SMSEagle

User's Manual

MHD-8100-3G
MHD-8100-4G

rev.1 / rev1.1

CONGRATULATIONS ON PURCHASING SMSEagle

Document version: 6.14

CONTENTS

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 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 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 PROMIXUS, 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

1.01 "Agreement" or "License" or "EULA" shall mean this End User License Agreement.

1.02 "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.

1.03 "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.

1.04 "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.

1.05 "Upgrade" means a major, standalone version of SMSEagle Software, which may include additional applications, features, or functionality.

1.06 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.

1.07 Words in the singular shall include the plural and vice versa.

1.08 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.

1.10 A reference to writing or written includes e-mail.

1.11 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.

1.12 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.

1.13 References to articles, sections, or clauses are to the articles, sections, and clauses of this Agreement.

1.14 "We", "Us", and "Our" refer to Proximus Sp. z o.o. (“PROXIMUS”).

1.15 The “Parties” to this Agreement are You and Proximus Sp. z o.o. (“PROXIMUS”).

1.16 "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

2.01 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:

(a) **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.

(b) **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.

2.02 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.

3. INTELLECTUAL PROPERTY

3.01 **PROTECTED SMSEAGLE SOFTWARE**. The SMSEagle Software is protected by copyright and other Intellectual Property laws and treaties.

3.02 **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; (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.

3.03 **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.

4. 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.

5. LIMITATION OF LIABILITY AND REMEDIES

IN SPITE OF ANY DAMAGES ARISING FROM OR RELATED TO THE SMSEAGLE DEVICE AND SMSEAGLE SOFTWARE OR ITS OPERATION THAT YOU MAY INCUR FOR ANY REASON, WHICH MAY INCLUDE, BUT ARE NOT LIMITED TO, ANY AND ALL DAMAGES IN CONTRACT, TORT OR OTHERWISE, THE ENTIRE LIABILITY OF PROXIMUS AND/OR ANY OF THE AFOREMENTIONED PERSONS REFERRED TO IN SECTION 4 ABOVE, AS WELL AS ANY LICENSORS

REFERRED TO IN SECTION 6 BELOW, SHALL NOT EXCEED YOUR TOTAL PAYMENTS (IF ANY) WITH RESPECT TO THE PERTINENT SMSEAGLE DEVICE, WHICH HAS BECOME DUE FOR DURING THE PERIOD OF PRIOR 12 MONTHS BEFORE THE MONTH DAMAGE HAS BEEN SUFFERED. THIS LIMITATION IS CUMULATIVE AND SHALL COVER THE TOTAL FOR ALL SUCH INCIDENTS AND CLAIMS. THE AFOREMENTIONED LIMITATIONS, EXCLUSIONS AND ANY DISCLAIMERS SHALL APPLY TO THE MAXIMUM EXTENT ALLOWABLE BY LAW, EVEN SHOULD ANY PROPOSED REMEDY FAIL OF ITS ESSENTIAL PURPOSE.

6. 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.

7. 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 DCR 52.227-19 of the Commercial Computer Software clause, as applicable.

8. DATA PRIVACY

8.01 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.

8.02 GDPR. For your rights according to European Union General Data Protection Regulation (GDPR) see Privacy Policy available under this website: https://www.smseagle.eu/privacy-policy/

9. MISCELLANEOUS

9.01 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.

9.02 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.

9.03 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.

9.04 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.

9.05 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.

9.06 **DISPUTE RESOLUTION**. All disputes arising from the present Agreement and/or in connection with it shall be finally decided with the Arbitration Court attached to the Czech Chamber of Commerce and the Agricultural Chamber of the Czech Republic according to its Rules by one arbitrator appointed by the President of the Arbitration Court.

9.07 **ASSIGNMENTS**. You may not transfer the SMSEagle device on which SMSEagle Software is installed unless the transferee agrees to the terms of this Agreement.

9.08 **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.

9.09 **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.

9.10 **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.

9.11 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.

10. 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
hello@smseagle.eu
support@smseagle.eu

01 GET READY TO START

What's In The Box

Your SMSEagle box contains:

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

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 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 23 cm (9 inches) from all persons and must not be co-located or operating in conjunction with antenna from any other transmitter.
- Antennas must not be installed inside metal cases.

Screw antennas to the antenna connector on the back of the enclosure of SMSEagle device.

STEP 2: Insert SIM Card

Please install SIM Card when the device is SWITCHED OFF. SIM Card slots is located on the front panel of the device. SIM metal contacts should face down when inserting SIM into slot.

STEP 3: Power the device

The device is powered with AC power cable delivered in the box. The device needs a power source of 100-240V AC.

STEP 4: Configure IP settings

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 and ETH1 port
- 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 /opt/smseagle/syscfg

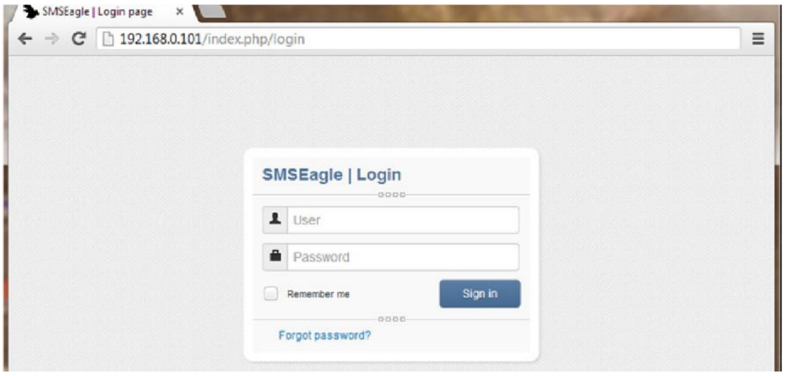
  change the following lines:

  ETH1_HOST_IP= (*set IP address for your device*)
  ETH1_GW_IP= (*default gateway IP address*)
  ETH1_NET_MASK= (*set subnet mask*)
  ETH1_START_DHCP=Y (*set to ETH1_START_DHCP=N to disable DHCP client*)
- save and exit the file
- shutdown the device
- now connect SMSEagle to your LAN using Ethernet cable

Current IP address can be read from the display on front panel.

C) **LOG IN** TO SMSEAGLE

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



192.168.0.101/index.php/login

SMSEAGLE DEFAULT USER:

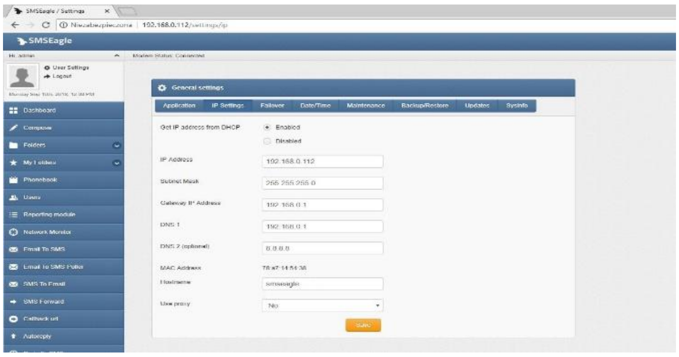
Username: admin

Password: password

Login to application with above username and password.

D) CONFIGURE STATIC IP SETTINGS IN WEB-GUI **(OPTIONAL)**

Click on menu position “Settings” and navigate to tab “IP Settings”.



Niezabezpieczona | 192.168.0.112/settings/ip

Modem Status: Connected

Get IP address from DHCP ● Enabled ○ Disabled

IP Address: 192.168.0.112

Subnet Mask: 255.255.255.0

Gateway IP Address: 192.168.0.1

DNS 1: 192.168.0.1

DNS 2 (optional): 8.8.8.8

MAC Address: 78:a7:14:54:38

Hostname: smseagle

Use proxy: No

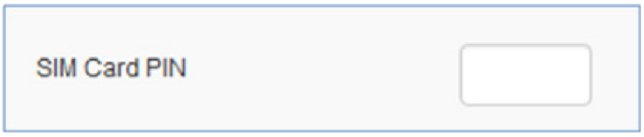
Disable DHCP server. Enter your IP settings. > Press “Save” button.

STEP 5: Setting SIM Cards PIN

This step should ONLY be done if your SIM-cards requires PIN.

If your SIM-card requires PIN number at startup, go to Settings > **Maintenance Tab.**

Enter your PIN number in the field “SIM Card PIN”



> Press “Save” button.

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

Installing your own SSL certificate

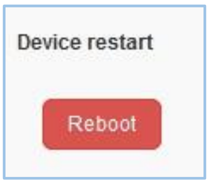
SMSEagle device comes with a self-signed SSL certificate. Follow the instructions in the chapter SSL Certificate and HTTPS Redirection if you want to install your own SSL certificate or a free Let’s Encrypt SSL certificate.

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

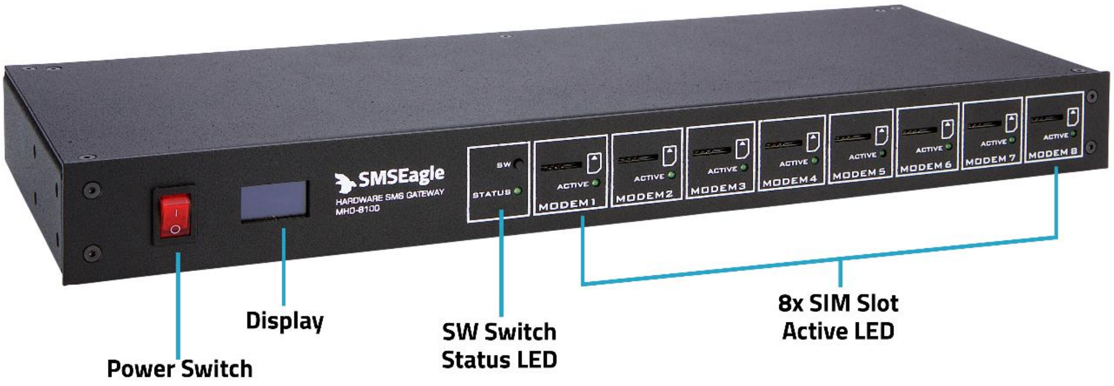
Go to Settings > Maintenance Tab. Press **Reboot** button.



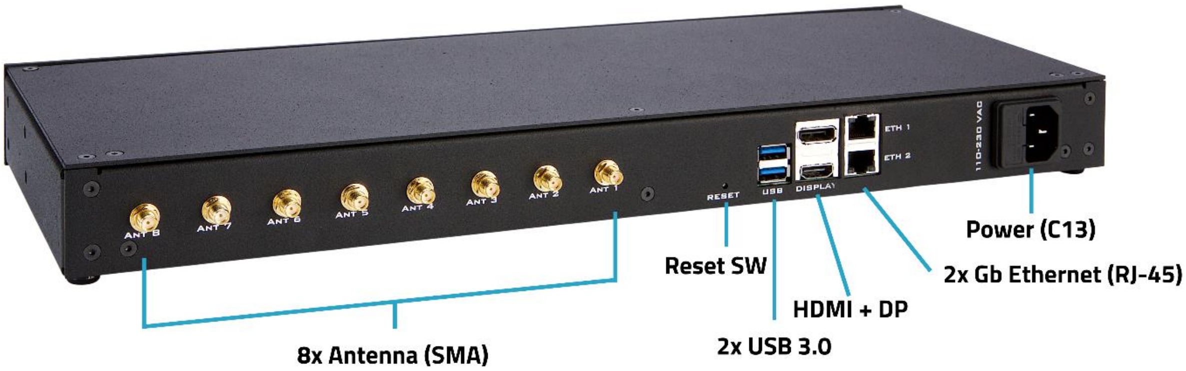
02 USING OF SMSEAGLE

GET TO KNOW CONNECTORS, PORTS AND LED'S

Front Panel



Back Panel

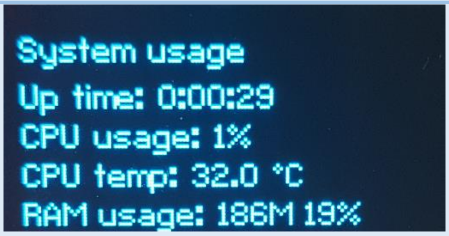
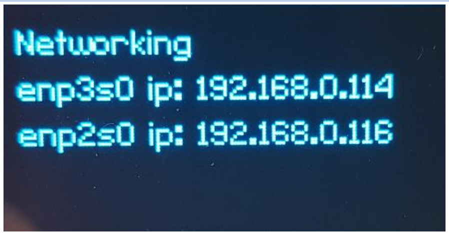
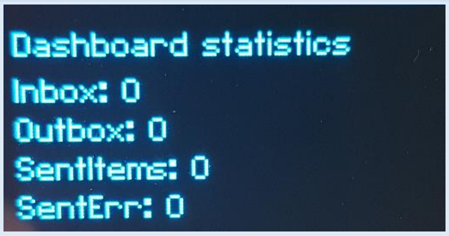


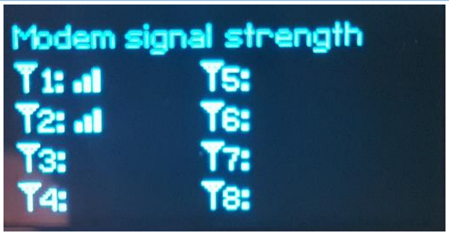
Element	Label	Description
Power switch	-	Power switch to turn on/off the device
Display	-	Display screen
User Switch	SW	Switch to toggle information on the display, restore settings to factory defaults
Status LED	STATUS	LED indicating device status
SIM slot	-	8x SIM slot - mini size
SIM Active LED	ACTIVE	8x LED indicator for modem status
Antenna	ANT1-8	Antenna socket (SMA)

Reset	RESET	Switch for rebooting the device
USB	USB	2x USB 3.0 port
Display ports	DISPLAY	HDMI & Display Port2.4.1.1._Sprawdzenie_działania_diod|out (for debugging purposes only)
Ethernet ports	ETH1-2	Gigabit Ethernet RJ45 ports
Power socket	110-230VAC	Power socket

Display

MHD-8100 display has 5 screens with different information on each screen. Using SW switch, you can change screens of the display.

Screen 1: SMSEagle Logo	 SMSEagle Hardware SMS Gateway
Screen 2: System Usage 1. Device power on time 2. CPU usage in % 3. CPU temperature in Celsius 4. RAM usage in Mb and %	 System usage Up time: 0:00:29 CPU usage: 1% CPU temp: 32.0 °C RAM usage: 186M 19%
Screen 3: Networking IP list	 Networking enp3s0 ip: 192.168.0.114 enp2s0 ip: 192.168.0.116
Screen 4: Dashboard Statistics list of messages in 1. Inbox 2. Outbox 3. Sentitems 4. Sent Errors	 Dashboard statistics Inbox: 0 Outbox: 0 SentItems: 0 SentErr: 0

Screen 5: Modem signal strength list of all modems	 Modem signal strength T1: .ıl T5: T2: .ıl T6: T3: T7: T4: T8:

Automatic power saving: The display will automatically turn off after 5min of inactivity (SW button is not pressed for 5min). To restore the display's work, simply press the SW button.

BASIC OPERATIONS

SMSEagle is capable to work in various screen resolutions, making it accessible for 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 previous chapter). At login screen type in your username/password. Default username and password is given in chapter **Prepare for First Start**.

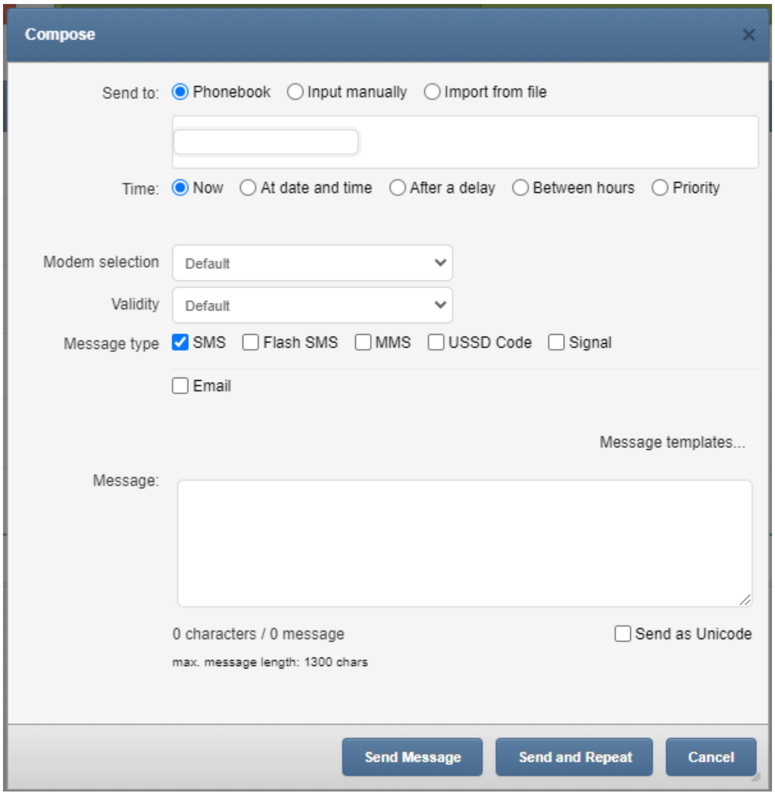
Important Notice: The Web-GUI requires a modern web browser with JavaScript support. Older web browsers (like Internet Explorer) are not supported and may not work properly.

SMSEAGLE BASIC FEATURES

- 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)

Compose SMS

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



Compose

Send to: ● Phonebook ○ Input manually ○ Import from file

Time: ● Now ○ At date and time ○ After a delay ○ Between hours ○ Priority

Modem selection: Default

Validity: Default

Message type: ☑ SMS □ Flash SMS □ MMS □ USSD Code □ Signal

□ Email

Message templates...

Message:

0 characters / 0 message

□ Send as Unicode

max. message length: 1300 chars

Screenshot of default Compose SMS view

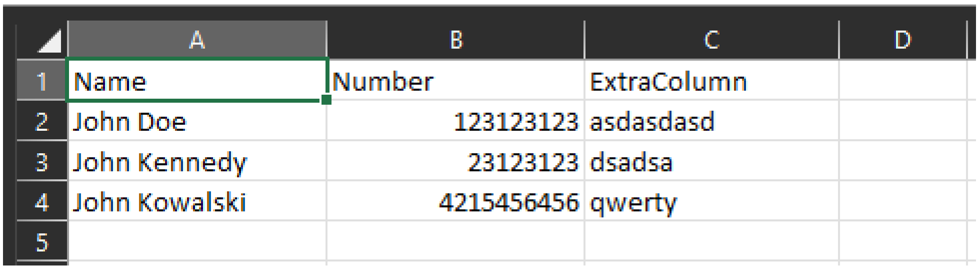
In Compose SMS users can:

- 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: SMS, normal, flash, MMS, USSD Code, Email or Signal
- 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

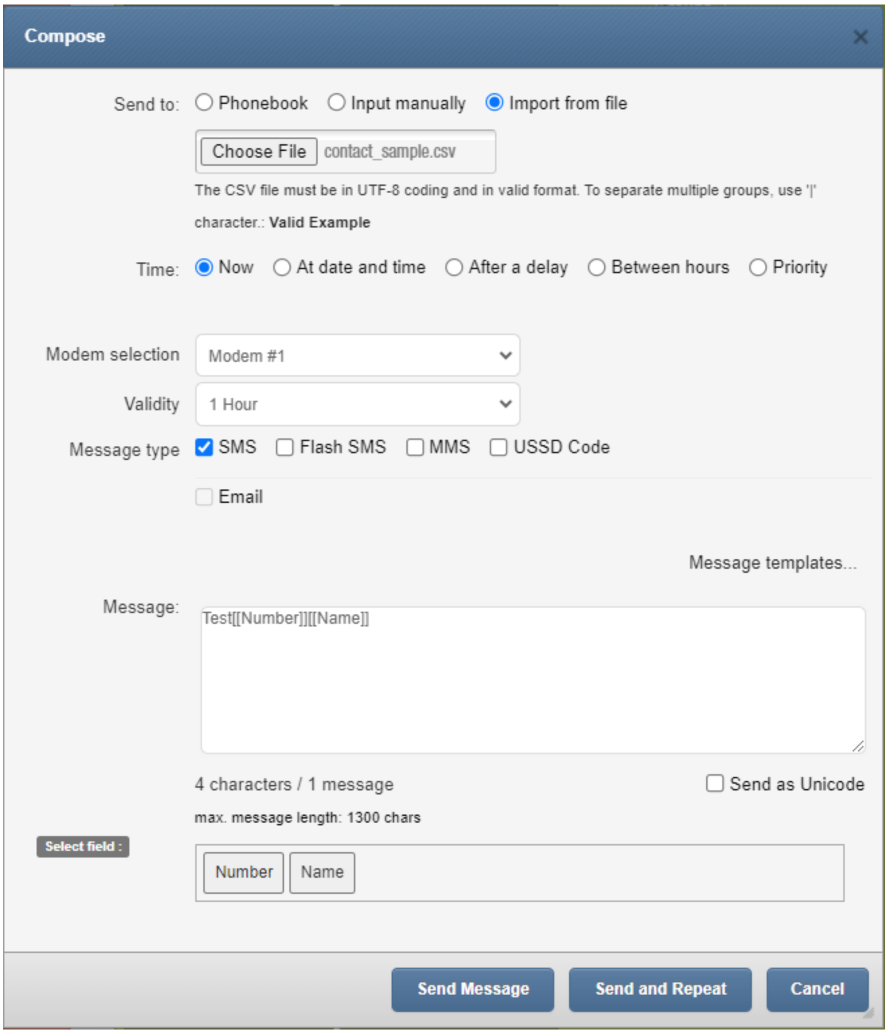
SMSEagle software allows you to import SMS text from CSV file and (optionally) use special placeholders in a message body. Placeholders are special fields which are replaced with unique values for each message.

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.



Compose

Send to: ○ Phonebook ○ Input manually ● Import from file

Choose File contact_sample.csv

The CSV file must be in UTF-8 coding and in valid format. To separate multiple groups, use '|' character.: **Valid Example**

Time: ● Now ○ At date and time ○ After a delay ○ Between hours ○ Priority

Modem selection: Modem #1

Validity: 1 Hour

Message type: ☑ SMS ☐ Flash SMS ☐ MMS ☐ USSD Code

☐ Email

Message templates...

Message: Test[[Number]][[Name]]

4 characters / 1 message ☐ Send as Unicode

max. message length: 1300 chars

Select field : Number Name

Screenshot of "Compose SMS" with imported .csv file.

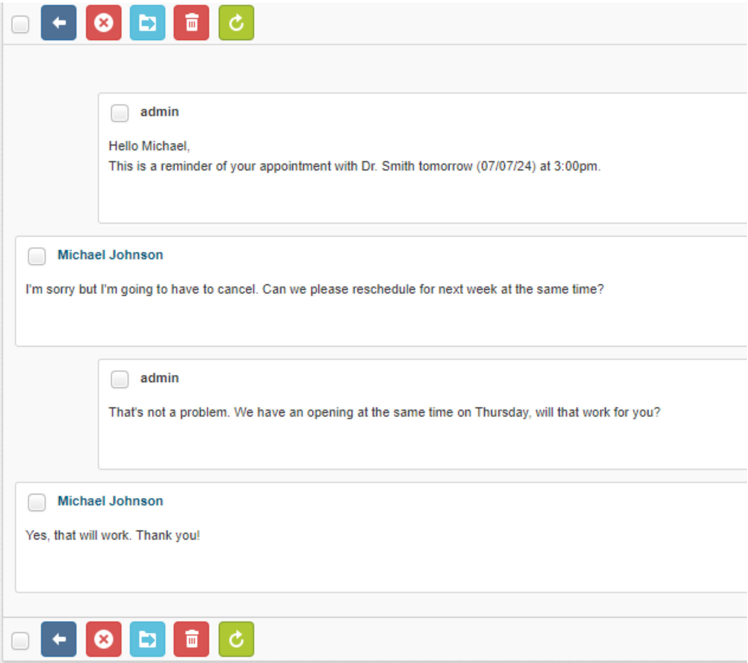
Folders

Folders contain your messages. They are conveniently grouped into 5 categories:

- Inbox
- Outbox
- Sent Items
- Spam
- 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:



□ admin

Hello Michael,
This is a reminder of your appointment with Dr. Smith tomorrow (07/07/24) at 3:00pm.

□ Michael Johnson

I'm sorry but I'm going to have to cancel. Can we please reschedule for next week at the same time?

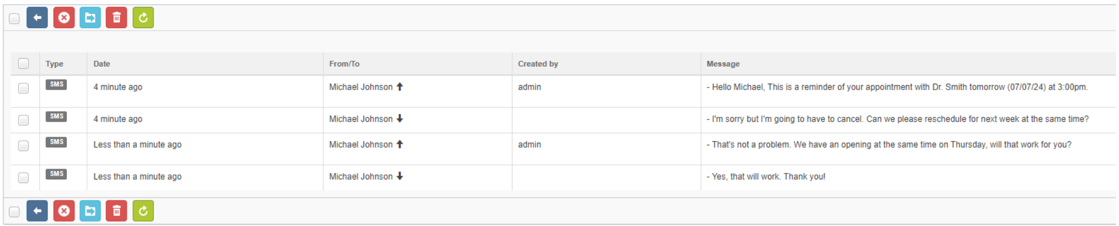
□ admin

That's not a problem. We have an opening at the same time on Thursday, will that work for you?

□ Michael Johnson

Yes, that will work. Thank you!

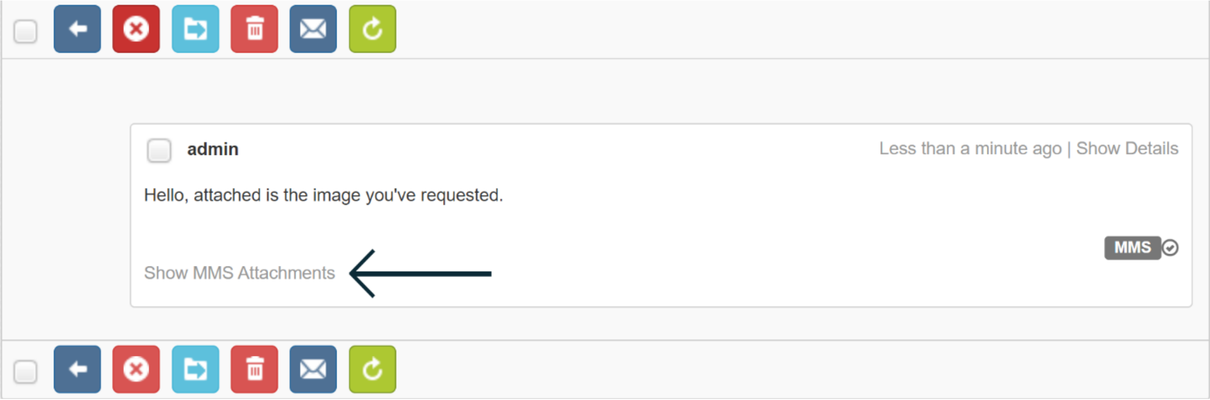
Table view type:



□	Type	Date	From/To	Created by	Message
□	SMS	4 minute ago	Michael Johnson ↑	admin	- Hello Michael, This is a reminder of your appointment with Dr. Smith tomorrow (07/07/24) at 3:00pm.
□	SMS	4 minute ago	Michael Johnson ↓		- I'm sorry but I'm going to have to cancel. Can we please reschedule for next week at the same time?
□	SMS	Less than a minute ago	Michael Johnson ↑	admin	- That's not a problem. We have an opening at the same time on Thursday, will that work for you?
□	SMS	Less than a minute ago	Michael Johnson ↓		- Yes, that will work. Thank you!

MMS

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



admin

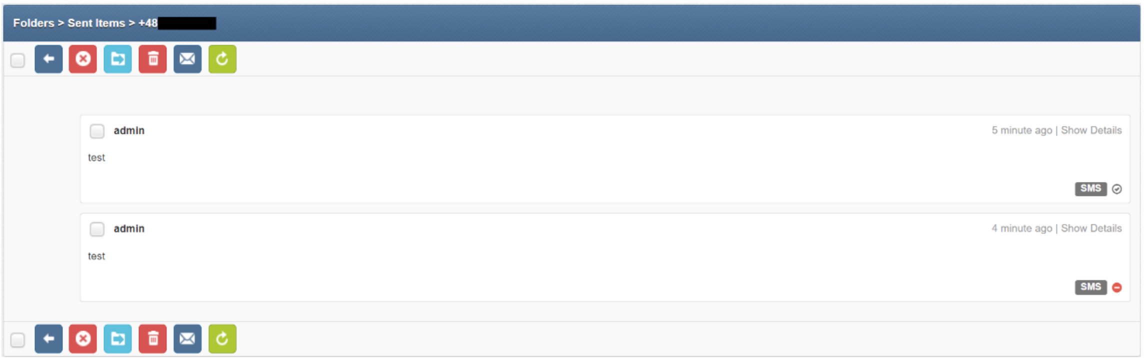
Less than a minute ago | Show Details

Hello, attached is the image you've requested.

Show MMS Attachments

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”).



Folders > Sent Items > +48[redacted]

admin

5 minute ago | Show Details

test

admin

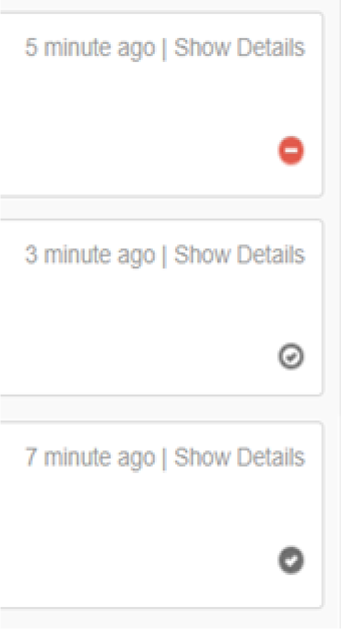
4 minute ago | Show Details

test

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)



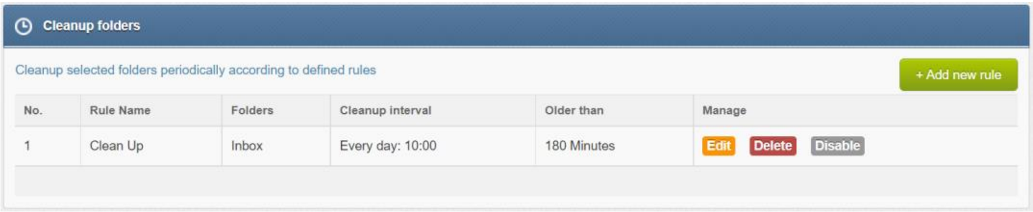
5 minute ago | Show Details

3 minute ago | Show Details

7 minute ago | Show Details

Cleanup Folders

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

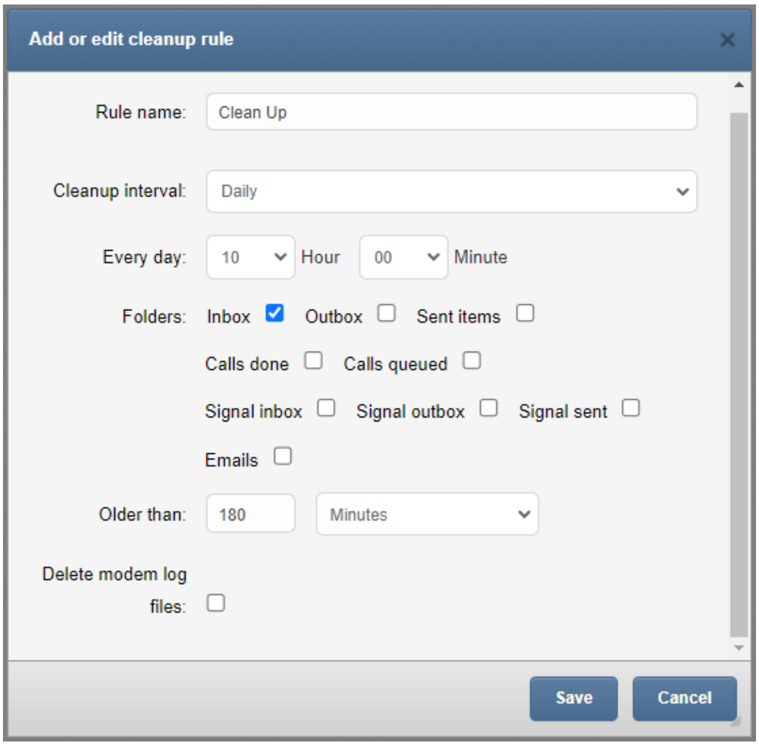


Cleanup folders

Cleanup selected folders periodically according to defined rules

No.	Rule Name	Folders	Cleanup interval	Older than	Manage
1	Clean Up	Inbox	Every day: 10:00	180 Minutes	Edit Delete Disable

Screenshot with example from Cleanup folders screen



Rule name: Clean Up

Cleanup interval: Daily

Every day: 10 Hour 00 Minute

Folders: Inbox ☑ Outbox □ Sent items □
Calls done □ Calls queued □
Signal inbox □ Signal outbox □ Signal sent □
Emails □

Older than: 180 Minutes

Delete modem log files: □

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, Call done, Calls queued, Signal inbox, Signal outbox, Signal sent or Emails)
- Set time span of messages
- Select to delete modem log files

Calls (Voice feature) *

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)

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 SMSEagle device will ring to a specified phone number or phonebook entry for a specified number of seconds.

TEXT-TO-SPEECH (TTS) CALLS **

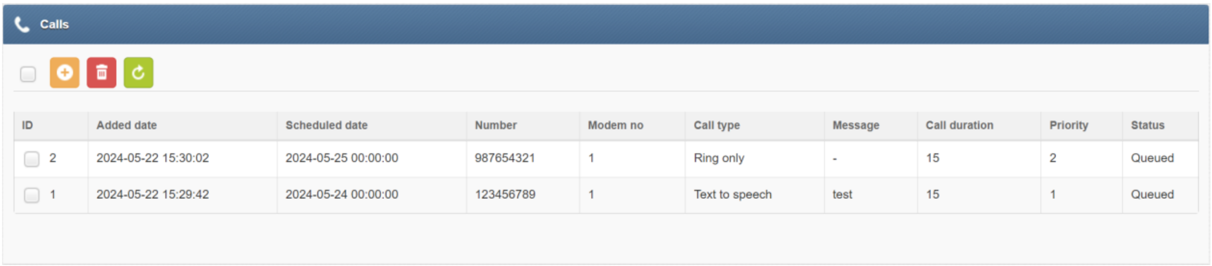
Text-To-Speech call allows converting of text message to voice call. This feature is particularly useful for businesses or organizations that must deliver important messages via voice. When a TTS call is made SMSEagle device will call a specified phone number or phonebook contact/group. The text message will be read by a built-in voice synthesizer. There are 2 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

Text to Speech Advanced feature has 2 pre-uploaded language models: English, German. You can upload additional voice models via the webGUI >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.

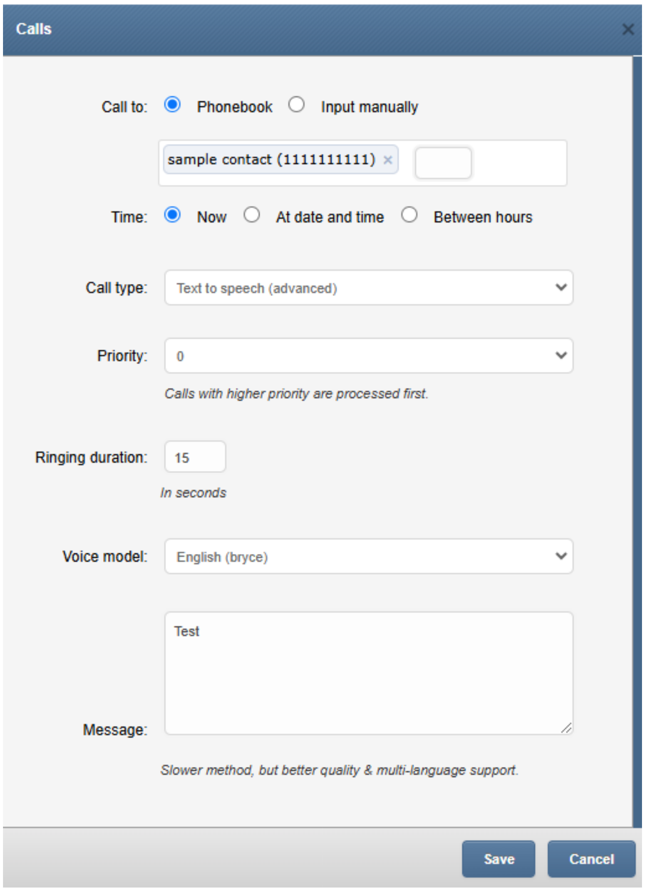
AUDIO FILE CALLS

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.



ID	Added date	Scheduled date	Number	Modem no	Call type	Message	Call duration	Priority	Status
□ 2	2024-05-22 15:30:02	2024-05-25 00:00:00	987654321	1	Ring only	-	15	2	Queued
□ 1	2024-05-22 15:29:42	2024-05-24 00:00:00	123456789	1	Text to speech	test	15	1	Queued

Screenshot with examples from "Calls" menu



Call to: ● Phonebook ○ Input manually

sample contact (1111111111) ×

Time: ● Now ○ At date and time ○ Between hours

Call type: Text to speech (advanced)

Priority: 0

Calls with higher priority are processed first.

Ringing duration: 15

In seconds

Voice model: English (bryce)

Message: Test

Slower method, but better quality & multi-language support.

Screenshot from New Call window

In New call window you can set:

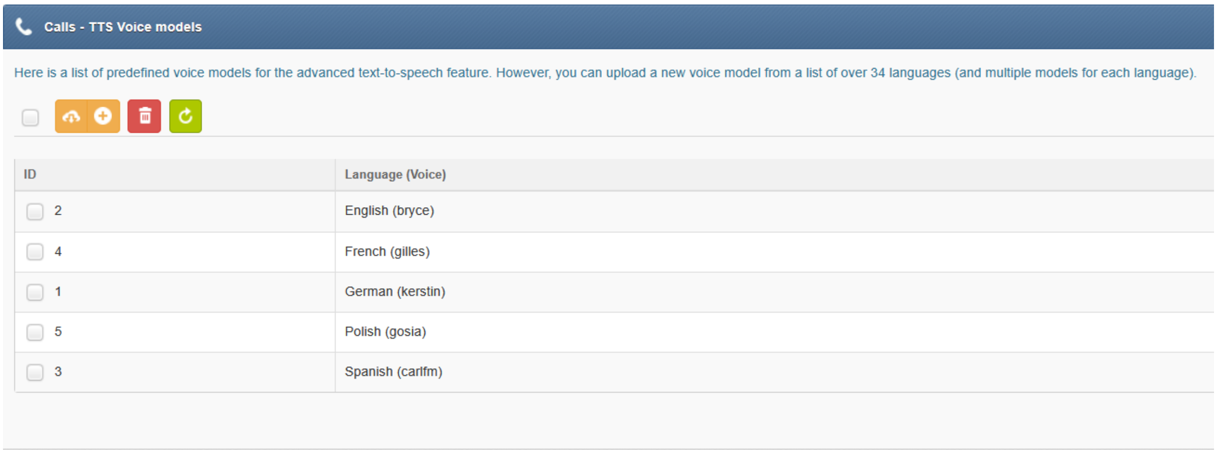
- Contact or group from Phonebook or manual input
- Select if a call should be made immediately, at a specified date/time, or between hours
- Which modem to call from (when using a multi-modem device)
- Set call priority from 0-5
- Select call type, Ring only, Text to Speech Simple, Text to Speech Advanced, Audio File
- For Text to Speech Advanced you can select language and voice model
- For Audio File you may select an existing file or upload a file from your computer
- Input message when Text-to-speech call type is selected. For "Text-to-Speech Simple" the length of the text message is limited to 950 characters.

RETRY ATTEMPTS

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

TTS VOICE MODELS

New voice models can be added semi-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).



Calls - TTS Voice models

Here is a list of predefined voice models for the advanced text-to-speech feature. However, you can upload a new voice model from a list of over 34 languages (and multiple models for each language).

ID	Language (Voice)
2	English (bryce)
4	French (gilles)
1	German (kerstin)
5	Polish (gosia)
3	Spanish (carlfm)

Screenshot from menu Calls>TTS Voice models

IMPORTANT NOTICE

*** Calls functions are only available to users who have purchased the *VOICE* add-on for their SMSEagle device.**

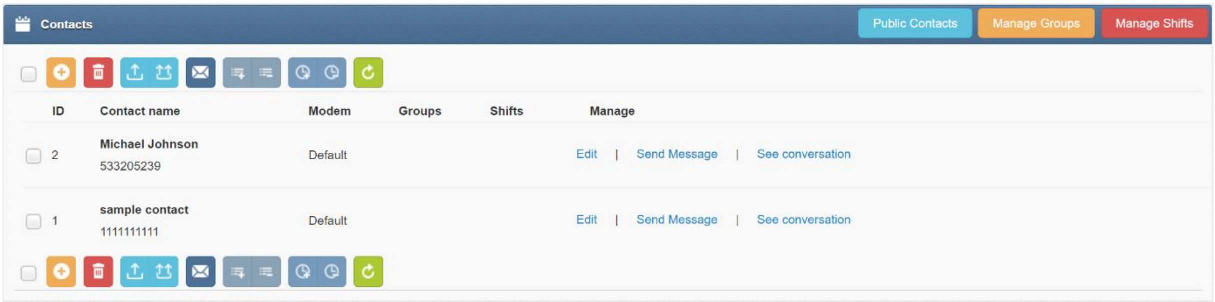
**** Due to technical limitations, the Text to Speech (TTS) and Audio Files function is only available on NXS hardware Rev. 4 and MHD-8100-4G devices.**

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.

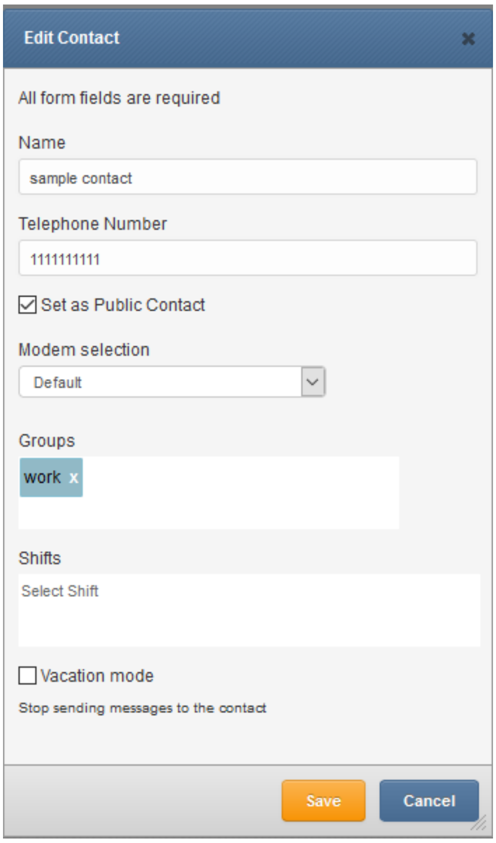


ID	Contact name	Modem	Groups	Shifts	Manage
2	Michael Johnson 533205239	Default			Edit | Send Message | See conversation
1	sample contact 1111111111	Default			Edit | Send Message | See conversation

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
- Send message to a contact
- Export selected contact or all contacts
- View message conversation of a contact



Edit Contact

All form fields are required

Name: sample contact

Telephone Number: 1111111111

☑ Set as Public Contact

Modem selection: Default

Groups: work x

Shifts: Select Shift

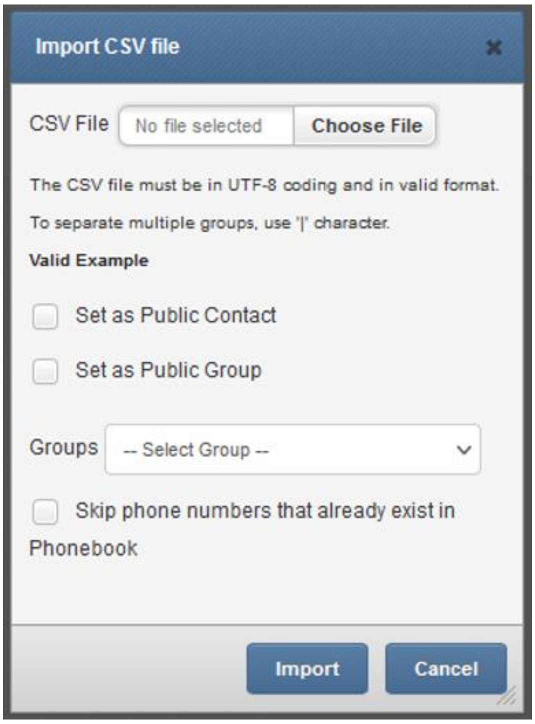
□ Vacation mode

Stop sending messages to the 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)



Import CSV file

CSV File: No file selected

The CSV file must be in UTF-8 coding and in valid format.

To separate multiple groups, use '|' character.

Valid Example

□ Set as Public Contact

□ Set as Public Group

Groups: -- Select Group --

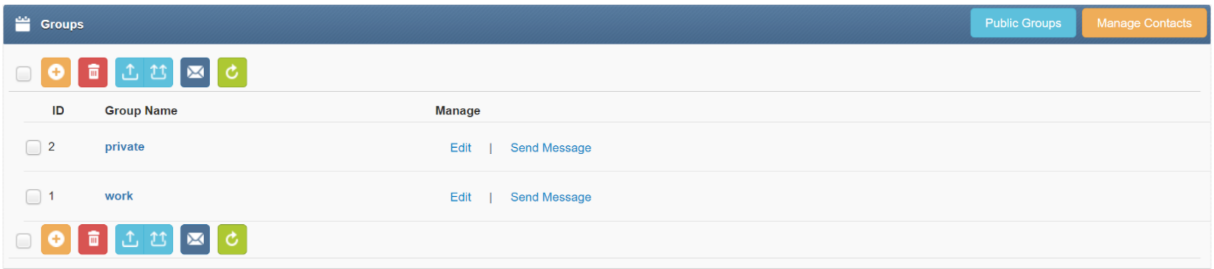
□ Skip phone numbers that already exist in Phonebook

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



Groups

	ID	Group Name	Manage
□	2	private	Edit | Send Message
□	1	work	Edit | Send Message

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 beloning to the group)
- Send message to a group

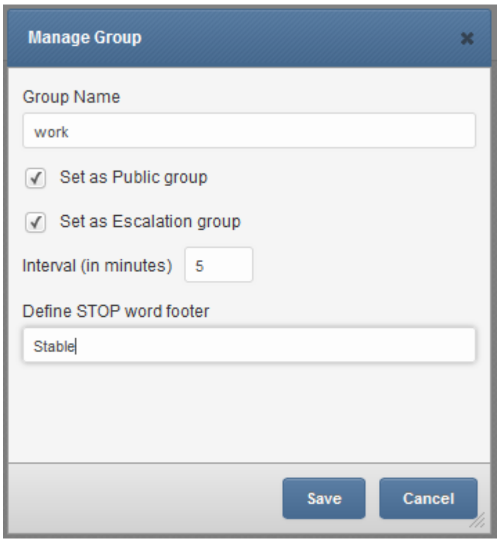
- Export selected groups or all groups

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.



Group Name: work

☑ Set as Public group

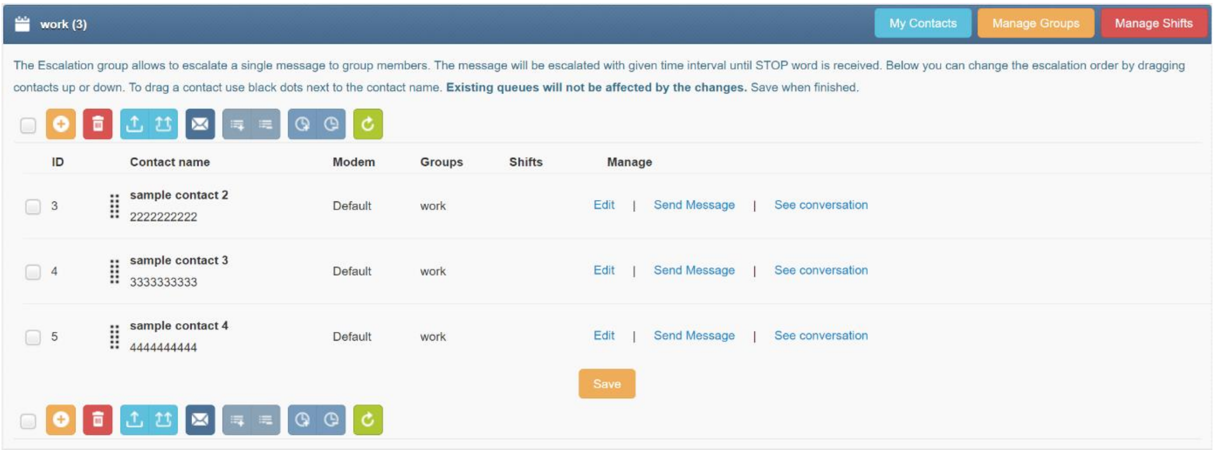
☑ Set as Escalation group

Interval (in minutes): 5

Define STOP word footer: Stable

Screenshot from Manage Group view

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

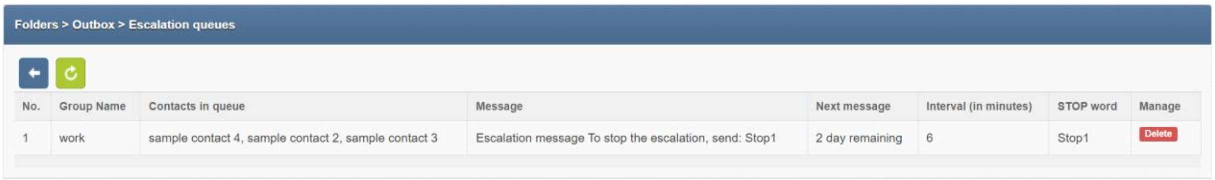


The Escalation group allows to escalate a single message to group members. The message will be escalated with given time interval until STOP word is received. Below you can change the escalation order by dragging contacts up or down. To drag a contact use black dots next to the contact name. **Existing queues will not be affected by the changes.** Save when finished.

	ID	Contact name	Modem	Groups	Shifts	Manage
□	3	**sample contact 2** 2222222222	Default	work		Edit | Send Message | See conversation
□	4	**sample contact 3** 3333333333	Default	work		Edit | Send Message | See conversation
□	5	**sample contact 4** 4444444444	Default	work		Edit | Send Message | See conversation

Screenshot from Manage Groups with set escalation

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



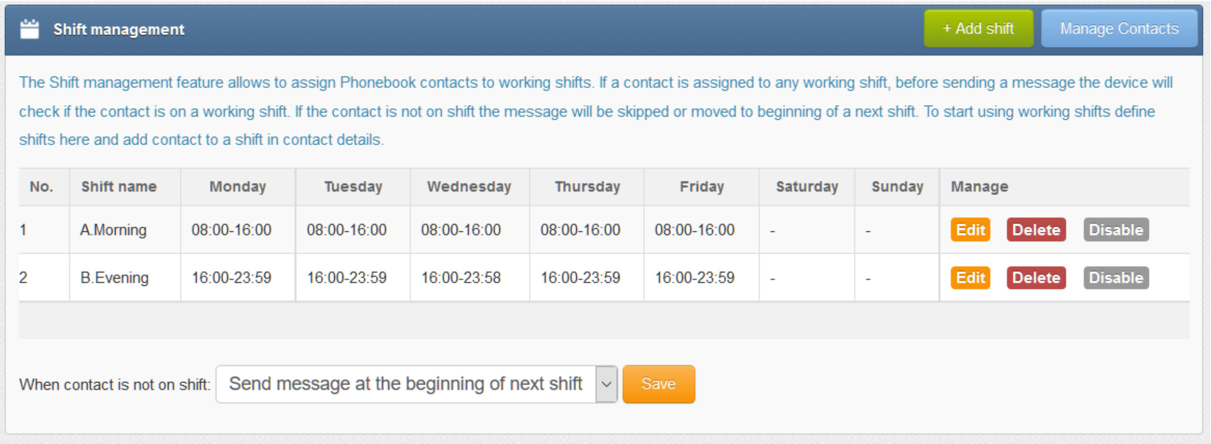
Folders > Outbox > Escalation queues

No.	Group Name	Contacts in queue	Message	Next message	Interval (in minutes)	STOP word	Manage
1	work	sample contact 4, sample contact 2, sample contact 3	Escalation message To stop the escalation, send: Stop1	2 day remaining	6	Stop1	Delete

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.



The Shift management feature allows to assign Phonebook contacts to working 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.

No.	Shift name	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Manage
1	A.Morning	08:00-16:00	08:00-16:00	08:00-16:00	08:00-16:00	08:00-16:00	-	-	Edit Delete Disable
2	B.Evening	16:00-23:59	16:00-23:59	16:00-23:58	16:00-23:59	16:00-23:59	-	-	Edit Delete Disable

When contact is not on shift: Send message at the beginning of next shift

Screenshot of shift management in phonebook

Users

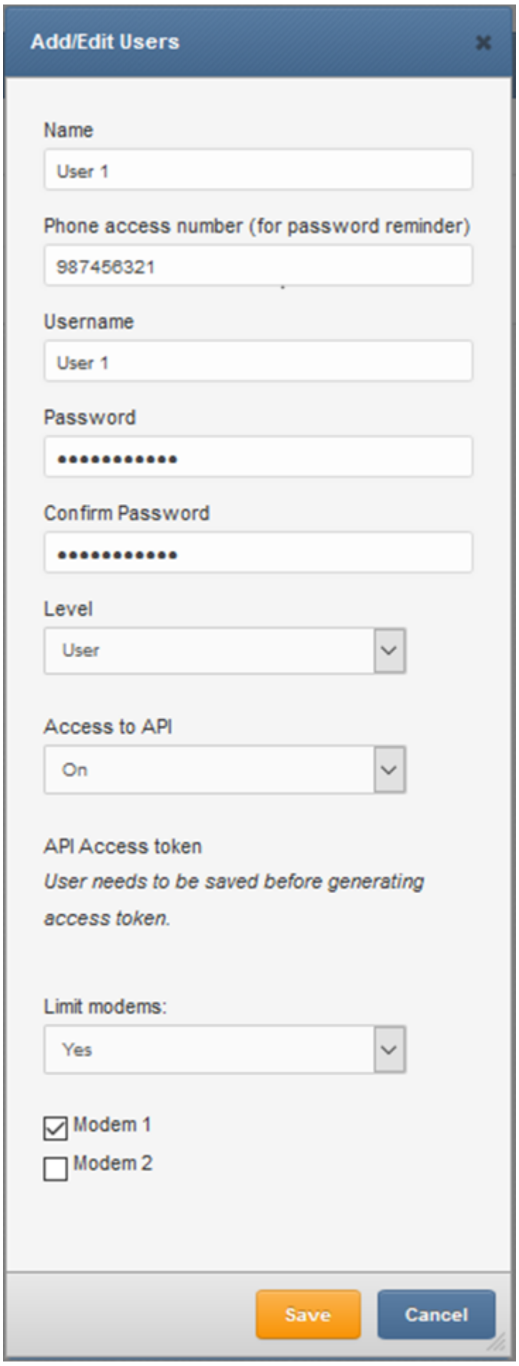
The Users function allows you to manage access to your device. It allows you to add, edit and remove users and set their permissions. There are two access levels for a user:

- 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

Screenshot of Edit/Add User window

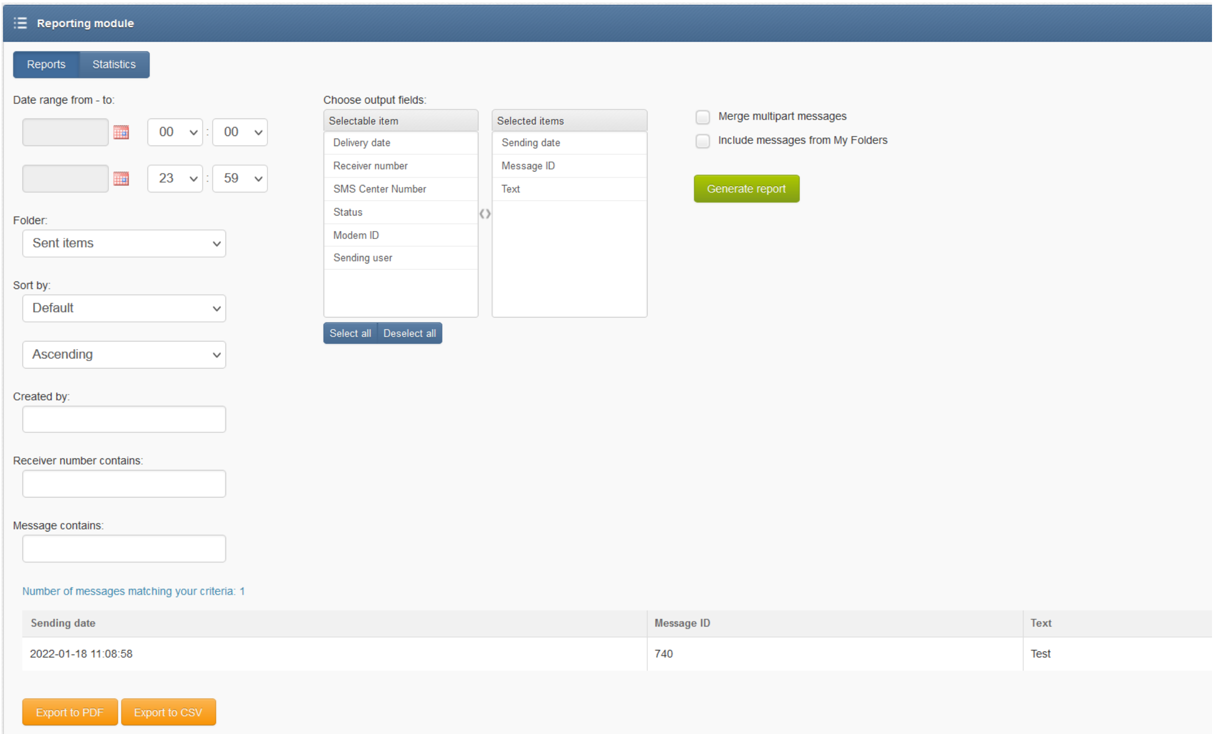
Multi-User Capabilities

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)*

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.



Date range from - to:

00 : 00

23 : 59

Folder: Sent items

Sort by: Default

Ascending

Created by:

Receiver number contains:

Message contains:

Choose output fields:

Selectable item	Selected items
Delivery date	Sending date
Receiver number	Message ID
SMS Center Number	Text
Status	
Modem ID	
Sending user	

☐ Merge multipart messages

☐ Include messages from My Folders

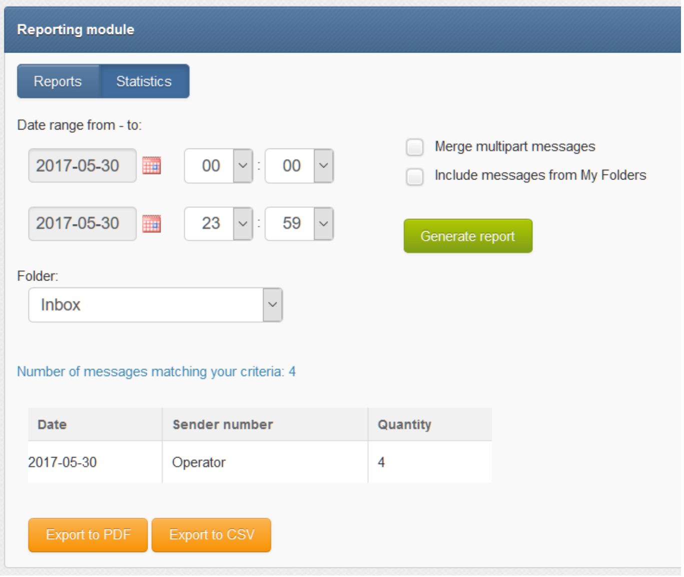
Number of messages matching your criteria: 1

Sending date	Message ID	Text
2022-01-18 11:08:58	740	Test

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.



Number of messages matching your criteria: 4

Date	Sender number	Quantity
2017-05-30	Operator	4

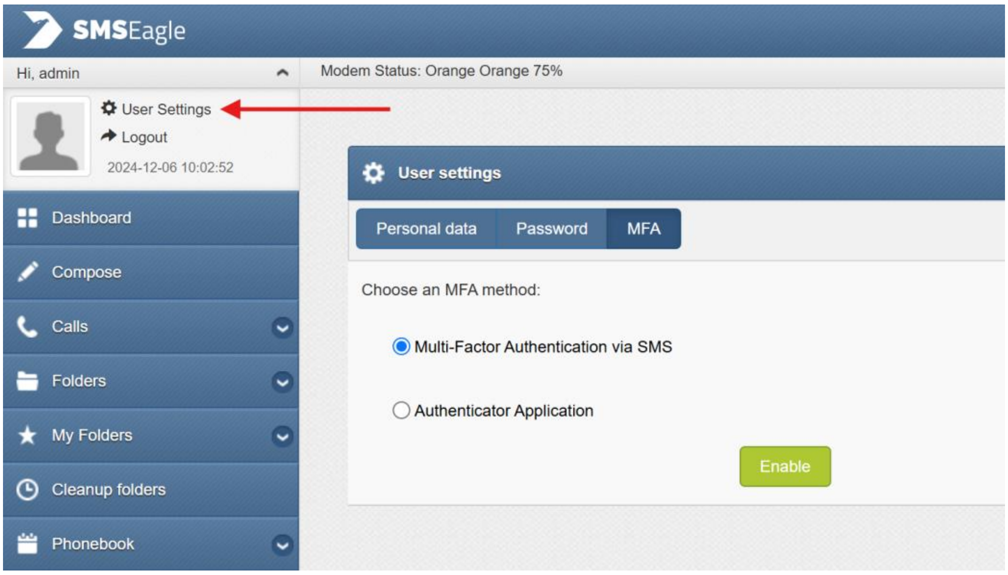
Screenshot of Statistics view in Reporting module

Multi-Factor Authentication

Multifactor Authentication (MFA) 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.



Choose an MFA method:

● Multi-Factor Authentication via SMS

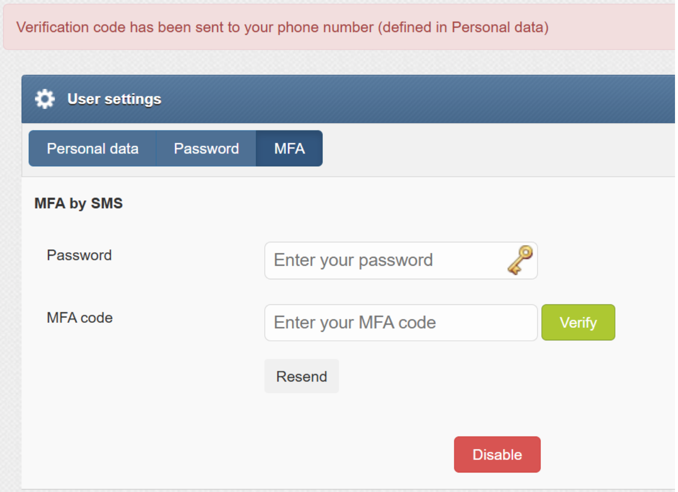
○ Authenticator Application

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.

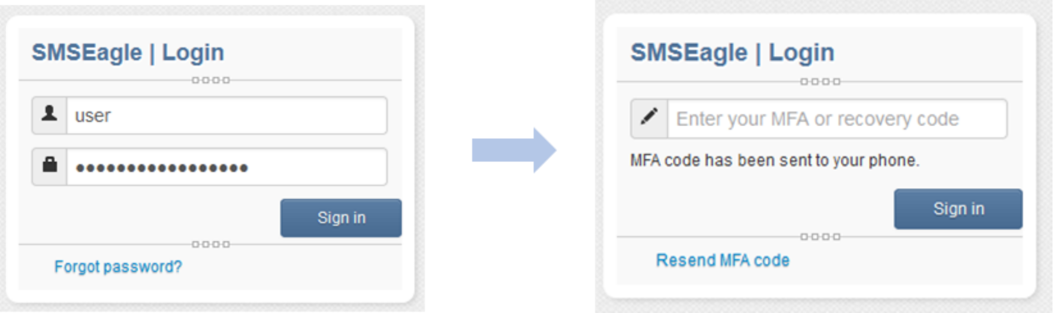


Verification code has been sent to your phone number (defined in Personal data)

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.

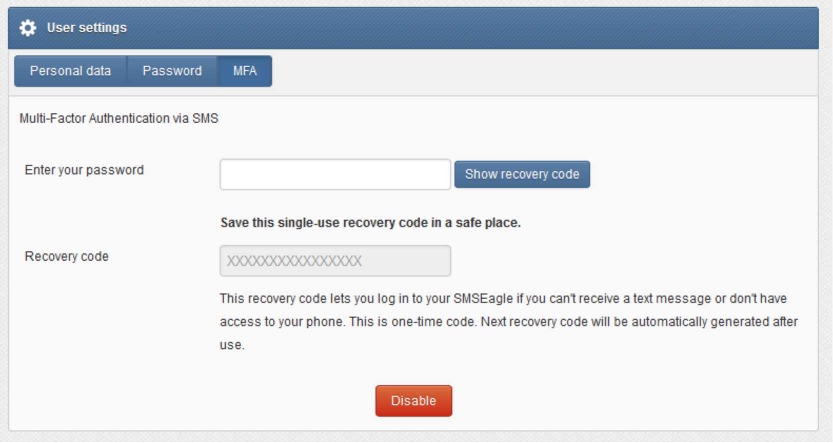


MFA code has been sent to your phone.

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.



Multi-Factor Authentication via SMS

Enter your password

Save this single-use recovery code in a safe place.

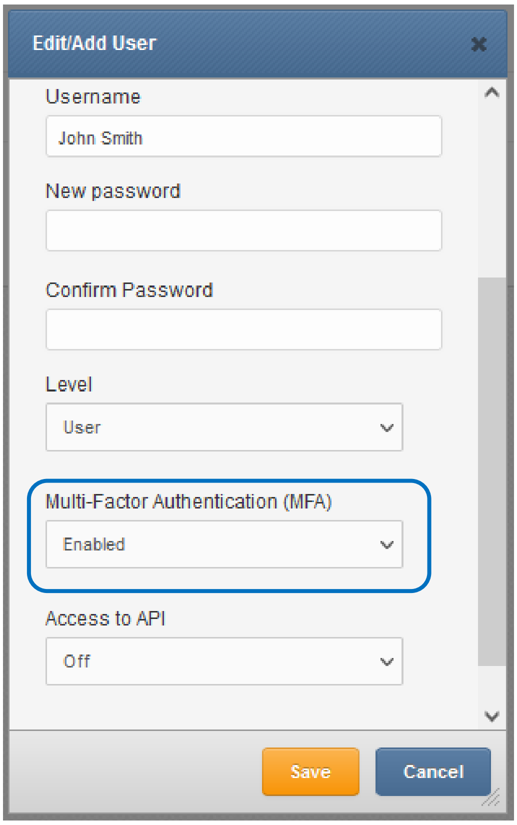
Recovery code: XXXXXXXXXXXXXXXX

This recovery code lets you log in to your SMSEagle if you can't receive a text message or don't have access to your phone. This is one-time code. Next recovery code will be automatically generated 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.



Edit/Add User

Username: John Smith

New password:

Confirm Password:

Level: User

Multi-Factor Authentication (MFA): Enabled

Access to API: Off

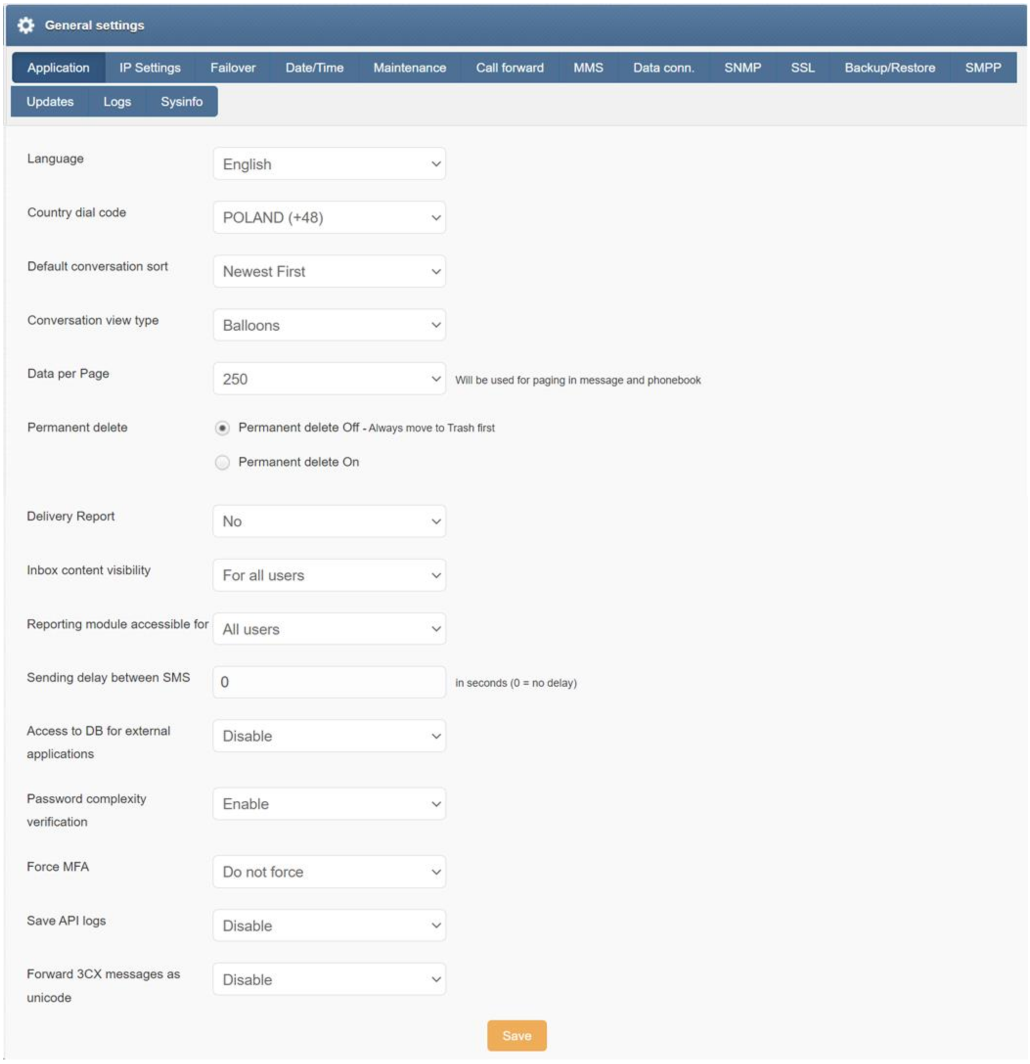
Screenshot from Edit/Add User

Settings

Settings menu is divided into several tabs for easier maintenance.

Application Settings

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



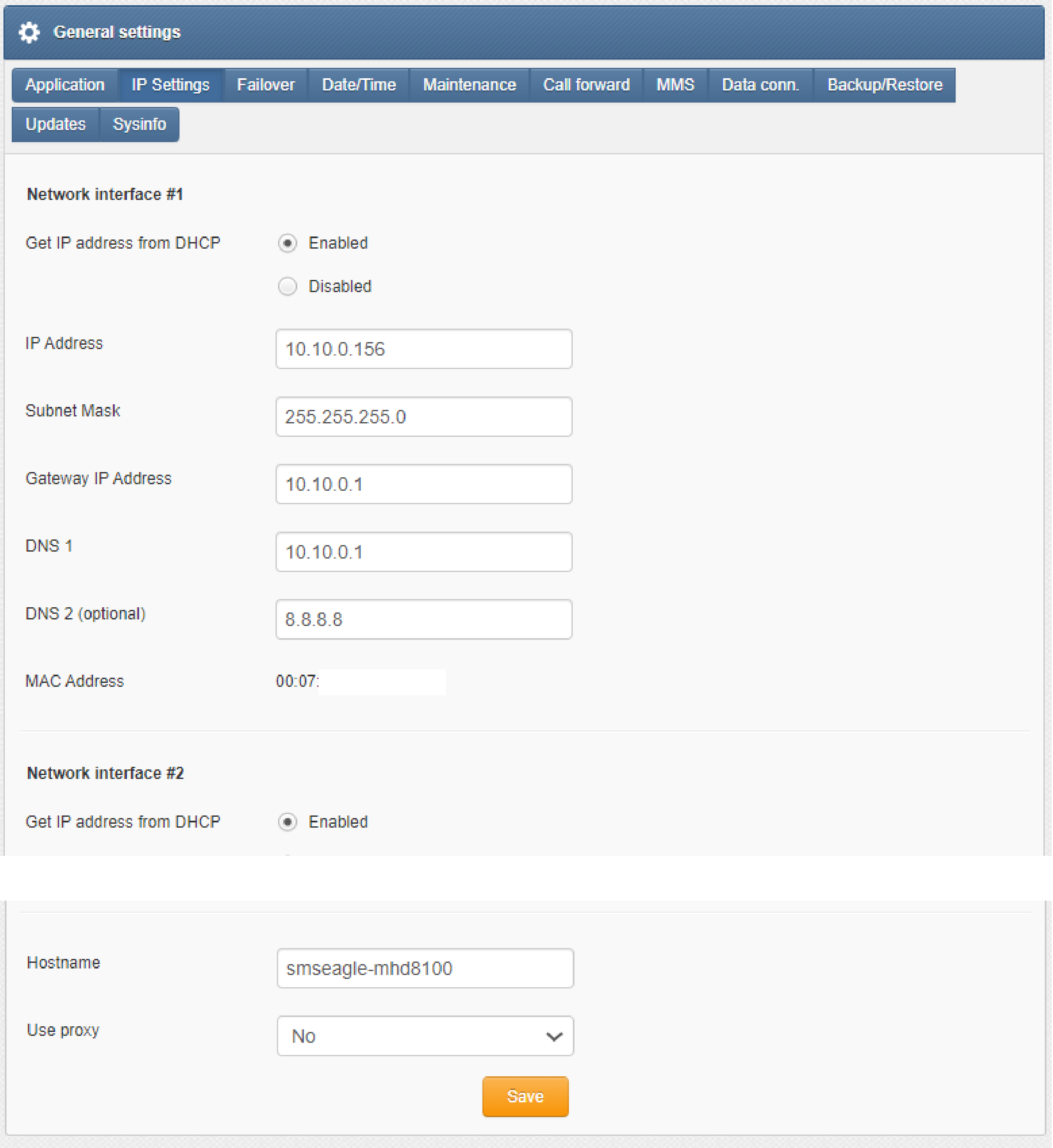
Language	English	
Country dial code	POLAND (+48)	
Default conversation sort	Newest First	
Conversation view type	Balloons	
Data per Page	250	Will be used for paging in message and phonebook
Permanent delete	● Permanent delete Off - Always move to Trash first ○ Permanent delete On	
Delivery Report	No	
Inbox content visibility	For all users	
Reporting module accessible for	All users	
Sending delay between SMS	0	in seconds (0 = no delay)
Access to DB for external applications	Disable	
Password complexity verification	Enable	
Force MFA	Do not force	
Save API logs	Disable	
Forward 3CX messages as unicode	Disable	

- 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.



Network interface #1

Get IP address from DHCP ● Enabled ○ Disabled

IP Address: 10.10.0.156

Subnet Mask: 255.255.255.0

Gateway IP Address: 10.10.0.1

DNS 1: 10.10.0.1

DNS 2 (optional): 8.8.8.8

MAC Address: 00:07:

Network interface #2

Get IP address from DHCP ● Enabled

Hostname: smseagle-mhd8100

Use proxy: No

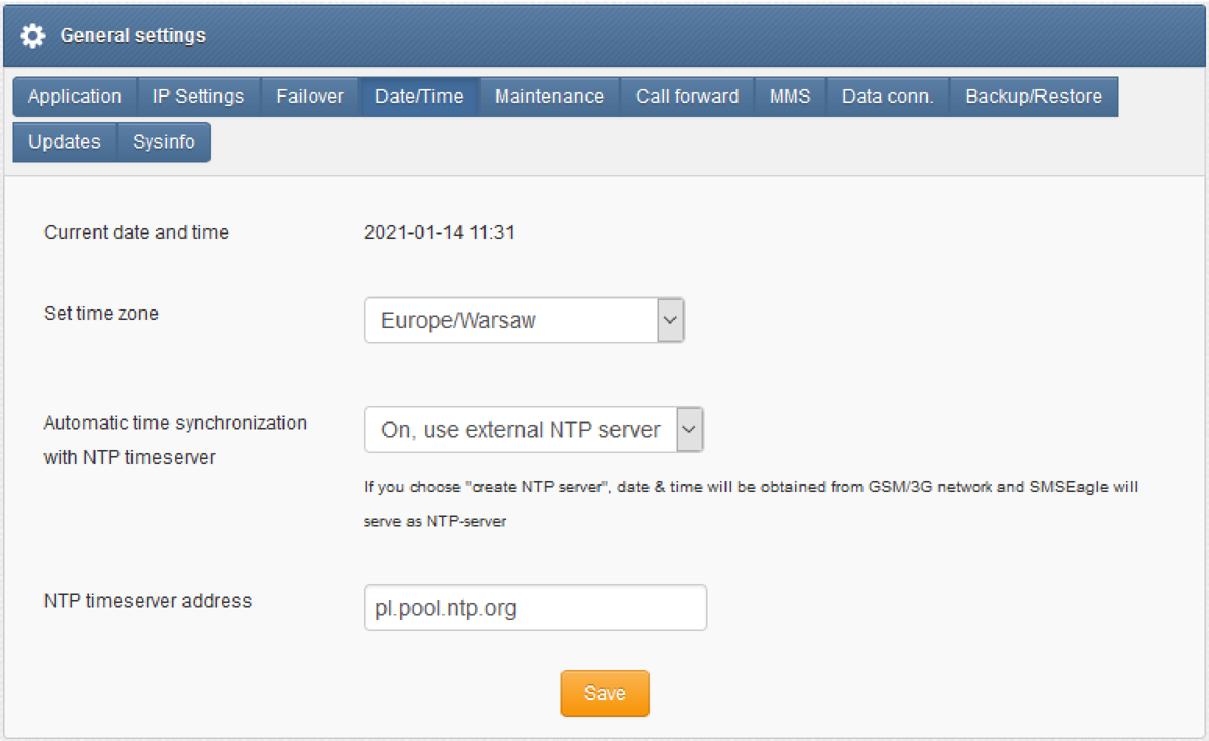
- You can enable or disable Get IP address from DHCP
- You can input the IP address
- You can input the Subnet Mast
- You can set the Gateway IP Address
- You can set DNS 1
- You can optionally set DNS 2
- You can view the MAC address of your device
- You can input Hostname
- You can choose to Use proxy

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



Current date and time: 2021-01-14 11:31

Set time zone: Europe/Warsaw

Automatic time synchronization with NTP timeserver: On, use external NTP server

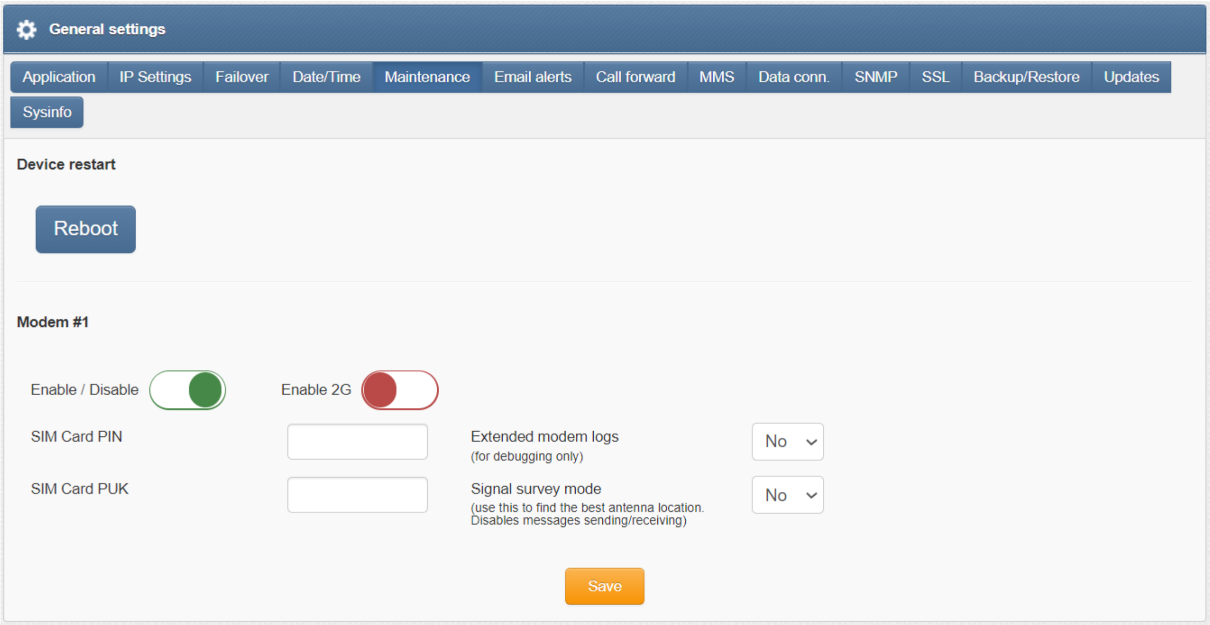
If you choose "create NTP server", date & time will be obtained from GSM/3G network and SMSEagle will serve as NTP-server

NTP timeserver address: pl.pool.ntp.org

- 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 modem software (debug mode)
- You can enable signal survey mode (for finding the best antenna location)

Multimodem settings are described in chapter Multimodem features.

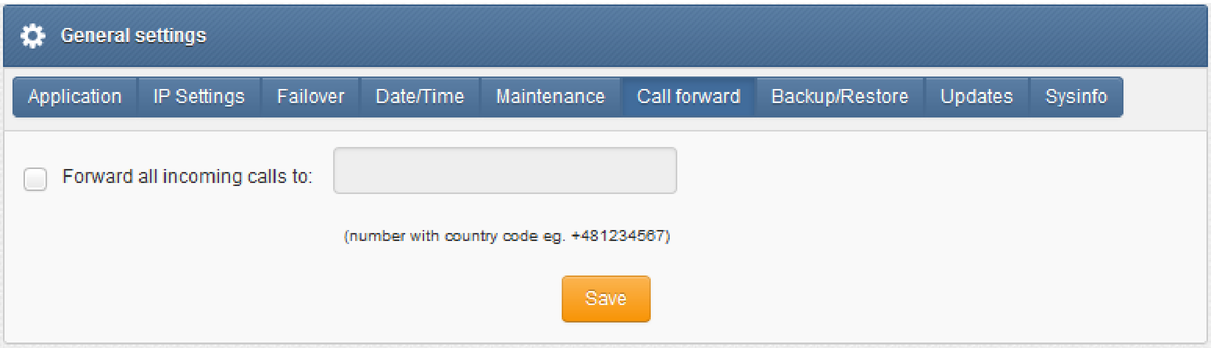
SIGNAL SURVEY MODE

This feature allows you to find the best location of 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 location of 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.



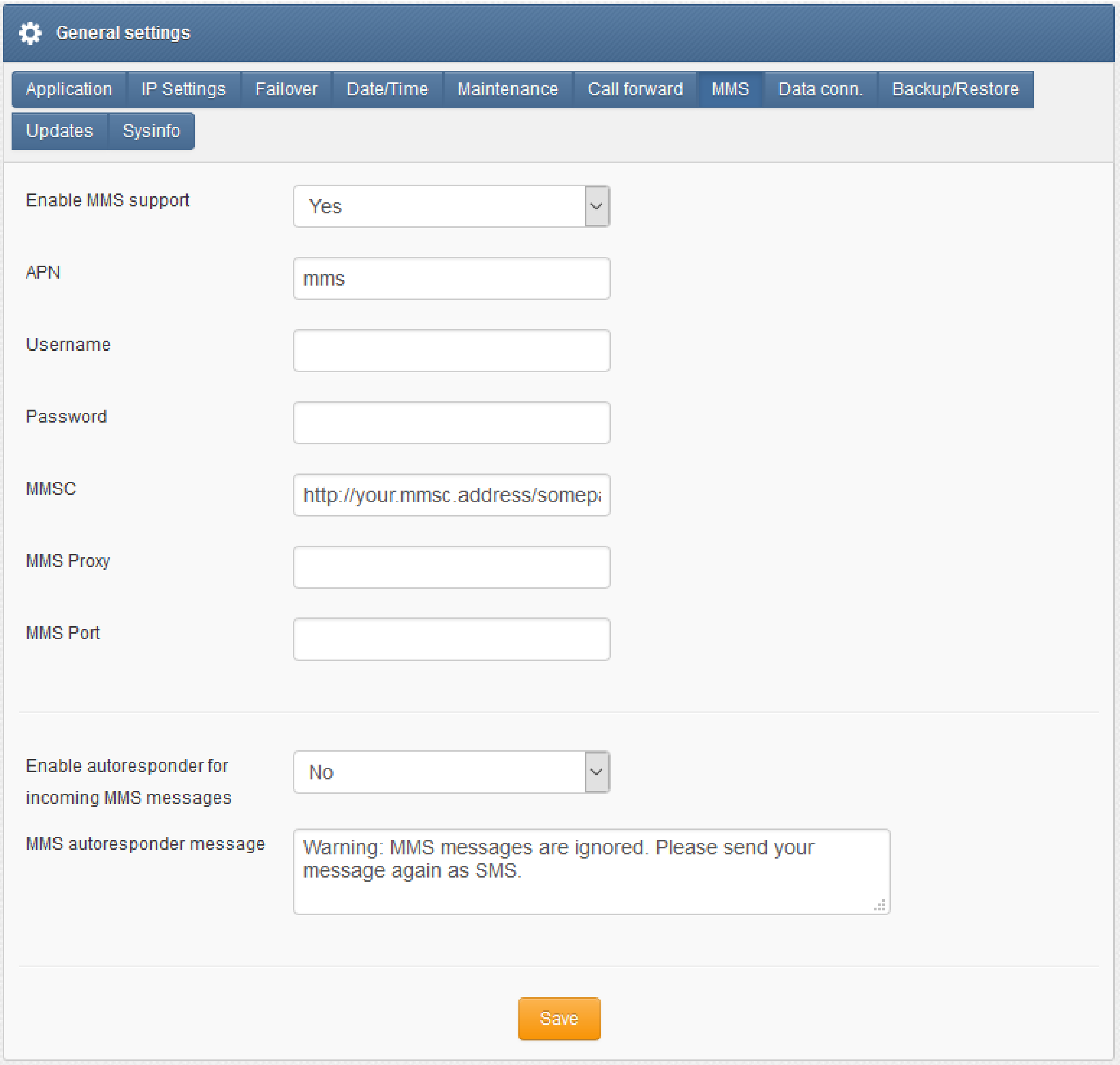
□ Forward all incoming calls to:

(number with country code eg. +481234567)

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

MMS

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



Enable MMS support: Yes

APN: mms

Username:

Password:

MMSC: http://your.mmsc.address/somep

MMS Proxy:

MMS Port:

Enable autoresponder for incoming MMS messages: No

MMS autoresponder message: Warning: MMS messages are ignored. Please send your message again as SMS.

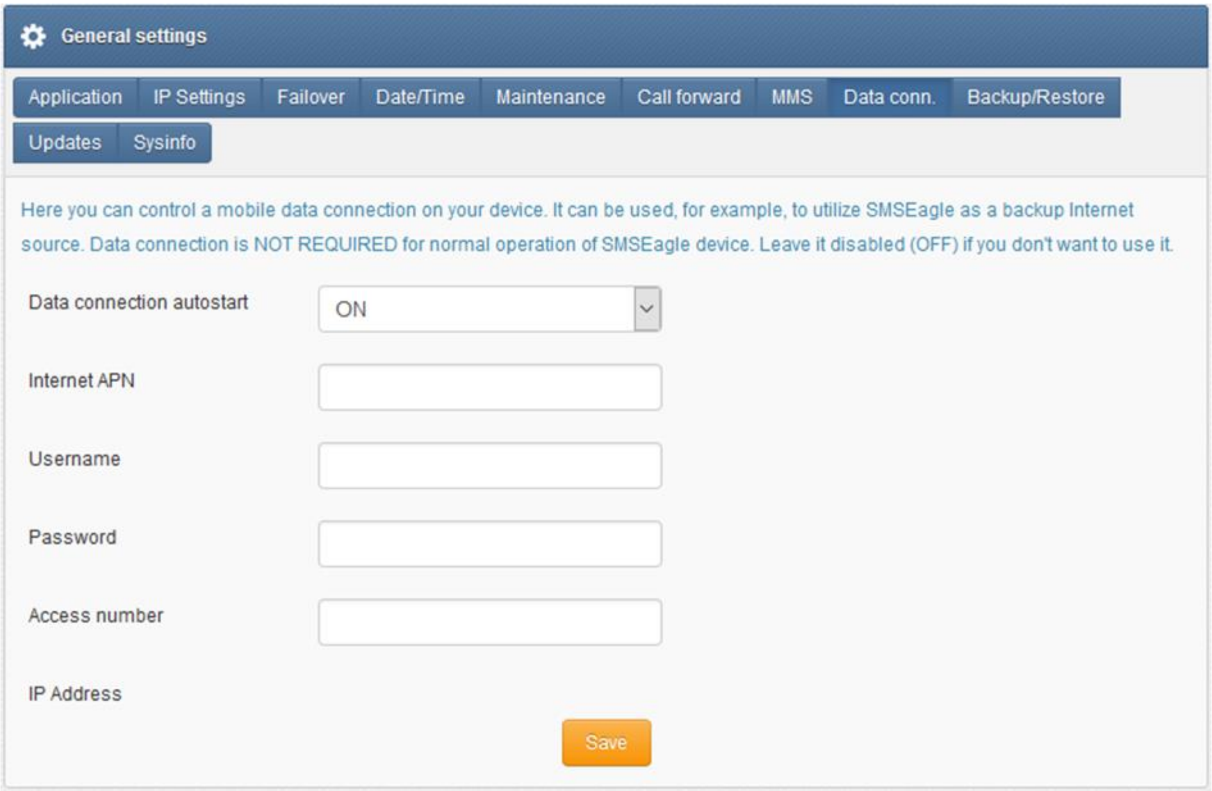
- You can enable MMS support
- You can set APN value
- You can input APN username
- You can input APN password
- You can set MMSC
- You can set MMS Proxy
- You can set MMS Port
- You can set autoresponder for incoming MMS messages
- You can input MMS autoresponder message

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.



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.

Data connection autostart	ON
Internet APN	
Username	
Password	
Access number	
IP Address	

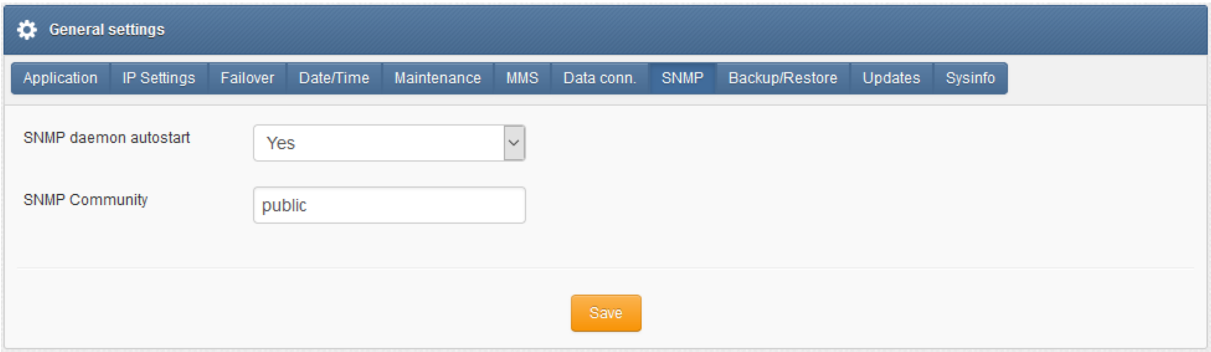
- You can choose to autorestart data connection
- You can input Internet APN
- You can input APN username

- 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



SNMP daemon autostart: Yes

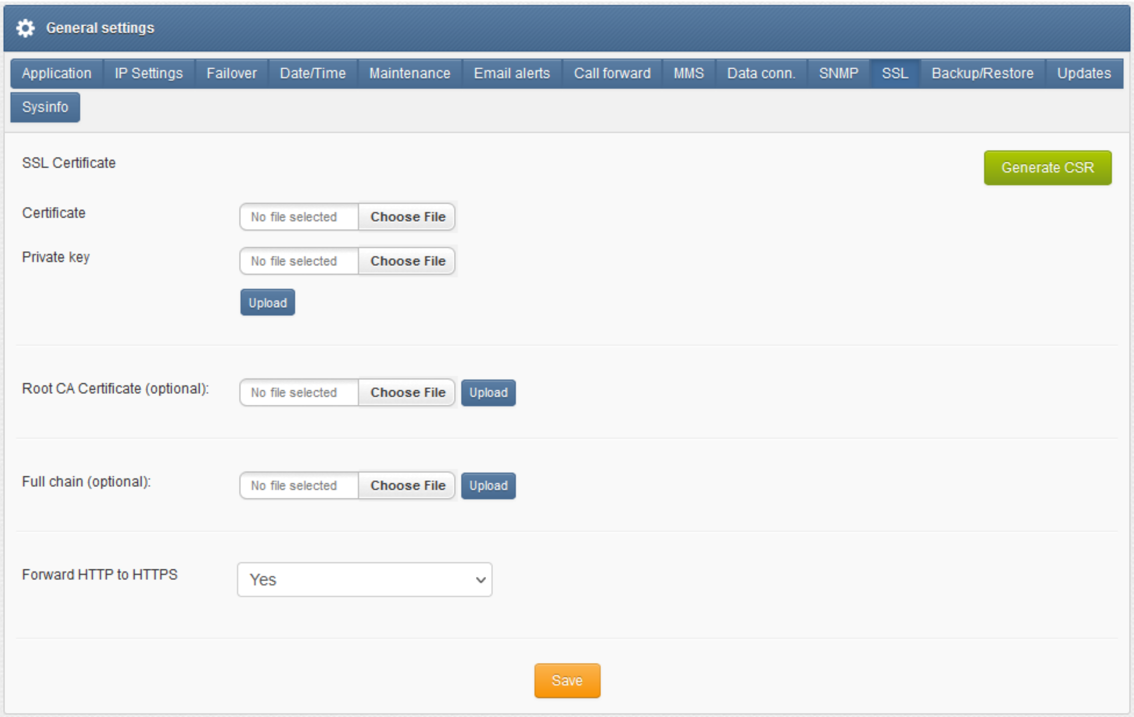
SNMP Community: public

- 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

Certificate: No file selected

Private key: No file selected

Root CA Certificate (optional): No file selected

Full chain (optional): No file selected

Forward HTTP to HTTPS: Yes

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".

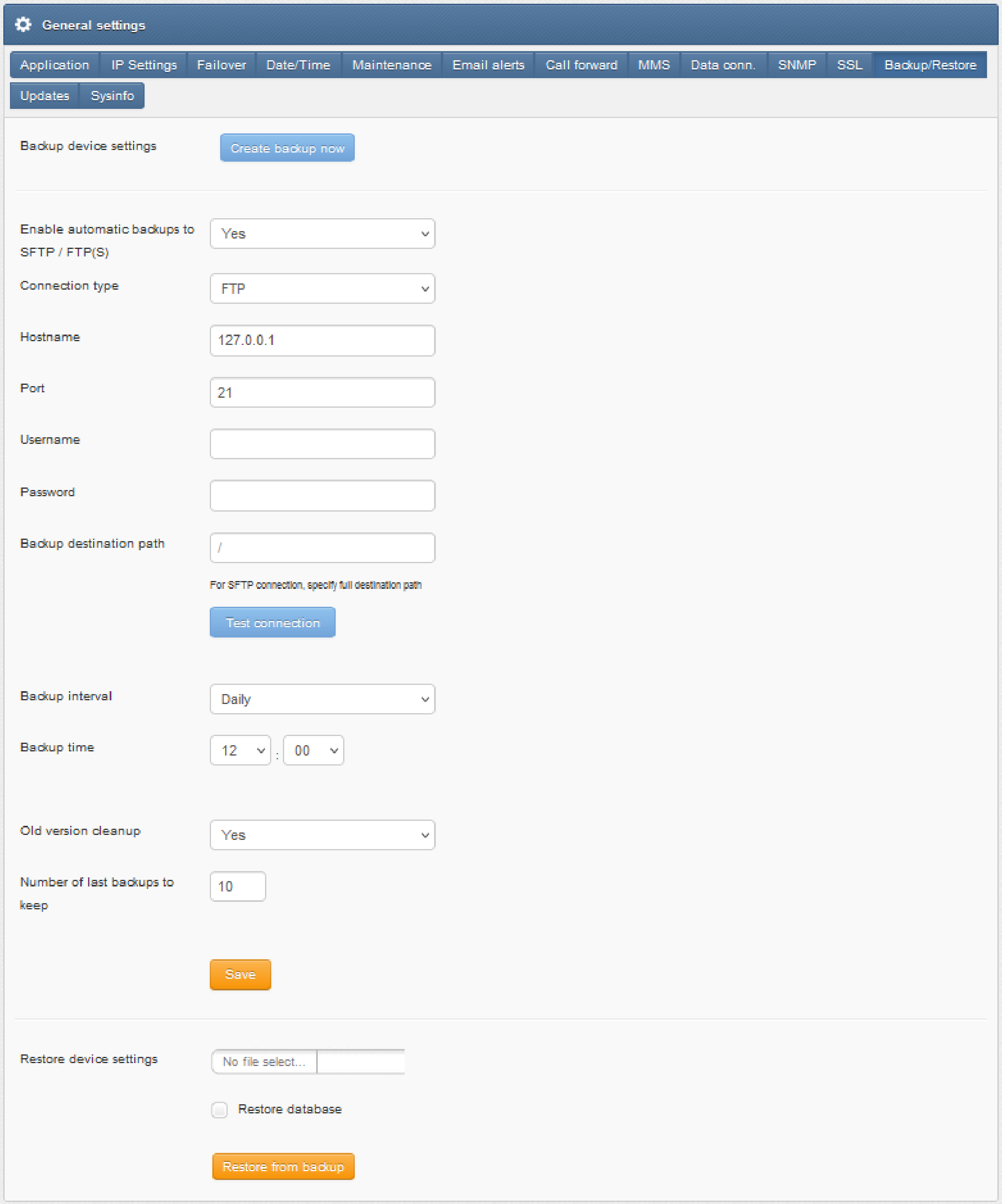
Generate CSR

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



Backup device settings

Enable automatic backups to SFTP / FTP(S): Yes

Connection type: FTP

Hostname: 127.0.0.1

Port: 21

Username:

Password:

Backup destination path: /

For SFTP connection, specify full destination path

Backup interval: Daily

Backup time: 12 : 00

Old version cleanup: Yes

Number of last backups to keep: 10

Restore device settings: No file select...

□ Restore database

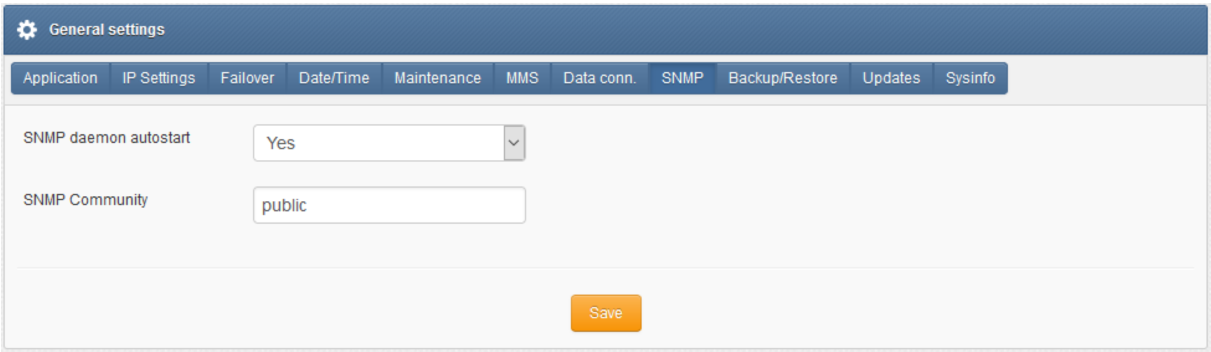
- You can create a backup of your device settings
- You can enable automatic backup to SFTP/FTP(S)
    - You can set automatic backup interval (daily/weekly/monthly) and time

  - 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.*

SNMP

SNMP Settings can be accessed under the Settings tab > SNMP



SNMP daemon autostart: Yes

SNMP Community: public

- 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 **Błąd! Nie można odnaleźć źródła odwołania.** chapter.

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.

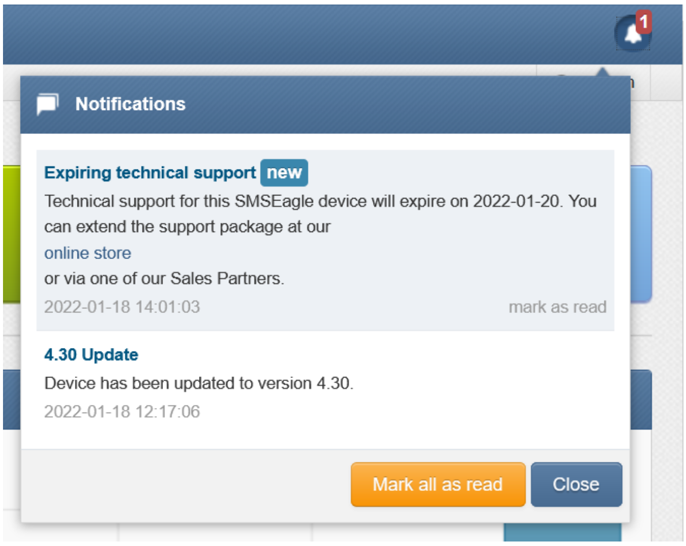
AUTOMATIC CHECK

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.



Expiring technical support new

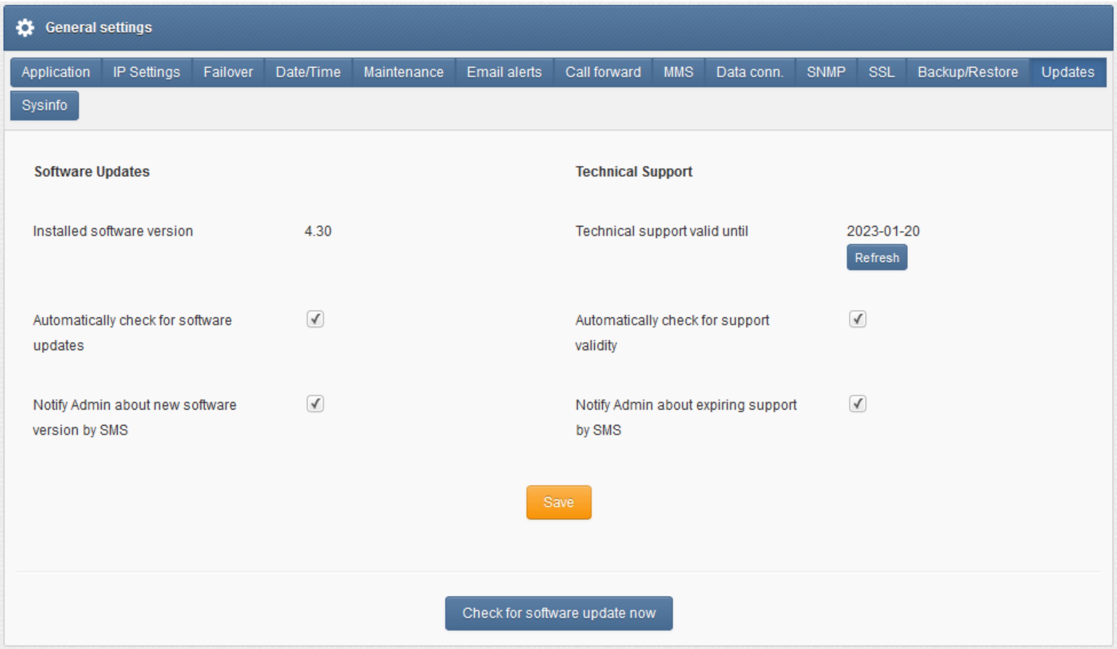
Technical support for this SMSEagle device will expire on 2022-01-20. You can extend the support package at our
online store
or via one of our Sales Partners.

2022-01-18 14:01:03 mark as read

4.30 Update

Device has been updated to version 4.30.

2022-01-18 12:17:06



Software Updates

Installed software version 4.30

Automatically check for software updates ☑

Notify Admin about new software version by SMS ☑

Technical Support

Technical support valid until 2023-01-20

Automatically check for support validity ☑

Notify Admin about expiring support by SMS ☑

Screenshot from "General Settings-Updates"

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

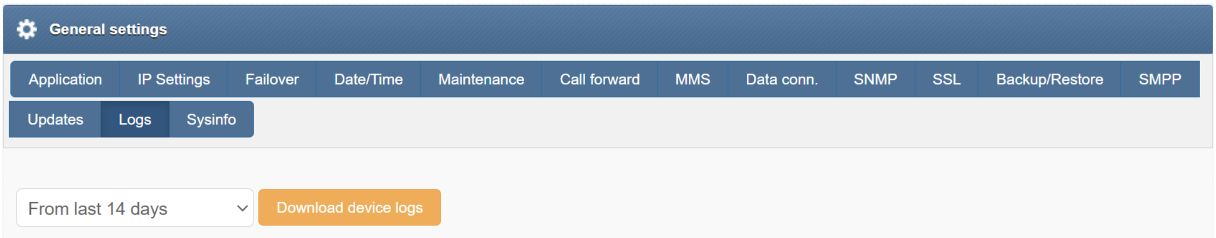
Logs

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

The following device logs are available via web-GUI:

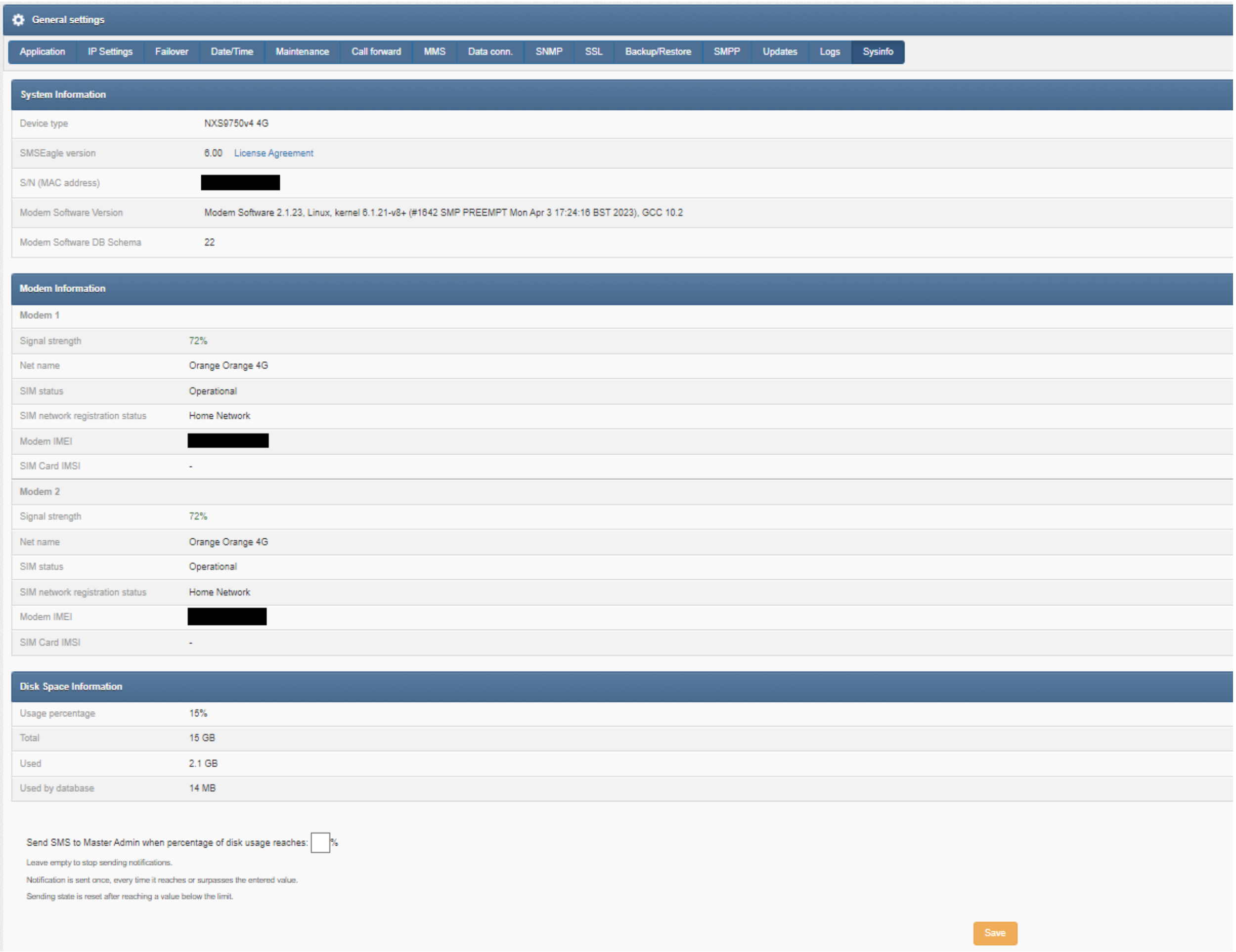
1. Modem log
2. Database log
3. System log
4. Application log

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



Sysinfo

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



System Information	
Device type	NXS9750v4 4G
SMSEagle version	6.00 License Agreement
S/N (MAC address)	[redacted]
Modem Software Version	Modem Software 2.1.23, Linux, kernel 6.1.21-v8+ (#1642 SMP PREEMPT Mon Apr 3 17:24:16 BST 2023), GCC 10.2
Modem Software DB Schema	22

Modem Information	
Modem 1	
Signal strength	72%
Net name	Orange Orange 4G
SIM status	Operational
SIM network registration status	Home Network
Modem IMEI	[redacted]
SIM Card IMSI	-
Modem 2	
Signal strength	72%
Net name	Orange Orange 4G
SIM status	Operational
SIM network registration status	Home Network
Modem IMEI	[redacted]
SIM Card IMSI	-

Disk Space Information	
Usage percentage	15%
Total	15 GB
Used	2.1 GB
Used by database	14 MB

Send SMS to Master Admin when percentage of disk usage reaches: □%

Leave empty to stop sending notifications.

Notification is sent once, every time it reaches or surpasses the entered value.

Sending state is reset after reaching a value below the limit.

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

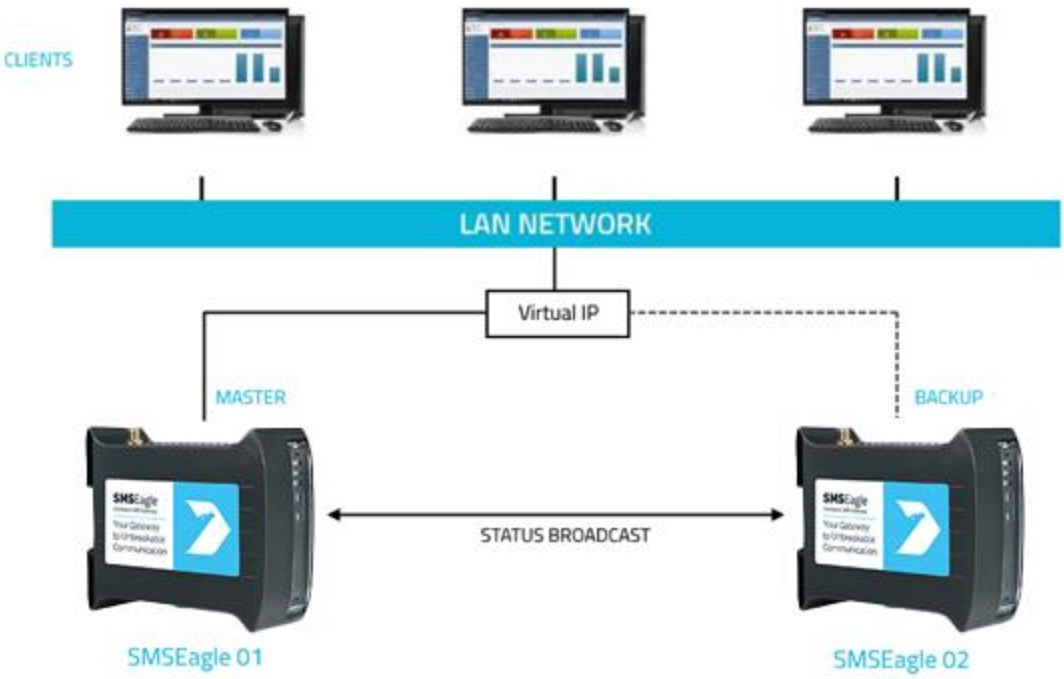
"High-availability clusters (also known as HA clusters or fail over clusters) are groups of computers (...) that can be reliably utilized with a minimum of down-time. They operate by using high availability software to harness redundant computers in groups or clusters that provide continued service when 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.

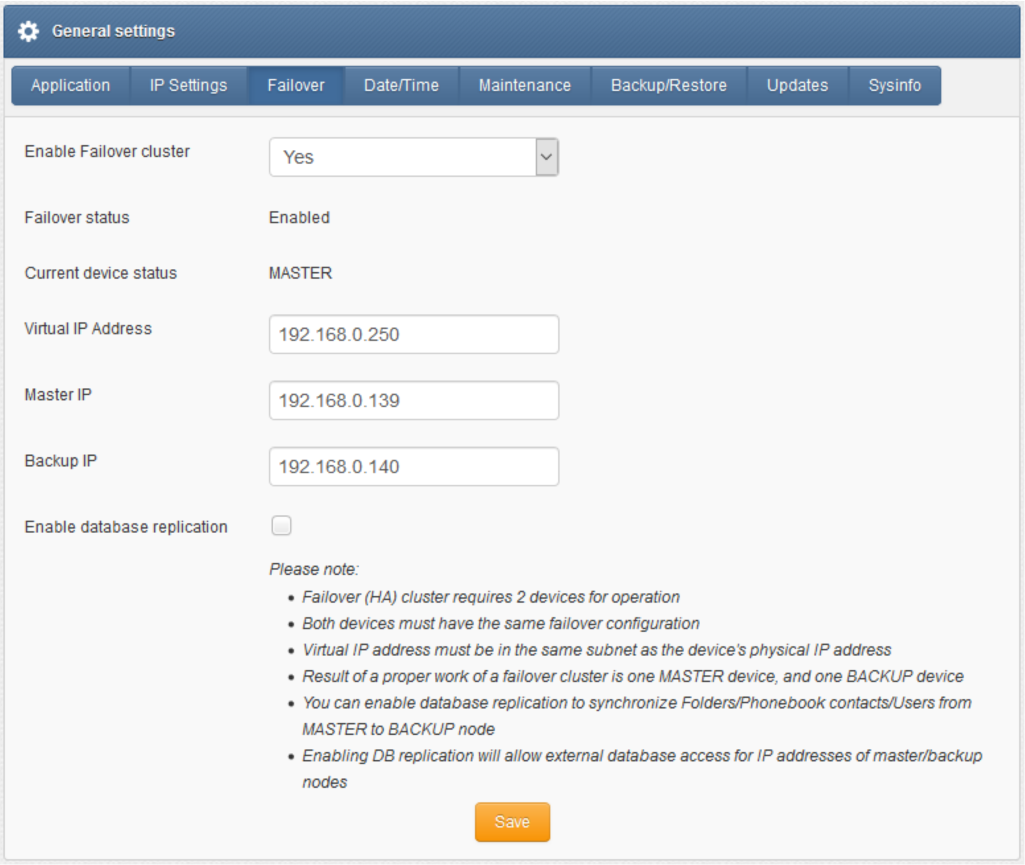
Devices (nodes) should see each other on the network. By default, HA-nodes use 224.0.0.18 multicast IP address for VRRP (Virtual Router Redundancy Protocol) for communication between two nodes. If nodes are on the same network (same subnet & IP range) there is no need for any network configuration. If 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.



Enable Failover cluster: Yes

Failover status: Enabled

Current device status: MASTER

Virtual IP Address: 192.168.0.250

Master IP: 192.168.0.139

Backup IP: 192.168.0.140

Enable database replication: □

Please note:

- *Failover (HA) cluster requires 2 devices for operation*
- *Both devices must have the same failover configuration*
- *Virtual IP address must be in the same subnet as the device's physical IP address*
- *Result of a proper work of a failover cluster is one MASTER device, and one BACKUP device*
- *You can enable database replication to synchronize Folders/Phonebook contacts/Users from MASTER to BACKUP node*
- *Enabling DB replication will allow external database access for IP addresses of master/backup nodes*

Screenshot from "General Settings-Failover"

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.

Please note that this feature is only available in devices with hardware Rev.2 and higher. We recommend to use the same device models 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`

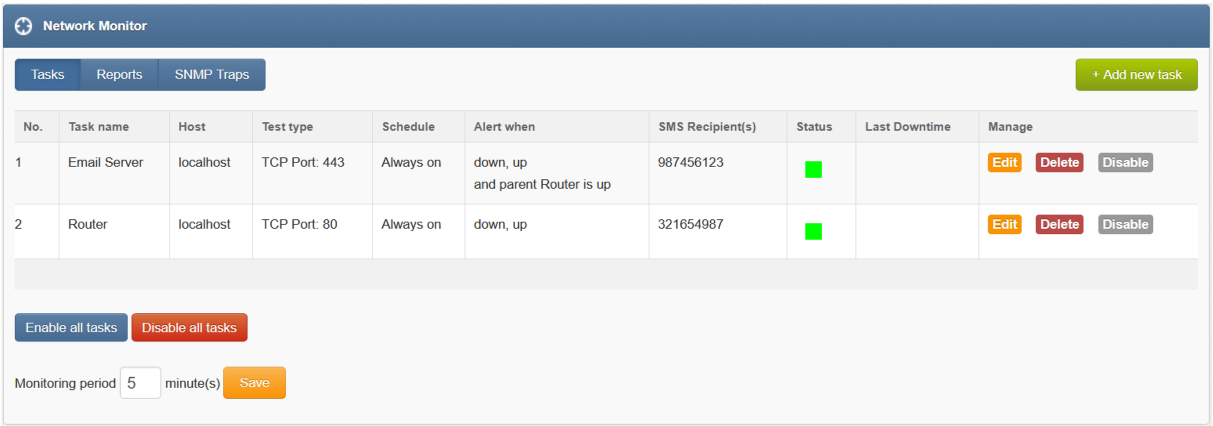
ADVANCED FEATURES

Basic features of SMSEagle software are extended by plugins that provide extra features to the software. Below you will find a description of features available in each SMSEagle device. All features are an integral part of SMSEagle software. That means that all described features are installed in a standard software of SMSEagle device and are available for free.

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

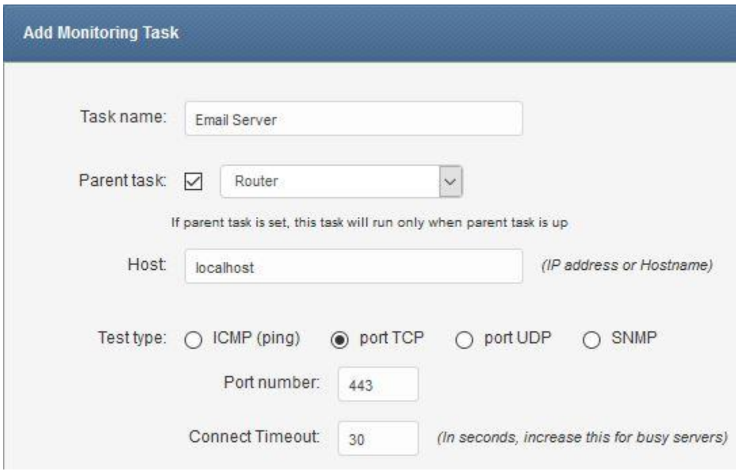


No.	Task name	Host	Test type	Schedule	Alert when	SMS Recipient(s)	Status	Last Downtime	Manage
1	Email Server	localhost	TCP Port: 443	Always on	down, up and parent Router is up	987456123	🟩		Edit Delete Disable
2	Router	localhost	TCP Port: 80	Always on	down, up	321654987	🟩		Edit Delete Disable

Monitoring period 5 minute(s)

- 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



Add Monitoring Task

Task name: Email Server

Parent task: ☑ Router

If parent task is set, this task will run only when parent task is up

Host: localhost *(IP address or Hostname)*

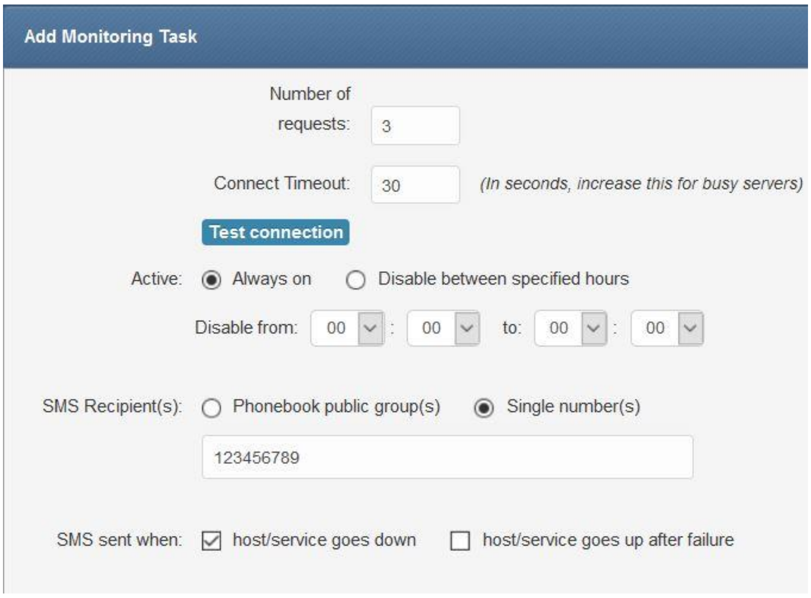
Test type: ○ ICMP (ping) ● port TCP ○ port UDP ○ SNMP

Port number: 443

Connect Timeout: 30 *(In seconds, increase this for busy servers)*

- 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)
- increase a default timeout value for busy servers (by default we set it to 30 seconds)
- test the connection of server

Define a schedule



Add Monitoring Task

Number of requests: 3

Connect Timeout: 30 *(In seconds, increase this for busy servers)*

Test connection

Active: ● Always on ○ Disable between specified hours

Disable from: 00 : 00 to: 00 : 00

SMS Recipient(s): ○ Phonebook public group(s) ● Single number(s)

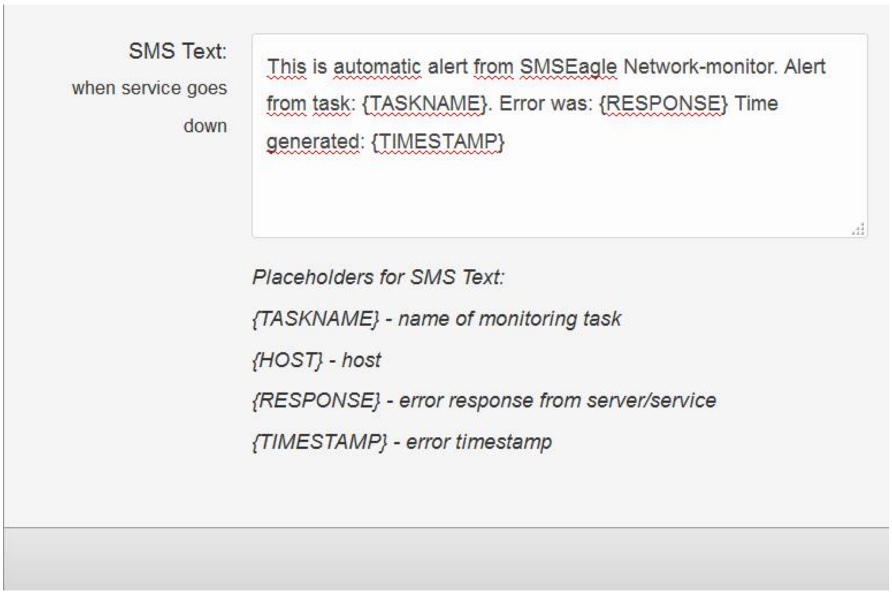
123456789

SMS sent when: ☑ host/service goes down □ host/service goes up after failure

- 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



SMS Text:
when service goes down

This is automatic alert from SMSEagle Network-monitor. Alert from task: {TASKNAME}. Error was: {RESPONSE} Time generated: {TIMESTAMP}

Placeholders for SMS Text:

{TASKNAME} - name of monitoring task

{HOST} - host

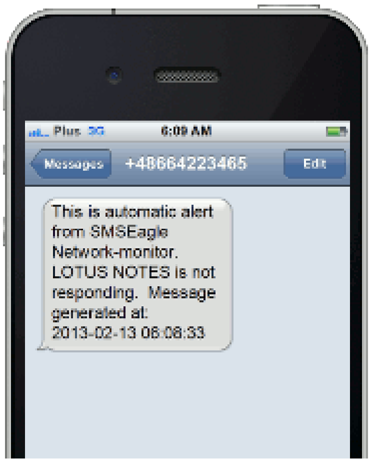
{RESPONSE} - error response from server/service

{TIMESTAMP} - error timestamp

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



This is automatic alert from SMSEagle Network-monitor. LOTUS NOTES is not responding. Message generated at: 2013-02-13 06:08:33

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

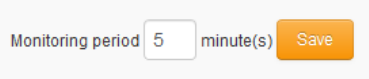
VOICE CALL

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.

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:

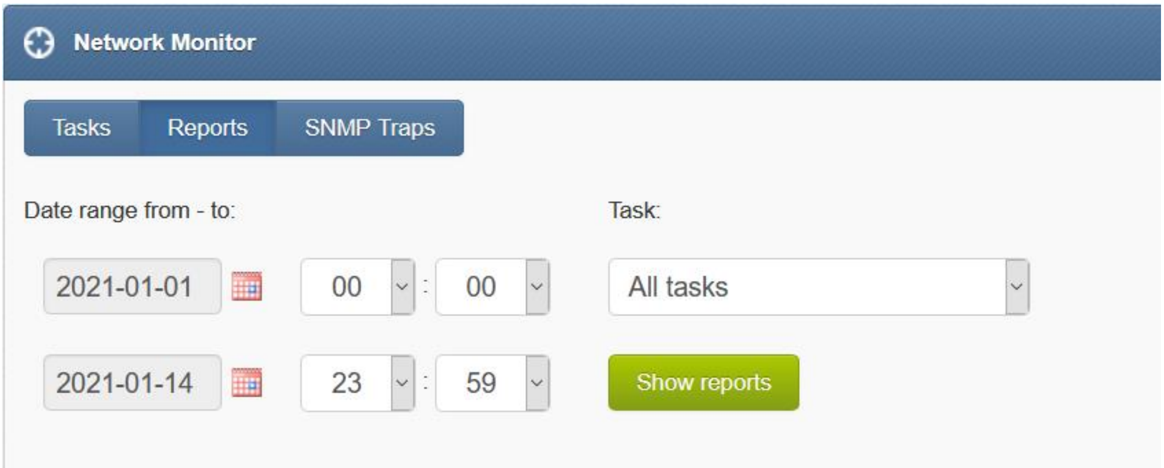


Monitoring period 5 minute(s)

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.



Network Monitor

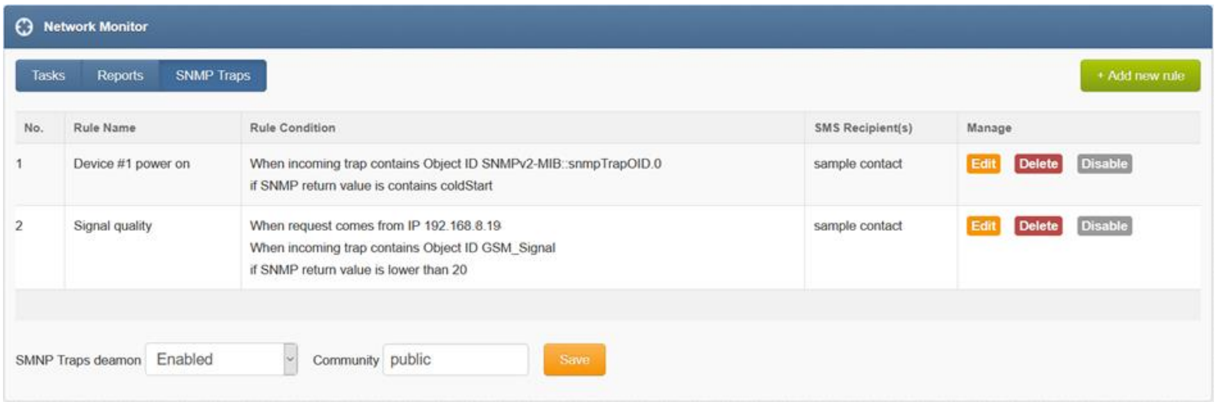
Date range from - to: 2021-01-01 00 : 00 – 2021-01-14 23 : 59

Task: All tasks

Screenshot from Network Monitor > Reports window.

SNMP TRAPS

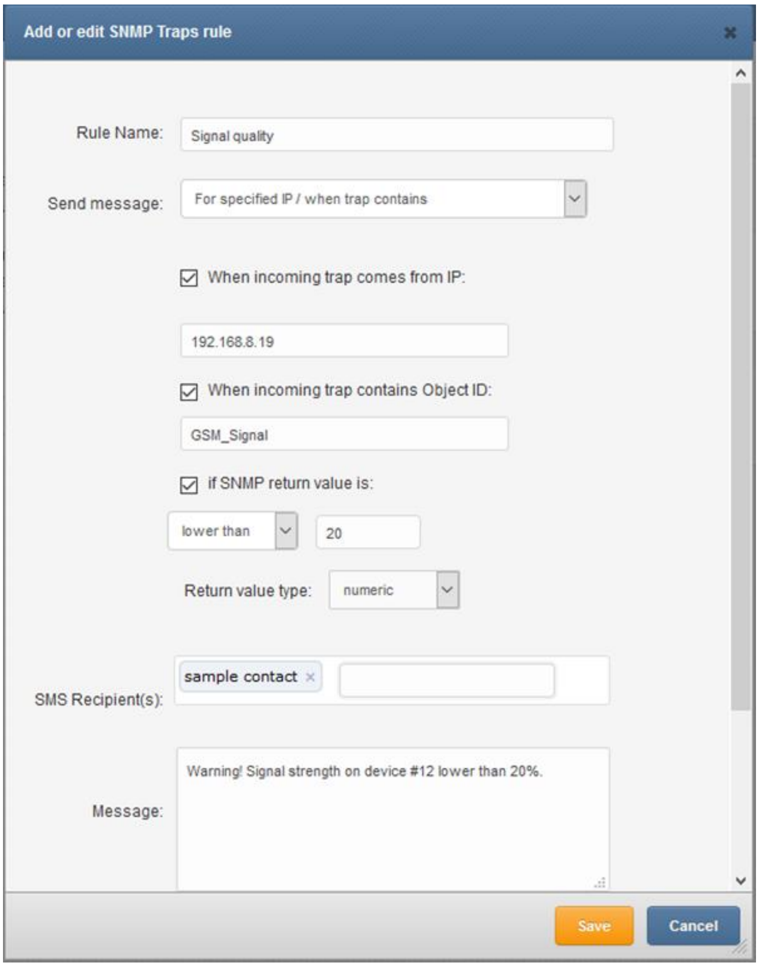
SNMP trap is a popular mechanism used to manage and monitor devices' activities via SNMP protocol. What makes the Trap unique is that they are triggered instantaneously by an agent, rather than waiting for a status request from SNMP get query.



No.	Rule Name	Rule Condition	SMS Recipient(s)	Manage
1	Device #1 power on	When incoming trap contains Object ID SNMPv2-MIB::snmpTrapOID.0 if SNMP return value is contains coldStart	sample contact	Edit Delete Disable
2	Signal quality	When request comes from IP 192.168.8.19 When incoming trap contains Object ID GSM_Signal if SNMP return value is lower than 20	sample contact	Edit Delete Disable

SMNP Traps deamon: Enabled
Community: public

Screenshot from Network Monitor > SNMP TRAPS window.



Rule Name: Signal quality

Send message: For specified IP / when trap contains

☑ When incoming trap comes from IP:

192.168.8.19

☑ When incoming trap contains Object ID:

GSM_Signal

☑ if SNMP return value is:

lower than 20

Return value type: numeric

SMS Recipient(s): sample contact ×

Message: Warning! Signal strength on device #12 lower than 20%.

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

Email to SMS

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

BASIC USAGE

If the feature 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)

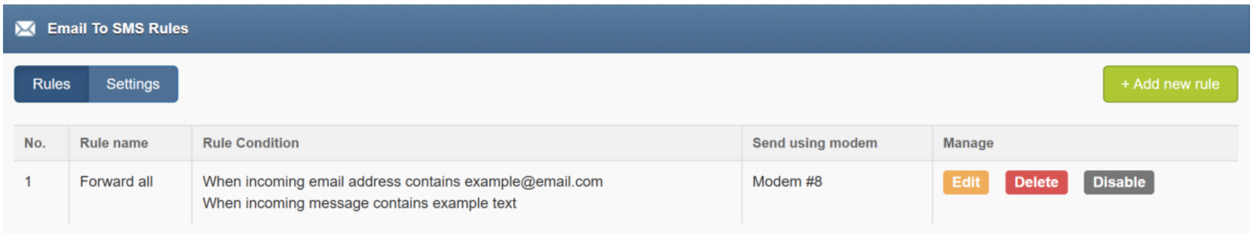
If you send email with subject containing FLAG=VALUE the flag will be set for this particular email2SMS message.

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.

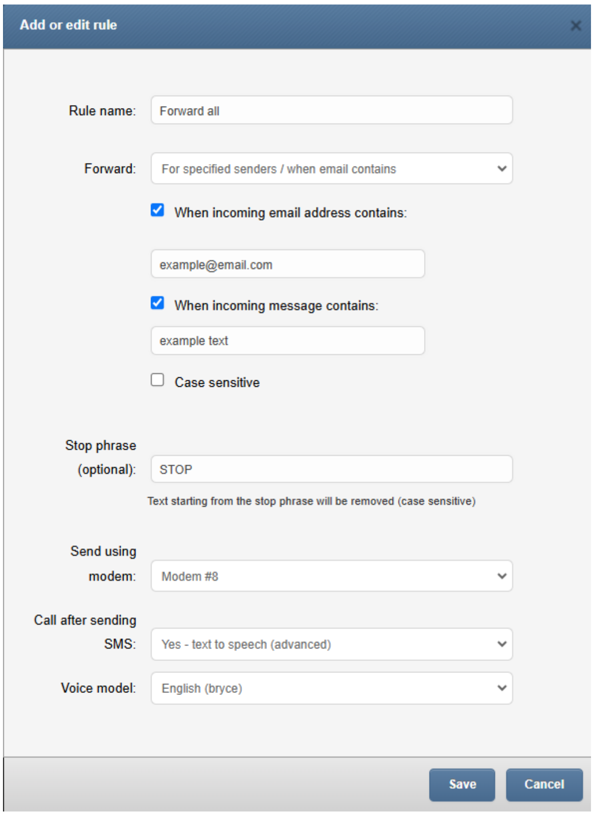
FEATURE CONFIGURATION

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



No.	Rule name	Rule Condition	Send using modem	Manage
1	Forward all	When incoming email address contains example@email.com When incoming message contains example text	Modem #8	Edit Delete Disable

Screenshot from Email To SMS > Rules window



Rule name: Forward all

Forward: For specified senders / when email contains

☑ When incoming email address contains:

example@email.com

☑ When incoming message contains:

example text

□ Case sensitive

Stop phrase (optional): STOP

Text starting from the stop phrase will be removed (case sensitive)

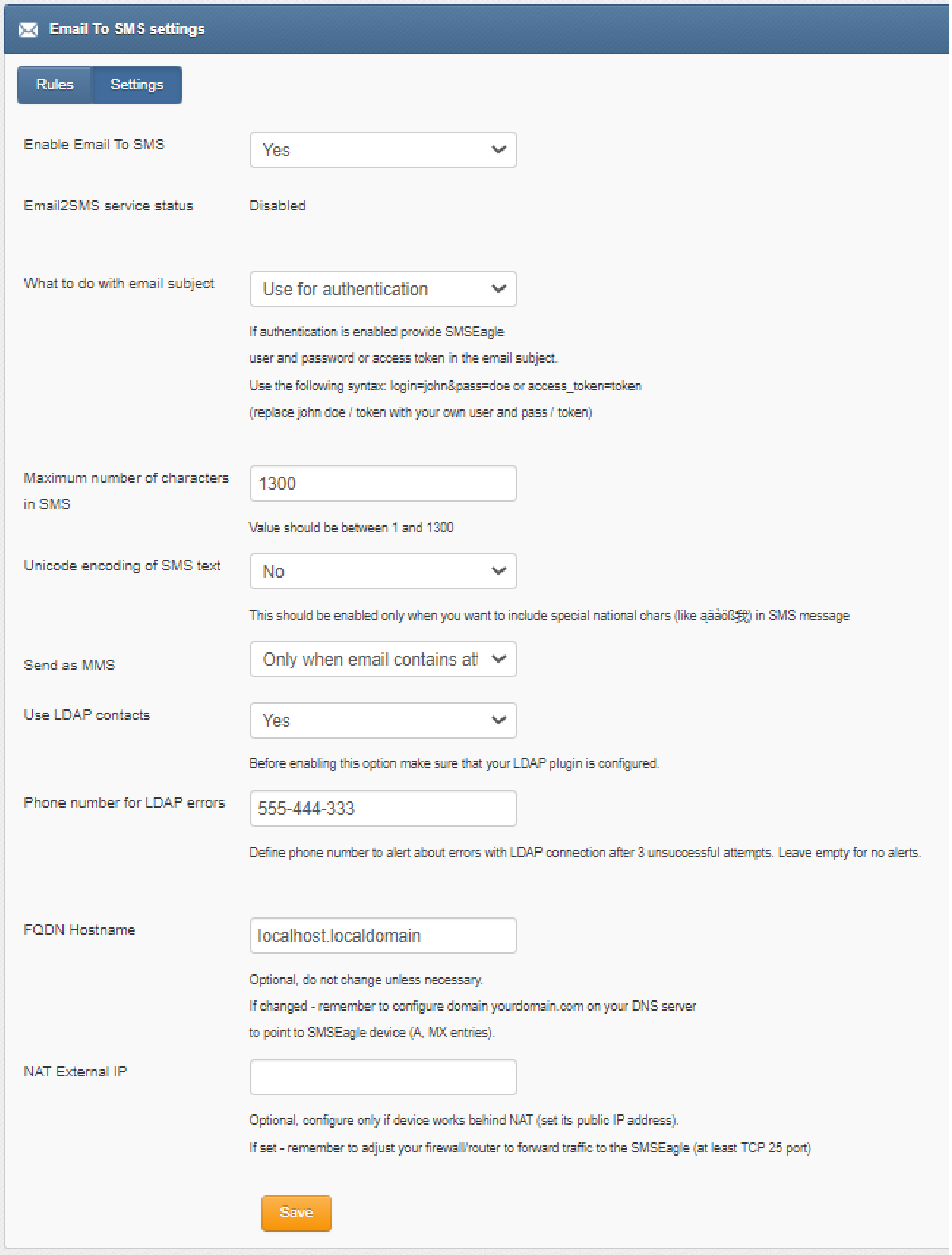
Send using modem: Modem #8

Call after sending SMS: Yes - text to speech (advanced)

Voice model: English (bryce)

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 choose sending modem no.
- You can define "Stop phrase". Text starting from the stop phrase will be removed (case sensitive) from the message



Enable Email To SMS: Yes

Email2SMS service status: Disabled

What to do with email subject: Use for authentication

If authentication is enabled provide SMSEagle
user and password or access token in the email subject.
Use the following syntax: login=john&pass=doe or access_token=token
(replace john doe / token with your own user and pass / token)

Maximum number of characters in SMS: 1300

Value should be between 1 and 1300

Unicode encoding of SMS text: No

This should be enabled only when you want to include special national chars (like ąäàöß我) in SMS message

Send as MMS: Only when email contains at

Use LDAP contacts: Yes

Before enabling this option make sure that your LDAP plugin is configured.

Phone number for LDAP errors: 555-444-333

Define phone number to alert about errors with LDAP connection after 3 unsuccessful attempts. Leave empty for no alerts.

FQDN Hostname: localhost.localdomain

Optional, do not change unless necessary.
If changed - remember to configure domain yourdomain.com on your DNS server
to point to SMSEagle device (A, MX entries).

NAT External IP:

Optional, configure only if device works behind NAT (set its public IP address).
If set - remember to adjust your firewall/router to forward traffic to the SMSEagle (at least TCP 25 port)

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 ąäàöß 我) 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 feature should be used when you need to fetch emails from an existing mailbox on your mail server. The Email2SMS Poller 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 and 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.

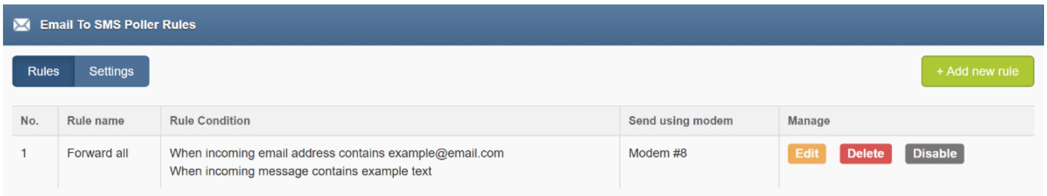
VOICE CALL

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 a situation with resending the same message (marking unread already processed read message).

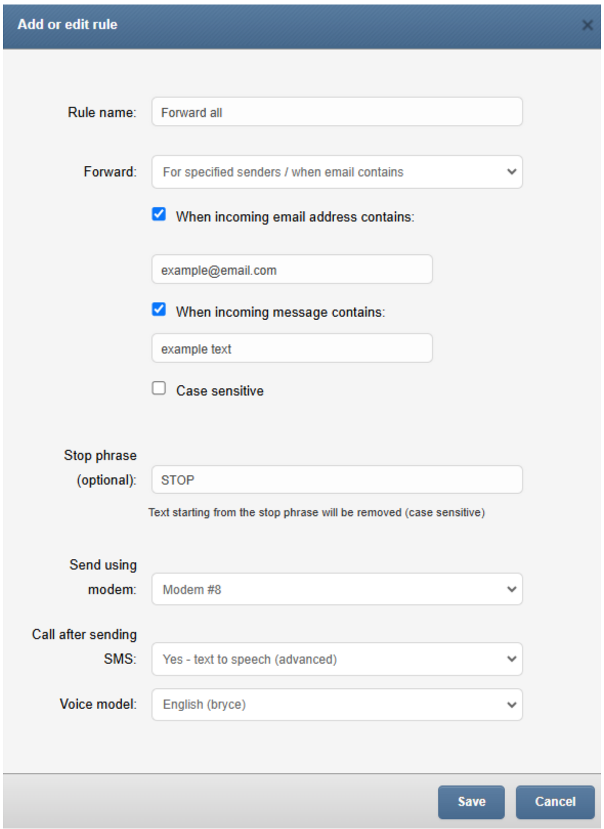
FEATURE CONFIGURATION

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



No.	Rule name	Rule Condition	Send using modem	Manage
1	Forward all	When incoming email address contains example@email.com When incoming message contains example text	Modem #8	Edit Delete Disable

Screenshot from Email to SMS Poller Rules



Add or edit rule

Rule name: Forward all

Forward: For specified senders / when email contains

☑ When incoming email address contains:

example@email.com

☑ When incoming message contains:

example text

☐ Case sensitive

Stop phrase (optional): STOP

Text starting from the stop phrase will be removed (case sensitive)

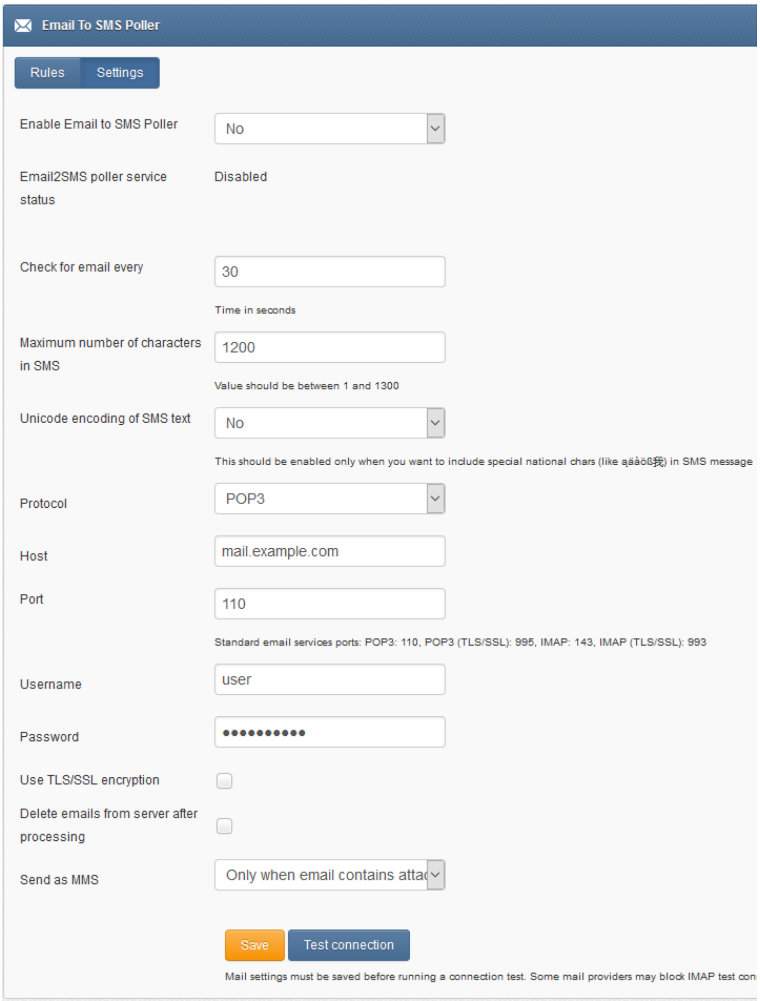
Send using modem: Modem #8

Call after sending SMS: Yes - text to speech (advanced)

Voice model: English (bryce)

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 a sending modem no.
- You can define "Stop phrase". Text starting from the stop phrase will be removed (case sensitive) from the message



Email To SMS Poller

Enable Email to SMS Poller: No

Email2SMS poller service status: Disabled

Check for email every: 30

Time in seconds

Maximum number of characters in SMS: 1200

Value should be between 1 and 1300

Unicode encoding of SMS text: No

This should be enabled only when you want to include special national chars (like ąäàöß我) in SMS message

Protocol: POP3

Host: mail.example.com

Port: 110

Standard email services ports: POP3: 110, POP3 (TLS/SSL): 995, IMAP: 143, IMAP (TLS/SSL): 993

Username: user

Password: ●●●●●●●●●●

Use TLS/SSL encryption ☐

Delete emails from server after processing ☐

Send as MMS: Only when email contains attac

Mail settings must be saved before running a connection test. Some mail providers may block IMAP test con

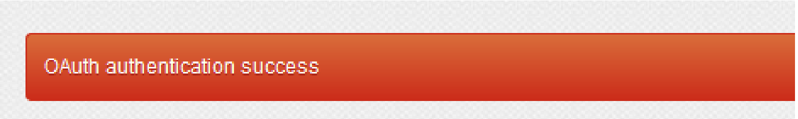
Screenshot from Email to SMS Poller settings

- 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 OFFICE365 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 web GUI


OAuth authentication success

SMS to Email

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

The plugin can be used in two modes:

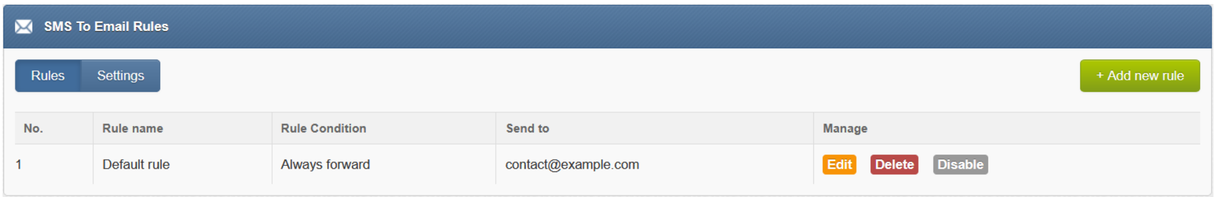
a. forwarding of incoming SMS/MMS to email of last sender (so called **Two-way Email2SMS & SMS2Email**)
In this mode, when SMSEagle receives incoming SMS, it checks if earlier anyone was sending SMS to the number from incoming SMS using Emai2SMS. If last sender is found, the incoming SMS is forwarded 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.

b. It forwards all the incoming messages to one fixed email address.
In this mode incoming SMS/MMS messages are forwarded to always the same email address.

FEATURE CONFIGURATION

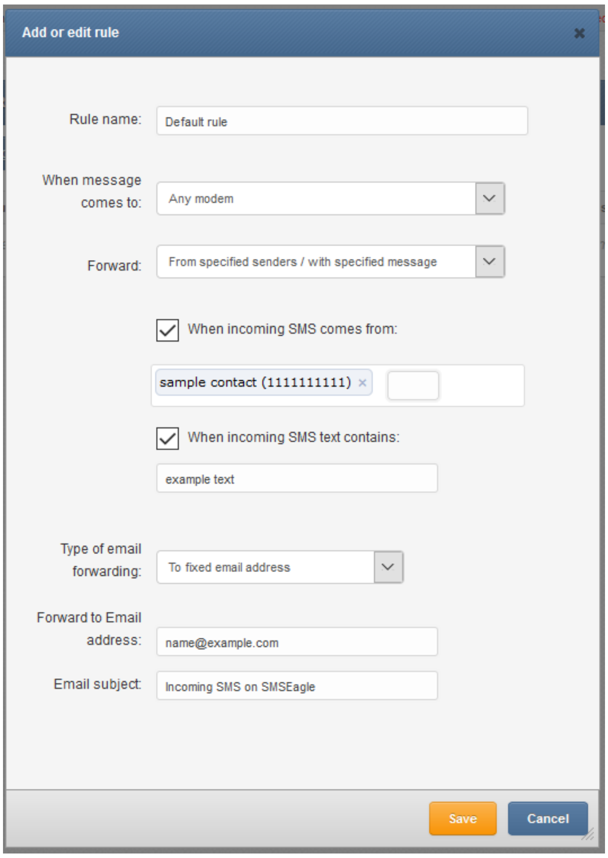
The feature uses an external SMTP email server for sending emails. You can configure the email server via menu Emails > SMTP Configuration. Please add at least one configuration and select the configuration in the drop-down parameter “SMS To Email” below.

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



No.	Rule name	Rule Condition	Send to	Manage
1	Default rule	Always forward	contact@example.com	Edit Delete Disable

Screenshot from SMS to Email > Rules



Rule name: Default rule

When message comes to: Any modem

Forward: From specified senders / with specified message

☑ When incoming SMS comes from:

sample contact (1111111111) ×

☑ When incoming SMS text contains:

example text

Type of email forwarding: To fixed email address

Forward to Email address: name@example.com

Email subject: Incoming SMS on SMSEagle

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:

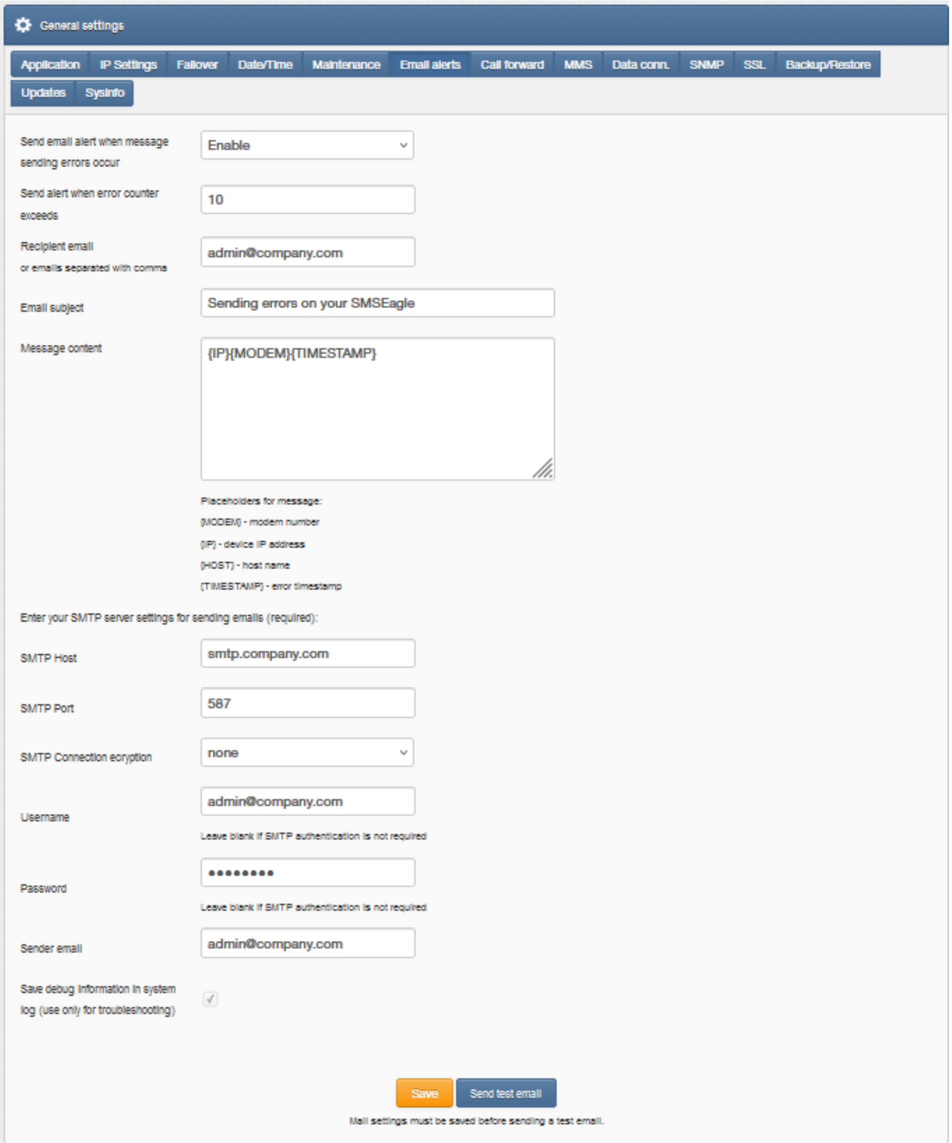
From: +483334455 (John Doe)

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.



Send email alert when message sending errors occur: Enable

Send alert when error counter exceeds: 10

Recipient email or emails separated with comma: admin@company.com

Email subject: Sending errors on your SMSEagle

Message content: {IP}{MODEM}{TIMESTAMP}

Placeholders for message:
{MODEM} - modem number
{IP} - device IP address
{HOST} - host name
{TIMESTAMP} - error timestamp

Enter your SMTP server settings for sending emails (required):

SMTP Host: smtp.company.com

SMTP Port: 587

SMTP Connection ecryption: none

Username: admin@company.com
Leave blank if SMTP authentication is not required

Password: ••••••••
Leave blank if SMTP authentication is not required

Sender email: admin@company.com

Save debug information in system log (use only for troubleshooting): ☑

Mail settings must be saved before sending a test email.

- 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)

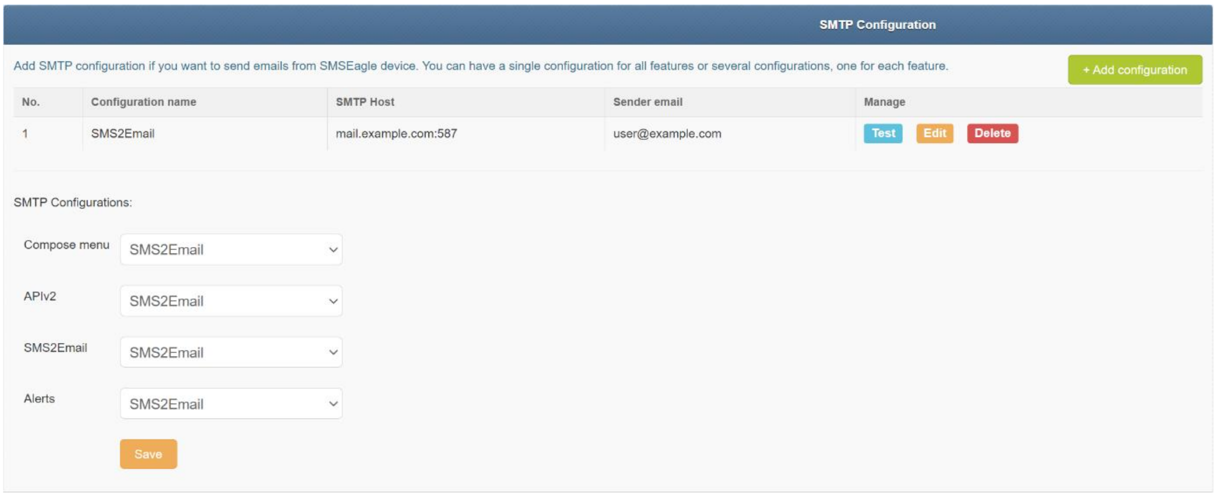
Notice: To prevent false alarms we recommend to set parameter "Send alert when error counter exceeds" to value > 2.

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

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.



SMTP Configuration

Add SMTP configuration if you want to send emails from SMSEagle device. You can have a single configuration for all features or several configurations, one for each feature.

No.	Configuration name	SMTP Host	Sender email	Manage
1	SMS2Email	mail.example.com:587	user@example.com	Test Edit Delete

SMTP Configurations:

Compose menu: SMS2Email

APIv2: SMS2Email

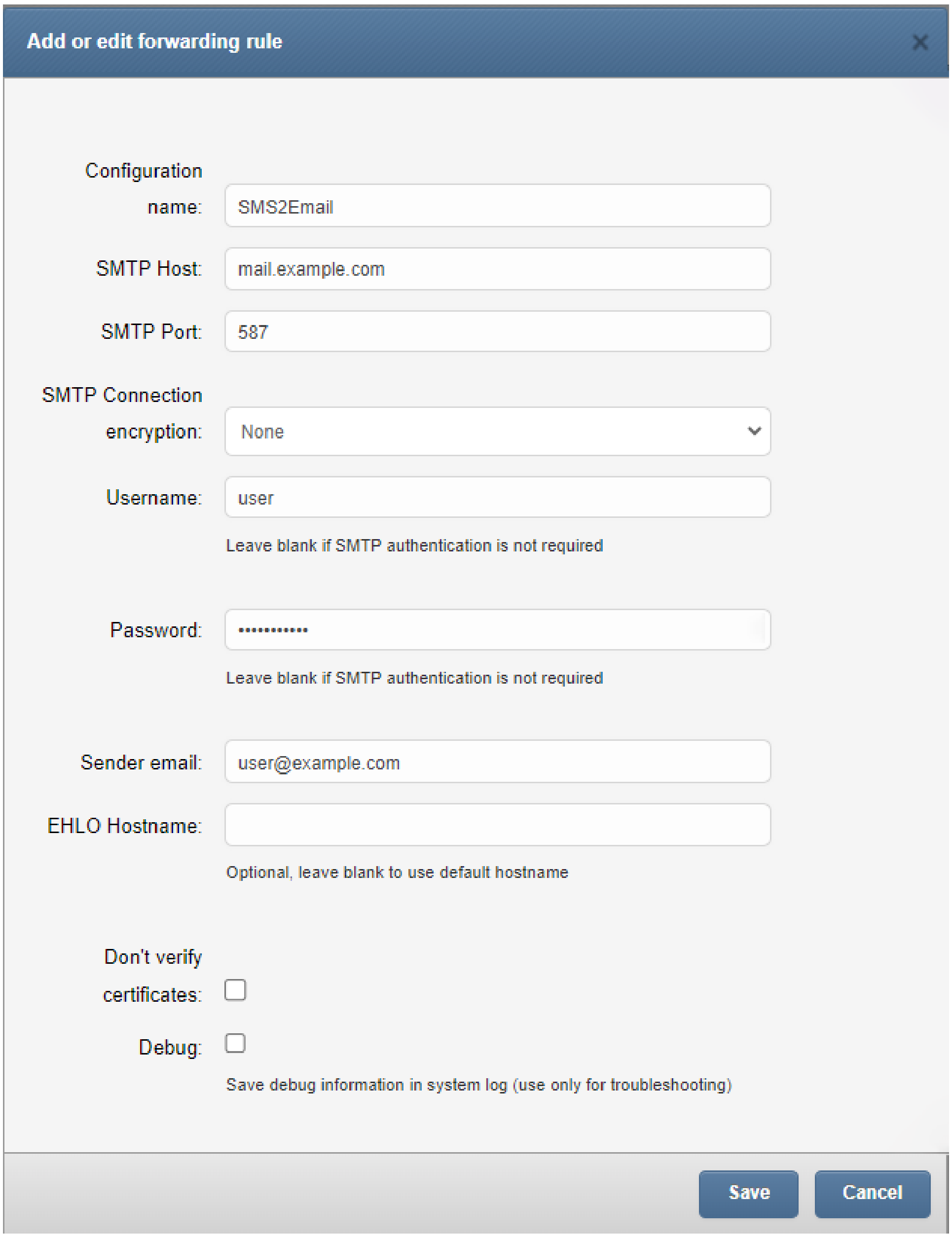
SMS2Email: SMS2Email

Alerts: SMS2Email

screenshot from menu SMTP Configuration

To start using Email features on your SMSEagle:

1. Create at least one configuration



Configuration name: SMS2Email

SMTP Host: mail.example.com

SMTP Port: 587

SMTP Connection encryption: None

Username: user

Leave blank if SMTP authentication is not required

Password: •••••••••••

Leave blank if SMTP authentication is not required

Sender email: user@example.com

EHLO Hostname:

Optional, leave blank to use default hostname

Don't verify certificates: □

Debug: □

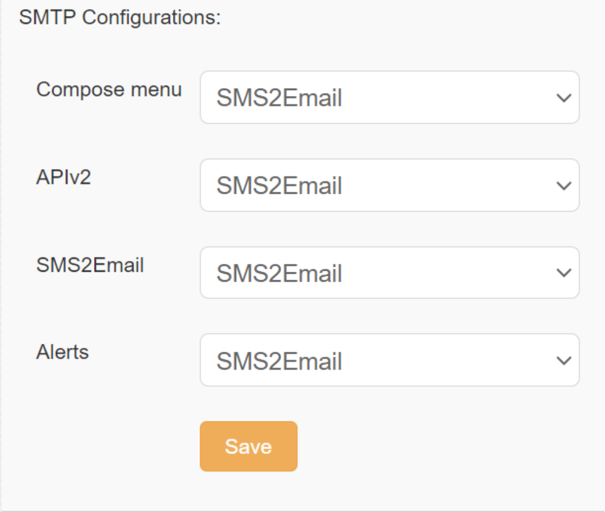
Save debug information in system log (use only for troubleshooting)

screenshot from SMTP add configuration

- Set 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.



SMTP Configurations:

Compose menu: SMS2Email

APIv2: SMS2Email

SMS2Email: SMS2Email

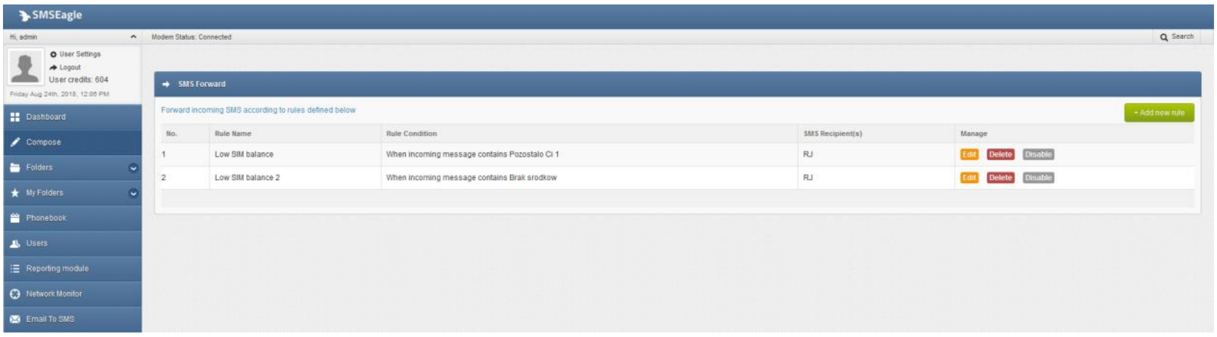
Alerts: SMS2Email

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.



User credits: 604

Friday Aug 24th, 2018, 12:06 PM

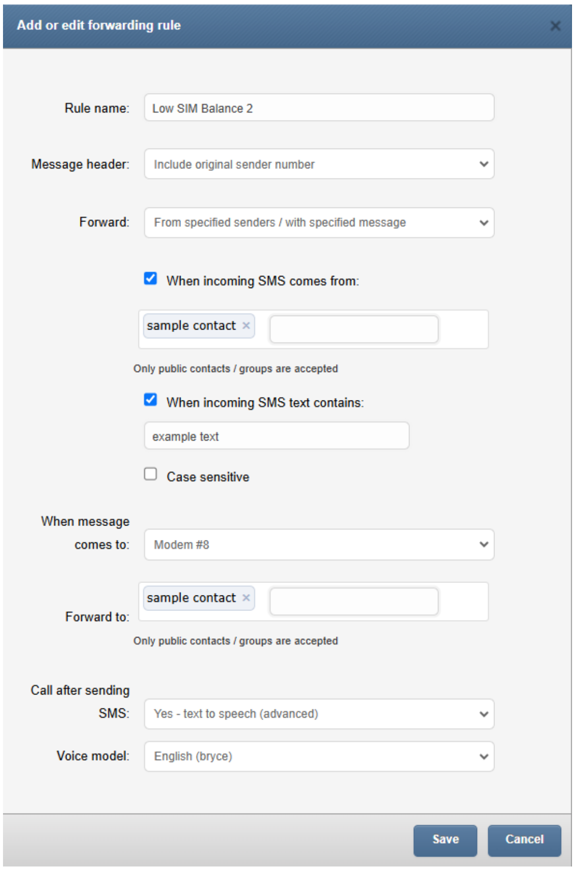
Forward incoming SMS according to rules defined below

No.	Rule Name	Rule Condition	SMS Recipient(s)	Manage
1	Low SIM balance	When incoming message contains Pozostalo Ci 1	RJ	Edit Delete Disable
2	Low SIM balance 2	When incoming message contains Brak srodkow	RJ	Edit Delete Disable

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.
- There is a possibility to enable/disable each rule.



Rule name: Low SIM Balance 2

Message header: Include original sender number

Forward: From specified senders / with specified message

☑ When incoming SMS comes from:

sample contact ×

Only public contacts / groups are accepted

☑ When incoming SMS text contains:

example text

☐ Case sensitive

When message comes to: Modem #8

Forward to: sample contact ×

Only public contacts / groups are accepted

Call after sending SMS: Yes - text to speech (advanced)

Voice model: English (bryce)

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.

Callback URL (webhooks)

Callback URL feature allows you to:

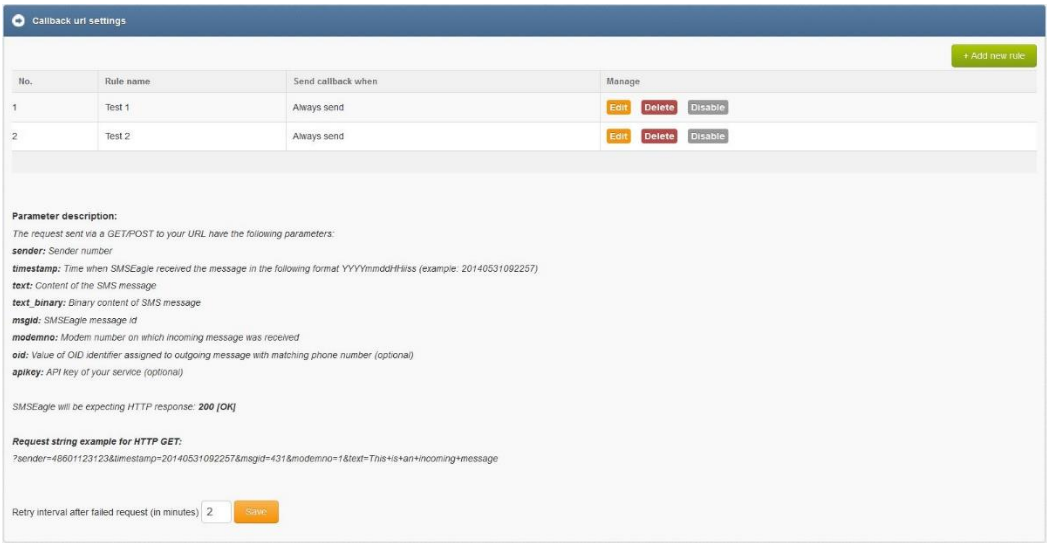
- forward incoming message to a defined URL address

- 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 feature "Callback URL" allows to add unlimited number of rules. Each rule can be enabled or disabled by user.



No.	Rule name	Send callback when	Manage
1	Test 1	Always send	Edit Delete Disable
2	Test 2	Always send	Edit Delete Disable

Parameter description:
The request sent via a GET/POST to your URL have the following parameters:
sender: *Sender number*
timestamp: *Time when SMSEagle received the message in the following format YYYYmmddHHiiss (example: 20140531092257)*
text: *Content of the SMS message*
text_binary: *Binary content of SMS message*
msgid: *SMSEagle message id*
modemno: *Modem number on which incoming message was received*
oid: *Value of OID identifier assigned to outgoing message with matching phone number (optional)*
apikey: *API key of your service (optional)*

SMSEagle will be expecting HTTP response: ***200 [OK]***

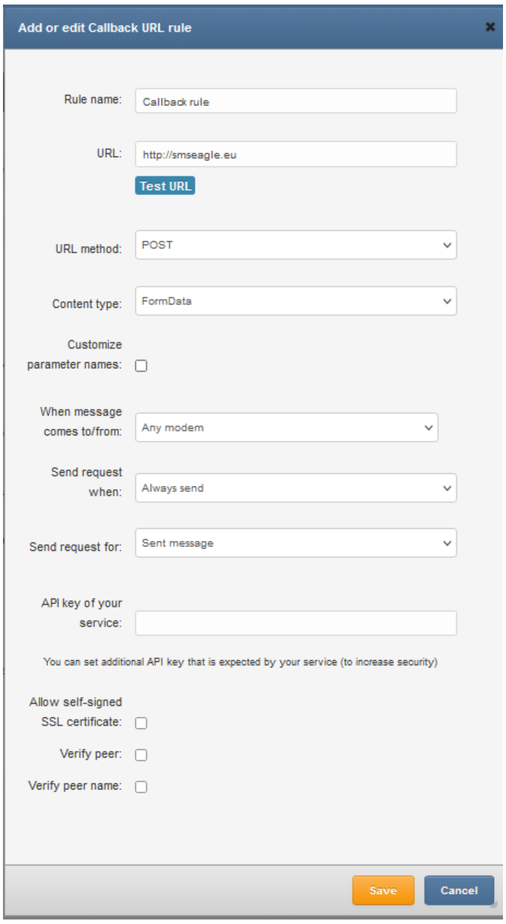
Request string example for HTTP GET:
?sender=48601123123&timestamp=20140531092257&msgid=431&modemno=1&text=This+is+an+incoming+message

Retry interval after failed request (in minutes) 2 Save

Screenshot from Callback URL 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 Callback URL 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 message sent, on message delivery)
- 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
- User may also choose whether to enable support of self-signed SSL certificate



Add or edit Callback URL rule

Rule name: Callback rule

URL: http://smseagle.eu

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:

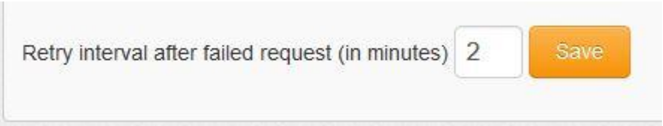
You can set additional API key that is expected by your service (to increase security)

Allow self-signed SSL certificate: □

Verify peer: □

Verify peer name: □

After sending HTTP(S) GET/POST request to your callback URL, SMSEagle will be expecting HTTP response: 200 [OK]. 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:



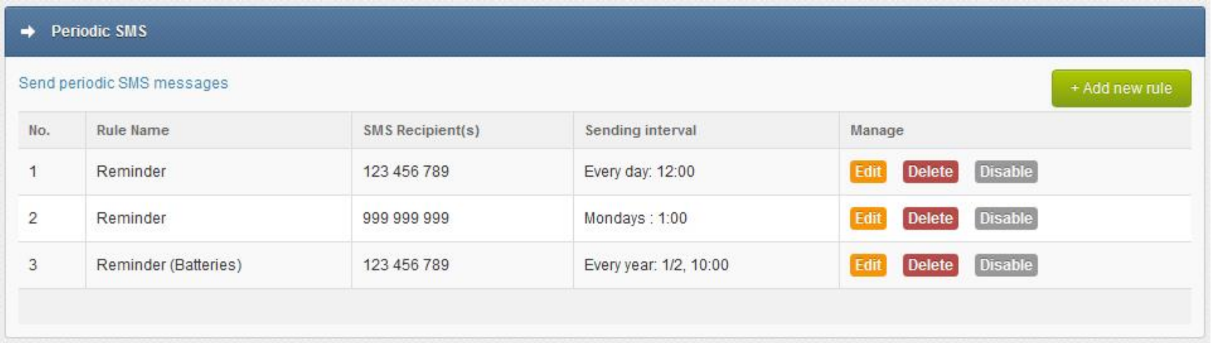
Retry interval after failed request (in minutes) 2

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.



Periodic SMS

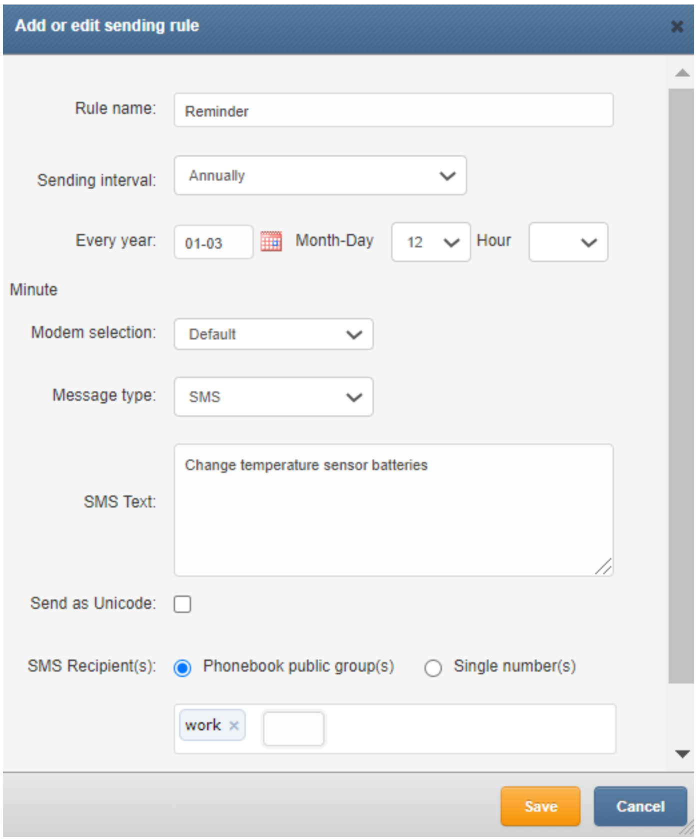
Send periodic SMS messages

No.	Rule Name	SMS Recipient(s)	Sending interval	Manage
1	Reminder	123 456 789	Every day: 12:00	Edit Delete Disable
2	Reminder	999 999 999	Mondays : 1:00	Edit Delete Disable
3	Reminder (Batteries)	123 456 789	Every year: 1/2, 10:00	Edit Delete Disable

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)



Add or edit sending rule

Rule name: Reminder

Sending interval: Annually

Every year: 01-03 Month-Day 12 Hour

Minute

Modem selection: Default

Message type: SMS

SMS Text: Change temperature sensor batteries

Send as Unicode: □

SMS Recipient(s): ● Phonebook public group(s) ○ Single number(s)

work ×

Screenshot from "Add new rule" window

VOICE CALL

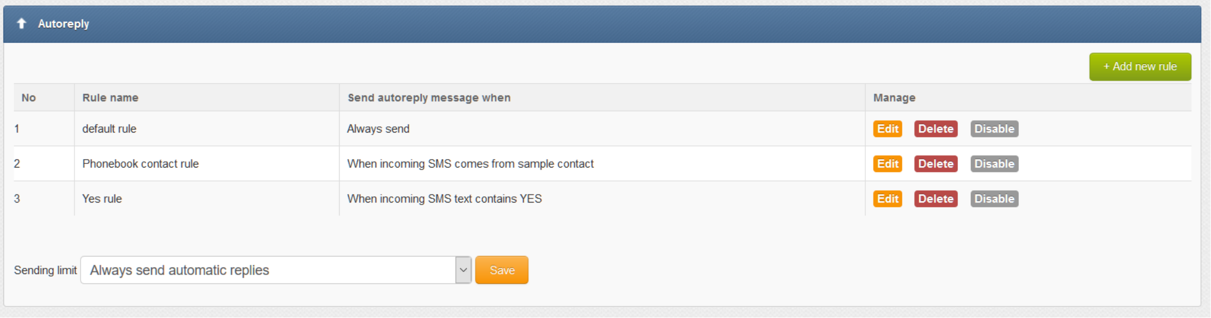
A SMS message can be optionally followed by a wake-up call or text-to-speech call. This can be enabled in the rule definition. The feature requires a device with an active Voice-Call add-on.

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.



No	Rule name	Send autoreply message when	Manage
1	default rule	Always send	Edit Delete Disable
2	Phonebook contact rule	When incoming SMS comes from sample contact	Edit Delete Disable
3	Yes rule	When incoming SMS text contains YES	Edit Delete Disable

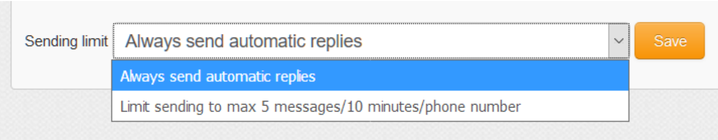
Sending limit: Always send automatic replies

Screenshot from plugin main window

For each rule user can define:

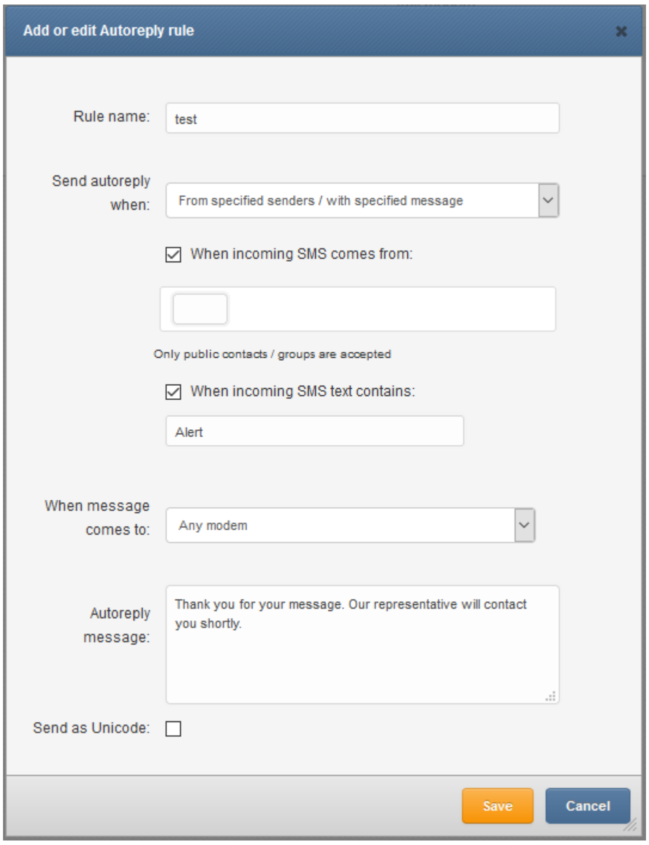
- When autoreply message should be sent:
  - always,
  - when incoming message contains defined text,
  - and/or when message sender belongs to Phonebook contact/group
  - if incoming SMS text comes to a selected modem
- If autoreply message text should be sent as Unicode characters

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.



Sending limit: Always send automatic replies

Always send automatic replies
Limit sending to max 5 messages/10 minutes/phone number



Add or edit Autoreply rule

Rule name: test

Send autoreply when: From specified senders / with specified message

☑ When incoming SMS comes from:

Only public contacts / groups are accepted

☑ When incoming SMS text contains:

Alert

When message comes to: Any modem

Autoreply message: Thank you for your message. Our representative will contact you shortly.

Send as Unicode: □

Screenshot form "Add/edit autoreply rule"

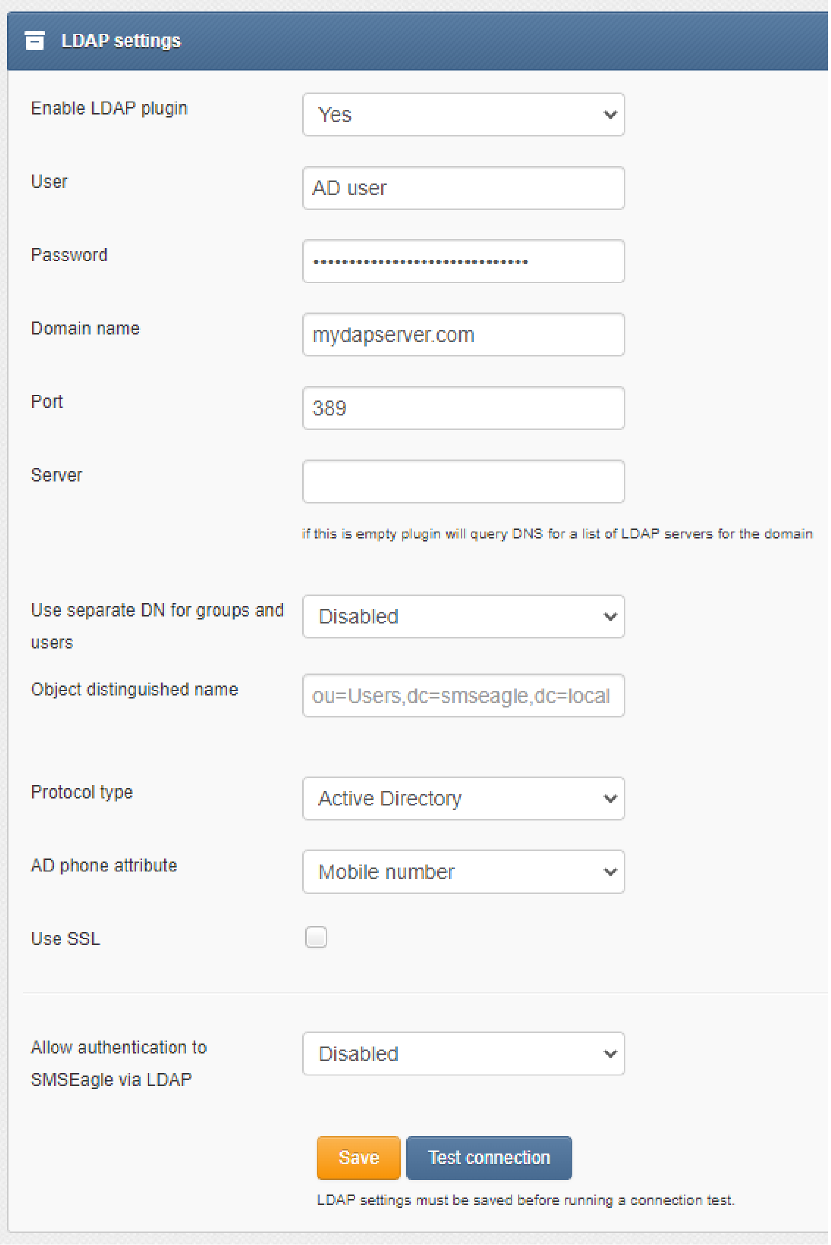
LDAP

The LDAP feature allows to access directory services: Active Directory (hereinafter referred to as "AD") and OpenLDAP. The feature 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 feature configuration. After enabling the feature, 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.



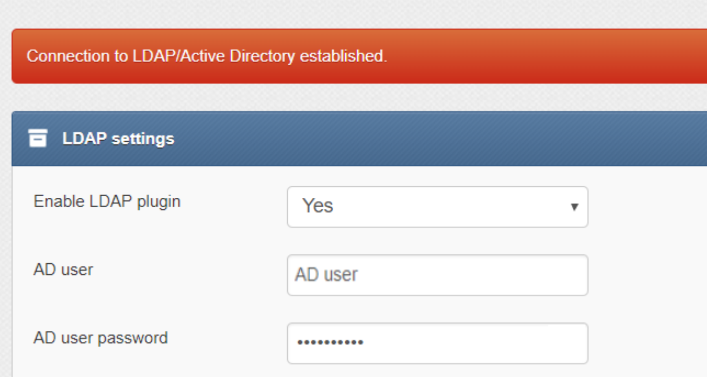
LDAP settings

Enable LDAP plugin	Yes
User	AD user
Password	••••••••••••••••••••••••••••••
Domain name	mydapserver.com
Port	389
Server	
	if this is empty plugin will query DNS for a list of LDAP servers for the domain
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	□
Allow authentication to SMSEagle via LDAP	Disabled

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.



Connection to LDAP/Active Directory established.

LDAP settings

Enable LDAP plugin: Yes

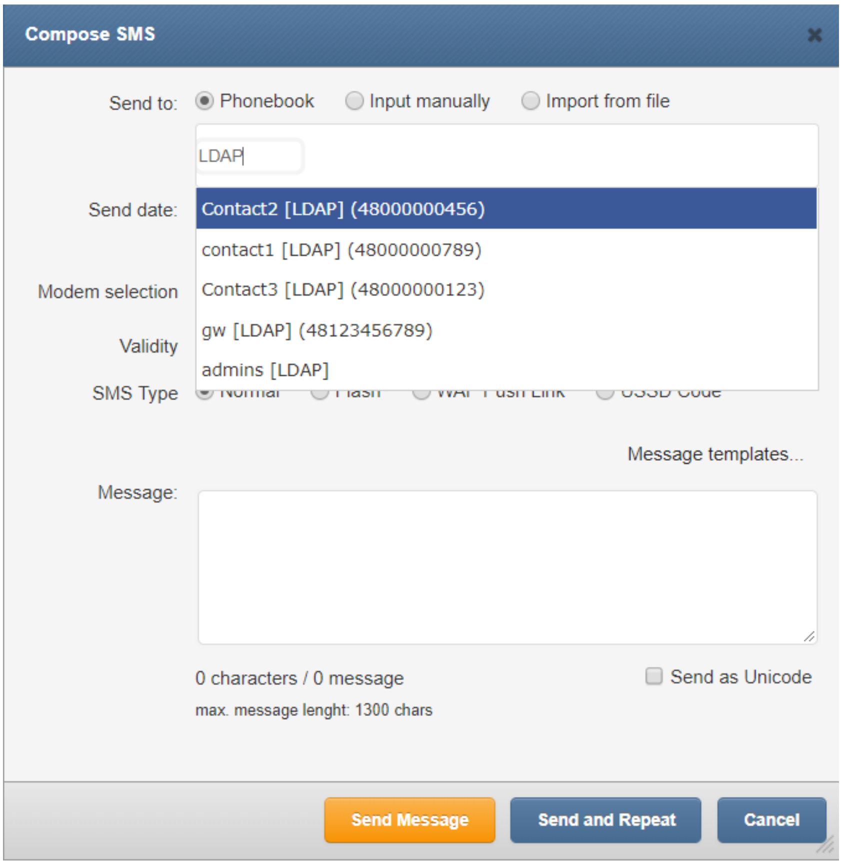
AD user: AD user

AD user password: ••••••••••

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” to check all contacts listed in AD directory.



Compose SMS

Send to: ● Phonebook ○ Input manually ○ Import from file

LDAP

Contact2 [LDAP] (48000000456)
contact1 [LDAP] (48000000789)
Contact3 [LDAP] (48000000123)
gw [LDAP] (48123456789)
admins [LDAP]

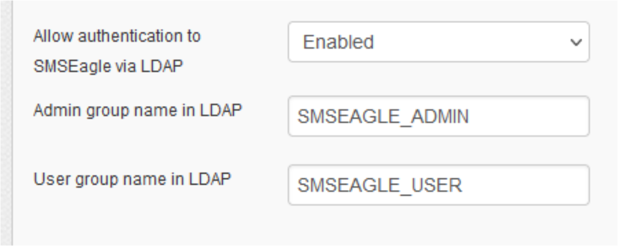
Screenshot from “Compose” module with LDAP connection enabled

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)

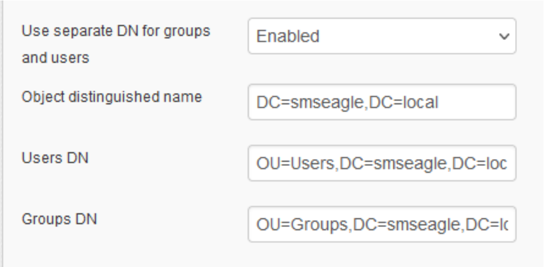
This feature allows authentication to your SMSEagle device using LDAP. To start using it:

- 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"



Allow authentication to SMSEagle via LDAP	Enabled
Admin group name in LDAP	SMSEAGLE_ADMIN
User group name in LDAP	SMSEAGLE_USER

- 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)

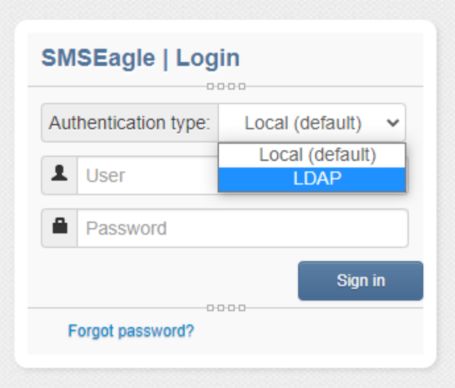


Use separate DN for groups and users	Enabled
Object distinguished name	DC=smseagle,DC=local
Users DN	OU=Users,DC=smseagle,DC=loc
Groups DN	OU=Groups,DC=smseagle,DC=lc

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



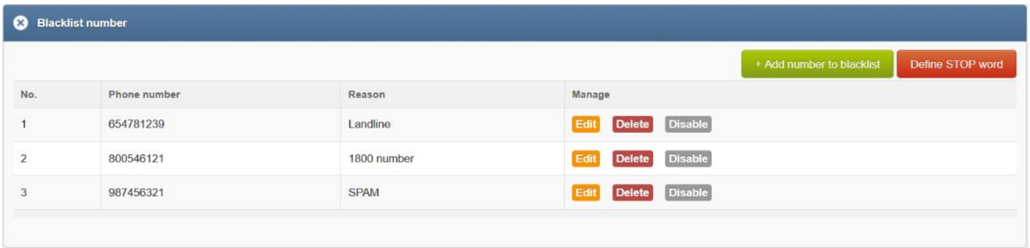
SMSEagle | Login

Authentication type: Local (default)

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.

Blacklist

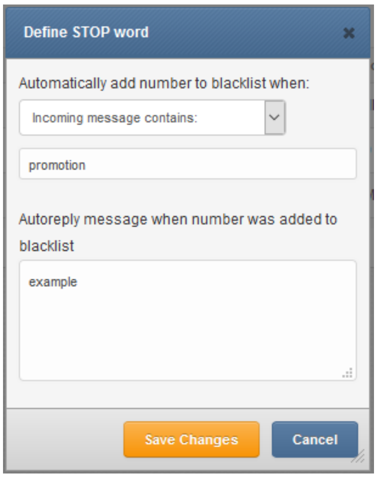
This feature allows you to add a number to a Blacklist. When a number is on this list, the device automatically blocks any sent and received SMS from the number as well as deletes the messages from your inbox.



Blacklist number

No.	Phone number	Reason	Manage
1	654781239	Landline	Edit Delete Disable
2	800546121	1800 number	Edit Delete Disable
3	987456321	SPAM	Edit Delete Disable

Screenshot from "Blacklist" feature



Define STOP word

Automatically add number to blacklist when:

Incoming message contains:

promotion

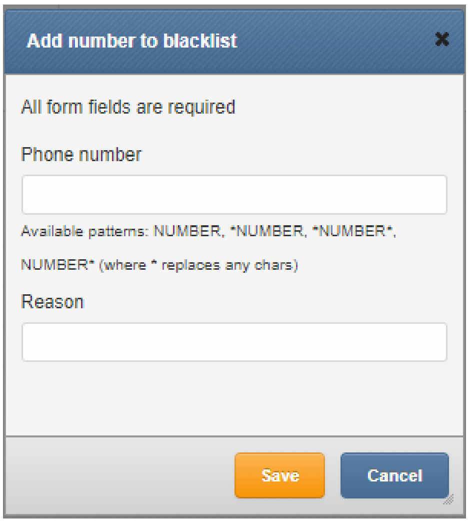
Autoreply message when number was added to blacklist

example

Screenshot from Blacklist > Define STOP word feature

In "Define STOP word" window:

- You may add a defined a STOP keyword. When incoming message contains the keyword then the sender number will be automatically added to exclude-list.



Add number to blacklist

All form fields are required

Phone number

Available patterns: NUMBER, *NUMBER, *NUMBER*, NUMBER* (where * replaces any chars)

Reason

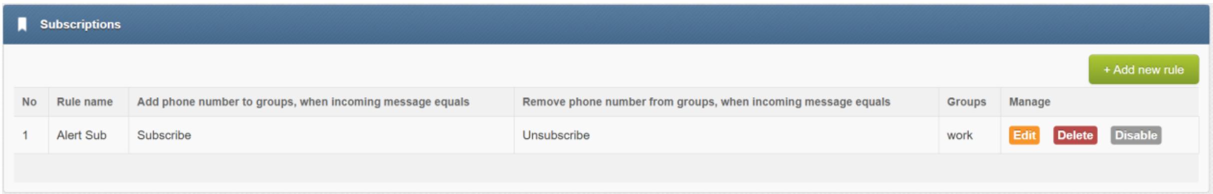
Screenshot from Blacklist > Add number to blacklist

In "Add number to blacklist" window:

- You may add excluded phone number(s). The following wildcards may be used for multiple numbers: *NUMBER, *NUMBER*, NUMBER* (where * replaces any chars)
- You may add a comment (a reason) for blacklisting the number

Subscriptions (newsletter)

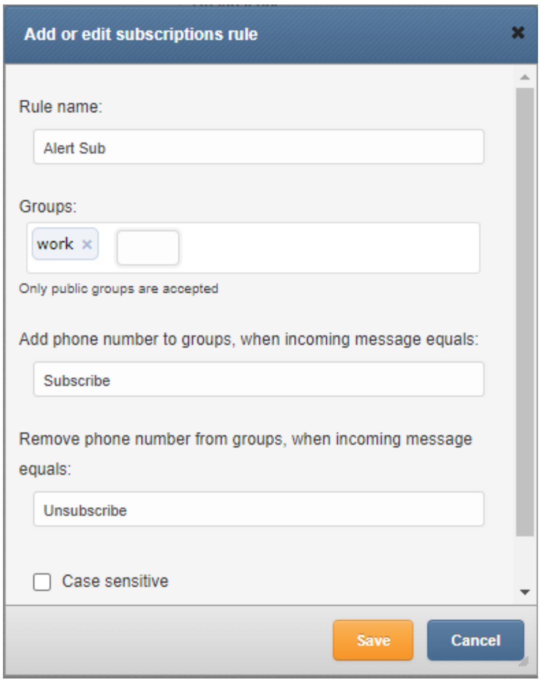
This feature allows to enable newsletter-style subscriptions via SMS. When someone sends a message to your SMSEagle which includes a defined text, the sending number will be automatically added to a Phonebook group. This group can be later used to send messages via web-GUI/API/Email To SMS. Automatic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



Subscriptions

No	Rule name	Add phone number to groups, when incoming message equals	Remove phone number from groups, when incoming message equals	Groups	Manage
1	Alert Sub	Subscribe	Unsubscribe	work	Edit Delete Disable

Screenshot from "Subscriptions" feature



Add or edit subscriptions rule

Rule name: Alert Sub

Groups: work ×

Only public groups are accepted

Add phone number to groups, when incoming message equals: Subscribe

Remove phone number from groups, when incoming message equals: Unsubscribe

□ Case sensitive

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.

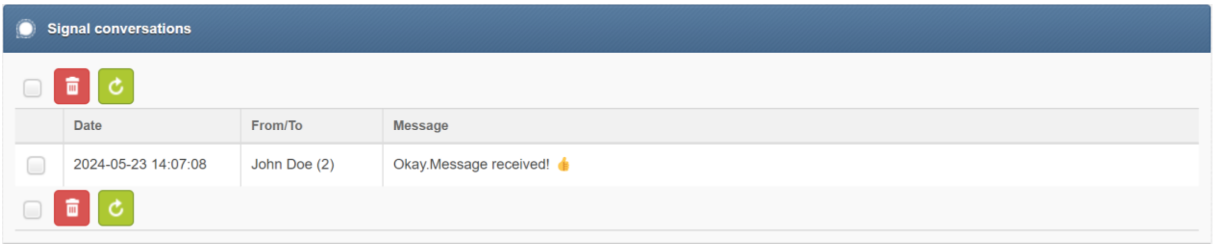
Signal (beta)

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. The messaging relies on data, so your device should be connected to the Internet via Ethernet or mobile data.

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.

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



	Date	From/To	Message
□	2024-05-23 14:07:08	John Doe (2)	Okay.Message received! 👍

Screenshot from menu Signal > Conversations

MQTT

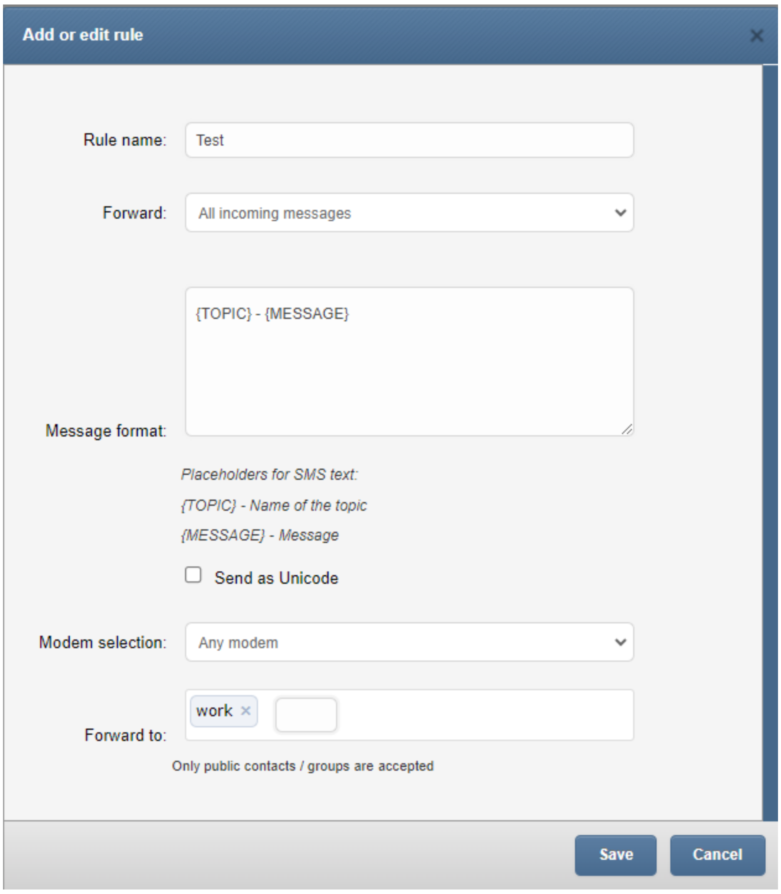
MQTT is a messaging protocol for the Internet of Things (IoT). It is designed as an extremely lightweight publish/subscribe messaging transport that is ideal for connecting remote devices with a minimal network bandwidth. MQTT today is used in a wide variety of industries, such as automotive, manufacturing,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

The MQTT feature on SMSEagle lets you convert MQTT to SMS & SMS to MQTT. You can 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.



Rule name: Test

Forward: All incoming messages

Message format: {TOPIC} - {MESSAGE}

Placeholders for SMS text:
{TOPIC} - Name of the topic
{MESSAGE} - Message

□ Send as Unicode

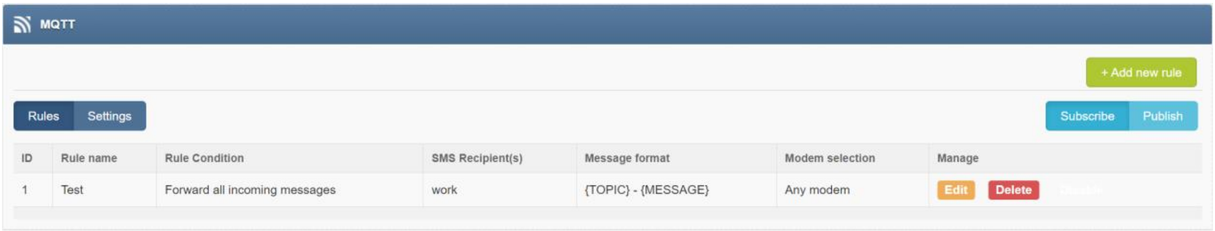
Modem selection: Any modem

Forward to: work ×

Only public contacts / groups are accepted

Screenshot from MQTT add rule

SUBSCRIBE RULES



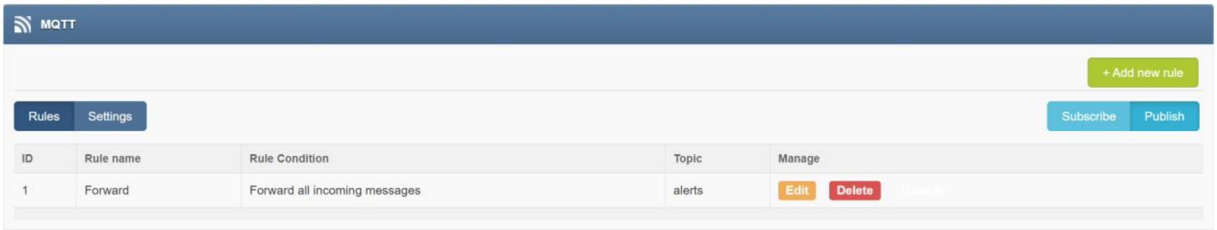
ID	Rule name	Rule Condition	SMS Recipient(s)	Message format	Modem selection	Manage
1	Test	Forward all incoming messages	work	{TOPIC} - {MESSAGE}	Any modem	Edit Delete

Screenshot from MQTT subscribe window

For each processing rule user can define:

1. if forwarding should always be sent or only form 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



ID	Rule name	Rule Condition	Topic	Manage
1	Forward	Forward all incoming messages	alerts	Edit Delete

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

SMPP

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.

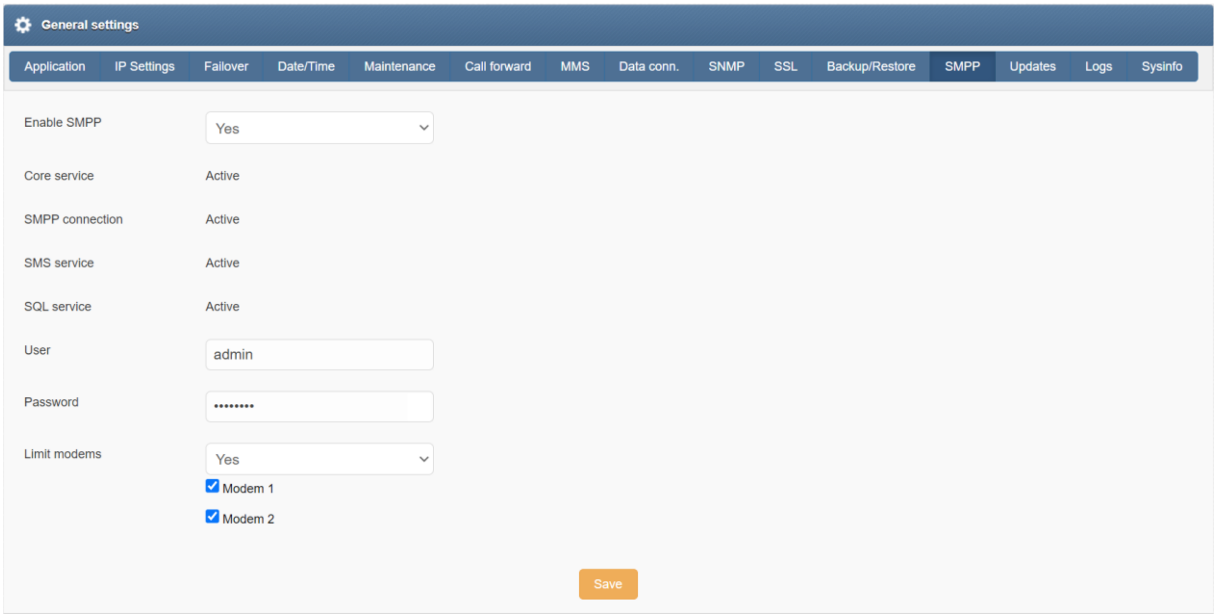
The SMPP protocol is often used to allow third parties to send messages to SMS gateways for further processing.

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)



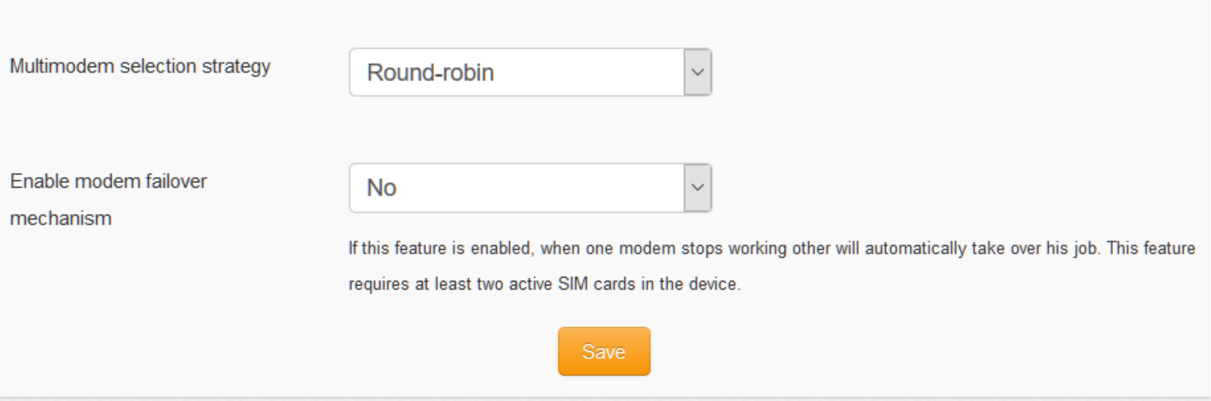
Enable SMPP	Yes
Core service	Active
SMPP connection	Active
SMS service	Active
SQL service	Active
User	admin
Password	••••••••
Limit modems	Yes ☑ Modem 1 ☑ Modem 2

screenshot from menu Settings > SMPP

The SMPP server supports SMPP version 3.4.

MULTIMODEM FEATURES

SMSEagle MHD-8100 device is equipped with eight built-in modems. You can manage modem settings in web-GUI menu Settings > Maintenance Tab. There are following options available for multimodem device:



Multimodem selection strategy: Round-robin

Enable modem failover mechanism: No

If this feature 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.

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 > modem3 > modem4, etc.
- SIMX as Master modem
  In this strategy modemX is always selected when sending out SMS messages. If failover is enabled (see below) other modems 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.

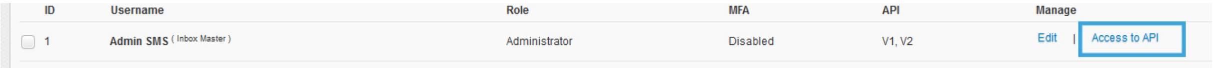
- **API v2 – recommended for new projects**
  Modern RESTful API based on OpenAPI 3.0 specification
  Link to APIv2 Reference

- **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.

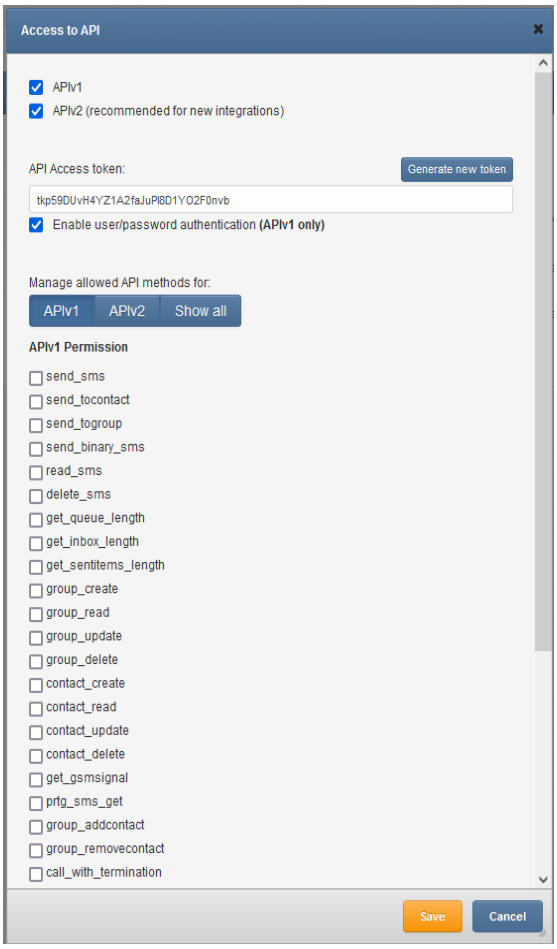
API Access

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.



	ID	Username	Role	MFA	API	Manage
□	1	Admin SMS (Inbox Master)	Administrator	Disabled	V1, V2	Edit | Access to API

Screenshot from menu "Users" with marked "Access to API" link.



Access to API

☑ APIv1
☑ APIv2 (recommended for new integrations)

API Access token: Generate new token

tkp59DUvH4YZ1A2faJuPl8D1YO2F0nvb

☑ Enable user/password authentication **(APIv1 only)**

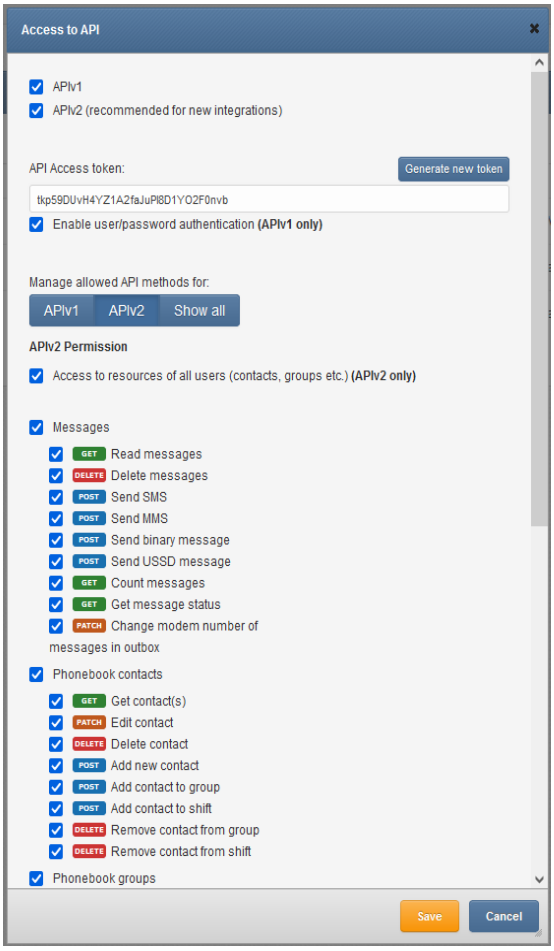
Manage allowed API methods for:

APIv1 | APIv2 | Show all

APIv1 Permission

□ send_sms
□ send_tocontact
□ send_togroup
□ send_binary_sms
□ read_sms
□ delete_sms
□ get_queue_length
□ get_inbox_length
□ get_sentitems_length
□ group_create
□ group_read
□ group_update
□ group_delete
□ contact_create
□ contact_read
□ contact_update
□ contact_delete
□ get_gsmsignal
□ prtg_sms_get
□ group_addcontact
□ group_removecontact
□ call_with_termination

Save | Cancel



Access to API

☑ APIv1
☑ APIv2 (recommended for new integrations)

API Access token: Generate new token

tkp59DUvH4YZ1A2faJuPl8D1YO2F0nvb

☑ Enable user/password authentication **(APIv1 only)**

Manage allowed API methods for:

APIv1 | APIv2 | Show all

APIv2 Permission

☑ Access to resources of all users (contacts, groups etc.) **(APIv2 only)**

☑ Messages

- ☑ GET Read messages
- ☑ DELETE Delete messages
- ☑ POST Send SMS
- ☑ POST Send MMS
- ☑ POST Send binary message
- ☑ POST Send USSD message
- ☑ GET Count messages
- ☑ GET Get message status
- ☑ PATCH Change modem number of messages in outbox

☑ Phonebook contacts

- ☑ GET Get contact(s)
- ☑ PATCH Edit contact
- ☑ DELETE Delete contact
- ☑ POST Add new contact
- ☑ POST Add contact to group
- ☑ POST Add contact to shift
- ☑ DELETE Remove contact from group
- ☑ DELETE Remove contact from shift

☑ Phonebook groups

Save | Cancel

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 INTEGRATION MANUALS FOR NMS & AUTH SYSTEMS

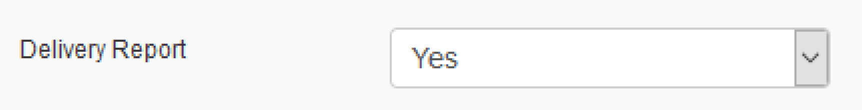
SMSEagle has a number of ready-to-use plugins and integration manuals for an easy and quick integration of SMSEagle device with external software (Network Monitoring Systems, Authentication Systems and other). The list grows constantly and is published on SMSEagle website. For a complete and up to date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

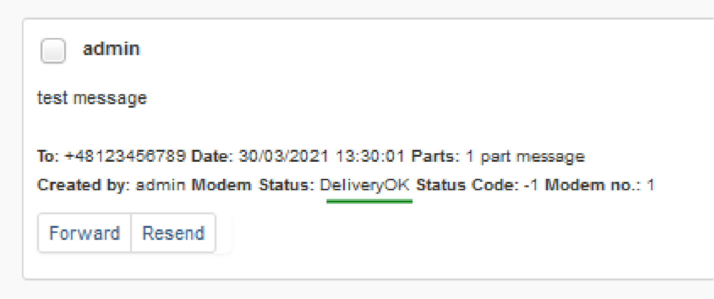
In order to enable delivery reports, please go to web-GUI > menu Settings and set "Delivery Reports" to "Yes"



Delivery Report: 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



☐ admin

test message

To: +48123456789 Date: 30/03/2021 13:30:01 Parts: 1 part message
Created by: admin Modem Status: DeliveryOK Status Code: -1 Modem no.: 1

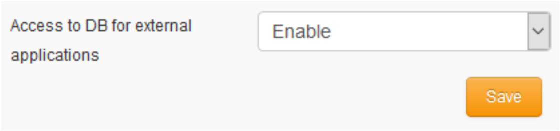
- **Using Callback URL**
  CallbackURL feature allows to define a webook for the change of delivery status. Webhooks are standard HTTP endpoints implemented in your external application that will accept HTTP requests from SMSEagle device. Webhooks save you from having to continuously send requests to 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 chapter **Błąd! Nie można odnaleźć źródła odwołania.** table "Field Description Of Response Data – Sentitems Folder."

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:



Access to DB for external applications: Enable

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

POSTGRESQL DATABASE 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, SenderID = smseagle2 for modem 2, etc.

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:

```
/opt/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 /opt/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 1 st modem) .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 modem) Etc.

FolderOutbox_Total	Returns number of SMS messages in Outbox folder (outgoing queue length)	.1.3.6.1.4.1.8072.1.3.2.3.1.2.18.70.111.108.100.101.114.79.117.116.98.111.120.95.84.111.116.97.108
FolderInbox_Total	Returns number of SMS messages in Inbox folder	.1.3.6.1.4.1.8072.1.3.2.3.1.2.17.70.111.108.100.101.114.73.110.98.111.120.95.84.111.116.97.108
FolderSent_Last24H	Returns number of SMS messages sent from the device within last 24 hours	.1.3.6.1.4.1.8072.1.3.2.3.1.2.18.70.111.108.100.101.114.83.101.110.116.95.76.97.115.116.50.52.72
FolderSent_Last1M	Returns number of SMS messages sent from the device within last month	.1.3.6.1.4.1.8072.1.3.2.3.1.2.17.70.111.108.100.101.114.83.101.110.116.95.76.97.115.116.49.77
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)	.1.3.6.1.4.1.8072.1.3.2.3.1.2.25.70.111.108.100.101.114.83.101.110.116.95.76.97.115.116.50.52.72.83.101.110.100.69.114.114
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 modem) .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 modem) Etc.
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 (for 1st modem) .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 (for 2nd modem) Etc.

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 **SYSTEMUPTIME** 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 hours, 6.22 minutes

EXAMPLE OF BROWSING SMSEAGLE EXTENSION PARAMETERS IN MIB TREE USING NET-SNMP LIBRARY

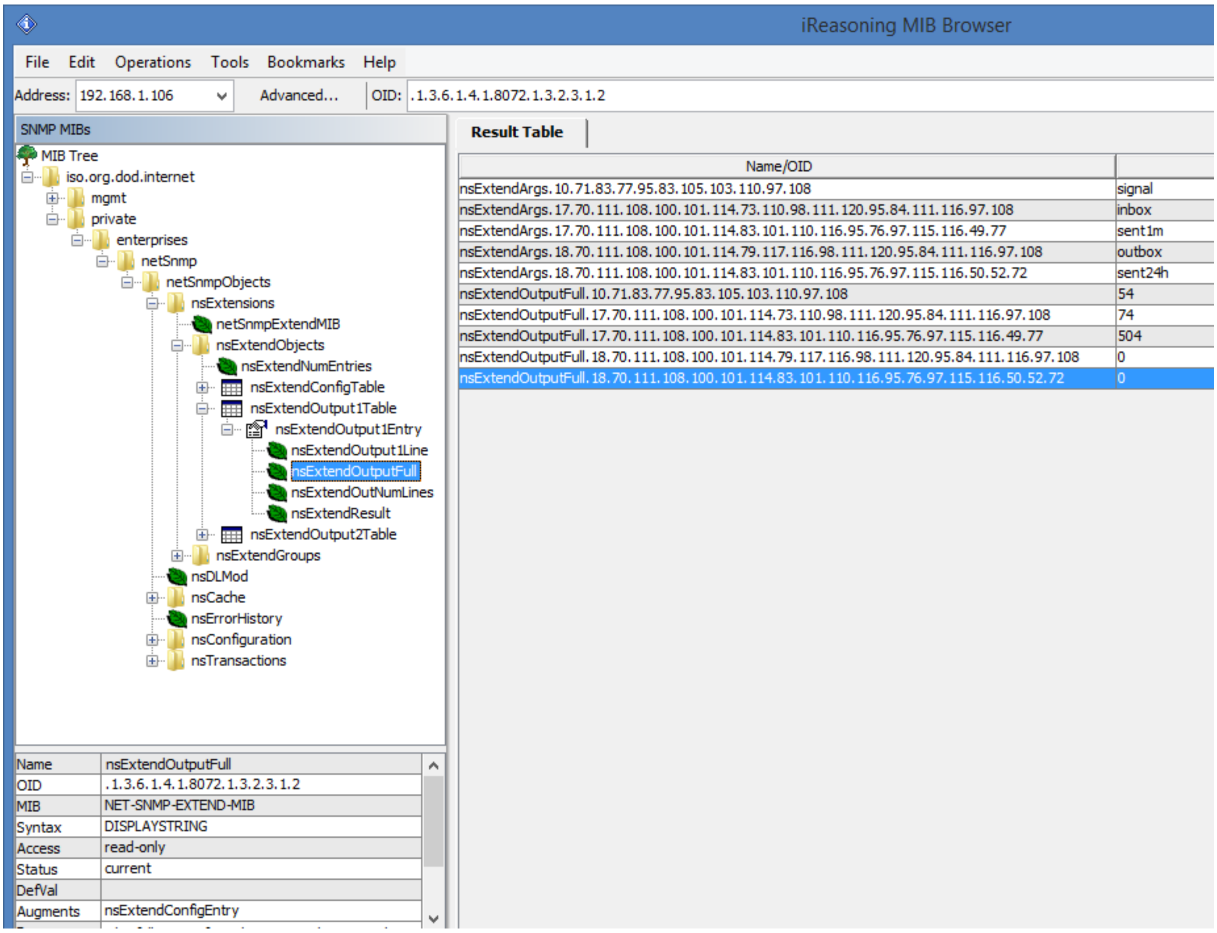
a) Command for reading the result value:

```
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_Signal2" = 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



Name/OID	
nsExtendArgs.10.71.83.77.95.83.105.103.110.97.108	signal
nsExtendArgs.17.70.111.108.100.101.114.73.110.98.111.120.95.84.111.116.97.108	inbox
nsExtendArgs.17.70.111.108.100.101.114.83.101.110.116.95.76.97.115.116.49.77	sent1m
nsExtendArgs.18.70.111.108.100.101.114.79.117.116.98.111.120.95.84.111.116.97.108	outbox
nsExtendArgs.18.70.111.108.100.101.114.83.101.110.116.95.76.97.115.116.50.52.72	sent24h
nsExtendOutputFull.10.71.83.77.95.83.105.103.110.97.108	54
nsExtendOutputFull.17.70.111.108.100.101.114.73.110.98.111.120.95.84.111.116.97.108	74
nsExtendOutputFull.17.70.111.108.100.101.114.83.101.110.116.95.76.97.115.116.49.77	504
nsExtendOutputFull.18.70.111.108.100.101.114.79.117.116.98.111.120.95.84.111.116.97.108	0
nsExtendOutputFull.18.70.111.108.100.101.114.83.101.110.116.95.76.97.115.116.50.52.72	0

Name	nsExtendOutputFull
OID	.1.3.6.1.4.1.8072.1.3.2.3.1.2
MIB	NET-SNMP-EXTEND-MIB
Syntax	DISPLAYSTRING
Access	read-only
Status	current
DefVal	
Augments	nsExtendConfigEntry

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 */opt/smseagle* directory.

1. *Log in via SSH using root account*
2. *Navigate to:*
   cd /opt/smseagle/
3. *Configuration script:*
   ./snmpv3
4. *Script can run with following parameters:*
   i. *add*
   ii. *del*
   iii. *enablev2*
   iv. *disablev2*
5. *To add v3 USER please run:*
   ./snmpv3 add USERNAME PASSWORD ENCRYPTIONPASSWORD

6. *To delete USER please run:*
   ./snmpv3 del

7. *To disable v2 access policy run:*
   ./snmpv3 disablev2

8. *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: https://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

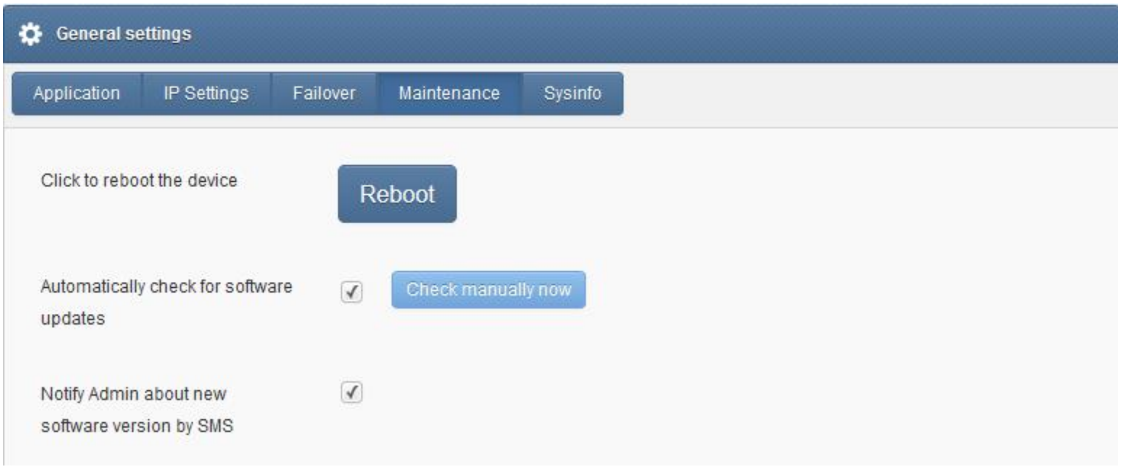
SMSEagle software is under process of continual improvement. We listen to our customers, and new releases are based on our customer's inputs/requests. Software updates are released frequently, and offer access to new features and fixes to reported issues. Web-GUI offers you a possibility to automatically 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 Maintenance. Click on the button "Check manually 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 Maintenance, 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.



Click to reboot the device

Automatically check for software updates ☑

Notify Admin about new software version by SMS ☑

Screenshot from "General settings-Maintenance"

Notice: Your SMSEagle device must have a HTTPS connectivity with address www.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

03 TROUBLESHOOTING

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

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

LED	Correct operation
Power (button light)	Continuously lit
STATUS	Blinking
ACTIVE1-8	Slow flashing in stand-by mode, Quick flashing when modem 1 in use

Checking the device information

The device information (device type, software version, modem IMEI, IMSI, network signal strength, network name) can be found under 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

This action restores the following settings to default values: **IP settings, time zone settings, database content**, **Linux OS users/passwords**

In order to restore factory defaults, proceed with the following steps:

1. When the device is ready to operate (STATUS LED is blinking)
2. **Press and hold SW button for 10 seconds**
3. Release SW button after 10 seconds (you will see "*Factory reset*" on display)
4. Wait until system reboots.

Please note, that after reboot the device will be finishing the process of factory reset, therefore it can take longer for the system to start.

04 SERVICE & REPAIR

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 a detailed information on warranty terms and conditions check warranty card that comes with your device or follow the link: www.smseagle.eu/docs/general_warranty_terms_and_conditions.pdf

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

05 TECH SPECS & SAFETY INFORMATION

TECH SPECS & SAFETY INFORMATION

Technical Specification

HARDWARE SPECIFICATION

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

    MHD-8100-3G:

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

    MHD-8100-4G:

    - Wavebands: UMTS, LTE

    - LTE FDD: B1/B2/B3/B4/B5/B7/B8/B12/B13/B18/B19/B20/B25/B26/B28
    - LTE TDD: B38/B39/B40/B41
    - UMTS: B1/B2/B4/B5/B6/B8/B19
    - Output power (Rated):
        - Class 3 (24dBm+1/-3dB) for WCDMA bands
        - Class 3 (23dBm±2dB) for LTE-FDD bands
        - Class 3 (23dBm±3dB) for LTE-TDD bands

- SIM card standard: mini
- Antenna connector: 8x SMA
- Country of origin: European Union (Poland)

POWER SUPPLY

AC line input

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

Frequency: 50–60Hz single phase

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

ANTENNA

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

SENDING/RECEIVING THROUGHPUT

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

SOFTWARE PLATFORM

- Operating system:
    - device Rev.1.1: Ubuntu 22.04
    - device Rev.1: Ubuntu 18.04

- built-in Apache2 web server
- built-in PostgreSQL database server
- built-in Postfix email server
- built-in SNMP agent
- built-in NTP-client
- built-in Failover (HA-cluster) service
- watchdog mechanism for built-in modems
- failover mechanism for built-in modems
- modern responsive web interface

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

RESPONSIBLE PARTY located in the United States:

Testing Partners LLC
18200 SR 306
Chagrin Falls, OH 44023
info@testingpartners.com

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

Canadian Regulatory Statement

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

(1) this device may not cause interference, and
(2) this device must accept any interference, including interference that may cause undesired operation of the device.

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

CAN ICES-3 (B)/NMB-3(B)

Avis de conformité à la réglementation d'Industrie Canada

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

(1) l'appareil ne doit pas produire de brouillage,
(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Cet appareil numérique de classe B répond aux exigences du Règlement sur le matériel brouilleur du Canada.

CAN ICES-3 (B)/NMB-3(B)

UK Declaration of Conformity

Hereby, Proximus Sp. z o.o., owner of SMSEagle brand, declares that the radio equipment type SMSEagle MHD-8100-4G 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

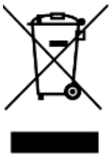
RF Exposure Limits

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 31 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.1-3	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.1-3:

- 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").

SMSEagle

Your Gateway
to Unbreakable
Communication

Proximus Sp. z o.o.
ul. Piątkowska 163
60-650 Poznań, Poland 1 Europe

T +48 61 6713 413
E hello@smseagle.eu
www.smseagle.eu