers.
- If several SNMP trap rules match the same trap, **each** of them sends its own SMS.

Digital Input / Output



Digital Input/Output overview

What this feature does

Digital inputs and outputs are physical ports that let SMSEagle talk to the world outside the network:

Direction	What it does
Input	A voltage change on an input port (a door contact closing, an alarm relay tripping, a UPS reporting a fault) makes the device send an SMS.
Output	An incoming SMS makes the device switch an output port on or off, so it can start a siren, open a gate or reset a machine.

You configure this with **rules**. An Input rule says “when port 2 goes high, text the maintenance team”. An Output rule says “when an SMS containing OPEN arrives, set port 1 high for 5 seconds”.

> **MHD-8100 has no built-in digital input or output ports.** To use this feature, connect the **Digital I/O Extender** accessory (product code ACCDPIOKIT) to the device. It is a USB module with 32 ports, each configurable as an input or an output, with all signals on screw terminals. See Accessories for details and ordering.

Beside the rules there is one page that shows the ports themselves: **External pins**, where you define and control the ports of the Digital I/O Extender.

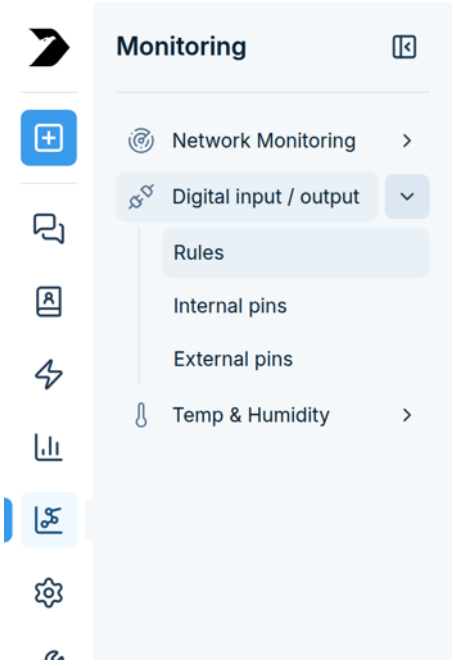
Before you start

- Connect the Digital I/O Extender to the device and wire your equipment to its terminals. Then define the ports you use on the **External pins** page (see Part 3 below). The port lists in the rule forms only offer ports defined there.
- The device must be able to send SMS. Check that at least one modem is connected and registered on the network.
- Recipients of Input rules must be marked as **Public** in the Phonebook.

Where to find it

In the sidebar, go to **Monitoring > Digital input / output**. It has two pages:

Page	What it is for
Rules	Create the Input and Output rules. This is where you spend most of your time.
External pins	Define and control the ports of the Digital I/O Extender.

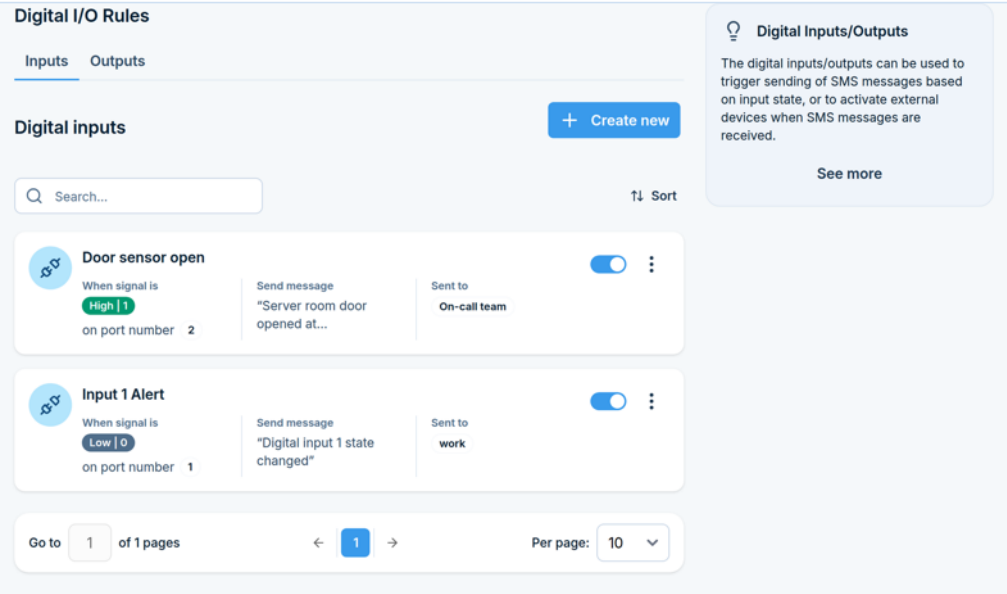


Where to find the Digital I/O pages

Part 1: Input rules (input signal into SMS)

Step 1: Open the rules page

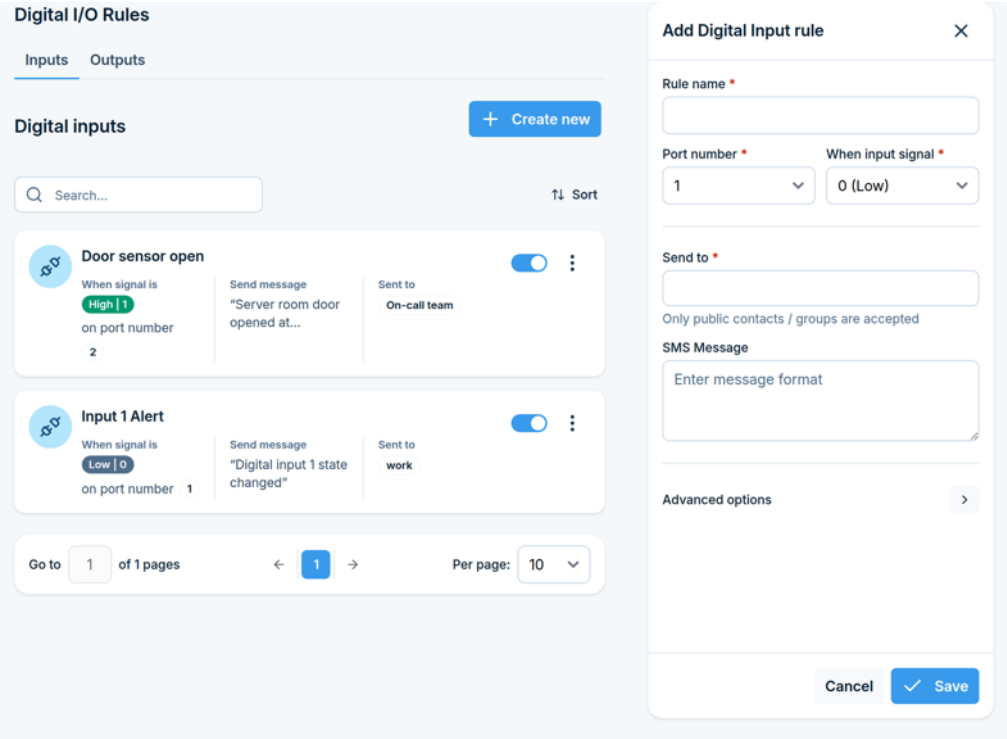
Go to **Monitoring > Digital input / output > Rules** and make sure the **Inputs** tab is selected.



Digital input rules

Step 2: Create an Input rule

Click **Create new** in the top right corner. A side panel opens.



A new digital input rule

Name the rule

In **Rule name**, type something descriptive, for example `Server room door opened`. Maximum 100 characters.

Choose the port and the signal

Field	What to enter
Port number	The input port the equipment is wired to. The list shows the Digital I/O Extender ports defined on the **External pins** page, marked `(Ext)`.
When input signal	`0 (Low)` or `1 (High)`. This is the state that triggers the rule.

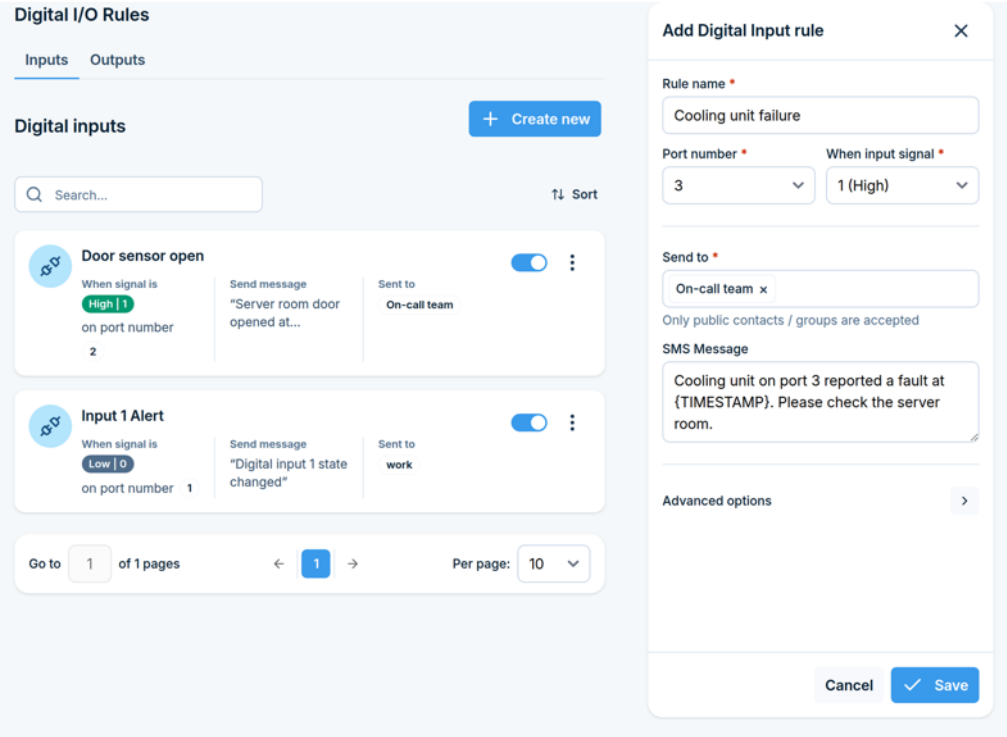
Pick the value that represents the alarm condition on your equipment. Which value that is depends on the contact type (NO or NC) and on how it is wired to the Digital I/O Extender. To check it, trigger the alarm condition once and read the state of the port on the **External pins** page.

Choose the recipients

In **Send to**, select the contacts or groups that should receive the SMS. Only **public** contacts and groups can be selected here. This field is required.

Write the SMS text

SMS Message is the text that is sent when the rule fires. Maximum 1000 characters. The same text goes to every recipient, so name the location or the machine in it, for example `ALARM: server room door opened`.

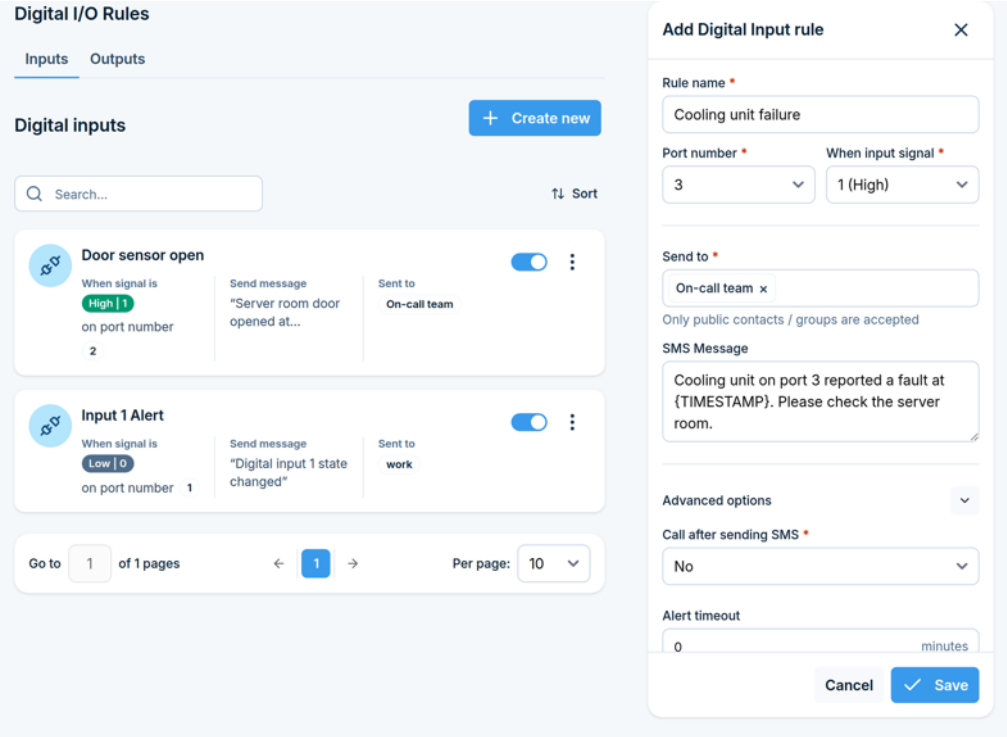


A completed input rule

Advanced options

Click **Advanced options** to expand this section. You do not need it for a basic setup.

- **Call after sending SMS** - also place a voice call to the same recipients. Options are **No**, **Ring**, **Text-to-speech (TTS)** and **Text-to-speech (advanced)**, depending on what your device model supports. With the advanced option you also pick a **Voice model**.
- **Alert timeout** - the number of minutes that must pass before the same rule may alert again. `0` means no limit, so every signal change sends an SMS.



Input rule advanced options

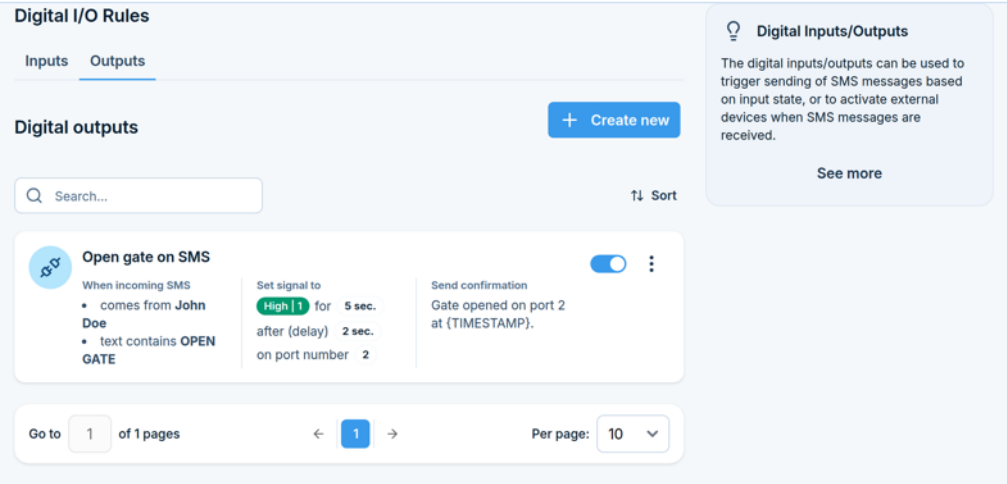
Set an alert timeout for noisy inputs. A contact that flutters, or equipment that trips repeatedly, can produce a burst of messages. A timeout of a few minutes keeps one real event to one SMS.

Click **Save**. The rule starts working on signal changes from now on.

Part 2: Output rules (SMS into output signal)

Step 1: Open the rules page

Go to **Monitoring > Digital input / output > Rules** and choose the **Outputs** tab.



Digital output rules

Step 2: Create an Output rule

Click **Create new** in the top right corner. A side panel opens.

Name the rule and pick the port

In **Rule name**, type something descriptive, for example `Open gate on SMS`. Maximum 100 characters. In **Port number**, choose the output port your equipment is wired to. The list shows the Digital I/O Extender ports defined on the **External pins** page, marked `(Ext)`.

Decide which SMS messages trigger the rule

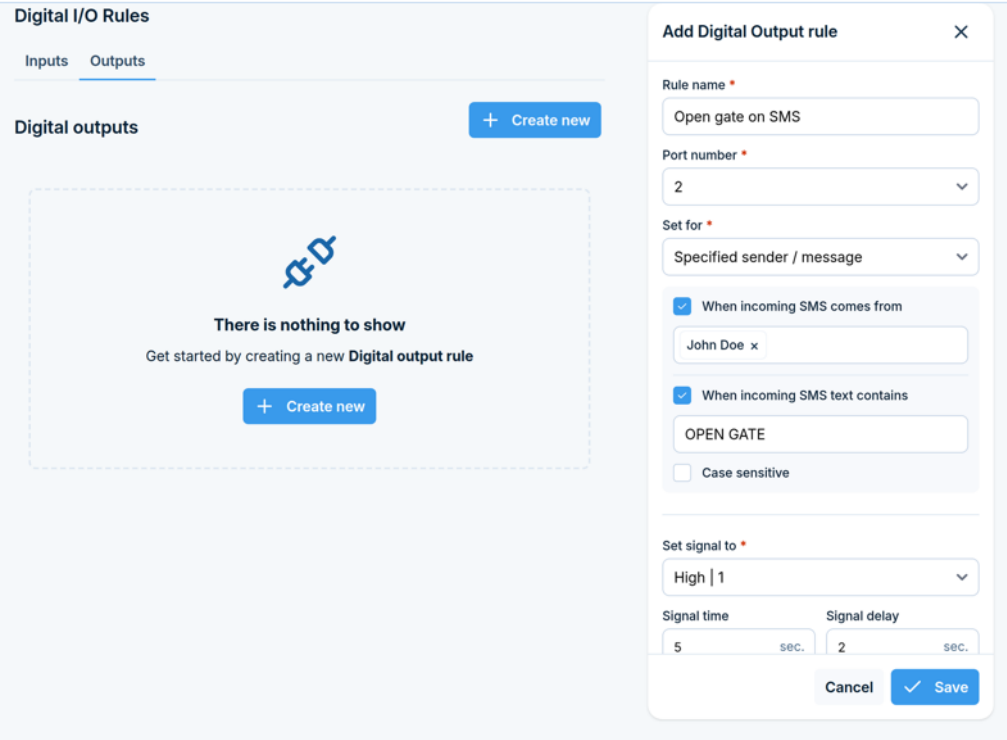
Choose **Set for**:

Option	What it means
All incoming messages	Every incoming SMS switches the output.
Specified sender / message	Only messages matching the conditions you set below switch it.

If you chose **Specified sender / message**, two conditions become available. You can use one or both. When you use both, a message must satisfy **both**.

When incoming SMS comes from Tick this and select the sender contacts or groups.

When incoming SMS text contains Tick this and type the phrase in **Text**, for example `OPEN`. Tick **Case sensitive** if `open` and `OPEN` should be treated as different.



Output rule conditions

Restrict output rules by sender. An output rule switches physical equipment. Without a sender condition, anybody who knows your number can operate it.

Decide what the output does

Field	What it means
Set signal to	`Low | 0` or `High | 1`. The state the port is switched into.
Signal time	How many seconds the port stays in that state before returning. `0` means it stays there indefinitely.
Signal delay	How many seconds to wait after the SMS arrives before switching the port.

Advanced options

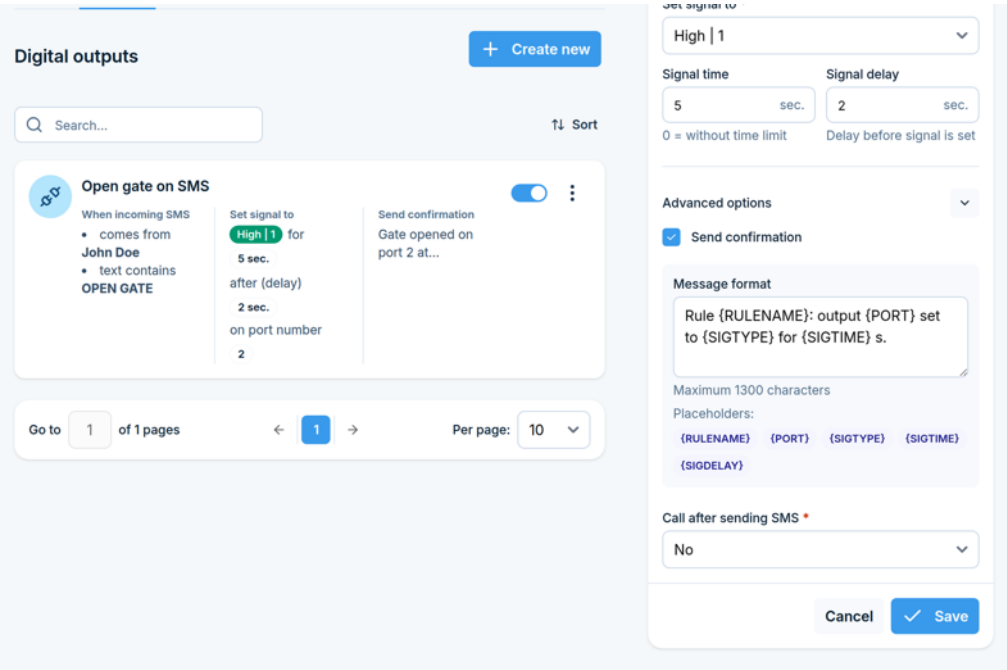
Click **Advanced options** to expand this section.

Send confirmation Tick this to send an SMS back to the sender after the output has been switched. The **Message format** field appears, maximum 1300 characters. You can build the text from placeholders:

Placeholder	Replaced with
{RULENAME}	The name of the rule that fired
{PORT}	The output port number
{SIGTYPE}	The signal the port was set to
{SIGTIME}	The signal time in seconds
{SIGDELAY}	The signal delay in seconds

For example, `{RULENAME}: port {PORT} set to {SIGTYPE} for {SIGTIME}s` produces a clear receipt for the person who sent the command.

Call after sending SMS Also place a voice call, exactly as described for Input rules above.



Output rule confirmation message

Click **Save**. The rule starts working on messages received from now on.

Part 3: External pins

External pins are the ports of the Digital I/O Extender connected to the device. On MHD-8100 these are the only digital input and output ports.

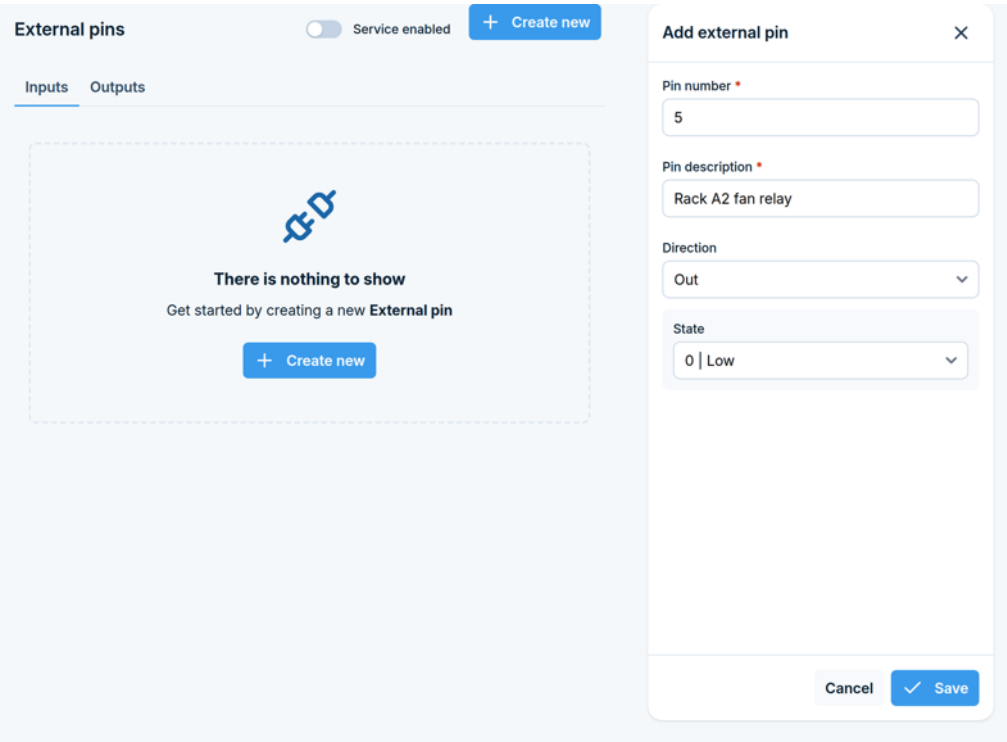
Go to **Monitoring > Digital input / output > External pins**. The page has an **Inputs** tab and an **Outputs** tab, plus a **Service enabled** switch that starts and stops the io-bridge service, which reads and drives the Digital I/O Extender ports. **While it is off, Input and Output rules do not work.**

Add an external pin

Click **Create new**. A side panel opens.

Field	What to enter
Pin number	The port number on the Digital I/O Extender, for example `1`. Each number can only be configured once.
Pin description	A short name, maximum 64 characters. Only letters, digits and spaces are allowed.
Direction	**In** for a port you read, **Out** for a port you drive.
State	Only shown for **Out** pins: the state the port starts in, `1 | High` or `0 | Low`.

Click **Save**.



Adding an external pin

Use the pins

- On the **Outputs** tab you can flip a pin's state directly from the list.
- On the **Inputs** tab the state is read-only, because the value is driven by whatever is wired to the pin.
- Once defined, external pins also appear in the **Port number** lists of Input and Output rules, marked `(Ext)`.

- The **Inputs** tab shows the live state of each input, which is useful for checking your wiring before you write a rule.

How Digital I/O rules behave

- Rules only act on events that happen after the rule was created and enabled. Use the switch next to a rule to pause it without deleting it.
- If several rules match the same event, **each** of them runs, so one input signal can send several messages and one SMS can switch several ports.
- The text condition on Output rules is a **contains** match, not an exact match.
- Rules need the **External pins** service on.

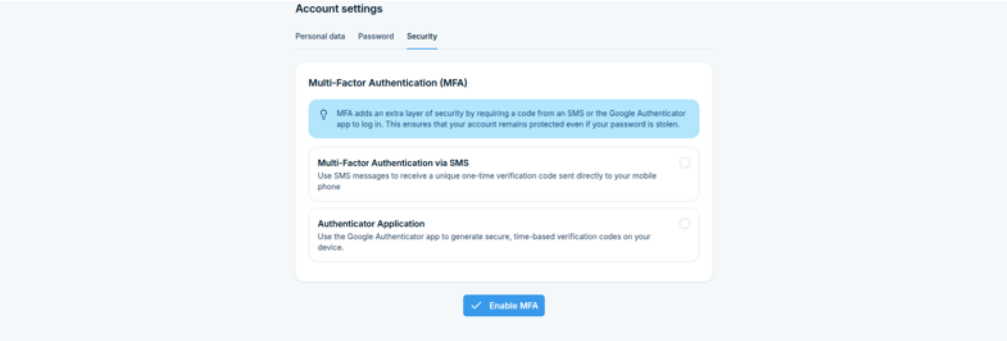
Settings

This chapter covers the **Settings** section of the web interface, following the same second-level menu you see in the sidebar.

Account settings

Click your avatar (bottom-left) and choose **Account settings** to manage your own account, under three tabs: **Personal data** (name, login, phone number, interface language, compose defaults, notification sound), **Password**, and **Security** - see Web Interface Overview for the full tab layout.

How to configure Multi-Factor Authentication (MFA)



MFA setup under Account settings > Security

MFA adds an extra layer of security by requiring a one-time code, in addition to the password, to sign in. This keeps the account protected even if the password is stolen.

Where to find it

- **Per user**: **Account settings > Security** (`/settings/account/security`), for your own account.
- **Device-wide**: the **Two-factor authentication** option on the Administrator step of the Configuration Wizard, and when creating or editing a user under **System > Users**.

Step 1: Choose an MFA method

Under **Account settings > Security**, choose one of:

- **Multi-Factor Authentication via SMS** - a one-time verification code is sent to your mobile phone by SMS at each sign-in.
- **Authenticator Application** - time-based codes are generated by an app such as Google Authenticator.

Click **Enable MFA** and follow the on-screen steps to confirm the chosen method.

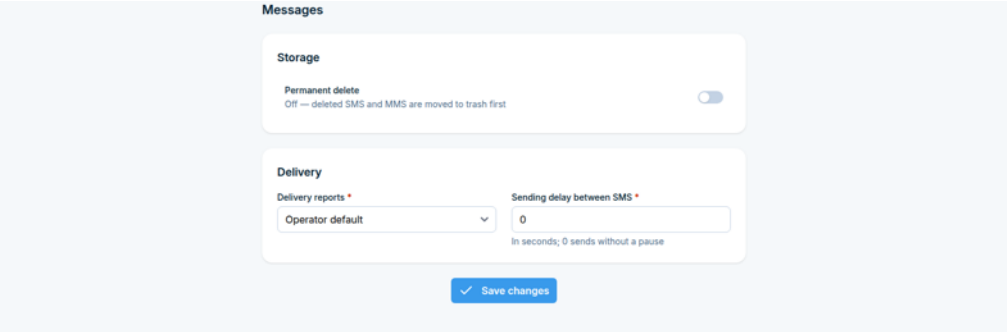
Step 2: Enforce MFA device-wide (optional)

An administrator can require MFA for every account instead of leaving it optional per user. Under **Administrator** in the setup wizard (or per user under **System > Users**), set **Two-factor authentication** to:

- **Do not enforce** - each user decides individually whether to enable MFA.
- **Enforce for all users** - every existing and new user must set up MFA.
- **Enforce for new users** - MFA is required only for accounts created from now on.

SMS / MMS

Messages



Messages settings under SMS / MMS

Settings > SMS / MMS > Messages (`/settings/sms-mms/messages/`) groups the general behavior of the SMS/MMS storage and delivery pipeline.

Storage

Permanent delete - off by default, so deleted SMS and MMS are moved to Trash first instead of being removed immediately.

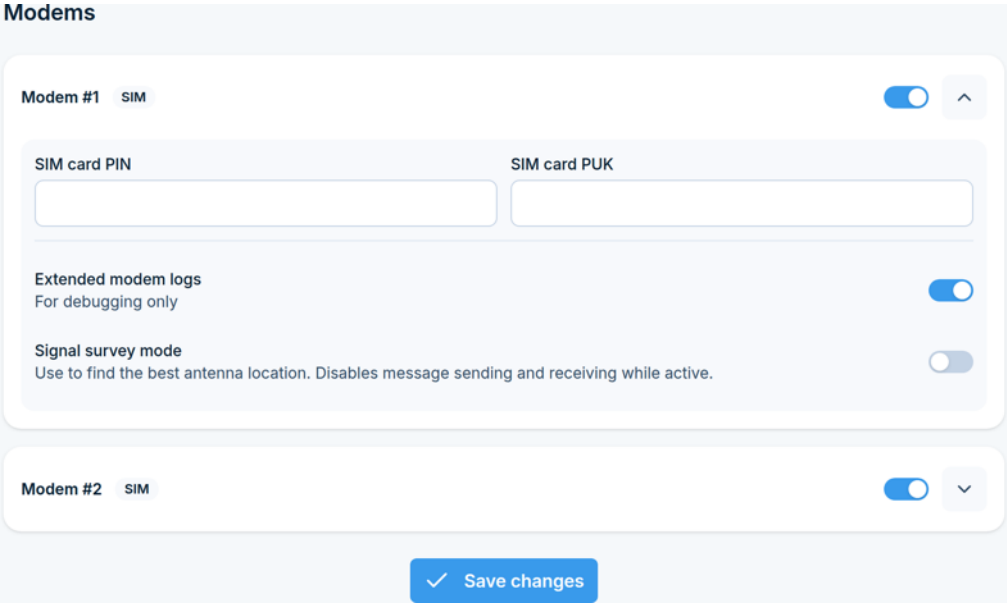
Delivery

Delivery reports let you find out whether a sent SMS actually reached the recipient's phone.

- **Delivery reports** - Operator default (use whatever behavior your mobile operator applies by default), Always request, or Never request. Also offered during the Configuration Wizard.
- **Sending delay between SMS** - a pause, in seconds, inserted between consecutive outgoing SMS. `0` sends without a pause.

When a delivery report is requested, SMSEagle updates the message's status in Sent Items / Outbox once the network confirms delivery (or reports a failure), and the report becomes visible in the message's details.

Modems



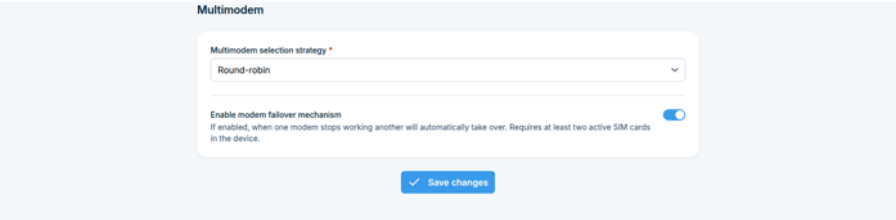
Modems settings, with the first modem's section expanded

Settings > SMS / MMS > Modems (`/settings/sms-mms/modems/`) lists each built-in modem (Modem #1, Modem #2 on multi-modem devices) with a switch to enable its SIM. Expanding a modem's section reveals four settings:

- **SIM card PIN** and **SIM card PUK** - only needed if the card asks for them. The same two fields are offered during the Configuration Wizard.
- **Extended modem logs** - verbose modem logging, for debugging only.
- **Signal survey mode** - use it to find the best antenna location. It **disables message sending and receiving** while active, so turn it off when you are done.

Multimodem

Settings > SMS / MMS > Multimodem (`/settings/sms-mms/multimodem/`) decides which of the device's eight built-in modems sends each outgoing SMS, and whether another modem takes over when one stops working. The page is available to administrators only.

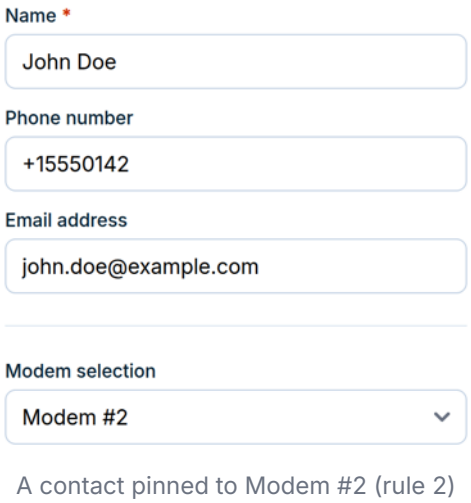


Multimodem settings, shown here on a two-modem device. MHD-8100 lists SIM 1 to SIM 8

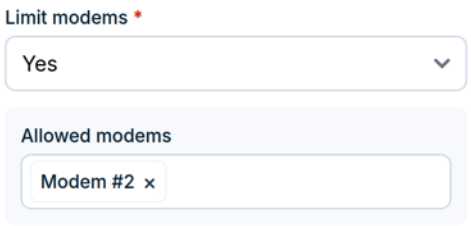
How SMSEagle picks a modem

The two settings on this page are only part of the decision. For every outgoing SMS, SMSEagle checks these rules in order:

1. **A modem chosen for the message.** When the sender picks a modem, for example in Compose, with the modem parameter of an API call, or in an Automation rule limited to one modem, that modem is used and nothing below applies. The sender must be allowed to use it (see rule 3), otherwise the message is rejected.
2. **A modem pinned to the contact.** When the message goes to a Phonebook contact whose **Modem selection** is set, that modem is used and nothing below applies.
3. **The sender's allowed modems. Limit modems** in the user's settings under **System > Users** restricts the user to the **Allowed modems** listed there. Without a limit, the user may use every modem. Modems whose SIM is switched off under Modems are left out, unless that would leave none.
4. **The selection strategy** picks one of the allowed modems. See Multimodem selection strategy below.
5. **Modem failover**, when enabled, swaps the picked modem for the next working one if the picked modem is not working at that moment. See Modem failover below.



A contact pinned to Modem #2 (rule 2)



A user limited to Modem #2 (rule 3)

Multimodem selection strategy

Multimodem selection strategy offers **Round-robin** and one **SIM N as Master modem** option for each built-in modem (**SIM 1** to **SIM 8**):

- **Round-robin** - the sender's allowed modems take turns: modem 1 > modem 2 > ... > modem 8 > modem 1, and so on. Each user has a rotation of their own, so two users sending at the same time do not move each other's turn.
- **SIM N as Master modem** - modem N sends every message, and the other modems are used only by modem failover, when modem N is not working. A user who is not allowed to use modem N cannot send with this strategy, except for messages with a modem chosen for them (rule 1) or to a contact pinned to a modem (rule 2). Their messages are rejected with a missing modem access error.

Modem failover

Turn on **Enable modem failover mechanism** so that a working modem takes over from one that stops working. This requires at least two active SIM cards in the device. Failover acts at two moments:

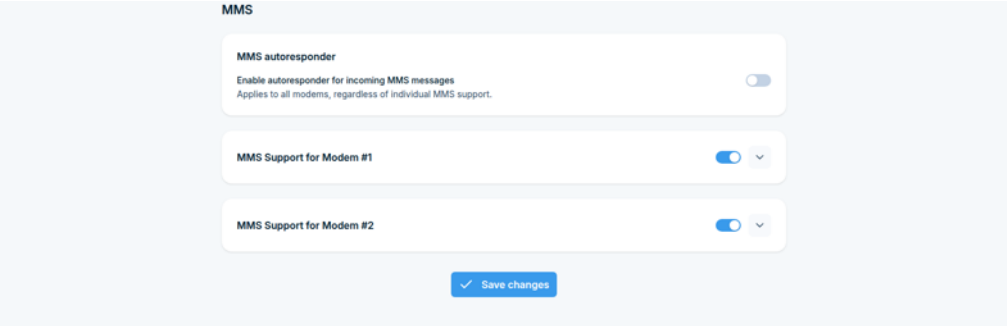
- **When a message is sent.** If the modem picked by the strategy is not working, SMSEagle tries the next of the sender's allowed modems, in modem number order and starting again from the first after the last one, and uses the first working one. Messages with a modem chosen for them (rule 1) or to a pinned contact (rule 2) are not redirected at this point.
- **Every 2 minutes.** SMSEagle checks all modems. Messages still waiting in the Outbox of a modem that is not working are moved to the next working modem that the message's author is allowed to use. If there is no such modem, the messages stay where they are.

A modem counts as not working when any of these is true:

- it has not reported to the device for more than 4 minutes,
- its SIM card is not ready, for example missing or waiting for a PIN,
- the device's watchdog, which checks every modem every 2 minutes, has restarted its modem service at least 3 times in quick succession (less than 5 minutes apart), the last time within the past 5 minutes,
- messages on it keep failing: at least one message in its queue has been retried 3 times, and the modem has sent nothing successfully in the last 5 minutes. When other messages in the same queue have not reached 3 retries, the problem is taken to be with the failing recipients, not with the modem.

Every redirected message is recorded in the **Application** log under **System > Logs**, as a line starting with `Modem: Modem failover triggered`.

MMS



MMS settings

What this feature does

MMS lets the device send and receive **multimedia messages**: a text with images or other files attached, rather than plain SMS.

Unlike SMS, MMS does not travel over the plain GSM channel. It goes through the operator's data network to an MMS centre, so each SIM card needs its own set of connection parameters (APN, MMSC and optionally a proxy). In SMSEagle those parameters are set **per modem**, under **Settings > Channels > SMS / MMS > MMS**.

The same screen also holds the **MMS autoresponder**, which sends an automatic reply to every incoming MMS.

Before you start

- You need the MMS settings for each SIM card from its operator: **APN**, **MMSC** address, and a **proxy** with **port** if the operator uses one. Some operators also require a username and password.
- The SIM must have MMS enabled on the tariff. A SIM that can text but has no data or MMS service will fail no matter how the settings are filled in.
- Many operator profiles are already known to the device, so try **Read APN settings** before you go looking for the values yourself.

Step 1: Open the MMS page

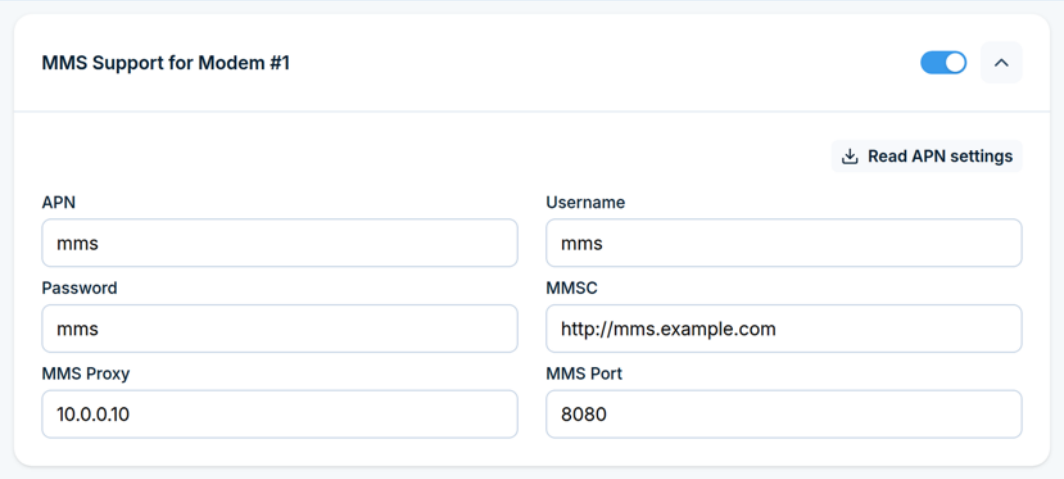
In the sidebar, go to **Settings > Channels > SMS / MMS > MMS**.

The MMS page shows the **MMS autoresponder** box at the top, then one collapsible section per modem, headed **MMS Support for Modem #1**, **#2** and so on, as in the figure at the start of this section.

Step 2: Enable MMS on a modem

Each modem section has a switch next to its heading. Turn it on for every SIM that should handle MMS.

Then click the arrow on the right of the heading to expand the section and fill in the connection parameters.



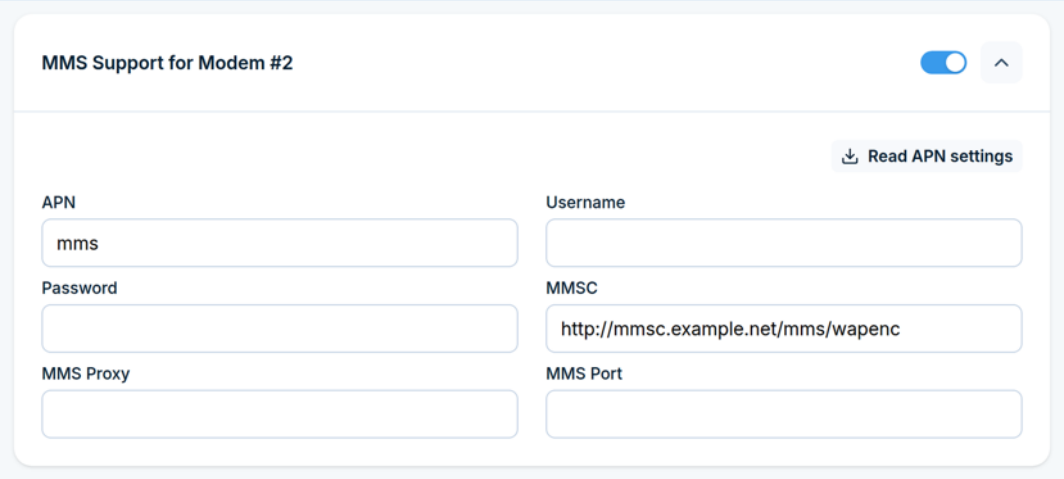
An expanded modem section, with **Read APN settings** above the fields

Step 3: Fill in the connection parameters

The quickest route is the **Read APN settings** button at the top of the expanded section. It looks up a matching configuration for the SIM currently in that modem and fills the fields in for you. If no match is found, SMSEagle reports it and you enter the values by hand.

Field	What to enter
APN	The operator's access point name, for example `internet`.
Username	The APN user, if the operator requires one. Leave empty otherwise.
Password	The APN password, if required.
MMSC	The address of the operator's MMS centre, for example `http://mms.example.com`.
MMS Proxy	The proxy address, if the operator uses one. Leave empty otherwise.
MMS Port	The proxy port. Only needed together with a proxy.

Every field belongs to **that one modem**. Two SIM cards from different operators need two different sets of values, so repeat this for each modem you enabled.



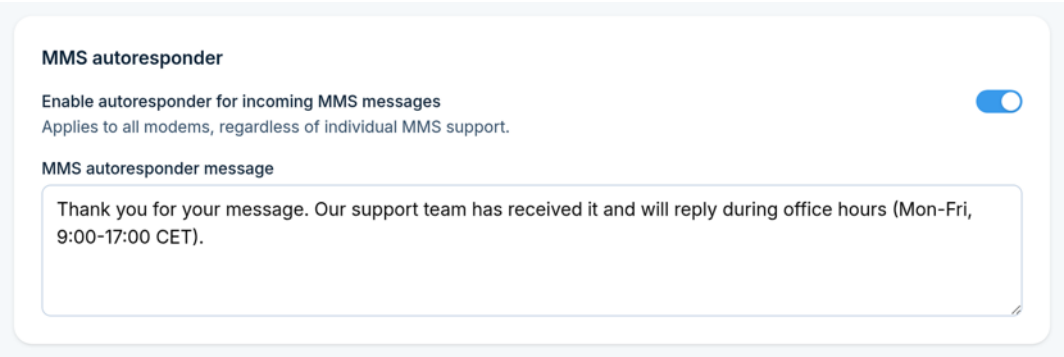
The second modem carries its own values, and needs no proxy in this example

Step 4: Set up the autoresponder (optional)

The **MMS autoresponder** box at the top of the MMS page sends an automatic reply whenever an MMS arrives.

1. Turn on **Enable autoresponder for incoming MMS messages**.
2. Type the reply in **MMS autoresponder message**.

The autoresponder **applies to all modems, regardless of individual MMS support**. It is a single global setting, not a per-modem one, and there is one reply text shared by every incoming MMS, so keep the wording general.



The autoresponder, enabled with a sample reply

Step 5: Save and reboot

Click **Save changes**.

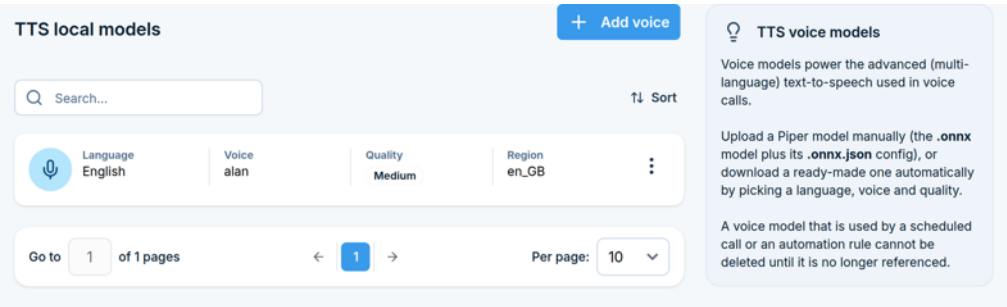
> **A reboot is needed.** After saving, SMSEagle asks you to reboot the device so the MMS changes take effect. Until you do, the new parameters are stored but not yet in use.

Calls

TTS local models

Local voice models power **Text to speech - advanced**. They run on the device, so no internet connection is needed once a model is installed.

Go to **Settings > Channels > Calls > TTS local models**. The page lists the installed models with their language, region and quality.



TTS local models

Add a model

Click **Add voice** in the top right corner. The panel offers two ways to do it.

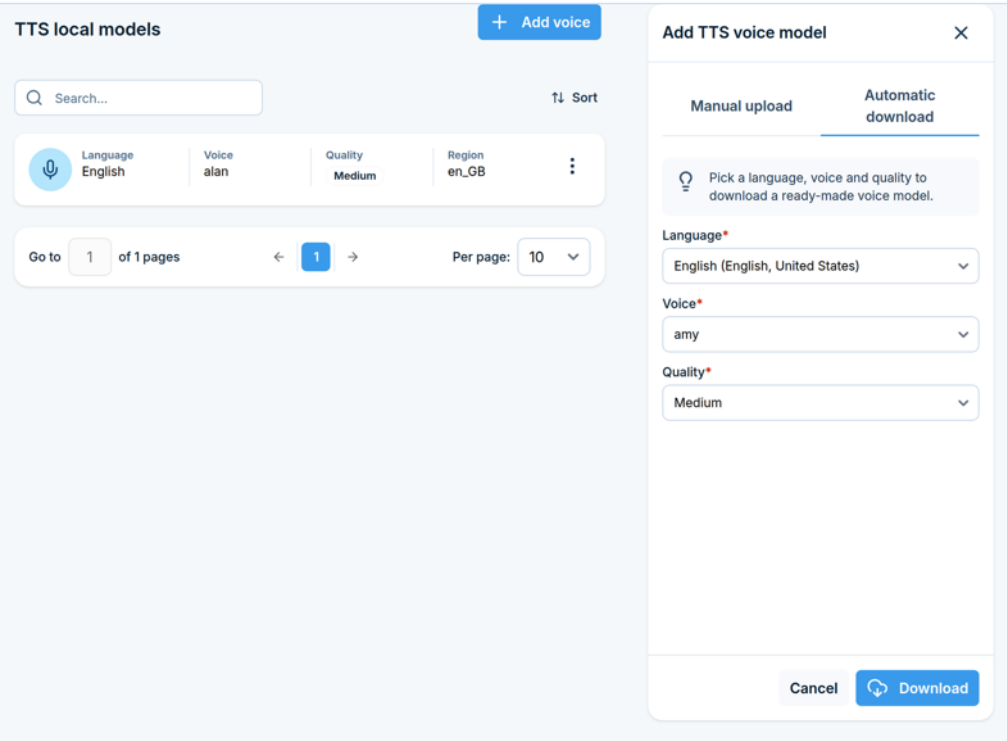
Automatic download (the easy way)

On the **Automatic download** tab, pick in order:

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

Click **Download**. A progress bar shows the download, and the model appears in the list when it finishes.

Higher quality means a more natural voice but a larger file and slightly slower synthesis. **Medium** is a good default.



Downloading a ready-made voice model

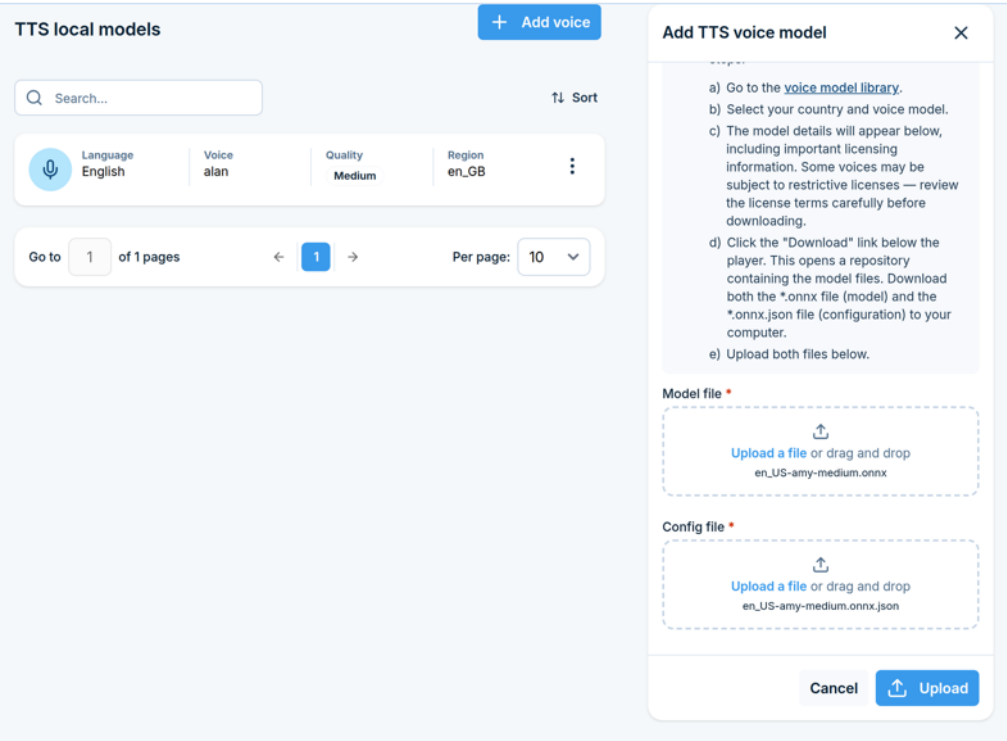
If the panel reports “Voice list unavailable”, the device could not reach the online voice catalogue. Check the network settings and try again later, or use manual upload instead.

Manual upload

On the **Manual upload** tab you provide a voice model yourself:

1. **Model file (.onnx)** - the model itself.
2. **Config file (.onnx.json)** - its matching config file.

Both files are required and must belong together. Click **Upload**.



Uploading a Piper model manually

Delete a model

Use the **Delete** action next to a model, or tick several and delete them together.

A model that is still referenced somewhere cannot be deleted. The message tells you where it is used, for example in a scheduled call, an Email to SMS rule, a digital input or output action, or a Network Monitor task. Change or remove that reference first, then delete the model.

TTS online models (ElevenLabs)

Online models produce the most natural-sounding speech, but they use the ElevenLabs API, so they require an ElevenLabs account and an internet connection.

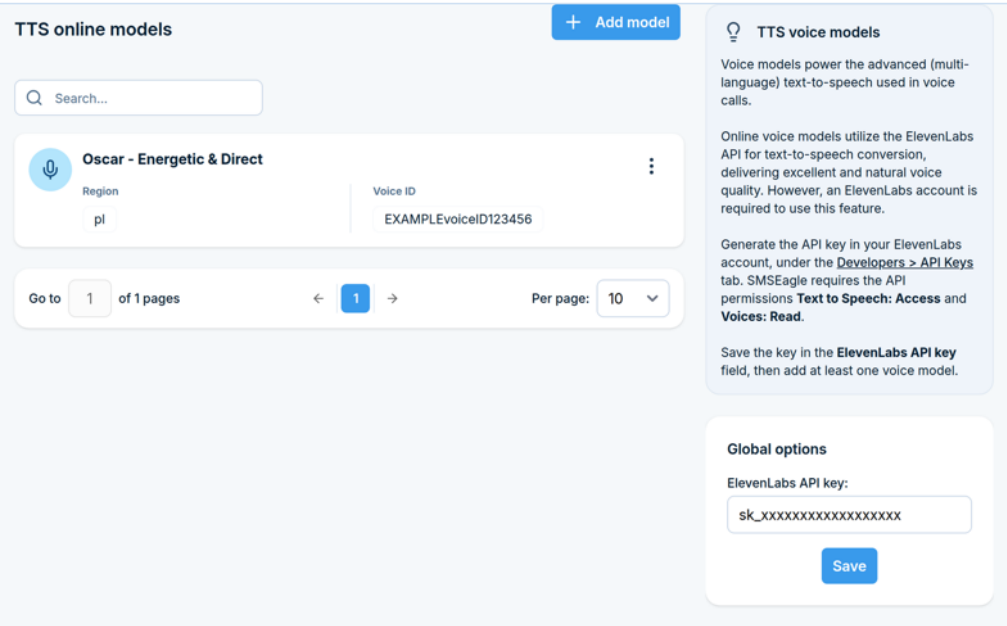
Go to **Settings > Channels > Calls > TTS online models**.

Step 1: Prepare the ElevenLabs account

In your ElevenLabs account:

1. Go to **Developers > API Keys** and generate an API key.
2. Give the key the permissions **Text to Speech: Access** and **Voices: Read**, then save.
3. Go to the **Voices** tab, choose the voice you want and add it to your account.
4. Open **My Voices** and copy the **voice ID** of that voice.

The page has a button that takes you straight to the ElevenLabs settings.



TTS online models

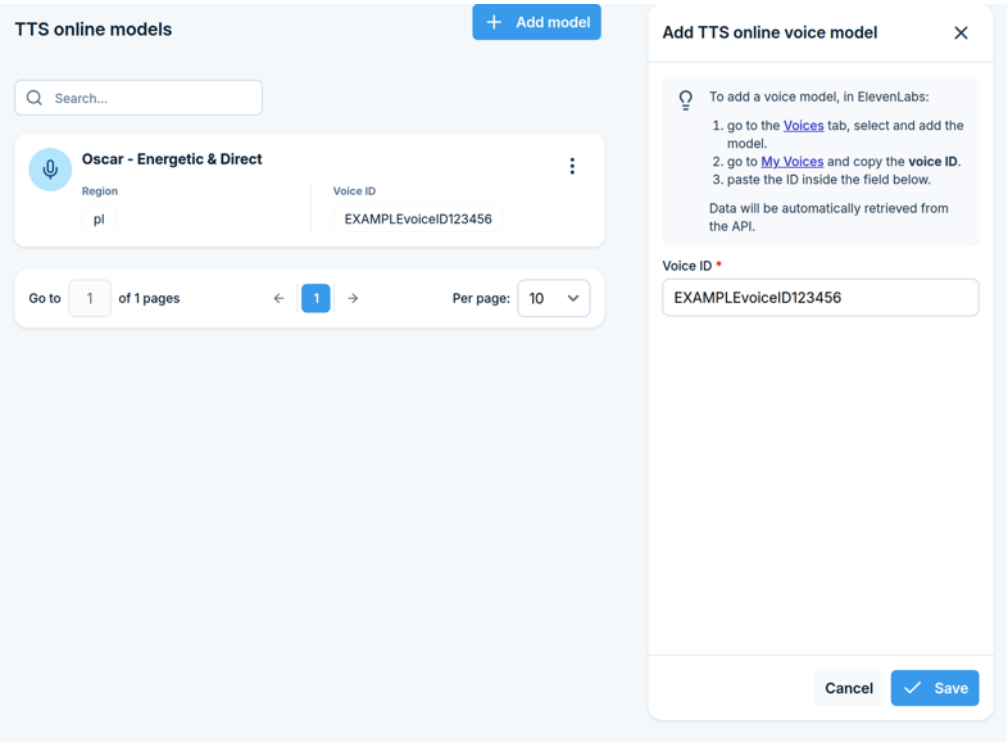
Step 2: Save the API key

In the **Global options** box on the right, paste the key into **ElevenLabs API key** and click **Save**.

Step 3: Add a voice model

Click **Add model** in the top right corner, paste the **Voice ID** you copied and click **Save**.

The rest of the model data (name, language, region) is fetched from the API automatically and shown in the list.



Adding an ElevenLabs voice model

Models can be edited (to point at a different voice ID) or deleted from the list, individually or in bulk.

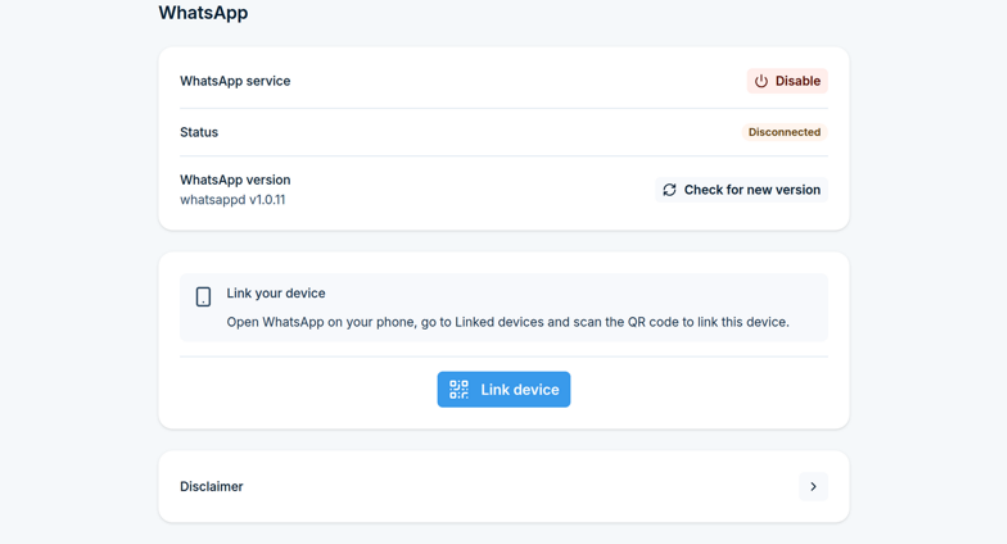
Incoming calls

Settings > Channels > Calls > Incoming calls (`/settings/calls/incoming-calls`) sets, per modem, how an inbound voice call is handled: **Always accept**, **Always reject**, or **Ignore**.

Call forward

Settings > Channels > Calls > Call forward (`/settings/calls/call-forward`) manages call-forwarding codes per modem. Not every network carrier supports forwarding codes - check with your operator before relying on this.

WhatsApp



WhatsApp settings and device linking

What this feature does

WhatsApp support lets your SMSEagle send and receive **WhatsApp messages** in addition to SMS. The device is linked to a WhatsApp account the same way a desktop or browser session is: you scan a QR code with the phone that owns the account.

Once linked, WhatsApp becomes another channel you can pick when composing a message, with its own conversation view. There is also a **fallback** option, which sends an SMS or MMS instead whenever a recipient turns out not to have WhatsApp.

Typical uses: reaching people who use WhatsApp, sending longer notifications without splitting them into several SMS parts, or cutting the cost of messages to recipients abroad.

Setting it up is a two-part job: first you enable the service and link a device (**Settings > Channels > WhatsApp**), then you use the channel (**Messages > WhatsApp**, or the Compose window).

Before you start

- WhatsApp is available on selected device models only. If **Settings > Channels > WhatsApp** is not in your sidebar, your device does not support it.
- You need a phone with an active WhatsApp account, in your hands, to scan the QR code.
- The device must be able to reach the internet. WhatsApp messages travel over the network connection, not through the modem.

> **The linked account is a real WhatsApp account.** Everything the gateway sends appears to come from that account, and messages sent to it appear in SMSEagle.

Step 1: Open the WhatsApp settings

In the sidebar, go to **Settings > Channels > WhatsApp**.

The **Connection** box shows the installed **WhatsApp version** and the current **Status**. On a fresh device the status is **Disabled** and a warning explains that the service must be enabled before a device can be linked.

Step 2: Enable the service

Click **Enable** at the bottom of the page. The status changes to **Disconnected**, which means the service is running but no account is linked yet. That is the state shown in the figure at the start of this section, with the **Link device** button waiting below the Connection box.

Step 3: Link your phone

1. Click **Link device**. A QR code appears on screen.
2. On your phone, open **WhatsApp**, go to **Linked devices** and choose to link a new device.
3. Point the phone at the QR code on screen.

While the code is displayed, the page keeps checking whether it has been scanned and refreshes the code by itself. When the phone confirms, the status changes to **Connected**.

> **The QR code does not wait forever.** If nothing scans it within a short time, linking is cancelled and the page returns to **Disconnected**. Have the phone open on the **Linked devices** screen before you click **Link device**, and simply click it again if the code expires.

You can also stop the process yourself with **Cancel linking**.

Step 4: Decide what happens to non-WhatsApp recipients

Once the status is **Connected**, a **Fallback** box appears with one switch:

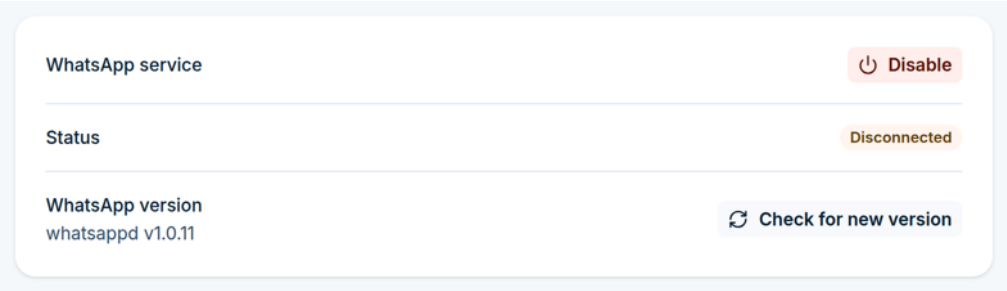
Fall back to SMS/MMS When it is on, a message addressed to a number that is not registered on WhatsApp is sent as an SMS or MMS instead of failing. When it is off, such a message is simply not delivered.

The switch is saved as soon as you flip it, there is no separate save button.

Step 5: Keep the service up to date

The **Connection** box has a **Check for new version** button. Click it to ask whether a newer WhatsApp version is available:

Result	What to do
No new version found	Nothing. You are current.
A new version is available	The button turns into **Update now**, which takes you to the patch page where the update can be installed.
Could not fetch the newest version	The device could not reach the update server. Check the network settings and try again later.



The Connection box, with **Check for new version** beside the installed version

Unlinking and switching off

Two buttons at the bottom of the settings page do different things:

Button	What it does
Unlink device	Logs the account out. The service keeps running, the page returns to **Disconnected** and you can link another account. **Fall back to SMS/MMS** is turned off at the same time.
Disable	Stops the WhatsApp service altogether. The channel disappears from the Compose window.

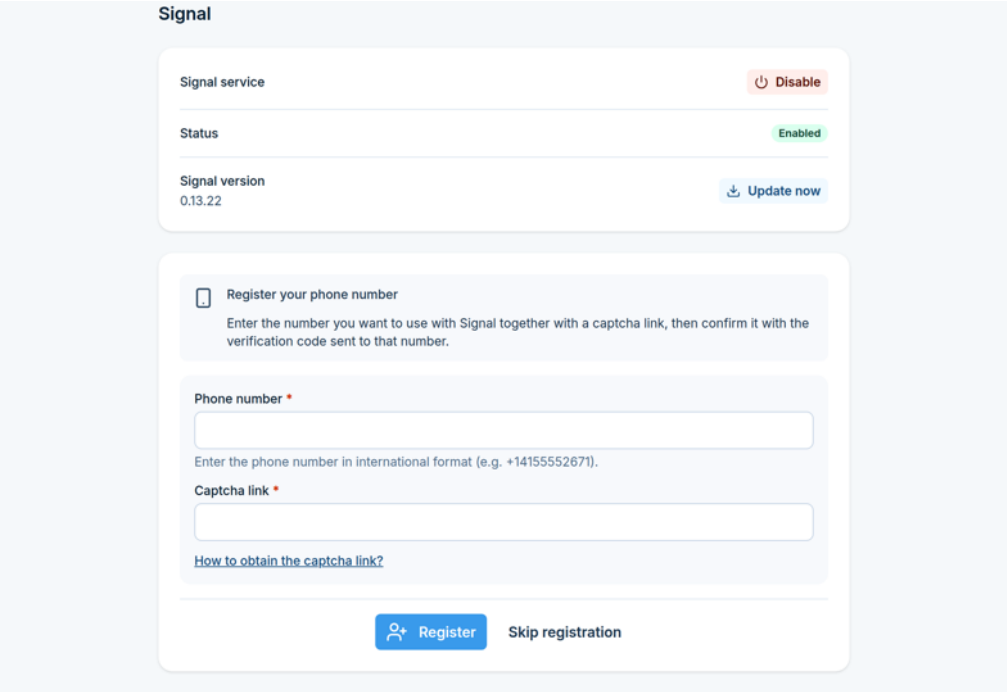
You can also unlink from the phone side, in **WhatsApp > Linked devices**. The page then shows **Disconnected** at its next refresh.

Good to know

- WhatsApp messages use the network connection, so they do not consume SIM credit and do not depend on GSM coverage. The **Fall back to SMS/MMS** option is the exception: those fallback messages do go through the modem.

- The link lives on the device. Restoring a backup onto different hardware, or unlinking from the phone, requires scanning a new QR code.
- Only messages received after the device was linked appear in the conversation list.

Signal



Signal service settings

What this feature does

Signal support lets your SMSEagle send and receive **Signal messages** in addition to SMS. The device registers itself with the Signal network using a phone number, and from then on Signal becomes another channel you can pick when composing a message, with its own conversation view.

Typical uses: reaching people who prefer Signal over SMS, or sending alerts to recipients who are abroad and would otherwise cost roaming charges.

Setting it up is a two-part job: first you enable the service and register a number (**Settings > Channels > Signal**), then you use the channel (**Messages > Signal**, or the Compose window).

Before you start

- Signal is available on selected device models only. If **Settings > Channels > Signal** is not in your sidebar, your device does not support it.
- You need a phone number that can receive a verification code, and it must not already be registered with Signal on another device.

- Registration requires a **captcha link**, which you generate in a browser. Keep the link handy before you start; it expires quickly.

Step 1: Open the Signal settings

In the sidebar, go to **Settings > Channels > Signal**.

The **Service** box at the top shows the installed **Signal version** and the current **Status**. On a fresh device the status is **Disabled** and a warning explains that the service must be enabled before a number can be registered.

Step 2: Enable the service

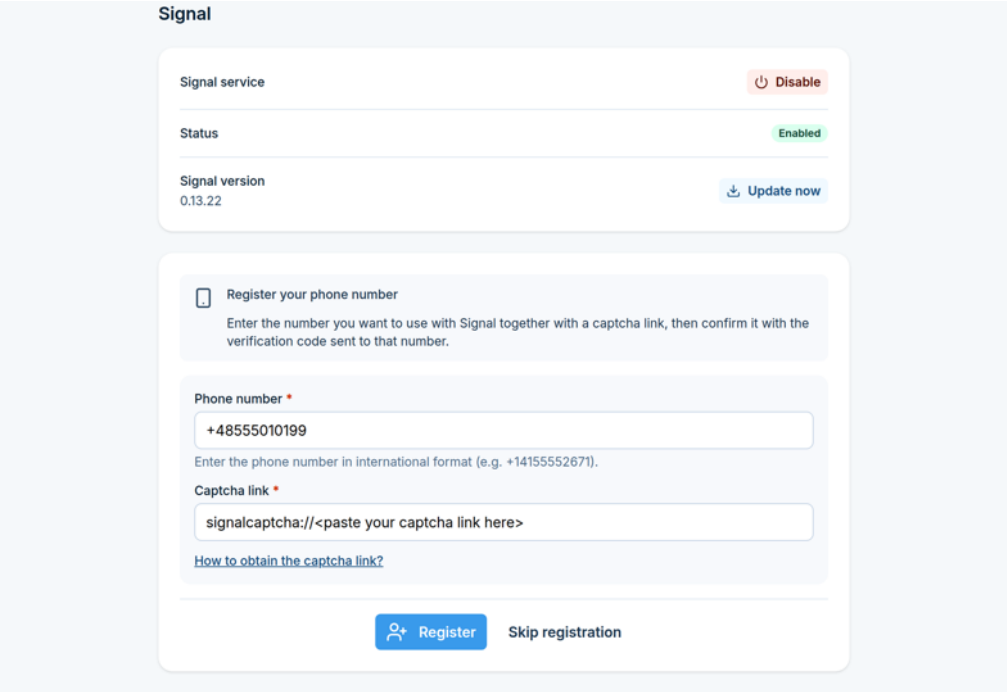
Click **Enable** at the bottom of the page. The status changes to **Enabled** and the registration form appears, as in the figure at the start of this section.

Step 3: Register a phone number

In the **Register a phone number** box:

1. In **Phone number**, type the number in international format, for example `+14155552671`.
2. In **Captcha link**, paste the captcha link. The link **How to obtain the captcha link?** below the field opens step-by-step instructions in a new tab.
3. Click **Register**.

Signal then sends a verification code to the number.



Registering a phone number

Already registered this number recently? Click **Skip registration** instead. The form jumps straight to the verification step, where you can enter a code you already received.

Step 4: Verify the number

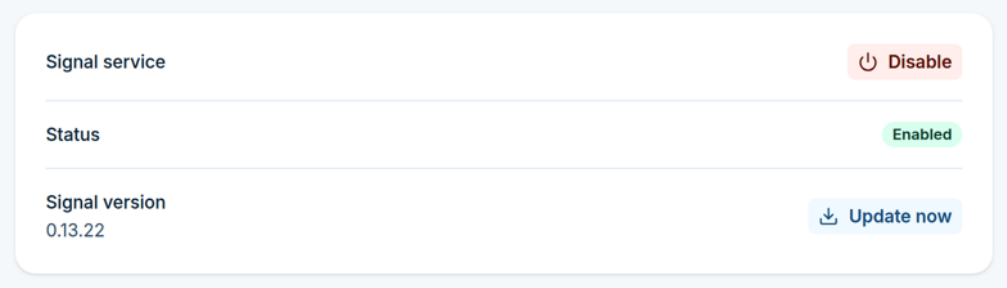
The form now asks for the **Verification code**. Type the code you received and click **Verify**.

On success the page reports that Signal is connected and shows the **Registered number** box.

Step 5: Keep the service up to date

The **Service** box has a **Check for new version** button. Click it to ask whether a newer Signal version is available:

Result	What to do
No new version found	Nothing. You are current.
A new version is available	The button turns into **Update now**, which takes you to the patch page where the update can be installed.
Could not fetch the newest version	The device could not reach the update server. Check the network settings and try again later.

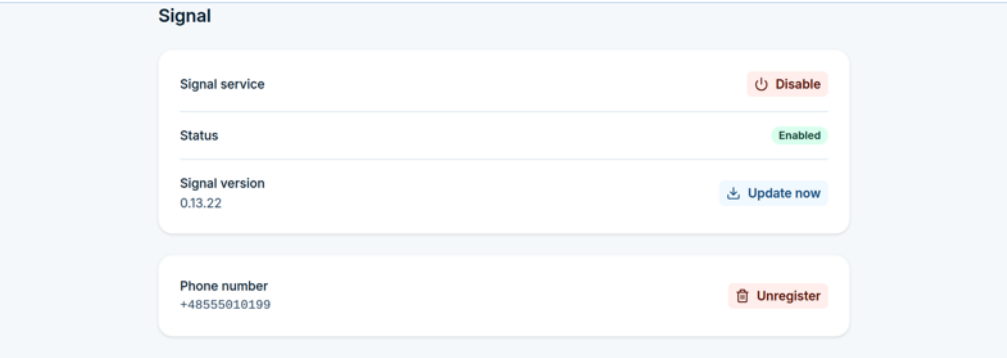


The Service box. Here a check has already found a newer version, so the button reads **Update now**

Removing the number

To unregister the device from Signal, go back to **Settings > Channels > Signal** and click **Unregister** in the **Registered number** box. The number is released and the page returns to the registration form.

To turn the channel off without unregistering, click **Disable** at the bottom of the page. The service stops and Signal disappears from the Compose window, but the registration is kept, so enabling it again does not require a new verification.



A registered Signal number

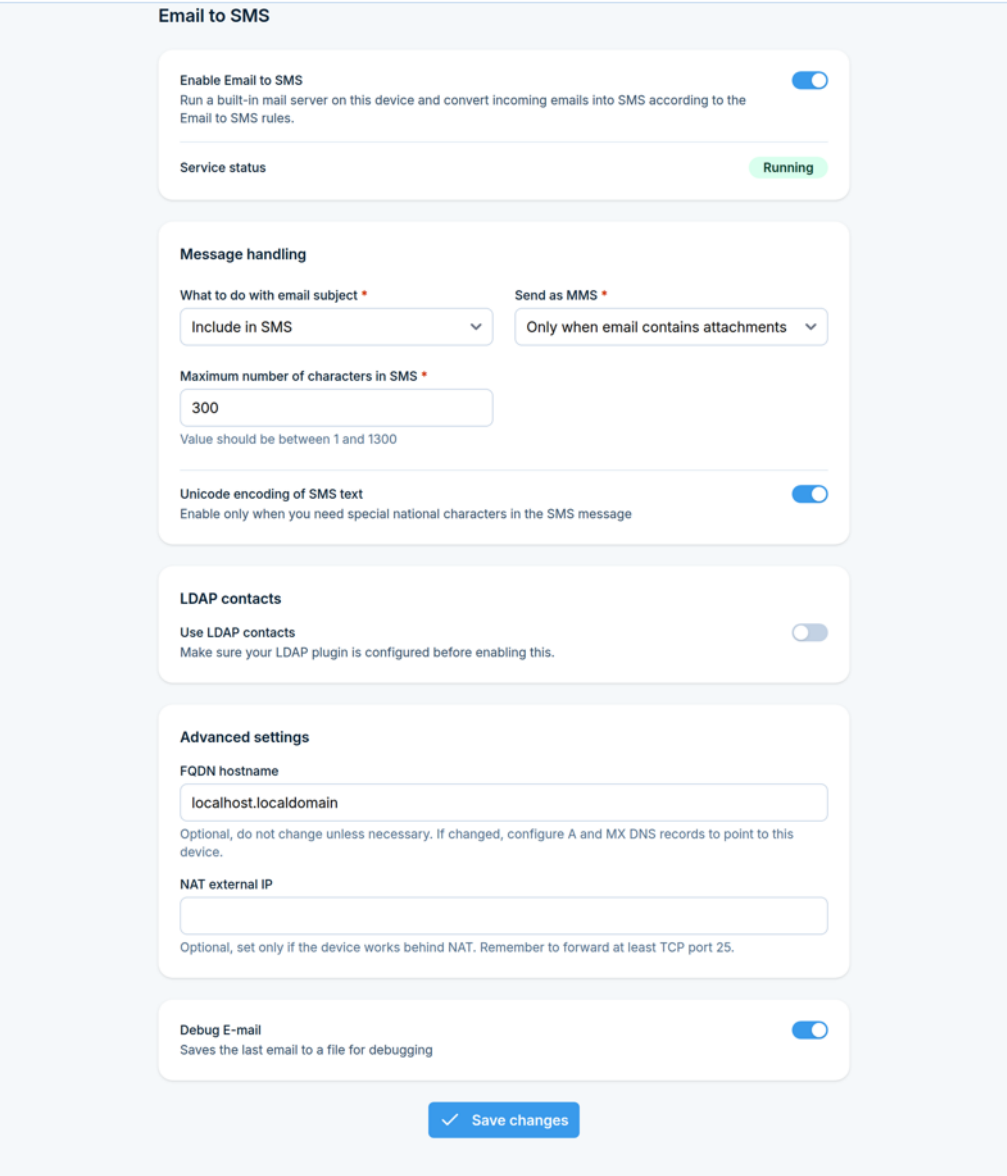
Good to know

- Signal messages are sent over the network connection, not through the modem, so they do not use SIM credit and do not depend on GSM coverage.
- The registration lives on the device. Restoring a backup onto different hardware, or removing the number, requires registering again.
- Only messages received after the service was enabled appear in the conversation list.

Email

Email to SMS

Settings > Channels > Email > Email to SMS (`/settings/email/email-to-sms`) starts a built-in mail server on the device and converts incoming emails into SMS, according to the rules you define under Email to SMS in Automation.



Email to SMS settings

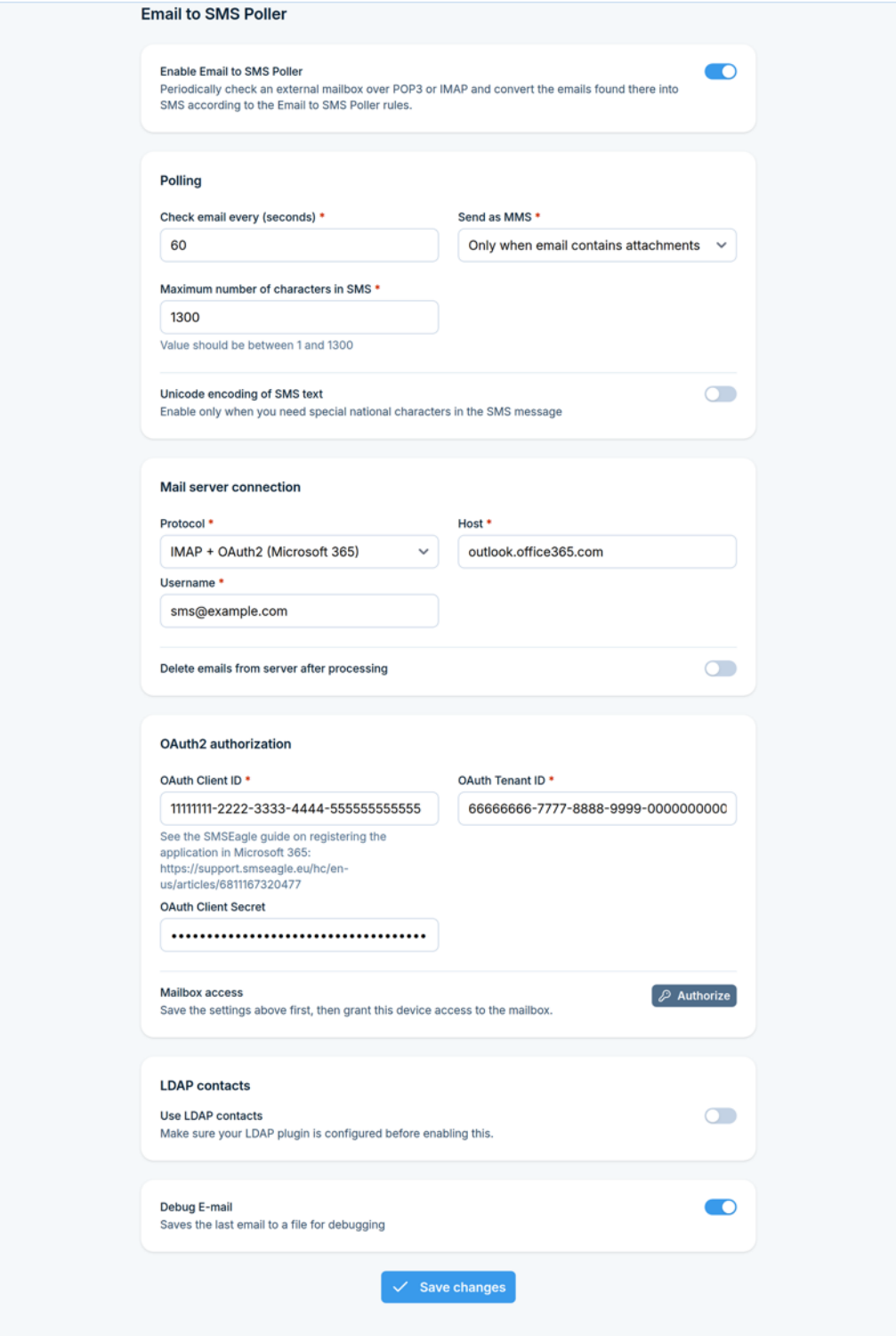
Turn on **Enable Email to SMS** to start the mail server. **Service status** shows whether it is **Running** or **Stopped**. The rest of the page decides how an email becomes an SMS:

- **What to do with email subject** - **Ignore** it, **Include in SMS**, **Use for authentication**, or **Send only subject without email body**.
- **Send as MMS** - **Never**, **Always**, or **Only when email contains attachments**.
- **Maximum number of characters in SMS** - from 1 to 1300.
- **Unicode encoding of SMS text** - turn it on only when messages need national characters that the standard SMS alphabet does not have.
- **Use LDAP contacts** - lets the recipient part of the address name a directory contact or group. Configure LDAP first.
- **FQDN hostname** (under **Advanced settings**) - optional domain name to use in recipient addresses instead of the device's IP address. If you change it, point the A and MX DNS records for that name at the device.

- **NAT external IP** - set it only when the device sits behind NAT, and forward at least TCP port 25 to the device.
- **Debug E-mail** - saves the last received email to a file for troubleshooting.

Email to SMS Poller

Settings > Channels > Email > Email to SMS Poller (`/settings/email/email-to-sms-poller`) connects the device to an existing mailbox, checks it at a fixed interval, and converts the emails it finds into SMS according to the rules under Email to SMS Poller in Automation. Unlike Email to SMS, no mail has to be delivered to the device itself.



Email to SMS Poller settings, connected to a Microsoft 365 mailbox

Turn on **Enable Email to SMS Poller**. The form below it has these parts:

Polling

- **Check email every (seconds)** - how often the mailbox is checked.
- **Send as MMS**, **Maximum number of characters in SMS** and **Unicode encoding of SMS text** - same meaning as for Email to SMS.

Mail server connection

- **Protocol** - **POP3**, **IMAP**, or **IMAP + OAuth2 (Microsoft 365)**.
- **Host** and **Username** of the mailbox.
- With **POP3** and **IMAP** only: **Port**, **Password** and **Use TLS/SSL encryption**. The page lists the standard ports: POP3 110, POP3 with TLS/SSL 995, IMAP 143, IMAP with TLS/SSL 993.
- **Delete emails from server after processing** - removes each email from the mailbox once it has been handled. Leave it off to keep the mailbox untouched.

OAuth2 authorization (only with **IMAP + OAuth2 (Microsoft 365)**)

- **OAuth Client ID**, **OAuth Tenant ID** and **OAuth Client Secret** of the application registered in Microsoft 365. See the SMSEagle guide on registering the application in Microsoft 365.
- Save the settings first, then click **Authorize** under **Mailbox access** and grant the device access to the mailbox.

Use LDAP contacts and **Debug E-mail** work as for Email to SMS.

For POP3 and IMAP the page also has a **Test connection** button. Save the settings before you use it. Some mail providers block IMAP test connections under their default security settings, so a failed test does not always mean the settings are wrong.

SMTP Configuration

Settings > Channels > Email > SMTP Configuration (`/settings/email/smtp`) manages a list of reusable SMTP server presets, and assigns one to each feature that sends outgoing email:

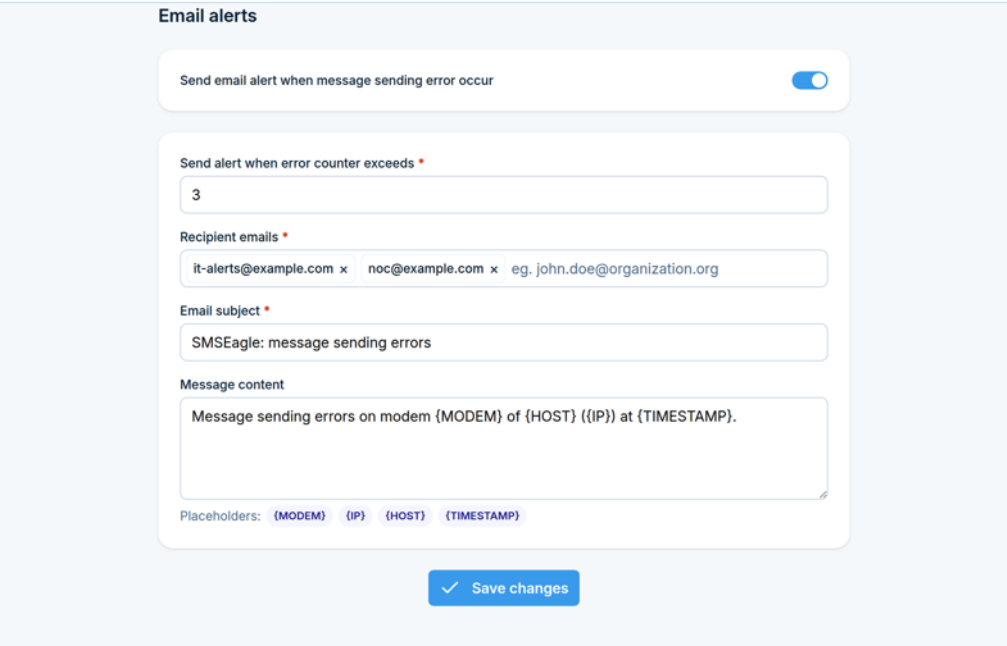
- **Compose menu**, **APIv2**, **SMS to Email**, **Alerts**, **Reporting module**, **Workflows**

Each of these can be set to **None** or to one of your saved presets. Unassigning a preset from a feature disables that feature's existing email setup.

Click **Create new** under **Configuration presets** to add an SMTP server (host, port, encryption, sender address, credentials); presets can then be picked from the dropdown for any of the features above.

Email alerts

Settings > Channels > Email > Email alerts (`/settings/email/alerts`) emails an alert when outgoing messages keep failing to send. It needs an SMTP preset assigned to **Alerts** under SMTP Configuration.



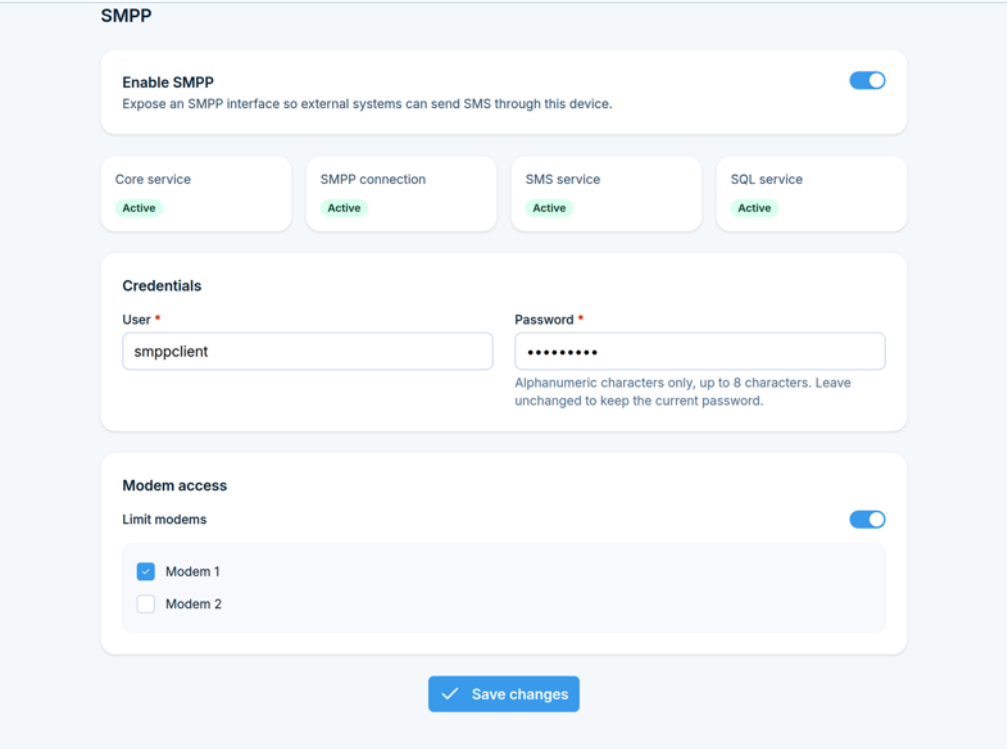
Email alerts settings

Turn on **Send email alert when message sending error occur**, then set:

- **Send alert when error counter exceeds** - how many sending errors are counted before the alert goes out. A value above 2 avoids alerts caused by a single temporary failure.
- **Recipient emails** - one or more addresses.
- **Email subject** and **Message content** - the text of the alert. The placeholders **{MODEM}** (the modem that raised the alert), **{IP}** (the device's IP address), **{HOST}** (its host name) and **{TIMESTAMP}** (when the error was detected) are replaced with real values. Click a placeholder under the message field to insert it.

SMPP

Settings > Channels > SMPP (`/settings/smpp/`) turns on the device's built-in SMPP server. An external application acting as an SMPP client can then submit SMS through the device's modems, and receives incoming SMS and delivery reports back over the same connection.



SMPP settings

Connection details

Parameter	Value
Protocol	SMPP 3.4
Port	TCP 2770
Client to SMSEagle	SMS to be sent through the device's modems
SMSEagle to client	Incoming SMS and delivery reports

The SMPP client binds with the **User** and **Password** set on this page, as its `system_id` and `password`.

Incoming SMS and delivery reports are queued on the device while no SMPP client is connected. As soon as a client binds, SMSEagle delivers everything in that queue, so the client must be ready to receive and acknowledge `deliver_sm` messages from the moment it binds.

Turning SMPP on

1. Turn on **Enable SMPP**. The service status cards, **Credentials** and **Modem access** appear.
2. Under **Credentials**, set the **User** and **Password** the SMPP client will bind with. The password can contain letters and digits only, up to 8 characters. When a password is already stored, leave the field as it is to keep it.

3. Under **Modem access**, turn on **Limit modems** to let SMPP traffic use only the modems you tick. Leave it off to allow all modems.
4. Click **Save changes**.

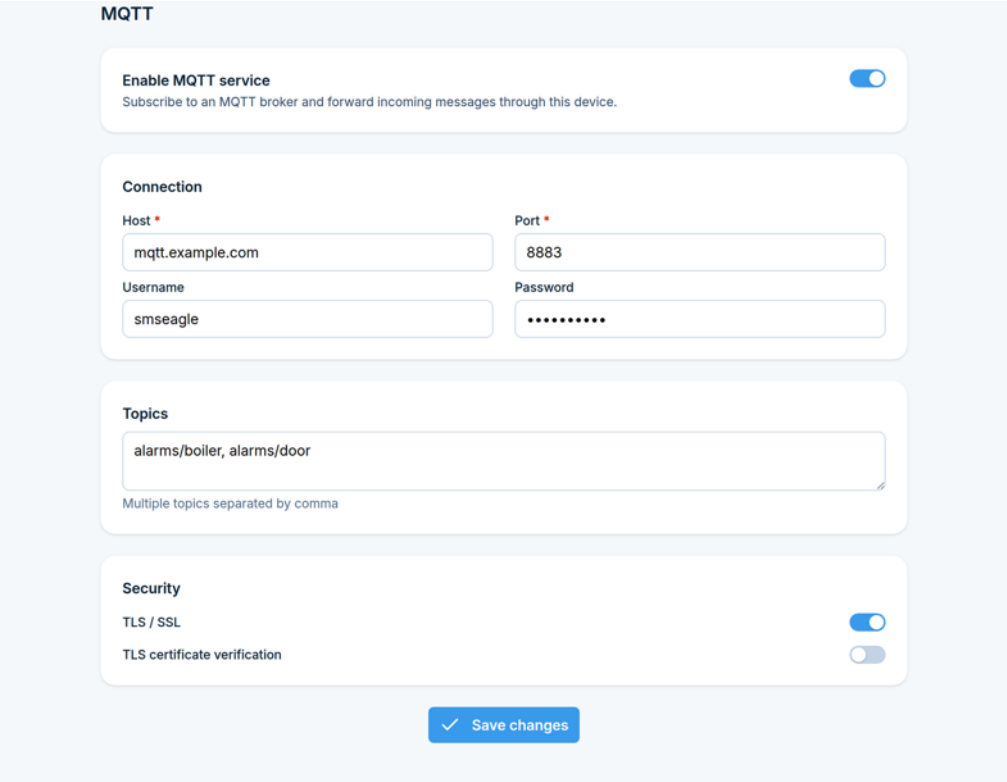
   A reboot is needed. After saving, SMSEagle asks you to reboot the device so the SMPP changes take effect. Until you do, the new settings are stored but not yet in use. Use **System > Restart** when you are ready.

After the reboot, the four status cards (**Core service**, **SMPP connection**, **SMS service**, **SQL service**) show whether each part of the SMPP server is running. All four must read **Active** for SMPP clients to connect and exchange messages.

The first time you enable SMPP, SMSEagle also creates an internal user for SMPP traffic, with its own API key listed under **Settings > API v2 keys**, and the internal rules that pass incoming SMS and delivery reports to the SMPP client. Do not revoke or edit them. Turning SMPP off removes the user and the rules again.

MQTT

Settings > Channels > MQTT (`/settings/mqtt/`) connects the device to the MQTT broker it listens to. The Subscribe rules under MQTT in Automation, which turn MQTT messages into SMS, use this connection. Publish rules do not: each of them names its own broker.



MQTT broker connection settings

Turn on **Enable MQTT service**, then set:

- **Host** and **Port** of the broker (both required).

- **Username** and **Password**, if the broker requires them.
- **Topics** - the topics the device subscribes to, separated by commas.
- **TLS / SSL** - encrypts the connection to the broker. **TLS certificate verification** also checks the broker's certificate, so leave it off only for a broker with a self-signed certificate.

Click **Save changes**.

> **A reboot is needed.** After saving, SMSEagle asks you to reboot the device so the MQTT changes take effect. Until you do, the new settings are stored but not yet in use. Use **System > Restart** when you are ready.

Network

IP Settings

Settings > Global settings > Network > IP Settings (`/settings/network/ip`) shows the device's **MAC address** (read-only) and lets you configure:

- **Get IP address from DHCP** - toggle DHCP on, or off to set a static IP.
- **Hostname**
- **Use proxy** - route the device's outgoing connections through an HTTP proxy.
- **IP address restriction** - **Allow**, **Deny**, or **Disabled**, with a list of IP addresses the rule applies to. When restriction is active, all ports except 22 (SSH) are blocked for everyone not on the list.

  > **Be careful with IP address restriction.** A misconfigured allow-list can lock you out of the web interface from your own machine. Add your current IP first (the page offers an **Add your IP address** shortcut) before saving.

SSL

Settings > Global settings > Network > SSL (`/settings/network/ssl`) lets you replace the device's default self-signed certificate with your own: upload a **Certificate**, its **Private key**, and optionally a **Root CA certificate** and **Full chain**. A separate switch, **Forward HTTP to HTTPS**, redirects plain HTTP requests to HTTPS.

Failover

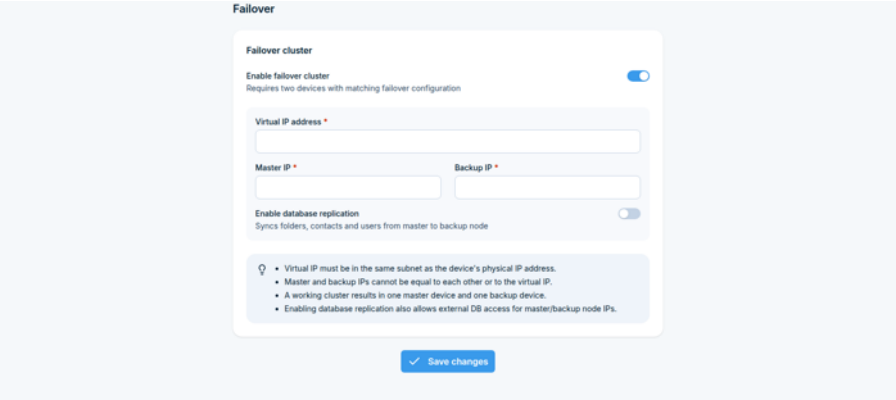
Failover cluster provides device-level high availability: a second SMSEagle device stands by as a backup, ready to take over if the master device stops responding. This is different from modem failover, which switches between two SIM cards inside the same device - a failover cluster protects against the whole device going down.

Where to find it

Settings > Global settings > Network > Failover (`/settings/network/failover`).

Enabling failover cluster

Turn on **Enable failover cluster**. This requires two devices with matching failover configuration, one acting as master and the other as backup.



Failover cluster settings

Set the same values on both devices:

- **Virtual IP address** - the address your users and integrations connect to.
- **Master IP** and **Backup IP** - the physical IP addresses of the two devices. Each device takes its role from its own address: the one whose IP matches **Master IP** becomes the master, the one matching **Backup IP** the backup. One of the two must therefore be the address of the device you are configuring.
- **Enable database replication** - copies folders, contacts and users from the master to the backup node (see below).

Click **Save changes**.

> **A reboot is needed.** After saving, SMSEagle asks you to reboot the device so the failover changes take effect. Until you do, the new settings are stored but not yet in use. Use **System > Restart** when you are ready.

Master/backup roles and virtual IP

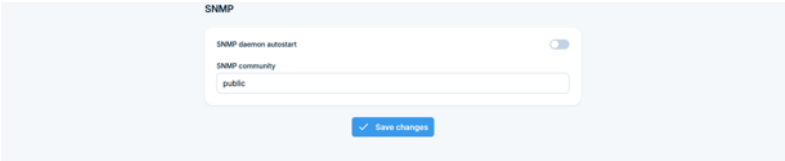
The cluster is reached through a single **virtual IP address**, which always points at whichever device is currently active:

- The virtual IP must be in the same subnet as each device's own physical IP address.
- The master IP, backup IP, and virtual IP must all be different from each other.
- A working cluster always has exactly one master device and one backup device at any given time; if the master stops responding, the backup takes over the virtual IP.

Database replication and external access

Enabling failover cluster also enables database replication between the master and backup, so the backup device has an up-to-date copy of messages, contacts, and settings if it needs to take over. This same setting also allows external database access for the master and backup node IPs specifically, which is required for replication to work.

SNMP



SNMP Agent settings

The SNMP Agent lets external tools (an NMS, a MIB browser, or a plain `snmpget`/`snmpwalk` call) poll SMSEagle for its own metrics - signal strength, network name, folder message counts, system uptime, and more. This is the opposite direction from SNMP Traps: the agent is polled by an external tool, rather than SMSEagle pushing an alert to one.

Where to find it

Settings > Global settings > Network > SNMP (`/settings/network/snmp`).

Configuring the SNMP Agent

Enable **SNMP daemon autostart** so the agent starts automatically with the device, and set the **SNMP community** string used to authenticate read requests.

Once enabled, SMSEagle's extension parameters (signal strength, network name, folder counters, uptime, and others) can be read from the device's MIB tree using any standard SNMP tool, for example NET-SNMP's `snmpget`/`snmpwalk` or a graphical MIB browser.

Available metrics

On top of the standard Linux host metrics, SMSEagle publishes its own metrics through NET-SNMP-EXTEND-MIB. Each one can be read by its OID, or by name as `NET-SNMP-EXTEND-MIB::nsExtendOutputFull."<metric name>"`.

Metrics that describe a modem end in the modem number: 1 to 8. The tables show them for modem 1. A metric returns `-1` when its value cannot be read, for example when the modem is switched off.

Metric	Returns
`GSM_Signal1`	Signal strength of the modem, in percent (0-100).
`GSM_NetName1`	Name of the mobile network the modem is registered to.
`GSM_ModemState1`	`on` or `off`: whether the modem is switched on under Modems.
`SIM_State1`	SIM card status as reported by the modem: `READY` when the SIM is ready, otherwise the modem's own status such as `SIM PIN` or `SIM PUK`, or an error such as `NOSIM`.
`SIM_RegState1`	Network registration: `Registered Home`, `Registered Roaming`, `Searching`, `Not Registered`, `Denied`, `Registered Emergency`, `Unknown` or `Unset`.
`SMSCountIn1`	SMS received by the modem today, since midnight.
`SMSCountOut1`	SMS sent by the modem today, since midnight.
`FolderInbox_Total`	**Unread** messages in Inbox. A multipart message counts once.
`FolderOutbox_Total`	Messages waiting in Outbox, the sending queue.
`FolderSent_Last24H`	Messages sent in the last 24 hours. Each part of a multipart message counts separately.
`FolderSent_Last1M`	Messages sent in the last month, counted the same way.
`FolderSent_Last24HSendErr`	Messages that failed to send in the last 24 hours, because the modem could not send them or the network rejected them.

Metric	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

The OID of any metric is `.1.3.6.1.4.1.8072.1.3.2.3.1.2`, followed by the number of characters in the metric name and the ASCII code of each character. For another modem, only the last number changes: it is 48 plus the modem number, so `GSM_Signal2` ends in `.50`.

If your SNMP tool does not know NET-SNMP-EXTEND-MIB names, load the MIB definition file.

Reading metrics

Replace `public` with your **SNMP community** and `192.0.2.10` with the device's IP address.

Read one metric by 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
```

Read one metric by name:

```
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
```

List all SMSEagle metrics at once:

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

What can be read from the network

Queries from the device itself (`localhost`) see the whole MIB tree. Queries from other hosts see a restricted part of it: the SMSEagle metrics above, and from the standard MIBs the system group (including uptime), network interfaces, storage, processors, memory, load and CPU usage. The process list and other details are not exposed to the network.

The same **SNMP community** applies to both. After you change it, reboot the device for the new value to take effect.

Using SNMP v3

The page configures SNMP v1/v2c. For SNMP v3 with authentication and encryption, use the `snmpv3` script over SSH:

1. Log in to the device over SSH as `root`.
2. Go to the SMSEagle directory:

   ```
   cd /opt/smseagle/
   ```

3. Add a read-only SNMP v3 user. It uses SHA for authentication and AES for encryption. Both passwords must be at least 8 characters long.

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

4. Optionally, turn off SNMP v1/v2c access so that only SNMP v3 users can read the agent:

```
./snmpv3 disablev2
```

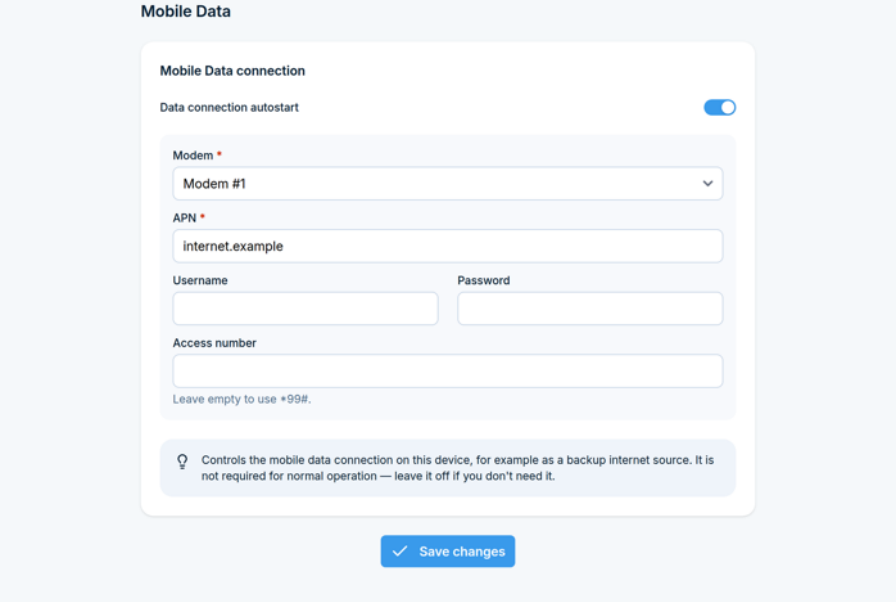
`./snmpv3 enablev2` turns it back on, and `./snmpv3 del USERNAME` removes the user.

The script restarts the SNMP agent itself. A v3 query then looks like this:

```
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
```

Mobile Data

Settings > Global settings > Network > Mobile Data (`/settings/network/mobile-data`) controls a mobile data connection over one of the device's modems, for example as a backup internet source. It is not required for sending or receiving SMS. Leave it off if you do not need it.



Mobile Data settings

Turn on **Data connection autostart**, then set:

- **Modem** - the modem whose SIM carries the data connection.
- **APN** of the SIM's operator (required), and **Username** and **Password** if the operator requires them.
- **Access number** - leave it empty to use `*99#`.

Click **Save changes**.

A reboot is needed. After saving, SMSEagle asks you to reboot the device so the mobile data changes take effect. Until you do, the new settings are stored but not yet in use. Use **System > Restart** when you are ready.

Application

Settings > Global settings > Application (`/settings/application/`) holds device-wide behavior that does not fit under a single channel or feature, grouped into four sections:

Regional

Language (device-wide default) and **Country dial code** (used when a phone number is entered without one).

Security

- **Force MFA** - For all users, For new users, or Do not force (same effect as the wizard's device-wide MFA setting, see MFA).
- **Password complexity verification** - require the password rules (length, mixed case, number, special character) for every user.
- **Access to DB for external applications** - enables direct PostgreSQL access for external applications, disabled by default. Full connection details and example SQL are covered separately in Advanced, since that is a power-user topic on its own.

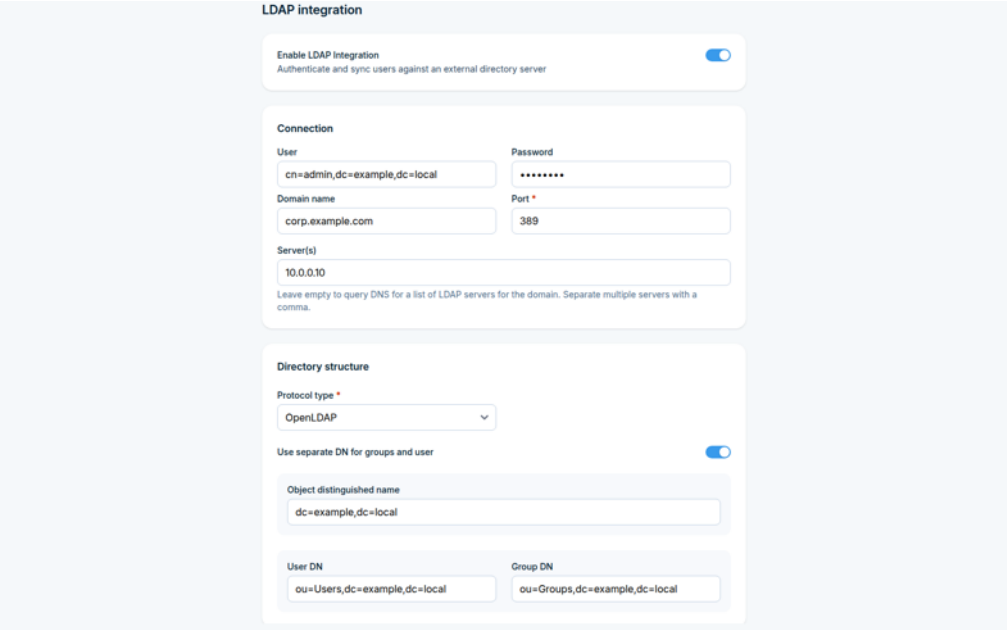
Access and visibility

- **Inbox content visibility** - For all users, Only for admins, or Only messages from the modems assigned to the user (modems are assigned per user in **System > Users**).
- **Email inbox content visibility** - For all users or Only for admins.
- **Reporting module accessible for** - All users or Only admins.

API and integrations

- **Save API logs** - logs every API v1 and v2 call (method, path and parameters) to `/var/log/smseagle/api.log`. Access tokens are masked and message text is left out. The file is not shown in the log browser under **System > Logs**, but **Download logs** on that page includes it. Turn it on while you set up or debug an integration.
- **Forward 3CX messages as unicode** - messages that 3CX sends to SMSEagle through the API v2 3CX endpoint go out as Unicode SMS instead of the standard SMS alphabet. Turn it on when 3CX users send national characters.

LDAP



LDAP integration settings

What this feature does

LDAP integration connects SMSEagle to your company directory, such as Active Directory or OpenLDAP. It does two separate jobs, and you can use either or both:

Job	What it gives you
Contacts	The Phonebook is filled from the directory, so you send messages to the same people and groups your company already maintains, without typing numbers twice.
Authentication	Users sign in to SMSEagle with their directory account, and their permission level is decided by their directory group membership.

Typical uses: keeping the Phonebook in step with staff changes automatically, and letting people use their existing company password instead of a separate SMSEagle one.

Before you start

Collect this from whoever administers the directory:

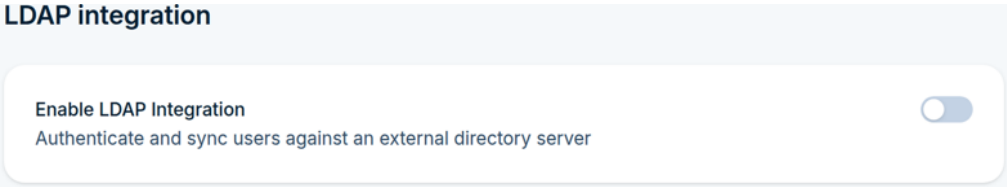
- The **domain name** and the **port** (389 for plain LDAP, usually 636 with SSL).
- A **service account** (user and password) that may read the directory.
- The **distinguished name** of the branch holding your users, for example `ou=Users,dc=company,dc=local`, and the branch holding groups if it is different.
- Which **attribute** holds the phone number you want to text.

- If you want directory sign-in: the names of the groups whose members should become SMSEagle administrators and regular users.

Step 1: Open the LDAP page

In the sidebar, go to **Settings > Global settings > LDAP**.

The page starts with a single switch, **Enable LDAP Integration**. Until you turn it on, nothing else is shown.



With the integration off, the page shows nothing but the switch

Step 2: Enable the integration

Turn **Enable LDAP Integration** on. Four sections appear: **Connection**, **Directory structure**, **Attributes and security** and **Sync and access**.

Step 3: Connection

Field	What to enter
User	The service account used to read the directory.
Password	Its password. The field is shown empty when you come back to the page; leave it empty to keep the stored password.
Domain name	The directory domain, for example `company.local`.
Port	389 for plain LDAP, 636 for LDAP over SSL. Required.
Server(s)	Specific servers, separated by commas, for example `ldap1.company.local`, `ldap2.company.local`. Leave empty to let the device look the servers up in DNS for the domain.



Connection section, filled in with example values

Step 4: Directory structure

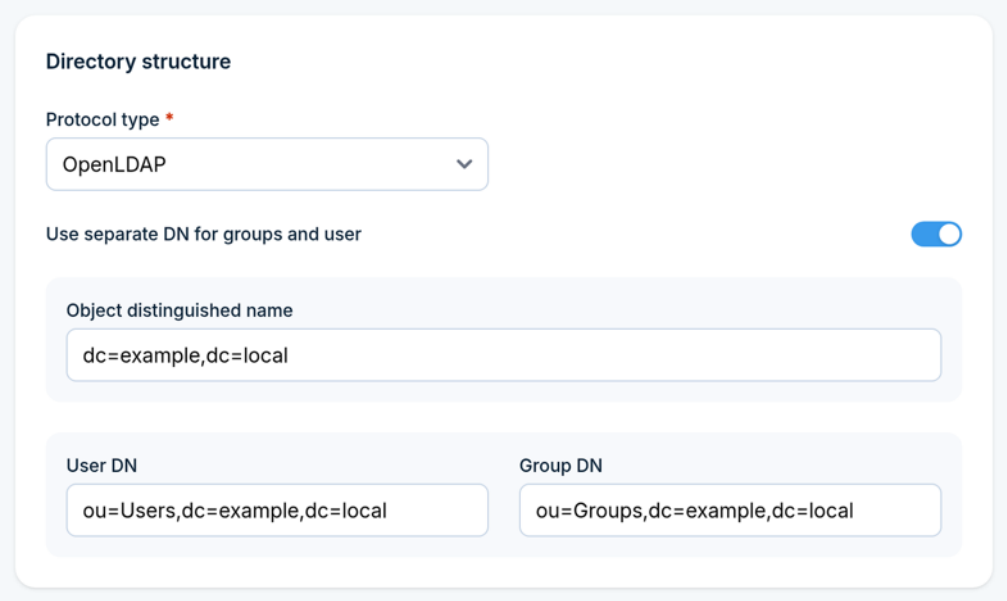
Protocol type Choose **Active Directory** or **OpenLDAP**, matching your server.

Use separate DN for groups and user Leave this off if users and groups live under the same branch. One field is then shown:

- **Object distinguished name**, for example `ou=Users,dc=smseagle,dc=local`.

Turn it on if they live in different branches. **Object distinguished name** stays, and two more fields appear below it:

- **User DN**, for example `ou=Users,dc=smseagle,dc=local`
- **Group DN**, for example `ou=Groups,dc=smseagle,dc=local`



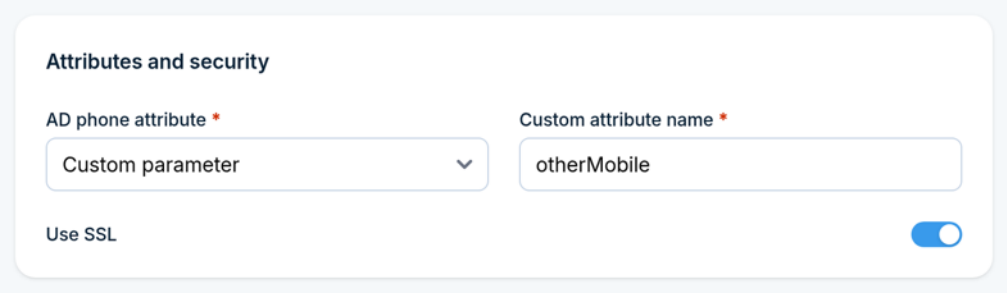
Directory structure with separate DNs turned on

Step 5: Attributes and security

AD phone attribute Which directory attribute holds the number SMSEagle should text: **Telephone number**, **Mobile number**, **Home number**, **Pager number**, **Fax number**, **IP phone number**, or **Custom parameter**.

Choosing **Custom parameter** reveals **Custom attribute name**, where you type the attribute yourself, for example `otherMobile`. Only plain attribute names are accepted; punctuation such as `< > / \ : ; , . + ' " & =` is rejected.

Use SSL Turn this on to encrypt the connection to the directory. Remember to set the matching **Port** in the Connection section.



Attributes and security, with **Custom parameter** selected and SSL turned on

Step 6: Sync and access

Contacts and group fetch method

Option	What happens
Fetch from LDAP server	Contacts and groups are read from the directory every time they are needed. Always current, but every lookup depends on the directory being reachable.
Store offline (sync manually/periodically)	A copy is kept on the device. Messaging keeps working when the directory is unreachable, at the cost of the copy being slightly stale.

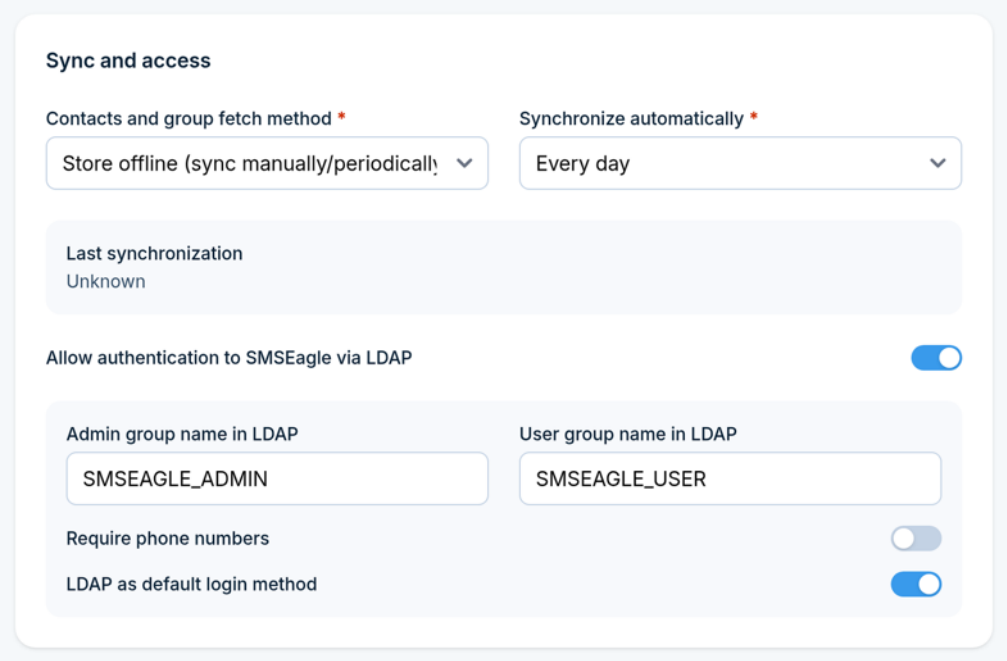
If you chose **Store offline**, **Synchronize automatically** appears: **Never**, **Every hour**, **Every day**, **Every week** or **Every month**. **Never** means the copy is only refreshed when you trigger a sync yourself.

Last synchronization below the fetch method is read-only, and shows when the offline copy was last refreshed. It reads Unknown until the first sync runs.

Allow authentication to SMSEagle via LDAP Turn this on to let people sign in with their directory account. Four more fields appear:

- **Admin group name in LDAP** - members of this group sign in as administrators.
- **User group name in LDAP** - members of this group sign in as regular users.
- **Require phone numbers** - only directory accounts that have a number in the chosen phone attribute may sign in. Off by default.

- **LDAP as default login method** - preselects LDAP instead of Local in the sign-in form's authentication type, so directory users do not have to change it every time.



Sync and access, with offline storage and directory sign-in enabled

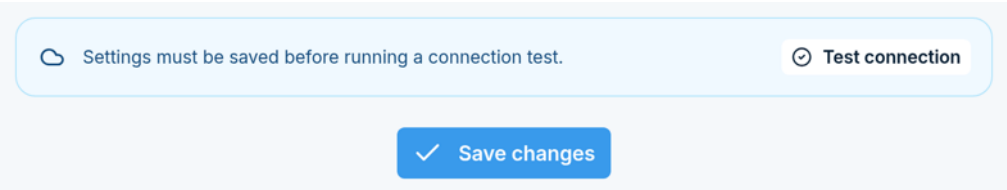
Check the group names before you rely on them. A member of neither group cannot sign in, and a typo in the admin group name is only noticed when nobody can administer the device. Keep at least one local SMSEagle administrator account working until you have verified a directory sign-in.

Step 7: Save and test

Click **Save changes** at the bottom of the page.

Then click **Test connection**. The device connects to the directory with the settings you just saved and reports either that the connection was established, or what went wrong.

Save first, then test. The test uses the stored settings, not what is currently on screen, so testing before saving checks the previous configuration. The note next to the button says the same.



The test panel repeats the rule: save first, then test

Date / Time

Settings > Global settings > Date / Time (`/settings/datetime/`) shows the current system date and time (read-only), and lets you set:

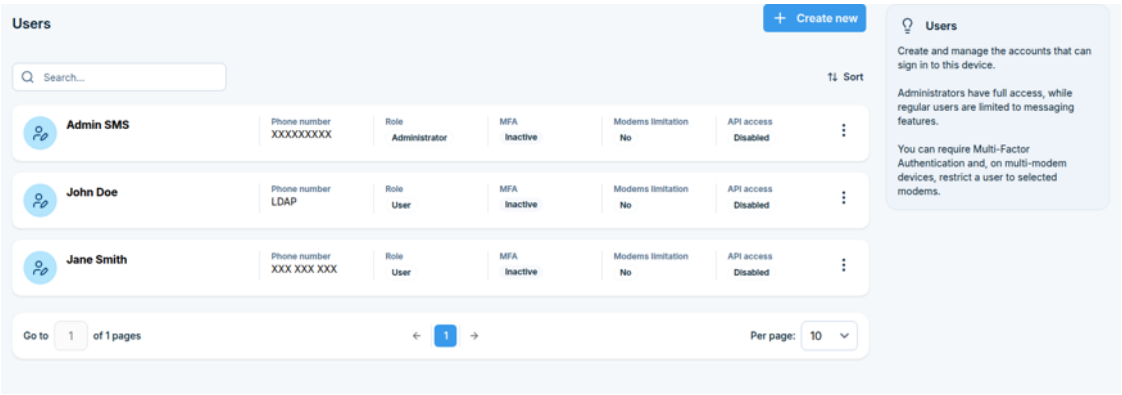
- **Time zone**
- **NTP time synchronization** - when enabled, reveals **NTP server address**. Also offered during the Configuration Wizard.

System

This chapter covers the **System** section of the web interface: managing user accounts and the device itself.

Users

System > Users (`/system/users/`) is where you create and manage the accounts that can sign in to the device. Administrators have full access, while regular users are limited to messaging features.



Users, in the System section of the menu

For each user you can set their **Access level** (Administrator or User), require Multi-Factor Authentication, and, on multi-modem devices, restrict a user to selected modems. API access (see API and Developer Integration) is also granted per user from here.

System info

System > System info (`/system/info/`) shows read-only information about the device and its modems:

- Device type, SMSEagle software version, serial number (MAC address), modem software version, and database schema version
- **Disk space** usage, with an optional SMS notification to the Master Admin when usage crosses a threshold you set
- Per-modem details: signal strength, network name, SIM status and registration status, IMEI, and SIM card IMSI

Logs

System > Logs (`/system/logs/`) lets you browse and search the device's own logs, grouped into per-modem logs and system logs (Database, System, Application, Message). Use **Search by phrase** to filter, or **Download logs** to save them for support. Logs can also be forwarded to an external syslog server for centralized collection, see Forwarding logs to an external server.

Updates

System > Updates (`/system/updates/`) shows the installed software version and lets you check for updates manually or automatically; you can also have the device notify the admin by SMS when a new version is available. The same page shows your technical support validity and lets you check that automatically too.

Patches

System > Patches (`/system/patches/`) installs a targeted fix or extra component delivered by SMSEagle support: either enter a **patch code** to download and install it directly, or upload a **patch file** (a `.bin` file, up to 100 MB) provided by support.

Backup / Restore

System > Backup / Restore (`/system/backup/`) covers both directions:

- **Manual backups** - create a backup of the database and device settings on demand.
- **Automatic backups** - enable scheduled backups to an SFTP/FTP(S) server, with cleanup of old backup versions.
- **Restore data** - restore the database from a backup file.

Restart

System > Restart (`/system/restart/`) reboots the device on demand - sending and receiving is unavailable until it comes back online - or lets you enable a scheduled restart on a recurring basis.

Advanced

Direct database access and other power-user, off-the-beaten-path topics have their own chapter: see Advanced.

API and Developer Integration

SMSEagle offers a powerful built-in REST API. The API is dedicated to integrating SMSEagle with any external system or application.

API Reference

SMSEagle offers two API versions:

- **API v2 - recommended, use it for every new integration.** A modern RESTful API based on the OpenAPI 3.0 specification. API v2 Reference
- **API v1 - the legacy API, kept for backward compatibility only.** A simple HTTP and JSON-RPC API. It still works and is still supported, but it gets no new features - do not write new integrations against it. API v1 Reference

Because of the extensive content of the API documentation, it is maintained as a separate document. Follow the links above for the full specification of each API.

API keys

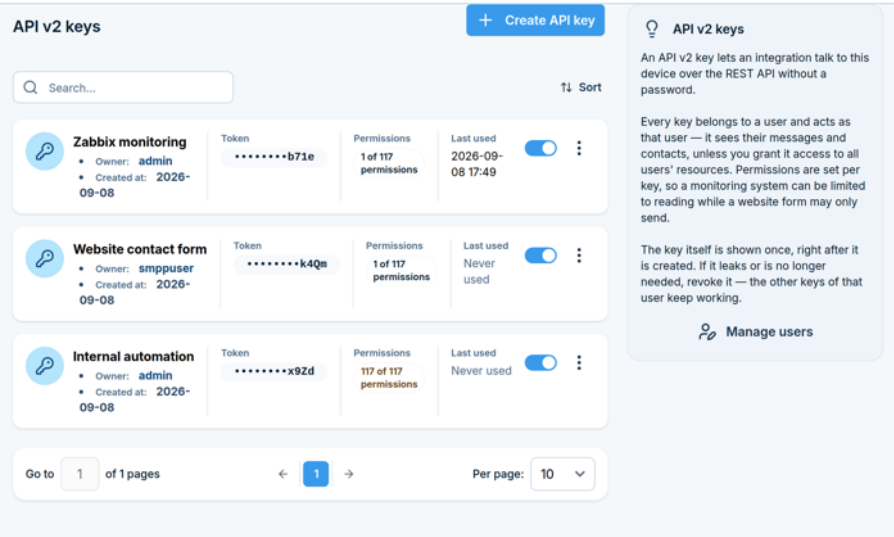
An integration authenticates with an **API key** instead of a user password. Keys are kept separately for each API version, on two pages:

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

A key always belongs to a user and acts as that user, so it sees that user's messages and contacts. Permissions are granted per key, which lets you limit a monitoring system to reading while a website form may only send.

API v2 keys

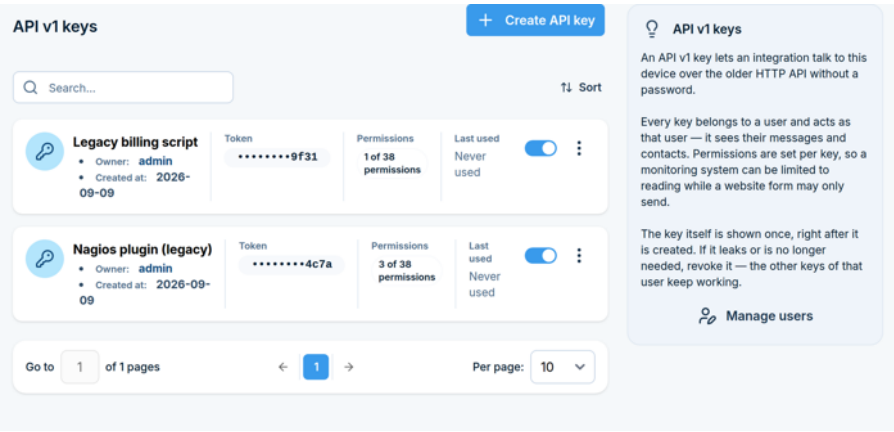
This is the page to use for a new integration.



API v2 keys

API v1 keys

API v1 is the legacy API. Create a v1 key only for an existing integration that cannot be moved to v2 - for anything new, create an API v2 key instead.



API v1 keys

Creating a key

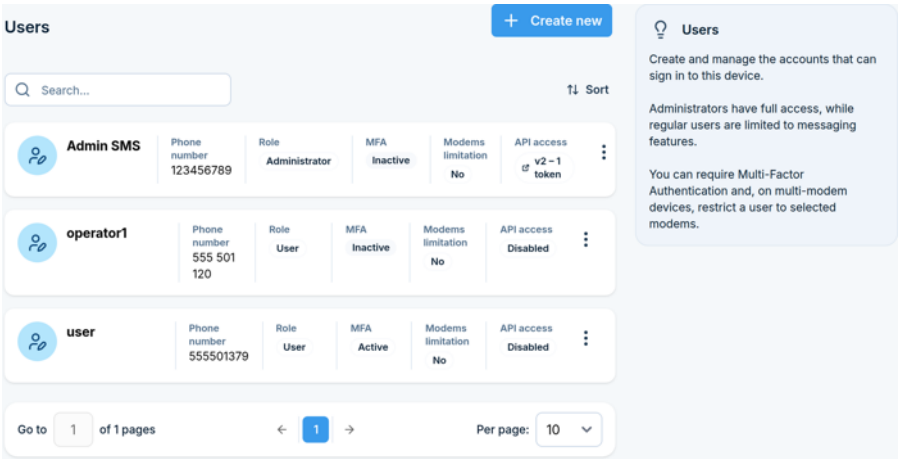
Create API key opens the form for the API version whose page you are on:

Field	What it does
Key name	How you will recognise this integration later, for example Zabbix or Website form.
Owner	The user the key acts as. The key sees that user's messages and contacts.
Key enabled	A disabled key is refused by the API without being deleted, which switches an integration off without losing its configuration.
Access to all users' resources	API v2 only. Lets the key read and change resources owned by other users (see below).
Permissions	Only the methods you switch on can be called with this key.

The key itself is shown once, right after it is created. Copy it then and store it somewhere safe. If you lose it, revoke that key and create a new one - the other keys of the same user keep working.

Which users have API access

System > Users shows, per user, how many API keys the user has and for which API version. The badge links straight to the matching keys page.



API access, shown per user in the Users list

Access to resources of other users

The two API versions differ in how broadly an API key can see other users' data:

- In **API v1**, a key has access by default to resources of every other user - phonebook contacts, groups, and so on.
- In **API v2**, access is more granular: a key has access by default only to resources it created itself. To allow access to resources of all other users, enable **Access to all users' resources** on the key.

Plugins and integrations

SMSEagle can be integrated with external software such as Network Monitoring Systems, Authentication Systems and many others. Most integrations use one of two methods:

- **API** - the external system sends and receives messages through the SMSEagle REST API. This is the most flexible method and gives access to all device functions. See API and Developer Integration.
- **Email to SMS** - the external system sends a regular email and SMSEagle converts it into an SMS. No coding is needed, so it works with any software that can already send email notifications. See Email to SMS.

Depending on your environment, you can also use MQTT or SMPP.

For many popular systems you do not need to build the integration yourself. SMSEagle provides ready-to-use plugins and step-by-step integration manuals, and the list grows constantly. For a complete and up-to-date list, go to: https://www.smseagle.eu/integration-plugins/

Advanced

This chapter covers power-user topics that go around the normal web interface rather than through it: direct database access and SQL, and command-line database cleaning scripts. Most users will never need this chapter.

Connecting directly to the SMSEagle database

SMSEagle's database runs on PostgreSQL. You can access it directly for reading or writing SMS messages via SQL queries, instead of going through the web interface or the API.

Database access for external applications is **disabled by default**. Enable it under **Settings > Global settings > Application > Access to DB for external applications**.

Once enabled, connect to the database from an external application using:

- Host: the device's IP address
- Database name: `smseagle`
- User: `smseagleuser`
- Password: `postgreeagle`

Injecting a short SMS using SQL

A short text message (up to 160 characters):

```
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;
```

The message above belongs to the user with `id_user` 1 (the default `admin` user) - other users' `id_user` values are in table `public."user"`. The `SenderID` field identifies which modem sends the message: `smseagle1` for modem 1, `smseagle2` for modem 2.

Injecting a long SMS using SQL

Multipart messages also need a UDH header, stored as a hex string in the `UDH` field. Unless you have a specific reason to do this manually, use the API instead (see API and Developer Integration).

For a long text message, the UDH starts with `050003`, followed by one byte used as a message reference (any hex value, but different for each message - `D3` below), one byte for the total number of parts (`02` below, unique per message sent to the same number), and one byte for the current part number (`01` for the first part, `02` for the second, and so on).

A two-part long message looks like this:

```
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;
```

Adding a UDH leaves less room for text - the example above allows only 153 characters per message part.

Database cleaning scripts

A few scripts are available for deleting SMS messages from the database via the Linux CLI, located at `/mnt/nand-user/scripts/`:

Script	Usage	Purpose
`db_delete`	`./db_delete YYYYMMDDhhmm`	Delete SMS from Inbox and SentItems older than the given date
`db_delete_7days`	`./db_delete_7days`	Delete SMS from Inbox and SentItems older than 7 days
`db_delete_allfolders`	`./db_delete_allfolders`	Clean Inbox, SentItems, and Outbox - designed to run periodically via cron
`db_delete_select`	`./db_delete_select {inbox|outbox|sentitems|trash}`	Delete SMS from one chosen folder

Adding a script to cron: create a file under `/etc/cron.d/` (for example `db_cleaner`) with content such as:

```
0 0 1 * * root /mnt/nand-user/scripts/db_delete_allfolders
```

This example runs the cleaning script on the 1st of every month.

Forwarding logs to an external server

SMSEagle writes its logs through rsyslog. To send a copy of them to a central syslog server, add a forwarding rule over SSH. There is no setting for this in the web interface.

1. Log in to the device over SSH as `root`.
2. Create the file `/etc/rsyslog.d/005-remote.conf` with this rule, replacing the address, port and protocol with your server's:

   ```
   *.* action(type="omfwd" target="192.0.2.250" port="514" protocol="udp"
              action.resumeRetryCount="10"
              queue.type="linkedList" queue.size="10000")
   ```

   - `target` - IP address or host name of the syslog server.
   - `port` - port the server listens on, usually `514`.

- `protocol` - `udp` or `tcp`.
- The queue settings keep up to 10000 messages on the device while the server is unreachable, and send them once it is back.

3. Check the configuration, then restart rsyslog:

```
rsyslogd -N1
systemctl restart rsyslog
```

Keep the file name. SMSEagle's own logs (Application, API, Message, and the email, call, Signal and WhatsApp services) are written by rules in `/etc/rsyslog.d/010-*.conf` to `018-*.conf`, and each of those rules stops further processing of its messages. A forwarding rule placed after them, for example at the end of `/etc/rsyslog.conf`, only forwards the system logs. The `005-` prefix makes rsyslog read the forwarding rule first, so every message is forwarded.

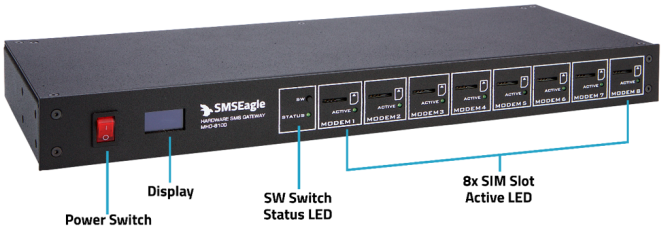
To encrypt the log traffic with TLS, see the rsyslog guide Encrypting Syslog Traffic with TLS.

Troubleshooting

To make sure that the device is working properly, follow the three steps:

1. Verification of LEDs
2. Checking the device information (System info)
3. Check the device logs (description below)

Verification of LEDs



Front panel LEDs

Normal operation of the device is signaled by LEDs as follows:

LED	Correct operation
Power (button light)	Continuously lit
STATUS	Blinking
ACTIVE1-8	Slow flashing in stand-by mode, quick flashing when the corresponding modem is in use

Checking the device information

The device information (device type, software version, modem IMEI, IMSI, network signal strength, network name) can be found under **System > System info**. See System.

Device logs

Under **System > Logs** you can find the latest lines of device logs: modem log, database log, and system log. In case of any problems with the device, these logs are a valuable source of troubleshooting information.

Extended device logs can be downloaded via the **Download logs** button on the same page. See System.

When the device is not reachable

1. Check if the device is correctly connected to the network. Check the LED status of the RJ45 socket.
2. If the device does not respond due to a malfunction or incorrect user settings, reboot the device using the power switch (or the RESET switch on the back panel).
3. If you still cannot connect to the device, it is possible to restore factory IP settings using the SW button.

Restoring factory defaults

The Reset to Default Settings function allows you to quickly restore the device to its original factory configuration.

> **Warning**
>
> Restoring factory defaults permanently removes current user configuration. Ensure any necessary settings or data are backed up before proceeding.

Restoring factory defaults resets the following to their default values: **IP settings, time zone settings, database content, and Linux OS users/passwords.**

To initiate the reset:

1. **When the device is ready to operate** (STATUS LED is blinking), press and hold the **SW** button for 10 seconds.
2. Release the SW button after 10 seconds - the display shows **"Factory reset"**.
3. Wait until the system reboots. Default settings are restored.

Note: after the reboot the device is still finishing the factory-reset process, so the system can take longer than usual to start.

Service & Repair

Warranty

Your SMSEagle comes with a standard 2 years of technical support and hardware repair warranty coverage. The standard warranty can be extended during device purchase to 3-years coverage (check your purchase conditions). For detailed information on warranty terms and conditions check the warranty card that comes with your device or follow the link: www.smseagle.eu/downloads

Service

Before contacting the support team, be sure that you have read the Troubleshooting section of this manual. More information and useful hints about SMSEagle device configuration can also be found in our online knowledgebase, at the same address as the support portal below.

SMSEagle Support Team is available by email or telephone.

Support Portal & Knowledgebase: https://support.smseagle.eu

Email: support@smseagle.eu

Phone: + 48 61 6713 413

The support service is provided by: Proximus Sp. z o.o. ul. Piątkowska 163, 60-650 Poznan, Poland

When contacting the support team, be prepared to provide the following information:

System Logs

Go to **System > Logs > Download logs**. Provide the log package to the support team when requested.

MAC address

Each SMSEagle device has a unique MAC address. It is printed on the device body, or can be found under **System > System info**.

Tech Specs & Safety Information

Technical Specification

Hardware Specification

- Processor type: Intel(R) Celeron(R) CPU N3350
- Operational memory (RAM): 2GB DDR4
- 32GB eMMC storage
- Network interface: Gigabit Ethernet 10/100/1000 TX (2xRJ45)
- HDMI+DP (for debugging purposes only)
- Other external ports: 2x USB 3.0
- Power consumption: 40W max
- Noise level: Fan-less
- Dimensions: (width x depth x height) 44 × 15.5 × 4.5 cm
- Weight: 1.8 kg
- Casing: metal (rack mount)
- Operating parameters:
    - Operating temperature: 32-140°F / 0~60°C
    - Humidity: 0%~90%RH (non-condensing)
- 8x Internal modem

Device type MHD-8100-3G

- Waveband: GSM, UMTS
- GSM/GPRS quad-band 850/900/1800/1900 MHz
- UMTS 800/850/900/AWS 1700/1900/2100 MHz
- Output power (Rated):
    - E-GSM 900: Class 4, DCS 1800: Class1
    - EDGE 900: Class E2, EDGE 1800: Class E2
    - FDD I: Class 3, FDD VIII: Class 3

Device type MHD-8100-4G

- Wavebands: UMTS, LTE
- 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
- Output power (Rated):
    - Class 3 (24dBm+1/-3dB) for WCDMA bands
    - Class 3 (23dBm±2dB) for LTE-FDD bands
    - Class 3 (23dBm±3dB) for LTE-TDD bands
- SIM card standard: mini
- Antenna connector: 8x SMA
- Country of origin: European Union (Poland)

Power Supply

AC line input

Voltage ranges: 100-240V alternating current (AC)

Frequency: 50-60Hz single phase

AC plug type: IEC13 (AC socket type: IEC14)

Antenna

- Omnidirectional max. 2dBi
- Wavebands: UMTS, LTE
- Plug type: SMA
- Impedance: 50 Ohm

Sending/Receiving Throughput

- Incoming transmission rate: up to 8× 30 SMS/min
- Outgoing transmission rate: up to 8× 30 SMS/min

Software Platform

- Operating system:
    - device Rev.1.1: Ubuntu 22.04
    - device Rev.1: Ubuntu 18.04
- built-in Apache2 web server
- built-in PostgreSQL database server
- built-in Postfix email server
- built-in SNMP agent
- built-in NTP-client

- built-in Failover (HA-cluster) service
- watchdog mechanism for built-in modems
- failover mechanism for built-in modems
- modern responsive web interface
- list of open TCP/UDP ports in default configuration:
    - TCP: 22 (SSH), 80 (HTTP), 443 (HTTPS), 5432 (Postgresql with access restriction to localhost only)
    - UDP: 68 (DHCP client), 323 (NTP client)

Important Safety Information

This chapter provides important information about safety procedures. For your safety and that of your equipment, follow these rules for handling your device.

> **Warning**
>
> Incorrect storage or use of your device may void the manufacturer's warranty. Failure to follow these safety instructions could result in fire, electric shock, or other injury or damage.

Always take the following precautions.

Disconnect the power plug from AC power source or if any of the following conditions exist:

- the power cord or plug becomes frayed or otherwise damaged
- you spill something into the case
- the device is exposed to rain or any other excess moisture
- the device has been dropped or the case has been otherwise damaged

Be sure that the use of this product is allowed in your country and in the environment required. As with any other telecommunication equipment, the use of this product may be dangerous and has to be avoided in the following areas: where it can interfere with other electronic devices located in close proximity in environments such as hospitals, airports, aircrafts, etc.; where there is risk of explosion such as gasoline stations, oil refineries, etc.

It is the responsibility of the user to enforce the country regulation and the specific environment regulation.

Do not disassemble the product; any mark of tampering will compromise the warranty validity.

Every device has to be equipped with a proper antenna with specific characteristics. The antenna has to be installed with care in order to avoid any interference with other electronic devices and has to be installed with the guarantee of a minimum 23 cm distance from the body. In case this requirement cannot be satisfied, the system integrator has to assess the final product against the SAR regulation.

DISCLAIMER: The manufacturer is not responsible for any damages caused by inappropriate installation, not maintaining the proper technical condition or using a product against its destination.

Regulatory Statements

EU Declaration of Conformity

Hereby, Proximus Sp. z o.o., owner of SMSEagle brand, declares that the radio equipment type SMSEagle MHD-8100-4G, MHD-8100-3G is in compliance with Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at the following internet address: www.smseagle.eu/certification

FCC Compliance Statement

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

Note:

This equipment has been tested and found to comply with the limits for a Class B device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a business/commercial non-residential environment. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

Important:

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instruction manual, may cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense. The FCC regulations provide that changes or modifications not expressly approved by SMSEagle™ could void your authority to operate this equipment. This product has demonstrated EMC compliance under conditions that included the use of compliant peripheral devices (antennas)

and shielded cables between system components. It is important that you use compliant peripheral devices and shielded cables between system components to reduce the possibility of causing interference to radios, televisions, and other electronic devices.

FCC Supplier's Declaration of Conformity



This Supplier's Declaration of Conformity is hereby issued according to Chapter 1, Subpart A, Part 2 of Title 47 of the Code of Federal Regulations by:

Proximus Sp. z o.o. ul. Piatkowska 163 60-650 Poznan, Poland

The product MHD-8100-4G complies with the applicable requirements of FCC Rule Part 15B for the corresponding equipment classes of Unintentional Radiators.

RESPONSIBLE PARTY located in the United States:

Testing Partners LLC

18200 SR 306

Chagrin Falls, OH 44023

info@testingpartners.com

The responsible party warrants that each unit of equipment marketed under this Declaration of Conformity will be identical to the unit tested and found acceptable with the standards and that the records maintained by the responsible party continue to reflect the equipment being produced under such Supplier's Declaration of Conformity continue to comply within the variation that can be expected due to quantity production and testing on a statistical basis.

Canadian Regulatory Statement (ISED)

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) this device may not cause interference, and

(2) this device must accept any interference, including interference that may cause undesired operation of the device.

This Class B digital apparatus meets the requirements of the Canadian Interference-Causing Equipment Regulations.

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)

UK Declaration of Conformity

Hereby, Proximus Sp. z o.o., owner of SMSEagle brand, declares that the radio equipment type SMSEagle MHD-8100-4G, MHD-8100-3G is in compliance with The Radio Equipment Regulations 2017.

The full text of the EU declaration of conformity is available at the following internet address: www.smseagle.eu/certification

RF Exposure Limits

This device complies with radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the radio frequency exposure limits, human proximity to the antenna shall not be less than 23 cm (9 inches) during normal operation.

Disposal and Recycling Information

Your SMSEagle device contains a lithium battery for RTC backup. Dispose of the device and/or battery in accordance with local environmental laws and guidelines.

European Union - Disposal Information



The symbol above means that according to local laws and regulations your product shall be disposed of separately from household waste. When this product reaches its end of life, take it to a collection point designated by local authorities. The separate collection and recycling of your

product at the time of disposal will help conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment.

For disposal in countries outside of the European Union

This symbol is only valid in the European Union (EU). If you wish to discard this product please contact your local authorities or dealer and ask for the correct method of disposal.

Information gemäß § 4 Absatz 4 Elektrogesetz (DE)

Folgende Batterien bzw. Akkumulatoren sind in diesem Elektrogerät enthalten

Hardware	Batterietyp	Chemisches System
Rev.1 Rev.1.1	CR2032	Lithium

Angaben zur sicheren Entnahme der Batterien oder der Akkumulatoren

Öffnen Sie die obere Abdeckung des Geräts. Die Batterie der Echtzeituhr (RTC) befindet sich in der Nähe der Rückseite des Geräts. Trennen Sie den 2-poligen PicoBlade-Stecker (rotes und schwarzes Kabel) von der Hauptplatine und entnehmen Sie anschließend die Batterie aus dem Gerät. Die Batterie und das Gerät können anschließend getrennt entsorgt werden.

Restriction of Hazardous Substances Directive (RoHS)

European Union RoHS

SMSEagle devices sold in the European Union, on or after 3 January 2013 meet the requirements of Directive 2015/863 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (“RoHS 3”).