DOKUMENTATION 7.00

MHD-8100 Benutzerhandbuch

Dokumentation

DEUTSCH · SMSEAGLE

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

Table of contents

Deckblatt . . . 8

Informationen zur SMSEagle-Softwarelizenzierung . . . 9

Was ist in der Box . . . 18

Konfigurationsassistent . . . 19

- Schritt 1: Sprache & Zeit . . . 19
- Schritt 2: Administratorkonto . . . 19
- Schritt 3: Benachrichtigungen . . . 20
- Schritt 4: Modems . . . 21

Anschlüsse, Anschlussports und LEDs . . . 22

- Frontplatte . . . 23
- Rückplatte . . . 23
- Display . . . 23

Übersicht der Weboberfläche . . . 27

- Anmelden . . . 27
- Schnittstellenlayout . . . 28
- Dashboard . . . 28
  - Benötigt Ihre Aufmerksamkeit . . . 29
  - Verkehr . . . 29
  - Ungelesene Nachrichten . . . 30
  - System . . . 30
  - Neueste Nachrichten und Anrufe . . . 31
  - Modems . . . 31
- Schnellaktionen . . . 31
- Persönliche Kontoeinstellungen . . . 32
  - Persönliche Daten . . . 32
  - Passwort . . . 33
  - Sicherheit . . . 33

Nachrichten . . . 34

- SMS (Unterhaltungen) . . . 34
  - Eine Nachricht verfassen . . . 35
- Ordner . . . 36
- Gruppennachrichten . . . 37
- Eskalationswarteschlange . . . 38
- Anrufe . . . 39
  - Verlauf . . . 39
- WhatsApp . . . 40
- Signal . . . 42
- E-Mails . . . 43
- Nachrichtenvorlagen . . . 43

Telefonbuch . . . 45
Kontakte . . . 45
Gruppen . . . 45
Eskalationsgruppen . . . 46
Schichten . . . 48
Bevor Sie beginnen . . . 48
Schritt 1: Öffnen Sie die Seite „Shifts“ . . . 48
Schritt 2: Erstellen Sie eine Schicht . . . 48
Schritt 3: Weisen Sie Kontakte der Schicht zu . . . 49
Schritt 4: Wählen Sie, was außerhalb der Schichtzeiten geschieht . . . 49

Automatisierung . . . 50
E-Mail zu SMS . . . 50
Wo finde ich diese Funktion . . . 50
Schritt 1: Understand the recipient address format . . . 50
Schritt 2: Create a new rule . . . 51
Schritt 3: Filterbedingungen hinzufügen (optional) . . . 52
Schritt 4: Vorhandene Regeln verwalten . . . 53
Email to SMS Poller . . . 53
Wo finde ich diese Funktion . . . 53
Erstellen einer Regel . . . 54
SMS to Email . . . 54
Was diese Funktion macht . . . 54
Bevor Sie beginnen . . . 54
Schritt 1: SMS to Email-Seite öffnen . . . 55
Schritt 2: Erstellen Sie eine Regel . . . 55
SMS Forward . . . 56
Was diese Funktion macht . . . 56
Bevor Sie beginnen . . . 57
Schritt 1: Öffnen Sie die Seite SMS Forward . . . 57
Schritt 2: Erstellen Sie eine Regel . . . 57
Wie die Weiterleitung funktioniert . . . 59
Autoreplies . . . 60
Was diese Funktion macht . . . 60
Bevor Sie beginnen . . . 60
Schritt 1: Öffnen Sie die Autoreplies-Seite . . . 60
Schritt 2: Erstellen Sie eine Regel . . . 60
Schritt 3: Sendegrenze festlegen . . . 61
Wie Matching funktioniert . . . 62
Periodische SMS . . . 62
Was diese Funktion macht . . . 62
Bevor Sie beginnen . . . 63
Schritt 1: Öffnen Sie die Seite „Periodic SMS“ . . . 63
Schritt 2: Erstellen Sie eine Regel . . . 63
Subscriptions . . . 65
Was diese Funktion macht . . . 65
Bevor Sie beginnen . . . 65

Schritt 1: Öffnen Sie die Subscriptions-Seite . . . 66
Schritt 2: Erstellen Sie eine Regel . . . 66
Wie Matching funktioniert . . . 66
Was passiert, wenn sich jemand abonniert . . . 67
Allow / Deny List . . . 67
Was diese Funktion macht . . . 67
Bevor Sie beginnen . . . 68
Schritt 1: Öffnen Sie die Seite Allow / Deny List . . . 68
Schritt 2: Wählen Sie den aktiven Modus . . . 68
Schritt 3: Fügen Sie eine Nummer hinzu . . . 68
Schritt 4: Importieren Sie eine Liste aus CSV . . . 69
Schritt 5: Konfigurieren Sie das STOP-Wort (optional) . . . 69
Wie die Filterung funktioniert . . . 70
Workflows . . . 71
Wo finde ich diese Funktion . . . 71
Schritt 1: Erstellen Sie einen Workflow und wählen Sie einen Trigger . . . 71
Schritt 2: Bedingungsgruppen hinzufügen (optional) . . . 71
Schritt 3: Aktionen hinzufügen . . . 71
Webhooks . . . 72
Was diese Funktion macht . . . 72
Bevor Sie beginnen . . . 72
Schritt 1: Webhooks-Seite öffnen . . . 72
Schritt 2: Erstellen Sie eine Regel . . . 73
Schritt 3: Basiskonfiguration . . . 73
Schritt 4: Auslösebedingungen . . . 75
Schritt 5: Sicherheitseinstellungen . . . 76
Schritt 6: Wiederholungsintervall festlegen . . . 77
Verhalten von Webhooks . . . 77
MQTT . . . 77
Was diese Funktion macht . . . 77
Bevor Sie beginnen . . . 78
Teil 1: Subscribe (MQTT in SMS) . . . 78
Teil 2: Publish (SMS in MQTT) . . . 80
Inbox Rules . . . 82
Wo finde ich diese Funktion . . . 82
Konfigurieren einer Posteingangsregel . . . 82
Cleanup Folders . . . 82
Wo finde ich diese Funktion . . . 82
Konfigurieren einer Bereinigungsregel . . . 83
Berichte & Statistiken . . . 84
Berichte . . . 84
Periodische Berichte . . . 85
Statistiken . . . 86
Periodische Statistiken . . . 87
Überwachung . . . 88
Network Monitor . . . 88

Was diese Funktion bewirkt . . . 88
Vor Ihrem Start . . . 88
Teil 1: Tasks . . . 89
Teil 2: Berichte . . . 94
Teil 3: SNMP Traps . . . 96
Verhalten des Netzwerk-Monitors . . . 98
Digitaler Ein- und Ausgang . . . 98
Was diese Funktion bewirkt . . . 98
Vor Ihrem Start . . . 99
Wo man es findet . . . 99
Teil 1: Eingaberegeln (Eingangssignal in SMS) . . . 100
Teil 2: Ausgaberegeln (SMS in Ausgangssignal) . . . 102
Part 3: External pins . . . 105
Verhalten von Digital I/O-Regeln . . . 107
Einstellungen . . . 108
Kontoeinstellungen . . . 108
Multi-Faktor-Authentifizierung (MFA) konfigurieren . . . 108
SMS / MMS . . . 109
Nachrichten . . . 109
Modems . . . 110
Multi-Modem . . . 110
MMS . . . 113
Anrufe . . . 116
TTS-Lokalmodelle . . . 116
TTS-Online-Modelle (ElevenLabs) . . . 118
Eingehende Anrufe . . . 120
Anrufweiterleitung . . . 120
WhatsApp . . . 121
Was diese Funktion bewirkt . . . 121
Bevor Sie beginnen . . . 121
Schritt 1: Öffnen Sie die WhatsApp-Einstellungen . . . 122
Schritt 2: Aktivieren Sie den Dienst . . . 122
Schritt 3: Verknüpfen Sie Ihr Telefon . . . 122
Schritt 4: Entscheiden Sie, was mit Nicht-WhatsApp-Empfängern geschieht . . . 122
Schritt 5: Halten Sie den Dienst auf dem neuesten Stand . . . 122
Verknüpfung aufheben und ausschalten . . . 123
Wissenswert . . . 123
Signal . . . 124
Was diese Funktion bewirkt . . . 124
Bevor Sie beginnen . . . 124
Schritt 1: Öffnen Sie die Signal-Einstellungen . . . 125
Schritt 2: Aktivieren Sie den Dienst . . . 125
Schritt 3: Registrieren Sie eine Telefonnummer . . . 125
Schritt 4: Überprüfen Sie die Nummer . . . 126
Schritt 5: Halten Sie den Dienst auf dem neuesten Stand . . . 126
Entfernen der Nummer . . . 126
Wissenswert . . . 127

Email . . . 127
Email to SMS . . . 127
Email to SMS Poller . . . 129
SMTP-Konfiguration . . . 131
E-Mail-Warnungen . . . 131
SMPP . . . 132
Verbindungsdetails . . . 133
SMPP einschalten . . . 133
MQTT . . . 134
Netzwerk . . . 135
IP-Einstellungen . . . 135
SSL . . . 136
Failover . . . 136
SNMP . . . 137
Mobile Daten . . . 142
Anwendung . . . 143
Regionale Einstellungen . . . 143
Sicherheit . . . 143
Zugriff und Sichtbarkeit . . . 143
API und Integrationen . . . 143
LDAP . . . 144
Was diese Funktion bewirkt . . . 144
Bevor Sie beginnen . . . 144
Schritt 1: LDAP-Seite öffnen . . . 145
Schritt 2: Integration aktivieren . . . 145
Schritt 3: Connection . . . 145
Schritt 4: Verzeichnisstruktur . . . 146
Schritt 5: Attribute und Sicherheit . . . 147
ausgewählt und SSL aktiviert . . . 147
Schritt 7: Speichern und testen . . . 148
Datum / Uhrzeit . . . 149

System . . . 150
Benutzer . . . 150
Systeminformationen . . . 150
Protokolle . . . 151
Updates . . . 151
Patches . . . 151
Sicherung / Wiederherstellung . . . 151
Neustart . . . 151
Erweitert . . . 152

API und Entwicklerintegration . . . 153
API-Referenz . . . 153
API-Schlüssel . . . 153
API v2-Schlüssel . . . 153
API v1-Schlüssel . . . 154
Erstellen eines Schlüssels . . . 154

Welche Benutzer haben API-Zugriff . . . 155
Zugriff auf Ressourcen anderer Benutzer . . . 156

Plugins und Integrationen . . . 157

Erweitert . . . 158
Direkte Verbindung zur SMSEagle-Datenbank . . . 158
Einfügen einer kurzen SMS über SQL . . . 158
Einfügen einer langen SMS über SQL . . . 159
Datenbankbereinigungsskripte . . . 161
Weitergabe von Protokollen an einen externen Server . . . 161

Fehlerbehebung . . . 163
Überprüfung der LEDs . . . 163
Überprüfung der Geräteinformationen . . . 163
Gerätelogs . . . 164
Wenn das Gerät nicht erreichbar ist . . . 164
Wiederherstellen der Werkseinstellungen . . . 164
Service & Reparatur . . . 165
Garantie . . . 165
Service . . . 165

Technische Daten und Sicherheitsinformationen . . . 166
Technische Spezifikation . . . 166
Hardwarespezifikation . . . 166
Stromversorgung . . . 167
Antenne . . . 167
Durchsatz beim Senden/Empfangen . . . 167
Softwareplattform . . . 167
Wichtige Sicherheitsinformationen . . . 168

Behördliche Erklärungen . . . 170
EU-Konformitätserklärung . . . 170
FCC-Konformitätserklärung . . . 170
FCC-Konformitätserklärung des Lieferanten . . . 171
Kanadische behördliche Erklärung (ISED) . . . 171
Avis de conformité à la réglementation d'Industrie Canada . . . 172
UK Declaration of Conformity . . . 172
Grenzwerte für die HF-Exposition . . . 172
Entsorgung und Recycling-Informationen . . . 172
Entsorgung in Ländern außerhalb der Europäischen Union . . . 173
Information gemäß § 4 Absatz 4 Elektrogesetz (DE) . . . 173
Angaben zur sicheren Entnahme der Batterien oder der Akkumulatoren . . . 173
Restriction of Hazardous Substances Directive (RoHS) . . . 173
Europäische Union RoHS . . . 173

Deckblatt

Willkommen im MHD-8100 Benutzerhandbuch!

Das MHD-8100 ist ein Hardware-SMS-Gateway mit acht integrierten Modems und Ihren eigenen SIM-Karten, sodass Ihre Nachrichten direkt über das Mobilfunknetz aus Ihrer eigenen Infrastruktur versendet werden, ohne dass ein SMS-Provider von Drittanbietern zwischengeschaltet ist.

Dieses Handbuch ist die vollständige Referenz für das Gerät und gilt für alle MHD-8100-Varianten; wo das Verhalten vom Modemtyp oder der Hardwarerevision abhängt, ist der betreffende Abschnitt mit einem Badge gekennzeichnet. Wenn sich Ihr Gerät noch in der Verpackung befindet, beginnen Sie mit Was in der Box enthalten ist und führen Sie dann den Konfigurationsassistenten aus. Andernfalls verwenden Sie die Navigation auf der linken Seite oder das Suchfeld, um direkt zum benötigten Thema zu gelangen.

Die in dieser Publikation verwendeten Materialien sind urheberrechtlich geschützt und dürfen ohne vorherige Zustimmung des Urheberrechtsinhabers nicht vervielfältigt, kopiert oder verwendet werden. Technische Spezifikationen und Informationen in diesem Dokument können ohne vorherige Ankündigung geändert werden.

Informationen zur SMSEagle-Softwarelizenzierung

WICHTIG – VOR DEM BETRIEB LESEN

SMSEAGLE-SOFTWARE-ENDBENUTZERLIZENZVEREINBARUNG

Die hierin enthaltene Endbenutzerlizenzvereinbarung (die „**Vereinbarung**“ oder „**Lizenz**“ oder „**EULA**“) gilt als rechtsverbindliche Vereinbarung zwischen Ihnen (einer natürlichen oder juristischen Person, nachfolgend „**Lizenznehmerin**“ oder „**Sie**“ oder „**Ihr**“) und Proximus Sp. z o.o., ul. Piątkowska 163, Poznań, Polen, Postleitzahl 60-650 (nachfolgend „**PROXIMUS**“) für die Nutzung der auf einem SMSEagle-Gerät vorinstallierten Software (d. h. Software, die mit diesem Gerät installiert und geliefert wird), die zugehöriges Druckmaterial und weitere Komponenten und/oder Softwaremodule, einschließlich, aber nicht beschränkt auf erforderliche Treiber, umfassen kann (die „**SMSEagle-Software**“). Andere Aspekte der SMSEagle-Software können auch, aber nicht ausschließlich, Softwareaktualisierungen und alle Upgrades umfassen, die PROXIMUS Ihnen zur Verfügung stellt oder zur Verfügung stellen kann, oder die Sie nach dem Erwerb des SMSEagle-Geräts erhalten, und insofern diese Elemente nicht von einer separaten Lizenzvereinbarung oder Nutzungsbedingungen begleitet werden.

DURCH AKZEPTANZ DIESER BEDINGUNGEN IN DER GRAFISCHEN BENUTZEROBERFLÄCHE (GUI) DES SMSEAGLE-GERÄTS, DURCH IHRE NUTZUNG DES SMSEAGLE-GERÄTS ODER DURCH AKTUALISIERUNG ODER UPGRADE DER SMSEAGLE-SOFTWARE ERKLÄREN SIE SICH RECHTLICH AN DIE HIERIN ENTHALTENEN BEDINGUNGEN DIESER LIZENZVEREINBARUNG GEBUNDEN. WENN SIE SICH AN DIE BEDINGUNGEN DIESER EULA NICHT GEBUNDEN ERKLÄREN, NUTZEN SIE DAS SMSEAGLE-GERÄT NICHT UND SIE KÖNNEN DAS GERÄT PROMPT ZUR RÜCKERSTATTUNG SEINES KAUFPREISES ZURÜCKGEBEN, INDEM SIE PROXIMUS UNTER DER OBEN ANGEGEBENEN ADRESSE KONTAKTIEREN. Die aktuelle Version dieser EULA wird Ihnen vor dem Kauf unter www.smseagle.eu zur Verfügung gestellt und wird während der Ersteinrichtung und nach jeder wesentlichen Änderung ihrer Bedingungen in der GUI des SMSEagle-Geräts angezeigt. Ihre Akzeptanz in der GUI (einschließlich Datum, Version und Gerätekennung) wird lokal in der Datenbank des SMSEagle-Geräts aufgezeichnet. Wenn Sie die Bedingungen in der GUI nicht akzeptieren, wird die SMSEagle-Software nicht zur Nutzung aktiviert.

DIE SMSEAGLE-SOFTWARE IST DURCH URHEBERRECHTSGESETZE SOWIE ALLE ANDEREN EINSCHLÄGIGEN GESETZE ZUM SCHUTZ VON GEISTIGEM EIGENTUM GESCHÜTZT. DIE SMSEAGLE-SOFTWARE IST LIZENZIERT UND NICHT VERKAUFT. ALLE RECHTE, EINSCHLIESSLICH URHEBERRECHTE, AN DER SMSEAGLE-SOFTWARE BLEIBEN AUSSCHLIESSLICHES EIGENTUM VON PROXIMUS, DARÜBER HINAUS, WIE NACHFOLGEND DARGELEGT, UMFASST DIE SMSEAGLE-SOFTWARE EINIGE MODULE, DIE VON DRITTEN ENTWICKELT WURDEN UND DIE HIERMIT GEMÄSS DEN VON DEM ENTWICKLER ZULÄSSIGEN BEDINGUNGEN AN SIE SUBLIZENZIERT WERDEN.

Diese EULA gewährt Ihnen bestimmte Rechte, und Sie können auch über weitere gesetzliche Rechte verfügen, die von Gerichtsbarkeit zu Gerichtsbarkeit unterschiedlich sind. Die

Haftungsausschlüsse, Ausschlüsse und Haftungsbeschränkungen im Rahmen dieser EULA gelten nicht insoweit, als dies durch anwendbares Recht verboten ist. Einige Gerichtsbarkeiten verbieten den Ausschluss stillschweigender Garantien oder den Ausschluss oder die Beschränkung zufälliger oder Folgeschäden oder anderer Rechte. In diesem Fall können diese Bestimmungen dieser EULA für Sie nicht gelten. Dies beeinträchtigt jedoch nicht die Durchsetzbarkeit und Anwendbarkeit aller anderen Bestimmungen der EULA.

1. **DEFINITIONEN UND AUSLEGUNGEN**
    1. „Vereinbarung“ oder „Lizenz“ oder „EULA“ bezeichnen diese Endbenutzerlizenzvereinbarung.
    2. „Lizenznehmerin“ 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“ bedeutet aktuelle und zukünftige weltweite Rechte im Rahmen des Urheberrechtsgesetzes, Patentgesetzes, Gesetzes zum Schutz von Geschäftsgeheimnissen, Markengesetzes, Gesetzes zum Schutz moralischer Rechte und anderer ähnlicher Rechte.
    4. „Aktualisierung“ bedeutet die Wartung oder Behebung einer Version der SMSEagle-Software, einschließlich, aber nicht beschränkt auf einen Hotfix, Patch oder eine Erweiterung, die nicht als eigenständiger Service oder anderes Softwarepaket funktionieren und für einen bestehenden Lizenznehmer keine zusätzlichen Kosten verursachen.
    5. „Upgrade“ bedeutet eine Hauptversion der SMSEagle-Software als eigenständiges Paket, das zusätzliche Anwendungen, Funktionen oder Funktionalitäten enthalten kann.
    6. Eine Bezugnahme auf „Person“ umfasst eine natürliche Person, einen Körperverband oder nicht eingetragenen Verband (mit oder ohne separate juristische Persönlichkeit) und die Rechtsvertreter, Nachfolger und zulässigen abgetretenen Rechte dieser Person.
    7. Wörter in der Einzahl schließen die Mehrzahl ein und umgekehrt.
    8. Eine Bezugnahme auf ein Gesetz, eine gesetzliche Bestimmung oder untergeordnete Rechtsvorschrift ist eine Bezugnahme darauf, wie es von Zeit zu Zeit Bestand hat, unter Berücksichtigung einer Änderung oder Neuerlass, und umfasst alle Gesetze, gesetzlichen Bestimmungen oder untergeordneten Rechtsvorschriften, die sie ändert oder neu erlässt; vorausgesetzt, dass zwischen den Parteien keine solche Änderung oder Neuerlass für die Zwecke dieser Vereinbarung soweit angewendet wird, dass sie neue oder erweiterte Verpflichtungen, Haftung oder Einschränkungen auferlegten würde oder die Rechte einer Partei anderweitig nachteilig beeinflussen würde.
    1. Eine Bezugnahme auf Schreiben oder schriftlich umfasst E-Mail.
    2. Jede Verpflichtung in dieser Vereinbarung für eine Person, etwas nicht zu tun, umfasst auch die Verpflichtung, nicht zuzustimmen oder zuzulassen, dass dies geschieht.

3. Jeder Satz, der durch die Begriffe „einschließlich“, „umfasst“, „insbesondere“ oder einen ähnlichen Ausdruck eingeleitet wird, ist als veranschaulichend auszulegen und beschränkt nicht die Bedeutung der Wörter, die diesen Begriffen vorangehen.
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 auf eine Weise, die es PROXIMUS oder Drittpartnern ermöglicht, auf diese 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, und zur Installation von Aktualisierungen und Upgrades gemäß den hierin festgelegten Bedingungen und Bestimmungen:

1. **Nutzung.** PROXIMUS gewährt Ihnen das Recht, eine einzelne Instanz der SMSEagle-Software auf dem SMSEagle-Gerät zu nutzen, das Sie erworben haben. Die Nutzung auf einem anderen Gerät oder Computer ist verboten.
2. **Sicherungskopie.** Sie dürfen eine einzelne Kopie der aktuellen Version der SMSEagle-Software für Ihr SMSEagle-Gerät, soweit erforderlich, zu Sicherungszwecken aufbewahren.
    1. Darüber hinaus gilt diese EULA auch für alle Software-Aktualisierungen und Upgrades, die PROXIMUS bereitstellt und die die ursprüngliche installierte Version der SMSEagle-Software ersetzen, überschreiben und/oder ergänzen können, es sei denn, diese Aktualisierungen und Upgrades werden durch eine separate Lizenz abgedeckt. In diesem Fall gelten die Bedingungen dieser Lizenz.

1. **GEISTIGES EIGENTUM**
    1. **GESCHÜTZTE SMSEAGLE-SOFTWARE**. Die SMSEagle-Software ist durch Urheberrecht und andere Gesetze und Verträge zum Schutz von geistigem Eigentum geschützt.
    2. **NUTZUNGSBESCHRÄNKUNGEN**. Als Lizenzinhaber dürfen Sie nicht: (a) Die SMSEagle-Software gleichzeitig auf mehr als einem Gerät nutzen, ohne vorherigen Kauf zusätzlicher Geräte; (b) Die SMSEagle-Software in irgendeiner Form an Dritte weitergeben oder anderweitig zur Verfügung stellen; (c) Die SMSEagle-Software oder Teile davon ändern, anpassen, abgeleitete Werke davon erstellen oder übersetzen, außer soweit dies innerhalb Ihres SMSEagle-Geräts gemäß dieser Lizenz zulässig ist; (d) Die SMSEagle-Software dekompilieren, disassemblieren oder zurückentwickeln, noch versuchen, ihren Quellcode zu ermitteln oder zu beschaffen (außer soweit solche Handlungen durch zwingende Bestimmungen des anwendbaren Rechts zulässig sind, einschließlich Artikel 6 der Richtlinie 2009/24/EG zur Dekompilierung für Interoperabilität mit anderen Programmen); (e) Versuchen, Markenzeichen, Urheberrechte oder andere Eigentumsvermerke in der SMSEagle-Software zu ändern oder zu entfernen; oder (f) Die SMSEagle-Software auf andere Weise nutzen, als in

dieser EULA oder in der Dokumentation des SMSEagle-Geräts, auf dem sie installiert ist, vorgegeben.

3. **UPDATES/UPGRADES**. PROXIMUS kann es für angebracht halten, Updates oder Upgrades der SMSEagle-Software zur Verfügung zu stellen. Sie können den Installationsprozess für ein Update oder Upgrade initiieren, etwa durch Klicken auf die Schaltfläche „Check for software updates now“ in der Weboberfläche des SMSEagle-Geräts. Alternativ (wenn das Gerät keinen Internetzugang hat) können Sie ein Update- oder Upgrade-Paket vom SMSEagle-Support unter https://support.smseagle.eu erhalten und später auf dem SMSEagle-Gerät installieren. Es liegt im alleinigen Ermessen von PROXIMUS, die Bereitstellung dieser Updates oder Upgrades an Ihre Akzeptanz einer anderen EULA oder den Abschluss einer anderen separaten Vereinbarung zu knüpfen. Mit der Entscheidung, diese Updates oder Upgrades zu installieren und zu nutzen, erklären Sie sich mit allen geltenden Lizenzbedingungen, Bedingungen und Konditionen dieser EULA und/oder einer anderen Vereinbarung einverstanden. PROXIMUS verpflichtet sich, Security Updates für die SMSEagle-Software für einen Mindestzeitraum von fünf (5) Jahren ab dem Zeitpunkt des ersten Verkaufs des betreffenden SMSEagle-Gerätemodells bereitzustellen (der „Update-Zeitraum“). Nach Ablauf des Update-Zeitraums kann PROXIMUS nach eigenem Ermessen Updates oder Upgrades weiterhin bereitstellen, ist aber nicht dazu verpflichtet. PROXIMUS wird das End-of-Life-Datum jedes SMSEagle-Gerätemodells auf seiner Website spätestens zwölf (12) Monate vor diesem Datum ankündigen. Diese Zusage beeinträchtigt nicht längere Supportzeiträume, die nach zwingenden Bestimmungen des anwendbaren Rechts erforderlich sind, einschließlich des Cyber Resilience Act und der NIS2-Richtlinie.

2. **GEWÄHRLEISTUNGSAUSSCHLUSS**

PROXIMUS wird angemessene Anstrengungen unternehmen, die den gängigen Software-Entwicklungsstandards entsprechen, um die SMSEagle-Software so zu pflegen, dass Fehler und Unterbrechungen minimiert werden.

JEDOCH GARANTIERT PROXIMUS NICHT, DASS DIE NUTZUNG DER SMSEAGLE-SOFTWARE UNTERBRECHUNGSFREI ODER FEHLERFREI ERFOLGT; UND ÜBERNIMMT KEINE GARANTIE HINSICHTLICH DER ERGEBNISSE, DIE SICH AUS DER NUTZUNG DER SMSEAGLE-SOFTWARE ERGEBEN.

SOWEIT NACH ANWENDBAREM RECHT ZULÄSSIG, AUSSER WIE HIERIN AUSDRÜCKLICH VORGESEHEN UND UNGEACHTET GEGENTEILIGER BESTIMMUNGEN, ERTEILT WEDER PROXIMUS NOCH EIN LEITENDER ANGESTELLTER, DIREKTOR, TOCHTERUNTERNEHMEN, VERBUNDENES UNTERNEHMEN, AUTORISIERTER WIEDERVERKÄUFER ODER ARBEITNEHMER DAVON IRGENDWELCHE ANDEREN GARANTIEN JEGLICHER ART, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND, GESETZLICH ODER ANDERWEITIG, EINSCHLIESSLICH, ABER NICHT

BEGRENZT AUF GARANTIEN DER MARKTGÄNGIGKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND GEWÄHRUNG VON RECHTEN.

1. **HAFTUNGSBEGRENZUNG**
    1. Die Haftung von PROXIMUS für einen Anspruch, der durch die Nutzung der SMSEagle-Software verursacht, damit verbunden oder sich daraus ergibt, oder für die Summe solcher Ansprüche, wird niemals die Kosten des SMSEagle-Geräts übersteigen, in Bezug auf das der Schaden aufgetreten ist, es sei denn, eine solche Haftungsbegrenzung ist nach anwendbarem polnischem Recht nicht zulässig.
    2. PROXIMUS haftet gegenüber dem Lizenzinhaber nicht für indirekte oder Folgeschäden, einschließlich Gewinnausfälle jeglicher Art und Kundenausfälle, Umsatzausfälle, Margenausfälle, Produktionsausfälle, Reputationsschäden, Daten- oder Konfigurationsverluste, vorausgesetzt, dass der obige Ausschluss nicht für Schäden gilt, die vorsätzlich (absichtlich) durch PROXIMUS verursacht werden.
    3. PROXIMUS haftet insbesondere nicht für: (i) Daten- oder Konfigurationsverluste; (ii) Gewinnausfälle des Lizenzinhabers; (iii) indirekte oder Folgeschäden; (iv) Handlungen Dritter.
    4. Bezüglich der Haftung von PROXIMUS für Ansprüche des Endnutzers ist die Haftung von PROXIMUS auf Situationen beschränkt, in denen der Schaden das Ergebnis einer direkten Handlung oder Unterlassung durch PROXIMUS ist, und nur auf die Kosten des SMSEagle-Geräts, in Bezug auf das der Schaden aufgetreten ist, es sei denn, eine solche Haftungsbegrenzung ist nach anwendbarem polnischem Recht nicht zulässig.
    5. Die Bestimmungen dieses Abschnitts gelten nicht für Lizenzinhaber, die Verbraucher oder Einzelunternehmer gemäß polnischem Recht sind, soweit die hierin festgelegten Beschränkungen durch zwingende Verbraucherschutzbestimmungen verboten sind.
2. **OPEN SOURCE**

Bestimmte Softwaremodule in der PROXIMUS-Software unterliegen „Open-Source“- oder „Free-Software“-Lizenzen („Open-Source-Software“). Ein Teil der Open-Source-Software ist Eigentum Dritter. Solche Open-Source-Software unterliegt nicht den Bedingungen dieser Vereinbarung. Stattdessen wird jedes Element der Open-Source-Software unter den Bedingungen der End-User-Lizenz lizenziert, die mit dieser Open-Source-Software geliefert wird. Nichts in dieser Vereinbarung schränkt Ihre Rechte unter den Bedingungen einer zutreffenden End-User-Lizenz für die Open-Source-Software ein oder vergibt Ihnen Rechte, die diese übersteigen. Zutreffende Open-Source-Lizenzen sind: MIT-Lizenz; GNU General Public License v. 2.0; GNU Lesser General Public License v. 2.1; BSD-3-Klausel-Lizenz; Apache-Lizenz 2.0. Soweit erforderlich durch eine Lizenz für bestimmte Open-Source-Software, stellt PROXIMUS diese Open-Source-Software und unsere Modifikationen derselben durch schriftliche Anfrage an uns unter der angegebenen E-Mail- oder Postadresse zur Verfügung.

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

Die SMSEagle-Software wird an die U.S. Government mit eingeschränkten Rechten lizenziert. Die Nutzung, Vervielfältigung oder Offenlegung durch die U.S. Government unterliegt Beschränkungen

gemäß DFARS 252.227-7013 der Technical Data and Computer Software-Klausel und 48 CFR 52.227-19 der Commercial Computer Software-Klausel, je nach Anwendbarkeit.

1. **DATENSCHUTZ**
    1. **DATENSCHUTZERKLÄRUNG**. PROXIMUS erfasst KEINE Daten, mit denen Sie bei Verwendung des SMSEagle-Geräts arbeiten. Wir können keine Daten, die auf dem SMSEagle-Gerät gespeichert sind, sehen oder erfassen, da wir keinen Zugriff auf Ihr Gerät haben. Bei der Bereitstellung der SMSEagle-Software und des damit verbundenen Supports kann PROXIMUS jedoch bestimmte personenbezogene Daten des Lizenzinhabers (oder, wenn der Lizenzinhaber eine juristische Person ist, deren bevollmächtigte 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 personenbezogener Daten, die verarbeitet werden: (a) Registrierungs- und Lizenzierungsdaten (Unternehmensname, Kontaktperson, E-Mail, Geräteseriennummer); (b) Update-/Upgrade-Telemetrie, streng begrenzt auf Softwareversion, Gerätemodell, Geräteseriennummer, IP-Adresse, sofern zutreffend. Personenbezogene Daten, die im Zusammenhang mit der Bereitstellung technischer Unterstützung verarbeitet werden, unterliegen einer separaten Technical Support Services Policy, die auf der Proximus-Website verfügbar ist: www.smseagle.eu.
    4. Zwecke und Rechtsgrundlagen der Verarbeitung: (a) Erfüllung dieser EULA und Bereitstellung von Updates und Upgrades - Artikel 6 Absatz 1 Buchstabe b DSGVO; (b) Einhaltung rechtlicher Verpflichtungen (Steuern, Buchhaltung) - Artikel 6 Absatz 1 Buchstabe c DSGVO; (c) berechtigte Interessen von PROXIMUS an der Verbesserung der SMSEagle-Software und der Verteidigung gegen Ansprüche - Artikel 6 Absatz 1 Buchstabe f DSGVO.
    5. Empfänger personenbezogener Daten: bevollmächtigte Mitarbeiter und Auftragnehmer von PROXIMUS, die der Vertraulichkeit unterliegen, IT-Dienstleister (Hosting, E-Mail, Ticketing), die als Auftragsverarbeiter gemäß Artikel 28 DSGVO tätig sind, und zuständige öffentliche Behörden, soweit dies gesetzlich erforderlich ist.
    6. Übermittlungen in Drittländer: Personenbezogene Daten werden hauptsächlich im Europäischen Wirtschaftsraum verarbeitet. Soweit Übermittlungen in Drittländer erfolgen (z. B. Nutzung bestimmter IT-Anbieter), erfolgen sie auf der Grundlage eines Angemessenheitsbeschlusses oder angemessener Schutzmaßnahmen, wie etwa der EU-Standardvertragsklauseln.
    7. Aufbewahrungsfrist: Registrierungs- und Lizenzierungsdaten – für die Dauer dieser EULA und für den Zeitraum, der nach anwendbarem Recht erforderlich ist (insbesondere Steuer- und Buchhaltungsrecht, typischerweise 5 Jahre); auf Grundlage berechtigter Interessen verarbeitete Daten – bis ein wirksamer Einspruch erhoben wird oder das berechtigte Interesse endet.
    8. Rechte der betroffenen Personen: Der Lizenzinhaber hat das Recht auf Zugang, Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenportabilität seiner

personenbezogenen Daten sowie das Recht, der Verarbeitung auf Grundlage berechtigter Interessen zu widersprechen.

9. Beschwerderecht: Der Lizenzinhaber hat das Recht, eine Beschwerde bei der Direktorin oder dem Direktor des Amts für den Schutz personenbezogener Daten (Prezes Urzędu Ochrony Danych Osobowych), ul. Stawki 2, 00-193 Warschau, Polen, einzureichen.
10. Automatisierte Entscheidungsfindung: PROXIMUS führt keine automatisierte Entscheidungsfindung, einschließlich Profiling, im Sinne von Artikel 22 DSGVO im Zusammenhang mit dieser EULA durch.
11. Die Bereitstellung personenbezogener Daten ist freiwillig, aber notwendig für den Abschluss und die Erfüllung dieser EULA und für die Bereitstellung von Supportdiensten. Weitere Einzelheiten, einschließlich etwaiger Aktualisierungen dieser Informationen, finden Sie in der Datenschutzrichtlinie unter https://www.smseagle.eu/privacy-policy/.

2. **BEENDIGUNG**

1. PROXIMUS behält sich das Recht vor, diese EULA mit sofortiger Wirkung zu beenden, falls: (i) der Lizenzinhaber einen wesentlichen Verstoß gegen die im Abschnitt „Nutzungsbeschränkungen“ festgelegten Lizenzbeschränkungen begeht; (ii) unzulässige Vervielfältigung, Verbreitung oder Änderung der SMSEagle-Software erfolgt; oder (iii) technische Schutzmaßnahmen umgangen oder manipuliert werden.
2. PROXIMUS und ein Lizenzgeber, der das SMSEagle-Gerät direkt von PROXIMUS erworben hat, können diese EULA mit mindestens dreißig (30) Tagen schriftlicher Kündigung beenden.
3. Vorbehaltlich zwingender Verbraucherschutzgesetze hat der Lizenzgeber keinen Anspruch auf Rückerstattung des Kaufpreises des SMSEagle-Geräts oder von Gebühren im Zusammenhang mit der SMSEagle-Software, wenn PROXIMUS diese EULA aus den in Abschnitt 9.01 genannten Gründen kündigt.
4. Nach Beendigung dieser EULA muss der Lizenzgeber die Nutzung der SMSEagle-Software einstellen und alle vorhandenen Sicherungskopien unbrauchbar machen. Die Abschnitte „Geistiges Eigentum“, „Haftungsausschluss“, „Haftungsbeschränkung und Abhilfe“, „Datenschutz“, „Anwendbares Recht“ und „Streitbeilegung“ bleiben nach Beendigung bestehen.
5. Falls der Lizenzgeber das SMSEagle-Gerät von einem Wiederverkäufer oder autorisierten Partner erworben hat, sind die Regeln für Rückgaben, Stornierungen und Rückerstattungen des SMSEagle-Geräts in der Rechnung oder in anderen vom Wiederverkäufer oder autorisierten Partner bereitgestellten Verkaufsunterlagen angegeben.
6. Diese EULA wird unabhängig von einer auf das SMSEagle-Gerät anwendbaren Hardwaregarantie bereitgestellt. Das Ablaufen oder die Beendigung dieser EULA beeinträchtigt nicht die Gültigkeit und Dauer der dem SMSEagle-Gerät zugewiesenen Hardwaregarantie und die Bedingungen der Hardwaregarantie beschränken auch nicht die Rechte des Lizenzgebers gemäß dieser EULA.

3. **SONSTIGES**
    1. **NACHFOLGER UND ABTRETUNGEN**. Diese EULA ist in ihrer Gesamtheit rechtlich bindend für PROXIMUS und Sie sowie für unsere jeweiligen Nachfolger und zulässigen Abtretungsempfänger.
    2. **SALVATORISCHE KLAUSEL**. Sollte eine Bestimmung dieser Vereinbarung von einem zuständigen Gericht für rechtswidrig, ungültig oder nicht durchsetzbar befunden werden, sind die übrigen Bestimmungen nicht betroffen.
    3. **VERZICHT**. Wenn es einen Verzicht auf die Geltendmachung einer Verletzung oder ein Versäumnis gibt, diese EULA oder eine ihrer Bestimmungen durchzusetzen, gilt dies nicht als zukünftiger Verzicht auf diese Bedingungen oder als Verzicht auf eine andere Bestimmung dieser EULA.
    4. **ÄNDERUNGEN**. Jede Abänderung, Ergänzung, Änderung oder Novellierung einer Bestimmung dieser EULA ist nur wirksam, wenn sie schriftlich erfolgt und von PROXIMUS unterzeichnet ist.
    5. **ANWENDBARES RECHT**. In Angelegenheiten, die hierin nicht geregelt sind, gelten die Bestimmungen des Polnischen Zivilgesetzbuches und die Bestimmungen des Polnischen Urheberrechtsgesetzes vom 4· Februar 1994 (Amtsblatt 1994, Nr. 24, Punkt 83). Diese Vereinbarung unterliegt in allen Aspekten den Gesetzen der Republik Polen.
    6. **STREITBEILEGUNG**. Alle Streitigkeiten, die sich aus dieser Vereinbarung ergeben oder mit ihr zusammenhängen, unterliegen der ausschließlichen Gerichtsbarkeit der ordentlichen Gerichte, die für den eingetragenen Sitz von PROXIMUS in Poznań, Polen zuständig sind. Diese Bestimmung gilt nicht für Lizenzgeber, die Verbraucher oder Einzelunternehmer gemäß polnischem Recht sind, die das Recht behalten, Klage vor dem nach den geltenden zwingenden Rechtsvorschriften zuständigen Gericht einzureichen.
    7. **ABTRETUNGEN**. Sie haben das Recht, die SMSEagle-Software an einen Dritten nur zusammen mit der dauerhaften Übertragung des Eigentums an dem SMSEagle-Gerät, auf dem sie vorinstalliert war, zu übertragen. In diesem Fall ist der Empfänger verpflichtet, diese EULA in ihrer aktuellen Form vor der Nutzung der SMSEagle-Software zu akzeptieren, und Sie müssen alle von Ihnen gehaltenen Sicherungs- oder sonstigen Kopien der SMSEagle-Software zum Zeitpunkt der Übertragung unbrauchbar machen. Diese Bestimmung lässt die Erschöpfungslehre gemäß Artikel 4 Absatz 2 der Richtlinie 2009/24/EG und alle zwingenden Rechte des Lizenzgebers gemäß EU-Recht unberührt.
    8. **GÜLTIGKEIT UND BINDENDE WIRKUNG**. Diese Vereinbarung stellt eine gültige und rechtlich bindende Verpflichtung der Parteien dar, die gemäß ihren Bedingungen gegen die Parteien durchsetzbar ist, wobei alle Auswirkungen von Insolvenz, Zahlungsunfähigkeit, betrügerischer Übertragung, Umstrukturierung, Moratorium und anderen Gesetze im Zusammenhang mit oder zur Beeinträchtigung von Gläubigerrechten und allgemeinen billigen Grundsätzen berücksichtigt werden.

9. **WIRKUNG VON TITEL UND ÜBERSCHRIFTEN**. Der Titel der Vereinbarung und die Überschriften von Abschnitten und Klauseln sind aus Gründen der Klarheit enthalten und beeinflussen nicht die Bedeutung der Vereinbarung oder des Abschnitts.
10. **HÖHERE GEWALT**. Außer bei Zahlungsverpflichtungen wird die Leistung ausgesetzt und die Leistungsfrist verlängert sich entsprechend, wenn eine Partei daran gehindert ist oder nicht in der Lage ist, eine ihrer Verpflichtungen aus dieser Vereinbarung aufgrund von Ursachen, die außerhalb der angemessenen Kontrolle der Partei liegen, die diese Bestimmung geltend macht, zu erfüllen, einschließlich, aber nicht begrenzt auf Naturkatastrophen, Handlungen von Zivil- oder Militärbehörden, Unruhen oder ziviler Ungehorsam, Kriege, Streiks oder Arbeitskonflikte (jeweils ein „**Ereignis höherer Gewalt**"), sofern die Partei unverzüglich alle angemessenerweise notwendigen Schritte unternimmt, um die vollständige Leistung wieder aufzunehmen.

4. **VERBRAUCHERSCHUTZ UND SCHUTZ VON EINZELUNTERNEHMERN**

Die Bestimmungen dieser EULA beeinträchtigen nicht die Bestimmungen zum Schutz von Verbrauchern und Unternehmern, wenn Sie eine natürliche Person sind, die das Gerät kauft und diese EULA nicht in direktem Zusammenhang mit seiner geschäftlichen oder beruflichen Tätigkeit abschließt, oder im Fall eines Unternehmers, der eine natürliche Person ist – nicht in direktem Zusammenhang mit seiner beruflichen Tätigkeit (angewendet auf die EULA, die ab dem 1. Januar 2021 abgeschlossen wurde). Wenn eine Bestimmung dieser EULA mit zwingenden Verbraucherschutz- oder Einzelunternehmer-Schutzgesetzen nicht vereinbar ist, gilt diese Bestimmung nicht für den Verbraucher/Einzelunternehmer und es gilt die gesetzliche Bestimmung, die dieser Bestimmung am nächsten kommt.

1. **KONTAKTINFORMATIONEN**

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

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

Was ist in der Box



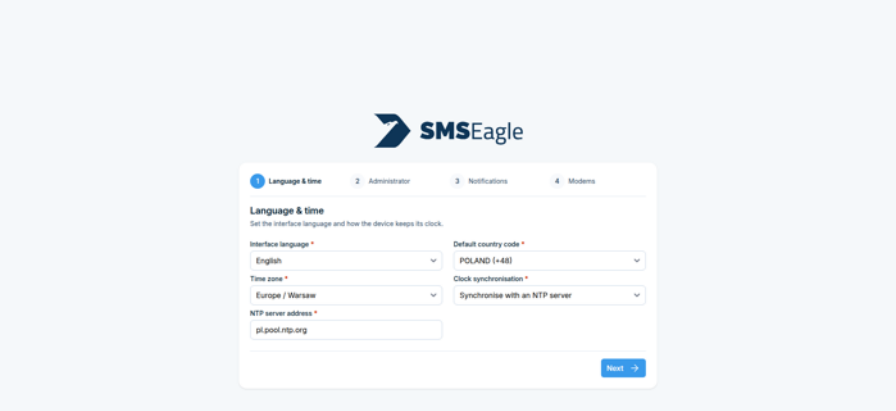
SMSEagle Boxinhalt

Ihre SMSEagle Box enthält:

- SMSEagle Hardware SMS Gateway
- 8x externe omnidirektionale Antenne
- Stromkabel
- Rackmontage-Halterungen
- Schnellstartanleitung

Konfigurationsassistent

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

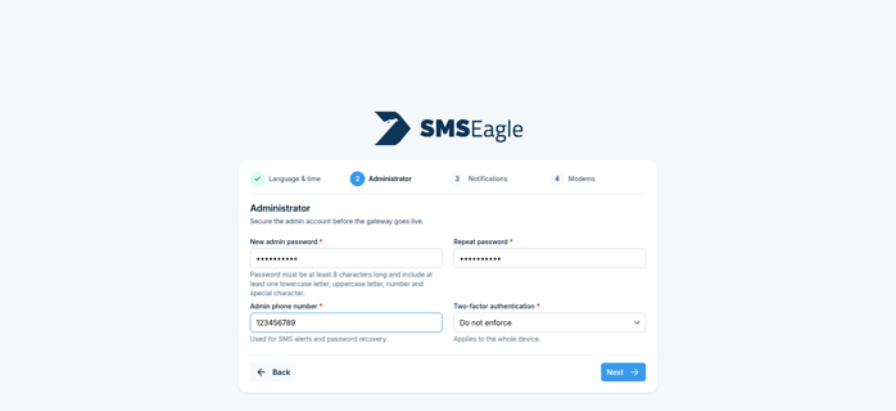


Schritt 1: Sprache & Zeit

Schritt 1: Sprache & Zeit

Stellen Sie die Schnittstellensprache, den Standard-Ländercode (wird verwendet, wenn eine Telefonnummer ohne einen eingegeben wird), die Geräte-Zeitzone und die Zeitsynchronisierung ein. Wenn Sie **Mit 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 wieder an, um den Assistenten fortzusetzen.

Schritt 3: Benachrichtigungen

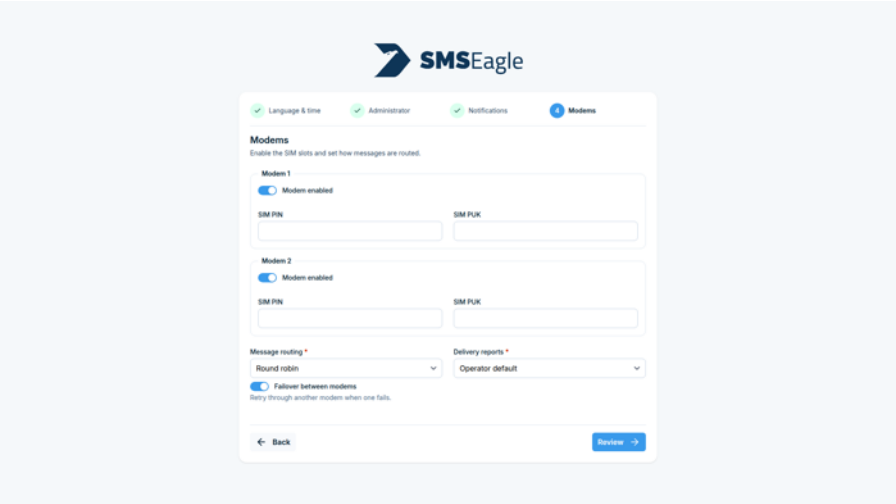


Schritt 3: Benachrichtigungen

Wählen Sie, über welche Ereignisse das Gerät Sie informieren soll:

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

Schritt 4: Modems



Schritt 4: Modems

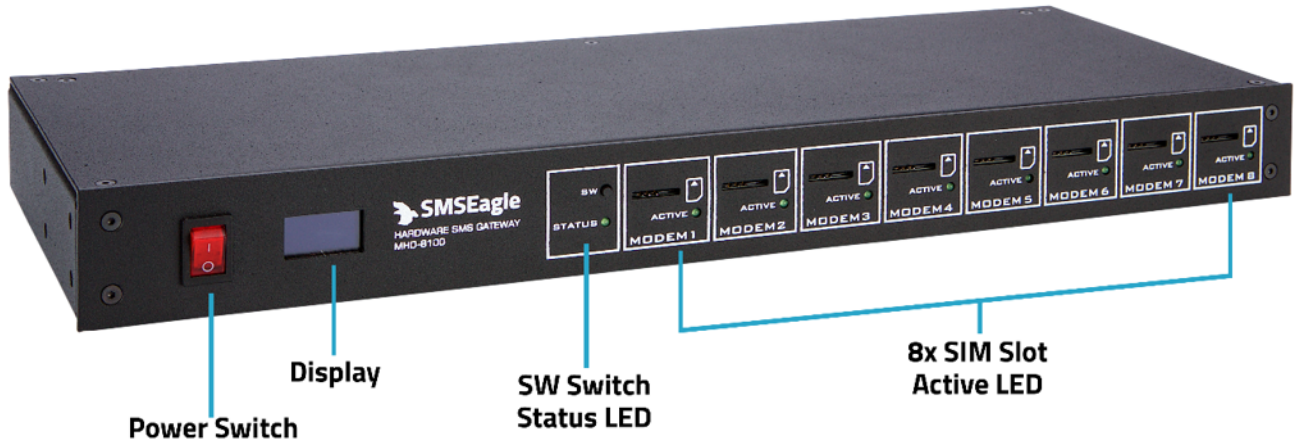
Aktivieren Sie für jedes integrierte Modem (Modem 1, Modem 2 auf Multi-Modem-Geräten) dieses und geben Sie bei Bedarf seine **SIM-PIN** und **SIM-PUK** ein. Stellen Sie dann Folgendes ein:

- **Nachrichtenrouting** – Round Robin, SIM 1 als Master oder SIM 2 als Master (siehe Multimodem-Auswahlstrategie)
- **Zustellungsberichte** – Betreiber Standard, Immer anfordern oder Niemals anfordern
- **Failover zwischen Modems** – Wiederholung über das andere Modem bei Fehler eines Modems

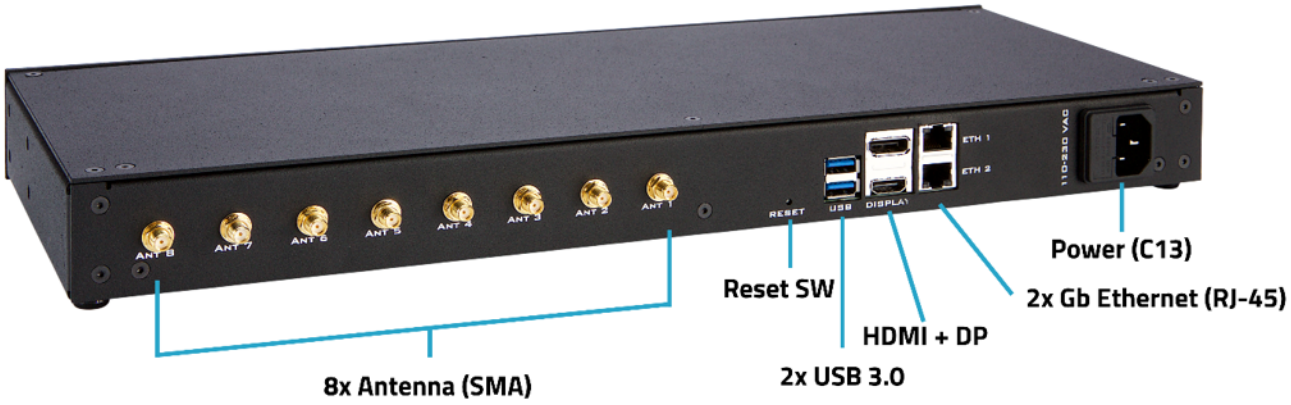
Überprüfen Sie Ihre Einstellungen und schließen Sie den Assistenten ab, um das normale Dashboard zu erreichen.

Anschlüsse, Anschlussports und LEDs

Frontplatte



Rückplatte



Frontplatte

Element	Bezeichnung	Beschreibung
Netzschalter	-	Netzschalter zum Ein- und Ausschalten des Geräts
Display	-	Anzeigebildschirm
Benutzer-Schalter	SW	Schalter zum Umschalten von Informationen auf dem Display und zum Wiederherstellen von Werkseinstellungen
Status-LED	STATUS	LED zur Anzeige des Gerätestatus
SIM-Slot	-	8x SIM-Slot – Minigröße
SIM-aktive LED	ACTIVE	8x LED-Anzeige für Modemstatus

Rückplatte

Element	Bezeichnung	Beschreibung
Antenne	ANT1-8	Antennenbuchse (SMA)
Reset	ZURÜCKSETZEN	Schalter zum Neustart des Geräts
USB	USB	2x USB 3.0-Anschluss
Display-Anschlüsse	DISPLAY	HDMI und Display Port (nur zu Debugging-Zwecken)
Ethernet-Anschlüsse	ETH1-2	Gigabit-Ethernet-RJ45-Anschlüsse
Stromversorgungsanschluss	110-230VAC	Stromversorgungsanschluss

Display

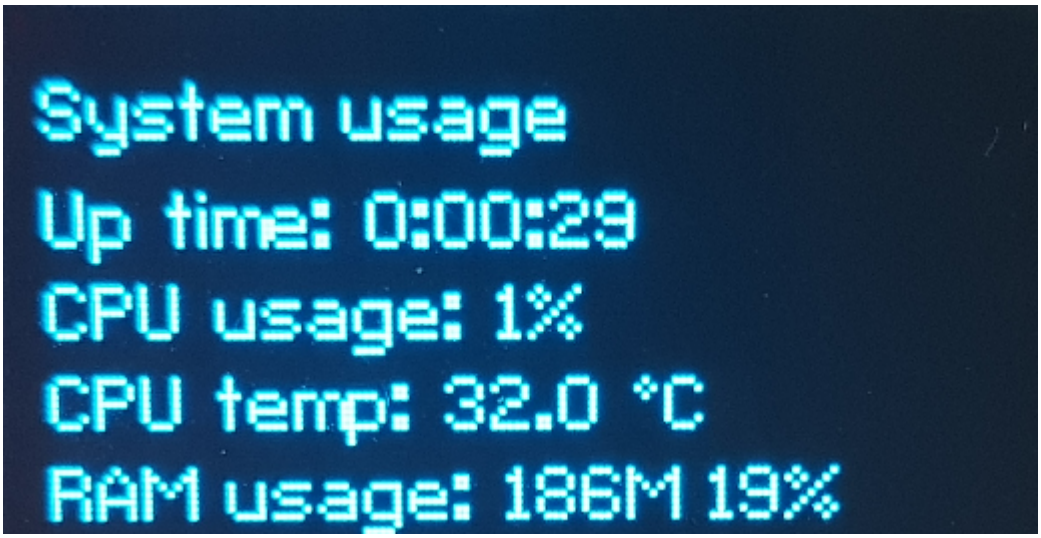
Das MHD-8100 verfügt über ein eingebautes Display mit 5 Bildschirmen, von denen jeder unterschiedliche Informationen anzeigt. Drücken Sie den **SW**-Schalter, um durch die Bildschirme zu wechseln.

Bildschirm 1: SMSEagle-Logo

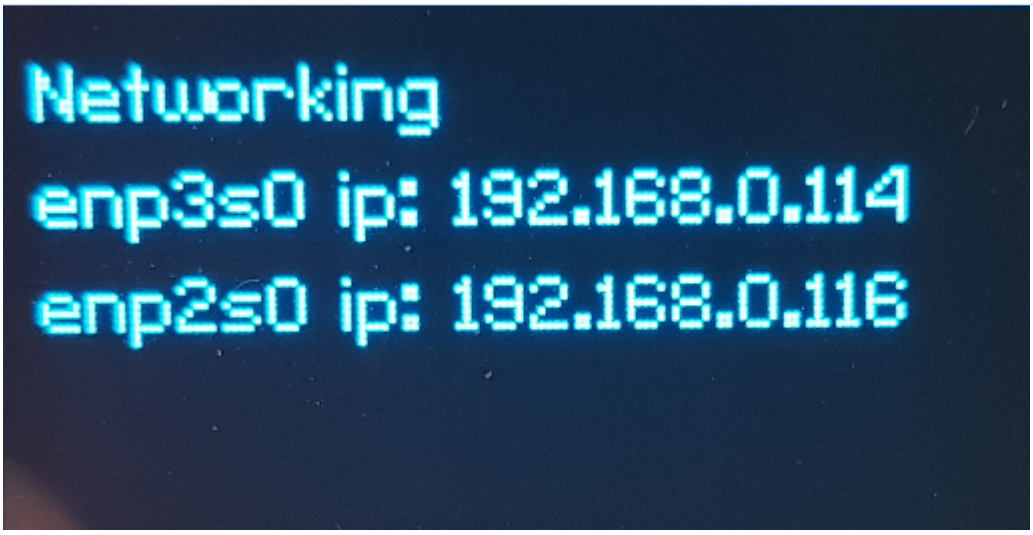


Bildschirm 2: Systemauslastung

1. Gerätebetriebszeit
2. CPU-Auslastung in %
3. CPU-Temperatur in Celsius
4. RAM-Auslastung in MB und %

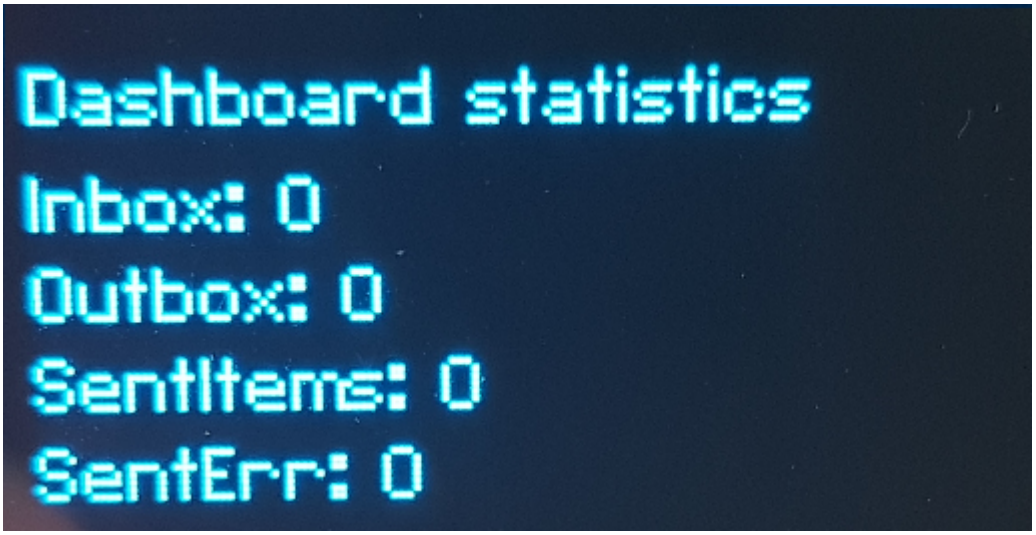


Bildschirm 3: Netzwerk-IP-Liste

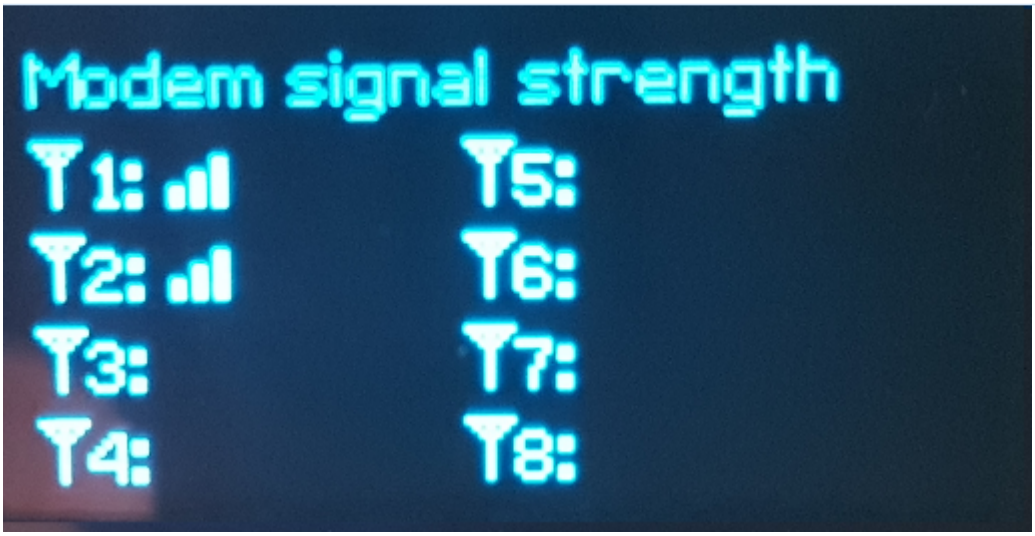


Bildschirm 4: Dashboard-Statistiken - Zählwerte für:

1. Eingang
2. Ausgang
3. Gesendete Elemente
4. Versandfehler



Bildschirm 5: Modulsignalstärke für alle 8 Modems



Automatische Stromsparverwaltung: Das Display schaltet sich nach 5 Minuten Inaktivität aus (keine SW-Taste gedrückt). Drücken Sie die SW-Taste, um es wieder zu aktivieren.

Übersicht der Weboberfläche

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

Anmelden

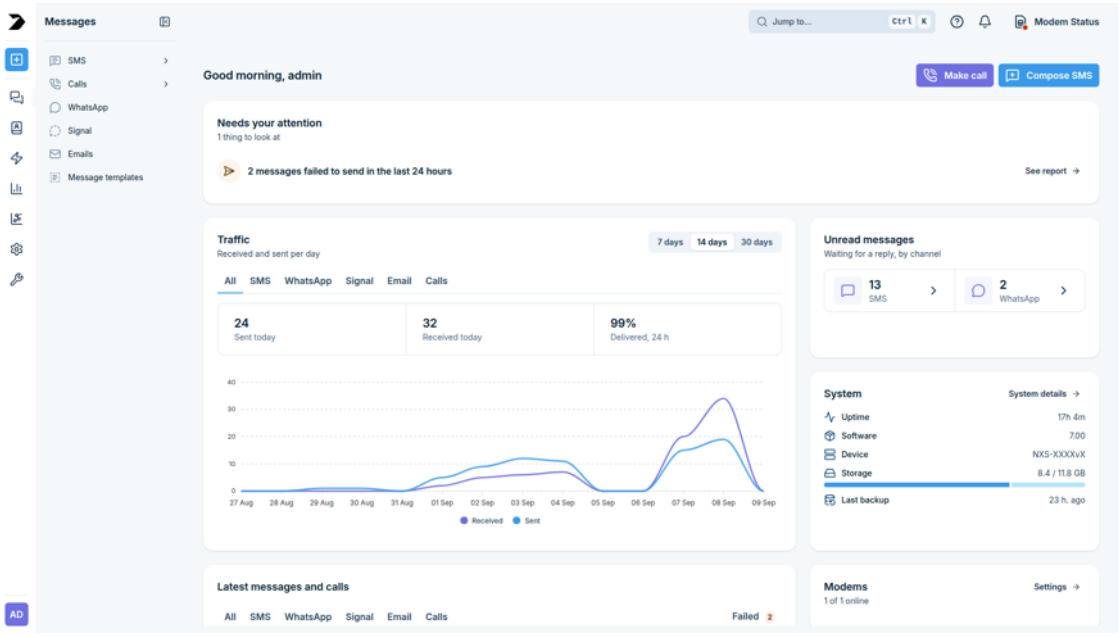


Die Anmeldeseite

Öffnen Sie die IP-Adresse oder den Hostnamen des Geräts in einem Browser und melden Sie sich mit Ihrem Login und Passwort an. Wenn die Mehrfaktor-Authentifizierung auf Geräteebene erzwungen wurde (siehe MFA), werden Sie auch aufgefordert, einen Einmalcode einzugeben.

- **Authentifizierungstyp** bestimmt, wo die Anmeldedaten überprüft werden: **Local (Standard)** gegen die eigene Benutzerliste des Geräts oder **LDAP** gegen einen Verzeichnisserver, den ein Administrator zunächst unter LDAP konfiguriert.
- **Passwort vergessen?** sendet Wiederherstellungsanweisungen unter Verwendung von SMS an die Telefonnummer des Kontos. Identifizieren Sie sich dort mit Ihrem Benutzernamen oder dieser Telefonnummer.
- Die Auswahl in der unteren rechten Ecke legt die Sprache der Anmeldeseite fest. Die Sprache der Oberfläche nach der Anmeldung stammt aus Ihrem eigenen Konto, siehe Persönliche Kontoeinstellungen.

Schnittstellenlayout

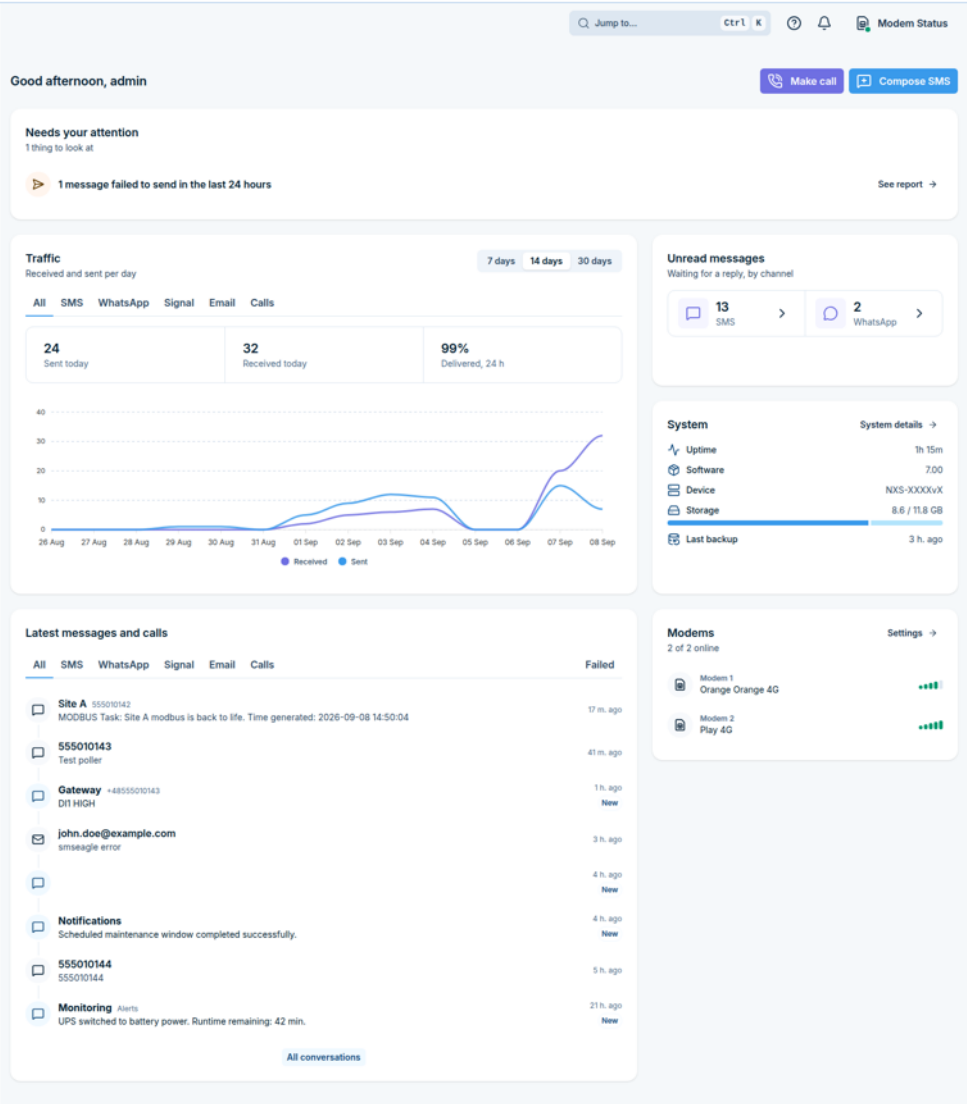


Linke Navigation erweitert über dem Hauptinhaltsbereich mit der oberen Leiste darüber

- **Linke Navigation** – eine Symbolleiste mit Zugriff auf Meldungen, Telefonbuch, Automatisierung, Berichte, Überwachung, Einstellungen und System. Das Hovern über ein Symbol benennt den Abschnitt; das Anklicken erweitert ein Panel, das die Seiten dieses Abschnitts nach Name auflistet, wie **Meldungen** oben. Die Schaltfläche in der eigenen Kopfzeile des Panels schließt es erneut.
- **Obere Leiste** – die **Gehe zu…** Suche (`Ctrl K`) ermöglicht es Ihnen, direkt zu jeder Seite nach Name zu springen, statt das Menü zu navigieren; sie zeigt auch Benachrichtigungen, Hilfe und die Modemstatusanzeige an.
- **Hauptinhaltsbereich** – die Seite für den derzeit ausgewählten Abschnitt.

Dashboard

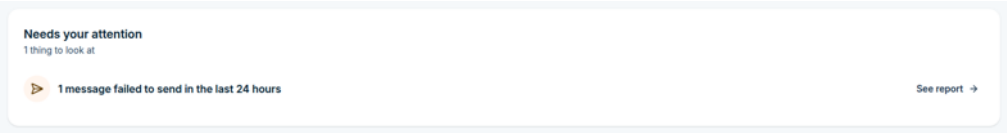
Das Dashboard ist die Landingpage nach der Anmeldung. Es öffnet sich mit einer Begrüßung und Schnellaktionsschaltflächen, gefolgt von Karten, die zusammenfassen, was beachtet werden muss, den Nachrichtenverkehr, unbeantwortete Gespräche, die Gerätegesundheit, die aktuelle Aktivität und den Modemstatus.



Das Dashboard

Benötigt Ihre Aufmerksamkeit

Sammelt die Elemente, die sofort beachtet werden sollten, mit der Anzahl unter dem Kartentitel und wie viele davon kritisch sind. Jeder Eintrag verweist auf die Seite, auf der Sie damit umgehen können, sodass eine im Postausgang hängende Nachricht auf den Postausgang-Ordner verweist und ein Zustellungsfehler-Eintrag auf Berichte und Statistiken verweist.



Benötigt Ihre Aufmerksamkeit

Verkehr

Empfangene und gesendete Nachrichten pro Tag. Die Registerkarten grenzen die Karte auf einen einzelnen Kanal (SMS, WhatsApp, Signal, E-Mail oder Anrufe) ein, und die Schaltflächen **7 Tage** /

14 Tage / **30 Tage** legen den Bereich des Diagramms unten fest. Drei Zähler sitzen über dem Diagramm:

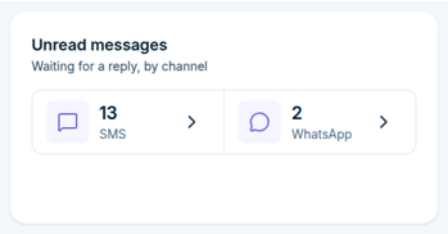
- **Heute gesendet** – Nachrichten, die seit Mitternacht gesendet wurden
- **Heute empfangen** – Nachrichten, die seit Mitternacht empfangen wurden
- **Zugestellt, 24 h** – Anteil der in den letzten 24 Stunden gesendeten Nachrichten, die als zugestellt bestätigt wurden



Verkehr

Ungelesene Nachrichten

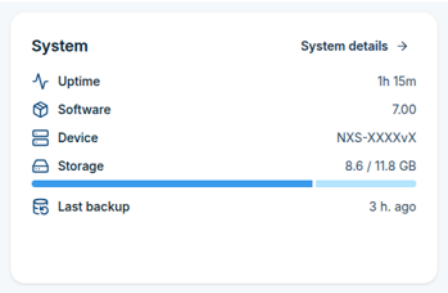
Gespräche, auf die noch eine Antwort wartet, gezählt pro Kanal. Jede Kachel öffnet die Gesprächsliste dieses Kanals, siehe Meldungen.



Ungelesene Nachrichten

System

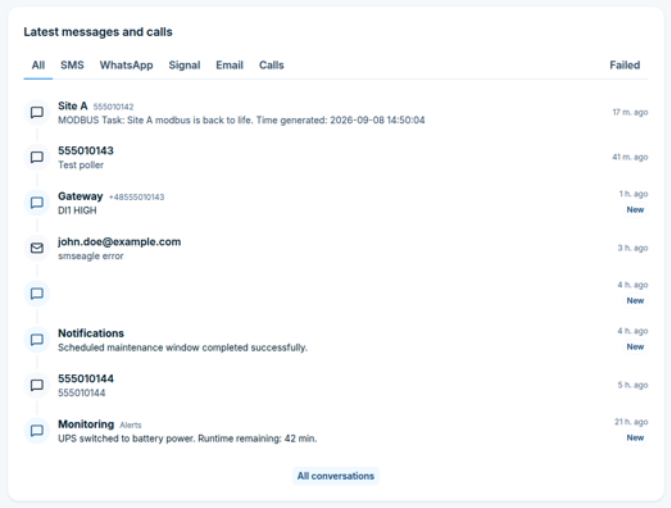
Systemzustand auf einen Blick: Betriebszeit, Softwareversion, Gerätetyp, verwendeter Speicher von insgesamt verfügbarem, und wann die letzte Sicherung durchgeführt wurde. **System details** öffnet den Abschnitt System.



System

Neueste Nachrichten und Anrufe

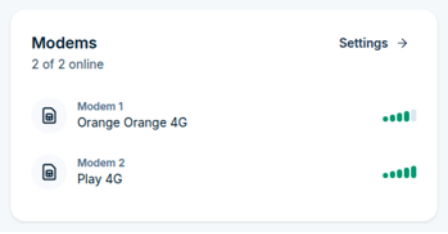
Der neueste Datenverkehr über alle Kanäle hinweg, neueste zuerst, mit Absender, Nachrichtenbeginn und Zeitpunkt der Ankunft. Die Registerkarten beschränken die Liste auf einen Kanal, und **Failed** zeigt, was nicht versendet wurde. Alles noch Ungelesene ist als **New** gekennzeichnet. **All conversations** öffnet die vollständige Liste unter Messages.



Neueste Nachrichten und Anrufe

Modems

Wie viele Modems online sind von denen, die installiert sind, und für jedes die Netzwerk-Registrierung, die Funktechnik und die Signalstärke. **Settings** öffnet die Modem-Konfiguration, siehe Settings.



Modems

Schnellaktionen

Zwei Schaltflächen in der oberen rechten Ecke des Dashboards.



Schnellaktionen

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

- **Compose SMS** öffnet ihn auf der Registerkarte **Message** – wählen Sie den Nachrichtentyp (SMS, Flash SMS, MMS, USSD Code, Signal, WhatsApp, Email), die Empfänger (aus dem

Phonebook, manuell eingegeben oder aus einer CSV-Datei), den Sendezeitpunkt und die Nachricht selbst aus. Statt den Text zu tippen, kann eine gespeicherte Vorlage verwendet werden, siehe Messages.

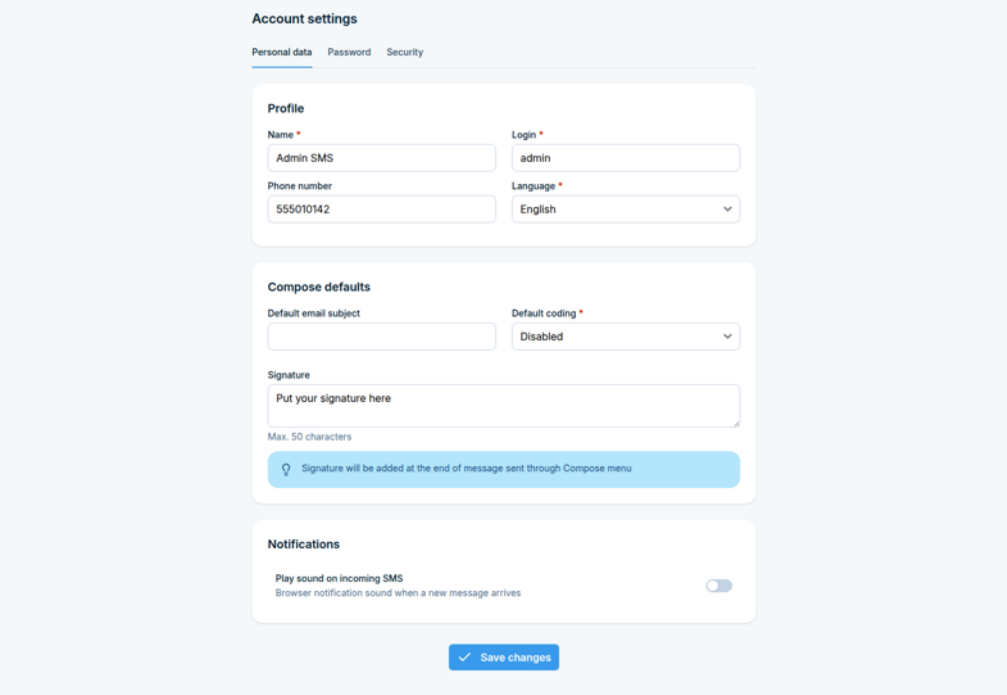
- **Make call** öffnet ihn auf der Registerkarte **Call** – wählen Sie den Anruftyp (nur klingeln, Text-zu-Sprache, eine Audiodatei), die Empfänger und wann der Anruf getätigt werden soll, siehe Messages.

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

Persönliche Kontoeinstellungen

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

Persönliche Daten

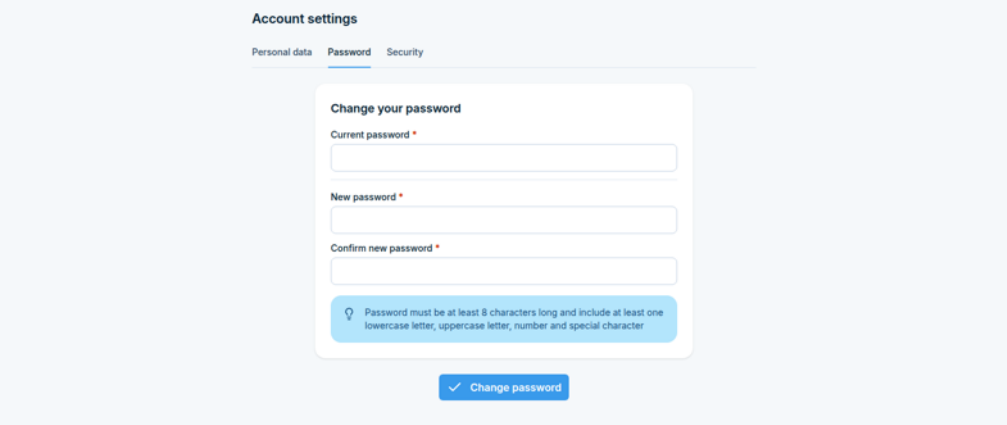


Account settings > Personal data

- **Profile** – Name, Anmeldedaten, Telefonnummer und die Oberflächensprache für Ihr Konto
- **Compose defaults** – der Standard-E-Mail-Betreff, die Standard-SMS-Codierung und eine Signatur von bis zu 50 Zeichen, die an über Compose versendete Nachrichten angehängt wird
- **Notifications** – ob der Browser einen Ton abspielt, wenn eine neue Nachricht ankommt

Save changes wendet die gesamte Registerkarte auf einmal an.

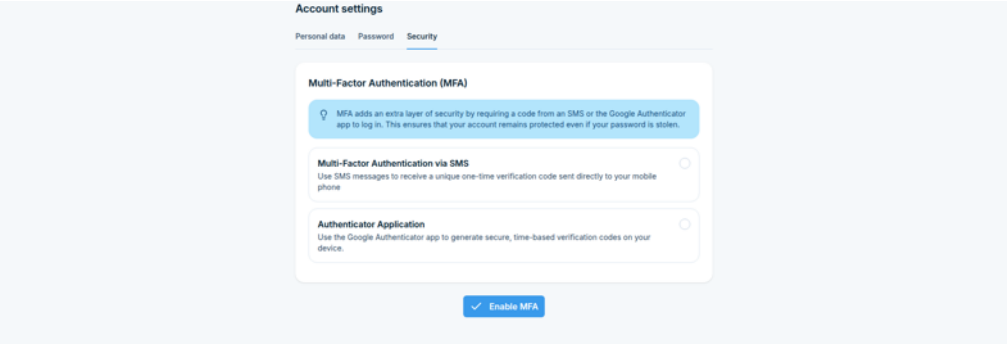
Passwort



Account settings > Password

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

Sicherheit



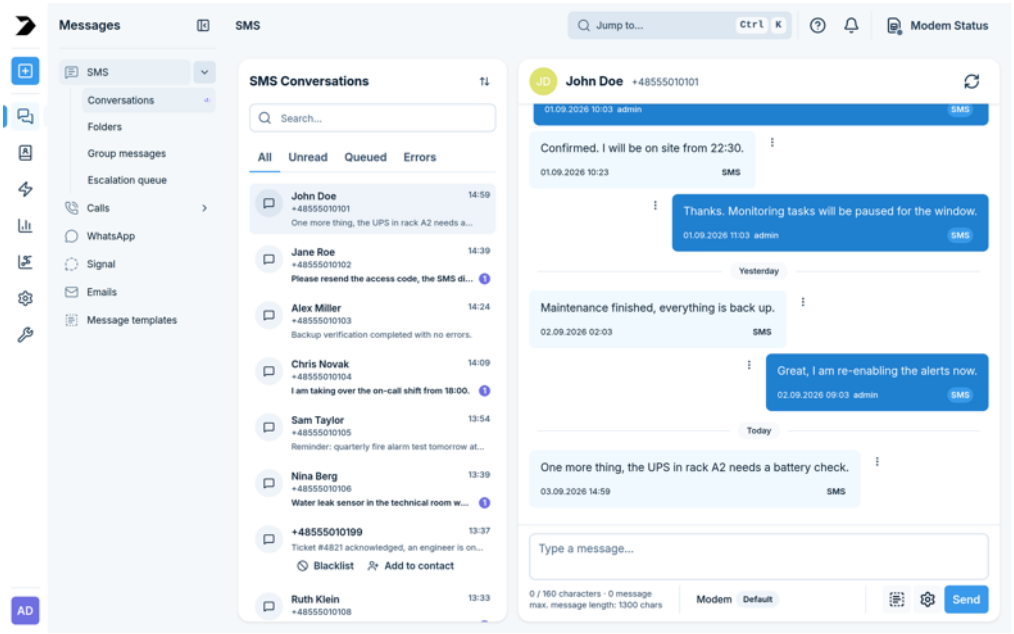
Account settings > Security

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

Nachrichten

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

SMS (Unterhaltungen)

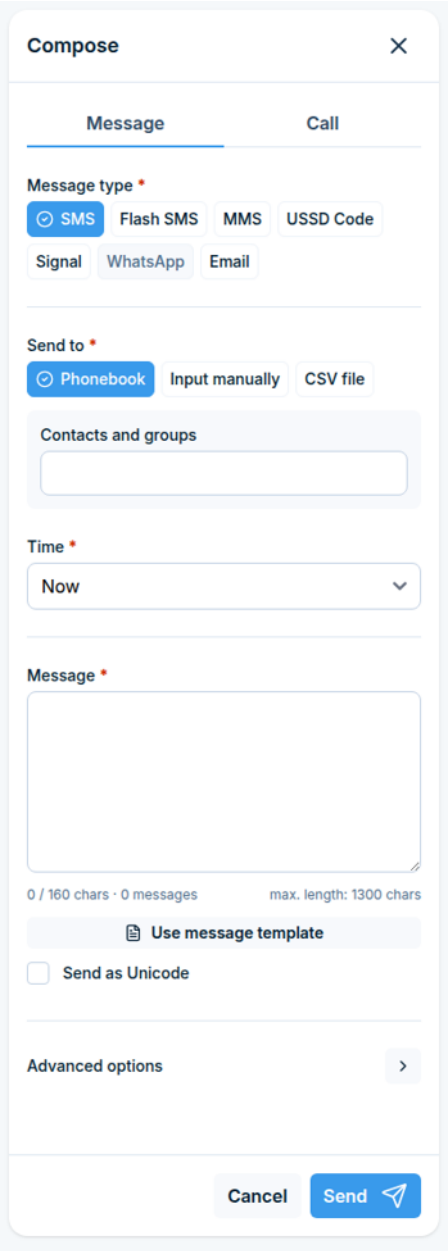


SMS-Unterhaltungen mit offenem Thread

Nachrichten > SMS > Unterhaltungen (`/messages/sms/`) ist das Haupt-SMS/MMS-Postfach: einen Thread pro Telefonnummer, neueste zuerst.

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

Eine Nachricht verfassen



Das Compose-Dialog

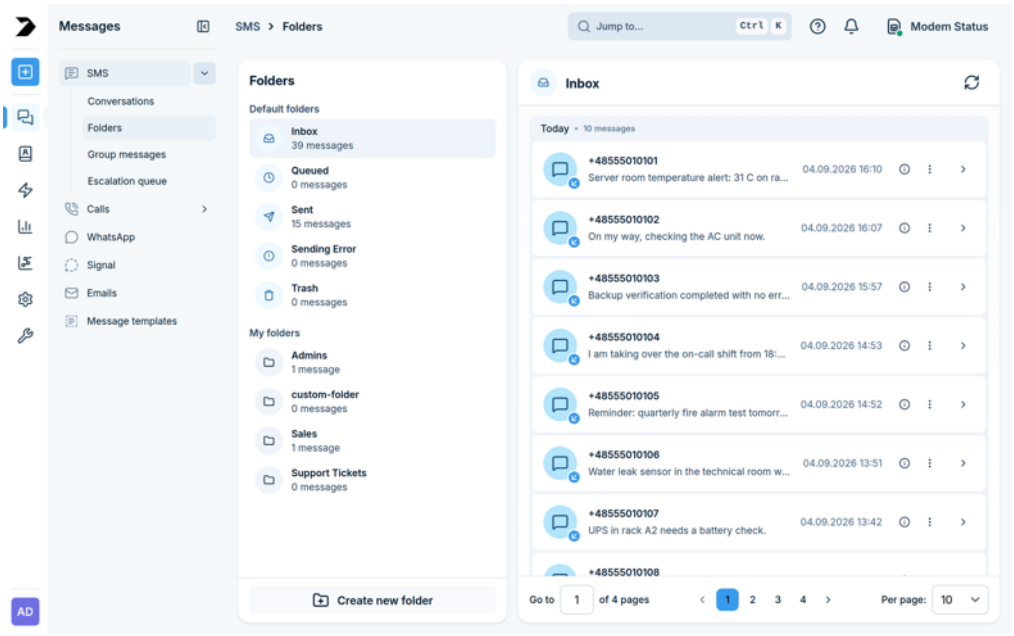
Compose wird als Panel auf der rechten Seite geöffnet und hat eine Registerkarte **Nachricht** und eine Registerkarte **Anruf**. Die Registerkarte „Nachricht“ enthält:

- **Nachrichtentyp** – SMS, Flash-SMS, MMS, USSD-Code, Signal, WhatsApp oder E-Mail. Ein Kanal, der auf diesem Gerät nicht konfiguriert ist, wird grau angezeigt, siehe Einstellungen.
- **Senden an** – wählen Sie Empfänger aus dem **Phonebook** (Kontakte und Gruppen), geben Sie sie manuell ein mit **Input manually** oder laden Sie eine **CSV-Datei** hoch.
- **Zeit** – senden Sie **Jetzt**, **Am Datum und Uhrzeit**, **Nach Verzögerung** oder **Zwischen Uhrzeiten**.
- **Nachricht** – der Text mit einem Live-Zähler der Zeichen und wie viele SMS-Teile sie bilden. **Use message template** füllt ihn aus einer gespeicherten Vorlage, und **Send as Unicode** wechselt die Kodierung für Nicht-GSM-Zeichen.

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

Senden reiht die Nachricht ein; der Thread wird sofort in Unterhaltungen angezeigt.

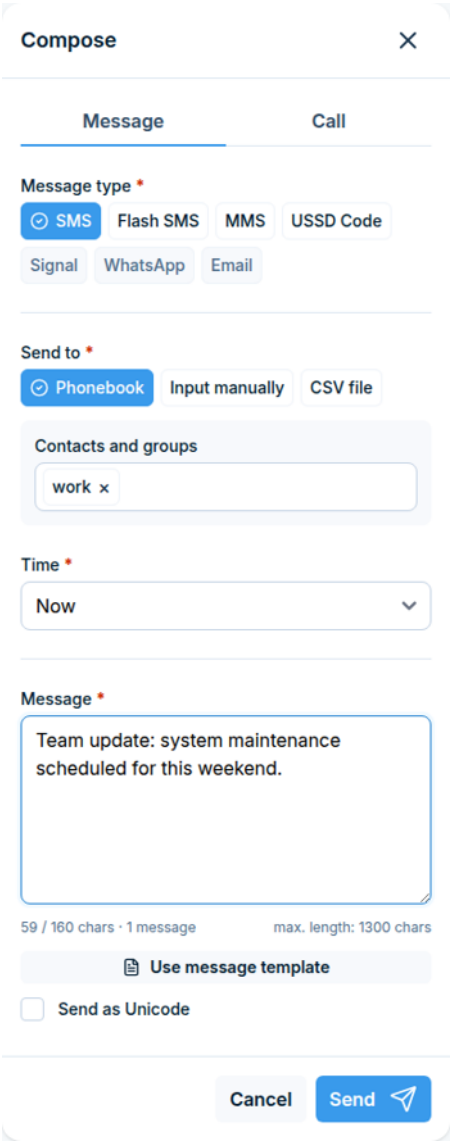
Ordner



Ordner

Nachrichten > SMS > Ordner (`/messages/sms/folders/`) listet die Standard-Ordner (Posteingang, In Warteschlange, Gesendet, Sendefehler, Papierkorb) zusammen mit allen benutzerdefinierten Ordnern auf, die Sie unter **Meine Ordner** erstellt haben. Jeder Ordner zeigt, wie viele Nachrichten er enthält. Klicken Sie auf **Neuen Ordner erstellen**, um einen eigenen hinzuzufügen – nützlich zusammen mit Inbox Rules, um eingehende Nachrichten automatisch zu sortieren, und Cleanup Folders, um sie automatisch zu bereinigen.

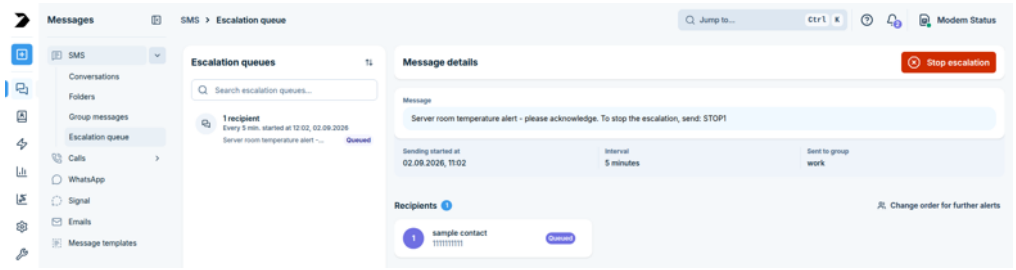
Gruppennachrichten



Eine Nachricht an eine Phonebook-Gruppe verfassen

Nachrichten > SMS > Gruppennachrichten (`/messages/sms/groups/`) listet Unterhaltungen auf, die Sie durch Versand an eine Phonebook-Gruppe anstelle einer einzelnen Nummer gestartet haben – einen Eintrag pro Gruppensendung, damit Sie überprüfen können, an wen eine Gruppennachricht ging, ohne einzelne Threads durchsuchen zu müssen.

Eskalationswarteschlange



Eskalationswarteschlange

Nachrichten > SMS > Eskalationswarteschlange (`/messages/sms/escalation/`) zeigt alle derzeit laufenden Eskalationen – eine Nachricht, die an eine Eskalationsgruppe gesendet wurde und ihren Weg durch die Kontaktliste noch nicht abgeschlossen hat. Die Einrichtung einer Eskalationsgruppe selbst wird unter Phonebook behandelt; diese Seite ist der Ort, an dem Sie eine bereits laufende Eskalation beobachten und kontrollieren können.

Jede laufende Eskalation wird mit ihrer Nachricht, dem Startdatum und dem Intervall aufgelistet. Wenn man eine öffnet, werden **Nachrichtendetails** angezeigt: der Nachrichtentext, die Startzeit, das Intervall, die Zielgruppe und jeder Empfänger mit einem Status von **Zugestellt**, **Wird gesendet**, **In Warteschlange** oder **Sendefehler**.

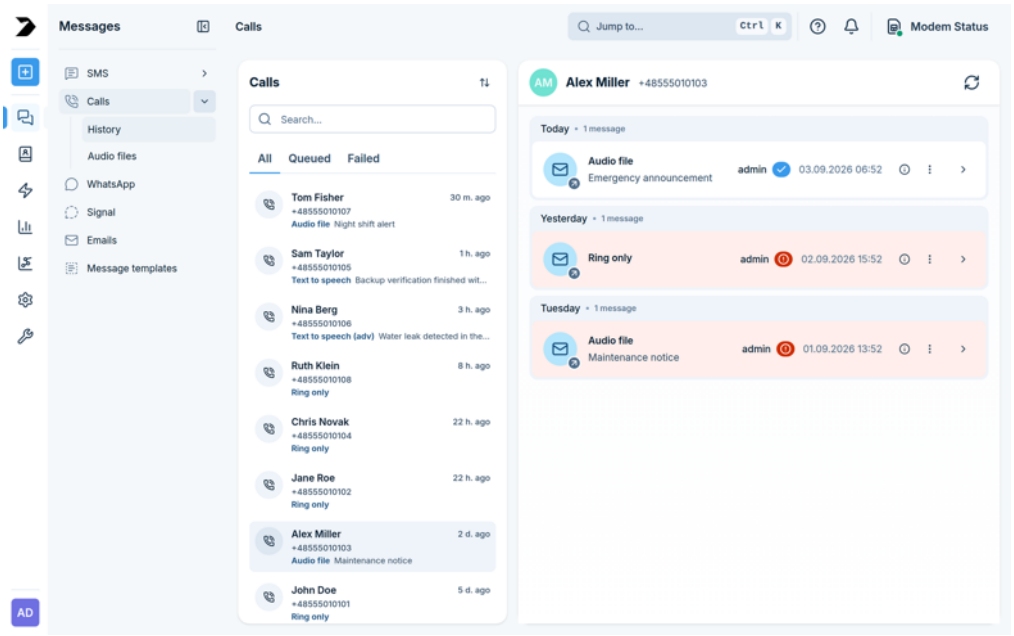
In dieser Ansicht können Sie:

- **Reihenfolge für weitere Benachrichtigungen ändern** – Ordnen Sie die Personen neu, die noch nicht kontaktiert wurden.
- **Eskalation beenden** – Brechen Sie die gesamte Eskalation sofort ab; niemand anders auf der Liste wird kontaktiert.

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

Anrufe

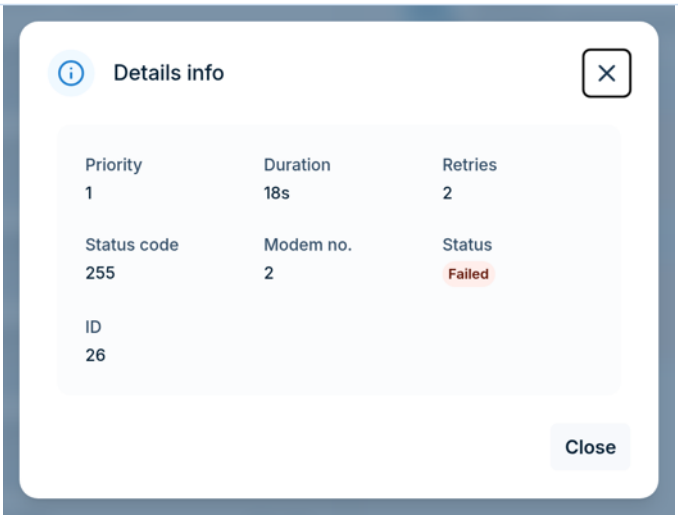
Verlauf



Anrufverlauf

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

- Die Registerkarten **Alle**, **In Warteschlange** und **Fehlgeschlagen** grenzen die Liste ein.
- Das Suchfeld findet Anrufe nach Nummer, Kontaktname oder nach dem vorgelesenen Text.
- Wenn Sie einen Anruf öffnen, werden seine Details angezeigt: Priorität, Dauer, Wiederholungen, Statuscode, Modemnummer und ID. Der Statuscode ist der, den Sie zitieren sollten, wenn Sie den Support zu einem fehlgeschlagenen Anruf befragen.
- Löschen Sie einen einzelnen Anruf oder wählen Sie mehrere aus und löschen Sie diese zusammen.

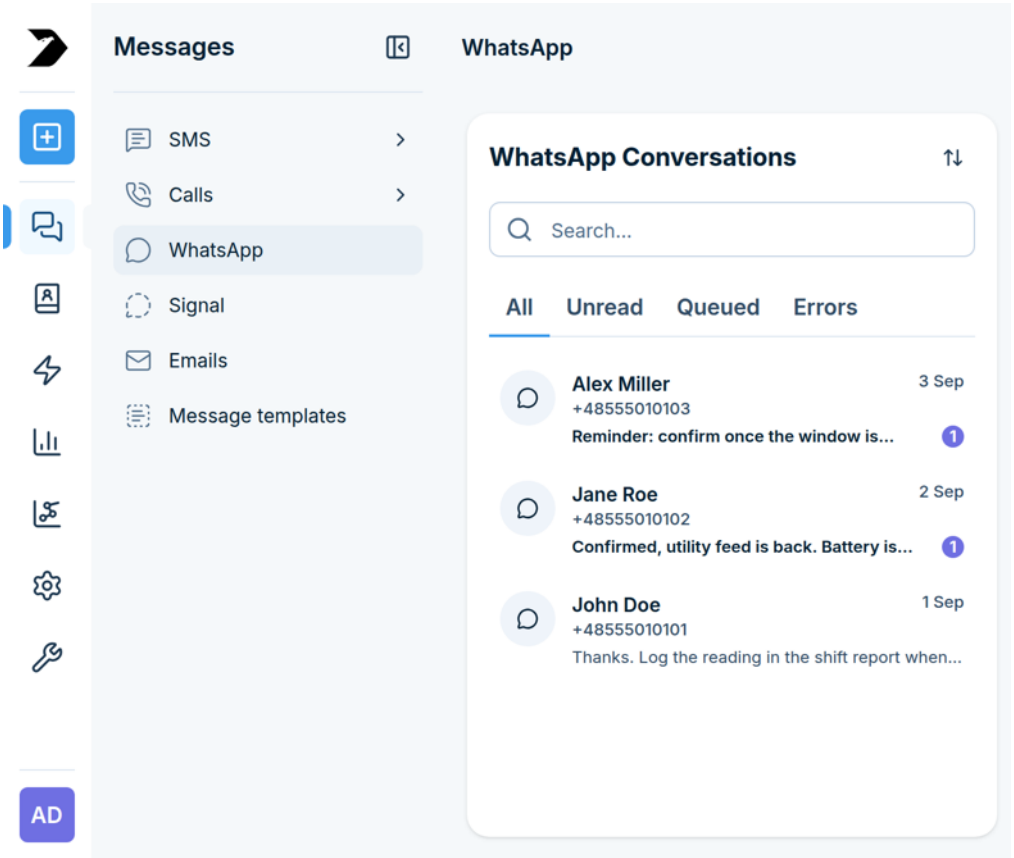


Anrufdetails

Anrufe werden wie Nachrichten in die Warteschlange gestellt: Einer, der später eingeplant ist, oder einer, der durch Priorität zurückgehalten wird, bleibt in dieser Liste als **In Warteschlange** bis er getätigt wird. Das Tätigen eines Anrufs (Anruftypen, Sprachmodelle und das Fenster „Verfassen

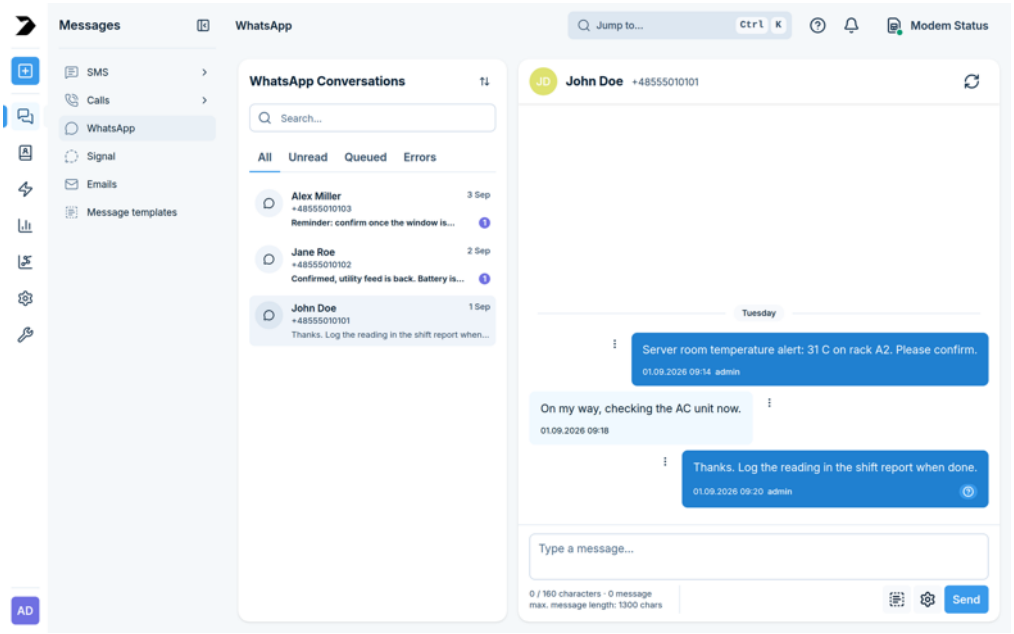
Anruf-Panel) wird unter Anrufe in den Einstellungen behandelt.

WhatsApp



Messages > WhatsApp (`/messages/whatsapp/`) listet WhatsApp-Konversationen auf – eine pro Nummer, neueste zuerst – nachdem der Kanal unter Settings verknüpft wurde.

- Filtern Sie mit den Registerkarten **Alle**, **Ungelesen**, **In Warteschlange** und **Fehler**.
- Anrufe wird hier weder ihre begebenheiten beschrieben werden. Die Verlauf wird seit einrichtung. Verlauf sind die nummern angerufen werden. Die historischen anrufen sind verfügbar mit richtiger informations zur überprüfung. Das gerät speichert dabei die anzahl der anrufe mit allen detalliert auf ihrer status und informationen die benötigen werden.
- Öffnen Sie ein Gespräch und antworten Sie direkt aus dem Feld unten (maximal 1300 Zeichen).
- Löschen Sie ein einzelnes Gespräch, oder wählen Sie mehrere aus und löschen Sie diese zusammen.

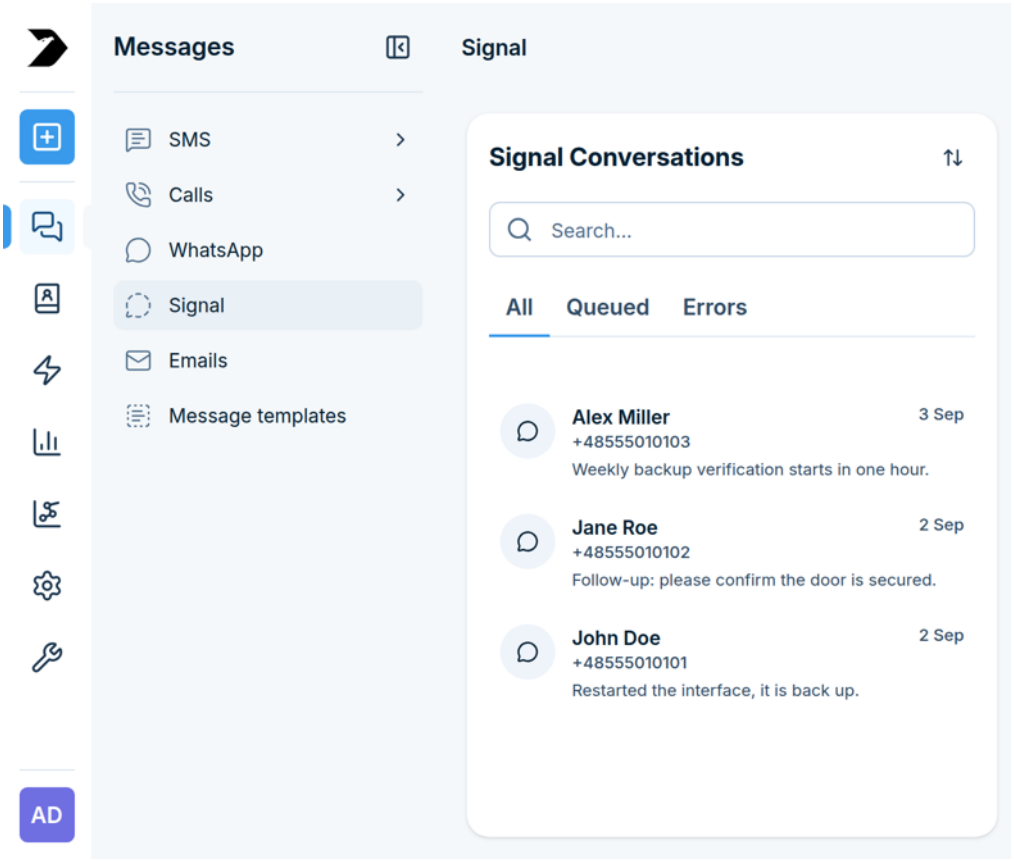


Ein offenes WhatsApp-Gespräch

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

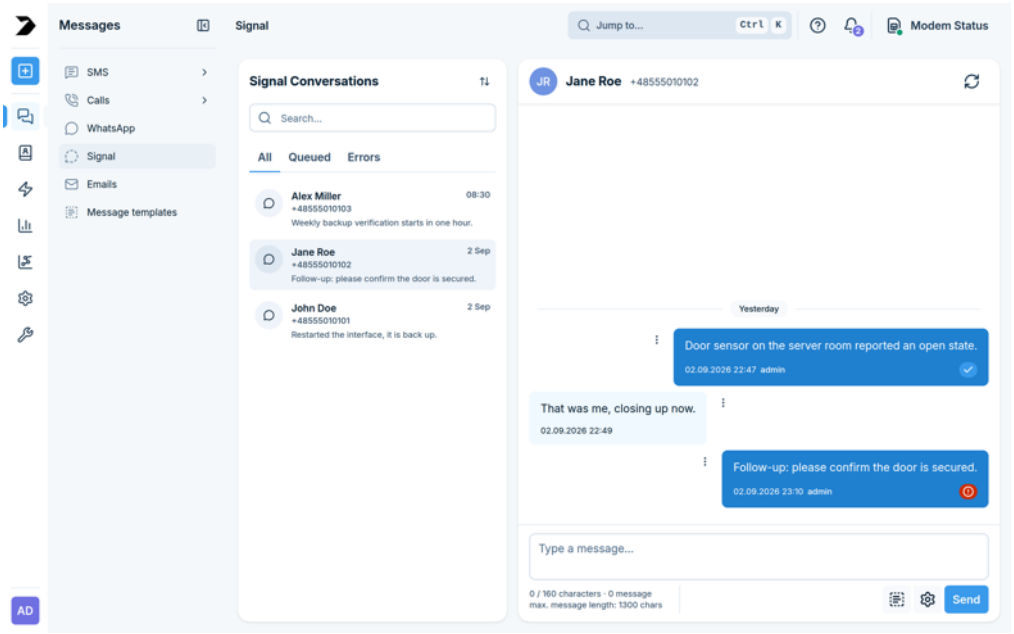
Hier werden nur Nachrichten angezeigt, die empfangen wurden, nachdem das Gerät verknüpft wurde.

Signal



Signal-Konversationen

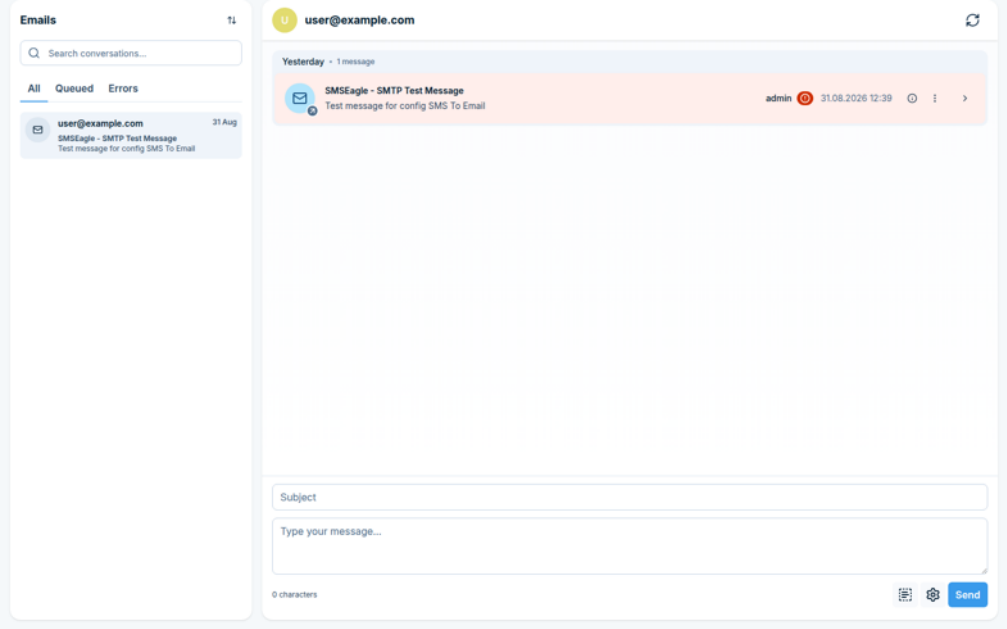
Messages > Signal (`/messages/signal/`) funktioniert wie WhatsApp oben, sobald eine Nummer unter Settings registriert wurde: eine Konversation pro Nummer, die Filter **All / Queued / Errors**, und Antwort über das Eingabefeld unten (maximal 1300 Zeichen). Signal hat keinen Tab **Unread**.



Eine offene Signal-Konversation

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

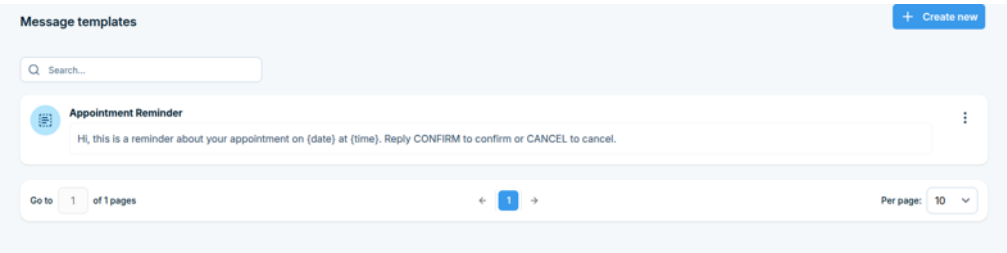
E-Mails



E-Mail-Konversationen

Messages > Emails (`/messages/email/`) listet E-Mail-Konversationen auf, einen Thread pro Adresse, neueste zuerst, mit den Filtern **All**, **Queued** und **Errors** – die gleiche Konversationsansicht wie bei SMS, WhatsApp und Signal für Post, die über SMS to Email und Email to SMS gesendet oder empfangen wird.

Nachrichtenvorlagen



Nachrichtenvorlagen

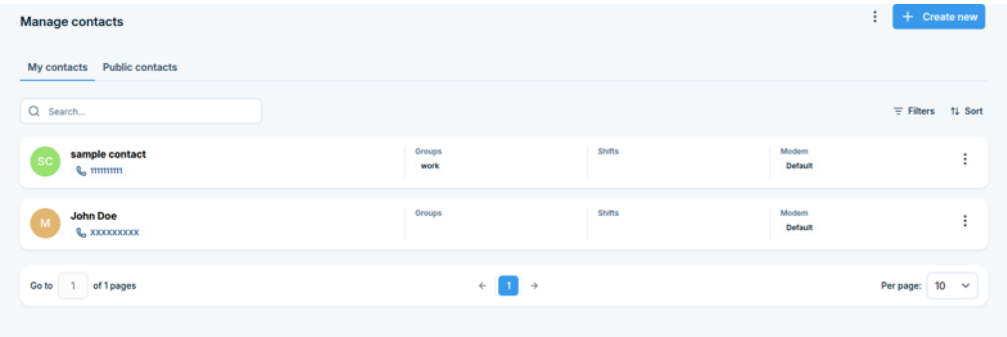
Messages > Message templates (`/messages/templates/`) speichert wiederverwendbare Nachrichtentexte für Compose, damit häufige Nachrichten nicht jedes Mal neu eingegeben werden müssen.

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

Telefonbuch

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

Kontakte



Telefonbuch-Kontaktliste

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

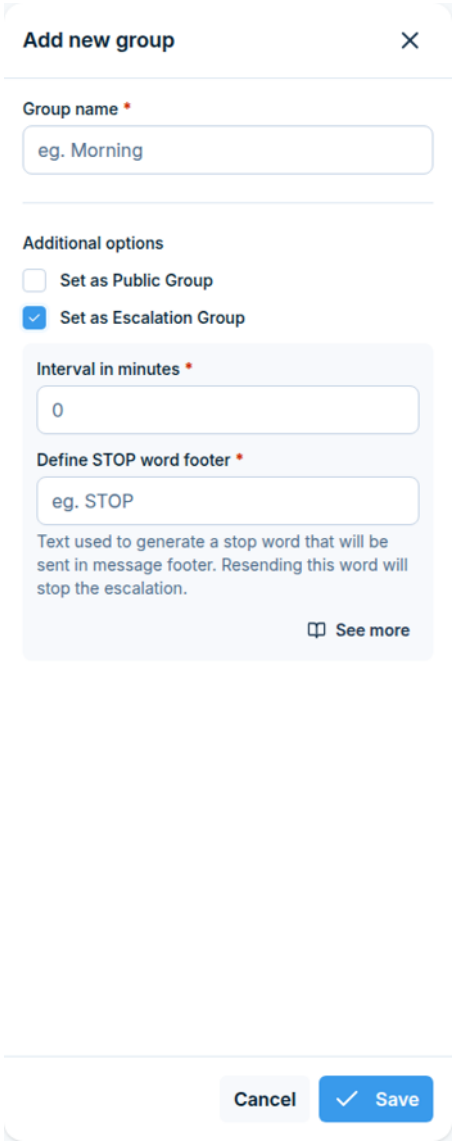
- **My contacts** - Kontakte, die nur Sie sehen und verwenden können.
- **Public contacts** - Kontakte, die mit anderen Benutzern des Geräts gemeinsam genutzt werden (notwendig, damit beispielsweise ein öffentlicher Kontakt von E-Mail zu SMS adressiert werden kann).

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

Gruppen

Telefonbuch > Gruppen (`/phonebook/groups`). Mit Gruppen können Sie eine ganze Menge von Kontakten auf einmal adressieren (zum Beispiel 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**, wenn andere Benutzer, Automatisierungsregeln oder die API an diese Gruppe senden können sollen.

Eskalationsgruppen



Eskalationsgruppenoptionen im Dialog „Add new group“

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

Schritt 1: Erstellen Sie die Eskalationsgruppe

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

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.
    - Maximal 8 Zeichen.
    - Nur Buchstaben, keine Ziffern, Leerzeichen oder Satzzeichen.
    - Es muss eindeutig sein – jede Eskalationsgruppe benötigt ihr eigenes Stopwort.
6. Klicken Sie auf **Save**.

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

Schritt 2: Fügen Sie Personen hinzu und legen Sie deren Reihenfolge fest

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 ganz oben wird zuerst kontaktiert – dies ist genau die Reihenfolge, in der Benachrichtigungen gesendet werden.

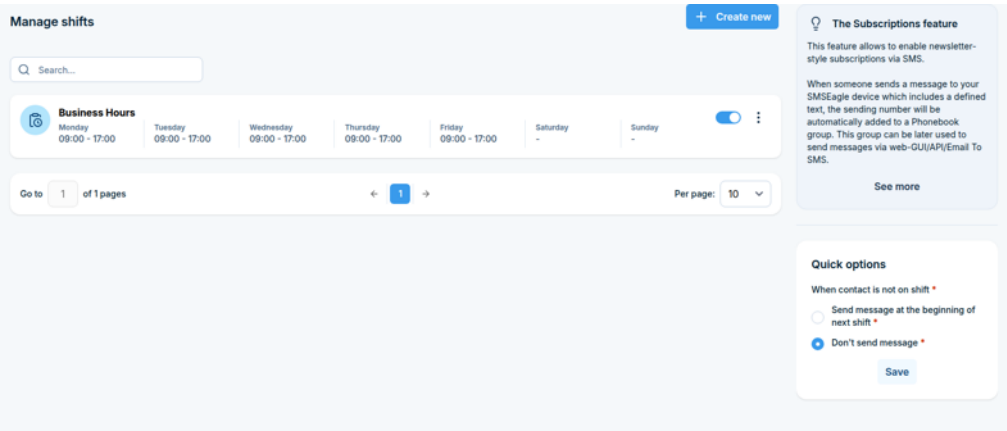
Schritt 3: Eine Eskalation auslösen

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

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

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

Schichten



Übersicht der Schichtverwaltung

Schichten beschreiben **wann eine Person Dienst hat**. Sobald Sie eine Schicht einem Kontakt zuweisen, prüft SMSEagle die Schicht vor dem Versand einer Nachricht: Wenn eine Nachricht an einen Kontakt adressiert ist, der sich derzeit außerhalb seiner Schichtzeiten befindet, hält SMSEagle die Nachricht entweder bis zum Beginn der nächsten Schicht und liefert sie dann aus, oder sendet sie gar nicht - Sie wählen, was geschieht (siehe Schritt 4 unten).

Typische Verwendung: ein Bereitschaftsplan, bei dem die Nachtschicht nicht durch Benachrichtigungen für die Tagschicht geweckt werden sollte.

> **Gut zu wissen:** ein Kontakt mit **keiner zugewiesenen Schicht** wird immer als verfügbar angesehen. Schichten beschränken nur die Kontakte, denen sie zugewiesen sind.

Bevor Sie beginnen

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

Schritt 1: Öffnen Sie die Seite „Shifts“

Phonebook > Shifts (`/phonebook/shifts`) listet die bereits erstellten Schichten auf, mit einem **Quick options** Kasten 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** aktiviert, 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 Zeiten für jeden Wochentag fest: geben Sie eine **From** und eine **To** Zeit für jeden Tag ein, an dem die Person Dienst hat, und lassen Sie einen Tag leer, wenn sie nicht tätig ist.

5. Klicken Sie auf **Save**.

Regeln für Schichtzeiten

- **From** muss früher als **To** am selben Tag sein.
- Sowohl **From** als auch **To** müssen ausgefüllt sein oder beide leer gelassen sein. Ein halb ausgefüllter Tag wird mit einer Fehlermeldung abgelehnt.
- Mindestens ein Tag muss Zeiten haben.

  Schichten über Mitternacht: Eine Schicht, die Mitternacht überquert (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.

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

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

Schritt 4: Wählen Sie, was außerhalb der Schichtzeiten geschieht

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 erfasst.

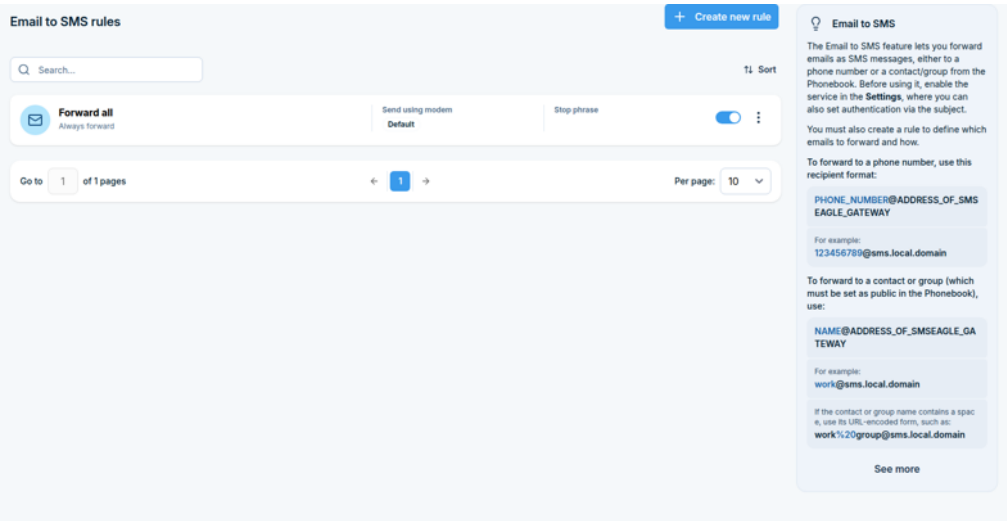
Wählen Sie die gewünschte Option aus und klicken Sie auf **Save**.

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

Automatisierung

Dieses Kapitel behandelt den Abschnitt **Automatisierung** der Web-Oberfläche in der gleichen Reihenfolge, in der die Regeln dort angezeigt werden.

E-Mail zu SMS



E-Mail-zu-SMS-Regeln

Mit der Funktion E-Mail zu SMS können Sie eingehende E-Mails als SMS-Nachrichten an eine Telefonnummer oder an einen Kontakt/eine Gruppe aus Ihrem Telefonbuch weiterleiten.

Wo finde ich diese Funktion

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 Service aktivieren und konfigurieren, wie E-Mails in Nachrichten konvertiert werden – siehe E-Mail zu SMS unter Einstellungen.

Schritt 1: Understand the recipient address format

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

Zur Weiterleitung an eine Telefonnummer:

```
PHONE_NUMBER@ADDRESS_OF_SMSEAGLE_GATEWAY
```

Beispiel: `999888777@gateway.smseagle.eu`

Zur Weiterleitung an einen Kontakt oder eine Gruppe aus dem Telefonbuch (der Kontakt oder die Gruppe muss als **öffentlich** eingestellt sein):

```
NAME@ADDRESS_OF_SMSEAGLE_GATEWAY
```

Beispiel: `work@gateway.smseagle.eu`

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

Anstelle der Gateway-IP-Adresse können Sie einen Fully Qualified Domain Name verwenden, der unter **Einstellungen > Kanäle > E-Mail > E-Mail zu SMS > Erweiterte Einstellungen > FQDN-Hostname** eingestellt wird. Wenn dort **LDAP-Kontakte verwenden** aktiviert ist, wird dasselbe `NAME@GATEWAY`-Format auch Kontakte und Gruppen aufgelöst, die in LDAP / Active Directory definiert sind.

Standardmäßig wird der Inhalt 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, zur Authentifizierung verwendet oder statt des Hauptteils gesendet werden.

Schritt 2: Create a new rule

Gehen Sie zu **Automatisierung > E-Mail > E-Mail zu SMS** und klicken Sie auf **Create new rule**. Ein Bereich mit dem Titel Add Email to SMS rule wird auf der rechten Seite angezeigt.

Feld	Beschreibung
Rule name *	Ein Name zur Identifizierung der Regel (erforderlich, max. 100 Zeichen)
Forward for *	Always send leitet jede eingehende E-Mail weiter, die dem Adressformat entspricht. Specified sender / message contains fügt Filterbedingungen hinzu, siehe Schritt 3.
Send using modem	Welches Modem das SMS sendet. Standard ist Default. Wird nur auf Geräten mit mehr als einem Modem angezeigt.
Stop phrase	Text starting from this phrase will be removed from the message (case sensitive)
Priorität	Sendpriorität von 0 bis 5. Nachrichten mit höherer Priorität werden zuerst verarbeitet.
Anruf nach SMS-Versand	Nein, Nur Klingelton, Ja - Text-zu-Sprache, or Ja - Text-zu-Sprache (erweitert). Die verfügbaren Optionen hängen von der Stimme und den TTS-Fähigkeiten Ihres Geräts ab.
Sprachmodell	Stimme für den Text-zu-Sprache-Anruf. Wird nur auf Geräten angezeigt, die erweiterte TTS unterstützen, und nur nach Auswahl von Ja - Text-zu-Sprache (erweitert).
UTF-8-Konvertierung erzwingen	Erzwingt die Konvertierung des Nachrichtentexts zu UTF-8
Gesprächsverlauf entfernen	Entfernt den zitierten Verlauf der E-Mail-Konversation aus dem Nachrichtentext

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

Schritt 3: Filterbedingungen hinzufügen (optional)

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

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

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

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

Schritt 4: Vorhandene Regeln verwalten

Jede Regel wird als Karte in der E-Mail-zu-SMS-Liste angezeigt mit:

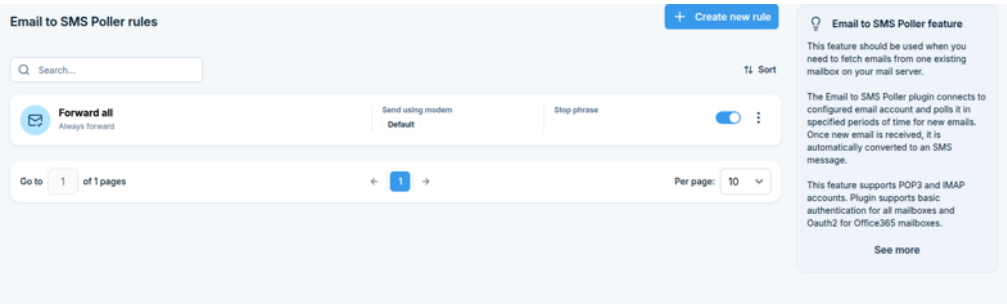
- dem Regelnamen
- der Weiterleitungsbedingung, z. B. Forward when incoming: email address contains: ..., oder Always forward, wenn keine Bedingung festgelegt ist
- das Modem, das zum Versand verwendet wird
- die konfigurierte Stop-Phrase
- ein Ein-/Aus-Schalter zum Aktivieren oder Deaktivieren der Regel, ohne sie zu löschen
- ein ⋮ Menü mit **Edit** und **Delete**

Zusätzliche Steuerelemente in der Liste:

- **Search** filtert Regeln nach Namen.
- Das Auswählen von Regelkontrollkästchen enthüllt Massenaktionen: **Enable / Disable** und **Delete**.
- 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 erläutert die Formate der Empfängeradressen und enthält einen Button **See more** (Mehr anzeigen), der auf die Funktionsseite unter smseagle.eu verlinkt.

Email to SMS Poller



E-Mail-zu-SMS-Poller-Regeln

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

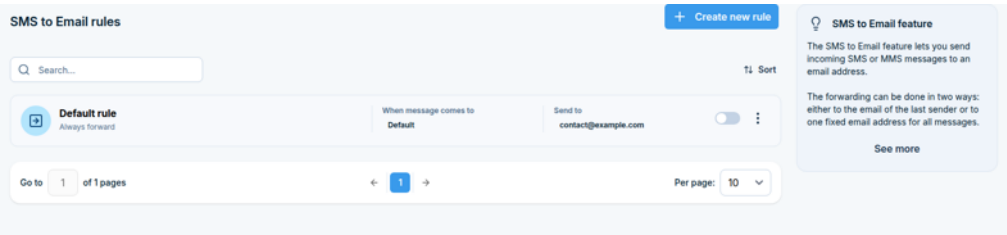
Wo finde ich diese Funktion

Unter **Automation > Email > Email to SMS Poller** (`/automation/email-to-sms-poller/`) erstellen und verwalten Sie Regeln. 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 – Sie benennen die Regel, wählen, ob sie alle eingeholten E-Mails weiterleitet oder nur solche, die bestimmte Sender-/Betreff-/Inhalts-Bedingungen erfüllen, und legen dieselben Pro-Regel-Optionen fest (Modem, Stoppphrase, Priorität, Anruf nach dem Versand).

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 diese in Ihrem Postfach lesen können, anstatt sich bei SMSEagle anzumelden.

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

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

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 diese ausgefüllt und getestet ist – siehe SMTP Configuration. Ohne diese werden Regeln zwar abgeglichen, aber es kommt keine E-Mail an.

Wenn Sie die Weiterleitung auf Grundlage von Sender-Kontakten oder Gruppen durchführen möchten, müssen diese Kontakte und Gruppen im Phonebook als **Public** (Öffentlich) gekennzeichnet sein.

Schritt 1: SMS to Email-Seite öffnen

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

Schritt 2: Erstellen Sie eine Regel

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

Benennen Sie die Regel

Geben Sie unter **Rule name** (Regelname) etwas Aussagekräftiges ein, z. B. `Forward all to support` (Alles an Support weiterleiten). Maximal 100 Zeichen.

Entscheiden Sie, welche Nachrichten weitergeleitet werden sollen

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

Option	Was es bedeutet
Always forward (Immer weiterleiten)	Jede eingehende SMS und MMS wird weitergeleitet.
Angegeben Absender / Nachricht	Nur Nachrichten, die die unten festgelegten Bedingungen erfüllen, werden weitergeleitet.

Wenn Sie **Angegeben Absender / Nachricht** gewählt haben, stehen zwei Bedingungen zur Verfügung. Sie können eine oder beide verwenden. Bei Verwendung beider Bedingungen muss eine Nachricht **beide** erfüllen, um weitergeleitet zu werden.

Wenn eingehende SMS von kommt Aktivieren Sie diese Option und wählen Sie die Kontakte oder Gruppen aus, deren Nachrichten weitergeleitet werden sollen. Beginnen Sie zu tippen, um zu suchen. Nur **öffentliche** Kontakte und Gruppen können hier ausgewählt werden.

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

Beschränken Sie die Regel auf ein Modem (nur Multi-Modem-Geräte)

Wenn Ihr Gerät mehr als ein Modem hat, wird ein Feld **Wenn Nachricht ankommt bei** angezeigt. Lassen Sie es auf **Beliebiges Modem** oder wählen Sie ein bestimmtes Modem aus, sodass die Regel nur für Nachrichten gilt, die auf dieser SIM-Karte ankommen. Bei Single-Modem-Geräten wird dieses Feld nicht angezeigt.

Wählen Sie die Ziel-E-Mail-Adresse aus

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

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

Legen Sie den E-Mail-Betreff fest

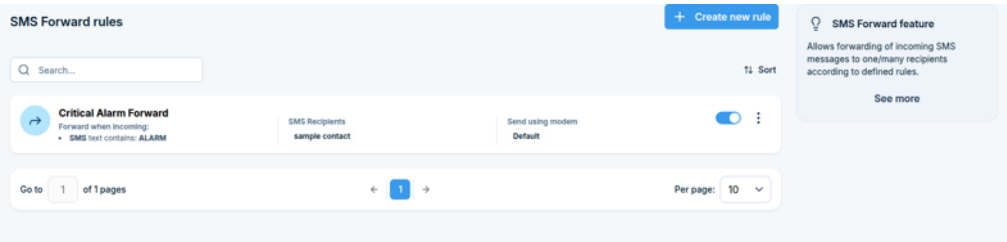
E-Mail-Betreff steuert die Betreffzeile der weitergeleiteten E-Mail. Sie können Platzhalter verwenden, die beim Versand der E-Mail durch reale Werte ersetzt werden:

Platzhalter	Ersetzt durch
`{SENDER}`	Die Telefonnummer, von der die SMS kam
`{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: Temperaturalarm im Serverraum ausgelöst`. Maximal 150 Zeichen.

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

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 auf die weitergeleitete SMS aufsetzen, damit eine Benachrichtigung nicht überschlafen wird.

Typische Einsatzbereiche: Alarmmeldungen von einer Maschine an das gesamte On-Call-Team senden, Nachrichten von einer gemeinsamen Nummer an die gerade diensthabende Person weitergeben, oder einen kurzen Maschinencode in einen lesbaren Satz für das Team umwandeln.

Bevor Sie beginnen

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

Schritt 1: Öffnen Sie die Seite SMS Forward

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

Schritt 2: Erstellen Sie eine Regel

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

Benennen Sie die Regel und legen Sie ihre Priorität fest

Rule name Etwas Aussagekräftiges, zum Beispiel `Alarms to on-call team`. Maximal 100 Zeichen.

Priority Eine Zahl von 0 bis 9. Nachrichten, die von einer höherprioritären Regel erzeugt werden, werden zum Versand früher in die Warteschlange eingefügt als Nachrichten von einer niedrigerprioritären Regel. Belassen Sie es bei der Standardeinstellung, es sei denn, Sie haben dringende Regeln, die Massenregeln übertreffen müssen.

Entscheiden Sie, welche Nachrichten weitergeleitet werden sollen

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

Option	Was es bedeutet
All incoming messages	Jede eingehende SMS wird weitergeleitet.
Angegeben Absender / Nachricht	Nur Nachrichten, die die unten festgelegten Bedingungen erfüllen, werden weitergeleitet.

Wenn Sie **Angegeben Absender / Nachricht** gewählt haben, stehen zwei Bedingungen zur Verfügung. Sie können eine oder beide verwenden. Bei Verwendung beider Bedingungen muss eine Nachricht **beide** erfüllen, um weitergeleitet zu werden.

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

Beschränken Sie die Regel auf ein Modem (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, damit die Regel nur auf Nachrichten angewendet wird, die auf dieser SIM-Karte eingehen. Bei Geräten mit nur 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 Wahl erscheint, **Message header**:

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

Option B: Custom text

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

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

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

Wählen Sie die Empfänger

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

Optionalen Telefonanruf hinzufügen

Call after sending SMS bewirkt, dass das Gerät auch einen Sprachanruf an dieselben Empfänger tätigt. Die verfügbaren Optionen hängen von Ihrem Gerätemodell ab:

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

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

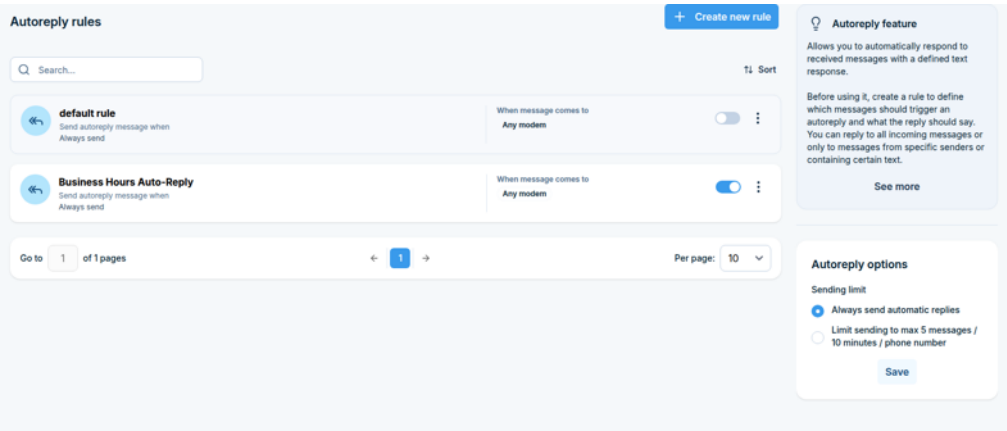
Klicken Sie auf **Save**. Die Regel beginnt sofort mit neu eingegangenen Nachrichten zu wirken.

Wie die Weiterleitung funktioniert

- Die Textbedingung ist eine **Contains**-Übereinstimmung, keine exakte Übereinstimmung. Eine Regel, die nach `ALARM` sucht, leitet eine Nachricht weiter, die `ROOM 4 ALARM triggered` lautet.
- Wenn mehrere Regeln auf dieselbe eingehende Nachricht zutreffen, leitet **jede** von ihnen separat weiter, sodass Empfänger mehr als eine SMS erhalten können. Halten Sie die Bedingungen unterschiedlich, um Duplikate zu vermeiden.
- Regeln gelten nur für Nachrichten, die eintreffen, nachdem die Regel erstellt und aktiviert wurde. Sie verarbeiten keine Nachrichten, die sich bereits im Posteingang befinden.
- Empfänger können aus eigenen Gründen übersprungen werden: **Vacation mode** beim Kontakt, eine Schicht, die derzeit außerhalb ihrer Zeiten liegt (siehe Shifts), oder die Nummer 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 immer wieder Nachrichten hin und her.

Autoreplies



Autoreply-Regeln und Optionen für Sendungslimit

Was diese Funktion macht

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

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

Typische Anwendungen: Bestätigung, dass eine Bestellanfrage eingegangen ist, Mitteilung, dass die Nummer nachts unbeaufsichtigt ist, oder Antwort auf ein Stichwort mit festen Informationen wie Öffnungszeiten.

Bevor Sie beginnen

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

Schritt 1: Öffnen Sie die Autoreplies-Seite

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 in Schritt 3 beschrieben ist.

Schritt 2: Erstellen Sie eine Regel

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

Benennen Sie die Regel

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

Entscheiden Sie, welche Nachrichten beantwortet werden sollen

Wählen Sie **Autoantwort senden für**:

Option	Was es bedeutet
All incoming messages	Jede eingehende SMS erhält eine Antwort.
Angegeben 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 von kommt Aktivieren Sie dies und wählen Sie die Kontakte oder Gruppen aus, die eine Antwort erhalten sollen. Geben Sie zur Suche an zu tippen. Nur **öffentliche** Kontakte und Gruppen können hier ausgewählt werden.

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

Beschränken Sie die Regel auf ein Modem (nur Multi-Modem-Geräte)

Wenn Ihr Gerät mehr als ein Modem hat, wird ein Feld **Wenn Nachrichten zu kommt** angezeigt. Lassen Sie es auf **Beliebiges Modem**, oder wählen Sie ein bestimmtes Modem, damit die Regel nur auf diesem SIM-Kartenschacht eingehende Nachrichten beantwortet. Bei Single-Modem-Geräten wird dieses Feld nicht angezeigt.

Schreiben Sie die Antwort

Autoantwortnachricht Der Text, der zurückgesendet wird. Maximal 2000 Zeichen. Der gleiche Text geht an alle, 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, z. B. 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 wirken.

Schritt 3: Sendegrenze festlegen

Das Feld **Autoantwortoptions** auf der rechten Seite der Seite kontrolliert, wie oft das Gerät bereit ist, automatisch auf dieselbe Telefonnummer zu antworten:

Option	Ergebnis
Immer automatische Antworten senden	Jede passende Nachricht erhält eine Antwort, egal wie viele ankommen.
Senden auf maximal 5 Nachrichten / 10 Minuten / Telefonnummer begrenzen	Maximal 5 automatische Antworten gehen in 10 Minuten an dieselbe Telefonnummer. Weitere Nachrichten von dieser Nummer werden erst nach Ablauf des Zeitfensters beantwortet.

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

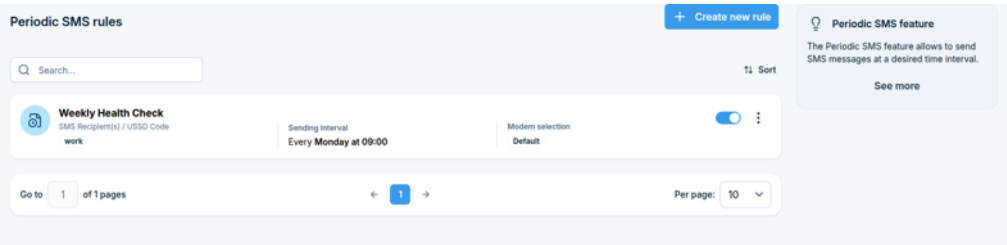
> **Die Verwendung der Grenze wird dringend empfohlen.** Ohne sie können sich zwei Geräte, die beide automatisch antworten, gegenseitig antworten, was SMS-Gutschriften schnell aufbraucht. Die Grenze ist der Schutz davor.

Diese Einstellung ist **global**. Sie gilt für alle Autoantwortregel auf dem Gerät.

Wie Matching funktioniert

- Die Textbedingung ist ein **enthält**-Match, kein exaktes Match. Eine Regel, die nach `PRICE` sucht, beantwortet eine Nachricht mit dem Inhalt `what is the PRICE of item 5`.
- Wenn mehrere Regeln auf die gleiche eingehende Nachricht zutreffen, sendet **jede** von ihnen eine eigene Antwort, sodass der Absender mehr als eine SMS erhalten kann. Halten Sie die Bedingungen unterschiedlich, wenn Sie nur eine Antwort möchten.
- Regeln gelten nur für Nachrichten, die eintreffen, nachdem die Regel erstellt und aktiviert wurde. Sie verarbeiten keine Nachrichten, die sich bereits im Posteingang befinden.

Periodische SMS



Dialog zum Hinzufügen einer periodischen SMS-Regel

Was diese Funktion macht

Periodische SMS sendet eine Nachricht **automatisch nach einem sich wiederholenden Zeitplan**, ohne dass jemand auf „Senden

Sie können zwei Dinge planen:

- eine **SMS** an Telefonnummern oder eine Adressbuchgruppe, 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 „System aktiv“-Nachricht, eine wöchentliche Erinnerung an ein Bereitschaftsteam, eine monatliche Abfrage des Guthabens einer Prepaid-SIM.

Bevor Sie beginnen

- Wenn Sie an eine Gruppe senden möchten, muss die Gruppe in **Phonebook > Groups** existieren 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 die Liste der Regeln, die Sie bereits haben.

Schritt 2: Erstellen Sie eine Regel

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

Benennen Sie die Regel

Geben Sie unter **Rule name** etwas ein, das Sie später wiedererkennen, z. B. `Daily heartbeat` oder `Monthly SIM balance`. Maximum 100 Zeichen.

Legen Sie den Zeitplan fest

Wählen Sie ein **Sending interval**. Die Felder unter dem Auswahlfeld ändern sich je nachdem, was Sie wählen:

Interval	Was Sie festlegen	Beispiel
Hourly	**At minute** (in 5-Minuten-Schritten)	`15` sendet um 00:15, 01:15, 02:15 und so weiter
Daily	**At time**	`07:30` sendet jeden Morgen um 07:30 Uhr
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 es nicht gibt:** Wenn Sie etwas für den 31. Tag jeden Monats planen, wird es nicht in Monaten mit weniger Tagen versendet. Verwenden Sie den 28. oder einen früheren Tag, wenn die Nachricht jeden Monat versendet werden muss.

Wählen Sie das Modem (nur bei Multi-Modem-Geräten)

Wenn Ihr Gerät mehr als ein Modem hat, wird ein Feld **Modem selection** angezeigt. Lassen Sie es auf der Standardeinstellung, um SMSEagle die Auswahl zu überlassen, oder wählen Sie ein bestimmtes Modem, wenn die Nachricht über eine bestimmte SIM-Karte versendet werden muss. Bei Geräten mit einem Modem wird dieses Feld nicht angezeigt.

Wählen Sie aus, was versendet werden soll

Verwenden Sie den Schalter **Message type** am Anfang 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**, wohin die Nachricht gesendet wird:
    - **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 von beiden ausfüllen, sonst kann die Regel nicht gespeichert werden.

Option B: USSD Code

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

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

Optionalen Telefonanruf hinzufügen

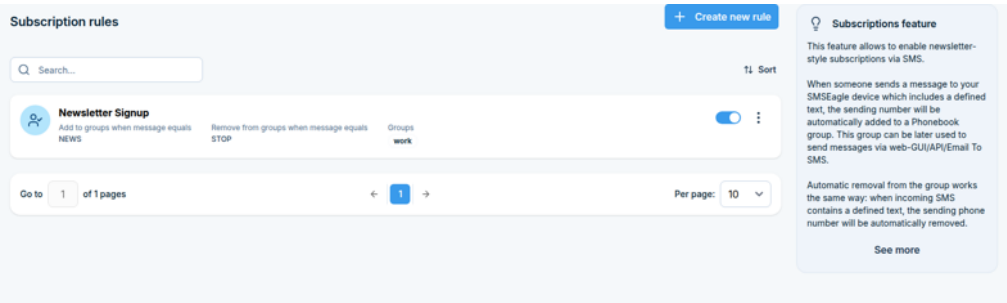
Call after sending SMS veranlasst das Gerät, auch einen Sprachanruf an dieselben Empfänger zu tätigen, was für Warnmeldungen nützlich ist, die nicht übersehen werden dürfen. Die verfügbaren Optionen hängen von Ihrem Gerätemodell ab:

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

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

Klicken Sie auf **Save**. Die Regel wird in der Liste angezeigt und startet zur nächsten geplanten Zeit.

Subscriptions



Subscription rules

Was diese Funktion macht

Mit Subscriptions können sich Personen **per SMS in eine Telefonbuchgruppe ein- und austragen**, ähnlich wie bei einem Newsletter-Opt-in.

Sie definieren zwei Stichwörter: eines, das den Absender zu einer Gruppe hinzufügt, und eines, das ihn entfernt. Wenn jemand Ihre SMSEagle-Nummer mit einem dieser Stichwörter anschreibt, wird seine Telefonnummer automatisch zur Gruppe hinzugefügt oder entfernt. Sie können dann Nachrichten an diese Gruppe von Compose, der API oder E-Mail-zu-SMS senden.

Typische Anwendungen: eine öffentliche Warnliste, in die sich Bewohner eintragen können, oder eine Schichtkontaktliste, der sich Mitarbeiter selbst beitreten können, ohne dass ein Administrator tätig wird.

Bevor Sie beginnen

Erstellen Sie die Gruppe, der Nutzer beitreten können:

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

Nur **öffentliche** Gruppen können in einer Subscription-Regel verwendet werden.

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

Schritt 1: Öffnen Sie die Subscriptions-Seite

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

Schritt 2: Erstellen Sie eine Regel

Klicken Sie oben rechts auf **Create new rule**. Ein Seitenpanel wird geöffnet. 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 zu **allen** aufgelisteten Gruppen hinzugefügt oder entfernt. Nur öffentliche Gruppen können ausgewählt werden.

Telefonnummer zu Gruppen hinzufügen, wenn eingehende Nachricht gleich 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 Das Schlüsselwort, das jemanden abmeldet, z. B. `STOP` oder `LEAVE`.

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

Klicken Sie auf **Save**.

Wie 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 (sofern **Groß-/Kleinschreibung beachten** nicht aktiviert ist)
Benutzer sendet `Please JOIN me`	Nichts passiert
Benutzer sendet `JOIN ALERTS`	Nichts passiert

Halten Sie deshalb Schlüsselwörter kurz und leicht zu tippen, und weisen Sie Ihre Benutzer an, nur das Schlüsselwort zu senden.

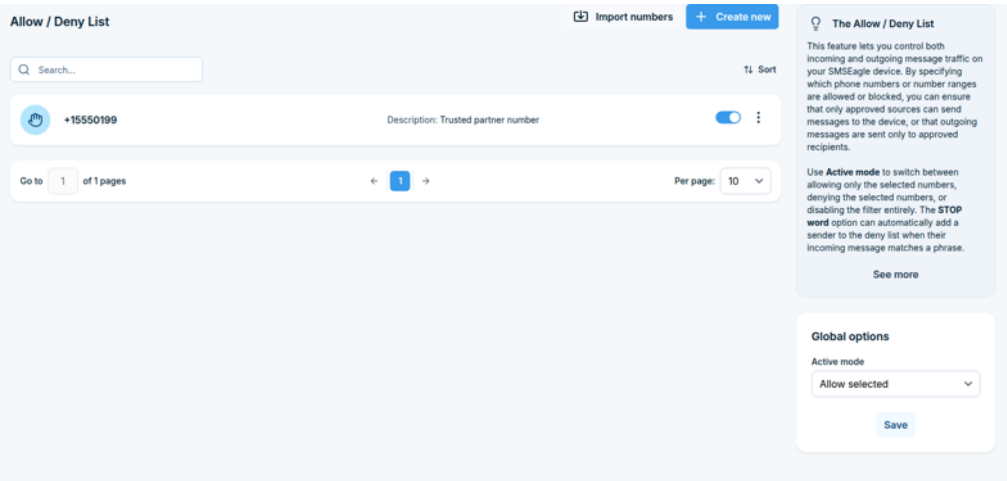
Was passiert, wenn sich jemand abonniert

- Wenn die Telefonnummer des Absenders **bereits im Adressbuch** vorhanden ist, wird dieser bestehende Kontakt zur Gruppe hinzugefügt.
- Wenn die Nummer **nicht im Adressbuch** 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 bleibt im Adressbuch.

Sie können jederzeit überprüfen, wer beigetreten ist: Gehen Sie zu **Adressbuch > Gruppen**, suchen Sie die Gruppe und öffnen Sie **Kontakte verwalten**.

Allow / Deny List



Allow / Deny List globale Optionen

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 sie behandelt:

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

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

Es gibt auch eine **STOP word**-Option, die einen Absender automatisch zur Liste hinzufügt, wenn seine Nachricht einem von Ihnen definierten Ausdruck entspricht. Dies ist der Grund, warum ein Opt-out-Schlüsselwort wie `STOP` funktioniert.

Bevor Sie beginnen

Entscheiden Sie, welche Arbeitsrichtung Sie verwenden möchten. **Allow selected** und **Deny selected** verwenden zwei separate Listen, daher sind die Regeln, die Sie in einem Modus hinzufügen, im anderen Modus nicht sichtbar. Wenn Sie den Modus wechseln, wird die gesamte Liste gewechselt, nicht invertiert.

Schritt 1: Öffnen Sie die Seite Allow / Deny List

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

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

Schritt 2: Wählen Sie den aktiven Modus

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

> Während der Modus **Disabled** ist, zeigt die Seite eine Meldung „Filtering is disabled“ anstelle der Liste an, und Regeln können nicht hinzugefügt oder bearbeitet werden. Wechseln Sie zu **Allow selected** oder **Deny selected**, um sie erneut zu verwalten.

Schritt 3: Fügen Sie eine Nummer hinzu

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

Phone number Die Nummer, auf die diese Regel angewendet wird. Maximal 15 Zeichen. Nur Ziffern, + und * sind zulässig, 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	Entspricht
`NUMBER`	Genau diese Nummer
`*NUMBER`	Jede Nummer, die damit endet
`NUMBER*`	Jede Nummer, die damit anfängt
`*NUMBER*`	Jede Nummer, die sie enthält

Zum Beispiel deckt `48512*` jede Nummer ab, die mit `48512` anfängt, und `*12345678` entspricht demselben Teilnehmer unabhängig davon, welches Ländervorwahl-Format ankommt.

Description Eine kurze Notiz, die erklärt, warum die Nummer auf der Liste steht, zum Beispiel `Spam` oder `Alarm panel, HQ`. Erforderlich, maximal 255 Zeichen.

Klicken Sie auf **Save**.

Schritt 4: Importieren Sie eine Liste aus CSV

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

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

Die Nummern werden zur aktuell aktiven Liste hinzugefügt.

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

Das STOP-Wort fügt Absender automatisch zur Liste hinzu, sodass Personen durch Eingabe eines Schlüsselworts abmelden können.

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

Option	Was es bedeutet
Never	Das STOP-Wort ist deaktiviert. Nummern werden nur manuell oder durch Import hinzugefügt.
Incoming message equals to…	Die vollständige Nachricht muss genau der eingegebenen Phrase entsprechen.
Incoming message contains to…	Die Phrase kann überall in der Nachricht erscheinen.

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

- Die Phrase selbst, maximal 160 Zeichen, zum Beispiel `STOP`.
- **Autoreply message**, 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.

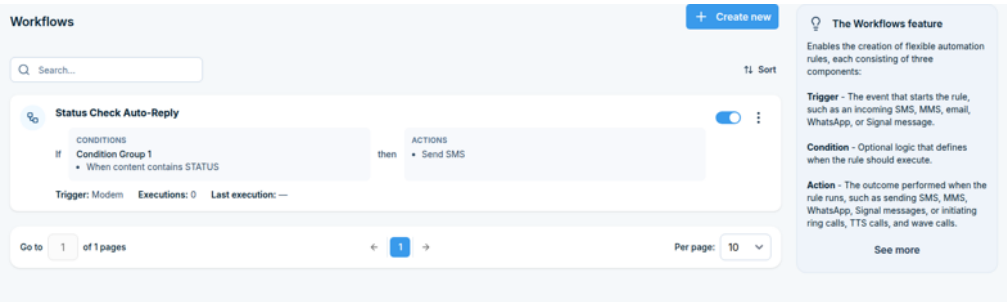
Klicken Sie auf **Save**. Die Zusammenfassung im Feld **Global options** zeigt nun die aktive Bedingung und den Antwortext an.

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

Wie die Filterung funktioniert

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

Workflows



Workflows – Übersicht

Workflows ermöglichen Ihnen, flexible Automatisierungsregeln zu 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).
- **Condition** – optionale Logik, die entscheidet, ob die Regel für ein bestimmtes Ereignis ausgeführt werden soll.
- **Action** – was geschieht, wenn die Regel ausgeführt wird: Senden einer SMS-, MMS-, WhatsApp- oder Signal-Nachricht, oder Initiieren eines Anrufs, TTS-Anrufs oder Wave-Anrufs.

Wo finde ich diese Funktion

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

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

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

Schritt 2: Bedingungsgruppen hinzufügen (optional)

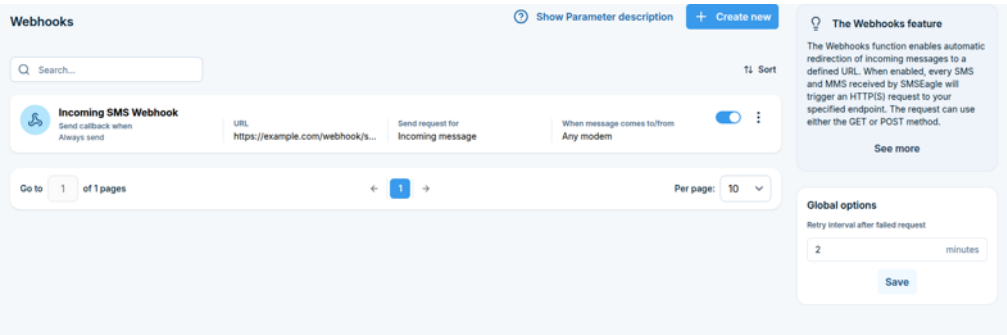
Unter **Bedingungsgruppen** klicken Sie auf **Gruppe hinzufügen**, um eine oder mehrere Bedingungen hinzuzufügen, die das eingehende Ereignis erfüllen muss, bevor der Workflow ausgeführt wird. Lassen Sie diesen Bereich leer, wenn der Workflow für jedes Ereignis ausgeführt werden soll, das den Trigger erfüllt.

Schritt 3: Aktionen hinzufügen

Unter **Aktionen** klicken Sie auf **Aktion hinzufügen**, um zu definieren, was der Workflow bei der Ausführung tut – beispielsweise eine Antwort senden, die Nachricht an einen anderen Kanal weiterleiten oder einen Anruf tätigen.

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

Webhooks



Webhooks-Übersicht

Was diese Funktion macht

Ein Webhook veranlasst SMSEagle, **Ihr** System aufzurufen. 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 URL Ihrer Wahl und überträgt die Details als Parameter.

Dies ist die Methode, um SMS-Verkehr in ein Ticketing-System, ein CRM, einen Chatbot oder Ihre eigene Anwendung zu übertragen, ohne die API abzufragen.

Zwei Integrationen erhalten dedizierte Unterstützung:

Methode	Wofür sie gedacht ist
POST (3CX)	Senden von Nachrichten in ein 3CX-Telefonsystem.
POST (Zabbix)	Bestätigung von Zabbix-Ereignissen per SMS, damit ein Techniker mit `ACK 12345` antworten kann, um eine Warnung 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 aktiviert wird und auf Multi-Modem-Geräten, auf welches Modem sie begrenzt ist. Jede Regel hat einen Schalter zum **Aktivieren oder Deaktivieren**, eine **Bearbeiten**-Aktion und eine **Löschen**-Aktion.

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

Schritt 2: Erstellen Sie eine Regel

Klicken Sie auf **Neue erstellen** in der oberen rechten Ecke. Das Webhook-Formular wird als Vollseite mit drei Abschnitten geöffnet.

Schritt 3: Basiskonfiguration

Feld	Was Sie eingeben müssen
Regelname	Ein beschreibender Name mit 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**.
An (3CX)	Nur für **POST (3CX)**: das Ziel in Ihrem 3CX-System.

Klicken Sie neben der URL auf **Test connection**, um sofort eine Beispielanfrage zu senden. Das Ergebnis wird unter dem Feld angezeigt und zeigt den zurückgekommenen HTTP-Status, damit Sie vor dem Speichern bestätigen können, dass der Endpunkt funktioniert.

Für **GET** und **POST** wird unter den Feldern ein Beispiel der Anforderungszeichenfolge 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 es trägt
`sender`	Absendernummer.
`timestamp`	Wann SMSEagle die Nachricht empfangen oder gesendet hat, als `YYYYmmddHHiiss`, zum Beispiel `20140531092257`.
`msgid`	Die SMSEagle-Nachrichten-ID.
`modemno`	Das Modem, auf dem die eingehende Nachricht empfangen wurde, oder das Modem, von dem die Nachricht gesendet wurde.
`apikey`	Der API-Schlüssel Ihres Service, falls Sie einen in den **Security settings** festgelegt haben. Optional.

Nur für SMS und MMS gesendet

Parameter	Was es trägt
`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 übereinstimmenden Telefonnummer zugewiesen ist. Optional.
`attachments`	MMS-Anhänge, zum Beispiel `[0 => [name => image.png, content-type => image/png, content => wfFWgwOlgBRwdWvsvs=]]`. **Nur POST**, da eine GET-Abfragezeichenfolge keine Dateidaten transportieren kann. Optional.

Wird nur für eingehende Sprachanrufe gesendet

Parameter	Was es trägt
`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 einem **Incoming call**-Auslöser sendet beispielsweise niemals `text` oder `attachments`.

SMSEagle erwartet, 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 Beispiel-GET-Anfrage:

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

Parameternamen anpassen

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

Das Umbenennen ändert nur den **Namen** des Parameters in der Anfrage, nie seinen Wert oder den Zeitpunkt seiner Übermittlung.

Schritt 4: Auslösebedingungen

Send request for bestimmt, welches Ereignis den Webhook auslöst:

Option	Wird ausgelöst, wenn
Incoming message	Eine SMS oder MMS kommt an.
Sent message	Eine ausgehende Nachricht wurde 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 es bedeutet
Always	Jedes Ereignis des gewählten Typs löst den Webhook aus.
Für angegebene Absender / wenn Text enthält	Nur Ereignisse, die die nachfolgenden Bedingungen erfüllen, lösen dies aus.

Wenn Sie die zweite Option gewählt haben, sind zwei Bedingungen verfügbar. Sie können eine oder beide verwenden, und ein Ereignis muss alle aktivierten Bedingungen 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 die Phrase ein. Aktivieren Sie **Case sensitive**, wenn Groß- und Kleinschreibung unterschiedlich behandelt werden sollen. Diese Bedingung ist nicht für den Auslöser **Incoming call** verfügbar, da ein Anruf keinen Text hat.

Bei Multi-Modem-Geräten schränkt **When message comes to/from** die Regel auf ein einzelnes Modem ein. Lassen Sie es andernfalls auf **Any modem**.

Schritt 5: Sicherheitseinstellungen

Feld	Funktionsweise
API-Schlüssel Ihres Service	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 Erfolg zählen. Ein oder mehrere dreistellige Codes, durch Kommas getrennt, z. B. `200,201,202`. Standard ist `200`, Maximum 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, erscheinen zusätzliche Felder:

- **Zabbix action** - **Acknowledge (ACK)**, **Unacknowledge (NOACK)** oder beide. Das Panel 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. Mit einem Token geben Sie ihn im API key-Feld ein; mit Login geben Sie **Zabbix username** und **Zabbix password** ein.
- **Test values** - eine **Event ID** und **Message**, die nur von **Test connection** verwendet werden, nie gespeichert.

Klicken Sie auf **Save webhook**.

Schritt 6: Wiederholungsintervall festlegen

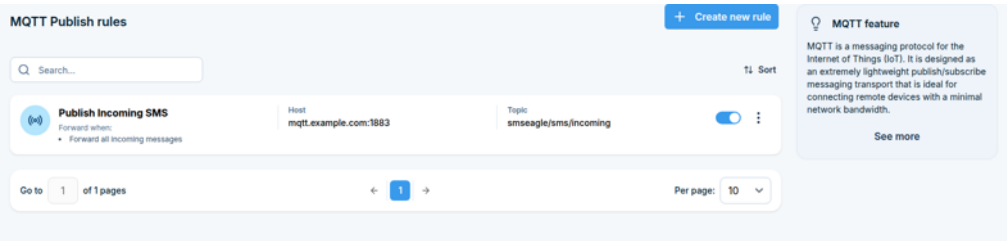
Das Feld **Global options** auf der Regelseite enthält **Retry interval after failed request** in Minuten. Wenn eine Anfrage fehlschlägt, wartet das Gerät diese Zeit, bevor es erneut versucht.

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 spielen keine vergangenen Nachrichten ab.
- Die Textbedingung ist eine **Enthält**-Übereinstimmung, keine exakte Übereinstimmung.
- Wenn mehrere Regeln dasselbe Ereignis erfüllen, sendet **jede** davon ihre eigene Anfrage, sodass eine Nachricht mehrere Endpunkte erreichen kann.
- Eine Anfrage zählt nur dann als erfolgreich, wenn der Antwortstatus einer der **Erwarteten HTTP-Statuscodes** ist. Alles andere, einschließlich gar keiner Antwort, ist ein Fehler und wird wiederholt.
- **Test connection** sendet eine Beispiel-Nutzlast, keine echte Nachricht, daher ist es sicher, gegen einen Produktions-Endpunkt 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**, die jeweils mit einem **Topic** wie `building/boiler/temperature` gekennzeichnet sind. Jeder, der mit dem Broker verbunden ist, kann die Topics abhören, die ihn interessieren.

SMSEagle sitzt auf beiden Seiten dieser Konversation:

Regeltyp	Richtung	Funktionsweise
Subscribe	MQTT in SMS	Überwacht einen Broker und wandelt eingehende MQTT-Nachrichten in SMS-Nachrichten um, die an Ihre Mitarbeiter gesendet werden.
Publish	SMS in MQTT	Nimmt eingehende SMS-Nachrichten und veröffentlicht sie auf einem Broker, damit Ihr IoT-System darauf reagieren kann.

Typische Anwendungen: Umwandlung eines Sensoralarms in eine SMS an das Wartungsteam (Subscribe) oder Ermöglichung, dass ein Techniker einen Befehl textet, der vom Automatisierungssystem aufgegriffen wird (Publish).

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

Bevor Sie beginnen

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

Für **Subscribe**-Regeln benötigen Sie auch die Liste der zu überwachenden Topics (ebenfalls in den Einstellungen festgelegt). Für **Publish**-Regeln benötigen Sie das Topic zum Veröffentlichen (pro Regel unten festgelegt).

Teil 1: Subscribe (MQTT in SMS)

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

Schritt 1: Öffnen Sie die Subscribe-Regelseite

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

Schritt 2: Erstellen Sie eine Subscribe-Regel

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

Benennen Sie die Regel

Geben Sie in **Rule name** etwas Aussagekräftiges ein, zum Beispiel `Boiler alarm to maintenance`. Maximal 100 Zeichen.

Entscheiden Sie, auf welche MQTT-Nachrichten reagiert werden soll

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

Option	Was es bedeutet
Any message	Jede MQTT-Nachricht, die das Gerät empfängt, löst diese Regel aus.
Angegebenes Thema / Nachricht	Nur Nachrichten, die Ihre nachfolgenden Bedingungen erfüllen, lösen die Regel aus.

Wenn Sie **Angegebenes Thema / Nachricht** wählen, stehen zwei Bedingungen zur Verfügung. 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 **Topic** ein, z. B. `building/boiler`.

Wenn eingehende Nachricht enthält Aktivieren Sie dies und geben Sie die Phrase in **Message phrase** ein, z. B. `ALARM`. Aktivieren Sie **Case sensitive**, wenn `alarm` und `ALARM` unterschiedlich behandelt werden sollen.

Wählen Sie die Empfänger

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

Schreiben Sie den SMS-Text

Message format steuert, was die SMS aussagt. 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

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

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

Erweiterte Optionen

Klicken Sie auf **Advanced options**, um diesen Bereich zu erweitern. Sie benötigen dies nicht für eine grundlegende Einrichtung.

- **Modem** (nur Multi-Modem-Geräte) – senden Sie die SMS über eine bestimmte SIM-Karte statt über die Standardkarte.
- **Call after sending SMS** – führen Sie auch einen Sprachanruf an die gleichen Empfänger durch. Optionen sind **No**, **Ring only**, **Yes - text to speech** und **Yes - text to speech**

(advanced), je nach den Funktionen Ihres Gerätemodells. Mit der erweiterten Option wählen Sie auch ein **Voice model**.

Klicken Sie auf **Save**. Die Regel beginnt ab sofort auf eingehende MQTT-Nachrichten zu reagieren.

So funktioniert die Subscribe-Zuordnung

- Die **Topic**-Bedingung ist eine **contains**-Zuordnung und ignoriert Groß- und Kleinschreibung. Eine Regel mit Topic `boiler` erfasst auch `building/boiler/temperature`.
- Das Kontrollkästchen **Case sensitive** gilt nur für die Nachrichtenphrase, nie für das Thema.
- Wenn mehrere Subscribe-Regeln die gleiche MQTT-Nachricht erfassen, sendet **jede** ihre eigene SMS.

Teil 2: Publish (SMS in MQTT)

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

Schritt 1: Öffnen Sie die Seite „Publish rules“

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

Schritt 2: Erstellen Sie eine Publish-Regel

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

Benennen Sie die Regel

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

Entscheiden Sie, welche SMS-Nachrichten veröffentlicht werden

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

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

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

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

When incoming SMS text contains Aktivieren Sie dies und geben Sie den Ausdruck unter **Text fragment** ein. Aktivieren Sie **Case sensitive**, wenn Groß- und Kleinbuchstaben als unterschiedlich behandelt werden sollen.

When messages comes to (nur Multi-Modem-Geräte) Lassen Sie es auf **Any modem**, oder wählen Sie ein bestimmtes Modem, damit nur auf dieser SIM-Karte ankommende Nachrichten veröffentlicht werden.

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

Geben Sie die Broker-Verbindung ein

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

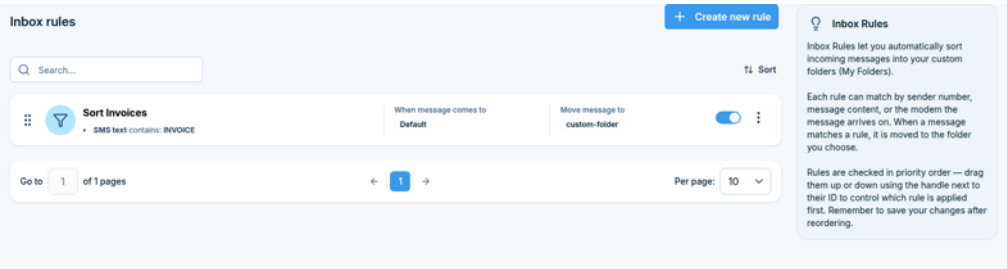
Feld	Was Sie eingeben müssen
Host	Die Broker-Adresse, zum Beispiel `test.host.io`
Port	Der Broker-Port, zum Beispiel 1883. Der zulässige Bereich liegt zwischen 1 und 65535.
Username	Der Broker-Benutzer, falls erforderlich. Lassen Sie es leer für einen offenen Broker.
Password	Das Broker-Passwort, falls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

Klicken Sie auf **Save**. Eingehende SMS-Nachrichten, die der Regel entsprechen, werden von nun an veröffentlicht.

Funktionsweise von Publish-Abgleich

- Die Textbedingung ist eine **Enthält**-Übereinstimmung, keine exakte Übereinstimmung.
- Wenn mehrere Publish-Regeln dieselbe SMS abgleichen, veröffentlicht **jede** von ihnen, sodass die Nachricht auf mehr als einem Broker oder Topic landen kann.
- Regeln gelten nur für Nachrichten, die eintreffen, nachdem die Regel erstellt und aktiviert wurde. Sie verarbeiten keine Nachrichten, die sich bereits im Posteingang befinden.

Inbox Rules



Übersicht über Inbox Rules

Inbox Rules sortieren eingehende Nachrichten automatisch in Ihre benutzerdefinierten Ordner (My Folders), anstatt alles im Hauptpostfach zu belassen.

Wo finde ich diese Funktion

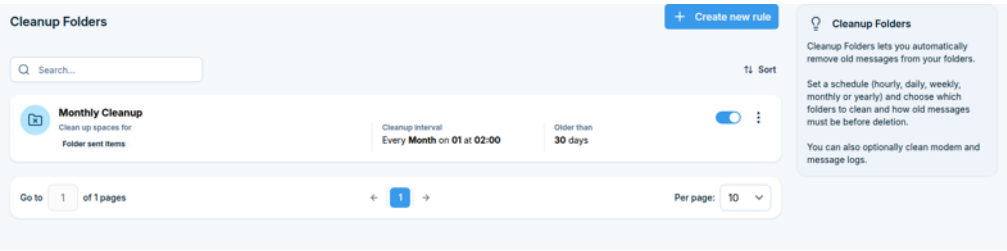
Automation > Folders > Inbox Rules (`/automation/inbox-rules/`).

Konfigurieren einer Posteingangsregel

Klicken Sie auf **Create new rule**. Jede Regel kann nach Absendernummer, Nachrichteninhalt oder dem Modem, auf dem die Nachricht empfangen wurde, gefiltert werden. Eine Nachricht, die der Regel entspricht, wird in den von Ihnen gewählten Ordner verschoben.

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

Cleanup Folders



Cleanup Folders-Übersicht

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

Wo finde ich diese Funktion

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

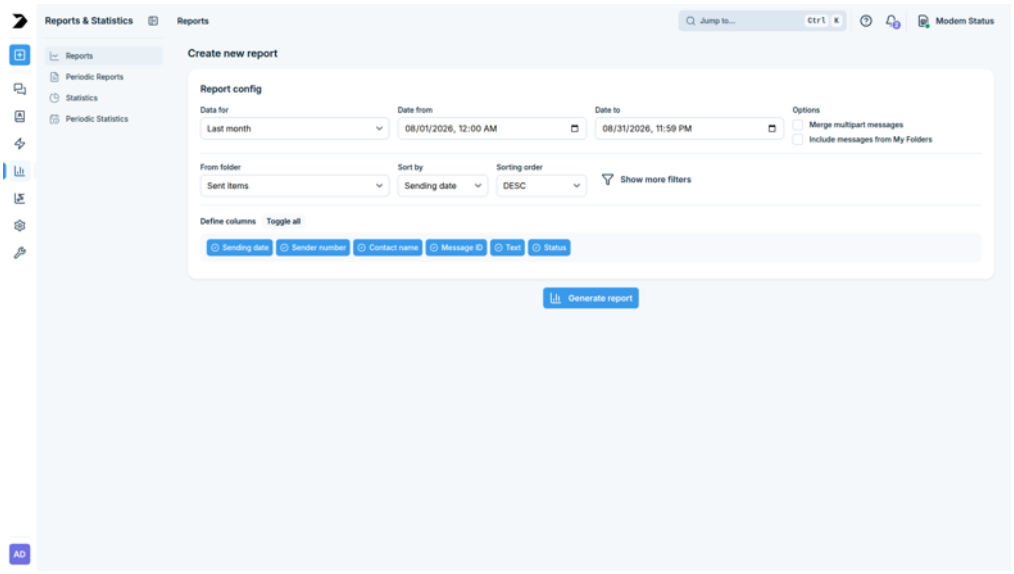
Konfigurieren einer Bereinigungsregel

Klicken Sie auf **Create new rule**, legen Sie einen Zeitplan fest (stündlich, täglich, wöchentlich, monatlich oder jährlich), wählen Sie die zu bereinigenden Ordner und das Alter aus, das eine Nachricht haben muss, bevor sie gelöscht wird. Sie können auch optional Modem- und Nachrichtenprotokolle nach dem gleichen Zeitplan bereinigen.

Berichte & Statistiken

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

Berichte



Neuen Bericht erstellen

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

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

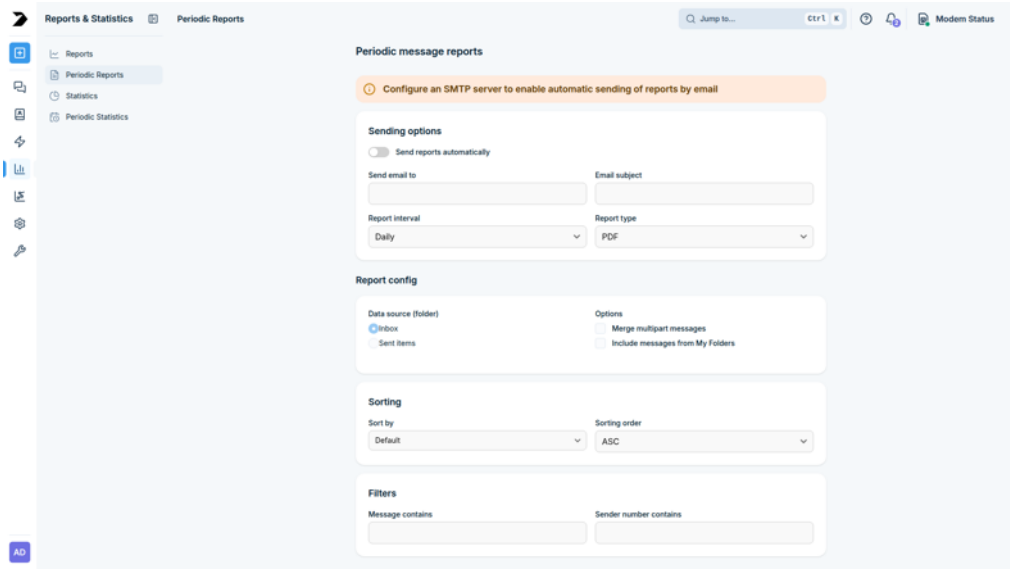
Unter **Options**:

Option	Funktion
Merge multipart messages	Kombiniert eine lange SMS, die in mehrere Teile aufgeteilt wurde, wieder in einer Zeile.
Include messages from My Folders	Bezieht auch Nachrichten ein, die in einen benutzerdefinierten Ordner verschoben wurden.
From folder	Ordner für den Bericht: **Sent items**, **Inbox** oder **Outbox**.
Sort by / **Sorting order**	Spalte, nach der sortiert werden soll (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 auszuwählen, welche Spalten im generierten Bericht angezeigt werden – **Toggle all** aktiviert oder deaktiviert 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 Erstellung und den automatischen Versand eines Berichts auf wiederkehrender Basis, anstatt jedes Mal manuell einen Bericht zu erstellen.

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

Aktivieren Sie unter **Sending options** die Option **Send reports automatically** und füllen Sie aus:

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

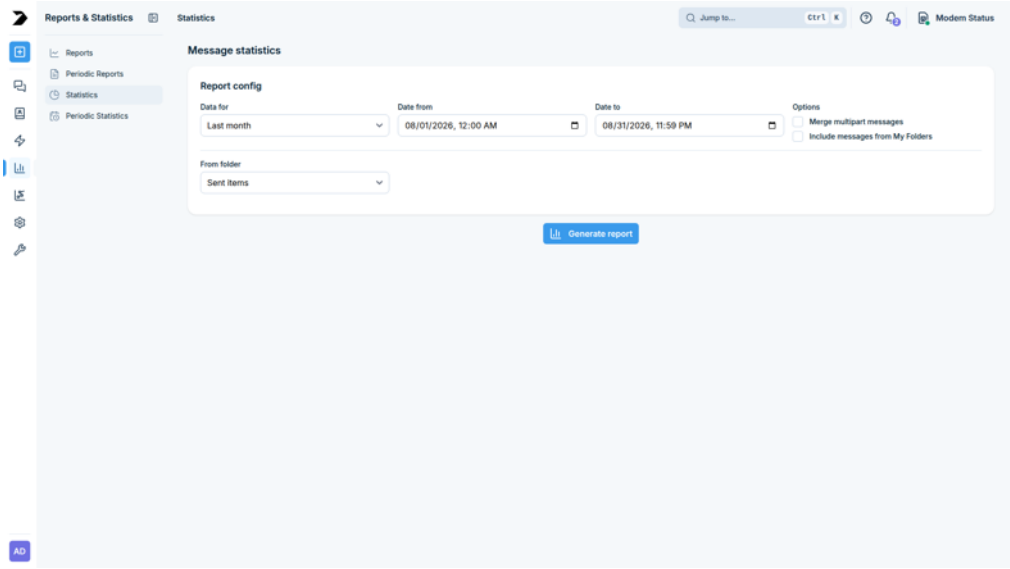
Wählen Sie unter **Report config** die **Data source (folder)** (**Inbox** oder **Sent items**), die gleichen **Merge multipart messages** / **Include messages from My Folders** Optionen wie für einen einmaligen Bericht und **Sorting** (Sortierfeld und ASC/DESC Reihenfolge).

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**.

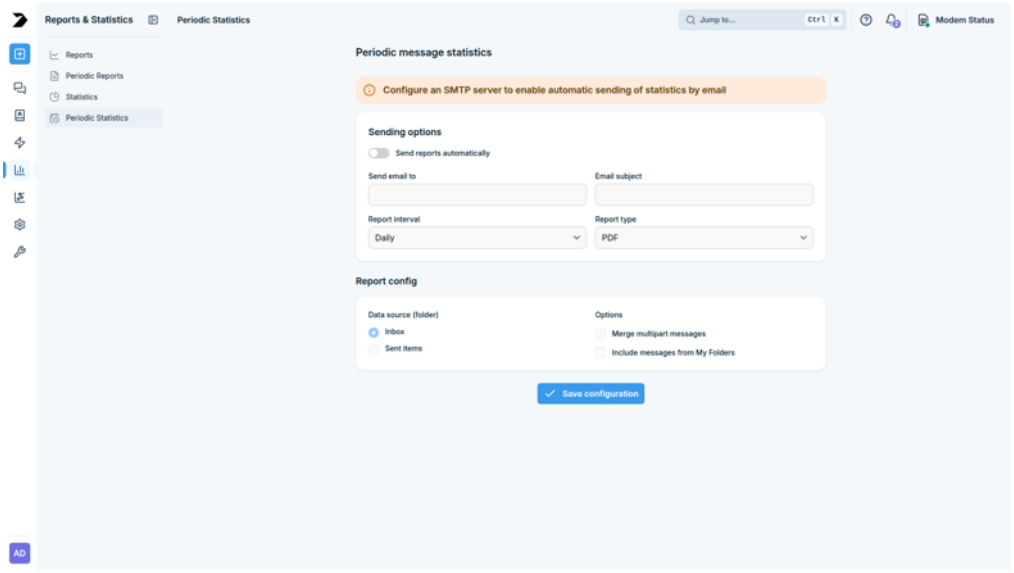
Statistiken



Nachrichtenstatistik

Reports & Statistics > Statistics (`/reports/statistics`) funktioniert genauso wie Reports oben - mit den gleichen **Data for** Zeitbereichs-Wahlen und **Merge multipart messages** / **Include messages from My Folders** / **From folder** Optionen - erzeugt aber zusammengefasste Verkehrsstatistiken statt eines zeilenweisen Exports. Klicken Sie auf **Generate report**, um den Bericht zu erstellen.

Periodische Statistiken



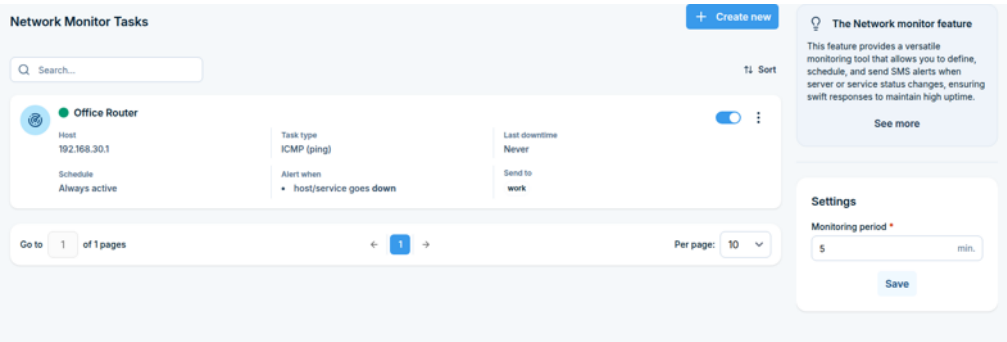
Periodische Nachrichtenstatistik

Reports & Statistics > Periodic Statistics (`/reports/periodic-statistics`) plant die obige Statistik ein, um automatisch generiert und per E-Mail versendet zu werden, genauso wie Periodic Reports für den zeilenweisen Export: Es ist eine funktionierende SMTP Configuration erforderlich und bietet die gleichen **Sending options** (Empfänger, Betreff, **Daily / Weekly / Monthly** Intervall, **PDF / CSV** Berichtstyp) plus einen **Report config** Bereich (Datenquellen-Ordner, Multipart-Nachrichten zusammenführen, My Folders einbeziehen). Klicken Sie auf **Save configuration**.

Überwachung

Dieses Kapitel behandelt den Abschnitt **Monitoring** der Weboberfläche: Überprüfung externer Hosts und Services sowie das Auslesen digitaler Ein-/Ausgänge.

Network Monitor



Network Monitor-Übersicht

Was diese Funktion bewirkt

Network Monitor verwandelt Ihren SMSEagle in eine kleine Überwachungsstation. Es überprüft Server, Geräte und Dienste nach einem Zeitplan und sendet eine SMS, wenn etwas nicht mehr antwortet, wieder verfügbar ist oder einen Wert außerhalb des erwarteten Bereichs meldet.

Es hat drei Teile:

Seite	Was es bewirkt
Tasks	Die Überwachungsregeln: was zu überprüfen ist, wie häufig und wer benachrichtigt wird.
Reports	Ein Verlauf von Ausfallzeiten, gefiltert nach Datumsbereich und Task, exportierbar in CSV.
SNMP Traps	Regeln, die SNMP-Traps, die an das Gerät gesendet werden, in SMS-Nachrichten umwandeln.

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

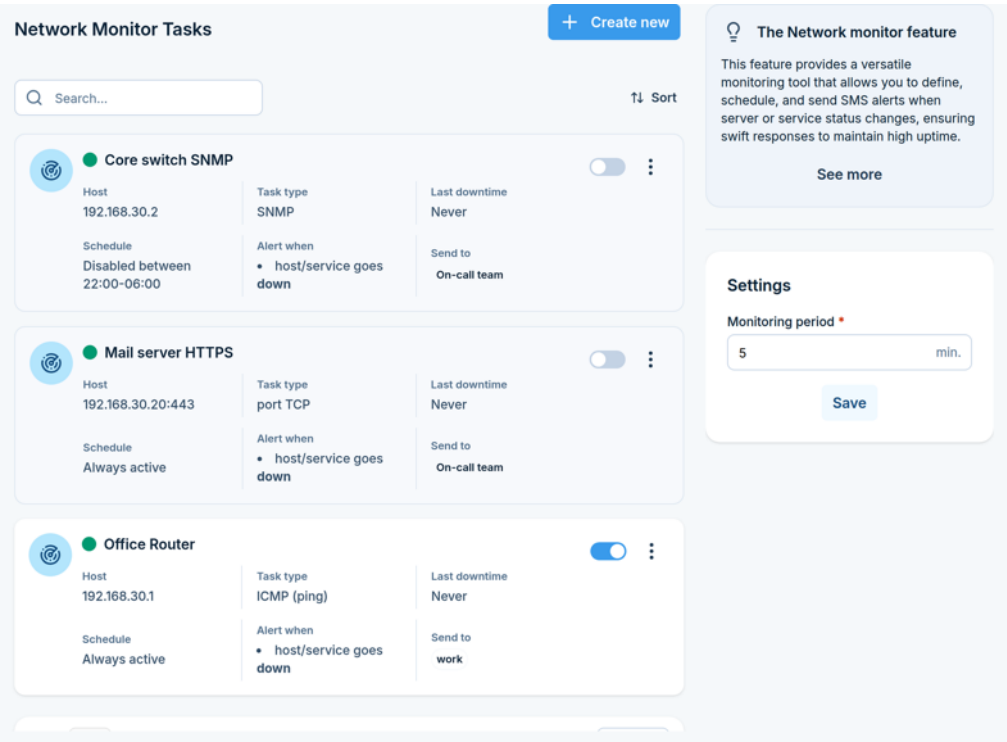
Vor Ihrem Start

- Das Gerät muss die Hosts, die Sie überwachen möchten, erreichen können. Überprüfen Sie zunächst die Netzwerkeinstellungen unter **Settings > Network**.
- Empfänger müssen im Telefonbuch als **Public** gekennzeichnet sein, wenn Sie eine Gruppe benachrichtigen möchten. Andernfalls können Sie einfache Telefonnummern in die 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 Tasks-Seite

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



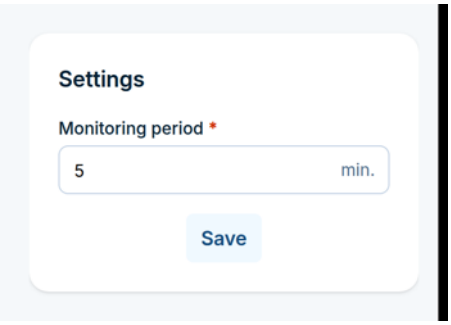
Network Monitor Tasks

Jede Task in der Liste zeigt ihren Host, Zeitplan, Task-Typ, worauf sie reagiert, wann der Host zuletzt nicht erreichbar war und wer benachrichtigt wird. Ein grünes oder rotes Zeichen 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 für **alle** Tasks gilt: **Monitoring period**, in Minuten. Dies ist die Häufigkeit, in der das Gerät die Überprüfungen durchführt.

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



Überwachungsperiode

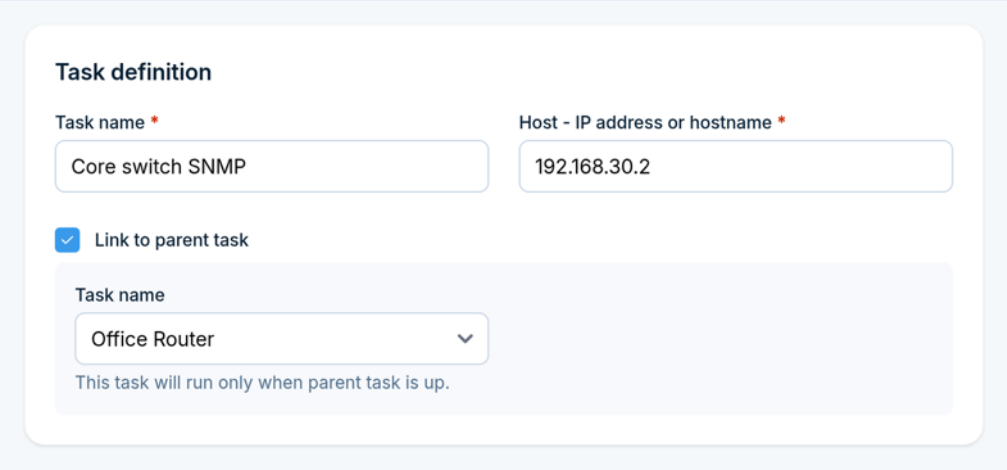
Schritt 3: Aufgabe erstellen

Klicken Sie auf **Neue erstellen** in der oberen rechten Ecke. Das Aufgabenformular wird als vollständige Seite geöffnet, unterteilt in fünf Abschnitte.

Aufgabendefinition

Feld	Was Sie eingeben sollten
Aufgabenname	Ein aussagekräftiger 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 zu übergeordneter Aufgabe	Aktivieren Sie dies, um die Aufgabe von einer anderen abhängig zu machen.
Aufgabenname (übergeordnet)	Wird angezeigt, nachdem das Kontrollkästchen aktiviert wurde: die Aufgabe, von der diese abhängt.

Eine verlinkte Aufgabe **wird nur ausgeführt, während ihre übergeordnete Aufgabe läuft**. Verwenden Sie dies, um Alarmfluten zu vermeiden: Wenn der Router vor zehn Servern ausfällt, warnt nur die Router-Aufgabe, und die zehn Server-Aufgaben bleiben stumm.



Aufgabendefinition

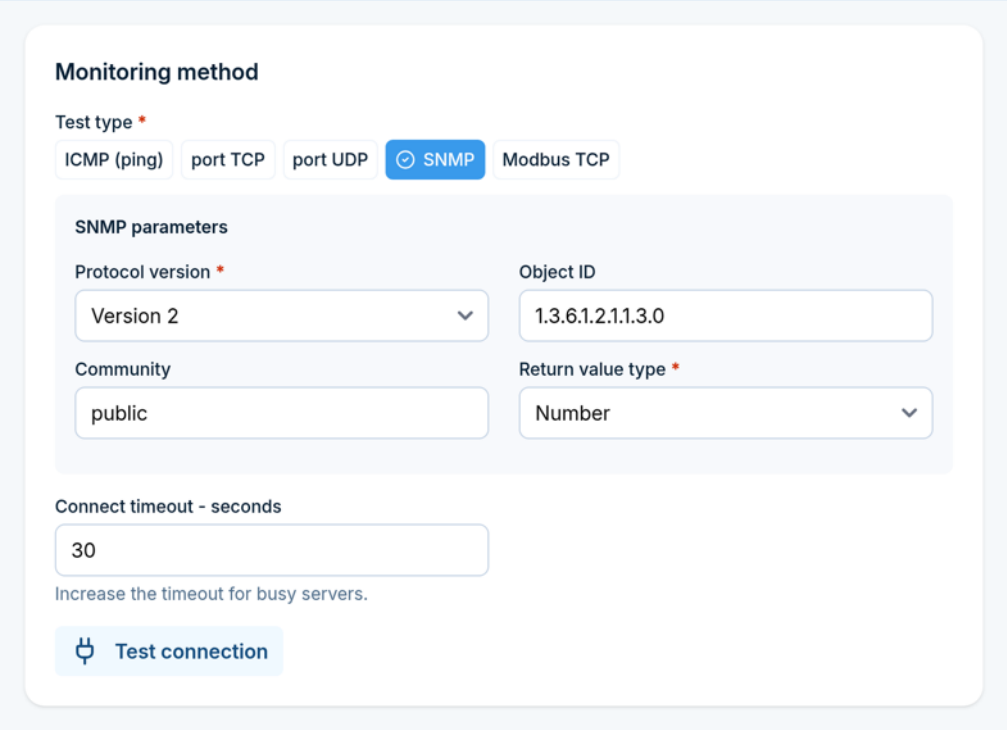
Überwachungsmethode

Wählen Sie den **Testtyp** und füllen Sie dann die Parameter aus, die dafür angezeigt werden:

Testtyp	Parameter
ICMP (Ping)	**Anzahl der Anfragen** – wie viele Pings pro Überprüfung gesendet werden.
Port TCP	**Port** – der TCP-Port, der eine Verbindung akzeptieren muss.
Port UDP	**Port** – der UDP-Port, der abgefragt werden soll.
SNMP	**Protokollversion** (1 oder 2), **Object ID**, **Community**, **Rückgabewerttyp** (Zahl oder String).
Modbus TCP	**Port**, **Unit ID**, **Register**, **Function code** (Spulen auslesen, Diskrete Eingänge auslesen, Holding Registers auslesen, Input Registers auslesen).

Connect timeout - Sekunden gilt für jeden Test-Typ. Erhöhen Sie den Wert für überarbeitete Server, die langsam antworten; der Standard beträgt 30 Sekunden.

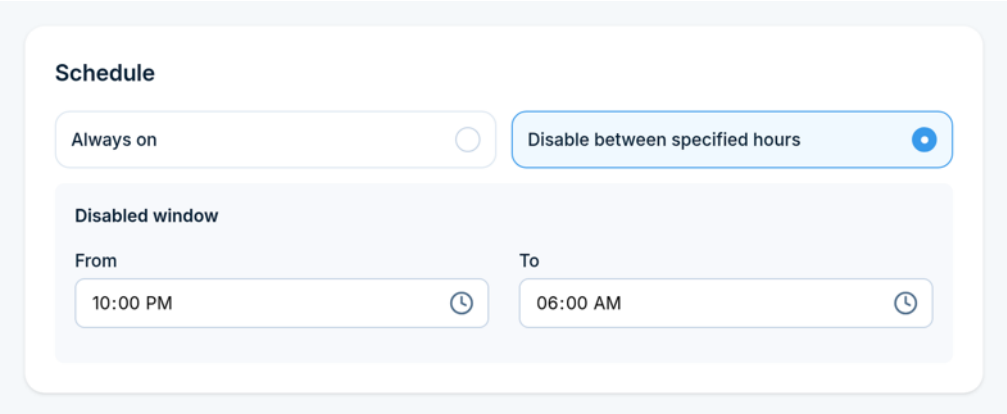
Klicken Sie auf **Test connection**, um die Überprüfung sofort durchzuführen. Das Ergebnis wird neben der Schaltfläche angezeigt, sodass Sie bestätigen können, dass der Host antwortet, bevor Sie die Aufgabe speichern.



Überwachungsmethode

Zeitplan

Wählen Sie **Always on**, wenn die Aufgabe rund um die Uhr ausgeführt werden soll, oder **Disable between specified hours** und stellen Sie **From** und **To** ein, um ein ruhiges Fenster zu schaffen, z. B. während einer nächtlichen Sicherung, die den Service immer offline nimmt.



Zeitplan

Warnungsauslöser

Wählen Sie zuerst, wer die Warnung erhalten soll:

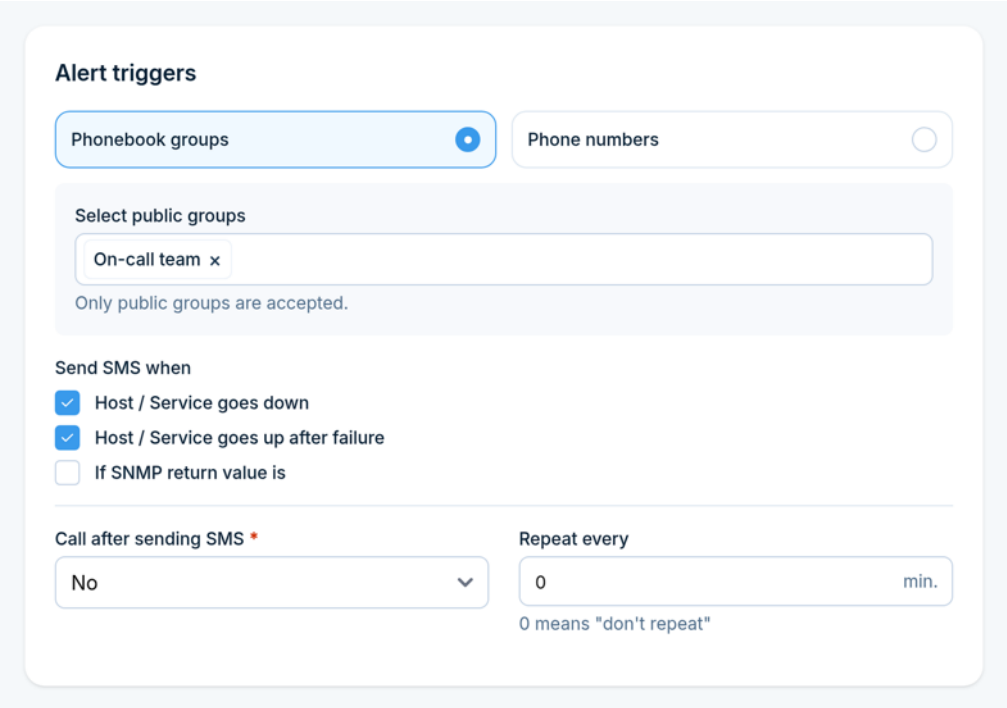
Option	Was Sie eingeben sollten
Phonebook groups	Wählen Sie öffentliche Gruppen. Nur öffentliche Gruppen werden akzeptiert.
Phone numbers	Geben Sie die Nummern direkt ein, durch Kommas getrennt. Maximal 100 Zeichen insgesamt.

Aktivieren Sie dann mindestens eine **Send SMS when**-Bedingung. Ohne eine kann die Aufgabe nicht gespeichert werden:

- **Host / Service goes down**
- **Host / Service goes up after failure**
- **If SNMP return value is** - nur für SNMP-Aufgaben. Wählen Sie einen **Operator** (Equal to, Not equal to, Greater than, Less than, Contains, Does not contain) und einen **Value**.
- **If Modbus return value is** - nur für Modbus-Aufgaben, mit denselben Operator- und Wertfeldern.

Zwei weitere Einstellungen schließen den Abschnitt:

- **Call after sending SMS** - auch einen Sprachanruf tätigen. Die Optionen sind **No**, **Ring only**, **Yes - text to speech** und **Yes - text to speech (advanced)**, je nach Ihrem Gerätemodell. Mit der erweiterten Option wählen Sie auch ein **Voice model**.
- **Repeat every** - die Warnung alle X Minuten erneut senden, solange das Problem andauert. `0` bedeutet, einmal senden und ruhig bleiben.



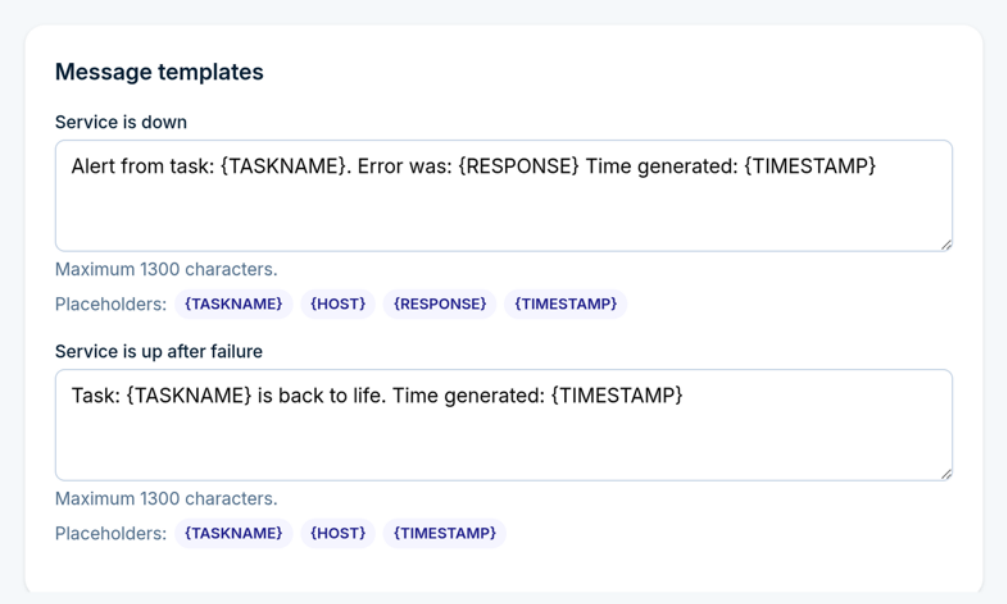
Warnungsauslöser

Nachrichtenvorlagen

Schreiben Sie den Text für jede Warnung, die Sie aktiviert haben. Jede Nachricht kann bis zu 1300 Zeichen lang sein und kann Platzhalter verwenden:

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

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



Nachrichtenvorlagen

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

Teil 2: Berichte

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

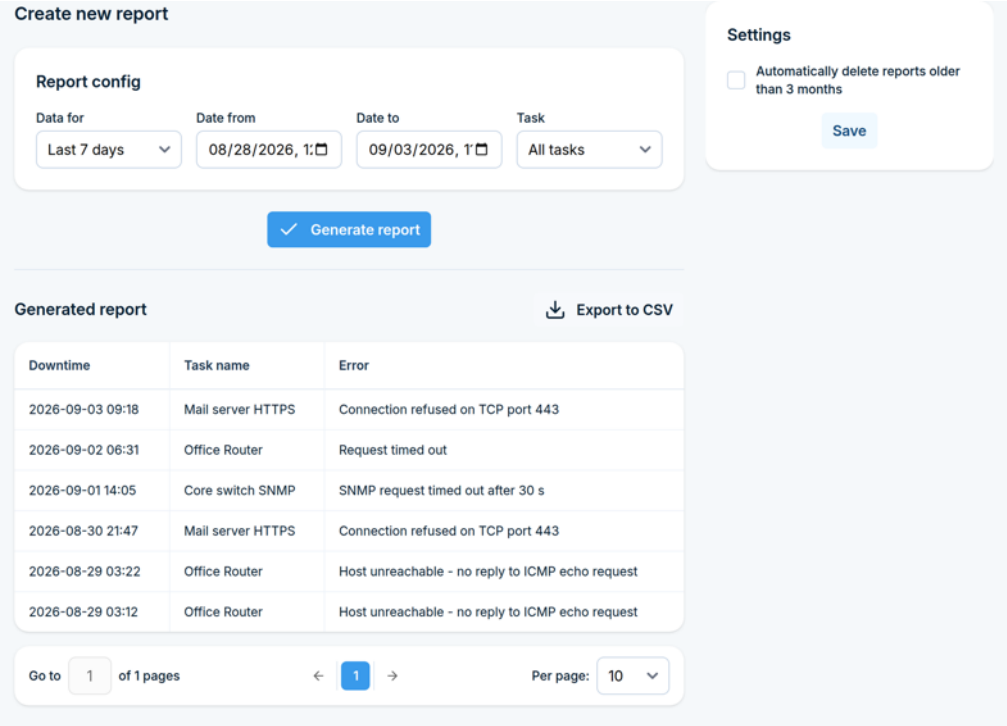
Bericht erstellen

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

Feld	Was es bewirkt
Data for	Ein vordefinierter Datumsbereich. Die Auswahl füllt die unten stehenden Daten aus.
Date from / **Date to**	Der genaue Bereich. Das Bearbeiten dieser Felder setzt **Data for** auf einen benutzerdefinierten Bereich.
Task	Eine einzelne Task oder **All tasks**.

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

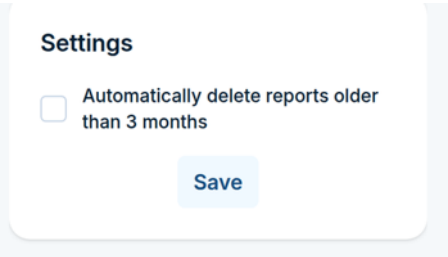
Klicken Sie über den Ergebnissen auf **Export to CSV**, um diese herunterzuladen.



Generierter Bericht

Berichtsverwaltung

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



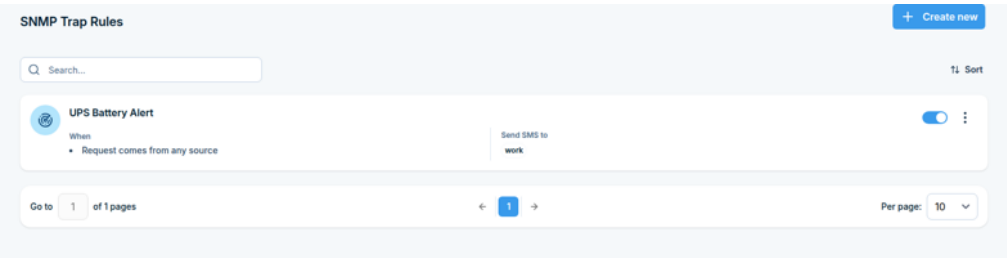
Berichtsverwaltung

Teil 3: SNMP Traps

Tasks überprüfen Dinge proaktiv. SNMP-Trap-Regeln funktionieren auf andere Weise: Ein anderes Gerät sendet einen Trap **an** das SMSEagle, und die Regel wandelt ihn in eine SMS um.

Schritt 1: SNMP Traps-Seite öffnen

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



SNMP Trap Rules

Schritt 2: Regel erstellen

Klicken Sie auf **Create new** in der oberen rechten Ecke. Ein Seitenpaneel öffnet sich.

Benennen Sie die Regel

Geben Sie in **Rule name** etwas Aussagekräftiges ein, zum Beispiel `UPS battery trap`. Maximum 100 Zeichen.

Entscheiden Sie, welche Traps bearbeitet werden sollen

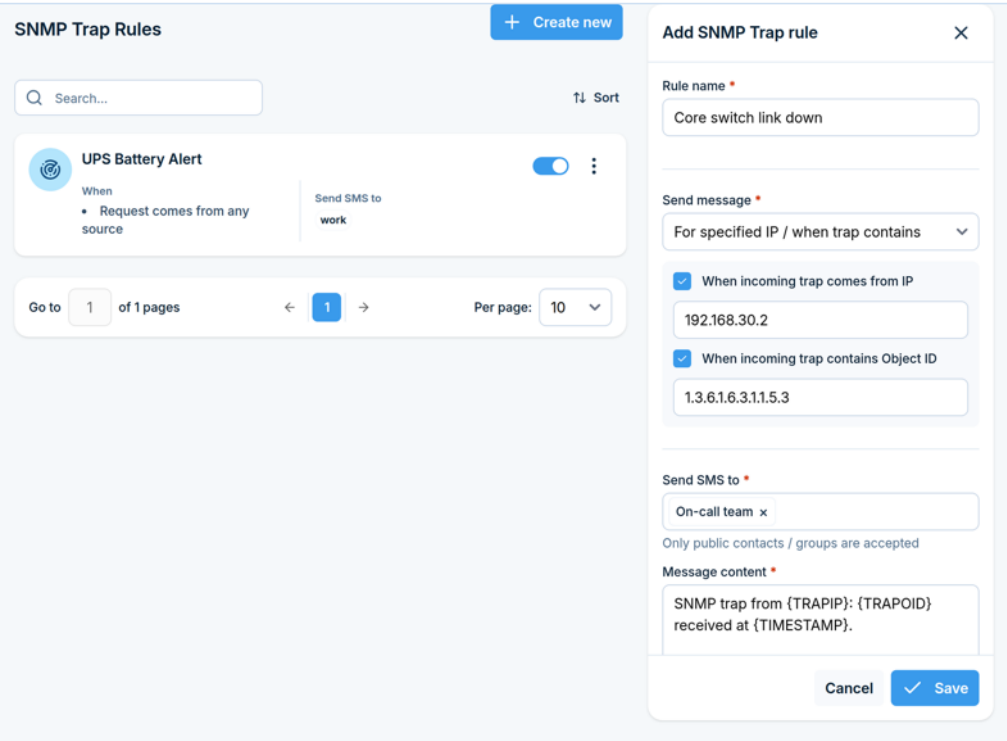
Wählen Sie **Send message**:

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

Wenn Sie die zweite Option gewählt haben, werden 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 die Kontakte oder Gruppen. Nur **public** Kontakte und Gruppen werden akzeptiert.

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

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

Optionale Einstellungen

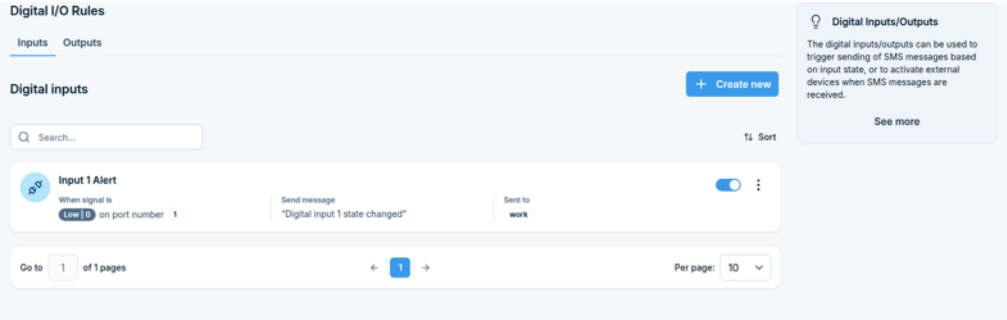
- **Modem** (nur Multi-Modem-Geräte) – Versand über eine bestimmte SIM-Karte statt über die Standardeinstellung.
- **Call after sending SMS** – auch einen Sprachanruf tätigen, mit den gleichen Optionen wie in Aufgaben.

Klicken Sie auf **Save**. Die Regel wird ab sofort auf empfangene Traps angewendet.

Verhalten des Netzwerk-Monitors

- Tasks werden im gemeinsamen **Monitoring period** überprüft, sodass eine Task nicht schneller als dieses Intervall erlaubt warnen kann.
- Eine „down"-Warnung wird einmal versendet, wenn sich der Zustand ändert, und wird dann nur wiederholt, wenn Sie **Repeat every** festlegen.
- Eine Task, die mit einem übergeordneten Element verknüpft ist, wird vollständig übersprungen, während das übergeordnete Element ausfällt, daher bleiben die eigenen Warnungen stumm, bis sich das übergeordnete Element wiederherstellt.
- Wenn mehrere SNMP-Trap-Regeln denselben Trap erfüllen, versendet **jede** von ihnen ihre eigene SMS.

Digitaler Ein- und Ausgang



Digitale Ein-/Ausgangsübersicht

Was diese Funktion bewirkt

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

Richtung	Was es bewirkt
Input	Eine Spannungsänderung an einem Eingangsport (ein schließender Türkontakt, ein auslösendes Alarm-Relais, eine USV-Fehlerberichte) veranlasst das Gerät, eine SMS zu versenden.
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 hochgeht, benachrichtige das Wartungsteam". Eine Output-Regel besagt „wenn eine SMS mit OPEN ankommt, setze Port 1 für 5 Sekunden auf High".

> **MHD-8100 has no built-in digital input or output ports.** To use this feature, connect the **Digital I/O Extender** accessory (product code ACCDPIOKIT) to the device. It is a USB

module with 32 ports, each configurable as an input or an output, with all signals on screw terminals. See Accessories for details and ordering.

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

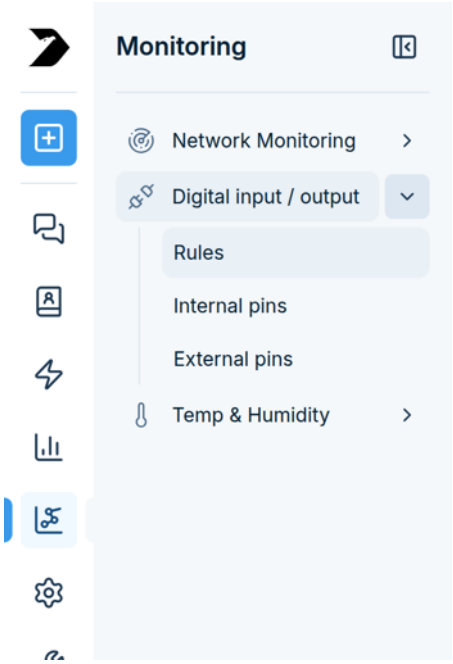
Vor Ihrem Start

- Connect the Digital I/O Extender to the device and wire your equipment to its terminals. Then define the ports you use on the **External pins** page (see Part 3 below). The port lists in the rule forms only offer ports defined there.
- Das Gerät muss SMS versenden können. Überprüfen Sie, dass mindestens ein Modem verbunden und im Netzwerk registriert ist.
- Empfänger von Input-Regeln müssen im Phonebook als **Public** markiert sein.

Wo man es findet

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

Seite	Wofür es ist
Rules	Erstellen Sie die Input- und Output-Regeln. Hier verbringen Sie die meiste Zeit.
External pins	Define and control the ports of the Digital I/O Extender.

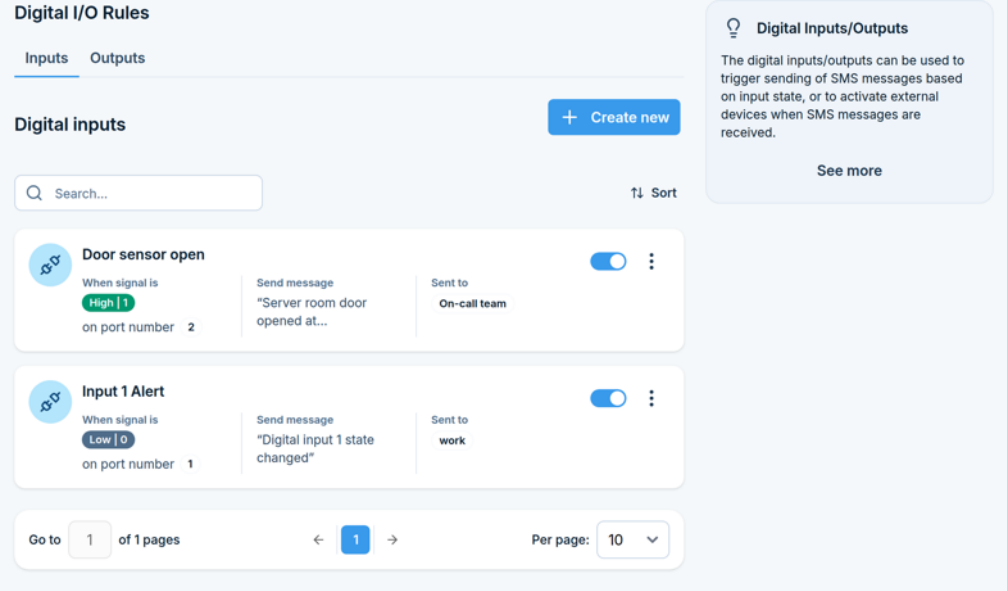


Wo sich die Digital I/O-Seiten befinden

Teil 1: Eingaberegeln (Eingangssignal in SMS)

Schritt 1: Öffnen Sie die Regelseite

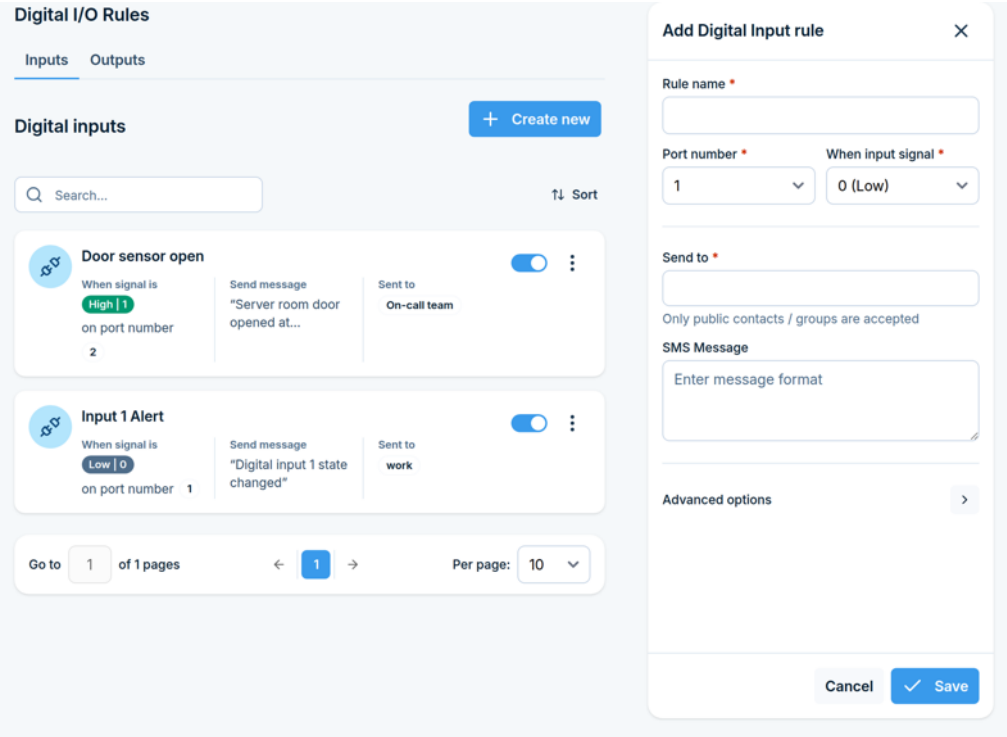
Gehen Sie zu **Monitoring > Digital input / output > Rules** und stellen Sie sicher, dass die Registerkarte **Inputs** ausgewählt ist.



Digitale Eingaberegeln

Schritt 2: Erstellen Sie eine Eingaberegel

Klicken Sie auf **Create new** in der oberen rechten Ecke. Ein Seitenpaneel öffnet sich.



Eine neue digitale Eingaberegel

Benennen Sie die Regel

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

Wählen Sie den Port und das Signal

Feld	Was Sie eingeben sollten
Port number	The input port the equipment is wired to. The list shows the Digital I/O Extender ports defined on the **External pins** page, marked `(Ext)`.
When input signal	`0 (Low)` oder `1 (High)`. Dies ist der Zustand, der die Regel auslöst.

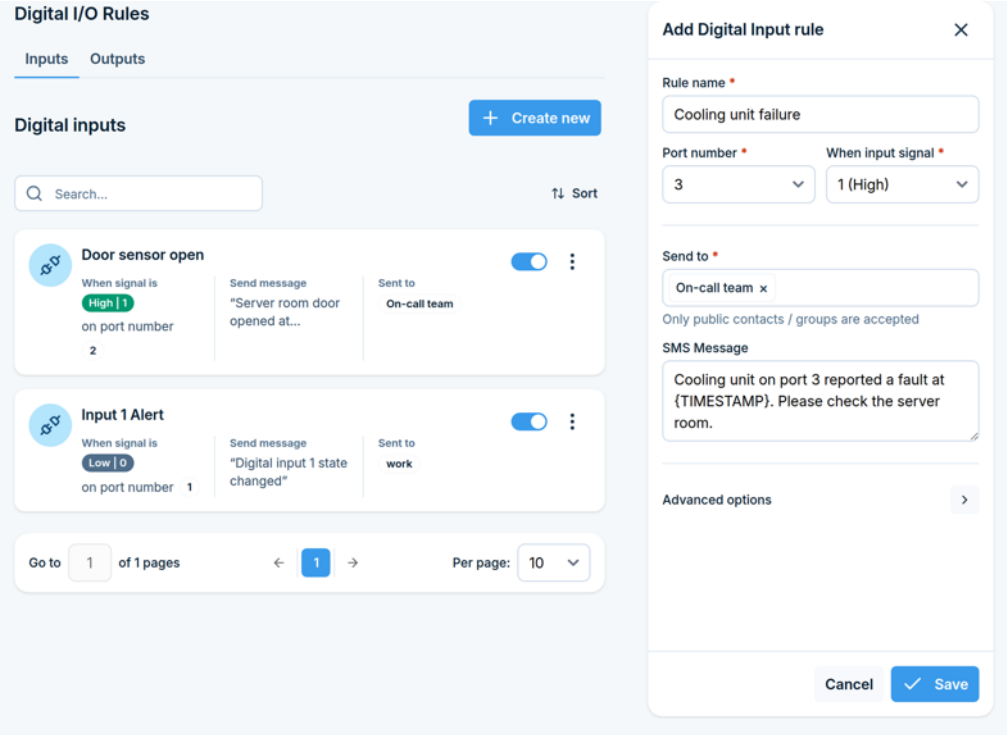
Pick the value that represents the alarm condition on your equipment. Which value that is depends on the contact type (NO or NC) and on how it is wired to the Digital I/O Extender. To check it, trigger the alarm condition once and read the state of the port on the **External pins** page.

Wählen Sie die Empfänger aus

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

Schreiben Sie den SMS-Text

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

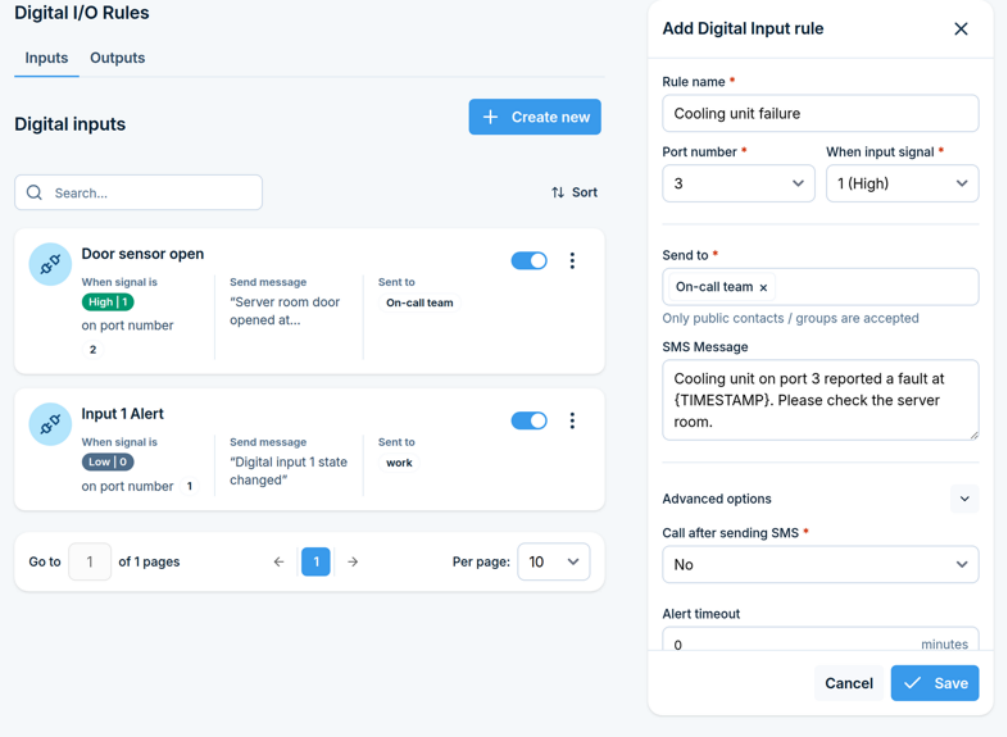


Eine abgeschlossene Eingaberegel

Erweiterte Optionen

Klicken Sie auf **Advanced options**, um diesen Abschnitt zu erweitern. Sie benötigen es nicht für ein grundlegendes Setup.

- **Call after sending SMS** - auch einen Sprachanruf an die gleichen Empfänger tätigen. Die Optionen sind **No**, **Ring**, **Text-to-speech (TTS)** und **Text-to-speech (advanced)**, je nachdem, welches Gerätemodell Sie haben. Mit der erweiterten Option wählen Sie auch ein **Voice model**.
- **Alert timeout** - die Anzahl der Minuten, die vergehen müssen, bevor die gleiche Regel erneut einen Alert auslösen kann. `0` bedeutet keine Begrenzung, daher sendet jede Signaländerung eine SMS.



Input rule erweiterte Optionen

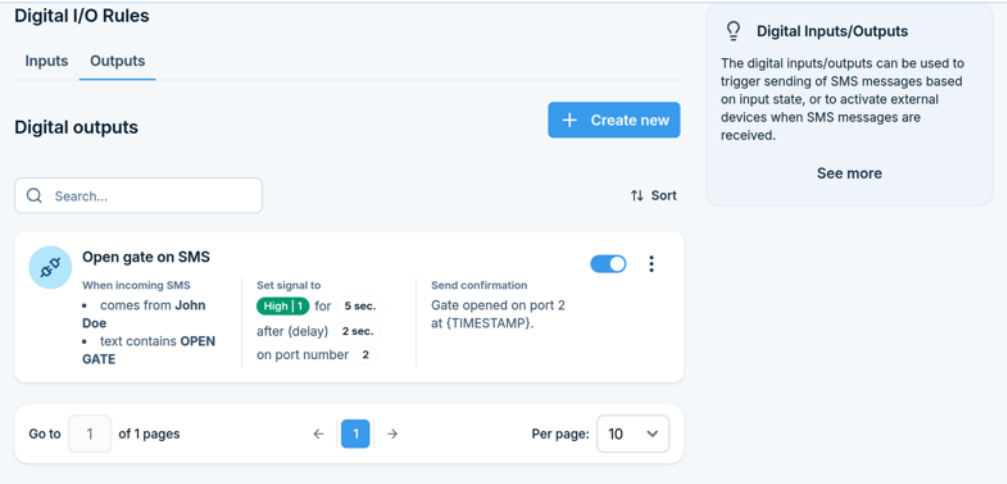
> **Legen Sie einen Alert-Timeout für verrauschte Eingaben fest.** Ein Kontakt, der flattert, oder Ausrüstung, die wiederholt auslöst, kann einen Nachrichtenstoß erzeugen. Ein Timeout von einigen Minuten beschränkt ein echtes Ereignis auf eine SMS.

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

Teil 2: Ausgaberegeln (SMS in Ausgangssignal)

Schritt 1: Öffnen Sie die Regelseite

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



Digitale Ausgaberegeln

Schritt 2: Eine Ausgaberegel erstellen

Klicken Sie auf **Create new** in der oberen rechten Ecke. Ein Seitenpaneel öffnet sich.

Benennen Sie die Regel und wählen Sie den Port

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

Entscheiden Sie, welche SMS-Nachrichten die Regel auslösen

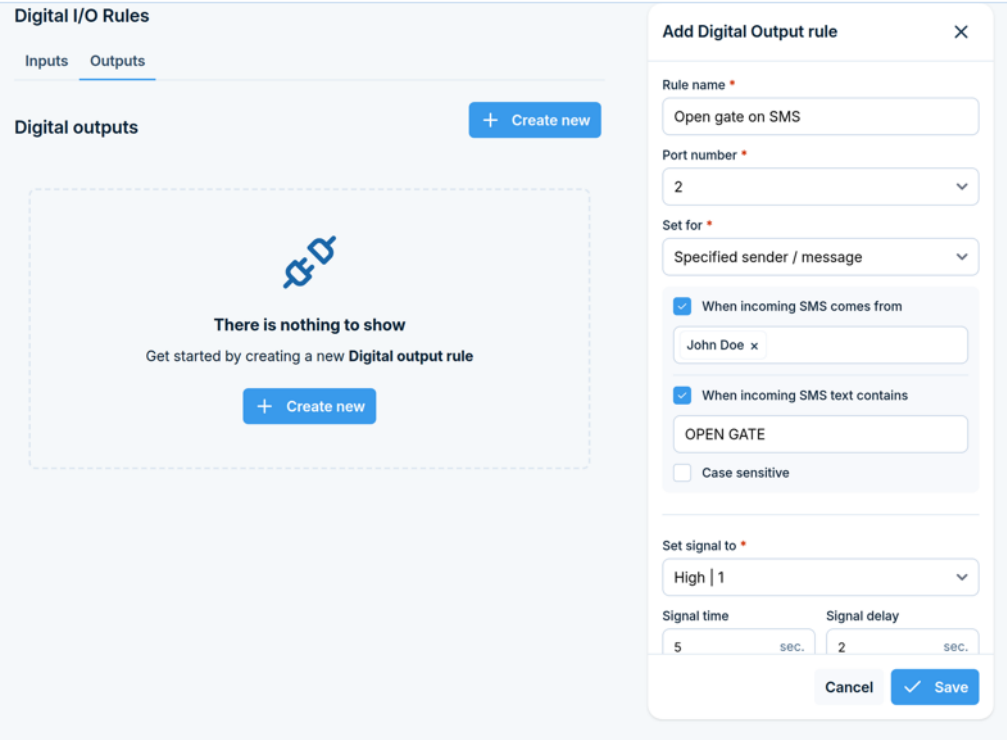
Wählen Sie **Set for**:

Option	Was dies bedeutet
All incoming messages	Jede eingehende SMS schaltet die Ausgabe.
Specified sender / message	Nur Nachrichten, die den unten festgelegten Bedingungen entsprechen, schalten sie.

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

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

When incoming SMS text contains Aktivieren Sie dies und geben Sie die Phrase unter **Text** ein, z. B. `OPEN`. Aktivieren Sie **Case sensitive**, wenn `open` und `OPEN` unterschiedlich behandelt werden sollen.



Bedingungen der Ausgaberegel

Beschränken Sie Ausgaberegeln durch den Sender. Eine Ausgaberegel schaltet physische Ausrüstung. Ohne Senderbedingung kann jeder, der Ihre Nummer kennt, damit arbeiten.

Entscheiden Sie, was die Ausgabe tut

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

Erweiterte Optionen

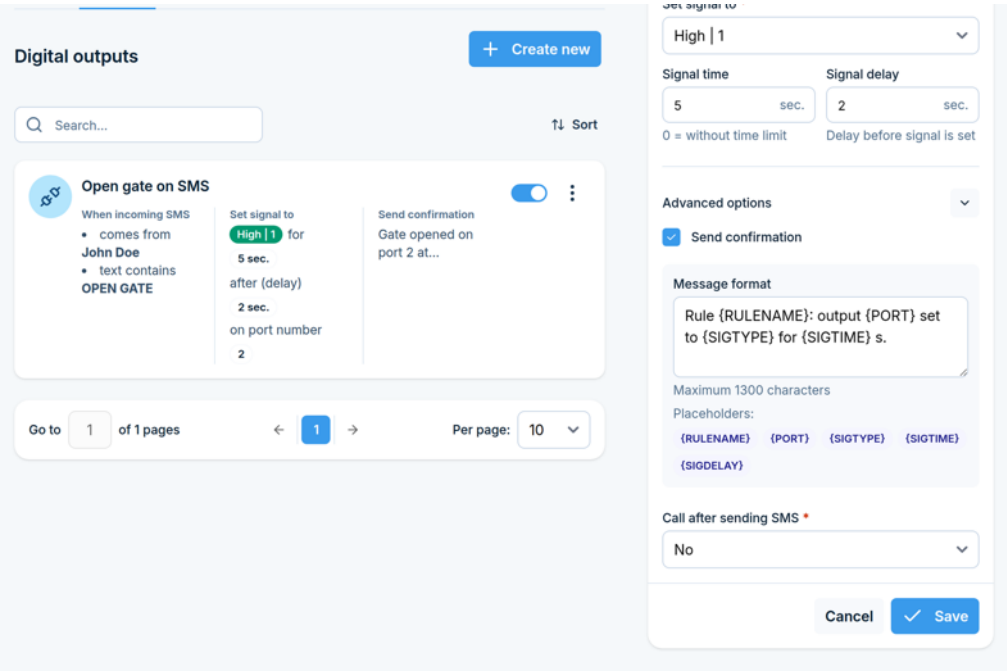
Klicken Sie auf **Advanced options**, um diesen Bereich zu erweitern.

Send confirmation Aktivieren Sie diese Option, um eine SMS an den Absender zu senden, nachdem die Ausgabe geschaltet wurde. Das Feld **Message format** erscheint mit maximal 1300 Zeichen. Sie können den Text aus Platzhaltern zusammenstellen:

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

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

Nach dem Senden einer SMS anrufen Führen Sie auch einen Sprachanruf durch, genau wie oben für Eingaberegeln beschrieben.



Bestätigungsmeldung der Ausgaberegel

Klicken Sie auf **Save** (Speichern). Die Regel funktioniert ab sofort bei empfangenen Nachrichten.

Part 3: External pins

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

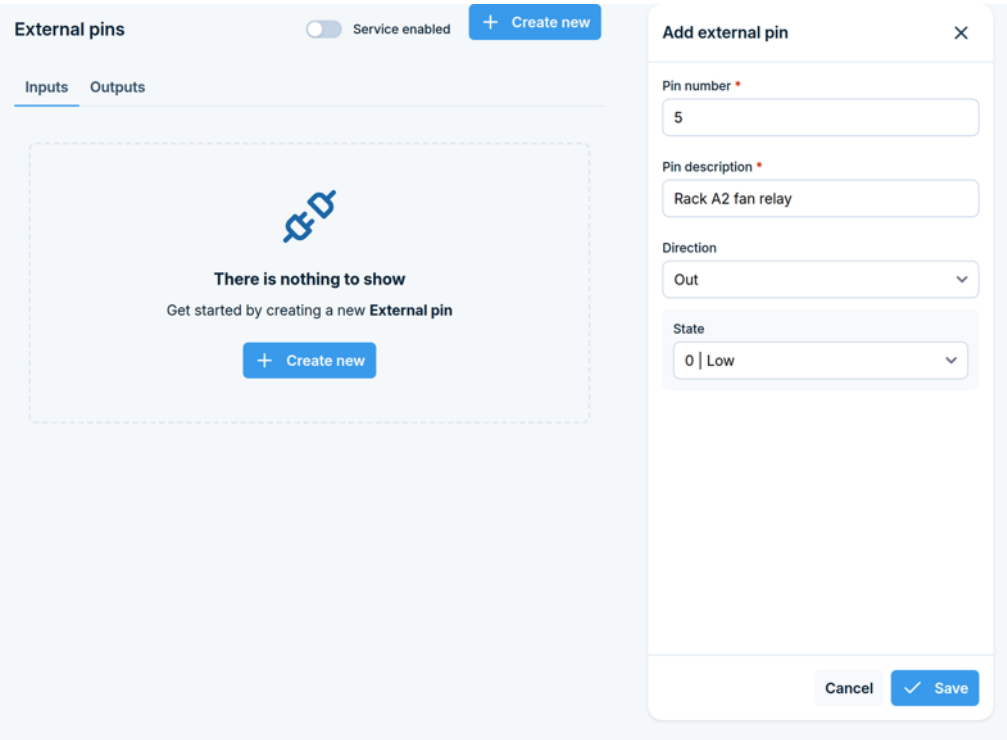
Go to **Monitoring > Digital input / output > External pins**. The page has an **Inputs** tab and an **Outputs** tab, plus a **Service enabled** switch that starts and stops the io-bridge service, which reads and drives the Digital I/O Extender ports. **While it is off, Input and Output rules do not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

Externen Anschluss hinzufügen

Klicken Sie auf **Create new** (Neu erstellen). Ein Seitenpanel wird geöffnet.

Feld	Was Sie eingeben sollten
Pin number (Anschlussnummer)	The port number on the Digital I/O Extender, for example 1. Each number can only be configured once.
Pin description (Anschlussbeschreibung)	Ein Kurzname mit maximal 64 Zeichen. Nur Buchstaben, Ziffern und Leerzeichen sind zulässig.
Direction (Richtung)	**In** für einen Anschluss, den Sie lesen, **Out** für einen Anschluss, den Sie steuern.
Zustand	Nur für **Out**-Pins angezeigt: der Zustand, in dem der Port startet, `1 | High` oder `0 | Low`.

Klicken Sie auf **Save**.



Externe Pin wird hinzugefügt

Die Pins verwenden

- Auf der Registerkarte **Outputs** können Sie den Zustand eines Pins direkt aus der Liste ändern.
- Auf der Registerkarte **Inputs** ist der Zustand schreibgeschützt, da der Wert durch das an den Pin angeschlossene Element gesteuert wird.

- Once defined, external pins also appear in the **Port number** lists of Input and Output rules, marked `(Ext)`.
- The **Inputs** tab shows the live state of each input, which is useful for checking your wiring before you write a rule.

Verhalten von Digital I/O-Regeln

- Regeln reagieren nur auf Ereignisse, die nach dem Erstellen und Aktivieren der Regel auftreten. Verwenden Sie den Schalter neben einer Regel, um sie zu unterbrechen, ohne sie zu löschen.
- Wenn mehrere Regeln das gleiche Ereignis erfüllen, wird **jede** von ihnen ausgeführt, sodass ein Eingangssignal mehrere Nachrichten senden und eine SMS mehrere Ports schalten kann.
- Die Textbedingung für Output-Regeln ist ein **contains**-Abgleich, kein exakter Abgleich.
- Rules need the **External pins** service on.

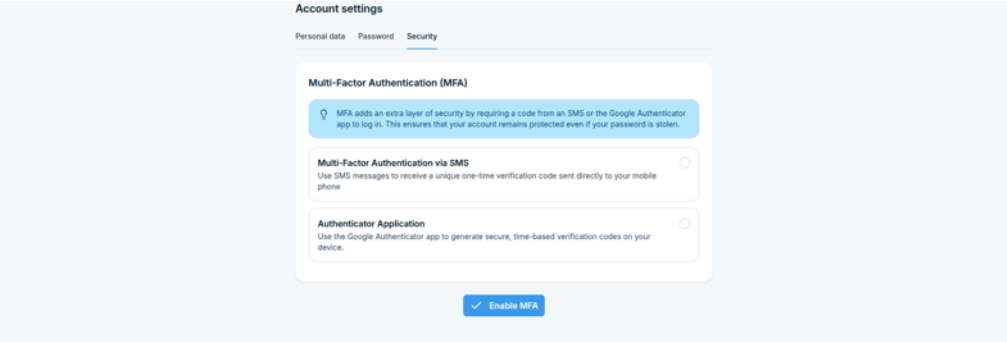
Einstellungen

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

Kontoeinstellungen

Klicken Sie auf Ihren Avatar (unten links) und wählen Sie **Kontoeinstellungen**, um Ihr eigenes Konto zu verwalten, auf drei Registerkarten: **Persönliche Daten** (Name, Benutzername, Telefonnummer, Oberflächensprache, Voreinstellungen für das Verfassen, Benachrichtigungston), **Passwort** und **Sicherheit** – siehe Web Interface Overview für das vollständige Layout der Registerkarten.

Multi-Faktor-Authentifizierung (MFA) konfigurieren



MFA-Einrichtung unter Kontoeinstellungen > Sicherheit

MFA fügt eine zusätzliche Sicherheitsebene hinzu, indem zusätzlich zum Passwort ein Einmalcode erforderlich ist, um sich anzumelden. Dies schützt das Konto, auch wenn das Passwort gestohlen wird.

Wo Sie es finden

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

Schritt 1: Wählen Sie eine MFA-Methode

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

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

- **Authenticator-Anwendung** – zeitbasierte Codes werden durch eine App wie Google Authenticator generiert.

Klicken Sie auf **MFA aktivieren** und folgen Sie den Anweisungen auf dem Bildschirm, um die gewählte Methode zu bestätigen.

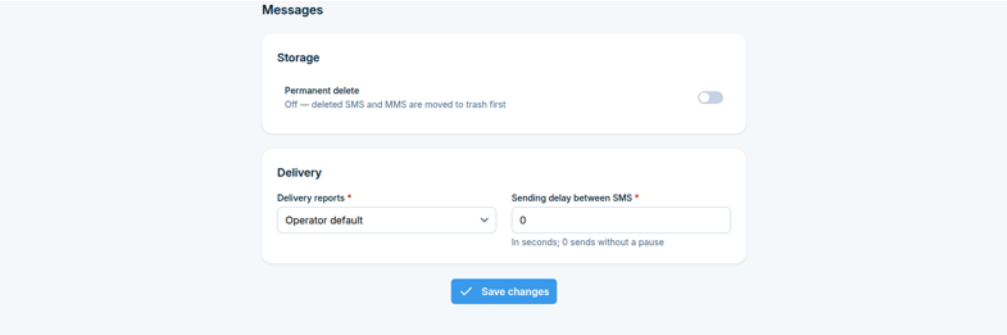
Schritt 2: MFA geräteübergreifend erzwingen (optional)

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

- **Nicht erzwingen** – jeder Benutzer entscheidet einzeln, ob MFA aktiviert werden soll.
- **Für alle Benutzer erzwingen** – jeder vorhandene und neue Benutzer muss MFA einrichten.
- **Für neue Benutzer erzwingen** – MFA ist nur für ab sofort 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-Speicherungs- und Lieferpipeline zusammen.

Speicherung

Permanent löschen – standardmäßig aus, daher werden gelöschte SMS und MMS zunächst in den Papierkorb verschoben, statt sofort entfernt zu werden.

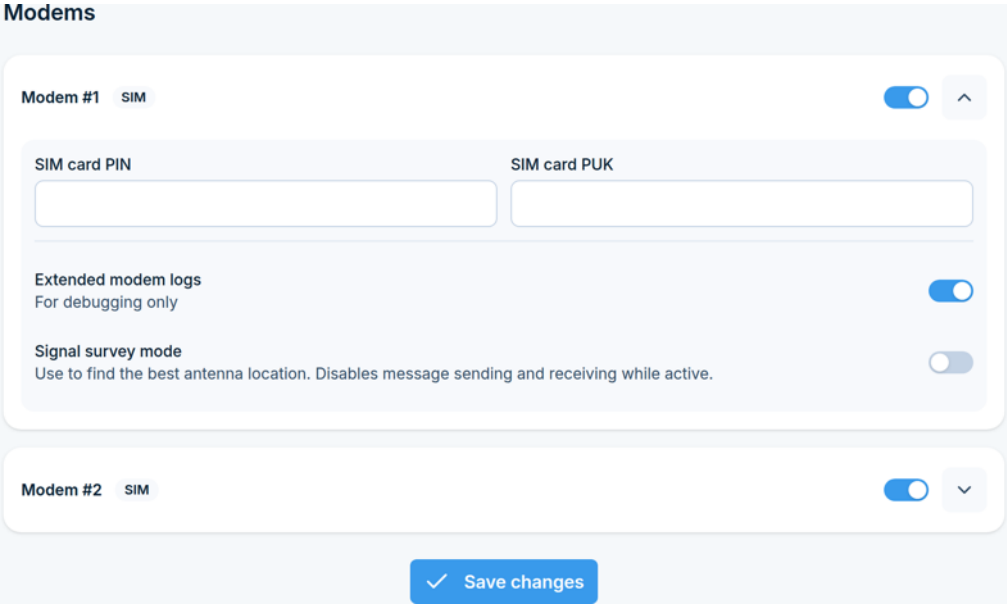
Lieferung

Lieferberichte zeigen Ihnen, ob eine gesendete SMS das Telefon des Empfängers tatsächlich erreicht hat.

- **Lieferberichte** - Standardverhalten des Betreibers (Standardverhalten des Mobilfunkbetreibers verwenden), Immer anfordern oder Nie anfordern. Wird auch während des Konfigurationsassistenten angeboten.
- **Verzögerung beim SMS-Versand** - eine Pausierung in Sekunden zwischen aufeinanderfolgenden ausgehenden SMS. `0` versendet ohne Pausierung.

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

Modems



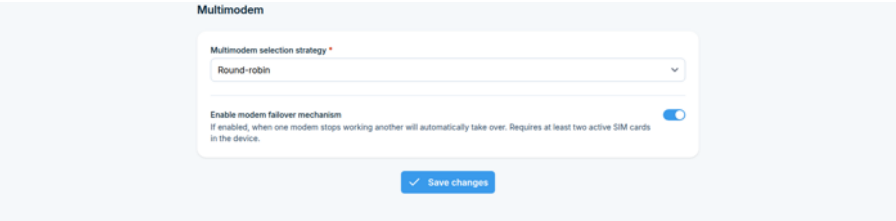
Modem-Einstellungen mit erweitertem Bereich des ersten Modems

Einstellungen > SMS / MMS > Modems (`/settings/sms-mms/modems/`) listet jedes integrierte Modem (Modem #1, Modem #2 bei Multi-Modem-Geräten) mit einem Schalter zum Aktivieren der SIM auf. Das Erweitern des Bereichs eines Modems zeigt vier Einstellungen:

- **SIM-Kartenpin** und **SIM-Kartenpuk** - nur erforderlich, wenn die Karte danach fragt. Die gleichen zwei Felder werden auch während des Konfigurationsassistenten angeboten.
- **Erweiterte Modem-Protokolle** - ausführliches Modem-Logging nur zum Debuggen.
- **Signalumfragemodus** - verwenden Sie diesen, um den besten Antennenstandort zu finden. Er **deaktiviert das Senden und Empfangen von Nachrichten** während er aktiv ist. Schalten Sie ihn aus, wenn Sie fertig sind.

Multi-Modem

Einstellungen > SMS / MMS > Multimodem (`/settings/sms-mms/multimodem/`) bestimmt, welche der acht eingebauten Modems des Geräts jede ausgehende SMS sendet, und ob ein anderes Modem übernimmt, wenn eines ausfällt. Die Seite ist nur für Administratoren verfügbar.

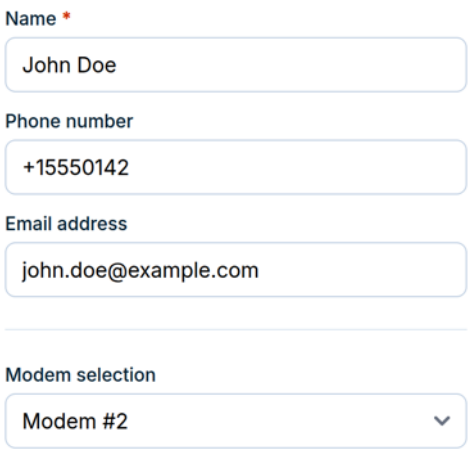


Multimodem-Einstellungen, hier auf einem Gerät mit zwei Modems dargestellt. MHD-8100 listet SIM 1 bis SIM 8 auf

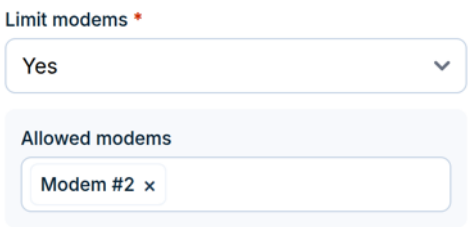
Wie SMSEagle ein Modem auswählt

Die beiden Einstellungen auf dieser Seite sind nur ein 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 Automation-Regel, die auf ein Modem beschränkt ist, wird dieses Modem verwendet und nichts Nachfolgendes gilt. Der Absender muss berechtigt sein, es zu verwenden (siehe Regel 3), andernfalls wird die Nachricht abgelehnt.
2. **Ein an den Kontakt gebundenes Modem.** Wenn die Nachricht an einen Phonebook-Kontakt geht, dessen **Modem-Auswahl** festgelegt ist, wird dieses Modem verwendet und nichts Nachfolgendes gilt.
3. **Die erlaubten Modems des Absenders. Limit modems** in den Einstellungen des Benutzers unter **System > Users** beschränkt den Benutzer auf die dort aufgelisteten **Allowed modems**. Ohne eine Beschränkung kann der Benutzer jedes Modem verwenden. Modems, deren SIM unter Modems ausgeschaltet ist, werden ausgelassen, es sei denn, es würde keine übrig bleiben.
4. **Die Auswahlstrategie** wählt eines der erlaubten Modems. Siehe Multimodem selection strategy unten.
5. **Modem failover**, wenn aktiviert, ersetzt das ausgewählte Modem durch das nächste funktionierende, wenn das ausgewählte Modem in diesem Moment nicht funktioniert. Siehe Modem failover unten.



Ein Kontakt, der an Modem #2 gebunden ist (Regel 2)



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

Multi-Modem-Auswahlstrategie

Multimodem selection strategy bietet **Round-robin** und eine Option **SIM N as Master modem** für jedes eingebaute Modem (**SIM 1** bis **SIM 8**):

- **Round-robin** - die erlaubten Modems des Absenders wechseln sich ab: Modem 1 > Modem 2 > ... > Modem 8 > Modem 1, und so weiter. Jeder Benutzer hat seine eigene Rotation, daher verschieben zwei Benutzer, die gleichzeitig senden, nicht gegenseitig ihre Reihenfolge.
- **SIM N as 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 nicht mit dieser Strategie senden, außer bei Nachrichten mit einem für sie ausgewählten Modem (Regel 1) oder an einen Kontakt, der an ein Modem gebunden ist (Regel 2). Die Nachrichten werden mit einem Fehler zum Fehlen des Modem-Zugriffs abgelehnt.

Modem-Failover

Aktivieren Sie **Enable modem failover mechanism**, damit ein funktionierendes Modem eines ersetzt, das ausfällt. Dies erfordert mindestens zwei aktive SIM-Karten im Gerät. Failover wirkt an zwei Stellen:

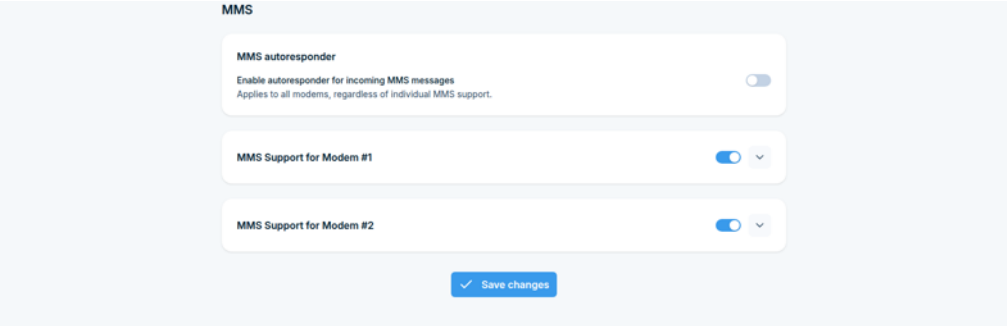
- **Wenn eine Nachricht gesendet wird.** Wenn das von der Strategie ausgewählte Modem nicht funktioniert, versucht SMSEagle das nächste der erlaubten Modems des Absenders in Modem-Nummernreihenfolge, beginnend nach dem letzten wieder von vorne, und verwendet das erste funktionierende. Nachrichten mit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

Ein Modem gilt als nicht funktionierend, wenn eines der folgenden zutrifft:

- es hat sich mehr als 4 Minuten lang nicht zum Gerät gemeldet,
- seine SIM-Karte ist nicht bereit, z. B. fehlt oder wartet auf eine PIN,
- das Watchdog des Geräts, das alle 2 Minuten jedes Modem prüft, hat seinen Modem-Service mindestens 3 Mal schnell hintereinander neu gestartet (weniger als 5 Minuten auseinander), das letzte Mal innerhalb der letzten 5 Minuten,
- Nachrichten auf ihm schlagen wiederholt fehl: mindestens eine Nachricht in seiner Warteschlange wurde 3 Mal erneut versucht, und das Modem hat in den letzten 5 Minuten nichts erfolgreich gesendet. Wenn andere Nachrichten in der gleichen Warteschlange nicht 3 Wiederholungen erreicht haben, wird das Problem als eines mit den fehlgeschlagenen Empfängern angesehen, nicht mit dem Modem.

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

MMS



MMS-Einstellungen

Was diese Funktion bewirkt

MMS ermöglicht dem Gerät das Senden und Empfangen von **Multimedianachrichten**: ein Text mit angehängten Bildern oder anderen Dateien, statt einfacher SMS.

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

Der gleiche Bildschirm enthält auch den **MMS-Autoresponder**, der automatisch eine 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 Daten- oder MMS-Dienst hat, schlägt fehl, egal wie die Einstellungen ausgefüllt sind.
- Viele Operatorprofile sind dem Gerät bereits bekannt. Versuchen Sie **APN-Einstellungen auslesen**, bevor Sie die Werte selbst nachschlagen.

Schritt 1: Öffnen Sie die MMS-Seite

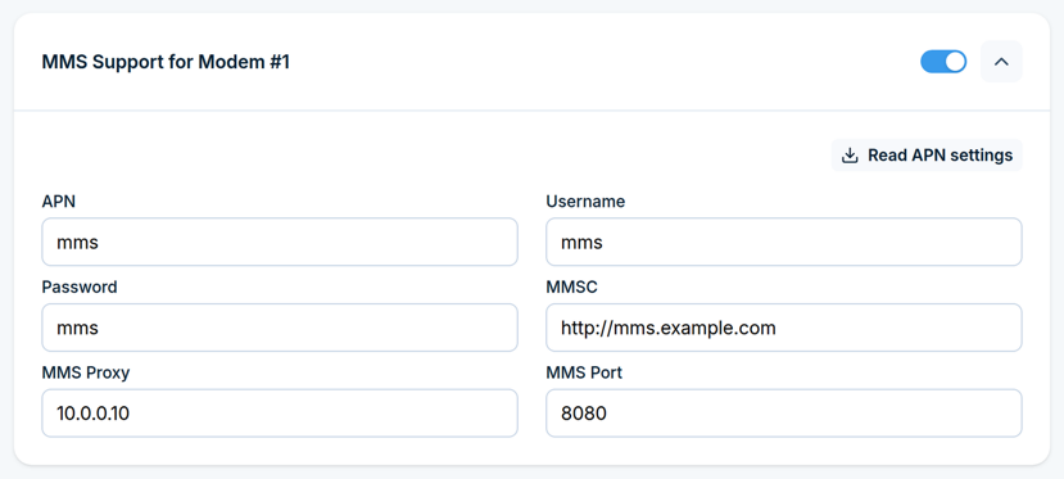
Gehen Sie in der Seitenleiste zu **Einstellungen > Kanäle > SMS / MMS > MMS**.

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

Schritt 2: MMS auf einem Modem aktivieren

Jeder Modem-Bereich 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 Bereich zu erweitern und füllen Sie die Verbindungsparameter aus.



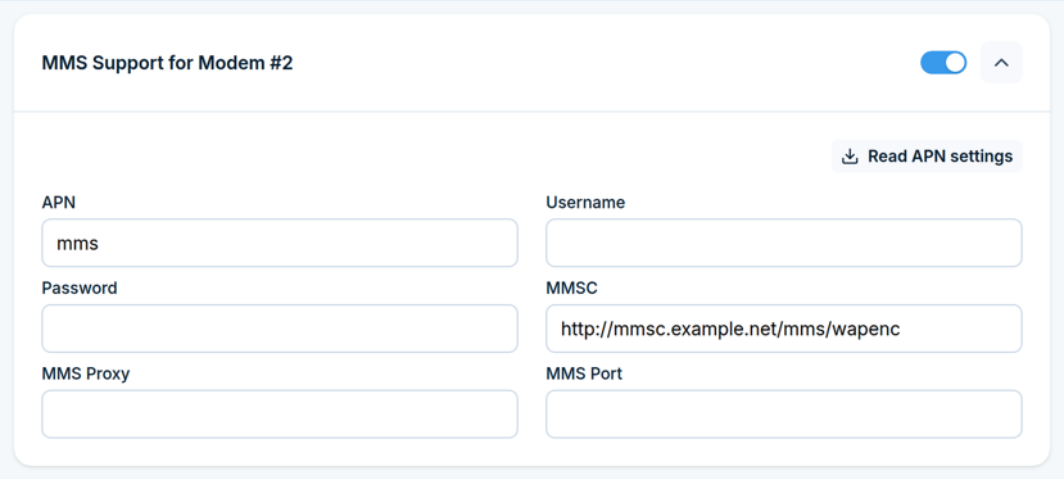
Ein erweiterter Modem-Bereich mit **APN-Einstellungen auslesen** über den Feldern

Schritt 3: Füllen Sie die Verbindungsparameter aus

Der schnellste Weg ist die Schaltfläche **APN-Einstellungen auslesen** oben im erweiterten Bereich. Sie sucht eine passende Konfiguration für die SIM-Karte im Modem und füllt die Felder automatisch aus. Wenn keine Übereinstimmung gefunden wird, meldet SMSEagle dies und Sie tragen die Werte von Hand ein.

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

Jedes Feld gehört zu **diesem einen Modem**. Zwei SIM-Karten von verschiedenen Betreibern benötigen zwei verschiedene Sätze von Werten, also wiederholen Sie dies für jedes Modem, das Sie aktiviert haben.



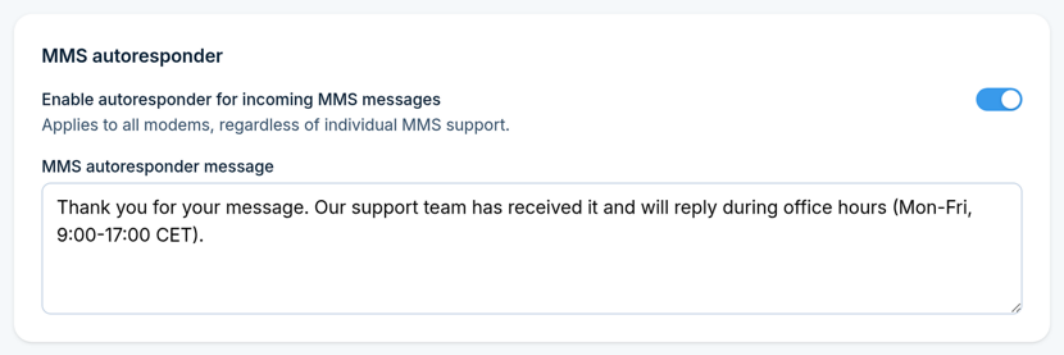
Das zweite Modem trägt seine eigenen Werte und benötigt in diesem Beispiel keinen Proxy

Schritt 4: Richten Sie den Autoresponder ein (optional)

Das **MMS-Autoresponder**-Feld oben auf der MMS-Seite versendet eine automatische 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 globale Einstellung, nicht pro Modem, und es gibt einen gemeinsamen Antworttext für jede eingehende MMS. Wählen Sie daher eine allgemeine Formulierung.



Der Autoresponder aktiviert mit einer Beispielantwort

Schritt 5: Speichern und neu starten

Klicken Sie auf **Save changes**.

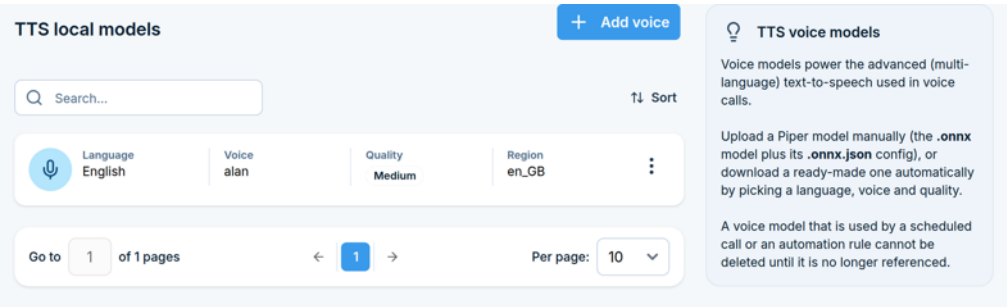
> **Ein Neustart ist erforderlich.** Nach dem Speichern fordert SMSEagle Sie auf, das Gerät neu zu starten, damit die MMS-Änderungen wirksam werden. Bis dahin sind die neuen Parameter gespeichert, aber noch nicht in Betrieb.

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 zeigt die installierten Modelle mit Sprache, Region und Qualität.



TTS-Lokalmodelle

Ein Modell hinzufügen

Klicken Sie oben rechts auf **Add voice**. Das Panel bietet zwei Möglichkeiten.

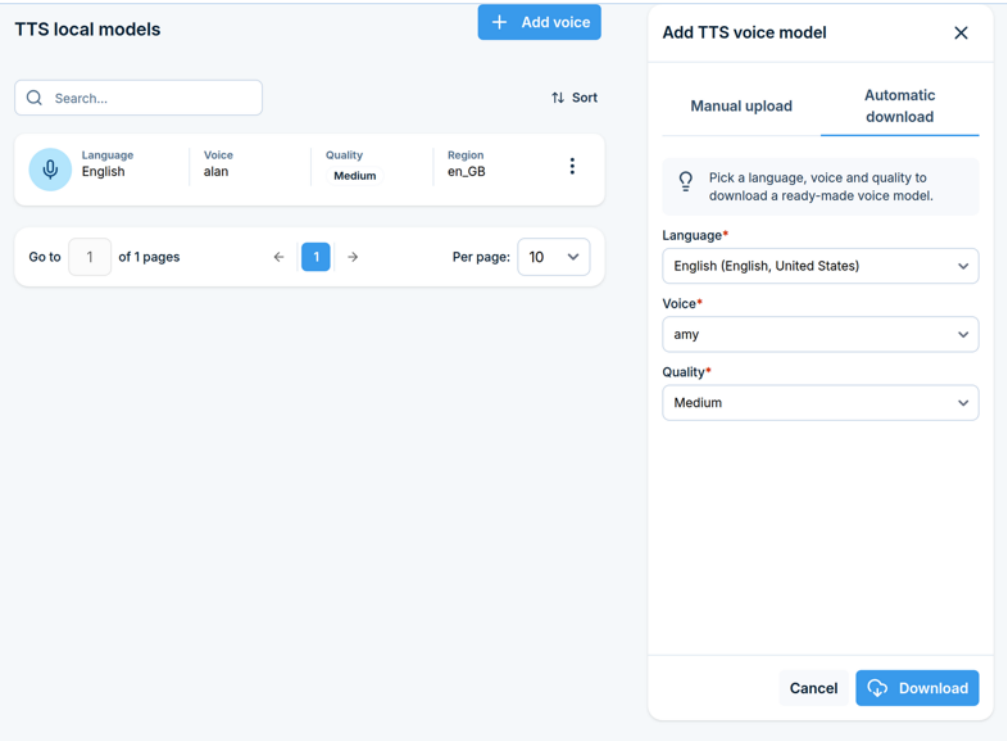
Automatischer Download (die einfache Methode)

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

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

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

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



Download eines vorkonfigurierten Sprachmodells

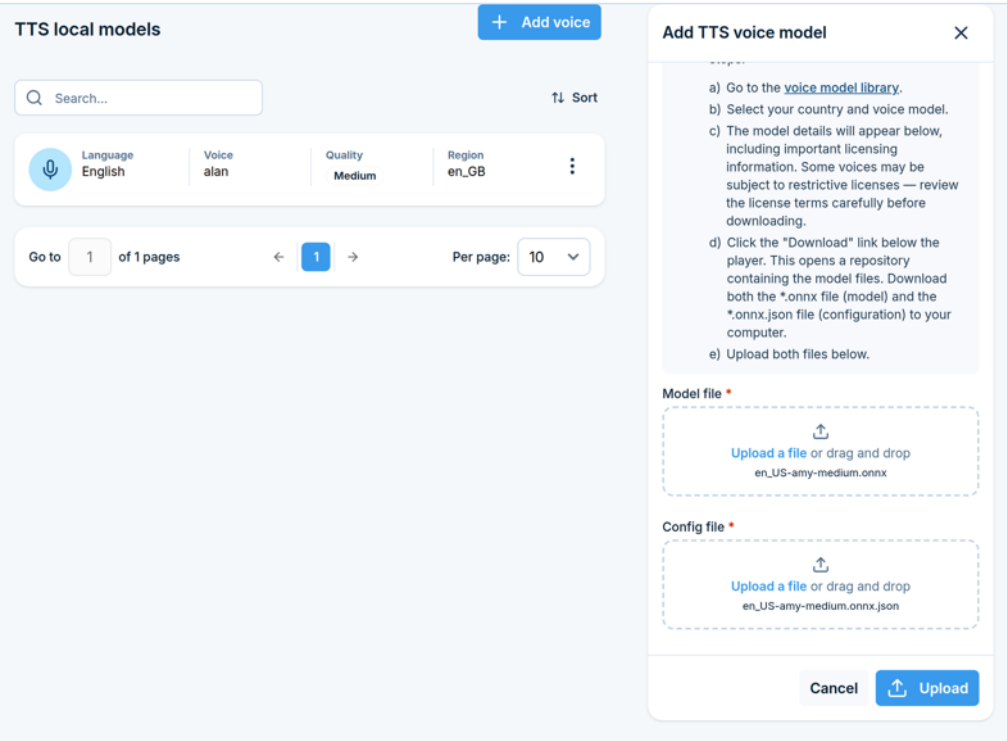
Wenn das Panel „Voice list unavailable

Manueller Upload

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

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

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



Manuelles Hochladen eines Piper-Modells

Ein Modell löschen

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

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

TTS-Online-Modelle (ElevenLabs)

Online-Modelle erzeugen die natürlichsten Sprachausgaben, verwenden aber die ElevenLabs-API und erfordern daher ein ElevenLabs-Konto und eine Internetverbindung.

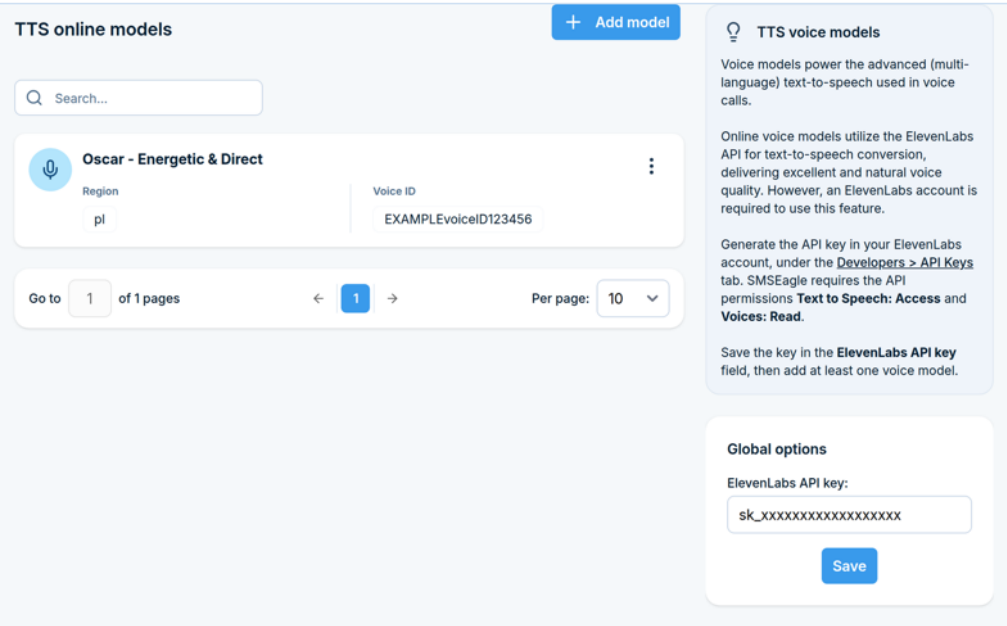
Navigieren Sie zu **Settings > Channels > Calls > TTS online models**.

Schritt 1: ElevenLabs-Konto vorbereiten

In Ihrem ElevenLabs-Konto:

1. Gehen Sie zu **Developers > API Keys** und generieren Sie einen API-Schlüssel.
2. Gewähren Sie dem Schlüssel die Berechtigungen **Text to Speech: Access** und **Voices: Read**, dann speichern Sie.
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 einen Button, der Sie direkt zu den ElevenLabs-Einstellungen führt.



TTS-Online-Modelle

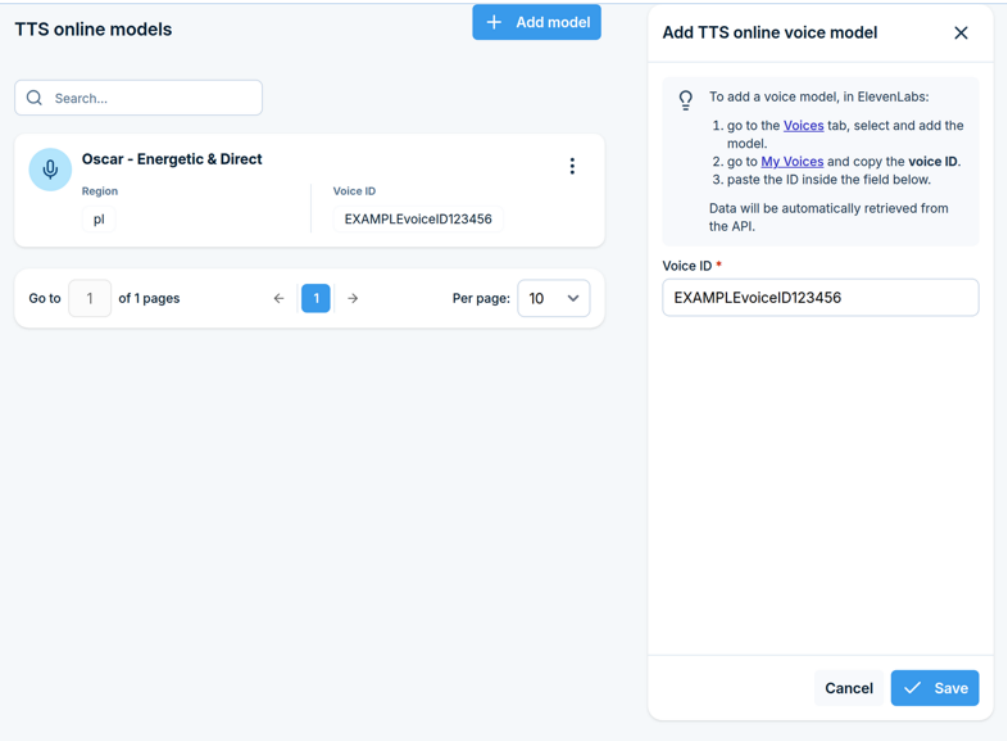
Schritt 2: API-Schlüssel speichern

Fügen Sie den Schlüssel im Feld **ElevenLabs API key** in der Box **Global options** auf der rechten Seite 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 aus der Liste bearbeitet werden (um auf eine andere Voice ID zu verweisen) oder gelöscht werden, einzeln oder in Menge.

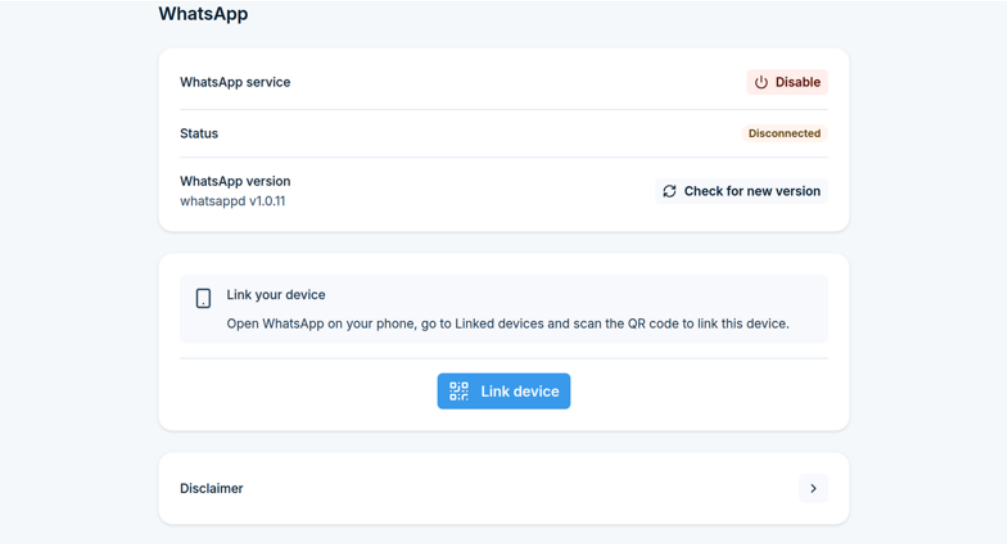
Eingehende Anrufe

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 Anrufweiterleitungscodes pro Modem. Nicht jeder Netzwerkbetreiber unterstützt Weiterleitungscodes – erkundigen Sie sich vor der Nutzung bei Ihrem Betreiber.

WhatsApp



WhatsApp-Einstellungen und Geräteverknüpfung

Was diese Funktion bewirkt

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

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

Typische Anwendungen: Erreichen von Personen, die WhatsApp nutzen, Versenden von längeren Benachrichtigungen ohne Aufteilung in mehrere SMS-Teile oder Kosteneinsparung bei Nachrichten an Empfänger im Ausland.

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

Bevor Sie beginnen

- WhatsApp ist nur auf ausgewählten Gerätemodellen verfügbar. Falls **Settings > Channels > WhatsApp** nicht in Ihrer Seitenleiste angezeigt wird, unterstützt Ihr Gerät dies nicht.
- Sie benötigen ein Telefon mit einem aktiven WhatsApp-Konto in Ihren Händen, um den QR-Code zu scannen.
- Das Gerät muss auf das Internet zugreifen können. WhatsApp-Nachrichten werden über die Netzwerkverbindung übertragen, nicht durch das Modem.

> **Das verknüpfte Konto ist ein echtes WhatsApp-Konto.** Alles, was das Gateway sendet, erscheint als von diesem Konto stammend, 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** an. Bei einem neuen Gerät ist der Status **Disabled** und eine Warnung erläutert, dass der Dienst aktiviert werden muss, bevor ein Gerät verknüpft werden kann.

Schritt 2: Aktivieren Sie den Dienst

Klicken Sie auf **Enable** am unteren Ende der Seite. Der Status ändert sich zu **Disconnected**, was bedeutet, dass der Dienst läuft, aber noch kein Konto verknüpft ist. Dies ist der Zustand, der in der Abbildung zu Beginn dieses Abschnitts gezeigt wird, mit der Schaltfläche **Link device**, die unter dem Connection-Feld wartet.

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 ein neues Gerät zum Verknüpfen aus.
3. Richten Sie das Telefon auf den QR-Code auf dem Bildschirm.

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

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

Sie können den Prozess auch selbst mit **Cancel linking** stoppen.

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

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

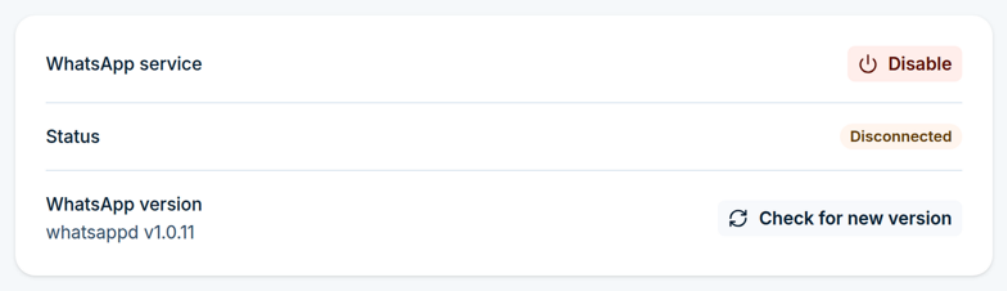
Fall back to SMS/MMS Wenn aktiviert, wird eine Nachricht an eine Nummer, die nicht auf WhatsApp registriert ist, statt als Fehler als SMS oder MMS gesendet. Wenn deaktiviert, wird eine solche Nachricht einfach nicht zugestellt.

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

Schritt 5: Halten Sie den Dienst auf dem neuesten Stand

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

Ergebnis	Was tun
Keine neue Version gefunden	Nichts. Sie haben die aktuelle Version.
Eine neue Version ist verfügbar	Die Schaltfläche wird zu **Jetzt aktualisieren**, was Sie zur Patch-Seite führt, auf der die Aktualisierung 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 **Nach neuer Version suchen** neben der installierten Version

Verknüpfung aufheben und ausschalten

Zwei Schaltflächen unten auf der Einstellungsseite haben unterschiedliche Funktionen:

Schaltfläche	Was sie tut
Gerät verknüpfung aufheben	Meldet das Konto ab. Der Service läuft weiter, die Seite kehrt zu **Getrennt** zurück und Sie können ein anderes Konto verknüpfen. **Auf SMS/MMS zurückgreifen** wird gleichzeitig ausgeschaltet.
Deaktivieren	Stoppt den WhatsApp-Service vollständig. Der Kanal verschwindet aus dem Verfassen-Fenster.

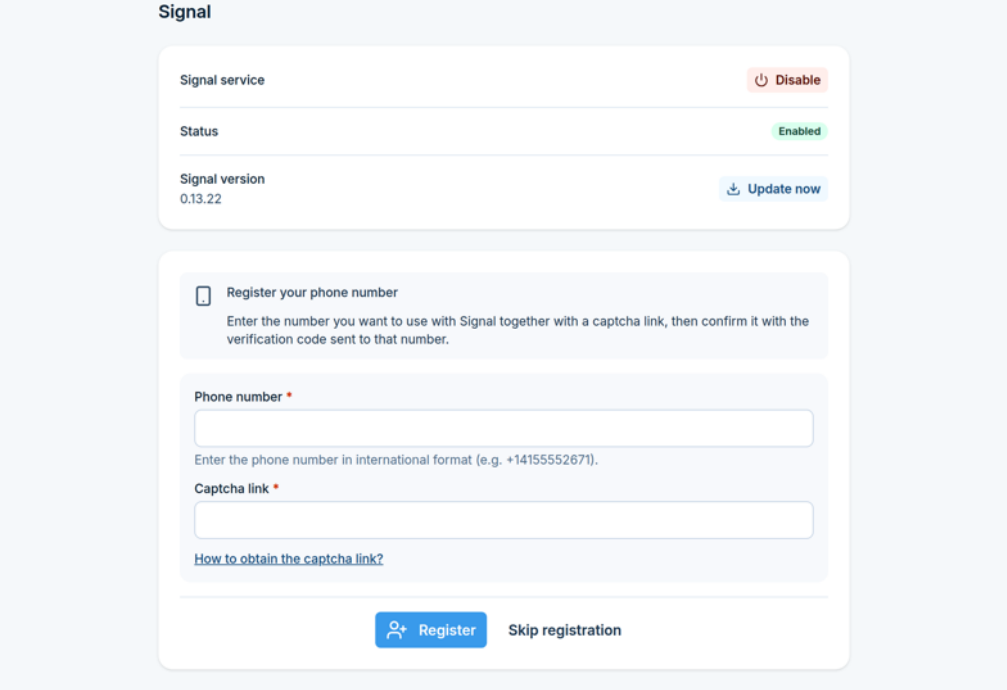
Sie können die Verknüpfung auch von der Telefonseite aus aufheben, in **WhatsApp > Verknüpfte Geräte**. Die Seite zeigt dann beim nächsten Aktualisieren **Getrennt** an.

Wissenswert

- WhatsApp-Nachrichten verwenden die Netzwerkverbindung, daher verbrauchen sie kein SIM-Guthaben und sind nicht von der GSM-Abdeckung abhängig. Die Option **Auf SMS/MMS zurückgreifen** ist die Ausnahme: Diese Fallback-Nachrichten gehen über das Modem.

- Die Verknüpfung liegt auf dem Gerät. Das Wiederherstellen eines Backups auf anderer Hardware oder das Aufheben der Verknüpfung vom Telefon erfordert das Scannen eines neuen QR-Codes.
- Nur Nachrichten, die empfangen wurden, nachdem das Gerät verknüpft wurde, werden in der Gesprächsliste angezeigt.

Signal



Signal-Serviceeinstellungen

Was diese Funktion bewirkt

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

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

Die Einrichtung besteht aus zwei Teilen: Zuerst aktivieren Sie den Service und registrieren eine Nummer (**Einstellungen > Kanäle > Signal**), dann verwenden Sie den Kanal (**Nachrichten > Signal** oder das Verfassen-Fenster).

Bevor Sie beginnen

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

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

Schritt 2: Aktivieren Sie den Dienst

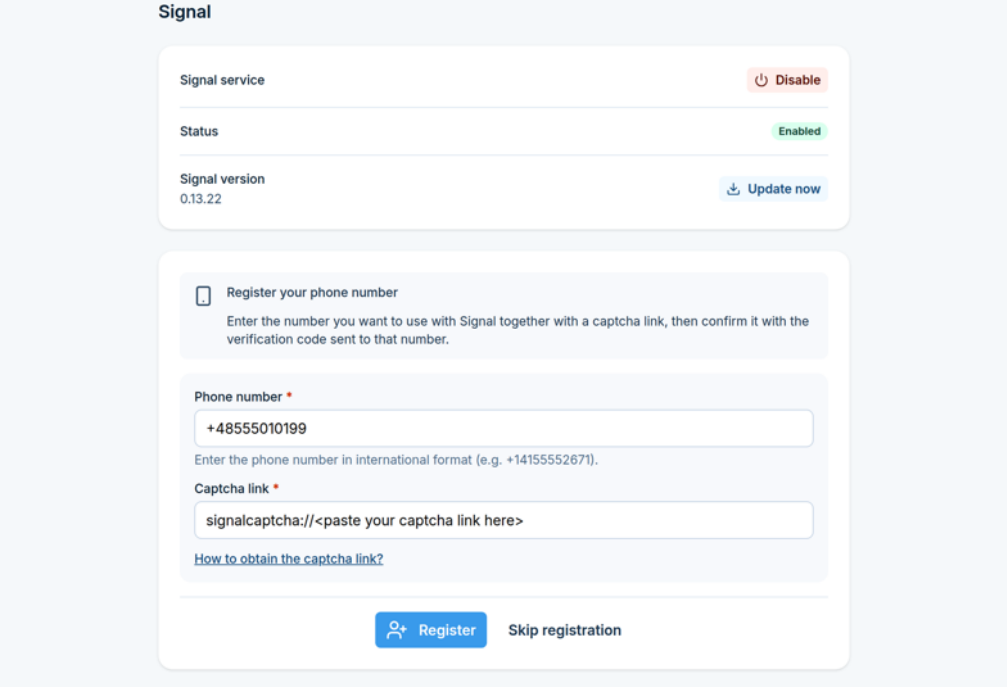
Klicken Sie **Enable** am unteren Ende der Seite. Der Status ändert sich zu **Enabled** und das Registrierungsformular erscheint, wie in der Abbildung am Anfang dieses Abschnitts.

Schritt 3: Registrieren Sie eine Telefonnummer

Im Feld **Register a phone number**:

1. In **Phone number** geben Sie die Nummer im internationalen Format ein, zum Beispiel `+14155552671`.
2. In **Captcha link** fügen Sie den Captcha-Link ein. Der Link **How to obtain the captcha link?** unterhalb des Felds öffnet Schritt-für-Schritt-Anweisungen in einem neuen Tab.
3. Klicken Sie **Register**.

Signal sendet dann einen Verifizierungscode an die Nummer.



Registrierung einer Telefonnummer

Haben Sie diese Nummer kürzlich bereits registriert? Klicken Sie stattdessen **Skip registration**. Das Formular springt direkt zum Verifizierungsschritt, in dem Sie einen Code eingeben können, den Sie bereits erhalten haben.

Schritt 4: Überprüfen Sie die Nummer

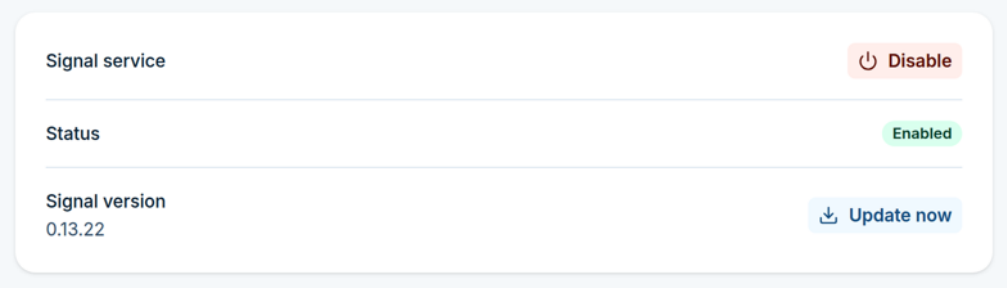
Das Formular fragt nun nach dem **Verification code**. Geben Sie den erhaltenen Code ein und klicken Sie **Verify**.

Bei erfolgreicher Ausführung meldet die Seite, dass Signal verbunden ist, und zeigt das Feld **Registered number**.

Schritt 5: Halten Sie den Dienst auf dem neuesten Stand

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

Ergebnis	Was tun
Keine neue Version gefunden	Nichts. Sie haben die aktuelle Version.
Eine neue Version ist verfügbar	Die Schaltfläche wird zu **Jetzt aktualisieren**, was Sie zur Patch-Seite führt, auf der die Aktualisierung 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.

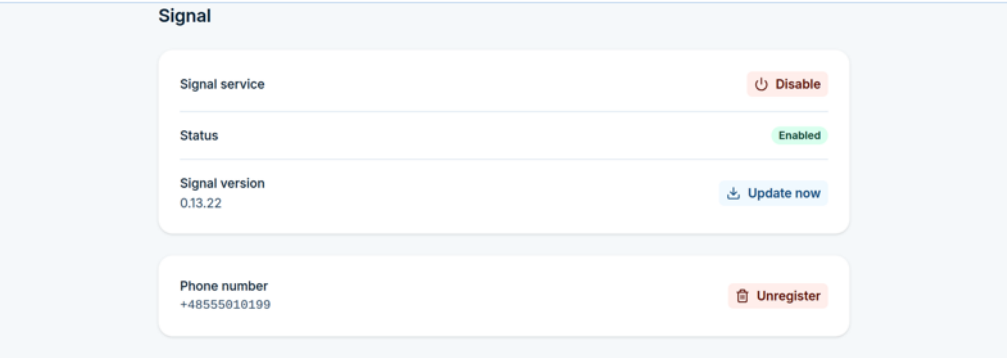


Das Service-Feld. Hier hat eine Prüfung bereits eine neuere Version gefunden, daher lautet die Schaltfläche **Update now**

Entfernen der Nummer

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

Um den Kanal zu deaktivieren, ohne die Registrierung aufzuheben, klicken Sie **Disable** am unteren Ende der Seite. Der Service stoppt und Signal verschwindet aus dem Fenster „Compose“, aber die Registrierung wird beibehalten, daher ist bei erneuter Aktivierung keine neue Verifizierung erforderlich.



Eine registrierte Signal-Nummer

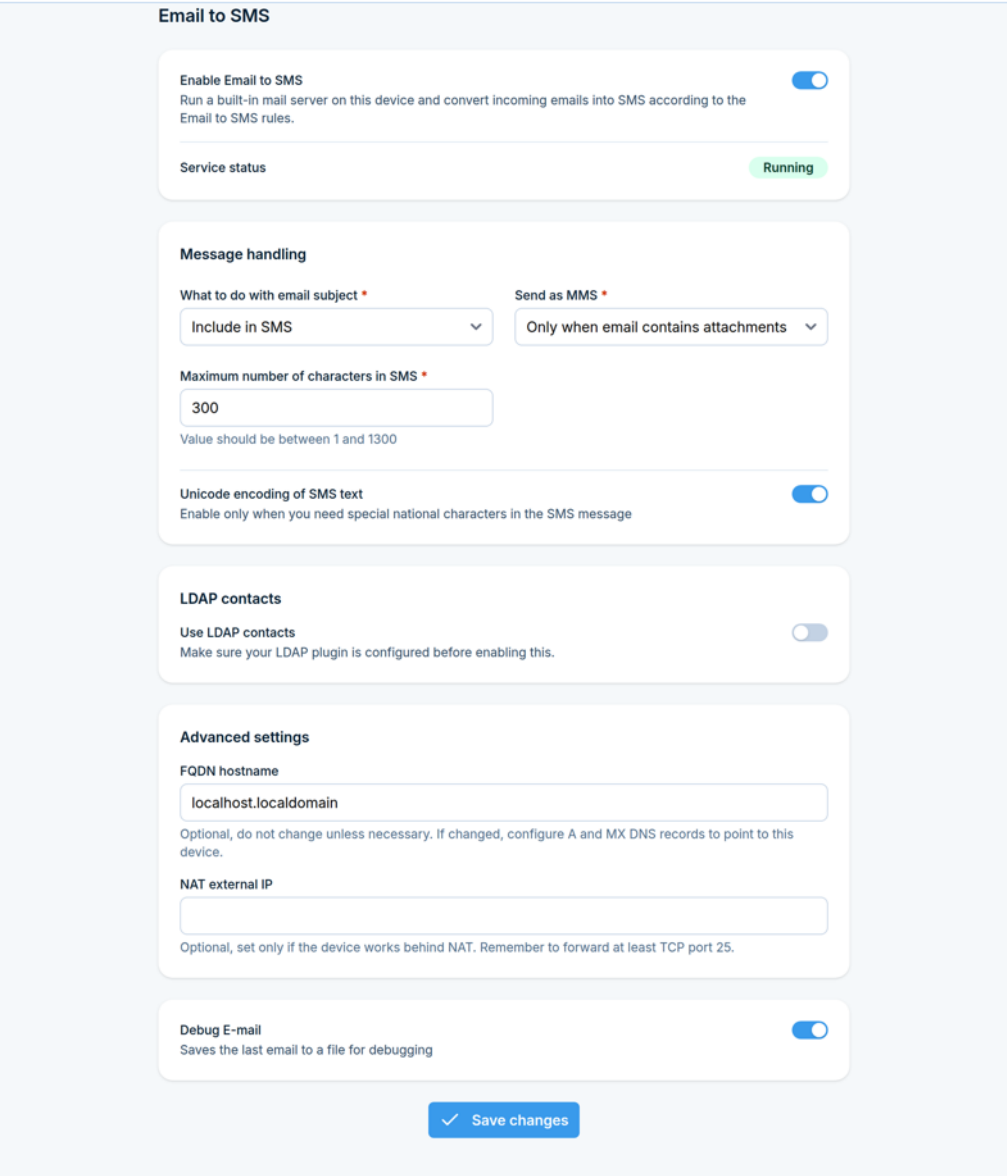
Wissenswert

- Signal-Nachrichten werden über die Netzwerkverbindung versendet, nicht über das Modem, daher verbrauchen sie kein SIM-Guthaben und hängen nicht von der GSM-Abdeckung ab.
- Die Registrierung befindet sich auf dem Gerät. Eine Wiederherstellung einer Sicherung auf anderer Hardware oder das Entfernen der Nummer erfordert eine erneute Registrierung.
- Nur nach der Aktivierung des Service empfangene Nachrichten erscheinen in der Unterhaltungsliste.

Email

Email to SMS

Einstellungen > Channels > Email > Email to SMS (`/settings/email/email-to-sms`) startet einen eingebauten Mail-Server auf dem Gerät und konvertiert eingehende E-Mails in SMS gemäß den Regeln, die Sie unter Email to SMS in Automation definieren.



Email to SMS-Einstellungen

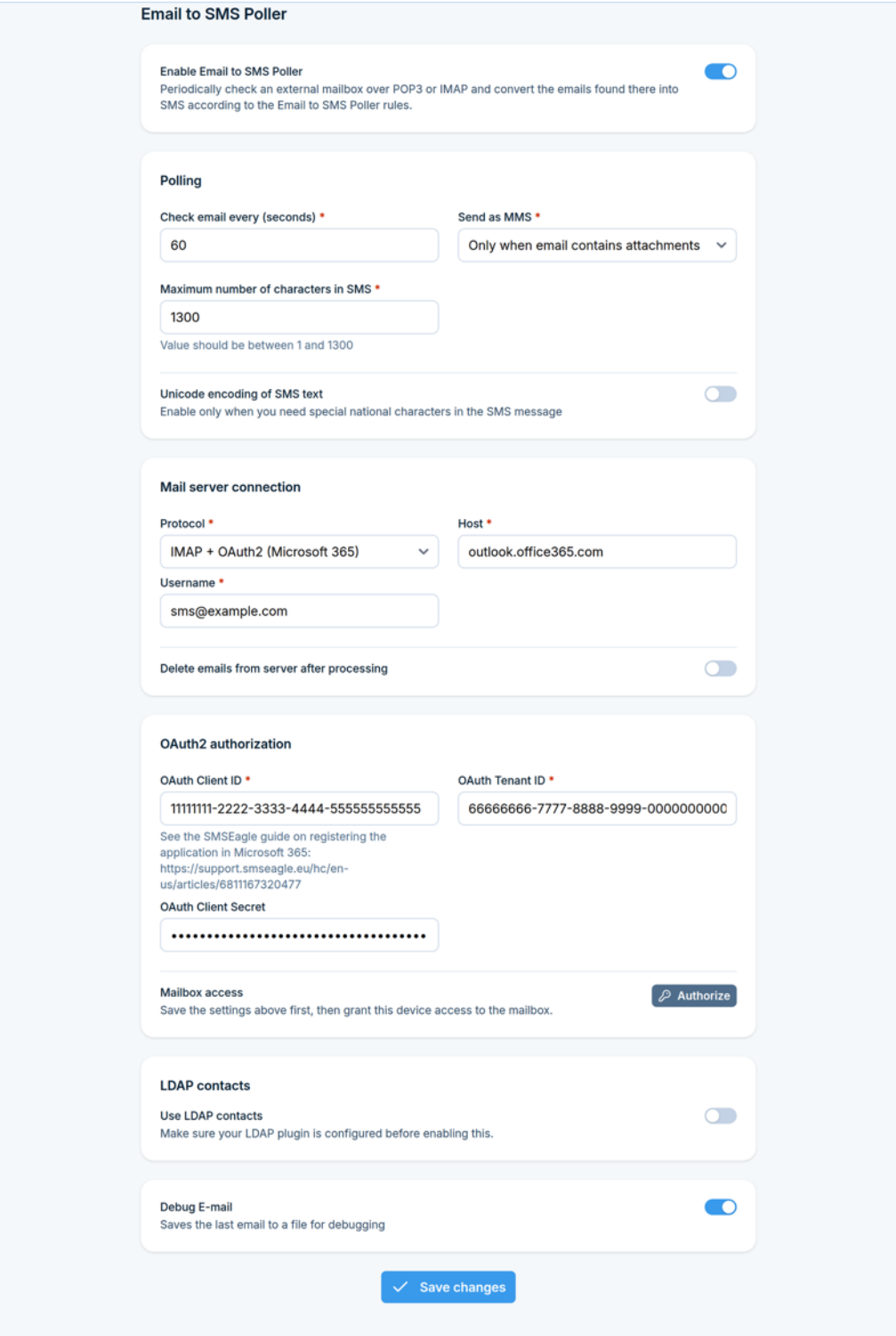
Aktivieren Sie **Enable Email to SMS**, um den Mail-Server zu starten. **Service status** zeigt, ob er **Running** oder **Stopped** ist. Der Rest der Seite bestimmt, wie eine E-Mail zu einer SMS wird:

- **What to do with email subject** - **Ignore** it, **Include in SMS**, **Use for authentication**, oder **Send only subject without email body**.
- **Als MMS senden** - **Nie**, **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 Sonderzeichen benötigen, die das Standard-SMS-Alphabet nicht hat.
- **LDAP-Kontakte verwenden** - ermöglicht es, im Empfängerteil der Adresse einen Verzeichniskontakt oder eine Gruppe zu benennen. Konfigurieren Sie zuerst LDAP.
- **FQDN-Hostname** (unter **Erweiterte Einstellungen**) - optionaler Domänenname zur Verwendung in Empfängeradressen anstelle der IP-Adresse des Geräts. Wenn Sie ihn ändern, richten Sie die A- und MX-DNS-Einträge für diesen Namen auf das Gerät.

- **NAT 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 in einer Datei zur Fehlerbehebung.

Email to SMS Poller

Einstellungen > Kanäle > E-Mail > Email to SMS Poller (`/settings/email/email-to-sms-poller`) verbindet das Gerät mit einem vorhandenen Postfach, überprüft es in festgelegten Abständen und konvertiert die gefundenen E-Mails gemäß den Regeln unter Email to SMS Poller in der Automatisierung in SMS. Anders als bei Email to SMS muss keine Mail 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 diese Teile:

Polling

- **E-Mail alle (Sekunden) überprüfen** - wie oft das Postfach überprüft wird.
- **Als MMS senden**, **Maximale Anzahl von Zeichen in SMS** und **Unicode-Kodierung von SMS-Text** - gleiche Bedeutung wie bei Email to SMS.

Mailserver-Verbindung

- **Protokoll** - **POP3**, **IMAP**, oder **IMAP + OAuth2 (Microsoft 365)**.
- **Host** und **Benutzername** des Postfachs.
- Nur bei **POP3** und **IMAP**: **Port**, **Passwort** und **TLS/SSL-Verschlüsselung verwenden**. Die Seite listet die Standardports auf: POP3 110, POP3 mit TLS/SSL 995, IMAP 143, IMAP mit TLS/SSL 993.
- **E-Mails nach der Verarbeitung vom Server löschen** - entfernt jede E-Mail aus dem Postfach, nachdem sie bearbeitet wurde. Lassen Sie dies aus, um das Postfach unverändert zu lassen.

OAuth2-Autorisierung (nur mit **IMAP + OAuth2 (Microsoft 365)**)

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

LDAP-Kontakte verwenden und **Debug E-Mail** funktionieren wie bei Email to SMS.

Bei POP3 und IMAP hat die Seite auch eine Schaltfläche **Verbindung testen**. Speichern Sie die Einstellungen, bevor Sie sie 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 ordnet jeder Funktion, die ausgehende E-Mails versendet, eine zu:

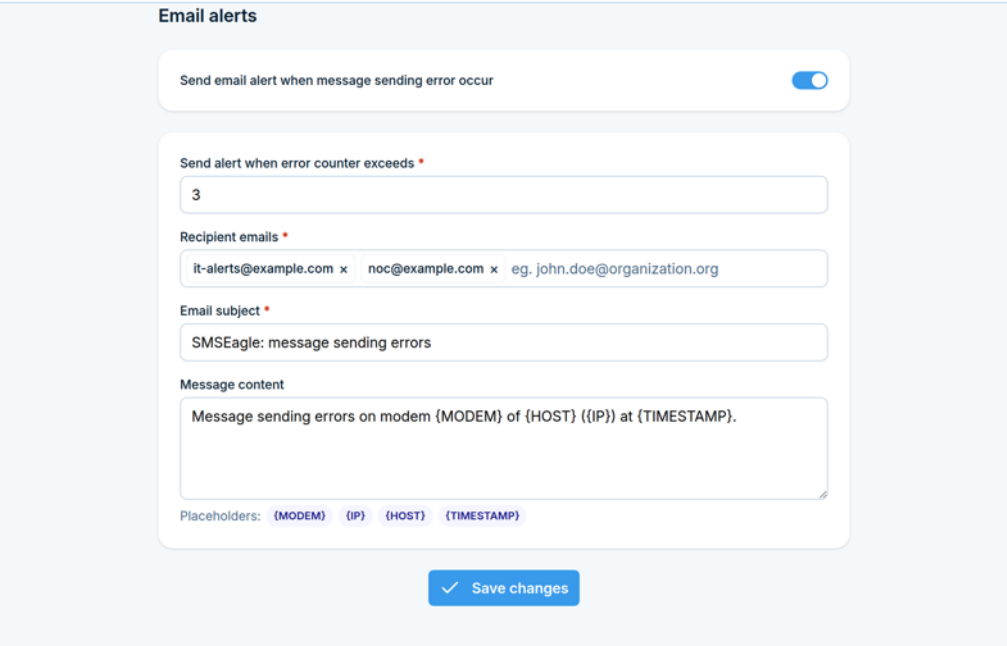
- **Compose menu**, **APIv2**, **SMS to Email**, **Alerts**, **Reporting module**, **Workflows**

Jede dieser Optionen kann auf **None** oder auf eine Ihrer gespeicherten Voreinstellungen gesetzt werden. Das Aufheben der Zuweisung einer Voreinstellung zu einer Funktion deaktiviert die vorhandene E-Mail-Einrichtung dieser Funktion.

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

E-Mail-Warnungen

Einstellungen > Kanäle > E-Mail > E-Mail-Warnungen (`/settings/email/alerts`) sendet eine Benachrichtigung per E-Mail, wenn ausgehende Nachrichten weiterhin nicht gesendet werden können. Es muss eine SMTP-Voreinstellung unter SMTP-Konfiguration zu **Alerts** zugewiesen sein.



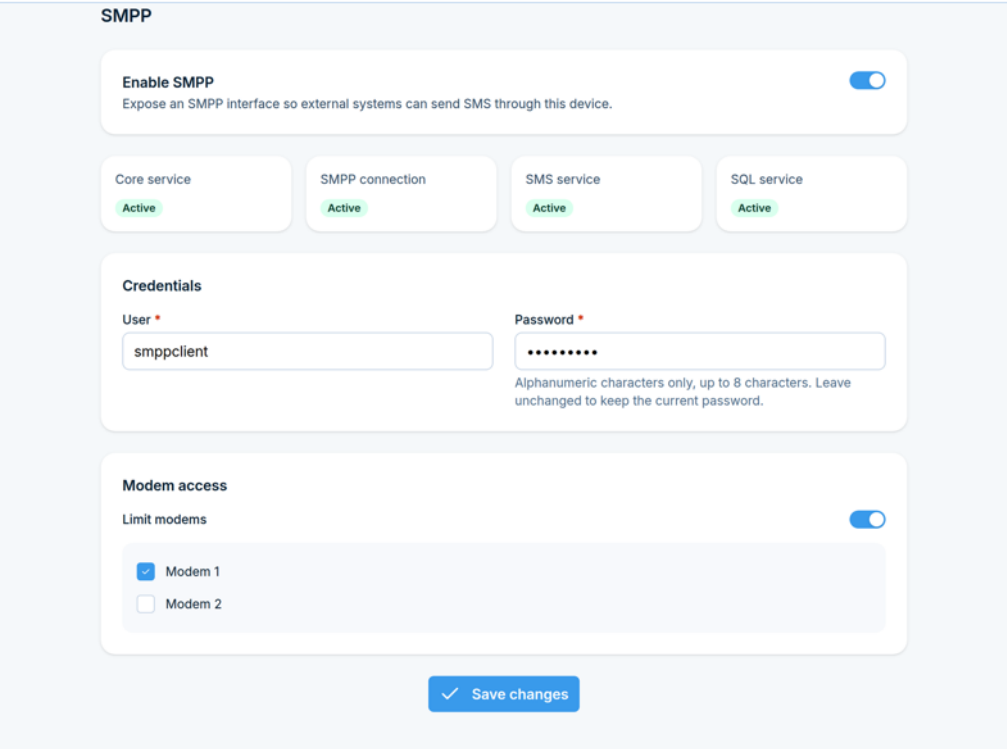
E-Mail-Warnungseinstellungen

Aktivieren Sie **Send email alert when message sending error occur**, dann setzen Sie:

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

SMPP

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



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 Zustellungsberichte

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

Eingehende SMS und Zustellungsberichte werden auf dem Gerät in eine Warteschlange eingereiht, während kein SMPP-Client verbunden ist. Sobald sich ein Client bindet, stellt SMSEagle alles in dieser Warteschlange bereit, daher muss der Client bereit sein, `deliver_sm`-Meldungen vom Moment der Bindung an zu empfangen und zu bestätigen.

SMPP einschalten

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

2. Legen Sie unter **Credentials** den **User** und **Password** fest, mit denen sich der SMPP-Client bindet. Das Passwort darf nur Buchstaben und Ziffern enthalten, maximal 8 Zeichen. Wenn bereits ein Passwort gespeichert ist, lassen Sie das Feld so, wie es ist, um es zu behalten.
3. Schalten Sie unter **Modem access** die Option **Limit modems** ein, um SMPP-Traffic nur über die angehakten Modems zu ermöglichen. Lassen Sie diese aus, um alle Modems zu erlauben.
4. Klicken Sie auf **Save changes**.

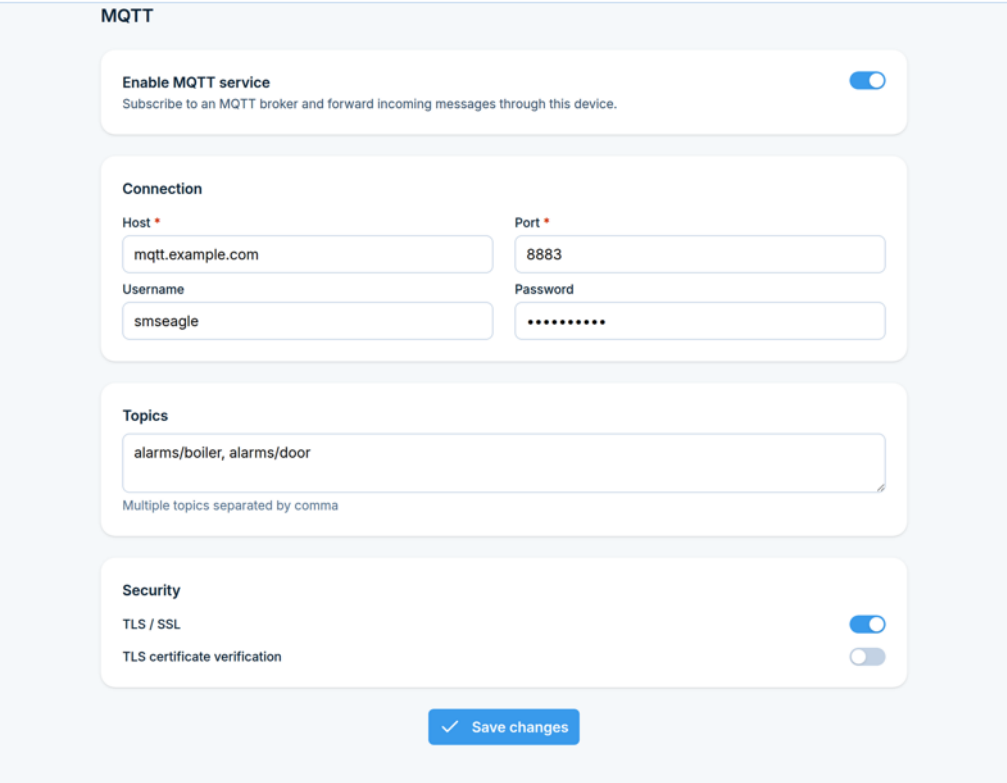
   Ein Neustart ist erforderlich. Nach dem Speichern fordert SMSEagle Sie auf, das Gerät neu zu starten, damit die SMPP-Änderungen wirksam werden. Bis dahin werden die neuen Einstellungen gespeichert, sind aber noch nicht in Gebrauch. Verwenden Sie **System > Restart**, wenn Sie bereit sind.

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

Beim ersten Aktivieren von SMPP erstellt SMSEagle auch einen internen Benutzer für SMPP-Traffic mit seinem eigenen API-Schlüssel, der unter **Settings > API v2 keys** aufgelistet ist, sowie die internen Regeln, die eingehende SMS und Zustellungsberichte an den SMPP-Client weiterleiten. Widerrufen oder bearbeiten Sie diese nicht. Das Ausschalten von SMPP entfernt den Benutzer und die Regeln wieder.

MQTT

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



MQTT-Broker-Verbindungseinstellungen

Schalten Sie **Enable MQTT service** ein und legen Sie fest:

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

Klicken Sie auf **Save changes**.

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

Netzwerk

IP-Einstellungen

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

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

- **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 sich die Regel bezieht. Wenn die Einschränkung aktiv ist, werden alle Ports außer 22 (SSH) für alle blockiert, die nicht auf der Liste stehen.

  Seien Sie vorsichtig mit IP address restriction. Eine falsch konfigurierte Zulassungsliste kann Sie aus dem Web-Interface auf Ihrem eigenen Computer aussperren. Fügen Sie zuerst Ihre aktuelle IP-Adresse hinzu (die Seite bietet eine **Add your IP address**-Verknüpfung), bevor Sie speichern.

SSL

Einstellungen > Globale Einstellungen > Netzwerk > SSL (`/settings/network/ssl`) ermöglicht es Ihnen, das selbstsignierte Standardzertifikat 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

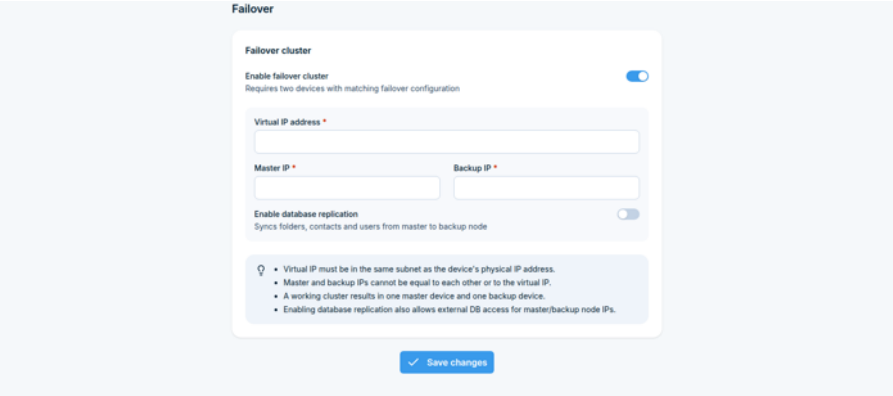
Der Failover-Cluster bietet Hochverfügbarkeit auf Geräteebene: Ein zweites SMSEagle-Gerät steht als Backup bereit und kann übernahmefähig werden, wenn das Master-Gerät nicht mehr reagiert. Dies unterscheidet sich vom modem failover, das zwischen zwei SIM-Karten im selben Gerät wechselt – ein Failover-Cluster schützt vor dem Ausfall des gesamten Geräts.

Wo Sie es 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 wird anhand seiner Adresse seiner Rolle zugeordnet: Das Gerät, dessen IP mit **Master IP** übereinstimmt, wird zum Master, das mit **Backup IP** übereinstimmende wird 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, sind aber noch nicht aktiv. Verwenden Sie **System > Restart**, wenn Sie bereit sind.

Master-/Backup-Rollen und virtuelle IP

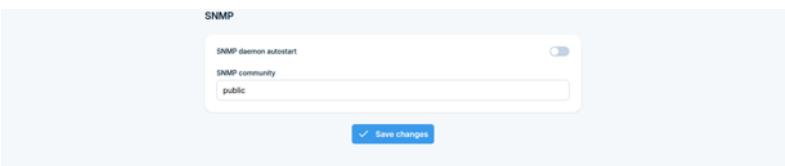
Der Cluster wird über eine einzelne **virtuelle IP-Adresse** erreicht, die immer auf das derzeit aktive Gerät verweist:

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

Datenbankreplikation und externer Zugriff

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

SNMP



SNMP-Agent-Einstellungen

Der SNMP-Agent ermöglicht es externen Tools (einem NMS, einem MIB-Browser oder einem einfachen `snmpget`/`snmpwalk`-Aufruf), SMSEagle nach seinen eigenen Metriken abzufragen - Signalstärke, Netzwerkname, Nachrichtenzählungen in Ordnern, System-Uptime und mehr. Dies ist

die entgegengesetzte Richtung zu SNMP Traps: Der Agent wird von einem externen Tool abgefragt, anstatt dass SMSEagle eine Warnung an einen sendet.

Wo Sie es finden

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

Konfiguration des SNMP-Agenten

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

Nach der Aktivierung können SMSEagles Erweiterungsparameter (Signalstärke, Netzwerkname, Ordnerzähler, Uptime und andere) mithilfe eines Standard-SNMP-Tools aus dem MIB-Baum des Geräts ausgelesen werden, z. B. NET-SNMP's `snmpget`/`snmpwalk` oder ein grafischer MIB-Browser.

Verfügbare Metriken

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

Metriken, die ein Modem beschreiben, enden mit der Modemnummer: 1 bis 8. 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.

Metrik	Gibt zurück
`GSM_Signal1`	Signalstärke des Modems in Prozent (0-100).
`GSM_NetName1`	Name des Mobilfunknetzes, in 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 eigene Status des Modems wie `SIM PIN` oder `SIM PUK` oder ein Fehler wie `NOSIM`.
`SIM_RegState1`	Netzregistrierung: `Registered Home`, `Registered Roaming`, `Searching`, `Not Registered`, `Denied`, `Registered Emergency`, `Unknown` oder `Unset`.
`SMSCountIn1`	Vom Modem heute seit Mitternacht empfangene SMS.
`SMSCountOut1`	Vom Modem heute seit Mitternacht gesendete SMS.
`FolderInbox_Total`	**Ungelesene** Nachrichten im Posteingang. Eine mehrteilige Nachricht zählt einmal.
`FolderOutbox_Total`	Nachrichten, die im Postausgang, der Sendewarteschlange, warten.
`FolderSent_Last24H`	In den letzten 24 Stunden gesendete Nachrichten. Jeder Teil einer mehrteiligen Nachricht zählt separat.
`FolderSent_Last1M`	Im letzten Monat gesendete Nachrichten, auf die gleiche Weise gezählt.
`FolderSent_Last24HSendErr`	Nachrichten, die in den letzten 24 Stunden nicht gesendet werden konnten, weil das Modem sie nicht senden konnte oder das Netz sie abgelehnt hat.

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

Die OID einer 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. Für ein anderes Modem ändert sich nur die letzte Zahl: Sie ist 48 plus die Modemnummer, daher endet `GSM_Signal2` mit `.50`.

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

Metriken auslesen

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

Eine Metrik nach OID auslesen:

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

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

Eine Metrik nach Name auslesen:

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

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

Alle SMSEagle-Metriken auf einmal auflisten:

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

Was aus dem Netzwerk ausgelesen werden kann

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

Dieselbe **SNMP-Community** gilt für beide. Nach einer Änderung starten Sie das Gerät neu, damit der neue Wert wirksam wird.

SNMP v3 verwenden

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

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

   ```
   cd /opt/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, sodass nur SNMP-v3-Benutzer den Agent auslesen können:

   ```
   ./snmpv3 disablev2
   ```

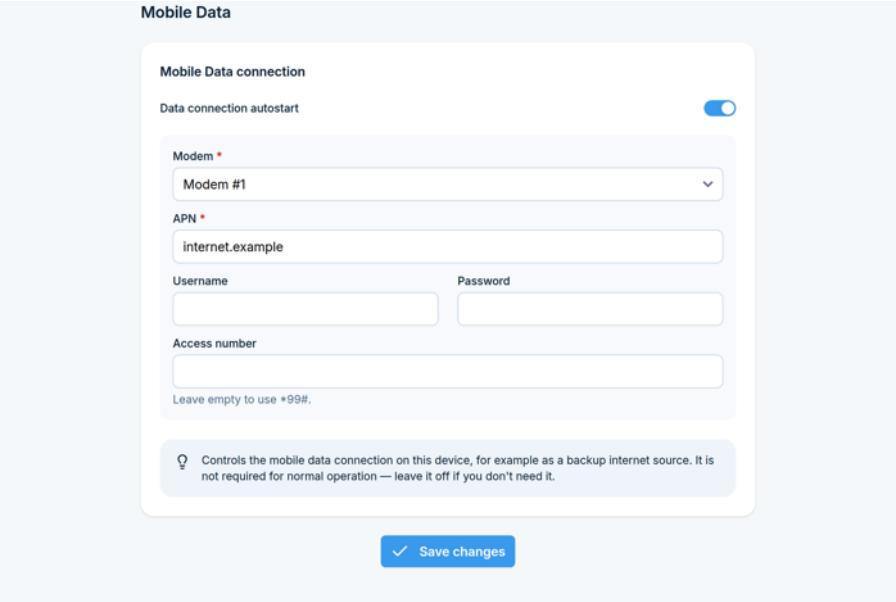
   `./snmpv3 enablev2` aktiviert es wieder, und `./snmpv3 del USERNAME` löscht den Benutzer.

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

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

Mobile Daten

Settings > Global settings > Network > Mobile Data (`/settings/network/mobile-data`) steuert eine Mobilfunkdatenverbindung über eines der Modems des Geräts, beispielsweise als Backup-Internetquelle. Dies ist nicht erforderlich zum Senden oder Empfangen von SMS. Deaktivieren Sie es, wenn Sie es nicht benötigen.



Mobilfunkdaten-Einstellungen

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

- **Modem** – das Modem, dessen SIM-Karte die Datenverbindung trägt.

- **APN** des SIM-Betreibers (erforderlich) sowie **Username** und **Password**, wenn der Betreiber diese verlangt.
- **Access number** – leer lassen, 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 Mobilfunkdaten-Änderungen wirksam werden. Bis dahin werden die neuen Einstellungen gespeichert, sind aber noch nicht aktiv. Verwenden Sie **System > Restart**, wenn Sie bereit sind.

Anwendung

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

Regionale Einstellungen

Language (geräteweiter Standard) und **Country dial code** (verwendet, wenn eine Telefonnummer ohne diesen eingegeben wird).

Sicherheit

- **Force MFA** - For all users, For new users oder Do not force (gleiche Auswirkung wie die geräteweite MFA-Einstellung des Assistenten, siehe MFA).
- **Password complexity verification** - Anforderung der Passwortregeln (Länge, Groß-/Kleinschreibung, Zahl, Sonderzeichen) für jeden Benutzer.
- **Access to DB for external applications** - aktiviert direkten PostgreSQL-Zugriff für externe Anwendungen, standardmäßig deaktiviert. Vollständige Verbindungsdetails und Beispiel-SQL werden separat in Advanced behandelt, da dies ein eigenständiges Thema für fortgeschrittene 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 in **System > Users** zugewiesen).
- **Email inbox content visibility** - For all users oder Only for admins.
- **Reporting-Modul verfügbar für** - Alle Benutzer oder Nur Administratoren.

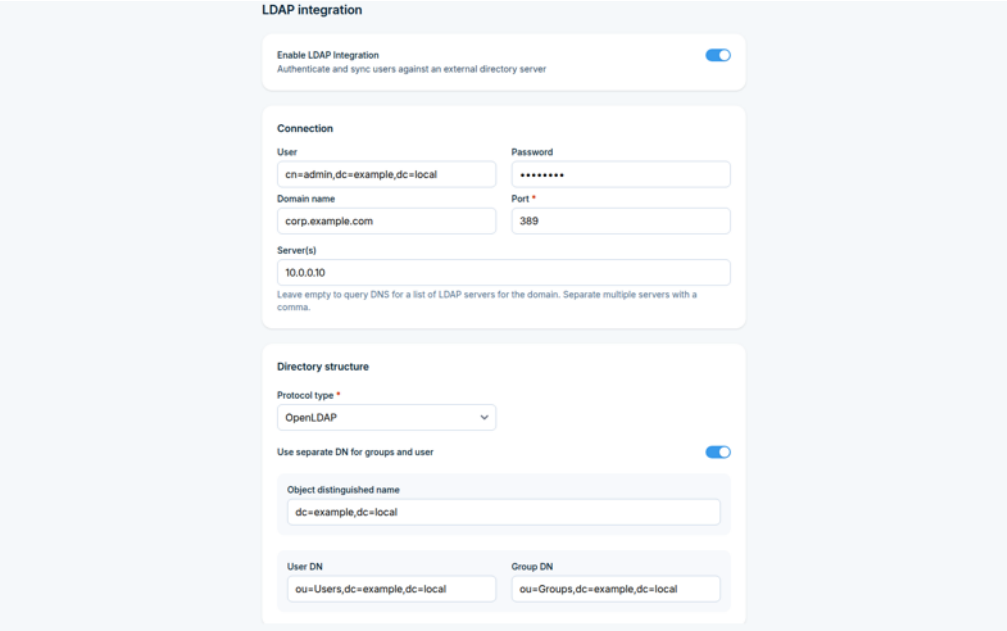
API und Integrationen

- **Save API logs** – protokolliert alle API v1 und v2 Aufrufe (Methode, Pfad und Parameter) in `/var/log/smseagle/api.log`. Zugriffstokens werden maskiert und Nachrichtentexte werden ausgelassen. Die Datei wird nicht im Logbrowser unter **System > Logs** angezeigt, aber

Download logs auf dieser Seite bezieht sie ein. Aktivieren Sie es beim Einrichten oder 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 versendet. 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, z. B. Active Directory oder OpenLDAP. Sie führt zwei separate Funktionen aus, und Sie können eine oder beide verwenden:

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

Typische Anwendungsfälle: Automatische Synchronisation des Telefonbuchs mit Personalveränderungen und Verwendung des vorhandenen Unternehmenspassworts statt eines separaten SMSEagle-Passworts.

Bevor Sie beginnen

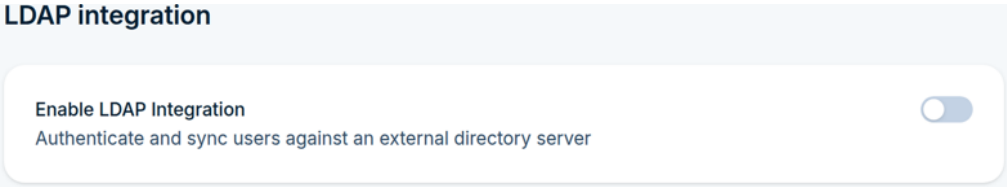
Sammeln Sie diese Informationen von der Person, die das Verzeichnis verwaltet:

- 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** des Branches mit Ihren Benutzern, zum Beispiel `ou=Users,dc=company,dc=local`, und der Branch mit Gruppen, falls dieser sich unterscheidet.
- Welches **Attribut** die Telefonnummer enthält, an die Sie Nachrichten senden möchten.
- Falls Sie die Verzeichnisanmeldung verwenden möchten: die Namen der Gruppen, deren Mitglieder SMSEagle-Administratoren und reguläre Benutzer werden sollen.

Schritt 1: LDAP-Seite öffnen

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

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



Mit deaktivierter Integration zeigt die Seite nur den Schalter an

Schritt 2: Integration aktivieren

Aktivieren Sie **Enable LDAP Integration**. Es erscheinen vier Abschnitte: **Connection**, **Directory structure**, **Attributes and security** und **Sync and access**.

Schritt 3: Connection

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



Verbindungsbereich, ausgefüllt mit Beispielwerten

Schritt 4: Verzeichnisstruktur

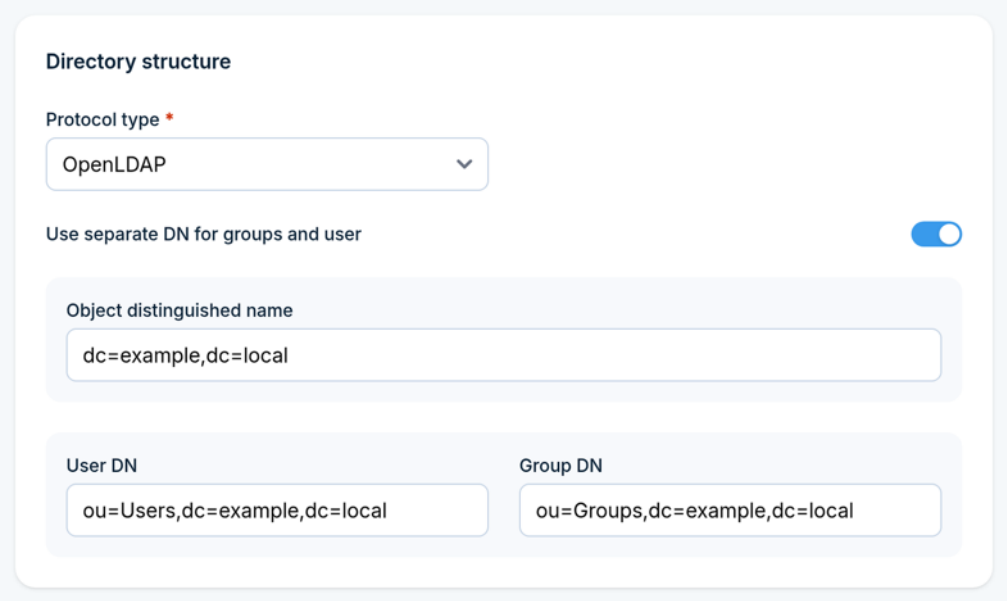
Protokolltyp Wählen Sie **Active Directory** oder **OpenLDAP**, je nach Ihrem Server.

Separate DN für Gruppen und Benutzer verwenden Lassen Sie dies deaktiviert, wenn sich Benutzer und Gruppen unter dem gleichen Branch befinden. Dann wird ein Feld angezeigt:

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

Aktivieren Sie dies, wenn sie sich in verschiedenen Branches befinden. **Objekt Distinguished Name** bleibt erhalten, und zwei weitere Felder werden darunter angezeigt:

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



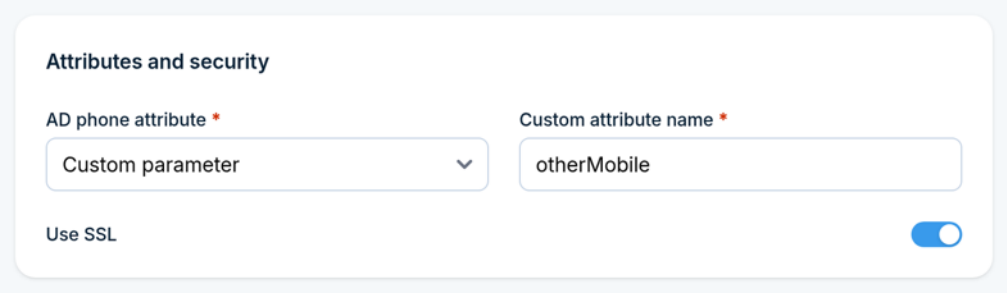
Verzeichnisstruktur mit aktivierten separaten DNs

Schritt 5: Attribute und Sicherheit

AD-Telefonattribut Welches Verzeichnisattribut enthält die Nummer, die SMSEagle texten soll: **Telefonnummer**, **Mobilnummer**, **Privatnummer**, **Pagernummer**, **Faxnummer**, **IP-Telefonnummer** oder **Benutzerdefinierter Parameter**.

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

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



:Benutzerdefinierter Parameter

ausgewählt und SSL aktiviert

Contacts and group fetch method

Option	Was geschieht
Fetch from LDAP server	Kontakte und Gruppen werden aus dem Verzeichnis jedes Mal 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, auf Kosten einer leicht veralteten Kopie.

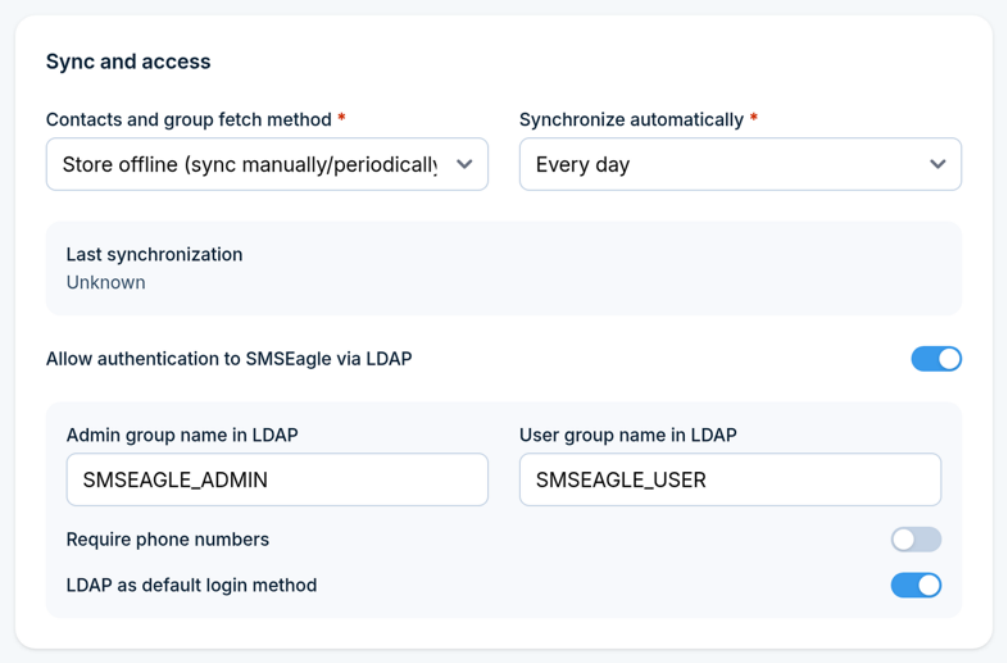
Wenn Sie **Offline speichern** gewählt haben, wird **Automatisch synchronisieren** angezeigt: **Nie**, **Jede Stunde**, **Täglich**, **Wöchentlich** oder **Monatlich**. **Nie** bedeutet, dass die Kopie nur aktualisiert wird, wenn Sie selbst eine Synchronisierung auslösen.

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

LDAP-Authentifizierung für SMSEagle ermöglichen Schalten Sie dies ein, um Benutzern die Anmeldung mit ihrem Verzeichniskonto zu ermöglichen. Es erscheinen vier weitere Felder:

- **Admin-Gruppenname 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, die eine Nummer im ausgewählten Telefon-Attribut haben, können sich anmelden. Standardmäßig deaktiviert.
- **LDAP als Standard-Anmeldeverfahren** – wählt LDAP statt Lokal im Authentifizierungstyp des Anmeldeformulars vor, sodass Verzeichnisbenutzer dies nicht jedes Mal ändern müssen.



Sync und Zugriff mit aktiviertem Offline-Speicher und Verzeichnis-Anmeldung

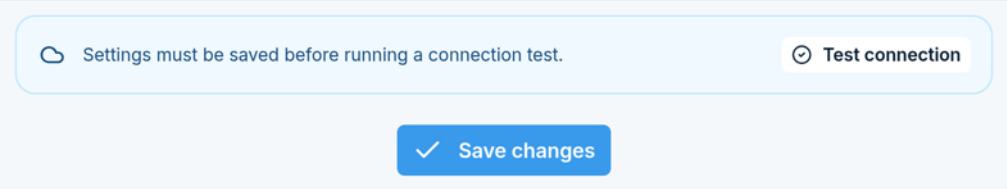
> **Überprüfen Sie die Gruppennamen, bevor Sie sich darauf verlassen.** Ein Mitglied keiner Gruppe kann sich nicht anmelden, und ein Tippfehler im Admin-Gruppennamen wird nur bemerkt, wenn niemand das Gerät verwalten kann. Halten Sie mindestens ein lokales SMSEagle-Administratorkonto funktionsfähig, bis Sie sich einer Verzeichnis-Anmeldung vergewissert haben.

Schritt 7: Speichern und testen

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

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

> **Erst speichern, dann testen.** Der Test verwendet die gespeicherten Einstellungen, nicht das, was derzeit auf dem Bildschirm angezeigt wird, daher wird vor dem Speichern getestet und die vorherige Konfiguration überprüft. Der Hinweis neben der Schaltfläche sagt das gleiche.



Das Test-Panel wiederholt die Regel: erst speichern, dann testen

Datum / Uhrzeit

Settings > Global settings > Date / Time (`/settings/datetime/`) zeigt das aktuelle Systemdatum und die aktuelle Systemzeit (schreibgeschützt) an und lässt Sie folgende Einstellungen vornehmen:

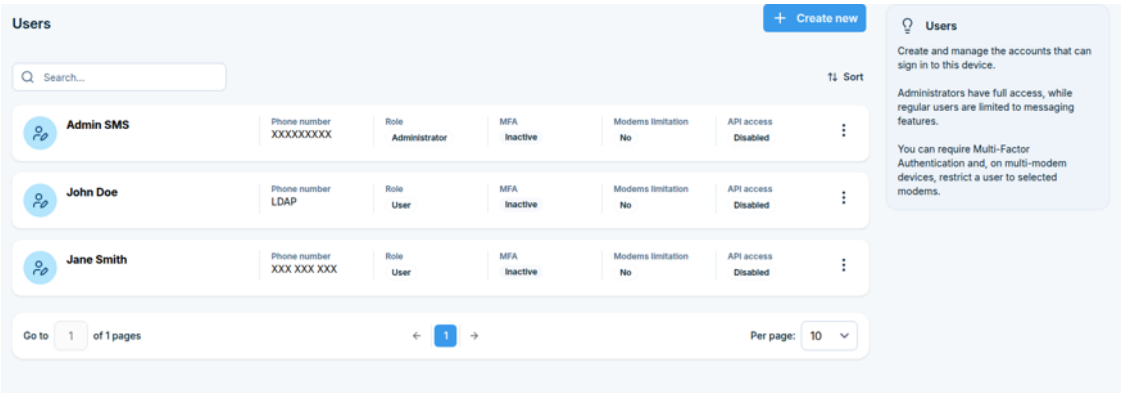
- **Zeitzone**
- **NTP-Zeitsynchronisierung** – wenn aktiviert, wird **NTP-Serveradresse** angezeigt. Wird auch während des Configuration Wizard angeboten.

System

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

Benutzer

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



Benutzer im Abschnitt „System

Für jeden Benutzer können Sie seine **Zugriffsebene** (Administrator oder Benutzer) festlegen, Multi-Faktor-Authentifizierung verlangen und auf Multi-Modem-Geräten einen Benutzer auf bestimmte Modems beschränken. Der API-Zugriff (siehe API und Entwicklerintegration) wird auch hier pro Benutzer gewährt.

Systeminformationen

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

- Gerätetyp, SMSEagle-Softwareversion, Seriennummer (MAC-Adresse), Modem-Softwareversion und Datenbankschema-Version
- **Speicherplatz**-Auslastung mit optionaler SMS-Benachrichtigung an den Master-Administrator, wenn die Auslastung einen von Ihnen festgelegten Schwellenwert überschreitet
- Details pro Modem: Signalstärke, Netzwerkname, SIM-Status und Registrierungsstatus, IMEI und SIM-Karten-IMSI

Protokolle

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

Updates

System > Updates (`/system/updates/`) zeigt die installierte Softwareversion an und ermöglicht es Ihnen, manuell oder automatisch auf Updates zu überprüfen. Sie können auch das Gerät so konfigurieren, dass der Administrator per SMS benachrichtigt wird, wenn eine neue Version verfügbar ist. Auf der gleichen Seite wird auch Ihre Gültigkeitsdauer des technischen Supports angezeigt und Sie können auch dies automatisch überprüfen.

Patches

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

Sicherung / Wiederherstellung

System > Sicherung / Wiederherstellung (`/system/backup/`) behandelt beide Richtungen:

- **Manuelle Sicherungen** - Erstellen Sie bei Bedarf eine Sicherung der Datenbank und der Geräteeinstellungen.
- **Automatische Sicherungen** - Aktivieren Sie zeitgesteuerte Sicherungen auf einem SFTP/FTP(S)-Server mit Cleanup alter Sicherungsversionen.
- **Daten wiederherstellen** - Stellen Sie die Datenbank aus einer Sicherungsdatei wieder her.

Neustart

System > Neustart (`/system/restart/`) startet das Gerät bei Bedarf neu – Senden und Empfangen sind nicht verfügbar, bis es wieder online ist – oder ermöglicht es Ihnen, einen zeitgesteuerten Neustart auf wiederkehrlicher Basis zu aktivieren.

Erweitert

Der direkte Datenbankzugriff und andere Themen für fortgeschrittene Benutzer haben ihr eigenes Kapitel: siehe Erweitert.

API und Entwicklerintegration

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

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 aus Gründen der Abwärtskompatibilität 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 diese als separate Dokumentation gepflegt. Folgen Sie den obigen Links für die vollständige Spezifikation jeder API.

API-Schlüssel

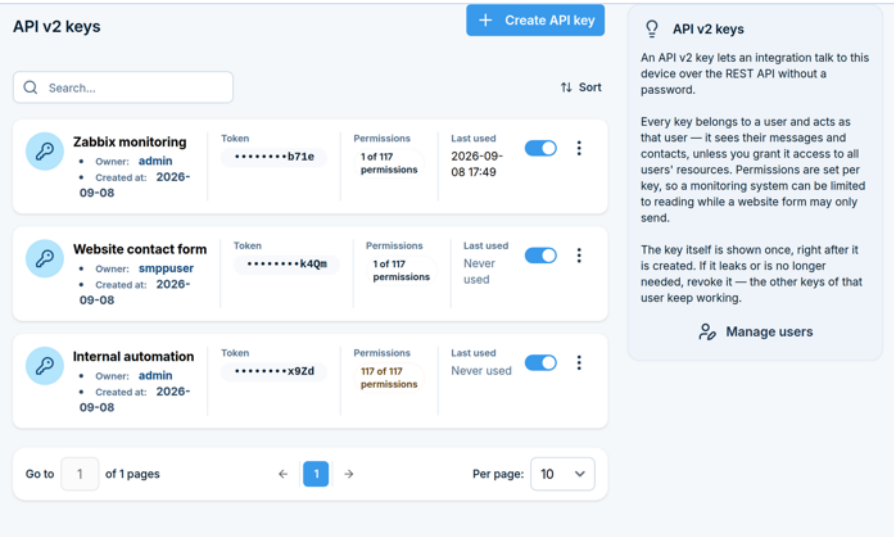
Eine Integration authentifiziert sich mit einem **API-Schlüssel** statt mit einem Benutzerkennwort. Schlüssel werden für jede API-Version separat auf zwei Seiten gespeichert:

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

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

API v2-Schlüssel

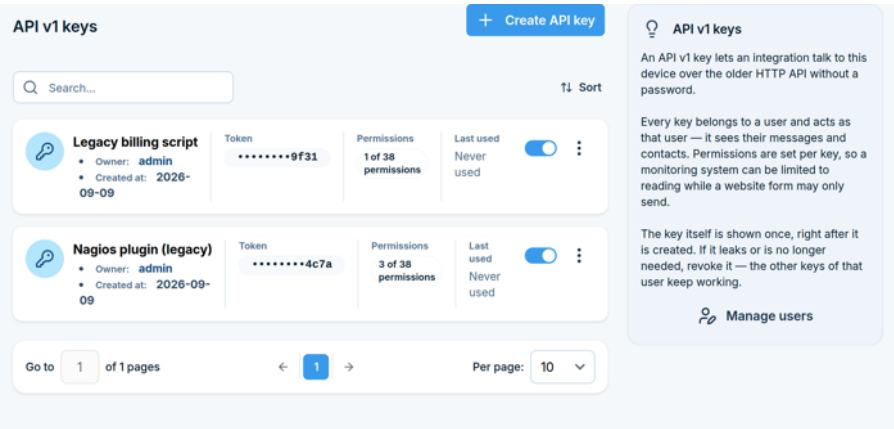
Dies ist die Seite für eine neue Integration.



API v2-Schlüssel

API v1-Schlüssel

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



API v1-Schlüssel

Erstellen eines Schlüssels

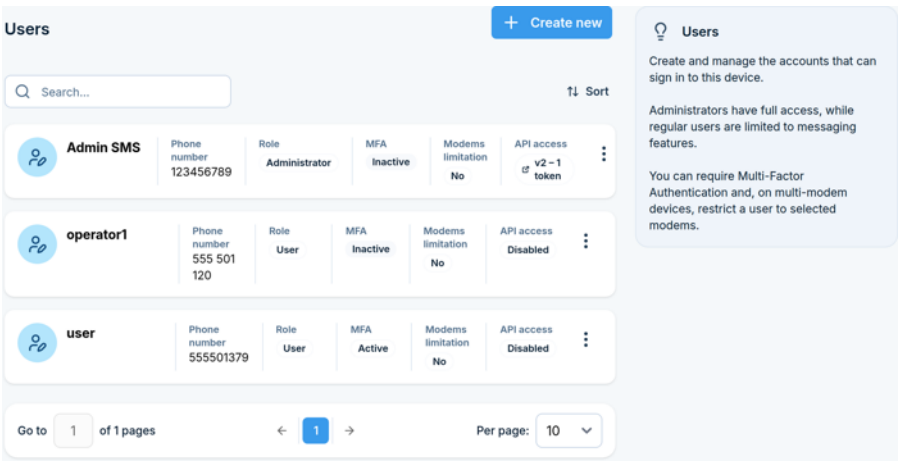
Create API key öffnet das Formular für die API-Version, auf deren Seite Sie sich befinden:

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

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

Welche Benutzer haben API-Zugriff

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



API-Zugriff, angezeigt pro Benutzer in der Benutzerliste

Zugriff auf Ressourcen anderer Benutzer

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

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

Plugins und Integrationen

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

- **API** – das externe System sendet und empfängt Nachrichten über die SMSEagle REST API. Dies ist die flexibelste Methode und bietet Zugriff auf alle Gerätefunktionen. Siehe API und Entwicklerintegration.
- **Email zu SMS** – das externe System sendet eine reguläre E-Mail und SMSEagle konvertiert sie in eine SMS. Es ist keine Programmierung erforderlich, daher funktioniert es mit jeder Software, die bereits E-Mail-Benachrichtigungen versenden kann. Siehe Email zu SMS.

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

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

Erweitert

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

Direkte Verbindung zur SMSEagle-Datenbank

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

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

Nachdem Sie ihn aktiviert haben, verbinden Sie sich von einer externen Anwendung aus mit der Datenbank, indem Sie Folgendes verwenden:

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

Einfügen einer kurzen SMS über SQL

Eine kurze Textnachricht (bis zu 160 Zeichen):

```
INSERT INTO outbox (
    DestinationNumber,
    TextDecoded,
    CreatorID,
    Coding,
    Class,
    SenderID
) VALUES (
    '1234567',
    'This is a SQL test message',
    'Program',
    'Default_No_Compression',
    -1,
    'smseagle1'
);
INSERT INTO user_outbox (
    id_outbox,
    id_user
) SELECT CURRVAL(pg_get_serial_sequence('outbox','ID')), 1;
```

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

Einfügen einer langen SMS über SQL

Mehrteilige Nachrichten benötigen auch einen UDH-Header, der als Hexadezimal-String im Feld `UDH` gespeichert ist. Sofern Sie keinen speziellen Grund haben, dies manuell zu tun, verwenden Sie stattdessen die API (siehe API and Developer Integration).

Bei einer langen Textnachricht beginnt der UDH mit `050003`, gefolgt von einem Byte als Nachrichtenreferenz (ein beliebiger Hexadezimalwert, aber unterschiedlich für jede Nachricht – `D3` unten), einem Byte für die Gesamtzahl der Teile (`02` unten, eindeutig pro Nachricht, die an die gleiche Nummer versendet wird), und einem Byte für die Nummer des aktuellen Teils (`01` für den ersten Teil, `02` für den zweiten usw.).

Eine zweiteilige lange Nachricht 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

Es stehen mehrere Skripte zum Löschen von SMS-Nachrichten aus der Datenbank über die Linux CLI zur Verfügung, die sich unter `/mnt/nand-user/scripts/` befinden:

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

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

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

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

Weitergabe von Protokollen an einen externen Server

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

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

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

   - `target` - IP-Adresse oder Hostname des Syslog-Servers.

- `port` - Port, auf dem der Server lauscht, normalerweise `514`.
- `protocol` - `udp` oder `tcp`.
- Die Warteschlangeneinstellungen halten bis zu 10000 Nachrichten auf dem Gerät, während der Server nicht erreichbar ist, und senden sie, sobald er wieder verfügbar ist.

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

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

Behalten Sie den Dateinamen bei. Die eigenen Protokolle von SMSEagle (Application, API, Message und die E-Mail-, Call-, Signal- und WhatsApp-Dienste) 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, zum Beispiel am Ende von `/etc/rsyslog.conf`, leitet nur die Systemprotokolle weiter. Das Präfix `005-` bewirkt, dass rsyslog die Weiterleitungsregel zuerst liest, sodass jede Nachricht weitergeleitet wird.

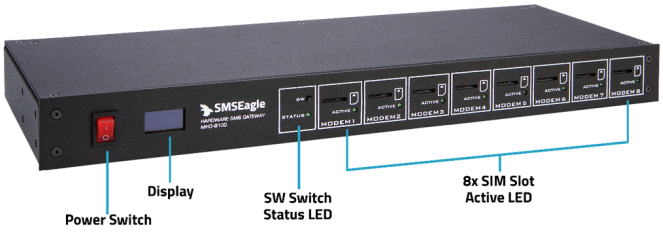
Um den Protokolldatenverkehr mit TLS zu verschlüsseln, siehe das rsyslog-Handbuch Encrypting Syslog Traffic with TLS.

Fehlerbehebung

Führen Sie die folgenden drei Schritte durch, um sicherzustellen, dass das Gerät ordnungsgemäß funktioniert:

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

Überprüfung der LEDs



Front Panel LEDs

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

LED	Korrekter Betrieb
Power (Tastaturlicht)	Dauerhaft leuchtend
STATUS	Blinkend
ACTIVE1-8	Langsames Blinken im Standby-Modus, schnelles Blinken, wenn das entsprechende Modem in Verwendung ist

Überprüfung der Geräteinformationen

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

Gerätelogs

Unter **System > Logs** finden Sie die neuesten Zeilen der Gerätelogs: Modem-Log, Datenbank-Log und Systemlog. Im Falle von Problemen mit dem Gerät sind diese Logs eine wertvolle Quelle für Fehlerbehebungsinformationen.

Erweiterte Gerätelogs 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 ordnungsgemäß mit dem Netzwerk verbunden ist. Überprüfen Sie den LED-Status der RJ45-Buchse.
2. Wenn das Gerät aufgrund einer Fehlfunktion oder falscher Benutzereinstellungen nicht antwortet, starten Sie das Gerät mit dem Netzschalter (oder dem RESET-Schalter auf der Rückseite) neu.
3. Wenn Sie immer noch keine Verbindung zum Gerät herstellen können, können Sie die Werks-IP-Einstellungen mit der SW-Taste wiederherstellen.

Wiederherstellen der Werkseinstellungen

Die Funktion „Auf Standardeinstellungen zurücksetzen“ ermöglicht es Ihnen, das Gerät schnell auf seine ursprüngliche Werkskonfiguration zurückzusetzen.

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

Das Wiederherstellen der Werkseinstellungen setzt die folgenden Werte auf ihre Standardwerte zurück: **IP-Einstellungen, Zeitzonen-Einstellungen, Datenbankinhalt und Linux OS-Benutzer/ Passwörter.**

Um den Reset zu initiieren:

1. **Wenn das Gerät betriebsbereit ist** (STATUS-LED blinkt), halten Sie die **SW**-Taste 10 Sekunden lang gedrückt.
2. Geben Sie die SW-Taste nach 10 Sekunden frei – das Display zeigt **„Factory reset“** an.
3. Warten Sie, bis das System neu startet. Die Standardeinstellungen werden wiederhergestellt.

Hinweis: Nach dem Neustart wird der Werksreset vom Gerät immer noch durchgeführt, daher kann das System länger als gewöhnlich zum Starten benötigen.

Service & Reparatur

Garantie

Ihr SMSEagle wird mit standardmäßiger 2-jähriger technischer Unterstützung und Hardwarereparatur-Garantieabdeckung geliefert. Die Standardgarantie kann während des Gerätekaufs auf 3 Jahre erweitert werden (siehe Ihre Kaufbedingungen). Ausführliche Informationen zu Garantiebedingungen finden Sie auf der Garantiekarte, die Ihrem Gerät beiliegt, oder folgen Sie dem Link: www.smseagle.eu/downloads

Service

Bevor Sie das Support-Team kontaktieren, stellen Sie bitte sicher, dass Sie den Abschnitt „Fehlerbehebung“ dieses Handbuchs gelesen haben. Weitere Informationen und nützliche 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-Dienst wird bereitgestellt von: Proximus Sp. z o.o. ul. Piątkowska 163, 60-650 Poznan, Polen

Bereiten Sie sich darauf vor, dem Support-Team die folgenden Informationen zu geben:

Systemprotokolle

Gehen Sie zu **System > Logs > Download logs**. Stellen Sie das Protokollpaket dem Support-Team zur Verfügung, wenn es angefordert wird.

MAC-Adresse

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

Technische Daten und Sicherheitsinformationen

Technische Spezifikation

Hardwarespezifikation

- Prozessortyp: Intel(R) Celeron(R) CPU N3350
- Arbeitsspeicher (RAM): 2GB DDR4
- 32GB eMMC-Speicher
- Netzwerkschnittstelle: Gigabit Ethernet 10/100/1000 TX (2xRJ45)
- HDMI+DP (nur zu Debugging-Zwecken)
- Weitere externe Anschlüsse: 2x USB 3.0
- Stromverbrauch: max. 40W
- Geräuschpegel: Lüfterlos
- Abmessungen: (Breite x Tiefe x Höhe) 44 × 15,5 × 4,5 cm
- Gewicht: 1,8 kg
- Gehäuse: Metall (Rack-Mount)
- Betriebsparameter:
    - Betriebstemperatur: 32-140°F / 0~60°C
    - Luftfeuchtigkeit: 0%~90%RH (nicht kondensierend)
- 8x Internes Modem

Device type MHD-8100-3G

- Frequenzband: 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

Device type MHD-8100-4G

- Frequenzbänder: UMTS, LTE
- LTE FDD: B1/B2/B3/B4/B5/B7/B8/B12/B13/B18/B19/B20/B25/B26/B28

- LTE TDD: B38/B39/B40/B41
- UMTS: B1/B2/B4/B5/B6/B8/B19
- Ausgangsleistung (Nennwert):
    - Klasse 3 (24dBm+1/-3dB) für WCDMA-Bänder
    - Klasse 3 (23dBm±2dB) für LTE-FDD-Bänder
    - Klasse 3 (23dBm±3dB) für LTE-TDD-Bänder
- SIM-Kartennorm: mini
- Antennenanschluss: 8x SMA
- Herkunftsland: Europäische Union (Polen)

Stromversorgung

AC-Netzeingang

Spannungsbereiche: 100-240V Wechselstrom (AC)

Frequenz: 50-60Hz einphasig

AC-Steckertyp: IEC13 (AC-Buchsentyp: IEC14)

Antenne

- Omnidirektional max. 2dBi
- Frequenzbänder: UMTS, LTE
- Steckertyp: SMA
- Impedanz: 50 Ohm

Durchsatz beim Senden/Empfangen

- Eingangsübertragungsrate: bis zu 8× 30 SMS/min
- Ausgangsübertragungsrate: bis zu 8× 30 SMS/min

Softwareplattform

- Betriebssystem:
    - device Rev.1.1: Ubuntu 22.04
    - device Rev.1: Ubuntu 18.04
- integrierter Apache2-Webserver
- integrierter PostgreSQL-Datenbankserver
- integrierter Postfix-E-Mail-Server
- integrierter SNMP-Agent
- integrierter NTP-Client

- integrierter Failover (HA-Cluster)-Dienst
- Watchdog-Mechanismus für integrierte Modems
- Failover-Mechanismus für integrierte Modems
- modernes responsives Web-Interface
- Liste der offenen TCP/UDP-Ports in der Standardkonfiguration:
    - TCP: 22 (SSH), 80 (HTTP), 443 (HTTPS), 5432 (Postgresql mit Zugriffsbeschränkung auf localhost nur)
    - UDP: 68 (DHCP-Client), 323 (NTP-Client)

Wichtige Sicherheitsinformationen

Dieses Kapitel bietet wichtige Informationen zu Sicherheitsverfahren. Befolgen Sie diese Regeln für den Umgang mit Ihrem Gerät zu Ihrer Sicherheit und zum Schutz Ihrer Ausrüstung.

> **Warnung**
>
> Unsachgemäße Lagerung oder Verwendung Ihres Geräts kann die Herstellergarantie ungültig machen. Die Nichtbeachtung dieser Sicherheitsanweisungen kann zu Brand, elektrischem Schlag oder anderen Verletzungen oder Beschädigungen führen.

Treffen Sie immer die folgenden Vorsichtsmaßnahmen.

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

- das Stromkabel oder der Stecker wird ausgefranst oder anderweitig beschädigt
- Sie verschütten etwas in das Gehäuse
- das Gerät wird Regen oder übermäßiger Feuchtigkeit ausgesetzt
- das Gerät ist heruntergefallen oder das Gehäuse wurde 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 Krankenhäusern, Flughäfen, Flugzeugen usw.; wo es Explosionsrisiko gibt, wie an Tankstellen, Ölraffinerien usw.

Es ist Aufgabe des Benutzers, die Landesvorschriften und die spezifischen Umweltvorschriften 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 einem Mindestabstand von 23 cm zum Körper installiert werden. Falls diese Anforderung nicht erfüllt werden kann, muss der Systemintegrator das Endprodukt gegen die SAR-Richtlinie bewerten.

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

Behördliche Erklärungen

EU-Konformitätserklärung

Hiermit erklärt Proximus Sp. z o.o., Eigentümer der Marke SMSEagle, dass die Funkgerätetypen SMSEagle MHD-8100-4G, MHD-8100-3G der Richtlinie 2014/53/EU entsprechen.

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

FCC-Konformitätserklärung

Dieses Gerät entspricht Teil 15 der FCC-Vorschriften. Der Betrieb unterliegt den folgenden zwei Bedingungen:

(1) Dieses Gerät darf keine schädlichen Störungen verursachen, und

(2) dieses Gerät muss alle empfangenen Störungen akzeptieren, einschließlich Störungen, die zu unerwünschtem Betrieb führen können.

Hinweis:

Dieses Gerät wurde getestet und erfüllt die Grenzwerte für ein Gerät der Klasse B gemäß Teil 15 der FCC-Vorschriften. Diese Grenzwerte wurden entwickelt, um angemessenen Schutz vor schädlichen Störungen in einer geschäftlichen/kommerziellen Nicht-Wohnumgebung zu bieten. Es gibt jedoch keine Garantie, dass Störungen bei einer bestimmten Installation nicht auftreten. Wenn dieses Gerät Störungen bei Radio- oder Fernsehempfang verursacht, was durch Aus- und Einschalten des Geräts festgestellt werden kann, wird der Benutzer ermutigt, zu versuchen, die Störung durch eine oder mehrere der folgenden Maßnahmen zu beheben:

- Neuausrichtung oder Umplatzierung der Empfangsantenne
- Vergrößerung des Abstands zwischen dem Gerät und dem Empfänger
- Anschluss des Geräts an eine Steckdose in einem anderen Stromkreis als dem des Empfängers
- Konsultation des Händlers oder eines erfahrenen Radio-/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, schädliche Störungen bei Radiokommunikationen verursachen. Der Betrieb dieses Geräts in einem Wohngebiet kann zu schädlichen Störungen führen, in welchem Fall Sie verpflichtet sind, die Störung auf Ihre eigenen Kosten zu beheben. Die FCC-Vorschriften sehen vor, dass Änderungen oder Modifizierungen, die nicht ausdrücklich von SMSEagle™ genehmigt wurden, Ihre Betriebserlaubnis für dieses Gerät ungültig machen können. Dieses Produkt hat EMC-Konformität

unter Bedingungen nachgewiesen, die die Verwendung von konformen Peripheriegeräten (Antennen) und abgeschirmten Kabeln zwischen Systemkomponenten einschlossen. Es ist wichtig, dass Sie konforme Peripheriegeräte und abgeschirmte Kabel zwischen Systemkomponenten verwenden, um die Möglichkeit von Störungen bei Radios, Fernsehgeräten und anderen elektronischen Geräten zu verringern.

FCC-Konformitätserklärung des Lieferanten

Diese Konformitätserklärung des Lieferanten wird hiermit gemäß Kapitel 1, Unterabschnitt A, Teil 2 von Titel 47 des Code of Federal Regulations ausgestellt von:

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

Das Produkt MHD-8100-4G entspricht den geltenden Anforderungen der FCC-Regelung Teil 15B für die entsprechenden Geräteklassen von unbeabsichtigten Strahlern.

VERANTWORTLICHE PARTEI in den Vereinigten Staaten:

Testing Partners LLC

18200 SR 306

Chagrin Falls, OH 44023

info@testingpartners.com

Die verantwortliche Partei garantiert, dass jede unter dieser Konformitätserklärung vermarktete Geräteeinheit mit dem getesteten Gerät identisch ist und als mit den Standards konform befunden wurde, und dass die von der verantwortlichen Partei geführten Aufzeichnungen weiterhin widerspiegeln, dass die unter dieser Konformitätserklärung des Lieferanten hergestellten Geräte weiterhin den Anforderungen entsprechen, wobei die Abweichung berücksichtigt wird, die durch Massenproduktion und statistische Prüfung zu erwarten ist.

Kanadische behördliche Erklärung (ISED)

Dieses Gerät entspricht den lizenzbefreiten RSS-Standards der kanadischen Behörde ISED. Der Betrieb unterliegt den folgenden zwei Bedingungen:

(1) dieses Gerät darf keine Störungen verursachen, und

(2) dieses Gerät muss alle Störungen akzeptieren, einschließlich Störungen, die zu unerwünschtem Betrieb des Geräts führen können.

Dieses digitale Gerät der Klasse B erfüllt die Anforderungen der kanadischen Interference-Causing Equipment Regulations.

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

Avis de conformité à la réglementation d'Industrie Canada

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

(1) l'appareil ne doit pas produire de brouillage,

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

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

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

UK Declaration of Conformity

Hiermit erklärt Proximus Sp. z o.o., Eigentümer der Marke SMSEagle, dass der Funkgerätetyp SMSEagle MHD-8100-4G, MHD-8100-3G die Anforderungen der Radio Equipment Regulations 2017 erfüllt.

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

Grenzwerte für die HF-Exposition

Dieses Gerät erfüllt die Grenzwerte für die Strahlenexposition in einer unkontrollierten Umgebung. Um die Möglichkeit einer Überschreitung der Grenzwerte für die Hochfrequenzexposition zu vermeiden, darf die menschliche Nähe zur Antenne während des normalen Betriebs nicht weniger als 23 cm (9 Zoll) betragen.

Entsorgung und Recycling-Informationen

Ihr SMSEagle-Gerät enthält eine Lithiumbatterie für die RTC-Sicherung. Entsorgen Sie das Gerät und/oder die Batterie gemäß den örtlichen Umweltgesetzen und -richtlinien.

Europäische Union – Entsorgungsinformationen



Das oben angegebene Symbol bedeutet, dass Ihr Produkt gemäß den örtlichen Gesetzen und Vorschriften getrennt vom Haushaltsmüll entsorgt werden muss. Wenn dieses Produkt das Ende seiner Lebensdauer erreicht, bringen Sie es zu einer von den örtlichen Behörden angegebenen

Sammelstelle. Die separate Sammlung und das Recycling Ihres Produkts zum Zeitpunkt der Entsorgung trägt zur Schonung natürlicher Ressourcen bei und sorgt dafür, dass es auf eine Weise recycelt wird, die die menschliche Gesundheit und die Umwelt schützt.

Entsorgung in Ländern außerhalb der Europäischen Union

Dieses Symbol gilt nur in der Europäischen Union (EU). Falls Sie dieses Produkt entsorgen möchten, wenden Sie sich bitte an Ihre örtlichen Behörden oder Ihren Händler und fragen Sie nach der korrekten Entsorgungsmethode.

Information gemäß § 4 Absatz 4 Elektrogesetz (DE)

Folgende Batterien bzw. Akkumulatoren sind in diesem Elektrogerät enthalten

Hardware	Batterietyp	Chemisches System
Rev.1 Rev.1.1	CR2032	Lithium

Angaben zur sicheren Entnahme der Batterien oder der Akkumulatoren

Öffnen Sie die obere Abdeckung des Geräts. Die Batterie der Echtzeituhr (RTC) befindet sich in der Nähe der Rückseite des Geräts. Trennen Sie den 2-poligen PicoBlade-Stecker (rotes und schwarzes Kabel) von der Hauptplatine und entnehmen Sie anschließend die Batterie aus dem Gerät. Die Batterie und das Gerät können anschließend getrennt entsorgt werden.

Restriction of Hazardous Substances Directive (RoHS)

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“).