EINFÜHRUNG

GPS-Tracker liefern wertvolle Daten für die Geschäftseffizienz und schützen Fahrzeuge vor Diebstahl. Gleichzeitig können Tracker zum Verkauf gestohlen, sabotiert werden, indem sie mit fehlerhaften Parametern neu konfiguriert werden, oder gehackt werden, um sensible Daten zu stehlen. Um einen unbefugten Zugriff auf die Tracker zu verhindern, sind zusätzliche Sicherheitsmaßnahmen für die Anmeldung über alle möglichen Geräte erforderlich. Wenn eine Anmeldung fehlschlägt, wird dem Benutzer der Zugriff verweigert und die Tracker bleiben sicher.

HERAUSFORDERUNG

Fahrzeug-Tracker speichern **vertrauliche** Geschäftsdaten und helfen dank verschiedener Funktionen dabei, optimale Routen zu planen, um Verzögerungen zu vermeiden, den Kraftstoffverbrauch zu senken, rechtzeitige Wartung zu erhalten und die Ladung mit einem Fahrzeug zu sichern. Wenn ein Unternehmen seinen Tracker oder die Kontrolle darüber verliert, verliert es die Möglichkeit, ein Fahrzeug zu überwachen, was schwerwiegende Folgen haben kann.

Der Diebstahl eines Trackers oder die Übernahme seiner Kontrolle kann sowohl für große als auch für kleine Unternehmen große Probleme verursachen. Sie können jedoch viel tun, um **die Sicherheit** Ihrer Tracker zu verbessern. Obwohl es keine absoluten Garantien gibt, sollten Sie es den Dieben so schwer wie möglich machen, die Tracker zu überholen, in deren Installation und Konfiguration Sie viel Zeit investiert haben, um eine effiziente Datenerfassung und -überwachung zu gewährleisten. Andernfalls bedeutet der Verlust eines Trackers auch den Verlust Ihres Einkommens.

Unsere Tracking-Lösungen bieten viel mehr als nur einfaches Tracking. Es steht eine breite Palette an Funktionalitäten zur Verfügung und – was am wichtigsten ist – wir bieten **sichere Konnektivität** für alle unsere Geräte.

LÖSUNG

Das Einrichten eines Passworts, einer PIN oder eines Schlüsselworts vor der Verwendung des Trackers ist ein Muss. Einen Tracker sofort zu installieren, ohne ihn aus Sicherheitsgründen neu zu konfigurieren, ist einer der häufigsten Fehler, die Integratoren machen. Dies lässt sich jedoch leicht beheben, indem **sichere Passwörter** erstellt werden (mindestens 8 Zeichen: eine Mischung aus Groß- und Kleinbuchstaben, Zahlen und mindestens einem Sonderzeichen). Wenn diese Änderungen nicht vorgenommen werden, ist es für Diebe einfacher, Zugriff auf die

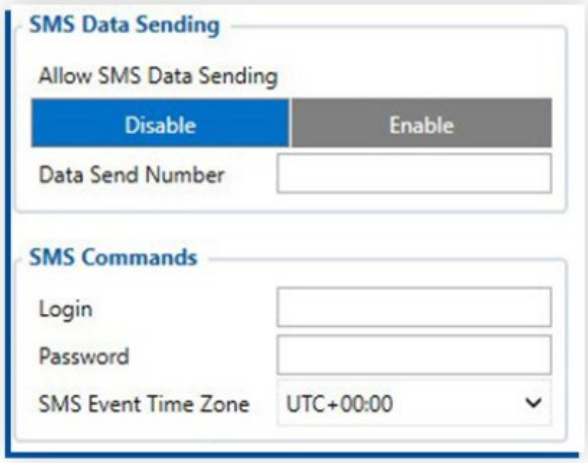
Tracker zu erhalten, da sie möglicherweise die ursprünglichen Einstellungen kennen oder herausfinden.
Mit den Teltonika-Optionen für sichere Verbindungen wird es schwierig, die Tracker zu stehlen oder zu sabotieren. Alle Ortungsgeräte von Teltonika unterstützen die unten aufgeführten Sicherheitsmaßnahmen, einschließlich FMB130 , das eine perfekte Wahl für verschiedene Einsatzszenarien ist.

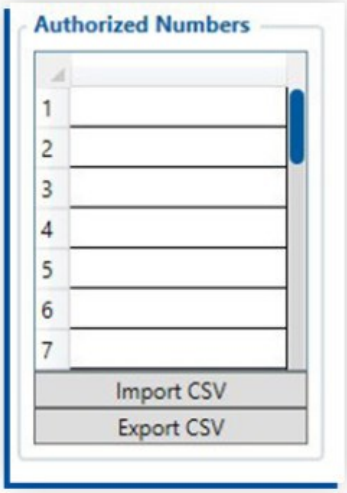
KONFIGURATOR-SCHLÜSSELWORT

Der Zugriff auf den Konfigurator sollte nur denjenigen vorbehalten sein, die ihn nutzen müssen. Damit Mitarbeiter des Unternehmens Tracker über den Computer konfigurieren können, ist bei der Verbindung über USB ein Schlüsselwort erforderlich. Beim Zugriff auf die Tracker-Konfiguration über eine Bluetooth®-Verbindung wird neben einem Schlüsselwort auch eine PIN zum Koppeln mit dem Gerät verwendet.

SMS-SICHERHEIT

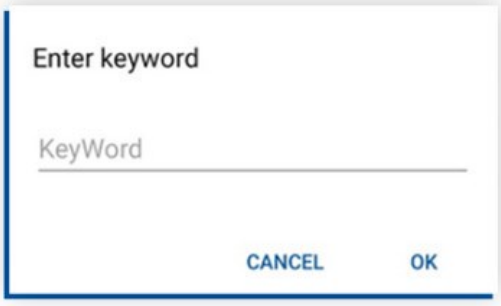
Sie können SMS-Login und SMS-Passwort verwenden, um auf Teltonika-Tracker zuzugreifen. Darüber hinaus ist es auch möglich, Geräte über SMS-Befehle zu konfigurieren.
Für eine zusätzliche Sicherheit per SMS können Sie im Teltonika-Konfigurator Telefonnummern zur Liste der autorisierten Nummern hinzufügen. Die Tracker ignorieren alle Befehle von Nummern, die nicht im Konfigurator aufgeführt sind, sodass niemand sonst die Geräte konfigurieren oder sabotieren kann.





FMBT-APP

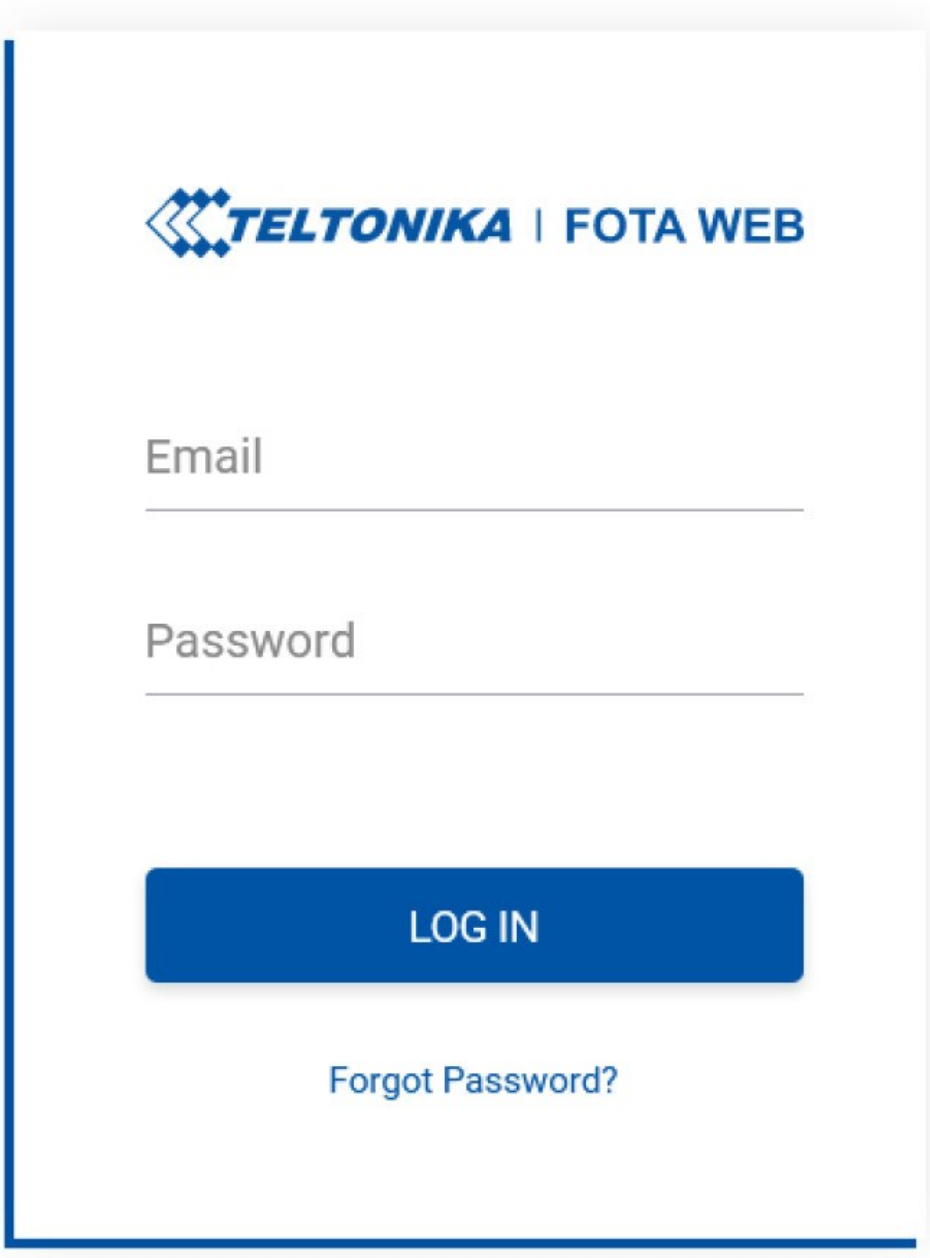
Indem Sie die Teltonika FMBT-Anwendung auf Smartphones verwenden und eine PIN für die Kopplung mit einem Tracker eingeben oder Ihr Gerät zur MAC-Liste der autorisierten Geräte des Konfigurators hinzufügen, können Sie jedes Detail Ihres Geräts sehen, einschließlich Primärinformationen, GNSS, GSM und I/O-Elemente Status, OBD und LV-CAN200/ALL-CAN300 Live-Daten. Um einen Tracker über eine Bluetooth®-Verbindung einzurichten, müssen Sie ein Schlüsselwort eingeben und die Anwendung ermöglicht Ihnen, die IP-Adresse Ihres Servers, den Port und die APN-Daten auf dem Gerät zu ändern.



FOTA WEB

Mit FOTA WEB haben Sie von überall auf der Welt einfachen Zugriff auf Ihre Flotte. Um die Firmware zu aktualisieren oder Konfigurationsänderungen vorzunehmen, müssen Sie lediglich einen Benutzernamen und ein Passwort in Ihren Browser eingeben, der das HTTPS-Protokoll verwendet – das bedeutet, dass die gesamte Kommunikation zwischen Ihrem Browser und der Website verschlüsselt

ist! Bitte geben Sie Ihre Anmeldedaten aus Sicherheitsgründen nicht an unbefugte Personen weiter.



BLE-STANDARD AES-128

Ab der Firmware-Basisversion **03.27.07** haben wir den Advanced Encryption Standard AES-128 erfolgreich implementiert, um die sicherste Übertragung von Bluetooth® Low Energy (auch bekannt als BLE)-Daten zwischen Teltonika GPS-Trackern und dedizierten mobilen Apps zu gewährleisten. Wenn ein AES-Schlüssel im

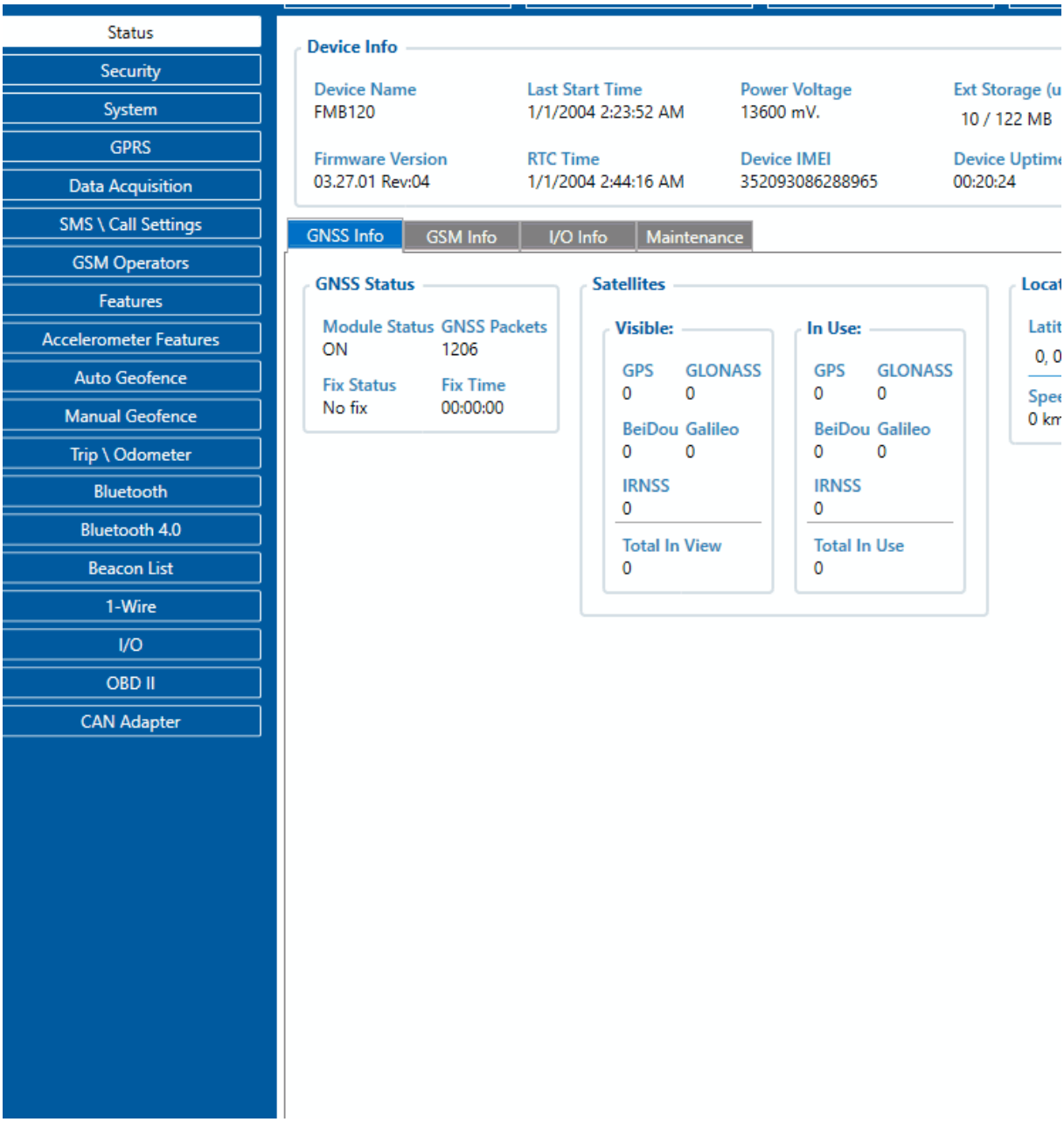
HEX-Format vorhanden ist, werden die ausgehenden Daten durch den konfigurierten Schlüssel verschlüsselt und die eingehenden Daten entschlüsselt.
Bitte beachten Sie, dass dies heute eines der robustesten und ausgefeiltesten seriellen Verschlüsselungsschemata ist. Weitere Informationen zu den technischen Aspekten dieser Funktion finden Sie hier .

BLUETOOTH®-PAIRING-PIN-ÄNDERUNG

Das Ändern der für die Bluetooth®-Kopplung verwendeten PIN kann eine wirksame Möglichkeit sein, unbefugten Zugriff auf Teltonika-GPS-Tracker zu verhindern. Die regelmäßige Aktualisierung dieser PIN bietet eine zusätzliche Sicherheitsebene. Darüber hinaus verfügt diese Funktion über mehrere verschiedene Sicherheitsmodi. Mehr zu den technischen Aspekten erfahren Sie hier .

SICHERE VERBINDUNG ZUM SERVER (TLS)

Darüber hinaus wurde ab der Basis-Firmware-Version **03.27.07** die Transport Layer Security TLS-Funktionalität aktualisiert und für die GPS-Geräteserien FMB0YX, FMB9X0, FMB1YX, FMM1YX, FMC1YX, FMB2YX und das Modell FMT100 von Teltonika implementiert. Bei der Schicht handelt es sich um ein kryptografisches Protokoll, das eine durchgängige Sicherheit der zwischen dem Server und dem GPS-Tracker des Fahrzeugs gesendeten Daten bietet. Mehr über die technischen Aspekte des TLS-Updates erfahren Sie hier .



VPN

Es bestehen Sicherheitsbedenken hinsichtlich der Verbindung privater Smartphones und mobiler Geräte mit Trackern. Privattelefone sind anfälliger für Hackerangriffe als Server, die mit einem Unternehmensnetzwerk verbunden sind. Viele Unternehmen bieten kostengünstige mobile Software an, die den Datenverkehr verschlüsselt oder Telefone auf verdächtige Aktivitäten überwacht. Bisher waren die Bedrohungen minimal und eher ärgerlich, aber man sollte sie im Auge behalten. Für eine sichere Verbindung können Sie eine SIM-Karte verwenden, die VPN-Konnektivität unterstützt. Mit einem VPN können Sie über das Internet eine sichere Verbindung zu einem anderen Netzwerk herstellen und Ihre Surfaktivitäten sichern.

VORTEILE

- **Sicherheitsoptionen für verschiedene Geräte** – stellen Sie sicher, dass Teltonika-Tracker in Ihrem Unternehmen sicher verwendet werden können, mit verschiedenen Sicherheitsoptionen (Schlüsselwörter, Anmeldungen, Passwörter, PINs und Listen autorisierter Nummern) für alle Arten von Geräten (Telefone, Smartphones, Computer, Server usw.) und FMBT-App) sorgen für die Sicherheit Ihrer Daten.
- **Schnelle Möglichkeit, sichere Anmeldungen zu konfigurieren** – im Teltonika-Konfigurator ist es einfach, Schlüsselwörter, Anmeldungen und Passwörter einzurichten oder zu ändern, autorisierte Telefonnummern hinzuzufügen oder die MAC-Liste der autorisierten Geräte zu füllen.
- **Sicherer Datenversand** – VPN-Datenverschlüsselung.

WARUM TELTONIKA?

Eine sichere Verbindung zu Teltonika-Trackern gibt Ihnen die Gewissheit, dass Ihre sensiblen Geschäftsdaten sicher sind und niemand sonst eine Verbindung zu den Geräten herstellen kann. Unter unserem Motto „Easy Key to IoT“ bieten wir eine schnelle Möglichkeit zur Einrichtung von Sicherheitsanmeldungen, Passwörtern oder Schlüsselwörtern sowie problemlose Firmware-Upgrades und Konfiguration von Teltonika-Trackern.