DOKUMENTATION 7.00

NXS-9750 Benutzerhandbuch

Dokumentation

DEUTSCH · SMSEAGLE

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

Table of contents

Cover . . . 9

SMSEagle Software-Lizenzinformationen . . . 10

Lieferumfang . . . 19

Konfigurationsassistent . . . 20

- Schritt 1: Sprache & Zeit . . . 20
- Schritt 2: Administratorkonto . . . 20
- Schritt 3: Benachrichtigungen . . . 21
- Schritt 4: Modems . . . 22

Anschlüsse, Anschlussports und LEDs . . . 23

Webinterface – Überblick . . . 25

- Anmeldung . . . 25
- Schnittstellenlayout . . . 26
- Dashboard . . . 26
  - Needs your attention . . . 27
  - Traffic . . . 27
  - Unread messages . . . 28
  - System . . . 28
  - Neueste Nachrichten und Anrufe . . . 29
  - Modems . . . 29
- Schnellaktionen . . . 29
- Persönliche Kontoeinstellungen . . . 30
  - Persönliche Daten . . . 30
  - Passwort . . . 31
  - Sicherheit . . . 31

Nachrichten . . . 32

- SMS (Konversationen) . . . 32
  - Nachricht verfassen . . . 33
- Ordner . . . 34
- Gruppennachrichten . . . 35
- Eskalationswarteschlange . . . 36
- Anrufe . . . 37
  - Verlauf . . . 37
- WhatsApp . . . 38
- Signal . . . 40
- E-Mails . . . 41
- Nachrichtenvorlagen . . . 41

Telefonbuch . . . 43

- Kontakte . . . 43
- Gruppen . . . 43
  - Eskalationsgruppen . . . 44

Schichten . . . 46
Bevor Sie beginnen . . . 46
Schritt 1: Öffnen Sie die Seite Schichten . . . 46
Schritt 2: Erstellen Sie eine Schicht . . . 46
Schritt 3: Weisen Sie Kontakte der Schicht zu . . . 47
Schritt 4: Wählen Sie, was außerhalb der Schichtzeiten passiert . . . 47
Automatisierung . . . 48
E-Mail zu SMS . . . 48
Wo finde ich es . . . 48
Schritt 1: Das Empfängeradressenformat verstehen . . . 48
Schritt 2: Eine neue Regel erstellen . . . 49
Schritt 3: Filterungsbedingungen hinzufügen (optional) . . . 50
Schritt 4: Vorhandene Regeln verwalten . . . 51
Email to SMS Poller . . . 51
Wo finde ich es . . . 51
Erstellen einer Regel . . . 52
SMS to Email . . . 52
Was diese Funktion macht . . . 52
Bevor Sie beginnen . . . 52
Schritt 1: Öffnen Sie die SMS to Email-Seite . . . 52
Schritt 2: Erstellen Sie eine Regel . . . 52
SMS Forward . . . 54
Was diese Funktion macht . . . 54
Bevor Sie beginnen . . . 55
Schritt 1: Öffnen Sie die SMS Forward-Seite . . . 55
Schritt 2: Erstellen Sie eine Regel . . . 55
Funktionsweise der Weiterleitng . . . 57
Automatische Antworten . . . 58
Was diese Funktion macht . . . 58
Bevor Sie beginnen . . . 58
Schritt 1: Öffnen Sie die Seite Autoreplies . . . 58
Schritt 2: Erstellen Sie eine Regel . . . 58
Schritt 3: Legen Sie das Sendeverbot fest . . . 59
Wie das Matching funktioniert . . . 60
Periodische SMS . . . 60
Was diese Funktion macht . . . 60
Bevor Sie beginnen . . . 61
Schritt 1: Öffnen Sie die Seite „Periodic SMS“ . . . 61
Schritt 2: Erstellen Sie eine Regel . . . 61
Abos . . . 63
Was diese Funktion macht . . . 63
Bevor Sie beginnen . . . 64
Schritt 1: Öffnen Sie die Seite „Subscriptions . . . 64
Schritt 2: Erstellen Sie eine Regel . . . 64
Wie das Matching funktioniert . . . 64
Was passiert, wenn sich jemand abonniert . . . 65
Allow / Deny List . . . 65

Was diese Funktion macht . . . 65
Bevor Sie beginnen . . . 66
Schritt 1: Öffnen Sie die Seite „Zulassen/Ablehnen-Liste“ . . . 66
Schritt 2: Wählen Sie den aktiven Modus . . . 66
Schritt 3: Fügen Sie eine Nummer hinzu . . . 66
Schritt 4: Importieren Sie eine Liste aus einer CSV-Datei . . . 67
Schritt 5: Konfigurieren Sie das STOP-Wort (optional) . . . 67
So funktioniert die Filterung . . . 68
Workflows . . . 69
Wo finde ich es . . . 69
Schritt 1: Erstellen Sie einen Workflow und wählen Sie einen Trigger . . . 69
Schritt 2: Bedingungsgruppen hinzufügen (optional) . . . 69
Schritt 3: Aktionen hinzufügen . . . 69
Webhooks . . . 70
Was diese Funktion macht . . . 70
Bevor Sie beginnen . . . 70
Schritt 1: Webhooks-Seite öffnen . . . 70
Schritt 2: Erstellen Sie eine Regel . . . 71
Schritt 3: Grundkonfiguration . . . 71
Schritt 4: Auslösebedingungen . . . 73
Schritt 5: Sicherheitseinstellungen . . . 74
Schritt 6: Wiederholungsintervall festlegen . . . 75
Verhalten von Webhooks . . . 75
MQTT . . . 75
Was diese Funktion macht . . . 75
Bevor Sie beginnen . . . 76
Teil 1: Subscribe (MQTT zu SMS) . . . 76
Teil 2: Publish (SMS in MQTT) . . . 78
Posteingangsregeln . . . 80
Wo finde ich es . . . 80
Konfigurieren einer Posteingangsregel . . . 80
Ordner bereinigen . . . 80
Wo finde ich es . . . 80
Konfigurieren einer Bereinigungsregel . . . 81
Berichte & Statistiken . . . 82
Berichte . . . 82
Periodische Berichte . . . 83
Statistiken . . . 84
Periodische Statistiken . . . 85
Überwachung . . . 86
Netzwerkmonitor . . . 86
Funktion dieser Funktion . . . 86
Bevor Sie beginnen . . . 86
Teil 1: Tasks . . . 87
Teil 2: Reports . . . 92
Teil 3: SNMP Traps . . . 94

Verhalten der Netzwerküberwachung . . . 96
Digitale Ein-/Ausgabe . . . 96
Funktion dieser Funktion . . . 96
Bevor Sie beginnen . . . 97
Hardware: ports, logic levels and wiring . . . 97
Wo man es findet . . . 100
Teil 1: Eingaberegeln (Eingangssignal in SMS) . . . 101
Teil 2: Ausgangsregeln (SMS in Ausgangssignal) . . . 104
Teil 3: Interne Pins . . . 107
Teil 4: Externe Pins . . . 108
So verhalten sich Digital-I/O-Regeln . . . 109
Temperatur- und Feuchtigkeitssensoren . . . 110
Funktion dieser Funktion . . . 110
Bevor Sie beginnen . . . 110
Wo man es findet . . . 111
Teil 1: Sensoren hinzufügen und benennen . . . 111
Teil 2: Alarmregeln . . . 114
Teil 3: Messwerte und Berichte . . . 116
Verhalten . . . 117
Einstellungen . . . 118
Kontoeinstellungen . . . 118
Konfiguration der Multi-Faktor-Authentifizierung (MFA) . . . 118
SMS / MMS . . . 119
Nachrichten . . . 119
Modems . . . 120
Multimodem . . . 120
MMS . . . 123
Anrufe . . . 126
TTS-Lokalmodelle . . . 126
TTS-Online-Modelle (ElevenLabs) . . . 128
Eingehende Anrufe . . . 130
Anrufweiterleitung . . . 130
WhatsApp . . . 131
Was diese Funktion bewirkt . . . 131
Bevor Sie beginnen . . . 131
Schritt 1: Öffnen Sie die WhatsApp-Einstellungen . . . 132
Schritt 2: Aktivieren Sie den Service . . . 132
Schritt 3: Verknüpfen Sie Ihr Telefon . . . 132
Schritt 4: Entscheiden Sie, was mit Empfängern ohne WhatsApp passiert . . . 132
Schritt 5: Halten Sie den Service auf dem neuesten Stand . . . 132
Verknüpfung aufheben und ausschalten . . . 133
Gut zu wissen . . . 133
Signal . . . 134
Was diese Funktion bewirkt . . . 134
Bevor Sie beginnen . . . 134
Schritt 1: Öffnen Sie die Signal-Einstellungen . . . 135
Schritt 2: Aktivieren Sie den Service . . . 135

Schritt 3: Registrieren Sie eine Telefonnummer . . . 135
Schritt 4: Verifizieren Sie die Nummer . . . 136
Schritt 5: Halten Sie den Service auf dem neuesten Stand . . . 136
Die Nummer entfernen . . . 136
Gut zu wissen . . . 137
, aber die Registrierung bleibt erhalten, sodass eine erneute Aktivierung keine neue Verifikation erfordert. . . . 137
, Eine registrierte Signal-Nummer . . . 137
Email to SMS Poller . . . 139
SMTP-Konfiguration . . . 141
E-Mail-Warnungen . . . 141
SMPP . . . 142
Verbindungsdetails . . . 143
SMPP aktivieren . . . 143
MQTT . . . 144
Netzwerk . . . 145
IP-Einstellungen . . . 145
SSL . . . 146
Failover . . . 146
SNMP . . . 147
Mobile Daten . . . 152
Anwendung . . . 153
Regional . . . 153
Sicherheit . . . 153
Zugriff und Sichtbarkeit . . . 153
API und Integrationen . . . 154
LDAP . . . 154
Was diese Funktion bewirkt . . . 154
Bevor Sie beginnen . . . 155
Schritt 1: LDAP-Seite öffnen . . . 155
Schritt 2: Integration aktivieren . . . 155
Schritt 3: Verbindung . . . 156
Schritt 4: Verzeichnisstruktur . . . 156
Schritt 5: Attribute und Sicherheit . . . 157
Schritt 6: Synchronisierung und Zugriff . . . 157
Schritt 7: Speichern und testen . . . 159
Datum / Zeit . . . 160

System . . . 161
Benutzer . . . 161
Systeminformationen . . . 161
Protokolle . . . 162
Updates . . . 162
Patches . . . 162
Backup / Restore . . . 162
Neustart . . . 162
Erweitert . . . 162

API und Entwicklerintegrationen . . . 163
API-Referenz . . . 163
API-Schlüssel . . . 163
API v2-Schlüssel . . . 163
API v1-Schlüssel . . . 164
Schlüssel erstellen . . . 164
Welche Benutzer haben API-Zugriff . . . 165
Zugriff auf Ressourcen anderer Benutzer . . . 166
Plugins und Integrationen . . . 167
Erweitert . . . 168
Direkter Zugriff auf die SMSEagle-Datenbank . . . 168
Injizieren einer Kurz-SMS mit SQL . . . 168
Injizieren einer Langtext-SMS mit SQL . . . 169
Datenbankbereinigungsskripte . . . 171
Weitergabe von Logs an einen externen Server . . . 171
Fehlerbehebung . . . 173
Überprüfung der LEDs . . . 173
Überprüfung der Geräteinformationen . . . 174
Geräteprotokolle . . . 174
Wenn das Gerät nicht erreichbar ist . . . 174
Wiederherstellen von Werkseinstellungen . . . 174
Hardware Rev.5 und später . . . 175
Hardware Rev.3–Rev.4 . . . 175
Service & Reparatur . . . 176
Garantie . . . 176
Service . . . 176
Technische Spezifikationen & Sicherheitsinformationen . . . 177
Technische Spezifikation . . . 177
Hardware-Spezifikation . . . 177
Stromversorgung . . . 179
Antenne . . . 179
Durchsatz beim Senden/Empfangen . . . 179
Software-Plattform . . . 180
Wichtige Sicherheitsinformationen . . . 180
Behördliche Erklärungen . . . 182
EU-Konformitätserklärung . . . 182
FCC-Konformitätserklärung . . . 182
FCC-Konformitätserklärung des Lieferanten . . . 183
Kanadische behördliche Erklärung (ISED) . . . 183
Avis de conformité à la réglementation d'Industrie Canada . . . 184
UK Declaration of Conformity . . . 184
RF-Expositionsgrenzen . . . 184
Entsorgung und Recyclinginformationen . . . 184

Europäische Union – Entsorgungsinformationen 184
Für die Entsorgung in Ländern außerhalb der Europäischen Union 185
Information gemäß § 4 Absatz 4 Elektrogesetz (DE) 185
Angaben zur sicheren Entnahme der Batterien oder der Akkumulatoren 185
Richtlinie zur Beschränkung gefährlicher Stoffe (RoHS) 186
Europäische Union RoHS 186

Cover

Willkommen zum Benutzerhandbuch des NXS-9750!

Der NXS-9750 ist ein Hardware-SMS-Gateway mit zwei integrierten Modems und Ihren eigenen SIM-Karten, sodass Ihre Nachrichten direkt über das Mobilfunknetz aus Ihrer eigenen Infrastruktur versendet werden, ohne einen Drittanbieter-SMS-Dienst dazwischen.

Dieses Handbuch ist das vollständige Nachschlagewerk für das Gerät und gilt für alle NXS-9750-Varianten. Falls das Verhalten vom Modemtyp oder der Hardwarereversion abhängt, ist der entsprechende 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. Nutzen Sie andernfalls die Navigation auf der linken Seite oder das Suchfeld, um direkt zum gewünschten Thema zu gelangen.

Die in dieser Veröffentlichung verwendeten Materialien sind urheberrechtlich geschützt 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.

SMSEagle Software-Lizenzinformationen

WICHTIG – VOR DER INBETRIEBNAHME LESEN

SMSEAGLE SOFTWARE-ENDBENUTZER-LIZENZVERTRAG

Der hierin enthaltene Endbenutzer-Lizenzvertrag (die „**Vereinbarung**“ oder „**Lizenz**“ oder „**EULA**“) gilt als rechtsverbindliche Vereinbarung zwischen Ihnen (einer natürlichen oder juristischen Person, nachfolgend „**Lizenznehmer**“ oder „**Sie**“ oder „**Ihr**“) und Proximus Sp. z o.o., ul. Piątkowska 163, Poznań, Polen, PLZ 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 weitere Komponenten und/oder Softwaremodule enthalten kann, einschließlich, aber nicht beschränkt auf erforderliche Treiber (die „**SMSEagle-Software**“). Weitere Aspekte der SMSEagle-Software können unter anderem auch Software-Updates und Upgrades umfassen, die PROXIMUS Ihnen zur Verfügung stellt oder zugänglich macht, oder die Sie nach dem Erwerb des SMSEagle-Geräts erhalten, sofern diesen Elementen kein separater Lizenzvertrag oder eigene 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, DÜRFEN SIE DAS SMSEAGLE-GERÄT NICHT VERWENDEN UND KÖNNEN DAS GERÄT UMGEHEND ZUR RÜCKERSTATTUNG DES KAUFPREISES ZURÜCKGEBEN, 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 in der GUI des SMSEagle-Geräts während der Ersteinrichtung sowie nach jeder wesentlichen Änderung ihrer Bedingungen 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 GEISTIGEN EIGENTUM GESCHÜTZT. DIE SMSEAGLE-SOFTWARE WIRD LIZENZIERT UND NICHT VERKAUFT. SÄMTLICHE RECHTE, EINSCHLIESSLICH DER URHEBERRECHTE AN DER SMSEAGLE-SOFTWARE, VERBLEIBEN IM ALLEINIGEN EIGENTUM VON PROXIMUS. ZUSÄTZLICH ENTHÄLT DIE SMSEAGLE-SOFTWARE, WIE UNTEN AUSGEFÜHRT, EINIGE VON DRITTEN ENTWICKELTE MODULE, DIE IHNEN HIERMIT GEMÄSS DEN VOM ENTWICKLER ZUGELASSENEN BEDINGUNGEN UNTERLIZENZIERT WERDEN.

Diese EULA gewährt Ihnen bestimmte Rechte, und Sie können darüber hinaus über weitere gesetzliche Rechte verfügen, die je nach Rechtsordnung variieren. Die Haftungsausschlüsse, Ausschlüsse und Haftungsbeschränkungen im Rahmen dieser EULA gelten nur insoweit, als dies nach geltendem Recht nicht untersagt ist. Einige Rechtsordnungen lassen den Ausschluss stillschweigender Gewährleistungen oder den Ausschluss bzw. die Beschränkung von Neben- oder Folgeschäden oder anderen Rechten nicht zu, sodass diese Bestimmungen der EULA in solchen

Fällen möglicherweise nicht auf Sie anwendbar sind. Dies beeinträchtigt jedoch nicht die Durchführbarkeit und Anwendbarkeit aller übrigen Bestimmungen der EULA.

1. **DEFINITIONEN UND AUSLEGUNGEN**
    1. „Vereinbarung“ oder „Lizenz“ oder „EULA“ bezeichnet diesen Endbenutzer-Lizenzvertrag.
    2. „Lizenznehmer“ oder „Sie“ oder „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, Recht des Geschäftsgeheimnisses, Markenrecht, Urheberpersönlichkeitsrecht und anderen ähnlichen Rechten.
    4. „Update“ bezeichnet die Wartung oder Behebung von Fehlern einer Version der SMSEagle-Software, einschließlich, aber nicht beschränkt auf Hotfixes, Patches oder Verbesserungen, die keine eigenständige Dienstleistung oder ein separates Softwarepaket darstellen und für die bestehende Lizenznehmer keine zusätzlichen Kosten anfallen.
    5. „Upgrade“ bezeichnet eine bedeutende, eigenständige Version der SMSEagle-Software, die zusätzliche Anwendungen, Funktionen oder Fähigkeiten enthalten kann.
    6. Ein Verweis auf „Person“ umfasst eine natürliche Person, eine Körperschaft oder nicht rechtsfähige Vereinigung (unabhängig davon, ob diese eine eigene Rechtspersönlichkeit besitzt) sowie deren gesetzliche und persönliche Vertreter, Rechtsnachfolger und zulässige Rechtsnachfolger.
    7. Wörter im Singular schließen den Plural ein und umgekehrt.
    8. Ein Verweis auf ein Gesetz, eine gesetzliche Bestimmung oder untergeordnete Rechtsvorschriften bezieht sich auf deren jeweils gültige Fassung, unter Berücksichtigung etwaiger Änderungen oder Neufassungen, und umfasst auch jedes Gesetz, jede gesetzliche Bestimmung oder untergeordnete Rechtsvorschrift, die dadurch geändert oder neu gefasst wird; vorausgesetzt, dass zwischen den Parteien keine solche Änderung oder Neufassung im Rahmen dieser Vereinbarung insoweit Anwendung findet, als sie eine neue oder erweiterte Verpflichtung, Haftung oder Beschränkung auferlegen oder die Rechte einer Partei anderweitig beeinträchtigen würde.
    1. Ein Verweis auf Schriftform oder schriftlich schließt E-Mail ein.
    2. Jede Verpflichtung in dieser Vereinbarung, wonach eine Person etwas nicht tun darf, umfasst auch die Verpflichtung, nicht zuzustimmen oder zuzulassen, dass diese Handlung vorgenommen wird.
    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 dieser Vereinbarung.

5. „Wir“, „Uns“ und „Unser“ beziehen sich auf Proximus Sp. z o.o. („PROXIMUS“).
6. Die „Parteien“ dieser Vereinbarung sind Sie und Proximus Sp. z o.o. („PROXIMUS“).
7. „Erfassen“ bezieht sich auf die Übertragung von Daten vom Gerät in einer Weise, die es PROXIMUS oder Drittpartnern ermöglicht, darauf zuzugreifen.

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 dargelegten 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 alle 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 sowie andere Gesetze und Abkommen zum geistigen Eigentum 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 ihnen zugänglich machen; (c) Teile der SMSEagle-Software modifizieren, anpassen, davon abgeleitete Werke erstellen oder übersetzen, sofern dies nicht im Rahmen der Nutzung auf Ihrem SMSEagle-Gerät gemäß dieser Lizenz erfolgt; (d) die SMSEagle-Software zurückentwickeln (Reverse Engineering), dekompilieren oder disassemblieren, noch versuchen, deren Quellcode zu ermitteln oder zu erhalten (außer soweit dies durch zwingende Bestimmungen des anwendbaren Rechts gestattet ist, einschließlich Artikel 6 der Richtlinie 2009/24/EG über die Dekompilierung zum Zweck der Interoperabilität mit anderen Programmen); (e) versuchen, Marken-, Urheberrechts- oder sonstige Eigentumshinweise innerhalb der SMSEagle-Software zu verändern oder zu entfernen; oder (f) die SMSEagle-Software in einer Weise nutzen, die nicht in dieser EULA oder der dem SMSEagle-Gerät beiliegenden Dokumentation vorgesehen ist, auf dem sie vorinstalliert war.
    3. **UPDATES/UPGRADES**. PROXIMUS kann es für angebracht halten, Updates oder Upgrades für die SMSEagle-Software bereitzustellen. Sie können den Installationsprozess für ein Update oder Upgrade einleiten, indem Sie beispielsweise auf die Schaltfläche „Check for software updates now“ in der Weboberfläche des SMSEagle-Geräts 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 dieser Updates oder Upgrades an Sie von der Annahme einer weiteren EULA oder dem Abschluss einer anderen 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 dieser EULA und/oder einer anderen Vereinbarung zu unterliegen. PROXIMUS verpflichtet sich, für die SMSEagle-Software für einen Mindestzeitraum von fünf (5) Jahren ab dem Datum des ersten Verkaufs des jeweiligen SMSEagle-Gerätemodells Sicherheitsupdates 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 etwaigen längeren Supportzeitraums, der durch zwingende Bestimmungen des anwendbaren Rechts vorgeschrieben sein könnte, einschließlich des Cyber Resilience Act und der NIS2-Richtlinie.

2. **HAFTUNGSAUSSCHLUSS FÜR GEWÄHRLEISTUNG**

PROXIMUS wird angemessene Anstrengungen im Einklang mit den vorherrschenden Standards der Softwareentwicklung unternehmen, 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 ÜBERNIMMT PROXIMUS EINE GEWÄHRLEISTUNG FÜR DIE ERGEBNISSE, DIE DURCH DIE NUTZUNG DER SMSEAGLE-SOFTWARE ERZIELT WERDEN KÖNNEN.

SOWEIT NACH ANWENDBAREM RECHT ZULÄSSIG, ÜBERNIMMT AUSSER WIE HIERIN AUSDRÜCKLICH VORGESEHEN UND UNGEACHTET GEGENTEILIGER BESTIMMUNGEN WEDER PROXIMUS NOCH EIN LEITENDER ANGESTELLTER, DIREKTOR, TOCHTERUNTERNEHMEN, VERBUNDENES UNTERNEHMEN, AUTORISIERTER WIEDERVERKÄUFER ODER MITARBEITER DAVON EINE WEITERE GEWÄHRLEISTUNG JEGLICHER ART, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND, GESETZLICH ODER ANDERWEITIG, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF GEWÄHRLEISTUNGEN DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN DRITTER.

1. **HAFTUNGSBESCHRÄNKUNG**
    1. Die Haftung von PROXIMUS im Zusammenhang mit einem Anspruch, der durch die Nutzung der SMSEagle-Software verursacht wird, damit zusammenhängt oder daraus entsteht, oder die Summe solcher Ansprüche, überschreitet niemals 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.
    2. PROXIMUS haftet gegenüber dem Lizenznehmer nicht für indirekte oder Folgeschäden, einschließlich entgangenen Gewinns jeglicher Art sowie des Verlusts von Kunden,

Umsatz, Marge, Produktion, Image, Daten oder Konfiguration, wobei der vorstehende Ausschluss nicht für Schäden gilt, die von PROXIMUS vorsätzlich verursacht wurden.

3. PROXIMUS haftet insbesondere nicht für: (i) den Verlust von Daten oder Konfigurationen; (ii) entgangenen Gewinn des Lizenznehmers; (iii) indirekte oder Folgeschäden; (iv) Handlungen Dritter.
4. Im Hinblick auf die Haftung von PROXIMUS für Ansprüche des Endnutzers ist die Haftung von PROXIMUS ausschließlich auf Situationen beschränkt, in denen der Schaden das Ergebnis einer direkten Handlung oder Unterlassung von PROXIMUS ist, und nur 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 im Sinne des polnischen Rechts Verbraucher oder Einzelunternehmer sind, soweit die hierin enthaltenen Beschränkungen nach zwingenden verbraucherschützenden Bestimmungen unzulässig sind.

2. **OPEN SOURCE**

Bestimmte Softwaremodule in der PROXIMUS-Software unterliegen „Open-Source"- oder „freien 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 unter den Bedingungen der Endnutzerlizenz lizenziert, die dieser Open-Source-Software beiliegt. Nichts in dieser Vereinbarung schränkt Ihre Rechte im Rahmen der geltenden Endnutzerlizenz für die Open-Source-Software ein oder gewährt Ihnen Rechte, die diese Bedingungen ersetzen. Zu den geltenden Open-Source-Lizenzen gehören: MIT-Lizenz; GNU General Public License v. 2.0; GNU Lesser General Public License v. 2.1; BSD-3-Clause-Lizenz; Apache-Lizenz 2.0. Sofern von einer bestimmten Open-Source-Software-Lizenz verlangt, stellt PROXIMUS diese Open-Source-Software sowie Unsere Änderungen an dieser Open-Source-Software auf schriftliche Anfrage an Uns über die angegebene E-Mail- oder Postadresse zur Verfügung.

1. **ENDNUTZER DER US-REGIERUNG**

Die SMSEagle-Software wird der US-Regierung mit EINGESCHRÄNKTEN RECHTEN lizenziert. Die Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt, soweit anwendbar, den Einschränkungen gemäß DFARS 252.227-7013 der Klausel zu Technischen Daten und Computersoftware sowie 48 CFR 52.227-19 der Klausel zu Commercial Computer Software.

1. **DATENSCHUTZ**

1. **ERKLÄRUNG ZUR DATENERFASSUNG**. PROXIMUS erfasst KEINE Daten, mit denen Sie bei der Nutzung des SMSEagle-Geräts arbeiten. Wir können keine auf dem SMSEagle-Gerät gespeicherten Daten einsehen oder erfassen, 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, dessen

bevollmächtigter 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 Lizenzdaten (Firmenname, Ansprechpartner, E-Mail, Seriennummer des Geräts); (b) Update-/Upgrade-Telemetriedaten, die streng auf Softwareversion, Gerätemodell, Seriennummer des Geräts und, sofern zutreffend, IP-Adresse beschränkt sind. Die im Zusammenhang mit der Bereitstellung von technischem Support verarbeiteten personenbezogenen Daten unterliegen einer separaten Richtlinie zu technischen Support-Dienstleistungen, die auf der Website von Proximus verfügbar ist: www.smseagle.eu.
4. Zwecke und Rechtsgrundlagen der Verarbeitung: (a) Erfüllung dieser 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 Abwehr von Ansprüchen – Artikel 6 Abs. 1 lit. f DSGVO.
5. Empfänger personenbezogener Daten: autorisierte Mitarbeiter und Auftragnehmer von PROXIMUS, die zur Vertraulichkeit verpflichtet sind, IT-Dienstleister (Hosting, E-Mail, Ticketing), die als Auftragsverarbeiter gemäß Artikel 28 DSGVO handeln, 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. durch die Nutzung bestimmter IT-Anbieter), erfolgen diese auf Grundlage eines Angemessenheitsbeschlusses oder geeigneter Garantien wie den EU-Standardvertragsklauseln.
7. Aufbewahrungsdauer: Registrierungs- und Lizenzdaten – für die Laufzeit dieser EULA sowie für den nach geltendem Recht erforderlichen Zeitraum (insbesondere Steuer- und Buchhaltungsrecht, typischerweise 5 Jahre); auf Grundlage berechtigter Interessen verarbeitete Daten – bis zum Eingang eines wirksamen Widerspruchs oder bis das berechtigte Interesse entfällt.
8. Rechte der betroffenen Personen: Der Lizenznehmer hat das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragbarkeit 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 dieser EULA keine automatisierte Entscheidungsfindung, einschließlich Profiling, im Sinne von Artikel 22 DSGVO durch.

11. Die Bereitstellung personenbezogener Daten ist freiwillig, jedoch für den Abschluss und die Erfüllung dieser 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, diese EULA mit sofortiger Wirkung zu kündigen im Falle: (i) einer wesentlichen Verletzung der im Abschnitt „Einschränkungen der Nutzung“ festgelegten Lizenzbeschränkungen durch den Lizenznehmer; (ii) einer unbefugten Vervielfältigung, Verbreitung oder Modifikation der SMSEagle-Software; oder (iii) der 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 Kündigungsfrist von mindestens dreißig (30) Tagen kündigen.
    3. Vorbehaltlich zwingender Verbraucherschutzgesetze ist der Lizenznehmer, falls PROXIMUS diese EULA aus den in Abschnitt 9.01. oben genannten Gründen kündigt, nicht berechtigt, eine Rückerstattung des Kaufpreises des SMSEagle-Geräts oder etwaiger im Zusammenhang mit der SMSEagle-Software gezahlter Gebühren zu erhalten.
    4. Nach Beendigung dieser EULA hat der Lizenznehmer jede Nutzung der SMSEagle-Software einzustellen und alle vorhandenen Sicherungskopien unbrauchbar zu machen. Die Abschnitte „Geistiges Eigentum“, „Gewährleistungsausschluss“, „Haftungsbeschränkung und Rechtsmittel“, „Datenschutz“, „Anwendbares Recht“ und „Streitbeilegung“ bleiben auch nach Beendigung wirksam.
    5. Wenn der Lizenznehmer das SMSEagle-Gerät von einem Wiederverkäufer oder autorisierten Partner erworben hat, sind die Regeln für Rückgaben, Stornierungen und Rückerstattungen des SMSEagle-Geräts auf der Rechnung oder in anderen Verkaufsunterlagen des jeweiligen Wiederverkäufers oder autorisierten Partners angegeben.
    6. Diese EULA gilt unabhängig von einer für das SMSEagle-Gerät geltenden Hardware-Garantie. Das Erlöschen oder die Beendigung dieser EULA berührt nicht die Gültigkeit und Dauer der dem SMSEagle-Gerät zugewiesenen Hardware-Garantie, ebenso wie die Bedingungen der Hardware-Garantie die Rechte des Lizenznehmers aus dieser EULA nicht einschränken.

3. **SONSTIGES**

    1. **RECHTSNACHFOLGER UND ABTRETUNGSEMPFÄNGER**. Diese EULA ist in ihrer Gesamtheit rechtlich bindend für und kommt zugute von PROXIMUS und Ihnen sowie unseren jeweiligen Rechtsnachfolgern und zulässigen Abtretungsempfängern.
    2. **TEILBARKEIT**. Sollte eine Bestimmung dieser Vereinbarung von einem zuständigen Gericht für rechtswidrig, unwirksam oder nicht durchsetzbar erklärt werden, bleiben die übrigen Bestimmungen davon unberührt.

3. **VERZICHT**. Ein Verzicht auf die Geltendmachung eines Verstoßes oder die Nichtdurchsetzung 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 Modifikation einer Bestimmung dieser EULA ist nur wirksam, wenn sie schriftlich erfolgt und von PROXIMUS unterzeichnet wird.
5. **ANWENDBARES RECHT**. In nicht hierin geregelten Angelegenheiten gelten die Bestimmungen des polnischen Zivilgesetzbuches sowie die Bestimmungen des polnischen Urheberrechtsgesetzes vom 4. Februar 1994 (Gesetzblatt 1994, Nr. 24, Pos. 83). Diese Vereinbarung unterliegt in allen Belangen dem Recht der Republik Polen.
6. **STREITBEILEGUNG**. Alle Streitigkeiten, die sich aus oder im Zusammenhang mit dieser Vereinbarung ergeben, unterliegen der ausschließlichen Zuständigkeit der ordentlichen Gerichte am Sitz von PROXIMUS in Posen, Polen. Diese Bestimmung gilt nicht für Lizenznehmer, die Verbraucher oder Einzelunternehmer im Sinne des polnischen Rechts sind und die das Recht behalten, Verfahren vor dem nach zwingenden Rechtsvorschriften zuständigen Gericht anzustrengen.
7. **ÜBERTRAGUNGEN**. Sie sind berechtigt, die SMSEagle-Software nur zusammen mit der dauerhaften Übertragung des Eigentums an dem SMSEagle-Gerät, auf dem sie vorinstalliert war, an einen Dritten zu übertragen. In diesem Fall ist der Erwerber verpflichtet, diese EULA in ihrer aktuellen Fassung vor der Nutzung der SMSEagle-Software zu akzeptieren, und Sie haben alle bei Ihnen vorhandenen Sicherungs- oder sonstigen Kopien der SMSEagle-Software zum Zeitpunkt der Übertragung unbrauchbar zu machen. Diese Bestimmung lässt die Doktrin der Erschöpfung von Rechten gemäß Artikel 4 Absatz 2 der Richtlinie 2009/24/EG sowie etwaige zwingende Rechte des Lizenznehmers nach EU-Recht unberührt.
8. **GÜLTIGKEIT UND VERBINDLICHKEIT**. Diese Vereinbarung stellt eine gültige und rechtlich bindende Verpflichtung der Parteien dar, die gemäß ihren Bedingungen gegenüber den Parteien durchsetzbar ist, vorbehaltlich in allen Belangen der Auswirkungen von Insolvenz, Zahlungsunfähigkeit, betrügerischer Vermögensübertragung, Reorganisation, Moratorium und anderen Gesetzen, die die Rechte von Gläubigern im Allgemeinen betreffen, sowie allgemeiner Grundsätze der Billigkeit.
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 ist eine Partei, die durch Umstände, die außerhalb ihrer angemessenen Kontrolle liegen, an der Erfüllung ihrer Verpflichtungen aus dieser Vereinbarung gehindert oder daran unfähig ist – einschließlich, aber nicht beschränkt auf höhere Gewalt, Handlungen zivilen oder militärischen Behörden, Aufstände oder zivilen Ungehorsam, Kriege, Streiks oder Arbeitskonflikte (jeweils ein „**Ereignis höherer Gewalt**“) –, von der Erfüllung befreit, und

die Erfüllungsfrist verlängert sich entsprechend, sofern die betroffene Partei unverzüglich alle angemessenen und notwendigen Schritte unternimmt, um die vollständige Erfüllung wieder aufzunehmen.

4. **VERBRAUCHERSCHUTZ UND SCHUTZ VON EINZELUNTERNEHMERN**

Die Bestimmungen dieser EULA beeinträchtigen nicht die Bestimmungen zum Verbraucherschutz und zum Schutz von Einzelunternehmern, falls Sie eine natürliche Person sind, die das Gerät kauft und diese EULA nicht direkt im Zusammenhang mit ihrer geschäftlichen oder beruflichen Tätigkeit abschließt, oder im Fall eines Einzelunternehmers, der eine natürliche Person ist – nicht direkt im Zusammenhang mit ihrer beruflichen Tätigkeit (anwendbar auf die EULA, die ab dem 1. Januar 2021 abgeschlossen wird). Sollte eine Bestimmung dieser EULA mit zwingenden Gesetzen zum Verbraucherschutz oder zum Schutz von Einzelunternehmern unvereinbar sein, bindet die Bestimmung den Verbraucher/Einzelunternehmer nicht, und es gilt die Bestimmung des allgemein geltenden Gesetzes, die dieser Bestimmung am nächsten kommt.

1. **KONTAKTINFORMATIONEN**

Falls Sie Fragen zu dieser EULA haben, kontaktieren Sie bitte PROXIMUS unter:

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

Lieferumfang



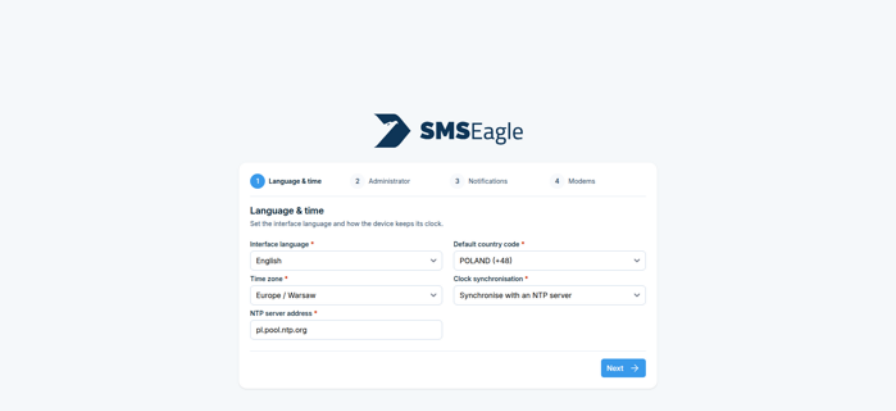
Inhalt der SMSEagle Box

Ihre SMSEagle Box enthält:

- SMSEagle Hardware SMS-Gateway
- 2x externe omnidirektionale Antenne (mit Magnetfuß)
- AC/DC-Netzteil (Eingangsspannung: 100-240V)
- Schnellstartanleitung
- Garantiekarte

Konfigurationsassistent

Wenn Sie sich zum ersten Mal bei 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 die restliche Weboberfläche nicht zugreifen, bis dieser abgeschlossen ist.

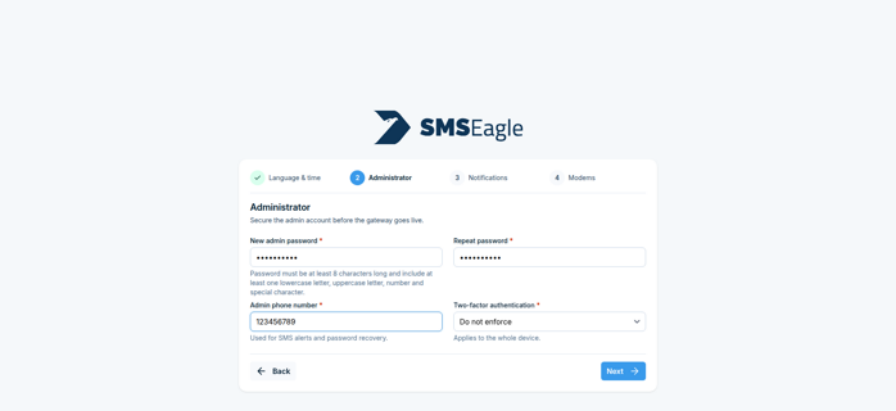


Schritt 1: Sprache & Zeit

Schritt 1: Sprache & Zeit

Legen Sie die Oberflächensprache, 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: Administratorkonto



Schritt 2: Administratorkonto

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-Benachrichtigungen und Passwortwiederherstellung verwendet
Zwei-Faktor-Authentifizierung	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

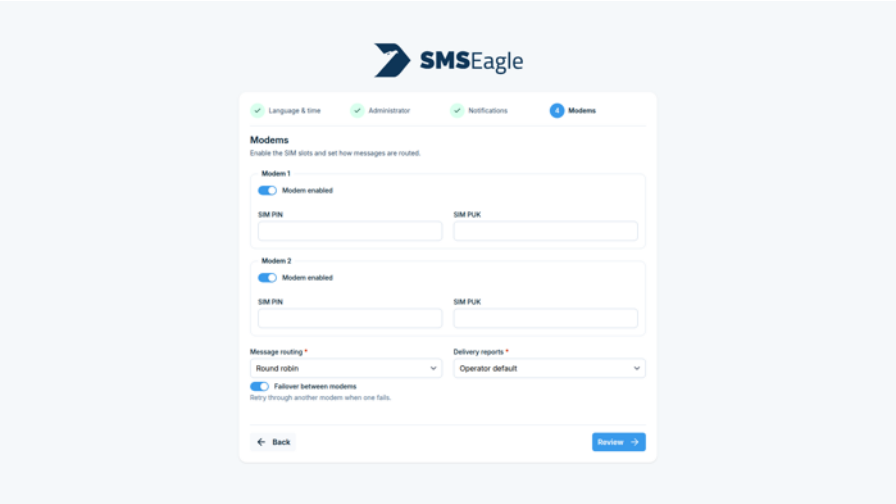


Schritt 3: Benachrichtigungen

Wählen Sie, worüber Sie das Gerät benachrichtigen soll:

- Automatisch auf Software-Updates prüfen und den Admin optional per SMS benachrichtigen, wenn eine neue Version verfügbar ist
- Automatisch die Supportgültigkeit prüfen und den Admin optional per SMS benachrichtigen, wenn der Support bald abläuft

Schritt 4: Modems



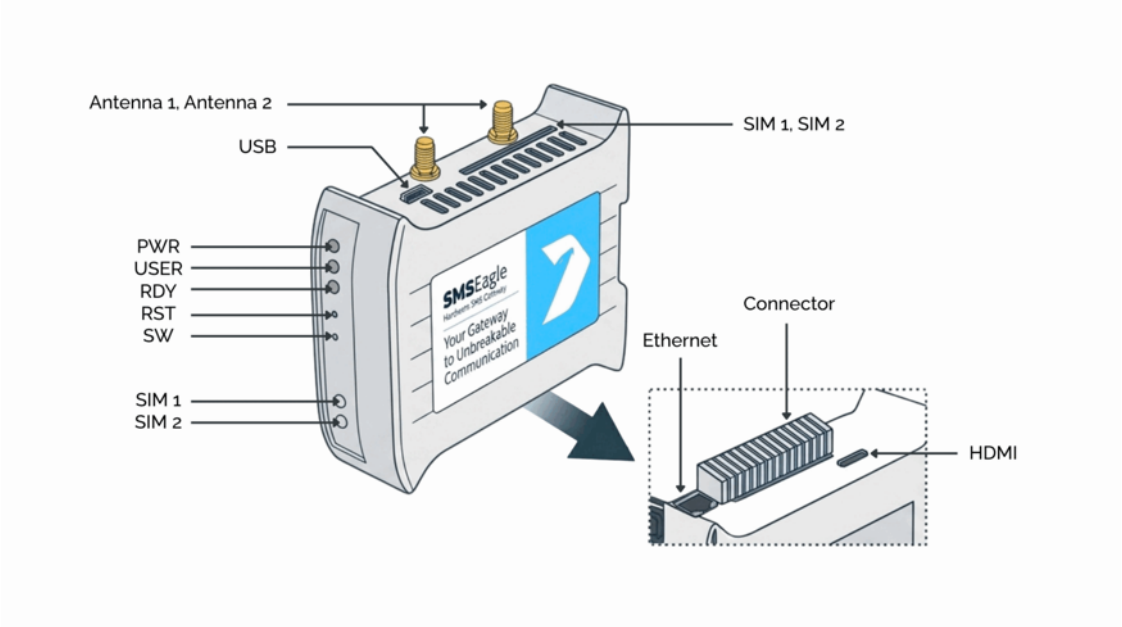
Schritt 4: Modems

Aktivieren Sie für jedes integrierte Modem (Modem 1, Modem 2 auf Multi-Modem-Geräten) und geben Sie ggf. seine **SIM-PIN** und **SIM-PUK** ein. Legen Sie dann Folgendes fest:

- **Nachrichtenrouting** – Round Robin, SIM 1 als Master oder SIM 2 als Master (siehe Multimodem-Auswahlstrategie)
- **Zustellungsberichte** – Operator-Standard, Immer anfordern oder Nie anfordern
- **Failover zwischen Modems** – Wiederholung über das andere Modem, wenn eines ausfällt

Überprüfen Sie Ihre Einstellungen und beenden Sie den Assistenten, um das normale Dashboard zu erreichen.

Anschlüsse, Anschlussports 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	SIM1, SIM2	SIM-Kartensteckplätze
HDMI-Port	HDMI	HDMI-Port (nur zu Debugging-Zwecken)
USB-Port	USB	USB-Port (nur zu Debugging-Zwecken)
Ethernet-Port	ETH	Ethernet-RJ45-Buchse
Antenne	ANT1, ANT2	Zwei Antennenbuchsen, eine pro Modem
Power-LED	PWR	LED zur Anzeige des Einschaltzustands
User LED	USER	LED für Anwenderzwecke
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

Webinterface – Überblick

Dieses Kapitel bietet einen schnellen Überblick über die SMSEagle-Weboberfläche selbst, bevor die einzelnen Funktionen im Rest dieses Handbuchs behandelt werden.

Anmeldung

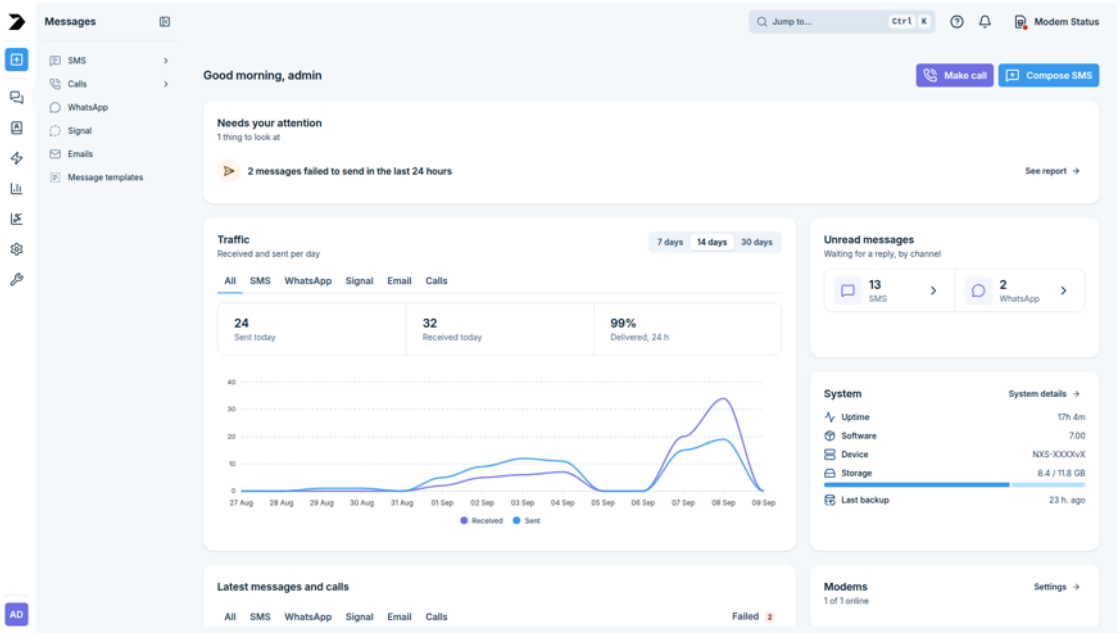


Die Anmeldungsseite

Geben Sie die IP-Adresse oder den Hostnamen des Geräts in einen Browser ein und melden Sie sich mit Benutzername und Passwort an. Falls Multi-Faktor-Authentifizierung geräteweit erzwungen wurde (siehe MFA), werden Sie auch nach einem Einmalcode gefragt.

- **Authentication type** legt fest, wo die Anmeldedaten überprüft werden: **Local (default)** gegen die eigene Benutzerliste des Geräts oder **LDAP** gegen einen Verzeichnisserver, den ein Administrator zunächst unter LDAP konfiguriert.
- **Forgot password?** sendet Wiederherstellungsanweisungen an die im Konto hinterlegte Telefonnummer per SMS. Identifizieren Sie sich dort mit Ihrem Benutzernamen oder dieser Telefonnummer.
- Der Selektor in der unteren rechten Ecke legt die Sprache der Anmeldungsseite fest. Die Sprache der Oberfläche nach der Anmeldung stammt aus Ihrem eigenen Konto, siehe Personal account settings.

Schnittstellenlayout

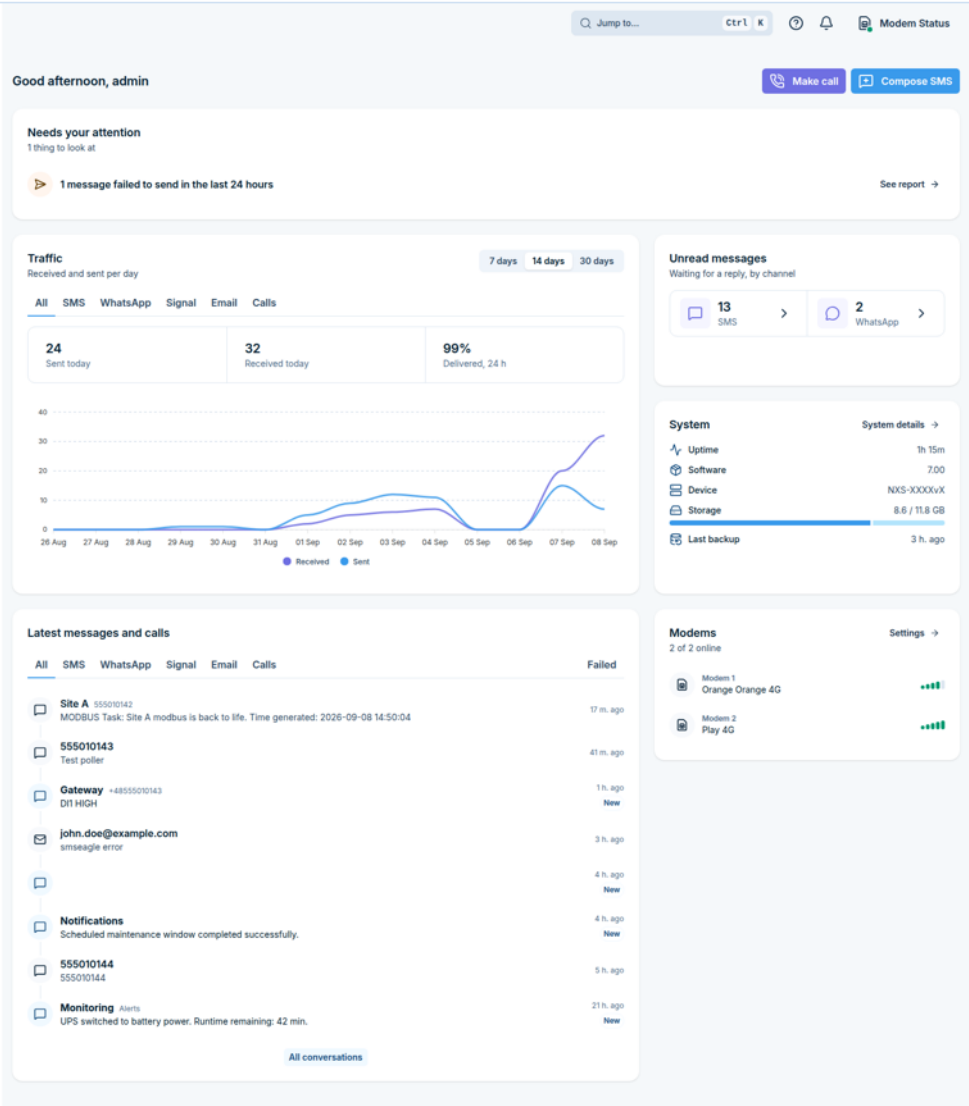


Linke Navigation über dem Hauptinhaltsbereich erweitert, mit der Top-Leiste darüber

- **Left navigation** – eine Symbolleiste für den Zugriff auf Messages, Phonebook, Automation, Reports, Monitoring, Settings und System. Wenn Sie ein Symbol überfahren, wird der Bereich benannt; ein Klick erweitert ein Panel mit den Seiten dieses Bereichs nach Namen, wie oben **Messages**. Die Schaltfläche in der Panel-Kopfzeile schließt es erneut.
- **Top bar** – die **Jump to…** Suchfunktion (`Ctrl K`) ermöglicht einen direkten Sprung zu jeder Seite nach Namen statt Navigation durch das Menü; sie zeigt auch Benachrichtigungen, Hilfe und den Modem-Statusindikator an.
- **Main content area** – die Seite für den derzeit ausgewählten Bereich.

Dashboard

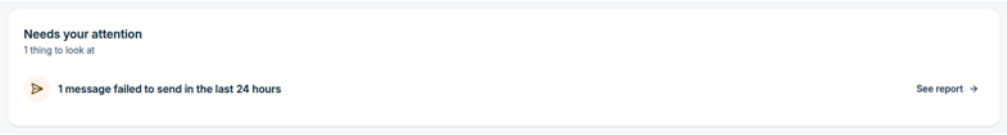
Das Dashboard ist die Landingpage nach der Anmeldung. Es öffnet mit einer Begrüßung und den Schnellaktionsschaltflächen, gefolgt von Karten, die zusammenfassen, was beachtet werden muss, Nachrichtenverkehr, unbeantwortete Konversationen, Gerätezustand, aktuelle Aktivitäten und Modem-Status.



Das Dashboard

Needs your attention

Fasst die aktuell zu bearbeitenden Elemente zusammen, mit der Anzahl darunter im Kartentitel und wie viele davon kritisch sind. Jeder Eintrag verlinkt auf die Seite, wo Sie ihn bearbeiten können, sodass eine im Ausgang stecken gebliebene Nachricht auf den Ausgangsordner verlinkt und ein fehlgeschlagener Zustellungseintrag auf Reports & Statistics.



Needs your attention

Traffic

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

days / **30 days** legen den Bereich des untenstehenden Diagramms fest. Drei Zähler befinden sich über dem Diagramm:

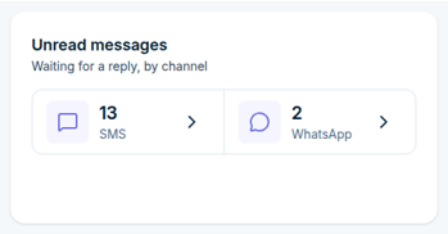
- **Sent today** – Nachrichten seit Mitternacht versendet
- **Received today** – Nachrichten seit Mitternacht empfangen
- **Delivered, 24 h** – Anteil der in den letzten 24 Stunden gesendeten Nachrichten, die als zugestellt bestätigt wurden



Traffic

Unread messages

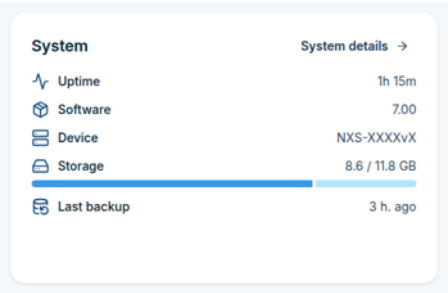
Konversationen, die noch auf eine Antwort warten, gezählt pro Kanal. Jede Kachel öffnet die Konversationsliste dieses Kanals, siehe Messages.



Unread messages

System

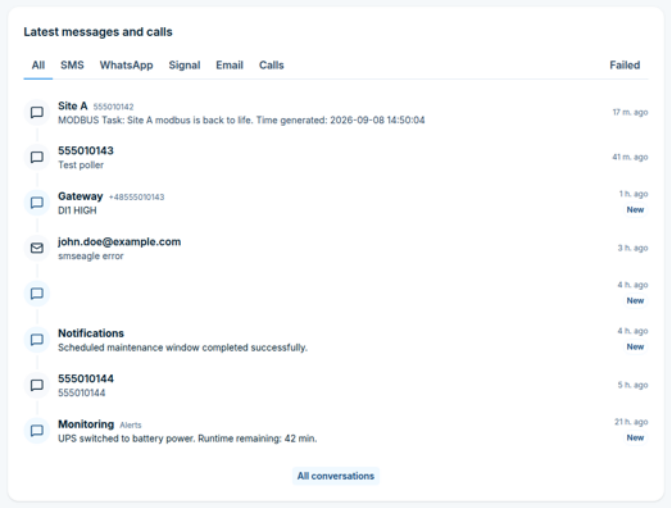
Systemzustand auf einen Blick: Betriebszeit, Softwareversion, Gerätetyp, verwendeter Speicher von insgesamt verfügbarem Speicher und wann die letzte Sicherung durchgeführt wurde. **Systemdetails** öffnet den Bereich System.



System

Neueste Nachrichten und Anrufe

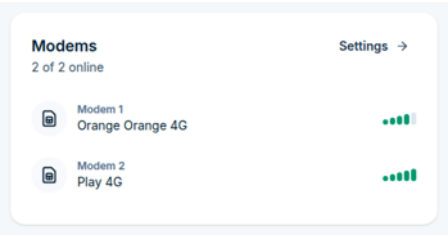
Der neueste Datenverkehr über alle Kanäle, neueste zuerst, mit dem Absender, dem Anfang der Nachricht und wann sie angekommen ist. Die Registerkarten beschränken die Liste auf einen Kanal, und **Fehlgeschlagen** zeigt an, was nicht versendet wurde. Alles, das noch ungelesen ist, wird als **Neu** markiert. **Alle Gespräche** öffnet die vollständige Liste unter Nachrichten.



Neueste Nachrichten und Anrufe

Modems

Wie viele Modems online sind von den installierten, und für jedes die Netzwerkzugehörigkeit, die Funktechnologie und die Signalstärke. **Einstellungen** öffnet die Modem-Konfiguration, siehe Einstellungen.



Modems

Schnellaktionen

Zwei Schaltflächen in der oberen rechten Ecke des Dashboards.



Schnellaktionen

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

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

dem Telefonbuch, manuell eingegeben oder aus einer CSV-Datei), wann versendet werden soll, und die Nachricht selbst. Eine gespeicherte Vorlage kann anstelle des Tippens verwendet werden, siehe Nachrichten.

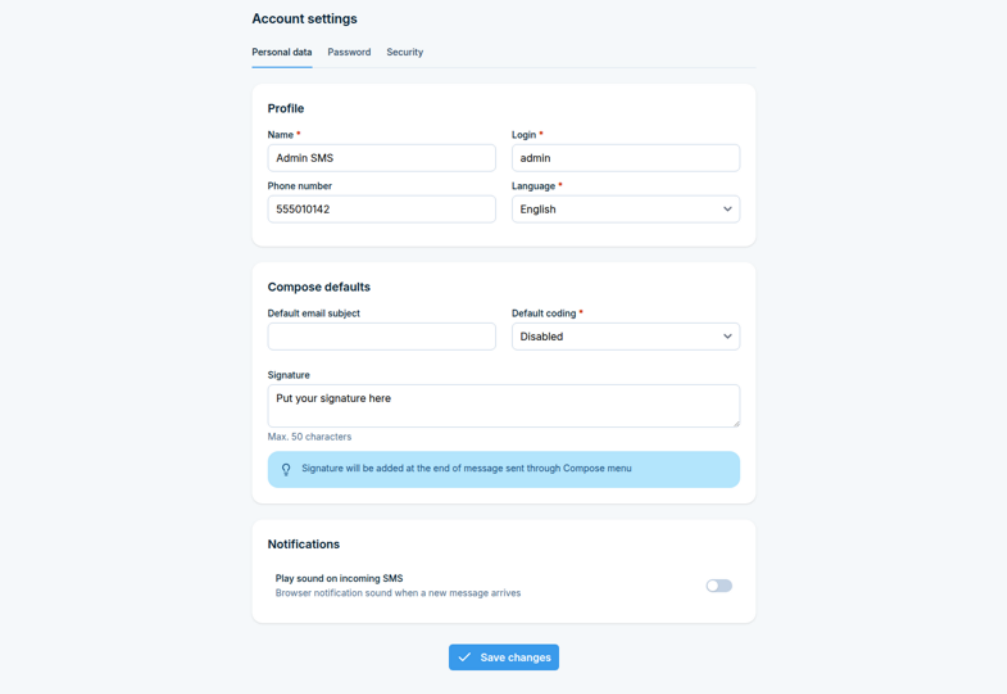
- **Anruf tätigen** öffnet ihn auf der Registerkarte **Anruf** – wählen Sie den Anruftyp aus (nur klingeln, Sprachausgabe, eine Audiodatei), die Empfänger und wann der Anruf getätigt werden soll, siehe Nachrichten.

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

Persönliche Kontoeinstellungen

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

Persönliche Daten

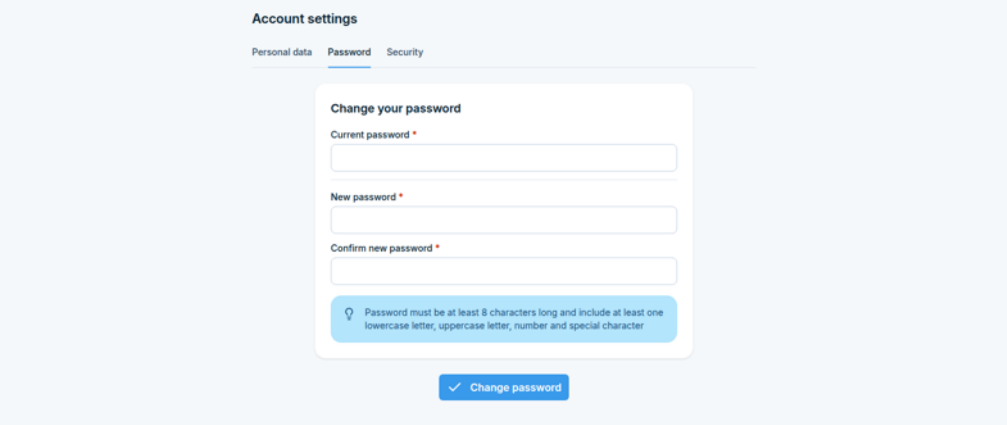


Kontoeinstellungen > Persönliche Daten

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

Änderungen speichern wendet die ganze Registerkarte auf einmal an.

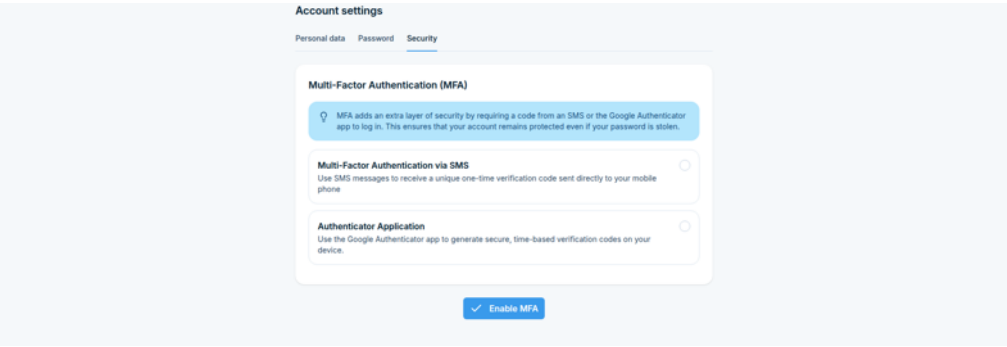
Passwort



Kontoeinstellungen > Passwort

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

Sicherheit



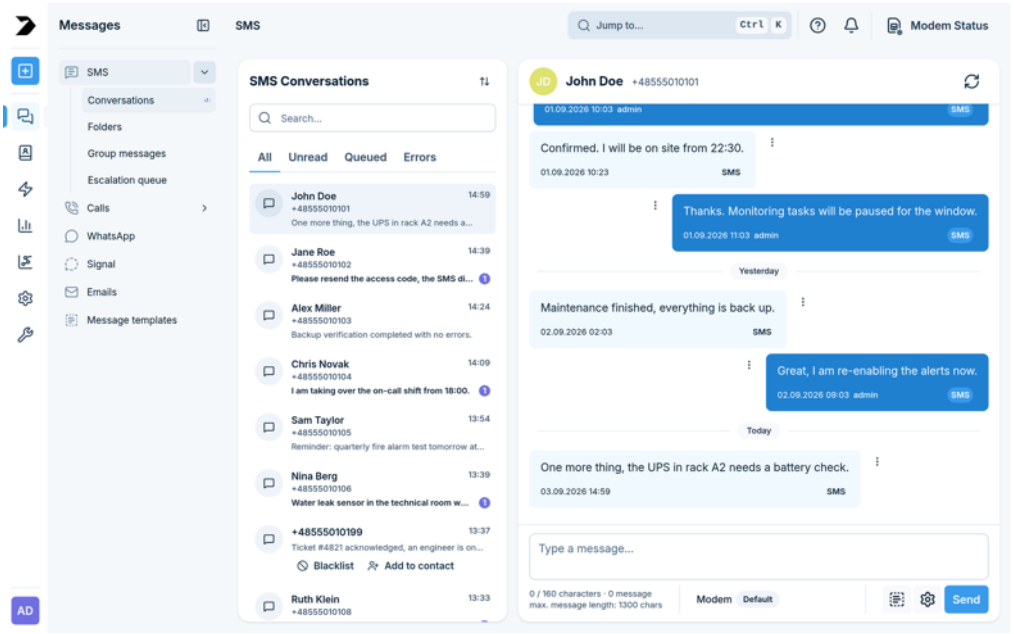
Account settings > Security

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

Nachrichten

Dieses Kapitel behandelt den Bereich **Nachrichten** der Weboberfläche – wo Sie Konversationen auf jedem Kanal lesen, verfassen und verwalten. Die Konfiguration eines Kanals (Aktivierung von WhatsApp, Verbindung von SMTP, Einrichtung von Modems) wird separat unter Einstellungen behandelt; dieses Kapitel ist zur täglichen Nutzung eines Kanals.

SMS (Konversationen)

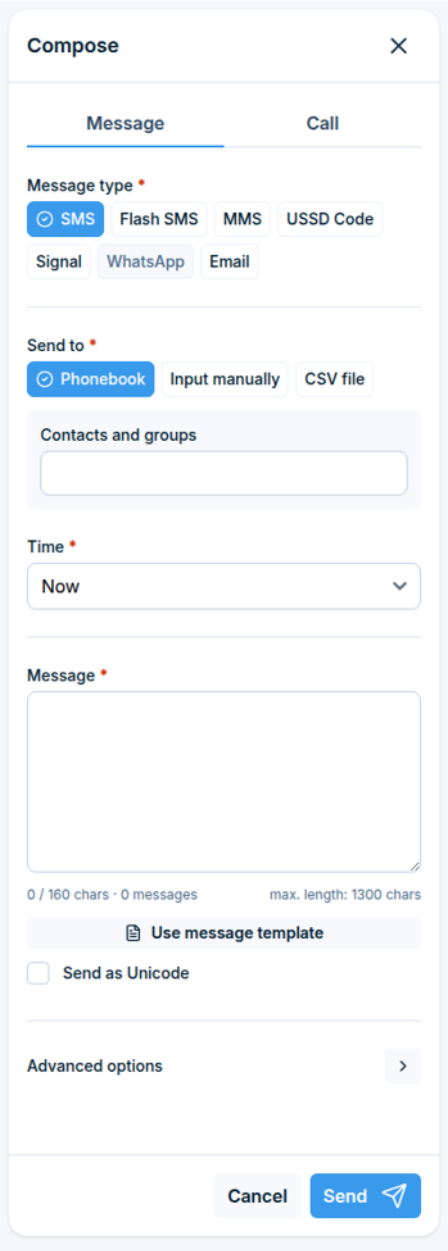


SMS-Konversationen mit offentem Thread

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

- Filtern Sie mit den Tabs **All**, **Unread**, **Queued** und **Errors**.
- Öffnen Sie einen Thread, um die vollständige Chronik zu lesen und von dem Feld am unteren Ende aus zu antworten.
- MMS-Anhänge (Bilder, Dateien) werden im Thread inline angezeigt, sobald ein Modem für MMS konfiguriert wurde – siehe MMS in Einstellungen.
- Verfassen Sie eine neue Nachricht mit der Schaltfläche **+** oben in der linken Leiste oder der Schnellaktion **Compose** im Dashboard.

Nachricht verfassen



Das Verfassen-Dialog

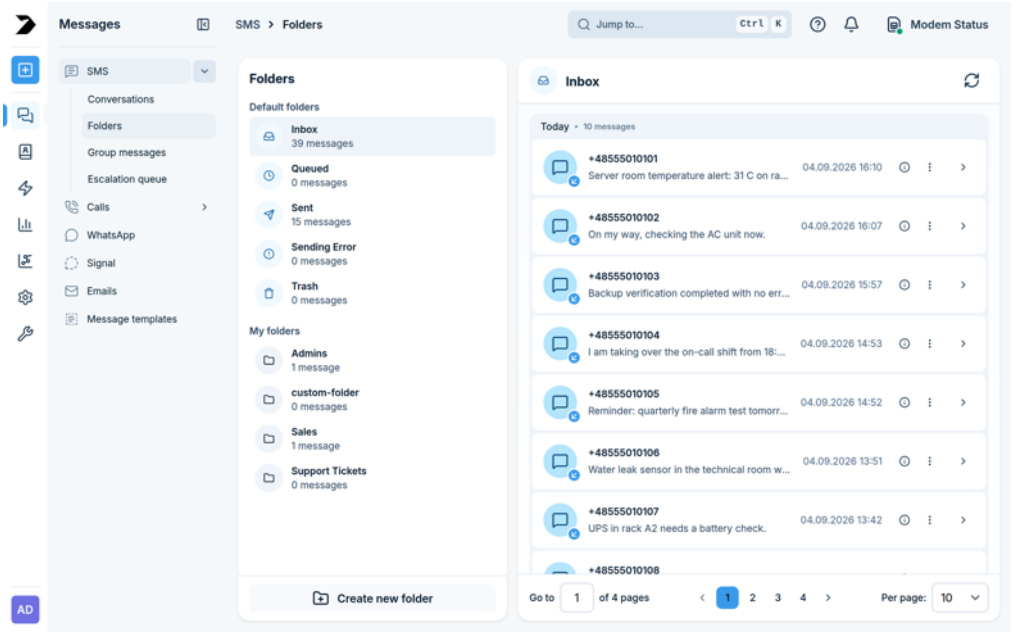
Compose öffnet sich als Panel auf der rechten Seite mit einer Registerkarte **Message** und einer Registerkarte **Call**. Die Registerkarte Nachricht enthält:

- **Message type** – SMS, Flash SMS, MMS, USSD Code, Signal, WhatsApp oder Email. Ein auf diesem Gerät nicht konfigurierter Kanal ist ausgegraut, siehe Einstellungen.
- **Send to** – Wählen Sie Empfänger aus dem **Phonebook** (Kontakte und Gruppen), geben Sie sie mit **Input manually** ein oder laden Sie eine **CSV file** hoch.
- **Time** – senden Sie **Now**, **At date and time**, **After delay** oder **Between hours**.
- **Message** – der Text mit einem Live-Zähler der Zeichen und wie viele SMS-Teile sie ergeben. **Use message template** füllt ihn aus einer gespeicherten Vorlage, und **Send as Unicode** wechselt die Kodierung für Nicht-GSM-Zeichen.

- **Advanced options** – weitere Per-Message-Einstellungen.

Send reiht die Nachricht ein; der Thread erscheint sofort in Konversationen.

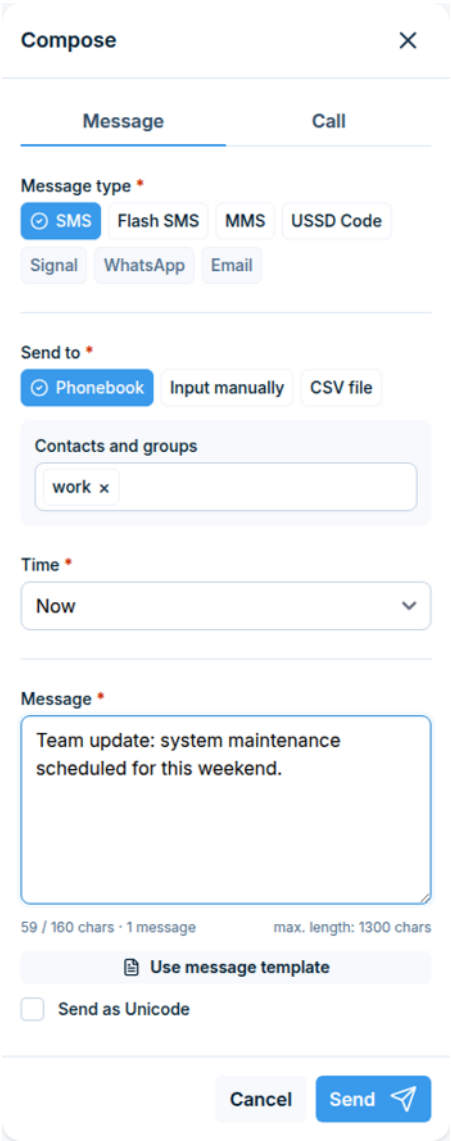
Ordner



Ordner

Nachrichten > SMS > Ordner (`/messages/sms/folders/`) listet die Standardordner (Inbox, Queued, Sent, Sending Error, Trash) zusammen mit allen benutzerdefinierten Ordnern auf, die Sie unter **My folders** erstellt haben. Jeder Ordner zeigt, wie viele Nachrichten er enthält. Klicken Sie auf **Create new folder**, um Ihren eigenen hinzuzufügen – nützlich zusammen mit Inbox Rules, um eingehende Nachrichten automatisch zu sortieren, und Cleanup Folders, um sie automatisch zu bereinigen.

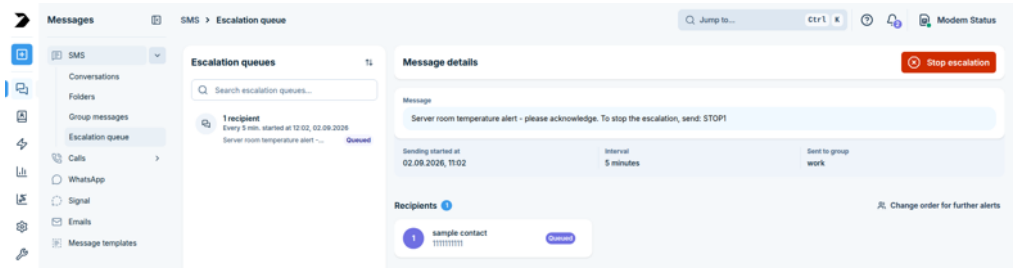
Gruppennachrichten



Verfassen einer Nachricht an eine Phonebook-Gruppe

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

Eskalationswarteschlange



Eskalationswarteschlange

Nachrichten > SMS > Escalation queue (`/messages/sms/escalation/`) zeigt jede derzeit laufende Eskalation – eine an eine Eskalationsgruppe gesendete Nachricht, die noch die Kontaktliste hinunterarbeitet. Das Einrichten einer Eskalationsgruppe selbst wird in Phonebook behandelt; diese Seite zeigt, wo Sie eine bereits laufende Eskalation beobachten und steuern können.

Jede laufende Eskalation wird mit ihrer Nachricht, ihrem Startzeitpunkt und ihrem Intervall aufgelistet. Beim Öffnen wird **Nachrichtendetails** angezeigt: der Nachrichtentext, Startzeitpunkt, Intervall, Zielgruppe und jeder Empfänger mit dem Status **Zugestellt**, **Wird gesendet**, **In Warteschlange** oder **Fehler beim Senden**.

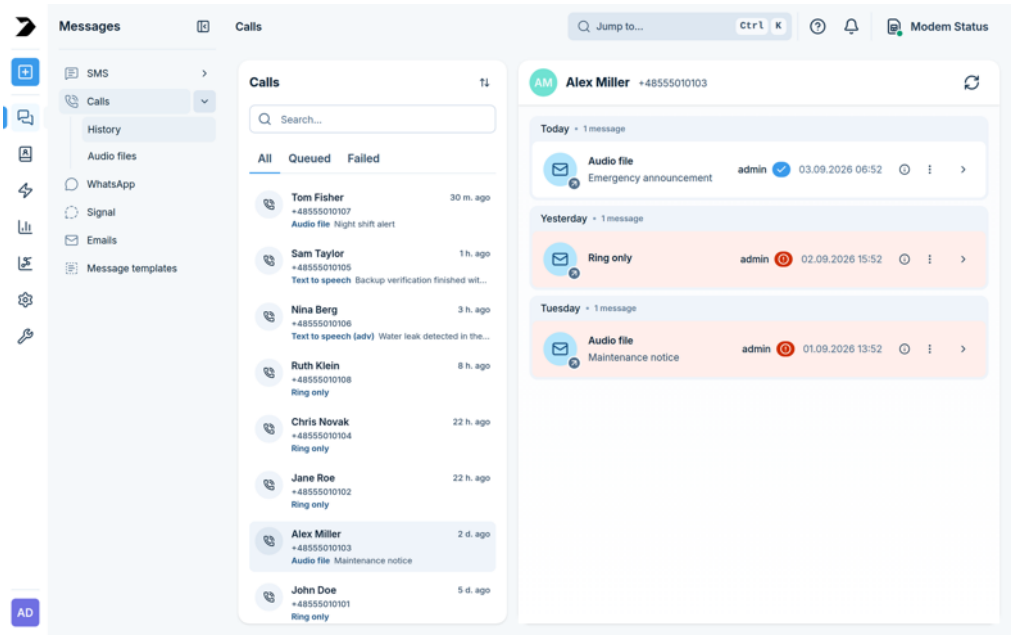
In dieser Ansicht können Sie:

- **Reihenfolge für weitere Warnungen ändern** – Ändern Sie die Reihenfolge der Personen, die noch nicht kontaktiert wurden.
- **Eskalation stoppen** – Brechen Sie die gesamte Eskalation sofort ab; niemand sonst auf der Liste wird kontaktiert.

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

Anrufe

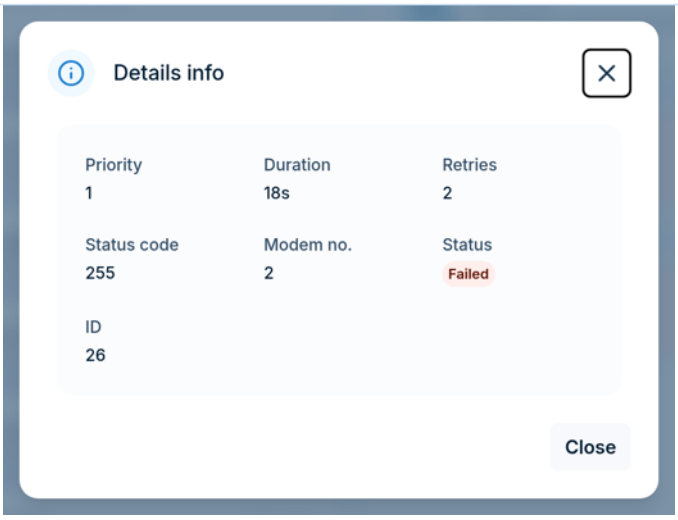
Verlauf



Anrufverlauf

Nachrichten > Anrufe > Verlauf (`/messages/calls/`) listet jeden Anruf auf, den das Gerät getätigt hat, gruppiert nach Telefonnummer, die neuesten zuerst.

- Die Registerkarten **Alle**, **In Warteschlange** und **Fehlgeschlagen** grenzen die Liste ein.
- Das Suchfeld findet Anrufe nach Nummer, Kontaktname oder nach dem vorgelesenen Text.
- Beim Öffnen eines Anrufs werden seine Details angezeigt: Priorität, Dauer, Wiederholungen, Statuscode, Modemnummer und ID. Der Statuscode ist das Referenzmaterial, wenn Sie den Support zu einem fehlgeschlagenen Anruf befragen.
- Löschen Sie einen einzelnen Anruf, oder wählen Sie mehrere aus und löschen Sie sie gemeinsam.

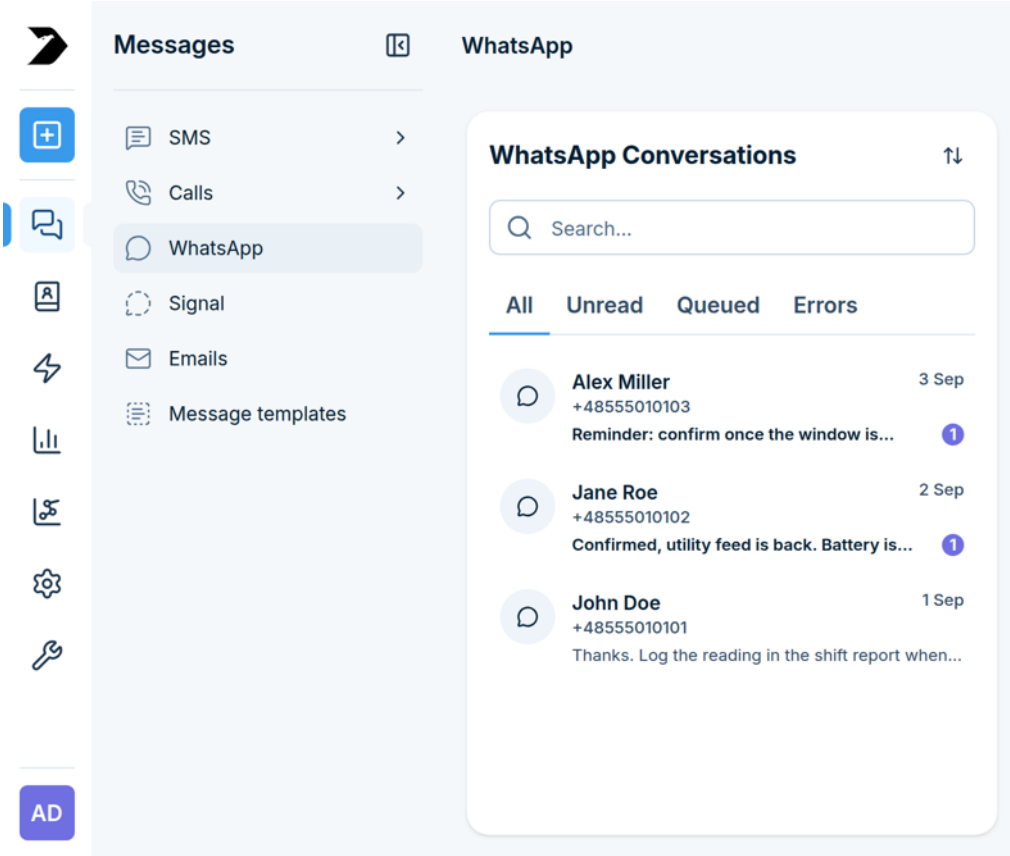


Anrufdetails

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

Anruffeld) wird unter Anrufe in den Einstellungen behandelt.

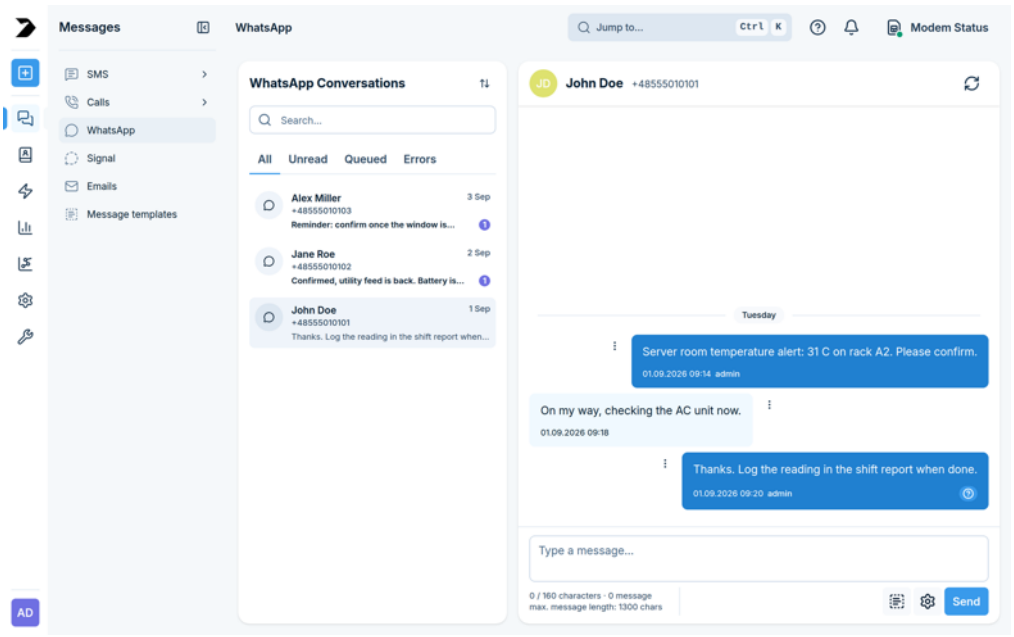
WhatsApp



WhatsApp-Gespräche

Nachrichten > WhatsApp (`/messages/whatsapp/`) listet WhatsApp-Gespräche auf, eines pro Nummer, die neuesten zuerst, sobald der Kanal unter Einstellungen verknüpft wurde.

- Filtern Sie mit den Tabs **All**, **Unread**, **Queued** und **Errors**.
- Suchen und sortieren Sie Gespräche nach Datum oder Telefonnummer.
- Öffnen Sie ein Gespräch und antworten Sie direkt aus dem Feld am unteren Rand (maximal 1300 Zeichen).
- Löschen Sie ein einzelnes Gespräch, oder wählen Sie mehrere aus und löschen Sie sie gemeinsam.

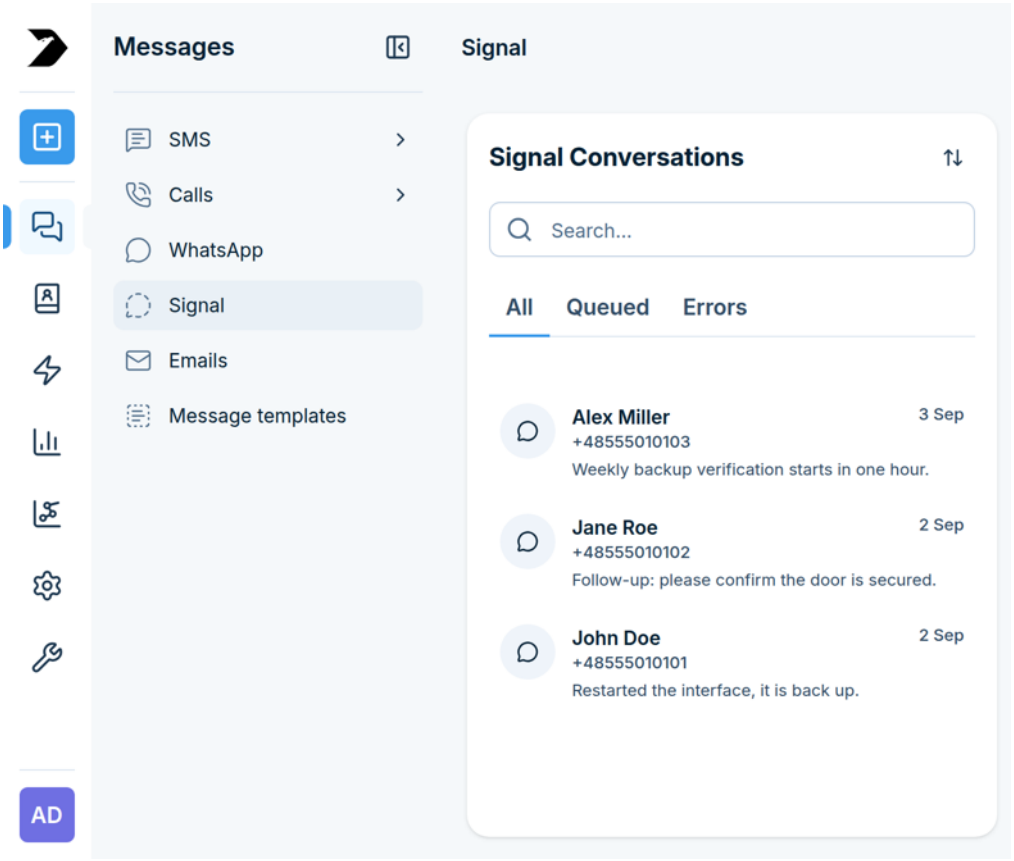


Ein offenes WhatsApp-Gespräch

Wenn WhatsApp noch nicht konfiguriert wurde, zeigt diese Seite einen Hinweis mit einer Schaltfläche, die Sie direkt zu den WhatsApp-Einstellungen führt. Zum Senden einer neuen WhatsApp-Nachricht öffnen Sie **Compose**, aktivieren Sie **WhatsApp** als Nachrichtentyp und schreiben Sie wie gewohnt.

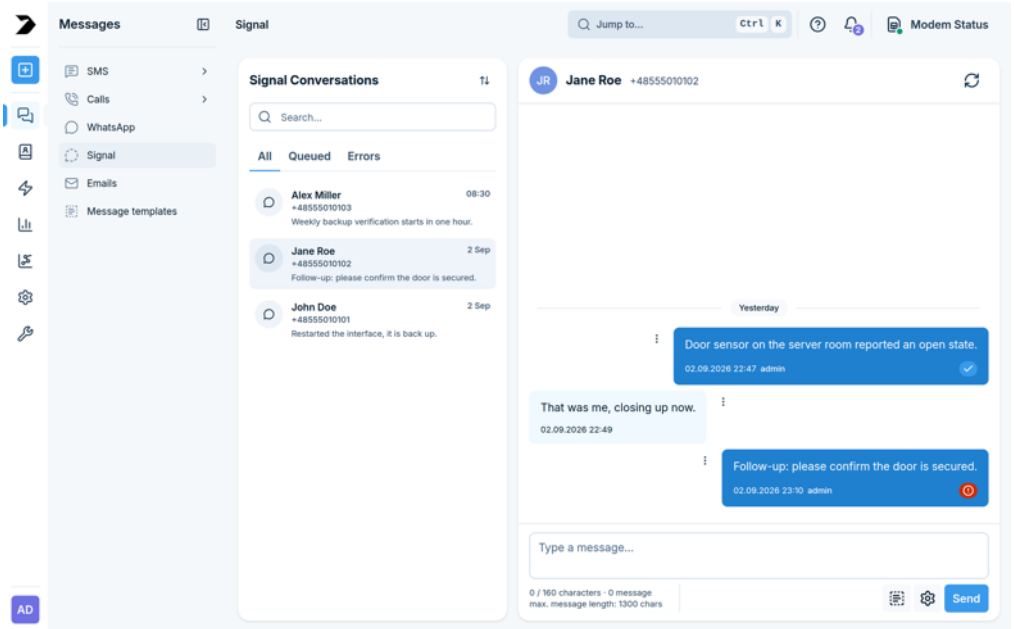
Hier werden nur Nachrichten angezeigt, die nach der Verknüpfung des Geräts empfangen wurden.

Signal



Signal-Unterhaltungen

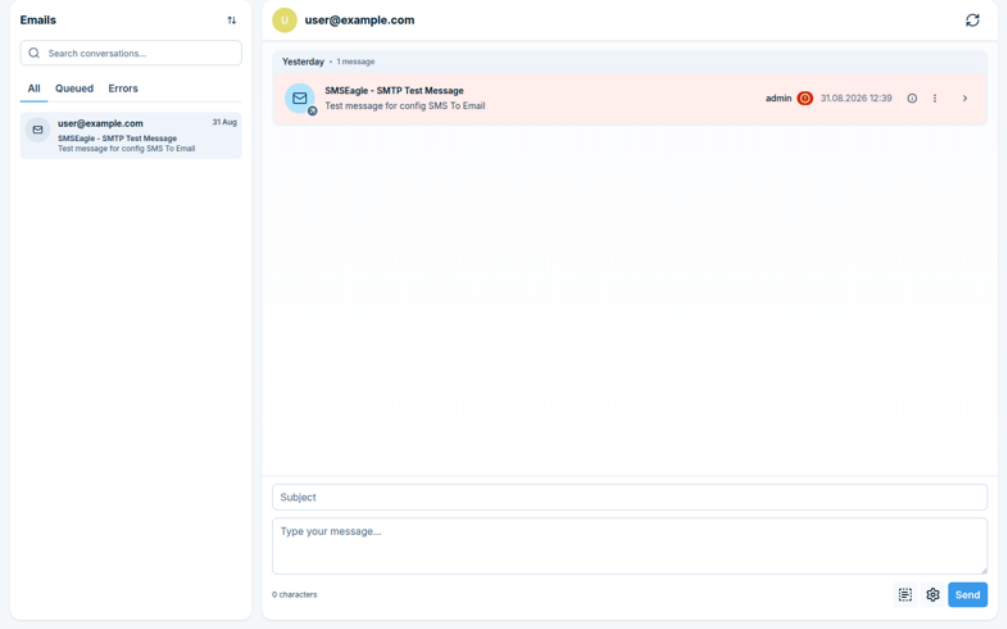
Messages > Signal (`/messages/signal/`) funktioniert genauso wie WhatsApp oben, sobald eine Nummer unter Einstellungen registriert wurde: eine Unterhaltung pro Nummer, die Filter **All / Queued / Errors**, und Antwort aus dem Feld unten (maximal 1300 Zeichen). Signal hat keine Registerkarte **Unread**.



Ein offenes Signal-Gespräch

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

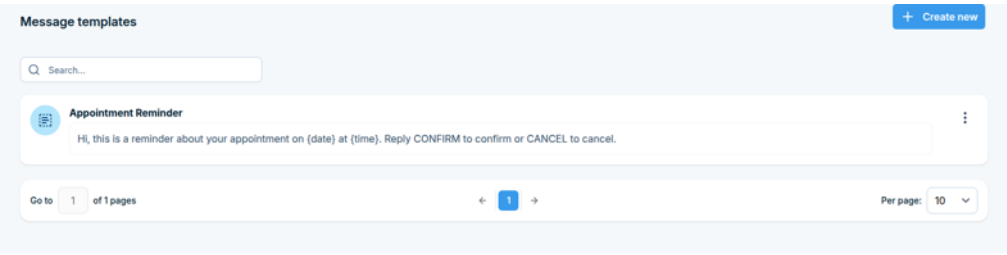
E-Mails



E-Mail-Unterhaltungen

Messages > Emails (`/messages/email/`) listet E-Mail-Unterhaltungen auf, ein Thread pro Adresse, die neuesten zuerst, mit **All**-, **Queued**- und **Errors**-Filtern – die gleiche Gesprächsansicht wie SMS, WhatsApp und Signal, für E-Mails, die über SMS to Email und Email to SMS gesendet oder empfangen wurden.

Nachrichtenvorlagen



Nachrichtenvorlagen

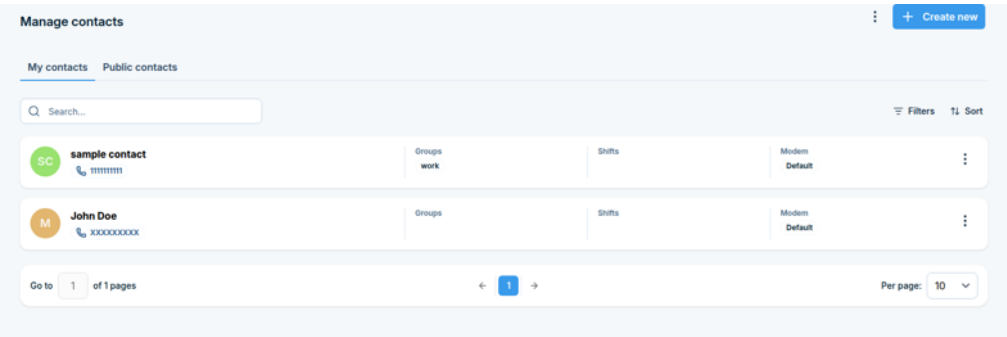
Messages > Message templates (`/messages/templates/`) speichert wiederverwendbaren Nachrichtentext für Compose, damit häufige Nachrichten nicht jedes Mal neu eingegeben werden müssen.

Klicken Sie auf **Create new**, geben Sie der Vorlage einen **Template name** und schreiben Sie den **Message content**. Gespeicherte Vorlagen können dann im Compose-Bereich ausgewählt werden, anstatt die Nachricht von Grund auf neu 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 unterteilt:

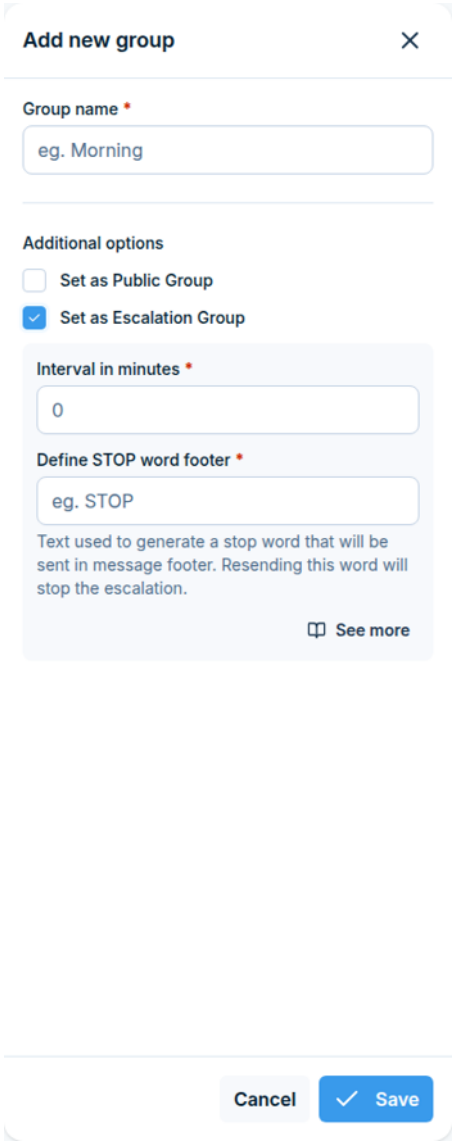
- **My contacts** - Kontakte, die nur Sie sehen und verwenden können.
- **Public contacts** - Kontakte, die mit anderen Benutzern des Geräts geteilt werden (erforderlich, damit beispielsweise ein öffentlicher Kontakt nach Namen von E-Mail-zu-SMS adressiert werden kann).

Jeder Kontakt kann zu einer oder mehreren **Groups** gehören, einen **Shift** zugewiesen bekommen (siehe Shifts unten) und an ein bestimmtes **Modem** für ausgehende Nachrichten gebunden 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 Reihe von Kontakten auf einmal anzusprechen (z. B. von Compose SMS oder als Ziel einer Automatisierungsregel), anstatt jeden Kontakt einzeln auszuwählen. Klicken Sie auf **Add new**, geben Sie der Gruppe einen **Name**, und aktivieren Sie **Set as Public Group**, falls andere Benutzer, Automatisierungsregeln oder die API an die Gruppe senden können sollen.

Eskalationsgruppen



Eskalationsgruppenoptionen im Dialog „Add new group“

Eine Eskalationsgruppe benachrichtigt Menschen **der Reihe nach, nicht alle auf einmal**, bis jemand bestätigt, dass er sich des Problems annimmt – ordnen Sie Ihre Bereitschaftspersonen in einer gewählten Reihenfolge in einer Gruppe, legen Sie ein Intervall fest, und wenn Sie eine Nachricht an die Gruppe senden, erhält die erste Person sie sofort, die zweite erhält sie, wenn niemand die Eskalation stoppt, und so weiter die Liste hinunter. Die Überwachung und Kontrolle einer laufenden Eskalation erfolgt in Escalation queue unter Messages; dieser Abschnitt ist der Ort, an dem Sie diese einrichten.

Schritt 1: Eskalationsgruppe erstellen

1. Klicken Sie auf **Add new**. Ein Seitenpanel wird geöffnet.
2. Füllen Sie **Name** aus, z. B. `Night on-call`.
3. Aktivieren Sie **Escalation group**. Zwei zusätzliche Felder erscheinen.

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

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

Schritt 2: Personen hinzufügen und ihre Reihenfolge festlegen

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

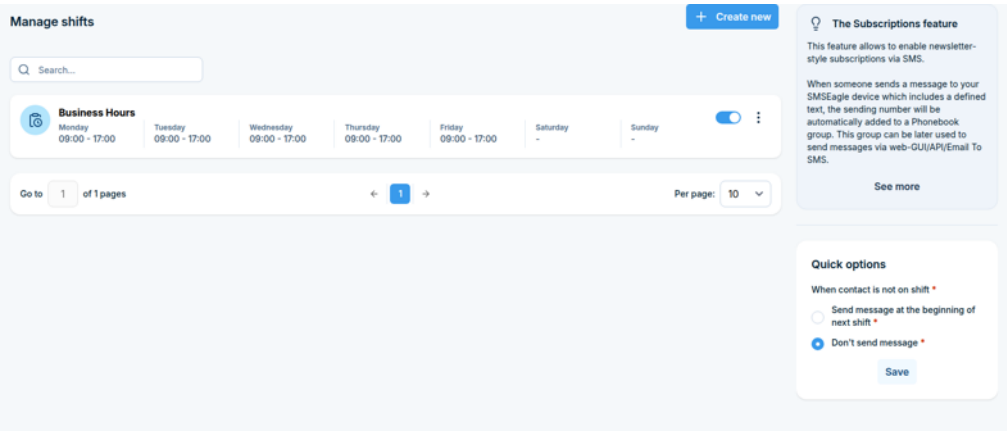
Schritt 3: Eine Eskalation auslösen

Senden Sie eine Nachricht an die Gruppe auf dieselbe 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 dieselbe Nachricht für die nächsten Kontakte mit dem von Ihnen festgelegten Intervall.

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

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

Schichten



Übersicht der Schichtverwaltung

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

Typische Anwendung: eine On-Call-Rota, bei der die Nachtschicht nicht durch Warnungen aufgeweckt 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 Adressbuch (**Phonebook > Contacts**).
- Stellen Sie sicher, dass die Geräteuhr und die Zeitzone korrekt sind, da Schichtzeiten mit der Gerätezeit verglichen werden. Überprüfen Sie dies in **Settings > Date/Time**.

Schritt 1: Öffnen Sie die Seite Schichten

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

Schritt 2: Erstellen Sie eine Schicht

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

5. Klicken Sie auf **Save**.

Regeln für Schichtzeiten

- **From** muss früher als **To** am selben Tag sein.
- Beide **From** und **To** müssen ausgefüllt sein, oder beide müssen leer gelassen werden. Ein halb ausgefüllter Tag wird mit einer Fehlermeldung abgelehnt.
- Mindestens ein Tag muss Uhrzeiten haben.

> **Schichten über Mitternacht:** Eine Schicht, die Mitternacht überschreitet (zum Beispiel 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 aus tun.

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

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

Schritt 4: Wählen Sie, was außerhalb der Schichtzeiten passiert

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

Option	Ergebnis
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 an diesen Kontakt nicht gesendet. Sie wird als nicht zugestellt aufgezeichnet.

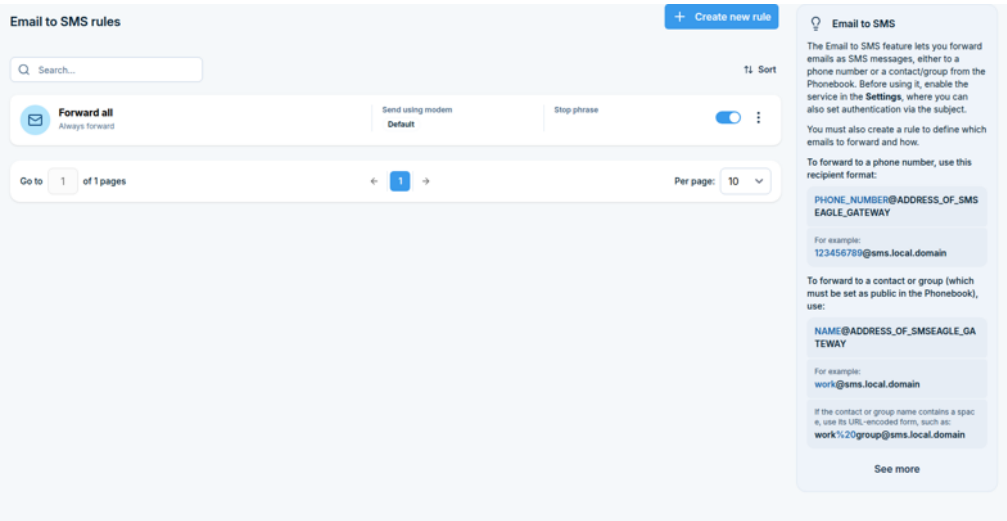
Wählen Sie die gewünschte Option aus und klicken Sie auf **Save**.

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

Automatisierung

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

E-Mail zu SMS



Email-zu-SMS-Regeln

Die Funktion E-Mail zu SMS ermöglicht es Ihnen, eingehende E-Mails als SMS-Nachrichten weiterzuleiten, entweder an eine Telefonnummer oder an einen Kontakt/eine Gruppe aus Ihrem Telefonbuch.

Wo finde ich es

Die Funktion ist an zwei Stellen in der WebGUI verteilt:

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

Schritt 1: Das Empfängeradressenformat verstehen

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

Um an eine Telefonnummer weiterzuleiten:

```
PHONE_NUMBER@ADDRESS_OF_SMSEAGLE_GATEWAY
```

Beispiel: `999888777@gateway.smseagle.eu`

Um an einen Kontakt oder eine Gruppe aus dem Telefonbuch weiterzuleiten (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 seine URL-codierte Form: `work%20group@gateway.smseagle.eu`

Anstelle der Gateway-IP-Adresse können Sie einen vollqualifizierten Domänennamen verwenden, der unter **Einstellungen > Kanäle > E-Mail > E-Mail zu SMS > Erweiterte Einstellungen > FQDN-Hostname** eingestellt ist. Wenn dort **LDAP-Kontakte verwenden** aktiviert ist, wird das gleiche `NAME@GATEWAY`-Format auch in LDAP / Active Directory definierte Kontakte und Gruppen aufgelöst.

Standardmäßig wird der Text der E-Mail zum Text der SMS. Dies hängt von der Einstellung **Was ist mit dem E-Mail-Betreff zu tun** unter Einstellungen ab: Der Betreff kann ignoriert, der Nachricht vorangestellt, für die Authentifizierung verwendet oder statt des Textes gesendet werden.

Schritt 2: Eine neue Regel erstellen

Gehen Sie zu **Automatisierung > E-Mail > E-Mail zu SMS** und klicken Sie auf **Neue Regel erstellen**. Ein Fenster mit dem Titel E-Mail-zu-SMS-Regel hinzufügen öffnet sich rechts.

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 Adressenformat entspricht. Angegebener Absender / Nachricht enthält fügt Filterbedingungen hinzu, siehe Schritt 3.
Senden mit Modem	Welches Modem die SMS sendet. Standard ist Standard. Wird nur auf Geräten mit mehr als einem Modem angezeigt.
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 SMS-Versand	Nein, Nur Klingeln, Ja - Text-zu-Sprache oder Ja - Text-zu-Sprache (erweitert). Die verfügbaren Optionen hängen von der Stimme und den TTS-Funktionen Ihres Geräts ab.
Sprachmodell	Stimme für den Text-zu-Sprache-Anruf. Wird nur für Geräte mit erweiterter TTS angezeigt und nur nach Auswahl von Ja - Text-zu-Sprache (erweitert).
Erzwinge Konvertierung in UTF-8	Erzwingt die Konvertierung des Nachrichtentexts in UTF-8
Konversationsverlauf entfernen	Entfernt den zitierten Verlauf der E-Mail-Konversation aus dem Nachrichtentext

Klicken Sie **Speichern**, um die Regel zu erstellen, oder **Abbrechen**, um sie zu verwerfen.

Schritt 3: Filterungsbedingungen hinzufügen (optional)

Wenn Sie unter Weiterleiten für die Option **Angegebener Absender / Nachricht enthält** wählen, stehen drei unabhängige Bedingungen zur Verfügung, jeweils mit eigenem Kontrollkästchen und Textfeld:

- **Wenn eingehende E-Mail-Adresse enthält** filtert nach der E-Mail-Adresse des Absenders
- **Wenn eingehende Nachrichtenbetreffzeile enthält** filtert nach der E-Mail-Betreffzeile
- **Wenn eingehender Nachrichteninhalt enthält** filtert nach dem E-Mail-Text

Der Schalter **Groß-/Kleinschreibung beachten** 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 wird als Karte in der Liste „E-Mail zu SMS“ angezeigt und zeigt:

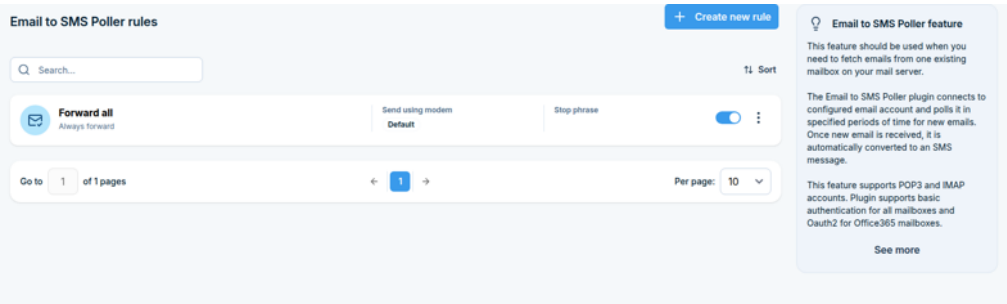
- den Regelnamen
- die Weiterleitungsbedingung, z. B. Weiterleiten wenn eingehend: E-Mail-Adresse enthält: … oder Immer weiterleiten, wenn keine Bedingung festgelegt ist
- das zum Versand verwendete Modem
- die konfigurierte Stoppphrase
- einen Ein-/Aus-Schalter zum Aktivieren oder Deaktivieren der Regel, ohne sie zu löschen
- ein ⋮-Menü mit **Bearbeiten** und **Löschen**

Zusätzliche Steuerelemente in der Liste:

- **Suche** filtert Regeln nach Name.
- Durch Auswahl von Regelkontrollkästchen werden Massenaktionen angezeigt: **Aktivieren / Deaktivieren** und **Löschen**.
- Mit den Paginierungssteuerelementen am unteren Rand können Sie zu einer Seite springen und ändern, wie viele Regeln pro Seite angezeigt werden.

Das Hilfefenster auf der rechten Seite erklärt die Formate für Empfängeradressen und enthält eine Schaltfläche **See more** (Mehr anzeigen), die zur Funktionsseite auf smseagle.eu führt.

Email to SMS Poller



Email-zu-SMS-Poller-Regeln

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

Wo finde ich es

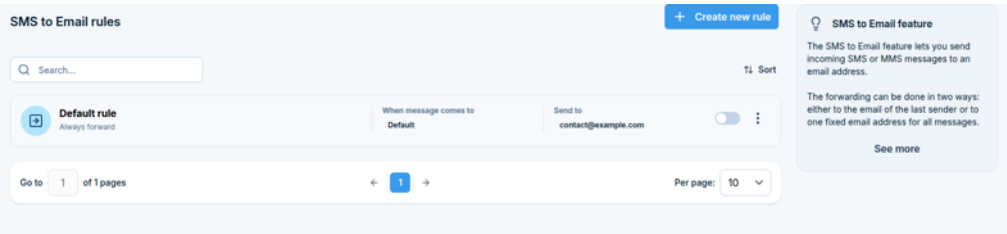
Automation > Email > Email to SMS Poller (`/automation/email-to-sms-poller/`) ist der Ort, an dem Sie Regeln erstellen und verwalten. Das Aktivieren des Dienstes und das Verbinden des Postfachs

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

Erstellen einer Regel

Klicken Sie auf **Create new rule** (Neue Regel erstellen). Regeln funktionieren hier genauso wie Email to SMS-Regeln – benennen Sie die Regel, wählen Sie, ob alle abgerufenen E-Mails weitergeleitet werden 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 Versenden).

SMS to Email



SMS to Email-Regeln

Was diese Funktion macht

SMS to Email leitet **eingehende** SMS- und MMS-Nachrichten an eine E-Mail-Adresse weiter, damit Sie sie in Ihrem Postfach lesen können, anstatt sich bei 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 eine bestimmte Phrase enthalten.

Typische Anwendungen: Weiterleitung von Antworten von Außendienstmitarbeitern an ein gemeinsames Support-Postfach oder Archivierung von Benachrichtigungsbestätigungen in den E-Mail-Posteingang eines Ticketing-Systems.

Bevor Sie beginnen

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

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

Schritt 1: Öffnen Sie die SMS to Email-Seite

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

Schritt 2: Erstellen Sie eine Regel

Klicken Sie in der oberen rechten Ecke auf **Create new rule** (Neue Regel erstellen). Ein Seitenfenster öffnet sich.

Benennen Sie die Regel

Geben Sie in **Rule name** (Regelname) etwas Beschreibendes ein, zum Beispiel `Forward all to support`. Maximale Länge: 100 Zeichen.

Entscheiden Sie, welche Nachrichten weitergeleitet werden sollen

Wählen Sie **Forward for** (Weiterleiten für):

Option	Was das bedeutet
Always forward (Immer weiterleiten)	Jede eingehende SMS und MMS wird weitergeleitet.
Angegebener Absender / Nachricht	Nur Nachrichten, die den nachfolgend festgelegten Bedingungen entsprechen, werden weitergeleitet.

Wenn Sie **Angegebener Absender / Nachricht** wählen, werden zwei Bedingungen verfügbar. Sie können eine oder beide verwenden. Wenn Sie beide verwenden, muss eine Nachricht **beiden** Bedingungen entsprechen, 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 den Namen ein, um zu suchen. Nur **öffentliche** Kontakte und Gruppen können hier ausgewählt werden.

Wenn eingehende SMS-Text enthält Aktivieren Sie dies und geben Sie den zu suchenden Ausdruck ein, z. B. `URGENT`. Der Ausdruck kann überall im Nachrichtentext vorkommen. Aktivieren Sie **Groß-/Kleinschreibung beachten**, wenn `urgent` und `URGENT` unterschiedlich behandelt werden sollen.

Regel auf ein Modem beschränken (nur Multi-Modem-Geräte)

Wenn Ihr Gerät mehr als ein Modem hat, wird ein Feld **Wenn Nachricht empfangen auf** angezeigt. Lassen Sie es auf **Beliebiges Modem**, oder wählen Sie ein bestimmtes Modem, damit die Regel nur auf Nachrichten zutrifft, die auf dieser SIM-Karte ankommen. Bei Geräten mit einem Modem wird dieses Feld nicht angezeigt.

Wählen Sie die Ziel-E-Mail-Adresse

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

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

Legen Sie den E-Mail-Betreff fest

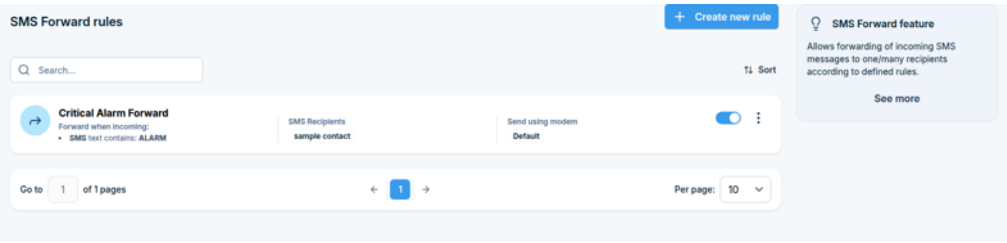
E-Mail-Betreff steuert die Betreffzeile der weitergeleiteten E-Mail. Sie können Platzhalter verwenden, die beim Versand der E-Mail durch echte Werte ersetzt werden:

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

Klicken Sie auf **Save**. Die Regel beginnt sofort mit neu eingegangenen Nachrichten zu funktionieren.

SMS Forward



Dialog zum Hinzufügen einer Weiterleitungsregel

Was diese Funktion macht

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 weiterleiten, wie sie eingegangen 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: Versenden von Alarmmeldungen von einer Maschine an das gesamte On-Call-Team, Weiterleitung von Nachrichten von einer gemeinsamen Nummer an die Person, die gerade Dienst hat, oder Umwandlung eines kurzen Maschinencodes in einen verständlichen Satz für das Team.

Bevor Sie beginnen

- Die Kontakte und Gruppen, an die Sie **weiterleiten**, müssen im Phonebook vorhanden sein. Kontakte und Gruppen, die als Weiterleitungsempfänger oder als Senderbedingungen verwendet werden, müssen als **Public** markiert sein.
- Entscheiden Sie, ob die Empfänger den ursprünglichen Wortlaut oder eine umformulierte Nachricht benötigen.

Schritt 1: Öffnen Sie die SMS Forward-Seite

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

Schritt 2: Erstellen Sie eine Regel

Klicken Sie in der oberen rechten Ecke auf **Create new rule** (Neue Regel erstellen). Ein Seitenfenster öffnet sich.

Benennen Sie die Regel und legen Sie ihre Priorität fest

Rule name Eine aussagekräftige Beschreibung, zum Beispiel `Alarms to on-call team`. Maximum 100 Zeichen.

Priority Eine Zahl von 0 bis 9. Nachrichten, die von einer Regel mit höherer Priorität erzeugt werden, werden früher zum Versenden eingeplant als Nachrichten von einer Regel mit niedrigerer Priorität. Belassen Sie es bei der Standardeinstellung, es sei denn, Sie haben dringende Regeln, die Massen-Meldungen überlagern müssen.

Entscheiden Sie, welche Nachrichten weitergeleitet werden sollen

Wählen Sie **Forward for** (Weiterleiten für):

Option	Was das bedeutet
All incoming messages	Jede eingehende SMS wird weitergeleitet.
Angegebener Absender / Nachricht	Nur Nachrichten, die den nachfolgend festgelegten Bedingungen entsprechen, werden weitergeleitet.

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

When incoming SMS comes from Aktivieren Sie dies 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 dies und geben Sie den Satz unter **Text fragment** ein, zum Beispiel `ALARM`. Der Satz kann an einer beliebigen Stelle in der Nachricht vorkommen. Aktivieren Sie **Case sensitive**, wenn `alarm` und `ALARM` als unterschiedlich behandelt werden sollen.

Regel auf ein Modem beschränken (nur Multi-Modem-Geräte)

Wenn Ihr Gerät mehr als ein Modem hat, erscheint ein Feld **When messages comes to**. Belassen Sie es bei der Standardeinstellung, oder wählen Sie ein bestimmtes Modem, sodass die Regel nur für Nachrichten gilt, die auf dieser SIM-Karte ankommen. Bei Geräten mit einem Modem wird dieses Feld nicht angezeigt.

Wählen Sie, was die weitergeleitete Nachricht aussagt

Verwenden Sie **Message content**:

Option A: Original message

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

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

Option B: Custom text

Die Empfänger erhalten stattdessen Ihren eigenen Text. Geben Sie ihn unter **Custom message** ein (Maximum 500 Zeichen). Sie können Teile der ursprünglichen Nachricht mit Platzhaltern einfügen:

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

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

Wählen Sie die Empfänger

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

Optional einen Telefonanruf hinzufügen

Anruf nach SMS-Versand lässt das Gerät auch einen Sprachanruf an die gleichen Empfänger tätigen. Die verfügbaren Optionen hängen von Ihrem Gerätemodell ab:

Option	Was geschieht
Nein	Es wird kein Anruf getätigt. Dies ist die Standardeinstellung.
Nur Klingeln	Das Gerät ruft den Empfänger an und legt auf. Es wird keine Sprachnachricht abgespielt.
Ja – Text-zu-Sprache	Das Gerät ruft an und liest den Nachrichtentext vor.
Ja – Text-zu-Sprache (erweitert)	Wie oben, aber mit einer wählbaren, natürlicheren Stimme. Wählen Sie die Stimme im Feld **Voice model** aus, das angezeigt wird.

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

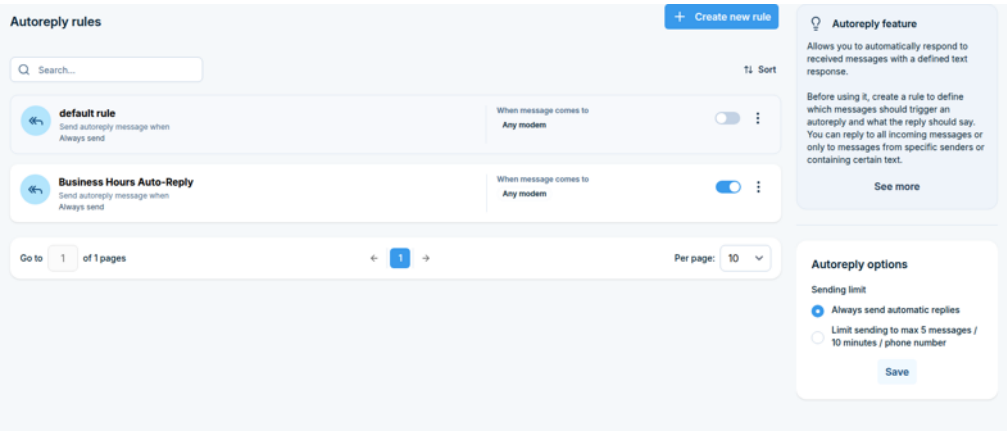
Klicken Sie auf **Save**. Die Regel beginnt sofort mit neu eingegangenen Nachrichten zu funktionieren.

Funktionsweise der Weiterleitng

- Die Textbedingung ist eine **contains**-Abfrage (Enthält), 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 Erstellung und Aktivierung der Regel ankommen. Sie verarbeiten nicht bereits im Posteingang vorhandene Nachrichten.
- Empfänger können aus anderen Gründen übersprungen werden: **Urlaubsmodus** für den Kontakt, ein Schichtplan, der gerade außerhalb seiner Arbeitszeiten liegt (siehe Shifts), oder die Nummer steht auf der Blacklist.

  Vermeiden Sie Weiterleitungsschleifen. Leiten Sie Nachrichten nicht an eine Nummer weiter, die selbst an Ihr Gerät zurückleitet. Zwei Geräte, die aufeinander zeigen, senden sich gegenseitig ständig Nachrichten zu.

Automatische Antworten



Regeln für automatische Antworten und Versandlimit-Optionen

Was diese Funktion macht

Automatische Antworten senden eine **automatische Textantwort auf eingehende SMS-Nachrichten**.

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

Typische Anwendungen: Bestätigung des Eingangs einer Bestellanfrage, Benachrichtigung, dass die Nummer nachts unbesetzt ist, oder Antwort auf ein Schlüsselwort mit festen Informationen wie Öffnungszeiten.

Bevor Sie beginnen

- Das Gerät muss SMS versenden können. Überprüfen Sie, dass mindestens ein Modem angeschlossen und im Netz registriert ist.
- Wenn Sie nur auf spezifische 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 für alle Regeln gilt und unter Schritt 3 beschrieben wird.

Schritt 2: Erstellen Sie eine Regel

Klicken Sie in der oberen rechten Ecke auf **Create new rule** (Neue Regel erstellen). Ein Seitenfenster öffnet sich.

Benennen Sie die Regel

Geben Sie im Feld **Rule name** einen aussagekräftigen Namen ein, zum Beispiel `Out of hours reply`. Maximal 100 Zeichen.

Entscheiden Sie, welche Nachrichten beantwortet werden sollen

Wählen Sie **Automatische Antwort senden für**:

Option	Was das bedeutet
All incoming messages	Jede eingehende SMS erhält eine Antwort.
Angegebener Absender / Nachricht	Nur Nachrichten, die die unten festgelegten Bedingungen erfüllen, erhalten eine Antwort.

Wenn Sie **Bestimmter Absender / Nachricht** gewählt haben, stehen zwei Bedingungen zur Verfügung. Sie können eine oder beide verwenden. Wenn Sie beide verwenden, muss eine Nachricht **beide** Bedingungen erfüllen, um eine Antwort zu erhalten.

Wenn eingehende SMS kommt von Aktivieren Sie dies und wählen Sie die Kontakte oder Gruppen aus, die eine Antwort erhalten sollen. Beginnen Sie zu tippen, um zu suchen. Nur **öffentliche** Kontakte und Gruppen können hier ausgewählt werden.

Wenn eingehender SMS-Text enthält Aktivieren Sie dies und geben Sie den zu suchenden Ausdruck ein, z. B. `PRICE`. Der Ausdruck kann überall im Nachrichtentext vorkommen. Aktivieren Sie **Groß-/Kleinschreibung beachten**, wenn `price` und `PRICE` unterschiedlich behandelt werden sollen.

Regel auf ein Modem beschränken (nur Multi-Modem-Geräte)

Wenn Ihr Gerät mehr als ein Modem hat, wird ein Feld **Wenn Nachrichten kommen zu** angezeigt. Lassen Sie es auf **Beliebiges Modem**, oder wählen Sie ein bestimmtes Modem aus, damit die Regel nur auf Nachrichten antwortet, die auf dieser SIM-Karte ankommen. Auf Geräten mit nur einem Modem wird dieses Feld nicht angezeigt.

Schreiben Sie die Antwort

Automatische Antwortnachricht Der Text, der zurückgesendet wird. Maximal 2000 Zeichen. Der gleiche Text wird an alle gesendet, die diese Regel auslösen, daher halten Sie ihn allgemein.

Als Unicode senden Aktivieren Sie dies, 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 beginnt sofort mit neu eingegangenen Nachrichten zu funktionieren.

Schritt 3: Legen Sie das Sendeverbot fest

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

Option	Ergebnis
Automatische Antworten immer senden	Jede übereinstimmende Nachricht erhält eine Antwort, egal wie viele ankommen.
Senden auf max. 5 Nachrichten / 10 Minuten / Telefonnummer begrenzen	Höchstens 5 automatische Antworten gehen an die gleiche Telefonnummer innerhalb von 10 Minuten. Weitere Nachrichten von dieser Nummer werden erst beantwortet, wenn das Zeitfenster vorbei ist.

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

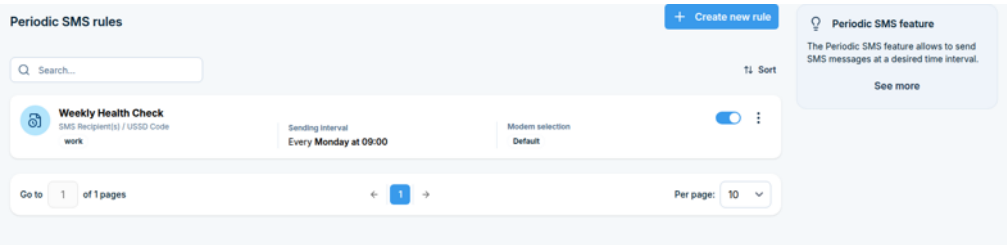
> **Es wird dringend empfohlen, das Limit zu verwenden.** Ohne es können zwei Geräte, die beide automatisch antworten, sich gegenseitig in einer Schleife beantworten, was SMS-Guthaben schnell aufzehrt. Das Limit ist der Schutz davor.

Diese Einstellung ist **global**. Sie gilt für jede Autoreply-Regel auf dem Gerät.

Wie das Matching funktioniert

- Die Textbedingung ist ein **contains**-Match, kein exakter Match. Eine Regel, die nach `PRICE` sucht, beantwortet eine Nachricht, die sagt `what is the PRICE of item 5`.
- Wenn mehrere Regeln die gleiche eingehende Nachricht erfüllen, sendet **jede** von ihnen ihre eigene Antwort, so dass 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 Erstellung und Aktivierung der Regel ankommen. Sie verarbeiten nicht bereits im Posteingang vorhandene Nachrichten.

Periodische SMS



Periodische SMS-Regel hinzufügen Dialog

Was diese Funktion macht

Periodische SMS sendet eine Nachricht **automatisch nach einem wiederholten Zeitplan**, ohne dass jemand auf Senden klicken muss. Sie erstellen eine Regel einmal, und SMSEagle sendet sie jede Stunde, täglich, wöchentlich, monatlich oder jährlich.

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 (z. B. um das Prepaid-Guthaben der SIM-Karte zu überprüfen).

Typische Anwendungen: eine tägliche „Systemlebt"-Nachricht, eine wöchentliche Erinnerung für ein Bereitschaftsteam, eine monatliche Gutschriftprüfung auf einer Prepaid-SIM.

Bevor Sie beginnen

- Wenn Sie an eine Gruppe senden 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 Zeitplan der Gerätezeit folgt. Überprüfen Sie dies in **Settings > Date/Time**.

Schritt 1: Öffnen Sie die Seite „Periodic SMS"

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

Schritt 2: Erstellen Sie eine Regel

Klicken Sie in der oberen rechten Ecke auf **Create new rule** (Neue Regel erstellen). Ein Seitenfenster öffnet sich.

Benennen Sie die Regel

Geben Sie in **Rule name** einen Text ein, den Sie später wiedererkennen werden, z. B. `Daily heartbeat` oder `Monthly SIM balance`. Maximum 100 Zeichen.

Zeitplan festlegen

Wählen Sie einen **Sending interval** aus. Die Felder unter dem Selector ändern sich je nach Ihrer Auswahl:

Interval	Ihre Einstellung	Beispiel
Hourly	**At minute** (in 5-Minuten-Schritten)	`15` sendet um 00:15, 01:15, 02:15 usw.
Daily	**At time**	`07:30` sendet jeden Morgen um 07:30
Weekly	**At week day** und **At time**	`Monday` + `08:00` sendet jeden Montagmorgen
Monthly	**At day of month** und **At time**	`1` + `09:00` sendet am ersten Tag jeden Monats
Annually	**At month - day** (Format `mm-dd`) und **At time**	`12-24` + `10:00` sendet jeden 24. Dezember

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

Wählen Sie das Modem (nur Multi-Modem-Geräte)

Wenn Ihr Gerät mehr als ein Modem hat, erscheint ein **Modem selection** Feld. Behalten Sie die Standardeinstellung bei, um SMSEagle auswählen zu lassen, oder wählen Sie ein bestimmtes Modem, wenn die Nachricht über eine bestimmte SIM-Karte gehen muss. Auf Einzelmodem-Geräten wird dieses Feld nicht angezeigt.

Wählen Sie aus, was Sie senden möchten

Verwenden Sie den Schalter **Message type** am oberen Rand dieses Abschnitts:

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 passen.
3. Wählen Sie unter **Send to** aus, wohin die Nachricht gehen soll:
    - **Public groups** – geben Sie einen Gruppennamen ein und wählen Sie ihn aus der Liste aus. 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 der 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 Ihrem Posteingang an.

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

Optional einen Telefonanruf hinzufügen

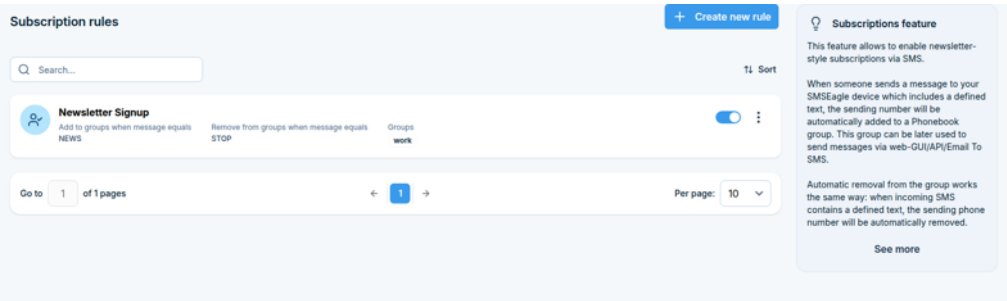
Call after sending SMS bewirkt, dass das Gerät auch einen Sprachanruf an die gleichen Empfänger tätigt, was für Warnungen nützlich ist, die nicht übersehen werden dürfen. Die verfügbaren Optionen hängen von Ihrem Gerätemodell ab:

Option	Was geschieht
Nein	Es wird kein Anruf getätigt. Dies ist die Standardeinstellung.
Nur Klingeln	Das Gerät ruft den Empfänger an und legt auf. Es wird keine Sprachnachricht abgespielt.
Ja – Text-zu-Sprache	Das Gerät ruft an und liest den Nachrichtentext vor.
Ja – Text-zu-Sprache (erweitert)	Wie oben, aber mit einer wählbaren, 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 erscheint in der Liste und wird zur nächsten geplanten Zeit ausgeführt.

Abos



Abonnement-Regeln

Was diese Funktion macht

Mit Abos können sich Personen **durch SMS an eine Telefonbuch-Gruppe anmelden und abmelden**, ähnlich wie bei einer Newsletter-Anmeldung.

Sie definieren zwei Schlüsselwörter: eines, das den Absender zu einer Gruppe hinzufügt, und eines, das ihn entfernt. Wenn jemand Ihre SMSEagle-Nummer mit einem dieser Schlüsselwörter textet, wird ihre Telefonnummer automatisch zur Gruppe hinzugefügt oder daraus entfernt. Sie können dann von Compose, der API oder Email to SMS aus Nachrichten an diese Gruppe senden.

Typische Anwendungen: eine öffentliche Benachrichtigungsliste, die Bewohner abonnieren können, oder eine Schicht-Benachrichtigungsliste, die Mitarbeiter selbst beitreten können, ohne dass ein Administrator eingreifen muss.

Bevor Sie beginnen

Erstellen Sie die Gruppe, für die 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 **public** Gruppen können in einer Abonnement-Regel verwendet werden.

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

Schritt 1: Öffnen Sie die Seite „Subscriptions

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

Schritt 2: Erstellen Sie eine Regel

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

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

Groups Geben Sie ein und wählen Sie eine oder mehrere Gruppen aus. Abonnenten werden in **alle** hier aufgelisteten Gruppen aufgenommen oder aus ihnen entfernt. Nur öffentliche Gruppen können ausgewählt werden.

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

Telefonnummer aus Gruppen entfernen, wenn eingehende Nachricht gleich ist Das Schlüsselwort, das jemanden abmeldet, z. B. `STOP` oder `LEAVE`.

Groß-/Kleinschreibung beachten Lassen Sie dies deaktiviert, damit `join`, `Join` und `JOIN` alle funktionieren. Aktivieren Sie diese Option nur, wenn das Schlüsselwort genau wie eingegeben übereinstimmen muss.

Klicken Sie auf **Save**.

Wie das Matching funktioniert

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

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

Schlüsselwort ist `JOIN`	Ergebnis
Benutzer sendet `JOIN`	Abonniert
Benutzer sendet `join`	Abonniert (es sei denn, **Groß-/Kleinschreibung beachten** 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, nur das Schlüsselwort zu senden.

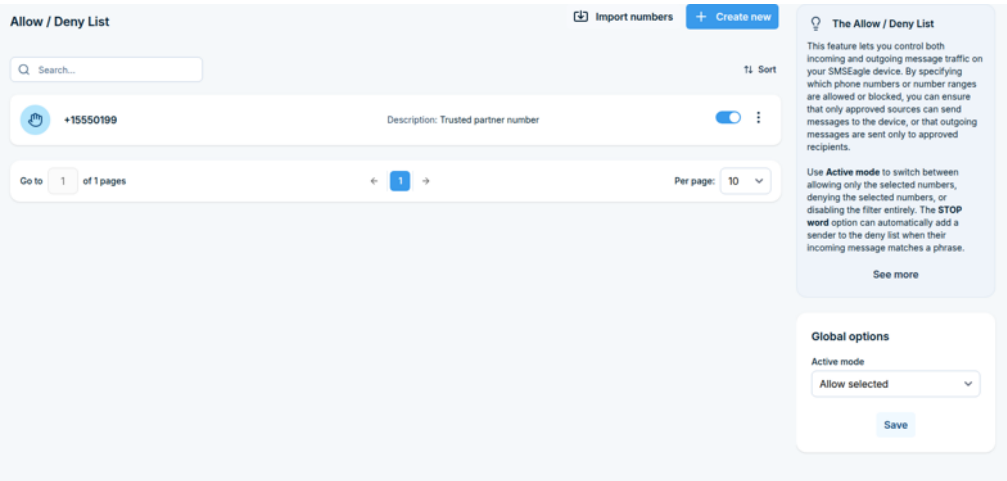
Was passiert, wenn sich jemand abonniert

- 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 und 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 wird im Telefonbuch beibehalten.

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

Allow / Deny List



Allow / Deny List-Globaloptionen

Was diese Funktion macht

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

Sie führen eine Liste von Nummern und wählen, wie das Gerät damit umgeht:

Active mode	Was geschieht
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	Überhaupt keine Filterung. Die Liste wird gespeichert, aber nicht verwendet.

Typische Anwendungen: Blockieren einer Nummer, die das Gerät ständig mit Spam bombardiert (Ablehnen), oder Sperren eines Gateways, damit nur Ihre eigenen Alarmsysteme damit kommunizieren können (Zulassen).

Es gibt auch eine **STOP-Wort**-Option, die einen Absender automatisch zur Liste hinzufügt, wenn seine Nachricht eine von Ihnen definierte Phrase enthält. Das ermöglicht Opt-out-Schlüsselwörter wie `STOP`.

Bevor Sie beginnen

Entscheiden Sie, wie Sie arbeiten möchten. **Zulassen (ausgewählt)** und **Ablehnen (ausgewählt)** verwenden zwei separate Listen, daher sind die Regeln, die Sie in einem Modus hinzufügen, im anderen nicht sichtbar. Das Wechseln des Modus wechselt die gesamte Liste, invertiert sie jedoch nicht.

Schritt 1: Öffnen Sie die Seite „Zulassen/Ablehnen-Liste“

Gehen Sie in der Seitenleiste zu **Automation > Allgemein > Zulassen/Ablehnen-Liste**.

Auf der rechten Seite befindet sich ein **Globale Optionen**-Feld mit der Einstellung **Aktiver Modus** und der Konfiguration **STOP-Wort**. Beide sind unten beschrieben.

Schritt 2: Wählen Sie den aktiven Modus

Legen Sie im **Globale Optionen**-Feld **Aktiver Modus** auf **Zulassen (ausgewählt)**, **Ablehnen (ausgewählt)** oder **Deaktiviert** fest und klicken Sie auf **Speichern**. Die Seite wird neu geladen und zeigt die Liste an, die zum gewählten Modus gehört.

> Während der Modus **Deaktiviert** ist, zeigt die Seite statt der Liste eine Meldung „Filterung ist deaktiviert“ an, und Regeln können nicht hinzugefügt oder bearbeitet werden. Wechseln Sie zu **Zulassen (ausgewählt)** oder **Ablehnen (ausgewählt)**, um sie wieder zu verwalten.

Schritt 3: Fügen Sie eine Nummer hinzu

Klicken Sie oben rechts auf **Neu erstellen**. Ein Seitenpanel wird geöffnet.

Telefonnummer Die Nummer, auf die diese Regel angewendet wird. Maximal 15 Zeichen. Nur Ziffern, + und * sind erlaubt, und der Eintrag muss mindestens eine Ziffer enthalten.

Sie können eine ganze Reihe von Nummern abgleichen, indem Sie * als Platzhalter verwenden, der für beliebige Zeichen steht:

Muster	Treffer
`NUMMER`	Genau diese Nummer
`*NUMMER`	Beliebige Nummer, die damit endet
`NUMMER*`	Beliebige Nummer, die damit beginnt
`*NUMMER*`	Beliebige Nummer, die das enthält

Beispielsweise deckt `48512*` jede Nummer ab, die mit `48512` beginnt, und `*12345678` passt zu demselben Teilnehmer unabhängig von dem ankommenden Länder-Präfix-Format.

Beschreibung Eine kurze Notiz, die erklärt, warum die Nummer auf der Liste steht, z. B. `Spam` oder `Alarmpanel, Hauptsitz`. Erforderlich, maximal 255 Zeichen.

Klicken Sie auf **Save**.

Schritt 4: Importieren Sie eine Liste aus einer CSV-Datei

Wenn Sie die Nummern bereits in einer Tabellenkalkulation haben, klicken Sie statt sie einzeln hinzuzufügen oben rechts auf **Regeln importieren**.

1. Bereiten Sie eine UTF-8-kodierte CSV-Datei mit genau zwei Spalten vor, mit den Überschriften **Nummer** und **Grund**.
2. Klicken Sie auf **Regeln importieren**, ziehen Sie die Datei in den Upload-Bereich oder klicken Sie, um zu durchsuchen.
3. Klicken Sie auf **Importieren**.

Die Nummern werden zur derzeit aktiven Liste hinzugefügt.

Schritt 5: Konfigurieren Sie das STOP-Wort (optional)

Das STOP-Wort fügt Absender automatisch zur Liste hinzu, sodass Personen sich abmelden können, indem sie ein Schlüsselwort texten.

Klicken Sie im Feld **Globale Optionen** auf **Konfiguration bearbeiten** neben **STOP-Wort**. Ein Seitenpanel wird geöffnet. Wählen Sie **Nummer automatisch zur Liste hinzufügen, wenn**:

Option	Was das bedeutet
Nie	Das STOP-Wort ist deaktiviert. Nummern werden nur manuell oder durch Import hinzugefügt.
Eingehende Nachricht ist gleich…	Die gesamte Nachricht muss genau der eingegebenen Phrase entsprechen.
Eingehende Nachricht enthält…	Die Phrase kann an beliebiger Stelle in der Nachricht erscheinen.

Wenn Sie eine der beiden Abgleichoptionen auswählen, erscheinen zwei weitere Felder:

- Die Phrase selbst, maximal 160 Zeichen, beispielsweise `STOP`.
- **Automatische Antwortnachricht**, maximal 160 Zeichen. Dieser Text wird an die Nummer zurückgesendet, nachdem sie zur Liste hinzugefügt wurde. Lassen Sie dieses Feld leer, wenn Sie die Abmeldung nicht bestätigen möchten.

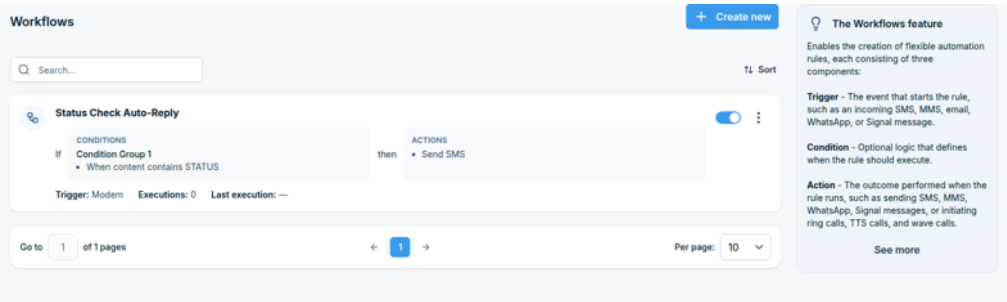
Klicken Sie auf **Speichern**. Die Zusammenfassung im Feld **Globale Optionen** zeigt nun die aktive Bedingung und den Antwortnachrichtentext an.

> **Verwenden Sie „ist gleich“ statt „enthält“ für Abmeldeschlüsselwörter.** Mit **enthält** 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. Es werden keine bereits im Posteingang vorhandenen Nachrichten erneut verarbeitet.
- Eine deaktivierte Regel wird vollständig ignoriert, unabhängig davon, welcher Modus aktiv ist.
- **Ausgewählte zulassen** und **Ausgewählte ablehnen** verwenden separate Listen. Wenn Sie den Modus wechseln und die Seite leer erscheint, sehen Sie die andere Liste, nichts wurde gelöscht.
- Die STOP-Wort-Einstellung ist **global**: Sie gilt für die derzeit aktive Liste.

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-/Gesendet-/Sendungsfehler-Ereignis).
- **Bedingung** – optionale Logik, die festlegt, ob die Regel für ein bestimmtes Ereignis ausgeführt werden soll.
- **Aktion** – was geschieht, wenn die Regel ausgeführt wird: Senden einer SMS-, MMS-, WhatsApp- oder Signal-Nachricht oder Initiieren eines Ringaufrufs, TTS-Aufrufs oder Wave-Aufrufs.

Wo finde ich es

Automatisierung > Allgemein > Workflows (`/automation/workflows/`).

Schritt 1: Erstellen Sie einen Workflow und wählen Sie einen Trigger

Klicken Sie auf **Neu erstellen**, geben Sie dem Workflow einen **Namen** und wählen Sie einen **Auslöser**: Modem, E-Mail, Signal, WhatsApp, Modem (zugestellt), Modem (gesendet) oder Modem (Sendefehler).

Schritt 2: Bedingungsgruppen hinzufügen (optional)

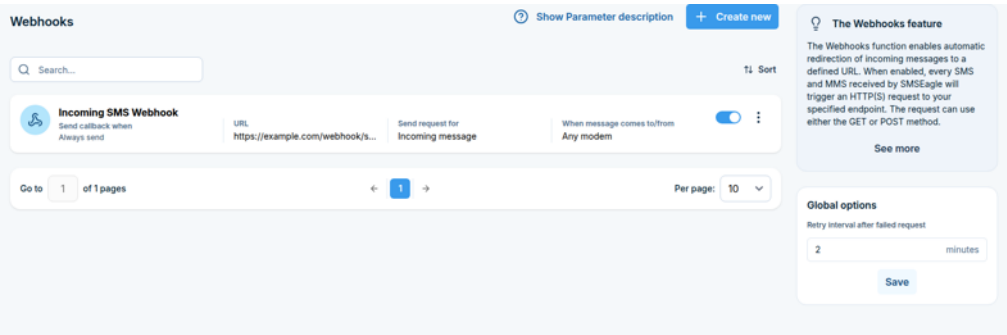
Klicken Sie unter **Bedingungsgruppen** auf **Gruppe hinzufügen**, um eine oder mehrere Bedingungen hinzuzufügen, die das eingehende Ereignis erfüllen muss, bevor der Workflow ausgeführt wird. Lassen Sie dies leer, wenn der Workflow für jedes Ereignis ausgeführt werden soll, das dem Auslöser entspricht.

Schritt 3: Aktionen hinzufügen

Klicken Sie unter **Aktionen** auf **Aktion hinzufügen**, um zu definieren, was der Workflow bei Ausführung tut – beispielsweise das Senden einer Antwort, das Weiterleiten der Nachricht an einen anderen Kanal oder das Tätigen eines Anrufs.

Klicken Sie auf **Workflow speichern**, um ihn zu aktivieren.

Webhooks



Webhooks-Übersicht

Was diese Funktion macht

Ein Webhook veranlasst SMSEagle, **Ihr** System aufzurufen. Immer wenn auf dem Gerät etwas passiert (eine Nachricht kommt an, eine Nachricht wird gesendet, ein Zustellbericht 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 Abrufen der API in ein Ticketing-System, ein CRM, einen Chatbot oder Ihre eigene Anwendung übertragen.

Zwei Integrationen erhalten dedizierte Unterstützung:

Methode	Wofür es ist
POST (3CX)	Übertragen von Nachrichten in ein 3CX-Telefonsystem.
POST (Zabbix)	Quittieren von Zabbix-Ereignissen per SMS, damit ein Techniker mit `ACK 12345` antworten kann, um eine Benachrichtigung 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 Endpunkt sollte mit HTTP **200 OK** antworten oder mit den Statuscodes, die Sie in der Regel konfigurieren.
- Für Zabbix benötigen Sie entweder ein API-Token (Zabbix 6.4 und neuer) oder einen Benutzernamen und ein Passwort.

Schritt 1: Webhooks-Seite öffnen

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

Jede Regel zeigt ihre URL, wofür sie ausgelöst wird und auf Multi-Modem-Geräten, auf welches Modem sie beschränkt ist. Jede Regel hat einen Schalter zum **Aktivieren oder Deaktivieren**, eine **Aktion bearbeiten** und eine **Aktion löschen**.

Das Feld **Globale Optionen** auf der rechten Seite enthält eine Einstellung, die für alle Regeln gilt und in Schritt 6 beschrieben wird.

Schritt 2: Erstellen Sie eine Regel

Klicken Sie auf **Neu erstellen** in der oberen rechten Ecke. Das Webhook-Formular öffnet sich als ganze Seite mit drei Abschnitten.

Schritt 3: Grundkonfiguration

Feld	Was Sie eingeben müssen
Regelname	Ein beschreibender Name, maximal 100 Zeichen.
URL	Die Adresse zum Aufrufen, maximal 300 Zeichen, zum Beispiel `https://example.com/webhook`.
URL-Methode	**GET**, **POST**, **POST (3CX)** oder **POST (Zabbix)**.
Content-Typ	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 unter dem Feld angezeigt und zeigt den zurückgegebenen HTTP-Status an, damit Sie bestätigen können, dass der Endpunkt funktioniert, bevor Sie speichern.

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

Was die Anfrage enthält

Die Anfrage, die Ihr Endpunkt erhält, trägt 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`	Sendernummer.
`timestamp`	Wann SMSEagle die Nachricht empfangen oder versendet hat, im Format `YYYYmmddHHiiss`, zum Beispiel `20140531092257`.
`msgid`	Die SMSEagle-Nachrichten-ID.
`modemno`	Das Modem, auf dem die eingehende Nachricht empfangen wurde, oder dasjenige, von dem die Nachricht versendet wurde.
`apikey`	Der API-Schlüssel Ihres Dienstes, falls Sie einen in den **Sicherheitseinstellungen** festgelegt 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 des OID-Identifikators, der einer ausgehenden Nachricht mit einer passenden Telefonnummer zugewiesen ist. Optional.
`attachments`	MMS-Anhänge, beispielsweise `[0 => [name => image.png, content-type => image/png, content => wfFWgwOlgBRwdWvsvs=]]`. **Nur POST**, da eine GET-Abfragezeichenfolge keine Dateidaten tragen 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 immer nur die Parameter dieses Typs. Eine Regel mit dem Trigger **Incoming call** sendet beispielsweise niemals `text` oder `attachments`.

Unabhängig von der Methode erwartet SMSEagle, dass Ihr Endpunkt mit **200 [OK]** antwortet, es sei denn, Sie erweitern dies mit **Expected HTTP Status Code(s)** in den Security settings.

Der Link **Show Parameter description** auf der Regelseite 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. Wenn Ihr Endpunkt andere erwartet, aktivieren Sie **Customize parameter names** und geben Sie neben jedem Parameter, den Sie umbenennen möchten, Ihren eigenen Namen ein. Alle Parameter in den drei Tabellen können umbenannt werden; die, bei denen Sie das Feld leer lassen, behalten ihren Standardnamen.

Das Umbenennen ändert nur den Parameter **name** in der Anfrage, niemals seinen Wert oder wann er gesendet wird.

Schritt 4: Auslösebedingungen

Send request for entscheidet, welches Ereignis den Webhook auslöst:

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

Send request when grenzt es weiter ein:

Option	Was das bedeutet
Always	Jedes Ereignis des ausgewählten Typs löst den Webhook aus.
Für angegebene Absender / wenn Text enthält	Nur Ereignisse, die die unten genannten Bedingungen erfüllen, lösen es aus.

Wenn Sie die zweite Option gewählt haben, werden zwei Bedingungen verfügbar. Sie können eine oder beide verwenden, und ein Ereignis muss jede aktivierte Bedingung erfüllen.

Wenn eingehende SMS von Aktivieren Sie dies und wählen Sie die Kontakte oder Gruppen aus. Nur öffentliche Kontakte und Gruppen werden akzeptiert.

Wenn eingehender SMS-Text enthält Aktivieren Sie dies und geben Sie den Satz ein. Aktivieren Sie **Case sensitive**, wenn Groß- und Kleinschreibung unterschiedlich behandelt werden sollen. Diese Bedingung ist nicht für den Trigger **Incoming call** verfügbar, da ein Anruf keinen Text hat.

Auf Multi-Modem-Geräten beschränkt **When message comes to/from** die Regel auf ein einzelnes Modem. Lassen Sie es ansonsten auf **Any modem**.

Schritt 5: Sicherheitseinstellungen

Feld	Funktionsweise
API-Schlüssel Ihres Dienstes	Ein optionaler Schlüssel, der mit der Anfrage gesendet wird, damit Ihr Endpunkt überprüfen kann, dass der Aufruf wirklich von Ihrem Gerät kommt.
Erwartete HTTP-Statuscodes	Welche Antworten als erfolgreich gelten. Ein oder mehrere dreistellige Codes, durch Kommas getrennt, z.B. `200,201,202`. Standard ist `200`, maximal 20 Zeichen.
Selbstsigniertes SSL-Zertifikat zulassen	Akzeptieren Sie ein Zertifikat, das nicht von einer öffentlichen Behörde signiert ist.
Peer überprüfen	Überprüfen Sie das Zertifikat des Servers.
Peer-Namen überprüfen	Überprüfen Sie, dass 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 action** - **Acknowledge (ACK)**, **Unacknowledge (NOACK)** oder beide. Das Feld zeigt das SMS-Format, das das Gerät erwartet, z.B. `ACK 12345 Problem resolved`.
- **Auth type** - **API Token** (Zabbix 6.4 und neuer, empfohlen) oder **Login/Password** für ältere Versionen. Bei einem Token geben Sie ihn in das API-Schlüssel-Feld ein, bei Login geben Sie **Zabbix username** und **Zabbix password** ein.
- **Test values** - eine **Event ID** und eine **Message**, die nur von **Test connection** verwendet und nie gespeichert werden.

Klicken Sie auf **Save webhook**.

Schritt 6: Wiederholungsintervall festlegen

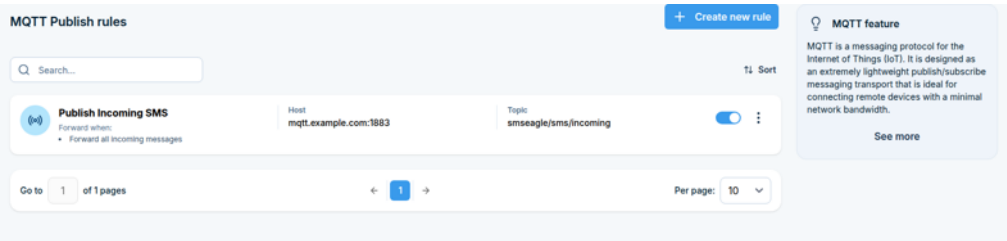
Das Feld **Global options** auf der Seite der Regeln enthält **Retry interval after failed request** in Minuten. Wenn eine Anfrage fehlschlägt, wartet das Gerät diese Zeit, bevor es erneut versucht.

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

Verhalten von Webhooks

- Regeln gelten für Ereignisse, die nach der Erstellung und Aktivierung der Regel auftreten. Sie wiederholen keine vergangenen Nachrichten.
- Die Textbedingung ist eine **contains**-Übereinstimmung, keine exakte Übereinstimmung.
- Wenn mehrere Regeln das gleiche Ereignis auslösen, sendet **jede** von ihnen eine eigene Anfrage, sodass eine Nachricht mehrere Endpunkte erreichen kann.
- Eine Anfrage gilt als erfolgreich nur, wenn der Antwortstatus einer der **Expected HTTP Status Code(s)** ist. Alles andere, einschließlich gar keine Antwort, ist ein Fehler und wird erneut versucht.
- **Test connection** sendet eine Beispiel-Payload, keine echte Nachricht, daher ist es sicher, sie gegen einen Produktionsendpunkt auszuführen, der nur protokolliert.

MQTT



MQTT Publish-Regeln

Was diese Funktion macht

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

SMSEagle sitzt auf beiden Seiten dieser Kommunikation:

Regeltyp	Richtung	Funktionsweise
Subscribe	MQTT zu SMS	Abhören eines Brokers und Umwandlung eingehender MQTT-Nachrichten in SMS-Nachrichten, die an Ihre Mitarbeiter gesendet werden.
Publish	SMS zu MQTT	Nimmt eingehende SMS-Nachrichten auf und veröffentlicht sie auf einem Broker, damit Ihr IoT-System darauf reagieren kann.

Typische Anwendungen: Umwandlung einer Sensoralarmierung in eine SMS an das Wartungsteam (Subscribe) oder Ermöglichung für einen Techniker, einen Text mit einem Befehl zu senden, der vom Automationssystem aufgegriffen wird (Publish).

Die beiden Regeltypen werden separat konfiguriert und sind nicht voneinander abhängig. Verwenden Sie den Typ, den Sie benötigen.

Bevor Sie beginnen

Sie benötigen die Verbindungsdetails Ihres MQTT-Brokers: Host-Adresse, Port und Benutzername und Passwort, falls der Broker diese benötigt – einmalig konfiguriert unter MQTT in Einstellungen, bevor Sie hier Subscribe-Regeln schreiben.

Für **Subscribe**-Regeln benötigen Sie auch die Liste der Themen zum Abhören (auch unter Einstellungen festgelegt). Für **Publish**-Regeln benötigen Sie das Thema zum Veröffentlichen (pro Regel festgelegt, unten).

Teil 1: Subscribe (MQTT zu SMS)

Subscribe-Regeln wandeln eingehende MQTT-Nachrichten in SMS um, sobald die Broker-Verbindung selbst unter Einstellungen konfiguriert ist.

Schritt 1: Öffnen Sie die Seite Subscribe-Regeln

Gehen Sie in der Seitenleiste zu **Automation > General > MQTT**, wählen Sie dann **Subscribe**.

Schritt 2: Erstellen Sie eine Subscribe-Regel

Klicken Sie in der oberen rechten Ecke auf **Create new rule** (Neue Regel erstellen). Ein Seitenfenster öffnet sich.

Benennen Sie die Regel

Geben Sie unter **Rule name** etwas Beschreibendes ein, z. B. `Boiler alarm to maintenance`. Maximal 100 Zeichen.

Entscheiden Sie, auf welche MQTT-Nachrichten Sie reagieren möchten

Wählen Sie **Forward for** (Weiterleiten für):

Option	Was das bedeutet
Any message	Jede MQTT-Nachricht, die das Gerät empfängt, löst diese Regel aus.
Angegebenes Thema / Nachricht	Nur Nachrichten, die den von Ihnen festgelegten Bedingungen entsprechen, lösen es aus.

Wenn Sie **Angegebenes Thema / Nachricht** wählen, werden zwei Bedingungen verfügbar. Sie können eine oder beide verwenden. Wenn Sie beide verwenden, muss eine Nachricht **beide** erfüllen.

Wenn eingehende Nachricht das Thema hat Aktivieren Sie dies und geben Sie das Thema in **Thema** ein, z. B. `building/boiler`.

Wenn eingehende Nachricht enthält Aktivieren Sie dies und geben Sie den Ausdruck in **Nachrichtensatz** ein, z. B. `ALARM`. Aktivieren Sie **Groß-/Kleinschreibung beachten**, wenn `alarm` und `ALARM` als unterschiedlich behandelt werden sollen.

Wählen Sie die Empfänger

Wählen Sie in **Weiterleiten an** die Kontakte oder Gruppen aus, die die SMS erhalten sollen. Hier können nur **öffentliche** Kontakte und Gruppen ausgewählt werden. Dieses Feld ist erforderlich.

Schreiben Sie den SMS-Text

Nachrichtenformat steuert, was die SMS sagt. Sie erstellen es aus der MQTT-Nachricht mit Platzhaltern:

Platzhalter	Ersetzt durch
`{TOPIC}`	Das Thema, auf dem die MQTT-Nachricht ankam
`{MESSAGE}`	Der Inhalt der MQTT-Nachricht

Der Standard ist `{TOPIC}: {MESSAGE}`, was eine SMS wie `building/boiler/temperature: 94` erzeugt. Sie können auch Ihren eigenen Satz um sie schreiben, z. B. `Boiler warning on {TOPIC}, value {MESSAGE}`.

Aktivieren Sie **Als Unicode senden**, wenn der Text Zeichen außerhalb des Standard-GSM-Alphabets enthält, z. B. polnische, deutsche oder kyrillische Buchstaben.

Erweiterte Optionen

Klicken Sie auf **Erweiterte Optionen**, um diesen Abschnitt zu erweitern. Sie benötigen dies nicht für eine grundlegende Einrichtung.

- **Modem** (nur Multi-Modem-Geräte) – SMS über eine bestimmte SIM-Karte statt der Standardeinstellung senden.
- **Anruf nach dem Versenden von SMS** – auch einen Sprachanruf an die gleichen Empfänger tätigen. Die Optionen sind **Nein**, **Nur klingeln**, **Ja – Sprachsynthese** und **Ja – Sprachsynthese**

(erweitert), je nach den Funktionen Ihres Gerätemodells. Mit der erweiterten Option wählen Sie auch ein **Sprachmodell** aus.

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

Wie Subscribe-Matching funktioniert

- Die **Thema**-Bedingung ist eine **Enthält**-Übereinstimmung und ignoriert Groß- und Kleinschreibung. Eine Regel mit dem Thema `boiler` passt auch auf `building/boiler/temperature`.
- Das Kontrollkästchen **Groß-/Kleinschreibung beachten** gilt nur für den Nachrichtensatz, niemals für das Thema.
- Wenn mehrere Subscribe-Regeln zu derselben MQTT-Nachricht passen, sendet **jede** davon ihre eigene SMS.

Teil 2: Publish (SMS in MQTT)

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

Schritt 1: Öffnen Sie die Seite der Publish-Regeln

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

Schritt 2: Erstellen Sie eine Publish-Regel

Klicken Sie in der oberen rechten Ecke auf **Create new rule** (Neue Regel erstellen). Ein Seitenfenster öffnet sich.

Benennen Sie die Regel

Geben Sie in **Regelname** etwas Aussagekräftiges ein, z. B. `Technician commands to automation`. Maximal 100 Zeichen.

Entscheiden Sie, welche SMS-Nachrichten veröffentlicht werden sollen

Wählen Sie **Forward for** (Weiterleiten für):

Option	Was das bedeutet
Any message	Jede eingehende SMS wird an den Broker veröffentlicht.
Angegebener Absender / Nachricht	Nur Nachrichten, die den unten festgelegten Bedingungen entsprechen, werden veröffentlicht.

Wenn Sie **Angegebener Absender / Nachricht** gewählt haben, werden die folgenden Bedingungen verfügbar. Sie können diese kombinieren, und eine Nachricht muss dann alle aktivierten Bedingungen erfüllen.

Wenn eingehende SMS von Aktivieren Sie dies und wählen Sie die Absenderkontakte oder Gruppen aus. Hier können nur **öffentliche** Kontakte und Gruppen ausgewählt werden.

Wenn eingehende SMS-Text enthält Aktivieren Sie dies und geben Sie den Ausdruck unter **Textfragment** ein. Aktivieren Sie **Groß- und Kleinschreibung beachten**, wenn Groß- und Kleinbuchstaben unterschiedlich behandelt werden sollen.

Wenn Nachrichten ankommen bei (nur Multi-Modem-Geräte) Lassen Sie auf **Beliebiges Modem**, oder wählen Sie ein bestimmtes Modem aus, sodass nur Nachrichten, die auf dieser SIM-Karte eingehen, veröffentlicht werden.

> Eine Publish-Regel durch einen Absenderzustand einzuschränken ist eine sinnvolle Vorsichtsmaßnahme. Ohne Absenderbedingung kann jeder, der Ihre Nummer kennt, Inhalte in Ihr IoT-System einspeisen.

Geben Sie die Broker-Verbindung ein

Füllen Sie den Broker aus, an den diese Regel veröffentlicht:

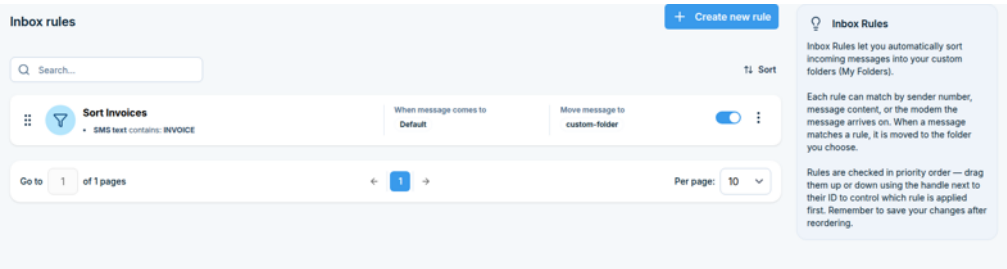
Feld	Was Sie eingeben müssen
Host	Die Broker-Adresse, z. B. `test.host.io`
Port	Der Broker-Port, z. B. 1883. Der zulässige Bereich ist 1 bis 65535.
Benutzername	Der Broker-Benutzer, falls erforderlich. Lassen Sie das Feld leer für einen offenen Broker.
Passwort	Das Broker-Passwort, falls erforderlich.
Topic	Das Topic, in das veröffentlicht werden soll, z. B. `smseagle/incoming`
TLS/SSL	Aktivieren Sie dies, wenn der Broker eine verschlüsselte Verbindung verwendet.
TLS-Zertifikatprüfung	Lassen Sie diese 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 Publish-Zuordnung

- Die Textbedingung ist eine **contains**-Übereinstimmung, keine exakte Übereinstimmung.
- Wenn mehrere Publish-Regeln die gleiche SMS erfüllen, veröffentlicht **jede** von ihnen, sodass die Nachricht auf mehr als einem Broker oder Topic landen kann.
- Regeln gelten nur für Nachrichten, die nach Erstellung und Aktivierung der Regel ankommen. Sie verarbeiten nicht bereits im Posteingang vorhandene Nachrichten.

Posteingangsregeln



Übersicht der Posteingangsregeln

Posteingangsregeln sortieren eingehende Nachrichten automatisch in Ihre benutzerdefinierten Ordner (Meine Ordner), anstatt alles im Hauptpostfach zu belassen.

Wo finde ich es

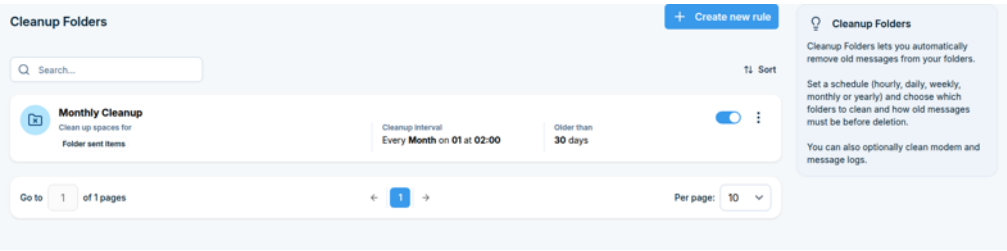
Automation > Folders > Inbox Rules (`/automation/inbox-rules/`).

Konfigurieren einer Posteingangsregel

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

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

Ordner bereinigen



Ordner bereinigen – Übersicht

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

Wo finde ich es

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

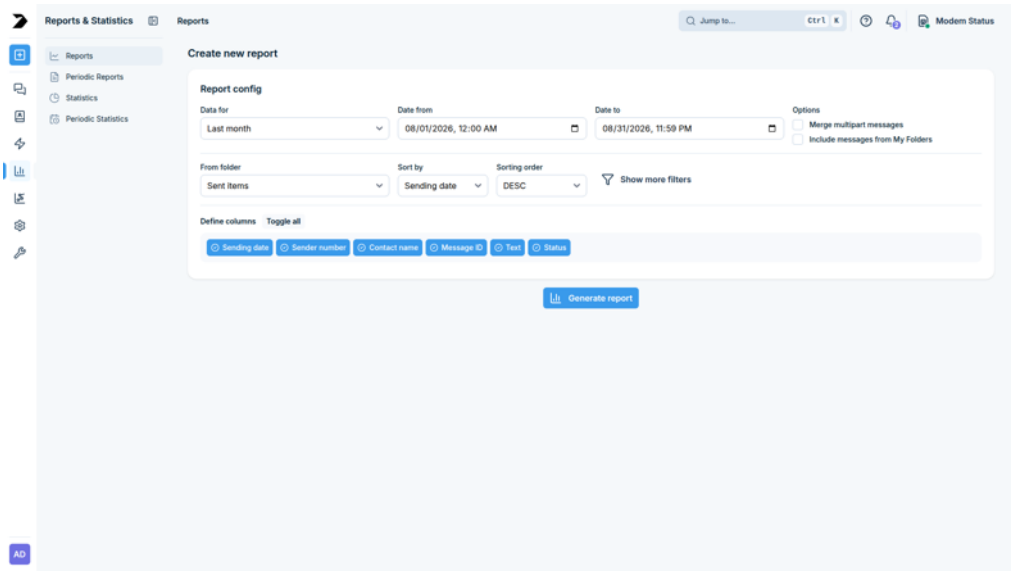
Konfigurieren einer Bereinigungsregel

Klicken Sie auf **Create new rule**, legen Sie dann einen Zeitplan fest (stündlich, täglich, wöchentlich, monatlich oder jährlich), wählen Sie die zu bereinigenden Ordner aus, 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 Bereich **Berichte & Statistiken** der Weboberfläche – das Exportieren von Nachrichtendaten als einmaligen Bericht oder das Planen von Berichten, die automatisch per E-Mail versendet werden.

Berichte



Create new report

Berichte & Statistiken > Berichte (`/reports/`) erstellt einen einmaligen Bericht Ihrer Nachrichtenhistorie.

Wählen Sie unter **Report config** den Zeitbereich mit **Data for** aus (ein vordefinierter Bereich wie Today, Last 7 days oder This month, oder **Custom range** mit expliziten Feldern **Date from** / **Date to**).

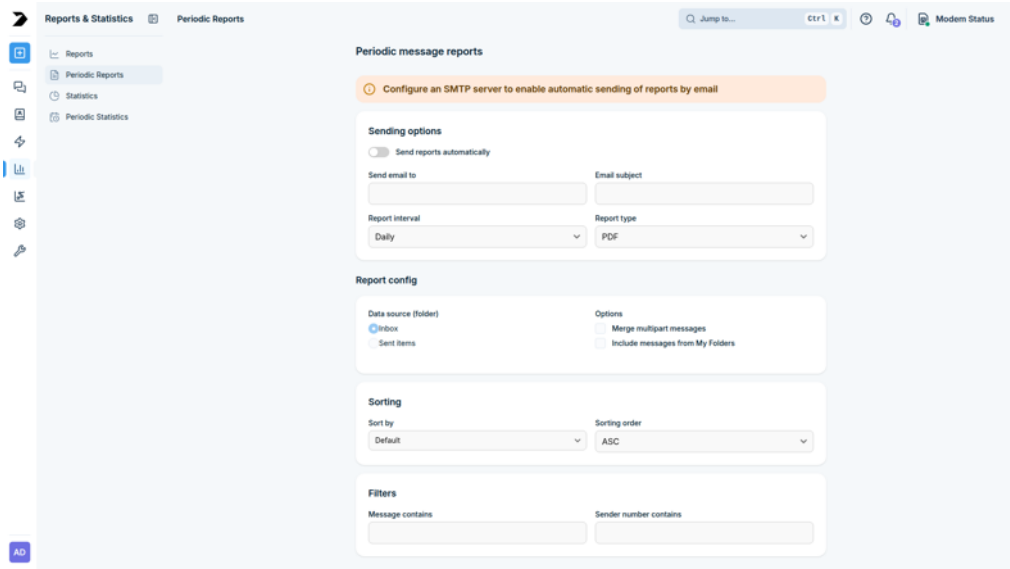
Unter **Options**:

Option	Funktion
Merge multipart messages	Kombiniert eine lange SMS, die in mehrere Teile aufgeteilt wurde, wieder in eine Zeile.
Include messages from My Folders	Bezieht auch Nachrichten ein, die in einen benutzerdefinierten Ordner verschoben wurden.
From folder	Welcher Ordner gemeldet werden soll: **Sent items**, **Inbox** oder **Outbox**.
Sort by / **Sorting order**	Spalte zum Sortieren nach (Sendedatum, Absendernummer, Kontaktname, Nachrichten-ID, Text oder Status) und Richtung (ASC/DESC).

Klicken Sie auf **Show more filters** für zusätzliche Filter und nutzen Sie **Define columns**, um zu wählen, welche Spalten im generierten Bericht angezeigt werden – **Toggle all** wählt oder löscht alle Spalten auf einmal.

Klicken Sie auf **Generate report**, um den Bericht zu erstellen.

Periodische Berichte



Periodische Nachrichtenberichte

Berichte & Statistiken > Periodische Berichte (`/reports/periodic-reports`) plant die automatische Generierung und den E-Mail-Versand eines Berichts in regelmäßigen Abständen, statt ihn jedes Mal manuell auszuführen.

Dies erfordert eine funktionierende SMTP-Konfiguration – auf der Seite wird eine Erinnerung zur Konfiguration angezeigt, falls diese fehlt.

Aktivieren Sie unter **Sending options Send reports automatically** und füllen Sie folgende Felder aus:

Feld	Funktion
Send email to	Die Empfängeradresse für den generierten Bericht.
Email subject	Die Betreffzeile der E-Mail.
Berichtintervall	**Täglich**, **Wöchentlich** oder **Monatlich**.
Berichttyp	**PDF** oder **CSV**.

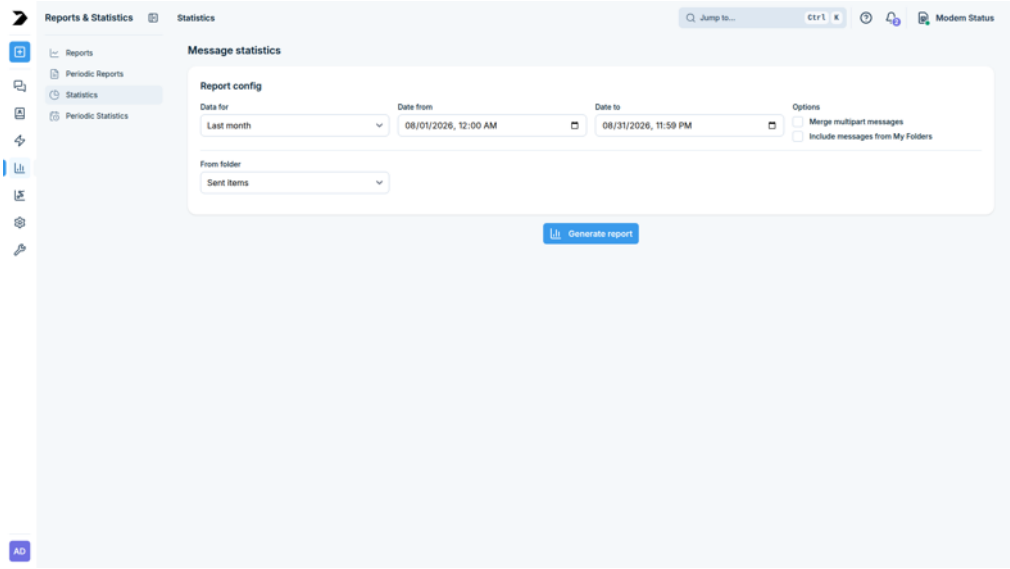
Wählen Sie unter **Report config** die **Data source (folder)** (**Inbox** oder **Sent items**), die gleichen Optionen **Merge multipart messages** / **Include messages from My Folders** wie bei einem einmaligen Bericht und **Sorting** (Sortierfeld und ASC/DESC-Reihenfolge).

Unter **Filters** grenzen Sie den Bericht mit **Message contains** und/oder **Sender number contains** ein.

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

Klicken Sie auf **Save configuration**.

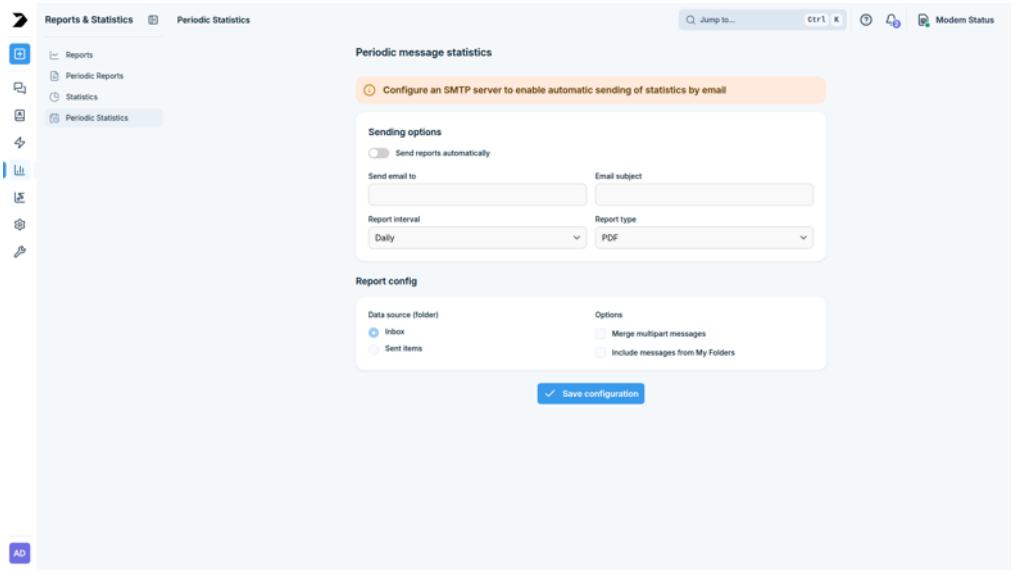
Statistiken



Nachrichtenstatistiken

Reports & Statistics > Statistics (`/reports/statistics`) funktioniert auf die gleiche Weise wie Reports oben – mit dem gleichen **Data for**-Zeitbereichswähler und **Merge multipart messages** / **Include messages from My Folders** / **From folder**-Optionen – erstellt aber aggregierte Datenverkehrsstatistiken statt eines zeilenweisen Exports. Klicken Sie auf **Generate report**, um ihn zu erstellen.

Periodische Statistiken



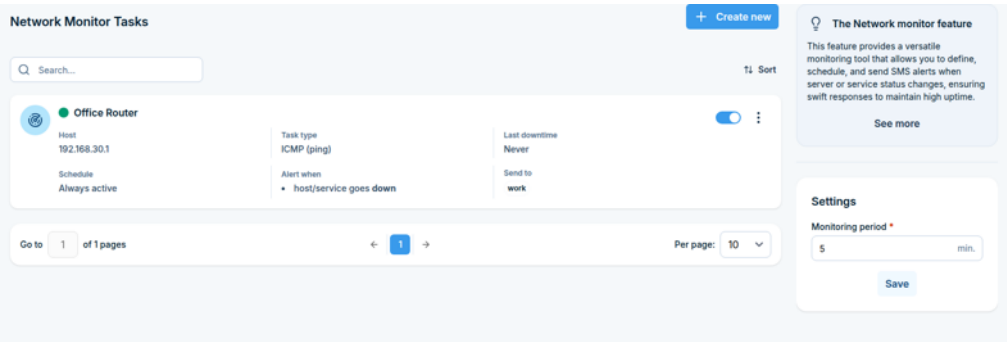
Periodische Nachrichtenstatistiken

Reports & Statistics > Periodic Statistics (`/reports/periodic-statistics`) plant die obige Statistikberechnung so ein, dass sie automatisch generiert und per E-Mail versendet wird, auf die gleiche Weise wie Periodic Reports für den zeilenweisen Export: eine funktionierende SMTP Configuration ist erforderlich, und es werden die gleichen **Sending options** angeboten (Empfänger, Betreffzeile, **Daily / Weekly / Monthly**-Intervall, **PDF / CSV**-Berichttyp) sowie ein Abschnitt **Report config** (Datenquellordner, Multipart-Nachrichten zusammenführen, My Folders einbeziehen). Klicken Sie auf **Save configuration**.

Überwachung

Dieses Kapitel behandelt den Bereich **Monitoring** (Überwachung) der Weboberfläche: Überprüfung externer Hosts und Dienste, Auslesen digitaler E/A und physischer Sensoren.

Netzwerkmonitor



Netzwerkmonitor-Übersicht

Funktion dieser Funktion

Der Netzwerkmonitor wandelt Ihren SMSEagle in eine kleine Überwachungsstation um. Er überprüft Server, Geräte und Dienste nach einem Zeitplan und sendet eine SMS, wenn etwas nicht antwortet, wieder verfügbar wird oder einen Wert außerhalb des erwarteten Bereichs meldet.

Es besteht aus drei Teilen:

Seite	Funktion
Tasks	Die Überwachungsregeln: was zu überprüfen ist, wie häufig, wen zu benachrichtigen.
Reports	Eine Ausfallhistorie, gefiltert nach Datumsbereich und Task, exportierbar als CSV.
SNMP Traps	Regeln, die SNMP-Traps, die an das Gerät gesendet werden, in SMS-Nachrichten umwandeln.

Typische Anwendungen: Benachrichtigung des diensthabenden Ingenieurs, wenn ein Produktionsserver nicht mehr auf Pings antwortet, Warnung bei einer Temperaturablesung von einem SNMP-Sensor oder Weiterleitung eines UPS-Traps an ein Telefon.

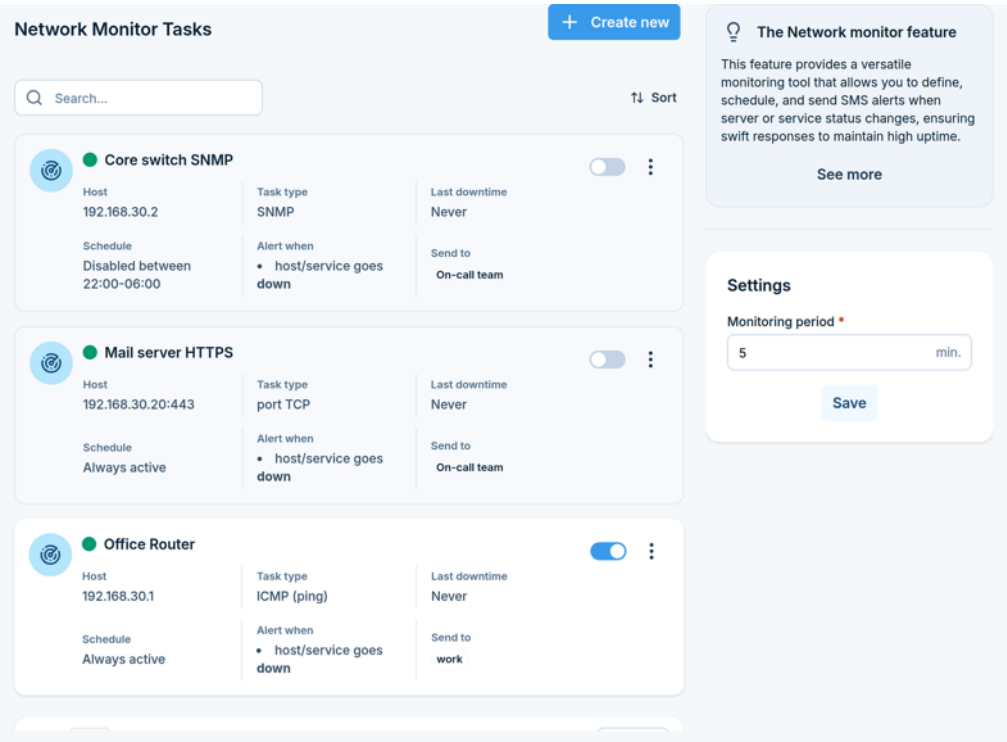
Bevor Sie beginnen

- Das Gerät muss die Hosts erreichen können, die Sie überwachen möchten. Überprüfen Sie zuerst die Netzwerkeinstellungen unter **Settings > Network**.
- Empfänger müssen in dem Adressbuch als **Public** markiert sein, wenn Sie eine Gruppe benachrichtigen möchten. Andernfalls können Sie einfache Telefonnummern in den Task eingeben.
- Für SNMP-Überprüfungen benötigen Sie die Community-Zeichenfolge und die Object ID (OID), die Sie auslesen möchten. Für Modbus-Überprüfungen benötigen Sie die Unit-ID, das Register und den Funktionscode.

Teil 1: Tasks

Schritt 1: Öffnen Sie die Seite „Tasks

Gehen Sie in der Seitenleiste zu **Monitoring > Network Monitoring > Tasks**.



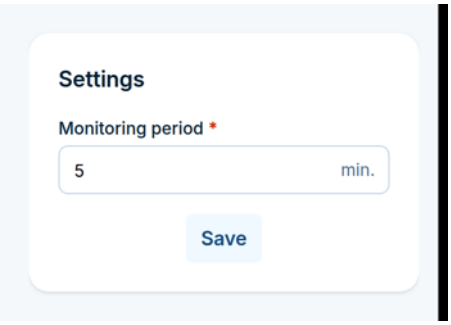
Netzwerkmonitor-Tasks

Jeder Task in der Liste zeigt seinen Host, den Zeitplan, den Task-Typ, worauf er reagiert, wann er zuletzt ausfiel und wen er benachrichtigt. Ein grüner oder roter Marker zeigt an, ob der Host derzeit antwortet.

Schritt 2: Legen Sie den Überwachungszeitraum fest

Das Feld **Settings** auf der rechten Seite der Tasks-Seite enthält eine Einstellung, die auf **alle** Tasks angewendet wird: **Monitoring period** (Überwachungszeitraum) in Minuten. Dies ist die Häufigkeit, mit der das Gerät die Überprüfungen durchführt.

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



Überwachungszeitraum

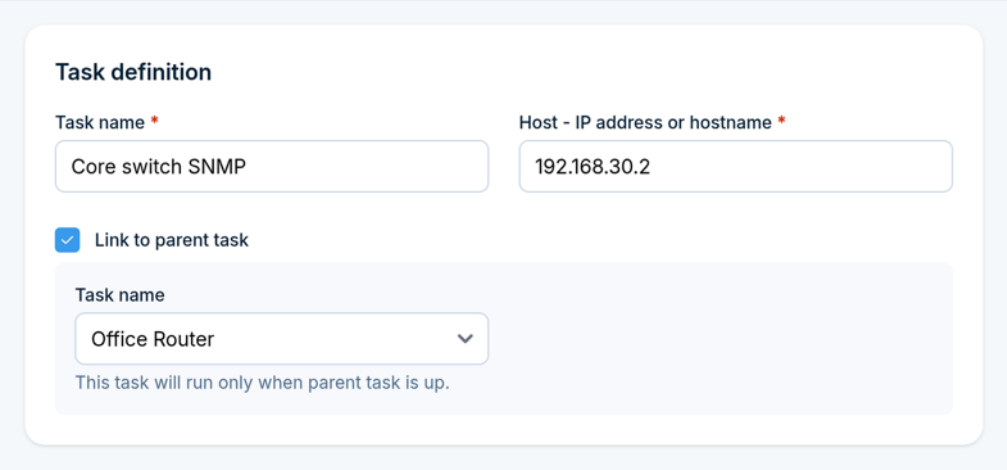
Schritt 3: Eine Aufgabe erstellen

Klicken Sie auf **Neu erstellen** in der oberen rechten Ecke. Das Aufgabenformular öffnet sich als vollständige Seite, unterteilt in fünf Abschnitte.

Aufgabendefinition

Feld	Was eingeben
Aufgabenname	Ein beschreibender Name mit maximal 100 Zeichen, zum Beispiel `Mail server`.
Host – IP-Adresse oder Hostname	Was zu überprüfen ist, zum Beispiel `192.168.1.10` oder `mail.example.com`.
Link zur übergeordneten Aufgabe	Aktivieren Sie dies, um die Aufgabe von einer anderen abhängig zu machen.
Aufgabenname (übergeordnet)	Wird angezeigt, sobald das Kontrollkästchen aktiviert ist: die Aufgabe, von der diese abhängt.

Eine verknüpfte Aufgabe **wird nur ausgeführt, wenn ihre übergeordnete Aufgabe verfügbar ist**. Verwenden Sie dies, um Alert-Fluten zu vermeiden: Falls der Router vor zehn Servern ausfällt, warnt nur die Router-Aufgabe, und die zehn Server-Aufgaben bleiben stumm.



Aufgabendefinition

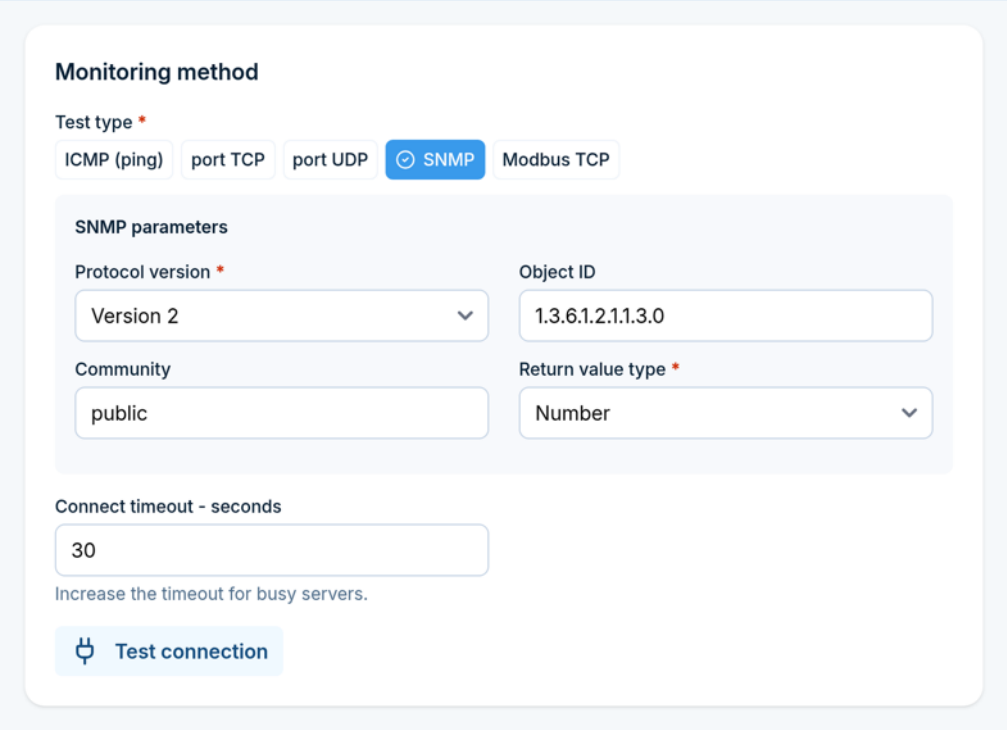
Überwachungsmethode

Wählen Sie den **Testtyp**, und füllen Sie dann die für diesen Typ angezeigten Parameter aus:

Testtyp	Parameter
ICMP (Ping)	**Anzahl der Anforderungen** – wie viele Pings pro Überprüfung zu senden sind.
Port TCP	**Port** – der TCP-Port, der eine Verbindung akzeptieren muss.
Port UDP	**Port** – der zu überprüfende UDP-Port.
SNMP	**Protokollversion** (1 oder 2), **Object ID**, **Community**, **Rückgabewerttyp** (Zahl 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.

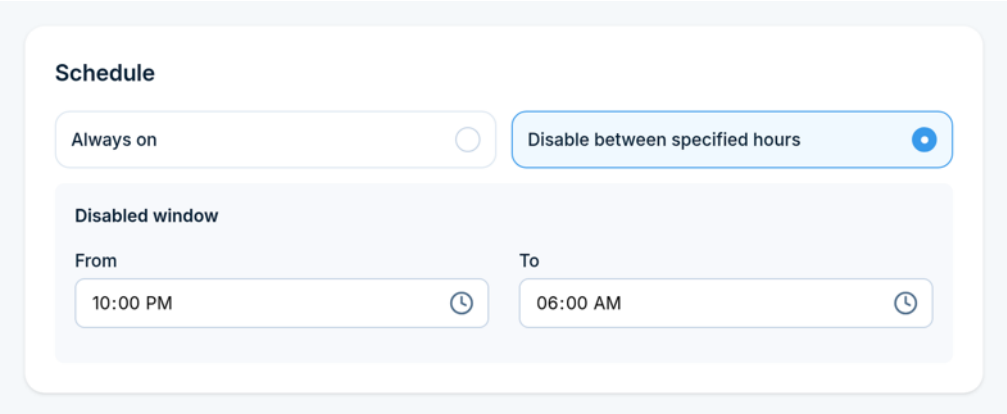
Click **Test connection** to try the check straight away. The result appears next to the button, so you can confirm the host answers before you save the task.



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

Warnauslöser

First choose who gets the alert:

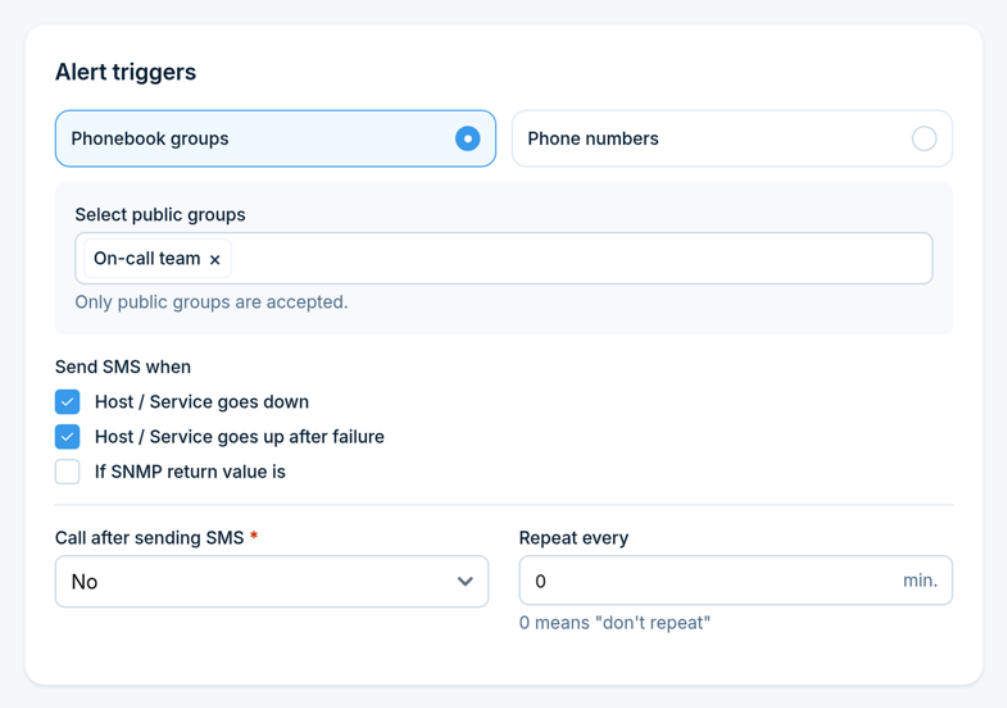
Option	Was eingeben
Phonebook groups	Select public groups. Only public groups are accepted.
Phone numbers	Type the numbers directly, separated by commas. Maximum 100 characters in total.

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.



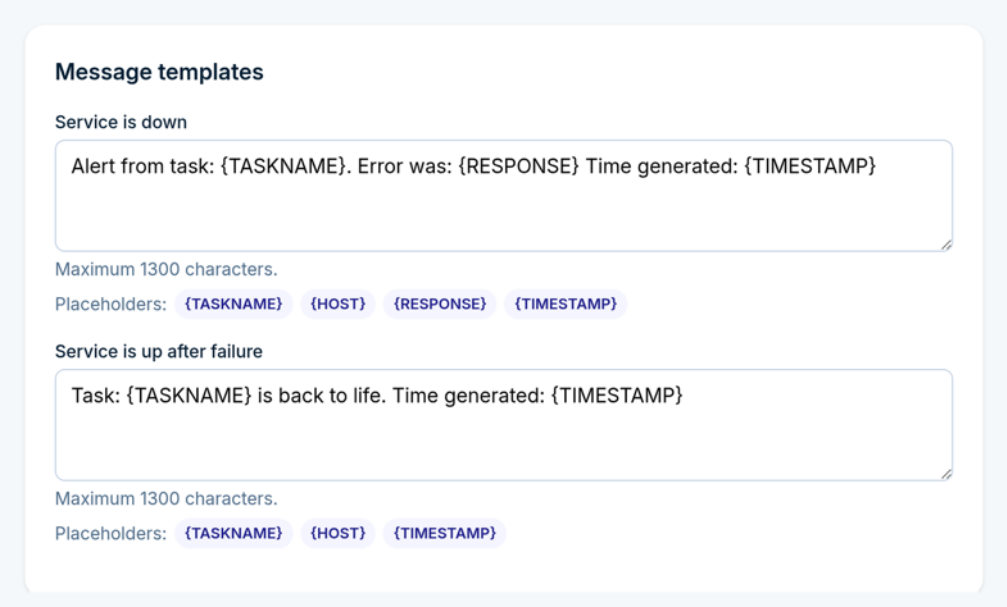
Warnauslöser

Nachrichtenvorlagen

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

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

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



Nachrichtenvorlagen

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

Teil 2: Reports

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

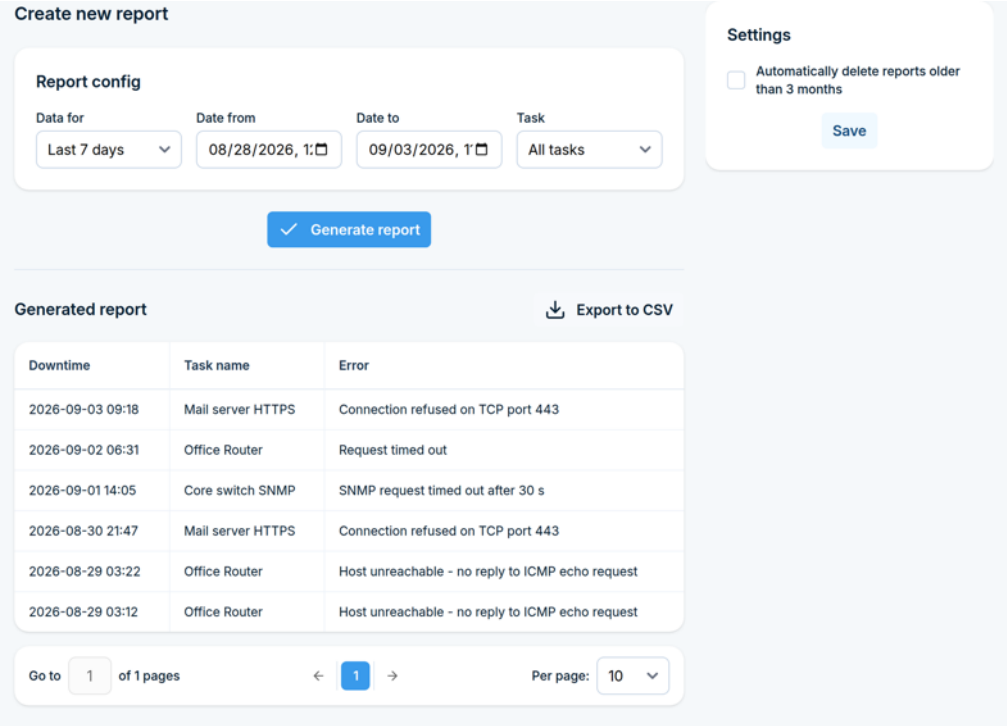
Bericht generieren

Wählen Sie im Feld **Report config** aus:

Feld	Funktion
Data for	Ein vordefinierter Datumsbereich. Wenn Sie einen auswählen, werden die Daten unten eingefüllt.
Date from / **Date to**	Der genaue Bereich. Diese Felder zu bearbeiten schaltet **Data for** auf einen benutzerdefinierten Bereich um.
Task	Eine einzelne Aufgabe oder **All tasks**.

Klicken Sie auf **Generate report**. Die Ergebnisse werden unten angezeigt und listen für jeden Incident die Ausfallzeit, den Aufgabennamen und den aufgezeichneten Fehler auf.

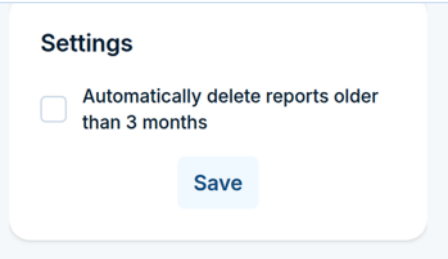
Klicken Sie auf **Export to CSV** über den Ergebnissen, um diese herunterzuladen.



Generierter Bericht

Report-Aufbewahrung

Das Kästchen auf der rechten Seite enthält eine Option: **Automatically delete reports older than 3 months**. Schalten Sie diese ein, um zu verhindern, dass der Report-Verlauf unbegrenzt wächst, und klicken Sie dann auf **Save**.



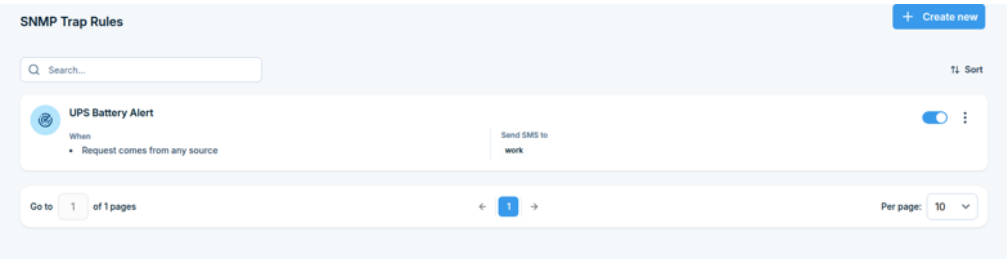
Report-Aufbewahrung

Teil 3: SNMP Traps

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

Schritt 1: Öffnen Sie die Seite SNMP Traps

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



SNMP Trap Rules

Schritt 2: Erstellen Sie eine Regel

Klicken Sie auf **Neue erstellen** in der oberen rechten Ecke. Ein Seitenpanel wird geöffnet.

Benennen Sie die Regel

Geben Sie unter **Rule name** einen aussagekräftigen Namen ein, z. B. `UPS battery trap`. Maximal 100 Zeichen.

Entscheiden Sie, welche Traps bearbeitet werden sollen

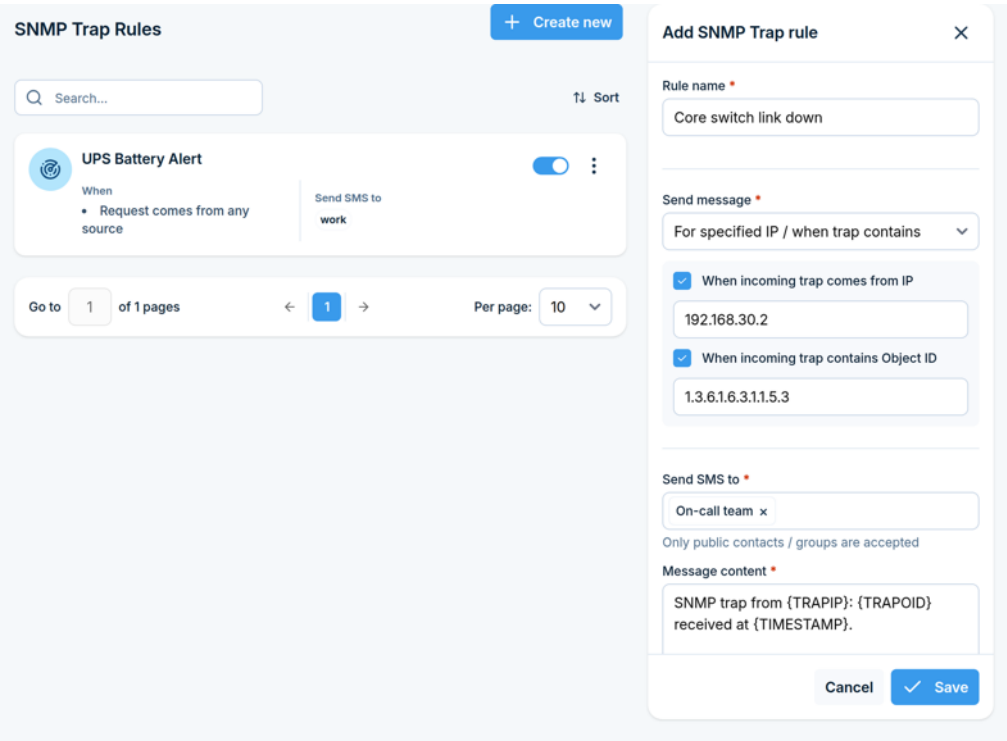
Wählen Sie **Send message**:

Option	Was es bedeutet
Always send	Jeder Trap, den das Gerät empfängt, löst diese Regel aus.
For specified IP / when trap contains	Nur Traps, die den folgenden Bedingungen entsprechen, lösen sie aus.

Wenn Sie die zweite Option gewählt haben, sind zwei Bedingungen verfügbar. Sie können eine oder beide verwenden, und ein Trap muss jede aktivierte Bedingung erfüllen.

When incoming trap comes from IP Aktivieren Sie dies und geben Sie die IP-Adresse des sendenden Geräts ein.

When incoming trap contains Object ID Aktivieren Sie dies und geben Sie die OID ein, die im Trap vorhanden sein muss.



Eine SNMP-Trap-Regel mit Bedingungen

Wählen Sie die Empfänger und schreiben Sie die Nachricht

Send SMS to – Wählen Sie Kontakte oder Gruppen aus. Nur **öffentliche** Kontakte und Gruppen werden akzeptiert.

Message content – Der zu sendende Text, maximal 1300 Zeichen. Sie können diese Platzhalter verwenden:

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

Optionale Einstellungen

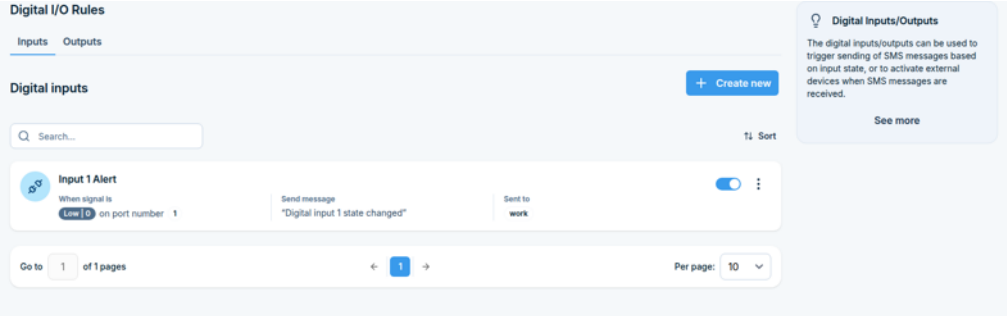
- **Modem** (nur Multi-Modem-Geräte) – Senden über eine bestimmte SIM-Karte statt über die Standard-SIM.
- **Call after sending SMS** – Auch einen Sprachanruf durchführen, mit denselben Optionen wie in Aufgaben.

Klicken Sie auf **Save**. Die Regel gilt für Traps, die ab sofort empfangen werden.

Verhalten der Netzwerküberwachung

- Tasks werden im gemeinsamen **Monitoring period** überprüft, daher kann eine Task nicht schneller als dieses Intervall warnen.
- Eine „down"-Warnung wird einmal gesendet, wenn sich der Status ändert, und dann nur wiederholt, wenn Sie **Repeat every** einstellen.
- Eine Task, die mit einer übergeordneten Task verknüpft ist, wird vollständig übersprungen, während die übergeordnete Task nicht verfügbar ist, daher bleiben ihre eigenen Warnungen stumm, bis die übergeordnete Task wiederhergestellt ist.
- Wenn mehrere SNMP-Trap-Regeln denselben Trap erfassen, sendet **jede** von ihnen ihre eigene SMS.

Digitale Ein-/Ausgabe



Übersicht über digitale Ein-/Ausgabe

Funktion dieser Funktion

Die digitalen Ein- und Ausgänge sind der physische Anschluss auf dem Gerät, der es SMSEagle ermöglicht, mit der Welt außerhalb des Netzwerks zu kommunizieren:

Richtung	Funktion
Input	Eine Spannungsänderung an einem Eingangsport (ein Türkontakt schließt sich, ein Alarmrelais wird ausgelöst, eine USV meldet einen Fehler) veranlasst das Gerät, eine SMS zu senden.
Output	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 **rules**. Eine Input-Regel besagt „wenn Port 2 High wird, texte das Wartungsteam". Eine Output-Regel besagt „wenn eine SMS mit OPEN ankommt, stelle Port 1 für 5 Sekunden auf 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 über 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 Portlisten in den Regelformularen werden aus Ihrem Gerätemodell erstellt, daher bieten sie nur Ports an, die physisch vorhanden sind.
- Das Gerät muss SMS senden können. Überprüfen Sie, dass mindestens ein Modem verbunden und im Netz registriert ist.
- Empfänger von Input-Regeln müssen im Phonebook als **Public** 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)**

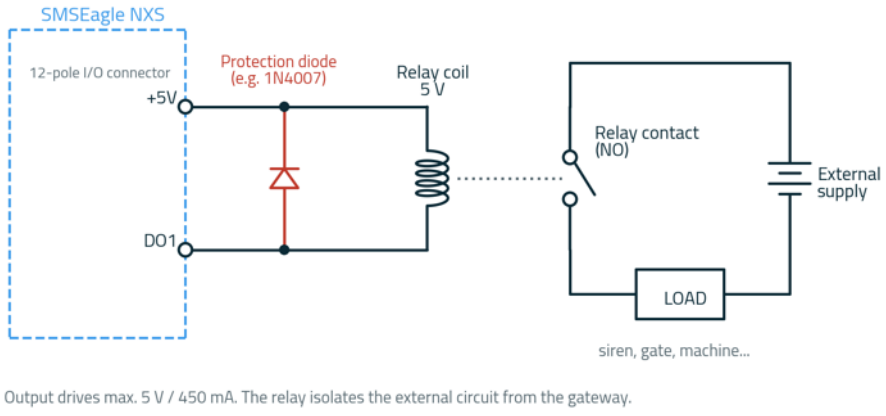
> **Prefer NC contacts for alarm circuits.** With an NC contact, a cut or disconnected cable opens the circuit in the same way as a real alarm, so a wiring fault also triggers an SMS. With an NO contact, a broken cable goes unnoticed.

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.

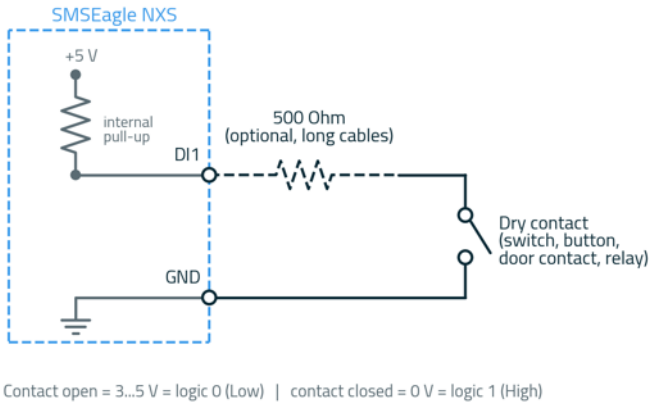
Using digital inputs

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)

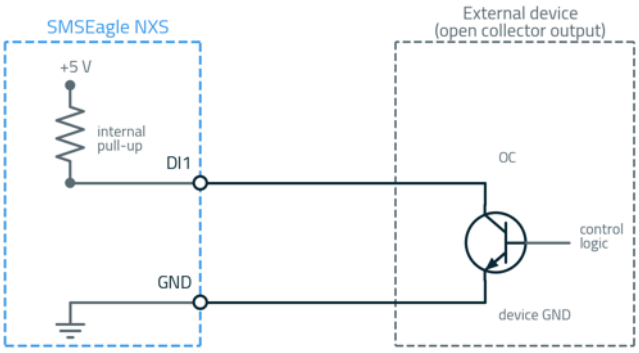
Connect a potential-free (dry) contact between the input and GND: a switch, push button, door or window contact, PIR detector output, alarm panel output or relay contact. Both **NO** (normally open) and **NC** (normally closed) contacts can be used; set **When input signal** according to the table in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

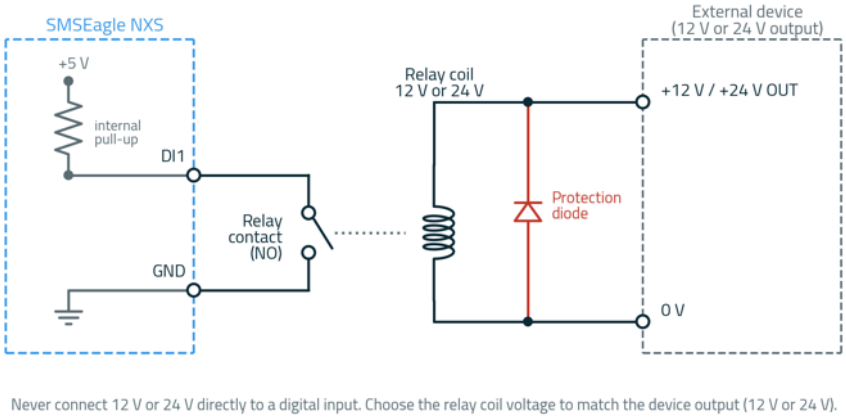


Digital input: connection with a device with an open collector output

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)**.

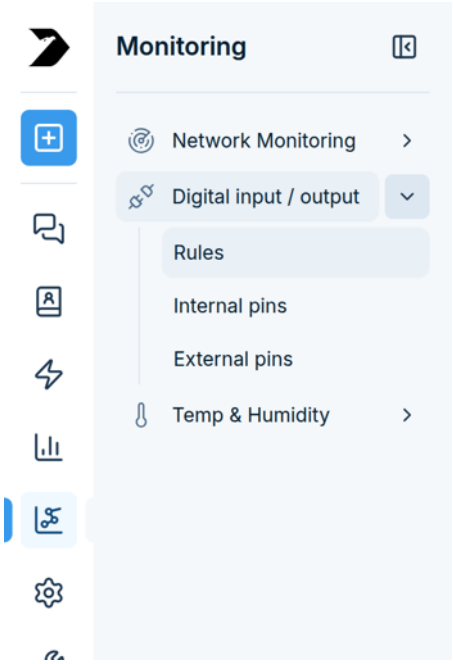


Digital input: connection with a device with a 12 V or 24 V output

Wo man es findet

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

Seite	Wofür es gedacht ist
Rules	Erstellen Sie die Input- und Output-Regeln. Hier verbringen Sie die meiste Zeit.
Internal pins	Sehen Sie den Live-Status der integrierten Ports und aktivieren oder deaktivieren Sie den Service.
External pins	Definieren und steuern Sie zusätzliche Ports, die von einem io-bridge-Modul bereitgestellt werden.

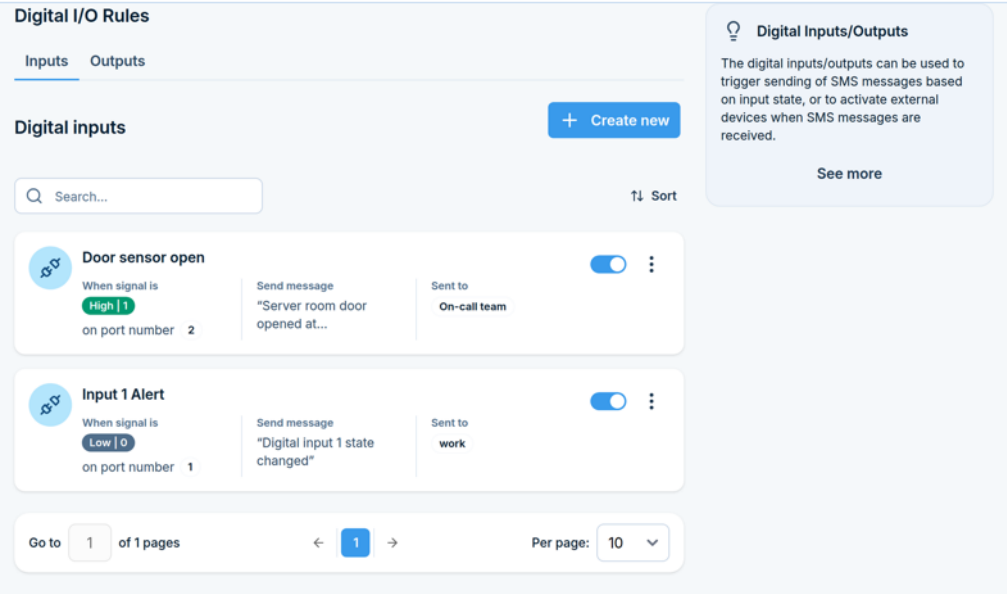


Wo Sie die Digital I/O-Seiten finden

Teil 1: Eingaberegeln (Eingangssignal in SMS)

Schritt 1: Öffnen Sie die Regelseite

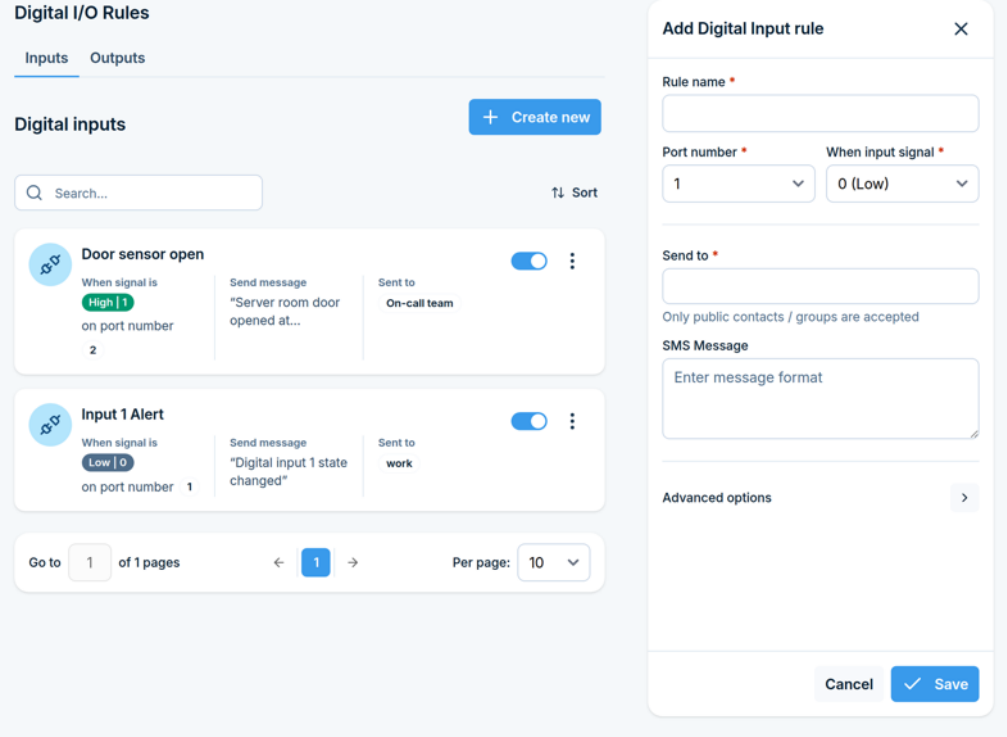
Gehen Sie zu **Monitoring > Digital input / output > Rules** und stellen Sie sicher, dass die Registerkarte **Inputs** ausgewählt ist.



Digitale Eingaberegeln

Schritt 2: Erstellen Sie eine Eingaberegel

Klicken Sie auf **Neue erstellen** in der oberen rechten Ecke. Ein Seitenpanel wird geöffnet.



Eine neue digitale Eingaberegel

Benennen Sie die Regel

Geben Sie im Feld **Rule name** etwas Aussagekräftiges ein, z. B. `Server room door opened`. Maximal 100 Zeichen.

Wählen Sie den Port und das Signal

Feld	Was eingeben
Port number	Der Eingangsport, an den die Ausrüstung verkabelt ist. Externe (io-bridge) Ports erscheinen in der Liste mit der Markierung `(Ext)`.
When input signal	`0 (Low)` oder `1 (High)`. Dies ist der Zustand, der die Regel auslöst.

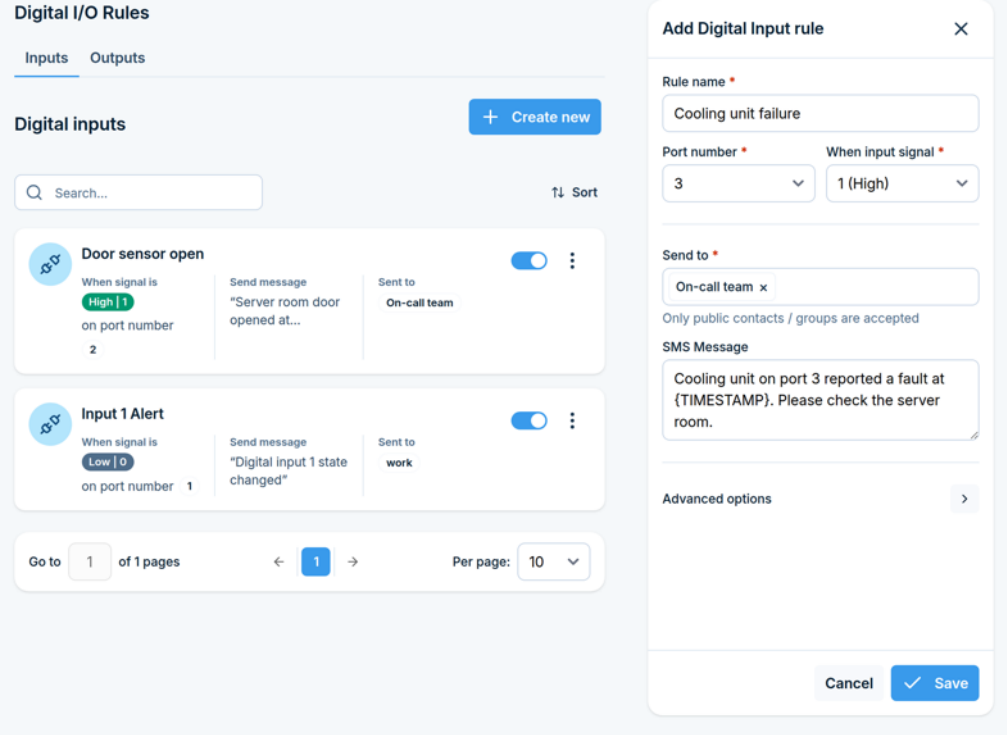
Pick the value that represents the alarm condition on your equipment. A **NO** (normally open) contact that closes on alarm needs **1 (High)**; a **NC** (normally closed) contact that opens on alarm needs **0 (Low)**. See NO and NC contacts for details.

Wählen Sie die Empfänger

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

Schreiben Sie den SMS-Text

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

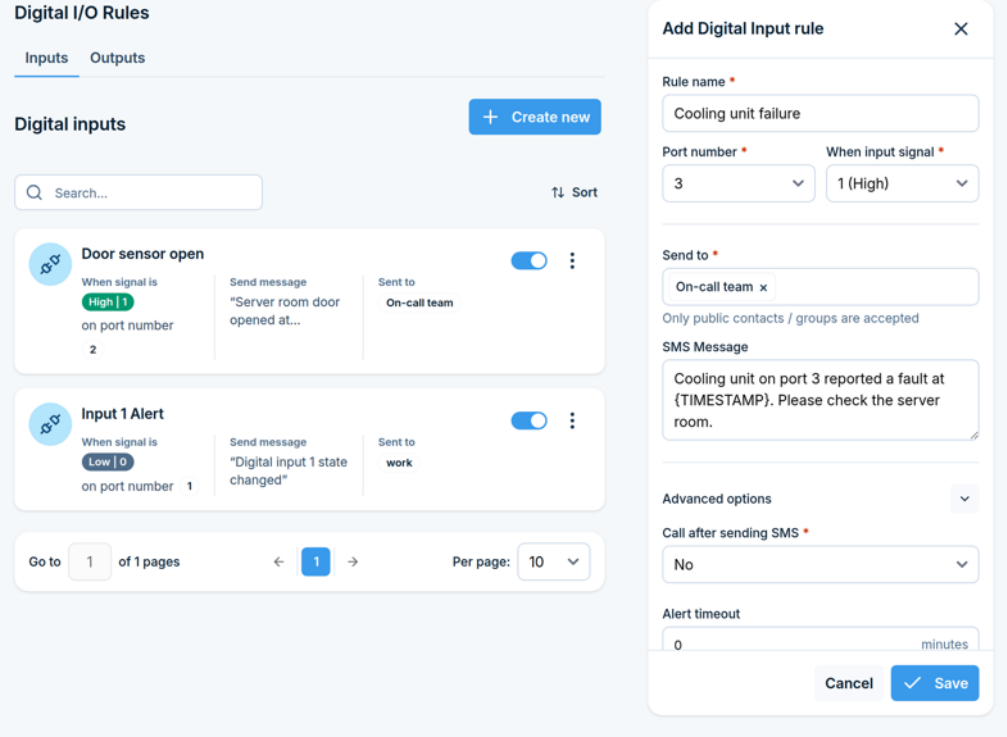


Eine abgeschlossene Eingaberegel

Erweiterte Optionen

Klicken Sie auf **Advanced options**, um diesen Abschnitt zu erweitern. Sie brauchen ihn für ein einfaches Setup nicht.

- **Call after sending SMS** – platzieren Sie auch einen Sprachanruf an dieselben Empfänger. Optionen sind **No**, **Ring**, **Text-to-speech (TTS)** und **Text-to-speech (advanced)**, je nachdem, was Ihr Gerätemodell unterstützt. Mit der erweiterten Option wählen Sie auch ein **Voice model** aus.
- **Alert timeout** – die Anzahl der Minuten, die verstreichen müssen, bevor dieselbe Regel erneut benachrichtigen kann. `0` bedeutet keine Begrenzung, daher sendet jede Signaländerung eine SMS.



Erweiterte Optionen für Eingaberegeln

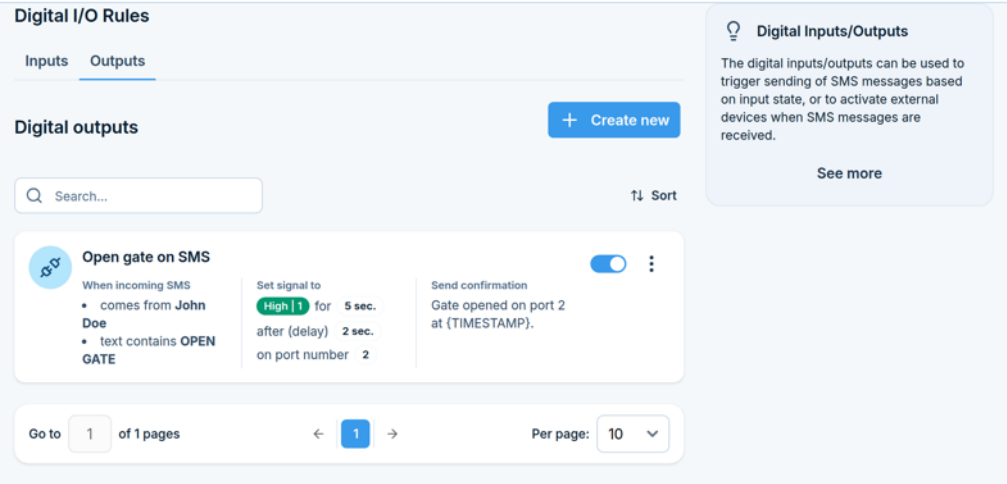
Legen Sie ein Alert-Timeout für verrauschte Eingänge fest. Ein Kontakt, der flattert, oder Ausrüstung, die wiederholt auslöst, kann eine Nachrichtenlawine erzeugen. Ein Timeout von wenigen Minuten reduziert ein echtes Ereignis auf eine SMS.

Klicken Sie auf **Save**. Die Regel beginnt ab sofort mit Signaländerungen zu funktionieren.

Teil 2: Ausgangsregeln (SMS in Ausgangssignal)

Schritt 1: Öffnen Sie die Regelseite

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



Digitale Ausgangsregeln

Schritt 2: Eine Ausgangsregel erstellen

Klicken Sie auf **Neue erstellen** in der oberen rechten Ecke. Ein Seitenpanel wird geöffnet.

Nennen Sie die Regel und wählen Sie den Anschluss

Geben Sie unter **Rule name** einen aussagekräftigen Namen ein, z. B. `Open gate on SMS`. Maximal 100 Zeichen. Wählen Sie unter **Port number** den Ausgangsanschluss, mit dem Ihre Ausrüstung verdrahtet ist. Externe (io-bridge) Anschlüsse werden mit `(Ext)` gekennzeichnet angezeigt.

Entscheiden Sie, welche SMS-Nachrichten die Regel auslösen

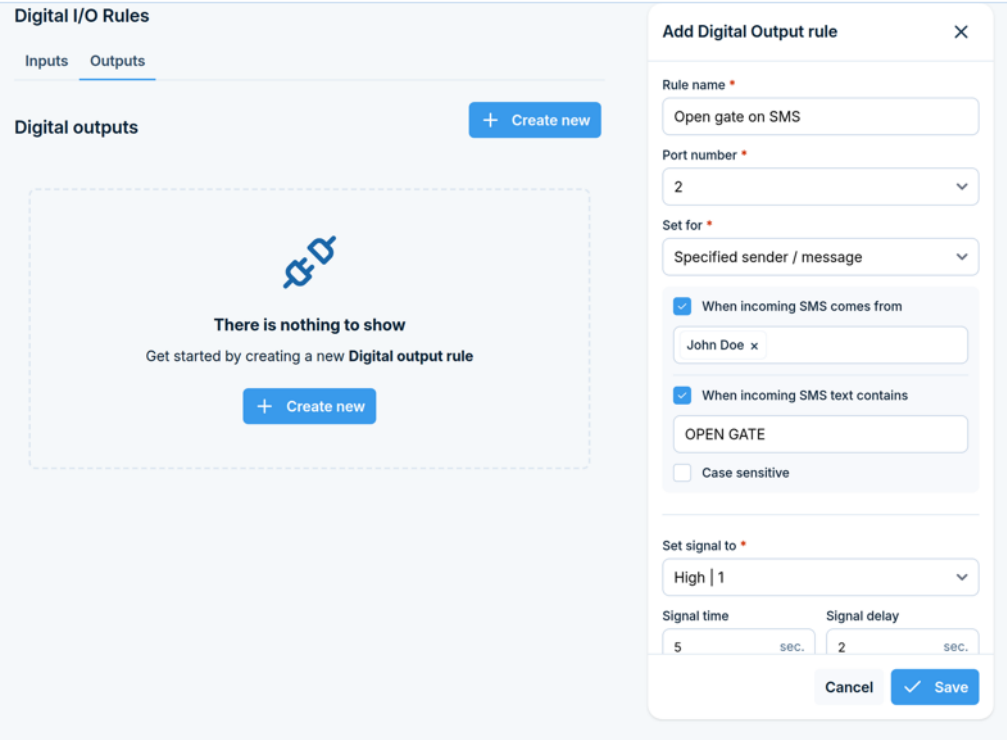
Wählen Sie **Set for**:

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

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** erfüllen.

When incoming SMS comes from Aktivieren Sie dieses Kontrollkästchen und wählen Sie die Absenderkontakte oder Gruppen.

When incoming SMS text contains Aktivieren Sie dieses Kontrollkästchen und geben Sie den Ausdruck unter **Text** ein, z. B. `OPEN`. Aktivieren Sie **Case sensitive**, wenn `open` und `OPEN` unterschiedlich behandelt werden sollen.



Bedingungen für Ausgangsregeln

Beschränken Sie Ausgangsregeln nach Absender. Eine Ausgangsregel schaltet physische Ausrüstung. Ohne Absenderbedingung kann jeder, der Ihre Nummer kennt, diese bedienen.

Entscheiden Sie, was der Ausgang tut

Feld	Was es bedeutet
Set signal to	`Low` | `0` oder `High` | `1`. Der Status, in den der Anschluss geschaltet wird.
Signal time	Wie viele Sekunden der Anschluss in diesem Status verbleibt, bevor er zurückkehrt. `0` bedeutet, dass er auf unbestimmte Zeit in diesem Status verbleibt.
Signal delay	Wie viele Sekunden nach dem Eintreffen der SMS gewartet werden soll, bevor der Anschluss geschaltet wird.

Erweiterte Optionen

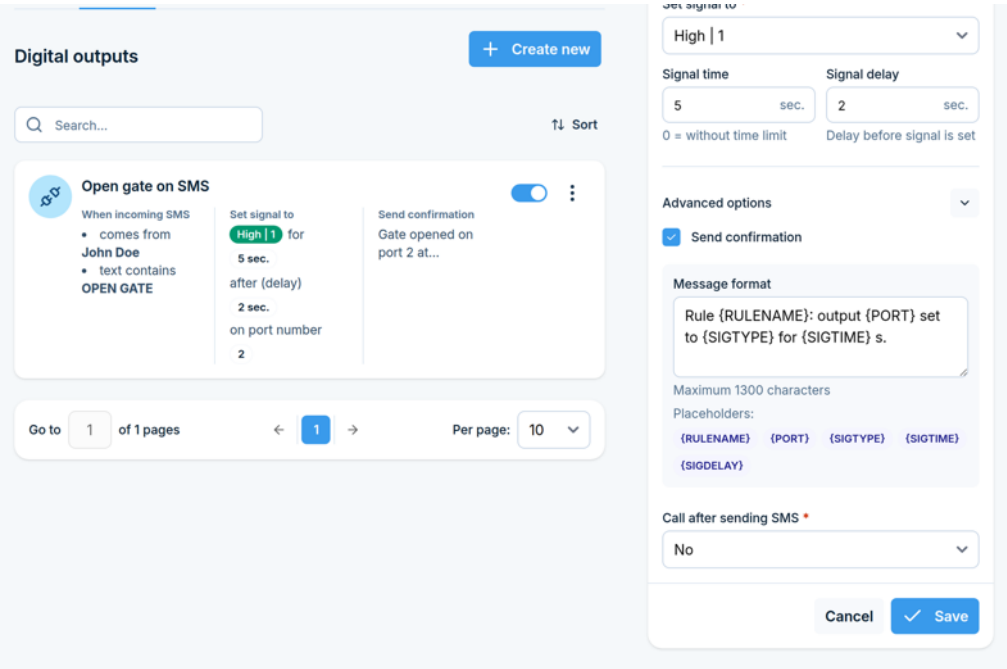
Klicken Sie auf **Advanced options**, um diesen Abschnitt zu erweitern.

Send confirmation Aktivieren Sie dieses Kontrollkästchen, um nach dem Schalten des Ausgangs eine SMS an den Absender zurückzusenden. Das Feld **Message format** wird angezeigt, maximal 1300 Zeichen. Sie können den Text aus Platzhaltern erstellen:

Platzhalter	Ersetzt durch
`{RULENAME}`	Der Name der ausgelösten Regel
`{PORT}`	Die Ausgabeportnummer
`{SIGTYPE}`	Das Signal, auf das der Port 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 Input-Regeln beschrieben.



Bestätigungsmeldung der Ausgaberegel

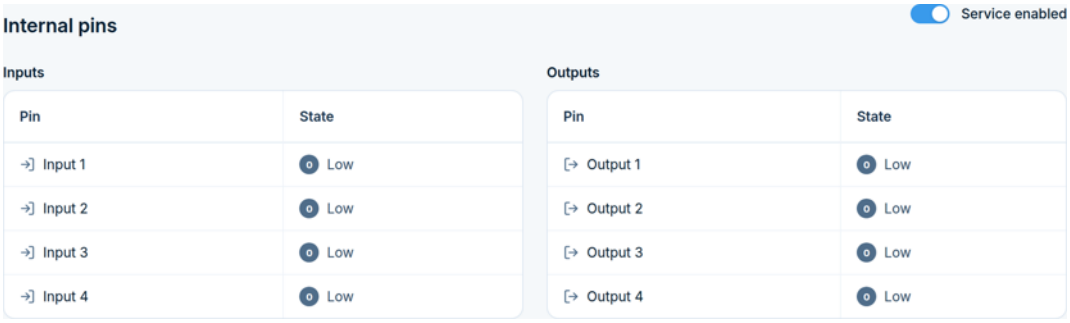
Klicken Sie auf **Save**. Die Regel beginnt, auf ab sofort empfangene Nachrichten zu reagieren.

Teil 3: Interne Pins

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

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

Oben auf der Seite befindet sich ein Schalter **Service enabled**. Er startet und stoppt den Service, der die integrierten Ports ausliest und ansteuert. **Wenn er ausgeschaltet ist, funktionieren Input- und Output-Regeln auf internen Ports nicht.**



Interne Pins mit laufendem Service. Jeder Port hier zeigt `0` Low an, weil nichts daran angeschlossen ist

---

Teil 4: Externe Pins

Externe Pins sind zusätzliche Ports, die von einem an das Gerät angeschlossenen io-bridge-Modul bereitgestellt werden.

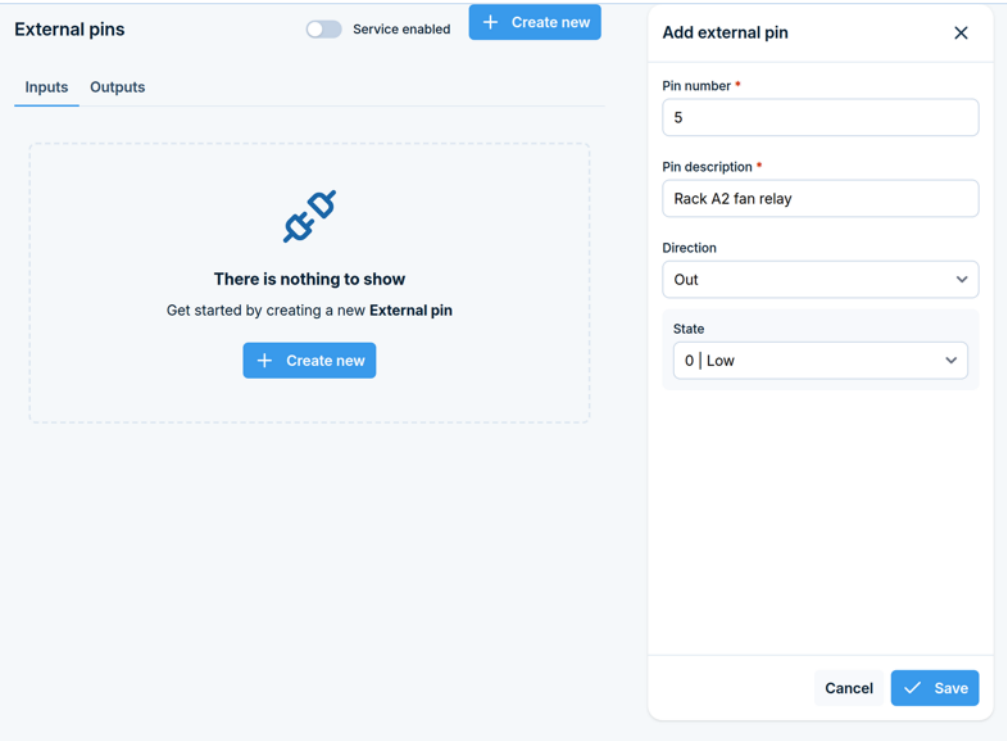
Gehen Sie zu **Monitoring > Digital input / output > External pins**. Die Seite hat eine Registerkarte **Inputs** und eine Registerkarte **Outputs** sowie einen Schalter **Service enabled**, der den io-bridge-Service startet und stoppt.

Externen Pin hinzufügen

Klicken Sie auf **Create new**. Ein Seitenpanel wird geöffnet.

Feld	Was eingeben
Pin number	Die Portnummer auf dem io-bridge-Modul, beispielsweise `1`. Jede Nummer kann nur einmal konfiguriert werden.
Pin description	Ein Kurzname mit maximal 64 Zeichen. Es sind nur Buchstaben, Ziffern und Leerzeichen zulässig.
Direction	**In** für einen Port, den Sie auslesen, **Out** für einen Port, den Sie ansteuern.
Status	Nur für **Out**-Pins angezeigt: der Zustand, in dem der Port startet, `1 | High` oder `0 | Low`.

Klicken Sie auf **Save**.



Einen externen Pin hinzufügen

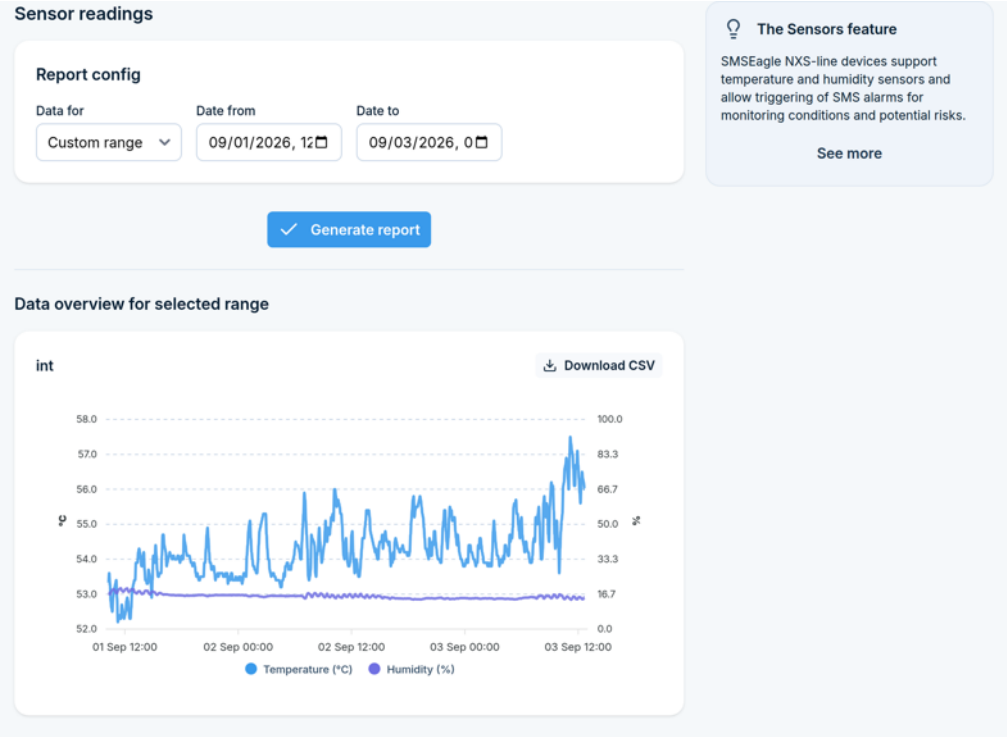
Die Pins verwenden

- 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.
- Nach der Definition werden externe Pins auch in den Listen **Port number** von Input- und Output-Regeln angezeigt, gekennzeichnet mit `(Ext)`, sodass Regeln sie genau wie integrierte Ports verwenden können.

So verhalten sich Digital-I/O-Regeln

- 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 pausieren, ohne sie zu löschen.
- Wenn mehrere Regeln auf dasselbe Ereignis zutreffen, wird **jede** ausgeführt, sodass ein Eingangssignal mehrere Nachrichten senden und eine SMS mehrere Ports umschalten kann.
- Die Textbedingung für Output-Regeln ist eine **contains**-Übereinstimmung, keine genaue Übereinstimmung.
- Regeln, die interne Ports verwenden, benötigen den Service **Internal pins**; Regeln, die `(Ext)`-Ports verwenden, benötigen den Service **External pins**.

Temperatur- und Feuchtigkeitssensoren



Übersicht über Temperatur- und Feuchtigkeitssensoren

Funktion dieser Funktion

Geräte der SMSEagle NXS-Serie unterstützen Temperatur- und Feuchtigkeitssensoren, die mit dem Gerät verbunden sind. Sobald ein Sensor angeschlossen ist, liest das Gerät ihn nach einem Zeitplan aus, speichert einen Verlauf der Messwerte und kann eine SMS senden, wenn ein Wert einen von Ihnen definierten Schwellenwert überschreitet.

Die Funktion hat drei Seiten:

Seite	Wofür es gedacht 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 die Häufigkeit ihrer Abfrage.

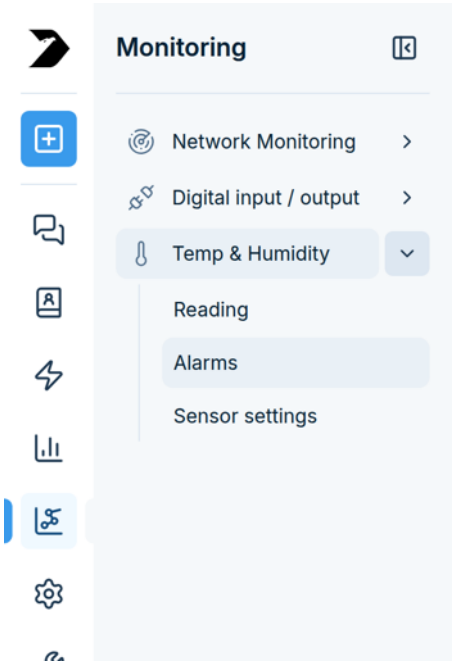
Typische Anwendungen: Überwachung eines Serverraums, einer Kühlanlage oder eines Technikschranks und Benachrichtigung des Bereitschaftspersonals per SMS, wenn es zu warm oder zu feucht wird.

Bevor Sie beginnen

- Verbinden Sie den Sensor mit dem Gerät, 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 Adressbuch als **Public** markiert sein.

Wo man es findet

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



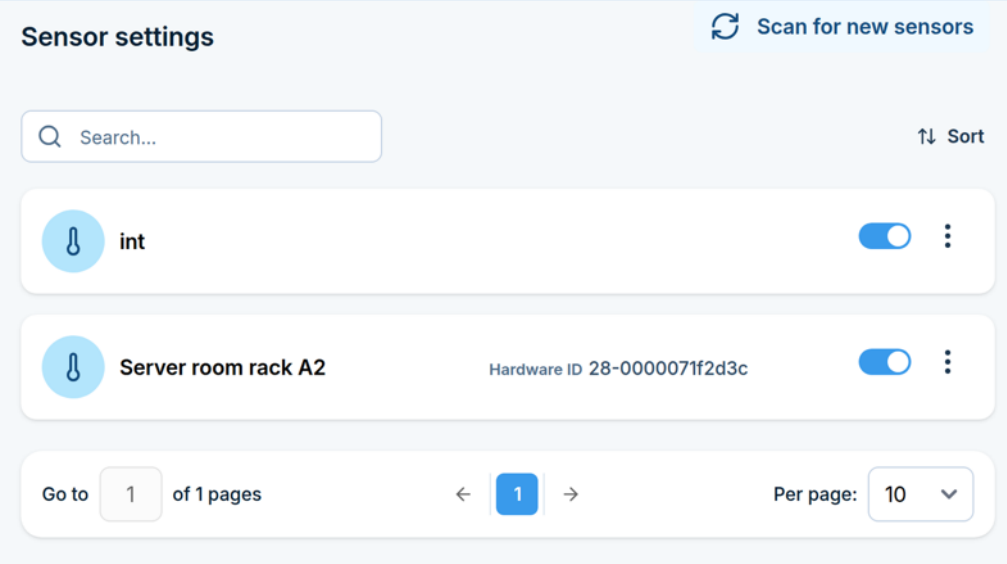
Wo sich die Sensorseiten befinden

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 hinzu, was es findet. Die Seite zeigt entweder an, dass neue Sensoren hinzugefügt wurden, oder dass keine gefunden wurden.



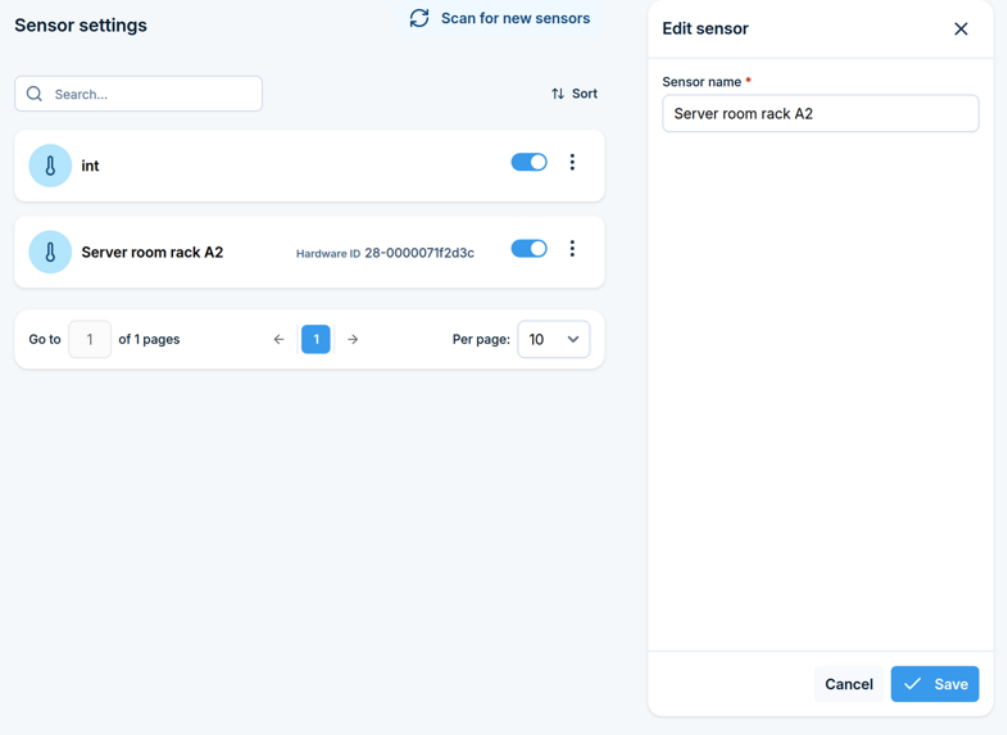
Sensor settings

Jeder Sensor in der Liste zeigt seinen **Sensor name** und seine **Hardware ID**. Die Hardware-ID ist die Art, wie das Gerät den physischen Sensor identifiziert; sie ist nicht bearbeitbar.

Schritt 2: Geben Sie den Sensoren aussagekräftige Namen

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

Dieser Name erscheint in den Diagrammen, in den Alarmregeln und im CSV-Export, daher lohnt es sich, dies zu tun, bevor Sie Regeln erstellen.



Umbenennen eines Sensors

Schritt 3: Verwalten Sie die Liste

Jeder Sensor hat:

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

Sie können auch mehrere Sensoren anwählen und sie gemeinsam aktivieren, deaktivieren oder löschen.

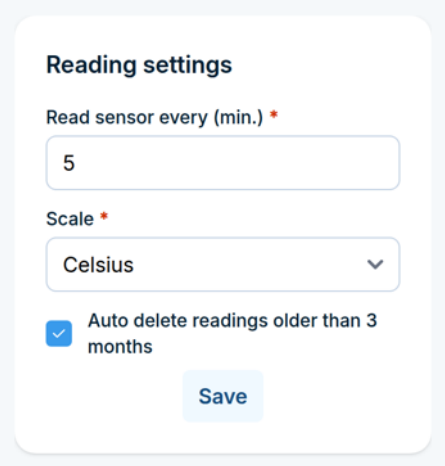
> Der **interne Sensor kann nicht gelöscht werden**. Geräte mit einem eingebauten Sensor behalten ihn immer in der Liste; deaktivieren Sie ihn, wenn Sie seine Messwerte nicht benötigen.

Schritt 4: Stellen Sie die Lesevorgänge-Einstellungen ein

Das Feld **Reading settings** auf der rechten Seite der Sensor settings-Seite steuert, wie die Sensoren gelesen werden. Diese Einstellungen sind **global**, sie gelten für jeden Sensor:

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

Klicken Sie auf **Save**.

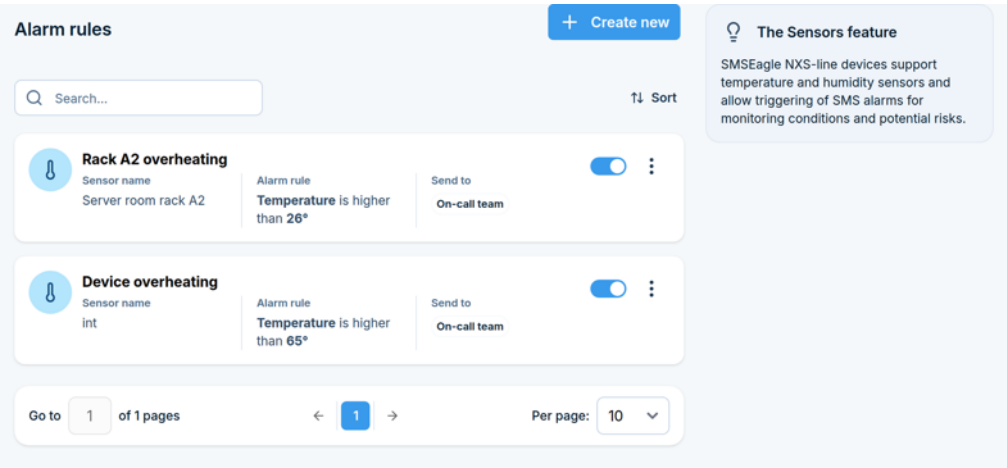


Reading settings

Teil 2: Alarmregeln

Schritt 1: Öffnen Sie die Seite „Alarms“

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



Alarmregeln

Schritt 2: Erstellen Sie eine Regel

Klicken Sie auf **Neue erstellen** in der oberen rechten Ecke. Ein Seitenpanel wird geöffnet.

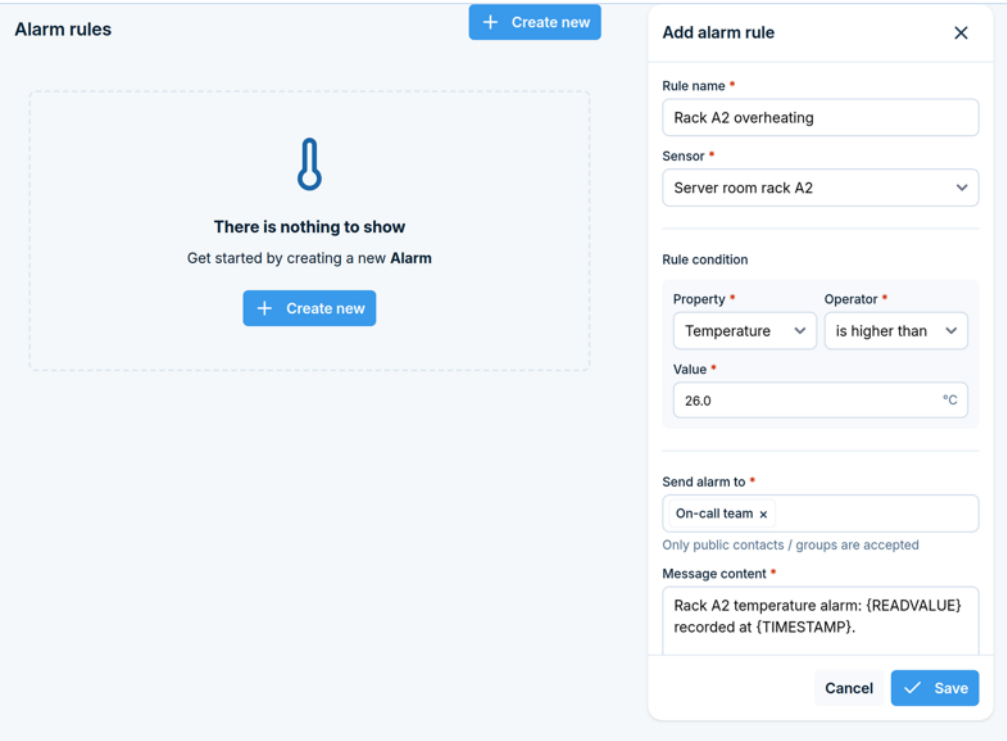
Benennen Sie die Regel

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

Definieren Sie die Bedingung

Feld	Was zu wählen ist
Sensor	Welcher Sensor von der Regel überwacht wird.
Property	**Temperature** oder **Humidity**.
Operator	**is higher than** oder **is lower than**.
Value	Der Schwellenwert mit einer Dezimalstelle, zum Beispiel `27.5`.

Der Temperaturschwellenwert wird in der **Scale** gelesen, die Sie in den Leseeinstellungen festlegen. Eine für Celsius geschriebene Regel 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

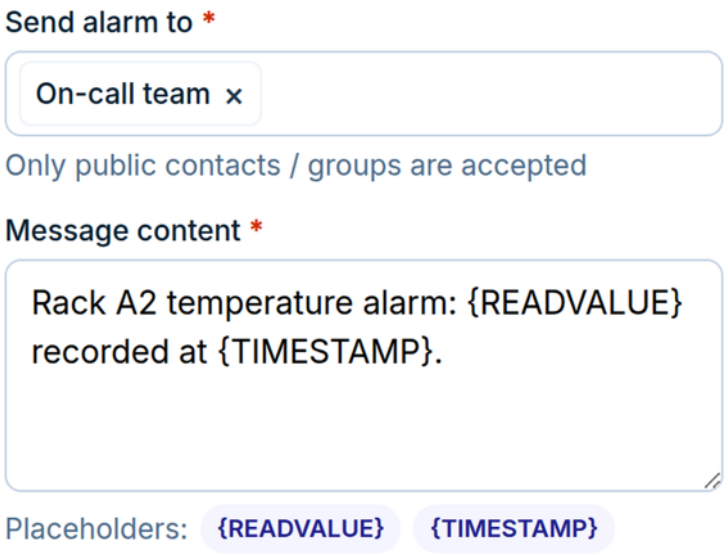
Wählen Sie unter **Send alarm to** die Kontakte oder Gruppen aus. Nur **public** Kontakte und Gruppen können hier ausgewählt werden. Dieses Feld ist erforderlich.

Schreiben Sie die Nachricht

Message content ist die SMS, die gesendet wird, Maximum 2000 Zeichen. Sie können sie aus Platzhaltern zusammenstellen:

Platzhalter	Ersetzt durch
`{READVALUE}`	Der Wert, der den Alarm ausgelöst hat
`{TIMESTAMP}`	Zeitpunkt der Messung

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



Die Badges unter dem Feld fügen an der Cursor-Position einen Platzhalter ein

Klicken Sie auf **Save**. Die Regel wird von nun an bei jeder Ablesung überprüft.

Teil 3: Messwerte und Berichte

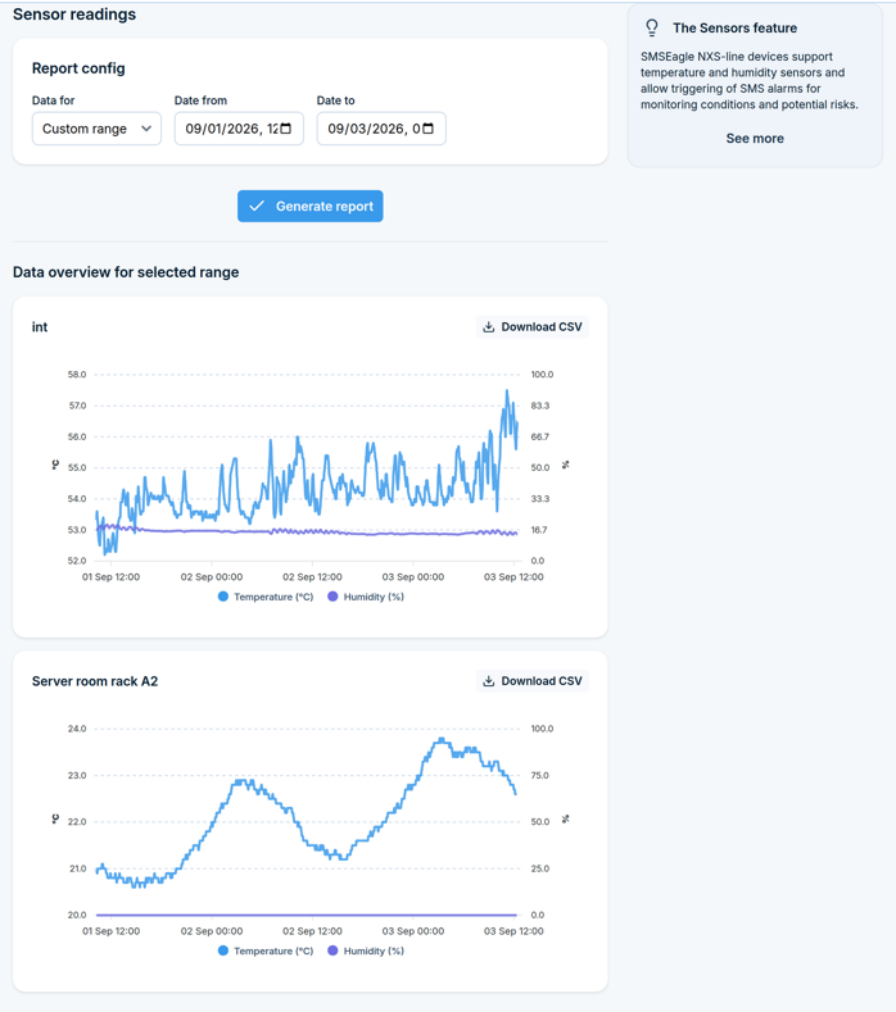
Gehen Sie zu **Monitoring > Temp & Humidity > Reading**.

Wählen Sie im Feld **Report config** aus:

Feld	Funktion
Data for	Ein vordefinierter Datumsbereich. Wenn Sie einen auswählen, werden die Daten unten eingefüllt.
Date from / **Date to**	Der genaue Bereich. Diese Felder zu bearbeiten schaltet **Data for** auf einen benutzerdefinierten Bereich um.

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

Jedes Diagramm hat einen **Download CSV**-Button, der die Messwerte dieses Sensors für den ausgewählten Zeitraum exportiert.



Sensor readings

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

Verhalten

- Alarme werden ausgewertet, wenn ein Messwert erfasst wird. Die Reaktionszeit hängt daher von **Read sensor every** ab. Ein 15-Minuten-Intervall bedeutet, dass ein Alarm bis zu 15 Minuten später erfolgen kann.
- Ein deaktivierter Sensor wird überhaupt nicht ausgelesen, sodass Alarmregeln, die auf ihn verweisen, stumm bleiben.
- Wenn mehrere Regeln denselben Messwert erfüllen, sendet **jede** von ihnen ihre eigene SMS.

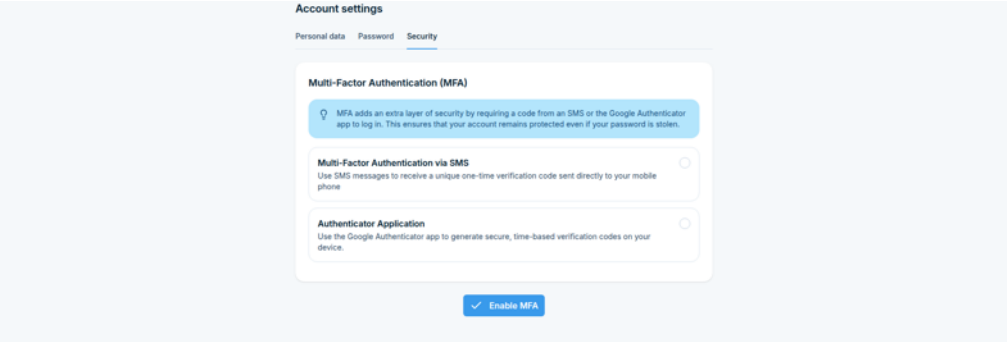
Einstellungen

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

Kontoeinstellungen

Klicken Sie auf Ihren Avatar (unten links) und wählen Sie **Kontoeinstellungen**, um Ihr Konto zu verwalten. Dies erfolgt über drei Reiter: **Persönliche Daten** (Name, Anmeldung, Telefonnummer, Oberflächensprache, Standardeinstellungen für Entwürfe, Benachrichtigungston), **Passwort** und **Sicherheit** – siehe Web Interface Overview für das komplette Reiter-Layout.

Konfiguration der Multi-Faktor-Authentifizierung (MFA)



MFA-Setup unter Kontoeinstellungen > Sicherheit

MFA bietet eine zusätzliche Sicherheitsebene, indem es neben dem Passwort auch einen einmaligen Code zur Anmeldung erfordert. Dies schützt das Konto auch dann, wenn das Passwort gestohlen wird.

Wo zu finden

- **Pro Benutzer**: **Kontoeinstellungen > Sicherheit** (`/settings/account/security`), für Ihr eigenes Konto.
- **Geräteübergreifend**: die Option **Zwei-Faktor-Authentifizierung** im Schritt „Administrator

Schritt 1: Wählen Sie eine MFA-Methode

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

- **Multi-Faktor-Authentifizierung per SMS** – ein einmaliger Bestätigungscode wird bei jeder Anmeldung 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 Anweisungen auf dem Bildschirm, um die gewählte Methode zu bestätigen.

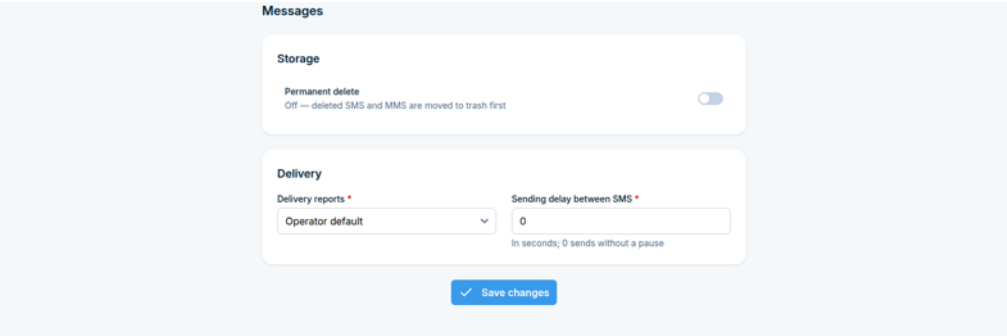
Schritt 2: Erzwingen Sie MFA geräteübergreifend (optional)

Ein Administrator kann MFA für jedes Konto obligatorisch machen, anstatt es pro Benutzer optional zu lassen. Im Einrichtungsassistenten unter **Administrator** (oder pro Benutzer unter **System > Benutzer**) setzen Sie **Zwei-Faktor-Authentifizierung** auf:

- **Nicht erzwingen** – jeder Benutzer entscheidet einzeln, ob er MFA aktivieren möchte.
- **Für alle Benutzer erzwingen** – jeder vorhandene und neue Benutzer muss MFA einrichten.
- **Für neue Benutzer erzwingen** – MFA ist nur für ab jetzt erstellte Konten erforderlich.

SMS / MMS

Nachrichten



Nachrichteneinstellungen unter SMS / MMS

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

Speicherung

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

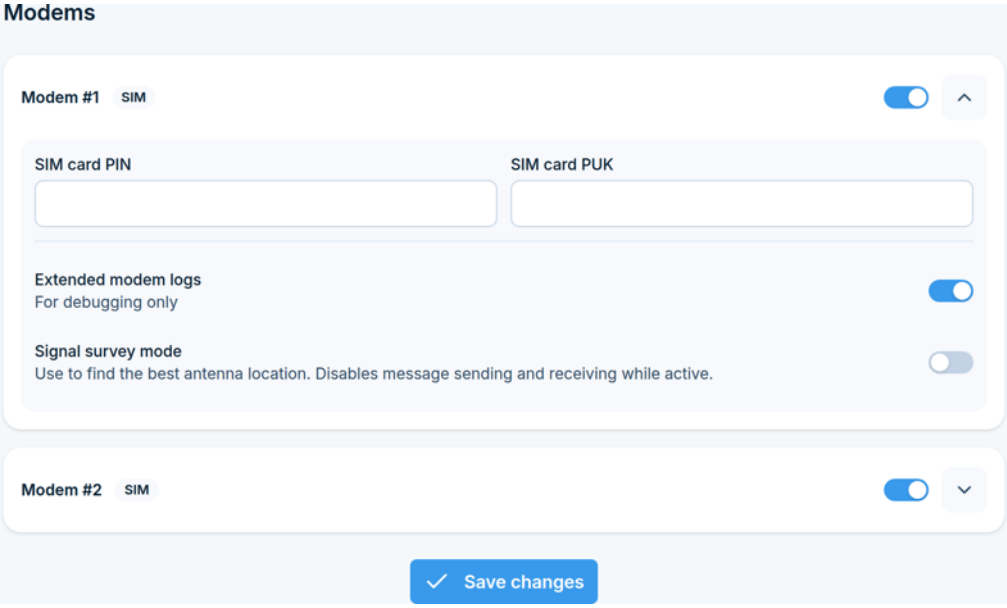
Versand

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

- **Lieferberichte** - Standard des Betreibers (verwenden Sie das Standardverhalten Ihres Mobilfunkbetreibers), Immer anfordern oder Niemals anfordern. Wird auch im Konfigurationsassistenten angeboten.
- **Sendeverzögerung zwischen SMS** - eine Pause in Sekunden zwischen aufeinanderfolgenden ausgehenden SMS. `0` sendet ohne Pause.

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

Modems



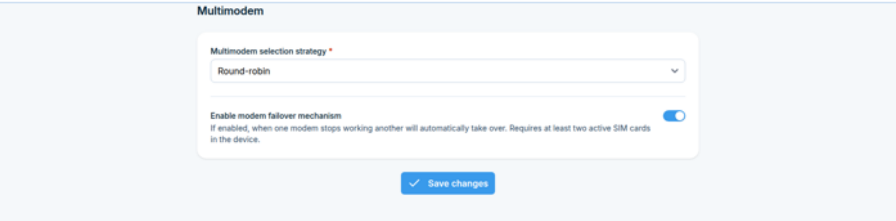
Modemeinstellungen mit erweitertem Abschnitt des ersten Modems

Einstellungen > SMS / MMS > Modems (`/settings/sms-mms/modems/`) listet jedes integrierte Modem (Modem #1, Modem #2 auf Multi-Modem-Geräten) mit einem Schalter zum Aktivieren seiner SIM auf. Durch Erweitern des Modemabschnitts werden vier Einstellungen angezeigt:

- **SIM-Kartenstift** und **SIM-Kartenstift-PUK** - nur erforderlich, wenn die Karte danach fragt. Dieselben zwei Felder werden auch im Konfigurationsassistenten angeboten.
- **Erweiterte Modemprotokolle** - ausführliches Modemlogging, nur zum Debuggen.
- **Vermessungsmodus Signal** - verwenden Sie ihn, um den besten Antennenstandort zu finden. Er **deaktiviert das Versenden und Empfangen von Nachrichten** während er aktiv ist. Schalten Sie ihn aus, wenn Sie fertig sind.

Multimodem

Einstellungen > SMS / MMS > Multimodem (`/settings/sms-mms/multimodem/`) bestimmt, welches der beiden integrierten Modems des Geräts jede ausgehende SMS sendet, und ob ein anderes Modem übernimmt, wenn eines nicht mehr funktioniert. Die Seite ist nur für Administratoren verfügbar.

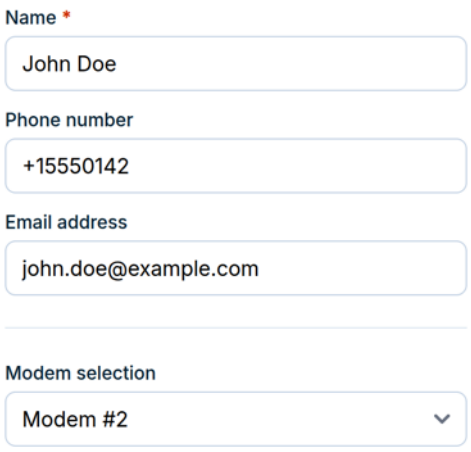


Multimodem-Einstellungen

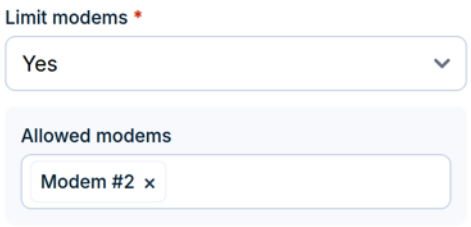
Wie SMSEagle ein Modem auswählt

Die beiden Einstellungen auf dieser Seite sind nur Teil der Entscheidung. Für jede ausgehende SMS prüft SMSEagle diese Regeln der Reihe nach:

1. **Ein für die Nachricht ausgewähltes Modem.** Wenn der Absender ein Modem auswählt, z. B. in Compose, mit dem Modem-Parameter eines API-Aufrufs oder in einer auf ein Modem beschränkten Automationsregel, wird dieses Modem verwendet und nichts Folgendes gilt. Der Absender muss berechtigt sein, es zu verwenden (siehe Regel 3), sonst wird die Nachricht abgelehnt.
2. **Ein an den Kontakt angeheftetes Modem.** Wenn die Nachricht an einen Phonebook-Kontakt geht, dessen **Modem-Auswahl** eingestellt ist, wird dieses Modem verwendet und nichts Folgendes gilt.
3. **Die zulässigen Modems des Absenders. Modems begrenzen** in den Benutzereinstellungen unter **System > Benutzer** beschränkt den Benutzer auf die dort aufgelisteten **zulässigen Modems**. Ohne eine Begrenzung kann der Benutzer jedes Modem verwenden. Modems, deren SIM unter Modems ausgeschaltet ist, werden ausgelassen, es sei denn, es bleiben keine übrig.
4. **Die Auswahlstrategie** wählt eines der zulässigen Modems aus. Siehe Multimodem-Auswahlstrategie unten.
5. **Modem-Failover** wechselt bei Aktivierung das ausgewählte Modem zu dem nächsten funktionierenden Modem, wenn das ausgewählte Modem zu diesem Zeitpunkt nicht funktioniert. Siehe Modem-Failover unten.



Ein an Modem #2 angehefteter Kontakt (Regel 2)



Ein Benutzer, der auf Modem #2 beschränkt ist (Regel 3)

Multimodem-Auswahlstrategie

Multimodem-Auswahlstrategie bietet **Round-robin** und eine **SIM N als Master-Modem**-Option für jedes integrierte Modem (**SIM 1** und **SIM 2**):

- **Round-robin** - die zulässigen Modems des Absenders wechseln sich ab: Modem 1 > Modem 2 > Modem 1 > Modem 2 usw. Jeder Benutzer hat seine eigene Rotation, sodass zwei Benutzer, die gleichzeitig senden, den Turn des anderen nicht beeinflussen.
- **SIM N als Master-Modem** - Modem N sendet jede Nachricht, und die anderen Modems werden nur von Modem-Failover verwendet, wenn Modem N nicht funktioniert. Ein Benutzer, der Modem N nicht verwenden darf, kann mit dieser Strategie keine Nachrichten senden, außer Nachrichten mit einem für sie ausgewählten Modem (Regel 1) oder an einen an ein Modem angehefteten Kontakt (Regel 2). Seine Nachrichten werden mit einem Fehler „fehlender Modem-Zugriff

Modem-Failover

Aktivieren Sie **Modem-Failover-Mechanismus aktivieren**, damit ein funktionierendes Modem eines übernimmt, das nicht mehr funktioniert. Dies erfordert mindestens zwei aktive SIM-Karten im Gerät. Failover tritt zu zwei Zeitpunkten auf:

- **Wenn eine Nachricht gesendet wird.** Wenn das von der Strategie ausgewählte Modem nicht funktioniert, versucht SMSEagle das nächste der zulässigen Modems des Absenders in Modemnummerordnung, beginnend wieder vom ersten nach dem letzten, und verwendet das erste funktionierende. Nachrichten mit einem für sie ausgewählten Modem (Regel 1) oder an einen angehefteten Kontakt (Regel 2) werden zu diesem Zeitpunkt nicht umgeleitet.
- **Alle 2 Minuten.** SMSEagle prüft alle Modems. Nachrichten, die noch in der Outbox eines Modems warten, das nicht funktioniert, werden zu dem nächsten funktionierenden Modem verschoben, das der Autor der Nachricht verwenden darf. Wenn es kein solches Modem gibt, bleiben die Nachrichten dort, wo sie sind.

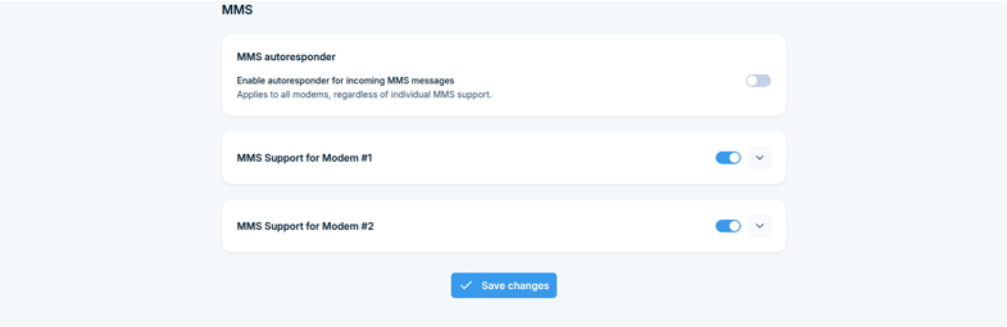
Ein Modem gilt als nicht funktionierend, wenn eine dieser Bedingungen erfüllt ist:

- es hat sich mehr als 4 Minuten nicht beim Gerät gemeldet,
- seine SIM-Karte ist nicht bereit, z. B. fehlt oder wartet auf eine PIN,
- die Watchdog-Funktion des Geräts, die alle 2 Minuten jedes Modem prüft, hat seinen Modem-Dienst mindestens 3-mal schnell hintereinander neu gestartet (weniger als 5 Minuten auseinander), das letzte Mal innerhalb der letzten 5 Minuten,

- Nachrichten darauf schlagen weiterhin fehl: mindestens eine Nachricht in seiner Warteschlange wurde 3-mal wiederholt, und das Modem hat in den letzten 5 Minuten nichts erfolgreich gesendet. Wenn andere Nachrichten in derselben Warteschlange nicht 3 Wiederholungen erreicht haben, wird das Problem als Fehler bei den fehlgeschlagenen Empfängern angesehen, nicht bei dem Modem.

Jede umgeleitete Nachricht wird im **Application**-Protokoll unter **System > Protokolle** aufgezeichnet, als Zeile, die mit `Modem: Modem failover triggered` beginnt.

MMS



MMS-Einstellungen

Was diese Funktion bewirkt

MMS ermöglicht dem Gerät das Versenden und Empfangen von **Multimedia-Nachrichten**: Text mit Bildern oder anderen angehängten Dateien statt normaler SMS.

Im Gegensatz zu SMS läuft MMS nicht über den einfachen GSM-Kanal. Es wird über das Datennetz des Betreibers an ein MMS-Zentrum geleitet. 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** festgelegt.

Der gleiche Bildschirm enthält auch den **MMS-Autoresponder**, 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 benötigen auch einen Benutzernamen und ein Passwort.
- Die SIM-Karte muss MMS im Tarif aktiviert haben. Eine SIM-Karte, die SMS versenden kann, aber keinen Datendienst oder MMS-Service hat, wird fehlschlagen, egal wie die Einstellungen ausgefüllt werden.
- Viele Operatorprofile sind dem Gerät bereits bekannt, daher versuchen Sie **APN-Einstellungen auslesen**, bevor Sie die Werte selbst suchen.

Schritt 1: Öffnen Sie die MMS-Seite

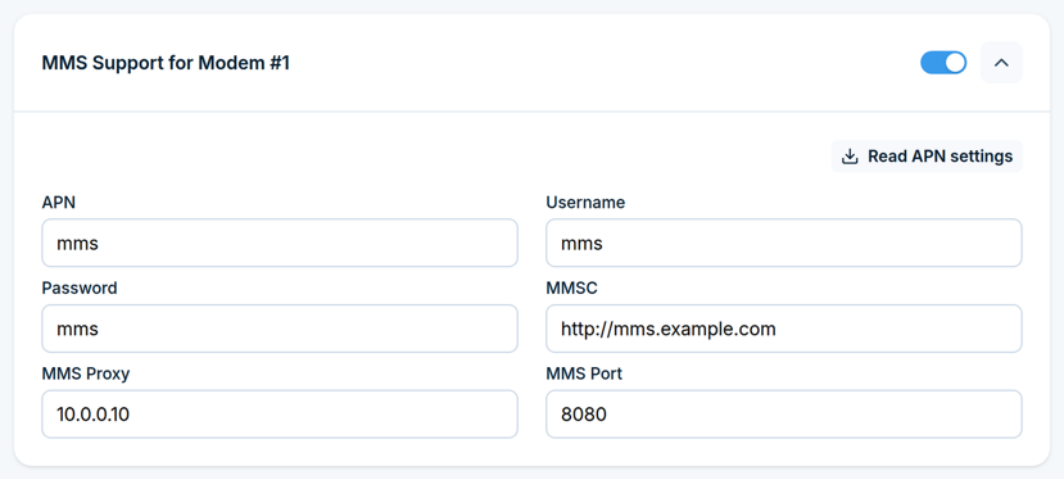
Gehen Sie in der Seitenleiste zu **Einstellungen > Kanäle > SMS / MMS > MMS**.

Die MMS-Seite zeigt das Feld **MMS-Autoresponder** oben an, dann einen ausklappbaren Abschnitt pro Modem mit der Überschrift **MMS-Support für Modem #1**, **#2** usw., wie in der Abbildung am Anfang dieses Abschnitts.

Schritt 2: Aktivieren Sie MMS auf einem Modem

Jeder Modem-Abschnitt hat einen Schalter neben seiner Überschrift. Schalten Sie ihn für jede SIM-Karte ein, die MMS verarbeiten soll.

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



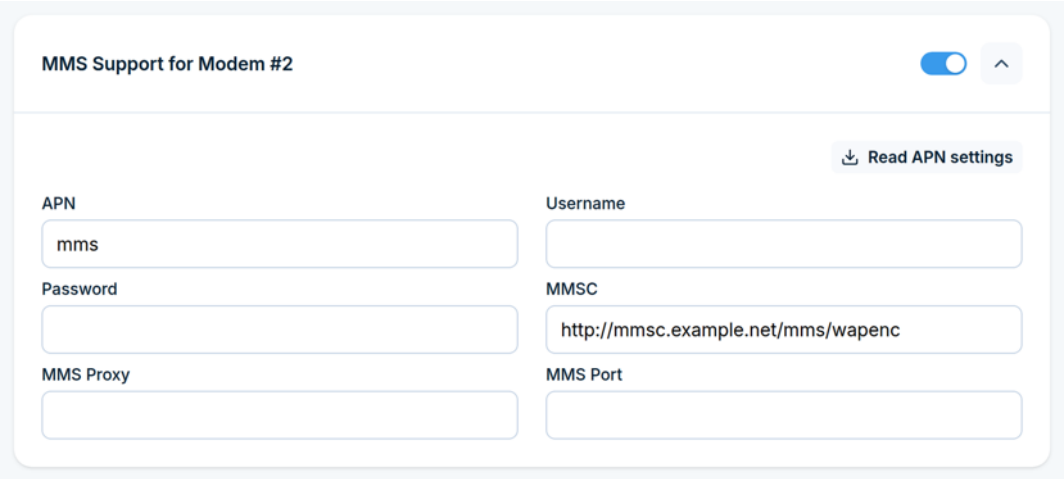
Ein erweiterter Modem-Abschnitt mit **APN-Einstellungen auslesen** über den Feldern

Schritt 3: Füllen Sie die Verbindungsparameter aus

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

Feld	Was Sie eingeben sollten
APN	Der Access Point Name des Betreibers, z. B. `internet`.
Benutzername	Der APN-Benutzer, falls vom Betreiber erforderlich. Lassen Sie das Feld andernfalls leer.
Passwort	Das APN-Passwort, falls erforderlich.
MMSC	Die Adresse des MMS-Zentrums des Betreibers, z. B. `http://mms.example.com`.
MMS-Proxy	Die Proxy-Adresse, falls vom Betreiber verwendet. Lassen Sie das Feld andernfalls leer.
MMS-Port	Der Proxy-Port. Nur zusammen mit einem Proxy erforderlich.

Jedes Feld gehört zu **diesem einen Modem**. Zwei SIM-Karten verschiedener Betreiber benötigen zwei verschiedene Wertsätze, daher wiederholen Sie dies für jedes Modem, das Sie aktiviert haben.



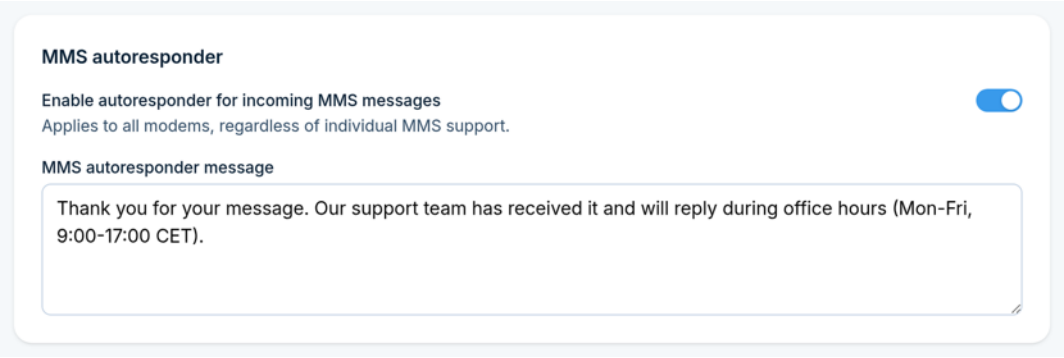
Das zweite Modem hat seine eigenen Werte und benötigt in diesem Beispiel keinen Proxy

Schritt 4: Richten Sie den Autoresponder ein (optional)

Das Feld **MMS-Autoresponder** oben auf der MMS-Seite sendet automatisch eine Antwort, wenn 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 der einzelnen MMS-Unterstützung**. Es ist eine einzelne globale Einstellung, keine Einstellung pro Modem, und es gibt einen gemeinsamen Antworttextfür jede eingehende MMS, halten Sie die Formulierung daher allgemein.



Der Autoresponder, aktiviert mit einer Beispielantwort

Schritt 5: Speichern und neu starten

Klicken Sie auf **Save changes**.

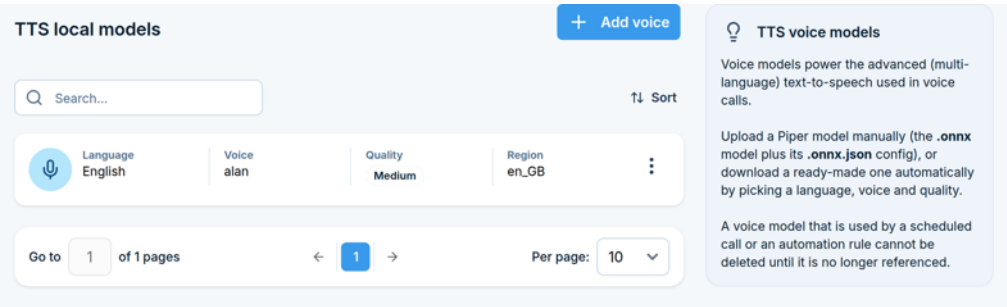
> **Ein Neustart ist erforderlich.** Nach dem Speichern fordert SMSEagle Sie auf, das Gerät neu zu starten, damit die MMS-Änderungen wirksam werden. Bis dahin werden die neuen Parameter gespeichert, aber noch nicht verwendet.

Anrufe

TTS-Lokalmodelle

Lokale Sprachmodelle ermöglichen **Text to speech - advanced**. 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 ihrer Sprache, Region und Qualität auf.



TTS-Lokalmodelle

Ein Modell hinzufügen

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

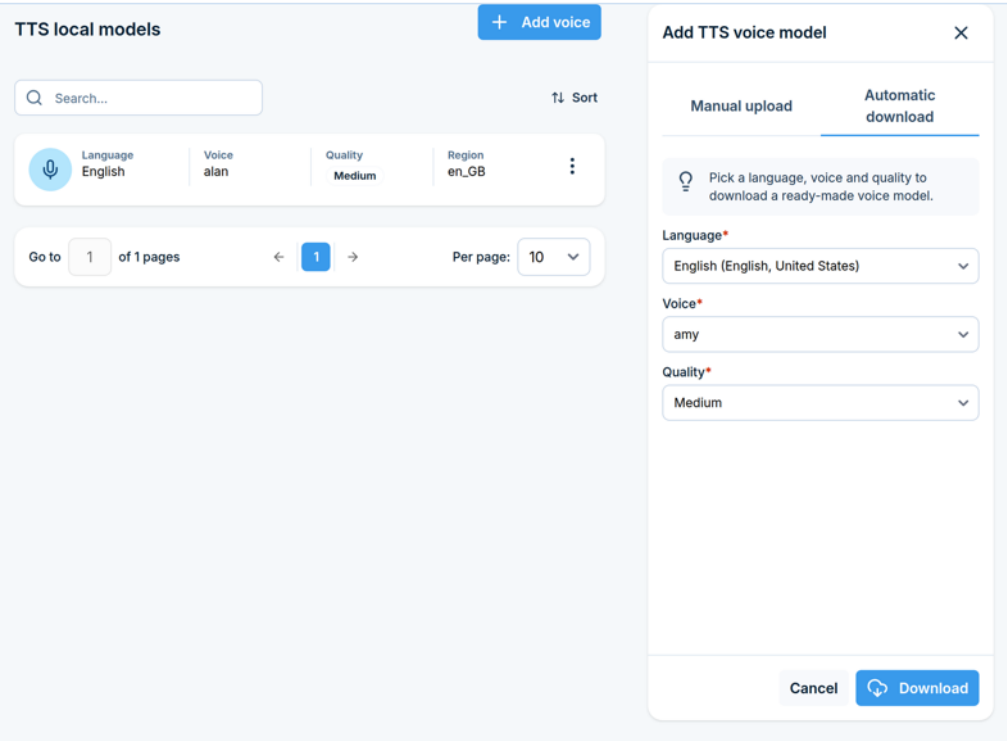
Automatischer Download (der einfache Weg)

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 Fortschrittsanzeige zeigt den Download an, und das Modell erscheint in der Liste, wenn er abgeschlossen ist.

Höhere Qualität bedeutet eine natürlichere Stimme, aber eine größere Datei und eine etwas langsamere Synthese. **Medium** ist ein guter Standard.



Herunterladen eines vorgefertigten Sprachmodells

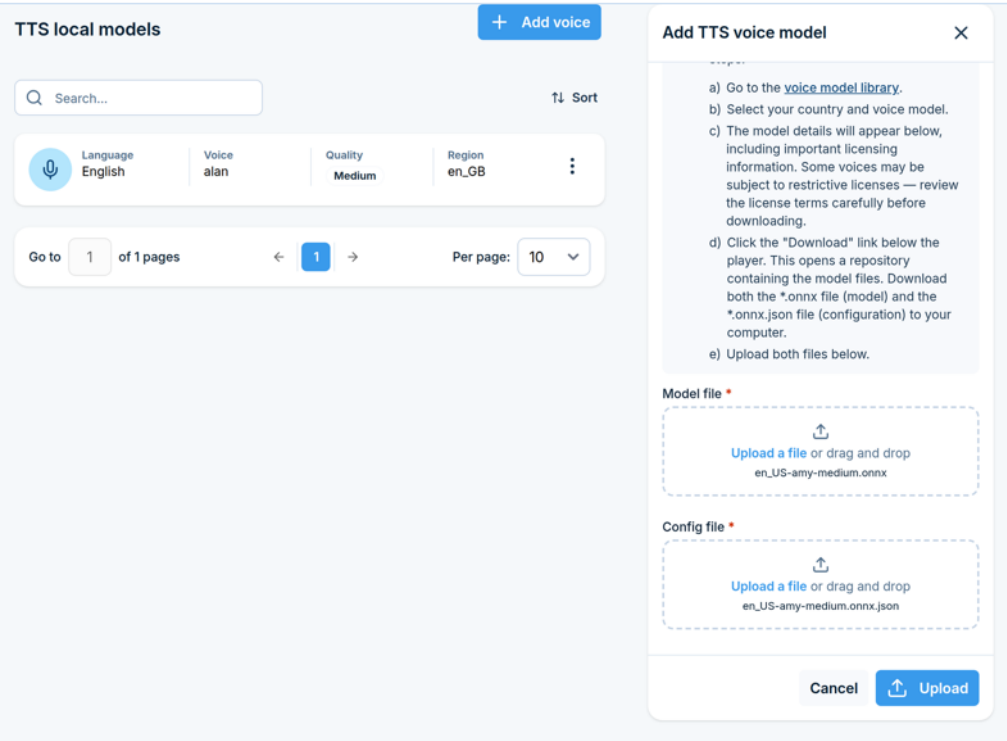
Wenn das Bedienfeld „Voice list unavailable“ meldet, konnte das Gerät den Online-Stimmenkatalog nicht erreichen. Überprüfen Sie die Netzwerkeinstellungen und versuchen Sie es später erneut, oder verwenden Sie stattdessen manuelles Hochladen.

Manuelles Hochladen

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

1. **Model file (.onnx)** - das Modell selbst.
2. **Config file (.onnx.json)** - die dazugehörige Konfigurationsdatei.

Beide Dateien sind erforderlich und müssen zusammenpassen. Klicken Sie auf **Upload**.



Manuelles Hochladen eines Piper-Modells

Ein Modell löschen

Verwenden Sie die Aktion **Delete** neben einem Modell, oder markieren Sie mehrere Modelle und löschen Sie diese zusammen.

Ein Modell, das noch irgendwo referenziert wird, kann nicht gelöscht werden. Die Meldung zeigt Ihnen an, wo es verwendet wird, z. B. in einem geplanten Anruf, einer Email-to-SMS-Regel, einer Digital-Input- oder Digital-Output-Aktion oder einer Network-Monitor-Aufgabe. Ändern oder entfernen Sie diese Referenz zunächst und löschen Sie dann das Modell.

TTS-Online-Modelle (ElevenLabs)

Online-Modelle erzeugen die natürlichsten Sprachausgaben, nutzen aber die ElevenLabs-API, weshalb sie ein ElevenLabs-Konto und eine Internetverbindung erfordern.

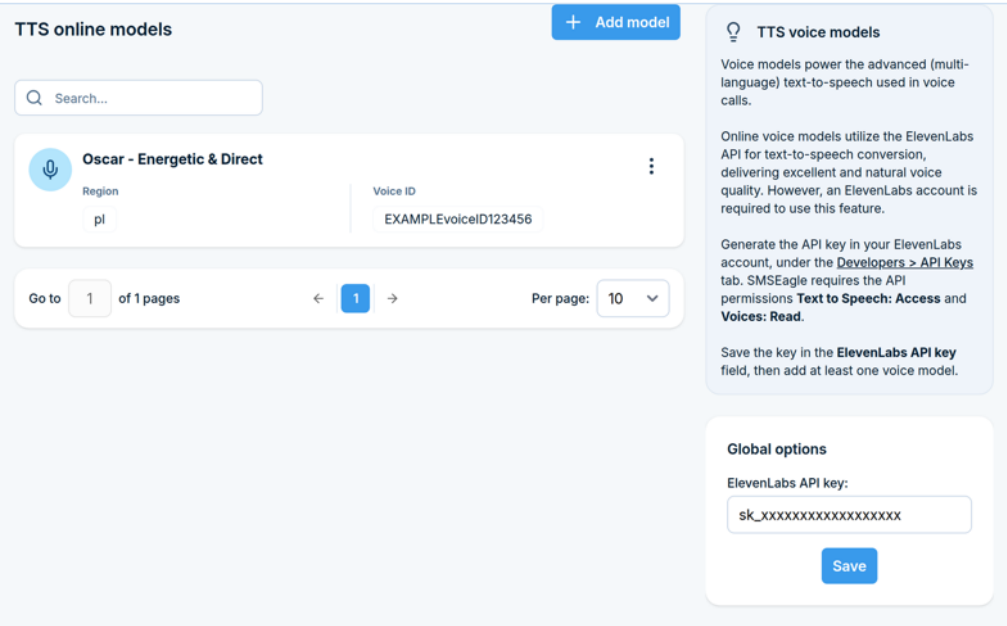
Gehen Sie zu **Settings > Channels > Calls > TTS online models**.

Schritt 1: ElevenLabs-Konto vorbereiten

In Ihrem ElevenLabs-Konto:

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

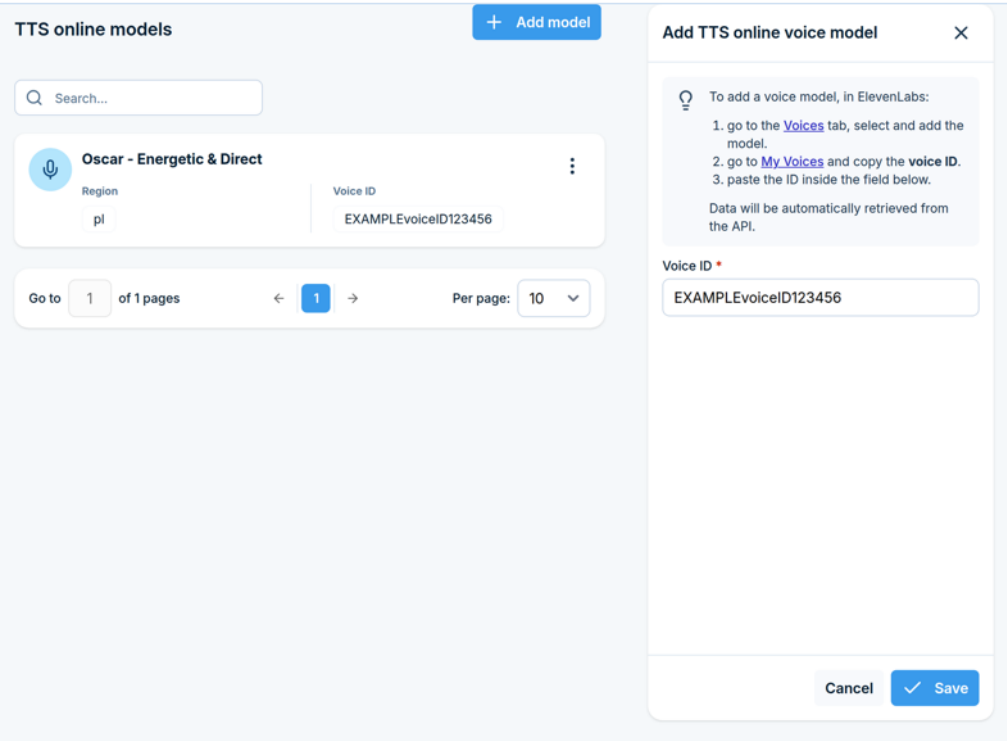
Schritt 2: API-Schlüssel speichern

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

Schritt 3: Ein Sprachmodell 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.



Hinzufügen eines ElevenLabs-Sprachmodells

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

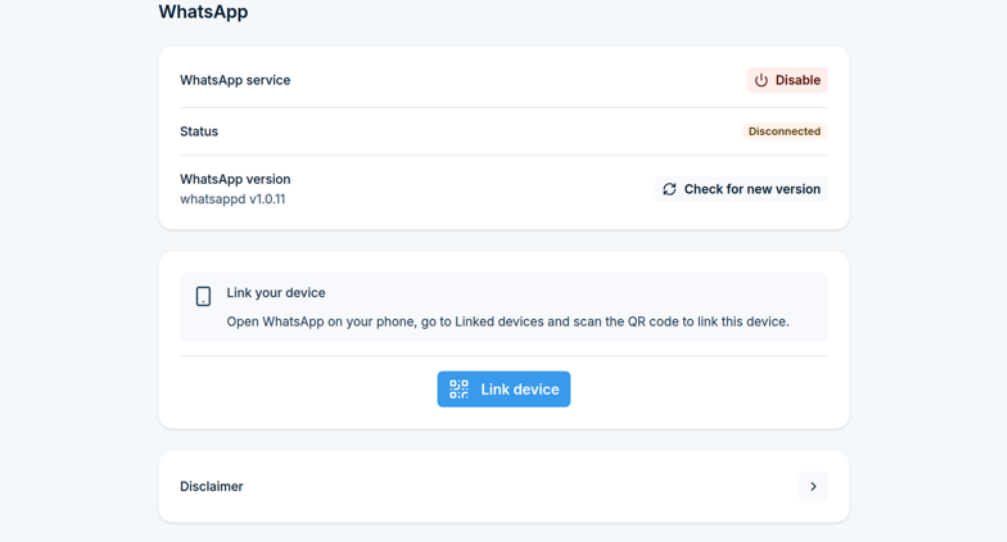
Eingehende Anrufe

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 Anruferweiterungscodes pro Modem. Nicht jeder Netzbetreiber unterstützt Anruferweiterungscodes – prüfen Sie dies mit Ihrem Betreiber, bevor Sie sich darauf verlassen.

WhatsApp



WhatsApp-Einstellungen und Geräteverbindung

Was diese Funktion bewirkt

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

Nach der Verknüpfung wird WhatsApp zu einem weiteren Kanal, den Sie beim Verfassen einer Nachricht auswählen können, mit eigenem Nachrichtenverlauf. Es gibt auch eine **Fallback**-Option, die eine SMS oder MMS sendet, falls sich herausstellt, dass ein Empfänger kein WhatsApp hat.

Typische Anwendungen: Menschen erreichen, die WhatsApp nutzen, längere Benachrichtigungen senden, ohne sie in mehrere SMS-Teile aufzuteilen, oder die Kosten für Nachrichten an Empfänger im Ausland senken.

Die Einrichtung besteht aus zwei Teilen: Zuerst aktivieren Sie den Service und verknüpfen ein Gerät (**Settings > Channels > WhatsApp**), dann verwenden 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 Ihrer Seitenleiste vorhanden 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 eine Internetverbindung erreichen können. 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 kommen, und Nachrichten, die an es gesendet werden, erscheinen in SMSEagle.

Schritt 1: Öffnen Sie die WhatsApp-Einstellungen

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

Das Feld **Connection** zeigt die installierte **WhatsApp version** und den aktuellen **Status**. Auf einem neuen Gerät ist der Status **Disabled** und eine Warnung erklärt, dass der Service aktiviert werden muss, bevor ein Gerät verknüpft werden kann.

Schritt 2: Aktivieren Sie den Service

Klicken Sie unten auf der Seite auf **Enable**. Der Status ändert sich zu **Disconnected**, was bedeutet, dass der Service ausgeführt wird, aber noch kein Konto verknüpft ist. Das ist der in der Abbildung am Anfang dieses Abschnitts gezeigte Status mit der Schaltfläche **Link device** unter dem Feld Connection.

Schritt 3: Verknüpfen Sie Ihr Telefon

1. Klicken Sie auf **Link device**. Ein QR-Code wird auf dem Bildschirm angezeigt.
2. Öffnen Sie auf Ihrem Telefon **WhatsApp**, gehen Sie zu **Linked devices** und wählen Sie aus, um ein neues Gerät zu verknüpfen.
3. Richten Sie das Telefon auf den QR-Code auf dem Bildschirm.

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

> **Der QR-Code wartet nicht für immer.** Wenn er nicht innerhalb einer kurzen Zeit gescannt wird, wird die Verknüpfung abgebrochen und die Seite kehrt zu **Disconnected** zurück. Halten Sie das Telefon auf dem Bildschirm **Linked devices** offen, bevor Sie auf **Link device** klicken, und klicken Sie einfach erneut darauf, wenn der Code abläuft.

Sie können den Vorgang auch selbst mit **Cancel linking** beenden.

Schritt 4: Entscheiden Sie, was mit Empfängern ohne WhatsApp passiert

Sobald der Status **Connected** ist, wird ein Feld **Fallback** mit einem Schalter angezeigt:

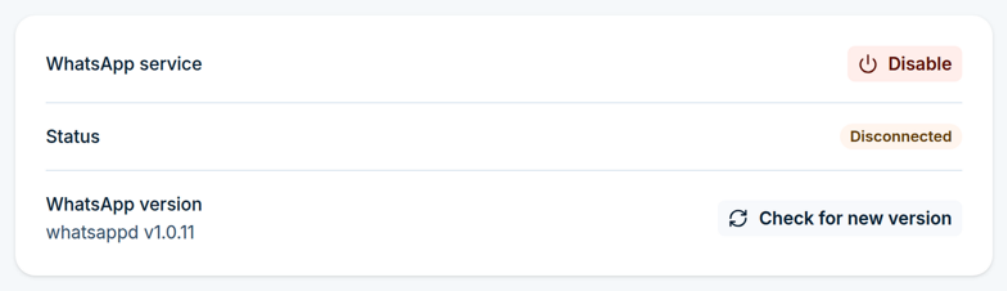
Fall back to SMS/MMS Wenn dies aktiviert ist, wird eine Nachricht an eine Nummer, die nicht bei WhatsApp registriert ist, stattdessen als SMS oder MMS gesendet. Wenn dies deaktiviert ist, wird eine solche Nachricht einfach nicht zugestellt.

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

Schritt 5: Halten Sie den Service auf dem neuesten Stand

Das Feld **Connection** hat eine Schaltfläche **Check for new version**. Klicken Sie darauf, um zu prüfen, ob eine neuere WhatsApp-Version verfügbar ist:

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



Das Verbindungsfeld mit **Check for new version** neben der installierten Version

Verknüpfung aufheben und ausschalten

Zwei Schaltflächen am unteren Rand der Einstellungsseite erfüllen unterschiedliche Funktionen:

Schaltfläche	Funktion
Unlink device	Meldet das Konto ab. Der Service läuft weiter, die Seite kehrt zu **Disconnected** zurück und Sie können ein anderes Konto verknüpfen. **Fall back to SMS/MMS** wird gleichzeitig ausgeschaltet.
Disable	Stoppt den WhatsApp-Service vollständig. Der Kanal verschwindet aus dem Compose-Fenster.

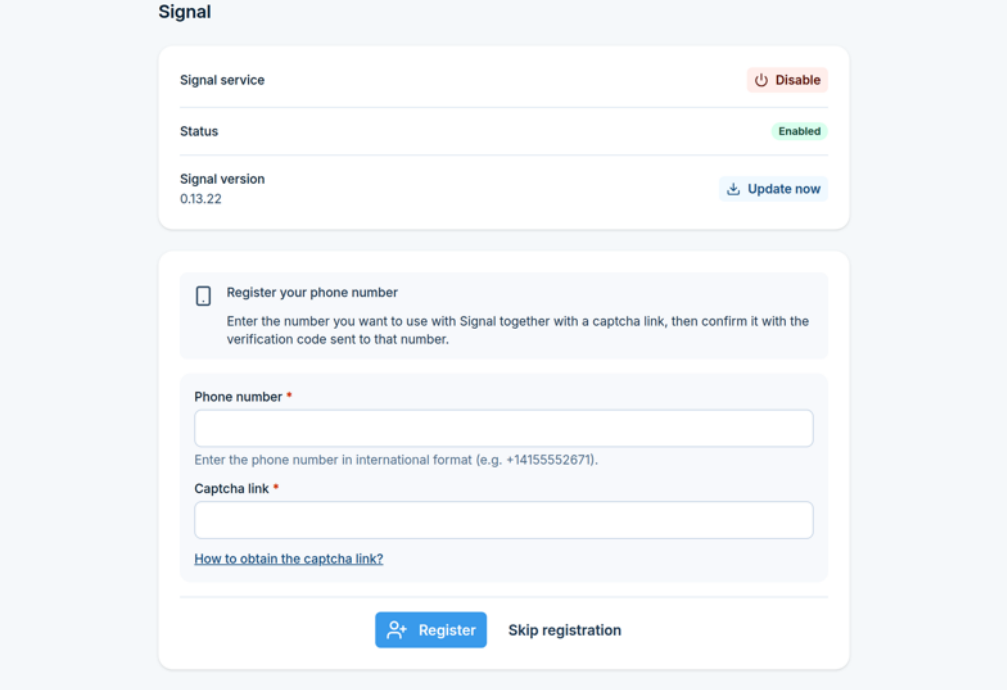
Sie können die Verknüpfung auch auf der Telefonseite aufheben, in **WhatsApp > Linked devices**. Die Seite zeigt dann bei der nächsten Aktualisierung **Disconnected** an.

Gut zu wissen

- WhatsApp-Nachrichten verwenden die Netzwerkverbindung, daher verbrauchen sie kein SIM-Guthaben und sind nicht vom GSM-Netz abhängig. Die Option **Fall back to SMS/MMS** ist die Ausnahme: Diese Fallback-Nachrichten gehen durch das Modem.

- Die Verknüpfung befindet sich auf dem Gerät. Das Wiederherstellen einer Sicherung auf anderen Hardware oder das Aufheben der Verknüpfung vom Telefon erfordert das Scannen eines neuen QR-Codes.
- In der Konversationsliste werden nur Nachrichten angezeigt, die nach der Geräteverbindung empfangen wurden.

Signal



Signal-Service-Einstellungen

Was diese Funktion bewirkt

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

Typische Verwendungen: Menschen erreichen, die Signal gegenüber SMS bevorzugen, oder Benachrichtigungen an Empfänger im Ausland senden, die sonst Roaming-Gebühren verursachen würden.

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 Compose-Fenster).

Bevor Sie beginnen

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

- Sie benötigen eine Telefonnummer, die einen Verifizierungscode empfangen kann, und sie 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 **Einstellungen > Kanäle > Signal**.

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

Schritt 2: Aktivieren Sie den Service

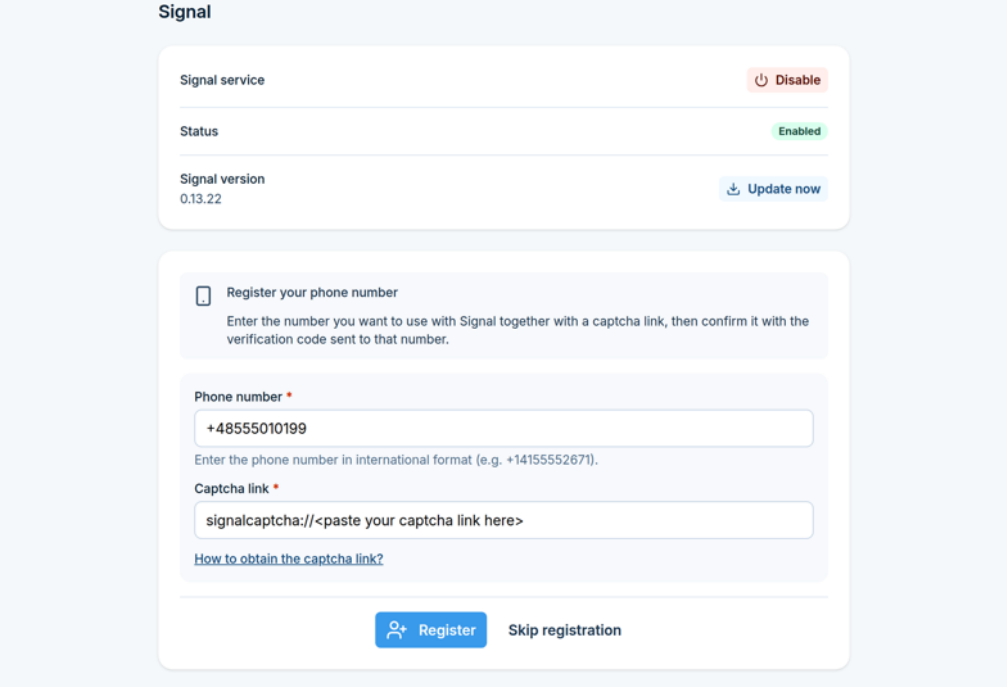
Klicken Sie auf **Aktivieren** unten auf der Seite. Der Status wechselt zu **Aktiviert** und das Registrierungsformular erscheint, wie in der Abbildung am Anfang dieses Abschnitts.

Schritt 3: Registrieren Sie eine Telefonnummer

Im Feld **Eine Telefonnummer registrieren**:

1. Geben Sie unter **Telefonnummer** die Nummer im internationalen Format ein, z. B. `+14155552671`.
2. Fügen Sie unter **Captcha-Link** den Captcha-Link ein. Der Link **Wie erhalte ich den Captcha-Link?** unterhalb des Feldes öffnet eine Schritt-für-Schritt-Anleitung in einem neuen Tab.
3. Klicken Sie auf **Registrieren**.

Signal sendet dann einen Bestätigungscode an die Nummer.



Eine Telefonnummer registrieren

Haben Sie diese Nummer kürzlich bereits registriert? Klicken Sie stattdessen auf **Registrierung überspringen**. Das Formular geht direkt zum Verifikationsschritt, wo Sie einen bereits empfangenen Code eingeben können.

Schritt 4: Verifizieren Sie die Nummer

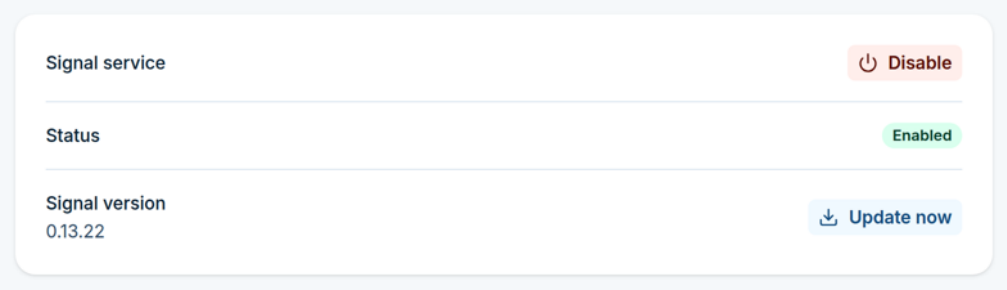
Das Formular fragt nun nach dem **Bestätigungscode**. Geben Sie den empfangenen Code ein und klicken Sie auf **Verifizieren**.

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

Schritt 5: Halten Sie den Service auf dem neuesten Stand

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

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

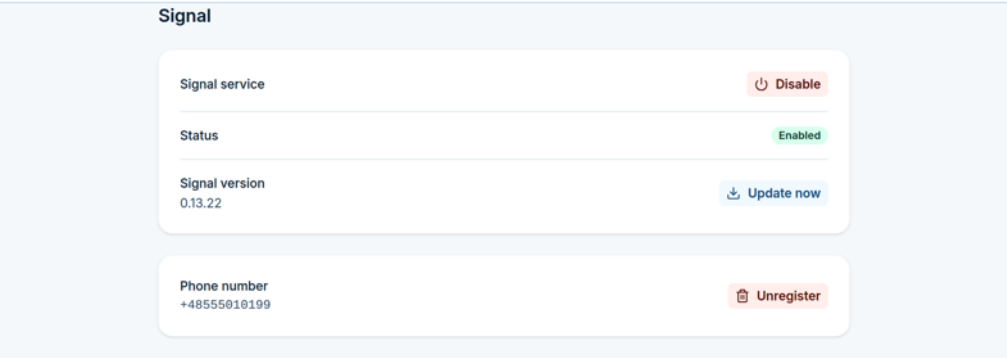


Das Feld Dienst. Hier wurde bereits eine neuere Version gefunden, daher lautet der Button **Jetzt aktualisieren**

Die Nummer entfernen

Um die Registrierung des Geräts bei Signal zu beenden, gehen Sie zurück zu **Einstellungen > Kanäle > Signal** und klicken Sie auf **Unregister** im Feld **Registrierte Nummer**. Die Nummer wird freigegeben und die Seite kehrt zum Registrierungsformular zurück.

Um den Kanal zu deaktivieren, ohne die Registrierung aufzuheben, klicken Sie auf **Deaktivieren** unten auf der Seite. Der Dienst wird beendet und Signal verschwindet aus dem Fenster „Verfassen



Neue Texte und Mitteilungen

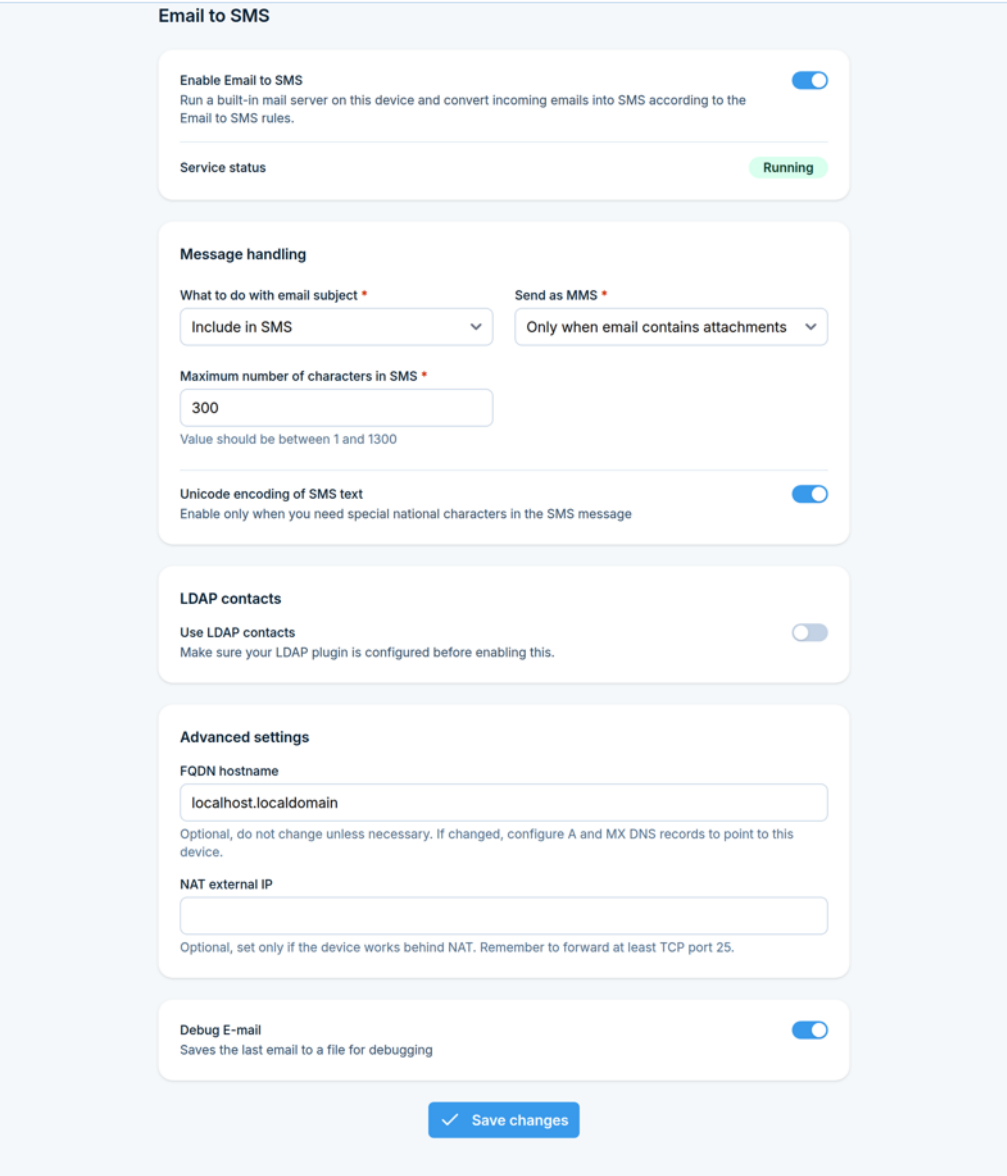
Gut zu wissen

- , aber die Registrierung bleibt erhalten, sodass eine erneute Aktivierung keine neue Verifikation erfordert.
- , aber die Registrierung bleibt erhalten, sodass eine erneute Aktivierung keine neue Verifikation erfordert.
- Signal-Einstellungen mit der registrierten Telefonnummer und dem Button Unregister

, aber die Registrierung bleibt erhalten, sodass eine erneute Aktivierung keine neue Verifikation erfordert.

, Eine registrierte Signal-Nummer

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



E-Mail-zu-SMS-Einstellungen

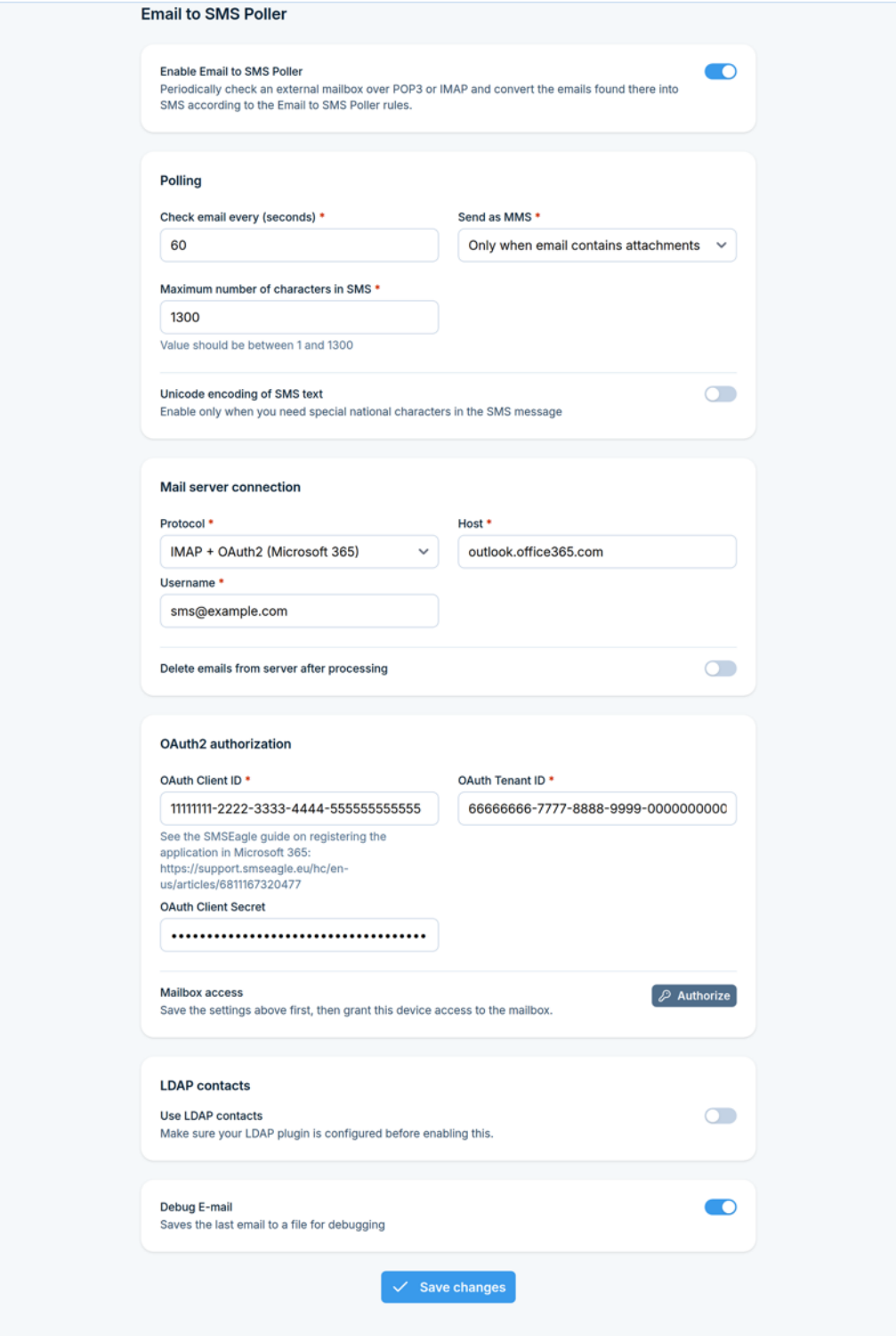
Aktivieren Sie **E-Mail zu SMS aktivieren**, um den Mail-Server zu starten. **Dienststatus** zeigt, ob er **Ausgeführt** oder **Gestoppt** ist. Der Rest der Seite bestimmt, wie eine E-Mail zu einer SMS wird:

- **Was mit dem E-Mail-Betreff zu tun ist** - **Ignorieren**, **In SMS einschließen**, **Zur Authentifizierung verwenden** oder **Nur Betreff ohne E-Mail-Text senden**.
- **Als MMS senden** - **Niemals**, **Immer** oder **Nur wenn E-Mail Anhänge enthält**.
- **Maximale Anzahl von Zeichen in SMS** - von 1 bis 1300.
- **Unicode-Kodierung von SMS-Text** - aktivieren Sie dies nur, wenn Nachrichten nationale Zeichen benötigen, die das Standard-SMS-Alphabet nicht enthält.
- **LDAP-Kontakte verwenden** - ermöglicht es, einen Verzeichniskontakt oder eine Gruppe im Adressteil des Empfängers zu benennen. Konfigurieren Sie zunächst LDAP.
- **FQDN-Hostname** (unter **Erweiterte Einstellungen**) - optionaler Domänenname für die Verwendung in Empfängeradressen anstelle der IP-Adresse des Geräts. Wenn Sie ihn ändern, verweisen Sie die A- und MX-DNS-Einträge für diesen Namen auf das Gerät.

- **NAT externe IP** - setzen Sie dies nur, wenn sich das Gerät hinter NAT befindet, und leiten Sie mindestens TCP-Port 25 an das Gerät weiter.
- **Debug E-Mail** - speichert die zuletzt empfangene E-Mail zur Fehlerbehebung in einer Datei.

Email to SMS Poller

Settings > Channels > Email > Email to SMS Poller (`/settings/email/email-to-sms-poller`) verbindet das Gerät mit einem vorhandenen Postfach, überprüft es in einem festen Intervall und konvertiert die gefundenen E-Mails gemäß den Regeln unter Email to SMS Poller in der Automation in SMS. Im Gegensatz zu Email to SMS müssen keine E-Mails an das Gerät selbst zugestellt werden.



Email to SMS Poller-Einstellungen, verbunden mit einem Microsoft 365-Postfach

Aktivieren Sie **Enable Email to SMS Poller**. Das Formular darunter hat folgende 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 für Email to SMS.

Mail server connection

- **Protocol** - **POP3**, **IMAP** oder **IMAP + OAuth2 (Microsoft 365)**.
- **Host** und **Username** des Postfachs.
- Nur mit **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 dies deaktiviert, um das Postfach unverändert zu halten.

OAuth2 authorization (nur mit **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 auf **Authorize** unter **Mailbox access** und gewähren Sie dem Gerät Zugriff auf das Postfach.

Use LDAP contacts und **Debug E-mail** funktionieren wie für Email to SMS.

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

SMTP-Konfiguration

Einstellungen > Kanäle > E-Mail > SMTP-Konfiguration (`/settings/email/smtp`) verwaltet eine Liste wiederverwendbarer SMTP-Server-Voreinstellungen und weist jeder Funktion, die ausgehende E-Mails versendet, eine zu:

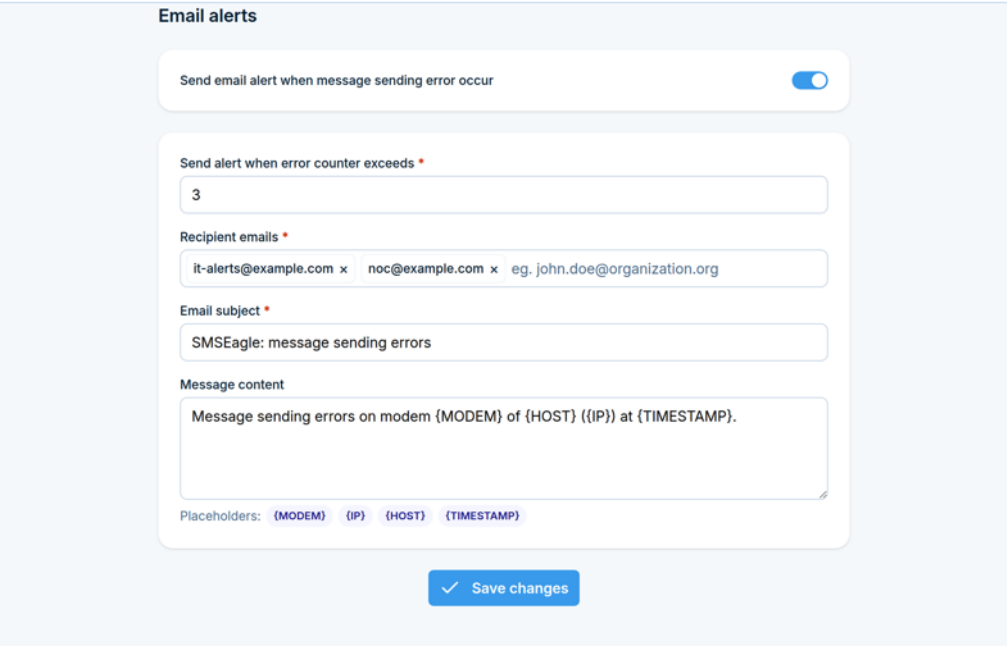
- **Compose menu**, **APIv2**, **SMS to Email**, **Alerts**, **Reporting module**, **Workflows**

Jede dieser Funktionen kann auf **None** oder auf eine Ihrer gespeicherten Voreinstellungen eingestellt werden. Das Zuweisen einer Voreinstellung zu einer Funktion deaktiviert die bestehende E-Mail-Konfiguration dieser Funktion.

Klicken Sie unter **Configuration presets** auf **Create new**, um einen SMTP-Server hinzuzufügen (Host, Port, Verschlüsselung, Absenderadresse, Anmeldedaten); Voreinstellungen können dann aus dem Dropdown-Menü für jede der oben genannten Funktionen ausgewählt werden.

E-Mail-Warnungen

Settings > Channels > Email > Email alerts (`/settings/email/alerts`) sendet eine Benachrichtigung per E-Mail, wenn ausgehende Nachrichten weiterhin nicht gesendet werden können. Es benötigt eine SMTP-Voreinstellung, die unter SMTP Configuration den **Alerts** zugewiesen ist.



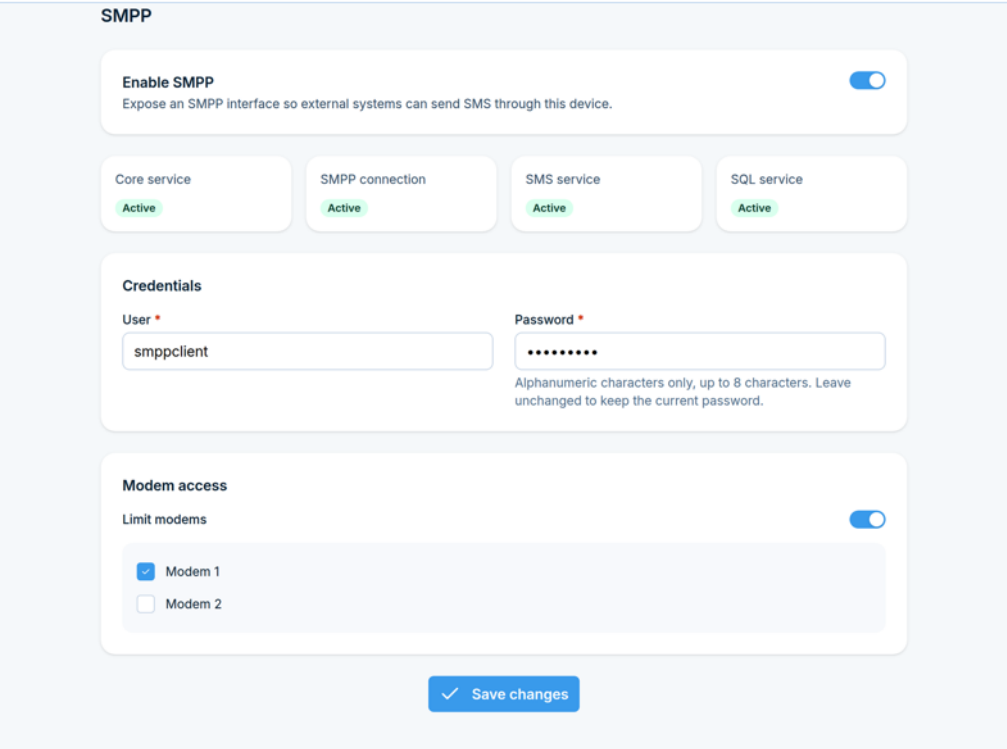
Email-Benachrichtigungseinstellungen

Aktivieren Sie **Send email alert when message sending error occur** und legen Sie fest:

- **Send alert when error counter exceeds** - wie viele Fehler beim Senden gezählt werden, bevor die Benachrichtigung versendet wird. Ein Wert über 2 vermeidet Benachrichtigungen durch einen einzelnen vorübergehenden Fehler.
- **Recipient emails** - eine oder mehrere Adressen.
- **Email subject** und **Message content** - der Text der Benachrichtigung. Die Platzhalter **{MODEM}** (das Modem, das die Benachrichtigung ausgelöst hat), **{IP}** (die IP-Adresse des Geräts), **{HOST}** (sein Host-Name) und **{TIMESTAMP}** (wann der Fehler erkannt wurde) werden durch echte Werte ersetzt. Klicken Sie auf einen Platzhalter unter dem Nachrichtenfeld, um ihn einzufügen.

SMPP

Einstellungen > Kanäle > 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 eingehende SMS sowie Lieferberichte über dieselbe Verbindung zurückerhalten.



SMPP-Einstellungen

Verbindungsdetails

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

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

Eingehende SMS und Lieferberichte werden auf dem Gerät in eine Warteschlange eingereiht, während kein SMPP-Client verbunden ist. Sobald sich ein Client verbindet, liefert SMSEagle alles aus dieser Warteschlange, daher muss der Client ab dem Verbindungszeitpunkt bereit sein, `deliver_sm`-Nachrichten zu empfangen und zu bestätigen.

SMPP aktivieren

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

2. Legen Sie unter **Credentials** den **User** und das **Password** fest, mit denen sich der SMPP-Client verbindet. Das Passwort darf nur Buchstaben und Ziffern enthalten und maximal 8 Zeichen lang sein. Wenn bereits ein Passwort gespeichert ist, lassen Sie das Feld unverändert, um es beizubehalten.
3. Aktivieren Sie unter **Modem access** die Option **Limit modems**, um SMPP-Verkehr nur über die von Ihnen ausgewählten Modems zu ermöglichen. Lassen Sie diese Option deaktiviert, um alle Modems zu erlauben.
4. Klicken Sie auf **Save changes**.

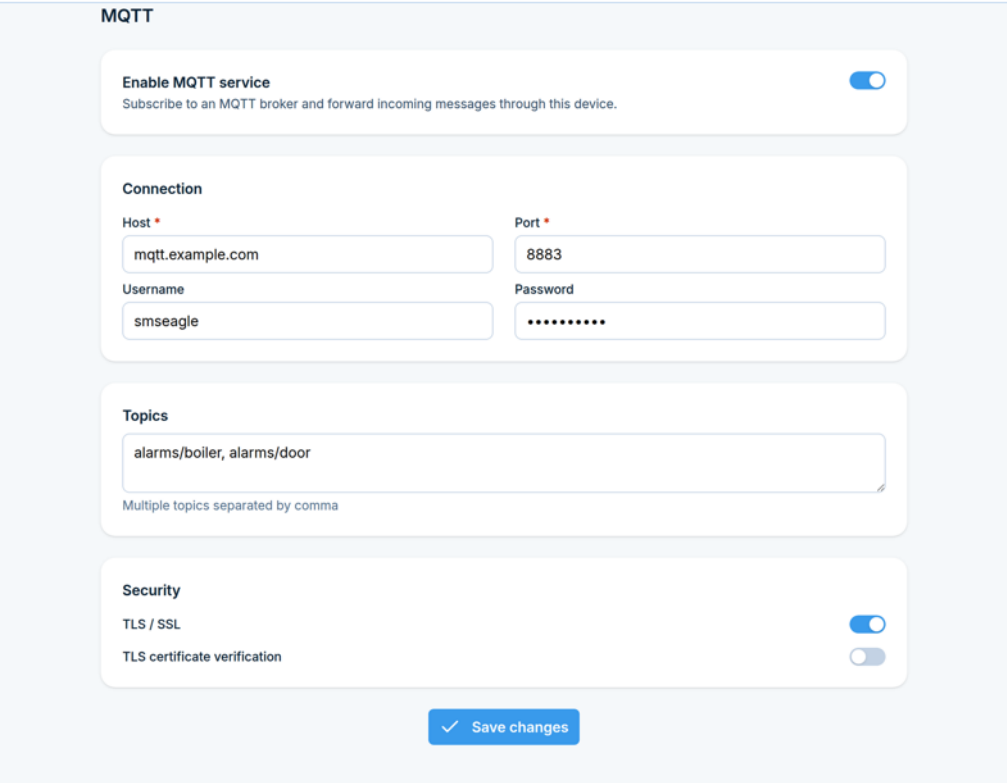
   Ein Neustart ist erforderlich. Nach dem Speichern fordert SMSEagle Sie auf, das Gerät neu zu starten, damit die SMPP-Änderungen wirksam werden. Bis dahin werden die neuen Einstellungen gespeichert, sind aber noch nicht aktiv. Verwenden Sie **System > Restart**, wenn Sie bereit sind.

Nach dem Neustart zeigen die vier Status-Karten (**Core service**, **SMPP connection**, **SMS service**, **SQL service**) an, ob jeder Teil des SMPP-Servers läuft. 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-Verkehr mit seinem eigenen API-Schlüssel, der unter **Settings > API v2 keys** aufgelistet ist, sowie 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

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



MQTT-Broker-Verbindungseinstellungen

Aktivieren Sie **Enable MQTT service**, dann legen Sie fest:

- **Host** und **Port** des Brokers (beide erforderlich).
- **Username** und **Password**, falls der Broker diese benötigt.
- **Topics** - die Themen, auf die das Gerät abonniert, getrennt durch Kommas.
- **TLS / SSL** - verschlüsselt die Verbindung zum Broker. Die **TLS certificate verification** überprüft auch das Zertifikat des Brokers. Lassen Sie es nur bei einem Broker mit selbstsigniertem Zertifikat deaktiviert.

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, aber noch nicht verwendet. 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 an (schreibgeschützt) und ermöglicht Ihnen die Konfiguration von:

- **Get IP address from DHCP** – DHCP aktivieren oder deaktivieren, um eine statische IP-Adresse einzustellen.

- **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 zutrifft. Wenn die Beschränkung aktiv ist, werden alle Ports außer 22 (SSH) für alle außerhalb der Liste blockiert.

  Seien Sie vorsichtig mit IP address restriction. Eine falsch konfigurierte Positivliste kann Sie von Ihrem eigenen Computer aus von der Weboberfläche abschneiden. Fügen Sie zunächst Ihre aktuelle IP-Adresse hinzu (die Seite bietet eine Verknüpfung **Add your IP address**), bevor Sie speichern.

SSL

Einstellungen > Globale Einstellungen > Netzwerk > SSL (`/settings/network/ssl`) ermöglicht es Ihnen, das Standard-Selbstsignierungszertifikat 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 an HTTPS weiter.

Failover

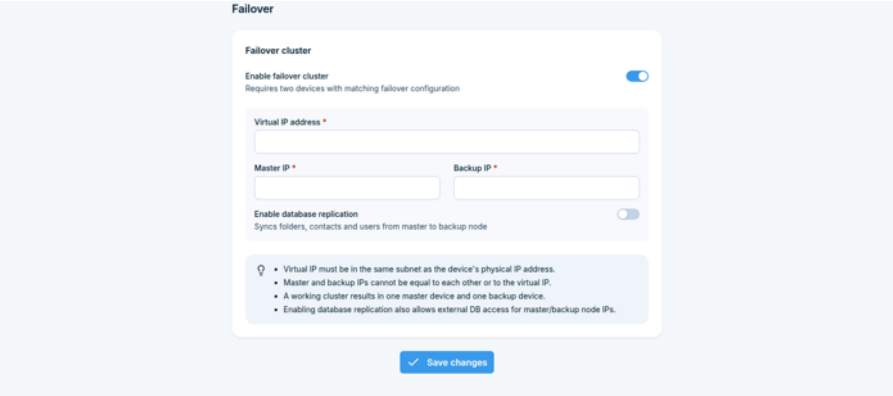
Failover Cluster bietet Hochverfügbarkeit auf Geräteebene: Ein zweites SMSEagle-Gerät steht als Sicherung zur Verfügung und ist bereit, die Kontrolle zu übernehmen, wenn das Master-Gerät nicht mehr antwortet. Dies unterscheidet sich vom Modem-Failover, das zwischen zwei SIM-Karten im selben Gerät umschaltet – ein Failover Cluster schützt vor dem Ausfall des gesamten Geräts.

Wo zu finden

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

Failover Cluster aktivieren

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



Failover-Cluster-Einstellungen

Legen Sie die gleichen Werte auf beiden Geräten fest:

- **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 zum Master, das mit **Backup IP** übereinstimmende zum 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- 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, aber noch nicht verwendet. Verwenden Sie **System > Restart**, wenn Sie bereit sind.

Master/Backup-Rollen und virtuelle IP

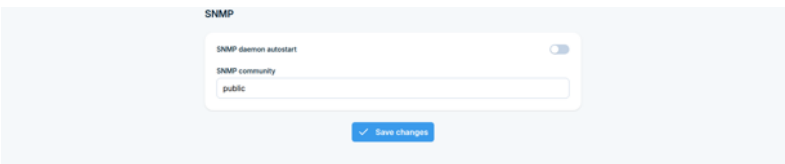
Der Cluster wird über eine einzelne **virtuelle IP-Adresse** erreicht, die immer auf das aktuell aktive Gerät verweist:

- Die virtuelle IP muss sich im selben Subnetz befinden wie die physische IP-Adresse jedes Geräts.
- Die Master-IP, Backup-IP und virtuelle IP müssen sich voneinander unterscheiden.
- Ein funktionierender Cluster hat zu jedem Zeitpunkt genau ein Master-Gerät und ein Backup-Gerät. Falls der Master nicht mehr antwortet, übernimmt das Backup die virtuelle IP.

Datenbankreplikation und externer Zugriff

Durch Aktivierung des Failover-Clusters wird auch die Datenbankreplikation zwischen Master und Backup aktiviert, sodass das Backup-Gerät eine aktuelle Kopie von Nachrichten, Kontakten und Einstellungen hat, falls es die Kontrolle übernehmen muss. Diese Einstellung ermöglicht auch externen Datenbankzugriff speziell für die IP-Adressen der Master- und Backup-Knoten, was für die Replikation erforderlich ist.

SNMP



SNMP-Agent-Einstellungen

Der SNMP-Agent ermöglicht externen Tools (einem NMS, einem MIB-Browser oder einem einfachen `snmpget`/`snmpwalk`-Aufruf), SMSEagle nach seinen Metriken abzufragen – Signalstärke, Netzwerkname, Ordnernachrichtenzähler, Systemlaufzeit und mehr. Dies ist die entgegengesetzte

Richtung von SNMP Traps: Der Agent wird von einem externen Tool abgefragt, anstatt dass SMSEagle eine Benachrichtigung an diesen sendet.

Wo zu finden

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

Konfigurieren des SNMP-Agenten

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

Nach Aktivierung können die Erweiterungsparameter von SMSEagle (Signalstärke, Netzwerkname, Ordnerzähler, Laufzeit und weitere) aus dem MIB-Baum des Geräts mithilfe eines beliebigen Standard-SNMP-Tools ausgelesen werden, z. B. NET-SNMPs `snmpget`/`snmpwalk` oder ein grafischer MIB-Browser.

Verfügbare Metriken

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

Metriken, die ein Modem beschreiben, enden mit der Modemannummer: 1 und 2. Die Tabellen zeigen sie für Modem 1. Eine Metrik gibt `-1` zurück, wenn ihr Wert nicht gelesen werden kann, beispielsweise wenn das Modem ausgeschaltet ist oder der Temperatursensor nicht aktiviert ist.

Metrik	Rückgabewert
`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, andernfalls der 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`	SMS vom Modem heute empfangen, seit Mitternacht.
`SMSCountOut1`	SMS vom Modem heute versendet, seit Mitternacht.
`FolderInbox_Total`	**Ungelesene** Nachrichten im Posteingang. Eine mehrteilige Nachricht zählt einmal.
`FolderOutbox_Total`	Nachrichten im Postausgang, der Warteschlange zum Versenden.
`FolderSent_Last24H`	Nachrichten in den letzten 24 Stunden versendet. Jeder Teil einer mehrteiligen Nachricht zählt separat.
`FolderSent_Last1M`	Nachrichten im letzten Monat versendet, auf die gleiche Weise gezählt.
`FolderSent_Last24HSendErr`	Nachrichten, deren Versand in den letzten 24 Stunden fehlgeschlagen ist, weil das Modem sie nicht versenden konnte oder das Netz 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, nach der Nummerierung der Temperatur- und Feuchtigkeitssensoren. Die folgende OID ist für `Temp1`.
`Humidity`	Luftfeuchte 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 Metriknamen und dem ASCII-Code jedes Zeichens. Bei einem anderen Modem ändert sich nur die letzte Zahl: Sie ist 48 plus die Modemnummer, also endet `GSM_Signal2` mit `.50`.

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

Metriken auslesen

Ersetzen Sie `public` durch Ihr **SNMP-Passwort** 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 vom Netzwerk aus abgerufen 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, Speicher, Last und CPU-Auslastung. Die Prozessliste und andere Details werden dem Netzwerk nicht offengelegt.

Die gleiche **SNMP-Community** gilt für beide. Nach dem Ändern müssen Sie das Gerät neu starten, damit der neue Wert aktiv wird.

SNMP v3 verwenden

Die Seite konfiguriert SNMP v1/v2c. Für SNMP v3 mit Authentifizierung und Verschlüsselung verwenden Sie das `snmpv3`-Skript 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 zur Authentifizierung und AES zur Verschlüsselung. Beide Passwörter müssen mindestens 8 Zeichen lang sein.

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

4. Deaktivieren Sie optional den SNMP v1/v2c-Zugriff, damit nur SNMP v3-Benutzer den Agent lesen können:

   ```
   ./snmpv3 disablev2
   ```

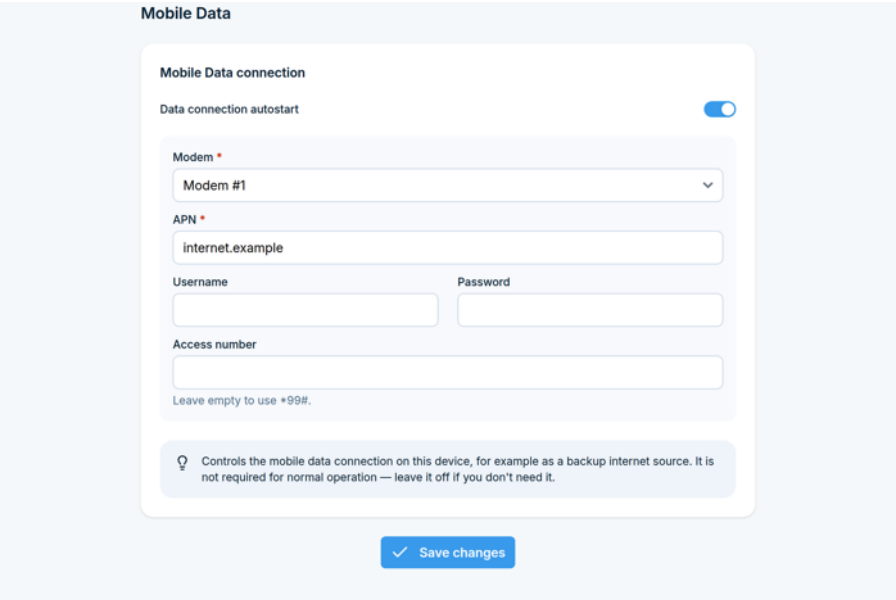
   `./snmpv3 enablev2` aktiviert es wieder, und `./snmpv3 del USERNAME` entfernt den Benutzer.

Das Skript startet den SNMP-Agent selbst neu. Eine v3-Abfrage sieht dann wie folgt 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, beispielsweise als Backup-Internetquelle. Sie ist nicht erforderlich zum Senden oder Empfangen von SMS. Lassen Sie sie ausgeschaltet, wenn Sie sie nicht benötigen.



Mobile Data-Einstellungen

Aktivieren Sie **Data connection autostart**, dann legen Sie fest:

- **Modem** - das Modem, dessen SIM die Datenverbindung trägt.
- **APN** des Betreibers der SIM (erforderlich), sowie **Username** und **Password**, falls der Betreiber diese erfordert.
- **Access number** - lassen Sie dieses Feld 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, aber noch nicht verwendet. 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 (geräteweiter Standard) und **Country dial code** (wird verwendet, wenn eine Telefonnummer ohne diesen eingegeben wird).

Sicherheit

- **Force MFA** - For all users, For new users oder Do not force (gleiche Auswirkung wie die geräteweite MFA-Einstellung des Assistenten, siehe MFA).
- **Password complexity verification** – erzwingt die Kennwortregeln (Länge, gemischte Groß- und Kleinschreibung, Zahl, Sonderzeichen) für jeden Benutzer.
- **Access to DB for external applications** – aktiviert direkten PostgreSQL-Zugriff für externe Anwendungen, standardmäßig deaktiviert. Vollständige Verbindungsdetails und SQL-Beispiele werden separat unter Advanced behandelt, da dies ein eigenständiges Thema für erfahrene Benutzer ist.

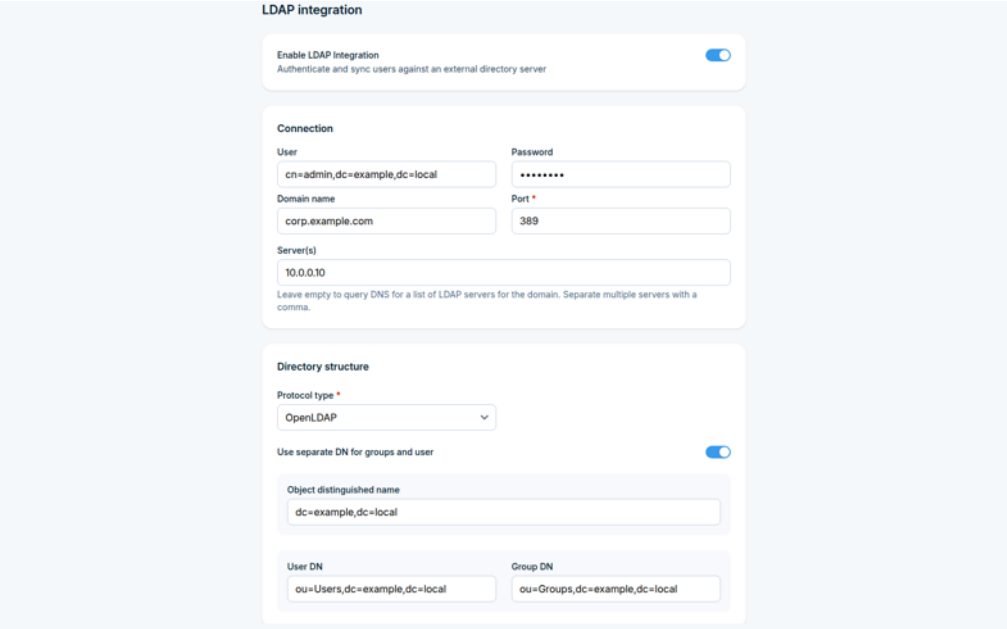
Zugriff und Sichtbarkeit

- **Inbox content visibility** - For all users, Only for admins oder Only messages from the modems assigned to the user (Modems werden pro Benutzer unter **System > Users** zugewiesen).
- **Email inbox content visibility** - For all users oder Only for admins.
- **Berichterstattungsmodul zugänglich für** - Alle Benutzer oder Nur Administratoren.

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 Nachrichtentexte werden weggelassen. Die Datei wird nicht im Log-Browser unter **System > Logs** angezeigt, aber **Download logs** auf dieser Seite enthält sie. Aktivieren Sie diese Option während der Einrichtung oder beim Debuggen einer Integration.
- **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 gesendet. Aktivieren Sie diese Option, wenn 3CX-Benutzer nationale Zeichen senden.

LDAP



LDAP-Integrationseinstellungen

Was diese Funktion bewirkt

Die LDAP-Integration verbindet SMSEagle mit Ihrem Unternehmensverzeichnis, beispielsweise Active Directory oder OpenLDAP. Sie erfüllt zwei separate Aufgaben, und Sie können eine oder beide verwenden:

Aufgabe	Das erhalten Sie
Kontakte	Das Telefonbuch wird aus dem Verzeichnis gefüllt, sodass Sie Nachrichten an die gleichen Personer Unternehmen bereits verwaltet, ohne Nummern doppelt einzutippen.
Authentifizierung	Benutzer melden sich bei SMSEagle mit ihrem Verzeichniskonto an, und ihre Berechtigungsstufe wir gehörigkeit festgelegt.

Typische Anwendungen: Automatisches Synchronisieren des Telefonbuchs mit Personalveränderungen und Ermöglichung für Benutzer, ihr bestehendes Unternehmenspasswort anstelle eines separaten SMSEagle-Passworts zu verwenden.

Bevor Sie beginnen

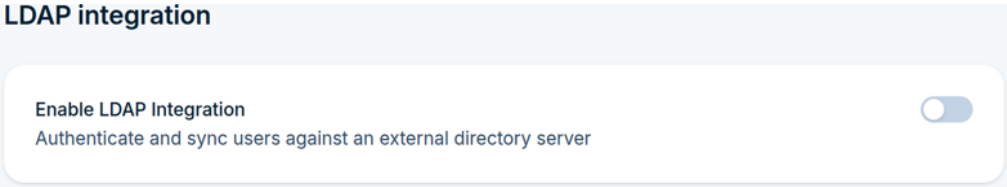
Beschaffen Sie diese Informationen von demjenigen, der das Verzeichnis verwaltet:

- Der **Domänenname** und der **Port** (389 für einfaches LDAP, normalerweise 636 mit SSL).
- Ein **Servicekonto** (Benutzer und Passwort), das das Verzeichnis lesen darf.
- Der **Distinguished Name** der Niederlassung, die Ihre Benutzer enthält, beispielsweise `ou=Users,dc=company,dc=local`, und die Niederlassung mit Gruppen, wenn diese unterschiedlich ist.
- Welches **Attribut** die Telefonnummer enthält, an die Sie eine Nachricht senden möchten.
- Wenn Sie die Verzeichnisanmeldung wünschen: die Namen der Gruppen, deren Mitglieder SMSEagle-Administratoren und normale Benutzer werden sollten.

Schritt 1: LDAP-Seite öffnen

Gehen Sie in der Seitenleiste zu **Settings > Global settings > LDAP** (Einstellungen > Globale Einstellungen > LDAP).

Die Seite beginnt mit einem einzelnen Schalter, **Enable LDAP Integration** (LDAP-Integration aktivieren). Bis Sie diesen aktivieren, wird nichts Weiteres angezeigt.



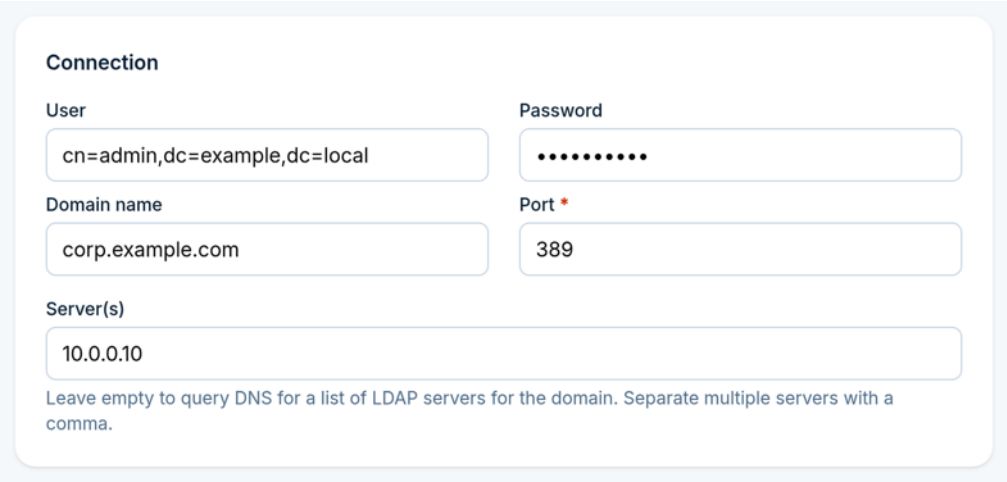
Mit deaktivierter Integration zeigt die Seite nur den Schalter

Schritt 2: Integration aktivieren

Aktivieren Sie **Enable LDAP Integration** (LDAP-Integration aktivieren). Vier Abschnitte werden angezeigt: **Connection** (Verbindung), **Directory structure** (Verzeichnisstruktur), **Attributes and security** (Attribute und Sicherheit) und **Sync and access** (Synchronisierung und Zugriff).

Schritt 3: Verbindung

Feld	Was Sie eingeben sollten
Benutzer	Das Dienstkonto zum Lesen des Verzeichnisses.
Passwort	Sein Passwort. Das Feld wird leer angezeigt, wenn Sie zur Seite zurückkehren; lassen Sie es leer, um das gespeicherte Passwort beizubehalten.
Domänenname	Die Verzeichnisdomäne, zum Beispiel `company.local`.
Port	389 für einfaches LDAP, 636 für LDAP über SSL. Erforderlich.
Server	Spezifische Server, durch Kommas getrennt, zum Beispiel `ldap1.company.local, ldap2.company.local`. Lassen Sie das Feld leer, damit das Gerät die Server für die Domäne im DNS nachschlägt.



Verbindungsabschnitt, ausgefüllt mit Beispielwerten

Schritt 4: Verzeichnisstruktur

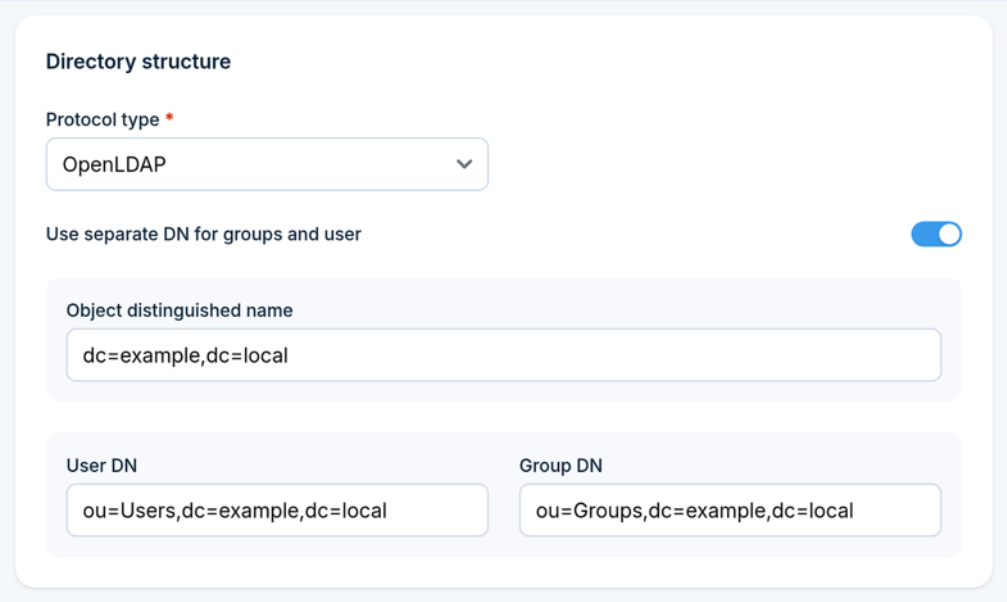
Protokolltyp Wählen Sie **Active Directory** oder **OpenLDAP**, je nach Ihrem Server.

Separate DN für Gruppen und Benutzer verwenden Lassen Sie dies aus, wenn sich Benutzer und Gruppen in demselben Zweig befinden. Ein Feld wird dann angezeigt:

- **Objekt-Distinguished Name**, zum Beispiel `ou=Users,dc=smseagle,dc=local`.

Aktivieren Sie dies, wenn sie in verschiedenen Zweigen vorhanden sind. **Objekt-Distinguished Name** bleibt erhalten, und zwei weitere Felder erscheinen darunter:

- **Benutzer-DN**, zum Beispiel `ou=Users,dc=smseagle,dc=local`
- **Gruppen-DN**, zum Beispiel `ou=Groups,dc=smseagle,dc=local`



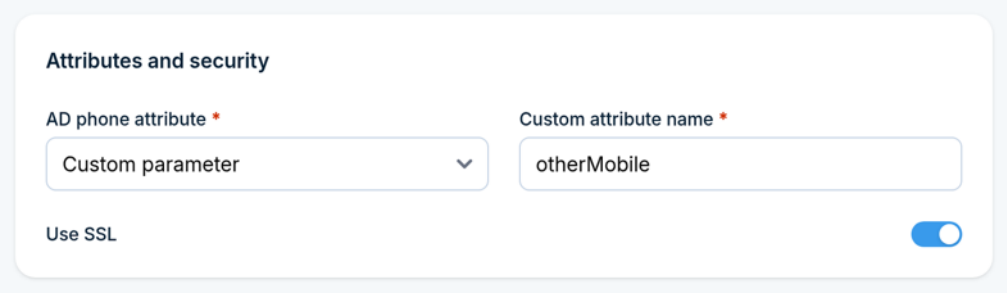
Verzeichnisstruktur mit separaten DNs aktiviert

Schritt 5: Attribute und Sicherheit

AD-Telefonattribut Welches Verzeichnisattribut enthält die Nummer, an die SMSEagle SMS senden soll: **Telefonnummer**, **Mobilfunknummer**, **Heimnummer**, **Pagernummer**, **Faxnummer**, **IP-Telefonnummer** oder **Benutzerdefinierten Parameter**.

Wenn Sie **Benutzerdefinierten Parameter** wählen, wird **Benutzerdefinierten Attributnamen** angezeigt, in dem Sie das Attribut selbst eingeben können, zum Beispiel `otherMobile`. Es werden nur einfache Attributnamen akzeptiert; Satzzeichen wie `< > / \ : ; , . + ' " & =` werden abgelehnt.

SSL verwenden Aktivieren Sie dies, um die Verbindung zum Verzeichnis zu verschlüsseln. Denken Sie daran, den entsprechenden **Port** im Verbindungsabschnitt festzulegen.



Attribute und Sicherheit, mit ausgewähltem **benutzerdefinierten Parameter** und SSL aktiviert

Schritt 6: Synchronisierung und Zugriff

Methode zum Abrufen von Kontakten und Gruppen

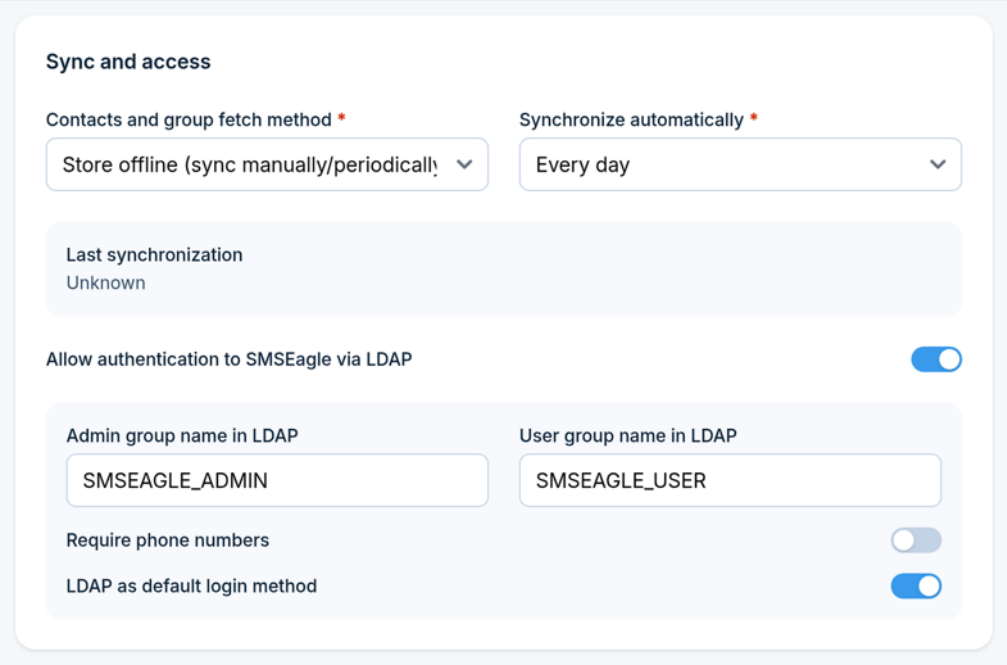
Option	Was geschieht
Vom LDAP-Server abrufen	Kontakte und Gruppen werden jedes Mal aus dem Verzeichnis gelesen, wenn sie benötigt werden. Immer aktuell, aber jeder Lookup hängt davon ab, dass das Verzeichnis erreichbar ist.
Offline speichern (manuell/ regelmäßig synchronisieren)	Eine Kopie wird auf dem Gerät gespeichert. Messaging funktioniert weiterhin, wenn das Verzeichnis nicht erreichbar ist, allerdings auf Kosten einer leicht veralteten Kopie.

Wenn Sie **Offline speichern** wählen, erscheint **Automatisch synchronisieren**: **Nie**, **Jede Stunde**, **Täglich**, **Wöchentlich** oder **Monatlich**. **Nie** bedeutet, dass die Kopie nur aktualisiert wird, wenn Sie eine Synchronisierung selbst auslösen.

Letzte Synchronisierung unter der Abrufmethode ist schreibgeschützt und zeigt, wann die Offline-Kopie zuletzt aktualisiert wurde. Sie lautet Unbekannt, bis die erste Synchronisierung ausgeführt wird.

Authentifizierung bei SMSEagle über LDAP zulassen Aktivieren Sie diese Option, um Benutzern die Anmeldung mit ihrem Verzeichniskonto zu ermöglichen. Es erscheinen vier weitere Felder:

- **Administratorgruppenname in LDAP** - Mitglieder dieser Gruppe melden sich als Administratoren an.
- **Benutzergruppenname in LDAP** - Mitglieder dieser Gruppe melden sich als normale Benutzer an.
- **Telefonnummern erforderlich** - nur Verzeichniskonten mit einer Nummer im gewählten Telefonattribut dürfen sich anmelden. Standardmäßig deaktiviert.
- **LDAP als Standard-Anmeldemethode** - wählt LDAP statt Lokal im Authentifizierungstyp des Anmeldeformulars vor, sodass Verzeichnisbenutzer ihn nicht jedes Mal ändern müssen.



Synchronisierung und Zugriff mit aktiviertem Offline-Speicher und Verzeichnisanmeldung

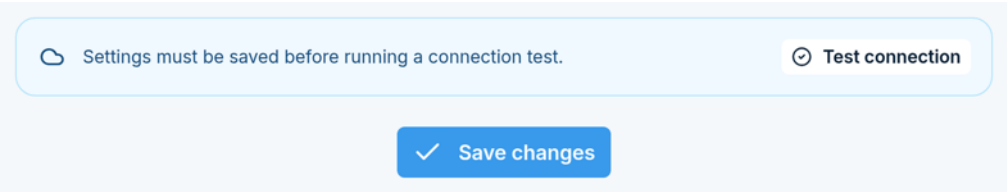
Überprüfen Sie die Gruppennamen, bevor Sie sich auf sie verlassen. Ein Mitglied von keiner Gruppe kann sich nicht anmelden, und ein Tippfehler im Administratorgruppenname wird erst bemerkt, wenn niemand das Gerät administrieren kann. Halten Sie mindestens ein lokales SMSEagle-Administratorkonto funktionsfähig, bis Sie eine Verzeichnisanmeldung verifiziert haben.

Schritt 7: Speichern und testen

Klicken Sie unten auf der Seite auf **Save changes**.

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

Speichern Sie zuerst, testen Sie dann. Der Test verwendet die gespeicherten Einstellungen, nicht das aktuelle Bildschirminhalt. Wenn Sie vor dem Speichern testen, überprüfen Sie die vorherige Konfiguration. Der Hinweis neben der Schaltfläche besagt dasselbe.



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

Datum / Zeit

Settings > Global settings > Date / Time (`/settings/datetime/`) zeigt das aktuelle Systemdatum und die aktuelle Systemzeit (schreibgeschützt) an und ermöglicht es Ihnen, Folgendes einzustellen:

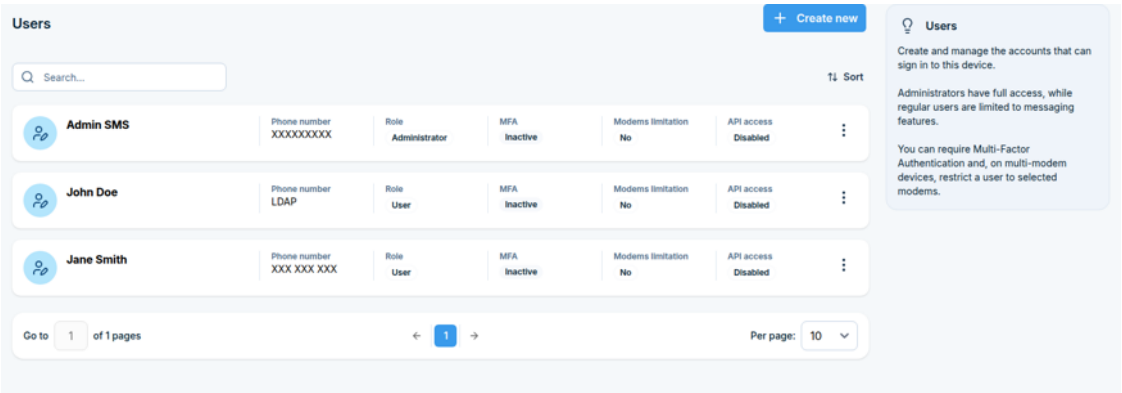
- **Zeitzone**
- **NTP-Zeitsynchronisierung** - wenn aktiviert, wird **NTP-Serveradresse** angezeigt. Wird auch während des Configuration Wizard angeboten.

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.



Benutzer im Bereich „System

Für jeden Benutzer können Sie die **Access level** (Administrator oder User) festlegen, Multi-Factor Authentication anfordern und auf Multi-Modem-Geräten einen Benutzer auf ausgewählte Modems beschränken. Der API-Zugriff (siehe API and Developer Integration) wird auch pro Benutzer von hier aus gewährt.

Systeminformationen

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

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

Protokolle

System > Logs (`/system/logs/`) ermöglicht es Ihnen, die Protokolle des Geräts zu durchsuchen und anzuzeigen, gruppiert nach Pro-Modem-Protokollen und Systemprotokollen (Database, System, Application, Message). Verwenden Sie **Search by phrase** zum Filtern oder **Download logs**, um sie für den Support zu speichern. Protokolle 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 nach Updates zu suchen. Sie können das Gerät auch per SMS benachrichtigen lassen, wenn eine neue Version verfügbar ist. Dieselbe Seite zeigt die Gültigkeit des technischen Supports an und ermöglicht es Ihnen, dies auch automatisch zu überprüfen.

Patches

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

Backup / Restore

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

- **Manual backups** - Erstellen Sie bei Bedarf ein Backup der Datenbank und der Geräteeinstellungen.
- **Automatic backups** - Aktivieren Sie geplante Sicherungen auf einem SFTP/FTP(S)-Server mit Bereinigung alter Sicherungsversionen.
- **Restore data** - Stellen Sie die Datenbank aus einer Sicherungsdatei wieder her.

Neustart

System > Restart (`/system/restart/`) startet das Gerät bei Bedarf neu – Senden und Empfangen sind erst wieder verfügbar, wenn es wieder online ist – oder ermöglicht es Ihnen, einen geplanten Neustart auf Basis eines wiederkehrenden Plans zu aktivieren.

Erweitert

Direkter Datenbankzugriff und andere Themen für erfahrene Benutzer finden Sie in einem eigenen Kapitel: siehe Advanced.

API und Entwicklerintegrationen

SMSEagle bietet eine leistungsstarke integrierte REST-API. Die API ist für die Integration von SMSEagle mit jedem externen System oder jeder Anwendung konzipiert.

API-Referenz

SMSEagle bietet zwei API-Versionen:

- **API v2 – empfohlen, verwenden Sie es für jede neue Integration.** Eine moderne RESTful-API basierend auf der OpenAPI-3.0-Spezifikation. API v2-Referenz
- **API v1 – die Legacy-API, nur zur 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 Inhalts der API-Dokumentation wird sie als separates Dokument gepflegt. Folgen Sie den obigen Links für die vollständige Spezifikation jeder API.

API-Schlüssel

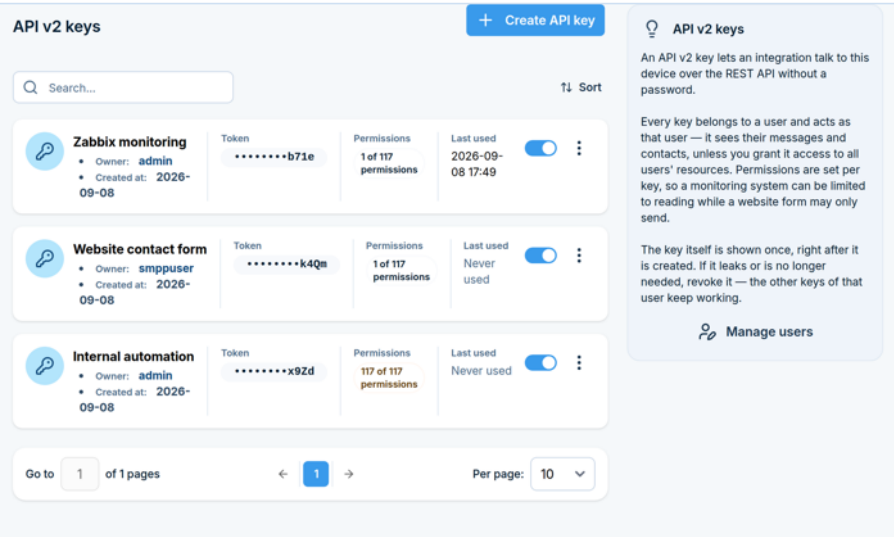
Eine Integration authentifiziert sich mit einem **API-Schlüssel** statt mit einem Benutzerpasswort. Schlüssel werden für jede API-Version separat auf zwei Seiten gespeichert:

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

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

API v2-Schlüssel

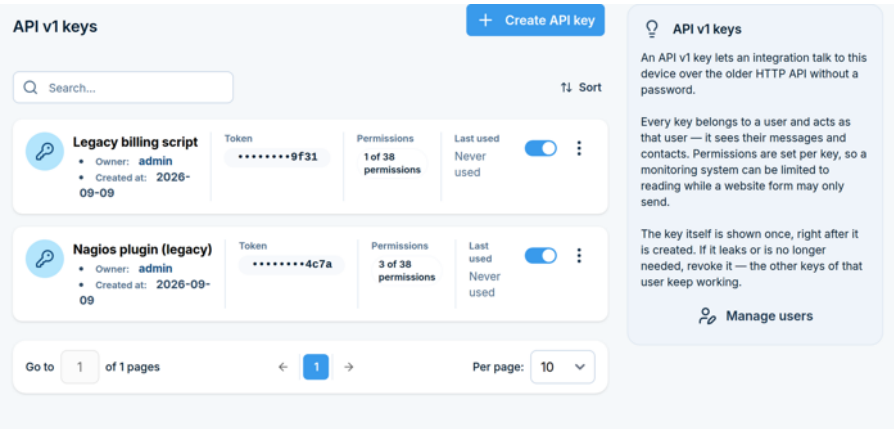
Dies ist die Seite für eine neue Integration.



API v2-Schlüssel

API v1-Schlüssel

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



API v1-Schlüssel

Schlüssel erstellen

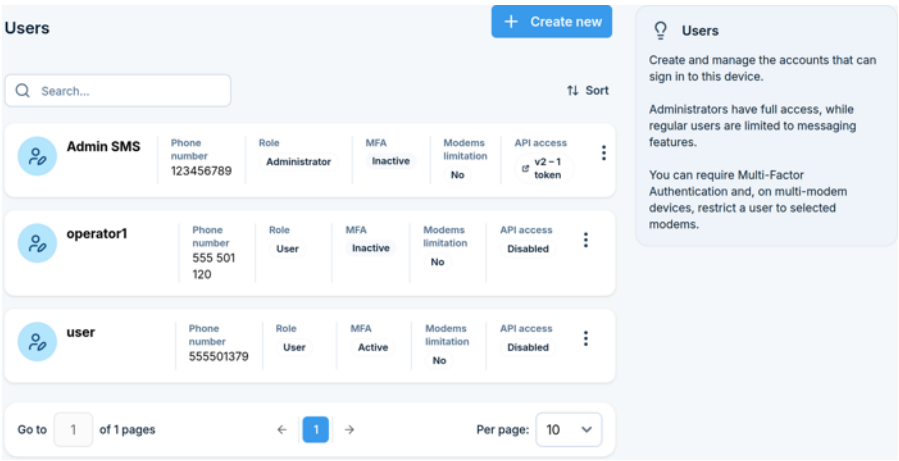
Create API key öffnet das Formular für die API-Version, deren Seite Sie sich ansehen:

Feld	Was es macht
Key name	Wie Sie diese Integration später erkennen, zum Beispiel Zabbix oder Website form.
Owner	Der Benutzer, als der der Schlüssel agiert. 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 deaktiviert, 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 aktivieren.

Der Schlüssel wird genau nach seiner Erstellung einmal angezeigt. 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 > Benutzer zeigt pro Benutzer, wie viele API-Schlüssel der Benutzer hat und für welche API-Version. Das Symbol 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 breit ein API-Schlüssel Daten anderer Benutzer einsehen kann:

- In **API v1** hat ein Schlüssel standardmäßig Zugriff auf Ressourcen aller anderen Benutzer – Kontakte im Telefonbuch, Gruppen und so weiter.
- 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 **Zugriff auf Ressourcen aller Benutzer** auf dem Schlüssel.

Plugins und Integrationen

SMSEagle kann mit externer Software wie Netzwerküberwachungssystemen, 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 Entwicklerintegration.
- **Email zu SMS** – das externe System sendet eine normale E-Mail und SMSEagle konvertiert diese in eine SMS. Es ist keine Programmierung erforderlich, daher funktioniert es mit jeder Software, die bereits E-Mail-Benachrichtigungen senden kann. Siehe Email zu SMS.

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

Für viele populäre Systeme müssen Sie die Integration nicht selbst erstellen. SMSEagle bietet einsatzbereite Plugins und Schritt-für-Schritt-Integrationsanleitungen, und die Liste wächst ständig. Für eine vollständige und aktuelle Liste gehen Sie zu: https://www.smseagle.eu/integration-plugins/

Erweitert

Dieses Kapitel behandelt Themen für fortgeschrittene Benutzer, die den normalen Web-Interface umgehen und direkt mit ihm arbeiten: direkter Datenbankzugriff und SQL sowie Kommandozeilen-Datenbankbereinigungsskripte. Die meisten Benutzer werden dieses Kapitel nie benötigen.

Direkter Zugriff auf die SMSEagle-Datenbank

Die Datenbank von SMSEagle wird mit PostgreSQL betrieben. Sie können direkt darauf zugreifen, um SMS-Nachrichten über SQL-Abfragen zu lesen oder zu schreiben, anstatt über die Web-Oberfläche oder die API zu gehen.

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

Stellen Sie nach der Aktivierung eine Verbindung zur Datenbank von einer externen Anwendung aus her mit:

- Host: die IP-Adresse des Geräts
- Datenbankname: `smseagle`
- Benutzer: `smseagleuser`
- Passwort: `postgreeagle`

Injizieren einer Kurz-SMS mit SQL

Eine Kurznachricht (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 zum Benutzer mit `id_user` 1 (dem Standard-Benutzer `admin`) – die `id_user`-Werte anderer Benutzer finden Sie in der Tabelle `public."user"`. Das Feld `SenderID` bezeichnet, welches Modem die Nachricht sendet: `smseagle1` für Modem 1, `smseagle2` für Modem 2.

Injizieren einer Langtext-SMS mit SQL

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

Bei einer Langtextnachricht beginnt der UDH mit `050003`, gefolgt von einem Byte, das als Nachrichtenreferenz verwendet wird (ein beliebiger Hexadezimalwert, aber unterschiedlich für jede Nachricht – `D3` unten), einem Byte für die Gesamtzahl der Teile (`02` unten, eindeutig pro an die gleiche Nummer gesendete Nachricht) und einem Byte für die aktuelle Teilenummer (`01` für den ersten Teil, `02` für den zweiten usw.).

Eine zweiteilige Langnachricht sieht folgendermaßen 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 lässt weniger Platz für Text – das obige Beispiel ermöglicht nur 153 Zeichen pro Nachrichtenteil.

Datenbankbereinigungsskripte

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

Skript	Verwendung	Zweck
`db_delete`	`./db_delete YYYYMMDDhhmm`	SMS aus Inbox und SentItems löschen, die älter als das angegebene Datum sind
`db_delete_7days`	`./db_delete_7days`	SMS aus Inbox und SentItems löschen, die älter als 7 Tage sind
`db_delete_allfolders`	`./db_delete_allfolders`	Inbox, SentItems und Outbox bereinigen – konzipiert für regelmäßige Ausführung über cron
`db_delete_select`	`./db_delete_select {inbox|outbox|sentitems|trash}`	SMS aus einem gewählten Ordner löschen

Skript zu cron hinzufügen: erstellen Sie eine Datei unter `/etc/cron.d/` (zum Beispiel `db_cleaner`) mit folgendem Inhalt:

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

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

Weitergabe von Logs an einen externen Server

SMSEagle schreibt seine Logs über rsyslog. Um eine Kopie davon an einen zentralen Syslog-Server zu senden, fügen Sie eine Weiterleitungsregel über SSH hinzu. Es gibt keine Einstellung dafür in der Weboberfläche.

1. Melden Sie sich über SSH als `root` am Gerät an.
2. Erstellen Sie die Datei `/etc/rsyslog.d/005-remote.conf` mit dieser Regel, 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 Warteschlangeneinstellungen behalten 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 dann rsyslog neu:

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

Behalten Sie den Dateinamen bei. SMSEagles eigene Logs (Application, API, Message und die E-Mail-, Anruf-, 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 danach platziert ist, beispielsweise am Ende von `/etc/rsyslog.conf`, leitet nur die Systemlogs weiter. Das Präfix `005-` bewirkt, dass rsyslog die Weiterleitungsregel zuerst liest, sodass jede Nachricht weitergeleitet wird.

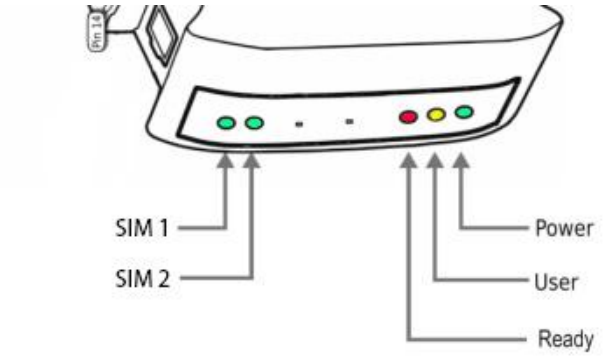
Um den Log-Datenverkehr mit TLS zu verschlüsseln, siehe das rsyslog-Handbuch Encrypting Syslog Traffic with TLS.

Fehlerbehebung

Um sicherzustellen, dass das Gerät ordnungsgemäß funktioniert, folgen Sie diesen drei Schritten:

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

Überprüfung der LEDs



LED-Positionen

Der normale Betrieb des Geräts wird durch LEDs wie folgt signalisiert:

LED	Korrekte Funktion
Power (PWR)	Kontinuierlich leuchtend
User	Blinkt während Flashdisk-Lese-/Schreibvorgängen
Ready (RDY)	Blinkend
SIM1 NXS-9750-3G	Langsames Blinken im Standby-Modus, schnelles Blinken bei Verwendung von Modem 1
SIM2 NXS-9750-3G	Nicht verwendet

Überprüfung der Geräteinformationen

Die Geräteinformationen (Gerätetyp, Softwareversion, Modem IMEI, IMSI, Netzwerksignalstärke, Netzwerkname) finden Sie unter **System > System info**. Siehe System.

Geräteprotokolle

Unter **System > Logs** finden Sie die neuesten Zeilen der Geräteprotokolle: Modemprotokoll, Datenbankprotokoll und Systemprotokoll. Im Falle von Problemen mit dem Gerät sind diese Protokolle eine wertvolle Quelle für Informationen zur Fehlerbehebung.

Erweiterte Geräteprotokolle können über die Schaltfläche **Download logs** auf derselben Seite heruntergeladen werden. Siehe System.

Wenn das Gerät nicht erreichbar ist

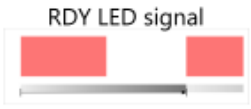
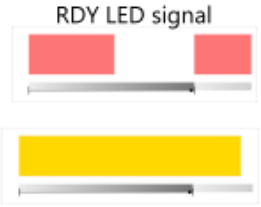
1. Überprüfen Sie, ob das Gerät korrekt mit dem Netzwerk verbunden ist. Überprüfen Sie den LED-Status der RJ45-Buchse.
2. Wenn das Gerät aufgrund einer Störung oder falscher Benutzereinstellungen nicht reagiert, starten Sie das Gerät neu, indem Sie die Stromversorgung trennen und erneut verbinden (oder den Reset-Schalter drücken).
3. Wenn Sie immer noch keine Verbindung zum Gerät herstellen können, können die werkseitigen IP-Einstellungen mit dem SW-Schalter wiederhergestellt werden.

Wiederherstellen von Werkseinstellungen

Die Funktion „Zurücksetzen auf Standardeinstellungen

> **Warnung**
>
> Das Zurücksetzen auf Werkseinstellungen entfernt permanent die aktuelle Benutzerkonfiguration. Stellen Sie sicher, dass alle erforderlichen Einstellungen oder Daten gesichert werden, bevor Sie fortfahren.

Um das Zurücksetzen einzuleiten, drücken und halten Sie die SW-Taste 10 Sekunden lang. Das Gerät wechselt in den Wiederherstellungsmodus.

LED-Signalisierung	USER-Aktionen	Systemreaktion
	1. **When the device is ready to operate**	–
–	2. **Press and hold SW button for 10 seconds**	Wiederherstellungsdienst läuft ab.
	3. **Release SW button after 10 seconds.** User LED will begin to blink.	Das System liest Werkseinstellungen. Werksvorgaben 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 nutzt eine dedizierte schreibgeschützte Wiederherstellungspartition, um sicherzustellen, dass das Wiederherstellungsabbild intakt bleibt und nicht durch den normalen Gerätebetrieb beeinträchtigt wird. Nach Eintritt in den Wiederherstellungsmodus startet ein 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 in eine Service-Shell für Diagnosen.

Hardware Rev.3–Rev.4

Rev.3 Rev.4

Die Zurücksetzen-Funktion stellt nur folgende Einstellungen auf ihre Standardwerte zurück: IP-Einstellungen, Zeitzoneeinstellungen, Datenbankinhalt und Linux-OS-Benutzer/Passwörter.

Service & Reparatur

Garantie

Ihr SMSEagle wird mit 2 Jahren Standard-Technischer Support und Hardwarereparatur-Garantieabdeckung geliefert. Die Standardgarantie kann während des Gerätekaufs auf 3 Jahre verlängert werden (überprüfen Sie Ihre Kaufbedingungen). Detaillierte Informationen zu Garantiebedingungen finden Sie auf der Garantiekarte, die mit Ihrem Gerät mitgeliefert wird, oder folgen Sie dem Link: www.smseagle.eu/downloads

Service

Bevor Sie sich an das Support-Team wenden, stellen Sie sicher, dass Sie den Abschnitt Fehlerbehebung in diesem Handbuch gelesen haben. Weitere Informationen und hilfreiche Hinweise zur SMSEagle-Gerätekonfiguration finden Sie auch in unserer Online-Wissensdatenbank unter der gleichen Adresse wie das Support-Portal unten.

Das SMSEagle Support-Team ist per E-Mail oder Telefon erreichbar.

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, Polen

Bereiten Sie die folgenden Informationen vor, wenn Sie sich an das Support-Team wenden:

Systemprotokolle

Gehen Sie zu **System > Logs > Download logs**. Stellen Sie das Protokollpaket dem Support-Team auf Anfrage zur Verfügung.

MAC-Adresse

Jedes SMSEagle-Gerät hat eine eindeutige MAC-Adresse. Sie ist auf dem Gerät aufgedruckt oder kann unter **System > System info** gefunden werden.

Technische Spezifikationen & 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-/Ausgabeanschlusstypen: DI-Typ „Pull-up-Widerstand“. DO-Typ „Open Collector“
- RTC-Uhr: RTC 240B SRAM, Watchdog-Timer
- Interner Feuchte- & Temperatursensor: Genauigkeit ± 0,5 °C, ±2 %RH
- Stromverbrauch:
  - hardware Rev.5, Rev.4: max 35W
  - hardware Rev.3: max 20W
- Geräuschpegel: Lüfterlos
- Abmessungen: (Breite x Tiefe x Höhe) 45 × 120 × 101 mm
- Gewicht: 350g
- Gehäuse: ABS, DIN-Hutschienen-Installation
- Betriebsparameter:
  - Betriebstemperatur: 0 ~ 40°C
  - Luftfeuchtigkeit: 8 ~ 90% RH (keine Kondensation)

- 2x Internes Modem

Gerätetyp NXS-9750-4G Rev.4 Rev.5

- Wellenbereiche: 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-9750-4G Rev.3

- Wellenbereich: UMTS, LTE
- LTE-Bänder: LTE FDD: 1–5, 7, 8, 12, 13, 17, 20, 25, 26, 28, 29, 30 (nur Empfang), 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-9750-3G Rev.3

- Wellenbereich: 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-Karten-Standard: mini
- Antennenverbinder: SMA
- Herkunftsland: Europäische Union (Polen)

Stromversorgung

- Hardware Rev.5, Rev.4:
  - Externes Netzteil mit Ausgangsschaltung bewertet ES1 (12Vdc; min. 3,3A), PS2 (LPS – Limited Power Source). AC-Netzeingang:
    - Spannungsbereiche: 100–240V Wechselstrom (AC)
    - Frequenz: 50–60Hz Einphase
    - DC-Steckertyp: 5.5/2.5
  - Alternative Stromquelle: PoE+ (IEEE 802.3at Type 2). Mit PoE+ versorgter Schaltkreis: bewertet ES1 (50-57Vdc; 30W), PS2 (LPS – Limited Power Source)
- Hardware Rev.3:
  - Externes Netzteil mit Ausgangsschaltung bewertet ES1 (12Vdc; min. 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-9750-4G:
  - 2x omnidirektionale 2dBi-Antenne mit Magnetfuß
  - Wellenbereich: UMTS, LTE
  - Kabellänge 3m
  - Steckertyp: SMA
  - Impedanz: 50 Ohm
- Gerätetyp NXS-9750-3G:
  - 2x omnidirektionale 3dBi-Antenne mit Magnetfuß
  - Wellenbereich: GSM, UMTS
  - Kabellänge 3m
  - Steckertyp: SMA
  - Impedanz: 50 Ohm

Durchsatz beim Senden/Empfangen

- Eingangsübertragungsrate: bis zu 60 SMS/min
- Ausgangsübertragungsrate: bis zu 60 SMS/min

Software-Plattform

- 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 (HA-Cluster)-Service
- 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 nur auf localhost)
  - UDP: 68 (DHCP-Client), 323 (NTP-Client)

Wichtige Sicherheitsinformationen

Dieses Kapitel enthält wichtige Informationen zu Sicherheitsverfahren. Folgen Sie für Ihre Sicherheit und die Sicherheit Ihrer Ausrüstung diesen Regeln zum Umgang mit Ihrem Gerät.

> **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.

Treffen Sie immer die folgenden Vorsichtsmaßnahmen.

Trennen Sie das Netzkabel von der Stromquelle oder falls eine der folgenden Bedingungen vorliegt:

- das Netzkabel oder der Stecker wird ausgefranst oder anderweitig beschädigt
- Sie verschütten etwas in das Gehäuse
- das Gerät ist Regen oder anderer übermäßiger 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 es Explosionsrisiko gibt, wie Tankstellen, Ölraffinerien usw.

Es ist die Verantwortung des Benutzers, die Landesbestimmungen und die spezifischen Umgebungsbestimmungen durchzusetzen.

Zerlegen Sie das Produkt nicht; jedes Zeichen von Manipulationen 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 einer minimalen Entfernung von 31 cm (12,2 Zoll) vom Körper installiert werden. Falls diese Anforderung nicht erfüllt werden kann, muss der Systemintegrator das Endprodukt gemäß der SAR-Bestimmung bewerten.

HAFTUNGSAUSSCHLUSS: Der Hersteller ist nicht verantwortlich für Schäden, die durch unsachgemäße Installation, Nichtbeachtung des ordnungsgemäßen technischen Zustands oder die Verwendung eines Produkts gegen seinen Bestimmungszweck verursacht werden.

Behördliche Erklärungen

EU-Konformitätserklärung

Hiermit erklärt Proximus Sp. z o.o., Eigentümer der Marke SMSEagle, dass der Funkgerätetyp SMSEagle NXS-9750-3G, NXS-9750-4G der Richtlinie 2014/53/EU entspricht.

Der vollständige Text der EU-Konformitätserklärung ist unter folgender Internetadresse verfügbar: www.smseagle.eu/certification

FCC-Konformitätserklärung

Dieses Gerät entspricht Teil 15 der FCC-Bestimmungen. 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-Bestimmungen. Diese Grenzwerte sind so ausgelegt, dass sie in einer geschäftlichen/kommerziellen Nicht-Wohnumgebung angemessenen Schutz vor schädlichen Störungen bieten. Es gibt jedoch keine Garantie dafür, dass Störungen bei einer bestimmten Installation nicht auftreten. Falls dieses Gerät zu schädlichen Störungen des Radio- oder Fernsehempfangs führt, was durch Aus- und Einschalten des Geräts bestimmt werden kann, wird der Benutzer aufgefordert, die Störungen durch eine oder mehrere der folgenden Maßnahmen zu beheben:

- Reorientierung oder Umpositionierung der Empfängerantenne
- Vergrößerung des Abstands zwischen Gerät und Empfänger
- Anschluss des Geräts an eine Steckdose in einem anderen Stromkreis als der des Empfängers
- Konsultation des Händlers oder eines erfahrenen Funk-/Fernsehtechnikers um Hilfe

Wichtig:

Dieses Gerät erzeugt, nutzt und kann Hochfrequenzenergie abstrahlen und kann, wenn es nicht gemäß der Bedienungsanleitung des Herstellers installiert und verwendet wird, zu schädlichen Störungen der Funkkommunikation führen. Der Betrieb dieses Geräts in einem Wohngebiet wird wahrscheinlich zu schädlichen Störungen führen, in welchem Fall Sie aufgefordert werden, die Störungen auf eigene Kosten zu beheben. Die FCC-Bestimmungen sehen vor, dass Änderungen oder Modifizierungen, die nicht ausdrücklich von SMSEagle™ genehmigt wurden, Ihre Betriebserlaubnis für dieses Gerät ungültig machen könnten. 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 des Titels 47 des Code of Federal Regulations ausgestellt von:

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

Das Produkt NXS-9750-3G, NXS-9750-4G entspricht den anwendbaren Anforderungen der FCC-Bestimmung Teil 15B für die entsprechenden Geräteklassen der ungezielten Strahler.

VERANTWORTLICHE STELLE in den Vereinigten Staaten:

Testing Partners LLC

18200 SR 306

Chagrin Falls, OH 44023

info@testingpartners.com

Die verantwortliche Stelle garantiert, dass jedes unter dieser Konformitätserklärung vermarktete Gerät identisch mit dem getesteten und akzeptierten Gerät ist und die Standards erfüllt, und dass die von der verantwortlichen Stelle geführten Aufzeichnungen weiterhin widerspiegeln, dass die unter dieser Konformitätserklärung des Lieferanten hergestellten Geräte weiterhin mit der Variation entsprechen, die aufgrund der Massenproduktion und statistischen Prüfung zu erwarten ist.

Kanadische behördliche Erklärung (ISED)

Dieses Gerät entspricht den lizenzfreien RSS-Standards der Industry Canada. Der Betrieb unterliegt den folgenden zwei Bedingungen:

(1) dieses Gerät darf keine Störungen verursachen, und

(2) dieses Gerät muss alle empfangenen 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

Hiermit erklärt Proximus Sp. z o.o., Eigentümer der Marke SMSEagle, dass die Funkgerätetypen SMSEagle NXS-9750-3G, NXS-9750-4G der Funk-Geräte-Richtlinie 2017 entsprechen.

Der vollständige Text der EU-Konformitätserklärung ist unter folgender Internetadresse verfügbar: www.smseagle.eu/certification

RF-Expositionsgrenzen

Dieses Gerät erfüllt die Grenzwerte für die Strahlenexposition in einer unkontrollierten Umgebung. Um die Möglichkeit zu vermeiden, die Hochfrequenz-Expositionsgrenzen zu überschreiten, darf die menschliche Nähe zur Antenne während des normalen Betriebs nicht weniger als 30 cm (12 Zoll) betragen.

Entsorgung und Recyclinginformationen

Ihr SMSEagle-Gerät enthält eine Lithium-Batterie für die RTC-Sicherung. Entsorgen Sie das Gerät und/oder die Batterie gemäß den geltenden Umweltgesetzen und Richtlinien.

Europäische Union – Entsorgungsinformationen



Das obige Symbol bedeutet, dass Ihr Produkt gemäß lokalen Gesetzen und Vorschriften getrennt vom Hausmüll entsorgt werden muss. Wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat, bringen Sie es zu einer von den lokalen Behörden bestimmten Sammelstelle. Die getrennte Erfassung und das Recycling Ihres Produkts bei der Entsorgung helfen, natürliche Ressourcen zu

schonen 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 die zuständigen Behörden oder den Händler vor Ort 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

Richtlinie zur Beschränkung gefährlicher Stoffe (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“).