DOKUMENTATION 7.00

NXS-9700 Benutzerhandbuch

Dokumentation

DEUTSCH · SMSEAGLE

Dieses Dokument wurde automatisch (KI) übersetzt und kann Fehler enthalten.

Table of contents

Cover . . . 9

Lizenzinformationen zur SMSEagle-Software . . . 10

Was im Lieferumfang enthalten ist . . . 19

Konfigurationsassistent . . . 21

- Schritt 1: Sprache & Zeit . . . 21
- Schritt 2: Administrator-Konto . . . 21
- Schritt 3: Benachrichtigungen . . . 22
- Schritt 4: Modems . . . 23

Anschlüsse, Anschlussöffnungen und LEDs . . . 24

Übersicht der Weboberfläche . . . 26

- Anmeldung . . . 26
- Oberflächenlayout . . . 27
- Dashboard . . . 27
  - Needs your attention . . . 28
  - Traffic . . . 28
  - Unread messages . . . 29
  - System . . . 29
  - Neueste Nachrichten und Anrufe . . . 30
  - Modems . . . 30
- Schnellaktionen . . . 30
- Persönliche Kontoeinstellungen . . . 31
  - Persönliche Daten . . . 31
  - Passwort . . . 32
  - Sicherheit . . . 32

Nachrichten . . . 33

- SMS (Konversationen) . . . 33
  - Verfassen einer Nachricht . . . 34
- Ordner . . . 35
- Gruppennachrichten . . . 36
- Eskalationswarteschlange . . . 37
- Anrufe . . . 38
  - Verlauf . . . 38
- WhatsApp . . . 39
- Signal . . . 41
- E-Mails . . . 42
- Nachrichtenvorlagen . . . 42

Telefonbuch . . . 44

- Kontakte . . . 44
- Gruppen . . . 44
  - Eskalationsgruppen . . . 45

Schichten . . . 47
Bevor Sie beginnen . . . 47
Schritt 1: Öffnen Sie die Seite „Shifts“ . . . 47
Schritt 2: Erstellen Sie eine Schicht . . . 47
Schritt 3: Weisen Sie Kontakte der Schicht zu . . . 48
Schritt 4: Wählen Sie, was außerhalb der Schichtzeiten passiert . . . 48
Automatisierung . . . 49
Email zu SMS . . . 49
Wo finden Sie es . . . 49
Schritt 1: Verstehen Sie das Format der Empfängeradresse . . . 49
Schritt 2: Erstellen Sie eine neue Regel . . . 50
Schritt 3: Filterbedingungen hinzufügen (optional) . . . 51
Schritt 4: Vorhandene Regeln verwalten . . . 52
Email zu SMS Poller . . . 52
Wo finden Sie es . . . 52
Eine Regel erstellen . . . 53
SMS zu Email . . . 53
Was diese Funktion bewirkt . . . 53
Bevor Sie beginnen . . . 53
Schritt 1: SMS zu Email-Seite öffnen . . . 53
Schritt 2: Eine Regel erstellen . . . 53
SMS Forward . . . 55
Was diese Funktion bewirkt . . . 55
Bevor Sie beginnen . . . 55
Schritt 1: Öffnen Sie die Seite SMS Forward . . . 56
Schritt 2: Eine Regel erstellen . . . 56
So funktioniert die Weiterleitung . . . 58
Automatische Antworten . . . 58
Was diese Funktion bewirkt . . . 58
Bevor Sie beginnen . . . 58
Schritt 1: Öffnen Sie die Seite Autoreplies . . . 59
Schritt 2: Eine Regel erstellen . . . 59
Schritt 3: Sendegrenze festlegen . . . 60
Wie Matching funktioniert . . . 60
Periodische SMS . . . 61
Was diese Funktion bewirkt . . . 61
Bevor Sie beginnen . . . 61
Schritt 1: Öffnen Sie die Seite Periodische SMS . . . 61
Schritt 2: Eine Regel erstellen . . . 61
Abos . . . 63
Was diese Funktion bewirkt . . . 63
Bevor Sie beginnen . . . 64
Schritt 1: Öffnen Sie die Abos-Seite . . . 64
Schritt 2: Eine Regel erstellen . . . 64
Wie Matching funktioniert . . . 64
Was passiert, wenn sich jemand anmeldet . . . 65
Allow / Deny List . . . 65

Was diese Funktion bewirkt . . . 65
Bevor Sie beginnen . . . 66
Schritt 1: Öffnen Sie die Allow / Deny List-Seite . . . 66
Schritt 2: Wählen Sie den aktiven Modus . . . 66
Schritt 3: Eine Nummer hinzufügen . . . 66
Schritt 4: Eine Liste aus CSV importieren . . . 67
Schritt 5: Das STOP-Wort konfigurieren (optional) . . . 67
So funktioniert die Filterung . . . 68
Workflows . . . 68
Wo finden Sie es . . . 69
Schritt 1: Einen Workflow erstellen und einen Trigger auswählen . . . 69
Schritt 2: Bedingungsgruppen hinzufügen (optional) . . . 69
Schritt 3: Aktionen hinzufügen . . . 69
Webhooks . . . 70
Was diese Funktion bewirkt . . . 70
Bevor Sie beginnen . . . 70
Schritt 1: Webhooks-Seite öffnen . . . 70
Schritt 2: Eine Regel erstellen . . . 71
Schritt 3: Grundkonfiguration . . . 71
Schritt 4: Triggerbedingungen . . . 73
Schritt 5: Sicherheitseinstellungen . . . 74
Schritt 6: Wiederholungsintervall festlegen . . . 74
Verhalten von Webhooks . . . 75
MQTT . . . 75
Was diese Funktion bewirkt . . . 75
Bevor Sie beginnen . . . 76
Teil 1: Abonnieren (MQTT in SMS) . . . 76
Teil 2: Publish (SMS in MQTT) . . . 78
Inbox-Regeln . . . 79
Wo finden Sie es . . . 79
Konfigurieren einer Inbox-Regel . . . 80
Ordner bereinigen . . . 80
Wo finden Sie es . . . 80
Konfigurieren einer Bereinigungsregel . . . 80
Berichte & Statistiken . . . 81
Berichte . . . 81
Regelmäßige Berichte . . . 82
Statistiken . . . 83
Periodische Statistiken . . . 84
Überwachung . . . 85
Netzwerküberwachung . . . 85
Was diese Funktion tut . . . 85
Bevor Sie beginnen . . . 85
Teil 1: Aufgaben . . . 86
Teil 2: Berichte . . . 91
Teil 3: SNMP Traps . . . 92

Verhalten des Netzwerk-Monitors . . . 94
Digitale Ein-/Ausgangsports . . . 95
Was diese Funktion tut . . . 95
Bevor Sie beginnen . . . 95
Hardware: ports, logic levels and wiring . . . 96
Wo zu finden . . . 99
Teil 1: Eingaberegeln (Eingabesignal in SMS) . . . 100
Teil 2: Ausgaberegeln (SMS in Ausgabesignal) . . . 103
Teil 3: Interne Anschlüsse . . . 106
Teil 4: Externe Anschlüsse . . . 107
Wie sich Digital-I/O-Regeln verhalten . . . 108
Temperatur- und Feuchtigkeitssensoren . . . 109
Was diese Funktion tut . . . 109
Bevor Sie beginnen . . . 109
Wo zu finden . . . 110
Teil 1: Sensoren hinzufügen und benennen . . . 110
Teil 2: Alarmregeln . . . 113
Teil 3: Messwerte und Berichte . . . 115
Funktionsweise . . . 116
Einstellungen . . . 117
Kontoeinstellungen . . . 117
Konfiguration der Multi-Faktor-Authentifizierung (MFA) . . . 117
SMS / MMS . . . 118
Nachrichten . . . 118
Modems . . . 119
Multi-Modem . . . 119
MMS . . . 120
Anrufe . . . 122
TTS-Lokalmodelle . . . 122
mit ausgewähltem .onnx-Modell und .onnx.json-Konfiguration . . . 124
Eingehende Anrufe . . . 126
Anrufweiterleitung . . . 126
WhatsApp . . . 127
Was diese Funktion tut . . . 127
Bevor Sie beginnen . . . 127
Schritt 1: Öffnen Sie die WhatsApp-Einstellungen . . . 128
Schritt 2: Aktivieren Sie den Dienst . . . 128
Schritt 3: Verknüpfen Sie Ihr Telefon . . . 128
Schritt 4: Entscheiden Sie, was mit Nicht-WhatsApp-Empfängern geschieht . . . 128
Schritt 5: Halten Sie den Dienst auf dem neuesten Stand . . . 128
Verknüpfung aufheben und Ausschalten . . . 129
Wichtig zu wissen . . . 129
Signal . . . 130
Was diese Funktion tut . . . 130
Bevor Sie beginnen . . . 130
Schritt 1: Öffnen Sie die Signal-Einstellungen . . . 131
Schritt 2: Aktivieren Sie den Dienst . . . 131

Schritt 3: Registrieren Sie eine Telefonnummer . . . 131
Schritt 4: Nummer verifizieren . . . 132
Schritt 5: Halten Sie den Dienst auf dem neuesten Stand . . . 132
Entfernung der Nummer . . . 132
Wichtig zu wissen . . . 133
Email . . . 133
E-Mail zu SMS . . . 133
Email to SMS Poller . . . 135
SMTP-Konfiguration . . . 137
E-Mail-Benachrichtigungen . . . 137
SMPP . . . 138
Verbindungsdetails . . . 139
SMPP aktivieren . . . 139
MQTT . . . 140
Netzwerk . . . 141
IP-Einstellungen . . . 141
SSL . . . 142
Failover . . . 142
SNMP . . . 143
Mobile Daten . . . 148
Anwendung . . . 149
Regional . . . 149
Sicherheit . . . 149
Zugriff und Sichtbarkeit . . . 149
API und Integrationen . . . 150
LDAP . . . 150
Was diese Funktion tut . . . 150
Bevor Sie beginnen . . . 151
Schritt 1: Öffnen Sie die LDAP-Seite . . . 151
Schritt 2: Aktivieren Sie die Integration . . . 151
Schritt 3: Verbindung . . . 152
Schritt 4: Verzeichnisstruktur . . . 152
Schritt 5: Attribute und Sicherheit . . . 153
Schritt 6: Synchronisierung und Zugriff . . . 153
Schritt 7: Speichern und testen . . . 155
Datum / Zeit . . . 155

System . . . 156
Benutzer . . . 156
Systeminformationen . . . 156
Logs . . . 157
Updates . . . 157
Patches . . . 157
Backup / Restore . . . 157
Restart . . . 157
Advanced . . . 158

API und Entwicklerintegrationen . . . 159
API-Referenz . . . 159
API-Schlüssel . . . 159
API v2-Schlüssel . . . 159
API v1-Schlüssel . . . 160
Erstellen eines Schlüssels . . . 160
Welche Benutzer haben API-Zugriff . . . 161
Zugriff auf Ressourcen anderer Benutzer . . . 162
Plugins und Integrationen . . . 163
Erweitert . . . 164
Direktes Verbinden mit der SMSEagle-Datenbank . . . 164
Einfügen einer kurzen SMS über SQL . . . 164
Einfügen einer langen SMS über SQL . . . 165
Datenbankbereinigungsskripte . . . 167
Weiterleitungsprotokolle an einen externen Server . . . 167
Fehlerbehebung . . . 169
Überprüfung der LEDs . . . 169
Überprüfung der Geräteinformationen . . . 170
Gerätelogs . . . 170
Wenn das Gerät nicht erreichbar ist . . . 170
Wiederherstellen der Werkseinstellungen . . . 170
Hardware Rev. 5 und später . . . 171
Hardware Rev. 3–Rev. 4 . . . 171
Service & Reparatur . . . 172
Garantie . . . 172
Service . . . 172
Technische Spezifikationen und Sicherheitsinformationen . . . 173
Technische Spezifikation . . . 173
Hardware-Spezifikation . . . 173
Stromversorgung . . . 176
Antenne . . . 176
Durchsatz beim Senden/Empfangen . . . 177
Softwareplattform . . . 177
Wichtige Sicherheitsinformationen . . . 177
Behördliche Erklärungen . . . 179
EU-Konformitätserklärung . . . 179
FCC-Konformitätserklärung . . . 179
FCC-Konformitätserklärung des Lieferanten . . . 180
Kanadische Behördenerklärung (ISED) . . . 180
Avis de conformité à la réglementation d'Industrie Canada . . . 181
UK Declaration of Conformity . . . 181
HF-Expositionsgrenzwerte . . . 181
Entsorgung und Recycling-Informationen . . . 181

Europäische Union – Entsorgungsinformationen 181
Für die Entsorgung in Ländern außerhalb der Europäischen Union 182
Information gemäß § 4 Absatz 4 Elektrogesetz (DE) 182
Angaben zur sicheren Entnahme der Batterien oder der Akkumulatoren 182
Restriction of Hazardous Substances Directive (RoHS) 183
Europäische Union RoHS 183

Cover

Willkommen im NXS-9700 Benutzerhandbuch!

Das NXS-9700 ist ein Hardware-SMS-Gateway mit einem integrierten Modem und Ihrer eigenen SIM-Karte. Ihre Nachrichten werden direkt über das Mobilfunknetz aus Ihrer eigenen Infrastruktur versendet – ohne einen SMS-Provider eines Drittanbieters dazwischen.

Dieses Handbuch ist die vollständige Referenz für das Gerät und gilt für alle NXS-9700-Varianten. Wenn das Verhalten vom Modemtyp oder der Hardware-Revision abhängt, ist der betreffende Abschnitt mit einem Badge gekennzeichnet. Wenn sich Ihr Gerät noch in der Verpackung befindet, beginnen Sie mit What's In The Box und führen Sie dann den Configuration Wizard aus. Verwenden Sie andernfalls die Navigation auf der linken Seite oder das Suchfeld, um direkt zum benötigten Thema zu gelangen.

Die in dieser Veröffentlichung verwendeten Materialien unterliegen dem Urheberrecht und dürfen nicht ohne vorherige Zustimmung des Urheberrechtsinhabers vervielfältigt, kopiert oder verwendet werden. Die technischen Spezifikationen und Informationen in diesem Dokument können ohne vorherige Ankündigung geändert werden.

Lizenzinformationen zur SMSEagle-Software

WICHTIG – VOR DER INBETRIEBNAHME LESEN!

SMSEAGLE-SOFTWARE-ENDBENUTZER-LIZENZVERTRAG

Der hierin enthaltene Endbenutzer-Lizenzvertrag (der „**Vertrag**“ oder die „**Lizenz**“ oder der „**EULA**“) gilt als rechtlich bindende Vereinbarung zwischen Ihnen (einer natürlichen oder juristischen Person, nachfolgend „**Lizenznehmer**“ oder „**Sie**“ bzw. „**Ihr**“) und Proximus Sp. z o.o., ul. Piątkowska 163, Poznań, Polen, Postleitzahl 60-650 (nachfolgend „**PROXIMUS**“) für die Nutzung der auf einem SMSEagle-Gerät vorinstallierten Software (d. h. Software, die zusammen mit diesem Gerät installiert und ausgeliefert wird), die gedrucktes Begleitmaterial sowie beliebige weitere Komponenten und/oder Softwaremodule umfassen kann, einschließlich, aber nicht beschränkt auf erforderliche Treiber (die „**SMSEagle-Software**“). Weitere Aspekte der SMSEagle-Software können außerdem, jedoch nicht ausschließlich, Software-Updates und Upgrades umfassen, die PROXIMUS Ihnen liefert oder zur Verfügung stellt oder die Sie nach dem Erwerb des SMSEagle-Geräts erhalten, sofern diesen Elementen kein separater Lizenzvertrag oder separate Nutzungsbedingungen beiliegen.

DURCH DIE ANNAHME DIESER BEDINGUNGEN IN DER GRAFISCHEN BENUTZEROBERFLÄCHE (GUI) DES SMSEAGLE-GERÄTS, DURCH DIE NUTZUNG DES SMSEAGLE-GERÄTS ODER DURCH DIE AKTUALISIERUNG BZW. DAS UPGRADE DER SMSEAGLE-SOFTWARE ERKLÄREN SIE SICH DAMIT EINVERSTANDEN, RECHTLICH AN DIE HIERIN ENTHALTENEN BEDINGUNGEN DIESES LIZENZVERTRAGS GEBUNDEN ZU SEIN. WENN SIE DEN BEDINGUNGEN DIESER EULA NICHT ZUSTIMMEN, VERWENDEN SIE DAS SMSEAGLE-GERÄT NICHT UND KÖNNEN DAS GERÄT UMGEHEND GEGEN ERSTATTUNG DES KAUFPREISES ZURÜCKSENDEN, INDEM SIE PROXIMUS UNTER DER OBEN GENANNTEN ADRESSE KONTAKTIEREN. Die aktuelle Version dieser EULA wird Ihnen vor dem Kauf auf www.smseagle.eu zur Verfügung gestellt und wird während der Ersteinrichtung sowie nach jeder wesentlichen Änderung ihrer Bedingungen in der GUI des SMSEagle-Geräts angezeigt. Ihre Zustimmung in der GUI (einschließlich Datum, Version und Gerätekennung) wird lokal in der Datenbank des SMSEagle-Geräts gespeichert. Wenn Sie den Bedingungen in der GUI nicht zustimmen, wird die SMSEagle-Software nicht zur Nutzung aktiviert.

DIE SMSEAGLE-SOFTWARE IST DURCH URHEBERRECHTSGESETZE SOWIE ALLE ANDEREN EINSCHLÄGIGEN GESETZE ZUM SCHUTZ GEISTIGEN EIGENTUMS GESCHÜTZT. DIE SMSEAGLE-SOFTWARE WIRD LIZENZIERT UND NICHT VERKAUFT. ALLE RECHTE, EINSCHLIESSLICH DER URHEBERRECHTE, AN DER SMSEAGLE-SOFTWARE VERBLEIBEN AUSSCHLIESSLICH IM EIGENTUM VON PROXIMUS. WIE NACHSTEHEND BESCHRIEBEN, ENTHÄLT DIE SMSEAGLE-SOFTWARE ZUSÄTZLICH EINIGE VON DRITTEN ENTWICKELTE MODULE, DIE IHNEN HIERMIT GEMÄSS DEN VOM ENTWICKLER ZUGELASSENEN BEDINGUNGEN UNTERLIZENZIERT WERDEN.

Diese EULA gewährt Ihnen bestimmte gesetzliche Rechte; darüber hinaus können Sie je nach Rechtsordnung weitere gesetzliche Rechte besitzen. Die in dieser EULA enthaltenen Haftungsausschlüsse, Ausschlüsse und Haftungsbeschränkungen gelten nur insoweit, als dies nach geltendem Recht nicht untersagt ist. Manche Rechtsordnungen erlauben den Ausschluss stillschweigender Gewährleistungen oder den Ausschluss bzw. die Beschränkung von Neben- oder

Folgeschäden oder anderer Rechte nicht; in solchen Fällen gelten die entsprechenden Bestimmungen dieser EULA für Sie möglicherweise nicht. Dies beeinträchtigt jedoch nicht die Durchsetzbarkeit und Anwendbarkeit aller übrigen Bestimmungen der EULA.

1. **DEFINITIONEN UND AUSLEGUNG**
    1. „Vertrag“ oder „Lizenz“ oder „EULA“ bezeichnet diesen Endbenutzer-Lizenzvertrag.
    2. „Lizenznehmer“ oder „Sie“ bzw. „Ihr“ bezieht sich auf Sie, die natürliche oder juristische Person, die ein SMSEagle-Gerät erwirbt, auf dem die SMSEagle-Software installiert wurde.
    3. „Geistiges Eigentum“ bezeichnet gegenwärtige und zukünftige weltweite Rechte gemäß Urheberrecht, Patentrecht, Geschäftsgeheimnisrecht, Markenrecht, Urheberpersönlichkeitsrecht und anderen vergleichbaren Rechten.
    4. „Update“ bezeichnet die Wartung oder Korrektur einer Version der SMSEagle-Software, einschließlich, aber nicht beschränkt auf einen Hotfix, Patch oder eine Verbesserung, wobei keines dieser Elemente als eigenständiger Dienst oder eigenständiges Softwarepaket fungiert und für bestehende Lizenznehmer keine zusätzlichen Kosten verursacht.
    5. „Upgrade“ bezeichnet eine größere, eigenständige Version der SMSEagle-Software, die zusätzliche Anwendungen, Funktionen oder Funktionalitäten enthalten kann.
    6. Ein Verweis auf „Person“ umfasst eine natürliche Person, eine körperschaftlich verfasste oder nicht verfasste Einrichtung (unabhängig davon, ob diese eine eigene Rechtspersönlichkeit besitzt) sowie deren gesetzliche und persönliche Vertreter, Rechtsnachfolger und zugelassene Rechtsübernehmer.
    7. Wörter in der Einzahl schließen die Mehrzahl ein und umgekehrt.
    8. Ein Verweis auf ein Gesetz, eine gesetzliche Bestimmung oder untergeordnete Rechtsvorschriften bezieht sich auf deren jeweils geltende Fassung unter Berücksichtigung etwaiger Änderungen oder Neuerlassungen und umfasst jedes Gesetz, jede gesetzliche Bestimmung oder untergeordnete Rechtsvorschrift, die dadurch geändert oder neu erlassen wird; wobei zwischen den Parteien keine solche Änderung oder Neuerlassung für die Zwecke dieses Vertrags gilt, soweit sie einer Partei eine neue oder erweiterte Pflicht, Haftung oder Beschränkung auferlegen oder deren Rechte anderweitig nachteilig beeinträchtigen würde.
    1. Ein Verweis auf Schriftform oder schriftlich umfasst auch E-Mail.
    2. Jede in diesem Vertrag enthaltene Verpflichtung einer Person, etwas nicht zu tun, umfasst auch die Verpflichtung, der Vornahme dieser Sache nicht zuzustimmen oder sie nicht zuzulassen.
    3. Jede durch die Begriffe „einschließlich“, „umfasst“, „insbesondere“ oder einen ähnlichen Ausdruck eingeleitete Formulierung ist als beispielhaft zu verstehen und schränkt die Bedeutung der vorangehenden Begriffe nicht ein.
    4. Verweise auf Artikel, Abschnitte oder Klauseln beziehen sich auf die Artikel, Abschnitte und Klauseln dieses Vertrags.

5. „Wir“, „Uns“ und „Unser“ bezeichnen Proximus Sp. z o.o. („PROXIMUS“).
6. Die „Parteien“ dieses Vertrags sind Sie und Proximus Sp. z o.o. („PROXIMUS“).
7. „Erfassen“ bezeichnet die Übertragung von Daten außerhalb des Geräts in einer Weise, die PROXIMUS oder Drittpartnern den Zugriff darauf ermöglicht.

2. **LIZENZGEWÄHRUNG**
    1. PROXIMUS gewährt Ihnen eine nicht-exklusive Lizenz zur Nutzung der SMSEagle-Software auf dem SMSEagle-Gerät, auf dem sie vorinstalliert war, sowie zur Installation von Updates und Upgrades vorbehaltlich der hierin festgelegten Bedingungen:

1. **Nutzung.** PROXIMUS gewährt Ihnen das Recht, eine einzelne Instanz der SMSEagle-Software auf dem von Ihnen erworbenen SMSEagle-Gerät zu nutzen. Die Nutzung auf einem anderen Gerät oder Computer ist untersagt.
2. **Sicherungskopie.** Sie dürfen eine einzelne Kopie der aktuellen Version der SMSEagle-Software für Ihr SMSEagle-Gerät zu Sicherungszwecken aufbewahren.
    1. Darüber hinaus gilt diese EULA auch für sämtliche von PROXIMUS bereitgestellten Software-Updates und Upgrades, die die ursprünglich installierte Version der SMSEagle-Software ersetzen, überschreiben und/oder ergänzen, sofern diese anderen Updates und Upgrades nicht durch eine separate Lizenz abgedeckt sind; in diesem Fall gelten die Bedingungen dieser Lizenz.

1. **GEISTIGES EIGENTUM**
    1. **GESCHÜTZTE SMSEAGLE-SOFTWARE**. Die SMSEagle-Software ist durch Urheberrecht und andere Gesetze und Abkommen zum Schutz geistigen Eigentums geschützt.
    2. **EINSCHRÄNKUNGEN DER NUTZUNG**. Als Lizenznehmer dürfen Sie nicht: (a) die SMSEagle-Software auf mehr als einem Gerät gleichzeitig nutzen, ohne vorher zusätzliche Geräte erworben zu haben; (b) die SMSEagle-Software in irgendeiner Weise an Dritte weitergeben oder anderweitig zugänglich machen; (c) einen Teil der SMSEagle-Software modifizieren, anpassen, davon abgeleitete Werke erstellen oder übersetzen, außer soweit dies im Rahmen der Nutzung innerhalb Ihres SMSEagle-Geräts gemäß dieser Lizenz zulässig ist; (d) die SMSEagle-Software zurückentwickeln (Reverse Engineering), dekompilieren oder disassemblieren, noch versuchen, deren Quellcode zu ermitteln oder zu erlangen (außer soweit solche Handlungen durch zwingende Bestimmungen des geltenden Rechts gestattet sind, einschließlich Artikel 6 der Richtlinie 2009/24/EG zur Dekompilierung zum Zweck der Herstellung der Interoperabilität mit anderen Programmen); (e) versuchen, Marken-, Urheberrechts- oder sonstige Eigentumsvermerke innerhalb der SMSEagle-Software zu ändern oder zu entfernen; oder (f) die SMSEagle-Software in einer Weise nutzen, die nicht in diesem EULA oder in der dem SMSEagle-Gerät beiliegenden Dokumentation, auf dem sie vorinstalliert war, vorgesehen ist.
    3. **UPDATES/UPGRADES**. PROXIMUS kann es für angebracht halten, Updates oder Upgrades für die SMSEagle-Software bereitzustellen. Sie können den Vorgang zur Installation eines Updates oder Upgrades starten, indem Sie beispielsweise in der Weboberfläche des SMSEagle-Geräts auf die Schaltfläche „Check for software

updates now“ klicken. Alternativ (wenn das Gerät keinen Internetzugang hat) können Sie ein Update- oder Upgrade-Paket vom SMSEagle-Support unter https://support.smseagle.eu beziehen, um es später auf dem SMSEagle-Gerät zu installieren. Es liegt im alleinigen Ermessen von PROXIMUS, die Bereitstellung solcher Updates oder Upgrades an Sie von Ihrer Zustimmung zu einem weiteren EULA oder dem Abschluss einer separaten Vereinbarung abhängig zu machen. Wenn Sie sich entscheiden, diese Updates oder Upgrades zu installieren und zu nutzen, erklären Sie sich damit einverstanden, allen geltenden Lizenzbedingungen dieses EULA und/oder einer anderen Vereinbarung zu unterliegen. PROXIMUS verpflichtet sich, Sicherheitsupdates für die SMSEagle-Software für einen Mindestzeitraum von fünf (5) Jahren ab dem Datum des ersten Verkaufs des jeweiligen SMSEagle-Gerätemodells bereitzustellen (der „Update-Zeitraum“). Nach Ablauf des Update-Zeitraums kann PROXIMUS nach eigenem Ermessen weiterhin Updates oder Upgrades bereitstellen, ist dazu jedoch nicht verpflichtet. PROXIMUS wird das End-of-Life-Datum jedes SMSEagle-Gerätemodells spätestens zwölf (12) Monate vor diesem Datum auf seiner Website bekannt geben. Diese Verpflichtung erfolgt unbeschadet eines längeren Support-Zeitraums, der durch zwingende Bestimmungen des geltenden Rechts vorgeschrieben sein kann, einschließlich des Cyber Resilience Act und der NIS2-Richtlinie.

2. **HAFTUNGSAUSSCHLUSS FÜR GEWÄHRLEISTUNG**

PROXIMUS wird angemessene Anstrengungen unternehmen, die den vorherrschenden Standards der Softwareentwicklung entsprechen, um die SMSEagle-Software so zu pflegen, dass Fehler und Unterbrechungen minimiert werden.

PROXIMUS GARANTIERT JEDOCH WEDER, DASS DIE NUTZUNG DER SMSEAGLE-SOFTWARE UNUNTERBROCHEN ODER FEHLERFREI SEIN WIRD, NOCH GIBT PROXIMUS EINE GARANTIE HINSICHTLICH DER ERGEBNISSE, DIE AUS DER NUTZUNG DER SMSEAGLE-SOFTWARE ERZIELT WERDEN KÖNNEN.

SOWEIT NACH GELTENDEM RECHT ZULÄSSIG, ÜBERNEHMEN, VORBEHALTLICH DER AUSDRÜCKLICHEN BESTIMMUNGEN HIERIN UND UNGEACHTET GEGENTEILIGER AUSSAGEN, WEDER PROXIMUS NOCH DEREN LEITENDE ANGESTELLTE, GESCHÄFTSFÜHRER, TOCHTERGESELLSCHAFTEN, VERBUNDENE UNTERNEHMEN, AUTORISIERTE WIEDERVERKÄUFER ODER MITARBEITER IRGENDEINE ANDERE GARANTIE JEGLICHER ART, OB AUSDRÜCKLICH, STILLSCHWEIGEND, GESETZLICH ODER ANDERWEITIG, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF GARANTIEN DER MARKTGÄNGIGKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND NICHTVERLETZUNG VON RECHTEN DRITTER.

1. **HAFTUNGSBESCHRÄNKUNG**
    1. Die Haftung von PROXIMUS im Zusammenhang mit Ansprüchen, die durch die Nutzung der SMSEagle-Software verursacht werden, damit im Zusammenhang stehen oder daraus entstehen, oder die Summe solcher Ansprüche, darf niemals die Kosten des SMSEagle-Geräts übersteigen, in Bezug auf das der Schaden entstanden ist, es sei denn, eine solche Haftungsbeschränkung ist nach geltendem polnischem Recht nicht zulässig.

2. PROXIMUS haftet dem Lizenznehmer gegenüber nicht für indirekte oder Folgeschäden, einschließlich entgangener Gewinne jeglicher Art sowie des Verlusts von Kunden, Umsätzen, Marge, Produktion, Image, Daten oder Konfiguration, sofern der vorstehende Ausschluss nicht für Schäden gilt, die von PROXIMUS vorsätzlich (absichtlich) verursacht wurden.
3. PROXIMUS haftet insbesondere nicht für: (i) den Verlust von Daten oder Konfigurationen; (ii) entgangene Gewinne des Lizenznehmers; (iii) indirekte oder Folgeschäden; (iv) Handlungen Dritter.
4. In Bezug auf die Haftung von PROXIMUS für etwaige Ansprüche des Endnutzers ist die Haftung von PROXIMUS nur auf Situationen beschränkt, in denen der Schaden das Ergebnis einer direkten Handlung oder Unterlassung von PROXIMUS ist, und ausschließlich auf die Kosten des SMSEagle-Geräts, in Bezug auf das der Schaden entstanden ist, es sei denn, eine solche Haftungsbeschränkung ist nach geltendem polnischem Recht nicht zulässig.
5. Die Bestimmungen dieses Abschnitts gelten nicht für Lizenznehmer, die Verbraucher oder Einzelunternehmer im Sinne des polnischen Rechts sind, soweit die hierin enthaltenen Beschränkungen durch zwingende Verbraucherschutzbestimmungen untersagt sind.

2. **OPEN SOURCE**

Bestimmte Softwaremodule in der PROXIMUS-Software unterliegen „Open-Source"- oder „Freie Software"-Lizenzen („Open-Source-Software"). Ein Teil der Open-Source-Software steht im Eigentum Dritter. Diese Open-Source-Software unterliegt nicht den Bedingungen dieser Vereinbarung. Stattdessen wird jede Open-Source-Software-Komponente gemäß den Bedingungen der beigefügten Endnutzerlizenz für diese Open-Source-Software lizenziert. Nichts in dieser Vereinbarung schränkt Ihre Rechte gemäß den geltenden Bedingungen der Endnutzerlizenz für die Open-Source-Software ein oder gewährt Ihnen Rechte, die diese außer Kraft setzen. Zu den geltenden Open-Source-Lizenzen gehören: 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. Falls dies für eine bestimmte Open-Source-Software erforderlich ist, stellt PROXIMUS diese Open-Source-Software sowie Unsere Änderungen an dieser Open-Source-Software auf schriftliche Anfrage an Uns per E-Mail oder Postanschrift zur Verfügung.

1. **ENDNUTZER DER US-REGIERUNG**

Die SMSEagle-Software wird der US-Regierung mit EINGESCHRÄNKTEN RECHTEN (RESTRICTED RIGHTS) lizenziert. Die Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Beschränkungen gemäß DFARS 252.227-7013 der Klausel über technische Daten und Computersoftware sowie 48 CFR 52.227-19 der Klausel über kommerzielle Computersoftware, je nach Anwendbarkeit.

1. **DATENSCHUTZ**

1. **ERKLÄRUNG ZUR DATENERHEBUNG**. PROXIMUS erhebt KEINERLEI Daten, mit denen Sie bei der Nutzung des SMSEagle-Geräts arbeiten. Wir können keine auf dem SMSEagle-Gerät gespeicherten Daten einsehen oder erheben, da wir keinerlei Zugriff

auf Ihr Gerät haben. Im Rahmen der Bereitstellung der SMSEagle-Software und des zugehörigen Supports kann PROXIMUS jedoch bestimmte personenbezogene Daten des Lizenznehmers (oder, sofern der Lizenznehmer eine juristische Person ist, seiner bevollmächtigten Vertreter und Endnutzer) verarbeiten. Die folgenden Informationen werden gemäß Artikel 13 der Verordnung (EU) 2016/679 (DSGVO) bereitgestellt:

2. Verantwortlicher: Proximus Sp. z o.o., ul. Piątkowska 163, 60-650 Poznań, Polen; E-Mail: odo@smseagle.eu.
3. Kategorien der verarbeiteten personenbezogenen Daten: (a) Registrierungs- und Lizenzierungsdaten (Firmenname, Ansprechpartner, E-Mail, Seriennummer des Geräts); (b) Update-/Upgrade-Telemetriedaten, die streng auf Softwareversion, Gerätemodell, Seriennummer des Geräts und ggf. IP-Adresse beschränkt sind. Personenbezogene Daten, die im Zusammenhang mit der Bereitstellung des technischen Supports verarbeitet werden, unterliegen einer separaten Richtlinie zu technischen Support-Dienstleistungen, die auf der Proximus-Website www.smseagle.eu verfügbar ist.
4. Zwecke und Rechtsgrundlagen der Verarbeitung: (a) Erfüllung dieses EULA und Bereitstellung von Updates und Upgrades – Artikel 6 Abs. 1 lit. b DSGVO; (b) Erfüllung rechtlicher Verpflichtungen (Steuer, Buchhaltung) – Artikel 6 Abs. 1 lit. c DSGVO; (c) berechtigte Interessen von PROXIMUS an der Verbesserung der SMSEagle-Software und der Verteidigung gegen Ansprüche – Artikel 6 Abs. 1 lit. f DSGVO.
5. Empfänger personenbezogener Daten: autorisierte, zur Vertraulichkeit verpflichtete Mitarbeiter und Auftragnehmer von PROXIMUS, IT-Dienstleister (Hosting, E-Mail, Ticketing), die als Auftragsverarbeiter gemäß Artikel 28 DSGVO tätig sind, sowie zuständige Behörden, soweit gesetzlich vorgeschrieben.
6. Übermittlungen in Drittländer: Personenbezogene Daten werden hauptsächlich innerhalb des Europäischen Wirtschaftsraums verarbeitet. Sofern Übermittlungen in Drittländer erfolgen (z. B. bei der Nutzung bestimmter IT-Anbieter), erfolgen diese auf Grundlage eines Angemessenheitsbeschlusses oder geeigneter Garantien wie der EU-Standardvertragsklauseln.
7. Aufbewahrungsdauer: Registrierungs- und Lizenzierungsdaten – für die Laufzeit dieses EULA und für den nach geltendem Recht erforderlichen Zeitraum (insbesondere Steuer- und Buchhaltungsrecht, in der Regel 5 Jahre); Daten, die auf Grundlage berechtigter Interessen verarbeitet werden – bis ein wirksamer Widerspruch erhoben wird oder das berechtigte Interesse entfällt.
8. Rechte der betroffenen Personen: Der Lizenznehmer hat das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragbarkeit hinsichtlich seiner personenbezogenen Daten sowie das Recht, der auf berechtigten Interessen beruhenden Verarbeitung zu widersprechen.
9. Recht auf Beschwerde: Der Lizenznehmer hat das Recht, eine Beschwerde beim Präsidenten des Amtes für den Schutz personenbezogener Daten (Prezes Urzędu Ochrony Danych Osobowych), ul. Stawki 2, 00-193 Warschau, Polen, einzureichen.

10. Automatisierte Entscheidungsfindung: PROXIMUS führt im Zusammenhang mit diesem EULA keine automatisierte Entscheidungsfindung, einschließlich Profiling, im Sinne von Artikel 22 DSGVO durch.
11. Die Bereitstellung personenbezogener Daten erfolgt freiwillig, ist jedoch für den Abschluss und die Erfüllung dieses EULA sowie für die Bereitstellung von Support-Dienstleistungen erforderlich. Weitere Einzelheiten, einschließlich etwaiger Aktualisierungen dieser Informationen, finden Sie in der Datenschutzrichtlinie unter https://www.smseagle.eu/privacy-policy/.

2. **KÜNDIGUNG**

1. PROXIMUS behält sich das Recht vor, dieses EULA mit sofortiger Wirkung zu kündigen im Falle von: (i) einem wesentlichen Verstoß des Lizenznehmers gegen die im Abschnitt „Restrictions on Use“ festgelegten Lizenzbeschränkungen; (ii) unbefugter Vervielfältigung, Verbreitung oder Modifikation der SMSEagle-Software; oder (iii) Umgehung oder Manipulation technischer Schutzmaßnahmen.
2. PROXIMUS und ein Lizenznehmer, der das SMSEagle-Gerät direkt von PROXIMUS erworben hat, können diese EULA mit einer schriftlichen Frist von mindestens dreißig (30) Tagen kündigen.
3. Vorbehaltlich zwingender Verbraucherschutzgesetze hat der Lizenznehmer keinen Anspruch auf Rückerstattung des Kaufpreises des SMSEagle-Geräts oder von Gebühren, die im Zusammenhang mit der SMSEagle-Software gezahlt wurden, wenn PROXIMUS diese EULA aus den in Abschnitt 9.01. oben genannten Gründen kündigt.
4. Nach Beendigung dieser EULA muss der Lizenznehmer jegliche Nutzung der SMSEagle-Software einstellen und alle vorhandenen Sicherungskopien unbrauchbar machen. Die Abschnitte „Geistiges Eigentum“, „Gewährleistungsausschluss“, „Haftungsbeschränkung und Rechtsmittel“, „Datenschutz“, „Anwendbares Recht“ und „Streitbeilegung“ bleiben auch nach Beendigung wirksam.
5. Hat der Lizenznehmer das SMSEagle-Gerät von einem Wiederverkäufer oder autorisierten Partner erworben, so richten sich die Regelungen zu Rückgaben, Stornierungen und Rückerstattungen des SMSEagle-Geräts nach der Rechnung oder anderen Verkaufsunterlagen, die von diesem Wiederverkäufer oder autorisierten Partner bereitgestellt werden.
6. Diese EULA gilt unabhängig von einer für das SMSEagle-Gerät geltenden Hardware-Garantie. Das Erlöschen oder die Beendigung dieser EULA berührt weder die Gültigkeit und Dauer der dem SMSEagle-Gerät zugeordneten Hardware-Garantie, noch schränken die Bedingungen der Hardware-Garantie die Rechte des Lizenznehmers aus dieser EULA ein.

3. **SONSTIGES**

1. **RECHTSNACHFOLGER UND ZESSIONARE**. Diese EULA ist in ihrer Gesamtheit für PROXIMUS und Sie sowie unsere jeweiligen Rechtsnachfolger und zulässigen Zessionare rechtlich bindend und kommt ihnen zugute.

2. **SALVATORISCHE KLAUSEL**. Sollte eine Bestimmung dieser Vereinbarung von einem zuständigen Gericht für ungültig, unwirksam oder nicht durchsetzbar erklärt werden, bleiben die übrigen Bestimmungen davon unberührt.
3. **VERZICHT**. Der Verzicht auf die Geltendmachung einer Verletzung oder Nichteinhaltung einer der hierin enthaltenen Bestimmungen gilt nicht als zukünftiger Verzicht auf diese Bedingungen oder als Verzicht auf eine andere Bestimmung dieser EULA.
4. **ÄNDERUNGEN**. Jeder Verzicht, jede Ergänzung, Änderung oder Anpassung einer Bestimmung dieser EULA ist nur wirksam, wenn sie schriftlich erfolgt und von PROXIMUS unterzeichnet wird.
5. **ANWENDBARES RECHT**. In Angelegenheiten, die hierin nicht geregelt sind, gelten die Bestimmungen des polnischen Zivilgesetzbuchs sowie die Bestimmungen des polnischen Urheberrechtsgesetzes vom 4. Februar 1994 (Journal of Laws 1994, Nr. 24, Punkt 83). Diese Vereinbarung unterliegt in allen Belangen den Gesetzen der Republik Polen.
6. **STREITBEILEGUNG**. Streitigkeiten, die sich aus dieser Vereinbarung ergeben oder im Zusammenhang mit ihr stehen, unterliegen der ausschließlichen Zuständigkeit der ordentlichen Gerichte, die für den Sitz von PROXIMUS in Poznań, Polen, zuständig sind. Diese Bestimmung gilt nicht für Lizenznehmer, die Verbraucher oder Einzelunternehmer im Sinne des polnischen Rechts sind; diese behalten das Recht, Verfahren vor dem gemäß den geltenden zwingenden Rechtsvorschriften zuständigen Gericht einzuleiten.
7. **ÜBERTRAGUNGEN**. Sie sind berechtigt, die SMSEagle-Software an Dritte weiterzugeben, jedoch nur zusammen mit der dauerhaften Eigentumsübertragung des SMSEagle-Geräts, auf dem sie vorinstalliert war. In diesem Fall ist der Erwerber verpflichtet, diese EULA in ihrer aktuellen Fassung vor Nutzung der SMSEagle-Software anzunehmen, und Sie müssen alle bei Ihnen vorhandenen Sicherungskopien oder sonstigen Kopien der SMSEagle-Software zum Zeitpunkt der Übertragung unbrauchbar machen. Diese Bestimmung berührt nicht den Grundsatz der Erschöpfung der Rechte gemäß Artikel 4(2) der Richtlinie 2009/24/EG sowie etwaige zwingende Rechte des Lizenznehmers nach EU-Recht.
8. **GÜLTIGKEIT UND VERBINDLICHKEIT**. Diese Vereinbarung stellt eine gültige und rechtsverbindliche Verpflichtung der Parteien dar, die gegenüber den Parteien gemäß ihren Bedingungen durchsetzbar ist, vorbehaltlich der Auswirkungen von Insolvenz, Zahlungsunfähigkeit, betrügerischer Vermögensübertragung, Reorganisation, Moratorien und anderer Gesetze, die die Rechte von Gläubigern im Allgemeinen betreffen oder beeinflussen, sowie allgemeiner Grundsätze des Billigkeitsrechts.
9. **BEDEUTUNG VON TITEL UND ÜBERSCHRIFTEN**. Der Titel der Vereinbarung sowie die Überschriften von Abschnitten und Klauseln dienen lediglich der Übersichtlichkeit und haben keinen Einfluss auf die Bedeutung der Vereinbarung oder des jeweiligen Abschnitts.
10. **HÖHERE GEWALT**. Mit Ausnahme von Zahlungsverpflichtungen gilt: Ist eine Partei aufgrund von Umständen, die außerhalb ihrer angemessenen Kontrolle liegen, an der

Erfüllung einer ihrer Verpflichtungen aus dieser Vereinbarung gehindert oder dazu nicht in der Lage – einschließlich, aber nicht beschränkt auf höhere Gewalt, Maßnahmen zivilstaatlicher oder militärischer Behörden, Unruhen oder ziviler Ungehorsam, Kriege, Streiks oder Arbeitskämpfe (jeweils ein „**Ereignis höherer Gewalt**“) –, so wird die Erfüllung dieser Partei entschuldigt und die Erfüllungsfrist entsprechend verlängert, vorausgesetzt, die Partei unternimmt umgehend alle angemessenen und notwendigen Schritte, um die vollständige Erfüllung wiederherzustellen.

4. **VERBRAUCHERSCHUTZ UND SCHUTZ VON EINZELUNTERNEHMERN**

Die Bestimmungen dieser EULA beeinträchtigen nicht die Bestimmungen zum Verbraucherschutz und zum Schutz von Einzelunternehmern, wenn Sie eine natürliche Person sind, die das Gerät kauft und diese EULA nicht direkt mit ihrer beruflichen oder Geschäftstätigkeit verbunden abschließt, oder im Fall eines Unternehmers, der eine natürliche Person ist – nicht direkt mit seiner beruflichen Tätigkeit verbunden (anwendbar auf die ab 1. Januar 2021 abgeschlossene EULA). Sollte eine Bestimmung dieser EULA mit zwingenden Verbraucherschutz- oder Schutzgesetzen für Einzelunternehmer unvereinbar sein, bindet diese Bestimmung den Verbraucher/Einzelunternehmer nicht, und es gilt die Bestimmung des allgemein geltenden Gesetzes, die dieser Bestimmung am nächsten kommt.

1. **KONTAKTINFORMATIONEN**

Wenn Sie Fragen zu dieser EULA haben, wenden Sie sich bitte an PROXIMUS unter:

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

Was im Lieferumfang enthalten ist



SMSEagle ausgepackt

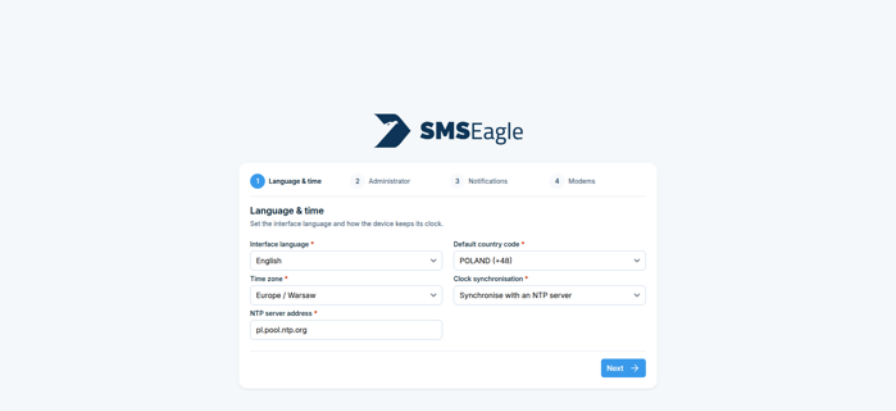
Ihr SMSEagle-Karton enthält:

- SMSEagle Hardware-SMS-Gateway
- Externe omnidirektionale Antenne (mit Magnetfuß) NXS-9700-3G NXS-9700-4G

- 2x externe MIMO-Antennen (mit magnetischem/Klebefuß) NXS-9700-5G
- AC/DC-Stromversorgung (Eingangsspannung: 100–240 V)
- Schnellstartanleitung
- Garantiekarte

Konfigurationsassistent

Wenn Sie sich zum ersten Mal in einem neu eingerichteten SMSEagle-Gerät anmelden, führt Sie ein Konfigurationsassistent durch die erforderlichen Einstellungen, bevor das Gateway in Betrieb geht. Der Assistent hat vier Schritte; Sie können auf den Rest der Weboberfläche nicht zugreifen, bis dieser abgeschlossen ist.

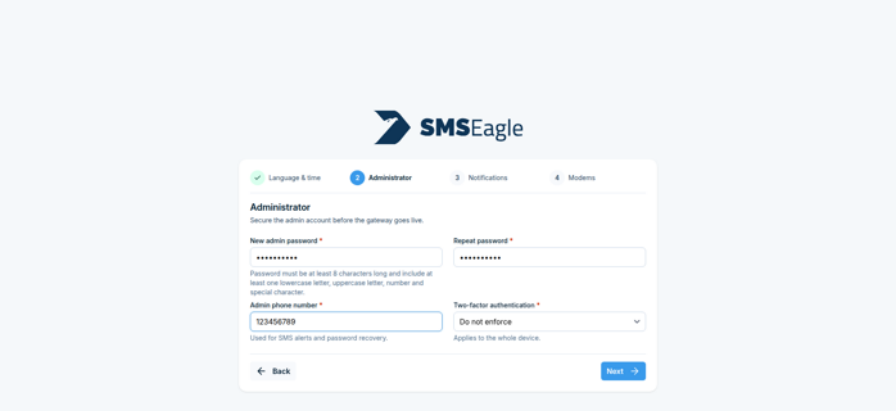


Schritt 1: Sprache & Zeit

Schritt 1: Sprache & Zeit

Legen Sie die Schnittstellensprache, den Standard-Ländercode (wird verwendet, wenn eine Telefonnummer ohne einen eingegeben wird), die Gerätezeitzone und die Zeitsynchronisierung fest. Wenn Sie **Mit einem NTP-Server synchronisieren** wählen, geben Sie auch die **NTP-Serveradresse** ein.

Schritt 2: Administrator-Konto



Schritt 2: Administrator-Konto

Sichern Sie das Admin-Konto, bevor das Gateway in Betrieb geht:

Feld	Beschreibung
Neues Admin-Passwort / Passwort wiederholen	Muss mindestens 8 Zeichen lang sein und einen Kleinbuchstaben, einen Großbuchstaben, eine Zahl und ein Sonderzeichen enthalten
Admin-Telefonnummer	Wird für SMS-Warnungen und Passwortwiederherstellung verwendet
Authentifizierung mit zwei Faktoren	Nicht erzwingen, Für alle Benutzer erzwingen oder Für neue Benutzer erzwingen – gilt für das gesamte Gerät, siehe Multi-Faktor-Authentifizierung (MFA)

Das Ändern des Admin-Passworts hier meldet Sie ab; melden Sie sich mit dem neuen Passwort an, um den Assistenten fortzusetzen.

Schritt 3: Benachrichtigungen

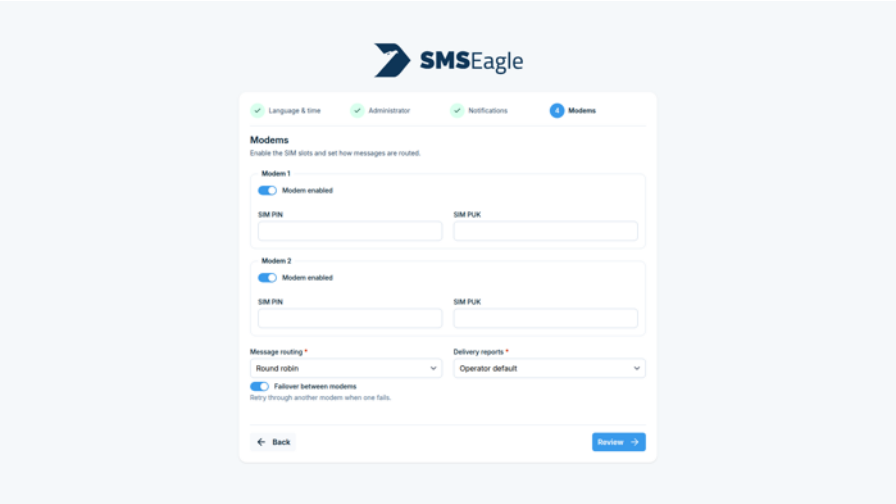


Schritt 3: Benachrichtigungen

Wählen Sie, über was das Gerät Sie benachrichtigen soll:

- Automatisch auf Softwareaktualisierungen prüfen und optional den Admin per SMS benachrichtigen, wenn eine neue Version verfügbar ist
- Automatisch auf Gültigkeit des Supports prüfen und optional den Admin per SMS benachrichtigen, wenn der Support bald abläuft

Schritt 4: Modems



Schritt 4: Modems

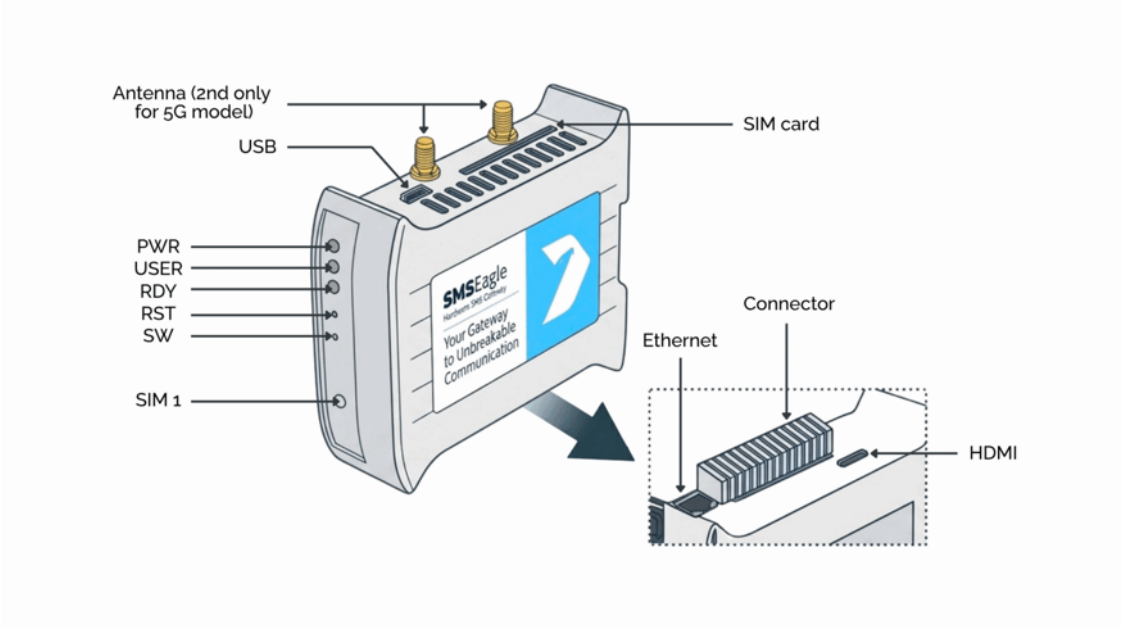
Aktivieren Sie das integrierte Modem für das integrierte Modem und geben Sie gegebenenfalls seine **SIM-PIN** und **SIM-PUK** ein. Legen Sie dann fest:

- **Zustellungsberichte** - Standardeinstellung des Betreibers, Immer anfordern oder Nie anfordern

NXS-9700 wird mit einem einzigen integrierten Modem ausgeliefert, daher gelten die Einstellungen für Modem-zu-Modem-Nachrichtenrouting und Failover (verfügbar bei Multi-Modem-SMSEagle-Produkten) hier nicht.

Überprüfen Sie Ihre Einstellungen und beenden Sie den Assistenten, um zum normalen Dashboard zu gelangen.

Anschlüsse, Anschlussöffnungen und LEDs



Anschlüsse, Ports und LEDs

Element	Bezeichnung	Beschreibung
VCC Rev.3 Rev.4	VCC	Stromanschluss
12-poliger Anschluss	–	4x digitaler Eingang, 4x digitaler Ausgang, 1× 1Wire, 1× 5V, 2x GND
SIM-Kartensteckplatz	SIM	SIM-Kartensteckplatz
HDMI-Port	HDMI	HDMI-Port (nur zu Debugging-Zwecken)
USB-Port	USB	USB-Port (nur zu Debugging-Zwecken)
Ethernet-Port	ETH	Ethernet RJ45-Port
Antenne	ANT	Antennensteckplatz Zweiter Steckplatz für MIMO NXS-9700-5G
Power-LED	PWR	LED zur Anzeige des Einschaltzustands
User LED	USER	LED für Benutzeranwendungszwecke
SIM1,2 LEDs	Modem 1,2 (optional)	LED-Anzeige für Modemstatus
Ready LED	RDY	LED-Anzeige für Gerätestatus
Reset	RST	Schalter zum Neustarten des Geräts
User Switch	SW	Schalter zum Wiederherstellen der Werkseinstellungen

Übersicht der Weboberfläche

Dieses Kapitel bietet eine kurze Einführung in die SMSEagle-Weboberfläche selbst, bevor die einzelnen Funktionen im Rest dieses Handbuchs behandelt werden.

Anmeldung

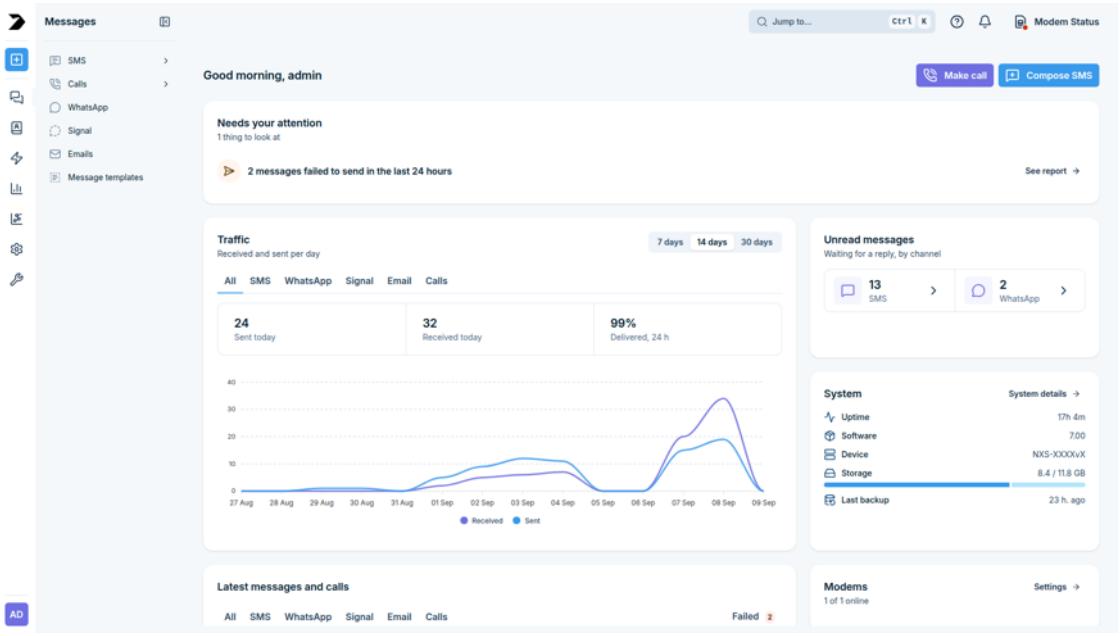


Die Anmeldeseite

Öffnen Sie die IP-Adresse oder den Hostnamen des Geräts in einem Browser und melden Sie sich mit Ihrem Login und Passwort an. Falls Multi-Factor Authentication auf Geräteebene erzwungen worden ist (siehe MFA), werden Sie auch nach einem Einmalcode gefragt.

- **Authentication type** bestimmt, wo die Anmeldedaten überprüft werden: **Local (Standard)** gegen die Benutzerliste des Geräts, oder **LDAP** gegen einen Verzeichnisserver, den zuvor ein Administrator unter LDAP konfiguriert.
- **Forgot password?** sendet Wiederherstellungsanweisungen per SMS an die Telefonnummer des Kontos. Identifizieren Sie sich dort mit Ihrem Benutzernamen oder dieser Telefonnummer.
- Der Selektor in der unteren rechten Ecke stellt die Sprache der Anmeldeseite ein. Die Sprache der Oberfläche nach der Anmeldung stammt aus Ihrem eigenen Konto, siehe Persönliche Kontoeinstellungen.

Oberflächenlayout

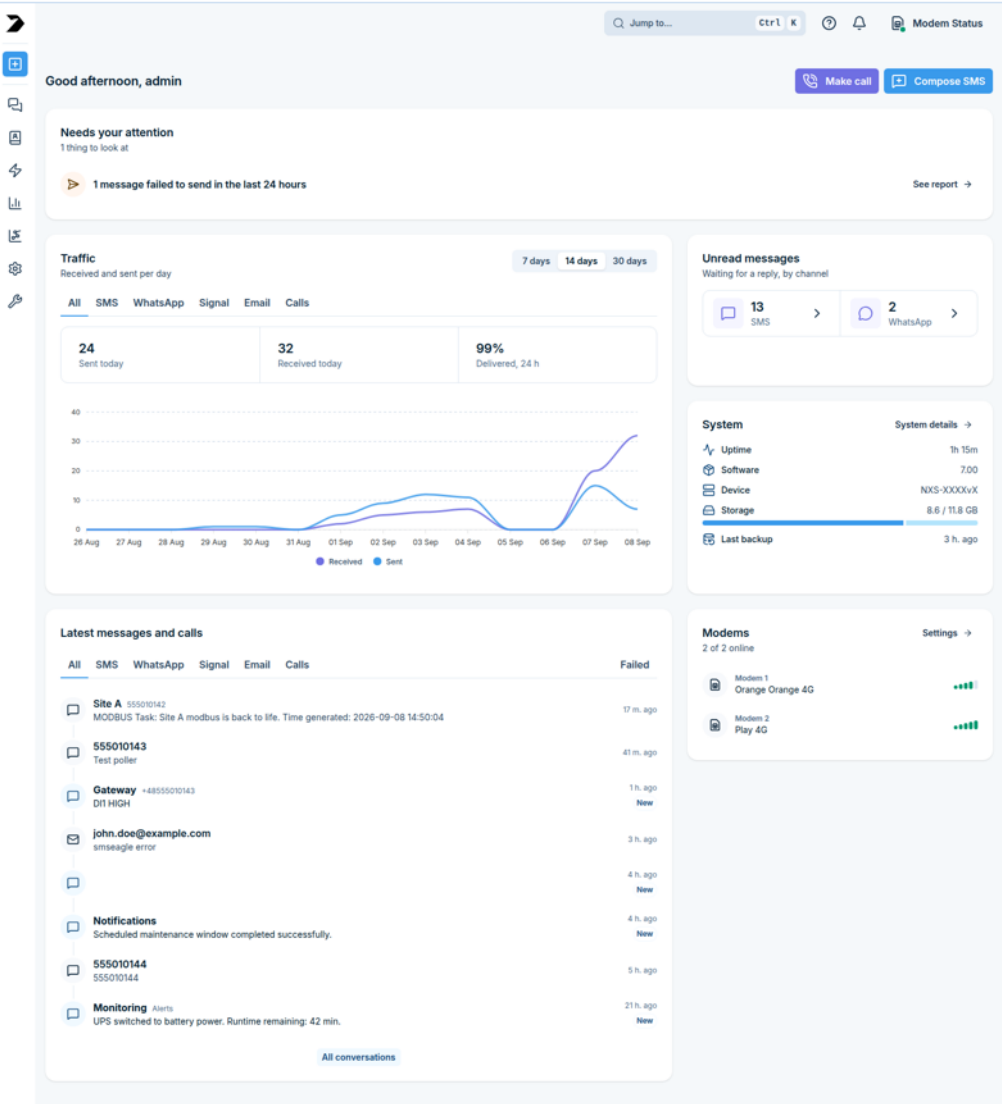


Linke Navigation über dem Hauptinhaltsbereich erweitert, mit der oberen Leiste darüber

- **Left navigation** - eine Symbolliste für den Zugriff auf Messages, Phonebook, Automation, Reports, Monitoring, Settings und System. Durch Hovern über einem Symbol wird der Bereich benannt; durch Klicken wird ein Panel erweitert, das die Seiten dieses Bereichs nach Namen auflistet, wie **Messages** oben. Die Schaltfläche in der eigenen Kopfzeile des Panels schließt es wieder.
- **Top bar** - die **Jump to...**-Suche (`Ctrl K`) ermöglicht es Ihnen, direkt zu einer beliebigen Seite nach Name zu springen, anstatt das Menü zu durchlaufen; sie zeigt auch Benachrichtigungen, Hilfe und den Modem-Statusindikator.
- **Main content area** - die Seite für den derzeit ausgewählten Bereich.

Dashboard

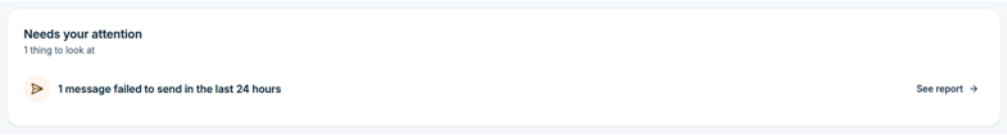
Das Dashboard ist die Landing Page nach der Anmeldung. Es öffnet sich mit einer Begrüßung und den Quick-Action-Schaltflächen, gefolgt von Karten, die zusammenfassen, was Aufmerksamkeit erfordert, Nachrichtenverkehr, unbeantwortete Konversationen, Gerätezustand, kürzliche Aktivität und Modem-Status.



Das Dashboard

Needs your attention

Sammelt Einträge, die sofort bearbeitet werden sollten, mit der Anzahl darunter im Kartentitel und wie viele davon kritisch sind. Jeder Eintrag verlinkt auf die Seite, auf der Sie ihn bearbeiten können, sodass eine in der Outbox steckengebliebene Nachricht zur Outbox-Ordner führt, und ein fehlgeschlagener Liefereintrag führt zu Reports & Statistics.



Needs your attention

Traffic

Empfangene und gesendete Nachrichten pro Tag. Die Registerkarten begrenzen die Karte auf einen einzelnen Kanal (SMS, WhatsApp, Signal, Email oder Calls), und die Schaltflächen **7 days** / **14**

days / **30 days** setzen den Bereich des Diagramms darunter. Drei Zähler befinden sich über dem Diagramm:

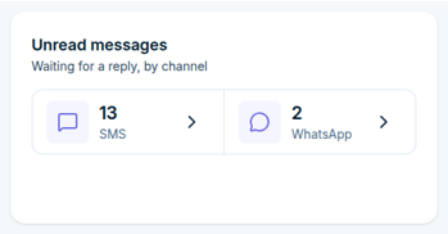
- **Sent today** - Nachrichten, die seit Mitternacht gesendet wurden
- **Received today** - Nachrichten, die seit Mitternacht empfangen wurden
- **Delivered, 24 h** - Anteil der Nachrichten, die in den letzten 24 Stunden gesendet wurden und als zugestellt bestätigt wurden



Traffic

Unread messages

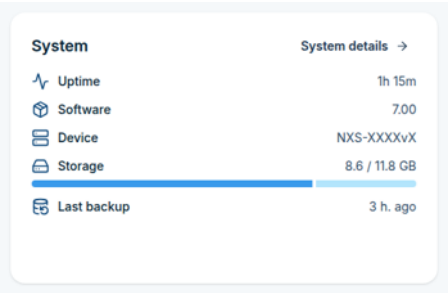
Konversationen, die noch auf eine Antwort warten, gezählt pro Kanal. Jede Kachel öffnet die Konversationsliste dieses Kanals, siehe Messages.



Unread messages

System

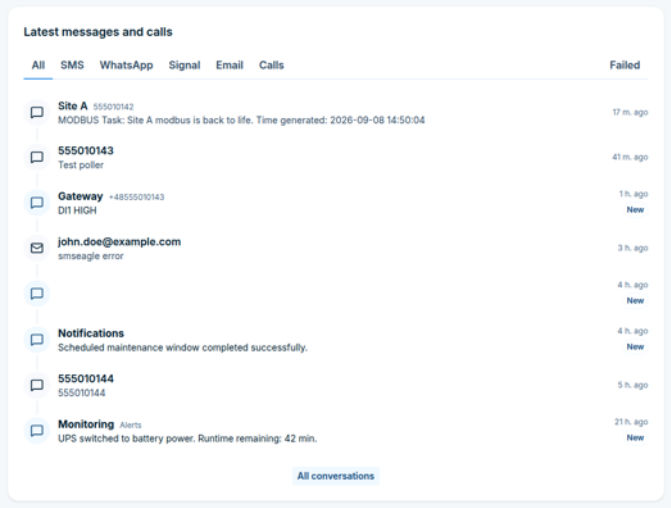
Systemzustand auf einen Blick: Betriebszeit, Softwareversion, Gerätetyp, genutzter Speicher von insgesamt verfügbarem Speicher und Zeitpunkt der letzten Sicherung. **Systemdetails** öffnet den Abschnitt System.



System

Neueste Nachrichten und Anrufe

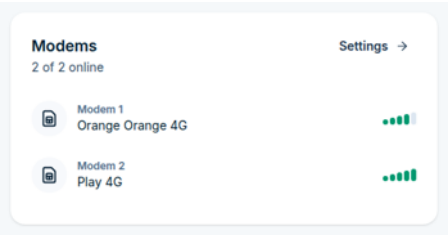
Der aktuellste Datenverkehr über alle Kanäle, neueste zuerst, mit Absender, Anfang der Nachricht und Zeitpunkt des Empfangs. Die Registerkarten begrenzen die Liste auf einen Kanal, und **Fehlgeschlagen** listet auf, was nicht gesendet wurde. Noch ungelesene Einträge sind mit **Neu** gekennzeichnet. **Alle Unterhaltungen** öffnet die vollständige Liste unter Nachrichten.



Neueste Nachrichten und Anrufe

Modems

Wie viele Modems online sind von den installierten Modems, und für jedes die Netzwerk, auf dem es registriert ist, die Funktechnologie und die Signalstärke. **Settings** öffnet die Modemkonfiguration, siehe Einstellungen.



Modems

Schnellaktionen

Zwei Schaltflächen in der oberen rechten Ecke des Dashboards.



Schnellaktionen

Beide öffnen denselben Dialog **Verfassen**, auf einer anderen Registerkarte:

- **SMS verfassen** öffnet es auf der Registerkarte **Nachricht** - wählen Sie den Nachrichtentyp (SMS, Flash-SMS, MMS, USSD-Code, Signal, WhatsApp, E-Mail), die Empfänger (aus dem

Telefonbuch, manuell eingegeben oder aus einer CSV-Datei), den Sendezeitpunkt und die Nachricht selbst. Eine gespeicherte Vorlage kann anstelle von Text verwendet werden, siehe Nachrichten.

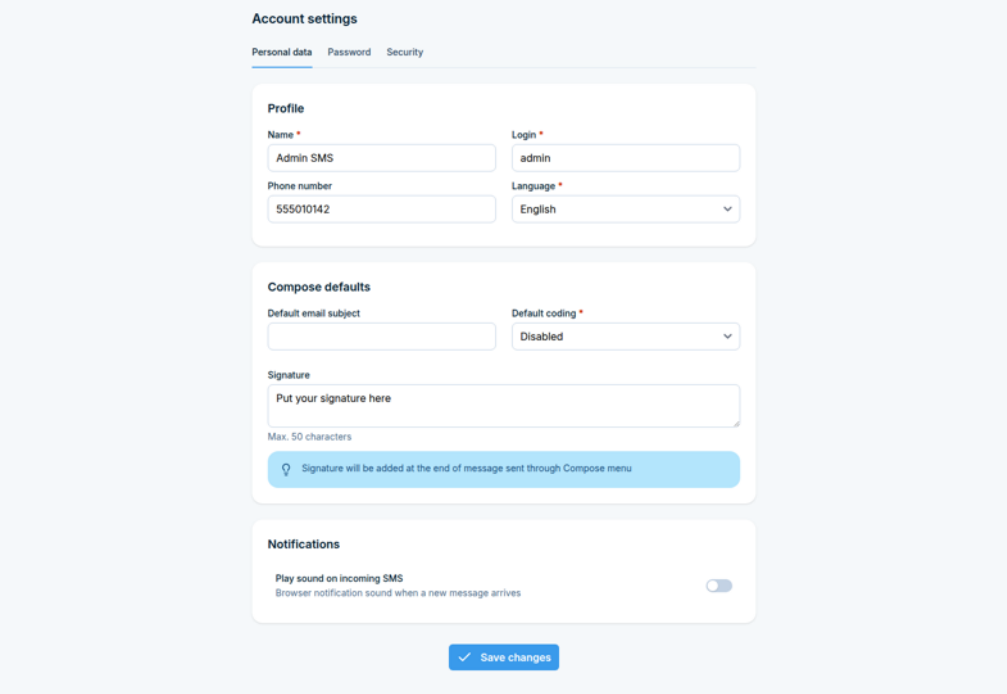
- **Anruf tätigen** öffnet es auf der Registerkarte **Anruf** - wählen Sie den Anruftyp (nur Klingeln, Text-to-Speech, eine Audiodatei), die Empfänger und den Zeitpunkt des Anrufs, siehe Nachrichten.

Ein Kanal, der auf diesem Gerät nicht konfiguriert ist, wird in der Nachrichtentypenliste ausgegraut.

Persönliche Kontoeinstellungen

Klicken Sie auf Ihren Avatar (unten links) und wählen Sie **Kontoeinstellungen**, um Ihr eigenes Konto auf drei Registerkarten zu verwalten.

Persönliche Daten

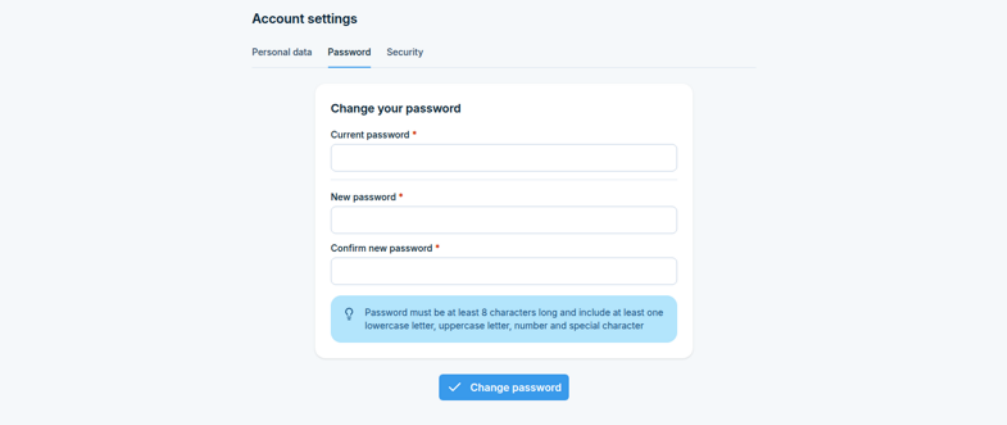


Kontoeinstellungen > Persönliche Daten

- **Profil** - Name, Anmeldename, Telefonnummer und Oberflächensprache für Ihr eigenes Konto
- **Standardeinstellungen für Verfassen** - Standard-E-Mail-Betreff, Standard-SMS-Codierung und eine Signatur mit bis zu 50 Zeichen, die an von Verfassen gesendete Nachrichten angehängt wird
- **Benachrichtigungen** - ob der Browser einen Ton abspielt, wenn eine neue Nachricht ankommt

Änderungen speichern wendet die ganze Registerkarte auf einmal an.

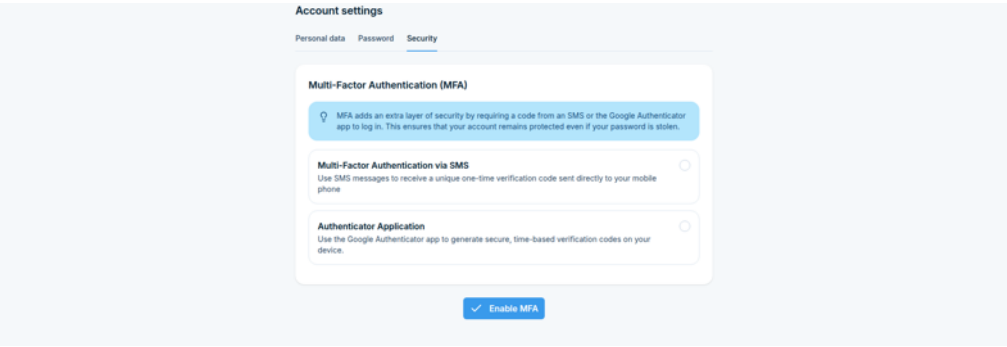
Passwort



Kontoeinstellungen > Passwort

Ändern Sie Ihr eigenes Passwort, indem Sie das aktuelle und das neue Passwort zweimal eingeben. Das neue Passwort muss mindestens 8 Zeichen lang sein und einen Kleinbuchstaben, einen Großbuchstaben, eine Zahl und ein Sonderzeichen enthalten.

Sicherheit



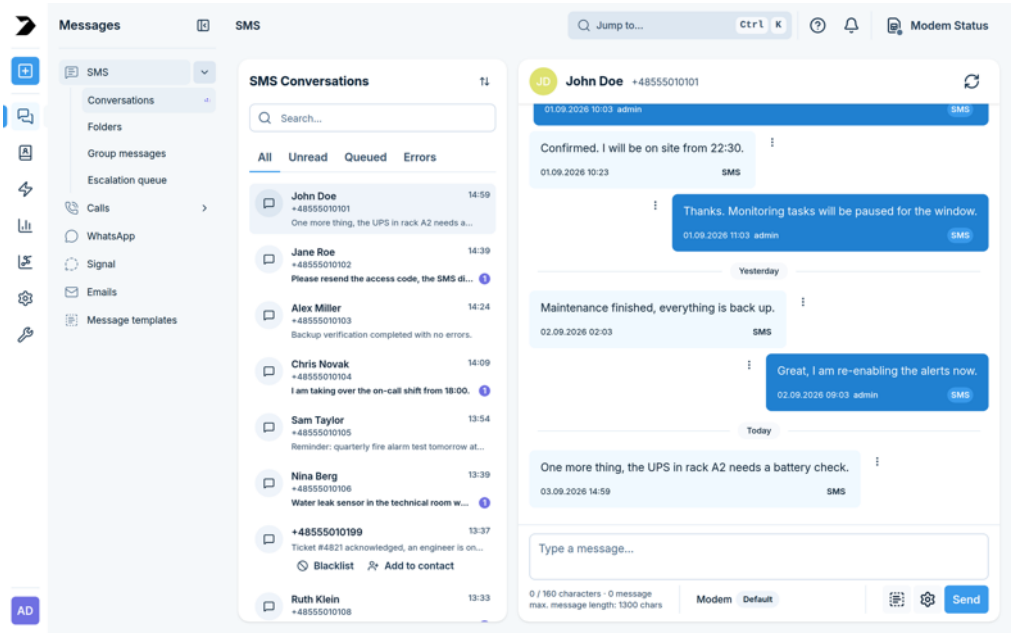
Account settings > Security

Konfigurieren Sie Ihre eigene Multi-Faktor-Authentifizierung, entweder per SMS oder mit einer Authenticator-Anwendung. Die vollständige Anleitung, einschließlich der Erzwingung von MFA auf Geräteebene, finden Sie unter MFA.

Nachrichten

Dieses Kapitel behandelt den Bereich **Nachrichten** der Weboberfläche – hier lesen, verfassen und verwalten Sie Konversationen aller Kanäle. Die Konfiguration eines Kanals (WhatsApp aktivieren, SMTP verbinden, Modems einrichten) wird separat unter Einstellungen behandelt; dieses Kapitel befasst sich mit der täglichen Nutzung eines Kanals.

SMS (Konversationen)

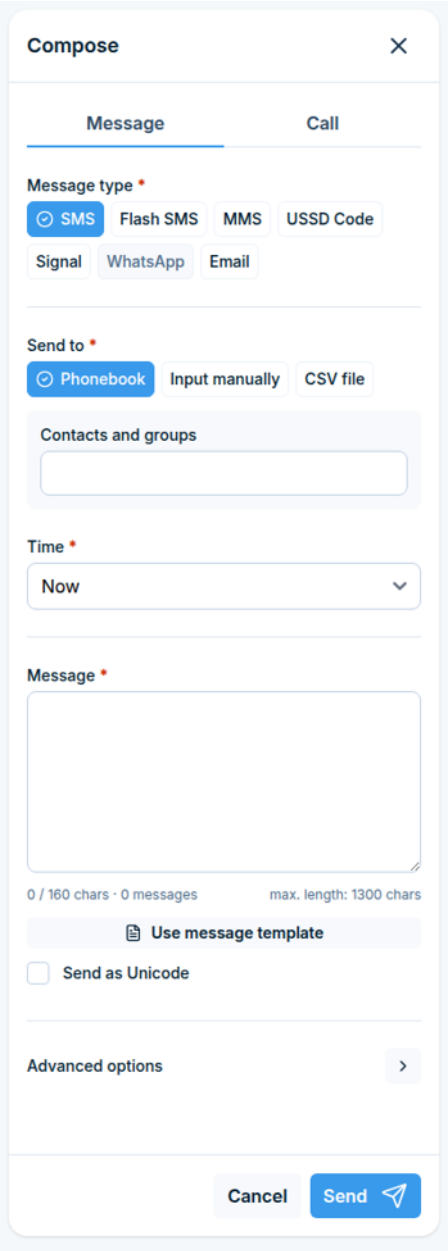


SMS-Konversationen mit geöffnetem Thread

Nachrichten > SMS > Konversationen (`/messages/sms/`) ist der Haupt-SMS/MMS-Eingang: ein Thread pro Telefonnummer, neueste zuerst.

- Filtern Sie mit den Registerkarten **Alle**, **Ungelesen**, **In Warteschlange** und **Fehler**.
- Öffnen Sie einen Thread, um den vollständigen Verlauf zu lesen und vom Feld unten zu antworten.
- MMS-Anhänge (Bilder, Dateien) erscheinen inline im Thread, sobald ein Modem MMS konfiguriert hat – siehe MMS in Einstellungen.
- Verfassen Sie eine neue Nachricht mit der Schaltfläche **+** oben in der linken Leiste oder der Schnellaktion **Verfassen** im Dashboard.

Verfassen einer Nachricht



Der Dialog zum Verfassen

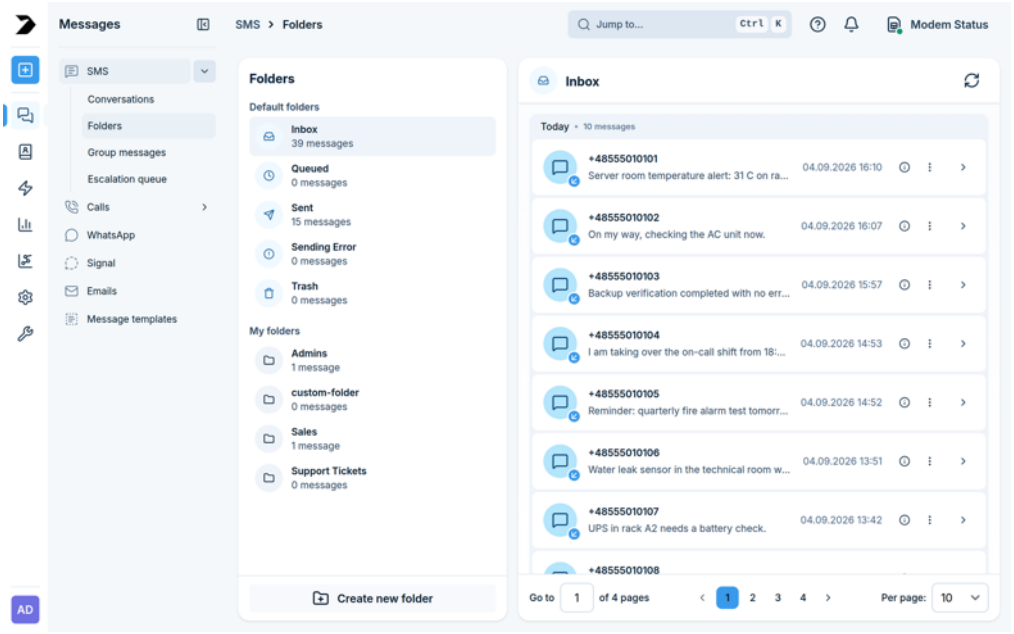
Das Verfassen-Fenster wird als Bereich auf der rechten Seite geöffnet, mit einer Registerkarte **Nachricht** und einer **Anruf**-Registerkarte. Die Registerkarte Nachricht enthält:

- **Nachrichtentyp** – SMS, Flash SMS, MMS, USSD-Code, Signal, WhatsApp oder E-Mail. Ein Kanal, der auf diesem Gerät nicht konfiguriert ist, wird abgeblendet; siehe Einstellungen.
- **Senden an** – wählen Sie Empfänger aus dem **Adressbuch** (Kontakte und Gruppen) aus, geben Sie diese mit **Manuell eingeben** ein, oder laden Sie eine **CSV-Datei** hoch.
- **Zeit** – senden Sie **Jetzt**, **Zu Datum und Uhrzeit**, **Nach Verzögerung** oder **Zwischen Stunden**.
- **Nachricht** – der Text mit einem Live-Zähler für Zeichen und wie viele SMS-Teile sie ausmachen. **Nachrichtenvorlage verwenden** füllt ihn aus einer gespeicherten Vorlage, und **Als Unicode senden** schaltet die Codierung für Nicht-GSM-Zeichen um.

- **Erweiterte Optionen** – weitere Einstellungen pro Nachricht.

Senden stellt die Nachricht in die Warteschlange; der Thread erscheint sofort in Konversationen.

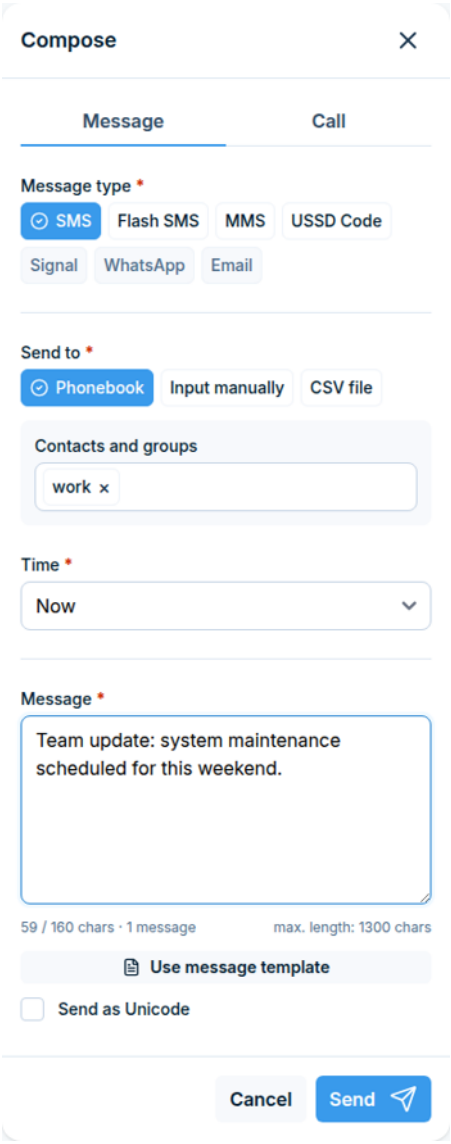
Ordner



Ordner

Nachrichten > SMS > Ordner (`/messages/sms/folders/`) listet die Standardordner (Eingang, In Warteschlange, Gesendet, Fehler beim Senden, Papierkorb) neben allen benutzerdefinierten Ordnern auf, die Sie unter **Meine Ordner** erstellt haben. Jeder Ordner zeigt, wie viele Nachrichten er enthält. Klicken Sie auf **Neuen Ordner erstellen**, um Ihren eigenen hinzuzufügen – nützlich zusammen mit Postfachregeln zum automatischen Sortieren eingehender Nachrichten und Ordner bereinigen zum automatischen Löschen.

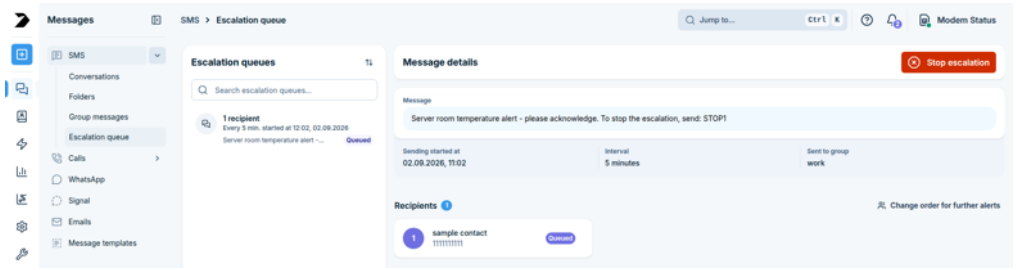
Gruppennachrichten



Verfassen einer Nachricht an eine Adressbuch-Gruppe

Nachrichten > SMS > Gruppennachrichten (`/messages/sms/groups/`) listet Konversationen auf, die Sie durch Senden an eine Adressbuch-Gruppe statt an eine einzelne Nummer gestartet haben – ein Eintrag pro Gruppensendung, damit Sie überprüfen können, an wen eine Gruppennachricht gesendet wurde, ohne einzelne Threads durchsuchen zu müssen.

Eskalationswarteschlange



Eskalationswarteschlange

Nachrichten > SMS > Eskalationswarteschlange (`/messages/sms/escalation/`) zeigt jede derzeit laufende Eskalation – eine Nachricht, die an eine Eskalationsgruppe gesendet wurde und sich noch durch die Kontaktliste arbeitet. Die Einrichtung einer Eskalationsgruppe selbst wird unter Adressbuch behandelt; diese Seite ist der Ort, an dem Sie eine bereits laufende überwachen und steuern können.

Jede laufende Eskalation wird mit ihrer Nachricht, ihrem Startzeitpunkt und ihrem Intervall aufgelistet. Das Öffnen einer zeigt **Nachrichtendetails**: den Nachrichtentext, die Startzeit, das Intervall, die Zielgruppe und jeden Empfänger mit einem Status von **Delivered**, **Sending**, **Queued** oder **Sending error**.

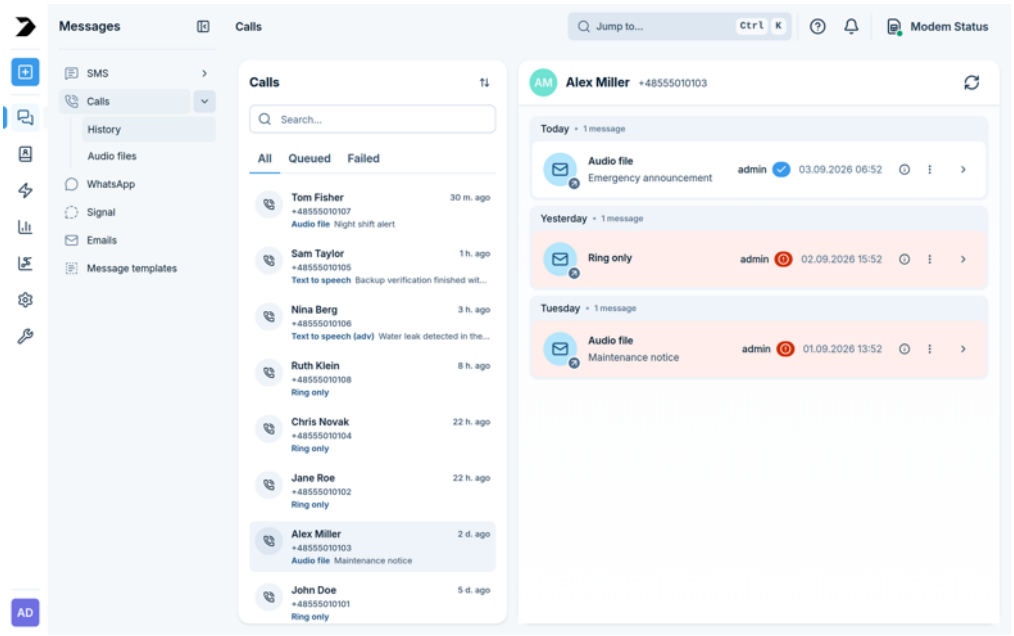
Aus dieser Ansicht können Sie:

- **Change order for further alerts** - Neuordnung der Personen, die noch nicht kontaktiert wurden.
- **Stop escalation** - Beendet die gesamte Eskalation sofort; niemand anderes auf der Liste wird kontaktiert.

Eine Eskalation endet auch automatisch, wenn ein Empfänger das Stoppwort der Gruppe antwortet oder sobald die letzte Person auf der Liste kontaktiert wurde.

Anrufe

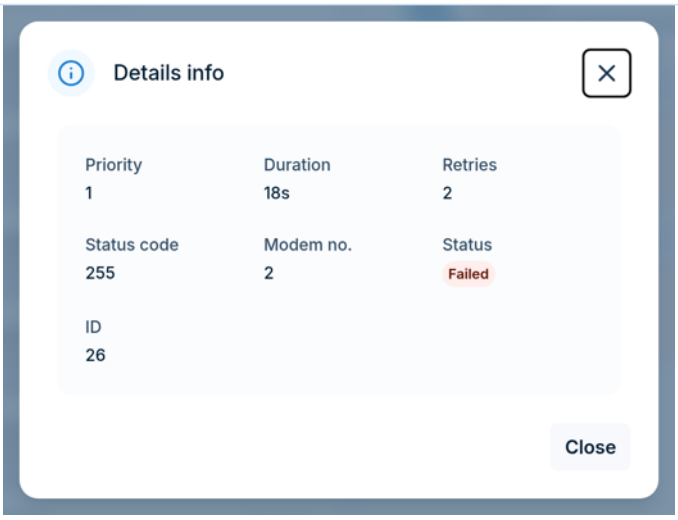
Verlauf



Anrufverlauf

Messages > Calls > History (`/messages/calls/`) listet jeden Anruf auf, den das Gerät getätigt hat, gruppiert nach Telefonnummer, neueste zuerst.

- Die Registerkarten **All**, **Queued** und **Failed** grenzen die Liste ein.
- Das Suchfeld findet Anrufe nach Nummer, nach Kontaktname oder nach dem vorgelesenen Text.
- Das Öffnen eines Anrufs zeigt seine Details: Priorität, Dauer, Wiederholungen, Statuscode, Modemnnummer und ID. Der Statuscode ist das, was Sie beim Support angeben sollten, wenn Sie nach einem fehlgeschlagenen Anruf fragen.
- Löschen Sie einen einzelnen Anruf oder wählen Sie mehrere aus und löschen Sie sie zusammen.

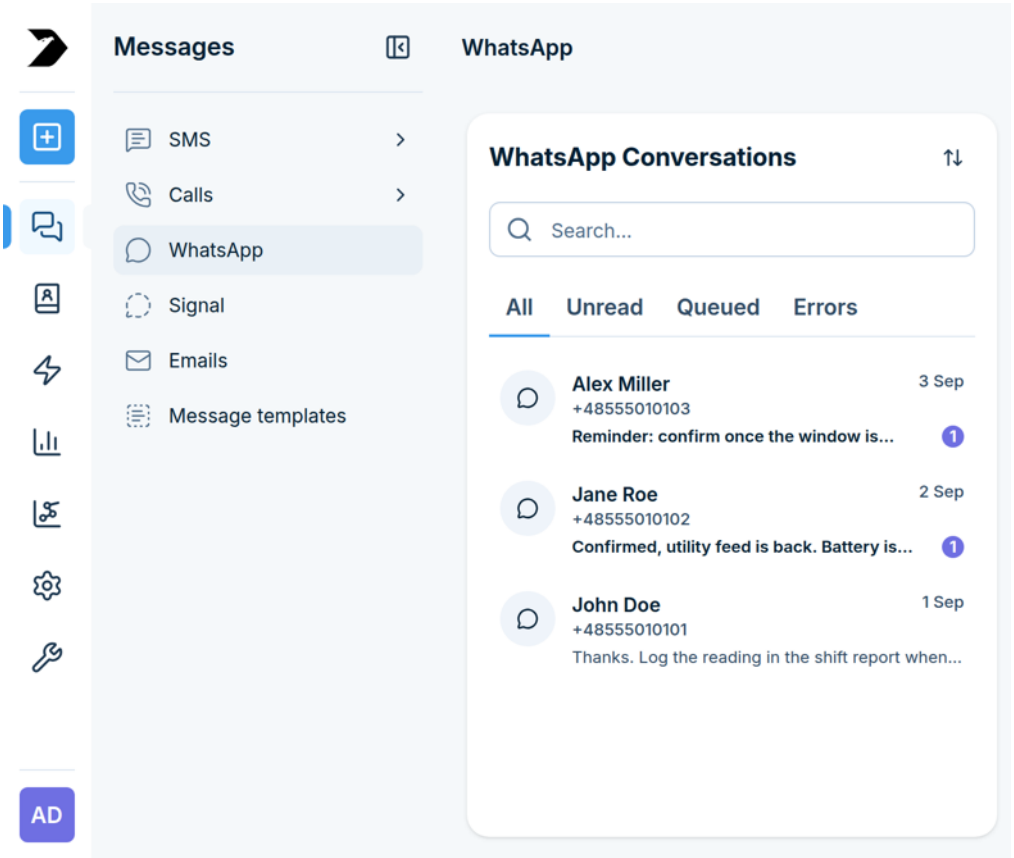


Anrufdetails

Anrufe werden wie Nachrichten in die Warteschlange eingereiht: Ein für später geplanter oder durch Priorität zurückgehaltener Anruf bleibt in dieser Liste als **Queued**, bis er getätigt wird. Das Tätigen eines Anrufs (Anruftypen, Sprachmodelle und das Compose

Call panel) wird unter Calls in den Einstellungen behandelt.

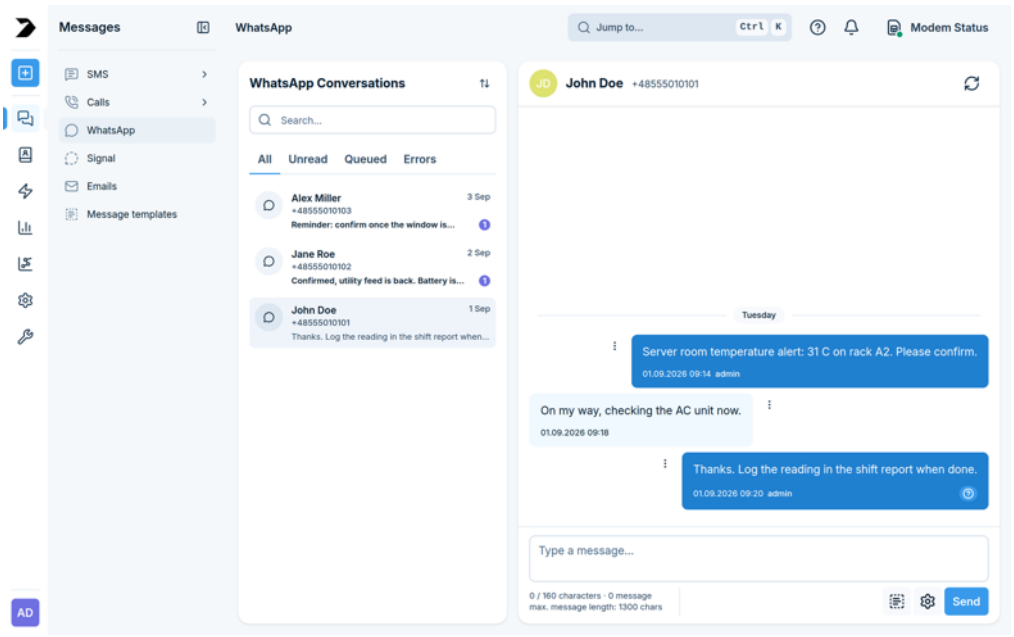
WhatsApp



WhatsApp-Gespräche

Messages > WhatsApp (`/messages/whatsapp/`) listet WhatsApp-Gespräche auf, eines pro Nummer, neueste zuerst, sobald der Kanal unter Einstellungen verlinkt wurde.

- Filtern Sie mit den Registerkarten **Alle**, **Ungelesen**, **In Warteschlange** und **Fehler**.
- Durchsuchen und sortieren Sie Gespräche nach Datum oder Telefonnummer.
- Öffnen Sie ein Gespräch und antworten Sie direkt aus dem Feld unten (maximal 1300 Zeichen).
- Löschen Sie ein einzelnes Gespräch oder wählen Sie mehrere aus und löschen Sie sie zusammen.

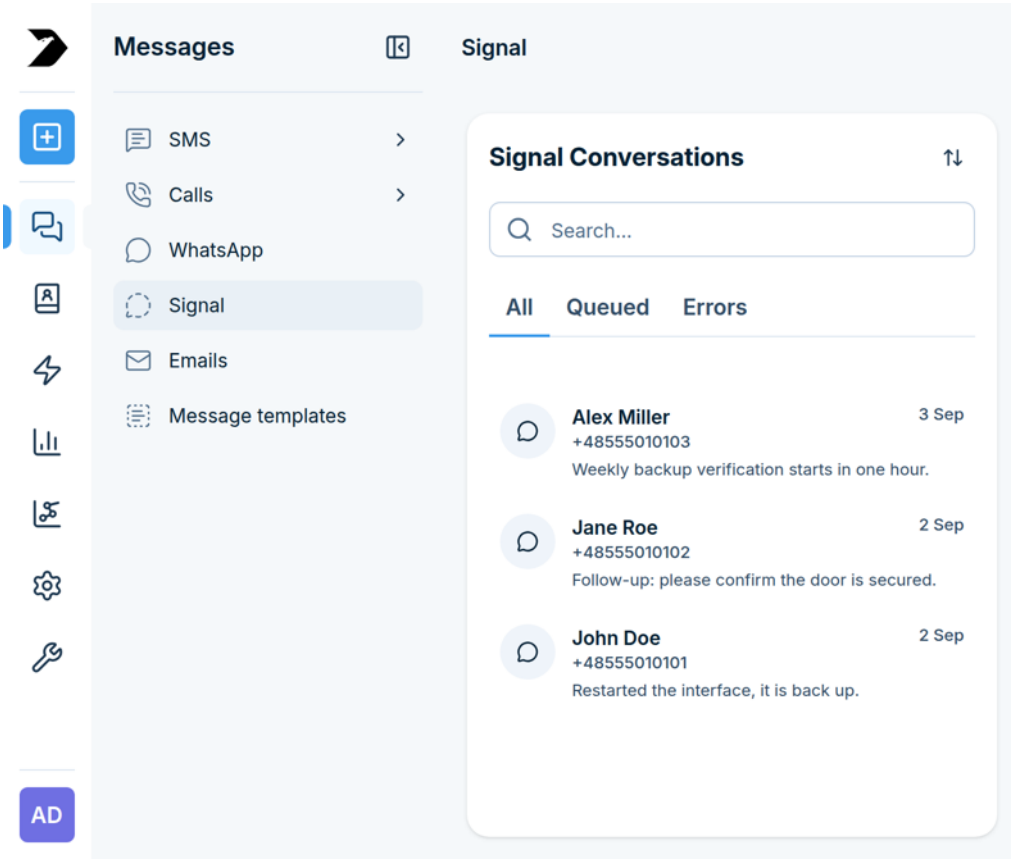


Ein offenes WhatsApp-Gespräch

Wenn WhatsApp noch nicht konfiguriert wurde, zeigt diese Seite einen Hinweis mit einer Schaltfläche, die Sie direkt zu den WhatsApp-Einstellungen bringt. Um eine neue WhatsApp-Nachricht zu senden, öffnen Sie **Compose**, aktivieren Sie **WhatsApp** als Nachrichtentyp und schreiben Sie wie gewohnt.

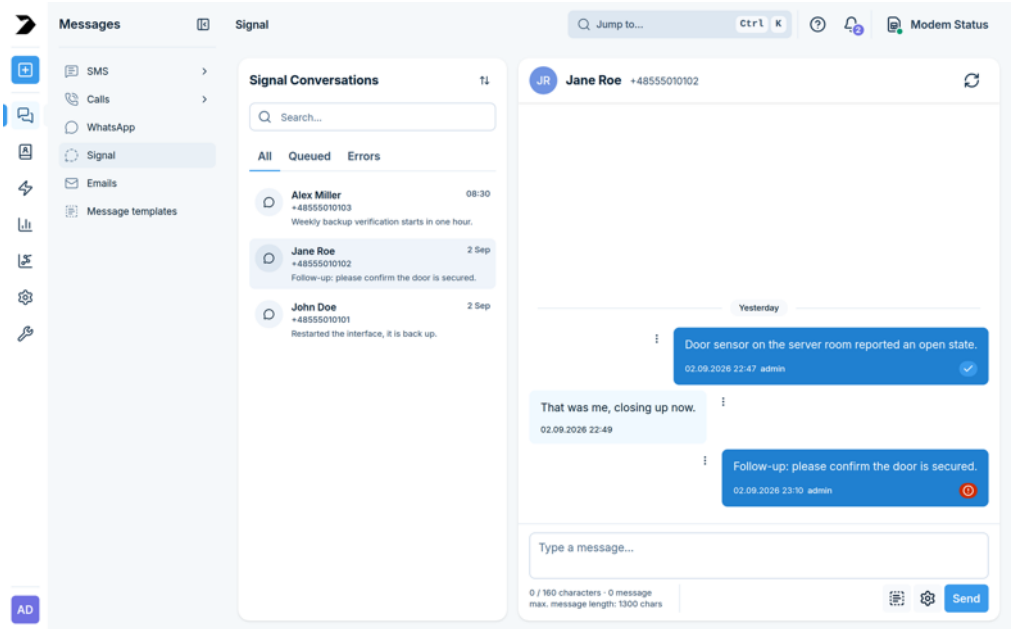
Nur Nachrichten, die nach dem Verlinken des Geräts empfangen wurden, erscheinen hier.

Signal



Signal-Gespräche

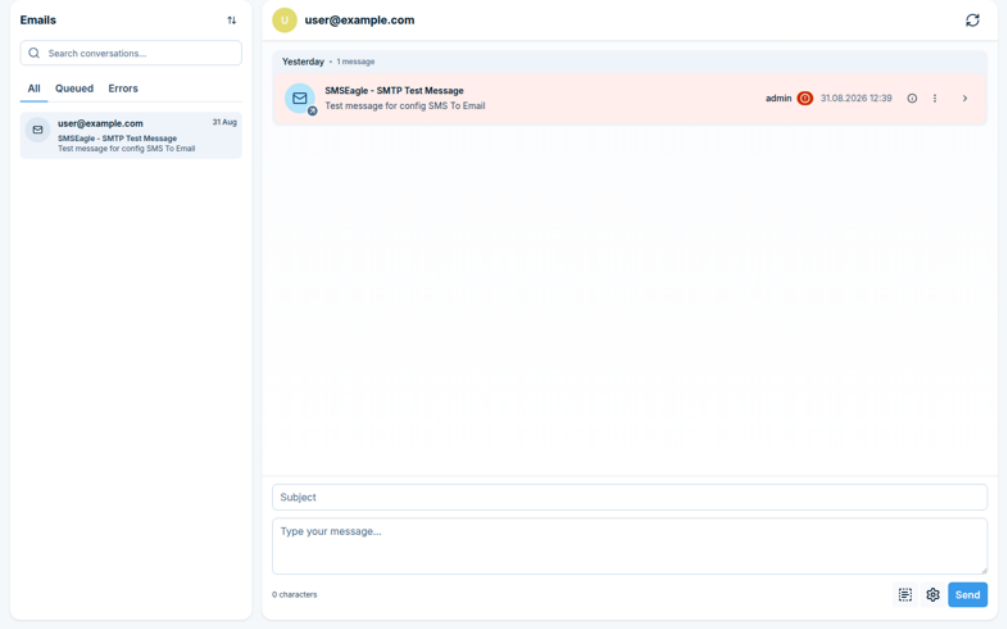
Nachrichten > Signal (`/messages/signal/`) funktioniert wie WhatsApp oben, sobald eine Nummer unter Einstellungen registriert wurde: ein Gespräch pro Nummer, die Filter **Alle / In der Warteschlange / Fehler** und Antwort aus dem Feld unten (maximal 1300 Zeichen). Signal hat keine **Ungelesen**-Registerkarte.



Ein offenes Signal-Gespräch

Um eine neue Signal-Nachricht zu senden, öffnen Sie **Compose**, wählen Sie **Signal** als Nachrichtentyp aus und schreiben Sie wie gewohnt. Hier werden nur Nachrichten angezeigt, die nach der Aktivierung des Dienstes empfangen wurden.

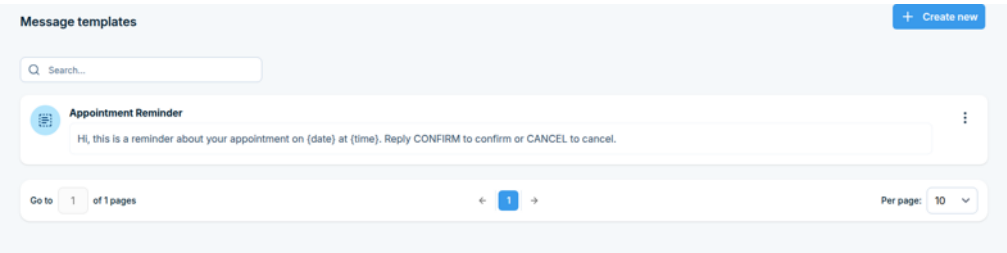
E-Mails



E-Mail-Gespräche

Nachrichten > E-Mails (`/messages/email/`) listet E-Mail-Gespräche auf, ein Thread pro Adresse, neueste zuerst, mit den Filtern **Alle**, **In der Warteschlange** und **Fehler** – dieselbe Gesprächsansicht wie SMS, WhatsApp und Signal für E-Mails, die über SMS to Email und Email to SMS gesendet oder empfangen wurden.

Nachrichtenvorlagen



Nachrichtenvorlagen

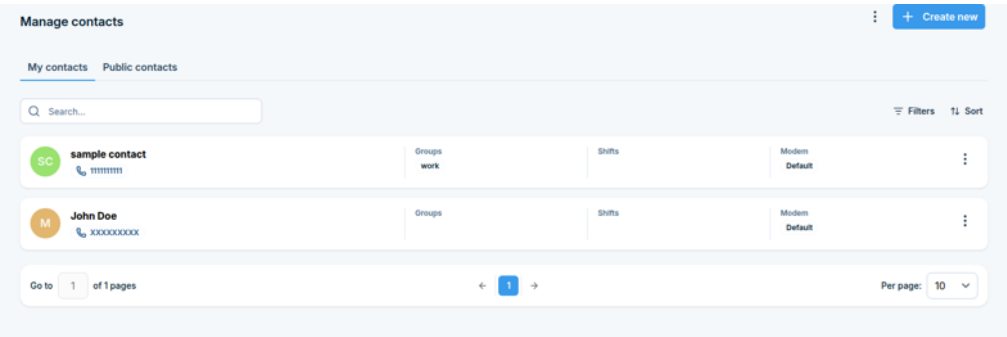
Nachrichten > Nachrichtenvorlagen (`/messages/templates/`) speichert wiederverwendbare Nachrichtentexte für Compose, damit häufig verwendete Nachrichten nicht jedes Mal neu eingegeben werden müssen.

Klicken Sie auf **Create new**, geben Sie einen **Template name** ein und schreiben Sie den **Message content**. Gespeicherte Vorlagen können dann in Compose ausgewählt werden, anstatt die Nachricht von Grund auf zu schreiben.

Telefonbuch

Das Telefonbuch ist der Ort, an dem Sie die Kontakte und Gruppen speichern, an die Sie Nachrichten senden oder von denen Sie Nachrichten erhalten.

Kontakte



Telefonbuch-Kontaktliste

Telefonbuch > Kontakte (`/phonebook/contacts`). Klicken Sie auf **Create new**, um einen Kontakt hinzuzufügen. Die Kontaktliste ist in zwei Registerkarten aufgeteilt:

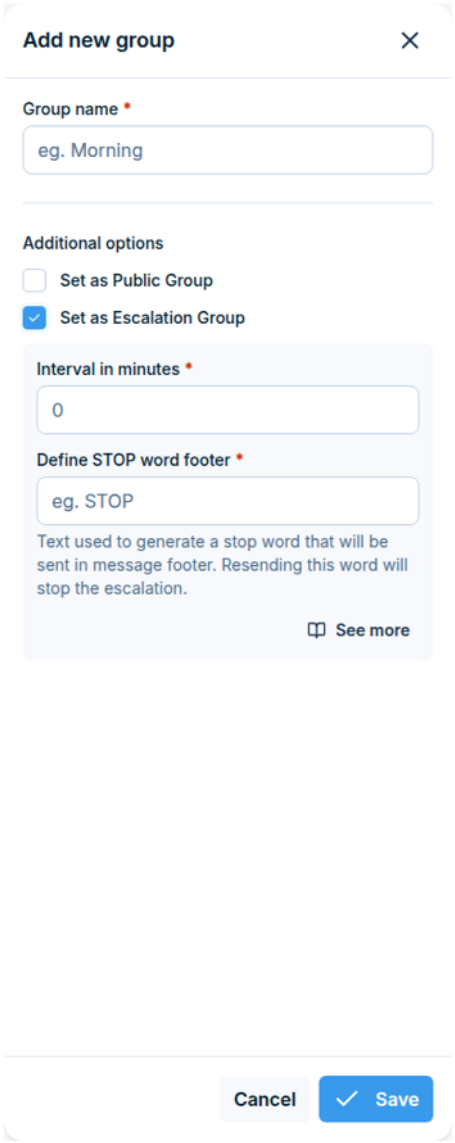
- **My contacts** - Kontakte, die nur Sie sehen und verwenden können.
- **Public contacts** - Kontakte, die mit anderen Benutzern des Geräts geteilt werden (erforderlich, damit ein öffentlicher Kontakt beispielsweise von Email to SMS angesprochen werden kann).

Jeder Kontakt kann zu einer oder mehreren **Groups** gehören, einen **Shift** (siehe Shifts unten) zugewiesen bekommen und an ein bestimmtes **Modem** für ausgehende Nachrichten angeheftet werden. Verwenden Sie **Filters** und **Sort**, um einen Kontakt in einem großen Telefonbuch zu finden.

Gruppen

Telefonbuch > Groups (`/phonebook/groups`). Gruppen ermöglichen es Ihnen, eine ganze Gruppe von Kontakten auf einmal anzusprechen (beispielsweise aus Compose SMS oder als Ziel einer Automatisierungsregel), statt jeden Kontakt einzeln auszuwählen. Klicken Sie auf **Add new**, geben Sie der Gruppe einen **Name**, und aktivieren Sie **Set as Public Group**, wenn andere Benutzer, Automatisierungsregeln oder die API an diese Gruppe senden sollen.

Eskalationsgruppen



Eskalationsgruppenoptionen im Dialog „Add new group“

Eine Eskalationsgruppe warnt Personen **nacheinander, nicht alle auf einmal**, bis jemand bestätigt, dass er sich des Problems annimmt – geben Sie Ihre On-Call-Mitarbeiter in einer gewählten Reihenfolge in eine Gruppe ein, legen Sie ein Intervall fest, und wenn Sie eine Nachricht an die Gruppe senden, erhält die erste Person sie sofort, die zweite bekommt sie, wenn niemand die Eskalation stoppt, und so weiter die Liste hinunter. Die Überwachung und Steuerung einer laufenden Eskalation erfolgt in Escalation queue unter Messages; in diesem Abschnitt richten Sie eine ein.

Schritt 1: Eskalationsgruppe erstellen

1. Klicken Sie auf **Add new**. Ein Seitenpanel öffnet sich.
2. Füllen Sie **Name** aus, z. B. `Night on-call`.
3. Aktivieren Sie **Escalation group**. Zwei weitere Felder werden angezeigt.

4. Füllen Sie **Escalation interval (minutes)** aus: wie lange Sie warten müssen, bevor Sie die nächste Person warnen. Zulässige Werte sind 1 bis 999.
5. Füllen Sie **Escalation stop word** aus: das Wort, das die Empfänger zurückschreiben, um die Eskalation zu stoppen.
    - Maximal 8 Zeichen.
    - Nur Buchstaben, keine Ziffern, Leerzeichen oder Satzzeichen.
    - Es muss eindeutig sein – jede Eskalationsgruppe benötigt ihr eigenes Stop-Wort.
6. Klicken Sie auf **Save**.

    Aktivieren Sie auch **Set as Public Group**, wenn andere Benutzer des Geräts, Automatisierungsregeln oder die API an diese Gruppe senden sollen.

Schritt 2: Personen hinzufügen und ihre Reihenfolge festlegen

1. Suchen Sie auf der Seite **Groups** Ihre Eskalationsgruppe und öffnen Sie **Manage contacts**.
2. Fügen Sie die Kontakte hinzu, die benachrichtigt werden sollen.
3. Bringen Sie sie in die richtige Reihenfolge, indem Sie die Karten **nach oben und unten ziehen**. Die Person oben wird zuerst kontaktiert – dies ist genau die Reihenfolge, in der Warnungen gesendet werden.

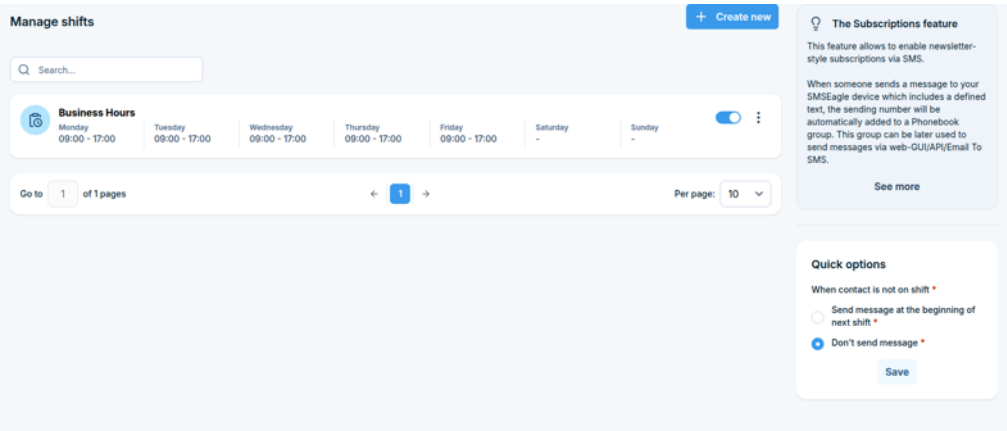
Schritt 3: Eine Eskalation auslösen

Senden Sie eine Nachricht an die Gruppe auf die gleiche Weise wie jede andere Nachricht, von **Compose** aus. SMSEagle fügt dann eine Zeile hinzu, die dem Empfänger mitteilt, was er zurückschreiben soll, um die Eskalation zu stoppen (in der Form `To stop the escalation, send: <stop word><number>`), sendet die Nachricht sofort an den ersten Kontakt und plant die gleiche Nachricht für die nächsten Kontakte ein, mit dem von Ihnen festgelegten Abstand.

> **Teilen Sie Ihren Empfängern genau mit, was sie antworten sollen.** Die Nummer nach dem Stoppwort identifiziert diese bestimmte Eskalation, daher muss die Antwort das Ganze enthalten, z. B. `ACK17`, was genau übereinstimmen muss - das Stoppwort **und** die Nummer ohne Leerzeichen verbunden, in der gleichen Groß- und Kleinschreibung, und nichts anderes in der Nachricht. Nur jemand, der ein Mitglied der Eskalationsgruppe ist, kann diese stoppen; eine Antwort von einer unabhängigen Nummer wird ignoriert.

Sie können eine Eskalationsgruppe auch über die API, von E-Mail zu SMS oder von jeder Automatisierungsregel auslösen, die an eine Gruppe sendet.

Schichten



Übersicht der Schichtverwaltung

Schichten beschreiben **wann eine Person im Dienst ist**. Sobald Sie einem Kontakt eine Schicht zuweisen, prüft SMSEagle die Schicht vor dem Versand einer Nachricht: Wenn eine Nachricht an einen Kontakt adressiert ist, der sich derzeit außerhalb seiner Schichtzeiten befindet, hält SMSEagle die Nachricht entweder an und sendet sie zu Beginn seiner nächsten Schicht, oder sendet sie überhaupt nicht - Sie wählen, welches der Fall ist (siehe Schritt 4 unten).

Typische Verwendung: ein On-Call-Dienst, bei dem die Nachtschicht nicht durch Warnungen geweckt werden sollte, die für die Tagesschicht bestimmt sind.

> **Gut zu wissen:** ein Kontakt mit **keine Schicht zugewiesen** wird immer als verfügbar betrachtet. Schichten beschränken nur die Kontakte, denen Sie sie zuweisen.

Bevor Sie beginnen

- Sie benötigen mindestens einen Kontakt im Phonebook (**Phonebook > Contacts**).
- Stellen Sie sicher, dass die Gerätuhr und die Zeitzone korrekt sind, da Schichtzeiten gegen die Gerätezeit verglichen werden. Überprüfen Sie dies unter **Settings > Date/Time**.

Schritt 1: Öffnen Sie die Seite „Shifts“

Phonebook > Shifts (`/phonebook/shifts`) listet die bereits erstellten Schichten auf, mit einem **Quick options**-Feld auf der rechten Seite.

Schritt 2: Erstellen Sie eine Schicht

1. Klicken Sie auf **Create new** in der oberen rechten Ecke. Ein Seitenpanel wird geöffnet.
2. Füllen Sie **Name** aus, zum Beispiel `Night shift` oder `Weekend duty`.
3. Lassen Sie **Enabled** aktiviert, damit die Schicht sofort funktioniert. Deaktivieren Sie es, um die Schicht jetzt vorzubereiten und später zu aktivieren.
4. Legen Sie unter **Active from - to** die Stunden für jeden Wochentag fest: Geben Sie eine **From**- und eine **To**-Zeit für jeden Tag ein, an dem die Person im Dienst ist, und lassen Sie einen Tag leer, wenn dies nicht der Fall ist.

5. Klicken Sie auf **Save**.

Regeln für Schichtzeiten

- **From** muss früher als **To** am gleichen Tag sein.
- Sowohl **From** als auch **To** müssen ausgefüllt sein, oder beide müssen leer gelassen werden. Ein halb ausgefüllter Tag wird mit einer Fehlermeldung abgelehnt.
- Mindestens ein Tag muss Stunden haben, die festgelegt sind.

  Nachtschichten: Eine Schicht, die Mitternacht überschreitet (z. B. 22:00 bis 06:00), muss als zwei Einträge eingegeben werden: `22:00 - 23:59` am ersten Tag und `00:00 - 06:00` am nächsten Tag.

Schritt 3: Weisen Sie Kontakte der Schicht zu

Sie können dies von beiden Seiten tun.

Von der Schicht aus: Suchen Sie auf der Seite **Shifts** Ihre Schicht, öffnen Sie ihre Aktionen und wählen Sie **Manage contacts**.

Vom Kontakt aus: Gehen Sie zu **Phonebook > Contacts**, wählen Sie einen oder mehrere Kontakte mit ihren Kontrollkästchen aus, wählen Sie **Edit shifts**, wählen Sie die Schichten aus, die Sie zuweisen möchten, und klicken Sie auf **Assign shifts**.

Schritt 4: Wählen Sie, was außerhalb der Schichtzeiten passiert

Das Feld **Quick options** auf der rechten Seite der Shifts-Seite enthält **When contact is not on shift**:

Option	Result
Send message at the beginning of next shift	Die Nachricht wartet in der Warteschlange und wird automatisch zugestellt, wenn die nächste Schicht des Kontakts beginnt.
Don’t send message	Die Nachricht wird nicht an diesen Kontakt gesendet. Sie wird als nicht zugestellt verzeichnet.

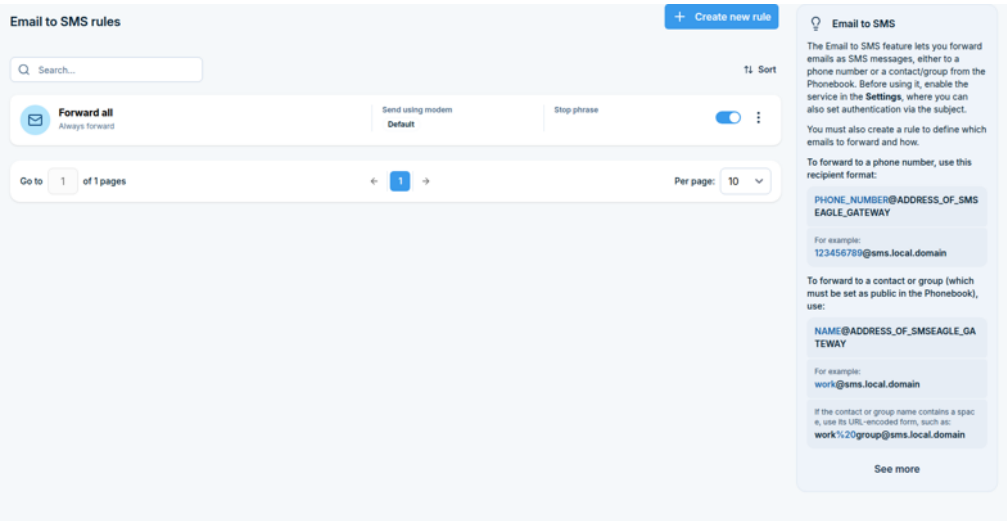
Wählen Sie die gewünschte Option aus und klicken Sie auf **Save**.

> Diese Einstellung ist **global**. Sie gilt für jede Schicht und jeden Kontakt auf dem Gerät, nicht nur für die Schicht, die Sie derzeit anzeigen.

Automatisierung

Dieses Kapitel behandelt den Bereich **Automatisierung** der Weboberfläche in derselben Reihenfolge wie die Regeln dort angezeigt werden.

Email zu SMS



Email to SMS-Regeln

Mit der Funktion „Email zu SMS“ können Sie eingehende E-Mails als SMS-Nachrichten weiterleiten, entweder an eine Telefonnummer oder an einen Kontakt/eine Gruppe aus Ihrem Adressbuch.

Wo finden Sie es

Die Funktion ist an zwei Stellen in der WebGUI verteilt:

- **Automation > Email > Email zu SMS** (`/automation/email-to-sms`) ist der Ort, an dem Sie Weiterleitungsregeln erstellen und verwalten.
- **Einstellungen > Kanäle > Email > Email zu SMS** (`/settings/email/email-to-sms`) ist der Ort, an dem Sie den Dienst aktivieren und konfigurieren, wie E-Mails in Nachrichten konvertiert werden – siehe Email zu SMS in Einstellungen.

Schritt 1: Verstehen Sie das Format der Empfängeradresse

E-Mails müssen an eine speziell formatierte Adresse gesendet werden, damit SMSEagle weiß, wohin die Nachricht zugestellt werden soll.

So leiten Sie an eine Telefonnummer weiter:

```
PHONE_NUMBER@ADDRESS_OF_SMSEAGLE_GATEWAY
```

Beispiel: `999888777@gateway.smseagle.eu`

So leiten Sie an einen Kontakt oder eine Gruppe aus dem Adressbuch weiter (der Kontakt oder die Gruppe muss als **öffentlich** eingestellt sein):

```
NAME@ADDRESS_OF_SMSEAGLE_GATEWAY
```

Beispiel: `work@gateway.smseagle.eu`

Wenn der Kontakt- oder Gruppenname ein Leerzeichen enthält, verwenden Sie die URL-codierte Form: `work%20group@gateway.smseagle.eu`

Anstelle der Gateway-IP-Adresse können Sie einen vollständig qualifizierten Domänennamen verwenden, der unter **Einstellungen > Kanäle > Email > Email zu SMS > Erweiterte Einstellungen > FQDN-Hostname** festgelegt ist. Wenn dort **LDAP-Kontakte verwenden** aktiviert ist, werden mit demselben `NAME@GATEWAY`-Format auch Kontakte und Gruppen aus LDAP/Active Directory aufgelöst.

Standardmäßig wird der Text der E-Mail zum SMS-Text. Dies hängt von der Einstellung **Was soll mit dem E-Mail-Betreff geschehen** in den Einstellungen ab: Der Betreff kann ignoriert, dem Nachrichtentext vorangestellt, zur Authentifizierung verwendet oder statt des Texts gesendet werden.

Schritt 2: Erstellen Sie eine neue Regel

Gehen Sie zu **Automation > Email > Email zu SMS** und klicken Sie auf **Neue Regel erstellen**. Ein Panel mit dem Titel Email-zu-SMS-Regel hinzufügen öffnet sich auf der rechten Seite.

Feld	Beschreibung
Regelname *	Ein Name zur Identifizierung der Regel (erforderlich, max. 100 Zeichen)
Weiterleiten für *	Immer senden leitet jede eingehende E-Mail weiter, die dem Adressformat entspricht. Angefügte Absender/Nachricht enthält fügt Filterbedingungen hinzu, siehe Schritt 3.
Stoppphrase	Text ab dieser Phrase wird aus der Nachricht entfernt (Groß-/Kleinschreibung beachtet)
Priorität	Sendpriorität von 0 bis 5. Nachrichten mit höherer Priorität werden zuerst verarbeitet.
Anruf nach dem Versand von SMS	Nein, Nur Klingeln, Ja – Sprachsynthese, oder Ja – Sprachsynthese (erweitert). Die verfügbaren Optionen hängen von der Stimme und den TTS-Fähigkeiten Ihres Geräts ab.
Sprachmodell	Stimme für den Sprachsynthese-Anruf. Wird nur bei Geräten angezeigt, die erweiterte TTS unterstützen, und nur nach Auswahl von Ja – Sprachsynthese (erweitert).
Erzwinge Konvertierung zu UTF-8	Erzwingt die Konvertierung des Nachrichtentexts zu UTF-8
Gesprächsverlauf entfernen	Entfernt zitierte Verlaufsangaben der E-Mail-Konversation aus dem Nachrichtentext

Klicken Sie auf **Save**, um die Regel zu erstellen, oder auf **Cancel**, um sie zu verwerfen.

Schritt 3: Filterbedingungen hinzufügen (optional)

Wenn Sie unter Forward for die Option **Specified sender / message contains** auswählen, stehen drei unabhängige Bedingungen zur Verfügung, jeweils mit einem Kontrollkästchen und einem Textfeld:

- **When incoming email address contains** filtert nach der E-Mail-Adresse des Absenders
- **When incoming messages subject contains** filtert nach der Betreffzeile der E-Mail
- **When incoming message content contains** filtert nach dem E-Mail-Text

Der Schalter **Case sensitive** gilt für alle aktivierten Bedingungen.

Sie können eine, zwei oder alle drei Bedingungen aktivieren. Die Regel wird nur ausgelöst, wenn **alle** aktivierten Bedingungen erfüllt sind.

Schritt 4: Vorhandene Regeln verwalten

Jede Regel erscheint als Karte in der Liste „Email to SMS

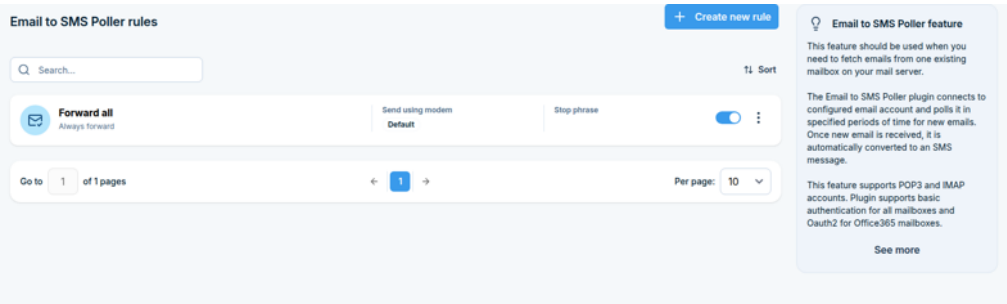
- der Name der Regel
- die Weiterleitungsbedingung, z. B. Forward when incoming: email address contains: ..., oder Always forward, wenn keine Bedingung festgelegt ist
- das für den Versand verwendete Modem
- die konfigurierte Stoppphrase
- ein Ein-/Ausschalter zum Aktivieren oder Deaktivieren der Regel, ohne sie zu löschen
- ein Menü ⋮ mit **Edit** und **Delete**

Zusätzliche Steuerelemente in der Liste:

- **Search** filtert Regeln nach Name.
- Die Auswahl von Regel-Kontrollkästchen zeigt Massenaktionen an: **Enable / Disable** und **Delete**.
- Mit den Paginierungssteuerelementen unten können Sie zu einer Seite springen und ändern, wie viele Regeln pro Seite angezeigt werden.

Das rechte Hilfefenster erklärt die Formate der Empfängeradresse, mit einer Schaltfläche **See more**, die auf die Seite dieser Funktion auf smseagle.eu verlinkt.

Email zu SMS Poller



Email to SMS Poller-Regeln

Der Email zu SMS Poller prüft regelmäßig ein externes Postfach über POP3, IMAP oder IMAP mit OAuth2 (Microsoft 365 / Outlook) und konvertiert die dort gefundenen E-Mails gemäß den Email zu SMS Poller-Regeln in SMS-Nachrichten. Im Gegensatz zu Email zu SMS (das seinen eigenen Mail-Server betreibt und aktiv E-Mails empfängt) greift der Poller auf ein vorhandenes Postfach zu, das Sie bereits haben.

Wo finden Sie es

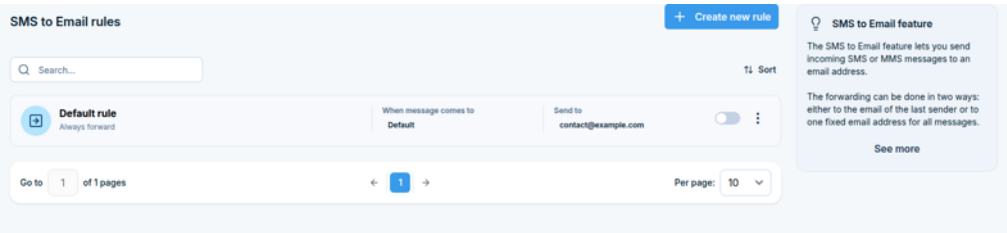
Automation > Email > Email zu SMS Poller (`/automation/email-to-sms-poller/`) ist der Ort, an dem Sie Regeln erstellen und verwalten. Das Aktivieren des Dienstes und das Verbinden des Postfachs

(POP3, IMAP oder IMAP + OAuth2 für Microsoft 365) erfolgt unter Email zu SMS Poller in den Einstellungen.

Eine Regel erstellen

Klicken Sie auf **Create new rule**. Regeln funktionieren hier genauso wie Email zu SMS-Regeln - benennen Sie die Regel, wählen Sie, ob sie jede gescannte E-Mail weiterleitet oder nur solche, die Bedingungen für Absender/Betreff/Inhalt erfüllen, und legen Sie die gleichen Pro-Regel-Optionen fest (Modem, Stoppphrase, Priorität, Anruf nach dem Senden).

SMS zu Email



SMS zu Email-Regeln

Was diese Funktion bewirkt

SMS zu Email leitet **eingehende** SMS- und MMS-Nachrichten an eine E-Mail-Adresse weiter, damit Sie diese in Ihrem Postfach lesen können, anstatt sich in SMSEagle anzumelden.

Sie erstellen Regeln, die festlegen, welche Nachrichten weitergeleitet werden und wohin sie gehen. Eine Regel kann alles weiterleiten oder nur Nachrichten von bestimmten Absendern oder nur Nachrichten, die einen bestimmten Ausdruck enthalten.

Typische Anwendungsfälle: Weiterleitung von Antworten von Feldpersonal an ein gemeinsames Support-Postfach oder Archivierung von Warnbestätigungen in einem Ticketing-System-Posteingang.

Bevor Sie beginnen

SMSEagle benötigt eine funktionierende Mail-Server-Konfiguration zum Senden der E-Mails. Gehen Sie zu **Settings > Channels > Email > SMTP Configuration** und stellen Sie sicher, dass diese ausgefüllt und getestet ist - siehe SMTP Configuration. Ohne sie werden Regeln zwar abgeglichen, aber keine E-Mail kommt an.

Wenn Sie auf Basis von Sender-Kontakten oder -Gruppen weiterleiten möchten, müssen diese Kontakte und Gruppen im Phonebook als **Public** gekennzeichnet sein.

Schritt 1: SMS zu Email-Seite öffnen

Gehen Sie in der Seitenleiste zu **Automation > Email > SMS to Email**.

Schritt 2: Eine Regel erstellen

Klicken Sie oben rechts auf **Create new rule**. Ein Seitenpanel wird geöffnet.

Benennen Sie die Regel

Geben Sie unter **Rule name** einen aussagekräftigen Namen ein, z. B. `Forward all to support`. Maximum 100 Zeichen.

Entscheiden Sie, welche Nachrichten weitergeleitet werden sollen

Wählen Sie **Forward for**:

Option	Bedeutung
Always forward	Jede eingehende SMS und MMS wird weitergeleitet.
Specified sender / message	Nur Nachrichten, die den unten festgelegten Bedingungen entsprechen, werden weitergeleitet.

Wenn Sie **Angegebener Absender / Nachricht** wählen, sind zwei Bedingungen verfügbar. Sie können eine oder beide verwenden. Wenn Sie beide verwenden, muss eine Nachricht **beide** erfüllen, um weitergeleitet zu werden.

Wenn eingehende SMS von Aktivieren Sie dies und wählen Sie die Kontakte oder Gruppen aus, deren Nachrichten weitergeleitet werden sollen. Geben Sie zum Suchen etwas ein. Nur **öffentliche** Kontakte und Gruppen können hier ausgewählt werden.

Wenn eingehender SMS-Text enthält Aktivieren Sie dies und geben Sie die zu suchende Phrase ein, beispielsweise `URGENT`. Die Phrase kann überall im Nachrichtentext erscheinen. Aktivieren Sie **Groß-/Kleinschreibung beachten**, wenn `urgent` und `URGENT` als unterschiedlich behandelt werden sollen.

Wählen Sie die Ziel-E-Mail-Adresse

Wählen Sie **Art der E-Mail-Weiterleitung**:

Option	Bedeutung
An feste E-Mail-Adresse	Jede passende Nachricht geht an die eine Adresse, die Sie in **Weiterleiten an E-Mail-Adresse** eingeben.
An E-Mail des letzten sendenden Benutzers	Die Nachricht wird an die E-Mail-Adresse der Person zurückgesendet, die zuletzt eine SMS an diese Telefonnummer über SMSEagle gesendet hat. Dies schließt die Schleife einer E-Mail-zu-SMS-Konversation. Geben Sie eine **Standardmailadresse** als Fallback ein, die verwendet wird, wenn kein letzter Absender erfasst ist.

Legen Sie den E-Mail-Betreff fest

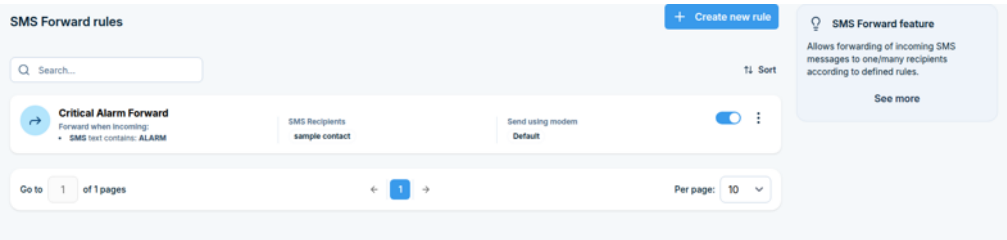
Email subject steuert die Betreffzeile der weitergeleiteten E-Mail. Sie können Platzhalter verwenden, die beim Versenden der E-Mail durch tatsächliche Werte ersetzt werden:

Platzhalter	Ersetzt durch
`{SENDER}`	Die Telefonnummer, von der die SMS stammt
`{WORDS,X}`	Die ersten X Wörter des Nachrichtentexts
`{CHARS,X}`	Die ersten X Zeichen des Nachrichtentexts

Beispiel: `SMS from {SENDER}: {WORDS,5}` erzeugt einen Betreff wie `SMS from +48111222333: Server room temperature alarm triggered`. Maximum 150 Zeichen.

Klicken Sie auf **Save**. Die Regel wird sofort auf neu empfangene Nachrichten angewendet.

SMS Forward



Dialog zum Hinzufügen einer Weiterleitungsregel

Was diese Funktion bewirkt

SMS Forward leitet **eingehende SMS-Nachrichten an andere Personen weiter**. Wenn eine Nachricht ankommt, sendet SMSEagle sie erneut an die von Ihnen gewählten Empfänger.

Sie können die Nachricht genau so weitergeben, wie sie angekommen ist, oder sie durch Ihren eigenen Text ersetzen. Sie können auch einen Sprachanruf zusätzlich zur weitergeleiteten SMS hinzufügen, damit eine Benachrichtigung nicht übersehen werden kann.

Typische Anwendungen: Versand von Alarmmeldungen von einer Maschine an das gesamte On-Call-Team, Weitergabe von Nachrichten von einer gemeinsamen Nummer an die gerade zuständige Person oder Umwandlung eines kurzen Maschinencodes in einen verständlichen Satz für das Team.

Bevor Sie beginnen

- Die Kontakte und Gruppen, an die Sie **weiterleiten**, müssen in dem Phonebook existieren. Kontakte und Gruppen, die als Weiterleitungsempfänger oder als Absenderbedingungen verwendet werden, müssen als **Public** gekennzeichnet sein.

- Entscheiden Sie, ob die Empfänger den Originalwortlaut oder eine umgeschriebene Nachricht benötigen.

Schritt 1: Öffnen Sie die Seite SMS Forward

Gehen Sie in der Seitenleiste zu **Automation > SMS > SMS Forward**.

Schritt 2: Eine Regel erstellen

Klicken Sie oben rechts auf **Create new rule**. Ein Seitenpanel wird geöffnet.

Nennen Sie die Regel und legen Sie ihre Priorität fest

Rule name Eine aussagekräftige Bezeichnung, z. B. `Alarms to on-call team`. Maximale Länge: 100 Zeichen.

Priority Eine Zahl von 0 bis 9. Nachrichten, die von einer Regel mit höherer Priorität erzeugt werden, werden früher zum Versand eingeplant als Nachrichten von einer Regel mit niedrigerer Priorität. Behalten Sie die Standardeinstellung bei, es sei denn, Sie haben dringende Regeln, die Massenversände überholen müssen.

Entscheiden Sie, welche Nachrichten weitergeleitet werden sollen

Wählen Sie **Forward for**:

Option	Bedeutung
All incoming messages	Jede eingehende SMS wird weitergeleitet.
Specified sender / message	Nur Nachrichten, die den unten festgelegten Bedingungen entsprechen, werden weitergeleitet.

Wenn Sie **Angegebener Absender / Nachricht** wählen, sind zwei Bedingungen verfügbar. Sie können eine oder beide verwenden. Wenn Sie beide verwenden, muss eine Nachricht **beide** erfüllen, um weitergeleitet zu werden.

When incoming SMS comes from Aktivieren Sie diese Option und wählen Sie die Absenderkontakte oder Gruppen unter **Sender contacts** aus. Hier können nur **öffentliche** Kontakte und Gruppen ausgewählt werden.

When incoming SMS text contains Aktivieren Sie diese Option und geben Sie den Ausdruck unter **Text fragment** ein, z. B. `ALARM`. Der Ausdruck kann überall in der Nachricht vorkommen. Aktivieren Sie **Case sensitive**, wenn `alarm` und `ALARM` unterschiedlich behandelt werden sollen.

Legen Sie fest, was die weitergeleitete Nachricht enthalten soll

Verwenden Sie **Message content**:

Option A: Originalnachricht

Die Empfänger erhalten den eingehenden Text unverändert. Eine zusätzliche Option erscheint: **Message header**:

Option	Ergebnis
Don't include	Nur der Originaltext wird weitergeleitet.
Include sender	Die Telefonnummer des ursprünglichen Absenders wird zur weitergeleiteten Nachricht hinzugefügt, damit die Empfänger wissen, woher sie kommt.

Option B: Benutzerdefinierter Text

Die Empfänger erhalten Ihren eigenen Text statt der Originalnachricht. Geben Sie ihn unter **Custom message** ein (maximale Länge: 500 Zeichen). Sie können Teile der Originalnachricht mit Platzhaltern einfügen:

Platzhalter	Ersetzt durch
`{SENDER}`	Die Telefonnummer, von der die SMS stammt
`{MESSAGE}`	Der vollständige Text der Originalnachricht

Beispiel: `Alarm from {SENDER}. Details: {MESSAGE}` sendet einen lesbaren Satz, der um den Maschinentext aufgebaut ist.

Wählen Sie die Empfänger

Wählen Sie unter **Forward to** die Kontakte oder Gruppen aus, die die Nachricht erhalten sollen. Beginnen Sie zu tippen, um zu suchen. Dieses Feld ist erforderlich; eine Regel kann nicht ohne mindestens einen Empfänger gespeichert werden.

Fügen Sie optional einen Sprachanruf hinzu

Call after sending SMS lässt das Gerät auch einen Sprachanruf an dieselben Empfänger tätigen. Die verfügbaren Optionen hängen von Ihrem Gerätemodell ab:

Option	Was passiert
No	Es wird kein Anruf getätigt. Dies ist die Standardeinstellung.
Nur klingeln	Das Gerät ruft den Empfänger an und legt auf. Es wird keine Audioausgabe wiedergegeben.
Ja – Sprachausgabe	Das Gerät ruft an und liest den Nachrichtentext vor.
Ja – Sprachausgabe (erweitert)	Dasselbe wie oben, mit einer auswählbaren, natürlicheren Stimme. Wählen Sie die Stimme im Feld **Voice model** aus, das angezeigt wird.

Wenn Ihr Gerät keine Sprachanrufe unterstützt, ist nur **Nein** verfügbar.

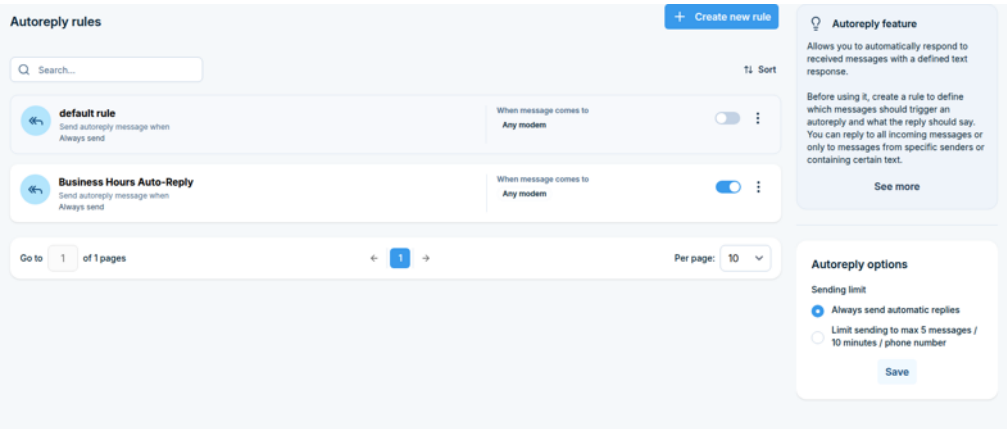
Klicken Sie auf **Save**. Die Regel wird sofort auf neu empfangene Nachrichten angewendet.

So funktioniert die Weiterleitung

- Die Textbedingung ist eine **Contains**-Übereinstimmung, keine exakte Übereinstimmung. Eine Regel, die nach `ALARM` sucht, leitet eine Nachricht mit dem Text `ROOM 4 ALARM triggered` weiter.
- Wenn mehrere Regeln auf die gleiche eingehende Nachricht zutreffen, leitet **jede** von ihnen separat weiter, sodass Empfänger mehrere SMS erhalten können. Halten Sie die Bedingungen unterschiedlich, um Duplikate zu vermeiden.
- Regeln gelten nur für Nachrichten, die nach der Erstellung und Aktivierung der Regel eingehen. Sie verarbeiten keine bereits im Posteingang vorhandenen Nachrichten.
- Empfänger können aus ihren eigenen Gründen übersprungen werden: **Abwesenheitsmodus** im Kontakt, eine Schicht, die derzeit außerhalb ihrer Zeiten liegt (siehe Shifts), oder die Nummer auf der Ablehnungsliste.

  Vermeiden Sie Weiterleitungsschleifen. Leiten Sie Nachrichten nicht an eine Nummer weiter, die ihrerseits an Ihr Gerät zurückleitet. Zwei Geräte, die aufeinander verweisen, senden sich gegenseitig immer wieder Nachrichten zu.

Automatische Antworten



Autoreply-Regeln und Sendebeschränkungsoptionen

Was diese Funktion bewirkt

Autoreplies sendet eine **automatische Textantwort auf eingehende SMS-Nachrichten**.

Sie erstellen Regeln, die festlegen, welche eingehenden Nachrichten eine Antwort erhalten und wie die Antwort aussieht. Eine Regel kann auf alles antworten oder nur auf Nachrichten von bestimmten Absendern oder nur auf Nachrichten mit einer bestimmten Phrase.

Typische Verwendungen: Bestätigung, dass eine Bestellanfrage eingegangen ist, Benachrichtigung der Personen, dass die Nummer nachts nicht besetzt ist, oder Beantwortung eines Schlüsselwortes mit festen Informationen wie Öffnungszeiten.

Bevor Sie beginnen

- Das Gerät muss SMS senden können. Überprüfen Sie, dass mindestens ein Modem angeschlossen und im Netz registriert ist.
- Wenn Sie nur auf bestimmte Absender antworten möchten, müssen diese Kontakte und Gruppen im Phonebook als **Public** gekennzeichnet sein.

Schritt 1: Öffnen Sie die Seite Autoreplies

Gehen Sie in der Seitenleiste zu **Automation > SMS > Autoreplies**.

Auf der rechten Seite der Seite befindet sich ein Feld **Autoreply options**. Es enthält eine Einstellung, die auf alle Regeln angewendet wird und in Schritt 3 beschrieben wird.

Schritt 2: Eine Regel erstellen

Klicken Sie oben rechts auf **Create new rule**. Ein Seitenpanel wird geöffnet.

Benennen Sie die Regel

Geben Sie in **Rule name** etwas Aussagekräftiges ein, z. B. `Out of hours reply`. Maximum 100 Zeichen.

Entscheiden Sie, auf welche Nachrichten geantwortet werden soll

Wählen Sie **Send autoreply for**:

Option	Bedeutung
All incoming messages	Jede eingehende SMS erhält die Antwort.
Specified sender / message	Nur Nachrichten, die die unten festgelegten Bedingungen erfüllen, erhalten eine Antwort.

Wenn Sie **Specified sender / message** gewählt haben, werden zwei Bedingungen verfügbar. Sie können eine oder beide verwenden. Wenn Sie beide verwenden, muss eine Nachricht **beide** Bedingungen erfüllen, um eine Antwort zu erhalten.

Wenn eingehende SMS von Aktivieren Sie diese Option und wählen Sie die Kontakte oder Gruppen aus, die eine Antwort erhalten sollen. Beginnen Sie mit der Eingabe zum Suchen. Nur **öffentliche** Kontakte und Gruppen können hier ausgewählt werden.

Wenn eingehender SMS-Text enthält Aktivieren Sie diese Option und geben Sie den zu suchenden Ausdruck ein, beispielsweise `PRICE`. Der Ausdruck kann überall im Nachrichtentext vorkommen. Aktivieren Sie **Case sensitive**, wenn `price` und `PRICE` unterschiedlich behandelt werden sollen.

Schreiben Sie die Antwort

Autoreply-Nachricht Der Text, der zurückgesendet wird. Maximal 2000 Zeichen. Derselbe Text wird an alle gesendet, die diese Regel auslösen. Halten Sie ihn daher allgemein.

Als Unicode versenden Aktivieren Sie diese Option, wenn die Antwort Zeichen außerhalb des Standard-GSM-Alphabets enthält, wie polnische, deutsche oder kyrillische Buchstaben. Unicode-Nachrichten passen weniger Zeichen pro SMS-Teil.

Klicken Sie auf **Save**. Die Regel wird sofort auf neu empfangene Nachrichten angewendet.

Schritt 3: Sendegrenze festlegen

Das Feld **Autoreply-Optionen** auf der rechten Seite der Seite steuert, wie oft das Gerät bereit ist, dieselbe Telefonnummer automatisch zu beantworten:

Option	Ergebnis
Immer automatische Antworten versenden	Jede übereinstimmende Nachricht erhält eine Antwort, egal wie viele ankommen.
Versand auf maximal 5 Nachrichten / 10 Minuten / Telefonnummer begrenzen	Höchstens 5 automatische Antworten gehen innerhalb von 10 Minuten an dieselbe Telefonnummer. Weitere Nachrichten von dieser Nummer werden nicht beantwortet, bis das Zeitfenster verstrichen ist.

Wählen Sie die gewünschte Option und klicken Sie auf **Save**.

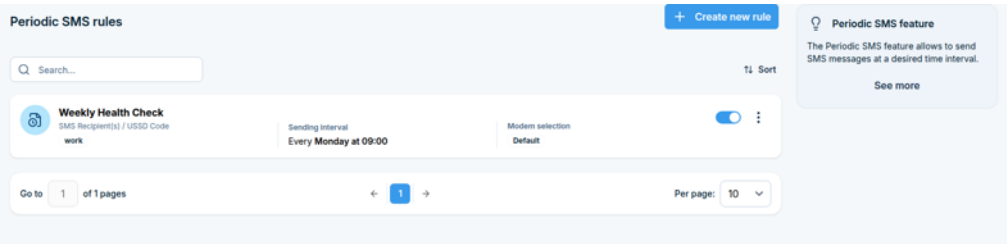
> **Es wird dringend empfohlen, die Begrenzung zu verwenden.** Ohne diese können zwei Geräte, die beide automatisch antworten, sich gegenseitig in einer Schleife beantworten, was SMS-Guthaben schnell aufbraucht. Die Begrenzung ist der Schutz dagegen.

Diese Einstellung ist **global**. Sie gilt für alle Autoreply-Regeln auf dem Gerät.

Wie Matching funktioniert

- Die Textbedingung ist ein **enthält**-Match, kein exakter Match. Eine Regel, die nach `PRICE` sucht, beantwortet eine Nachricht mit `what is the PRICE of item 5`.
- Wenn mehrere Regeln auf dieselbe eingehende Nachricht zutreffen, sendet **jede** von ihnen ihre eigene Antwort, sodass der Absender mehr als eine SMS erhalten kann. Halten Sie die Bedingungen unterschiedlich, wenn Sie nur eine Antwort möchten.
- Regeln gelten nur für Nachrichten, die nach der Erstellung und Aktivierung der Regel eingehen. Sie verarbeiten keine bereits im Posteingang vorhandenen Nachrichten.

Periodische SMS



Dialog für periodische SMS-Regel hinzufügen

Was diese Funktion bewirkt

Periodische SMS sendet eine Nachricht **automatisch nach einem wiederholten Plan**, ohne dass jemand auf Senden klicken muss. Sie erstellen eine Regel einmal, und SMSEagle sendet sie weiterhin jede Stunde, jeden Tag, jede Woche, jeden Monat oder jedes Jahr.

Sie können zwei Dinge planen:

- eine **SMS** an Telefonnummern oder an eine Phonebook-Gruppe, optional gefolgt von einem Telefonanruf,
- einen **USSD-Code**, der an Ihren Mobilfunkanbieter gesendet wird (um beispielsweise das Prepaid-Guthaben der SIM-Karte zu überprüfen).

Typische Anwendungen: eine tägliche „System aktiv“-Nachricht, eine wöchentliche Erinnerung an ein Schichtteam, eine monatliche Guthabenprüfung auf einer Prepaid-SIM.

Bevor Sie beginnen

- Wenn Sie an eine Gruppe versenden möchten, muss die Gruppe in **Phonebook > Groups** vorhanden sein und als **Public** gekennzeichnet sein. Private Gruppen können hier nicht ausgewählt werden.
- Stellen Sie sicher, dass die Geräteuhr und die Zeitzone korrekt sind, da der Plan der Gerätezeit folgt. Überprüfen Sie dies in **Settings > Date/Time**.

Schritt 1: Öffnen Sie die Seite Periodische SMS

Gehen Sie in der Seitenleiste zu **Automation > SMS > Periodic SMS**. Sie sehen die Liste der Regeln, die Sie bereits haben.

Schritt 2: Eine Regel erstellen

Klicken Sie oben rechts auf **Create new rule**. Ein Seitenpanel wird geöffnet.

Benennen Sie die Regel

Geben Sie unter **Rule name** etwas ein, das Sie später erkennen werden, beispielsweise `Daily heartbeat` oder `Monthly SIM balance`. Maximal 100 Zeichen.

Den Zeitplan festlegen

Wählen Sie ein **Sendungsintervall**. Die Felder unterhalb des Selektors ändern sich je nach Ihrer Auswahl:

Intervall	Was Sie einstellen	Beispiel
Stündlich	**Bei Minute** (in 5-Minuten-Schritten)	`15` sendet um 00:15, 01:15, 02:15 usw.
Täglich	**Um Zeit**	`07:30` sendet jeden Morgen um 07:30
Wöchentlich	**Am Wochentag** und **Um Zeit**	`Monday` + `08:00` sendet jeden Montagmorgen
Monatlich	**Am Tag des Monats** und **Um Zeit**	`1` + `09:00` sendet am ersten Tag eines jeden Monats
Jährlich	**Am Monat - Tag** (Format `mm-dd`) und **Um Zeit**	`12-24` + `10:00` sendet jeden 24. Dezember

> **Tage, die nicht existieren:** Wenn Sie etwas für den 31. Tag eines jeden Monats einplanen, wird es in kürzeren Monaten nicht gesendet. Verwenden Sie den 28. Tag oder früher, wenn die Nachricht jeden Monat gesendet werden muss.

Wählen Sie aus, was gesendet werden soll

Verwenden Sie den **Message type** Schalter oben in diesem Abschnitt:

Option A: SMS

1. Geben Sie den Text in **SMS Text** ein (maximal 2000 Zeichen).
2. Aktivieren Sie **Send as Unicode**, wenn der Text Zeichen außerhalb des Standard-GSM-Alphabets enthält, z. B. polnische, deutsche oder kyrillische Buchstaben. Beachten Sie, dass Unicode-Nachrichten weniger Zeichen pro SMS-Teil fassen.
3. Wählen Sie unter **Send to** aus, wohin die Nachricht gesendet wird:
   - **Public groups** - geben Sie einen Gruppennamen ein und wählen Sie ihn aus der Liste. Sie können mehrere Gruppen hinzufügen.
   - **Input manually** - geben Sie die Telefonnummern ein. Trennen Sie mehrere Nummern durch Kommas, z. B. `+48111222333,+48444555666`.

   Sie müssen eines von beiden ausfüllen, sonst kann die Regel nicht gespeichert werden.

Option B: USSD-Code

Geben Sie den Code in **USSD-Code** ein, z. B. `*100#`. Die Antwort des Betreibers kommt als eingehende Nachricht in Ihren Posteingang.

> USSD-Codes werden über das Modem an Ihren Mobilfunkbetreiber gesendet. Die verfügbaren Codes hängen vom Betreiber ab, nicht von SMSEagle.

Fügen Sie optional einen Sprachanruf hinzu

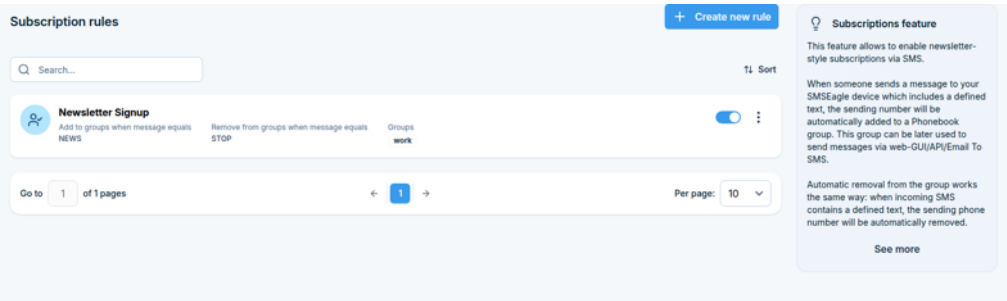
Anruf nach SMS-Versand veranlasst das Gerät auch, einen Sprachanruf an dieselben Empfänger zu tätigen, was für Benachrichtigungen nützlich ist, die nicht übersehen werden dürfen. Die verfügbaren Optionen hängen von Ihrem Gerätemodell ab:

Option	Was passiert
No	Es wird kein Anruf getätigt. Dies ist die Standardeinstellung.
Nur klingeln	Das Gerät ruft den Empfänger an und legt auf. Es wird keine Audioausgabe wiedergegeben.
Ja – Sprachausgabe	Das Gerät ruft an und liest den Nachrichtentext vor.
Ja – Sprachausgabe (erweitert)	Dasselbe wie oben, mit einer auswählbaren, natürlicheren Stimme. Wählen Sie die Stimme im Feld **Voice model** aus, das angezeigt wird.

Wenn Ihr Gerät keine Sprachanrufe unterstützt, ist nur **Nein** verfügbar.

Klicken Sie auf **Save**. Die Regel wird in der Liste angezeigt und beginnt zu ihrer nächsten geplanten Zeit auszuführen.

Abos



Abonnementregeln

Was diese Funktion bewirkt

Abos ermöglichen es Personen, **sich durch Senden einer SMS zu einer Phonebook-Gruppe anzumelden oder abzumelden**, ähnlich wie eine Newsletter-Anmeldung.

Sie definieren zwei Schlüsselwörter: eines, das den Absender zu einer Gruppe hinzufügt, und eines, das sie entfernt. Wenn jemand Ihre SMSEagle-Nummer mit einem dieser Schlüsselwörter anschreibt, wird die Telefonnummer automatisch zur Gruppe hinzugefügt oder entfernt. Sie können dann über Compose, die API oder E-Mail zu SMS Nachrichten an diese Gruppe versenden.

Typische Anwendungen: eine öffentliche Benachrichtigungsliste, bei der sich Einwohner anmelden können, oder eine Benachrichtigungsliste für Schichten, der sich Mitarbeiter selbst anmelden können, ohne dass ein Administrator eingreifen muss.

Bevor Sie beginnen

Erstellen Sie die Gruppe, bei der sich Personen anmelden werden:

1. Gehen Sie zu **Phonebook > Groups**.
2. Klicken Sie auf **Add new**, geben Sie der Gruppe einen Namen und aktivieren Sie **Set as Public Group**.
3. Klicken Sie auf **Save**.

Nur **öffentliche** Gruppen können in einer Abonnementregel verwendet werden.

Sie müssen Ihren Benutzern auch mitteilen, welche Nummer sie anschreiben sollen und welches Schlüsselwort sie senden sollen. SMSEagle kündigt dies nicht automatisch an.

Schritt 1: Öffnen Sie die Abos-Seite

Gehen Sie in der Seitenleiste zu **Automation > SMS > Subscriptions**.

Schritt 2: Eine Regel erstellen

Klicken Sie auf **Create new rule** in der oberen rechten Ecke. Ein Seitenpanel öffnet sich. Füllen Sie die Felder aus:

Rule name Etwas, das Sie erkennen werden, z. B. `Flood alerts opt-in`. Maximal 100 Zeichen.

Groups Beginnen Sie mit der Eingabe und wählen Sie eine oder mehrere Gruppen. Abonnenten werden zu **allen** aufgelisteten Gruppen hinzugefügt oder daraus entfernt. Es können nur öffentliche Gruppen ausgewählt werden.

Telefonnummer zu Gruppen hinzufügen, wenn eingehende Nachricht gleich Das Schlüsselwort, das jemanden abonniert, beispielsweise `JOIN` oder `START ALERTS`. Das Schlüsselwort muss für die Abonnementregel eindeutig sein.

Remove phone number from groups, when incoming message equals Das Schlüsselwort, das jemanden abmeldet, z. B. `STOP` oder `LEAVE`.

Case sensitive Lassen Sie dies deaktiviert, damit `join`, `Join` und `JOIN` alle funktionieren. Aktivieren Sie es nur, wenn das Schlüsselwort exakt übereinstimmen muss, wie eingegeben.

Klicken Sie auf **Save**.

Wie Matching funktioniert

Dies ist das wichtigste Detail, das Sie Ihren Benutzern mitteilen müssen:

> Die gesamte eingehende Nachricht muss **exakt** das Schlüsselwort sein. Nichts anderes darf sich in der Nachricht befinden.

Schlüsselwort ist `JOIN`	Ergebnis
Benutzer schreibt `JOIN`	Abonniert
Benutzer sendet `join`	Abonniert (es sei denn, **Case sensitive** ist aktiviert)
Benutzer sendet `Please JOIN me`	Nichts passiert
Benutzer sendet `JOIN ALERTS`	Nichts passiert

Halten Sie Schlüsselwörter daher kurz und leicht zu tippen, und teilen Sie Ihren Benutzern mit, dass sie nur das Schlüsselwort senden sollen.

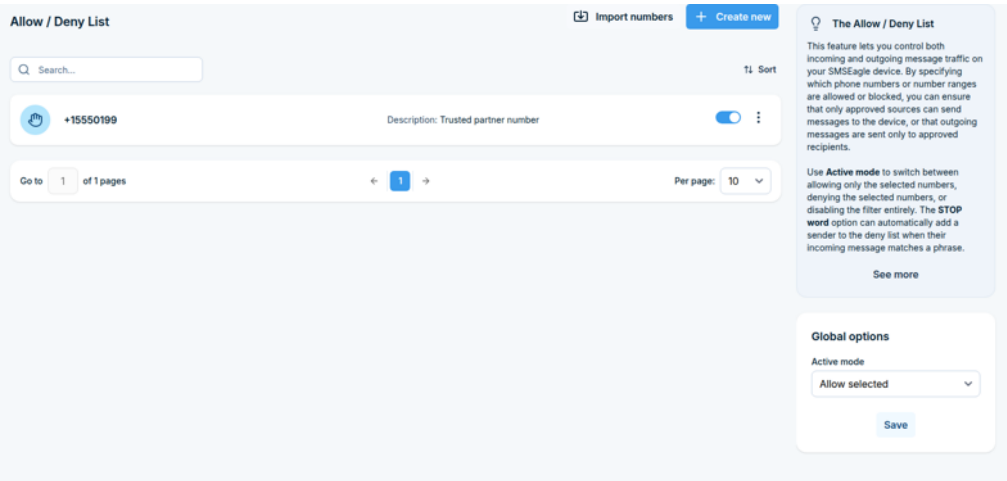
Was passiert, wenn sich jemand anmeldet

- Wenn die Telefonnummer des Absenders **bereits im Telefonbuch vorhanden** ist, wird dieser vorhandene Kontakt zur Gruppe hinzugefügt.
- Wenn die Nummer **nicht im Telefonbuch vorhanden** ist, erstellt SMSEagle automatisch einen neuen Kontakt dafür. Der Kontakt wird nach der Regel plus der Telefonnummer benannt, z. B. `Flood alerts opt-in +48111222333`, und wird als privater Kontakt erstellt.

Wenn sich jemand abmeldet, wird er aus der Gruppe entfernt, aber der Kontakt selbst bleibt im Telefonbuch erhalten.

Sie können jederzeit überprüfen, wer beigetreten ist: Gehen Sie zu **Phonebook > Groups**, suchen Sie die Gruppe und öffnen Sie **Manage contacts**.

Allow / Deny List



Globale Optionen für Allow / Deny List

Was diese Funktion bewirkt

Die Allow / Deny List filtert SMS-Verkehr auf Ihrem Gerät nach Telefonnummer.

Sie führen eine Liste mit Nummern und wählen, wie das Gerät damit umgehen soll:

Active mode	Was passiert
Allow selected	Nur die Nummern auf der Liste werden akzeptiert. Alles andere wird ignoriert.
Deny selected	Die Nummern auf der Liste werden ignoriert. Alles andere wird akzeptiert.
Disabled	Keine Filterung. Die Liste wird beibehalten, aber nicht verwendet.

Typische Anwendungsfälle: Blockieren einer Nummer, die das Gerät ständig mit Spam bombardiert (Deny), oder Sperren eines Gateways so, dass nur Ihre eigenen Alarmsysteme damit kommunizieren können (Allow).

Es gibt auch eine **STOP word**-Option, die einen Absender automatisch zur Liste hinzufügt, wenn seine Nachricht einem von Ihnen definierten Ausdruck entspricht. Das ermöglicht die Funktion eines Opt-out-Schlüsselworts wie `STOP`.

Bevor Sie beginnen

Entscheiden Sie, in welche Richtung Sie arbeiten möchten. **Allow selected** und **Deny selected** verwenden zwei separate Listen, sodass die Regeln, die Sie in einem Modus hinzufügen, nicht im anderen sichtbar sind. Das Wechseln des Modus wechselt die ganze Liste, es invertiert sie nicht.

Schritt 1: Öffnen Sie die Allow / Deny List-Seite

Gehen Sie in der Seitenleiste zu **Automation > General > Allow / Deny List**.

Auf der rechten Seite befindet sich ein **Global options**-Feld mit der **Active mode**-Einstellung und der **STOP word**-Konfiguration. Beide werden nachfolgend beschrieben.

Schritt 2: Wählen Sie den aktiven Modus

Stellen Sie im Feld **Global options** die Option **Active mode** auf **Allow selected**, **Deny selected** oder **Disabled** und klicken Sie auf **Save**. Die Seite lädt neu und zeigt die Liste, die zu dem gewählten Modus gehört.

> Solange der Modus auf **Disabled** eingestellt ist, zeigt die Seite statt der Liste einen Hinweis „Filtering is disabled“ an, und Regeln können nicht hinzugefügt oder bearbeitet werden. Wechseln Sie zu **Allow selected** oder **Deny selected**, um sie erneut zu verwalten.

Schritt 3: Eine Nummer hinzufügen

Klicken Sie auf **Create new** in der oberen rechten Ecke. Ein Seitenpanel wird geöffnet.

Phone number Die Nummer, auf die sich diese Regel bezieht. Maximal 15 Zeichen. Nur Ziffern, `+` und `*` sind zulässig, und die Eingabe muss mindestens eine Ziffer enthalten.

Sie können eine ganze Nummernreihe abdecken, indem Sie `*` als Platzhalter verwenden, der für beliebige Zeichen steht:

Muster	Stimmt überein mit
`NUMBER`	Genau diese Nummer
`*NUMBER`	Jede Nummer, die damit endet
`NUMBER*`	Jede Nummer, die damit beginnt
`*NUMBER*`	Jede Nummer, die dies enthält

Beispielsweise deckt `48512*` alle Nummern ab, die mit `48512` beginnen, und `*12345678` stimmt mit demselben Teilnehmer überein, unabhängig welches Ländervorwahl-Format ankommt.

Description Eine kurze Notiz, die erklärt, warum sich die Nummer in der Liste befindet, z. B. `Spam` oder `Alarm panel, HQ`. Erforderlich, maximal 255 Zeichen.

Klicken Sie auf **Save**.

Schritt 4: Eine Liste aus CSV importieren

Wenn Sie die Nummern bereits in einer Tabellenkalkulation haben, klicken Sie statt sie einzeln hinzuzufügen auf **Import rules** in der oberen rechten Ecke.

1. Bereiten Sie eine UTF-8-kodierte CSV-Datei mit genau zwei Spalten vor, mit den Überschriften **Number** und **Reason**.
2. Klicken Sie auf **Import rules**, ziehen Sie die Datei in den Upload-Bereich oder klicken Sie darauf zum Durchsuchen.
3. Klicken Sie auf **Import**.

Die Nummern werden zur derzeit aktiven Liste hinzugefügt.

Schritt 5: Das STOP-Wort konfigurieren (optional)

Das STOP-Wort fügt Absender automatisch zur Liste hinzu, so dass Personen sich durch das Senden eines Schlüsselworts abmelden können.

Klicken Sie im Feld **Global options** auf **Edit config** neben **STOP word**. Ein Seitenpanel wird geöffnet. Wählen Sie **Auto add number to list when**:

Option	Bedeutung
Never	Das STOP-Wort ist ausgeschaltet. Nummern werden nur manuell oder durch Import hinzugefügt.
Incoming message equals to…	Die gesamte Nachricht muss exakt der eingegebenen Phrase entsprechen.
Eingehende Nachricht enthält…	Die Phrase kann an beliebiger Stelle in der Nachricht vorkommen.

Wenn Sie eine der beiden Matching-Optionen wählen, erscheinen zwei weitere Felder:

- Die Phrase selbst, maximal 160 Zeichen, zum Beispiel `STOP`.
- **Autoreply-Nachricht**, maximal 160 Zeichen. Dieser Text wird an die Nummer zurückgesendet, nachdem sie der Liste hinzugefügt wurde. Lassen Sie dieses Feld leer, wenn Sie keine Bestätigung des Opt-out senden möchten.

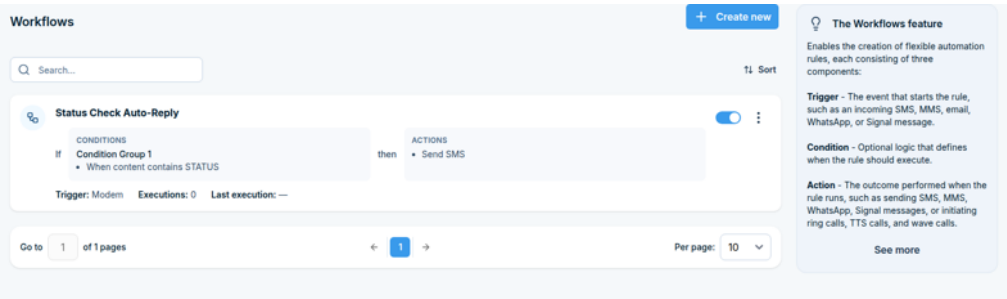
Klicken Sie auf **Save**. Die Zusammenfassung im Feld **Global options** zeigt nun die aktive Bedingung und den Autoreply-Text.

> **Verwenden Sie „equals" statt „contains" für Opt-out-Schlüsselwörter.** Mit **contains** würde eine gewöhnliche Nachricht wie `please stop sending the night reports` den Absender ebenfalls entfernen.

So funktioniert die Filterung

- Der Filter wird auf Nachrichten angewendet, die nach der Erstellung und Aktivierung der Regel eintreffen. Er verarbeitet nicht bereits im Posteingang vorhandene Nachrichten erneut.
- Eine deaktivierte Regel wird vollständig ignoriert, unabhängig davon, welcher Modus aktiv ist.
- **Allow selected** und **Deny selected** verwalten separate Listen. Wenn Sie den Modus wechseln und die Seite leer aussieht, betrachten Sie die andere Liste – nichts wurde gelöscht.
- Die STOP-Wort-Einstellung ist **global**: Sie gilt für die Liste, die derzeit aktiv ist.

Workflows



Workflows-Übersicht

Mit Workflows können Sie flexible Automatisierungsregeln erstellen, ohne dass Sie für jede Kombination von Trigger und Aktion eine separate Integration benötigen. Jeder Workflow besteht aus drei Teilen:

- **Trigger** – das Ereignis, das die Regel startet: eine eingehende SMS-, MMS-, E-Mail-, WhatsApp- oder Signal-Nachricht (oder ein Modem-Zustellungs-/Sent-/Sending-Error-Ereignis).
- **Condition** – optionale Logik, die bestimmt, ob die Regel für ein bestimmtes Ereignis ausgeführt werden soll.
- **Action** – was geschieht, wenn die Regel ausgeführt wird: Senden einer SMS-, MMS-, WhatsApp- oder Signal-Nachricht oder Initiieren eines Ring-Anrufs, TTS-Anrufs oder Wave-Anrufs.

Wo finden Sie es

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

Schritt 1: Einen Workflow erstellen und einen Trigger auswählen

Klicken Sie auf **Create new**, geben Sie dem Workflow einen **Name** und wählen Sie einen **Trigger**: Modem, Email, Signal, WhatsApp, Modem (delivered), Modem (sent) oder Modem (sending error).

Schritt 2: Bedingungsgruppen hinzufügen (optional)

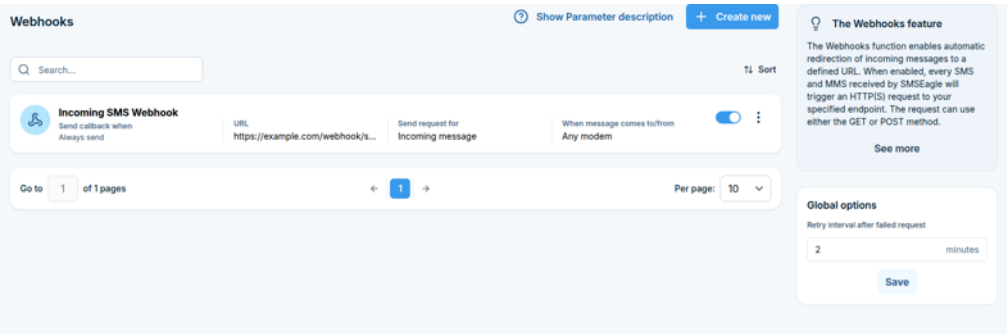
Klicken Sie unter **Condition groups** auf **Add group**, um eine oder mehrere Bedingungen hinzuzufügen, die das eingehende Ereignis erfüllen muss, bevor der Workflow ausgeführt wird. Lassen Sie dieses Feld leer, wenn der Workflow für jedes Ereignis ausgeführt werden soll, das dem Trigger entspricht.

Schritt 3: Aktionen hinzufügen

Klicken Sie unter **Actions** auf **Add action**, um festzulegen, was der Workflow bei der Ausführung tut – zum Beispiel eine Antwort senden, die Nachricht an einen anderen Kanal weiterleiten oder einen Anruf tätigen.

Klicken Sie auf **Save workflow**, um den Workflow zu aktivieren.

Webhooks



Webhooks – Übersicht

Was diese Funktion bewirkt

Ein Webhook veranlasst SMSEagle, **Ihr** System aufzurufen. Immer wenn etwas auf dem Gerät geschieht (eine Nachricht kommt an, eine Nachricht wird gesendet, ein Lieferbericht kommt zurück, ein Anruf kommt herein), sendet das Gerät eine HTTP(S)-Anfrage an eine von Ihnen gewählte URL mit den Details als Parameter.

So können Sie SMS-Datenverkehr ohne API-Abfragen in ein Ticketingsystem, ein CRM, einen Chatbot oder Ihre eigene Anwendung übertragen.

Zwei Integrationen erhalten dedizierte Unterstützung:

Methode	Wofür sie gedacht ist
POST (3CX)	Übermittlung von Nachrichten an eine 3CX-Telefonanlage.
POST (Zabbix)	Bestätigung von Zabbix-Ereignissen per SMS, damit ein Ingenieur `ACK 12345` antworten kann, um einen Alert zu schließen.

Bevor Sie beginnen

- Sie benötigen die URL, die die Anfragen empfängt und vom Gerät erreichbar ist. Lokale und private Adressen werden abgelehnt.
- Ihr Endpoint sollte mit HTTP **200 OK** oder mit den in der Regel konfigurierten Statuscodes antworten.
- Für Zabbix benötigen Sie entweder ein API-Token (Zabbix 6.4 und neuere Versionen) oder einen Benutzernamen und ein Passwort.

Schritt 1: Webhooks-Seite öffnen

Gehen Sie in der Seitenleiste zu **Automation > General > Webhooks**.

Jede Regel zeigt ihre URL und wofür sie ausgelöst wird. Jede Regel verfügt über einen Schalter zum **Aktivieren oder Deaktivieren**, eine **Edit**-Aktion und eine **Delete**-Aktion.

Das Feld **Global options** auf der rechten Seite enthält eine Einstellung, die für alle Regeln gilt und in Schritt 6 beschrieben ist.

Schritt 2: Eine Regel erstellen

Klicken Sie auf **Create new** in der oberen rechten Ecke. Das Webhook-Formular wird als vollständige Seite mit drei Abschnitten geöffnet.

Schritt 3: Grundkonfiguration

Feld	Was Sie eingeben müssen
Rule name	Ein aussagekräftiger Name, maximal 100 Zeichen.
URL	Die aufzurufende Adresse, maximal 300 Zeichen, z. B. `https://example.com/webhook`.
URL method	**GET**, **POST**, **POST (3CX)** oder **POST (Zabbix)**.
Content type	Nur für einfaches **POST**: **FormData** oder **JSON**.
To (3CX)	Nur für **POST (3CX)**: das Ziel in Ihrem 3CX-System.

Klicken Sie auf **Test connection** neben der URL, um sofort eine Beispielanfrage zu senden. Das Ergebnis wird unterhalb des Feldes angezeigt und zeigt den HTTP-Status, damit Sie bestätigen können, dass der Endpunkt funktioniert, bevor Sie speichern.

Für **GET** und **POST** wird unter den Feldern ein Beispiel der Anfrageparameter angezeigt, damit Sie genau sehen können, was Ihr Endpunkt empfängt.

Was die Anfrage enthält

Die Anfrage, die Ihr Endpunkt empfängt, enthält die Ereignisdetails als Parameter. Einige werden für jedes Ereignis gesendet, andere nur für Nachrichten oder nur für Anrufe.

Immer gesendet

Parameter	Was er enthält
`sender`	Absendernummer.
`timestamp`	Zeitpunkt, zu dem SMSEagle die Nachricht empfangen oder gesendet hat, als `YYYYmmddHHiiss`, zum Beispiel `20140531092257`.
`msgid`	Die SMSEagle-Nachrichten-ID.
`modemno`	Das Modem, auf dem die eingehende Nachricht empfangen wurde, oder das Modem, von dem die Nachricht gesendet wurde.
`apikey`	Der API-Schlüssel Ihres Dienstes, falls Sie einen in den **Security settings** eingestellt haben. Optional.

Nur für SMS und MMS gesendet

Parameter	Was er enthält
`text`	Inhalt der SMS-Nachricht.
`text_binary`	Binärer Inhalt der SMS-Nachricht.
`status`	Nachrichtenstatus.
`oid`	Wert der OID-Kennung, die einer ausgehenden Nachricht mit einer übereinstimmenden Telefonnummer zugewiesen ist. Optional.
`attachments`	MMS-Anhänge, zum Beispiel `[0 => [name => image.png, content-type => image/png, content => wfFWgwOlgBRwdWvsvs=]]`. **Nur POST**, da eine GET-Abfrageparameter keine Dateidaten übertragen kann. Optional.

Nur für eingehende Sprachanrufe gesendet

Parameter	Was er enthält
`status`	Status des eingehenden Anrufs: `accepted`, `rejected` oder `ignored`.

Eine Regel wird für einen Ereignistyp ausgelöst, daher enthält eine Anfrage nur jeweils die Parameter dieses Typs. Eine Regel mit dem Trigger **Eingehender Anruf** sendet beispielsweise niemals `text` oder `attachments`.

SMSEagle erwartet unabhängig von der Methode, dass Ihr Endpunkt mit **200 [OK]** antwortet, sofern Sie dies nicht mit **Expected HTTP Status Code(s)** in den Sicherheitseinstellungen erweitern.

Der Link **Show Parameter description** auf der Seite „rules“ öffnet diese Liste in der Anwendung zusammen mit einer GET-Beispielanfrage:

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

Parameternamen anpassen

Standardmäßig verwendet die Anfrage die oben aufgelisteten SMSEagle-Parameternamen. Falls Ihr Endpunkt andere erwartet, aktivieren Sie **Customize parameter names** und geben Sie Ihren Namen neben jedem Parameter ein, den Sie umbenennen möchten. Alle Parameter in den drei Tabellen können umbenannt werden; die, die Sie leer lassen, behalten ihren Standardnamen.

Das Umbenennen ändert nur den Parameter **name** in der Anfrage, niemals seinen Wert oder den Zeitpunkt seiner Übermittlung.

Schritt 4: Triggerbedingungen

Send request for bestimmt, welches Ereignis den Webhook auslöst:

Option	Wird ausgelöst, wenn
Incoming message	Eine SMS oder MMS kommt an.
Sent message	Eine ausgehende Nachricht wurde versendet.
Delivery report	Ein Zustellbericht kommt zurück.
Sending error	Eine ausgehende Nachricht ist fehlgeschlagen.
Incoming call	Ein Anruf kommt ein.

Send request when grenzt dies weiter ein:

Option	Bedeutung
Always	Jedes Ereignis des gewählten Typs löst den Webhook aus.
For specified senders / when text contains	Nur Ereignisse, die die folgenden Bedingungen erfüllen, lösen ihn aus.

Wenn Sie die zweite Option gewählt haben, stehen zwei Bedingungen zur Verfügung. Sie können eine oder beide verwenden, und ein Ereignis muss alle aktivierten Bedingungen erfüllen.

When incoming SMS comes from Aktivieren Sie dies und wählen Sie die Kontakte oder Gruppen. Es werden nur öffentliche Kontakte und Gruppen akzeptiert.

When incoming SMS text contains Aktivieren Sie dies und geben Sie die Phrase ein. Aktivieren Sie **Case sensitive**, wenn Groß- und Kleinschreibung unterschiedlich behandelt werden sollen. Diese Bedingung ist für den Trigger **Incoming call** nicht verfügbar, da ein Anruf keinen Text hat.

Schritt 5: Sicherheitseinstellungen

Feld	Zweck
API key of your service	Ein optionaler Schlüssel, der mit der Anfrage gesendet wird, damit Ihr Endpunkt überprüfen kann, dass der Aufruf wirklich von Ihrem Gerät kommt.
Erwarteter HTTP-Statuscode(s)	Welche Antworten gelten als erfolgreich. Ein oder mehrere dreistellige Codes, durch Kommas getrennt, beispielsweise `200,201,202`. Standard ist `200`, maximal 20 Zeichen.
Selbstsigniertes SSL-Zertifikat zulassen	Akzeptieren Sie ein Zertifikat, das nicht von einer öffentlichen Zertifizierungsstelle signiert ist.
Peer überprüfen	Überprüfen Sie das Zertifikat des Servers.
Peer-Namen überprüfen	Überprüfen Sie, ob das Zertifikat dem Hostnamen entspricht.

Alles, was nicht den erwarteten Statuscodes entspricht, gilt als fehlgeschlagene Anfrage und wird gemäß dem globalen Wiederholungsintervall erneut versucht.

Zabbix-Regeln

Wenn Sie **POST (Zabbix)** als Methode gewählt haben, werden zusätzliche Felder angezeigt:

- **Zabbix-Aktion** - **Acknowledge (ACK)**, **Unacknowledge (NOACK)** oder beides. Das Panel zeigt das SMS-Format an, das das Gerät erwartet, beispielsweise `ACK 12345 Problem resolved`.
- **Auth-Typ** - **API Token** (Zabbix 6.4 und neuer, empfohlen) oder **Anmeldename/Passwort** für ältere Versionen. Mit einem Token geben Sie ihn im Feld API-Schlüssel ein; bei Anmeldename geben Sie **Zabbix-Benutzername** und **Zabbix-Passwort** ein.
- **Testwerte** - eine **Event-ID** und **Nachricht**, die nur von **Verbindung testen** verwendet werden, werden niemals gespeichert.

Klicken Sie auf **Webhook speichern**.

Schritt 6: Wiederholungsintervall festlegen

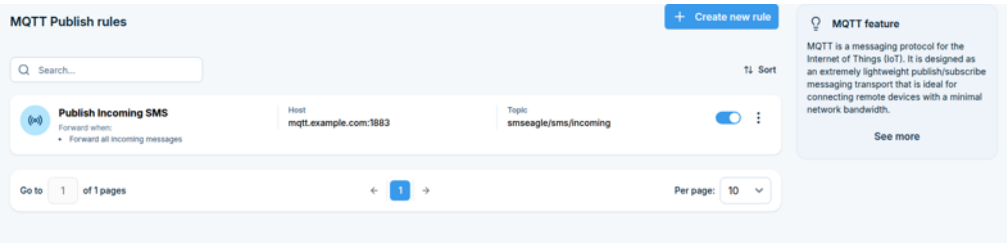
Das Feld **Globale Optionen** auf der Regelseite enthält **Wiederholungsintervall nach fehlgeschlagener Anfrage** in Minuten. Wenn eine Anfrage fehlschlägt, wartet das Gerät diese Zeit lang, bevor es erneut versucht.

Geben Sie eine ganze Anzahl von Minuten ein und klicken Sie auf **Speichern**. Die Einstellung ist **global**: Sie gilt für alle Webhook-Regeln auf dem Gerät.

Verhalten von Webhooks

- Regeln gelten für Ereignisse, die nach dem Erstellen und Aktivieren der Regel auftreten. Sie spielen keine Nachrichten der Vergangenheit ab.
- Die Textbedingung ist eine **enthält**-Abfrage, keine genaue Übereinstimmung.
- Wenn mehrere Regeln auf dasselbe Ereignis zutreffen, sendet **jede** von ihnen ihre eigene Anfrage, sodass eine Nachricht mehrere Endpunkte erreichen kann.
- Eine Anfrage gilt nur dann als erfolgreich, wenn der Antwortstatus einer der **Erwarteten HTTP-Statuscodes** ist. Alles andere, einschließlich gar keiner Antwort, ist ein Fehler und wird wiederholt.
- **Verbindung testen** sendet ein Beispiel-Payload, keine echte Nachricht, daher kann es sicher gegen einen Produktionsendpunkt ausgeführt werden, der nur protokolliert.

MQTT



MQTT Publish-Regeln

Was diese Funktion bewirkt

MQTT ist das Nachrichtenprotokoll, das von den meisten IoT-Geräten, Sensoren und Gebäudeautomationssystemen verwendet wird. Geräte senden kurze Nachrichten an einen **Broker**, die jeweils mit einem **Thema** wie `building/boiler/temperature` versehen sind. Jeder, der mit dem Broker verbunden ist, kann die Themen überwachen, die ihn interessieren.

SMSEagle sitzt auf beiden Seiten dieser Konversation:

Regeltyp	Richtung	Zweck
Abonnieren	MQTT in SMS	Überwacht einen Broker und konvertiert eingehende MQTT-Meldungen in SMS-Nachrichten, die an Ihre Benutzer versendet werden.
Veröffentlichen	SMS in MQTT	Nimmt eingehende SMS-Nachrichten auf und veröffentlicht sie auf einem Broker, damit Ihr IoT-System darauf reagieren kann.

Typische Anwendungsfälle: Umwandlung einer Sensor-Alarmmeldung in eine SMS an das Wartungsteam (Abonnieren) oder Ermöglichung einer Textnachricht eines Technikers, die vom Automatisierungssystem erfasst wird (Veröffentlichen).

Die beiden Regeltypen werden separat konfiguriert und sind voneinander unabhängig. Verwenden Sie den für Sie benötigten Typ.

Bevor Sie beginnen

Sie benötigen die Verbindungsdetails Ihres MQTT-Brokers: Hostadresse, Port und einen Benutzernamen und ein Passwort, falls der Broker diese erfordert – einmalig konfiguriert unter MQTT in Einstellungen, bevor Sie hier Abonnieren-Regeln schreiben.

Für **Abonnieren**-Regeln benötigen Sie auch die Liste der zu überwachenden Themen (ebenfalls in Einstellungen definiert). Für **Veröffentlichen**-Regeln benötigen Sie das Thema, in das veröffentlicht wird (pro Regel festgelegt, unten).

Teil 1: Abonnieren (MQTT in SMS)

Abonnieren-Regeln konvertieren eingehende MQTT-Meldungen in SMS, sobald die Broker-Verbindung selbst unter Einstellungen konfiguriert ist.

Schritt 1: Öffnen Sie die Seite der Abonnieren-Regeln

Gehen Sie in der Seitenleiste zu **Automation > Allgemein > MQTT** und wählen Sie **Abonnieren**.

Schritt 2: Erstellen Sie eine Abonnieren-Regel

Klicken Sie oben rechts auf **Create new rule**. Ein Seitenpanel wird geöffnet.

Benennen Sie die Regel

Geben Sie in **Rule name** einen aussagekräftigen Namen ein, z. B. `Boiler alarm to maintenance`. Maximum 100 Zeichen.

Entscheiden Sie, auf welche MQTT-Meldungen reagiert werden soll

Wählen Sie **Forward for**:

Option	Bedeutung
Any message	Jede MQTT-Meldung, die das Gerät empfängt, löst diese Regel aus.
Specified topic / message	Nur Meldungen, die den unten festgelegten Bedingungen entsprechen, lösen die Regel aus.

Wenn Sie **Specified topic / message** gewählt haben, stehen zwei Bedingungen zur Verfügung. Sie können eine oder beide verwenden. Wenn Sie beide verwenden, muss eine Meldung **beide** erfüllen.

When incoming message has topic Aktivieren Sie dies und geben Sie das Thema in **Topic** ein, z. B. `building/boiler`.

When incoming message contains Aktivieren Sie dies und geben Sie den Ausdruck in **Message phrase** ein, z. B. `ALARM`. Aktivieren Sie **Case sensitive**, wenn `alarm` und `ALARM` als unterschiedlich behandelt werden sollen.

Wählen Sie die Empfänger

Wählen Sie in **Forward to** die Kontakte oder Gruppen aus, die die SMS erhalten sollen. Nur **öffentliche** Kontakte und Gruppen können hier ausgewählt werden. Dieses Feld ist erforderlich.

Schreiben Sie den SMS-Text

Message format bestimmt, was die SMS aussagt. Sie erstellen ihn aus der MQTT-Meldung mit Platzhaltern:

Platzhalter	Ersetzt durch
`{TOPIC}`	Das Thema, zu dem die MQTT-Nachricht eingetroffen ist
`{MESSAGE}`	Der Inhalt der MQTT-Nachricht

Die Standardeinstellung ist `{TOPIC}: {MESSAGE}`, was eine SMS wie `building/boiler/temperature: 94` erzeugt. Sie können auch einen eigenen Satz um diese Elemente herum schreiben, z. B. `Boiler warning on {TOPIC}, value {MESSAGE}`.

Aktivieren Sie **Send as Unicode**, wenn der Text Zeichen außerhalb des Standard-GSM-Alphabets enthält, wie polnische, deutsche oder kyrillische Buchstaben.

Erweiterte Optionen

Klicken Sie auf **Advanced options**, um diesen Bereich zu erweitern. Sie benötigen diese Funktion nicht für ein einfaches Setup.

- **Call after sending SMS** – platziert auch einen Sprachanruf zu denselben Empfängern. Die Optionen sind **No**, **Ring only**, **Yes - text to speech** und **Yes - text to speech (advanced)**, je nach Modell Ihres Geräts. Mit der erweiterten Option wählen Sie auch ein **Voice model**.

Klicken Sie auf **Save**. Die Regel beginnt ab sofort mit MQTT-Nachrichten zu arbeiten.

Wie die Subscribe-Zuordnung funktioniert

- Die **Topic**-Bedingung ist eine **contains**-Zuordnung und ignoriert Groß- und Kleinschreibung. Eine Regel mit dem Thema `boiler` passt auch zu `building/boiler/temperature`.
- Das Kontrollkästchen **Case sensitive** gilt nur für die Nachrichtentextphrase, niemals für das Thema.
- Wenn mehrere Subscribe-Regeln auf dieselbe MQTT-Nachricht passen, sendet **jede** von ihnen ihre eigene SMS.

Teil 2: Publish (SMS in MQTT)

Publish-Regeln verwenden **nicht** die MQTT-Diensteinstellungen unter Settings. Jede Regel hat ihre eigene Broker-Verbindung, daher können verschiedene Regeln zu verschiedenen Brokern publishen.

Schritt 1: Öffnen Sie die Seite für Publish-Regeln

Gehen Sie in der Seitenleiste zu **Automation > General > MQTT** und wählen Sie dann **Publish**.

Schritt 2: Erstellen Sie eine Publish-Regel

Klicken Sie oben rechts auf **Create new rule**. Ein Seitenpanel wird geöffnet.

Benennen Sie die Regel

Geben Sie unter **Rule name** einen aussagekräftigen Namen ein, z. B. `Technician commands to automation`. Maximal 100 Zeichen.

Entscheiden Sie, welche SMS-Nachrichten publishen sollen

Wählen Sie **Forward for**:

Option	Bedeutung
Any message	Jede eingehende SMS wird zum Broker publishen.
Specified sender / message	Nur Nachrichten, die Ihre nachstehenden Bedingungen erfüllen, werden publishen.

Wenn Sie **Specified sender / message** gewählt haben, werden die nachstehenden Bedingungen verfügbar. Sie können sie kombinieren, und eine Nachricht muss dann alle aktivierten Bedingungen erfüllen.

When incoming SMS comes from Aktivieren Sie dies und wählen Sie die Sender-Kontakte oder Gruppen aus. Nur **öffentliche** Kontakte und Gruppen können hier ausgewählt werden.

When incoming SMS text contains Aktivieren Sie dies und geben Sie die Textphrase unter **Text fragment** ein. Aktivieren Sie **Case sensitive**, wenn Groß- und Kleinschreibung unterschiedlich behandelt werden sollen.

> Das Beschränken einer Publish-Regel durch den Absender ist eine sinnvolle Vorsichtsmaßnahme. Ohne eine Absenderbedingung kann jeder, der Ihre Nummer kennt, Inhalte in Ihr IoT-System einspeisen.

Geben Sie die Broker-Verbindung ein

Füllen Sie den Broker aus, zu dem diese Regel publishen soll:

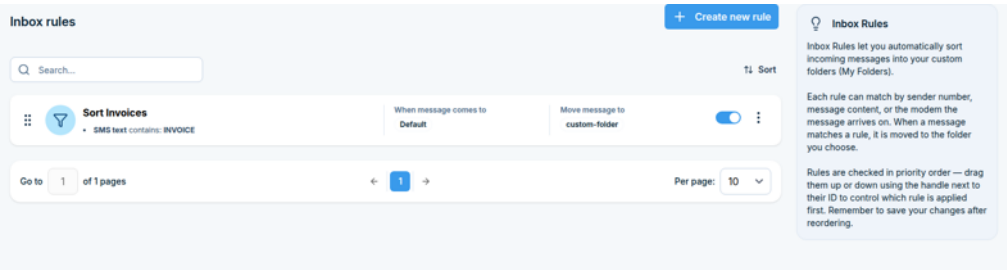
Feld	Was Sie eingeben müssen
Host	Die Broker-Adresse, z. B. `test.host.io`
Port	Der Broker-Port, zum Beispiel 1883. Der zulässige Bereich liegt zwischen 1 und 65535.
Benutzername	Der Broker-Benutzer, falls erforderlich. Lassen Sie dieses Feld leer für einen offenen Broker.
Passwort	Das Broker-Passwort, falls erforderlich.
Thema	Das Thema, in das veröffentlicht werden soll, zum Beispiel `smseagle/incoming`
TLS/SSL	Aktivieren Sie diese Option, wenn der Broker eine verschlüsselte Verbindung verwendet.
TLS-Zertifikatvalidierung	Lassen Sie diese Option aktiviert, es sei denn, der Broker verwendet ein selbstsigniertes Zertifikat, das das Gerät nicht validieren kann.

Klicken Sie auf **Save**. Eingehende SMS-Nachrichten, die der Regel entsprechen, werden ab sofort veröffentlicht.

Funktionsweise der Veröffentlichungsabstimmung

- Die Textbedingung ist eine **enthält**-Abfrage, keine genaue Übereinstimmung.
- Wenn mehrere Veröffentlichungsregeln derselben SMS entsprechen, veröffentlicht **jede** von ihnen, sodass die Nachricht auf mehreren Brokern oder Themen landen kann.
- Regeln gelten nur für Nachrichten, die nach der Erstellung und Aktivierung der Regel eingehen. Sie verarbeiten keine bereits im Posteingang vorhandenen Nachrichten.

Inbox-Regeln



Inbox-Regeln – Übersicht

Inbox-Regeln sortieren eingehende Nachrichten automatisch in Ihre benutzerdefinierten Ordner (My Folders), anstatt alles in der Hauptablage zu belassen.

Wo finden Sie es

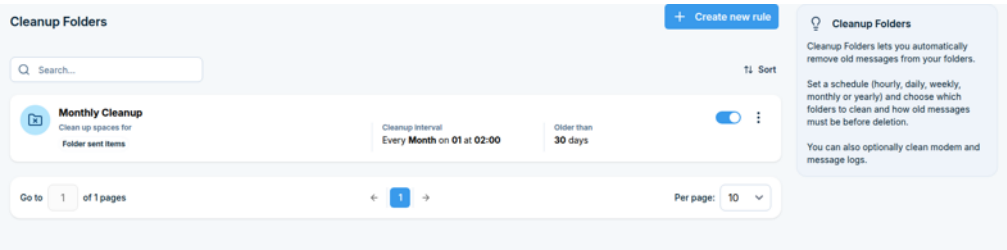
Automation > Folders > Inbox Rules (`/automation/inbox-rules/`).

Konfigurieren einer Inbox-Regel

Klicken Sie auf **Create new rule**. Jede Regel kann nach Absendernummer, Nachrichteninhalt oder dem Modem abgestimmt werden, über das die Nachricht eingegangen ist; eine Nachricht, die der Regel entspricht, wird in den von Ihnen gewählten Ordner verschoben.

Regeln werden in der Prioritätsreihenfolge überprüft. Verschieben Sie eine Regel mithilfe des Griffs neben ihrer ID nach oben oder unten, um zu steuern, welche Regel zuerst angewendet wird. Denken Sie daran, Ihre Änderungen nach dem Neuordnen zu speichern.

Ordner bereinigen



Cleanup Folders – Übersicht

Cleanup Folders entfernt alte Nachrichten automatisch aus Ihren Ordnern, damit diese sich nicht unbegrenzt ansammeln.

Wo finden Sie es

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

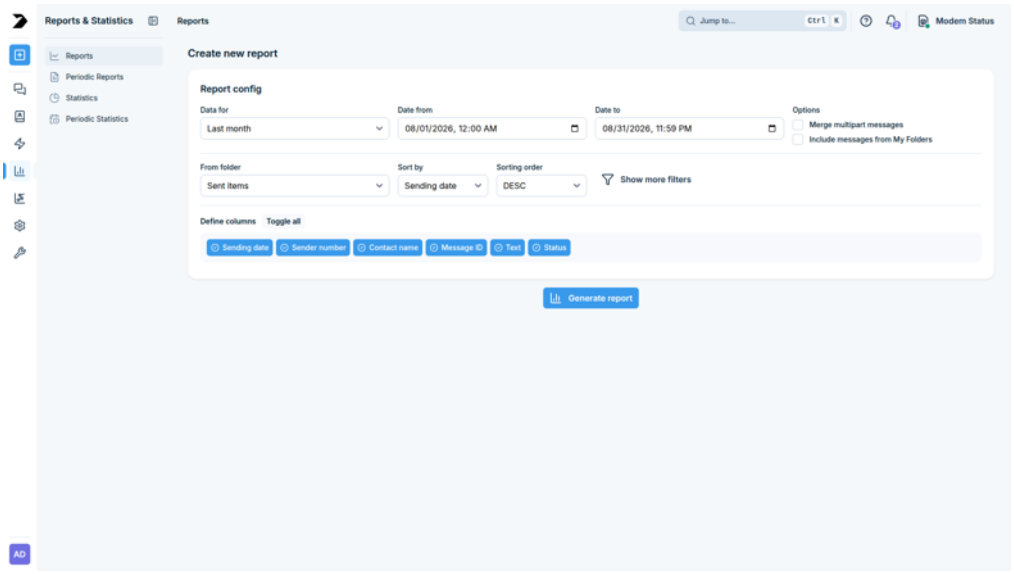
Konfigurieren einer Bereinigungsregel

Klicken Sie auf **Create new rule**, legen Sie dann einen Zeitplan fest (stündlich, täglich, wöchentlich, monatlich oder jährlich), wählen Sie aus, welche Ordner bereinigt werden sollen, und geben Sie an, wie alt eine Nachricht sein muss, bevor sie gelöscht wird. Sie können optional auch Modem- und Nachrichtenprotokolle nach dem gleichen Zeitplan bereinigen.

Berichte & Statistiken

Dieses Kapitel behandelt den Abschnitt **Berichte & Statistiken** der Weboberfläche - Exportieren von Nachrichtendaten als einmaligen Bericht oder Planen von Berichten, die automatisch per E-Mail versendet werden.

Berichte



Neuen Bericht erstellen

Berichte & Statistiken > Berichte (`/reports/`) erstellt einen einmaligen Bericht Ihres Nachrichtenverlaufs.

Wählen Sie unter **Berichtkonfiguration** den Zeitraum mit **Daten für** (ein vorgefertigter Bereich wie Heute, Letzte 7 Tage oder Dieser Monat, oder **Benutzerdefinierter Bereich** mit expliziten Feldern **Datum von** / **Datum bis**).

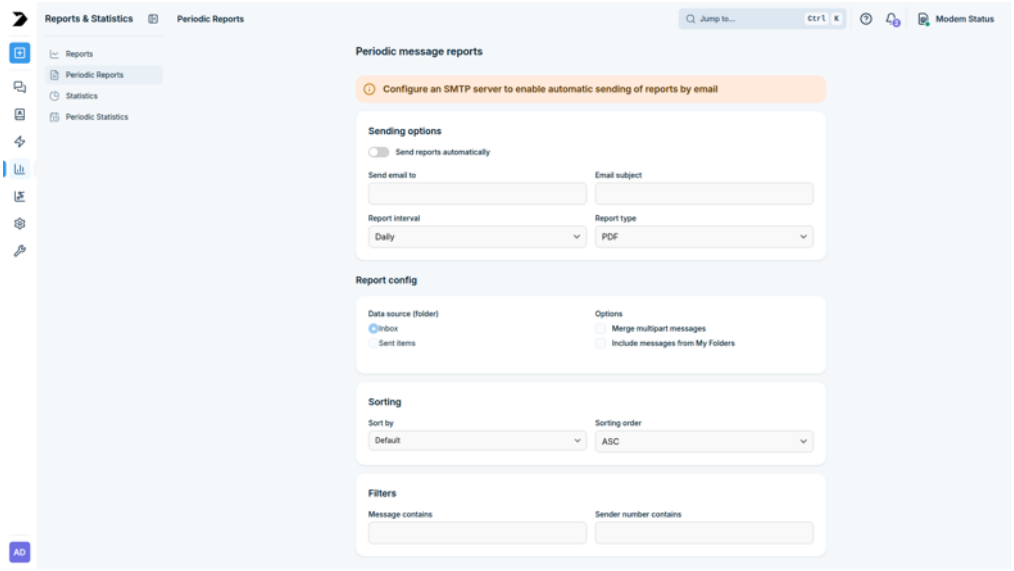
Unter **Optionen**:

Option	Funktion
Mehrteilige Nachrichten zusammenführen	Kombiniert eine lange SMS, die in mehrere Teile aufgeteilt wurde, wieder in eine Zeile.
Nachrichten aus Eigenen Ordnern einschließen	Schließt auch Nachrichten ein, die in einen benutzerdefinierten Ordner verschoben wurden.
Aus Ordner	Welcher Ordner zu melden ist: **Gesendete Elemente**, **Posteingang** oder **Postausgang**.
Sortieren nach / **Sortierreihenfolge**	Spalte zum Sortieren nach (Sendedatum, Absendernummer, Kontaktname, Nachrichten-ID, Text oder Status) und Richtung (ASC/DESC).

Klicken Sie auf **Weitere Filter anzeigen** für zusätzliche Filterung und verwenden Sie **Spalten definieren**, um auszuwählen, welche Spalten im generierten Bericht angezeigt werden - **Alle umschalten** wählt alle Spalten auf einmal aus oder hebt die Auswahl auf.

Klicken Sie auf **Bericht generieren**, um ihn zu erstellen.

Regelmäßige Berichte



Regelmäßige Nachrichtenberichte

Berichte & Statistiken > Regelmäßige Berichte (`/reports/periodic-reports`) plant die automatische Generierung und den E-Mail-Versand eines Berichts auf wiederkehrender Basis, anstatt ihn jedes Mal manuell auszuführen.

Dies erfordert eine funktionierende SMTP-Konfiguration - die Seite zeigt eine Erinnerung, eine zu konfigurieren, wenn diese fehlt.

Aktivieren Sie unter **Versendungsoptionen** die Option **Berichte automatisch versenden** und füllen Sie aus:

Feld	Funktion
E-Mail senden an	Die Empfängeradresse für den generierten Bericht.
E-Mail-Betreff	Die Betreffzeile der E-Mail.
Berichtsintervall	**Täglich**, **Wöchentlich** oder **Monatlich**.
Berichtstyp	**PDF** oder **CSV**.

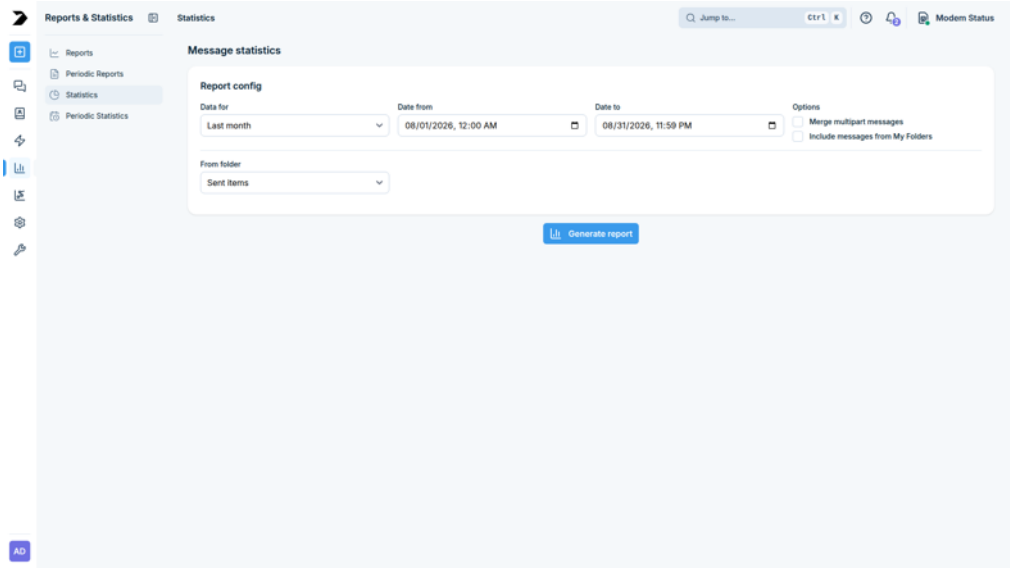
Wählen Sie unter **Report config** die **Data source (folder)** (**Inbox** oder **Sent items**), dieselben Optionen **Merge multipart messages** / **Include messages from My Folders** wie bei einem einmaligen Bericht und **Sorting** (Sortierfeld und ASC/DESC-Reihenfolge).

Grenzen Sie den Bericht unter **Filters** mit **Message contains** und/oder **Sender number contains** ein.

Wählen Sie unter **Output** mit **Select table columns** (mit einer **Toggle all**-Verknüpfung) die Spalten aus, die die generierte Datei enthält: Empfangsdatum, Absendernummer, Kontaktname, SMS Center Number, Nachrichten-ID, Text, Lesestatus und Modem-ID.

Klicken Sie auf **Save configuration**.

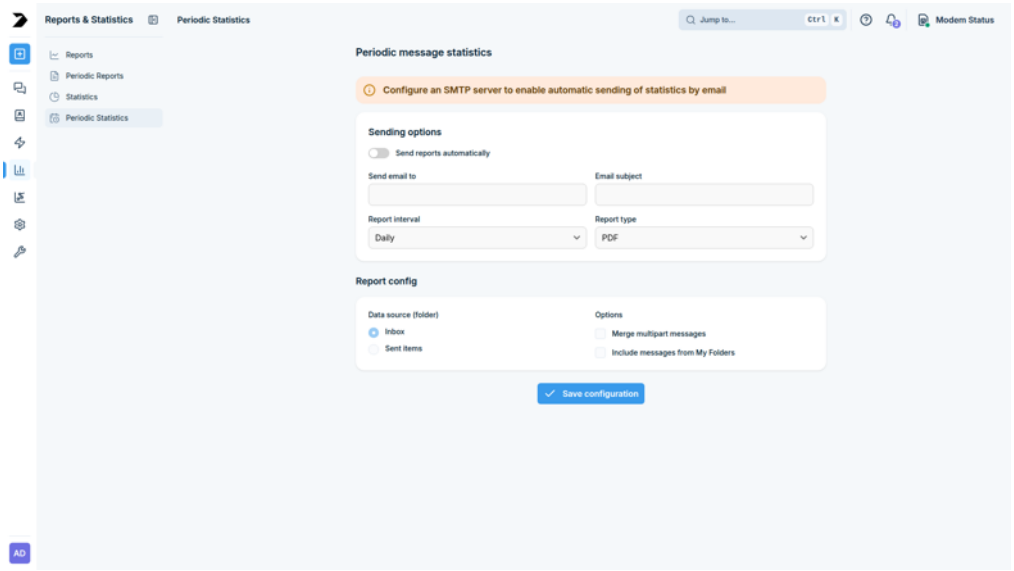
Statistiken



Nachrichtenstatistiken

Reports & Statistics > Statistics (`/reports/statistics`) funktioniert genauso wie Reports oben - mit denselben **Data for**-Zeitraum-Auswahloptionen und **Merge multipart messages** / **Include messages from My Folders** / **From folder**-Optionen - erzeugt aber aggregierte Verkehrsstatistiken anstelle eines zeilenweise sortierten Exports. Klicken Sie auf **Generate report**, um ihn zu erstellen.

Periodische Statistiken



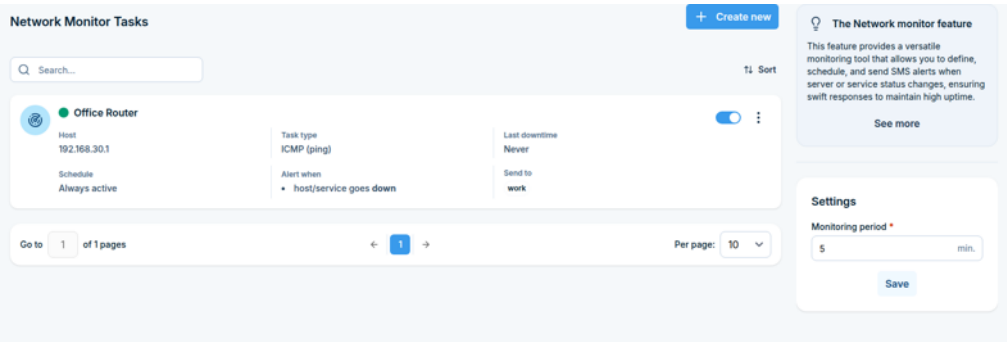
Periodische Nachrichtenstatistiken

Reports & Statistics > Periodic Statistics (`/reports/periodic-statistics`) plant die oben beschriebene Statistikabruf so ein, dass sie automatisch generiert und per E-Mail versendet wird, genauso wie Periodic Reports für den zeilenweise sortierten Export: Es ist eine funktionsfähige SMTP Configuration erforderlich, und es bietet dieselben **Sending options** (Empfänger, Betreff, **Daily / Weekly / Monthly**-Intervall, **PDF / CSV**-Berichtstyp) plus einen **Report config**-Abschnitt (Datenquellen-Folder, Merge multipart messages, Include My Folders). Klicken Sie auf **Save configuration**.

Überwachung

Dieses Kapitel behandelt den Bereich **Überwachung** der Weboberfläche: Überprüfung von externen Hosts und Services, Lesen von digitalen E/A und physikalischen Sensoren.

Netzwerküberwachung



Übersicht Netzwerküberwachung

Was diese Funktion tut

Network Monitor verwandelt Ihren SMSEagle in eine kleine Überwachungsstation. Er prüft Server, Geräte und Services nach Plan und sendet eine SMS, wenn etwas nicht mehr antwortet, wieder online geht oder einen Wert außerhalb des erwarteten Bereichs meldet.

Es hat drei Teile:

Seite	Was es tut
Aufgaben	Die Überwachungsregeln: Was zu überprüfen ist, wie oft, wen zu benachrichtigen ist.
Berichte	Eine Ausfallhistorie, gefiltert nach Datumsbereich und Aufgabe, exportierbar als CSV.
SNMP Traps	Regeln, die SNMP Traps, die an das Gerät gesendet werden, in SMS-Nachrichten umwandeln.

Typische Anwendungen: Benachrichtigung des bereitschaftshaben Ingenieurs, wenn ein Produktionsserver nicht mehr antwortet, Warnung vor einer Temperaturmessung von einem SNMP-Sensor oder Weiterleitungseines UPS-Traps an ein Telefon.

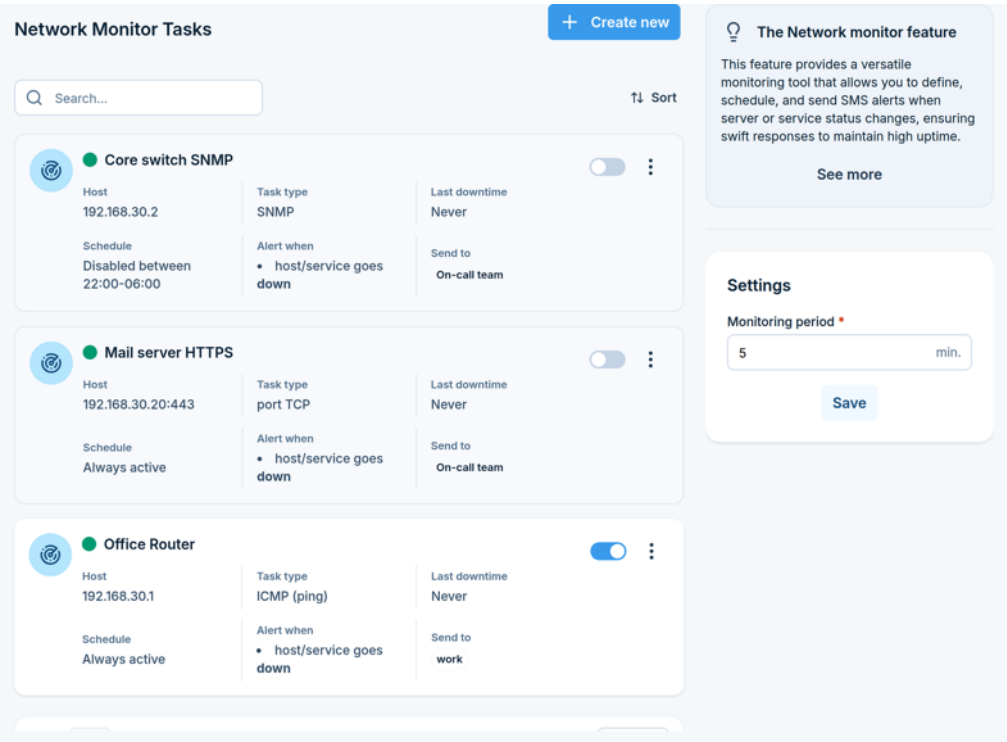
Bevor Sie beginnen

- Das Gerät muss die Hosts erreichen können, die Sie überwachen möchten. Überprüfen Sie zunächst die Netzwerkeinstellungen unter **Einstellungen > Netzwerk**.
- Empfänger müssen im Telefonbuch als **Öffentlich** gekennzeichnet sein, wenn Sie eine Gruppe benachrichtigen möchten. Andernfalls können Sie schlichte Telefonnummern in die Aufgabe eingeben.
- Für SNMP-Abfragen benötigen Sie die Community-Zeichenfolge und die Object ID (OID), die Sie lesen möchten. Für Modbus-Abfragen benötigen Sie die Unit-ID, das Register und den Funktionscode.

Teil 1: Aufgaben

Schritt 1: Öffnen Sie die Seite Aufgaben

Gehen Sie in der Seitenleiste zu **Überwachung > Netzwerküberwachung > Aufgaben**.



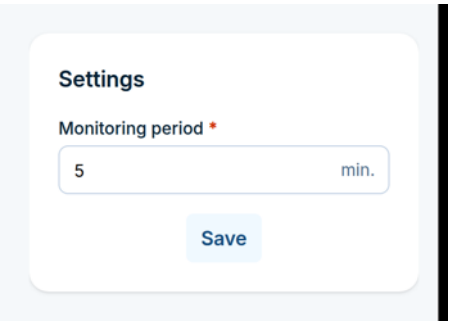
Netzwerküberwachung - Aufgaben

Jede Aufgabe in der Liste zeigt seinen Host, Plan, Aufgabentyp, worauf er aufmerksam macht, wann es zuletzt nicht verfügbar war und wen es benachrichtigt. Ein grüner oder roter Marker teilt mit, ob der Host derzeit antwortet.

Schritt 2: Stellen Sie den Überwachungszeitraum ein

Das Feld **Einstellungen** auf der rechten Seite der Seite Aufgaben enthält eine Einstellung, die auf **alle** Aufgaben anwendbar ist: **Überwachungszeitraum** in Minuten. Dies ist, wie oft das Gerät die Abfragen ausführt.

Geben Sie einen Wert ein und klicken Sie auf **Speichern**.



Überwachungsperiode

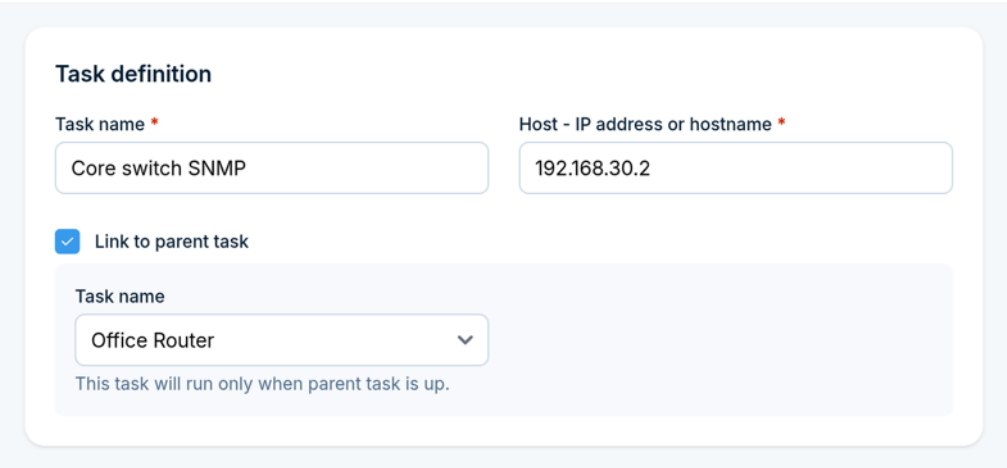
Schritt 3: Erstellen Sie eine Aufgabe

Klicken Sie auf **Create new** in der oberen rechten Ecke. Das Aufgabenformular wird als vollständige Seite angezeigt und ist in fünf Abschnitte unterteilt.

Task-Definition

Feld	Was Sie eingeben müssen
Task name	Ein aussagekräftiger Name mit maximal 100 Zeichen, z. B. `Mail server`.
Host - IP-Adresse oder Hostname	Was überprüft werden soll, z. B. `192.168.1.10` oder `mail.example.com`.
Link to parent task	Aktivieren Sie dies, um die Aufgabe von einer anderen abhängig zu machen.
Task name (parent)	Wird angezeigt, sobald das Kontrollkästchen aktiviert ist: die Aufgabe, von der diese abhängig ist.

Eine verknüpfte Aufgabe **läuft nur, während ihre übergeordnete Aufgabe aktiv ist**. Verwenden Sie dies, um Alert-Überflutungen zu vermeiden: Wenn der Router vor zehn Servern ausfällt, meldet nur die Router-Aufgabe einen Alert, und die zehn Server-Aufgaben bleiben still.



Task-Definition

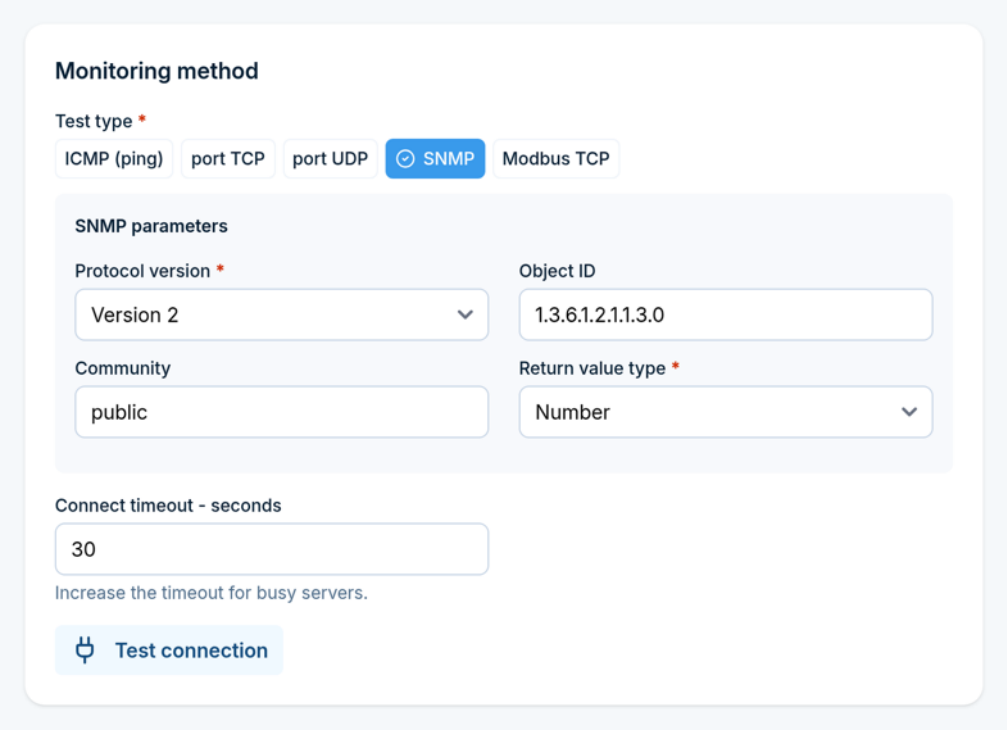
Überwachungsmethode

Wählen Sie den **Test type** und füllen Sie die Parameter ein, die dafür angezeigt werden:

Test type	Parameter
ICMP (ping)	**Number of requests** - wie viele Pings pro Überprüfung gesendet werden sollen.
port TCP	**Port** - der TCP-Port, der eine Verbindung akzeptieren muss.
port UDP	**Port** - der UDP-Port, der überprüft werden soll.
SNMP	**Protocol version** (1 oder 2), **Object ID**, **Community**, **Return value type** (Number oder String).
Modbus TCP	**Port**, **Unit ID**, **Register**, **Function code** (Read coils, Read Discrete Inputs, Read Holding Registers, Read Input Registers).

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

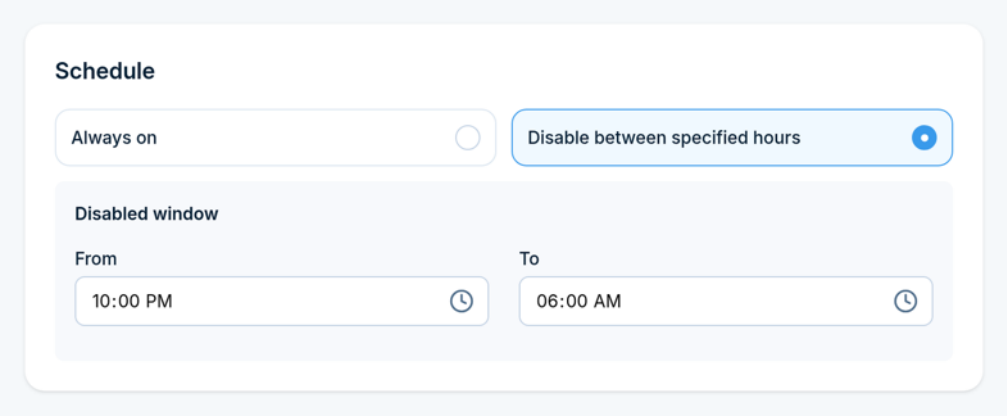
Click **Test connection** to try the check straight away. The result appears next to the button, so you can confirm the host answers before you save the task.



Überwachungsmethode

Zeitplan

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



Zeitplan

Alertauslöser

First choose who gets the alert:

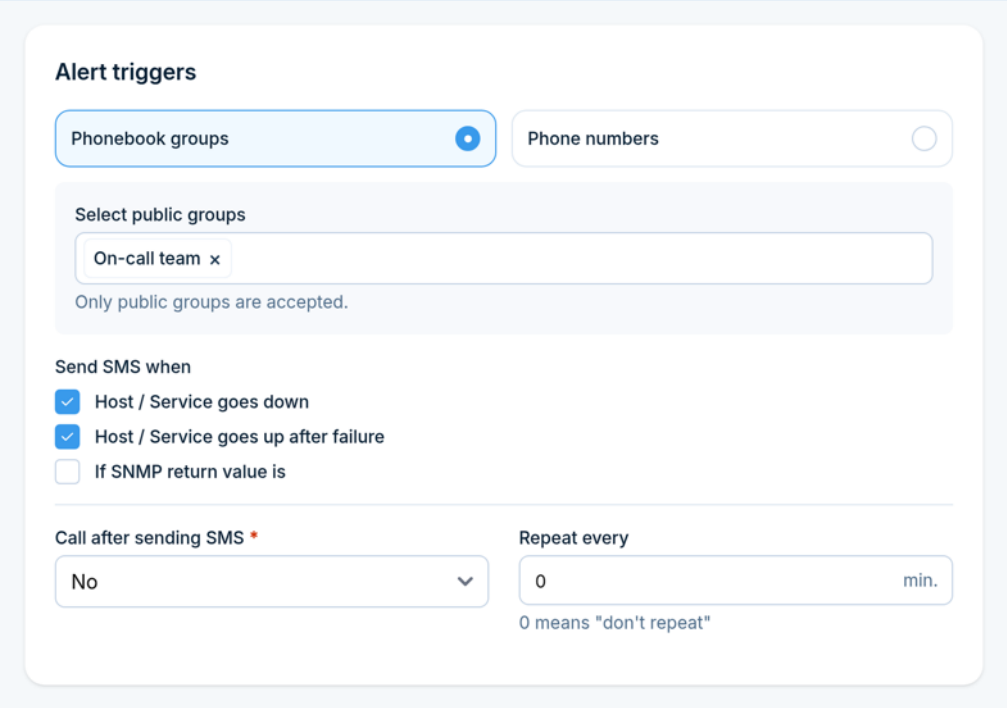
Option	Was Sie eingeben müssen
Phonebook groups	Select public groups. Only public groups are accepted.
Phone numbers	Type the numbers directly, separated by commas. Maximum 100 characters in total.

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

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

Two more settings close the section:

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



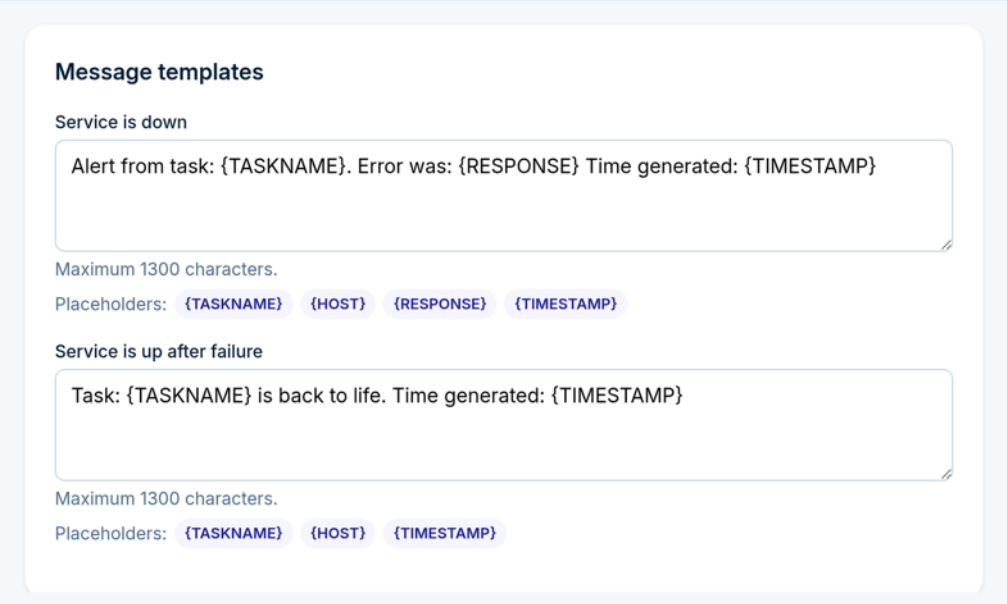
Alertauslöser

Nachrichtenvorlagen

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

Nachricht	Verfügbare Platzhalter
Service is down	`{TASKNAME}`, `{HOST}`, `{RESPONSE}`, `{TIMESTAMP}`
Service is up after failure	`{TASKNAME}`, `{HOST}`, `{TIMESTAMP}`
SMS-Text (SNMP)	`{TASKNAME}`, `{VALUE}`, `{TIMESTAMP}`
SMS-Text (Modbus)	`{TASKNAME}`, `{VALUE}`, `{TIMESTAMP}`

Zum Beispiel: `DOWN: {TASKNAME} ({HOST}) at {TIMESTAMP}` erzeugt eine Nachricht, die anzeigt, was fehlgeschlagen ist, wo und wann.



Nachrichtenvorlagen

Klicken Sie auf **Create task**. Die Aufgabe wird bei der nächsten Überwachungsrunde überprüft.

Teil 2: Berichte

Gehen Sie zu **Monitoring > Network Monitoring > Reports**.

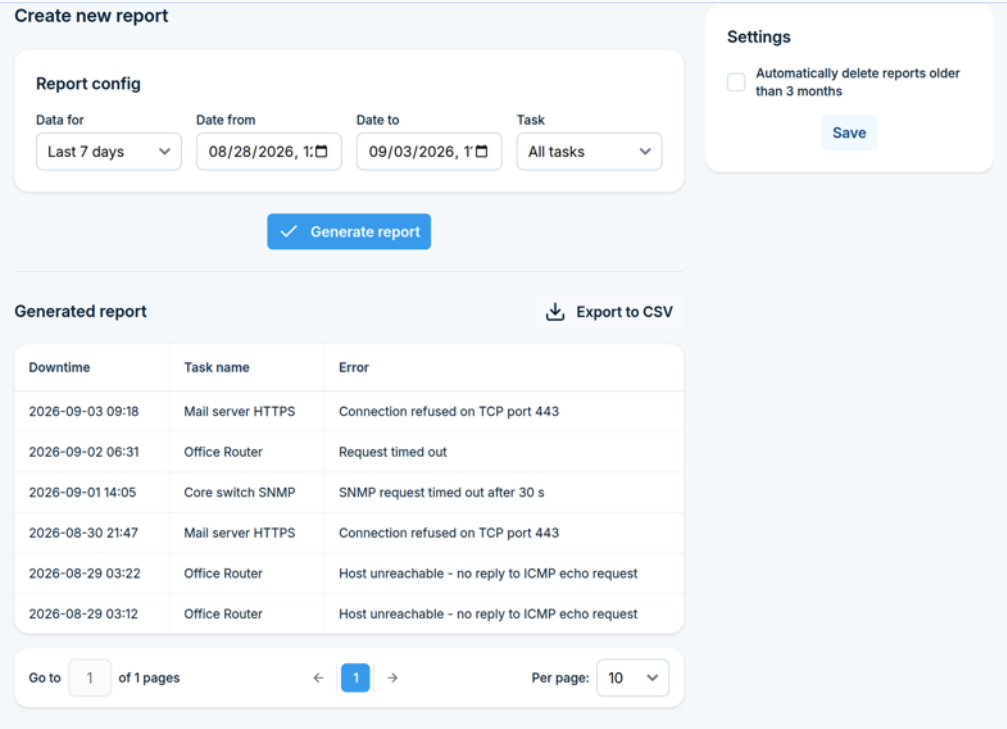
Einen Bericht generieren

Wählen Sie im Feld **Report config**:

Feld	Was es tut
Data for	Ein vordefinierter Datumsbereich. Wenn Sie einen auswählen, werden die Datumsangaben darunter automatisch ausgefüllt.
Date from / **Date to**	Der exakte Bereich. Wenn Sie diese Felder bearbeiten, wird **Data for** auf einen benutzerdefinierten Bereich umgeschaltet.
Task	Eine einzelne Aufgabe oder **All tasks**.

Klicken Sie auf **Generate report**. Die Ergebnisse werden darunter angezeigt und enthalten die Ausfallzeit, den Aufgabennamen und den Fehler, der für jeden Vorfall aufgezeichnet wurde.

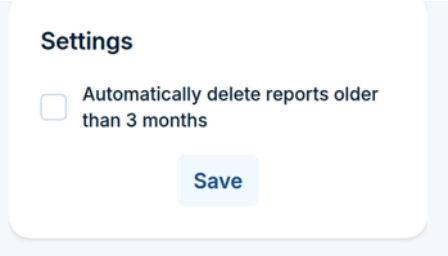
Klicken Sie auf **Export to CSV** über den Ergebnissen, um diese herunterzuladen.



mit ausgewähltem Datumsbereich und Aufgabe sowie eine generierte Ausfallzeittabelle darunter

Aufbewahrung von Berichten

Das Feld auf der rechten Seite enthält eine Option: **Automatically delete reports older than 3 months**. Aktivieren Sie diese Option, um zu verhindern, dass der Berichtsverlauf unbegrenzt wächst, und klicken Sie dann auf **Save**.



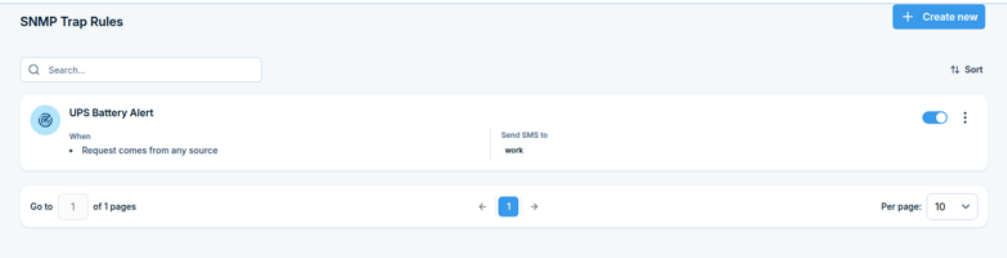
Aufbewahrung von Berichten

Teil 3: SNMP Traps

Aufgaben überprüfen proaktiv Geräte. SNMP-Trap-Regeln funktionieren umgekehrt: Ein anderes Gerät sendet einen Trap **an** die SMSEagle, und die Regel wandelt ihn in eine SMS um.

Schritt 1: SNMP-Traps-Seite öffnen

Gehen Sie zu **Monitoring > Network Monitoring > SNMP Traps**.



mit einer Beispielregel“}}] { „29“: „SNMP Trap Rules“ // ← comment: keep in English per Rule 3 (GUI element labels) }}]}}] { „29“: „SNMP Trap Rules“ // ← comment: keep in English per Rule 3 (GUI element labels) [}, „28“: „SNMP Trap Rules-Seite mit einer Beispielregel“, „29“: „SNMP Trap Rules“}

Schritt 2: Erstelle eine Regel

Klicke auf **Neue erstellen** in der oberen rechten Ecke. Ein Seitenpanel öffnet sich.

Benenne die Regel

Gib unter **Regelname** einen aussagekräftigen Text ein, beispielsweise `UPS-Batteriefalle`. Maximum 100 Zeichen.

Entscheide, welche Traps bearbeitet werden sollen

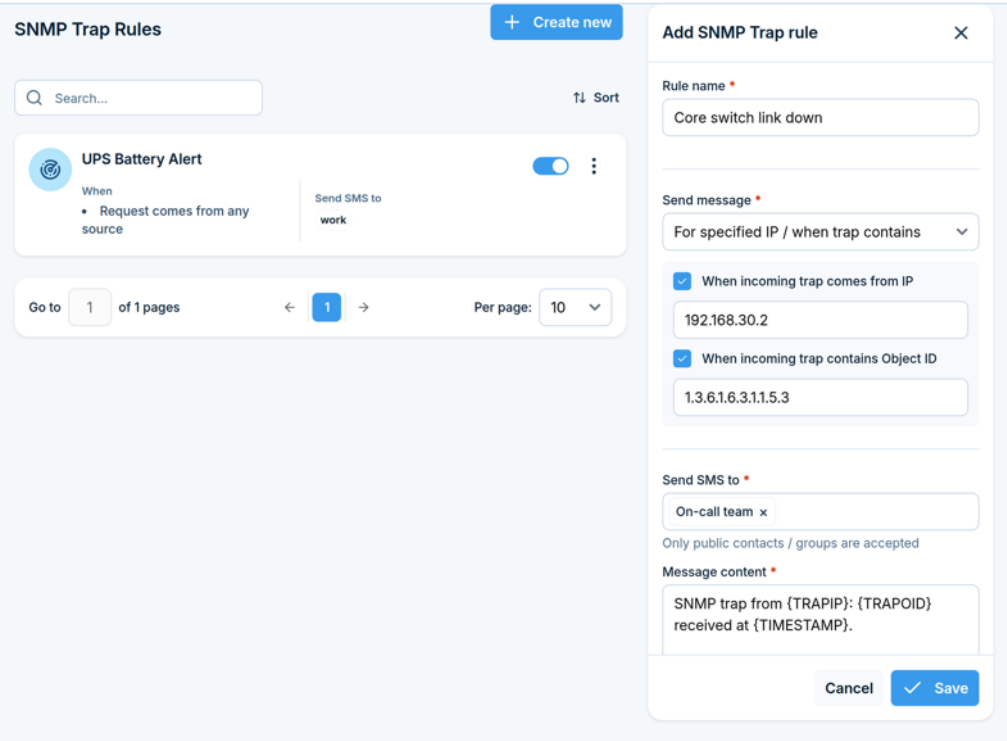
Wähle **Nachricht senden**:

Option	Was es bedeutet
Immer senden	Jeder Trap, den das Gerät empfängt, löst diese Regel aus.
Für angegebene IP / wenn Trap enthält	Nur Traps, die die Bedingungen unten erfüllen, lösen sie aus.

Wenn du die zweite Option gewählt hast, werden zwei Bedingungen verfügbar. Du kannst eine oder beide verwenden, und ein Trap muss alle aktivierten Bedingungen erfüllen.

Wenn eingehender Trap von IP kommt Aktiviere dies und gib die IP-Adresse des sendenden Geräts ein.

Wenn eingehender Trap Object ID enthält Aktiviere dies und gib die OID ein, die im Trap vorhanden sein muss.



Eine SNMP-Trap-Regel mit Bedingungen

Wähle die Empfänger und schreibe die Nachricht

SMS senden an – wähle die Kontakte oder Gruppen. Nur **öffentliche** Kontakte und Gruppen werden akzeptiert.

Nachrichteninhalt – der zu sendende Text, Maximum 1300 Zeichen. Du kannst diese Platzhalter verwenden:

Platzhalter	Ersetzt durch
`{TASKNAME}`	Der Name der Regel
`{IP}`	Die IP-Adresse, von der der Trap kam
`{TRAP}`	Der Inhalt des Traps

Optionale Einstellungen

- **Anruf nach SMS senden** – auch einen Sprachanruf durchführen, mit den gleichen Optionen wie bei Aufgaben.

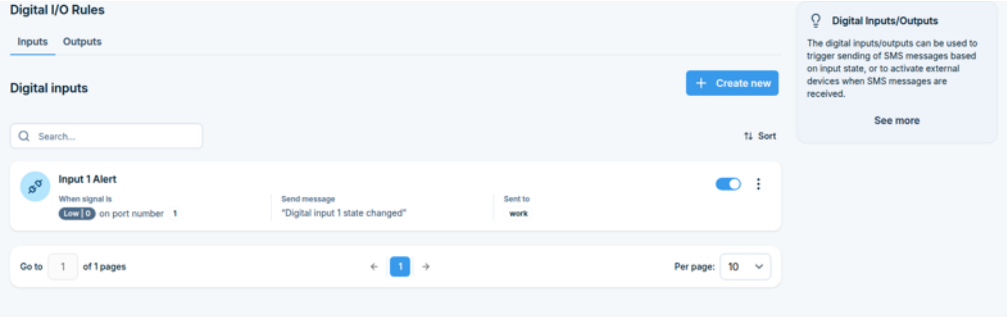
Klicke auf **Speichern**. Die Regel gilt für Traps, die ab jetzt empfangen werden.

Verhalten des Netzwerk-Monitors

- Aufgaben werden im gemeinsamen **Monitoring-Intervall** überprüft, daher kann eine Aufgabe nicht schneller als dieses Intervall erlaubt, eine Warnung auslösen.

- Eine „down“-Warnung wird einmalig gesendet, wenn sich der Zustand ändert, und wird dann nur wiederholt, wenn Sie **Repeat every** (Wiederholen alle) einstellen.
- Eine Aufgabe, die mit einer übergeordneten Aufgabe verknüpft ist, wird vollständig übersprungen, während die übergeordnete Aufgabe ausfällt, daher bleiben ihre eigenen Warnungen stillschweigend, bis die übergeordnete Aufgabe wiederhergestellt wird.
- Wenn mehrere SNMP-Trap-Regeln den gleichen Trap erfassen, sendet **jede** von ihnen eine eigene SMS.

Digitale Ein-/Ausgangsports



Übersicht Digital Input/Output

Was diese Funktion tut

Die digitalen Ein- und Ausgänge sind der physische Anschluss am Gerät, mit dem SMSEagle mit der Außenwelt außerhalb des Netzwerks kommuniziert:

Richtung	Was es tut
Eingang	Eine Spannungsänderung an einem Eingangsport (ein Türkontakt schließt sich, ein Alarm-Relais wird ausgelöst, eine USV meldet einen Fehler) veranlasst das Gerät, eine SMS zu senden.
Ausgang	Eine eingehende SMS veranlasst das Gerät, einen Ausgangsport ein- oder auszuschalten, damit es eine Sirene starten, ein Tor öffnen oder eine Maschine zurücksetzen kann.

Sie konfigurieren dies mit **Regeln**. Eine Eingangsregel besagt: „wenn Port 2 high wird, SMS an das Wartungsteam senden“. Eine Ausgangsregel besagt: „wenn eine SMS mit OPEN ankommt, stelle Port 1 für 5 Sekunden high“.

Neben den Regeln gibt es zwei Seiten, die die Ports selbst anzeigen: **Internal pins** (die in das Gerät integrierten Ports) und **External pins** (zusätzliche Ports, die durch ein io-bridge-Modul hinzugefügt werden).

Bevor Sie beginnen

- Überprüfen Sie, wie viele Ein- und Ausgangsports Ihr Gerätemodell hat, und verbinden Sie Ihre Ausrüstung damit. Die Port-Listen in den Regelformularen werden aus Ihrem Gerätemodell erstellt, daher bieten sie nur Ports an, die physisch vorhanden sind.
- Das Gerät muss in der Lage sein, SMS zu versenden. Überprüfen Sie, dass mindestens ein Modem verbunden und im Netz registriert ist.
- Empfänger von Eingabenregeln müssen im Adressbuch als **Public** (Öffentlich) gekennzeichnet sein.

Hardware: ports, logic levels and wiring

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

Number of ports

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

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

Logic levels

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

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

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

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

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

NO and NC contacts (normally open / normally closed)

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

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

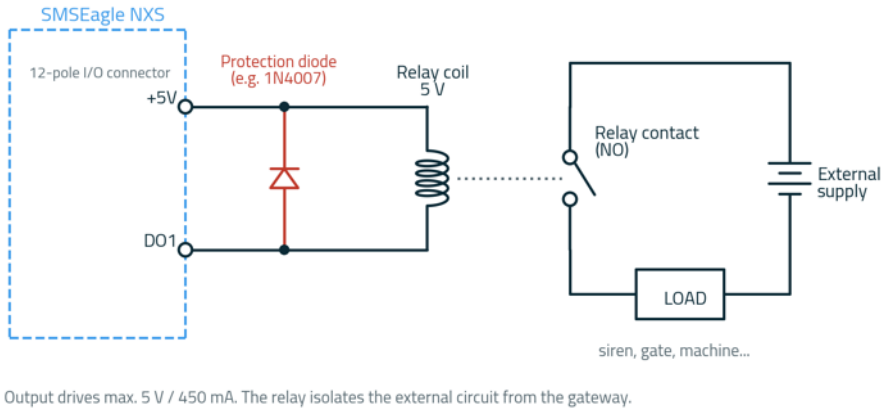
> **Prefer NC contacts for alarm circuits.** With an NC contact, a cut or disconnected cable opens the circuit in the same way as a real alarm, so a wiring fault also triggers an SMS. With an NO contact, a broken cable goes unnoticed.

Using digital outputs

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

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

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



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

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

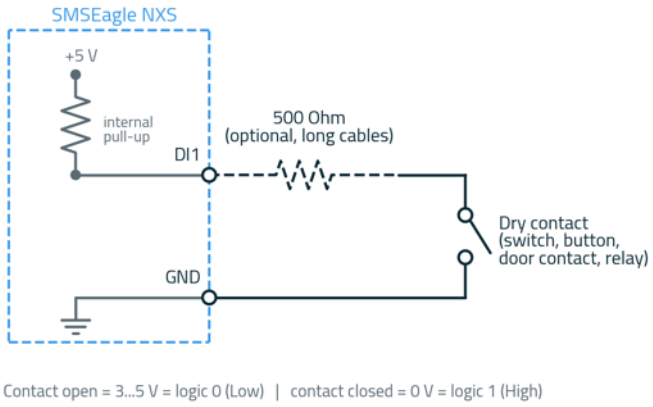
Using digital inputs

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

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

Dry contact, NO or NC (simplest connection)

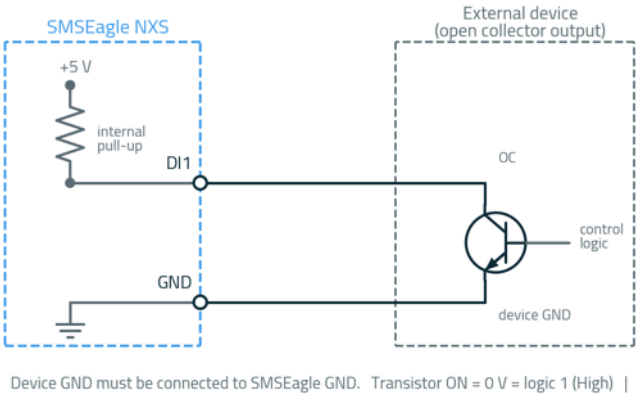
Connect a potential-free (dry) contact between the input and GND: a switch, push button, door or window contact, PIR detector output, alarm panel output or relay contact. Both **NO** (normally open) and **NC** (normally closed) contacts can be used; set **When input signal** according to the table in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



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

Device with an open collector output

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

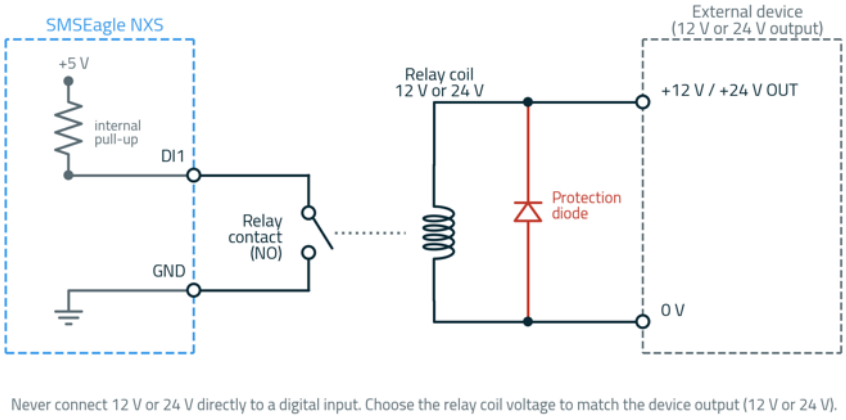


Digital input: connection with a device with an open collector output

Device with a 12 V or 24 V output

A 12 V or 24 V signal must **never** be connected directly to a digital input. Use the output of the device to drive the coil of an intermediary relay (with a protection diode), and connect the relay contact between the input and GND. Choose a relay with a coil voltage matching the output of the device: **12 V** coil for a 12 V output, **24 V** coil for a 24 V output. An optocoupler module rated for the same voltage can be used in the same way. This keeps the 12 V or 24 V circuit fully separated from the gateway.

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

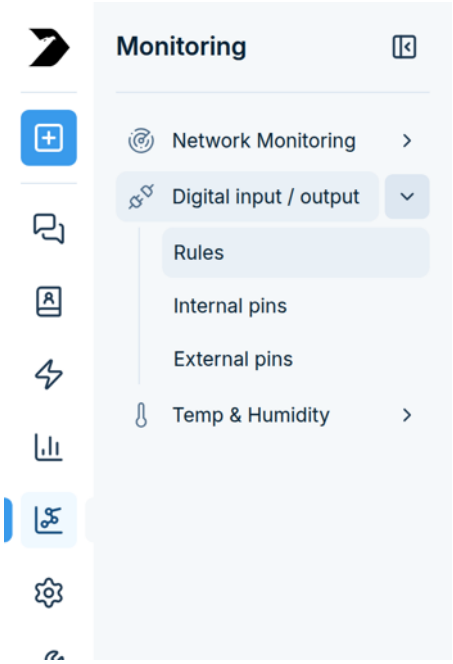


Digital input: connection with a device with a 12 V or 24 V output

Wo zu finden

Gehen Sie in der Seitenleiste zu **Monitoring > Digital input / output**. Es gibt drei Seiten:

Seite	Wofür es nützlich ist
Rules	Erstellen Sie die Eingangs- und Ausgangsregeln. Hier verbringen Sie die meiste Zeit.
Internal pins	Sehen Sie den Live-Status der integrierten Ports und schalten Sie den Service ein oder aus.
External pins	Definieren und steuern Sie zusätzliche Ports, die durch ein io-bridge-Modul bereitgestellt werden.

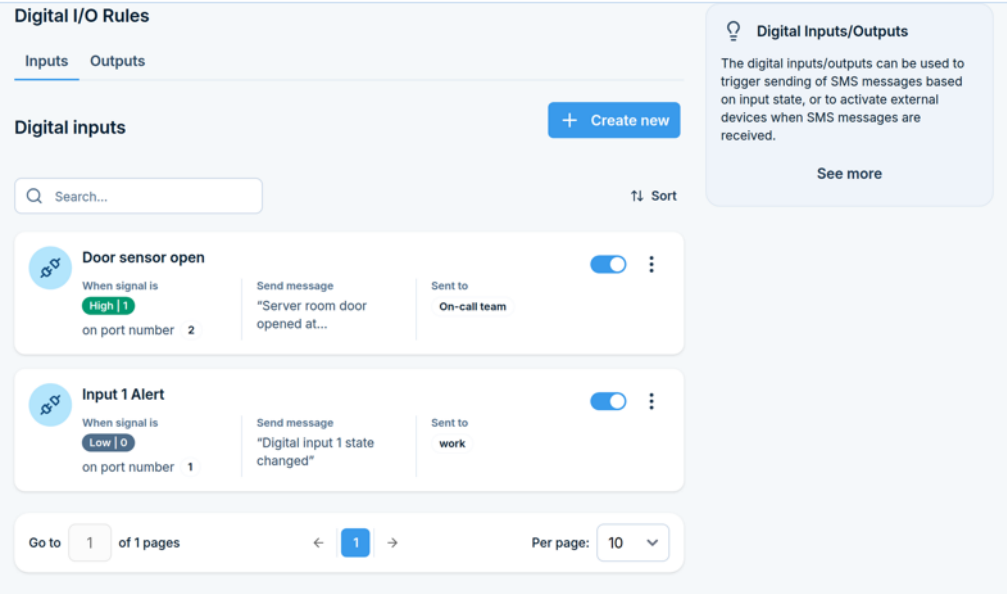


Wo die Digital-I/O-Seiten zu finden sind

Teil 1: Eingaberegeln (Eingabesignal in SMS)

Schritt 1: Öffnen Sie die Seite „Regeln“

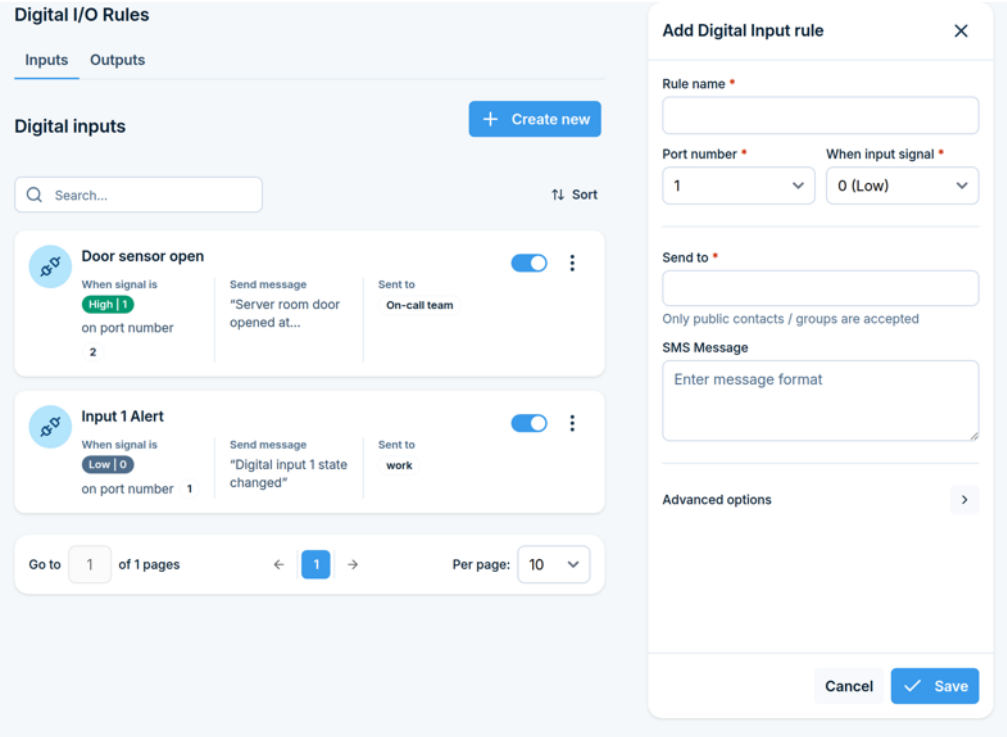
Gehen Sie zu **Monitoring > Digital input / output > Rules** und stellen Sie sicher, dass die Registerkarte **Inputs** ausgewählt ist.



Digitale Eingaberegeln

Schritt 2: Erstellen Sie eine Eingaberegel

Klicke auf **Neue erstellen** in der oberen rechten Ecke. Ein Seitenpanel öffnet sich.



Eine neue digitale Eingaberegel

Benenne die Regel

Geben Sie in **Rule name** etwas Aussagekräftiges ein, z. B. `Server room door opened`. Maximum 100 Zeichen.

Wählen Sie den Port und das Signal

Feld	Was Sie eingeben müssen
Port number	Der Eingabeanschluss, mit dem die Ausrüstung verdrahtet ist. Externe (io-bridge) Anschlüsse werden in der Liste mit `(Ext)` gekennzeichnet.
When input signal	`0 (Low)` oder `1 (High)`. Dies ist der Zustand, der die Regel auslöst.

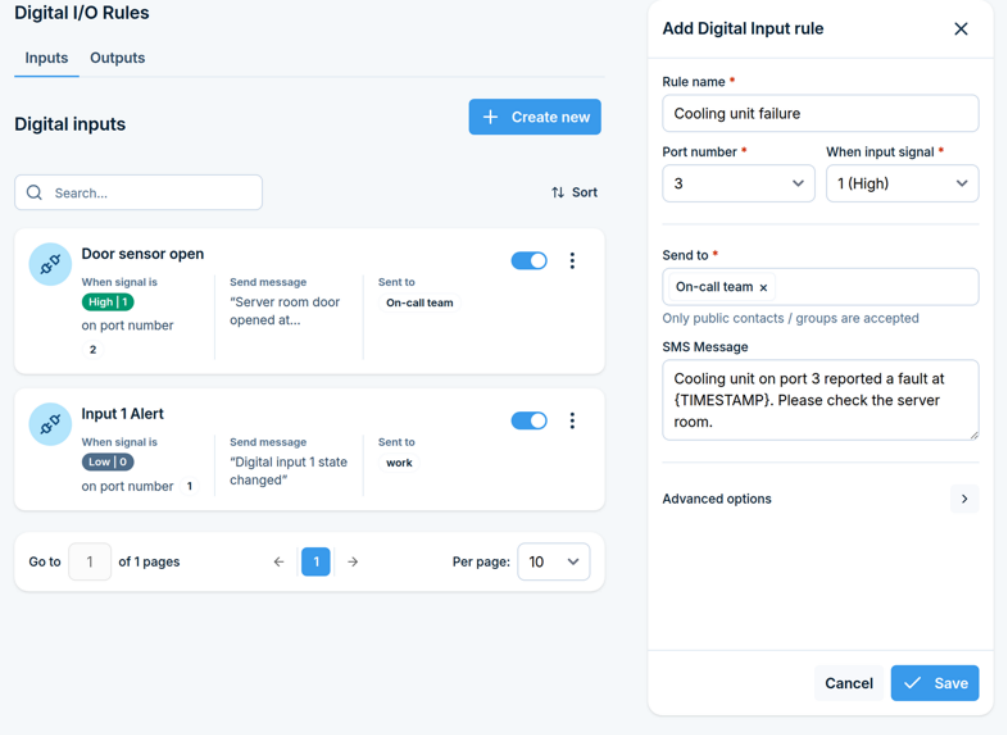
Pick the value that represents the alarm condition on your equipment. A **NO** (normally open) contact that closes on alarm needs **1 (High)**; a **NC** (normally closed) contact that opens on alarm needs **0 (Low)**. See NO and NC contacts for details.

Wählen Sie die Empfänger

Wählen Sie in **Send to** die Kontakte oder Gruppen aus, die die SMS erhalten sollen. Nur **public** Kontakte und Gruppen können hier ausgewählt werden. Dieses Feld ist erforderlich.

Schreiben Sie den SMS-Text

SMS Message ist der Text, der gesendet wird, wenn die Regel ausgelöst wird. Maximum 1000 Zeichen. Der gleiche Text wird an jeden Empfänger gesendet, daher geben Sie den Standort oder die Maschine darin an, z. B. `ALARM: server room door opened`.

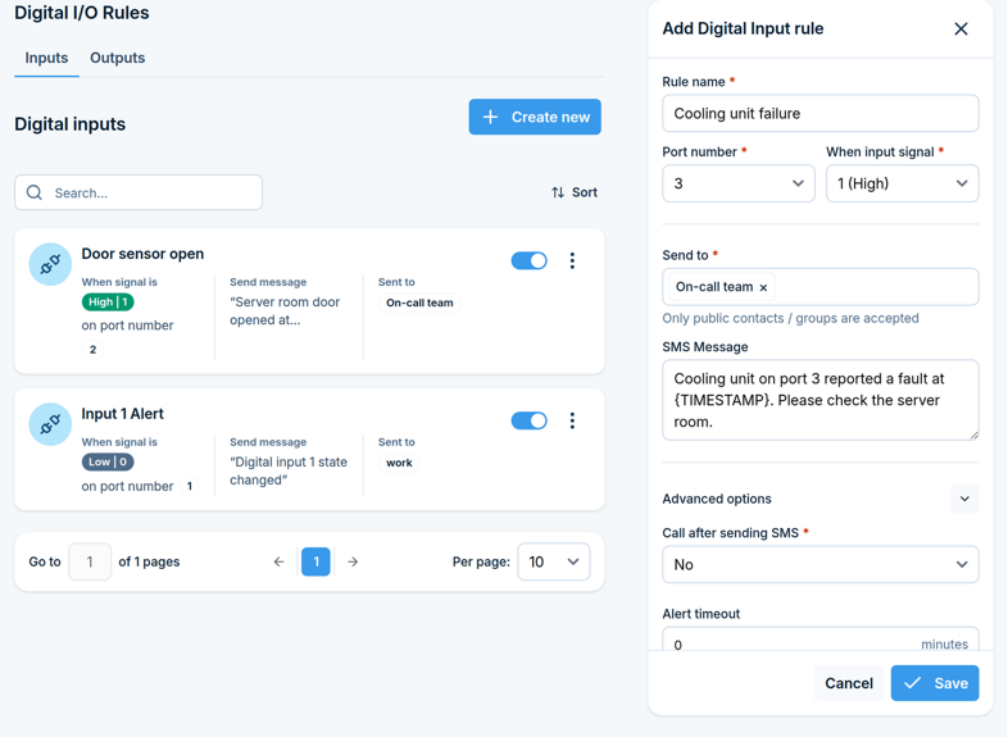


Eine vollständige Eingaberegel

Erweiterte Optionen

Klicken Sie auf **Advanced options**, um diesen Abschnitt zu erweitern. Sie benötigen ihn nicht für eine grundlegende Konfiguration.

- **Call after sending SMS** - führt auch einen Sprachanruf an die gleichen Empfänger durch. Die Optionen sind **No**, **Ring**, **Text-to-speech (TTS)** und **Text-to-speech (advanced)**, je nachdem, welche Funktionen Ihr Gerätemodell unterstützt. Mit der erweiterten Option können Sie auch ein **Voice model** auswählen.
- **Alert timeout** - die Anzahl der Minuten, die verstreichen müssen, bevor die gleiche Regel erneut einen Alarm auslösen darf. `0` bedeutet kein Limit, daher sendet jede Signaländerung eine SMS.



Erweiterte Optionen der Eingaberegel

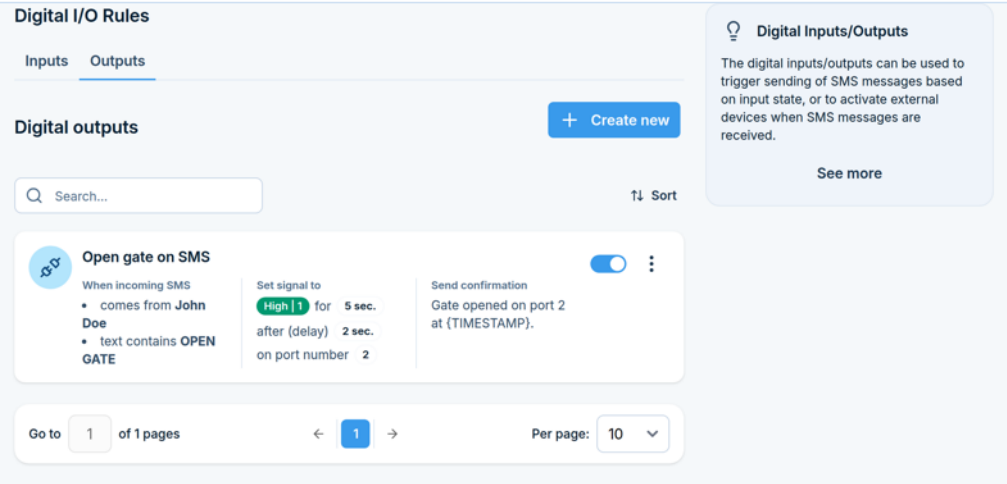
Stellen Sie ein Alert-Timeout für verrauschte Eingaben ein. Ein flatternder Kontakt oder eine Ausrüstung, die sich wiederholt auslöst, kann einen Nachrichtenstoß verursachen. Ein Timeout von einigen Minuten führt dazu, dass ein echtes Ereignis zu einer SMS wird.

Klicken Sie auf **Save**. Die Regel wird ab sofort bei Signaländerungen aktiv.

Teil 2: Ausgaberegeln (SMS in Ausgabesignal)

Schritt 1: Öffnen Sie die Seite „Regeln“

Gehen Sie zu **Monitoring > Digital input / output > Rules** und wählen Sie die Registerkarte **Outputs** aus.



Regeln für digitale Ausgänge

Schritt 2: Erstellen Sie eine Ausgaberegel

Klicke auf **Neue erstellen** in der oberen rechten Ecke. Ein Seitenpanel öffnet sich.

Benennen Sie die Regel und wählen Sie den Port

Geben Sie im Feld **Rule name** etwas Aussagekräftiges ein, beispielsweise `Open gate on SMS`. Maximale Länge: 100 Zeichen. Wählen Sie im Feld **Port number** den Ausgangsport aus, an den Ihre Ausrüstung angeschlossen ist. Externe (io-bridge) Ports werden mit `(Ext)` gekennzeichnet.

Entscheiden Sie, welche SMS-Nachrichten die Regel auslösen

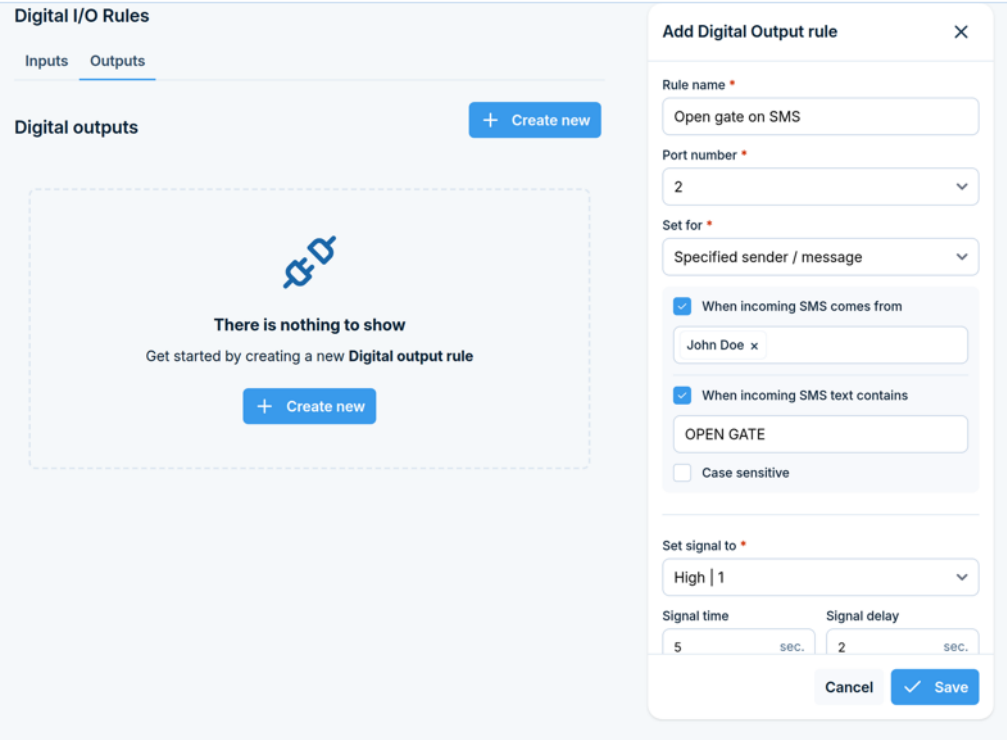
Wählen Sie **Set for**:

Option	Was es bedeutet
All incoming messages	Jede eingehende SMS schaltet den Ausgang um.
Specified sender / message	Nur Nachrichten, die den von Ihnen festgelegten Bedingungen entsprechen, schalten ihn um.

Wenn Sie **Specified sender / message** gewählt haben, stehen zwei Bedingungen zur Verfügung. Sie können eine oder beide verwenden. Wenn Sie beide verwenden, muss eine Nachricht **beide** erfüllen.

When incoming SMS comes from Aktivieren Sie dieses Kontrollkästchen und wählen Sie die Sender-Kontakte oder Gruppen aus.

When incoming SMS text contains Aktivieren Sie dieses Kontrollkästchen und geben Sie den Satz im Feld **Text** ein, beispielsweise `OPEN`. Aktivieren Sie **Case sensitive**, wenn `open` und `OPEN` unterschiedlich behandelt werden sollen.



Bedingungen für Ausgaberegeln

Beschränken Sie Ausgaberegeln nach Sender. Eine Ausgaberegel schaltet physische Geräte. Ohne eine Senderbedingung kann jeder, der Ihre Nummer kennt, damit arbeiten.

Entscheiden Sie, was der Ausgang tut

Feld	Was es bedeutet
Set signal to	`Low` | `0` oder `High` | `1`. Der Zustand, in den der Port geschaltet wird.
Signal time	Wie viele Sekunden der Port in diesem Zustand bleibt, bevor er in den Ausgangszustand zurückkehrt. `0` bedeutet, dass er auf unbestimmte Zeit bleibt.
Signal delay	Wie viele Sekunden nach Ankunft der SMS auf das Umschalten des Ports gewartet wird.

Erweiterte Optionen

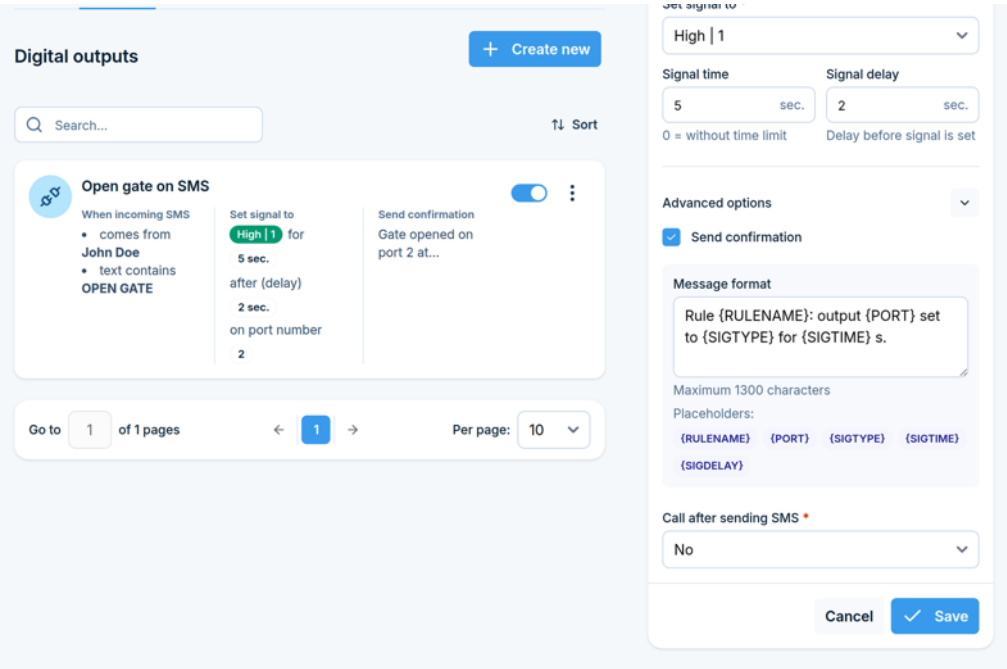
Klicken Sie auf **Advanced options**, um diesen Abschnitt zu erweitern.

Send confirmation Aktivieren Sie dieses Kontrollkästchen, um eine SMS an den Absender zu senden, nachdem der Ausgang umgeschaltet wurde. Das Feld **Message format** erscheint, maximale Länge 1300 Zeichen. Sie können den Text aus Platzhaltern erstellen:

Platzhalter	Ersetzt durch
`{RULENAME}`	Der Name der Regel, die ausgelöst wurde
`{PORT}`	Die Ausgabeanschlussnummer
`{SIGTYPE}`	Das Signal, auf das der Anschluss eingestellt wurde
`{SIGTIME}`	Die Signalzeit in Sekunden
`{SIGDELAY}`	Die Signalverzögerung in Sekunden

Beispiel: `{RULENAME}: port {PORT} set to {SIGTYPE} for {SIGTIME}s` erzeugt eine klare Bestätigung für die Person, die den Befehl gesendet hat.

Anruf nach SMS-Versand Führen Sie auch einen Sprachanruf durch, genau wie oben für Eingaberegeln beschrieben.



Bestätigungsmeldung der Ausgaberegel

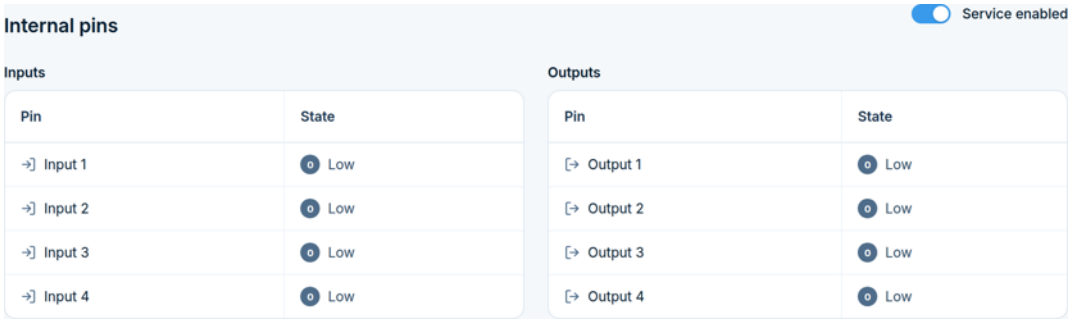
Klicken Sie auf **Save**. Die Regel beginnt sofort mit der Bearbeitung von ab sofort eingegangenen Nachrichten.

Teil 3: Interne Anschlüsse

Gehen Sie zu **Monitoring > Digital input / output > Internal pins**.

Die Seite zeigt zwei Tabellen, **Inputs** und **Outputs**, die jeden integrierten Anschluss mit seinem aktuellen Zustand auflistet (`0` Low oder `1` High). Dies ist eine Live-Abfrage der Hardware und ist nützlich, um Ihre Verdrahtung zu überprüfen, bevor Sie eine Regel schreiben.

Oben auf der Seite befindet sich ein **Service enabled**-Schalter. Er startet und stoppt den Dienst, der die integrierten Anschlüsse liest und steuert. **Während er ausgeschaltet ist, funktionieren Input- und Output-Regeln auf internen Anschlüssen nicht.**



Interne Anschlüsse mit laufendem Dienst. Jeder Anschluss liest hier `0` Low, weil nichts angeschlossen ist

---

Teil 4: Externe Anschlüsse

Externe Anschlüsse sind zusätzliche Anschlüsse, die von einem io-bridge-Modul bereitgestellt werden, das an das Gerät angeschlossen ist.

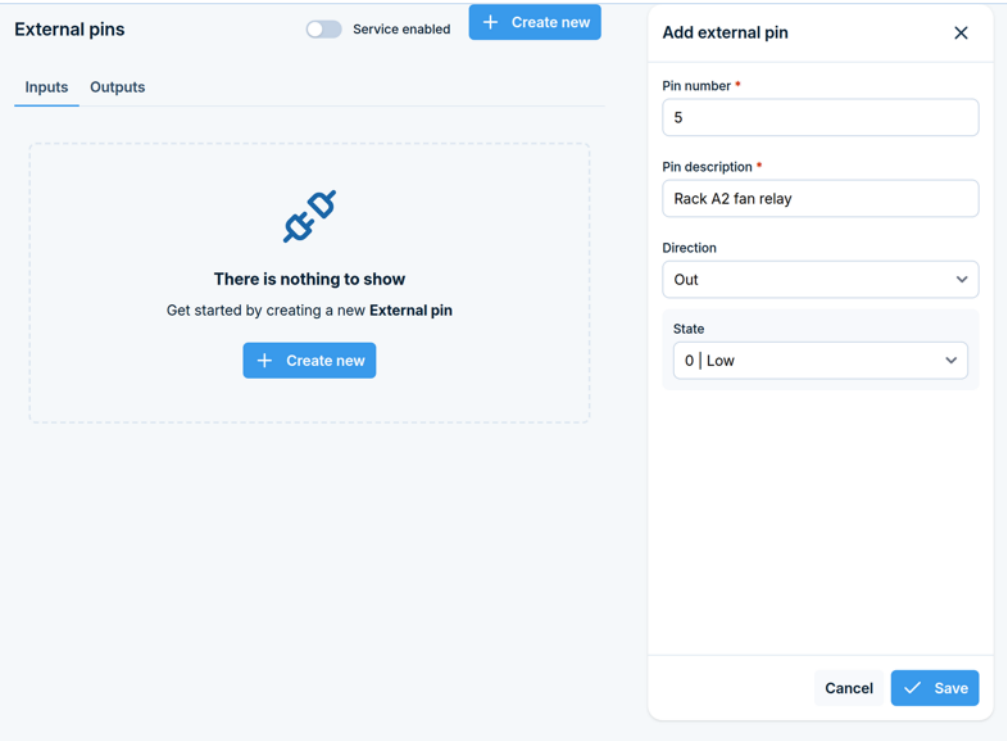
Gehen Sie zu **Monitoring > Digital input / output > External pins**. Die Seite hat einen **Inputs**-Reiter und einen **Outputs**-Reiter, sowie einen **Service enabled**-Schalter, der den io-bridge-Dienst startet und stoppt.

Externen Anschluss hinzufügen

Klicken Sie auf **Create new**. Ein Seitenpanel öffnet sich.

Feld	Was Sie eingeben müssen
Pin number	Die Anschlussnummer auf dem io-bridge-Modul, zum Beispiel 1. Jede Nummer kann nur einmal konfiguriert werden.
Pin description	Ein kurzer Name, maximal 64 Zeichen. Nur Buchstaben, Ziffern und Leerzeichen sind erlaubt.
Direction	**In** für einen Anschluss, den Sie lesen, **Out** für einen Anschluss, den Sie steuern.
State	Wird nur für **Out**-Pins angezeigt: der Zustand, in dem der Port startet, `1 | High` oder `0 | Low`.

Klicken Sie auf **Save**.



Hinzufügen eines externen Pins

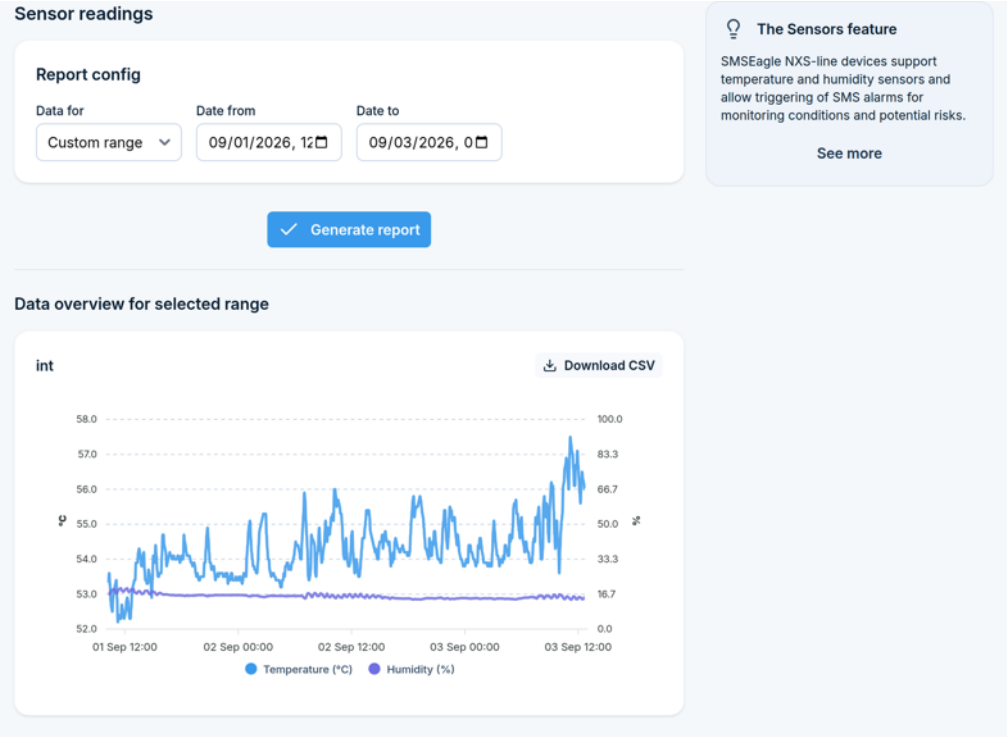
Verwenden Sie die Pins

- Auf der Registerkarte **Outputs** können Sie den Zustand eines Pins direkt aus der Liste umschalten.
- Auf der Registerkarte **Inputs** ist der Zustand schreibgeschützt, da der Wert durch das bestimmt wird, was an den Pin angeschlossen ist.
- Externe Pins erscheinen nach ihrer Definition auch in den **Port number**-Listen von Input- und Output-Regeln, gekennzeichnet mit `(Ext)`, sodass Regeln sie genau wie integrierte Ports verwenden können.

Wie sich Digital-I/O-Regeln verhalten

- Regeln wirken sich nur auf Ereignisse aus, die nach der Erstellung und Aktivierung der Regel auftreten. Verwenden Sie den Schalter neben einer Regel, um sie zu unterbrechen, ohne sie zu löschen.
- Wenn mehrere Regeln auf dasselbe Ereignis zutreffen, werden **alle** ausgeführt, sodass ein Eingangssignal mehrere Nachrichten senden kann und eine SMS mehrere Ports umschalten kann.
- Die Textbedingung bei Output-Regeln ist eine **contains**-Übereinstimmung, keine genaue Übereinstimmung.
- Regeln, die interne Ports verwenden, benötigen den Dienst **Internal pins**; Regeln, die `(Ext)`-Ports verwenden, benötigen den Dienst **External pins**.

Temperatur- und Feuchtigkeitssensoren



Übersicht über Temperatur- und Feuchtigkeitssensoren

Was diese Funktion tut

SMSEagle-Geräte der NXS-Reihe unterstützen Temperatur- und Feuchtigkeitssensoren, die an das Gerät angeschlossen sind. Nachdem ein Sensor angeschlossen ist, liest das Gerät ihn nach einem Zeitplan aus, speichert den Leseverlauf und kann eine SMS senden, wenn ein Wert einen von Ihnen definierten Grenzwert überschreitet.

Die Funktion hat drei Seiten:

Seite	Wofür es nützlich ist
Reading	Diagramme der aufgezeichneten Werte mit CSV-Download.
Alarms	Die Regeln, die eine Messung in eine SMS umwandeln.
Sensor settings	Die Liste der angeschlossenen Sensoren, ihre Namen und wie oft sie gelesen werden.

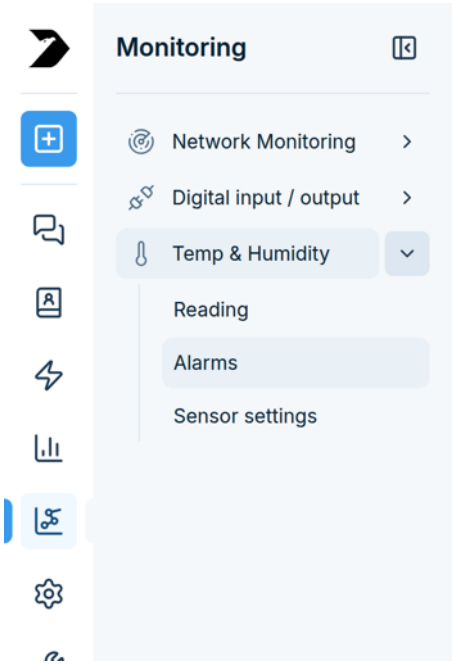
Typische Anwendungen: Überwachung eines Serverraums, einer Kühlanlage oder eines technischen Schranks sowie Benachrichtigung des Bereitschaftsdiensts per SMS, wenn es zu warm oder zu feucht wird.

Bevor Sie beginnen

- Schließen Sie den Sensor an das Gerät an, bevor Sie etwas konfigurieren. Das Gerät findet Sensoren durch Scannen der Hardware, sodass ein nicht angeschlossener Sensor nicht konfiguriert werden kann.
- Empfänger von Alarmregeln müssen im Phonebook als **Public** gekennzeichnet sein.

Wo zu finden

Gehen Sie in der Seitenleiste zu **Monitoring > Temp & Humidity**. Die drei oben aufgeführten Seiten erscheinen darunter.



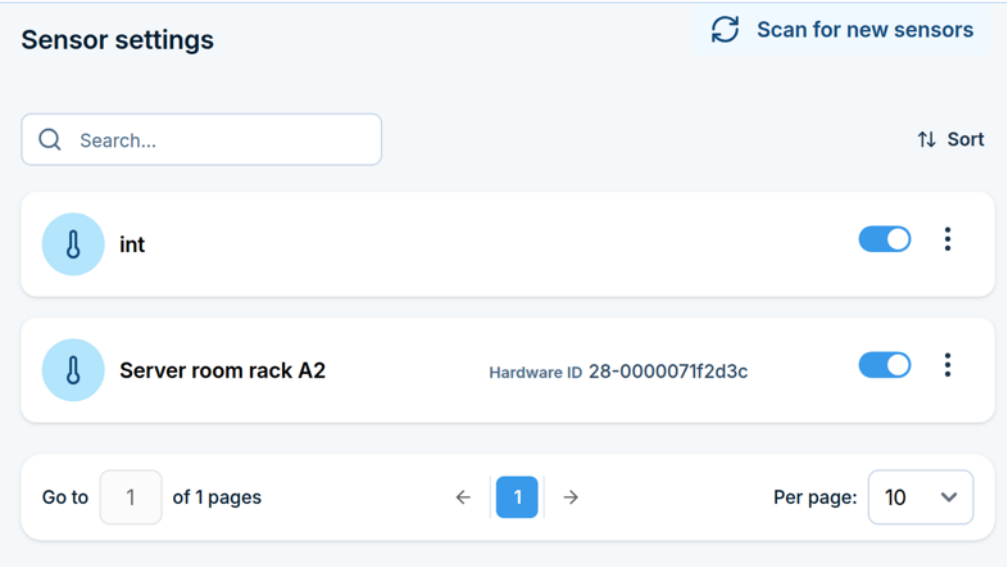
Wo sich die Sensorseiten befinden

Teil 1: Sensoren hinzufügen und benennen

Schritt 1: Nach Sensoren scannen

Gehen Sie zu **Monitoring > Temp & Humidity > Sensor settings** und klicken Sie in der oberen rechten Ecke auf **Scan for new sensors**.

Das Gerät prüft seine Eingänge und fügt alles Gefundene hinzu. Die Seite zeigt an, ob neue Sensoren hinzugefügt wurden oder keine gefunden wurden.



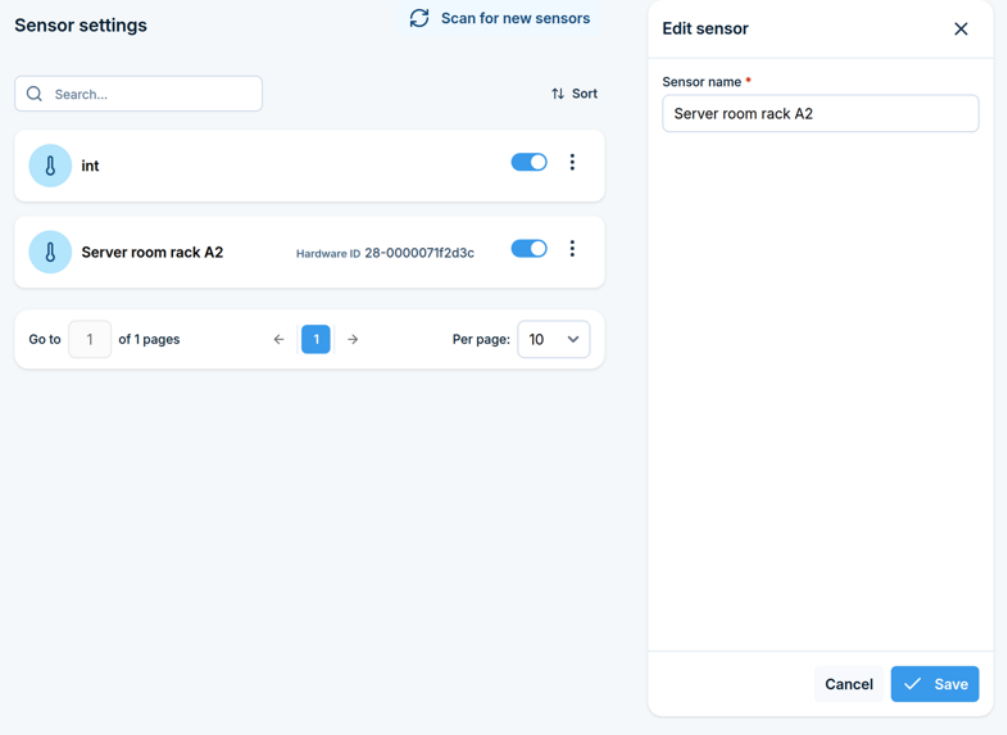
Sensor settings

Jeder Sensor in der Liste zeigt seinen **Sensor name** und seine **Hardware ID**. Die Hardware ID ist die Kennung des Geräts für den physischen Sensor; sie ist nicht bearbeitbar.

Schritt 2: Sensoren aussagekräftige Namen geben

Ein neu erkannter Sensor ist nicht nach dem Ort benannt, den er überwacht. Benennen Sie ihn daher um: Klicken Sie neben einem Sensor auf **Edit** und geben Sie einen **Sensor name** ein, maximal 255 Zeichen, zum Beispiel `Server room rack A`.

Dieser Name wird in den Diagrammen, in den Alarmregeln und im CSV-Export angezeigt, daher lohnt es sich, ihn vor dem Erstellen von Regeln einzutragen.



Umbenennen eines Sensors

Schritt 3: Liste verwalten

Jeder Sensor verfügt über:

- einen Schalter zum **Aktivieren oder Deaktivieren**, der das Auslesen stoppt, ohne ihn zu entfernen,
- eine **Edit**-Aktion für den Namen,
- eine **Delete**-Aktion.

Sie können auch mehrere Sensoren auswählen und diese gemeinsam aktivieren, deaktivieren oder löschen.

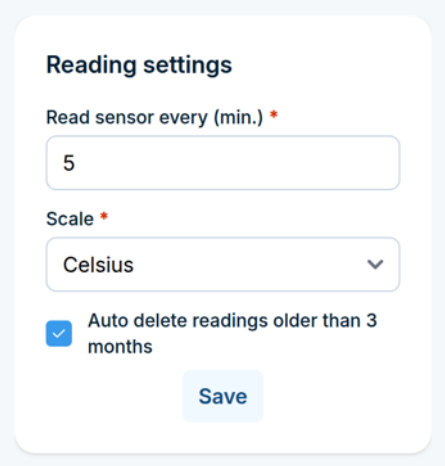
> Der **interne Sensor kann nicht gelöscht werden**. Geräte mit einem integrierten Sensor behalten ihn immer in der Liste; deaktivieren Sie ihn, falls Sie seine Messwerte nicht benötigen.

Schritt 4: Auslesungseinstellungen konfigurieren

Das Feld **Reading settings** auf der rechten Seite der Seite Sensor settings steuert die Auslesung der Sensoren. Diese Einstellungen sind **global** und gelten für jeden Sensor:

Feld	Was es tut
Read sensor every (min.)	Wie oft die Sensoren ausgelesen werden, von 1 bis 59 Minuten.
Scale	**Celsius** oder **Fahrenheit**. Gilt für die Diagramme, Alarme und den Export.
Auto delete readings older than 3 months	Verhindert, dass der Messverlauf unbegrenzt wächst.

Klicken Sie auf **Save**.

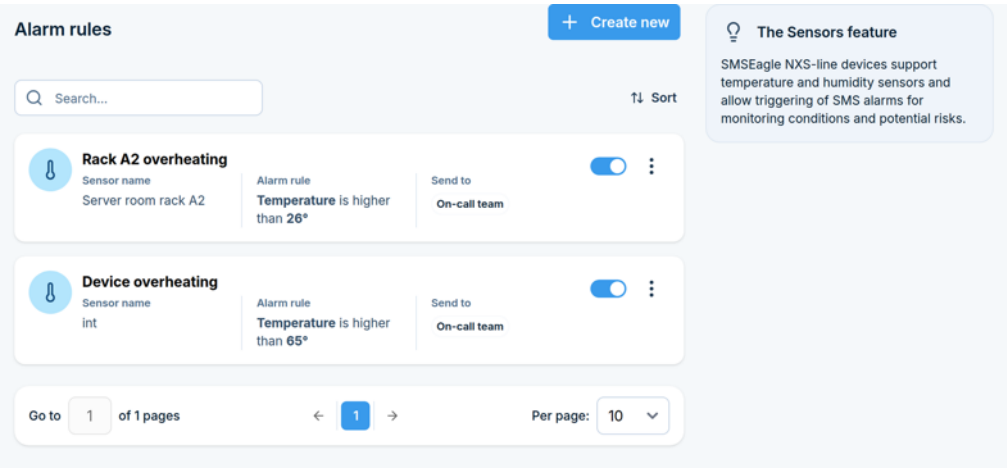


Reading settings

Teil 2: Alarmregeln

Schritt 1: Öffnen Sie die Seite Alarme

Gehen Sie zu **Monitoring > Temp & Humidity > Alarme**.



Alarmregeln

Schritt 2: Erstelle eine Regel

Klicke auf **Neue erstellen** in der oberen rechten Ecke. Ein Seitenpanel öffnet sich.

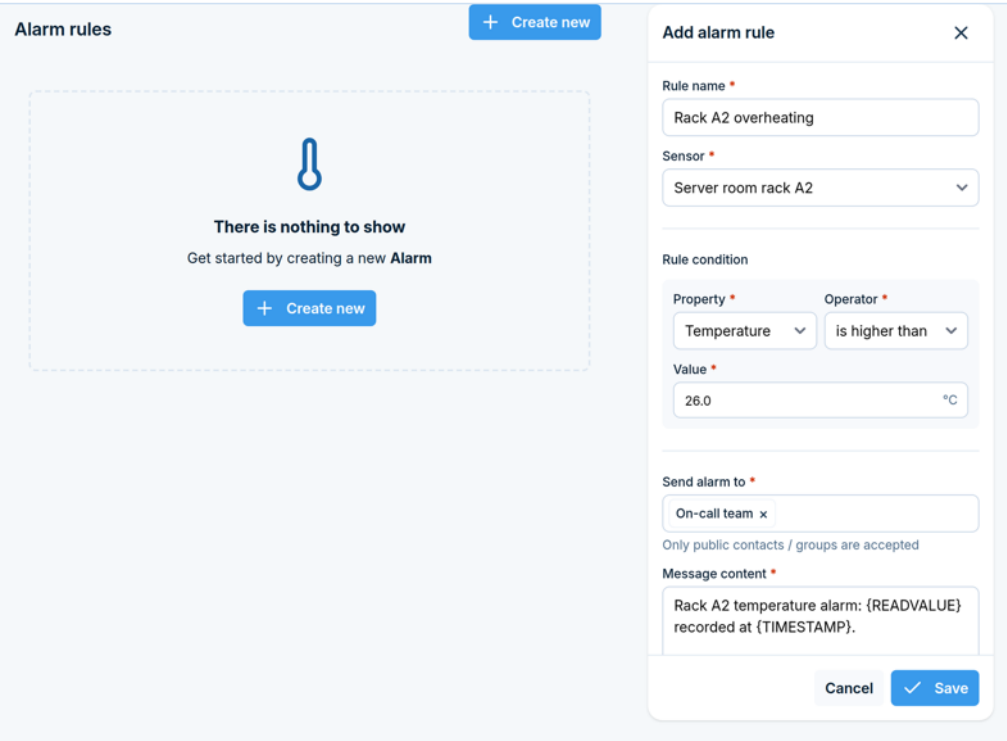
Benenne die Regel

Geben Sie unter **Regelname** etwas Aussagekräftiges ein, zum Beispiel `Server room too warm`. Maximum 100 Zeichen.

Definieren Sie die Bedingung

Feld	Was man wählen sollte
Sensor	Welcher Sensor von der Regel überwacht wird.
Eigenschaft	**Temperatur** oder **Luftfeuchtigkeit**.
Operator	**is higher than** oder **is lower than**.
Wert	Der Schwellenwert mit einer Dezimalstelle, zum Beispiel `27.5`.

Der Temperaturschwellenwert wird in der **Scale** gelesen, die Sie in den Lesezugangseinstellungen festgelegt haben. Eine Regel, die für Celsius geschrieben wird, bedeutet etwas anderes, nachdem Sie das Gerät auf Fahrenheit umgestellt haben. Überprüfen Sie Ihre Regeln, wenn Sie die Skala ändern.



Erstellen einer Alarmregel

Wählen Sie die Empfänger

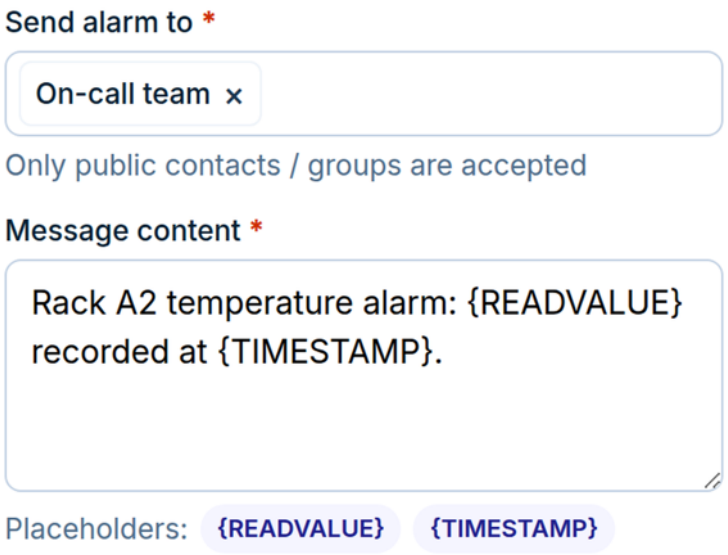
Wählen Sie unter **Alarm senden an** die Kontakte oder Gruppen. Nur **öffentliche** Kontakte und Gruppen können hier ausgewählt werden. Dieses Feld ist erforderlich.

Schreiben Sie die Nachricht

Nachrichteninhalt ist die SMS, die gesendet wird, maximal 2000 Zeichen. Sie können sie aus Platzhaltern aufbauen:

Platzhalter	Ersetzt durch
`{READVALUE}`	Der Wert, der den Alarm ausgelöst hat
`{TIMESTAMP}`	Wann die Messung durchgeführt wurde

Zum Beispiel produziert `ALARM: server room at {READVALUE} ({TIMESTAMP})` eine Nachricht, die anzeigt, was gemessen wurde und wann, ohne dass jemand die Benutzeroberfläche öffnen muss.



Die Abzeichen unter dem Feld fügen einen Platzhalter am Cursor ein

Klicken Sie auf **Speichern**. Die Regel wird von nun an bei jeder Messung überprüft.

Teil 3: Messwerte und Berichte

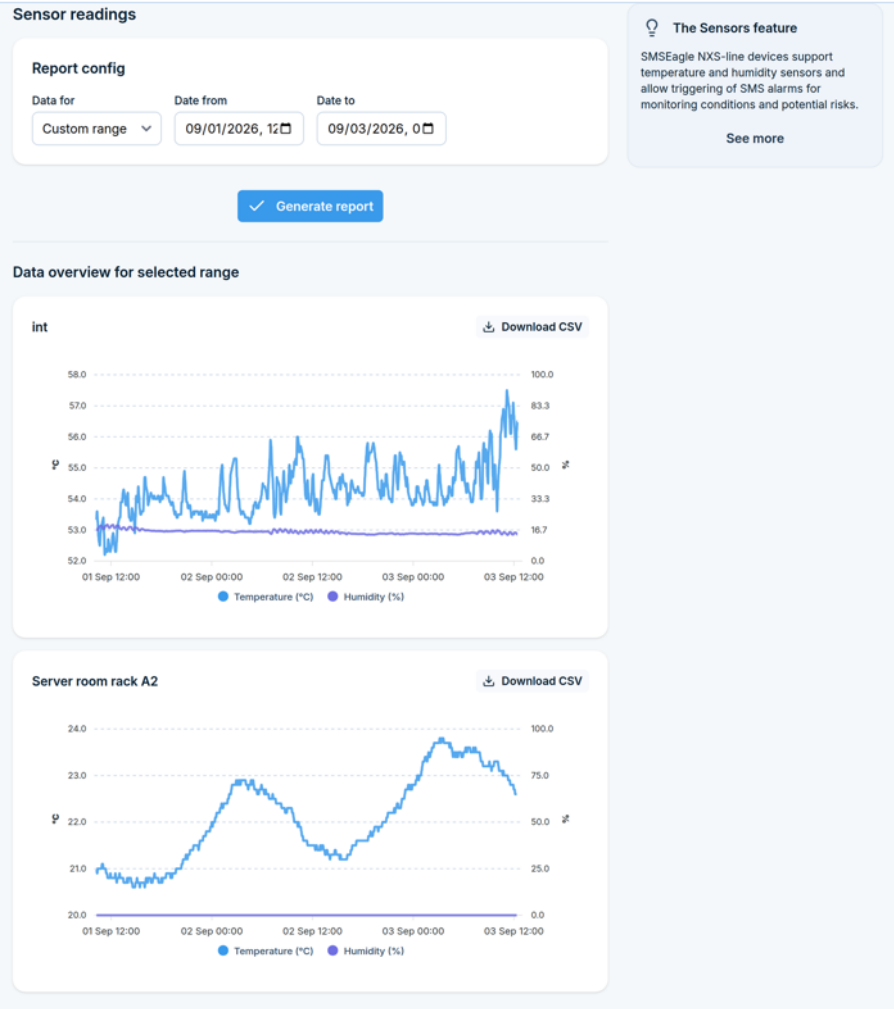
Gehen Sie zu **Monitoring > Temp & Humidity > Reading**.

Wählen Sie im Feld **Report config**:

Feld	Was es tut
Data for	Ein vordefinierter Datumsbereich. Wenn Sie einen auswählen, werden die Datumsangaben darunter automatisch ausgefüllt.
Date from / **Date to**	Der exakte Bereich. Wenn Sie diese Felder bearbeiten, wird **Data for** auf einen benutzerdefinierten Bereich umgeschaltet.

Klicken Sie auf **Generate report**. Darunter finden Sie unter **Data overview for selected range** ein Diagramm pro Sensor, das Temperatur und Luftfeuchtigkeit über den Zeitraum darstellt.

Jedes Diagramm hat eine Schaltfläche **Download CSV**, mit der die Messwerte dieses Sensors für den ausgewählten Zeitraum exportiert werden.



Sensormesswerte

Wenn die Seite **No sensors found** anzeigt, wurde noch kein Sensor erkannt. Verbinden Sie einen und führen Sie **Scan for new sensors** auf der Seite Sensor settings aus.

Funktionsweise

- Alarme werden ausgewertet, wenn eine Messung durchgeführt wird. Die Reaktionszeit hängt daher von **Read sensor every** ab. Ein Intervall von 15 Minuten bedeutet, dass ein Alarm bis zu 15 Minuten verspätet auslösen kann.
- Ein deaktivierter Sensor wird überhaupt nicht gelesen, daher bleiben Alarmregeln, die auf ihn verweisen, stumm.
- Wenn mehrere Regeln dieselbe Messung erfüllen, sendet **jede** von ihnen ihre eigene SMS.

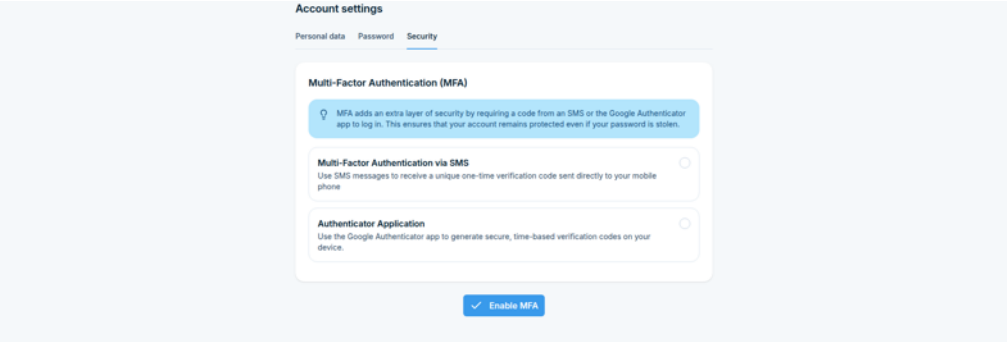
Einstellungen

Dieses Kapitel behandelt den Bereich **Einstellungen** der Weboberfläche, gemäß dem gleichen Menü der zweiten Ebene, das Sie in der Seitenleiste sehen.

Kontoeinstellungen

Klicken Sie auf Ihren Avatar (unten links) und wählen Sie **Kontoeinstellungen**, um Ihr eigenes Konto zu verwalten, aufgeteilt in drei Registerkarten: **Persönliche Daten** (Name, Login, Telefonnummer, Oberflächensprache, Verfassungsstandardeinstellungen, Benachrichtigungston), **Passwort** und **Sicherheit** – siehe Weboberflächen-Übersicht für das vollständige Layout der Registerkarten.

Konfiguration der Multi-Faktor-Authentifizierung (MFA)



MFA-Setup unter Kontoeinstellungen > Sicherheit

MFA fügt eine zusätzliche Sicherheitsebene hinzu, indem neben dem Passwort auch ein Einmalcode erforderlich ist, um sich anzumelden. Dies schützt das Konto selbst dann, wenn das Passwort gestohlen wurde.

Wo Sie dies finden

- **Pro Benutzer**: **Kontoeinstellungen > Sicherheit** (`/settings/account/security`), für Ihr eigenes Konto.
- **Geräteübergreifend**: die Option **Zwei-Faktor-Authentifizierung** im Schritt „Administrator“ des Konfigurationsassistenten, und beim Erstellen oder Bearbeiten eines Benutzers unter **System > Benutzer**.

Schritt 1: Wählen Sie eine MFA-Methode

Wählen Sie unter **Kontoeinstellungen > Sicherheit** eine der folgenden Optionen:

- **Multi-Faktor-Authentifizierung via SMS** – bei jeder Anmeldung wird ein Einmalverifizierungscode per SMS an Ihr Mobiltelefon gesendet.

- **Authentifizierungs-App** – zeitbasierte Codes werden von einer App wie Google Authenticator generiert.

Klicken Sie auf **MFA aktivieren** und folgen Sie den angezeigten Schritten, um die gewählte Methode zu bestätigen.

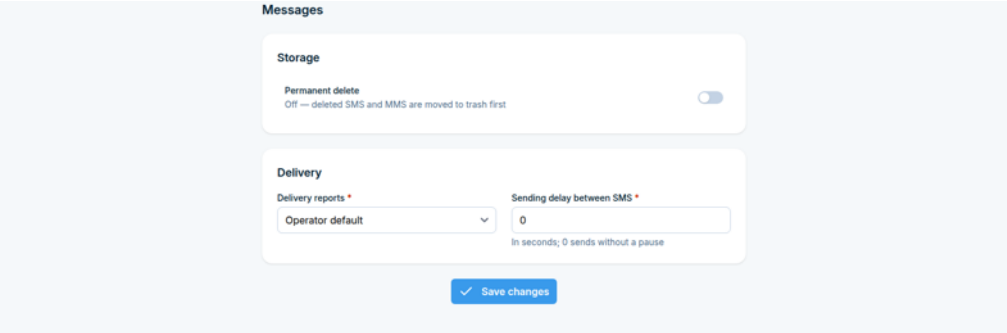
Schritt 2: MFA geräteübergreifend erzwingen (optional)

Ein Administrator kann MFA für jedes Konto erforderlich machen, anstatt es pro Benutzer optional zu lassen. Setzen Sie im Setup-Assistent unter **Administrator** (oder pro Benutzer unter **System > Benutzer**) die Option **Zwei-Faktor-Authentifizierung** auf:

- **Nicht erzwingen** – jeder Benutzer entscheidet individuell, ob MFA aktiviert werden soll.
- **Für alle Benutzer erzwingen** – jeder existierende und neue Benutzer muss MFA einrichten.
- **Für neue Benutzer erzwingen** – MFA ist nur für Konten erforderlich, die ab sofort erstellt werden.

SMS / MMS

Nachrichten



Nachrichteneinstellungen unter SMS / MMS

Einstellungen > SMS / MMS > Nachrichten (`/settings/sms-mms/messages/`) gruppiert das allgemeine Verhalten der SMS-/MMS-Speicherung und Zustellungs-Pipeline.

Speicher

Dauerhaft löschen – standardmäßig deaktiviert, sodass gelöschte SMS und MMS zunächst in den Papierkorb verschoben werden, statt sofort entfernt zu werden.

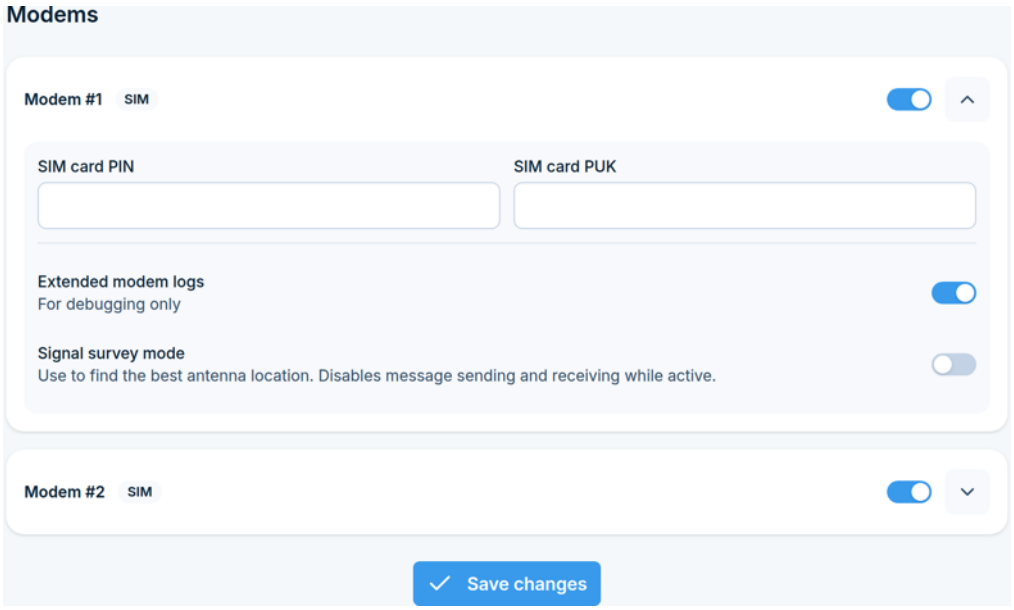
Zustellung

Liefermeldungen ermöglichen es Ihnen, herauszufinden, ob eine gesendete SMS tatsächlich das Telefon des Empfängers erreicht hat.

- **Lieferberichte** - Operator-Standard (Standardverhalten des Netzbetreibers), Immer anfordern oder Nie anfordern. Wird auch im Konfigurationsassistenten angeboten.
- **Verzögerung zwischen SMS-Versand** - eine Pausierung in Sekunden zwischen aufeinanderfolgenden ausgehenden SMS. `0` versendet ohne Pausierung.

Wenn ein Lieferbericht angefordert wird, aktualisiert SMSEagle den Status der Nachricht unter „Gesendete Elemente“ / „Postausgang“, sobald das Netz die Zustellung bestätigt (oder einen Fehler meldet), und der Bericht wird in den Details der Nachricht sichtbar.

Modems



Modems-Einstellungen mit ausgeweitertem Abschnitt des ersten Modems. NXS-9700 listet einen Modem-Abschnitt auf

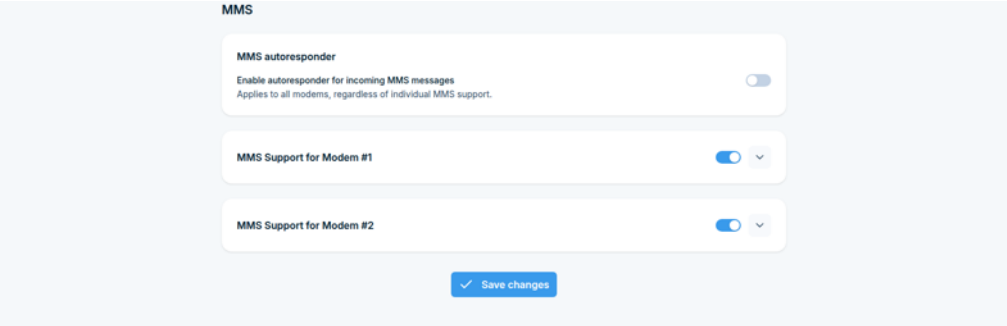
Einstellungen > SMS / MMS > Modems (`/settings/sms-mms/modems/`) listet das integrierte Modem (Modem Nr. 1) mit einem Schalter zum Aktivieren seiner SIM-Karte auf. Das Expandieren eines Modem-Abschnitts zeigt vier Einstellungen:

- **SIM-Kartenstift** und **SIM-Kartenpuk** - nur erforderlich, wenn die Karte dies verlangt. Die gleichen zwei Felder werden auch im Konfigurationsassistenten angeboten.
- **Erweiterte Modem-Protokolle** - ausführliches Modem-Logging nur zum Debuggen.
- **Signalumfragemodus** - verwenden Sie ihn, um die beste Antennenposition zu finden. Er **deaktiviert den Nachrichtenversand und -empfang** während er aktiv ist, schalten Sie ihn also aus, wenn Sie fertig sind.

Multi-Modem

NXS-9700 wird mit einem einzelnen integrierten Modem geliefert, sodass die Modem-Auswahlstrategie und die Failover-Einstellungen für Modems nicht gelten - der gesamte SMS/MMS-Verkehr verläuft über das eine integrierte Modem. Multi-Modem-SMSEagle-Produkte (NXS-9750, NXS-9850, MHD-8100) zeigen diese Seite unter **Einstellungen > SMS / MMS > Multi-Modem** mit einer Auswahlstrategie (Round-Robin, SIM 1/SIM 2 als Master-Modem) und einem Modem-Failover-Mechanismus zwischen ihren integrierten Modems.

MMS



MMS-Einstellungen, hier auf einem Gerät mit zwei Modems angezeigt. NXS-9700 listet einen Modem-Abschnitt auf

Was diese Funktion tut

MMS ermöglicht es dem Gerät, **Multimedianachrichten** zu senden und zu empfangen: ein Text mit angehängten Bildern oder anderen Dateien, nicht nur SMS.

Im Gegensatz zu SMS verläuft MMS nicht über den einfachen GSM-Kanal. Sie verläuft über das Datennetz des Betreibers zu einem MMS-Zentrum, daher benötigt jede SIM-Karte einen eigenen Satz von Verbindungsparametern (APN, MMSC und optional einen Proxy). In SMSEagle werden diese Parameter **pro Modem** unter **Einstellungen > Kanäle > SMS / MMS > MMS** gesetzt.

Der gleiche Bildschirm enthält auch den **MMS-Autoantwortdienst**, der eine automatische Antwort auf jede eingehende MMS sendet.

Bevor Sie beginnen

- Sie benötigen die MMS-Einstellungen für jede SIM-Karte von ihrem Betreiber: **APN**, **MMSC**-Adresse und einen **Proxy** mit **Port**, falls der Betreiber einen verwendet. Einige Betreiber erfordern auch einen Benutzernamen und ein Passwort.
- Die SIM-Karte muss MMS im Tarif aktiviert haben. Eine SIM-Karte, die SMS-Nachrichten senden kann, aber keinen Datendienst oder MMS-Dienst hat, funktioniert nicht, egal wie die Einstellungen ausgefüllt werden.
- Viele Operatorprofile sind dem Gerät bereits bekannt, versuchen Sie daher **APN-Einstellungen auslesen**, bevor Sie nach den Werten selbst suchen.

Schritt 1: Öffnen Sie die MMS-Seite

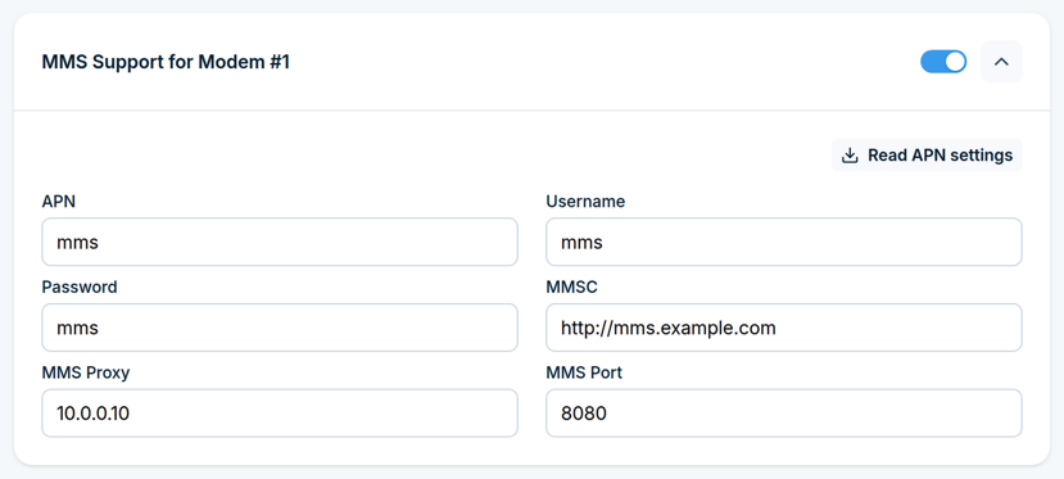
Gehen Sie in der Seitenleiste zu **Einstellungen > Kanäle > SMS / MMS > MMS**.

Die MMS-Seite zeigt die Box **MMS-Autoantwort** oben, dann einen zusammenklappbaren Abschnitt pro Modem. NXS-9700 hat ein einzelnes integriertes Modem, daher gibt es einen Abschnitt mit der Überschrift **MMS-Unterstützung für Modem Nr. 1**.

Schritt 2: Aktivieren Sie MMS auf einem Modem

Der Modem-Abschnitt hat einen Schalter neben der Überschrift. Schalten Sie ihn ein, wenn die SIM-Karte MMS verarbeiten soll.

Klicken Sie dann auf den Pfeil rechts neben der Überschrift, um den Abschnitt zu erweitern und die Verbindungsparameter auszufüllen.



Ein erweiterter Modem-Abschnitt mit **Read APN settings** über den Feldern

Schritt 3: Verbindungsparameter ausfüllen

Der schnellste Weg ist die Schaltfläche **Read APN settings** oben im erweiterten Abschnitt. Sie sucht eine passende Konfiguration für die SIM-Karte im betreffenden Modem und füllt die Felder automatisch aus. Falls keine Übereinstimmung gefunden wird, meldet SMSEagle dies und Sie geben die Werte manuell ein.

Feld	Einzugebender Wert
APN	Der Access Point Name des Betreibers, beispielsweise `internet`.
Benutzername	Der APN-Benutzer, falls vom Betreiber erforderlich. Andernfalls leer lassen.
Passwort	Das APN-Passwort, falls erforderlich.
MMSC	Die Adresse des MMS-Centers des Betreibers, beispielsweise `http://mms.example.com`.
MMS Proxy	Die Proxy-Adresse, falls der Betreiber einen verwendet. Andernfalls leer lassen.
MMS Port	Der Proxy-Port. Nur erforderlich zusammen mit einem Proxy.

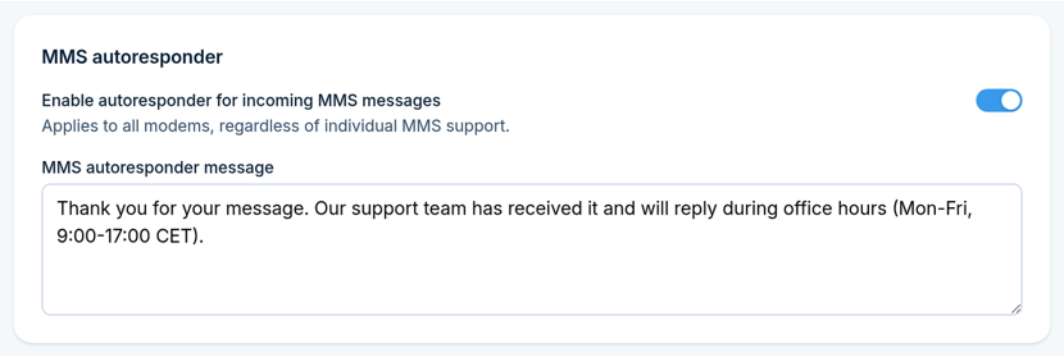
Alle diese Werte gehören zur SIM-Karte in diesem Modem und stammen vom Betreiber dieser SIM-Karte. Lassen Sie **MMS Proxy** und **MMS Port** leer, es sei denn, der Betreiber verwendet tatsächlich einen Proxy.

Schritt 4: Autoantwort einrichten (optional)

Das Feld **MMS autoresponder** oben auf der MMS-Seite sendet eine automatische Antwort, sobald eine MMS ankommt.

1. Aktivieren Sie **Enable autoresponder for incoming MMS messages**.
2. Geben Sie die Antwort in **MMS autoresponder message** ein.

Der Autoresponder **gilt für alle Modems, unabhängig von individueller MMS-Unterstützung**. Es ist eine einzelne globale Einstellung, nicht eine pro Modem, und es gibt einen Antworttexxt, der von jeder eingehenden MMS geteilt wird, daher sollten Sie die Formulierung allgemein halten.



Der Autoresponder, aktiviert mit einer Beispielantwort

Schritt 5: Speichern und Neustart

Klicken Sie auf **Save changes**.

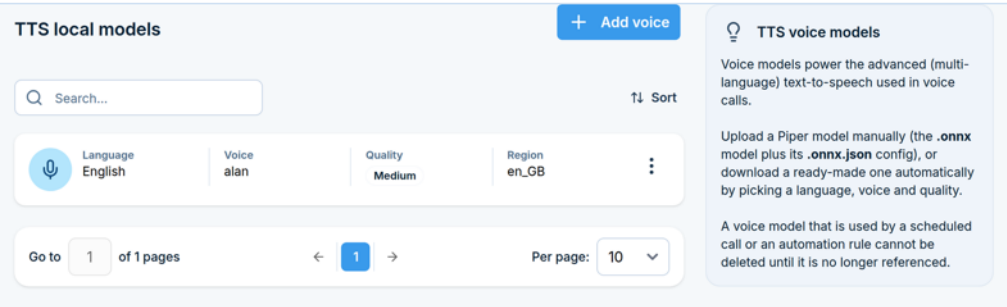
> **Ein Neustart ist erforderlich.** Nach dem Speichern fragt SMSEagle Sie auf, das Gerät neu zu starten, damit die MMS-Änderungen wirksam werden. Bis dahin werden die neuen Parameter gespeichert, aber noch nicht verwendet.

Anrufe

TTS-Lokalmodelle

Lokale Sprachmodelle unterstützen **Text to Speech – erweitert**. Sie laufen auf dem Gerät, daher ist nach der Installation eines Modells keine Internetverbindung erforderlich.

Gehen Sie zu **Settings > Channels > Calls > TTS local models**. Die Seite listet die installierten Modelle mit Sprache, Region und Qualität auf.



TTS-Lokalmodelle

Ein Modell hinzufügen

Klicken Sie in der oberen rechten Ecke auf **Add voice**. Das Panel bietet zwei Möglichkeiten.

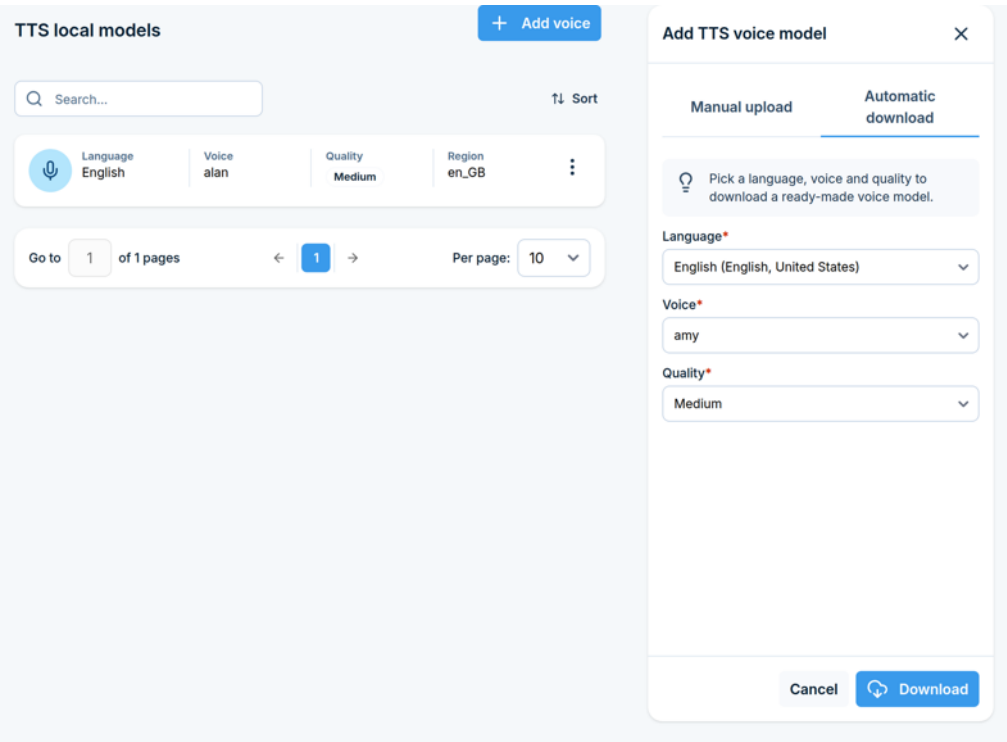
Automatischer Download (der einfache Weg)

Wählen Sie auf der Registerkarte **Automatic download** der Reihe nach:

1. **Language**
2. **Voice**
3. **Quality** – **Very low**, **Low**, **Medium** oder **High**

Klicken Sie auf **Download**. Eine Fortschrittsleiste zeigt den Download an, und das Modell erscheint in der Liste, wenn er beendet ist.

Höhere Qualität bedeutet eine natürlichere Stimme, aber eine größere Datei und eine leicht langsamere Synthese. **Medium** ist eine gute Standardeinstellung.



: auf der Registerkarte „Automatic download

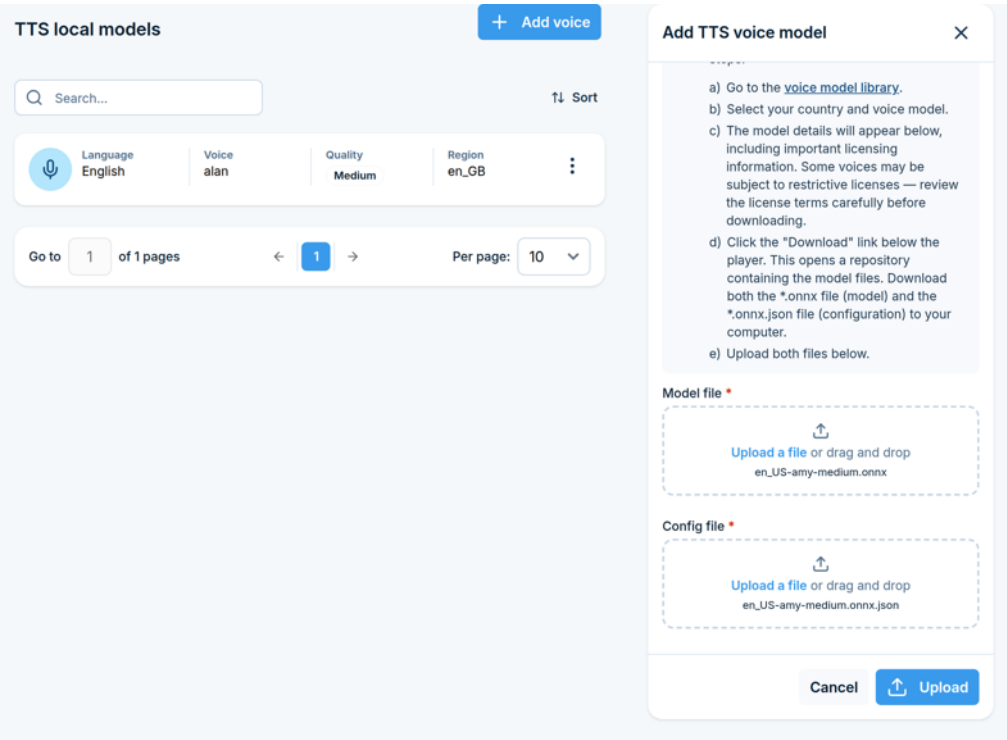
mit ausgewählter Sprache, Stimme und Qualität

Herunterladen eines vordefinierten Sprachmodells

Wenn das Panel „Voice list unavailable

1. anzeigt, konnte das Gerät den Online-Sprachkatalog nicht erreichen. Überprüfen Sie die Netzwerkeinstellungen und versuchen Sie es später erneut, oder verwenden Sie stattdessen das manuelle Hochladen.
2. Manuelles Hochladen

Auf der Registerkarte **Manual upload** stellen Sie ein Sprachmodell selbst bereit:



Config file (.onnx.json) – die entsprechende Konfigurationsdatei.

Beide Dateien sind erforderlich und müssen zusammengehören. Klicken Sie auf Upload.

Panel „Add TTS voice model

auf der Registerkarte „Manual upload

mit ausgewähltem .onnx-Modell und .onnx.json-Konfiguration

Manuelles Hochladen eines Piper-Modells

Ein Modell löschen

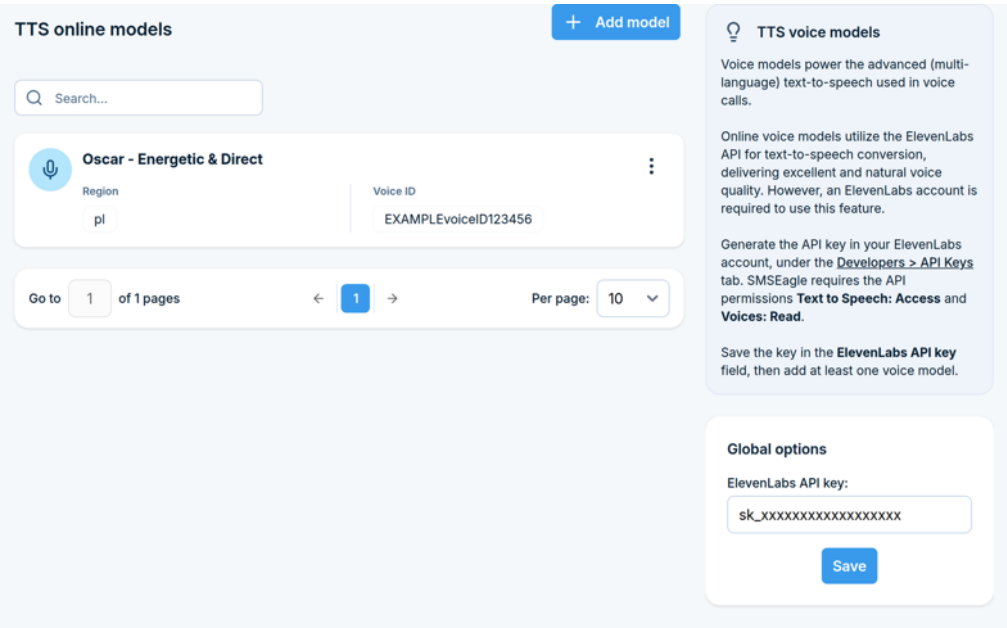
Verwenden Sie die Aktion Delete neben einem Modell, oder wählen Sie mehrere aus und löschen Sie sie zusammen.

Ein Modell, das noch irgendwo referenziert wird, kann nicht gelöscht werden. Die Meldung teilt Ihnen mit, wo es verwendet wird, beispielsweise in einem geplanten Anruf, einer E-Mail-an-SMS-

Regel, einer Digital-Ein-/Ausgangsoperation oder einer Network-Monitor-Aufgabe. Ändern oder entfernen Sie diese Referenz zuerst, dann löschen Sie das Modell.

1. Gehen Sie zu **Developers > API Keys** und generieren Sie einen API-Schlüssel.
2. Geben Sie dem Schlüssel die Berechtigungen **Text to Speech: Access** und **Voices: Read** und speichern Sie dann.
3. Gehen Sie zur Registerkarte **Voices**, wählen Sie die gewünschte Stimme aus und fügen Sie sie zu Ihrem Konto hinzu.
4. Öffnen Sie **My Voices** und kopieren Sie die **voice ID** dieser Stimme.

Die Seite hat eine Schaltfläche, die Sie direkt zu den ElevenLabs-Einstellungen führt.



TTS-Online-Modelle

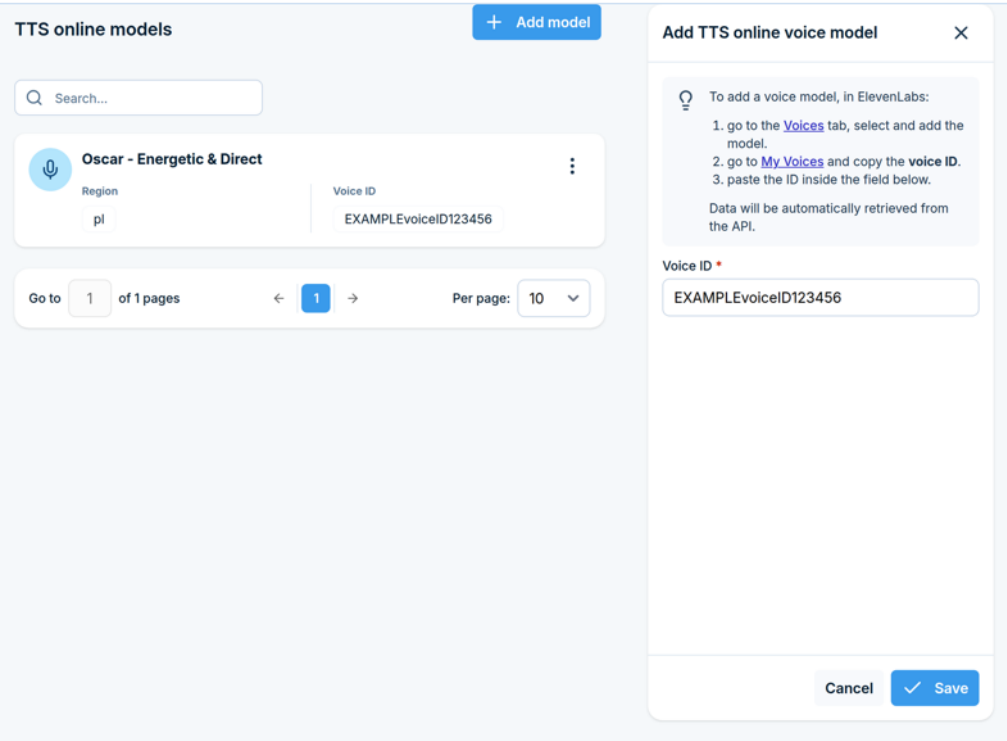
Schritt 2: API-Schlüssel speichern

Fügen Sie den Schlüssel im Feld **Global options** auf der rechten Seite in **ElevenLabs API key** ein und klicken Sie auf **Save**.

Schritt 3: Ein Stimmmodell hinzufügen

Klicken Sie auf **Add model** in der oberen rechten Ecke, fügen Sie die kopierte **Voice ID** ein und klicken Sie auf **Save**.

Die restlichen Modelldaten (Name, Sprache, Region) werden automatisch von der API abgerufen und in der Liste angezeigt.



Ein ElevenLabs-Stimmmodell hinzufügen

Modelle können bearbeitet (um auf eine andere Voice ID zu verweisen) oder einzeln oder in großen Mengen aus der Liste gelöscht werden.

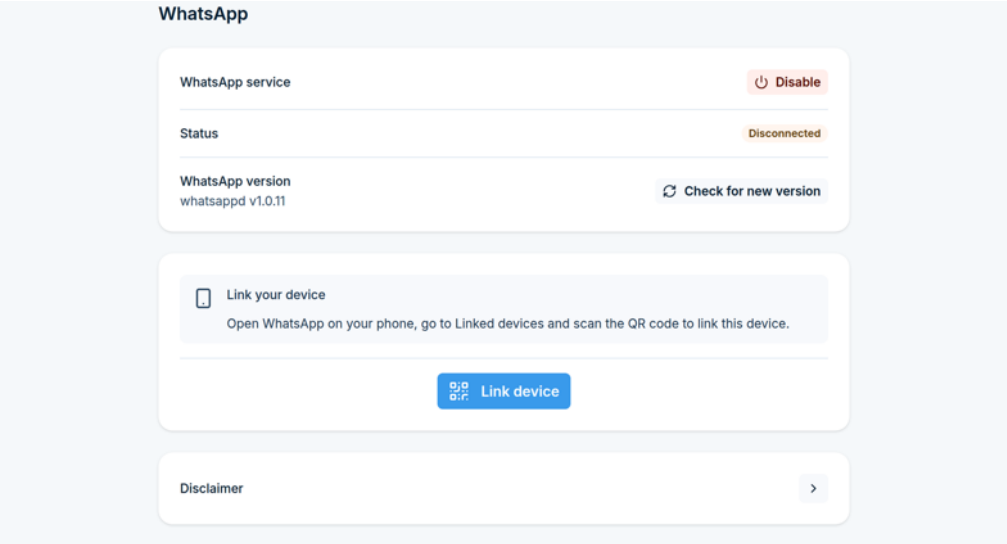
Eingehende Anrufe

Settings > Channels > Calls > Incoming calls (`/settings/calls/incoming-calls`) legt pro Modem fest, wie ein eingehender Sprachanruf behandelt wird: **Always accept**, **Always reject** oder **Ignore**.

Anrufweiterleitung

Settings > Channels > Calls > Call forward (`/settings/calls/call-forward`) verwaltet Anrufumleitungscodes pro Modem. Nicht alle Netzbetreiber unterstützen Umleitungscodes – fragen Sie Ihren Anbieter, bevor Sie sich darauf verlassen.

WhatsApp



WhatsApp-Einstellungen und Geräteverbindung

Was diese Funktion tut

WhatsApp-Unterstützung ermöglicht Ihrem SMSEagle das Senden und Empfangen von **WhatsApp-Nachrichten** zusätzlich zu SMS. Das Gerät wird mit einem WhatsApp-Konto auf die gleiche Weise verknüpft wie eine Desktop- oder Browser-Sitzung: Sie scannen einen QR-Code mit dem Telefon, das das Konto besitzt.

Nach der Verknüpfung wird WhatsApp zu einem weiteren Kanal, den Sie beim Verfassen einer Nachricht auswählen können, mit einer eigenen Gesprächsansicht. Es gibt auch eine **fallback**-Option, die eine SMS oder MMS sendet, wenn sich herausstellt, dass ein Empfänger WhatsApp nicht hat.

Typische Verwendungszwecke: Erreichen von Personen, die WhatsApp nutzen, Versenden von längeren Benachrichtigungen ohne Aufteilen in mehrere SMS-Teile oder Senkung der Kosten für Nachrichten an Empfänger im Ausland.

Die Einrichtung ist ein zweiteiliger Prozess: Zunächst aktivieren Sie den Dienst und verknüpfen ein Gerät (**Settings > Channels > WhatsApp**), dann nutzen Sie den Kanal (**Messages > WhatsApp** oder das Fenster „Compose“).

Bevor Sie beginnen

- WhatsApp ist nur auf ausgewählten Gerätemodellen verfügbar. Wenn **Settings > Channels > WhatsApp** nicht in der Seitenleiste enthalten ist, unterstützt Ihr Gerät WhatsApp nicht.
- Sie benötigen ein Telefon mit einem aktiven WhatsApp-Konto in Ihren Händen, um den QR-Code zu scannen.
- Das Gerät muss in der Lage sein, das Internet zu erreichen. WhatsApp-Nachrichten werden über die Netzwerkverbindung übertragen, nicht über das Modem.

> **Das verknüpfte Konto ist ein echtes WhatsApp-Konto.** Alles, was das Gateway sendet, scheint von diesem Konto zu stammen, und Nachrichten, die an dieses Konto gesendet werden, erscheinen im SMSEagle.

Schritt 1: Öffnen Sie die WhatsApp-Einstellungen

Gehen Sie in der Seitenleiste zu **Einstellungen > Kanäle > WhatsApp**.

Das Feld **Verbindung** zeigt die installierte **WhatsApp-Version** und den aktuellen **Status**. Auf einem neuen Gerät ist der Status **Deaktiviert** und eine Warnung erklärt, dass der Dienst aktiviert werden muss, bevor ein Gerät verknüpft werden kann.

Schritt 2: Aktivieren Sie den Dienst

Klicken Sie unten auf der Seite auf **Aktivieren**. Der Status ändert sich zu **Getrennt**, was bedeutet, dass der Dienst läuft, aber noch kein Konto verknüpft ist. Dies ist der Zustand, der in der Abbildung am Anfang dieses Abschnitts gezeigt wird, mit der Schaltfläche **Gerät verknüpfen**, die unter dem Feld Verbindung wartet.

Schritt 3: Verknüpfen Sie Ihr Telefon

1. Klicken Sie auf **Gerät verknüpfen**. Ein QR-Code erscheint auf dem Bildschirm.
2. Öffnen Sie auf Ihrem Telefon **WhatsApp**, gehen Sie zu **Verknüpfte Geräte** und wählen Sie ein neues Gerät zum Verknüpfen.
3. Richten Sie das Telefon auf den QR-Code auf dem Bildschirm.

Während der Code angezeigt wird, prüft die Seite kontinuierlich, ob er gescannt wurde, und aktualisiert den Code automatisch. Wenn das Telefon bestätigt, ändert sich der Status zu **Verbunden**.

> **Der QR-Code wartet nicht ewig.** Wenn er nicht innerhalb kurzer Zeit gescannt wird, wird die Verknüpfung abgebrochen und die Seite kehrt zu **Getrennt** zurück. Öffnen Sie das Telefon auf dem Bildschirm **Verknüpfte Geräte**, bevor Sie auf **Gerät verknüpfen** klicken, und klicken Sie einfach erneut darauf, wenn der Code abläuft.

Sie können den Vorgang auch selbst mit **Verknüpfung abbrechen** stoppen.

Schritt 4: Entscheiden Sie, was mit Nicht-WhatsApp-Empfängern geschieht

Sobald der Status **Verbunden** ist, erscheint ein Feld **Fallback** mit einem Schalter:

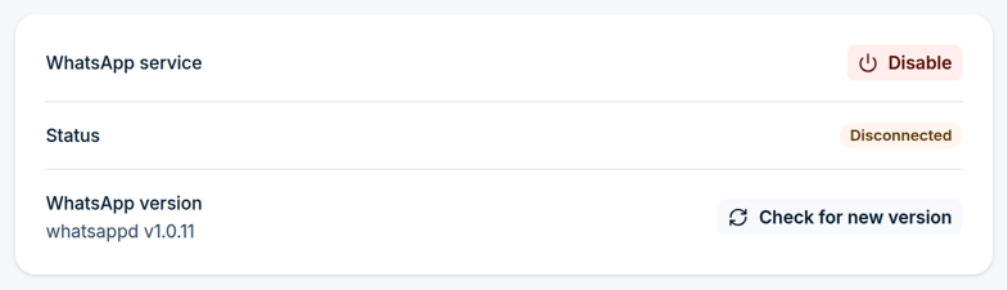
Fallback auf SMS/MMS Wenn diese Option aktiviert ist, wird eine Nachricht an eine Nummer, die nicht in WhatsApp registriert ist, stattdessen als SMS oder MMS versendet. Wenn sie deaktiviert ist, wird eine solche Nachricht einfach nicht zugestellt.

Der Schalter wird gespeichert, sobald Sie ihn umschalten. Es gibt keine separate Schaltfläche zum Speichern.

Schritt 5: Halten Sie den Dienst auf dem neuesten Stand

Das Feld **Verbindung** hat eine Schaltfläche **Nach neuer Version suchen**. Klicken Sie darauf, um zu fragen, ob eine neuere WhatsApp-Version verfügbar ist:

Ergebnis	Was zu tun ist
Keine neue Version gefunden	Nichts. Sie sind aktuell.
Eine neue Version ist verfügbar	Die Schaltfläche wird zu **Jetzt aktualisieren**, die Sie zur Patch-Seite führt, auf der das Update installiert werden kann.
Konnte die neueste Version nicht abrufen	Das Gerät konnte den Update-Server nicht erreichen. Überprüfen Sie die Netzwerkeinstellungen und versuchen Sie es später erneut.



Das Verbindungsfeld mit **Nach neuer Version suchen** neben der installierten Version

Verknüpfung aufheben und Ausschalten

Zwei Schaltflächen unten auf der Einstellungsseite tun unterschiedliche Dinge:

Schaltfläche	Funktion
Gerät trennen	Meldet das Konto ab. Der Service läuft weiter, die Seite wechselt zu **Disconnected** und Sie können ein anderes Konto verknüpfen. **Fall back to SMS/MMS** wird gleichzeitig deaktiviert.
Deaktivieren	Beendet den WhatsApp-Service vollständig. Der Kanal verschwindet aus dem Fenster „Verfassen

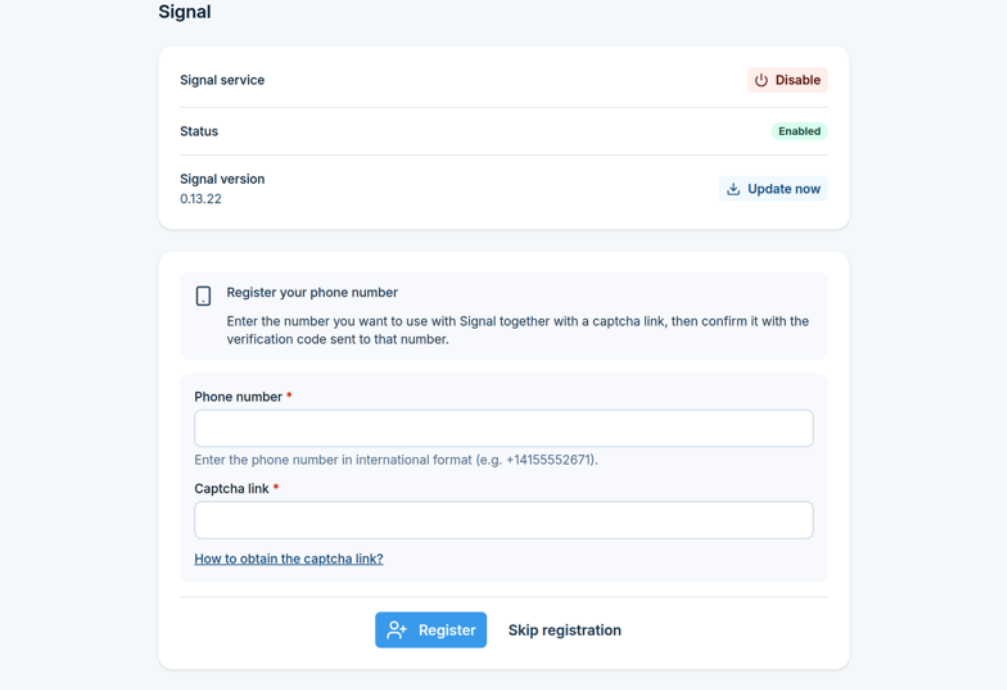
Sie können die Verknüpfung auch von der Telefonseite aus trennen, unter **WhatsApp > Linked devices**. Die Seite zeigt dann beim nächsten Aktualisieren **Disconnected** an.

Wichtig zu wissen

- WhatsApp-Nachrichten nutzen die Netzwerkverbindung und verbrauchen daher kein SIM-Guthaben und hängen nicht von der GSM-Abdeckung ab. Die Option **Fall back to SMS/MMS** ist die Ausnahme: diese Fallback-Nachrichten gehen über das Modem.

- Die Verknüpfung befindet sich auf dem Gerät. Das Wiederherstellen einer Sicherung auf anderer Hardware oder das Trennen vom Telefon erfordert das Scannen eines neuen QR-Codes.
- Nur Nachrichten, die empfangen werden, nachdem das Gerät verknüpft wurde, werden in der Konversationsliste angezeigt.

Signal



Signal-Serviceeinstellungen

Was diese Funktion tut

Signal-Unterstützung ermöglicht es Ihrem SMSEagle, zusätzlich zu SMS **Signal-Nachrichten** zu senden und zu empfangen. Das Gerät registriert sich im Signal-Netzwerk mit einer Telefonnummer, und danach wird Signal ein weiterer Kanal, den Sie beim Verfassen einer Nachricht auswählen können, mit eigener Konversationsansicht.

Typische Anwendungen: Erreichen Sie Menschen, die Signal gegenüber SMS bevorzugen, oder versenden Sie Warnmeldungen an Empfänger im Ausland, um Roaming-Gebühren zu sparen.

Die Einrichtung besteht aus zwei Teilen: Zuerst aktivieren Sie den Service und registrieren eine Nummer (**Settings > Channels > Signal**), dann nutzen Sie den Kanal (**Messages > Signal** oder das Fenster „Verfassen ,).

Bevor Sie beginnen

- Signal ist nur auf ausgewählten Gerätemodellen verfügbar. Wenn **Settings > Channels > Signal** nicht in Ihrer Seitenleiste angezeigt wird, unterstützt Ihr Gerät Signal nicht.

- Sie benötigen eine Telefonnummer, die einen Verifizierungscode empfangen kann, und diese darf nicht bereits bei Signal auf einem anderen Gerät registriert sein.
- Die Registrierung erfordert einen **Captcha-Link**, den Sie in einem Browser generieren. Halten Sie den Link bereit, bevor Sie beginnen; er verfällt schnell.

Schritt 1: Öffnen Sie die Signal-Einstellungen

Gehen Sie in der Seitenleiste zu **Settings > Channels > Signal**.

Das Feld **Service** oben zeigt die installierte **Signal version** und den aktuellen **Status** an. Auf einem neuen Gerät ist der Status **Disabled** und eine Warnung erklärt, dass der Service aktiviert werden muss, bevor eine Nummer registriert werden kann.

Schritt 2: Aktivieren Sie den Dienst

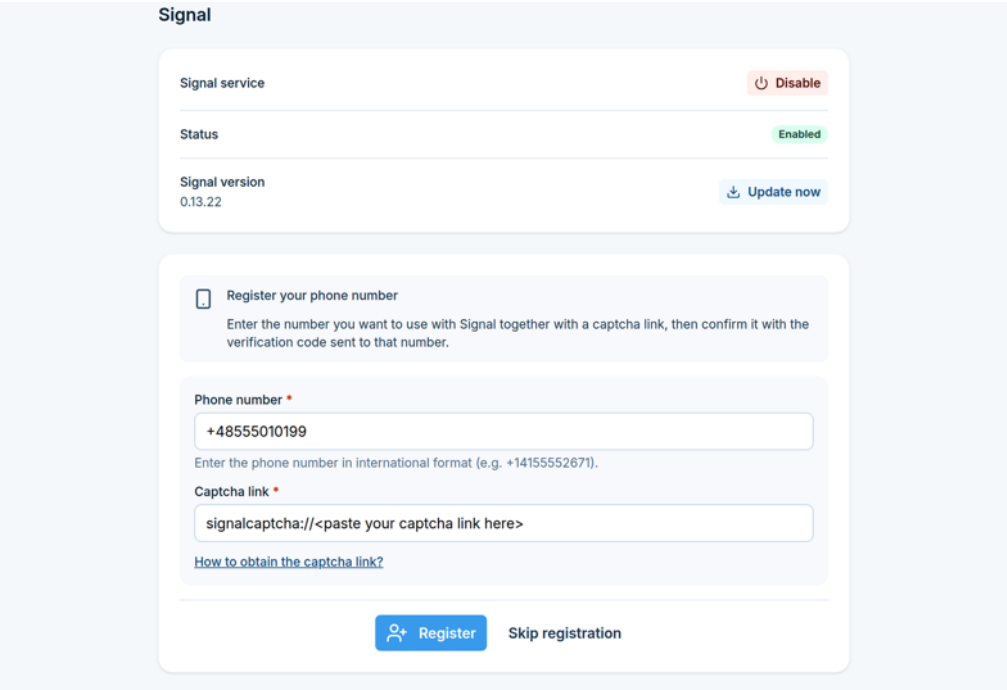
Klicken Sie **Enable** am unteren Ende der Seite. Der Status wechselt zu **Enabled** und das Registrierungsformular wird angezeigt, wie in der Abbildung am Anfang dieses Abschnitts.

Schritt 3: Registrieren Sie eine Telefonnummer

Im Feld **Register a phone number**:

1. Geben Sie in **Phone number** die Nummer im internationalen Format ein, zum Beispiel `+14155552671`.
2. Fügen Sie in **Captcha link** den Captcha-Link ein. Der Link **How to obtain the captcha link?** unter dem Feld öffnet Schritt-für-Schritt-Anweisungen in einem neuen Tab.
3. Klicken Sie **Register**.

Signal sendet daraufhin einen Verifizierungscode an die Nummer.



Registrierung einer Telefonnummer

Diese Nummer bereits kürzlich registriert? Klicken Sie stattdessen auf **Registrierung überspringen**. Das Formular springt direkt zum Verifizierungsschritt, wo Sie einen bereits erhaltenen Code eingeben können.

Schritt 4: Nummer verifizieren

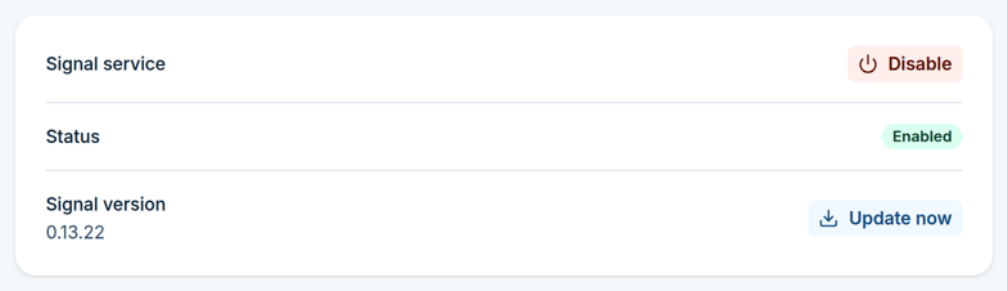
Das Formular fordert nun den **Verifizierungscode** an. Geben Sie den erhaltenen Code ein und klicken Sie auf **Verifizieren**.

Bei Erfolg zeigt die Seite an, dass Signal verbunden ist, und zeigt das Feld **Registrierte Nummer**.

Schritt 5: Halten Sie den Dienst auf dem neuesten Stand

Das Feld **Service** hat eine Schaltfläche **Nach neuer Version suchen**. Klicken Sie darauf, um zu prüfen, ob eine neuere Signal-Version verfügbar ist:

Ergebnis	Was zu tun ist
Keine neue Version gefunden	Nichts. Sie sind aktuell.
Eine neue Version ist verfügbar	Die Schaltfläche wird zu **Jetzt aktualisieren**, die Sie zur Patch-Seite führt, auf der das Update installiert werden kann.
Konnte die neueste Version nicht abrufen	Das Gerät konnte den Update-Server nicht erreichen. Überprüfen Sie die Netzwerkeinstellungen und versuchen Sie es später erneut.

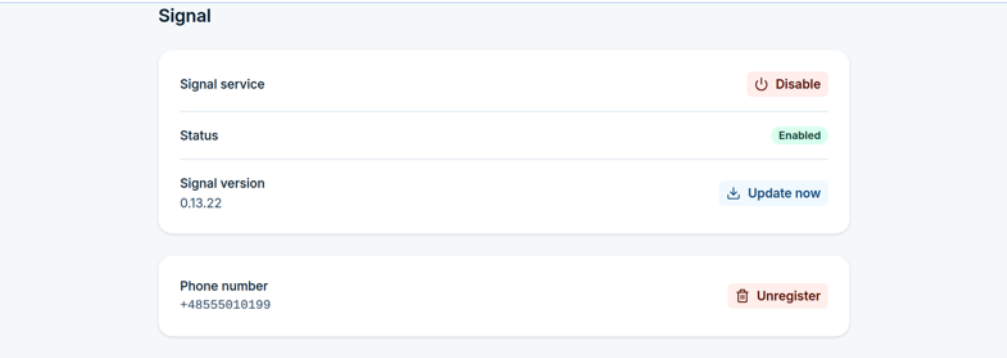


Das Service-Feld. Hier hat eine Überprüfung bereits eine neuere Version gefunden, daher lautet die Schaltfläche **Jetzt aktualisieren**

Entfernung der Nummer

Um die Registrierung des Geräts von Signal aufzuheben, gehen Sie zurück zu **Settings > Channels > Signal** und klicken Sie auf **Unregister** im Feld **Registered number**. Die Nummer wird freigegeben und die Seite kehrt zum Registrierungsformular zurück.

Um den Kanal zu deaktivieren, ohne die Registrierung aufzuheben, klicken Sie am unteren Ende der Seite auf **Disable**. Der Service stoppt und Signal verschwindet aus dem Fenster „Compose“, aber die Registrierung bleibt erhalten, sodass das erneute Aktivieren keine neue Verifizierung erfordert.



Eine registrierte Signal-Nummer

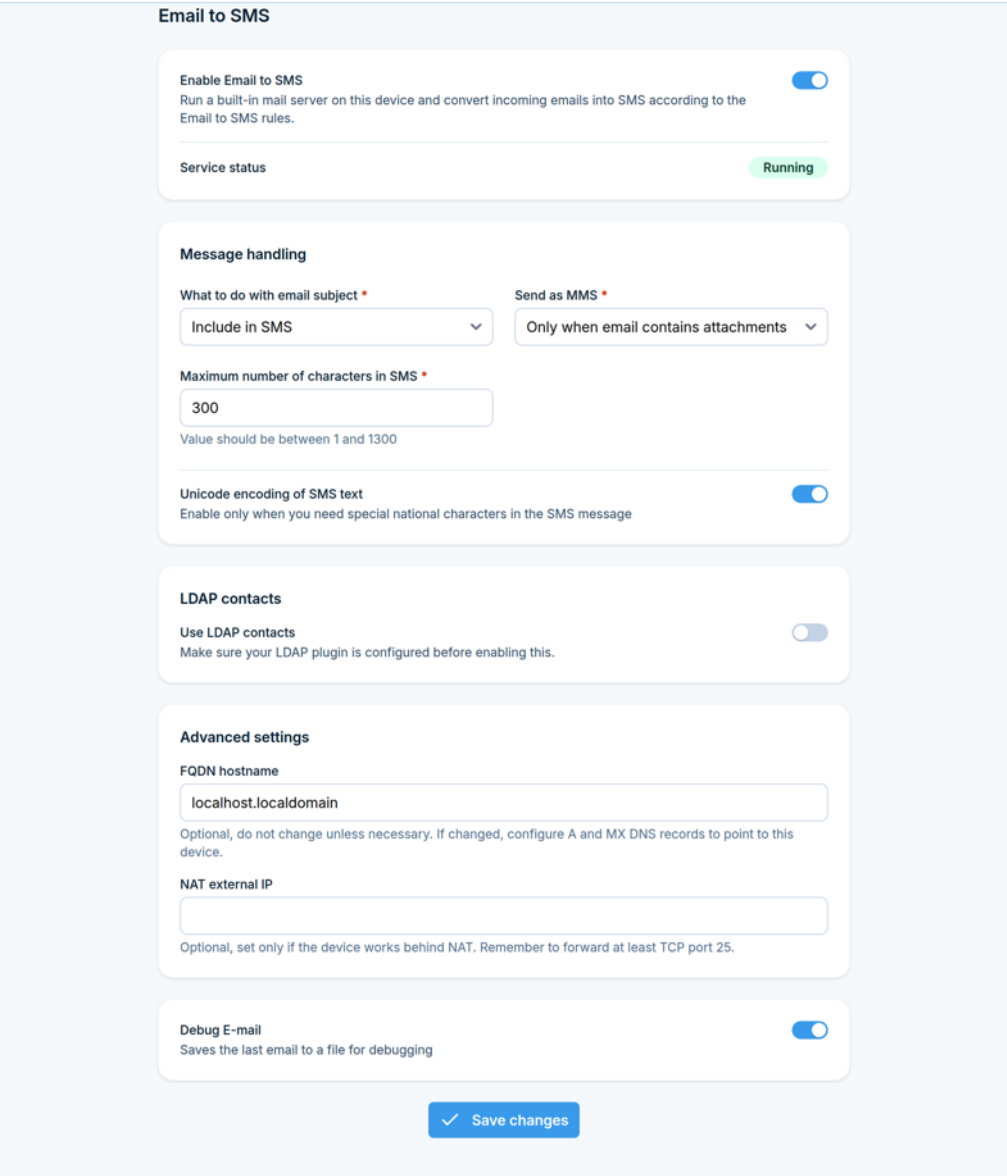
Wichtig zu wissen

- Signal-Nachrichten werden über die Netzwerkverbindung gesendet, nicht über das Modem, daher verwenden sie nicht das SIM-Guthaben und hängen nicht von der GSM-Abdeckung ab.
- Die Registrierung befindet sich auf dem Gerät. Das Wiederherstellen einer Sicherung auf verschiedener Hardware oder das Entfernen der Nummer erfordert eine erneute Registrierung.
- Nur Nachrichten, die nach der Aktivierung des Service empfangen wurden, erscheinen in der Konversationsliste.

Email

E-Mail zu SMS

Einstellungen > Kanäle > E-Mail > E-Mail zu SMS (`/settings/email/email-to-sms`) startet einen integrierten Mailserver auf dem Gerät und konvertiert eingehende E-Mails gemäß den von Ihnen unter E-Mail zu SMS in Automation definierten Regeln in SMS.



E-Mail-zu-SMS-Einstellungen

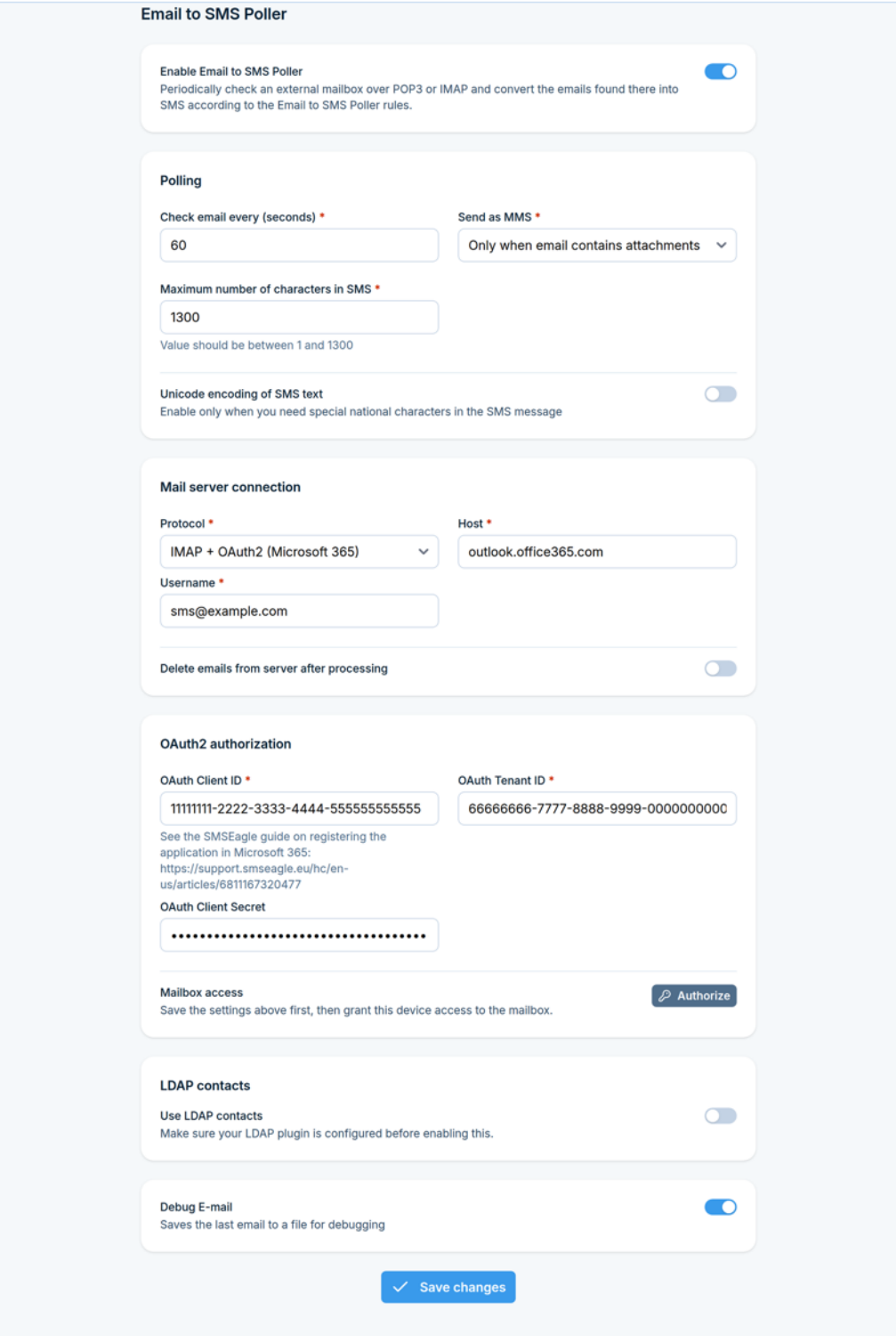
Aktivieren Sie **Enable Email to SMS**, um den Mailserver zu starten. **Service status** zeigt an, ob er **Running** oder **Stopped** ist. Der Rest der Seite bestimmt, wie eine E-Mail zu einer SMS wird:

- **What to do with email subject** - **Ignore** (ignorieren), **Include in SMS** (in SMS einbeziehen), **Use for authentication** (für Authentifizierung verwenden) oder **Send only subject without email body** (nur Betreff ohne E-Mail-Text senden).
- **Send as MMS** - **Never** (niemals), **Always** (immer) oder **Only when email contains attachments** (nur wenn E-Mail Anhänge enthält).
- **Maximum number of characters in SMS** - von 1 bis 1300.
- **Unicode encoding of SMS text** - aktivieren Sie es nur, wenn Nachrichten Sonderzeichen benötigen, die das Standard-SMS-Alphabet nicht unterstützt.
- **Use LDAP contacts** - ermöglicht es dem Empfängerteil der Adresse, einen Verzeichniskontakt oder eine Gruppe zu benennen. Konfigurieren Sie zunächst LDAP.

- **FQDN hostname** (unter **Advanced settings**) - optionaler Domänenname zur Verwendung in Empfängeradressen anstelle der IP-Adresse des Geräts. Wenn Sie ihn ändern, richten Sie die A- und MX-DNS-Einträge für diesen Namen auf das Gerät.
- **NAT external IP** - setzen Sie dies nur, wenn sich das Gerät hinter NAT befindet, und leiten Sie mindestens TCP-Port 25 zum Gerät weiter.
- **Debug E-mail** - speichert die zuletzt empfangene E-Mail in einer Datei zur Fehlerbehebung.

Email to SMS Poller

Einstellungen > Kanäle > E-Mail > E-Mail zu SMS Poller (`/settings/email/email-to-sms-poller`) verbindet das Gerät mit einem vorhandenen Postfach, überprüft es in regelmäßigen Abständen und konvertiert die gefundenen E-Mails gemäß den Regeln unter E-Mail zu SMS Poller in Automation in SMS. Anders als bei E-Mail zu SMS müssen keine E-Mails zum Gerät selbst zugestellt werden.



E-Mail-zu-SMS-Poller-Einstellungen, verbunden mit einem Microsoft-365-Postfach

Aktivieren Sie **Enable Email to SMS Poller**. Das folgende Formular hat diese Teile:

Polling

- **Check email every (seconds)** - wie oft das Postfach überprüft wird.
- **Send as MMS**, **Maximum number of characters in SMS** und **Unicode encoding of SMS text** - gleiche Bedeutung wie bei E-Mail zu SMS.

Mail server connection

- **Protocol** - **POP3**, **IMAP** oder **IMAP + OAuth2 (Microsoft 365)**.
- **Host** und **Username** des Postfachs.
- Nur bei **POP3** und **IMAP**: **Port**, **Password** und **Use TLS/SSL encryption**. Die Seite listet die Standard-Ports auf: POP3 110, POP3 mit TLS/SSL 995, IMAP 143, IMAP mit TLS/SSL 993.
- **Delete emails from server after processing** - entfernt jede E-Mail aus dem Postfach, nachdem sie verarbeitet wurde. Lassen Sie diese Option deaktiviert, um das Postfach unverändert zu lassen.

OAuth2 authorization (nur bei **IMAP + OAuth2 (Microsoft 365)**)

- **OAuth Client ID**, **OAuth Tenant ID** und **OAuth Client Secret** der in Microsoft 365 registrierten Anwendung. Siehe SMSEagle-Anleitung zur Registrierung der Anwendung in Microsoft 365.
- Speichern Sie die Einstellungen zunächst, klicken Sie dann unter **Mailbox access** auf **Authorize** und gewähren Sie dem Gerät Zugriff auf das Postfach.

Use LDAP contacts und **Debug E-mail** funktionieren wie bei E-Mail zu SMS.

Für POP3 und IMAP enthält die Seite auch eine Schaltfläche **Test connection**. Speichern Sie die Einstellungen, bevor Sie diese verwenden. Einige E-Mail-Provider blockieren IMAP-Testverbindungen unter ihren Standard-Sicherheitseinstellungen, daher bedeutet ein fehlgeschlagener Test nicht immer, dass die Einstellungen falsch sind.

SMTP-Konfiguration

Settings > Channels > Email > SMTP Configuration (`/settings/email/smtp`) verwaltet eine Liste wiederverwendbarer SMTP-Server-Voreinstellungen und weist jedem Feature, das ausgehende E-Mails sendet, eine zu:

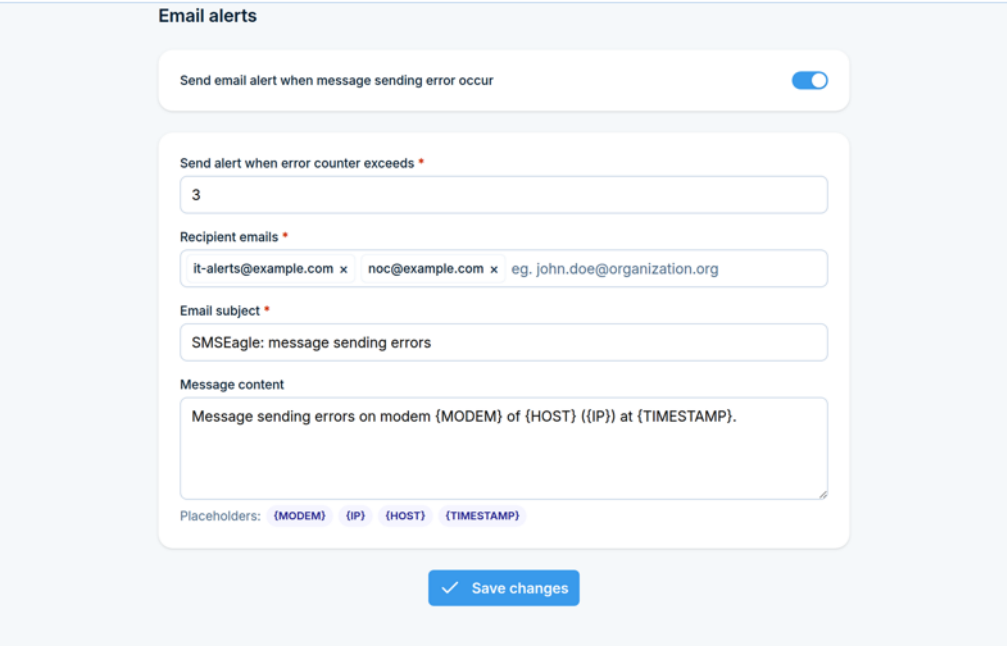
- **Compose menu**, **APIv2**, **SMS to Email**, **Alerts**, **Reporting module**, **Workflows**

Jedes dieser Features kann auf **None** oder auf eine Ihrer gespeicherten Voreinstellungen gesetzt werden. Das Aufheben der Zuweisung einer Voreinstellung zu einem Feature deaktiviert die bestehende E-Mail-Konfiguration dieses Features.

Klicken Sie auf **Create new** unter **Configuration presets**, um einen SMTP-Server hinzuzufügen (Host, Port, Verschlüsselung, Absenderadresse, Anmeldedaten); Voreinstellungen können dann aus der Dropdown-Liste für eines der oben aufgeführten Features ausgewählt werden.

E-Mail-Benachrichtigungen

Einstellungen > Kanäle > E-Mail > Email alerts (`/settings/email/alerts`) versendet einen Alert per E-Mail, wenn ausgehende Nachrichten weiterhin nicht versendet werden können. Dazu muss unter SMTP Configuration eine SMTP-Voreinstellung für **Alerts** zugewiesen werden.



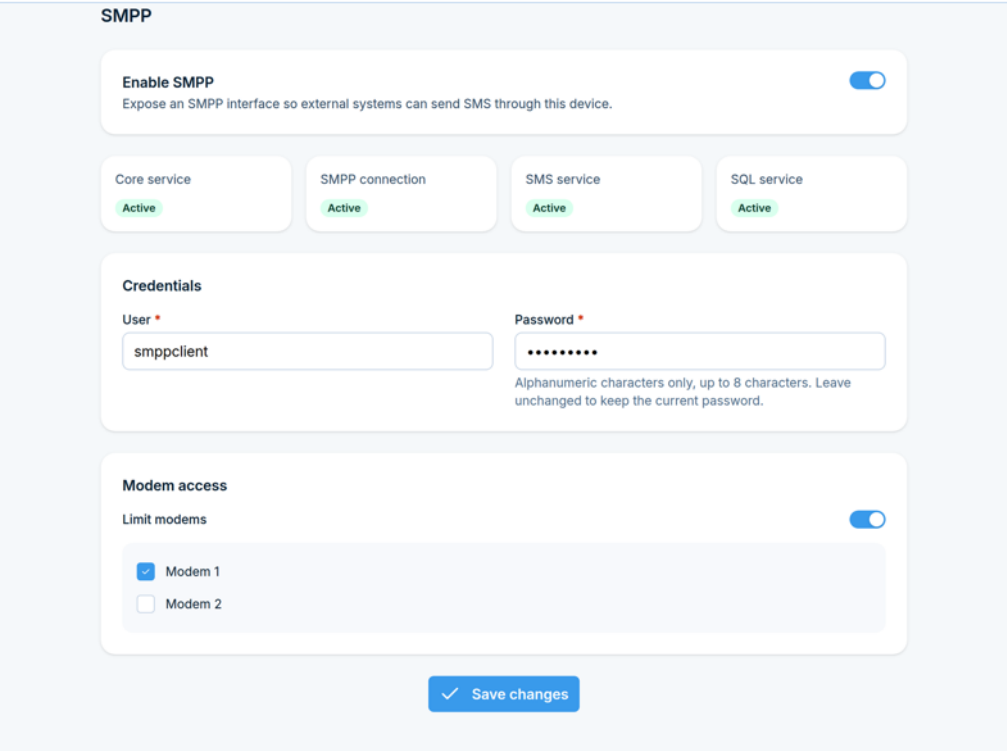
E-Mail-Benachrichtigungseinstellungen

Aktivieren Sie **E-Mail-Benachrichtigung bei Nachrichtensendungsfehlern senden**, dann stellen Sie Folgendes ein:

- **Benachrichtigung senden, wenn Fehler-Zähler übersteigt** – wie viele Sendefehler gezählt werden, bevor die Benachrichtigung gesendet wird. Ein Wert über 2 vermeidet Benachrichtigungen, die durch einen einzelnen temporären Fehler verursacht werden.
- **Empfänger-E-Mails** – eine oder mehrere Adressen.
- **E-Mail-Betreff** und **Nachrichteninhalt** – der Text der Benachrichtigung. Die Platzhalter **{MODEM}** (das Modem, das die Benachrichtigung ausgelöst hat), **{IP}** (die IP-Adresse des Geräts), **{HOST}** (sein Hostname) und **{TIMESTAMP}** (wenn der Fehler erkannt wurde) werden durch echte Werte ersetzt. Klicken Sie auf einen Platzhalter unter dem Nachrichtenfeld, um ihn einzufügen.

SMPP

Settings > Channels > SMPP (`/settings/smpp/`) aktiviert den integrierten SMPP-Server des Geräts. Eine externe Anwendung, die als SMPP-Client fungiert, kann dann SMS über die Modems des Geräts einreichen und empfängt eingehende SMS und Lieferberichte über dieselbe Verbindung zurück.



SMPP-Einstellungen, hier auf einem Gerät mit zwei Modems dargestellt. NXS-9700 listet ein Modem auf

Verbindungsdetails

Parameter	Wert
Protokoll	SMPP 3.4
Port	TCP 2770
Client zu SMSEagle	SMS, die über die Modems des Geräts gesendet werden sollen
SMSEagle zu Client	Eingehende SMS und Lieferberichte

Der SMPP-Client verbindet sich mit **User** und **Password**, die auf dieser Seite als `system_id` und `password` festgelegt sind.

Eingehende SMS und Lieferberichte werden in der Warteschlange des Geräts gespeichert, während kein SMPP-Client verbunden ist. Sobald sich ein Client verbindet, stellt SMSEagle alles in dieser Warteschlange bereit, daher muss der Client bereit sein, `deliver_sm`-Meldungen vom Moment der Verbindung an zu empfangen und zu bestätigen.

SMPP aktivieren

1. Aktivieren Sie **Enable SMPP**. Die Service-Statuskarten, **Credentials** und **Modem access** werden angezeigt.

2. Unter **Credentials** stellen Sie **User** und **Password** ein, mit denen sich der SMPP-Client verbindet. Das Passwort kann nur Buchstaben und Ziffern enthalten, maximal 8 Zeichen. Wenn ein Passwort bereits gespeichert ist, lassen Sie das Feld unverändert, um es beizubehalten.
3. Lassen Sie **Limit modems** unter **Modem access** deaktiviert. NXS-9700 hat ein einzelnes integriertes Modem, daher verwendet der gesamte SMPP-Datenverkehr ohnehin dieses.
4. Klicken Sie auf **Save changes**.

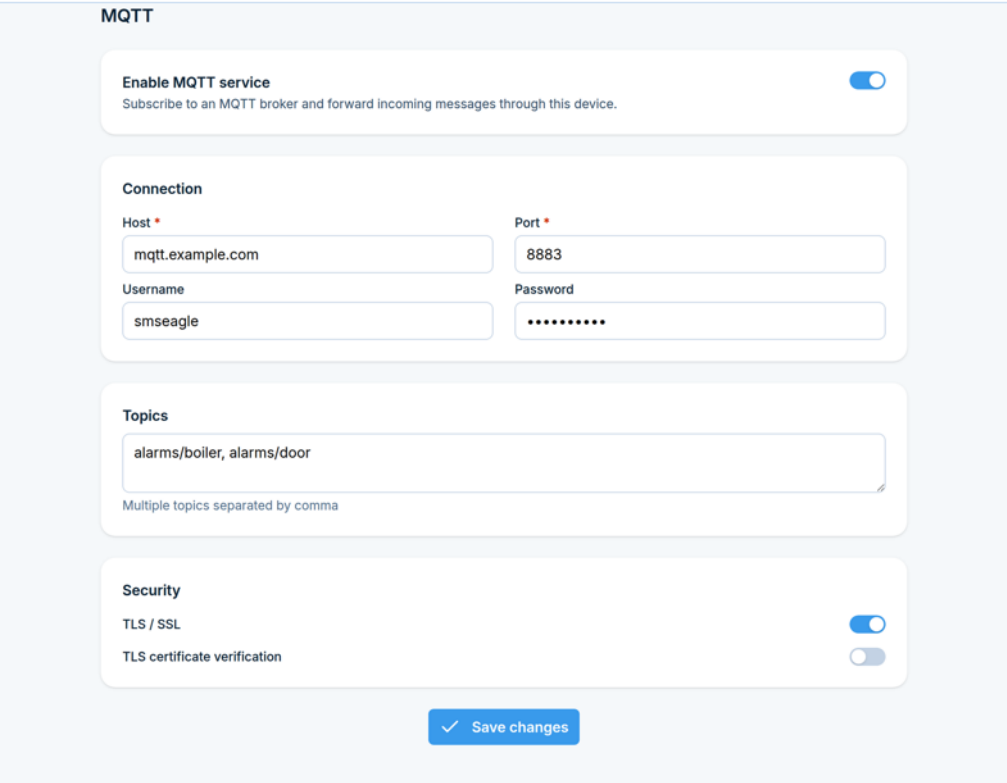
   Ein Neustart ist erforderlich. Nach dem Speichern fordert SMSEagle Sie auf, das Gerät neu zu starten, damit die SMPP-Änderungen wirksam werden. Bis dahin werden die neuen Einstellungen gespeichert, aber noch nicht verwendet. Verwenden Sie **System > Restart**, wenn Sie bereit sind.

Nach dem Neustart zeigen die vier Statuskarten (**Core service**, **SMPP connection**, **SMS service**, **SQL service**), ob jeder Teil des SMPP-Servers ausgeführt wird. Alle vier müssen **Active** anzeigen, damit sich SMPP-Clients verbinden und Nachrichten austauschen können.

Wenn Sie SMPP zum ersten Mal aktivieren, erstellt SMSEagle auch einen internen Benutzer für SMPP-Datenverkehr mit seinem eigenen API-Schlüssel unter **Settings > API v2 keys**, und die internen Regeln, die eingehende SMS und Lieferberichte an den SMPP-Client weitergeben. Widerrufen oder bearbeiten Sie diese nicht. Das Deaktivieren von SMPP entfernt den Benutzer und die Regeln erneut.

MQTT

Settings > Channels > MQTT (`/settings/mqtt/`) verbindet das Gerät mit dem MQTT-Broker, den es abhört. Die Subscribe-Regeln unter MQTT in Automation, die MQTT-Meldungen in SMS umwandeln, verwenden diese Verbindung. Publish-Regeln tun dies nicht: jede von ihnen benennt ihren eigenen Broker.



MQTT-Broker-Verbindungseinstellungen

Schalten Sie **Enable MQTT service** ein und stellen Sie dann folgende Werte fest:

- **Host** und **Port** des Brokers (beide erforderlich).
- **Username** und **Password**, falls der Broker diese erfordert.
- **Topics** – die Topics, auf die sich das Gerät abonniert, durch Kommas getrennt.
- **TLS / SSL** – verschlüsselt die Verbindung zum Broker. **TLS certificate verification** überprüft auch das Zertifikat des Brokers. Schalten Sie es nur für einen Broker mit selbstsigniertem Zertifikat aus.

Klicken Sie auf **Save changes**.

> **Ein Neustart ist erforderlich.** Nach dem Speichern fordert SMSEagle Sie auf, das Gerät neu zu starten, damit die MQTT-Änderungen wirksam werden. Bis dahin werden die neuen Einstellungen gespeichert, sind aber noch nicht aktiv. Verwenden Sie **System > Restart**, wenn Sie bereit sind.

Netzwerk

IP-Einstellungen

Einstellungen > Globale Einstellungen > Netzwerk > IP-Einstellungen (`/settings/network/ip`) zeigt die **MAC-Adresse** des Geräts (schreibgeschützt) an und ermöglicht die Konfiguration von:

- **Get IP address from DHCP** - DHCP aktivieren oder deaktivieren, um eine statische IP zu setzen.

- **Hostname**
- **Use proxy** - Leiten Sie die ausgehenden Verbindungen des Geräts über einen HTTP-Proxy weiter.
- **IP address restriction** - **Allow**, **Deny** oder **Disabled**, mit einer Liste von IP-Adressen, auf die die Regel angewendet wird. Wenn die Beschränkung aktiv ist, werden alle Ports außer 22 (SSH) für alle blockiert, die nicht auf der Liste stehen.

  Seien Sie vorsichtig mit IP-Adressenbeschränkung. Eine falsch konfigurierte Allow-Liste kann Sie vom Web-Interface auf Ihrem eigenen Computer aussperren. Fügen Sie zuerst Ihre aktuelle IP hinzu (die Seite bietet eine **Add your IP address**-Verknüpfung) bevor Sie speichern.

SSL

Einstellungen > Globale Einstellungen > Netzwerk > SSL (`/settings/network/ssl`) ermöglicht es, das Standard-Self-Signed-Zertifikat des Geräts durch Ihr eigenes zu ersetzen: Laden Sie ein **Certificate**, seinen **Private key** und optional ein **Root CA certificate** und **Full chain** hoch. Ein separater Schalter, **Forward HTTP to HTTPS**, leitet einfache HTTP-Anfragen zu HTTPS weiter.

Failover

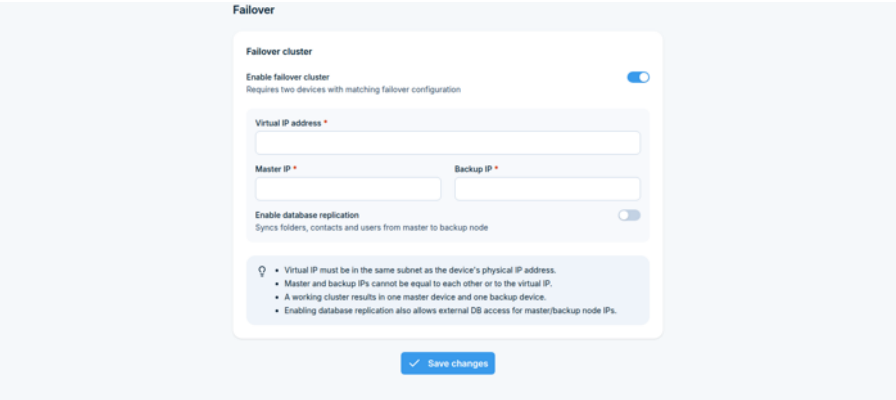
Der Failover-Cluster bietet Hochverfügbarkeit auf Geräteebene: Ein zweites SMSEagle-Gerät steht als Sicherung bereit und übernimmt, wenn das Master-Gerät nicht mehr reagiert.

Wo Sie dies finden

Einstellungen > Globale Einstellungen > Netzwerk > Failover (`/settings/network/failover`).

Failover-Cluster aktivieren

Schalten Sie **Enable failover cluster** ein. Dies erfordert zwei Geräte mit übereinstimmender Failover-Konfiguration, eines als Master und eines als Backup.



Failover-Cluster-Einstellungen

Stellen Sie die gleichen Werte auf beiden Geräten ein:

- **Virtual IP address** – die Adresse, mit der sich Ihre Benutzer und Integrationen verbinden.

- **Master IP** und **Backup IP** – die physischen IP-Adressen der beiden Geräte. Jedes Gerät übernimmt seine Rolle von seiner eigenen Adresse: Das Gerät, dessen IP mit **Master IP** übereinstimmt, wird der Master, das mit **Backup IP** übereinstimmende das Backup. Eine der beiden Adressen muss daher die Adresse des Geräts sein, das Sie konfigurieren.
- **Enable database replication** – kopiert Ordner, Kontakte und Benutzer vom Master-Knoten zum Backup-Knoten (siehe unten).

Klicken Sie auf **Save changes**.

> **Ein Neustart ist erforderlich.** Nach dem Speichern fordert SMSEagle Sie auf, das Gerät neu zu starten, damit die Failover-Änderungen wirksam werden. Bis dahin werden die neuen Einstellungen gespeichert, sind aber noch nicht aktiv. Verwenden Sie **System > Restart**, wenn Sie bereit sind.

Master-/Backup-Rollen und virtuelle IP

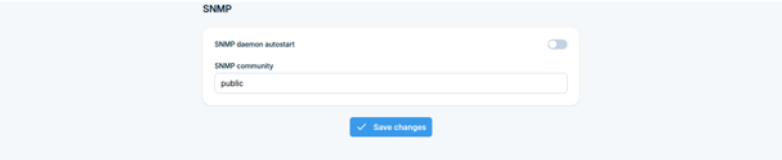
Der Cluster wird über eine einzelne **virtual IP address** erreicht, die immer auf das gerade aktive Gerät zeigt:

- Die virtuelle IP muss sich im gleichen Subnetz befinden wie die eigene physische IP-Adresse jedes Geräts.
- Die Master-IP, Backup-IP und virtuelle IP müssen alle unterschiedlich voneinander sein.
- Ein funktionierender Cluster hat zu jedem Zeitpunkt genau ein Master-Gerät und ein Backup-Gerät; wenn das Master-Gerät nicht mehr reagiert, übernimmt die Sicherung die virtuelle IP.

Datenbankreplikation und externer Zugriff

Das Aktivieren des Failover-Clusters ermöglicht auch die Datenbankreplikation zwischen dem Master und der Sicherung, so dass das Backup-Gerät bei Bedarf eine aktuelle Kopie von Nachrichten, Kontakten und Einstellungen hat. Diese gleiche Einstellung ermöglicht auch externen Datenbankzugriff speziell für die Master- und Backup-Knoten-IPs, was für die Replikation erforderlich ist.

SNMP



SNMP-Agent-Einstellungen

Der SNMP-Agent ermöglicht externen Tools (ein NMS, ein MIB-Browser oder ein einfacher `snmpget`/`snmpwalk`-Aufruf), SMSEagle nach seinen eigenen Metriken abzufragen – Signalstärke, Netzwerkname, Nachrichtenzählungen in Ordnern, Systemlaufzeit und mehr. Dies ist die entgegengesetzte Richtung zu SNMP Traps: Der Agent wird von einem externen Tool abgefragt, anstatt dass SMSEagle eine Warnung an einen schiebt.

Wo Sie dies finden

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

Konfiguration des SNMP-Agenten

Aktivieren Sie **SNMP daemon autostart**, damit der Agent automatisch mit dem Gerät startet, und legen Sie die **SNMP community**-Zeichenkette fest, die für die Authentifizierung von Leseanfragen verwendet wird.

Sobald aktiviert, können SMSEagles Erweiterungsparameter (Signalstärke, Netzwerkname, Ordnerzähler, Laufzeit und andere) vom MIB-Baum des Geräts mit jedem Standard-SNMP-Tool gelesen werden, beispielsweise NET-SNMP's `snmpget`/`snmpwalk` oder ein grafischer MIB-Browser.

Verfügbare Metriken

Zusätzlich zu den Standard-Linux-Host-Metriken veröffentlicht SMSEagle seine eigenen Metriken über NET-SNMP-EXTEND-MIB. Jede kann über ihre OID oder über ihren Namen als `NET-SNMP-EXTEND-MIB::nsExtendOutputFull."<metric name>"` gelesen werden.

Metriken, die ein Modem beschreiben, enden mit der Modem-Nummer. Das NXS-9700 hat ein Modem, daher enden diese Metriken mit `1`. Eine Metrik gibt `-1` zurück, wenn ihr Wert nicht gelesen werden kann, z. B. wenn das Modem ausgeschaltet ist oder der Temperatursensor nicht aktiviert ist.

Metrik	Gibt zurück
`GSM_Signal1`	Signalstärke des Modems in Prozent (0-100).
`GSM_NetName1`	Name des Mobilfunknetzes, bei dem das Modem registriert ist.
`GSM_ModemState1`	on oder `off`: ob das Modem unter Modems eingeschaltet ist.
`SIM_State1`	SIM-Kartenstatus wie vom Modem gemeldet: `READY`, wenn die SIM bereit ist, ansonsten der eigene Status des Modems wie `SIM PIN` oder `SIM PUK` oder ein Fehler wie `NOSIM`.
`SIM_RegState1`	Netzwerkregistrierung: `Registered Home`, `Registered Roaming`, `Searching`, `Not Registered`, `Denied`, `Registered Emergency`, `Unknown` oder `Unset`.
`SMSCountIn1`	Vom Modem heute empfangene SMS seit Mitternacht.
`SMSCountOut1`	Vom Modem heute gesendete SMS seit Mitternacht.
`FolderInbox_Total`	**Ungelesene** Nachrichten in Inbox. Eine mehrteilige Nachricht wird einmal gezählt.
`FolderOutbox_Total`	Nachrichten, die in der Warteschlange Outbox warten und gesendet werden sollen.
`FolderSent_Last24H`	Nachrichten, die in den letzten 24 Stunden gesendet wurden. Jeder Teil einer mehrteiligen Nachricht wird separat gezählt.
`FolderSent_Last1M`	Nachrichten, die im letzten Monat gesendet wurden, auf die gleiche Weise gezählt.
`FolderSent_Last24HSendErr`	Nachrichten, die in den letzten 24 Stunden nicht gesendet werden konnten, weil das Modem sie nicht senden konnte oder das Netzwerk sie abgelehnt hat.
`Temp`	Temperatur von Sensor 1 in °C. Gleicher Wert wie `Temp1`.
`Temp1`	Temperatur von Sensor 1 bis 4 (`Temp1` bis `Temp4`), in °C, in der Nummerierung der Temperatur- und Feuchtigkeitssensoren. Die folgende OID ist für `Temp1`.
`Humidity`	Feuchte von Sensor 1 in %.

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

Die OID einer beliebigen Metrik ist `.1.3.6.1.4.1.8072.1.3.2.3.1.2`, gefolgt von der Anzahl der Zeichen im Metrik-Namen und dem ASCII-Code jedes Zeichens. Die letzte Zahl einer Modem-Metrik-OID ist 48 plus die Modem-Nummer, weshalb die Modem-Metriken oben mit `.49` enden.

Wenn Ihr SNMP-Tool die NET-SNMP-EXTEND-MIB-Namen nicht kennt, laden Sie die MIB-Definitionsdatei.

Metriken auslesen

Ersetzen Sie `public` durch Ihre **SNMP-Community** und `192.0.2.10` durch die IP-Adresse des Geräts.

Eine Metrik nach OID auslesen:

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

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

Eine Metrik nach Name auslesen:

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

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

Alle SMSEagle-Metriken auf einmal auflisten:

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

Was aus dem Netzwerk ausgelesen werden kann

Abfragen vom Gerät selbst (`localhost`) sehen den gesamten MIB-Baum. Abfragen von anderen Hosts sehen einen eingeschränkten Teil davon: die oben aufgeführten SMSEagle-Metriken und aus den Standard-MIBs die Systemgruppe (einschließlich Betriebszeit), Netzwerkschnittstellen, Speicher, Prozessoren, Arbeitsspeicher, Last und CPU-Auslastung. Die Prozessliste und andere Details werden nicht ins Netzwerk übertragen.

Die gleiche **SNMP-Community** gilt für beide. Nachdem Sie sie ändern, starten Sie das Gerät neu, damit der neue Wert wirksam wird.

SNMP v3 verwenden

Die Seite konfiguriert SNMP v1/v2c. Für SNMP v3 mit Authentifizierung und Verschlüsselung verwenden Sie das Skript `snmpv3` über SSH:

1. Melden Sie sich über SSH als `root` beim Gerät an.
2. Gehen Sie zum SMSEagle-Verzeichnis:

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

3. Fügen Sie einen schreibgeschützten SNMP v3-Benutzer hinzu. Er verwendet SHA für die Authentifizierung und AES für die Verschlüsselung. Beide Passwörter müssen mindestens 8 Zeichen lang sein.

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

4. Optional können Sie den SNMP v1/v2c-Zugriff deaktivieren, sodass nur SNMP v3-Benutzer den Agent lesen können:

   ```
   ./snmpv3 disablev2
   ```

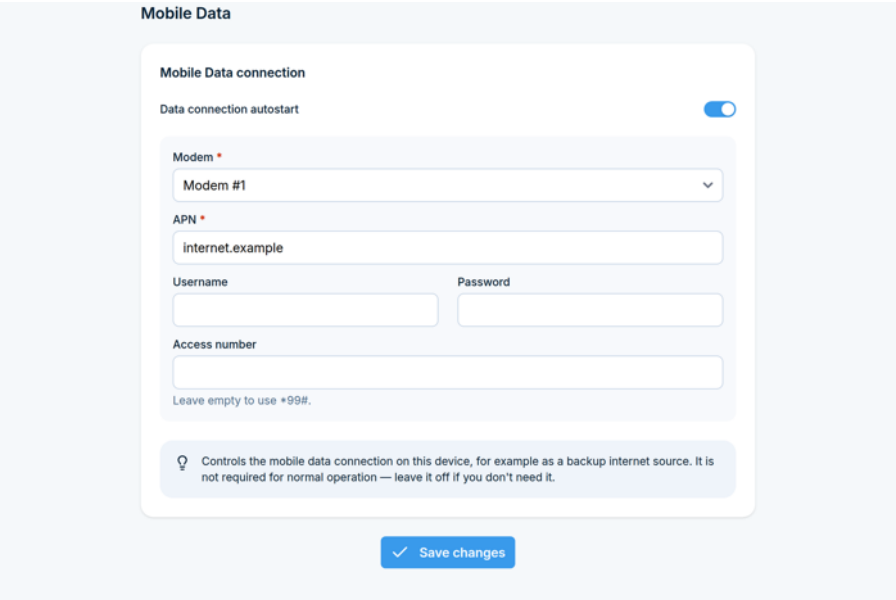
   `./snmpv3 enablev2` aktiviert es wieder, und `./snmpv3 del USERNAME` entfernt den Benutzer.

Das Skript startet den SNMP-Agent selbst neu. Eine v3-Abfrage sieht dann so aus:

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

Mobile Daten

Settings > Global settings > Network > Mobile Data (`/settings/network/mobile-data`) steuert eine Mobilfunkdatenverbindung über eines der Modems des Geräts, z. B. als Backup-Internetquelle. Sie ist nicht erforderlich zum Senden oder Empfangen von SMS. Lassen Sie sie ausgeschaltet, falls Sie sie nicht benötigen.



Mobile Data-Einstellungen, hier auf einem Gerät mit zwei Modems dargestellt. NXS-9700 hat kein **Modem**-Feld

Schalten Sie **Data connection autostart** ein und stellen Sie dann folgende Werte fest:

- **APN** des Betreibers der SIM (erforderlich) und **Username** und **Password**, falls der Betreiber diese erfordert.
- **Access number** – lassen Sie es leer, um `*99#` zu verwenden.

Klicken Sie auf **Save changes**.

> **Ein Neustart ist erforderlich.** Nach dem Speichern fordert SMSEagle Sie auf, das Gerät neu zu starten, damit die Änderungen der Mobilfunkdaten wirksam werden. Bis dahin werden die neuen Einstellungen gespeichert, sind aber noch nicht aktiv. Verwenden Sie **System > Restart**, wenn Sie bereit sind.

Anwendung

Settings > Global settings > Application (`/settings/application/`) enthält geräteweit gültiges Verhalten, das nicht unter einen einzelnen Kanal oder eine einzelne Funktion passt, gruppiert in vier Abschnitte:

Regional

Language (geräteweit gültige Standardeinstellung) und **Country dial code** (verwendet, wenn eine Telefonnummer ohne diesen eingegeben wird).

Sicherheit

- **Force MFA** - For all users, For new users, oder Do not force (gleiche Wirkung wie die geräteweit gültige MFA-Einstellung des Assistenten, siehe MFA).
- **Password complexity verification** - erzwingen Sie die Kennwortregeln (Länge, gemischte Groß-/Kleinschreibung, Zahl, Sonderzeichen) für jeden Benutzer.
- **Access to DB for external applications** - ermöglicht direkten PostgreSQL-Zugriff für externe Anwendungen, standardmäßig deaktiviert. Vollständige Verbindungsdetails und Beispiel-SQL werden separat unter Advanced behandelt, da es sich dabei um ein eigenständiges Thema für Power-User handelt.

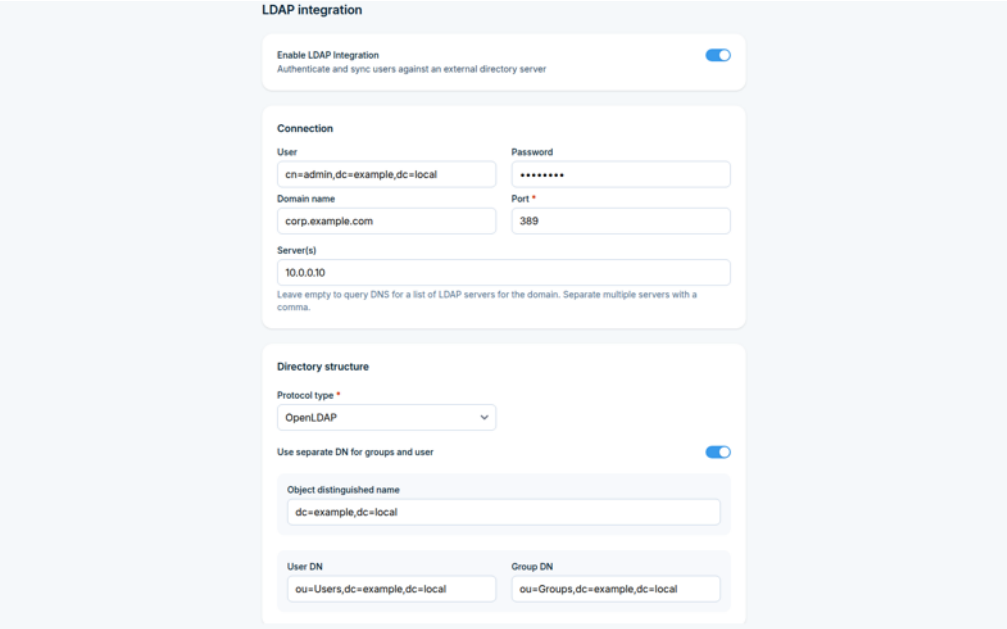
Zugriff und Sichtbarkeit

- **Inbox content visibility** - For all users, Only for admins, oder Only messages from the modems assigned to the user (Modems werden pro Benutzer in **System > Users** zugewiesen).
- **Email inbox content visibility** - For all users oder Only for admins.
- **Reporting module accessible for** - All users oder Only admins.

API und Integrationen

- **Save API logs** – protokolliert jeden API v1- und v2-Aufruf (Methode, Pfad und Parameter) in `/var/log/smseagle/api.log`. Zugriffstokens werden maskiert und Nachrichtentext wird ausgelassen. Die Datei wird nicht im Log-Browser unter **System > Logs** angezeigt, aber **Download logs** auf dieser Seite bezieht sie ein. Schalten Sie es ein, während Sie eine Integration einrichten oder debuggen.
- **Forward 3CX messages as unicode** – Nachrichten, die 3CX über den API v2 3CX-Endpunkt an SMSEagle sendet, werden als Unicode-SMS statt als Standard-SMS-Alphabet versendet. Schalten Sie es ein, wenn 3CX-Benutzer Nationalzeichen senden.

LDAP



LDAP-Integrationseinstellungen

Was diese Funktion tut

Die LDAP-Integration verbindet SMSEagle mit Ihrem Unternehmensverzeichnis, z. B. Active Directory oder OpenLDAP. Sie führt zwei separate Aufgaben durch, und Sie können beide oder eine nutzen:

Aufgabe	Was Sie bekommen
Kontakte	Das Telefonbuch wird aus dem Verzeichnis gefüllt, sodass Sie Nachrichten an dieselben Personen und Gruppen senden können, die Ihr Unternehmen bereits verwaltet, ohne Nummern zweimal einzutippen.
Authentifizierung	Benutzer melden sich bei SMSEagle mit ihrem Verzeichniskonto an, und ihre Berechtigung wird durch ihre Verzeichnisgruppentzugehörigkeit bestimmt.

Typische Anwendungen: Das Telefonbuch automatisch mit Personalveränderungen synchron zu halten und Benutzern die Verwendung ihres bestehenden Unternehmenspassworts anstelle eines separaten SMSEagle-Passworts zu ermöglichen.

Bevor Sie beginnen

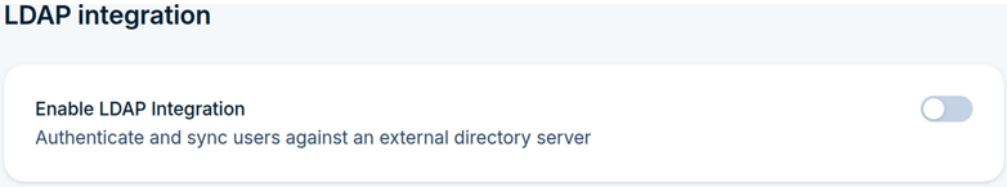
Sammeln Sie diese Informationen von demjenigen, der das Verzeichnis verwaltet:

- Der **Domänenname** und der **Port** (389 für einfaches LDAP, normalerweise 636 mit SSL).
- Ein **Dienstkonto** (Benutzer und Passwort), das das Verzeichnis lesen darf.
- Der **Distinguished Name** der Abteilung mit Ihren Benutzern, beispielsweise `ou=Users,dc=company,dc=local`, und die Abteilung mit Gruppen, falls unterschiedlich.
- Welches **Attribut** die Telefonnummer enthält, die Sie texten möchten.
- Falls Sie Verzeichnisanmeldung wünschen: die Namen der Gruppen, deren Mitglieder SMSEagle-Administratoren und reguläre Benutzer werden sollten.

Schritt 1: Öffnen Sie die LDAP-Seite

Gehen Sie in der Seitenleiste zu **Settings > Global settings > LDAP**.

Die Seite beginnt mit einem einzelnen Schalter, **Enable LDAP Integration**. Solange Sie ihn nicht einschalten, wird nichts anderes angezeigt.



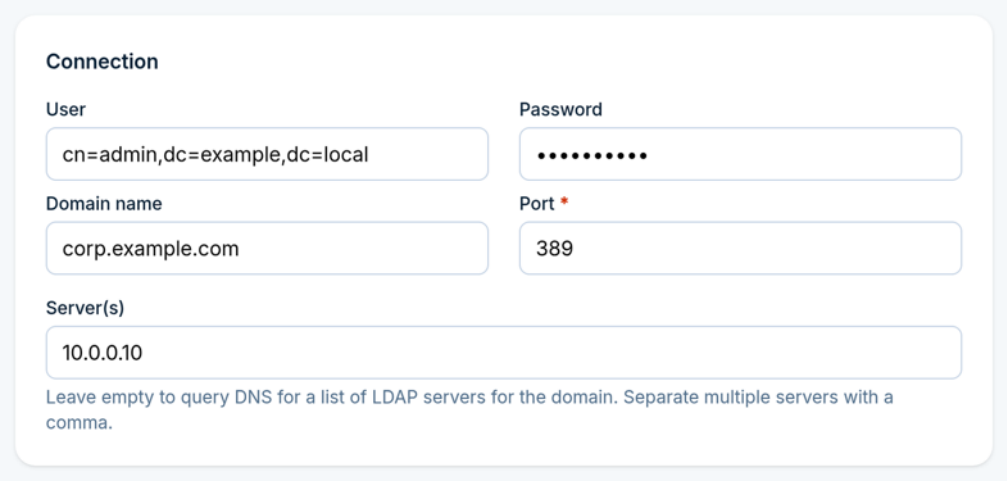
Mit ausgeschalteter Integration zeigt die Seite nur den Schalter an

Schritt 2: Aktivieren Sie die Integration

Schalten Sie **Enable LDAP Integration** ein. Vier Abschnitte werden angezeigt: **Connection**, **Directory structure**, **Attributes and security** und **Sync and access**.

Schritt 3: Verbindung

Feld	Einzugebender Wert
User	Das Dienstkonto, das zum Lesen des Verzeichnisses verwendet wird.
Passwort	Sein Passwort. Das Feld wird leer angezeigt, wenn Sie zur Seite zurückkehren; lassen Sie es leer, um das gespeicherte Passwort beizubehalten.
Domain name	Die Verzeichnisdomäne, beispielsweise `company.local`.
Port	389 für einfaches LDAP, 636 für LDAP über SSL. Erforderlich.
Server(s)	Spezifische Server, durch Kommas getrennt, beispielsweise `ldap1.company.local`, `ldap2.company.local`. Lassen Sie das Feld leer, damit das Gerät die Server im DNS für die Domäne nachschlägt.



Connection-Abschnitt mit Beispielwerten ausgefüllt

Schritt 4: Verzeichnisstruktur

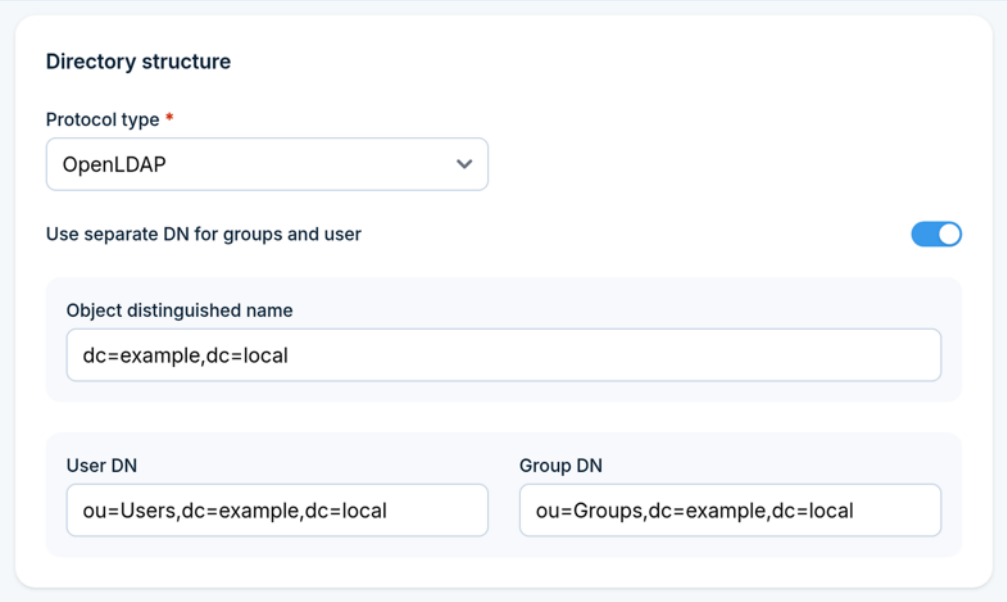
Protokolltyp Wählen Sie **Active Directory** oder **OpenLDAP**, entsprechend Ihrem Server.

Separate DN für Gruppen und Benutzer verwenden Lassen Sie dies aus, wenn Benutzer und Gruppen unter demselben Branch liegen. Dann wird ein Feld angezeigt:

- **Object distinguished name**, zum Beispiel `ou=Users,dc=smseagle,dc=local`.

Schalten Sie dies ein, wenn sie in verschiedenen Branches liegen. **Object distinguished name** bleibt erhalten, und zwei weitere Felder werden darunter angezeigt:

- **User DN**, zum Beispiel `ou=Users,dc=smseagle,dc=local`
- **Group DN**, zum Beispiel `ou=Groups,dc=smseagle,dc=local`



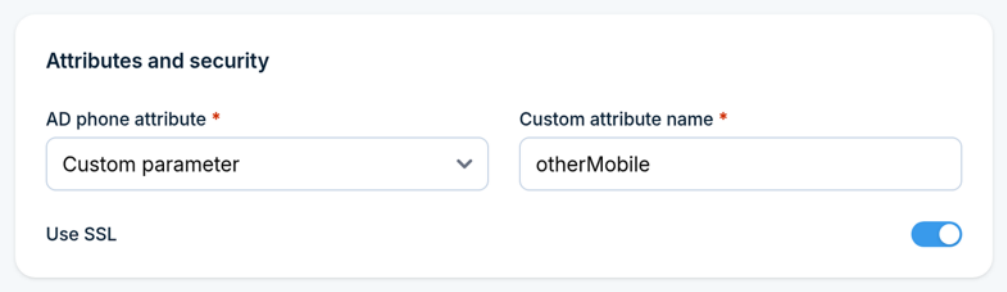
Directory-Struktur mit aktivierten separaten DNs

Schritt 5: Attribute und Sicherheit

AD-Telefon-Attribut Welches Directory-Attribut enthält die Nummer, die SMSEagle anrufen soll: **Telephone number**, **Mobile number**, **Home number**, **Pager number**, **Fax number**, **IP phone number** oder **Custom parameter**.

Wenn Sie **Custom parameter** wählen, wird **Custom attribute name** angezeigt, wo Sie das Attribut selbst eingeben können, zum Beispiel `otherMobile`. Nur einfache Attributnamen werden akzeptiert; Sonderzeichen wie `< > / \ : ; , . + ' " & =` werden abgelehnt.

Use SSL Schalten Sie dies ein, um die Verbindung zum Directory zu verschlüsseln. Denken Sie daran, den entsprechenden **Port** im Abschnitt Connection einzustellen.



Attribute und Sicherheit, mit ausgewähltem **Custom parameter** und aktiviertem SSL

Schritt 6: Synchronisierung und Zugriff

Contacts and group fetch method

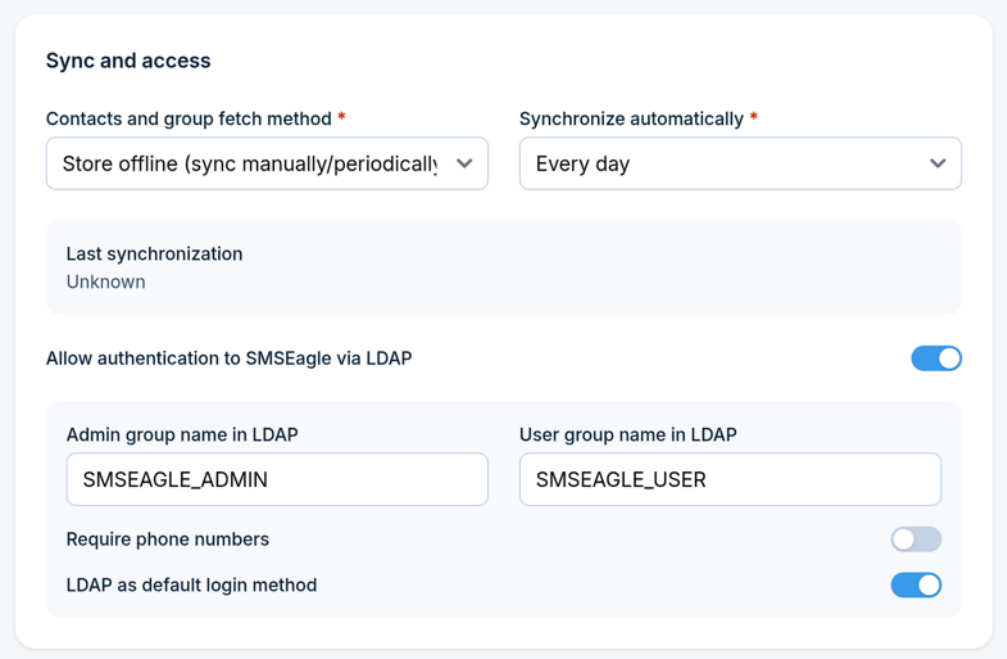
Option	Was passiert
Fetch from LDAP server	Kontakte und Gruppen werden jedes Mal aus dem Directory gelesen, wenn sie benötigt werden. Immer aktuell, aber jede Abfrage hängt davon ab, dass das Directory erreichbar ist.
Store offline (sync manually/periodically)	Eine Kopie wird auf dem Gerät gespeichert. Das Messaging funktioniert weiterhin, wenn das Directory nicht erreichbar ist, auf Kosten der leicht veralteten Kopie.

Wenn Sie **Store offline** gewählt haben, wird **Synchronize automatically** angezeigt: **Never**, **Every hour**, **Every day**, **Every week** oder **Every month**. **Never** bedeutet, dass die Kopie nur aktualisiert wird, wenn Sie selbst eine Synchronisierung auslösen.

Last synchronization unterhalb der Fetch-Methode ist schreibgeschützt und zeigt, wann die Offline-Kopie zuletzt aktualisiert wurde. Sie zeigt Unknown an, bis die erste Synchronisierung ausgeführt wird.

Allow authentication to SMSEagle via LDAP Schalten Sie dies ein, damit sich Benutzer mit ihrem Directory-Konto anmelden können. Es werden vier weitere Felder angezeigt:

- **Admin group name in LDAP** - Mitglieder dieser Gruppe melden sich als Administratoren an.
- **User group name in LDAP** - Mitglieder dieser Gruppe melden sich als normale Benutzer an.
- **Require phone numbers** - Nur Directory-Konten mit einer Nummer im gewählten Telefon-Attribut dürfen sich anmelden. Standardmäßig aus.
- **LDAP as default login method** - Wählt LDAP statt Local im Authentifizierungstyp des Anmeldeformulars vor, sodass Directory-Benutzer diesen nicht jedes Mal ändern müssen.



Synchronisierung und Zugriff mit Offline-Speicherung und aktivierter Verzeichnisanmeldung

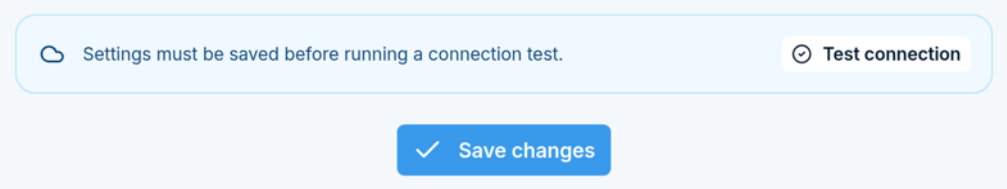
> **Überprüfen Sie die Gruppennamen, bevor Sie sich auf sie verlassen.** Ein Mitglied, das zu keiner Gruppe gehört, kann sich nicht anmelden, und ein Tippfehler im Admin-Gruppennamen wird erst bemerkt, wenn niemand das Gerät verwalten kann. Behalten Sie mindestens ein lokales SMSEagle-Administratorkonto, das funktioniert, bis Sie die Verzeichnisanmeldung überprüft haben.

Schritt 7: Speichern und testen

Klicken Sie auf **Save changes** am unteren Ende der Seite.

Klicken Sie dann auf **Test connection**. Das Gerät verbindet sich mit dem Verzeichnis unter Verwendung der gerade gespeicherten Einstellungen und meldet entweder, dass die Verbindung hergestellt wurde, oder was schief gelaufen ist.

> **Speichern Sie zuerst, dann testen Sie.** Der Test verwendet die gespeicherten Einstellungen, nicht das, was derzeit auf dem Bildschirm angezeigt wird. Wenn Sie also vor dem Speichern testen, überprüfen Sie die vorherige Konfiguration. Die Notiz neben der Schaltfläche sagt dasselbe.



Das Test-Panel wiederholt die Regel: Speichern Sie zuerst, dann testen Sie

Datum / Zeit

Settings > Global settings > Date / Time (`/settings/datetime/`) zeigt das aktuelle Systemdatum und die aktuelle Systemzeit (schreibgeschützt) und ermöglicht Ihnen das Einstellen von:

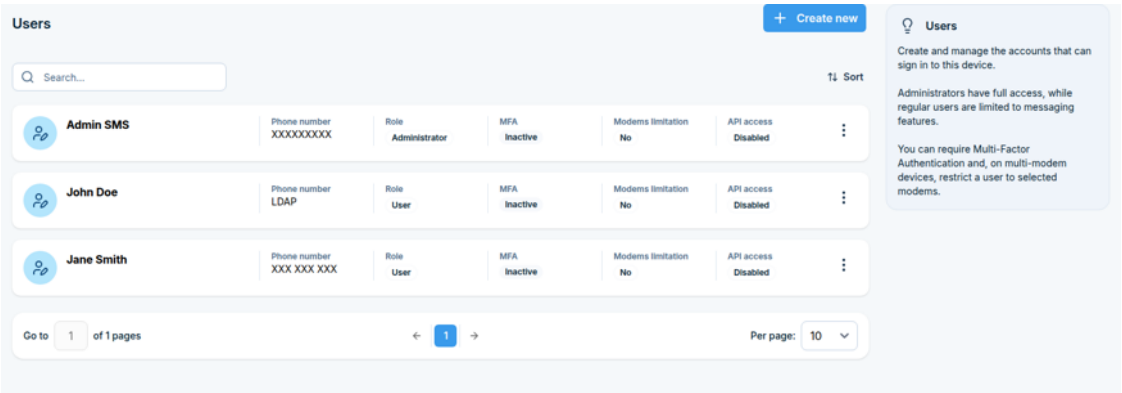
- **Time zone**
- **NTP time synchronization** - wenn aktiviert, werden die **NTP server address** angezeigt. Dies wird auch während des Configuration Wizard angeboten.

System

Dieses Kapitel behandelt den Bereich **System** der Weboberfläche: Verwaltung von Benutzerkonten und des Geräts selbst.

Benutzer

System > Users (`/system/users/`) ist der Ort, an dem Sie die Konten erstellen und verwalten, die sich auf dem Gerät anmelden können. Administratoren haben vollständigen Zugriff, während normale Benutzer auf Messaging-Funktionen beschränkt sind.



Users im System-Abschnitt des Menüs

Für jeden Benutzer können Sie seine **Access level** (Administrator oder User) festlegen und Multi-Factor Authentication erforderlich machen. API-Zugriff (siehe API and Developer Integration) wird ebenfalls pro Benutzer von hier aus gewährt.

Systeminformationen

System > System info (`/system/info/`) zeigt schreibgeschützte Informationen über das Gerät und seine Modems:

- Gerätetyp, SMSEagle-Softwareversion, Seriennummer (MAC-Adresse), Modem-Softwareversion und Datenbankschema-Version
- **Disk space** Nutzung, mit einer optionalen SMS-Benachrichtigung an den Master Admin, wenn die Nutzung einen von Ihnen festgelegten Schwellenwert überschreitet
- Pro-Modem-Details: Signalstärke, Netzwerkname, SIM-Status und Registrierungsstatus, IMEI und SIM-Karten-IMSI

Logs

System > Logs (`/system/logs/`) ermöglicht es Ihnen, die Logs des Geräts zu durchsuchen, gruppiert nach Pro-Modem-Logs und Systemlogs (Datenbank, System, Anwendung, Nachricht). Verwenden Sie **Search by phrase**, um zu filtern, oder **Download logs**, um sie für den Support zu speichern. Logs können auch an einen externen Syslog-Server weitergeleitet werden, um sie zentral zu sammeln. Siehe Forwarding logs to an external server.

Updates

System > Updates (`/system/updates/`) zeigt die installierte Softwareversion an und ermöglicht es Ihnen, manuell oder automatisch auf Updates zu prüfen. Sie können das Gerät auch so einstellen, dass der Administrator per SMS benachrichtigt wird, wenn eine neue Version verfügbar ist. Auf der gleichen Seite wird auch Ihre technische Support-Gültigkeit angezeigt und Sie können diese ebenfalls automatisch überprüfen.

Patches

System > Patches (`/system/patches/`) installiert einen gezielten Fix oder eine zusätzliche Komponente, die von SMSEagle-Support bereitgestellt wird: Geben Sie entweder einen **patch code** ein, um ihn direkt herunterzuladen und zu installieren, oder laden Sie eine **patch file** (eine `.bin`-Datei bis 100 MB) hoch, die vom Support bereitgestellt wird.

Backup / Restore

System > Backup / Restore (`/system/backup/`) behandelt beide Richtungen:

- **Manual backups** - erstellen Sie bei Bedarf ein Backup der Datenbank und der Geräteeinstellungen.
- **Automatic backups** - aktivieren Sie geplante Backups auf einem SFTP/FTP(S)-Server mit Bereinigung alter Backup-Versionen.
- **Restore data** - stellen Sie die Datenbank aus einer Backup-Datei wieder her.

Restart

System > Restart (`/system/restart/`) startet das Gerät bei Bedarf neu – Senden und Empfangen ist bis zum erneuten Online-Gehen nicht verfügbar – oder ermöglicht es Ihnen, einen geplanten Neustart auf wiederkehrender Basis zu aktivieren.

Advanced

Direkter Datenbankzugriff und weitere Power-User-Themen außerhalb des gewöhnlichen Pfads haben ihr eigenes Kapitel: siehe Advanced.

API und Entwicklerintegrationen

SMSEagle bietet eine leistungsstarke integrierte REST-API. Die API ist für die Integration von SMSEagle mit einem externen System oder einer Anwendung vorgesehen.

API-Referenz

SMSEagle bietet zwei API-Versionen:

- **API v2 – empfohlen, verwenden Sie sie für jede neue Integration.** Eine moderne RESTful-API basierend auf der OpenAPI-3.0-Spezifikation. API v2-Referenz
- **API v1 – die ältere API, wird nur aus Gründen der Rückwärtskompatibilität beibehalten.** Eine einfache HTTP- und JSON-RPC-API. Sie funktioniert immer noch und wird weiterhin unterstützt, erhält aber keine neuen Funktionen – schreiben Sie keine neuen Integrationen dagegen. API v1-Referenz

Aufgrund des umfangreichen API-Dokumentationsinhalts wird diese als separates Dokument gepflegt. Folgen Sie den obigen Links für die vollständige Spezifikation jeder API.

API-Schlüssel

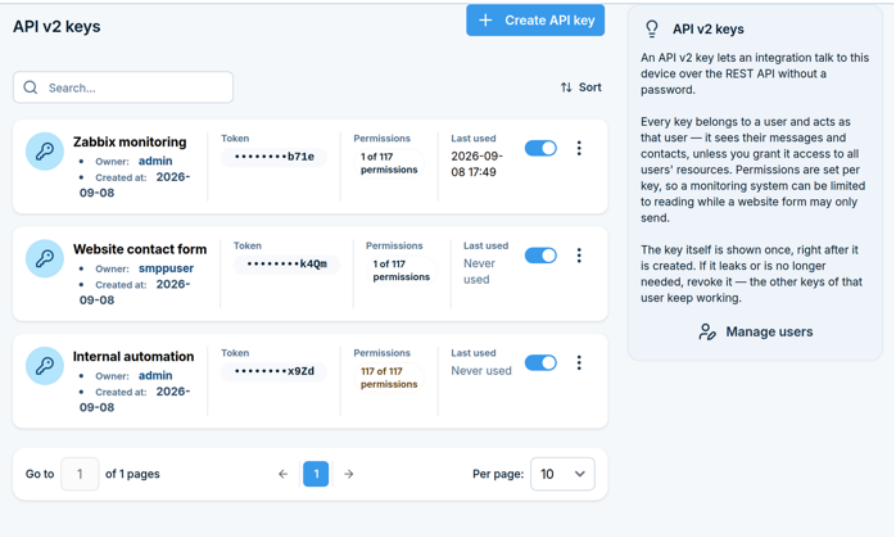
Eine Integration authentifiziert sich mit einem **API-Schlüssel** anstelle eines Benutzerpassworts. Schlüssel werden für jede API-Version separat auf zwei Seiten aufbewahrt:

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

Ein Schlüssel gehört immer einem Benutzer und fungiert als dieser Benutzer, daher sieht er die Nachrichten und Kontakte dieses Benutzers. Berechtigungen werden pro Schlüssel gewährt, sodass Sie ein Überwachungssystem auf Lesen begrenzen können, während ein Website-Formular möglicherweise nur senden darf.

API v2-Schlüssel

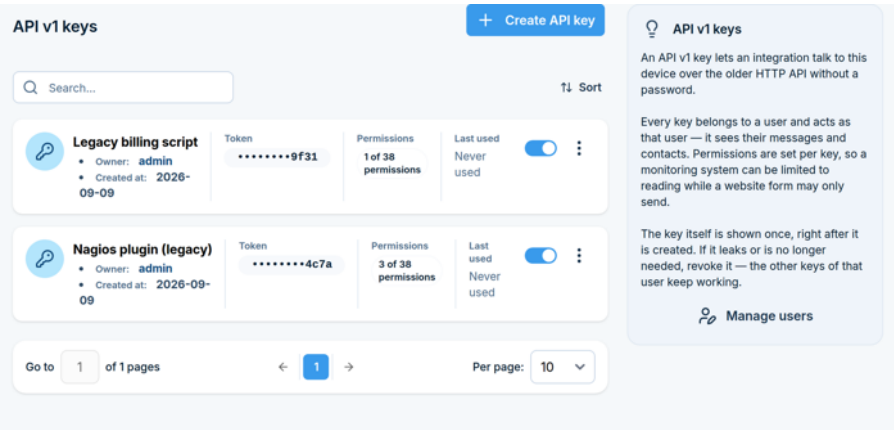
Dies ist die Seite, die für eine neue Integration verwendet werden sollte.



API v2-Schlüssel

API v1-Schlüssel

API v1 ist die ältere API. Erstellen Sie einen v1-Schlüssel nur für eine vorhandene Integration, die nicht zu v2 verschoben werden kann – für alles Neue erstellen Sie stattdessen einen API v2-Schlüssel.



API v1-Schlüssel

Erstellen eines Schlüssels

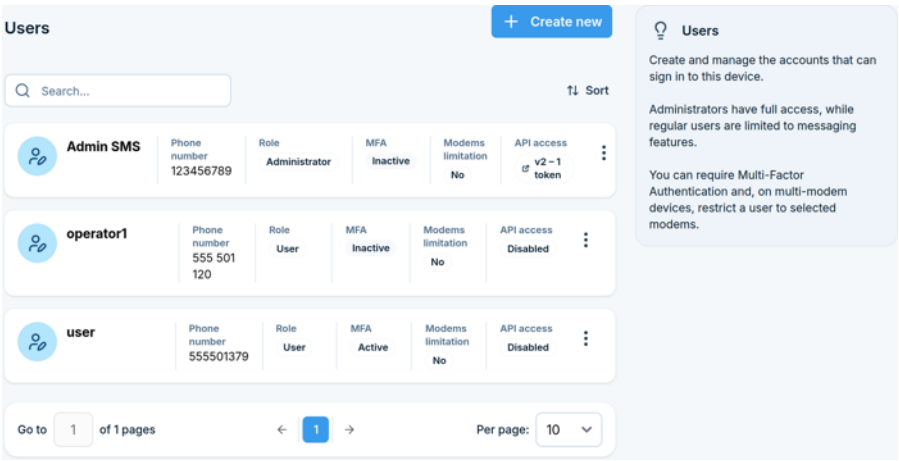
Create API key öffnet das Formular für die API-Version, deren Seite Sie besuchen:

Feld	Funktion
Key name	Wie Sie diese Integration später erkennen werden, z. B. Zabbix oder Website form.
Owner	Der Benutzer, als der der Schlüssel fungiert. Der Schlüssel sieht die Nachrichten und Kontakte dieses Benutzers.
Key enabled	Ein deaktivierter Schlüssel wird von der API abgelehnt, ohne gelöscht zu werden, was eine Integration ausschaltet, ohne ihre Konfiguration zu verlieren.
Access to all users' resources	Nur API v2. Ermöglicht dem Schlüssel, Ressourcen anderer Benutzer zu lesen und zu ändern (siehe unten).
Berechtigungen	Mit diesem Schlüssel können nur die Methoden aufgerufen werden, die Sie aktiviert haben.

Der Schlüssel selbst wird nur einmal angezeigt, unmittelbar nach seiner Erstellung. Kopieren Sie ihn dann und speichern Sie ihn an einem sicheren Ort. Wenn Sie ihn verlieren, widerrufen Sie diesen Schlüssel und erstellen Sie einen neuen – die anderen Schlüssel desselben Benutzers funktionieren weiterhin.

Welche Benutzer haben API-Zugriff

System > Users zeigt pro Benutzer an, wie viele API-Schlüssel der Benutzer hat und für welche API-Version. Das Abzeichen verlinkt direkt zur entsprechenden Schlüsselseite.



API-Zugriff, pro Benutzer in der Benutzerliste angezeigt

Zugriff auf Ressourcen anderer Benutzer

Die beiden API-Versionen unterscheiden sich darin, wie umfassend ein API-Schlüssel Daten anderer Benutzer einsehen kann:

- In **API v1** hat ein Schlüssel standardmäßig Zugriff auf Ressourcen jedes anderen Benutzers – Phonebuch-Kontakte, Gruppen usw.
- In **API v2** ist der Zugriff granularer: Ein Schlüssel hat standardmäßig nur Zugriff auf Ressourcen, die er selbst erstellt hat. Um Zugriff auf Ressourcen aller anderen Benutzer zu ermöglichen, aktivieren Sie **Access to all users' resources** auf dem Schlüssel.

Plugins und Integrationen

SMSEagle kann mit externer Software wie Netzwerk-Überwachungssystemen, Authentifizierungssystemen und vielen anderen integriert werden. Die meisten Integrationen verwenden eine von zwei Methoden:

- **API** – das externe System sendet und empfängt Nachrichten über die SMSEagle REST API. Dies ist die flexibelste Methode und bietet Zugriff auf alle Gerätefunktionen. Siehe API und Developer Integration.
- **Email to SMS** – das externe System sendet eine normale E-Mail und SMSEagle wandelt sie in eine SMS um. Es ist keine Kodierung erforderlich, sodass es mit jeder Software funktioniert, die bereits E-Mail-Benachrichtigungen senden kann. Siehe Email to SMS.

Je nach Ihrer Umgebung können Sie auch MQTT oder SMPP verwenden.

Für viele beliebte Systeme müssen Sie die Integration nicht selbst erstellen. SMSEagle bietet gebrauchsfertige Plugins und schrittweise Integrationsleitfäden, und die Liste wächst ständig. Eine vollständige und aktuelle Liste finden Sie unter: https://www.smseagle.eu/integration-plugins/

Erweitert

Dieses Kapitel behandelt Themen für fortgeschrittene Benutzer, die die normale Weboberfläche umgehen: direkter Datenbankzugriff und SQL sowie Befehlszeilenskripte zur Datenbankbereinigung. Die meisten Benutzer werden dieses Kapitel nie benötigen.

Direktes Verbinden mit der SMSEagle-Datenbank

Die Datenbank von SMSEagle läuft auf PostgreSQL. Sie können direkt auf sie zugreifen, um SMS-Nachrichten über SQL-Abfragen zu lesen oder zu schreiben, anstatt die Weboberfläche oder die API zu verwenden.

Der Datenbankzugriff für externe Anwendungen ist **standardmäßig deaktiviert**. Aktivieren Sie ihn unter **Settings > Global settings > Application > Access to DB for external applications**.

Verbinden Sie sich von einer externen Anwendung aus mit der Datenbank mit:

- Host: Die IP-Adresse des Geräts
- Database name: `smseagle`
- User: `smseagleuser`
- Password: `postgreeagle`

Einfügen einer kurzen SMS über SQL

Eine kurze Textnachricht (bis zu 160 Zeichen):

```
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;
```

Die obige Nachricht gehört dem Benutzer mit `id_user` 1 (dem Standard-Benutzer `admin`) – die `id_user`-Werte anderer Benutzer befinden sich in der Tabelle `public."user"`. Das Feld `SenderID` identifiziert, welches Modem die Nachricht sendet: `smseagle1` für Modem 1, `smseagle2` für Modem 2.

Einfügen einer langen SMS über SQL

Mehrteilige Nachrichten benötigen auch einen UDH-Header, der als Hexadezimalstring im Feld `UDH` gespeichert ist. Verwenden Sie stattdessen die API, wenn Sie keinen spezifischen Grund haben, dies manuell zu tun (siehe API and Developer Integration).

Bei einer langen Textnachricht beginnt der UDH mit `050003`, gefolgt von einem Byte als Nachrichtenreferenz (beliebiger Hexwert, aber unterschiedlich für jede Nachricht – `D3` unten), einem Byte für die Gesamtzahl der Teile (`02` unten, eindeutig pro Nachricht an dieselbe Nummer) und einem Byte für die aktuelle Teilenummer (`01` für den ersten Teil, `02` für den zweiten usw.).

Eine zweiteilige lange Nachricht sieht wie folgt aus:

```
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;
```

Das Hinzufügen eines UDH nimmt Platz für Text weg – das obige Beispiel ermöglicht nur 153 Zeichen pro Nachrichtenteil.

Datenbankbereinigungsskripte

Mehrere Skripte sind über die Linux-CLI zum Löschen von SMS-Nachrichten aus der Datenbank verfügbar, die sich unter `/mnt/nand-user/scripts/` befinden:

Skript	Verwendung	Zweck
`db_delete`	`./db_delete YYYYMMDDhhmm`	Löschen von SMS aus Inbox und SentItems älter als das angegebene Datum
`db_delete_7days`	`./db_delete_7days`	Löschen von SMS aus Inbox und SentItems älter als 7 Tage
`db_delete_allfolders`	`./db_delete_allfolders`	Inbox, SentItems und Outbox bereinigen – zum regelmäßigen Ausführen per Cron vorgesehen
`db_delete_select`	`./db_delete_select {inbox|outbox|sentitems|trash}`	Löschen von SMS aus einem ausgewählten Ordner

Ein Skript zu Cron hinzufügen: erstellen Sie eine Datei unter `/etc/cron.d/` (z. B. `db_cleaner`) mit folgendem Inhalt:

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

Dieses Beispiel führt das Bereinigungsskript am 1. eines jeden Monats aus.

Weiterleitungsprotokolle an einen externen Server

SMSEagle schreibt seine Protokolle über rsyslog. Um eine Kopie davon an einen zentralen Syslog-Server zu senden, fügen Sie eine Weiterleitungsregel über SSH hinzu. Hierfür gibt es keine Einstellung in der Webschnittstelle.

1. Melden Sie sich über SSH als `root` auf dem Gerät an.
2. Erstellen Sie die Datei `/etc/rsyslog.d/005-remote.conf` mit dieser Regel und ersetzen Sie die Adresse, den Port und das Protokoll durch die Ihres Servers:

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

- `target` - IP-Adresse oder Hostname des Syslog-Servers.
- `port` - Port, auf dem der Server lauscht, normalerweise `514`.
- `protocol` - `udp` oder `tcp`.
- Die Warteschlangen-Einstellungen speichern bis zu 10000 Nachrichten auf dem Gerät, während der Server nicht erreichbar ist, und senden diese, sobald er wieder verfügbar ist.

3. Überprüfen Sie die Konfiguration und starten Sie rsyslog neu:

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

Behalten Sie den Dateinamen. Die eigenen Protokolle von SMSEagle (Application, API, Message und die E-Mail-, Call-, Signal- und WhatsApp-Services) werden durch Regeln in `/etc/rsyslog.d/010-*.conf` bis `018-*.conf` geschrieben, und jede dieser Regeln stoppt die weitere Verarbeitung ihrer Nachrichten. Eine Weiterleitungsregel, die nach diesen platziert wird, beispielsweise am Ende von `/etc/rsyslog.conf`, leitet nur die Systemprotokolle weiter. Das Präfix `005-` veranlasst rsyslog, die Weiterleitungsregel zuerst zu lesen, sodass jede Nachricht weitergeleitet wird.

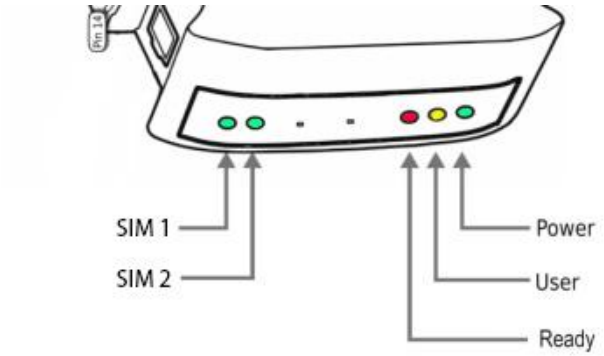
Um den Protokolldatenverkehr mit TLS zu verschlüsseln, siehe das rsyslog-Handbuch Encrypting Syslog Traffic with TLS.

Fehlerbehebung

Um sicherzustellen, dass das Gerät ordnungsgemäß funktioniert, führen Sie die drei Schritte aus:

1. Überprüfung der LEDs
2. Überprüfung der Geräteinformationen (Systeminfo)
3. Überprüfung der Gerätelogs (Beschreibung unten)

Überprüfung der LEDs



LED-Positionen

Der ordnungsgemäße Betrieb des Geräts wird durch LEDs wie folgt signalisiert:

LED	Ordnungsgemäße Funktion
Power (PWR)	Dauerhaft leuchtend
User	Blinkt während Flashdisk-Lese-/Schreibvorgang
Ready (RDY)	Blinkend
SIM1 NXS-9700-3G	Langsames Blinken im Standby-Modus, schnelles Blinken wenn Modem 1 in Betrieb ist
SIM2 NXS-9700-3G	Nicht verwendet

Überprüfung der Geräteinformationen

Die Geräteinformationen (Gerätetyp, Softwareversion, Modem IMEI, IMSI, Netzwerksignalstärke, Netzwerkname) finden Sie unter **System > System info**. Siehe System.

Gerätelogs

Unter **System > Logs** finden Sie die neuesten Zeilen der Gerätelogs: Modem-Log, Datenbankprotokoll und Systemprotokoll. Im Falle von Problemen mit dem Gerät sind diese Logs eine wertvolle Quelle für Fehlerbehebungsinformationen.

Erweiterte Gerätelogs können über die Schaltfläche **Download logs** auf der gleichen Seite heruntergeladen werden. Siehe System.

Wenn das Gerät nicht erreichbar ist

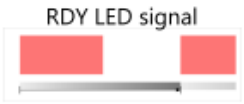
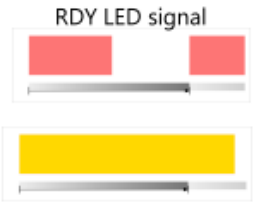
1. Überprüfen Sie, ob das Gerät korrekt mit dem Netzwerk verbunden ist. Überprüfen Sie den LED-Status des RJ45-Anschlusses.
2. Wenn das Gerät aufgrund eines Fehlers oder falscher Benutzereinstellungen nicht reagiert, starten Sie das Gerät neu, indem Sie die Stromversorgung trennen und wieder verbinden (oder den Reset-Schalter drücken).
3. Wenn Sie sich immer noch nicht mit dem Gerät verbinden können, ist es möglich, die Standard-IP-Einstellungen mit dem SW-Schalter wiederherzustellen.

Wiederherstellen der Werkseinstellungen

Die Funktion „Auf Standardeinstellungen zurücksetzen“ ermöglicht es Ihnen, das Gerät schnell auf seine ursprüngliche Werkkonfiguration zurückzusetzen.

> **Warnung**
>
> Das Wiederherstellen der Werkseinstellungen entfernt permanent die aktuelle Benutzerkonfiguration. Stellen Sie sicher, dass alle notwendigen Einstellungen oder Daten vor dem Fortfahren gesichert werden.

Um das Zurücksetzen einzuleiten, halten Sie die SW-Taste 10 Sekunden lang gedrückt. Das Gerät wechselt in den Wiederherstellungsmodus.

LED-Signalisierung	BENUTZER-Aktionen	Systemreaktion
	1. **When the device is ready to operate**	–
–	2. **Press and hold SW button for 10 seconds**	Wiederherstellungsdienst wird heruntergerechnet.
	3. **Release SW button after 10 seconds.** User LED will begin to blink.	Das System liest Werkseinstellungen. Werkseinstellungen werden auf das Gerät angewendet.
	4. **Wait until system reboots.** Default settings are restored.	Das System wird neu gestartet.

Hardware Rev. 5 und später

Rev.5

Der Prozess verwendet eine dedizierte, schreibgeschützte Wiederherstellungspartition, um sicherzustellen, dass das Wiederherstellungsabbild intakt bleibt und durch den normalen Gerätebetrieb nicht beeinträchtigt wird. Nach dem Eintritt in den Wiederherstellungsmodus startet ein einzelner kurzer Piepton einen 10-Sekunden-Countdown. Ein zweiter kurzer Piepton bestätigt den Beginn des Wiederherstellungsprozesses. Der gesamte Prozess dauert normalerweise einige Minuten.

Nach erfolgreichem Abschluss signalisiert das Gerät mit drei kurzen Pieptönen, gefolgt von einem 10-Sekunden-Countdown vor dem automatischen Neustart. Wenn der Vorgang während des Countdowns abgebrochen wird, werden zwei kurze Pieptöne ausgegeben. Im Falle eines Wiederherstellungsfehlers gibt das Gerät einen langen Piepton, gefolgt von zwei kurzen Pieptönen, aus und wechselt dann zu einer Service-Shell für die Diagnose.

Hardware Rev. 3–Rev. 4

Rev.3 Rev.4

Die Rücksetfunktion stellt nur die folgenden Einstellungen auf ihre Standardwerte zurück: IP-Einstellungen, Zeitzoneneinstellungen, Datenbankinhalt und Linux-OS-Benutzer/Passwörter.

Service & Reparatur

Garantie

Ihr SMSEagle wird mit einer standardmäßigen 2-jährigen technischen Unterstützung und Hardwarereparatur-Garantieabdeckung geliefert. Die Standardgarantie kann beim Gerätekauf auf 3 Jahre verlängert werden (überprüfen Sie Ihre Kaufbedingungen). Weitere Informationen zu Garantiebedingungen finden Sie auf der Garantiekarte, die mit Ihrem Gerät geliefert wird, oder folgen Sie dem Link: www.smseagle.eu/downloads

Service

Stellen Sie vor der Kontaktaufnahme mit dem Support-Team sicher, dass Sie den Abschnitt Fehlerbehebung dieser Anleitung gelesen haben. Weitere Informationen und hilfreiche Hinweise zur Konfiguration des SMSEagle-Geräts finden Sie auch in unserer Online-Wissensdatenbank unter der gleichen Adresse wie das Support-Portal unten.

Das SMSEagle Support Team steht per E-Mail oder Telefon zur Verfügung.

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

E-Mail: support@smseagle.eu

Telefon: + 48 61 6713 413

Der Support-Service wird bereitgestellt von: Proximus Sp. z o.o. ul. Piątkowska 163, 60-650 Poznan, Poland

Wenn Sie das Support-Team kontaktieren, seien Sie bereit, die folgenden Informationen bereitzustellen:

Systemprotokolle

Navigieren Sie zu **System > Logs > Download logs**. Stellen Sie das Protokollpaket dem Support-Team auf Anforderung zur Verfügung.

MAC-Adresse

Jedes SMSEagle-Gerät hat eine eindeutige MAC-Adresse. Sie ist auf dem Gerätekörper gedruckt oder kann unter **System > System info** gefunden werden.

Technische Spezifikationen und Sicherheitsinformationen

Technische Spezifikation

Hardware-Spezifikation

- Prozessortyp:
  - hardware Rev.5, Rev.4: Broadcom BCM2711 1,5 GHz Quad-Core Cortex-A72 (ARM v8) 64-Bit
  - hardware Rev.3: Broadcom BCM2837 1,2 GHz Quad-Core ARM Cortex-A53 (64-Bit)
- Betriebsspeicher (RAM):
  - hardware Rev.5, Rev.4: 2GB LPDDR4
  - hardware Rev.3: 1GB LPDDR2 @ 900 MHz
- eMMC-Speicher
  - hardware Rev.5, Rev.4: 16GB
  - hardware Rev.3: 4GB
- Netzwerkschnittstelle: Ethernet (1xRJ45): Gigabit Ethernet 10/100/1000 TX
- 1x HDMI-Anschluss für Debugging-Zwecke
- Weitere externe Anschlüsse: 4x DI, 4x DO, 1× 1Wire, 2x USB 2.0 (max. 300mA)
- Digitale Ein-/Ausgangsanschlusstypen: DI-Typ „Pull-up-Widerstand“. DO-Typ „Open Collector“
- RTC-Uhr: RTC 240B SRAM, Watchdog-Timer
- Interner Feuchte- und Temperatursensor: Genauigkeit ± 0,5 °C, ±2 %RH
- Stromverbrauch:
  - hardware Rev.5, Rev.4: max 25W
  - hardware Rev.3: max 12W
- Geräuschpegel: Lüfterlos
- Abmessungen: (Breite x Tiefe x Höhe) 45 × 120 × 101 mm
- Gewicht: 350g
- Gehäuse: ABS, DIN-Schienenmontage
- Betriebsparameter:
  - Betriebstemperatur: 0 ~ 40°C

    - Luftfeuchtigkeit: 8 ~ 90% RH (keine Kondensation)
- Internes Modem

Gerätetyp NXS-9700-5G Rev.5

- Frequenzbänder: 5G NR, LTE.
- 5G NR 3GPP Release 17 RedCap SA-Betrieb, Sub-6 GHz
- 5G NR SA: n1/ 2/ 3/ 5/ 7/ 8/ 12/ 13/ 14/ 18/ 20/ 25/ 26/ 28/ 30/ 38/ 40/ 41/ 48/ 66/ 70/ 71/ 77/ 78/ 79
- LTE FDD: B1/ 2/ 3/ 4/ 5/ 7/ 8/ 12/ 13/ 14/ 17/ 18/ 19/ 20/ 25/ 26/ 28/ 30/ 66/ 70/ 71
- LTE TDD: B34/ 38/ 39/ 40/ 41/ 42/ 43/ 48
- Datenraten (Max)
    - 5G SA Sub-6: 223 Mbps (DL)/ 123 Mbps (UL)
    - LTE: 195 Mbps (DL)/ 105 Mbps (UL)
- Ausgangsleistung (Nennwert):
    - Klasse 3 (23dBm±2dB) für 5G NR-Bänder
    - Klasse 2 (26dBm+2/-3dB) für 5G NR HPUE-Bänder (n38/n40/n41/n77/n78/n79)
    - Klasse 3 (23dBm±2dB) für LTE-Bänder
    - Klasse 2 (26dBm±2dB) für LTE HPUE-Bänder (B38/B40/B41/B42/B43)

Gerätetyp NXS-9700-5G Rev.4

- Frequenzbänder: 5G NR, LTE, UMTS.
- 5G NR 3GPP Release 15 NSA/SA-Betrieb, Sub-6 GHz
- 5G NR NSA/SA: n1/n2/n3/n5/n7/n8/n12/n20/n25/n28/n38/n40/n41/ /n66/n71/n77/n78/n79
- LTE DL Cat 16/ UL Cat 18
- LTE FDD: B1/B2/B3/B4/B5/B7/B8/B12(B17)/B13/B14/B18/B19/B20/B25/B26/B28/B29/B30/B32/B66/B71
- LTE TDD: B34/B38/B39/B40/B41/B42/B43/B48
- WCDMA: B1/B2/B3/B4/B5/B6/B8/B19
- Ausgangsleistung (Nennwert):
    - Klasse 3 (23dBm±2dB) für 5G NR-Bänder
    - Klasse 2 (26dBm±2dB) für 5G NR HPUE-Bänder (n41/n77)
    - Klasse 3 (23dBm±2dB) für LTE-Bänder
    - Klasse 2 (26dBm±2dB) für LTE HPUE-Bänder (B38/B41)
    - Klasse 3 (24dBm+1/-3dB) für WCDMA-Bänder

Gerätetyp NXS-9700-4G Rev.4

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

Gerätetyp NXS-9700-4G Rev.3

- Waveband: UMTS, LTE
- LTE-Bänder: LTE FDD: 1-5, 7, 8, 12, 13, 17, 20, 25, 26, 28, 29, 30 (Rx nur), 66 LTE TDD: 38, 40, 41
- 3G-Bänder: 1, 2, 4, 5, 8
- Ausgangsleistung:
    - Klasse 3 (0,2 W, 23 dBm) @ LTE
    - Klasse 3 (0,25 W, 23 dBm) @ 3G

Gerätetyp NXS-9700-3G Rev.3

- Waveband: GSM, UMTS
- GSM/GPRS Quad-Band 850/900/1800/1900 MHz
- UMTS 800/850/900/AWS 1700/1900/2100 MHz
- Ausgangsleistung (Nennwert):
    - E-GSM 900: Klasse 4, DCS 1800: Klasse 1
    - EDGE 900: Klasse E2, EDGE 1800: Klasse E2
    - FDD I: Klasse 3, FDD VIII: Klasse 3
- SIM-Kartenstandard: Mini
- Antennenstecker: SMA
- Herkunftsland: Europäische Union (Polen)

Stromversorgung

- Hardware Rev.5, Rev.4:
  - Externes Netzteil mit Ausgangsstromkreis bewertet ES1 (12Vdc; min, 3,3A), PS2 (LPS – Limited Power Source). Netzeingang:
    - Spannungsbereiche: 100–240V Wechselstrom (AC)
    - Frequenz: 50–60Hz Einphase
    - DC-Steckertyp: 5,5/2,5
  - Alternative Stromquelle: PoE+ (IEEE 802.3at Typ 2). Stromkreis mit PoE+: bewertet ES1 (50-57Vdc; 30W), PS2 (LPS – Limited Power Source)
- Hardware Rev.3:
  - Externes Netzteil mit Ausgangsschaltung gemäß ES1 (12Vdc; mind. 1A), PS2 (LPS – Limited Power Source). AC-Netzeingang:
    - Spannungsbereiche: 100–240V Wechselstrom (AC)
    - Frequenz: 50–60Hz Einphase
    - DC-Steckertyp: 5,5/2,5

Antenne

- Gerätetyp NXS-9700-5G Rev.5:
  - 2x omnidirektionale 2,5dBi-Antenne mit Magnetfuß
  - Frequenzband: 4GLTE, 5GNR
  - Kabellänge 2m
  - Steckertyp: SMA
  - Impedanz: 50 Ohm
  - Abmessungen Ø 31 × 109 mm
- Gerätetyp NXS-9700-5G Rev.4:
  - 2x omnidirektionale MIMO-Antenne 2,5dBi mit Magnet-/Klebefuß
  - Frequenzband: UMTS, LTE, 5GNR
  - Kabellänge 2m
  - Steckertyp: SMA
  - Impedanz: 50 Ohm
- Gerätetyp NXS-9700-4G:
  - Omnidirektionale 2dBi-Antenne mit Magnetfuß
  - Waveband: UMTS, LTE
  - Kabellänge 3m
  - Steckertyp: SMA

    - Impedanz: 50 Ohm
- Gerätetyp NXS-9700-3G:
    - Omnidirektionale 3dBi-Antenne mit Magnetfuß
    - Waveband: GSM, UMTS
    - Kabellänge 3m
    - Steckertyp: SMA
    - Impedanz: 50 Ohm

Durchsatz beim Senden/Empfangen

- Eingangsübertragungsrate: bis zu 30 SMS/min
- Ausgangsübertragungsrate: bis zu 30 SMS/min

Softwareplattform

- Betriebssystem: Linux
    - Hardware Rev. 5: Kernel 6.12
    - Hardware Rev. 4: Kernel 5.1x
    - Hardware Rev. 3: Kernel 4.14
- Integrierter Apache2-Webserver
- Integrierter PostgreSQL-Datenbankserver
- Integrierter Postfix-E-Mail-Server
- Integrierter SNMP-Agent
- Integrierter NTP-Client
- integrierter Failover-Service (HA-Cluster)
- Watchdog-Mechanismus für 3G/4G/5G-Modem
- moderne responsive Weboberfläche
- Liste der offenen TCP/UDP-Ports in der Standardkonfiguration:
    - TCP: 22 (SSH), 80 (HTTP), 443 (HTTPS), 5432 (PostgreSQL mit Zugriffsbeschränkung auf localhost)
    - UDP: 68 (DHCP-Client), 323 (NTP-Client)

Wichtige Sicherheitsinformationen

Dieses Kapitel enthält wichtige Informationen zu Sicherheitsverfahren. Befolgen Sie diese Regeln zum Umgang mit Ihrem Gerät zu Ihrer Sicherheit und zum Schutz Ihrer Ausrüstung.

> **Warnung**
>
> Unsachgemäße Lagerung oder Verwendung Ihres Geräts kann die Herstellergarantie ungültig machen. Die Nichtbeachtung dieser Sicherheitsanweisungen kann zu Feuer, Stromschlag oder anderen Verletzungen oder Schäden führen.

Ergreifen Sie immer die folgenden Vorsichtsmaßnahmen.

Trennen Sie den Stromstecker von der Stromquelle oder wenn eine der folgenden Bedingungen vorliegt:

- das Stromkabel oder der Stecker wird ausgefranst oder beschädigt
- Sie verschütten etwas in das Gehäuse
- das Gerät ist Regen oder andere Feuchtigkeit ausgesetzt
- das Gerät ist heruntergefallen oder das Gehäuse ist anderweitig beschädigt

Stellen Sie sicher, dass die Verwendung dieses Produkts in Ihrem Land und in der erforderlichen Umgebung zulässig ist. Wie bei allen anderen Telekommunikationsgeräten kann die Verwendung dieses Produkts gefährlich sein und muss in den folgenden Bereichen vermieden werden: wo es mit anderen elektronischen Geräten in unmittelbarer Nähe interferieren kann, in Umgebungen wie Krankenhäuser, Flughäfen, Flugzeuge usw.; wo Explosionsgefahr besteht, wie an Tankstellen, Ölraffinerien usw.

Es ist Aufgabe des Benutzers, die Landesvorschriften und die spezifischen Umgebungsvorschriften einzuhalten.

Disassemblieren Sie das Produkt nicht; jede Spur von Manipulation beeinträchtigt die Gültigkeit der Garantie.

Jedes Gerät muss mit einer geeigneten Antenne mit spezifischen Eigenschaften ausgestattet sein. Die Antenne muss sorgfältig installiert werden, um Interferenzen mit anderen elektronischen Geräten zu vermeiden und muss mit Garantie eines Mindestabstands von 30 cm (12 Zoll) vom Körper installiert werden. Sollte diese Anforderung nicht erfüllt werden können, muss der Systemintegrator das Endprodukt gemäß der SAR-Verordnung bewerten.

HAFTUNGSAUSSCHLUSS: Der Hersteller ist nicht verantwortlich für Schäden, die durch unsachgemäße Installation, Nichtbeachtung des ordnungsgemäßen technischen Zustands oder Verwendung eines Produkts gegen seinen Bestimmungszweck verursacht werden.

Behördliche Erklärungen

EU-Konformitätserklärung

Hiermit erklärt Proximus Sp. z o.o., Inhaber der Marke SMSEagle, dass der Funkanlagentyp SMSEagle NXS-9700-3G, NXS-9700-4G, NXS-9700-5G die Richtlinie 2014/53/EU erfüllt.

Der vollständige Text der EU-Konformitätserklärung ist unter folgender Internetadresse verfügbar: www.smseagle.eu/certification

FCC-Konformitätserklärung

Dieses Gerät erfüllt Teil 15 der FCC-Vorschriften. Der Betrieb unterliegt den folgenden zwei Bedingungen:

(1) Dieses Gerät darf keine schädlichen Störungen verursachen, und

(2) dieses Gerät muss alle empfangenen Störungen akzeptieren, einschließlich Störungen, die zu unerwünschtem Betrieb führen können.

Hinweis:

Dieses Gerät wurde getestet und erfüllt die Grenzwerte für ein Gerät der Klasse B gemäß Teil 15 der FCC-Vorschriften. Diese Grenzwerte sollen einen angemessenen Schutz vor schädlichen Störungen in einer geschäftlichen/kommerziellen Nicht-Wohnumgebung bieten. Es kann jedoch nicht garantiert werden, dass Störungen in einer bestimmten Installation nicht auftreten. Wenn dieses Gerät Störungen bei Radio- oder Fernsehempfang verursacht, was durch Ausschalten und Einschalten des Geräts festgestellt werden kann, wird der Benutzer aufgefordert, die Störung durch eine oder mehrere der folgenden Maßnahmen zu beheben:

- Neusausrichtung oder Umpositionierung der Empfangsantenne
- Vergrößerung des Abstands zwischen dem Gerät und dem Empfänger
- Anschluss des Geräts an eine Steckdose in einem anderen Stromkreis als derjenige, an den der Empfänger angeschlossen ist
- Konsultation des Händlers oder eines erfahrenen Rundfunk-/Fernsehtechnikers um Hilfe

Wichtig:

Dieses Gerät erzeugt, nutzt und kann Hochfrequenzenergie abstrahlen und kann bei Nicht-Installation und Nicht-Verwendung gemäß dem Herstelleranleitung schädliche Störungen in der Radiokommunikation verursachen. Der Betrieb dieses Geräts in einem Wohngebiet wird wahrscheinlich schädliche Störungen verursachen, in welchem Fall Sie verpflichtet sind, die Störungen auf Ihre Kosten zu beheben. Die FCC-Vorschriften sehen vor, dass Änderungen oder Modifikationen, die nicht ausdrücklich von SMSEagle™ genehmigt wurden, Ihre Betriebserlaubnis für dieses Gerät erlöschen lassen können. Dieses Produkt hat EMC-Konformität unter Bedingungen

nachgewiesen, die die Verwendung konformer Peripheriegeräte (Antennen) und abgeschirmter Kabel zwischen Systemkomponenten einschlossen. Es ist wichtig, dass Sie konforme Peripheriegeräte und abgeschirmte Kabel zwischen Systemkomponenten verwenden, um die Möglichkeit von Störungen bei Radios, Fernsehgeräten und anderen elektronischen Geräten zu verringern.

FCC-Konformitätserklärung des Lieferanten



Diese Konformitätserklärung des Lieferanten wird hiermit gemäß Kapitel 1, Unterabschnitt A, Teil 2 von Titel 47 des Codes der föderalen Vorschriften ausgestellt von:

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

Das Produkt NXS-9700-4G, NXS-9700-5G erfüllt die geltenden Anforderungen der FCC-Regel Teil 15B für die entsprechenden Geräteklassen von unbeabsichtigten Strahlern.

VERANTWORTLICHE PARTEI in den Vereinigten Staaten:

Testing Partners LLC

18200 SR 306

Chagrin Falls, OH 44023

info@testingpartners.com

Die verantwortliche Partei garantiert, dass jede unter dieser Konformitätserklärung vermarktete Geräteeinheit mit der getesteten und als annehmbar befundenen Einheit identisch ist und die Aufzeichnungen der verantwortlichen Partei weiterhin widerspiegeln, dass die Ausrüstung, die unter einer solchen Konformitätserklärung des Lieferanten produziert wird, innerhalb der Abweichung, die aufgrund von Massenproduktion und statistischer Prüfung erwartet werden kann, konform bleibt.

Kanadische Behördenerklärung (ISED)

Dieses Gerät erfüllt die lizenzfreien RSS-Standards von Innovation, Science and Economic Development Canada. Der Betrieb unterliegt den folgenden zwei Bedingungen:

(1) dieses Gerät darf keine Störungen verursachen, und

(2) dieses Gerät muss alle Störungen akzeptieren, einschließlich Störungen, die zu unerwünschtem Betrieb des Geräts führen können.

Dieses digitale Gerät der Klasse B erfüllt die Anforderungen der kanadischen Interference-Causing Equipment Regulations.

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

Avis de conformité à la réglementation d'Industrie Canada

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

(1) l'appareil ne doit pas produire de brouillage,

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

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

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

UK Declaration of Conformity

Hereby, Proximus Sp. z o.o., owner of SMSEagle brand, declares that the radio equipment type SMSEagle NXS-9700-3G, NXS-9700-4G, NXS-9700-5G is in compliance with The Radio Equipment Regulations 2017.

Der vollständige Text der EU-Konformitätserklärung ist unter folgender Internetadresse verfügbar: www.smseagle.eu/certification

HF-Expositionsgrenzwerte

Dieses Gerät erfüllt die Grenzwerte für die Strahlenexposition in einer unkontrollierten Umgebung. Um die Möglichkeit einer Überschreitung der Hochfrequenz-Expositionsgrenzwerte zu vermeiden, darf der menschliche Abstand zur Antenne während des normalen Betriebs nicht weniger als 30 cm (12 Zoll) betragen.

Entsorgung und Recycling-Informationen

Ihr SMSEagle-Gerät enthält eine Lithiumbatterie für RTC-Backup. Entsorgen Sie das Gerät und/oder die Batterie gemäß lokalen Umweltgesetzen und -richtlinien.

Europäische Union – Entsorgungsinformationen



Das obige Symbol bedeutet, dass Ihr Produkt gemäß lokalen Gesetzen und Vorschriften getrennt von Haushaltsabfällen entsorgt werden muss. Wenn dieses Produkt das Ende seiner Lebensdauer erreicht, bringen Sie es zu einer von den lokalen Behörden bestimmten Sammelstelle. Die getrennte

Sammlung und das Recycling Ihres Produkts zum Zeitpunkt der Entsorgung tragen dazu bei, natürliche Ressourcen zu sparen und sicherzustellen, dass es auf eine Weise recycelt wird, die die menschliche Gesundheit und die Umwelt schützt.

Für die Entsorgung in Ländern außerhalb der Europäischen Union

Dieses Symbol ist nur in der Europäischen Union (EU) gültig. Wenn Sie dieses Produkt entsorgen möchten, wenden Sie sich bitte an Ihre lokalen Behörden oder Ihren Händler und fragen Sie nach der korrekten Entsorgungsmethode.

Information gemäß § 4 Absatz 4 Elektrogesetz (DE)

Folgende Batterien bzw. Akkumulatoren sind in diesem Elektrogerät enthalten

Hardware	Batterietyp	Chemisches System
Rev.4 Rev.5	CR1216	Lithium
Rev.3	CR1632	Lithium

Angaben zur sicheren Entnahme der Batterien oder der Akkumulatoren

Hardware Rev.4-5

Rev.4 Rev.5

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

Hardware Rev.3

Rev.3

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

Restriction of Hazardous Substances Directive (RoHS)

Europäische Union RoHS

SMSEagle-Geräte, die in der Europäischen Union ab dem 3. Januar 2013 verkauft werden, erfüllen die Anforderungen der Richtlinie 2015/863 zur Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronikgeräten („RoHS 3“).