

Benutzerdokumentation

CipherLab RS36 für CGM AMOR Mobile und CGM MUSE Mobile

Copyright © Aescudata GmbH – All rights reserved

Dieses Dokument ist **vertraulich** zu behandeln und darf nicht ohne Zustimmung der Aescudata GmbH vervielfältigt, veröffentlicht oder an Dritte weitergegeben werden.

© Aescudata GmbH

Inhaltsverzeichnis

1	Barcodescanner	3
1.1	CipherLab RS36 für CGM AMOR Mobile und CGM MUSE Mobile	3
1.1.1	Ersteinrichtung	3
1.1.2	Firmware aktualisieren	4
1.1.3	Android Einstellungen	5
1.1.4	App installieren	10
1.1.5	ReaderConfig Einstellungen	11
1.1.6	AppLock einrichten	27
1.1.7	CGM MUSE Mobile installieren	28
1.1.8	Unbekannte Apps installieren	28
1.1.9	Zusatzfunktionen	28
1.1.10	Fernwartungszugriff	29
1.1.11	Remote Desktop Client	29

1 Barcodescanner

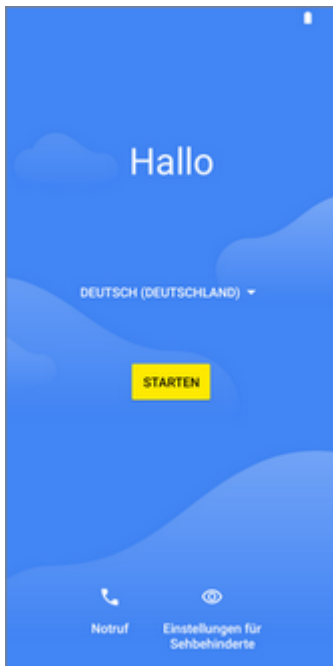
Nachfolgend werden die Informationen zum Barcodescanner und die Konfiguration beschrieben.

1.1 CipherLab RS36 für CGM AMOR Mobile und CGM MUSE Mobile

Nachfolgend finden Sie Informationen zum Einrichten des Barcodescanners **CipherLab RS36** für CGM AMOR Mobile und CGM MUSE Mobile.

1.1.1 Ersteinrichtung

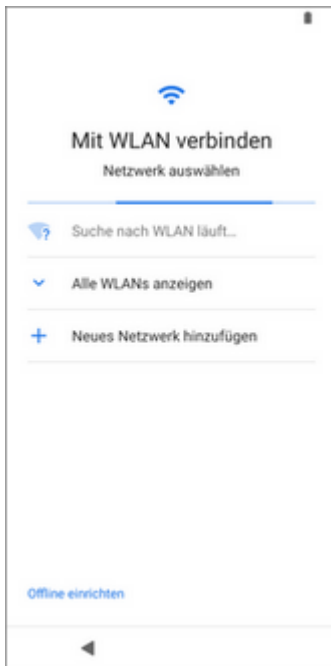
Wird der PDA das erste Mal gestartet, öffnet sich der Dialog für die Ersteinrichtung. Wählen Sie die gewünschte Sprache und Starten Sie die Ersteinrichtung.



CipherLab RS36 - Startbildschirm
Ersteinrichtung

Folgen Sie den vorgegebenen Einrichtungsschritten. Das Scannen des Barcodes und die Einrichtung der Mobilfunkverbindung kann übersprungen werden.

Das WLAN können Sie zu diesem Zeitpunkt bereits hinzufügen, da es für das Firmwareupdate benötigt wird. Nach der Fertigstellung sollte es wieder entfernt werden.



CipherLab RS36 - WLAN einrichten

Danach folgt eine Abfrage, ob Apps & Daten kopiert werden sollen. Treffen Sie eine Auswahl und überspringen Sie im nächsten Schritt die Anmeldung eines Google-Kontos.

Die Displaysperre wird standardmäßig deaktiviert. Dafür müssen Sie eine Sicherheitsabfrage bestätigen.

Nach der Ersteinrichtung wird der Home-Bildschirm angezeigt.

1.1.2 Firmware aktualisieren

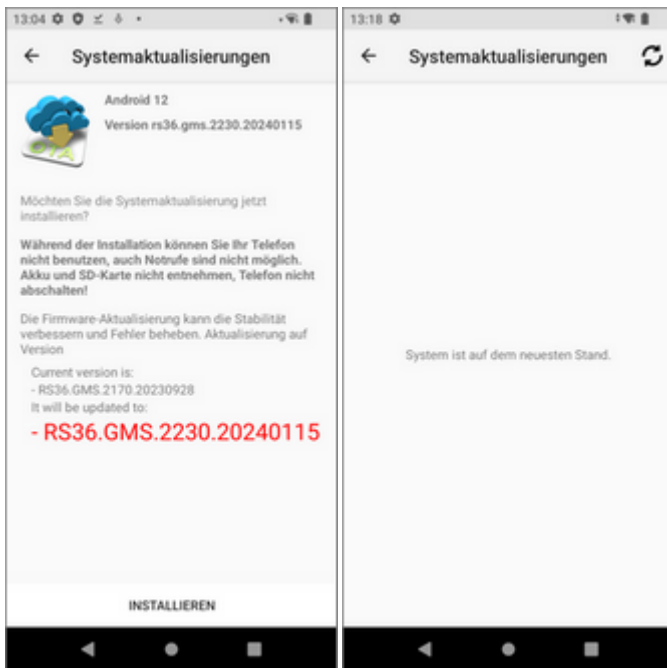
Die Version sollte vor dem Ausliefern immer auf den aktuellsten Stand gebracht werden. In der Erstellungsversion steht am Ende das Versionsdatum.

Zuerst muss eine WLAN-Verbindung hergestellt werden.

Firmwareupdates sind **kein Kumulativupdate**, d. h. die Suche nach Updates und die Aktualisierung der Firmware muss so lange wiederholt werden, bis die Meldung **System ist auf dem neuesten Stand** erscheint.

Durch ein Firmwareupdate gehen alle ReaderConfig Einstellungen verloren!

Wiederholen Sie den Vorgang so lange, bis Sie in den **Systemaktualisierungen** die Meldung **System ist auf dem neuesten Stand** erhalten.

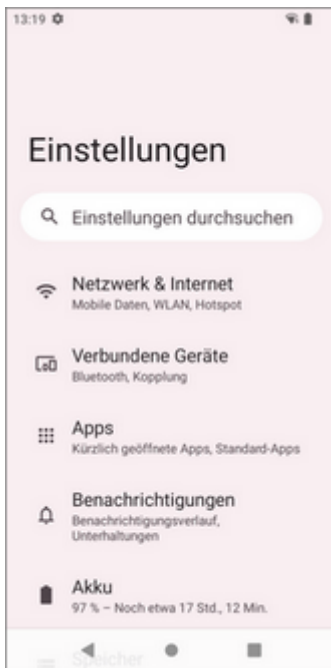


CipherLab RS36 -
Systemaktualisierung

CipherLab RS36 -
Systemaktualisierung: System ist auf
dem neuesten Stand

Nach dem Firmwareupdate entfernen Sie die WLAN-Verbindung wieder.

1.1.3 Android Einstellungen

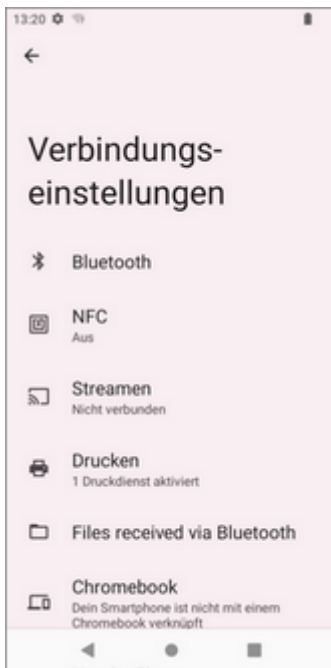


CipherLab RS36 - Einstellungen

Folgende Einstellungen sind in den Android Einstellungen zu treffen.

Netzwerk & Internet

- WLAN entfernen und deaktivieren (→ Internet)

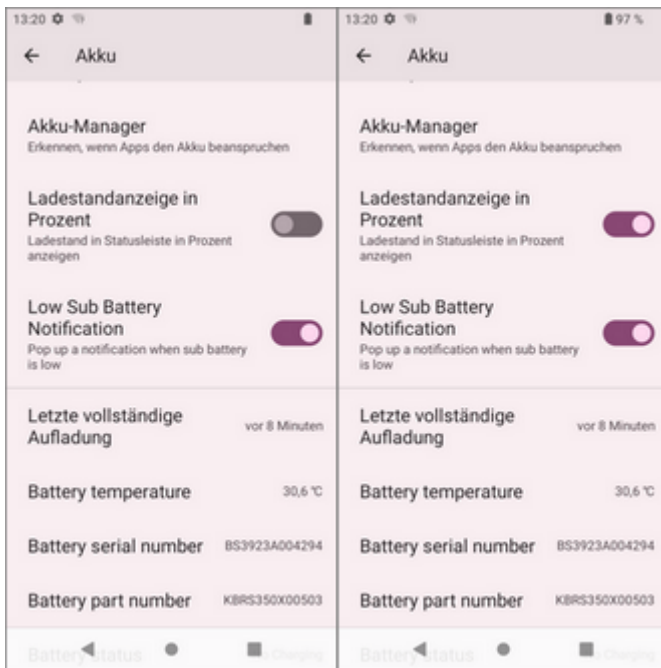


Verbundene Geräte → Verbindungseinstellungen

- Bluetooth deaktivieren
- NFC ausschalten

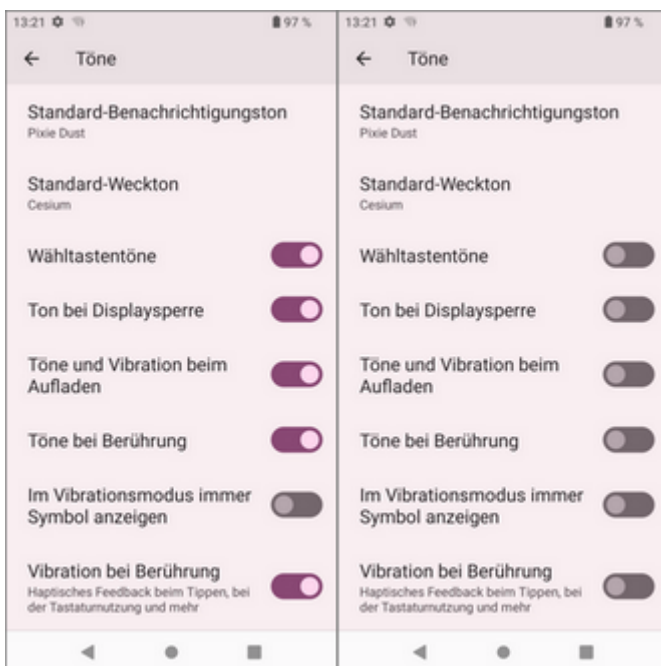
Akku

- Ladestandanzeige in Prozent aktivieren



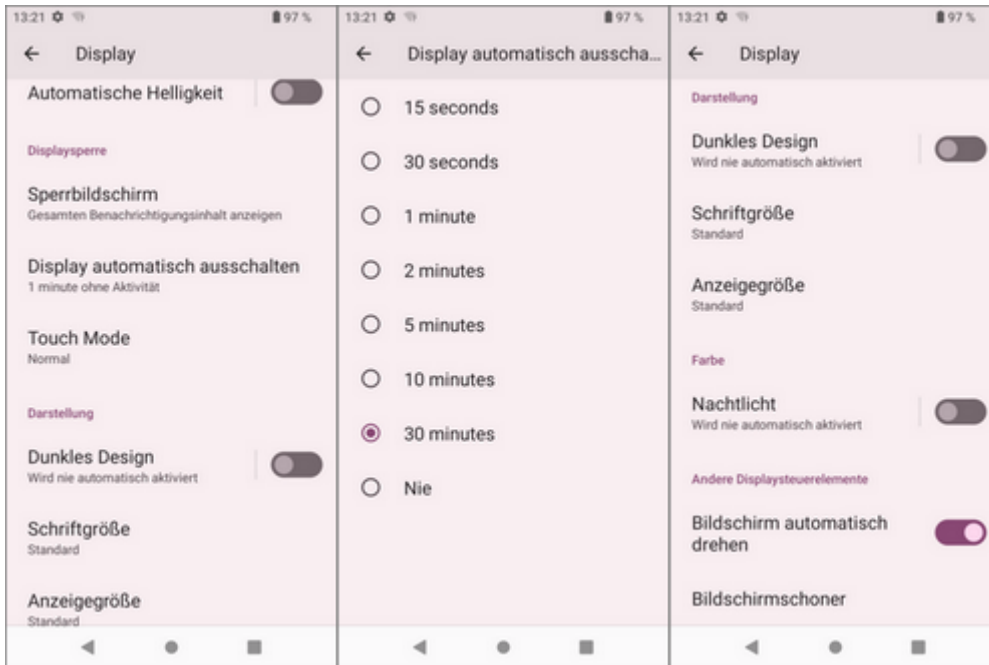
Töne

- Wähltastentöne ausschalten
- Ton bei Displaysperre ausschalten
- Töne und Vibration beim Aufladen ausschalten
- Töne bei Berührung ausschalten
- Vibration bei Berührung ausschalten



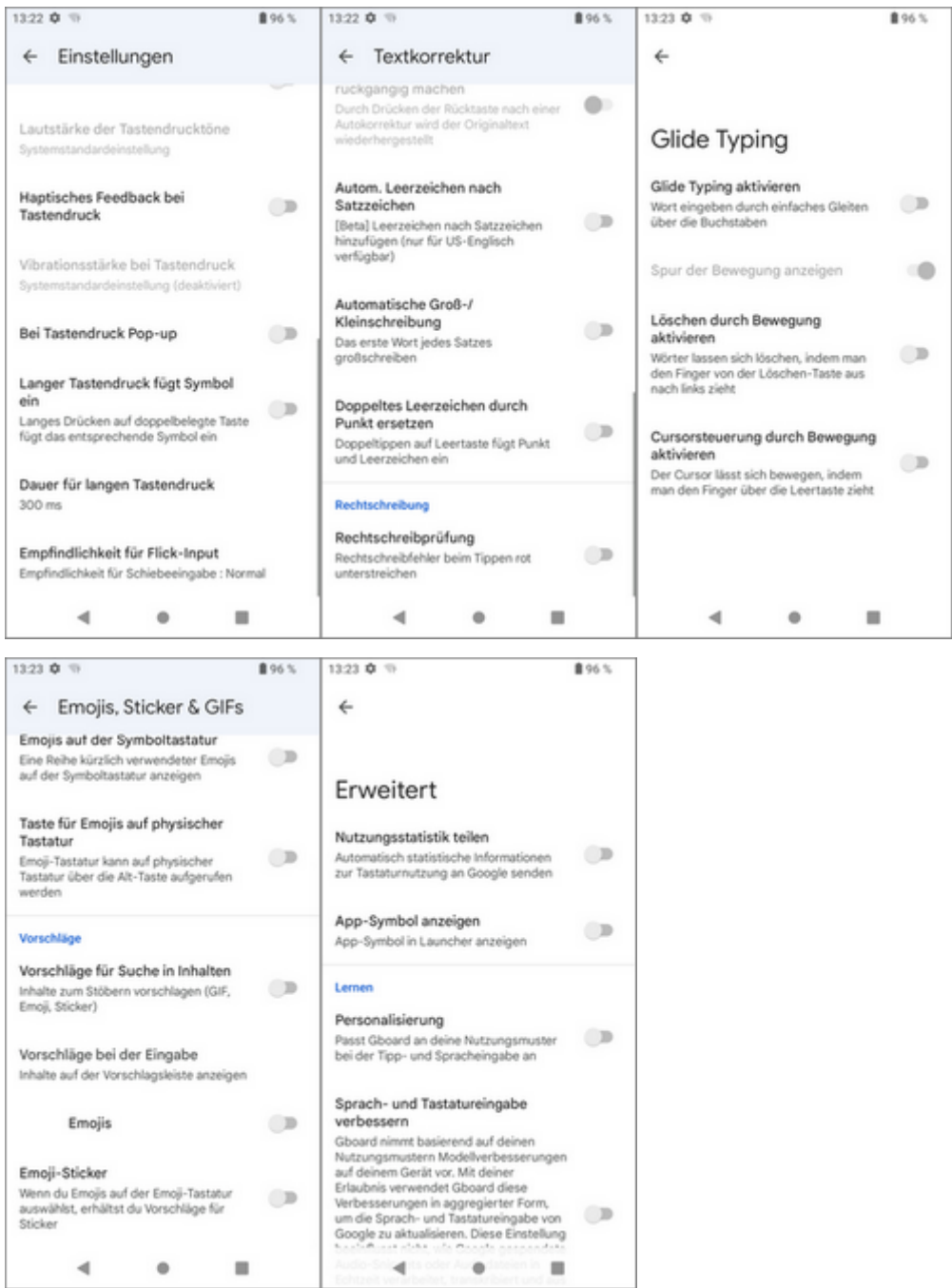
Display

- Automatische Helligkeit deaktivieren
- Display automatisch ausschalten: nach 30 Minuten
- Bildschirm automatisch drehen deaktivieren



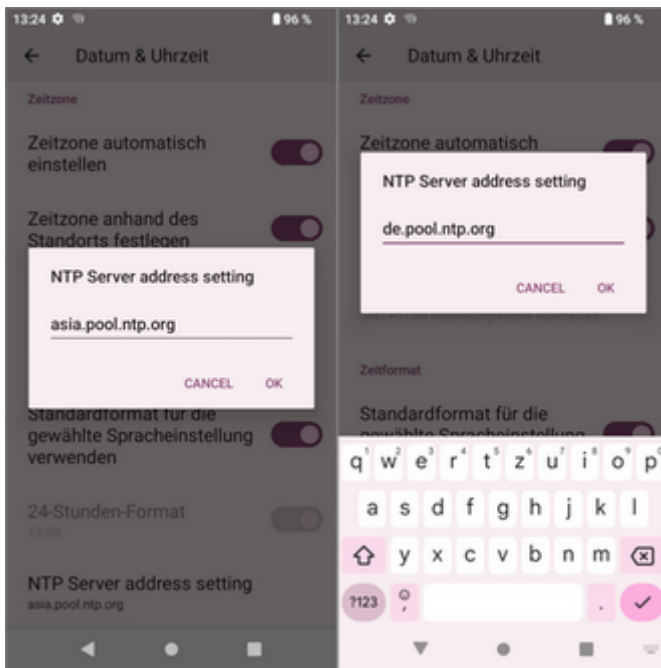
System → Sprachen und Eingabe → Bildschirmtastatur → Gboard

- Einstellungen: Alles deaktivieren
- Textkorrektur: Alles deaktivieren
- Glide Typing: Alles deaktivieren
- Emojis, Sticker & GIFs: Alles deaktivieren
- Erweitert: Alles deaktivieren



System → Datum & Uhrzeit

- NTP Server anpassen: von **asia.pool.ntp.org** auf **de.pool.ntp.org** ändern
- 24-Stunden-Format aktivieren



Datenschutz → Erweitert → Werbung

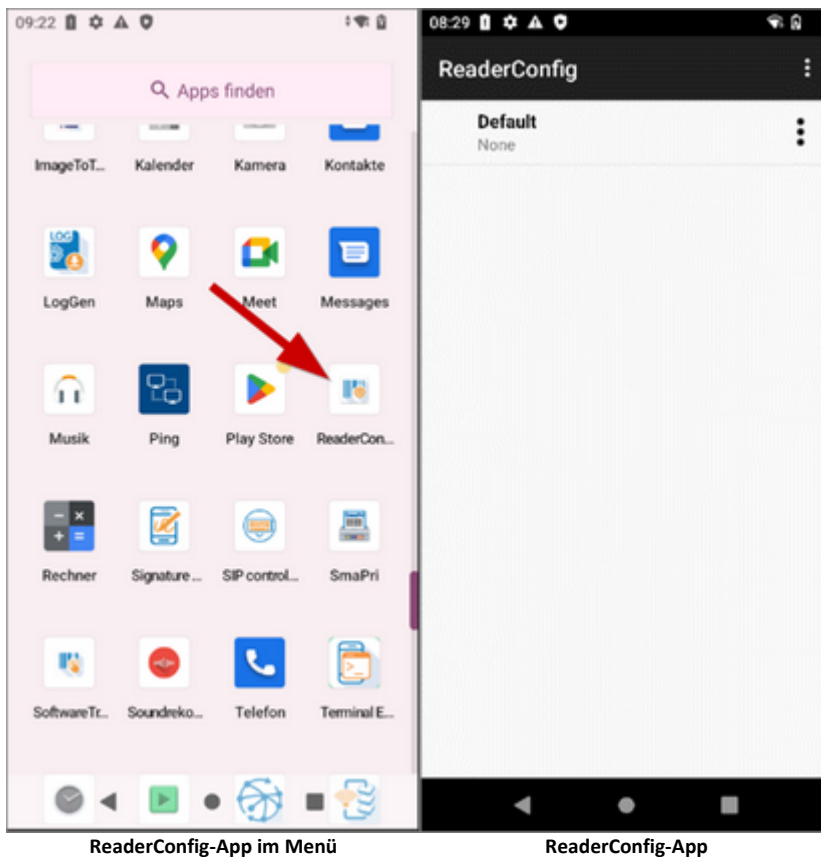
- Personalisierte Werbung deaktivieren

1.1.4 App installieren

Die Installation erfolgt über

Die Dateien können einfach via USB-Kabel vom PC auf den PDA übertragen werden. Für die Dateiablage bietet sich das Download-Verzeichnis an. Sobald die Dateien übertragen wurden, kann der Pfad über den **Dateimanager** (Hauptmenü) auf dem PDA aufgerufen und die APK-Dateien können installiert werden. Abfragen werden mit **Weiter** bestätigt.

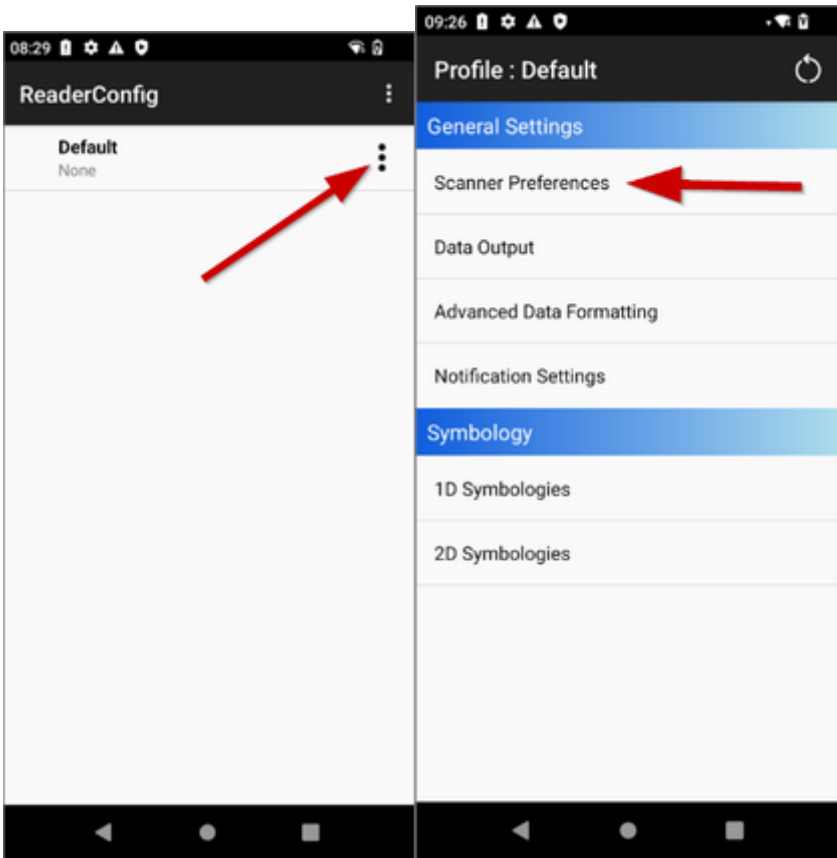
1.1.5 ReaderConfig Einstellungen



Folgende Einstellungen sind in der ReaderConfig zu treffen.

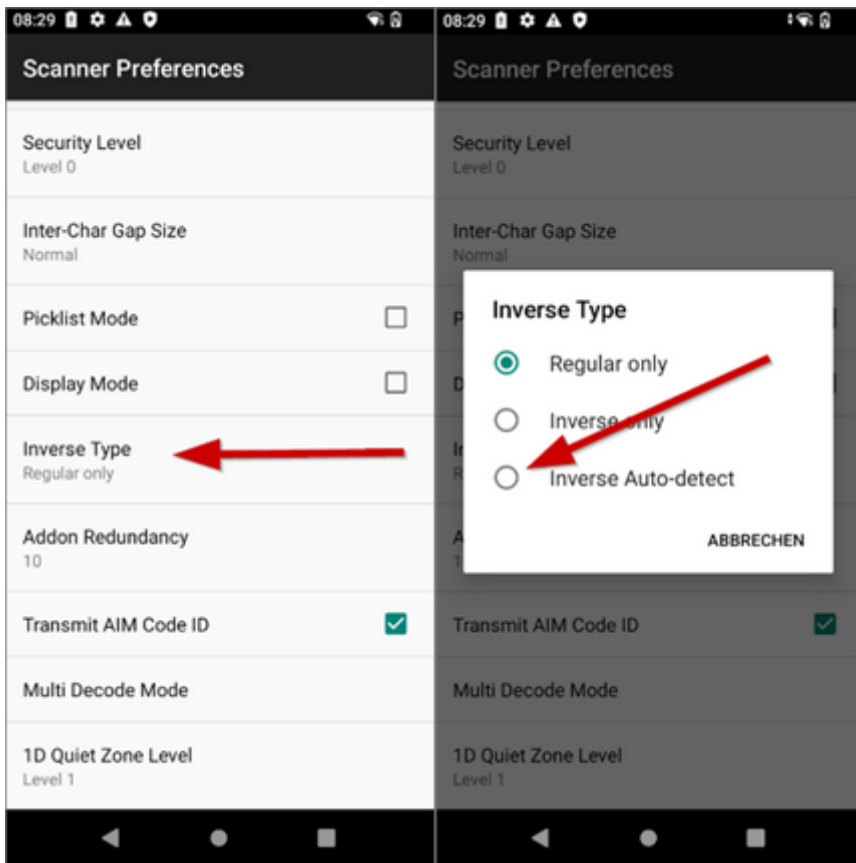
Default - Scanner Preferences

Inverse Type: Inverse Auto-detect



ReaderConfig-App: Einstellungen öffnen

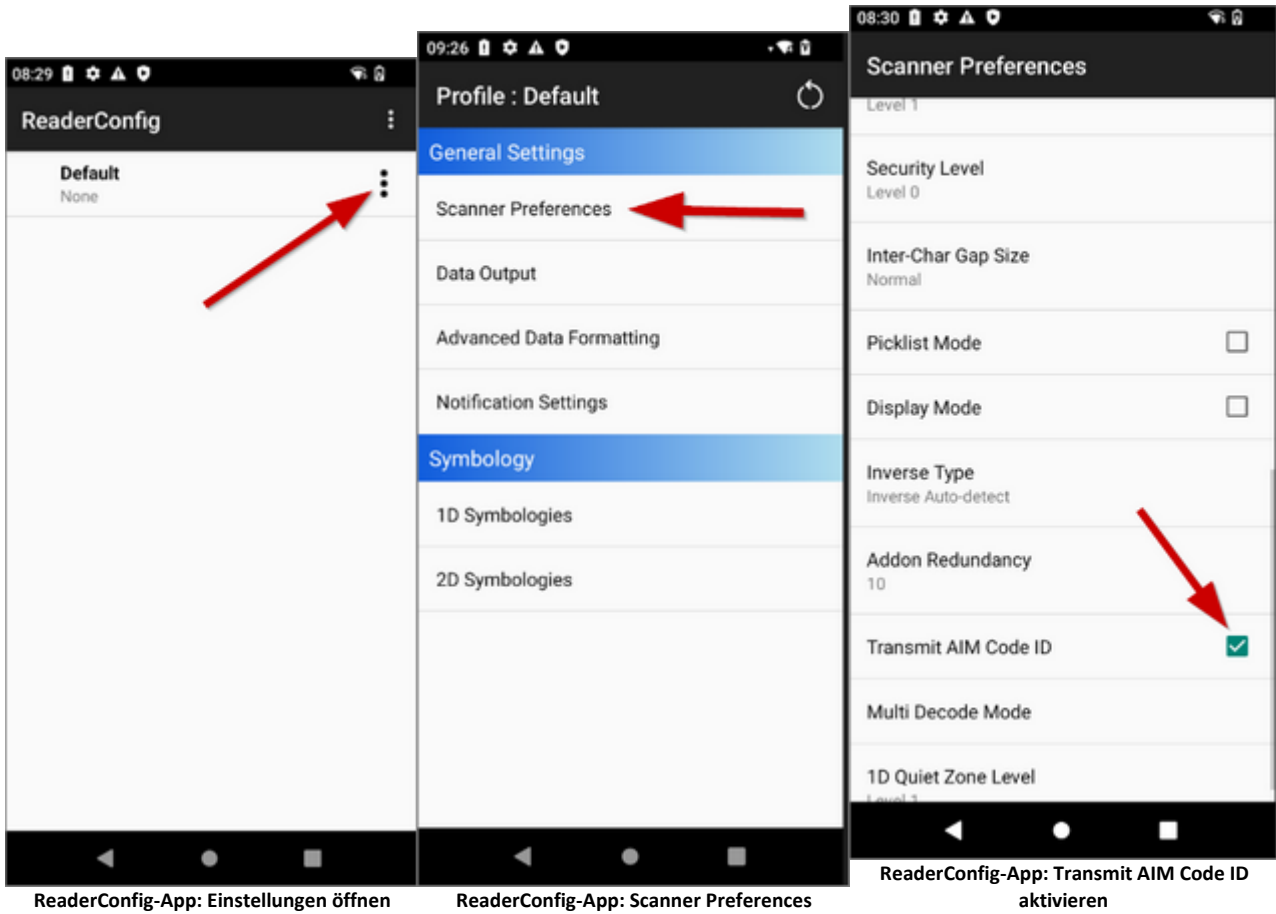
ReaderConfig-App: Scanner Preferences



ReaderConfig-App: Inverse Type

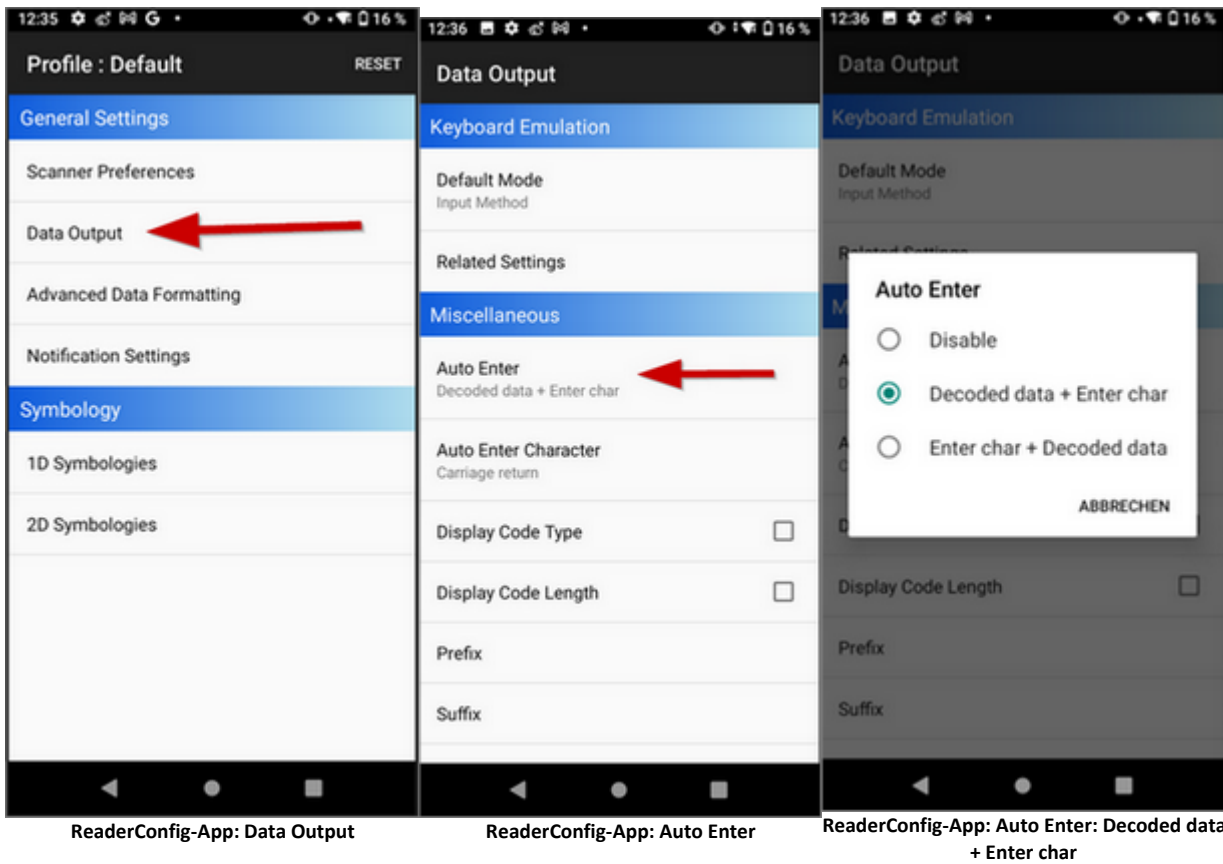
ReaderConfig-App: Inverse Auto-detect

Transmit AIM Code ID: Aktivieren



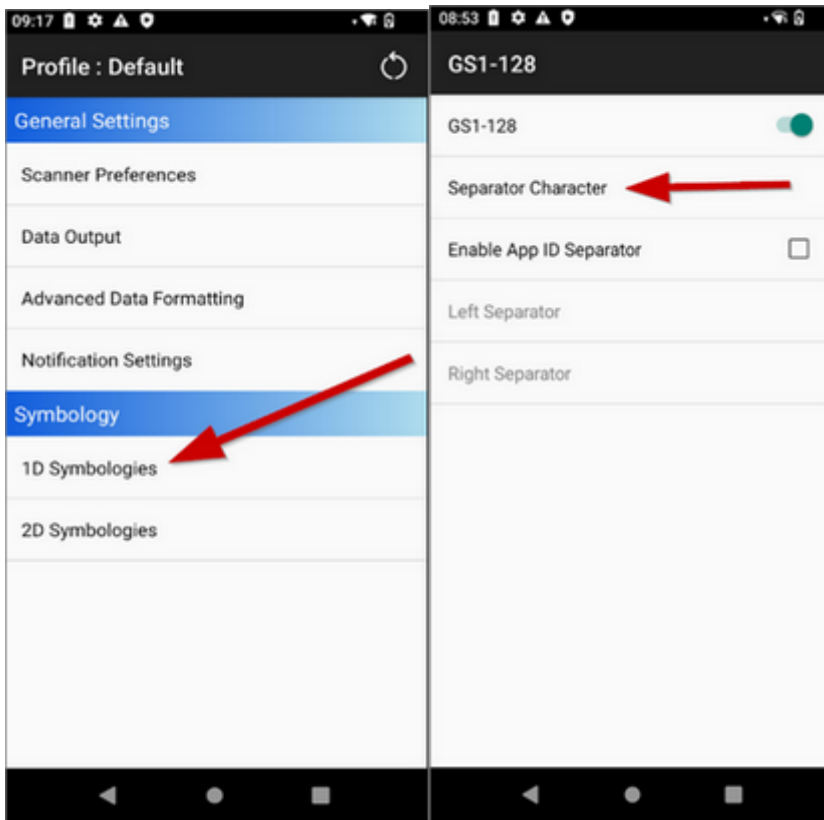
Data Output

Auto Enter: Decoded data + Enter char



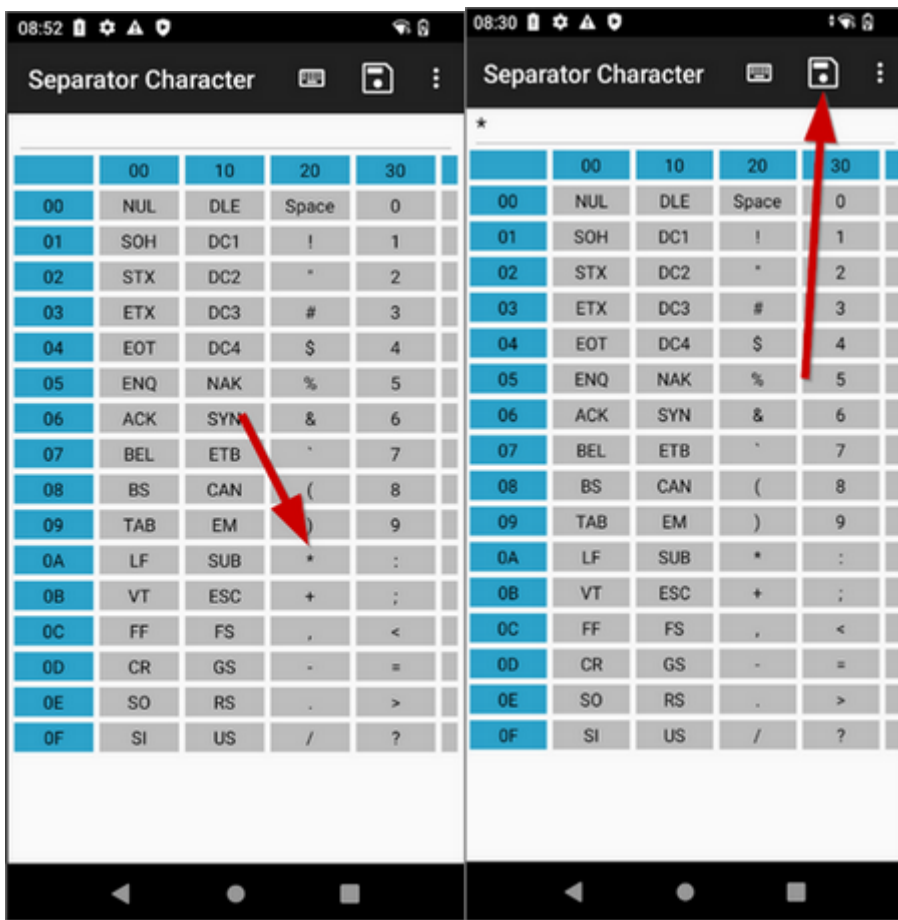
1D Symbologies

Separator Character: *



ReaderConfig-App: 1D Symbologies

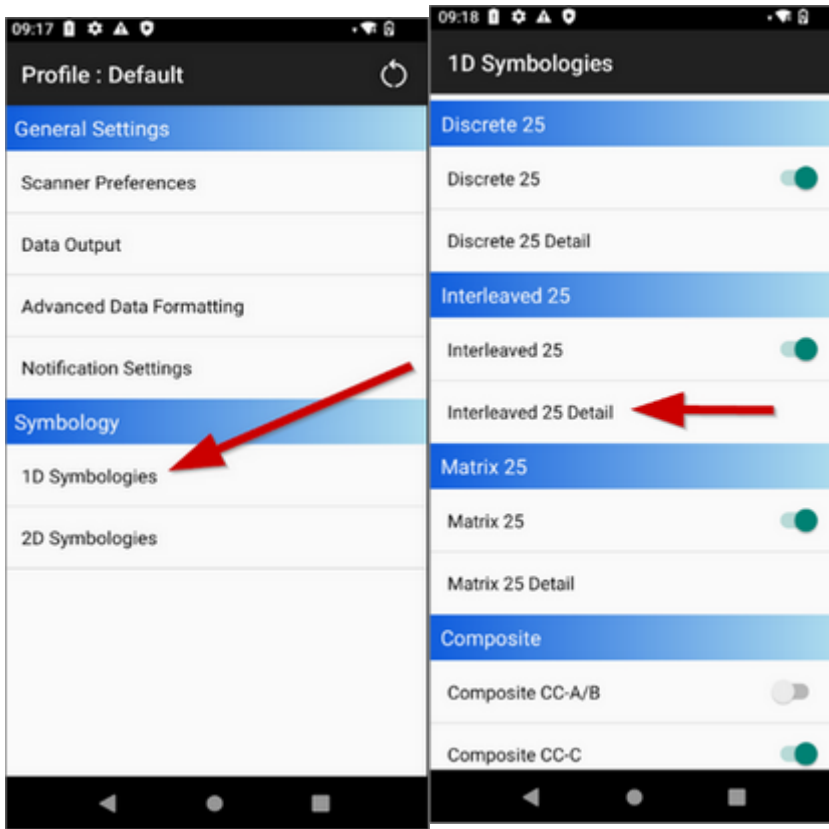
ReaderConfig-App: Separator Character



ReaderConfig-App: * auswählen

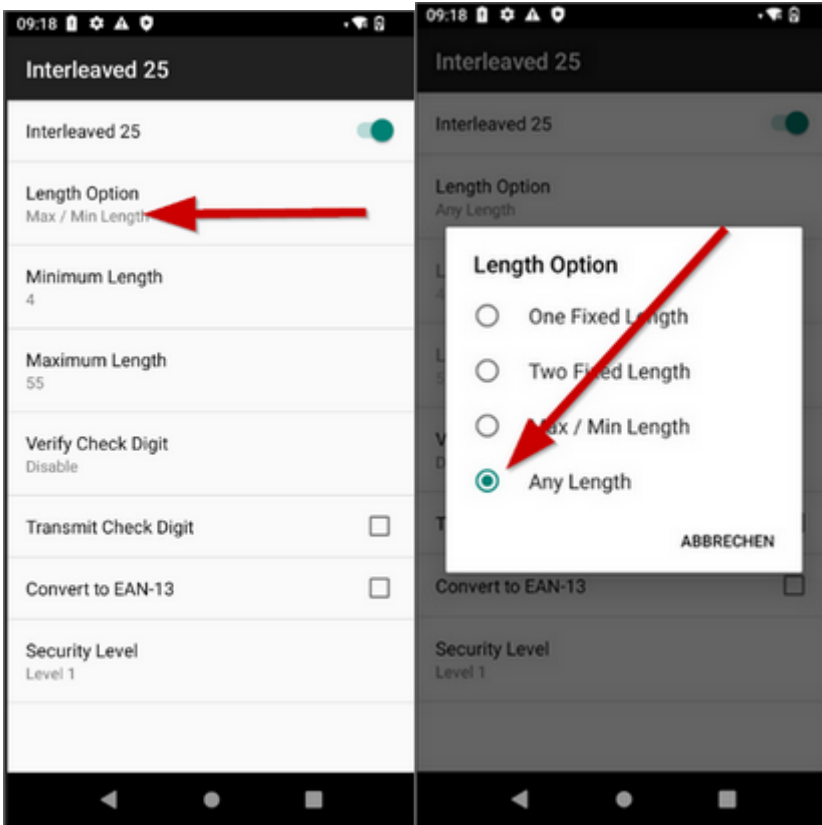
ReaderConfig-App: Symbol speichern

Interleaved 25 Detail: Zeichenlänge ist Any Length



ReaderConfig-App: 1D Symbologies

ReaderConfig-App: 1D Symbologies -
Interleaved 25 Detail

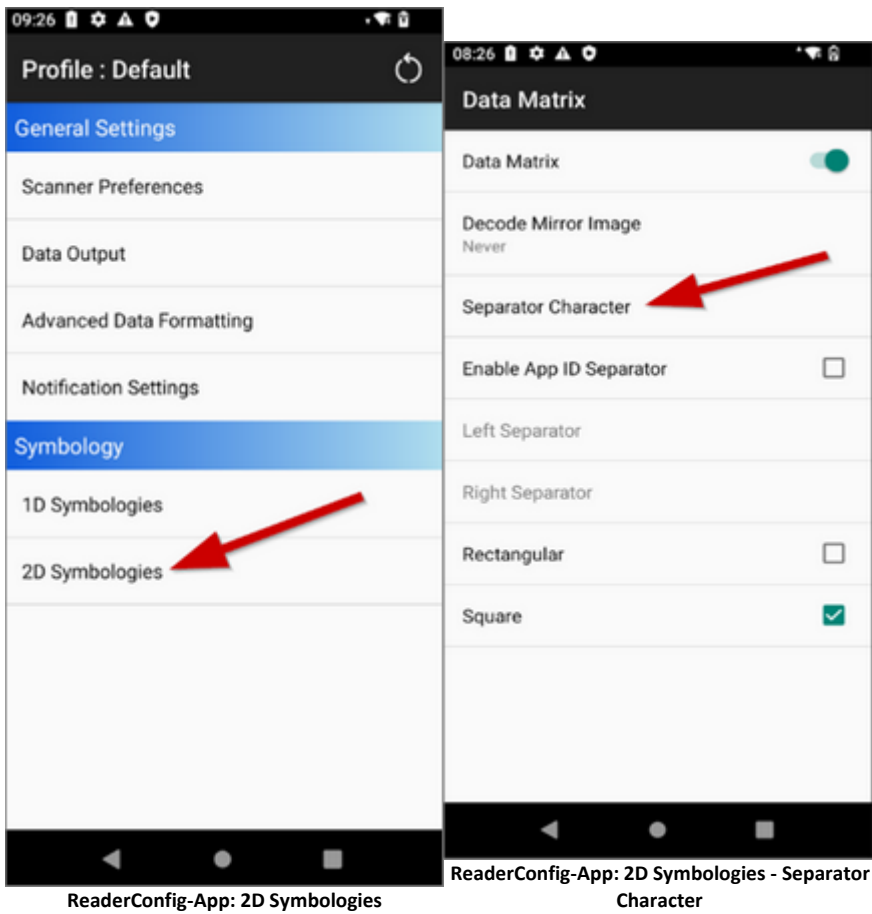


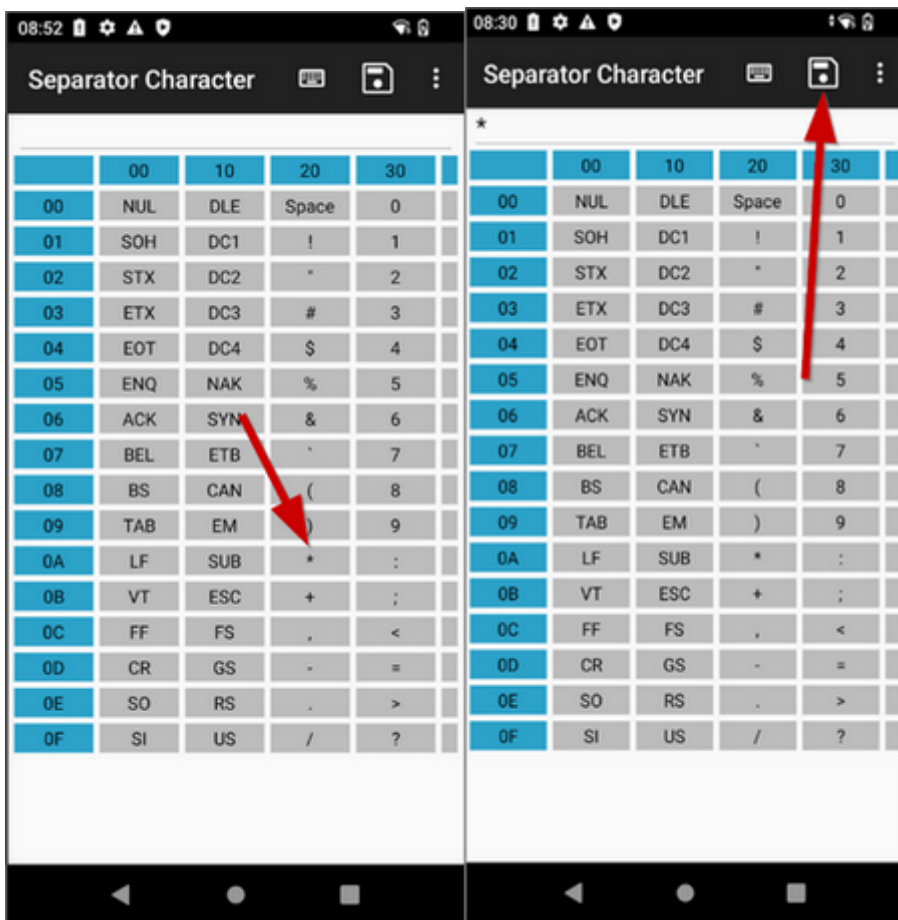
ReaderConfig-App: 1D Symbolologies - Length Option

ReaderConfig-App: 1D Symbolologies - Any Length

2D Symbologies

Separator Character (Data Matrix): *



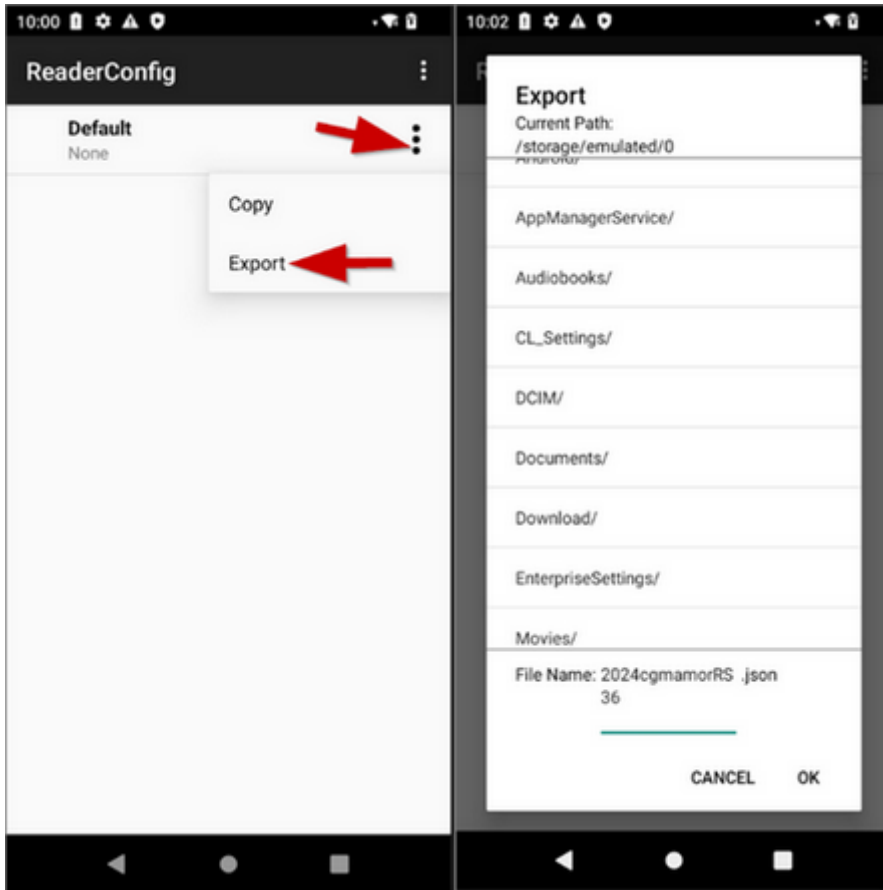


ReaderConfig-App: * auswählen

ReaderConfig-App: Symbol speichern

ReaderConfig Export

Zum Exportieren der ReaderConfig klicken Sie im Menü auf **Export** und definieren Sie einen sprechenden Namen. Der vorgeschlagene Speicherort kann für den Export verwendet werden.

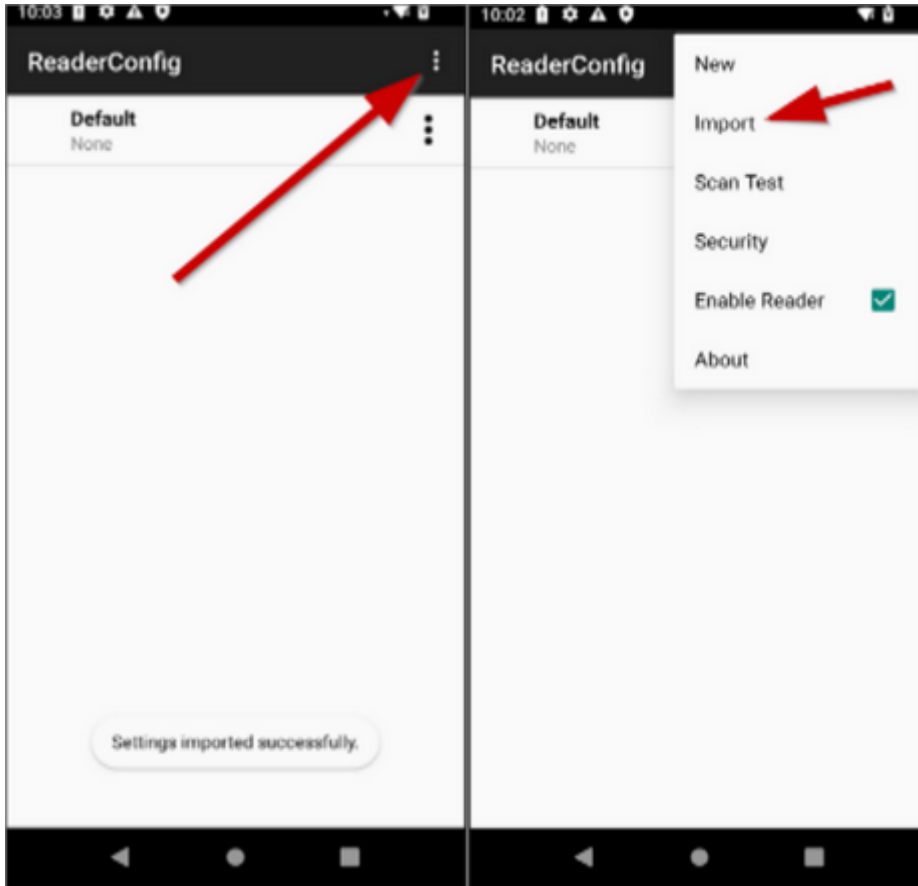


ReaderConfig-App: Menü - Export

ReaderConfig: Export

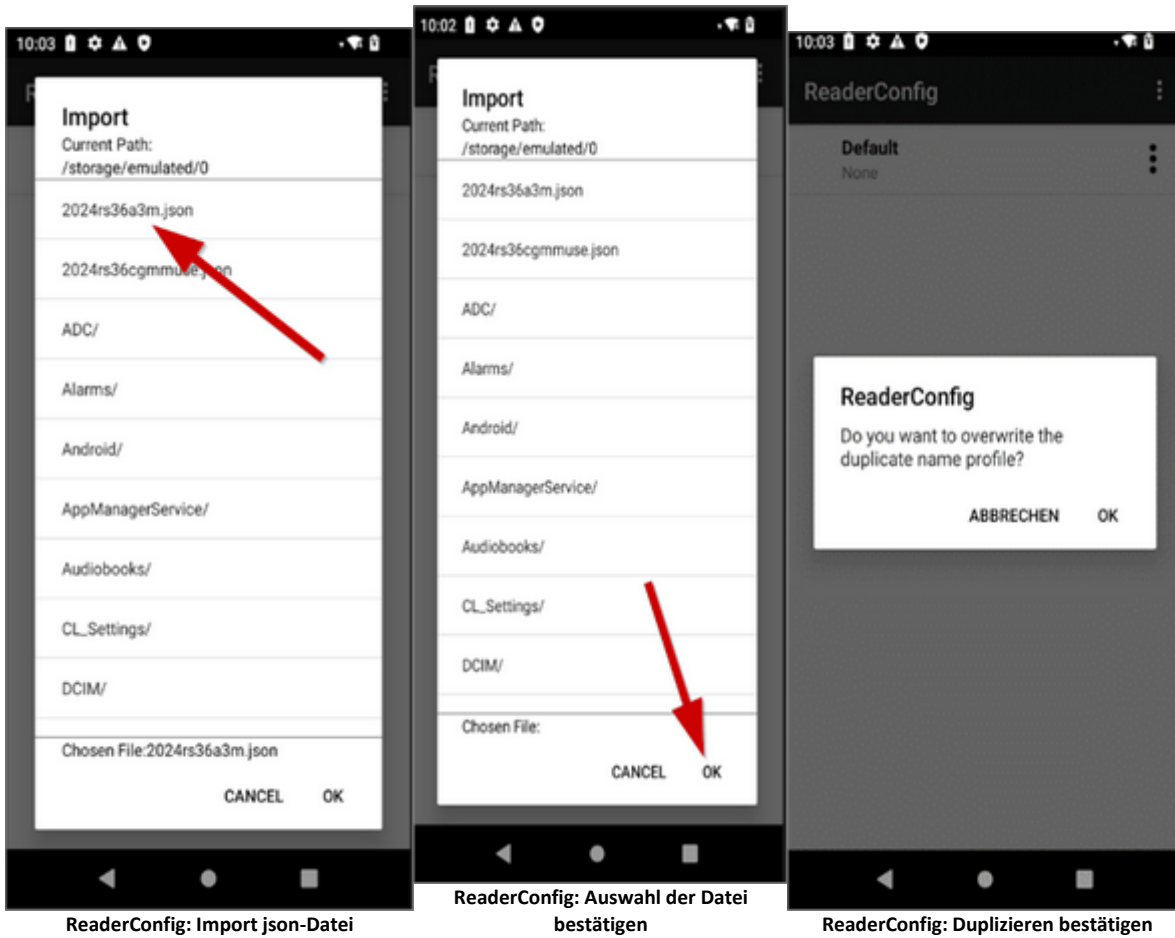
ReaderConfig Import

Zum Importieren der ReaderConfig klicken Sie im Menü auf **Import** und wählen Sie die **.json**-Datei aus. Über **OK** wird der Import gestartet.



ReaderConfig: Einstellungen

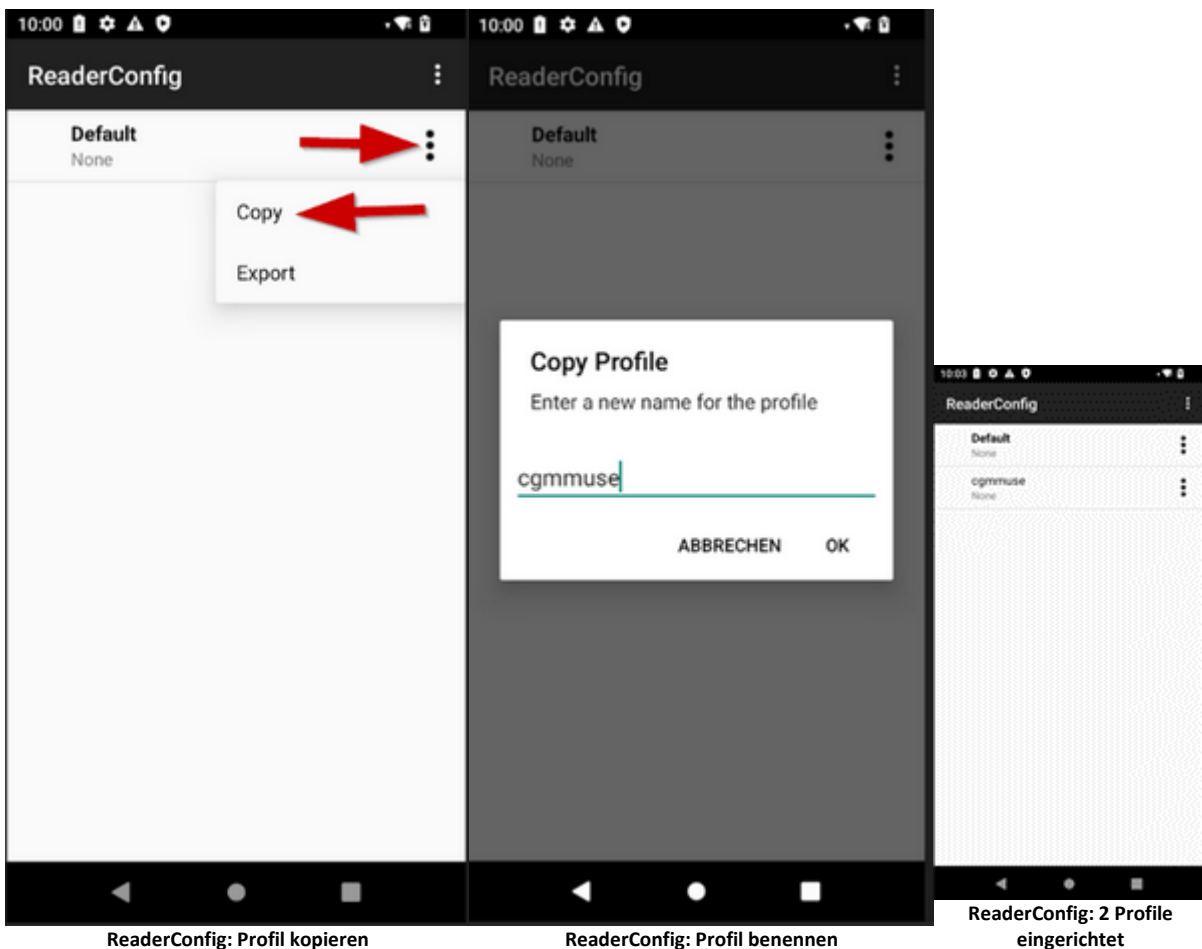
ReaderConfig: Import



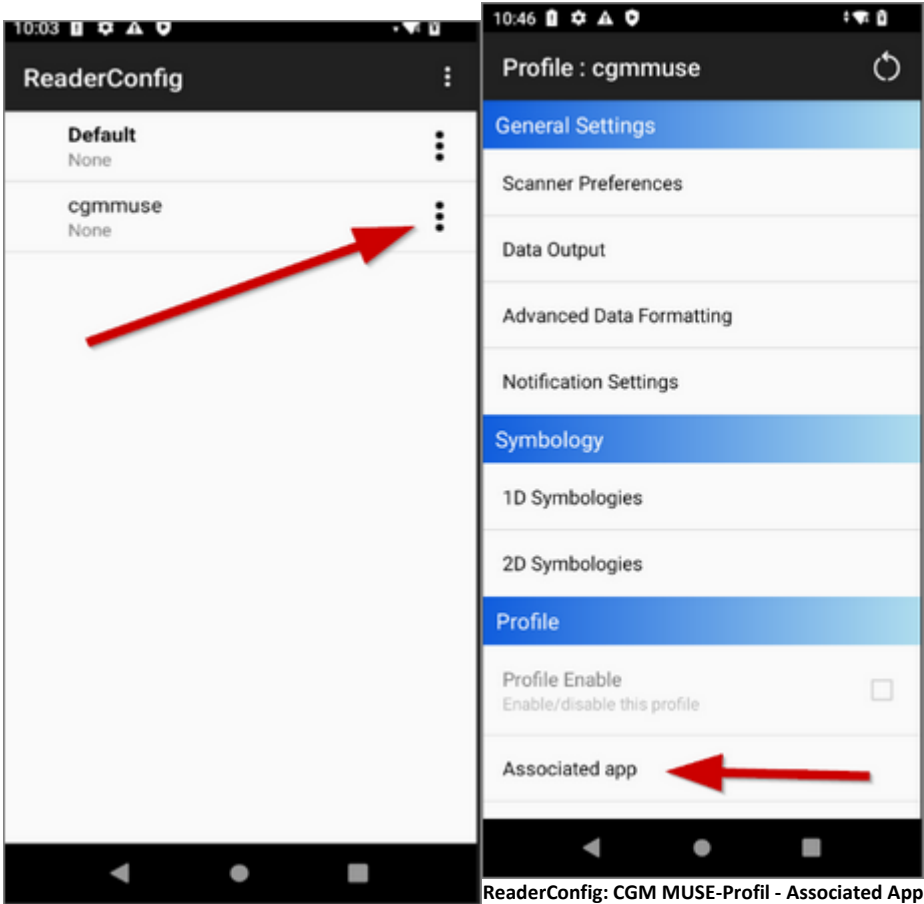
CGM MUSE Mobile

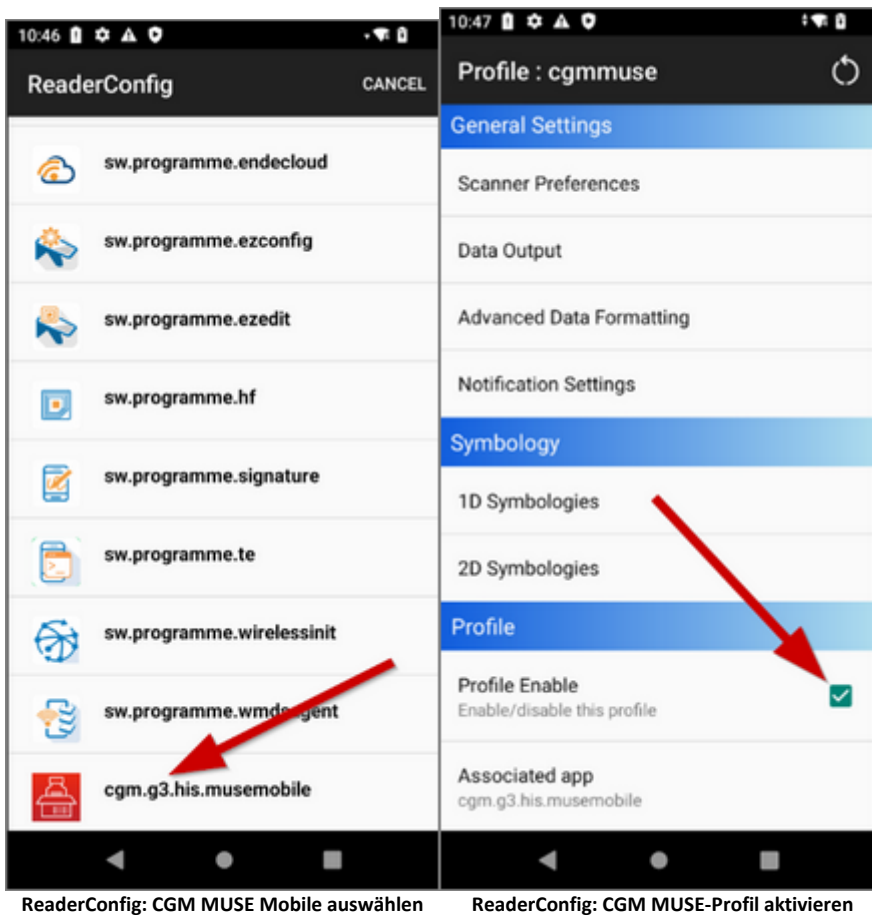
CGM MUSE Mobile: Für die Nutzung des CipherLab RS36 in Verbindung mit CGM MUSE Mobile muss **Auto Enter Character** auf **LF Character** eingestellt werden. Danach muss CGM MUSE Mobile unter **Profile** hinzugefügt und aktiviert werden.

Bei einer gemeinsamen Nutzung mit CGM AMOR Mobile hat dies zur Folge, dass je Produkt eine eigene Konfiguration auf dem Gerät hinterlegt werden muss.



Anschließend muss CGM MUSE Mobile zu dem erstellten Profil hinzugefügt und das Profil aktiviert werden.





1.1.6 AppLock einrichten

Damit die Anwender nicht den vollen Zugriff auf alle Apps des Geräts bekommen, muss **AppLock** eingerichtet werden.

Je nach Beauftragung müssen folgende Apps hinzugefügt werden:

- AnyDesk
- CGM MUSE Mobile
- Citrix Receiver
- Uhr
- Rechner
- Terminalclient
- VA Scan

Über das **Apps Management** können die Programme hinzugefügt werden. Wählen Sie alle benötigten Apps an, ausgenommen CGM MUSE Mobile (siehe dazu Kapitel CGM MUSE Mobile installieren). Wird kein CGM MUSE Mobile verwendet, kann AppLock (über die drei Punkte rechts oben) auf **User Mode** gestellt werden.

1.1.7 CGM MUSE Mobile installieren

Die Scanner- und PDA-Einstellungen für CGM MUSE Mobile und CGM AMOR Mobile sind gleich.

Die aktuellste zu installierende APK-Datei liegt im CGM MUSE Auslieferungsverzeichnis. Nach der Installation kann CGM MUSE Mobile zum **AppLock** hinzugefügt werden.

Ein **Cold Boot** löscht **alle** Programme und Einstellungen des PDA und setzt diesen auf den (Hersteller-) Auslieferungszustand zurück. In diesem Fall muss die Datensicherung zurückgespielt oder der PDA manuell eingerichtet und GCM MUSE Mobile neu installiert werden.

1.1.8 Unbekannte Apps installieren

Es gibt keine globale Option, um die Installation unbekannter Apps aktivieren zu können. Daher muss dies nach der Installation der benötigten Apps unter **Apps & Benachrichtigungen - Erweitert - Spezieller App-Zugriff - Installieren unbekannter Apps** pro App einzeln berechtigt werden.

1.1.9 Zusatzfunktionen

Profile anlegen

In der ReaderConfig können verschiedene Scan-Profile für verschiedene Apps angelegt werden. Dafür muss ein neues Profil erstellt und die gewünschte App ausgewählt werden. Nach der Erstellung kann das Profil umbenannt, kopiert, exportiert und auch wieder gelöscht werden.

Für alle anderen Apps gilt weiterhin das **Default**-Profil.

ReaderConfig sperren

Um zu verhindern, dass jeder Anwender die ReaderConfig ändern kann, besteht die Möglichkeit, ein Kennwort zu vergeben und damit die ReaderConfig zu sperren. Wahlweise können alle Funktionen oder auch nur einzelne (z. B. Import, Export) gesperrt werden.

Mehrfachscan

In der ReaderConfig gibt es die Möglichkeit, einen Mehrfachscan zu aktivieren. Das bedeutet, dass die Scannertaste dauerhaft gedrückt wird und so mehrere Barcodes abgescannt werden können. Die Option **Picklist Mode** verhindert, dass ein Barcode während des Scanvorgangs mehrfach gescannt wird.

Folgende Einstellungen müssen gesetzt werden, um den Mehrfachscan zu aktivieren:

- Scan Mode: Presentation Mode
- Presentation Trigger: Aktivieren
- Picklist Mode: Aktivieren

Schnelleres Scannen

Barcodes können ohne weitere Einstellungen gescannt werden, allerdings dauert das Scannen teilweise recht lange. Unter **Data Output - Keyboard Emulation** kann der **Default Mode** auf **KeyEvent** und der zugehörige **Optimization Mode** auf **Via Activity** eingestellt werden. Dadurch wird die Scanzzeit minimiert.

1.1.10 Fernwartungszugriff

Der Zugriff via Fernwartung ist mit AnyDesk möglich. Die Fernsteuerung ist mit einem AddOn verfügbar.

Für den Erstzugriff müssen folgende Abfragen bestätigt werden:

- AnyDesk nimmt alle auf deinem Bildschirm angezeigten Aktivitäten auf
- Zulassen, dass die App AnyDesk auf Fotos, Medien und Dateien auf deinem Gerät zugreifen darf?
- Sicherheitswarnung
- Eingehende Verbindungsanfrage
- Einblendung über anderen Apps zulassen

1.1.11 Remote Desktop Client

Als Remote Desktop Client ist der **Parallels Client** zu verwenden, da nur dieser Client die Möglichkeit bietet, die Auflösung auf 540 x 1080 (Custom) einzustellen. Diese Auflösung passt am besten für CGM AMOR Mobile, weil hier die Auswahl von Entnahmelagerbereichen und dergleichen noch groß genug dargestellt wird.

Erfolg durch Kompetenz und Engagement.

CGM – CompuGroup Medical SE & Co. KGaA

CompuGroup Medical ist eines der führenden E-Health Unternehmen weltweit und erwirtschaftete im Jahr 2023 einen Jahresumsatz von EUR 1,19 Mrd. Die Softwareprodukte des Unternehmens zur Unterstützung aller ärztlichen und organisatorischen Tätigkeiten in Arztpraxen, Apotheken, Laboren, Krankenhäusern und sozialen Einrichtungen, die Informationsdienstleistungen für alle Beteiligten im Gesundheitswesen und die webbasierten persönlichen Gesundheitsakten dienen einem sichereren und effizienteren Gesundheitswesen.

Grundlage der CompuGroup Medical-Leistungen ist die einzigartige Kundenbasis, darunter Ärzte, Zahnärzte, Apotheken, weitere Gesundheitsprofis in ambulanten und stationären Einrichtungen sowie Versicherungs- und Pharma-Unternehmen. CompuGroup Medical unterhält eigene Standorte in 20 Ländern und vertreibt Produkte in 60 Ländern weltweit. Über 9.000 hochqualifizierte Mitarbeiterinnen und Mitarbeiter stehen für nachhaltige Lösungen bei ständig wachsenden Anforderungen im Gesundheitswesen.

We create the future of e-Health.

Aescudata GmbH

Lindenplatz 2

20099 Hamburg

vertrieb@aescudata.de

T +49 (0) 40-74 325 19-92

F +49 (0) 40-74 325 19-99

aescudata.de

cgm.com/de

