DOCUMENTATION 6.32

NXS-9750 User's Manual

Documentation

ENGLISH · SMSEAGLE

Table of contents

Cover . . . 7

SMSEagle Software Licensing Information . . . 8

What's In The Box . . . 16

Prepare for First Start . . . 17

Connectors, Ports and LEDs . . . 21

Basic Operations . . . 23

SMSEagle features . . . 24

- Compose SMS . . . 24
  - Importing SMS from CSV and using placeholders . . . 25
- Calls (Voice feature) . . . 26
  - Wake Up Calls (Ring only) . . . 27
  - Text-To-Speech (TTS) Calls . . . 27
  - Audio file calls . . . 27
  - Incoming calls . . . 29
  - Retry attempts . . . 29
  - TTS offline voice models . . . 29
  - TTS online Voice models . . . 29
  - Temporary files cleanup . . . 30
- Folders . . . 30
  - MMS . . . 31
  - Sent items status . . . 32
  - Inbox rules . . . 33
  - Cleanup Folders . . . 35
- Phonebook . . . 36
  - Phonebook Contacts . . . 36
  - Phonebook Groups . . . 39
  - Phonebook Escalation Groups . . . 39
  - Phonebook Working Shifts . . . 40
- Users . . . 41
- Multi-User Capabilities . . . 43
- User Settings . . . 43
  - Personal Data . . . 43
  - Password . . . 44
- Multi-Factor Authentication (MFA) . . . 44
  - Enable MFA from User Settings . . . 44
  - User login with MFA . . . 45
  - Recovery code . . . 46
  - Enable MFA by administrator . . . 46
- Reporting module . . . 47
  - Statistics view . . . 48
  - Periodic reports/statistics . . . 49

Network Monitoring . . . 49
Control status of all your defined tasks . . . 50
Define what you want to monitor in each task . . . 50
Define a schedule . . . 51
Define a SMS alert message . . . 52
Receive SMS alerts . . . 52
Voice Call . . . 53
Network Monitoring Probes . . . 53
Reports . . . 55
SNMP Traps . . . 55
Emails . . . 57
Email to SMS . . . 57
Basic usage . . . 57
Send to username/group . . . 57
Send to Ldap contacts/groups . . . 58
Voice Call . . . 58
Using FQDN in email address . . . 58
Email subject - additional parameters (optional) . . . 58
Feature configuration . . . 59
Email to SMS Poller . . . 62
Basic example . . . 63
Send to username/group . . . 63
Send to Ldap contacts/groups . . . 63
Voice Call . . . 63
Feature configuration . . . 63
Feature configuration for Office 365 OAuth2 . . . 67
SMS to Email . . . 67
Feature configuration . . . 67
Email text from this feature . . . 70
Email Alerts . . . 70
Email Conversations . . . 72
SMTP Configuration . . . 72
Workflows . . . 74
Workflow builder . . . 75
Dynamic recipient placeholders . . . 78
SMS Forward . . . 78
Feature configuration . . . 78
Voice Call . . . 79
MQTT . . . 79
Feature configuration . . . 80
Subscribe rules . . . 81
Publish rules . . . 81
WhatsApp . . . 81
Send WhatsApp message with SMS/MMS fallback . . . 84
Signal (beta) . . . 85
Webhooks (aka. Callback URL) . . . 85
Feature configuration . . . 85

Request parameters . . . 88
Expected HTTP response & retry attempts . . . 88
Zabbix ACK with SMS . . . 88
Autoreply . . . 89
Feature configuration . . . 89
Subscriptions (newsletter) . . . 90
Periodic SMS . . . 92
Feature configuration . . . 92
Voice Call . . . 93
Digital I/O . . . 93
Using digital outputs . . . 94
Using digital inputs . . . 95
DI/DO feature configuration . . . 96
Voice Call . . . 100
Temperature & humidity sensors . . . 101
Feature configuration - Alarms . . . 102
Feature configuration - settings . . . 103
Reading Temp/Humidity via SNMP Protocol . . . 104
Connecting an External Temperature sensor . . . 104
LDAP . . . 105
Feature configuration . . . 105
Authentication to SMSEagle via LDAP (optional) . . . 108
Allow/Deny List . . . 110
Mode: Allow selected . . . 111
Mode: Deny selected . . . 112
Stop word . . . 113
SMPP . . . 114
Settings . . . 115
Application Settings . . . 115
IP Settings . . . 117
Failover . . . 118
Date/Time . . . 118
Maintenance . . . 118
Call Forward . . . 120
MMS . . . 120
Data Connection . . . 121
SNMP . . . 122
SSL Certificate and HTTPS Redirection . . . 123
Backup/Restore . . . 124
Updates . . . 125
Logs . . . 127
Sysinfo . . . 128
Failover (HA-cluster) feature . . . 129
How to configure failover (HA-cluster): . . . 130
SNMP-monitoring of HA-cluster . . . 131
Multimodem features . . . 133
Multimodem selection strategy . . . 133

Enable modem failover mechanism . . . 133

SMSEagle API . . . 134
API Reference (Documentation) . . . 134
API Access . . . 134
Access to resources of other users in API . . . 134

Plugins and integrations . . . 136

Extras . . . 137
Delivery Reports . . . 137
Connecting directly to SMSEagle database . . . 138
Injecting short SMS using SQL . . . 138
Injecting long SMS using SQL . . . 139
Database cleaning scripts . . . 141
SNMP agent . . . 141
Example of readingGSM_Signal1value using NET-SNMP library . . . 146
Example of readingGSM_NetName1value using NET-SNMP library . . . 146
Example of readingFolderOutbox_Totalvalue using NET-SNMP library (and textual name of metric) . . . 146
Example of readingsystem uptimefrom Linux host using NET-SNMP library . . . 146
Example of browsing SMSEagle extension parameters IN mib tree using NET-SNMP library . . . 147
Example of browsing SMSEagle extension parameters IN mib tree using mib-browser . . . 147
Setting up SNMP v3 access control . . . 148
Forwarding logs to external server . . . 148
Automatic software updates check . . . 149
Manual CHECK . . . 149
Automatic check . . . 149
Knowledgebase & Support Portal . . . 150

Troubleshooting . . . 151
Verification of LEDs . . . 151
Checking the device information . . . 151
Device logs . . . 152
When the device is not reachable . . . 152
Restoring factory defaults . . . 152
Service & Repair . . . 153
Warranty . . . 153
Service . . . 154
When contacting support team, be prepared to provide the following information: . . . 154

Tech Specs & Safety Information . . . 155
Technical Specification . . . 155
Hardware Specification . . . 155
Power Supply . . . 157
Antenna . . . 157
Sending/Receiving Throughput . . . 157
Software Platform . . . 158
Important Safety Information . . . 158

Regulatory Statements 160
EU Declaration of Conformity 160
FCC Compliance Statement 160
FCC Supplier's Declaration of Conformity 161
Canadian Regulatory Statement (ISED) 161
Avis de conformité à la réglementation d'Industrie Canada 162
UK Declaration of Conformity 162
RF Exposure Limits 162
Disposal and Recycling Information 162
Information gemäß § 4 Absatz 4 Elektrogesetz (DE) 163
Restriction of Hazardous Substances Directive (RoHS) 163

Cover

CONGRATULATIONS ON PURCHASING

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
- 2x External omnidirectional antenna (with magnetic foot)
- AC/DC power supply (input voltage: 100-240V)
- Quick Start Guide
- Warranty card

Prepare for First Start

Your SMSEagle is designed so that you can set it up quickly and start using it right away. Follow the steps below to get started.

STEP 1: Install 3G/4G antennas

Antenna installation guidelines

- Install antennas in a location with access to a cellular network radio signal.
- Antennas must be installed such that it provides a separation distance of at least 30 cm (12 inches) from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Antennas must not be installed inside metal cases.
- Make sure the SMSEagle antennas are placed at least 50cm (20 inches) from each other to avoid cross-modulation.

Plug in both antenna connectors to the SMSEagle device.

STEP 2: Insert SIM Card

Please install SIM Card when the device is SWITCHED OFF. SIM Card slots is located at the bottom of the device. Use a ball-pen or small screwdriver to eject SIM Card tray. Insert card into tray and push it gently into slot.



Insert SIM card

STEP 3: Power the device

The device is powered with AC/DC power supply adaptor delivered in the box. The device needs a power source of 12V. In order to power the device simply plug in a connector from AC/DC adaptor into the device. Alternatively device can be powered via PoE+ (hardware Rev.4 only).

STEP 4: Configure IP settings



Network connection diagram

> **Note**
>
> **SMSEagle default network configuration: DHCP client is on** (IP address will be obtained automatically from your DHCP server)

A) Connect SMSEagle to your LAN and obtain IP address automatically

- connect the device to your LAN using Ethernet cable
- SMSEagle will obtain IP address automatically from your DHCP
- read assigned IP address on your DHCP server

B) Or set IP address for SMSEagle manually

- connect a display using HDMI connector, connect a keyboard to USB port (note: cables are not provided)
- login to the terminal window using root credentials (these were provided with your device)
- edit configuration file with command:

```
nano /mnt/nand-user/smseagle/syscfg
```

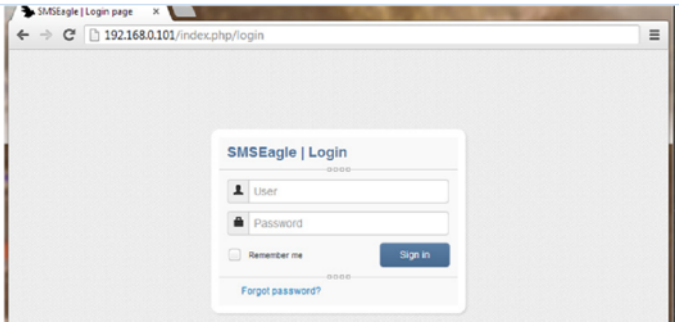
change the following lines:

```
HOST_IP= (set IP address for your device)
GW_IP= (default gateway IP address)
NET_MASK= (set subnet mask)
START_DHCP=Y (set to START_DHCP=N to disable DHCP client)
```

- save and exit the file
- shutdown the device
- now connect SMSEagle to your LAN using Ethernet cable

C) Log in to SMSEagle

Open an internet browser on your PC and go to the IP address assigned to your gateway

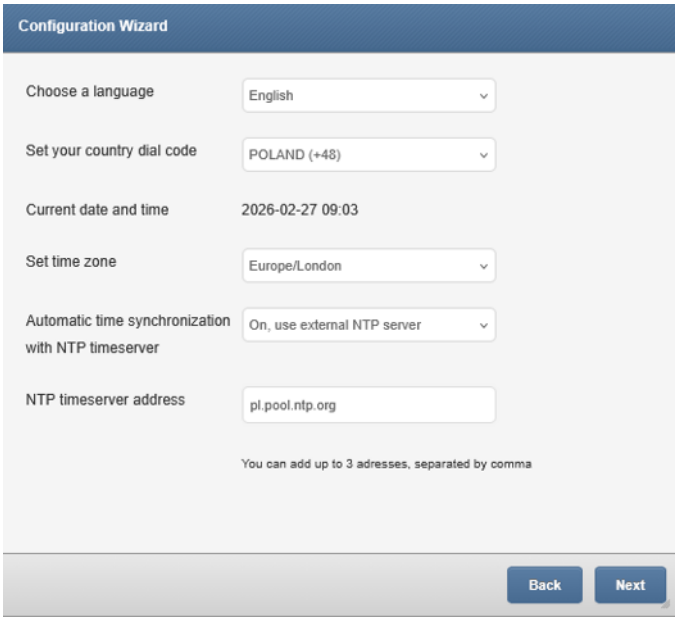


SMSEagle login page

> **Note**
>
> **SMSEagle default user:**
>
> Username: `admin` Password: `password`
>
> Login to application with above username and password.

STEP 5: Configuration Wizard

New SMSEagle devices are equipped with a built-in Configuration Wizard that guides the user through the initial setup process step by step. The wizard is launched automatically on first login and covers the most important configuration areas: SIM card setup, time zone, and user password change. The wizard can be skipped and accessed again later from the Settings menu.



Configuration Wizard

STEP 6: Installing custom SSL certificate and HTTPS-only **(OPTIONAL)**

Installing your own SSL certificate

SMSEagle device comes with a self-signed SSL certificate. Follow the instructions in the chapter SSL Certificate and HTTPS Redirection if you want to install your own SSL certificate or a free Let's Encrypt SSL certificate.

Using HTTPS only

By default, SMSEagle web GUI can be accessed via HTTP or HTTPS. For improved security we recommend using HTTPS. If you would like to redirect HTTP > HTTPS, follow instructions in the chapter SSL Certificate and HTTPS Redirection.

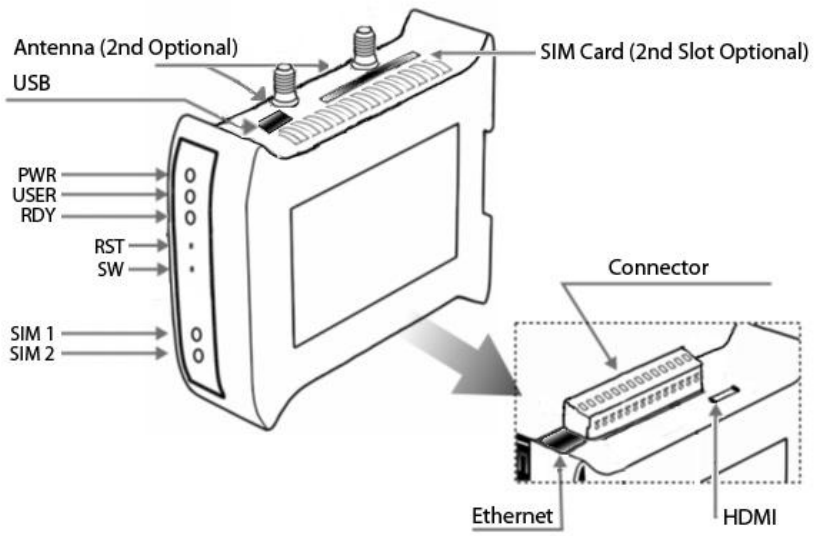
STEP 7: Reboot the device

Go to Settings > Maintenance Tab. Press **Reboot** button.



Reboot button

Connectors, Ports and LEDs

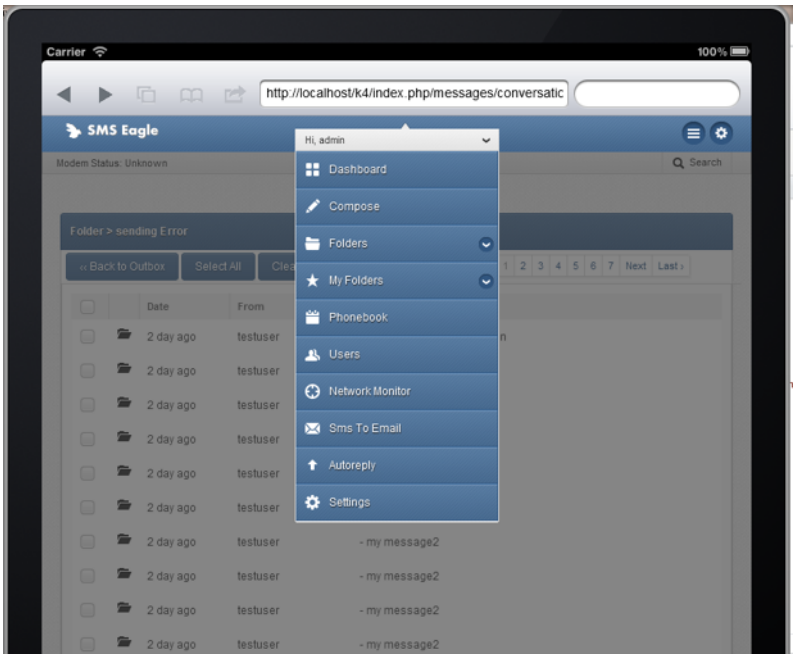


Connectors, ports and LEDs

Element	Label	Description
VCC (Rev.4,Rev.3 only)	VCC	Power connector
12-pole connector	–	4x digital Input, 4x digital output, 1× 1Wire, 1× 5V, 2x GND
SIM Card Slot	SIM1, SIM2	SIM card slots
HDMI port	HDMI	HDMI port (for debugging purposes only)
USB port	USB	USB port (for debugging purposes only)
Ethernet Port	ETH	Ethernet RJ45 socket
Antenna	ANT	Antenna socket
Power LED	PWR	LED indicating power-on
User LED	USER	LED for user application purpose
SIM1,2 LEDs	Modem 1,2 (optional)	LED indicator for modem status
Ready LED	RDY	LED indication device status
Reset	RST	Switch for rebooting the device
User Switch	SW	Switch for restoring to factory settings

Basic Operations

SMSEagle is capable of working at various screen resolutions, making it accessible for a wide range of devices: computers, laptops, tablets, smartphones, etc.



Open a web browser on your device, type in SMSEagle's IP address (as set in the previous chapter). At login screen type in your username/password. Default username and password is given in chapter **Prepare for the First Start**.

Important Notice: The Web-GUI requires a modern web browser with JavaScript support. Older web browsers (like Internet Explorer) are not supported and may not work properly.

Basic operations include:

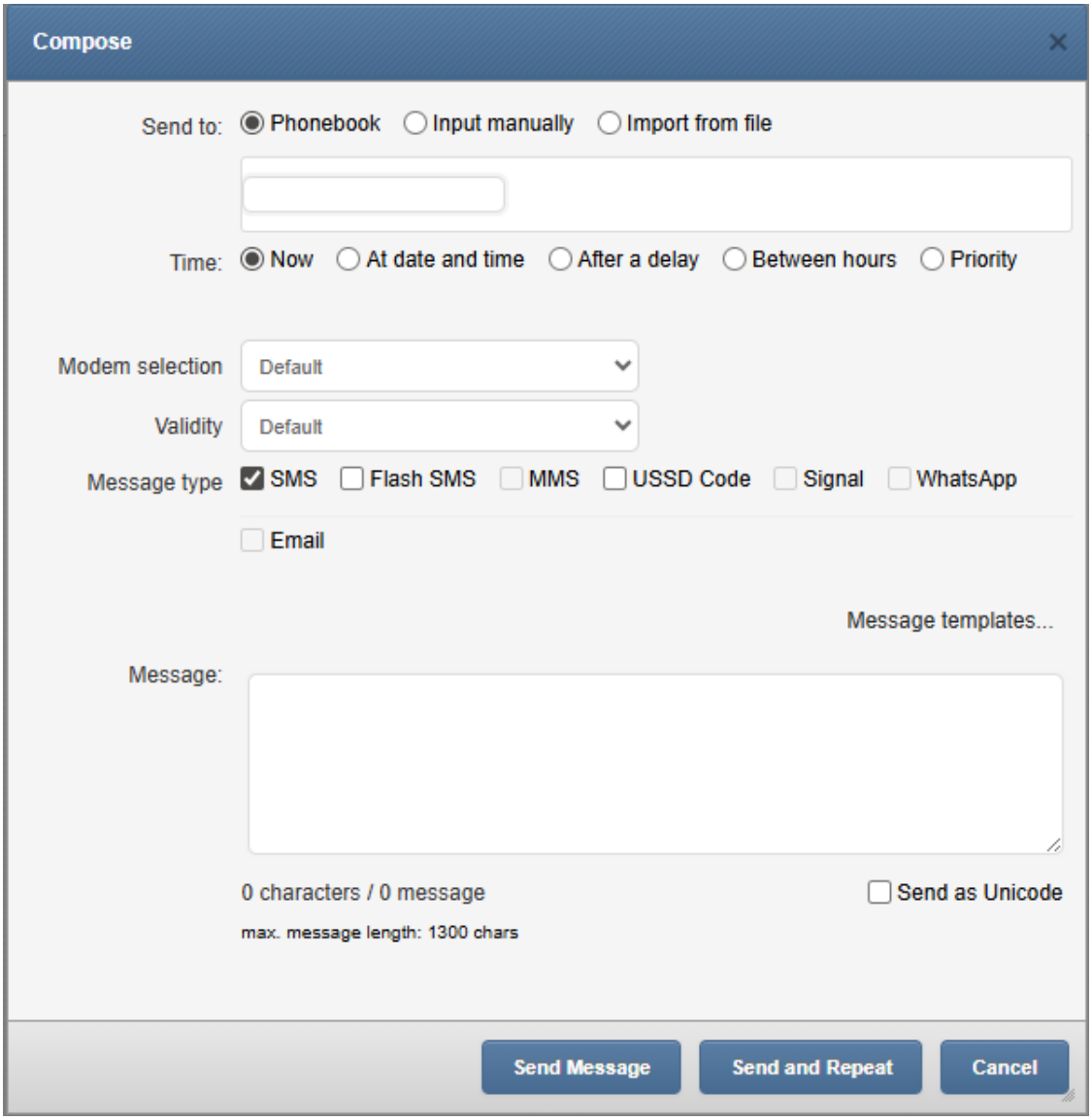
- Sending & Receiving SMS (managing messages with Inbox, Outbox, Sent Items). Different message types (normal SMS, flash, WAP push, USSD codes)
- Sending & Receiving MMS (web GUI & API)
- Smartphone-like conversation mode (messages are nicely grouped by phone number). You can easily track history of what you send and receive
- Sending to single numbers, contacts or groups from phonebook
- Import messages for sending from CSV file
- SMS Scheduling by specified date and time or delay
- SMS sending within specified time window (between selected hours)
- Message templates (save & edit your own templates)
- Unicode support (support of national characters)
- Multiuser support (each user has access to a private Inbox, Outbox, Sent Items)

SMSEagle features

Below you will find a detailed description of all the features offered by the SMSEagle software. The order of the descriptions matches that of the SMSEagle web GUI.

Compose SMS

Here we show the various ways of sending an SMS form your device.



Screenshot of default Compose SMS view

In Compose SMS users can:

- Send SMS to contact from phonebook, input manually or import from file

- When importing from file each column can be used as a placeholder in the message. During sending the placeholder will be replaced by a unique value for each imported row from CSV file. This allows you to send a personalized message to each recipient.
- Set send date to now, at a date and time, after a delay, between selected hours or with high priority.
- Set duration validity of SMS
- Select a type of message: normal SMS, flash SMS, MMS, USSD Code, Email, Signal or WhatsApp
- Set a message template to be saved and used at another time
- Send as Unicode (for special character use)
- Send message or Send and Repeat (window remains open, allowing modifications to next message)

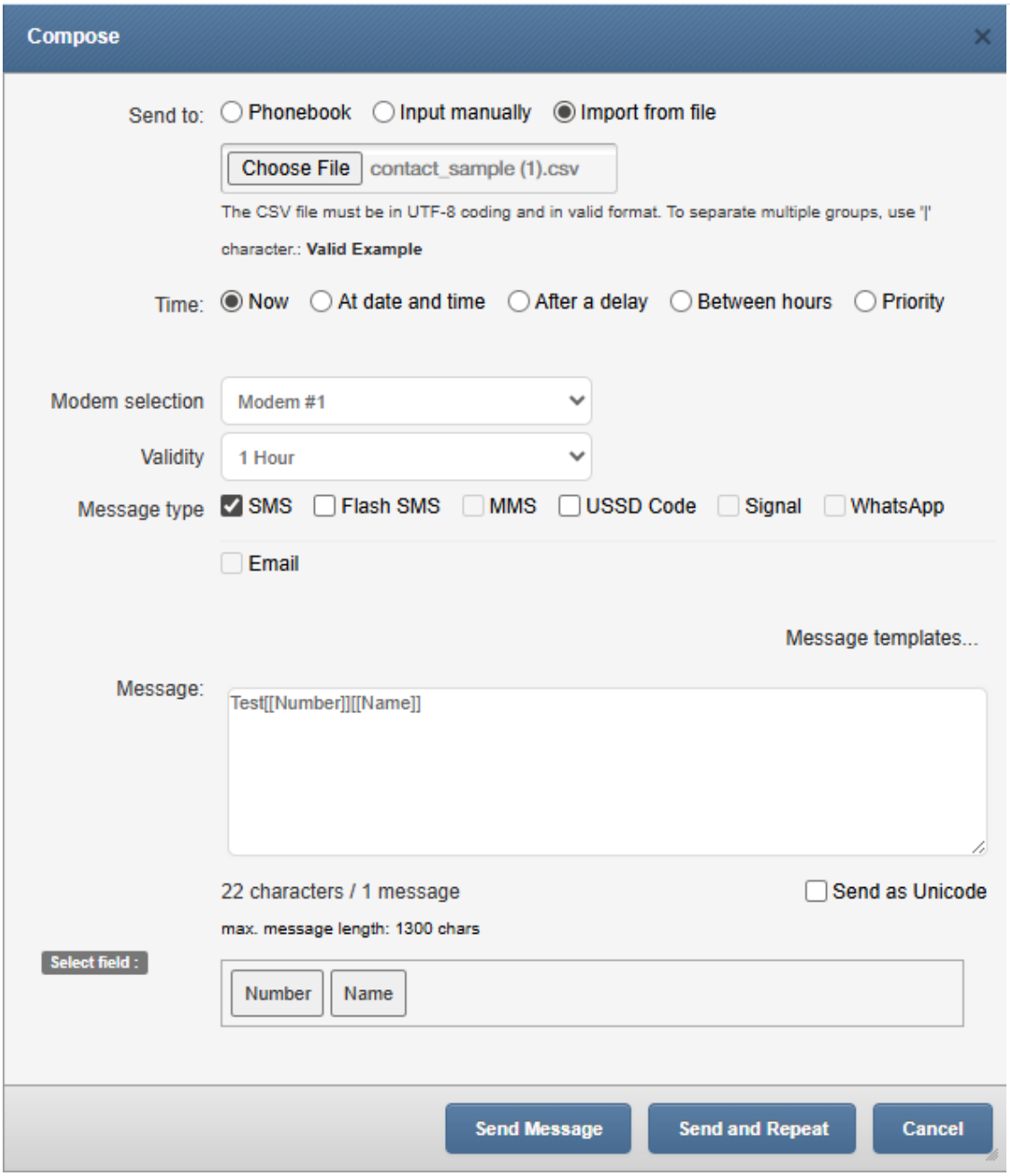
Importing SMS from CSV and using placeholders

SMSEagle software allows you to import SMS text from CSV file and (optionally) use special placeholders in a message body. Placeholders are special fields which are replaced with unique values for each message.

First a .csv file is needed like in the example below. Columns can be added and named as needed.

	A	B	C	D
1	Name	Number	ExtraColumn	
2	John Doe	123123123	asdasdasd	
3	John Kennedy	23123123	dsadsa	
4	John Kowalski	4215456456	qwerty	
5				

When composing an SMS using .csv file as a source, each column in the uploaded .csv file becomes a placeholder that will fill in the information from your file. Placeholders can be added to the message body by clicking the column name in the “Select field” as seen below.



Screenshot of “Compose SMS” with imported .csv file.

Calls (Voice feature)

Available only to users who have purchased the VOICE add-on for their SMSEagle device.

The Calls feature allows making wake-up calls (ring only), text-to-speech calls and audio file calls to a single phone number or group of recipients. This feature is ideal for delivering urgent messages or announcements, such as alerts, emergency notifications, or other time-sensitive information. A call request can be created via SMSEagle web-GUI or API.

Wake Up Calls (Ring only)

The Wake-up call is a ring-only call that can be used to capture a recipient's attention. This feature allows for example to wake up someone during the night to draw attention to SMS containing a critical alert. When a wake-up call is made, the SMSEagle device will ring to a specified phone number or phonebook entry for a specified number of seconds.

Text-To-Speech (TTS) Calls

Available only on NXS hardware Rev.4 and MHD-8100-4G devices, due to technical limitations.

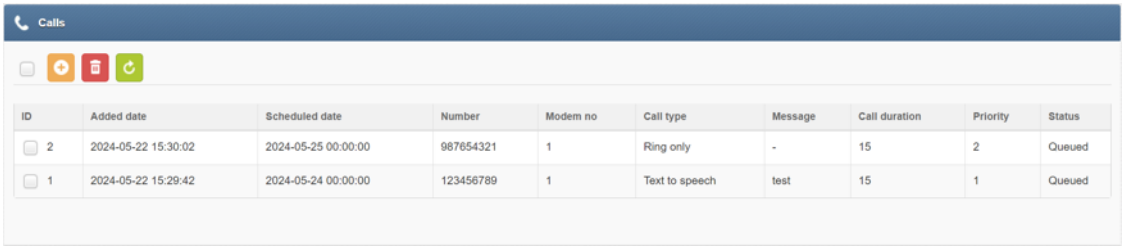
Text-To-Speech call allows converting of text message to voice call. This feature is particularly useful for businesses or organizations that must deliver important messages via voice. When a TTS call is made SMSEagle device will call a specified phone number or phonebook contact/group. The text message will be read by a built-in voice synthesizer.

There are 3 modes of text-to-speech function:

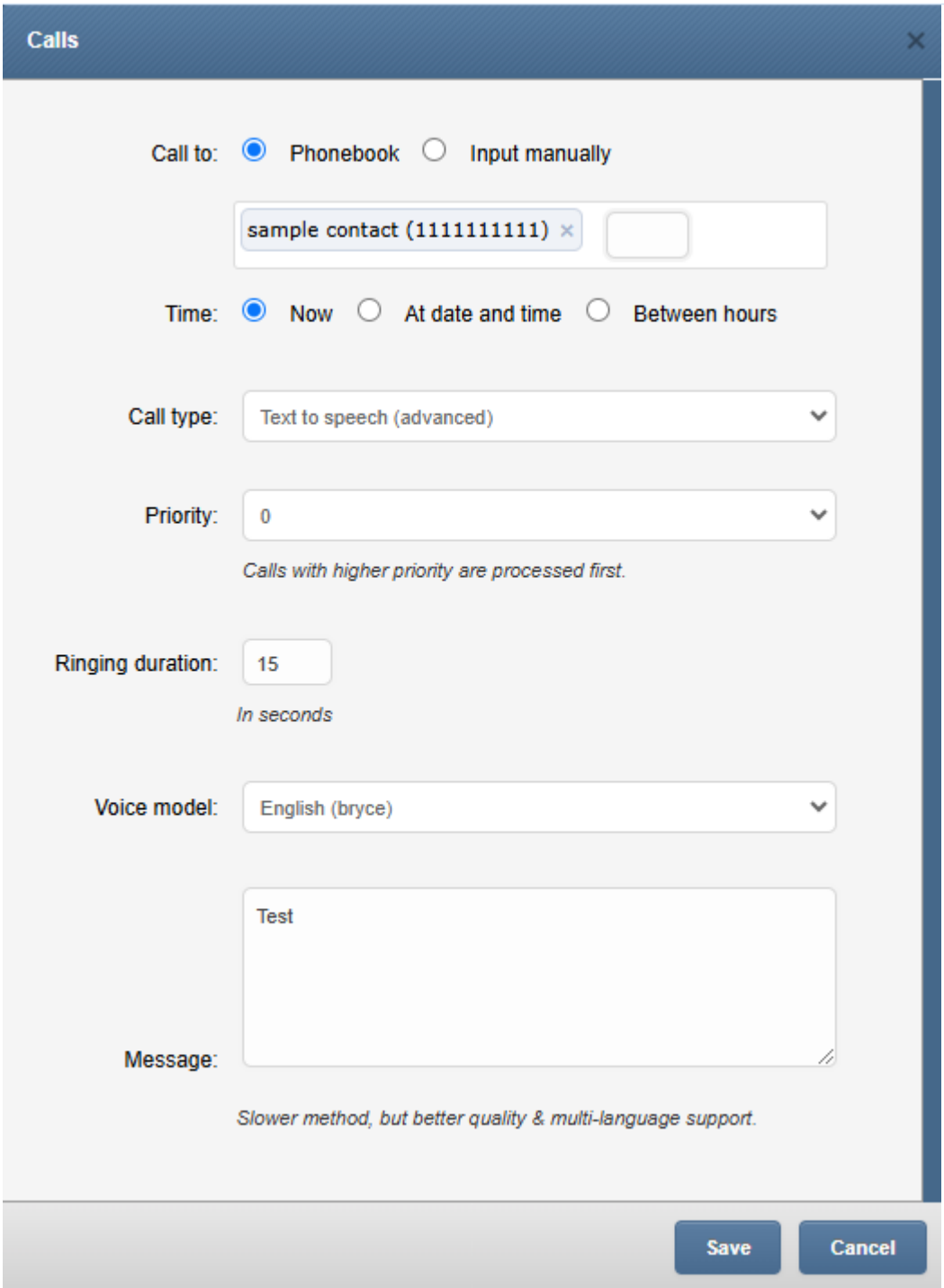
- Text to Speech Simple: faster method, but only supports English language.
- Text to Speech Advanced: supports multiple languages, provides better voice quality, but is slower for longer texts. Works offline. Playback speed can be adjusted to control how fast the message is read out.
- Elevenlabs TTS: multiple languages, excellent, natural-sounding voices. Requires an Elevenlabs account and internet access for text-to-speech conversion.

Audio file calls

The Audio File Call feature allows you to make voice calls using recorded audio (wave) files. This feature is ideal for those who prefer a personal touch for customized announcements or specific alerts. You can upload a pre-defined file in the Calls > Audio files menu. The file must meet the following requirements: Wave file format, 8 kHz or 16 kHz, mono, 16-bit PCM.



Screenshot with examples from "Calls" menu



Screenshot from New Call window

In New call window you can set:

- Contact or group from Phonebook or manual input
- Select if a call should be made immediately, at a specified date/time, or between hours
- Which modem to call from (when using a multi-modem device)
- Set call priority from 0-5
- Select call type, Ring only, Text to Speech Simple, Text to Speech Advanced, Audio File, ElevenLabs TTS

- For Text to Speech Advanced you can select language and voice model
- For Audio File you may select existing file or upload a file from your computer
- Input message when Text to speech call type is selected. Length of the text message is limited to 950 characters.

Incoming calls

SMSEagle supports handling of incoming voice calls. Incoming calls can be:

- Logged in the device call history
- Used as a trigger for Webhooks
- Configured globally via menu Settings > Maintenance, where you can set the default device behaviour to: always reject, accept or ignore incoming calls.

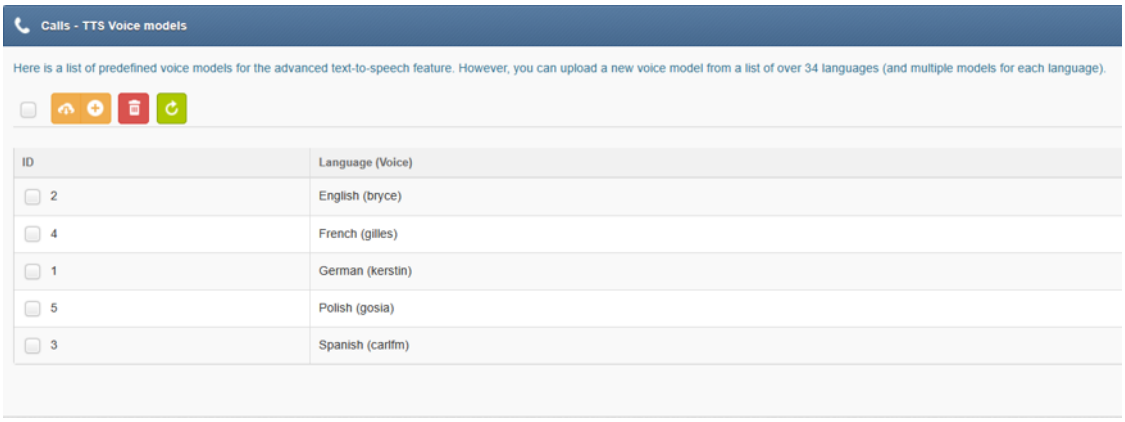
Retry attempts

If a call attempt fails, it will be automatically retried up to 2 more times.

TTS offline voice models

Text to Speech Advanced feature has 2 pre-uploaded language models: English, German. You can upload additional voice models via the Calls > TTS voice models menu. The voice model library currently contains **36 languages** and multiple voices for some of the languages. Refer to the page Voice Models to compare various voice models and listen to voice samples.

New voice models can be added automatically (the device downloads files from the repository on github.com) or manually (the files must be downloaded to the computer and uploaded using the dialog window). Once the voice model is uploaded, the TTS conversion works offline.



Screenshot from menu Calls>TTS Voice models

TTS online Voice models

Online voice models use the ElevenLabs API for text-to-speech conversion to deliver excellent, natural-sounding voices. However, you will need an ElevenLabs account to use this feature. Your SMSEagle device must also be connected to the internet for this feature to work.



Screenshot from menu Calls>TTS Online Voice models

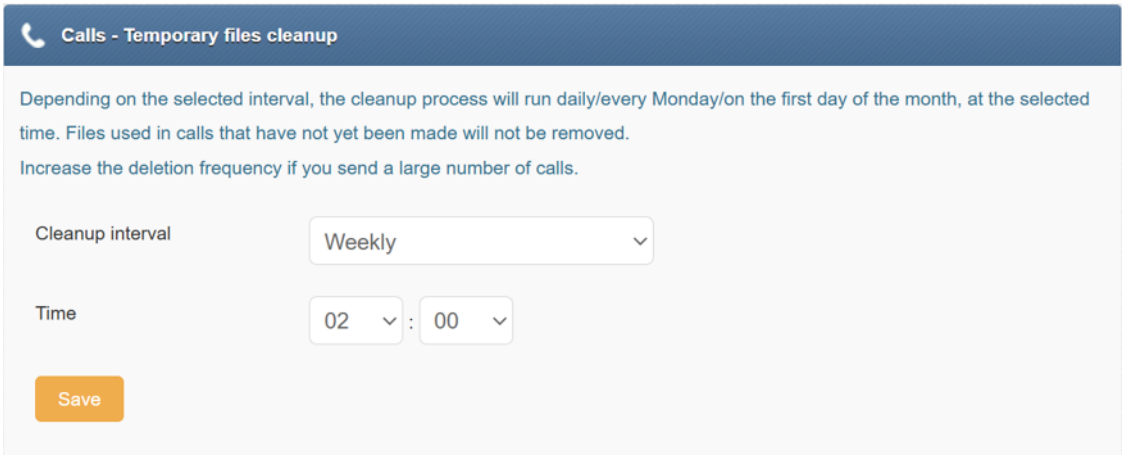
To use ElevenLabs voice calls in SMSEagle, you need to generate an ElevenLabs API key (under the Developers > API Keys tab). The following ElevenLabs API permissions are required:
Text to Speech: Access
Voices: Read.

After selecting them, save the settings and enter the ElevenLabs API key in SMSEagle web-GUI (menu Calls > TTS Online voice models, field ElevenLabs API key).

Temporary files cleanup

The Temporary voice files cleanup feature helps save storage space on the SMSEagle device by automatically removing unused temporary files created during Text-to-Speech (TTS) processing.

In the default configuration the process runs every Monday at 02:00. For systems that generate a large number of calls, it is recommended to increase the cleanup frequency to prevent excessive disk usage and ensure stable device operation. Files that are still required for scheduled or pending calls are not removed and remain fully protected.



Screenshot from menu Calls>Temporary files cleanup

Folders

Folders contain your SMS/MMS messages. Folders are conveniently grouped into 5 categories:

- Inbox
- Outbox
- Sent Items
- Inbox rules

- Trash

The view of conversations can be either of type “Balloons” (smartphone like conversation) or “Table” (tabular view). The view type can be changed in menu Settings > Application.

Balloons view type:

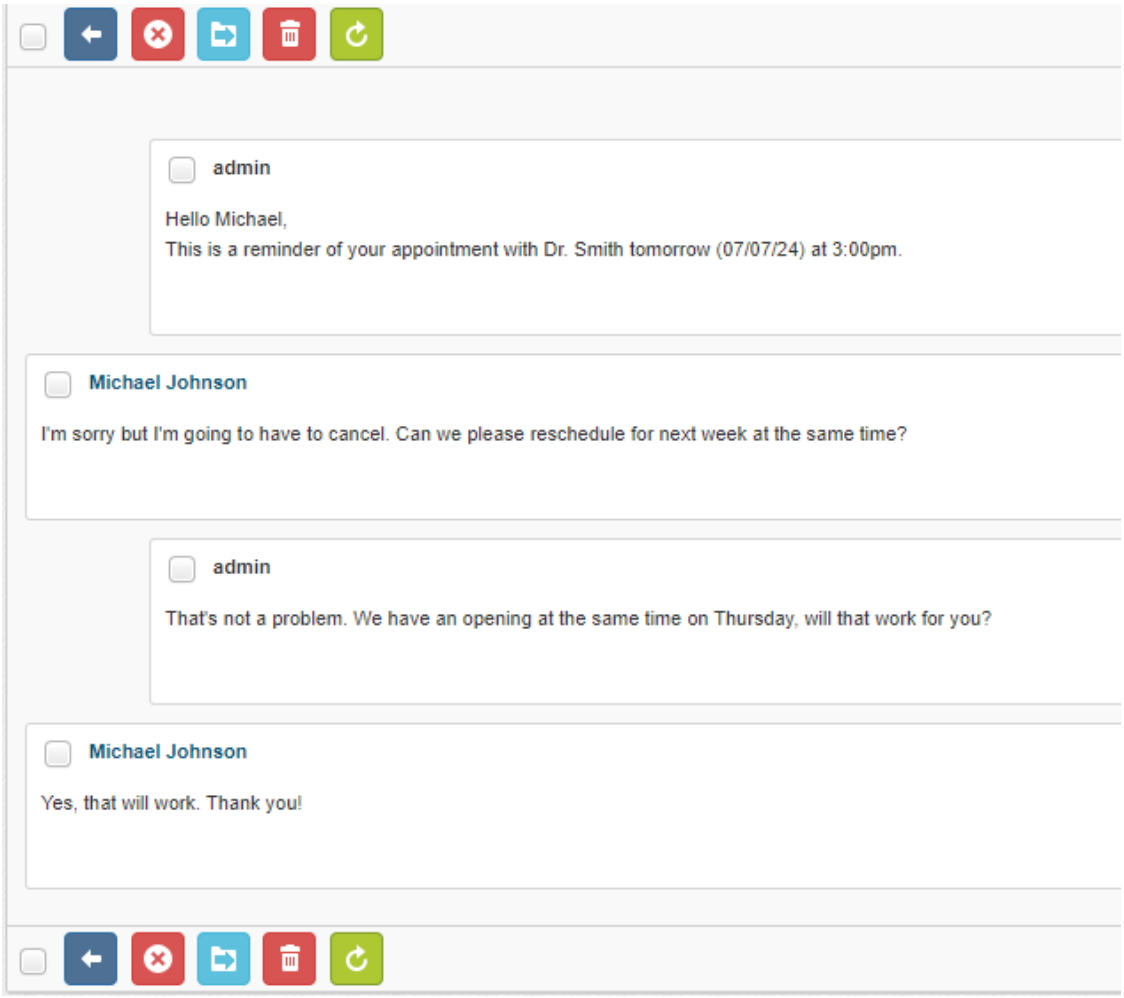
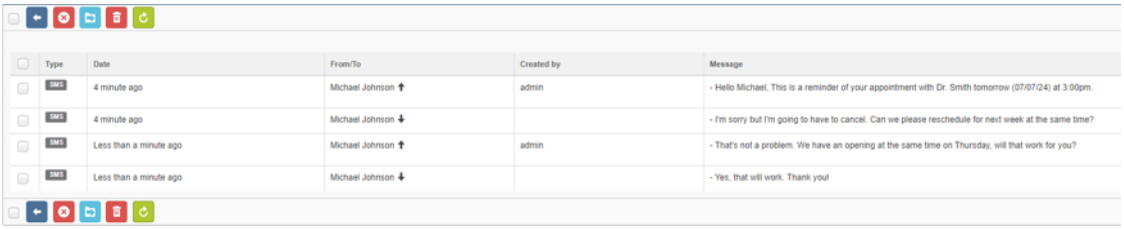
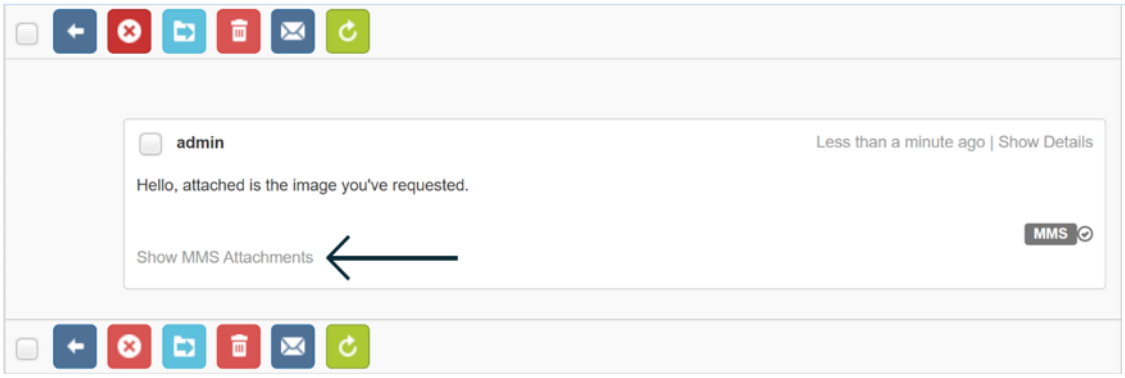


Table view type:



MMS

To view an MMS attachment, you need to click “show MMS attachment” in the inbox message.



Sent items status

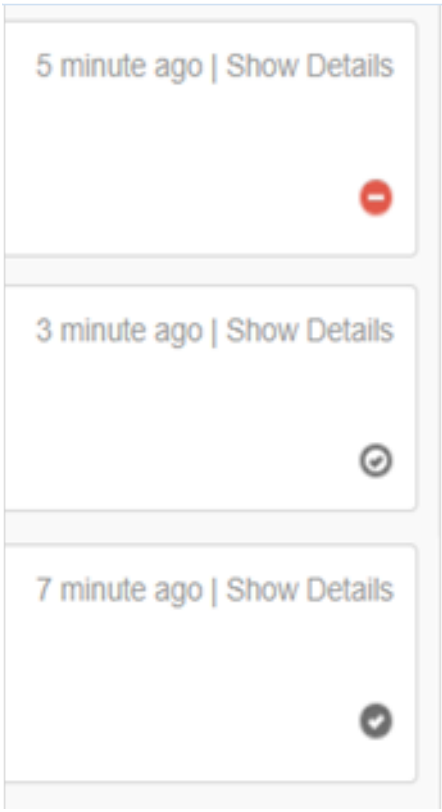
The status of a sent message can be seen in Folders>Sent Items>in selected message. There are 2 places where the sending status is displayed: status icon in the right bottom corner of each message and status text in message details (button “Show Details”).



Screenshot with examples from Folders>Sent Items>message example

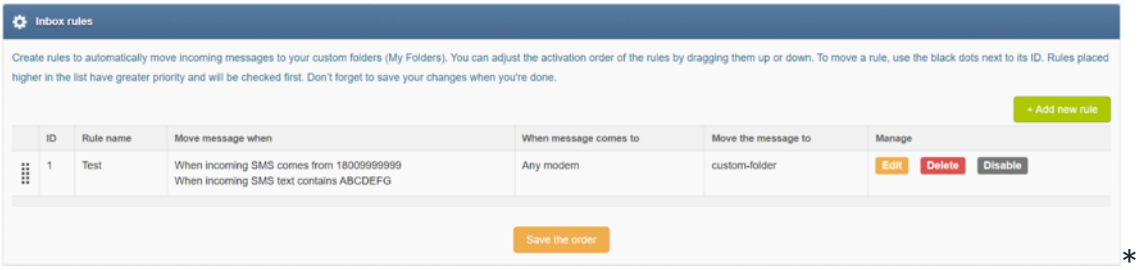
There are 3 different icons indicating the sending status:

- Sending Error
- Message Sent
- Message Delivered (only available when Delivery Reports are enabled)

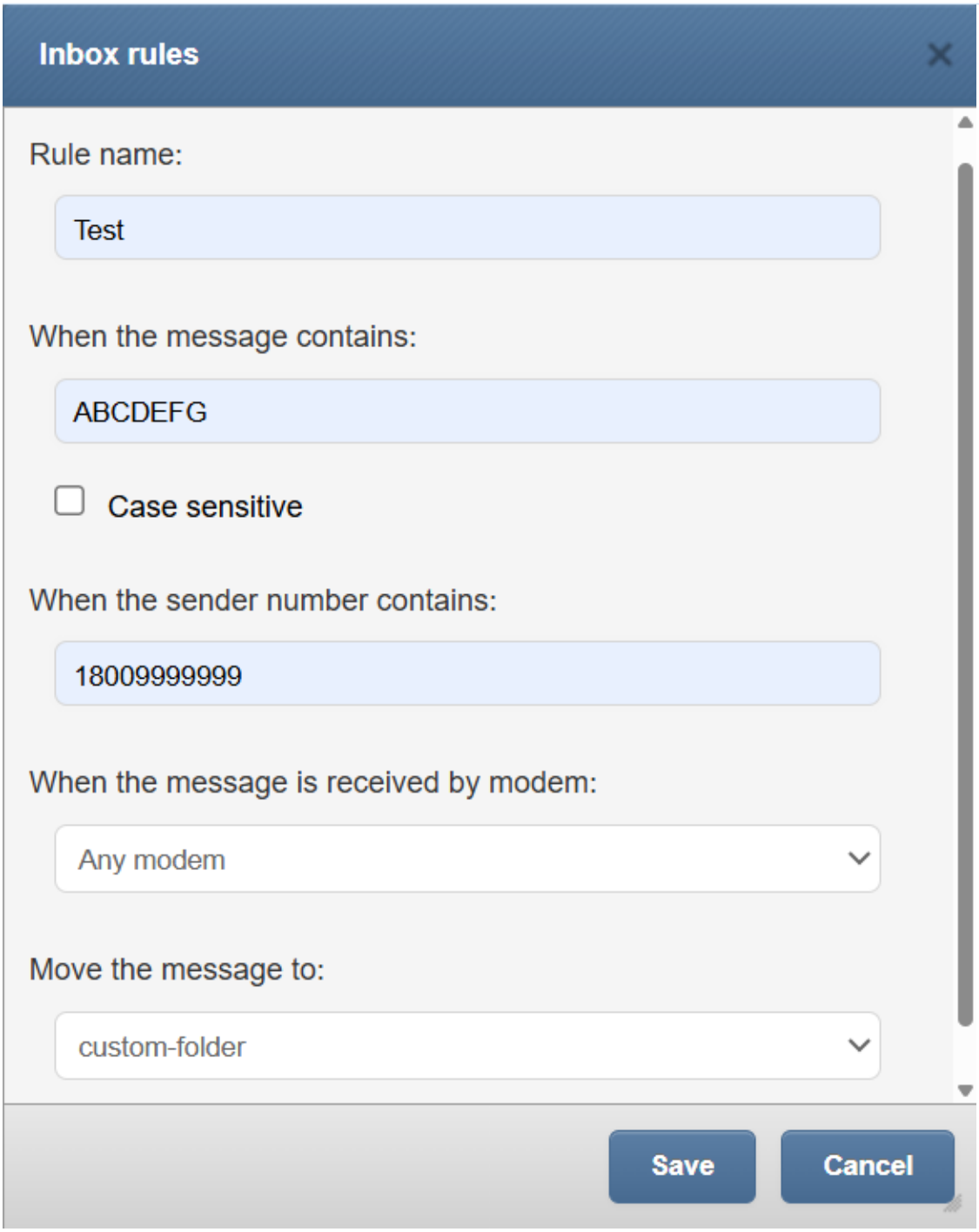


Inbox rules

You can create rules to automatically move incoming messages to your custom folders (My Folders). You can adjust the activation order of the rules by dragging them up or down. To move a rule, use the black dots next to its ID. Rules placed higher in the list have greater priority and will be checked first.



*Screenshot of “Inbox rules” *



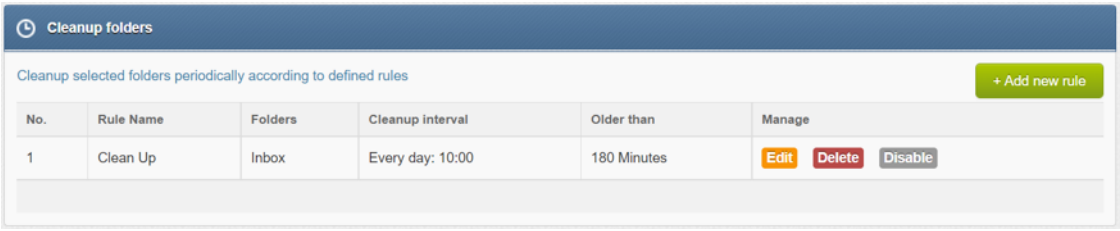
*Screenshot of “Add new inbox rule” *

In adding a new rule you can set:

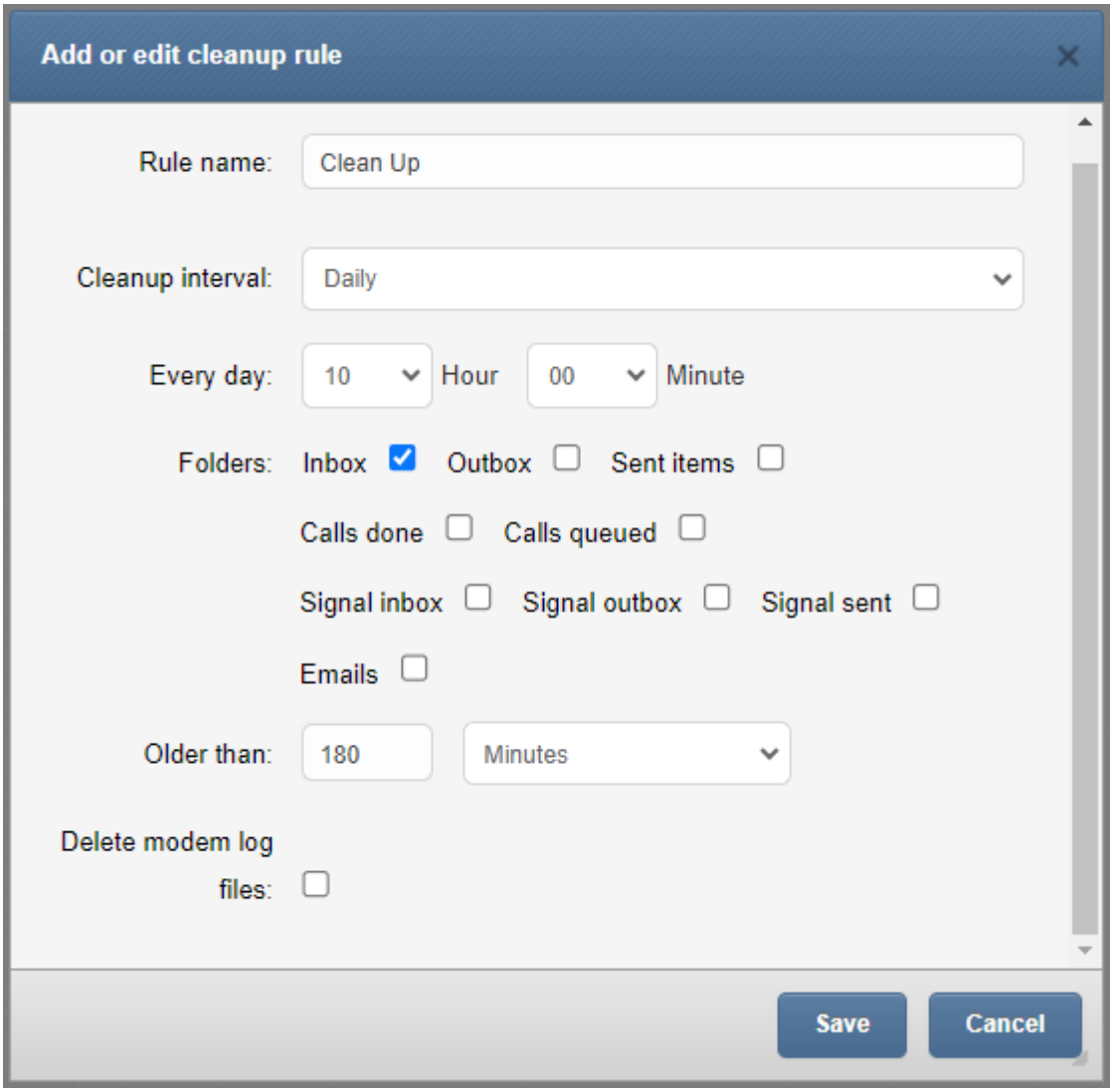
- Rule name
- What the message contains
- What the sender number contains
- Which modem the message is received from
- Which custom folder the message should be moved to

Cleanup Folders

This function allows you to add rules on when to automatically clean up messages & logs in selected folders.



Screenshot with example from Cleanup folders screen



Screenshot from Add or edit purging rule

In adding or editing a cleanup rule you can set:

- Rule name
- Purging interval (daily, weekly, monthly or annually)
- Set the time

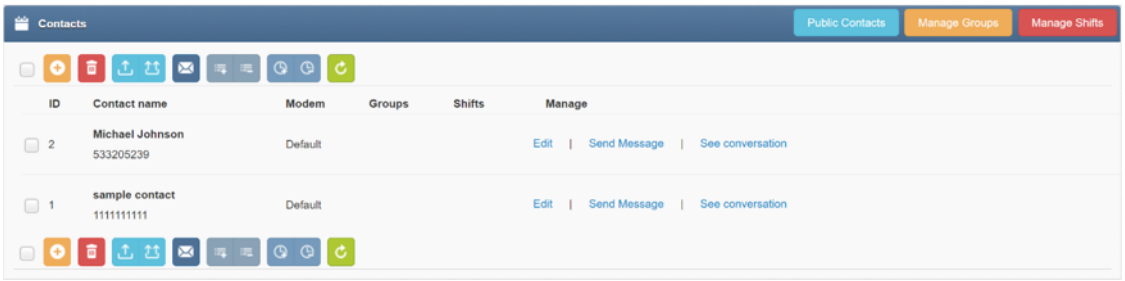
- Select the folder (Inbox, Outbox, Sent Items, Calls done, Calls queued, Signal inbox, Signal outbox, Signal sent, WhatsApp inbox, WhatsApp outbox, WhatsApp sent and Emails)
- Set time span of messages
- Select to delete modem log files

Phonebook

Web-GUI of SMSEagle device is equipped with Phonebook for managing contacts, groups and shifts. Each user can create private and public contacts, gather contacts in private and public groups. Contacts can also be optionally assigned to working shifts. Contacts and groups from Phonebook allows users efficient sending of messages.

Phonebook Contacts

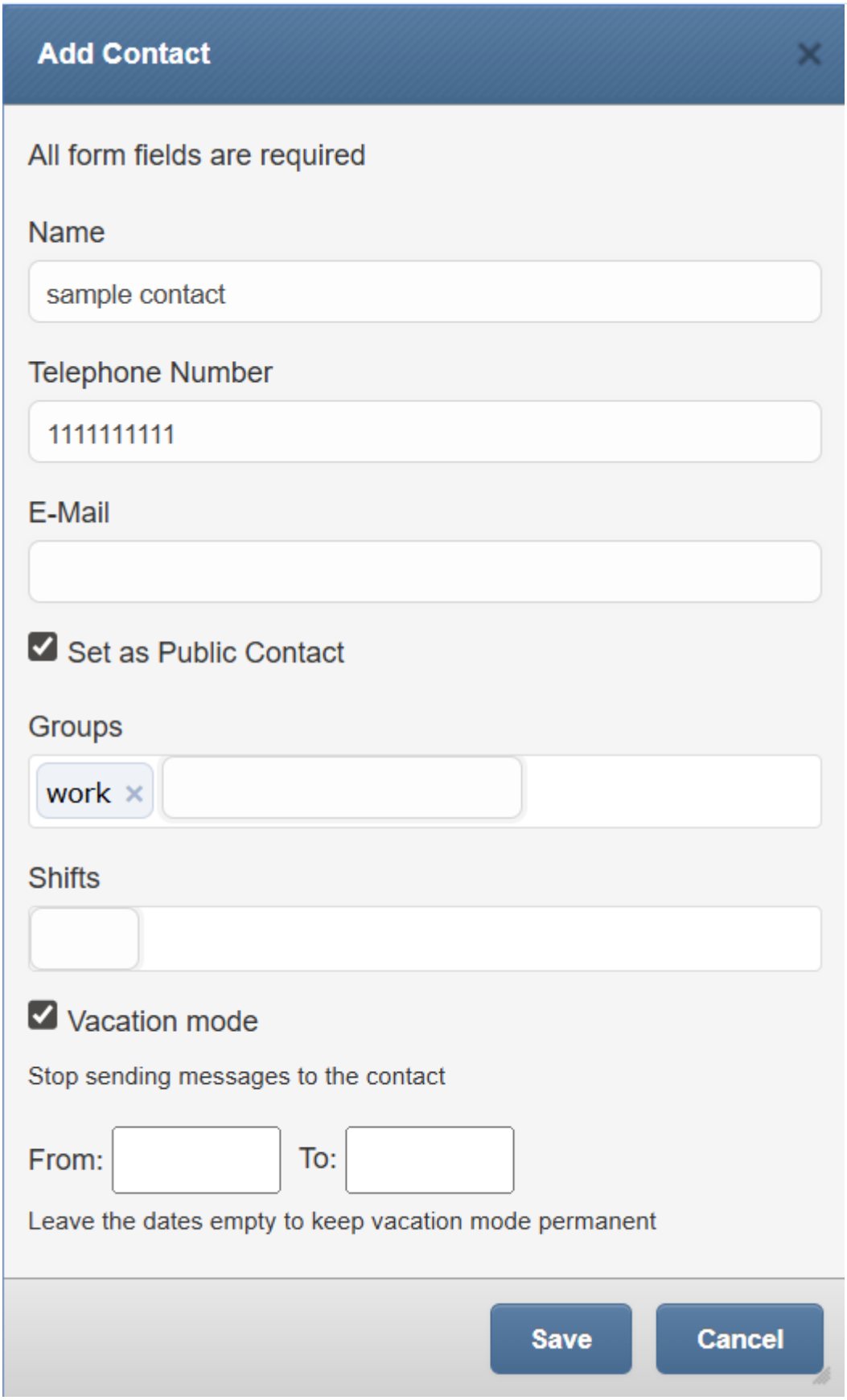
Below we present a main Phonebook view, where user manages his Contacts.



Screenshot of default phonebook view

In Phonebook Contact Management users can:

- Add/edit/delete contacts via Web-GUI
- Import contacts from CSV file
- Set contact to public or private visibility
- Add contacts to groups
- Add contacts to working shifts
- Set vacation mode (time range or permanent)
- Send message to a contact
- Export selected contact or all contacts
- View message conversation of a contact

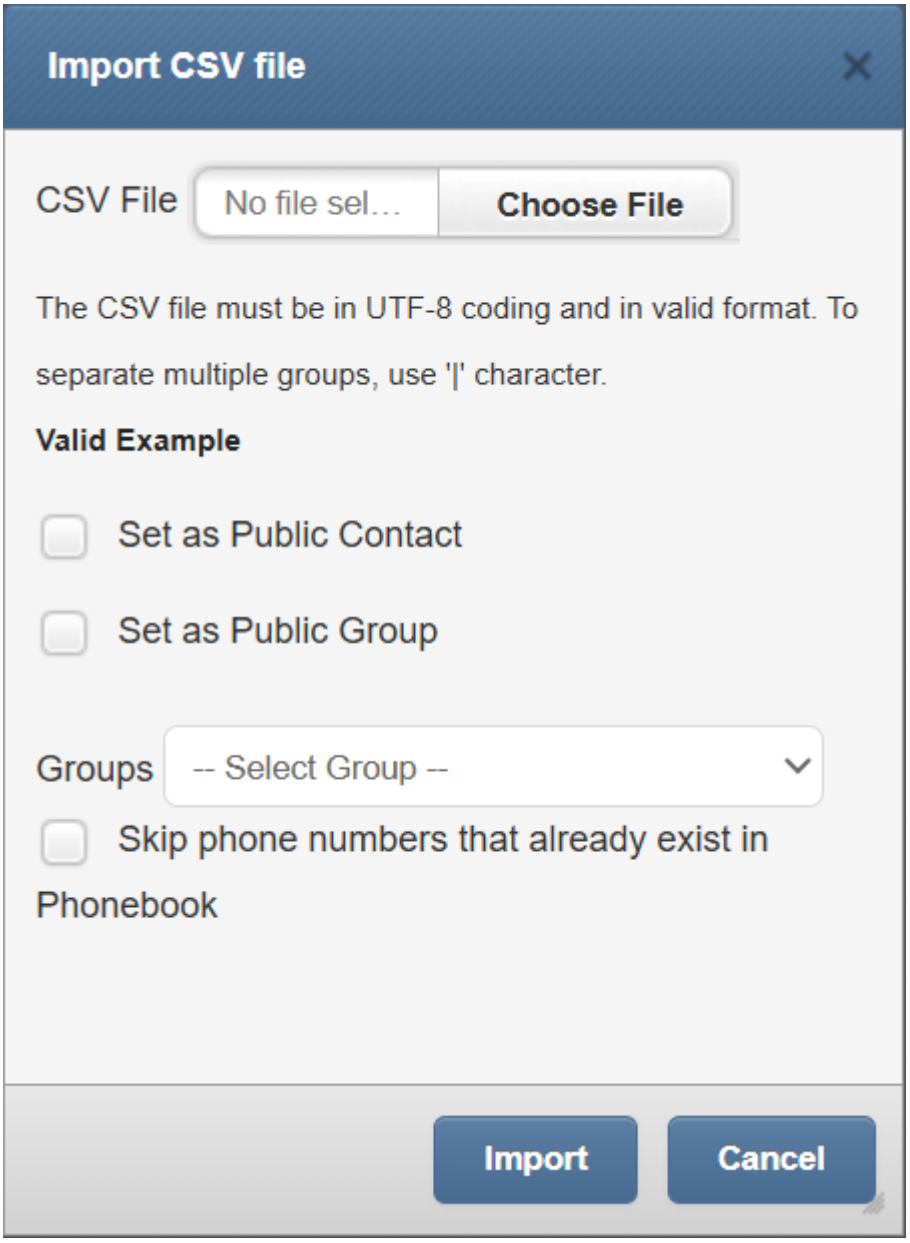


Screenshot of Edit/Add Contact window

In Phonebook Contact Edit/Add window users can:

- Define Contact name and Telephone number

- Choose if contact is Private/Public
- Assign a selected modem to the contact or leave default modem choice (according to global settings)
- Add contact to a Group
- Add contact to a Working Shift
- Enable/disable Vacation mode (messages are not sent when Vacation mode is enabled)



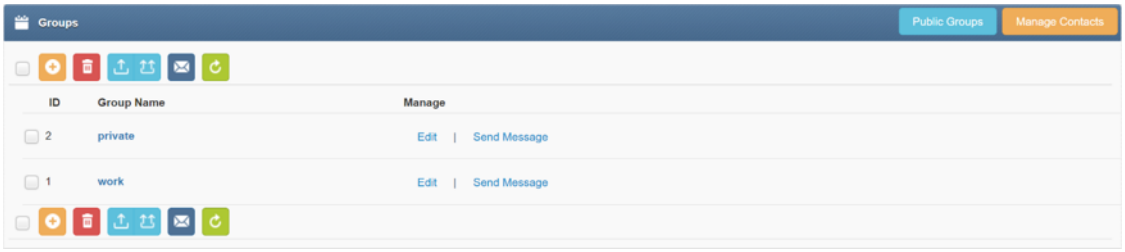
Screenshot of Import CSV file

In the Import CSV file window users can:

- Choose a CSV file to upload
- Set the uploaded contacts as a Public Contact
- Set the uploaded contacts as a Public Group

- Select which group to add the uploaded contacts to
- Choose to skip phone numbers that already exist in the Phonebook

Phonebook Groups



Screenshot taken from phonebook groups

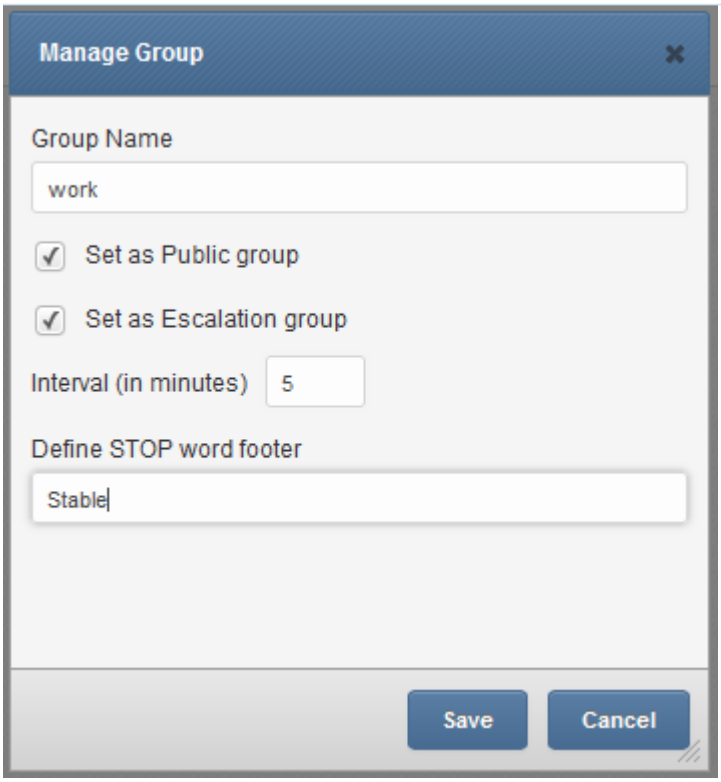
In Phonebook Group Management view users can:

- Add/edit/delete groups
- Set groups to public or private visbility
- View group content (contacts belonging to the group)
- Export selected group or all groups
- Send message to a group
- Add or remove contacts directly within the group view (without navigating to individual contact settings)
- Remove contacts from search results

Public and Private Contacts/Groups
Public contacts/groups are visible to all users on the device. A public contact/group may only be edited by the owner (the user who created the contact/group) . Private contacts/groups are visible to a single user (the owner).

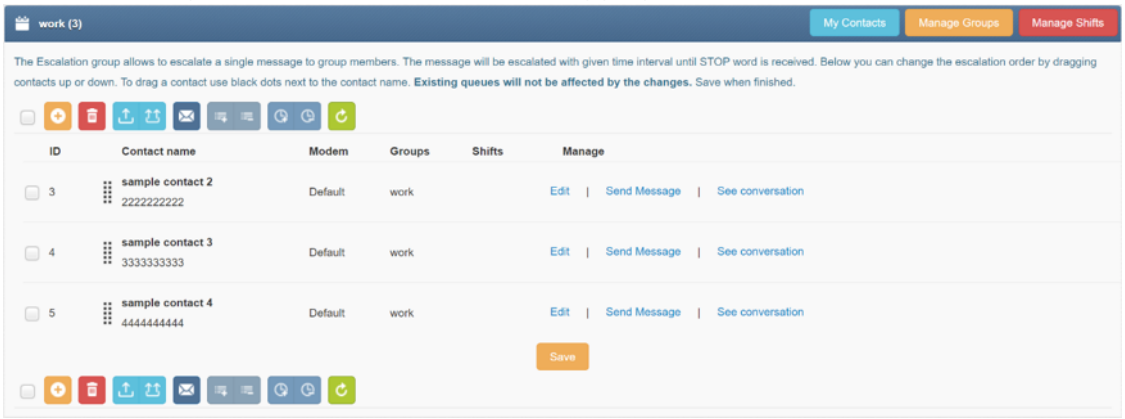
Phonebook Escalation Groups

Escalation group is a special version of a Phonebook group. When a group is set as an “Escallation group” a single message sent to the group will be escalated to the group members. The message will be escalated with given time interval until a set STOP word is received.



Screenshot from Manage Group view

You can change the escalation order by dragging contacts up or down.



Screenshot from Manage Groups with set escalation

Current escalation queue can be viewed and managed via menu Folders>Outbox>Escalation queues

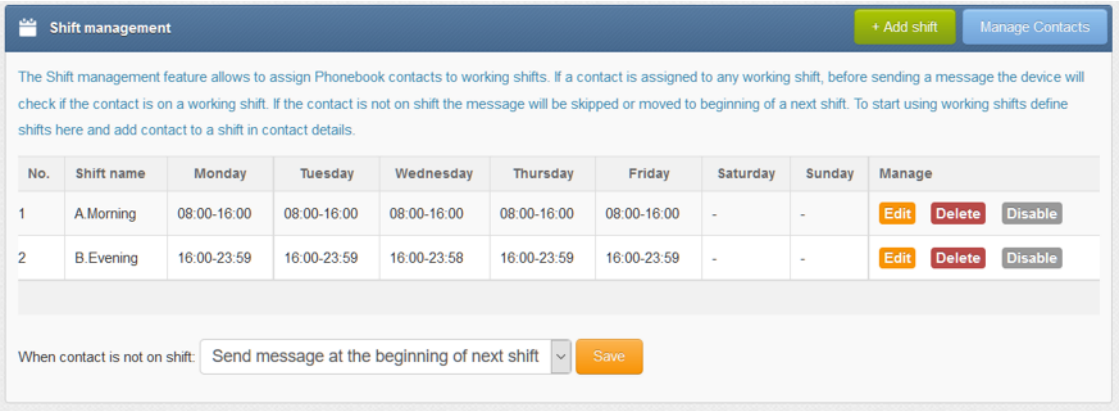


Screenshot with example from Folders>Outbox>Escalation queues window

Phonebook Working Shifts

The Shift management feature allows to assign Phonebook contacts to work in shifts. If a contact is assigned to any working shift, before sending a message the device will check if the contact is on a

working shift. If the contact is not on shift the message will be skipped or moved to beginning of a next shift. To start using working shifts define shifts here and add contact to a shift in contact details.



Screenshot of shift management in phonebook

Users

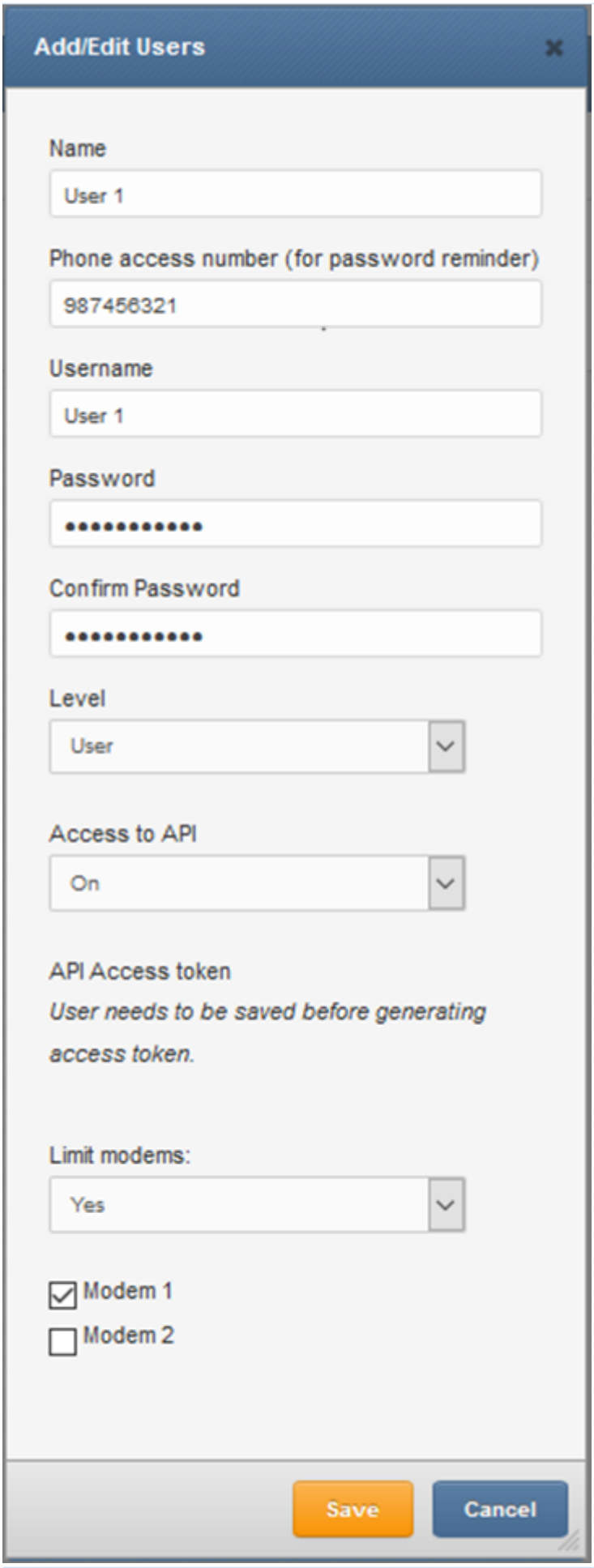
The Users function allows you to manage access to your device. It allows you to add, edit and remove users and set their permissions. There are two access levels for a user:

- User role “Administrator”:

  Allows full access & control of the device including settings and User management.

- User role “User”:

Limits access only allowing to Compose, Folders, Phonebook and Reporting module.


Add/Edit Users
Name
User 1
Phone access number (for password reminder)
987456321
Username
User 1
Password
Confirm Password
Level
User
Access to API
On
API Access token
User needs to be saved before generating access token.
Limit modems:
Yes
Modem 1
Modem 2
Save
Cancel

Screenshot of Edit/Add User window

Multi-User Capabilities

As described in the “Users” chapter, SMSEagle software allows to create multiple users with different access levels (Administrator or User). Those users may access the device simultaneously via web GUI or API. The following set of features is available in multi-user work scenario:

- Multiple users may acess the device simultaneously via webGUI or API
- Each user can create private or public (shared) Phonebook contacts and groups (see details in “Phonebook” chapter)
- Administrator may restrict a user with “User” role to use only selected modems to send messages (see details in “Users” chapter)
- Users with “User” role has its own private sent items folder (they cannot see messages sent by other users). Users with “Administrator” role can see messages sent by all users.
- the content of inbox folder (incoming messages) may be visible: for everybody/only for “Administrator” role/only for modems assigned to a user (see details in “Application settings” chapter)

User Settings

The User Settings menu allows each user to manage their personal preferences, authentication options, and interface behavior within the SMSEagle web UI. These settings apply only to the currently logged-in user and do not affect other accounts.

The menu is divided into three tabs:

- Personal data
- Password
- MFA

Personal Data

The Personal data tab is used to configure user identity details, message preferences, and interface behavior. Available settings:

- Language: Selects the display language of the SMSEagle web interface for the current user.
- Name: Defines the user’s display name. This name may be used in internal views and message-related contexts.
- Login: Shows the user’s login name. This field is informational and cannot be modified.
- Telephone Number: Specifies the user’s phone number. The number is used for password reminder.

- Signature: Allows the user to define a personal message signature:
    - Signature Off: no signature is added
    - Signature On: the entered text is appended to messages sent from Compose menu.
- Default e-mail subject in Compose menu: Defines a default subject line that is automatically prefilled when sending messages via the Compose menu.
- Default SMS encoding in Compose menu: Specifies the preferred SMS encoding method that will be set in Compose menu. Available options: Standard, Unicode or Automatic.
- Play notification sound on incoming SMS: Enables or disables an audible notification when a new SMS message is received in the web interface.
- Conversation sort: Determines the order in which conversations are displayed
- Conversation view type: Defines how message threads are visually presented (e.g. balloon/ chat-style view).
- Data per Page: Sets the number of items displayed per page in message lists and the phonebook. This affects pagination throughout the interface.

Password

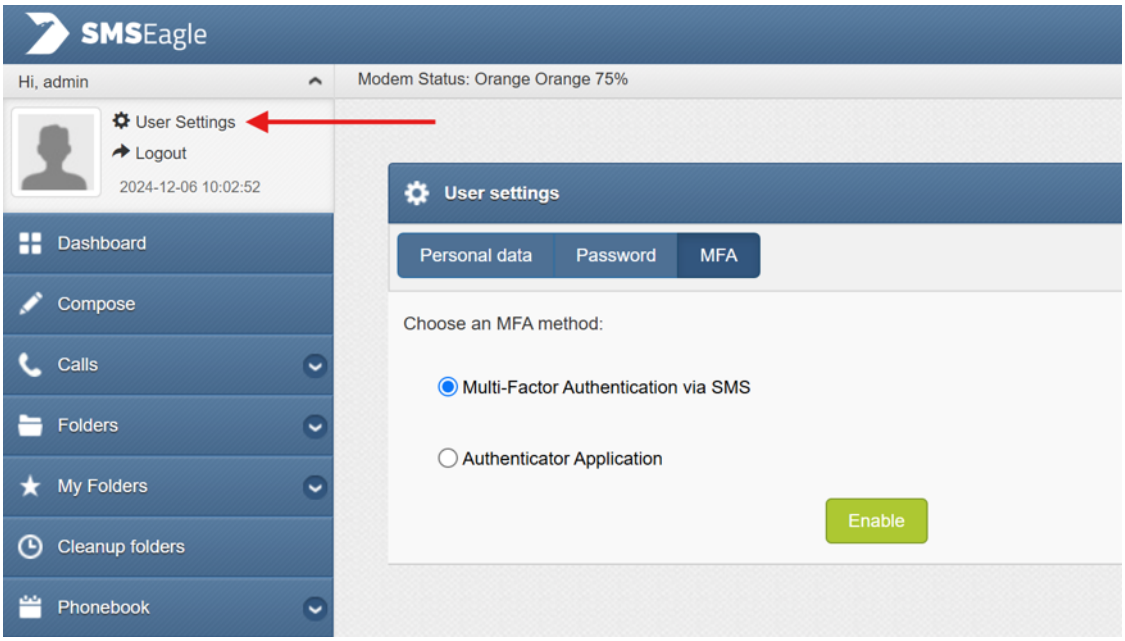
The Password tab allows the user to change their account password.

Multi-Factor Authentication (MFA)

Multifactor Authentication adds a layer of protection to the sign-in process. When accessing web-GUI accounts, users provide a username and a password plus additional identity verification, such as a code received via SMS text or a token from authenticator application.

Enable MFA from User Settings

MFA can be enabled by each user in User Settings menu > MFA tab.

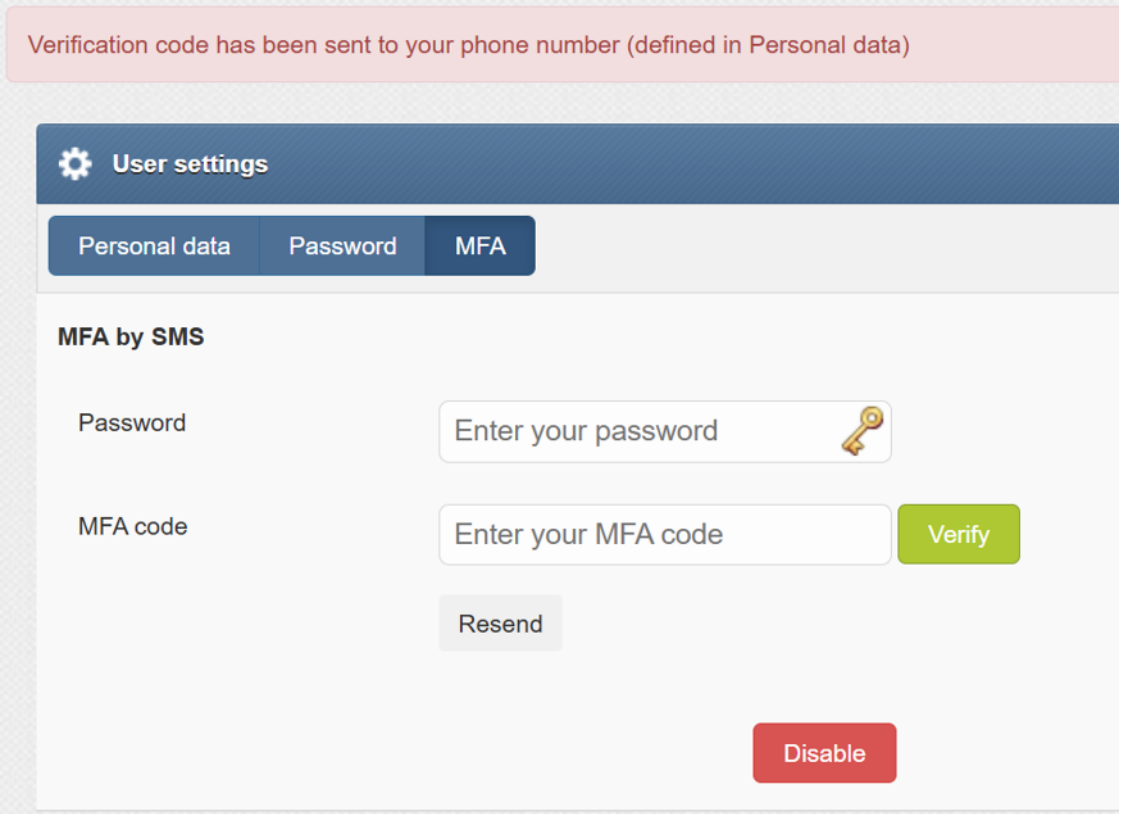


Screenshot from User Settings > MFA.

You may choose authentication method from: SMS or Authenticator App (like Google Authenticator, MS Authenticator, Authy, FreeOTP, Aegis, etc.).

When SMS is selected as the authentication method, a verification code is sent via SMS (text) to the number specified in Personal data tab. The SMS OTP code must be entered in to complete the process.

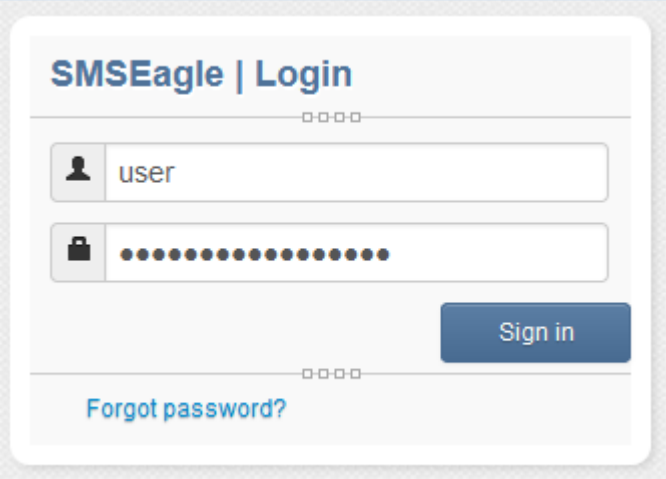
When Authenticator app is selected, a user password must be entered to display a QR code for the authenticator app. QR code must be scanned in the app, and then OTP from the app must be entered in web-GUI to complete the process.



Screenshot from User Settings > MFA. Verification code request.

User login with MFA

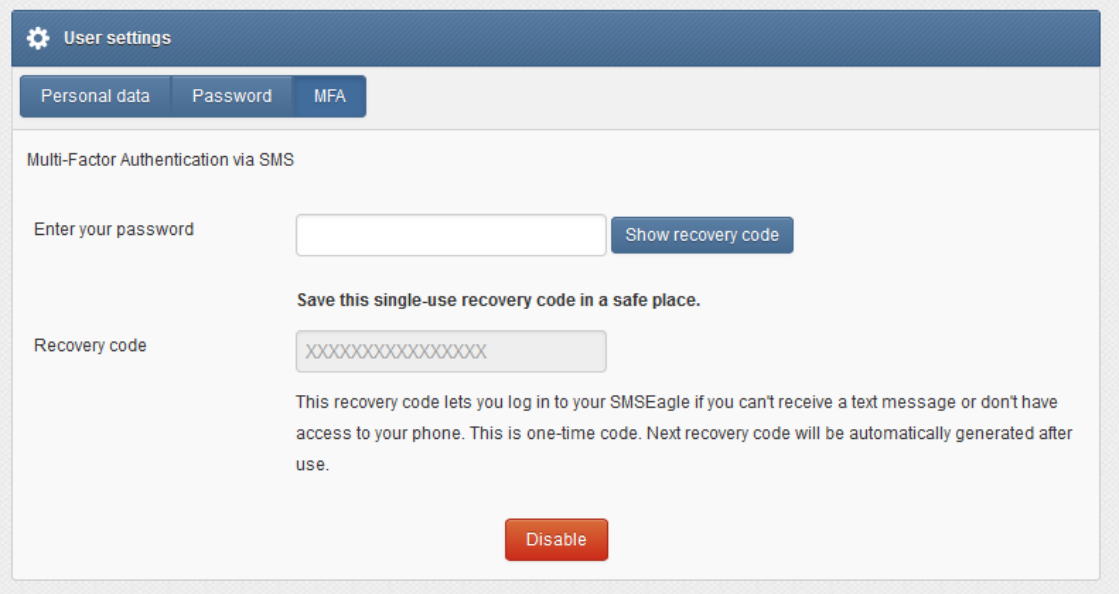
Once MFA is activated, the user must provide two factor authentication (user and password + one-time SMS token) every time he logs in to web-GUI. One-time SMS token is valid for 10 minutes.



Screenshot from login process with enabled MFA.

Recovery code

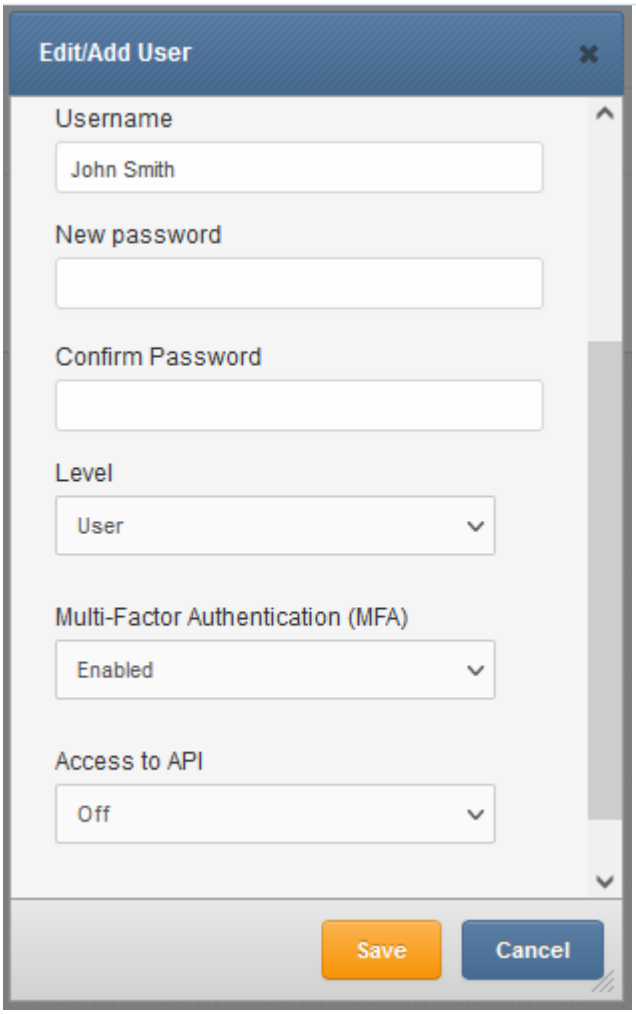
If for some reason a user can't receive a text message or don't have access to his phone, a recovery code can be used. The recovery code can be found in User Settings > MFA tab. **Remember to save the single-use recovery code in a safe place.** Recovery code is recreated after use.



Screenshot from User Settings > MFA. Recovery code is revealed after entering password

Enable MFA by administrator

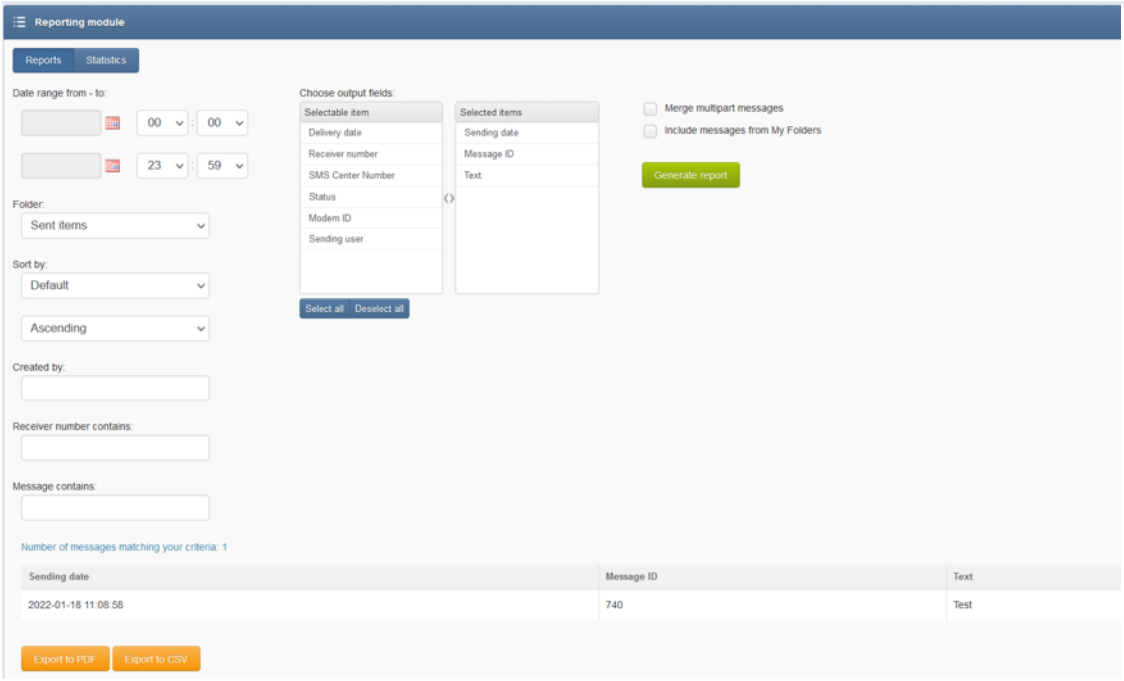
MFA can also be enabled by an administrator role for selected users. This is done in the menu Users > Edit User.



Screenshot from Edit/Add User

Reporting module

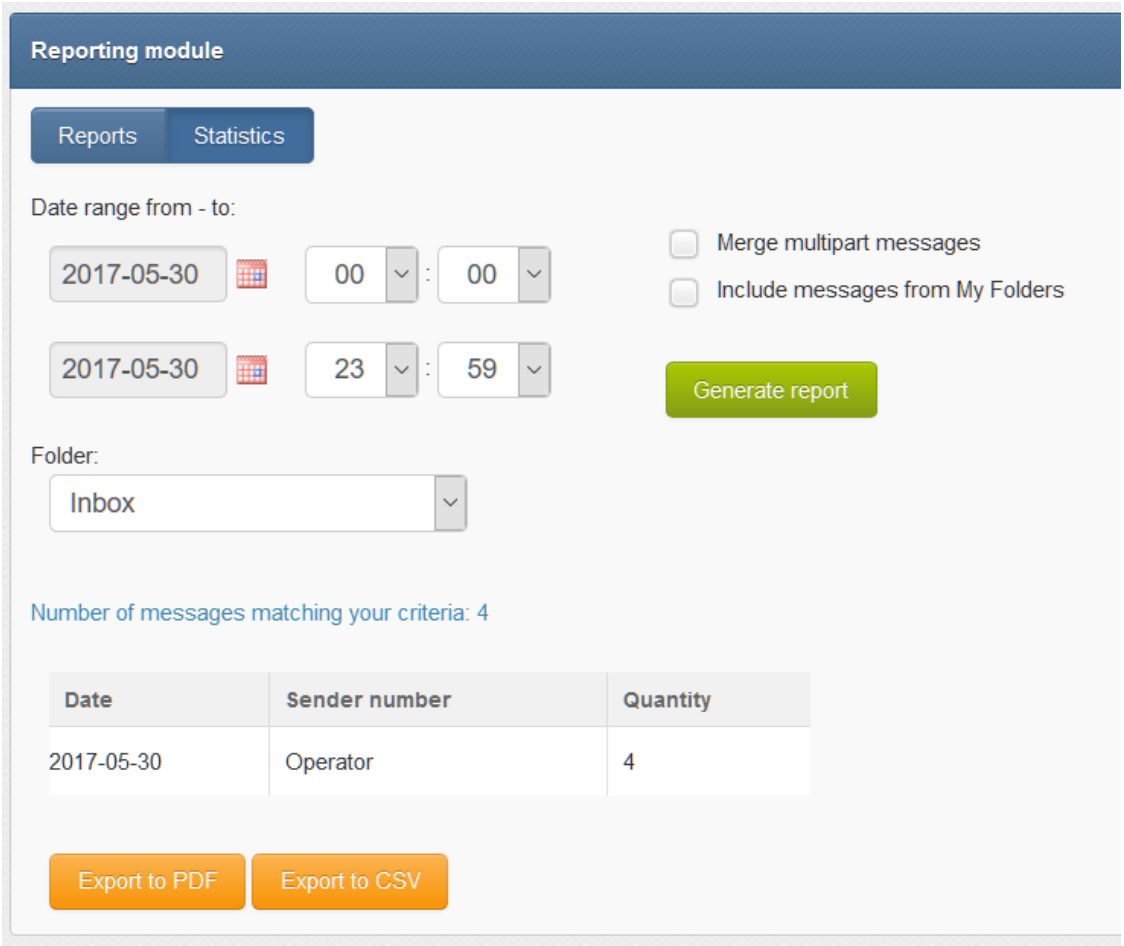
Reporting module is an extension of basic search feature. The module allows users to filter messages from Inbox/Sent items folders based on custom criteria and display filtered messages. Filtered list of messages can be exported to PDF or CSV file.



Screenshot of Reporting module

Statistics view

The reporting module allows also to view daily statistics of sent/received messages. The statistics view displays number of messages per day and sender/receiver number.

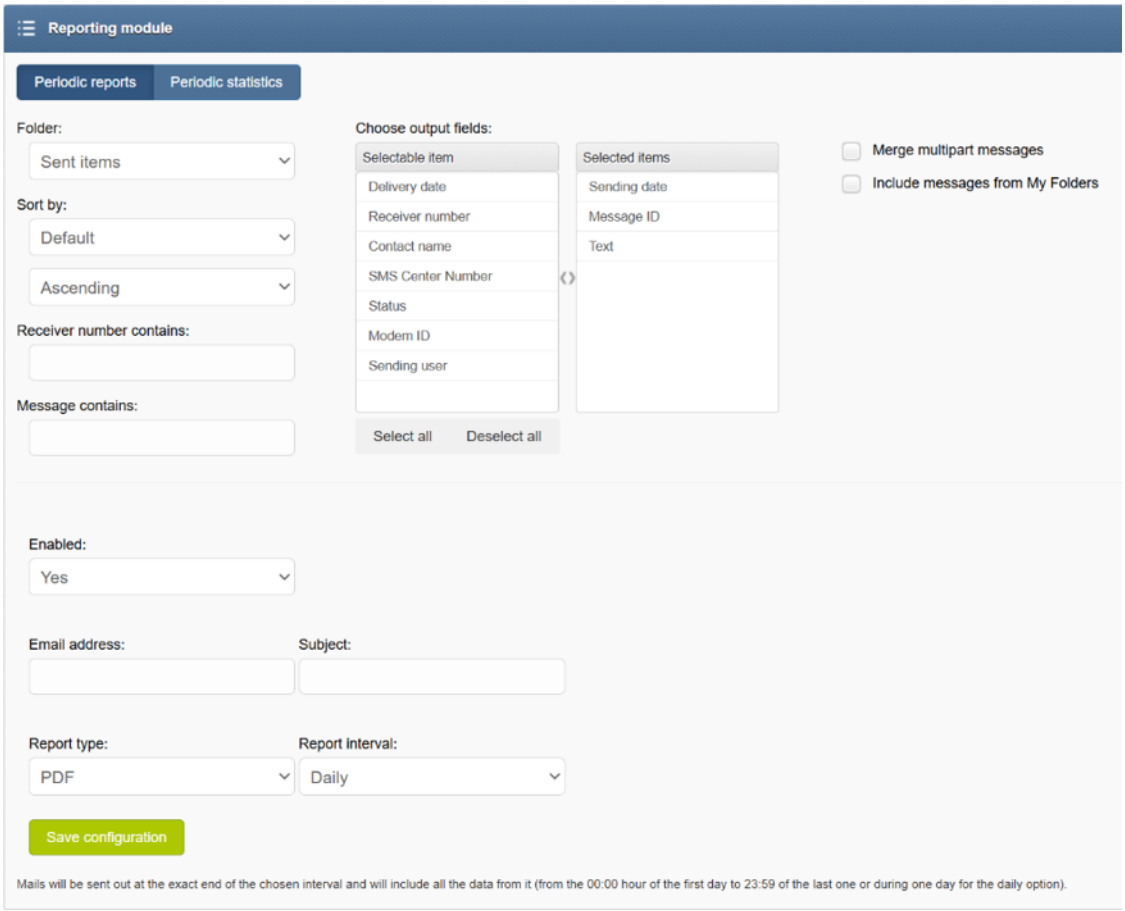


Screenshot of Statistics view in Reporting module

Periodic reports/statistics

You can choose to send automatic reports daily, weekly, or monthly. Mails will be sent out at the exact end of the chosen interval and will include all the data from it (from the 00:00 hour of the first day to 23:59 of the last one or during one day for the daily option).

Important
For Periodic reports/statistics, remember that you must configure the SMTP settings for sending emails in the 'Emails' > 'SMTP Configuration' menu and assign them to the 'Reporting module'.

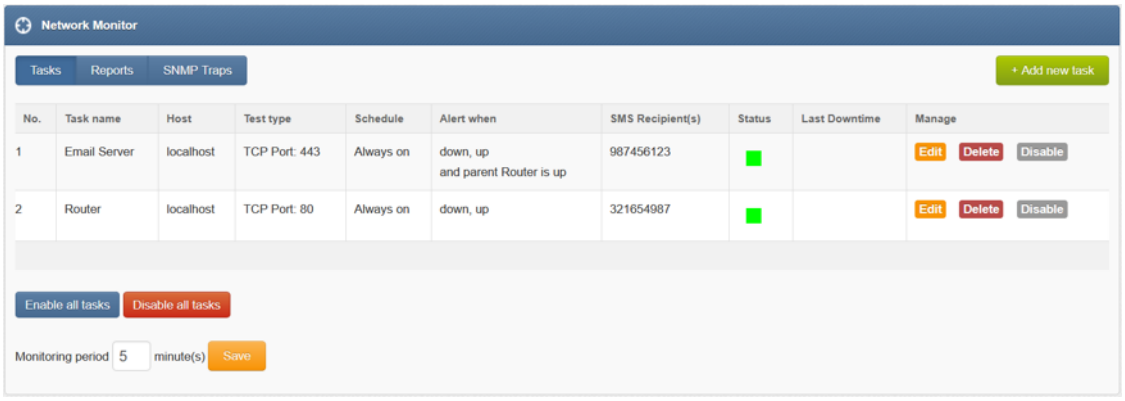


Screenshot of Periodic reports in Reporting module

Network Monitoring

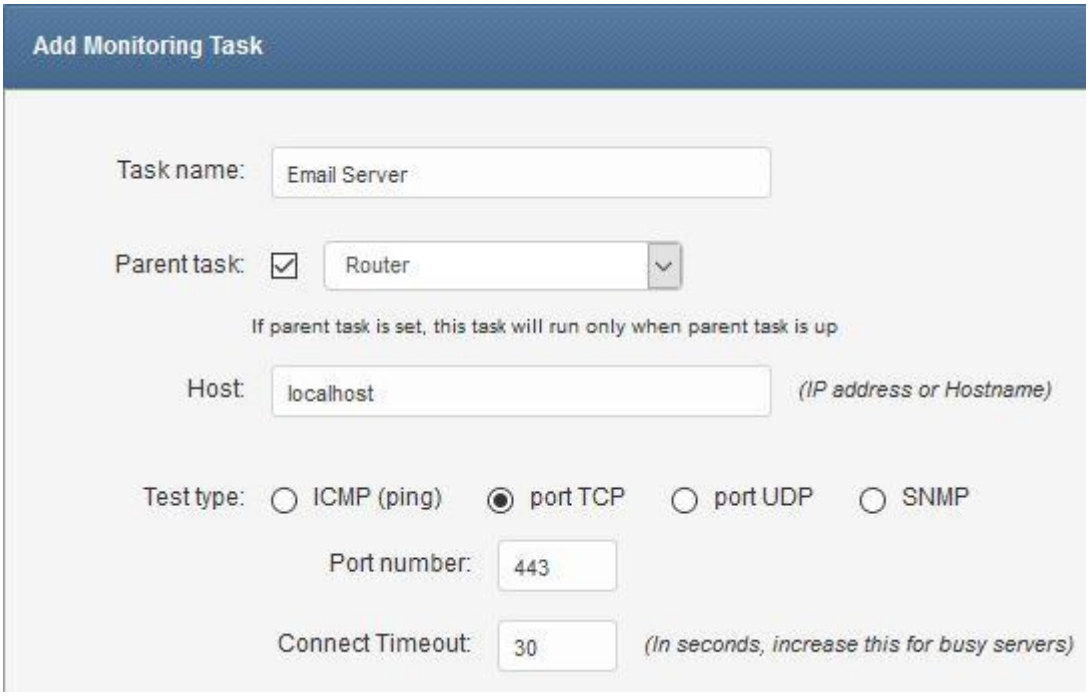
SMSEagle is equipped with network monitoring features. With that features you can monitor any device or service that operates ICMP, TCP, UDP or SNMP protocol. SMSEagle Network Monitoring plugin sequentially controls availability of defined hosts/services in Network Monitoring feature and sends defined SMS alert when host/service is unavailable/goes back to life or when SNMP return value reaches required criteria. Below you will find a brief overview of plugin capabilities.

Control status of all your defined tasks



- see a settings' overview for all of your tasks
- check which server/service is currently unavailable
- see when a specific server/service was last down (last downtime)
- check what happened at last downtime (see server/service response)
- edit/delete your tasks
- disable tasks when needed (e.g. when doing a machine upgrades)

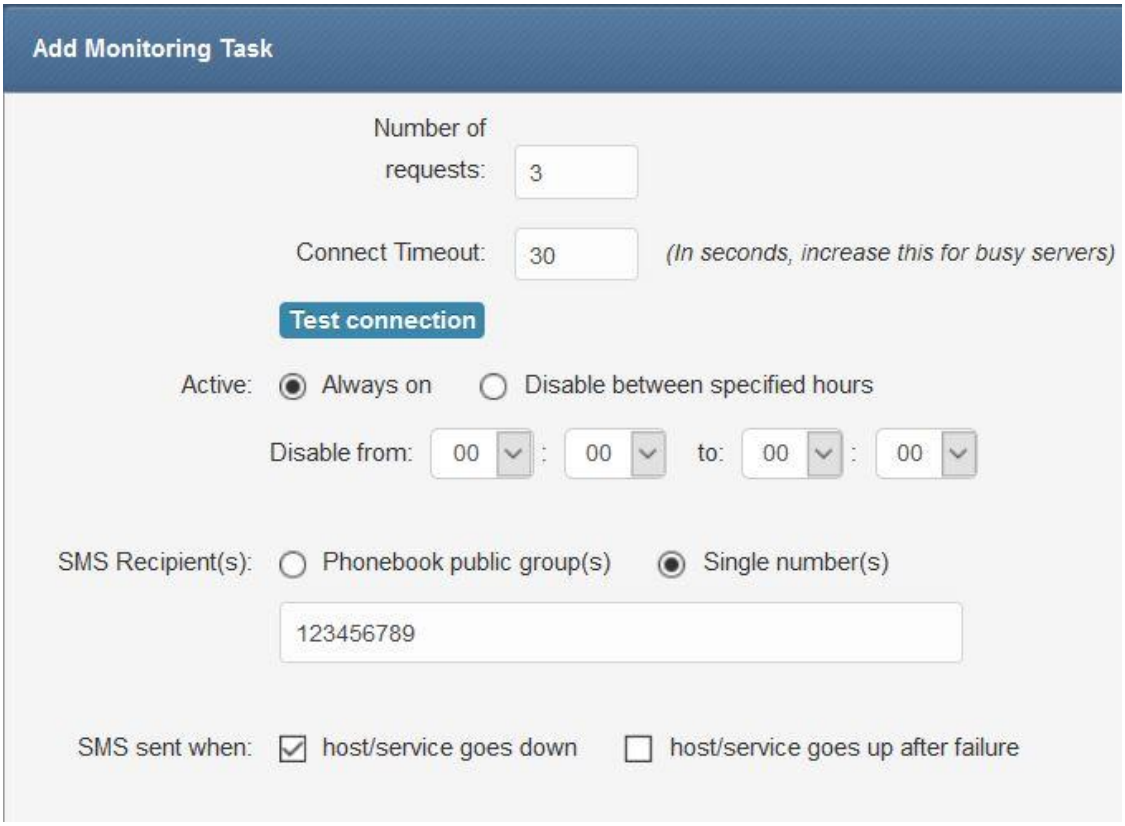
Define what you want to monitor in each task



- choose a name for the task
- set parent task. If parent task is defined, network monitor will monitor child task health only if parent task is healthy
- enter a host (IP address or Hostname)
- choose ICMP (ping) to monitor a server with ICMP protocol

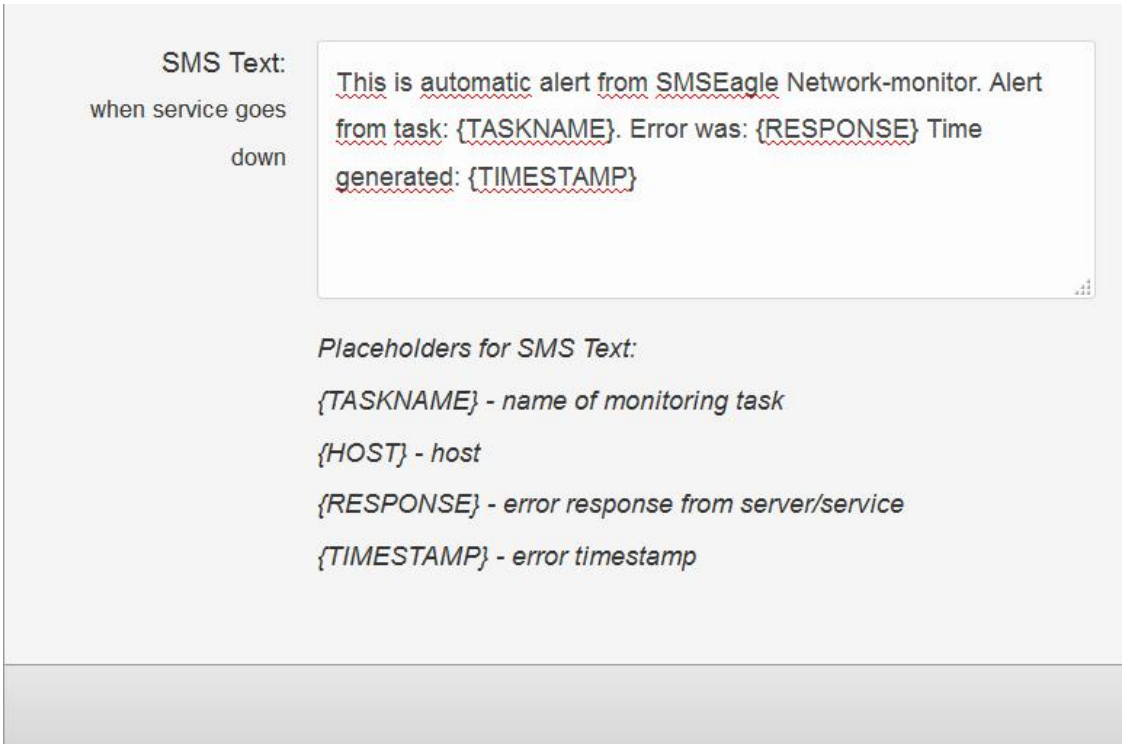
- or PORT (TCP/UDP) to monitor your service on a selected port (SMSEagle will check if port is open)
- or SNMP to monitor objects via SNMP protocol (supported return types: numeric, string)
- or Modbus TCP to monitor objects & register values via Modbus protocol (with function code 1-4)
- increase a default timeout value for busy servers (by default we set it to 30 seconds)
- test the connection of server

Define a schedule



- choose if task should be always enabled...
- ...or disable it at chosen times
  (during a night, when a machine goes through planned restarts, during resource intensive backups, etc.)
- enter a phone number or choose a group of users to send your SMS alert to
- select when to send SMS alert (when host/service goes down, when host/service goes up after failure)
- choose if the SMS alert should be sent once or repeated every X-minutes

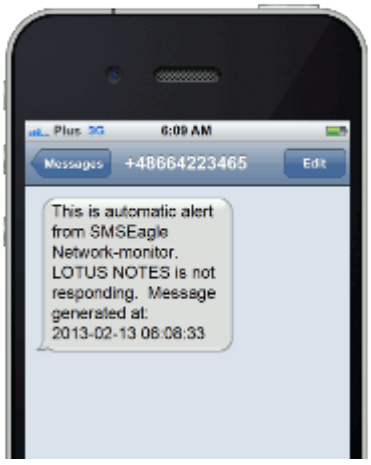
Define a SMS alert message



Define your SMS messages when host or service becomes unavailable/comes back to life. Choose field placeholders for your SMS text:

- {TASKNAME} – puts a taskname inside SMS text
- {HOST} – hostname or IP address
- {RESPONSE} – message received (in case of no response from server/service)
- {TIMESTAMP} – timestamp of an error

Receive SMS alerts



- be alerted when your services/servers go down (or go up after failure)
- give yourself a chance to react quickly

Voice Call

An SMS message can be optionally followed by a wake-up call or text-to-speech call. This can be enabled in the rule definition. The feature requires a device with an active Voice-Call add-on.

Network Monitoring Probes

The Network Monitoring feature in SMSEagle devices allows you to continuously supervise the availability and health of network devices, services, and industrial systems. Each monitoring task is based on a **test type**, which defines how the target is checked. When a problem is detected, SMSEagle can immediately send SMS alerts (and optionally voice calls), ensuring fast reaction to incidents.

ICMP (Ping)

The ICMP (Ping) verifies basic network reachability of a host by sending ICMP echo requests.

Available parameters:

- Host (IP or hostname)
- Number of requests
- Connect Timeout

Typical use cases:

- Checking whether a server, router, firewall, or network device is online
- Detecting total connectivity loss or device outages

TCP Port

The TCP Port probe checks whether a specific TCP service is accessible by attempting to establish a TCP connection to a defined port.

Available parameters:

- Host: IP address or hostname
- Port number
- Connect Timeout

Typical use cases:

- Monitoring services such as HTTP/HTTPS, SMTP, SSH, FTP, databases, or application servers
- Verifying not only that a host is online, but that a service is actually running

UDP Port

The UDP Port probe monitors availability of services that rely on the UDP protocol.

Available parameters:

- Host: IP address or hostname

- Port number
- Connect Timeout

Typical use cases:

- DNS services
- Custom or proprietary UDP-based applications

SNMP Probe

The SNMP (Simple Network Management Protocol) probe allows SMSEagle to monitor specific parameters exposed by SNMP-enabled devices.

Available parameters:

- Host: IP address or hostname
- Protocol version: v1/v2
- Object ID
- Community
- Return value type (numeric/string)
- Connect Timeout
- SMS sent when: defines a condition when an SMS alert should be triggered (e.g. value is equal to / not equal to/ greater than / less than a defined threshold)

Typical use cases:

- Monitoring routers, switches, UPS systems, servers, and network appliances
- Tracking metrics such as temperature, CPU load, memory usage, link status, or power conditions

Modbus TCP

The Modbus TCP probe is designed for monitoring industrial and OT environments. This allows you to read values directly from PLCs, sensors, controllers, and other industrial equipment that support Modbus TCP/IP communication, and trigger SMS alerts when a register value meets defined criteria.

Available parameters:

- Host: IP address or hostname of the Modbus device
- Port: TCP port of the Modbus server (default: 502)
- Unit ID: Modbus unit identifier
- Function code: type of register to read: Read Coils (1), Read Discrete Inputs (2), Read Holding Registers (3) or Read Input Registers (4)
- Register: address of the register to be monitored

- SMS sent when: defines a condition when an SMS alert should be triggered (e.g. value is equal to / not equal to/ greater than / less than a defined threshold)

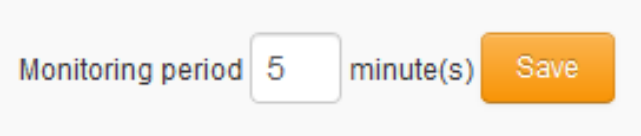
Typical use cases:

- PLCs,
- SCADA systems
- Industrial sensors and automation equipment

Monitoring frequency

Monitoring tasks are performed in a parallel mode. Software automatically optimizes number of parallel tasks and frequency of tasks taking into account the performance of the device and adjusts monitoring period when needed.

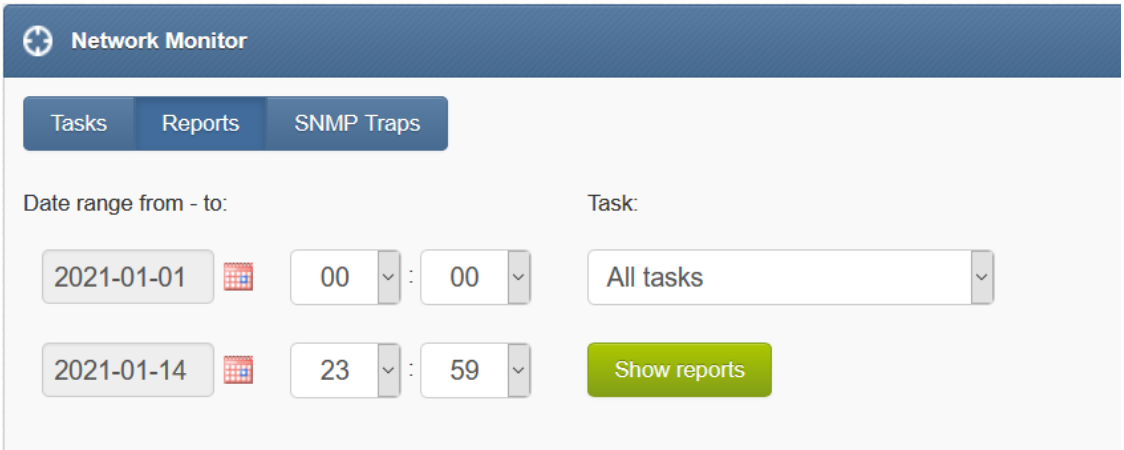
You can manually increase/decrease monitoring period in Network Monitor settings:



If monitoring period value is too small (there are too many monitoring tasks to perform in parallel), the software will adjust the value to ensure optimal workload and performance of your device.

Reports

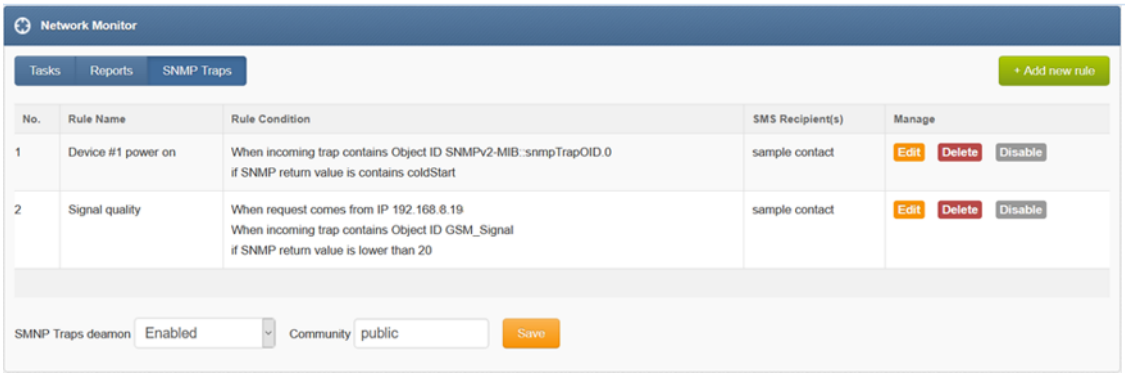
This tab allows you to view reports of task errors in the Network Monitor for a selected period of time.



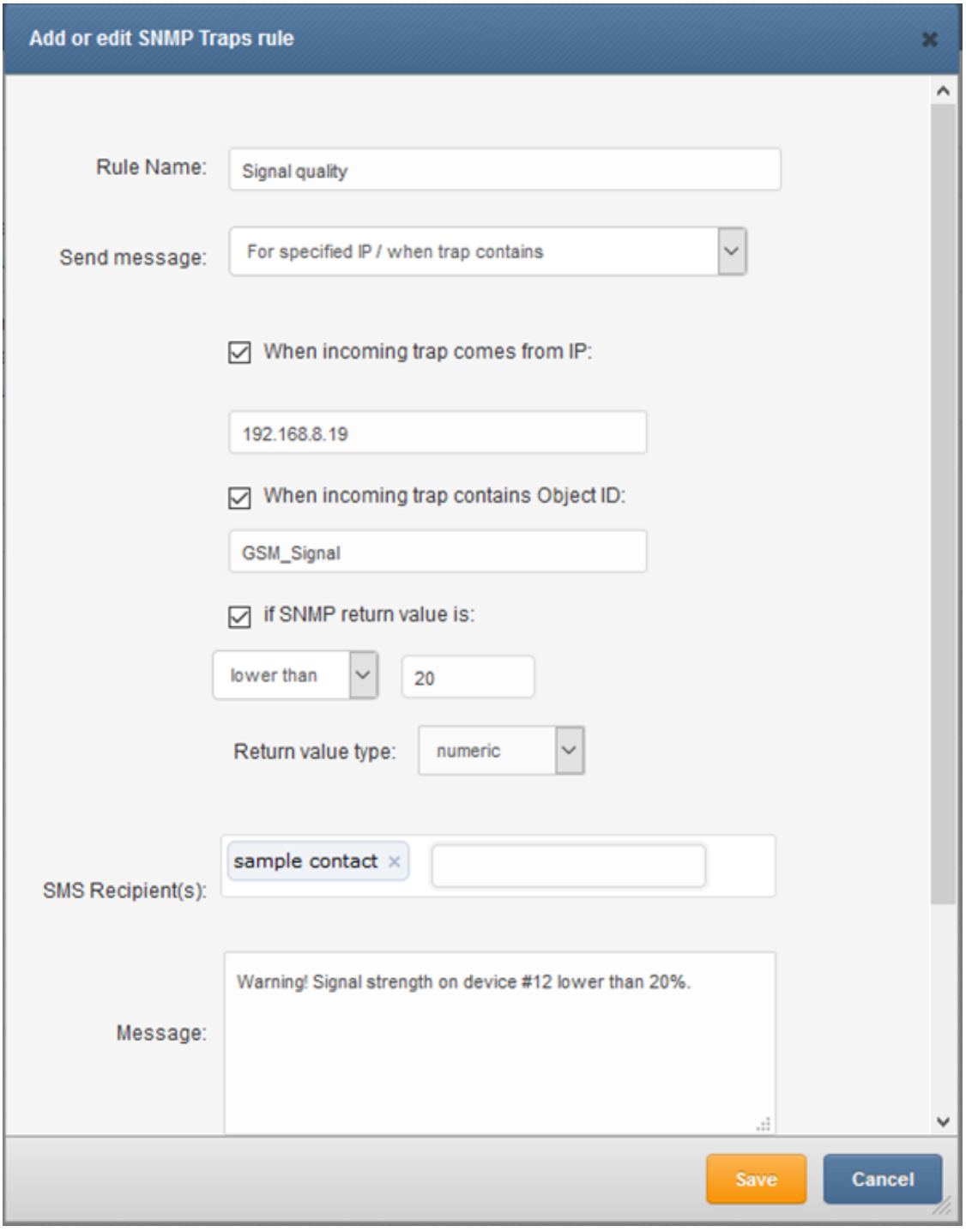
Screenshot from Network Monitor > Reports window.

SNMP Traps

SNMP trap is a popular mechanism used to manage and monitor devices' activities via SNMP protocol. What makes the Trap unique is that they are triggered instantaneously by an agent, rather than waiting for a status request from SNMP get query.



Screenshot from Network Monitor > SNMP TRAPS window.



Screenshot from Network Monitor > SNMP TRAPS Add or Edit window.

SMSEagle can act as an SNMP trap receiver. For each incoming trap, you can define a rule that triggers an SMS message.

- Trap content matching options:
  - Match all OIDs in the trap — alert is triggered whenever a trap from a defined source arrives
  - Match a specific OID value — alert is triggered only when a trap contains a specific OID matching a defined value (equal/not equal/greater/less than)

The single-OID-value match is useful when a device sends multiple OIDs in one trap and you only want to react to a specific one.

SMSEagle also supports displaying the value of a specific OID from an incoming SNMP trap directly in alert messages. You can use a dedicated placeholder to reference a single OID value in the message content, for example: {TRAP:OID_IDENTIFIER}. At runtime, the placeholder is replaced with the actual value received in the SNMP trap.

This is especially useful when a single trap contains multiple OIDs, but only one specific value is relevant for the alert recipient.

Emails

Email to SMS

Email to SMS feature allows you to convert an email to SMS message.

Basic usage

If the plugin is enabled, email sent to the email address:

PHONE_NUMBER@IP_ADDRESS_OF_SMSEAGLE will be converted to SMS message.

Where:

PHONE_NUMBER - is a destination phone number

IP_ADDRESS_OF_SMSEAGLE - is the IP address of your device.

The text of the email is the text of the SMS message (optionally you can append email subject at the beginning of SMS message).

Example: email message sent to the address: 123456789@192.168.0.101 will be converted to SMS message and delivered to phone number 123456789.

Send to username/group

Email sent to the email address:

NAME_IN_PHONEBOOK@IP_ADDRESS_OF_SMSEAGLE will be converted to SMS message and will be sent to a user or users' group from SMSEagle's phonebook.

Where:

NAME_IN_PHONEBOOK - is a username or group name (must be a public group) from SMSEagle's phonebook

IP_ADDRESS_OF_SMSEAGLE - is the IP address of your device.

The text of the email is the text of the SMS message (optionally you can append email subject at the beginning of SMS message).

Example: email message sent to the address: db-admins@192.168.0.101 will be converted to SMS message and delivered to all members of db-admin group. The db-admin group must be defined in your SMSEagle phonebook.

Send to Ldap contacts/groups

If your company uses LDAP (Active Directory or OpenLDAP) for contacts management, you may use LDAP Contacts or Groups to send email to SMS text message.

Example: email message sent to the address: myldap-admins1@192.168.0.101 will be converted to SMS message and delivered to all members of myldap-admins1 group. The myldap-admins1 group must be defined in your LDAP directory and LDAP plugin must be configured on your SMSEagle device.

Voice Call

An SMS message converted from email can be optionally followed by a wake-up call or text-to-speech call. This can be enabled in the rule definition. The feature requires a device with an active Voice-Call add-on.

Using FQDN in email address

It is also possible to use Fully Qualified Domain Name in an email address sent to SMSEagle box (eg.: 123456789@mydomain.com). Please refer to our FAQ article: How do I configure Email2SMS plugin to accept FQDN email addresses for more details.

Email subject - additional parameters (optional)

It is possible to set additional flags for single converted message using email subject. Currently the following flags are available:

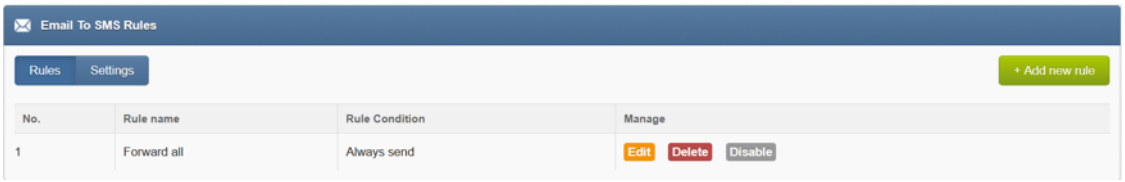
- date - date and time in format YYYYmmDDHHMM (YYYY – year, mm – month, DD – day, HH – hour, MM – minute). If this parameter is not null SMS will be scheduled for sending at the given date and time
- modemno - sets sending modem number (available only for multimodem devices)

If you send email with subject containing FLAG=VALUE the flag will be set for this particular email2SMS message.
Example 1: email message with subject containing **modemno=2** will be converted to SMS message

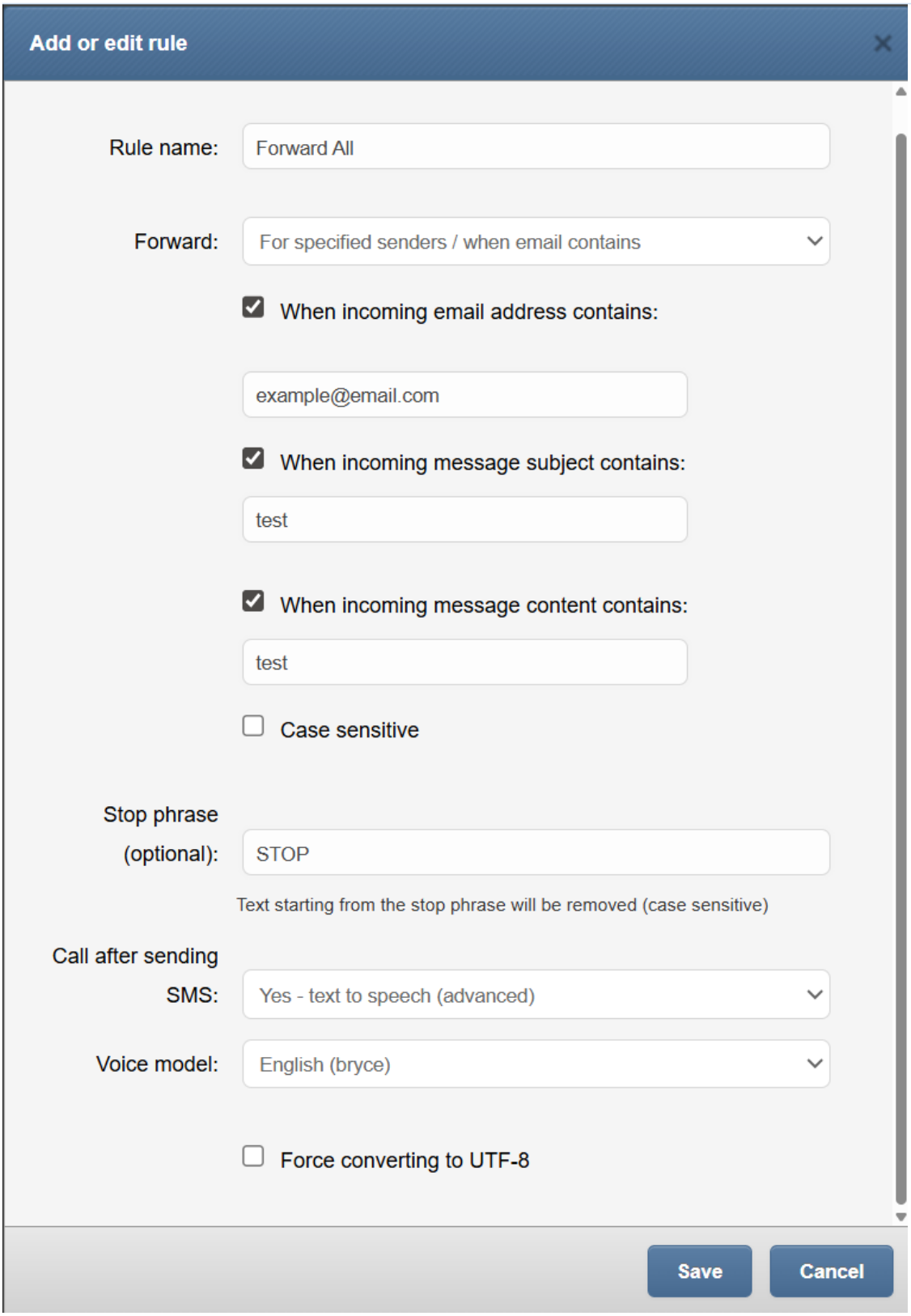
and sent via modem number 2.
Example 2: email message with subject containing **date=201801010005&modemno=2** will be converted to SMS message and sent on 2018-01-01 00:05 via modem number 2.

Feature configuration

The feature “Email To SMS” allows to add many forwarding rules. Each rule can be enabled or disabled by user.



Screenshot from Email To SMS > Rules window

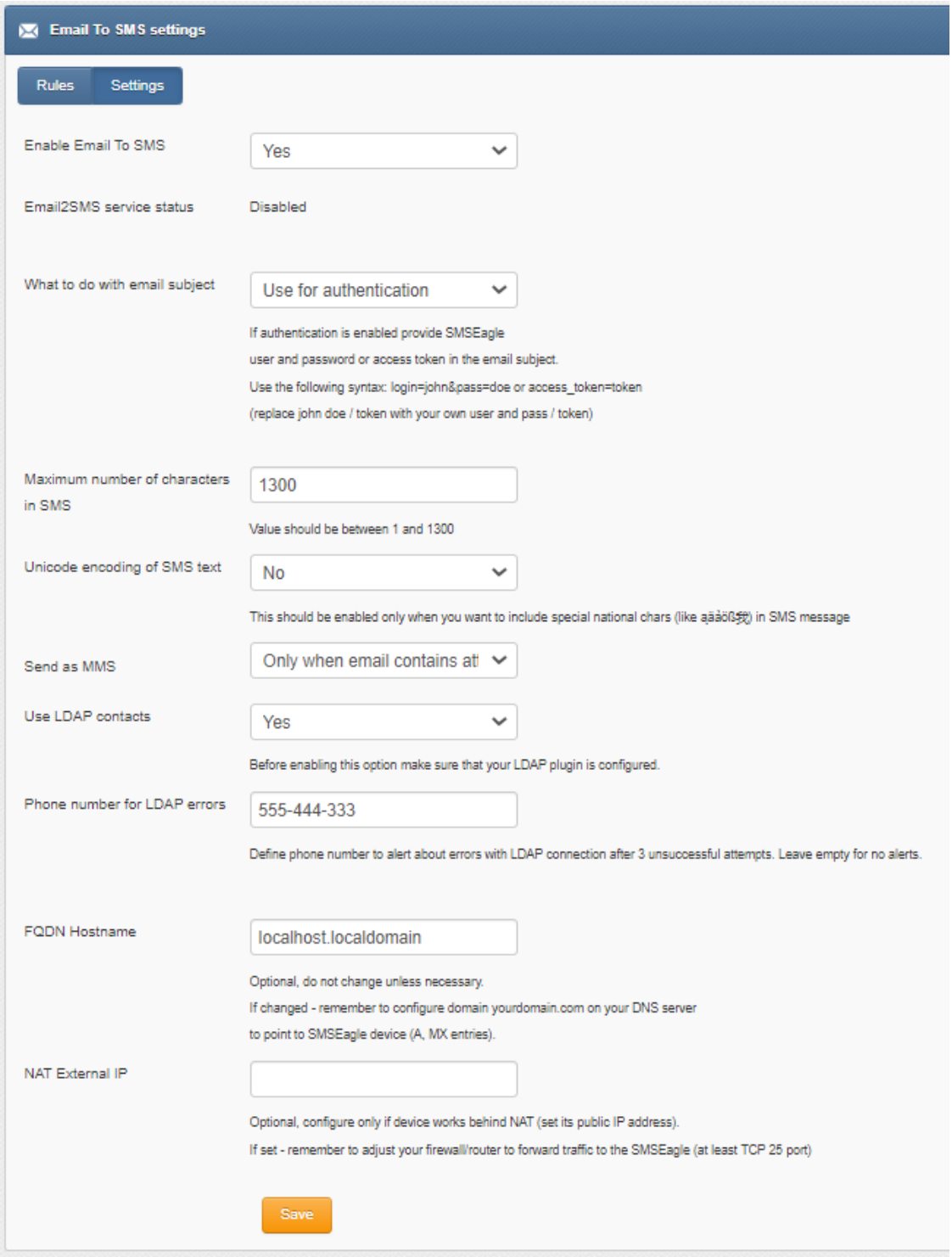


Screenshot from Email to SMS > Add new rule

- You can name your rule
- You can set forwarding to Always or For specified senders / when email contains
- You can set when subject contains and message content (choose to be case sensitive or not)

- You can define “Stop phrase”. Text starting from the stop phrase will be removed (case sensitive) from the message
- You can select if to call after sending SMS (No/Ring only/TTS or TTS advanced)*
- You can choose the voice model (English or German)*
- You can set message priority (0–9). Messages with higher priority will be processed earlier in the outbound queue

*Call options are only available when purchasing the Voice (Calls) feature for your device



Screenshot from Email to SMS settings

- if you want to use the plugin, set 'Email2SMS active' to 'Yes'
- if you want to include a subject of an email in SMS message, set 'What to do with email subject' setting to 'Include in SMS'. The email subject will be appended at the beginning of SMS message
- if you want to use user authentication, set 'What to do with email subject' setting to 'Use for authentication'. If user authentication is enabled, provide in a subject of an email your login and password in the following form: login=john&pass=doe OR provide API access token in the following form: access_token=token
- if you want to include only a subject of an email in SMS message, set 'What to do with email subject' setting to 'Send only subject without email body'. Only the email subject will be inserted in the SMS message
- the text of an email will be cropped to the value 'Maximum number of characters. Maximum allowed length of SMS message is 1300 characters
- if you want to include in SMS message special national characters (like ąääöß) set "Unicode encoding of SMS text" to 'Yes''
- if you want to send as MMS you can set as always or only when an email contains an attachment
- Choose if you want to use contacts from LDAP directory (Yes/No). LDAP plugin must be first configured to use this feature.
- If you enabled contacts from LDAP, define Phone number for LDAP errors. Alerts about errors with LDAP connection will be sent to this phone number after 3 unsuccessful LDAP connection attempts. Leave this field empty for no alerts.
- FQDN: Email2SMS Plugin can be configured to utilize alternative FQDN address instead of working with only device's IP in the email address. This requires configuring proper domain and DNS entries at your DNS server - both A and MX entries, pointing to the SMSEagle's IP. With this configured email sent to newly configured domain will reach the SMSEagle, and be properly processed by the plugin.
- NAT: If your device works in LAN behind NAT, and you want to be able to send emails to it from public internet, you need to configure here the public IP where it would be reachable. Have in mind that this would require additional configuration of your LAN/firewall, to forward traffic to the SMSEagle (at least forward TCP port 25).

Email to SMS Poller

Email2SMS Poller is an alternative for Email2SMS feature for converting emails to SMS messages. This plugin should be used when you need to fetch emails from an existing mailbox on your mail server. The Email2SMS Poller feature connects to a configured email account and polls it in specified periods of time for new emails. Once a new email is received, it is automatically converted to an SMS message.

The feature supports POP3 and IMAP accounts. Plugin supports basic authentication for all mailboxes and Oauth2 for Office365 mailboxes.

To send an SMS using Email2SMS Poller you have to send an email to a specified email account, with the email subject containing a mobile number (or multiple phone numbers separated with comma) or phonebook contact/group name.

Basic example

For example, such email message:

TO: smseagle@mycompany.com
FROM: john.doe@mycompany.com
SUBJECT: +48333444555
BODY: Hello world!

In this case SMSEagle gateway will fetch an incoming email from smseagle@mycompany.com account and send its body as SMS message to +48333444555 mobile number.

Send to username/group

If you want to send SMS to a contact or group from SMSEagle phonebook, put the contact/group name in SUBJECT field.

Send to Ldap contacts/groups

If your company uses LDAP (Active Directory or OpenLDAP) for contacts management, you may use LDAP Contacts or Groups to send email to SMS text message.

Example: email message sent with the subject myldap-admins will be converted to SMS message and delivered to all members of myldap-admins1 group. The myldap-admins1 group must be defined in your LDAP directory and LDAP plugin must be configured on your SMSEagle device.

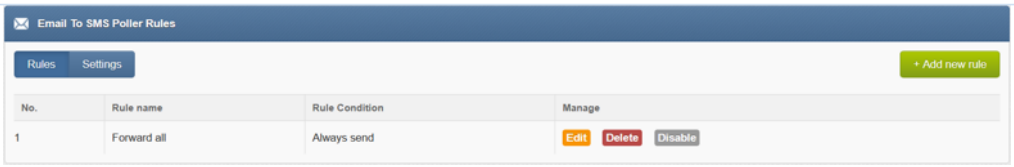
Voice Call

An SMS message converted from email can be optionally followed by a wake-up call or text-to-speech call. This can be enabled in the rule definition. The feature requires a device with an active Voice-Call add-on.

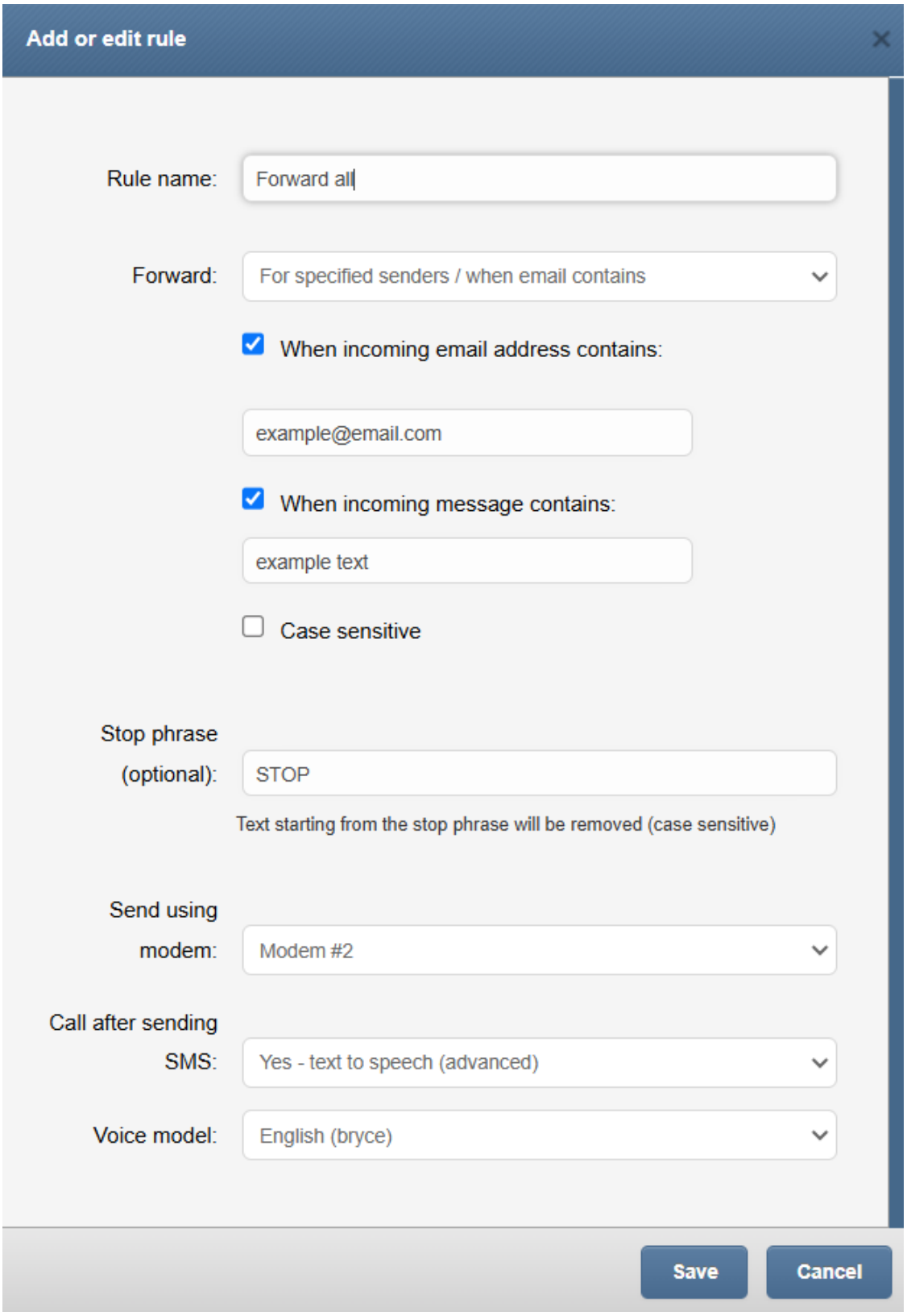
Important Notice:
Messages that are processed by Email2SMS Poller (but not deleted) are marked in the mailbox as read. Software is based on flagging messages- Read/Unread. Marking a read message in the mailbox as unread will result in being processed again by Email2SMS Poller. We suggest using a separate email account to avoid situation with resending the same message (marking unread already processed read message).

Feature configuration

The feature “Email To SMS Poller” allows to add many forwarding rules. Each rule can be enabled or disabled by user.

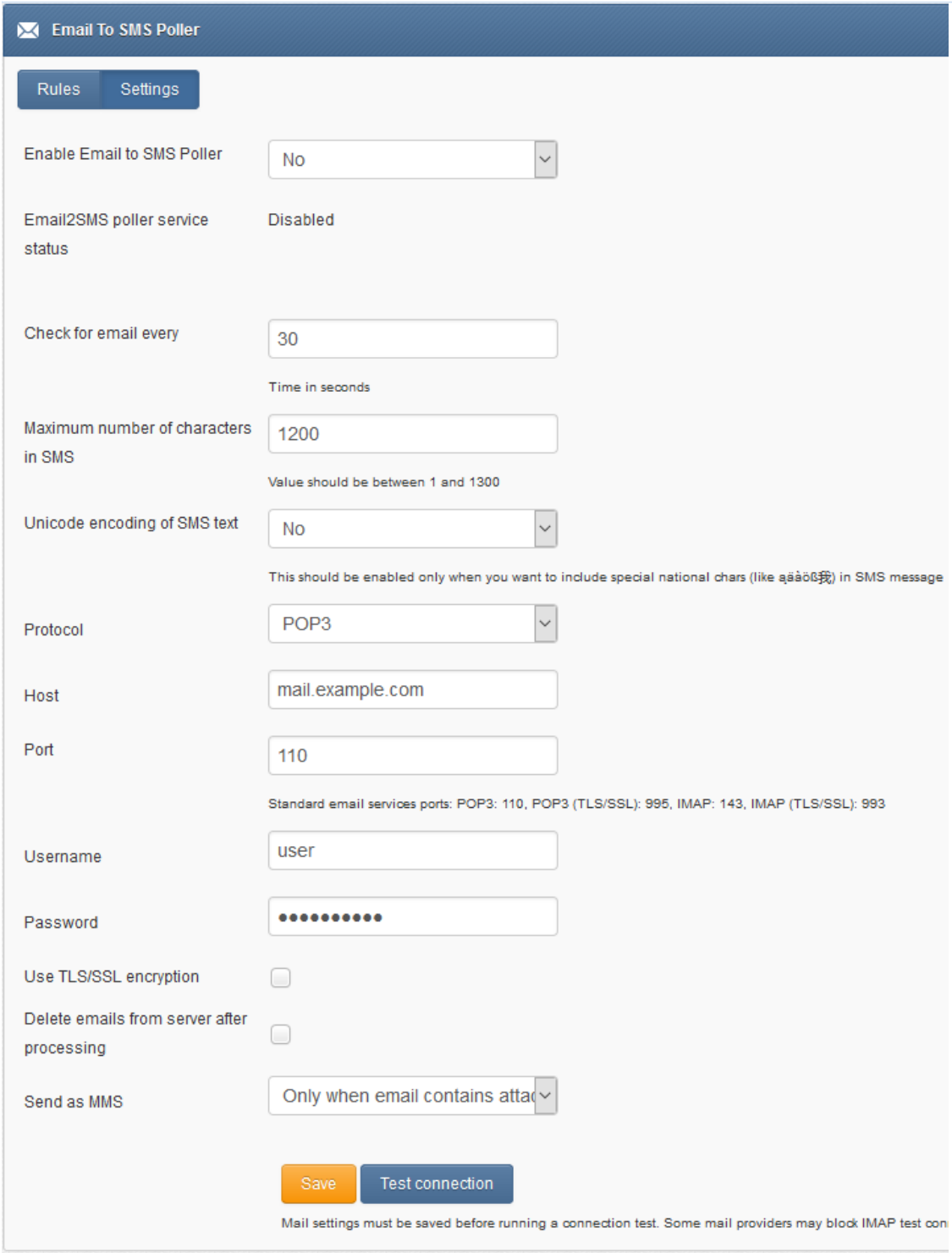


Screenshot from Email to SMS Poller Rules



Screenshot from Email to SMS Poller > Add new rule

- You can name your rule
- You can set forwarding to Always or For specified senders / when email contains
- You can choose sending modem no.
- You can define “Stop phrase”. Text starting from the stop phrase will be removed (case sensitive) from the message
- You can set message priority (0–9). Messages with higher priority will be processed earlier in the outbound queue



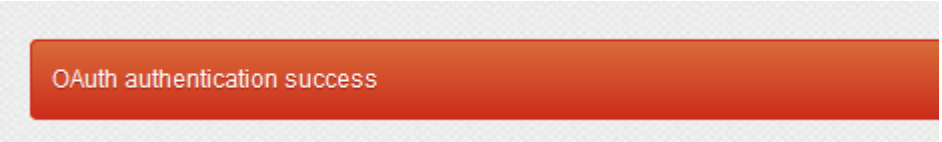
Screenshot from Email to SMS Poller settings

- if you want to use the plugin, set ‘Enable Email2SMS Poller’ to ‘Yes’
- Set email fetching interval (in seconds)
- the text of an email will be cropped to the value ‘Maximum number of characters. Maximum allowed length of SMS message is 1300 characters.
- If you want to include special national characters, enable “Unicode encoding of SMS text”
- Choose protocol from IMAP or POP3

- Provide mailbox configuration (host, port, user, password, encryption settings)
- If you want to delete emails from the mailbox after they are fetched by Email2SMS Poller, please mark “Delete emails from server after processing”
- If you want to send as MMS, select always or only when email contains an attachment

Feature configuration for Office 365 OAuth2

- in Settings tab > parameter “Protocol” choose “IMAP + Oauth2 (Office 365)”
- Host: enter IMAP server for Office365 (default: outlook.office365.com)
- Username: enter email address of the mailbox which will be used for Email2SMS Poller
- follow the instructions in the knowledgebase article: How to setup Office365 for Oauth2? to get values for Client ID, Tenant ID, Client Secret from Microsoft Azure Portal
- Enter the values Client ID, Tenant ID, Client Secret in plugin settings
- press “Save” button to save settings
- press “Authenticate via Oauth” button and login with email and password of the mailbox which will be used for Email2SMS Poller
- If the process is completed successfully you should see “Oauth authentication success” message in SMSEagle webGUI



SMS to Email

SMS to Email feature allows you to forward incoming SMS/MMS messages to email address.

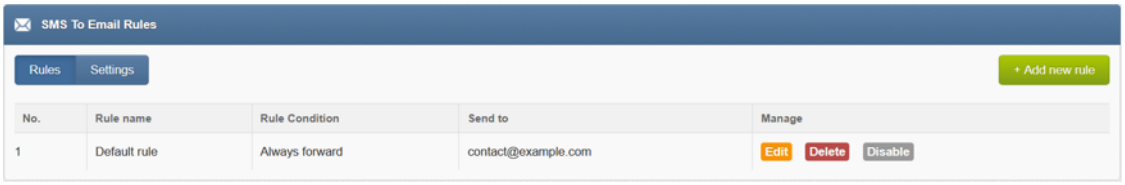
The feature can be used in two modes:

1. forwarding of incoming SMS to email of last sender (so called **Two-way Email2SMS & SMS2Email**)
   In this mode, when SMSEagle receives incoming SMS, it checks if earlier anyone was sending SMS to the number from incoming SMS using Emai2SMS. If last sender is found, the incoming SMS is forwarded to the email address of last sender. If no last sender is found, then the incoming message is forwarded to a default email address given in plugin settings.
2. It forwards all the incoming messages to one fixed email address.
   In this mode incoming SMS messages are forwarded to always the same email address.

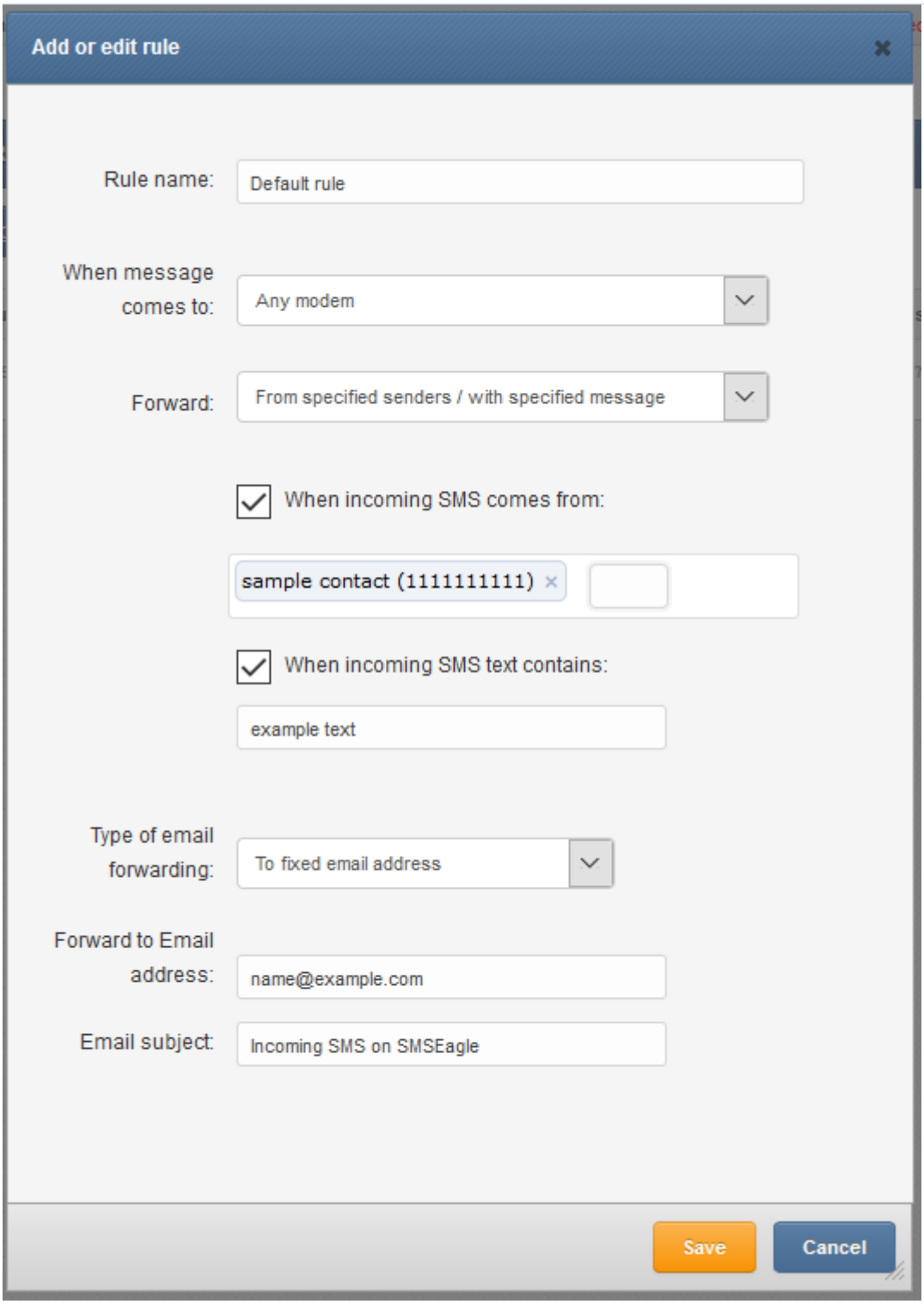
Feature configuration

The feature uses an external SMTP email server for sending emails. You can configure the email server via menu Emails > SMTP Configuration. Please add at least one configuration and select the configuration in the drop-down parameter “SMS To Email” below.

The “SMS To Email” allows to add multiple forwarding rules. Each rule can be enabled or disabled by a user.



Screenshot from SMS to Email > Rules



Screenshot from SMS to Email > Rules> Add or Edit rule

In the rule definition you may choose to forward all incoming messages or just messages from specified senders/with specific text. Email subject can be a fixed text or you can use placeholders: {SENDER} - Sender number, {WORDS,X} - First X words from the message, {CHARS,X} - First X characters from the message.

Email text from this feature

Email body from SMS To Email feature contains:

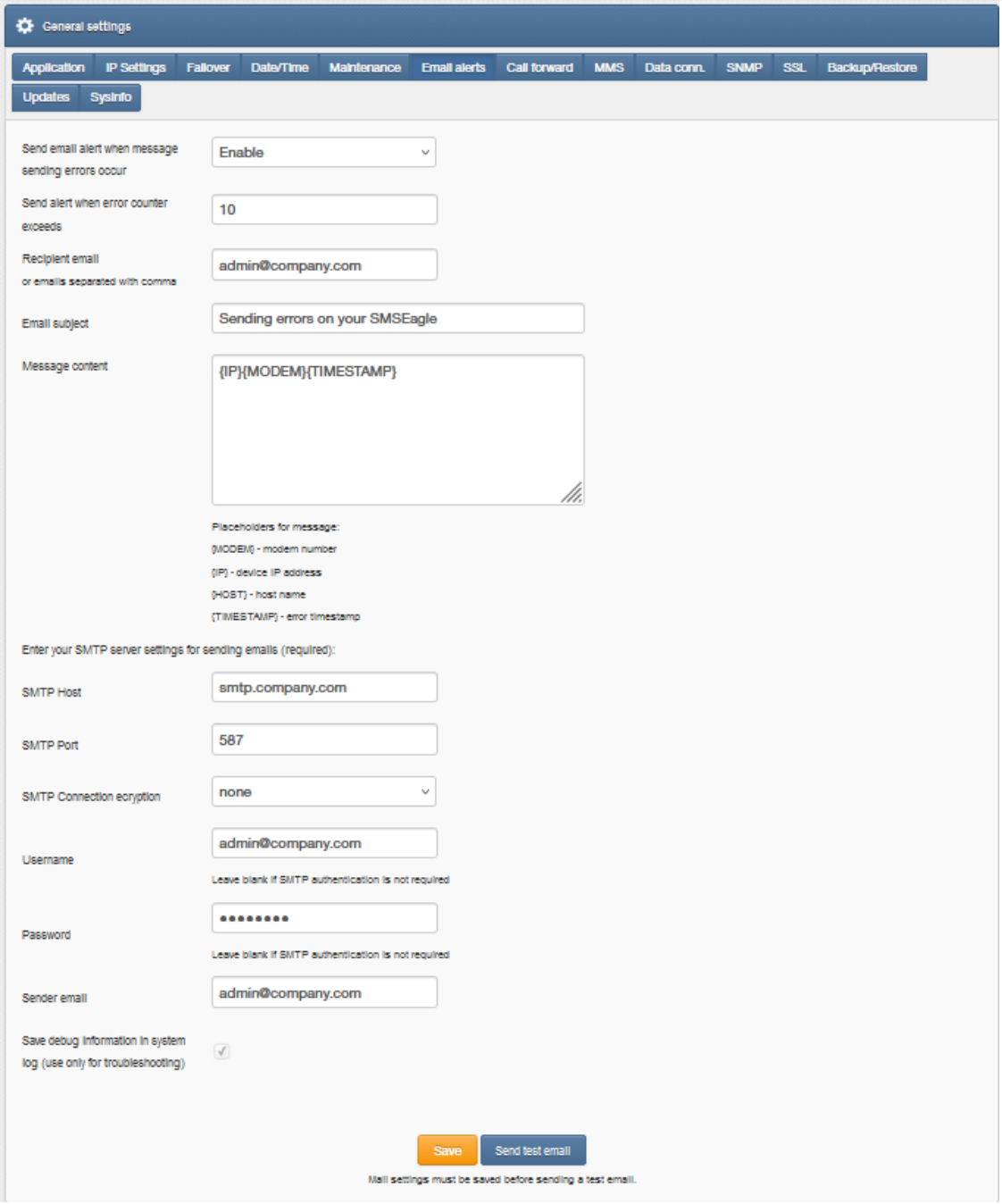
- phone number from incoming SMS (and phonebook contact name if found)
- Date, time when SMS is received
- SMS message

Example email text sent from SMSEagle:
From: +483334455 (John Doe)
Received: 2017-06-01 14:38:12
Message: My SMS message

Email Alerts

The Email Alerts feature allows sending of an email alert message to a selected email address once SMS sending errors occur. When a defined error counter threshold is reached, an alert email is triggered.

The feature can be accessed under Settings tab > Email Alerts



- You can Enable/Disable sending of an email alert when message sending occurs
- You can set the number of errors before an alert is sent
- You can set the email/s of recipients
- You can set the email subject and content of the message including placeholders.
- You can enter your SMTP server settings for sending emails
- You can save debug information in system log (enable this only for troubleshooting)

Email server that is used for SMS to Email is configured via menu Emails > SMTP Configuration. Please add at least one configuration and select it in the drop down parameter below.

Notice: To prevent false alarms we recommend to set parameter "Send alert when error counter exceeds" to value > 2.

Email Conversations

The Emails module includes a dedicated Conversations page, which displays incoming and outgoing email messages in a threaded view grouped by sender/recipient. This makes it easy to track the full history of email communication directly from the SMSEagle web GUI.

Incoming and outgoing email messages are automatically saved to the device and accessible from the Conversations page.

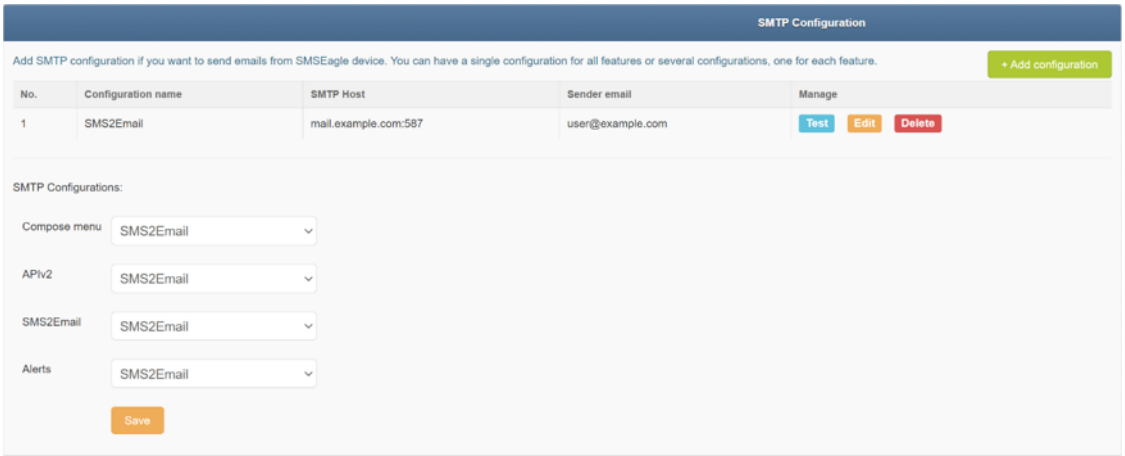


Screenshot from menu Emails>Conversations

SMTP Configuration

SMTP Configuration menu is a single point for configuration of SMTP settings. These settings are necessary if you want to send emails from SMSEagle device in various features like SMS to Email, API, Compose menu, Email Alerts.

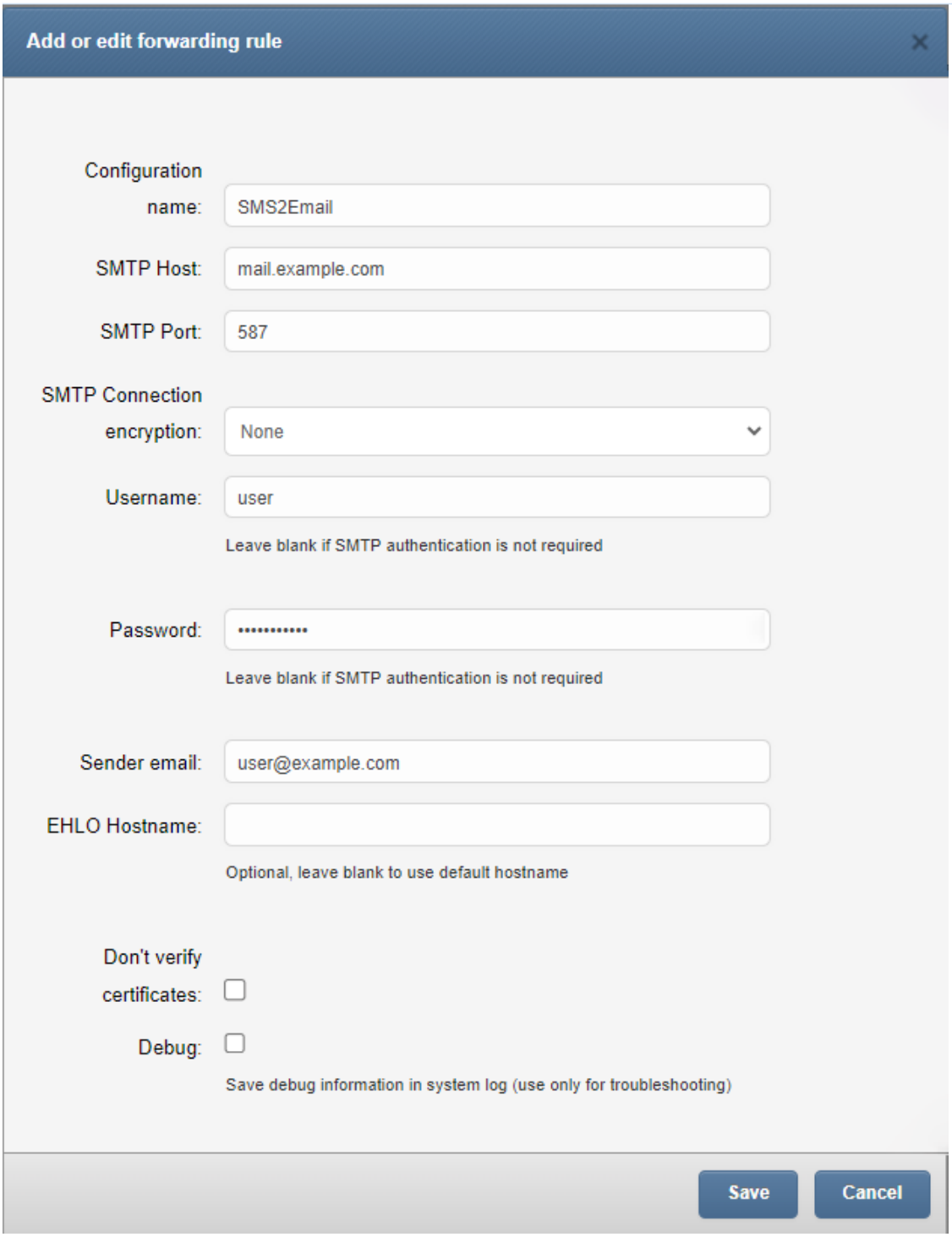
Here you can have a single configuration for all features or several configurations, one for each feature.



screenshot from menu SMTP Configuration

To start using Email features on your SMSEagle:

1. Create at least one configuration

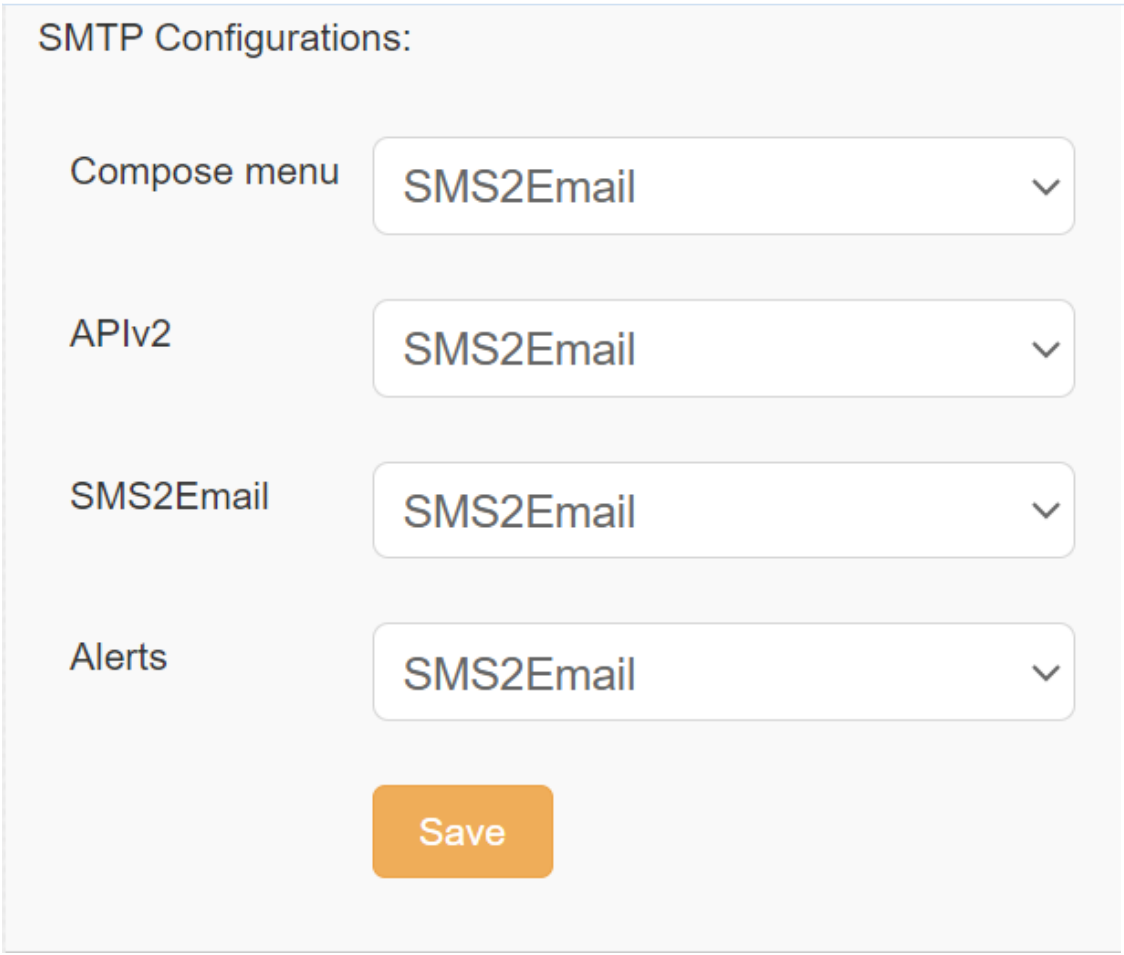


screenshot from SMTP add configuration

- Set a configuration name
- Set SMTP Host
- Set SMTP Port
- Select SMTP Connection encryption (none, SSL, TLS)

2. Assign configuration to a selected feature

Once a configuration entry is setup, assign it to a selected feature.

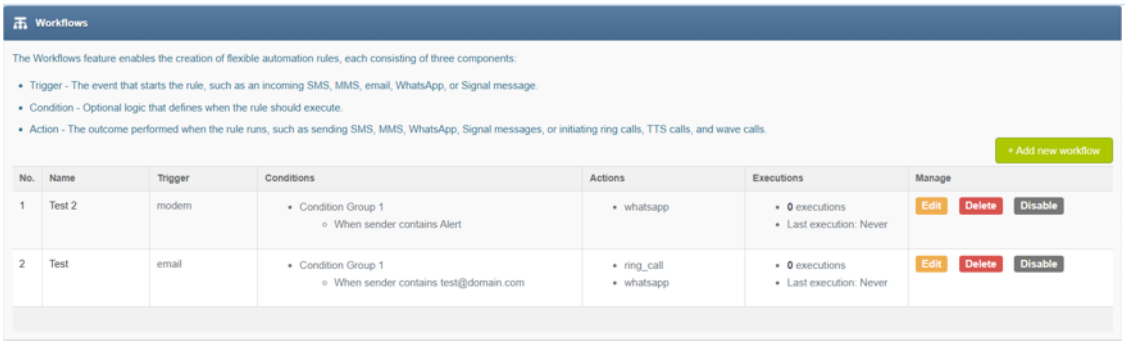


Workflows

The Workflows feature enables advanced management of inbound and outbound communications by defining rules and actions based on message content and source. It enables the creation of very flexible automation rules, each consisting of three components:

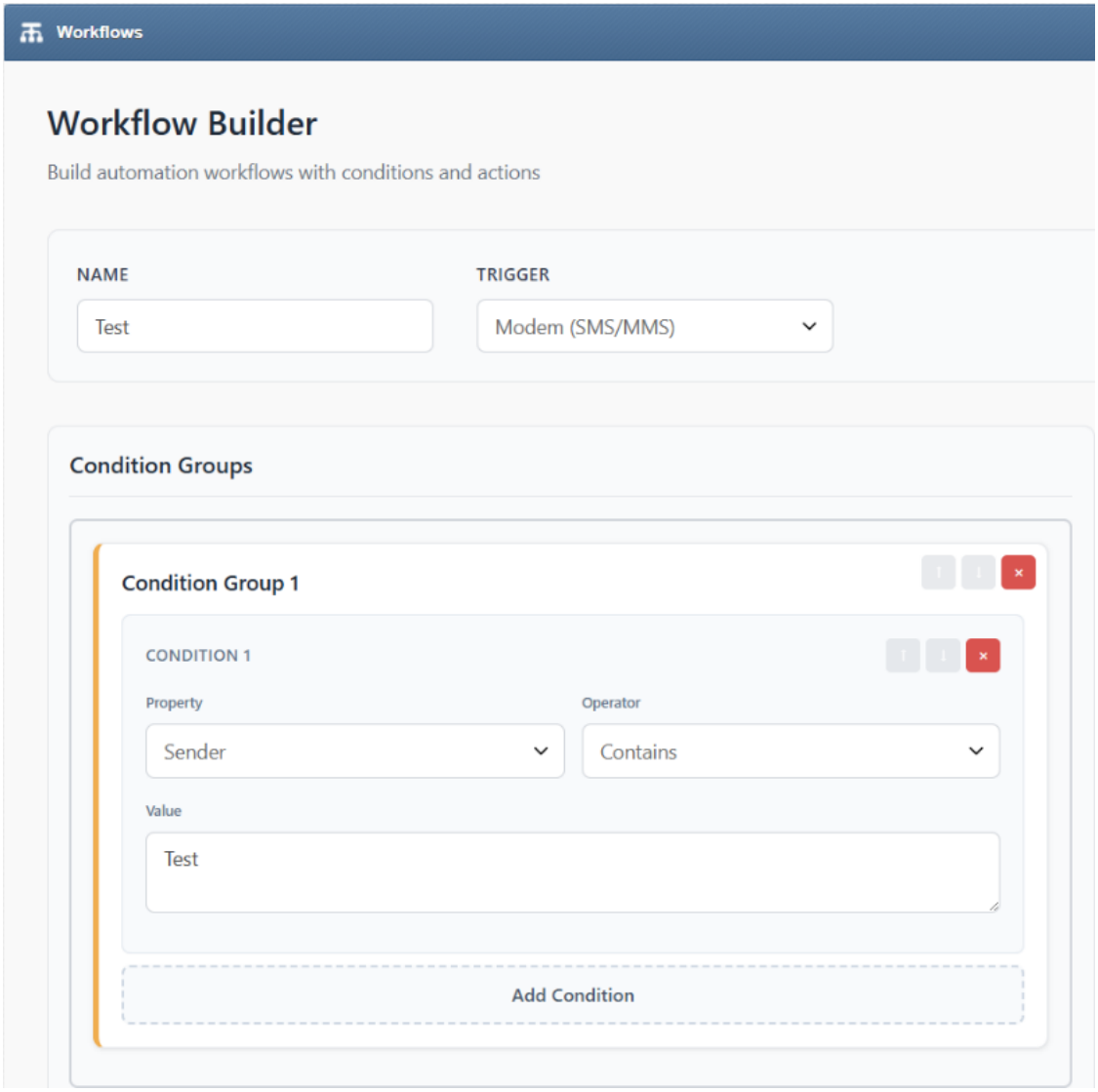
- **Trigger** - The event that starts the rule, such as an incoming SMS, MMS, email, WhatsApp, or Signal message.
- **Condition** - Optional logic that defines when the rule should execute.
- **Action** - The outcome performed when the rule runs, such as sending SMS, MMS, WhatsApp, Signal messages, or initiating ring calls, Text-To-Speech calls, and wave-file calls.

The Workflows feature allows you to add multiple processing rules. Each rule can be enabled or disabled by a user.



Workflow builder

To create a single Workflow rule, you use the Workflow Builder. This tool allows you to automate the processing of incoming messages (or other events) using point-and-click rules.



Screenshot from the Workflow Builder

In each workflow, you can configure:

Name
Enter a descriptive name for your rule.

Trigger
The trigger is an event that starts the rule. You can choose from triggers:

- Modem (SMS/MMS)
- Email
- WhatsApp
- Signal
- On Sent (SMS/MMS): triggered when an outgoing message has been sent
- On Error (SMS/MMS): triggered when a message sending error occurs
- On Delivery Report (SMS/MMS): triggered when a delivery report is received

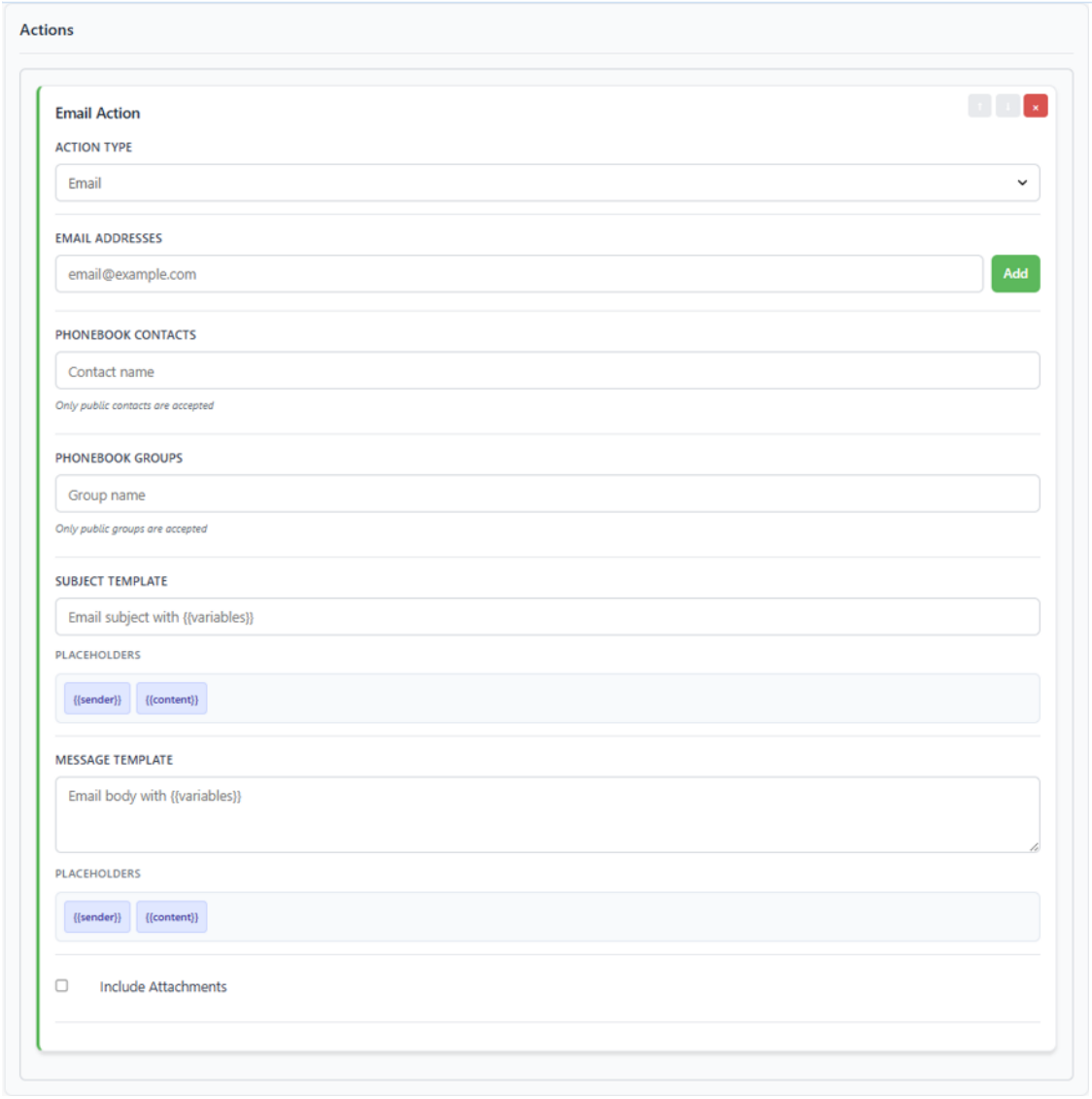
Condition Groups
Build a logic with groups of conditions. Each condition has:

- Property (Sender or Content)
- Operator (Contains, Equals, Not Equals, Ends With, Not Contains, Regex Match, Starts With, In Group or In Contact)
- Value (free text)

You can add multiple conditions inside a group connected with AND logic. You can add multiple condition groups connected with OR logic.

Actions
An action defines what will happen when the conditions are met. The following actions are available:

- SMS
- TTS Call
- TTS Advanced Call
- Ring Call
- Wave Call
- Email
- WhatsApp
- Signal



Screenshot from menu > Workflows > +Add new workflow > Email Action

The screenshot above shows an **Email Action Example**:

- Email addresses: Enter one or more recipients and click Add.
- Phonebook contacts / groups: Target saved public contacts or public groups (only public entries are accepted).
- Subject template and Message template: Compose the outgoing email using placeholders:
    - Available placeholders (as shown): {{sender}}, {{content}}
- Include attachments: Optional checkbox to forward any attachments.

You can add multiple actions within one workflow, for example: send SMS and make a call.

Dynamic recipient placeholders

When the trigger is set to **Email**, dynamic recipient placeholders are available, allowing the workflow to automatically route the message to recipient derived from the incoming message content. The recipient can be derived from:

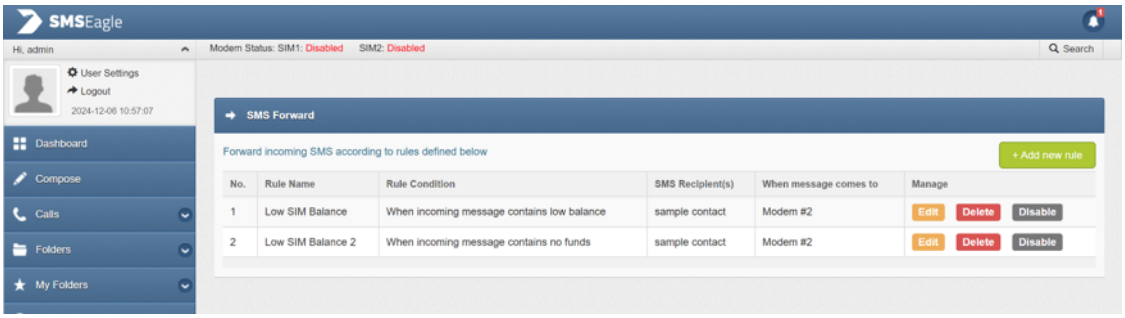
- email identifier: phone number extracted from to address (eg. from +48123456789@domain.com it takes +48123456789).
- subject: uses an email subject to extract a recipient phone number, or phonebook contact id, or phonebook group id

SMS Forward

The feature “SMS forward” allows to forward incoming SMS messages to one/may recipients according to defined rules.

Feature configuration

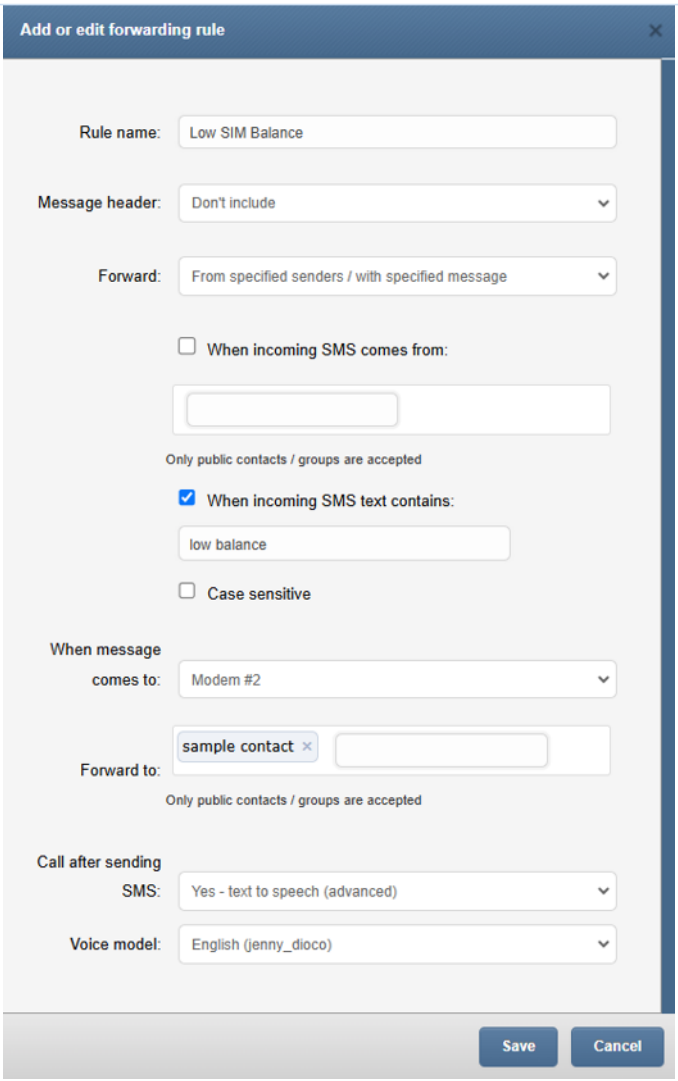
The feature “SMS Forward” allows to add many forwarding rules. Each rule can be enabled or disabled by user.



Screenshot from plugin main window

For each rule user can define:

- When incoming SMS should be forwarded (Rule type) and to what number(s) the message should be forwarded (SMS Recipient).
- Whether or not include in SMS a sender number from which original SMS came from.
- When defining a rule user can choose SMS recipient (who gets the forwarded SMS). It can be either phone number or name of group from phonebook.
- User may define many forwarding rules in the plugin.
- Each rule is processed independently.
- Priority can be set (0-9), message with a higher priority will be queued earlier.
- User may choose to include a custom text along with placeholders:
- {SENDER} - Sender number
  {MESSAGE} - Original message
- There is a possibility to enable/disable each rule.



Screenshot form “Add/edit forwarding rule”

Voice Call

An SMS message can be optionally followed by a wake-up call or text-to-speech call. This can be enabled in the rule definition. The feature requires a device with an active Voice-Call add-on.

MQTT

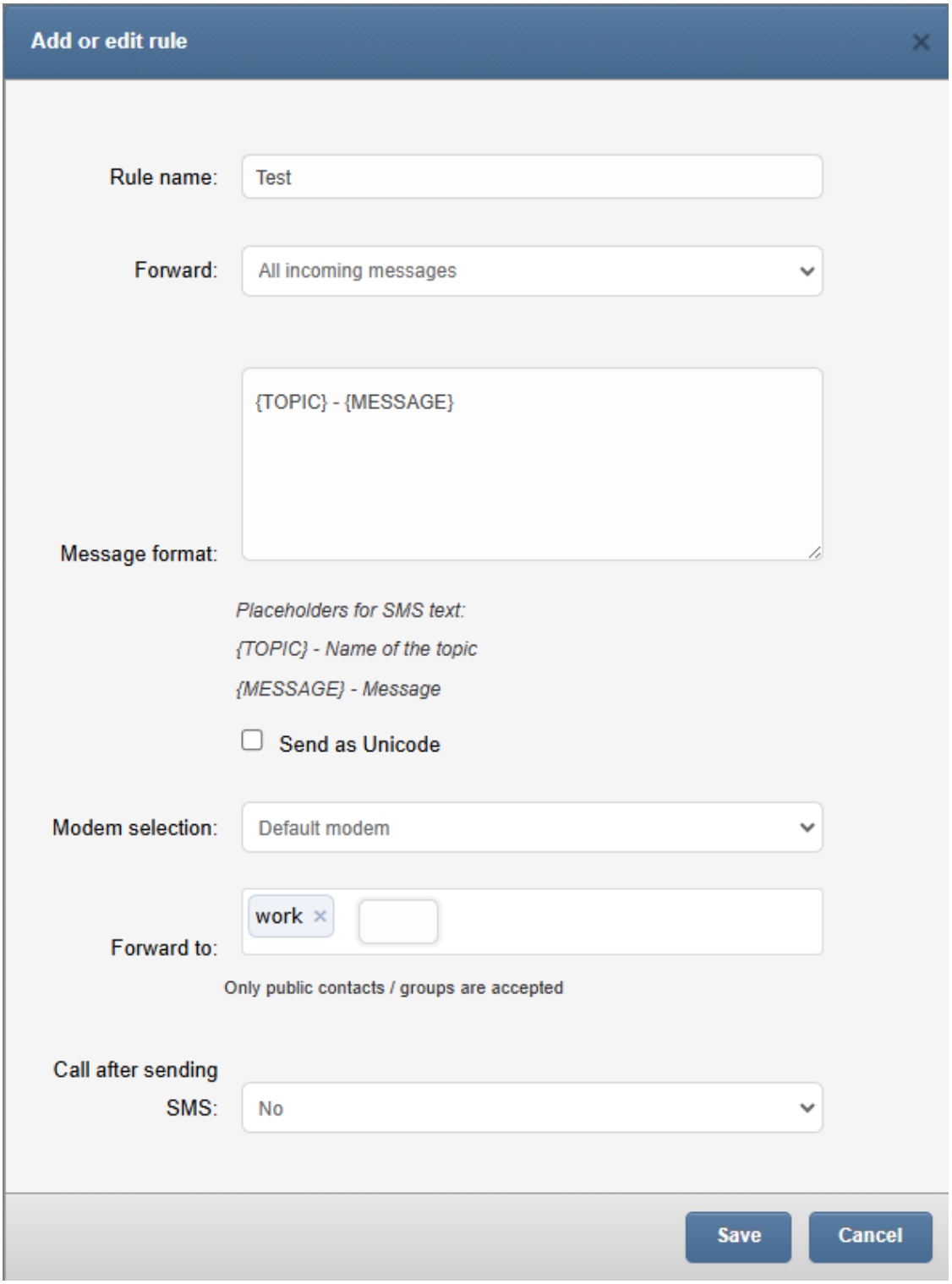
MQTT is a messaging protocol for the Internet of Things (IoT). It is designed as an extremely lightweight publish/subscribe messaging transport that is ideal for connecting remote devices with a minimal network bandwidth. MQTT today is used in a wide variety of industries, such as automotive, manufacturing, telecommunications, oil and gas, etc.

The MQTT feature on SMSEagle lets you create multiple conversion rules:

- when an SMS text arrives at the SMSEagle gateway with a predefined content, it is forwarded to MQTT
- when a message with a defined content arrives at MQTT, the SMSEagle gateway can send it as an SMS to single or multiple recipients

Feature configuration

The “MQTT” feature allows you to define several processing rules for both Subscribe and Publish scenario.



Screenshot from MQTT add rule

Subscribe rules



Screenshot from MQTT subscribe window

For each processing rule user can define:

1. if forwarding should always be sent or only from specified topic/when MQTT message contains
2. the text of the outgoing SMS message
3. message recipient (single or group)
4. for multi-modem devices users can also define from which modem the SMS is sent

Publish rules



Screenshot from MQTT publish window.

For each processing rule user can define:

1. if forwarding SMS should always be sent or only for specified sender/message text
2. host, port and topic of MQTT subscriber
3. for multi-modem devices users can also define from which modem the SMS is received

WhatsApp

The WhatsApp feature on the SMSEagle device enables you to send and receive WhatsApp messages via the web GUI or APIv2, or through automatic message conversion. Once you have connected a WhatsApp account in the 'Settings' menu, you can send WhatsApp messages via the 'Compose' menu. You can also configure automation workflows in combination with other sources, such as emails, SMS messages or Signal messages. This secure, on-premises extension to your messaging stack enables real-time incident handling and customer communication via the popular WhatsApp channel. The messaging relies on data, so your device should be connected to the Internet via Ethernet or mobile data.

The WhatsApp functionality enables users to send messages that include both text and images. Supported image formats include JPEG, GIF, PNG, and BMP, allowing for flexible and rich communication.

DISCLAIMER

- This integration operates through **a legitimate, user-authenticated session of WhatsApp Web.** It does not use any unofficial API or reverse-engineered protocol.
- WhatsApp Inc. does not officially support or endorse the use of automated systems, bots, or unofficial clients to access their platform.
- Users are responsible for complying with WhatsApp's Terms of Service, including restrictions on automation and third-party integrations.
- SMSEagle **provides this feature as-is**, and cannot guarantee uninterrupted functionality due to potential changes in WhatsApp's platform, policies, or technical infrastructure.
- Use of this feature may be subject to limitations or account restrictions imposed by WhatsApp.

By enabling and using this feature, the user acknowledges and accepts the above conditions.

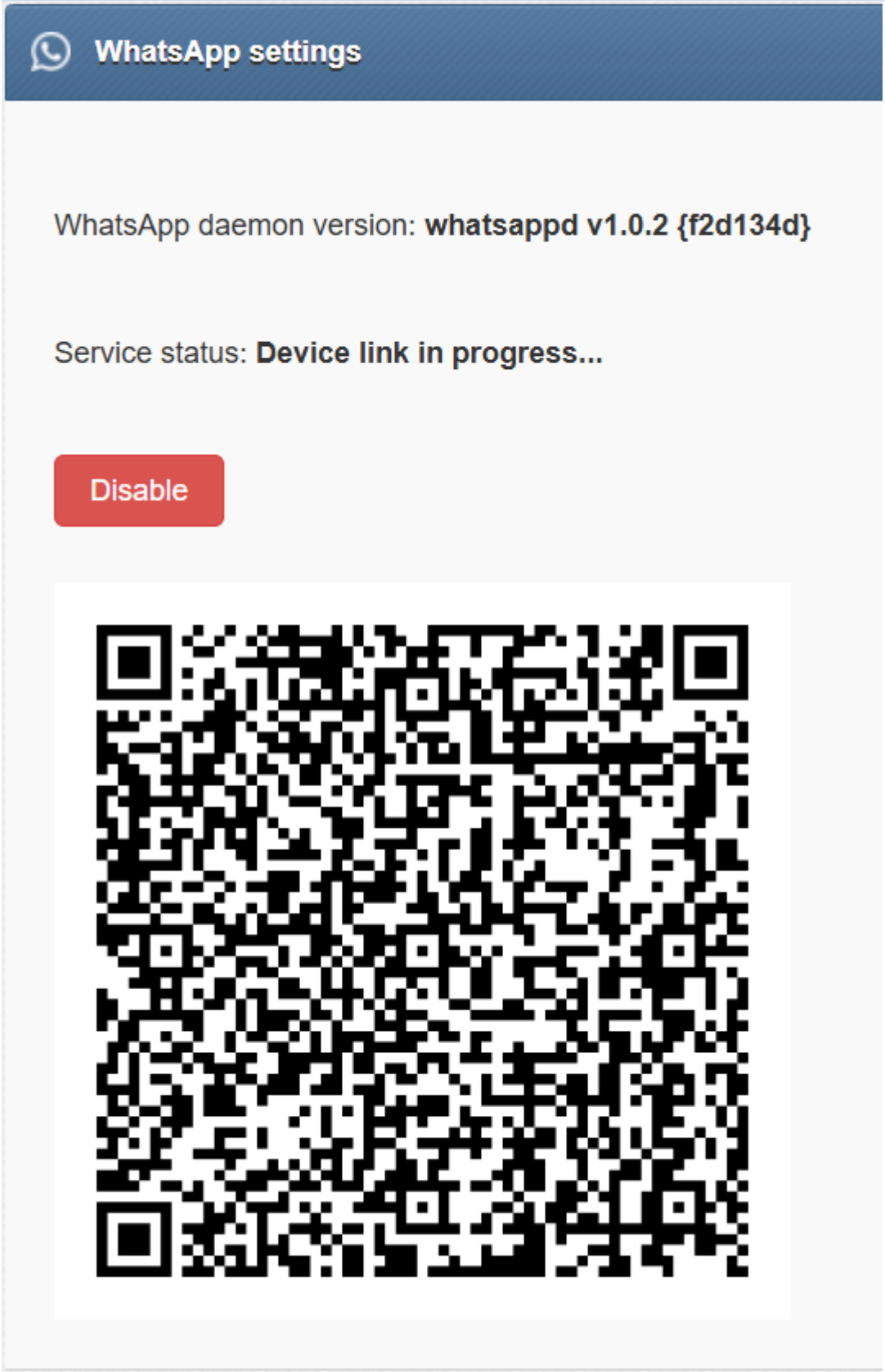
WhatsApp is a trademark of Meta Platforms, Inc. This product is not affiliated with, endorsed by, or sponsored by WhatsApp or Meta Platforms.

Setting up



Screenshot from menu > WhatsApp settings

1. In SMSEagle web-GUI > menu WhatsApp > select the Settings tab and click **Show QR code**
2. Open the **WhatsApp application on your mobile phone** (it must be already registered to a WhatsApp account), open the context menu (three dots) and go to **"Linked devices"**.
3. *Select **Link a device** and scan the QR code displayed in SMSEagle web-GUI. *
4. Once the app is paired you're ready to send/receive WhatsApp messages via SMSEagle.



Screenshot from menu > WhatsApp settings



* *

Screenshot from menu > WhatsApp settings

Send WhatsApp message with SMS/MMS fallback

In the WhatsApp Settings tab you can set a fallback to SMS/MMS. If the recipient's number is not registered with WhatsApp, the SMSEagle will send the message as an SMS or MMS (if the message includes attachments).

Library updates
SMSEagle includes a built-in mechanism for updating the WhatsApp integration library. Since WhatsApp periodically updates its platform, keeping the library up to date ensures continued compatibility and uninterrupted operation. Available updates can be checked and applied from the WhatsApp Settings tab.

Signal (beta)

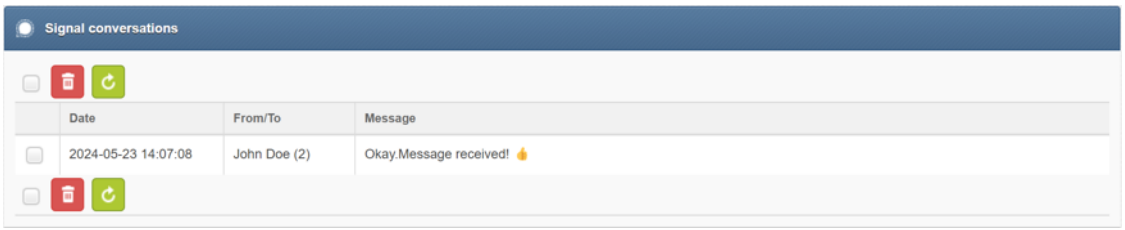
(available on NXS Rev. 4 devices)

Signal is a secure messaging app. It offers encrypted messages, voice and video calls. Security experts recommend Signal because it's end-to-end encrypted. This ensures that only your device and the recipient's device can read the messages you send. The team behind the software operates as a nonprofit, supported by grants and donations. Signal is open source, meaning its code is publicly accessible.

SMSEagle devices support Signal messaging when sending messages from web-GUI or APIv2. You can also configure automation workflows in combination with other sources, such as emails, SMS messages, etc.

To start using Signal, go to the menu Signal > Settings and register a phone number used in your SMSEagle device as described in the knowledgebase article: How to setup Signal on SMSEagle device. The messaging relies on data, so your device should be connected to the Internet via Ethernet or mobile data.

Sent/received Signal messages can be found in menu Signal > Conversations



Screenshot from menu Signal > Conversations

Webhooks (aka. Callback URL)

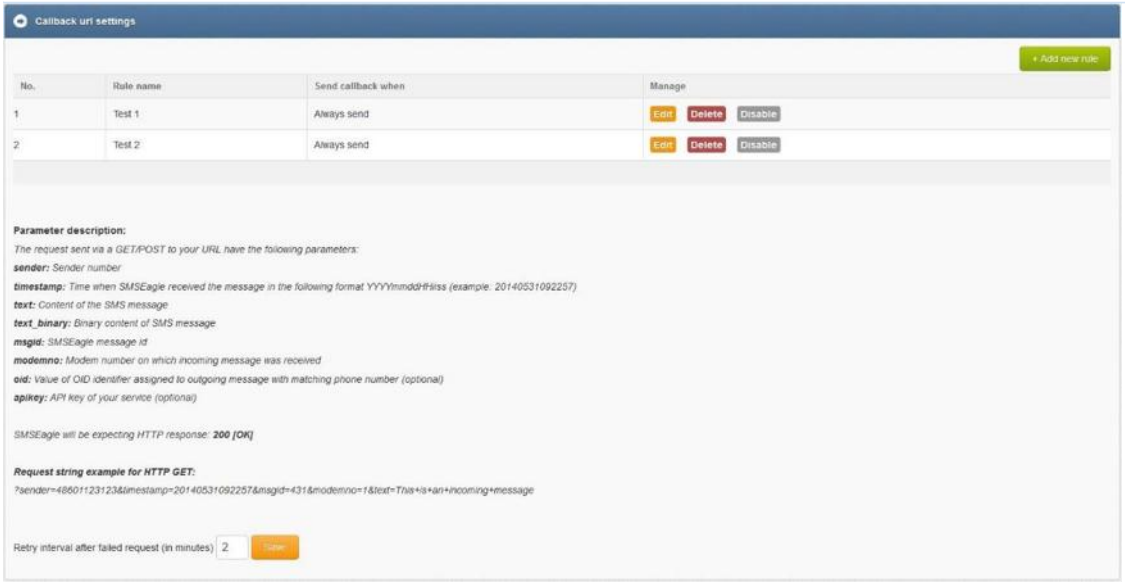
Webhooks URL feature allows you to:

- forward incoming message to a defined URL address
- call defined URL address if outgoing message status has changed (message was sent/ delivered or there was a sending error)

If the feature is enabled, each defined rule will trigger HTTP(S) request to a defined URL. HTTP(S) request can be of type GET or POST.

Feature configuration

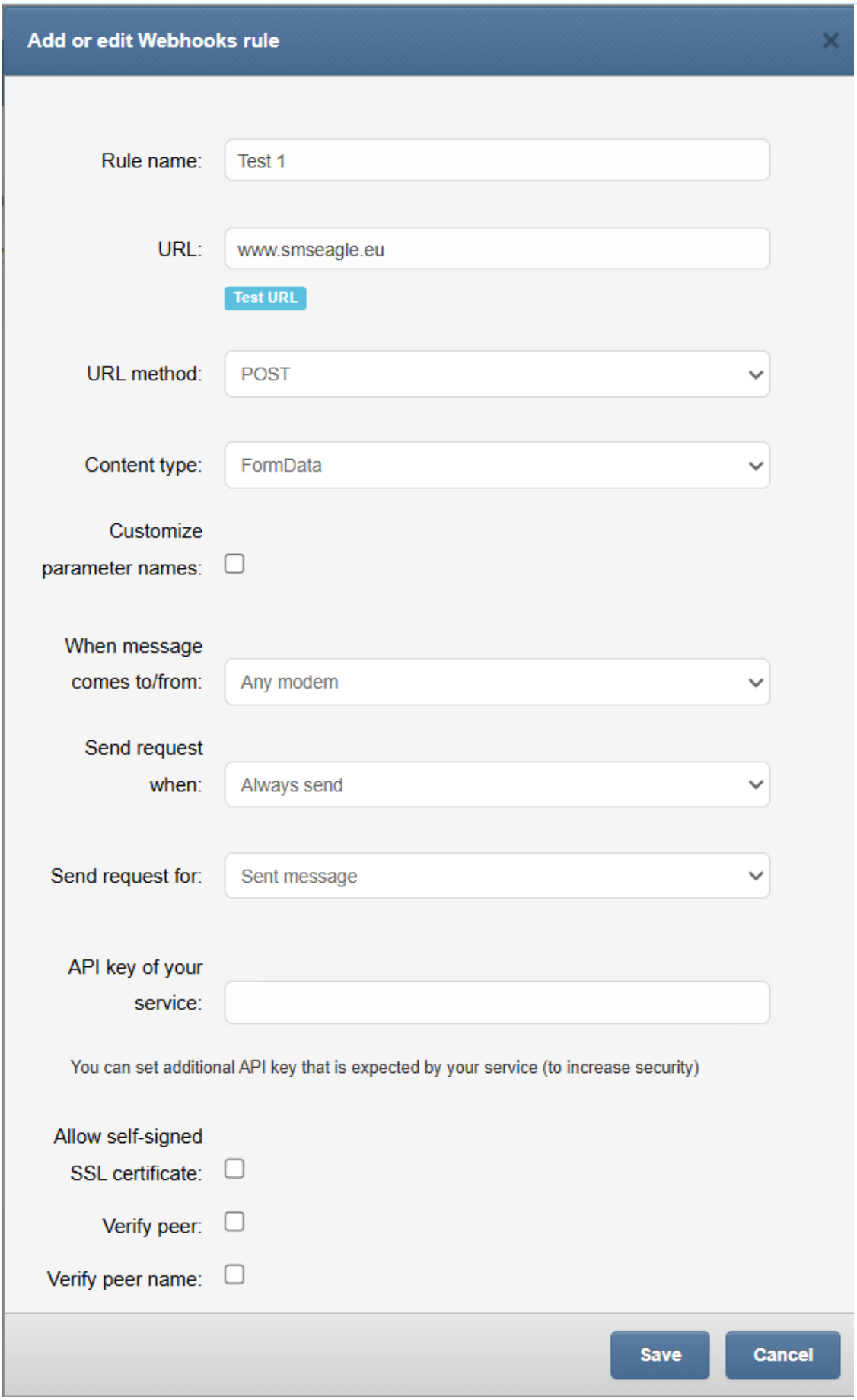
The Webhooks feature allows to add unlimited number of rules. Each rule can be enabled or disabled by user.



Screenshot from Webhooks settings

For each new rule user has to fill in the requested fields:

- Rule name
- 'URL' field defines remote address of your callback script
- 'Test URL' button allows to test whether your Webhooks configuration is correct. SMSEagle will make a callback request with test parameters and will verify the response of remote server
- 'URL method' allows to choose whether callback to your URL is done with HTTP(S) GET or POST method
- select triggers: on incoming message, on incoming call, on message sent, on message delivery, on sending error
- to change names of variables in GET/POST
- choose payload format for POST (form-data or json)
- "Send request when" defines if the request is always sent, sent only when SMS sender belongs to a given contact/group or only when incoming message contains a given character string
- Optionally you can define "API key of your service" value. This will be passed to your callback URL in parameter 'apikey'. If you leave the field blank, 'apikey' parameter will not be passed to your callback URL
- Expected HTTP Status Code(s): Defines which HTTP response codes are treated as a successful webhook delivery. The webhook is considered OK only if the HTTP response status matches one of the specified codes. Multiple status codes can be provided. Default: 200
- User may also choose whether to enable support of self-signed SSL certificate


Add or edit Webhooks rule
Rule name:
Test 1
URL:
www.smseagle.eu
Test URL
URL method:
POST
Content type:
FormData
Customize parameter names:
When message comes to/from:
Any modem
Send request when:
Always send
Send request for:
Sent message
API key of your service:
You can set additional API key that is expected by your service (to increase security)
Allow self-signed SSL certificate:
Verify peer:
Verify peer name:
Save
Cancel

Request parameters

The request sent via a GET/POST to your URL have the following parameters:
sender: Sender number
timestamp: Time when SMSEagle received/sent the message in the following format YYYYmmddHHiiss (example: 20140531092257)
text: Content of the SMS message
attachments: (POST only) MMS attachments in example format [0 ⇒ [name ⇒ image.png, content-type ⇒ image/png, content ⇒ wfFWgwOlgBRwdWvsvs=]] (optional)
text_binary: Binary content of SMS message
msgid: SMSEagle message id
modemno: Modem number on which incoming message was received/from which message was sent
status: Message status
oid: Value of OID identifier assigned to outgoing message with matching phone number (optional)
apikey: API key of your service (optional)

Expected HTTP response & retry attempts

After sending HTTP(S) GET/POST request to your callback URL, SMSEagle will be expecting HTTP response defined in parameter "Expected HTTP Status Code(s). If other or no response is received from your callback URL, SMSEagle will keep retrying every X minute for 24 hours. Retry interval can be set in main plugin

Window:



Zabbix ACK with SMS

SMSEagle Webhooks allows native integration with Zabbix API for two-way alert acknowledgment.

When configured:

- Zabbix sends an alert to recipients via SMSEagle
- When recipient replies to the SMS, SMSEagle automatically calls the Zabbix API to acknowledge the alert in Zabbix
- The reply text is added as a comment to the Zabbix problem

Configuration parameters in the webhook rule:

- Method: select "POST (Zabbix)", then choose mode:
    - Acknowledge only
    - Unacknowledge only

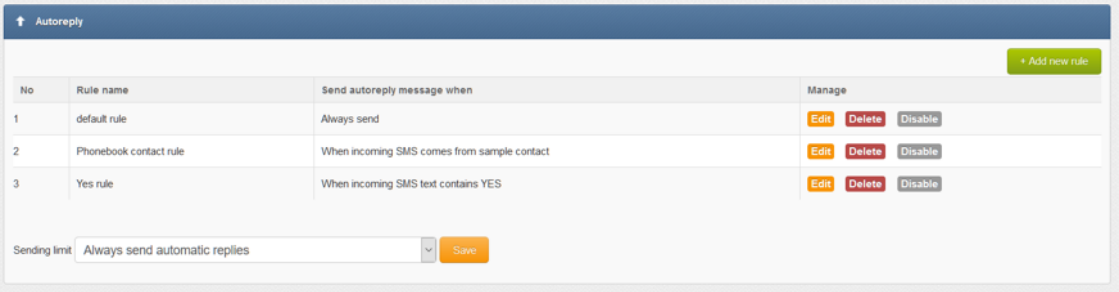
    - Both (ACK and NOACK — detected automatically from SMS prefix)
- Zabbix server URL
- Authentication type:
    - API Token (Zabbix ≥ 6.4)
    - Login/Password (for older Zabbix versions)
- SMS reply format expected: ACK [eventid] [optional message] or NOACK [eventid] [optional message]

Autoreply

The feature allows to automatically respond to each received message with defined text response.

Feature configuration

The feature “Autoreply” allows to add many autoreply rules. Each rule can be enabled or disabled by user.

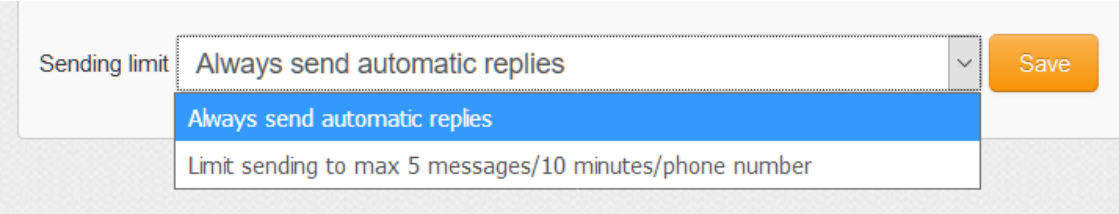


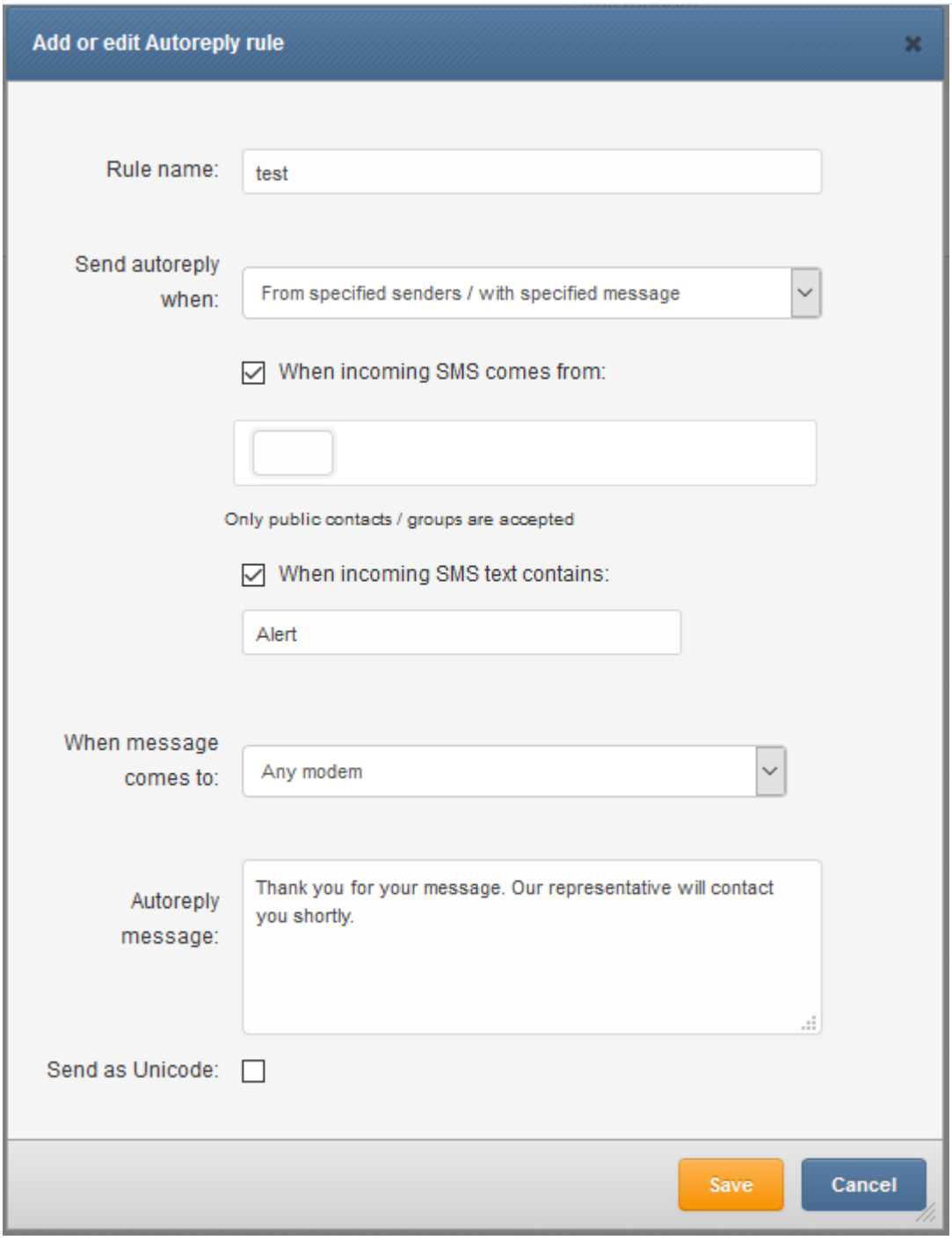
Screenshot from plugin main window

For each rule user can define:

- When autoreply message should be sent:
    - always,
    - when incoming message contains defined text,
    - and/or when message sender belongs to Phonebook contact/group
    - if incoming SMS text comes to a selected modem
- If autoreply message text should be sent as Unicode characters

The feature also allows to define sending limit for autoreply messages. It is possible to set limitation of max 5 messages / 10 minutes / phone number.

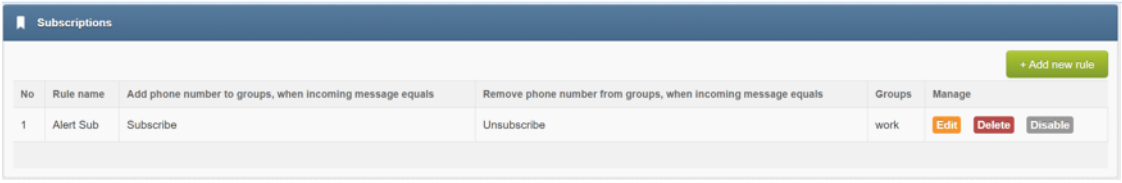




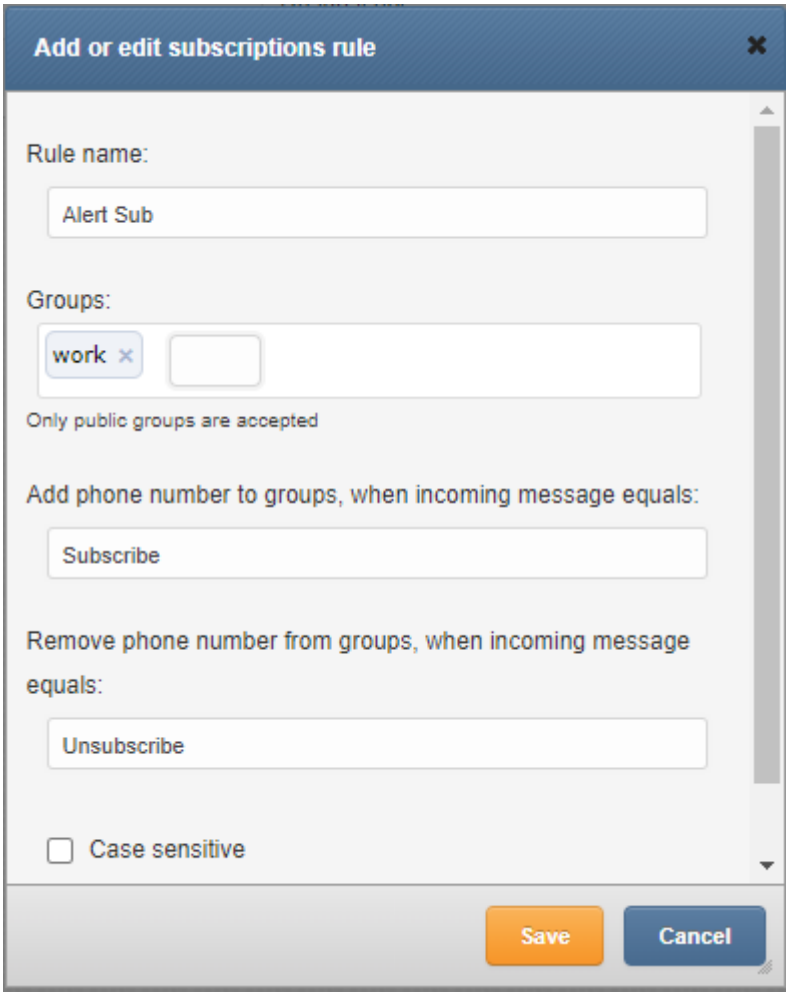
Screenshot form “Add/edit autoreply rule”

Subscriptions (newsletter)

This feature allows to enable newsletter-style subscriptions via SMS. When someone sends a message to your SMSEagle which includes a defined text, the sending number will be automatically added to a Phonebook group. This group can be later used to send messages via web-GUI/API/ Email To SMS. Automatic removal from the group works the same way: when incoming SMS contains a defined text, the sending phone number will be automatically removed.



Screenshot from “Subscriptions” feature



Screenshot from Subscriptions > Add or edit subscriptions rule

In the Add or edit subscriptions rule window:

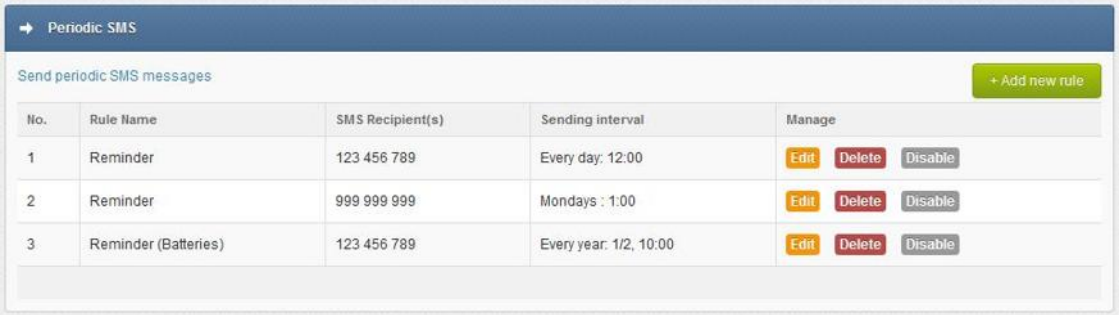
- You can add rule name
- Select group from Phonebook
- Define phrase which adds the phone number from incoming SMS to the group
- Define phrase which removes the number from the group
- Select if the phrase should be case sensitive
- When a phone number is added to SMSEagle Phonebook via this feature, first a phonebook contact is created with a name: [RULE NAME] [PHONE NUMBER]. For example: “Alert Sub +48123456789“. Then the contact is added to a defined Phonebook group.

Periodic SMS

The feature “Periodic SMS” allows to send SMS messages or USSD codes at a desired time interval. User may define many sending rules, and each rule will be processed independently.

Feature configuration

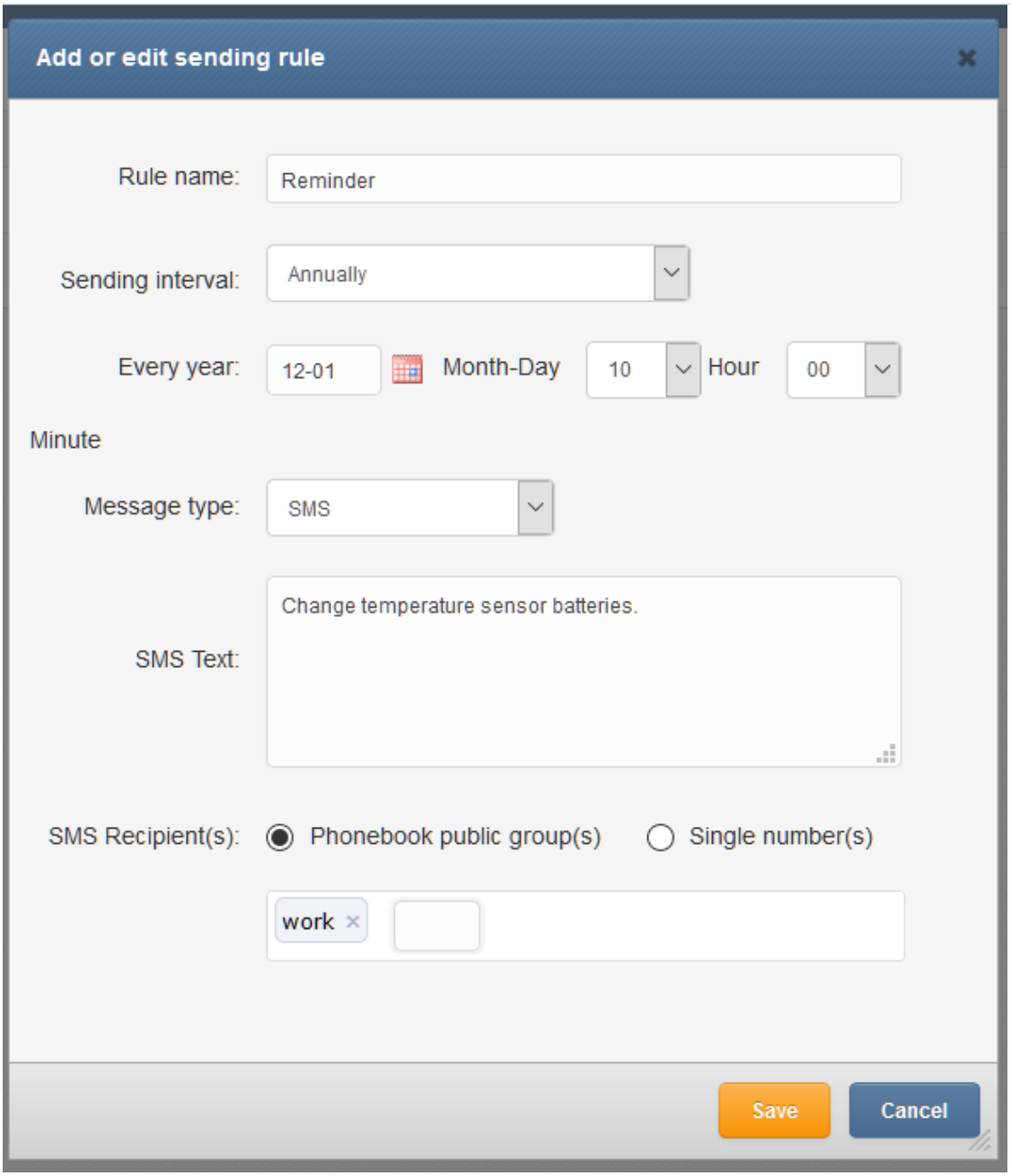
The feature “Periodic SMS” allows to add many sending rules. Each rule can be enabled or disabled by user.



Screenshot from main plugin window

For each rule the user can define:

- The rule name
- Sending interval (Hourly, Daily, Weekly, Monthly or Annually)
- Message type (SMS, USSD Code)
- The content of the SMS text
- The recipients (phone number(s) separated with comma or group(s) from phonebook)



Screenshot from “Add new rule” window

Voice Call

A SMS message can be optionally followed by a wake-up call or text-to-speech call. This can be enabled in the rule definition. The feature requires a device with an active Voice-Call add-on.

Digital I/O

The NXS- family of SMSEagle devices is equipped with digital inputs (DI) and digital outputs (DO). The digital inputs can be used to receive signals from outside sensors or devices and automatically trigger sending of SMS message based on input state. On the other hand, the digital outputs may be used to activate external devices connected to the outputs when certain SMS messages are received by SMSEagle.

Port type	Value
DI	4
DO	4

The logical states of inputs and outputs of SMSEagle NXS-family of devices are represented by the following states:

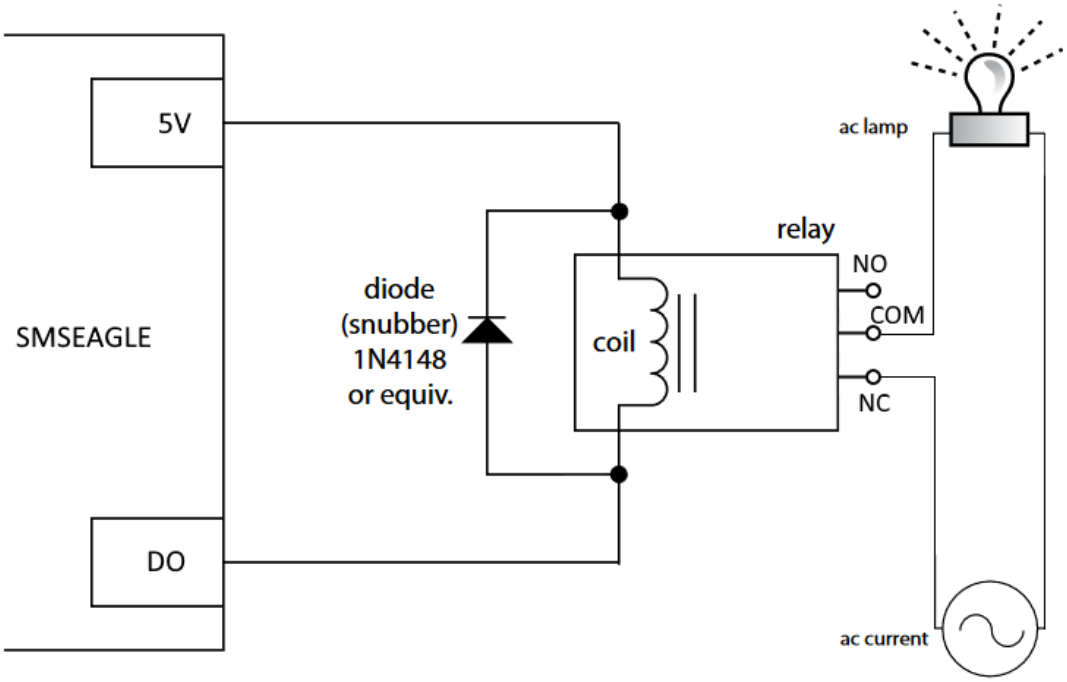
Logical level	Value
LOW (0)	+5V
HIGH (1)	0

Using digital outputs

From digital output, without side effects, you can directly control external circuit with a voltage not exceeding 5V and a current of max. 450mA.

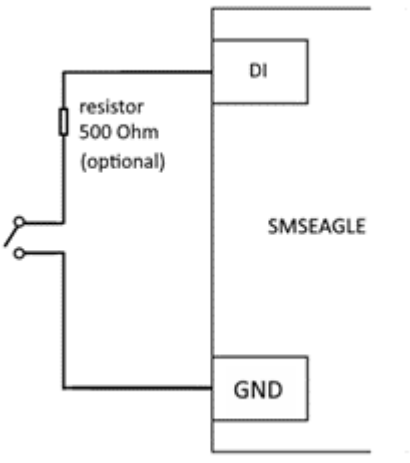
But the safest form of control external circuits is using an intermediary relay with a protection diode. Usage example has been shown on the picture below.

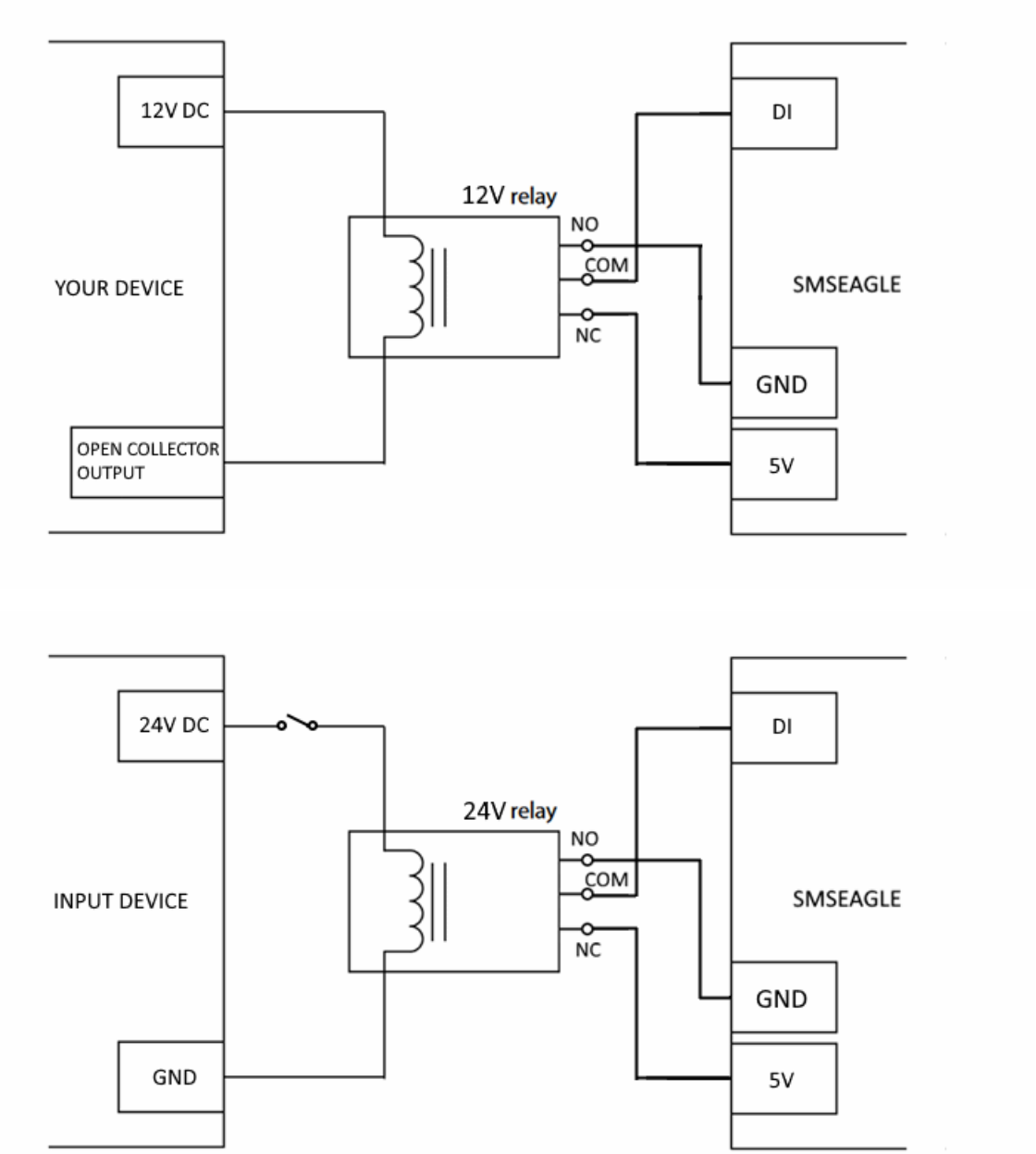
Warning: If you plan to use digital output with relay, it is strongly recommended to connect a separate protection diode (a.k.a. “snubber”) across the relay coil terminals as well. A diode snubber circuit can be added when ordering from some relay manufacturers. This diode is installed in the direction that does not ordinarily allow current to conduct. When current to the inductive load is rapidly interrupted, a large voltage spike is produced in the reverse direction as the inductor attempts to keep current flowing in the circuit. Placing the snubber diode in parallel with the inductive load for reversed-bias flow allows the current from the inductor to flow through the diode rather than through the switching element, dissipating the energy stored in the inductive load from its series resistance and instead goes through the much smaller resistance of the diode.



Using digital inputs

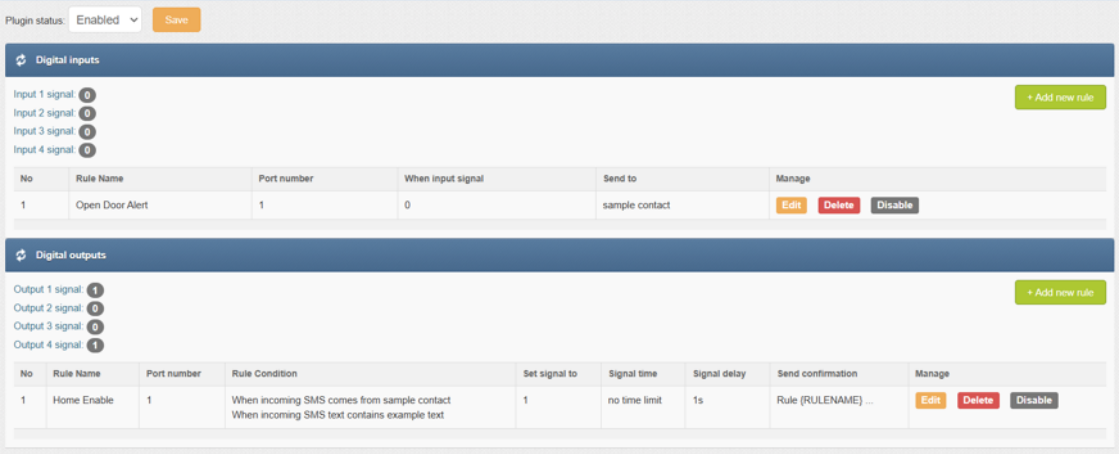
Digital inputs (DI) of SMSEagle device are of type “pull-up resistor”. This type of input is used to prevent accidental switching of digital circuits. In order to achieve it any unconnected inputs called “floating inputs” should be tied to a logic “1” or logic “0” as appropriate for the circuit. We do this by using what are commonly called Pull-up Resistors to give the input pin a defined default state, if there is nothing is connected to it. This can be observed with a voltage level of 3-5V on unconnected digital input.





DI/DO feature configuration

The feature “Digital input/output” allows you to define rules that control the behaviour of digital inputs/outputs on SMSEagle device. User may define several processing rules for both inputs and outputs.

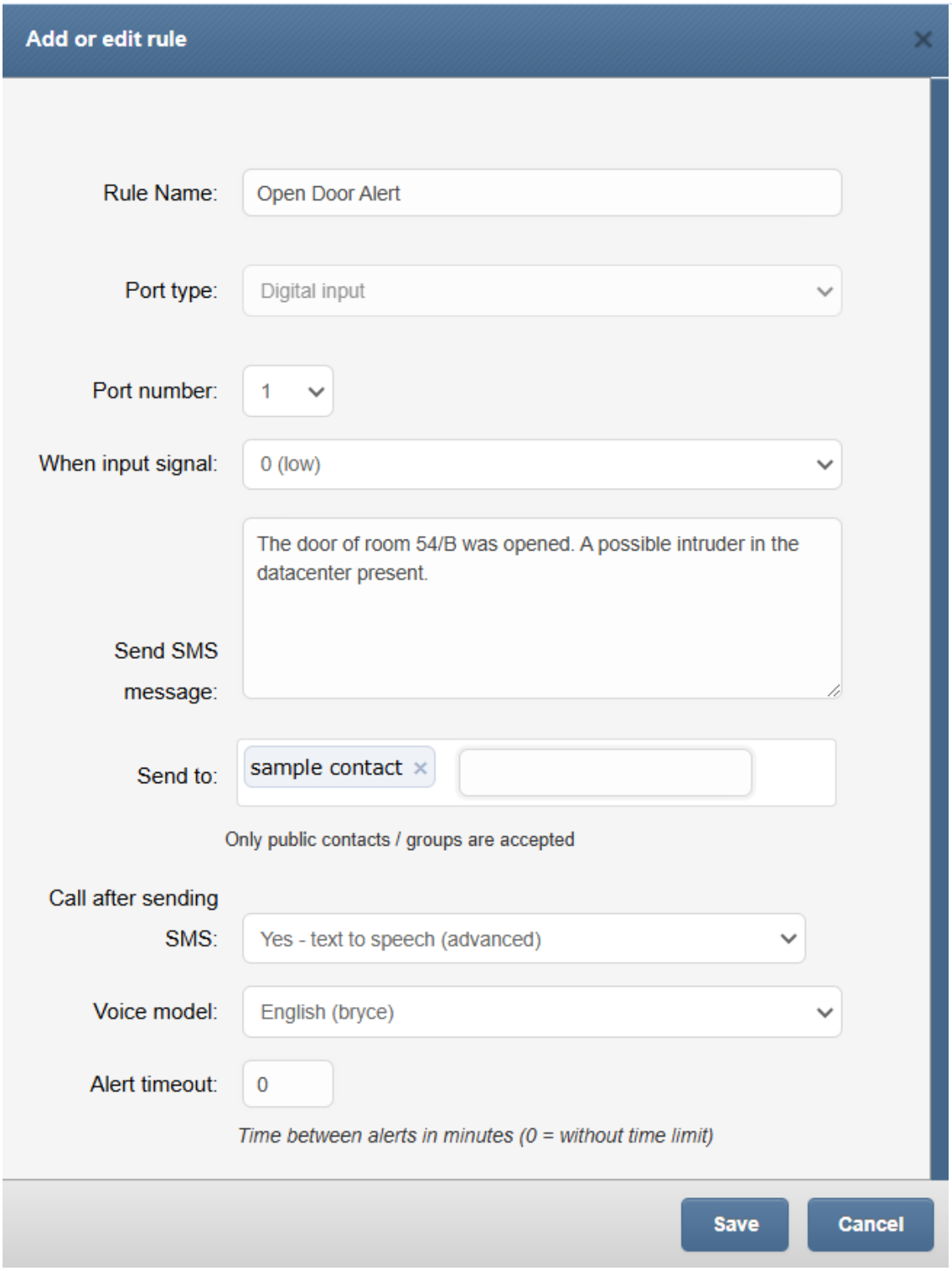


Screenshot from plugin window

Digital inputs

For each processing rule for digital input user can define:

- The rule name
- Port number
- State of input signal that will trigger sending of SMS message (field “When input signal”)
- SMS text (field “Send SMS message”)
- The recipient’s name from phonebook
- Alert timeout. This value defines time between consecutive alerts. If this value is set and input is triggered several times during the timeout, only one alert message will be sent.



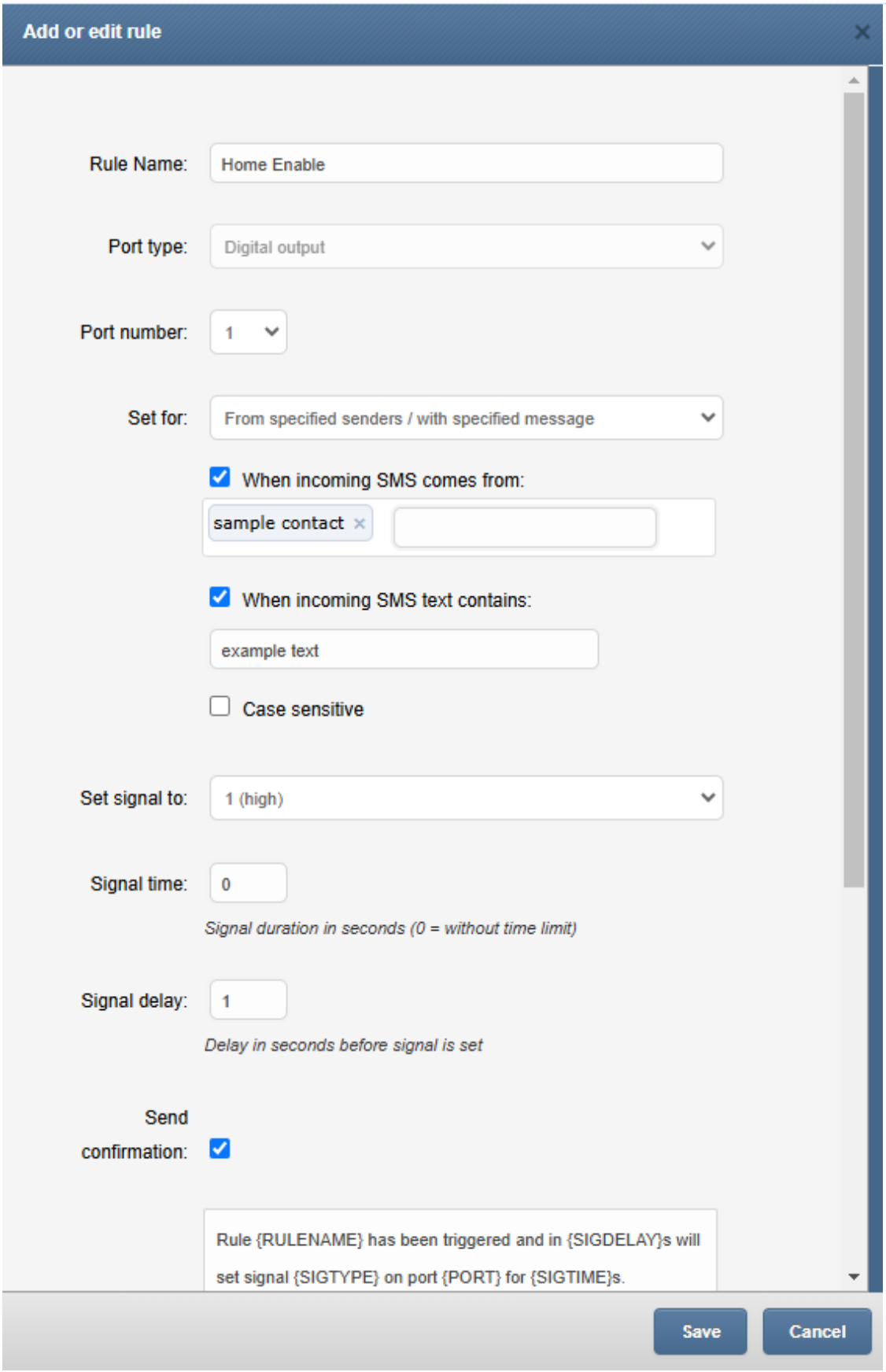
Screenshot from digital input “Add or edit rule” window

Digital outputs

For each processing rule for digital output user can define:

- The rule name
- Port number

- On what condition digital output should be set (all incoming messages, when incoming SMS comes from specified contact in phonebook or when incoming SMS text contains given value)
- State of output signal that will be triggered by incoming SMS message
- Output signal duration in seconds (0 = without time limit)
- Output signal delay before signal is set
- Define outgoing SMS that will be sent after output signal is triggered



Screenshot from digital output “Add or edit rule” window

Voice Call

An SMS message triggered by a digital input/output rule can be optionally followed by a wake-up call or text-to-speech call. This can be enabled in the rule definition. The feature requires a device with an active Voice-Call add-on.

Digital I/O Extender
The Digital I/O Extender is an expansion module designed for SMSEagle NXS and MHD devices. It extends the system's digital input and output capabilities by providing 32 additional configurable digital I/O ports. Each port can be individually configured as either a digital input or digital

output, allowing flexible adaptation to application requirements. The extender module connects to the SMSEagle device via a USB interface.

Once connected:

- Additional DI/DO ports become available in the rule definition (port number selection)
- The same rule logic applies as for built-in ports
- The external I/O device status is visible in menu Settings > Sysinfo

Check the SMSEagle online store or the Sales Partner network for the Digital I/O Extender (P/N: ACCDPIOKIT).

Temperature & humidity sensors

All NXS-family of SMSEagle devices is equipped with **internal** temperature and humidity sensor. The internal sensor allows to measure temperature with ±0.5°C accuracy and humidity with ±2% RH accuracy.

Additionally, NXS-97xx Rev.3 (and higher) devices also support **external** sensors via 1-Wire interface.

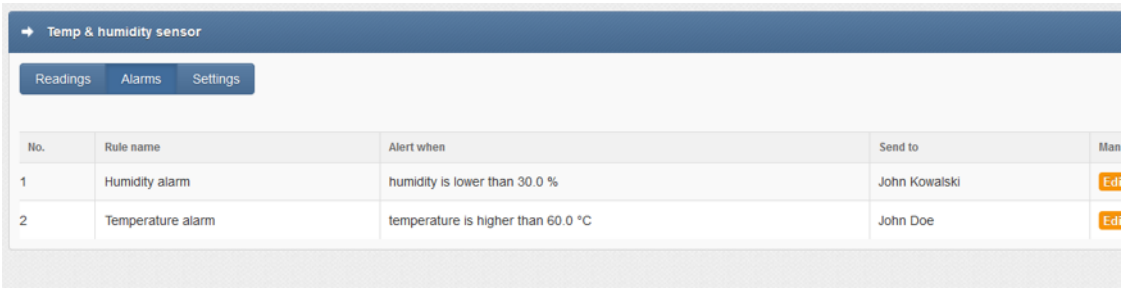
A measured values from sensors can be displayed in web-GUI of SMSEagle and used to trigger SMS message to single/many recipients.



Screenshot from plugin main window

Feature configuration - Alarms

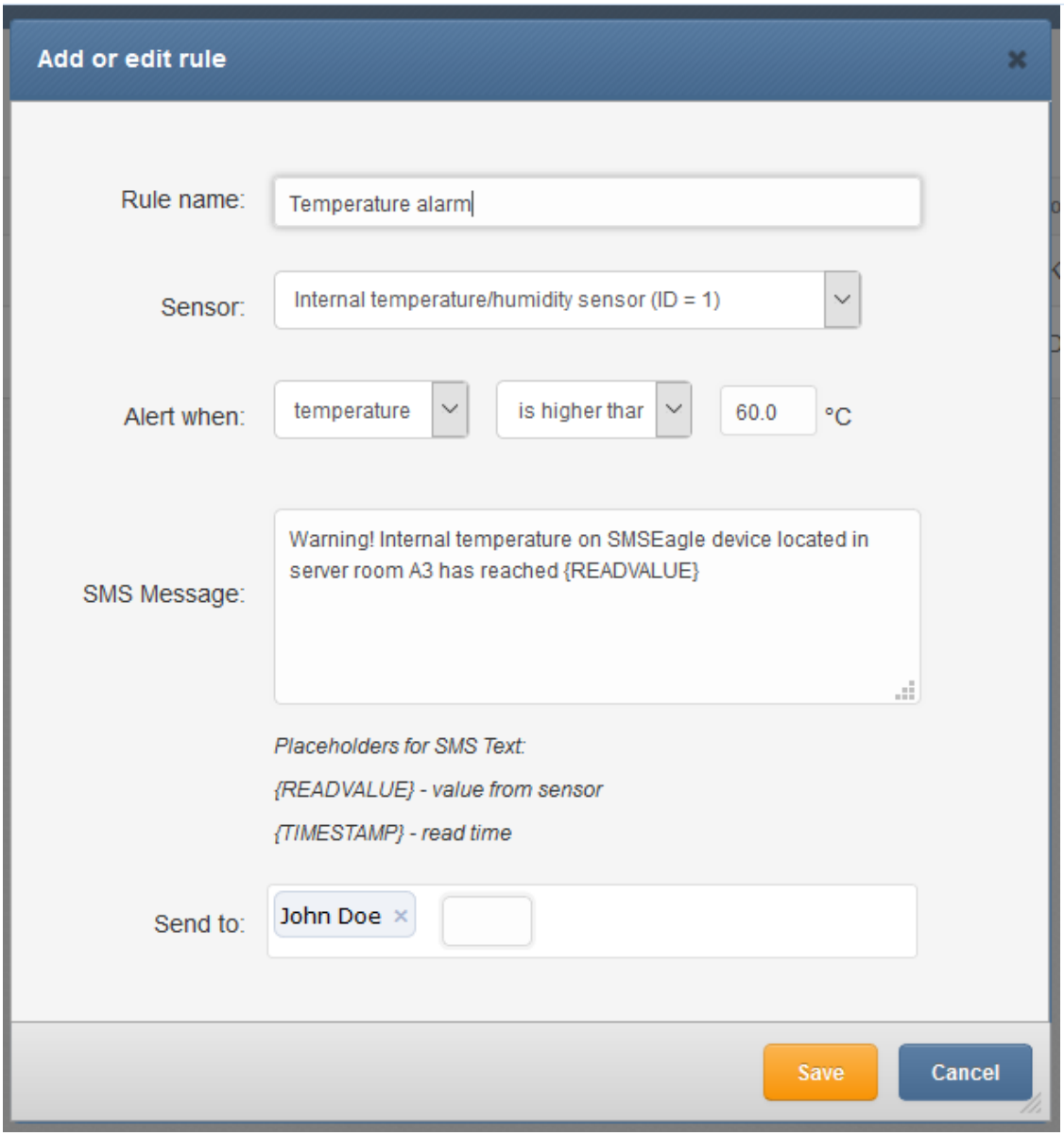
Tab “Alarms” allows to define triggering rules for SMS alarms for temperature and humidity. User may define several processing rules.



Screenshot from “Alarms” window

For each processing rule for digital output user can define:

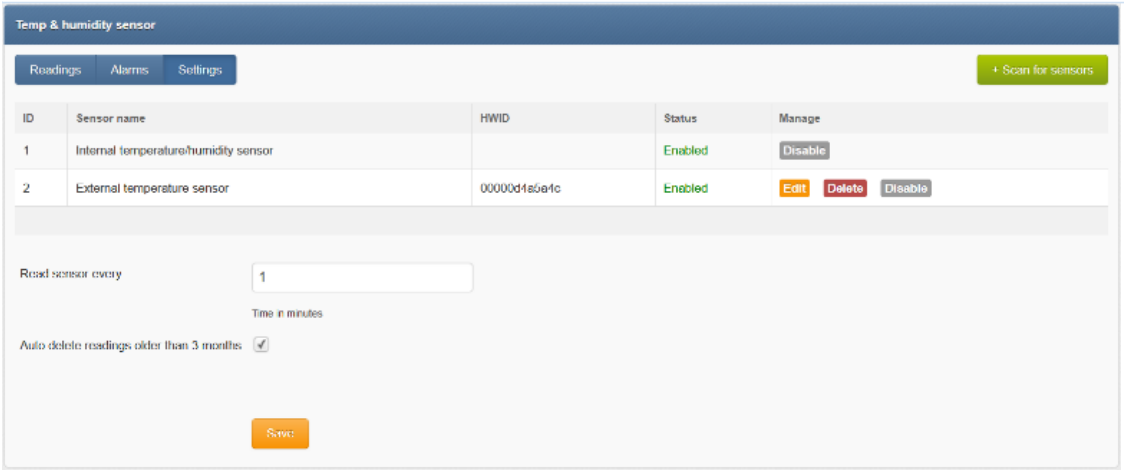
- The rule name
- Sensor (currently only 1 sensor is available)
- On what condition SMS alarm should be sent (temperature/humidity is higher/lower than given value)
- SMS text
- SMS recipient: contact name or group name from Phonebook



Screenshot from “Add or edit rule” window

Feature configuration - settings

Tab “Settings” allows to control sensor settings. User may enable/disable sensor and set sensor reading period (in minutes). If external sensors are supported they can be added and defined here. Temperature scale can be set for Celsius or Fahrenheit.



Screenshot from “Settings” window

Reading Temp/Humidity via SNMP Protocol

Current temperature and humidity values from internal/external sensor can be also read via SNMP protocol. See chapter “**SNMP agent**” for detailed description.

Connecting an External Temperature sensor

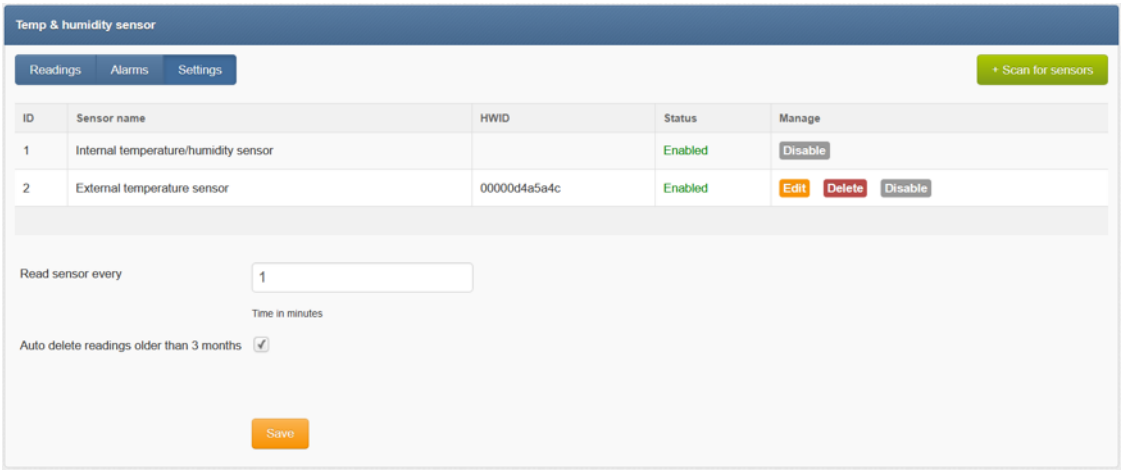
External probes with temperature sensors for SMSEagle NXS-97xx Rev.3 (and higher) devices can be purchased in our online store or via Sales Partner network. The purpose of the probes is to facilitate temperature measurement and SMS alerting via “Temp & humidity” menu in SMSEagle Web-GUI.

The external sensor connects to the device via block connector as follows:

- **Red** wire to (5V)
- **Yellow** wire to (1W)
- **Black** wire to (GND)

Multiple sensors are supported and can be attached in parallel.

Once attached to the device you need to “Scan for sensors” in Temp & Sensors > Settings menu



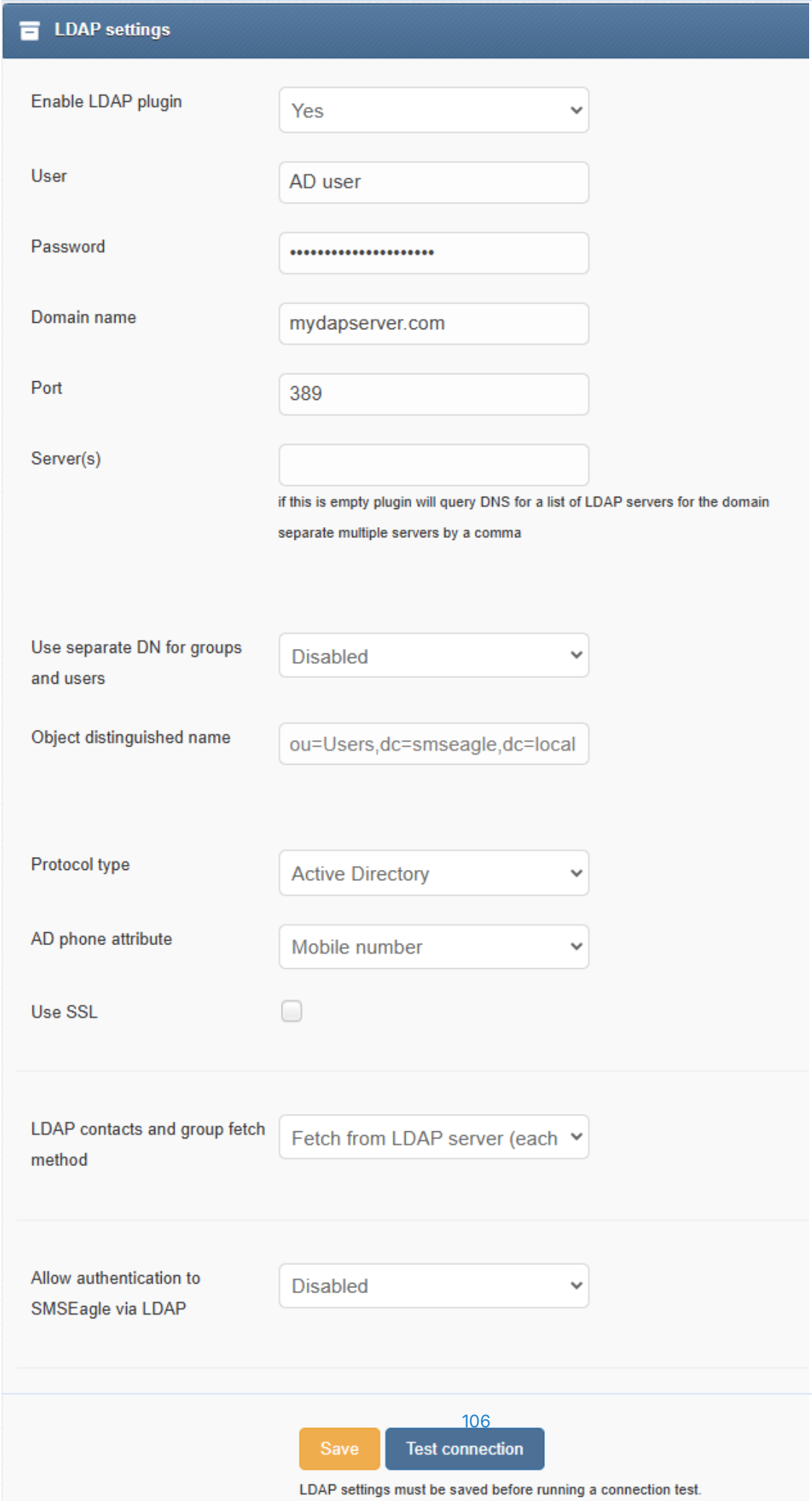
LDAP

The LDAP feature allows to access directory services: Active Directory (hereinafter referred to as “AD”) and OpenLDAP. The plugin allows reading directory contacts and groups in SMSEagle web-GUI. Optionally, it allows to authenticate to SMSEagle device using directory services.

Feature configuration

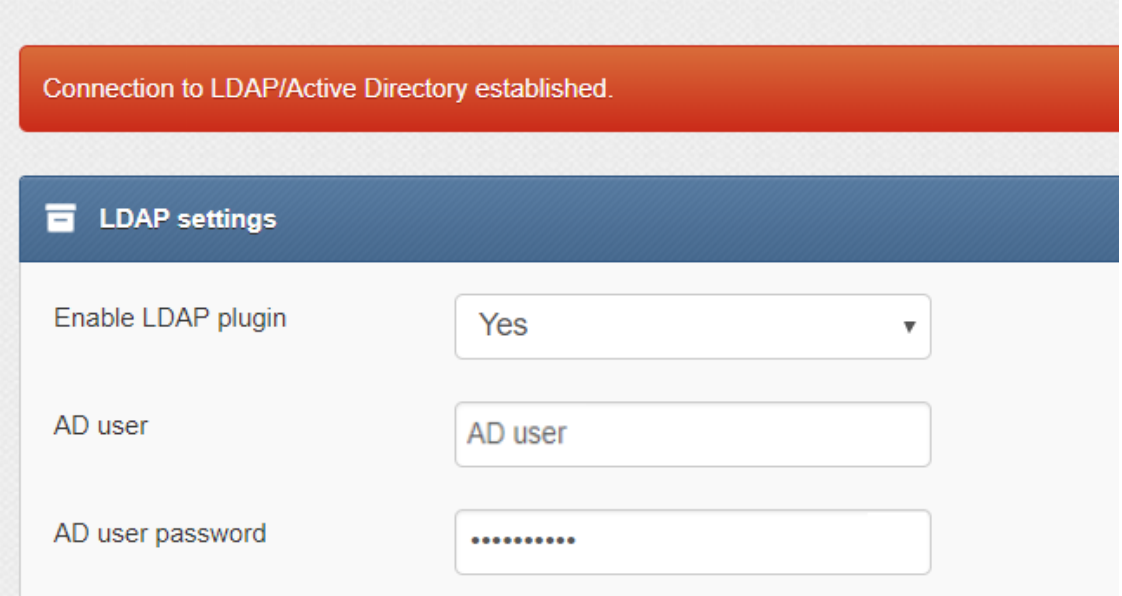
Choose “LDAP” from left side menu in SMSEagle web-GUI to access plugin configuration. After enabling the plugin, user needs to fill in all requested fields according to AD settings.

In the “AD phone attribute” field user needs to choose which phone attribute from AD will be shown in SMSEagle web-GUI.


LDAP settings
Enable LDAP plugin
Yes
User
AD user
Password
Domain name
mydapserver.com
Port
389
Server(s)
if this is empty plugin will query DNS for a list of LDAP servers for the domain
separate multiple servers by a comma
Use separate DN for groups and users
Disabled
Object distinguished name
ou=Users,dc=smseagle,dc=local
Protocol type
Active Directory
AD phone attribute
Mobile number
Use SSL
LDAP contacts and group fetch method
Fetch from LDAP server (each
Allow authentication to SMSEagle via LDAP
Disabled
Save
Test connection
LDAP settings must be saved before running a connection test.

Screenshot from “LDAP settings” window

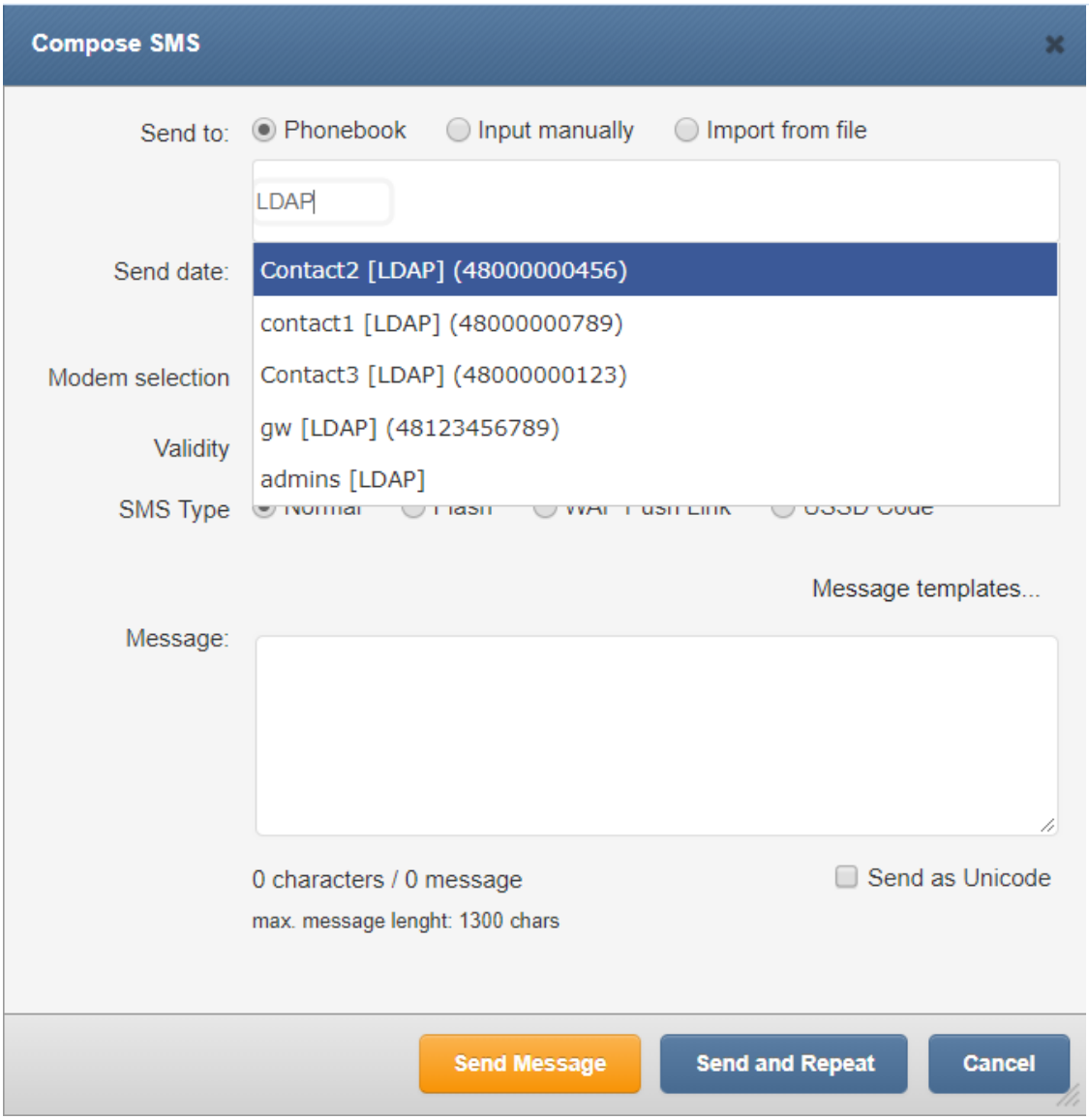
Click “Save” and “Test connection” to make sure that SMSEagle is connected with AD server.



Screenshot showing successful connection to AD server.

With connection established, AD contacts/groups suggestions are shown in selected modules of Web-GUI. Start typing any part of contact/group name or number to show AD contact suggestions.

Type “LDAP” (case sensitive) to check all contacts listed in AD directory.



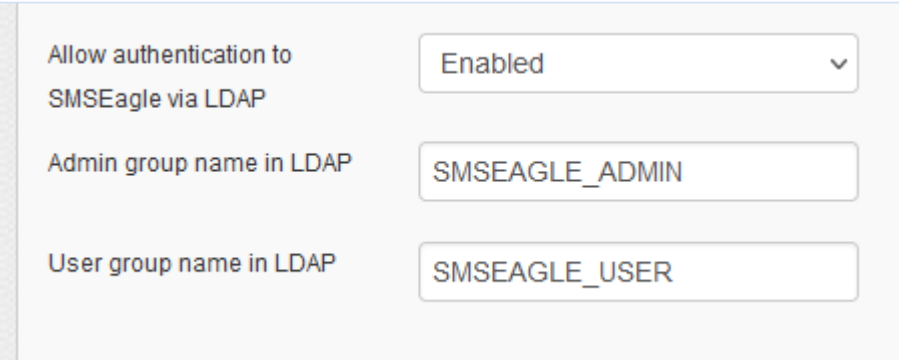
Screenshot from “Compose” module with LDAP connection enabled

LDAP directory suggestions can be used in “Compose”, “Autoreply”, “Digital input/output”, “Email To SMS” and “Email To SMS Poller” modules.

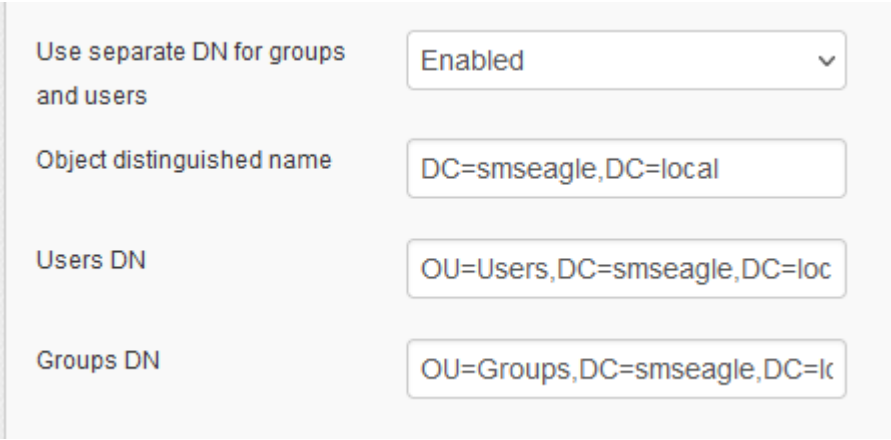
Authentication to SMSEagle via LDAP (optional)

This feature allows authentication to your SMSEagle device using LDAP. To start using it:

- create in your directory services a new group for SMSEagle admin role. Enter the created group name in SMSEagle web GUI > LDAP > “Admin group name in LDAP”
- create in your directory services a new group for SMSEagle user role. Enter the created group name in SMSEagle web GUI > LDAP > “User group name in LDAP”
- Set parameter “Allow authentication to SMSEagle via LDAP” to “Enable”
- press “Save” button”

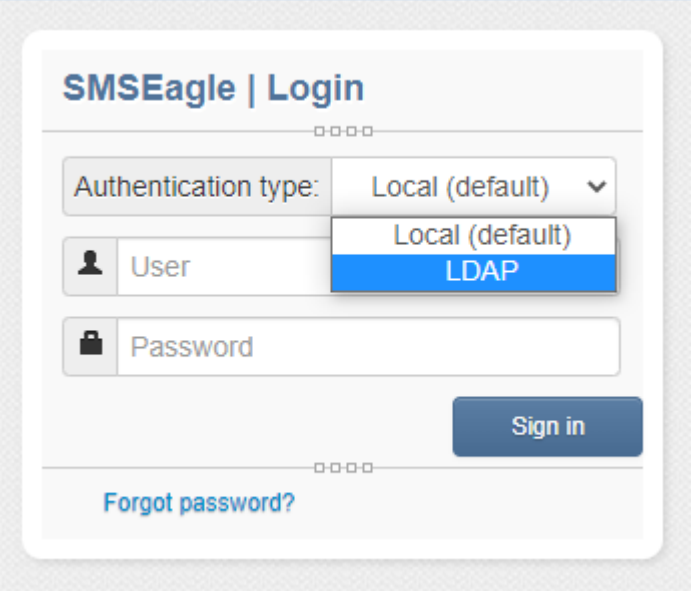


Depending on the directory structure of your LDAP server, for OpenLDAP you may also need to specify separate Distinguished Names for Users and Groups (if both are located under different paths):



On the login screen user will be able to choose between “Local” or “LDAP” authentication.
Use one of these parameters as your user in SMSEagle login form:

- Common Name
- givenName
- sAMAccountName
- displayName
- userPrincipalName



During first login using LDAP authentication type, the system will create a new user on SMSEagle device, linked to the LDAP account. This account settings will be synchronized with LDAP during every login.

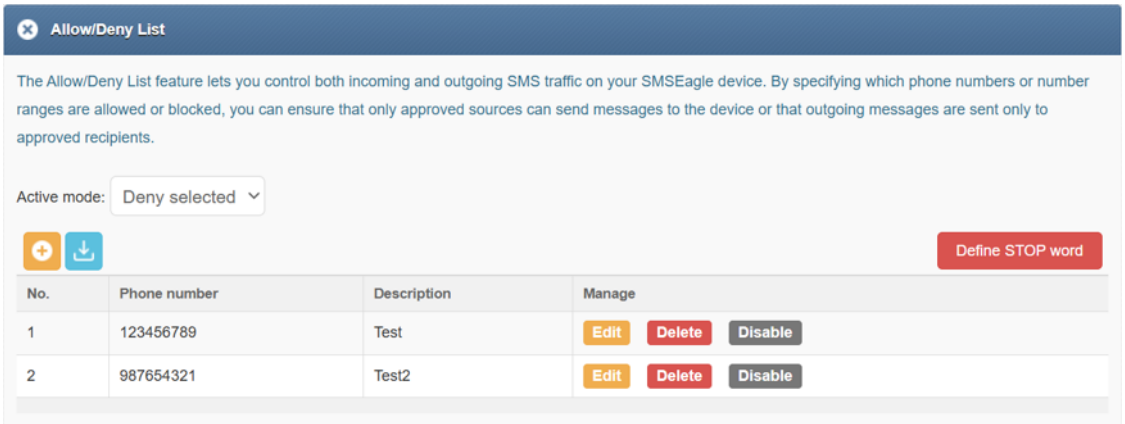
Allow/Deny List

The Allow/Deny List feature lets you control both incoming and outgoing SMS traffic on your SMSEagle device. By specifying which phone numbers or number ranges are allowed or blocked, you can ensure that only approved sources can send messages to the device or that outgoing messages are sent only to approved recipients.

The Allow/Deny List operates in one of two mutually exclusive modes:

- **Allow selected**
- **Deny selected**

Only one mode can be active at a time.



Screenshot from “Allow/Deny List” feature

Mode: Allow selected

In Allow selected mode, only phone numbers or number ranges explicitly defined on the list are permitted. All other numbers are automatically blocked.

Behavior:

- Incoming SMS

Only messages sent from numbers listed in the Allow List are accepted. Messages from all other numbers are rejected.

- Outgoing SMS
  The device can send messages only to numbers listed in the Allow List. Attempts to send messages to other numbers are blocked.

Typical use cases

- Restricting communication to a known set of trusted numbers
- Limiting outbound traffic to approved recipients only
- Creating a closed SMS environment for integrations, automation, or testing

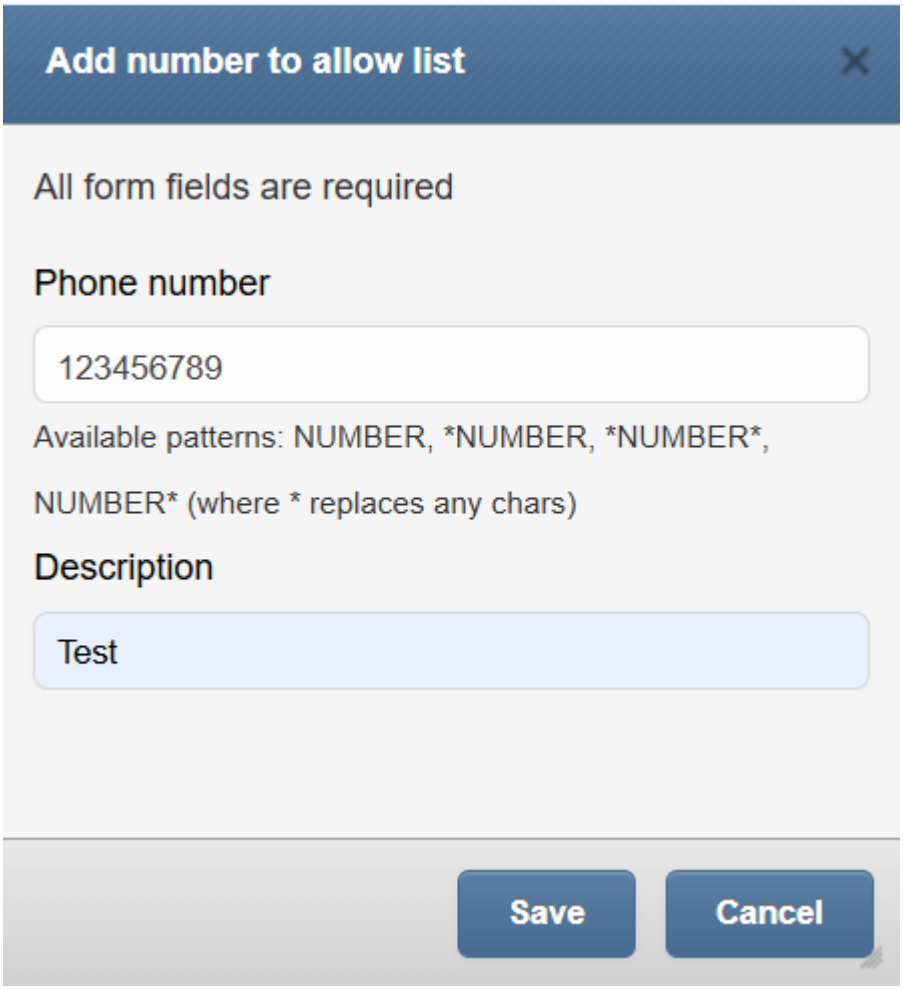
Example

If the list contains:

- +48123456789
- +4420*

Then:

- SMS traffic is allowed **only** to and from that specific number +48123456789 and all UK numbers starting with +4420
- Any SMS involving other numbers is blocked



Screenshot from “Add number to allow list” window

Mode: Deny selected

In Deny selected mode, all phone numbers are permitted by default, except those explicitly defined on the list.

Behavior:

- Incoming SMS
  Messages from numbers listed in the Deny List are blocked. Messages from all other numbers are accepted.
- Outgoing SMS
  The device cannot send messages to numbers listed in the Deny List, but can send messages to all other numbers.

Typical use cases:

- Blocking unwanted or abusive senders
- Preventing SMS delivery to specific destinations or number ranges
- Replacing traditional blacklist-style filtering with unified inbound and outbound control

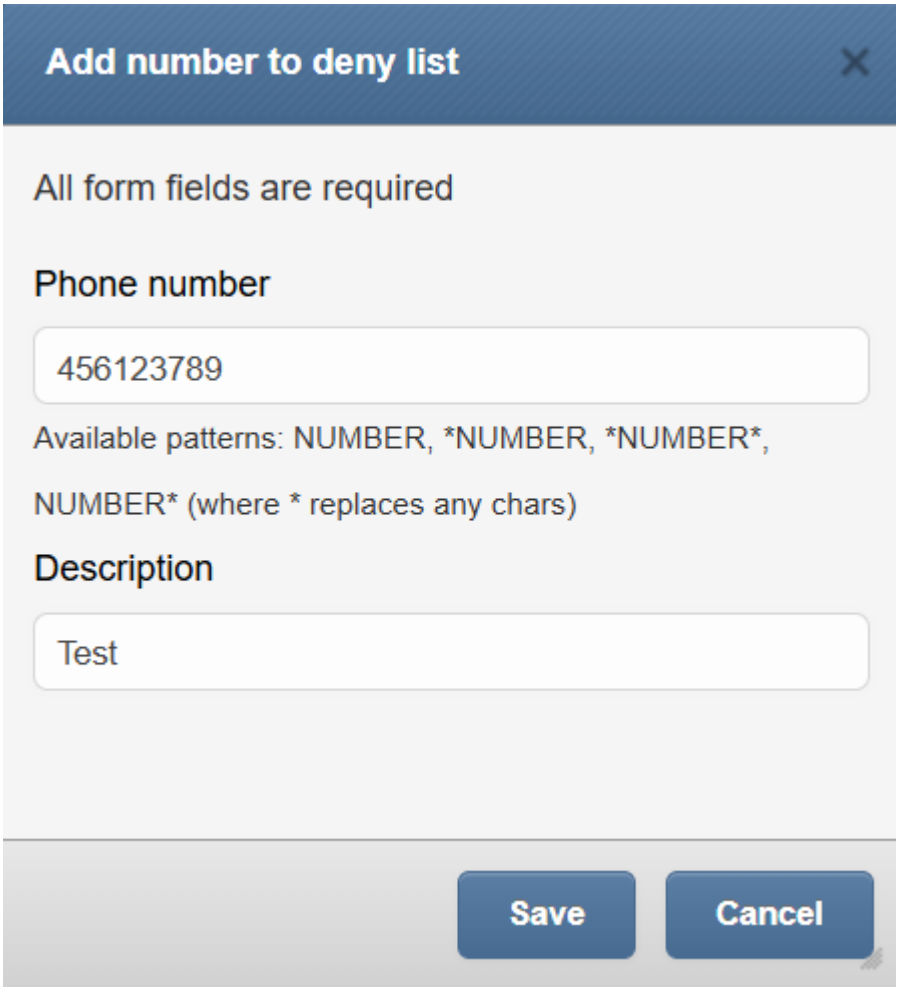
Example

If the list contains:

- +1555000000
- +31*

Then:

- Messages to or from those numbers are blocked
- All other SMS traffic is allowed



Screenshot from “Add number to deny list” window

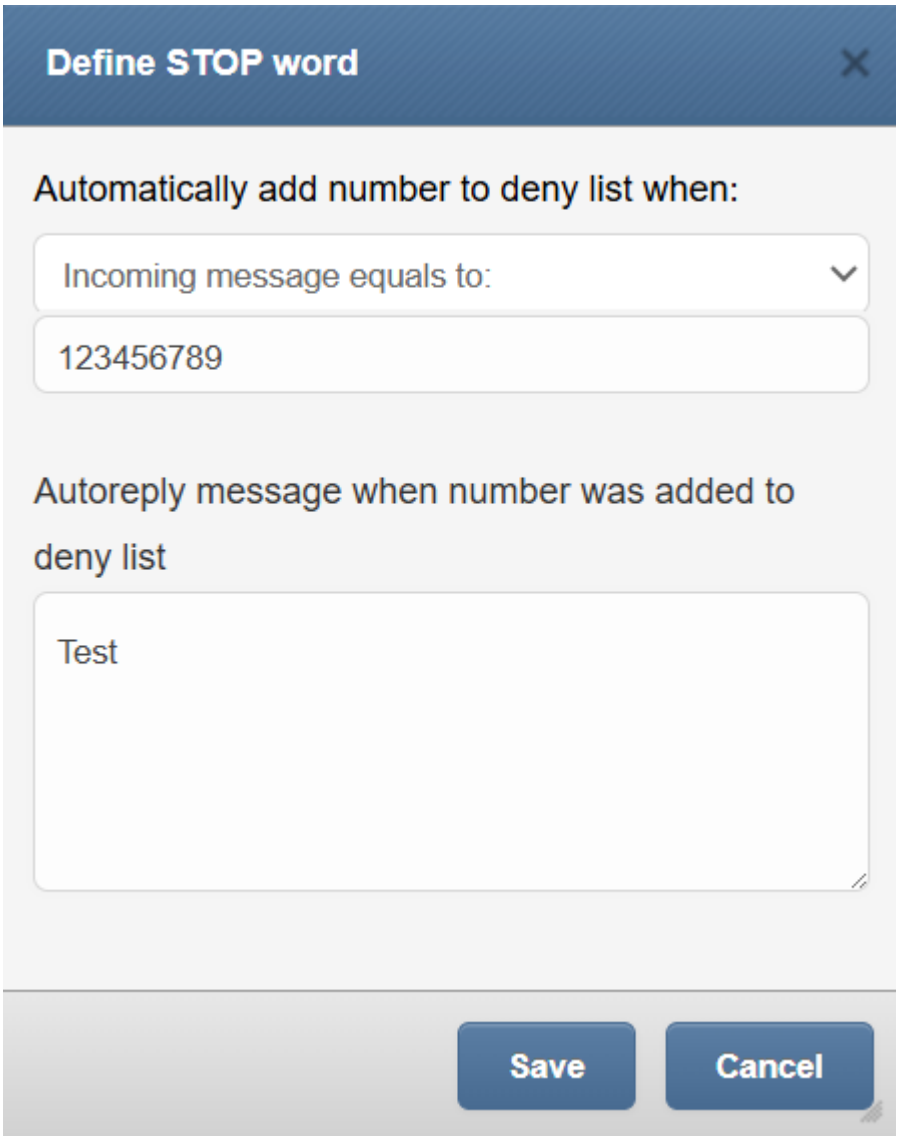
Stop word

The STOP Word feature provides an automated way to block unwanted SMS senders based on message content. When a STOP word is defined, the SMSEagle device monitors incoming SMS messages for this keyword. If an incoming message contains the defined STOP word, the sender’s phone number is automatically added to the Deny list. As a result, any further incoming or outgoing SMS communication with that number is blocked according to the Deny selected mode rules.

This feature is especially useful for:

- Automatically handling opt-out or unsubscribe requests

- Blocking senders who respond with predefined keywords (e.g. STOP, UNSUBSCRIBE)
- Reducing manual administration of blocked numbers



Screenshot from “Define STOP Word” window

Notes:

- The Allow/Deny List applies globally to SMS traffic on the device.
- Phone numbers can be defined as single numbers or number ranges using wildcards. The following wildcards may be used for multiple numbers: *NUMBER, *NUMBER*, NUMBER* (where * replaces any chars)

SMPP

(available on NXS Rev. 3 and Rev. 4 devices)

Short Message Peer-to-Peer (SMPP) is a protocol used in the telecommunications industry. It is an open, industry standard protocol designed to provide a data communication interface for the transfer of short message data between External Short Messaging Entities (ESMEs) and SMSCs.

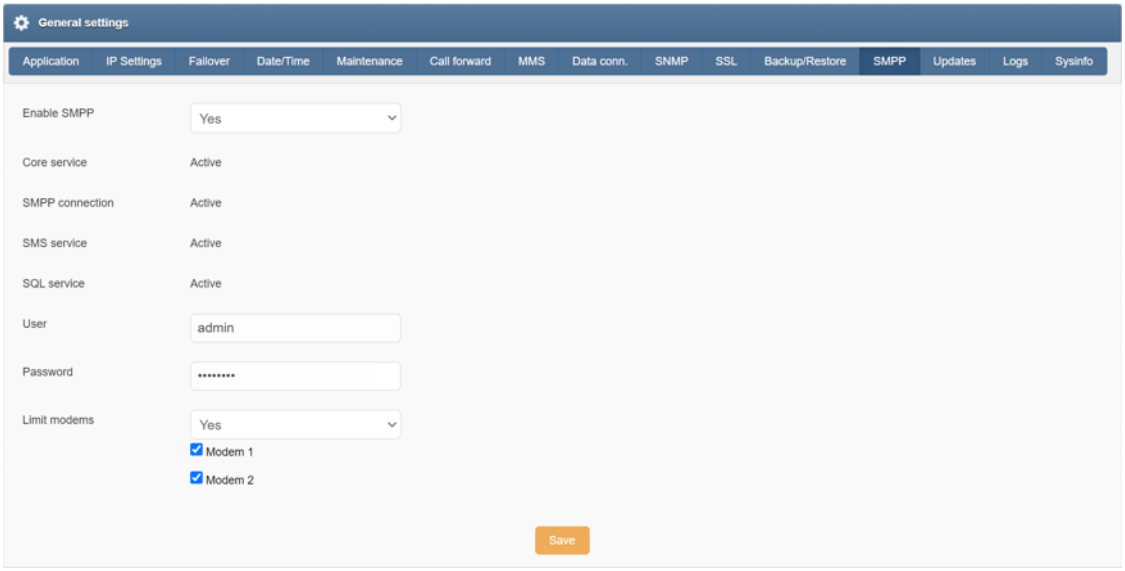
The SMPP protocol is often used to allow third parties to send messages to SMS gateways for further processing.

The SMSEagle device is equipped with an embedded SMPP server. It supports SMPP in the following scenarios:

- Receive SMS requests via SMPP and send messages to the carrier via SIM and radio module
- Receive incoming SMS from cellular carrier via radio-module with SIM and forward SMS to SMPP client

Within the SMPP feature it is possible to:

1. sending SMS text messages (max. 1300 characters)
2. receiving delivery reports
3. specifying the encoding of the message (7bit ASCII or UTF-8 is supported)
4. receiving incoming messages and forwarding them to the SMPP client
5. select modems that are used for sending/receiving SMS (only for multimodem devices)



Screenshot from menu Settings > SMPP.

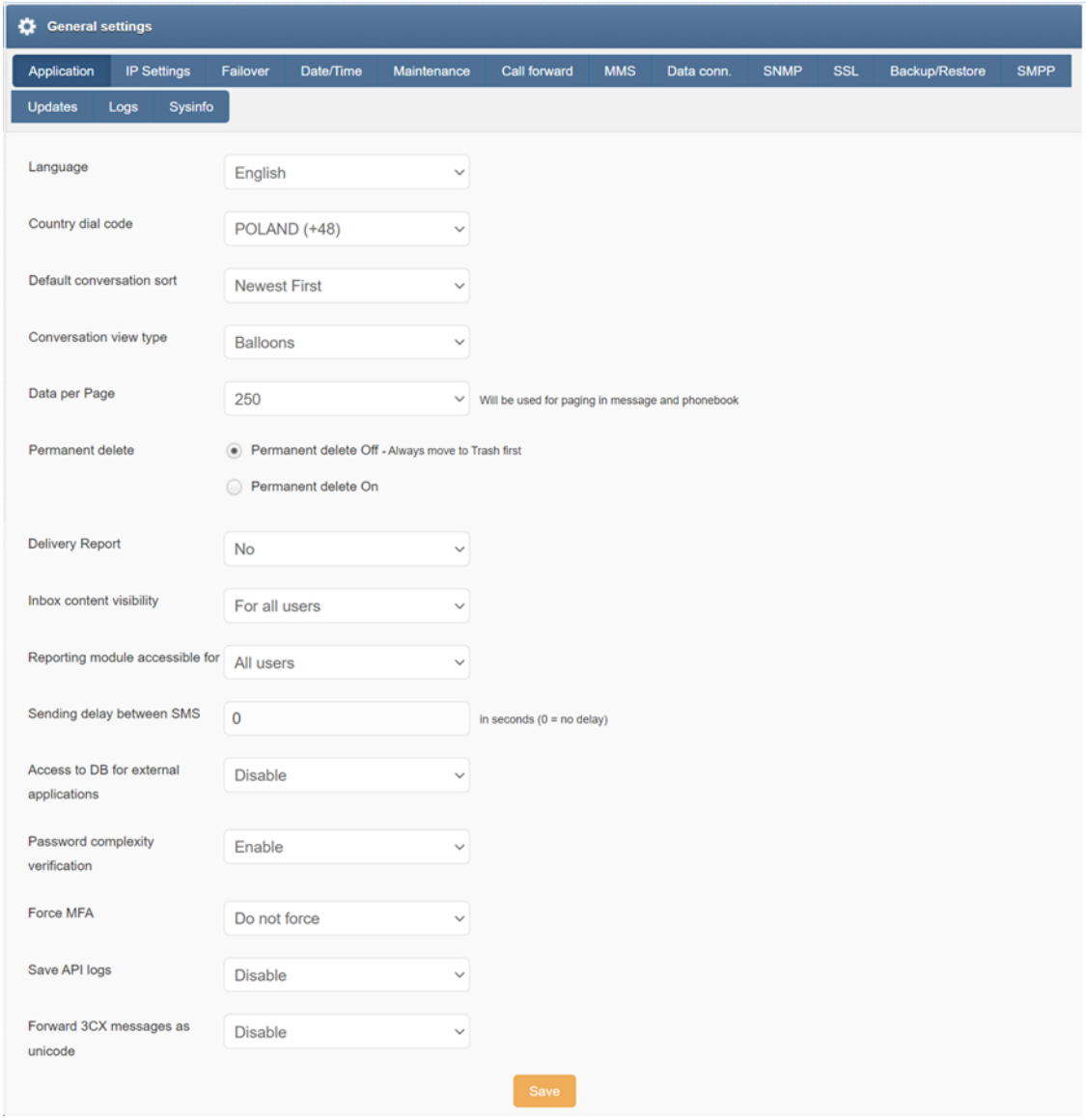
The SMPP server supports SMPP version 3.4.

Settings

Settings menu is divided into several tabs for easier maintenance.

Application Settings

Application settings can be changed under the Settings Tab > Application.

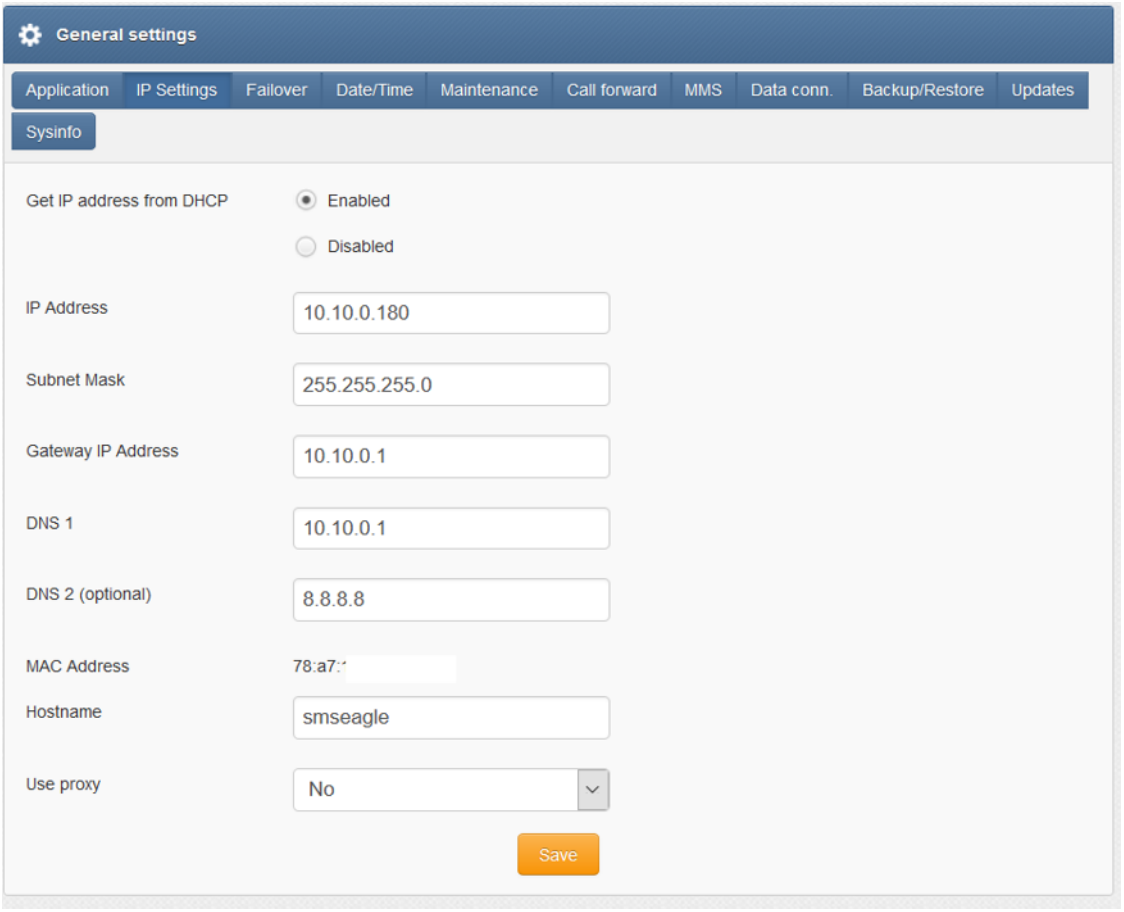


- You can change the language of the application to English, French, German, Polish and Spanish
- You can change the country dial code to your country (this setting affects only correct assignment of phone numbers to phonebook entries)
- You can sort the conversation to show messages either “Newest First” or “Oldest First”
- You can change the conversation view to either “Table” (tabular view) or “Balloons” (smartphone-like view), as shown in Folders chapter
- You can adjust the amount of data displayed on one page to 10, 15, 20, 25, 50, 100, 250 or Show all
- You can set for the messages to be permanently deleted or be moved to Trash first
- You can set the receiving of delivery reports to Yes, No or Default (network carrier setting)
- You can set the visibility of the Inbox content to All users, Only admins or Only from assigned modems
- You can set access of the reporting module to All users or Only admins

- You can set a delay between SMS sending in seconds (this setting may be useful for cases where cellular operator blocks a number due to intensive traffic. Note: setting delay between SMS sending also introduces a delay time between receiving SMS)
- You can enable or disable access to database for external applications
- You can enable/disable Password complexity verification. When enabled user password must be at least 8 characters long and include at least one lowercase letter, uppercase letter, number and special character
- You can enable to force MFA (Multifactor Authentication) for user role: for all users, only new users, or leave users to choose their MFA settings (disable force)

IP Settings

IP settings can be changed under the Settings tab > IP Settings.



- You can enable or disable Get IP address from DHCP
- You can input the IP address
- You can input the Subnet Mast
- You can set the Gateway IP Address
- You can set DNS 1
- You can optionally set DNS 2
- You can view the MAC address of your device

- You can input Hostname
- You can choose to Use proxy

Allow/Deny Rules For Ip Addresses

The IP Settings tab includes an option to define access control rules based on IP addresses. Administrators can create an allow list (whitelist) or deny list (blacklist) of IP addresses or ranges that are permitted or blocked from accessing the SMSEagle web GUI and API. This feature helps to restrict device access to trusted network segments only. Separate multiple addresses with a comma.

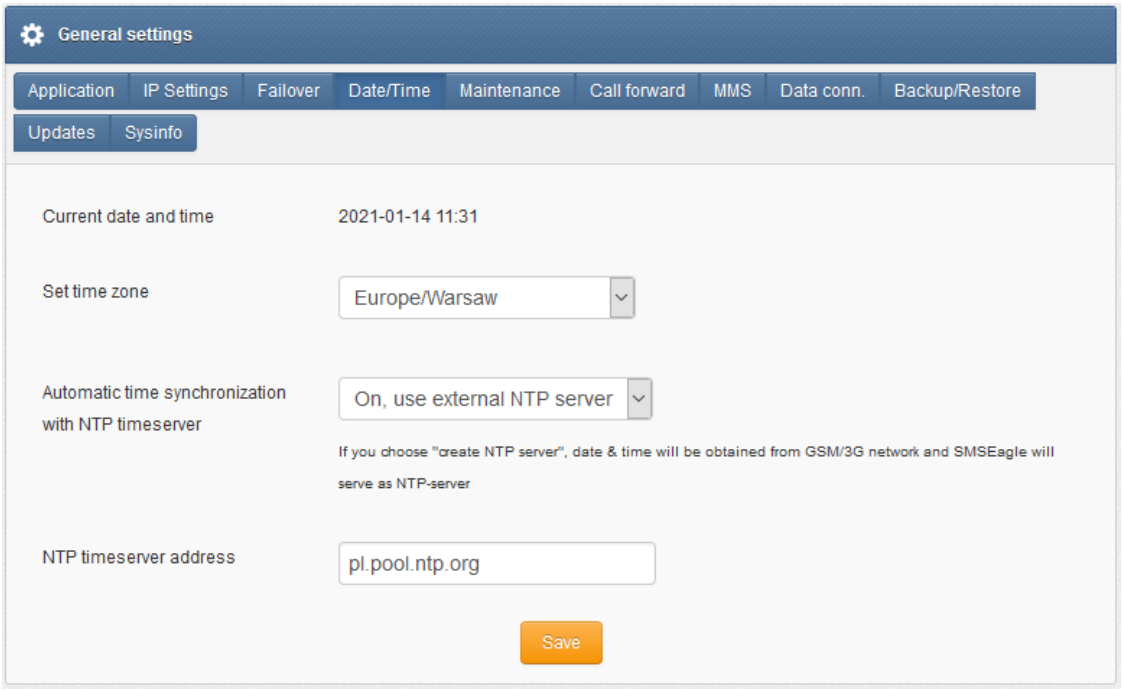
Notice: With the settings all ports are blocked except 22.

Failover

Failover configuration has been described in chapter "**Failover (HA-cluster) feature**".

Date/Time

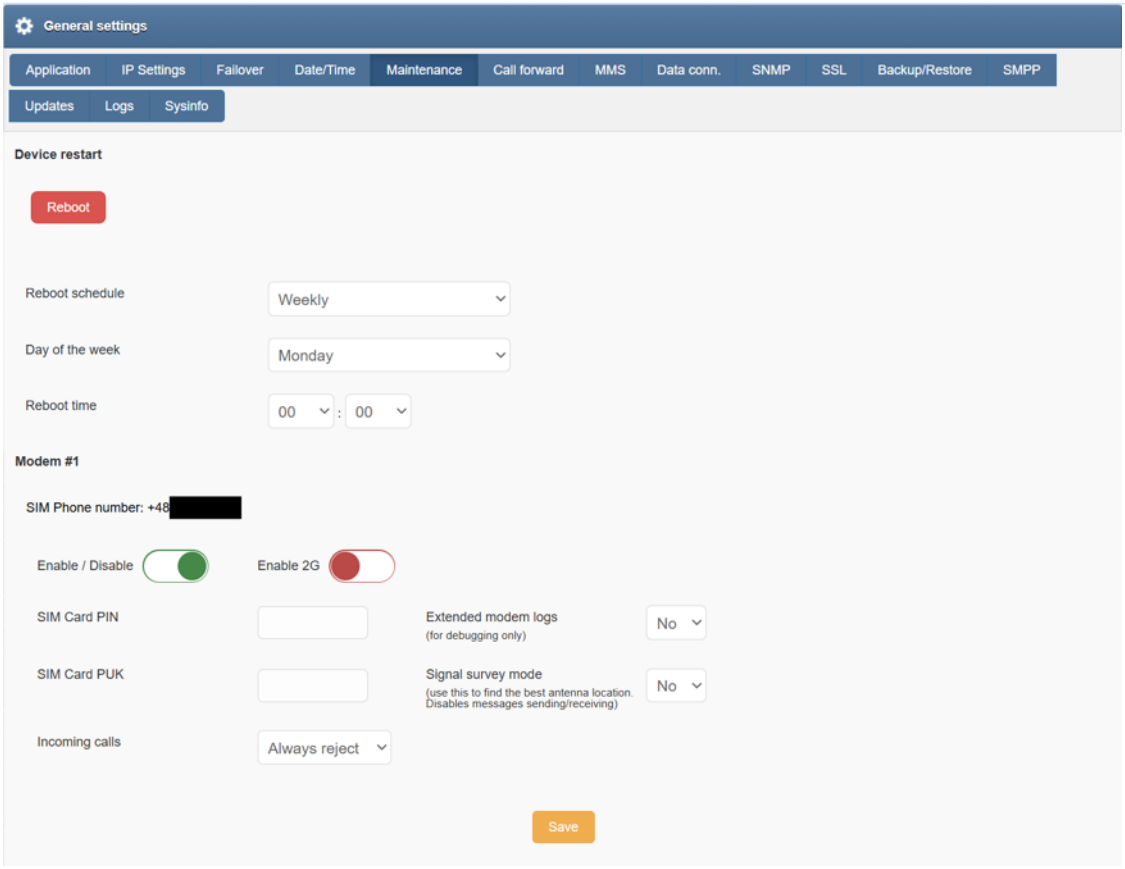
Date/Time settings can be changed under the Settings Tab > Date/Time



- You can check current device date and time
- You can set your time zone
- You can set automatic time synchronization with NTP timeserver, disable automatic time synchronization or create NTP server on SMSEagle device (date & time will be obtained from 3G/4G network)
- You can set NTP timeserver address (or several addresses separated with comma)

Maintenance

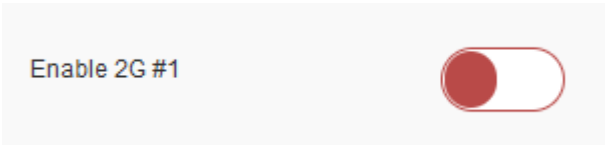
Maintenance settings can be accessed under the Settings tab > Maintenance



- You can reboot your device
- You can enable or disable the device modem
- You can input your SIM card PIN
- You can input your SIM card PUK
- You can enable extended modem logs (for debugging purposes)
- You can enable signal survey mode (for finding the best antenna location)
- You can set incoming call to always reject, accept or ignore

Multi-modem settings are described in chapter Multimodem features.

Enable 2G Connectivity



For hardware Rev.4 devices there is additional option which allows to enable 2G network connectivity. 2G is disabled by default, and should be only enabled for devices located in areas where there are connectivity problems with 4G/3G cellular networks.

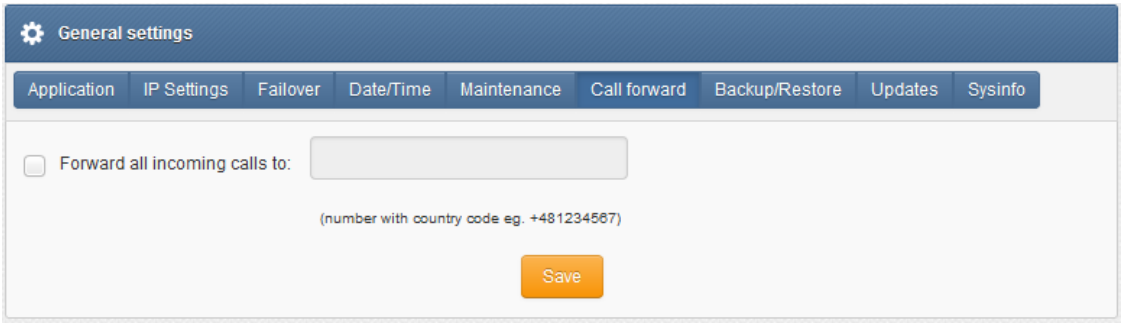
Signal survey mode

This feature allows you to find the best location of the antenna for environments with poor cellular signal strength. When enabled, signal strength value on SMSEagle dashboard will refresh every 3s. This allows you to try different locations of the antenna and find a spot with the best signal.

WARNING: when Signal survey mode is enabled you cannot send/receive messages on the device.

Call Forward

Call forward settings can be accessed under the Settings tab > Call forward.

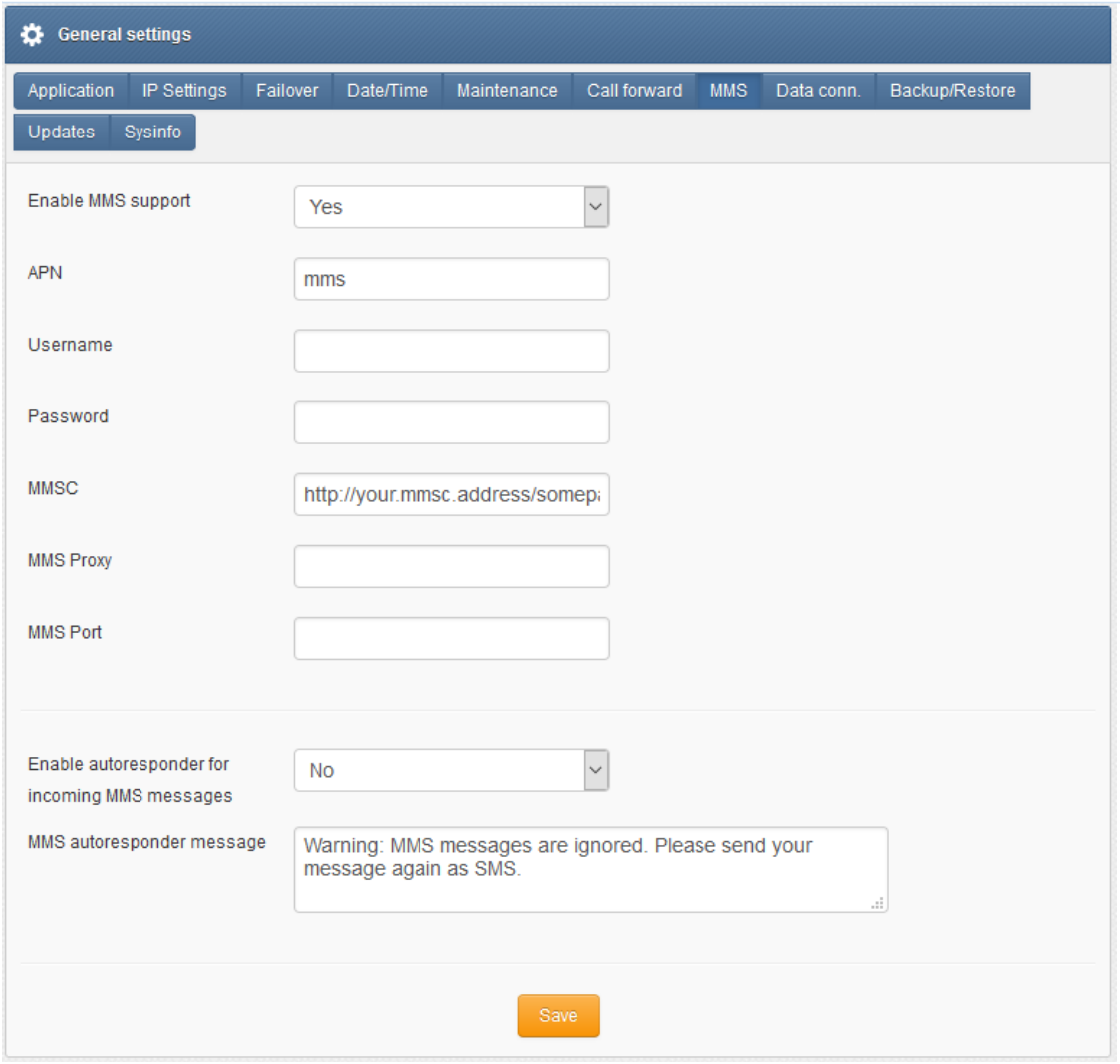


- You can choose to forward all incoming calls to a chosen number

Important Notice: This feature is not available in NXS-97xx-4G Rev.3 devices.

MMS

MMS Settings can be accessed under the Settings tab > MMS.



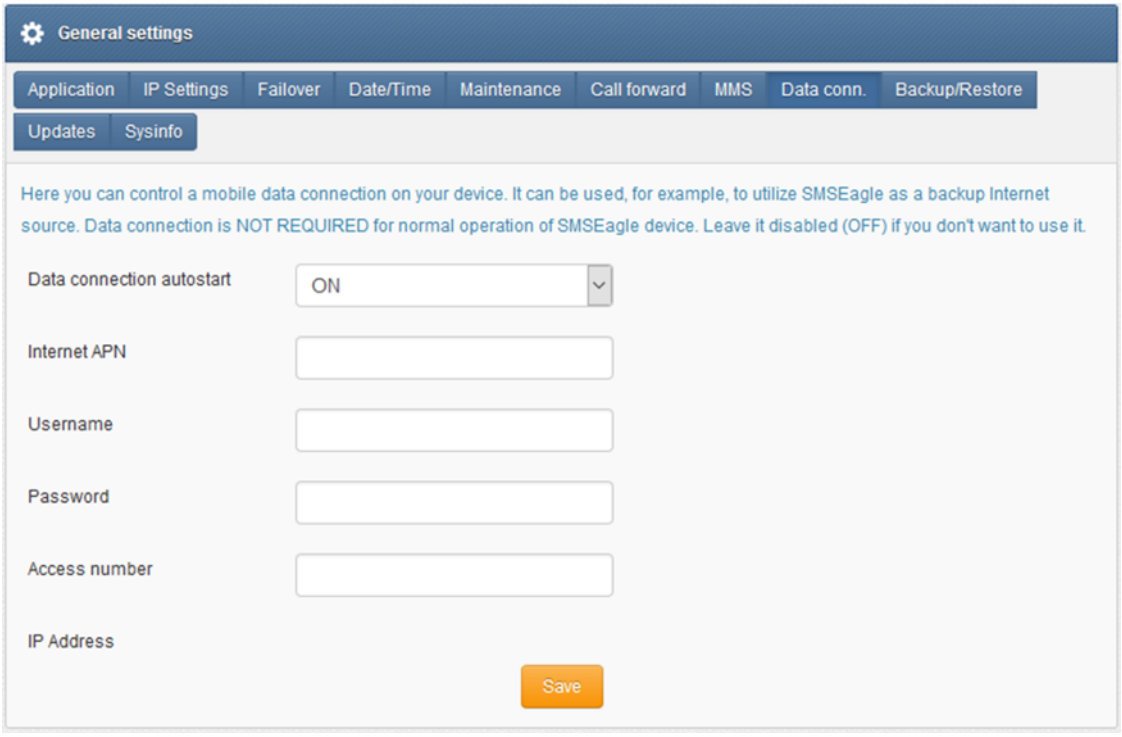
- You can enable MMS support
- You can set APN value
- You can input APN username
- You can input APN password
- You can set MMSC
- You can set MMS Proxy
- You can set MMS Port
- You can set autoresponder for incoming MMS messages
- You can input MMS autoresponder message

You can load the default values for your SIM carrier using "Read APN Settings" button or enter values found on the website of your SIM operator.

Data Connection

Data connection settings can be accessed under the Settings tab > Data conn.

Here you can control a mobile data connection on your device. It can be used, for example, to utilize SMSEagle as a backup Internet source. **Data connection is NOT REQUIRED for normal operation** of SMSEagle device. Leave it disabled (OFF) if you don't want to use it.

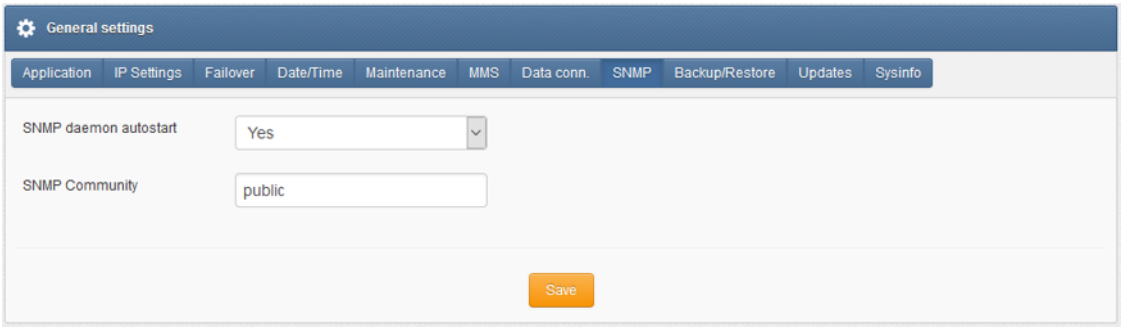


- You can choose to autorestart data connection
- You can input Internet APN
- You can input APN username
- You can input APN password
- You can input access number
- You can view the IP address of your device

You can load the default values for your SIM carrier using "Read APN Settings" button or enter values found on the website of your SIM operator.

SNMP

SNMP Settings can be accessed under the Settings tab > SNMP



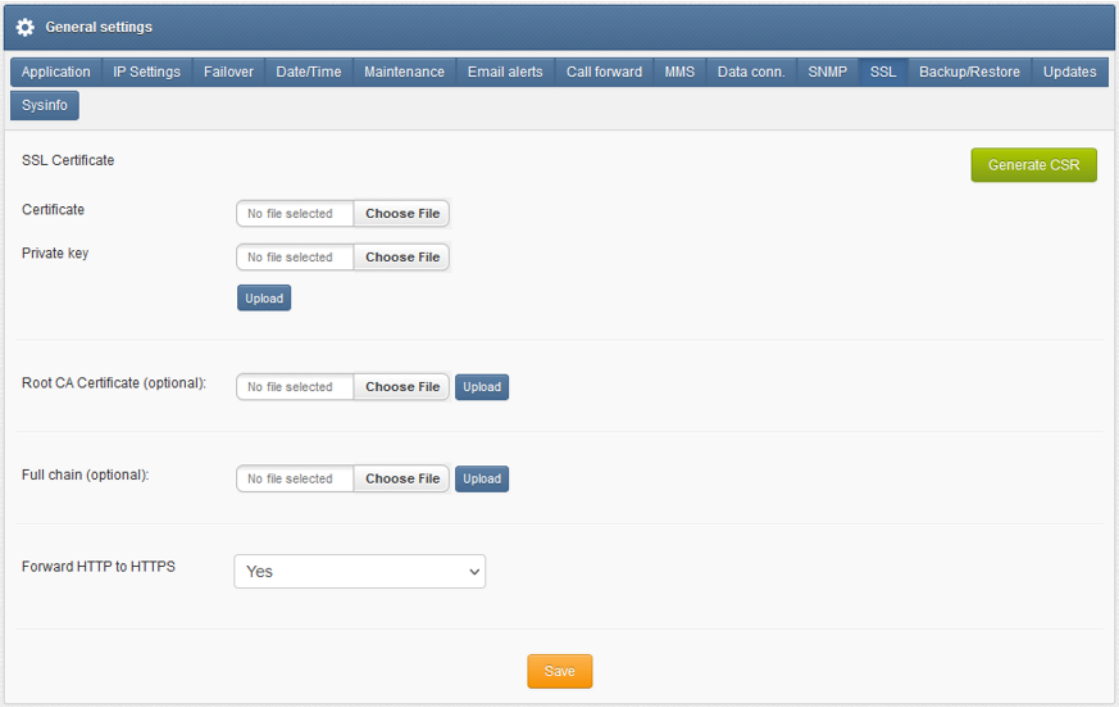
- You can enable/disable SNMP daemon

- You can set your SNMP community name (custom value)

SNMP deamon is required only when you want to monitor your device from external monitoring solutions like Network Monitoring Systems, etc. You can read more about custom SNMP metrics available on SMSEagle device in SNMP agent chapter.

SSL Certificate and HTTPS Redirection

SSL settings can be accessed under the Settings tab > SSL. The settings allows you to upload an SSL certificate to your device and forward HTTP to HTTPS traffic.



**

SSL Certificate**

BY default, SMSEagle device is equipped with a self-signed SSL certificate. If you want to install your own certificate on the device, please obtain a valid certificate file issued by a Certificate Authority. To upload the certificate, please provide the certificate file and private key in PEM format. The certificate cannot be password protected.

Notice: If you want to use Let's encrypt certificate, please follow this guide in our knowledgebase.

Root CA & Full chain (optional)

If you need to add root CA or full chain certificate, you may upload them using "Root CA Certificate" and "Full chain" controls.

Forward HTTP to HTTPS

For optimal security, we recommend using HTTPS-only connections with your SMSEagle. You may easily forward HTTP to HTTPS traffic by setting "Forward HTTP to HTTPS" to "Yes".

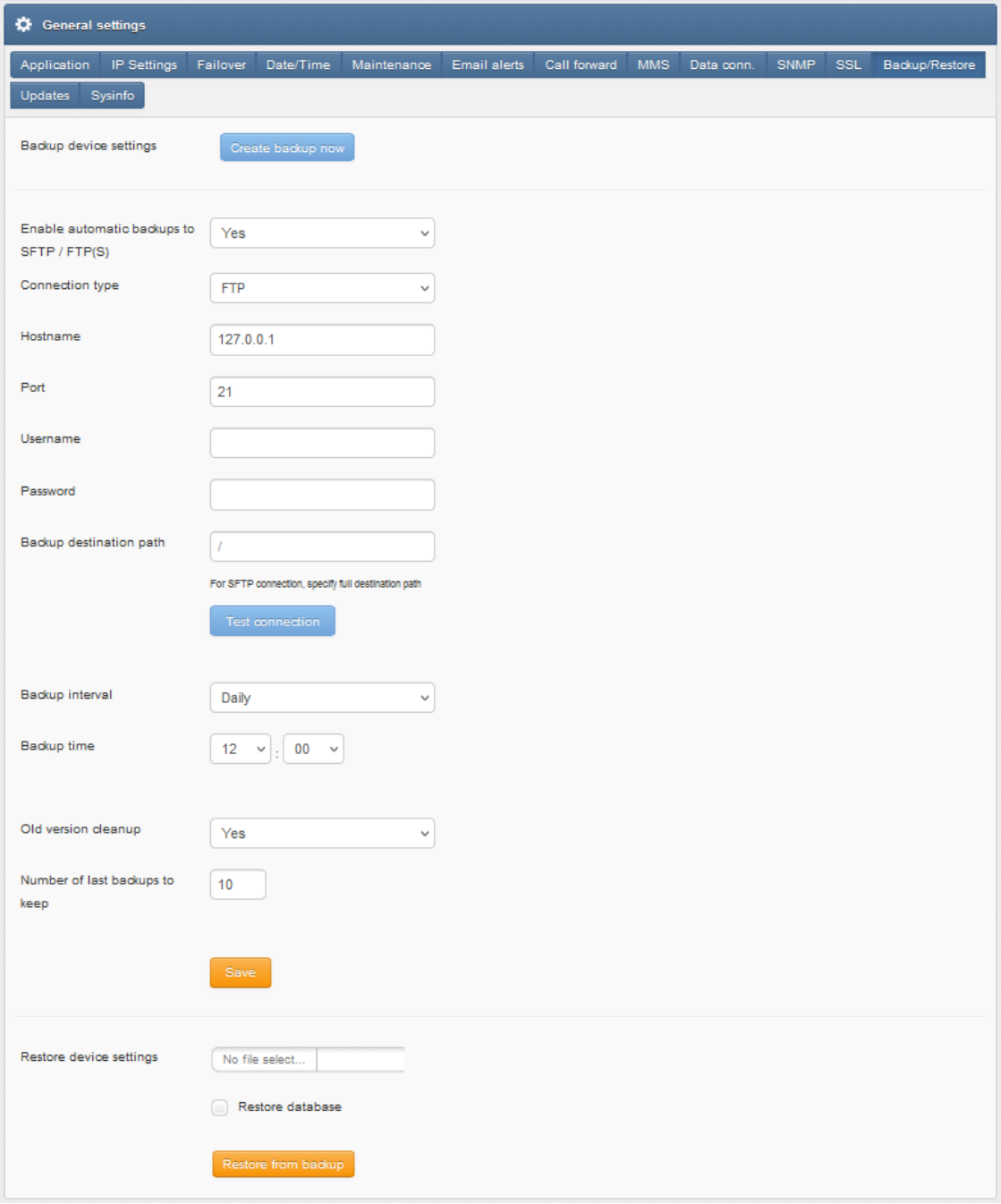
Generate CSR

This feature simplifies a process of obtaining SSL certificate. It creates two files:

- CSR file (Certificate Signing Request). It is needed in a SSL certification procedure. It is a file containing an encrypted text generated by the server on which the certificate is to run. It contains information that will be used in the certificate, such as: name of the organization, domain name, city, country. It also contains public key that is used to encrypt transmitted information.
- Private key. CSR file private key (decryption key) must be kept for exclusive information of the certificate owner. This file should be uploaded together with SSL certificate.

Backup/Restore

Backup and restore settings can be accessed under the Settings tab > Backup/Restore



- You can create a backup of your device settings
- You can enable automatic backup to SFTP/FTP(S)
    - You can set automatic backup interval (daily/weekly/monthly) and time
    - You can select how many backups to keep (delete backups)
- You can restore device settings form a previously saved file
- You can choose to additionally restore the database

WARNING Restore backup settings only works with the same version of device and software

Updates

Update settings can be accessed under the menu Settings > Updates tab.

SMSEagle software is under process of continual improvement. We listen to our customers, and new releases are based on our customer's inputs/requests. Software updates are released frequently, and offer access to new features and fixes to reported issues. Web-GUI offers you a possibility to automatically check for new software updates. This can be done in two ways:

Manual check

In order to manually check for available software updates, go to menu Settings > tab Updates. Click on the button "**Check for software update now**". At the top pops up a balloon in red with information if it is up-to-date.

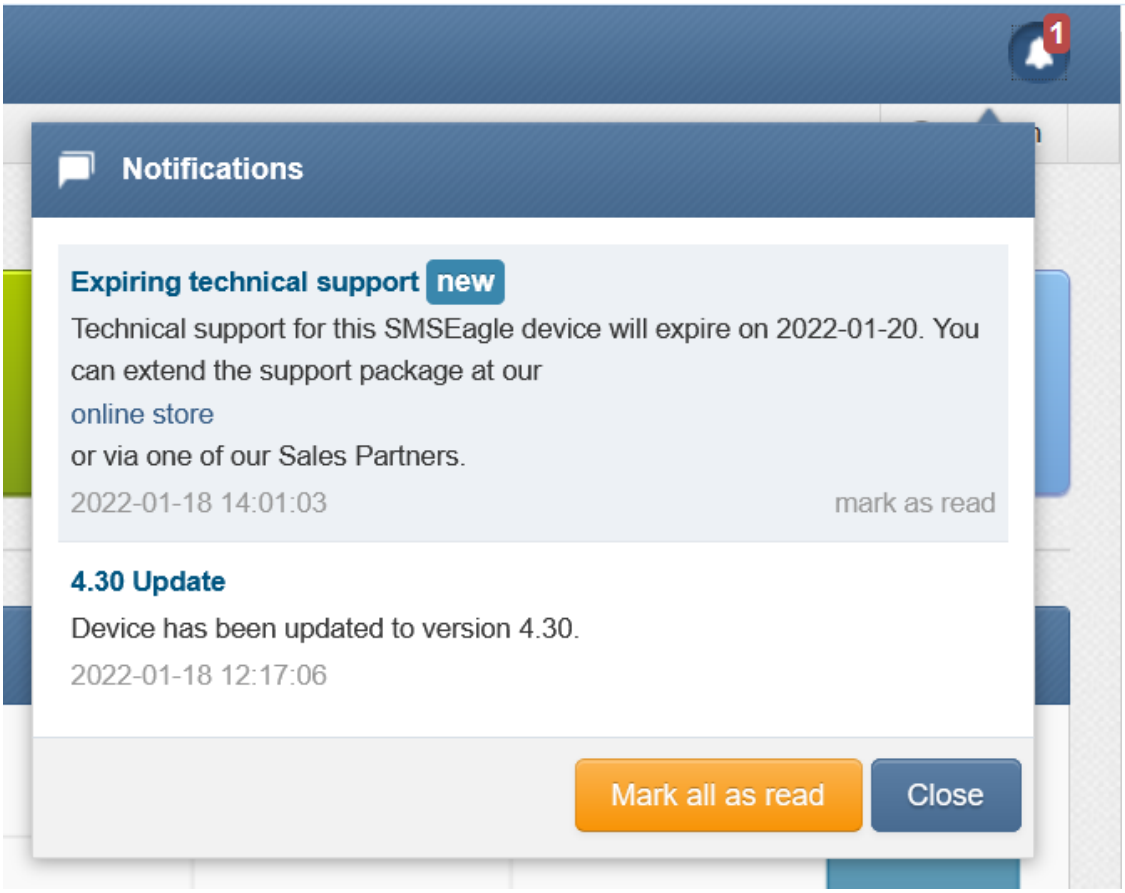
Automatic check

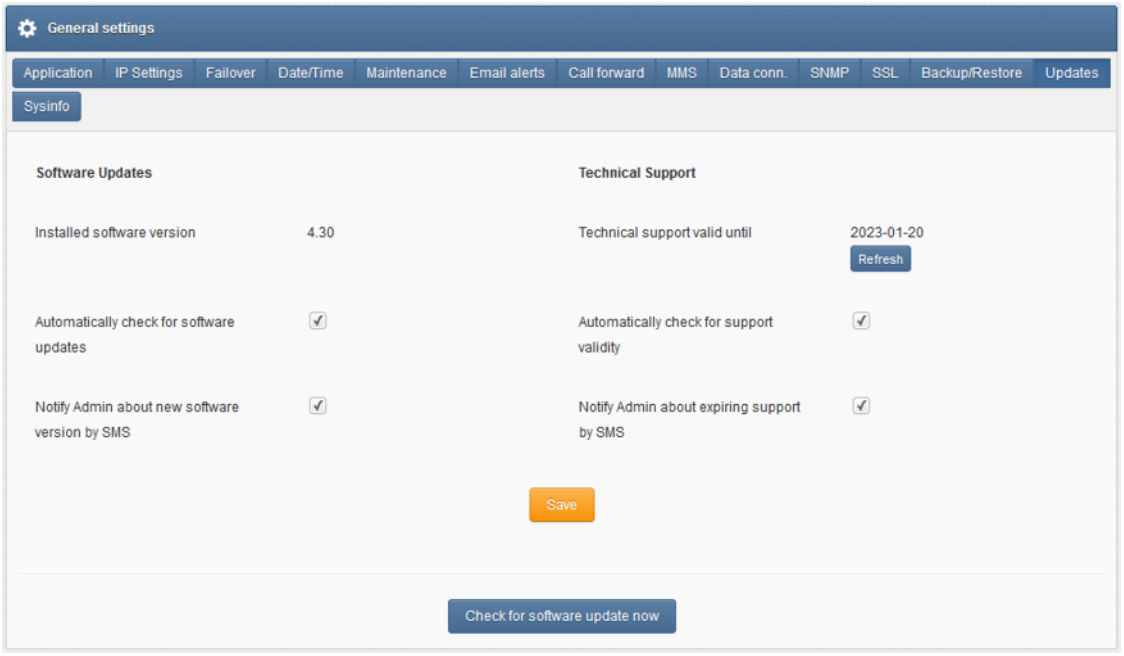
In order to start automatic checks for software updates go to menu Settings > tab Updates, and check the option "Automatically check for software updates". This will enable periodic checks (once a month) for available software updates. If a new update is available, a message "Update Available" will appear in menu Settings> Sysinfo – next to the current software version number.

If you select "Notify Admin about new software version by SMS", the device will additionally send SMS to the default admin account (if the phone number is entered in the account) with a notification about new software update.

Expiring Technical support Notification

Similar to automatic software update checks, mechanism for technical support validity provides information about the technical support expiry date. A month before expiration of a support package your device will notify you about the upcoming expiration date and conveniently provide a link to our online store and sales partners where you can renew your package.





Screenshot from “General Settings-Updates”

Notice: Your SMSEagle device must have a HTTPS connectivity with address updates.smseagle.eu in order for this feature to work.

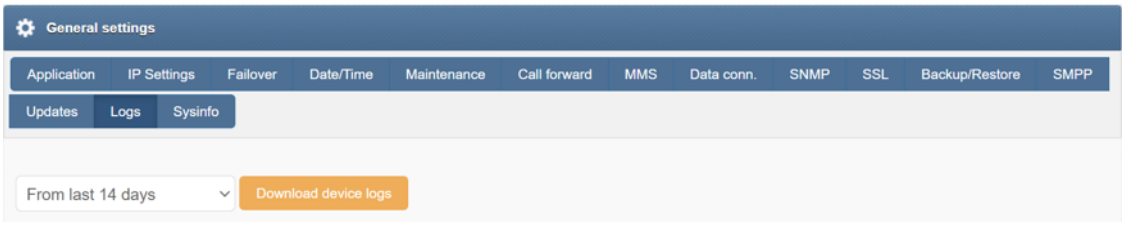
Logs

Available in menu Settings > Logs section presents a visual representation of the most important device logs.

The following device logs are available via web-GUI:

1. Modem log
2. Database log
3. System log
4. Application log

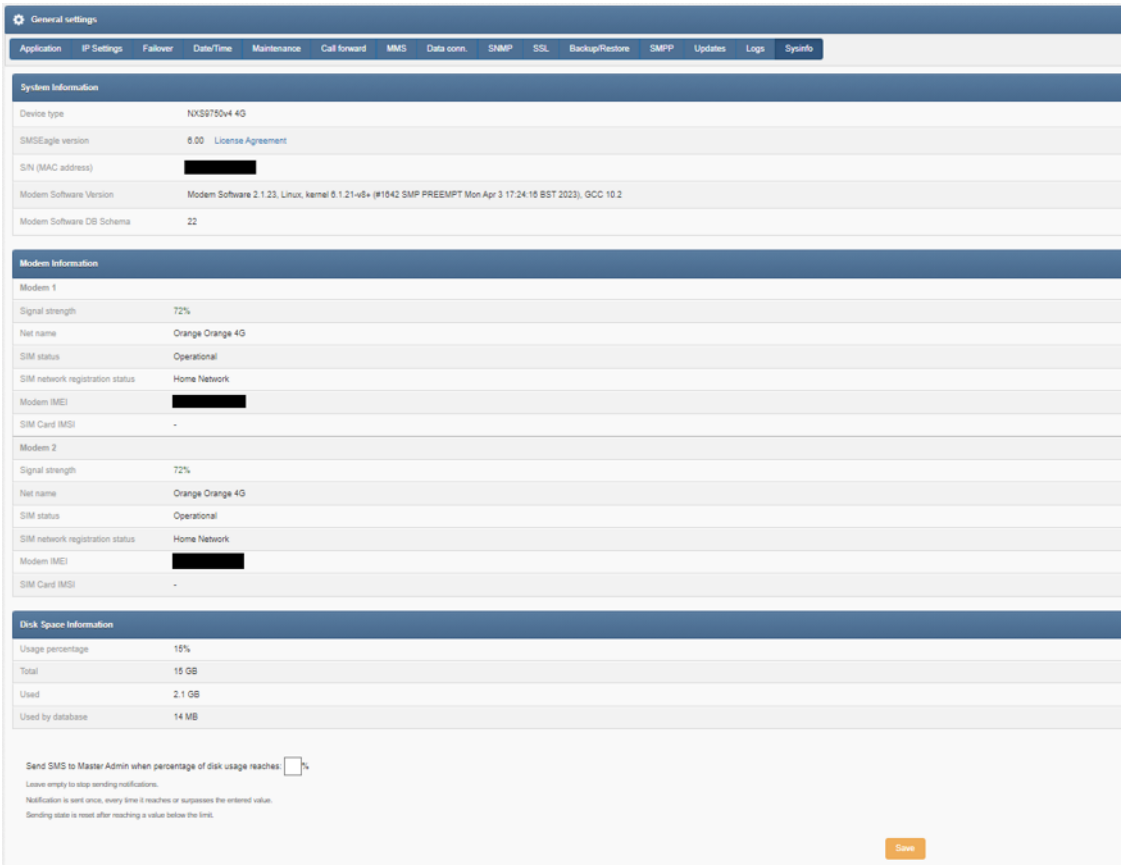
You may also download the full device log package for troubleshooting and support. This can be done using the button “Download device logs”



- You can choose to download device logs from last 14 days, 30 days or all.

Sysinfo

General device and system information can be accessed under the menu Settings > Sysinfo.



The system information contains:

- device model and serial number (MAC)
- software version

- modem information: SIM status, signal strength, network registration status, modem IMEI
- disk space availability

You can configure SMS notifications to be sent when disk usage reaches a specific value. The SMS alert will be sent to the phone number assigned to the user with the role of Master Admin (id=1).

Failover (HA-cluster) feature

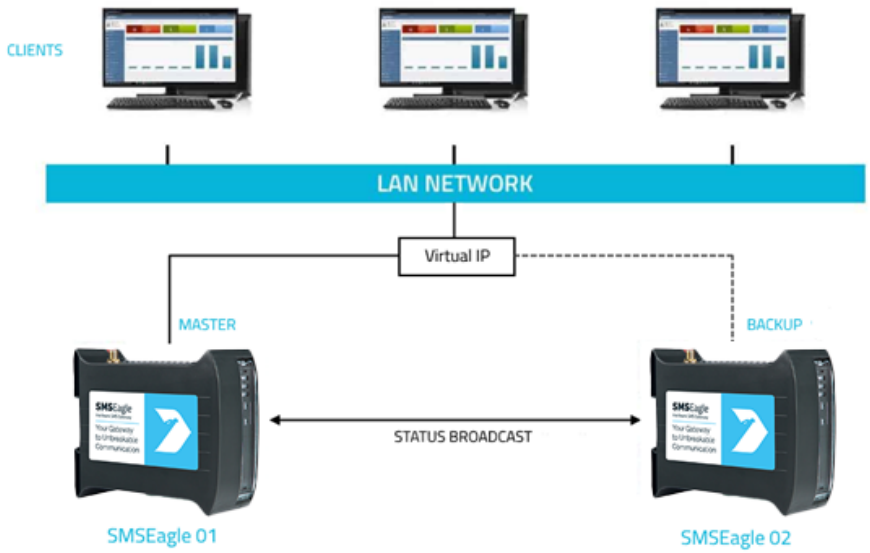
“High-availability clusters (also known as HA clusters or fail over clusters) are groups of computers (...) that can be reliably utilized with a minimum of down-time. They operate by using high availability software to harness redundant computers in groups or clusters that provide continued service when system components fail. Without clustering, if a server running a particular application crashes, the application will be unavailable until the crashed server is fixed. HA clustering remedies this situation by detecting hardware/software faults, and immediately restarting the application on another system or whole node without requiring administrative intervention, a process known as failover.” (source: Wikipedia)

SMSEagle NXS-family devices have their own failover mechanism based on HA-cluster. This feature allows you to assure high availability of SMSEagle devices in critical environments. To enable failover (HA-cluster) you need 2 devices (‘aka’ nodes). The failover feature monitors devices working in the cluster, and detects faults with the following services:

1. Apache2 WWW server
2. PostgreSQL database
3. SNMP agent
4. Modem software (Gammu-SMSD daemon)
5. Accessibility (response to ping) of whole node.

Every node in a cluster can have one of three states:

- **Master:** main healthy node in a cluster, by default accessible through Virtual IP
- **Backup:** second healthy node in a cluster, ready and waiting for replacing Master when needed
- **Fault:** node with detected service fault



In the cluster you have one MASTER device and one BACKUP device. **HA-cluster is accessed via Virtual IP address.** When the daemon running at MASTER device detects failure of at least one described feature it immediately automatically switches cluster's IP assignment to the BACKUP device (node) providing continuous usage of the SMSEagle HA-cluster for the user.

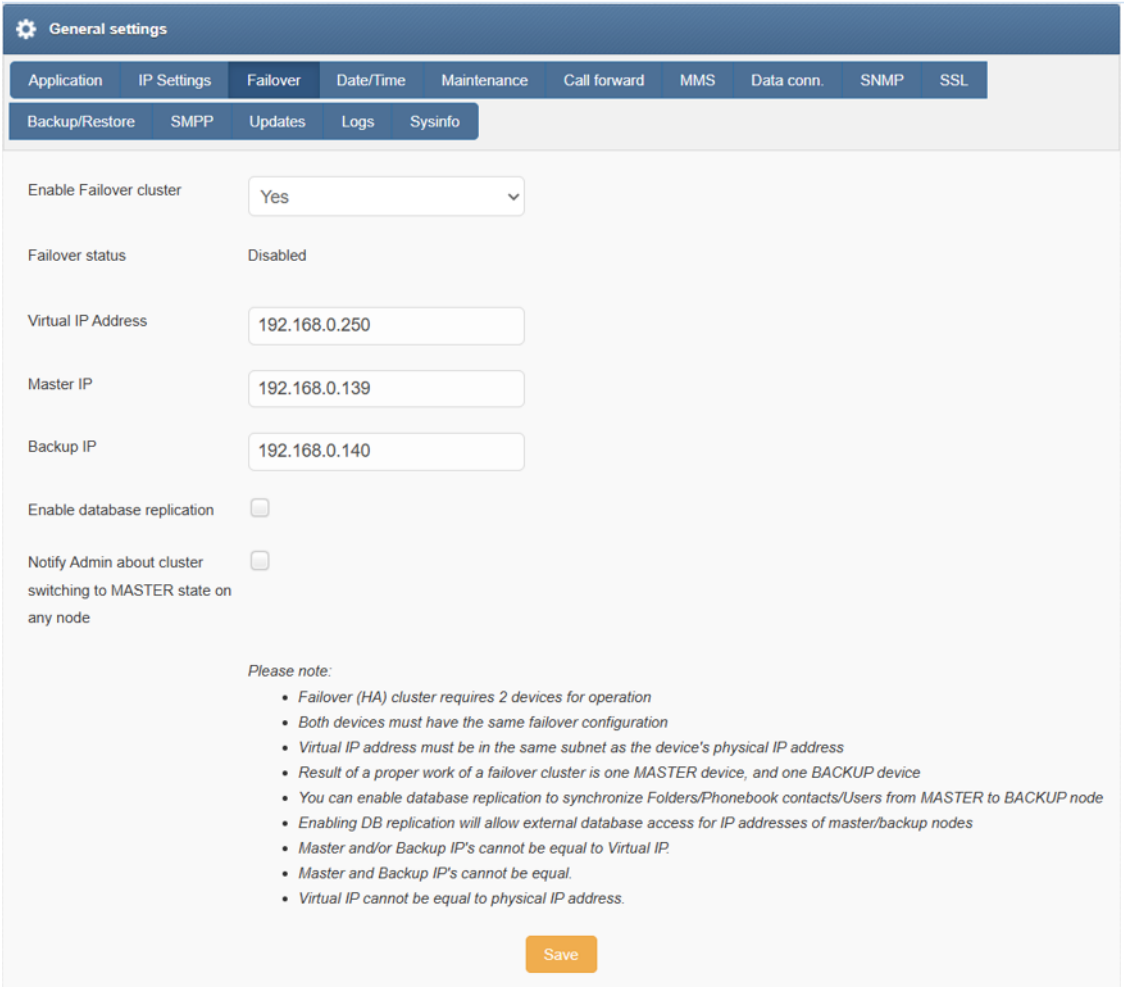
Devices (nodes) should see each other on the network. By default, HA-nodes use 224.0.0.18 multicast IP address for VRRP (Virtual Router Redundancy Protocol) for communication between two nodes. If nodes are on the same network (same subnet & IP range) there is no need for any network configuration. If two nodes are behind firewalls, make sure firewall is configured to accept multicast and VRRP protocol (IP Protocol #112).

How to configure failover (HA-cluster):

Failover cluster can be easily configured using web-gui. Configuration can be done in menu "Settings" > tab "Failover". The configuration should be exactly the same on both devices in HA-cluster.
Please configure first MASTER then BACKUP device. For **each** device in failover cluster:

- enter virtual IP address in the field "Virtual IP Address"
- enter Master and Backup IP addresses (these should be physical addresses of your devices)
- set "Enable Failover cluster" to "Yes"
- optionally you can enable database replication between nodes

Save configuration. **Reboot** each device after saving.



Screenshot from “General Settings-Failover”

SMS notification on state changes

The Failover feature can optionally send SMS notifications when the cluster state changes (e.g. when any node switches to MASTER state, for example: BACKUP > MASTER, or FAULT> MASTER). This allows administrators to react quickly to infrastructure failures without having to monitor the device manually. SMS notification can be enabled in the Failover configuration tab. Notifications are automatically sent to the phone number assigned to the primary Admin account (id=1).

Database replication

Database replication (optional) allows to automatically replicate database content between nodes from MASTER to BACKUP. In the current software version, the following content is replicated: Folders (with messages), Phonebook contacts, Users.
We recommend to use the same device models and the same software version on both devices for seamless replication between nodes.

After correct configuration of the HA-cluster **you should access the cluster via its Virtual IP address.**

SNMP-monitoring of HA-cluster

Failover feature uses KEEPALIVED-MIB for SNMP monitoring.

Example of reading device cluster state value using NET-SNMP library

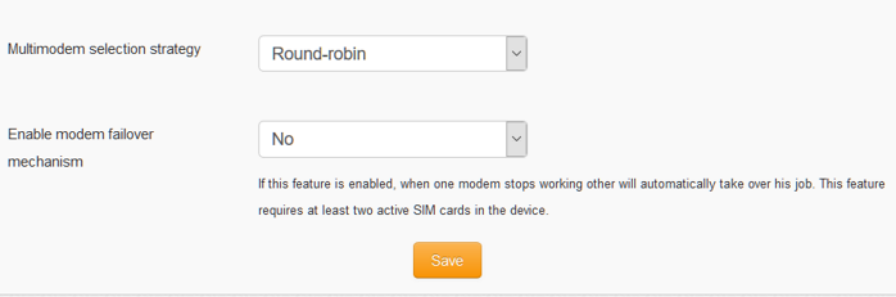
a) Command for reading the result value:*
*snmpget -v 2c -c public ip-of-smseagle .1.3.6.1.4.1.9586.100.5.2.3.1.4.1

Result:*
*KEEPALIVED-MIB::vrrpInstanceState.1 = INTEGER: master(2)

Comment: Current device state is master

Multimodem features

SMSEagle NXS-9750 is equipped with two built-in modems. You can manage modem settings in web-GUI menu Settings > Maintenance Tab. There are following options available for multimodem device:



Multimodem settings

Multimodem selection strategy

This setting is responsible for modem choice strategy when sending SMS messages from SMSEagle. The following options are possible:

- Round-robin

In this strategy modems are selected sequentially one-by-one when sending out SMS messages. This means that device sends messages using modem1 > modem2 > modem1 > modem2, etc.

- SIM1 as Master modem

In this strategy modem1 is always selected when sending out SMS messages. If failover is enabled (see below) modem2 will be always used as a backup in failover strategy

- SIM2 as Master modem

In this strategy modem2 is always selected when sending out SMS messages. If failover is enabled (see below) modem1 will be always used as a backup in failover strategy

Enable modem failover mechanism

If this setting is enabled, when one modem stops working other will automatically take over his job. This feature requires at least two active SIM cards in the device. The health check for each modem is performed with 3 minutes frequency. If during a health check a modem is not connected to network the other will automatically take over his jobs (including messages waiting in Outbox folder).

SMSEagle API

SMSEagle offers a powerful built-in REST API functionalities. API is dedicated for integration of SMSEagle with any external system or application.

API Reference (Documentation)

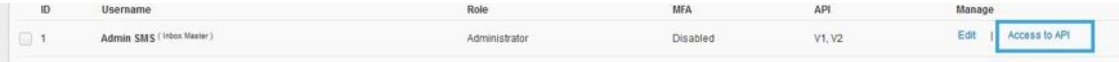
SMSEagle device offers two API versions APIv2 and APIv1.

- **API v2 – recommended for new projects**
  Modern RESTful API based on OpenAPI 3.0 specification
  Link to APIv2 Reference
- **API v1 – for existing projects and backward compatibility**
  Simple HTTP and JSONRPC API
  Link to APIv1 Reference

Due extensive content of API documentation it has been moved to a separate document. Follow the links above to find each specification of each API.

API Access

Before you can use SMSEagle API you must enable API access in web-GUI (menu Users). Below you can find the description how to enable API on your device.



Screenshot from menu “Users” with marked “Access to API” link.

Access can be granted to:

- APIv1
- APIv2
- API Access token can generated or entered
- For APIv1 user/password authentication can be granted (use this only for backward compatibility)
- For APIv2 access for resources of other users (created by others) can be granted
- Particular permissions can be granted for methods in APIv1 & APIv2

Access to resources of other users in API

In APIv1 an API user (single API key) by default has access to resources of all other users (phonebook contacts, groups, etc.). APIv2 is more granular when it comes to resource access: an

API user (single API key) by default has access to resources created by himself. If you want to allow access to resources of all other users, you must check the checkbox “Access to resources of all users” in Access to API window.

Plugins and integrations

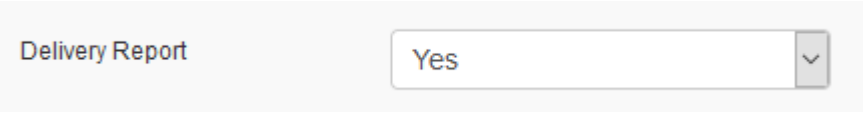
SMSEagle has a number of ready-to-use plugins and integration manuals for an easy and quick integration of SMSEagle device with external software (Network Monitoring Systems, Authentication Systems and other). The list grows constantly and is published on SMSEagle website. For a complete and up to date list of plugins please go to: https://www.smseagle.eu/integration-plugins/

Extras

Delivery Reports

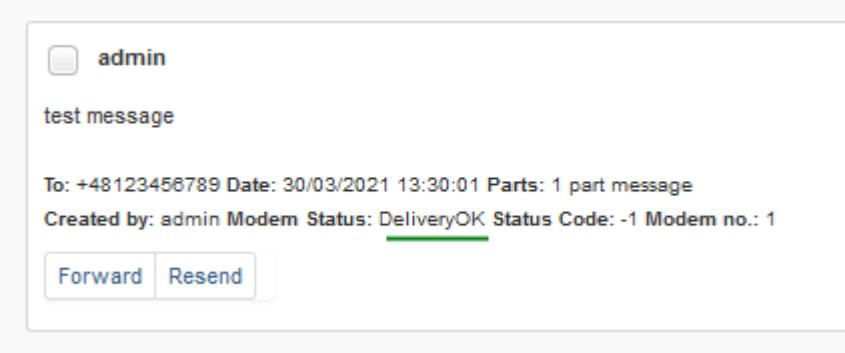
SMSEagle software allows you to enable delivery reports for each sent SMS. Delivery reports is afeature that allows to receive a confirmation that SMS was received on recipients phone.

In order to enable delivery reports, please go to web-GUI > menu Settings and set “Delivery Reports” to “Yes”



Once delivery reports are enabled in in web-GUI, you may verify whether SMS was delivered to recipient:

- **In web-GUI**
  In menu Folders > Sent items > open the message you want to check. Press “Show Details“ in top-right corner of the message. Field “Modem Status” contains information on delivery status



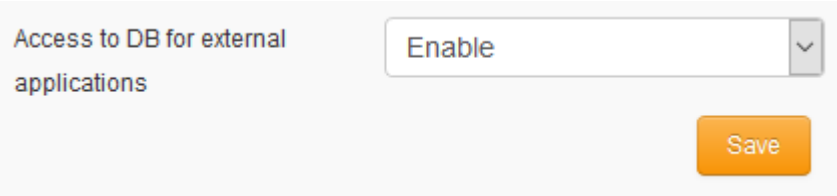
- **Using Webhooks**
  CallbackURL feature allows to define a webook for the change of delivery status. Webhooks are standard HTTP endpoints implemented in your external application that will accept HTTP requests from SMSEagle device. Webhooks save you from having to continuously send requests to the SMSEagle device asking for message status. See more details on Callback URL chapter of this User’s Manual.
- **Using API**

Use method “read_sms” to fetch data for a selected SMS in sentitems folder. The data will contain columns “Status” and “DeliveryDateTime” contain information about delivery status of the message. For more information about possible values for “Status” column, please refer to the table “Field Description Of Response Data – Sentitems Folder” in the APIv1 Reference.

Connecting directly to SMSEagle database

SMSEagle's database operates on PostgreSQL database engine. You may use a direct access to database for reading/writing SMS messages directly from/to database via SQL queries.

The database access for external applications is disabled by default. In order to enable it, go to webGUI > menu Settings and enable to following setting:



Once database access is enabled, it is possible to connect to the database from external application using the following credentials:

- Host: IP address of your device
- Database name: `smseagle`
- User: `smseagleuser`
- Password: `postgreeagle`

Injecting short SMS using SQL

The simplest example is short text message (limited to 160 chars):

```
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;
```

In the above example the message will belong to user with **id_user** 1 (default 'admin'). You can find id_user values for other users in table public."user". Field SenderID contains identification number of SMSEagle modem. For modem 1 SenderID = smseagle1 and for modem 2 SenderID = smseagle2.

Injecting long SMS using SQL

Inserting multipart messages is a bit more tricky, you need to construct also UDH header and store it hexadecimally written into UDH field. Unless you have a good reason to do this manually, use API.

For long text message, the UDH starts with 050003 followed by byte as a message reference (you can put any hex value there, but it should be different for each message, D3 in following example), byte for number of messages (02 in example, it should be unique for each message you send to same phone number) and byte for number of current message (01 for first message, 02 for second, etc.).

For example, long text message of two parts could look like following:

```
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;
```

Note: Adding UDH means that you have less space for text, in above example you can use only 153 characters in single message.

Database cleaning scripts

We have added some useful scripts which may be used to delete SMS messages from database through Linux CLI.
Scripts are located at following directory: `/mnt/nand-user/scripts/`

- **db_delete** – script for deleting SMS from folders Inbox, SentItems older than provided date. Usage: `./db_delete YYYYMMDDhhmm`
- **db_delete_7days** – script for deleting SMS from folders Inbox, Sentitems older than 7 days. Usage: `./db_delete_7days`
- **db_delete_allfolders** – script for cleaning PostgreSQL database folders (Inbox, SentItems, Outbox). Specially designed to run periodically through cron. Usage: `./db_delete_allfolders`
- **db_delete_select -** script for deleting SMS from chosen databse folder (Inbox, Outbox, SentItems, Trash). Usage: `./db_delete_select {inbox|outbox|sentitems|trash}`

  Adding script to system cron daemon

  1. Create a file inside /etc/cron.d/ directory with your desired name (eg. pico db_cleaner)
  2. Example content of this file: `0 0 1 * * root /mnt/nand-user/scripts/db_delete_allfolders`

  This will run cleaning script every 1st day of month.

SNMP agent

"Simple Network Management Protocol (**SNMP**) is an Internet-standard protocol for managing devices on IP networks. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention" (source: Wikipedia).

SMSEagle device has a built-in Net-SNMP agent. The SNMP agent provides access to Linux Host MIB tree of the device, and additionally (using extension NET-SNMP-EXTEND-MIB) allows access to custom metrics specific to SMSEagle.

Available SNMP metrics that describe a state of a SMSEagle device are:

Metric name	Description	OID
GSM_Signal1	Returns 3G/4G signal strength in percent for modem 1. Value range: 0-100. If modem is disconnected from cellular network GSM_Signal returns 0.	.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_Signal[X]	Returns 3G/4G signal strength in percent for modem X. Value range: 0-100. If modem is disconnected from cellular network GSM_Signal returns 0.	.1.3.6.1.4.1.8072.1.3.2.3.1.2.11.71.83.77.95.83.105.103.110.97.108.[48+X]
GSM_NetName1	Returns cellular network name on modem 1	.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_NetName[X]	Returns cellular network name used on modem X	.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.[48+X]
GSM_ModemState[X] where X is the no of modem	Returns modem state information enabled/disabled	.1.3.6.1.4.1.8072.1.3.2.3.1.2.11.77.111.100.101.109.83.116.97.116.101.49 (for 1st m .1.3.6.1.4.1.8072.1.3.2.3.1.2.11.77.111.100.101.109.83.116.97.116.101.50 (for 2nd

Metric name	Description	OID
FolderOutbox_Total	Returns number of SMS messages in Outbox folder (outgoing queue length)	.1.3.6.1.4.1.8072.1.3.2.3.1.2.18.70.111.108.100.101.114.79.117.116.98.111.120.95.8
FolderInbox_Total	Returns number of SMS messages in Inbox folder	.1.3.6.1.4.1.8072.1.3.2.3.1.2.17.70.111.108.100.101.114.73.110.98.111.120.95.84.1
FolderSent_Last24H	Returns number of SMS messages sent from the device within last 24 hours	.1.3.6.1.4.1.8072.1.3.2.3.1.2.18.70.111.108.100.101.114.83.101.110.116.95.76.97.1
FolderSent_Last1M	Returns number of SMS messages sent from the device within last month	.1.3.6.1.4.1.8072.1.3.2.3.1.2.17.70.111.108.100.101.114.83.101.110.116.95.76.97.11

Metric name	Description	OID
FolderSent_Last24HSendErr	Returns number of SMS messages sent with error within last 24h. Error occurs when 3G modem cannot send SMS message or message is rejected by 3G/4G carrier (mostly happens when a credit on pre-paid SIM card is over)	.1.3.6.1.4.1.8072.1.3.2.3.1.2.25.70.111.108.100.101.114.83.101.110.116.95.76.97.1
Temp	Returns last value of Temperature (in °C) from internal DHT22 sensor. Requires sensor to be enabled.	.1.3.6.1.4.1.8072.1.3.2.4.1.2.4.84.101.109.112.1
Humidity	Returns last value of Humidity (in %) from internal DHT22 sensor. Requires sensor to be enabled.	.1.3.6.1.4.1.8072.1.3.2.3.1.2.8.72.117.109.105.100.105.116.121

Metric name	Description	OID
Temp[X] where X is between 1 and 4	Returns last value of Temperature (in °C) from: Temp1: internal temperature sensor Temp2-Temp4: external 1-Wire temp sensors.	.1.3.6.1.4.1.8072.1.3.2.4.1.2.5.84.101.109.112.49.1 (for 1st sensor) .1.3.6.1.4.1.8072.1.3.2.4.1.2.5.84.101.109.112.50.1 (for 2nd sensor) etc.
SIM_State[X] where X is the no of modem	Returns information of physical SIM state	.1.3.6.1.4.1.8072.1.3.2.3.1.2.10.83.73.77.95.83.116.97.116.101.49 (for 1st mode .1.3.6.1.4.1.8072.1.3.2.3.1.2.10.83.73.77.95.83.116.97.116.101.50 (for 2nd mod
SIM_RegState[X] where X is the no of modem	Returns information of SIMcard registration state in the mobile network.	.1.3.6.1.4.1.8072.1.3.2.3.1.2.13.83.73.77.95.82.101.103.83.116.97.116.101.49 (fo .1.3.6.1.4.1.8072.1.3.2.3.1.2.13.83.73.77.95.82.101.103.83.116.97.116.101.50 (fo

Result values

- Using OID

Result values for each custom metric are available and can be fetched from OID given in table above.

- Using textual name

  Alternatively result values for each custom metric can be fetched using textual names from OID tree under: NET-SNMP-EXTEND-MIB::nsExtendOutputFull."[METRIC NAME]"

  For example:
  Result value for parameter **GSM_Signal1**:
  NET-SNMP-EXTEND-MIB::nsExtendOutputFull."GSM_Signal1"

  If your chosen SNMP tool cannot access NET-SNMP-EXTEND-MIB objects, you can download MIB definitions from: https://www.smseagle.eu/download/NET-SNMP-EXTEND-MIB.txt

Reading result values
In order to test-read the parameter values from SNMP agent you can use any tools available for SNMP protocol (for example: NET-SNMP library for Linux or iReasoning MiB-Browser for Windows).

Example of reading GSM_Signal1 value using NET-SNMP library

a) Command for reading the result value:

snmpget -v 2c -c public localhost .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

Result:

NET-SNMP-EXTEND-MIB::nsExtendOutputFull."GSM_Signal1" = STRING: 54

Comment: 3G/4G Signal strength value is 54%

Example of reading GSM_NetName1 value using NET-SNMP library

a) Command for reading the result value:

snmpget -v 2c -c public localhost .
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

Result:

NET-SNMP-EXTEND-MIB::nsExtendOutputFull."GSM_NetName1" = STRING: PLAY

Comment: Currently used network at SIM card #1 is PLAY

Example of reading FolderOutbox_Total value using NET-SNMP library (and textual name of metric)

a) Command for reading the result value:

snmpget -v 2c -c public ip-of-smseagle 'NET-SNMP-EXTEND-MIB::nsExtendOutputFull."FolderOutbox_Total"'

Result:

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

Comment: Number of SMS messages waiting in outbox queue is 0

Example of reading system uptime from Linux host using NET-SNMP library

a) Command for reading the result value:

snmpget -v 2c -c public ip-of-smseagle system.sysUpTime.0

Result:

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (216622) 0:36:06.22

Comment: Linux system is up for 36 minutes, 6.22 seconds

Example of browsing SMSEagle extension parameters IN mib tree using NET-SNMP library

a) Command for reading the result value:

snmpwalk -v 2c -c public ip-of-smseagle .1.3.6.1.4.1.8072.1.3.2.3.1.2

Result:

NET-SNMP-EXTEND-MIB::nsExtendOutputFull."GSM_Signal1" = STRING: 54

NET-SNMP-EXTEND-MIB::nsExtendOutputFull."GSM_NetName1" = STRING: PLAY

NET-SNMP-EXTEND-MIB::nsExtendOutputFull."GSM_NetName2" = STRING: PLAY

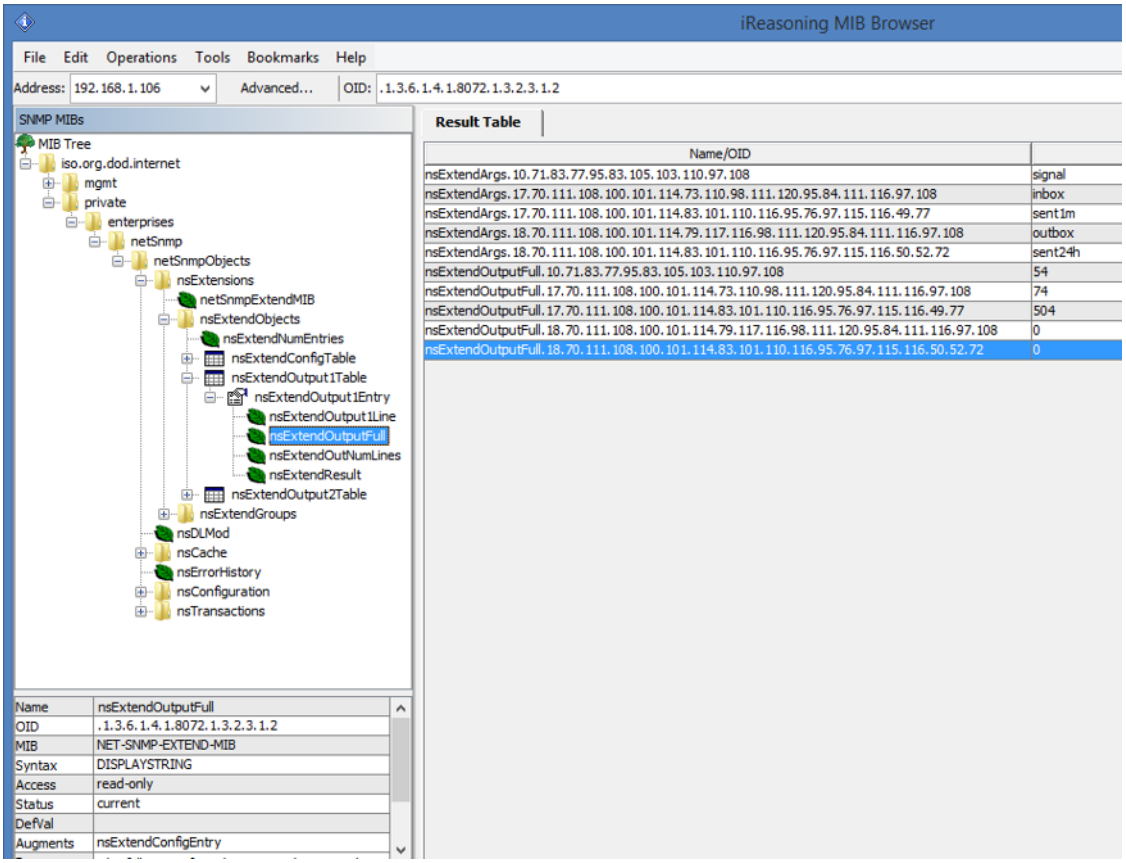
NET-SNMP-EXTEND-MIB::nsExtendOutputFull."FolderInbox_Total" = STRING: 15

NET-SNMP-EXTEND-MIB::nsExtendOutputFull."FolderSent_Last1M" = STRING: 19

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

NET-SNMP-EXTEND-MIB::nsExtendOutputFull."FolderSent_Last24H" = STRING: 0
NET-SNMP-EXTEND-MIB::nsExtendOutputFull." FolderSent_Last24HSendErr" = STRING: 0

Example of browsing SMSEagle extension parameters IN mib tree using mib-browser



Setting up SNMP v3 access control

By default, SMSEagle devices uses SNMP v2 access control. Using v3 can strengthen security, however is not mandatory. To easily switch to SNMP v3 access control we've prepared special shell script located at /mnt/nand-user/smseagle directory.

1. Log in via SSH using root account
2. Navigate to:
   cd /mnt/nand-user/smseagle/
3. Configuration script:
   ./snmpv3
4. Script can run with following parameters:
    1. add
    2. del
    3. enablev2
    4. disablev2
5. To add v3 USER please run:

   ./snmpv3 add USERNAME PASSWORD ENCRYPTIONPASSWORD

1. To delete USER please run:

   ./snmpv3 del

1. To disable v2 access policy run:

   ./snmpv3 disablev2

1. To enable v2 access policy run:

   ./snmpv3 enablev2

Forwarding logs to external server

Our devices run rsyslog for log managing. Here we describe how to configure additional rules for rsyslog daemon: rsyslogd. This is only a brief excerpt from rsyslog manual website. Full information is available at: http://www.rsyslog.com/

Rsyslogd configuration is managed using a configuration file located at /etc/rsyslog.conf

- At the bottom of the configuration file add:

  . action(type="omfwd" target="SERVER_IP" port="PORT" protocol="PROTOCOL"

action.resumeRetryCount="10"

queue.type="linkedList" queue.size="10000")

where: SERVER_IP – IP (or FQDN) address of receiving server
PORT – port on receiving server
PROTOCOL one of the values: tcp, udp

- Example:

. action(type="omfwd" target="192.168.0.250" port="10514" protocol="tcp"

action.resumeRetryCount="10"

queue.type="linkedList" queue.size="10000")

- SSL-encryption of your log traffic: please have a look at this article: https://www.rsyslog.com/doc/v8-stable/tutorials/tls_cert_summary.html

Automatic software updates check

SMSEagle software is under process of continual improvement. We listen to our customers, and new releases are based on our customer's inputs/requests. Software updates are released frequently, and offer access to new features and fixes to reported issues. Web-GUI offers you a possibility to automatically check for new software updates. This can be done in two ways:

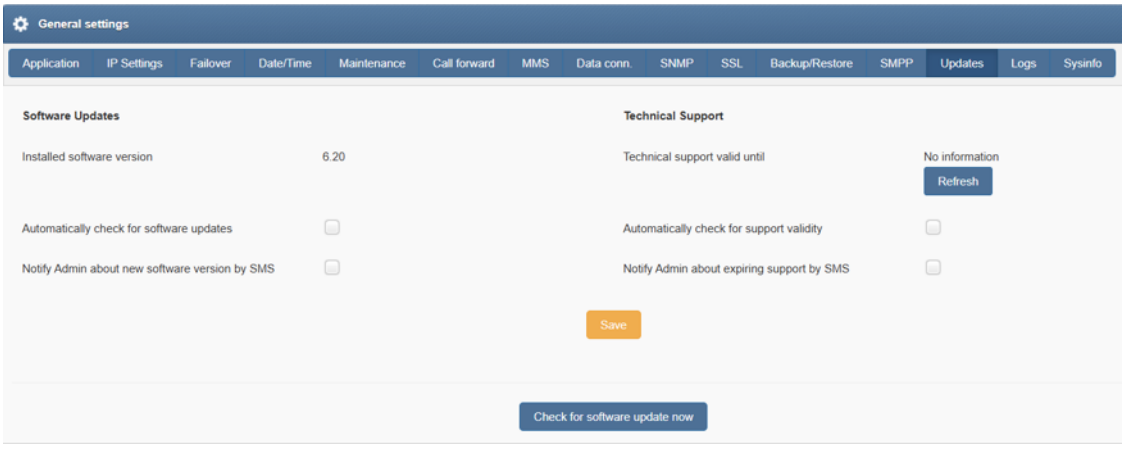
Manual CHECK

In order to manually check for available software updates, go to menu Settings > tab Updates. Click on the button "Check for software update now". At the top pops up a balloon in red with information if it is up-to-date.

Automatic check

In order to start automatic checks for software updates go to menu Settings > tab Updates, and check the option "Automatically check for software updates". This will enable periodic checks (once a month) for available software updates. If a new update is available, a message "Update Available" will appear in menu Settings> Sysinfo – next to the current software version number.

If you select "Notify Admin about new software version by SMS", the device will additionally send SMS to the default admin account (if the phone number is entered in the account) with a notification about new software update.



Screenshot from “General settings-Maintenance”

Notice: Your SMSEagle device must have a HTTPS connectivity with address updates.smseagle.eu in order for this feature to work.

Knowledgebase & Support Portal

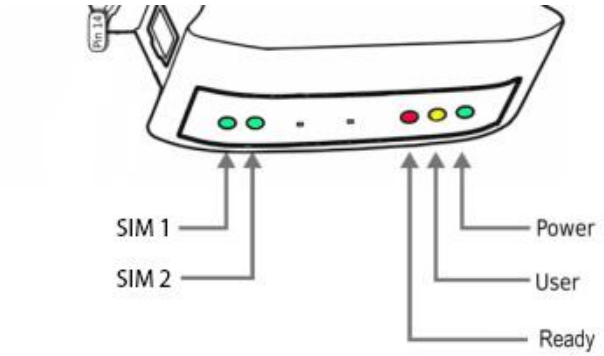
More information and useful hints about SMSEagle device configuration can be found in our online knowledgebase and support portal at: https://support.smseagle.eu

Troubleshooting

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

1. Verification of LEDs
2. Checking the device configuration (IP Settings)
3. Check the device logs (description below)

Verification of LEDs



LED locations

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

LED	Correct operation
Power (PWR)	Continuously lit
User	Blinks during flashdisk read/write
Ready (RDY)	Blinking
SIM1 (only 3G device)	Slow flashing in stand-by mode, Quick flashing when modem 1 in use
SIM2 (only 3G device)	Not used

Checking the device information

The device information (device type, software version, modem IMEI, IMSI, network signal strength, network name) can be found under menu “Settings” > “Sysinfo”.

Device logs

Under menu “Settings” > “Logs” you can find 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 button “Download device logs” in menu “Settings” > “Logs”.

When the device is not reachable

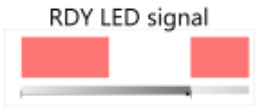
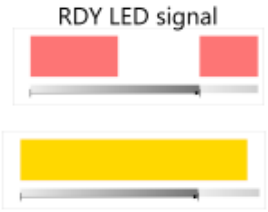
1. Check if the device is correctly connected to the network. Check LED status of RJ45 socket.
2. In the case when the device does not respond due to a malfunction or incorrect user settings please reboot the device by disconnecting and connecting power source (or pressing Reset switch).
3. If you still cannot connect with the device, it is possible to restore to factory IP settings by 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.

To initiate the reset, press and hold the SW button for 10 seconds. The device will enter recovery mode.

LED signaling	USER actions	System reaction
	1. **When the device is ready to operate**	–
–	2. **Press and hold SW button for 10 seconds**	Restore service is counting down.
	3. **Release SW button after 10 seconds.** User LED will begin to blink.	System is reading factory defaults. Factory settings are being applied to the device.
	4. **Wait until system reboots.** Default settings are restored.	System is going for a reboot.

Hardware Rev.5 and later

The process uses a dedicated read-only recovery partition, ensuring the restore image remains intact and unaffected by normal device operation. Once recovery mode is entered, a single short beep starts a 10s countdown. A second short beep confirms the start of the restore process. The entire process typically takes a few minutes to complete.

Upon successful completion, the device signals with three short beeps, followed by a 10s countdown before automatically restarting. If the operation is cancelled during the countdown, two short beeps are emitted. In the event of a restore error, the device emits one long beep followed by two short beeps, then exits to a service shell for diagnostics.

Hardware Rev.3–Rev.4

The reset function restores only the following settings to their default values: IP settings, time zone settings, database content, and Linux OS users/passwords.

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 with support team, be sure that you have read Troubleshooting section of this manual.
SMSEagle Support Team is available by email or telephone.

Support Portal: 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 support team, be prepared to provide the following information:

System Logs

Go to menu Settings > Logs > “Download device logs”. Provide log package to support team when requested.

MAC address

Each SMSEagle device has its unique MAC address. MAC address is printed on the device body or can be found in menu Settings > IP Settings

Tech Specs & Safety Information

Technical Specification

Hardware Specification

- Processor type:
  - hardware Rev.5, Rev.4: Broadcom BCM2711 1.5 GHz quad-core Cortex-A72 (ARM v8) 64-bit
  - hardware Rev.3: Broadcom BCM2837 1.2 GHz quad-core ARM Cortex-A53 (64-bit)
- Operational memory (RAM):
  - hardware Rev.5, Rev.4: 2GB LPDDR4
  - hardware Rev.3: 1GB LPDDR2 @ 900 MHz
- eMMC storage
  - hardware Rev.5, Rev.4: 16GB
  - hardware Rev.3: 4GB
- Network interface: Ethernet (1xRJ45): Gigabit Ethernet 10/100/1000 TX
- 1x HDMI port for debugging purposes
- Other external ports: 4x DI, 4x DO, 1× 1Wire, 2x USB 2.0 (max. 300mA)
- Digital Input/Output port types: DI type “pull-up resistor”. DO type “open collector”
- RTC Clock: RTC 240B SRAM, Watchdog timer
- Internal humidity & temperature sensor: Accuracy ± 0,5 °C, ±2 %RH
- Power consumption:
  - hardware Rev.5, Rev.4: max 35W
  - hardware Rev.3: max 20W
- Noise level: Fan-less
- Dimensions: (width x depth x height) 45 × 120 × 101 mm
- Weight: 350g
- Casing: ABS, DIN rail installation
- Operating parameters:
  - Operating temperature: 0 ~ 40°C
  - Humidity: 8 ~ 90% RH (no condensation)
- 2x Internal modem

Device type NXS-9750-4G Rev.5, Rev.4:

- Wavebands: LTE, UMTS. Optional GSM.
- LTE FDD: B1/B2/B3/B4/B5/B7/B8/B12/B13/B18/B19/B20/B25/B26/B28
- LTE TDD: B38/B39/B40/B41
- UMTS: B1/B2/B4/B5/B6/B8/B19
- GSM: B2/B3/B5/B8 (optional)
- Output power (Rated):
    - Class 3 (23dBm±2dB) for LTE-FDD, LTE-TDD bands
    - Class 3 (24dBm+1/-3dB) for WCDMA bands
    - Class 4 (33dBm±2dB) for GSM850, EGSM900
    - Class 1 (30dBm±2dB) for DCS1800, PCS1900
    - Class E2 (27dBm±3dB) for GSM850 8-PSK, EGSM900 8-PSK
    - Class E2 (26dBm±3dB) for DCS1800 8-PSK, PCS1900 8-PSK

Device type NXS-9750-4G Rev.3:

- Waveband: UMTS, LTE
- LTE Bands:
  LTE FDD: 1-5, 7, 8, 12, 13, 17, 20, 25, 26, 28, 29, 30 (Rx only), 66
  LTE TDD: 38, 40, 41
- 3G Bands: 1, 2, 4, 5, 8
- Output power:
    - Class 3 (0.2 W, 23 dBm) @ LTE
    - Class 3 (0.25 W, 23 dBm) @ 3G

Device type NXS-9750-3G Rev.3:

- 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
- SIM card standard: mini
- Antenna connector: SMA
- Country of origin: European Union (Poland)

Power Supply

- hardware Rev.5, Rev.4:
  - External power supply with output circuit rated ES1 (12Vdc; min, 3.3A), PS2 (LPS – Limited Power Source). AC line input:
    - Voltage ranges: 100–240V alternating current (AC)
    - Frequency: 50–60Hz single phase
    - DC plug type: 5.5/2.5
  - Alternative power source: PoE+ (IEEE 802.3at Type 2). Circuit provided with PoE+: rated ES1 (50-57Vdc; 30W), PS2 (LPS – Limited Power Source)
- hardware Rev.3:
  - External power supply with output circuit rated ES1 (12Vdc; min, 1A), PS2 (LPS – Limited Power Source). AC line input:
    - Voltage ranges: 100–240V alternating current (AC)
    - Frequency: 50–60Hz single phase
    - DC plug type: 5.5/2.5

Antenna

- Device type NXS-9750-4G:
  - 2x Omnidirectional 2dBi antenna with magnetic foot
  - Waveband: UMTS, LTE
  - Cable length 3m
  - Plug type: SMA
  - Impedance: 50 Ohm
- Device type NXS-9750-3G:
  - 2x Omnidirectional 3dBi antenna with magnetic foot
  - Waveband: GSM, UMTS
  - Cable length 3m
  - Plug type: SMA
  - Impedance: 50 Ohm

Sending/Receiving Throughput

- Incoming transmission rate: up to 60 SMS/min
- Outgoing transmission rate: up to 60 SMS/min

Software Platform

- Operating system: Linux
    - hardware Rev. 5: kernel 6.12
    - hardware Rev. 4: kernel 5.1x
    - hardware Rev. 3: kernel 4.14
- 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 3G/4G/5G modem
- 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 about 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 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 31cm (12.2 inches) distance from the body. In case of 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 NXS-9750-3G, NXS-9750-4G 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 NXS-9750-3G , NXS-9750-4G 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 NXS-9750-3G, NXS-9750-4G 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 30 cm (12 inches) during normal operation.

Disposal and Recycling Information

Your SMSEagle device contains 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.4	CR1216	Lithium
Rev.3	CR1632	Lithium

Angaben zur sicheren Entnahme der Batterien oder der Akkumulatoren:

Hardware Rev.4:

- Öffnen Sie die transparente Seitenwand
- Heben Sie die Klappe an der Seitenkante mit einem Schraubenzieher auf. Die Klappe herausnehmen
- Entnehmen Sie vorsichtig die Batterie aus der Halterung auf der linken Seite
- Die Batterie und das Gerät können jetzt getrennt entsorgt werden

Hardware Rev.3:

- Entfernen Sie die rote DIN-Verriegelung, indem Sie einen Schlitzschraubendreher unter die Unterseite der Verriegelung schieben. Heben Sie den Riegel an, der sich unter der entfernten DIN-Klappe befindet.
- Entfernen Sie das SIM-Fach
- Verwenden Sie einen Schlitzschraubendreher, um die vier Verriegelungen an den Ecken des Geräts anzuheben.
- Öffnen Sie das Gehäuse. Die Batterie befindet sich auf der zweiten Platte. Entfernen Sie die Batterie
- Die Batterie bzw. der Akkumulator und das Gerät können jetzt 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”).